

One-Voice Resiliency with SIP Trunking

for Microsoft™ Skype for Business Online

Version 7.2

Table of Contents

1	Introduction	7
1.1	Compatible Software Versions	9
1.2	One-Voice Resiliency Constraints	9
2	Overview	11
2.1	Normal Mode.....	11
2.2	Survivability Mode	13
3	Configuring the Device for OVR.....	17
3.1	Step 1: IP Network Interfaces Configuration	20
3.1.1	Step 1a: Configure VLANs.....	21
3.1.2	Step 1b: Configure Network Interfaces.....	22
3.2	Step 2: Enable the SBC Application	23
3.3	Step 3: SIP TLS Connection Configuration.....	24
3.3.1	Step 3a: Configure the NTP Server Address.....	24
3.3.2	Step 3b: Configure TLS for CCE Mediation Server.....	25
3.3.2.1	Configure TLS Version	25
3.3.2.2	Configure Certificate.....	26
3.3.3	Step 3c: Configure TLS for Cloud PBX	31
3.4	Step 4: Configure SRTP	32
3.5	Step 5: Configure Media Realms	33
3.6	Step 6: Configure SIP Interfaces	34
3.7	Step 7: Configure Proxy Sets	35
3.8	Step 8: Configure IP Profiles	37
3.9	Step 9: Configure IP Groups.....	40
3.10	Step 10: Configure a Classification Rule.....	42
3.11	Step 11: Configure IP-to-IP Call Routing Rules	43
3.11.1	Step 11a: Configure SBC Alternative Routing Reasons	44
3.12	Step 12: Configure a Number Manipulation Rule.....	45
3.13	Step 13: Configure Message Manipulation Rules	47
3.14	Step 14: Configure Graceful Period for Registration Expiry	50
3.15	Step 15: Configure SIP Forking	51
3.16	Step 16: Reset the SBC	52
4	Configuring AudioCodes IP Phones for OVR.....	53
4.1	Deployment Summary	53
4.2	Signing IP Phone into Skype for Business Online /Cloud PBX	54
4.2.1	Signing in with User Name and Password	55
4.2.2	Signing in with the Cloud PBX Web Option.....	56
4.3	Configuring IP Phones for OVR.....	57
4.3.1	Configuring IP Phones through the Web Interface.....	58
4.3.2	Configuring IP Phones through Device Manager Pro	59
4.3.3	Configuring the IP Phones through TFTP/HTTP	65

List of Figures

Figure 1-1: Typical OVR Deployment.....	7
Figure 2-1: Normal Mode - Calls between IP Phones.....	11
Figure 2-2: Normal Mode - Calls from IP Phone to PSTN	12
Figure 2-3: Normal Mode - Calls from PSTN to IP Phone	12
Figure 2-4: Survivability Mode - Calls between IP Phones	14
Figure 2-5: Survivability Mode - Calls from IP Phone to PSTN.....	14
Figure 2-6: Survivability Mode – Calls from SIP Trunk to IP Phone.....	15
Figure 3-1: OVR Example Topology and Configuration Entities	17
Figure 3-2: Network Interfaces in Interoperability Test Topology.....	20
Figure 3-3: Configured VLAN IDs in Ethernet Device	21
Figure 3-4: Configured Network Interfaces in IP Interfaces Table	22
Figure 3-5: Enabling SBC Application	23
Figure 3-6: Configuring NTP Server Address.....	24
Figure 3-7: Configuring TLS version	25
Figure 3-8: Certificate Signing Request – Creating CSR	26
Figure 3-9: Microsoft Certificate Services Web Page	27
Figure 3-10: Request a Certificate Page	27
Figure 3-11: Advanced Certificate Request Page	28
Figure 3-12: Submit a Certificate Request or Renewal Request Page	28
Figure 3-13: Certificate Issued Page	28
Figure 3-14: Download a CA Certificate, Certificate Chain, or CRL Page	29
Figure 3-15: Upload Device Certificate Files from your Computer Group	30
Figure 3-16: Importing Root Certificate into Trusted Certificates Store	30
Figure 3-17: Configuring TLS Context for Cloud PBX.....	31
Figure 3-18: Configuring SRTP	32
Figure 3-19: Configured SIP Interfaces.....	34
Figure 3-20: Configured Proxy Sets	35
Figure 3-21: Configured IP Groups	41
Figure 3-22: Configured Classification Table for Users	42
Figure 3-23: Configured IP-to-IP Routing Rules	44
Figure 3-24: SBC Alternative Routing Reasons Table	45
Figure 3-25: Configuring IP-to-IP Outbound Manipulation Rule.....	46
Figure 3-26: Call Transfer of PSTN Call to Another IP Phone User	47
Figure 3-27: Call Transfer of PSTN Call to Another PSTN User.....	47
Figure 3-28: Configured Message Manipulation Rules	49
Figure 3-29: Configuring Graceful Registration Expiry Time.....	50
Figure 3-30: Resetting the SBC	52
Figure 4-1: Configuring OVR on the IP Phone through Web Interface	58
Figure 4-2: Configuring Tenant for OVR in OVOC	60
Figure 4-3: Accessing Device Manager Pro from OVOC	61
Figure 4-4: Logging into Device Manager Pro.....	61
Figure 4-5: Selecting IP Phone Model on Devices Configuration Templates Page.....	61
Figure 4-6: Configuring Parameters on Device Configuration Template Page.....	62
Figure 4-7: Configuring DHCP Option 160.....	63
Figure 4-8: Configuring OVR Parameters for IP Phones of OVR Tenant	63
Figure 4-9: Assigning IP Phone Users to OVR Tenant	64
Figure 4-10: Generating Configuration File for Users of OVR Tenant	64

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
10722	Initial document release.
10725	TLS assignment updated for Cloud PBX; SIP forking added.
10726	Update for support for the Mediant 800C platform.
10728	Update to Section 'One-Voice Resiliency Constraints'.
10730	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>.

1 Introduction

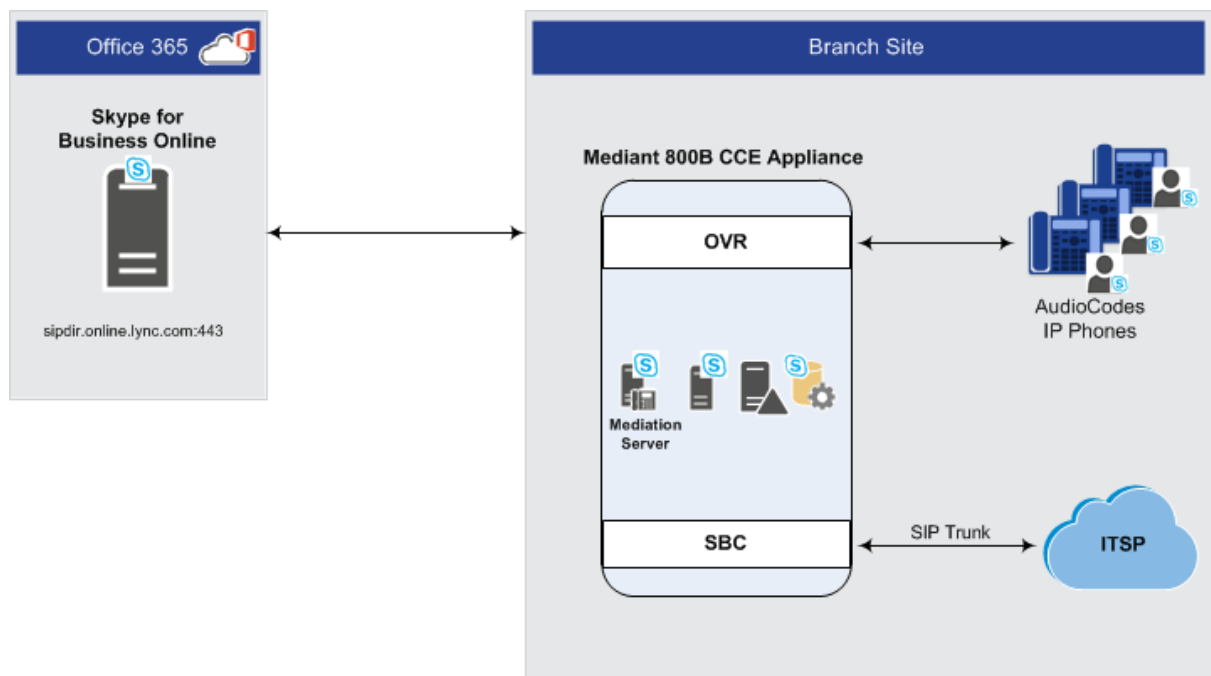
AudioCodes' One-Voice Resiliency (OVR) feature is a sophisticated and powerful VoIP application that runs on AudioCodes Mediant™ 800C and Mediant™ 800B devices, providing call survivability (branch-site resiliency) to AudioCodes IP Phone users at the branch site upon connectivity failure with the Office 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



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 3.8). 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 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).

This page is intentionally left blank.

2 Overview

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

2.1 Normal Mode

In normal mode of operation, OVR acts as an outbound proxy server for the IP Phone users, by seamlessly and transparently 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.

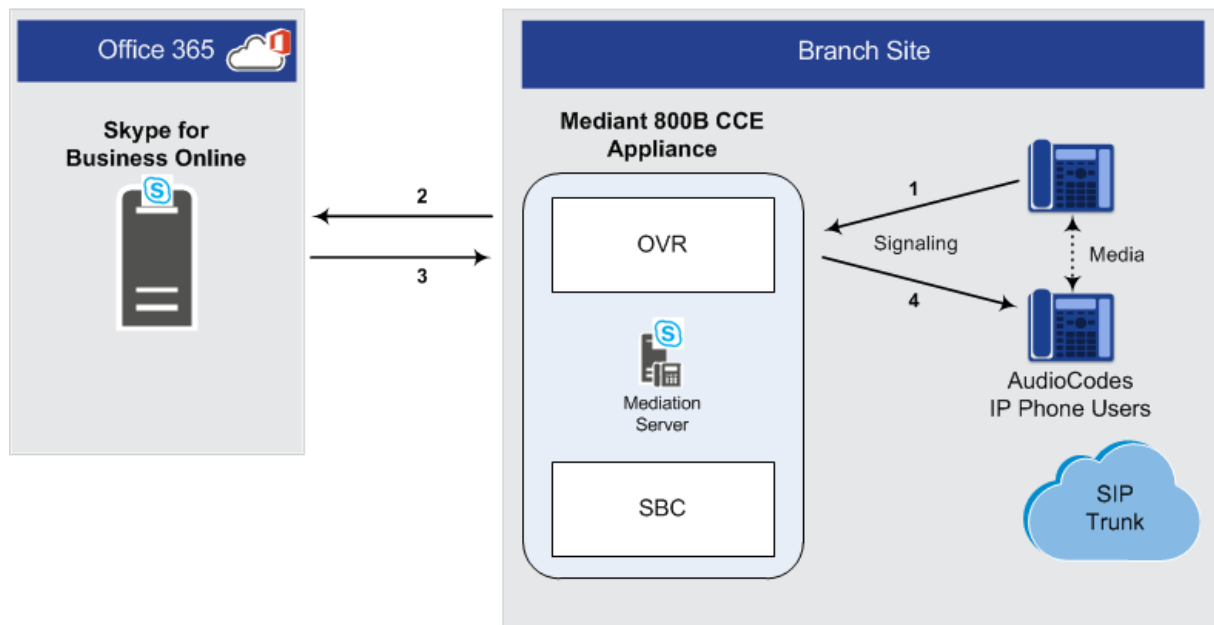
Direct media passes between the IP phones (media does not traverse OVR). When a call is escalated to the PSTN, in the current CCE version, the media from the IP Phone will pass through the Mediation server (in the next version of the CCE Appliance when Cloud PBX will support Media bypass, the media will 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 → IP Phone

