

Microsoft® Skype for Business Server 2015 and ITSP SIP Trunk using AudioCodes Mediant™ E-SBC

Version 7.2



Microsoft Partner

Gold Communications



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	Microsoft Skype for Business Server 2015 Version	9
2.3	Deploying the SBC	10
2.3.1	Example Environment.....	10
2.3.2	Environment Setup	11
3	Configuring Skype for Business Server 2015.....	13
3.1	Configuring the E-SBC as an IP / PSTN Gateway	13
3.2	Configuring the "Route" on Skype for Business Server 2015.....	21
4	Configuring AudioCodes E-SBC.....	31
4.1	Step 1: IP Network Interfaces Configuration	32
4.1.1	Step 1a: Configure VLANs.....	33
4.1.2	Step 1b: Configure IP Network Interfaces for LAN and WAN	33
4.2	Step 2: Enable the SBC Application	36
4.3	Step 3: Configure Media Realms	37
4.4	Step 4: Configure SIP Signaling Interfaces.....	40
4.5	Step 5: Configure Proxy Sets	42
4.6	Step 6: Configure Coders	45
4.7	Step 7: Configure IP Profiles	48
4.8	Step 8: Configure IP Groups.....	52
4.9	Step 9: SIP TLS Connection Configuration.....	54
4.9.1	Step 9a: Configure the NTP Server Address.....	54
4.9.2	Step 9b: Configure the TLS version	55
4.9.3	Step 9c: Configure a Certificate.....	56
4.10	Step 10: Configure SRTP	62
4.11	Step 11: Configure Maximum IP Media Channels	63
4.12	Step 12: Configure IP-to-IP Call Routing Rules	64
4.13	Step 13: Configure IP-to-IP Manipulation Rules.....	69
4.14	Step 14: Configure Message Manipulation Rules	71
4.15	Step 15: Configure Registration Accounts	73
4.16	Step 16: Miscellaneous Configuration.....	74
4.16.1	Step 16a: Configure Call Forking Mode	74
4.16.2	Step 16b: Configure SBC Alternative Routing Reasons	75
4.17	Step 17: Reset the E-SBC	76
A	Configuring SBC to Send 414 Request - URI Too Long.....	77
B	Configuring SBC to Send 503 Instead 500 Toward Skype for Business	83

This page is intentionally left blank.

Notice

This document describes how to connect the Microsoft Skype for Business Server 2015 and ITSP SIP Trunk using AudioCodes Mediant E-SBC product series.

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

© Copyright 2016 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: August-28-2016

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
54030	Initial document release for Version 7.2.

Documentation Feedback

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

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between ITSP's SIP Trunk and Microsoft's Skype for Business Server 2015 environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the E-SBC based on this interoperability setup. However, it is recommended to read through this document in order to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including download option, visit AudioCodes Web site at <http://www.audiocodes.com/sbc-wizard> (login required).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and ITSP Partners who are responsible for installing and configuring ITSP's SIP Trunk and Microsoft's Skype for Business Server 2015 for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

AudioCodes' family of E-SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The E-SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the E-SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes E-SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ▪ Mediant 500 E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (SE and VE)
Software Version	SIP_7.20A.000.058 or later
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP (to the ITSP SIP Trunk) ▪ SIP/TCP or TLS (to the S4B Front End Server)
Additional Notes	None

2.2 Microsoft Skype for Business Server 2015 Version

Table 2-2: Microsoft Skype for Business Server 2015 Version

Vendor	Microsoft
Model	Skype for Business
Software Version	Release 2015 6.0.9319.0
Protocol	SIP
Additional Notes	None

2.3 Deploying the SBC

2.3.1 Example Environment

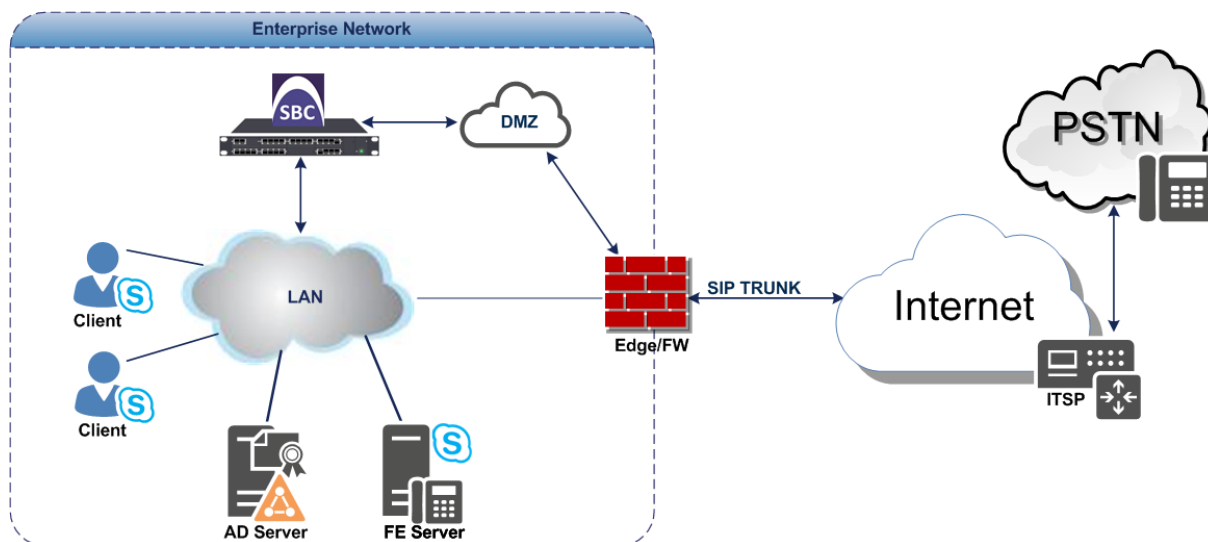
The example scenario below is referred to throughout this document in order to show how to deploy the SBC.

In the example environment:

- Enterprise deployed with Microsoft Skype for Business Server 2015 in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using ITSP's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
 - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
 - **Border:** IP-to-IP network border between Skype for Business Server 2015 network in the Enterprise LAN and ITSP's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Example Environment Topology between E-SBC and Microsoft Skype for Business with ITSP SIP Trunk



2.3.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-3: Environment Setup

Area	Setup
Network	<ul style="list-style-type: none">▪ Microsoft Skype for Business Server 2015 environment is located on the Enterprise's LAN▪ ITSP SIP Trunk is located on the WAN
Signaling Transcoding	<ul style="list-style-type: none">▪ Microsoft Skype for Business Server 2015 operates with SIP-over-TLS transport type▪ ITSP SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	<ul style="list-style-type: none">▪ Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders▪ ITSP SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	<ul style="list-style-type: none">▪ Microsoft Skype for Business Server 2015 operates with SRTP media type▪ ITSP SIP Trunk operates with RTP media type

This page is intentionally left blank.

3 Configuring Skype for Business Server 2015

This chapter describes how to configure Microsoft Skype for Business Server 2015 to operate with AudioCodes E-SBC.



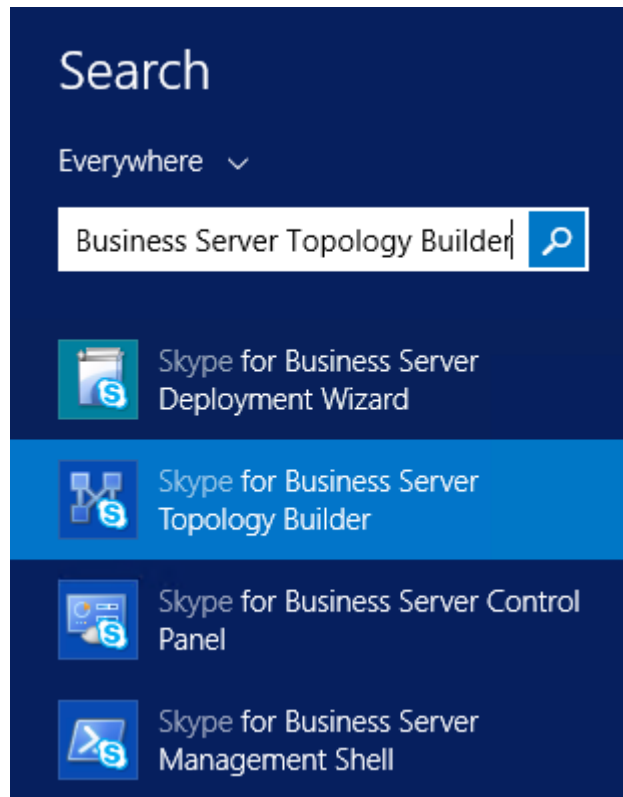
Note: Dial plans, voice policies, and PSTN usages are also necessary for Enterprise voice deployment; however, they are beyond the scope of this document.

3.1 Configuring the E-SBC as an IP / PSTN Gateway

The procedure below describes how to configure the E-SBC as an IP / PSTN Gateway.

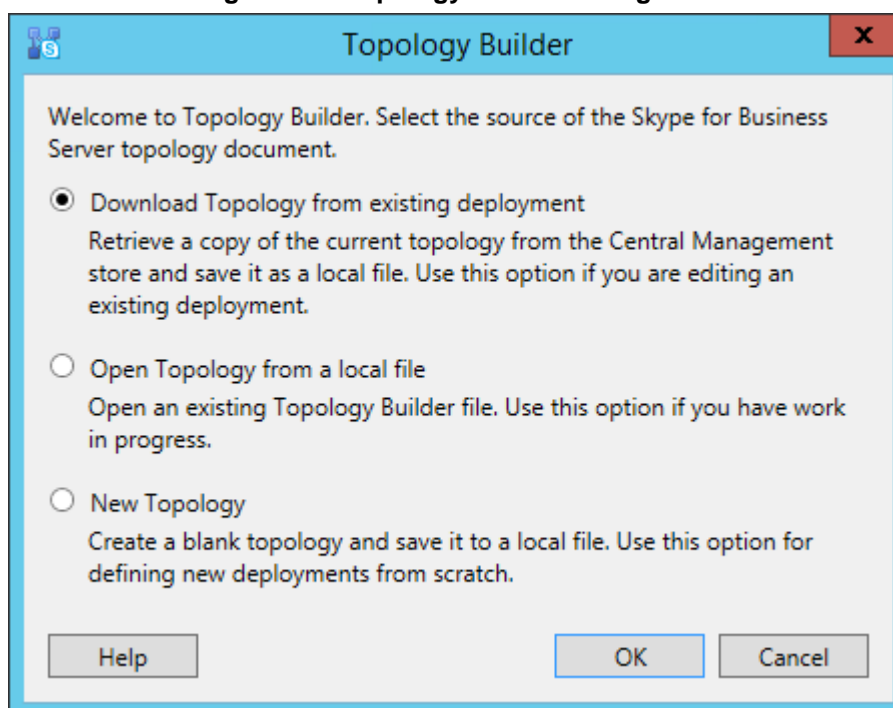
- **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**
- 1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

Figure 3-1: Starting the Skype for Business Server Topology Builder



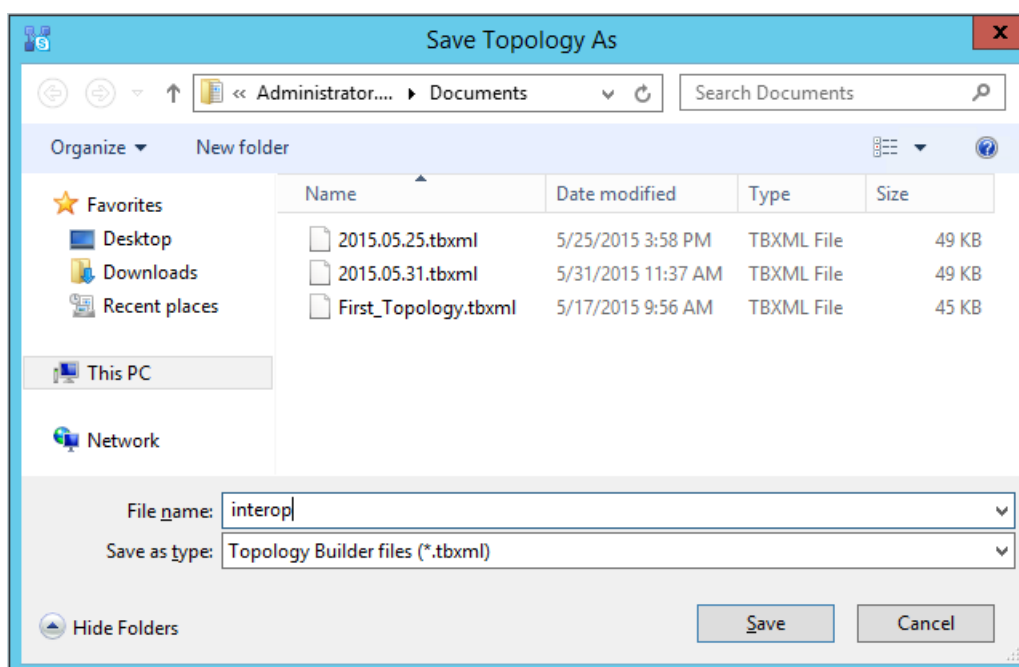
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



2. Select the **Download Topology from existing deployment** option, and then click **OK**; you are prompted to save the downloaded Topology:

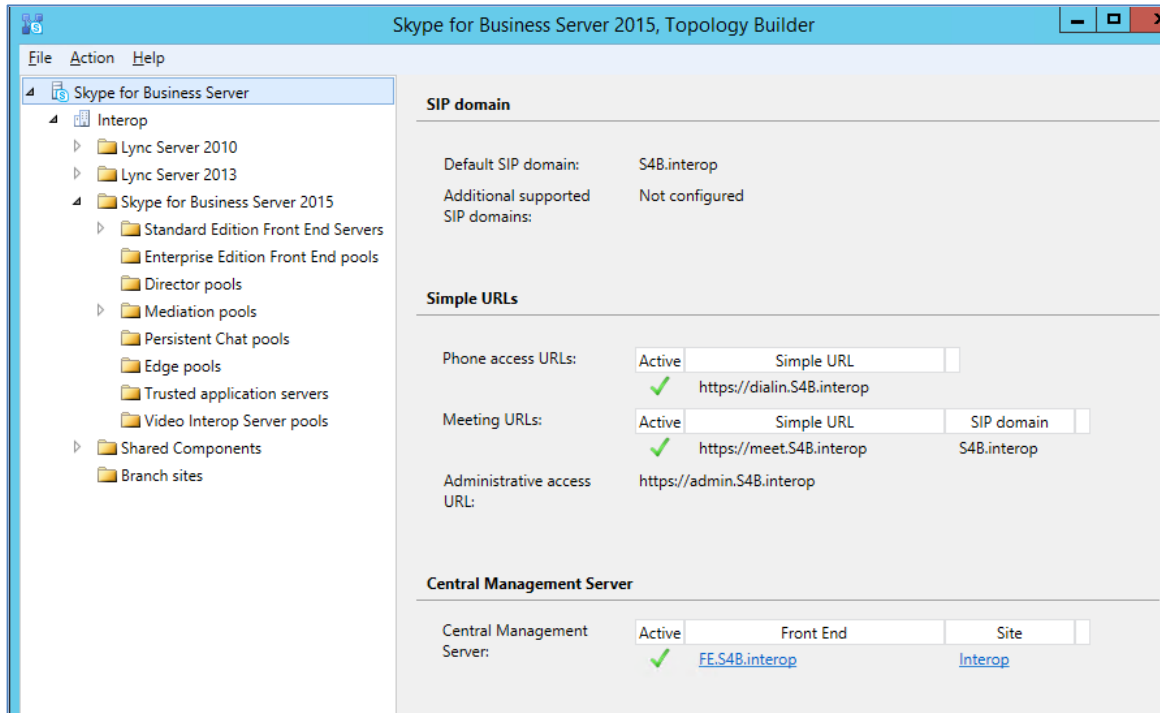
Figure 3-3: Save Topology Dialog Box



3. Enter a name for the Topology file, and then click **Save**. This step enables you to roll back from any changes you make during the installation.

