



# Preventing Unauthorized Calls on the Epygi QX

**Abstract:** This document explains how to properly secure the Epygi QX products and prevent unauthorized calls.

## Table of Contents

1	Introduction .....	4
2	Functional Description .....	4
3	Secure the System .....	4
4	Preventing SIP attacks .....	4
5	Securing Calls on Auto Attendant.....	5
5.1	Control of the Dialed Digits on Auto Attendant.....	5
5.2	Using Call Relay on Auto Attendant.....	7
6	Securing Call Routing rules from unwanted SIP calls.....	8
7	Using Local Authentication on Call Routing Rules .....	8
7.1	Local AAA Table Configuration .....	8
7.2	Enabling local authentication on the Call Routing rules .....	9
8	Using Filters on Call Routing Rules .....	12
8.1	Using Date/Time Limitations on Call Routing Rules .....	13
8.1.1	Examples .....	15
8.2	Using Overall Calling Time Limitations on Call Routing Rules .....	18
8.2.1	Examples .....	20
9	Securing 3PCC calls.....	21
9.1	Extensions 3pcc/Click2Dial Login Allowed option.....	21
9.2	Admin and Local admin access .....	22
10	System Security Management.....	22
11	Incoming and Outgoing Call Blocking .....	23
12	References.....	25

## Document Revision History

Revision	Date	Description	Valid for SW	Valid for models
1.0	12-Jan-15	Initial Version	6.0.x and higher	All QX products

## 1 Introduction

---

As with any business system, security is a top concern. This document explains how to protect your investment and ensure that your QX is secure from unauthorized callers. It contains instructions on how to prevent unwanted incoming and outgoing calls and how to restrict calls to authorized users only.

VoIP in particular offers a wide range of communication possibilities to businesses and any VoIP system, from any vendor is susceptible to abuse. Many of the recommendations in this document can be applied to any system.

This document is applicable to all QX IP PBX and QX Gateway models running 6.0.x software version and higher.

## 2 Functional Description

---

Each QX system has very powerful and secure call routing capabilities. However, a poorly configured system may allow unauthorized callers to place fraudulent calls, causing extra traffic and toll charges.

The following will provide details on how to secure the QX to prevent unwanted callers from using the system.

## 3 Secure the System

---

The default QX password for administrator login needs to be changed. It may seem like a simple and logical thing to do but many of the systems that Epygi has worked with are on a public IP address and the default for administrator login has not been changed. The concern with a QX IP PBX is that if someone can access to the system they could remotely configure and register an IP phone to make long distance calls. They could also alter Call Routing tables to allow calls to proceed.

Local and Remote IP phones require a User Name and Password to successfully register to the QX IP PBX. In addition, before any call can proceed the IP Phone must present a valid User Name and Password to the QX IP PBX. For phones that Plug and Play on the QX IP PBX a unique and random password is created and it is not visible to any user. It is a very secure password and it is suggested that it should be used. IP Phones should not use easily guessable User Names and Passwords to register (e.g. Extn/Extn, such as 7004/7004, Extn/1234, etc.). A remote user could guess a simple User Name and Password and register an IP Phone to make calls.

## 4 Preventing SIP attacks

---

In most cases the SIP attackers are malware applications which are scanning VoIP systems for security holes to make long distance calls at the expense of the PBX owner. Most of the methods to detect a security hole on the system are using a technique to send several dozen registration requests per second, in an attempt to hopefully guess a weak IP Phone User Name and Password. As the QX IP PBX is receiving, analysing and answering to all of these requests, it may cause a heavy load on the system and alter the system's ability to respond to legitimate requests by valid extension users.

The QX has implemented **Firewall->SIP IDS** Menu, which includes the **SIP IDS** tool to help prevent SIP attacks. If enabled, SIP IDS will detect repetitive, unsuccessful SIP authorization requests (e.g. failed SIP Registrations, failed SIP Subscribe messages) and automatically block the offender, adding the IP addresses to the Firewall's blocked IP list.

To enable/disable the **SIP IDS** option, follow the steps below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Firewall->SIP IDS** menu. (Figure 1).

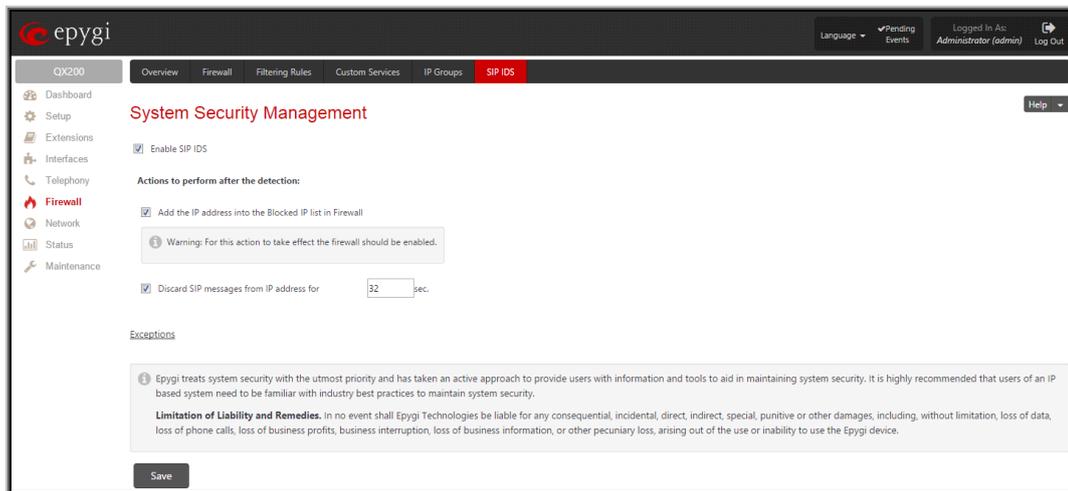


Figure 1: SIP IDS Settings page

**Please Note:** For **SIP IDS** to work the QX's Firewall will need to be enabled and at a minimum, be set to the Low Security level.

## 5 Securing Calls on Auto Attendant

By default, the QX is secured from unwanted calls through the use of the Auto Attendant. Only local PBX extensions are allowed to use the call routing rules for dialling to PSTN and IP networks. By default, external callers are unable to use the call routing rules for dialling PSTN and IP destinations when calling through the QX's Auto Attendant.

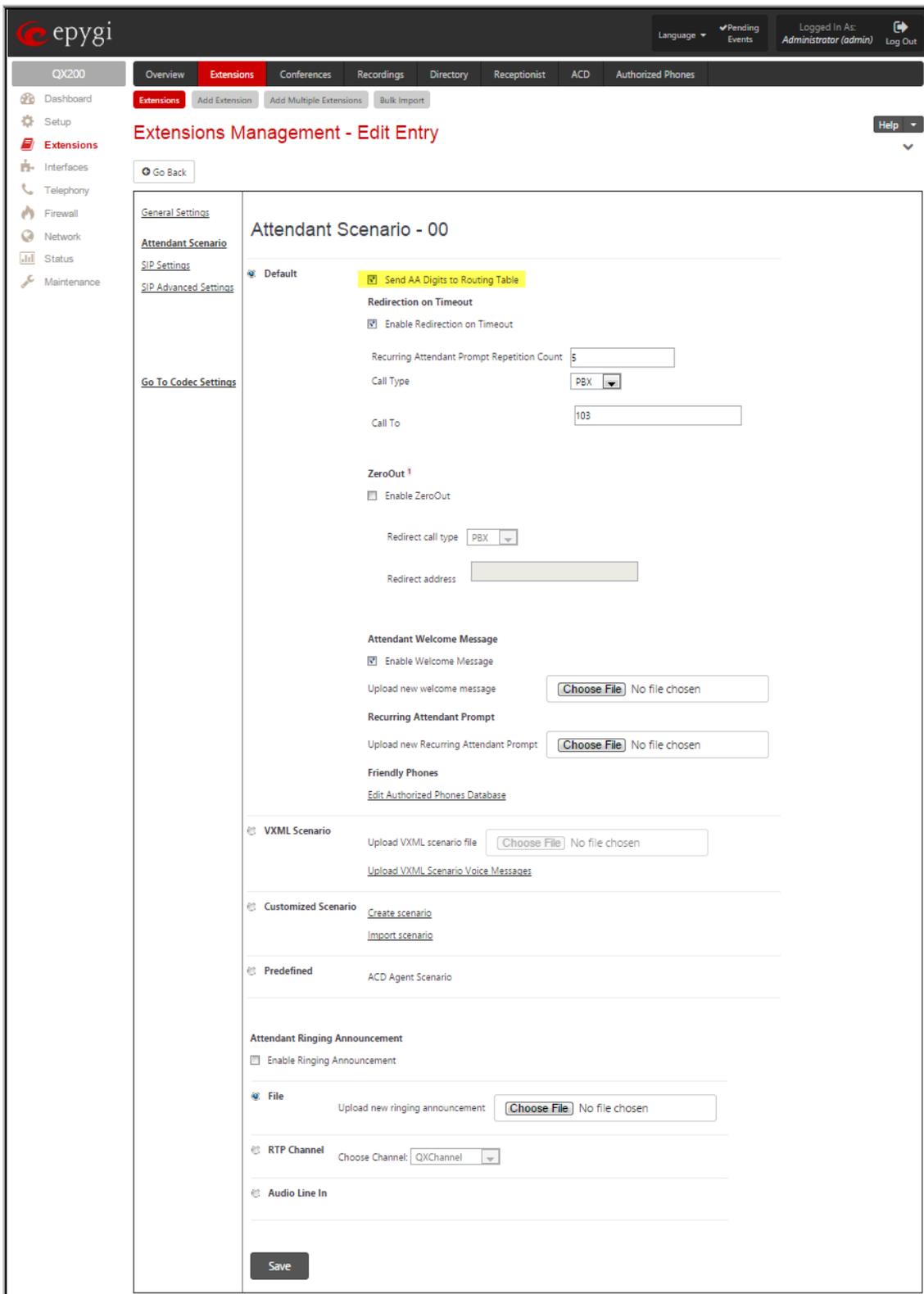
### 5.1 Control of the Dialed Digits on Auto Attendant

The Auto Attendant has a digit-parsing feature that can be enabled. This option can provide a lot of flexibility and dialling options for customers but it should be used with care. When the digit-parsing feature is enabled, all digits dialled by the caller while listening to the Auto Attendant greeting message, will be sent directly to the Call Routing table to determine the intended destination. With this option enabled the entries in the Call Routing table need to be properly secured.

