

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

Version 7.2



**Microsoft Partner**

Gold Communications





---

## Table of Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	Intended Audience .....	7
1.2	About AudioCodes E-SBC Product Series.....	7
<b>2</b>	<b>Component Information.....</b>	<b>9</b>
2.1	AudioCodes E-SBC Version .....	9
2.2	Bell Canada SIP Trunking Version .....	9
2.3	Microsoft Skype for Business Server 2015 Version .....	9
2.4	Interoperability Test Topology .....	10
2.4.1	Environment Setup .....	11
2.4.2	Known Limitations.....	11
<b>3</b>	<b>Configuring Skype for Business Server 2015.....</b>	<b>13</b>
3.1	Configuring the E-SBC as an IP / PSTN Gateway .....	13
3.2	Configuring the "Route" on Skype for Business Server 2015.....	21
<b>4</b>	<b>Configuring AudioCodes E-SBC.....</b>	<b>31</b>
4.1	Step 1: IP Network Interfaces Configuration .....	32
4.1.1	Step 1a: Configure VLANs.....	33
4.1.2	Step 1b: Configure Network Interfaces.....	34
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 .....	46
4.7	Step 7: Configure IP Profiles .....	49
4.8	Step 8: Configure IP Groups.....	53
4.9	Step 9: SIP TLS Connection Configuration.....	55
4.9.1	Step 9a: Configure the NTP Server Address.....	55
4.9.2	Step 9b: Configure the TLS version .....	56
4.9.3	Step 9c: Configure a Certificate.....	57
4.10	Step 10: Configure SRTP .....	63
4.11	Step 11: Configure Maximum IP Media Channels .....	64
4.12	Step 12: Configure IP-to-IP Call Routing Rules .....	65
4.13	Step 13: Configure IP-to-IP Manipulation Rules.....	70
4.14	Step 14: Configure Message Manipulation Rules .....	72
4.15	Step 15: Configure Registration Accounts .....	83
4.16	Step 16: Miscellaneous Configuration.....	85
4.16.1	Step 16a: Configure Call Forking Mode .....	85
4.16.2	Step 16b: Configure SBC Alternative Routing Reasons .....	86
4.16.3	Step 16c: Configure SBC Session Refreshing Policy .....	87
4.17	Step 17: Reset the E-SBC .....	88
<b>A</b>	<b>AudioCodes INI File .....</b>	<b>89</b>
<b>B</b>	<b>Configuring Dynamic ONND .....</b>	<b>101</b>
B.1	Configure SIP Message Manipulation Rules.....	101

**This page is intentionally left blank.**

## Notice

This document describes how to connect the Microsoft Skype for Business Server 2015 and Bell Canada 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:** October-30-2016

## Trademarks

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 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.

## 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](http://www.audiocodes.com/support).

## Document Revision Record

LTRT	Description
39234	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 Bell Canada'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 Bell Canada Partners who are responsible for installing and configuring Bell Canada'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

<b>SBC Vendor</b>	AudioCodes
<b>Models</b>	<ul style="list-style-type: none"> <li>▪ Mediant 500 E-SBC</li> <li>▪ Mediant 500L Gateway &amp; E-SBC</li> <li>▪ Mediant 800B Gateway &amp; E-SBC</li> <li>▪ Mediant 1000B Gateway &amp; E-SBC</li> <li>▪ Mediant 2600 E-SBC</li> <li>▪ Mediant 4000 SBC</li> <li>▪ Mediant 4000B SBC</li> <li>▪ Mediant 9000 SBC</li> <li>▪ Mediant Software SBC (SE and VE)</li> </ul>
<b>Software Version</b>	SIP_7.20A.001.501
<b>Protocol</b>	<ul style="list-style-type: none"> <li>▪ SIP/UDP (to the Bell Canada SIP Trunk)</li> <li>▪ SIP/TCP or TLS (to the S4B FE Server)</li> </ul>
<b>Additional Notes</b>	None

### 2.2 Bell Canada SIP Trunking Version

Table 2-2: Bell Canada Version

<b>Vendor/Service Provider</b>	Bell Canada
<b>SSW Model/Service</b>	BroadSoft
<b>Software Version</b>	
<b>Protocol</b>	SIP
<b>Additional Notes</b>	None

### 2.3 Microsoft Skype for Business Server 2015 Version

Table 2-3: Microsoft Skype for Business Server 2015 Version

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

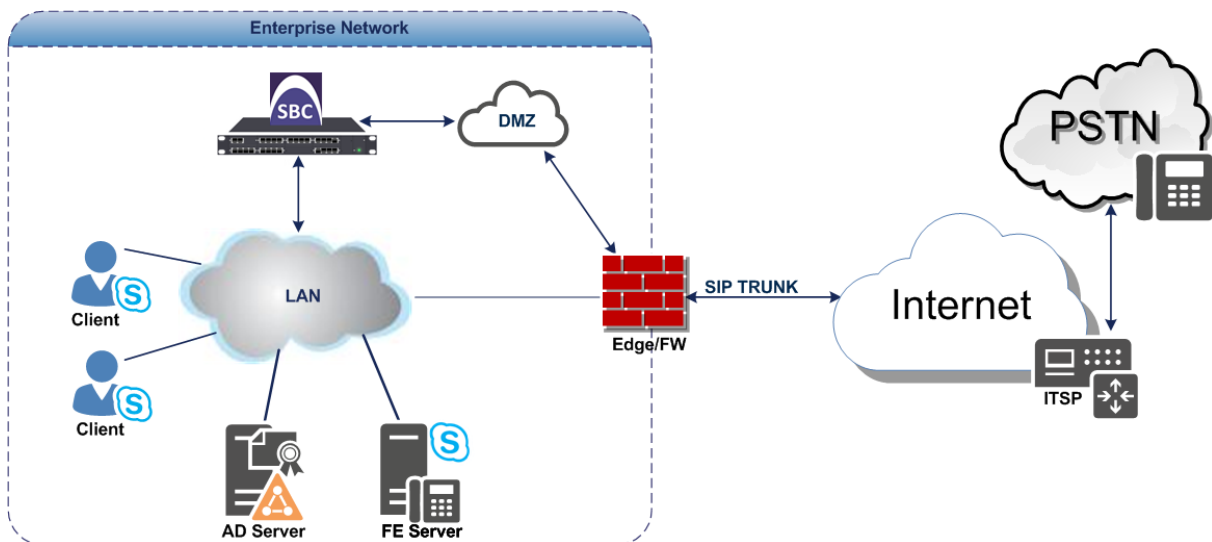
## 2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Bell Canada SIP Trunk with Skype for Business 2015 was done using the following topology setup:

- 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 Bell Canada'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 Bell Canada's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

**Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Skype for Business with Bell Canada SIP Trunk**



## 2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

**Table 2-4: Environment Setup**

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

## 2.4.2 Known Limitations

The following limitation was observed in the interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Skype for Business Server 2015 and Bell Canada's SIP Trunk:

- If, following a "603 Decline", an Error Response is sent from the Microsoft Skype for Business Server 2015, Bell Canada's SIP Trunk continues to send re-INVITEs and does not disconnect the call. To resolve this and disconnect the call correctly, a message manipulation rule is used to replace the Error Response with a "486 Busy Here" (see Section 4.14 on page 72).

**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.



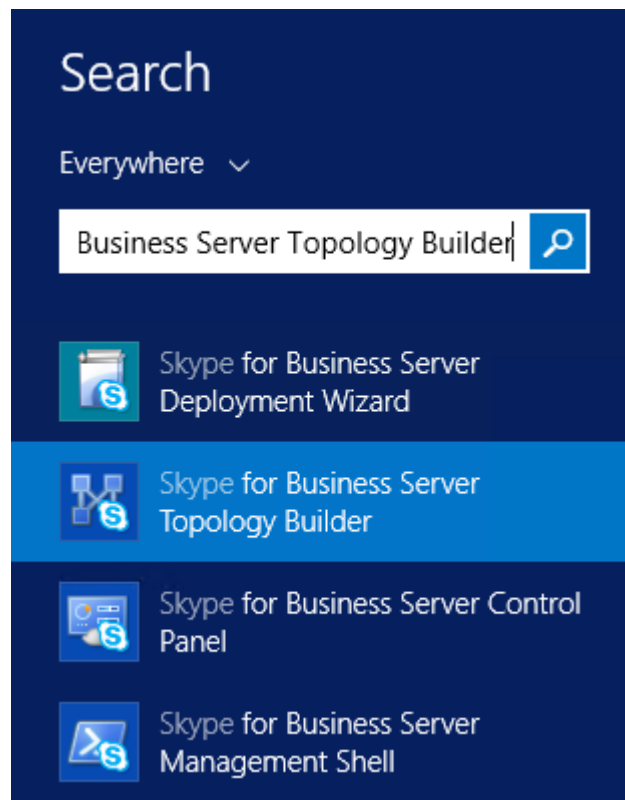
**Note:** Dial plans, voice policies, and PSTN usages are also necessary for Enterprise voice deployment; however, they are beyond the scope of this document.

### 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.

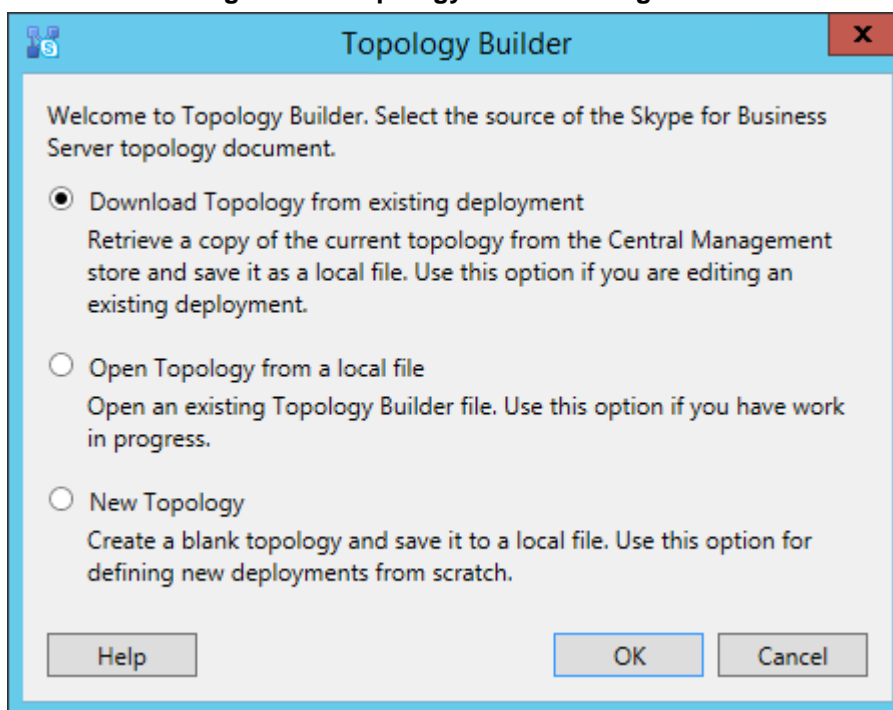
- **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**
- 1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