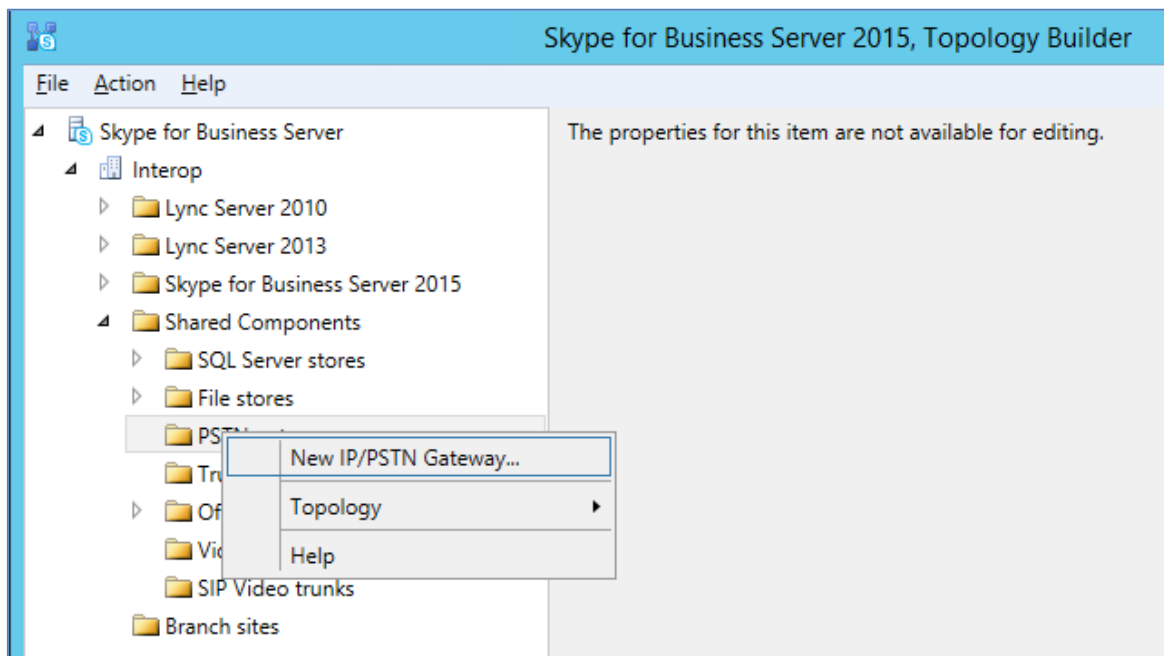
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN

5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP.S4B.interop**). This FQDN should be equivalent to the configured Subject Name (CN) in the TLS Certificate Context (see Section 4.9.3 on page 56).
6. Click **Next**; the following is displayed:

Figure 3-7: Define the IP Address

7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.
8. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server FQDN, Mediation Server listening port (TLS or TCP), gateway IP

and FQDN, and gateway listening port.

**Notes:**

- When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
- The root trunk cannot be removed until the associated PSTN gateway is removed.

Figure 3-8: Define the Root Trunk

Define New IP/PSTN Gateway

Define the root trunk

Trunk name: *
ITSP.S4B.interop

Listening port for IP/PSTN gateway: *
5067

SIP Transport Protocol:
TLS

Associated Mediation Server:
FE.S4B.interop Interop

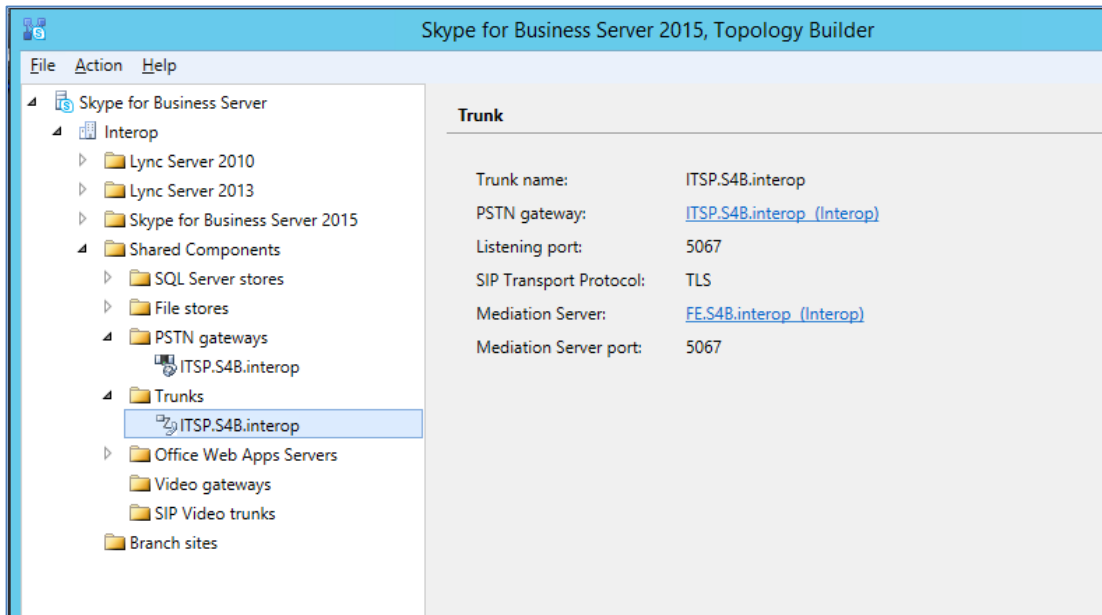
Associated Mediation Server port: *
5067

Help Back Finish Cancel

- a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**). This parameter is later configured in the SIP Interface table (see Section 4.3 on page 37).
- b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses. This parameter is later configured in the SIP Interface table (see Section 4.3 on page 37).
- c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
- d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
- e. Click **Finish**.

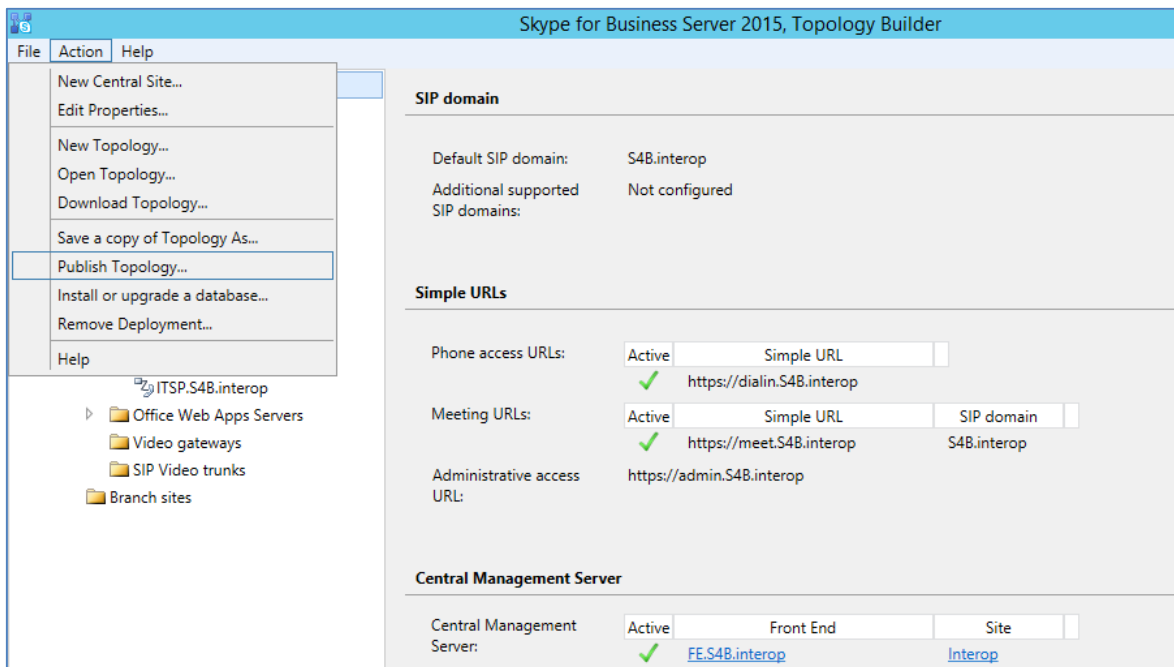
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

Figure 3-9: E-SBC added as IP/PSTN Gateway and Trunk Created



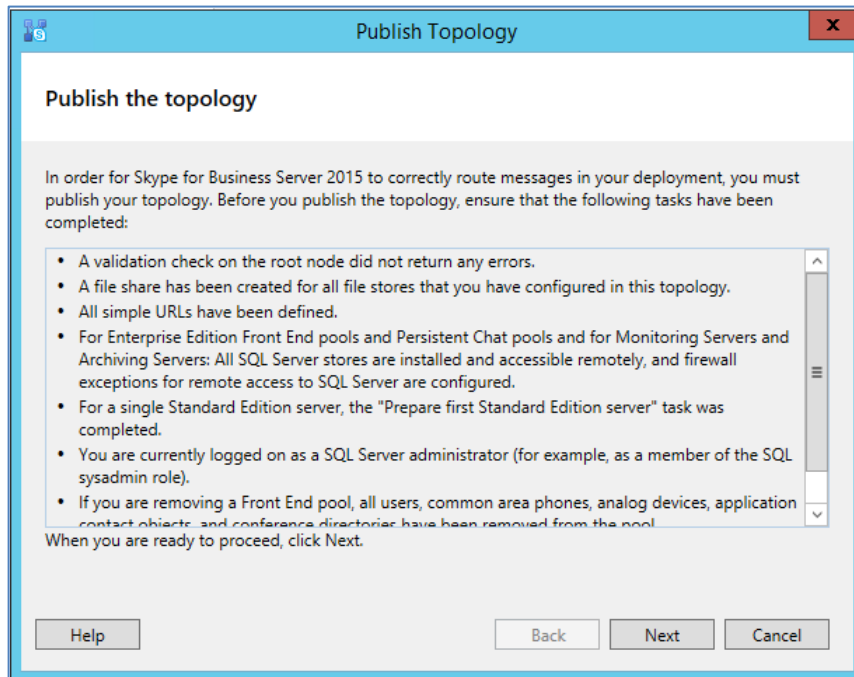
9. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



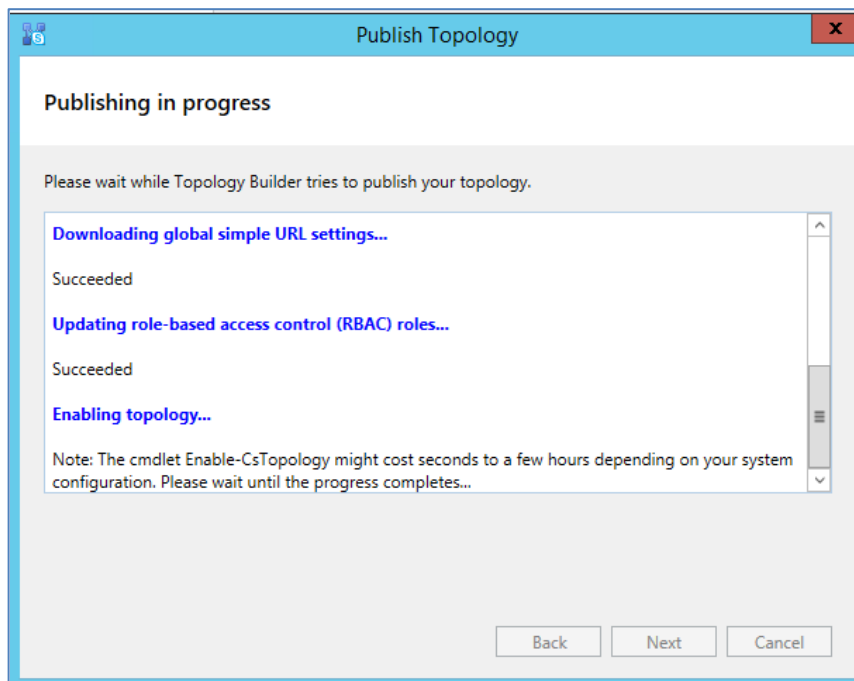
The following is displayed:

Figure 3-11: Publish the Topology



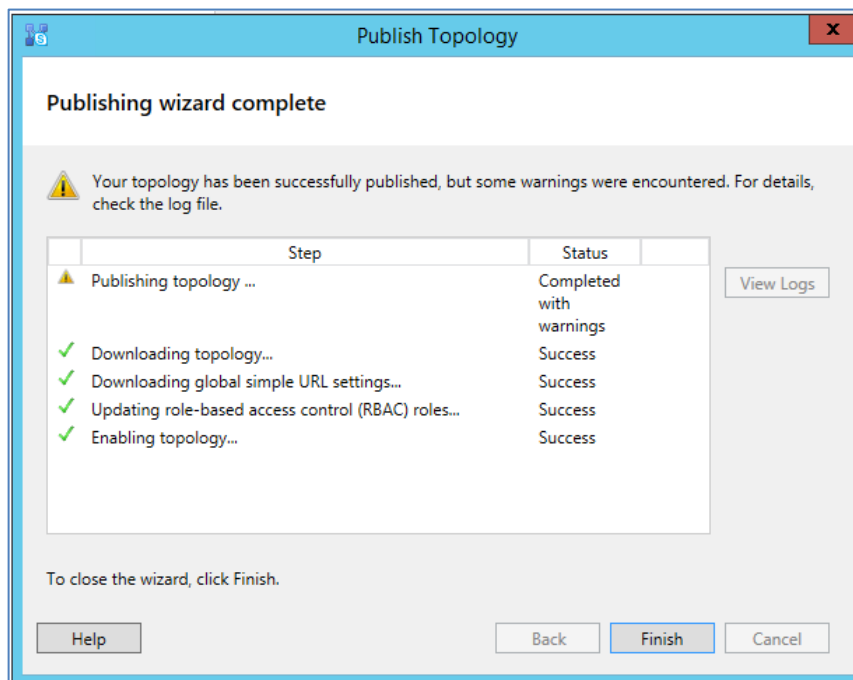
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



- Wait until the publishing topology process completes successfully, as shown below:

Figure 3-13: Publishing Wizard Complete



- Click **Finish**.

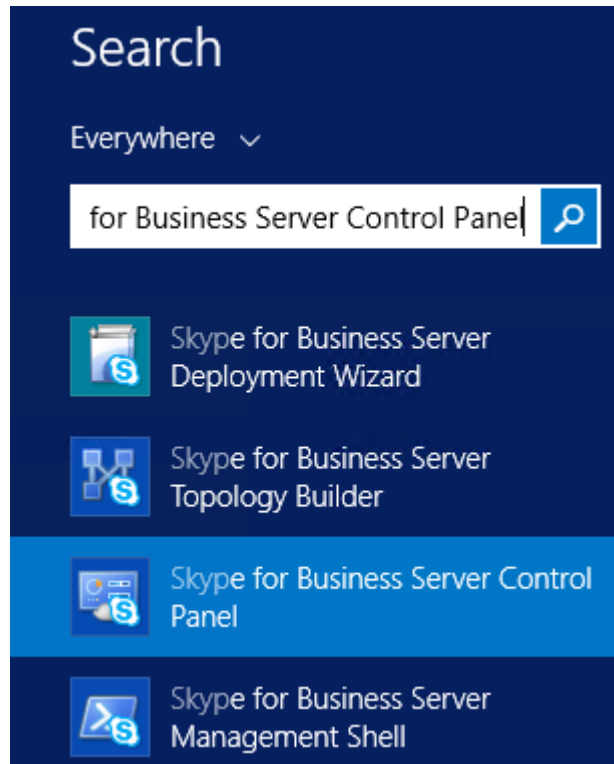
3.2 Configuring the "Route" on Skype for Business Server 2015

The procedure below describes how to configure a "Route" on the Skype for Business Server 2015 and to associate it with the E-SBC PSTN gateway.

