Configuration Note

AudioCodes One Voice for Skype For Business

One-Voice Resiliency

Branch Sites in Microsoft™ Lync® Server or Skype for Business Environments

Version 7.0

Table of Contents

List of Figures

Notice

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. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be downloaded by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: April-05-2016

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 CloudBond 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.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Document Revision Record

LTRT	Description
10540	Initial document release.
10541	Illustrations and configuration updates (including removal of SRD).
10542	Illustrations and configuration updates
10543	Document structure updates and minor configuration revisions.

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.

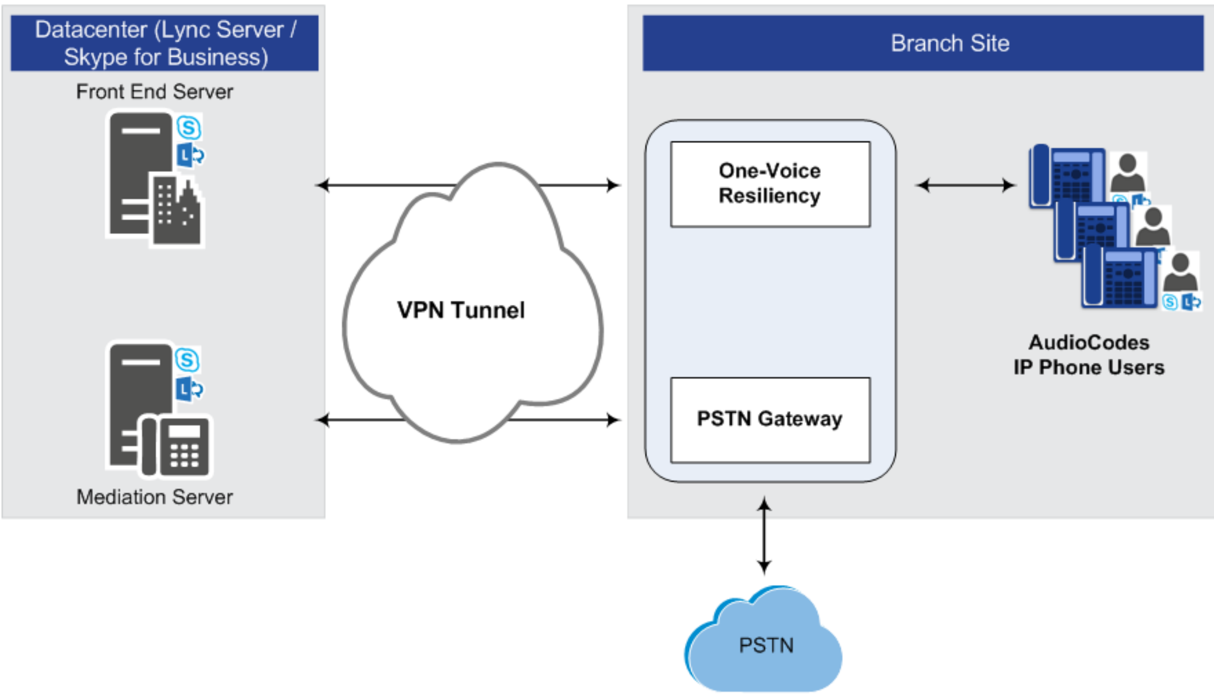
1 Introduction

AudioCodes' One-Voice Resiliency (OVR) feature is a sophisticated and powerful VoIP application that runs on AudioCodes Mediant™ 800B or 1000B devices, providing call survivability (branch-site resiliency) to AudioCodes IP Phone users at the branch site upon connectivity failure with the datacenter (central site or Enterprise headquarters) in a Microsoft® Lync™ / Skype for Business environment. The OVR solution is offered per branch site containing an AudioCodes Mediant device co-located with AudioCodes Lync/Skype for Business-compatible IP Phones. The solution can also include AudioCodes Web-based management tool, *IP Phone Management Interface*, enabling initial, mass provisioning of the IP Phones. Once-Voice Resiliency is a cost-effective solution, eliminating the need for costly Microsoft licenses and server.

In addition to branch-site resiliency, the OVR solution can also provide optional Gateway (Enhanced Gateway) and SBC functionalities, inherit in AudioCodes Mediant 800B/1000B devices, servicing all users in the Lync™ Server/Skype for Business environment in normal operation. If ordered with PSTN interfaces, the device can provide connectivity to the PSTN, enabling users (at branch and central sites) to make and receive PSTN calls during normal operation. In survivability mode, the device maintains PSTN services to the branch site users. The device can also provide direct connectivity to a SIP trunking service, enabling branch site users to make and receive calls during survivability mode.

A high-level illustration of a typical OVR deployment topology is shown below:

Figure 1-1: Typical OVR Deployment



Notes:

- OVR is a Feature-Key dependent feature. For more information, contact your AudioCodes sales representative.
- OVR supports Lync and Skype for Business environments.

1.1 Feature Comparison between SBA and OVR

The table below provides a comparative analysis between AudioCodes' Survivable Branch Appliance (SBA) and OVR in survivability mode.

Table 1-1: Feature Comparison between SBA and OVR in Survivability Mode

Feature	SBA	OVR
Clients (e.g., computer-installed clients)	√	Only AudioCodes IP Phones 400HD Series
Inbound and outbound public switched telephone network (PSTN) calls	√	√
Calls between users at the same site	√	√
Basic call handling, including call hold, retrieval, and transfer	√	√
Contact search	√ (if connectivity with Active Directory at datacenter)	√ (if connectivity with Active Directory at datacenter)
Calls between users in two different sites (via PSTN)	√	√
Two-party instant messaging (IM)	√	×
Call forwarding, simultaneous ringing of endpoints, call delegation, and team call services	√	×
User authentication	√	√
Voice mail capabilities (via PSTN)	√	√
Voice mail to unanswered calls (via PSTN)	√	√
IM, Web, and A/V conferencing	×	×
Presence and Do Not Disturb (DND)-based routing	×	×
Response Group application and Call Park application	×	×
Inter-site data (Desktop Sharing, App Sharing, etc.)	×	×
Conferencing via Conference server	×	×
Enhanced 9-1-1 (E9-1-1)	×	×

1.2 Compatible Software Versions

The table below lists the software versions that are compatible with the OVR solution.

Table 1-2: Compatible Software Versions for OVR Solution

Device	Software Version
Mediant 800B/1000B running OVR	SIP_7.00A.058.002 or later
400HD Series IP Phones	UC_2.0.13.120 or later

1.3 One-Voice Resiliency Constraints

OVR currently includes the following constraints:

- Supports only AudioCodes IP Phones; all other phones (Lync/Skype for Business clients or vendor phones) are not supported and operate according to Microsoft Front End Server or Edge Server.
- For security purposes, the OVR allows only IP Phone users who are currently registered with the Front End server ("approved") to receive service during survivability mode.
- OVR provides almost identical voice functionality in survivability mode as the SBA, with a few exceptions (see Section 1.3).
- Standard Lync deployment that also includes pool pair is supported, while Enterprise Lync deployments with multiple Front End servers managing the same users' pool is not supported in the current release.
- The OVR supports up to 50 branch site users.

This page is intentionally left blank.

2 Overview

This chapter provides a description of the OVR operation in normal mode and survivability mode.

2.1 Normal Mode

In normal mode of operation, OVR acts as an outbound proxy server for the IP Phone users, by seamlessly and transparently forwarding calls between the IP Phone users at the branch site and the Lync / Skype for Business based datacenter, which handles the call routing process (SIP INVITE messages). OVR either forwards the calls to Lync / Skype for Business Front End Server or Edge Server, depending on network architecture.

During normal mode, OVR stores information of the IP Phone users (e.g., phone number). Thus, in effect, not only are the IP Phone users registered with the Front End Server at the datacenter, but also with OVR. OVR uses the information for classifying incoming calls from IP Phone users as well as for routing calls between IP Phone users during call survivability when connectivity with the datacenter is down.

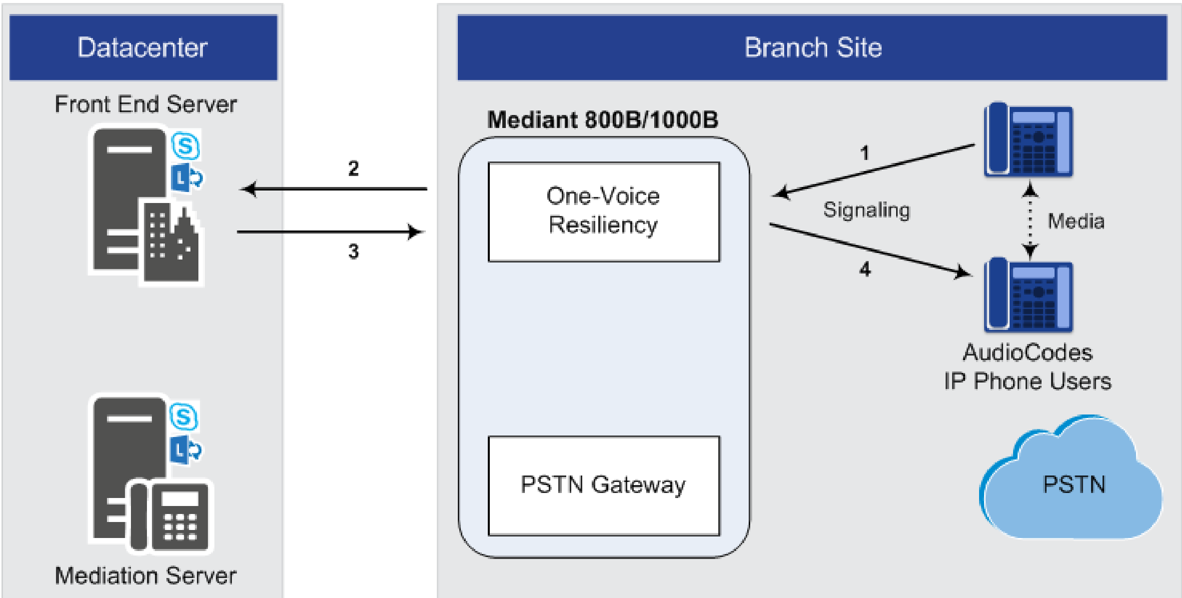
Direct media is employed in Lync/Skype for Business environments, whereby media does not traverse OVR, but flows directly between the IP Phone users. No special OVR configuration is required for this support.

Call flow example scenarios in the OVR solution when in normal mode are listed below:

- **IP Phone-to-IP Phone Calls:**

  IP Phone → OVR → Front End Server → OVR → IP Phone

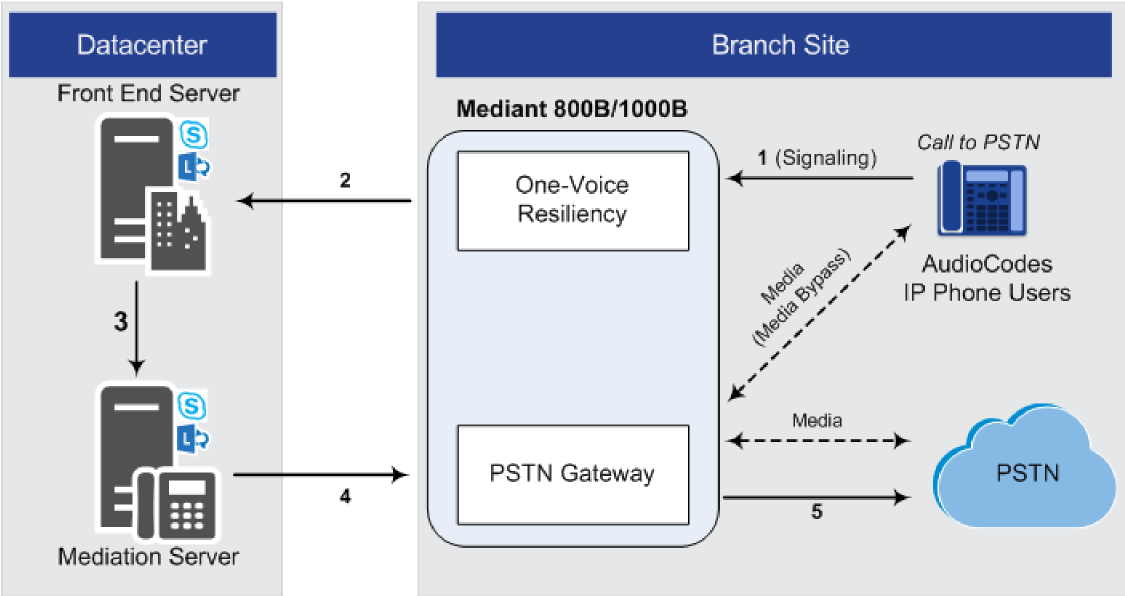
Figure 2-1: Normal Mode - Calls between IP Phones



- **IP Phone-to-PSTN Calls:**

  IP Phone → OVR → Front End Server → Mediation Server → PSTN Gateway → PSTN

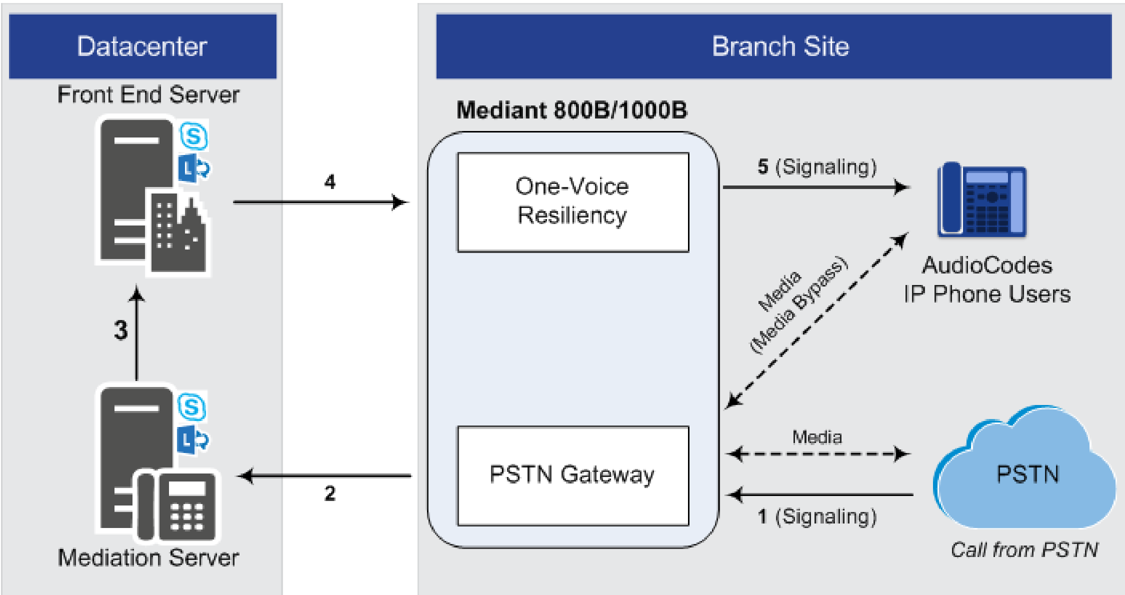
Figure 2-2: Normal Mode - Calls from IP Phone to PSTN



- **PSTN-to-IP Phone Calls:**

  PSTN → PSTN Gateway → Mediation Server → Front End Server → OVR → IP Phone

Figure 2-3: Normal Mode - Calls from PSTN to IP Phone



- **PC Client (Lync/Skype for Business) to IP Phone Calls:**

  PC client → Front End Server → OVR → IP Phone

- **IP Phone-to-PC Client Calls:**

  IP Phone → OVR → Front End Server → PC client

- **PC Client-to-PSTN Calls:**

  PC client → Front End Server → Mediation Server → PSTN Gateway → PSTN

2.2 Survivability Mode

OVR enters *survivability* mode of operation upon detection of connectivity loss with the Lync/Skype for Business based datacenter. In survivability mode, OVR acts as an SBA, providing voice connectivity at branch level and takes over the handling of call routing for the IP Phone users at the branch site. It enables call routing between the IP Phone users themselves, and between the IP Phone users and other optionally deployed entities such as a SIP Trunk and/or a PSTN network, where users can make and receive calls through the SIP Trunk and/or PSTN respectively.