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



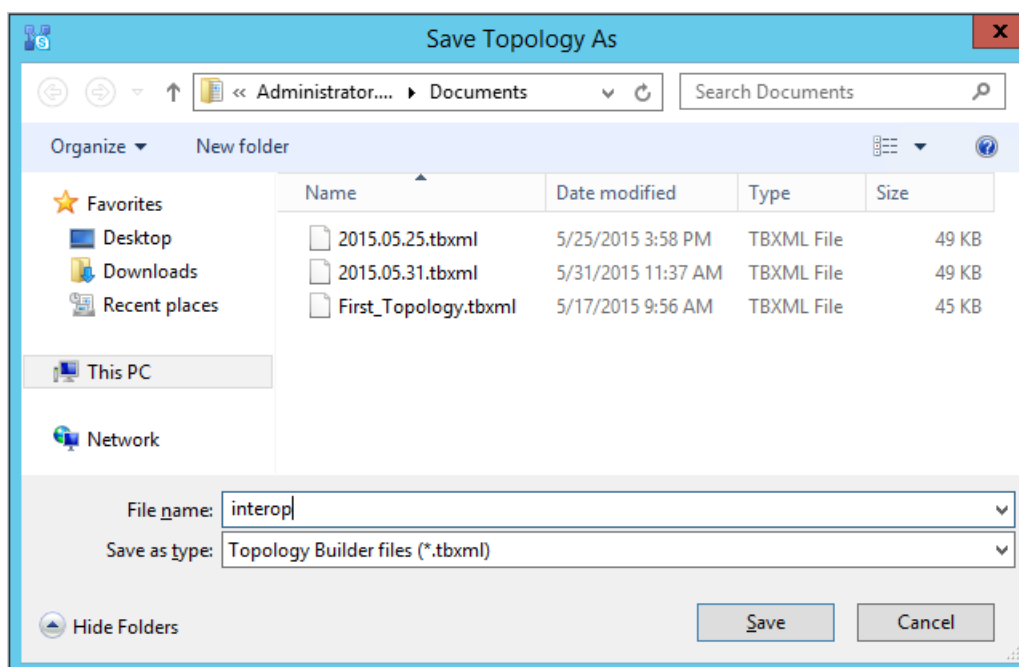
The following is displayed:

**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:

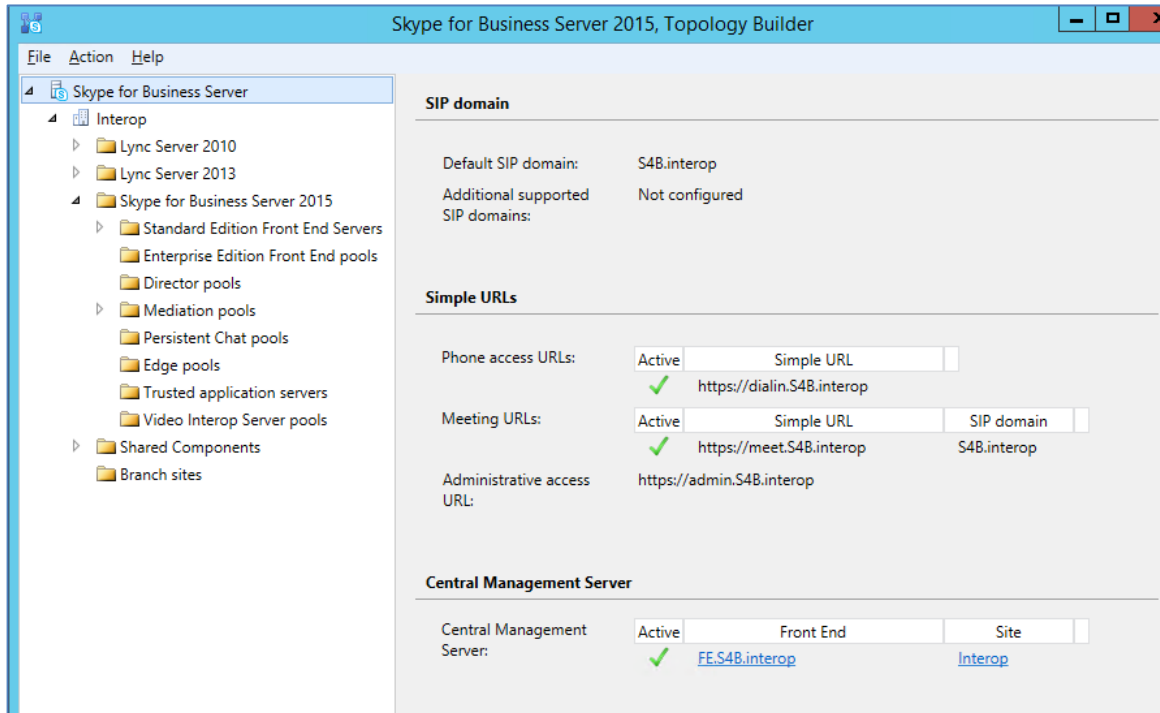
**Figure 3-3: Save Topology Dialog Box**



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.

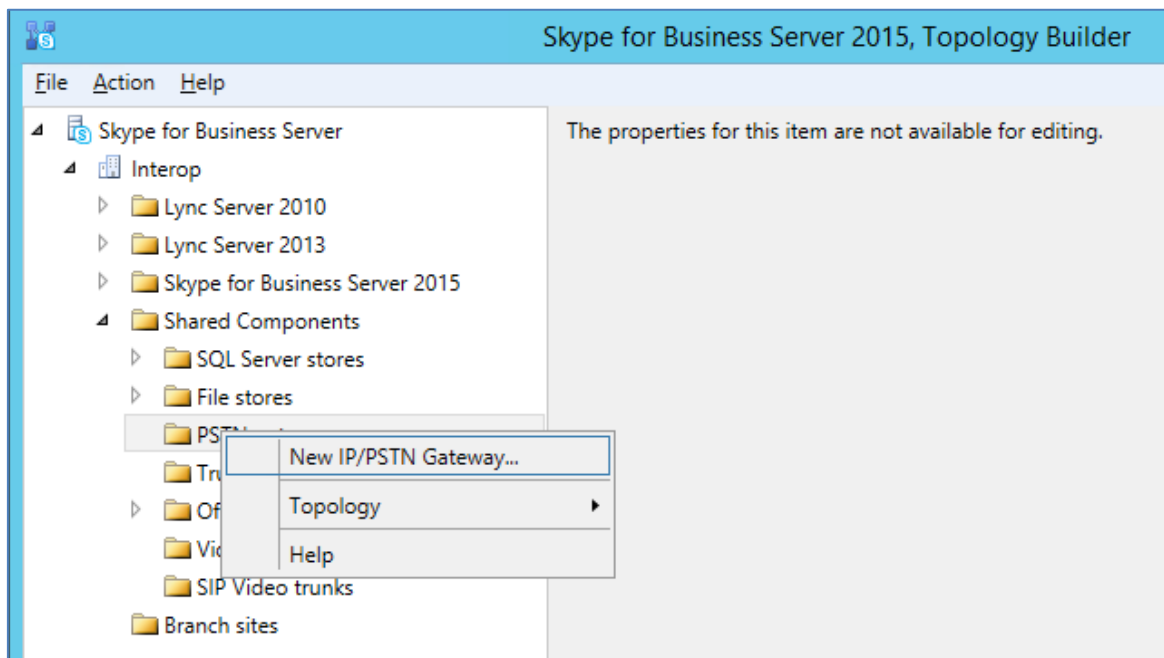
The Topology Builder screen with the downloaded Topology is displayed:

**Figure 3-4: Downloaded Topology**



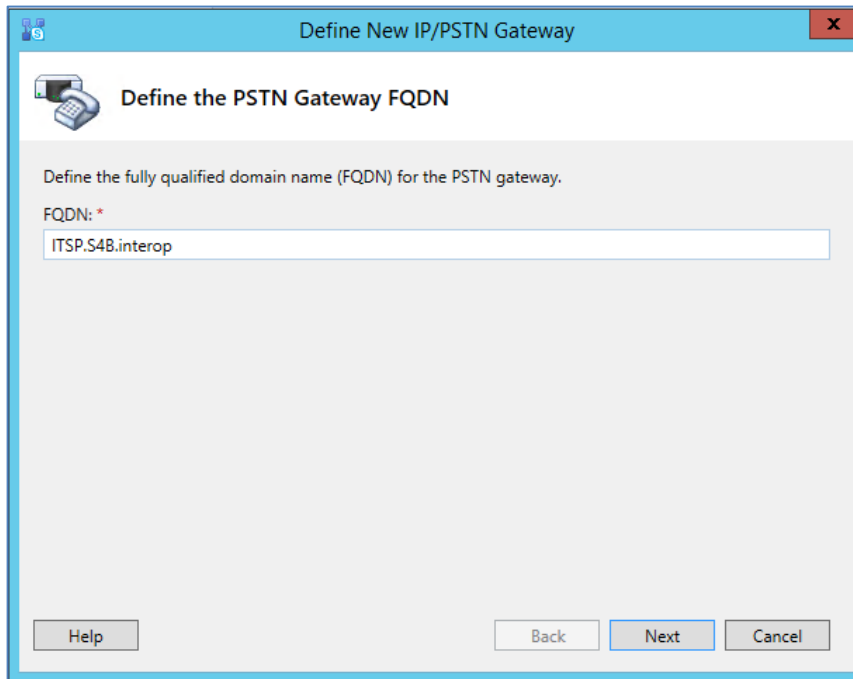
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

**Figure 3-5: Choosing New IP/PSTN Gateway**



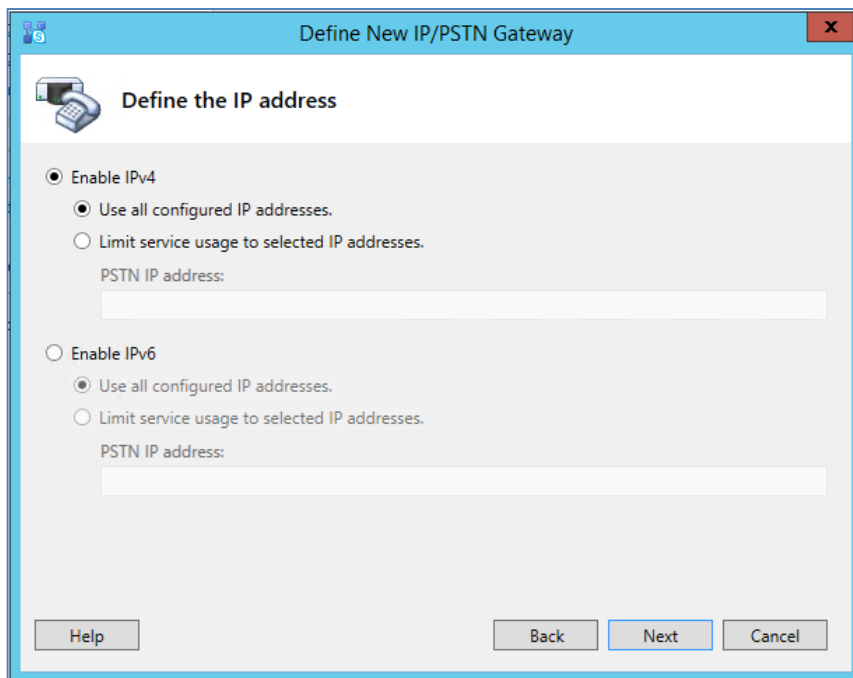
The following is displayed:

**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 57).
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

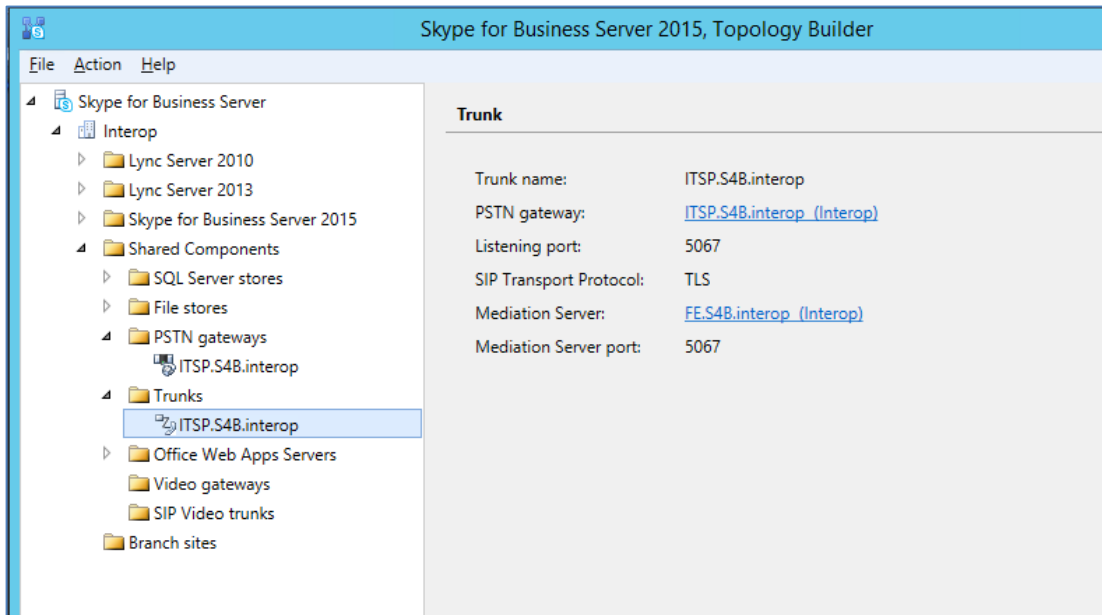
Associated Mediation Server port: \*  
5067

Help Back Finish Cancel

- 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).
- 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).
- In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
- 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**).
- Click **Finish**.