➤ **To configure the "route" on Skype for Business Server 2015:**

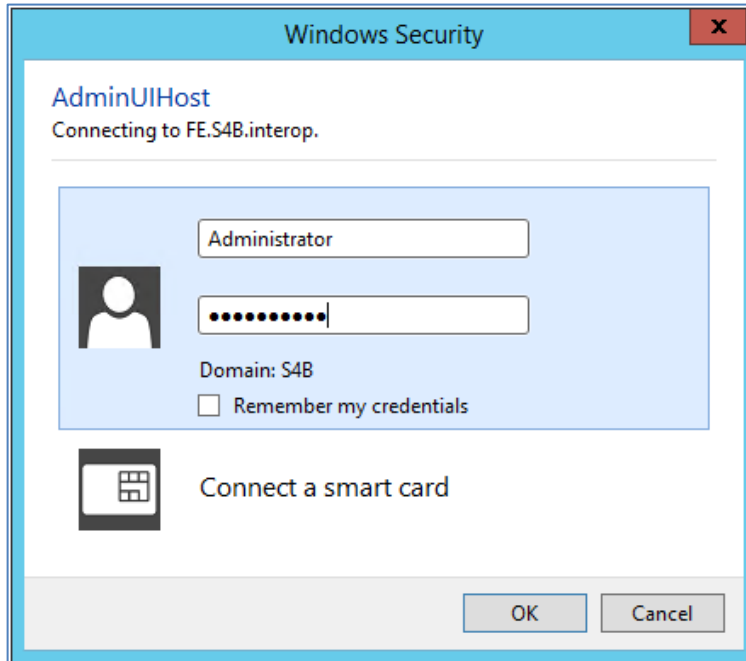
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

Figure 3-14: Opening the Skype for Business Server Control Panel



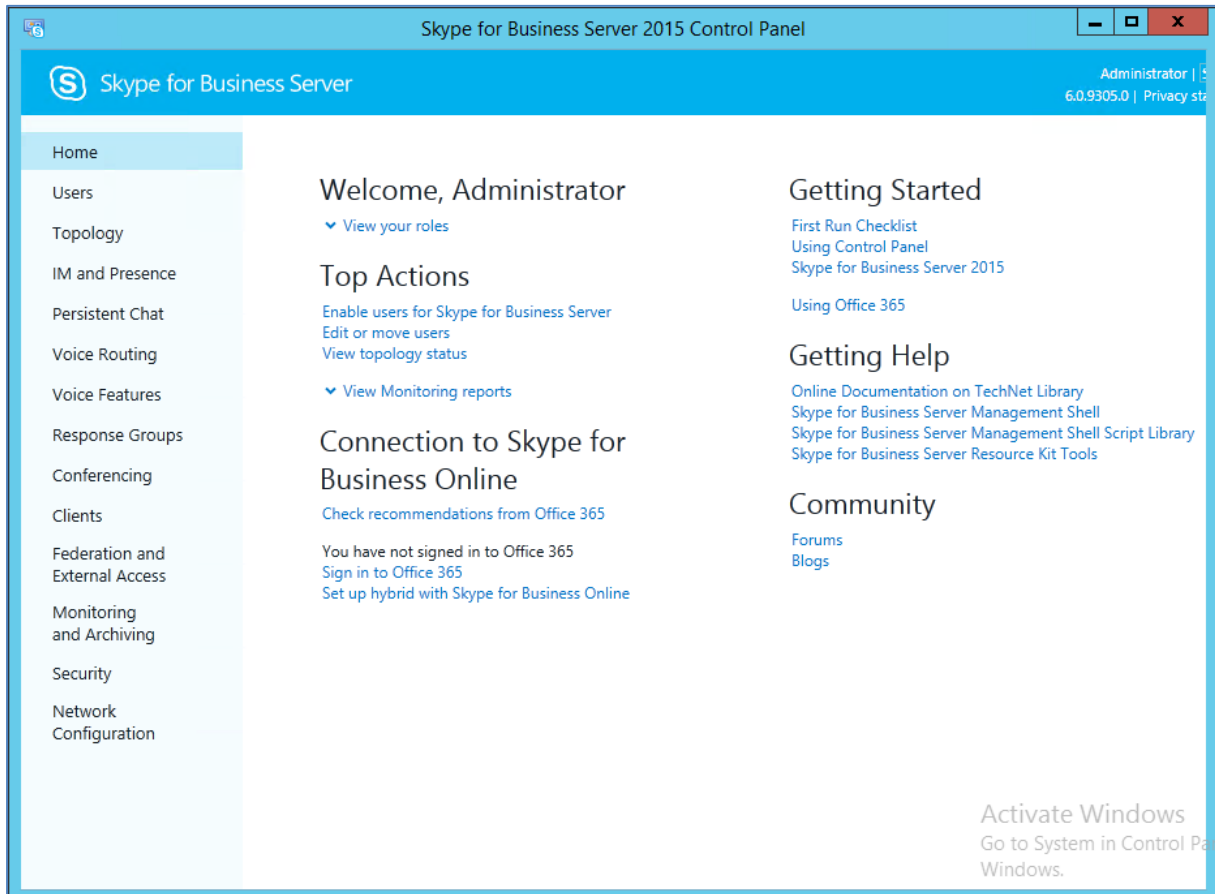
- You are prompted to enter your login credentials:

Figure 3-15: Skype for Business Server Credentials



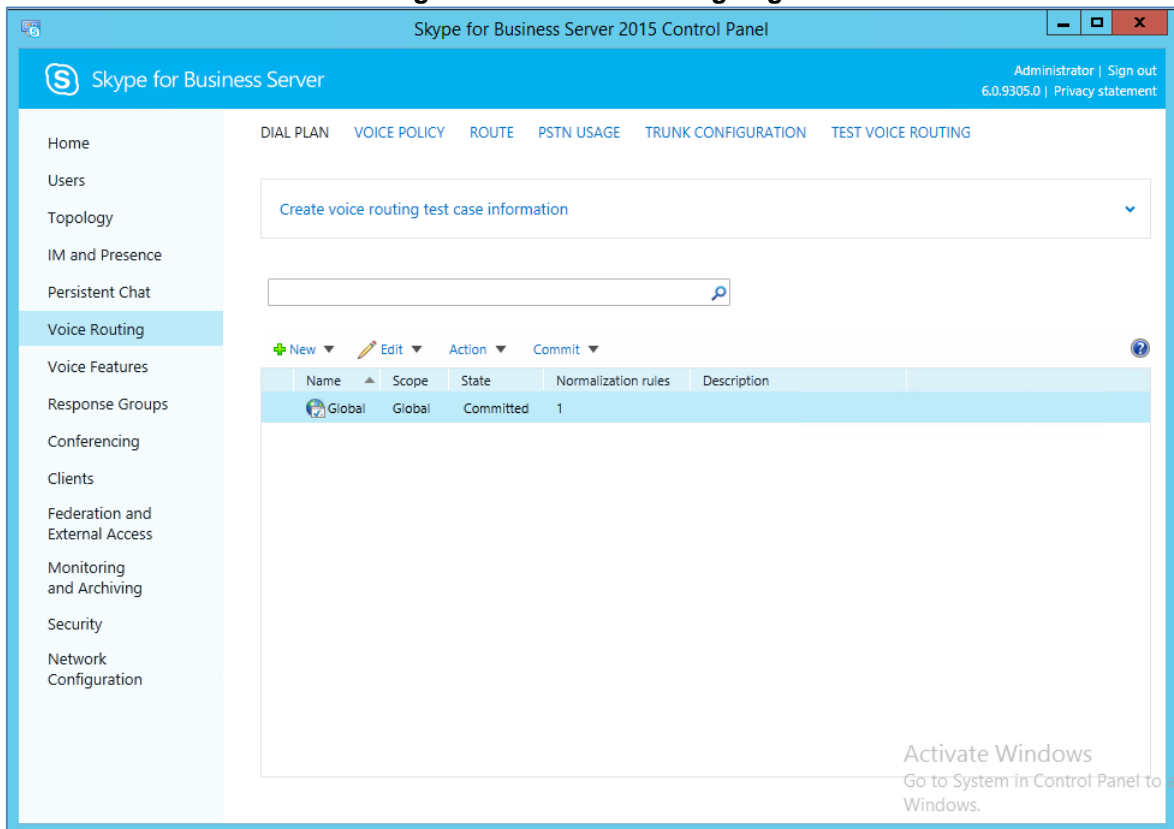
- Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

Figure 3-16: Microsoft Skype for Business Server 2015 Control Panel



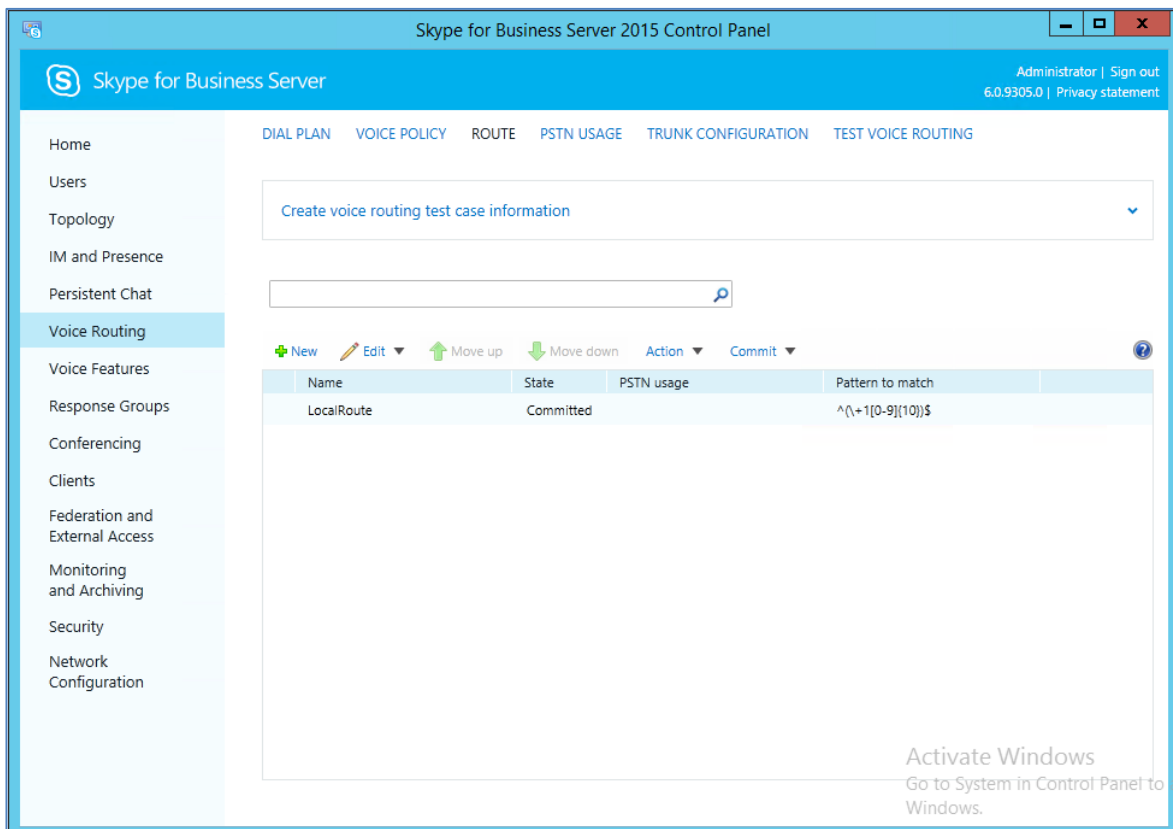
- In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



- In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



6. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route

The screenshot shows the 'New Voice Route' configuration page in the Skype for Business Server administration console. The page includes a left-hand navigation menu with 'Voice Routing' selected. The main content area contains the following fields and sections:

- Scope:** Name: ITSP
- Description:** (Empty text box)
- Build a Pattern to Match:**
 - Starting digits for numbers that you want to allow: (Empty text box with 'Add' button)
 - Match this pattern: *
- Associated trunks:** (Section with an 'Add' button)

7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).
8. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.
9. Associate the route with the E-SBC Trunk that you created:
 - a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-20: List of Deployed Trunks

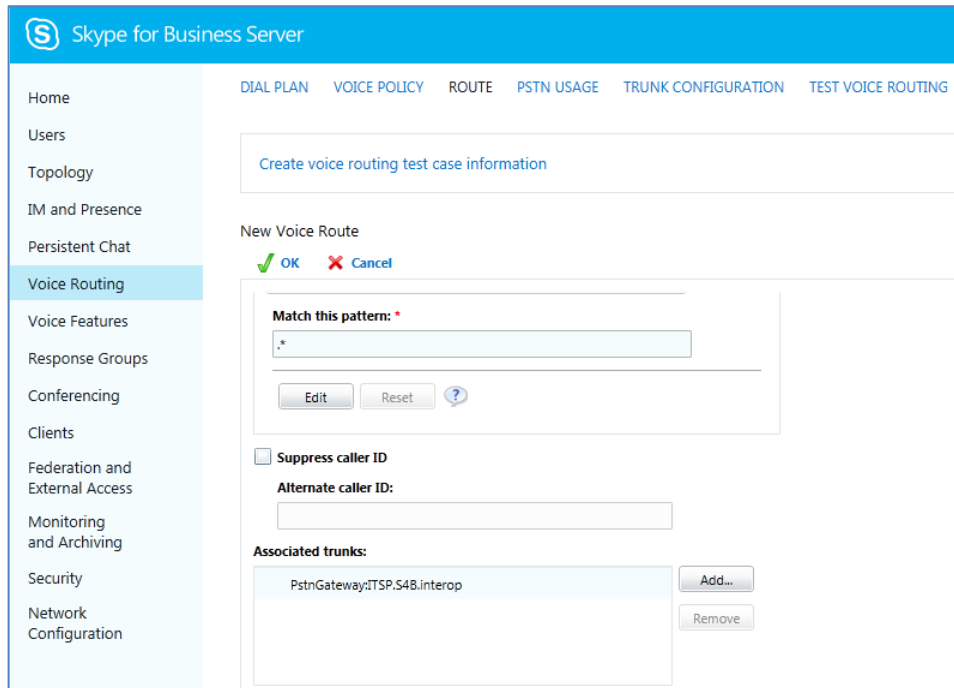
The screenshot shows the 'New Voice Route' configuration page with a 'Select Trunk' dialog box open. The dialog box displays a table of deployed trunks:

Service	Site
PstnGateway:ITSP.S4B.interop	Interop

The dialog box also includes a search bar at the top and 'OK' and 'Cancel' buttons at the bottom.

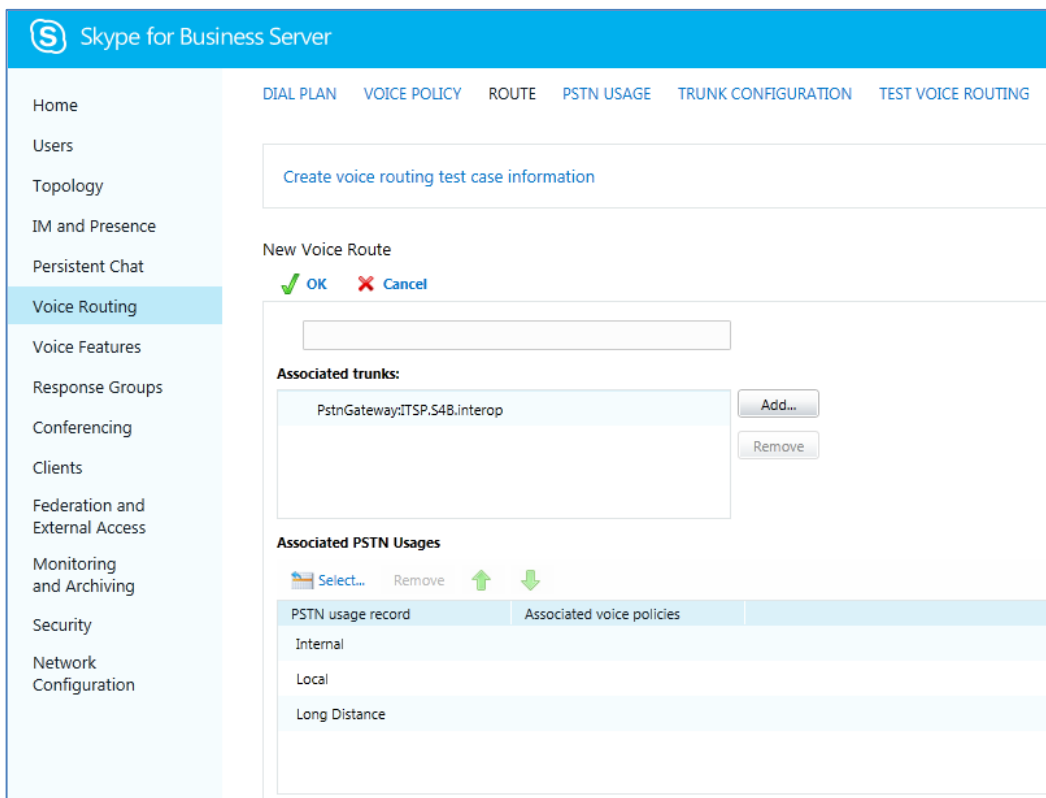
- b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-21: Selected E-SBC Trunk



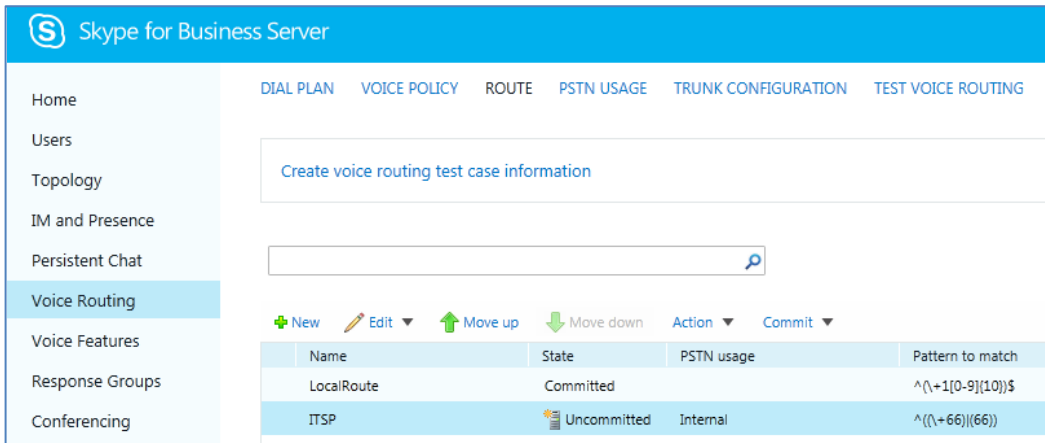
- 10. Associate a PSTN Usage to this route:
 - Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-22: Associating PSTN Usage to Route