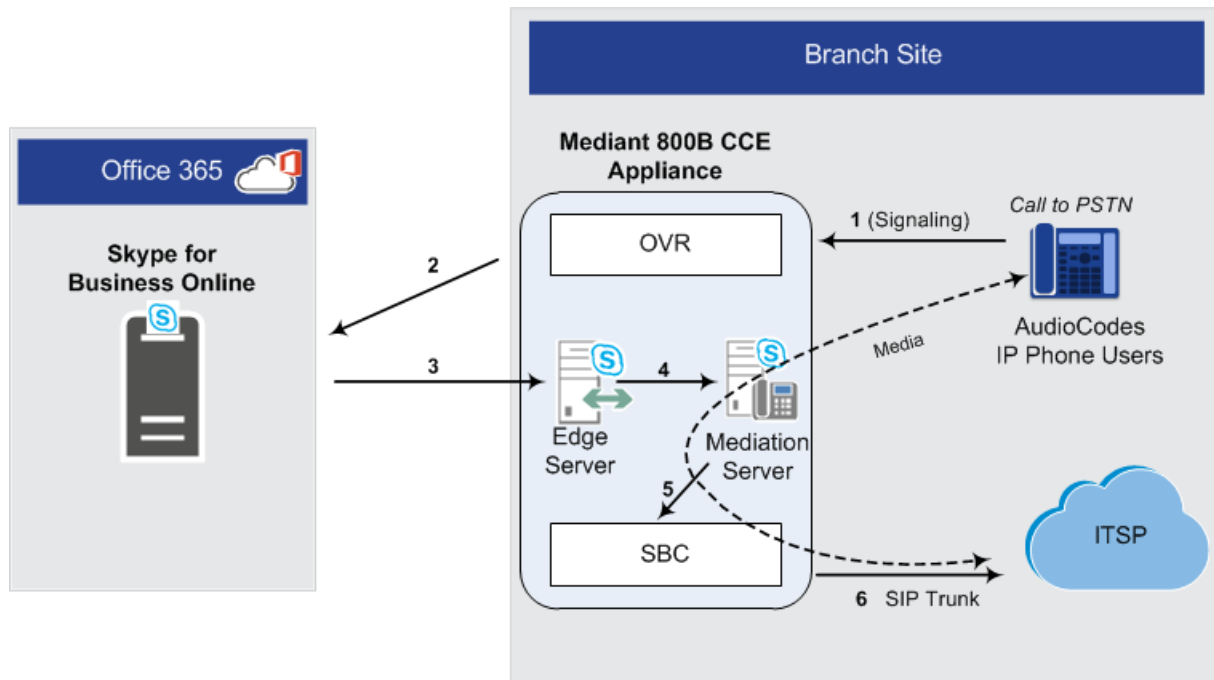
Figure 2-1: Normal Mode - Calls between IP Phones



■ **IP Phone-to-PSTN Calls:**

IP Phone → OVR → Cloud PBX → CCE Edge → CCE Mediation Server → SBC → SIP Trunk

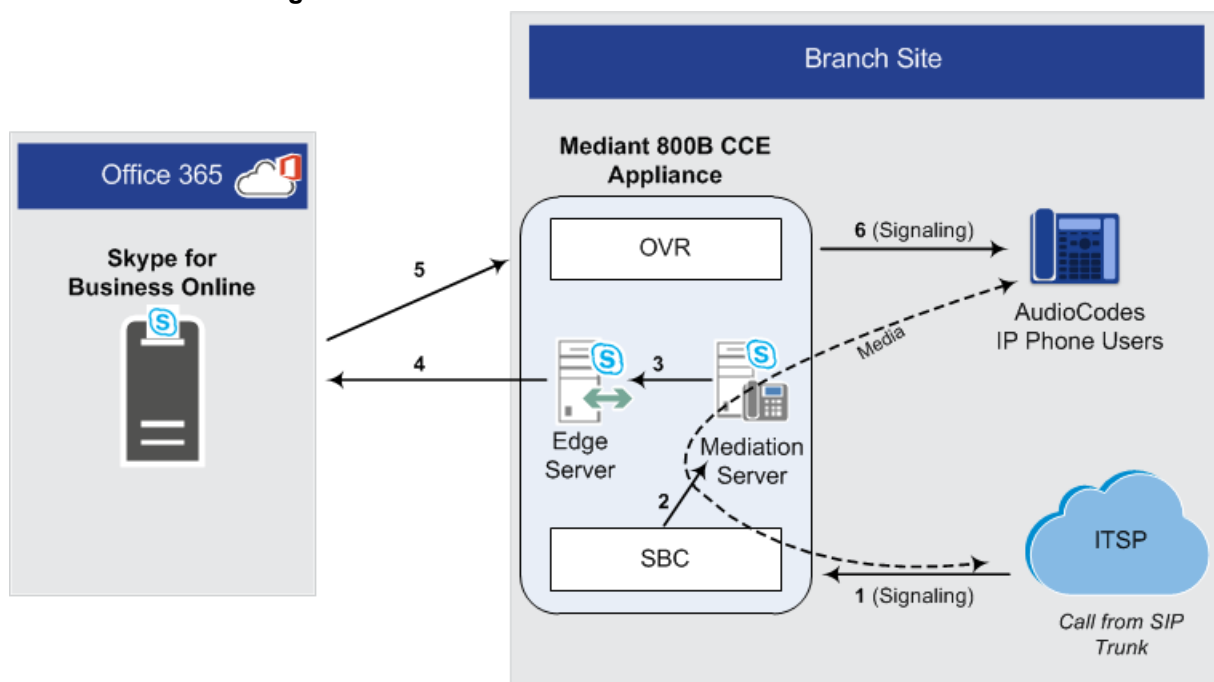
Figure 2-2: Normal Mode - Calls from IP Phone to PSTN



■ **PSTN-to-IP Phone Calls:**

SIP Trunk → SBC → 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 Edge → CCE Mediation Server → SBC → SIP-Trunk

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 3.14).

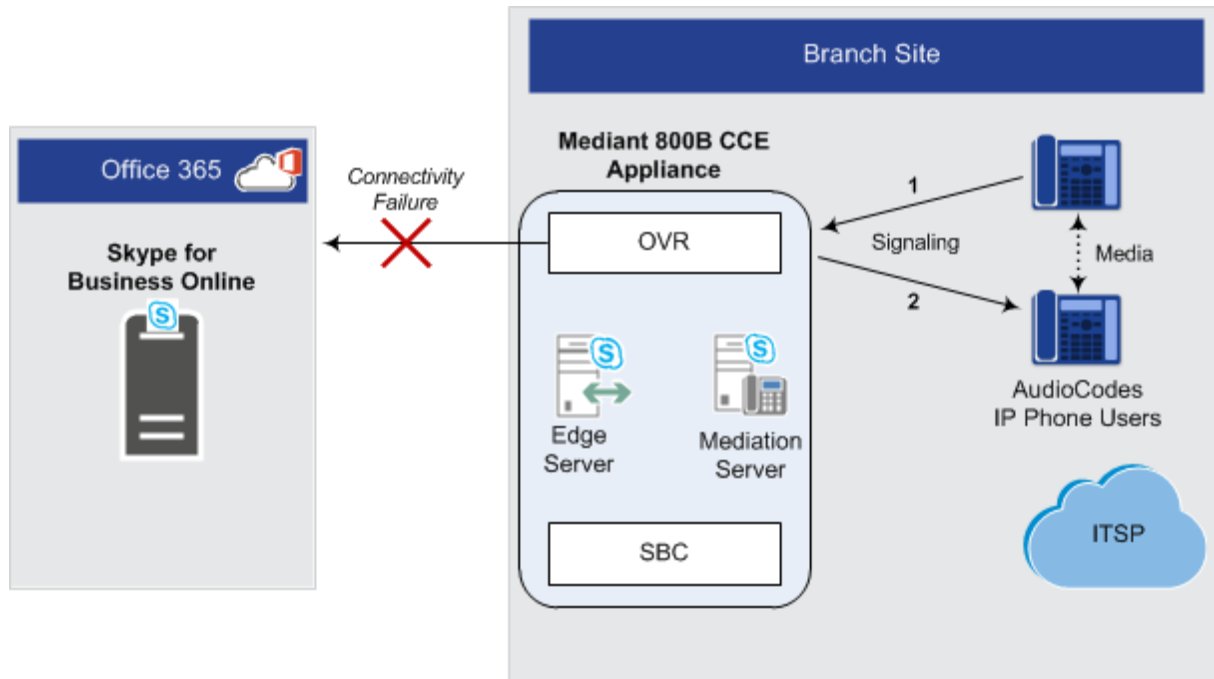
OVR handles call routing based on IP Phone user information that it accumulated during normal operation, as mentioned in Section 2.1. It identifies (classifies) incoming calls as received from IP Phone users based on the caller's IP address and routes the call to the destination based on the called telephone 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:

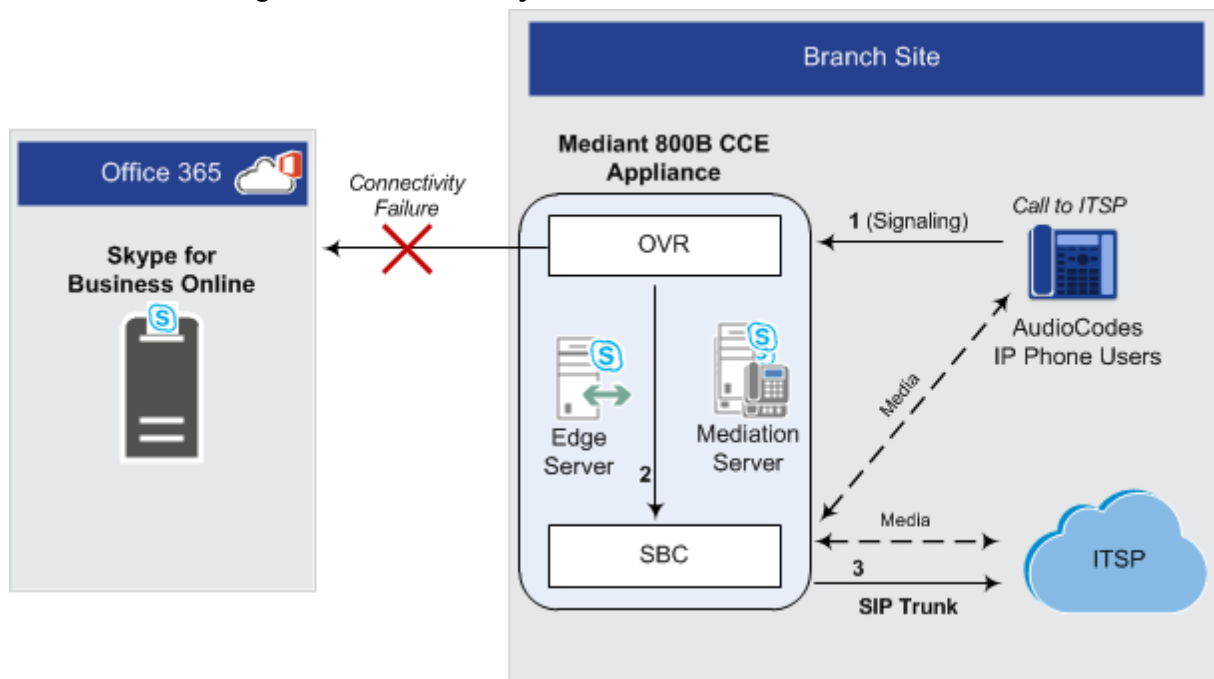
- **IP Phone-to-IP Phone Calls:** IP Phone → OVR → IP Phone

