VoIP Media Gateways

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Mediant Gateway for Microsoft® Office 365 Exchange Online Unified Messaging with Legacy PBX

Microsoft Partner

Gold Communications

Microsoft® Office 365

AudioCodes

Version 6.8

June 2015

Document # LTRT-40513

Table of Contents

List of Figures

List of Tables

Notice

This Configuration Note shows how to configure an AudioCodes gateway to establish communication between telephony equipment on customer premises and Office 365 Exchange Online Unified Messaging (UM). It also shows how to configure Exchange Online UM to work with the AudioCodes gateway.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: June-10-2015

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What’s Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and One Box 365 are trademarks or registered trademarks of AudioCodes Limited All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Related Documentation

Manual Name
Mediant 500 E-SBC User's Manual Ver. 6.8
Mediant 800B Gateway and E-SBC SIP User's Manual Ver. 6.8
Mediant 1000B Gateway & E-SBC User's Manual Ver. 6.8
Mediant 2600 E-SBC User's Manual Ver. 6.8
Mediant 3000 SIP User's Manual Ver. 6.8
Mediant 4000 E-SBC User's Manual Ver. 6.8

Document Revision Record

LTRT	Description
40512	Initial document release for Version 7.0.
40513	Updated procedure for loading certificates to the device.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://www.audiocodes.com/downloads.

1 Introduction

Exchange Online Unified Messaging (Exchange Online UM) supports a wide range of telephony/voice solutions, including many PBXs and IP PBXs. A list is published in the “Telephony Advisor for Exchange 2013”[1].

When making or receiving telephone calls, Exchange Online UM only communicates with Voice-over-IP (VoIP) protocols. PBXs that support circuit-switched telephony protocols must be connected to Exchange Online UM with a suitable VoIP gateway. The gateway performs the necessary protocol conversion. VoIP gateways are also listed in the Exchange Telephony Advisor.

The Exchange Telephony Advisor also includes links to configuration notes that explain how to configure the PBX to work with Exchange Online UM.

Exchange Online UM is now offered as an online service, in specific Microsoft Office 365 service plans. The telephony/voice solution remains on the customer’s premises, but Exchange Online UM is now “in the cloud”, and the VoIP communication between them is carried by the public IP network.

In this guide, we describe the AudioCodes Mediant gateway configuration necessary to deploy it in an organization's network’s edge for interoperability with Exchange Online UM.

The purpose of the configuration is to ensure that traffic from the PBX, which is sent to the gateway TDM interface, is routed to the Exchange Online UM.

Similarly, traffic from Exchange Online UM, arriving at the gateway IP interface, must be routed to the PBX.

Configuration of the routing rules between the gateway interfaces is the main subject of this document.

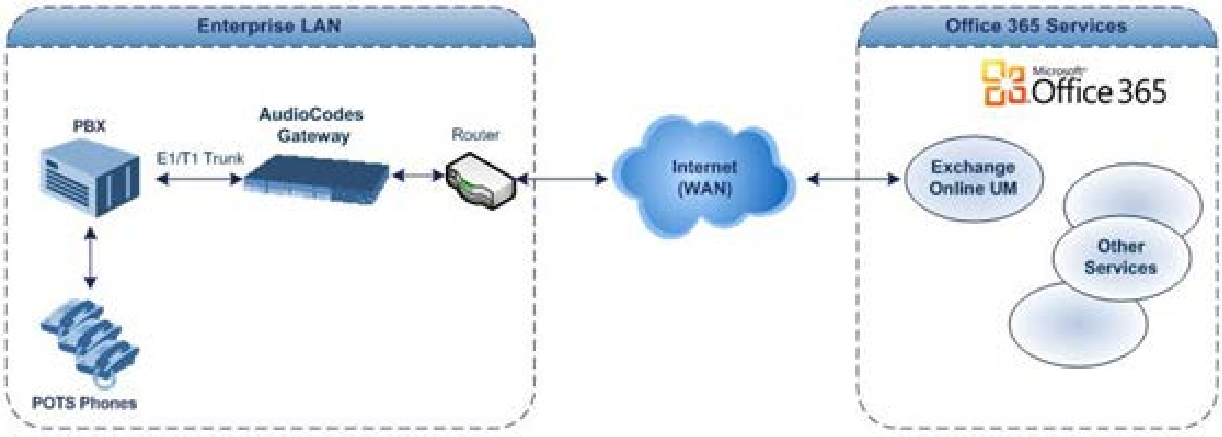
[1] http://technet.microsoft.com/en-us/library/ee364753.aspx

1.1 Focus of the Guide

This document focuses solely on the AudioCodes Mediant VoIP gateway features that are required for interoperability with Office 365 Exchange Online UM.

The AudioCodes Mediant gateway may support additional characteristics that are not described in this document. For a complete product description, refer to the AudioCodes gateway documentation.

Figure 1-1: AudioCodes Gateway Interfacing between Legacy PBX and Office 365



Note: The gateway communicates with the PBX by using either QSIG or Simplified Message Desk Interface (SMDI) via the serial RS-232 connection, or special in-band DTMF digit patterns. This document focuses on QSIG integration. Contact your AudioCodes sales representative for further information about other types of integration.

2 AudioCodes Interoperability with PBX Vendors

The table below lists the PBX vendors for which AudioCodes has successfully proven interoperability in Microsoft Unified Messaging Exchange 2007 environments.

Table 2-1: AudioCodes Interoperability with PBX Vendors

PBX Vendor	PBX Type	AudioCodes Product	Voice Mail Integration
Alcatel	4400	MP-11x FXO	DTMF
Alcatel-Lucent	OXE	Mediant 1000, Mediant 2000	E1 QSIG
Alcatel-Lucent	OXE	Mediant 1000	IP-to-IP
Asterisk	Business Edition	Mediant 1000, Mediant 2000	IP-to-IP
Avaya	Definity G3	Mediant 2000	T1 CAS (DTMF)
Avaya	Definity G3	MP-11x FXO	DTMF
Avaya	Definity G3	Mediant 1000, Mediant 2000	T1 QSIG
Avaya	Definity G3	Mediant 1000, Mediant 2000	E1 QSIG
Avaya	Merlin Magix	MP-11x FXO	DTMF
Avaya	S8300	MP-11x FXO	DTMF
Avaya	S8300	Mediant 2000	T1 CAS (DTMF)
Avaya	S8300	Mediant 1000, Mediant 2000	E1 QSIG
Avaya	S8700	Mediant 1000, Mediant 2000	E1 QSIG
Cisco	Call Manager 4.0	Mediant 1000, Mediant 2000	IP-to-IP
Ericsson	MD – 110	MP-11x FXO	SMDI
Intecom	PointSpan M6880	Mediant 2000	T1 CAS (SMDI)
Inter-Tel	Axxess	MP-11x FXO	DTMF
Inter-Tel	Axxess	Mediant 2000	T1 CAS (DTMF)
Inter-Tel	5000	Mediant 2000	T1 CAS (DTMF)
Inter-Tel	5000	MP-11x FXO	DTMF
Mitel	3300	Mediant 1000, Mediant 2000	T1 QSIG
NEC	Electra 192	MP-11x FXO	DTMF
NEC	NEAX 2400 IPX	Mediant 2000	T1 CAS (SMDI – MCI)
NEC	NEAX 2400 IPX	MP-11x FXO	SMDI – MCI
NEC	7600i	Mediant 2000	T1 CAS (SMDI)

PBX Vendor	PBX Type	AudioCodes Product	Voice Mail Integration
NeXspan	S	MP-11x FXO	DTMF
Nortel	CS1K (Communication Succession 1000)	Mediant 1000, Mediant 2000	E1 QSIG
Nortel	Meridian 11C, Meridian 51C, Meridian 61C, Meridian 81C	Mediant 1000, Mediant 2000	T1 QSIG
Nortel	Meridian 11C, Meridian 51C, Meridian 61C, Meridian 81C	Mediant 1000, Mediant 2000	E1 QSIG
Nortel	SL-100/DMS-100	Mediant 2000	T1 CAS (SMDI)
Nortel	SL-100/DMS-100	Mediant 1000 MP-11x	SMDI
Nortel	Meridian 1	Mediant 1000, Mediant 2000	T1 QSIG
Nortel	Meridian 1	Mediant 1000, Mediant 2000	E1 QSIG
Panasonic	KX-TDA30, KX-TDA100, KX-TDA200, KX-TDA600	MP-11x FXO	DTMF
Panasonic	KX-TDE2000, KX-TDE100, KX-TDE600	Mediant 1000 FXO	DTMF
Panasonic	KX-TES824, KX-TEA308	MP-11x FXO	DTMF
ShoreTel	IP Telephony System	MP-11x FXO	SMDI
ShoreTel	IP Telephony System	Mediant 1000 FXO	SMDI
Siemens	Hicom 150E	MP-11x FXO	DTMF
Siemens	HiPath 3550	MP-11x FXO	DTMF
Siemens	HiPath 4000	Mediant 1000, Mediant 2000	T1 QSIG
Siemens	HiPath 4000	MP-11x FXO	DTMF
Siemens	HiE9200	Mediant 1000, Mediant 2000	IP-to-IP
Tadiran	Coral Flexicom	MP-11x FXO	DTMF
Tadiran	Coral Flexicom	Mediant 2000	E1 CAS (DTMF)
Tadiran	Coral Flexicom	Mediant 1000, Mediant 2000	E1 QSIG
Tadiran	Coral Flexicom	Mediant 1000	BRI QSIG
Tadiran	Coral IPX	Mediant 1000	BRI QSIG
Tadiran	Coral IPX	Mediant 2000	E1 CAS (DTMF)

PBX Vendor	PBX Type	AudioCodes Product	Voice Mail Integration
Tadiran	Coral IPX	Mediant 1000, Mediant 2000	E1 QSIG
Tadiran	Coral IPX	MP-11x FXO	DTMF

This page is intentionally left blank.

3 Preparing for AudioCodes Gateway Configuration

Before configuring the gateway to route traffic to and from Office 365 Exchange Online UM, there are several steps that must be followed. Specifically, DNS configuration is required, followed by some Exchange Online UM configuration.

3.1 Configure DNS

The Exchange Online UM service in Office 365 must be able to locate the AudioCodes gateway when Exchange Online UM needs to initiate communication. Exchange Online UM relies on its own configuration and use of the Domain Name Service (DNS) to discover the address of the gateway.

Assign (have your network administrator assign) an IP address and host name for the gateway. For example, Contoso might decide to use *GW.contoso.com* as the name. Add this name and the corresponding address to the public DNS entries for your domain.

3.2 Generate Certificate

You must replace the gateway self-signed certificate. This can be done during the main process of gateway configuration. The new certificate must meet the following requirements:

- It must be signed by a recognized **Certificate Authority** (CA). Self-signed certificates (the kind that customers can generate and sign themselves) are **not** suitable for communication with Exchange Online UM.
- The **Subject Name** (CN) that is contained in the certificate must match the fully qualified domain name (FQDN) of the gateway as described in Section 3.1 above). For example, if the gateway will be addressed as *GW.contoso.com*, make sure that the Subject Name in the certificate contains exactly the same string (i.e., *GW.contoso.com*).
- The certificate should be suitable for use for Secure Sockets Layer (SSL).

You must generate and send a Certificate Signing Request to one of the supported Certificate Authorities (see below). The CA will sign and issue a certificate for the device. The details of submitting the request, making payment and receiving the certificate issued will depend on the CA chosen.

At the time of writing, the following Certificate Authorities are supported by Office 365 Exchange Online UM:

- DigiCert (http://www.digicert.com/)
- Entrust (http://www.entrust.com/)
- Geotrust (http://www.geotrust.com/)
- GoDaddy (http://www.godaddy.com/)
- GTE CyberTrust (http://www.verizonbusiness.com/Products/security/identity/ssl/)
- Network Solutions (http://www.networksolutions.com/)
- RSA Security (http://www.rsa.com/)
- Thawte (http://www.thawte.com/)
- Verisign (http://www.verisign.com/)

When the CA issues the certificate and returns it, save the certificate to a text file.

Further details of the process and how to load the certificate to the gateway are contained in Section 4.13 on page 36.

3.3 Configure UM

Before communication can be established from a telephony solution (via the gateway) to Office 365 Exchange Online UM, specific online Exchange Online UM configuration must be performed. This consists of, at least, creating and configuring a Dial Plan and an IP gateway. These are configuration objects that represent devices that are part of the telephony solution.