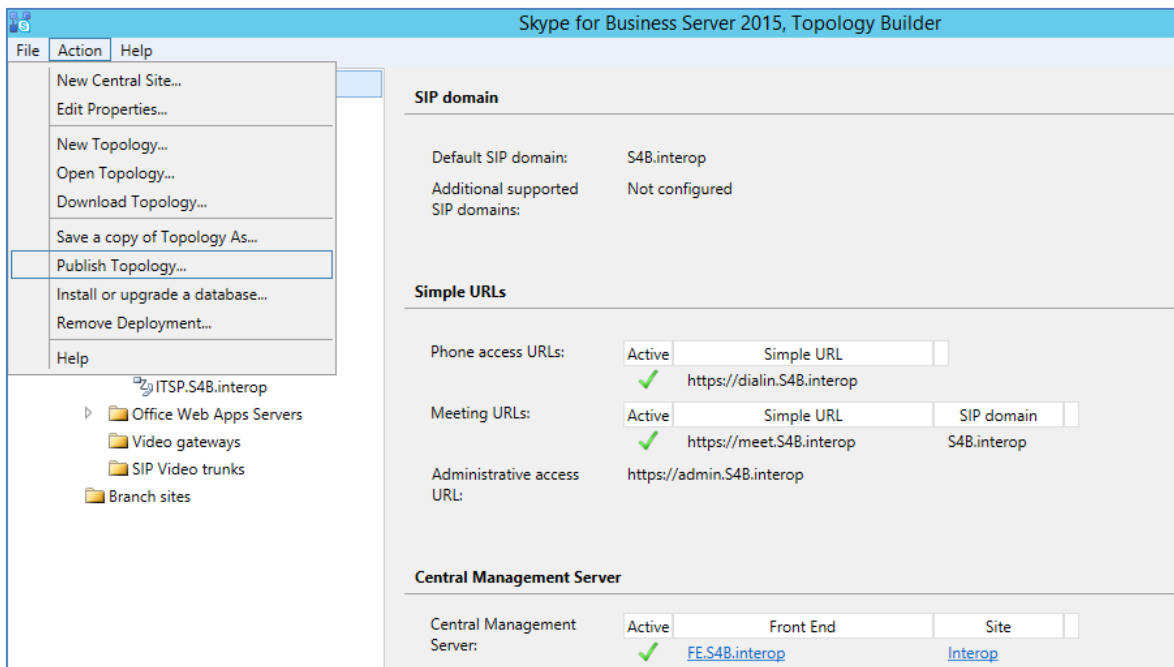
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



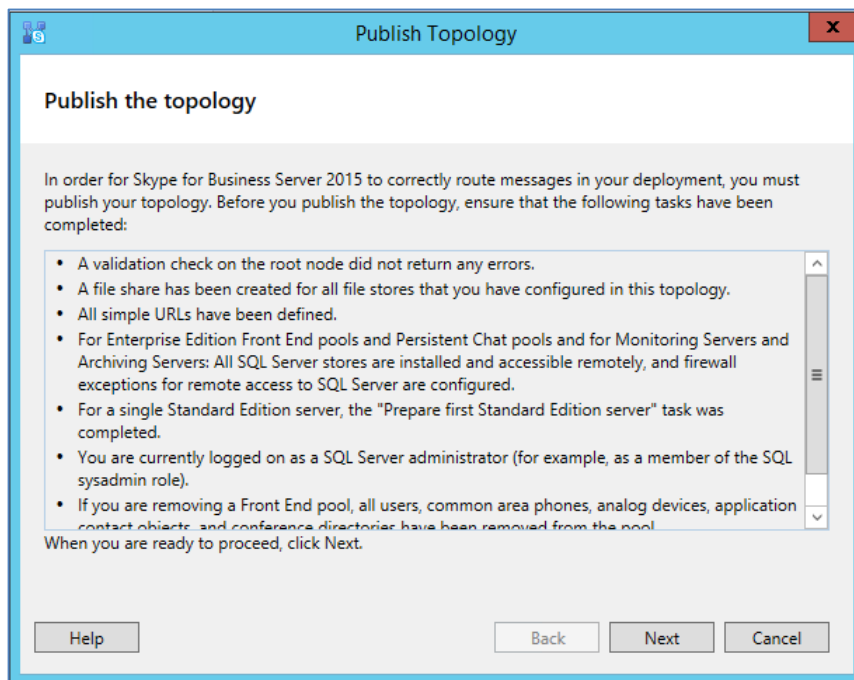
9. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

**Figure 3-10: Choosing Publish Topology**



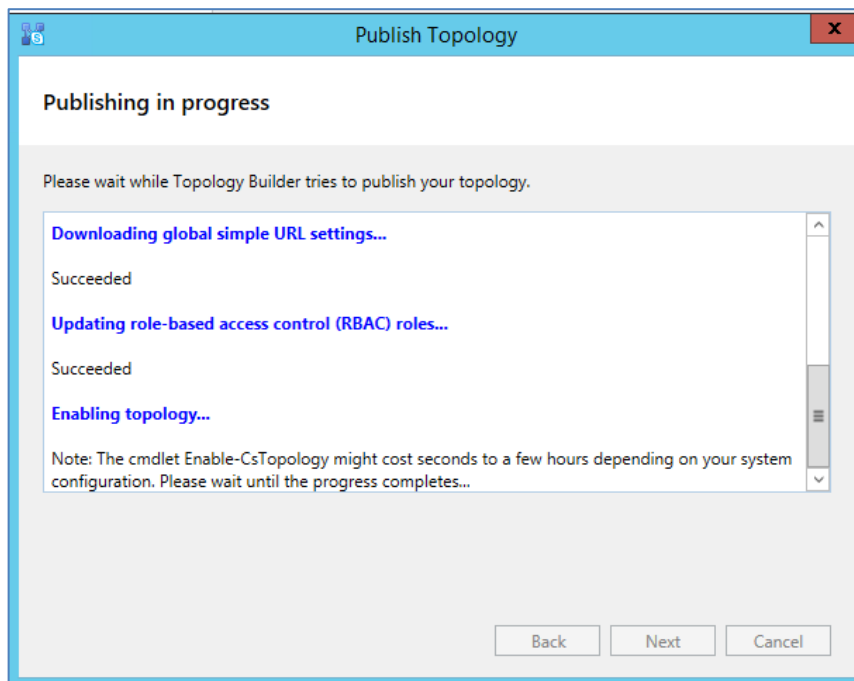
The following is displayed:

**Figure 3-11: Publish the Topology**



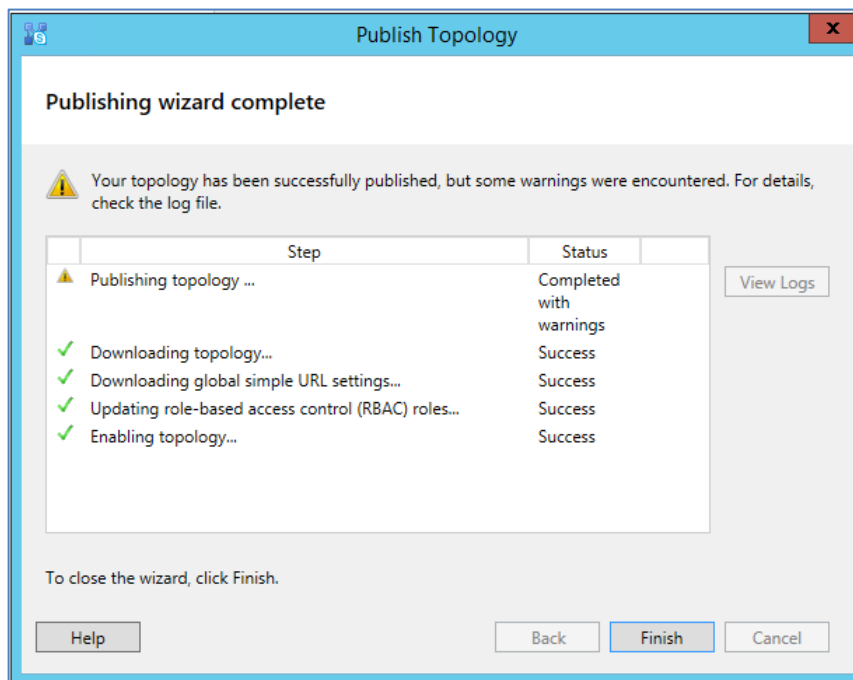
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

**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**.

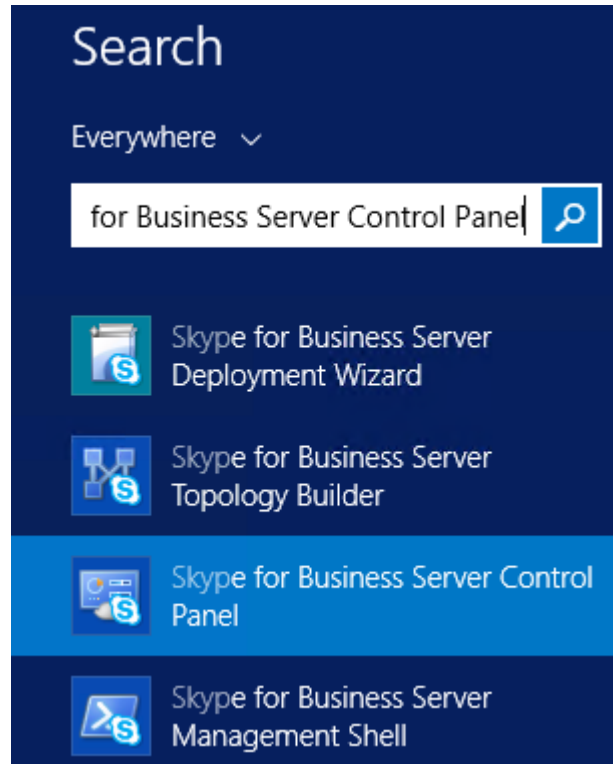
## 3.2 Configuring the "Route" on Skype for Business Server 2015

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:**

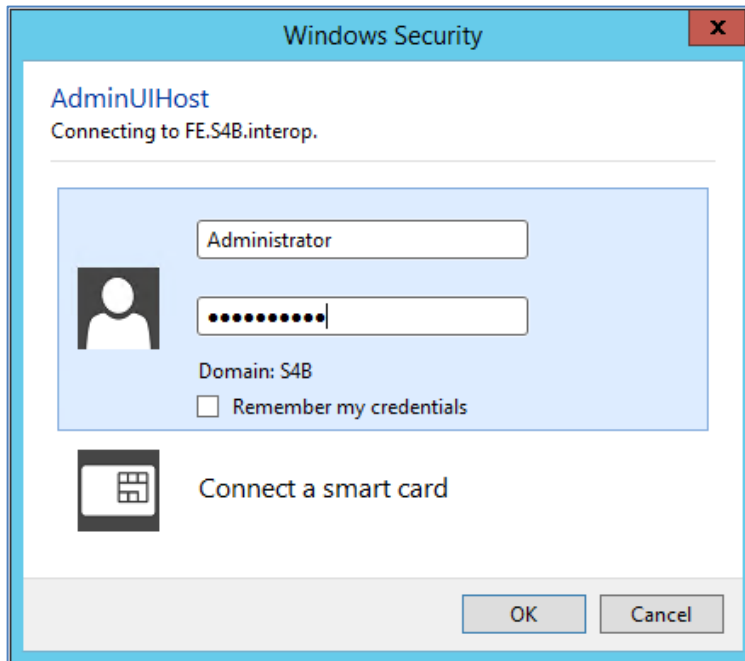
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