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



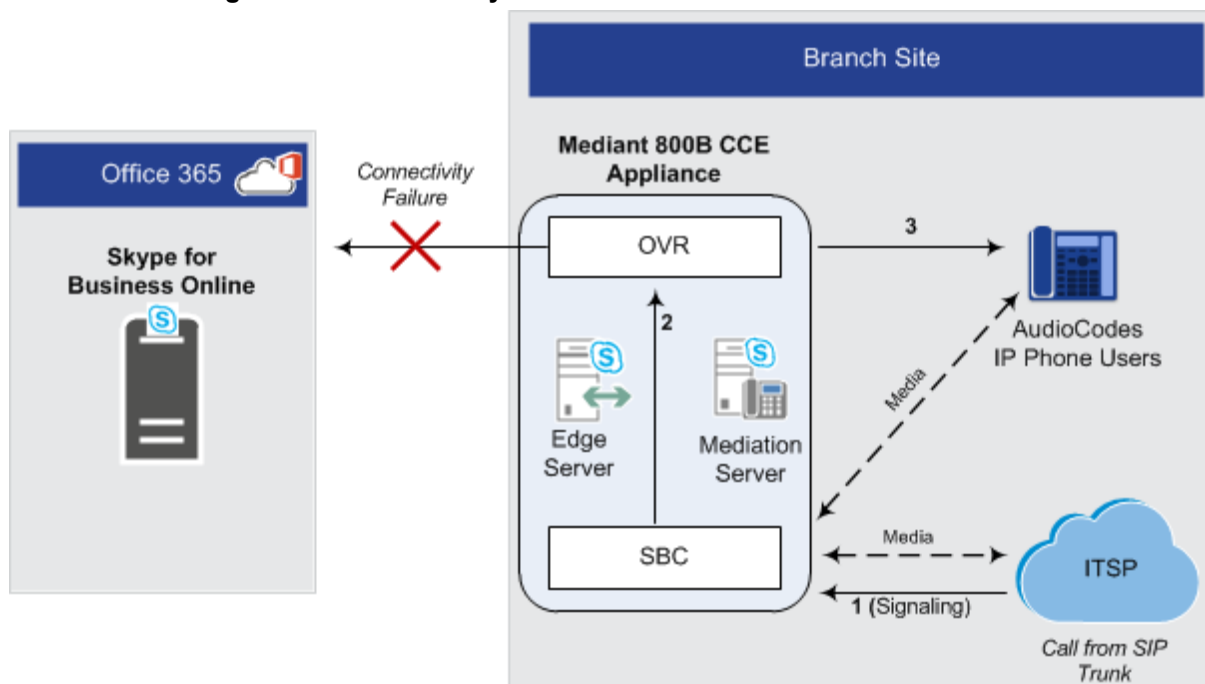
- IP Phone-to-PSTN Calls: IP Phone → OVR → SBC → SIP-Trunk

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



- **PSTN-to-IP Phone Calls: SIP-Trunk → SBC → OVR → IP Phone**

Figure 2-6: Survivability Mode – Calls from SIP Trunk to IP Phone

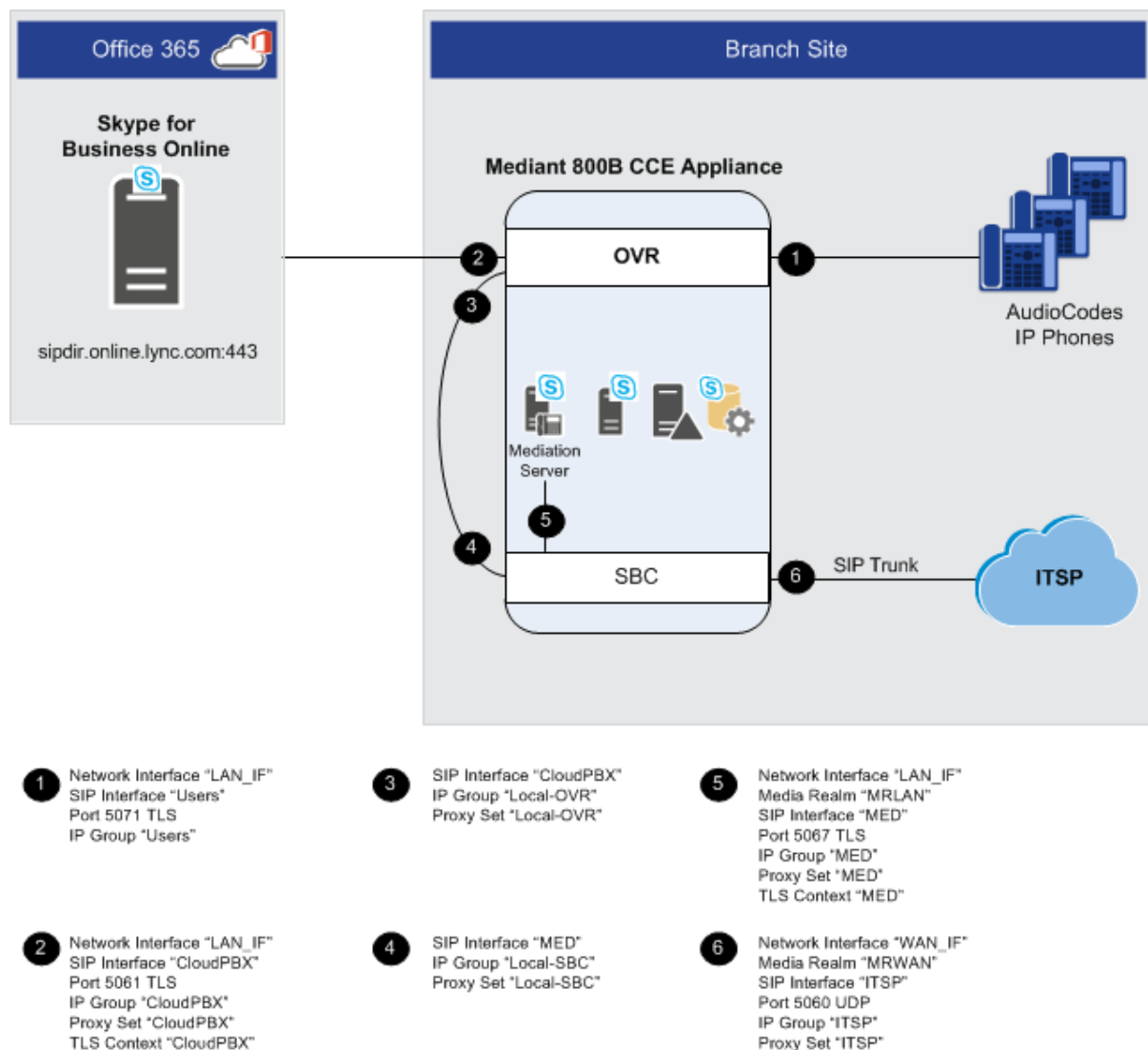


This page is intentionally left blank.

3 Configuring the Device for OVR

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

Figure 3-1: OVR Example Topology and Configuration Entities



Notes:



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

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

Table 3-1: Summary of Required Configuration

Configuration Entity	Configuration Requirement
Network Interface	<p>2 Network Interfaces were configured with the following:</p> <ul style="list-style-type: none"> ▪ LAN network interface of 10.15.44.112. runs SIP signaling, Media and OAMP. ▪ WAN network interface of 195.189.192.111 runs SIP signaling and Media.
TLS Contexts	<p>TLS certification (TLS Context) is required for the following:</p> <ul style="list-style-type: none"> ▪ Traffic between SBC 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.
Media Realm	<p>2 Media Realm were configured with the following:</p> <ul style="list-style-type: none"> ▪ LAN Media Realm for media traffic for CCE Mediation Server used with a port range of 6000-6999 on the LAN network interface. ▪ WAN Media Realm for media traffic for SIP Trunk used with a port range of 7000-7999 on the WAN network interface.
SIP Interfaces	<p>SIP Interfaces need to be configured for the following:</p> <ul style="list-style-type: none"> ▪ CCE Mediation Server ("MED"): Interfaces with CCE Mediation Server. ▪ Cloud PBX ("CloudPBX"): Interfaces with the Cloud PBX (port 5061). A TLS Context (TLS certificate) must be associated with the interface. ▪ Skype users ("Users"): Interfaces with Skype for Business users (IP Phones) at branch site (port 5071). ▪ SIP Trunk Provider ("ITSP"): Interfaces with SIP-Trunk at branch site (port 5060).
Proxy Sets	<p>Proxy Sets need to be configured for the following:</p> <ul style="list-style-type: none"> ▪ CCE Mediation Server ("MED"): Address and port of the CCE Mediation Server. The address can be an FQDN that is resolved into several IP addresses. ▪ Cloud PBX ("CloudPBX"): Address and port of the Cloud PBX (only a single IP address). ▪ SIP Trunk Provider ("ITSP"): Address and port of the ITSP. ▪ Local SBC ("Local-SBC"): Internal device leg entity that represents the SBC leg. ▪ Local OVR ("Local-OVR"): Internal device leg entity that represents the OVR leg.
IP Groups	<p>IP Groups need to be configured for the following:</p> <ul style="list-style-type: none"> ▪ CCE Mediation Server ("MED"): Server-type IP Group for the CCE Mediation Server. A typical IP Profile for interoperating with Skype for Business must be associated. The IP Group's mode of operation must be set to default. ▪ Cloud PBX ("CloudPBX"): Server-type IP Group for the CloudPBX. The IP Group's mode of operation must be set to Microsoft Server. It is recommended not associate an IP Profile. ▪ Skype users ("Users"): User-type IP Group for Skype for Business users (IP Phones). The IP Group's mode of operation must be set to Microsoft Server. When the device is in HA mode, an IP Profile must be associated. ▪ SIP Trunk Provider ("ITSP"): Server-type IP Group for the Sip Trunk. A typical IP Profile for interoperating with ITSP need to be associated. The IP Group's mode of operation must be set to default. ▪ Local SBC ("Local-SBC"): Internal IP Group that represents the SBC leg. ▪ Local OVR ("Local-OVR"): Internal IP Group that represents the OVR leg.
Classification Rules	<p>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).</p>