3.3.1 Create a UM Dial Plan

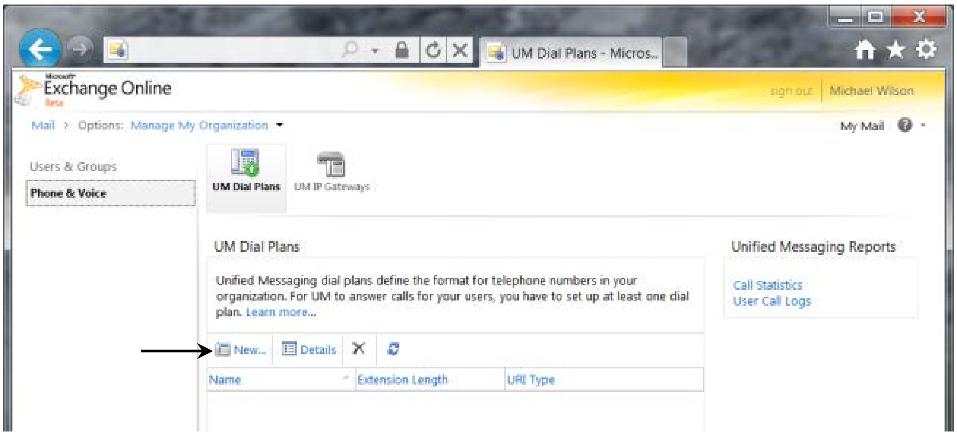
A UM Dial Plan represents a set of fixed-length telephone numbers and the PBX (or equivalent) to which they are attached. All Exchange users whose mailboxes are enabled for Exchange Online UM must be associated with a UM Dial Plan.

In the Exchange Control Panel (ECP), create a new UM Dial Plan (as shown below).

➢ **To create a new UM Dial Plan:**

1. Select the UM Dial Plans tab; the following screen appears.

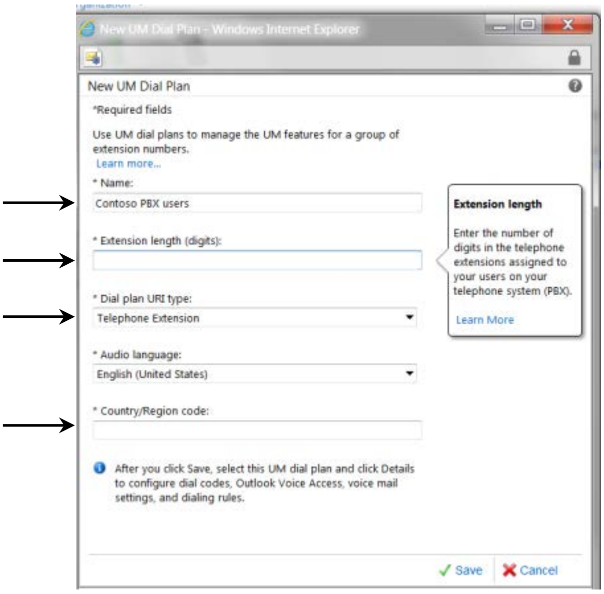
Figure 3-1: Initial (Empty) UM Dial Plans List in Exchange Control Panel



Unified Messaging dial plans define the format for telephone numbers in your organization. For UM to answer calls for your users, you have to set up at least one dial plan. Learn more...

2. Click on **New…** to create a new UM Dial Plan.

Figure 3-2: Specifying Properties for a New UM Dial Plan for a PBX



*Required fields

Use UM dial plans to manage the UM features for a group of extension numbers.
Learn more...

* Name: Contoso PBX users

* Extension length (digits):

* Dial plan URI type: Telephone Extension

* Audio language: English (United States)

* Country/Region code:

Extension length

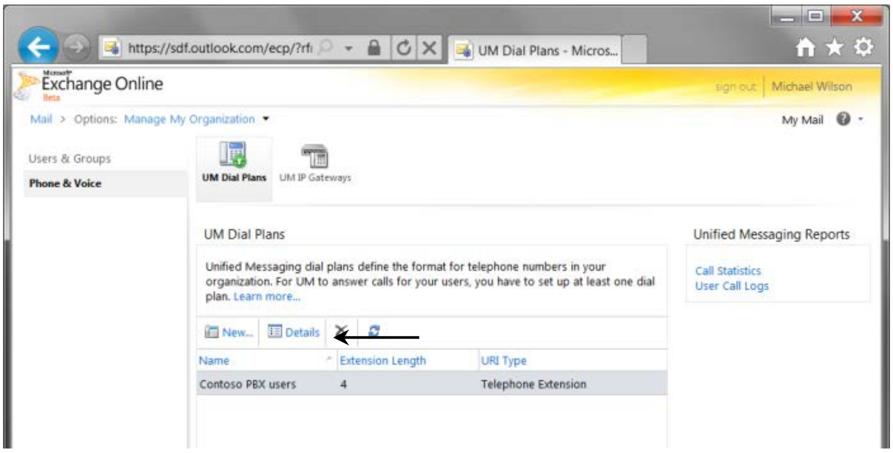
Enter the number of digits in the telephone extensions assigned to your users on your telephone system (PBX).

Learn More

After you click Save, select this UM dial plan and click Details to configure dial codes, Outlook Voice Access, voice mail settings, and dialing rules.

3. In the 'Name' field, enter the Name for the UM Dial Plan.
4. In the 'Extension length' field, enter the extension number length. The extension number (along with a PIN) is what UM-enabled users must enter to identify themselves to UM when they call it from a telephone, and try to log in to their mailbox. All extension numbers in a Dial Plan must have the same number of digits. This will be determined by the PBX's numbering plan.
5. From the 'Dial Plan URI Type' drop-down list select **Telephone Extension**. This indicates that the telephony solution in use is a PBX or IP PBX (and not Microsoft Lync).
6. In the 'Country/Region Code' field, enter the international dialing code for the country in which the telephony solution (PBX or IP PBX) is operating. For example, enter '1' for the United States, '44' for the United Kingdom, etc. The field accepts 1 to 4 numbers.
7. Click **Save** when you have entered all the information required to specify the new UM Dial Plan. The UM Dial Plan that you created is now listed, as shown in the example below.
8. Click the **Details** button to view and edit its properties, and those of associated objects such as **UM Mailbox Policies**.

Figure 3-3: List Showing One UM Dial Plan

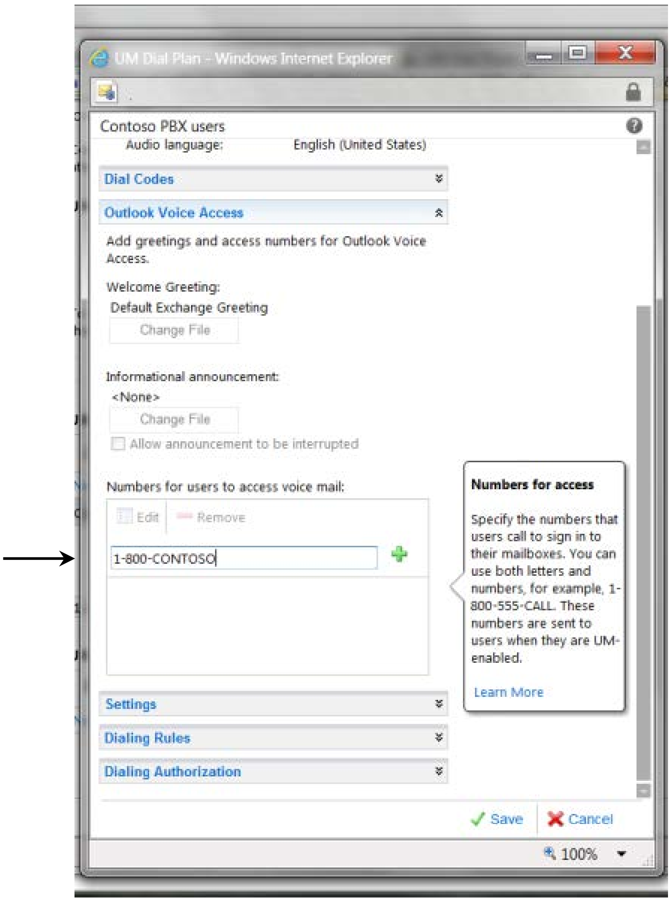

https://sdf.outlook.com/ecp/?rfi
UM Dial Plans - Micros...
Microsoft Exchange Online
Beta
sign out
Michael Wilson
Mail > Options: Manage My Organization
My Mail
Users & Groups
Phone & Voice
UM Dial Plans
UM IP Gateways
UM Dial Plans
Unified Messaging Reports
Call Statistics
User Call Logs
New...
Details

Unified Messaging dial plans define the format for telephone numbers in your organization. For UM to answer calls for your users, you have to set up at least one dial plan. Learn more...

Name	Extension Length	URI Type
Contoso PBX users	4	Telephone Extension

9. In the 'Number for Access' field, enter a number for user access on the new UM Dial Plan (see Figure 3-4 below). This can be in any readable format, because it is for display to users. For example, the user access number could be set to “(425) 266 8676” or “425-CONTOSO”. Two or more values can be supplied. The user access number(s) should be consistent with call routing number(s), or users will become confused. The user access number is included in the body of the “Welcome to Exchange Unified Messaging” e-mail that is sent to each user when they are UM-enabled. It is also displayed in the Outlook Voice Access section of the user’s Phone personal options (accessed via OWA/Exchange Control Panel).

Figure 3-4: Editing the Display Access Numbers for a UM Dial Plan



Contoso PBX users

Audio language: English (United States)

Add greetings and access numbers for Outlook Voice Access.

Welcome Greeting:
Default Exchange Greeting

Informational announcement:
<None>

□ Allow announcement to be interrupted

Numbers for users to access voice mail:

1-800-CONTOSO

Numbers for access

Specify the numbers that users call to sign in to their mailboxes. You can use both letters and numbers, for example, 1-800-555-CALL. These numbers are sent to users when they are UM-enabled.

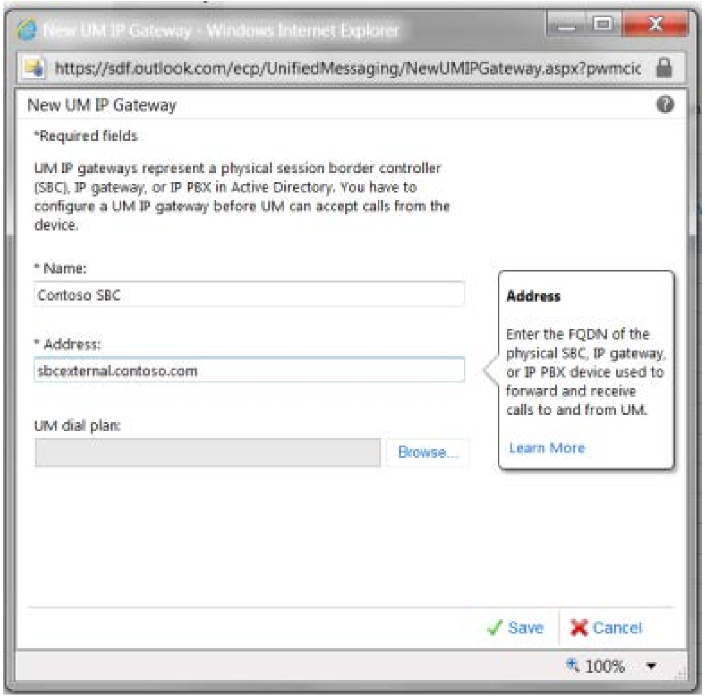
3.3.2 Create a UM IP Gateway

The procedure below describes how to create a UM IP gateway.

➢ **To create a UM IP gateway:**

1. In ECP, navigate to the 'UM IP Gateways' tab and create a new UM IP gateway (see Figure 3-5 below). For UM, this represents (the external interface of) your gateway.
2. Associate the UM IP gateway with the UM Dial Plan that you created by clicking the **Browse…** button and selecting the Dial Plan from the list that is displayed (see Figure 3-6 and Figure 3-7).

Figure 3-5: Creating New UM IP Gateway to Represent IP Gateway on Customer's Premises



New UM IP Gateway - Windows Internet Explorer

https://sdf.outlook.com/ecp/UnifiedMessaging/NewUMIPGateway.aspx?pwmcic

New UM IP Gateway

*Required fields

UM IP gateways represent a physical session border controller (SBC), IP gateway, or IP PBX in Active Directory. You have to configure a UM IP gateway before UM can accept calls from the device.

