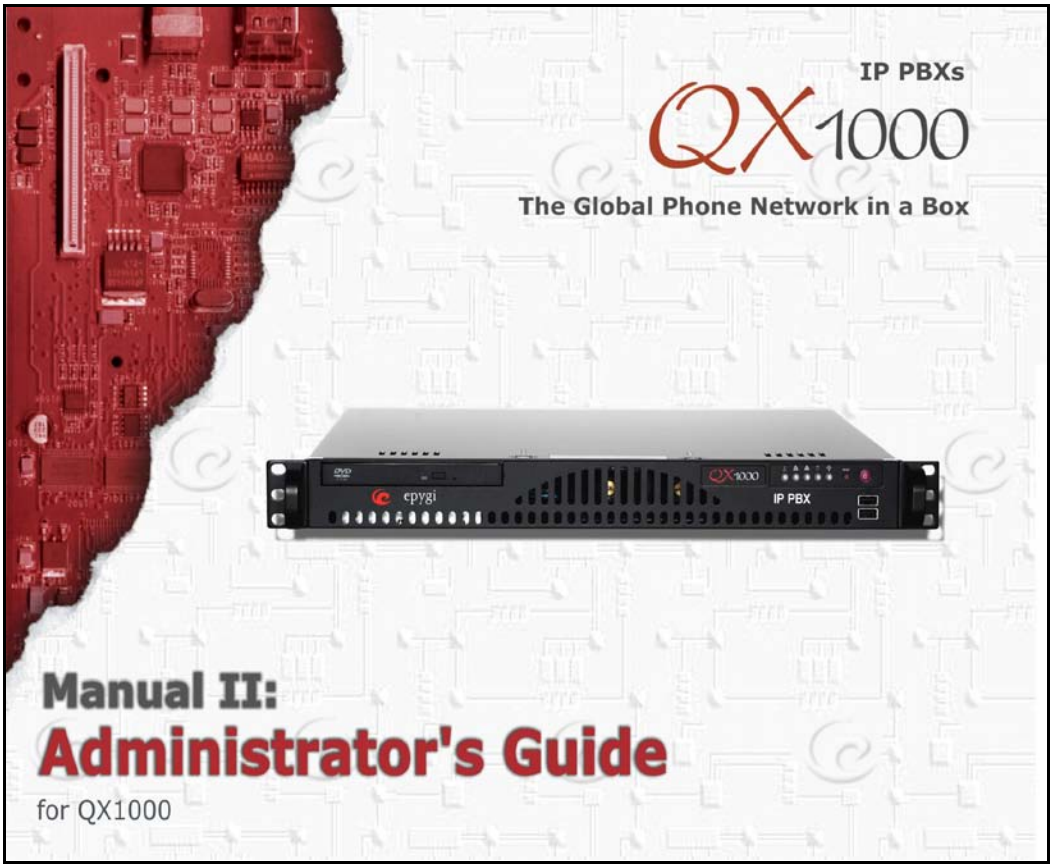


Edition 1, October 2013

SW Release 5.3.30 and higher

Table of Contents

Manual I: see Installation Guide

Step-by-step guide to install and configure QX1000 basically.

Manual II: Administrator's Guide

Manual III: see Extension User's Guide

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

About this Administrator's Guide

The QX1000 Manual is divided into three parts:

- Manual-I: Installation Guide gives step-by-step instructions to provision the QX1000 and configure the phone extensions with the Epygi SIP Server. After successfully configuring the QX1000, users will be able to make SIP phone calls to remote QX1000 devices, make local calls from extension to extension and access the Internet from devices connected to the WAN.
- Manual-II: Administrator's Guide explains all QX1000 management menus available for administrators only. It includes a list of all System Default Values.
- Manual-III: Extension User's Guide explains all QX1000 management menus available for extension users. A list of all call codes can be found there, too.

This guide contains many example screen illustrations. Since QX1000 offer a wide variety of features and functionality, the example screens shown may not appear exactly the same for your particular QX1000 as they appear in this manual. The example screens are for illustrative and explanatory purposes, and should not be construed to represent your own unique environment.

QX1000’s Graphical Interface describes to the QX1000's graphical user interface and explains all recurrent buttons.

Administrator’s Main Page explains the Administrator's management pages according to the menu structure shown on the main page of the QX1000 management.

Administrator’s Additional Features explains some input-options for administrators only that may be selected from the extension user's main page.

Appendix: PBX Services for QX1000’s Administrator explains PBX features for administrator accessible from the handset.

Appendix: Extension User's Welcome Page includes a form that allows the administrator to inform his extension user with all individually needed addresses and phone numbers.

Appendix: System Default Values lists all factory defaults.

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

Appendix: Software License Agreement includes the contract for using QX1000's hardware and software.

QX1000's Graphical Interface

Administrator's Main Page

When the administrator logs in, the **QX1000 Management** page is displayed with a table of active calls (including information about call peers, call duration and start time) at the startup. The number of total active calls is displayed above the table. The button **Terminate** next to each active call is used to terminate the corresponding call. The **Start Recording** button next to each active call (except for calls to Auto Attendant) is used to manually start the recording of the corresponding call. Once the call recording is started, the button changes to **Stop now** used to manually stop the call recording. The call recording can be restarted again if needed.

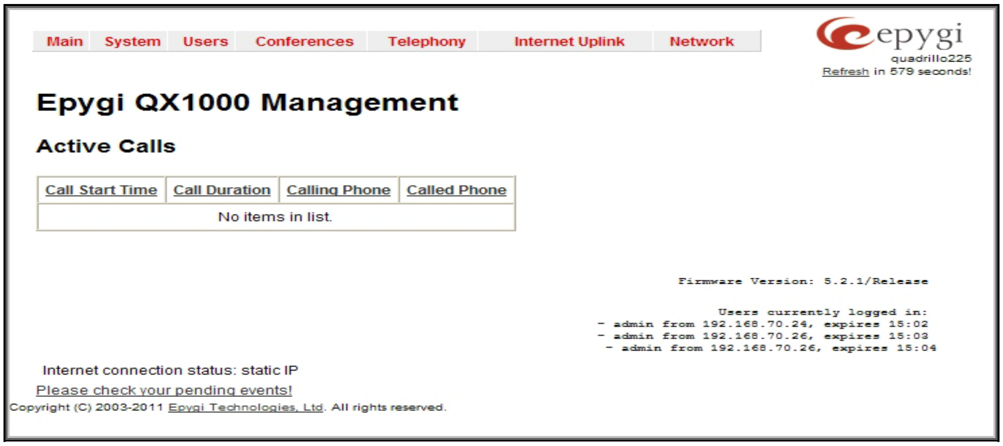


Fig. II: 1: QX1000 Management

Here the administrator may access the following settings and perform the actions:

By clicking on **System, Users, Telephony, Conferences, Internet Uplink** or **Network** the administrator may access the following settings in each respective category and perform actions specific to each category.

The **Install Checklist** option in the **Main Menu** opens a page that lists the most useful actions and the corresponding hyperlinks for the QX1000's initial setup and configuration procedure. From this page you can be linked to the appropriate pages where the corresponding configuration can be done. Here, you can also save your progress of QX1000's setup by selecting the corresponding action's checkbox and pressing **Save**.

System Menu

- System Configuration Wizard
- Uplink Configuration Wizard
- System Security Management
- Status
- IP Routing Configuration
- Configuration Management
- Events
- Time/Date Settings
- Mail Settings
- SMS Settings
- Firmware Update
- Networking Tools
- SNMP Settings
- Diagnostics
- Features
- Upload Language Pack
- User Rights Management
- Redundancy Settings

Users Menu

- Extensions Management
- Receptionist Management
- Extensions Directory
- Authorized Phones Database
- ACD Management

Conference Menu

- Conferences Management
- Conference Statistics
- Mail Default Settings

Telephony Menu

- Call Statistics
- SIP Settings
- RTP Settings
- NAT Traversal Settings
- Line Settings
- FXO Settings
- ISDN Settings
- External PSTN Gateways
- Gain Control
- SIP Tunnel Settings
- Call Routing
- VoIP Carrier Wizard
- RADIUS Client Settings
- Voice Mail Common Settings
- Dial Timeout
- 3PCC Settings
- RTP Streaming Channels
- Call Recording

Internet Uplink Menu

- Firewall

Network Menu

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

Registration Form
(in menu tree only)

Logout

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

The list of **Users currently logged into the system** is seen in the lower right corner of the Administrator's Main Menu. Information about IP address user accessed QX1000 GUI from, the username user is logged in and the time until the next automatically logout is provided herein. The current version of the QX1000's firmware and of its boot loader is also available here. The idle session timeout is set to 20 minutes. If no action is performed during that time, user will be automatically moved to the Login page and will be requested to login again.

Recurrent Buttons

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

Button	Description
Previous	This button leads back to the previous page of a fixed sequence of pages (used mainly in wizards).
Next	This button leads forward to the next page of a fixed sequence of pages (used mainly in wizards).
Cancel	This button discards the latest not yet confirmed entries.
Finish	This is the last button of a fixed sequence of pages that completes and saves the entries of an entire sequence.
Help	This button opens the help page belonging to the currently active QX1000 management page.
IP-Clipboard	This button opens a window where the last inserted IP addresses are listed. It allows the user to make a quick selection of an IP address that has been previously used. This will avoid the user needing type it again. The clipboard can hold up to 10 IP addresses and a new IP address will replace the oldest one from the list.

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

Recurrent Functional Buttons

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

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

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

Entering SIP Addresses Correctly

Calls over IP are implemented based on Session Initiating Protocol (SIP) on the QX1000. When making a call to a destination that is somewhere on the Internet, a SIP address must be provided.

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

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

For your convenience, the following combinations can be used:

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

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

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

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

Administrator's Menus

System Menu

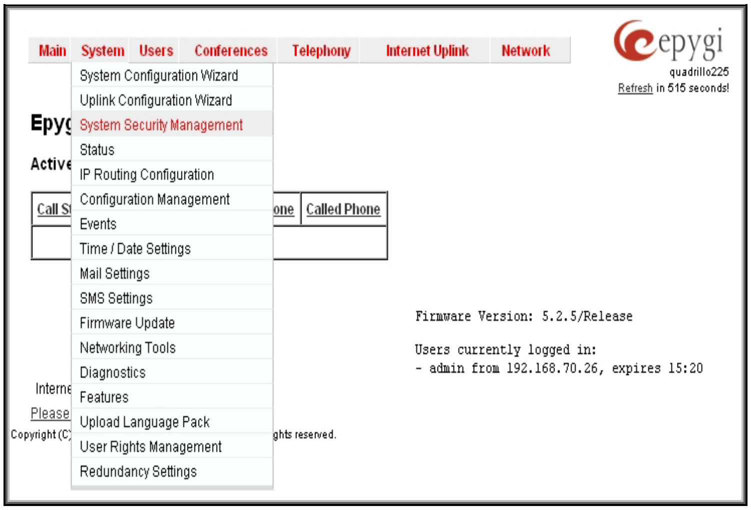


Fig. II-1: System Menu in Dynamo theme

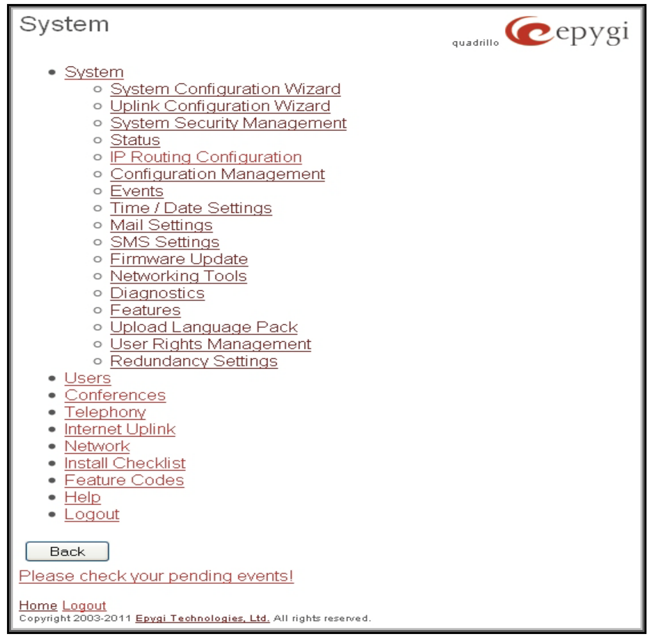


Fig. II-2: System Menu in Plain theme

System Configuration Wizard

The **System Configuration Wizard** allows the administrator to define the QX1000's Local Area Network settings and to specify regional configuration settings to make QX1000 operational in its LAN. The **System Configuration Wizard MUST be run upon QX1000's first startup** to make sure that it works properly in its network environment. The Wizard allows navigating through the following basic configuration parameters and settings:

- System Configuration
- DHCP Server Settings
- Regional Settings and Preferences (see below)
- Emergency Codes and PSTN Access Codes Settings (see below)

DHCP Server Settings are described in the chapters below. The LAN configuration and regional settings will be described later in this chapter.

Please Note: It is strongly recommended to leave the factory default settings if their meanings are not fully clear to the administrator.

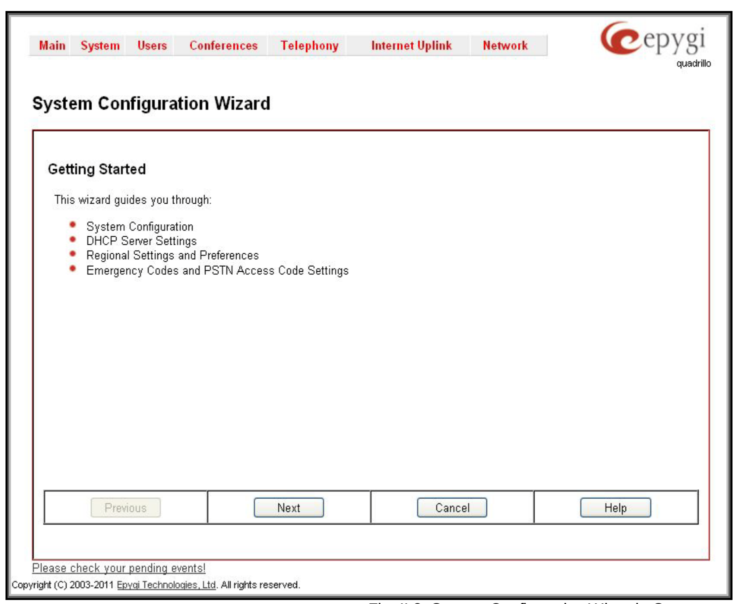


Fig. II-3: System Configuration Wizard - Start page

The **System Configuration** page contains the host name, IP address and Subnet Mask information about the QX1000 LAN interface. These settings make QX1000 available to the internal network.

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

Host Name requires a host name for the QX1000 device.

DNS suffix requires the LAN side domain name which the QX1000 belongs to.

IP Address requires the QX1000 host address for the LAN interface.

Subnet Mask requires the QX1000 host's Subnet Mask.

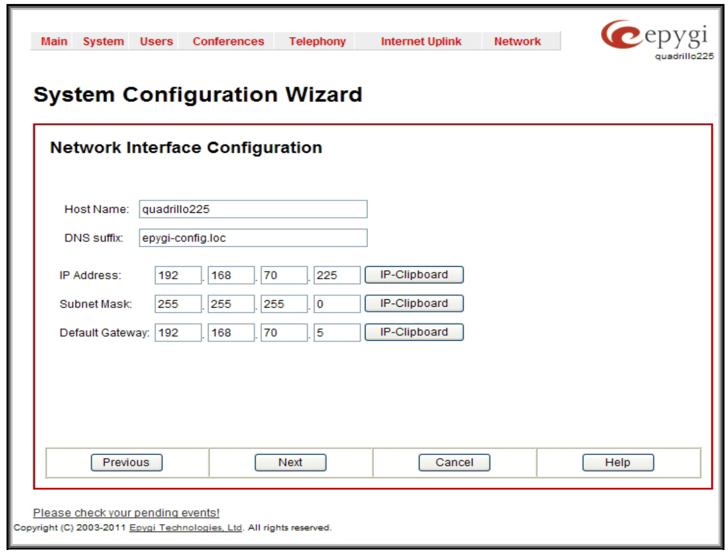


Fig. II-4: System Configuration Wizard - System Configuration page

The **Regional Settings and Preferences** are used to select settings specific to the location of the QX1000. This is important for the functionality of the voice subsystem.

The **Regional Settings and Preferences** page has two drop down lists to select the **Location** (country) and a corresponding **Timezone**. QX1000 will support Daylight Savings (DST) correction if it is available for the selected time zone.

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

- **System Language** – selection is available only when the custom Language Pack has been uploaded and it is used to enable custom language for system voice messages or returning back to the default language English.
- **GUI Theme** - selection used to select the GUI theme style of the web based configuration pages.
- The **Choose Theme on Login** checkbox indicates whether the GUI theme selection radio buttons should be displayed on the QX1000 Login page. Selecting the checkbox will allow users to choose the GUI theme before logging into the QX1000. Leaving the checkbox unselected will require the administrator to run the System Configuration Wizard to change the theme.

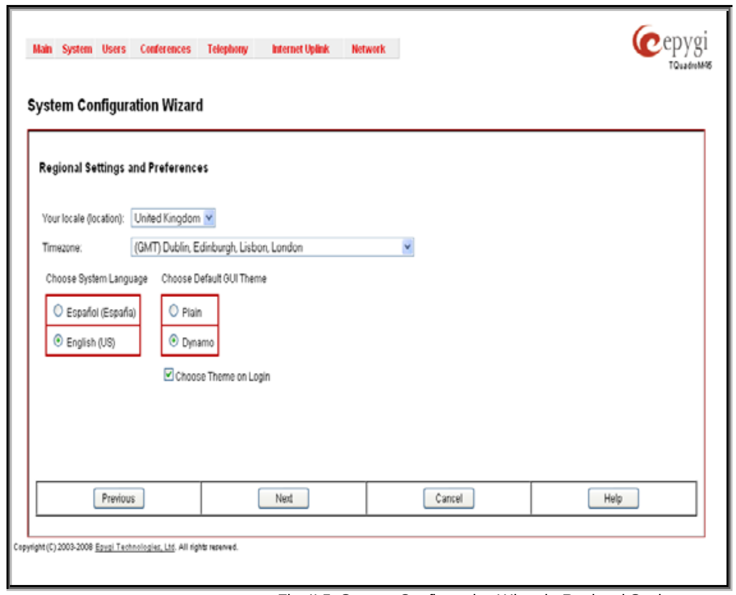


Fig. II-5: System Configuration Wizard - Regional Settings page

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

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

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

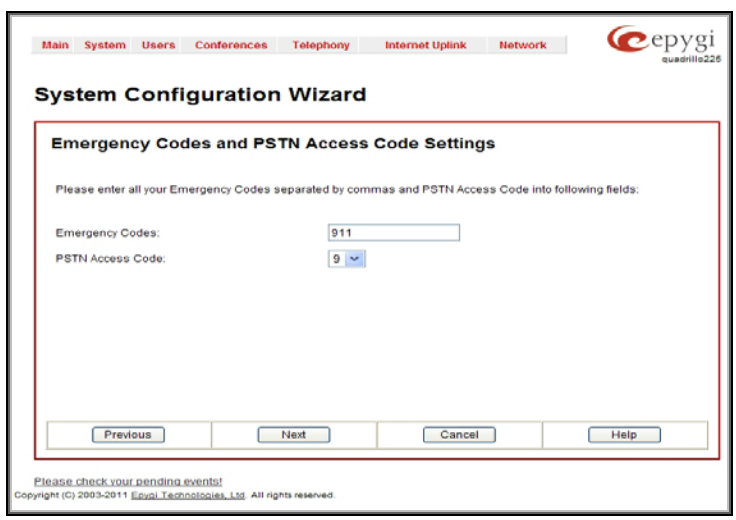


Fig. II-6: System Configuration Wizard - Emergency Codes and PSTN Codes Settings page

Uplink Configuration Wizard

The **Uplink Configuration Wizard** allows the administrator to configure the WAN interface settings and to adjust QX1000's connectivity with an external network. The **Uplink Configuration Wizard MUST be run for QX1000 to be connected to the Internet**.

All the settings of the **Uplink Configuration Wizard** are described in the chapters below except those for the IP settings, which will be described in this chapter.

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

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

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

- Uplink Selection
- Ethernet/Vlan IP Configuration
- DNS Settings

The **Uplink Configuration** page allows you to select the QX1000's WAN interface connection type and its bandwidth settings. These settings will make QX1000 available to the external network.

Depending on the Uplink **Interface Type** selection, the page following the **Uplink Configuration** page is different. Thus if **VLAN** (if configured) is selected, the next page will be VLAN IP Configuration, while selecting **Ethernet** will bring up the **Ethernet IP Configuration** page.

The bandwidth provided by the ISP has to be specified in the text fields **Upstream Speed** and **Downstream Speed**.This settings allow the specification of the upstream and downstream speeds in kbit/s, helping to assure the quality of IP calls. An IP call looses the voice quality if there is no available bandwidth. When approaching the limits of bandwidth capacity, another IP call will be declined.

The default entry in both fields is 1000000, the maximum bandwidth of a 1000 MB Ethernet. You may see the required bandwidth in the chapter Needed Bandwidth for IP Calls.

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

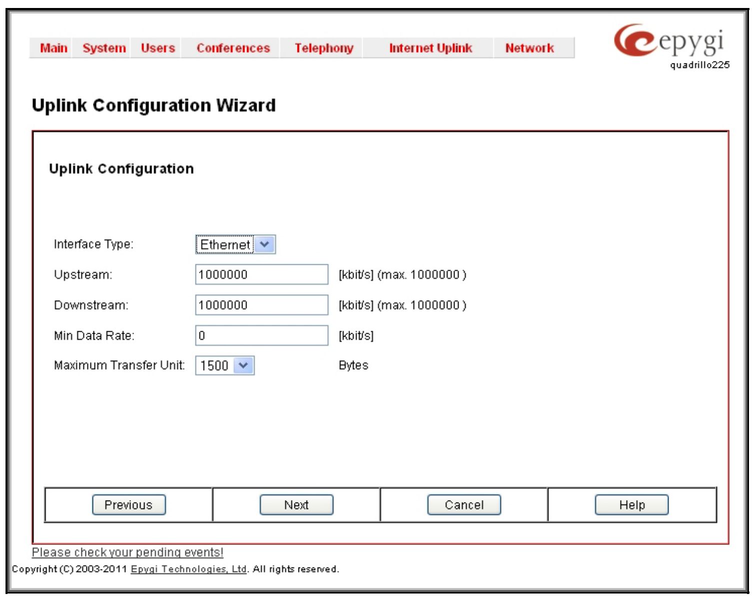


Fig. II-8: Internet Configuration Wizard - Uplink Configuration page

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

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

IP Address requires the IP address for the QX1000 WAN interface.

Subnet Mask requires the subnet mask for the QX1000 device WAN interface.

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

Please Note: DHCP referred to here is the one that runs on the provider's side and not the QX1000's personal DHCP server.

The **VLAN IP Configuration** page is only displayed if **VLAN** has been selected to be the uplink protocol and requires the VLAN IP address of the default gateway.

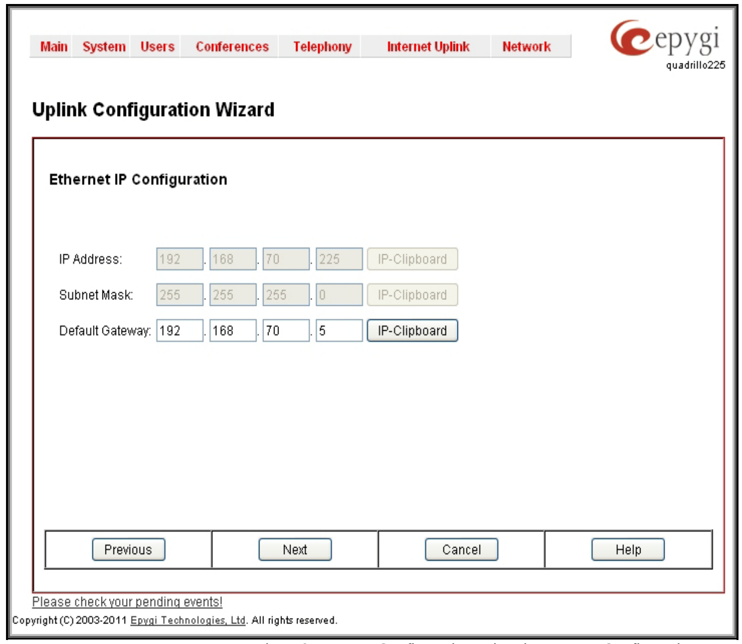


Fig. II-9: Internet Configuration Wizard - WAN IP Configuration page

The **DNS Settings** page provides the option of setting up a name server for the QX1000. It offers the following components:

- The **Nameserver** text field requires the IP address of an external name server.
- The **Alternative Nameserver** text field requires the IP address of the secondary name server. The **Alternative Nameserver** is used if the main name server cannot be accessed.

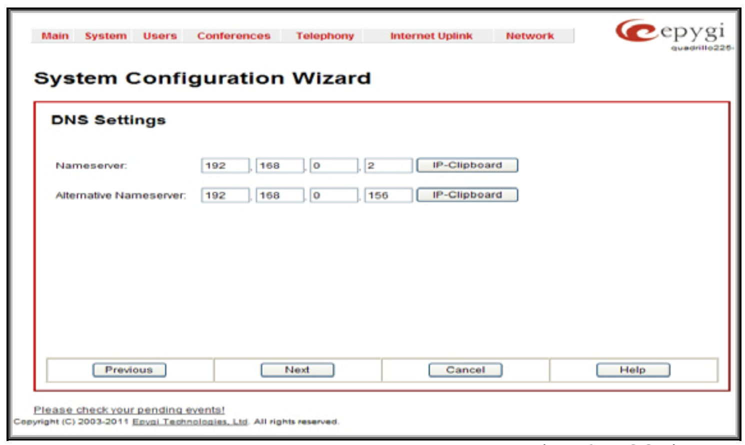


Fig. II-10: DNS Settings page

Needed Bandwidth for IP Calls

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

Required Bandwidth for Standard Packets:

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

Needed Bandwidth for Encrypted Packets when using a SRTP:

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:								
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	iLBC-13.33	G.722	G.722.1
10	114	66	74	82	90	58	-	114	82
20	89	41	49	57	65	33	-	89	57
30	81	33	41	49	57	26	31	81	49
40	76	28	36	44	52	20	-	76	44
50	74	26	34	42	50	18	-	74	42
60	72	24	32	40	48	16	22	72	40

Required Bandwidth for Encrypted Packets when a VPN is used:

Packet Size in msec.	Needed bandwidth in kbit/s using the Codecs:								
	G.711u/G.711a	G.726-16	G.726-24	G.726-32	G.726-40	G.729a	iLBC-13.33	G.722	G.722.1
10	148	98	105	118	124	92	-	148	118
20	105	59	65	74	81	49	-	105	74
30	90	43	52	60	66	35	41	90	60
40	85	38	45	53	61	30	-	85	53
50	80	34	41	48	56	26	-	80	48
60	74	29	37	45	52	22	26	74	45

System Security Management

The **System Security Management** offers a possibility of managing the global security levels, running the system security diagnostics program and receiving complete reports on the QX1000 configuration security. It includes three pages- the **System Security Settings** page, **System Security Diagnostics** page and the **SIP IDS Settings** page.

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

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

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

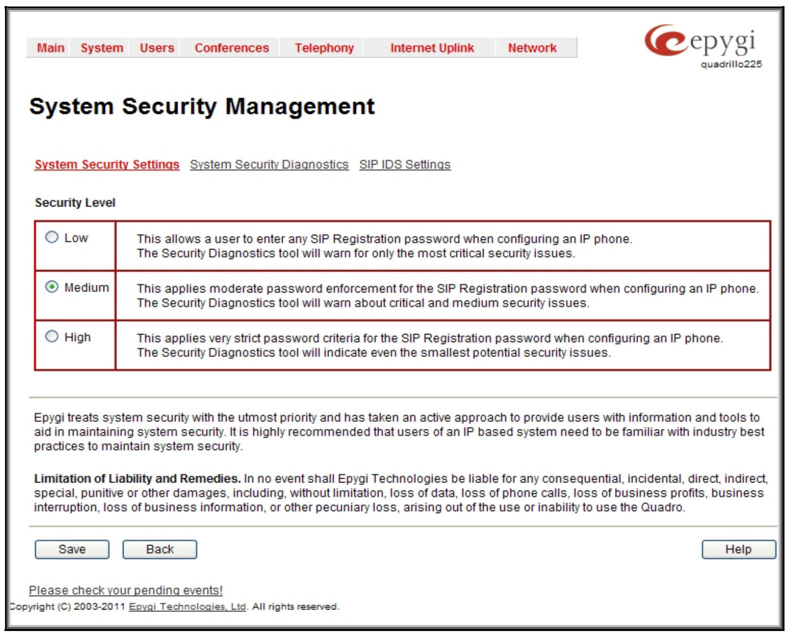


Fig. II-11: QX1000 System Security Management page

The **System Security Diagnostics** page allows running the security audit and getting the security reports. The **Start Security Audit** functional button is used for running the security audit. The QX1000 security audit is a security reporting system, which generates the warnings regarding the QX1000's weaknesses relative to the selected **Security Level**. The warnings may vary depending on the selected global security level. The security audit will detect the security related configuration issues in Firewall, IP Line passwords, Call Routing and extension settings.

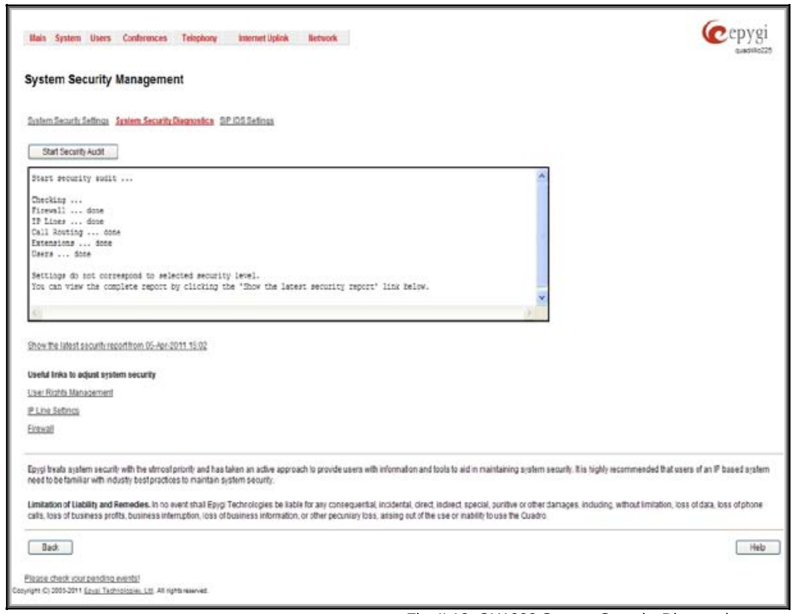


Fig. II-12: QX1000 System Security Diagnostics page

The output of security audit may look as follows:

Start security audit...

Checking...

Firewall ... done

IP Lines ... done

Call Routing ... done

Extensions ... done

Users ... done

Settings do not correspond to selected security level.

You can view the complete report by clicking the 'Show the latest security report' link below.

The **Show the latest security report** link allows to display the last security audit report. This page also contains the following useful links to adjust the system security:

- User Rights Management
- IP Line Settings
- Firewall

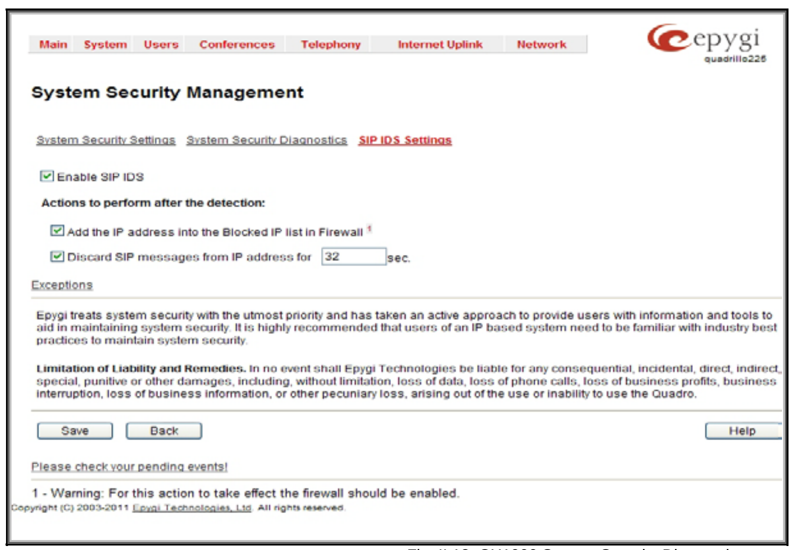


Fig. II-13: QX1000 System Security Diagnostics page

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

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

The **Add the IP address into the Blocked IP list in Firewall** checkbox allows to block SIP attacker's IP address. SIP attacker's IP address will be blocked by QX1000 Firewall and will be added on the Firewall **Blocked IP List** table.

The **Discard SIP messages from IP address for** checkbox allows to discard the accumulated SIP messages from the QX1000 SIP cash after defined timeout (default timeout value of "Discard SIP messages from IP address for" service is 32 seconds).

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

Delete removes the selected entries from the IP address table.

Select all selects all entries of the table.

Inverse Selection inverses the current selection (if no record is selected, clicking on inverse selection will check all records).

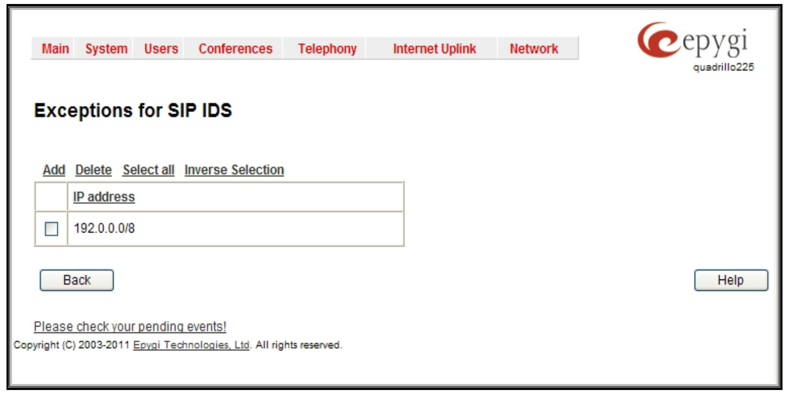


Fig. II-14: QX1000 Status - General Information page

Status

The system status window displays non-editable tables providing extensive system status information about QX1000: General Information, Network Status, Lines Status, Memory Status, Hardware Status, SIP Registration Status, IP Lines Registration Status and License Status. The links on this page lead to device Transfer Statistics, user mailboxes and supplementary services configuration pages.

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

General Information

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

- **Uptime duration -** Period QX1000 is running since last reboot.
- **Device hostname -** QX1000 device host name.
- **QX1000 Operating System -** QX1000 operating system version.
- **Application Software -** Software and file system versions of the QX1000.
- **Language Pack** – this field is present only when the custom language pack is uploaded and it indicates the version.

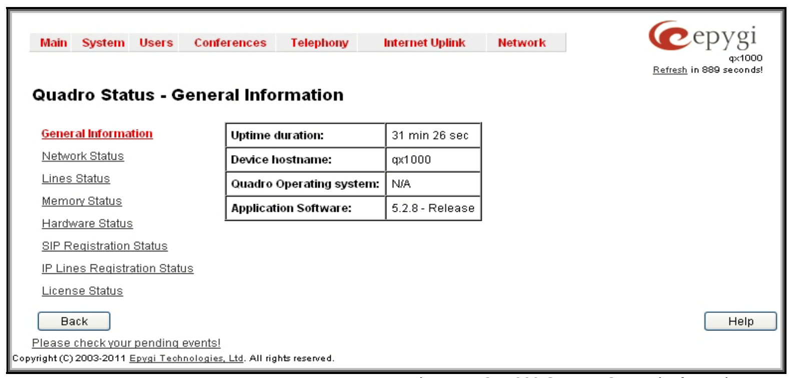


Fig. II-15: QX1000 Status - General Information page

Network Status

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

Interface Name lists the Network interfaces available on the QX1000 (LAN, VLAN, DSP).

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

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

Properties will list either the MAC address corresponding to each network interface on the QX1000.

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

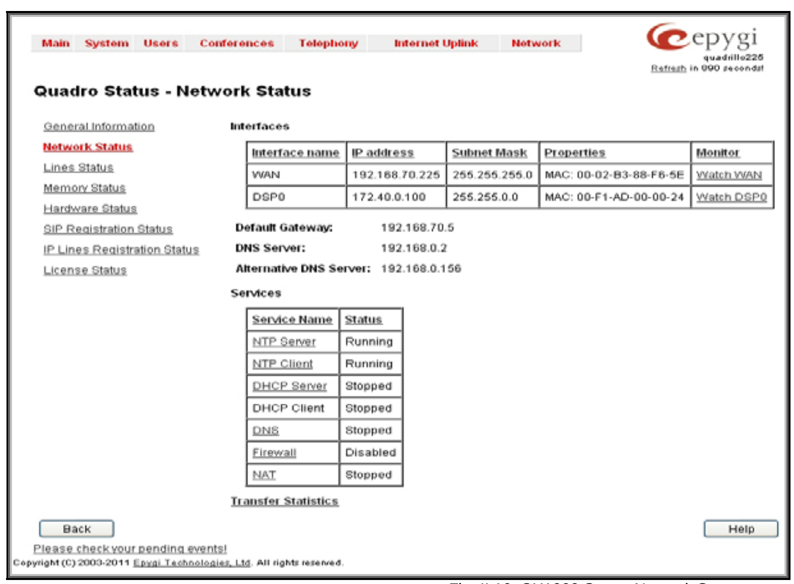


Fig. II-16: QX1000 Status Network Status page

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

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

DNS Server, **Alternative DNS Server** and **Default Gateway** - these display the QX1000 settings corresponding to what has been configured with the System Configuration Wizard.

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

Transfer Statistics - link to the Transfer Statistics page.

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

Time range of statistic table - the drop down list includes the period (in days) statistics data that is to be collected and the corresponding diagram charts that are to be built.

When **Show also as readable values** checkbox is selected, an additional table with statistics values will be displayed on the next page.

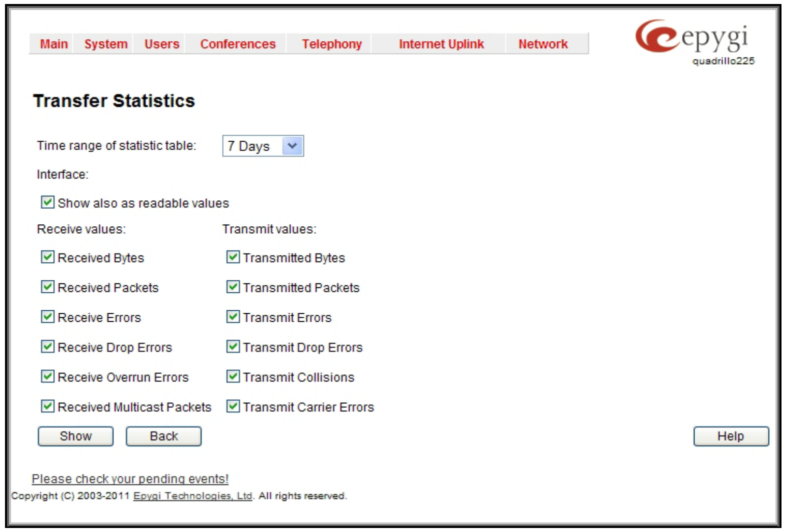


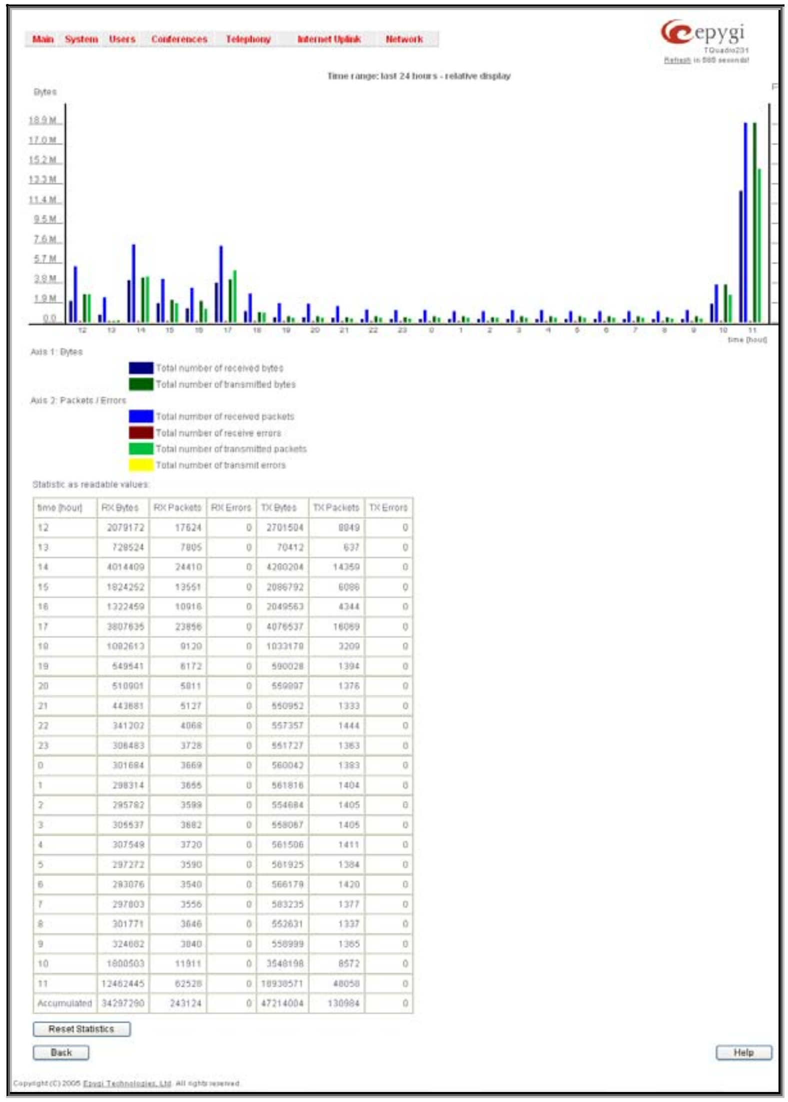
Fig. II-17: Transfer Statistics page

The area **Receive Values** provides the following:

- **Receive Bytes** - number of received bytes.
- **Receive Packets** - number of received Ethernet packets.
- **Receive Errors** - number of received packets containing errors.
- **Receive Drop Errors** - number of received packets that have been discarded.
- **Receive Overrun Errors** - number of received overrun errors that occur when the receive buffer is not large enough to hold all incoming packets. This error usually appears due to a slow receiving system.
- **Receive MultiCast Packets** - number of received broadcast packets.

The area **Transmit Values** provides the following:

- **Transmit Bytes** - number of transmitted bytes
- **Transmit Packets** - number of transmitted Ethernet packets.
- **Transmit Errors** - number of transmitted packets containing errors.
- **Transmit Drop Errors** - number of transmitted packets that have been discarded.
- **Transmit Carrier Errors** - number of transmit carrier errors that occur due to a defective or lost connection on the Ethernet link.
- **Transmit Collisions** - number of transfer errors that occurred during a simultaneous packet transmission from both sides.



time [hour]	RX Bytes	RX Packets	RX Errors	TX Bytes	TX Packets	TX Errors
12	2079172	17624	0	2701504	8049	0
13	728524	7805	0	70412	637	0
14	4014409	24410	0	4200204	14359	0
15	1824252	13551	0	2086792	6086	0
16	1322459	10916	0	2049563	4344	0
17	3807635	23856	0	4076537	16069	0
18	1082613	9120	0	1033178	3209	0
19	549541	6172	0	590028	1394	0
20	510901	5811	0	559897	1376	0
21	443681	5127	0	550952	1333	0
22	341202	4068	0	557357	1444	0
23	308483	3728	0	551727	1363	0
0	301684	3669	0	560042	1383	0
1	298314	3655	0	561816	1404	0
2	295782	3599	0	554684	1405	0
3	305537	3682	0	558067	1405	0
4	307549	3720	0	561506	1411	0
5	297272	3590	0	581925	1384	0
6	283076	3540	0	566178	1420	0
7	297803	3556	0	583235	1377	0
8	301771	3646	0	552631	1337	0
9	324682	3840	0	558999	1365	0
10	1800503	11911	0	3548198	8572	0
11	12462445	62528	0	18938571	48058	0
Accumulated	34297290	243124	0	47214004	130984	0

Fig. II-18: Transfer Statistics Diagram Chart

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

Lines Status

The **QX1000 Status** - **Lines Status** page shows the current status of each IP lines including details of the attached extension. Since only one line of information can be displayed at a time, the **IP Line** functional buttons are used to navigate through the information regarding other lines.

The **Lines Status** table displayed for **IP** lines includes a group of static and dynamic parameters. Static parameters are always displayed. Dynamic parameters only appear when an event takes place on the extension.

Static Parameters:

Extension shows the extension number of the selected telephone line.

Display Name shows the corresponding name.

Phone State may have the value **On Hook** or **Off Hook**. For IP Line Status, this field may additionally have **Not Configured** and **Temporary Offline** values.

Number of Active Calls shows the number of calls that are currently present on the phone.

Dynamic Parameters:

Call State shows the current state of the extension (in voice mail, in call, waiting, busy, call out, ring in, etc.).

Caller Party appears when a call is received and indicates the caller extension and the IP address or a phone number, depending on type of call.

Called Party appears when a call is placed and indicates the destination extension and the IP address or a phone number, depending on type of call.

Call Type shows whether the call is **Internal** or **External** and whether it is a **PSTN** call, **PBX** call or **IP** call.

Call Start Time shows the call start date and time.

Call Duration shows the current call duration.

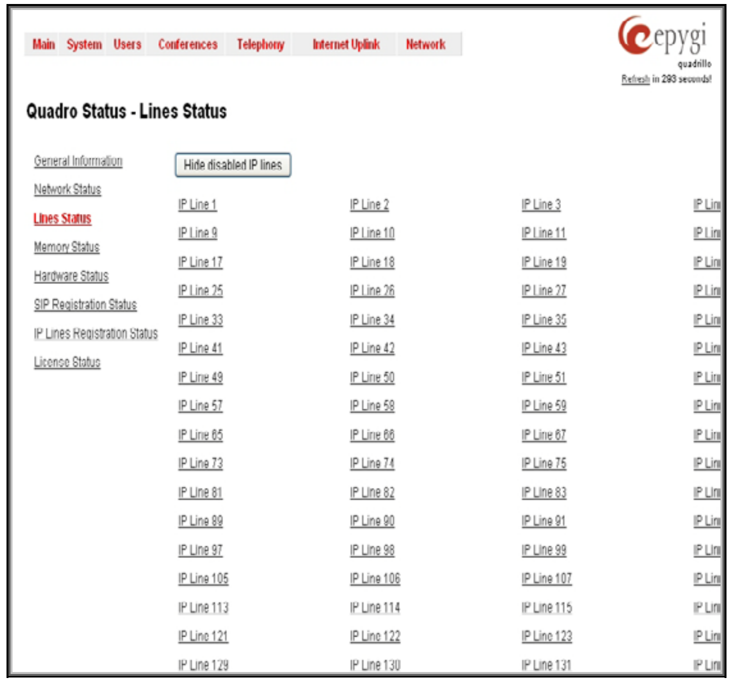


Fig. II-19: Lines Status - Lines Status page upon established call

RX Codec shows the codec used to encrypt the incoming packets. **TX Codec** shows the codec used to encrypt the outgoing packets. If RX and TX codecs are the same, only one **Codec** field will be displayed.

For IP Line Status, the following dynamical parameters appear on this page:

Username shows the IP phone's client name registered on the QX1000.

Last Registered shows the date and time, the corresponding IP phone has been last registered on the QX1000.

Expires In shows when the last registration of the IP phone will expire.

Binding IP Address shows the IP address of the IP phone within the QX1000's LAN network.

The list of supplementary services provides the following additional status information for each telephone line: **Enabled** or **Disabled**.

For **Incoming** and **Outgoing Call Blocking**, **Speed Calling, Hiding Caller Info**, **Voice Mailbox** and **Group List** services, the number of **Entries** will be displayed in the corresponding service table. For **Voice Mail Service**, the voice mailbox configuration mode is displayed here.

This allows administrator to view the status and to be notified about services running on QX1000 for every line. The services are designed as links that guide the administrator to the corresponding service page of the selected user.

Memory Status

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

Memory Size shows total memory space (counted in minutes/seconds) available on the QX1000 and assigned to all extensions.

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

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

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

Conference Memory Status shows total memory space (counted in minutes/seconds) available on the QX1000.

The table's links lead the administrator to the conference extension settings page where **Total Space** for the corresponding conference extension may be altered.

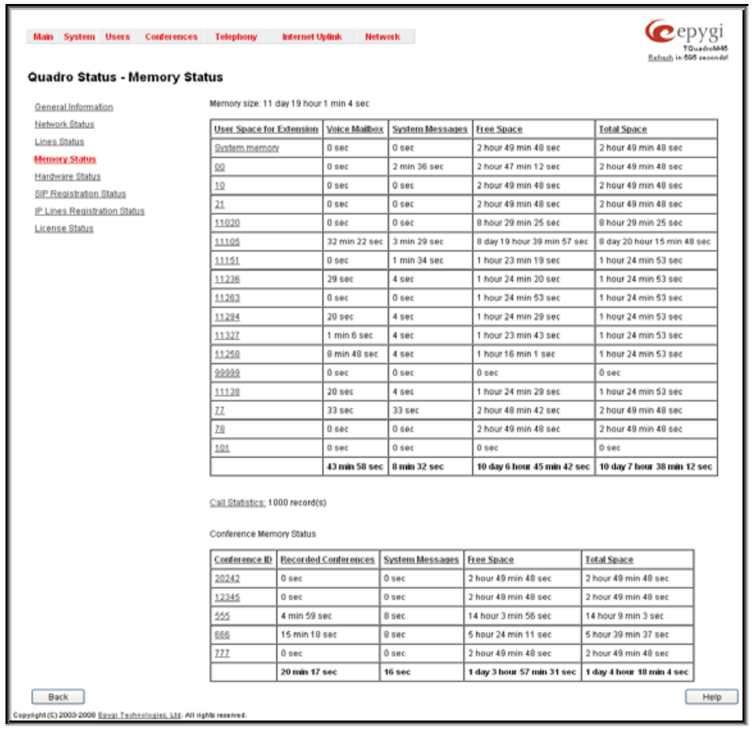


Fig. II-20: Memory Status page

Hardware Status

The **Hardware Status** table displays a list of the hardware devices and parts present and currently available on the QX1000 board. The hardware device version number and additional comments about its state are indicated here.

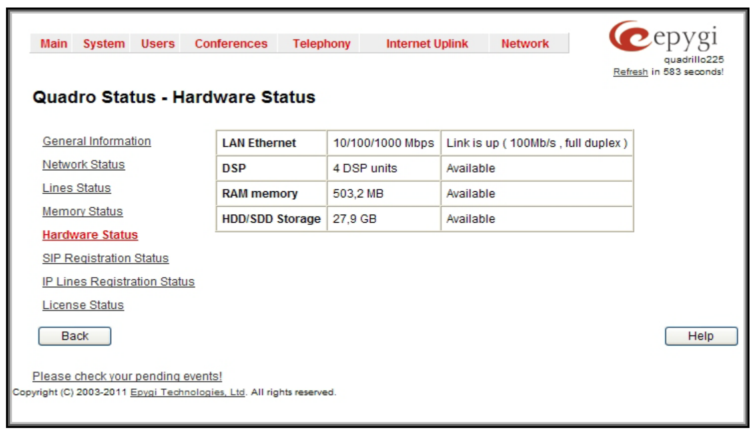


Fig. II-21: Hardware Status page

SIP Registration Status

The **SIP Registration Status** is a table displaying the SIP registration information of the QX1000 extensions.

The table contains a list of all the registered extensions of the QX1000, SIP registration name for each extension, addresses of SIP servers where they are registered (if applicable), whether or not it is registered for each extension, and the registration date and time. By clicking on the row heading, the table will be sorted by the selected column. When sorting (ascending or descending), arrows will be displayed next to the column heading.

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

The **Detected Connection Type** field displays the connection type QX1000 currently is acting in (direct connection or behind NAT). If QX1000 is acting behind NAT, the NAT machine IP address is also displayed.

The **Registered IP Lines** table lists the IP lines and remote extensions registered on the QX1000. The table indicates the actual IP addresses of the remote devices, the usernames by which the devices have been registered on the QX1000, as well as the registration status information.

The **SIP Tunnels to Slave Devices** and **SIP Tunnels to Master Devices** tables list the SIP tunnels between local and the remote QX1000s (see SIP Tunnel Settings). The **SIP Tunnels to Slave Devices** table lists those tunnels where local QX1000 acts as a master. The **SIP Tunnels to Master Devices** table lists those tunnels where local QX1000 acts as a slave.

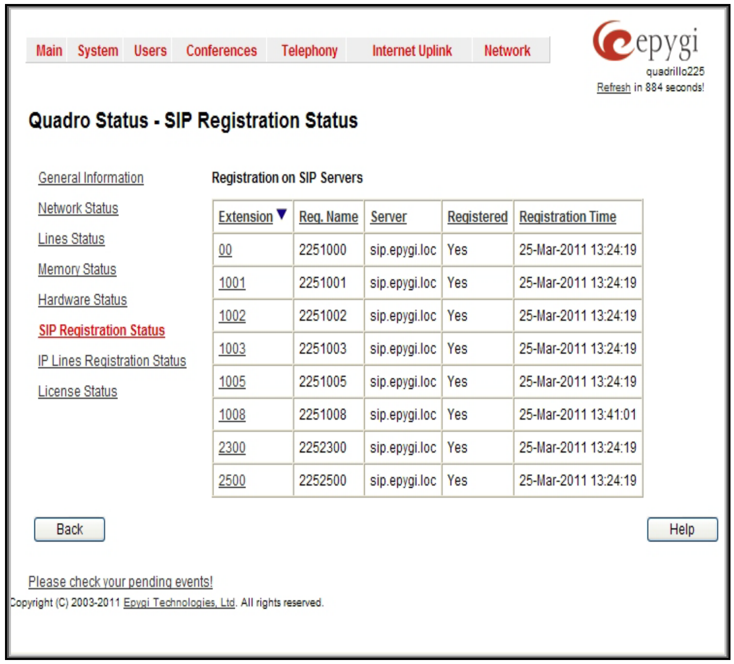


Fig. II-22: SIP Registration Status page

IP Lines Registration Status

The **IP Lines Registration Status** displays a table with the IP Lines registration information on the QX1000.

The table lists the IP lines and remote extensions registered on the QX1000. The table indicates the actual IP addresses of the remote devices, the usernames by which the devices have been registered on the QX1000, as well as the registration status information.

Subscription Count field indicates used and allowed number of subscriptions for all IP phones registered on the QX1000. Subscriptions are events originated by IP phones when watching other extensions or SLAs on the QX1000 and when monitoring voice mailbox for new received voice mails.

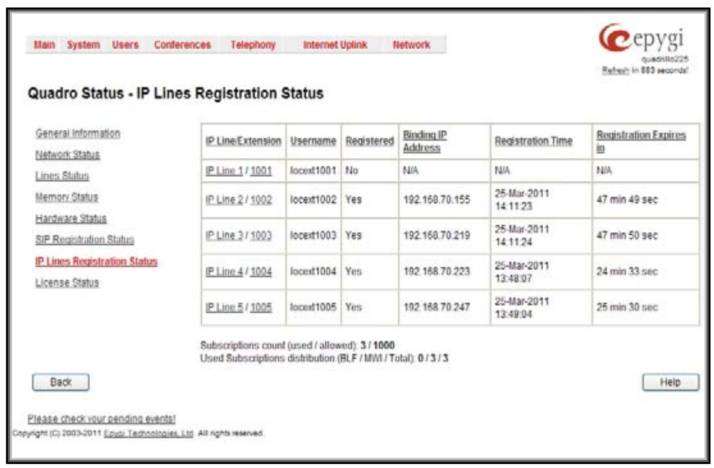


Fig. II-23: SIP Registration Status page

When the allowed number of subscriptions is reached, no new subscriptions are possible. Typically the number of subscription should be keep reasonably below the maximum allowed number, to avoid losing subscriptions. Thus, in case the actual subscription number is close to the limit, configuration of IP phones should be adjusted to decrease the number of total subscriptions on the QX1000.

Used Subscription Distribution field indicates IP phone's subscriptions distribution among BLF (Busy Lamp Field) subscriptions, which are used for watching extensions and SLAs on IP phones, and MWI (Message Waiting Indication) subscriptions, which are used for voice mailbox status indication on the phone.

License Status

The **License Status** page displays a table with all available licenses on the QX1000 and the corresponding settings for each license (Currently only QCM and DCC license statuses are displayed).

This page includes the following information:

Type indicates the type of the license available on the QX1000.

Count indicates the number of the corresponding licenses available on the QX1000.

In Use indicates the number of used licensed from the total available licenses.

Extension lists the extensions that are using the corresponding license. Links in this column move to the corresponding service configuration page for the extension.

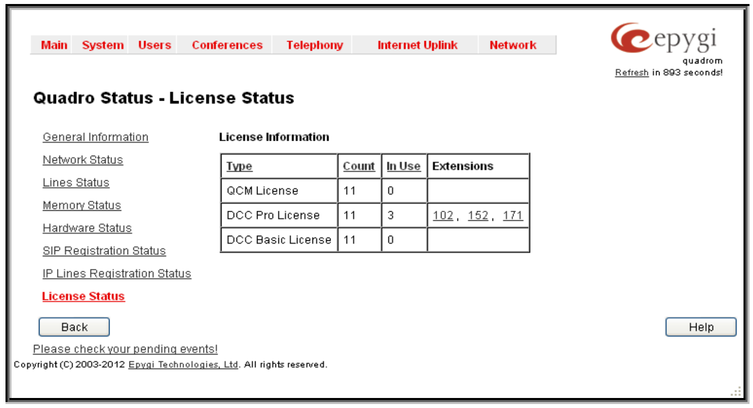


Fig. II-24: License Status page

IP Routing Configuration

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

QX1000's **IP Routing** service allows you to route IP packets from one destination to another (or to a specified router) through QX1000.

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

IP Static Routes are used to forward IP packets from the Network, where the QX1000 is connected, to the specified destination.

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

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

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

Fig. II-25: IP Static Routing table

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

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

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

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

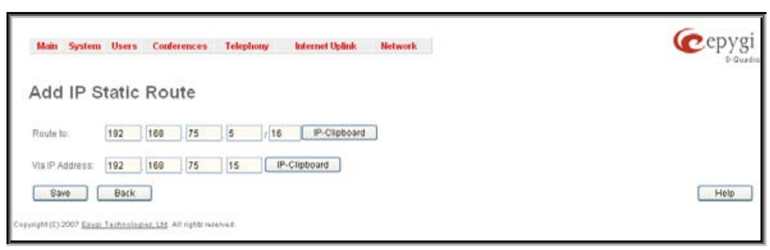


Fig. II-26: Add IP Static Routing page

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

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

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

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

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

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

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

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

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

Fig. II-27: IP Policy Routing table

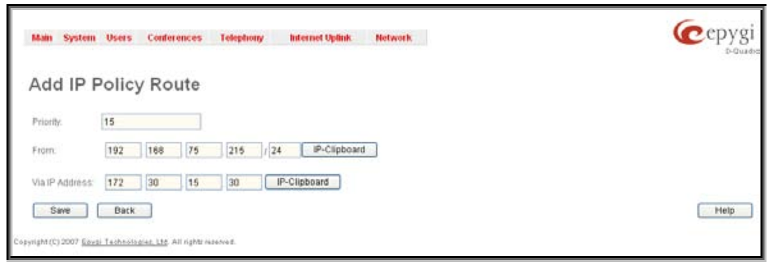


Fig. II-28: Add IP Policy Route page

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

To Add an IP Static Route

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

To Add an IP Policy Route

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

Configuration Management

The **Configuration Management** page assists the administrator with managing the system configuration settings and voice data. For example, the administrator is able to backup and download the settings to a PC and then upload and restore them back to the QX1000. Additionally, this page provides the possibility of restoring the factory default configuration settings.

The **Backup & Automatically Download all config & voice data** link leads to the **Automatically Backup Configuration Settings** page where the automatic backup of the system configuration and the voice data can be configured. The service allows you to setup QX1000 so it will automatically backup the system configuration and the voice data and store it in the specified location.

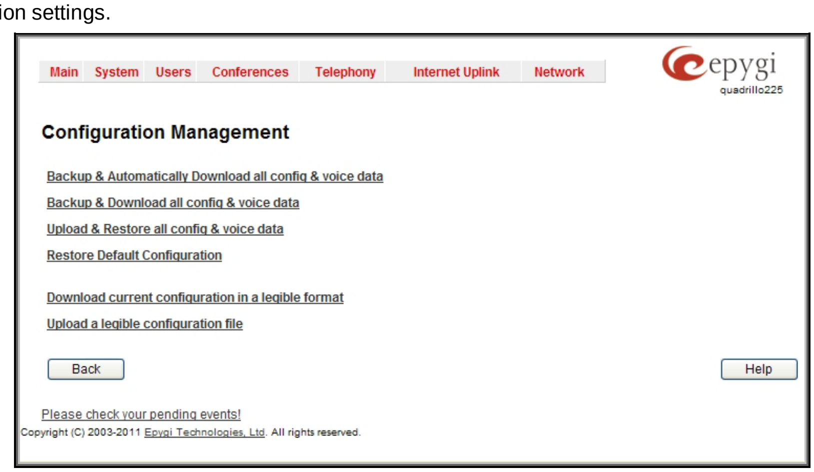


Fig. II-29: Configuration Management page

The **Automatically Backup Configuration** Settings page allows you to enable the automatic backup of the system configuration and the voice data on the QX1000. With this service, QX1000 will automatically backup the system configuration and the voice data and store it in the specified location.

This page contains the following components:

The **Enable Automatically Backup** checkbox enables automatic backup mechanism on the QX1000.

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

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

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

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

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

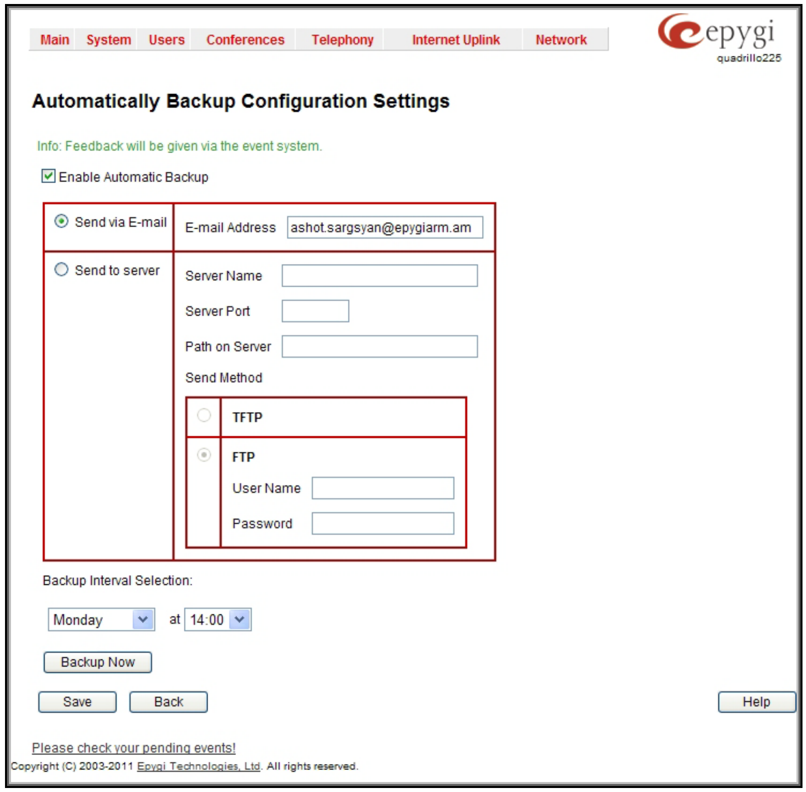


Fig. II-30: Configuration Management page

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

The **Backup Interval Selection** drop down lists is used to select the frequency and the time when the automatic backup of the QX1000's system configuration and the voice data will take place.

Backup Now button is used to perform a manually immediate backup of the system configuration and the voice data.

The **Backup & Download all config & voice data** link generates a backup file with all configuration settings and user uploaded greeting messages. It opens a file chooser window for immediate download to the users PC.

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

The **Restore Default Configuration** functional button resets all configuration settings and restores the board's factory default configuration. By restoring the default configuration you will replace your current configuration, lose all voice mails and reboot the device. You will not be automatically redirected to the GUI start page. After the successful reboot you will need to enter into the management page and login again to access the QX1000's configuration. A warning message will ask you to confirm your selection before restoring the default configuration.

Please Note: Unlike the factory default settings restore procedure initialized from the **Reset** button on the QX1000 board, this link will keep the following data:

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

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

Legible Configuration Management

The **Legible Configuration Management** is used to manually manage the configuration on the QX1000. This will allow you to download a piece of configuration from the QX1000 in the way of legible file, to make necessary changes in that file and to upload it back to the same or different QX1000. With this service, some pieces of configuration (like extension settings, NAT settings, etc.) of one QX1000 can be used on another QX1000. This also helps to apply the same group of settings to the several instances (for example, to apply the same SIP settings to multiple extensions on the QX1000) on the same or different QX1000s avoiding manual configuration of each of those instances (i.e. extension) from the web management on each of the QX1000s. The QX1000 reseller, distributor, ISP or carrier usually uses this service.

The **Download current configuration in a legible format** link refers to the **Configuration Summary** page where a partial or complete configuration can be defined and downloaded or viewed.

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

The manipulation radio buttons are used to select between particular CGI or a named group of CGIs for which the legible configuration file will be generated.

- The **Specific CGI** selection allows you to choose a certain CGI from the list of QX1000’s Web management pages for which the legible configuration can be manually managed. For example, selecting "RTP Settings" will generate a legible configuration file with parameters present on the RTP Settings page.
- The **Named Group of CGIs** selection allows you to choose among the four predefined groups: Internet Connection Settings, LAN Configuration Settings, Telephony General Settings and Extension Settings. Each of these groups refer to all CGIs characterized by the selected criteria, e.g. Internet Connection Settings group contains all parameters on the CGIs related to the networking and WAN configuration.

The **Extension** drop down list allows you to limit the settings in the generated legible configuration file to one specific extension. For example, each of the extensions on the QX1000 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 QX1000 (if the selected parameter applies to the extension and not to the overall system, like RTP settings).

The **Start generate a legible configuration file** button start parsing the configuration structure of the device for the defined parameters. The progress will be displayed in the area below.

Fig. II-31: Configuration Summary – Parameters page

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

The **Download generated configuration** button becomes available when the legible configuration generation is finished. It is used to download the generated file to the PC in a plain text format. Necessary changes can be made in the downloaded configuration file and then uploaded back to the system.
Attention: Make sure the changes you have done in the downloaded legible configuration file are valid and will not corrupt the system when being uploaded back to device.

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

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

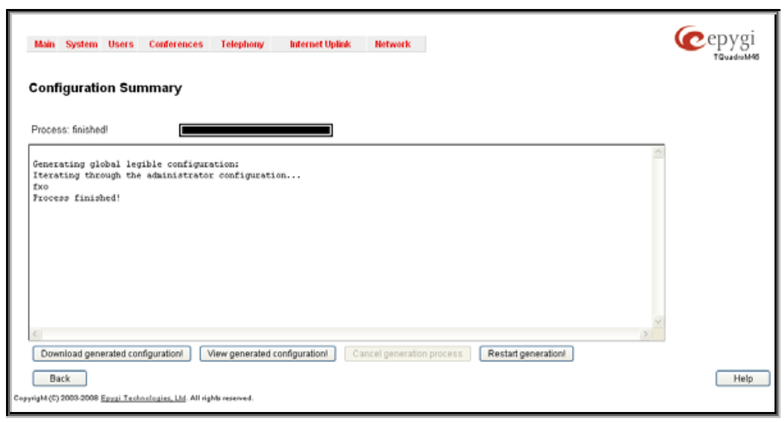


Fig. II-32: Configuration Summary Preview page

The **Upload Legible Configuration** page is used to upload a configuration file in a text format. The **Browse** button in the opened page is used to browse certain legible configuration file to be uploaded and updated into the system. The configuration files to be uploaded should be in the *.txt format, otherwise a system error occurs. Configuration file upload progress will be displayed in the area below. During legible configuration file upload, QX1000's functionality failures may occur.

Events

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

The **System Events** page may be accessed through the **Events** link from the main menu. It lists information about system events that have occurred on QX1000. When a new event takes place, a record is added to the System Event table. For failure events (priority 2 and 3, see below), the warning “Please check your pending events!” will appear at the bottom of all management pages.

The system events and the warning message are visible only for the administrator. The warning link, (which leads directly to the **System Events** page) will disappear from the management

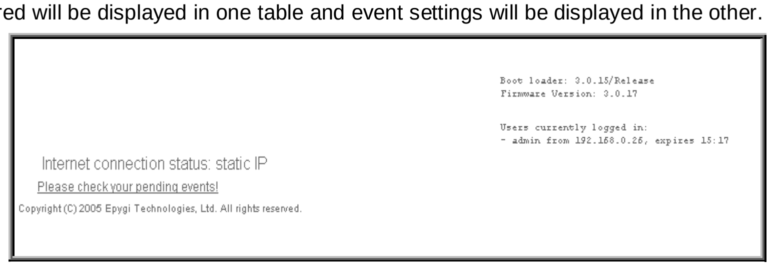


Fig. II-33: Event Warning on the Main Menu page pages if the administrator has marked all new events as "read".

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 has occurred due to incorrect mail sending or SIP registration, the corresponding links will be seen in the **Reference** column of the table. The administrator can view the detailed log for each event that has occurred.

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

Current System Time displays the local date and time on QX1000.

Mark all as read marks newly occurred events as "read".