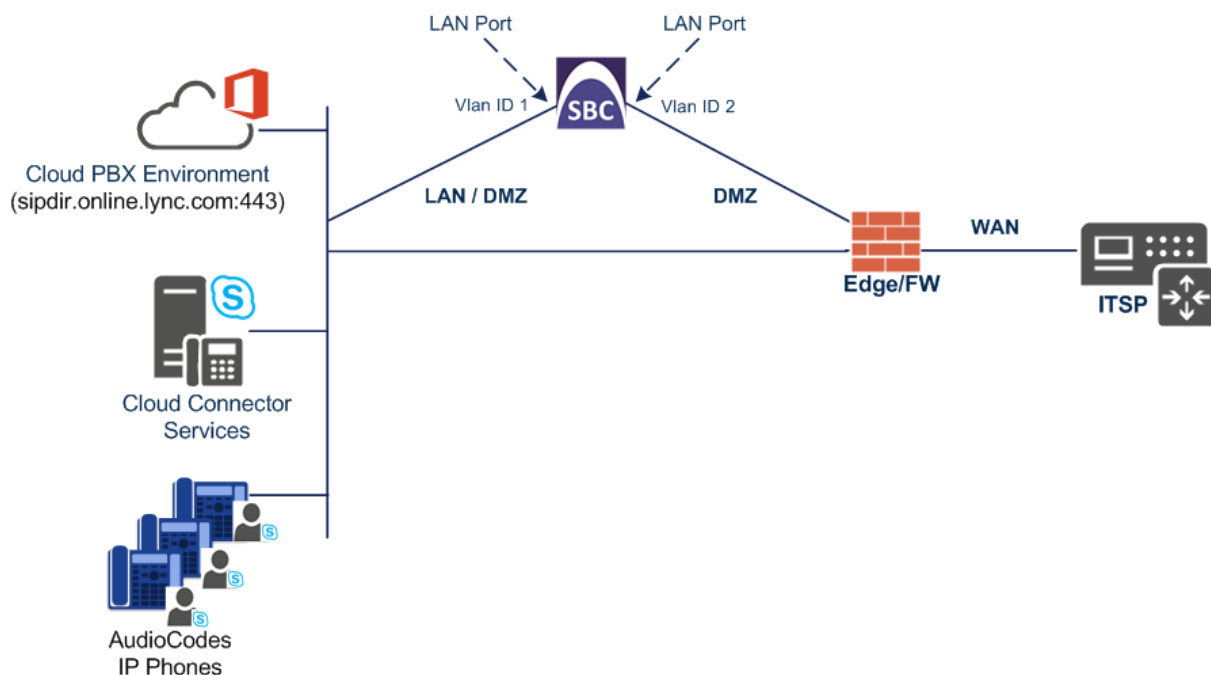
Configuration Entity	Configuration Requirement			
SBC IP-to-IP Routing Rules	Rule	Call Scenario	From (Source)	To (Destination)
	0	Terminate incoming OPTIONS from Mediation / ITSP	Any	Internal
	1	Calls from users to Cloud PBX.	Users	Cloud PBX
	2	Calls between users if unable to route to Cloud PBX (alternative route for 1).	Users	Users
	3	Calls from users to Local-SBC if unable to route to Cloud PBX (alternative route for 1). This is for calls made to the PSTN.	Users	Local-SBC
	4	Calls from Local-SBC to PSTN	Local-SBC	ITSP
	5	Calls from Cloud PBX to users.	Cloud PBX	Users
	6	Calls from PSTN to CCE Mediation Server	ITSP	MED
	7	Call Transfer from users in Resiliency mode (alternative route for 6)	ITSP	Local-OVR
	8	Calls from PSTN to Local-OVR if unable to route to CCE Mediation Server (alternative route for 6) This is for calls made to the Users	ITSP	Local-OVR
	9	Calls from Local-OVR to Users	Local-OVR	Users
	10	Calls from Mediation to PSTN	MED	ITSP

3.1 Step 1: IP Network Interfaces Configuration

This step describes how to configure the SBC's IP network interfaces. There are several ways to deploy the SBC; however, this interoperability test topology employs the following deployment method:

- SBC interfaces with the following IP entities:
 - Cloud Connector Edition, located on the LAN
 - Connectivity to the Cloud PBX Environment is through the LAN
 - ITSP SIP Trunk, located on the WAN
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, SBC connects to the LAN and DMZ using dedicated LAN ports (i.e., two physical ports are used).
- SBC also uses two logical network interfaces:
 - LAN (VLAN ID 1)
 - DMZ (VLAN ID 2)

Figure 3-2: Network Interfaces in Interoperability Test Topology



3.1.1 Step 1a: Configure VLANs

This step describes how to define VLANs for each of the following interfaces:

LAN VoIP (assigned the name "LAN_IF")

WAN VoIP (assigned the name "WAN_IF")

To configure the VLANs:

1. Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
Add another VLAN ID 2 for the WAN side as follows:

Parameter	Value
Index	1
VLAN ID	2
Underlying Interface	GROUP_2 (Ethernet port group)
Name	vlan 2
Tagging	Untagged

Figure 3-3: Configured VLAN IDs in Ethernet Device

Ethernet Devices (2)				
<div> + New Edit 🗑️ </div> <div> Page 1 of 1 Show 10 records per page </div>				
INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

3.1.2 Step 1b: Configure Network Interfaces

This step describes how to configure the IP network interfaces for each of the following interfaces:

LAN VoIP (assigned the name "LAN_IF")

WAN VoIP (assigned the name "WAN_IF")

To configure the IP network interfaces:

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Modify the existing LAN network interface:
 - a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
 - b. Configure the interface as follows:

Parameter	Value
Name	LAN_IF (arbitrary descriptive name)
Ethernet Device	vlan 1
IP Address	10.15.45.112 (LAN IP address of SBC)
Prefix Length	16 (i.e., 255.255.0.0)
Default Gateway	10.15.0.1 (LAN router's IP address)
Primary DNS	10.15.28.1

3. Add a network interface for the WAN side:
 - a. Click **New**.
 - b. Configure the interface as follows:

Parameter	Value
Name	WAN_IF
Application Type	Media + Control
Ethernet Device	vlan 2
IP Address	195.189.192.141 (DMZ IP address of SBC)
Prefix Length	25 (subnet mask in bits for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
Primary DNS	8.8.8.8

The configured IP network interfaces are shown below:

Figure 3-4: Configured Network Interfaces in IP Interfaces Table

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.45.112	16	10.15.0.1	10.15.28.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.141	25	195.189.192.129	8.8.8.8	0.0.0.0	vlan 2

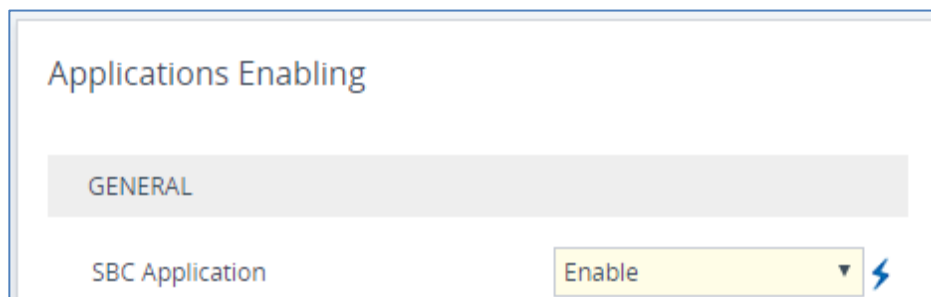
3.2 Step 2: Enable the SBC Application

This step describes how to 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**).

Figure 3-5: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select Enable.
3. Click Apply.
4. Reset the SBC with a burn to flash for this setting to take effect (see Section 3.14 on page 50).

3.3 Step 3: SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the Skype for Business Server 2015 CCE Mediation Server. This is essential for a secure SIP TLS connection.

3.3.1 Step 3a: Configure the NTP Server Address

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 SBC 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 Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.27.1**).

Figure 3-6: Configuring NTP Server Address

NTP SERVER	
Primary NTP Server Address (IP or FQDN)	• 10.15.27.1
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**.

3.3.2 Step 3b: Configure TLS for CCE Mediation Server

This step describes how to configure the SBC for using a TLS connection with the Skype for Business Server 2015 CCE Mediation Server. This is essential for a secure SIP TLS connection.

3.3.2.1 Configure TLS Version

This section describes how to configure the SBC to use TLS only. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➤ **Configure TLS version:**

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

Figure 3-7: Configuring TLS version

The screenshot shows the 'TLS Contexts [MED]' configuration window. It is divided into two main sections: 'GENERAL' and 'OCSP'.
GENERAL Section:
 - Index: 0
 - Name: MED
 - TLS Version: TLSv1.0 TLSv1.1 and TLSv1.2 (selected, indicated by a black arrow)
 - DTLS Version: Any
 - Cipher Server: RC4-AES128
 - Cipher Client: DEFAULT
 - Strict Certificate Extension Validation: Disable
 - DH key Size: 1024
OCSP Section:
 - OSCP Server: Disable
 - Primary OSCP Server: (empty field)
 - Secondary OSCP Server: (empty field)
 - OSCP Port: 2560
 - OSCP Default Response: Reject
 At the bottom of the window are 'Cancel' and 'APPLY' buttons.

4. Click **Apply**.

3.3.2.2 Configure Certificate

This section describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the SBC to authenticate the connection with Skype for Business 2015 CCE Mediation Server. 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 SBC.

To configure a certificate:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below 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 SBC FQDN name (e.g., **ITSP.S4B.interop**).
 - b. Fill in the rest of the request fields according to your security provider's instructions.
 - c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 3-8: Certificate Signing Request – Creating CSR

[TLS Context \[#0\] > Context Certificates](#)

CERTIFICATE SIGNING REQUEST

Subject Name [CN]

ITSP.S4B.interop

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

Signature Algorithm

SHA-1

Create CSR

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

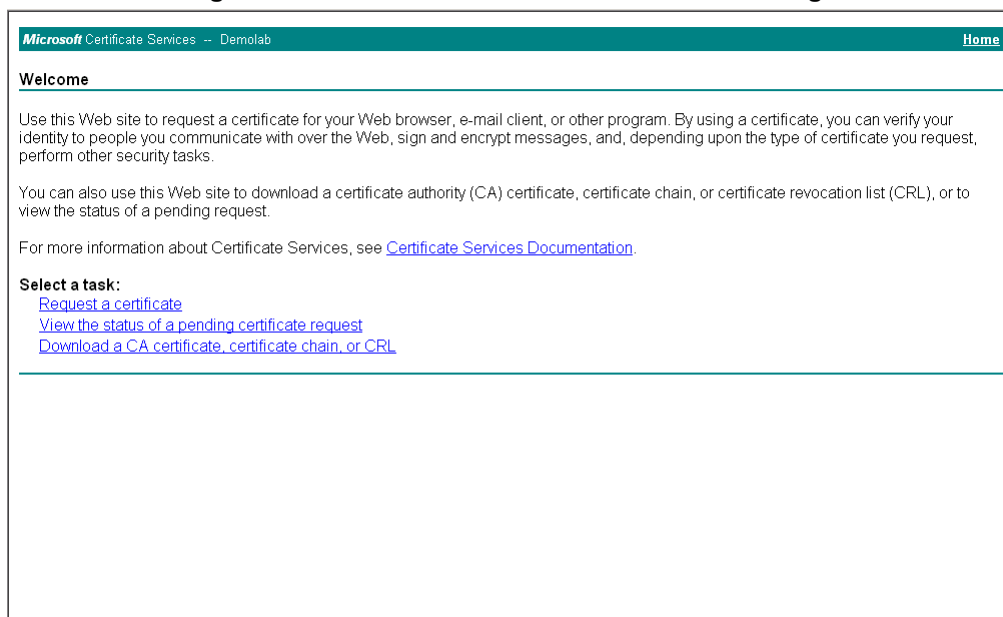
```

-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAlBADAQABAgQwFwYDVQDD8B3VFNQL1M0Q15pbmR1cm9wMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBggQzEs8XTnY8be/t77eEDG7rTg747GQ30DFOC4Rs
x+e9KfErZgxMYqGT8u04AU0wU9LUPkq+8gI6w2bg3boW0kg/9hrnNL2rf1tGcn
30oShP05PiKMRNznCC090b03tbr9kuHmlwPRQ7yT6k7xS3XBbSigqT4LQbjBT1tt
hDH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAIm/GA2E1ZQbZaR6CZyIaw11T
u65w450NFHmaC1uHSyZ8keM8d1Ux14hkw7t5ygAD8KbxVkhRVAcgcQrAK2v8u1Pf
TvN+bwJ+kQ0d59CiXa82e0o1WB3buPq5+qWDGTF+MyJWGVf8SIc1c6+zFoc+BEZY
7tQ8y0J8od0aDhStDfQ=
-----END CERTIFICATE REQUEST-----