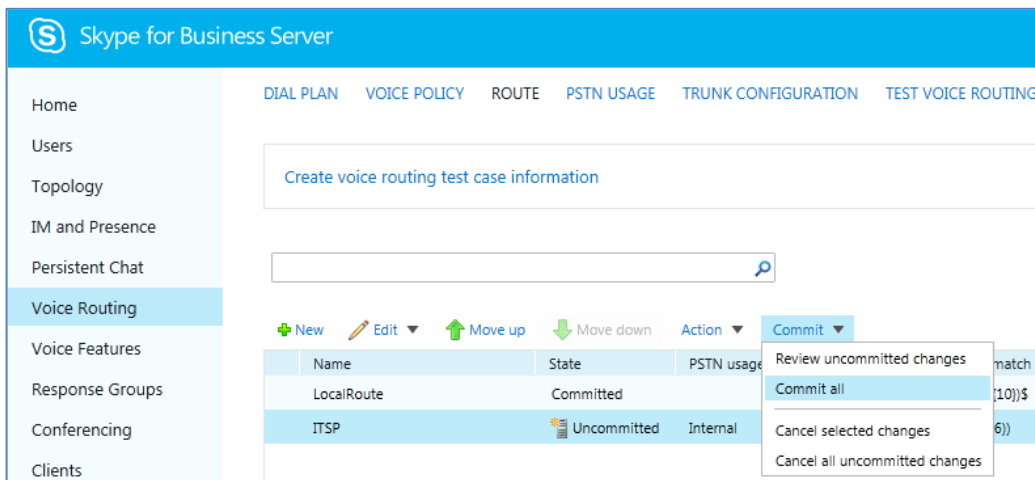
- Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-23: Confirmation of New Voice Route



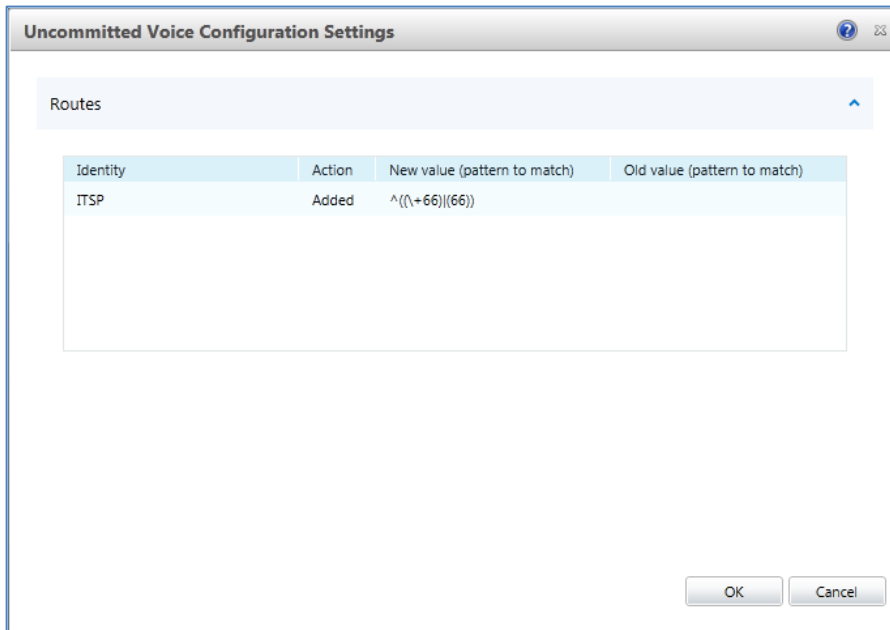
- From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-24: Committing Voice Routes



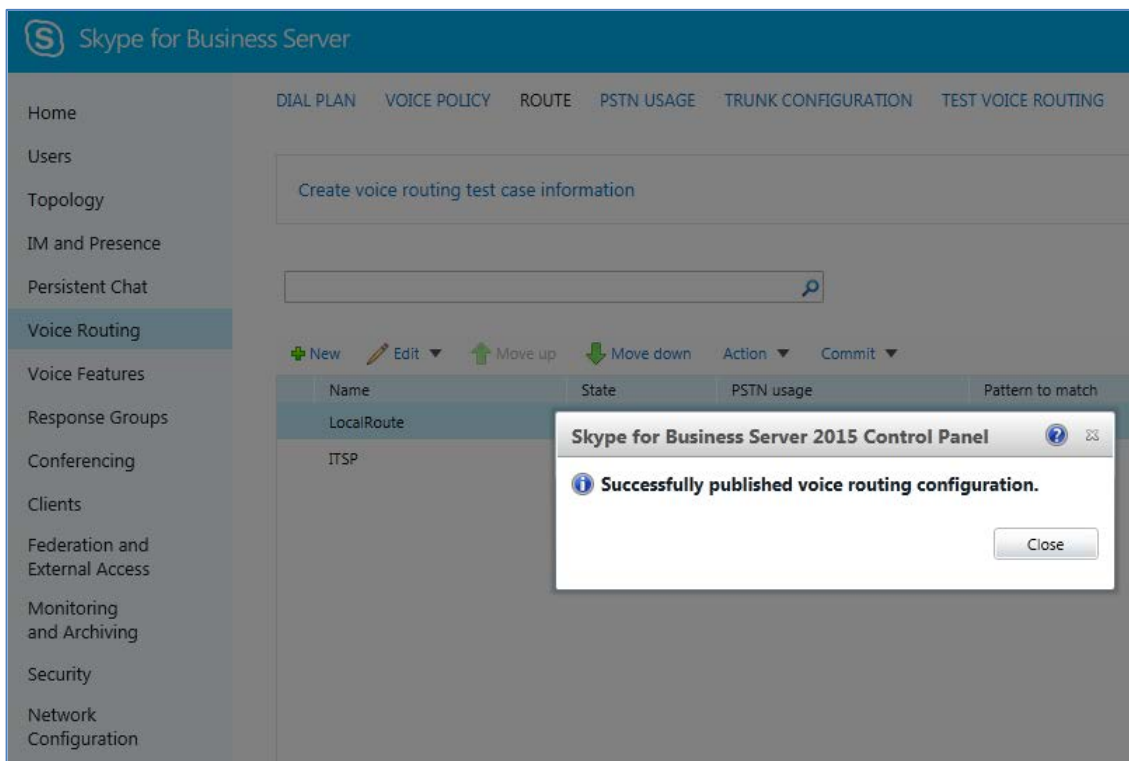
The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-26: Confirmation of Successful Voice Routing Configuration



14. Click **Close**; the new committed Route is displayed in the Voice Routing page, as shown below:

Figure 3-27: Voice Routing Screen Displaying Committed Routes

The screenshot shows the 'Voice Routing' configuration page in the Skype for Business Server administration console. The left-hand navigation pane is expanded to 'Voice Routing'. The main content area has several tabs: 'DIAL PLAN', 'VOICE POLICY', 'ROUTE', 'PSTN USAGE', 'TRUNK CONFIGURATION', and 'TEST VOICE ROUTING'. The 'ROUTE' tab is active. At the top, there is a dropdown menu for 'Create voice routing test case information' and a search bar. Below these are controls for '+ New', 'Edit', 'Move up', 'Move down', 'Action', and 'Commit'. A table displays the following routes:

Name	State	PSTN usage	Pattern to match
LocalRoute	Committed		^\{+1[0-9]{10}\}\$
ITSP	Committed	Internal	^\{+66\}\{66\}

15. For ITSPs that implement a call identifier, continue with the following steps:



Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Skype for Business user number). This ID is required by ITSP SIP Trunk in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 4.6 on page 45).

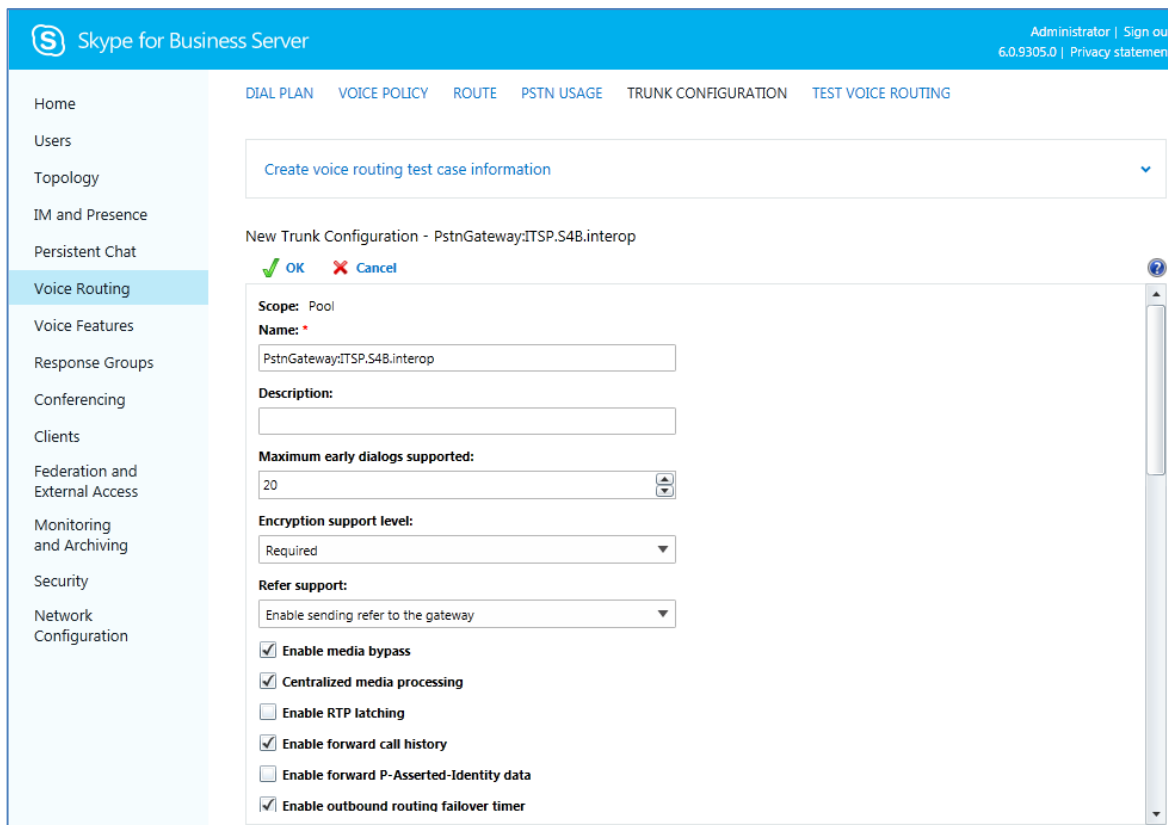
- a. In the Voice Routing page, select the **Trunk Configuration** tab. Note that you can add and modify trunk configuration by site or by pool.

Figure 3-28: Voice Routing Screen – Trunk Configuration Tab

The screenshot shows the 'Voice Routing' configuration page with the 'TRUNK CONFIGURATION' tab selected. The left-hand navigation pane is expanded to 'Voice Routing'. The main content area has tabs: 'DIAL PLAN', 'VOICE POLICY', 'ROUTE', 'PSTN USAGE', 'TRUNK CONFIGURATION', and 'TEST VOICE ROUTING'. The 'TRUNK CONFIGURATION' tab is active. At the top, there is a dropdown menu for 'Create voice routing test case information' and a search bar. Below these are controls for '+ New', 'Edit', 'Action', and 'Commit'. A table displays the following trunk configuration:

Name	Scope	State	Media bypass	PSTN usage	Calling number rules	Called number rules
Global	Global	Committed			0	0

- b. Click **Edit**; the Edit Trunk Configuration page appears:



- c. Select the **Enable media bypass** option.
- d. Select one of the following options from the 'Encryption Support Level' dropdown:
 - ◆ **Required** - SRTP encryption will be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
 - ◆ **Optional** - SRTP encryption will be used if the service provider or equipment manufacturer supports it.
 - ◆ **Not Supported** - SRTP encryption is not supported by the service provider or equipment manufacturer and will therefore not be used.

The option selected depends on customer configuration / requirements:

- ◆ If you set 'Encryption Support Level' to **Optional**, make sure the encryption is enabled in PowerShell (<https://support.microsoft.com/en-us/kb/2761579>):

```
Get-CsMediaConfiguration | Set-CsMediaConfiguration -
EncryptionLevel SupportEncryption
Identity                : Global
EnableQoS                : False
EncryptionLevel       : SupportEncryption
EnableSiren              : False
MaxVideoRateAllowed     : VGA600K
```

- e. Select the **Enable forward call history** check box, and then click **OK**.
- f. Repeat Steps 11 through 13 to commit your settings.

- 16. Use the following command on the Skype for Business Server Management Shell after reconfiguration to verify correct values:

- ◆ **Get-CsTrunkConfiguration**

```
Identity                :
Service:PstnGateway:ITSP.S4B.interop
OutboundTranslationRulesList :
SipResponseCodeTranslationRulesList : {}
```

```
OutboundCallingNumberTranslationRulesList : {}
PstnUsages                               : {}
Description                               :
ConcentratedTopology                      : True
EnableBypass                            : True
EnableMobileTrunkSupport                  : False
EnableReferSupport                      : True
EnableSessionTimer                    : True
EnableSignalBoost                         : False
MaxEarlyDialogs                          : 20
RemovePlusFromUri                        : False
RTCPActiveCalls                       : True
RTCPCallsOnHold                       : True
SRTPMode                               : Required
EnablePIDFLOSupport                      : False
EnableRTPLatching                        : False
EnableOnlineVoice                        : False
ForwardCallHistory                    : True
Enable3pccRefer                          : False
ForwardPAI                               : False
EnableFastFailoverTimer                  : True
EnableLocationRestriction                : False
NetworkSiteID                            :
```

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Skype for Business Server 2015 and the ITSP SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.3 and includes the following main areas:

- E-SBC WAN interface - ITSP SIP Trunking environment
- E-SBC LAN interface - Skype for Business Server 2015 environment

This configuration is done using the E-SBC's embedded Web server (hereafter, referred to as *Web interface*).



Notes:

- For implementing Microsoft Skype for Business and ITSP SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a License Key that includes the following software features:

- ✓ **Microsoft**
- ✓ **SBC**
- ✓ **Security**
- ✓ **DSP**
- ✓ **RTP**
- ✓ **SIP**

For more information about the License Key, contact your AudioCodes sales representative.

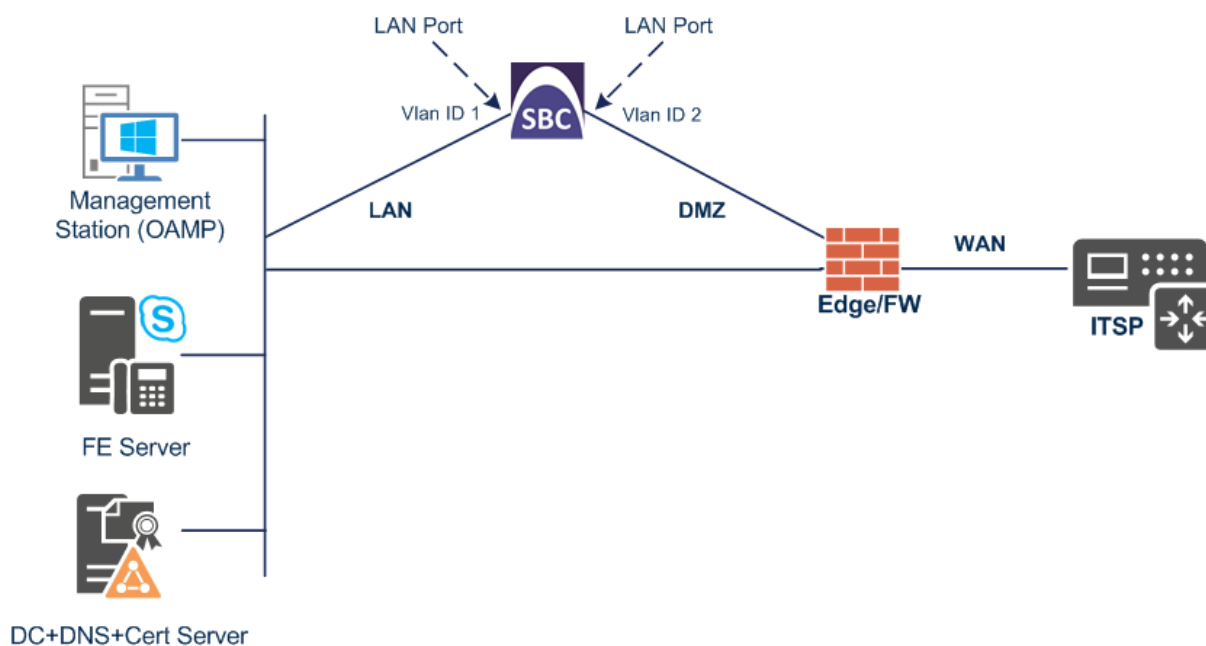
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.