By default, this option is disabled on the QX and all incoming calls to the Auto Attendant are limited to **ONLY** being able to dial PBX extensions.

The control for the digit-parsing feature is implemented via the "**Send AA Digits to Routing Table**" checkbox in the Auto Attendant settings. To check or change the status for this feature, follow the steps below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Extensions->Extensions** menu.
3. Click on the Auto Attendant extension.
4. Select the **Attendant Scenario** link (Figure 2).



The screenshot displays the 'Attendant Scenario - 00' configuration page in the Epygi QX200 web interface. The page is titled 'Extensions Management - Edit Entry' and is part of the 'Extensions' section. The configuration is for a 'Default' scenario. Key settings include: 'Send AA Digits to Routing Table' (checked), 'Redirection on Timeout' (checked), 'Recurring Attendant Prompt Repetition Count' (5), 'Call Type' (PBX), and 'Call To' (103). There are also sections for 'ZeroOut', 'Attendant Welcome Message', 'Recurring Attendant Prompt', 'VXML Scenario', 'Customized Scenario', and 'Predefined' scenarios. A 'Save' button is at the bottom.

Figure 2 Attendant Scenario page

**Please Note:** The Auto Attendant can be used in either the **Default** or **Custom** scenario type. This figure shows the **Default** scenario type for the Auto Attendant. By default the **“Send AA Digits to Routing Table”** option is not enabled. This is the recommended setting. If a **Custom** Auto Attendant scenario has been configured, then all digits are controlled by the custom XML script.

## 5.2 Using Call Relay on Auto Attendant

Even with the **“Send AA Digits to Routing Table”** option disabled there is still a possibility to send dialled digits directly to the Call Routing Table. It is done via the **Call Relay** feature, accessible by dialling **\*2** when the Auto Attendant is reached. After dialling **\*2** an authentication will be required - the extension number and the extension’s password. Once successfully entered, the caller can dial using entries listed in the Call Routing table. This is also a powerful option but it needs to be secured so that it is **ONLY** used by authorized callers.

The Call Relay option is enabled/disabled on a per extension basis. When enabling an extension to use **Call Relay** care should be taken to ensure a proper password is provided for the extension. The Call Relay feature cannot be used on the QX if it is not enabled on at least one of the extensions.

By default, **Call Relay** is disabled on all extensions. In addition, if **Call Relay** has been enabled and the extension password has not been set, a warning message will be displayed.

To check or change the status for the **Call Relay** service on an extension, follow the steps below:

1. Login as an Administrator to QX’s Web Management.
2. Go to **Extensions->Extensions** menu.
3. Choose the extension, click on the checkbox beside the extension number and press **Edit**.
4. Select the **General Settings** (
5. Figure 3).

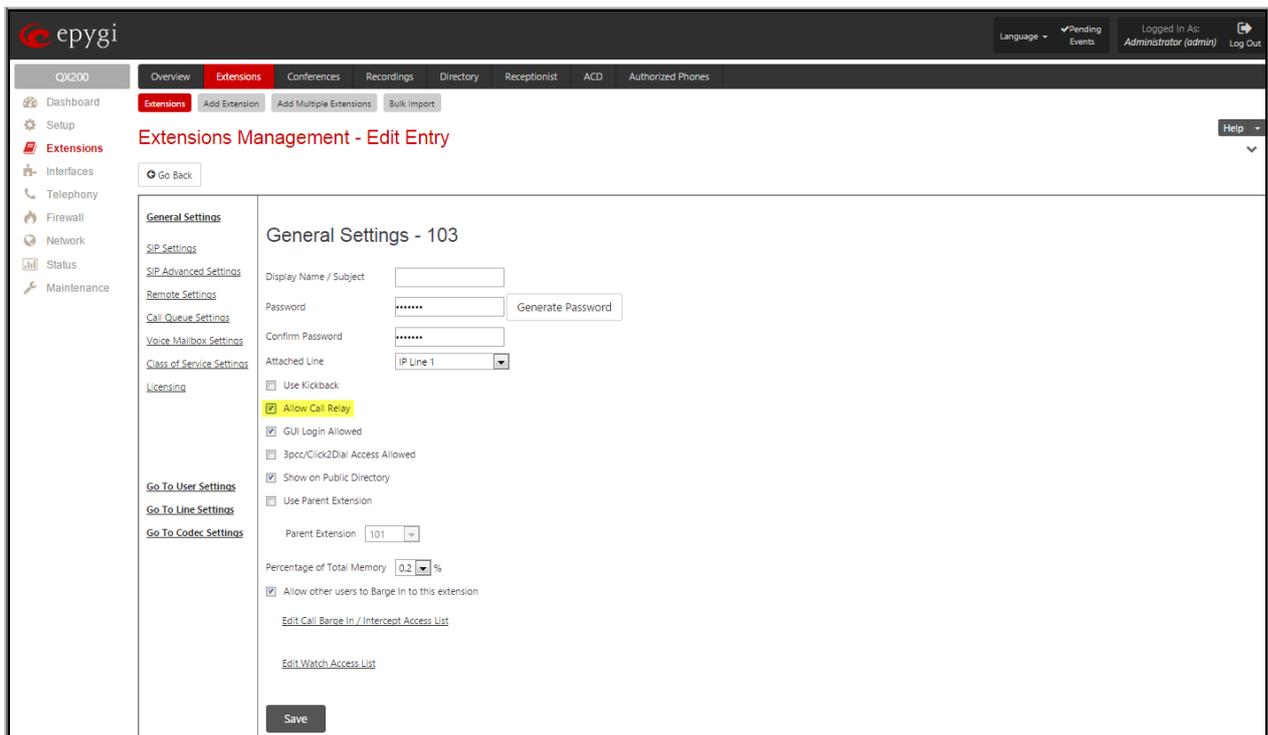


Figure 3 Extension’s General Settings page

**Please Note:** This figure shows extension 103 has been enabled to use the Call Relay option. This page also shows where to change the numerical password for the extension. When **“Send AA Digits to Routing Table”** is disabled and the Call Relay service has NOT been enabled on any extension, then incoming calls to the Auto Attendant can **ONLY** call to extensions.

## 6 Securing Call Routing rules from unwanted SIP calls

External callers can potentially use call routing rules on the QX. Unlike PSTN calls, SIP calls by default reach the Call Routing table directly, bypassing the Auto Attendant. Therefore, it is a high priority to secure the routing rules on the QX from unwanted external SIP calls.

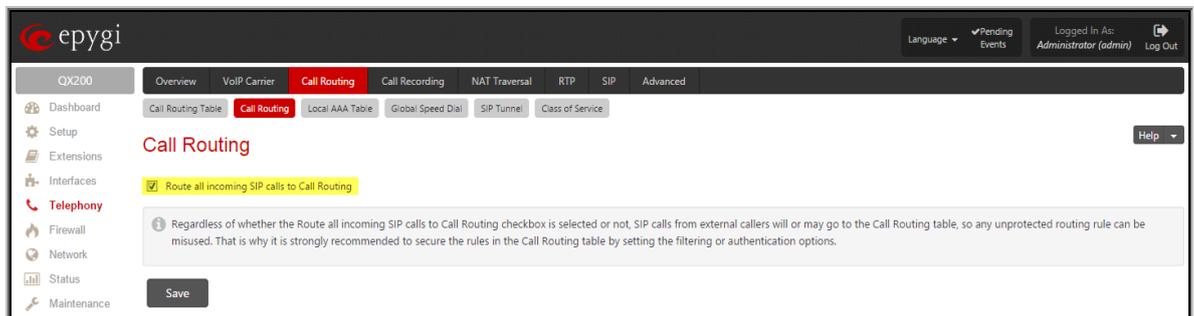


Figure 4 Call Routing page

**Attention:** Regardless whether the *Route all incoming SIP calls to Call Routing* checkbox is selected or not, SIP calls from external callers 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 (see [Using Filters on Call Routing Rules](#)) or authentication options (see [Using Local Authentication on Call Routing Rules](#)).

The **Route all incoming SIP calls to Call Routing** checkbox on the **Call Routing** page can be misleading. Disabling the **Route all incoming SIP calls to Call Routing** checkbox does not secure the QX. By default, this option is not selected and for each incoming SIP call, the QX will scan the extensions in the Extensions Management table to find the dialed SIP number. If the SIP number matches SIP User Name for an extension, the call will go to that extension. If there are no matches in the Extensions Management table, the Call Routing table will then be scanned for the dialed SIP number. When **Route all incoming SIP calls to Call Routing** is selected, the Call Routing table will be scanned directly, bypassing the initial search of the Extensions Management table.

## 7 Using Local Authentication on Call Routing Rules

Using local authentication to secure the QX's Call Routing entries can also be an effective way of adding another element of protection. The Local AAA Table can be used to create a list of trusted users (see Local AAA Table Configuration section below), for whom the corresponding Call Routing rule will be available.

A caller (local PBX user or external caller using digit-parsing from the Auto Attendant) trying to use a routing rule that has local authentication enabled, will need to pass the authorization on the pre-configured Local AAA Table. The authentication can be automatic by detecting the caller ID, manually by having the caller enter a specified login from the handset (username and password) or it can be by entering a PIN code.

If the authentication is successful, the caller will be able to use the call routing rule.