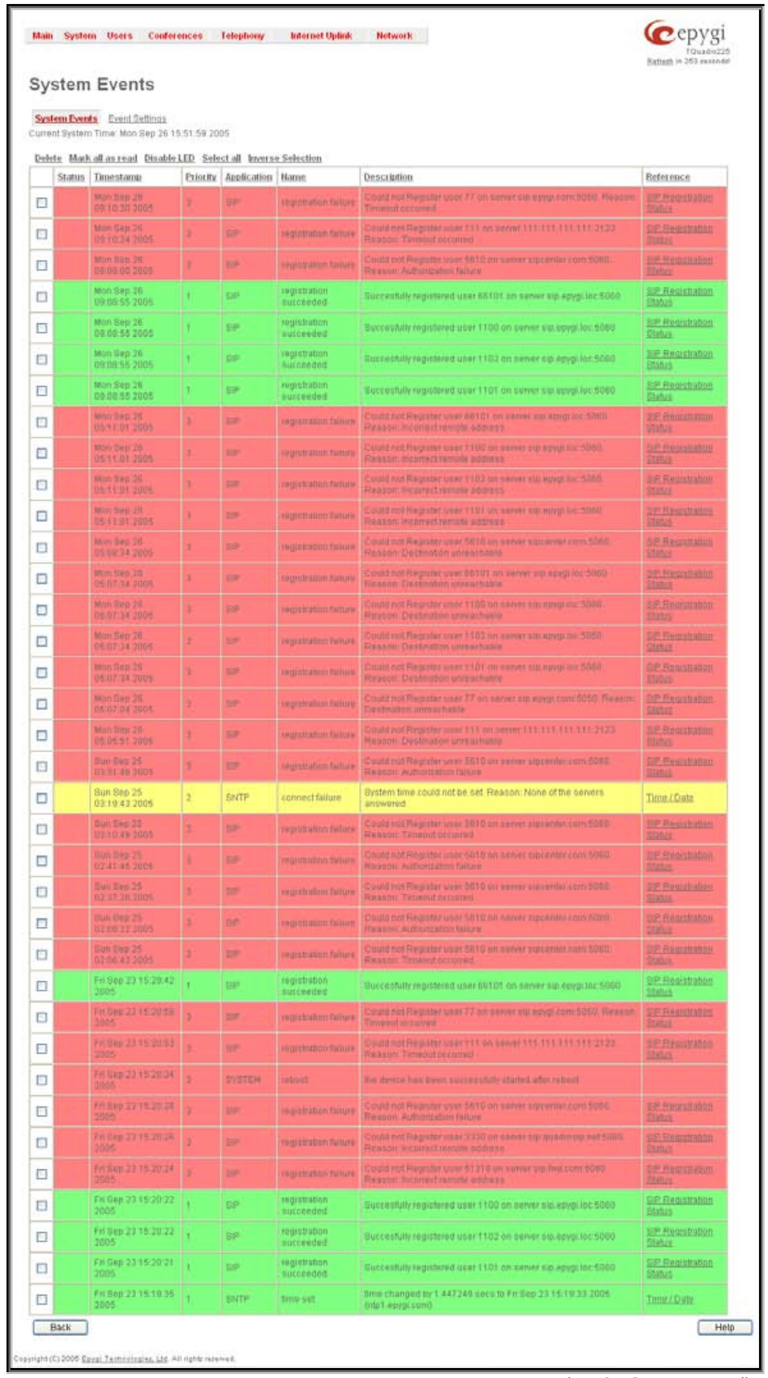


Fig. II-34: System Events list

Numerous circumstances may cause a certain application on QX1000 to flag an event.

The **Event Settings** page lists all possible events on the QX1000 and allows controlling notification (action) when an event takes place.

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

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

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

Fig. II-35: Event Configuration Settings page

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

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

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

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

Action offers radio buttons to choose one of the actions to notify the QX1000 administrator when an event(s) takes place. The following actions can be available:

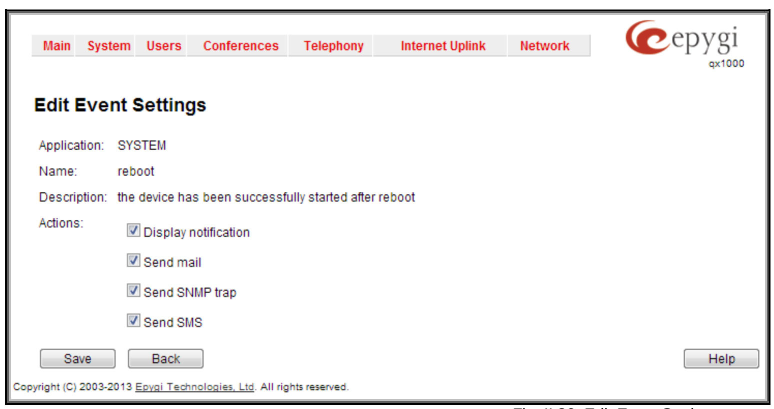


Fig. II-36: Edit Event Settings page

- **Display Notification** - A notification link will be displayed on the bottom of all pages and a record is added into the Events table. The notification is executed as a link “Please Check your pending events!”. The link leads to the System Events page. This action also will take place if Send Mail has been selected, even if not specifically selected.
- **Send Mail** – an e-mail notification about the new event on the QX1000 will be sent to the e-mail address specified in the Mail Settings page.
- **Send SNMP Trap** - an SNMP notification will be sent to the traphost(s) listed in the SNMP Trap Settings table.
- **Send SMS** – an SMS notification about the new event on the QX1000 will be sent to the mobile phone specified in the SMS Settings page.

Actions that are not allowed for the selected event (like mail notification if the PPP link is down or the mail server has been configured improperly) are hidden. For multiple events editing, actions that are not appropriate for least one of the selected events will also be hidden.

If QX1000 cannot receive an IP address from the DHCP 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 QX1000 raises an appropriate message.

To Assign an Action to the Event

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

Time / Date Settings

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

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

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

Enable Simple Network Time Protocol Server enables the SNTP (Simple Network Time Protocol) server on QX1000, thus QX1000 becomes the timeserver for its LAN.

Enable Simple Network Time Protocol Client enables the SNTP client on the QX1000, thus QX1000 becomes a client to an external timeserver. A checkbox disables Date and Time drop down lists and enables the following parameters:

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

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

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

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

Please Note: You can add another NTP server to the list if the defined NTP servers are not functional (for example, QX1000's date/time is not being updated automatically).

Polling Interval indicates the time interval for the periodical synchronization between the timeserver and QX1000. It counts in hours.

Attention: **Time and Date Settings** will be reset if QX1000 has lost power.

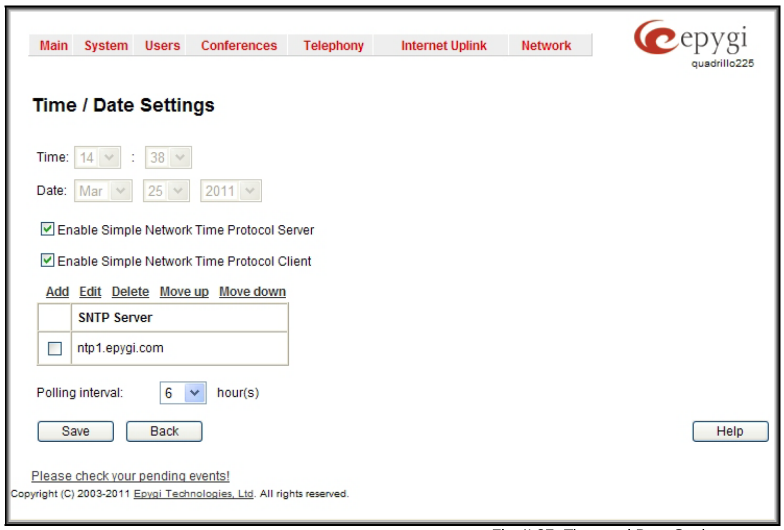


Fig. II-37: Time and Date Settings page

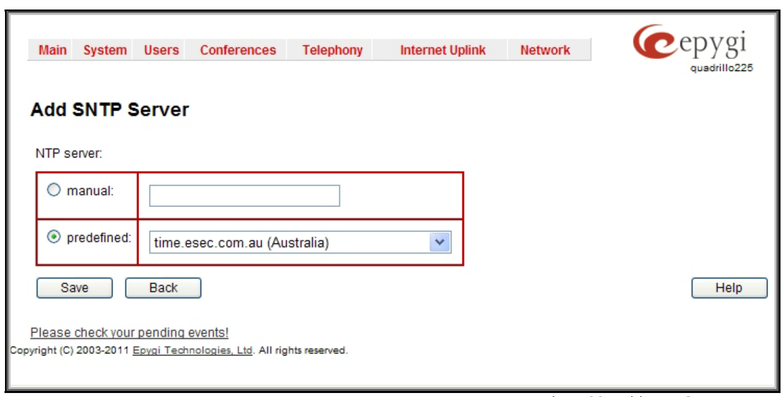


Fig. II-38: Add NTP Server page

Mail Settings

The **System Mail Settings** page allows you to send warnings automatically about the board status or problems to the administrator. System events that require email notification are selected on the Events page. System mail must be enabled and the SMTP server needs to be configured for voice message transmission to the extension user's mailing account.

QX1000 may automatically generate emails to the administrator:

- If events specified in the Events list occur,

- If voice mails are set from the Voice Mail Settings to be sent as e-mail.

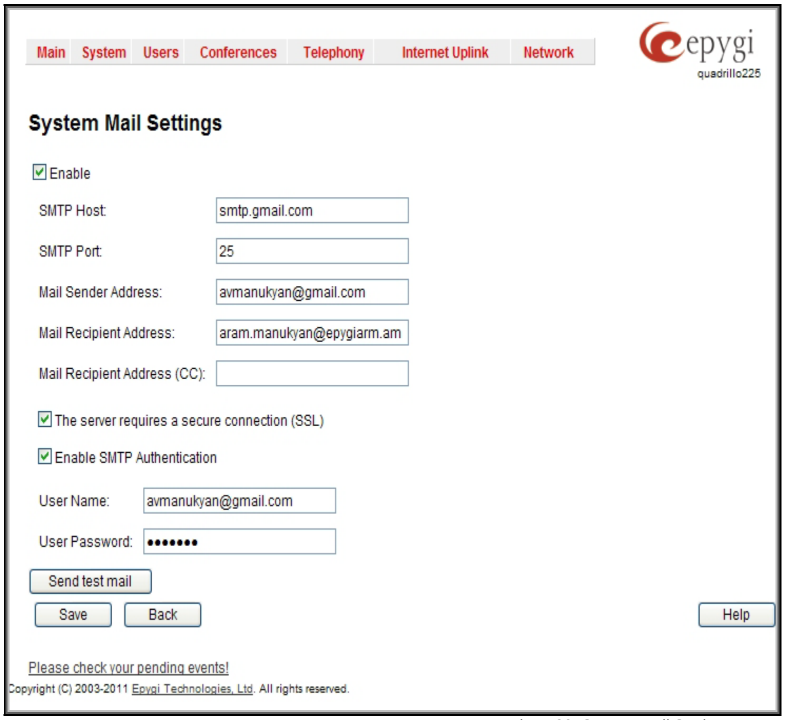


Fig. II-39: System Mail Settings page

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

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

SMTP Port requires the SMTP host port number.

Mail Sender Address text field requires the source address for the QX1000 notification emails. The email address defined here should be an existing valid email address registered on the selected SMTP server or it should have permission to use that particular SMTP server for e-mail transmission.

Mail Recipient Address text field requires an active email address where system emails will be delivered. The e-mail recipient here can be a QX1000 administrator or someone responsible for network and system problems.

Mail Recipient Address (CC) text field requires an active email address where a carbon copy (CC) of the system e-mails will be delivered.

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

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

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

With the button **Send Test Mail** a test mail can be sent to the defined email address to verify the settings. This button will be enabled if correct values have been submitted and saved on this page.

To configure the System Mail

1. Enable the system mail sending by the **Enable** checkbox selection.
2. Update or set the SMTP host in the **SMTP Host** text field.
3. Update or set the e-mail sender address in the **Mail Sender Address** text field.
4. Update or set the e-mail address in the **Mail Recipient Address** text field.
5. Enable **SMTP Authentication** if it is required on the server.
6. Insert into the corresponding text fields an authentication **User Name** and **User Password** defined by your SMTP server.
7. Press the **Save** button to submit these settings.
8. Use the **Send Test Mail** button to send a test e-mail with the configured settings.

SMS Settings

The **SMS Settings** are used to configure the SMS parameters that will allow QX1000 to send the voice mail notifications or event notifications via SMS to the extension user's mobile phone. Every extension user can enable voice mail notifications when a new voice mail is received and they can to define their own mobile numbers from the Voice Mail Settings or to set the certain Events notification to be delivered per SMS. However, for QX1000 to deliver SMS notifications, the SMS service should be enabled and SMS settings should be configured from this page.

Enable SMS Service enables the SMS service on the QX1000.

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

SMS Sender Address requires the source address for the QX1000 notification SMS. The address defined in this field will be seen in the "From" field of the SMS delivered to the mobile phone.

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

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

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

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

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

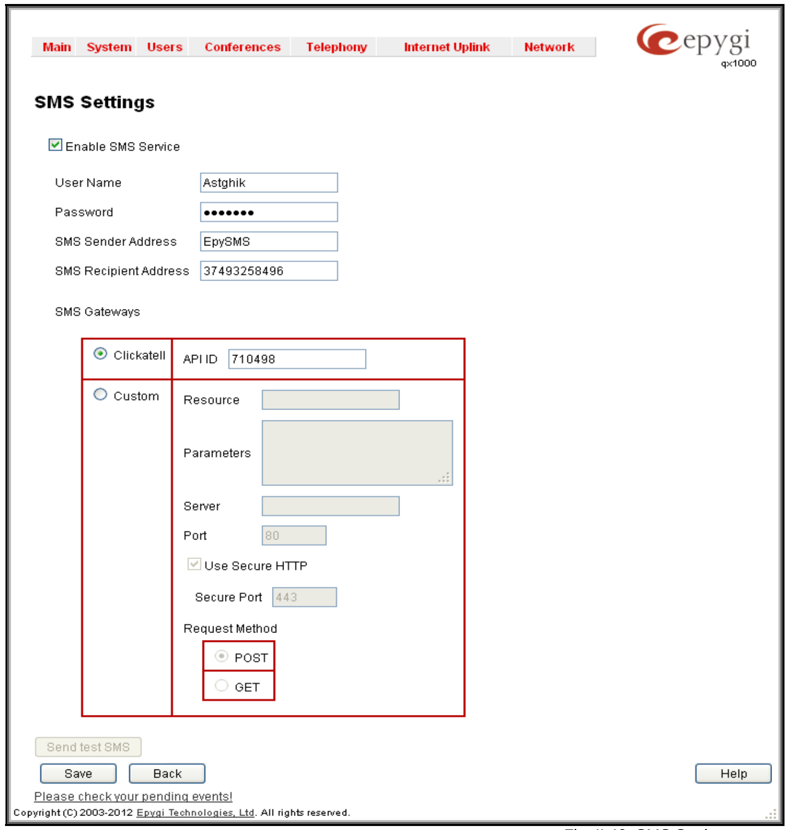


Fig. II-40: SMS Settings page

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

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

%username% – indicates the username defined in the field **Username**
%password% – indicates the password defined in the field **Password**
%to% - indicates the password defined in the field **SMS Recipient Address**
%from% - indicates the password defined in the field **SMS Sender Address**
%text% - indicates the SMS text generated by QX1000 (voice mail notification, event notification, etc.)

Server text field requires the IP address or the host name of the SMS gateway.
Port text field requires the port number of the SMS gateway.
Use Secure HTTP checkbox enables access to SMS server via HTTPS. Checkbox selection enables a **Secure Port** text field that requires the port number for HTTPS traffic.
Request Method manipulation radio buttons allow to select the HTTP request method used by QX1000 the access the SMS gateway: **POST** or **GET**.

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

Firmware Update

This window allows updating the software of QX1000 by installing new firmware (image). Users registered at Epygi will receive a notice when new firmware is available and will be able to download it from the Epygi Technical Support WEB page.

Please Note: Installing new firmware will take about 15 minutes. During this time, QX1000, telephony and Internet access will be disabled.

Attention: When the older firmware is installed on the QX1000, the system configuration will be lost and the device will be factory reset.

Please Note: It is recommended to backup the configuration prior to upgrading the firmware. You can do that by clicking the **Download Configuration** link, which generates a backup file with all configuration settings and user uploaded greeting messages. It opens a file chooser window for immediate download to the users PC.

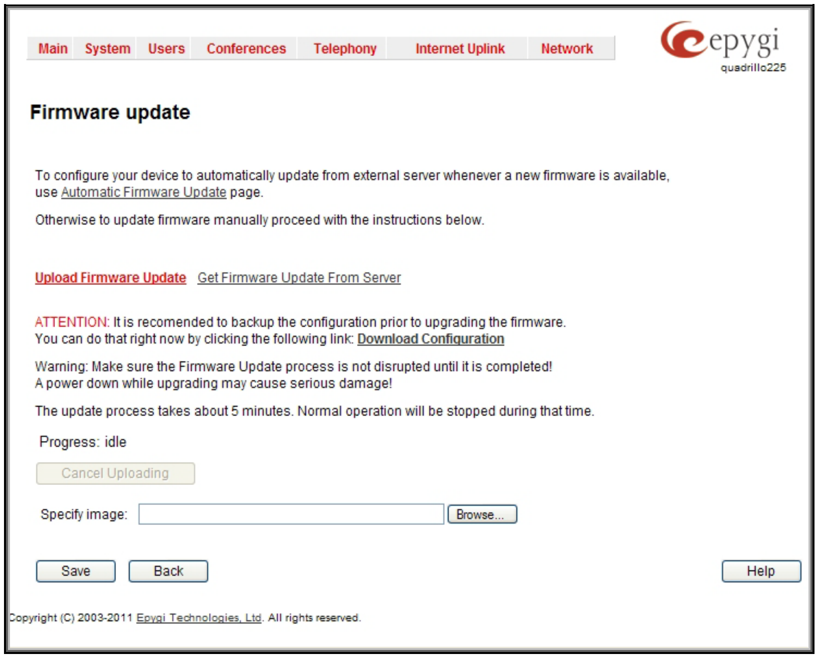


Fig. II-41: Firmware Update page

The following main processes will be stopped during the firmware update and will be restarted after the installation is completed:

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

The Automatic Firmware Update link leads you to the page where the automatic update of the QX1000's firmware (software image) can be configured.

To update firmware manually select one of the options: **Upload Firmware** or **Get Firmware From Server.**

The **Upload Firmware** procedure is created in 3 pages. In the first page of **Upload Firmware** the image file should be selected.

Specify Image text field displays the selected image filename.

Browse button used to browse the image file.

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

The **Cancel Uploading** button appears when the update procedure starts and it is used to stop it.

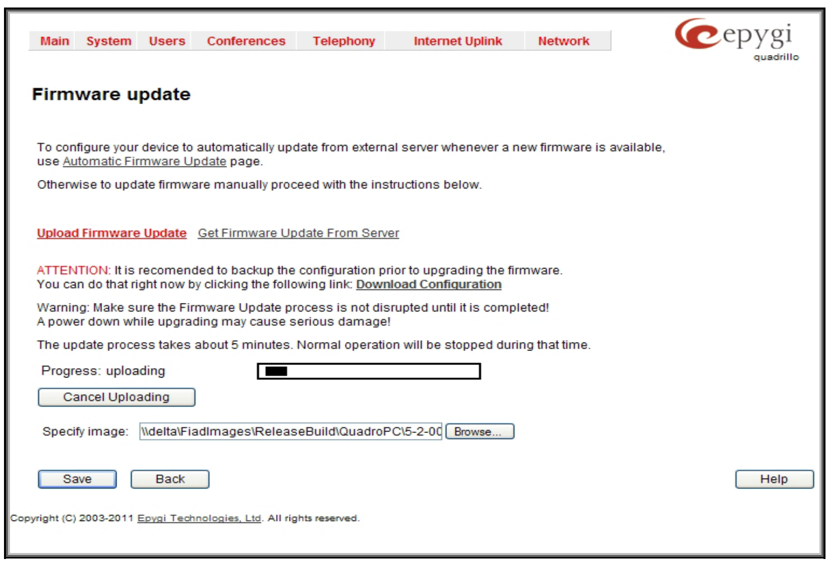


Fig. II-42: Firmware Update page

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

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

This page needs to be confirmed in order to continue image updating. If you are sure that the image version is appropriate for your device press **Yes,** otherwise press **No**.

After pressing **No**, press **Discard this image** button to start upload a new image.

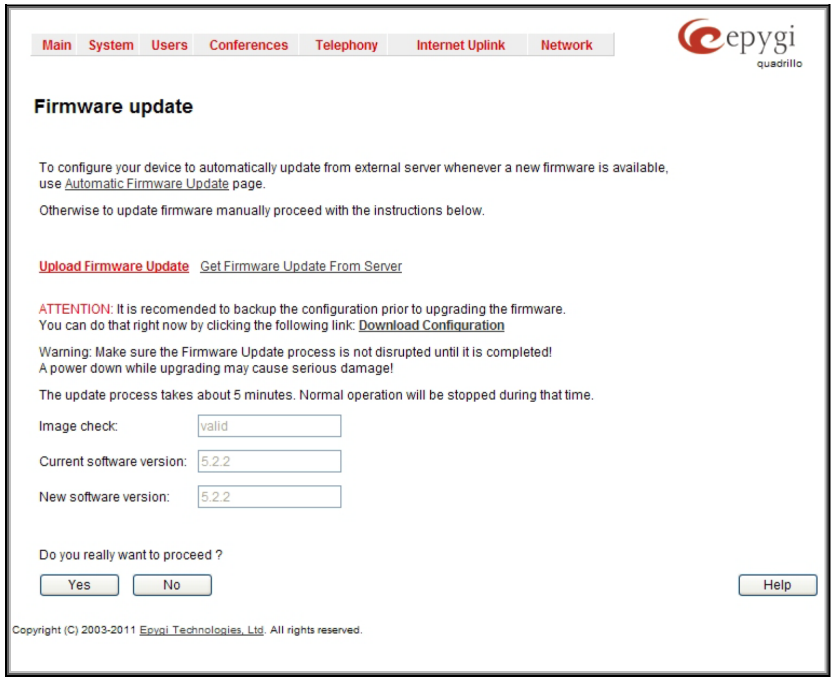


Fig. II-43: Firmware Check page

If you have confirmed the firmware version, a new page with firmware update progress will be displayed next. There are no functions available on this page, just information about the firmware update procedure. At some point the connection with the device is being lost and you need to wait until the firmware will be burned on the QX1000.

You will not be automatically redirected to the Login page. To access the QX1000’s Web GUI, you need to connect QX1000 again and login.

Attention: After the firmware update, all IP phones attached to the QX1000 should be restarted.

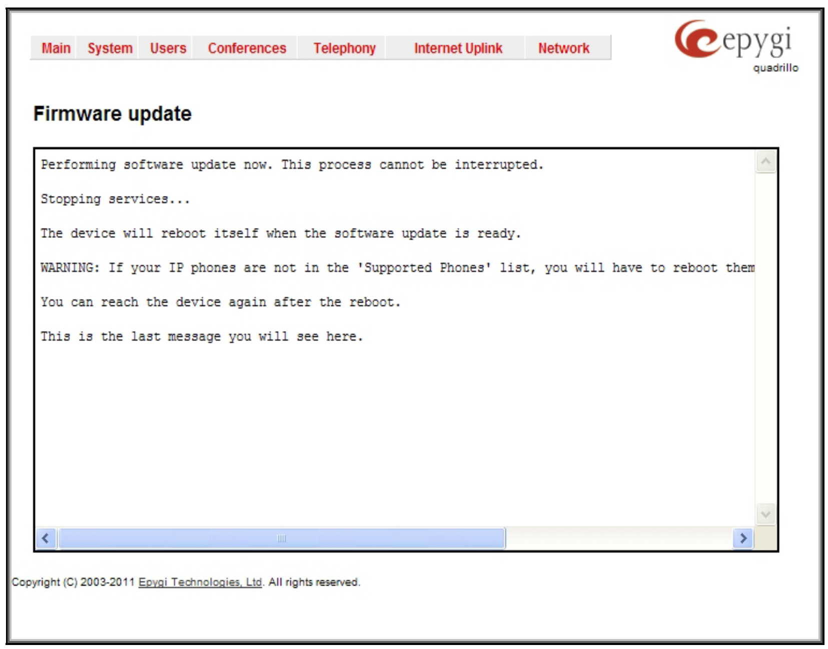


Fig. II-44: Firmware Update page

The **Get Firmware From Server** option allows you to get a new Firmware (image) from the FTP server.

Firmware URL text field requires the path of new firmware image which located on the FTP server.

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

You should save changes before **Download** or **Download and Update**.

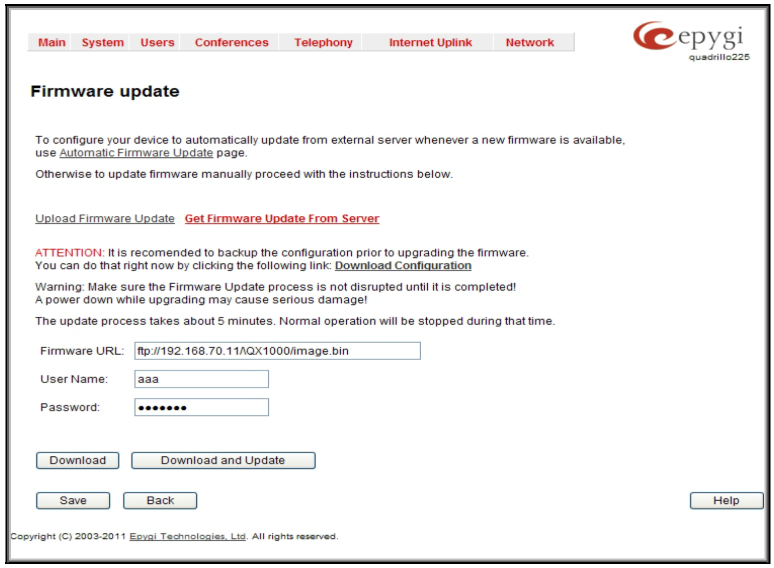


Fig. II-45: Firmware Update page

Pressing the **Download** functional button a new page with firmware download process will be displayed.

This page displays non-editable information about the image validity. **Last Status** shows that firmware download process is running and whether the new firmware version is downloaded or not.

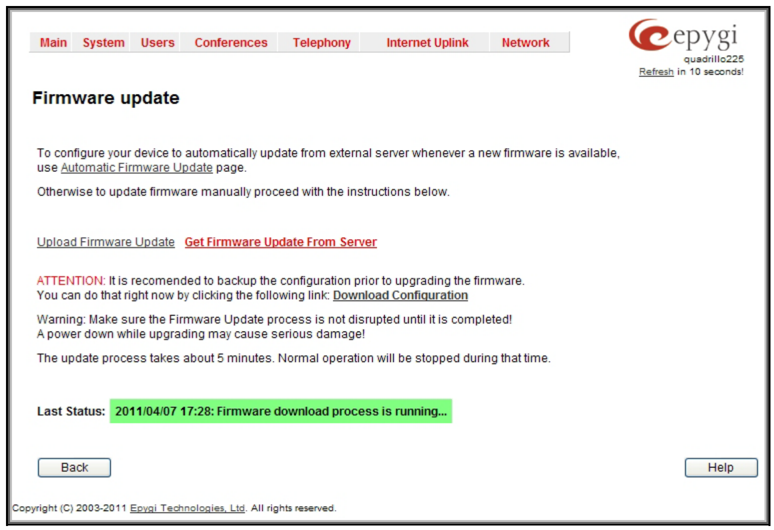


Fig. II-46: Firmware Update page

The **Image Check** field will display “invalid” if the image does not correspond to the hardware version.

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

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

If you have confirmed the firmware version, a new page with firmware update progress will be displayed next. There are no functions available on this page, just last status about the firmware update procedure. At some point the connection with the device is being lost and you need to wait until the firmware will be burned on the QX1000.

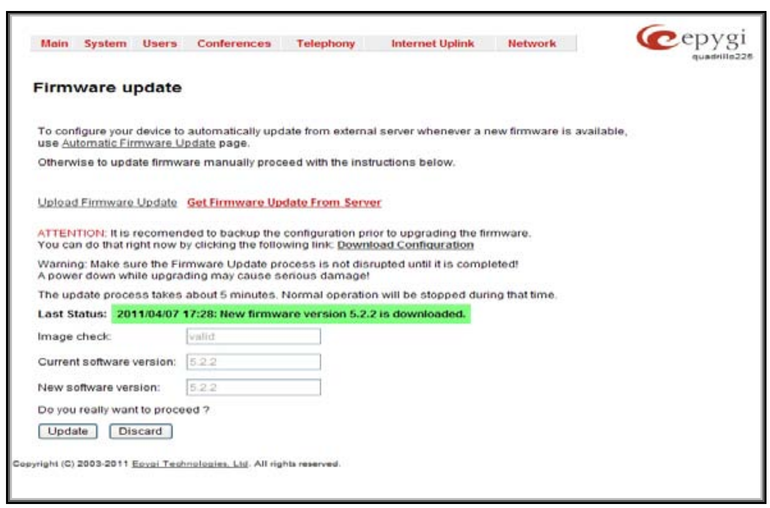


Fig. II-47: Firmware Update page

The **Download and Update** functional button will automatically download and update the firmware version from the FTP server.

Pressing the **Download and Update** functional button a new page with firmware download process will be displayed.

This page displays non-editable information about the image validity. **Last Status** shows that firmware download and updating process is running.

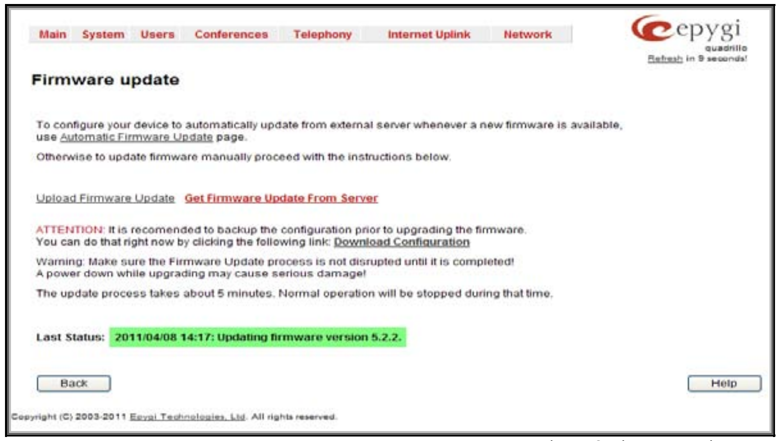


Fig. II-48: Firmware Update page

Automatic Firmware Update

The **Automatic Firmware Update** page allows you to configure an automatic update of the QX1000's firmware (software image) as it becomes available on the server. When this service is enabled, on the configured day and time QX1000 will automatically check for a new available firmware on the server and will either notify the administrator or update the firmware right away, depending on the configured settings.

The server configuration can be done manually.

Please Note: Independent on the selected server type, there should be an "**auto-update**" folder in the root directory of the server. QX1000 will check for any new firmware in that specific folder only. Besides the firmware *.bin file, the "**auto-update**" folder should contain supplementary file(s) to point to the correct firmware file.

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

This page consists of the following components:

The **Enable Automatically Firmware Update** checkbox selection enables the automatic firmware update service on the QX1000.

The **Server Name** (the IP address or hostname), the **Server Port** and the **Update Method** should be defined. The **Update Method** drop down list provides a possibility to choose among FTP, HTTP or HTTPS methods. For some of these selections, authentication **Username** and **Password** can be entered.

Please Note: In order to use Epygi's public ftp server leave the **Server Name**, **Server Port**, **Update Method, User Name** and **Password** text fields to their default values (*ftp.epygi.com*, *21*, *ftp* and *anonymous* respectively, use blank for password).

Check for updates options allow you to select the frequency of checking for a new update.

- **Check and notify** – choose this selection if you only wish to be notified about the new available firmware on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the QX1000 will check for a new firmware available on the server. The way of notification is configured from the Events page.
- **Check and update** – choose this selection to check and automatically install the new firmware on the QX1000 as it becomes available on the server. With this selection, on the indicated weekday and time, on daily or weekly basis, the QX1000 will check for a new firmware available on the server, will automatically download and install it on the QX1000.

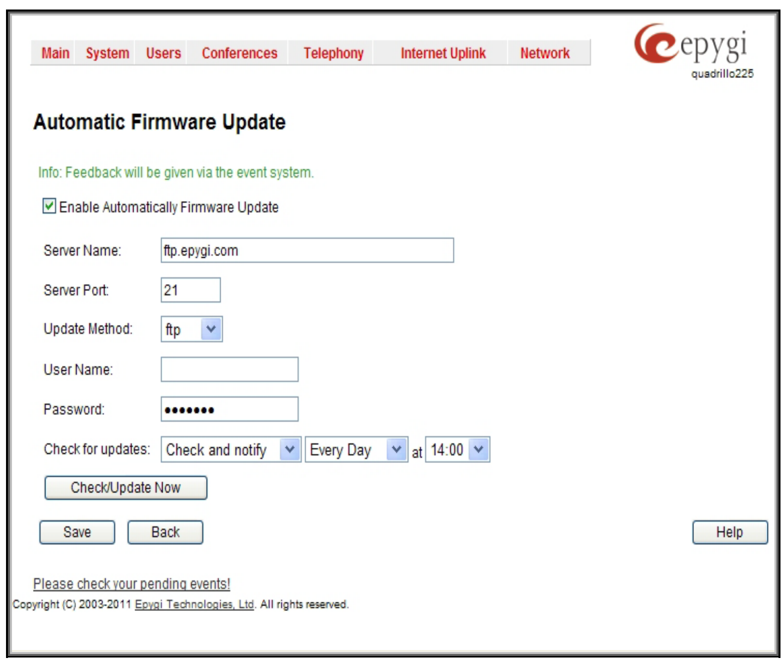


Fig. II-49: Upload Configuration page

The **Check/Update Now** button is used to manually initiate **Check and notify** or **Check and update** actions. The action to be executed depends on the options selected above.

Networking Tools

The **Networking Tools** page provides the possibility to check the Internet connection.

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

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

Attention: No **Traceroute** is possible if a high priority Firewall has been enabled (see chapter Firewall).

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

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

Ping Target requires the destination (IP address or host name) for the ping request. If **Use ICMP** checkbox is selected, an ICMP request will be send to the ping destination (MS Windows standard). Otherwise, if checkbox is not selected, a UDP request will be send (Linux standard).

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

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

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

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

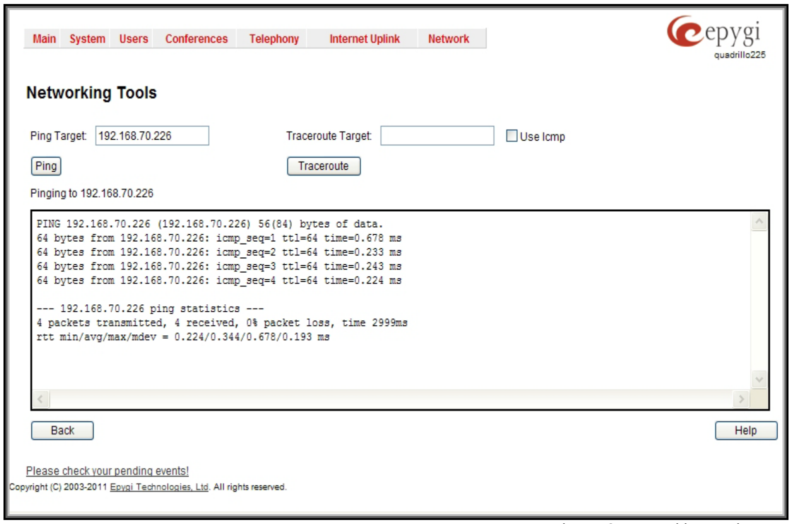


Fig. II-50: Networking Tools page

To Check the Internet connection

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

SNMP Settings

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

On QX1000, SNMP agent is running to allow administrators to remotely manage QX1000'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 QX1000 or remotely modify QX1000's settings.

SNMP Settings page is divided into two pages: **Global SNMP Settings** and **SNMP Trap Settings**. **Global SNMP Settings** are used to enable the SNMP agent on the QX1000, to select the SNMP protocol version for communication with the administrating application and to define the community for administrating application to connect the QX1000.

Enable SNMP checkbox is used to enable SNMP agent on the QX1000.

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

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

Enable SNMP v1 / 2c checkbox is used to enable SNMP v1/2c protocol version for the messaging between QX1000's SNMP agent and the administrating application. If this checkbox is not selected, **SNMP v1** will be implied.

SNMP v1 / v2c Read-Only Community text field is used to insert the community description (public, private, etc.) for the read-only management (like gathering information (events, statistics, etc.) about QX1000's). Field may contain some kind of password which should be matching both on QX1000 and on the administrating application for successful SNMP management.

Enable SNMP v1 / 2c Read-Write Access checkbox additionally enables a read-write access on the QX1000 for the SNMP monitoring application. With this checkbox enabled, administrator will be able to remotely configure the QX1000 via SNMP administrating program.

SNMP v1 / v2c Read-Write Community text field is used to insert the community description (public, private, etc.) for the read-write management (like gathering information (events, statistics, etc.) about QX1000's and remotely changing QX1000's configuration). Field may contain some kind of password which should be matching both on QX1000 and on the administrating application for successful SNMP management.

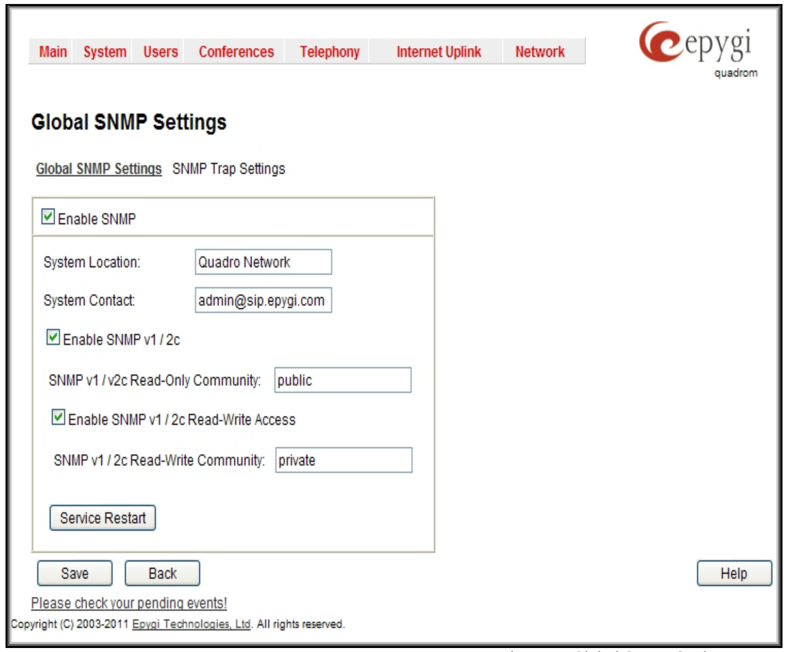


Fig. II-51: Global SNMP Settings page

The **Service Restart** button restarts the SNMP sub-system on the QX1000. Restarting the SNMP sub-system is recommended if it does not respond to a SNMP manager's requests.

SNMP Trap Settings are used to define the traphosts that should be informed when certain events occur on the QX1000. For the listed traphosts to be informed about the events on the QX1000, **Send SNMP Trap** action should be configured for the corresponding event(s) from the Events page.

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

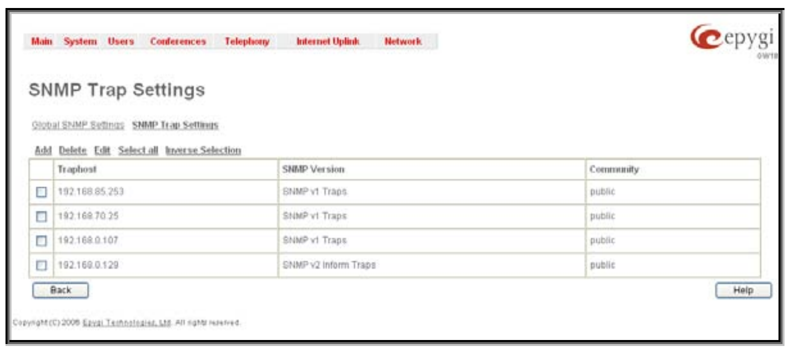


Fig. II-52: SNMP Trap Settings page

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

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

Community text field requires community description (public, private, etc.) for the administrating application to accept the notifications about the certain events on the QX1000. Field may contain some kind of password which should be the same both on QX1000 and on the administrating application for successful SNMP management.

A group of radio buttons is used to select the SNMP protocol version used for events notifications delivered by the QX1000 to the administrating application.

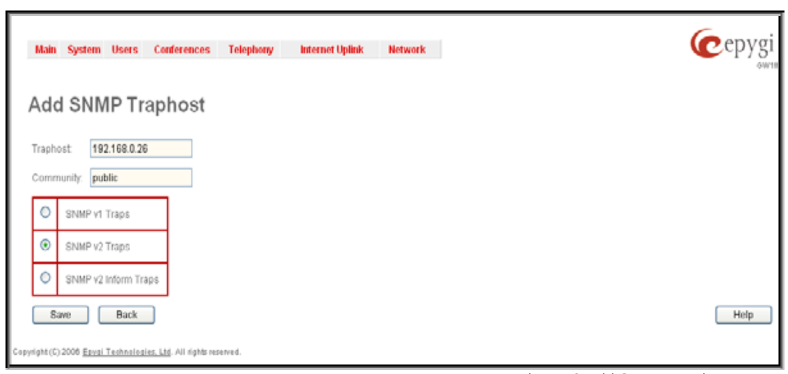


Fig. II-53:Add SNMP Traphost page

Diagnostics

The **System Diagnostic** page gives a possibility of running Network protocol diagnostics to verify QX1000's connectivity and to download all system logs for possible problems recovery.

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

The **Reboot this Device** button is used to reboot the QX1000. Please note that the session with the QX1000 will be closed, i.e., the QX1000 GUI should be newly opened and a new login will be required afterwards.

The **Download system logs** button is used to download all logs to the local PC as a *.tar archive file. These logs can then be used by the Epygi Technical Support Office to determine the problem that has occurred on your QX1000.

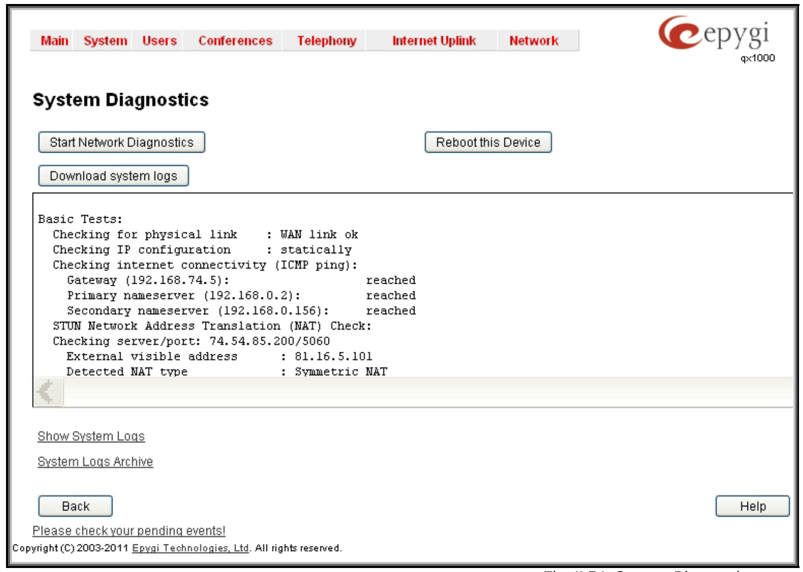


Fig. II-54: System Diagnostic page

The field below will display the diagnostics results and the connectivity conditions. The system should be reconfigured if problems occur during the diagnostics.

Show System Logs link leads to the page where QX1000’s logs might be viewed, downloaded and the logging setting may be adjusted.

System Logs Archive link leads to the page where an automatically collected system logs can be managed. System logs archive starts automatically each time you run QX1000 since last reboot.

System Logs

The **System Logs** page is accessible by pressing the **Show System Logs** link on the **Diagnostics** page. This page is used to adjust where system logging settings, view system logs directly in your browser or download them locally to your PC.

The **System Logs** page consists of three sub-pages.

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

The **Enable User Logging** checkbox is used to enable user level logging. This logging contains brief information about events on the QX1000.

The **Enable Developer Logging** checkbox is used to enable developer high level logging. This logging contains detailed information about events on the QX1000.

The **Mark all Logs** button is used to set a line marker in the logs. If you need to follow a certain piece of log, push this button to set a starting mark in all logs and then perform the needed actions over the QX1000. When the actions are done, push this button again to set an ending mark in all logs. This way you shall clearly see a piece of log between the staring and ending marks generated during the certain actions taken over the QX1000. The **Comment** text field is used to insert some text information which will be displayed next to the marks inserted in the logs. This comment may describe the problem captured in the following logs and may be useful for the Technical Support.

The **Download all Logs** button is used to download all logs to the local PC as a *.tar archive file. These logs can then be used by the Epygi Technical Support Office to determine the problem that has occurred on your QX1000.

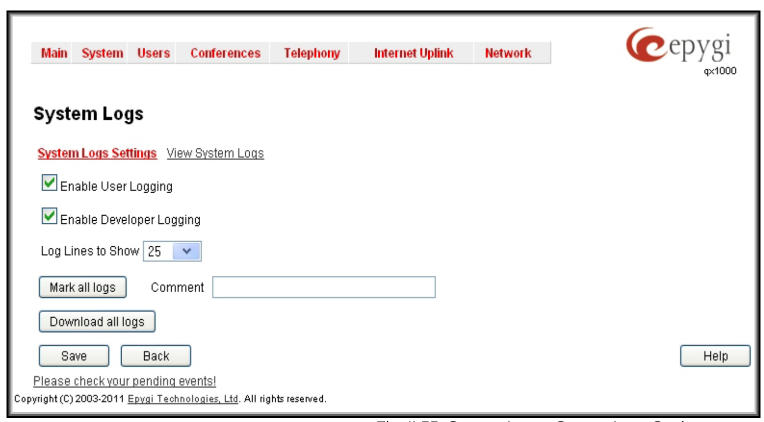


Fig. II-55: System Logs - System Logs Settings page

In the **View System Logs** page you may view the generated logs on the QX1000. System logs are useful to determine any kind of problems on the QX1000 as well as to monitor the user's access and the usage of it.

On the left side of the page, a list of main logs is displayed. Clicking on the needed link will display the most recent log lines. The number of log lines displayed on this page is set on the **System Logs Settings** page.

The text field on the left side is dedicated for support personnel only and is used to search a custom log not listed on this page. To do so, insert a required log name to the text field and press **Show Custom Log** functional button.

If the user has used **Logs Collection** (*82) feature code after or during (from another phone connected to the same QX1000) the call, a special log file will be generated containing the details of that call and few last calls done in the system. This log file will be internally kept in the system until the next time someone used the **Logs Collection** feature code again. The collected logs will be a part of the **System Logs** when user downloads them next time, so it can be reviewed by appropriate support staff. This could be used to collect the logs at the exact moment when a problem has happened.

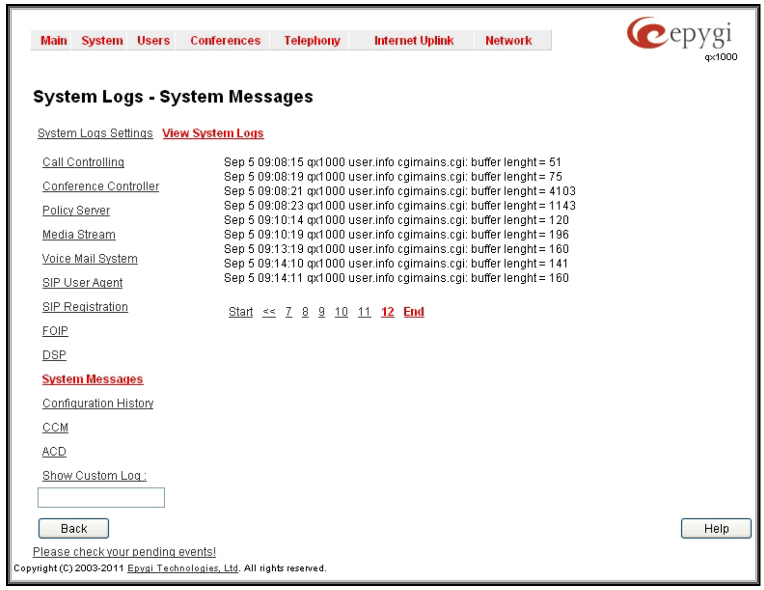


Fig. II-56: System Logs – View System Logs page

System Logs Archive

The **System Logs Archive** page is accessible by pressing the **System Logs Archive** link on the Diagnostics page. The **System Logs Archive** page shows the archived logs table with time period by **Date**. Clicking on the corresponding date will open the archived system logs table in hourly basis. **Hour** shows the initiation time of the system logs. This could be used to collect the logs at the exact moment when a problem has happened. The **Unpacked size on disk** shows the system logs size on disk for the corresponding **Date** and **Hour**.

The following functional buttons are available on this page:

Download link is used to download the archived system logs file to the PC and opens the file-chooser window where the saving location can be specified.

Delete removes the selected entry from the archived system logs table.

Select all selects all entries of the table.

Inverse Selection inverses the current selection (if no entries are selected, clicking on inverse selection will check all entries).

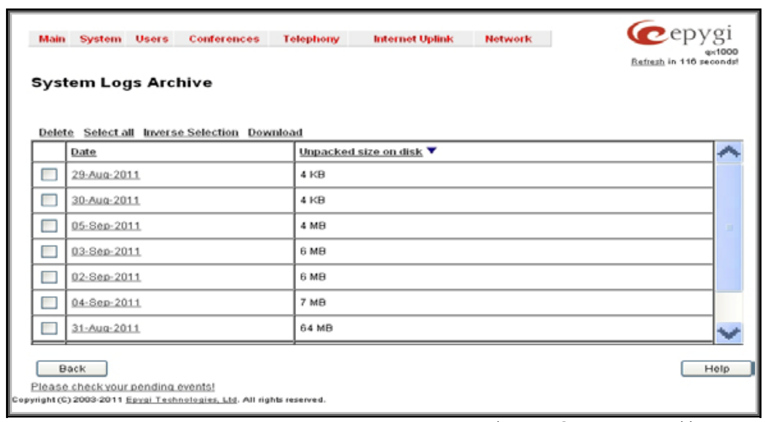


Fig. II-57: System Logs Archive page

Features

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

- **3 No Key Found** - the feature is currently not available
- **Reboot Needed** - the feature key has been entered and QX1000 needs to be rebooted
- **Activated** - the feature is now available on the QX1000

Following features may be activated via the software key:

- **Debug** – enables Telnet connection towards the Quadro for debugging purposes.
- **3pcc Support** - enables Third Party Call Control feature on the QX1000. The feature allows the call controlling applications running on a user PC to remotely initiate and handle calls on the QX1000 and to subscribe for certain event notifications from the QX1000.
- **ACD Support** – enables the ACD Management feature which provides contact center solution for queuing and automatic distribution of the calls between contact center agents.

- **Barge In** – enables the Barge In Service on the QX1000. The feature allows the PBX users to participate to the third party's calls while remaining imperceptible.
- **Redundancy** – activates the Redundancy feature on the QX1000.
- **DCC Pro Support** - allows run with QX1000 the Pro-level Desktop Communication Console (the application description can be found at Epygi Technical Support).
- **DCC Basic Support** - allows run with QX1000 the Basic-level Desktop Communication Console (the application description can be found at Epygi Technical Support).
- **IP Phone support** - enables additional LAN-sided IP phones support on the QX1000. 200 SIP phones are activated by default. Up to 800 additional SIP phones may be added with feature keys using the 16, 32 or 64 IP Phone Expansion Keys.
- **Autodialer Support** - allows run with QX1000 the Autodialer application (the application description can be found at Epygi Technical Support).
- **QCM Support** – allows QX1000's extensions to be used by QX1000 Communication Manager after QCM trial period expires. Depending on the feature key type, additional 4 or 10 QCM licenses can be activated on the QX1000.
- **Conference Server** – activates the Conference Server feature on the system, enabling it to act as a standalone conference server. This allows up to 288-person conference calls to be set up and offers a bundle of helpful features to manage the conferences.
- **Call Recording** – activates the **Call Recording** feature which is used to record PBX, SIP or PSTN calls on the QX1000 and save the recordings into the local recording box or upload to the remote server.
- **Video Conferencing** – activates the **Video Conferencing** feature on the system. This allows video conference calls of up to 104 participants.

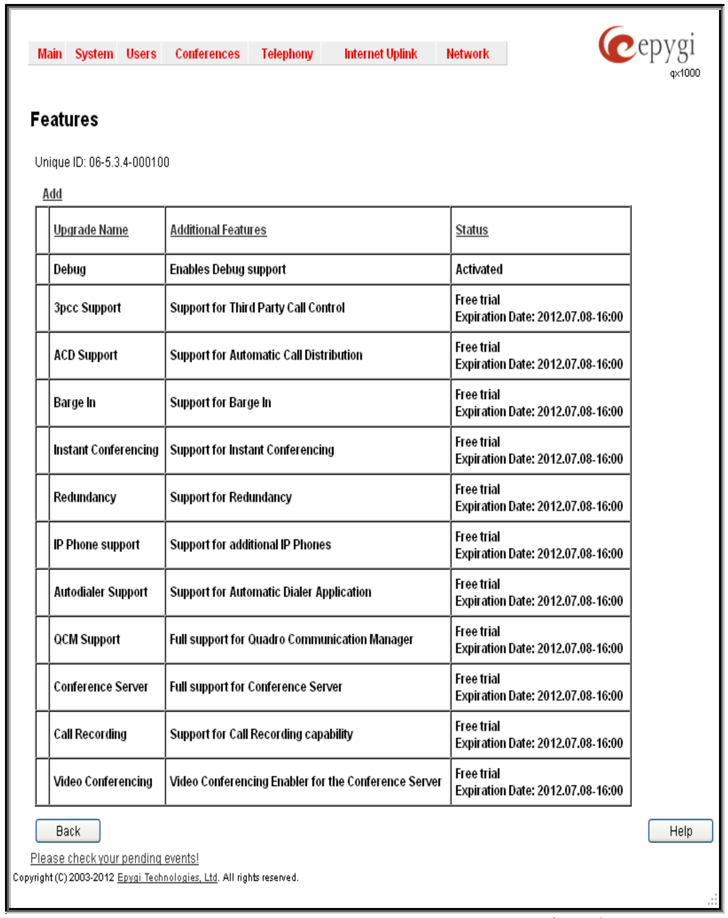


Fig. II-58: Features page

To enter a **Feature Key**, click **Add**. A page with the **Feature Key** text field is opened. Enter the key and press **Save**. The status of the selected feature entry will change to **Reboot needed**. Reboot the QX1000 and the feature will receive the status **Activated.**

To receive a **Feature Key**, register the QX1000 device and send a corresponding request to Epygi's Technical Support. This request must include the **Unique ID** that is displayed in the **Features** page above the features list.

Fig. II-59: Features Add page

Upload Language Pack

The **Upload Language Pack** page allows you to upload a custom language for GUI and Voice Messages of the QX1000. The language of voice messages can be switched to the custom Language Pack language from the GUI setting page in the System Configuration Wizard. The language of GUI session can be changed to the custom Language Pack language from the radio buttons on the login page.

Uploading a language pack will also change the language of some supported IP phones (Aastra, snom v.6.x, Grandstream GXP2000). After a custom Language Pack is uploaded onto the system, reboot the IP phone to load a matching language onto the phone.

Please Note: Only one custom Language Pack can be uploaded at the time. Uploading a Language Pack will remove the existing one (if applicable) and will reboot the QX1000.

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

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

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

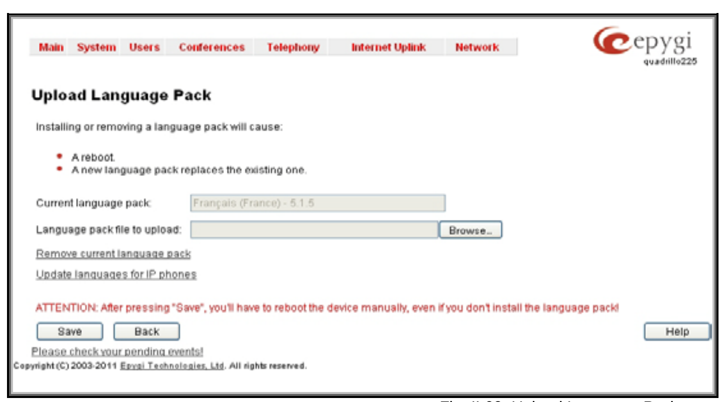


Fig. II-60: Upload Language Pack page

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

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

Attention: Pressing the **Save** button will stop some vital processes on the QX1000, therefore you will need to reboot your device manually even if you have cancelled the language pack update procedure on the following steps.

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

Update Languages for IP Phones

The **Update Languages for IP Phones** page is used to upload a custom language pack to the IP phone. This page only contains those IP phones that support custom language pack uploading from the QX1000.

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

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

Fig. II-61: Update Languages for IP Phones page

The next page displayed will show verification of the language pack being uploaded and asks for confirmation to overwrite the existing custom language pack (if applicable). After final confirmation, QX1000 will upload the selected custom Language Pack to your IP phone. You should then reboot your phone to make the new language pack active.

User Rights Management

The **User Rights Management** service sets restrictions on the GUI access for various users, permits or denies the access to certain Web GUI configuration pages and creates multilevel user management of the QX1000. The feature is useful to the ISPs in order to set the restrictions for certain customers to manage the QX1000's configuration.

Two levels of QX1000 GUI administration are available:

- **Administrator** – this is the main administrator's account. The administrator can configure to have the factory reset safe the default password or choose not to. The administrator has access to all Web GUI pages and no one else has configuration permission to adjust this account. The administrator is responsible for granting access to all other user groups.
- **Local Administrator** – this is a common (sub-) administrator's account. The password is not factory reset safe. Local Administrator can have permission to adjust each GUI page.
- **Extension** – this account refers to all extensions created on the QX1000. The password for default extensions is not factory reset safe but is contained in the backed up configuration. Permissions for an extension to access each GUI page can be adjusted here.

The **User Rights Management** page consists of two pages. The **Users** page is used to manage the available users on the QX1000. The **Roles** page is used to assign the corresponding permissions to the users.

The **Users** page contains a table where the Administrator and Local Administrator users are listed. This page allows them to modify the passwords of available users in the table and to manage the Local Administrator's account. The following functional buttons are available on this page:

The **Change Password** functional button is used to change the password of the Administrator and Local Administrator user's account. Select one of the available users in the table by toggling the corresponding checkbox and press **Change Password** to open the corresponding page.

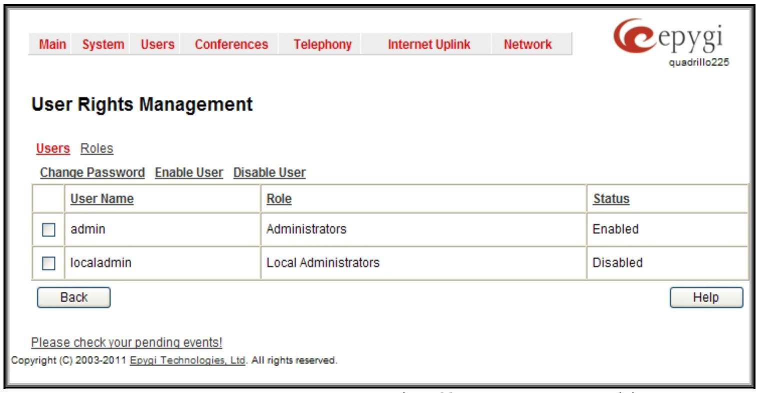


Fig. II-62: Users page at User Rights Management

For **Administrator** or **Local Administrator** account the **Change Password** page contains two parts - one for **GUI Access Password**, the other one for **Phone Access Password**.

The **GUI Access Password** offers the following components:

- The **Old Password** text field is only present when modifying the Administrator account password and requires the current password of the Administrator. An error message prevents entering the wrong password.
- The **New Password** text field requires a new password for the Administrator or Local Administrator. Reentering the new password in the **Confirm New Password** text field will confirm the new password. The **New Password** field is checked against its strength and you may see how strong is your inserted password right below that field.

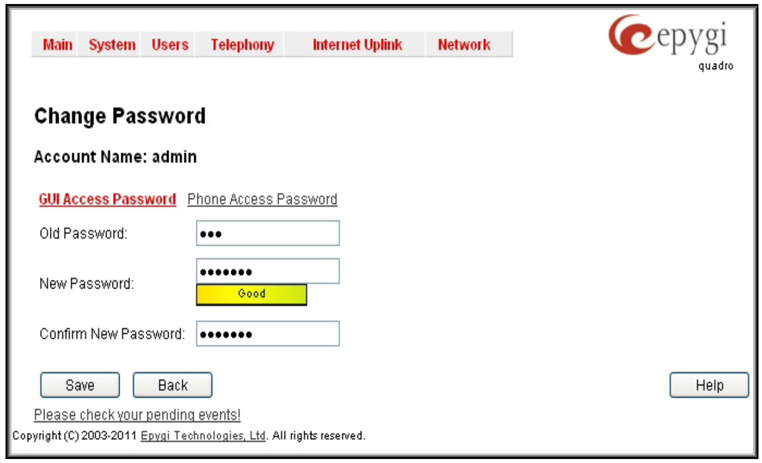
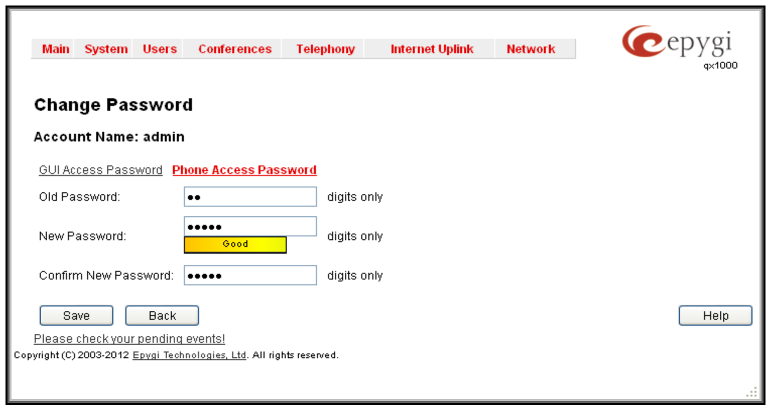


Fig. II-63: Change Password page

Please Note: The password can consist of numeric values and symbols. Up to twenty (0-20) digits and symbols are allowed.

The **Phone Access Password** offers the following components:

- The **Old Password** text field is present when modifying the Administrator account password and requires the current password of the Administrator. An error message prevents entering the wrong password.
- The **New Password** text field requires a new password for the Administrator or Local Administrator. Reentering the new password in the **Confirm New Password** text field will confirm the new password. The **New Password** field is checked against its strength and you may see how strong is your inserted password right below that field. The password can consist of numeric values only. Up to twenty (0-20) digits are allowed. A corresponding warning appears if any other symbols are inserted.



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

Attention: It is highly recommended to define a proper and non-empty password on this page if the extension is being used for the Call Relay service from the QX1000's Auto Attendant.

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

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

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

Fig. II-64: Roles page at User Rights Management

On the **Change Access Rights** page, **Grant Access**/**Deny Access** functional buttons are used to grant or deny access to certain GUI page(s) for the selected user.

When access to a certain GUI page is denied for a user, the "You are not authorized to access this page!" warning message will be displayed.

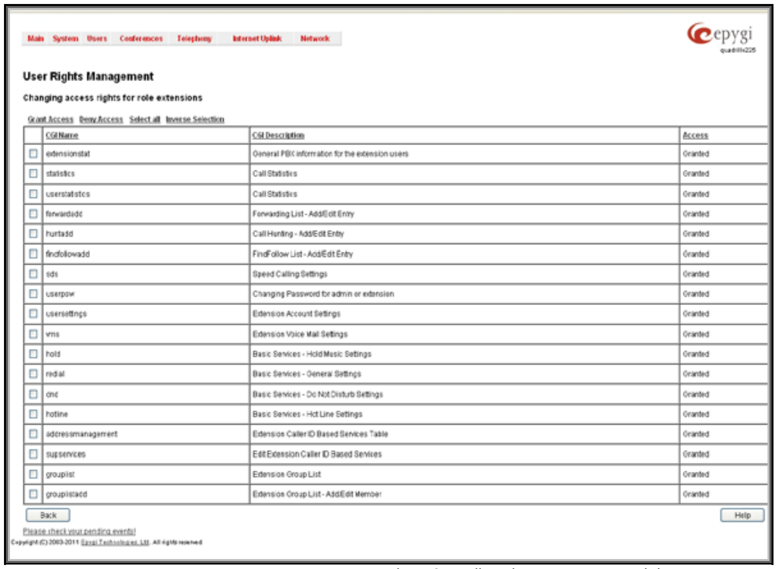


Fig. II-65: Edit Roles page at User Rights Management

Redundancy Settings

Redundancy feature is used to increase QX1000 device availability using second QX1000 as a backup unit. This requires two units running the same firmware version and connected to each other through Ethernet or LAN ports, depending on the device model.

The idea of redundancy is to ensure uninterrupted functionality of the QX1000. The Redundancy Settings should be configured on both QX1000s. One of the QX1000s is configured as a master, the second one as a backup unit.

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

If the master device becomes unavailable, which can be caused by power loss, reboot or network malconfiguration, the second QX1000 becomes automatically available and starts to run as a master device. Depending on the configuration, the second QX1000 can remain master or go to the backup mode once the first device becomes available again.

Attention: During failover procedure all active calls will be disconnected and the system will be out of service during 2-5 minutes (depending on the number of IP phones connected to the system), which is needed for running the applications and rebooting the phones. If there are IP phones in the network that are not auto configured by QX1000 (IP phones not supported by Epygi) or IP phones with the changed login name and password, you will need to reboot them manually. After failover the license keys, firmware and language pack are not being transferred from the master to backup QX1000 therefore, so make sure both QX1000s are configured identically in the redundant network before enabling redundancy mechanism.

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

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

Enable Redundancy checkbox is used to enable/disable the redundancy functionality on the QX1000.

Active Device Mode drop down list is only present on backup device and is used to adjust the behavior of the backup device during unavailability of master device. When **Active** is selected, backup device will become master once the original master device became unavailable. When **Passive** is selected, backup device stops its synchronization with the master device and will not take over the control even when the original master got failed unless **Swap Master Device** button is pressed on the master QX1000. The **Passive** mode is used for Firmware Update, Language Pack and License Key updates on master device when a reboot is required. After the reboot of master device, the **Active Device Mode** on the backup device should be changed back to **Active** to restore the redundant network functionality.

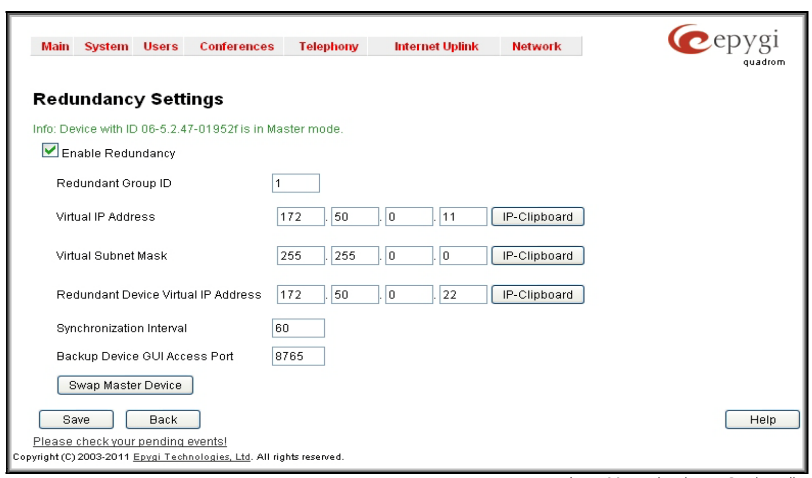


Fig. II-66: Redundancy Settings list

Redundant Group ID text field unique ID (values 1 and up) identifying master and backup devices. The same value must be set on both QX1000s.

Virtual IP Address text fields require the virtual IP address of the device where the configuration is done. **Virtual Subnet Mask** text fields require the virtual subnet mask of the device where the configuration is done. These two parameters identify an alternate IP network of the LAN interface which stays unchanged when the device switches its mode (from master to backup or vice versa). The configuration and voice data synchronization daemon uses this IP address to communicate with the second QX1000.

Redundant Device Virtual IP Address text fields require an alternate IP address of the LAN interface of the second QX1000.

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

Swap Master Device button is used for manual swapping of functionality of master and backup devices. This action will result in rebooting the current master. After rebooting the current master device will start running in a backup mode. Switching the backup to master starts all applications on QX1000 and causes all IP phones to reboot. The swapping takes around 1 minute however another 1-3 minutes are required in order to reboot all the IP phones connected to redundant system. If backup device before swapping was in passive mode then after swapping the master will start running as backup in passive mode, otherwise if it was in active mode then master will start running as backup in active mode.

Download system logs link is only present on backup device and is used to download system logs to the local PC as a *.tar archive file. These logs can then be used by the Epygi Technical Support Office to determine the problem that has occurred on your QX1000.

Users Menu

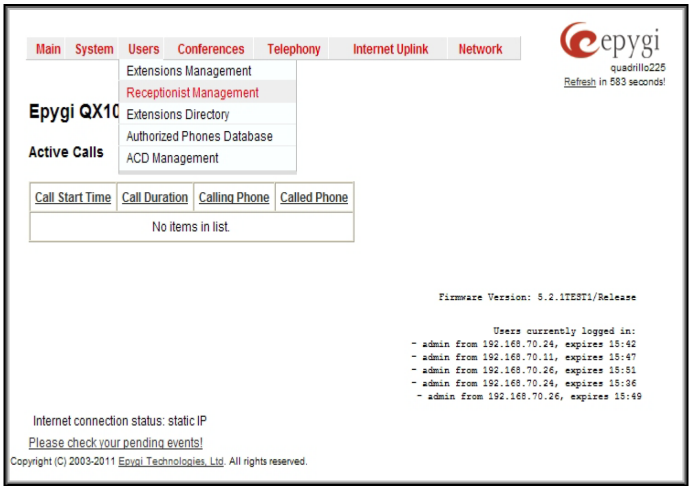


Fig. II-67: Telephone Users Menu in Dynamo Theme

Fig. II-68: Telephone Users Menu in Plain Theme

Extensions Management

The **Extensions Management** page is used to create a variety of extensions and auto attendants on the QX1000. From this page, by clicking on the user extension, the Administrator can go to the extension settings pages.

When this page is accessed for the first time after the QX1000's initial boot-up or the default configuration settings restore, an intermediate page is displayed.

The **Change Extension Length** page is used to define the extension settings applicable to all extensions on the QX1000. This page disappears once being saved.

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

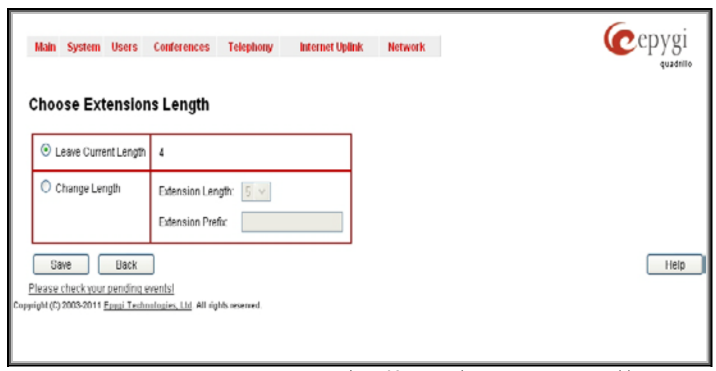


Fig. II-69: Extensions Management - Add Entry page

- **Leave Current Length** radio-button selection is used to leave the current length of extensions on the QX1000. Per default the extensions length on the QX1000 is 4. In front of this selection, the actual configured length of extensions is displayed.
- **Change Length** radio-button selection is used to change the actual length of extensions on the QX1000. This selection enables the following information to be defined:

  The **Extension Length** drop-down list requires you to choose the length of the extensions on the QX1000. This number will apply to all existing extensions on the QX1000 as well as to any newly created extensions. The length of the extension can be 2, 3, 4 or 5.

  The **Extension Prefix** text field is used to define a prefix with which all existing extensions on the QX1000 as well as to any newly created extensions should start. The prefix cannot start with the digits 0 or 9, otherwise an error message appears.

