Configuration Note

AudioCodes One Voice for Skype For Business

One-Voice Resiliency with PSTN

for Microsoft™ Skype for Business Online

Version 7.2

audiocodes

Table of Contents

List of Figures

This page is intentionally left blank.

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. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: March-30-2020

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 website at https://www.audiocodes.com/services-support/maintenance-and-support.

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
10550	Initial release for Version 7.2.
10551	TLS assignment typos Cloud PBX; new section on SIP forking configuration.
10552	Update to provide support for the Mediant 800C platform.
10553	Update to Section ‘One-Voice Resiliency Constraints’.
10554	IP Phone Manager section updated to Device Manager.

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 website at https://online.audiocodes.com/documentation-feedback.

This page is intentionally left blank.

1 Introduction

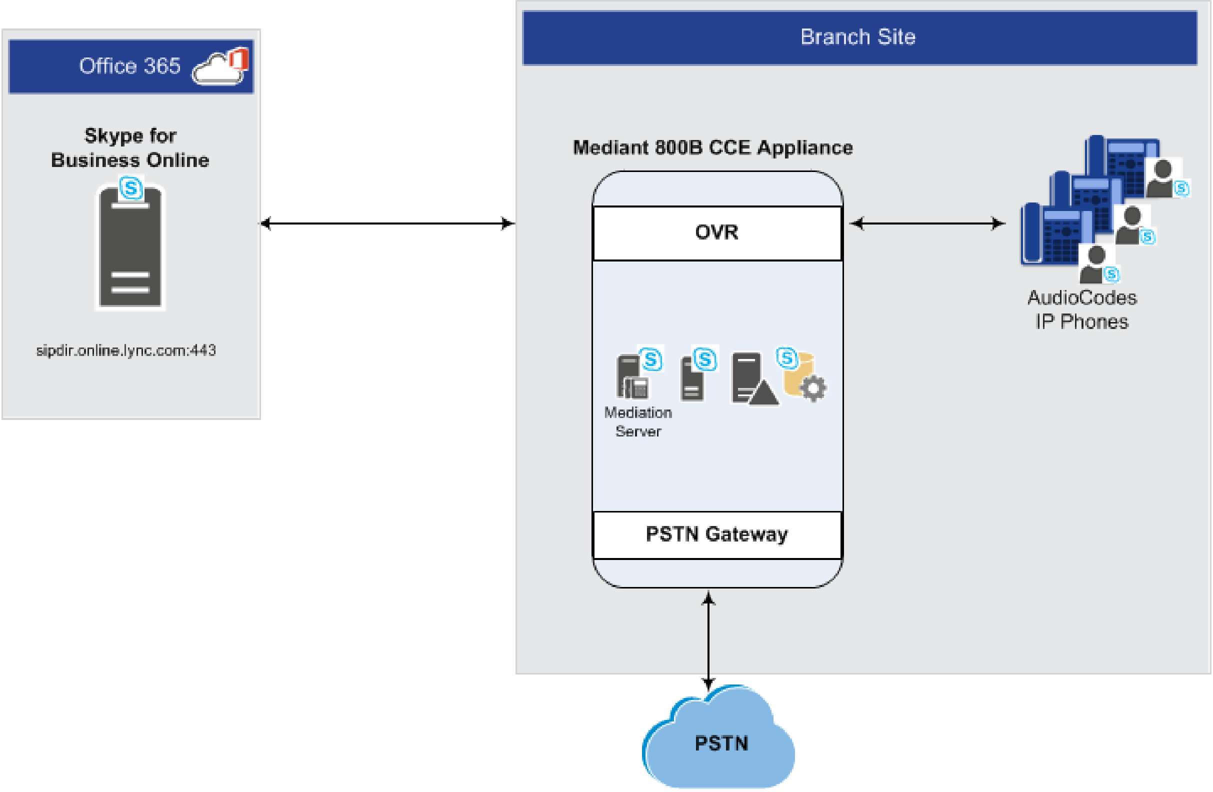
AudioCodes' One-Voice Resiliency (OVR) feature is a sophisticated and powerful VoIP application that runs on AudioCodes Mediant™ 800C and Mediant™ 800B devices, providing call survivability (branch-site resiliency) to AudioCodes IP Phone users at the branch site upon connectivity failure with the Office 365 Cloud PBX. The OVR solution is offered per branch site containing an AudioCodes Mediant device co-located with AudioCodes 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.

In addition to branch-site resiliency, the OVR solution can also provide optional Gateway (Enhanced Gateway) and SBC functionalities; inherit in AudioCodes Mediant 800C and Mediant 800B devices, servicing all users in the Skype for Business Online 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.

The OVR solution also operates with AudioCodes Mediant 800 Cloud Connector Edition (CCE) Appliance, which is used with the Skype for Business Cloud Connector Edition. The OVR solution also supports voice resiliency for Microsoft Cloud PBX (Skype for Business Online)..

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

Figure 1-1: Typical OVR Deployment


Office 365
Skype for Business Online
sipdir.online.lync.com:443
Branch Site
Mediant 800B CCE Appliance
OVR
Mediation Server
PSTN Gateway
AudioCodes IP Phones
PSTN

OVR is also supported by the Mediant 800C Gateway & SBC and Mediant 800B Gateway & SBC when it operates as a High-Availability (HA) system, in both Normal and Survivability (Limited Service) OVR modes. The only special configuration besides the usual HA and OVR configuration, is configuration for handling session expiry (see Section 3.11). For HA configuration, refer to the *Mediant 800 Gateway & SBC User's Manual.*

Notes:

- OVR is a license-based feature and is available only if it is included in the License Key installed on the device. For more information regarding pricing and usage with AudioCodes IP Phone series, contact your AudioCodes sales representative.
- OVR supports Lync and Skype for Business environments.
- In this document, where Skype for Business is mentioned, it also applies to Lync Server.
- In this document, Cloud PBX and Skype for Business Online are used interchangeably.

1.1 Compatible Software Versions

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

Table 1-1: Compatible Software Versions for OVR Solution

Device	Software Version
Mediant 800B Gateway & SBC	SIP_ 7.20A.150 or later
Mediant 800C Gateway & SBC	SIP_ 7.20A.202.112 or later
400HD Series IP Phones	UC_ 3.0.0.575.40 or later

1.2 One-Voice Resiliency Constraints

OVR currently includes the following constraints:

- Supports only AudioCodes IP Phones; all other phones (Skype for Business clients or vendor phones) are currently not supported.
- For security purposes, the OVR allows only IP Phone users who are currently registered with the Cloud PBX ("approved") to receive service during survivability mode.
- For the maximum number of branch site users supported by OVR, refer to the SBC-Gateway-MSBR Series Release Notes.
- OVR supports 3PIP with Microsoft Teams (only AudioCodes IP Phones).

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 passing calls between the IP Phone users at the branch site and the Skype for Business Online, which handles the call routing process (SIP INVITE messages). OVR either forwards the calls to Skype for Business Online.

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 Skype for Business at the Cloud PBX, 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 Cloud PBX is down.

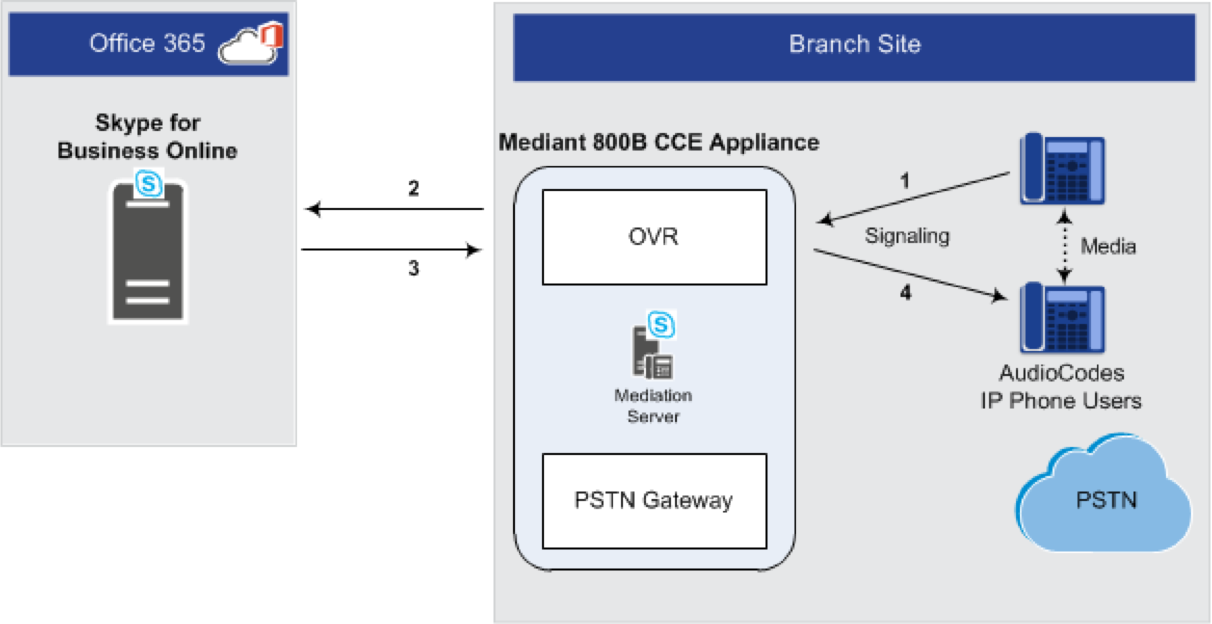
Direct media passes between the IP phones (media does not traverse OVR). When a call is escalated to the PSTN, in the current CCE version, the media from the IP Phone will pass through the Mediation server (in the next version of the CCE Appliance when Cloud PBX will support Media bypass, the media will flow between the local IP Phone and be directly terminated on the SBC/gateway.

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

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

  IP Phone → OVR → Cloud PBX → OVR → IP Phone

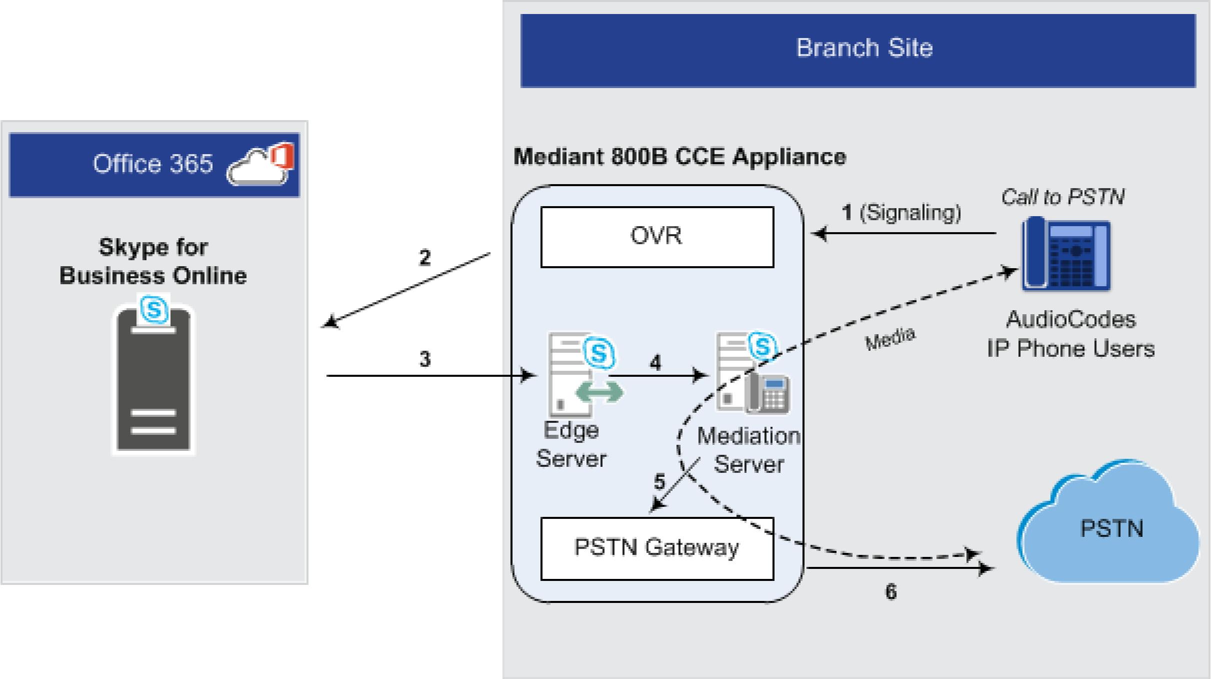
Figure 2-1: Normal Mode - Calls between IP Phones


Office 365
Skype for Business Online
2
3
Branch Site
Mediant 800B CCE Appliance
OVR
Mediation Server
PSTN Gateway
1
Signaling
4
Media
AudioCodes IP Phone Users
PSTN

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

  IP Phone → OVR → Cloud PBX → CCE Edge→CCE Mediation Server → PSTN Gateway → PSTN

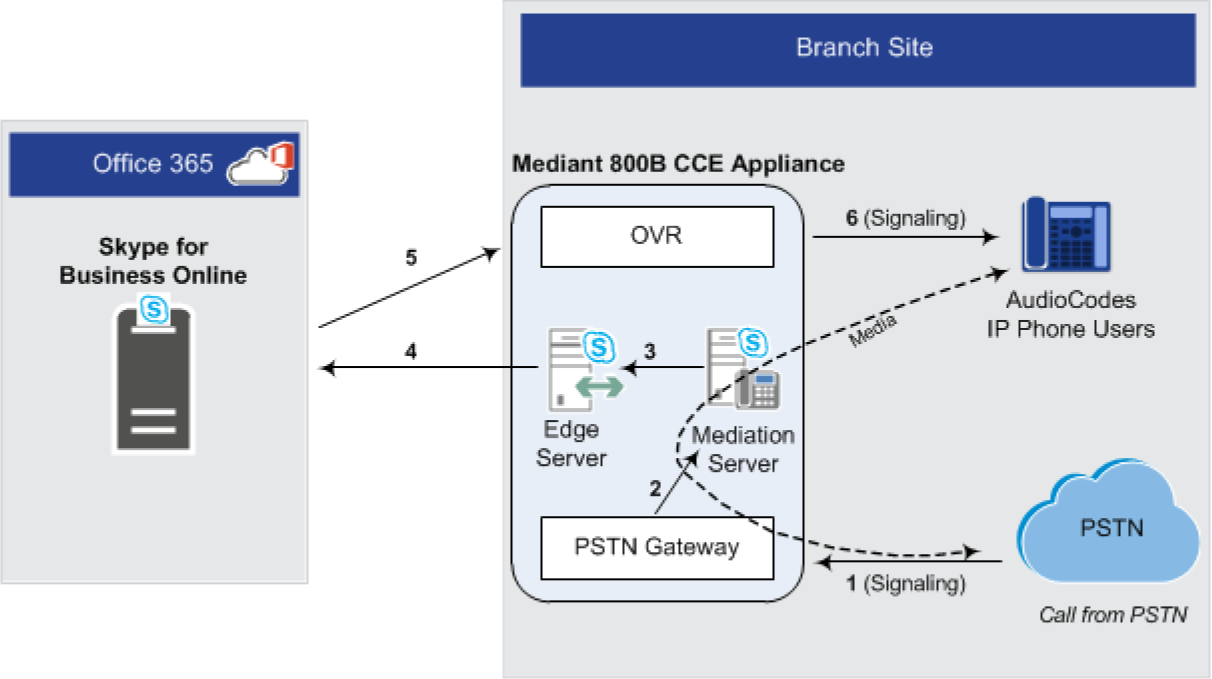
Figure 2-2: Normal Mode - Calls from IP Phone to PSTN



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

  PSTN → PSTN Gateway → CCE Mediation Server → CCE Edge → Cloud PBX → OVR → IP Phone

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



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

  PC client → Cloud PBX → OVR → IP Phone

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

  IP Phone → OVR → Cloud PBX → PC client

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

  PC client → Cloud PBX → CCE Mediation Server → PSTN Gateway → PSTN

2.2 Survivability Mode

OVR enters *survivability* mode of operation upon detection of connectivity loss with the Skype for Business online. In survivability mode, OVR provides 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 Skype for Business (e.g., presence) become unavailable. The OVR provides a mechanism to allow fast restoration of services, to the IP Phone users once connectivity to the Cloud PBX is restored. In addition, the OVR provides immediate but gradual registration mechanism, eliminating an "avalanche" or surge of user registrations on the Cloud PBX.

In survivability mode, the OVR maintains the connection and provides services only to users that have been authorized (registered) by the Cloud PBX. 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).