### 7.1 Local AAA Table Configuration

To configure the **Local AAA Table**, follow the instructions below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Telephony->Call Routing->Local AAA Table** menu.
3. Press **Add** to create a new authentication entry (or press **Edit** to change the settings of an existing entry). Local AAA Table – **Add Entry** page appears (Figure 5):

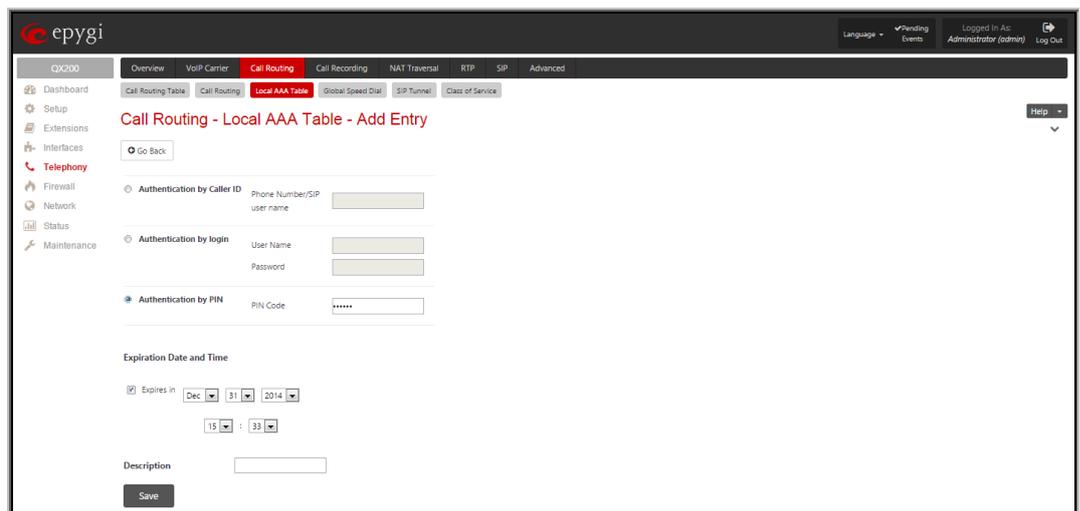


Figure 5 Local AAA Table – Add Entry page

Here you may choose the authentication type required for using the Call Routing rules (those rules that have the **Local Authentication** option enabled):

- **Authentication by Caller ID** – this is an automated method of authentication; it does not require any actions from the caller. When this type of authentication is chosen, the system will retrieve the caller ID (PSTN number or SIP username) of the caller and compare it with the number defined in the **Phone Number/SIP username** field on this page. If matched, the call will be allowed.
- **Authentication by Login** – this method of authentication requires the Username and the Password to be dialed by the caller. With this option selected, a Username and a Password needs to be defined in the corresponding fields. When the caller tries to use a Call Routing rule that requires local authentication, he will be prompted to dial the Username and then a Password. If the dialed authentication parameters match the ones inserted in this field, the user will be authenticated and the call will be allowed.
- **Authentication by PIN**- this selection is used to set the authentication based on the PIN. When the caller tries to use a Call Routing rule that requires local authentication, he will be prompted to dial the PIN number before the call will proceed. Only digit values are allowed for this field, otherwise the appropriate error message will be displayed.
- 4. Choose **Expiration Date and Time** options, if needed. This option is used to limit the registration parameters for a certain time frame. If you wish to use this option, click on the **Expires in** checkbox first and then define the date and time of the expiration from the corresponding drop down lists.
- 5. The **Description** text field is used to insert some optional information regarding the entry.
- 6. Press **Save** to add the registration with the provided parameters.

**Please Note:** The Username and Password defined in the Local AAA Table – **Add Entry** page are unique and are not connected to any other Username and Password defined on the QX. The Username and Password must be numerical since they will be entered from the

user's phone keypad.

## 7.2 Enabling local authentication on the Call Routing rules

To enable local authentication on a Call Routing rule, follow the instructions below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Telephony->Call Routing->Call Routing Table** menu.

- Press **Add** functional button to create a new rule (or select an existing rule and press **Edit** to change the settings). **Call Routing Wizard** is launched:
- On the second page of the wizard under **AAA Required** select Local Authentication checkbox (Figure 6).

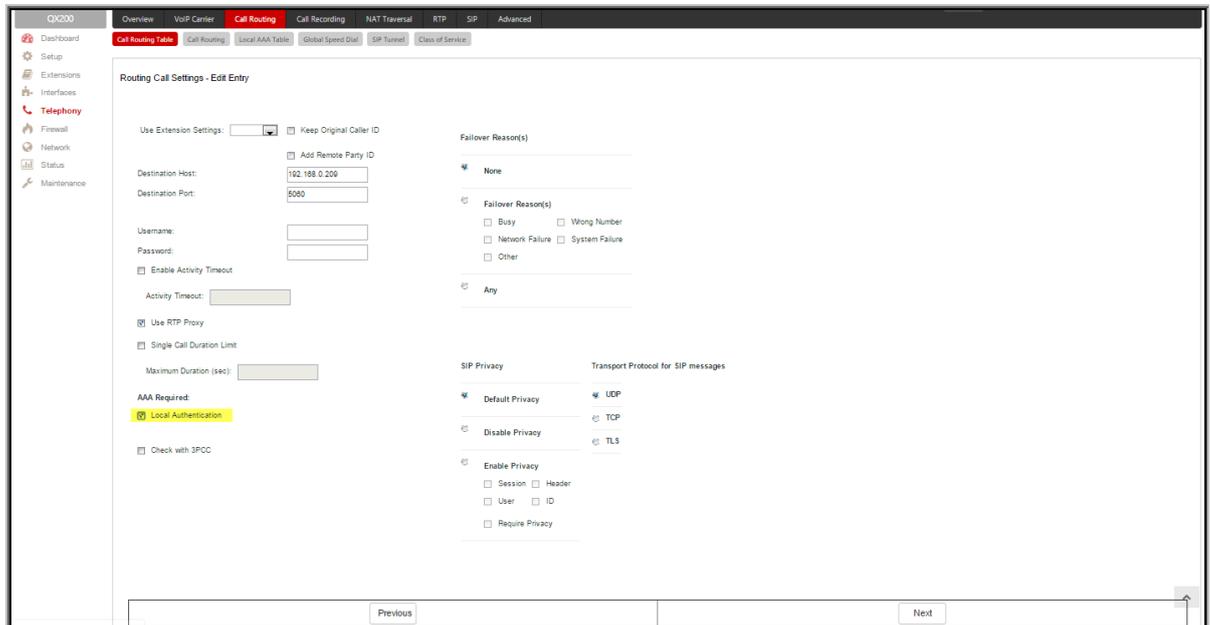
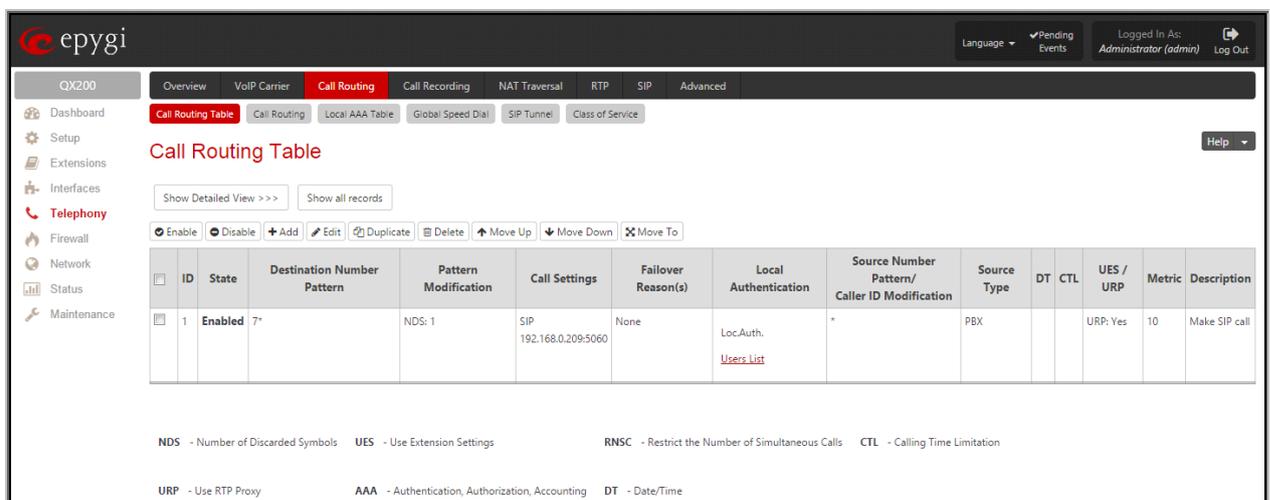


Figure 6 Call Routing Wizard – Page 2

- Proceed as needed in the wizard and finish it. The new/edited entry with local authentication will appear on the **Call Routing Table** (Figure 7).

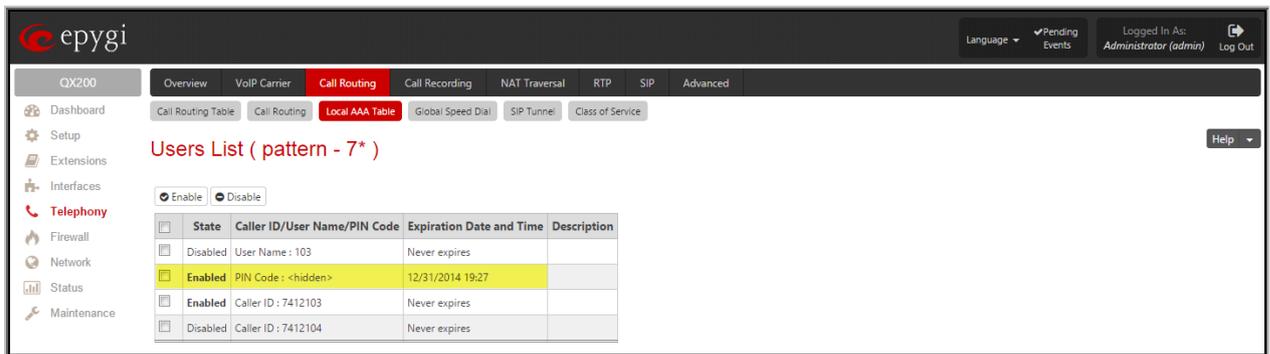


ID	State	Destination Number Pattern	Pattern Modification	Call Settings	Fallback Reason(s)	Local Authentication	Source Number Pattern/Caller ID Modification	Source Type	DT	CTL	UES / URP	Metric	Description
1	Enabled	7*	NDS: 1	SIP 192.168.0.209:5060	None	Loc.Auth. <a href="#">Users List</a>	*	PBX			URP: Yes	10	Make SIP call

NDS - Number of Discarded Symbols    UES - Use Extension Settings    RNSC - Restrict the Number of Simultaneous Calls    CTL - Calling Time Limitation  
 URP - Use RTP Proxy    AAA - Authentication, Authorization, Accounting    DT - Date/Time

Figure 7 Call Routing Table with newly created record

- On the **Call Routing Table**, press the **Users List** link in the **Local Authentication** column of the newly created/edited routing record. The **Users List** page for the corresponding routing record appears:



The screenshot shows the Epygi QX200 web interface. The top navigation bar includes 'Language', 'Pending Events', and 'Logged In As: Administrator (admin)'. The main menu is divided into 'Overview', 'VoIP Carrier', 'Call Routing', 'Call Recording', 'NAT Traversal', 'RTP', 'SIP', and 'Advanced'. Under 'Call Routing', there are sub-tabs for 'Call Routing Table', 'Call Routing', 'Local AAA Table', 'Global Speed Dial', 'SIP Tunnel', and 'Class of Service'. The 'Local AAA Table' tab is active, displaying a 'Users List (pattern - 7\*)'. Below the title are radio buttons for 'Enable' (selected) and 'Disable'. A table lists users with columns for 'State', 'Caller ID/User Name/PIN Code', 'Expiration Date and Time', and 'Description'.