```

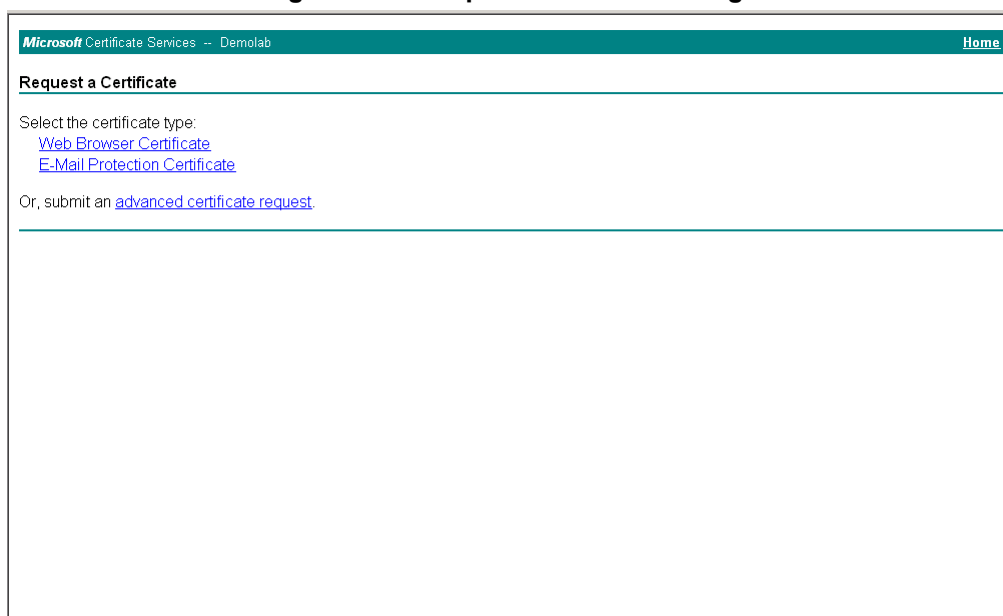
4. Copy the CSR from the line "**-----BEGIN CERTIFICATE REQUEST-----**" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
5. Open a Web browser and navigate to the Microsoft Certificates Services website at <http://<certificate server>/CertSrv>.

Figure 3-9: Microsoft Certificate Services Web Page



6. Click **Request a certificate**.

Figure 3-10: Request a Certificate Page



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

Figure 3-11: Advanced Certificate Request Page

Microsoft Certificate Services -- Demolab Home

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.](#)

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

Figure 3-12: Submit a Certificate Request or Renewal Request Page

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

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:

```

λ8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxvyKk1
rr4ootrnsPOCAuEAAaAAHAOGCSqGS Ib3DOEBBAUA
HnkHAAx8xHg9gaAgoLKmuch2Bo2m4gEcOGAFT8ok
9fSm8c4Bj81b+R5+YI+Ost.57xT9DZXNg5Yp4G+OB
vnQuXOUUX6BzVBT71aO83HcA
-----END CERTIFICATE REQUEST-----

```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >


- Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the 'Saved Request' field.
- From the 'Certificate Template' drop-down list, select **Web Server**.
- Click **Submit**.

Figure 3-13: Certificate Issued Page

Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)

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

Figure 3-14: Download a CA Certificate, Certificate Chain, or CRL Page

Microsoft Certificate Services -- Demolab Home

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](#)

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

19. In the SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; 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 13, and then click **Send File** to upload the certificate to the SBC.

Figure 3-15: Upload Device Certificate Files from your Computer Group

20. In the SBC's Web interface, return to the **TLS Contexts** page.
 - a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
 - b. Click the **Import** button, and then select the certificate file to load.

Figure 3-16: Importing Root Certificate into Trusted Certificates Store

21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the SBC with a burn to flash for your settings to take effect (see Section 3.14 on page 50).

3.3.3 Step 3c: 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 Add Row dialog box, configure the TLS Context as shown below:

Figure 3-17: Configuring TLS Context for Cloud PBX

The screenshot shows the 'TLS Contexts [FE]' configuration window. It has two tabs: 'GENERAL' and 'OCSP'. The 'GENERAL' tab is active, showing the following fields:

Field	Value
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

The 'OCSP' tab is also visible, showing the following fields:

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

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

3. Click **Apply**.

3.4 Step 4: Configure SRTP

As the 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**).

Figure 3-18: Configuring SRTP

Media Security

GENERAL		AUTHENTICATION & ENCRYPTION	
Media Security	Enable	Authentication On Transmitted RTP Packets	Active
Media Security Behavior	Preferable	Encryption On Transmitted RTP Packets	Active
Offered SRTP Cipher Suites	All	Encryption On Transmitted RTCP Packets	Active
Aria Protocol Support	Disable	SRTP Tunneling Authentication for RTP	Disable
		SRTP Tunneling Authentication for RTCP	Disable

MASTER KEY IDENTIFIER		GATEWAY SETTINGS	
Master Key Identifier (MKI) Size	0	Enable Rekey After 181	Disable
Symmetric MKI	Disable		

2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.
4. Reset the SBC with a burn to flash for your settings to take effect (see Section 3.14 on page 50).

3.5 Step 5: Configure Media Realms

This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Click **New**, and then in the Add Row dialog box, add a Media Realm.

In the example setup, add Media Realm with the following configuration:

Media Realm	Specific Configuration			
	Name	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
Interfacing with LAN	LAN_Realm	LAN_IF	6000	100
Interfacing with WAN	WAN_Realm	WAN_IF	7000	100

the configured Media Realms are shown in the figure below:

Figure 4-7: Configured Media Realms in Media Realm Table

INDEX ↕	NAME	IPv4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	LAN_Realm	LAN_IF	6000	100	6999	Yes
1	WAN_Realm	WAN_IF	7000	100	7999	No

3.6 Step 6: 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 Infrastructure Skype for Business users (IP Phones) at branch site
- SIP-Trunk - ITSP

➤ To add SIP Interfaces:

1. Open the SIP Interface table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Click **New**, and then in the Add Row dialog box, add a SIP Interface.

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

SIP Interface	Specific Configuration					
	Name	Network Interface	Application Type	UDP Port	TLS Port	TLS Context Name
Interfacing with CCE Mediation Server	MED	LAN_IF	SBC	0	5067	MED
Interfacing with Cloud PBX	Cloud PBX	LAN_IF	SBC	0	5061	FE
Interfacing with IP Phone users	Users	LAN_IF	SBC	0	5071	-
Interfacing with ITSP	ITSP	WAN_IF	SBC	5060	0	-

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

The figure below displays the configured SIP Interfaces:

Figure 3-19: Configured SIP Interfaces

The configured SIP Interfaces are shown in the figure below:

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	MED	DefaultSRD (i)	Voice	SBC	0	0	5067	No encapsulation	--
1	CloudPBX	DefaultSRD (i)	Voice	SBC	0	0	5061	No encapsulation	--
2	Users	DefaultSRD (i)	Voice	SBC	0	0	5071	No encapsulation	--
3	ITSP	DefaultSRD (i)	WAN_IF	SBC	5060	0	0	No encapsulation	--

3.7 Step 7: 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 Infrastructure
- SIP Trunk
- Entity to reach the local SBC
- Entity to reach the local OVR

➤ **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 Add Row dialog box, configure a Proxy Set.

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

Proxy Set	Configuration						
	Name	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	Cloud PBX	Cloud PBX	Using OPTIONS	30	FE	Round Robin	-
SIP Trunk	ITSP	ITSP	-	-	-	-	-
Entity to reach local SBC	Local-SBC	MED	-	-	-	-	-
Entity to reach local OVR	Local-OVR	CloudPBX	-	-	-	-	-

The figure below displays the configured Proxy Sets:

Figure 3-20: 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	Homing	Enable
1	CloudPBX	DefaultSRD (#0)	--	CloudPBX	30		Disable
2	ITSP	DefaultSRD (#0)	--	ITSP	60		Disable
3	Local-SBC	DefaultSRD (#0)	--	MED	60		Disable
4	Local-OVR	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 Table** 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 Name	Configuration	
	Proxy Address	Transport Type
MED	MEDserver.ES4B.interop:5067	TLS
CloudPBX	sipdir.online.lync.com:443	TLS
ITSP	Itsp.com:5060	UDP
Local-SBC	127.0.0.1:5067	TLS
Local-OVR	127.0.0.1:5061	TLS

3.8 Step 8: 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, the following IP Profile needs to be configured for:

- Microsoft Skype for Business CCE Mediation Server – to operate in secure mode using SRTP
- SIP trunk – to operate in non-secure mode using RTP for this ITSP
- Local-SBC – to operate in secure mode using SRTP
- 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 IP Profiles:**

1. Open the IP Profile Settings table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Add the following IP Profiles, using the **New** button:
 - **CCE Mediation Server:**

Parameter	Value
General	
Index	1
Name	MED
Media Security	
SBC Media Security Mode	SRTP
Symmetric MKI	Enable
MKI Size	1
Enforce MKI Size	Enforce
Reset SRTP State Upon Re-key	Enable
Generate SRTP Keys Mode:	Always
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Signaling	
Remote Update Support	Supported Only After Connect
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)

Parameter	Value
Remote 3xx Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)

- ITSP SIP Trunk:

Parameter	Value
General	
Index	2
Name	ITSP
Media Security	
SBC Media Security Mode	RTP
SBC Early Media	
Remote Can Play Ringback	No (required, as Skype for Business Server 2015 does not provide a ringback tone for incoming calls)
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally (required, as for ITSP not support receipt of SIP REFER)

- Local-OVR IP Profile:

Parameter	Value
General	
Index	3
Name	Local-OVR
Media Security	
SBC Media Security Mode	SRTP
SBC Signaling	
Remote Delayed Offer Support	Not Supported

- **Skype users:**

Parameter	Value
General	
Index	4
Name	Users
SBC Signaling	
Session Expires Mode	Observer

3.9 Step 9: 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 for Business users (IP Phones) at branch site
- SIP Trunk
- Local SBC
- Local OVR

➤ **To configure IP Groups:**

1. Open the IP Group Table page (**Setup menu > Signaling & Media tab > Core Entities folder > IP Groups**).
2. Click **New**, and then in the Add Row dialog box, configure an IP Group.