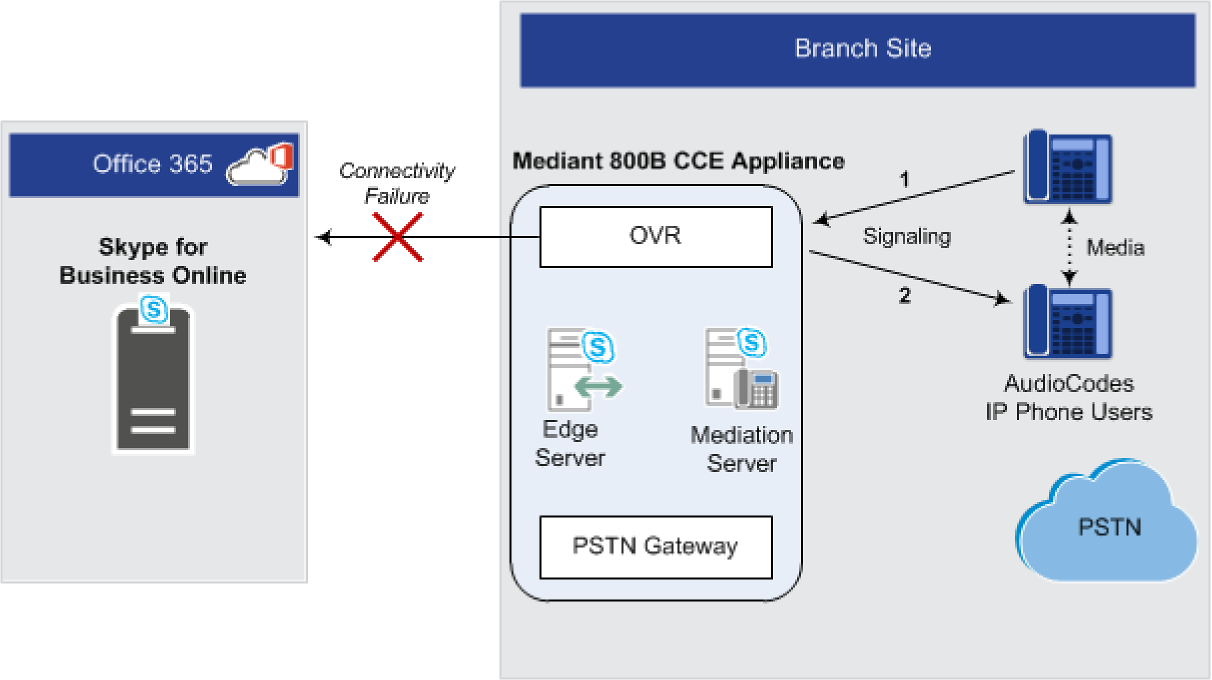
OVR handles call routing based on IP Phone user information that it accumulated during normal operation, as mentioned in Section 2.1. It identifies (classifies) incoming calls as received from IP Phone users based on the caller's IP address and routes the call to the destination based on the called telephone 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 Cloud PBX, currently active calls are maintained by the OVR (but may disconnect after a certain period of time).

When OVR detects that connectivity with the Cloud PBX has been restored, it exits survivability mode and begins normal operation mode, forwarding calls transparently between the IP Phones and the Cloud PBX. Full unified communication features provided by 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:

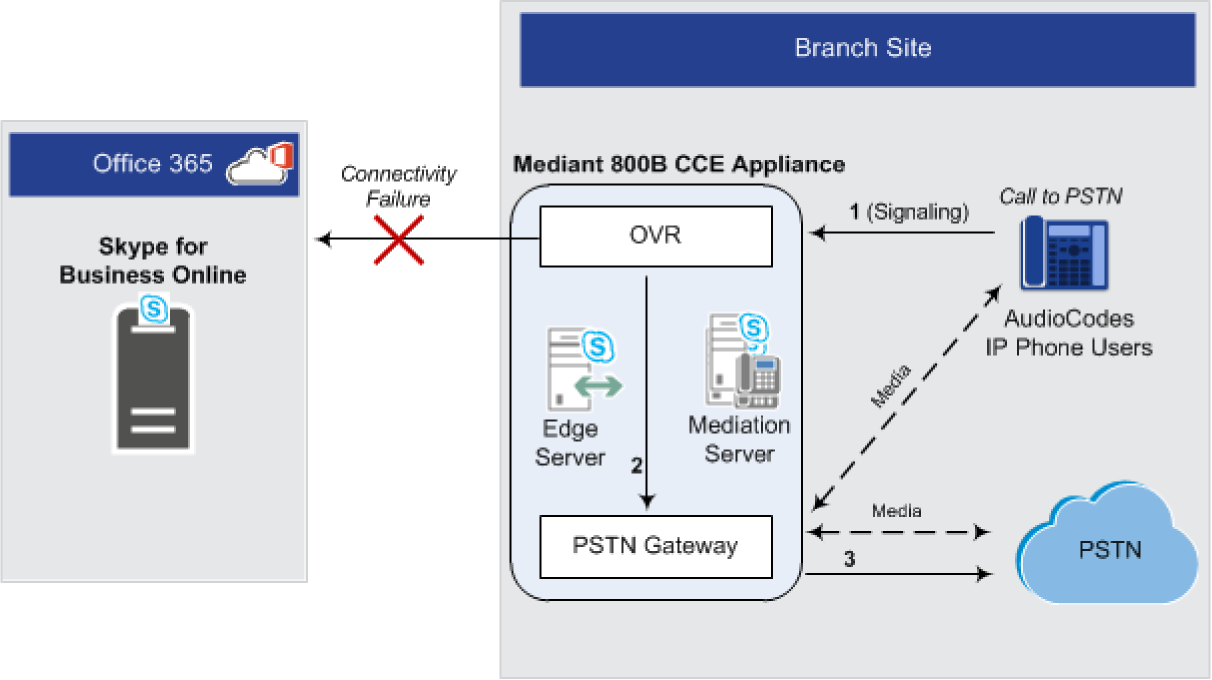
- **IP Phone-to-IP Phone Calls:** IP Phone → OVR → IP Phone

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



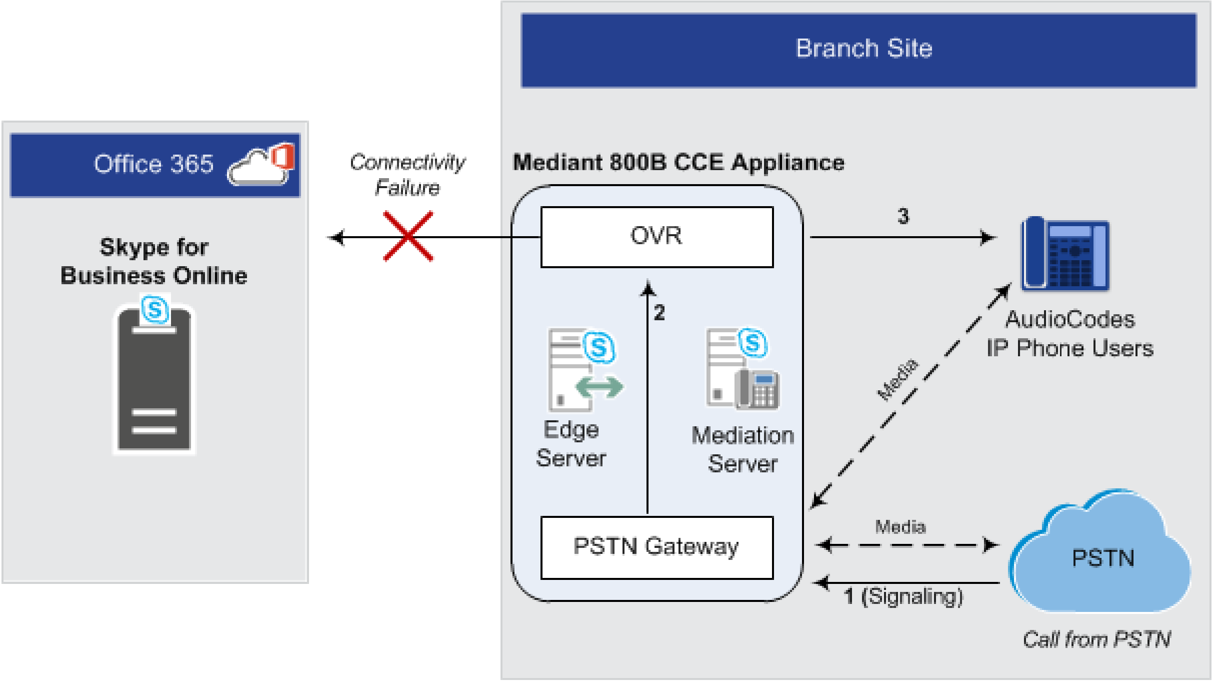
- **IP Phone-to-PSTN Calls:** IP Phone → OVR → PSTN Gateway → PSTN

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



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

Figure 2-6: Survivability Mode - Calls from PSTN to IP Phone

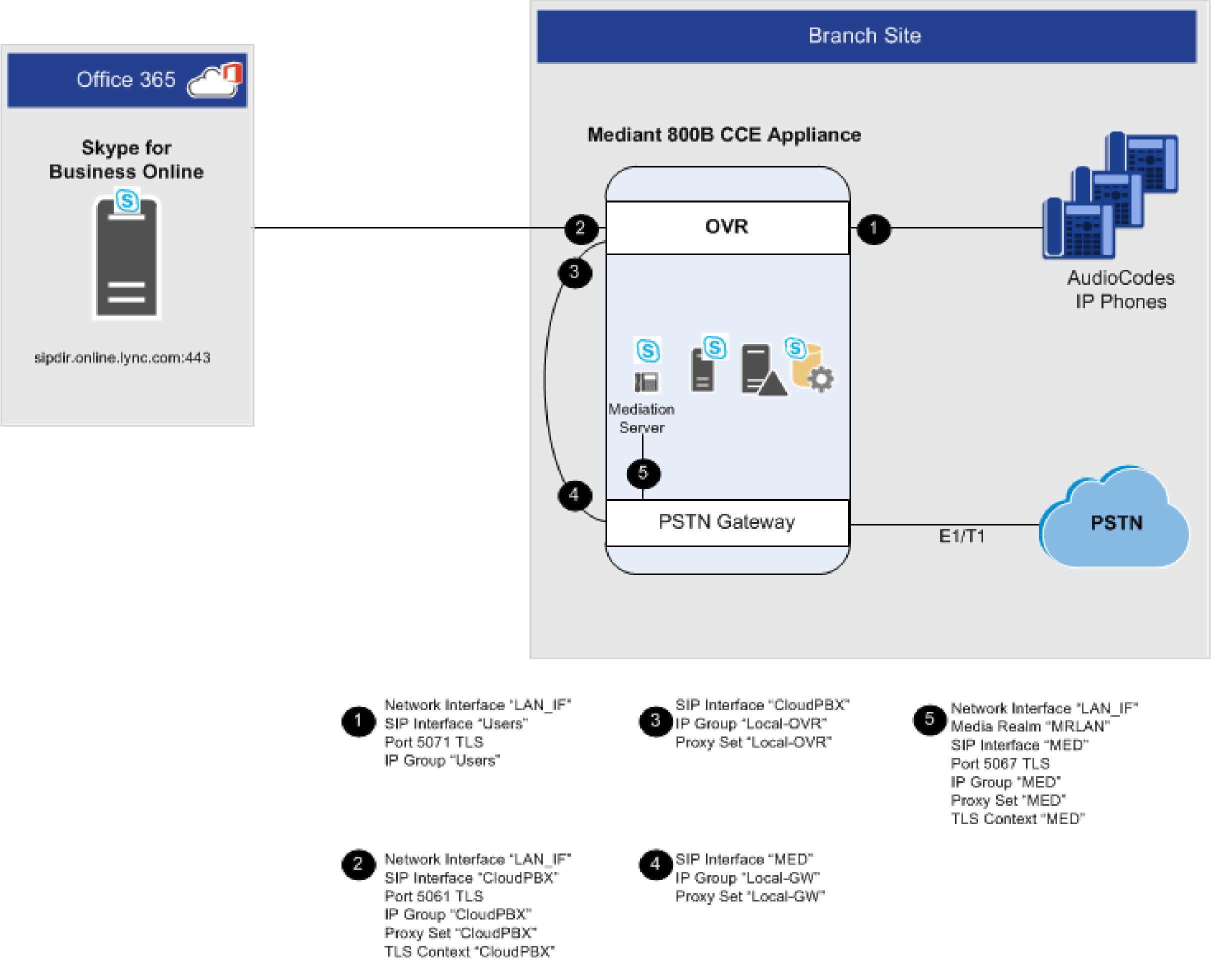


This page is intentionally left blank.

3 Configuring the Device for OVR

This chapter provides step-by-step instructions on how to configure AudioCodes' Mediant 800C Gateway & E-SBC or Mediant 800B Gateway & E-SBC for OVR. It is based on the following example network topology:

Figure 3-1: OVR Example Topology and Configuration Entities



1 Network Interface "LAN_IF"
SIP Interface "Users"
Port 5071 TLS
IP Group "Users"

2 Network Interface "LAN_IF"
SIP Interface "CloudPBX"
Port 5061 TLS
IP Group "CloudPBX"
Proxy Set "CloudPBX"
TLS Context "CloudPBX"

3 SIP Interface "CloudPBX"
IP Group "Local-OVR"
Proxy Set "Local-OVR"

4 SIP Interface "MED"
IP Group "Local-GW"
Proxy Set "Local-GW"

5 Network Interface "LAN_IF"
Media Realm "MRLAN"
SIP Interface "MED"
Port 5067 TLS
IP Group "MED"
Proxy Set "MED"
TLS Context "MED"

Note:

- 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).

<table>
<tr><th>Configuration Entity</th><th colspan="4">Configuration Requirement</th></tr>
<tr><td><b>TLS Context</b></td><td colspan="4">TLS certification (TLS Context) is required for the following:
▪ Traffic between OVR and CCE Mediation Server. This TLS configuration uses the default TLS Context (ID 0).
▪ Traffic between OVR and Cloud PBX. This TLS configuration uses TLS Context ID 1.</td></tr>
<tr><td><b>Media Realm</b></td><td colspan="4">A single Media Realm for media traffic is used with a port range of 6000-65520 on the network interface.</td></tr>
<tr><td><b>SIP Interface</b></td><td colspan="4">SIP Interfaces need to be configured for the following:
▪ <b>CCE Mediation Server ("MED"):</b> Interfaces with CCE Mediation Server.
▪ <b>Cloud PBX ("CloudPBX"):</b> Interfaces with the Cloud PBX (port 5061). A TLS Context (TLS certificate) must be associated with the interface.
▪ <b>Skype users ("Users"):</b> Interfaces with Skype users (IP Phones) at branch site (port 5071).</td></tr>
<tr><td><b>Proxy Set</b></td><td colspan="4">Proxy Sets need to be configured for the following:
▪ <b>CCE Mediation Server ("MED"):</b> Address and port of the CCE Mediation Server. The address can be an FQDN that is resolved into several IP addresses.
▪ <b>Cloud PBX ("CloudPBX"):</b> Address and port of the CloudPBX (only a single IP address).
▪ <b>Local Gateway ("Local-GW"):</b> Internal device leg entity that represents the Gateway leg.</td></tr>
<tr><td><b>IP Group</b></td><td colspan="4">IP Groups need to be configured for the following:
▪ <b>CCE Mediation Server ("MED"):</b> Server-type IP Group for the CCE Mediation Server. A typical IP Profile for interoperating with Skype must be associated. The IP Group's mode of operation must be set to default.
▪ <b>Cloud PBX ("CloudPBX"):</b> Server-type IP Group for the CloudPBX. The IP Group's mode of operation must be set to <b>Microsoft Server</b>. It is recommended not associate an IP Profile.
▪ <b>Skype users ("Users"):</b> User-type IP Group for Skype users (IP Phones). The IP Group's mode of operation must be set to <b>Microsoft Server</b>. For HA device, an IP Profile must be associated.
▪ <b>Local Gateway ("Local-GW"):</b> Internal device leg entity that represents the Gateway leg.</td></tr>
<tr><td><b>Classification Rule</b></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"><b>SBC IP-to-IP Routing Rule</b></td><td><b>Rule</b></td><td><b>Call Scenario</b></td><td><b>From (Source)</b></td><td><b>To (Destination)</b></td></tr>
<tr><td>0</td><td>Calls from users to Cloud PBX.</td><td>Users</td><td>Cloud PBX</td></tr>
<tr><td>1</td><td>Calls between users if unable to route to Cloud PBX (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 Cloud PBX (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 Cloud PBX to users.</td><td>Cloud PBX</td><td>Users</td></tr>
<tr><td>4</td><td>Calls from PSTN to users</td><td>Local-GW</td><td>Users</td></tr>
</table>

Configuration Entity	Configuration Requirement			
Tel-to-IP Routing Rule	**Rule**	**Call Scenario**	**From**	**To**
	0	Calls from the PSTN to users when unable to route to CCE Mediation Server (alternative route for default proxy).	GW Trunk	OVR
IP-to-Tel Routing Rule	**Rule**	**Call Scenario**	**From**	**To**
	0	Calls to the PSTN.	any	Gateway Trunk

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 logical IP network interfaces:**

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Select the OAMP interface row, click **Edit**, and then change the IP network interface as shown below:

Parameter	Value
General	
Index	**0**
Name	**Voice**
Application Type	**OAMP + Media + Control**
DNS	
Primary DNS	**10.15.25.1**
IP Address	
Interface Mode	**IPv4 Manual**
IP Address	**10.15.45.112**
Prefix Length	**16**
Default Gateway	**10.15.0.1**

3. Click **Apply**.
4. Connect to the device's Web interface using this new OAMP address.

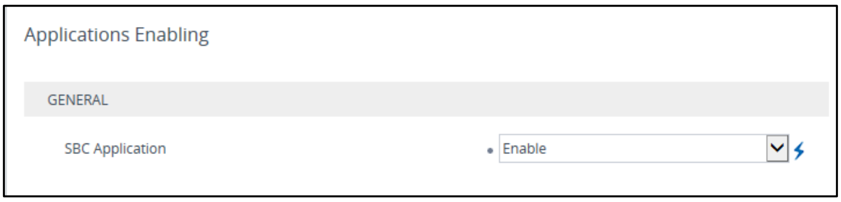
3.2 Step 2: Enable the SBC Application

For OVR functionality, you must enable the SBC application.