State	Caller ID/User Name/PIN Code	Expiration Date and Time	Description
<input type="checkbox"/>	Disabled User Name : 103	Never expires	
<input checked="" type="checkbox"/>	Enabled PIN Code : <hidden>	12/31/2014 19:27	
<input checked="" type="checkbox"/>	Enabled Caller ID : 7412103	Never expires	
<input type="checkbox"/>	Disabled Caller ID : 7412104	Never expires	

Figure 8 Call Routing Table – Users List

This table contains all of the trusted users that have been entered in the Local AAA table.

- From the **Users List** table choose those trusted users that can use the corresponding routing rule, select the checkboxes beside the chosen users and press the **Enable** functional button.

Now, the created routing rule will be available for the callers enabled in the Users List table. The caller who doesn't match the enabled Caller ID will be asked for authorization by PIN code.

**Please Note:** The trusted users should be enabled in the Users List table each time any of the authentication settings are changed on the existing Call Routing rule.

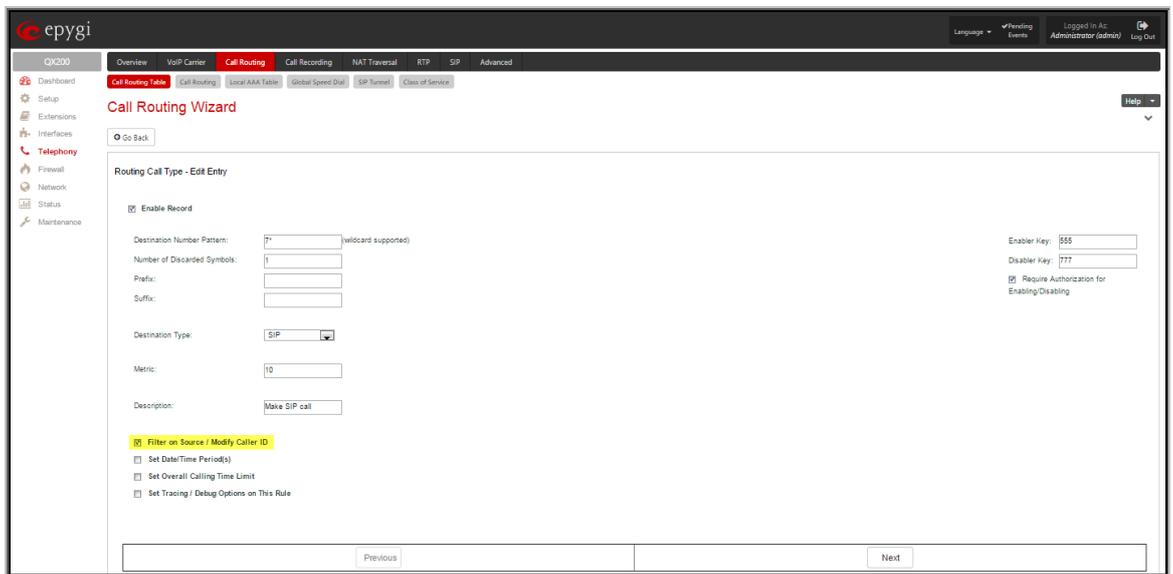
## 8 Using Filters on Call Routing Rules

Setting up filters on each call routing rule is one of the most effective and easiest methods to secure the QX from unwanted incoming and outgoing calls. For any outgoing call, the Call Routing table is used to determine the call path. Securing the long distance call routing entries is the single best way to prevent unauthorized calls.

When a filter is enabled on a Call Routing rule, only callers matching the filtering criteria will be allowed the use of that rule. This option directly restricts callers.

To configure filters on the Call Routing rules, follow the instructions below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Telephony->Call Routing->Call Routing Table** menu.
3. Press **Add** functional button to create a new routing rule (or press **Edit** to change the settings of an existing call routing rule). **Call Routing Wizard** is launched (Figure 9):



The screenshot shows the 'Call Routing Wizard - Edit Entry' page in the Epygi web management interface. The page is titled 'Routing Call Type - Edit Entry' and contains several configuration fields and checkboxes. The 'Filter on Source / Modify Caller ID' checkbox is checked and highlighted in yellow. Other fields include 'Destination Number Pattern' (with a wildcard symbol), 'Number of Discarded Symbols', 'Prefix', 'Suffix', 'Destination Type' (set to SIP), 'Metric' (set to 10), and 'Description' (set to 'Make SIP call'). There are also fields for 'Enable Record', 'Enabler Key', and 'Disabler Key'. The page has a 'Go Back' button and 'Previous' and 'Next' buttons at the bottom.

Figure 9 Call Routing Wizard – Page 1

4. Select the **Filter on Caller/Call Type/Modify Caller ID** checkbox.
5. Define the Call Routing rule as needed and press **Next** to move to the second page of the wizard.
6. Define the parameters on the second page of the Call Routing Wizard as needed and press **Next** to move to the third page of the wizard (Figure 10).
7. This page of the Call Routing Wizard appears only when the **Filter on Caller/Call Type/Modify Caller ID** checkbox has been previously selected on the first page of the wizard. This page is used to define the **Source Filter/Modify Caller ID** and other settings pertaining to the originator of the call.
8. The **Source Number Pattern** field requires the caller ID for which the Call Routing rule is applicable. Extensions, SIP usernames or PSTN numbers are applicable for this field. Letters, digits and any characters supported in the SIP username are also allowed for this field. Wildcard symbols can also be used - "\*" stands for any number of digits, "?" stands for one digit only. "[", "]", ",", "\_", "{", "}" are used to define a range or a quantity of numbers, "!" is used for exclusion.

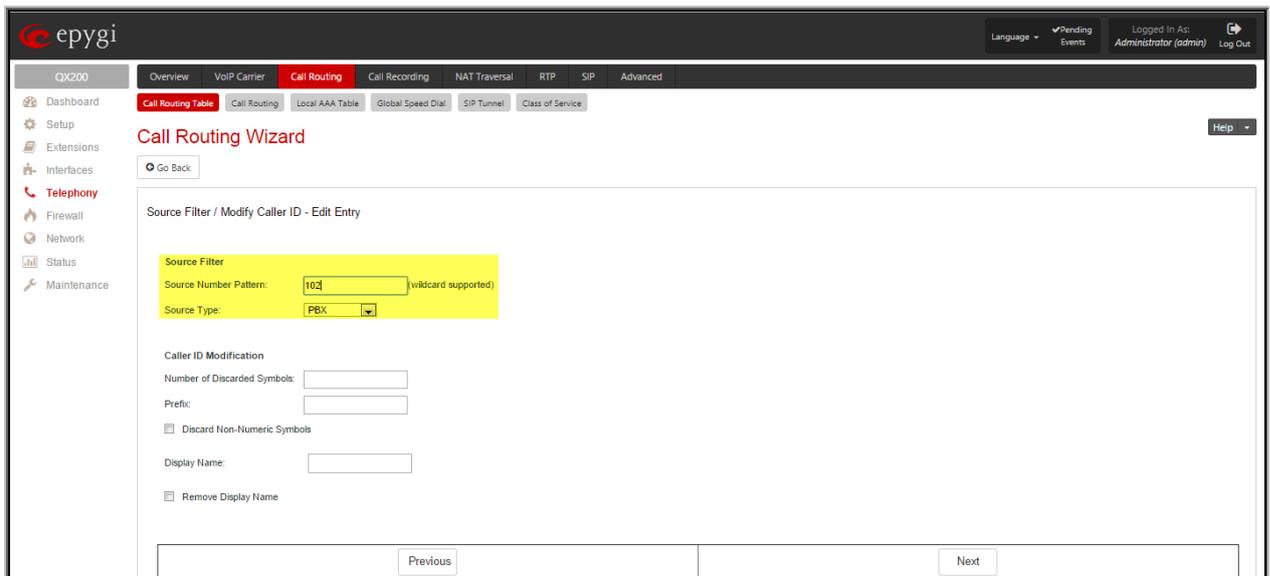


Figure 10 Call Routing Wizard – Source Filter/ Modify Caller ID page

### Examples:

The pattern 2[3,7] makes this rule available for extensions 23 or 27,

The pattern {11, 15, 23, 38, 45} makes this rule available for extensions 11, 15, 23, 38 and 45,

The pattern 2{15-30,!17} makes this rule available for extensions in the range: 215 to 230, with the exception of extension 217,

The pattern 083??????? makes this rule available for callers with caller ID starting with 083 and followed by seven digits.

9. Choose the **Source Type** from the drop down list to determine which category of callers will be allowed to use the specified routing entry.
  - Any – means that the routing entry is allowed to be used by any originating call type.
  - PBX - means that the routing entry is ONLY allowed to be used by QX local extensions. This is the default and recommended entry.
  - SIP – means that the routing entry is ONLY allowed to be used by SIP originated callers.
  - PSTN – means that the routing entry is ONLY allowed to be used by PSTN originated callers.

**Please Note:** Pay particular attention when choosing “Any” for the Call Type since the QX may not correctly determine that the caller ID is an extension, a PSTN number or a SIP username.

Other fields on this page are used to change the caller ID but they are not important to securing the use of Call Routing entries.

10. Proceed next as needed in the wizard and finish it.

Now the corresponding Call Routing rule will only be applicable to the caller whose caller ID will match to the number inserted into the **Source Number Pattern** text field. In the example shown in the Figure 10, the selected routing rule will only be available for PBX extension 102 on the QX.

## 8.1 Using Date/Time Limitations on Call Routing Rules

You may also secure Call Routing rules by limiting their availability for a certain time frame. When the caller attempts to use the specific Call Routing rule outside of the configured time frame, he will be denied access.