4.1 Step 1: IP Network Interfaces Configuration

This step describes how to configure the E-SBC's IP network interfaces. There are several ways to deploy the E-SBC; however, scenario exemplified in this document employs the following deployment method:

- E-SBC interfaces with the following IP entities:
 - Skype for Business servers, located on the LAN
 - ITSP SIP Trunk, located on the WAN
- E-SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In this example, E-SBC connects to the LAN and DMZ using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
 - LAN (VLAN ID 1)
 - DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 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.
3. 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 4-2: Configured VLAN IDs in Ethernet Device

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.1.2 Step 1b: Configure IP Network Interfaces for LAN and WAN

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	Example Setting for IPv4	Example Setting for IPv6
Name	LAN_IF (arbitrary descriptive name)	IPv6_LAN_IF (arbitrary descriptive name)
Application Type	OAMP + Media + Control	Media + Control (The OAMP application can be configured only with IPv4.)
Interface Mode	See IPv4 in the SBC documentation.	See IPv6 in the SBC documentation.
IP Address	10.15.17.77 (LAN IP address of E-SBC)	2001::77 (only a global address can be entered)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)	64 (only 64 is supported)
Default Gateway	10.15.0.1	2001::1
Primary DNS	10.15.27.1	2001::10
Secondary DNS	0.0.0.0	2001::10
Ethernet Device	vlan 1	vlan 1

3. Add a network interface for the WAN side:

- a. Click **New**.
- b. Configure the interface as follows:


Parameter	Example Setting for IPv4	Example Setting for IPv6
Name	WAN_IF (arbitrary descriptive name)	IPv6_WAN_IF (arbitrary descriptive name)
Application Type	Media + Control	Media + Control
Interface Mode	See IPv4 in the SBC documentation.	See IPv6 in the SBC documentation.
IP Address	195.189.192.157 (DMZ IP address of E-SBC)	2002::157
Prefix Length	25 (subnet mask in bits for 255.255.255.128)	64
Default Gateway	195.189.192.129 (router's IP address)	2002::129
Primary DNS	80.179.52.100	2001:4860:4860::8888
Secondary DNS	80.179.55.100	2001:4860:4860::8844
Ethernet Device	vlan 2	vlan 2

4. Click **Apply**.

The configured IP network interfaces are shown below:

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

IP Interfaces (2)

+ New Edit  Page 1 of 1 Show 10 records per page

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	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

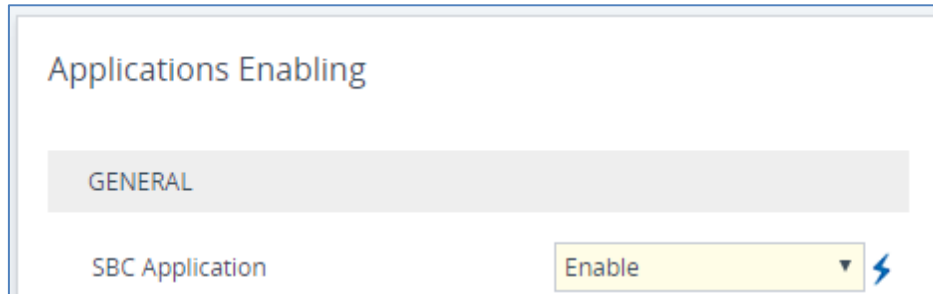
4.2 Step 2: Enable the SBC Application

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 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.17 on page 76).

4.3 Step 3: 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. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), however modify it as shown below:

Parameter	Value
Index	0
Name	MRLan (descriptive name)
IPv4 Interface Name	LAN_IF
IPv6 Interface Name	IPv6_LAN_IF (Only applicable if using IPv6)
Port Range Start	6000 (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-5: Configuring Media Realm for LAN

Media Realms [MRLan]
— ✕

GENERAL

Index

Name

Topology Location

IPv4 Interface Name [View](#)

Port Range Start

Number Of Media Session Legs

Port Range End

Default Media Realm

QUALITY OF EXPERIENCE

QoE Profile [View](#)

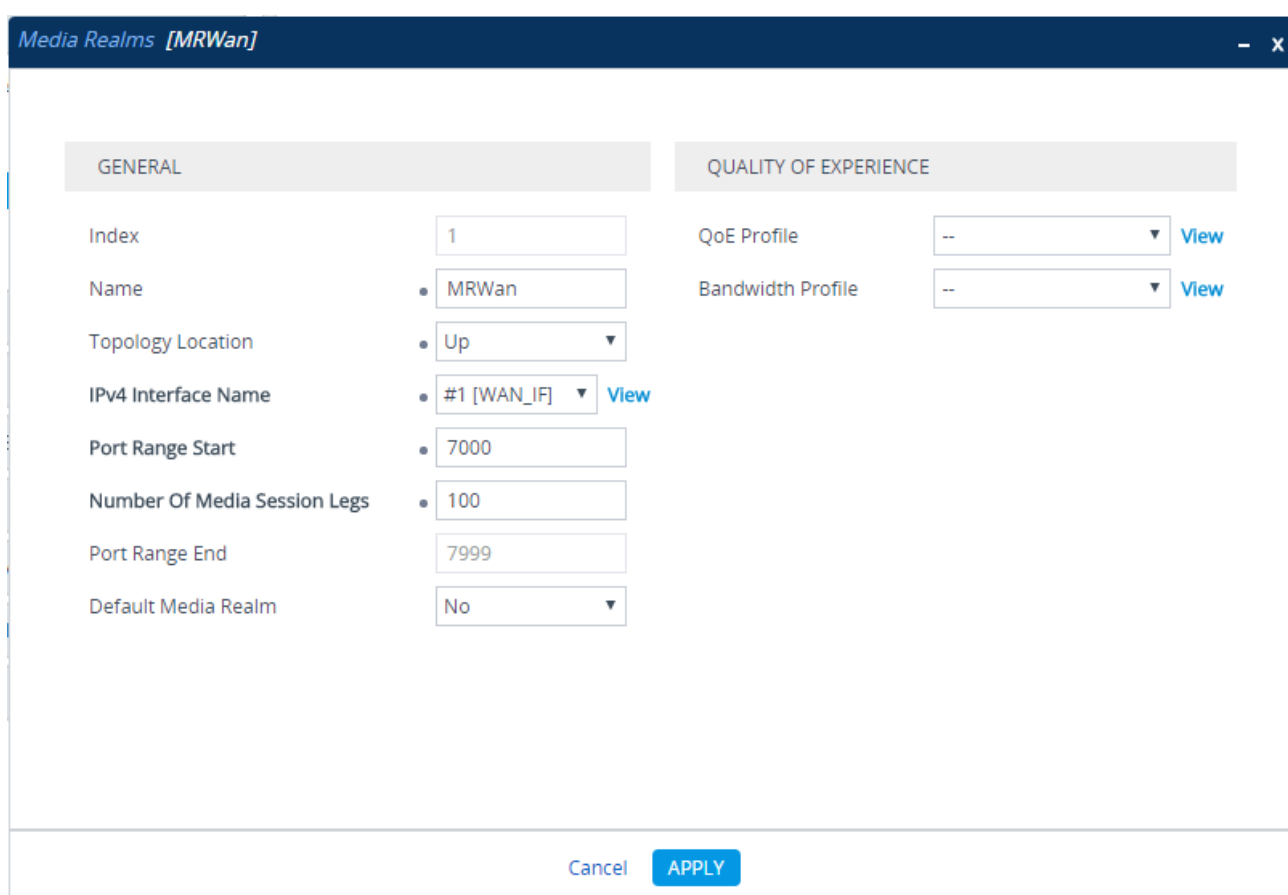
Bandwidth Profile [View](#)

Cancel
APPLY

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Name	MRWan (arbitrary name)
Topology Location	Up
IPv4 Interface Name	WAN_IF
IPv6 Interface Name	IPv6_WAN_IF (Only applicable if using IPv6)
Port Range Start	7000 (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



Media Realms [MRWan]


GENERAL		QUALITY OF EXPERIENCE	
Index	1	QoE Profile	-- View
Name	MRWan	Bandwidth Profile	-- View
Topology Location	Up		
IPv4 Interface Name	#1 [WAN_IF] View		
Port Range Start	7000		
Number Of Media Session Legs	100		
Port Range End	7999		
Default Media Realm	No		

Cancel APPLY

The configured Media Realms are shown in the figure below:

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

Media Realms (2)

+ New Edit  Page 1 of 1 Show 10 records per page

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MRLan	LAN_IF	6000	100	6999	No
1	MRWan	WAN_IF	7000	100	7999	No

4.4 Step 4: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. In the example scenario, an internal and external SIP Interface must be configured for the E-SBC.

➤ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Add a SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	S4B (see note at the end of this section)
Network Interface	LAN_IF
Application Type	SBC
UDP and TCP	0
TLS Port	5067 (see note below)
Media Realm	MRLan



Note: The TLS port parameter must be identically configured in the Skype for Business Topology Builder (see Section 3.1 on page 13).


3. Configure a SIP Interface for the WAN:



Parameter	Value
Index	1
Name	ITSP
Network Interface	WAN_IF
Application Type	SBC
UDP Port	5060
TCP and TLS	0
Media Realm	MRWan

The configured SIP Interfaces are shown in the figure below:

Figure 4-8: Configured SIP Interfaces in SIP Interface Table

SIP Interfaces (2)

+ New Edit  Page 1 of 1 Show 10 records per page

INDEX ↕	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	S4B	 DefaultSRD	LAN_IF	SBC	0	0	5067	No encapsulation	--
1	ITSP	 DefaultSRD	WAN_IF	SBC	5060	0	0	No encapsulation	--



Note: Current software releases uses the string **names** of the configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups). Therefore, it is recommended to configure each configuration entity with meaningful names for easy identification.

4.5 Step 5: Configure Proxy Sets

This step describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

In the example scenario, two Proxy Sets need to be configured for the following IP entities:

- Microsoft Skype for Business Server 2015
- ITSP SIP Trunk

The Proxy Sets will be later applied to the VoIP network by assigning them to IP Groups.

➤ To configure Proxy Sets:

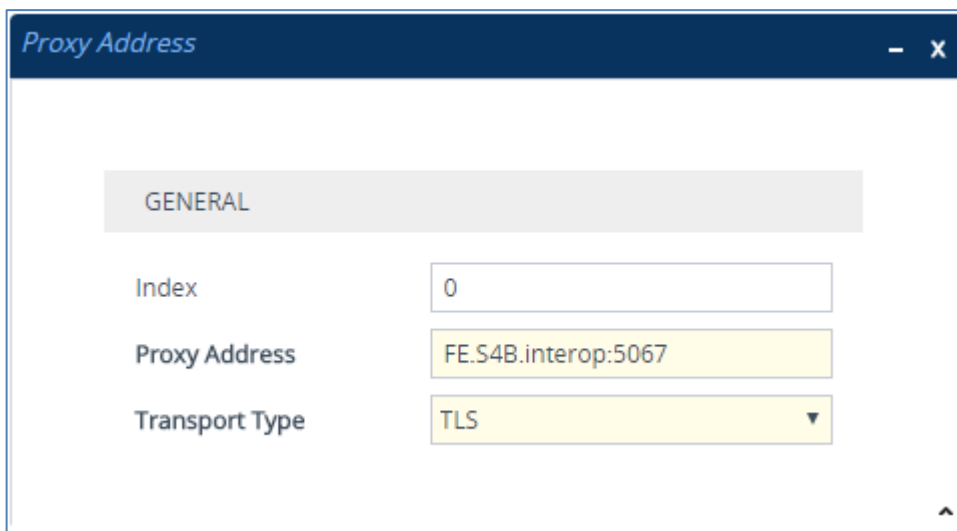
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Add a Proxy Set for the Skype for Business Server 2015 as shown below:

Parameter	Value
Index	1
Name	S4B
SBC IPv4 SIP Interface	S4B
Proxy Keep-Alive	Using Options
Redundancy Mode	Homing
Load Balancing Method	Round Robin
Proxy Hot Swap	Enable

Figure 4-9: Configuring Proxy Set for Microsoft Skype for Business Server 2015

- a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
- b. Click **New**; the following dialog box appears:

Figure 4-10: Configuring Proxy Address for Microsoft Skype for Business Server 2015



- c. Configure the address of the Proxy Set according to the parameters described in the table below.

Parameter	Value
Index	0
Proxy Address	FE.S4B.interop:5067 (Skype for Business Server 2015 IP address / FQDN and destination port)
Transport Type	TLS

- d. Click **Apply**.

3. Configure a Proxy Set for the ITSP SIP Trunk:

Parameter	Value
Index	2
Name	ITSP
SBC IPv4 SIP Interface	ITSP
Proxy Keep-Alive	Using Options
Keep-Alive Failure responses	503 (If this is received in response to a keep-alive message using SIP OPTIONS, the SBC considers the proxy as down and tries the next proxy.)
Proxy Hot Swap	Enable

Figure 4-11: Configuring Proxy Set for ITSP SIP Trunk

- a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
- b. Click **New**; the following dialog box appears:

Figure 4-12: Configuring Proxy Address for ITSP SIP Trunk

- c. Configure the address of the Proxy Set according to the parameters described in the table below.

Parameter	Value
Index	0
Proxy Address	ITSP.com:5060 (IP address / FQDN and destination port)
Transport Type	UDP

- d. Click **Apply**.

4.6 Step 6: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Skype for Business Server 2015 supports the G.711 coder while the network connection to ITSP SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the ITSP SIP Trunk.

Note that the Coder Group ID for this entity will be assign to its corresponding IP Profile in the next step.

➤ **To configure coders:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Configure a Coder Group for Skype for Business Server 2015:

Parameter	Value
Coder Group ID	1
Coder Name	<ul style="list-style-type: none"> ▪ G.711 U-law ▪ G.711 A-law
Silence Suppression	Enable (for both coders)

Figure 4-13: Configuring Coder Group for Skype for Business Server 2015

Coder Groups

Coder Group Name: 1 : AudioCodersGroups_1 Delete Group

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711U-law	20	64	0	Enable	
G.711A-law	20	64	8	Enable	

3. Configure a Coder Group for ITSP SIP Trunk:

Parameter	Value
Coder Group ID	2
Coder Name	G.729

Figure 4-14: Configuring Coder Group for ITSP SIP Trunk

Coder Groups

Coder Group Name: 2 : AudioCodersGroups_2 Delete Group

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.729	20	8	18	Disabled	

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the ITSP SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID will be assign to the IP Profile belonging to the ITSP SIP Trunk Profile in the next step.

➤ **To set a preferred coder for the ITSP SIP Trunk:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Video Coders Group for ITSP SIP Trunk.