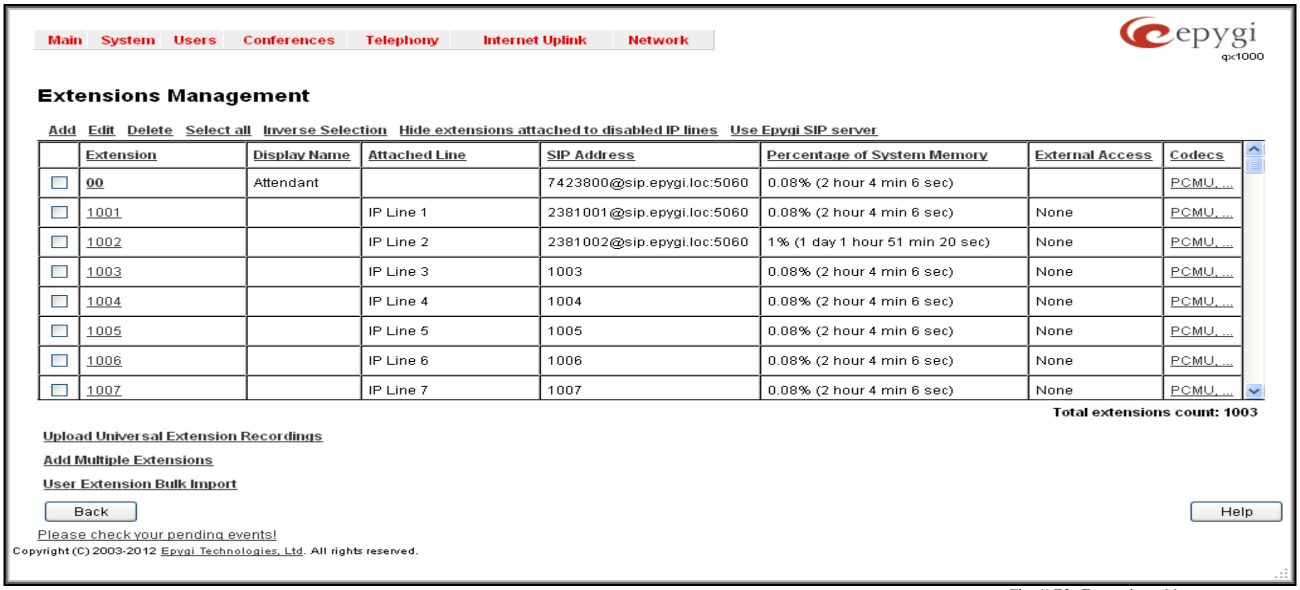
Please Note: By saving the settings on the **Change Extension Length** page, all existing extensions will lose the custom voice messages and voice mails in the voice mailbox. The device will be rebooted. You will not be automatically redirected to the login page, so you need to access it manually again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

Two types of user extensions, **active** and **inactive**, can be created on the QX1000. Active extensions are those that are attached to a line, can place and receive calls and use available telephony services. Inactive extensions are those that are not attached to the line. They can use some available telephony services but they cannot place and receive calls. Instead, inactive extensions have a voice mailbox available to store the messages from callers.

Attendant extensions are dedicated to the IVR system on the QX1000. These extensions are used by callers to reach QX1000’s users and use the remote access and call relay services. It is possible to create Auto Attendants with the custom scenarios. By default, QX1000 has one Auto Attendant extension (00) which is undeletable.

Attention: The system is limited to 1200 extensions! Once the number of extensions in the Extensions table reaches 1200, there will be no more possibility to add new extensions.

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



	Extension	Display Name	Attached Line	SIP Address	Percentage of System Memory	External Access	Codecs
☐	00	Attendant		7423800@sip.epygi.loc:5060	0.08% (2 hour 4 min 6 sec)		PCMU, ...
☐	1001		IP Line 1	2381001@sip.epygi.loc:5060	0.08% (2 hour 4 min 6 sec)	None	PCMU, ...
☐	1002		IP Line 2	2381002@sip.epygi.loc:5060	1% (1 day 1 hour 51 min 20 sec)	None	PCMU, ...
☐	1003		IP Line 3	1003	0.08% (2 hour 4 min 6 sec)	None	PCMU, ...
☐	1004		IP Line 4	1004	0.08% (2 hour 4 min 6 sec)	None	PCMU, ...
☐	1005		IP Line 5	1005	0.08% (2 hour 4 min 6 sec)	None	PCMU, ...
☐	1006		IP Line 6	1006	0.08% (2 hour 4 min 6 sec)	None	PCMU, ...
☐	1007		IP Line 7	1007	0.08% (2 hour 4 min 6 sec)	None	PCMU, ...

Fig. II-70: Extensions Management page

The following columns are present in the table:

- **Extension** - lists user or attendant extensions on the QX1000. This number is used for internal PBX calls.
- **Display Name** - indicates an optional display name to identify the caller.
- **Attached Line** - indicates the IP line corresponding extension it is attached to. “R” is displayed in this column when **SIP Remote Extension** (see below) functionality is enabled on the extension.
- **SIP Address** - displays the SIP address of the corresponding extension. The column displays the full SIP address, (i.e., username@sipserver:port) when the **Registration on SIP Server** checkbox is selected. If registration is disabled, the SIP address will be displayed in the following format: “username, Proxy: sipserver:port”. If no SIP registration server or SIP server port is defined, corresponding information will not be included in this column. If no username is defined, the extension number will be displayed instead.
- **Percentage of System Memory** - indicates the user space (in percentages) configured for each extension. The actual available duration (in minutes) for the extension voice mails, uploaded/recorded greetings and blocking messages is also displayed here. The available minutes corresponding to the selected user space are dependent on the Voice Recording codec selected from the Voice Mail page. For example, for the same amount of marked out user space, selection of the G726 voice recording codec will provide more space for voice mails and user defined voice greetings than the G711 codec selection.
- **External Access** - indicates whether the GUI Login, 3pcc/Click2Dial login or Call Relay options are enabled on the extension.
- **Codecs** – column lists the short information (full information is seen in the tool tip) about extension specific voice Codecs. Extension codec’s can be accessed and modified by clicking on the link of the corresponding extension’s Codecs. The link leads to the Extension Codecs page.

Clicking on each user extension in the Extensions table will open the extension specific **Extension Settings** menu. The Pickup Group, Call Park and Paging Group extensions are displayed without a link in the Extensions Management table and extension pages. Additionally, the supplementary services configuration pages will not be accessible for this type of extensions. Clicking on the Recording Box extension will move to the corresponding extension’s Recording Box where the recorded calls can be managed.

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

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

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

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

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

- Attendant ,
- User Extension,
- Pickup Group,
- Call Park,
- Paging Group,
- ACD Group (if this feature is previously activated from Features page),
- Recording Box (if the **Call Recording** feature is previously activated from Features page).

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

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

Please Note: Save changes before moving among settings groups.

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

Reset SIP Settings functional button is used to reset all SIP settings of the selected extension(s) to the default values, including all settings listed under SIP Settings and SIP Advanced Settings pages (see below).

The **Upload Universal Extension Recordings** link found at the bottom of the page leads to the Upload Universal Extension Recordings page, where universal default voice messages for all extensions can be defined.

The **Add Multiple Extensions** link leads to the Add Multiple Extensions page, where multiple extensions can be added to the Extensions Management table at once.

The **User Extension Bulk Import** link leads to the User Extension Bulk Import page, where group of user-type extensions can be added/modified, configuring their settings or modifying the configurations of group of existing extensions.

User Extension Settings

1. General Settings

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

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

Password requires a password for the new extension.

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

If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

The Password field is checked against its strength and you may see how strong is your inserted password right below that field.

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

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

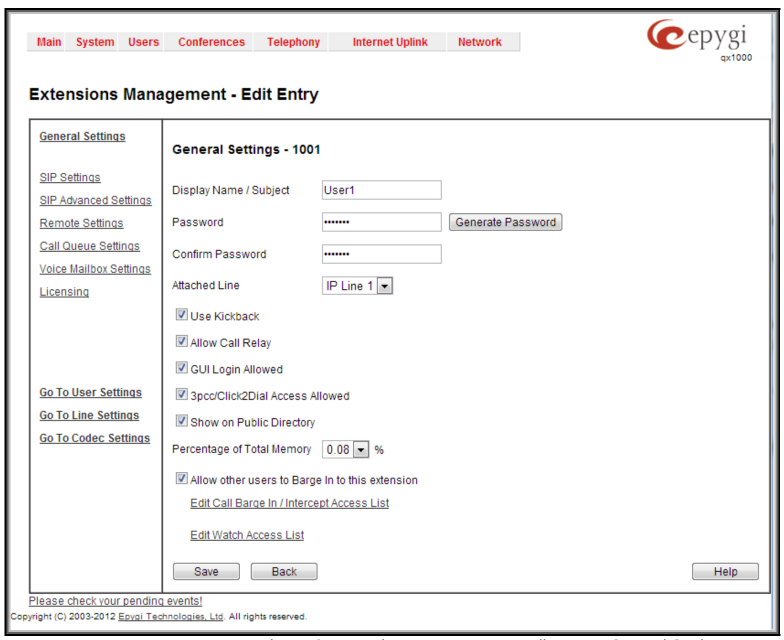


Fig. II-72: Extensions Management - Edit Entry – General Settings page

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

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

Allow Call Relay enables the current extension to be used to access the Call Relay service in the QX1000’s Auto Attendant. It is recommended to define a proper and non-empty password when enabling this feature in order to protect the Call Relay service from an unauthenticated access.

Login Allowed checkbox enables the current extension to be used to access the QX1000 via WEB interface by extension name and password.

3pcc/Click2Dial Access Allowed checkbox enables the current extension to be used with applications based on QX1000 3PCC interface and QX1000 Click to Dial application.

With the **Show on Public Directory** checkbox enabled, the details of the corresponding extension will be displayed in the User Settings table on the Main Page of the Extension’s QX1000 Web Management (accessed by the extension’s login, see Manual III – Extension User’s Guide). Besides this, the details of the extension will be displayed in the Public Directories on the snom and Aastra SIP phones. Leave this checkbox unselected if the extension is reserved or not used, or when the extension serves as an intermediate unit for call forwarding, etc.

The **Percentage of Total Memory** drop down list allows you to select the space for the extension’s voice mails and uploaded/recorded greetings and blocking messages. The maximum value in the drop down list is equal to the maximum available space for voice messages on QX1000. When editing an existing extension and decreasing the voice mailbox size, the system will check the present amount of voice mails in the mailbox of the extension. If the memory required for these voice mails exceeds the size entered, the system will suggest either to remove all voice messages from the extension’s voice mailbox or to select a larger size so that the existing voice messages can be stored in the mailbox.

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

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

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

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

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

Call Intercept Access List

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

This page contains the following functional buttons:

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

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

Attention: **Call Intercept** service calls are not displayed in **Active Calls** table on the Administrator’s Main Page, nor are registered in the Call Statistics.

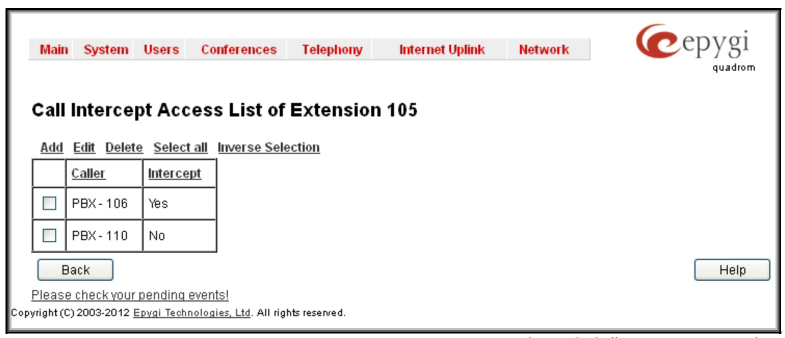


Fig. II-73: Call Intercept Access List

Fig. II-74: Call Intercept Access List - Add Entry

Call Barge In/Intercept Access List

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

This page contains the following functional buttons:

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

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

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

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

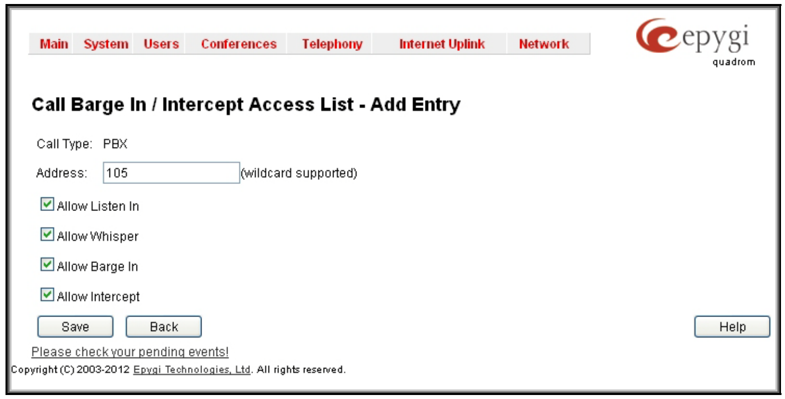


Fig. II-75: Call Barge In/Intercept Access List

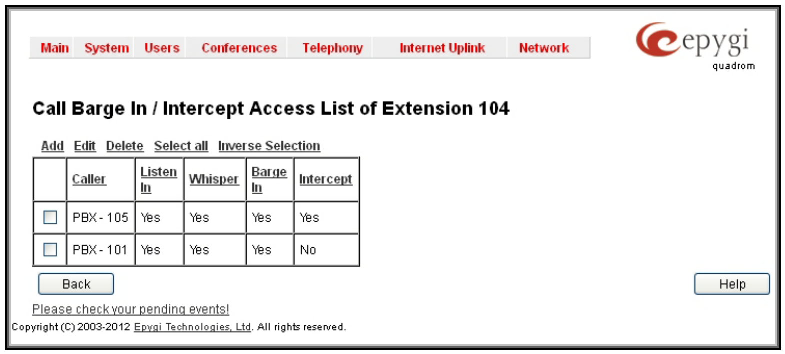


Fig. II-76: Call Barge In/Intercept Access List - Add Entry

Watch Access List

The **Watch Access List** page is used to define a list of extensions that are capable to watch the current extension calls and to define the appropriate permissions.
This page contains the following functional buttons:
Add functional button opens the **Watch Access List - Add Entry** page where extensions may be added to the Watch Access List.
The **Watch Access List - Add Entry** page consists of the following components:

- **Call Type** lists the available call types:
  PBX - local calls to QX1000's extensions.
  SIP - calls through a SIP server.
  Auto - used for undefined call types.

The destination (independent on whether it is a PBX number or a SIP address) will be reached through the Call Routing Table.

- The **Address** text field is used to define the address where the call will be redirected. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the PBX call type is selected, the QX1000 extension number should be defined in this field. For the SIP call type, the SIP address should be defined. For the Auto call type, a routing pattern needs to be defined. The SIP-Clipboard button at the end of the line can be used only when SIP is selected in the Call Type drop down list. It opens a small window where one of the previously entered 10 SIP addresses can be automatically selected again. If the address already exists in the table, selecting Save will cause the error "Caller address already exists". Wildcard is allowed in this field.

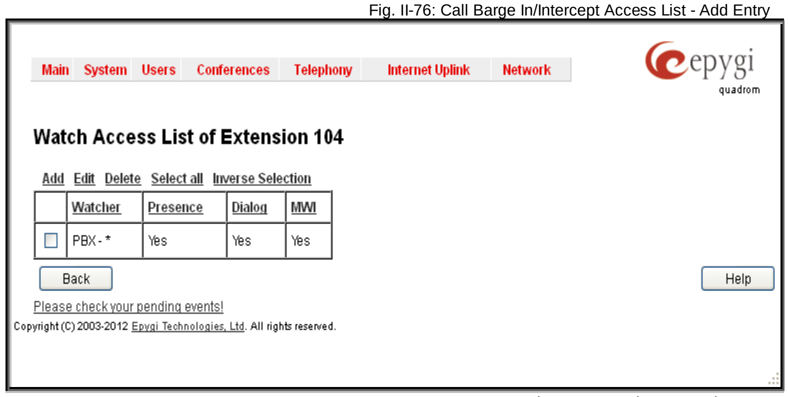


Fig. II-77: Watch Access List page

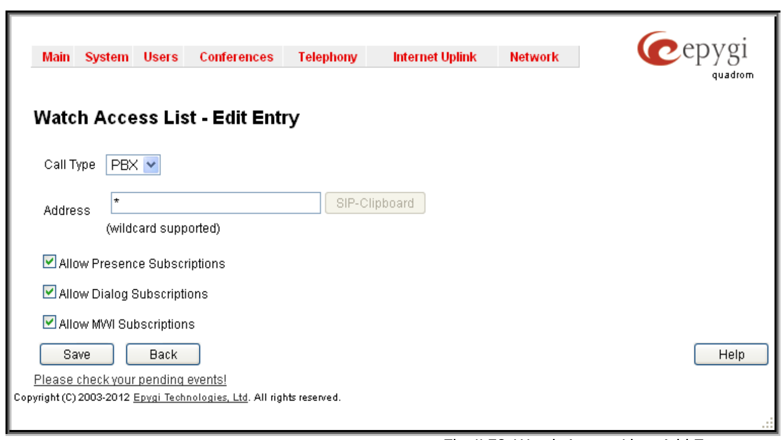


Fig. II-78: Watch Access List - Add Entry page

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

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

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

Delete removes the selected extensions from the list. If no records are selected an error message occurs.
Select all selects all existing records in the list.
Inverse selection inverses the current selection of records (if no records are selected, all records will be checked).

2. SIP Settings

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

User Name requires a user name for the extension registration on the SIP server. The registration user name needs to be unique on the SIP server and it is displayed on the called phone when performing an IP call. This field length is limited to 32 symbols.

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

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

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

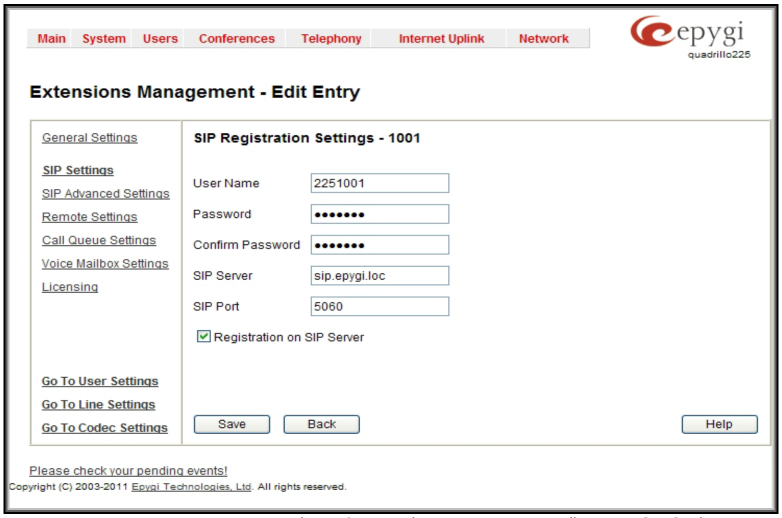


Fig. II-79: Extensions Management - Edit Entry – SIP Settings page

SIP Port indicates the host port number to connect to the SIP server. The SIP server port may only contain digit values, otherwise the error message "SIP Server Port is incorrect" will be displayed when applying the extension settings. If the SIP server port is not specified, QX1000 will access the SIP server through the default port 5060.

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

3. SIP Advanced Settings

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

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

The Secondary SIP Server acts as an alternative SIP registration server when the primary SIP Registration Server is inaccessible. If the connection with the primary SIP server fails, QX1000 will automatically start sending SIP messages to the Secondary SIP Server. It will switch back to the primary SIP server as soon as the connection is reestablished.

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

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

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

The **Do Not Use SIP Old Hold Method** checkbox enables the new recommended method of call hold in SIP, in which case the hold request is indicated with the "a=sendonly" media attribute, rather than with the IP address of 0.0.0.0 used before. The checkbox should be enabled if the remote party does not recognize hold requests initiated from the QX1000.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name) and the port numbers of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by QX1000 to reach the selected SIP servers.

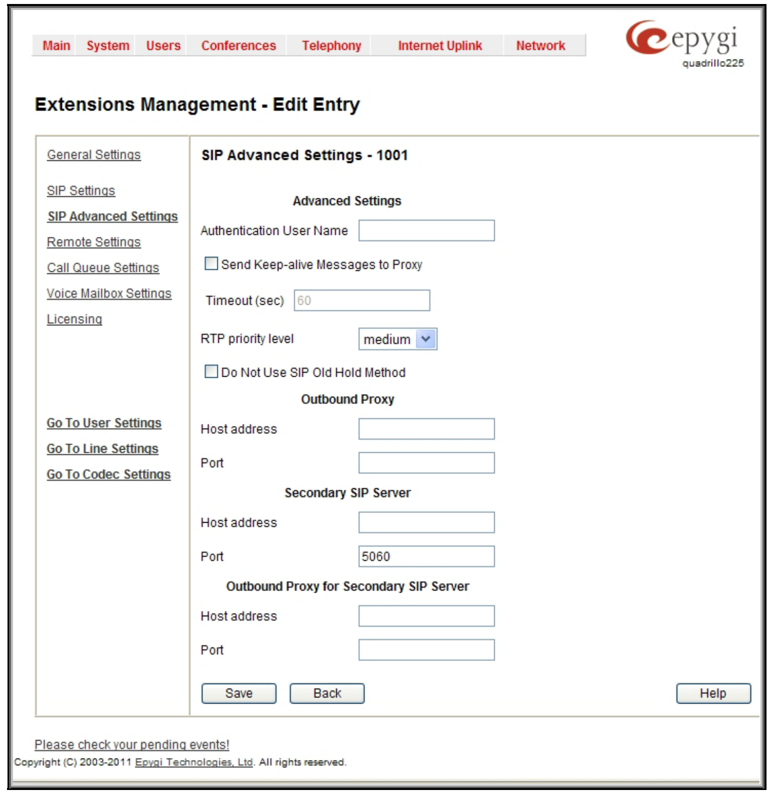


Fig. II-80: Extensions Management - Edit Entry – Advanced SIP Settings page

4. Remote Settings

This group is used to configure **SIP Remote Extension** functionality. This is an advanced telephony feature that allows QX1000 users to remotely operate QX1000. Users need to register a hardware or software SIP phone on the QX1000 by defining the QX1000's global IP address and an appropriate Username/Password. A registered SIP Remote phone can act fully as a phone connected locally to QX1000, i.e. it can use QX1000's PBX features, place and receive calls, access voice mails, etc.

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

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

Identification parameters used by the remote SIP device for registration on the QX1000 should be defined in the **Username** and **Password** text fields. They should match on both QX1000 and SIP phone for a successful connection. The Password field is checked against its strength and you may see how strong is your inserted password right below that field. To achieve the well protected strong password minimum 8 characters of letters in upper and lower case, symbols and numbers should be used. If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

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

When the **Enable RTP Proxy** checkbox is selected, incoming and outgoing RTP streams to and from the remote SIP phone will be routed through QX1000. When the checkbox is not selected, RTP packets will be moving directly between peers.

When the **Fallback To Local Extension When Not Registered** checkbox is selected, incoming calls towards the corresponding extension on the QX1000 will be forwarded to the remote SIP phone only if it is registered. Otherwise, when the remote SIP phone is unregistered, incoming calls will be routed to the line extension it is attached to. When this checkbox is not selected, all incoming calls will be routed to the remote SIP phone only if it is registered. Otherwise, if the remote SIP phone is unregistered, calls will be forwarded to the extension's voice mailbox.

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

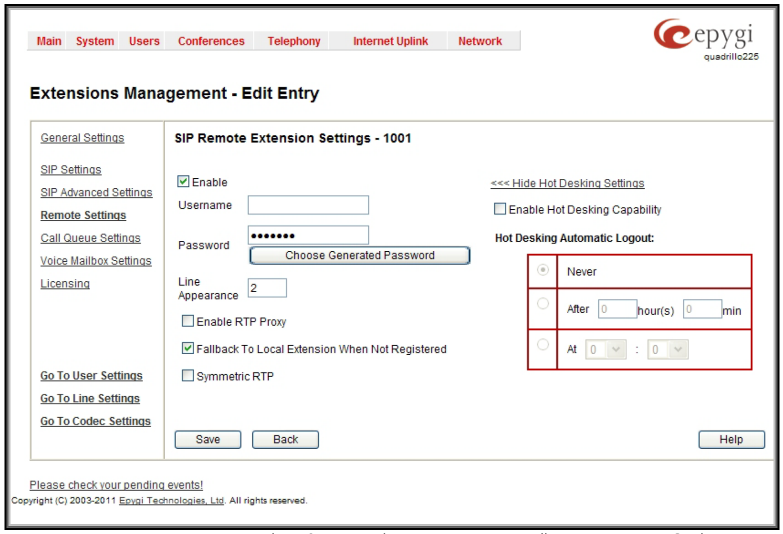


Fig. II-81: Extensions Management - Edit Entry – Remote Settings page

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

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

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

The following options are available:

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

5. Call Queue Settings

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

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

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

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

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

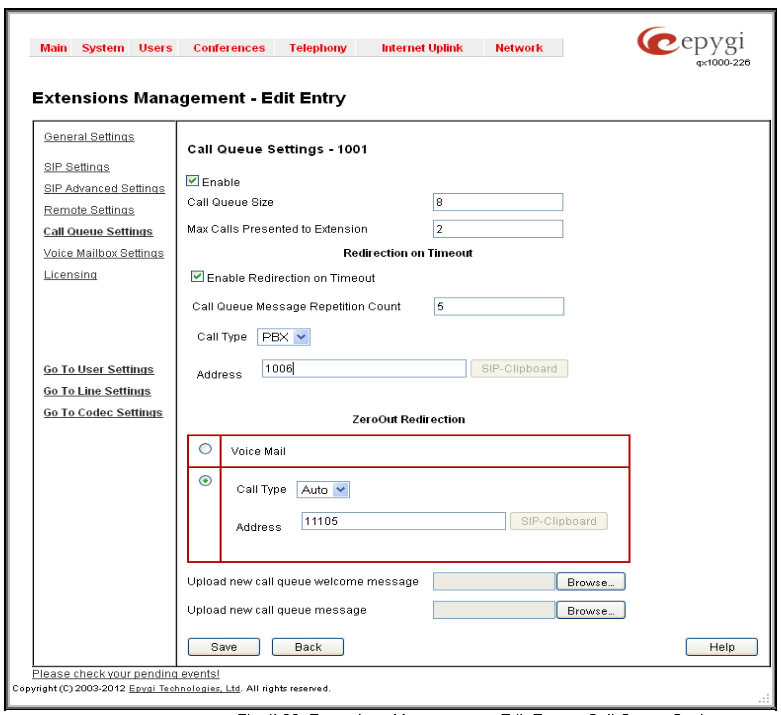


Fig. II-82: Extensions Management - Edit Entry – Call Queue Settings page

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

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

Call Type lists the available call types:

- **PBX** - local calls to QX1000's extensions
- **SIP** – calls through a SIP server
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, a SIP address or a PSTN number) will be reached through the Call Routing Table.

The **Address** text field is used to define the address where the call will be redirected. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX1000 extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **Auto** call type, a routing pattern needs to be defined.

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

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

Call Type lists the available call types:

  - **PBX** - local calls to QX1000's extensions.
  - **SIP** - calls through a SIP server.
  - **Auto** - used for undefined call types. The destination (independent on whether it is a PBX number or a SIP address) will be reached through the Call Routing Table.

The **Address** text field is used to define the address where the call will be redirected. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX1000 extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **Auto** call type, a routing pattern needs to be defined. The SIP-Clipboard button at the end of the line can be used only when **SIP** is selected in the **Call Type** drop down list. It opens a small window where one of the previously entered 10 SIP addresses can be automatically selected again. If the address already exists in the table, selecting **Save** will cause the error "Caller address already exists". Wildcard is allowed in this field.

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

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

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

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

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

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

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

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

6. Voice Mailbox Settings

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

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

- **Use Internal Voice Mail** – enables the Voice Mail service for the corresponding extension and defines the QX1000's internal storage as a location for the Voice Mails.

  This selection also allows you to manipulate with the **Voice Mail Configuration Wizard** used by the extension's user to setup personal settings (the password, the voice mail greeting message and the user's name for **Extensions Directory**) from the handset. By default, the **Voice Mail Configuration Wizard** is enabled when the QX1000's is in the factory reset state. It can be manually enabled from this page by pressing the **Activate** button. When the **Voice Mail Configuration Wizard** is activated, the extension's user is prompted to insert personal settings as he/she enters his/her Voice Mailbox for the first time. Unless the required information is not inserted, the button is changed to **Deactivate** and the **Configuration Wizard Status** becomes **Activated**. Use **Deactivate** button to stop **Voice Mail Configuration Wizard**. When the user inserted the required information, the **Configuration Wizard Status** on this page is changed to **Passed** and a **Reactivate** button appears. Using **Reactivate** button you might re-enable the **Voice Mail Configuration Wizard** so the user will be again prompted about his/her personal settings next time entering his/her Voice Mailbox.

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

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

- **Use External Voice Mail** – enables the Voice Mail service for the corresponding extension and is used to define a remote Voice Mail Server as a location for the Voice Mails. In this case recorded voice mails will be collected on the remote server. Radio button selection enables a sub-group of manipulation radio buttons:
  - If the remote Voice Mail Server is combined with the SIP Proxy server, it is recommended to select **Proxy Controlled Mailbox Type**. With this selection, SIP proxy will keep the recorded voice mail on itself. When extension accesses his mailbox by dialing *0, the call will be redirected to the voice mailbox on the proxy server.
  - If the remote Voice Mail Server acts as a standalone location of voice mails, it is recommended to select **Independent Mailbox Type**. With this selection, QX1000 redirects the recorded voice mails to the defined remote Voice Mail server. When extension accesses his mailbox by dialing *0, the call will be redirected to the remote voice mail server.

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

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

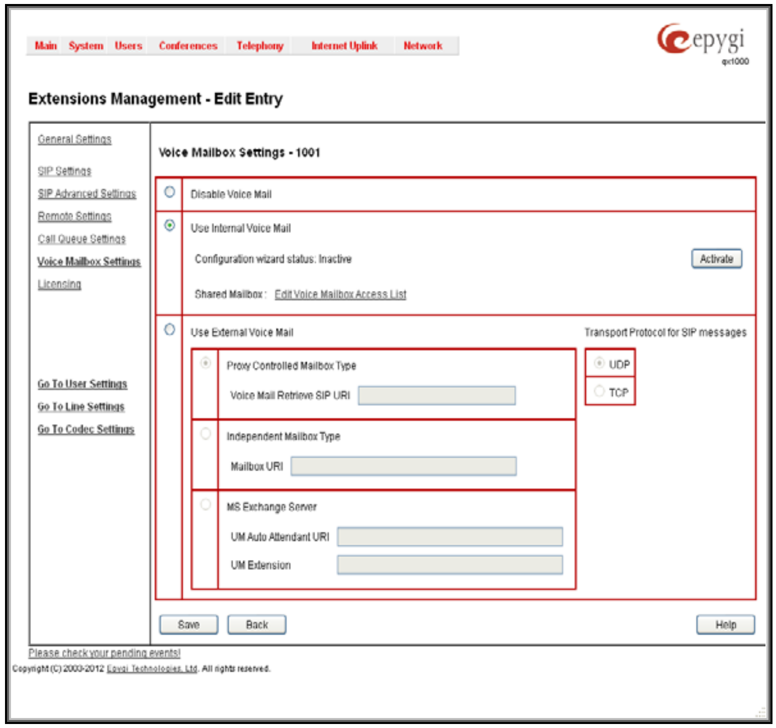


Fig. II-83: Extensions Management - Edit Entry – Voice Mailbox Settings page

- With **MS Exchange Server** you can keep recorded voice messages into one universal inbox.
  - **UM Auto Attendant URI** text field requires the SIP URI of the MS Exchange Server. When extension accesses his mailbox by dialing *0, the call will be redirected to the voice mailbox on the MS Exchange Server.
  - **UM Extension** text field requires an extension number that Unified Messaging will use when voice mail is submitted to the user's MS Exchange Server mailbox.

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

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

7. Licensing

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

This group allows you to configure the extension to be used by the Quadro Communication Manager (QCM) soft-phone application and the Pro/Basic level Desktop Communication Console.

The **Enable QCM (Quadro Communication Manager) license** checkbox allows you to set the corresponding extension to be used by the QCM application. When the checkbox is not selected on this page, the QCM will be functional with the extension only during trial period.

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

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

Please Note: These checkboxes can be simultaneously selected on as many extensions as QCM and/or DCC licenses are available on the QX1000.

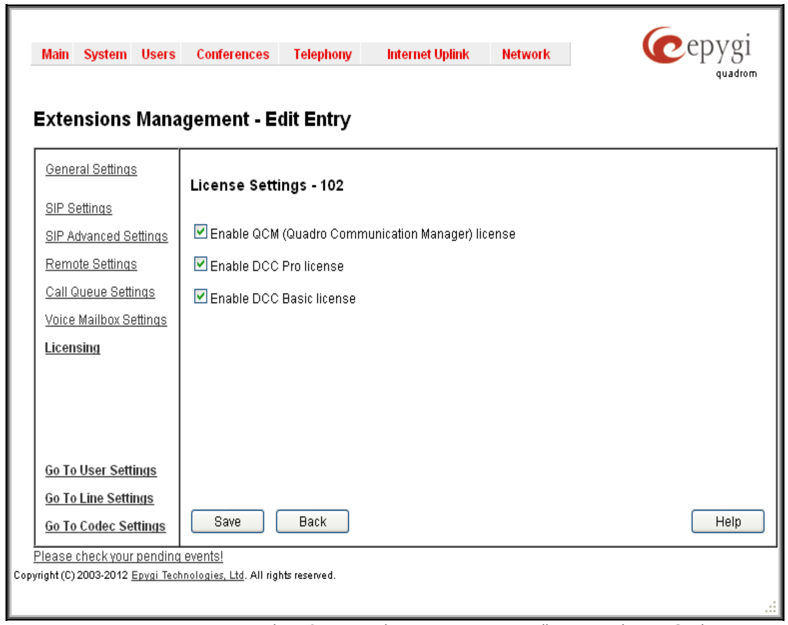


Fig. II-84: Extensions Management - Edit Entry – License Settings page

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

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

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

Pickup Group Extension Settings

Pickup Group & Access List

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

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

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

If a user dials the pickup extension when several extensions of the pickup group are ringing, the first (oldest in time) call will be picked up. When the user dials the pickup extension and no extensions of the pickup group are ringing, the "No call is available to pickup" message will be played to the user. When the user that is not listed in the **Access List** dials the pickup extension, password authorization (of the pickup extension) will be required to answer the call. When a denied user dials the pickup extension, the "Party does not accept your call" message will be played to the user.

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

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

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

Password requires a password for the new extension.

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

If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

The Password field is checked against its strength and you may see how strong is your inserted password right below that field.

Confirm Password requires a password confirmation. If the input is not corresponding to the one in the **Extension**

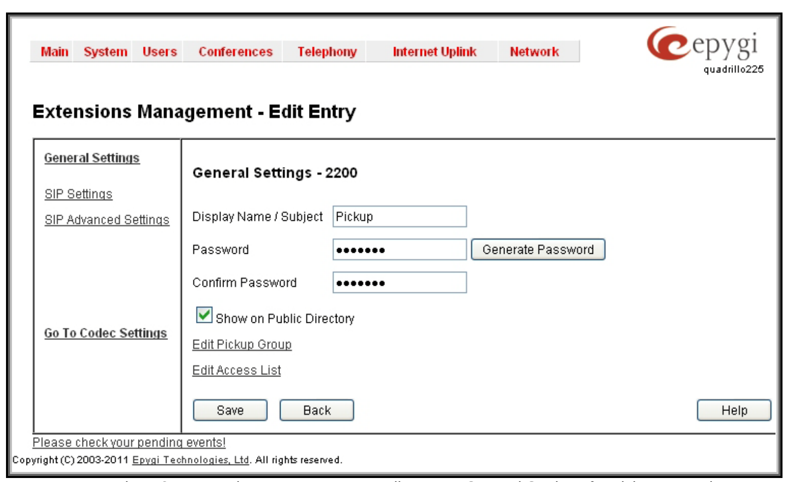


Fig. II-85: Extensions Management - Edit Entry – General Settings for pickup extension page

Password field, the “Incorrect Password confirm” error message will appear.

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

The **Pickup Group of Extension** page lists all available regular and virtual extensions on the QX1000 and allows you to manage the Pickup Group.

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

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

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

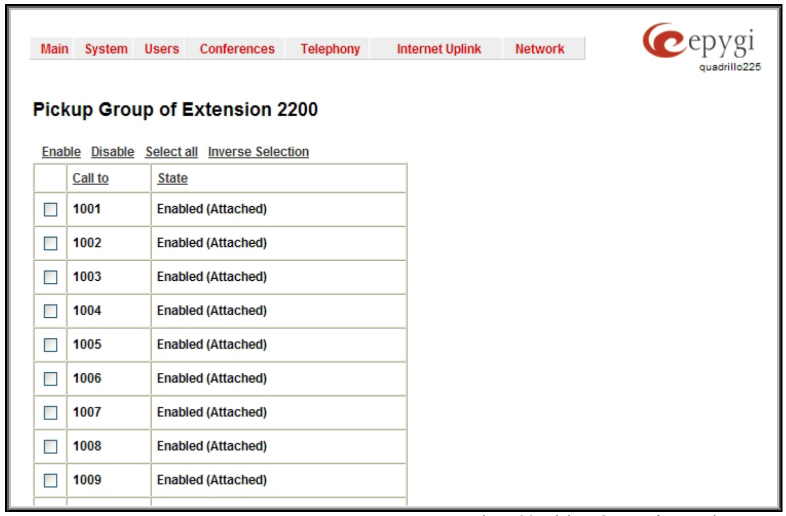


Fig. II-86: Pickup Group of Extension page

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

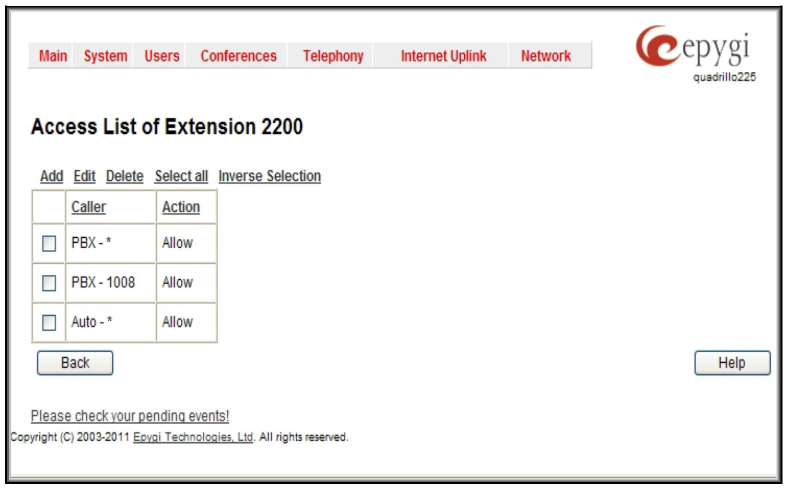


Fig. II-87: Access List of Extension page for Pickup Group

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

Call Type lists the available call types:

- **PBX** - local calls from QX1000’s extensions
- **SIP** – calls through a SIP server
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, SIP address or PSTN number) will be parsed through the Call Routing Table.

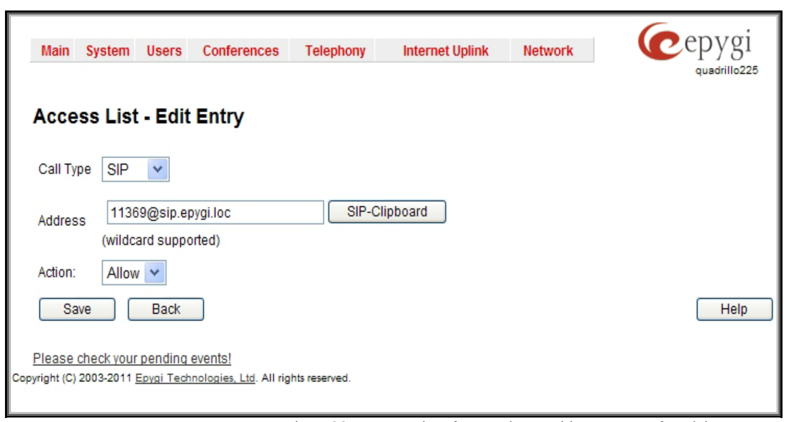


Fig. II-88: Access List of Extension –Add Entry page for Pickup group

The **Address** text field is used to define the address to be included in the Access List table. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the **PBX** call type is selected, the QX1000 extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **Auto** call type, a routing pattern needs to be defined.

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

Call Park Extension Settings

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

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

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

Password requires a password for the new extension.

The extension password may only contain digits. If non-numeric symbols are entered an "Incorrect Password: no symbol characters allowed" error will prevent making the extension. If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

The Password field is checked against its strength and you may see how strong is your inserted password right below that field.

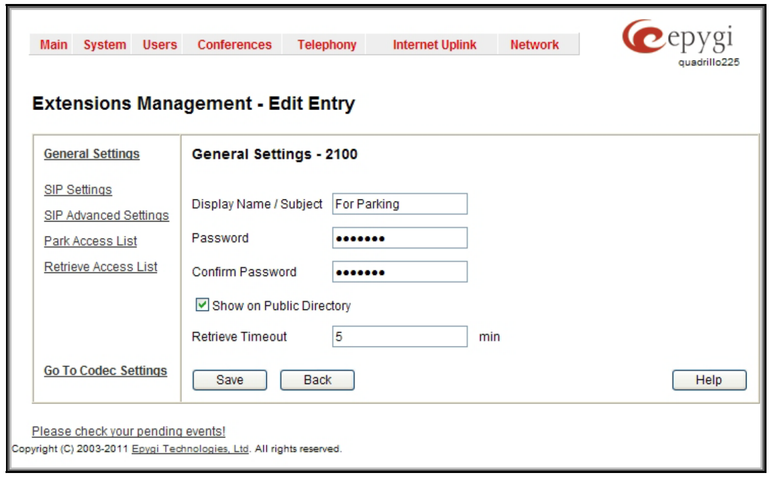


Fig. II-89: Extensions Management - Edit Entry – General Settings for call park extension

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

With the **Show on Public Directory** checkbox enabled, the details of the corresponding extension will be displayed in the User Settings table on the Main Page of the Extension's QX1000 Web Management (accessed by the extension's login, see Manual III – Extension User's Guide). Besides this, the details of the extension will be displayed in the Public Directories on the snom and Aastra SIP phones. Leave this checkbox unselected if the extension is reserved or not used, or when the extension serves as an intermediate unit for call forwarding, etc.

Retrieve Timeout text field requires a timeout (in minutes) during which the parked call will stay active, i.e. the parked user will remain on-hold. When the call park retrieve timeout expires, the hold music stops playing to the parked user and a new call is being placed towards the extension initiating the call park. If the extension initiating the call park does not answer the call, the caller which has been recently parked will reach the extension's Voice Mailbox, if enabled, otherwise will be disconnected.

2. Park Access List

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

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

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

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

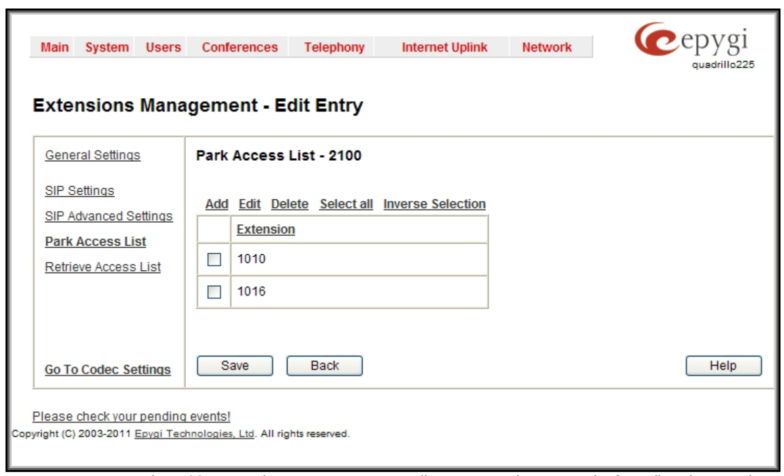


Fig. II-90: Extensions Management - Edit Entry – Park Access List for call park extension

3. Retrieve Access List

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

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

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

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

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

Call Type lists the available call types:

- **PBX** - local calls from QX1000's extensions
- **SIP** – calls through a SIP server
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, SIP address or PSTN number) will be parsed through Call Routing Table.

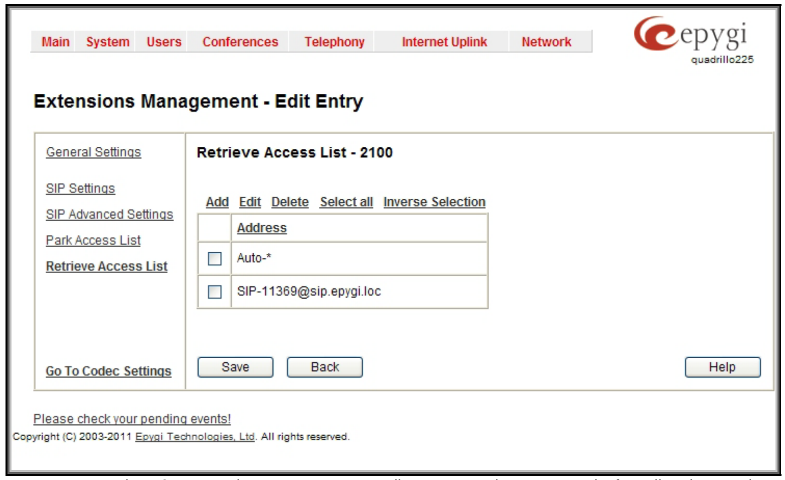


Fig. II-91: Extensions Management - Edit Entry – Retrieve Access List for call park extension

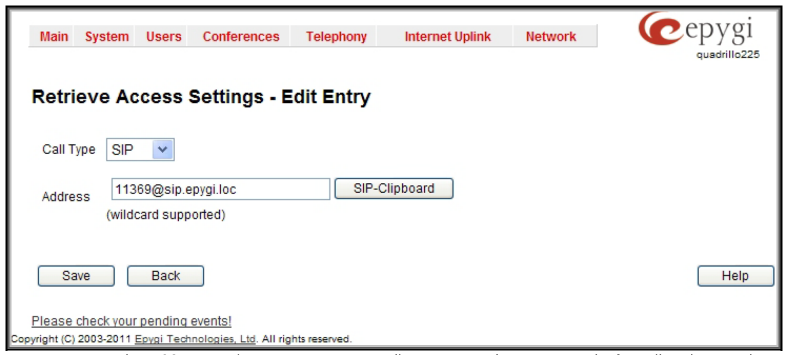


Fig. II-92: Extensions Management - Edit Entry – Retrieve Access List for call park extension

The **Address** text field is used to define the address to be included in the Retrieve Access List table. The value in this field is strictly dependent on the Call Type defined in the same named drop down list. If the **PBX** call type is selected, the QX1000 extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **Auto** call type, a routing pattern needs to be defined. The wildcard is supported in this field. Wildcard is available for this field.

Paging Group Extension Settings

Paging Group & Access List

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

Please Note: The **Paging Group** service requires called extensions to use one of the following SIP or analog phones which are able to automatically go off-hook:

- snom 300
- snom 320
- snom 360
- snom 370
- snom 710
- snom 720
- snom 760
- snom 820
- snom 821
- snom 870
- Aastra 480i
- Aastra 9133i
- Aastra 9112i
- Aastra 9143i
- Aastra 9480i (35i)
- Aastra 51i
- Grandstream BT200
- Grandstream GXP1400
- Grandstream GXP1405
- Grandstream GXP1450
- Grandstream GXP2000
- Grandstream GXP2100
- Grandstream GXP2110
- Grandstream GXP2120
- Grandstream GXP2124
- Grandstream GXV3140
- Grandstream GXV3175
- Fanvil C62
- Polycom SoundPoint IP 300SIP
- Polycom SoundPoint IP 330SIP
- Polycom SoundPoint IP 331SIP
- Polycom SoundPoint IP 501SIP
- Thomson ST2030S
- Yealink SIP-T22P
- Yealink SIP-T26P
- Yealink SIP-T28P
- Yealink SIP-T32G
- Yealink SIP-T38G
- Yealink VP-530
- Linksys SPA942
- Linksys SPA941
- Linksys SPA922
- Linksys SPA921
- Linksys SPA2002
- Linksys SPAPAP2T
- AudioCodes 310HD
- AudioCodes 320HD
- Panasonic KX-UT136-B

- Aastra 53i
- Aastra 55i
- Aastra 57i
- Aastra 6730i
- Aastra 6731i
- Aastra 6739i
- Aastra 480e (analog phone)
- Polycom SoundPoint IP 550SIP
- Polycom SoundPoint IP 601SIP
- Polycom SoundPoint IP 650SIP
- Polycom SoundStation IP 6000
- Polycom VVX 300/310
- Polycom VVX 400/410
- Yealink SIP-T20P
- Panasonic KX-UT123-B
- Panasonic KX-UT123NE-B
- Panasonic KX-TGP550T04
- Alcatel Temporis IP200
- Alcatel Temporis IP600
- Alcatel Temporis IP800

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

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

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

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

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

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

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

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

Password requires a password for the new extension.

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

If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

The Password field is checked against its strength and you may see how strong is your inserted password right below that field.

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

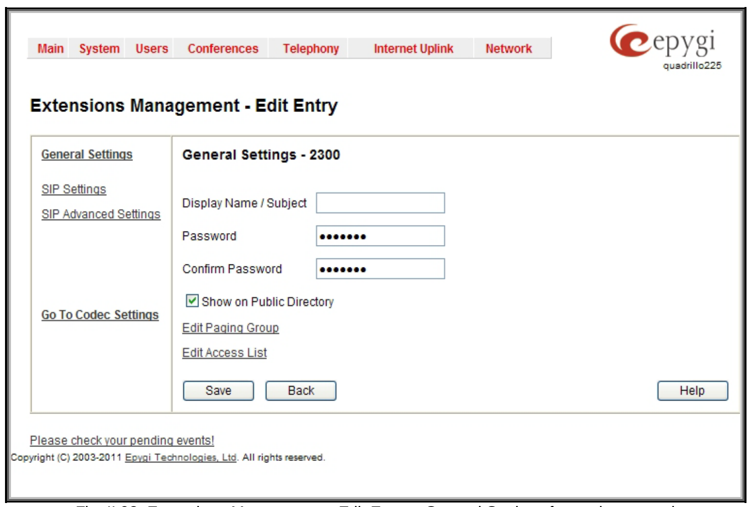


Fig. II-93: Extensions Management - Edit Entry – General Settings for paging extension page

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

The **Paging Group of Extension** page lists all available regular and virtual extensions on the QX1000 and allows you to manage the Paging Group.

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

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

Fig. II-94: Paging Group of Extension page

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

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

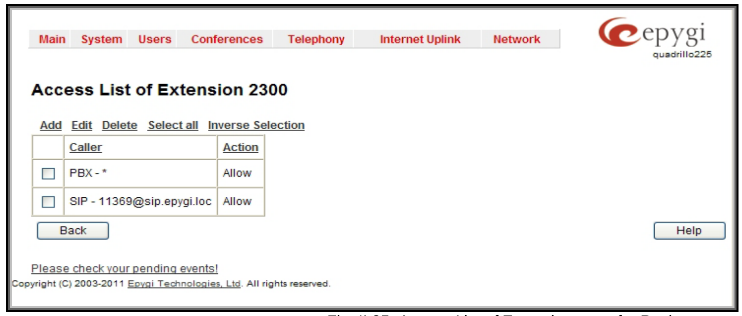


Fig. II-95: Access List of Extension page for Paging group

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

Call Type lists the available call types:

- **PBX** - local calls from QX1000's extensions
- **SIP** – calls through a SIP server
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, SIP address or PSTN number) will be parsed through Call Routing Table.

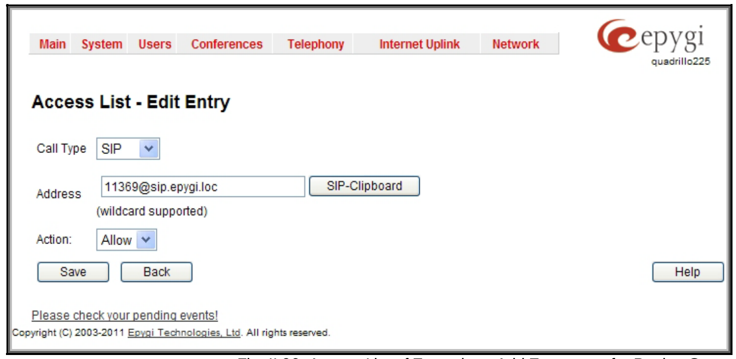


Fig. II-96: Access List of Extension –Add Entry page for Paging Group

The **Address** text field is used to define the address to be included in the Access List table. The value in this field is strictly dependent on the Call Type defined in the same named drop down list.

If the **PBX** call type is selected, the QX1000 extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **Auto** call type, a routing pattern needs to be defined.

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

ACD Group Extension Settings

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

1. General Settings (for ACD Group extension)

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

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

Password requires a password for the ACD Group extension.

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

If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

The Password field is checked against its strength and you may see how strong is your inserted password right below that field.

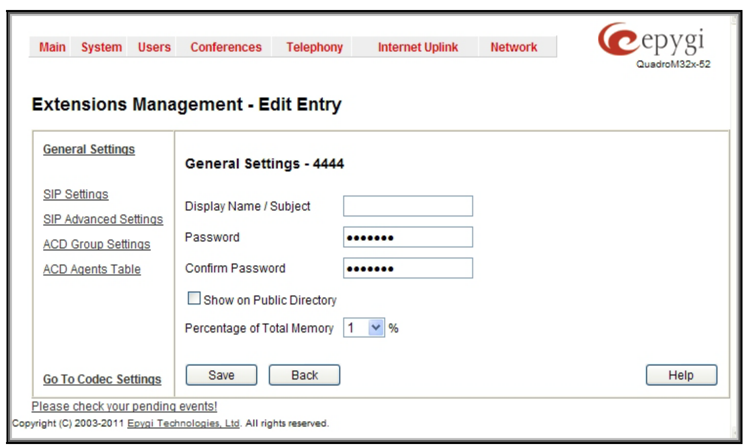


Fig. II-97: Extensions Management - Edit Entry – General Settings page (for ACD Group extension)

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

With the **Show on Public Directory** checkbox enabled, the details of the corresponding extension will be displayed in the User Settings table on the Main Page of the Extension's QX1000 Web Management (accessed by the extension's login, see Manual III – Extension User's Guide). Besides this, the details of the extension will be displayed in the Public Directories on the snom and Aastra SIP phones. Leave this checkbox unselected if the extension is reserved or not used, or when the extension serves as an intermediate unit for call forwarding, etc.

The **Percentage of Total Memory** drop down list allows you to select the space for the uploaded custom messages. The maximum value in the drop down list is equal to the maximum available space for voice messages on QX1000.

2. ACD Group Settings

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

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

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

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

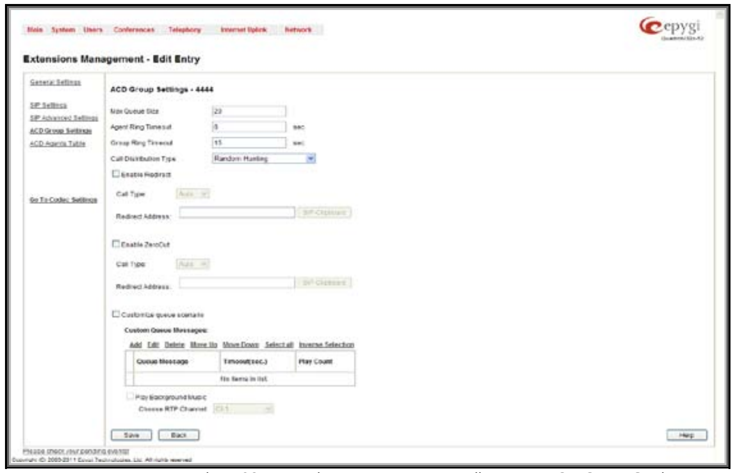


Fig. II-98: Extensions Management - Edit Entry – ACD Group Settings page

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

- **All Agents Ringing** – the system tries to reach all available agents in the group ringing their phones. As soon as the first answers, it cancels the calls to other agents (similar to Many Extension Ringing on the QX1000, see Manual III – Extension User's Guide). If no one answers within **Common Timeout**, the system either disconnects or redirects the call.
- **Round Robin** – the system calls to the first available agent in the list of agents configured with AG. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach the next agent in the list, etc. Reaching the end of the list it starts from the beginning again. If the call is not answered and the **Common Timeout** has expired, the system either disconnects or redirects the call.
- **Longest Idle** – the system calls to the first available agent who was longest idle after the last call. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach another agent who was longest idle, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.
- **Less Busy During Last Hour** - the system calls to the first available agent who was least busy during the last hour (in average). If the agent doesn't answer within **Ringing Timeout**, the system tries to reach the next least busy agent, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.
- **Random Hunting** – the system calls to the first available agent selected randomly from the list of agents configured with Agents Group. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach another agent selected randomly from the list, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.
- **Skills** - the system calls to the first available agent with the highest composite skill's grade in the group. If the agent doesn't answer within **Ringing Timeout**, the system tries to reach the next agent with the highest composite skill, etc. If the call is not answered within **Common Timeout**, the system either disconnects or redirects the call.

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

Call Type lists the available call types:

- **PBX** - local calls to QX1000's extensions
- **SIP** – calls through a SIP server
- **Auto** – used for undefined call types. The destination (independent on whether it is a PBX number, a SIP address or a PSTN number) will be reached through the Call Routing Table.

The Redirect **Address** text field is used to define the address where the call will be redirected. It might be within the scope of ACD, like the address of another ACD agent, or out of scope, like the address of some voice mailbox. The value in this field is strictly dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX1000 extension number should be defined in this field. For the **SIP** call type, the SIP address (see chapter Entering SIP Addresses Correctly) should be defined, for the **Auto** call type, a routing pattern needs to be defined.

Enable ZeroOut checkbox enables the ZeroOut feature. When this feature is enabled, callers that have reached the ACD Group extension may accelerate the automatic redirection instead of holding in the extension's queue. To activate this feature, caller should dial 0 digit (see Feature Codes) while in the queue of ACD Group extension. The caller will then be automatically transferred to the destination specified in this page. This selection activates the following fields to be inserted:

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

- **PBX** - local calls between QX1000 extensions and the Auto Attendant
- **SIP** – calls through a SIP server
- **Auto** – used for undefined call types. Destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

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

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

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

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

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

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

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

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

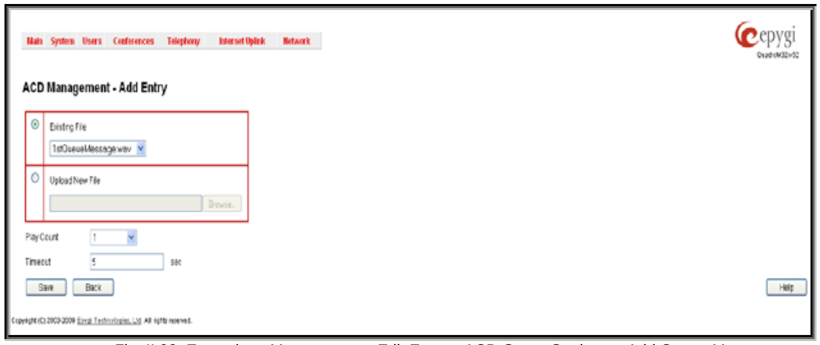


Fig. II-99: Extensions Management - Edit Entry – ACD Group Settings – Add Queue Message page

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

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

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

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

3. ACD Agents Table Settings

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

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

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

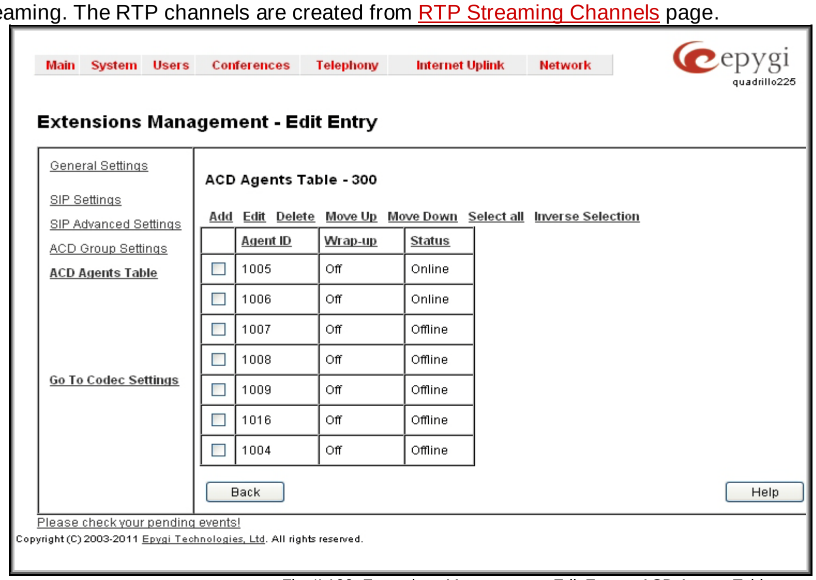


Fig. II-100: Extensions Management - Edit Entry – ACD Agents Table page

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

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

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

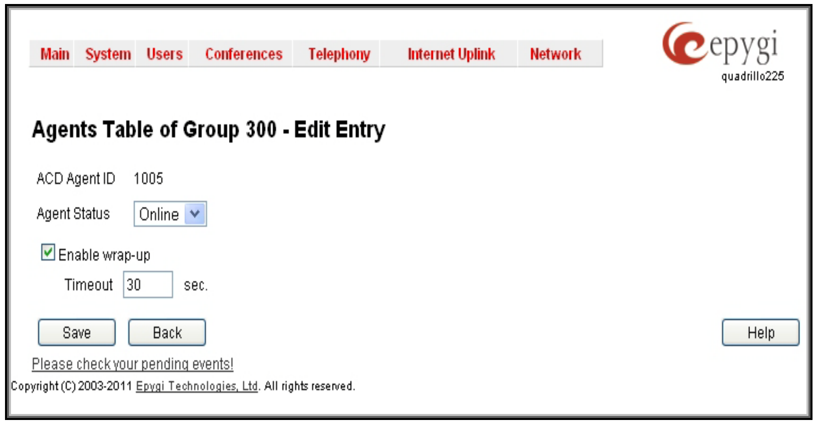


Fig. II-101: Agents Table of Group – Add Entry page

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

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

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

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

Recording Box Extension Settings

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

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

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

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

Password requires a password for the Recording Box extension.

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

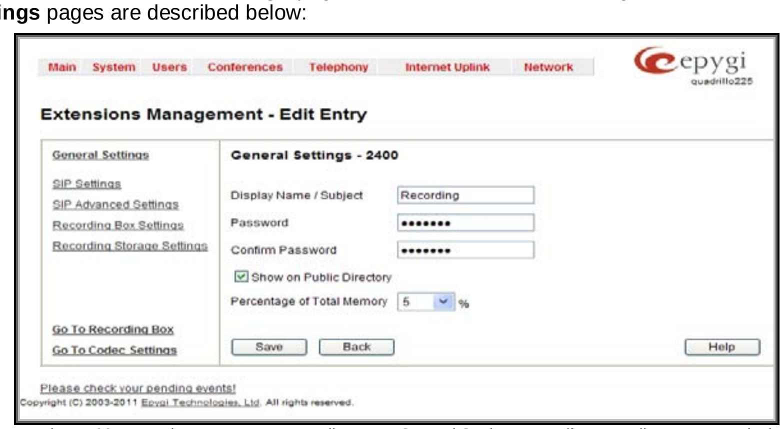


Fig. II-102: Extensions Management - Edit Entry – General Settings page (for Recording Box extension)

If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords.

The Password field is checked against its strength and you may see how strong is your inserted password right below that field.

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

With the **Show on Public Directory** checkbox enabled, the details of the corresponding extension will be displayed in the User Settings table on the Main Page of the Extension's QX1000 Web Management (accessed by the extension's login, see Manual III – Extension User's Guide). Besides this, the details of the extension will be displayed in the Public Directories on the snom and Aastra SIP phones. Leave this checkbox unselected if the extension is reserved or not used, or when the extension serves as an intermediate unit for call forwarding, etc.

The **Percentage of Total Memory** drop down list allows you to select the space for call recordings and the uploaded custom messages of Recording Box extension. The maximum value in the drop down list is equal to the maximum available space for voice messages on QX1000.

2. Recording Box Settings

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

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

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

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

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

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

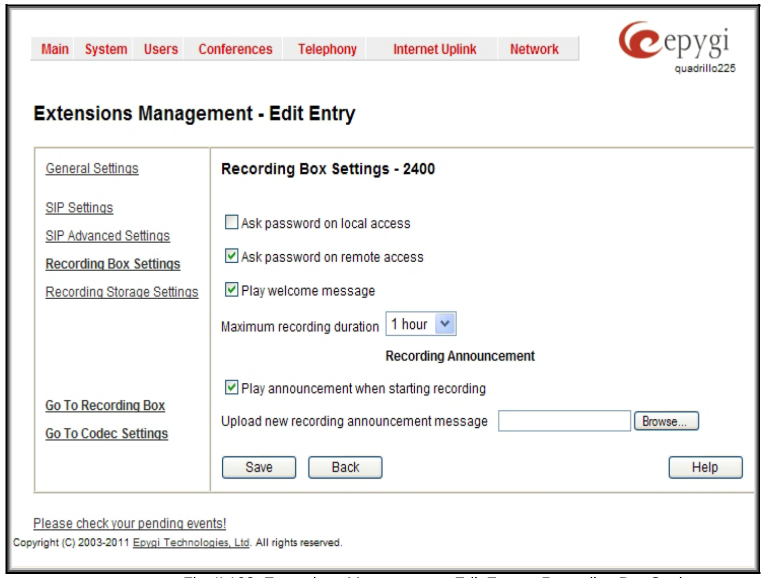


Fig. II-103: Extensions Management - Edit Entry – Recording Box Settings page

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

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

Upload new recording announcement message indicates the file name used to upload a new recording announcement message. The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading it and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension and the "You do not have enough space" warning message will appear.

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

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

3. Recording Storage Settings

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

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

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

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

Server Name text field requires the FTP server name.

Server Port text field requires the FTP server port number.

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

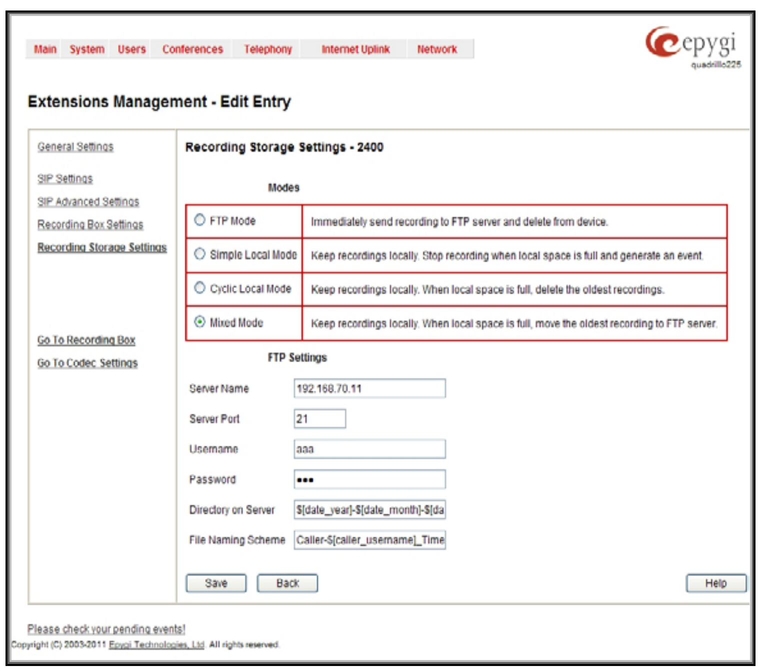


Fig. II-104: Extensions Management - Edit Entry – Recording Box Storage Settings

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

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

- caller_dispname – caller's display name
- caller_username – caller's username
- caller_fullname – caller's full name in the username@host[:port] format
- callee_dispname – called user's display name
- callee_username – called user's username
- callee_fullname – called user's full name in the username@host[:port] format
- duration – duration of the call
- time_hour – hour when the call recording started
- time_min – minute when the call recording started
- time_sec – second when the call recording started
- date_year – year when the call recording started
- date_month – month when the call recording started
- date_day – day when the call recording started
- extension – recording box extension
- hostname – QX1000's hostname

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

Example: MyQX1000-$[caller_dispname]-$[duration]-$[time_hour]-$[time_min]_business

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

MyQX1000-Andrew-15 sec-14-10-business.wav

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

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

Retry Timeout text field timeout between retries to access the server.

The **Go to Recording Box** link moves to the recording box of the corresponding extension's Recording Box where all recorded calls are locally stored. The Recording Box is also accessible from Extensions Management table, by clicking on the corresponding Recording Box extension.

Attendant Extension Settings

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

1. General Settings (for attendant extension)

This group requires AA extension information and has the following components:

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

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

The **Extension to forward** drop down list is used to choose the extension where the incoming FAX addressed to the QX1000's Auto Attendant will be forwarded. The list contains only those extensions that have FAX support enabled. FAX support can be enabled from the Extension Codecs page.

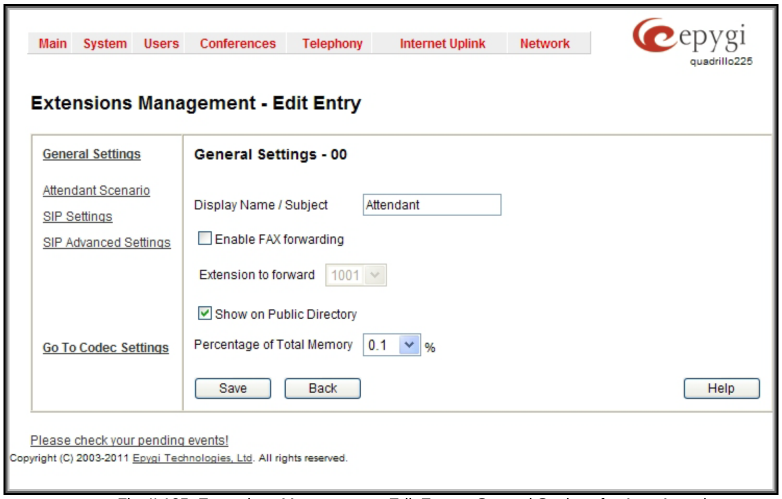


Fig. II-105: Extensions Management - Edit Entry – General Settings for Auto Attendant page

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

With the **Show on Public Directory** checkbox enabled, the details of the corresponding auto attendant extension will be displayed in the User Settings table on the Main Page of the Extension's QX1000 Web Management (accessed by the extension's login, see Manual III – Extension User's

Guide). Besides this, the details of the extension will be displayed in the Public Directories on the snom and Aastra SIP phones. Leave this checkbox unselected if this auto attendant extension is reserved or not used.

The **Percentage of System Memory** drop down list is used to define the space for the Auto Attendant’s system messages. The maximum value in the drop down list is equal to the maximum available space for voice messages on QX1000.

2. Attendant Scenario

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

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

- The **Send AA Digits to Routing Table** checkbox selection switches the Auto Attendant to the routing mode. Any inserted digits on the Auto Attendant prompt will be parsed through the Routing Table on the QX1000.