To configure date/time limitations on the Call Routing rules, follow the instructions below:

1. Login as an Administrator to QX’s Web Management.

2. Go to **Telephony->Call Routing->Call Routing Table** menu.
3. Press **Add** functional button to create a new call routing rule (or press **Edit** to change the settings of an existing call routing rule). **Call Routing Wizard** is launched (Figure 11):

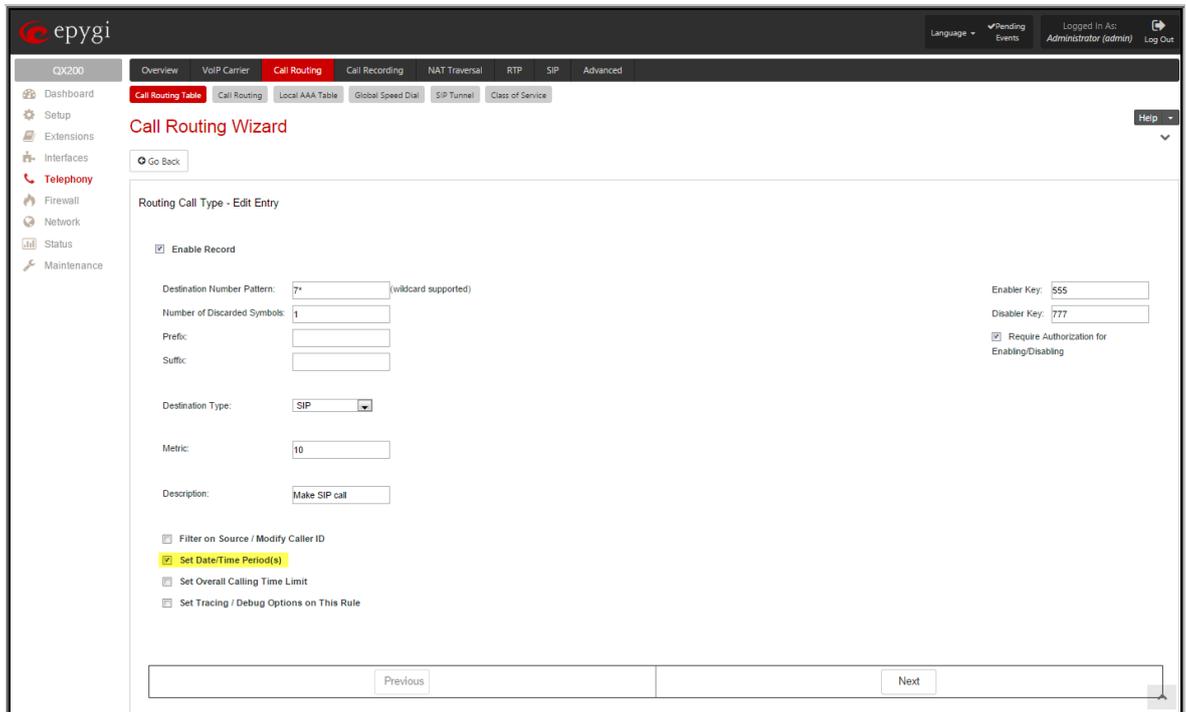


Figure 11 Call Routing Wizard – Page 1

4. Select the **Set Date/Time Period(s)** checkbox.
5. Define the Call Routing rule as needed and press **Next** to move to the second page of the wizard.
6. Define the parameters on the next page of the Call Routing Wizard as needed and move forward until the **Date/Time Rules** page is reached.

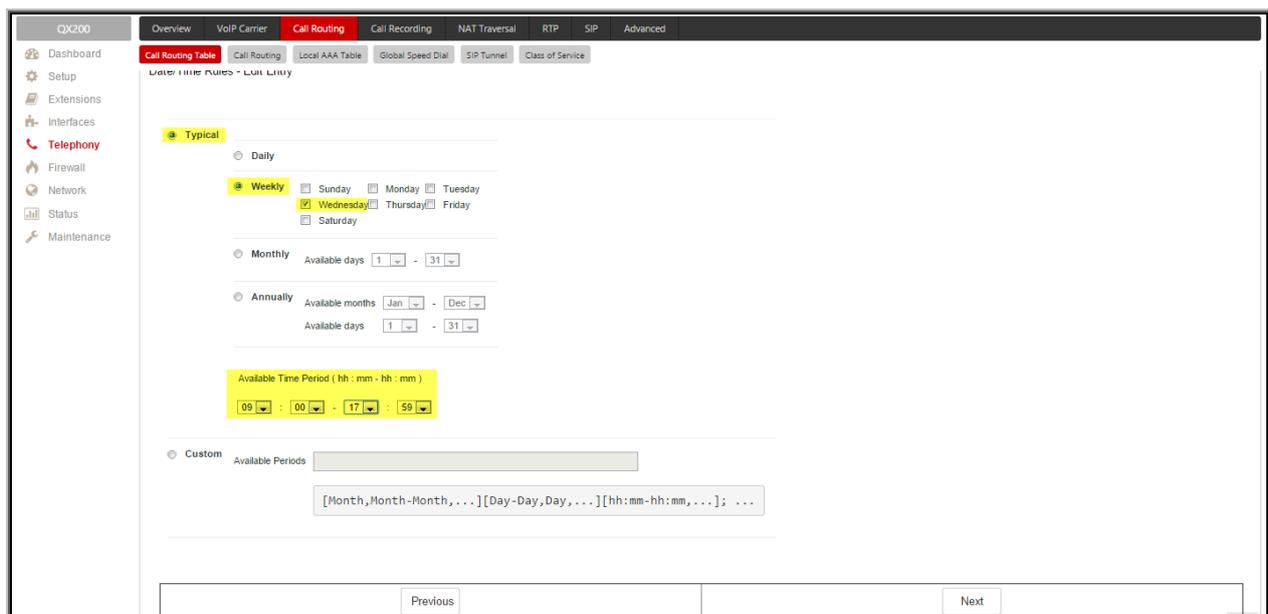


Figure 12 Call Routing Wizard –Date/Time Rules page

7. On the **Date/Time Rules** page you may define the validity period(s) of the selected Call Routing rule. You may choose between **Typical** and **Custom** time/date definitions.

The **Typical** selection contains a group of radio buttons that are used to select the frequency that the corresponding routing pattern will be in effect:

- **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 **Available Time Period** drop down lists, the time range of the pattern validation should be defined. The time selected in this field will be in relation to the QX's Time/Date Settings.

Custom selection provides a possibility 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,...]; ...

8. Proceed next as needed in the wizard and finish it.

Now the corresponding Call Routing rule will only be applicable in the defined time frame. In the example shown in Figure 12, the selected routing rule will be available weekly, every Wednesday from 9AM to 17:59PM.

### 8.1.1 Examples

This section provides examples on configuring the **Time/Date** limitations on the Call Routing entries with an explanation on how it is used.

#### Example 1

**Purpose** - User plans to configure the QX IP PBX so all incoming FXO calls during working hours (from 9:00 to 18:00) will ring on all available extensions. After working hours (from 18:00 to 9:00) and on the weekends, all incoming FXO calls will be forwarded to the Auto Attendant.

**To Implement** – Two routing rules should be created in the Call Routing table. One of the routing rules should have a **Time/Date** limitation service configured. The **Many Extension Ringing** service should be enabled to allow the call to ring on all extensions at the same time.

**To Configure** -

1. Go to **Telephony->Call Routing->Call Routing Table**. Add a new routing rule with the following parameters:
  - Pattern – 555
  - Number of Discarded Symbols – 3
  - Prefix – 110
  - Call Type - PBX
  - Set Date/Time Period(s) – enabled
  - Leave other settings unchanged.
2. On the **Source Filter / Modify Caller ID** page, set the Source Type to **FXO**.
3. On the **Date/Time Rules** page set the **Weekly** selection and select only working days (Monday, Tuesday, Wednesday, Thursday and Friday). Select the **Available Time Period** in the interval between 9:00 to 18:00. Finish the Call Routing Wizard.
4. Add another entry in **Call Routing Table** with the following parameters:
  - Pattern – 555
  - Number of Discarded Symbols – 3
  - Prefix – 00 (default auto attendant)
  - Call Type - PBX
 On the **Source Filter / Modify Caller ID** page, set the Source Type to **FXO**.

Leave other settings unchanged. Finish the Call Routing Wizard. The second entry should be listed below the previous entry in the **Call Routing Table**. This is important since entries will be matched from top down.

5. Go to the **Extension->Extension** menu, select 110 (for the current example) and go to the **Caller ID Services**. Enable **Many Extension Ringing (MER)** service from **CallerID Based Services** table. Enable all extensions in the list to participate in the **Many Extensions Ringing** for 110.
6. Go to **Telephony->FXO** page. Set the **Route Incoming FXO calls** to **Routing** for all FXO lines. Insert the Routing pattern that will be also used in Call Routing table (for current example: 555).

**Result** – Weekdays during working hours (from 9:00 to 18:00), all incoming FXO calls will ring on all phones on the QX IP PBX. Whoever will pick up the call will get it first. After working hours, as well as on weekends (Saturday and Sunday), all incoming FXO calls will be answered by the Auto Attendant.

## Example 2

**Purpose** - User plans to configure the QX IP PBX so all incoming FXO calls during working hours (from 9:00 to 18:00) will ring on extension 102. If extension 102 is unable to answer, the call should be forwarded to a mobile number. After working hours (from 18:00 to 9:00) and on weekends, all incoming FXO calls will be directly forwarded to the voice mailbox of extension 102, without ringing.

**To Implement** – Two routing rules should be created in the Call Routing table. One of the routing rules will have a **Time/Date** limitation service configured. The **No Answer Call Forwarding** service should be enabled to allow the call to be forwarded to the mobile phone.