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



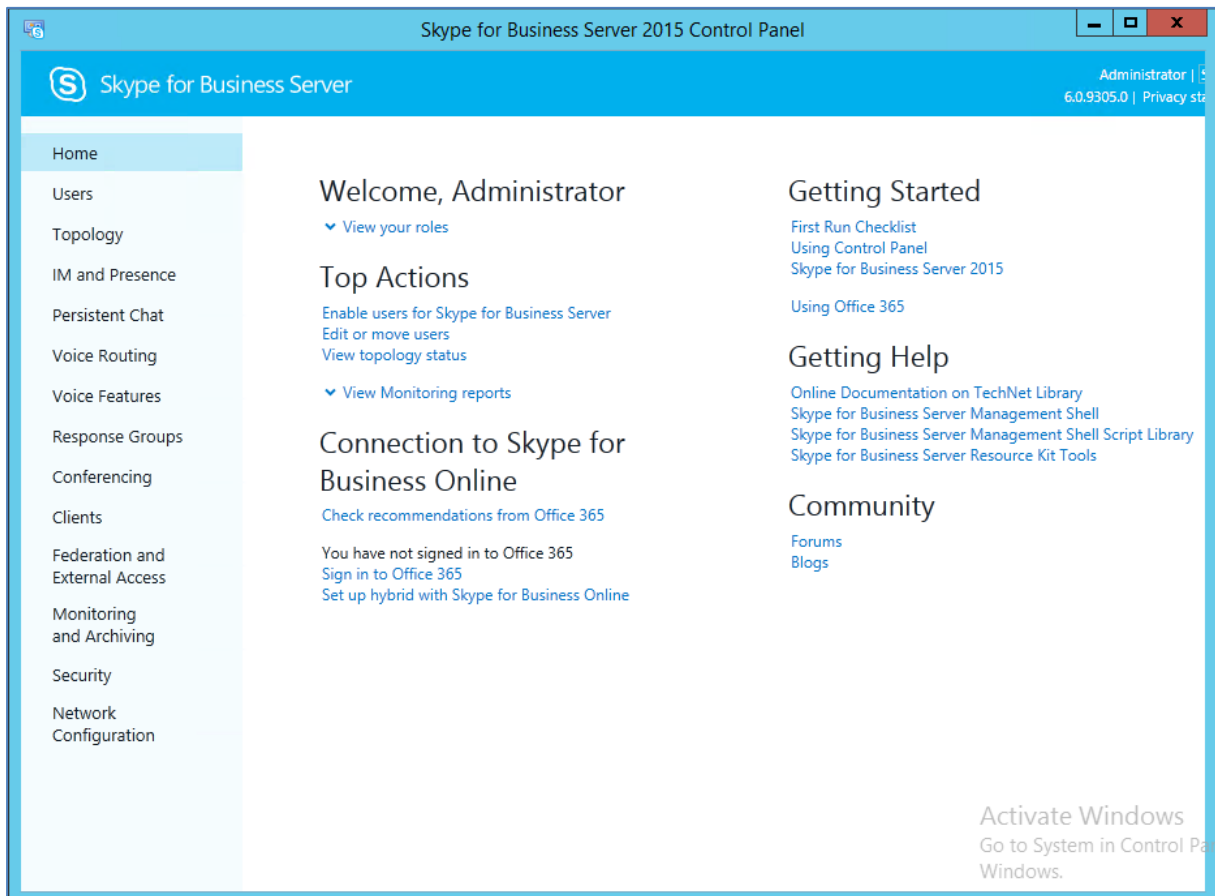
- You are prompted to enter your login credentials:

**Figure 3-15: Skype for Business Server Credentials**



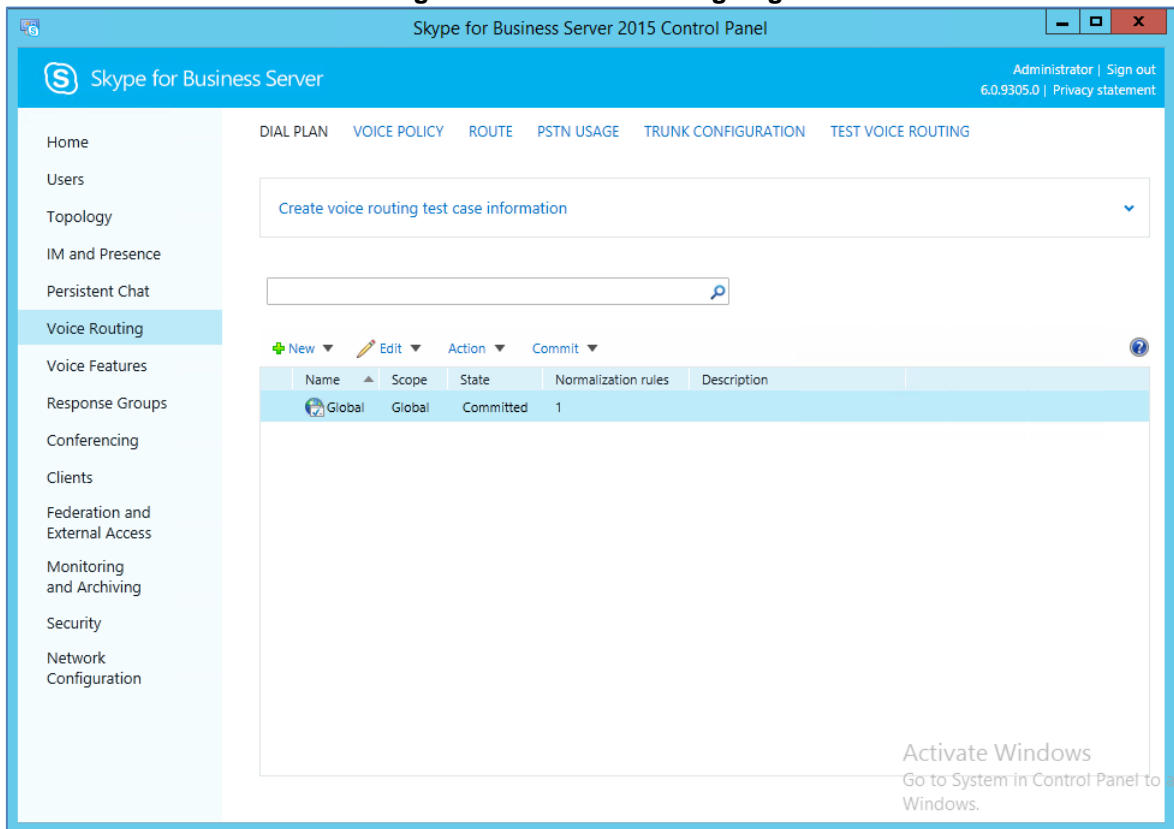
- Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

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



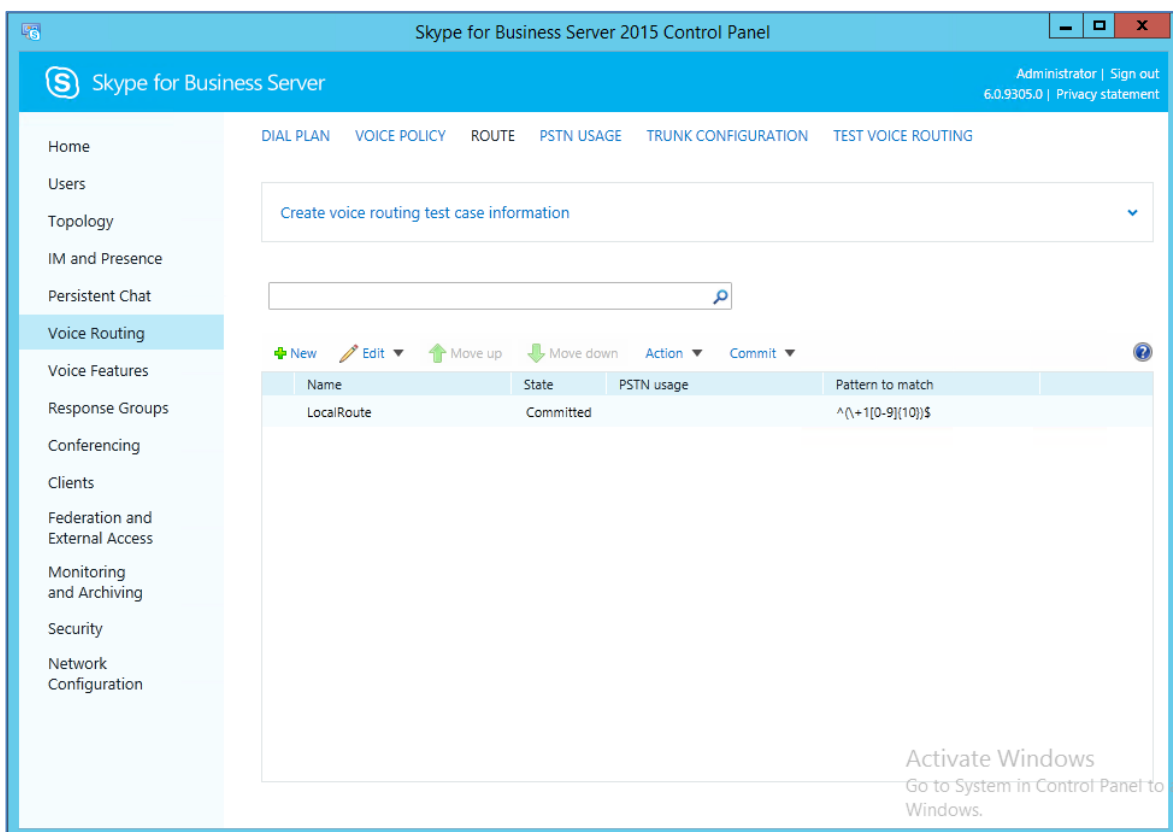
- In the left navigation pane, select **Voice Routing**.

**Figure 3-17: Voice Routing Page**



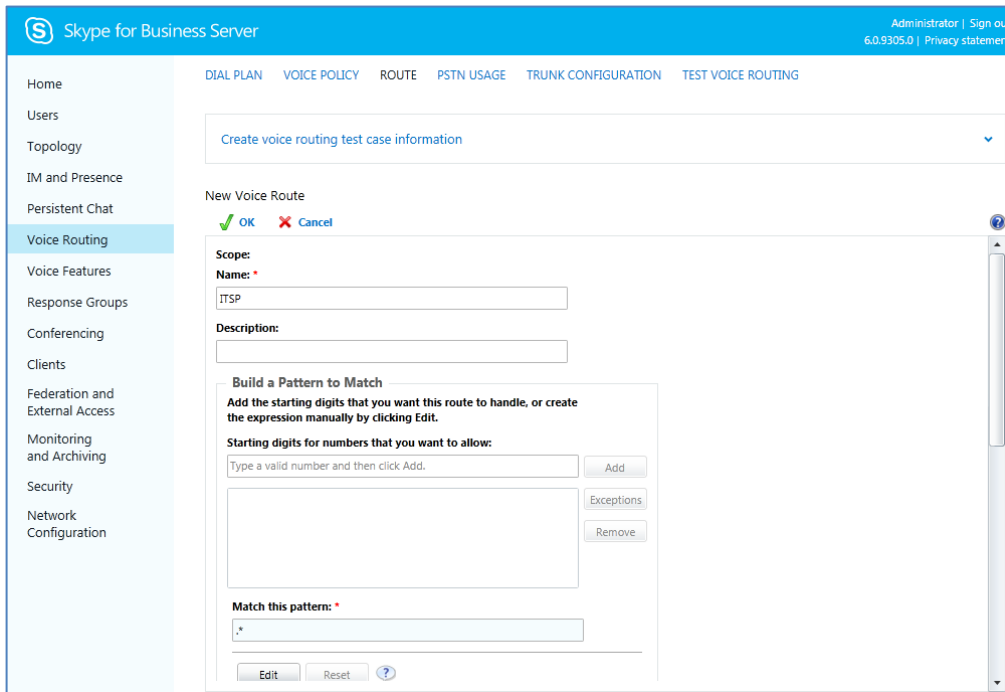
- In the Voice Routing page, select the **Route** tab.