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

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

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

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

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

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

  Enable ZeroOut checkbox selection enables the ZeroOut feature and activates the following fields to be inserted:

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

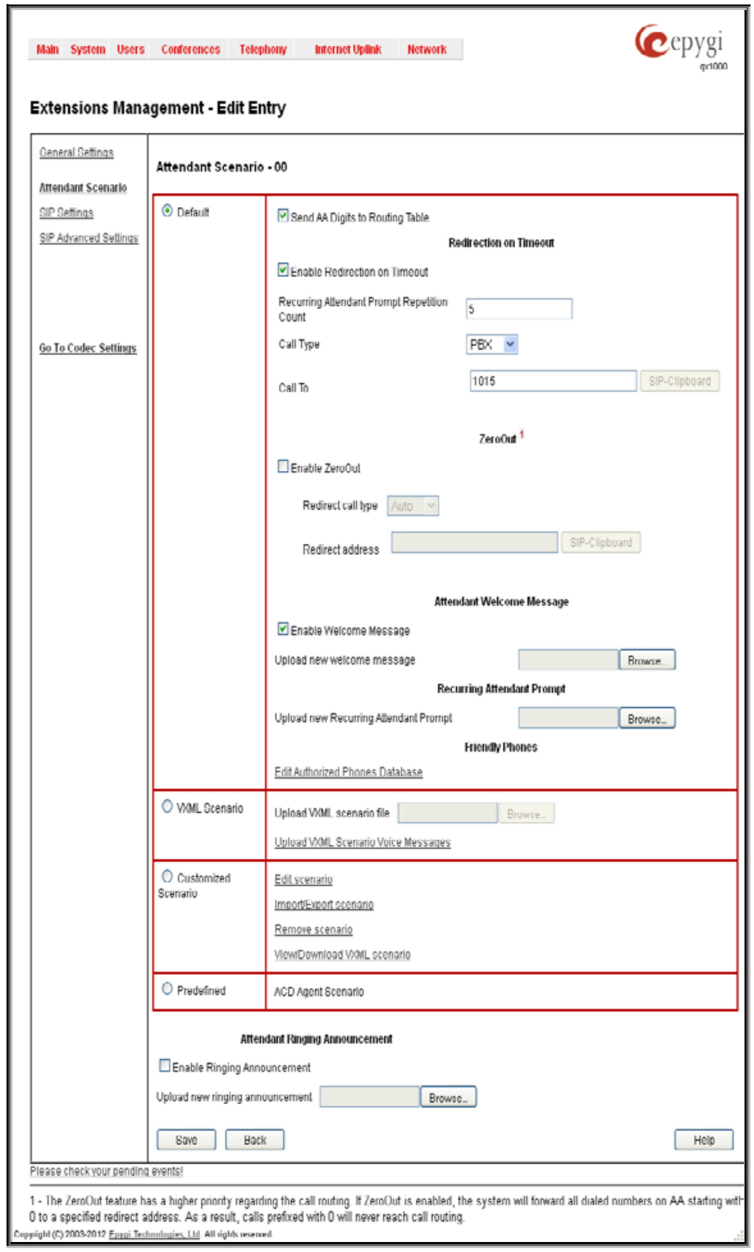


Fig. II-106: Extensions Management - Edit Entry – Attendant Scenario page

  - PBX - local calls between QX1000 extensions and the Auto Attendant
  - SIP – calls through a SIP server
  - Auto – used for undefined call types. Destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

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

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

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

  Enable Welcome Message checkbox is used to enable/disable the Auto Attendant welcome message (the default one or the custom one uploaded from this page or recorded from the handset (see Feature Codes) being played when callers enter QX1000's Auto Attendant.

  Upload new welcome message indicates the file name used to upload a new welcome message. The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading it and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension and the "You do not have enough space" warning message will appear.

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

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

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

  Upload new Recurring Attendant Prompt indicates the file name used to upload a new recurring auto attendant prompt. The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension. This will cause the "You do not have enough space" warning message to appear.

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

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

- **Friendly Phones -** the **Edit Authorized Phones Database** link refers to the Authorized Phones Database page where a list of trusted external phones can be created. If external SIP or PSTN users are added to the QX1000 Authorized Phones database, they are free to access the Auto Attendant Services without passing the authentication or to use the Call Back services.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Browse opens the file chooser window to browse for a new custom welcome or recurring message file.
Press the **Save** button to submit the changes or use **Back** to keep the initial data.

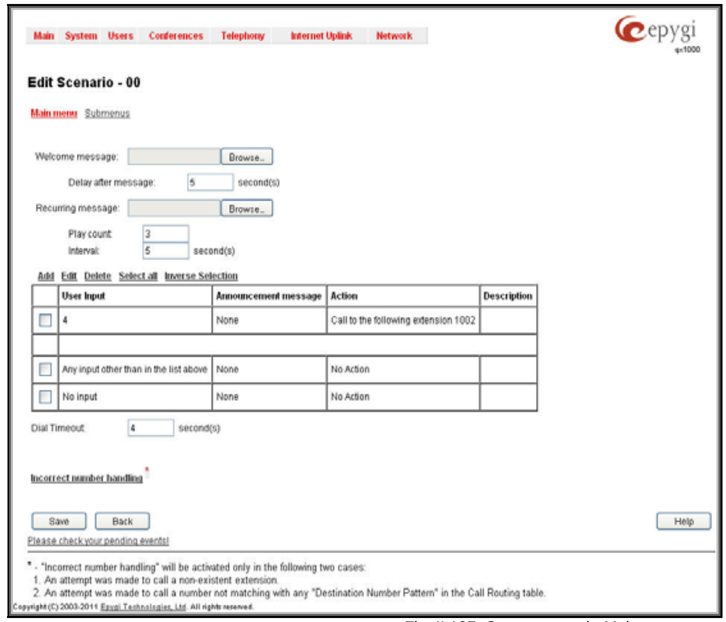


Fig. II-107: Create scenario-Main menu page

Attention: The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading it and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension and the "You do not have enough space" warning message will appear.

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

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

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

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

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

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

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

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

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

Description – text field for an optional description of the option.
Option is used for choosing the user input for which some announcement and/or action should be configured. The following input options are available in the list to configure the **Customized Scenario**:

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

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

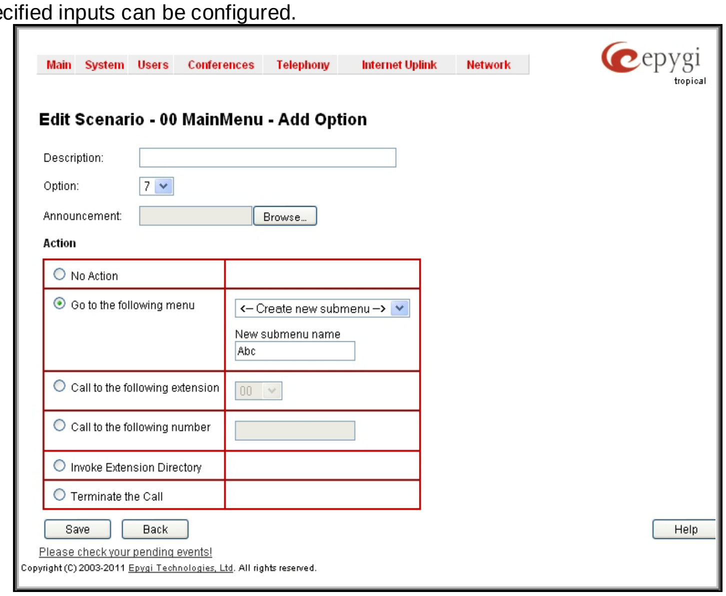


Fig. II-108: Upload Custom Voice Messages page

Attention: The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading it and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension and the "You do not have enough space" warning message will appear.
The **Download** and **Remove** links appear only if a file has been uploaded previously. The **Download** link is used to download the message file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove** link is used to restore the default welcome message.

Action is used to configure the action based on the caller's selection.
The **Action** radio buttons allows you to configure the action type after playing the **Announcement** message (if configured):

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

The following options can be configured too:

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

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

Delete removes the selected option(s) from the list of configured options.
Select all selects all existing options.
Inverse Selection inverses the current selection (if no record is selected, clicking on inverse selection will check all records).

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

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

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

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

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

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

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

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

Delete removes the selected submenu(s).

Select all selects all entries of the table.

Inverse Selection inverses the current selection (if no record is selected, clicking on inverse selection will check all records).

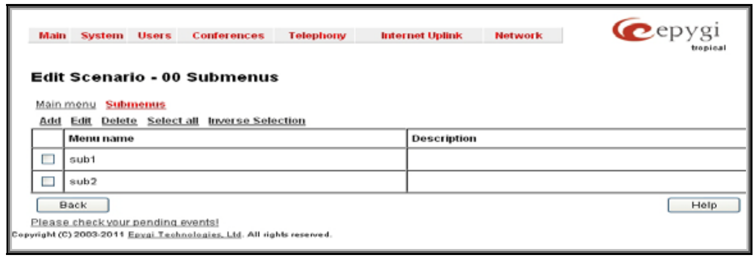


Fig. II-109: Upload Custom Voice Messages page

Fig. II-110: Upload Custom Voice Messages page

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

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

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

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

Fig. II-111: Upload Custom Voice Messages page

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

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

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

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

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

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

Fig. II-112: Upload Custom Voice Messages page

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

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

The group offers the following components:

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

Upload new Attendant Ringing Announcement indicates the file name used to upload an announcement. The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading and the "Invalid audio file, or format is not supported" warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding extension. This will cause the "You do not have enough space" warning message to appear.

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

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

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

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

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

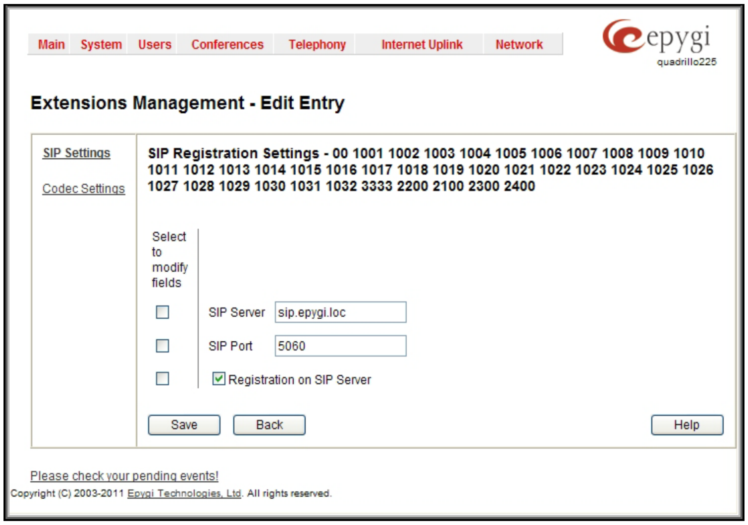


Fig. II-113: Extensions Management - Edit Entry page for multiple edit operation

Add Multiple Extensions

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

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

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

Start from the Extension text field requires the number of the first new extension to be created. Depending on the value in the **Quantity** text field, the next extensions to be created will have subsequent numbers. For example, if you have inserted 41 in this text field and the **Quantity** text field contains the value "5", then extensions 41, 42, 43, 44 and 45 will be added to the Extensions Management table. If non-digit symbols have been entered, the error "Incorrect Extension: no symbol characters allowed" will appear. If an extension with the given numbers already exists in the Extensions Management table, a next subsequent not used extension number will be used instead.
Please Note: Extension cannot start with the digit 0. You can add extensions of up to 20 digits long. However, the Call Routing won't be adjusted automatically; you may need to manually adjust the routing rules for extensions in custom length.

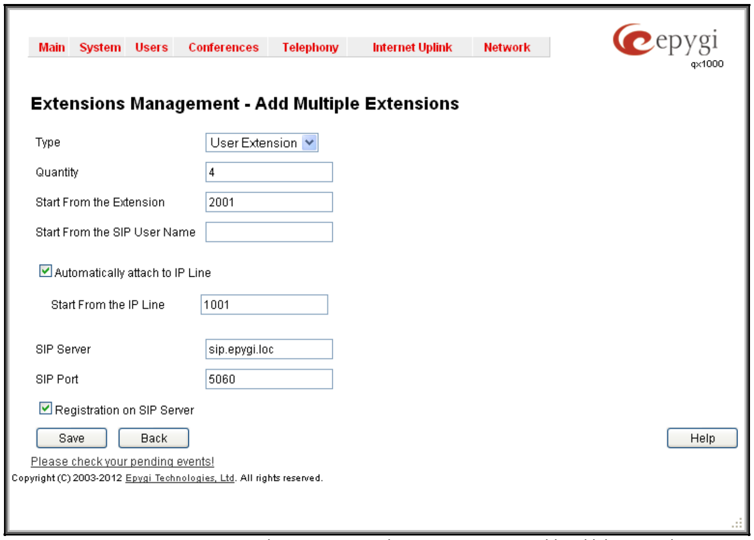


Fig. II-114: Extensions Management - Add Multiple Extensions page

Start from the SIP User Name text field requires the SIP server registration user name for the first extension to be created. Depending on the value in the **Quantity** text field, the next extensions to be created will have subsequent SIP user names. For example, if you have inserted 30201 in this text field and the **Quantity** text field contains the value "5", then the 5 newly created extensions will correspondingly have the following registration

SIP user names: 30201, 30202, 30203, 30204 and 30205. This user name is used for the registration on the SIP Server and should be unique on the SIP server. This field length is limited by 20 symbols and is not limited regarding the use of symbols. If an extension with the given SIP user name already exists in the Extensions Management table, a next subsequent not used SIP user name will be used instead.

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

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

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

SIP Port text field requires the port number to connect to the SIP server. The SIP Port may only contain digit values, otherwise an error message "SIP Port is incorrect" will appear. If the SIP server port is not specified, QX1000 will access the SIP server via the default 5060 port.

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

Extension Codecs

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

The **Codecs** table lists the voice and video codecs supported by the QX1000. Each table entry is assigned a checkbox that is used to manipulate the entry, for example to disable, to move it up or down, etc.
The table entries in bold type indicate codecs enabled for the selected extension/attendant/conference. The enabled codecs participate in codec negotiation at the call setup. The order of the enabled codecs is very important. Each codec in the table has a higher priority than the codecs below it, and a lower priority than the codecs above it. A codec placed at the top of the table is used as the preferred codec. When establishing a call, the system will try this codec first. If the remote party does not support the preferred codec, the following codecs will be tried out strictly in the order given in the **Codecs** table.

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

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

Select all selects all entries in the table.

Inverse Selection performs an inverse selection of the selected entries. Clicking this button when no entry is selected will select all entries.

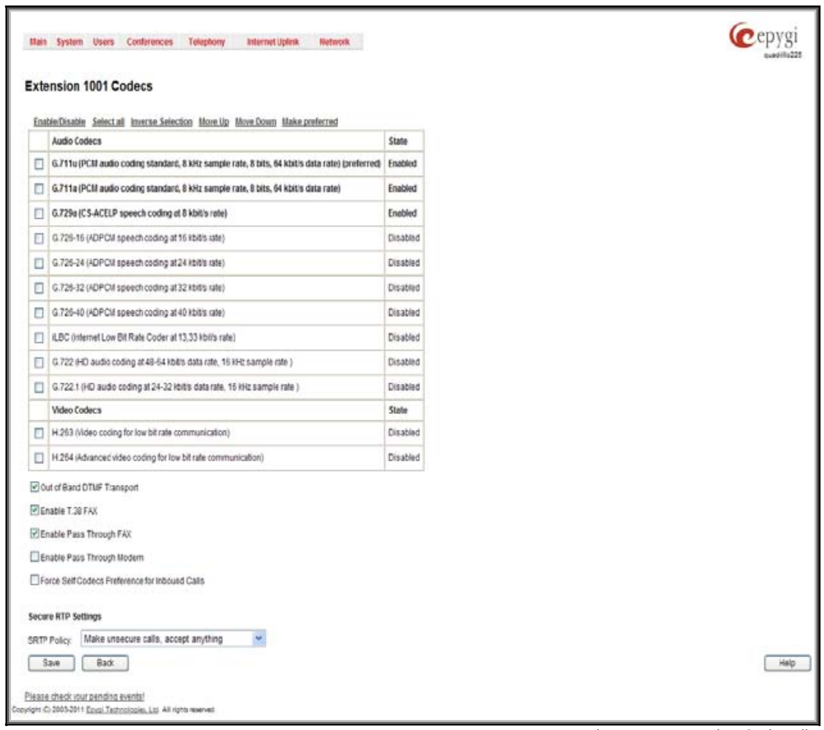


Fig. II-115: Extension Codecs list

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

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

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

Please Note: The **Call Recording** service is not available, if the call is established with TDVC or G722 codecs.

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

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

Enable T.38 FAX enables the FAX tone detection and the T.38 codec support for the FAX transmission from/to the FAX machine/modem attached to the line. It also enables the T.38 codec support for incoming unified FAX messages (fax to mailbox).

Enable Pass Through FAX enables the FAX tone detection and the G.711 codec support for the FAX transmission from/to the FAX machine/modem attached to the line. It also enables the G.711 codec support for incoming unified FAX messages (fax to mailbox).

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. If the extension is attached to the line that has no FAX machine/modem connected (the extension is virtual or is attached to an IP line), the incoming FAX can only be stored in the extension's voice mailbox. To allow FAX to be stored in the voice mailbox, the extension's user should not answer the incoming calls, so that they are forwarded to the voice mailbox.

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

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

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

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

Secure RTP Settings are used to configure secure voice over IP communication on the QX1000. The **SRTP Policy** drop down list is used to select the secure IP connection policy. For IP phones, the following options are available:

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

For Auto Attendant, the following options are available:

- **Accept only secure calls** - only the secure calls will be accepted.
- **Accept only unsecure calls** - only the unsecure calls will accepted.
- **Accept anything** - both secure and unsecure incoming calls will be accepted.

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

Call Park and Directed Call Park Services

The **Call Park** and **Directed Call Park** services are used to store a call on a specific number so that any other user on the system can retrieve it. For example, a user receives a call but wants to take it in a conference room where it is possible to speak privately. Transferring the call to the conference room is not an option because the conference room it is transferred to might be in use, or the user is unable to walk to the conference room in time to answer the call. The user can use **Call Park** and **Directed Call Park** to place the call at a specific number and then retrieve when they reach the conference room.
To use the **Call Park** or the **Directed Call Park** features, at least one Call Park extension should be created in the Extensions Management table. Additionally, two lists should be defined for the call park extension: **Park Access List** for users that might park a call to the corresponding Call Park extension and **Retrieve Access List** for the users that can pick up calls parked to that extension. By default, both of these lists have entries so any PBX extension on the QX1000 can park the call, and any destination can retrieve the parked call. Any limitations to these settings should be done individually for each call park extension.

To make a Call Park

To make a Call Park, the QX1000 user which has been previously added to the **Park Access List** for at least one of the available Call Park extension on the QX1000 should dial the appropriate digit combination (see Feature Codes in Manual III - Extension User's Guide) during the call. The active call will go on hold, while the PBX number and the SIP username (if it is registered on the SIP server) of the first available call park extension where the user is added will be played to him/her.

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

For example, the Call Park extension 77 is created which has been registered on the SIP Server under the 892220 registration username. The QX1000 user is added to the Park Access List, while the phone at the remote location is added to the Park Access List of that call park extension.
While being on a call with user A, the QX1000 user dials the appropriate calling code. As a reply, QX1000 will play the extension 77 and SIP username 892220 to the QX1000 user. The user A goes on hold. The QX1000 user moves to a remote location and makes a call to the call park extension. The QX1000 user enters call park extension's password and resumes the conversation with user A.

To make a Directed Call Park

To make a Directed Call Park, the QX1000 user, which has been previously added to the Park Access List for at least one of the available Call Park extension on the QX1000, should place the current call on hold and then dial the Call Park extension number within the five second timeout (see Feature Codes in Manual III - Extension User's Guide).

Attention: If the five second timeout is exceeded, then the QX1000 will consider it as an attempt for retrieving the parked call.

The Call Park extensions can be mapped directly to IP phones or simply announced via paging through the IP phones or analog paging system.

Calls can be easily parked by placing the current call on hold and then pressing the park button followed by the desired extension. This can be further simplified if the desired Call Park extension is already mapped to the phone, then the user will just press that specific park key and the call will automatically be parked to that extension.

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

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

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

Barge In Service

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

The **Barge In** service on the QX1000 allows the PBX users to participate to the third party's calls while remaining imperceptible. With the special feature codes (for details, see Feature Codes in the Manual III – Extension User's Guide), you may dial in to the active calls between the other local PBX user and his call partner and depending on the configuration and the feature code used you may listen to the call, additionally be able to speak to the extension user only or to all participants.
This service offers three options:

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

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

Upload Universal Extension Recordings

The **Upload Universal Extension Recordings** are to be defined by the QX1000 administrator and will be present instead of the default voice messages for all extensions on the QX1000. They will be used when no custom messages have been uploaded or recorded.
The following system messages can be uploaded from this page:

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

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

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

The **Memory Allocation** group includes a drop down list used to specify the **Percentage of System Memory** for the universal extension recordings. The maximum value in the drop down list is equal to the maximum available space for voice messages on QX1000.

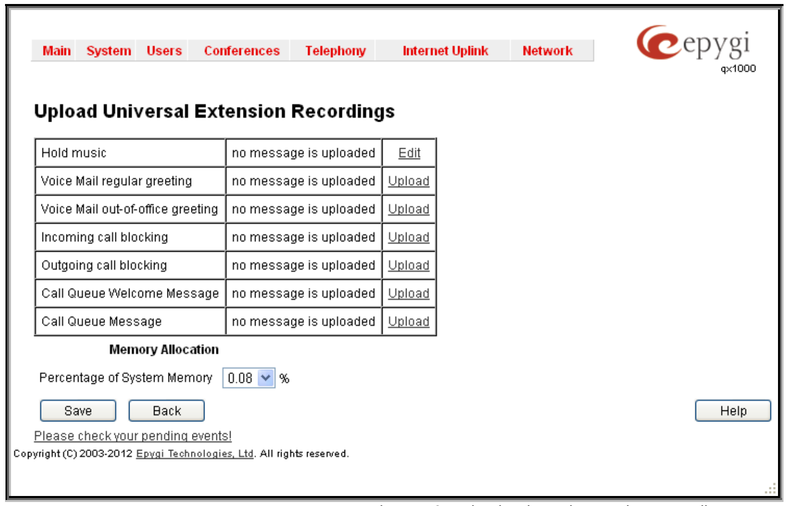


Fig. II-116: Upload Universal Extension Recordings page

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

Upload Universal Extension Recordings - Hold music

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

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

  Upload Recording text field can be used to type the path where hold music file is located. If hold music file is browsed with the help of file-chooser, this field displays the path of the browsed file. **Browse** button is used to browse for the hold music file.

  The music file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading the file and display the warning message "Invalid audio file or format is not supported". The system will refuse uploading also if there is not enough memory available for the corresponding extension and will then announce "You do not have enough space".

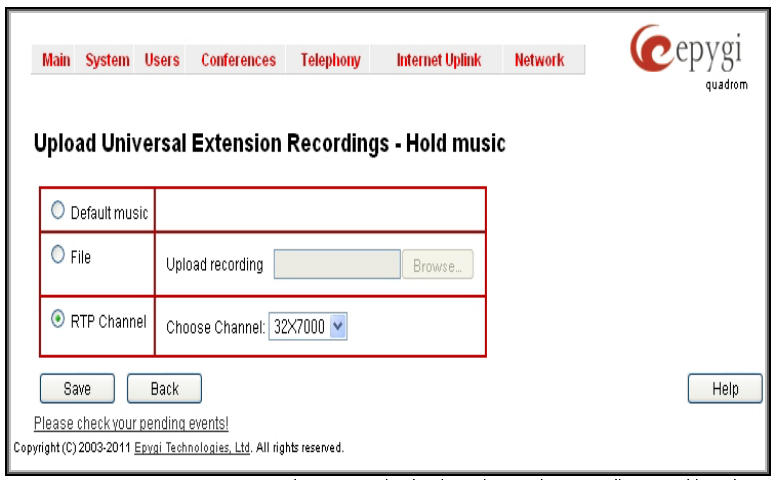


Fig. II-117: Upload Universal Extension Recordings p-Hold musicage

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

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

Recording Box

Recorded calls on the QX1000 can either be stored locally in the Recording Box or be uploaded to the remote FTP server. The **Recording Box** is used to locally store the recorded calls. The Recording Box can be accessible online from Web Management or from handset by calling the corresponding Recording Box extension. With both options, the user can play and delete the recorded calls located in the Recording Box.

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

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

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

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

The following information is available on this page:

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

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

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

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

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

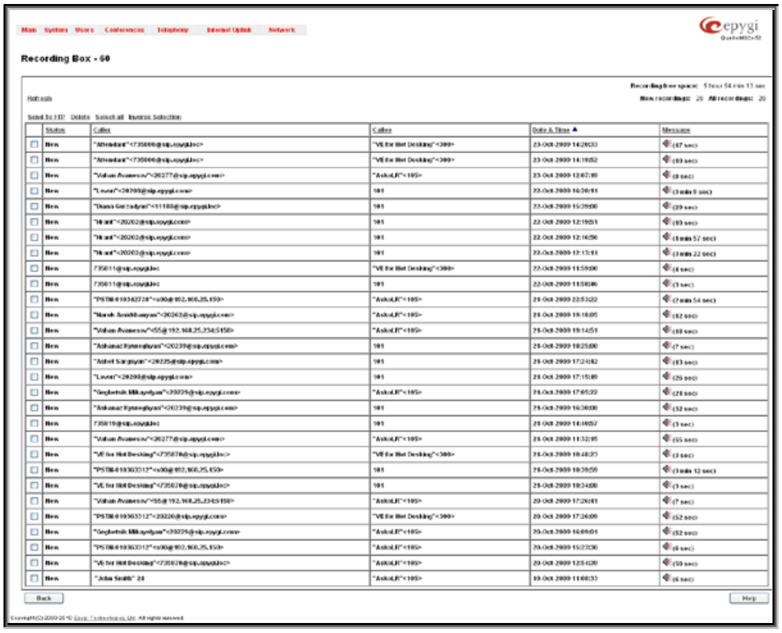


Fig. II-118 Extension's Recording Box

Recording Box table displays the following information:

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

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

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

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

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

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

Delete removes the selected recording(s).
Select All checks all existing entries in the table.
Inverse Selection inverses the current selection (if no entries are selected, clicking on inverse selection will check all entries).

To Play a Call Recording

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

To Delete a Call Recording

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

User Extension Bulk Import

The QX1000 **Extensions Template Management** feature and the PC-based **Bulk User Extensions Importer** tool are used to create and update multiple user-type extensions.

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

- Configure the common settings for a group of extensions, using the QX1000 Extension Template Management feature.

- Based on the common settings of these groups, configure the extensions specific settings using the Epygi **Bulk User Extensions Importer** tool. The tool will save the settings in a bulk User Extension configuration file that will be ready to upload to the QX1000.
- Import the configuration file to the QX1000, using the Extension Import feature.

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

To configure the Extension Templates on the QX1000, select the **Extension Template Management** tab from this page.
The **Extension Template Management** page is used to configure different sets of user extension settings. The **Extension Template Management** offers the following components:

Add opens the **Extension Template Management- Add Entry** page, where a new template can be created.

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

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

Select all selects all entries of the table.

Inverse Selection inverses the current selection (if no records are selected, clicking on inverse selection will select all records).

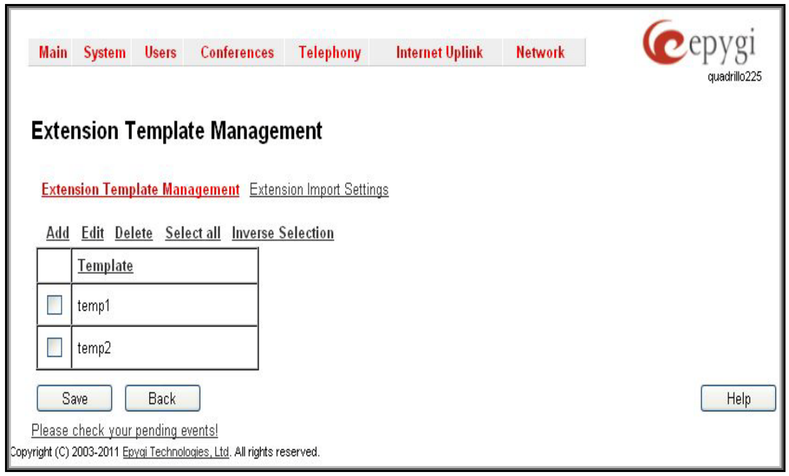


Fig. II-119 Extension Template Management page

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

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

When your configuration file is ready, select the **Extension Import Settings** tab to upload the Bulk User Extensions Importer configuration file to the QX1000.

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

The **Override Existing Extension** indicates whether the settings of the imported file should change the settings of existing extensions if the imported file is of the **Add** type. It can also contain the settings for extensions which already exist on the QX1000. When the **Override Existing Extension** is unchecked and the uploaded **Add** type CSV configuration file contains extensions which already exist on the QX1000, an error will appear and the conflicting extensions will be highlighted. If the uploaded file is of the **Add** type and the intent is to modify existing extensions, then the **Override Existing Extension** should be enabled, otherwise the file must be of the **Modify** type.

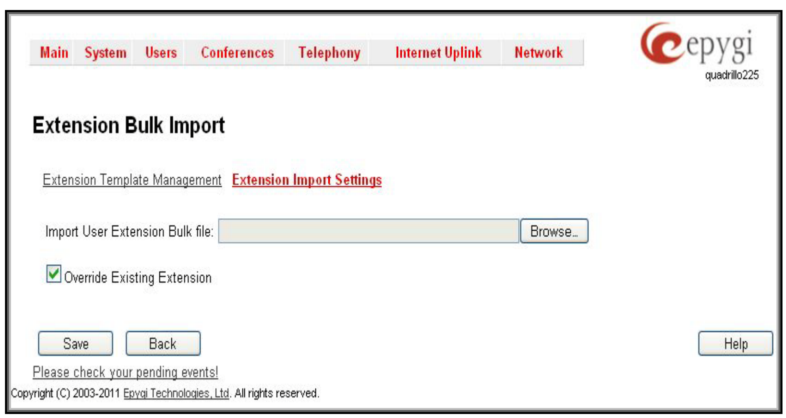


Fig. II-120 Extension Import Settings page

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

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

Receptionist Management

The receptionist feature on the QX1000 offers a variety of services to manipulate with multiple calls, to keep the calls in the queue with the perspective to be answered by the receptionist and finally to be forwarded to the corresponding destination, if needed.
The **Receptionist** service requires called extensions to use one of the following SIP Phones.

- Aastra 6730i
- Aastra 6731i
- Aastra 6739i
- Aastra 6755i (55i)
- Aastra 6757iCT (57iCT)
- Aastra 6757i (57i)
- Aastra 9133i
- Aastra 9143i (33i)
- Aastra 9480i (35i)
- Aastra 9480iCT (35iCT)
- Aastra 480i
- Aastra 480iCT
- Polycom SoundPoint IP 650
- snom 190
- snom 200
- snom 320
- snom 360
- snom 370
- snom 720
- snom 760
- snom 820
- snom 821
- snom 870
- Grandstream GXP 2000
- Grandstream GXP 2100
- Grandstream GXP 2110
- Grandstream GXP 2120
- Yealink SIP T-26P
- Yealink SIP T-28P
- Yealink SIP T-38G
- Epygi QCM

The following services are available to the receptionist:

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

Call Queue

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

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

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

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

Extension Status

QX1000 provides the possibility of controlling and determining the actual state of the managers phones' through the receptionist's IP phone (configuration of the IP phone is done automatically by QX1000 through the Receptionist Phone Configuration Wizard). A programmable key on the receptionist's IP phone that is assigned to the corresponding manager will blink when an incoming call to the manager's phone is currently ringing. The key lamp will be ON when manager is on a call and will be OFF if the manager's phone is in the idle state. The extension status can be watched (viewed) by the receptionist to determine the availability of managers for incoming call transfers to them.

Call Interception

To use Call Interception service, the managers' phones watch option should be enabled and each manager should have a programmable key assigned on the receptionist's IP phone. This is performed automatically by QX1000 through the Receptionist Phone Configuration Wizard.

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

Kickback

QX1000 allows the receptionist to forward the incoming calls to the manager's extension and if there is no answer or if the called extension is busy on another call, the call is returned to the receptionist's phone, instead of getting into Voice Mail Service or being disconnected. To use this service, receptionist should simply transfer the incoming call to the local extension. In case of no answer or busy, the call will automatically get back to the receptionist.

Voicemail Transfer

QX1000 allows the receptionist or extension user to forward incoming calls directly to the voice mail of the other attached extension. To do so, an appropriate routing pattern should be added to the Call Routing table. Hence, when transferring a call to the assigned extension, incoming call will directly go to the extension's voice mailbox.

Multi-Company Receptionist

QX1000 provides the possibility to use a single IP phone to manage the receptionist's features for multiple companies at the same time. To do so, the incoming line appearance for the phone should be created, attached to the IP line of the IP phone and be labeled to the corresponding company name. Being busy with a call related to one company, the receptionist is able to also receive the calls related to other companies. While calls are ringing in the background, the receptionist can switch between the incoming calls. If the receptionist does not answer the incoming calls, and if the Call Queue service is enabled on the extensions, the incoming calls will be stored in the queue specific for each company line.

The **Receptionist Management** page allows you to configure IP phones to be used as a receptionist on the QX1000. This page contains the list of configured receptionists with information about the attached IP lines and watched extensions.

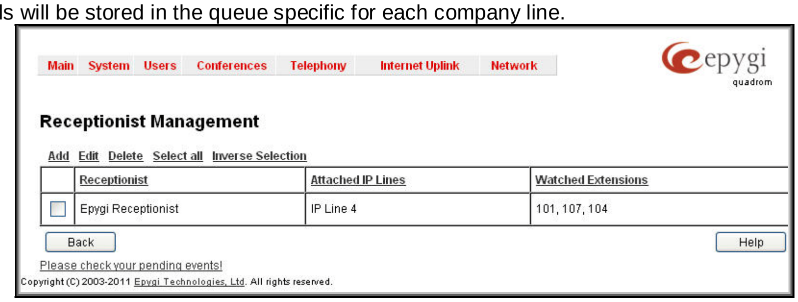


Fig. II-121: Receptionist Management page

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

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

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

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

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

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

The **Attached IP Lines** text field requires the numbers of QX1000's IP lines used by the receptionist. The IP lines should be separated by commas.

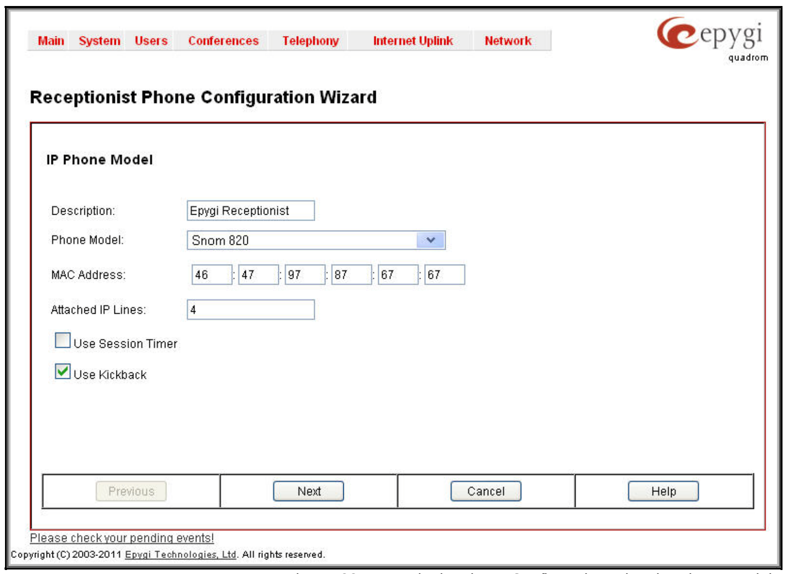


Fig. II-122: Receptionist Phone Configuration Wizard – Phone Model

The **Use Session Timer** enables the SIP session timer for the IP lines specified in the **Attached IP Lines** text field. This checkbox enables advanced mechanisms for connection activity checking. This option allows both user agents and proxies to determine if the SIP session is still active.

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

If you have selected the snom 320/360/370/720/760/ 820/821/870, Grandstream GXP 2000/2100/2110/2120, Yealink T-28P/T-26P/T-38G IP phones from the **Phone Model** drop down list, the next page in the wizard will be the **Receptionist Phone Configuration Wizard – Hardware Modules**. For all other phone models, this page is skipped.
For Grandstream GXP 2000/2100/2110/2120 IP phones, this page contains a single checkbox only:

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

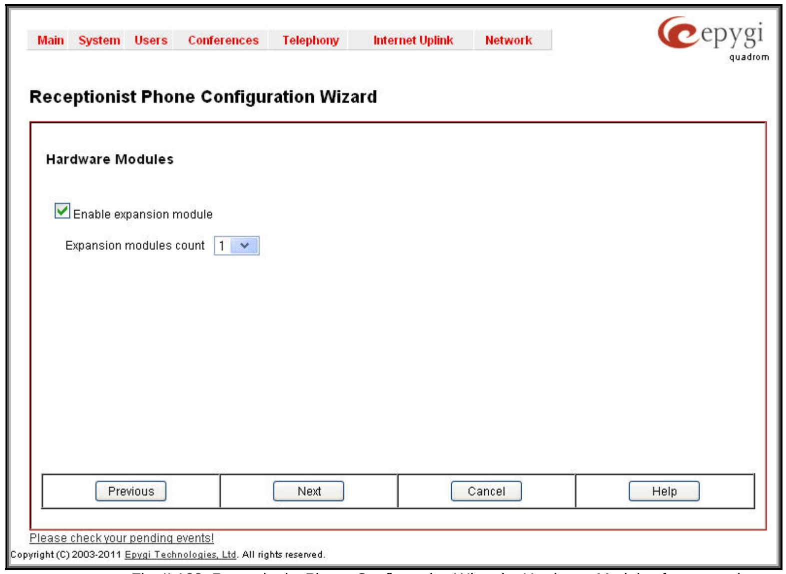


Fig. II-123: Receptionist Phone Configuration Wizard – Hardware Modules for snom phone

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

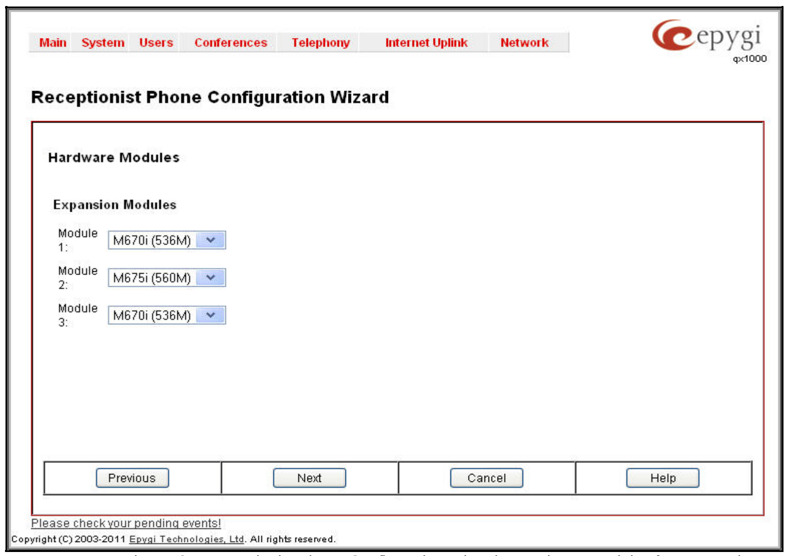


Fig. II-124: Receptionist Phone Configuration Wizard – Hardware Modules for Aastra phone

The next page of the wizard is skipped for QCM **Phone Model** selection. The content of this page depends on the configuration made on the first page of the **Receptionist Phone Configuration Wizard**.

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

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

- **Watch Ext. #** - watch the extension on the QX1000 and a possibility to pickup the call addressed to that extension.
- **Call Park Ext #** - watch the calls parked to the corresponding extensions and a possibility to retrieve the calls parked to that extension.

This list also contains a number of PBX services available on the QX1000 and accessible with the * key combination (see QX1000's Feature Codes). When configured from this page, the key combinations become transparent for the IP phones too.

- **Vmail** – accesses the voice mailbox of the extension to which the receptionist IP line is attached to.

- **DND** – enables the Do Not Disturb service on the extension to which the receptionist IP line is attached to.
- **CallFwd** – accessed Forwarding Management of the extension to which the receptionist IP line is attached to.
- **AutoReDI** – auto redials the last dialed call.
- **CallBack** – calls back to the last caller.
- **LineInfo** – gets the IP line information from the QX1000.
- **CallBlk** – blocks the last caller.
- **Record** – records the call (in case if the manual call recording is allowed for the call, configured from
- **Call Recording**– used for configuring the call recording rules
- **ACD Login/Logout** – allows the corresponding ACD agent to login to all groups it is involved in, if previously logged in, to log out from those groups. For details on ACD functionality, see ACD Management.

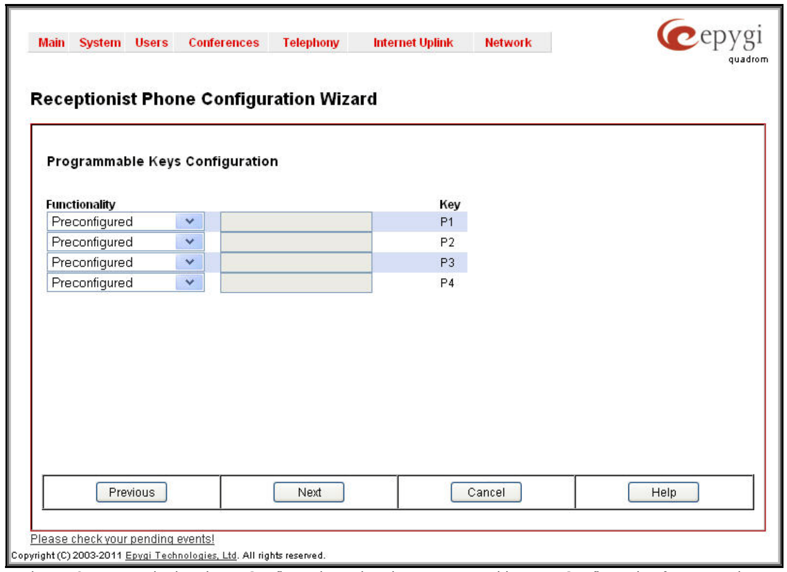


Fig. II-125: Receptionist Phone Configuration Wizard – Programmable Keys Configuration for snom phone

For snom phones, when multiple IP lines are selected on the **Attached IP Lines** text field on the first page of the **Receptionist Phone Configuration Wizard**, this list additionally contains the number of specified IP lines. That selection is used to set the correspondence between the selected IP lines and the available Programmable keys on the IP Phone. To do so, select the IP lines corresponding to each programmable key from the **Functions** drop down list on this page. Each programmable key on the snom IP phone will now be responsible for the selected IP line on the QX1000.

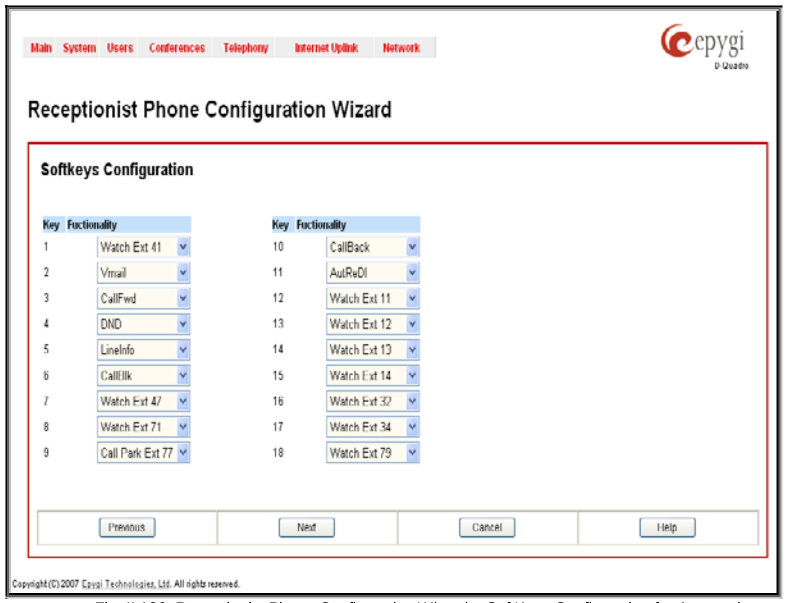


Fig. II-126: Receptionist Phone Configuration Wizard – SoftKeys Configuration for Aastra phone

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

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

Fig. II-127: Receptionist Phone Configuration Wizard – Summary page

Extensions Directory

The **Extensions Directory** is a useful tool for callers to get direct access to the QX1000 extensions by spelling the username with the help of the phone keypad. The Extensions Directory can be accessed through **QX1000's Auto Attendant Services** and it has its own manipulation buttons to browse the directory.

The **Extensions Directory Settings** page allows you to make a list of names assigned to the extensions on the QX1000. If the name spelled by the caller matches the one(s) listed in the Extensions Directory, the corresponding extension user name(s) will be played to the caller for verifying the input and selecting the user to connect. Each extension's user should record their name with the help of the handset (see chapter Update System Messages), or they can upload a wave file from the Account Settings page.

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

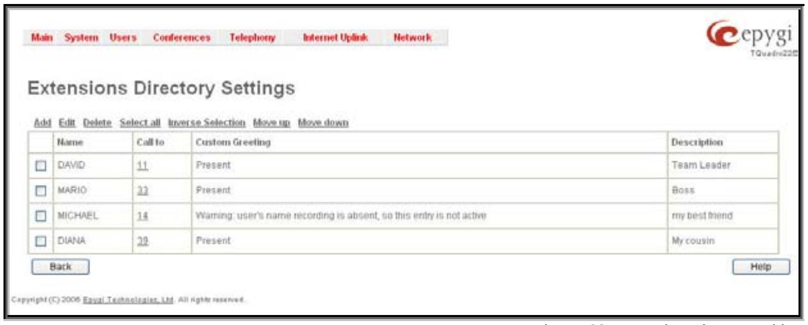


Fig. II-128: Extension Directory table

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

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

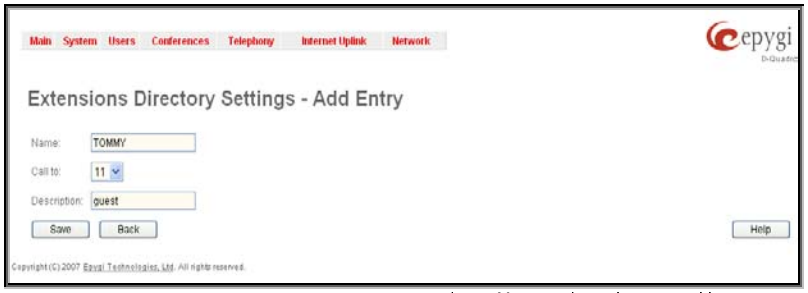


Fig. II-129: Extensions Directory - Add Entry page

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

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

Call to drop down list contains all extensions on the QX1000 that should ring when selecting the specified Name.

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

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

Authorized Phones Database

The **Authorized Phones Database** page is used to create a list of trusted external phones. If they are part of the QX1000 Authorized Phones database, external SIP or PSTN, then users are free to access the QX1000 Auto Attendant services without requiring authentication. When adding a trusted phone to the list, an existing extension has to be chosen. The parameters (extension number and password, as well as SIP and Speed Calling Settings) will be used automatically for the trusted caller access of the QX1000 Auto Attendant. A direct connection to the **Call Relay** menu can be optionally provided.

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

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

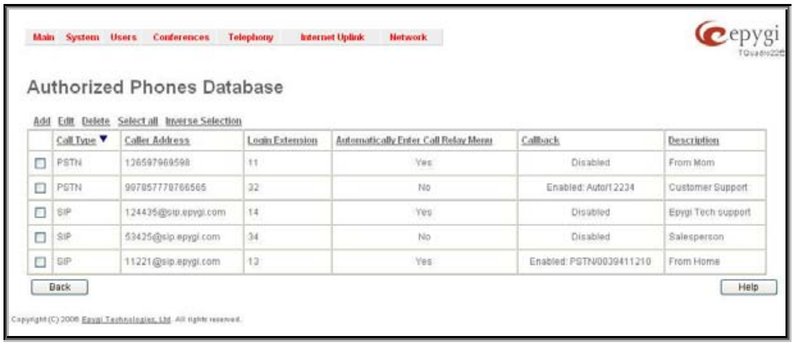


Fig. II-130: Authorized Phones Database

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

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

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

Caller Settings

The **Call Type** drop down list includes possible incoming call types (SIP or Auto). In **SIP**, the caller connects QX1000 through a SIP server and **Auto** is used for undefined call types and the destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.

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

Fig. II-131: Authorized Phones Database - Add Entry page

The **Login Extension** drop down list provides all existing extensions on the QX1000. When calling the QX1000 Auto Attendant, a trusted user will automatically be logged in as the selected extension, i.e., the extension number and its password will be automatically submitted by the QX1000 system. The trusted user will directly access the QX1000 Auto Attendant services. The SIP settings of the login extension will be used when making IP calls.

The **Automatically Enter Call Relay Menu** checkbox enables direct access for the trusted user to the QX1000 Auto Attendant Call Relay menu. If the checkbox is not selected, a trusted caller will be directed to the Auto Attendant's main menu, but will still be able to reach Remote Access (Voice Mailbox of the specified extension) and Call Relay services (see Feature Codes) with no authentication.

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

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

Callback Settings

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

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

The **Callback Destination** text field requires the destination number where QX1000 should instantly call back to. The value inserted in this field is dependent on the selected callback call type: for **PBX**, extension number is required, for **SIP**, the SIP address is requires and **Auto** is used for undefined call types: destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Call Routing table. If this field is left empty, the callers address will be implied as a callback destination.

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

To Add an Authorized phone to the database

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

To Delete an Authorized phone from the database

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

Call Back Services

With **Call Back** service, callers can save a call charge when calling to and through QX1000. QX1000 provides the possibility of creating a list of those trusted callers that are allowed to make free of charge calls to QX1000's Auto Attendant or through its Call Relay menu to the third party SIP or PSTN destination. Two types of Call Back services are available on the QX1000: **Pre-configured Call Back** and **Remote Call Back Configuration**.

Pre-Configured Call Back

For **Pre-configured Call Back**, a list of trusted callers must be configured in the QX1000's Authorized Phones Database using Web Management. The Call Back service should be enabled and a valid callback destination should be specified for each caller.

To use **Pre-configured Call Back**, the caller registered in the Authorized Phones Database should simply call to the QX1000's Auto Attendant through SIP or PSTN, let the call to ring twice and then hang up. Call Back will be instantly activated, and QX1000 will call back to the defined Call Back destination. By answering the incoming call caller will be connected to the Auto Attendant menu.

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

Remote Call Back

The **Remote Call Back Configuration** service is used by authorized callers to configure or reconfigure existing call back configuration on the QX1000. Remote Call Back Configuration is divided into two modes accessible from the QX1000's Auto Attendant: **Permanent Call Back** and **Non-Permanent Call Back**.

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

Permanent Call Back service allows callers registered in the Authorized Phones Database to create a new trusted caller with Call Back enabled. They can also modify the Call Back destination of existing callers in the Authorized Phones Database. By calling QX1000's Auto Attendant and entering the Auto Attendant menu, the caller can use the * 6 code (see Feature Codes) to create a new trusted caller as well as to modify the Call Back destination for the already registered callers in the Authorized Phones Database.

By entering **Permanent Call Back** reconfiguration menu, system asks caller to login by dialing the number and an appropriate password for the QX1000's extension that is used as login extension in the Call Back settings. After passing the login, callers should follow the voice instructions for configuring a new entry or reconfiguring existing entries in Authorized Phone database.

When system accepts the inserted settings, the corresponding entry will be logged to the Authorized Phones Database. The caller will then be disconnected from the QX1000's Auto Attendant and the defined Call Back destination will receive a call from the QX1000 within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX1000's Auto Attendant.

Please Note: The detected caller number must correspond to the one applied by the caller. In case of PSTN call back at least one PSTN line must be available on the QX1000. There must be network connectivity and the destination must be reachable.

Non-Permanent Call Back configuration service allows trusted caller to organize one-time Call Back to the defined destination. In this situation, no entry will be logged to the Authorized Phones Database. By calling QX1000's Auto Attendant and entering the Auto Attendant menu, the caller can use * 5 menu (see Feature Codes) to modify the Call Back destination for already registered callers in the Authorized Phones Database.

The system will ask to login by dialing the number and an appropriate password for the QX1000's extension that is used as login extension in the Call Back settings. After login, caller should follow the voice instructions for reconfiguring the existing entry in Authorized Phone database. The caller will then be disconnected from the QX1000's Auto Attendant and the defined Call Back destination will receive a call from the QX1000 within the next 45 seconds. Answering the incoming call, the caller will be reconnected to the QX1000's Auto Attendant.

Please Note: For both **Permanent Call Back** and **Non-Permanent Call Back**, the detected caller number must correspond to the one configured for trusted caller. In case of PSTN call back at least one PSTN line must be available on the QX1000. There must be network connectivity and the destination must be reachable.

ACD Management

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

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

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

- **Agent** – a call center user reachable via QX1000.
- **Agent Group** (AG) – comprises the call queue, collection of agents (call center users), and call distribution mechanism between its agents.
- **Interactive Voice Response system** (IVR) – a custom Auto Attendant on QX1000, answering the calls from remote callers/customers, collecting information from callers in the form of DTMF digits and, based on that, making the routing decision on delivering the call to proper Agent Group.
- **Predefined ACD Agent Auto Attendant** - used for agent login/logout and updating the current status of the agent from the phone.

To monitor ACD processes on the QX1000, Epygi provides a **Statistics, Monitoring and Reporting (SMR)** application, running on MS Windows PC. SMSR doesn't require the 3PCC license (see Features section) to be installed on the QX1000. It displays the current status and statistics on Agent Groups and Agents, builds the statistical reports and sends notifications and alerts to ACD supervisor/administrator. For more details and requests for this applications, contact Epygi sales division (www.epygi.com).

Agent

Agent is the call center user answering the customers' calls and reachable via QX1000 due to ACD. To receive the calls, agent needs to be logged into some Agent Group (AG). Agent is characterized by the agent ID, password, skills' levels and termination phone number. Agent can be logged into several agent groups at the same time and receive the calls distributed by those agent groups. For easy login/logout to all groups where the agent is subscribed, agent should use the ***83** feature code from the handset.

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

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

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

Agent Group

Agent Group (AG) is actually a QX1000 extension with enhanced capabilities. The type of that extension in QX1000 configuration is **ACD Group** (see ACD Group Extension Settings). Except for regular attributes intrinsic to extension (like extension number, SIP user name, etc.), it is characterized also by the collection of agents included into that group, call queue and the call distribution mechanism. These agent group specific parameters of extension are being configured from **ACD Group Settings** or **ACD Agents Table** accessible from ACD Group Extension Settings.

Call Queue of Agent Group

Agent Group receives the calls from customers via means existing currently on QX1000. For example, it may receive the direct call through ITSP on SIP number (DID number) assigned to AG, receive a call through ACD's IVR on AG's extension number, external call through Call Routing table on QX1000, etc.

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

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

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

Calculation of Composite Skill Grade

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

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

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

Interactive Voice Response system

ACD IVR is a custom Auto Attendant (see Attendant Extension Settings) configured on QX1000 with VoXML script and voice prompts designed for quizzing the customers, determining the set of required skills as described above and routing the call to the agent group having the maximum current value of the composite skill grade for required set. Since the general skill set is configured by ACD administrator and is application specific (call center specific), the VoXML script and voice prompts of IVR should be built taking into account the skill set configured by administrator.

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

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

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

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

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

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

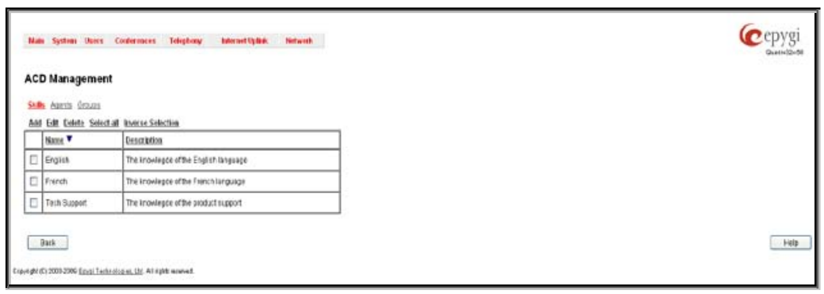


Fig. II-132: ACD Management - Skills page

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

Fig. II-133: ACD Management - Add Skill page

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

Add opens the **Add Agent** page where a new agent may be created. The **Add Agent** page contains the following components:

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

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

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

Description requires an optional description of the agent.

Call Type lists the available call types:

- **PBX** - extensions on the QX1000

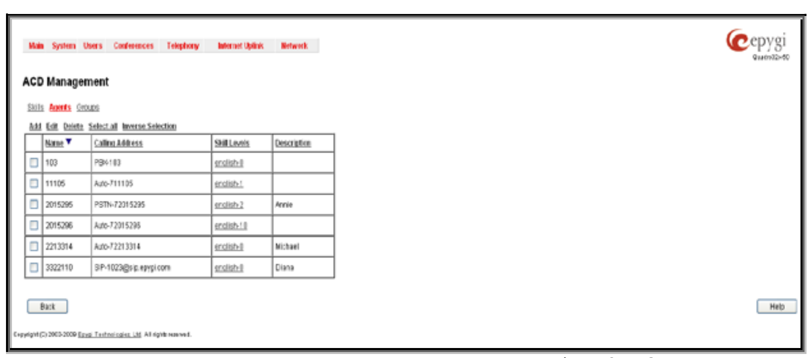


Fig. II-134: ACD Management page

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

Fig. II-135: ACD Management - Add Agent page

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

If the **PBX** call type is selected, the **Calling Address** field should contain the extension number on QX1000 and the corresponding agent can be reached by calling on extension number located on the same QX1000. However, it doesn't necessarily mean that the agent shall be located at that QX1000 – if the extension is remote extension then agent's location might be far from QX1000.

For the **SIP** call type, the **Calling Address** field should contain the SIP address (see chapter Entering a SIP Addresses correctly) and the corresponding agent can be reached by calling on SIP address. The agent with that kind of termination number might be located either at the same QX1000 or anywhere else in the SIP network.

For the **Auto** call type, the **Calling Address** field should contain the phone number routable through Call Routing table on QX1000. The agent with that kind of termination number might be positioned in any of the above mentioned locations.

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

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

Fig. II-136: ACD Management – Agent Skills page

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

Add opens the **Add Group** page where a new ACD Group may be created. The **Add Group** page includes the only **ACD Group ID** text field which requires the ACD Group number (extension).

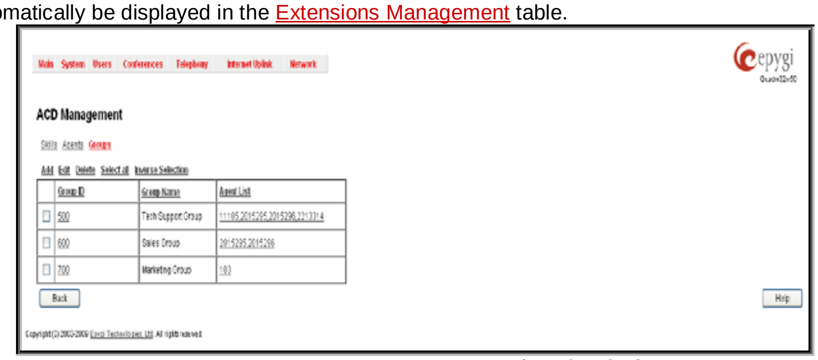


Fig. II-137: ACD Group Management page

The ACD Group ID should not match any existing extension in the Extensions Management table. Any newly created ACD Group will automatically appear in the Extensions Management table.

Edit opens ACD Group Extension Settings in the Extensions Management.

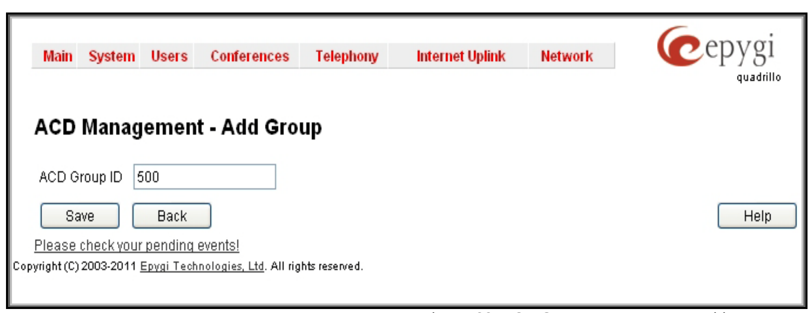


Fig. II-138: ACD Group Management - Add Entry page

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

Conferences Menu

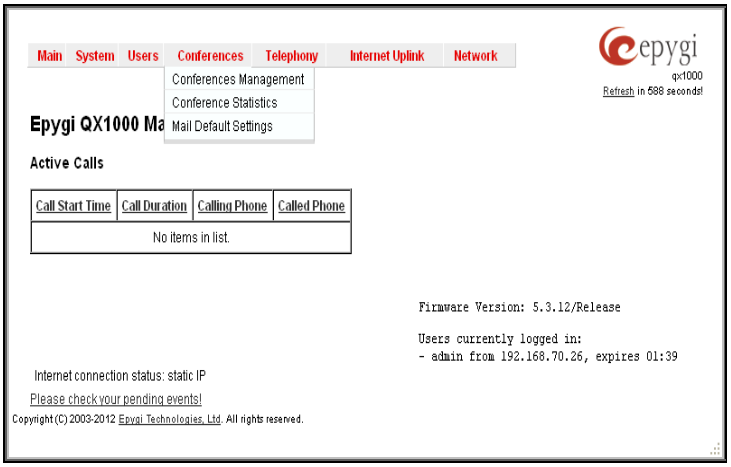


Fig. II-139: Conferences Menu in Dynamo Theme

Fig. II-140: Conferences Menu in Plain Theme

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

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

After activating Video Conferencing feature from the "features.cgi" GUI page, the video codecs will be available on the QX1000's "Conference Codecs" GUI page.

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

Video Conferencing provides possibility to view particular participant based on switching modes.

In general there are two switching modes for each phone:

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

- **Automatic –** In this mode the Epygi QX1000 determines the speaker (or loudest participant), and will automatically switch the video stream to show that speaker. As a result all the video phones, which are in automatic mode, will see the speaking participant. If participant does not have a video phone, then the other participants will see a black screen.

Please Note: Users can switch between manual and automatic mode by using *50/*51 and *52.
By default, **Automatic Speaker Detection** is switched off. From the **General settings (conferencegeneral.cgi)** GUI page admin can enable or disable the default mode for video conferencing (see Automatic Speaker Detection).

Conferences Management

The **Conference** page displays a table with the existing conferences on the system. This page allows you to create new conferences and manage the existing ones. The following columns are present in the **Conferences** table:

- **Conference ID** - indicates the unique ID of the conference. This number is used from Auto Attendant to reach the conference. The Conference ID is also used as the username for the moderator when logging into the QX1000.
- **Display Name** – any optional information about the conference.
- **Description** – any descriptive information about the conference.
- **SIP Address** - displays the SIP address of the conference.

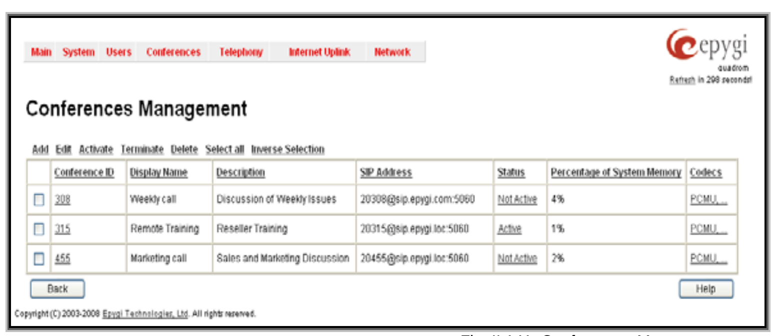


Fig. II-141: Conferences Management page

- **Status** - indicates the status of the conference (Active, Non Active or Waiting). Clicking on the conference status link will display the **Conference Progress** page with detailed information about the conference status, participants in the conference and description of each participant. This page additionally allows the administrator to drop a participant from the conference or invite new participants. It also allows the moderator to start/stop/resume/pause the conference recording and to terminate the conference.

- **Percentage of System Memory** - indicates the conference related memory space (in percents) dedicated to conference recordings and the conference specific custom system messages.
- **Codecs** - column lists the short information (full information is seen in the tool tip) about conference specific voice Codecs. Conference codec's can be accessed and modified by clicking on the link of the corresponding conference's Codecs. The Link moves to the Conference Codecs page.

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

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

Add opens the **Add Entry** page where a new conference can be created.

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

Please Note: The length of the Conference ID is limited to the extension length configured from Extensions Management. The Conference ID cannot start with the digit 0, which is a reserved character.

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

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

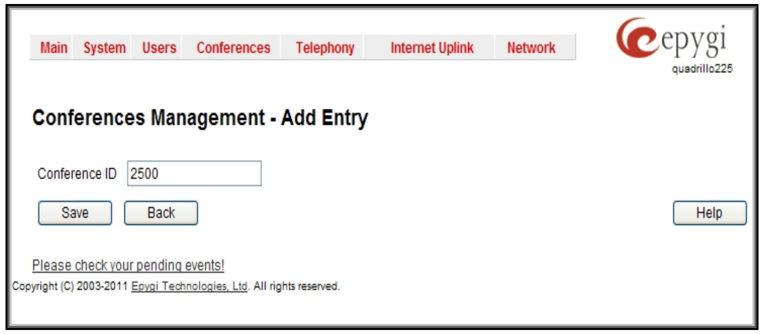


Fig. II-142: Conferences Management page

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

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

Please Note: Save changes before moving among settings groups.

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

- **Display Name** is any optional information about the subject of the conference.
- The **Password** text field requires a password for the moderator access to the conference. The password inserted here is used by the moderator to join the conference. The moderator is able to use conference codes during an active call conference and access conference specific GUI pages to coordinate the conference (view/change conference properties, activate/deactivate it, start/stop/resume recording, view conference statistics). The **Confirm Password** text field requires the confirmation of the moderator's password.
- The **Show on Public Directory** checkbox is selected, the details of the selected conference will be displayed in the User Settings table on the **Main Page** of the Extension's QX1000 Web Management. Besides this, the details of the conference will be displayed in the Public Directories on the snom and Aastra SIP phones. Leave this checkbox unselected if the conference is reserved or not used.
- The **Percentage of System Memory** drop-down list is used to select the memory space (in percents) that can be used for storing conference recordings.

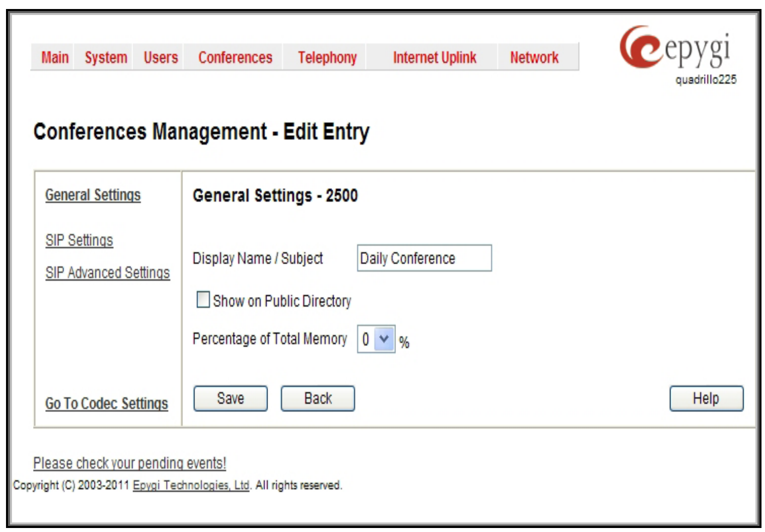


Fig. II-143: Edit Entry – General Settings page

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

Activate is used to activate the selected conferences.

Terminate is used to stop the selected conferences.

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

Select all selects all existing conferences.

Inverse selection inverses the current selection of conferences (if no records are selected, all records will be checked).

Conference Statistics

In the **Conference Statistics** page, the calls are classified by conferences. The call statistics (sent via 3PCC, Radius, email or FTP) is the same as is - it shows only the PBX calls not sorted out by the conference. The billing or accounting program can build the conference statistics analyzing the PBX CDRs (if the Called Phone is the Conference ID then it is a conference call).
The **Conference Call Statistics** page consists of four tables. They provide information on conference call details, successful incoming and outgoing, unsuccessful outgoing conference calls in the first three tables and statistics settings in the fourth one. Conference call statistics allows the collecting of conference call events on the QX1000 with their parameters and to search them by various criteria. Only the administrator is allowed to enable or disable the conference statistic services.The link **Statistics Settings** that is used for this purpose is only displayed when an administrator is logged in. The **Statistics Settings** page offers the following input options:

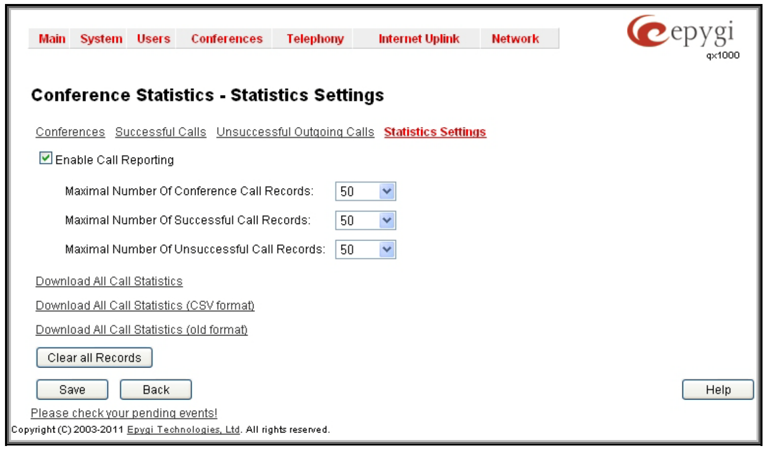


Fig. II-144: Conference Statistics-Statistics Settings page

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

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

The **Download All Call Statistics** link is used to download the entire displayed statistics in a file that can be viewed with a simple text editor. This type of conference call statistics file is easy-to-read and can be displayed in a spreadsheet.

The **Download All Call Statistics (CSV format)** link is used to download the entire displayed conference call statistics in a CSV (Comma-Separated Values) formatted file.
The **Download All Call Statistics (old format)** link is used to download the entire displayed conference call statistics in an old formatted file. This file can also be viewed with a simple text editor but contains more intricately aligned content.
The **Clear all Records** button is used to clear all conference call statistics records.
When the number of Conference Call Statistics entries exceeds the numbers specified in the **Statistics Settings** page, the oldest entries are being automatically deleted.

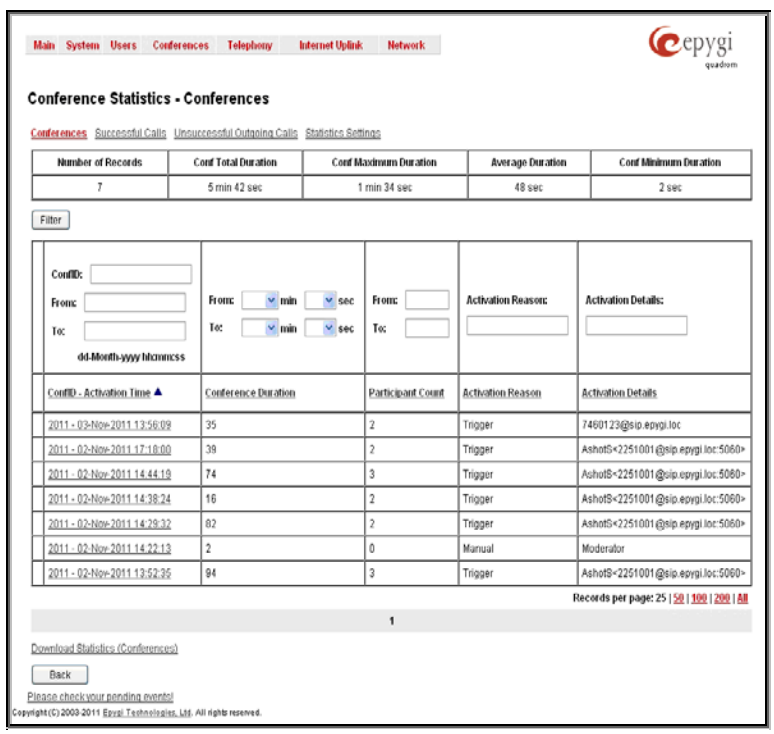


Fig. II-145: Conference Statistics-Conferences page

The **Conferences** page lists all Conference Calls and their parameters (**ConfID- Activation Time**, **Conference Duration**, **Participant Count**, **Activation Reason** and **Activation Details**). Each column heading in the tables is created as a link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending, descending) arrows will be displayed close to the column heading.