* Name: Contoso SBC

* Address: sbcexternal.contoso.com

UM dial plan:

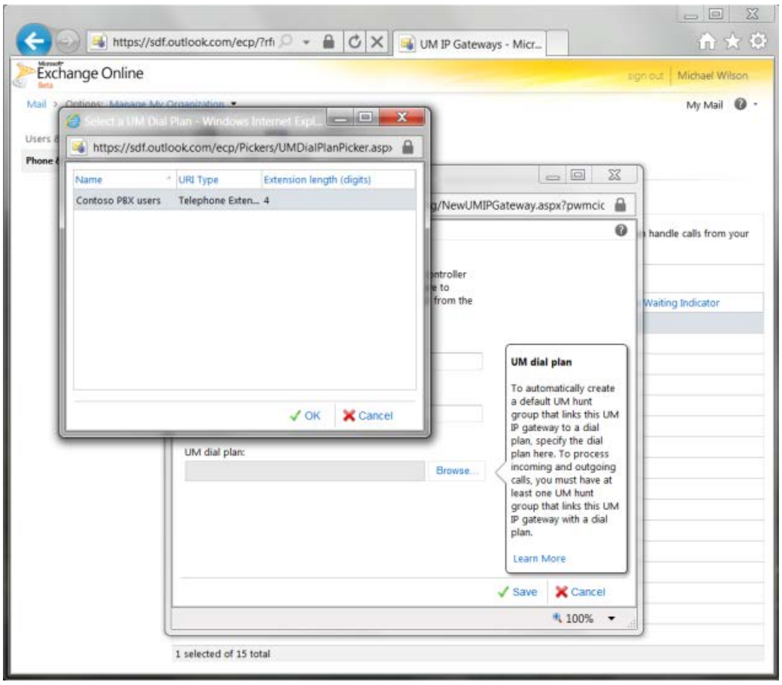
Address

Enter the FQDN of the physical SBC, IP gateway, or IP PBX device used to forward and receive calls to and from UM.

3. In the 'Name' field, enter the name of the UM IP gateway (for your reference only). It must be unique within your Office 365 organization. The object, for example, represents a gateway on Contoso’s premises. This example shows that the administrator chose a name to indicate this.
4. In the 'Address' field, enter the Address which must exactly match that of the public (external) interface of the gateway for your organization.

5. Click the **Browse…** button on the UM IP gateway details page. It displays a list of all the UM Dial Plans that have a type 'Telephone Extension'.

Figure 3-6: Associating the New UM IP Gateway with a UM Dial Plan



Select a UM Dial Plan - Windows Internet Expl...

https://sdf.outlook.com/ecp/Pickers/UMDialPlanPicker.aspx

Name	URI Type	Extension length (digits)
Contoso PBX users	Telephone Exten...	4

UM dial plan

To automatically create a default UM hunt group that links this UM IP gateway to a dial plan, specify the dial plan here. To process incoming and outgoing calls, you must have at least one UM hunt group that links this UM IP gateway with a dial plan.

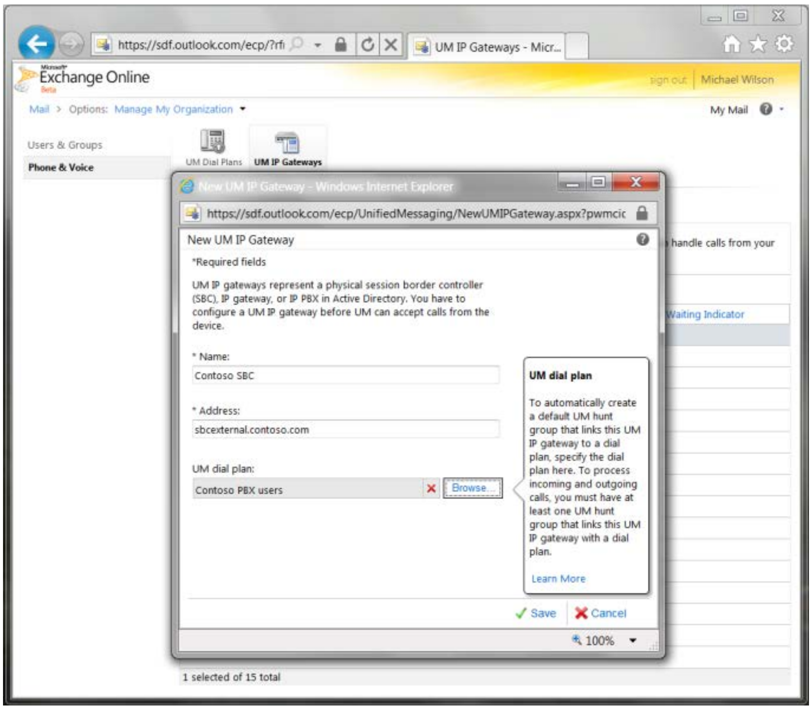
Learn More

UM dial plan:

1 selected of 15 total

6. Select one of these and click **OK**.

Figure 3-7: New UM IP Gateway Associated with a UM Dial Plan



New UM IP Gateway - Windows Internet Explorer

https://sdf.outlook.com/ecp/UnifiedMessaging/NewUMIPGateway.aspx?pwmcid

New UM IP Gateway

*Required fields

UM IP gateways represent a physical session border controller (SBC), IP gateway, or IP PBX in Active Directory. You have to configure a UM IP gateway before UM can accept calls from the device.

* Name: Contoso SBC

* Address: sbcexternal.contoso.com

UM dial plan: Contoso PBX users

UM dial plan

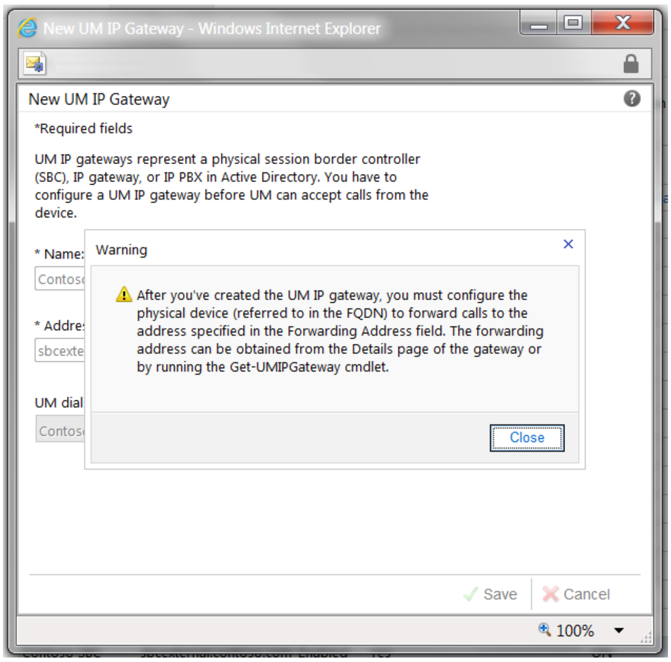
To automatically create a default UM hunt group that links this UM IP gateway to a dial plan, specify the dial plan here. To process incoming and outgoing calls, you must have at least one UM hunt group that links this UM IP gateway with a dial plan.

Learn More

1 selected of 15 total

7. When you create the UM IP gateway, it is automatically assigned a **Forwarding Address**. You're alerted to this when you save the gateway configuration (see Figure 3-8 below).

Figure 3-8: UM IP Gateway Forwarding Address Needed for Gateway Configuration Warning



New UM IP Gateway

*Required fields

UM IP gateways represent a physical session border controller (SBC), IP gateway, or IP PBX in Active Directory. You have to configure a UM IP gateway before UM can accept calls from the device.

* Name: Contoso

* Addre sbcexte

UM dial Contoso

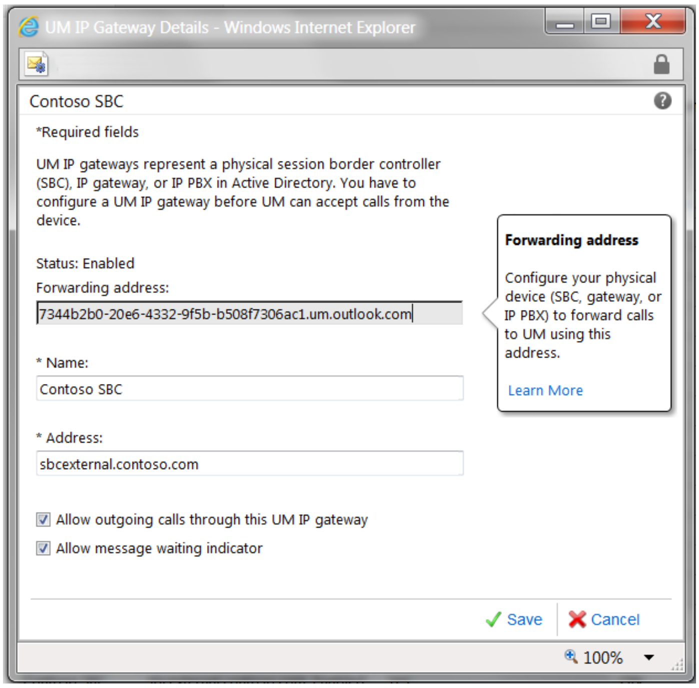
Warning

After you've created the UM IP gateway, you must configure the physical device (referred to in the FQDN) to forward calls to the address specified in the Forwarding Address field. The forwarding address can be obtained from the Details page of the gateway or by running the Get-UMIPGateway cmdlet.

Close

8. To see the **Forwarding Address**, view the details of the UM IP Gateway object (see Figure 3-9 below).

Figure 3-9: Viewing the Forwarding Address of a UM IP Gateway



Contoso SBC

*Required fields

UM IP gateways represent a physical session border controller (SBC), IP gateway, or IP PBX in Active Directory. You have to configure a UM IP gateway before UM can accept calls from the device.

Status: Enabled

Forwarding address: 7344b2b0-20e6-4332-9f5b-b508f7306ac1.um.outlook.com

* Name: Contoso SBC

* Address: sbcexternal.contoso.com

☑ Allow outgoing calls through this UM IP gateway

☑ Allow message waiting indicator

Forwarding address

Configure your physical device (SBC, gateway, or IP PBX) to forward calls to UM using this address.

Learn More

> **Note:** Forwarding addresses are in the form of *guid.um.outlook.com*, where *guid* is replaced by a 36-character string that uniquely identifies the organization (using UM) within the Office 365 system.

This page is intentionally left blank.

4 Configure AudioCodes Mediant Gateway

Using your Web browser, connect to the gateway's administration interface (the default address is **192.168.0.2**).

After providing the required credentials (the default user name is "Admin" and the default password is "Admin"), the Home page of the Web interface is displayed.

Use the **Full** navigation menu tree to perform gateway configuration.

4.1 Configure IP Network Interfaces

The procedure below describes how to assign an IP address to the VoIP / Management LAN interface.