➢ **To enable the SBC application:**

1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).
2. From the 'SBC Application' drop-down list, select **Enable**:

Figure 3-2: Enabling SBC Application



Applications Enabling

GENERAL

SBC Application • Enable

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

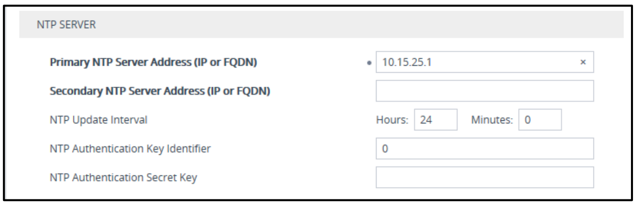
3.3 Step 3: Configure an NTP Server

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 (**Setup** menu > **Administration** tab > **Time & Date**).
2. Under the NTP Server group, in the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.25.1**):

Figure 3-3: Configuring NTP Server Address



NTP SERVER

Primary NTP Server Address (IP or FQDN)	• 10.15.25.1 ×
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

3. Click **Apply**.

3.4 Step 4: Configure TLS for CCE Mediation Server

TLS certificate negotiation occurs between the device and CCE Mediation Server.

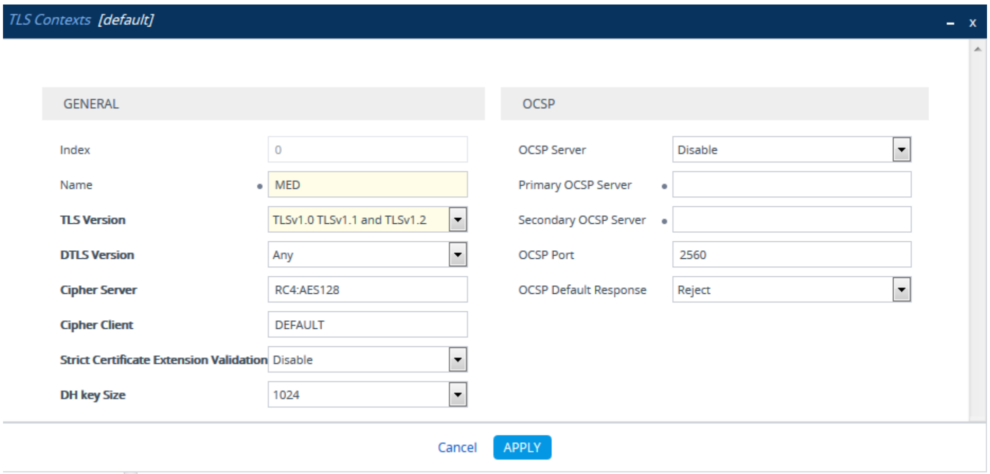
3.4.1 Enable TLS

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 table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Select the required TLS Context row (typically, the default index 0), and then click **Edit**.
3. In the 'Name' field, rename the TLS Context to "MED".
4. From the 'TLS Version' drop-down list, select **TLSv1.0 TLSv1.1 and TLSv1.2**:

Figure 3-4: Configuring TLS Version



TLS Contexts *[default]*

GENERAL

Index: 0
Name: MED
TLS Version: TLSv1.0 TLSv1.1 and TLSv1.2
DTLS Version: Any
Cipher Server: RC4:AES128
Cipher Client: DEFAULT
Strict Certificate Extension Validation: Disable
DH key Size: 1024

OCSP

OCSP Server: Disable
Primary OCSP Server:
Secondary OCSP Server:
OCSP Port: 2560
OCSP Default Response: Reject

5. Click **Apply.**

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:

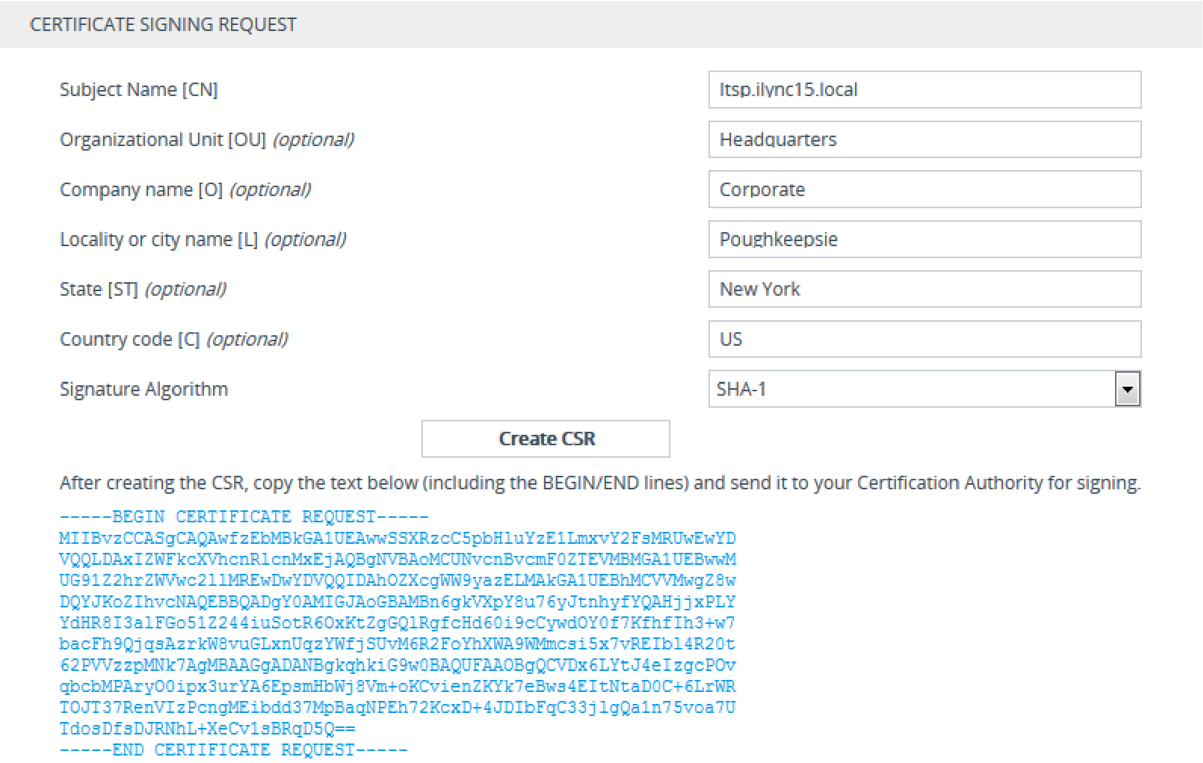
1. Generating a Certificate Signing Request (CSR).
2. Requesting Device Certificate from CA.
3. Obtaining Trusted Root Certificate from CA.
4. Deploying Device and Trusted Root Certificates on E-SBC.

➢ **To configure a certificate:**

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Select the TLS Context at index 0, and then click the **Change Certificate** link located at the bottom of the 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., **ltsp.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 3-5: Certificate Signing Request – Creating CSR



CERTIFICATE SIGNING REQUEST

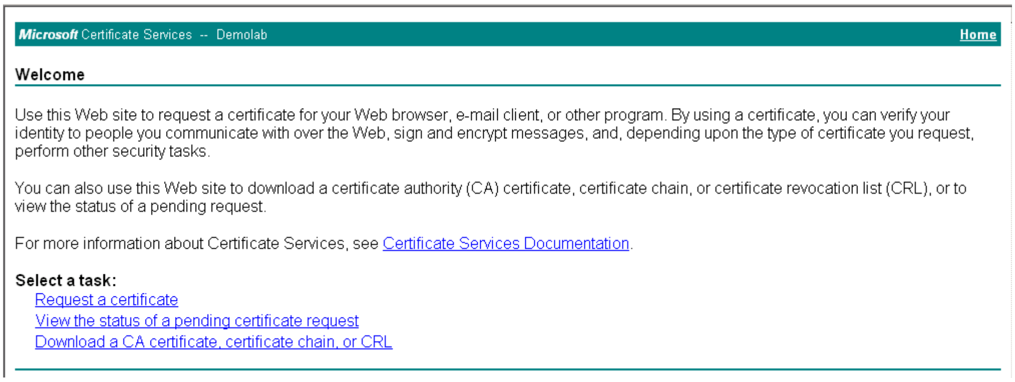
Subject Name [CN]	ltsp.ilync15.local
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US
Signature Algorithm	SHA-1