When OVR enters survivability mode, it notifies the IP Phones that they are now in Limited Services state (displayed on the LCD). During this mode, some advanced Microsoft unified communication features provided by Lync / Skype for Business (e.g., presence) become unavailable (see Section 1.3 for supported features during survivability). The OVR provides a mechanism to allow fast restoration of services, to the IP Phone users once connectivity to the Front End server is restored. In addition, the OVR provides immediate but gradual registration mechanism, eliminating an "avalanche" or surge of user registrations on the Front End server.

In survivability mode, the OVR maintains the connection and provides services only to users that have been authorized (registered) by the Front End Server. However, the OVR also provide services to IP Phone users that are no longer registered due to maintenance reasons (e.g., IP Phone reset or upgrade). This maintenance "grace" period is configurable (see Section 3.17).

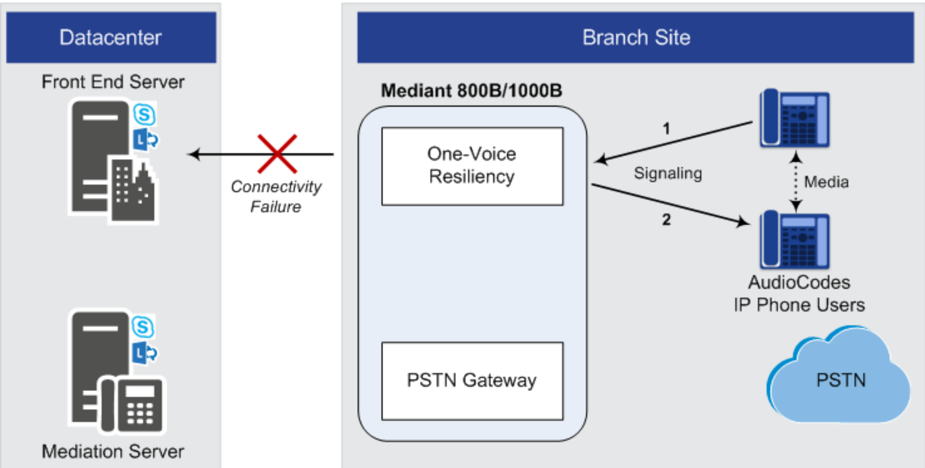
OVR handles call routing based on IP Phone user information that it accumulated during normal operation, as mentioned in Section 2.1. It identifies (classifies) incoming calls as received from IP Phone users based on the caller's IP address and routes the call to the destination based on the called telephone number. Only registered IP Phone users are processed; calls from unregistered IP Phone users are rejected. If the called telephone number is a branch site IP Phone user that is registered with OVR, the call is routed to the IP Phone user. If the called telephone number is not listed in OVR registration database, the call is routed to the PSTN if the setup includes PSTN connectivity; otherwise, the call is rejected. Upon connectivity loss with the Front End server, currently active calls are maintained by the OVR (but may disconnect after a certain period of time).

When OVR detects that connectivity with the datacenter has been restored, it exits survivability mode and begins normal operation mode, forwarding calls transparently between the IP Phones and the datacenter. Full unified communication features provided by Lync/Skype for Business are also restored to the IP Phones.

Call flow example scenarios in the OVR solution when in survivability mode are shown below:

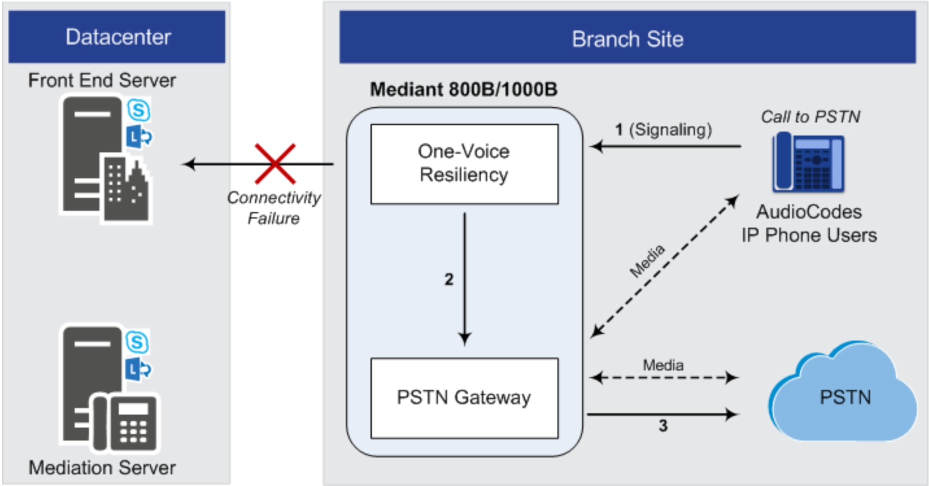
- **IP Phone-to-IP Phone Calls:** IP Phone → OVR → IP Phone

Figure 2-4: Survivability Mode - Calls between IP Phones

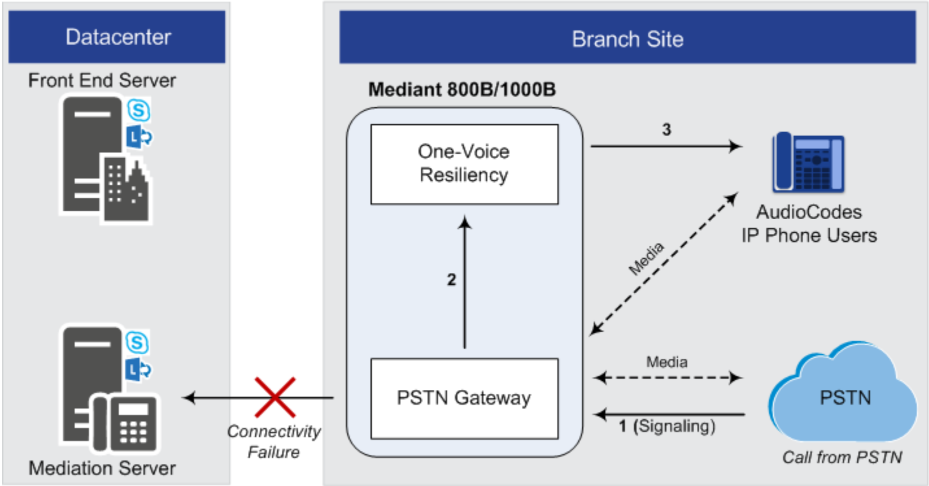


- **IP Phone-to-PSTN Calls:** IP Phone → OVR → PSTN Gateway → PSTN

Figure 2-5: Survivability Mode - Calls from IP Phone to PSTN



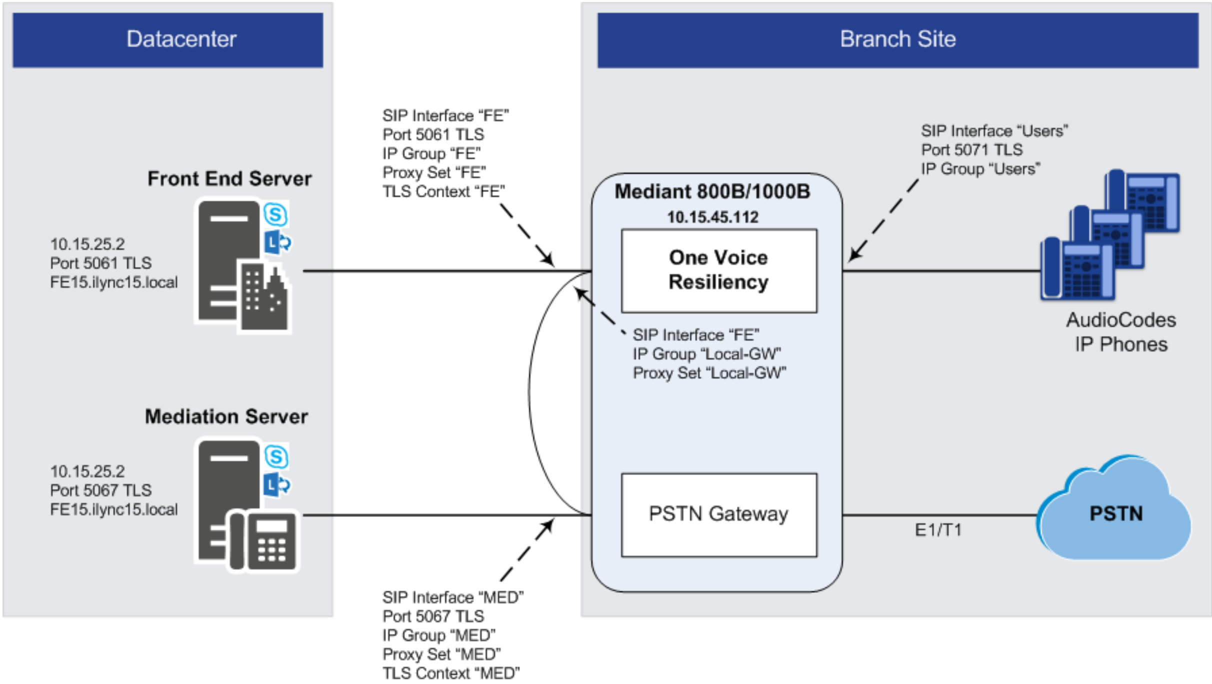
- **PSTN-to-IP Phone Calls:** PSTN → PSTN Gateway → OVR → IP Phone



3 Configuring the Device for OVR

This chapter provides step-by-step instructions on how to configure AudioCodes' device (Mediant 800B or Mediant 1000B) for OVR. It is based on the following example network topology:

Figure 3-1: OVR Example Topology and Configuration Entities



Notes:

- Configuration described in this chapter is based on the example setup scenario. Configuration for your deployment may be different depending on your specific deployment topology and architecture.
- Once you have completed configuration, make sure that you **reset the device with a save configuration to flash memory ("burn")**; otherwise, configuration will be lost after any subsequent device reset or power shut down.

The table below provides a summary of the main entities that need to be configured:

Table 3-1: Summary of Required Configuration

Configuration Entity	Configuration Requirement
Network Interface	A single, local IP network interface of 10.15.44.112. The interface is used for all traffic (SIP signaling, media and OAMP).
TLS Contexts	TLS certification (TLS Context) is required for the following: ▪ Traffic between OVR and Mediation Server. This TLS configuration uses the default TLS Context (ID 0). ▪ Traffic between OVR and Front End Server. This TLS configuration uses TLS Context ID 1.
Media Realm	A single Media Realm for media traffic is used with a port range of 6000-65520 on the network interface.

<table>
<tr><th>Configuration Entity</th><th colspan="4">Configuration Requirement</th></tr>
<tr><td>SIP Interfaces</td><td colspan="4">SIP Interfaces need to be configured for the following:
▪ Mediation Server ("MED"): Interfaces with Mediation Server.
▪ Front End Server ("FE"): Interfaces with the Front End Server (port 5061). A TLS Context (TLS certificate) must be associated with the interface.
▪ Lync users ("Users"): Interfaces with Lync users (IP Phones) at branch site (port 5071).</td></tr>
<tr><td>Proxy Sets</td><td colspan="4">Proxy Sets need to be configured for the following:
▪ Mediation Server ("MED"): Address and port of the Mediation Server. The address can be an FQDN that is resolved into several IP addresses.
▪ Front End Server ("FE"): Address and port of the FE (only a single IP address).
▪ Local Gateway ("Local-GW"): Internal device leg entity that represents the Gateway leg.</td></tr>
<tr><td>IP Groups</td><td colspan="4">IP Groups need to be configured for the following:
▪ Mediation Server ("MED"): Server-type IP Group for the Mediation Server. A typical IP Profile for interoperating with Lync must be associated. The IP Group's mode of operation must be set to default.
▪ Front End Server ("FE"): Server-type IP Group for the FE. The IP Group's mode of operation must be set to Microsoft Server. It is recommended not associate an IP Profile.
▪ Lync users ("Users"): User-type IP Group for Lync users (IP Phones). The IP Group's mode of operation must be set to Microsoft Server.
▪ Local Gateway ("Local-GW"): Internal device leg entity that represents the Gateway leg.</td></tr>
<tr><td>Classification Rules</td><td colspan="4">All Server-type IP Groups must be classified by Proxy Set (configured in the IP Group). The User-type IP Group must be classified according to domain name (configured in the Classification table).</td></tr>
<tr><td rowspan="6">SBC IP-to-IP Routing Rules</td><td>Rule</td><td>Call Scenario</td><td>From (Source)</td><td>To (Destination)</td></tr>
<tr><td>0</td><td>Calls from users to Front End Server.</td><td>Users</td><td>Front End Server</td></tr>
<tr><td>1</td><td>Calls between users if unable to route to Front End Server (alternative route for 1).</td><td>Users</td><td>Users</td></tr>
<tr><td>2</td><td>Calls from users to PSTN if unable to route to Front End Server (alternative route for 1). This is for calls made to the PSTN.</td><td>Users</td><td>Local-GW</td></tr>
<tr><td>3</td><td>Calls from Front End Server to users.</td><td>Front End Server</td><td>Users</td></tr>
<tr><td>4</td><td>Calls from PSTN to users</td><td>Local-GW</td><td>Users</td></tr>
<tr><td rowspan="2">Tel-to-IP Routing Rule</td><td>Rule</td><td>Call Scenario</td><td>From</td><td>To</td></tr>
<tr><td>0</td><td>Calls from the PSTN to users when unable to route to Mediation Server (alternative route for default proxy).</td><td>GW Trunk</td><td>OVR</td></tr>
<tr><td rowspan="2">IP-to-Tel Routing Rule</td><td>Rule</td><td>Call Scenario</td><td>From</td><td>To</td></tr>
<tr><td>0</td><td>Calls to the PSTN.</td><td>any</td><td>Gateway Trunk</td></tr>
<tr><td></td><td colspan="4">▪</td></tr>
</table>

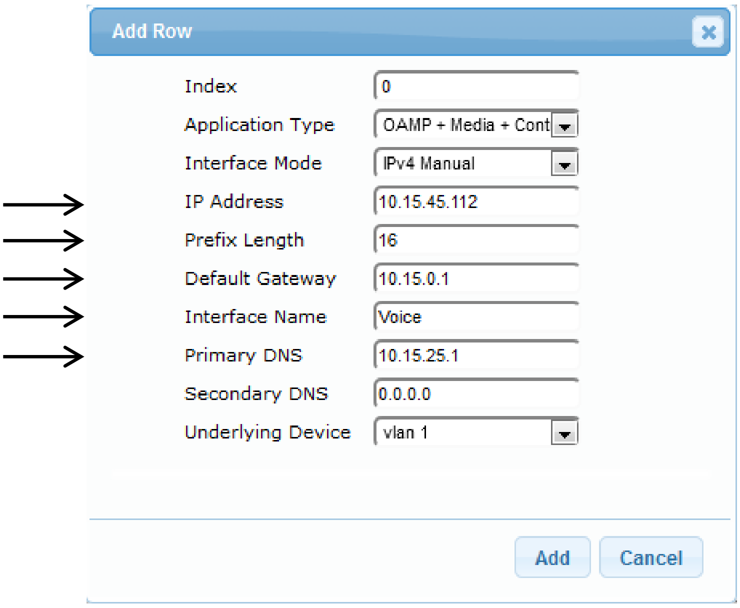
3.1 Step 1: Configure a Local IP Network Interface

In the example setup, a single IP network interface is used for all traffic (OAMP, media and signaling).

➢ **To add the logical IP network interfaces:**

1. Open the Interface table (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Select the OAMP interface row, click **Edit**, and then change the IP network interface as shown below:

Figure 3-2: Configuring Logical IP Network Interface



3. Click **Add**, and then reset the device with a burn-to-flash for your settings to take effect.
4. Connect to the device's management interface, using the new OAMP address.

3.2 Step 2: Enable the SBC Application

For OVR functionality, you must enable the SBC application.

➢ **To enable the SBC application:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).

Figure 3-3: Enabling SBC Application

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**, and then reset the device with a burn-to-flash for your settings to take effect.

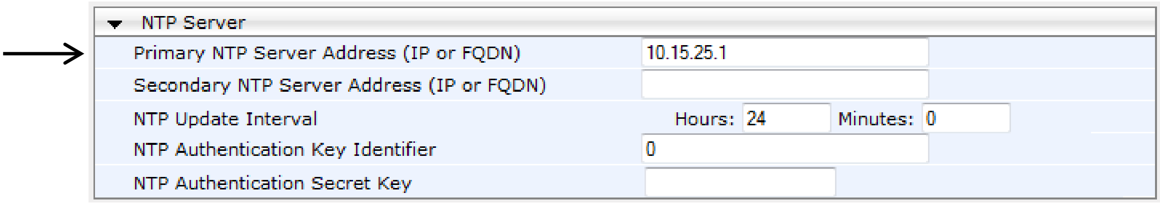
3.3 Step 3: Configure an NTP Server

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or a third-party server) to ensure that the device receives the accurate and current date and time. This is necessary for validating certificates of remote parties.