### **To Configure -**

1. Go to **Telephony->FXO** page. Set the **Route Incoming FXO calls** parameter to **Routing** for all FXO lines. Insert the Routing pattern that will be also used in the Call Routing table (for current example: 333).
2. Go to the **Caller ID Services** for extension 102 (for the current example) and activate the **No Answer Call Forwarding** service for the specific FXO caller. The destination address should be the user's mobile phone number.
3. Go to **Telephony->Call Routing->Call Routing Table**. Add a new routing rule with the following parameters:

Pattern – 333

Number of Discarded Symbols – 3

Prefix - 102

Call Type - PBX

Set Date/Time Period(s) – enabled

4. On the **Source Filter / Modify Caller ID** page, set the Source Type to FXO.
5. Move forward to the **Date/Time Rules** page of the **Call Routing Wizard**. Choose the **Weekly** selection and select only working days (Monday, Tuesday, Wednesday, Thursday and Friday). Select the **Available Time Period** in the interval between 9:00 to 18:00. Finish the Call Routing Wizard.
6. Add another routing rule to the **Call Routing Table** with the following parameters:

Pattern – 333

Number of Discarded Symbols – 3

Prefix - 102

Call Type – **PBX-Voicemail**

Leave other settings unchanged. Finish the Call Routing Wizard. The second entry should be listed below the previous entry in the **Call Routing Table**. This is important since entries will be matched from top down.

**Result** – During working hours (from 9:00 to 18:00) on each working day, all incoming FXO calls will ring on extension 102 on the QX IP PBX. If nobody answers, the call will be forwarded to the user’s mobile phone number. After working hours, as well as on weekend days (Saturday and Sunday), all incoming FXO calls will go to the voice mailbox of extension 102.

### **Example 3**

**Purpose** - User plans to configure the QX IP PBX so all incoming **ISDN** calls during working hours (from 9:00 to 18:00) will be answered by the Auto Attendant with default welcome message. After working hours (from 18:00 to 9:00) and on the weekends, all incoming ISDN calls will be answered by the Auto Attendant with custom welcome message.

**To Implement** – In order to achieve the above mentioned requirements need to create a new Auto Attendant extension (let say 10 for this example) additionally to the default 00 Auto Attendant. And two routing rules in the call routing table for QX IP PBX. These routing rules have the same pattern. The following instructions describe how to create the needed routing rules. For this scenario both two routing rules have the same pattern – 555.

#### **To Configure –**

1. First go to the **Extensions Management** and add a new Auto Attendant extension (for example 10).
2. Go to **Interfaces->ISDN Trunk Settings**, run the **ISDN Wizard** for selected ISDN Trunk(s), and change **Route Incoming Call to** extension 110 (for this example).
3. Go to **Telephony->Call Routing->Call Routing Table**. Add a new routing rule with the following parameters:

Pattern – 555

Number of Discarded Symbols – 3

Prefix –00

Call Type - PBX

Set Date/Time Period(s) – enabled

Leave other settings unchanged.

4. On the **Source Filter / Modify Caller ID** page, set the Source Type to **ISDN**.
5. On the **Date/Time Rules** page set the **Weekly** selection and select only working days (Monday, Tuesday, Wednesday, Thursday and Friday). Select the **Available Time Period** in the interval between 09:00 to 18:00. Finish the Call Routing Wizard.
6. Add another routing rule to the **Call Routing Table** with the following parameters:

Pattern – 555

Number of Discarded Symbols – 3

Prefix –10

Call Type - PBX

7. On the **Source Filter / Modify Caller ID** page, set the Source Type to **ISDN**.
8. Finish the Call Routing Wizard.
9. Go to the **Extensions->Extensions Management** menu, select 110 (for the current example) and go the **Caller ID Services**. Enable **Unconditional Call Forwarding** with the settings:

Call Type - Auto

Forward To - 555

Press **Save**.

10. And finally go to **Extensions->Extensions Management** menu, select the Auto Attendant extension 10 and upload a new welcome message for 10.

**Result** – Weekdays during working hours (from 9:00 to 18:00), all incoming ISDN calls will be answered by the default greeting for Auto Attendant 00. After working hours, as well as on weekends (Saturday and Sunday), all incoming ISDN calls will be answered by the custom greeting for Auto Attendant 10.

## 8.2 Using Overall Calling Time Limitations on Call Routing Rules

You may also secure Call Routing rules by limiting the overall call duration for all calls over a specific time frame for each Call Routing entry. Using the overall calling time limitation on call routing rules allows reducing the possible damage in case if unauthorized user access the system to make long distance calls.

To configure Overall Calling Time Limit on the Call Routing rules, follow the instructions below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Telephony->Call Routing->Call Routing Table** menu.
3. Press **Add** functional button to create a new routing rule (or press **Edit** to change the settings of an existing call routing rule). **Call Routing Wizard** is launched (Figure 13):

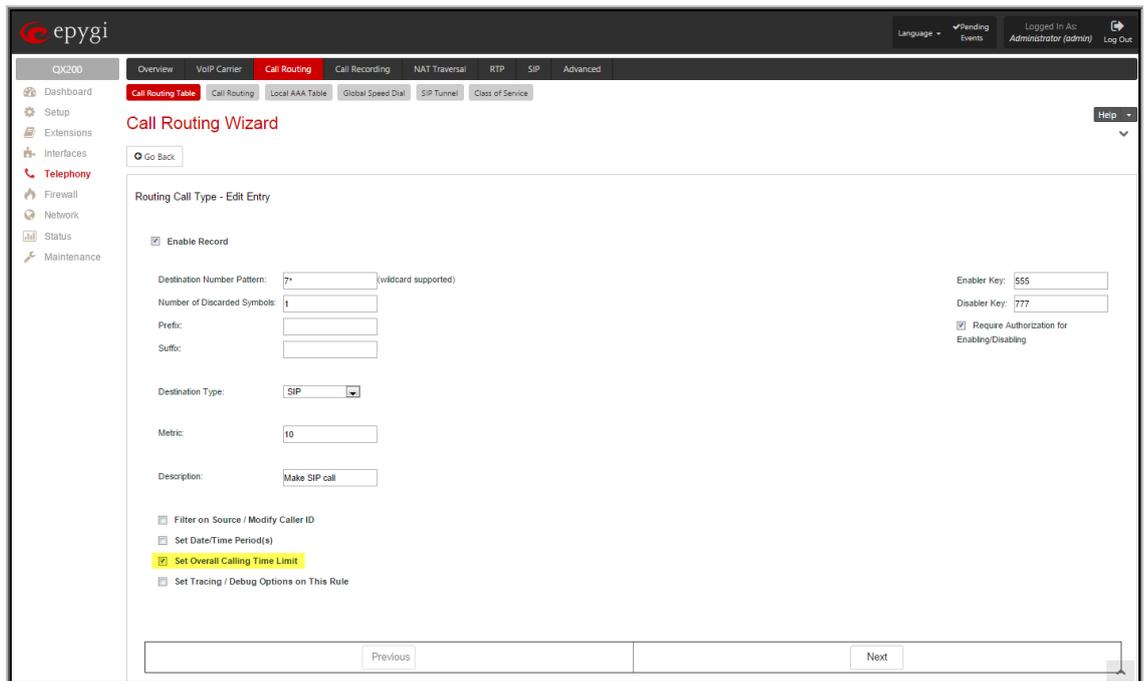


Figure 13 Call Routing Wizard – Page 1

4. Select the **Set Overall Calling Time Limit** checkbox.
5. Define the Call Routing rule as needed and press **Next** to move to the second page of the wizard.
6. Define the parameters on the next page of the Call Routing Wizard as needed and move forward until the **Routing Overall Calls Limitation** page is reached.

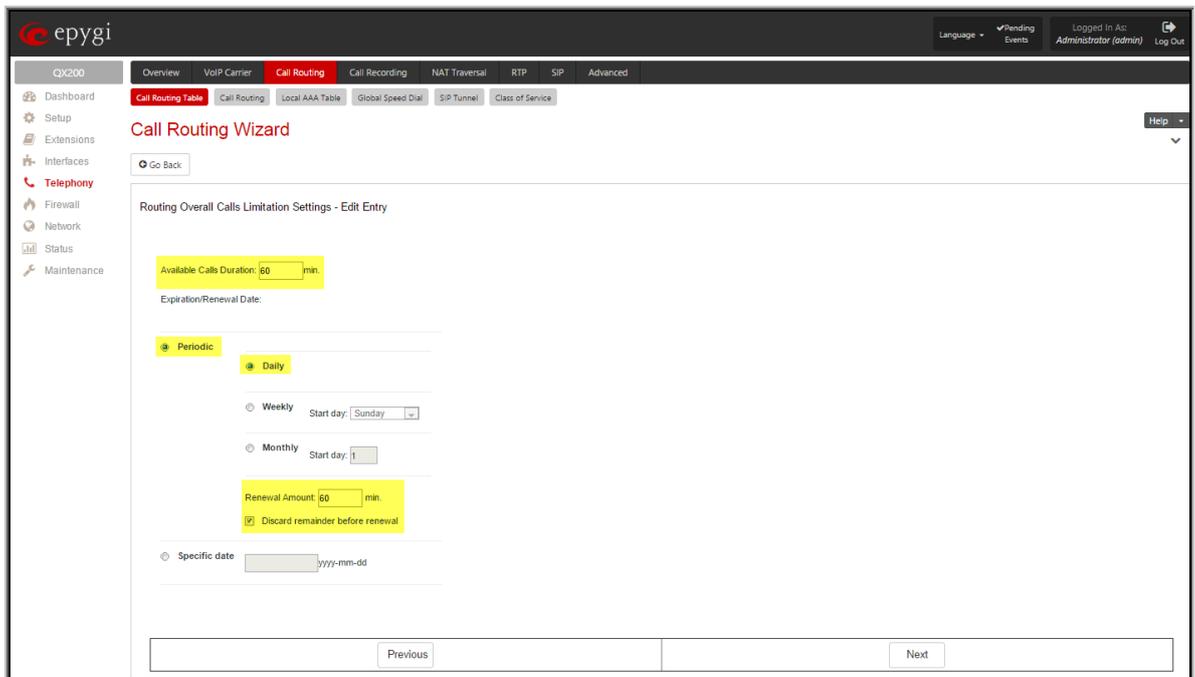


Figure 14 Call Routing Wizard – Routing Overall Calls Limitation Settings page

7. On the **Routing Overall Calls Limitation** page you may define the available duration of the calls with the selected routing rule as well as to specify the **Expiration/Renewal Date** for the available calls duration. The **Routing Overall Call Limitation Settings** page consists of the following components:

- The **Available Calls Duration** text field requires the maximum available duration of the calls (in minutes) placed with the selected routing rule. Once the **Available Calls Duration** reaches the value defined here, the current call will be disconnected without prior notice and no new call will be possible until this field is updated.
- The **Expiration/Renewal Date** settings are used to configure the **Expiration Date** and **Renewal Amount** of the **Available Calls Duration**. **Expiration/Renewal Date** field provides selection between Periodic and Specific Date.
  - The **Periodic** selection is used to define the expiration date of the allocated **Available Calls Duration** for the selected routing rule and has the following options:
    - **Daily**
    - **Weekly**
    - **Monthly**
  - The **Renewal Amount** text field requires the renewal amount (in minutes) to be added to the **Available Calls Duration** when the expiration date of the **Available Calls Duration** is reached.
  - The **Discard remainder before renewal** option selection allows discarding the remainder of **Available Calls Duration** before renewal and setting the **Renewal Amount** as an Available Calls Duration.
  - The **Specific Date** selection provides a possibility to manually define the expiration date allocated for the **Available Calls Duration** for the selected routing rule. When the **Specific Date** expires, the selected routing rule becomes unavailable automatically and no new call will be possible until this field is updated.