**Figure 3-18: Route Tab**



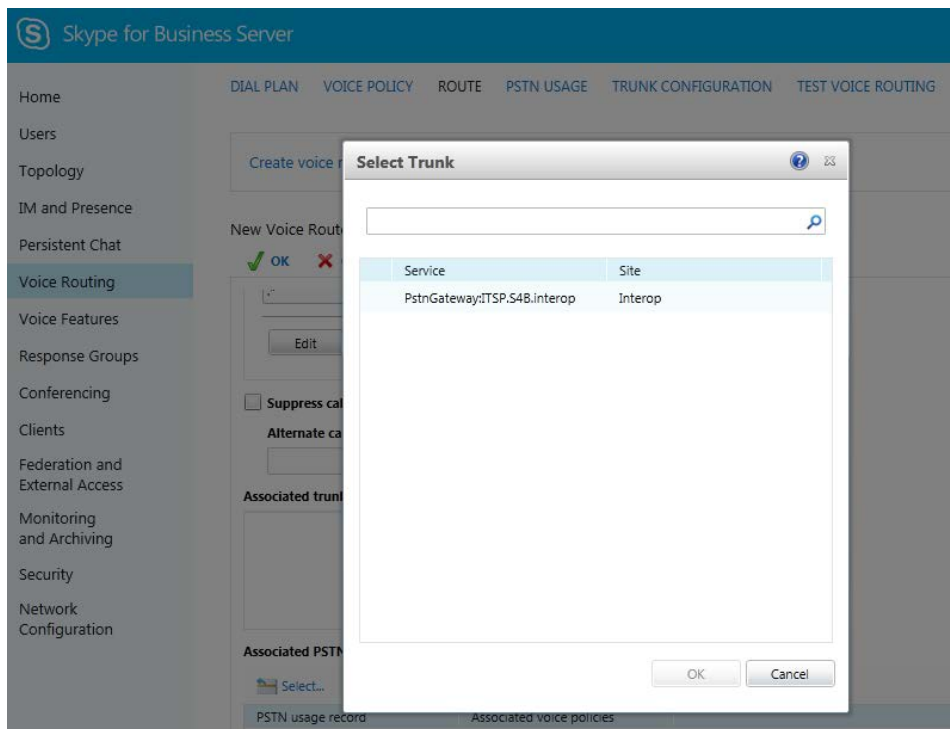
6. Click **New**; the New Voice Route page appears:

**Figure 3-19: Adding New Voice Route**



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:

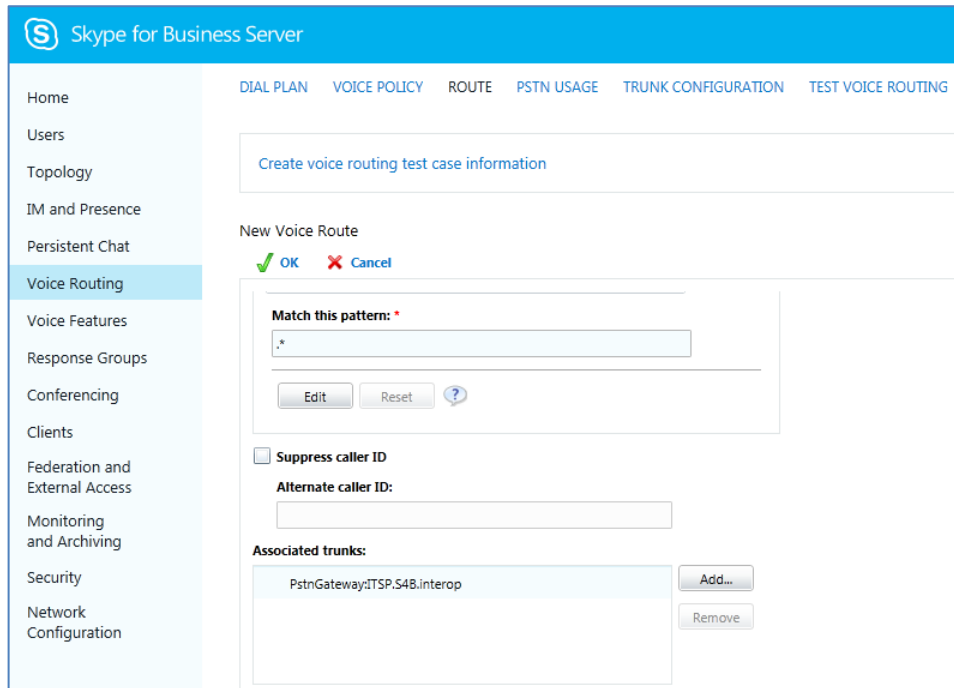
**Figure 3-20: List of Deployed Trunks**





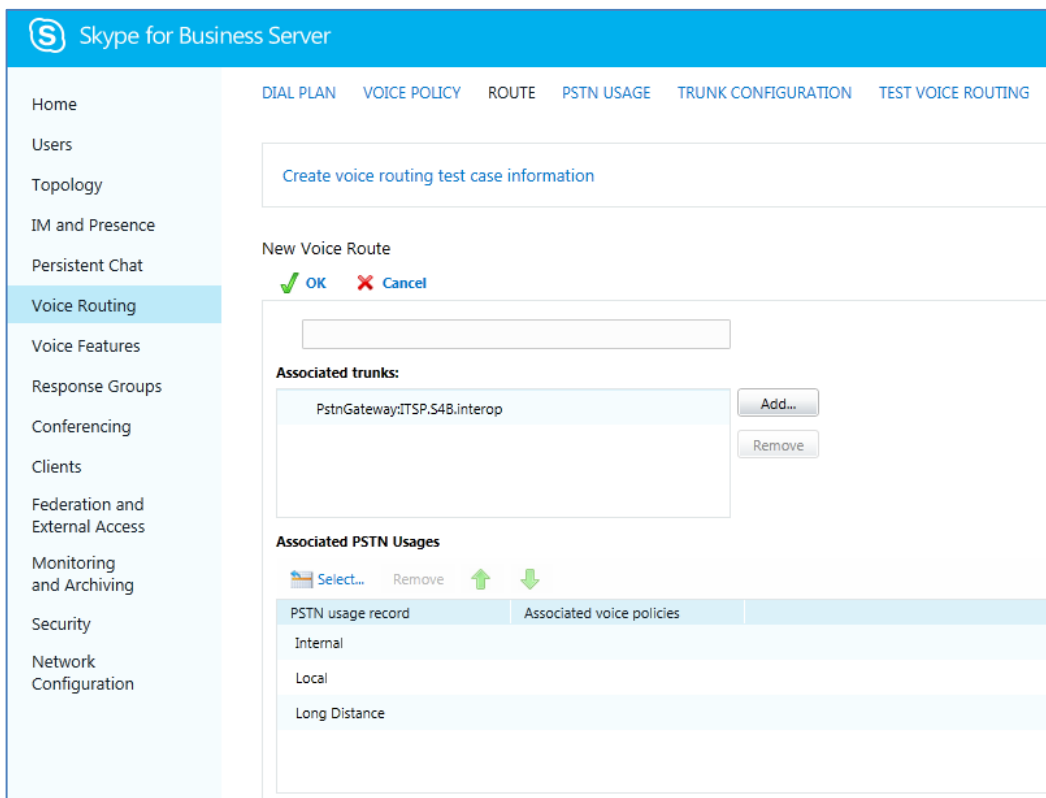
- b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

**Figure 3-21: Selected E-SBC Trunk**



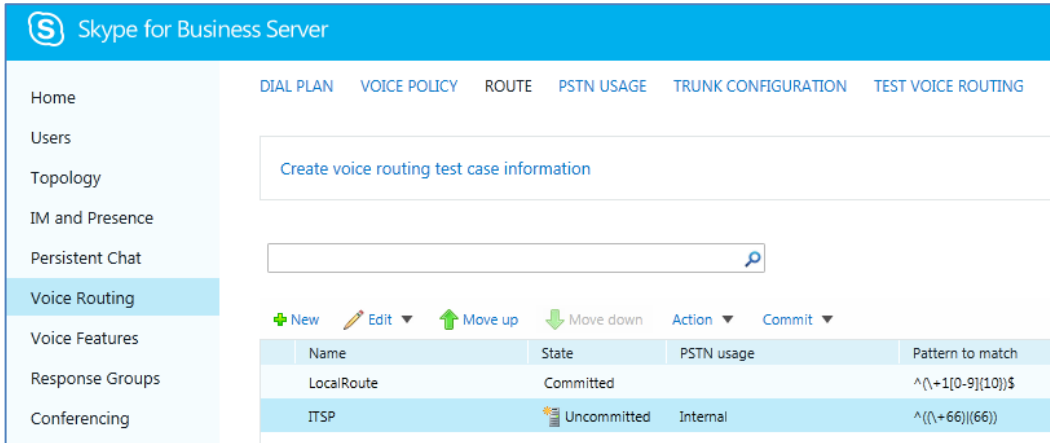
- 10. Associate a PSTN Usage to this route:
  - Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

**Figure 3-22: Associating PSTN Usage to Route**



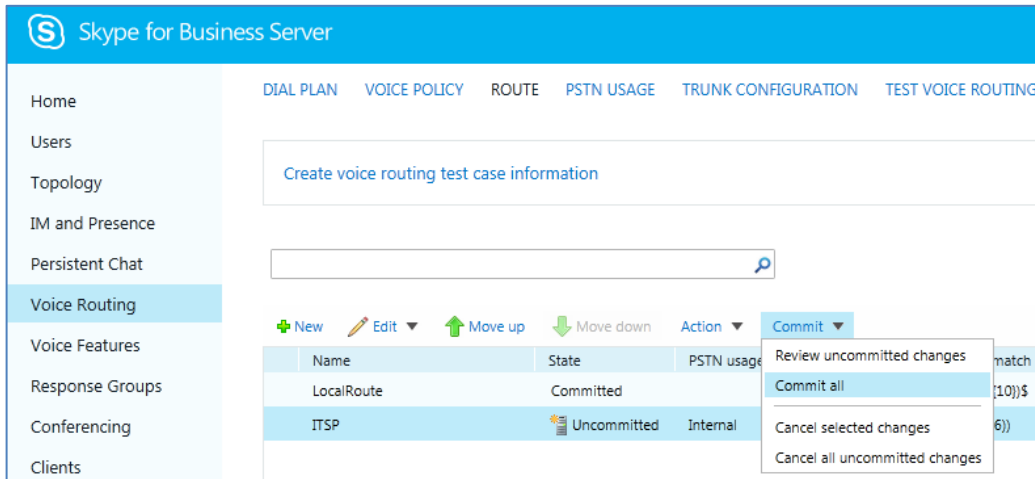
- Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