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

1. Open the Application Settings page (**Configuration** tab > **System** > **Time And Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.25.1**).

Figure 3-4: Configuring NTP Server Address



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

3.4 Step 4: Configure TLS for Mediation Server

TLS certificate negotiation occurs between the device and Mediation Server.

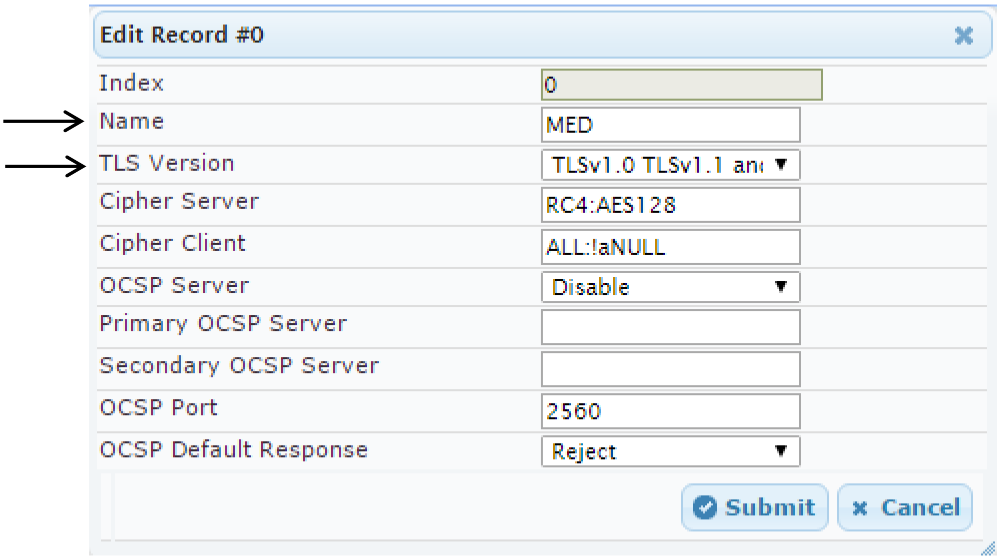
3.4.1 Enable TLS

This step describes how to configure the device to use TLS Version 1.0 and above. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➢ **To configure TLS Version:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click 'Edit'.
3. From the '**TLS Version**' drop-down list, select '**TLSv1.0 TLSv1.1 and TLSv1.2**'

Figure 3-5: Configuring TLS Version



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

3.4.2 Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by device to authenticate the connection with Lync / Skype for Business. The procedure involves the following main steps:

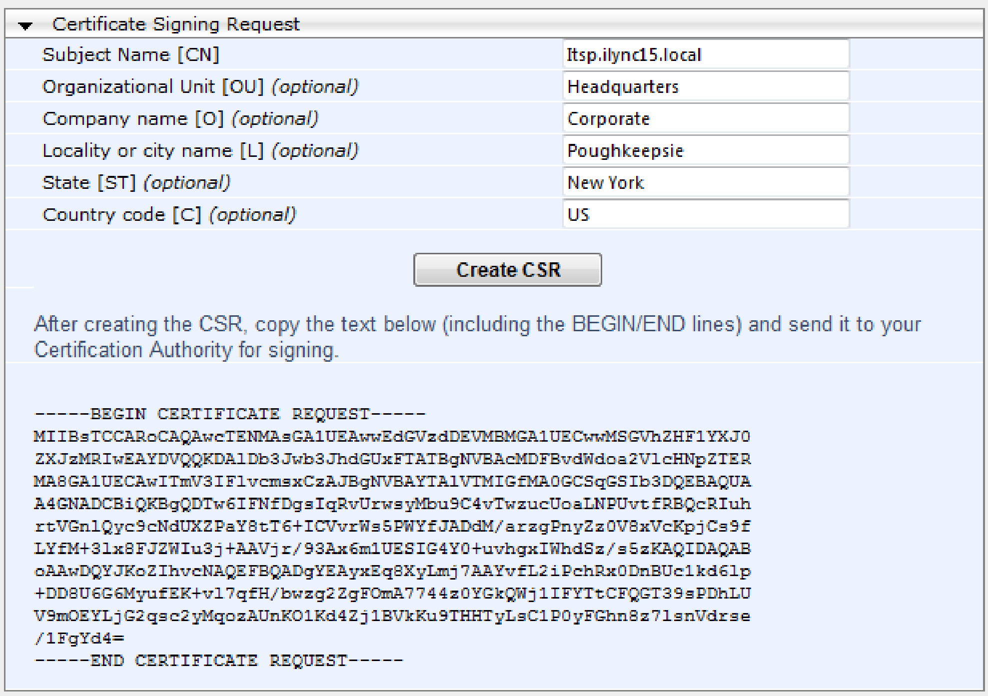
1. Generating a Certificate Signing Request (CSR).
2. Requesting Device Certificate from CA.
3. Obtaining Trusted Root Certificate from CA.
4. Deploying Device and Trusted Root Certificates on E-SBC.

➢ **To configure a certificate:**

1. Open the TLS Contexts table (**Configuration** tab > **System** menu > **TLS Contexts**).
2. Select the TLS Context at index 0, and then click the **TLS Context Certificates** button located at the bottom of the TLS Contexts table; the Context Certificates page appears.

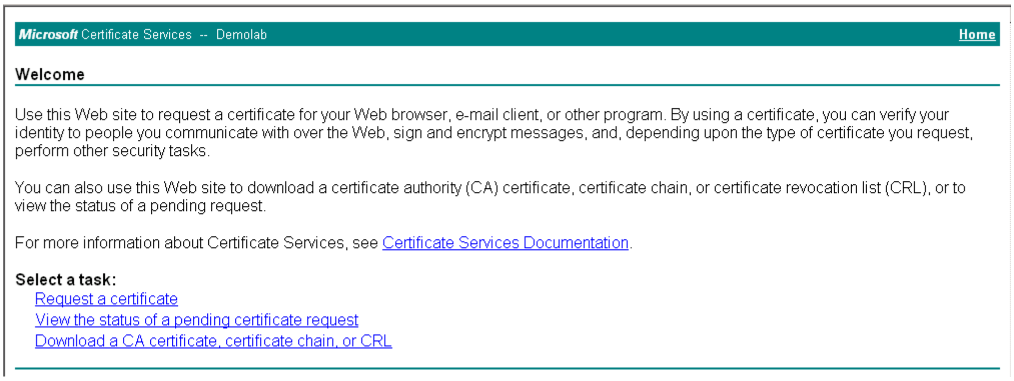
3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the FQDN of the device (e.g., **Itsp.ilync15.local**).
   b. Fill in the rest of the request fields according to your security provider's instructions.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 3-6: Certificate Signing Request – Creating CSR



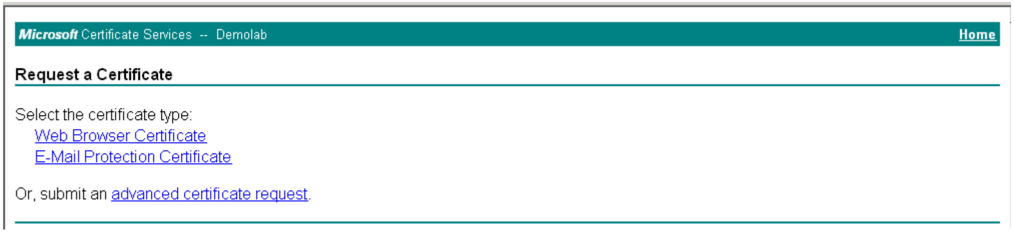
5. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----**" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 3-7: Microsoft Certificate Services Web Page



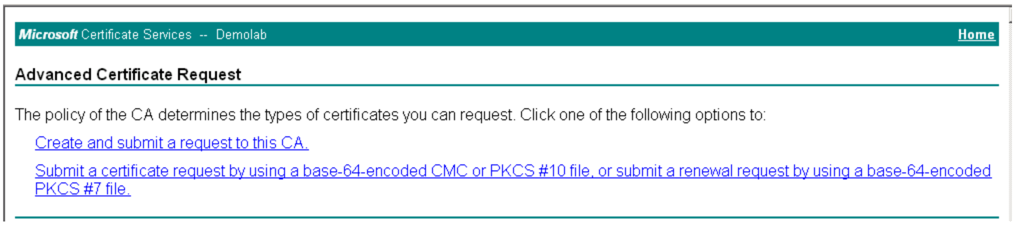
7. Click **Request a certificate**.

Figure 3-8: Microsoft Certificate Services - Request a Certificate Page



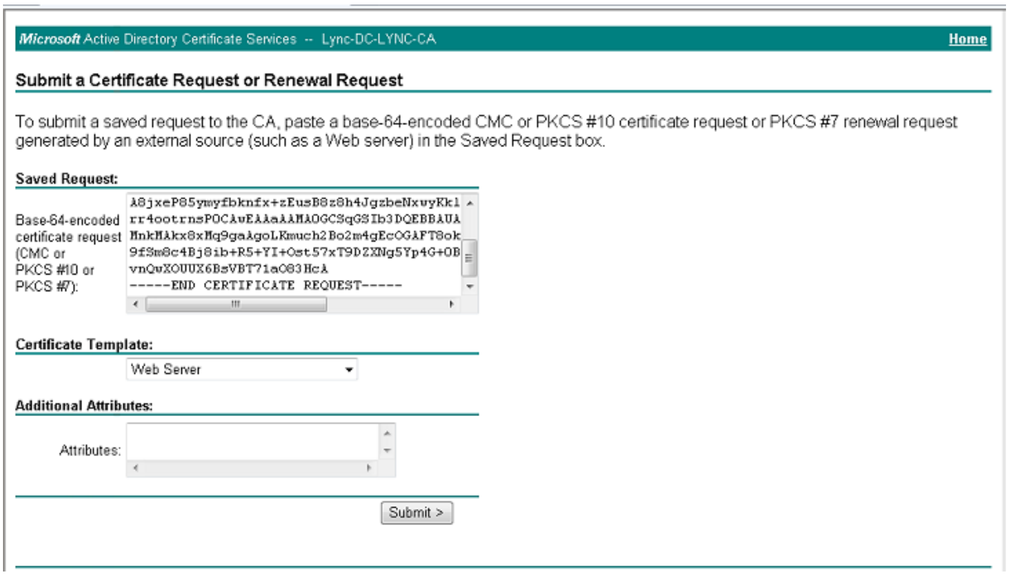
8. Click **advanced certificate request**, and then click **Next**.

Figure 3-9: Microsoft Certificate Services - Advanced Certificate Request Page



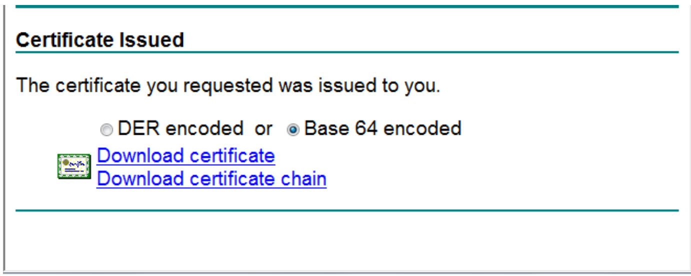
9. Click **Submit a certificate request ...**, and then click **Next**.

Figure 3-10: Microsoft Active Directory Certificate Services - Submit a Certificate Request or Renewal Request Page



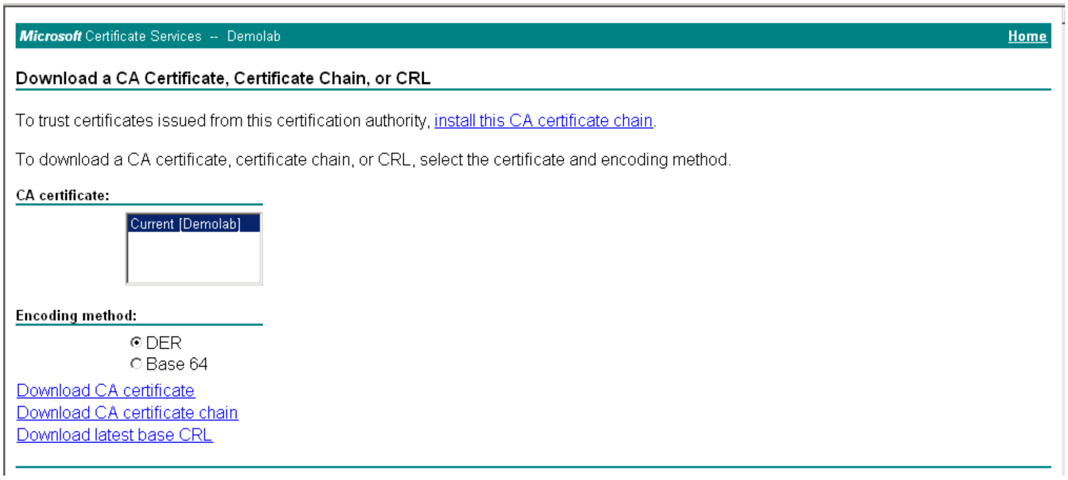
10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**.

Figure 3-11: Certificate Issued Page



13. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.
14. Save the file as *gateway.cer* to a folder on your computer.
15. Click the **Home** button or navigate to the certificate server at http://<Certificate Server>/CertSrv.
16. Click **Download a CA certificate**, **certificate chain, or CRL**.

Figure 3-12: Microsoft Certificate Services - Download a CA Certificate, Certificate Chain, or CRL Page



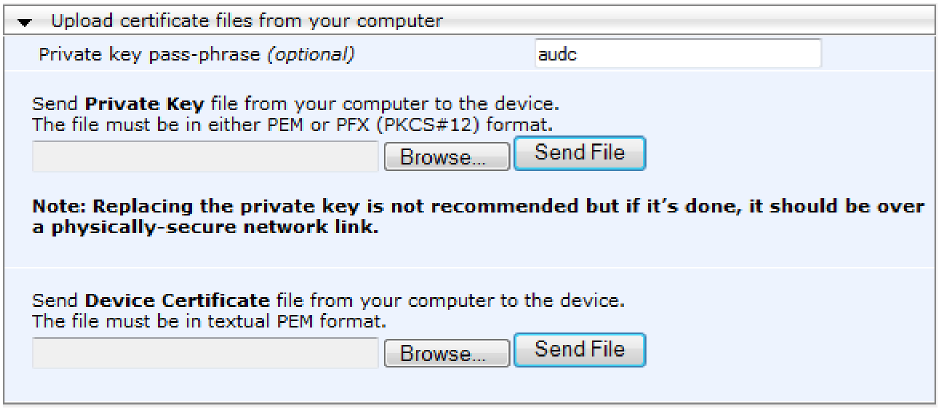
17. Under the 'Encoding method' group, select the **Base 64** option for encoding.
18. Click **Download CA certificate**.
19. Save the file as *certroot.cer* to a folder on your computer.

20. In the device's Web interface, return to the **TLS Contexts** table and do the following:

   a. Select TLS Context at index 0, and then click the **TLS Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.

   b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the device.

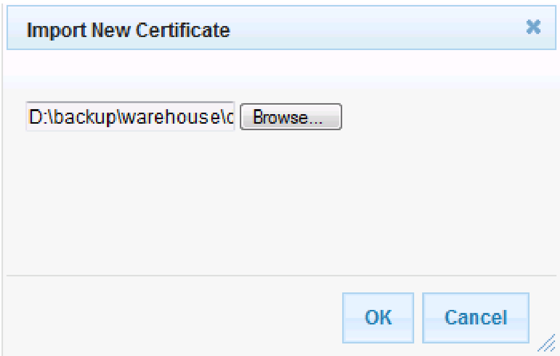
Figure 3-13: Upload Device Certificate Files from your Computer Group



   c. In the TLS Contexts table, select TLS Context at index 0, and then click the **TLS Context Trusted-Roots Certificates** button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.

   d. Click the **Import** button, and then select the certificate file to load.