8. Proceed **next** as needed in the wizard and finish it.

## 8.2.1 Examples

This section provides examples on configuring the Overall Calling Time Limitations on the Call Routing entries with an explanation on how it is used.

### Example 1

**Purpose** - User plans to configure the QX so outgoing FXO calls will be available only 45 minutes until the end of the day and add renewal amount (15 minutes) to the remainder of the available calls duration when the expiration date is reached.

**To Implement** – A calling time limitation routing rule should be created.

**To Configure** -

1. Go to *Telephony->Call Routing->Call Routing Table*. Add a new routing rule with the following parameters:
  - Pattern – 555
  - Number of Discarded Symbols – 3
  - Destination Call Type - FXO
  - Set Overall Calling Time Limit – enabled
  - Leave other settings unchanged.
2. Move forward to the **Calling Time Limitation Rules** page of the **Call Routing Wizard**. Specify 45 minutes in the **Available Calls Duration** text field. Choose the **End of day** option and set **Renewal Amount** to 15 minutes. Finish the Call Routing Wizard.

**Result** – All outgoing FXO calls will be available only 45 minutes until the end of the day. When the expiration date is reached, additional 15 minutes will be added to the available calls duration.

### Example 2

**Purpose** - User plans to configure the QX so outgoing FXO calls will be available only 45 minutes for each calendar day.

**To Implement** – A calling time limitation routing rule should be created.

**To Configure** -

1. Go to *Telephony->Call Routing->Call Routing Table*. Add a new routing rule with the following parameters:
  - Pattern – 333
  - Number of Discarded Symbols – 3
  - Call Type - FXO
  - Set Overall Calling Time Limit – enabled
  - Leave other settings unchanged.
2. Move forward to the **Calling Time Limitation Rules** page of the **Call Routing Wizard**. Specify 45 minutes in the **Available Calls Duration** text field. Choose the **End of day** option, set **Renewal Amount** to 45 minutes and enable the **Discard remainder before renewal** option. Finish the Call Routing Wizard.
 

Leave other settings unchanged. Finish the Call Routing Wizard.

**Result** – All outgoing FXO calls will be available only 45 minutes until the end of calendar day. When the expiration date is reached, system will discard the remainder of the Available Calls Duration and set a new 45 minutes for the available calls duration.

## 9 Securing 3PCC calls

The QX's "CallControl" interface allows remote applications to use the QX's facilities to make and handle various calls and to subscribe to some event notifications from the QX. Epygi has developed several applications that work through the 3pcc (Third Party Call Control) interface. Many customers have also written their own applications.

Any application should pass authentication on the QX before it is granted access to use the interface. In some scenarios the 3pcc application can perform an action depending on the user access privileges. There are three different user types that are allowed access privileges:

- **Admin**
- **Localadmin**
- **Extension**

The Admin, Localadmin and extensions are authorized to use the "CallControl" interface.

### 9.1 Extensions 3pcc/Click2Dial Login Allowed option

Every extension has a "**3pcc/Click2Dial Login Allowed**" option. This option enables the current extension to be used with applications based on the QX 3PCC interface, such as the **QX ClickToDial** and **CallControl Pack** applications.

By default, the "**3pcc/Click2Dial Login Allowed**" option is disabled on all extensions.

To activate/deactivate the **3pcc/Click2Dial Login Allowed** option on an extension, follow the steps below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Extensions->Extensions** menu.
3. Choose the extension, click on the checkbox beside the extension number and press **Edit**.
4. Select the **General Settings** (see Figure 15).

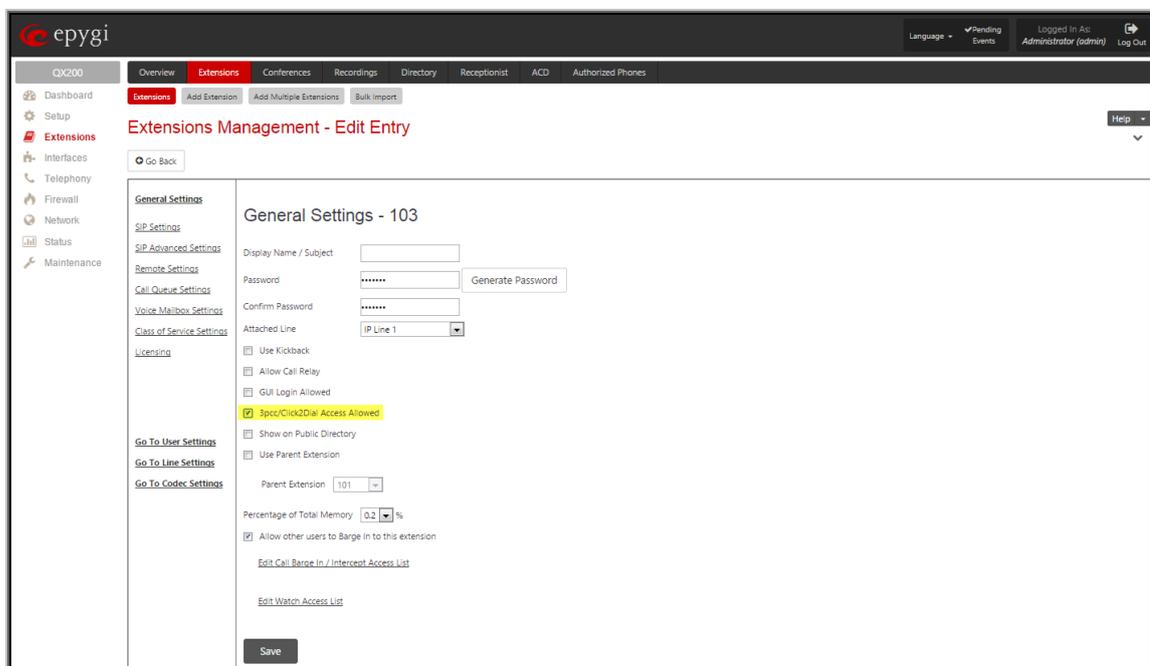


Figure 15 Extensions Management - Edit Entry – General Settings page

**Please Note:** The extension password is empty by default, so if you enable the "**3pcc/Click2Dial Login Allowed**" option on the extension and don't set a password on that extension, it will be possible to be authenticated on the QX from 3pcc with the extension number and a blank password.

## 9.2 Admin and Local admin access

The Admin's and Localadmin's Phone Passwords should be changed. The 3pcc application can be authenticated by the Admin and Localadmin Phone Passwords. Even if the GUI passwords are changed for Admin and Localadmin users, the 3pcc applications can still be authorized on the QX using the default passwords, because the 3pcc applications are being authorized by the Admin and Localadmin phone passwords and not by the GUI passwords.

# 10 System Security Management

The **System Security Diagnostics** tool is one of the **System Security Management** tools, which allows the security audit to be run and the resulting security report to be displayed.

To access the **System Security Diagnostics** follow the steps below:

1. Login as an Administrator to QX's Web Management.
2. Go to **Maintenance->Diagnostics->Security Diagnostics** menu.
3. Press the **Start Security Audit** button(see Figure 16).

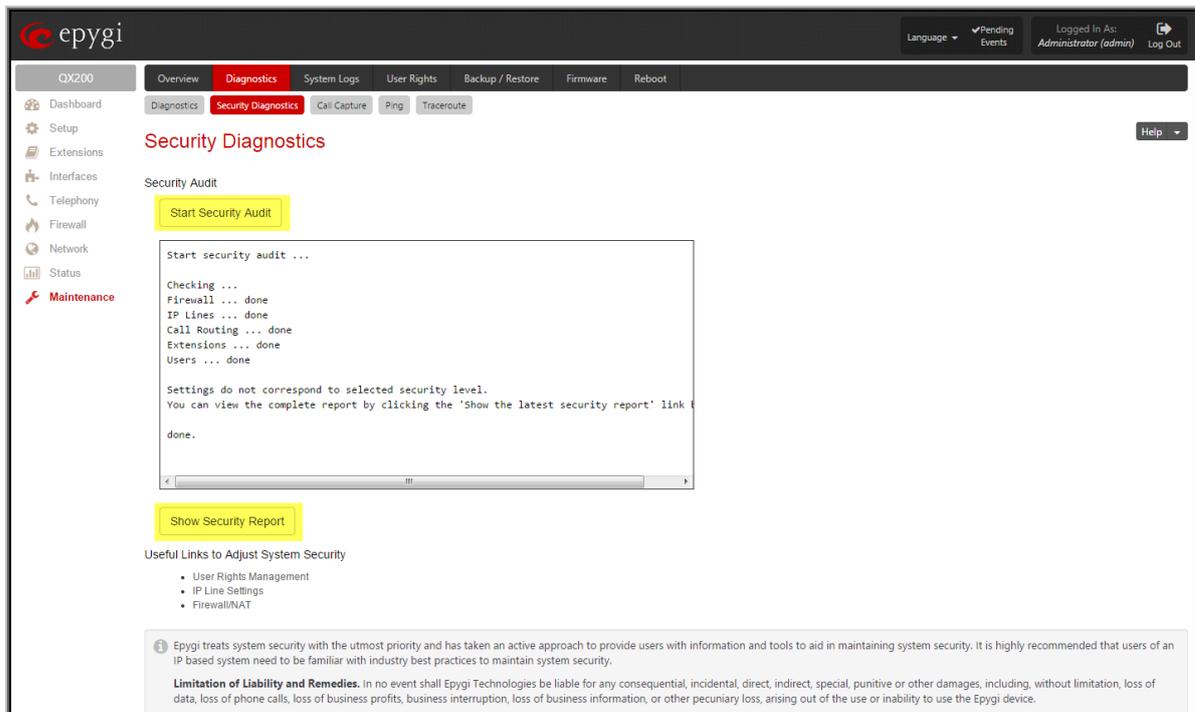


Figure 16 System Security Diagnostics page

The QX **Security Audit** is a security reporting system, which generates the warnings regarding the QX's weaknesses relative to the selected **Security Level**.