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-----
MIIBvzCCASgCAQAwfzEbMBkGA1UEAwwSSXRzcC5pbHluYzE1LmxvY2FsMRUwEwYD
VQQLDAxIZWFkcXVhcnRlcnMxEjAQBgNVBAoMCUNvcnBvcmF0ZTEVMBMGA1UEBwwM
UG91Z2hrZWVwc2llMREwDwYDVQQIDAhOZXcgWW9yazELMAkGA1UEBhMCVVMwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMBn6gkVXpY8u76yJtnhyfYQAHjjxPLY
YdHR8I3alFGo51Z244iuSotR6OxKtZgGQlRgfcHd60i9cCywdOY0f7KfhfIh3+w7
bacFh9QjqsAzrkW8vuGLxnUqzYWfjSUvM6R2FoYhXWA9WMmcsi5x7vREIbl4R20t
62PVVzzpMNk7AgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQCVDx6LYtJ4eIzgcPOv
qbcbMPAryO0ipx3urYA6EpsmHbWj8Vm+oKCvienZKYk7eBws4EItNtaD0C+6LrWR
TOJT37RenVIzPcngMEibdd37MpBaqNPEh72KcxD+4JDIbFqC33jlgQa1n75voa7U
TdosDfsDJRNhL+XeCv1sBRqD5Q==
-----END CERTIFICATE REQUEST-----
```

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 website at http://<certificate server>/CertSrv.

Figure 3-6: Microsoft Certificate Services Web Page



Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

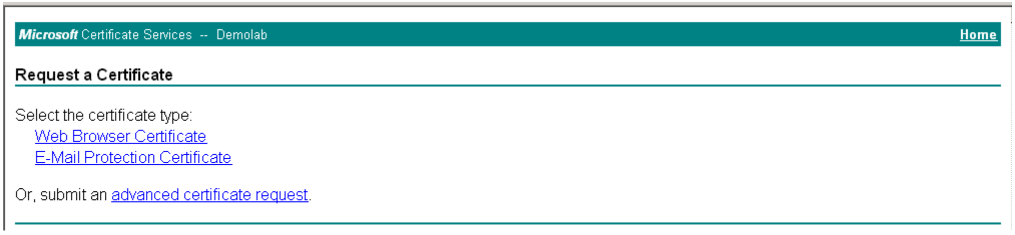
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

7. Click **Request a certificate**.

Figure 3-7: Microsoft Certificate Services - Request a Certificate Page



Microsoft Certificate Services -- Demolab

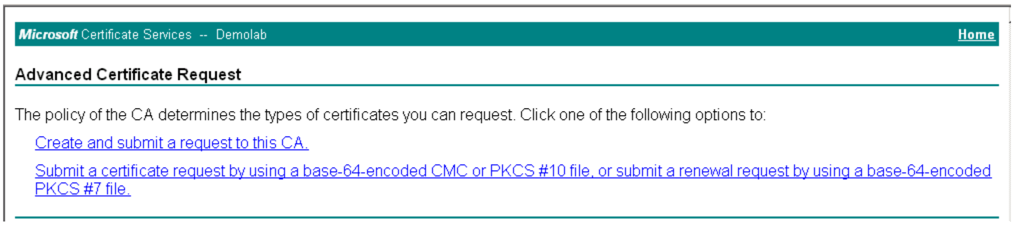
Request a Certificate

Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate

Or, submit an advanced certificate request.

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

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



Microsoft Certificate Services -- Demolab

Advanced Certificate Request

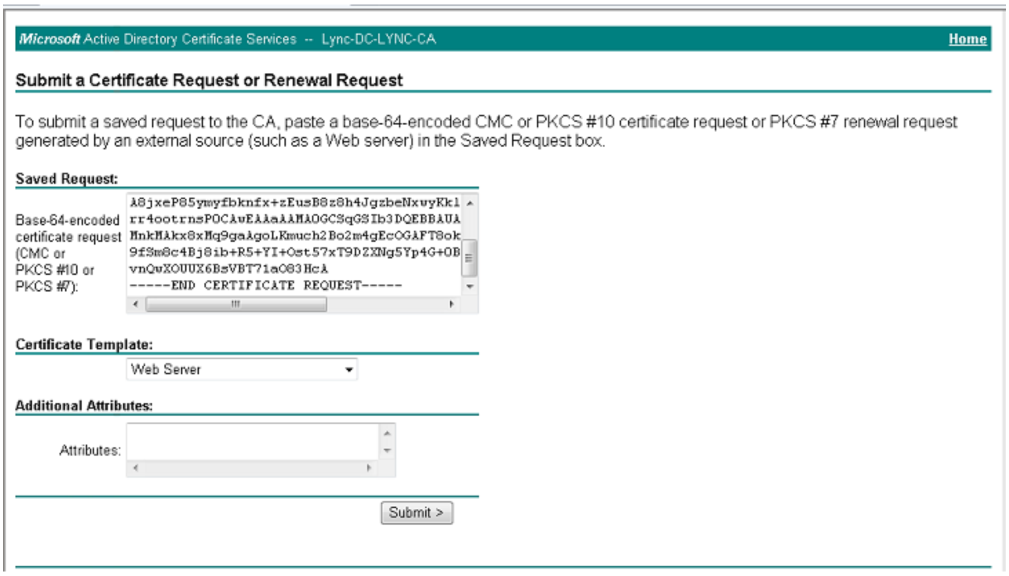
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

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

Figure 3-9: Microsoft Active Directory Certificate Services - Submit a Certificate Request or Renewal Request Page



Microsoft Active Directory Certificate Services -- Lync-DC-LYNC-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
A8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxuyKkl
rr4ootrnsPOCAvEAAaAAMAOGCSqGSIb3DQEBBAUA
MnkMAkx8xMq9gaAgoLKmuch2Bo2m4gEcOGAFT8ok
9fSm8c4Bj8ib+R5+YI+Ost57xT9DZXNg5Yp4G+OB
vnQvXOUUX6BsVBT71aO83HcA
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

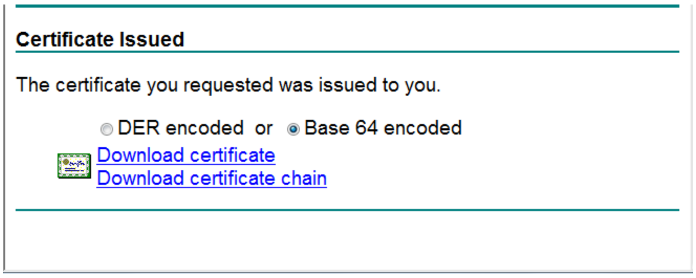
Web Server

Additional Attributes:

Attributes:

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 3-10: Certificate Issued Page



Certificate Issued

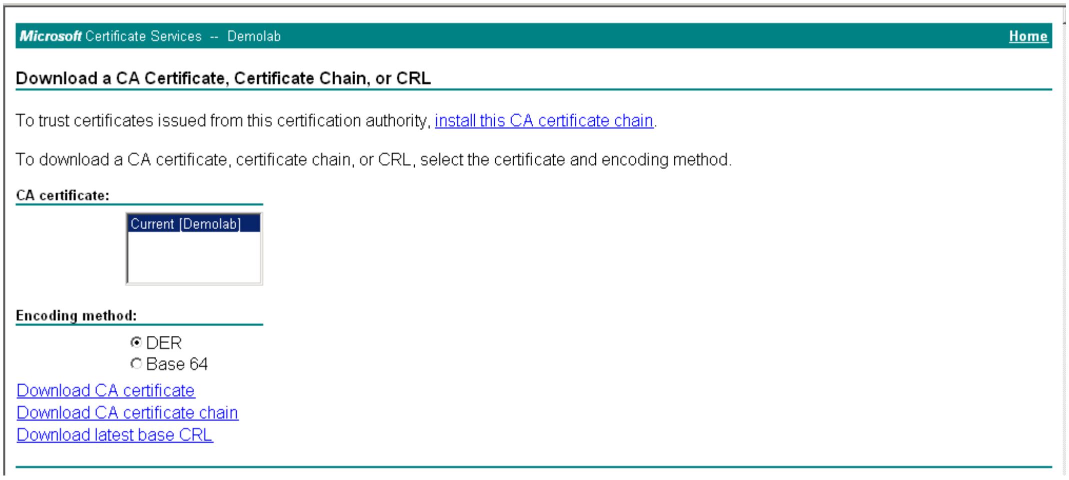
The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

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 3-11: Microsoft Certificate Services - Download a CA Certificate, Certificate Chain, or CRL Page



Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Demolab]

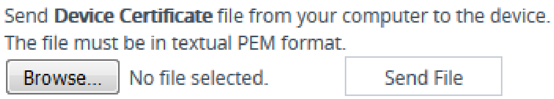
Encoding method:

● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL

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, open the TLS Contexts table and do the following:
    a. Select TLS Context at index 0, and then click the **Change Certificate** link 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:

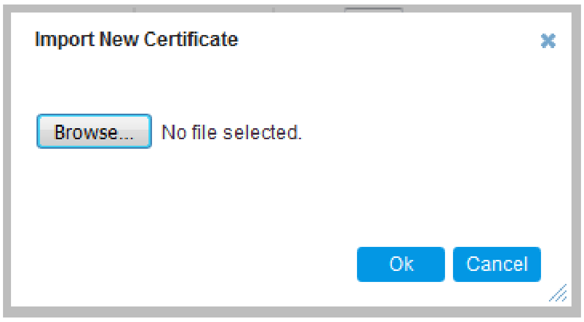
Figure 3-12: Upload Device Certificate Files from your Computer Group



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

    c. In the TLS Contexts table, select TLS Context at index 0, and then click the **Trusted Root Certificates** link 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 3-13: Importing Root Certificate into Trusted Certificates Store



Import New Certificate

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.

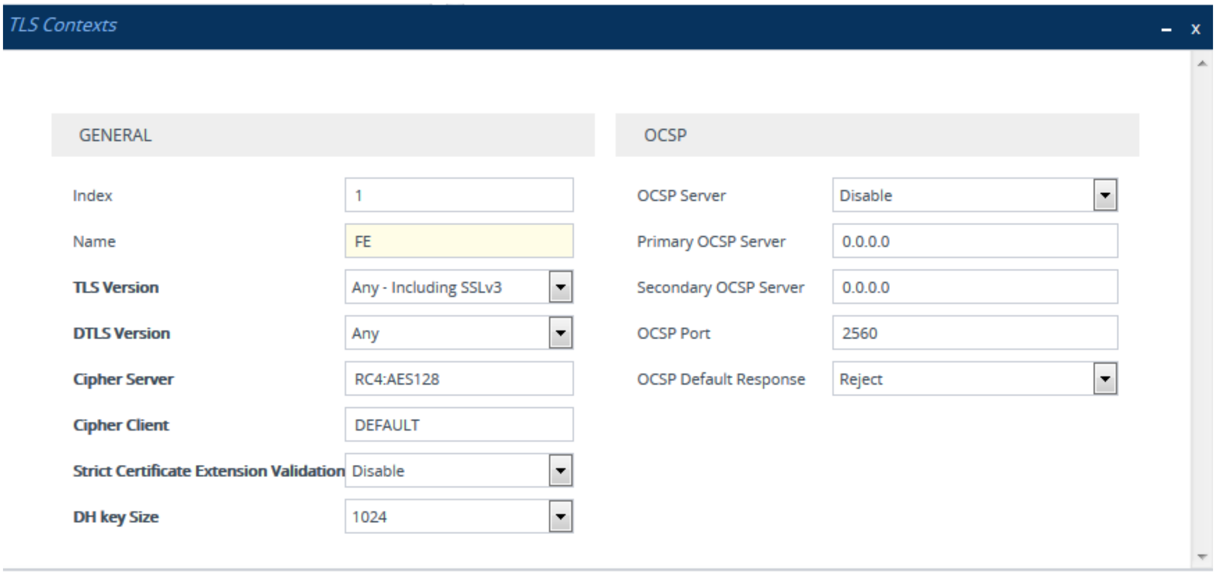
3.5 Step 5: Configure TLS for Cloud PBX

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

➢ **To configure TLS for Cloud PBX:**

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Click **New**, and then in the dialog box, configure the TLS Context as shown below:

Figure 3-14: Configuring TLS Context for Cloud PBX



GENERAL

Index	1
Name	FE
TLS Version	Any - Including SSLv3
DTLS Version	Any
Cipher Server	RC4:AES128
Cipher Client	DEFAULT
Strict Certificate Extension Validation	Disable
DH key Size	1024

OCSP

OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

3. Click **Apply**.

3.6 Step 6: Configure SRTP

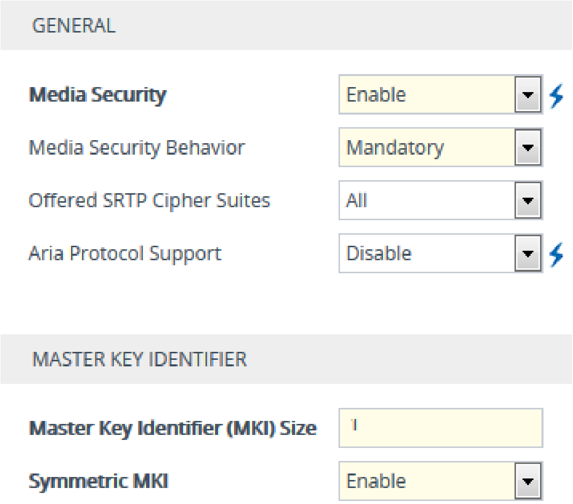
As CCE Mediation Server employs SRTP, you need to configure the device to also operate in the same manner.

➢ **To configure media security:**

1. Open the Media Security page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Security**).
2. Configure as follows:

Parameter	Value	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.
Master Key Identifier (MKI) Size	**1**	-
Symmetric MKI	**Enable**	-

Figure 3-15: Configuring SRTP



GENERAL

Media Security: Enable

Media Security Behavior: Mandatory

Offered SRTP Cipher Suites: All

Aria Protocol Support: Disable

MASTER KEY IDENTIFIER

Master Key Identifier (MKI) Size: 1

Symmetric MKI: Enable

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

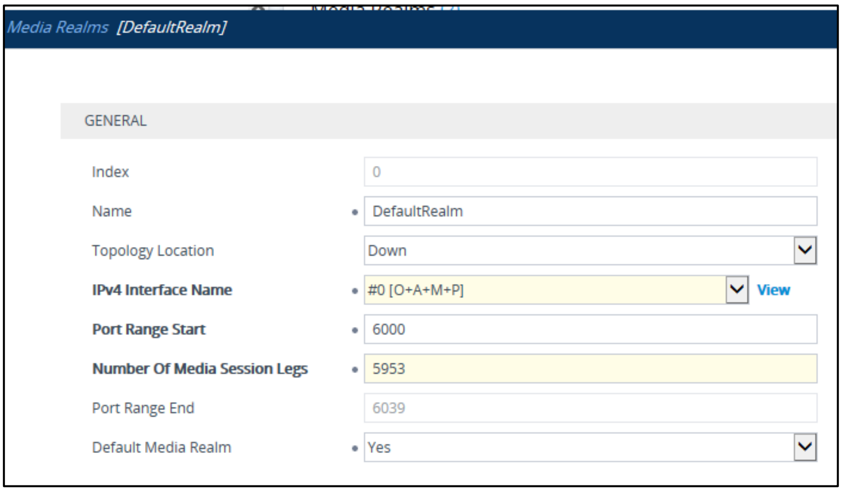
3.7 Step 7: Configure a Media Realm

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 Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Select the default Media Realm (Index 0), and then click **Edit**.
3. Modify the Media Realm according to your deployment:

Figure 3-16: Configuring a Media Realm



Media Realms [DefaultRealm]

GENERAL

Index	0
Name	• DefaultRealm
Topology Location	Down
IPv4 Interface Name	• #0 [O+A+M+P] View
Port Range Start	• 6000
Number Of Media Session Legs	• 5953
Port Range End	6039
Default Media Realm	• Yes

4. Click **Apply**.

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:

- CCE Mediation Server
- Cloud PBX
- Skype users (IP Phones) at branch site

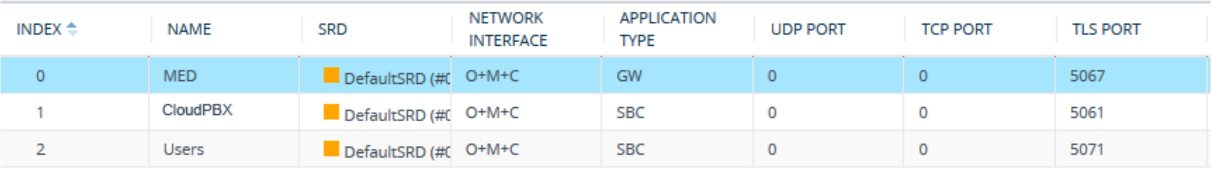
➢ To add SIP Interfaces:

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Click **New**, and then in the 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 CCE Mediation Server	**MED**	**GW**	**5067**	**MED**
Interfacing with Cloud PBX	**CloudPBX**	**SBC**	**5061**	**FE**
Interfacing with IP Phone users	**Users**	**SBC**	**5071**	**MED**

3. Click **Apply**. The figure below displays the configured SIP Interfaces:

Figure 3-17: Configured SIP Interfaces



INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT
0	MED	🟧 DefaultSRD (#0	O+M+C	GW	0	0	5067
1	CloudPBX	🟧 DefaultSRD (#0	O+M+C	SBC	0	0	5061
2	Users	🟧 DefaultSRD (#0	O+M+C	SBC	0	0	5071

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:

- CCE Mediation Server
- Cloud PBX
- Entity to reach the local PSTN Gateway

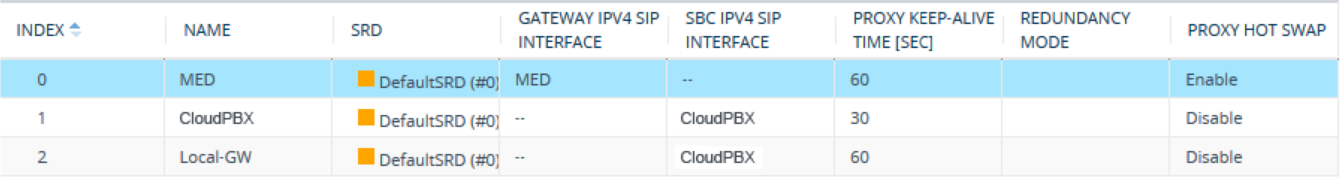
➢ To add Proxy Sets:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Click **New**, and then in the 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**
CCE Mediation Server	**MED**	**MED**	-	**Using OPTIONS**	**60**	**MED**	**Round Robin**	**Enable**
Cloud PBX	**CloudPBX**	-	**CloudPBX**	**Using OPTIONS**	**30**	**FE**	Round Robin	-
Entity to reach local PSTN Gateway	**Local-GW**	-	**CloudPBX**	-	-	-	-	-

The figure below displays the configured Proxy Sets:

Figure 3-18: 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	--	60		Enable
1	CloudPBX	🟧 DefaultSRD (#0)	--	CloudPBX	30		Disable
2	Local-GW	🟧 DefaultSRD (#0)	--	CloudPBX	60		Disable

3. Configure addresses per Proxy Set. For each Proxy Set, do the following:
   a. Select the Proxy Set row, and then click the **Proxy Address** link located below the table; the Proxy Address table appears.
   b. Click **New** and then in the dialog box, configure the address and transport protocol.

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

Proxy Set	Configuration	
	Proxy Address	Transport Type
MED	**med.ilync15.local:5067**	**TLS**
CloudPBX	**sipdir.online.lync.com:443**	**TLS**
Local-GW	**10.15.45.112:5067**	**TLS**

3.10 Step 10: Configure a Proxy Set for CCE Mediation Server

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

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

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

1. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** > **Proxy & Registration**), and then from the 'Use Default Proxy' drop-down list, select **Use Proxy**:

Figure 3-19: Configuring CCE Mediation Server as Proxy for PSTN Gateway

Use Default Proxy: Use Proxy

   This enables CCE Mediation Server to act as a proxy server for the PSTN Gateway.

2. Click **Apply**.
3. Open the Routing Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **Routing Settings**), and then from the 'Redundant Routing Mode' drop-down list, select **Routing Table**:

Figure 3-20: Configuring Redundant Routing Mode

Redundant Routing Mode: Routing Table

   If the CCE 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 3.20.6) 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.

4. Click **Apply**.

3.11 Step 11: Configure IP Profiles