Figure 3-14: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

22. Reset the device with a burn to flash for your settings to take effect.

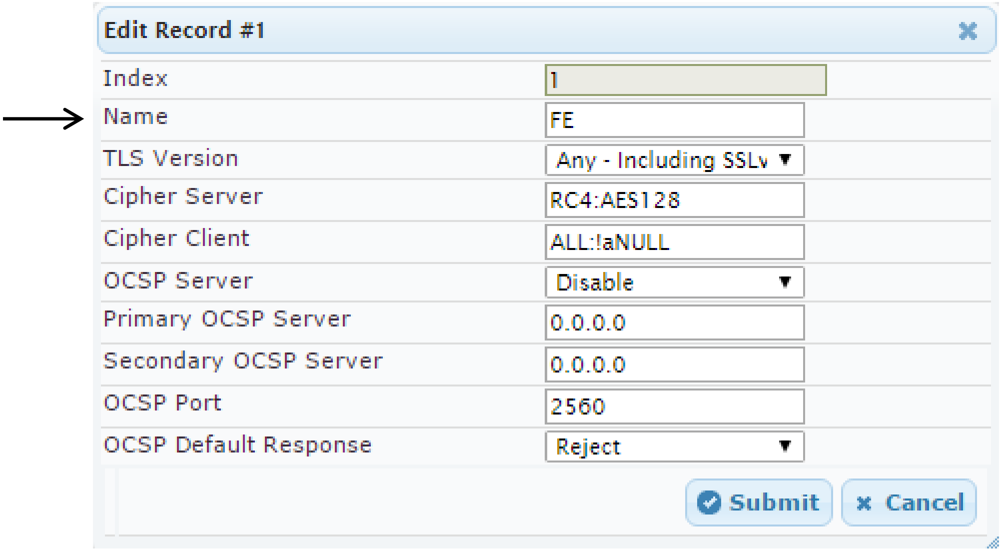
3.5 Step 5: Configure TLS for Front End Server

The following procedure describes how to configure TLS for communication with the Front End Server. Note that there is no certificate negotiation between the OVR and Front End Server.

➢ **To configure TLS for Front End Server:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. Click **Add**, and then in the Add Row dialog box, configure the TLS Context as shown below:

Figure 3-15: Configuring TLS Context for Front End Server



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

3.6 Step 6: Configure SRTP

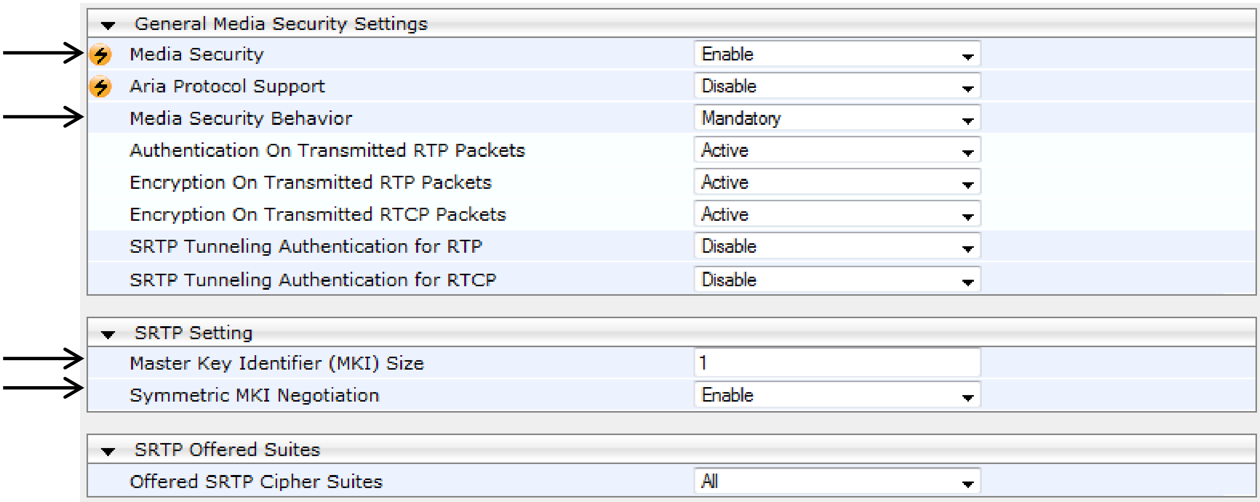
As Mediation Server employs SRTP, you need to configure the device to also operate in the same manner.

➢ **To configure media security:**

1. Open the Media Security page (**Configuration** tab > **VoIP** menu > **Media** menu > **Media Security**).
2. Do the following configuration:

Parameter	Configuration	Description
Media Security	**Enable**	-
Media Security Behavior	**Mandatory**	The device initiates encrypted calls. If negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected.

Figure 3-16: Configuring SRTP



Click **Submit**, and then reset the device with a burn-to-flash for your settings to take effect.

3.7 Step 7: Configure a Media Realm

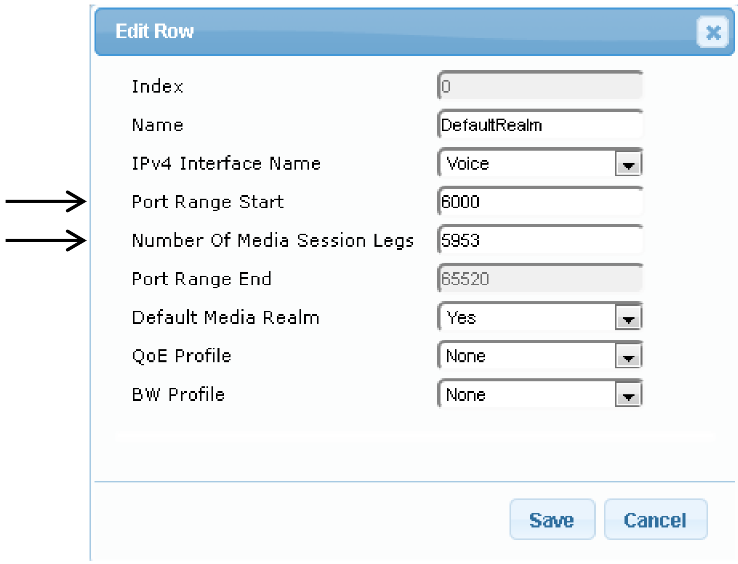
The Media Realm defines a port range for media (RTP) traffic on a specific network interface. In the example setup, only a single Media Realm is used (default).

➢ **To modify the default Media Realm:**

1. Open the Media Realm table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Select the default Media Realm (Index 0), and then click **Edit**.

3. Modify the Media Realm according to your deployment:

Figure 3-17: Configuring a Media Realm



4. Click **Save** to apply your settings.

3.8 Step 8: Configure SIP Interfaces

The SIP Interface represents a Layer-3 network that defines a local listening port for SIP signaling traffic on a specific network interface. In the example setup, you need to add SIP Interfaces for interfacing with the following:

- Mediation Server
- Front End Server
- Lync users (IP Phones) at branch site

➢ To add SIP Interfaces:

1. Open the SIP Interface table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Click **Add**, and then in the Add Row dialog box, add a SIP Interface.

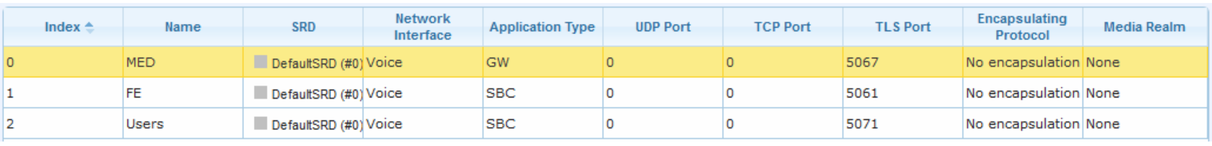
   In the example setup, add SIP Interfaces with the following configuration:

SIP Interface	Specific Configuration			
	Name	**Application Type**	**TLS Port**	**TLS Context Name**
Interfacing with Mediation Server	**MED**	**GW**	**5067**	**MED**
Interfacing with Front End Server	**FE**	**SBC**	**5061**	**MED**
Interfacing with IP Phone users	**Users**	**SBC**	**5071**	**MED**

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

   The figure below displays the configured SIP Interfaces:

Figure 3-18: Configured SIP Interfaces



Index	Name	SRD	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Encapsulating Protocol	Media Realm
0	MED	DefaultSRD (#0)	Voice	GW	0	0	5067	No encapsulation	None
1	FE	DefaultSRD (#0)	Voice	SBC	0	0	5061	No encapsulation	None
2	Users	DefaultSRD (#0)	Voice	SBC	0	0	5071	No encapsulation	None

3.9 Step 9: Configure Proxy Sets

The Proxy Set defines the actual address of SIP server entities in your network. In the example, you need to add Proxy Sets for the following:

- Mediation Server
- Front End Server
- Entity to reach the local PSTN Gateway

Note: If the datacenter employs Front End pool pairing and the main Front End server fails, the OVR enters survivability mode (i.e., ignores the pool pairing mechanism).

➢ **To add Proxy Sets:**

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Click **Add**, and then in the Add Row dialog box, configure a Proxy Set.

   In the example setup, add Proxy Sets with the following configuration:

Proxy Set	Configuration							
	Name	**Gateway IPv4 SIP Interface**	**SBC IPv4 SIP Interface**	**Proxy Keep-Alive**	**Proxy Keep-Alive Time**	**TLS Context Name**	**Proxy Load Balancing Method**	**Proxy Hot Swap**
Mediation Server	**MED**	**MED**	-	**Using OPTIONS**	**60**	**MED**	**Round Robin**	**Enable**
Front End Server	**FE**	-	**FE**	**Using OPTIONS**	**30**	**FE**	-	-
Entity to reach local PSTN Gateway	**Local-GW**	-	**FE**	-	-	-	-	-

The figure below displays the configured Proxy Sets:

Figure 3-19: Configured Proxy Sets

Index	Name	SRD	Gateway IPv4 SIP Interface	SBC IPv4 SIP Interface	Proxy Keep-Alive Time [sec]	Redundancy Mode	Proxy Hot Swap
0	MED	DefaultSRD (#0)	MED	None	60		Enable
1	FE	DefaultSRD (#0)	None	FE	30		Disable
2	Local-GW	DefaultSRD (#0)	None	FE	60		Disable

3. Configure addresses per Proxy Set. For each Proxy Set, do the following:
   - e. Select the Proxy Set row, and then click the **Proxy Address Table** link located below the table; the Proxy Address Table appears.
   - f. Click **Add**, and then in the Add Row dialog box, configure the address and transport protocol.

   In the example setup, configure the Proxy Sets with the following addresses:

Proxy Set Name	Configuration	
	Proxy Address	**Transport Type**
MED	**med.ilync15.local:5067**	**TLS**
FE	**10.15.25.2:5061**	**TLS**
Local-GW	**10.15.45.112:5067**	**TLS**

3.10 Step 10: Configure a Proxy Set for Mediation Server

The device communicates directly with Mediation Server through its' PSTN Gateway. The PSTN Gateway forwards calls from the PSTN to Mediation Server. The address of Mediation Server is defined by a Proxy Set, as configured in Section 3.9.

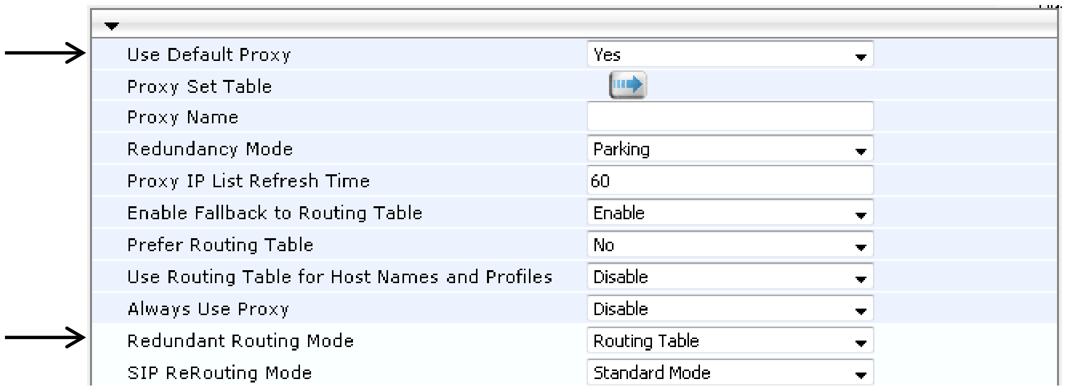
The following procedure provides advanced proxy configuration related to Mediation Server.

➢ **To configure advanced proxy server settings for Mediation Server:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**), and then do the following configuration:

Parameter	Configuration	Description
Use Default Proxy	**Yes**	Enables Mediation Server to act as a proxy server for PSTN Gateway
Redundant Routing Mode	**Routing Table**	If the Mediation Server is down (no response), the PSTN Gateway sends the call to the IP Phone user. To enable this alternative routing, you need to configure a Tel-to-IP routing rule (see Section 3.19.6) to route the call to the OVR, and then configure an SBC IP-to-IP Routing rule (see Section 3.14) to then route the call to the IP Phone user.

Figure 3-20: Configuring Proxy Parameters for Mediation Server



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

3.11 Step 11: Configure an IP Profile for Mediation Server

An IP Profile enables you to apply a group of specific settings to specific calls by associating it with an IP Group. In the example setup, the following IP Profile needs to be configured for Mediation Server.

➢ **To add an IP Profile:**

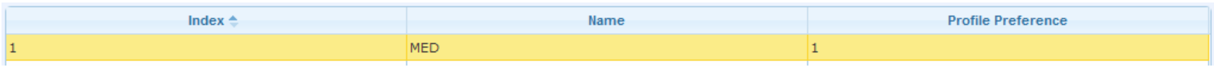
1. Open the IP Profile Settings table (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**, and then in the Add Row dialog box, add an IP Profile.

   In the example setup, add an IP Profile with the following configuration:

Common Configuration					Gateway Configuration		
Name	**Reset SRTP Upon Re-key**	**Symmetric MKI**	**MKI Size**	**Generate SRTP Keys Mode**	**Media Security Mode**	**Early Media**	**Early 183**
MED	**Enable**	**Enable**	**1**	**Always**	**Mandatory**	**Enable**	**Enable**

The figure below displays the configured IP Profile:

Figure 3-21: Configured IP Profile



Index	Name	Profile Preference
1	MED	1

3.12 Step 12: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the device communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. In the example, you need to add IP Groups for the following:

- Mediation Server
- Front End Server
- Lync users (IP Phones) at branch site
- Local Gateway

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Click **Add**, and then in the Add Row dialog box, configure an IP Group.