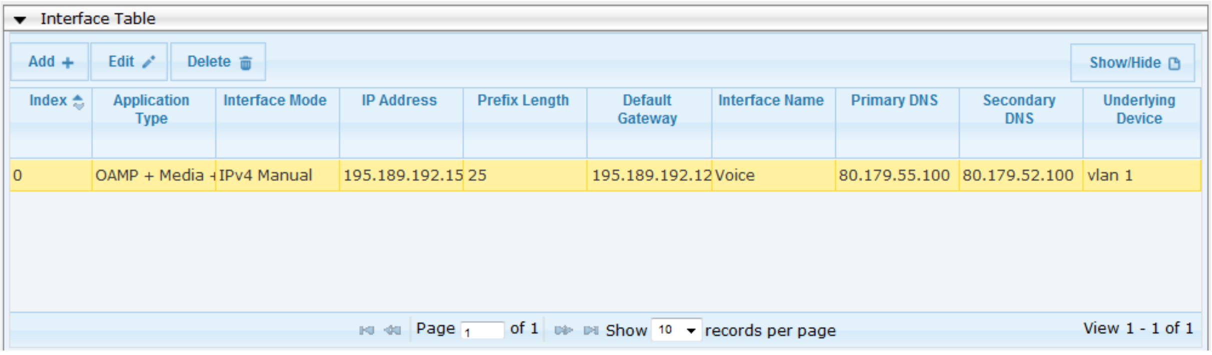
➢ **To configure the IP network interfaces:**

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Modify the existing LAN network interface:
   a. Select the **OAMP + Media + Control** table row, and click **Edit**.
   b. Configure the interface as follows:

Parameter	Value
Interface Mode	**IPv4 Manual**
IP Address	**195.189.192.155** (IP address of gateway)
Prefix Length	**25** (subnet mask in bits for 255.255.0.0)
Default Gateway	**195.189.192.129**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS	**80.179.55.100**
Secondary DNS	**80.179.52.100**
Underlying Device	**vlan 1**

3. Click **Submit**; the configured IP network interfaces are shown below:

Figure 4-1: Configured Network Interfaces in IP Interfaces Table



Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media +	IPv4 Manual	195.189.192.15	25	195.189.192.12	Voice	80.179.55.100	80.179.52.100	vlan 1

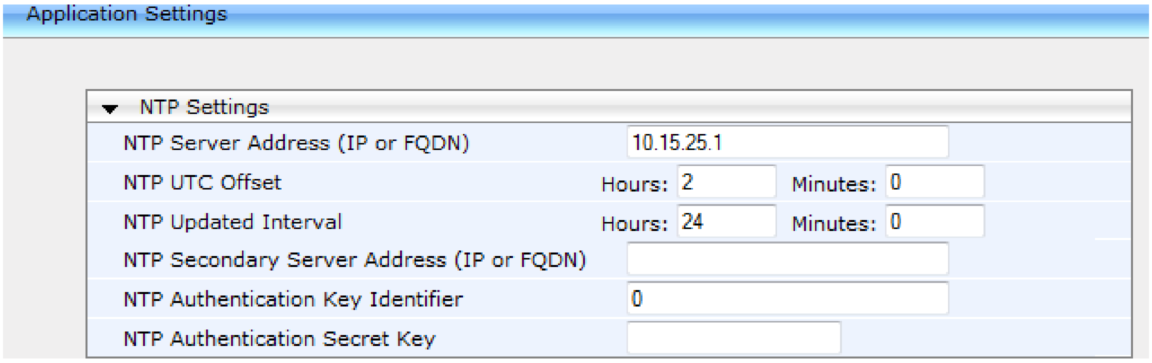
4.2 Configure Network Time Protocol Server IP Address

The procedure below describes how to configure the Network Time Protocol (NTP) server IP address. The gateway requires NTP for successful TLS negotiation with the Office 365 Exchange Online UM system[2].

➢ **To configure the NTP server IP address:**

1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).
2. Configure the NTP (e.g. server IP address), as required.

Figure 4-2: Application Settings Page



Application Settings

▼ NTP Settings

NTP Server Address (IP or FQDN)	10.15.25.1			
NTP UTC Offset	Hours:	2	Minutes:	0
NTP Updated Interval	Hours:	24	Minutes:	0
NTP Secondary Server Address (IP or FQDN)				
NTP Authentication Key Identifier	0			
NTP Authentication Secret Key				

3. Click **Submit**.

[2] In principle, all that is required is that the gateway and the Office 365 system have a sufficiently similar view of the current time. It's possible to set the date and time on the gateway itself, which provides a clock that maintains the time. However, without the use of NTP, it is likely that the gateway's time will eventually offset sufficiently, relative to the Office 365 system, for TLS negotiation to stop working. This may be difficult to diagnose and therefore it is recommended to use NTP to keep the gateway's time synchronized.

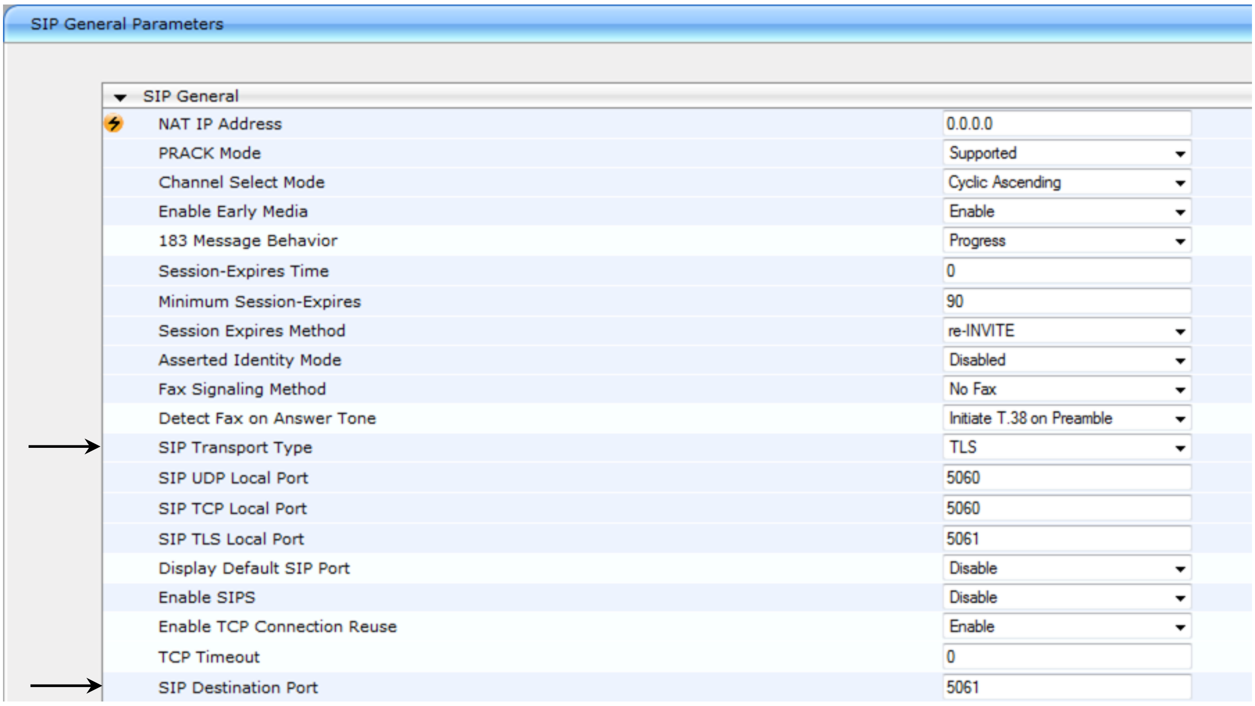
4.3 Configure SIP Transport Type

The procedure below describes how to set the SIP transport type to TLS.

➢ **To configure SIP Transport Type:**

1. Open the SIP General Parameters page (**Configuration** tab> **VoIP** menu > **SIP Definitions** > **General Parameters**).

Figure 4-3: SIP General Parameters



SIP General Parameters

▾ SIP General

NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Enable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	TLS
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Display Default SIP Port	Disable
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5061

2. From the 'SIP Transport Type' drop-down list, select **TLS**.
3. In the ‘SIP Destination Port’ , enter **5061**
4. Click **Submit**.

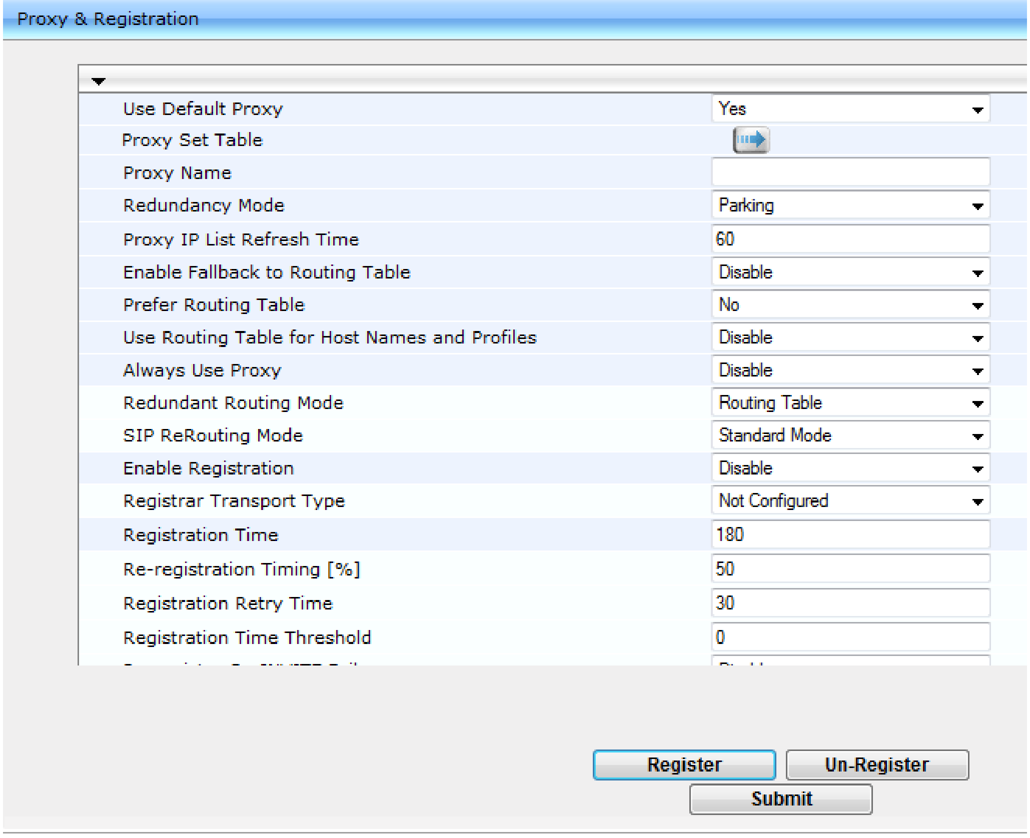
4.4 Configure Proxy and Registration

The procedure below describes how to configure the address (IP address or FQDN) of the Office 365 Exchange UM which communicates with the gateway. The PSTN gateway forwards all calls from the PSTN to the Exchange Online UM using this address.

➢ **To configure the Proxy and registration parameters:**

1. Open the **Proxy & Registration** page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).
2. Set **'Use Default Proxy'** to Yes.

Figure 4-4: Proxy and Registration Configuration



Proxy & Registration

Use Default Proxy	Yes
Proxy Set Table	
Proxy Name	
Redundancy Mode	Parking
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Redundant Routing Mode	Routing Table
SIP ReRouting Mode	Standard Mode
Enable Registration	Disable
Registrar Transport Type	Not Configured
Registration Time	180
Re-registration Timing [%]	50
Registration Retry Time	30
Registration Time Threshold	0

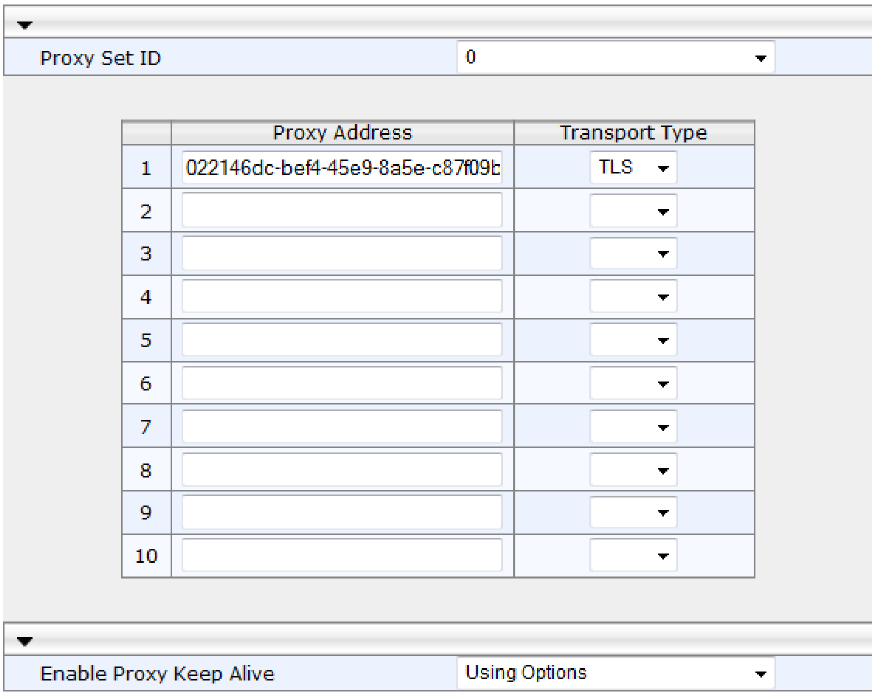
3. Click the arrow beneath the 'Use Default Proxy' parameter.
4. For the Proxy Address you must enter the Forwarding Address assigned to the UM IP gateway object created earlier (see Paragraph 8 on page 19). Only the end of a sample address is visible in the figure below. The length of the address is such that the view is clipped in the user interface, and only part of the address is visible.