**Figure 3-23: Confirmation of New Voice Route**



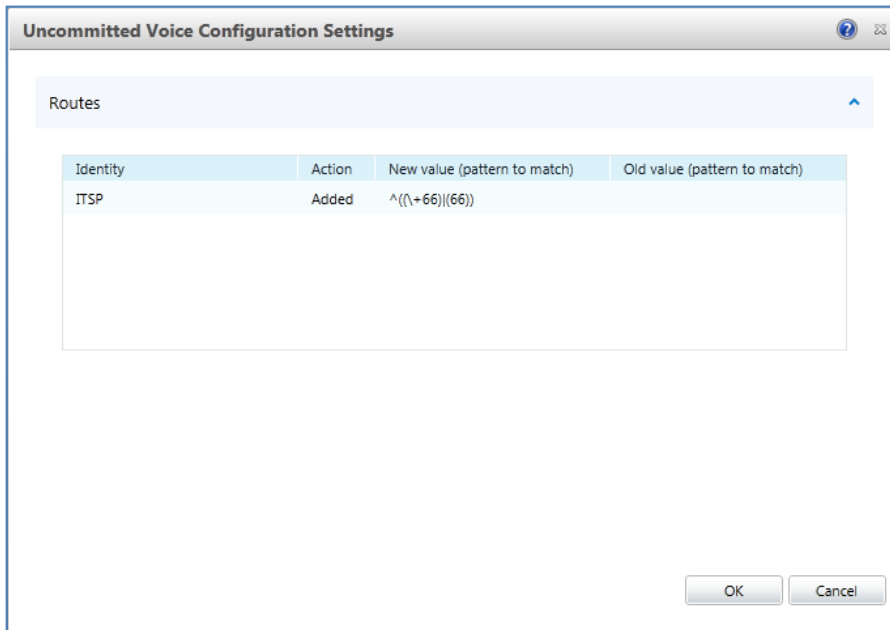
- From the **Commit** drop-down list, choose **Commit all**, as shown below:

**Figure 3-24: Committing Voice Routes**



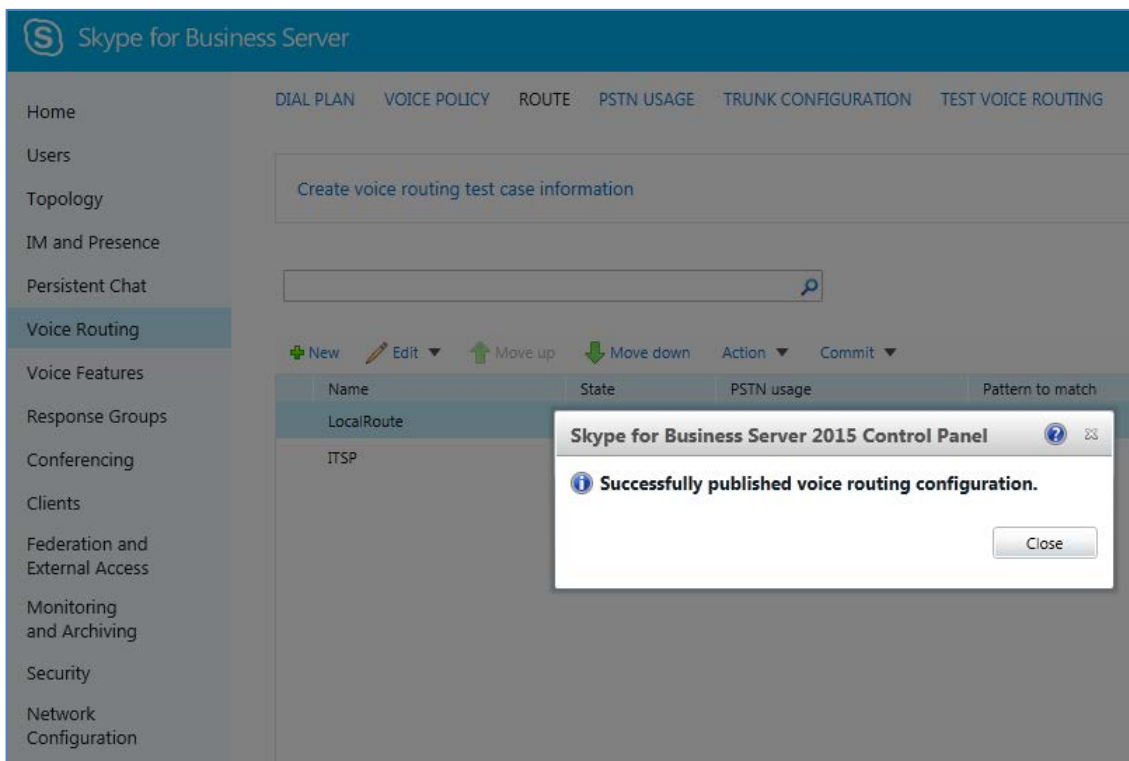
The Uncommitted Voice Configuration Settings page appears:

**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 search bar and a dropdown menu labeled 'Create voice routing test case information'. Below this is a toolbar with buttons for '+ New', 'Edit', 'Move up', 'Move down', 'Action', and 'Commit'. A table displays the committed 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 Bell Canada 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 46).

- 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 several 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 search bar and a dropdown menu labeled 'Create voice routing test case information'. Below this is a toolbar with buttons for '+ New', 'Edit', 'Action', and 'Commit'. A table displays the 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:

**Figure 3-29: Edit Trunk Configuration**

The screenshot shows the 'Edit Trunk Configuration' page in the Skype for Business Server Management Shell. The page title is 'New Trunk Configuration - PstnGateway:ITSP.S4B.interop'. The configuration options are as follows:

- Scope:** Pool
- Name:** PstnGateway:ITSP.S4B.interop
- Description:** (empty field)
- Maximum early dialogs supported:** 20
- Encryption support level:** Required
- Refer support:** Enable sending refer to the gateway
- Enable media bypass:**
- Centralized media processing:**
- Enable RTP latching:**
- Enable forward call history:**
- Enable forward P-Asserted-Identity data:**
- Enable outbound routing failover timer:**

- c. Select the **Enable forward call history** check box, and then click **OK**.
- d. 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 Bell Canada SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- E-SBC WAN interface - Bell Canada 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 Bell Canada 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**

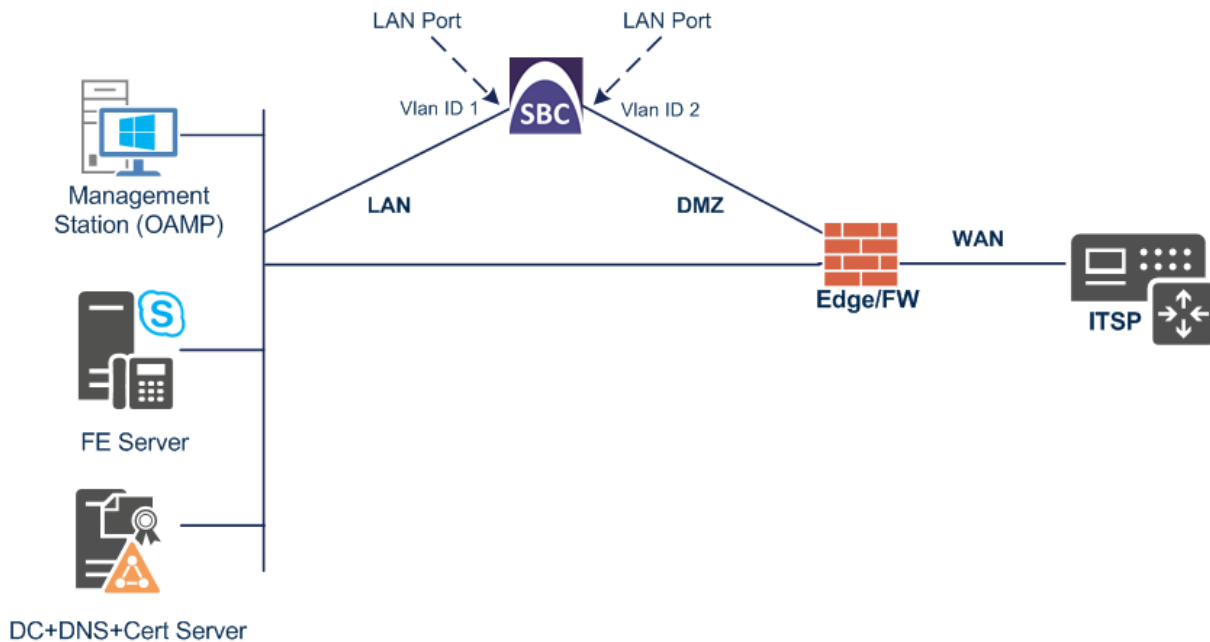
For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should 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, this interoperability test topology employs the following deployment method:

- E-SBC interfaces with the following IP entities:
  - Skype for Business servers, located on the LAN
  - Bell Canada 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 the interoperability test topology, 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	<b>1</b>
VLAN ID	<b>2</b>
Underlying Interface	<b>GROUP_2</b> (Ethernet port group)
Name	<b>vlan 2</b>
Tagging	<b>Untagged</b>

**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 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	<b>LAN_IF</b> (arbitrary descriptive name)
Ethernet Device	<b>vlan 1</b>
IP Address	<b>10.15.17.10</b> (LAN IP address of E-SBC)
Prefix Length	<b>16</b> (subnet mask in bits for 255.255.0.0)
Default Gateway	<b>10.15.0.1</b>
Primary DNS	<b>10.15.27.1</b>

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


Parameter	Value
Name	<b>WAN_IF</b>
Application Type	<b>Media + Control</b>
Ethernet Device	<b>vlan 2</b>
IP Address	<b>195.189.192.160</b> (DMZ IP address of E-SBC)
Prefix Length	<b>25</b> (subnet mask in bits for 255.255.255.128)
Default Gateway	<b>195.189.192.129</b> (router's IP address)
Primary DNS	<b>80.179.52.100</b>
Secondary DNS	<b>80.179.55.100</b>

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

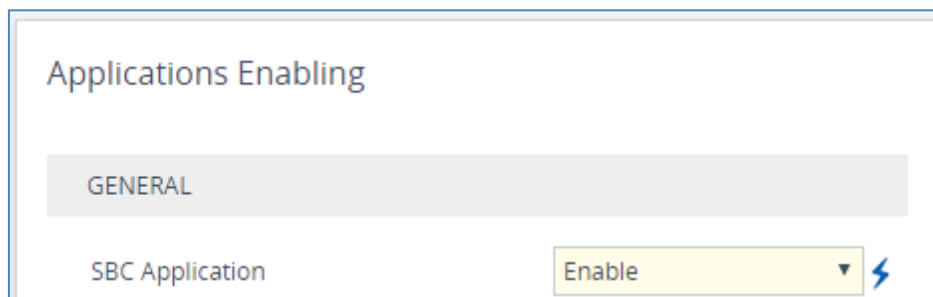
## 4.2 Step 2: Enable the SBC Application

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 88).