   In the example setup, add IP Groups with the following configuration:

IP Group	Specific Configuration					
	Name	**Type**	**Proxy Set**	**IP Profile**	**SBC Operation Mode**	**Outbound Message Manipulation Set**
Mediation Server	**MED**	**Server**	**MED**	**MED**	**B2BUA**	-
Front End Server	**FE**	**Server**	**FE**	-	**Microsoft Server**	-
Users	**Users**	**User**	-	-	**Microsoft Server**	-
Local Gateway	**Local-GW**	**Server**	**Local-GW**	-	**B2BUA**	**3** (configured in Section 3.18)

   The figure below displays the configured IP Groups:

Figure 3-22: Configured IP Groups

Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulation Set	Outbound Message Manipulation Set
0	MED	DefaultSRD	Server	B2BUA	MED	MED	None		Enable	-1	-1
1	FE	DefaultSRD	Server	Microsoft Serv	FE	None	None		Enable	-1	-1
2	Users	DefaultSRD	User	Microsoft Serv	None	None	None		Enable	-1	-1
3	Local-GW	DefaultSRD	Server	B2BUA	Local-GW	None	None		Enable	-1	3

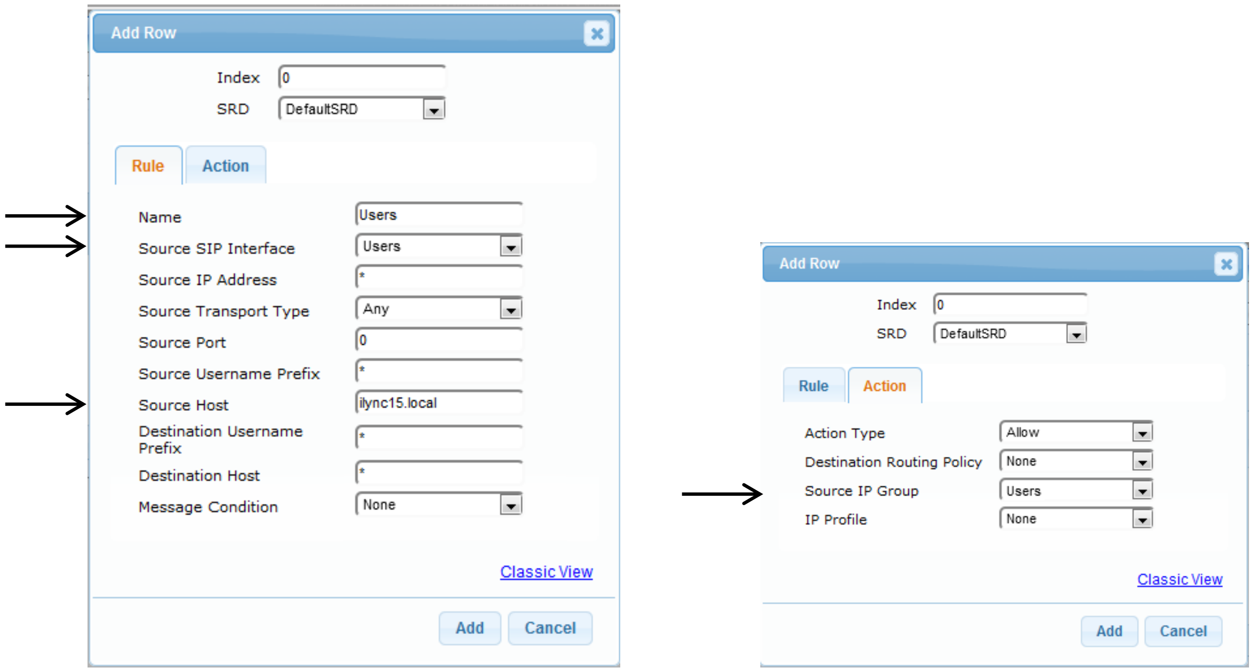
3.13 Step 13: Configure a Classification Rule

For the device to identify calls from IP Phone users at the branch site and classify them to their IP Group ("Users"), you need to add a Classification rule. Classification of calls from the other entities in the deployment (i.e., Mediation Server and Front End Server) are by Proxy Set (i.e., source IP address). In the example setup, calls received with the source host name, *ilync15.local* are considered as originating from IP Phone users.

➢ **To add a Classification rule for IP Phone users:**

1. Open the Classification table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Click **Add**, and then in the Add Row dialog box, add a Classification rule as shown below:

Figure 3-23: Classification Rule for Users



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

3.14 Step 14: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The device selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call.

In the example setup, you need to add routing rules for the following call scenarios:

- Routing calls from Users to Front End Server
- Routing calls between Users (alternative route for above)
- Routing calls from Users to PSTN (alternative route for above)
- Routing calls from Front End Server to Users
- Routing calls from PSTN to Users

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

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Click Add, and then in the Add Row dialog box, add an IP-to-IP Routing rule.

   In the example setup, add IP-to-IP Routing rules with the following configuration:

IP-to-IP Routing Rule	Specific Configuration				
	Name	Alternative Route Options	Source IP Group	Request Type	Destination IP Group
Users → Front End Server	**User-FE**	**Route Row**	**Users**	**All**	**FE**
Users → Users (alternative route for above)	**User-User**	**Alternative Route Consider Inputs**	**Users**	**INVITE and REGISTER**	**Users**
Users → PSTN (alternative route for above)	**User-GW**	**Alternative Route Consider Inputs**	**Users**	**INVITE and REGISTER**	**Local-GW**
Front End Server → Users	**FE-Users**	**Route Row**	**FE**	**All**	**Users**
PSTN → Users	**GW-Users**	**Route Row**	**Local-GW**	**All**	**Users**

The figure below displays the configured IP-to-IP Routing rules:

Figure 3-24: Configured IP-to-IP Routing Rules

Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destination SIP Interface	Destination Address
0	User-FE	Default_SBCI	Route Row	Users	All	*	*	IP Group	FE	None	
1	User-User	Default_SBCI	Alternative R	Users	INVITE and R	*	*	IP Group	Users	None	
2	User-GW	Default_SBCI	Alternative R	Users	INVITE and R	*	*	IP Group	Local-GW	None	
4	FE-Users	Default_SBCI	Route Row	FE	All	*	*	IP Group	Users	None	
9	GW-Users	Default_SBCI	Route Row	Local-GW	All	*	*	IP Group	Users	None	

3.15 Step 15: Configure Media Parameters

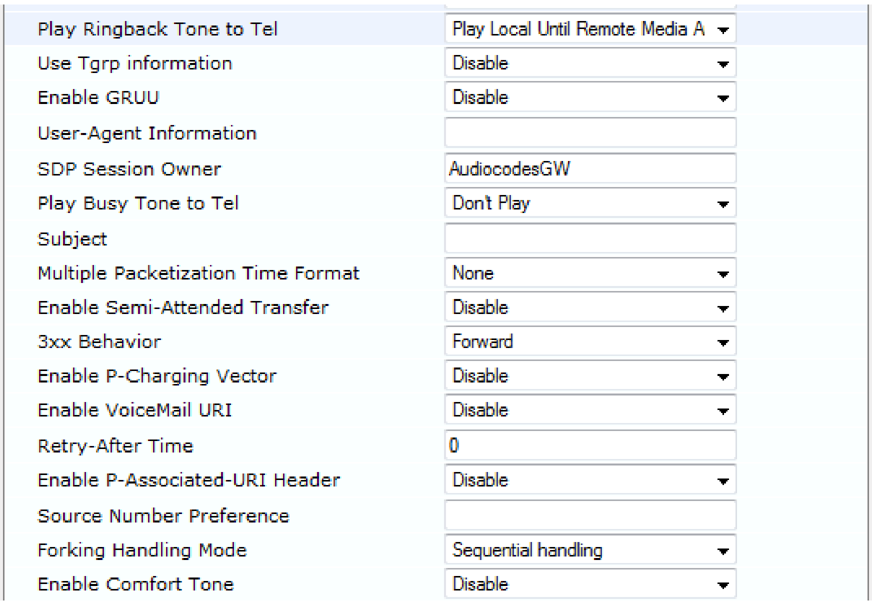
This step describes how to configure the gateway for Media behavior with Microsoft Lync / Skype for Business.

➢ **To configure Media Parameters:**

1. Open the General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).
2. Do the following configuration:

Parameter	Configuration	Description
Play Ringback Tone to Tel	**Play Local Until Remote Media Arrive**	If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the Enhanced Gateway plays a local ringback tone if there are no prior received RTP packets. The Enhanced Gateway stops playing the local ringback tone as soon as it starts receiving RTP packets. At this stage, if the Enhanced Gateway receives additional 18x responses, it does not resume playing the local ringback tone
Forking Handling Mode	**Sequential handling**	The PSTN Gateway re-opens the stream according to subsequently received 18x responses with SDP, or plays a ringback tone if 180 response without SDP is received

Figure 3-25: Configure Media Parameters

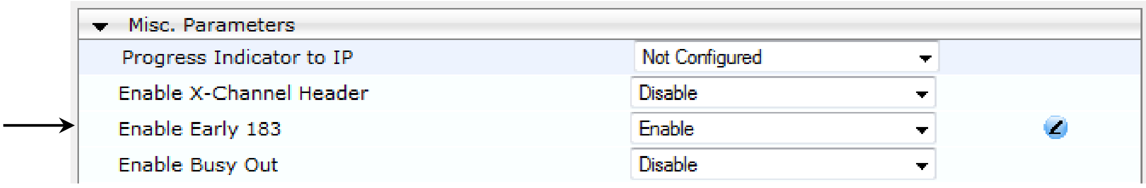


Click **Submit** to apply your settings.

3. Open the Advanced Parameters page (**Configuration tab** > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**), and then do the following configuration:

Parameter	Configuration	Description
Enable Early 183	**Enable**	**Note:** If the 'B-Channel Negotiation' parameter is set to **Preferred** or **Any**, the 'Enable Early 183' parameter is ignored and a SIP 183 is not sent upon receipt of an INVITE. In such a case, you can set the 'Progress Indicator to IP' (ProgressIndicator2IP) parameter to 1 (PI = 1) for the device to send a SIP 183 upon receipt of an ISDN Call Proceeding message.

Figure 3-26: Configuring Early Media in Advanced Parameters Page



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

3.16 Step 16: Restrict Communication with Mediation Server Only

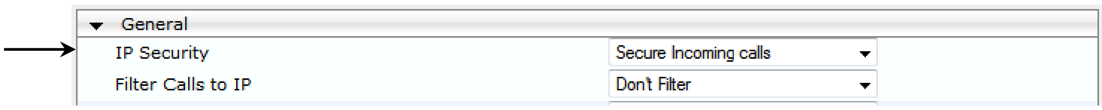
The procedure below describes how to restrict IP communication only between the PSTN Gateway and Mediation server. This ensures that the PSTN Gateway accepts / sends SIP calls **only** from / to Mediation Server (as required by Microsoft).

➢ **To restrict communication only between PSTN Gateway and Mediation Server:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
2. Do the following configuration:

Parameter	Configuration	Description
IP Security	**Secure Incoming calls**	-

Figure 3-27: Restricting Communication with Mediation Server



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

3.17 Step 17: Configure Graceful Period for Registration Expiry

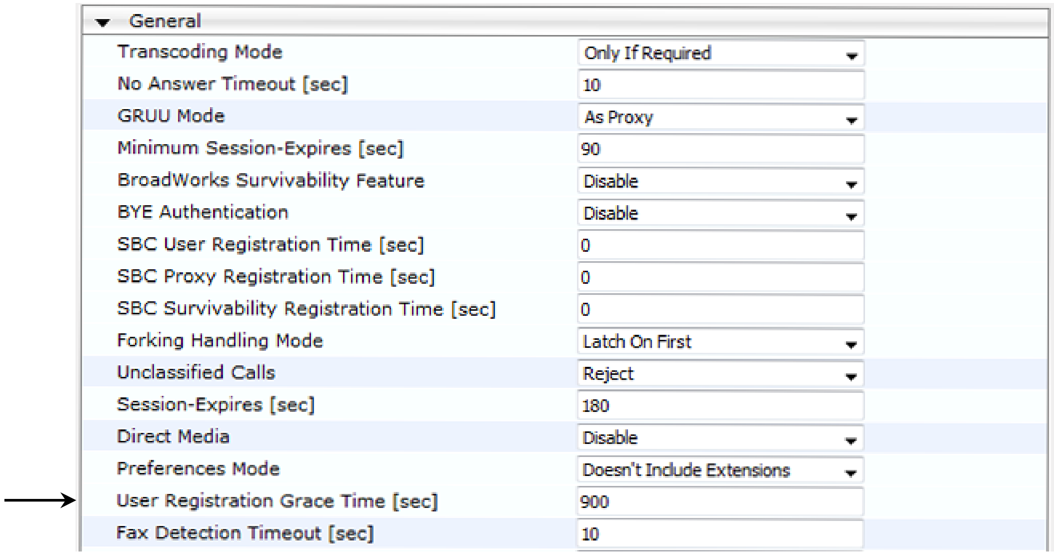
In survivability mode, if the registration time of the registered IP Phone at the OVR is about to expire and the IP Phone resets, by the time the IP Phone becomes available again, the OVR would have already removed the IP Phone from its database due to expiry time being reached. As the OVR does not support new registrations during survivability mode, the IP Phone user will not receive any service from the OVR. Thus, to prevent this scenario and keep the IP Phone registered in the database, you can configure the OVR to add time ("graceful") to the original expiry time.

The configuration below allows 15 minutes of the IP Phone to be in out-of-service state, allowing it to register with the OVR after this period and receive services from it.

➢ **To add a graceful period to the registration expiry time:**

1. Open the SBC General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **SBC General Settings**).
2. In the 'User Registration Grace Time' (SBCUserRegistrationGraceTime) field, enter "900" (in seconds).

Figure 3-28: Configuring Graceful Registration Expiry Time



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

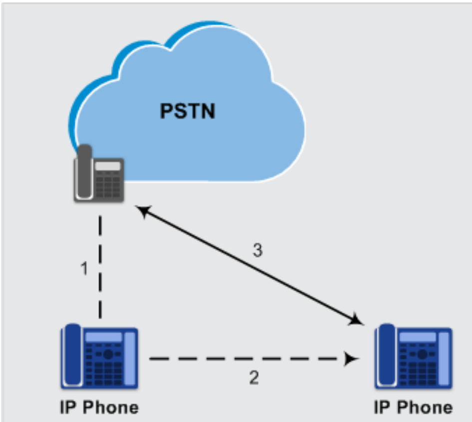
3.18 Step 18: Configure Message Manipulation Rules

In the example setup, you need to configure manipulation rules for the following:

- Incoming SIP INVITE messages received from the IP Phones contain the name (caller ID) and phone number of the IP Phones. In survivability mode, to enable the PSTN Gateway to send calls to the PSTN with the IP Phone's number as caller ID (source number), the name must be removed.
- For call transfers initiated by IP Phones:
    - Transfer of PSTN call to another IP Phone: The REFER message sent to the IP Phone must be manipulated so that the Refer-To header's host name is changed to the device's IP address and port (i.e., 10.15.45.112:5061) and the transport type changed to TLS.

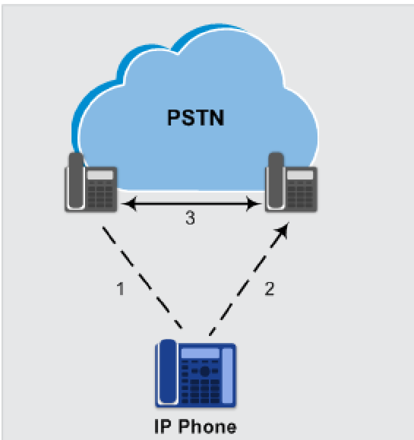
Note: The Message Manipulation Rules described above are only valid in Survivability mode.

Figure 3-29: Call Transfer of PSTN Call to Another IP Phone User



- Transfer of PSTN call to another PSTN user. The REFER message sent to the IP Phone must be manipulated so that the Refer-To header's host name is changed to the device's IP address and port (i.e., 10.15.45.112:5067) and the transport type changed to TLS.

Figure 3-30: Call Transfer of PSTN Call to Another PSTN User



Once configured, you need to assign the rules to the IP Group, "Local-GW" in the outbound direction (see Section 3.12), using the Manipulation Set ID (3) under which the rules are configured.

➢ **To configure Message Manipulation rules:**

1. Open the Message Manipulations table (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation > Message Manipulations**).
2. For each rule, click **Add**, and then in the Add Row dialog box, add a Message Manipulation rule. When you have finished, click **Add** to apply your settings. Add the following rules:
   - For setting IP Phone's number as Caller ID for calls to PSTN in survivability mode:

Parameter	Configuration
Index	**0**
Name	**Change Name to Number**
Manipulation Set ID	**3**
Message Type	**invite**
Action Subject	**header.p-asserted-identity.0**
Action Type	**Remove**

   - For transfer of PSTN call to another IP Phone user:

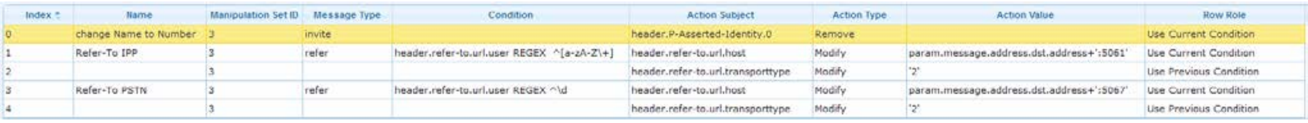
Parameter	Configuration
Index	**1**
Name	**Refer-To IPP**
Manipulation Set ID	**3**
Message Type	**REFER**
Condition	header.refer-to.url.user REGEX ^[a-zA-Z\+]
Action Subject	header.refer-to.url.host
Action Type	**Modify**
Action Value	**param.message.address.dst.address+':5061'**
Row Rule	**Use Current Condition**
Index	**2**
Name	
Manipulation Set ID	**3**
Message Type	
Condition	
Action Subject	**header.refer-to.url.transporttype**
Action Type	**Modify**
Action Value	**'2'**
Row Rule	**Use Previous Condition**

- For transfer of PSTN call to another PSTN user:

Parameter	Configuration
Index	**3**
Name	**Refer-To PSTN**
Manipulation Set ID	**3**
Message Type	**REFER**
Condition	**header.refer-to.url.user REGEX ^\d**
Action Subject	**header.refer-to.url.host**
Action Type	**Modify**
Action Value	**param.message.address.dst.address+':5067'**
Row Rule	**Use Current Condition**
Index	**4**
Name	
Manipulation Set ID	**3**
Message Type	
Condition	
Action Subject	**header.refer-to.url.transporttype**
Action Type	**Modify**
Action Value	**'2'**
Row Rule	**Use Previous Condition**

The figure below displays the configured Message Manipulation rule:

Figure 3-31: Configured Message Manipulation Rules



Index	Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	change Name to Number	3	invite		header.P-Asserted-Identity.0	Remove		Use Current Condition
1	Refer-To IPP	3	refer	header.refer-to.url.user REGEX ^[a-zA-Z\+]	header.refer-to.url.host	Modify	param.message.address.dst.address+':5061'	Use Current Condition
2		3			header.refer-to.url.transporttype	Modify	'2'	Use Previous Condition
3	Refer-To PSTN	3	refer	header.refer-to.url.user REGEX ^\d	header.refer-to.url.host	Modify	param.message.address.dst.address+':5067'	Use Current Condition
4		3			header.refer-to.url.transporttype	Modify	'2'	Use Previous Condition

3.19 Step 19: Configure the PSTN Gateway

This section describes the configuration required for interfacing with the PSTN. In the example, you need to configure the trunk as an E1 ISDN trunk.