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, you need to add IP Profiles for the following.

- CCE Mediation Server
- Skype users (IP Phones) at branch site: This IP Profile is **only required** when the device operates as an HA system. The configuration determines the device's handling of the SIP session expiry (Session-Expires header) for the IP Phones. The special configuration avoids scenarios where calls are "stuck" (never released by receiving BYE from phone or Microsoft server) for phones that were in a call before an HA switchover and that fail to register after the switchover. In such cases, the device disconnects the call.

➢ **To add an IP Profile:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then in the dialog box, add an IP Profile. In the example setup, add IP Profiles with the following configuration:

Index	Name	Reset SRTP Upon Re-key	Symmetric MKI	MKI Size	Generate SRTP Keys Mode	Gateway Media Security Mode	Early Media	Early 183	Session Expires Mode
	MED	Enable	Enable	1	Always	Mandatory	Enable	Enable	-
	Users	-	-	-	-	-	-	-	Observe

3. Click **Apply**.

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:

- CCE Mediation Server
- Cloud PBX
- Skype users (IP Phones) at branch site
- Local Gateway

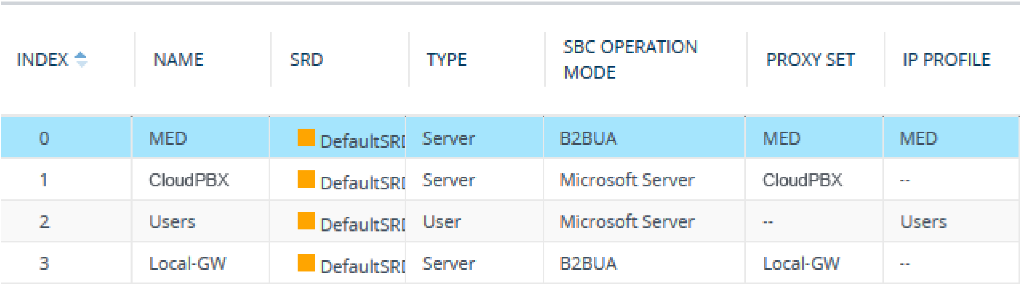
➢ To configure IP Groups:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Click **New**, and then in the 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**
CCE Mediation Server	**MED**	**Server**	**MED**	**MED**	**B2BUA**	-
Cloud PBX	**CloudPBX**	**Server**	**CloudPBX**	-	**Microsoft Server**	-
Users	**Users**	**User**	-	Users	**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 3-21: Configured IP Groups



INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE
0	MED	🟧 DefaultSRI	Server	B2BUA	MED	MED
1	CloudPBX	🟧 DefaultSRI	Server	Microsoft Server	CloudPBX	--
2	Users	🟧 DefaultSRI	User	Microsoft Server	--	Users
3	Local-GW	🟧 DefaultSRI	Server	B2BUA	Local-GW	--

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., CCE Mediation Server and Cloud PBX) 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 (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification**).
2. Click **New**, and then in the dialog box, add a Classification rule as shown below:

Parameter	Value
Match	
Index	**0**
Name	**Users**
Source SIP Interface	**Users**
Source Host	**Ilync15.local**
Action	
Source IP Group	**Users**

3. Click **Apply**.

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 Cloud PBX
- Routing calls between Users (alternative route for above)
- Routing calls from Users to PSTN (alternative route for above)
- Routing calls from Cloud PBX to Users
- Routing calls from PSTN to Users

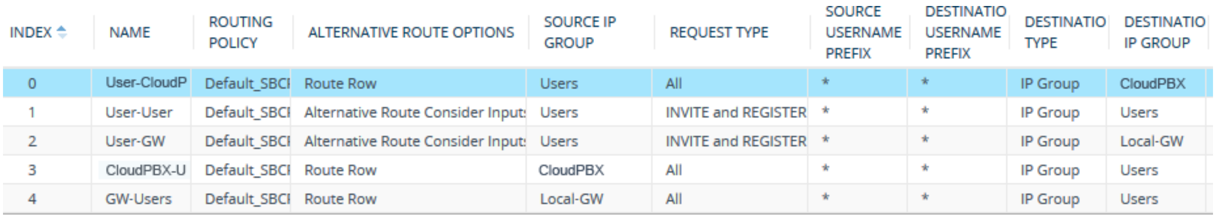
➢ To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Click **New**, and then in the 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 → Cloud PBX	**User-CloudPBX**	**Route Row**	**Users**	**All**	**CloudPBX**
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**
Cloud PBX → Users	**CloudPBX-Users**	**Route Row**	**CloudPBX**	**All**	**Users**
PSTN → Users	**GW-Users**	**Route Row**	**Local-GW**	**All**	**Users**

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

Figure 3-22: Configured IP-to-IP Routing Rules



INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATIO USERNAME PREFIX	DESTINATIO TYPE	DESTINATIO IP GROUP
0	User-CloudP	Default_SBCI	Route Row	Users	All	*	*	IP Group	CloudPBX
1	User-User	Default_SBCI	Alternative Route Consider Input:	Users	INVITE and REGISTER	*	*	IP Group	Users
2	User-GW	Default_SBCI	Alternative Route Consider Input:	Users	INVITE and REGISTER	*	*	IP Group	Local-GW
3	CloudPBX-U	Default_SBCI	Route Row	CloudPBX	All	*	*	IP Group	Users
4	GW-Users	Default_SBCI	Route Row	Local-GW	All	*	*	IP Group	Users

3.15 Step 15: Configure Media Parameters

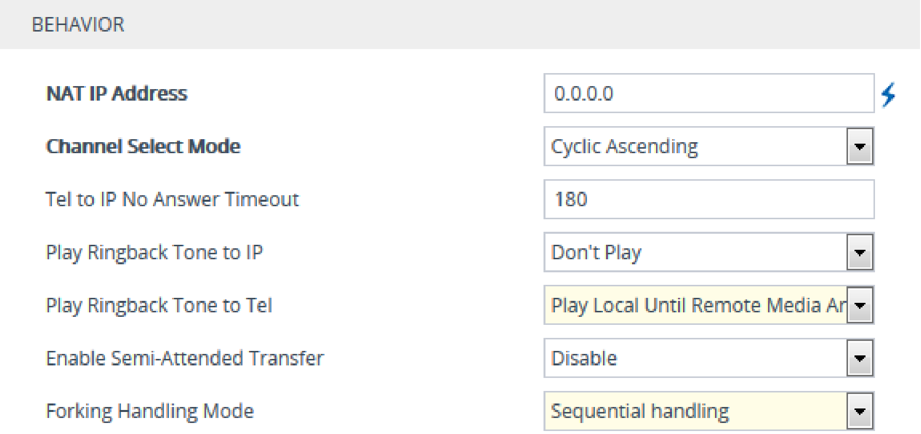
This step describes how to configure the gateway for Media behavior with Microsoft Lync / Skype for Business.

➢ **To configure Media Parameters:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**).
2. Configure as follows:

Parameter	Value	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 3-23: Configure Media Parameters



BEHAVIOR

NAT IP Address	0.0.0.0
Channel Select Mode	Cyclic Ascending
Tel to IP No Answer Timeout	180
Play Ringback Tone to IP	Don't Play
Play Ringback Tone to Tel	Play Local Until Remote Media Ar
Enable Semi-Attended Transfer	Disable
Forking Handling Mode	Sequential handling

3. Click **Apply**.

4. Open the SIP Definitions General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **SIP Definitions General Settings**).
5. Configure as follows:

Parameter	Value	Description
Early 183	**Enable**	**Note:** If the 'B-Channel Negotiation' parameter is set to **Preferred** or **Any**, the 'Early 183' parameter is ignored and a SIP 183 is not sent when an INVITE is received. 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 when an ISDN Call Proceeding message is received.

Figure 3-24: Configuring Early Media

Early 183: Enable

6. Click **Apply**.

3.16 Step 16: Restrict Communication with CCE 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 CCE Mediation Server (as required by Microsoft).

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

1. Open the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway Advanced Settings**).
2. From the 'IP Security' drop-down list, select **Secure Incoming calls**:

Figure 3-25: Restricting Communication with CCE Mediation Server

IP Security: Secure Incoming calls

3. Click **Apply**.

3.17 Step 17: Configure Graceful Period for Registration Expiry

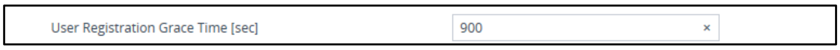
In survivability mode, if the registration time of the registered IP Phone at the OVR is about to expire and the IP Phone resets, by the time the IP Phone becomes available again, the OVR would have already removed the IP Phone from its database due to expiry time being reached. As the OVR does not support 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 Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
2. In the 'User Registration Grace Time' (SBCUserRegistrationGraceTime), enter **900** (in seconds):

Figure 3-26: Configuring Graceful Registration Expiry Time



User Registration Grace Time [sec] 900

3. Click **Apply**.

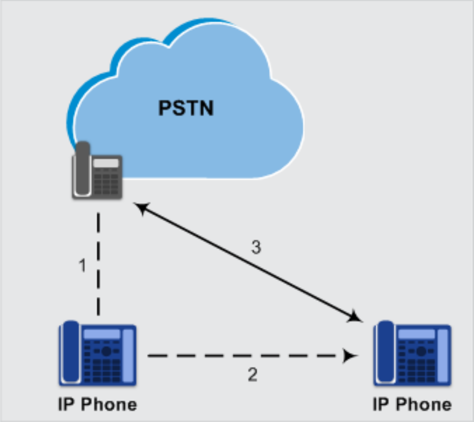
3.18 Step 18: Configure Message Manipulation Rules

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.

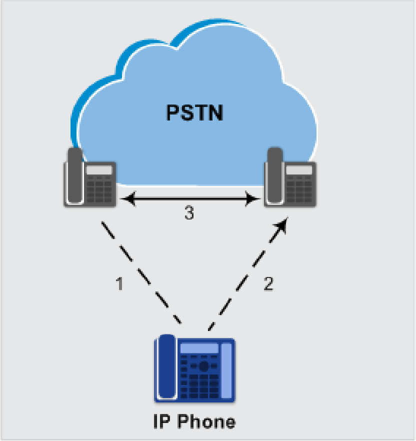
Note: The Message Manipulation Rules described above are only valid in Survivability mode.

Figure 3-27: 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 3-28: 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 0), using the Manipulation Set ID (3) under which the rules are configured.

➢ **To configure Message Manipulation rules:**

1. Open the Message Manipulations table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. For each rule, click **New**, and then in the dialog box, add a Message Manipulation rule. When you have finished, click **Apply**. Add the following rules:
   - For setting IP Phone's number as Caller ID for calls to PSTN in survivability mode:

Parameter	Value
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:

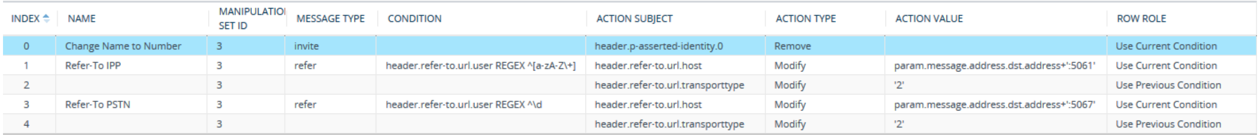
Parameter	Value
Index	**1**
Name	**Refer-To IPP**
Manipulation Set ID	**3**
Message Type	**REFER**
Condition	header.refer-to.url.user REGEX ^[a-zA-Z\+]
Action Subject	header.refer-to.url.host
Action Type	**Modify**
Action Value	**param.message.address.dst.address+':5061'**
Row Rule	**Use Current Condition**
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	Value
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 3-29: Configured Message Manipulation Rules



INDEX	NAME	MANIPULATIOI 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 SIP Forking

If the callee is registered from multiple devices (e.g., multiple IP Phones), the OVR will receive multiple SIP 180 Ringing responses from the Front End Server, with different SDP bodies (each originating from a different device belonging to the callee). For the OVR to forward these multiple 180 Ringing responses to the caller with the SDP bodies unchanged, you need to configure the OVR to handle call forking sequentially. Configuring sequential call forking enables the OVR to allow the callee to answer the call from any the callee's devices.

➢ **To configure sequential call forking mode:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling** & **Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'Forking Handling Mode' drop-down list (SBCForkingHandlingMode), select **Sequential**.
3. Click **Apply**.

3.20 Step 20: 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.

3.20.1 Configure the Trunk

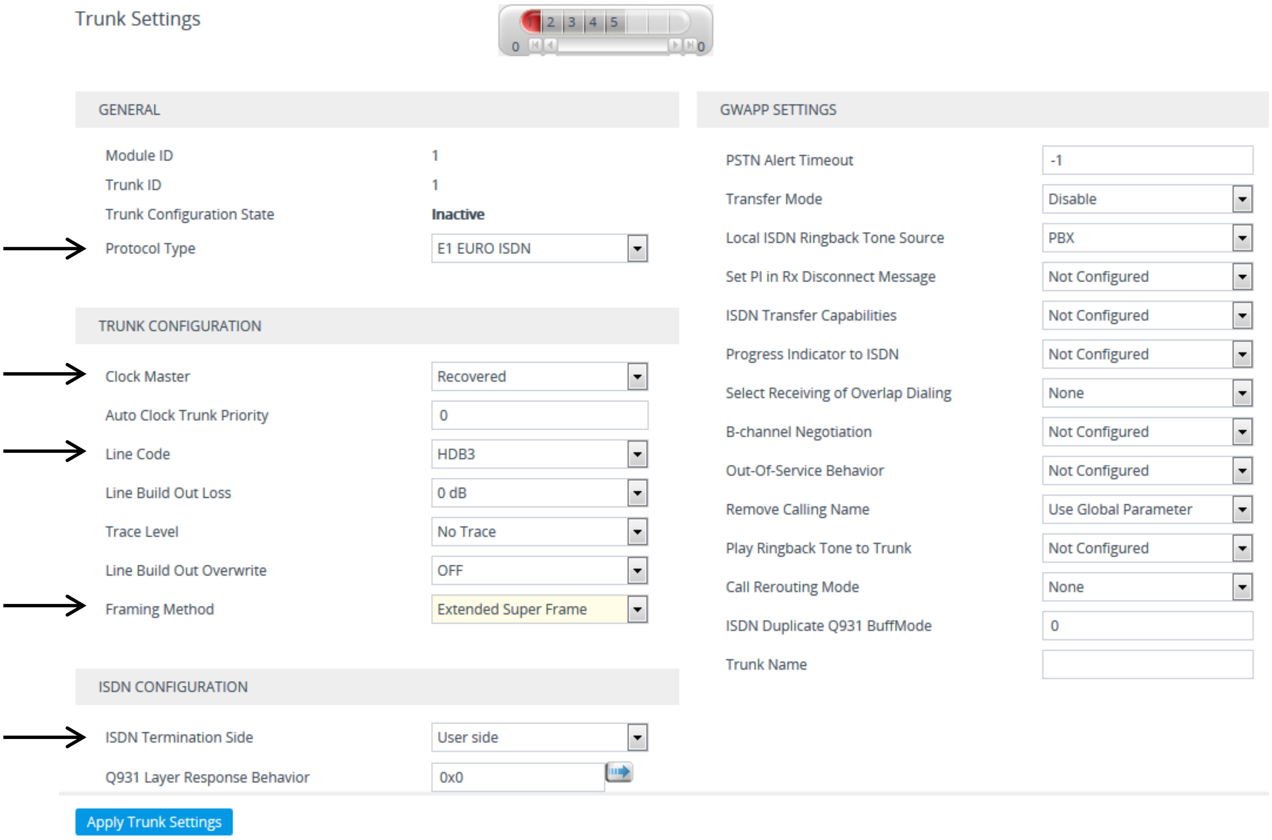
The procedure below describes basic configuration of the physical trunk.