### 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), but modify it as shown below:

Parameter	Value
Index	<b>0</b>
Name	<b>MRLan</b> (descriptive name)
IPv4 Interface Name	<b>LAN_IF</b>
Port Range Start	<b>6000</b> (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	<b>100</b> (media sessions assigned with port range)

**Figure 4-5: Configuring Media Realm for LAN**

The screenshot shows the configuration interface for a Media Realm named 'MRLan'. The 'GENERAL' tab is active, showing the following settings:

- Index:** 0
- Name:** MRLan
- Topology Location:** Down
- IPv4 Interface Name:** #0 [LAN\_IF]
- Port Range Start:** 6000
- Number Of Media Session Legs:** 100
- Port Range End:** 6999
- Default Media Realm:** No

The 'QUALITY OF EXPERIENCE' section shows:

- QoE Profile:** -- (View)
- Bandwidth Profile:** -- (View)

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

3. Configure a Media Realm for WAN traffic:

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

**Figure 4-6: Configuring Media Realm for WAN**

Media Realms [MRWan] - x

GENERAL

QUALITY OF EXPERIENCE


Index	<input type="text" value="1"/>	QoS Profile	<input type="text" value="--"/> <a href="#">View</a>
Name	<input type="text" value="MRWan"/>	Bandwidth Profile	<input type="text" value="--"/> <a href="#">View</a>
Topology Location	<input type="text" value="Up"/>		
IPv4 Interface Name	<input type="text" value="#1 [WAN_IF]"/> <a href="#">View</a>		
Port Range Start	<input type="text" value="7000"/>		
Number Of Media Session Legs	<input type="text" value="100"/>		
Port Range End	<input type="text" value="7999"/>		
Default Media Realm	<input type="text" value="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. For the interoperability test topology, 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	<b>0</b>
Name	<b>S4B</b> (see note at the end of this section)
Network Interface	<b>LAN_IF</b>
Application Type	<b>SBC</b>
TCP and UDP	<b>0</b>
TLS Port	<b>5067</b> (see note below)
Media Realm	<b>MRLan</b>



**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	<b>1</b>
Name	<b>BellCanada</b>
Network Interface	<b>WAN_IF</b>
Application Type	<b>SBC</b>
UDP Port	<b>5060</b>
TCP and TLS	<b>0</b>
Media Realm	<b>MRWan</b>





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	ENCAPSULATION PROTOCOL	MEDIA REALM
0	S4B	 DefaultSF	LAN_IF	SBC	0	0	5067	No encapsula	MRLan
1	BellCanada	 DefaultSF	WAN_IF	SBC	5060	0	0	No encapsula	MRWan



**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.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Microsoft Skype for Business Server 2015
- Bell Canada SIP Trunk

The Proxy Sets will be later applying 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	<b>1</b>
Name	<b>S4B</b>
SBC IPv4 SIP Interface	<b>S4B</b>
Proxy Keep-Alive	<b>Using Options</b>
Redundancy Mode	<b>Homing</b>
Proxy Hot Swap	<b>Enable</b>
Proxy Load Balancing Method	<b>Round Robin</b>

**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.
- d. Click **Apply**.

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

3. Configure a Proxy Set for the Bell Canada SIP Trunk:

Parameter	Value
Index	<b>2</b>
Name	<b>BellCanada</b>
SBC IPv4 SIP Interface	<b>BellCanada</b>
Proxy Keep-Alive	<b>Using Options</b>
Keep-Alive Failure Responses	<b>503</b>

**Figure 4-11: Configuring Proxy Set for Bell Canada SIP Trunk**

The screenshot shows the 'Proxy Sets [BellCanada]' configuration window. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this are three main sections: 'GENERAL', 'REDUNDANCY', and 'KEEP ALIVE'. The 'GENERAL' section includes fields for Index (2), Name (BellCanada), Gateway IPv4 SIP Interface (empty), SBC IPv4 SIP Interface (#1 [BellCanada]), and TLS Context Name (empty). The 'REDUNDANCY' section includes Redundancy Mode (empty), Proxy Hot Swap (Disable), Proxy Load Balancing Method (Disable), and Min. Active Servers for Load Balancing (1). The 'KEEP ALIVE' section includes Proxy Keep-Alive (Using OPTIONS), Proxy Keep-Alive Time [sec] (60), and Keep-Alive Failure Responses (503). At the bottom, there are 'Cancel' and 'APPLY' buttons.

- 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 Bell Canada SIP Trunk**

The screenshot shows a configuration window titled "Proxy Address". It has a "GENERAL" tab selected. The configuration fields are as follows:

- Index:** 0
- Proxy Address:** 123.123.123.123:5060
- Transport Type:** UDP

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

Parameter	Value
Index	<b>0</b>
Proxy Address	<b>123.123.123.123:5060</b> ( IP address / FQDN and destination port)
Transport Type	<b>UDP</b>

- d. Click **Apply**.

The configured Proxy Sets are shown in the figure below:

**Figure 4-13: Configured Proxy Sets in Proxy Sets Table**

The screenshot shows the "Proxy Sets (3)" table with the following data:

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (;	S4B	--	60		Disable
1	S4B	DefaultSRD (;	--	S4B	60	Homing	Enable
2	BellCanada	DefaultSRD (;	--	BellCanada	60		Disable

## 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 Bell Canada 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 Bell Canada 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 Name	<b>AudioCodersGroups_1</b>
Coder Name	<ul style="list-style-type: none"> <li>▪ <b>G.711 U-law</b></li> <li>▪ <b>G.711 A-law</b></li> </ul>
Silence Suppression	<b>Enable</b> (for both coders)

**Figure 4-14: 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 Bell Canada SIP Trunk:

Parameter	Value
Coder Group Name	<b>AudioCodersGroups_2</b>
Coder Name	<b>G.729</b>

**Figure 4-15: Configuring Coder Group for Bell Canada 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 Bell Canada 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 Bell Canada SIP Trunk in the next step.

➤ **To set a preferred coder for the Bell Canada 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 Audio Coders Group for Bell Canada SIP Trunk.

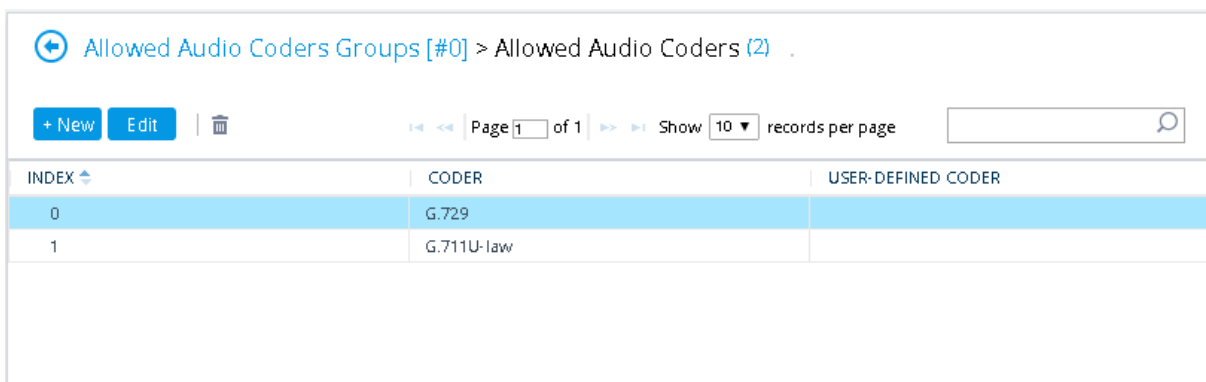
**Figure 4-16: Configuring Allowed Coders Group for Bell Canada SIP Trunk**



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

Parameter	Value
Coder	<b>G.729</b>
Coder	<b>G.711 U-law</b>

**Figure 4-17: Configuring Allowed Coders for Bell Canada SIP Trunk**



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

**Figure 4-18: SBC Preferences Mode**

Media Settings

<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">GENERAL</div> <p><b>NAT Traversal</b> <span style="float: right;">Disable NAT ▾</span></p> <p>Enable Continuity Tones <span style="float: right;">Disable ▾ ⚡</span></p> <p>Inbound Media Latch Mode <span style="float: right;">Dynamic ▾</span></p> <p>Number of Media Channels <span style="float: right;">0 ⚡</span></p> <p>Enforce Media Order <span style="float: right;">Disable ▾</span></p> <p>SDP Session Owner <span style="float: right;">AudiocodesGW</span></p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">SBC SETTINGS</div> <p>Preferences Mode <span style="float: right;">• Include Extensions ▾ ←</span></p> <p>Enforce Media Order <span style="float: right;">Disable ▾</span></p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">GATEWAY SETTINGS</div> <p><b>Enable Early Media</b> <span style="float: right;">Disable ▾</span></p> <p>Multiple Packetization Time Format <span style="float: right;">None ▾</span></p>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">ROBUSTNESS</div> <p>New RTP Stream Packets <span style="float: right;">3</span></p> <p>New RTCP Stream Packets <span style="float: right;">3</span></p> <p>New SRTP Stream Packets <span style="float: right;">3</span></p> <p>New SRTCP Stream Packets <span style="float: right;">3</span></p> <p>Timeout To Relatch RTP (msec) <span style="float: right;">200</span></p> <p>Timeout To Relatch SRTP (msec) <span style="float: right;">200</span></p> <p>Timeout To Relatch Silence (msec) <span style="float: right;">10000</span></p> <p>Timeout To Relatch RTCP (msec) <span style="float: right;">10000</span></p>
--	---

Cancel
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 this interoperability test topology, 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
- Bell Canada 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
<b>General</b>	
Index	<b>1</b>
Name	<b>S4B</b>
<b>Media Security</b>	
SBC Media Security Mode	<b>SRTP</b>
Symmetric MKI	<b>Enable</b>
MKI Size	<b>1</b>
Enforce MKI Size	<b>Enforce</b>
Reset SRTP State Upon Re-key	<b>Enable</b>
Generate SRTP Keys Mode:	<b>Always</b>
<b>SBC Early Media</b>	
Remote Early Media RTP Detection Mode	<b>By Media</b> (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)
<b>SBC Media</b>	
Extension Coders Group	<b>AudioCodersGroups_1</b>
RFC 2833 Mode	<b>Extended</b> (required, as Skype for Business does not support calls without RFC 2833)
<b>SBC Signaling</b>	
Remote Update Support	<b>Supported Only After Connect</b>
Remote re-INVITE Support	<b>Supported Only With SDP</b>
Remote Delayed Offer Support	<b>Not Supported</b>
<b>SBC Forward and Transfer</b>	
Remote REFER Mode	<b>Handle Locally</b> (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)

Remote 3xx Mode	<b>Handle Locally</b> (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)
SBC Hold	
Remote Hold Format	<b>Inactive</b> (required because Bell Canada's SIP Trunk sends 0.0.0.0 for Hold but Skype for Business Server 2015 does not recognize that format)

Figure 4-19: Configuring IP Profile for Skype for Business Server 2015

3. Click **Apply**.

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

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

Parameter	Value
<b>General</b>	
Index	<b>2</b>
Name	<b>BellCanada</b>
<b>Media Security</b>	
SBC Media Security Mode	<b>RTP</b>
<b>SBC Early Media</b>	
<b>SBC Media</b>	
Extension Coders Group	<b>AudioCodersGroups_2</b>
Allowed Audio Coders	<b>BellCanada Allowed Coders</b>
Allowed Coders Mode	<b>Restriction and Preference</b> (lists Allowed Coders first and then original coders in received SDP offer)
<b>SBC Signaling</b>	
P-Asserted-Identity Header Mode	<b>Add</b> (required for anonymous calls)
Diversion Header Mode	<b>Add</b> (required for transferred calls)
History-Info Header Mode	<b>Remove</b>
Session Expires Mode	<b>Not Supported</b>
<b>SBC Forward and Transfer</b>	
Remote REFER Mode	<b>Handle Locally</b> (required, as format of Skype for Business Server's SIP REFER message is not supported by the Bell Canada SIP Trunk )
Play RBT To Transferee	<b>Yes</b>

**Figure 4-20: Configuring IP Profile for Bell Canada SIP Trunk**

The screenshot shows the 'IP Profiles [BellCanada]' configuration window. It is divided into three main sections: GENERAL, MEDIA SECURITY, and SBC SIGNALING. At the bottom, there are 'Cancel' and 'APPLY' buttons.