3.19.1 Configure the Trunk

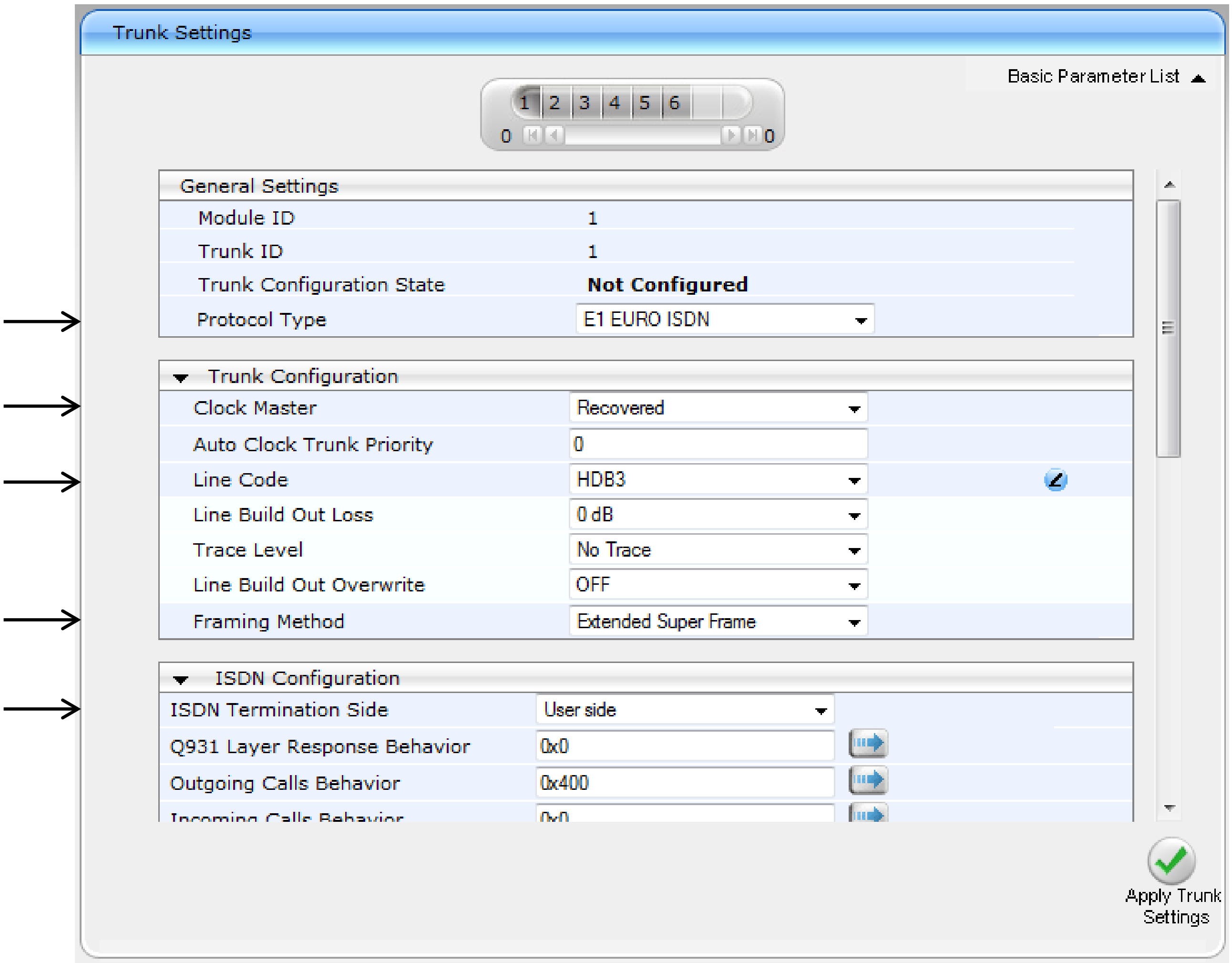
The procedure below describes basic configuration of the physical trunk.

➢ **To configure the physical trunk:**

1. Open the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Trunk Settings**).
2. Select the trunk that you want to configure, by clicking the corresponding trunk number icon.
3. If the trunk is new, configure the trunk as required. If the trunk was previously configured, click the **Stop Trunk** button to de-activate the trunk.
4. Basic trunk configuration:

Parameter	Configuration Example	Description
Protocol Type	**E1 Euro ISDN**	Defines the trunk protocol. **Notes:** ▪ If the parameter displays **NONE** (i.e., no protocol type selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the device. ▪ To delete a previously configured trunk, set the parameter to **NONE**. ▪ All PRI trunks must be of the same line type - E1 or T1. However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the Release Notes). ▪ BRI trunks can operate with E1 or T1 trunks. ▪ If the trunk can't be stopped because it provides the clock (assuming the device is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the clock or enable 'TDM Bus PSTN Auto Clock' in the TDM Bus Settings page (see Section 3.19.2).
Clock Master	**Recovered**	Defines the trunk's clock source: ▪ **Recovered**: clock source is recovered from the trunk. ▪ **Generated**: clock source is provided by the internal TDM bus clock source (according to the parameter 'TDM Bus Clock Source' - see Section 3.19.2).
Line Code	**HDB3**	Defines the line code: ▪ **B8ZS:** bipolar 8-zero substitution - for T1 trunks only ▪ **HDB3:** high-density bipolar 3 - for E1 trunks only ▪ **AMI:** for E1 and T1
Framing Method	**Extended Super Frame**	Defines the framing method. **Note:** For E1 trunks, always set this parameter to **Extended Super Frame**.
ISDN Termination	**User side**	Defines if the trunk is connected to the PSTN as User or Network side.

Figure 3-32: Configuring Trunk Settings



5. Continue configuring the trunk according to your requirements.
6. When you have completed configuration, click the **Apply Trunk Settings** button to apply the changes to the selected trunk.
7. Reset the device with a burn-to-flash for your settings to take effect...

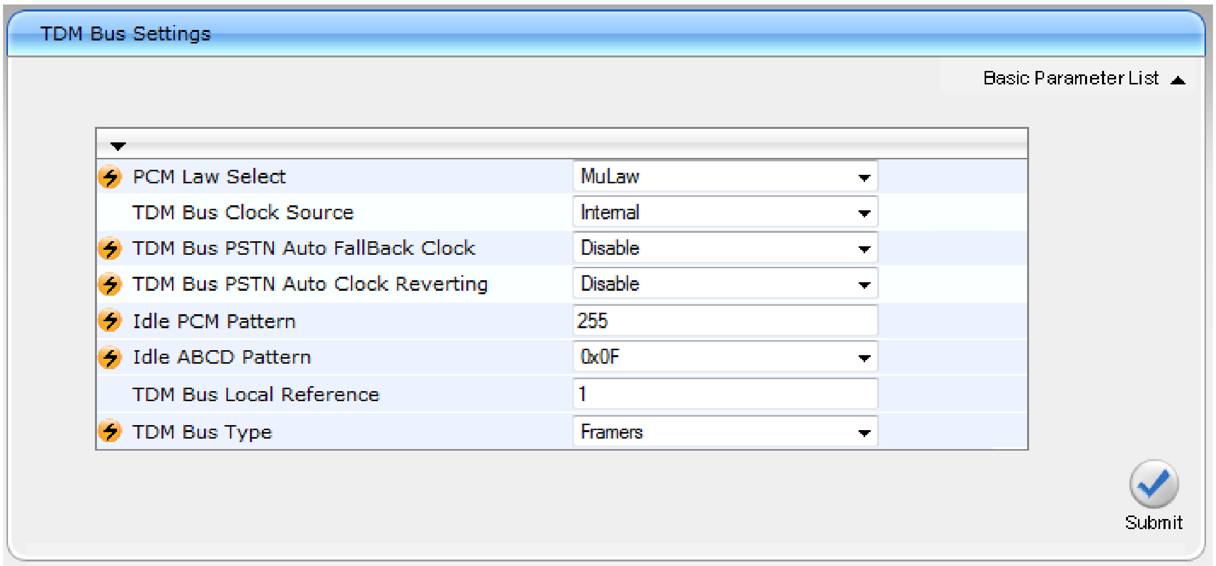
3.19.2 Configure the TDM Bus

The procedure below describes how to configure the TDM bus.

➢ **To configure the TDM bus:**

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

Figure 3-33: Configuring TDM Bus



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 Enhanced Gateway synchronizes - generate clock from local source (Internal) or recover clock from PSTN line (Network).
   - **TDM Bus Local Reference:** defines the physical trunk ID from which the Enhanced 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**, and then reset the device with a burn-to-flash for your settings to take effect.

3.19.3 Enable the Trunk

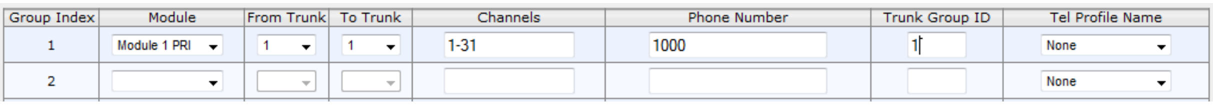
To enable trunks, you need to assign them to Trunk Groups. In the example setup, you need to enable the E1 trunk.

➢ **To enable the trunk:**

1. Open the Trunk Group table (**Configuration** tab > **VoIP** menu > **Gateway** > **Trunk Group** > **Trunk Group**), and then do the following configuration:

Parameter	Configuration	Description
Module	**Module 1 PRI**	Module number and type on which the trunk is located
From Trunk / To Trunk	**1 / 1**	Physical trunk range
Channels	**1-31**	B-channels to enable on the trunk
Phone Number	**1000**	Logical (used internally by device) phone number (e.g.,) for the first channel; phone numbers 1001, 1002, 1003, and so on are sequentially assigned to subsequent channels
Trunk Group ID	**1**	Trunk Group number for the trunk

Figure 3-34: Enabling Trunk by Assigning it a Trunk Group



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

3.19.4 Configure the Channel Select Method

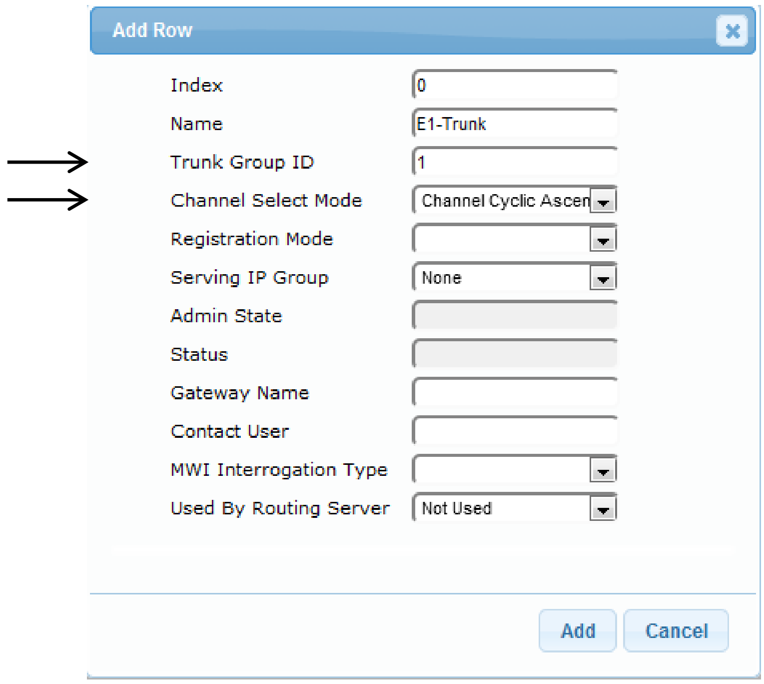
You need to configure the method for assigning IP-to-Tel calls to channels within the Trunk Group. In the example setup, a cyclic ascending method is used, whereby the device selects the next available channel in the Trunk Group, in ascending order. After the highest channel number (e.g., 31) in the Trunk Group, the device selects the lowest channel number (e.g., 1) and then starts ascending again.

➢ **To configure the channel select mode:**

1. Open the Trunk Group Settings page (**Configuration** tab > **VoIP** menu > **Gateway** > **Trunk Group** > **Trunk Group Settings**).
2. Click **Add**, and then in the Ad Row dialog box, configure the trunk as follows:

Parameter	Configuration	Description
Trunk Group ID	**1**	Trunk Group that you want to configure
Channel Select Mode	**Channel Cyclic Ascending**	-

Figure 3-35: Configuring the Channel Select Method



3. Click **Add** to apply your changes.

3.19.5 Configure an IP-to-Trunk Group Routing Rule

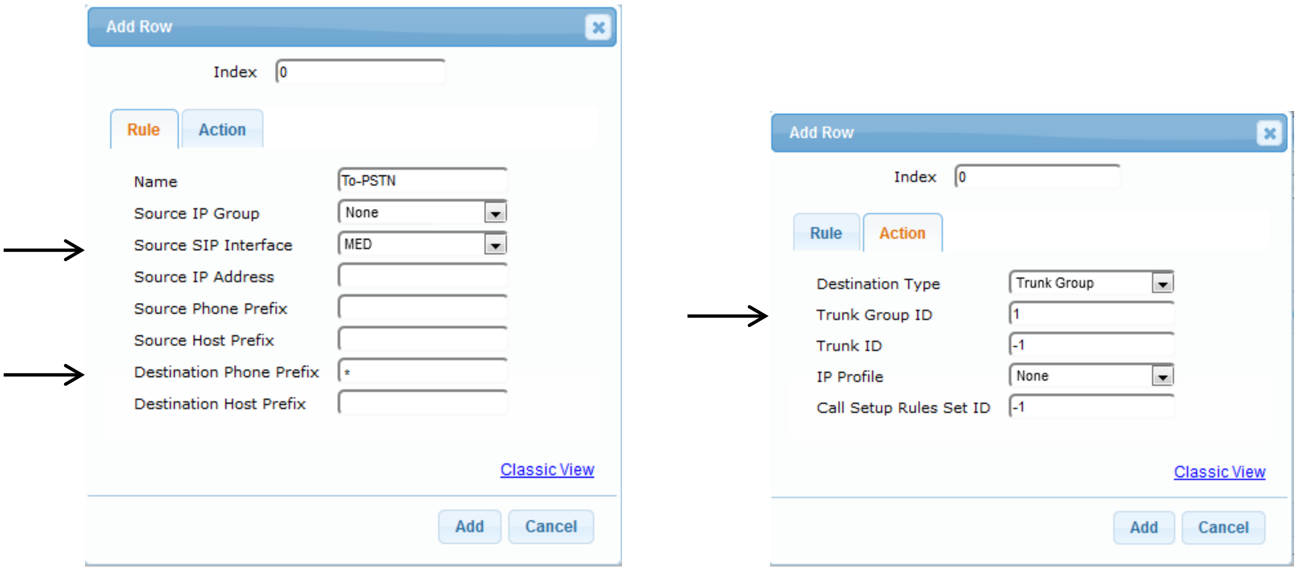
In the example setup, you need to configure an IP-to-Tel routing rule for routing calls to the PSTN.