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

IP Group	Specific Configuration							
	Name	Type	Proxy Set	IP Profile	Media Realm	SBC Operation Mode	Inbound Message Manipulation Set	Outbound Message Manipulation Set
CCE Mediation Server	MED	Server	MED	MED	LAN_Realm	B2BUA	-	-
Cloud PBX	CloudPBX	Server	CloudPBX	-	-	Microsoft Server	-	-
IPP Users	Users	User	-	Users	-	Microsoft Server	-	-
SIP Trunk	ITSP	Server	ITSP	ITSP	WAN_Realm	B2BUA	-	-
Local SBC	Local-SBC	Server	Local-SBC	-	LAN_Realm	B2BUA	4 (configured in Section 3.12)	5 (configured in Section 3.12)
Local OVR	Local-OVR	Server	Local-OVR	Local-OVR	LAN_Realm	B2BUA	-	5 (configured in Section 3.12)

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	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATING SET	OUTBOUND MESSAGE MANIPULATING SET
0	MED	DefaultSR	Server	B2BUA	MED	MED	LAN_Realm		Enable	-1	-1
1	CloudPBX	DefaultSR	Server	Microsoft Serv	CloudPBX	--	--		Enable	-1	-1
2	Users	DefaultSR	User	Microsoft Serv	--	--	--		Enable	-1	-1
3	ITSP	DefaultSR	Server	B2BUA	ITSP	ITSP	WAN_Realm		Enable	-1	-1
4	Local-SBC	DefaultSR	Server	B2BUA	Local-SBC	--	LAN_Realm		Enable	4	5
5	Local-OVR	DefaultSR	Server	B2BUA	Local-OVR	SRTP	LAN_Realm		Enable	-1	5

3.10 Step 10: 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, *ES4B.interop* 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 Table**).
2. Click **New**, and then configure the parameters as shown below:

Parameter	Value
General	
Index	0
Name	Users
Source SIP Interface	Users
Source Host	ES4B.interop
Action Type	Allow
Source IP Group	Users

Figure 3-22: Configured Classification Table for Users

INDEX	NAME	SRD	SOURCE SIP INTERFACE	SOURCE USERNAME PREFIX	SOURCE HOST	DESTINATION USERNAME PREFIX	DESTINATION HOST	ACTION TYPE	SOURCE IP GROUP
0	Users	DefaultSRD (i)	Users	*	ES4B.interop	*	*	Allow	Users

3.11 Step 11: 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 Local-SBC (alternative route for above)
- Routing calls from Local-SBC to ITSP
- Routing calls from Cloud PBX to Users
- Routing calls from ITSP to CCE Mediation Server
- Routing ITSP Transferred calls to Request URI (alternative route for above)
- Routing calls from ITSP to Local-OVR (alternative route for above)
- Routing calls from Local-OVR to User
- Routing calls from CCE Mediation Server to ITSP

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

1. Open the IP-to-IP Routing Table page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Click **New**, and then configure the parameters as shown below:

IP-to-IP Routing Rule	Specific Configuration					
	Name	Alternative Route Options	Source IP Group	Request Type	Destination Type	Destination IP Group
Terminate OPTIONS	Terminate Options	Route Row	Any	OPTIONS	Dest Address	internal
Users → Cloud PBX	User-CloudPBX	Route Row	Users	All	IP Group	CloudPBX
Users → Users (alternative route for above)	User-User	Alternative Route Consider Inputs	Users	INVITE and REGISTER	IP Group	Users
Users → Local SBC (alternative route for above)	User-Local SBC	Alternative Route Consider Inputs	Users	INVITE and REGISTER	IP Group	Local-SBC
Local-SBC → ITSP	Local-SBC-ITSP	Route Row	Local-SBC	All	IP Group	ITSP
Cloud PBX → Users	CloudPBX-Users	Route Row	CloudPBX	All	IP Group	Users
ITSP → CCE Mediation Server	ITSP-MED	Route Row	ITSP	All	IP Group	MED

IP-to-IP Routing Rule	Specific Configuration					
	Name	Alternative Route Options	Source IP Group	Request Type	Destination Type	Destination IP Group
Users Transfer with ITSP calls	REFER	Alternative Route Consider Inputs	ITSP	All	Request URI	Local-OVR
ITSP → Local OVR	ITSP-Local OVR	Alternative Route Consider Inputs	ITSP	All	IP Group	Local-OVR
Local OVR → Users	Local OVR - Users	Route Row	Local-OVR	All	IP Group	Users
CCE Mediation Server → ITSP	MED-ITSP	Route Row	MED	All	IP Group	ITSP

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

Figure 3-23: Configured IP-to-IP Routing Rules

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate OP	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	User-CloudPB	Default_SBCR	Route Row	Users	All	*	*	IP Group	CloudPBX	--	
2	User-User	Default_SBCR	Alternative Ro	Users	INVITE and RE	*	*	IP Group	Users	--	
3	User-Local SB	Default_SBCR	Alternative Ro	Users	INVITE and RE	*	*	IP Group	Local-SBC	--	
4	Local SBC-ITSP	Default_SBCR	Route Row	Local-SBC	All	*	*	IP Group	ITSP	--	
5	CloudPBX-Us	Default_SBCR	Route Row	CloudPBX	All	*	*	IP Group	Users	--	
6	ITSP-MED	Default_SBCR	Route Row	ITSP	All	*	*	IP Group	MED	--	
9	REFER	Default_SBCR	Alternative Ro	ITSP	All	*	*	Request URI	Local-OVR	--	
10	ITSP-Local OV	Default_SBCR	Alternative Ro	ITSP	All	*	*	IP Group	Local-OVR	--	
11	Local OVR-Us	Default_SBCR	Route Row	Local-OVR	All	*	*	IP Group	Users	--	
12	MED-ITSP	Default_SBCR	Route Row	MED	All	*	*	IP Group	ITSP	--	

3.11.1 Step 11a: Configure SBC Alternative Routing Reasons

This step describes how to configure the SBC's handling of SIP 504 responses received by CCE Mediation Server for outgoing SIP dialog-initiating to the Cloud PBX. In this case SBC performs alternative route for the call to the Local-OVR.

To configure SIP reason codes for alternative IP routing:

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons**).
2. Click **New**.
3. From the 'Release Cause' drop-down list, select **504 Server Timeout**.

Figure 3-24: SBC Alternative Routing Reasons Table

The screenshot shows a configuration window titled "Alternative Routing Reasons". It features a "GENERAL" tab. Within this tab, the "Index" field is set to "0". The "Release Cause" field is a dropdown menu currently displaying "504 Server Timeout". The window concludes with "Cancel" and "APPLY" buttons at the bottom.

4. Click **Apply**.

3.12 Step 12: 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).



Note: Adapt the manipulation table according to your environment dial plan.

➤ **To configure a number manipulation rule:**

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Add + from ITSP
Source IP Group	ITSP
Destination IP Group	Any
Destination Username Prefix	[1-9]
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 3-25: Configuring IP-to-IP Outbound Manipulation Rule

Outbound Manipulations [from ITSP]

GENERAL

Index: 1

Name: Add + From ITSP

Additional Manipulation: No

Call Trigger: Any

MATCH

Request Type: All

Source IP Group: #3 [ITSP]

Destination IP Group: Any

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: [1-9]

ACTION

Manipulated Item: Destination URI

Remove From Left: 0

Remove From Right: 0

Leave From Right: 255

Prefix to Add: +

Suffix to Add:

Privacy Restriction Mode: Transparent

Cancel APPLY

3. Click **Apply**.

3.13 Step 13: Configure Message Manipulation Rules

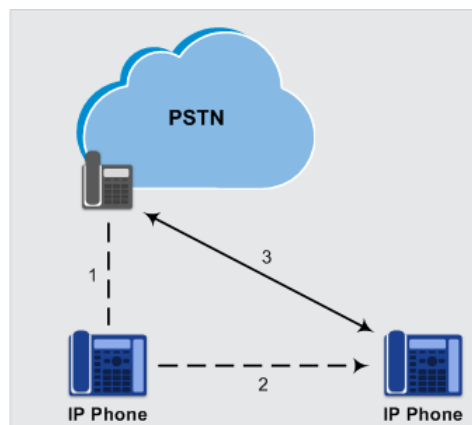
In the example setup, you need to configure manipulation rules for the following:

- 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 SBC to send calls to the ITSP 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.



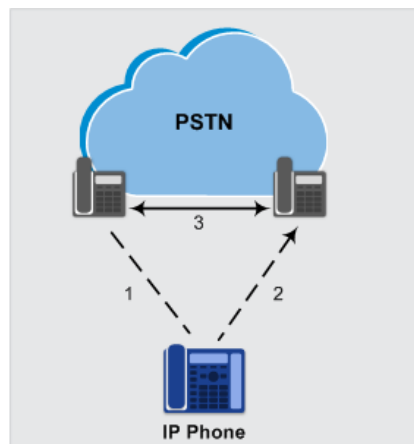
Note: The Message Manipulation Rules described above are only valid in Survivability mode.

Figure 3-26: 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 is changed to TLS.

Figure 3-27: Call Transfer of PSTN Call to Another PSTN User



Once configured, you need to assign the rules to the IP Groups "Local-OVR" and "Local-SBC" (see Section 0), using the Manipulation Set IDs 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 Add Row dialog box, add a Message Manipulation rule. When you have finished, click **Add** to apply your settings. Add the following rules:
 - For setting IP Phone's number as Caller ID for calls to PSTN in survivability mode:

Parameter	Value
Index	0
Name	Change Name to Number
Manipulation Set ID	4
Message Type	invite
Action Subject	header.p-asserted-identity.0
Action Type	Remove

- For transferring a PSTN call to another IP Phone user:

Parameter	Value
Index	1
Name	Refer-To IPP
Manipulation Set ID	5
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	5
Message Type	
Condition	
Action Subject	header.refer-to.url.transporttype
Action Type	Modify
Action Value	'2'
Row Rule	Use Previous Condition

- For transferring a PSTN call to another PSTN user:

Parameter	Value
Index	3
Name	Refer-To PSTN
Manipulation Set ID	5
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	5
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 rules:

Figure 3-28: Configured Message Manipulation Rules

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	change Name to Ni	4	invite		header.P-Asserted-	Remove		Use Current Condi
2	Refer-To IPP	5	refer	header.refer-to.url.	header.refer-to.url.	Modify	param.message.ad	Use Current Condi
3		5			header.refer-to.url.	Modify	'2'	Use Previous Condi
4	Refer-To PSTN	5	refer	header.refer-to.url.	header.refer-to.url.	Modify	param.message.ad	Use Current Condi
5		5			header.refer-to.url.	Modify	'2'	Use Previous Condi

3.14 Step 14: 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 within this period and receive services from it.

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

1. Open the SBC General Settings page (**Setup menu > Signaling & Media tab > SIP Definitions folder > Proxy & Registration**).
2. In the 'User Registration Grace Time' (SBCUserRegistrationGraceTime) field, enter "900" (in seconds).

Figure 3-29: Configuring Graceful Registration Expiry Time

SBC REGISTRATION	
User Registration Time [sec]	<input type="text" value="0"/>
Proxy Registration Time [sec]	<input type="text" value="0"/>
Survivability Registration Time [sec]	<input type="text" value="0"/>
→ User Registration Grace Time [sec]	<input checked="" type="radio"/> <input type="text" value="900"/>
GRUU Mode	<input type="text" value="As Proxy"/> ▼
DB Routing Search Mode	<input type="text" value="All permutations"/> ▼
Shared Line Registration Mode	<input type="text" value="As Configured"/> ▼

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

3.15 Step 15: 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**.

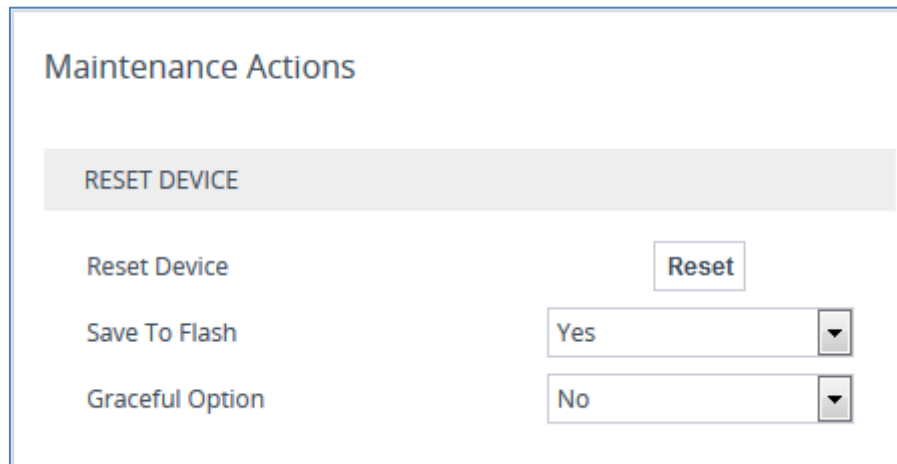
3.16 Step 16: Reset the SBC

After you have completed the configuration of the SBC described in this chapter, save ("burn") the configuration to the SBC's flash memory with a reset for the settings to take effect.