➢ **To configure the physical trunk:**

1. Open the Trunk Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunks**).
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 3.20.2).
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 3.20.2).
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 3-30: Configuring Trunk Settings



Trunk Settings

GENERAL

Module ID	1
Trunk ID	1
Trunk Configuration State	**Inactive**
Protocol Type	E1 EURO ISDN

TRUNK CONFIGURATION

Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	HDB3
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

GWAPP SETTINGS

PSTN Alert Timeout	-1
Transfer Mode	Disable
Local ISDN Ringback Tone Source	PBX
Set PI in Rx Disconnect Message	Not Configured
ISDN Transfer Capabilities	Not Configured
Progress Indicator to ISDN	Not Configured
Select Receiving of Overlap Dialing	None
B-channel Negotiation	Not Configured
Out-Of-Service Behavior	Not Configured
Remove Calling Name	Use Global Parameter
Play Ringback Tone to Trunk	Not Configured
Call Rerouting Mode	None
ISDN Duplicate Q931 BuffMode	0
Trunk Name	

Apply Trunk Settings

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

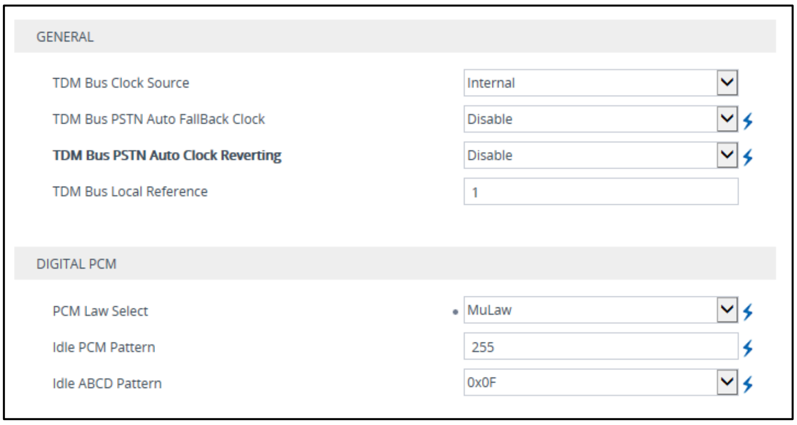
3.20.2 Configure the TDM Bus

The procedure below describes how to configure the TDM bus.

➢ **To configure the TDM bus:**

1. Open the TDM Bus Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **TDM Bus Settings**).

Figure 3-31: Configuring TDM Bus



GENERAL

TDM Bus Clock Source: Internal

TDM Bus PSTN Auto FallBack Clock: Disable

TDM Bus PSTN Auto Clock Reverting: Disable

TDM Bus Local Reference: 1

DIGITAL PCM

PCM Law Select: MuLaw

Idle PCM Pattern: 255

Idle ABCD Pattern: 0x0F

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

3.20.3 Enable the Trunk

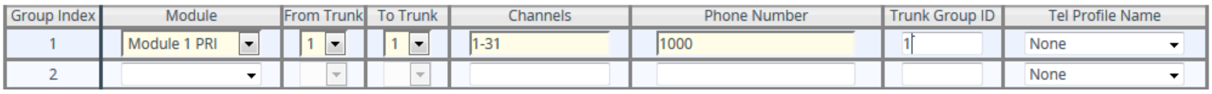
To enable trunks, you need to assign them to Trunk Groups. In the example setup, you need to enable the E1 trunk.

➢ **To enable the trunk:**

1. Open the Trunk Group table page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups > Trunk Groups**).
2. Configure as follows:

Parameter	Value	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 3-32: Enabling Trunk by Assigning it a Trunk Group



Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-31	1000	1	None
2							None

3. Click **Apply**.

3.20.4 Configure the Channel Select Method

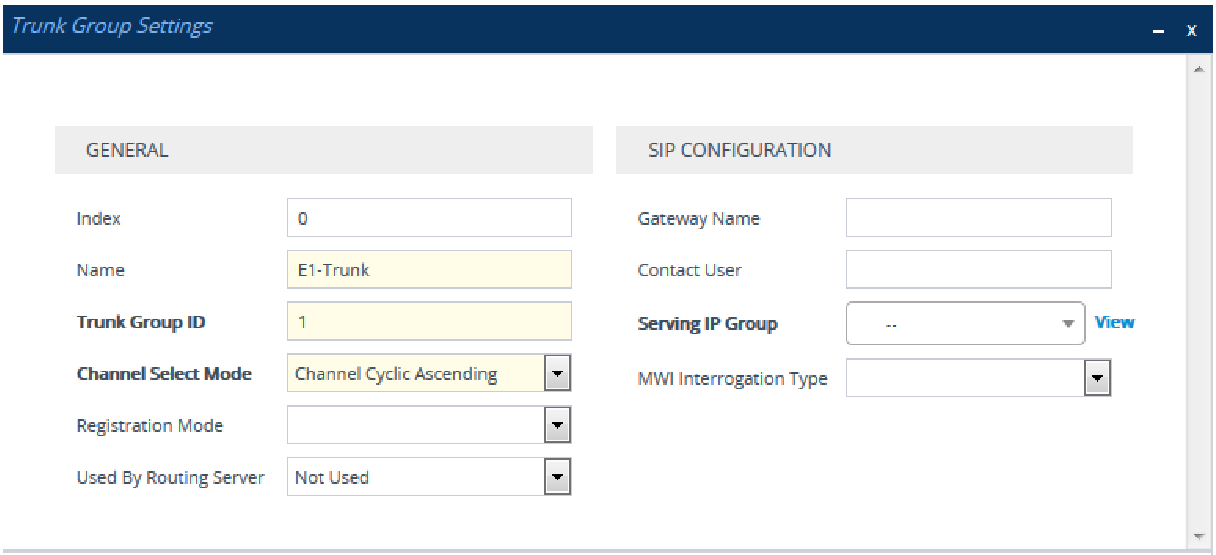
You need to configure the method for assigning IP-to-Tel calls to channels within the Trunk Group. In the example setup, a cyclic ascending method is used, whereby the device selects the next available channel in the Trunk Group, in ascending order. After the highest channel number (e.g., 31) in the 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 table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunk Group Settings**).
2. Click **New**, and then in the dialog box, configure the trunk as follows:

Parameter	Value
Index	**0**
Trunk Group ID	**1**
Channel Select Mode	**Channel Cyclic Ascending**

Figure 3-33: Configuring Channel Select Method



Trunk Group Settings

GENERAL

Index: 0
Name: E1-Trunk
Trunk Group ID: 1
Channel Select Mode: Channel Cyclic Ascending
Registration Mode:
Used By Routing Server: Not Used

SIP CONFIGURATION

Gateway Name:
Contact User:
Serving IP Group: --
MWI Interrogation Type:

3. Click **Apply**.

3.20.5 Configure an IP-to-Tel Routing Rule

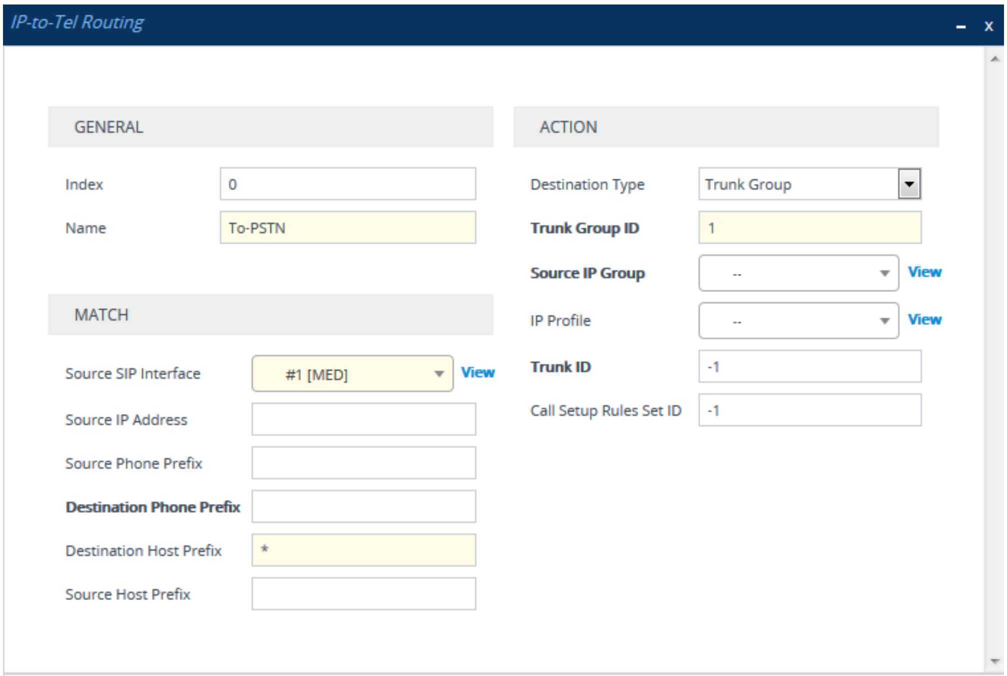
In the example setup, you need to configure an IP-to-Tel routing rule for routing calls to the PSTN.

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

1. Open the IP-to-Tel Routing table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **IP->Tel Routing**).
2. Click **New**, and then in the dialog box, configure an IP-to-Tel routing rule with the following configuration:

Parameter	Value	Description
Index	**0**	-
Match		
Source SIP Interface	**MED**	SIP Interface from where call is received
Destination Phone Prefix	*****	Any number
Action		
Trunk Group ID	**1**	Trunk Group to where call is sent

Figure 3-34: Configuring an IP-to-Tel Routing Rule



IP-to-Tel Routing

GENERAL

Index	0
Name	To-PSTN

MATCH

Source SIP Interface	#1 [MED]
Source IP Address	
Source Phone Prefix	
Destination Phone Prefix	
Destination Host Prefix	*
Source Host Prefix	

ACTION

Destination Type	Trunk Group
Trunk Group ID	1
Source IP Group	--
IP Profile	--
Trunk ID	-1
Call Setup Rules Set ID	-1

3. Click **Apply**.

3.20.6 Configure a Tel-to-IP Routing Rule

In normal operation, the device forwards calls from the PSTN to CCE Mediation Server. However, if connectivity with CCE 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.

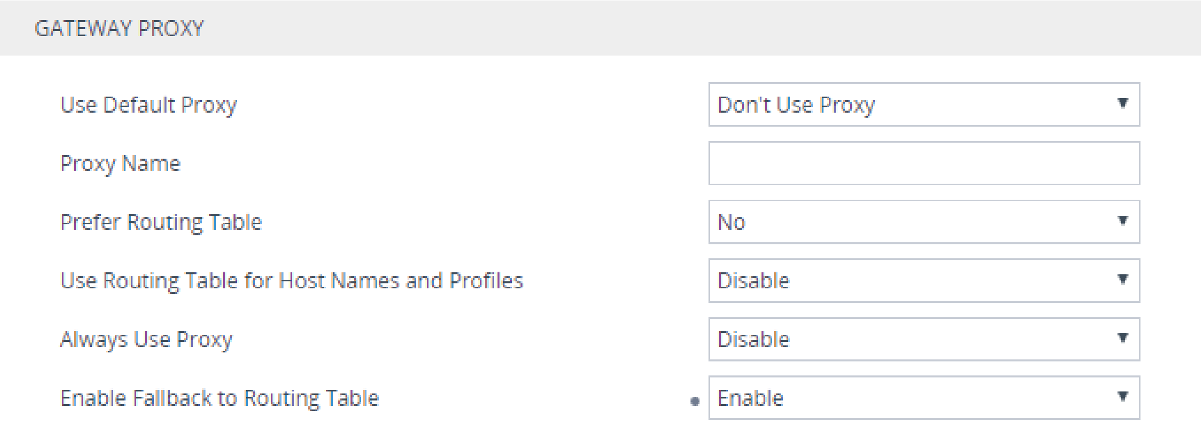
➢ **To configure a Tel-to-IP routing rule:**

1. Open the Tel-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **Tel ->IP Routing**).
2. Click **New**, and then add a routing rule as shown below:

Parameter	Value	Description
Index	**0**	-
Name	**PSTN-Users**	
Match		
Source Trunk Group ID	**1**	
Action		
SIP Interface	**MED**	
Destination IP Address	**127.0.0.1**	IP address 127.0.0.1 is a logical representation of the device's IP address. When you apply the configuration (i.e., click **Apply**), the actual address populates the field (i.e., 10.15.45.112).
Destination Port	**5061**	
Transport Type	**TLS**	

3. Click **Apply**.
4. Set the parameter Enable Fallback to Routing Table.to allow for an unsuccessful route in the Mediation Proxy Set to fall back to the routing table:
   a. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
   b. Set 'Enable Fallback to Routing Table' to **enable.**

Figure 3-35: Enable Fallback to Routing Table



GATEWAY PROXY

Use Default Proxy	Don't Use Proxy
Proxy Name	
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Enable Fallback to Routing Table	Enable

3.20.7 Configure Alternative Route in CCE Environment

In the CCE environment, the CCE Mediation Server is collocated with the OVR device because the CCE Mediation Server is always Up. So when a call passes from the PSTN to the Mediation server when Cloud connectivity is lost, the Mediation server takes several seconds until it responds with 504 message. Some ITSPs may disconnect the call before the Alternative route is applied. In order to resolve this issue, you need to configure the parameter 'Tel to IP No Answer Timeout' which defines the time (in seconds) the device waits for a 200 OK response from the Mediation after sending an INVITE message when an alternate route to the OVR is configured.

3.20.7.1 Configure Tel to IP No Answer Timeout

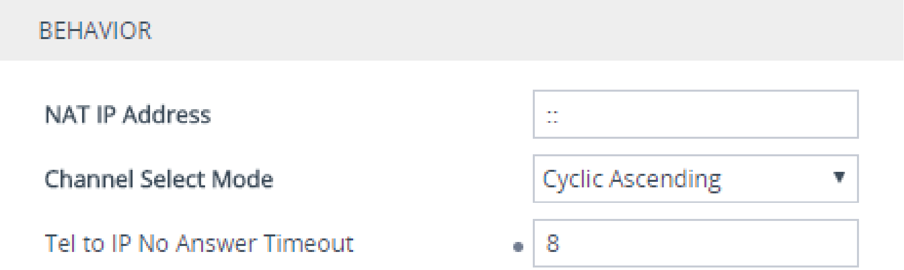
This step describes how to configure the Tel to IP No Answer Timeout.

➢ **To configure the Tel to IP No Answer Timeout:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**).
2. Configure the parameter Tel to IP No Answer Timeout to 8.

   The device waits for eight seconds for a 200 OK response from the Mediation server after sending an INVITE message for Tel-to-IP calls before routing the call to the OVR via the alternative route.

Figure 3-36: Configure Tel to IP No Answer Timeout



BEHAVIOR

NAT IP Address: ::

Channel Select Mode: Cyclic Ascending ▼

Tel to IP No Answer Timeout ● 8

3. Click **Apply**.

3.20.7.2 Configure Tel-to-IP Alternative Route Reason

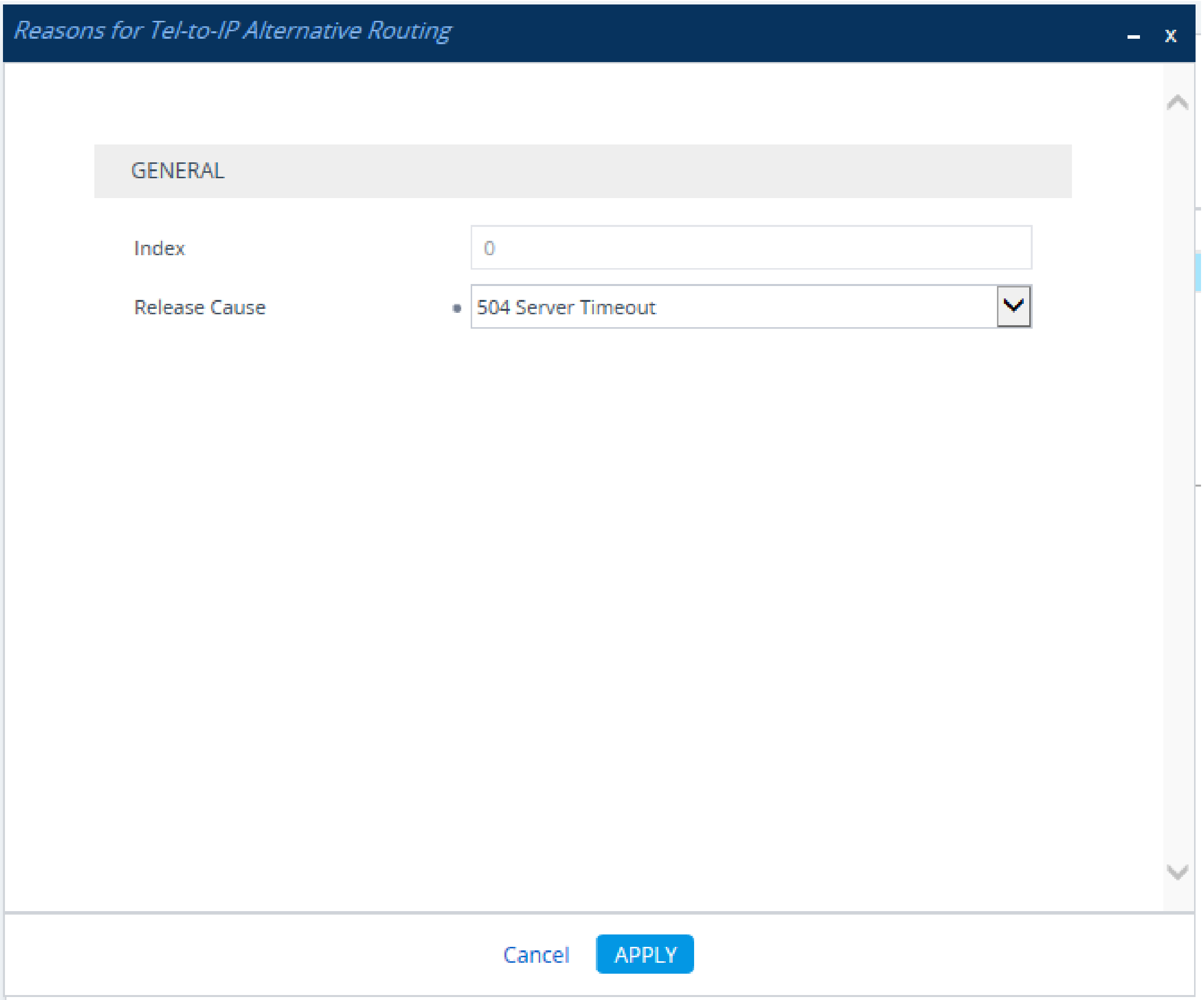
This step describes how to configure the Tel-to-IP Alternative Route Reason

➢ **To configure the Tel-to-IP Alternative Route Reason:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Alternative Routing Reasons > Reasons for Tel->IP**).

2. Click **New**.
3. From the 'Release Cause' drop-down list, select **504 Server Timeout**.

Figure 3-37: GW Alternative Routing Reasons Table



Reasons for Tel-to-IP Alternative Routing

GENERAL

Index: 0

Release Cause: 504 Server Timeout

4. Click **Apply**.

3.20.8 Configure a Number Manipulation Rule

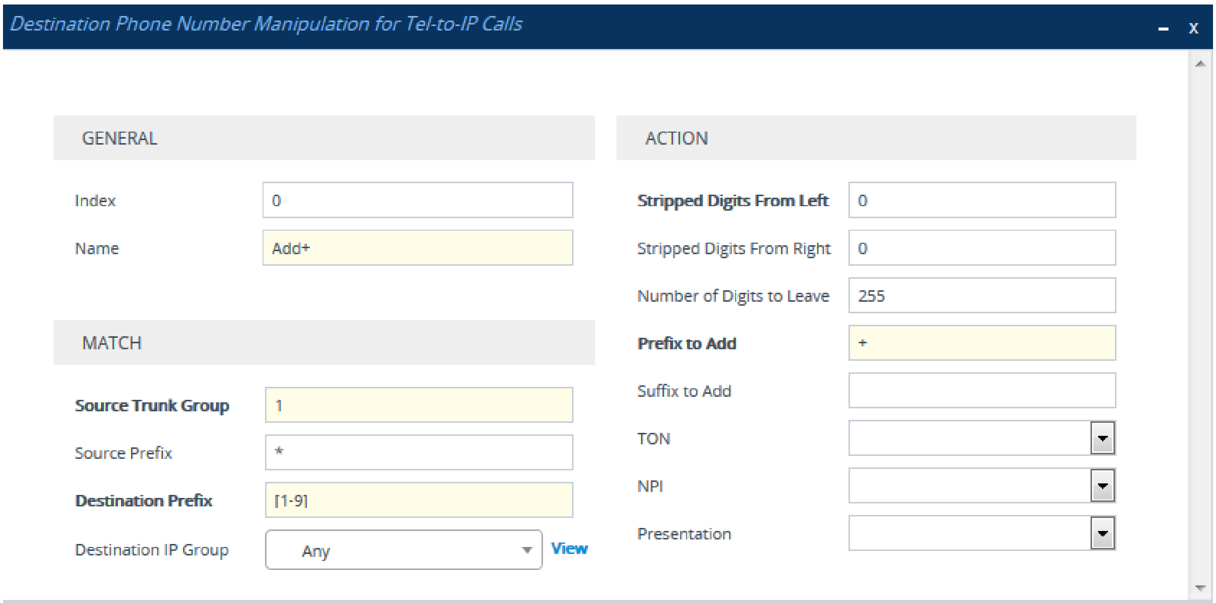
If necessary, you can configure number manipulation rules to manipulate the source and/or destination phone numbers routed between the entities. In the example, you need to configure a manipulation rule to add the plus sign (+) as a prefix to calls received from the PSTN if the destination number starts 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 for Tel-to-IP Calls table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Manipulation** > **Dest Number Tel -> IP**).
2. Click **New**, and then add a manipulation rule as shown below:

Parameter	Value	Description
Index	**0**	-
Name	**Add +**	-
Match		
Source Trunk Group	**1**	**-**
Destination Prefix	**[1-9]**	Any number with prefix from 1 to 9
Action		
Prefix to Add	**+**	-

Figure 3-38: Configuring a Number Manipulation Rule



Destination Phone Number Manipulation for Tel-to-IP Calls

GENERAL

Index	0
Name	Add+

MATCH

Source Trunk Group	1
Source Prefix	*
Destination Prefix	[1-9]