➢ **To configure an IP-to-Trunk Group routing rule:**

1. Open the IP to Trunk Group Routing table (**Configuration** tab > **VoIP** menu > **Gateway** > **Routing** > **IP to Trunk Group Routing**).
2. Click **Add**, and then in the Add Row dialog box, configure an IP-to-Tel routing rule with the following configuration:

Parameter	Configuration	Description
Source SIP Interface	**MED**	SIP Interface from where call is received
Destination Phone Prefix	*	Asterisk (*) sign denotes any number
Trunk Group ID	**1**	Trunk Group to where call is sent

Figure 3-36: Configuring an IP-to-Tel Routing Rule



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

3.19.6 Configure a Tel-to-IP Routing Rule

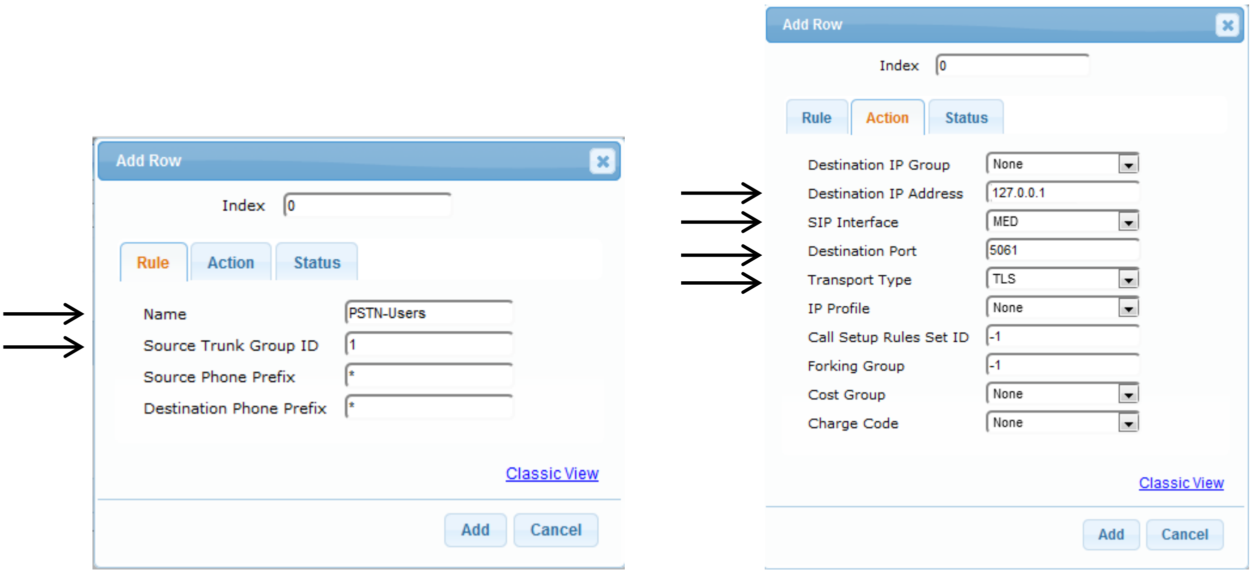
In normal operation, the device forwards calls from the PSTN to Mediation Server. However, if connectivity with Mediation Server is down, the device routes the PSTN call directly to the IP Phone users. To enable this functionality, you need to configure a Tel-to-IP routing rule, as described below. This rule routes the call to the OVR. The IP-to-IP Routing rule, "GW-Users" (see Section 3.14) is then used to route the call to the IP Phone user.

➢ **To configure a Tel-to-IP routing rule:**

1. Open the Tel to IP Routing table (**Configuration** tab > **VoIP** menu > **Gateway** > **Routing** > **Tel to IP Routing**).
2. Click **Add**, and then add a routing rule as shown below:

Parameter	Configuration	Description
Name	**PSTN-Users**	-
Source Trunk Group ID	**1**	-
Destination IP Address	**127.0.0.1**	The IP address 127.0.0.1 is a logical representation of the device's IP address. When you apply the configuration (i.e., click **Add**), the actual address populates the field (i.e., 10.15.45.112).
SIP Interface	**MED**	-
Destination Port	**5061**	-
Transport Type	**TLS**	-

Figure 3-37: Configuring a Tel-to-IP Routing Rule



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

3.19.7 Configure a Number Manipulation Rule

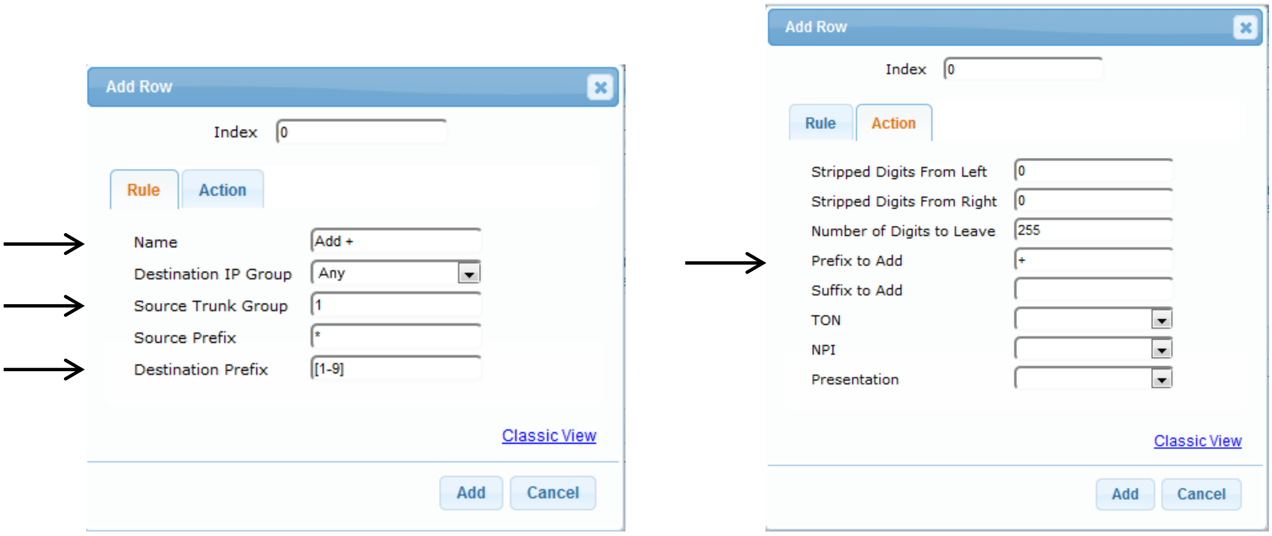
If necessary, you can configure number manipulation rules to manipulate the source and/or destination phone numbers routed between the entities. In the example, you need to configure a manipulation rule to add the plus sign (+) as a prefix to calls received from the PSTN if the destination number starts with any number between 1 and 9. For example, if the called number is 12063331212, the device changes it to +12063331212 (i.e., into an E.164 number format).

➢ **To configure number manipulation rules:**

1. Open the Destination Phone Number Manipulation Table for Tel-to-IP Calls table (**Configuration** tab > **VoIP** menu > **Gateway** > **Manipulations** > **Dest Number Tel -> IP**).
2. Click **Add**, and then add a manipulation rule as shown below:

Parameter	Configuration	Description
Name	**Add +**	-
Source Trunk Group	**1**	Calls received from this Trunk Group
Destination Prefix	**[1-9]**	Any number with prefix from 1 to 9
Prefix to Add	**+**	-

Figure 3-38: Configuring a Number Manipulation Rule



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

4 Configuring AudioCodes IP Phones for OVR

This chapter describes the configuration of AudioCodes Lync-compatible IP Phones located at the branch site with OVR.

4.1 Deployment Summary

The deployment for AudioCodes IP Phones with OVR in the Microsoft Lync / Skype for Business environment can be summarized in the following steps (in chronological order):

1. Remove the IP Phone from the shipped package.
2. Cable the IP Phone to the network.
3. Cable the IP Phone to the power supply to power up the IP Phone.
4. The IP Phone broadcasts a DHCP message to the network to discover a DHCP server and request information (DHCP Options). (DHCP is enabled by default.)
5. The DHCP server at the Microsoft datacenter responds to the IP Phone with DHCP Options providing, for example, networking settings (IP address and Default Gateway), NTP server address, LDAP server address (Front End server), DNS address, and TLS certificate.
6. The IP Phone applies the settings with a reset.
7. The IP Phone user initiates a sign-in (registration) to Microsoft Lync / Skype for Business (Front End server) with credentials (username and password, or PIN code) provided by the Administrator.
8. The Front End server registers the IP Phone.
9. The Administrator configures the IP Phone for OVR, which entails defining the IP address:port of the OVR (as an "outbound proxy server" for the IP Phone). Depending on management platform used to configure the IP Phone, this step may be done at this stage or before Step 3.
10. All traffic between the IP Phone and Front End server now pass transparently through the OVR.

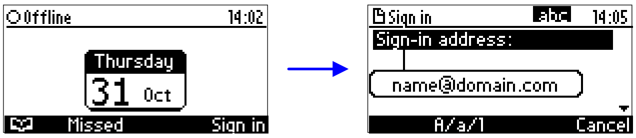
4.2 Signing IP Phone into Lync / Skype for Business

To register the IP Phone with the Front End server, the user must perform a sign-in procedure on the IP Phone. You can sign in using a username-password combination (default) or a PIN code, provided by the Administrator.

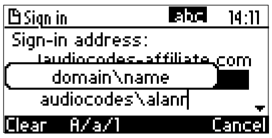
Note: The LCD screens shown in the procedure are of the 430HD and 440HD models; the 420HD model's LCD screens are similar.

➢ **To sign in the phone with Lync / Skype for Business:**

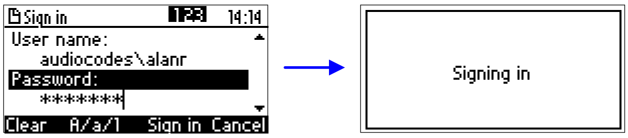
1. In the idle LCD, press the **Sign in** softkey:



2. In the 'Sign-in address' field, enter your SIP URI.
3. In the 'User name' field, enter the domain name, backslash, and then username:



4. In the 'Password' field, enter the password, and then press the **Sign in** softkey:



4.3 Configuring IP Phones for OVR

The configuration includes defining the IP address:port of the OVR so that it can function as an outbound proxy server for the IP Phone. Once configured, all subsequent SIP signaling traffic between IP Phone and datacenter traverses (transparently) the OVR.

The table below describes the parameters that must be configured on the IP Phone. Parameters enclosed with square brackets […] denote the parameters of the Configuration file; Parameters not enclosed denote the corresponding Web interface parameters.

Table 4-1: Parameter Settings of IP Phones for OVR

Parameter	Settings
Use Hosting Outbound Proxy [lync/sign_in/use_hosting_outbound_proxy]	Enables the use of an outbound proxy server (i.e., the OVR) for sending SIP messages. Set the parameter to **[1]** Enable.
Outbound Proxy IP Address or Host Name [lync/sign_in/fixed_outbound_proxy_address]	Defines the IP address of the outbound proxy (i.e., OVR). All outgoing SIP messages are sent to this proxy. Set the parameter to the IP address of the OVR.
Outbound Proxy Port [lync/sign_in/fixed_outbound_proxy_port]	Defines the SIP listening port on the outbound proxy (OVR). The valid value range is 1024 to 65535 (default is 5060). Set the parameter to the port of the OVR.

You can use the following platforms to configure the IP Phones:

- Web interface: This requires that you configure each IP Phone separately (see Section 4.3.1)
- AudioCodes EMS: Easy-to-use platform, enabling rapid mass provisioning of IP Phones (see Section 4.3.2)
- Third-party TFTP/HTTP server: Enables mass provisioning of IP Phones using a TFTP/HTTP server (see Section 4.3.3)

4.3.1 Configuring IP Phones through the Web Interface

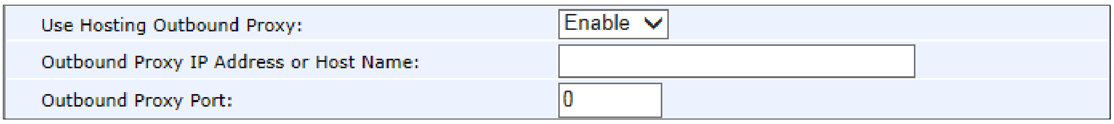
If you want to use the Web-based management platform for configuration, you need to perform the following procedure on each IP Phone. Perform this configuration

Note: Perform this configuration **only after** the IP Phone user has signed in to (registered with) Lync / Skype for Business, as described in Section 4.2.

➢ **To configure the IP Phone through Web interface:**

1. Open the Signaling Protocol page (**Configuration** tab > **Voice Over IP** menu > **Signaling Protocols**), and then scroll down to the SIP Proxy and Registrar group:

Figure 4-1: Configuring OVR on the IP Phone through Web Interface



2. Configure the parameters according to the instructions in Section 4.3.
3. Click **Submit** to apply your settings.

You can also configure the IP Phone by manually loading a Configuration file (.cfg) through the Web interface:

1. Create a Configuration file that contains the following parameter settings:

```
lync/sign_in/fixed_outbound_proxy_address=10.15.45.112
lync/sign_in/fixed_outbound_proxy_port=5071
lync/sign_in/use_hosting_outbound_proxy=1
```

2. Open the Configuration File page (**Management** tab > **Manual Update** menu > **Configuration File**).
3. Load the Configuration file, by clicking **Loading New Configuration File**.

4.3.2 Configuring IP Phones through the IP Phone Management Server

AudioCodes IP Phone Management Server can be used to mass provision the IP Phones deployed with OVR. The IP Phones "learn" of the address of the EMS through DHCP. The address must be configured on the DHCP server with the name of the Configuration file. The Configuration file must be sent to the IP Phones using DHCP Option 160 (when the IP Phones are initially powered up). Once the IP Phones connect to the IP Phone Management Server, the IP Phone Management Server sends the Configuration file over HTTP (dhcpoption160.cfg), which the IP Phones load and apply.

As the network may also include IP Phones that are not deployed for the OVR solution, it is crucial that the OVR-related Configuration file be sent only to the IP Phones that are deployed for the OVR solution; otherwise, all the IP Phones will receive the same Configuration file and thus, all will connect to the OVR. To ensure that only IP Phones for the OVR receive the OVR-related configuration, the IP Phone Management Server allows you to employ multiple *regions* and *placeholders* in order to create Configuration files, based on configuration *templates*, specific to selected IP Phones. The procedure below describes how to do this, indicating the steps required only for deployments where all IP phones are for OVR, or for deployments where only certain IP Phones are for OVR.

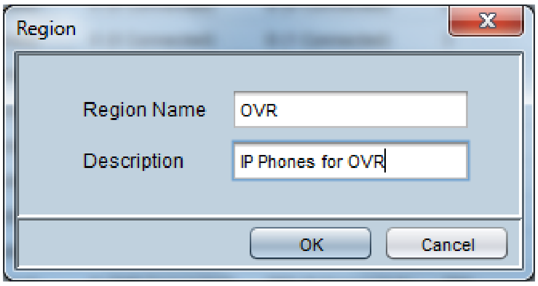
Note:

- This configuration is done before you initially connect the IP Phone to the network and power up.
- For detailed information on working with the IP Phone Management Server, refer to the document, *IP Phone Management Server Administrator's Manual*.

➢ **To configure the IP Phone through IP Phone Management Server:**

1. Log in to AudioCodes' EMS.
2. Add a Region to represent the IP Phones deployed in the OVR environment:
   a. In the MG tree, right-click the root (Globe), and then choose **Add Region**.
   b. Define a name for the Region (e.g., "OVR"):

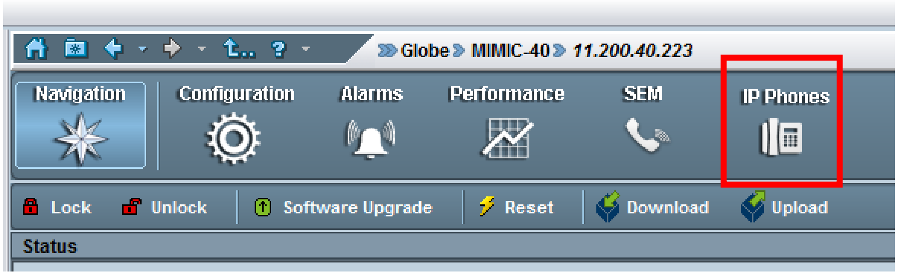
Figure 4-2: Configuring a Region for OVR in the EMS



   c. Click **OK**.