The **Activation Reason** column indicates whether the participant is a key member to start the conference, i.e. when participant dials into the conference, the conference is getting automatically activated and the dial out participants (if any) are called to join the conference (see Conference Progress).

The **Activation Details** column provides information about how the conference call is activated.

The **Filter** button performs searching within the statistics tables. The search may be done with several criteria at the same time.

The following search criteria are available:

- The text fields **ConfID**, **From** and **To** are used for the search by **ConfID-Activation Time**. **ConfID** requires the unique ID of the conference. For **From** and **To** fields the data must be entered in the format dd-mm-yyyy hh:mm:ss. The time criteria are optional, if it is not needed, leave the text fields empty. The **From** field must indicate an earlier date and time from that which is indicated in the **To** field. Otherwise the error message "Minimal date should be less than maximal date" prevents filtering and searching.
- The **From** and **To** drop down lists offer a search by the **Conference Duration**, specified by the list of values. The field **From** must indicate a shorter duration than the field **To**. Otherwise the error message "Minimal duration should be less than maximal duration" prevents statistics filtering.
- The **From** and **To** drop down lists offer a search by the **Participant Count**, specified by the list of values. The field **From** must indicate a shorter count than the field **To**. Otherwise the error message "Minimal count should be less than maximal count" prevents statistics filtering.
- The text fields **Activation Reason** and **Activation Details** require the reason and the details of the conference call activation to be defined.

Number of Records displays the current amount of conference call statistics entries in the table. For **Conferences** and **Successful Calls** pages **Total Duration**, **Maximum Duration**, **Conf Average Duration** and **Minimum Duration** statistics are organized at the top of the table.
The **Records per page** are used to select the number of displayed conference call statistic records per page. The **Previous** and **Next** can be utilized to switch between these pages.
The **Download Statistics (Conferences)** links are available below for all Conference Call Statistics tables and allows you to download the displayed conference call statistics in a text file.

The pages **Successful Calls** and **Unsuccessful Outgoing Calls** lists successful and unsuccessful outgoing calls and their parameters (**ConfID- Activation Time**, **Call Start Time**, **Call Duration**, **Calling Phone** and **Called Phone**). Each column heading in the tables is created as a link. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending, descending) arrows will be displayed close to the column heading.

The **Details** column is only present in **Successful Calls** table and provides the following information:

- Brief information about the call quality, voice codec used to receive and transmit packets and the close conference call reason. The close conference call reason appears to provide more information about the call termination reason which can be a network problem, termination by one of the conference call parties, voice mail service activation, etc. Clicking on the details information will open the RTP Statistics page where all RTP parameters of established conference call are provided.
- **Authenticated By** information details the conference participants that passed an authentication on the QX1000 as configured in the Local AAA Table.

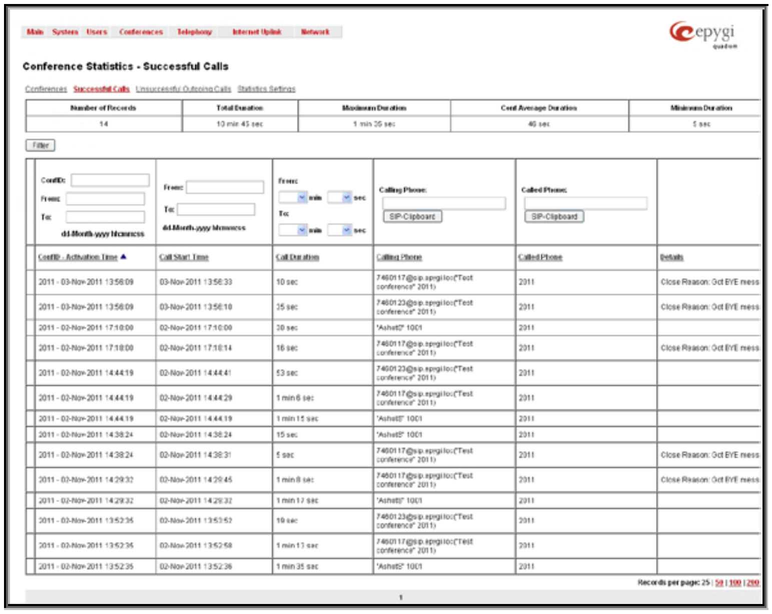


Fig. II-146: Conference Statistics-Successful Calls page

The **Call Detail** column is present only in the **Unsuccessful Outgoing Calls** table and indicates the reason why the call was unsuccessful.
The **Filter** button performs searching within the statistics tables. The search may be done with several criteria at the same time.
The following search criteria are available:

- The text fields **ConfID**, **From** and **To** are used for the search by **ConfID- Activation Time**. **ConfID** requires the unique ID of the conference. For **From** and **To** fields the data must be entered in the format dd-mm-yyyy hh:mm:ss. The time criteria are optional, if it is not needed, leave the text fields empty. The **From** field must indicate an earlier date and time from that which is indicated in the **To** field. Otherwise the error message "Minimal date should be less than maximal date" prevents filtering and searching.
- The text fields **From** and **To** drop down lists offer a search by the **Call Start Time**. The data must be entered in the format dd-mm-yyyy hh:mm:ss. The time criteria are optional, if it is not needed, leave the text fields empty. The **From** field must indicate an earlier date and time from that which is indicated in the **To** field. Otherwise the error message "Minimal date should be less than maximal date" prevents filtering and searching.
- The **From** and **To** drop down lists offer a search by the **Call Duration**, specified by the list of values. The field **From** must indicate a shorter duration than the field **To**. Otherwise the error message "Minimal duration should be less than maximal duration" prevents statistics filtering.
- The text fields **Calling Phone** and **Called Phone** require the calling and called conference party's SIP address, extension number or PSTN number as search criterion. Wildcard symbols are allowed here. The **SIP- Clipboard** buttons at the end of the lines open a small window where one of the previously entered 10 SIP addresses can be automatically selected again.

The **Records per page** are used to select the number of displayed statistic records per page. The **Previous** and **Next** can be utilized to switch between these pages.
The **Download Call Statistics** links are available below for all Conference Call Statistics tables and allows you to download the displayed call statistics in a text file.

Mail Default Settings

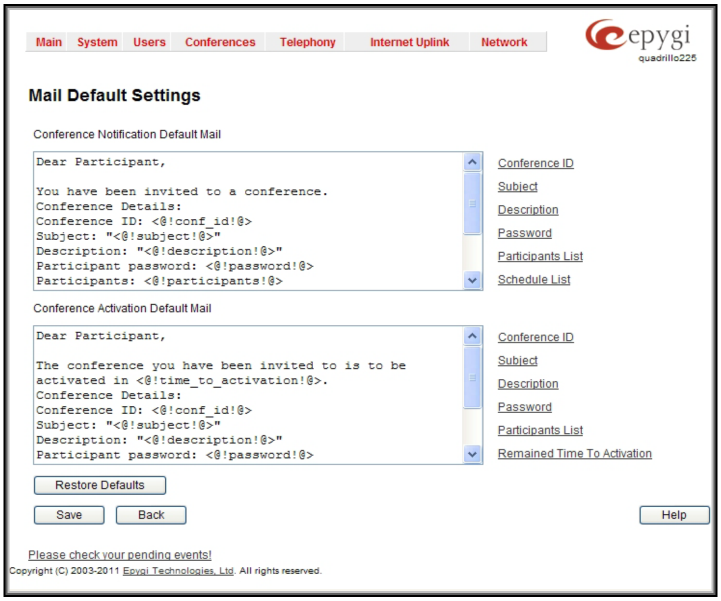


Fig. II-147: Edit Entry – General Settings page

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

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

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

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

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

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

Telephony Menu

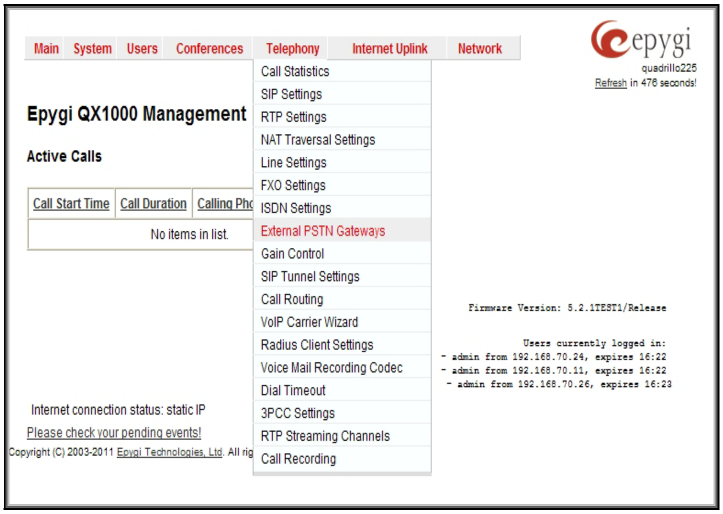


Fig. II-148: Telephony Menu in Dynamo Theme

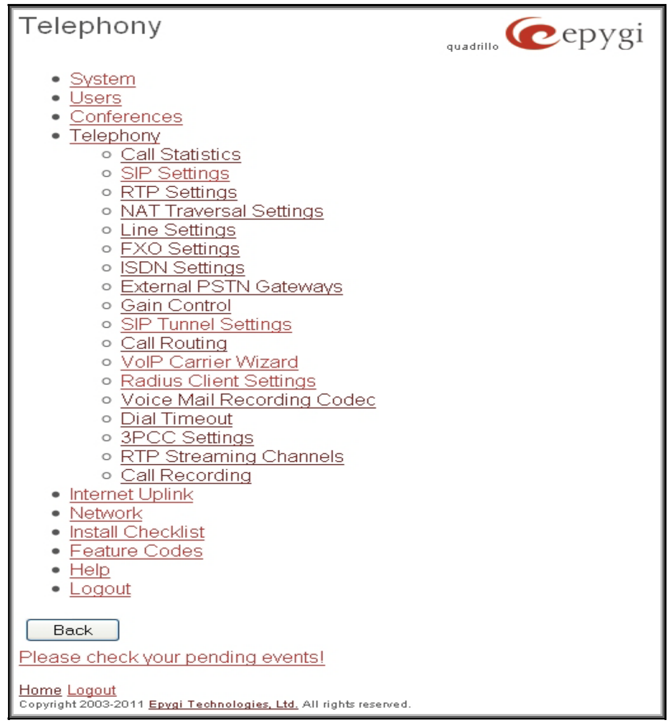


Fig. II-149: Telephony Menu in Plain Theme

Call Statistics

The **Call Statistics** page consists of five tables. They provide information on successful, unsuccessful and missed incoming and outgoing calls on the first three tables, statistics settings in the fourth table and statistics archive in the fifth one. Call statistics allows the collecting of call events on the QX1000 with their parameters and to search them by various criteria. The selected number of statistics entries will be displayed in the Call Statistics tables.

The Call Statistics page reports successful, non-successful and missed incoming/ outgoing calls and shows the call statistics settings. Only administrator is allowed to enable or disable the call statistic services. The link **Statistics Settings** that is used for this purpose is only displayed when an administrator is logged in.

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

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

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

The **Download All Call Statistics** link is used to download the entire displayed statistics in a file that can be viewed with a simple text editor. This type of call statistics file is easy-to-read and can be displayed in a spreadsheet.

The **Download All Call Statistics (CSV format)** link is used to download the entire displayed statistics in CSV (Comma-Separated Values) formatted file.

The **Download All Call Statistics (old format)** link is used to download the entire displayed statistics in an old formatted file. This file can also be viewed with a simple text editor but contains more intricately aligned content.

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

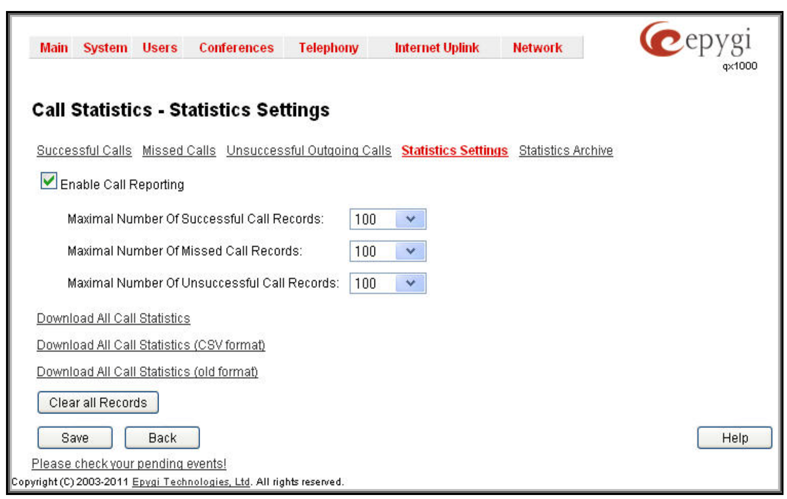


Fig. II-150: Call Statistics Settings page

When the number of Call Statistics entries exceeds the numbers specified in the **Statistics Settings** page, the oldest entries are being automatically deleted. In order to keep the call statistics entries safe, QX1000 allows you to configure the **Statistics Archive** service of the call statistics.

The **Statistics Archive** page is used to configure the automatic archiving of the call statistics.

The **Percentage of Total Memory used for Archive** drop-down list is used to select the internal memory space (in percents) that can be used for storing the archived call statistics. When the required memory exceeds the size entered, the oldest entries are being automatically deleted.

The **Enable Call Statistics Archive Collection** checkbox enables automatic downloading mechanism of the call statistics. **Please Note:** This service only refers to the statistics collected from the moment of enabling this service and forward; any previously generated statistics will not be downloaded.

The **Call Statistics Archive Structure** is used to configure the intervals for archiving the call statistics. The archiving structure allows to archive the call statistics either by time intervals or per statistics record count:

The **Call Records Count** drop down list is used to select the portion size of the call statistics (including all types of call statistic, i.e. successful, missed and unsuccessful outgoing call statistics) which will be archived locally. The number selected in this drop down list indicates the number of entries in the single archived call statistics file. If there are no enough entries in the call statistics table on the QX1000, the system will wait until the necessary number of entries will be collected and then will archive the statistics file.

The **Time Interval** drop down list is used to select the time interval by which the call statistics will be archived locally. After each time interval the system will archive the call statistics (including all types of call statistic, i.e. successful, missed and unsuccessful outgoing call statistics). If there are no any record made during last time interval the black file is archived.

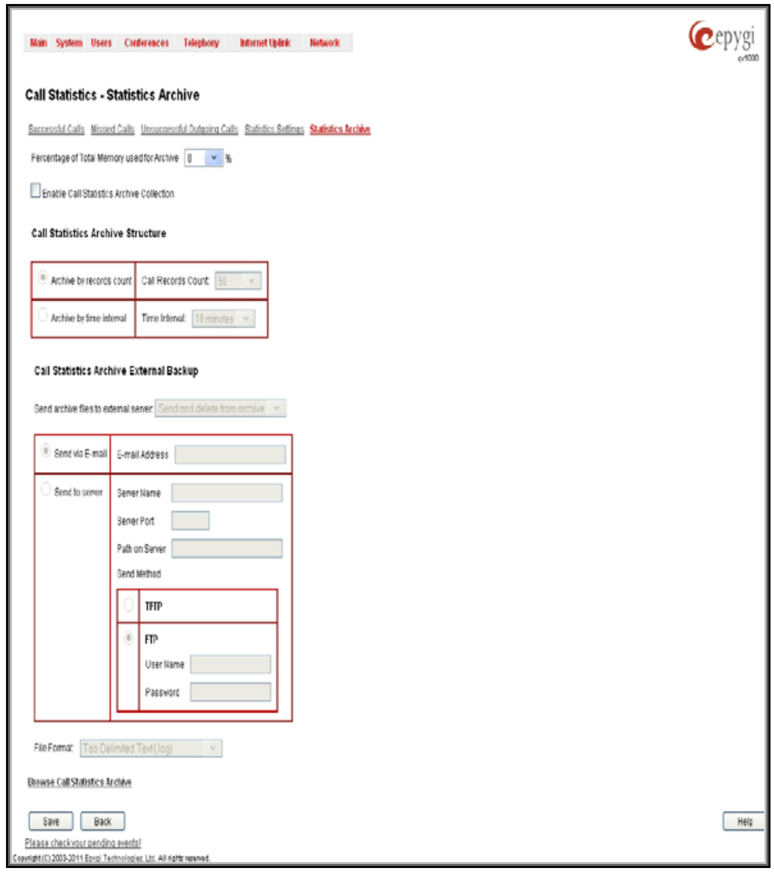


Fig. II-151: Call Statistics – Statistics Archive page

The **Call Statistics Archive External Backup** is used for configuring the call statistics backup service.

The **Send archive files to external server** is used to enable/disable the backup service and configuring whether the statistics should be kept locally after backing up them.

Two options of the call statistics backup are available: uploading the call statistics file to the server or sending it to the mailing address.

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

- The **Send via Email** radio button is used to send the call statistics files via email. The selection enables **Email Address** text field that requires the email address of the administrating person to receive the call statistics files.
- The **Send to Server** radio button is used to store the call statistics files on a remote server. This selection enables the following fields to be inserted:
    - The **Server Name** requires the IP address or the host name of the remote server.
    - The **Server Port** requires the port number of the remote server.
    - The **Path on Server** requires the path on the server to store the call statistics files in.

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

The **File Format** drop down list is used to select the format in which call statistics will be saved. This list offers to choose between Tab Delimited Text (.log) and Comma Separated Values (.csv) file formats.

The **Browse Call Statistics Archive** link opens the **Call Statistics Archive** page. In the table on this page all available call statistics archived files are listed.

The **Archive Record** field shows the time when the call statistics was archived.

The **[csv]** and **[log]** links in this field allows you to download the archived call statistics file to the PC in a Comma Separated Values (.csv) or Tab Delimited Text (.log) file formats and opens the file-chooser window where the saving location can be specified.

The **Number of Call Records** field shows the number of records in particular call statistics archive file.

The **External Backup Status** shows the status of the backup.

The following functional buttons are available on this page:

Delete removes the selected record(s) from the system and Call Statistics Archive table.

Select all selects all entries of the table.

Inverse Selection inverses the current selection (if no entries are selected, clicking on inverse selection will check all entries).

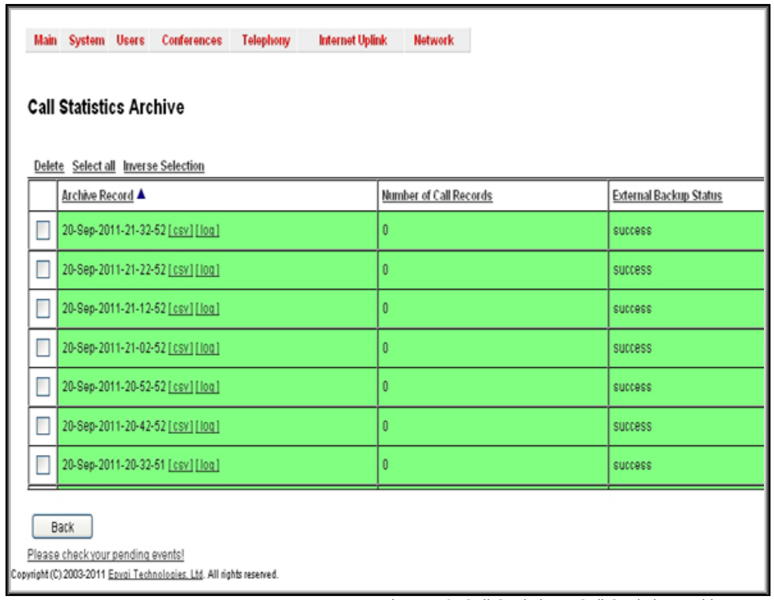


Fig. II-152: Call Statistics – Call Statistics Archive page

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

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

The **Call Statistics: Successful Calls, Missed Calls and Unsuccessful Outgoing Calls** pages consist of the general information on successful, missed and unsuccessful calls, search fields and the calls table. The Filter button performs searching within the statistics tables. The search may be done with several criteria at the same time.

The following search criteria are available:

- The text fields **From** and **To** are used for the search by **Call Start Time**. The data must be entered in the format dd-mm-yyyy hh:mm:ss. The time criteria are optional, if it is not needed, leave the text fields empty. In **From** field must indicate an earlier date and time from that which is indicated in the **To** field. Otherwise the error message "Minimal date should be less than maximal date" prevents filtering and searching.
- **From** and **To** drop down lists offer a search by the **Call Duration**, specified by the list of values. The field **From** must indicate a shorter duration than the field **To**. Otherwise the error message "Minimal duration should be less than maximal duration" prevents statistics filtering.
- The text fields **Calling Phone** and **Called Phone** require the calling and called party's SIP address, extension number or PSTN number as search criterion. Wildcard symbols are allowed here. The SIP-Clipboard buttons at the end of the lines open a small window where one of the previously entered 10 SIP addresses can be automatically selected again.

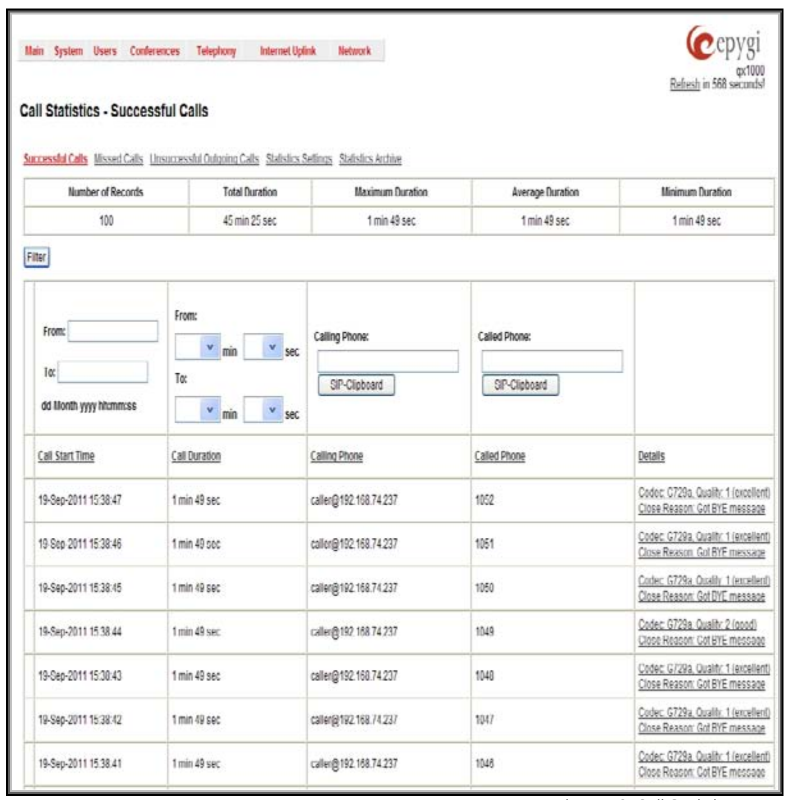


Fig. II-153: Call Statistics page

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

The **Details** column (available for the administrator) is only present in **Successful Calls** table and provides the following information:

- Brief information about the call quality, voice codec used to receive and transmit packets and the close call reason. The close call reason appears to provide more information about the call termination reason which can be a network problem, termination by one of the call parties, voice mail service activation, etc. Clicking on the details information will open the RTP Statistics page where all RTP parameters of established call are provided.

- **Authenticated By** information details the callers that passed an authentication on the QX1000 as configured in the Local AAA Table.
- Information about FAX statistics for the calls that have a FAX transmission handled. It only appears when there was a FAX transmission during the call. Clicking on the FAX link in the **Details** column will move to the FAX Statistics page.

The **Call Detail** column is present only in the Unsuccessful Calls table and indicates the reason why the call was unsuccessful.

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

The **Records per page** used to select the number of displayed statistic records per page. The **Previous** and **Next** allows to switch between these pages.

The **Download Call Statistics** links are available below for all Call Statistics tables (for administrator's access only) and allows you to download the displayed call statistics in a text file.

To Enable/Disable the Statistics

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

To Filter the Statistics

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

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

To Reset the Statistics

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

RTP Statistics

The **RTP Statistics** page provides detailed information about the established call is provided. When QX1000 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 QX1000's IP line to an external SIP destination or from one external SIP destination to another through the QX1000's Auto Attendant. Each group of parameters describes characteristics of a piece of RTP stream composing an overall SIP session. Normally, one leg describes the RTP stream from caller to the QX1000 and the other leg describes the RTP stream from QX1000 to the destination.

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

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

Fig. II-154: RTP Statistics page

The **Local** and **Remote** fields indicate the two peers between which the RTP stream is transmitted. The characteristics in the table below describes to the piece of RTP stream between these peers.

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

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

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

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

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

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

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

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

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

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

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

Rx Maximum Delay = max V(i) / 8

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

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

Please Note: RTP Statistics is logged only when at least one of the call endpoints is located on the QX1000. 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 QX1000’s routing rules.

In the first case, RTP statistics will be logged if remote extension or IP line user is calling locally to the QX1000’s extension or auto attendant.

The **Configure Call Quality Event Notification** link leads to the **Configure Call Quality Event Notification** page where call quality control notification specifics can be configured.

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

This page consists of a **Notify** checkbox, which enables the call quality monitoring mechanism for the corresponding event notifications, and a **Call Quality less than** drop down list where the least satisfactory call quality should be selected. When a call with the quality less than the level selected here is registered on the QX1000, an event notification will appear. When the **Notify** checkbox is disabled, no Call Quality events will occur on the QX1000.

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

Fig. II-155: Configure Call Quality Event Notification page

The **Configure System Events** link leads to the Events page where the methods of notification for each system event can be configured.

FAX Statistics

The **FAX statistics** page is accessed from the Call Statistics page by clicking on the **FAX** link in the **Details** column for the calls that contain T.38 FAX transmission.

The **FAX statistics** page provides information about received and transmitted packets, lost, bad and duplicated packets. This statistics refers only to the T.38 FAX transmission. The FAX statistics is not available for the FAX transmitted with other protocols.

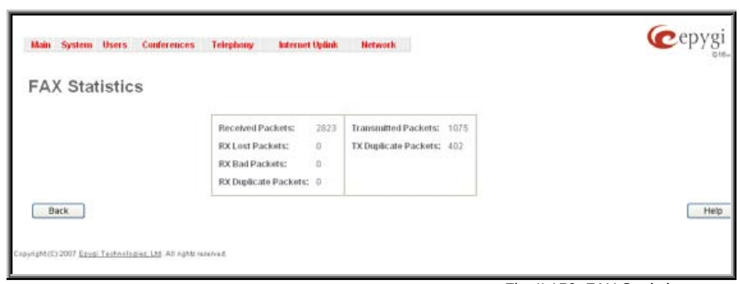


Fig. II-156: FAX Statistics page

SIP Settings

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

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

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

Please Note: QX1000 will not use TCP protocol as a transport for SIP messages if the **TCP Port** field is left empty.

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

The **Realm** text field requires messaging level information to be included in SIP messages sent by QX1000. 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.

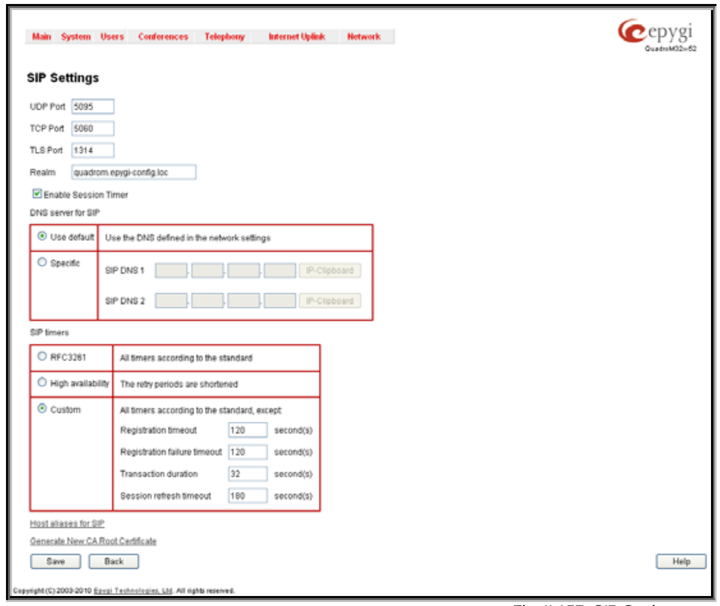


Fig. II-157: SIP Settings page

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

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

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

- **RFC 3261** will apply standard SIP timers described in the corresponding specification.
- **High availability** will apply SIP timers to shorten the call establishment, registration confirmation and registration failure procedures. This selection provides more firmness to the SIP connection but increases the network traffic on the QX1000.
- **Custom** allows manually defining the **Registration Timeout**, **Registration Failure Timeout**, **Transaction Duration** and **Session refresh timeout** SIP timers (in seconds).

Host aliases for SIP link leads to the page where QX1000's external aliases are listed.

Generate And Install New CA Root Certificate link leads to the page where new CA root certificate may be defined, generated and installed.

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

Host aliases for SIP

This page is used to create a list of QX1000's hostnames register on remote DNS servers. This list will be used to identify SIP packets received from remote servers where QX1000 is registered with different names.

The **Host aliases for SIP page** consists of a table where QX1000's aliases are listed. Add opens the **Add Entry** page where a new alias name for QX1000 should be defined.

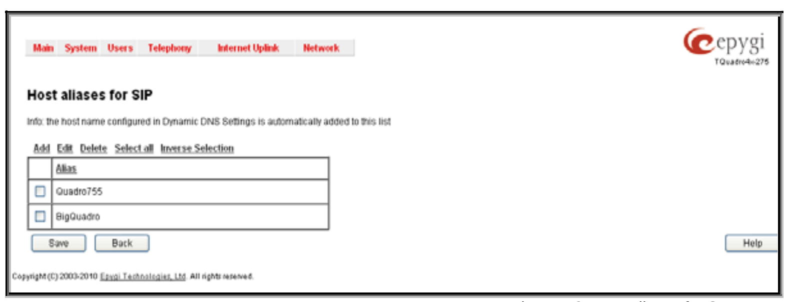


Fig. II-158: Host aliases for SIP page

Generate And Install New CA Root Certificate

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

The **General Certificate and Install** button is used to generate a new CA root certificate based on the defined data and to install it on the QX1000. QX1000 will get rebooted automatically once the new certificate is installed. You may download the actual copy of the certificate from SIP Settings page.

To ensure a secure TLS connection with the QX1000'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 QX1000. If the end user is a server or other device, you may download the certificate from the QX1000 and apply it manually on the remote side.

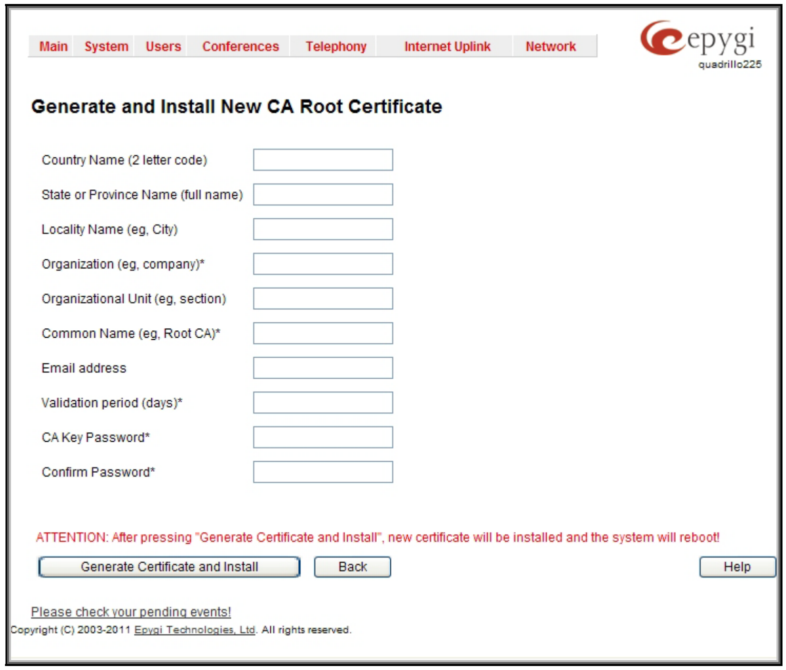


Fig. II-159: Generate and Install New CA Root Certificate page

RTP Settings

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

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

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

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

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

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

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

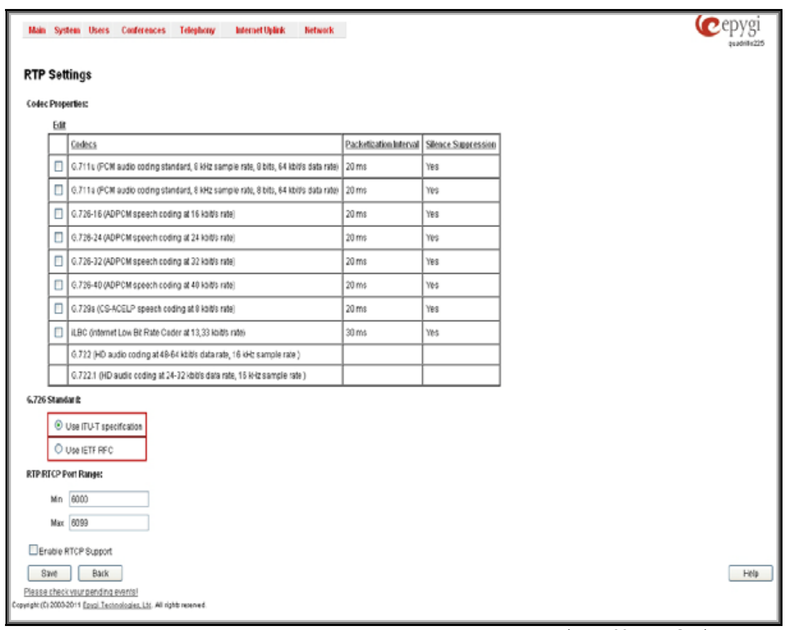


Fig. II-160: RTP Settings page

RTP/RTCP Port Range:

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

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

Telephone Event Draft Support enables telephony events transmission according to the draft-ietf-avt-rfc2833bis-04. The checkbox needs to be toggled if the SIP destination party phone or IVR has problems recognizing DTMFs generated by the QX1000.

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

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

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

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

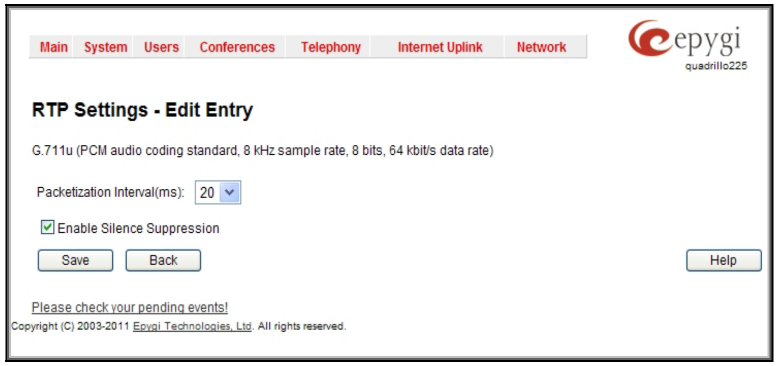


Fig. II-161: RTP Settings - Edit Entry

__To Edit Codec Parameters__

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

NAT Traversal Settings

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

The **General Settings** page consists of a manipulation radio buttons group to select the mode of the NAT Traversal usage for the SIP traffic (any incoming and outgoing SIP messages from and to the QX1000 will be routed through the NAT PC).

- **Automatic** – with this selection, system will analyze the QX1000's WAN IP address and if it is in the IP range specified for local networks (according to RFC), the SIP traffic will be routed through NAT. Otherwise, if QX1000's WAN IP address is outside the specified IP range, no SIP traffic will be routed through NAT server.
- **Force** – with this selection, all the SIP traffic will be routed through the NAT server.
- **Disable** – with this selection, no SIP traffic will be routed through the NAT server.

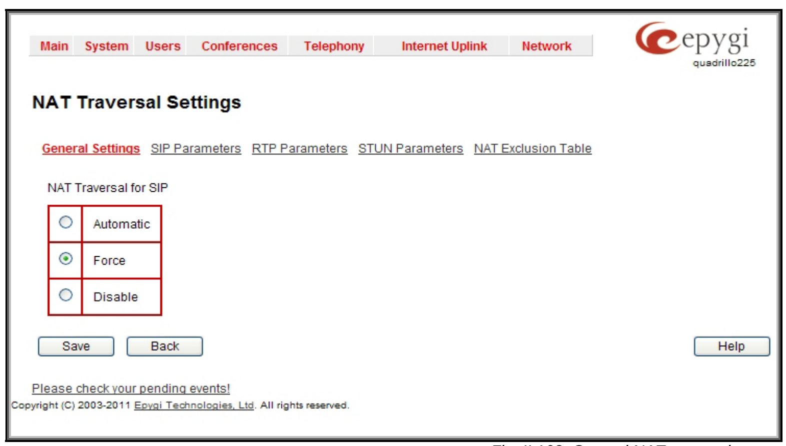


Fig. II-162: General NAT traversal page

The **SIP Parameters** page is used to configure NAT specific settings for SIP and offers two independent groups of settings:

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

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

Selecting **Use Manual NAT Traversal** allows you to manually define the mapped settings for the SIP UDP traffic over NAT:

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

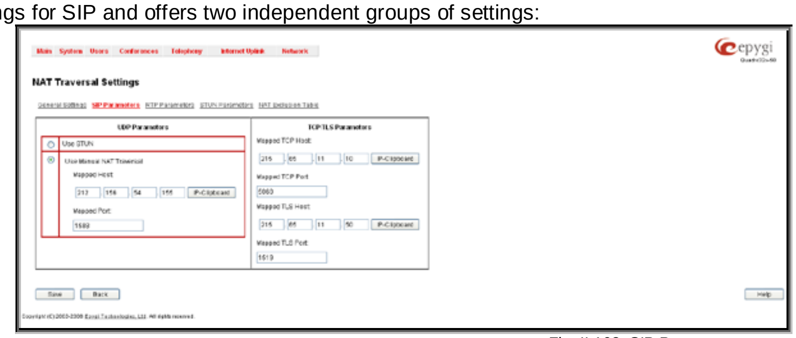


Fig. II-163: SIP Parameters page

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

TCP/TLS Parameters:

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

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

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

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

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

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

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

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

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

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

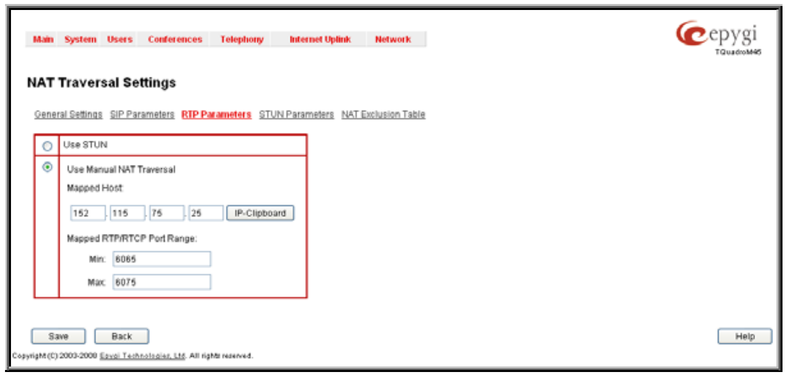


Fig. II-164: RTP Parameters page

The **STUN Parameters** page enables automatic NAT configuration through the STUN server and is used to configure the STUN (Simple Traversal of UDP over NAT) client on the QX1000. This page requires the following data to be inserted:

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

The **Secondary STUN Server** and **Secondary STUN Port** text fields respectively require the parameters of the secondary STUN server.

The **Polling Interval** drop down list contains the possible time intervals between referrals to the STUN server.

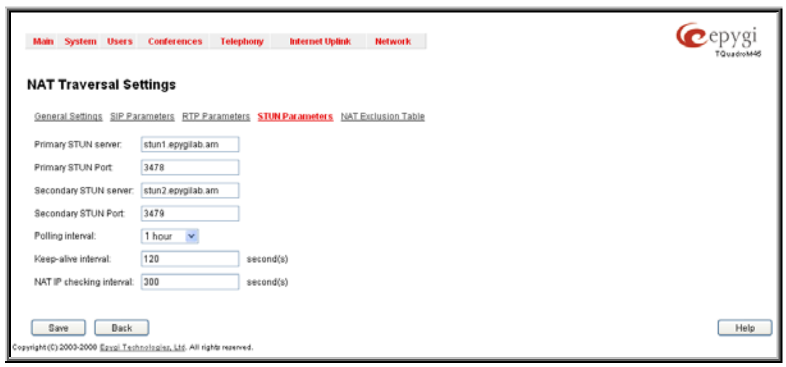


Fig. II-165: STUN Parameters page

The **Keep-alive interval** text field provides the options to select the time interval (in seconds) for keeping NAT mapping alive. The value should be in the range of 10 to 300 seconds.

The **NAT IP checking interval** text field indicates the interval (in seconds) between the NAT IP checking attempts (used to distinguish the possible NAT IP address changes and to perform registration on the new host). The value should be in the range of 10 to 3600.

The **NAT Exclusion Table** lists all possible IP ranges that are not included in the NAT process, but may be accessed directly. IP addresses that are not listed in the **NAT Exclusion Table** are accessed over NAT. For example, if a QX1000 user needs to make SIP calls within the local network as well as outside of that network, all local IP addresses are required to be excluded from NAT traversal settings by being listed in this table. Otherwise, a malfunction may occur in SIP operations.

The **NAT Exclusion Table** page offers the following input options:

Each record in the table has a corresponding checkbox assigned to its row. The checkbox is used to delete or to edit the corresponding record. Only one record may be edited at a time. An error message will appear if no selection is made or more than one is selected.

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

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

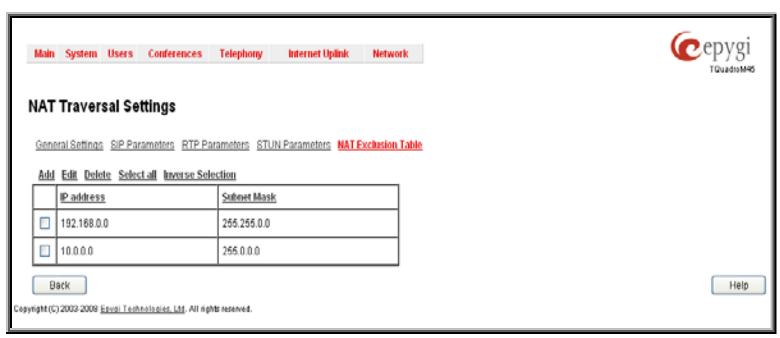


Fig. II-166: NAT Exclusion Table page

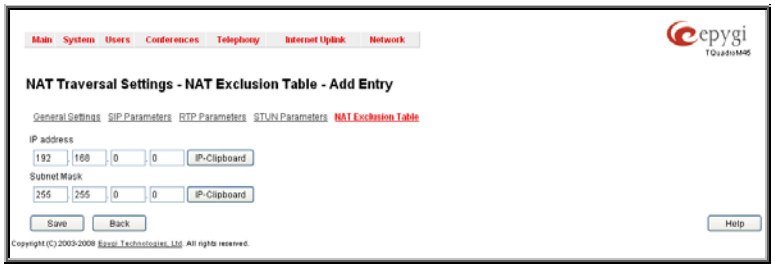


Fig. II-167: NAT Exclusion Table - Add Entry page

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

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

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

To Configure the NAT Exclusion Table

1. Press the **Add** button on the **NAT Exclusion Table** page. The **Add Entry** page will appear in the browser window.
2. Specify an **IP Address** and its **Subnet Mask** in the corresponding text fields.
3. Press **Save** on the **Add Entry** page to add the selected IP range to the **NAT Exclusion Table** list.

To Delete an IP Range from the NAT Exclusion Table

1. Select the checkboxes of the corresponding IP range(s) that should to be deleted from the **NAT Exclusion Table**. Press **Select all** if all IP ranges should to be deleted.
2. Press the **Delete** button on the **NAT Exclusion Table** page.
3. Confirm the deletion by pressing **Yes**. The IP range will then be deleted. To abort the deletion and keep the IP range in the list, press **No**.

Line Settings

The **Line Settings** are used to configure QX1000 IP Line settings. The **IP Line Settings** page is used to configure IP lines for IP phones to be connected to the QX1000. QX1000 provides the options to connect SIP phones to its WAN side, assign the corresponding IP line to an active extension, and use SIP phones as a simple phone with all telephony services of the QX1000 (for example, call hold, waiting, transfer, etc).

By default, 200 active IP Lines are available on the QX1000. The **IP Line Settings** page displays a table with the available IP lines on the QX1000. Entering the feature key in the Features page can enable more IP lines.

Enable PnP to IP lines checkbox is used to setup the SIP phones connected to the QX1000 via Plug and Play automatic configuration service. To use this service, this checkbox needs to be selected. The SIP phone should be reset then. After a clean boot-up of the SIP phone, QX1000 will detect the SIP phone and all its characteristics, generate the automatic configuration file and will upload it to the SIP phone. The SIP phone will be then configured on the first available IP line of the QX1000 and will become completely functional.

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

Enable Firmware Version Control checkbox is used to control the firmware version running on the SIP Phone attached to the QX1000. This service also allows you to have the new firmware automatically downloaded and installed on your SIP Phone (in case your SIP phone was running an old firmware upon connecting to the QX1000 or when the QX1000's firmware has been updated and the compatibility was changed to the higher firmware version of the SIP phone). Every new firmware of QX1000 is compatible to a certain firmware version of each supported SIP phone. If you are running older firmware on your SIP phone, this service will automatically download and install the newer firmware on your SIP phone.

Please Note: The Firmware Version Control service is only available for the supported SIP phones (see the list below).

Attention: Do not select this checkbox if you wish to run other firmware version on your SIP phone than the one compatible with the QX1000.

The **Phones Default Template** drop down list is used to select the QX1000 default template for the IP Phone which will be used if not selected otherwise on the particular line (see below).

The **Manage IP Phones Templates** link takes to the Manage IP Phones Templates page where custom IP phone templates may be created.

The **Upload IP Phones Logo** link takes to the IP Phones Logo page where custom logo for the IP phone may be uploaded.

The FXS Gateway Management link takes to the page where QX1000 FXS gateway devices may be defined in order to add additional FXS lines to the QX1000.

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

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

The alternating **Hide disabled IP lines** and **Show disabled IP lines** buttons are used to respectively hide or show the IP lines that have not been activated with a feature key. To enable the lines, install a feature key from the Features page.

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

Inactive – this selection disables the corresponding IP line.

SIP Phone – this selection configures the IP line for a SIP phone to be connected to the QX1000's LAN.

- **Phone Model** drop down list is used to select the IP phone model to be used by the receptionist. The drop down list, excluding **Other** selection, enables the MAC address text fields used to insert the **MAC Address** of the corresponding SIP phone. Use **Other** selection if your SIP phone is not in this list.
- **Line Appearance** text field requires a number of simultaneous calls supported by the SIP phone.
- **Username** and **Password** are required for this selection. They should match on both the QX1000 and the SIP phone for a successful connection. The **Password** field is checked against its strength and you may see how strong is your inserted password right below that field.To achieve the well protected strong password minimum 8 characters of letters in upper and lower case, symbols and numbers should be used. If you are unable to define a strong password, press **Generate Password** to use one of system defined strong passwords
- **Transport** drop down list is used to select the SIP protocol transport layer - UDP, TCP or TLS. For TLS you may activate the TLS certificate update mechanism from IP Phone to obtain the latest certificate generated by the QX1000.

For automatic SIP phone configuration, the SIP phone should be reset/rebooted. The appropriate configuration will then be automatically downloaded from QX1000 to the SIP Phone.

Please Note: For automatic configuration, some SIP phones may require additional actions to follow the restart. For example, by default the IP Dialog SIP Tone II is in a non-auto-provisioning mode, so it should be manually enabled on the phone.

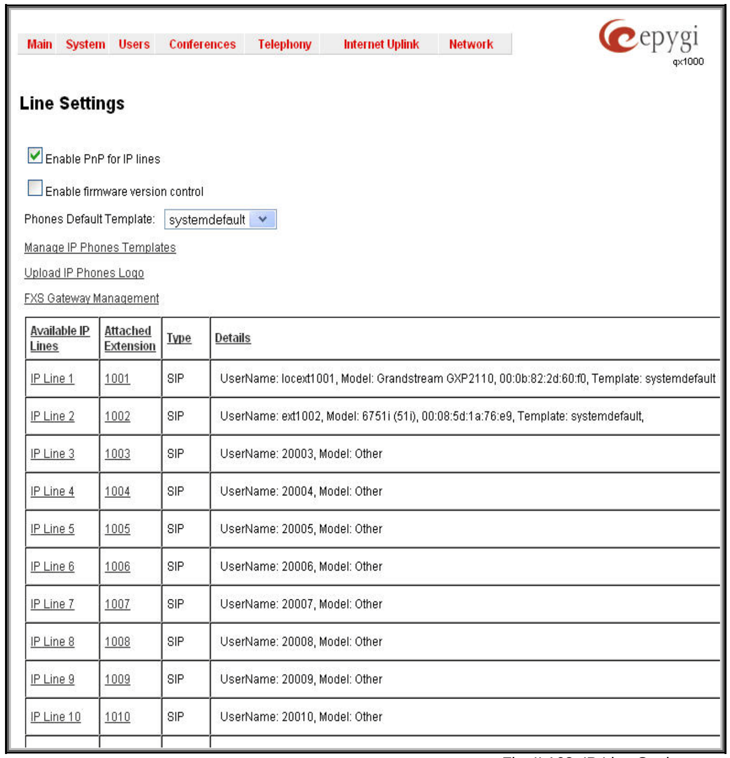


Fig. II-168: IP Line Settings page

Refer to the user's manual of the corresponding SIP phone for instructions on performing a factory reset or reboot on any of the supported phones, what additional configurations are required for a specific SIP phone, and how to manipulate with the GUI.

The **Use Session Timer** enables the SIP session timer for the corresponding IP line. This checkbox enables advanced mechanisms for connection activity checking. This option allows both user agents and proxies to determine if the SIP session is still active.

The **Use Template** drop down list is used select a preconfigured custom template for the IP phone. When the "Use default" is selected in this drop down list, the template selected on the **IP Line Settings** page will be used (see above).

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

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

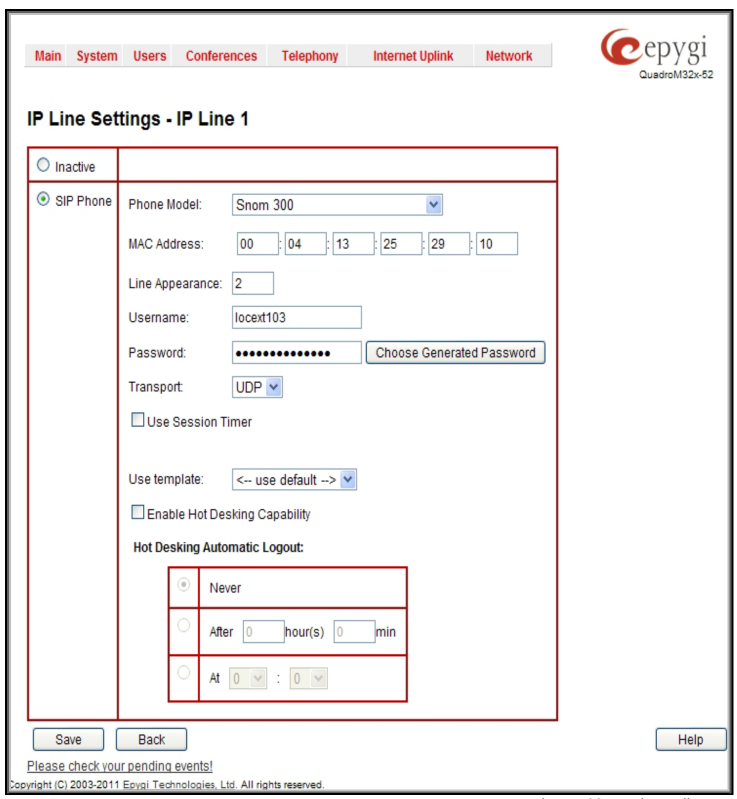


Fig. II-169: IP Line Edit page

The following options are available:

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

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

Please Note: This link only works from the LAN side of the QX1000, i.e. when the QX1000’s GUI is accessed from a PC located in the QX1000’s LAN. If you wish to connect the SIP phone’s GUI through the WAN, an appropriate **Incoming Traffic/Port Forwarding** Filtering Rules should be added on the QX1000.

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

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

Supported SIP Phones

Below is the list of IP phones supported by QX1000 and officially compatible with it. The **Plug-and-Play (PnP)** feature is working for all IP phones listed below, while **Firmware Version Control (FVC)** feature is working only for those phones which have a corresponding notice.

- snom 300 (also supports FVC)
- snom 320 (also supports FVC)
- snom 360 (also supports FVC)
- snom 710 (also supports FVC)
- snom 720 (also supports FVC)
- snom 760 (also supports FVC)
- snom 370 (also supports FVC)
- snom 820 (also supports FVC)
- snom 821 (also supports FVC)
- snom 870 (also supports FVC)
- snom m9
- snom MeetingPoint (also supports FVC)
- Aastra 6751i (also supports FVC)
- Aastra 6753i (also supports FVC)
- Aastra 6755i (also supports FVC)
- Aastra 6757i (also supports FVC)
- Aastra 480i (also supports FVC
- Aastra 480iCT
- Aastra 6730i (also supports FVC)
- Aastra 6731i (also supports FVC)
- Aastra 6739i
- Aastra 6757iCT
- Aastra 9112i (also supports FVC)
- Aastra 9133i (also supports FVC)
- Aastra 9143i(33i)(also supports FVC)
- Aastra 9480i(35i)(also supports FVC)
- Aastra 9480iCT
- Polycom SoundPoint IP 450SIP
- Polycom SoundPoint IP 501SIP
- Polycom SoundPoint IP 550SIP
- Polycom SoundPoint IP 601SIP
- Polycom SoundPoint IP 650SIP
- Polycom SoundStation IP 6000
- Polycom VVX 300/310
- Polycom VVX 400/410
- Grandstream BT200
- Grandstream GXP1400
- Grandstream GXP1405
- Grandstream GXP1450
- Grandstream GXP2000
- Grandstream GXP2100
- Grandstream GXP2110
- Grandstream GXP2120
- Grandstream GXP2124
- Grandstream GXV3140
- Grandstream GXV3175
- Linksys SPA921
- Linksys SPA922
- Linksys SPA941
- Linksys SPA942
- Yealink SIP-T20P
- Yealink SIP-T22P
- Yealink SIP-T26P
- Yealink SIP-T28P
- Yealink SIP-T32G
- Yealink SIP-T38G
- Yealink VP-530
- AudioCodes 310HD
- AudioCodes 320HD
- Panasonic KX-UT136-B
- Panasonic KX-UT123-B
- Panasonic KX-UT123NE-B
- Panasonic KX-TGP550T04
- Alcatel Temporis IP200
- Alcatel Temporis IP600
- Alcatel Temporis IP800

Programmable Keys Configuration

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

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

- **Watch Ext. #** - watch the extension on the QX1000 and a possibility to pickup the call addressed to that extension.
- **Park Answer Ext #** (on the phone can be visible as PkA Ext. #, PrkA Ext. #, PrkAn Ext. # or PrkAns Ext. #) - watch the calls parked to the corresponding extensions and a possibility to retrieve the calls parked to that extension.

This list also contains a number of PBX services available on the QX1000 and accessible with the * key combination (see QX1000's Feature Codes). When configured from this page, the key combinations become transparent for the IP phones too.

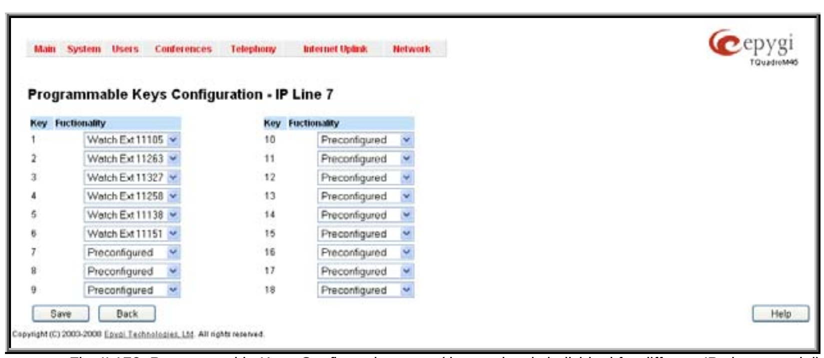


Fig. II-170: Programmable Keys Configuration page (the preview is individual for different IP phone model)

- **Vmail** - accesses the voice mailbox of the extension to which the receptionist IP line is attached to.
- **DND** - enables the Do Not Disturb service on the extension to which the receptionist IP line is attached to.

- **CallFwd** - accessed Forwarding Management of the extension to which the receptionist IP line is attached to.
- **AutoReDI** - auto redials the last dialed call.
- **CallBack** - calls back to the last caller.
- **LineInfo** - gets the IP line information from the QX1000.
- **CallBlk** - blocks the last caller.
- **Record** – records the call (in case if the manual call recording is allowed for the call, configured from Call Recording Settings.
- **ACD Login/Logout** – allows the corresponding ACD agent to login to all groups it is involved in, if previously logged in, to log out from those groups. For details on ACD functionality, see ACD Management.

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

Manage IP Phones Templates

The **Manage IP Phone Templates** page is used to create custom templates for the IP Phones. The templates contain a set of configuration settings that are uploaded to the IP phone once it is registered on the QX1000. With the custom templates the most popular configuration settings may be adjusted accordingly. The saved custom templates can be then configured from the **Edit IP Line Settings** page to be used on the particular IP phone.

The **Manage IP Phone Templates** page consists of a table where the available IP phone templates are listed. The **systemdefault** template in this table indicates the QX1000 default template for all IP phones. This template cannot be edited or deleted.

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

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

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

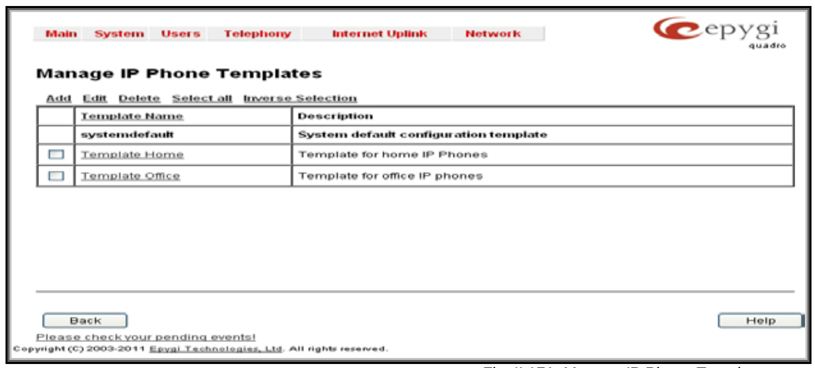


Fig. II-171: Manage IP Phone Templates page

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

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

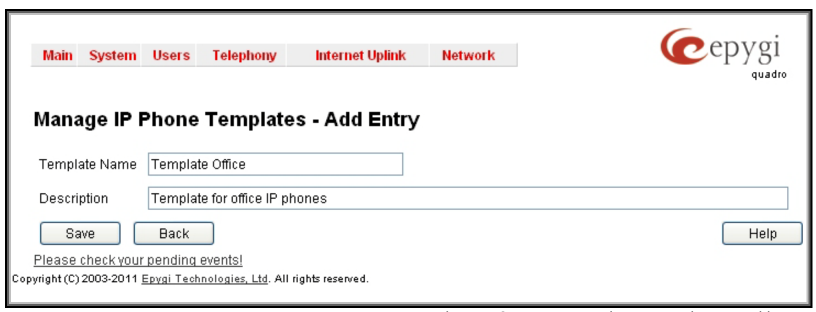


Fig. II-172: Manage IP Phone Templates – Add Entry

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

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

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

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

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

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

- **Dial-Plan String** – indicates a dial plan string used to match dialed digits from the handset to the certain actions, e.g. dialing.
  Dialog-Info Call Pickup - is used to switch a subscription to the status information of SIP URLs mapped as “Destination/Extension” on the programmable keys.
- **Transfer on Onhook** - is used to switch the call transfer when the handset is placed on hook.
- **Call join on Xfer (2 calls)** - when this option is enabled, you will connect the newly arrived incoming call to the call on hold by pressing Xfer button. When this option is disabled and you press the Xfer button, you will have an option to choose the call on hold to transfer the newly arrived incoming call to, or to dial a new destination manually.

- **Message LED for Dialog State/Missed Calls** – when this option is enabled, the phone will indicate missed calls and changing dialog states using the message LED.

- **Dialtone during Hold** - when this option is enabled and the call is held the caller gets dial tone. Otherwise there will be no dial tone after pressing **Hold**.

- **Do not Disturb** – this selection allows you to manipulate with the IP phone DND service. When the ***72** is selected from this list, the DND service of the IP Phone and the DND service of the QX1000 for the corresponding extension will be activated when enabling the DND service from IP Phone. This option is recommended. When **keyeventF_DND** is selected only DND service of the phone will be activated when enabling the DND.

- **Record Missed Calls** – when this option is selected, the information about the missed calls will be displayed on the IP Phone.

Any parameters not listed above or parameters defined in this page for other IP phone models can be found in the user's manual of the corresponding IP phone.
Please Note: Save changes before moving among the configuration pages.

IP Phones Logo

The **IP Phones Logo** page is used to upload a custom logo for the IP Phones. This page contains only those IP phones for which QX1000 supports the custom logo upload. The uploaded custom logo will be visible on the display of the IP phone.

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

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

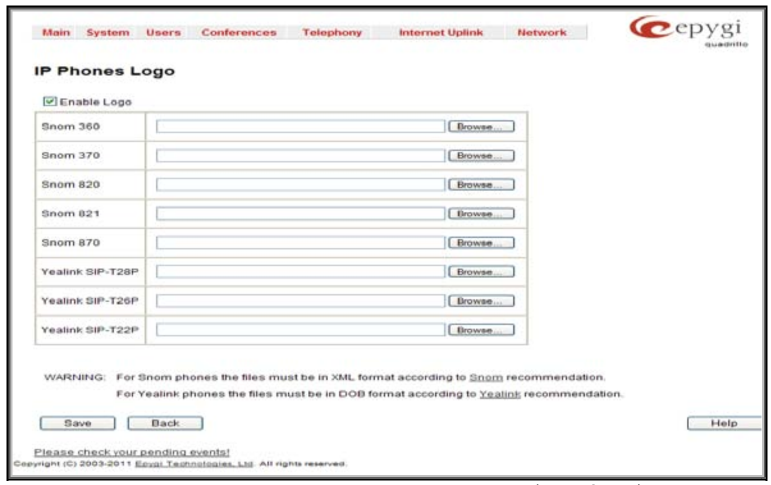


Fig. II-173: IP Phones Logo page

FXS Gateway Management

The QX1000 FXS Gateway is an analogue Gateway that allows connecting analogue phones to a VoIP network. The device can be used with QX1000 to emulate additional FXS ports. Both QX1000 and the FXS Gateway should be located in the same network. QX1000 is connected to the QX1000 FXS gateway through its MAC address.
The **FXS Gateway Management** page is used to define QX1000 FXS Gateway devices in your network that can serve as FXS expansion modules for your QX1000. Additional FXS lines provided by the FXS Gateway can be connected to the IP lines on the QX1000.

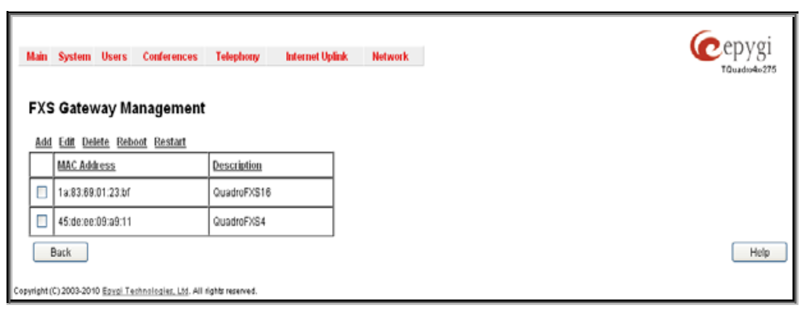


Fig. II-174: FXS Gateway Management page

Add functional button opens **FXS Gateway Management Wizard** where new FXS Gateway should be defined.
The **FXS Gateway Configuration Wizard - FXS Gateway Model** page contains following components:

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

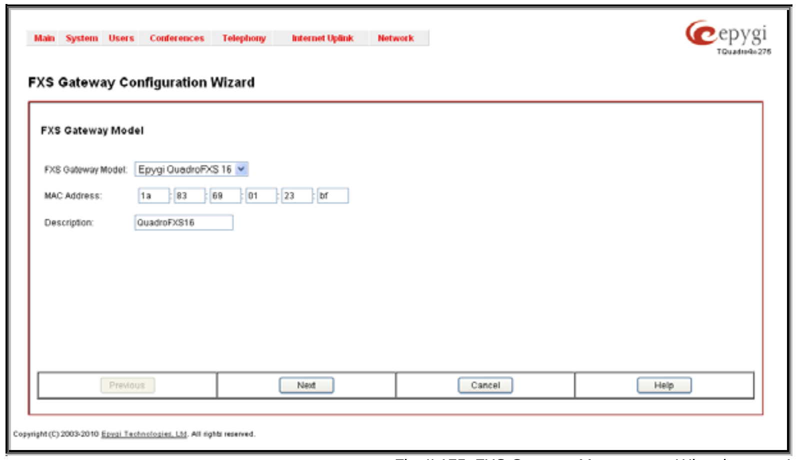


Fig. II-175: FXS Gateway Management Wizard – page 1

The next page of the wizard is **FXS Gateway Configuration Wizard - FXS Gateway Lines**. This page displays a list of FXS lines provided by the FXS Gateway and is used to assign each FXS line to an IP line on the QX1000. System will automatically assign the provided FXS lines to the first available IP lines on the QX1000. You may adjust the configuration from this page.

Please Note: The FXS lines can be assigned only to inactive IP lines on the QX1000. If there are no enough free IP lines available on the QX1000, you should first deactivate the IP line from the Line Settings page to use it in the FXS Gateway Configuration Wizard.

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

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

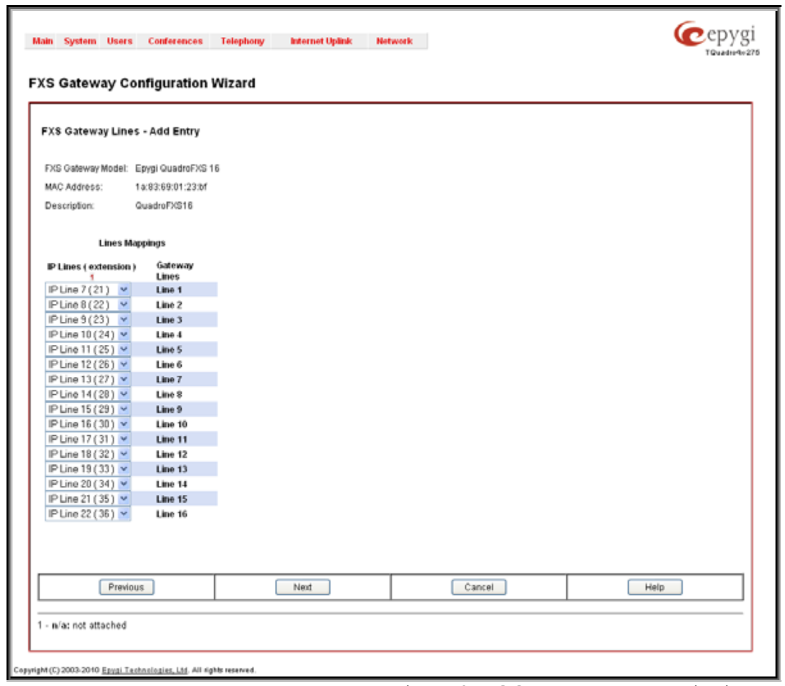


Fig. II-176: FXS Gateway Management Wizard – page 2

Hot Desking

If QX1000 has limited number of IP phones connected and much more users wishing to make and receive calls through the QX1000, some of the connected phones can be announced as public. Public phones have no static owners; they are just connected to the analogue or IP lines. Each user that accesses the public phone should first login with the previously created virtual extension and the corresponding password in order to make the phone assigned to the certain extension. From that point forward and unless the user with log off the phone, he may place and receive calls and use all the supplementary PBX services of the QX1000.

The **Hot Desking** feature is used to organize the user login/logout on the public phones. Each user should have a virtual extension configured in the Extensions Management table. The virtual extensions can be configured as needed to use all the available supplementary PBX features when the user will log in from the phone with that extension. The **Hot Desking** option should be enabled on the corresponding IP line from the Line Settings page.
To login to the phone, use the *78 feature code (for more details see Feature Codes chapter). You will be prompted for the extension and the password. When you login to the phone with your extension, the phone becomes a fully featured phone connected to the QX1000. You may place and received calls with the SIP address configured in the Extensions Management page, use Voice Mail services, etc. When you have finished using the phone, logout with the *78 feature code. From that moment forward, your extension becomes again virtual and is not connected to any analogue or IP line but it still can handle calls (using Call Forwarding, Many Extension Ringing, Hunt Grouping, etc. services) and voice mails according to the supplementary service configured on that virtual extension. The phone becomes no more assigned to your extension and is now available for other users to login and use it.

FXO Settings

The **FXO Settings** are used to configure the FXO support that allows QX1000 to connect to other PBXs or analog telephone lines.

The QX1000 has no own FXO lines, only shared FXO lines are displayed in this page, if available. The shared FXO lines can be edited from FXO setting page. Any changes applied in that page will be automatically reflected on the FXO gateway(s) that share its FXO lines.

The **FXO Settings** allows you to limit incoming or outgoing calls for the selected FXO line if required. Depending on configuration of the FXO gateways, multiple shared FXO ports from one or more FXO gateways may be available on the QX1000, thus giving you the option to use them simultaneously.

The administrator may assign a default recipient for each FXO line where calls from the Central Office (PSTN) will be routed. The assigned recipients become the QX1000 “default users”. If the QX1000 Auto Attendant has been selected as a “default user”, a caller from the PSTN needs to go through the attendant menu to reach the desired extension.