   As secured communication is required, note that **:5061** must be appended to the address[3.]
5. From the 'Transport Type' drop-down list, select **TLS**.

[3] Port 5061 is used by Office 365 Exchange Online UM for all SIP/TLS traffic.

6. From the ‘Enable Proxy Keep Alive’ drop-down list, select **Using Options**.

Figure 4-5: Default Proxy Sets Table Configuration



Proxy Set ID: 0

	Proxy Address	Transport Type
1	022146dc-bef4-45e9-8a5e-c87f09b	TLS
2		
3		
4		
5		
6		
7		
8		
9		
10		

Enable Proxy Keep Alive: Using Options

7. Click **Submit**.

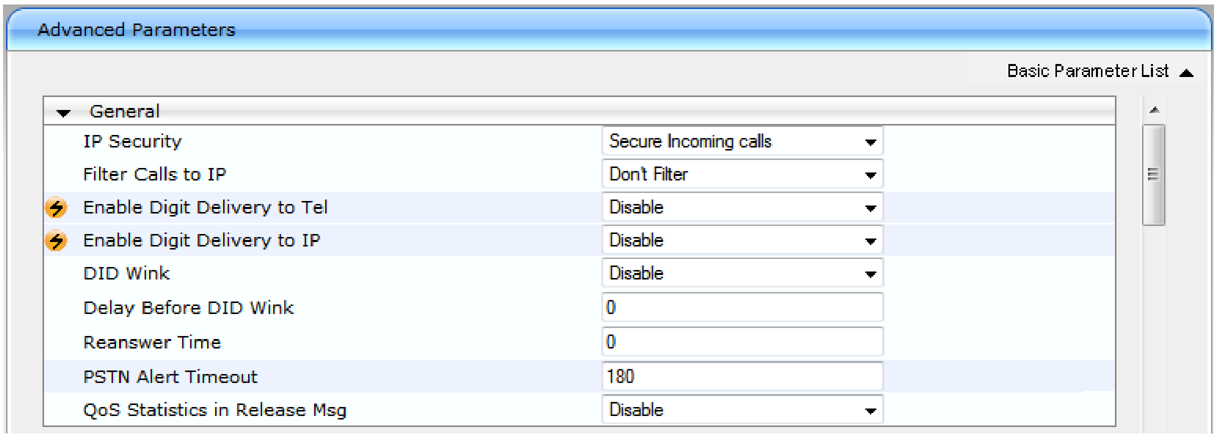
4.5 Restrict Communication to Exchange Online Only

The procedure below describes how to restrict IP communication, by allowing communication only between the PSTN gateway and the Exchange Online. This ensures that the PSTN gateway accepts and sends SIP calls **only** from and to the Exchange Online IP address. This is done by enabling the IP Security feature and then defining the allowed ("administrative" list) IP addresses (or FQDNs) in the Proxy Set table.

➢ **To allow IP communication only between the PSTN Gateway and Exchange Online:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).

Figure 4-6: Advanced Parameters Page



Advanced Parameters

Basic Parameter List ▲

General

IP Security	Secure Incoming calls
Filter Calls to IP	Don't Filter
Enable Digit Delivery to Tel	Disable
Enable Digit Delivery to IP	Disable
DID Wink	Disable
Delay Before DID Wink	0
Reanswer Time	0
PSTN Alert Timeout	180
QoS Statistics in Release Msg	Disable

2. From the 'IP Security' drop-down list, select **Secure Incoming calls** to enable the security feature to accept and send SIP calls only from and to user-defined IP addresses or FQDN configured in the 'Proxy Set table'.

3. Click **Submit** to apply your settings.

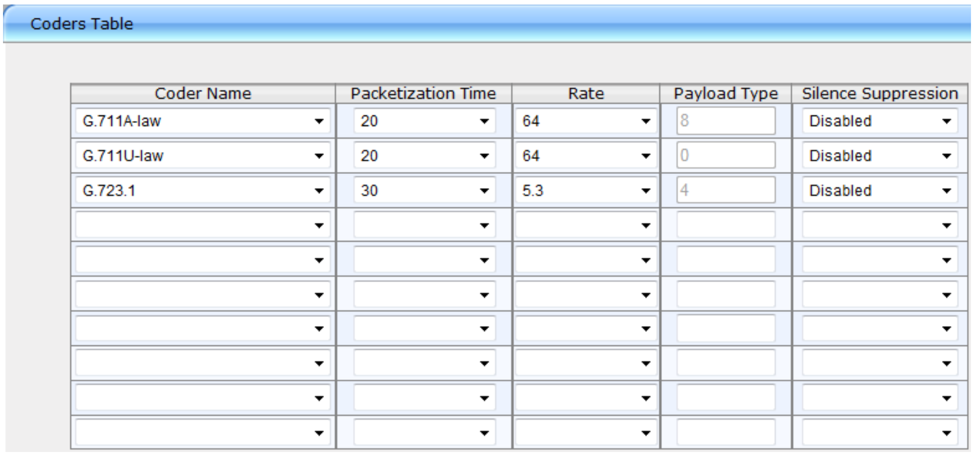
4.6 Configure Codecs

The procedure below describes how to configure codecs.

➢ **To configure codecs:**

1. Open the Coders page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders**).
2. From the 'Coder Name' drop-down list, select audio codecs supported by Office 365 Exchange Online UM.

Figure 7: Codec Configuration



Coders Table

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law	20	64	8	Disabled
G.711U-law	20	64	0	Disabled
G.723.1	30	5.3	4	Disabled

3. Click **Submit**.

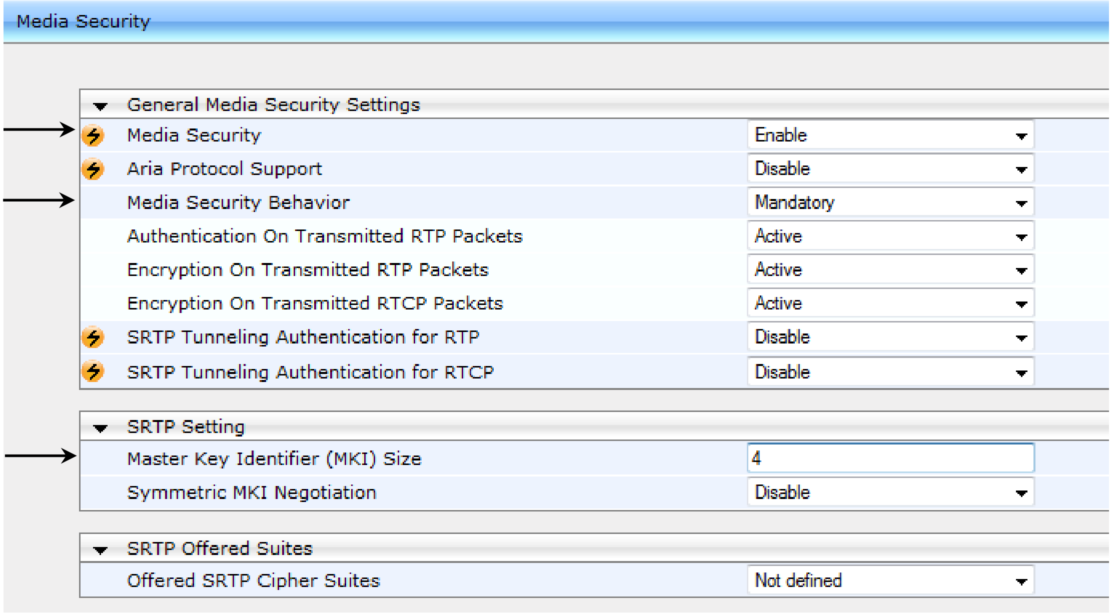
4.7 Configure Media Security

The procure below describes how to configure Media Security. This configuration forces the gateway to reject calls when the SIP peer does not use SRTP. Exchange Online UM requires that all (audio) media be secured with the SRTP protocol.

➢ **To configure media security:**

1. Open the Media Security page (**Configuration** tab > **VoIP** menu > **Media** > **Media Security**).
2. Set the 'Media Security' field to **Enable**.
3. Set the 'Media Security Behavior' field to **Mandatory**.
4. Set the 'Master Key Identifier (MKI) Size' field to "4".

Figure 4-8: Media Security Configuration



Media Security

General Media Security Settings

Media Security	Enable
Aria Protocol Support	Disable
Media Security Behavior	Mandatory
Authentication On Transmitted RTP Packets	Active
Encryption On Transmitted RTP Packets	Active
Encryption On Transmitted RTCP Packets	Active
SRTP Tunneling Authentication for RTP	Disable
SRTP Tunneling Authentication for RTCP	Disable

SRTP Setting

Master Key Identifier (MKI) Size	4
Symmetric MKI Negotiation	Disable

SRTP Offered Suites

Offered SRTP Cipher Suites	Not defined

5. Click **Submit**.

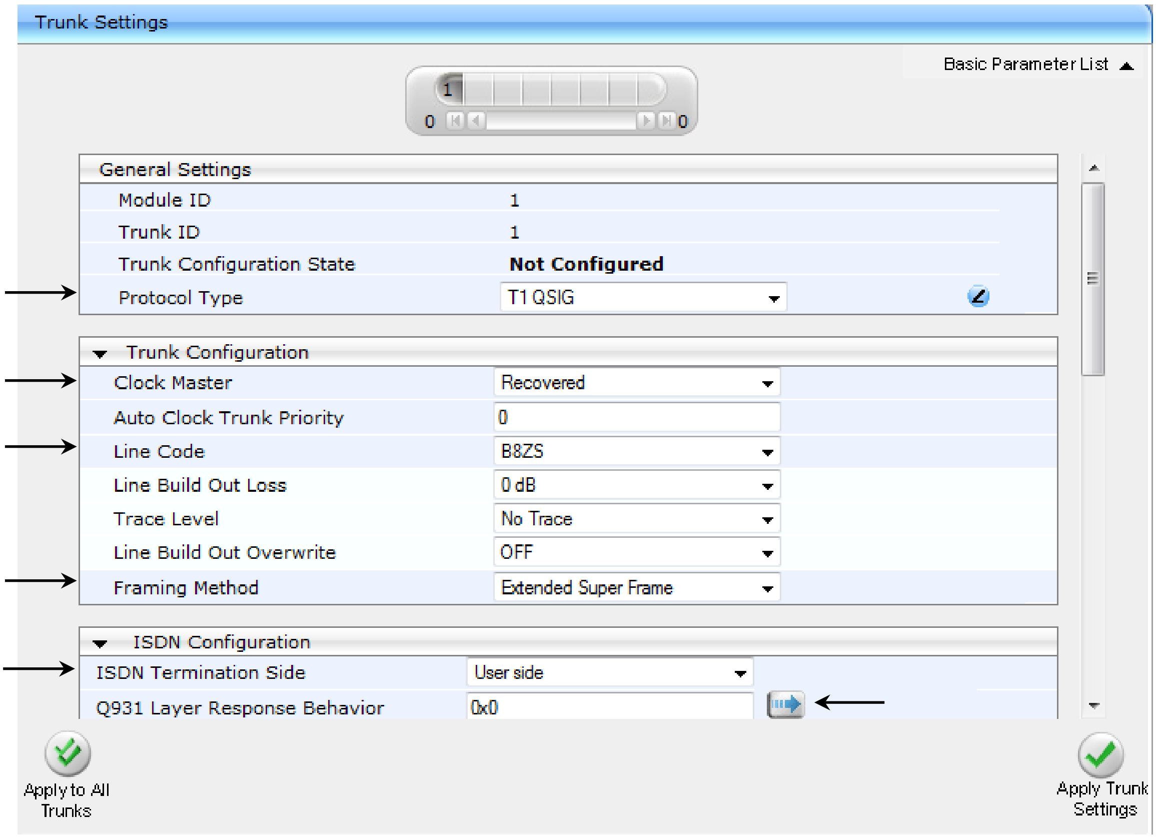
4.8 Configure PSTN Trunk Settings

The procedure below describes how to configure PSTN Trunk settings.