Destination IP Group	Any

ACTION

Stripped Digits From Left	0
Stripped Digits From Right	0
Number of Digits to Leave	255
Prefix to Add	+
Suffix to Add	
TON	
NPI	
Presentation	

3. Click **Apply**.

4 Configuring AudioCodes IP Phones for OVR

This chapter describes the configuration of AudioCodes Skype-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 Cloud PBX responds to the IP Phone with DHCP Options providing, for example, networking settings (IP address and Default Gateway), NTP server address, LDAP server address (Cloud PBX), 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 Skype for Business Online/Cloud PBX with credentials (username and password) provided by the Administrator.
8. The Skype for Business Online/Cloud PBX 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 Skype for Business Online/Cloud PBX now pass transparently through the OVR.

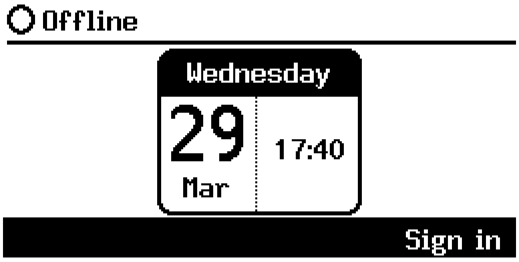
4.2 Signing IP Phone into Skype for Business Online /Cloud PBX

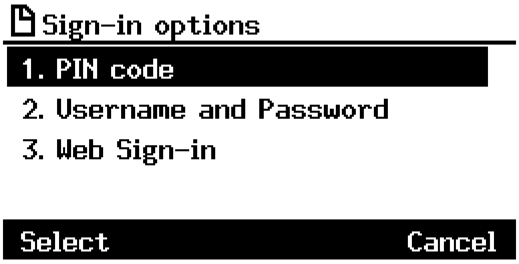
To register the IP Phone with Skype for Business Online /Cloud PBX, the user must perform a sign-in procedure on the IP Phone. Users can sign in using a username-password combination or by using the Cloud PBX Web option.

> **Note:** The LCD screens shown in the procedure are of the 430HD and 440HD models; the 420HD and 405 model's LCD screens are similar.

➢ **To sign in to the phone:**

1. In the idle screen, press the **Sign in** softkey; the sign-in options are displayed:





2. Sign-in using one of the following methods:
   - User name and Password - see Section 4.2.1
   - Web Sign-in - see Section 4.2.2

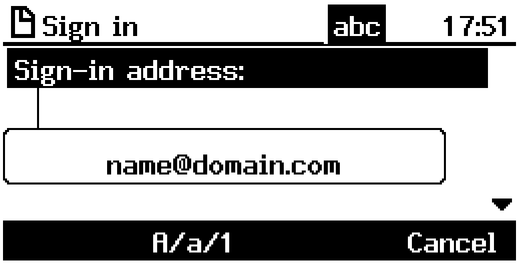
> **Note:**
>
> - After signing out, the next time you sign in the phone will present the option that was used to sign in before signing out.
> - If a user signs out and another signs in, the phone presents empty Speed Dials and empty Call Logs to the newly signed-in user. The Speed Dials and Call Logs of the signed-out user are not saved on the phone.

4.2.1 Signing in with User Name and Password

This section shows how to sign in with User Name and Password.

➢ **To sign in with User Name and Password:**

1. In the 'Sign-in options' screen, select **User name and Password**.



Sign in abc 17:51

Sign-in address:

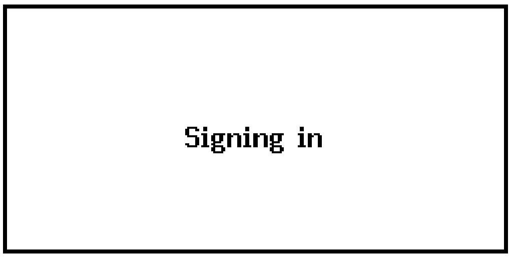
name@domain.com

A/a/1 Cancel

2. Sign-in as follows:
   - Sign-in address, i.e., SIP URI.
   - User name, in UPN (User Principal Name) format, i.e., the way the user's name appears in their e-mail address listed in the Active Directory: username@domain.com
   - User’s network IT password (the same password you use to access your PC)

Note: Signing in with a username that is a NetBIOS Domain Name, i.e., **domain\username** are *disallowed* for Skype for Business Online /Cloud PBX sign-in. They are only allowed for *on-premises* sign-in.

3. Press the **Sign in** softkey; after signing in successfully, the New Device Lock Code screen opens.

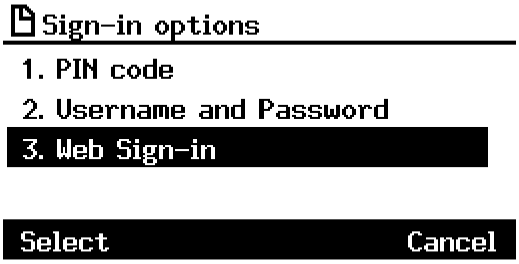


Signing in

4.2.2 Signing in with the Cloud PBX Web Option

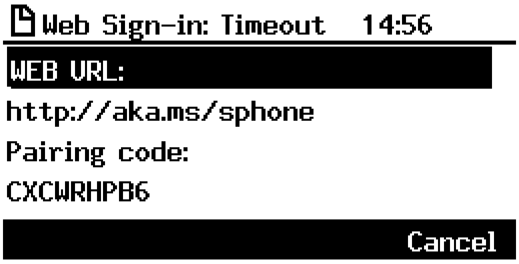
This section shows how to sign in with the Cloud PBX Web option, a.k.a. Device Pairing. Signing in with this option enables connectivity to Microsoft's Cloud PBX, Microsoft's cloud-hosted version of enterprise voice.

The option exempts users from having to laboriously key in their user name and password using the phone keypad. If the option is selected, a URL and a Pairing Code are displayed:



Sign-in options

1. PIN code
2. Username and Password
3. Web Sign-in



Web Sign-in: Timeout 14:56

WEB URL:

http://aka.ms/sphone

Pairing code:

CXCWRHPB6

Users must then point their browser to the URL and enter the Pairing Code in the Microsoft web page. Sign-in to Microsoft's Cloud PBX is then performed.

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 IP phone management interfaces 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

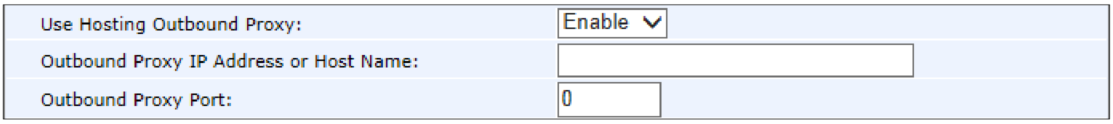
If you want to use the Web-based management platform for configuration, you need to perform the following procedure on each IP Phone. Perform this configuration

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

➢ **To configure the IP Phone through IP phone's 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



Use Hosting Outbound Proxy:	Enable
Outbound Proxy IP Address or Host Name:	
Outbound Proxy Port:	0

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 Device Manager Pro

AudioCodes Device Manager Pro can be used to mass provision the IP Phones deployed with OVR. The Device Manager Pro is accessed from AudioCodes' One Voice Operations Center (OVOC).

The IP Phones "learn" of the address of the Device Manager Pro 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 Device Manager Pro, the Device Manager Pro 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 Device Manager Pro allows you to create a Configuration file for the specific OVR tenant and the IP Phone users belonging to it. 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.

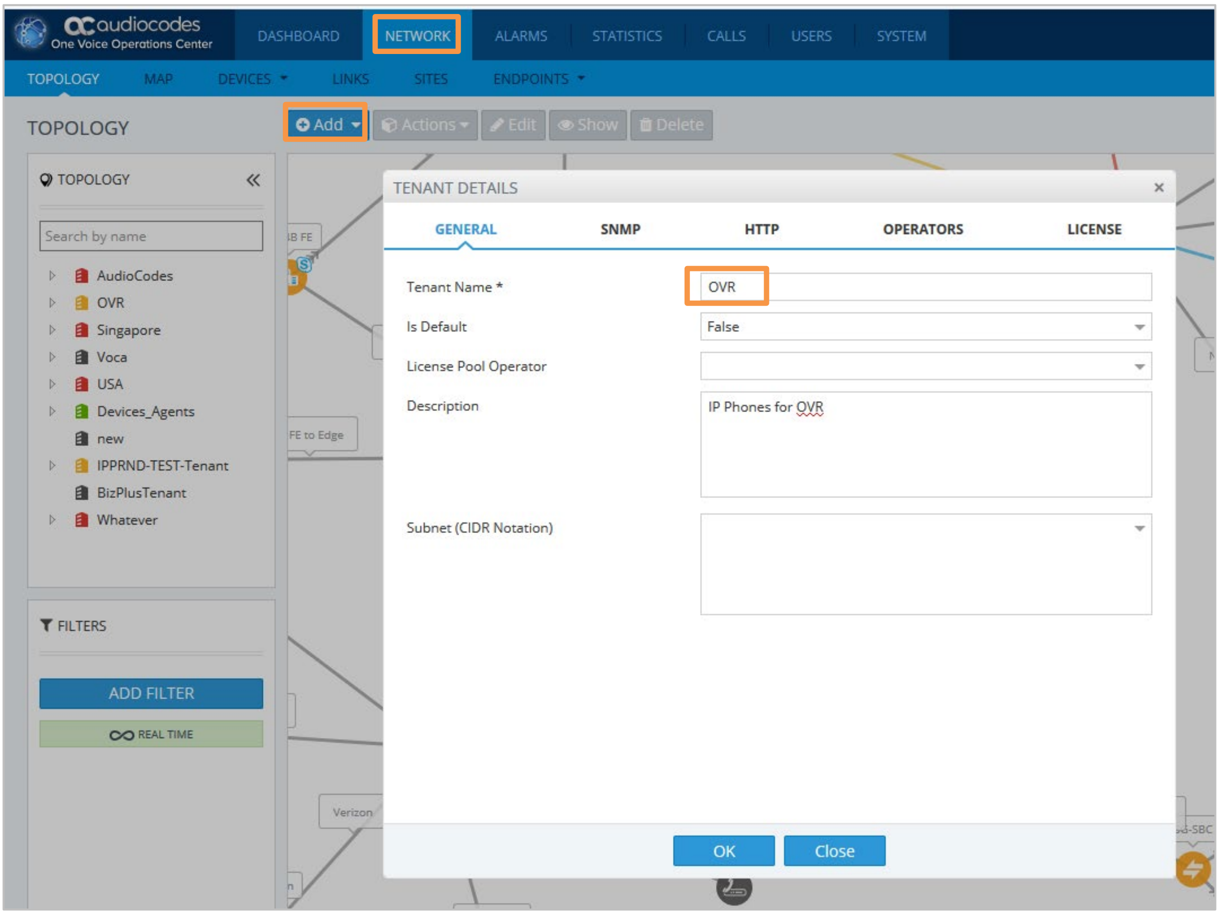
Note:

- This configuration is done before you initially connect the IP Phone to the network and power up.
- For detailed information on the Device Manager Pro, refer to the *Device Manager Pro Administrator's Manual*.

➢ To configure IP Phone through Device Manager Pro:

1. Log in to AudioCodes' OVOC.
2. Create a Tenant to represent the IP Phones deployed in the OVR environment:
   a. Select the **NETWORK** menu.
   b. Click the **Add** button, and then from the drop-down menu, choose **TENANT**.
   c. In the 'Tenant Name' field, configure a name for the OVR deployment (e.g., "OVR"), and then click **OK**.

Figure 4-2: Configuring Tenant for OVR in OVOC



Tenant Name *: OVR

Is Default: False

License Pool Operator:

Description: IP Phones for OVR

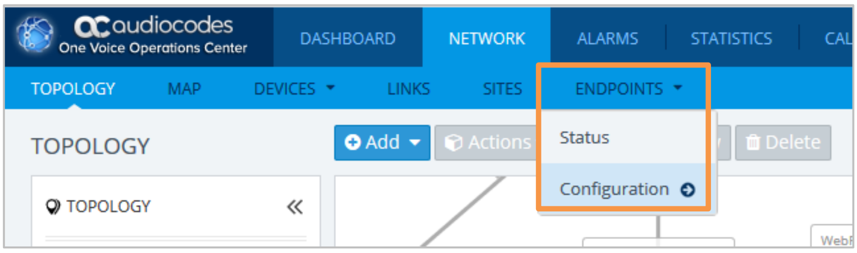
Subnet (CIDR Notation):

3. Access the Device Manager Pro from OVOC:

   a. Select the **NETWORK** menu.

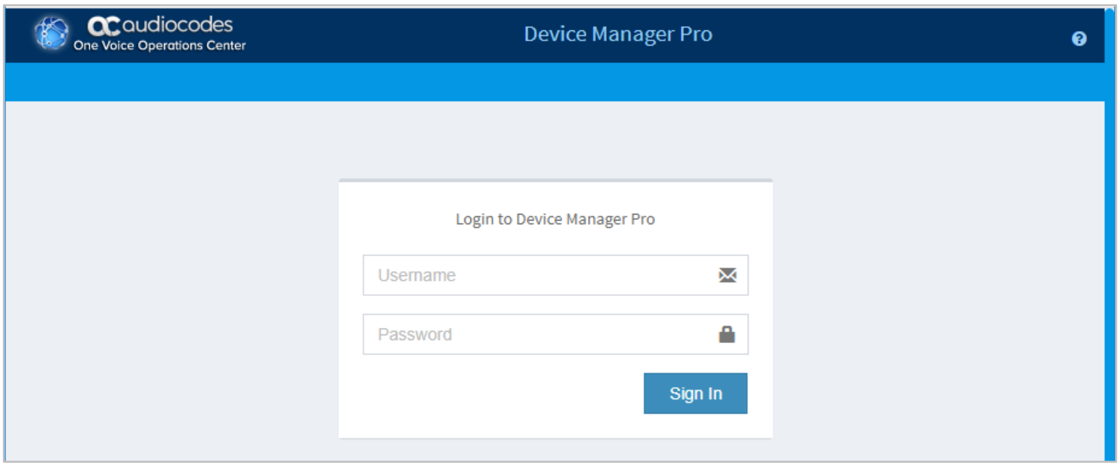
   b. Click **ENDPOINTS**, and then from the drop-down menu, choose **Configuration**.

Figure 4-3: Accessing Device Manager Pro from OVOC



The Login to Device Manager Pro screen appears:

Figure 4-4: Logging into Device Manager Pro

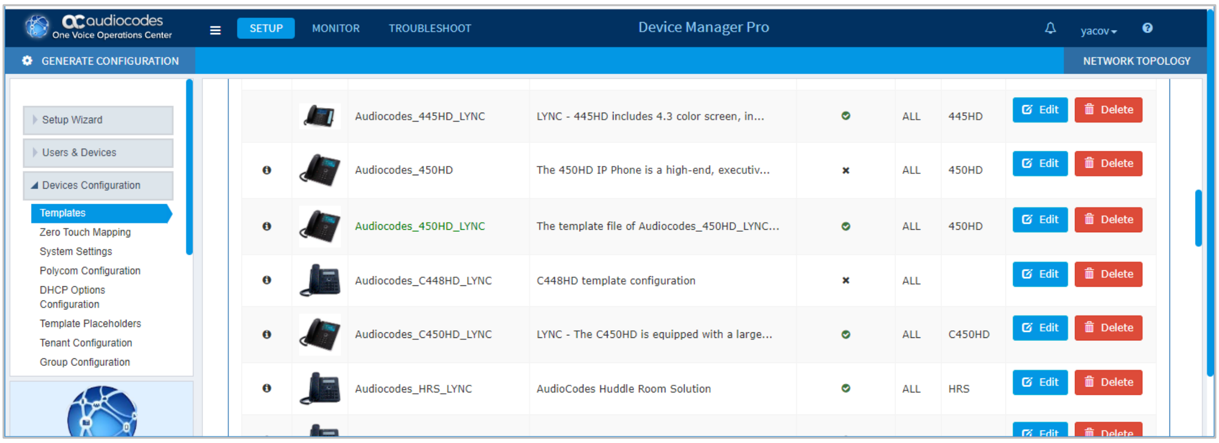


   c. Enter your username and password (default is **acladmin** and **pass_1234**, respectively), and then click **Sign In**.

4. (**All IP Phones for OVR Deployment**) Configure the OVR-related parameters in the IP Phone template(s):

   a. Access the Devices Configuration Templates page (**SETUP** menu > **Devices Configuration** folder > **Templates**).

Figure 4-5: Selecting IP Phone Model on Devices Configuration Templates Page



	Audiocodes_445HD_LYNC	LYNC - 445HD includes 4.3 color screen, in...	✓	ALL	445HD	Edit	Delete
ℹ	Audiocodes_450HD	The 450HD IP Phone is a high-end, executiv...	✗	ALL	450HD	Edit	Delete
ℹ	Audiocodes_450HD_LYNC	The template file of Audiocodes_450HD_LYNC...	✓	ALL	450HD	Edit	Delete
ℹ	Audiocodes_C448HD_LYNC	C448HD template configuration	✗	ALL		Edit	Delete
ℹ	Audiocodes_C450HD_LYNC	LYNC - The C450HD is equipped with a large...	✓	ALL	C450HD	Edit	Delete
ℹ	Audiocodes_HRS_LYNC	AudioCodes Huddle Room Solution	✓	ALL	HRS	Edit	Delete

b. Select the required IP Phone model (e.g., AudioCodes_440HD_LYNC), by clicking the model name or its corresponding **Edit** button; the Device Configuration Template page for the selected model opens.

c. For each parameter (lync/sign_in/fixed_outbound_proxy_address, lync/sign_in/fixed_outbound_proxy_port, and lync/sign_in/use_hosting_outbound_proxy), do the following under the **Edit configuration template values** group:

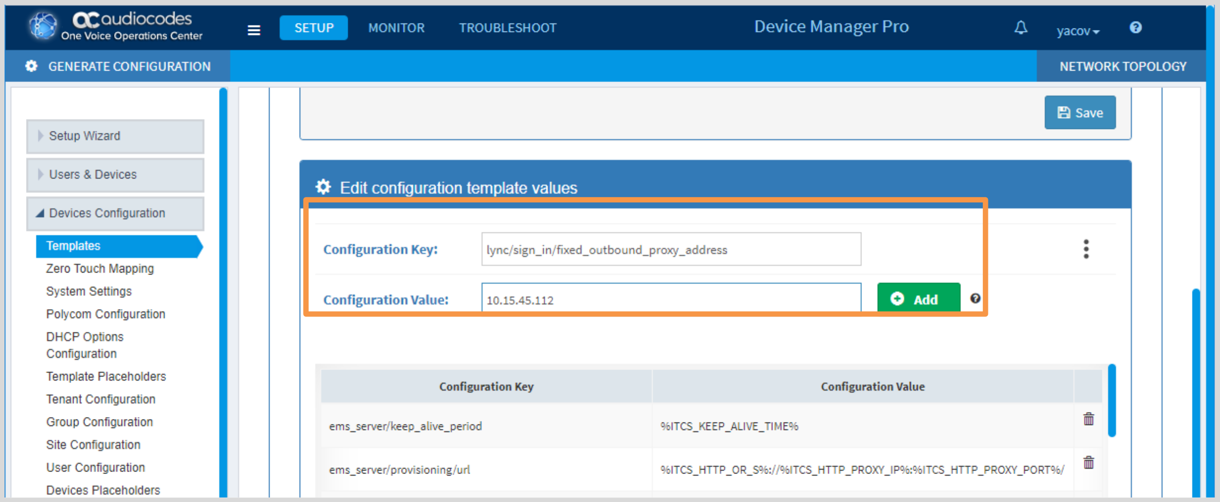
   a. In the 'Configuration Key' field, enter the parameter name.

   b. In the 'Configuration Value' field, enter the parameter's value.

   c. Click **Add**.

d. Repeat steps b) and c) for each relevant IP Phone model.

Figure 4-6: Configuring Parameters on Device Configuration Template Page



Configuration Key: lync/sign_in/fixed_outbound_proxy_address

Configuration Value: 10.15.45.112

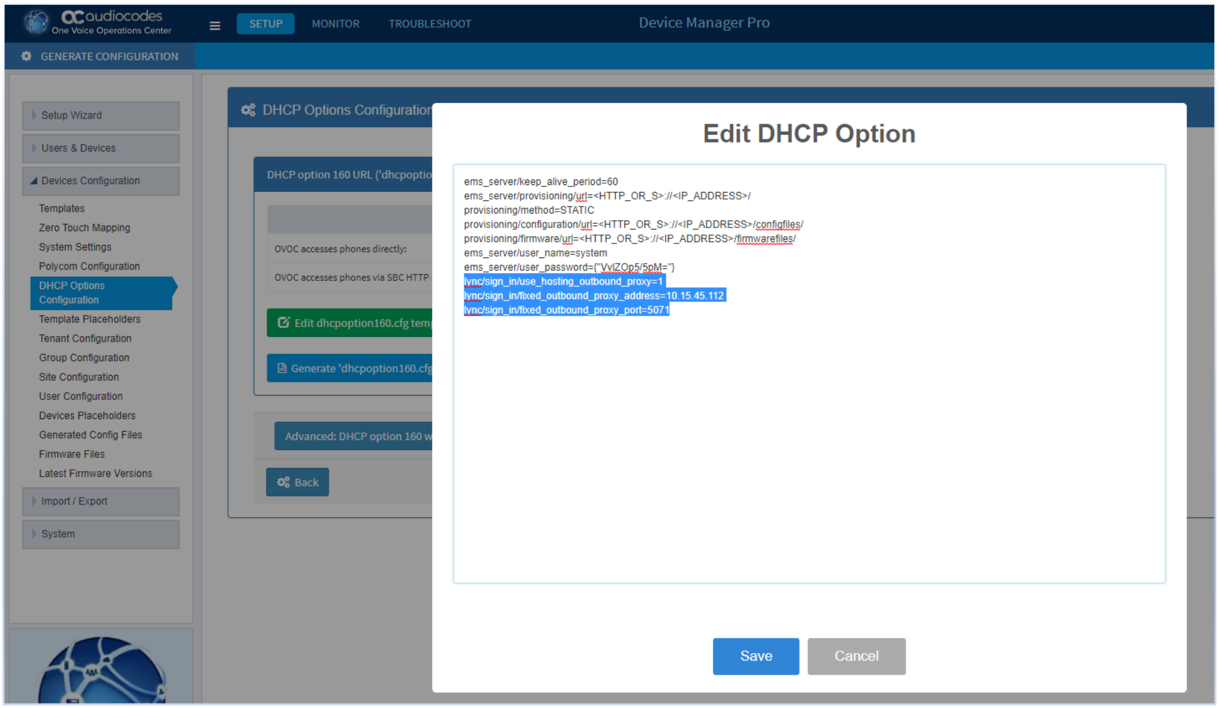
Configuration Key	Configuration Value
ems_server/keep_alive_period	%ITCS_KEEP_ALIVE_TIME%
ems_server/provisioning/url	%ITCS_HTTP_OR_S%://%ITCS_HTTP_PROXY_IP%:%ITCS_HTTP_PROXY_PORT%/

e. Access the DHCP Options Configuration page (**SETUP** menu > **Devices Configuration** folder > **DHCP Options Configuration**) to configure the DHCP Option 160 template.

f. Click the **Edit dhcpoption160.cfg template** button; the Edit DHCP Option dialog box appears.

g. Copy and paste the parameters with their values (see Step c above) into the text box, as shown highlighted below, and then click **Save**:

Figure 4-7: Configuring DHCP Option 160