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

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

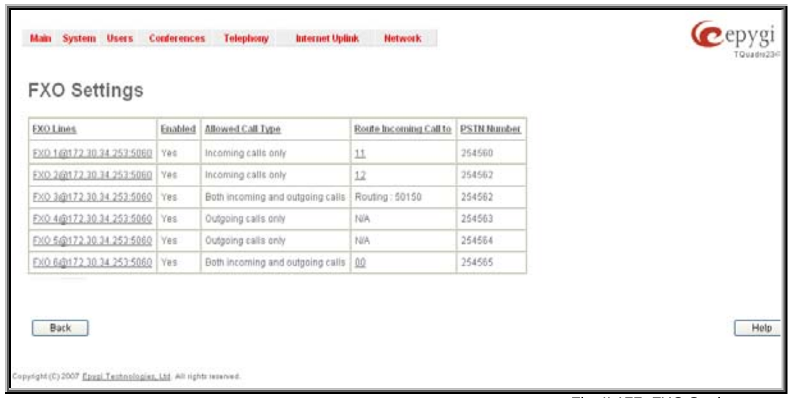


Fig. II-177: FXO Settings page

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

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

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

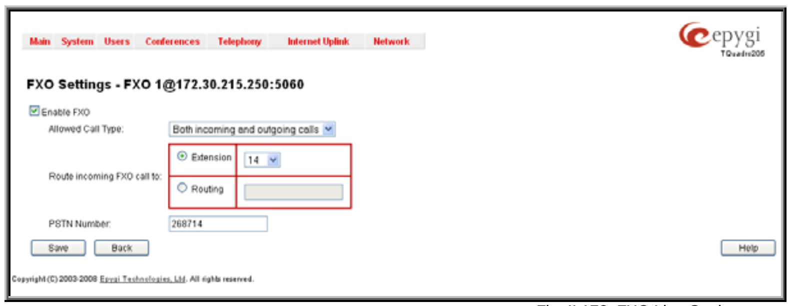


Fig. II-178: FXO Line Settings page

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

- **Extension** – this selection allows you to choose the local PBX user or auto attendant extension to forward calls. If an inactive extension is chosen from this list, the voice mail system will answer the call addressed to the corresponding FXO line. If the Auto Attendant extension is chosen, it will become the “default user” for the corresponding FXO line on the QX1000.
- **Routing** – this selection allows you to forward the incoming calls to the destination defined through Call Routing. This selection requires you to enter a routing pattern to the corresponding field. Based on the registered PSTN users, the caller will be able to reach the destination according to configurations in Call Routing Table.

By choosing a destination, the QX1000 administrator virtually assigns a default number that will start ringing when a call is initiated to the QX1000’s PSTN number.

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

Alternative AC Termination Mode appears if the local country (Germany, Israel, France, etc.) selected for QX1000 has two COs that use different types of AC termination. Contact your CO to learn about your AC termination mode. Selecting the checkbox may help if the voice quality over FXO is poor or an echo is noticed.

To modify the FXO Settings

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

ISDN Settings

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

The **ISDN service** allows QX1000 act as a user or as a network. If connected to a private PBX, the QX1000 should be configured in the network mode. If an ISDN trunk from the CO (Central Office) is connected to the QX1000, it should be configured as a user. QX1000 supports the MSN (Multiple Subscriber Number) service, i.e., it can be subscribed to multiple numbers from the CO, and two simultaneous calls can take place at a time.

The QX1000 has no own ISDN trunks, only shared ISDN trunks are displayed in this page, if available. The shared trunks can be edited from ISDN setting page. Any changes applied in that page will be automatically reflected on the ISDN gateway(s) that share its ISDN trunks.

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

The **Trunk Settings** table lists the available ISDN trunks on the QX1000 and their settings (trunk name and interface types).

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

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

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

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

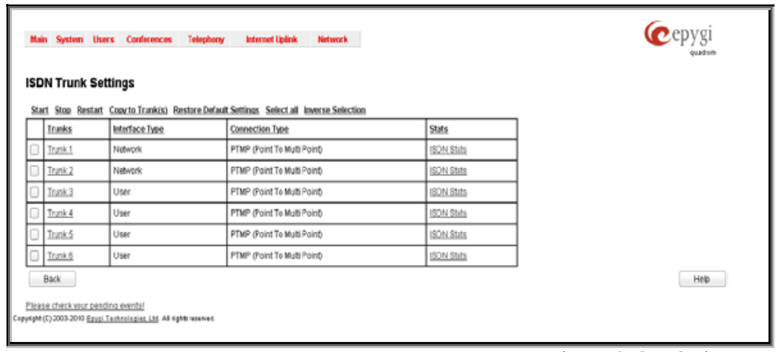


Fig. II-179: ISDN Settings page

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

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

The **Interface Type** drop down list allows you to select between the User and the Network interfaces. If the ISDN port of the QX1000 is connected to the CO then **User** interface type should be selected. If the ISDN port of the QX1000 is connected to the PBX then **Network** interface type should be selected (in that case QX1000 acts as a CO for that PBX).

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

- **PTP (Point to Point)**
  In case of connection to the CO (**User** interface type is selected on QX1000) choose this option if only QX1000 is connected to the ISDN trunk from CO (no other ISDN devices are connected to the particular ISDN trunk from CO besides the QX1000).
  In case of connection to the PBX (**Network** interface type is selected on QX1000) choose this option if only the PBX is connected to the ISDN trunk from the QX1000 (no other ISDN devices are connected to the particular ISDN trunk from the QX1000).
  In both cases, with this selection, QX1000 sets the TEI to manually mode assigning the default value of 0. If needed, that value can be changed later in the **Advanced Settings** page of ISDN Wizard.

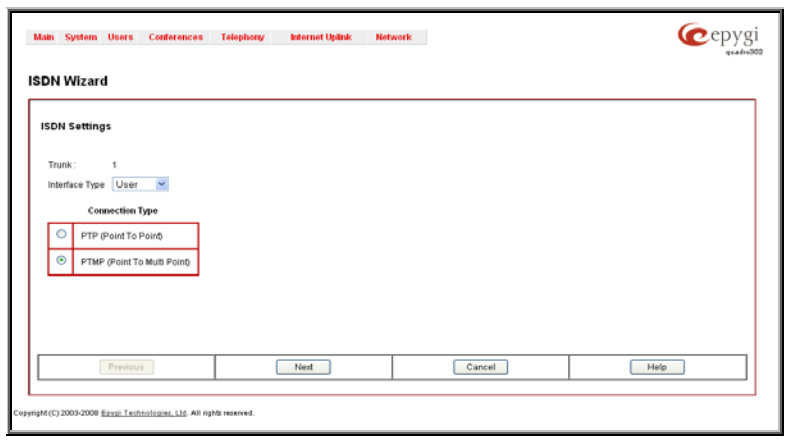


Fig. II-180: ISDN Wizard – ISDN Settings

- **PTMP (Point to Multi Point)**
  In case of connection to the CO (**User** interface type is selected on the QX1000) choose this option if there can be other devices connected to the same ISDN trunk from CO except the QX1000.
  In case of connection to PBX (**Network** interface type is selected on the QX1000) choose this option if there can be other devices connected to the same ISDN trunk from QX1000 except for the PBX.
  In both cases, with this selection QX1000 sets the TEI to automatic mode.

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

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

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

For MSN service enabled, the **Routing Settings** page is used to assign MSN numbers to the certain destinations on the QX1000. The MSN number can be assigned to the QX1000's extensions, to the Auto Attendant, or to the routing agent. The destination selected from this page will ring upon incoming call to the corresponding MSN number comes in.

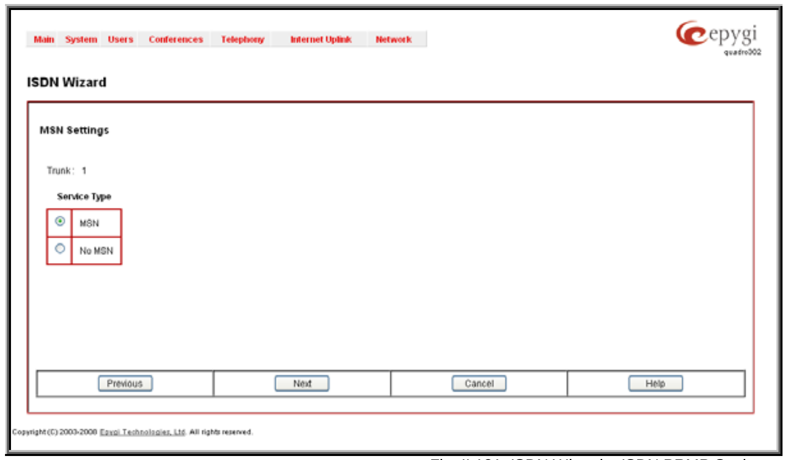


Fig. II-181: ISDN Wizard – ISDN PRMP Settings

The fields in the **MSN Number** column require the MSN numbers allocated to the QX1000.

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

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

Selecting the **Use Default outgoing Caller ID** allows you to overwrite the source caller information with the one specified in the **Default outgoing Caller ID** field when placing outgoing calls toward the CO. The **Default outgoing Caller ID** field requires the caller ID for the outgoing calls from the QX1000 through the ISDN trunk. That number should be registered at the CO and can be one of the MSNs provided by the CO. If this checkbox is enabled but no value is defined in the **Default outgoing Caller ID**, empty caller information will be sent to the CO. If this checkbox is disabled, the source caller information will be forwarded to the CO.

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

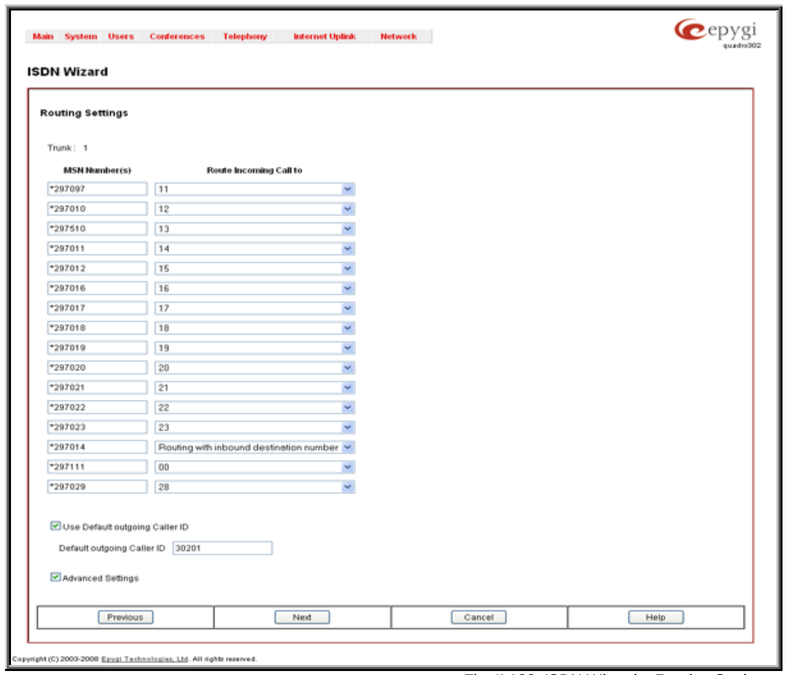


Fig. II-182: ISDN Wizard – Routing Settings

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

ISDN L2 Timers:

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

ISDN L3 Timers:

- The **T302 Timer** text field requires the value for the T302 timer in milliseconds (digit values from 0 to 15000). It indicates that the time frame system is waiting for a digit to be dialed. When the timer expires, it initiates the call.
- **T309 Timer** requires the value for the T309 timer in milliseconds (numeric values from 0 to 90000). It is responsible for call steadiness during link disconnection within the period equal to this timer value. If the value in this field is zero (0), the T309 timer will be disabled.
- **T310 Timer** requires the value for the T310 timer in milliseconds (numeric values from 1000 to 120000). It is responsible for the outgoing call steadiness when CALL PROCEEDING is already received from the destination but call confirmation (ALERT, CONNECT, DISC or PROGRESS) has not yet arrived.
- **Alert Guard Timeout** requires the value for the Alert Guard Timer in milliseconds (numeric values from 0 to 500) between CALL PROC and ALERT messages. Alert Guard Timer it is used when QX1000 is connected to a slow ISDN-PBX.
  Recommended values are:
  - fast connection (0ms);
  - normal (150ms), default;
  - slow ISDN-PBX (350ms);
  - very slow ISDN-PBX (500ms).

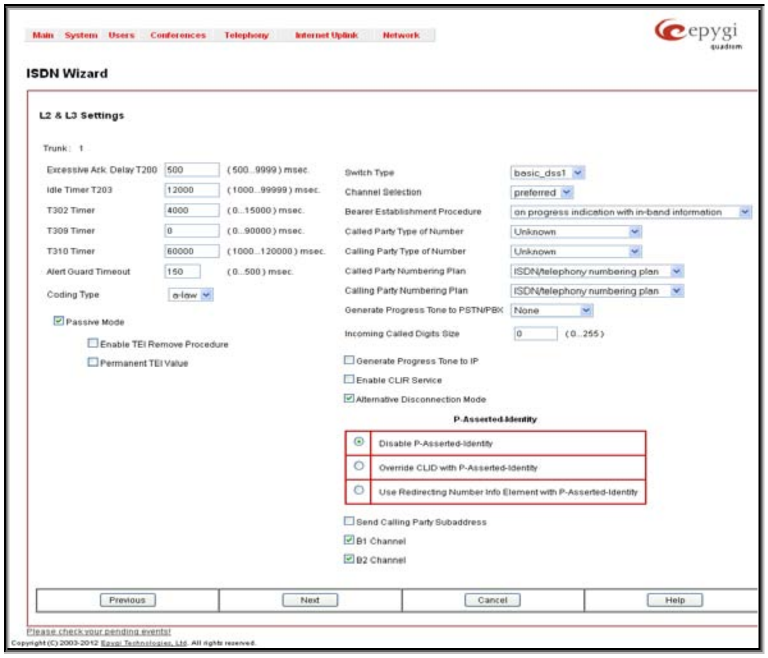


Fig. II-183: ISDN Wizard – l2&L3 Settings

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

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

The **Passive Mode** checkbox is used to leave the ISDN Layer1 connection in the Slave mode. When this checkbox is selected, Layer1 remains idle when calls are not available. When this checkbox is not selected, QX1000 keeps its Layer1 always active. This checkbox enables the **Enable TEI Remove Procedure** and **Permanent TEI Value** checkboxes. With the **Enable TEI Remove Procedure** checkbox is selected, the trunk will lose the assigned TEI when entering into passive mode on the Layer 2. With the **Permanent TEI Value** checkbox is selected, the trunk will keep the assigned TEI when entering into passive mode on the Layer 2 or when QX1000 detected ISDN link DOWN signal from carrier.

These checkboxes are present only for connection types different from **PTP (Point to Point)** selected on the first page of **ISDN Wizard**. In case if **PTP (Point to Point)** connection type is selected on the first page of the ISDN Wizard, these two checkboxes are replaced with a **TEI Address** text field that requires the channel number (digit values from 0 to 63) for connection establishment between the CO and the ISDN client.

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

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

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

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

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

The **Incoming Called Digits Size** text field indicates the number of received digits (in a range from 0 to 255) required to establish a call. When this field has a “0” value, the system uses either the timeout defined in the T302 field or the **Sending Complete Information element** messages to establish a call. Independent on the value in this field, **Sending Complete Information element** and the pound sign always result in call establishment.
The **Generate Progress tone on IP** checkbox selection will generate the progress tone to IP.
When **Generate Progress Tone to PSTN/PBX** checkbox is selected, QX1000 generates ring tones to callers during ISDN call dialing. This feature is mainly applicable to 2-stage dialing mode.

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

When the **Alternative Disconnection Mode** checkbox is not selected, QX1000 will disconnect the call as soon as the disconnect message has been received from the peer. When the checkbox is selected, QX1000’s user may hear a busy tone when peer has been disconnected.

P-Asserted-Identity:

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

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

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

When the **Send Calling Party Subaddress** checkbox is selected, QX1000 will send the extension number as subaddress and the value defined in the **Default outgoing Caller ID** field as caller ID on the outgoing call. When this checkbox is disabled, no subaddress information will be sent and the caller ID will be defined according to the selection of the **Use Default Outgoing Caller ID** checkbox (see above). Caller ID information, along with the Subaddress, can be displayed on the phone display depending on the phone and PBX settings and capabilities.

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

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

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

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

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

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

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

HDLC Packet Abort displays the number of received aborted packets.

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

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

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

TEI value shows the actual TEI value.

L2 State shows the actual BRI L2 state.

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

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

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

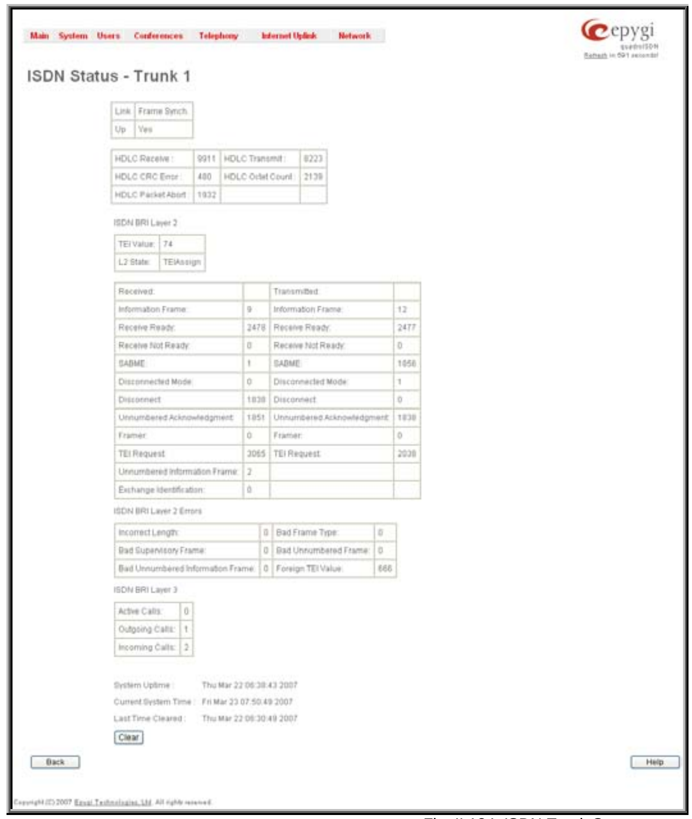


Fig. II-184: ISDN Trunk Status page

SABME shows the number of packets upon connection establishment.

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

Disconnect shows the number of packets upon connection termination.

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

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

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

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

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

ISDN BRI Layer 2 Errors statistics:

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

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

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

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

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

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

ISDN BRI Layer 3 statistics:

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

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

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

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

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

External PSTN Gateways

The **External PSTN Gateways** page allows QX1000 to use the PSTN lines (FXO lines and/or ISDN trunks) on other QX1000s. This provides the option to call not only through local PSTN lines but also through available shared FXO or ISDN lines in the network of QX1000s. When the sharing mode is enabled and one QX1000 is configured to use the shared PSTN lines of another QX1000, the corresponding routing patterns will automatically be created in the Call Routing Tables (see Call Routing) on both QX1000s. This will allow PSTN call routing between the two QX1000s.

The **Use PSTN lines of the other device** checkbox is used to enable QX1000 to use the shared PSTN lines on a remote device. This selection requires you to configure the Authorization Parameters. Use the same named link to access the **Authorization Parameters** table.

Fig. II-185: External PSTN Gateways page

The **Authorization Parameters** page is used to create accounts for the remote QX1000s allowing them to connect the QX1000 and share the available PSTN lines. The table on this page lists all registered accounts and account information. It will show the corresponding authentication parameters (username and password) and date/time of the last registration.

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

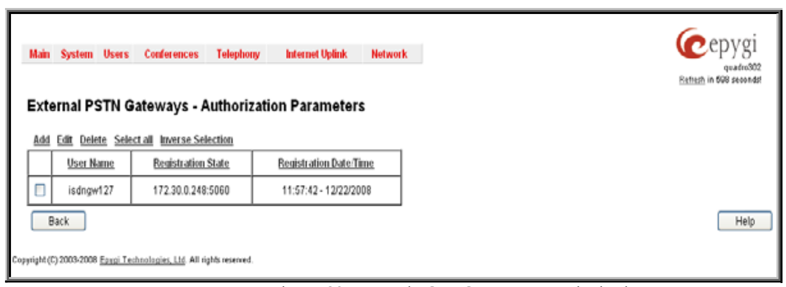


Fig. II-186: External PSTN Gateways – Authorization Parameters page

<u>To use the shared remote PSTN lines</u>

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

Gain Control

The **Gain Control** settings are used to define **Recording Gain** and **Playback Gain** drop down lists. They contain the allowed gain values, which can be set by the administrator.

For Voice Mail:

Recording Gain defines the volume of the phone microphone upon playing voice mails or system messages.

Playback Gain defines the phone speaker volume upon playing voice mails or system messages.

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

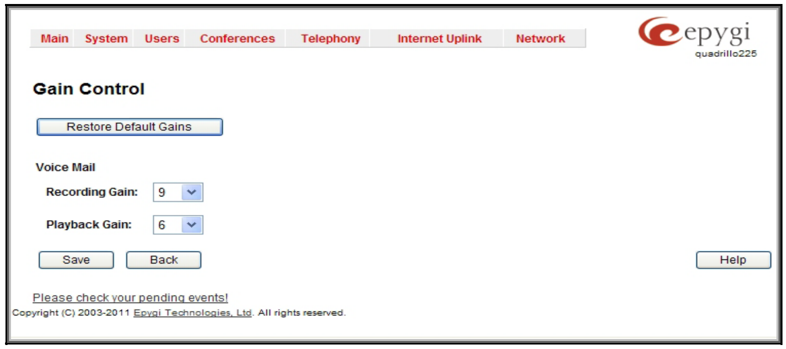


Fig. II-187: Gain Control page

SIP Tunnel Settings

The **SIP Tunneling** service is used to build a tunnel between QX1000s and to use that tunnel for routing the SIP calls through the remote QX1000s. When this service is enabled, slave QX1000s should be registered on the master QX1000 with the corresponding username/password. With the appropriate configuration done on the master QX1000, the master device can use the slave QX1000s for routing the SIP calls through them and accessing peers located behind the slave QX1000 or recognized by it. This enables the master QX1000 to locate the slave, even when the network settings, like IP address, SIP port and other settings are changed on the slave QX1000.

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

Optionally, a SIP tunnel can be mutually established on two QX1000s allowing to route SIP calls back and forth. A QX1000 can be at the same time configured both as a slave and as a master to the same remote device, i.e. the slave QX1000 can act as a master for the master device it is registered on. For example, the QX1000_1 can act as a slave for the QX1000_2. In its turn, the QX1000_2 can act as a slave for the QX1000_1. With this configuration and the corresponding routing rules added in the Call Routing table on both devices, the SIP calls will be routed from QX1000_1 to QX1000_2 and vice versa.

The **SIP Tunnel Settings** page is used to enable the QX1000 as a slave or master device for SIP tunneling. The page consists of the following components:

The **Enable Tunnels to Slave Devices** checkbox enables the QX1000 as a master device and allows you to configure the SIP tunnels to the slave QX1000s. When this checkbox is enabled the **Tunnels to Slave Devices** table needs to be configured.

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

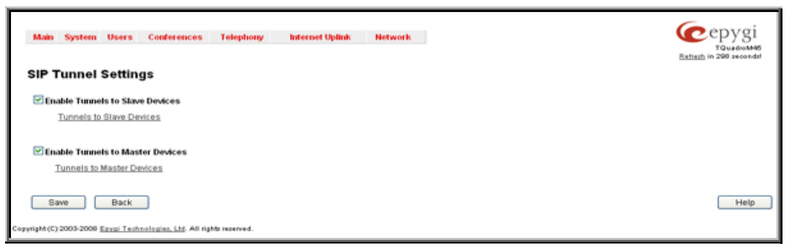


Fig. II-188: SIP Tunnel Settings page

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

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

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

The **SIP Tunnel Name** text field requires the tunnel name for the corresponding connection. System suggests you to start the SIP tunnel name with the “SIP_Tunnel_” words, according to the automatic prefix used for the SIP tunnels on the QX1000, however this is not mandatory.

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

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

Please Note: The **User Name** and **Password** should match both on master and slave QX1000s for the successful SIP tunnel establishment.

The **Symmetric NAT** checkbox should be selected when the slave QX1000 is located behind the symmetrical NAT.

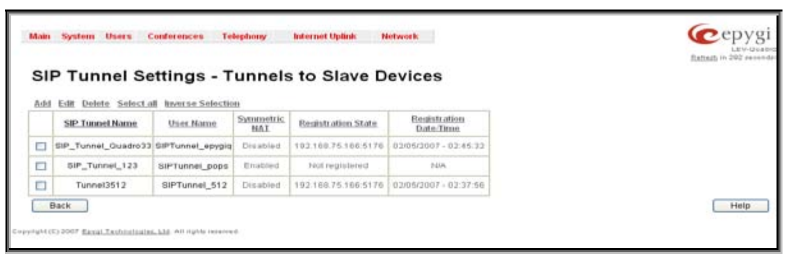


Fig. II-189: SIP Tunnel Settings – Tunnels to Slave Devices page

Fig. II-190: SIP Tunnel Settings – Tunnels to Slave Devices – Add Entry page

The **Enable Tunnels to Master Devices** checkbox enables the QX1000 as a slave device and allows connecting to the master QX1000 via SIP tunnel. When this checkbox is enabled the **Tunnels to Master Devices** table needs to be configured.

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

Fig. II-191: SIP Tunnel Settings – Tunnels to Master Devices page

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

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

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

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

The **Tunnel Name** text field requires the SIP tunnel name for the corresponding connection. System suggests you to start the SIP tunnel name with the "SIP_Tunnel_" words, according to the automatic prefix used for the SIP tunnels on the QX1000, however this is not mandatory.

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

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

Please Note: The **User Name** and **Password** should match both on master and slave QX1000s for the successful SIP tunnel establishment.

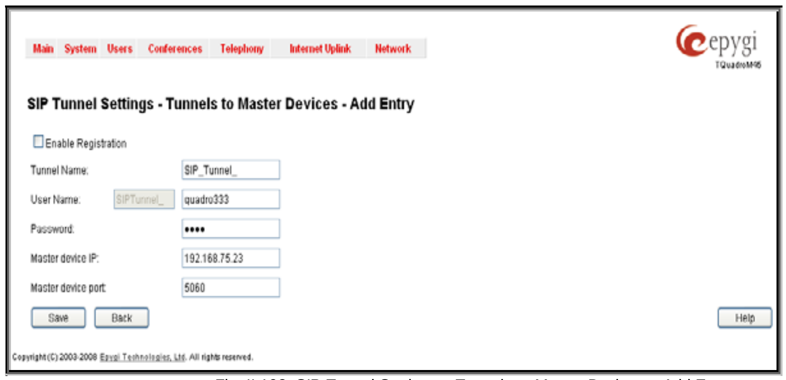


Fig. II-192: SIP Tunnel Settings – Tunnels to Master Devices – Add Entry page

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

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

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

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

Call Routing

The **Call Routing** service simplifies the calling procedure for QX1000 users, i.e., different types of calls (internal, SIP, PSTN or IP-PSTN) can be placed in the same way. SIP registration is not needed for extensions to make routing calls.

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

- When the **Route all incoming SIP calls to Call Routing** checkbox is disabled, for all incoming SIP calls QX1000 will first search the incoming SIP address in the Extensions Management table. If found, the incoming SIP call will ring on the corresponding extension. If not found, QX1000 will look for a matching routing rule in Call Routing table.
- When the **Route all incoming SIP calls to Call Routing** checkbox is enabled, for all incoming SIP calls QX1000 will directly look for a matching routing rule in Call Routing table and will ignore the possible matches in the Extensions Management table.

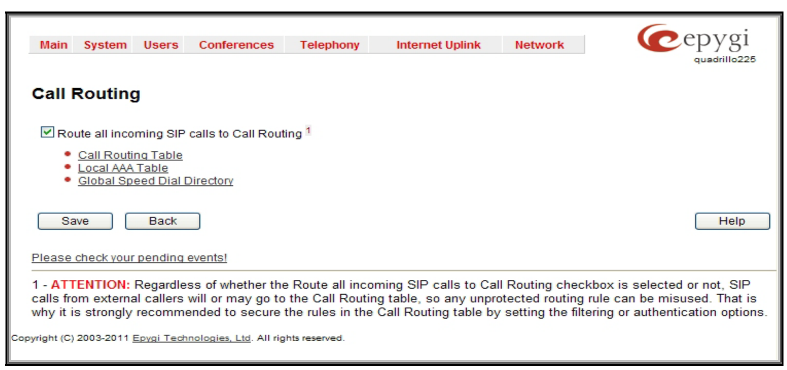


Fig. II-193: Call Routing page

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

- The **Call Routing Table** link leads to the **Call Routing** table where routing patterns may be manually defined.
- The Local AAA Table link leads to the page where local AAA (Authentication, Authorization, and Accounting) database can be managed.
- The Global Speed Dial Directory link leads to the page where global speed dialing rules may be uploaded in a file.

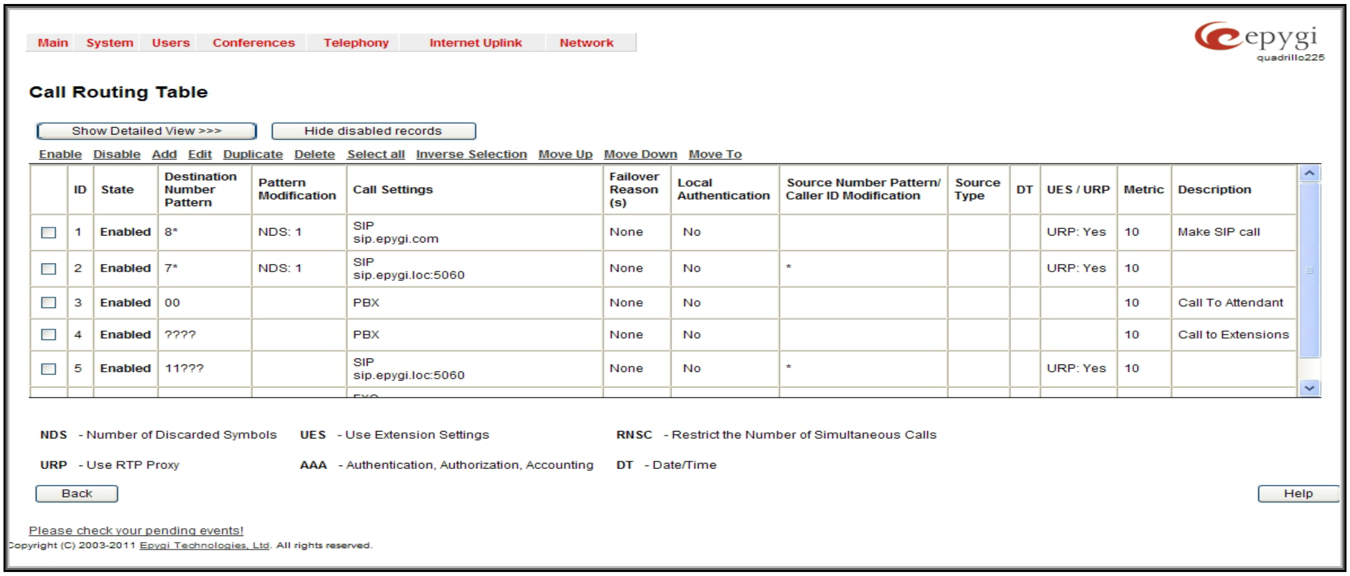


Fig. II-194: Call Routing table – brief preview

Defining patterns in the **Call Routing Table** avoids registering QX1000 at the routing management server and gives you an option to establish a direct connection to the destination or to use a SIP server for call routing.

The **Call Routing Table** lists manually defined routing patterns along with their parameters (pattern number, state, routing and source caller settings, RTP Proxy and Date/Time period settings, metric and description), as well as automatically created and undeletable patterns created from the System Configuration Wizard. The alternating **Show Detailed View** and **Show Brief View** buttons are used to display entries in the Call Routing table in detailed and brief views correspondingly. The brief view displays the most important settings of the routing rules. The detailed view displays all settings of the routing rules as they are configured in the Call Routing Wizard.

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

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

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

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

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

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

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

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

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

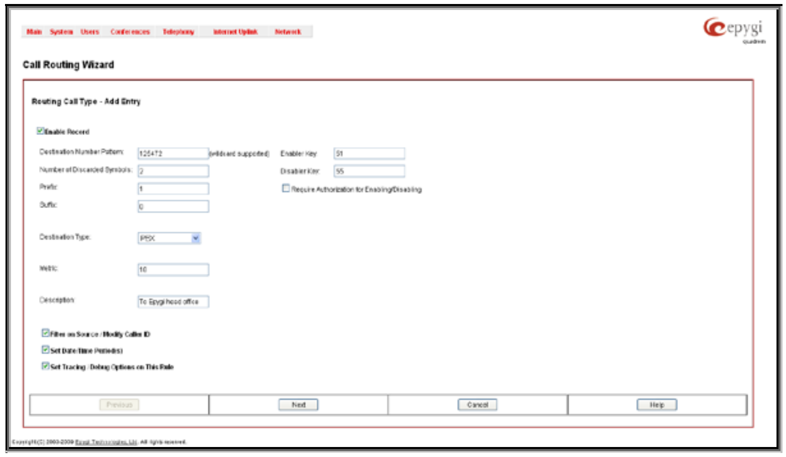


Fig. II-195: Call Routing Wizard - page 1

Number of Discarded Symbols requires the number of symbols that should be discarded from the beginning of the routing pattern. The field should be empty if digits do not need to be discarded. Only numeric values are allowed for this field, otherwise the error message “Error: Number of Discarded Symbols is incorrect - digits allowed only” will appear.

Prefix requires entering the symbols (letters, digits and any characters supported in the SIP username) that will be placed in front of the routing pattern instead of the discarded digits. The following tags can be used for this field:

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

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

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

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

- PBX - local calls to QX1000’s extensions
- PBX-Voicemail **-** calls directly to the voice mailbox of the local PBX extension
- PBX-Intercom - local calls to PBX extensions with the request of Intercom service (see Manual III – Extension Users Guide)
- SIP – calls through a SIP server
- SIP_Tunnel – calls through a SIP tunnels established (see SIP Tunnel Settings)
- IP-PSTN – calls through the IP-PSTN provider to the remote PSTN global telephone network

Metric allows entering a rating for the selected route in a range from 0 to 20. If a value is not inserted into this field, 10 will be used as the default. If two route entries match a user’s dial string, the route with the lower metric will be chosen.

The **Description** text field requires an optional description of the routing pattern.

The **Filter on Source / Modify Caller ID** checkbox selection allows limiting the functionality of the current route to be used by the defined caller(s) only. If this checkbox is enabled, source caller information (**Source Number Pattern**, **Source Type, Source Host**, etc.) will be required later in the **Call Routing Wizard**. This option is enabled by default.

The **Set Date / Time Period(s)** checkbox selection allows you to define a validity period(s) for current routing patterns to take place and to define pattern date/time rules. When this checkbox is enabled, the **Call Routing Wizard** - Page 5 will be displayed.
Set Tracing / Debug Options on This Rule checkbox is used to switch events notification on the certain execution results of the corresponding routing rule. When this checkbox is enabled, the **Call Routing Wizard** - Page 6 will be displayed.

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

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

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

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

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

SIP Tunnel drop-down list appears only when the "SIP_Tunnel" **Destination Type** is selected on the previous page. The list is used to select the particular SIP tunnel to route the calls through the corresponding QX1000.

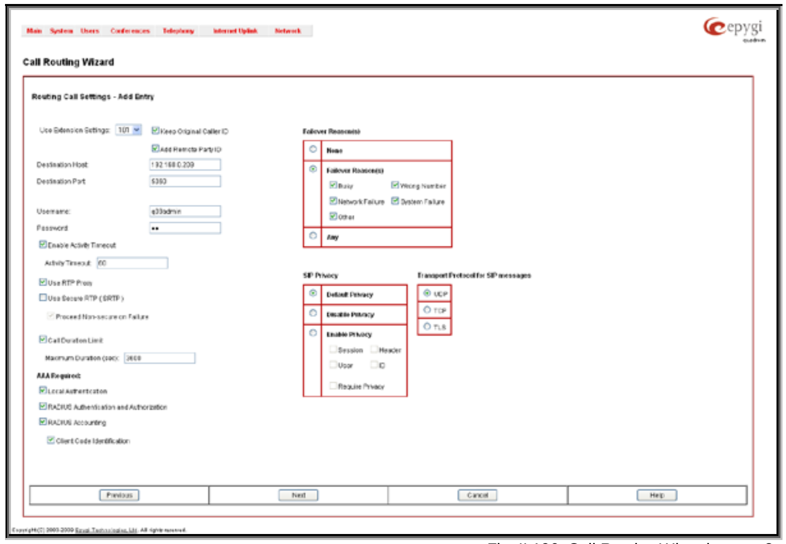


Fig. II-196: Call Routing Wizard - page 2

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

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

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

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

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

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

The **Use RTP Proxy** checkbox is available for SIP, PBX and IP-PSTN destination types and is applicable when a route is used for calls through QX1000 between peers that are both located outside the QX1000. When this checkbox is selected, RTP streams between external users will be routed through QX1000. When the checkbox is not selected, RTP packets will move directly between peers.

The **Callect Call** checkbox is available only for **E1/T1** destination type and is used when it is simply preferable for the called phone to pay for the call. This service is applicabe only if the **Collect Call** checkbox is enabled on both calling and called party's IP PBXs.

The **Call Duration Limit** checkbox is available for SIP, IP-PSTN and PSTN destination types and is used to limit the duration of the call placed with the selected routing rule. If this checkbox is not selected, the call duration will be unlimited. This checkbox selection enables the **Maximum Duration** text field where the maximum duration of the call (in seconds) should be defined. Once the call duration reaches the value defined here, the call will be disconnected without prior notice.

The **Play audible signal before Intercom activation** checkbox is appeared only if **PBX Intercom** is selected as **Destination Type** (see Manual III – Extension User's Guide-Intercom Service).

The **AAA Required** checkboxes are used to choose one or more of the following Authentication, Authorization, and Accounting (AAA) settings:

- **Local Authentication** – with this checkbox selected, callers will need to pass authentication through the Local AAA Table when dialing the current pattern.
- **RADIUS Authentication and Authorization** – this checkbox is present when a RADIUS client is enabled. With this checkbox selected, callers will need to pass the authentication through RADIUS server (see above) when dialing the current pattern.
- The **RADIUS Accounting** checkbox is accessible when the RADIUS Client is enabled. With this checkbox selected, no authentication will take place, but CDRs (call detail reports) of the calls made through this routing record will be sent to the RADIUS server. This checkbox selection enables the **Client Code Identification** checkbox. If the authentication is configured based on the caller's address, callers will pass the authentication automatically; otherwise they will be required to identify themselves by a username and a password.
- The **Client Code Identification** checkbox selection activates the code identification feature: a caller, after dialing the destination phone number, may optionally enter "*" and then an **Identity Code**. An **Identity Code** is an arbitrary digit string entered by the user to identify a specific call or call group. The **Identity Code** is sent with CDR to the RADIUS server and might be used by a billing program for grouping the calls having the same Identity Code.

Attention: It is highly recommended to secure PSTN and IP-PSTN routing rules by selecting **AAA Required** options. Unsecured routing rules may cause unexpected expenses.

The **Check with 3PCC** checkbox is used to request a 3PCC approval before placing a call with the specific routing rule. When this checkbox is selected and the corresponding routing rule is used to place a call, QX1000 sends a request to the call controlling application for the managing person to accept or reject the specific call (it can be a popup window or any other type of dialog box, depending on the call controlling application). If the request is accepted, the call will be placed. Otherwise, if the request is rejected, the call will be skipped. In case of no feedback from the call controlling application, the call will be accepted after a timeout defined in the configuration of the call controlling application.

The **Failover Reason(s)** radio buttons indicate whether the system should use the next matching pattern if call setup with the current routing rule fails and allows choosing the reasons to be considered as a failover.

- **None** - indicates that matching patterns should not be used regardless of the failover reason.
- **Failover Reason(s)** - indicates possible failure reasons. Failure reasons vary depending on the destination type selected on the previous page. If the call cannot be established due to selected Failure Reasons, the call routing table will be parsed for the next matching pattern and, if found, the call will be routed to the specified destination.

  Busy - available for PBX, SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when the dialed destination is busy.

  Wrong Number - available for PBX, SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when the dialed number is wrong.

  Network Failure - available for SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when system overload, network failure or timeout expiration occurred.

  System Failure - available for SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases indicated in **Network Failure** and **Other** fail reasons.

  Cannot Establish Connection – available for FXO, ISDN destination types and indicates cases when connection cannot be established.

  Other - available for SIP, SIP Tunnel, and IP-PSTN destination types and indicates cases when authorization, negotiation, not supported or request rejected or other unknown errors occur.
- **Any** stands for all failure reasons mentioned in the **Failover Reason(s)** group.

The **Custom Profile** text field is present if the **PBX-Voicemail** destination type has been selected on the first page of the Call Routing Wizard. This field requires the **Voice Mail Profile** name to activate the custom voice mail settings (see Voice Mail Profiles) on the extension when the corresponding routing rule will be used.

Please Note: If an extension does not have a profile specified here or the specified profile name is incorrect, the default Voice Mail Settings of the extension will be used.

The **Transport Protocol for SIP messages** manipulation radio buttons group is available for **SIP** or **IP-PSTN** destination types only and allows you to select the transport (UDP, TCP or TLS) to transmit the SIP messages through.

The **SIP Privacy** manipulation radio buttons group is only available for the **SIP** destination type and allows you to select the security of the SIP route by means of hiding (or replacing, depending on the configuration of the SIP server) the key headers of the SIP messages used to establish the call.

- **Default Privacy –** with this selection, QX1000 specific SIP privacy will not be applied and all privacy will rely on the configuration of the SIP Server.
- **Disable Privacy –** with this selection, SIP call security will not be disabled and all headers of the SIP message will be transparently visible to the destination.
- **Enable Privacy -** with this selection, SIP privacy will be specified for the corresponding route. This selection enables a group of checkboxes in order to choose the key headers that are to be fully or partly hidden or replaced. The **Require Privacy** checkbox selection is used to restrict the delivery of the SIP message if any of the selected headers cannot be hidden (or replaced, depending on the configuration of the SIP server) before being sent to the destination.

For **FXO** destination types, a group of **Port ID** radio buttons allows you to select whether a specific or any available FXO line will be used to route the call. The **Any@Any** selection indicates that the call will be routed through the first available FXO line. The **Specific Ports** selection is used to select a group of routing settings for shared FXO lines.

Each Shared Gateway Ports radio buttons group is dedicated to one shared FXO device and is used to configure shared FXO lines usage when using the corresponding routing entry. None selection means no shared FXO lines will be used for the call routing of the specific routing rule. Any Port@ipaddress (where ipaddress is the IP address of the FXO gateway that shares its FXO lines) selection means the call will be routed through the first available shared FXO line. FXO@ipaddress port checkboxes are used to select those which shared FXO ports will be used for the corresponding rule routing. In case if multiple shared FXO ports are selected here, the first available port will be used.

The **FXO Lines Load Balancing** drop down list is used to enable load balancing mechanism on the PSTN lines. The None selection in this list means that no load balancing will be applied and the call will be routed through the first available PSTN line (among the selected ones). The Round Robin selection means that according to an internally gained statistics of most used PSTN lines, the call will be routed to the less used and currently available PSTN line (among the selected ones).

For **ISDN** destination type, the **Port ID** drop down list contains the following options:

- **Any Port (User)@Any** - any shared ISDN trunks running in User mode.
- **Any Port (Network)@Any** - any shared ISDN trunks running in Network mode.
- **ISDN Trunk@ipaddress** - shared ISDN trunks on the selected gateway (where ipaddress is the IP address of the ISDN gateway that shares its ISDN trunks)

- **Any Port (User)@ipaddress** - any shared ISDN trunks from the selected gateway running in User mode.
- **Any Port (Network)@ipaddress** - any shared ISDN trunks from the selected gateway running in Network mode.

The **Call Routing Wizard** - Page 3 appears if the **Filter on Source / Modify Caller ID** checkbox had been enabled on Page 1 of the **Call Routing Wizard.** It will require information about the source caller.

The **Source Number Pattern** field requires the caller address for which the current route will be applied. The complete list of characters and wildcards is allowed in this text field (see chapter Allowed Characters and Wildcards).

The **Source Type** drop down list gives you the option to select the source type (PBX, SIP, ISDN, FXO) used by the source caller to reach the QX1000.

The settings in the **Caller ID Modification** group allow Caller IDs of source calls to be modified.

The **Number of Discarded Symbols (NDS)** text field requires the number of digits that should be discarded from the beginning of the **Source Number Pattern**. The field should be empty if digits do not need to be discarded. Only numeric values are allowed for this field, otherwise the error message "Error: Number of Discarded Symbols is incorrect - digits allowed only" will appear.

The **Prefix** text field requires entering the symbols (alphanumerics and any characters supported in the SIP username) that will be placed in front of the **Source Number Pattern** instead of the discarded digits. (For example, if the routing pattern is 12345, the Number of Discarded Symbols is two, and the prefix digits are 909, the final phone number will be 909345.) Wildcards are allowed here (see chapter Allowed Characters and Wildcards).
The two-stage dialing is available for PBX and ISDN destination types.
The **Discard Non-Numeric Symbols** checkbox is used to discard any non-numeric symbols from the **Source Number Pattern**.

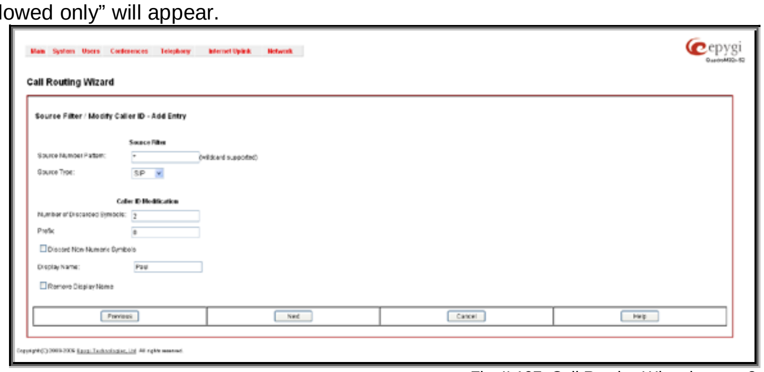


Fig. II-197: Call Routing Wizard - page 3

The **Display Name** text field allows you to replace an original caller's ID with the custom display name for the corresponding routing rule. This field is optional and when it is left empty, an original caller ID will be displayed on the called destination's phone, otherwise the name inserted here will appear on the phone. This field is not available for PBX-Voicemail destination type routing rules.
The **Remove Display Name** checkbox is used to remove caller IDs from calls made with this routing rule. This checkbox is not available for PBX-Voicemail destination type routing rules.

The **Next** button will open the **Call Routing Wizard** - Page 4 where different information about source caller will be required depending on the selected **Source Type**. For the **SIP** source type, the **Source Host** text field will require one or more IP addresses or host names of the SIP server where the caller is registered, or the caller's device if they are direct calls, separated by a space. The **Call Routing Wizard** - Page 5 appears if the **Set Date / Time Period(s)** checkbox previously had been enabled on Page 1 of the **Local Call Routing Wizard**. It will require information about the pattern validity period(s).

This page provides selection between **Typical** and **Custom** date/time rule definitions.

The **Typical** selection contains the following group of radio buttons that are used to select the frequency of the corresponding routing pattern that is to take place:

- **Daily**
- **Weekly** – the preferred weekday(s) should be selected for this option.
- **Monthly** – the calendar day should be selected for this option.
- **Annually** – the calendar day and month should be selected for this option.

In the **Available Time Period** drop down lists, the time range of the pattern validation should be defined. Any time selected in this field will be considered corresponding to the QX1000's Time/Date Settings.

The **Custom** selection provides the option to manually define the validity period(s). Use the following format to insert pattern date/time rule(s):
[Month,Month-Month,...][Day-Day,Day,...][hh:mm-hh:mm,...]; ...

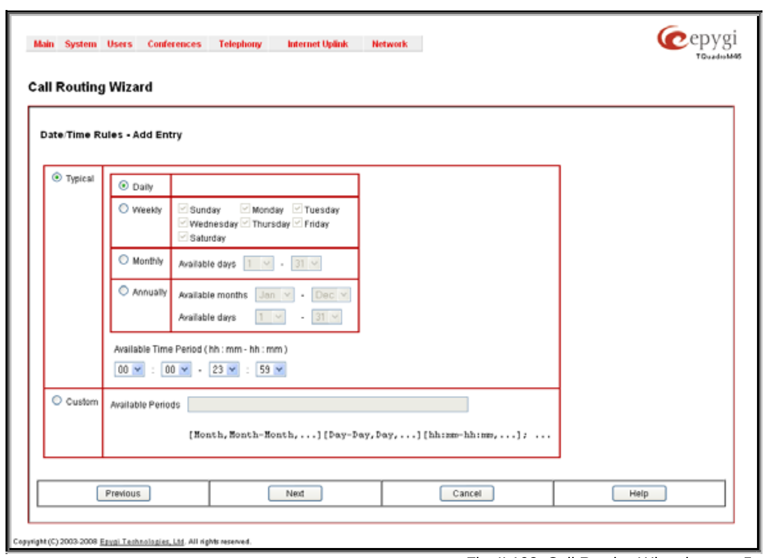


Fig. II-198: Call Routing Wizard - page 5

The **Call Routing Wizard** - Page 6 appears if the **Set Tracing / Debug Options on This Rule** checkbox was previously enabled on Page 1 of the **Local Call Routing Wizard**. It will require information about the tracing/debug options.

This page offers result options of the corresponding routing rule execution when the notification event will be printed in the Events page.

- **In Case of Successful Call** – a notification event is printed when the successful call was established with the routing rule.
- **In Case of Failover** – a notification event is printed when the call ends up on one of the failover reasons selected on the Page 2 of the **Local Call Routing Wizard.**
- **In Case if Call Failed to Establish** – a notification event is printed when the call executed with the routing rule failed.

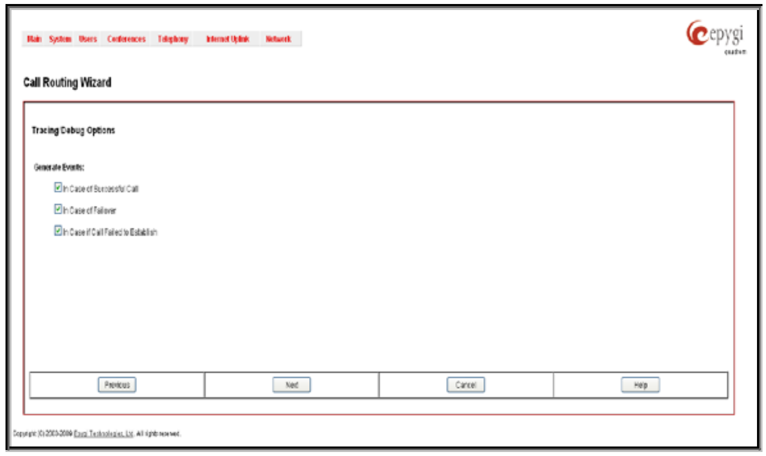


Fig. II-199: Call Routing Wizard – page 6

Please Note: Established patterns based on the **Emergency Codes and PSTN Access Codes Settings** in the System Configuration Wizard will be marked in bold and will be placed in the first position in the Call Routing Table. Additionally, they cannot be modified and deleted from the Call Routing Table.

The **Duplicate** functional button is used to create a routing pattern with the settings of an exiting one. This is to avoid configuring a new routing entry completely by duplicating an existing entry with different settings. To use the **Duplicate** button only one record may be selected, otherwise the error message “One row should be selected” will appear. The **Duplicate** button opens the **Call Routing Wizard** where all fields except the **Pattern** field are already filled in. A **Pattern** for the new route will be required anyway.

The **Move Up** and **Move Down** buttons are used to move call routing patterns one level up or down within the **Call Routing** table. The sequence of the routing patterns is important when making routing calls because the **Call Routing** table is parsed from the top down and routing will take place according to the first pattern that matches the dialed number. The **Move To** button is used to move the selected entry to a different position in the Call Routing Table. This will increase or decrease the selected pattern’s priority. Pressing the button will open the page where a row number should be specified together with the position the selected entry is to be placed (before or after the defined row).

Local AAA Table

The **Local AAA Table** page allows you to manage local authentication and the authorization database. Callers dialing the routes which have an AAA (Authentication, Authorization, and Accounting) option enabled, will pass the authorization on the **Local AAA Table** by using a phone number or username/password, depending on the corresponding entry configuration on this page.

The caller passes authorization automatically if the detected phone number of the caller dialing a route has the AAA option enabled and is registered in the **Local AAA Table**. If the caller ID service is disabled or the caller’s phone number is not registered, the caller is asked to enter a registration user name and password.

The **Add** functional button opens the **Call Routing – Local AAA Table - Add Entry** page where a new local AAA record can be created.

The **Call Routing – Local AAA Table - Add Entry** page offers a group of manipulation radio buttons to select the type of authorization and the following other parameters:

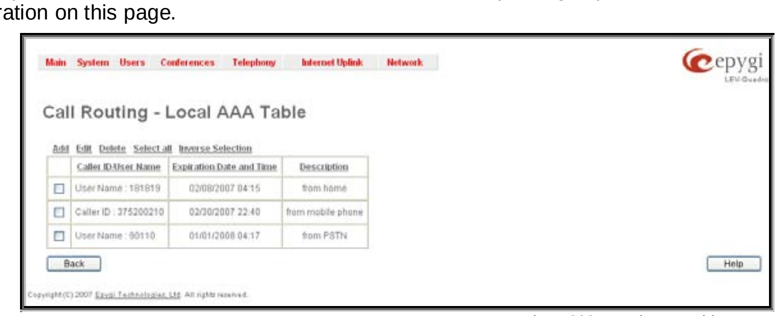


Fig. II-200: Local AAA Table page

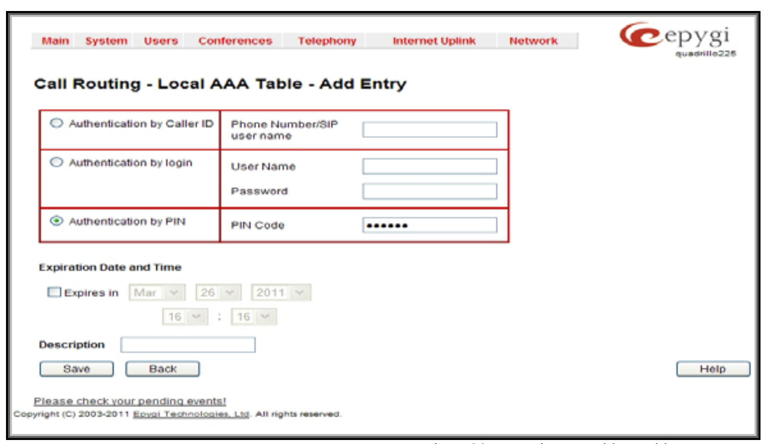


Fig. II-201: Local AAA Table - Add Entry page

- **Authentication by Caller ID** – this selection is used to set the authentication based on the caller’s phone number (which is considered to be automatically detected). The **Phone Number/SIP User Name** text field requires the caller’s phone number or the SIP username. Only numeric and wildcard characters (see chapter Entering SIP Addresses Correctly) are allowed for this field. '[' , ']' , ',', '-', ‘{‘, ‘}’ are used to define a range or a quantity of numbers. For example, 2{13-17, ww, a-c} means that the dialed number may be 213, 214, 215, 216, or 217, 2ww, 2a, 2b and 2c to match the specified phone number; in the case of 2[3,7], the dialed number may be 23 or 27 to match the specified phone number. The {11, 15, 23, 38, 45} pattern means that the dialed number may be 11, 15, 23, 38 or 45 to match the pattern.

- **Authentication by Login –** this selection is used to set the authentication based on the username and password inserted by the user upon login. The **Username** text field requires the authentication username. Only numeric values are allowed for this field, otherwise the error message "Incorrect Username - digits allowed only" will appear. The **Password** text field requires the authentication password. Only numeric values are allowed for this field, otherwise the error message "Incorrect Password - digits allowed only" will appear.
- **Authentication by PIN**- this selection is used to set the authentication based on the PIN inserted by the user upon login. Only digit values are allowed for this field, otherwise the appropriate error message will be displayed.

The **Expiration Date and Time** drop down-lists are used to set the date and time when the registration will expire.

The **Expires in** checkbox is used to enable the **Expiration Date and Time** feature.

The **Description** text field requires an optional description about the calling party.

Edit opens the **Edit Entry** page to modify the local AAA entry.

Delete removes the selected local AAA entry from the Local AAA Table.

Select all selects all records of the table.

Inverse selection inverses the current selection (if no records are selected, clicking on inverse selection will check all records).

Global Speed Dial Directory

The **Global Speed Dial Directory** link leads to the page where global speed dialing rules may be uploaded in a file. With this service, you may define multiple speed dial rules, write and save them in a file and then upload all of them at once.

To compose the configuration file, any text editor can be used which may produce files compatible to the CSV format: the speed dial code and destination should be separated by commas. There should be a line break after each code defined.

The **View/Download Speed Dial Directory** and **Remove Speed Dial Directory** links appear only if a global speed dial configuration file is uploaded previously.

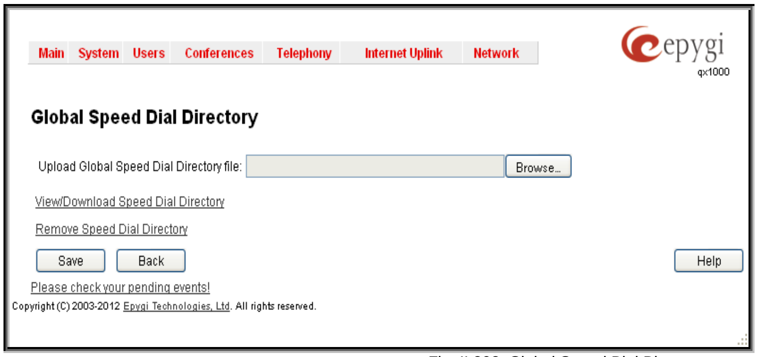


Fig. II-202: Global Speed Dial Directory page

The **View/Download Speed Dial Directory** link is used to download the configuration file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Speed Dial Directory** link is used to restore the default configuration.

The speed dial configuration file downloaded from the QX1000 is in the CSV format.

To use the global speed dialing rules, user should simply dial the speed dial code assigned to that speed dialing rule. The call will be parsed through the rules of Call Routing table.

To create a new Call Routing rule

1. Click on the **Call Routing Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Call Routing** page.
3. Specify the **Pattern** in the corresponding field.
4. Select the **Number of Discarded Symbols** and **Prefix** if required.
5. Select the **Destination Type** from the drop down list.
6. Define the **Metric** or leave the default.
7. Enter a **Description** if needed.
8. Enable the **Filter on Source / Modify Caller ID** checkbox, if the route functionality should be limited. This is dependent on the source caller information.
9. Enable the **Set Date/Time Period(s)** checkbox if a route should be functional within certain time/date intervals.
10. Press **Next**.
11. Select the user or attendant extension from the **Use Extension Settings** drop down list that the call will be placed on.
12. Specify the **Destination Host** and **Port Number**, **Username** and **Password** if an **IP** or **IP-PSTN** call type has been selected. For the **IP-PSTN** call type, enable **Multiple Logons** if necessary. Enable the **Use RTP Proxy** checkbox if needed.
13. Choose the Authentication and Accounting method from the **AAA Required** drop down list.
14. Choose a **Fail Reason** from the corresponding drop down list.
15. Configure **Transport Protocol for SIP messages** and **SIP Privacy** parameters as needed.
16. Press the **Next** button.
17. If the **Filter on Source / Modify Caller ID** checkbox has been previously enabled and the destination type is different from the FXO, fill in the **Source Number Pattern** into the corresponding text field. Choose the needed value from the **Source Type** drop down list, as well as the **Number of Discarded Symbols** and **Prefix** values.
18. Press the **Next** button.
19. If **IP** has been selected on the previous step in the **Source Type** drop down list, then **Source Host** should be inserted in the current page. If **FXO** or **ISDN** has been selected in the **Source Type** drop down list, then the ISDN trunk or the FXO line number should be selected here.
20. If the **Set Date/Time Period(s)** checkbox has been selected on the first page, pressing **Next** will open the **Date/Time Rules** page where route validity should be defined.

21. If the **Set Tracing / Debug Options on This Rule** checkbox has been selected on the first page, pressing **Nex**t will open the **Tracing/ Debug Options** page where the tracing/debug options should be defined.
22. Press the **Finish** button to establish a local route with the inserted settings.

To create a local AAA entry

1. Click on the **Local AAA Table** link on the **Call Routing** page.
2. Press the **Add** button on the **Local AAA Table** page.
3. Choose the Authentication type.
4. Enter the **Phone Number**, **Username** and **Password** or the **Authentication by PIN** depending on the selected Authentication type.
5. Use the **Expiration Date and Time** checkbox to enable the expiration timeout.
6. Select the **Expiration Date and Time** from the corresponding drop down lists.
7. Press **Save** to apply these settings.

Allowed Characters and Wildcards

The following is the set of characters and wildcards allowed in the **Pattern** and **Source Number Pattern** text fields of the Call Routing Wizard:

Characters:

0…9 A…Z

a…z + = $; / ~ _ - . & ( ) ' ! * ? {} , [ ]

Please Note: The symbols * and ? should be prefixed with a slash (\) if they are used as ordinary characters; otherwise the system will interpret them as wildcards.

Please Note: The symbols !, {, }, [,], - and , are used to define a range of characters and cannot be used as ordinary characters.

Wildcards:

* Any number of any characters

? Any single character

{ } A character or a string from the specified set of characters and strings.

The following control symbols are used to specify a set:

- Use a comma (,) to separate the elements of a set.

  Please Note: No spaces are allowed within braces.

  Example:

  The pattern is **9{1,3,11,a}**.

  Numbers matching the pattern are **91, 93 , 911, 9a.**

- Use a minus sign (-) to specify a range of characters. Each successive element of the range is obtained by increasing the previous element (the element code) by one.

  Example:

  The pattern is **2{11-15,a-d}5**.

  Numbers matching the pattern are **2115, 2125, 2135, 2145, 2155, 2a5, 2b5, 2c5, 2d5**.

- Use an exclamation point to exclude a character or a string from a set.

  Example:

  The pattern is **2{11-15,a-d,!14,!c}5**.

  Numbers matching the pattern are **2115, 2125, 2135, 2155, 2a5, 2b5, 2d5**.

  Please Note: You can use the wildcard ? within the braces, but not *. Thus, **{12-104,15?,36?}** is a valid pattern, whereas **{15*,36*}** is not.

  Please Note: The symbol ! cannot be used to exclude a range of symbols. For example **2{15-60,!23-32}** or **2{15-60,!23-!32}** are not valid patterns. To valid pattern will be to **2{15-22,33-60}**.

[] The same as above with the exception that character ranges can include single-digit/character elements only.

Example:

The pattern is **2[1-5, a-c]5**.

Numbers matching the pattern are **215, 225, 235, 245, 255, 2a5, 2b5, 2c5**.

**** Precedes a control symbol (*, ?, -, ! and ,) to indicate that it is used as an ordinary character, not a wildcard.

Example:

The pattern is **1*[1-3]**

Numbers matching the pattern are: **1*1, 1*2, 1*3**

Please Note: Patterns cannot be prefixed with the * symbol. The system considers the patterns starting with * as feature codes and does not parse them through the Call Routing table.

@ Used to indicate the full SIP address (example: 20233@sip.epygi.com). This pattern is mainly used to call back users registered on the SIP server different from the one where the called party is registered.

Please Note: Patterns containing @ symbol will not be parsed among those that do not have @ symbol in the Call Routing Table. When calling from local extensions (the calling number for local extension is sipnumber@ip_address_of_QX1000, e.g. 20233@192.168.35.25), only the sipnumber part of the pattern will be parsed among other entries with @ symbol in the Call Routing Table.

Best Matching Algorithm

All calls through and within a QX1000 are made according to call routing patterns that specify a destination based on a dialed number. When a user dials a number to make a call, the QX1000 matches the dialed number against the existing patterns that are specified in the Call Routing table. If the dialed number matches only to a single pattern, this pattern will be used to set up a call. If several patterns have been found to match the number, the QX1000 uses the Best Matching Algorithm to prioritize the matching patterns. Once the patterns are prioritized, the pattern with the highest priority will be used as a preferred route for call setup. The successive patterns will be used only if the destination specified by a higher priority pattern is unreachable.

To prioritize the matching patterns, the following criteria are sequentially applied to matching patterns. The criteria are ordered by their priorities: Each consecutive criterion is calculated only for the patterns that take the same value for the preceding criteria: that is Criterion 3 is calculated only for patterns that take the same value for Criterion 1 and Criterion 2.

Criterion 1	**The presence of asterisks ("*") in a pattern** The patterns without "*" have a higher priority.
Criterion 2	**The total number of matching digits/symbols inside and outside the braces/brackets** The more matching digits a pattern contains, the higher its priority.
Criterion 3	**The number of matching digits/symbols outside the braces/brackets** The more matching digits outside braces/brackets a pattern contains, the higher its priority. **Please Note:** This criterion is used only if several patterns take an equal but non-zero value for Criterion 2.
Criterion 4	**The total number of question marks ('?') inside and outside the braces/brackets** The more question marks a pattern contains, the higher its priority.
Criterion 5	**The number of question marks ("?") outside braces/brackets** The more question marks outside braces/brackets a pattern contains, the higher its priority. **Please Note:** This criterion is used only if several patterns take an equal but non-zero value for Criterion 4.
Criterion 6	**The number of square brackets ("[]")** The more brackets a pattern contains, the higher its priority.
Criterion 7	**The number of braces ("{}")** The more braces a pattern contains, the higher its priority.
Criterion 8	**The number of asterisks ("*")** The fewer asterisks a pattern contains, the higher its priority.
Criterion 9	**The value of the metric** The lower the metric of a pattern is, the higher its priority.
Criterion 10	**The position in the routing table** The higher the position of a pattern in the routing table is, the higher its priority.

Example: The user has dialed 1231 and the following matching patterns have been found.

The list of patterns
1
123*
{11-15}3*
?2?1
123?
[1-3]*
[1-3]???
{100-150, asd, *\?}1
12*31
1[1-3]3[0-8]
1231
*2*1
*

Step 1: The list is split into two groups separating the patterns with “*” from those without (Criterion 1). The patterns with “*” form a group with a lower priority and are pushed back to the end of the list.

Criterion 1

The list split into two subgroups
?2?1
123?
[1-3]???
{100-150, asd, *\?}1
1[1-3]3[0-8]
1231
1
123*
{11-15}3*
[1-3]*
12*31
*2*1
*

Step 2: The two groups of patterns are arranged separately from each other by the total number of matching digits inside and outside the braces/brackets in the descending order (Criterion 2). The patterns that contain the same number of matching digits are grouped into sub-lists.

Criterion 2

The list of patterns	Matching digits
?**2**?**1**	2
123?	3
[**1**-3]???	1
{**100-150**, asd, *\?}**1**	4
1[**1-3**]**3**[**0-8**]	4
1231	4
1	1
123*	3
{**11-15**}**3***	3
[**1-3**]*	1
12*31	4
*2*1	2
*	0

The list of patterns	Matching digits
1[1-3]3[0-8]	4
1231	4
{100-150, asd, *\?}1	4
123?	3
?2?1	2
[1-3]???	1
12*31	4
123*	3
{11-15}3*	3
*2*1	2
1	1
[1-3]*	1
*	0

Step 3: The new sub-lists are arranged separately from each other by the number of matching digits outside the braces/brackets (Criterion 3). The patterns that contain the same number of matching digits are grouped into sub-lists.

Criterion 3

The list of patterns	Matching digits
1[1-3]**3**[0-8]	2
1231	4
{100-150, asd, *\?}**1**	1
123?	-
?2?1	-
[1-3]???	-
12*31	-
123*	3
{11-15}**3***	1
*2*1	-
1	1
[1-3]*	0
*	-

The list of patterns	Matching digits
1231	4
1[1-3]3[0-8]	2
{100-150, asd, *\?}1	1
123?	-
?2?1	-
[1-3]???	-
12*31	-
123*	3
{11-15}3*	1
*2*1	-
1	1
[1-3]*	0
*	-

The Best Matching Algorithm will stop after executing step 3 as no new sub-lists are formed. The resultant list of prioritized patterns will be the following:

The prioritized list
1231
1[1-3]3[0-8]
{100-150, asd, *\?}1
123?
?2?1
[1-3]???
12*31
123*
{11-15}3*
*2*1
1
[1-3]*
*

VoIP Carrier Wizard

The **VoIP Carrier Wizard** is used to define access codes for available VoIP Carrier accounts which will particularly allow you to reach users over IP-PSTN providers or to call to the peers registered on the certain SIP servers by dialing simple digit combinations.

For each configured VoIP carrier, the wizard creates a specific IP-PSTN routing rule in the Call Routing table. This entry is available to PBX users only, which means only PBX users can make calls to the corresponding VoIP carrier. Additionally, a virtual extension automatically generated in Extensions Management will be registered on the defined VoIP Carrier's SIP server.

The settings of that extension will be used to make calls from QX1000's users towards the created VoIP Carrier will be placed.

VoIP Carrier Wizard – Page 1 provides a following option of describing the VoIP carrier:

When predefined carrier is selected in the **VoIP Carrier** drop down list, the SIP Server and Port will be already predefined in the next page. **Manual** selection allows you to manually set up the VoIP Carrier settings.
The **Description** field allows you to insert an optional description of the VoIP Carrier.

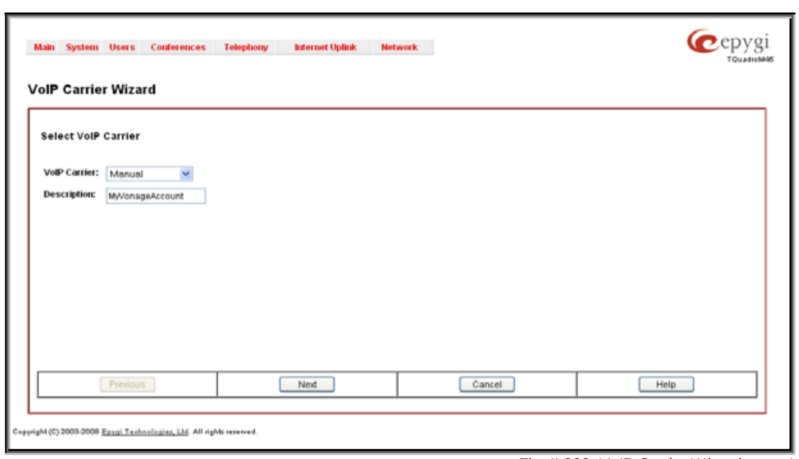


Fig. II-203: VoIP Carrier Wizard page 1

VoIP Carrier Wizard – Page 2 is used to define VoIP Carrier Settings. The page contains following components:

1. VoIP Carrier Common Settings

The **Account Name** text field requires a username for authentication on the defined SIP server.

The **Password** text field requires a password for authentication on the defined SIP server.

The **Confirm Password** text field requires a password confirmation. If the input is not corresponding to the one in the **Extension Password** field, the error message "Incorrect Password confirm" will appear.

The **SIP Server** text field requires an IP address or the hostname of the SIP server destination party it is registered on.

The **SIP Server Port** text field requires the port number of the SIP server destination party it is registered on.

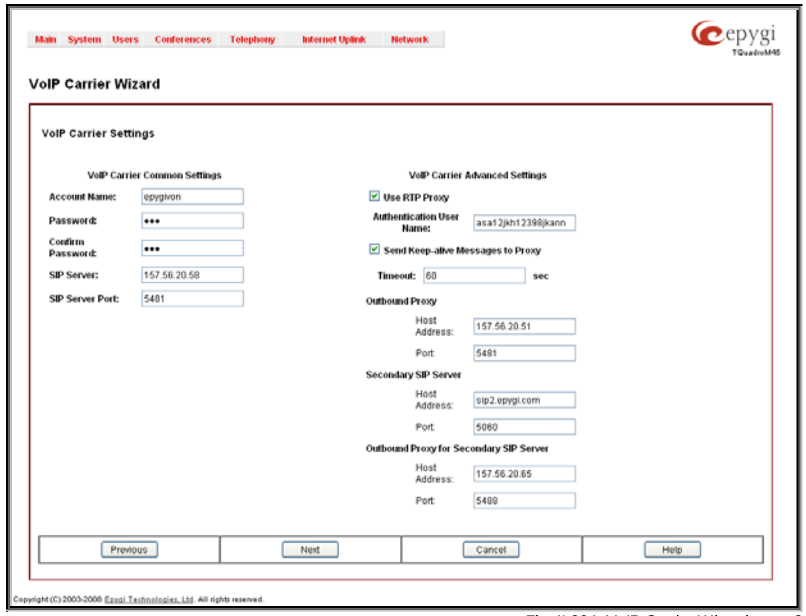


Fig. II-204: VoIP Carrier Wizard page 2

2. VoIP Carrier Advanced Settings

The **Use RTP Proxy** checkbox is applicable only when a route is used for calls towards a configured VoIP Carrier from a peer located outside the QX1000. When this checkbox is selected, the RTP streams between external users will be routed through QX1000. When the checkbox is not selected, RTP packets will move directly between peers.