➢ **To configure the PSTN Trunk Settings:**

1. Open the Trunk Settings page (**Configuration** tab **> VoIP** menu **> PSTN > Trunk Settings**).
2. Configure the following fields according to your PSTN physical Trunk deployment:
   - Protocol Type
   - Clock Master
   - Line Code
   - Framing Method
   - ISDN Termination Side

Figure 9: Trunk Configuration



General Settings

Module ID	1
Trunk ID	1
Trunk Configuration State	**Not Configured**
Protocol Type	T1 QSIG

Trunk Configuration

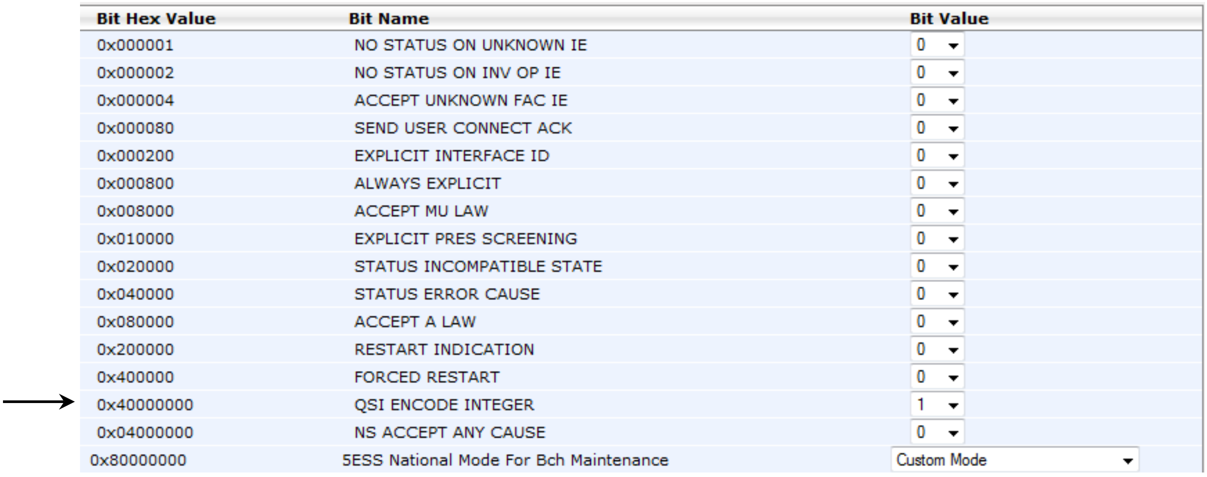
Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	B8ZS
Line Build Out Loss	0 dB
Trace Level	No Trace
Line Build Out Overwrite	OFF
Framing Method	Extended Super Frame

ISDN Configuration

ISDN Termination Side	User side
Q931 Layer Response Behavior	0x0

3. Click the arrow next to the 'Q931 Layer Response Behavior' field and configure the ‘QSI ENCODE INTEGER’ bit to **1**.

Figure 10: Q931 Layer Response Behavior Configuration



Bit Hex Value	Bit Name	Bit Value
0x000001	NO STATUS ON UNKNOWN IE	0
0x000002	NO STATUS ON INV OP IE	0
0x000004	ACCEPT UNKNOWN FAC IE	0
0x000080	SEND USER CONNECT ACK	0
0x000200	EXPLICIT INTERFACE ID	0
0x000800	ALWAYS EXPLICIT	0
0x008000	ACCEPT MU LAW	0
0x010000	EXPLICIT PRES SCREENING	0
0x020000	STATUS INCOMPATIBLE STATE	0
0x040000	STATUS ERROR CAUSE	0
0x080000	ACCEPT A LAW	0
0x200000	RESTART INDICATION	0
0x400000	FORCED RESTART	0
0x40000000	QSI ENCODE INTEGER	1
0x04000000	NS ACCEPT ANY CAUSE	0
0x80000000	5ESS National Mode For Bch Maintenance	Custom Mode

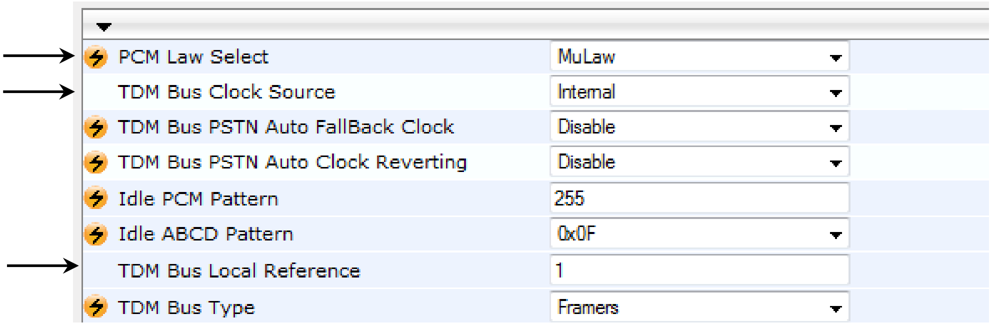
4.8.1 Configure TDM Bus

The procedure below describes how to configure the TDM bus of the PSTN gateway.

➢ **To configure the TDM bus:**

1. Open the TDM Bus Settings page (**Configuration** tab > **VoIP** menu > **TDM** > **TDM Bus Settings**).

Figure 4-11: TDM Bus Settings Page



⚡ PCM Law Select	MuLaw
TDM Bus Clock Source	Internal
⚡ TDM Bus PSTN Auto FallBack Clock	Disable
⚡ TDM Bus PSTN Auto Clock Reverting	Disable
⚡ Idle PCM Pattern	255
⚡ Idle ABCD Pattern	0x0F
TDM Bus Local Reference	1
⚡ TDM Bus Type	Framers

2. Configure the TDM bus parameters according to your deployment requirements. Below is a description of some of the main TDM parameters:
   - **PCM Law Select:** Defines the type of PCM companding law in the input/output TDM bus. Typically, A-Law is used for E1 and Mu-Law for T1/J1.
   - **TDM Bus Clock Source:** Defines the clock source to which the PSTN gateway synchronizes - generates clock from local source (Internal) or recovers clock from PSTN line (Network).
   - **TDM Bus Local Reference:** Defines the physical trunk ID from which the PSTN gateway recovers (receives) its clock synchronization when the TDM Bus Clock Source is configured to recover the clock from the PSTN line.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

Note: Changes to fields marked ⚡ill only take effect after a reset.

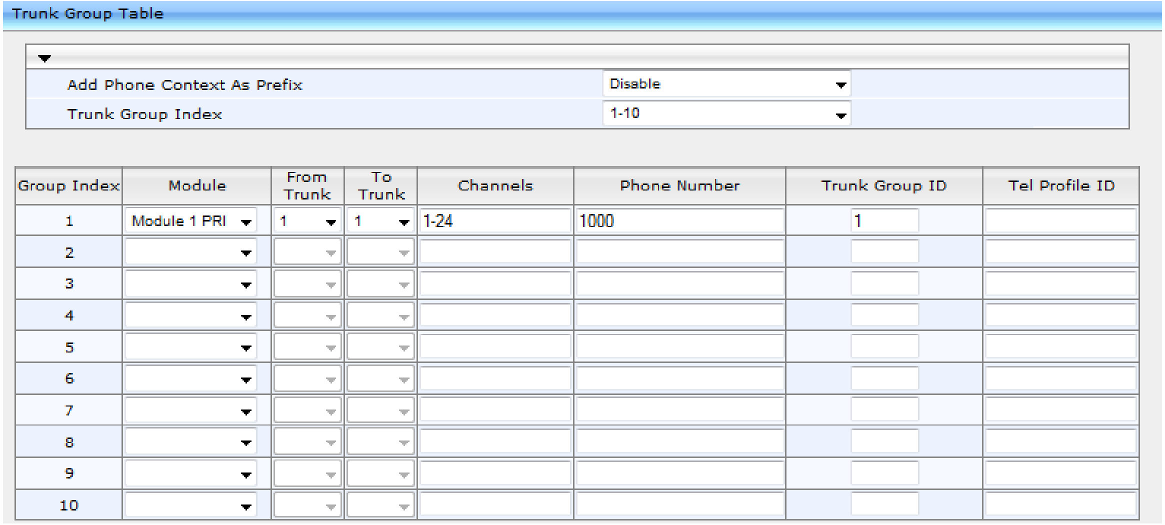
4.9 Configure Trunk Group

The procedure below describes how to configure and enable the PSTN network connected to the gateway's PRI TRUNK module.

➢ **To configure the Trunk Group:**

1. Open the Trunk Group Table page (**Configuration** tab> **VoIP** menu> **GW and IP to IP** > **Trunk Group** > **Trunk Group**).
2. From the 'Module' drop-down list, select **Module 1 PRI**.
3. In the 'From Trunk' and 'To Trunk' fields, select **1** (i.e., Trunk 1).
4. In the 'Channels' field, enter "1-24" for the number of channels in the T1 Trunk.
5. In the 'Phone Number' field, enter any phone number for the channels. This is only a logical phone number (i.e., not used).
6. In the 'Trunk Group ID' field, enter "1" as the Trunk Group ID.

Figure 4-12: Trunk Group Configuration



Trunk Group Table

Add Phone Context As Prefix	Disable
Trunk Group Index	1-10

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-24	1000	1	
2							
3							
4							
5							
6							
7							
8							
9							
10							

7. Click **Submit**.

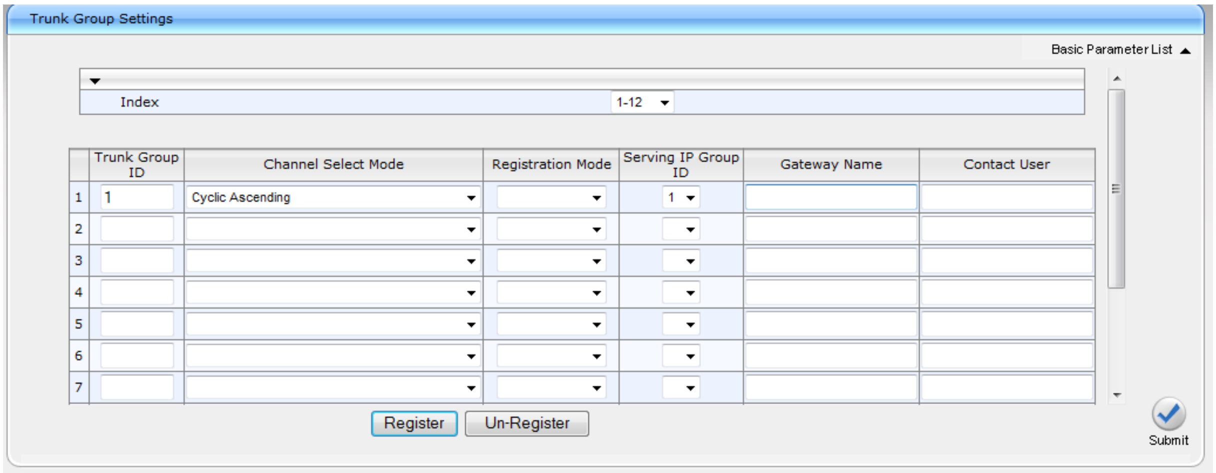
4.10 Configure Trunk Group Settings

The procedure below describes how to configure Trunk Group settings.

➢ **To configure Trunk Group settings:**

1. Open the Trunk Group Settings page (**Configuration** tab> **VoIP** menu > **GW and IP to IP** > **Trunk Group** > **Trunk Group Settings**).
2. In the 'Trunk Group ID' field, enter "1".
3. From the 'Channel Select Mode' drop-down list, select **Cyclic Ascending**.
4. From the 'Serving IP Group ID' drop-down list, select **1**.