3. Access the IP Phone Management Server:
   a. On the EMS main screen toolbar, click the **IP Phones** button.

Figure 4-3: IP Phones Button for Accessing IP Phone Management Server



The Welcome to the IP Phone Management Server screen opens:

Figure 4-4: Welcome to the IP Phone Management Server

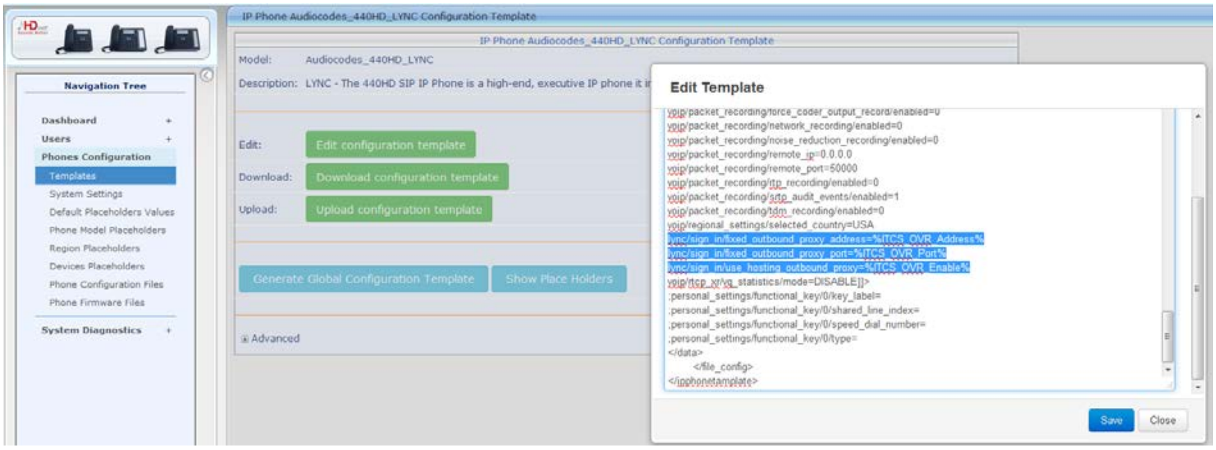
   b. Enter your username and password (default is **acladmin** and **pass_1234**, respectively), and then click **Login**.
4. Configure OVR-related parameters in the IP Phone template(s):
   a. Access the IP Phones Configuration Templates page (**Phones Configuration** > **Templates**).
   b. Select the required IP Phone model (e.g., AudioCodes 440HD LYNC); the Template page for the selected model opens.
   c. Click the **Edit configuration template** button; the Edit Template text box opens.

d. Copy and paste the following parameters into the text box under the "<user>" section, as shown highlighted in the figure below.

- **lync/sign_in/fixed_outbound_proxy_address=%ITCS_OVR_Address%**
- **lync/sign_in/fixed_outbound_proxy_port=%ITCS_OVR_Port%**
- **lync/sign_in/use_hosting_outbound_proxy=%ITCS_OVR_Enable%**

The values of the parameters are placeholders (shaded above). The placeholder names shown above are only used as an example; you can define them as desired (for syntax of placeholders, refer to the *IP Phone Management Server Administrator's Manual*). When you generate the Configuration file (see Step 8), the placeholders will be replaced by actual values (i.e., IP address, port number and proxy enabled). These values are configured in Step 6.

Figure 4-5: OVR Parameters Copied to Configuration Template of IP Phone Model



e. Click **Save**.

f. For additional IP Phone models, repeat Step 4.

5. Configure placeholders used in the template (see Step 4.d):

a. Access the Phone Model Placeholders page (**Phones Configuration** > **Phone Model Placeholders**).

b. From the 'Phone Model' drop-down list, select the required IP Phone model.

c. Click **Add new placeholder**, and then configure a placeholder.

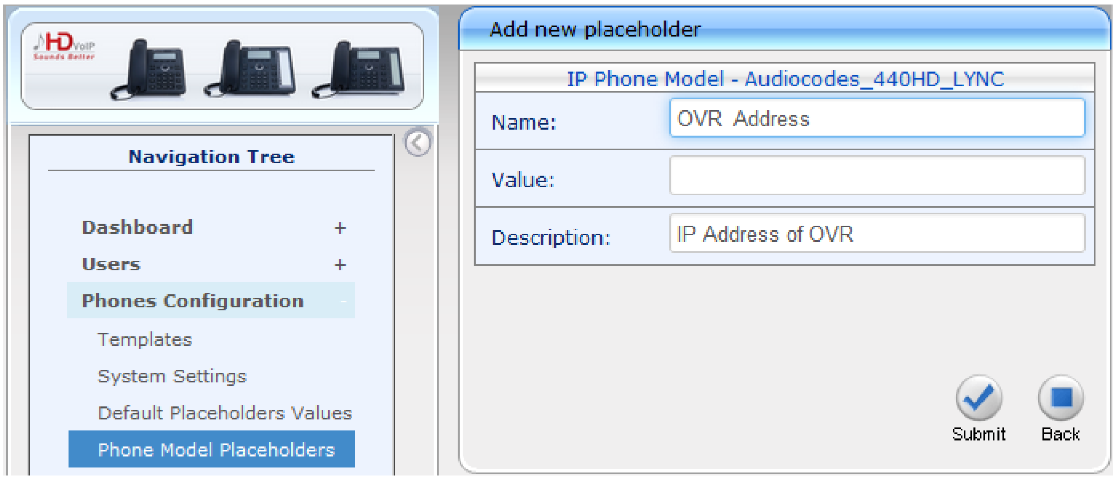
- **Only for Deployments where Certain IP Phones for OVR:**

Name	Value
OVR_Address	(empty)
OVR_Port	(empty)
OVR_Enable	0

- **Only for Deployments where All IP Phones for OVR:**

Name	Value
OVR_Address	10.15.45.112
OVR_Port	5071
OVR_Enable	1

Figure 4-6: Configuring Placeholders for OVR-related Parameters



d. Click **Submit**.

e. Repeat Step 5 to add all the placeholders.

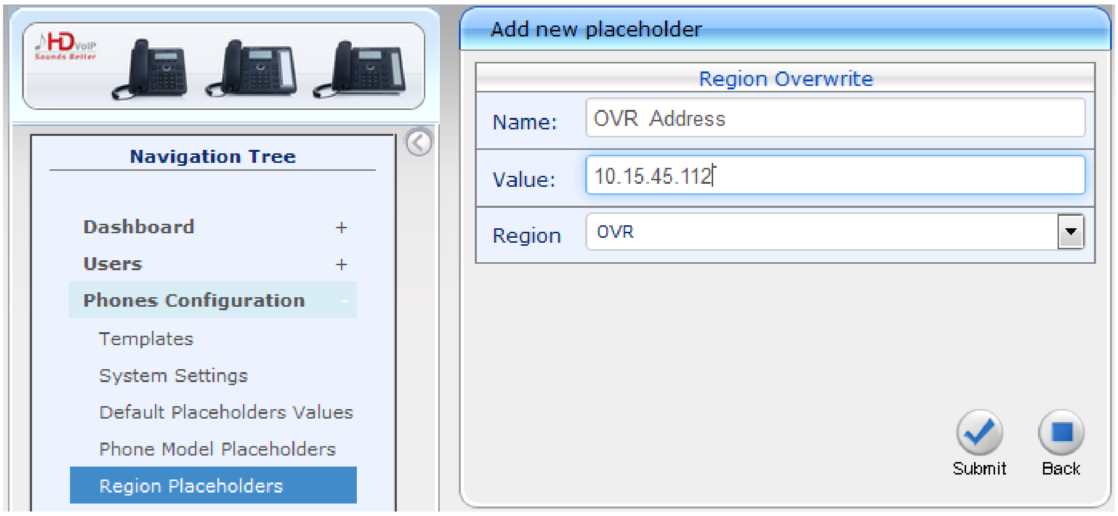
6. **(Only for Deployments where Certain IP Phones for OVR)** Assign the placeholders (configured in previous step) to the OVR region and configure their actual values for the IP Phones in the OVR environment. Do the following for each placeholder:

   a. Access the Manage Region Placeholders page (**Phones Configuration** > **Region Placeholders**).

   b. Click **Add new placeholder**, and then select the placeholder name, configure a value, and select the region. Assign the placeholders with the following settings:

Name	Value	Region
OVR_Address	10.15.45.112	OVR
OVR_Port	5071	OVR
OVR_Enable	1	OVR

Figure 4-7: Assigning Placeholders with Defined OVR Values to OVR Region

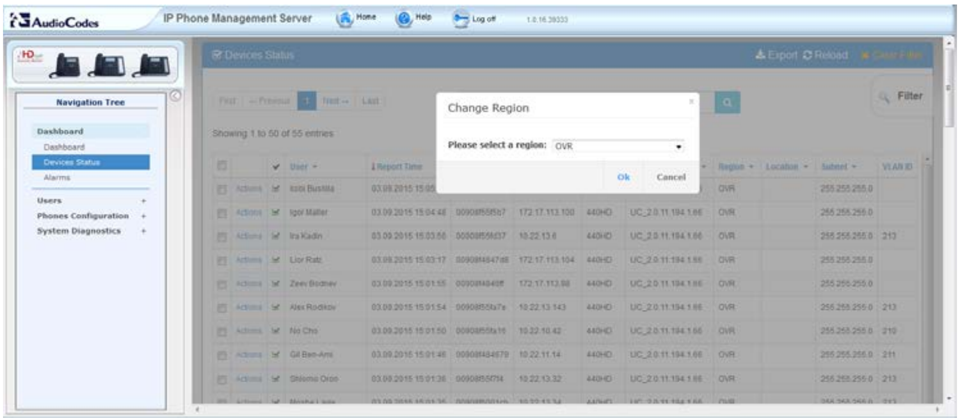


   c. Click **Submit**.

7. **(Only for Deployments where Certain IP Phones for OVR)** Assign IP Phone users to the OVR region. For each approved user, do the following:
   a. Access the Devices Status page (**Dashboard** > **Devices Status**).
   b. Click the **Actions** link corresponding to the desired user, and then from the pop-up menu, choose **Change Region**.
   c. From the drop-down list, select **OVR**, and then click **Ok**.

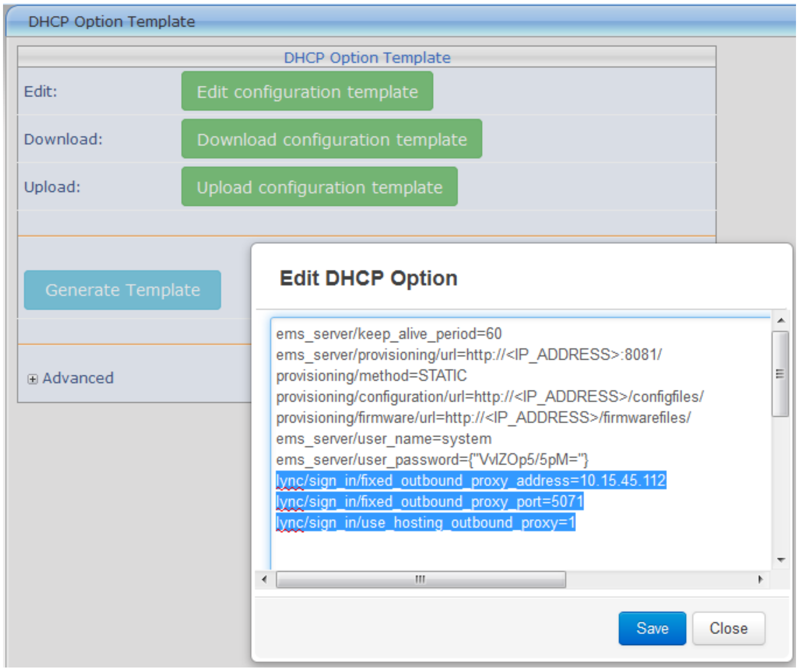
   If the user needs to be approved (i.e., **Approve** button appears alongside the user), skip steps b) and c), and click the **Approve** button to assign the region.

Figure 4-8: Assigning IP Phone Users to the OVR Region



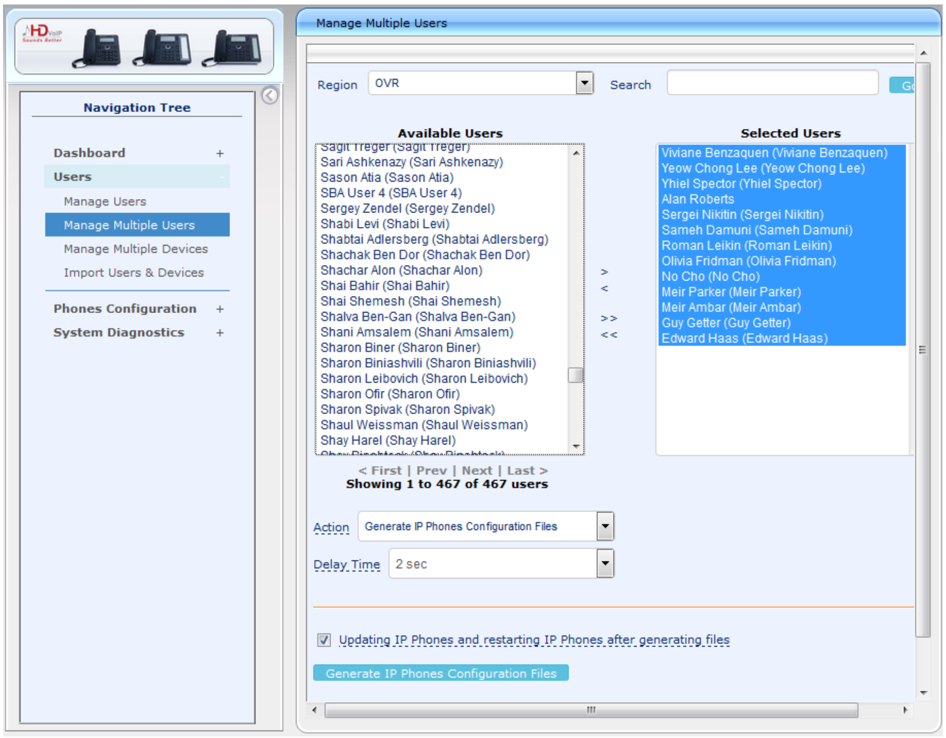
8. **(Only for Deployments where All IP Phones for OVR)** Configure default template for OVR:
   a. Access the System Settings page (**Phones Configuration** group > **System Settings** item), and then click the **DHCP Option Configuration** button; the DHCP Option Template page appears.
   b. Click the **Edit configuration template** button; the Edit DHCP Option pane opens.
   c. Copy and paste the configured parameters (Section 4.3) into the text box, as shown highlighted below:

Figure 4-9: Creating Configuration File Template for OVR



9. Generate the Configuration file for the users:
   a. Access the Manage Multiple Users page (**Dashboard** > **Manage Multiple Users**).
   b. From the 'Region' drop-down list, select **OVR**.
   c. In the Available Users pane, select the desired users and then add them to the Selected Users pane, using the arrow buttons.
   d. From the 'Action' drop-down list, select **Generate IP Phones Configuration Files**.
   e. Click the **Generate IP Phones Configuration Files** button.

Figure 4-10: Generating Configuration File for OVR Users



4.3.3 Configuring the IP Phones through TFPT/HTTP

You can use a third-party, TFTP/HTTP server to mass provision the IP Phones deployed with the OVR. The IP Phones "learn" of the address of the server through DHCP. The address can be configured on the DHCP server and sent to the IP Phones using DHCP Option 160 during the DHCP process (when the IP Phones are initially powered up). Once the IP Phones connect to the TFTP/HTTP server, the server sends the configuration over TFTP/HTTP as a Configuration file, which the IP Phones load and apply.

The Configuration file (.cfg) must be created with the required configuration and located on the TFTP/HTTP server. For more information on creating a Configuration file, refer to the document, *400HD Series IP Phone with Microsoft Lync Administrator's Manual*.

> **Note:** This configuration is done before you initially connect the IP Phone to the network and power up.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-10543