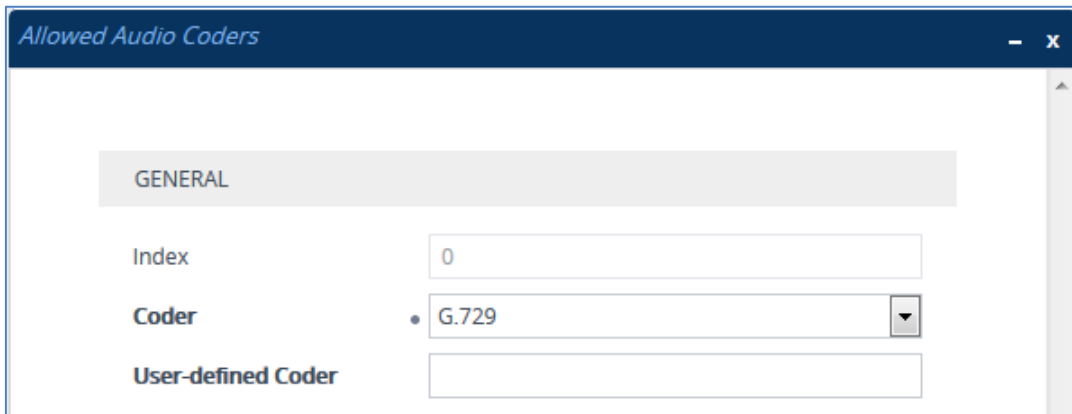
Figure 4-15: Configuring Allowed Coders Group for ITSP SIP Trunk



3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Video Coders** link located below the table; the Allowed Video Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Parameter	Value
Index	0
Coder	G.729

Figure 4-16: Configuring Allowed Coders for ITSP SIP Trunk



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

Figure 4-17: SBC Preferences Mode

The screenshot displays the 'Media Settings' configuration page, divided into several sections:

- GENERAL**
 - NAT Traversal:** Disable NAT (dropdown)
 - Enable Continuity Tones:** Disable (dropdown)
 - Inbound Media Latch Mode:** Dynamic (dropdown)
 - Number of Media Channels:** 0 (text input)
 - Enforce Media Order:** Disable (dropdown)
 - SDP Session Owner:** AudiocodesGW (text input)
- ROBUSTNESS**
 - New RTP Stream Packets:** 3 (text input)
 - New RTCP Stream Packets:** 3 (text input)
 - New SRTP Stream Packets:** 3 (text input)
 - New SRTCP Stream Packets:** 3 (text input)
 - Timeout To Relatch RTP (msec):** 200 (text input)
 - Timeout To Relatch SRTP (msec):** 200 (text input)
 - Timeout To Relatch Silence (msec):** 10000 (text input)
 - Timeout To Relatch RTCP (msec):** 10000 (text input)
- SBC SETTINGS**
 - Preferences Mode:** Include Extensions (dropdown, highlighted with a radio button and an arrow pointing to it)
 - Enforce Media Order:** Disable (dropdown)
- GATEWAY SETTINGS**
 - Enable Early Media:** Disable (dropdown)
 - Multiple Packetization Time Format:** None (dropdown)

At the bottom of the page, there are two buttons: 'Cancel' and 'APPLY'.

- From the 'Preferences Mode' drop-down list, select **Include Extensions**.
- Click **Apply**.

4.7 Step 7: Configure IP Profiles

This step describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In the example scenario, IP Profiles need to be configured for the following IP entities:

- Microsoft Skype for Business Server 2015 - to operate in secure mode using SRTP and TLS
- ITSP SIP trunk - to operate in non-secure mode using RTP and UDP

➤ **To configure IP Profile for the Skype for Business Server 2015:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	1
Name	S4B
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 Media	
Extension Coders Group	AudioCodersGroups_1
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)
Remote 3xx Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)

Media	
Media IP Version Preference	Only IPv4 or Only IPv6

Figure 4-18: Configuring IP Profile for Skype for Business Server 2015

The screenshot shows the 'IP Profiles [S4B]' configuration window. It is divided into three main sections: GENERAL, MEDIA SECURITY, and SBC SIGNALING. The GENERAL section includes fields for Index (1), Name (S4B), and Created by Routing Server (No). The MEDIA SECURITY section includes dropdowns for SBC Media Security Mode (SRTP), Gateway Media Security Mode (Preferable), Symmetric MKI (Enable), MKI Size (1), SBC Enforce MKI Size (Enforce), and SBC Media Security Method (SDES). The SBC SIGNALING section includes dropdowns for PRACK Mode (Transparent), P-Asserted-Identity Header Mode (As Is), Diversion Header Mode (As Is), History-Info Header Mode (As Is), Session Expires Mode (Transparent), Remote Update Support (Supported Only After Conn), Remote re-INVITE (Supported only with SDP), Remote Delayed Offer Support (Not Supported), Remote Representation Mode (According to Operation Mo), Keep Incoming Via Headers (According to Operation Mo), Keep Incoming Routing Headers (According to Operation Mo), and Keep User-Agent Header (According to Operation Mo). At the bottom, there are 'Cancel' and 'APPLY' buttons.

3. Click **Apply**.

➤ **To configure an IP Profile for the ITSP SIP Trunk:**

1. Click **New**, and then configure the parameters as follows:

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 Media	
Extension Coders Group	AudioCodersGroups_2
Allowed Audio Coders	ITSP Allowed Coders
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer)
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Media	
Media IP Version Preference	Only IPv4 or Only IPv6



Note: The SIP Trunk's IP Profile depends on the SIP Trunk behavior. Refer to the explanations of the IP Profile parameters in the *SBC User's Manual* in order to configure the profile according to SIP Trunk behavior.

Figure 4-19: Configuring IP Profile for ITSP SIP Trunk

The screenshot shows a configuration window titled "IP Profiles [ITSP]". It is divided into three main sections: GENERAL, MEDIA SECURITY, and SBC SIGNALING. Each section contains various settings, many of which are dropdown menus or text input fields.

Section	Parameter	Value
GENERAL	Index	2
	Name	ITSP
	Created by Routing Server	No
MEDIA SECURITY	SBC Media Security Mode	RTP
	Gateway Media Security Mode	Preferable
	Symmetric MKI	Disable
	MKI Size	0
	SBC Enforce MKI Size	Don't enforce
	SBC Media Security Method	SDES
SBC SIGNALING	PRACK Mode	Transparent
	P-Asserted-Identity Header Mode	Add
	Diversion Header Mode	As Is
	History-Info Header Mode	As Is
	Session Expires Mode	Transparent
	Remote Update Support	Supported
	Remote re-INVITE	Supported
	Remote Delayed Offer Support	Supported
	Remote Representation Mode	According to Operation
	Keep Incoming Via Headers	According to Operation
Keep Incoming Routing Headers	According to Operation	
Keep User-Agent Header	According to Operation	

At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

2. Click **Apply**.

4.8 Step 8: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-SBC 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. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In the example scenario, IP Groups must be configured for the following IP entities:

- Skype for Business Server 2015 (Mediation Server) located on LAN
- ITSP SIP Trunk located on WAN

➤ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Add an IP Group for the Skype for Business Server 2015:

Parameter	Value
Index	1
Name	S4B
Type	Server
Proxy Set	S4B
IP Profile	S4B
Media Realm	MRLan
SIP Group Name	(according to ITSP requirement)


3. Configure an IP Group for the ITSP SIP Trunk:




Parameter	Value
Index	2
Name	ITSP
Topology Location	Up
Type	Server
Proxy Set	ITSP
IP Profile	ITSP
Media Realm	MRWan
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-20: Configured IP Groups in IP Group Table

IP Groups (3)

+ New Edit  Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPG	 DefaultS	Server	Not Configur	ProxySet_0	--	--		Disable	-1	-1
1	S4B	 DefaultS	Server	Not Configur	S4B	S4B	MRLan		Enable	-1	-1
2	ITSP	 DefaultS	Server	Not Configur	ITSP	ITSP	MRWan		Enable	-1	-1

4.9 Step 9: SIP TLS Connection Configuration

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

4.9.1 Step 9a: 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 E-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 4-21: Configuring NTP Server Address

NTP SERVER	
Primary NTP Server Address (IP or FQDN)	<input type="text" value="10.15.27.1"/>
Secondary NTP Server Address (IP or FQDN)	<input type="text"/>
NTP Update Interval	Hours: <input type="text" value="24"/> Minutes: <input type="text" value="0"/>
NTP Authentication Key Identifier	<input type="text" value="0"/>
NTP Authentication Secret Key	<input type="text"/>

3. Click **Apply**.

4.9.2 Step 9b: Configure the TLS version

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

➤ **To configure the 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 4-22: Configuring TLS version

The screenshot shows the configuration window for the default TLS Context. The 'GENERAL' tab is selected, and the 'OCSP' tab is also visible. The 'TLS Version' dropdown menu is highlighted with an arrow, showing the selected option 'TLSv1.0 TLSv1.1 and TLSv1.2'. The 'OCSP' tab shows the 'OCSP Server' set to 'Disable', 'Primary OCSP Server' and 'Secondary OCSP Server' both set to '0.0.0.0', 'OCSP Port' set to '2560', and 'OCSP Default Response' set to 'Reject'. The 'GENERAL' tab shows the 'Index' set to '0', 'Name' set to 'default', 'Cipher Server' set to 'RC4:EXP', 'Cipher Client' set to 'ALL:!ADH', and 'Strict Certificate Extension Validation' set to 'Disable'. The 'APPLY' button is highlighted in blue.

4. Click **Apply**.

4.9.3 Step 9c: Configure a Certificate

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

The procedure involves the following main steps:

- a. Generating a Certificate Signing Request (CSR).
- b. Requesting Device Certificate from CA.
- c. Obtaining Trusted Root Certificate from CA.
- d. Deploying Device and Trusted Root Certificates on E-SBC.



Note: The Subject Name (CN) field parameter should be identically configured in the DNS Active Directory and Topology Builder (see Section 3.1 on page 13).

➤ **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 E-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 4-23: Certificate Signing Request – Creating CSR

← TLS Context [#0] > Context Certificates

CERTIFICATE SIGNING REQUEST

Subject Name [CN]	<input type="text" value="ITSP.S4B.interop"/>
Organizational Unit [OU] (optional)	<input type="text"/>
Company name [O] (optional)	<input type="text"/>
Locality or city name [L] (optional)	<input type="text"/>
State [ST] (optional)	<input type="text"/>
Country code [C] (optional)	<input type="text"/>
Signature Algorithm	<input type="text" value="SHA-1"/>

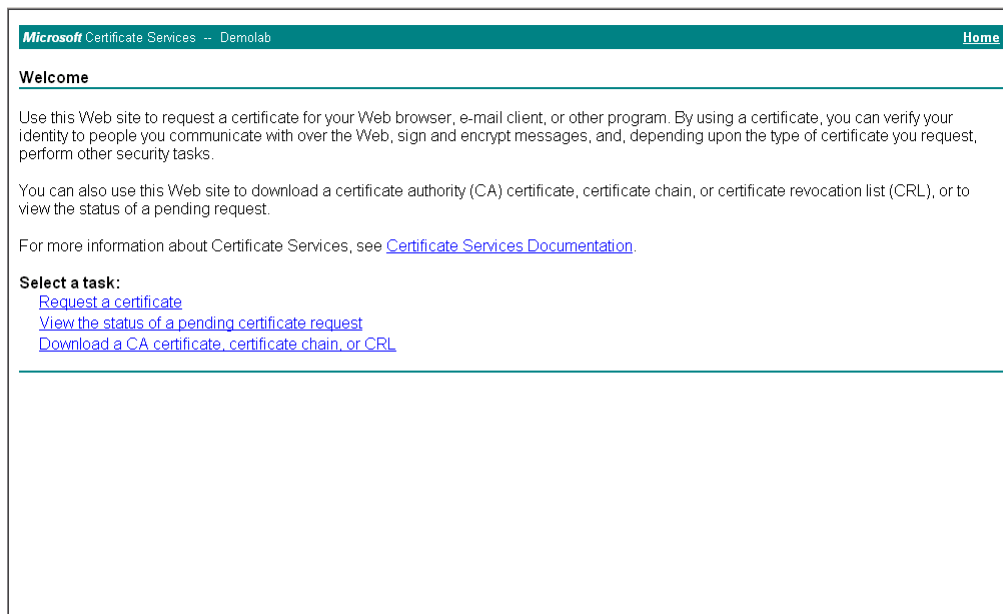
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```

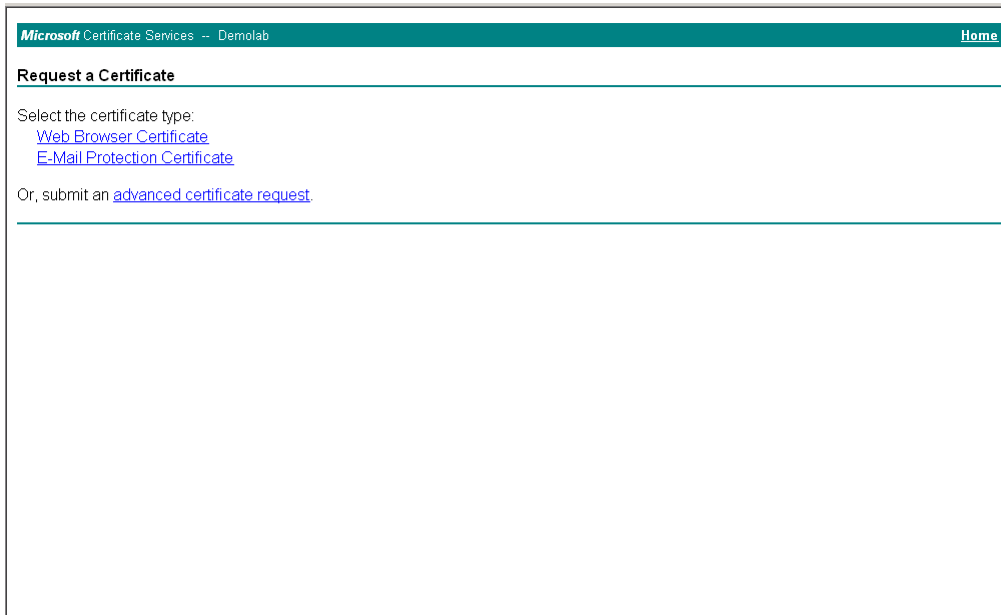
-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAIBADAbMRkwFwYDVQQDDBBjVFNQL1M0Qi5pbmR1cm9wMIGfMA0GC5qG
SIb3DQEBAQUAA4GNADCBiQKBgQCzEs8XTnY8be/t77eEDG7rTg747GQ3ODFOC4Rs
x+e9KfbErZgxMYqGT8u04AU0wU9LUPkq+8gI6w2bg3boW0kg/9hrnNL2rf1tGcn
30oShP05PiKmRNZnCC090b03tbr9kuHmlwPRQ7yT6k7xS3X8bSigqT4LQbJBT1tt
hdH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAim/GA2E1ZQbZaR6CZyIawilT
u65w450NFHmaCluHSyZ8keM8d1Ux14hkW7t5ygAD8KbxVkJHRVaCgcQrAK2v8u1Pf
TvN+bwJ+kQ0d59CiXa82e0o1W83buPq5+qMDGTF+MyJWGVf8SIc1c6+zFoc+BEZY
7tQ8y0J8od0aDhStDfQ=
-----END CERTIFICATE REQUEST-----
    