Figure 4-13: Trunk Group Configuration Trunk Group Settings



Trunk Group Settings

Basic Parameter List

Index 1-12

	Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	Cyclic Ascending		1		
2						
3						
4						
5						
6						
7						

5. Click **Submit**.

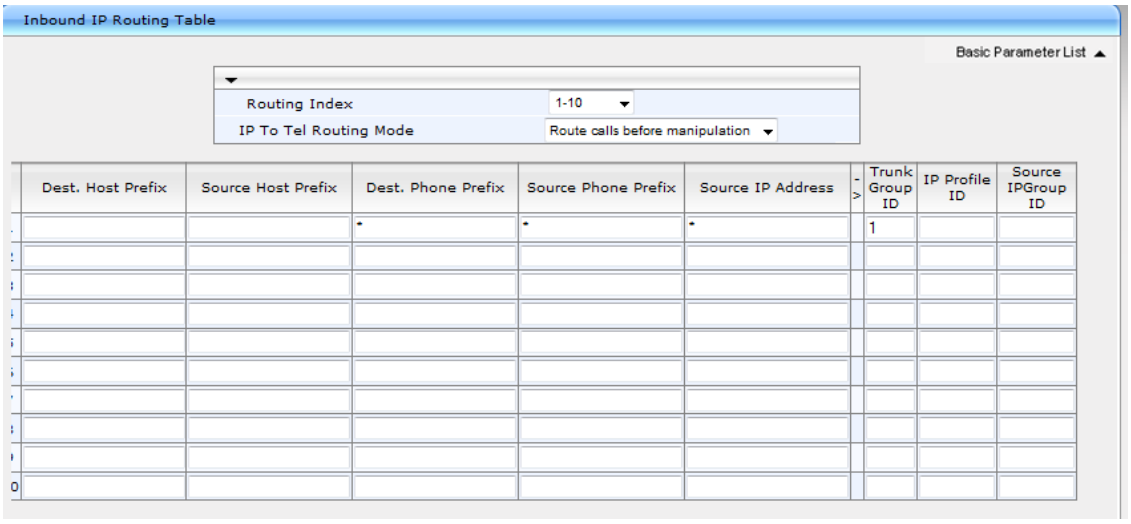
4.11 Configure VoIP Gateway IP-to-Tel Routing Rules

The procedure below describes how to configure VoIP gateway IP-to-Tel Routing Rules.

➢ **To configure IP-to-Tel routing rules:**

1. Open the Inbound IP Routing Table page (**Configuration** tab> **VoIP** menu > **GW and IP to IP** > **Routing** > **IP to Trunk Group Routing**).
2. In the 'Dest Phone Prefix' field, enter an asterisk.
3. In the 'Source Phone Prefix' and Source IP Address' fields, enter an asterisk symbol (*) to indicate any.
4. In the 'Trunk Group ID' field, enter "1".

Figure 4-14: IP-to-Tel Routing Rules Configuration



Inbound IP Routing Table

Basic Parameter List ▲

Routing Index: 1-10 ▾

IP To Tel Routing Mode: Route calls before manipulation ▾

Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	- >	Trunk Group ID	IP Profile ID	Source IPGroup ID
		*	*	*		1		

5. Click **Submit**.

4.12 Configure VoIP Gateway Tel-to-IP Routing Rules

The procedure below describes how to configure the VoIP gateway Tel-to-IP Routing Rules.

As mentioned in Section 4.5 on page 26, the gateway receives INVITEs from the Exchange server only. When a REFER message is received from the Exchange, the gateway sends a new INVITE message to itself.

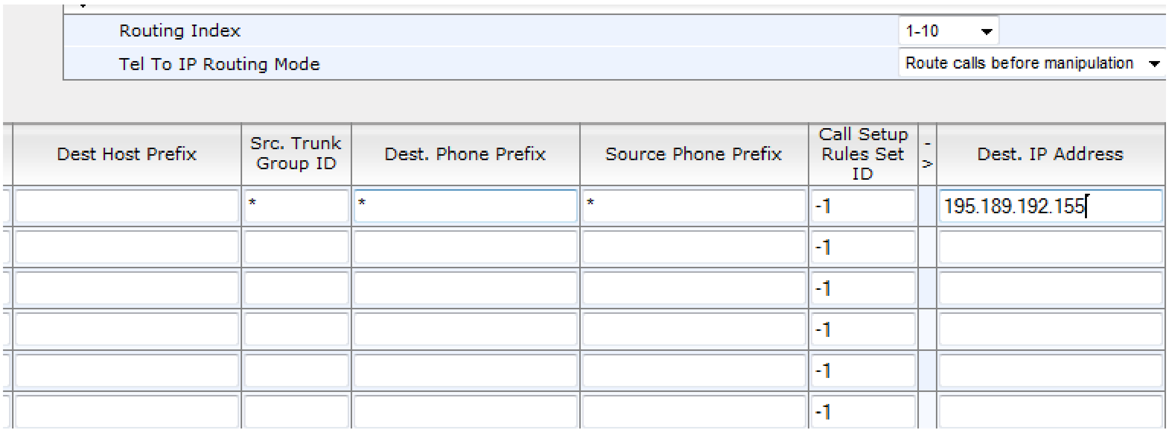
To allow the gateway to receive an INVITE from its own IP address, configure Tel to IP routing to use the gateway IP address in this table.

The routing table allows the gateway to route the call back to the PBX to reach the destination transferee.

➢ To configure Tel-to-IP routing rules:

1. Open the Outbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Tel to IP Routing**).
2. In the ‘Src. Trunk Group ID' field, enter an asterisk symbol (*) to indicate any.
3. In the 'Dest Phone Prefix' field, enter an asterisk symbol (*) to indicate any.
4. In the 'Source Phone Prefix' field, enter an asterisk symbol (*) to indicate any.
5. In the ‘Dest. IP Address’ field, enter the IP address of the gateway, i.e., "195.189.192.155”.

Figure 4-15: Tel-to-IP Routing Rules Configuration



Routing Index: 1-10

Tel To IP Routing Mode: Route calls before manipulation

Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Call Setup Rules Set ID	->	Dest. IP Address
	*	*	*	-1		195.189.192.155
				-1		
				-1		
				-1		
				-1		
				-1		

6. Click **Submit**.

4.13 Configure Certificates

As noted earlier in Section 3 on page 13, communication between the gateway and Office 365 Exchange Online UM requires the use of a digital certificate signed by a Certificate Authority (CA). The gateway is supplied with a self-signed certificate, which cannot be used because it is not signed by a supported CA.

Before certificate configuration takes place, ensure that the DNS (see Section 3.2 on page 13) and NTP (see Section 4.2 on page 22) settings have been configured correctly. If this is the case, proceed as follows.

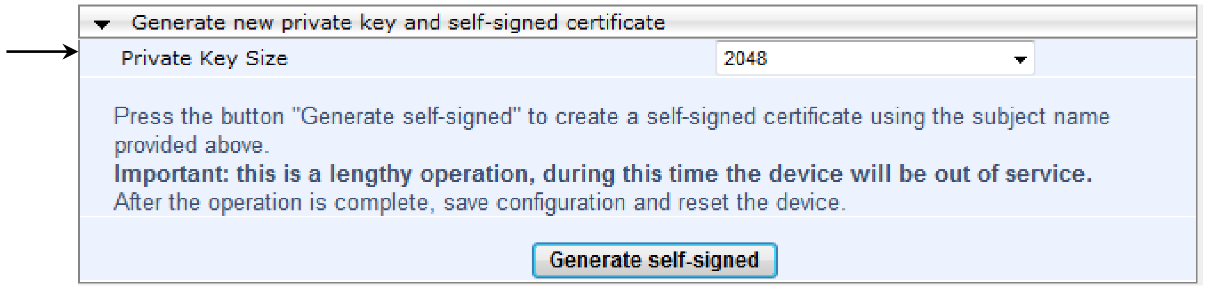
4.13.1 Configure Cryptographic Parameters

The procedure below describes how to configure cryptographic parameters.

➢ **To configure cryptographic parameters:**

1. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
2. Under the **Generate new private key and self-signed certificate** group, from the 'Private Key Size' drop-down list, select **2048** and then click **Generate self-signed**.

Figure 4-16: Cryptographic Configuration



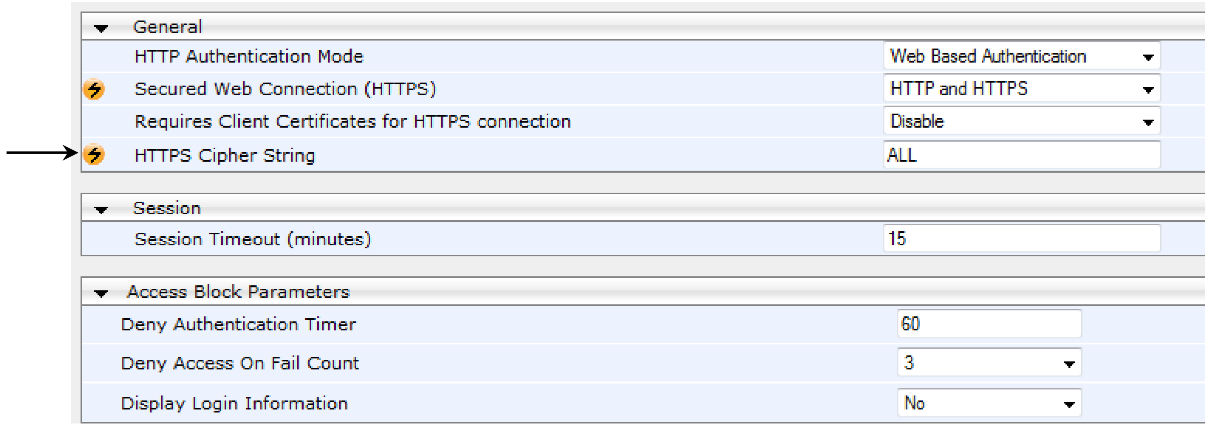
Generate new private key and self-signed certificate

Private Key Size	2048

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.
Important: this is a lengthy operation, during this time the device will be out of service.
After the operation is complete, save configuration and reset the device.

3. Open the Web Security Settings page (**Configuration** tab > **System** menu > **Management** > **Web Security Settings**).
4. Under the **General** group, in the 'HTTPS Cipher String' field, enter "ALL".

Figure 4-17: Web Security Settings



General

HTTP Authentication Mode	Web Based Authentication
Secured Web Connection (HTTPS)	HTTP and HTTPS
Requires Client Certificates for HTTPS connection	Disable
HTTPS Cipher String	ALL

Session

Session Timeout (minutes)	15

Access Block Parameters

Deny Authentication Timer	60
Deny Access On Fail Count	3
Display Login Information	No

5. Click **Submit**.
6. On the toolbar, click **Burn** to save the settings, and reset the device.

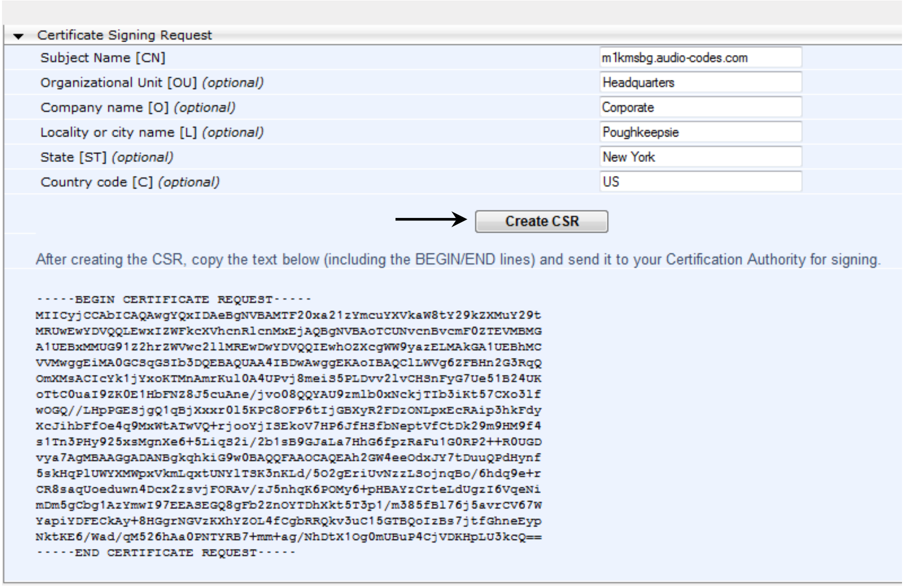
4.13.2 Generate Certificate Signing Request (CSR)

The procedure below describes how to generate certificate signing requests.