To reset the device through Web interface:

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

Figure 3-30: Resetting the SBC



The screenshot shows the 'Maintenance Actions' web page. At the top, there is a header 'Maintenance Actions'. Below it, a grey bar contains the text 'RESET DEVICE'. Underneath, there are three rows of configuration options. The first row is 'Reset Device' with a 'Reset' button to its right. The second row is 'Save To Flash' with a dropdown menu showing 'Yes'. The third row is 'Graceful Option' with a dropdown menu showing 'No'.

RESET DEVICE	
Reset Device	<input type="button" value="Reset"/>
Save To Flash	<input type="text" value="Yes"/>
Graceful Option	<input type="text" value="No"/>

2. Ensure that the ' Save To Flash' field is set to **Yes** (default).
3. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
4. Click **OK** to confirm device reset.

4 Configuring AudioCodes IP Phones for OVR

This chapter describes the configuration of AudioCodes Skype for Business 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 Skype for Business environment can be summarized in the following steps (in chronological order):

1. Remove the IP Phone from the shipped package.
2. Cable the IP Phone to the network.
3. Cable the IP Phone to the power supply to power up the IP Phone.
4. The IP Phone broadcasts a DHCP message to the network to discover a DHCP server and request information (DHCP Options). (DHCP is enabled by default.)
5. The DHCP server at the Microsoft datacenter responds to the IP Phone with DHCP Options providing, for example, networking settings (IP address and Default Gateway), NTP server address, LDAP server address (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 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

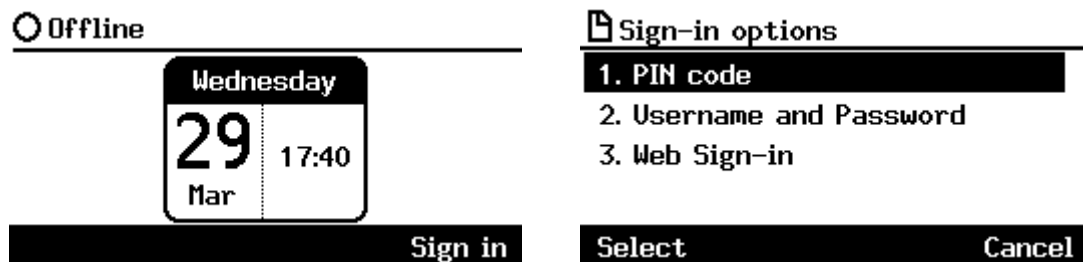
To register the IP Phone with Skype for Business Online /Cloud PBX, the user must perform a sign-in procedure on the IP Phone. Users can sign in using a username-password combination or by using the Cloud PBX Web option.



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 04.2.2



Note:

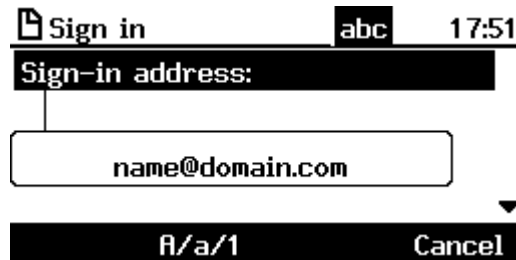
- After signing out, the next time you sign in the phone will present the option that was used to sign in before signing out.
- If a user signs out and another signs in, the phone presents empty Speed Dials and empty Call Logs to the newly signed-in user. The Speed Dials and Call Logs of the signed-out 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**.



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.



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:

<div>  Sign-in options </div> <hr/> <div> 1. PIN code 2. Username and Password 3. Web Sign-in </div> <div> <div>Select</div> <div>Cancel</div> </div>	<div>  Web Sign-in: Timeout 14:56 </div> <hr/> <div> WEB URL: <div>http://aka.ms/sphone</div> </div> <div> Pairing code: <div>CXCWRHPB6</div> </div> <div> <div>Cancel</div> </div>
--	---

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 (e.g., 10.15.45.112) 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 (e.g., 5071) on the outbound proxy (OVR). The valid value range is 1024 to 65535 (default is 5060). Set the parameter to the port of the OVR.

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

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

4.3.1 Configuring IP Phones through the Web Interface

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



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

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

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

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

Use Hosting Outbound Proxy:	Enable ▾
Outbound Proxy IP Address or Host Name:	<input type="text"/>
Outbound Proxy Port:	<input type="text" value="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 (dhcption160.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.

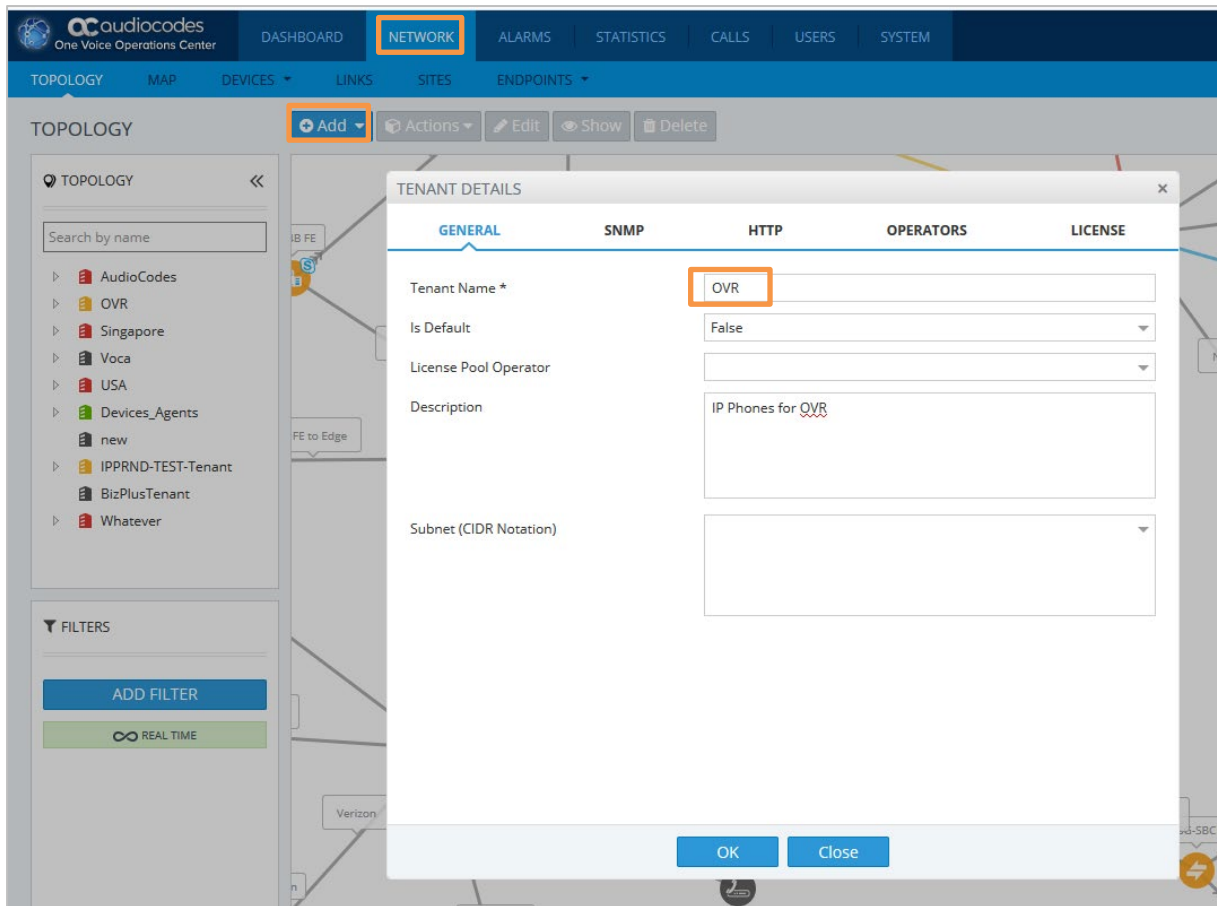
**Note:**

- 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:**

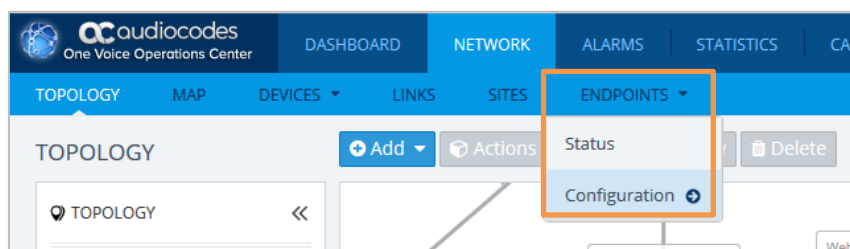
1. Log in to AudioCodes' OVOC.
2. Create a Tenant to represent the IP Phones deployed in the OVR environment:
 - a. Select the **NETWORK** menu.
 - b. Click the **Add** button, and then from the drop-down menu, choose **TENANT**.
 - c. In the 'Tenant Name' field, configure a name for the OVR deployment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

Figure 4-2: Configuring Tenant for OVR in OVOC



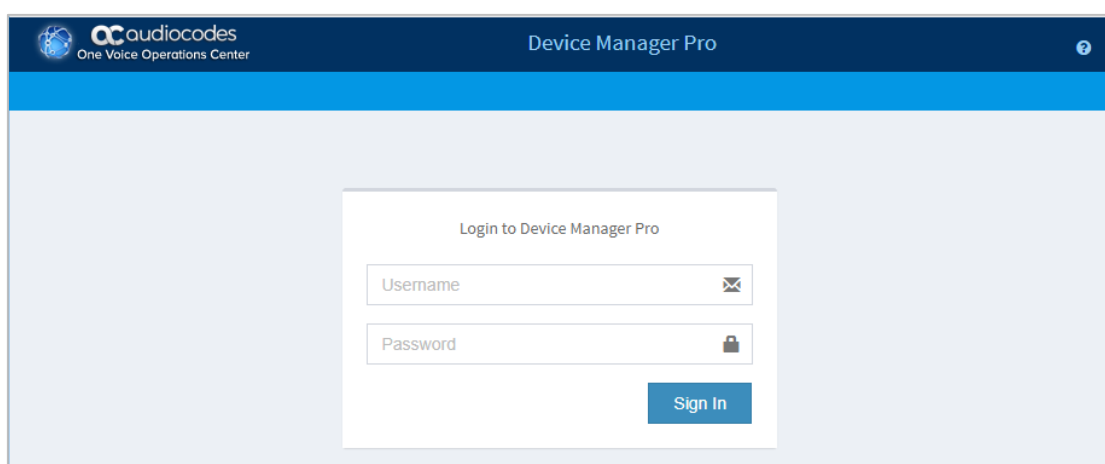
3. Access the Device Manager Pro from OVOC:
 - a. Select the **NETWORK** menu.
 - b. Click **ENDPOINTS**, and then from the drop-down menu, choose **Configuration**.