```
ems_server/keep_alive_period=60
ems_server/provisioning/url=<HTTP_OR_S>://<IP_ADDRESS>/
provisioning/method=STATIC
provisioning/configuration/url=<HTTP_OR_S>://<IP_ADDRESS>/configfiles/
provisioning/firmware/url=<HTTP_OR_S>://<IP_ADDRESS>/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={"VvlZOp5/5pM="}
lync/sign_in/use_hosting_outbound_proxy=1
lync/sign_in/fixed_outbound_proxy_address=10.15.45.112
lync/sign_in/fixed_outbound_proxy_port=5071
```

5. (**Only Selected IP Phones for OVR Deployment**):

   a. Open the Tenant Configuration page (**SETUP** menu > **Devices Configuration** folder > **Tenant Configuration**).

   b. From the 'Select Tenant' drop-down list, select the name of the Tenant that you configured for OVR in OVOC in Step 2 (e.g., "OVR").

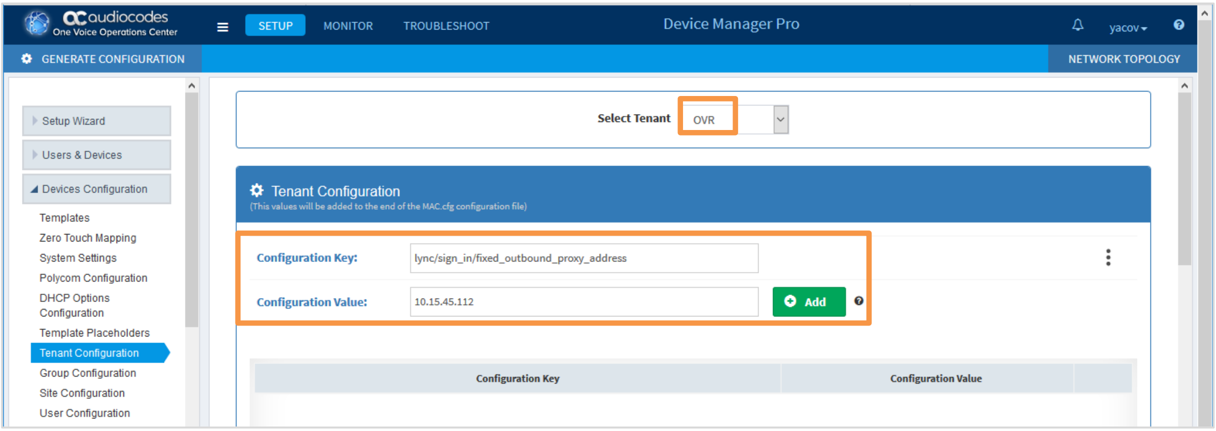
   c. For each parameter (lync/sign_in/fixed_outbound_proxy_address, lync/sign_in/fixed_outbound_proxy_port, and lync/sign_in/use_hosting_outbound_proxy), do the following:

      a. In the 'Configuration Key' field, enter the parameter name.

      b. In the 'Configuration Value' field, enter the parameter's value.

      c. Click **Add**.

Figure 4-8: Configuring OVR Parameters for IP Phones of OVR Tenant



Select Tenant: OVR

Configuration Key: lync/sign_in/fixed_outbound_proxy_address

Configuration Value: 10.15.45.112

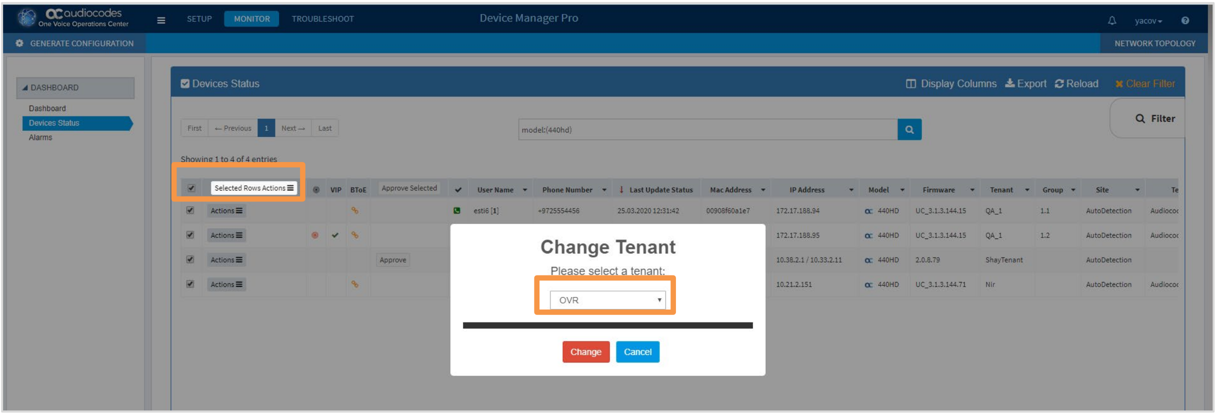
d. Access the Devices Status page (**MONITOR** menu > **DASHBOARD** folder > **Devices Status**) to assign specific users to the OVR tenant

e. Filter the list so that it displays only the specific IP Phone users, by clicking the **Filter** button (located on the right of the page) and then defining an appropriate filter.

f. In the list of users, select the top check box to select all the users, and then from the **Selected Rows Actions** drop-down list, choose **Change Tenant**.

g. From the drop-down list, select **OVR**, and then click **Change**.

Figure 4-9: Assigning IP Phone Users to OVR Tenant



Devices Status

model:(440hd)

Showing 1 to 4 of 4 entries

VIP	BToE	User Name	Phone Number	Last Update Status	Mac Address	IP Address	Model	Firmware	Tenant	Group	Site	Te
		esti6 [1]	+9725554456	25.03.2020 12:31:42	00908f60a1e7	172.17.188.94	440HD	UC_3.1.3.144.15	QA_1	1.1	AutoDetection	Audiococ
✓						172.17.188.95	440HD	UC_3.1.3.144.15	QA_1	1.2	AutoDetection	Audiococ
						10.38.2.1 / 10.33.2.11	440HD	2.0.8.79	ShayTenant		AutoDetection	
						10.21.2.151	440HD	UC_3.1.3.144.71	Nir		AutoDetection	Audiococ

Change Tenant

Please select a tenant:

OVR

6. Generate the Configuration file for the IP Phone users:

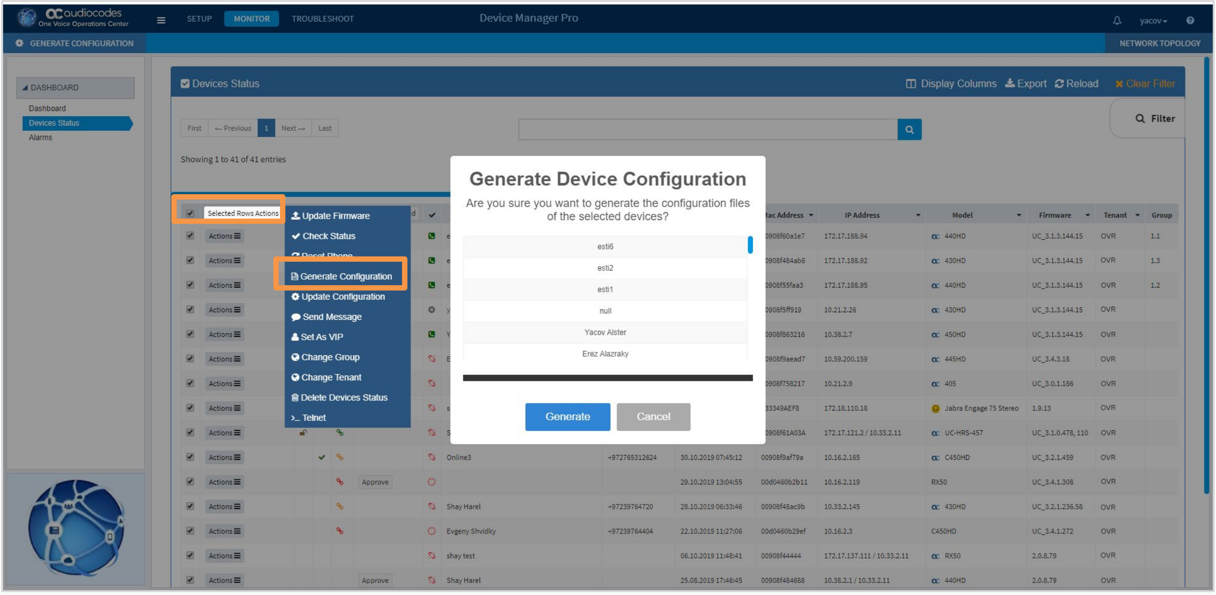
a. Access the Manage Multiple Users page (**MONITOR** menu > **DASHBOARD** folder > **Devices Status**).

b. Filter the list of users so that it displays only users belonging to the tenant configured for the OVR (e.g., "OVR"). Filtering is done by clicking the **Filter** button (located on the right of the page), and then selecting the OVR tenant from the 'Tenant' drop-down list.

c. In the list of users, select the top check box to select all the users, and then from the **Selected Rows Actions** drop-down list, choose **Generate Configuration**.

d. Click the **Generate** button.

Figure 4-10: Generating Configuration File for Users of OVR Tenant



Devices Status

Showing 1 to 41 of 41 entries

Generate Device Configuration

Are you sure you want to generate the configuration files of the selected devices?

esti6

esti2

esti1

null

Yacov Alster

Erez Alazraky

User Name	Phone Number	Last Update Status	Mac Address	IP Address	Model	Firmware	Tenant	Group
			00908f60a1e7	172.17.188.94	440HD	UC_3.1.3.144.15	OVR	1.1
			00908f484ab6	172.17.188.92	430HD	UC_3.1.3.144.15	OVR	1.3
			00908f55faa3	172.17.188.95	440HD	UC_3.1.3.144.15	OVR	1.2
			00908f5ff919	10.21.2.26	430HD	UC_3.1.3.144.15	OVR	
			00908f863216	10.38.2.7	450HD	UC_3.1.3.144.15	OVR	
			00908f9aead7	10.59.200.159	445HD	UC_3.4.3.18	OVR	
			00908f758217	10.21.2.9	405	UC_3.0.1.186	OVR	
			33349AEF8	172.18.110.18	Jabra Engage 75 Stereo	1.9.13	OVR	
			00908f61A03A	172.17.121.2 / 10.33.2.11	UC-HRS-457	UC_3.1.0.478, 110	OVR	
Online3	+972765312624	30.10.2019 07:45:12	00908f9af79a	10.16.2.165	C450HD	UC_3.2.1.459	OVR	
		29.10.2019 13:04:55	00d0460b2b11	10.16.2.119	RX50	UC_3.4.1.308	OVR	
Shay Harel	+97239764720	28.10.2019 06:33:46	00908f48ac9b	10.33.2.145	430HD	UC_3.2.1.236.58	OVR	
Evgeny Shvidky	+97239764404	22.10.2019 11:27:06	00d0460b29ef	10.16.2.3	C450HD	UC_3.4.1.272	OVR	
shay test		06.10.2019 11:48:41	00908f44444	172.17.137.111 / 10.33.2.11	RX50	2.0.8.79	OVR	
Shay Harel		25.08.2019 17:46:45	00908f484688	10.38.2.1 / 10.33.2.11	440HD	2.0.8.79	OVR	

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 for Microsoft Skype for Business 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.
200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/