The warnings may vary depending on the selected global **Security Level**. The **Security Audit** will detect the security related configuration issues in Firewall, IDS, IP Line passwords, Call Routing and extension settings and display the last **Security Report**.

From this report the administrator can identify possible security concerns in the QX configuration settings.

The final reports of the **Security Diagnostics** can differ depending on the **System Security Settings** level (can be configured from the **Setup->System Security** menu).

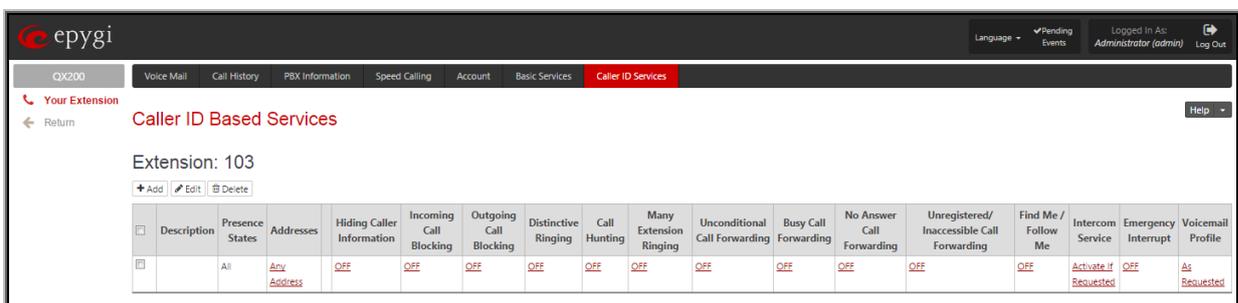
## 11 Incoming and Outgoing Call Blocking

The Incoming and Outgoing Call Blocking option is configured on each individual extension to block incoming/outgoing calls to specific numbers. It can be configured by the Administrator or by the extension user. The Call Blocking entries created by the Administrator can be protected from access by the extension user.

To access the Call Blocking pages of an extension, the Administrator should perform the following steps:

1. Login to the QX's Web Management as Administrator (username "admin").
2. Go to **Extensions->Extensions** menu.
3. Find the needed extension in the list and press on the corresponding extension number. The **Voice Mail->Voice Mailbox** page appears.
4. Navigate to **Caller ID Services** menu.

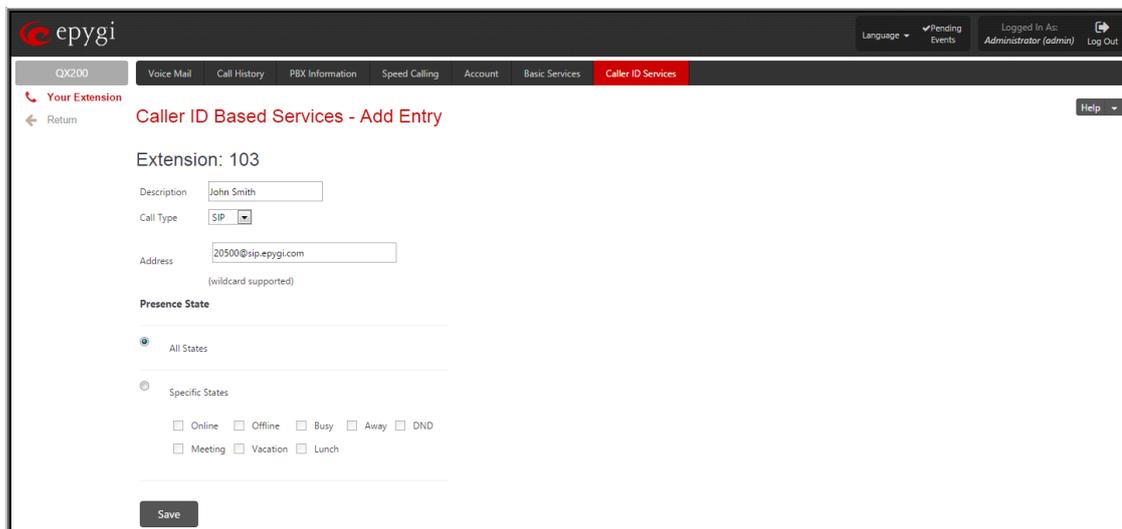
The **Caller ID Based Services** table appears:



	Description	Presence States	Addresses	Hiding Caller Information	Incoming Call Blocking	Outgoing Call Blocking	Distinctive Ringing	Call Hunting	Many Extension Ringing	Unconditional Call Forwarding	Busy Call Forwarding	No Answer Call Forwarding	Unregistered/Inaccessible Call Forwarding	Find Me / Follow Me	Intercom Service	Emergency Interrupt	Voicemail Profile
<input type="checkbox"/>		All	<a href="#">Any Address</a>	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	Activate if Requested	OFF	As Requested

Figure 17 Caller ID Based Services page

5. Press the **Add** functional button to add a new called (dialled number from the extn.) or caller (caller-Id received from an incoming call) destination on which call-blocking restrictions should take place. This functional button opens **Caller ID Based Services – Add Entry** page:



Extension: 103

Description:

Call Type:

Address:   
(wildcard supported)

Presence State

All States

Specific States

Online  Offline  Busy  Away  DND

Meeting  Vacation  Lunch

Figure 18 Caller ID Based Services – Add Entry page

6. Fill in a short description of the address owner into **Description** text field.
7. Choose the **Call Type** from the same named drop-down list:
  - PBX - local QX extensions and Auto Attendant.
  - SIP – caller or called destinations reached through a SIP server.
  - PSTN – caller or called destination dialled from or to the PSTN (FXO or E1/T1 port)

- Auto – used for undefined call types. In this case, for incoming calls from specific address, configuration of caller ID based services will apply either to PBX, SIP or PSTN callers. For outgoing calls, the called destination will be reached through Routing.
8. Type in the destination number into **Address** text field. This text field requires a SIP address, an extension or a PSTN number, for whom supplementary services should be applied. A wildcard is allowed in this field. Entering “\*” as PBX or PSTN addresses will block incoming or outgoing calls for all extensions or PSTN users. Two digits should be inserted in the **Address** text field for the PBX call type. The PSTN number length depends on the area code and phone number.
  9. Press **Save** to create a new entry with the defined settings. Once saved, a new entry will appear in the **Caller ID Based Services** table.
  10. Click on the newly created address in the **Caller ID Based Services** table. A page where supplementary services for the selected address can be configured appears.
  11. Go to **Incoming Call Blocking** or **Outgoing Call Blocking** functional link on the left side of the page, dependent on what restriction you wish to configure for the selected extension regarding the newly added address.

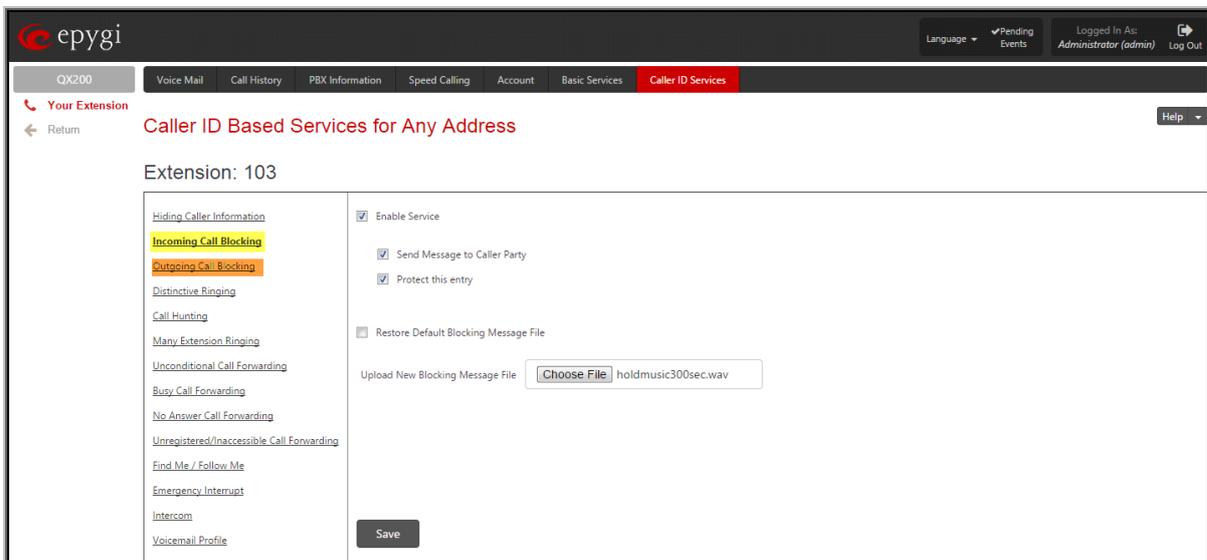


Figure 19 Incoming Call Blocking page

12. Select **Enable Service** checkbox to enable the incoming/outgoing blocking on the extension for the certain address.
13. Choose **Protect this Entry** checkbox if you want this blocking entry to be protected from access by the extension user. When this checkbox is selected, the extension user will not see this blocking when accessing the Caller ID Based Service page. The extension user will also be unable to deactivate this blocking entry.
14. Press **Save** to apply configuration.

**Please Note:** The same steps can be used to block any other incoming or outgoing destinations. The extension user can access the QX’s Web Management with the extn. Number and password to modify their features, including incoming/outgoing call blocking using steps 4-14. The Outgoing Call Blocking entries can also be entered from the user phone handset but using the feature code **\*79**.

## 12 References

---

Following documents for the corresponding software release:

- QX Manual I – Installation Guide
- QX Manual II - Administrators Guide
- QX Manual III – Extension User’s Guide
- Users Right Management on the QX

THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Epygi Technologies to be accurate as of the date of publication, is subject to change without notice. Epygi Technologies assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

Epygi is a registered trademark of Epygi Technologies, Ltd. All other products and services are the registered trademarks of their respective holders.