Figure 4-3: Accessing Device Manager Pro from OVOC



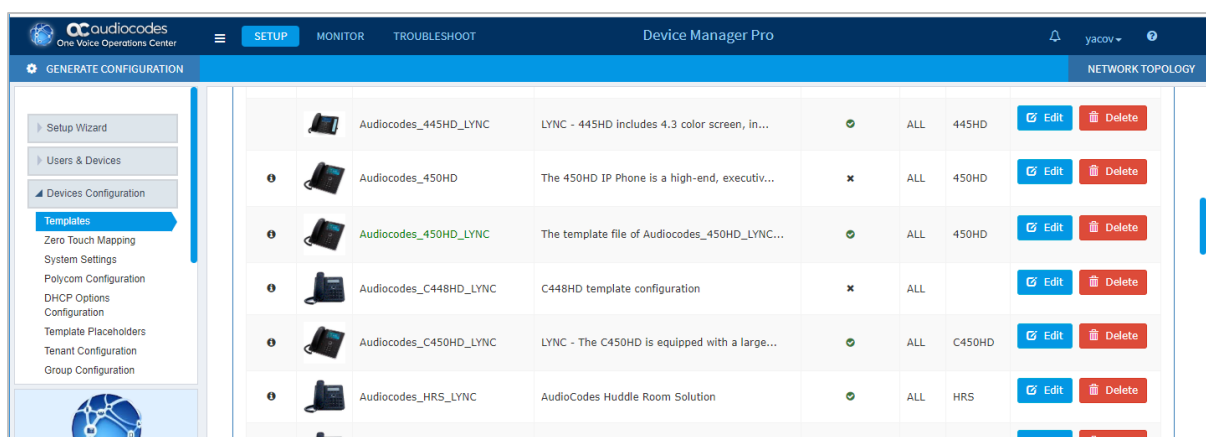
The Login to Device Manager Pro screen appears:

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



- 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

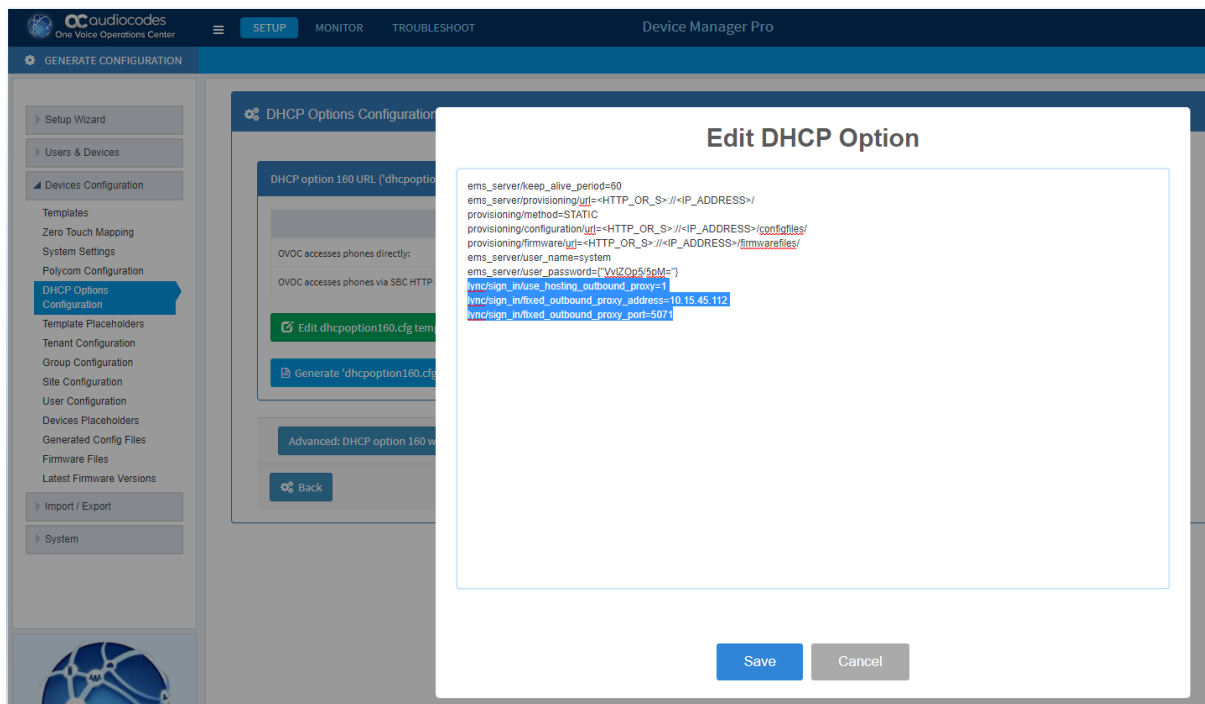
The screenshot displays the 'Device Manager Pro' interface. On the left, a sidebar contains a 'GENERATE CONFIGURATION' section with a 'Templates' link highlighted. The main content area is titled 'Edit configuration template values'. It features two input fields: 'Configuration Key' with the value 'lync/sign_in/fixed_outbound_proxy_address' and 'Configuration Value' with the value '10.15.45.112'. A green 'Add' button is positioned to the right of the 'Configuration Value' field. Below these fields is a table with two columns: 'Configuration Key' and 'Configuration Value'. The table contains two rows of data:

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.

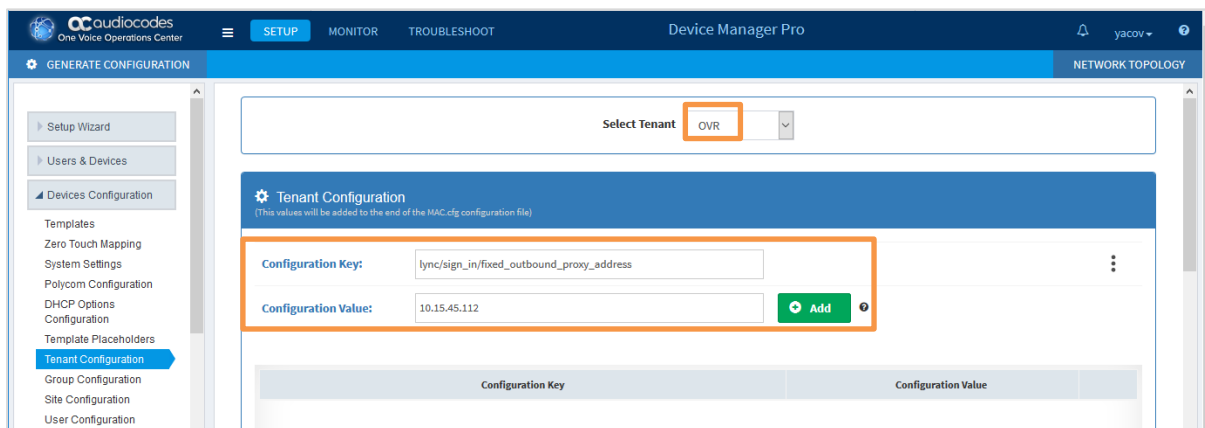
- f. Click the **Edit dhcpoption160.cfg template** button; the Edit DHCP Option dialog box appears.
- g. Copy and paste the parameters with their values (see Step c above) into the text box, as shown highlighted below, and then click **Save**:

Figure 4-7: Configuring DHCP Option 160



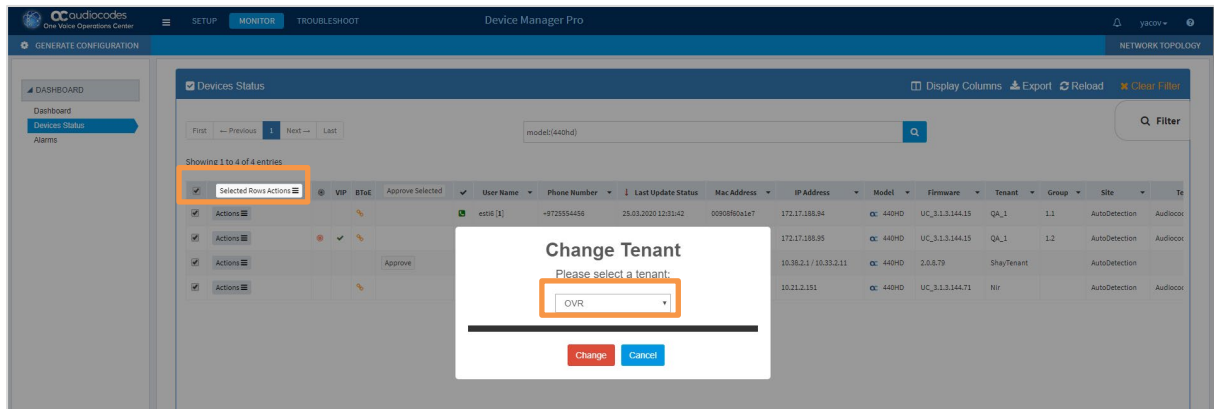
5. (Only Selected IP Phones for OVR Deployment):
 - a. Open the Tenant Configuration page (SETUP menu > **Devices Configuration** folder > **Tenant Configuration**).
 - b. From the 'Select Tenant' drop-down list, select the name of the Tenant that you configured for OVR in OVOC in Step 2 (e.g., "OVR").
 - 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



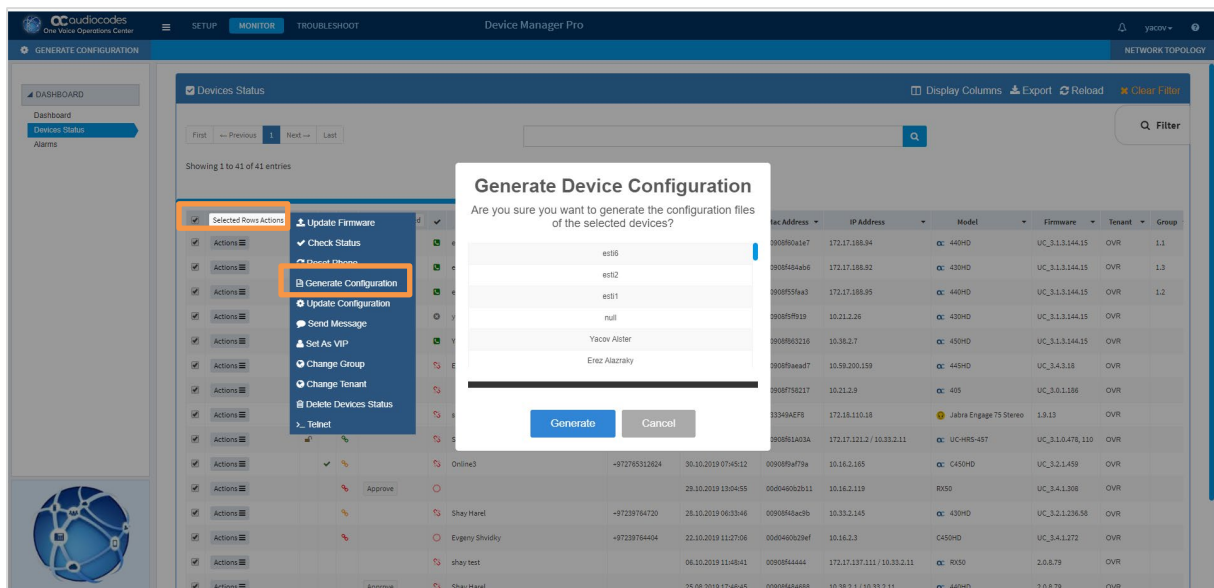
- d. Access the Devices Status page (**MONITOR** menu > **DASHBOARD** folder > **Devices Status**) to assign specific users to the OVR tenant
- e. Filter the list so that it displays only the specific IP Phone users, by clicking the **Filter** button (located on the right of the page) and then defining 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



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



4.3.3 Configuring the IP Phones through TFTP/HTTP

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

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

©2020 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-10731