UserID requires an identification parameter to reach the SIP server. It should have been provided by the SIP service provider and can be requested only for certain SIP servers. For others, the field should be left empty.

Send Keep-alive Messages to Proxy enables the SIP registration server accessibility to the verification mechanism. **Timeout** indicates the timeout between two attempts of SIP registration server accessibility verification. If a reply is not received from the primary SIP server within this timeout, the secondary SIP server will be contacted. When the primary SIP server recovers, SIP packets will continue to be sent to the server.

A group of **Host address** and **Port** text fields respectively require the host address (IP address or the host name), the port number of the **Outbound Proxy**, **Secondary SIP Server** and the **Outbound Proxy for the Secondary SIP Server**. These settings are provided by the SIP servers' providers and are used by QX1000 to reach the selected SIP servers.

VoIP Carrier Wizard – Page 3 contains the following VoIP Carrier access code selection components:

The **Access code** text field requires a digit combination by dialing which the corresponding VoIP Carrier will be reached. The **Access code** radio buttons allows you to create outbound routing rules.

- **By prefix** text field requires entering the prefix that will be placed in front of the routing pattern instead of the discarded digits. The Prefix field can consist of numeric values only. A corresponding warning appears if any other symbols are inserted.

- **By pattern** text field specifies calls to which the rule should be applied. If an outbound call has a destination number that matches the specified pattern, it will be completed according to the current rule. A routing pattern may contain wildcards. The complete list of characters and wildcards allowed in this text field is given on the Allowed Characters and Wildcards page.

The **Route Incoming Calls to** drop down list allows you to select an extension (or Auto Attendant) on the QX1000 where incoming calls from the configured VoIP Carrier should be routed to. For the selected extension there will be an unconditional forwarding set up which will care for incoming calls forwarding from the VoIP carrier to the corresponding extension.

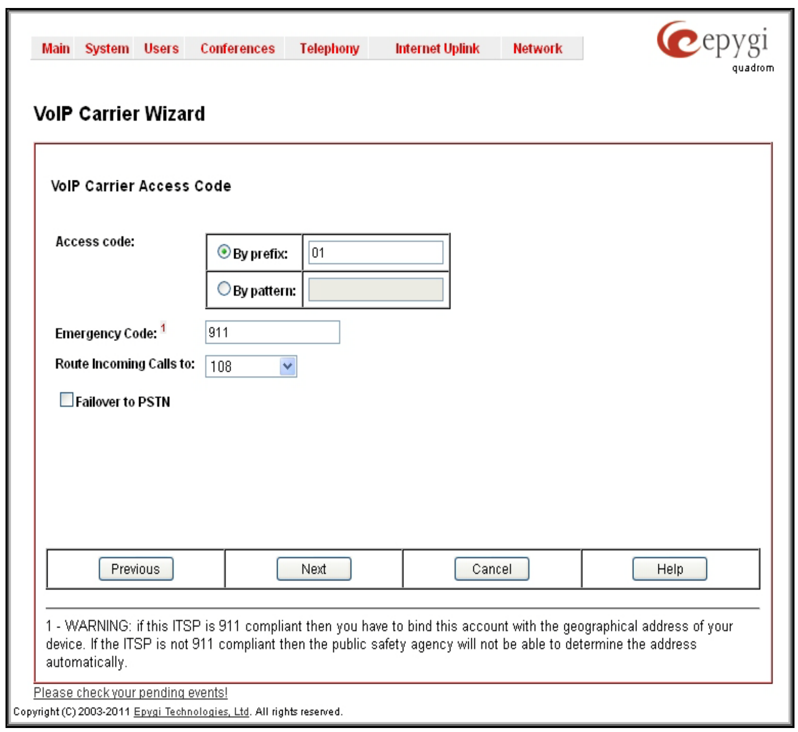


Fig. II-205: VoIP Carrier Wizard page 3

The **Emergency Code** text field requires the emergency code supported by the specified ITSP. By default is field is filled with the information defined in the QX1000's System Configuration Wizard, but this field also allows to define an ITSP specific emergency codes. In case your system has both local PSTN emergency codes and ITSP codes configured, when dialing the certain emergency code, QX1000 will first try to reach the local PSTN allocated emergency destination, and if failed will dial the ITSP emergency destination.

Please Note: If the defined ITSP is 911 compliant then you have to bind this account with the geographical address of your device. If the ITSP is not 911 compliant then the public safety agency will not be able to determine the address automatically.

The **Failover to PSTN** checkbox selection will route the call to the PSTN through the local FXO line in case if the VoIP Carrier is not available. When this checkbox is selected, an additional entry will be added to the Call Routing table. This maintains digit transmission to the local PSTN when an IP call towards the configured VoIP Carrier cannot be established.

Please Note: A warning message will appear when the defined **Access Code** already exists in the Call Routing table or causes a conflict with entries already in the Call Routing table. In this case, when continuing through the VoIP Carrier Wizard, the existing entry in the Call Routing table will automatically be overwritten by the new settings.

RADIUS Client Settings

RADIUS (Remote Authentication Dial In User Service) specifies the RADIUS protocol used for authentication, authorization and accounting, to differentiate, to secure and to account for the users. The RADIUS Server provides the option for a caller from/through QX1000 to pass authentication and to be able to dial a specific number.

When a RADIUS client is enabled on the QX1000, and according to the configuration of **AAA Required** option (see Call Routing table), the RADIUS server will be used to authenticate user and/or to account for the call. This can be accomplished by automatic detection of the caller's number or a customized login prompt where the caller is expected to enter a username and password.

Transactions between the client and the RADIUS server are authenticated through the use of a shared Secret Key, which is never sent over the network. In addition, user passwords are encrypted when sent between the client and RADIUS server to eliminate the possibility of a party viewing an unsecured network where they could determine a user's password. If no response from the RADIUS Server is returned after the Receive Timeout expires, the request is resent numerous times as defined in the Retry Count list. The client can also forward requests to an alternate server(s) if the primary server is down or unreachable. An alternate server can be used after a number of failed tries to the primary server.

Once the RADIUS server receives the request, it determines if the sending client is valid. A request from a client that the RADIUS server does not recognize must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements (username, password, etc.) that must be met to give access to the user. If all conditions are met, the user gets access to the QX1000 Network.

The **RADIUS Client Settings** page contains the **Enable RADIUS Client** checkbox that enables RADIUS client on the QX1000.

Please Note: The RADIUS Client cannot be disabled if there is at least one route with **RADIUS Authentication and Authorization** or **RADIUS Accounting** values configured in the **AAA Required** drop down list at the Call Routing table. In order to be able to disable the RADIUS Client on the QX1000, appropriate routes should be removed first.
The other RADIUS Client settings are divided into three groups:

1. Registration Settings

The **Primary Server** requires the IP address of the primary Radius Server.

The **Secondary Server** requires the IP address of the secondary Radius Server.

NAT Station IP text fields require the NAT PC WAN IP address. If no NAT Station is specified here, QX1000's IP address will be sent to the RADIUS server.

Secret Key is used to insert the secret key between the Radius client and the server. Contact the Radius server administrator to get the secret key for your QX1000.

The **Confirm Secret Key** field is used to verify the secret key. If the entered **Secret Key** does not correspond to the one in the **Confirm Secret Key** field, the error message "The Secret Key does not match. Please try again" will appear.

Retry Count allows you to select the number of attempts authorized before canceling the registration.

Receive Timeout allows you to select the timeout (in seconds) between two attempts to register.

Encoding Type allows you to select the encoding type (PAP or CHAP) that should be unique on both the client and the server sides for the establishment of a successful connection. Encoding type should also be requested from the Radius Server administrator.

The **Authorization Port** text field requires the port number on the RADIUS server where QX1000 is to send the authentication requests.

The **Accounting Port** text field requires the port number on the RADIUS server where QX1000 is to send the accounting messages.

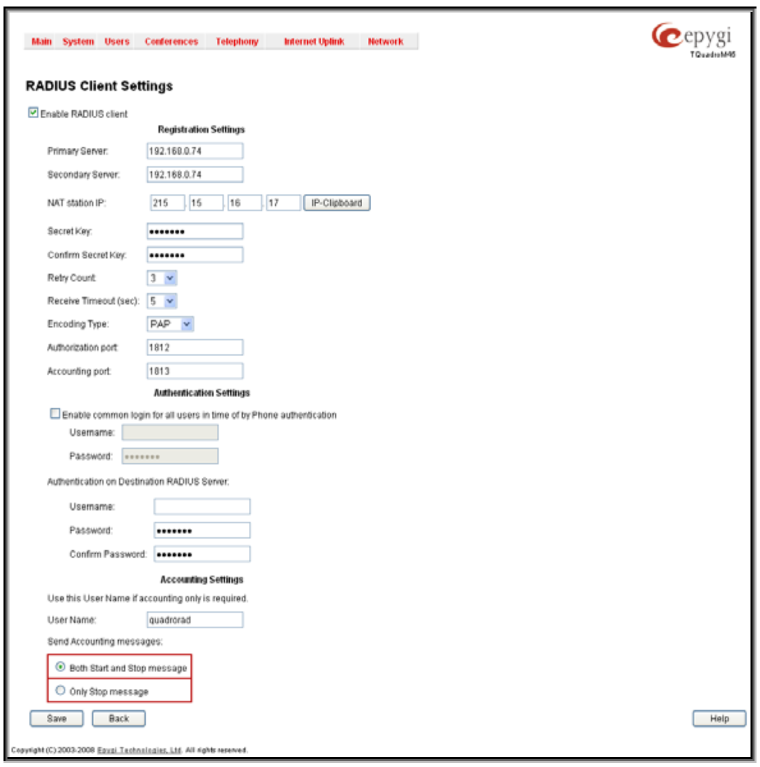


Fig. II-206: Radius Client Settings page

2. Authentication Settings

The **Enable common login for all users in time of by Phone authentication** checkbox enables custom settings for the callers who passed an authorization by phone on the QX1000. This checkbox enables **Username** and **Password** text fields to insert the custom settings that will stand instead of the source caller's settings when being delivered to the RADIUS server.

The **Authentication on Destination RADIUS Server** parameters group is used to insert a **Username** and a **Password** (followed by the password confirmation) to pass authentication on the RADIUS Server of the destination QX1000. If these fields are left empty, the original authentication settings that users enter for authentication will be used.

3. Accounting Settings

The **Username** field is dedicated for accounting services only. It is used to insert an identification username for accounting purposes. When no username is specified in this field, the source username will be used for accounting.

The **Send Accounting messages** manipulation radio buttons group is used to select sending both **Start** and **Stop** accounting messages or only **Stop** accounting message.

Voice Mail Common Settings

The **Voice Mail Recording Codec** page is used to configure the codec for the Voice Mail recording and other settings related to the voicemail to email and FAX to email sending. It offers the following components:

The **Recording Codec** drop down list contains the existing codecs for voice mail compression. Changing the Voice Mail recording codec will directly affect the allocated memory size for users.

Email Subject for voice field is used to when user enables **Send new voice messages via e-mail** option from his personal **Voice Mail Settings**. In this field you may define a flexible subject for all emails sent from the QX1000 and carrying the voice mails.

Besides using static text in the subject line, you may want to use the predefined tags to combine the needed subject:

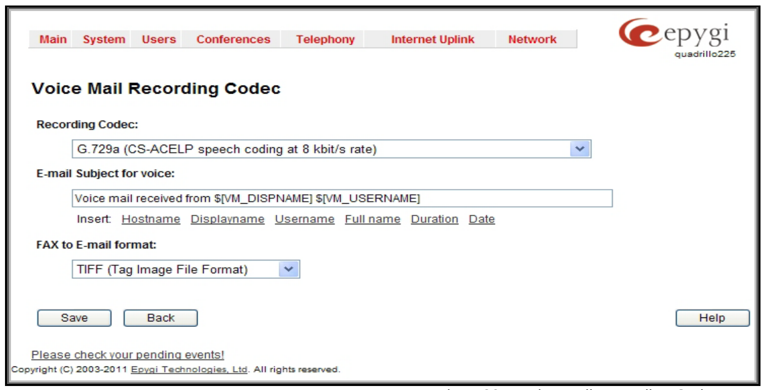


Fig. II-207: Voice Mail Recording Codec page

- **Hostname** - the hostname of the QX1000.
- **Displayname** - the caller's display name. This value is not displayed for PSTN callers.
- **Username** - the caller's SIP username. For PBX caller this is the caller's PBX number, for PSTN callers this is the caller's PSTN number.
- **Full name** - the caller's full SIP address (SIP username and the SIP server). For PBX caller this is the caller's PBX number, for PSTN callers this is the caller's PSTN number.
- **Duration** - the voice mail duration.
- **Date** - the date the voice mail was received.

To insert the predefined tag to the subject line, you should simply click on the corresponding tag. The following format should be maintained to create a flexible subject:

Example: Voice mail received from $[VM_DISPNAME] $[VM_DATE]

In this example, all email subjects will contain a static text "Voice mail received from" following by the display name of the caller and the date voice mail is received.

FAX to E-mail format drop down list is used to define the format of the FAX document received in the voice mail and to be attached to the email, in case user has enabled **Send new voice messages via e-mail** option from his personal **Voice Mail Settings**. TIFF or PDF formats may be selected here.

Dial Timeout

The **Dial Plan Settings** page is used to adjust the dialing timeout setting.

The **Routing Dial Timeout** setting specifies a period of time after the last dialed digit that the system identifies as a completion of dialing. If the user does not press any key within the specified timeout, the system assumes that the dialing is complete and starts calling the dialed number. Only predefined values included in the drop-down list can be used for this setting.

The **Routing Dial Timeout** setting will also be applied to all the supported IP phones that are auto-configured with the QX1000 and provide the possibility of changing this setting through the auto-configuration file. The modified value of the setting will take effect after rebooting the IP phones.

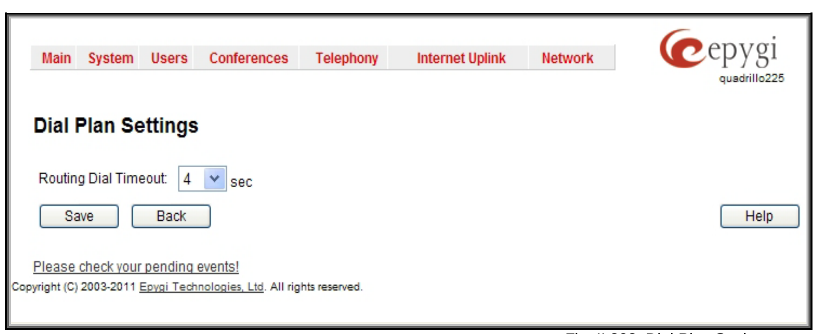


Fig. II-208: Dial Plan Settings page

3PCC Settings

The **3PCC Settings** page is used to adjust the third party call controlling settings. 3PCC service on the QX1000 allows call controlling applications to remotely initiate and handle calls on the QX1000 and to subscribe for certain event notifications from the QX1000.

This page consists of the following components:

The **Secure Connection** checkbox is used enable a secure encrypted connection between the call controlling application and the QX1000.

Please Note: For successful connection, this option should be set up in the same way on both sides (enabled or disabled on both sides).

The **Request Timeout** text field requires the timeout (in seconds) during which the QX1000 should receive a response to the request from the call controlling application. If the response is not received during this timeout, QX1000 will perform a request dependent default action. For example, if the call controlling application is configured to handle incoming calls on the QX1000.

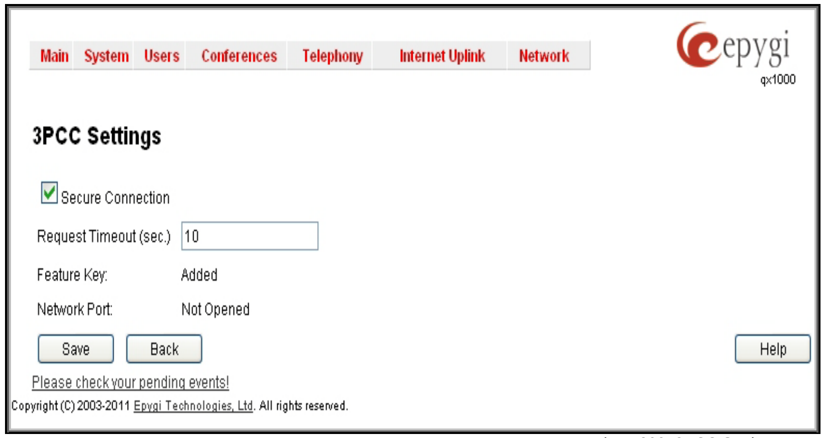


Fig. II-209: 3PCC Settings page

Once the incoming call occurs, QX1000 is trying to transfer the call to the call controlling application. If the call controlling application does not response within the mentioned timeout, QX1000 will answer the call or perform an action configured for unanswered incoming calls. This setting is dependent on the network conditions therefore consult with your network administrator before changing the default value.

The read-only **Feature Key** text field indicates whether the feature key for the 3PCC Support is installed on the system. The system will not accept connections from 3PCC applications if no key is found. The 3PCC support is an optional feature and can be activated with a feature key from the Features page.

The read-only **Network Port** text field indicates whether there is a filtering rule specified for the Call Control Access. If a third-party call control application connects to the QX1000 from the WAN interface, a filtering rule for the corresponding host should be created on the Call Control Access page to allow the application a remote access. Creating a filtering rule is not required if the firewall is not setup on the QX1000. The field shows **Opened** if there is at least one enabled filtering rule for the Call Control Access.

RTP Streaming Channels

The **RTP Streaming Channels** page is used to configure channels where the broadcast RTP streams are transmitted. These channels may be then configured to be used as hold music (see Manual III – Extension User's Guide) or any other type of music played to the caller.

The **RTP Streaming Channels** page consists of a table where RTP channels are listed.

Add opens the **Add Entry** page where a new RTP channel can be added.

The **Add Entry** page includes the following text fields:

The **RTP Channel Name** text field requires the name or the number of the RTP channel.

The **Port Number** text field requires the broadcasting RTP port number.

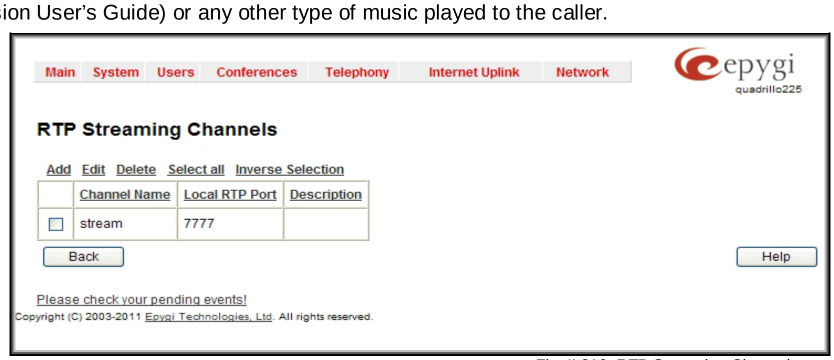


Fig. II-210: RTP Streaming Channel page

The **Description** text field requires optional information related to the RTP streaming channel.

Edit opens the **Edit Entry** page to modify the selected entry. This page contains all the same components as the **Add Entry** page does.

Delete removes the selected entries.

Select all selects all entries of the table.

Inverse Selection inverses the current selection (if no records are selected, clicking on inverse selection will check all records).

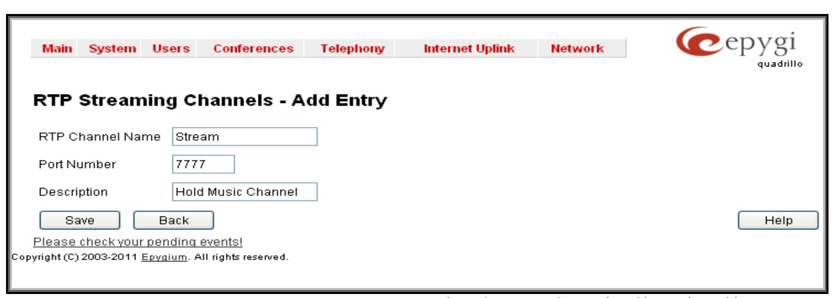


Fig. II-211: RTP Streaming Channel – Add Entry page

Call Recording

The **Call Recording** service is optional on the QX1000 and is activated from the Features page by inserting a feature key.

The **Call Recording** is used to record PBX, SIP or PSTN calls on the QX1000 and store the recorded calls either in the local Recording Box or upload them to the remote server. From Call Recording Settings page the call recording can be configured to be started automatically once the call starts or to be started manually from Administrator's Main Page of the QX1000's Web Management or by pressing the **Record** button on the IP phone during the call. If no such button exists on IP phone, the functional key can be configured from QX1000 to handle the recording functionality (see Programmable Keys Configuration).

To configure Call Recording, an extension of the Recording Box type should be created first. The memory allocated to that extension will be used for storing the recorded calls. There are two ways to access the recorded calls in the Recording Box: through handset and through Web Management. Through handset, Recording Box is accessible by calling the Recording Box extension. On QX1000's Web Management, call recordings are available from Extensions Management by clicking on the Recording Box extension.

Attention: Following limitations apply to the call recording on the QX1000:

- Only calls which are originated or terminated on the QX1000 extensions can be recorded. Pass through calls cannot be recorded.
- Calls to Auto Attendant or Voicemail cannot be recorded.

The **Call Recording Settings** page is used for configuring the call recording rules. It has two view modes - the **Basic View** and **Advanced View**, which can be switched by appropriate button.

The **Basic View** displays the table with the list of all active extensions, recording states of those extensions and recording parameters.

The **Advanced View displays** the table with all existing call recording rules. Click on the recording box extension number in the **Recorded To** column will move to the corresponding Recording Box**.**

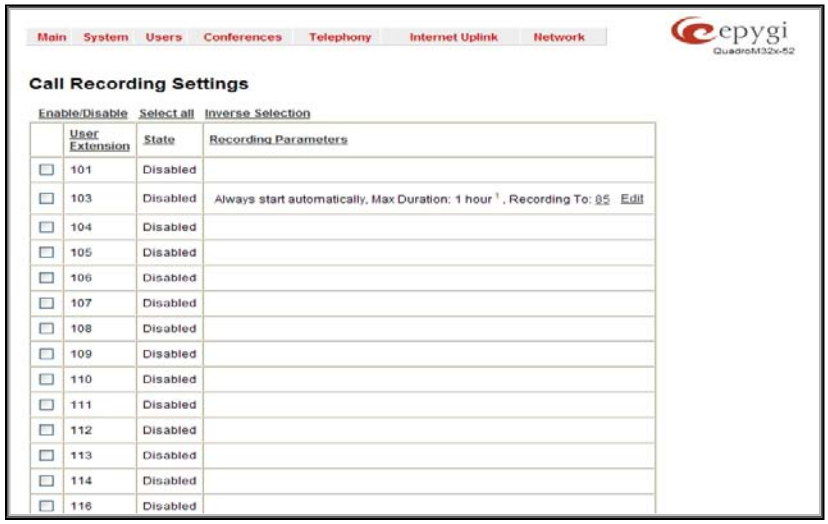


Fig. II-212: Call Recording Basic View Settings page

The **Call Recording Settings** table offers the following functions:

Enable and **Disable** functional buttons are used to activate and deactivate the selected call recording rule(s). At least one rule should be selected in order to use these functions, otherwise the following error message will appear: "No record(s) selected."

Add functional button opens the **Add Entry** page where a new call recording rule is being configured. The **Add Entry** page consists of the following components:

The **Caller Information** requires the **Call Type** and the caller's **Address**.

The **Called Party Information** consisting of the **Call Type** and the called party's **Address**.

The **Call Type** lists the available call types:

PBX - indicates that the calling or called party is QX1000 extension

SIP - indicates that the calling or called party is located in SIP network external to QX1000.

PSTN - indicates that the calling or called party is located in PSTN network external to QX1000.

Auto - indicates any of the types listed above.

The value in the **Address** text field is dependent on the **Call Type** defined in the same named drop down list. If the **PBX** call type is selected, the QX1000 extension number should be defined in this field. For the **SIP** call type, the SIP address should be defined, for the **PSTN** call type, the PSTN user number should be defined here. In case of **Auto** call type, any of the addresses listed above are allowed. Wildcards are applicable for this field.

The **Recording Type** drop down list allows you to select whether the recording will start automatically as soon as the call is established, or whether it will be activated manually by pressing the button on the phone during the call.

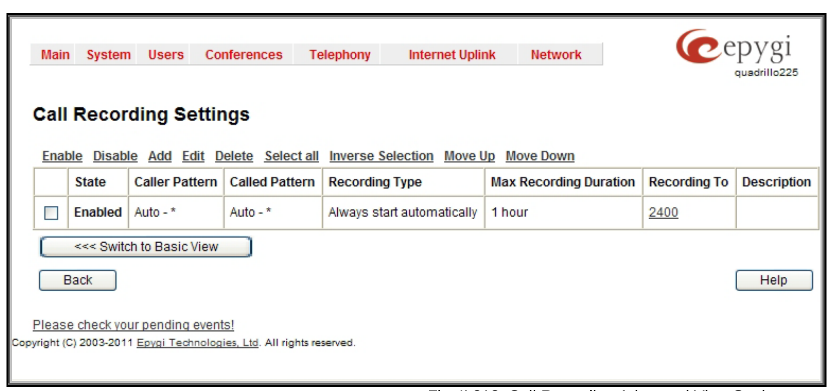


Fig. II-213: Call Recording Advanced View Settings page

The **Maximum Recording Duration** drop down list is used to select the maximum duration when the call between the defined caller and called parties will be recorded. When the call recording duration expires, it will be silently stopped while the call will stay active.

The **Recording To** drop down list is for selecting the Recording Box extension Extensions Management) to be used for storing the recordings.

The **Description** text field should contain some descriptive text related to recording rule.

Fig. II-214: Call Recording Settings – Add Entry page

Edit opens the **Edit Entry** page to modify the selected entry. This page contains all the same components as the **Add Entry** page does.

Delete removes the selected entries. **Select all** checks all entries, e.g. in order to be deleted.

Inverse selection inverses the current selection (if no records are selected, clicking on inverse selection will check all records).

Internet Uplink Menu

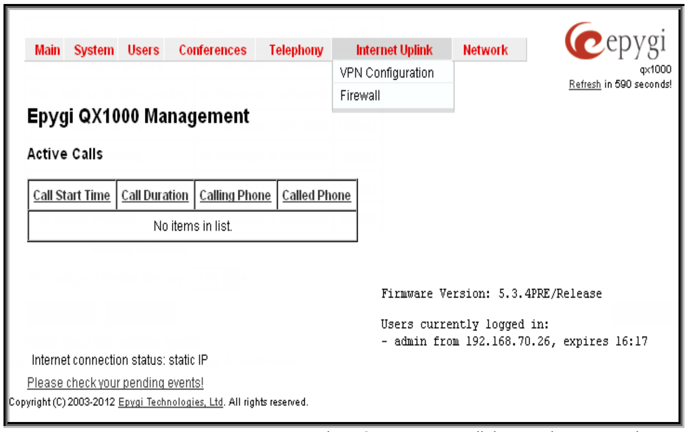


Fig. II-215: Internet Uplink menu in Dynamo theme

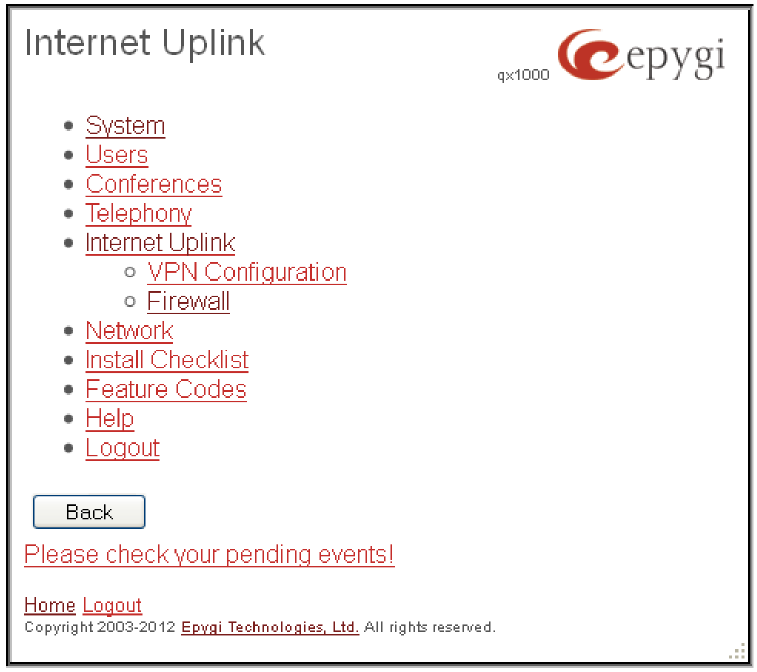


Fig. II-216: Internet Uplink menu in Plain theme

Firewall

The **Firewall Configuration** page allows setting up a firewall and configuring the security level.

A **Firewall** is a security service configured by the QX1000 administrator based on various criteria. The firewall allows or blocks traffic based on policies, services and/or IP addresses. The firewall has several levels of security policies (low, medium or high). The administrator may add additional service-based rules. Filtering rules will take effect only if the Firewall has been enabled and are independent from the selected firewall security level.

The **Firewall Configuration** page offers the following components:

The **Enable Firewall** checkbox selection enables the firewall security service. The firewall security level has to be selected, otherwise the firewall cannot be enabled.

The **Firewall Security** radio buttons are the following:

- **Low Security** - Everything that is not explicitly forbidden will be allowed. This security level doesn't block anything by default. It is recommended if the device is already located behind another firewall or if every filter has been configured correctly.
- **Medium Security** - Traffic originating from the LAN side may pass and traffic from the WAN side will be blocked by default. This is the recommended security level.
- **High Security** - Everything that is not explicitly allowed will be blocked, including traffic from the LAN side.

The Advanced Firewall Settings link refers to the page where QX1000's privacy can be configured.

The **View Filtering Rules** link opens the Filtering Rules page.

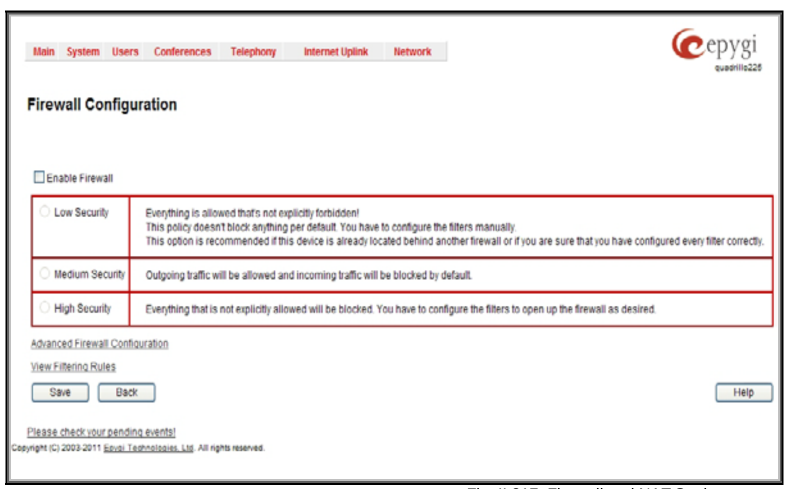


Fig. II-217: Firewall and NAT Settings page

Advanced Firewall Settings

Advanced Firewall Settings are used to deny Ping operation addressed towards the device. With this feature enabled, QX1000 will answer with inscrutable messages to the Ping operation.

Please Note: Operation is available only when the firewall is enabled from the Firewall page.

This page offers the following components:

The **Ping Stealth** checkbox selection prohibits a Ping operation toward QX1000 from its WAN.

Attention: Any changes applied in this page force a restart of the firewall, which might take a few seconds.

Fig. II-218: Advanced Firewall Settings page

Filtering Rules

The **Filtering Rules** page allows you to configure the filters for incoming and outgoing traffic.

To prevent inaccurate configuration, only one rule per service is allowed. The user may use IP groups to include several IP addresses for this rule. Since the filtering rules specify the operation mode of the firewall, they only take effect if the firewall has been enabled. The filtering rules are independent from the security level, so they will work if enabled, no matter what security level has been selected.

Please Note: Applying firewall rules will prevent the establishment of new connections that violate the rules. Applying rules does not kill existing connections that violate the rule.

Attention: The newly created blocking filtering rules will take effect immediately if there is no any active connection matching to that rule. Otherwise, if there is an active connection matching to the created blocking rule, please restart the QX1000 to make the newly created blocking rule effective immediately. However, if you are unable to restart the QX1000, you may need to stop an existing active connection to make the newly created blocking rule effective. Please note, that in this case the blocking rule will take effect only in 3 minutes.

View All displays all configured filters specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**). Since it is read-only, no modifications are allowed and no functional buttons are available.

Management Access is used to enable management access to the QX1000 from the Internet. A host on the Internet can be allowed to reach the QX1000.

Call Control Access is used to enable the access from the call controlling application from the Internet to the QX1000. The call controlling applications can be used to remotely initiate and handle calls on the QX1000 and to subscribe for certain event notifications from the QX1000.

SIP Access is to allow or deny the SIP access to or from the particular SIP servers, SIP hosts or a group of them. The **SIP Access** filtering rule may prevent or allow incoming or outgoing SIP calls to or from specified SIP server(s) or host(s).

When **Blocked IP List** is used, traffic from specific hosts may be blocked, no matter what services are opened in the other filters. NO traffic will be allowed to the specified hosts. The **Blocked IP List** service has a higher priority if the same host is also listed in the **Allowed IP List** table.

Allowed IP List allows trusted hosts to reach your network and vice versa. It is an exception to other rules and only all services may be allowed for a single host.

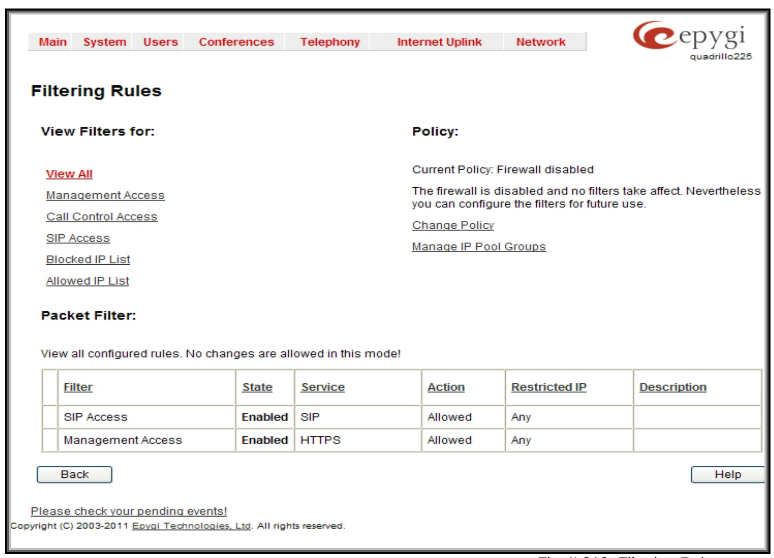


Fig. II-219: Filtering Rules page

The **Filtering Rules** page provides several links. Each link opens its specific parameters on the same page. Only **Change Policy** (see chapter), and **Manage IP Pool Groups** (see chapter IP Pool) lead to separate pages. The **Filtering Rules** page also includes the currently selected firewall security (**Policy**) level and its description.

The table displayed on the bottom of this page shows the filters selected above, specified by their **State** (enabled or disabled), the selected **Service**, the set **Action** (allowed or blocked), the IP addresses the filters apply to (if **Restricted**). With the exception of View All, the table offers the following functional buttons:

- **Enable** is used to enable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Disable** is used to disable the rule. If no records are selected the error message "No record(s) selected" will appear.
- **Add** opens a filter specific page where new rules may be defined by a **Service**, an **Action** to certain IP address(es) or IP groups.

The page to add a rule for **SIP Access** offers the following input options:

Service includes a list of possible services to be configured.

Action includes possible actions to setup the rule.

Restriction radio buttons:

- Selecting **Any** blocks or allows all host IP addresses. This selection is not present for the **Management Access**, **Blocked** and **Allowed IP List** rules.
- Selecting **Single IP** will require the IP address of the allowed or blocked host.
- Selecting **IP/Mask** will require the subnet to be allowed or blocked, specified by an IP address and the Maskbits. The following are **Maskbit** examples:
  255.0.0.0= /8,
  255.255.0.0 = /16,
  255.255.255.0 = /24,
  255.255.255.255= /32
- **Single URL** requires the hostname of the allowed or blocked host.
- **Group** indicates the user-defined groups that include IP addresses that should to be allowed or blocked.

The **Description** field is used to insert an optional description of the filtering rule.

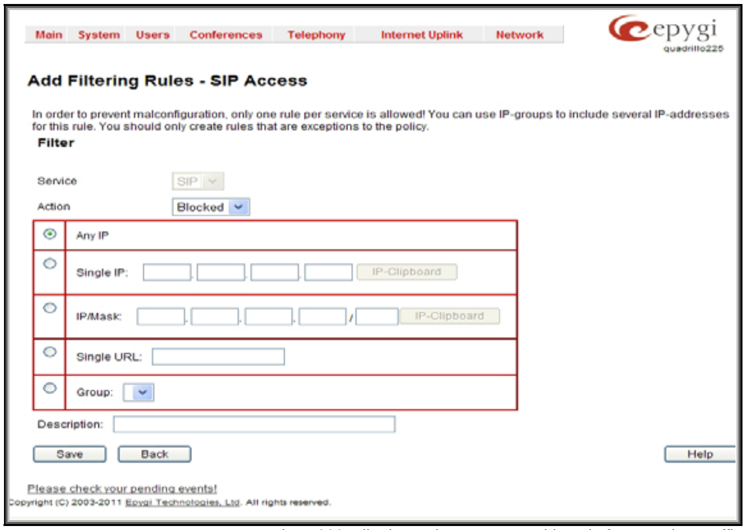


Fig. II-220: Filtering Rules - Page to add a rule for Incoming Traffic

To Add a Filtering Rule

1. Select the **Filter** link (Management Access, Call Control Access, SIP Access, Blocked IP List and Allowed IP List) to add a rule for it. The corresponding **Filter** table will appear in the same window.
2. Click **Add** on the **Filtering Rules** page. A page where a new rule may be added will appear in the browser window. The page will be named corresponding to the selected filter.
3. Select a service name from the **Service** list to configure a rule for it. If the list has a default value, do not change the default values.
4. Select an action from the **Action** list that is used in the rule. If the list has a default value, do not change the default values.
5. 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.
6. Insert a **Description**, if needed.
7. To add a rule with these parameters, press **Save**.

To Delete Filtering Rules

1. Select the **Filter** link to delete a rule from its table. The appropriate **Filter** table will appear in the same window.
2. Check one or more checkboxes of the corresponding rules that should be deleted from the rules table. Press **Select all** if all rules should to be deleted.
3. Press the **Delete** button on the **Filtering Rules** page.
4. Confirm the deletion by clicking on **Yes**, or cancel by clicking on **No**.

IP Pool

The **Manage IP Pool Groups** link opens the **IP Pool Configuration** page.

The **IP Pool** table is the list of all added groups and the members assigned to these groups. If a group is empty, **EMPTY** will be indicated in the **Members** column. If hidden, group members will still remain active but **HIDDEN** will be displayed in the **Members** column.

The **IP Pool Configuration** is used to add groups of IP addresses that have the same restriction criteria. When adding a new filtering rule, groups may be used instead of several IP addresses. **IP Pool Configuration** offers the following components:

View makes hidden groups visible.

Hide makes group members hidden and adds the **HIDDEN** comment in the member column.

Fig. II-221: IP Pool Configuration page

Add opens the **Add Group** page where a new group may be added. This page consists of the **Group Name** text field (requiring the group name) and the **Group Description** text field (requiring the optional group description), as well as standard **Save** and **Back** buttons to apply or abort changes.

Edit opens the **Edit Group** page where the service parameters can be modified. It provides the same components as the **Add Group** page. To operate with **Edit**, only one record may be selected, otherwise the error message “One row must be selected” will appear.

Please Note: Changing a group name will also change the references to this group, including groups where this group is a member of, and all affected filter rules (enabled and disabled ones, in all chains). Deleting a group will also delete any reference to the corresponding group, including filter-rules and member relations to the other groups.

Clicking on the **Group** name will display an **IP Pool Group Configuration** page with the **Members** list for the current group.

Fig. II-222: IP Pool configuration – Add Group page

The **IP Pool Group Configuration** page displays a list of all the added member IP addresses for the selected group. It offers the following components:

Fig. II-223: IP Pool Group Configuration page

Current Group provides read-only information about the current group name the members are listed for.

Add opens the **Add Member** page where a new member may be added.

Edit opens the **Edit Members** page where the service parameters can be modified. This page includes the same components as the **Add Member** page. To operate with **Edit**, only one record may be selected, otherwise the error message "One row must be selected" will appear.

The **Add Members** page provides the following radio buttons:

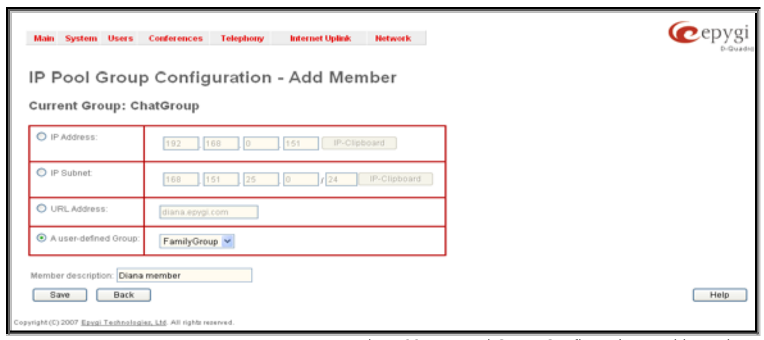


Fig. II-224: IP Pool Group Configuration – Add Member

IPaddress requires the member IP address that is to be added to the group.

IP Subnet requires the subnet specified by the IP address and the Maskbits. See above for more information about Maskbits.

URL Address requires the member hostname to be added to the group.

The **User-defined Group** includes previously added groups that may also be added as a member to another group.

Member description text fields can be used to enter an optional description of the member.

To Add a new Group with Members

1. Select the **Manage IP Pool Groups** link on the **Filtering Rules** page.
2. Click on the **Add** button on the **IP Pool Configuration** page. A page where a new group may be added will appear in the browser window.
3. Define a group name in the **Group Name** text field and fill in the **Group Description**, if needed.
4. To add a group with the given parameters, press **Save**.
5. Open the **IP Pool Group Configuration** page by clicking on the group name.
6. Select the **Add** button on the **IP Pool Group Configuration** page. A page opens where new members may be added to the group.
7. Enter an IP address for the member in the **IP Address** text fields, select a IP subnet or IP group from the **User defined Group** drop down list to assign it to the currently selected group.
8. Enter a **Member Description** in the corresponding text field, if needed.
9. To add a member with these parameters to the selected group press **Save**.

To Delete a Member

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Click on the desired members that should be deleted. The **IP Pool Group Configuration** list will appear.
3. Check one or more checkboxes of the corresponding members that should be deleted from the **Members** table. Press **Select all** if all members should be deleted.
4. Press the **Delete** button on the **IP Pool Group Configuration** page.
5. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

To Delete a Group

1. Select the **Manage IP Pool Groups** link. The **IP Pool Configuration** page appears with the table of groups (if any).
2. Check the one or more checkboxes of the corresponding groups that should be deleted from the groups table. Press **Select all** if all groups should be deleted.
3. Press the **Delete** button on the **IP Pool Configuration** page.
4. Confirm the deletion by pressing on **Yes** or cancel the deletion by pressing on **No**.

Network Menu

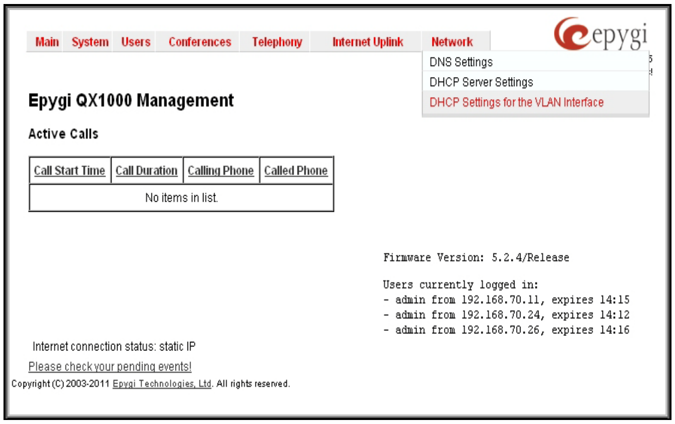


Fig. II-225: Network menu in Dynamo theme

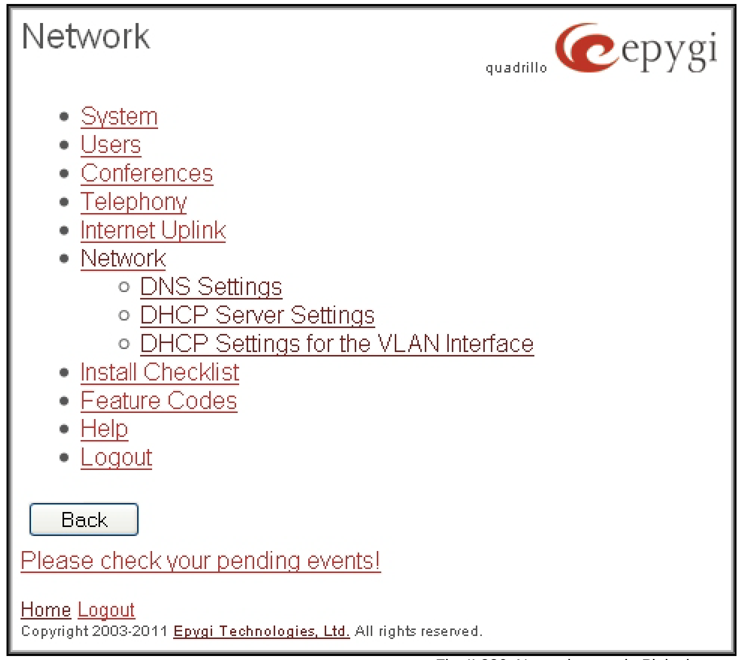


Fig. II-226: Network menu in Plain theme

DNS Settings

The **DNS Settings** page provides the option of setting up a name server for the QX1000. It offers the following components:

- The **Nameserver** text field requires the IP address of an external name server.
- The **Alternative Nameserver** text field requires the IP address of the secondary name server. The **Alternative Nameserver** is used if the main name server cannot be accessed.

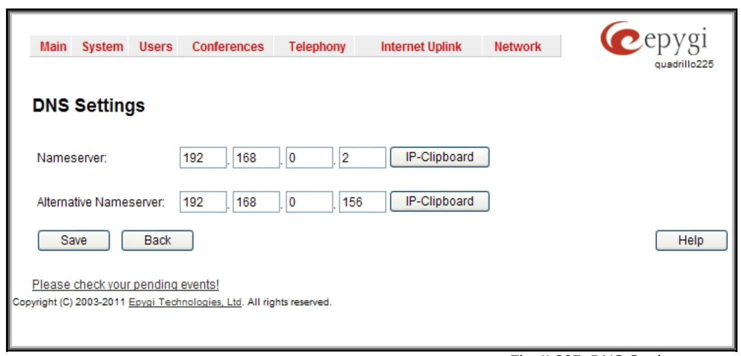


Fig. II-227: DNS Settings page

DHCP Server Settings

The **DHCP Server Settings** page provides the option of enabling a DHCP server and controlling the QX1000 user's LAN settings. Therefore, QX1000 LAN users will automatically be provided with the following settings using the configured parameters:

- IP addresses
- NTP (corresponds to the QX1000's IP address)
- WINS server
- Nameserver (corresponds to the QX1000's IP address)
- Domain name

The **DHCP Server Settings** page offers the following input options:

Enable DHCP Server checkbox activates the DHCP server on QX1000. With this checkbox enabled, QX1000 will be able to assign dynamic IP addresses to the devices in its LAN.

Give leases only to hosts listed in the static MAC address binding table checkbox enables the DHCP services only for the devices listed in the table below. With this checkbox selected, no DHCP services will be provided to the other devices.

Please Note: When this checkbox is selected, all IP phones configured to use plug and play or auto configuration services (see Line Settings) will keep their IP addresses received from the DHCP server of the QX1000. The IP phones that are configured manually should be added to the **Special Devices** table to keep their IP addressed.

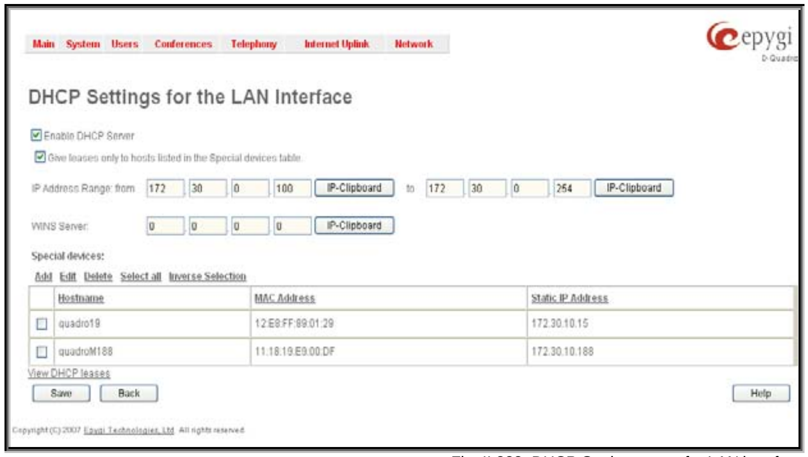


Fig. II-228: DHCP Settings page for LAN interface

IP Address Range defines a range of IP addresses that will be assigned to the QX1000 LAN users. The IP range must be at least 6, otherwise the error message “Address Range too small” will prevent it from being saved. The error message “Address Range too large” will appear if the IP range is greater than 254.

WINS Server defines a WINS server IP address for the QX1000 LAN users.

DHCP Advanced Settings link leads to the page where the advanced options of the QX1000's DHCP server can be configured.

The **Special Devices** table on this page allows you to set a static IP address binding on the MAC address of the device in the QX1000’s LAN. When this table is configured, the devices with defined hostnames and MAC addresses will always get the same LAN IP address from the DHCP server. Otherwise, devices not listed in this table will get dynamic LAN IP addresses. This table is also displayed in the System Configuration Wizard.

Add functional button opens an **Add Host** page where a new static MAC address binding can be defined. The page consists of the following components:

Hostname text field requires the hostname of the device in the QX1000’s LAN.

MAC Address text fields require the MAC address of the device in the QX1000’s LAN.

Static IP Address text fields require a fixed IP address of the device in the QX1000’s LAN.

Please Note: If you leave this field empty, the device in the QX1000’s LAN will get the first available IP address from range defined in the **DHCP Settings** page (see above).

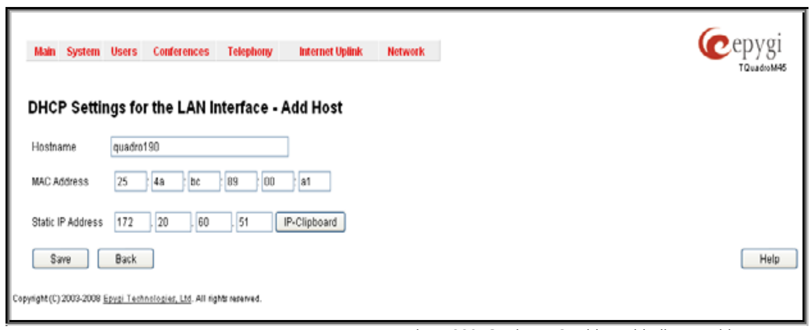


Fig. II-229: Static MAC address binding – Add Host page

View DHCP Leases leads to the page where the DHCP leased LAN IP addresses are listed.

The **DHCP Leases** page includes a list of the leased host addresses that are part of the QX1000’s LAN. For these hosts, QX1000 acts as a server supplying them with a unique IP address. It displays a read-only table describing all the leased IP hosts and their parameters. The table contains the following columns:

IP address - host IP address, assigned by QX1000.

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.

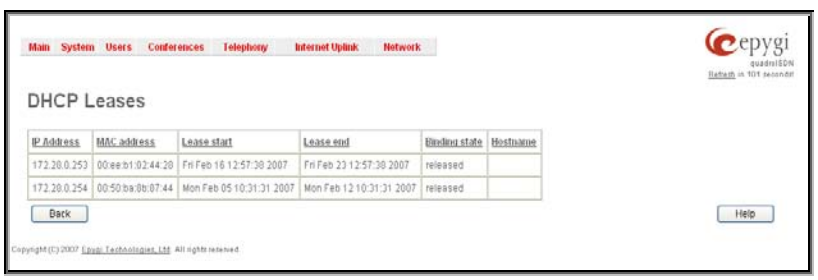


Fig. II-230: DHCP Leases page for LAN interface

DHCP Advanced Settings

The **DHCP Advanced Settings** page is used to modify the advanced options of the DHCP server on the QX1000. This page contains a table where a list of default DHCP server options is already defined. More options can be added from this page, as well as settings of the existing options can be modified. All options in the table on this page are then sent to the DHCP clients.

- The **Authoritative** checkbox is used to enable/disable authoritative mode on the QX1000 DHCP server. Disabling the checkbox is recommended if several DHCP servers are used on the network and the QX1000 should provide network parameters to IP phones only.

- The **Ping Check** checkbox enables checking the availability of an IP address on the network before providing it to a client. If this checkbox is selected, the QX1000 will first ping an IP address retrieved from the IP pool and wait for a reply. If no a reply is received within a timeout specified in the **Ping timeout** text field (by default 1 sec), the retrieved IP address will be provided to the client. If otherwise, a new IP address will be retrieved from the IP pool and the procedure will be repeated. If this checkbox is not selected, the QX1000 will provide an IP address immediately when requested.

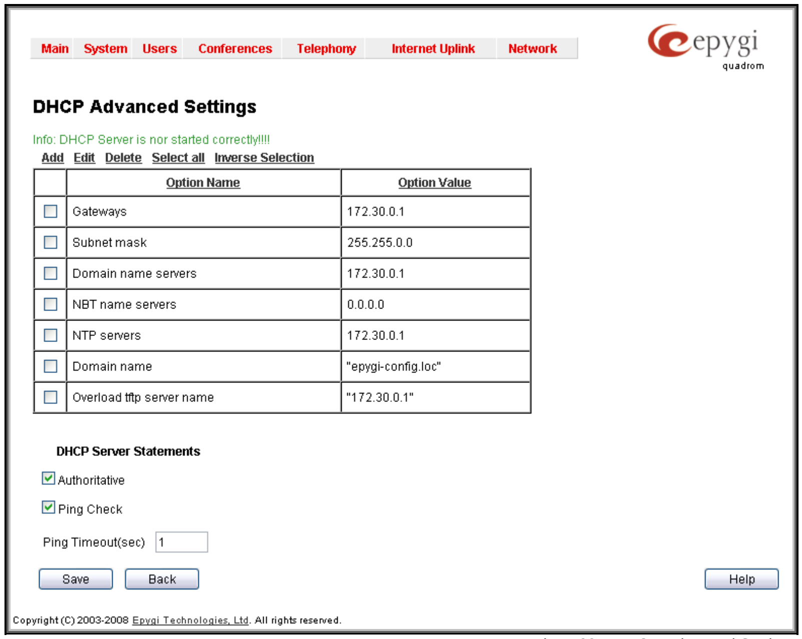


Fig. II-231: DHCP Advanced Settings

The following functional buttons are available for managing DHCP options:

Add opens a page **Add Entry** page where a new DHCP server option can be defined. The Add Entry page contains a group of manipulation radio buttons to select between the predefined DHCP server options or to define your own DHCP server option:

- **Predefined** - this selection allows you to select from the predefined DHCP server options.

  The **Option Name** drop down list contains the most common DHCP server options.

  The **Option Value** text field requires the value for the selected option. The type and format of the value inserted in this field is dependent on the option selected from the Option Name drop down list.

- **Custom** - this selection allows you to define a new DHCP server options. The following parameters are required to be inserted for a new option:

  The **Option Code** text field is used to insert a code of the option. It may have values in a range from 0 to 255.

  The **Option Value** Type drop down list is used to select the type of the option value. It may be an IP address, a boolean or integer value, etc.

  The **Option Value** text field is used to insert the value of an option. Depending on the selected Option Value Type, this field should have the corresponding value. Warning messages will prevent saving if the value inserted in this field does not correspond to the requirements of the Option Value Type. If an array should be inserted here, the values should be separated with a comma.

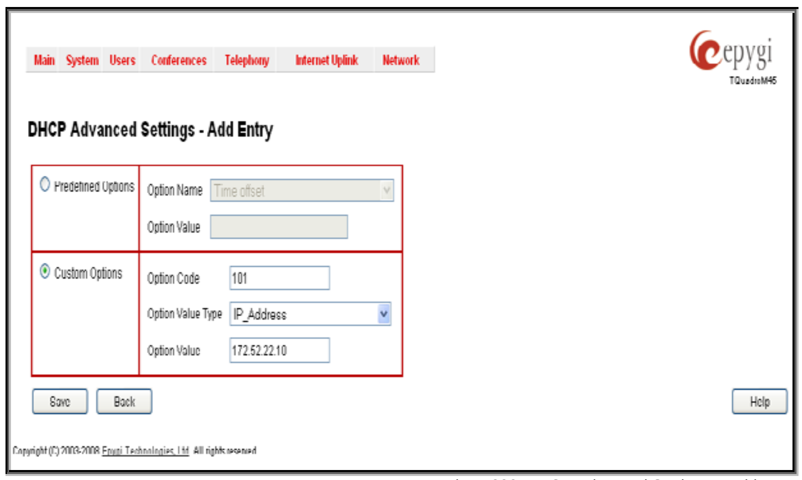


Fig. II-232: DHCP Advanced Settings – Add Entry

DHCP Settings for the VLAN Interface

DHCP Settings for the VLAN Interface is used to establish virtual networks in the QX1000's LAN or to integrate the QX1000 into the corporate network's virtual LAN/WAN. DHCP service can be activated both on virtual LAN or WAN interfaces. VLAN is useful in corporate companies to divide large networks into groups and to have devices like QX1000s and IP phones in each network separated (for example, to separate networks for data and voice transmission). Priorities may be assigned to the interfaces for packets prioritization.

With VLAN configuration, each virtual network will be characterized with a VLAN ID (tag). Packets addressed to that network will be checked towards the ID and if the ID number defined in the incoming packets matched the corresponding network's ID, the packets will be accepted. Otherwise, if the ID does not match, the packets will be dropped. In the same way, if the QX1000 is integrated into the network that uses VLAN technology, outgoing packets should have the ID number of the corresponding virtual network, for the remote party to accept the packets from the QX1000.

The **DHCP Settings for the VLAN Interface** page contains a table with all enabled VLAN interfaces created in VLAN Settings page (see below) and the corresponding parameters (VLAN ID, IP Address Range and WINS Server). This page contains the following components:

Enable DHCP Server checkbox activates the DHCP server on QX1000 for VLAN. With this checkbox enabled, QX1000 will be able to assign dynamic IP addresses to the devices in its VLAN.

Activate functional button is used to activate DHCP service on one of the VLAN interfaces in the list. Only one VLAN interface can have DHCP service activated.

Edit functional button opens a page where the corresponding VLAN interface can be configured and controlled. This page contains all the same components as the DHCP Server Settings page does.

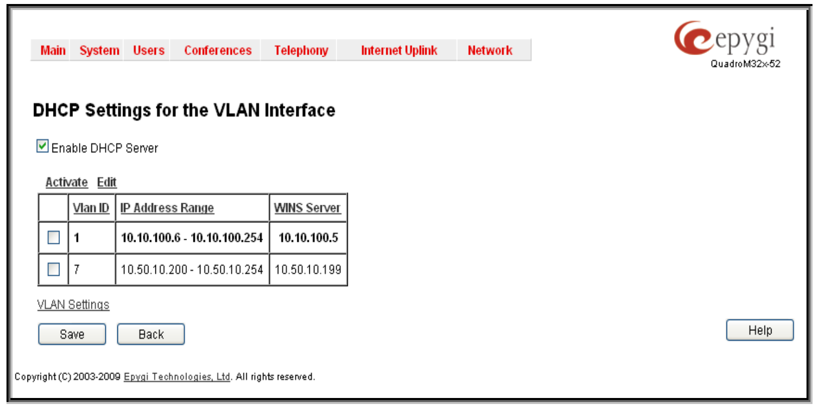


Fig. II-233: DHCP Settings page for VLAN interface

VLAN Settings link moves to the page where virtual LAN/WAN interfaces may be created.
VLAN Settings page lists all existing virtual interfaced created on the QX1000 and allows you to create new interfaces.
Enable and **Disable** functional buttons are used to correspondingly enable and disable the selected virtual interface(s).

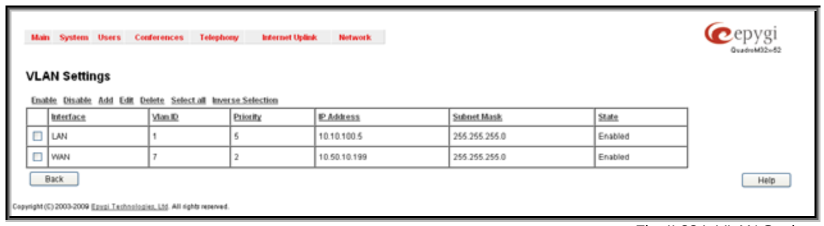


Fig. II-234: VLAN Settings

Add functional button opens an **Add Entry** page where a new virtual network can be defined. The page consists of the following components:

Enable checkbox is used to select whether the corresponding virtual interface will be enabled or disabled after it is created.

Interface Type manipulation radio buttons selection allows to choose whether the virtual interface will be LAN or WAN.

VLAN ID text field requires the virtual network ID. Numeric value in a range from 0 to 4094 is allowed in this field.

Priority drop down list is used to select the priority of packets in the corresponding interface. Packets with the lower priority (0) will be delivered first.

IP Address text field requires the IP address of the virtual interface.
Subnet Mask text field requires the subnet of the virtual interface.

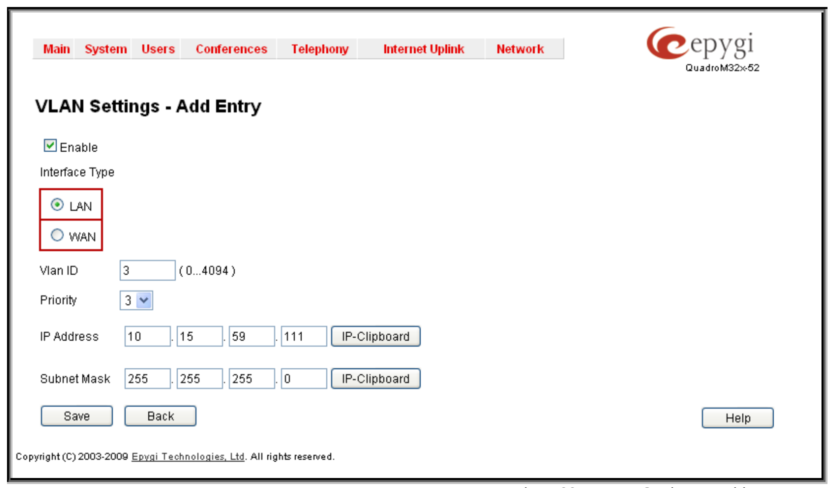


Fig. II-235: VLAN Settings – Add Entry page

Registration Form

The **Registration Form** page appears when administrating an unregistered QX1000 and it has been created for customer support purposes. The page requires customer registration at the Epygi Technical Support Center. It provides several links offering the following registration options:

Register now leads to the Epygi Technical Support System Registration page and requires customer's information to submit the QX1000 registration form.

Remind me later hides the registration notification in the QX1000 through System Configuration Wizard or Uplink Configuration Wizard until the next administrating activities.

Fig. II-236: Device Registration page

Don't remind me more hides the registration notification forever.

Administrator's Additional Features

Incoming Call Blocking and Outgoing Call Blocking

The **Incoming Call Blocking** and **Outgoing Call Blocking** pages offer extended features for the administrator to activate incoming/outgoing call blocking services for certain callers. The users cannot change this information.

For more information on the **Call Blocking Settings** pages, see the Incoming Call Blocking and Outgoing Call Blocking chapters of the Extensions Users Guide - Manual III.

The **Call Blocking** pages accessed from the **Caller ID Based Services** table by clicking on the corresponding address, gives the administrator the option to enable blocking services which could not be disabled by the users.

Along with the components seen by the user, an additional **Protect this entry** checkbox is available in the **Call Blocking - Add Entry** pages for administrator access only. With this checkbox selected, the user will be unable to deactivate the blocking services configured by the administrator.

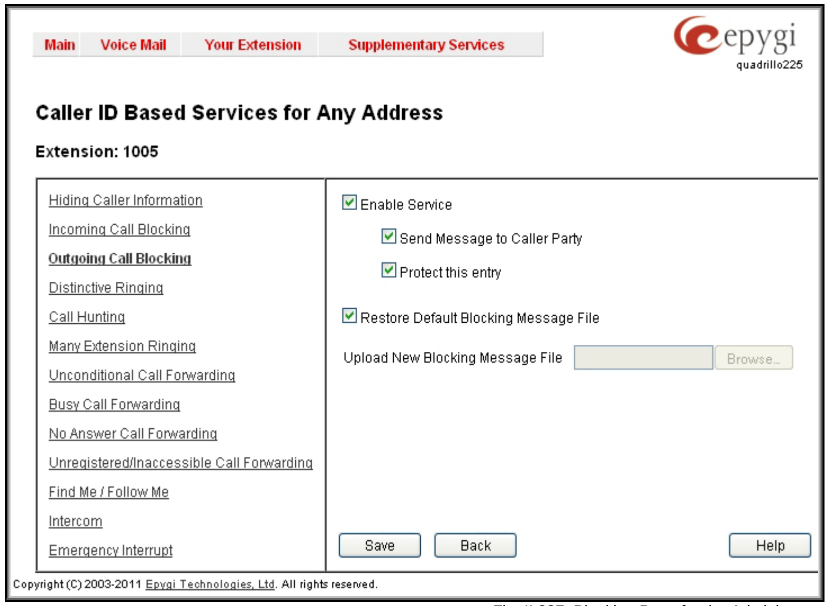


Fig. II-237: Blocking Page for the Administrator

Voice Mail Profiles

When the administrator accesses the **Voice Mail Settings** of an extension, there is an additional **Voice Mail Profiles** link present that leads to the page where custom voice mail profiles and their settings can be defined. This link is hidden for the extension user's access.
The **Voice Mail Profiles** page is used to define and configure custom voice mail profiles.

The **Voice Mail Profile** is a group of most common Voice Mail Settings which can be saved under a specific name. This allows you to have several versions of Voice Mail Settings configurations per extension.

Each Voice Mail Profile may have custom voice mail greeting, maximum voice mail duration, new voice mail notifications and Zero-Out settings. The Voice Mail Profiles are activated based on the call routing rule used to establish a call. This is limited to the **PBX-Voicemail** type of calls used for a direct access to the extension's voice mailbox. The Voice Mail Profile name should be provided in the Call Routing wizard when defining a PBX-Voicemail routing rule. When the rule is used, caller accesses the called extension's mailbox with the settings configured in the corresponding voice mail profile.
With this service, you can pre-configure several versions of Voice Mail Settings and save them as Voice Mail Profiles. For example, if a call is originated from the PSTN network to the corresponding extension's voice mailbox, the greeting message can tell the caller: "You have reached the ... company, please leave a message." and the maximum voice mail duration is configured to 15 minutes. This voice mail profile can be saved as "ForPSTN" and its name should be defined in the routing rule responsible for incoming PSTN calls distribution. In parallel to this voice mail profile, there can be another profile designed for internal PBX calls. It will play the following voice mail greeting: "Hi, you have reached Mike's voice mailbox, please drop me a message and I shall call you back.", the maximum voice mail duration is 5 minutes and there is a Zero-Out feature configured to call Mike's cellular phone. This voice mail profile can be saved as "ForPBX" and its name should be defined in the routing rule responsible for PBX calls distribution to the local extensions.

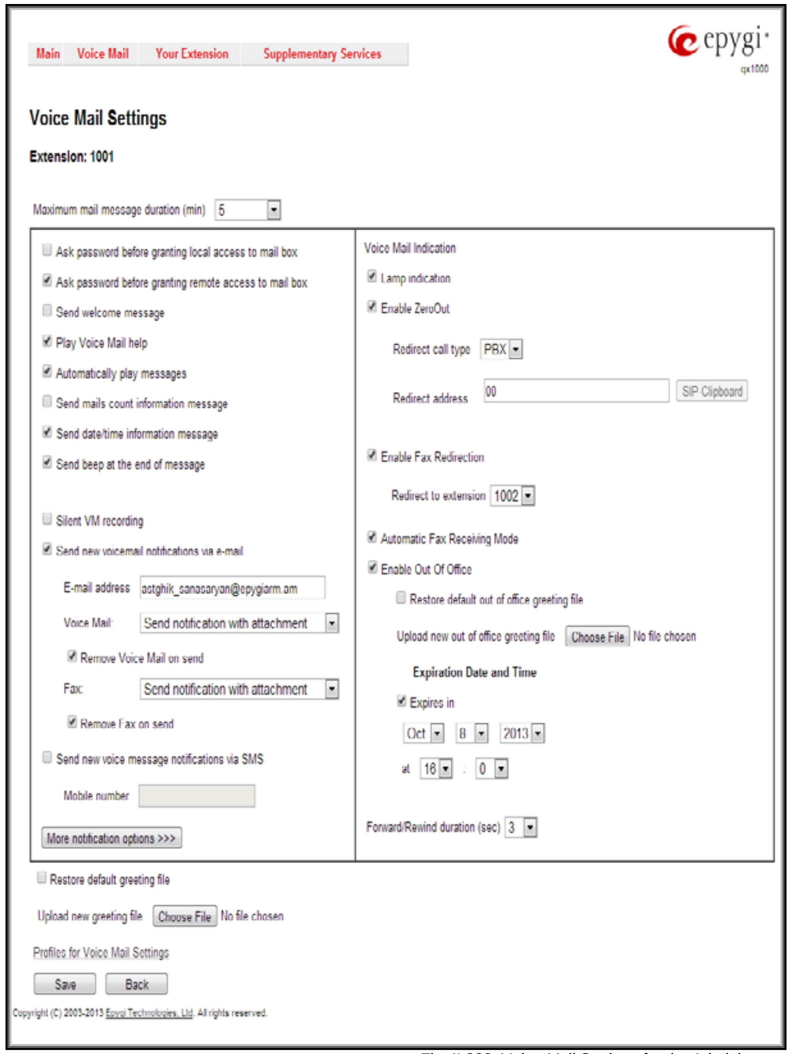


Fig. II-238: Voice Mail Settings for the Administrator

When the first routing rule is used and the call reaches the extension that has the corresponding voice mail profile, the settings of the ForPSTN voice mail profile will be activated. For the second routing rule, when the call reaches Mike's voice mailbox, the settings of the ForPBX voice mail profile will be activated.
The same profile name can be used to create profiles for different extensions. This is useful if the profiles have a similar purpose but differ in certain user-specific settings, such as voice mail greeting, Zero-Out destination number, new voice mail notification options, and so on. Creating multiple profiles with the same name gives a wide flexibility to have different voice mail settings activated depending on which extension is called.