➢ **To generate certificate signing requests:**

1. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
2. In the 'Subject Name' field, enter the DNS name assigned to your device (see Section 3.1 on page 13).
3. Enter all other certificate details.
4. Click **Create CSR**. After a few seconds, a text rendering of the certificate signing request is displayed:

Figure 4-18: Generating Certificate Signing Requests



Subject Name [CN]	m1kmsbg.audio-codes.com
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyjCCAbICAQAwgYQxIDAeBgNVBAMTF20xa21zYmcuYXVkaW8tY29kZXMuY29t
MRUwEwYDVQQLEwxIZWFkcXVhcnRlcnMxEjAQBgNVBAoTCUNvcnBvcmF0ZTEVMBMG
A1UEBxMMUG91Z2hrZWVwc2llMREwDwYDVQQIEwhOZXcgWW9yazELMAkGA1UEBhMC
VVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQClLWVg6ZFBHn2G3RqQ
OmXMsACIcYk1jYxoKTMnAmrKul0A4UPvj8meiS5PLDvv2lvCHSnFyG7Ue51B24UK
oTtC0uaI9ZK0E1HbFNZ8J5cuAne/jvo08QQYAU9zmlb0xNckjTIb3iKt57CXo3lf
wOGQ//LHpPGESjgQ1qBjXxxr0l5KPC8OFP6tIjGBXyR2FDzONLpxEcRAip3hkFdy
XcJihbFfOe4q9MxWtATwVQ+rjooYjISEkoV7HP6JfHSfbNeptVfCtDk29m9HM9f4
s1Tn3PHy925xsMgnXe6+5LiqS2i/2b1sB9GJaLa7HhG6fpzRaFu1G0RP2++R0UGD
vya7AgMBAAGgADANBgkqhkiG9w0BAQQFAAOCAQEAh2GW4eeOdxJY7tDuuQPdHynf
5skHqPlUWYXMWpxVkmLqxtUNYlTSK3nKLd/5O2gEriUvNzzLSojnqBo/6hdq9e+r
CR8saqUoeduwn4Dcx2zsvjFORAv/zJ5nhqK6POMy6+pHBAYzCrteLdUgzI6VqeNi
mDm5gCbg1AzYmwI97EEASEGQ8gFb2ZnOYTDhXkt5T3p1/m385fBl76j5avrCV67W
YapiYDFECkAy+8HGgrNGVzKXhYZOL4fCgbRRQkv3uC15GTBQoIzBs7jtfGhneEyp
NktKE6/Wad/qM526hAa0PNTYRB7+mm+ag/NhDtX1Og0mUBuP4CjVDKHpLU3kcQ==
-----END CERTIFICATE REQUEST-----
```

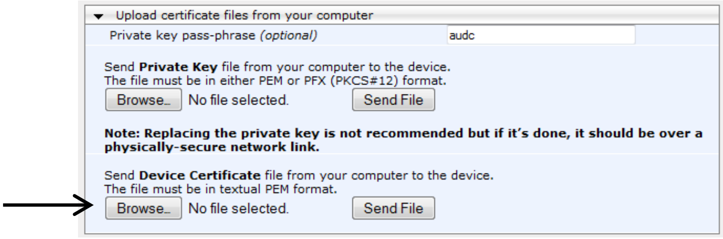
5. Copy **all** the text of the certificate request (including the BEGIN and END sections and dashes) and provide it to the Certificate Authority (CA) as part of their certificate generation process (see Section 3 on page 13).

4.13.3 Loading the Certificate

The procedure below describes how to load the certificate files. You will receive the certificate files from the CA as text files (or in a form that can be saved as a text file).

➢ **To load the certificates:**

1. Open the TLS Contexts table (**Configuration** tab > **System** menu > **TLS Contexts**).
2. Select the default TLS Context (index 0), and then click the **TLS Context Certificate** button, located below the table.
3. In the **Upload certificate files from your computer** group, locate the text “Send Device Certificate file from your computer to the device". Click the **Browse** button below this text, navigate to the certificate file, and then click **Send File**.



Upload certificate files from your computer

Private key pass-phrase *(optional)*: audc

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

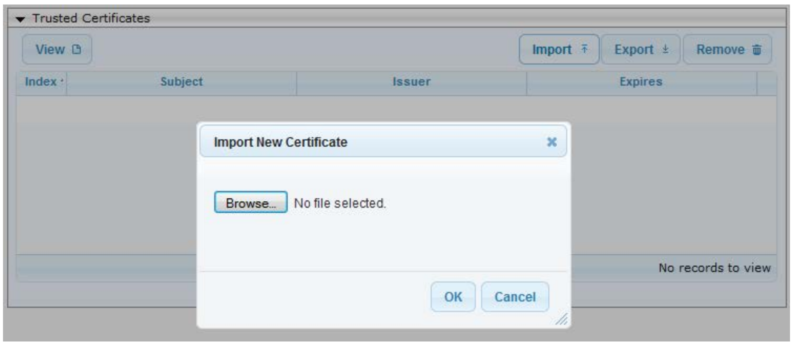
No file selected.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

No file selected.

4. Download the trusted-root CA certificate and intermediate CA certificate from the CA Web site (varies from one enterprise CA to another).
5. Return to the TLS Contexts table.
6. Select the default TLS Context (index 0), and then click the **TLS Context Trusted Root Certificates** button, located below the table.
7. For each trusted-root certificate, do the following:
   a. Click the **Import** button, and then click the **Browse** button to navigate and select the certificate file to load.



Trusted Certificates

Index	Subject	Issuer	Expires

No records to view

Import New Certificate

No file selected.

   b. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
8. Reset the device with a flash-to-burn to apply your settings.

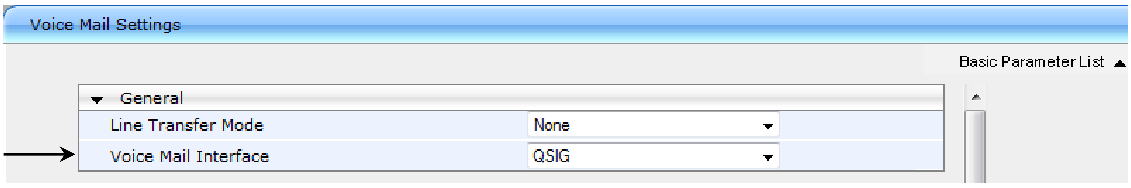
4.14 Configure Voice Mail Interface

The procedure below describes how to configure the voice mail interface. This enables the device's Voice Mail application and determines the communication method between the PBX and the device.

➢ **To configure the voice mail interface:**

1. Open the Voice Mail Settings page (**Configuration** tab > **VoIP** menu > **Services** > **Voice Mail Settings**).

Figure 4-19: Voice Mail Interface Configuration



Voice Mail Settings

Basic Parameter List

General

Line Transfer Mode: None

Voice Mail Interface: QSIG

2. From the 'Voice Mail Interface' drop-down list, select your voice mail interface to the PBX (i.e. **QSIG**).
3. Click **Submit**.

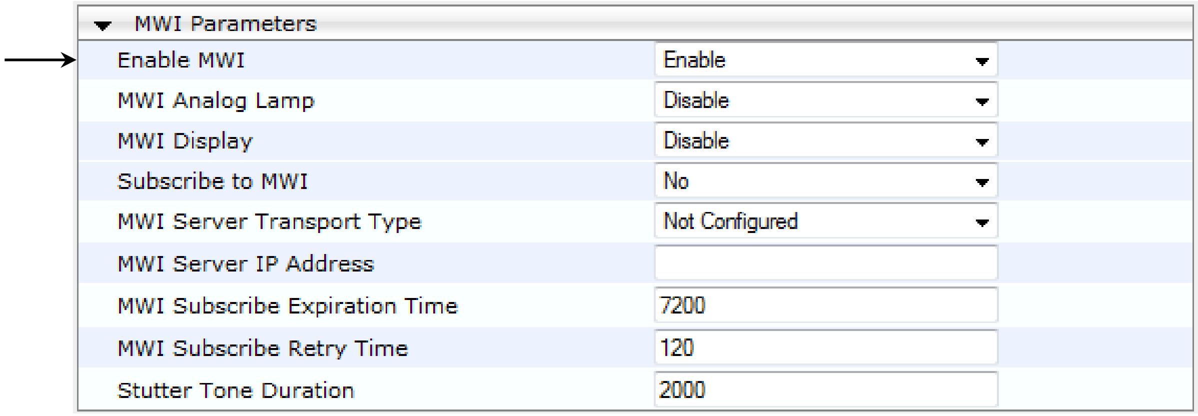
4.15 Configure Message Waiting Indicator

The procedure below describes how to configure the Message Waiting Indicator (MWI).

➢ **To configure MWI:**

1. Open the Supplementary Services page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **Supplementary Services**).

Figure 4-20: MWI Configuration

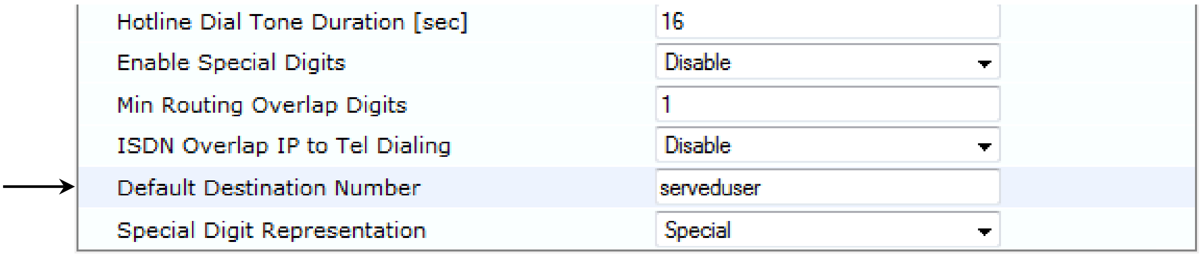


MWI Parameters

Enable MWI	Enable
MWI Analog Lamp	Disable
MWI Display	Disable
Subscribe to MWI	No
MWI Server Transport Type	Not Configured
MWI Server IP Address	
MWI Subscribe Expiration Time	7200
MWI Subscribe Retry Time	120
Stutter Tone Duration	2000

2. From the 'Enable MWI' drop-down list, select **Enable**.
3. Open the DTMF & Dialing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **DTMF & Dialing**).
4. Set the ‘Default Destination Number’ field to "serveduser".

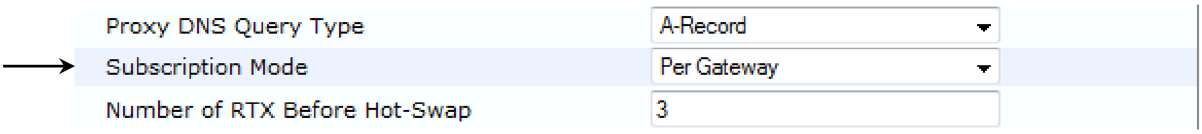
Figure 4-21: Default Destination Number Configuration



Hotline Dial Tone Duration [sec]	16
Enable Special Digits	Disable
Min Routing Overlap Digits	1
ISDN Overlap IP to Tel Dialing	Disable
Default Destination Number	serveduser
Special Digit Representation	Special

5. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).
6. From the ‘Subscription Mode’ drop-down list, select **Per Gateway**.

Figure 4-22: Subscription Mode Configuration



Proxy DNS Query Type	A-Record
Subscription Mode	Per Gateway
Number of RTX Before Hot-Swap	3

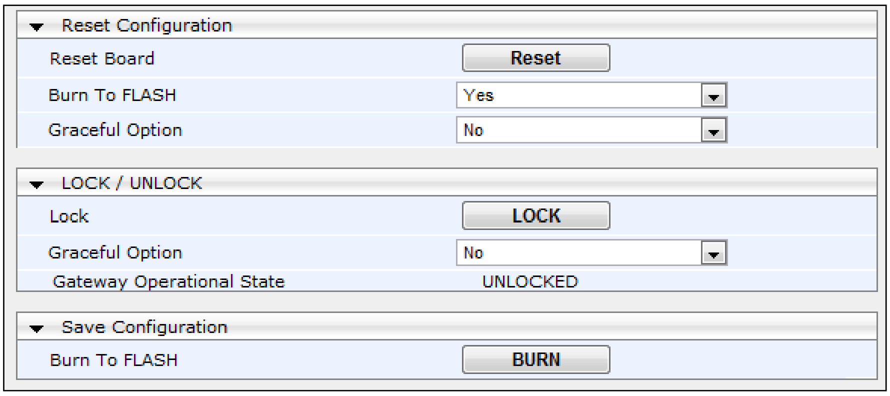
4.16 Reset the Gateway

After completing the configuration of the Gateway, save ("burn") the configuration to the Gateway's flash memory with a reset, for the settings to take effect.

➢ **To save the configuration to flash memory:**

1. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).

Figure 4-23: Resetting the SBC



Reset Configuration

Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No

LOCK / UNLOCK

Lock	LOCK
Graceful Option	No
Gateway Operational State	UNLOCKED

Save Configuration

Burn To FLASH	BURN

2. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).
3. Click the **Reset** button.

Configuration Note