```

- 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*.
- Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

Figure 4-24: Microsoft Certificate Services Web Page



- Click **Request a certificate**.

Figure 4-25: Request a Certificate Page


Microsoft Certificate Services -- Demolab Home

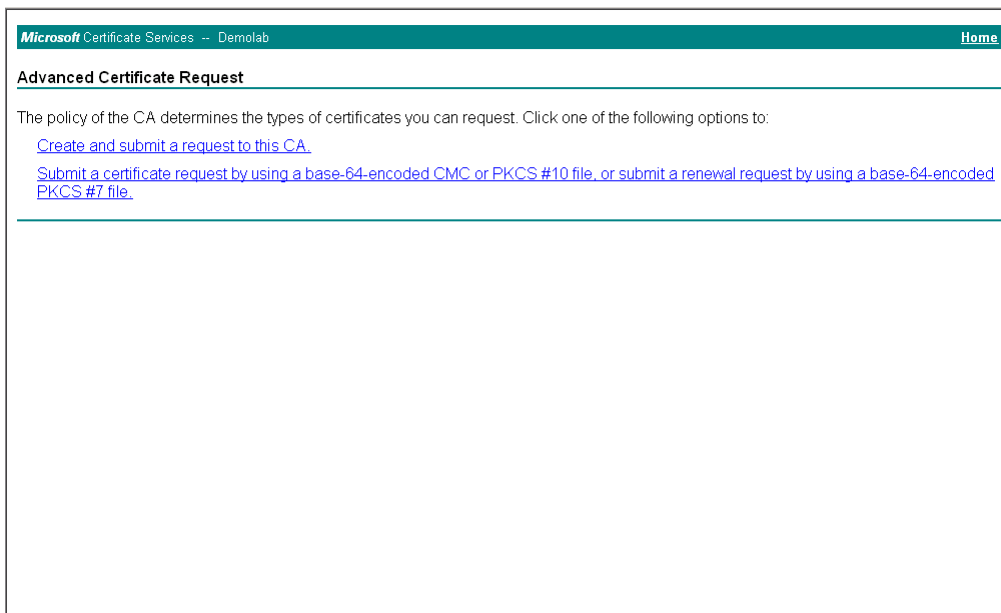
Request a Certificate

Select the certificate type:

- [Web Browser Certificate](#)
- [E-Mail Protection Certificate](#)

Or, submit an [advanced certificate request](#).

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

Figure 4-26: 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.](#)
- [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.](#)

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

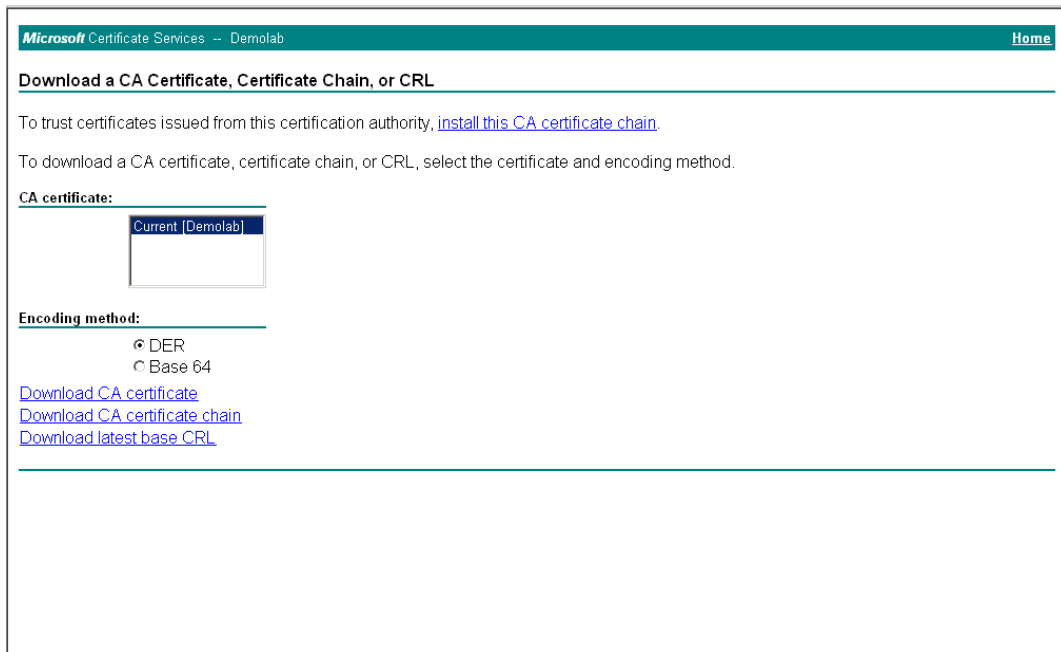
Figure 4-27: Submit a Certificate Request or Renewal Request Page

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

Figure 4-28: Certificate Issued Page

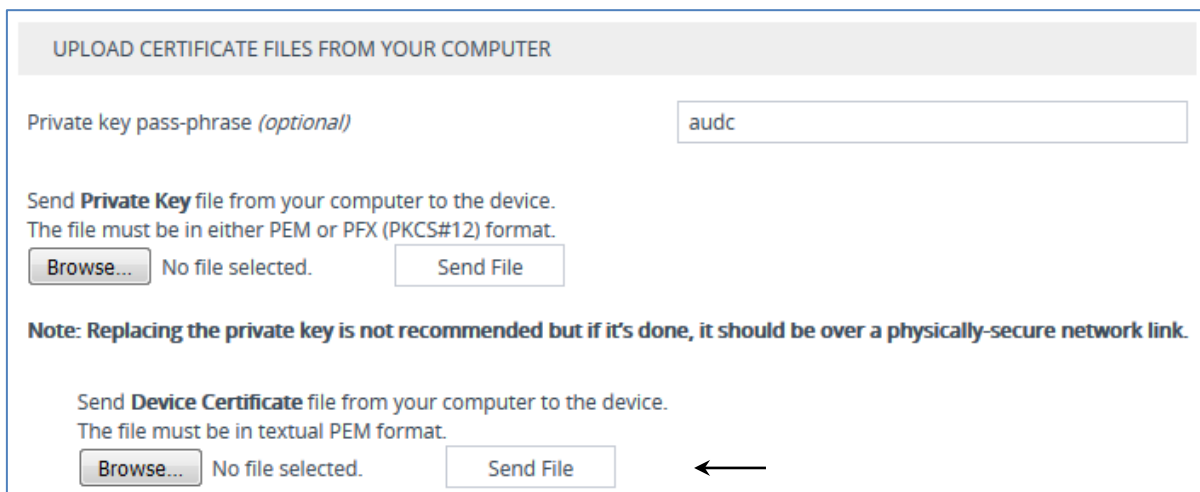
12. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.
13. Save the file as *gateway.cer* to a folder on your computer.
14. Click the **Home** button or navigate to the certificate server at <http://<Certificate Server>/CertSrv>.
15. Click **Download a CA certificate,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

Figure 4-29: Download a CA Certificate, Certificate Chain, or CRL Page



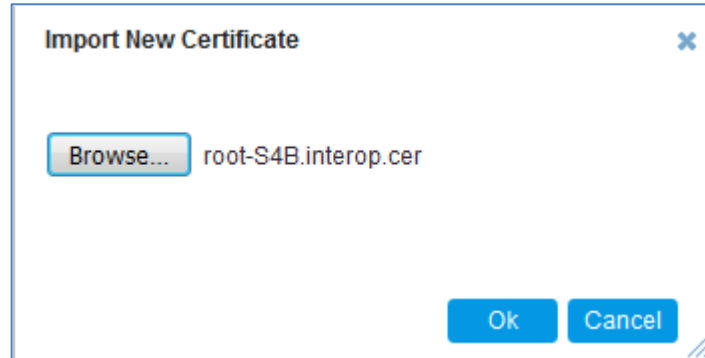
16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file as *certroot.cer* to a folder on your computer.
19. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts 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 E-SBC.

Figure 4-30: Upload Device Certificate Files from your Computer Group



20. In the E-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 4-31: 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 E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 76).

4.10 Step 10: Configure SRTP

This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 4.6 on page 45).

➤ **To configure media security:**

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

Figure 4-32: Configuring SRTP

2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 76).



Note: If you are implementing SRTP, make sure that you also configure the Lync server for SRTP 'Encryption Support Level'). For more information, see [here](#).

4.11 Step 11: Configure Maximum IP Media Channels

This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.



Note: This step is required **only** if transcoding is required.

➤ **To configure the maximum number of IP media channels:**

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

Figure 4-33: Configuring Number of Media Channels

The screenshot shows the 'Media Settings' page with a 'GENERAL' tab. The following settings are visible:

Setting	Value
NAT Traversal	Disable NAT
Enable Continuity Tones	Disable
Inbound Media Latch Mode	Dynamic
Number of Media Channels	100
Enforce Media Order	Disable
SDP Session Owner	AudiocodesGW

An arrow points to the 'Number of Media Channels' field, which is highlighted with a blue lightning bolt icon.

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., 100).
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 76).

4.12 Step 12: 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 E-SBC 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 (as configured in Section 4.8 on page 52,) to denote the source and destination of the call.

In the example scenario, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business Server 2015 (LAN) and ITSP SIP Trunk (DMZ):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
- Calls from Skype for Business Server 2015 to ITSP SIP Trunk
- Calls from ITSP SIP Trunk to Skype for Business Server 2015

➤ **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. Configure a rule to terminate SIP OPTIONS messages received from the both LAN and DMZ:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Terminate OPTIONS (arbitrary descriptive name)
Source IP Group	Any
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

Figure 4-34: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

- b. Click **Apply**.
- 3. Configure a rule to route calls from Skype for Business Server 2015 to ITSP SIP Trunk:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	1
Name	S4B to ITSP (arbitrary descriptive name)
Source IP Group	S4B
Destination Type	IP Group
Destination IP Group	ITSP
Destination SIP Interface	ITSP

Figure 4-35: Configuring IP-to-IP Routing Rule for S4B to ITSP

IP-to-IP Routing [S4B to ITSP]
– x

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL	ACTION
Index <input style="width: 80%;" type="text" value="1"/>	Destination Type IP Group
Name • S4B to ITSP	Destination IP Group • #2 [ITSP] View
Alternative Route Options Route Row	Destination SIP Interface • #1 [ITSP] View
MATCH	
Source IP Group • #1 [S4B] View	Destination Address <input style="width: 80%;" type="text"/>
Request Type All	Destination Port <input style="width: 80%;" type="text" value="0"/>
Source Username Prefix <input style="width: 80%;" type="text" value="*"/>	Destination Transport Type
Source Host <input style="width: 80%;" type="text" value="*"/>	Call Setup Rules Set ID <input style="width: 80%;" type="text" value="-1"/>
Source Tag <input style="width: 80%;" type="text"/>	Group Policy Sequential
	Cost Group -- View

Cancel
APPLY

b. Click **Apply**.

4. Configure rule to route calls from ITSP SIP Trunk to Skype for Business Server 2015:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	2
Name	ITSP to S4B (arbitrary descriptive name)
Source IP Group	ITSP
Destination Type	IP Group
Destination IP Group	S4B
Destination SIP Interface	S4B

Figure 4-36: Configuring IP-to-IP Routing Rule for ITSP to S4B

- b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 4-37: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (3)

+ New Edit Insert ↑ ↓ | Page 1 of 1 | Show 10 records per page

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 O	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Address:	--	--	internal
1	S4B to ITSP	Default_SBC	Route Row	S4B	All	*	*	IP Group	ITSP	ITSP	
2	ITSP to S4B	Default_SBC	Route Row	ITSP	All	*	*	IP Group	S4B	S4B	



Note: The routing configuration may change according to your specific deployment topology.

4.13 Step 13: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.8 on page 52) to denote the source and destination of the call.



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

For this example scenario, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from the ITSP SIP Trunk IP Group to the Skype for Business Server 2015 IP Group for any destination username prefix.

➤ **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 + toward S4B
Source IP Group	SP
Destination IP Group	S4B
Destination Username Prefix	* (asterisk sign)
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 4-38: Configuring IP-to-IP Outbound Manipulation Rule

3. Click **Apply**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between Skype for Business Server 2015 IP Group and ITSP SIP Trunk IP Group:

Figure 4-39: Example of Configured IP-to-IP Outbound Manipulation Rules

INDEX	NAME	ROUTING POLICY	ADDITION MANIPULATION	SOURCE IP GROUP	DESTINATION IP GROUP	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	MANIPULATION ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Add + toward S4B	Default_SE	No	ITSP	S4B	*	*	Destination URI	0	0	255	+	
1	Remove + from S4B	Default_SE	No	S4B	ITSP	*	+	Destination URI	1	0	255		
2	Remove + from S4B	Default_SE	No	S4B	ITSP	+	*	Source URI	1	0	255		

Rule Index	Description
1	Calls from ITSP IP Group to S4B IP Group with any destination number (*), add "+" to the prefix of the destination number.
2	Calls from S4B IP Group to ITSP IP Group with the prefix destination number "+", remove "+" from this prefix.
3	Calls from S4B IP Group to ITSP IP Group with source number prefix "+", remove the "+" from this prefix.

4.14 Step 14: Configure Message Manipulation Rules

This step describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

See an example below of a message manipulation rule configuration; use the *SBC User's Manual* for detailed instructions on how to configure message manipulation rules according to your requirements.

In the example scenario, the configured manipulation rule replaces the user part of the SIP From Header with the value from the SIP History-Info Header.

➤ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for ITSP SIP Trunk. This rule applies to messages sent to the ITSP SIP Trunk IP Group in a call forward scenario.

Parameter	Value
Index	0
Name	Call Forward
Manipulation Set ID	4
Condition	header.history-info.0 regex (<sip:)(.*)((@)(.))
Action Subject	header.from.url.user
Action Type	Modify
Action Value	\$2

Figure 4-40: Configuring SIP Message Manipulation Rule 0 (for ITSP SIP Trunk)

The screenshot shows the 'Message Manipulations' configuration window. It is divided into several sections:

- GENERAL:**
 - Index: 0
 - Name: Call Forward
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: header from url user
 - Action Type: Modify
 - Action Value: \$2
- MATCH:**
 - Message Type: (empty)
 - Condition: header.history-info.0 regex (< sip: X.*)(@ X.*)

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

3. Assign Manipulation Set ID 4 to the ITSP SIP trunk IP Group:
 - a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
 - b. Select the row of the ITSP SIP trunk IP Group, and then click **Edit**.
 - c. Set the 'Outbound Message Manipulation Set' field to 4.

Figure 4-41: Assigning Manipulation Set 4 to the ITSP SIP Trunk IP Group

The screenshot shows the 'IP Groups [SP]' configuration window. It is divided into several sections:

- GENERAL:**
 - Index: 1
 - Name: SP
 - Topology Location: Up
 - Type: Server
 - Proxy Set: #1 [SP]
 - IP Profile: #2 [SP]
 - Media Realm: #1 [MRWan]
 - SIP Group Name: (empty)
 - Created By Routing Server: No
 - Used By Routing Server: Not Used
- QUALITY OF EXPERIENCE:**
 - QoE Profile: --
 - Bandwidth Profile: --
- MESSAGE MANIPULATION:**
 - Inbound Message Manipulation Set: -1
 - Outbound Message Manipulation Set: 4
 - Message Manipulation User-Defined String 1: (empty)
 - Message Manipulation User-Defined String 2: (empty)

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

- d. Click **Apply**.

4.15 Step 15: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the ITSP SIP Trunk on behalf of Skype for Business Server 2015. The ITSP SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Skype for Business Server 2015 IP Group and the Serving IP Group is ITSP SIP Trunk IP Group.

➤ **To configure a registration account:**

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from , for example:

Parameter	Value
Served IP Group	S4B
Application Type	SBC
Serving IP Group	ITSP
Host Name	As provided by the SIP Trunk provider
Register	Regular
Contact User	1234567890 (trunk main line)
User Name	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-42: Configuring a SIP Registration Account

The screenshot shows a web-based configuration window titled "Accounts". At the top, there is a dropdown menu for "Served IP Group" with the value "#1 [S4B]". Below this, the configuration is split into two columns: "GENERAL" and "CREDENTIALS".

GENERAL fields:

- Index: 0
- Served Trunk Group: -1
- Application Type: SBC
- Serving IP Group: #2 [ITSP] (with a "View" link)
- Host Name: HostName.com
- Register: Regular
- Contact User: 1234567890

CREDENTIALS fields:

- User Name: UserName
- Password: *

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

4. Click **Apply**.

4.16 Step 16: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

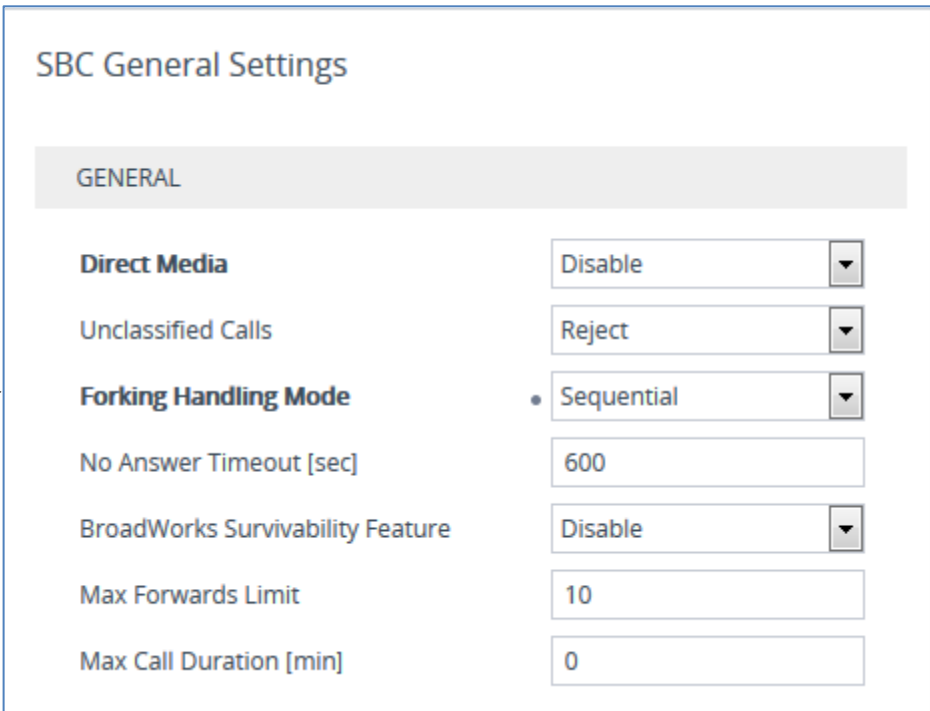
4.16.1 Step 16a: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. In the example scenario, if a SIP 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if a 180 response without SDP is received. It is mandatory to set this field for the Skype for Business Server 2015 environment.

➤ **To configure call forking:**

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

Figure 4-43: Configuring Forking Mode



The screenshot shows the 'SBC General Settings' configuration page. A grey bar at the top indicates the 'GENERAL' tab is selected. Below this, several settings are listed in a table-like format:

GENERAL	
Direct Media	Disable
Unclassified Calls	Reject
Forking Handling Mode	• Sequential
No Answer Timeout [sec]	600
BroadWorks Survivability Feature	Disable
Max Forwards Limit	10
Max Call Duration [min]	0

An arrow points to the 'Forking Handling Mode' dropdown menu, which is currently set to 'Sequential'.

3. Click **Apply**.

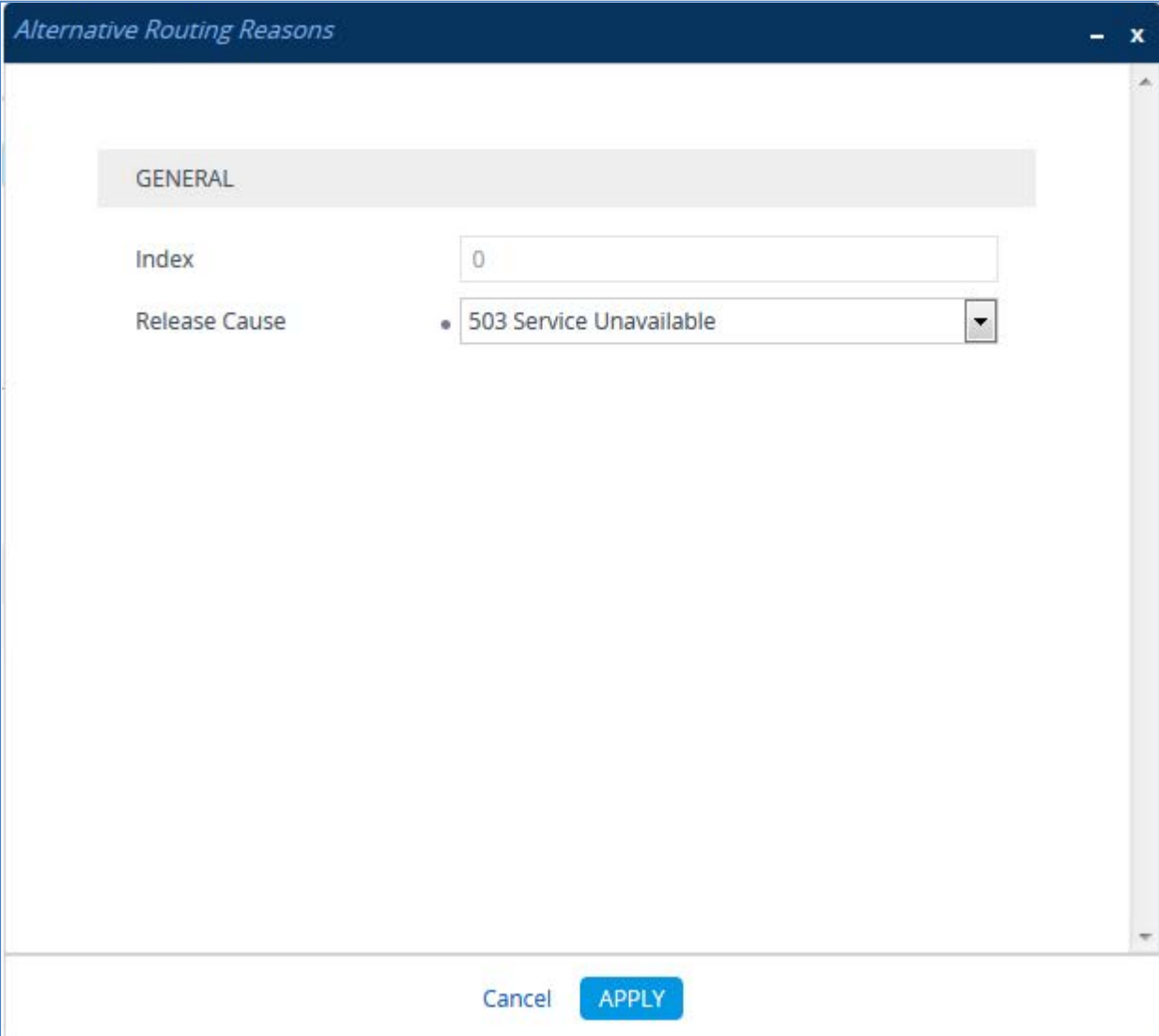
4.16.2 Step 16b: Configure SBC Alternative Routing Reasons

This step describes how to configure the E-SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case E-SBC attempts to locate an alternative route for the call.

➤ **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 **503 Service Unavailable**.

Figure 4-44: SBC Alternative Routing Reasons Table



The screenshot shows a configuration window titled "Alternative Routing Reasons". The window has a dark blue header with the title and standard window controls (minimize, maximize, close). Below the header is a light gray bar labeled "GENERAL". Underneath, there are two configuration fields: "Index" with a text input field containing the number "0", and "Release Cause" with a dropdown menu currently showing "503 Service Unavailable". At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

4. Click **Apply**.

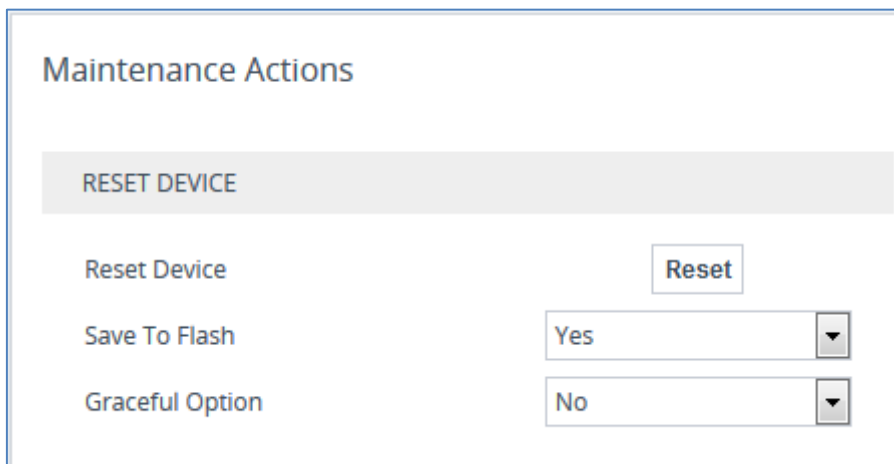
4.17 Step 17: Reset the E-SBC

After you have completed the configuration of the E-SBC described in this chapter, save ("burn") the configuration to the E-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 4-45: Resetting the E-SBC



The screenshot shows the 'Maintenance Actions' web interface. 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 controls:

- The first row has the label 'Reset Device' on the left and a 'Reset' button on the right.
- The second row has the label 'Save To Flash' on the left and a dropdown menu on the right showing 'Yes'.
- The third row has the label 'Graceful Option' on the left and a dropdown menu on the right showing '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.

A Configuring SBC to Send 414 Request - URI Too Long

The procedure below describes how to configure the SBC to send a 414 Request-URI Too Long response, when it encounters a Request URI it cannot handle due to excessive length.

When the SBC receives an INVITE with a long Request URI (a condition rule), it routes it to an unknown destination IP address (i.e., 1.1.1.1). It sets a variable for this call to 1. After a timeout, the SBC generates an internal 408 Request Timeout response. Using message manipulation, the SBC converts this response to a 414 Request-URI Too Long response (only if the variable value is 1).

➤ **To configure a condition for this route:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**).
2. Click the **New** tab and configure the parameters as follows:

Parameter	Example Setting
Index	0
Name	R-URI Too Long
Condition	header.request-uri.url.host.name len>'100' (You can choose the length of the Request-URI to process)

Figure A-1: Configuring a Condition for the Route

The screenshot shows a window titled "Message Conditions [R-URI Too Long]". It has a "GENERAL" tab selected. The configuration fields are as follows:

- Index:** 0
- Name:** R-URI Too Long
- Condition:** header.request-uri.url.host.name len>'100'

3. Click **Apply**.

- **To configure IP-to-IP routing route:**
- 1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
- 2. Add a rule to route long-URI calls to unknown IP address:
 - a. Click **Insert** (This rule should be the first rule in the table).
 - b. Configure the parameters like this:

Parameter	Example Setting
Index	0 (This rule should be the first rule in the table)
Message Condition	R-URI Too Long (The condition configured above)
Destination Type	Dest Address
Destination Address	1.1.1.1 (fake IP address)

Figure A-2: IP-to-IP Routing Rule for Long-URI Calls

The screenshot shows the configuration window for an IP-to-IP Routing rule named "R-URI Too Long". The window title is "IP-to-IP Routing [R-URI Too Long]". At the top, the "Routing Policy" is set to "#0 [Default_SBCRoutingPolicy]".

The configuration is divided into three main sections:

- GENERAL:**
 - Index: 0
 - Name: R-URI Too Long
 - Alternative Route Options: Route Row
- MATCH:**
 - Source IP Group: Any
 - Request Type: All
 - Source Username Prefix: *
 - Source Host: *
 - Source Tag: (empty)
- ACTION:**
 - Destination Type: Dest Address
 - Destination IP Group: --
 - Destination SIP Interface: --
 - Destination Address: 1.1.1.1
 - Destination Port: 0
 - Destination Transport Type: (empty)
 - Call Setup Rules Set ID: -1
 - Group Policy: Sequential
 - Cost Group: --

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

- c. Click **Apply**.

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

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 1) to set a variable to **1** in the case of a long-URI call:
 - a. Click **New**.
 - b. Configure the parameters as follows:

Parameter	Example Setting
Index	0
Name	Long URI
Manipulation Set ID	1
Message Type	invite.request
Condition	header.request-uri.url.host.name len>'100'
Action Subject	var.call.src.0
Action Type	Modify
Action Value	1

Figure A-3: Manipulation Rule to Set a Variable to '1' in Case of Long-URI Call

The screenshot shows a configuration window titled "Message Manipulations [Long URI]". It is divided into three main sections: GENERAL, ACTION, and MATCH. Each section contains several input fields and dropdown menus. At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

Section	Parameter	Value
GENERAL	Index	0
	Name	Long URI
	Manipulation Set ID	1
	Row Role	Use Current Condition
ACTION	Action Subject	var.call.src.0
	Action Type	Modify
	Action Value	1
MATCH	Message Type	invite.request
	Condition	header.request-uri.url.host.name len>'100'

- c. Click **Apply**.

3. Configure a new manipulation rule (Manipulation Set 2) to convert '408' response to '414':
 - a. Click **New**.
 - b. Configure the parameters as follows:

Parameter	Example Setting
Index	1
Name	Long URI
Manipulation Set ID	2
Message Type	invite.response.408
Condition	var.call.src.0 == '1'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'414'

Figure A-4: Manipulation Rule to Convert '408' to '414'

The screenshot shows a configuration window titled "Message Manipulations [Long URI]". It is divided into three main sections: GENERAL, ACTION, and MATCH. Each section contains several input fields with radio buttons next to them, indicating they are selected.

- GENERAL:**
 - Index: 1
 - Name: Long URI
 - Manipulation Set ID: 2
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: header.request-uri.methodtype
 - Action Type: Modify
 - Action Value: '414'
- MATCH:**
 - Message Type: invite.response.408
 - Condition: var.call.src.0 == '1'

At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

- c. Click **Apply**.

4. Assign Manipulation Set IDs 1 and 2 to the Skype for Business 2015 IP Group:
 - a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
 - b. Select the row of the Skype for Business 2015 IP Group, and then click **Edit**.
 - c. Set the 'Inbound Message Manipulation Set' field to **1**.
 - d. Set the 'Outbound Message Manipulation Set' field to **2**.

Figure A-5: Assigning Manipulation Set to the Skype for Business 2015 IP Group

The screenshot shows the configuration window for IP Groups, specifically for the S4B group. The 'MESSAGE MANIPULATION' section is expanded, showing the following settings:

- Inbound Message Manipulation Set:** 1
- Outbound Message Manipulation Set:** 2
- Message Manipulation User-Defined String 1:** (empty)
- Message Manipulation User-Defined String 2:** (empty)

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons. The 'APPLY' button is highlighted in blue.

- e. Click **Apply**.

This page is intentionally left blank.

B Configuring SBC to Send 503 Instead 500 Toward Skype for Business

The procedure below describes how to configure the SBC to send a 503 Service Unavailable instead of 500 Server Internal Error response toward Skype for Business, when the routed IP Group is down or no route is available.

When the SBC receives an INVITE from Skype for Business and determines that no route is available (IP Group is down), the usual behavior is to send 500 Server Internal Error response to the Skype for Business. However, if there is alternative trunk configured in the Skype for Business, it will re-route only by receiving 503 Service Unavailable response. In order to overcome this problem two message manipulation rules are inserted.

➤ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set **2**). This rule applies to reply messages sent to the Skype for Business IP Group in cases where the destination route is not reachable.

Parameter	Value
Index	0
Name	Change 500 to 503
Manipulation Set ID	2
Message Type	invite.response.500
Condition	header.request-uri.methodtype=='500'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'503'

Figure B-1: Configuring SIP Message Manipulation Rule

The screenshot shows the configuration window for a SIP message manipulation rule. The window title is "Message Manipulations [Change 500 to 503]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

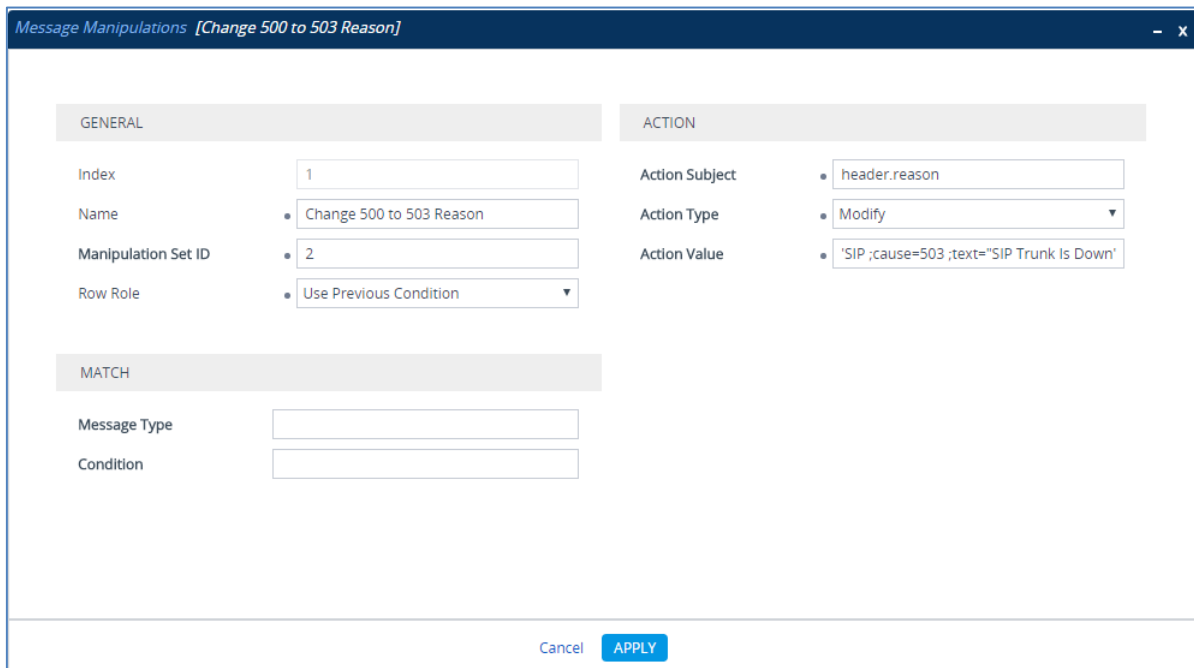
- GENERAL:**
 - Index: 0
 - Name: Change 500 to 503
 - Manipulation Set ID: 2
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: header.request-uri.methodtype
 - Action Type: Modify
 - Action Value: '503'
- MATCH:**
 - Message Type: invite.response.500
 - Condition: header.request-uri.methodtype=='500'

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

3. Configure another manipulation rule (Manipulation Set 2). This rule applies to reply messages sent to the Skype for Business IP Group in cases where the destination route is not reachable.

Parameter	Value
Index	1
Name	Change 500 to 503 Reason
Manipulation Set ID	2
Row Role	Use Previous Condition
Action Subject	header.reason
Action Type	Modify
Action Value	'SIP ;cause=503 ;text="SIP Trunk Is Down"'

Figure B-2: Configuring SIP Message Manipulation Rule



The screenshot shows a configuration window titled "Message Manipulations [Change 500 to 503 Reason]". The window is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 1
 - Name: Change 500 to 503 Reason
 - Manipulation Set ID: 2
 - Row Role: Use Previous Condition
- ACTION:**
 - Action Subject: header.reason
 - Action Type: Modify
 - Action Value: 'SIP ;cause=503 ;text="SIP Trunk Is Down"'
- MATCH:**
 - Message Type: (empty field)
 - Condition: (empty field)

At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

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

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com



Document #: LTRT-54030