Please Note: If an extension does not have a profile specified in a call routing rule or the specified profile name is incorrect, the default Voice Mail Settings of the extension will be used.

The **Voice Mail Profiles** page contains a table where all Voice Mail Profiles for the corresponding extension are listed. The following functional buttons are available:

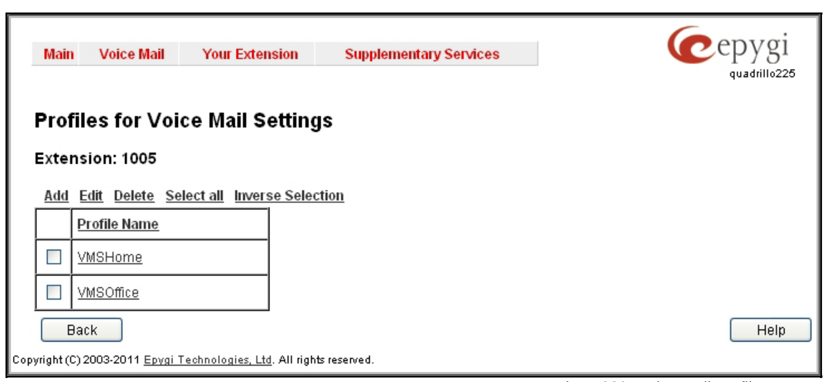


Fig. II-239: Voice Mail Profiles page

Add opens the **Add Entry** page where a new **Profile Name** should be defined.

Edit opens the **Edit Entry** page where **Voice Mail Profile** settings should be defined.

The **Voice Mail Profiles - Edit Entry** page is used configure the profile specific voice mail settings. This page contains the following components:

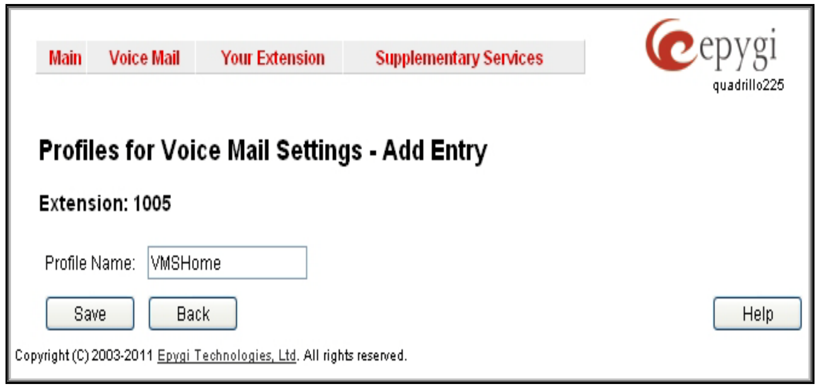


Fig. II-240: Voice Mail Profiles – Add Entry page

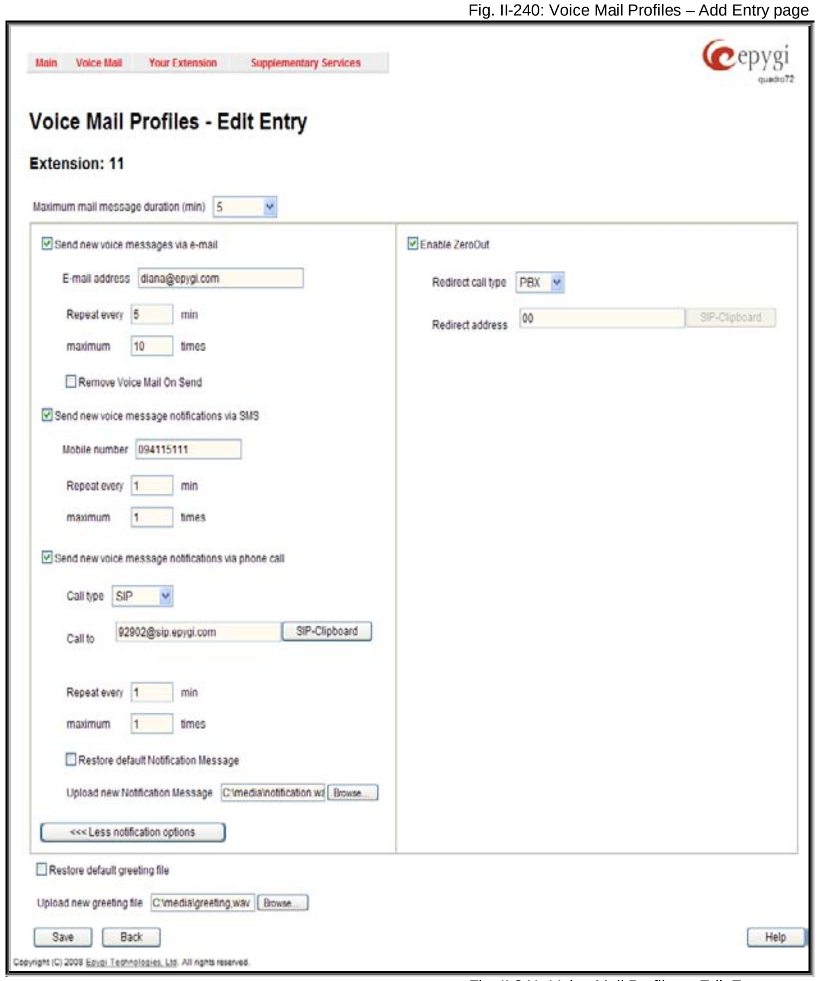


Fig. II-241: Voice Mail Profiles – Edit Entry page

Maximum Mail Message Duration lists the possible values for maximum mail duration (counted in minutes) during which a voice mail will be recorded. The **Unlimited** selection allows voice message to be recorded as long as the user's space could hold.

Send new voice message via email is an option to send new voice mail files via e-mail to the defined recipients. Mails will be automatically converted to the PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format before being attached to the e-mail. Checkbox activates the following input options:

- **Email Address** requires the mailing address(s) of the person(s) that should to receive the newly arrived voice mails on their email accounts. Use a space or a comma to separate the mailing addresses in the text field.
- The next two fields are used for retransmission of voice mails via email. **Number of times** text field requires the maximum number of times the voice mail will be delivered via email to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If the voice mail is required to be sent only once, insert "1" in **Repeat every** text field and "0" in the Number of times text field.
- The **Voice Mail** and **Fax** dropdown lists allow to select the email sent options- do not send notification, send notification without attachment or send notification with voice or fax attachments.
- **Remove Voice Mail on send** removes the voice mail from the user mailbox after sending it to the email recipient(s).
- **Remove Fax On Send** removes the fax attachment from the user mailbox after sending it to the email recipient(s).

Attention: The e-mail can only handle up to 3 minutes long voice mails. If the voice mail is longer than 3 minutes, it will be truncated and only the first 3 minutes of it will be sent to the indicated e-mail address. However, in the e-mail body the recipient will receive the information that the attached voice mail is truncated and the total length of the voice mail. Please note that the voice mails longer than 3 minutes will not be removed from the voice mailbox once they are sent per e-mail even if the **Remove Voice Mail on send** checkbox is selected. This gives you a possibility to listen to the ending of the voice mail directly from your voice mailbox (from the handset or by downloading it from the Web management).

Please Note: This service will work only when System Mail is enabled on the QX1000 (see Mail Settings). Contact your system administrator, if you have problems with voice mail delivery via email.

Send new voice message notification via SMS allows voice mail notification delivery via SMS to the defined mobile number. Checkbox activates the following input options:

- **Mobile Number** text field requires the destination's mobile number.
- The next two fields are used for retransmission of SMS notifications. The **Number of times** text field requires the maximum number of times the notification should be delivered to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If notification is required to be sent only once, insert "1" in **Repeat every** text field and "0" in the **Number of times** text field.

Please Note: This service will work only when SMS Service is enabled on the QX1000 (see SMS Settings). Contact your system administrator, if you have problems with voice mail notifications delivery via SMS.

Send new voice message notification via phone call enables the voice mail notification delivery via phone call to the defined phone number. The checkbox activates the following input options:

- **Call Type** drop down list includes the available call types:
  PBX - local calls to QX1000 extensions;
  SIP - calls through a SIP server;
  Auto - for undefined call types. Destination (independent on whether it is a PBX number or SIP address) will be reached through Routing;
  Callback - automatic call to the voice mail author. This can be used as notification that the recipient has received the voice mail but has not yet played it.
- **Call To** text field requires the destination's phone number depending on the selected call type. For Callback call type, no destination's phone number is required.
- The next two fields are used for retransmission of phone notifications. The number of times text field indicates the maximum number of times the notification should be delivered to the recipient within the interval (in minutes) defined in the **Repeat every** text field. If the notification is specified to be sent only once, insert "1" in **Repeat every** text field and "0" in the Number of times text field. For **Callback** call type, the first notification is sent to the voice mail author after the first expiration of the interval defined in the **Repeat every** text field. For calls with call type different from Callback, the first notification will be sent immediately.
- **Restore default Notification Message** restores the default notification message. If the checkbox is selected, the file upload will be disabled.
- **Upload new Notification Message** will show the attached notification file selected by the current extension. Please note that a different notification message can be uploaded in case this service serves as a notification to the extension user (to inform about the new voice mail received) or if it serves as a notification for the voice mail author to be informed that the message has been received by the QX1000 but is not yet played by the extension user). The uploaded file needs to be in the PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading with the "Invalid audio file, or format is not supported" warning message. The system also prevents uploading in case not enough space is available on QX1000 for the corresponding extension and gives a "You do not have enough space" warning.
- **Browse** browses for the notification file that must be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format.
- **Download Notification Message** appears only if a file has been uploaded previously. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.
- The **ZeroOut** voice mail feature allows a caller that has reached the called extension's voice mailbox to accelerate the automatic redirection feature instead of leaving a message in the extension's Voice Mailbox. To activate this feature, the caller should dial **0** digit (see Feature Codes) during the voice mail greeting which invites the caller to leave a message. The caller will then be automatically transferred to the destination specified in this page.

Enable ZeroOut checkbox selection enables the ZeroOut feature and activates the following fields to be inserted:

- **Redirect Call Type** drop down list includes the available call types:
  PBX - local calls between QX1000 extensions and the Auto Attendant
  SIP - calls through a SIP server
  PSTN - calls through the FXO/ISDN
  Auto - used for undefined call types. Destination (independent on whether it is a PBX number, SIP address or PSTN number) will be reached through Routing.
- **Redirect Address** text field requires the destination address where caller should be automatically forwarded in case of activating the ZeroOut feature.

Restore Default Greeting File will restore the default greeting file. If the checkbox is selected, the file upload will be disabled.
Upload New Greeting File shows an attached greeting file selected by the current user. The greeting file will be played to a caller party when it is entering the voice mail system. The uploaded file needs to be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format, otherwise the system will prevent uploading and the "Invalid audio file, or format is not supported" warning message will be received. The system also prevents uploading in case not enough space is available on QX1000 for the corresponding extension. In this situation, the "You do not have enough space" warning will be received. Optionally, greeting file can be recorded from the phone handset (see Feature Codes).
The **Browse** button helps to choose the desired greeting file that should be in PCMU (CCITT u-law, 8 kHz, 8 bit Mono) wave format.
Download Greeting File appears only if a file has been previously uploaded. The link is used to download the audio file to the PC and opens the file-chooser window where the saving location can be specified.

Logout

This option is used to close the session between the user PC and QX1000 and to leave the QX1000 Web Management or to enter the management with another login. By selecting the **Logout** button, the startup page will be displayed and the user needs to login again.

Appendix: PBX Services for QX1000's Administrator

The following **PBX Services** are accessible at the dial tone, characterized by beginning with the key *:

Administrator Login Allows to modify Auto Attendant greeting and menu messages, as well as to manage universal extension messages.	* 7 5
Enabling/disabling the Call Routing rules Allows managing the routing entries in the Call Routing table, i.e. to enable/disable certain dialing rules by dialing key combinations pre-configured on each routing entry. By dialing * 7 7, you will be required to dial enabler/disabler key to enable or disable the routing rule(s) correspondingly. Since multiple routing rules may have the same enabler/disabler key combinations (the same key may be used as enabler for one routing rule, and as disabler for another one), dialing the certain key will affect all pre-configured routing rules. If the routing record has an authorization enabled on the enabler/disabler key, administrator's password will be required to be inserted after the key. Once the administrator's password is dialed, system plays a confirmation about the accepted configuration and the state of the certain routing rule(s) is getting modified. If administrator's password has been inserted incorrectly for 3 times, no status changes will be applied to any of the routing record(s), even to those which have no authorization enabled.	* 7 7

Administrator Login menu has the following sub-menus and the management keys:

* 7 5 Administrator's Login								
1 Auto Attendant Greeting	2 Auto Attendant Menu Message	3 Universal Extension Messages						
Dial **AA Number** (in case of multiple AAs on the QX1000)	Dial **AA Number** (in case of multiple AAs on the QX1000)	1 Greeting Message	3 Incoming Blocking Message	4 Outgoing Blocking Message	5 Your Name	6 Out of Office Message	7 Find Me/Follow Me Welcome Message
1 Listen to Current AA Greeting	1 Listen to AA Menu Message	1 Listen to Current Greeting Message	1 Listen to Current Incoming Blocking Message	1 Listen to Current Outgoing Blocking Message	1 Listen to Current Name recorded	1 Listen to Current Out of Office Message	1 Listen to Current Find Me/Follow Me Welcome Message
2 Record a New AA Greeting	2 Record a New AA Menu Message	2 Record a Universal Greeting Message	2 Record a Universal Incoming Blocking Message	2 Record a Universal Outgoing Blocking Message	2 Record a Universal Name	2 Record a Universal Out of Office Message	2 Record a Universal Find Me/Follow Me Welcome Message
3 Restore Default AA Greeting	3 Restore Default AA Menu Message	3 Restore System Default Greeting Message	3 Restore System Default Incoming Blocking Message	3 Restore System Default Outgoing Blocking Message	3 Restore System Default Name	3 Restore System Default Out of Office Message	3 Restore System Default Find Me/Follow Me Welcome Message
# Stop Recording or Playback	# Stop Recording or Playback	# Stop Recording or Playback Greeting Message	# Stop Recording or Playback Incoming Blocking Message	# Stop Recording or Playback Outgoing Blocking Message	# Stop Recording or Playback Name Message	# Stop Recording or Playback Out of Office Message	# Stop Recording or Playback Find Me/Follow Me Welcome Message
* 0 Administrator's Logout							

Appendix: Conference Services for Moderators and Participants

This chapter describes the feature codes for the Conference Services that enable the moderator and participants to manage call conferences from the phone.

Conference Services accessible during the conference:	Keys
Invite Participant To invite a participant dial *1 + Participant's SIP address (or *1 + Routing Number). Service is available for Moderators only.	* 1
Get the number of participants in the conference Plays information about the total number of participants in the conference at the certain moment.	* 2 1
Get the state of recording Plays the state of conference recording (started, stopped or paused).	* 2 2
Lock the conference Locks the conference. When conference is locked, nobody can dial in any more. Service is available for Moderators only.	* 3 1
Unlock the conference Unlocks the conference. Now participants are allowed to dial in to the conference. Service is available for Moderators only.	* 3 2
Dial out to all users with dial out settings enabled Initiates the dial-out to all participants currently inactive in the conference but configured to be dialed out (also those added manually from the handset by moderator). Service is available for Moderators only.	* 4 1
Dial out to all users participant to the conference Initiates the dial-out to all participants currently inactive in the conference. Service is available for Moderators only.	* 4 2
Next Phone with Video Capability Shows the next phone with video capability. Also switches from automatic mode to manual one.	* 5 0
Previous Phone with Video Capability Shows the previous phone with video capability. Also switches from automatic mode to manual one.	* 5 1
Automatic Video Switching Mode With this key combination, the loudest speaking participant is displayed on all video-capable phones. If that participant has no video capability, a black screen will be displayed.	* 5 2
Start or Resume Conference Recording Service is available for Moderators only.	* 8 1
Pause Conference Recording Service is available for Moderators only.	* 8 2
Stop Conference Recording Service is available for Moderators only.	* 8 3
Request to Speak With this key combination, a listener requests to speak and a notification hand-up icon is displayed in the Conference Progress table. The moderator can then switch the particular listener either to speaker or lecture mode. With a speaker permission granted, listener can speak to the conference along with other participants. With a lecturer permission granted, listener can speak to the conference having all other participants muted in the conference. This service is available for listener participants only.	* 9 1
Cancel the Request to Speak With this key combination, listener cancels his request to speak and a notification hand-up icon disappears from the Conference Progress table. This service is available for listener participants only.	* 9 2

Mute/Unmute With this key combination, any participants in the conference may mute and unmute themselves during the conference.	#

Please Note: You may accelerate dial out by a pound (#) sign at the end of your dialed number.

Call Codes available in the Auto Attendant:

For external IP calls addressed to the Auto Attendant following key combination is available to access and manipulate within Auto Attendant services:

Incoming Call to Auto Attendant	Key Combination
Conferences Menu - used to access conferences. **Conference ID** should be dialed here.	already in

Appendix: Extension User's Welcome Page

This welcome page may be helpful, if administrators want to inform their extension users about individual data, they need to use the extensions, such as phone numbers, phone lines, IP addresses and SIP numbers. To get a word form that may be edited and sent by mail, double-click on the paperclip sidewise.

Welcome

You are using a **QX1000 IP PBX** made by Epygi Technologies, Ltd. This product incorporates SIPVoice™ Digital Signal Processing technology to send crystal clear voice around the globe without associated fees for long distance. But, you will soon learn, it does much more. Your **QX1000 IP PBX, The Global Phone Network in a Box**, operates in much the same way as systems with which you are already familiar: a telephone, a PBX, voice mail, a phone book, et cetera. Beyond that the **QX1000 IP PBX** provides capabilities you never believed were accessible in a customer premise telephony product. Soon you will experience the freedom and power of the **QX1000 IP PBX, The Global Phone Network in a Box.**

To get started the following information is helpful.

PHONES

Your extension number is **<extension number>** and your password is **<password>** (optional).

Remember to type **00** when you pick up your phone receiver to find THE WELCOME SPOT. ***0** will take you directly to voice mail for your extension. ***74** will confirm your extension number.

IP

To reach your QX1000 from a network connection inside your office, home or place of utilization, connect a Web browser to **<IP address>** (192.168.0.200 is the default IP address).

The email address of your QX1000 System Administrator is **<email address>**

His phone numbers are **<phone numbers>**

SIP

Your SIP number (an Internet phone number) is **<SIP number>**@sip.epygi.com.

This is a number you can give people to reach you.

The SIP number to reach the Auto Attendant of your local QX1000 is **<SIP number>**@sip.epygi.com.

Your SIP group link to provide you a phone directory of numbers to call is:

http://www.epygi.com/sip/grp_view.php?viewgrp=**<groupname>**

The email address of your SIP System Administrator is **<email address>**
His phone numbers are <phone numbers>

Appendix: System Default Values

Administrator Settings

Parameter	System Default Value
Admin Settings	Login name -admin Password - 19
QX1000 Hostname	quadrillo
QX1000 Domain Name	epygi-config.loc
LAN IP Address	192.168.0.200 Subnet Mask - 255.255.255.0
Regional Settings and Preferences	Locale – US, TimeZone – Central Time (US&Canada), Theme – Dynamo, Choose Theme on Login – disabled.
Emergency and PSTN codes	Emergency Code – empty, PSTN Access Code - empty.
Uplink Configuration	Interface Type – Ethernet, Upstream – 1000000, Downstream – 1000000, Min Data Rate – 0, Maximum Transfer Unit –1500
System Security Management	Security Level-Medium
SIP IDS Settings	Enable SIP IDS – enabled Add the IP address into the Blocked IP list in Firewall – enabled Discard SIP messages from IP address – enabled.
IP Routing Configuration	No Routes
Configuration Management	Automatically Backup Configuration – disabled.
Event Settings	”Display notification” for all events except Login and Firmware Update events. Those events have a “Do nothing” action assigned.
Time/Date Settings	Simple Network Time Protocol Server and Client – enabled, SNTP Server – ntp1.epygi.com, Polling interval – 6.
Mail Settings	System Mail Settings-disabled, SSL– disabled , Enable SMTP Authentication-disabled, User Name and Password-empty.
SMS Settings	Enable SMS Service-disabled
Firmware Update	**Automatic Firmware Update**- Enabled **Upload Firmware:** Server Name – ftp.epygi.com, Server Port – 21, Update Method – ftp, Username – anonymous, Password – empty, Check for updates – Check and notify, Every day at 0:00. **Get Firmware From Server:** Firmware URL – empty, User Name – empty, Password – empty.
SNMP Settings	SNMP – disabled.
System Logs Settings	User Logging – enabled, Developer Logging – enabled, Comment – undefined,
Features	3pcc support – No key found, ACD support – No key found, Barge In – No key found, Redundancy– No key found, DCC Pro Support – No key found, DCC Basic Support – No key found, IP Phone support – No key found,

Parameter	System Default Value
	Autodialer Support – No key found, QCM support – No key found, Conference Server – No key found, Video Conferencing – No key found, Call Recording – No key found.
Language Pack	Default – English, Current Language Pack – none.
User Rights Management	Users – admin (enabled), localadmin (disabled). Roles – Extension (all accessible pages for extension except for Extension Voice Mail Profiles), Local Administrators (all accessible pages for localadmin). GUI Access Password–Old Password (empty), New Password (empty), Confirm New Password (empty). Phone Access Password–Old Password (empty), New Password (empty), Confirm New Password (empty).
Redundancy Settings	Disabled
Extensions Management	Extension Length – 4, once applied extensions 00, 1001-2000 appear
Extension Settings – General	Display name – none, Password – empty, 1001-2000 extensions attached to the IP lines 1-1000, Kickback – disabled, Call Relay – disabled, Login Allowed-disabled, 3pcc/Click2Dial Access Allowed-disabled Show on Public Directory – disabled, Percentage of Total Memory for extensions 1001-2000 – 0.08%, Allow other users to Barge In to this extension – disabled.
Extension Settings – SIP	For extensions 1001-2000: Registration username – same as extension number, Registration password - empty, SIP server - emty, SIP Server port – 5060, SIP Server Registration – disabled.
Extension Settings – SIP Advanced	Authentication User Name – undefined, Send Keep-alive Messages to Proxy – disabled, RTP Priority Level – medium, Do Not use SIP Old Hold Method - disabled, Outbound Proxy, Secondary SIP Server and Outbound Proxy for Secondary SIP Server – undefined.
Extension Settings – Remote	Remote Extension – disabled.
Extension Settings – Call Queue	Call Queue – disabled.
Extension Settings – Voice Mailbox	Internal Voice Mail for all extensions, Configuration wizard – activated, Shared Mailbox – undefined.
Extension Settings – Codecs	For extensions 1001-2000: Codecs for IP lines - G711u (preferred), G711a, G729a– enabled, G726/32, G726/16, G726/24, G726/40, iLBC, G.722, G.722.1, TDVC, H.263, H.263+, and H.264 – disabled, Out of Band DTMF Transport – enabled, T.38 FAX – enabled, Pass Through FAX – enabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls – disabled, SRTP Policy – Make unsecure calls, accept anything.
Attendant 00 Settings – General	Display name – Attendant, FAX forwarding – disabled, Show on Public Directory – enabled, Percentage of System Memory – 0.08%.

Parameter	System Default Value
Attendant 00 Settings – Attendant Scenario	Scenario – default, Send AA digits to Routing Table – disabled, Redirection on Timeout – disabled, ZeroOut – disabled, Welcome Message – enabled, Ringing Announcement – disabled, Welcome Message, Recurring Attendant Prompt and Attendant Ringing Announcement – default.
Attendant 00 Settings – SIP	Registration username – 00, Registration password - empty, SIP server - empty, SIP Server port – 5060, SIP Server Registration – disabled.
Attendant 00 Settings – SIP Advanced	Same as for extensions.
Attendant 00 Settings - Codecs	Codecs – G711u (preferred), G711a, G726/16, G726/24, G726/32, G726/40, G729a, iLBC – enabled, H.263, H.263+ and H.264 – disabled, Out of Band DTMF Transport – enabled, T.38 FAX – enabled, Pass Through FAX – enabled, Pass Through Modem – disabled, Force Self Codecs Preference for Inbound Calls – disabled, SRTP Policy – Make unsecure calls, accept anything.
Universal Extension Recordings	Default, Percentage of System Memory – 0.08%.
Receptionist Management	No entries.
Extension Directory	No entries.
Authorized Phones Database	No entries.
ACD Management	Undefined.
Conference Management and Mail Default Settings	Feature is disabled by default.
Call Statistics	Enable Call Reporting– enabled, 100 entries for all type of calls. Percentage of Total Memory used for Archive – 0% Enable Call Statistics Archive Collection – disabled Call Statistics Archive Structure – Archive by records count Call Records Count – 50 Time Interval – 10min Send archive files to external server – Send and delete from archive File Format –Tab Delimited Text (.log)
SIP Settings	UDP and TCP Port – 5060, TLS Port-empty Realm – Quadro, Session Timer – disabled, DNS Server for SIP – default, SIP timers – RFC 3261, Host Aliases for SIP – undefined.
RTP Settings	Properties for all Codecs except iLBC, G.722. G.722.1, TDVC : Packetization -20ms Silence Suppression -yes iLBC properties: Packetization - 30ms Silence Suppression – yes G.722. G.722.1, TDVC properties-undefined, G.726 Standard - ITU-T specification RTP/RTCP port range - 6000-7199 RTCP Support - disabled
NAT Traversal Settings	NAT Traversal for SIP – Automatic SIP and RTP Parameters - Use STUN SIP TCP Port – 5060 STUN Parameters:

Parameter	System Default Value
	Primary STUN Server - stun.epygi.com Primary STUN Port – 3478 Secondary STUN Server – undefined Secondary STUN Port - undefined Polling Interval: 1 hour Keep-alive interval: 120 seconds NAT IP checking interval: 300 seconds No entries in NAT Exclusion table.
Line Settings	IP Lines Configuration: Enable PnP for IP lines – enabled, Enable firmware version control – enabled, Phones Default Template – systemdefault, IP Phone Templates – no custom templates, IP Phone Logo – disabled, no custom logos uploaded, FXS Gateway Management – undefined, 1-1000 IP Lines attached to 1001-2000 extensions. All IP lines are in inactive mode.
FXO Settings	FXO is not installed
ISDN Settings	ISDN is not Installed
External PSTN Gateways	Use PSTN lines of the other device - disabled, Authorization Parameters – undefined.
Gain Control Settings	Voice Mail: Recording Gain: 0 Playback Gain: 0
SIP Tunnel Settings	Enable Tunnels to Slave Devices – disabled, Tunnels to Slave Devices – no entries, Enable Tunnels to Master Devices – disabled, Tunnels to Master Devices – no entries.
Call Routing	Route all incoming SIP calls to Call Routing - disabled Local Routing table - 3 entries defined for a call to the default Auto Attendant 00, for calls to PBX, SIP. Local AAA Table - Authentication by Caller ID-enabled, Global Speed Dial Directory – undefined.
RADIUS Settings	RADIUS client – disabled.
Voice Mail Common Settings	Voice Mail Recording - G729a, Email Subject for voice - Voice mail received from $[VM_DISPNAME] $[VM_USERNAME], FAX to E-mail format – TIFF.
Dial Timeouts	4 seconds.
3PCC Settings	Secure Connection – disabled, Request Timeout – 10, Feature Key – not added, Network Port – not opened.
RTP Streaming Channels	Undefined.
Call Recording	**Basic View**: All extensions are disabled. **Advanced View**: Call Type – Auto, Address-empty, Recording Type – Always start automatically, Max Recording Duration – 1 hour, Recording To – same as extension number Description – empty.
Firewall	Firewall - disabled, Ping Stealth – enabled,
Filtering Rules	SIP Access (Allowed for all),

Parameter	System Default Value
	Management Access (Allowed for all), No user defined services and IP pool groups.
DNS Settings	Nameserver-127.0.0.1
DHCP Server Settings	Disabled.
DHCP Advanced Settings	DHCP Options: Gateways – 192.168.0.200 Subnet mask – 255.255.0.0 Domain name servers – 192.168.0.200 NBT name servers – 0.0.0.0 NTP servers – 192.168.0.200 Domain name – epygi-config.loc Overload tftp server name – 192.168.0.200 DHCP Server Statements: Authoritative – enabled. Ping Check – enabled, Ping timeout – 1 sec.
VLAN Settings	Undefined.

Extension Settings

Parameter	System Default Value
Voice Mail Settings	Maximal mail message duration - 5 min, Ask password before granting local access to mail box – disabled, Ask password before granting remote access to mail box – enabled, Send welcome message – disabled, Play Voice Mail help – enabled, Automatically play messages - enabled, Send mails count information message – disabled, Send date/time information message – enabled, Send beep at the end of message – enabled, Silent VM recording – disabled, Send new voice messages via e-mail – disabled, Voice Mail–Send notification with attachment Remove Voice Mail On Send-disabled Fax– Send notification with attachment Remove Fax On Send-disabled Send new voice message notifications via SMS – disabled, Send new voice message notifications via phone call – disabled, Voice Mail Indication: Lamp indication – enabled for IP lines only, Tone indication – enabled for FXS lines only, Ringing indication – disabled, Zero Out – enabled, Redirect Call Type – PBX, Redirect Address - 00, FAX Redirection – disabled, Automatic Fax Receiving Mode – disabled, Out of Office – disabled, Forward/rewind duration – 3 seconds, Greeting message – default, VM Profiles – undefined.
Group List	No entries.
Speed Calling	No entries.
Account Settings	Display Name – undefined, User Password Protection – disabled both for incoming and outgoing calls, User's Name for Extensions Directory – default, Custom Voice Messages – default.
Caller ID Based Services	No entries in the table. For Any Callers – all services are disabled, Call Blocking message files – default,

Parameter	System Default Value
	Intercom – Allow Activation on Request, Activation Signal –Ring Only if Requested.
Basic Services - General	No answer timeout – 20 sec, Call Waiting Service – enabled, Autoredial Interval - 10 sec, Autoredial Period - 15 min.
Basic Services - Hold Music	Send Hold Music to remote IP party – enabled, Hold Music – Own Music, Music file – default.
Basic Services - Do Not Disturb	Disabled, Timeout – 30 min, Send Message to Caller – enabled.

Appendix: Moderator's Menus

This Appendix explains all menus that can be accessed and configured by conference moderators. (Applicable if the Conference Server and/or Video Conferencing feature is activated on the system.)

Conference Moderator's Main Page

The Moderator's Main Page can be accessed by clicking on the conference ID link on the Conferences Management page or by logging as a moderator on the QX1000 login page.

After logging in as a moderator, the page Conference Progress is displayed. Here you may see the active conferences and the participants. From this page you may also access the settings of the conference to operate and perform actions that are available only to the moderator of each conference.

Conference Menu

- Conference Progress
- Activate Conference
- Send Notification Mail
- Recorded Conferences

Conference Properties Menu

- General Settings
- Recording Settings
- Customization
- Participants
- Schedule

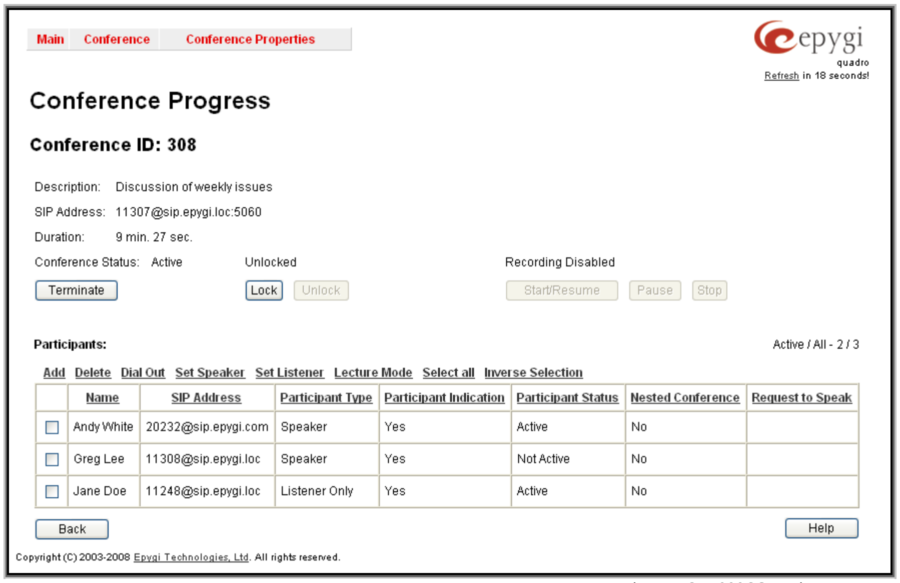


Fig. II-1: QX1000CS Moderator's page

Conference Menu

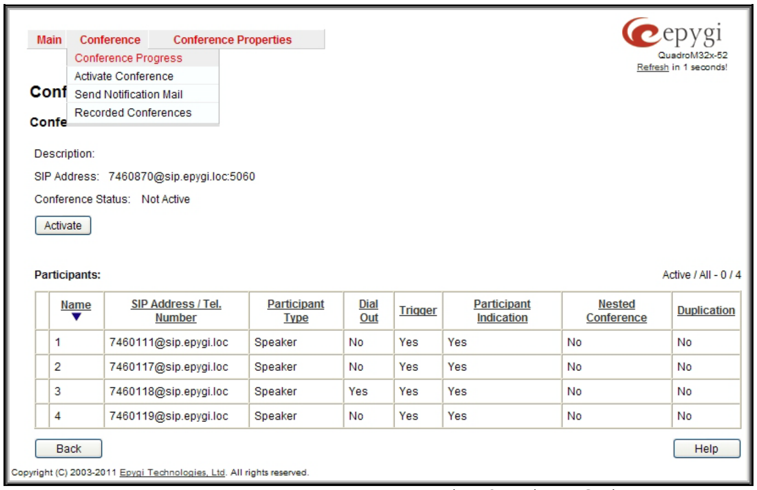


Fig. II-2: Moderator Settings Dynamo Menu

Fig. II-3: Moderator's Settings Tree Menu

Conference Progress

The **Conference Progress** page displays information about the conference, including the list of participants, and allows moderator to manage the conference.

The following read-only data is displayed on this page:

Conference ID – the unique ID on the conference.

Info Text – displays the text uploaded in the Info File from Customization page. In the picture illustration on the right side, the Info Text says "WELCOME to EPYGI's CONFERENCE!!!".

Description – any descriptive information about the conference (optional).

SIP Address - the SIP address of the conference.

Duration – the time the current conference is active.

Conference Status – the conference status (active, not active or waiting). If the conference is active, the information whether the conference is locked or not, and the recording status (recording started, recording paused and recording stopped) is also displayed herein.

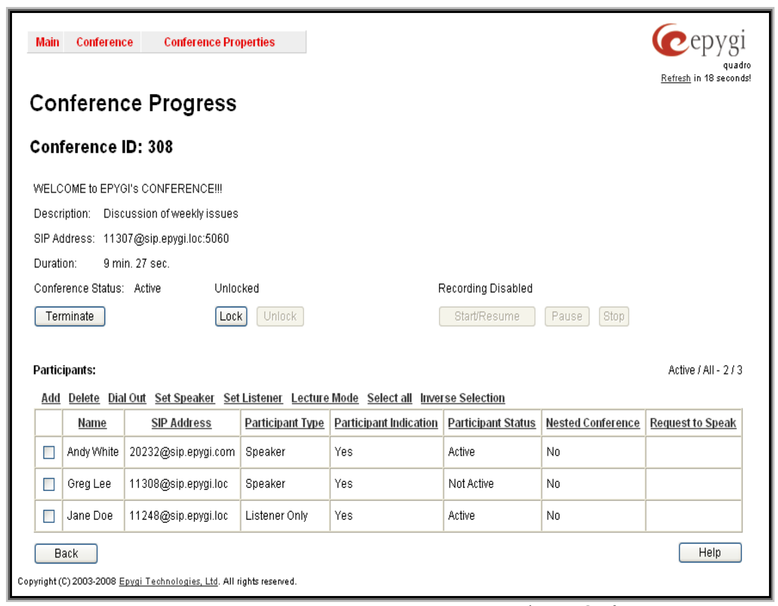


Fig. II-4: Conference Progress Page

The following buttons are available on this page to manage the active conference:

Activate – available for an inactive conference only and used to activate the conference.

Terminate – available for an active conference only and used to terminate the active conference

Lock – available for an active conference only and used to lock the conference. When a conference is locked, no users can connect to it.

Unlock - available for an active conference only and used to unlock the conference.

Start/Resume – available for an active conference only and used to start the recording of the conference or to resume the recording if it was paused.

Pause - available for an active conference only and used to pause the recording of the conference.

Stop - available for an active conference only and used to stop the recording of the conference.

Please Note: **Pausing** and **Resuming** the conference recording can be used to edit the recorded conference audio file. When pause/resume operations are used, conference is recorded in a single file, leaving out the conversation during which conference recording was paused. When using stop/start operations, new files are created each time conference recording is started. All recorded conferences are listed in the Recorded Conferences page only after conference recording termination. In case of **pause/resume**, the recorded file is not terminated. In case of **stop/start** recording starts in new file.

The table of participants on this page lists all preconfigured participants (independent of the conference status), as well as new participants joined the conference (if still connected to the conference) and those participants added from the handset or GUI (unless the conference is terminated).

For the active conference, the table also displays participants added manually from GUI or from the handset and those participants that called in to the conference.

The **Conference Progress** table contains the following information for each participant.

Name – this information is specific to manually added participants only (see below).

SIP Address – indicates the SIP address of the participant.

Participant Type – indicates whether the participant is a speaker or a listener only.

Participant Indication – indicates whether or not a beep indication during the call conference is configured for this participant to be played when he joins or leaves the conference.

Participant Status – this column is only present for active conferences and indicates the state of the participant (active for participants currently in the conference, not active for participants not in the conference, and joining for participants currently joining but not yet connected to the conference).

Nested Conference – indicates if the participant acts as a nested conference or not.

Request to Speak - this column is only present for active conferences and indicates whether a listener participant has requested to speak (by dialing ***9** from the handset, see Feature Codes). When a listener participant requests to speak, a hand-up icon appears in this column. Clicking on the hand icon in this column will grant the speaker permission to the corresponding participant. Participant with the speaker permissions are able to speak to the conference.

The following functional buttons are present on **Conference Progress** page to manipulate with the participants in the conference:

Add functional button opens the **Add Participant** page where a new participant can be manually added to the conference. The **Conference Progress – Add Participant** page consists of the following components:

Participant Name requires optional information (first name, last name, nickname, etc.) about the participant.

SIP Address/Tel. number requires the contact phone number (SIP address or Routing Number) of the participant. This number automatically will be dialed by the system when the participant is configured to be a Dial Out (see below) or when a corresponding Conference Code is used (see Conference Codes).

The participant's SIP address should be a combination of username@hostaddress:port (where hostaddress can be an IP address, for example, 192.168.90.10, or a host name, e.g., sip.epygi.com). The port number is optional for the SIP address. If no port is specified, 5060 will be used. The range of valid ports is between 1024 and 65536.

Please Note: A direct call will be placed toward a participant's SIP address if the corresponding conference is registered on a different SIP server than the participant is registered on, or if the participant is not registered on any SIP server.

The value will be implied as a Routing Number and will be parsed through the Call Routing table if it does not match the SIP URI syntax.

Participant Type list is used to select the type (speaker or listener) of participant in the conference.

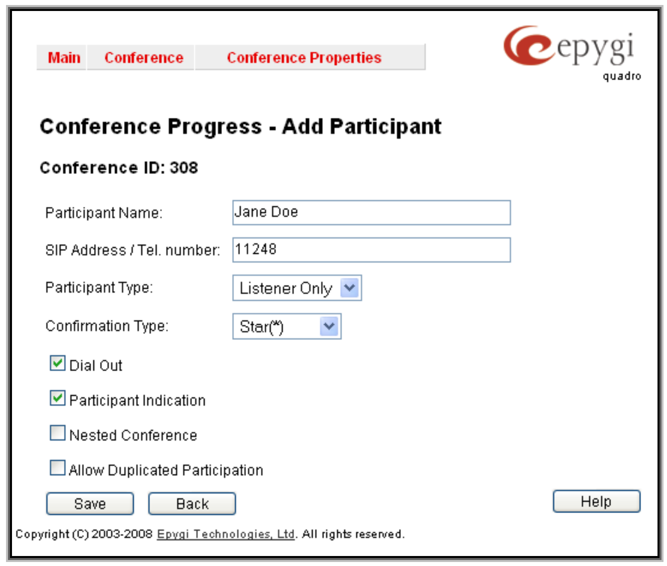


Fig. II-5: Conference Progress – Add Participant Page

Confirmation Type list is used to set the password protection for the participant joining the active conference. **Star (*)** selection allows the participant to accept the conference invitation by pressing the * button. Only participants connected to the conference with the moderator password will be provided with permissions to manipulate the conference.

A group of checkboxes on this page allow configuration of participant specific settings:

- When the **Dial Out** checkbox is selected, the participant will be automatically dialed out when the conference is activated.
- **Participant Indication** enables the beep indication during the conference when this participant joins or leaves the conference.
- **Nested Conference** must be selected if the participant is a Conference itself and enables the correct behavior of conference termination.
- **Allow Duplicated Participation** checkbox allows multiple participants with the selected Caller ID (calling address) to join the corresponding conference. This is applicable when different participants are using the same shared number to place a call.

Dial Out functional button is used call one or more inactive participant(s) inviting them to join the conference.

Delete removes the selected participants from the conference.

Set Speaker functional button is used to grant selected participants a speaker's permissions. A participant with speaker permissions is able to speak to the conference.

Set Listener functional button is used to grant selected participants a listener's permissions. A participant with listener permissions is not able to speak to the conference and is only a listener.

Lecture Mode functional button is used to grant selected participants a lecturer's permissions. Both listener and speaker participants can get lecturer permissions. Enabling lecture mode for a participant will allow him to speak to the conference and will mute all other participants of the conference.

Please Note: Only one participant can act in a lecture mode at the same time.

Select all checks all existing participants in the table.

Inverse selection inverses the current selection (if no records are selected, clicking on inverse selection will check all records).

Activate Conference

This link is used to activate a conference.

Send Notification Mail

This link is used to send an email to the participants notifying them about the start of a conference and inviting them to join. The text of the notification email is being configured by the administrator.

Recorded Conferences

Conference recording service allows you to record conferences and save them on the system internal or external storage space (depending on the configuration). To use conference recording service, it should be enabled from the Recording Settings page.

The maximum duration of the recorded conference can be optionally limited from the Recording Settings page.

Conference recording can be manipulated either from the Conference Progress page or from the handset (see Feature Codes). If the **Recording Indication** is also enabled from the **Recording Settings** page, voice announcements will be played in the conference to inform participants that the conference recording is started, stopped, paused or resumed.

Recorded conferences are stored and are listed in the Recorded Conferences page accessible by the moderator from QX1000 Web Management.

The **Recorded Conferences** page displays a table where recorded conferences are listed. The recorded conferences can be played and deleted from this page.

The **Recording free space** field displays the free space allocated for the corresponding conference.

The **New recordings** field displays the number of new recorded conferences in the recording box. All new recordings are marked in bold.

The **All recordings** field displays the number of all recorded conferences in the recording box, including new and played recordings.

The **Check Recordings** functional link refreshes the recording box with any latest recordings (if any).

The **Recorded Conferences** table displays all the recorded conferences with the following parameters:

Date & Time shows the initiation date and time of the recorded conference.

Duration shows the duration of the recorded conference (in minutes/seconds).

Play - by clicking on the speaker sign beside every record in the table, the recorded conference will be played (using the available media player supported by your Operatinig System).

The column headings of the **Recorded Conferences** table are organized as links. By clicking on the column heading, the table will be sorted by the selected column. Upon sorting (ascending or descending), arrows will appear next to the column heading. Each row in the table of Recorded Conferences can be selected by the checkbox for deletion.

Fig. II-6: Recorded Conference

To Play a Conference

1. Click on the speaker sign of the corresponding recorded conference.
2. Depending on you browser settings, the .wav file will be played directly or an application will ask you to save the .wav file locally to the PC. If you need to save the file, please specify the path then run the media file from the specified location.

To Delete a Recorded Conference

1. Select the checkbox of the corresponding record(s) in the **Recorded Conferences** table that will be deleted. Click on **Select all** if all records should be deleted.
2. Select the **Delete** button.
3. Confirm the deletion clicking **Yes**. The selected conference then will be deleted. To abort the deletion and keep the conference on the QX1000 CS, select **No**.

Inverse Selection inverses the current selection (if no records are selected, clicking on inverse selection will check all records).

Conference Properties Menu

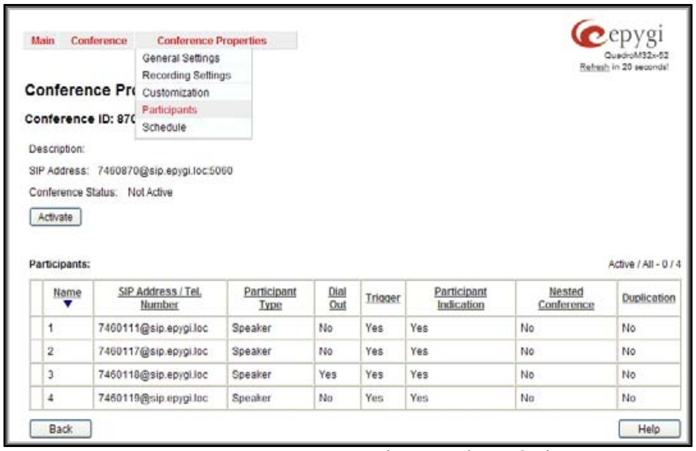


Fig. II-7: Moderator Settings Dynamo Menu

Fig. II-8: Moderator's Settings Tree Menu

General Settings

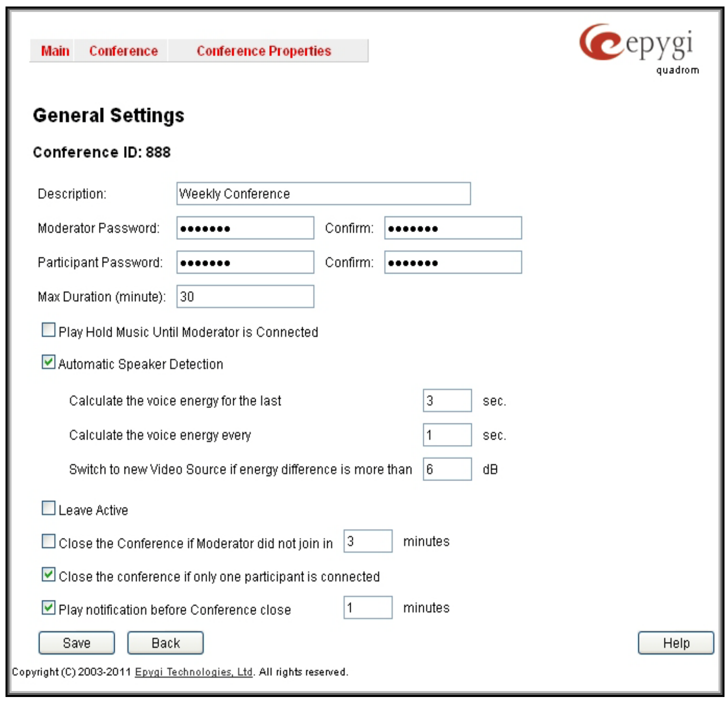


Fig. II-9: General Settings Page

The **General Settings** page is used to configure the basic conference settings.

The page contains the following components:

Conference ID indicates the unique ID of the conference.

Description indicates any descriptive information about the conference.

Moderator Password text field requires a password for the moderator access to the conference. The password inserted here should be used by the moderator to join the conference. Moderator is able to use conference codes during the active call conference as well as to access conference specific GUI pages and coordinate the conference (view/change conference properties, activate/deactivate it, start/stop/resume recording, view conference statistics). **Confirm** text field requires the confirmation of the Moderator Password. Error appears if the password inserted in the **Confirm** text field does not match the one inserted in the **Moderator Password** text field.

Participant Password can be entered to require a password for participant access to the conference. It has to be entered twice for confirmation. The password entered here should be used by the participant to join the conference. The participant can participate in the conference only according to the rights (speaker or listener) granted by the moderator.

Max. Duration sets the conference to be limited to a maximum duration (in minutes). Leave the field empty for unlimited conference duration.

With the **Play Hold Music Until Moderator is Connected** checkbox selected, participants connected to the conference will listen to the hold music unless moderator will join the conference.

Automatic Speaker Detection checkbox enables the automatic detection of the loudest participant in the conference (the current speaker) and switching the video on all of the video conferencing phones in automatic mode to the video from that participant. Initially, when the user joins a conference with **Automatic Speaker Detection** checkbox enabled, his video phone works in automatic mode. Dialing *50 or *51 feature codes will switch the phone to manual mode, displaying the video of the next or previous participant correspondingly. When the phone is in manual mode, it will not switch automatically to display the loudest participant, but it will show the video of the same participant until next time when *50 or *51 is being pressed. Entering the *52 feature code will switch the phone back to automatic mode.

For making the video source switching decision in automatic mode, the video conferencing uses the values of the following parameters:

- **Calculate the voice energy for the last [ ] sec.**
- **Calculate the voice energy every [ ] sec.**
- **Switch to new Video Source if energy difference is more than [ ] dB.**

For example, if the values of the parameters are 3, 1 and 6 (default values) correspondingly, the Conference Server will calculate every one second the average voice energy of each participant during the last three seconds. Then the largest calculated value will be compared to the average voice energy of the participant providing currently the video for all phones in automatic mode. If the difference between energies is more than 6dB then the Conference Server will switch the video to a new source having the largest voice energy.

Leave Active checkbox will keep conference active, even if all participants have left it.

Close the Conference if Moderator did not join in - the idea of including this parameter is as follows:

If the conference is activated by one of the existing ways and the moderator does not join the conference within the first **X** minutes then the conference will be closed by the system. No message will be played to the joined users in this case. The conference will be closed in one of the following cases:

- The conference is activated by a schedule, and the moderator did not join within the first **X** minutes after activation. The only method of distinguishing the moderator from the other participants is the moderator's password. If the user entered the moderator's password during the joining process then he/she is a moderator. There are no other means of distinguishing the moderator from the regular participant.

- The conference is activated by a participant when dialing in, and the **Activate On Dial In** checkbox is enabled for that conference. During the joining process, the participant either did not enter any password or entered a regular participant's password. In this case, the same as above, if the moderator did not join the conference within the first **X** minutes entering moderator's password, the conference will be closed.

- The conference is activated by a moderator from GUI. In this case, even though the moderator activated the conference and did not join within the first **X** minutes, the conference will be closed. In all the above mentioned cases, the conference will be closed regardless of the number of regular participants already joined.

Close the conference if only one participant is connected - if enabled, then the conference will be closed as soon as there is only one participant connected to the conference, after the moderator left the conference. If the moderator did not join yet (during the first **X** minutes as described above), the conference will stay active even if there is only one participant connected yet. If the moderator is the only participant connected to conference then it will stay active.

Play notification before Conference close. When the **Max Duration (M)** of the conference is reached (see **Instant Conferencing Settings**), the system will close the conference and **M** minutes before closing the conference the system will play the warning message to all participants.

Recording Settings

The settings on this page are addressed to the conference recording configuration, enabling conference recording, defining the recording memory allocation (internal or external storage), etc.

The **Recording Settings** page offers the following components:

The **Enable Recording** checkbox enables an option to be used for active conferences to perform the online recordings. With this checkbox selected, a group of radio buttons is activated to select the storage for the recorded conference audio files.

- **Use Internal Storage** switches the location used to store the recorded conference audio files to the system internal memory. **Max Recording Time** requires the maximum duration (in minutes) of one recording to be done. If the conference recording has been paused and resumed again, the Max Recording Time value will indicate the actual recorded time. Leave this field empty not to limit the duration of the conference recording.
- **Use External Storage** switches the location used to store the recorded conference audio files to an external destination, which can be any device or application that has audio recording capabilities. The **SIP Address** of the remote destination where the recorded conference will be stored is required to be defined for this selection. Optionally, the SIP address of a user can be inserted here. In this case, the conference will be recorded to the private mailbox of the user or will be directly played to him if he answers the incoming call.

Fig. II-10: Recording Settings page

Recording Indication selection enables voice announcements played in the conference to inform participants that the conference recording is started, stopped, paused or resumed.

When the **Start Recording Automatically** checkbox is selected, the conference recording will start automatically as soon as the corresponding conference is activated.

Customization

The **Customization** page is used to manage the voice prompts played during an active conference. The page offers the following options:

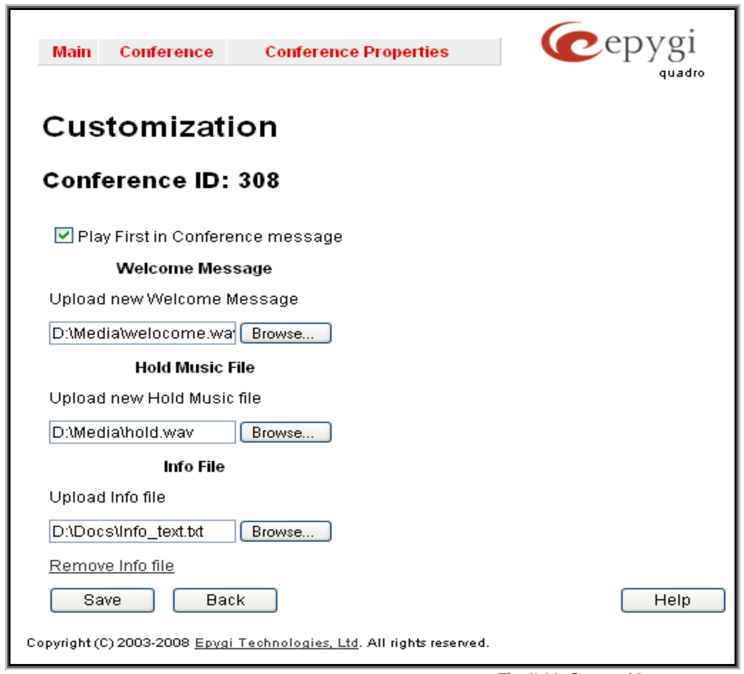


Fig. II-11: System Messages page

When the **Play First in Conference message** checkbox is selected, the system will play a “You are the first participant in the conference” notification message informing you that no more participants are yet connected.

Welcome Message parameters group allows updating the active conference welcome message (played once a user is connected to the conference), downloading it to the PC or removing the custom welcome message. The group offers the following components:

Upload new welcome message indicates the file name used to upload a new welcome message. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading it and the “Invalid audio file, or format is not supported” warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding conference and the “You do not have enough space” warning message will appear.

Browse opens the file chooser window to browse for a new welcome message file.

The **Download Welcome Message** and **Remove Welcome Message** links appear only if a file has been uploaded previously. The **Download Welcome Message** link is used to download the message file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Welcome Message** link is used to restore the default welcome message.

Hold Music File parameters group allows updating the hold music (played when you are alone in the conference), downloading it to the PC or removing the custom welcome message. The group offers the following components:

Upload new hold music file indicates the file name used to upload a new hold music file. The uploaded file needs to be in PCMU wave format, otherwise the system will prevent uploading it and the “Invalid audio file, or format is not supported” warning message will appear. The system also prevents uploading if there is not enough memory available for the corresponding conference and the “You do not have enough space” warning message will appear.

Browse opens the file chooser window to browse for a new hold music file.

The **Download Hold Music File** and **Remove Hold Music File** links appear only if a file has been uploaded previously. The **Download Hold Music File** link is used to download the hold music file to the PC and opens the file-chooser window where the saving location may be specified. The **Remove Hold Music File** link is used to restore the default hold music.

Info File parameters group allows you to upload a text file with some conference related announcement, advertisement or any other information to be displayed on the Conference Progress page. The group offers the following components:

Upload Info file indicates the information file name. The system will display the file content exactly in the way it is formatted in the file. It is recommended to use a *.txt formatted plain text file. The uploaded file should not exceed the size of 2000 bytes. The system also prevents uploading if there is not enough memory available for the corresponding conference and the “You do not have enough space” warning message will appear.

Browse opens the file chooser window to browse for an information file.

The **Remove Info File** link appears only when a file has been previously uploaded and is used to remove the uploaded information file.

Participants

This page allows to configure participants of the conference as well as to adjust settings of the participants dialed out during the conference or independently connected to the conference.

The New Participants Configuration moves to the page where the settings of participants independently dialed in to the conference can be configured. Once the new participant connects the conference, he will automatically appear in the Conference Progress table on this page and remain there unless disconnected from the conference.

The Handset Added Participants Configuration moves to the page where the settings of participants dialed out from the handset by the moderator during the active conference can be configured. Once a handset added participant connects the conference, he will automatically be added to the Conference Progress table on this page and remain there unless the conference is terminated.

The table on this page lists all preconfigured participants, allows to add new participants and to modify the settings of the exiting ones.

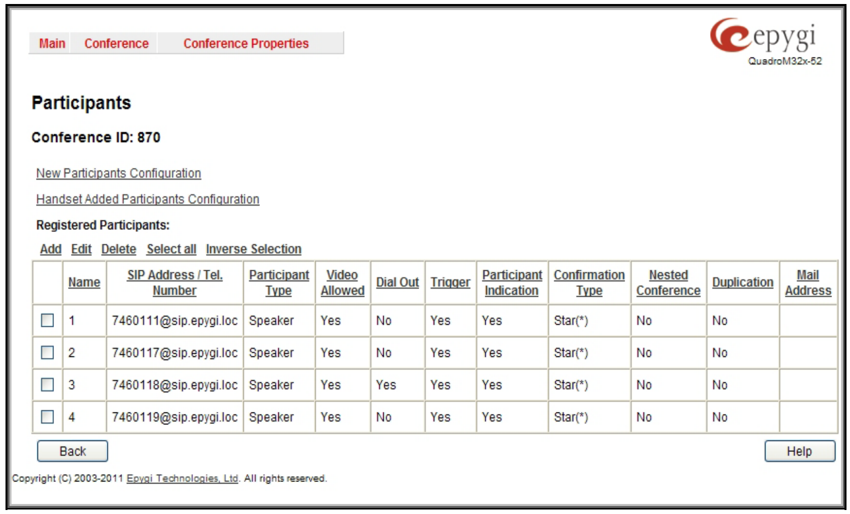


Fig. II-12: Participants Page

Please Note: By default, no participant is able to make video calls. Administrator should set one of the following checkboxes to enable the video capability of the participant:

- **Allow Video** checkbox from the **Participants - Add Entry** GUI page (see Fig. II-13).
- **New Participant Can Make Video Call** checkbox from the New Participants Configuration GUI page (see Fig. II-15).
- **Allow Video** checkbox from the Handset Added Participants Configuration GUI page (see Fig. II-16).

Add opens an **Add Entry** page where new participants can be added to the conference. The following parameters are needed to configure participant settings:

Participant Name requires optional information (first name, last name, nickname, etc.) about the participant.

SIP Address/Tel. number requires the contact phone number (SIP address or Routing Number) of the participant. This number automatically will be dialed by the system when the participant is configured to be a Dial Out (see below) or when a corresponding Conference Code is used (see Conference Codes).

The participant's SIP address should be a combination of username@hostaddress:port (where hostaddress can be an IP address, for example, 192.168.90.10, or a host name, e.g., sip.epygi.com). The port number is optional for the SIP address. If no port is specified, 5060 will be used. The range of valid ports is between 1024 and 65536.

Please Note: A direct call will be placed toward a participant's SIP address if the corresponding conference is registered on a different SIP server than the participant is registered on, or if the participant is not registered on any SIP server.

The value will be implied as a Routing Number and will be parsed through the Call Routing table if it does not match the SIP URI syntax.

Email Address requires the email address of the participant. Conference related notifications (configured from the Schedule page or using the Send Notification Mail option) will be sent automatically to this address. This field is not available on this page when it is reached from the Conference Progress page.

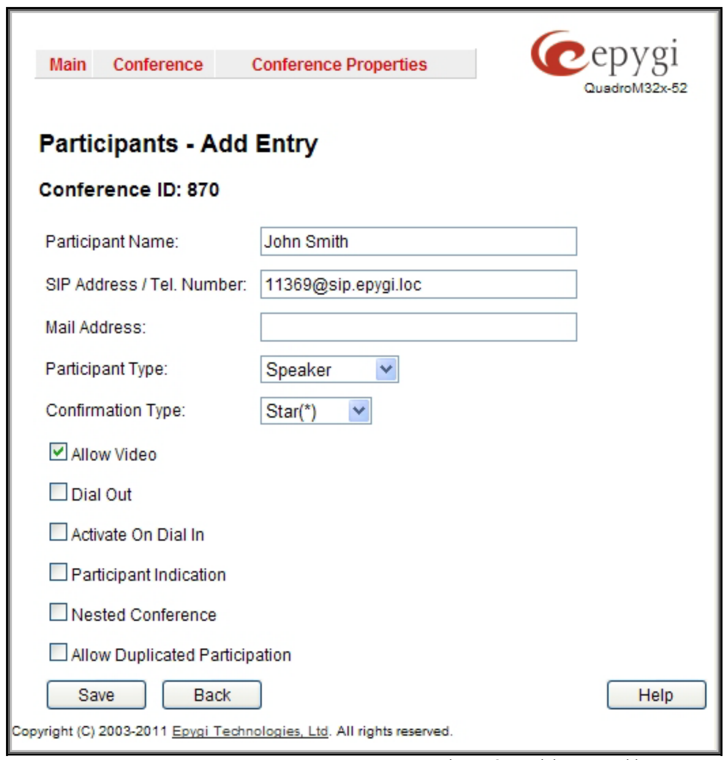


Fig. II-13: Participants - Add Entry Page

Participant Type list is used to select the type (speaker or listener) of the participant in the conference.

Confirmation Type list is used to set the password protection for the participant joining the active conference. **Star (*)** selection allows the participant to accept the conference invitation by pressing the * button. Only participants connected to the conference with the moderator password will be provided with the permissions to manipulate the conference.

Please Note: Confirmation Type should be selected to "none" when the **Participant Type** is listener.

A group of checkboxes on this page allow configuration of participant specific settings:

- **Allow Video** checkbox will allow participant to join the video conference. This checkbox is not available on this page when it is reached from the Conference Progress page.

- When the **Dial Out** checkbox is selected, the participant will be automatically dialed out when the conference is activated.
- **Activate On Dial In** automatically activates the conference when this participant joins the conference call. This checkbox is not available on this page when it is reached from the Conference Progress page.
- **Participant Indication** enables the beep indication during the conference when this participant joins or leaves the conference.
- **Nested Conference** should be selected if the participant is a Conference itself and enables the correct behavior of conference termination.
- **Allow Duplicated Participation** checkbox allows multiple participants with the selected Caller ID (calling address) to join the corresponding conference. This is applicable when different participants are using the same shared number to place a call.

The **Edit** functional button provides a possibility of editing multiple participants at the same time. A **Select to modify fields** checkbox alongside the fields to be modified needs to be selected to submit changes, otherwise the fields will not be updated.

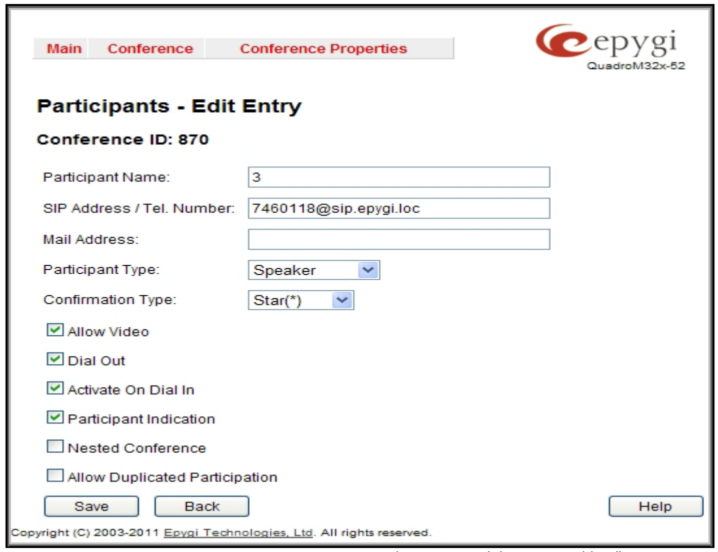


Fig. II-14: Participants – Multi-Edit Entry Page

New Participants Configuration

This page is used to configure settings of participants independently dialed in to the conference. Once the new participant connects the conference, he will automatically appear in the Conference Progress table and remain there unless disconnected from the conference.

The page consists of the following components:

Selecting the **New Participant Allowed to Join** checkbox will allow new users to connect the conference by simply dialing in (no previous registration in Participants table is needed). If this checkbox is selected, the following settings should be provided:

Max New Participant Count text field requires the maximum number of new users allowed to connect to the conference. Leave this field empty to allow unlimited number of new users connecting the conference.

New Participant Type drop down list is used to select the state (speaker or listener only) of the new participants connected to the conference.

Selecting the **New Participant Can Make Video Call** checkbox will allow participant to join the video conference.

New Participant Confirmation Type drop down list is used to select whether the conference is password protected for the new users or not.

Selecting the **New Participant Can Activate Conference** checkbox will allow new users to activate the conference.

When **Conference Inactive Until Moderator Login** option is enabled, participants will not be able to join the conference until the moderator has logged in. **New Participant Confirmation Type** field should also be set to **Password** to enable this option.

Fig. II-15: New Participants Configuration Page

Selecting the **New Participant Indication** checkbox will enable a beep indication during the active conference when a new user joins or leaves the conference.

Handset Added Participants Configuration

This page is used to configure the settings of participants dialed out from the handset by the moderator during the active conference. Once the handset added participant connects the conference, he will automatically appear in the Conference Progress table and remain there unless the conference is terminated. This will allow the handset dialed participant to hang up and dial in to the corresponding conference again while it is active.

The page consists of the following components:

Participant Type drop down list is used to select the state (speaker or listener only) of the handset added participants connected to the conference.

Confirmation Type drop down list is used to select whether the conference is password protected for the handset added users or not. When **Star (*)** selection is chosen, the handset added user should accept the conference invitation by pressing the * button.

Selecting the **Allow Video** checkbox will allow participant to join the video conference.
Selecting the **Participant Indication** checkbox will enable a beep indication during the active conference when a handset added user joins or leaves the conference.
The **Allow Duplicated Participation** checkbox selection allows several instances of callers with the same handset added number (caller address) to join the corresponding conference at the same time. This option may be used to allow users from the same network (with the same caller address), like PSTN network, to reach the conference.

Fig. II-16: New Participants Configuration Page

Schedule

The **Schedule** page is used to configure and manage the conference scheduling rules, so that a conference can be automatically activated on the date and time. The Scheduling service may also be configured to send invitation emails to the participants asking them to join the conference or informing about a new conference.

The **Conference Schedule** page offers a table that lists all scheduling rules configured for the corresponding conference. When a scheduled conference is activated, all participants with dial-out option enabled will be dialed.

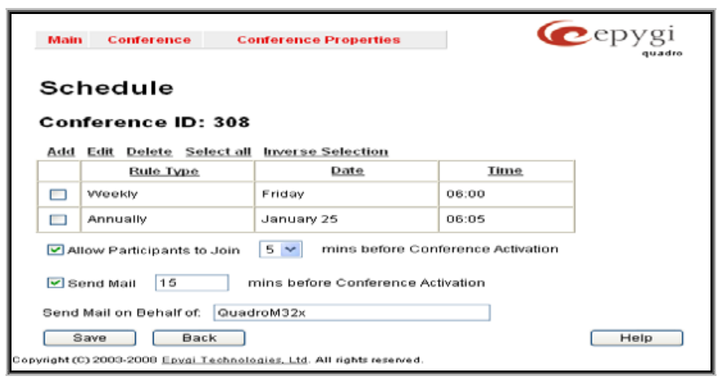


Fig. II-17: Schedule Page

Clicking the **Add** button takes you to the **Add Entry** page where new scheduling rule can be configured. This page offers the following components:

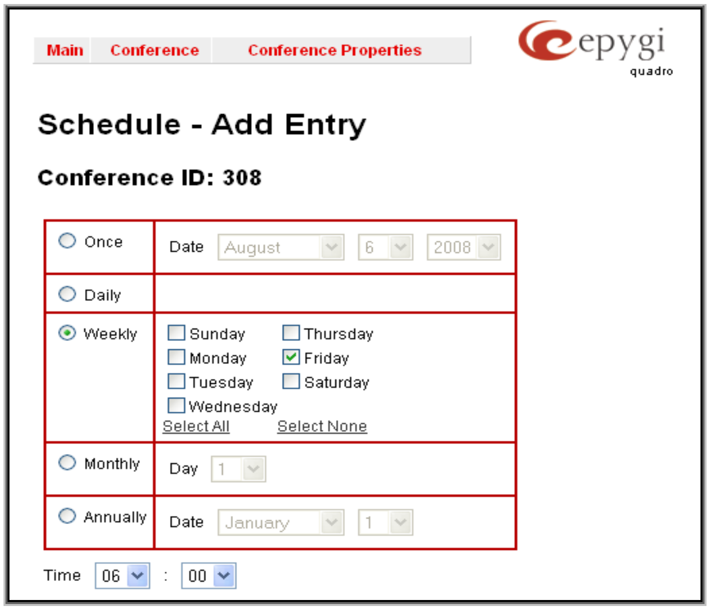


Fig. II-18: Schedule – Add Entry page

A group of radio buttons that are used for selecting the frequency of the scheduled conference:

- **Once** – the calendar date (month, day, year) should be specified for this option.
- **Daily**
- **Weekly** – weekdays when scheduling out to be activates should be selected for this option. Use **Select All** and **Select None** to select or deselect all weekdays.
- **Monthly** – the calendar day should be selected for this option.
- **Annually** – the calendar day and the month should be selected for this option.

In the **Time** text fields, the time of the scheduled conference activation should be defined. The time selected in these fields will be considered according to the system date and time settings.

The **Allow Participants to join conference before Conference Activation** checkbox selection allows participants to dial in to the conference before conference activation. During this period, participants will be able to communicate with each other. However, this does not mean that the conference is activated; the participants will be dialed out (if any) and the recording will start (if configured) only after the configured scheduled time comes.

The **Send Mail before Conference Activation** checkbox enables email notification delivery to the participants before the conference activation. The text field requires the timeout (in minutes) before the conference activation when the email notifications to the conference participants with **Email Address** configured from the Add Participants page should be delivered. This option is only valid if the Email Address is configured for the participant.

The **Send Mail on behalf of** text field requires an email address or a conditional name related to the conference to be transmitted in the **From** field of the email notifications.

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 QX1000 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 QX1000 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 QX1000. 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 QX1000 or any Quadro SIP Gateway product. If you sell your license rights in the Licensed Materials you must at the same time transfer the documentation to the acquirer. Also, you cannot sell your license rights in the Licensed Materials to another party unless that party also agrees to the terms and conditions of this Agreement. Except as expressly permitted by this section, you may not transfer the Licensed Materials to a third party.

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 QX1000 Installation Guide and User's Manual, constitute the complete and exclusive agreement between you and the Licensor and supersede any proposal or prior agreement or license, oral or written, and any other communications related to the subject matter hereof. If one or more of the provisions of this Agreement is found to be illegal or unenforceable, this Agreement shall not be rendered inoperative but the remaining provisions shall continue in full force and effect.

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 6900 North Dallas Parkway, Suite 850, Plano, Texas 75024 or call Epygi at (972) 692-1166.