Section	Property	Value
GENERAL	Index	2
	Name	BellCanada
	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	Add
	History-Info Header Mode	Remove
	Session Expires Mode	Transparent
	Remote Update Support	Supported
	Remote re-INVITE	Supported
	Remote Delayed Offer Support	Supported
	Remote Representation Mode	According to Offer
	Keep Incoming Via Headers	According to Offer
Keep Incoming Routing Headers	According to Offer	
Keep User-Agent Header	According to Offer	

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 this interoperability test topology, IP Groups must be configured for the following IP entities:

- Skype for Business Server 2015 (Mediation Server) located on LAN
- Bell Canada 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	<b>1</b>
Name	<b>S4B</b>
Type	<b>Server</b>
Proxy Set	<b>S4B</b>
IP Profile	<b>S4B</b>
Media Realm	<b>MRLan</b>
SIP Group Name	<b>customer.bell.ca</b> (according to ITSP requirement)

3. Configure an IP Group for the Bell Canada SIP Trunk:

Parameter	Value
Index	<b>2</b>
Name	<b>BellCanada</b>
Topology Location	<b>Up</b>
Type	<b>Server</b>
Proxy Set	<b>BellCanada</b>
IP Profile	<b>BellCanada</b>
Media Realm	<b>MRWan</b>
SIP Group Name	<b>siptrunking.bell.ca</b> (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

**Figure 4-21: Configured IP Groups in IP Group Table**

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 Configured	ProxySet_0	--	--		Disable	-1	-1
1	S4B	DefaultS	Server	Not Configured	S4B	S4B	MRLan	customer.bel	Enable	-1	-1
2	BellCanada	DefaultS	Server	Not Configured	BellCanada	BellCanada	MRWan	siptrunking.t	Enable	-1	4

## 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 4-22: 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**.

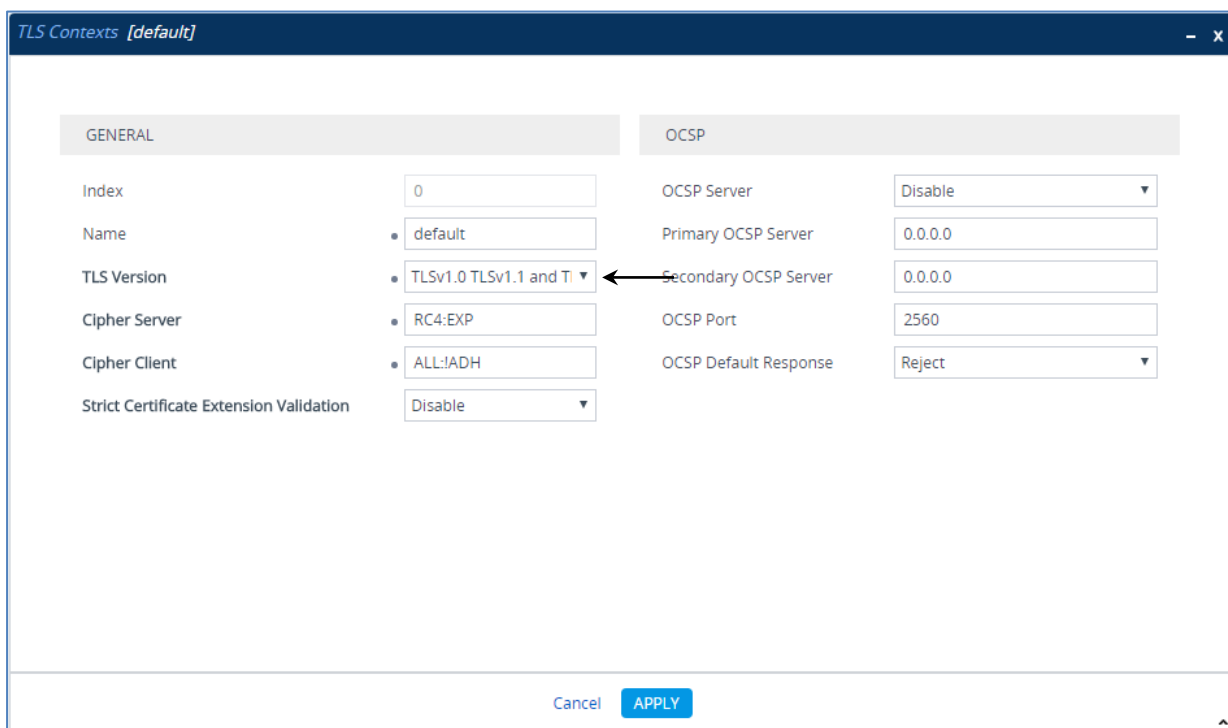
## 4.9.2 Step 9b: Configure the TLS version

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 4-23: 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 open, showing the selected option 'TLSv1.0 TLSv1.1 and TLSv1.2'. An arrow points to this dropdown menu.

GENERAL		OCSP	
Index	0	OCSP Server	Disable
Name	default	Primary OCSP Server	0.0.0.0
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2	Secondary OCSP Server	0.0.0.0
Cipher Server	RC4:EXP	OCSP Port	2560
Cipher Client	ALL:!ADH	OCSP Default Response	Reject
Strict Certificate Extension Validation	Disable		

Buttons: Cancel, APPLY

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 4-24: 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

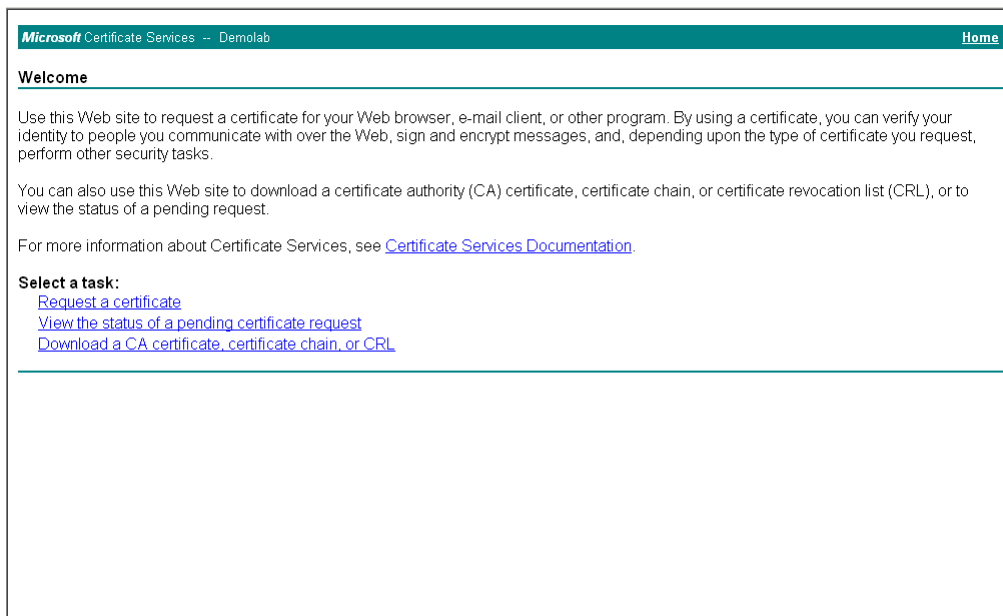
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAIBADAbMRkwFwYDVQQDBB1VFNQQL1M0Q15pbmR1cm9wMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCzEs8XTnY8be/t77eEDG7rTg747GQ30DFOC4Rs
x+e9KfbErZgxMYqGT8u04AU0wU9LUPkkq+8gI6w2bg3boW0kg/9hrnNL2rf1tGcn
30oSHP05PiKmRNZnCC090b03tbr9kuHmlwPRQ7yT6k7xS3X8bSigqT4LQbJBT1tt
hDH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAim/GA2E1ZQbZaR6CZyIawilT
u65w450NFHmaCluHSyZ8keM8d1Ux14hkw7t5ygAD8KbxVkhRVaCgcQrAK2v8u1Pf
TvN+bwJ+kQ0d59CiXa82e0o1WB3buPq5+qWdGTF+MyJWGVf8SIC1c6+zFoc+BEZY
7tQ8y0J8od0aDhStDfQ=
-----END CERTIFICATE REQUEST-----
    
```

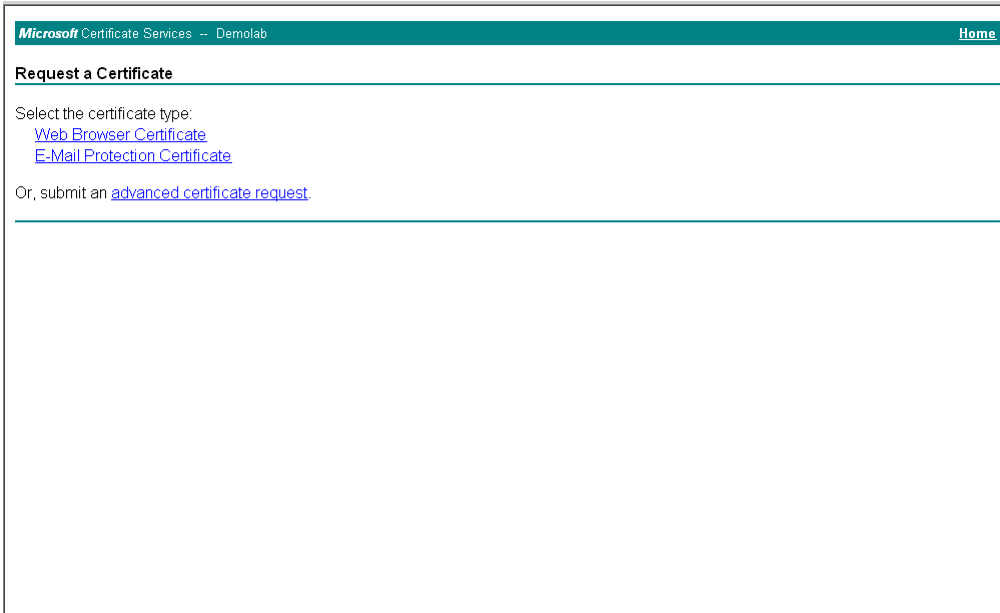
- Copy the CSR from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
- Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate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

Figure 4-25: Microsoft Certificate Services Web Page



- Click **Request a certificate**.

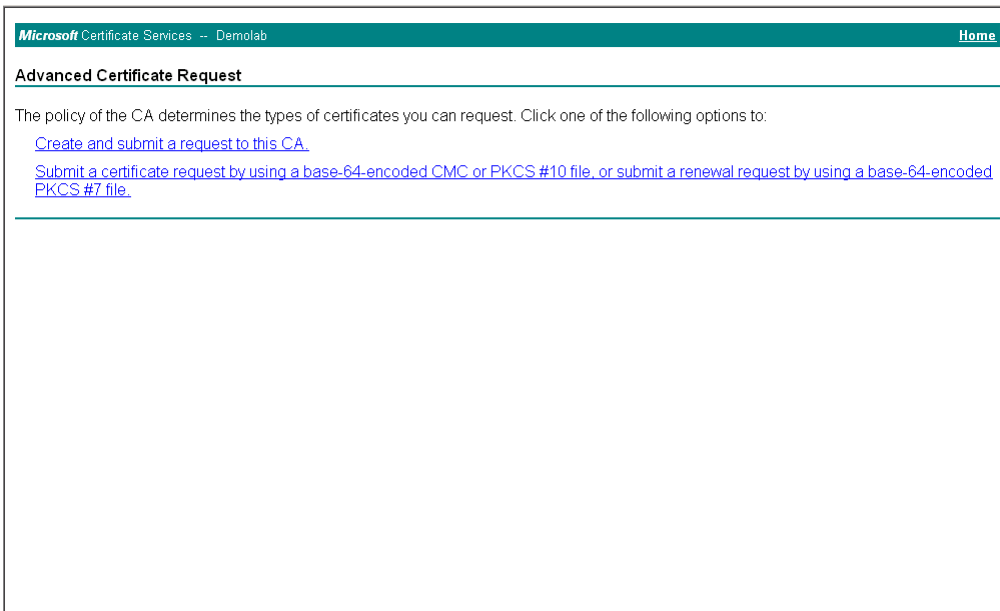
Figure 4-26: Request a Certificate Page



The screenshot shows a web page titled "Request a Certificate" from Microsoft Certificate Services. The page has a green header bar with "Microsoft Certificate Services -- Demolab" on the left and "Home" on the right. Below the header, the title "Request a Certificate" is followed by a horizontal line. The main content area contains the text "Select the certificate type:" followed by two blue links: "Web Browser Certificate" and "E-Mail Protection Certificate". Below this, it says "Or, submit an [advanced certificate request](#)". A horizontal line is positioned below the "advanced certificate request" link.

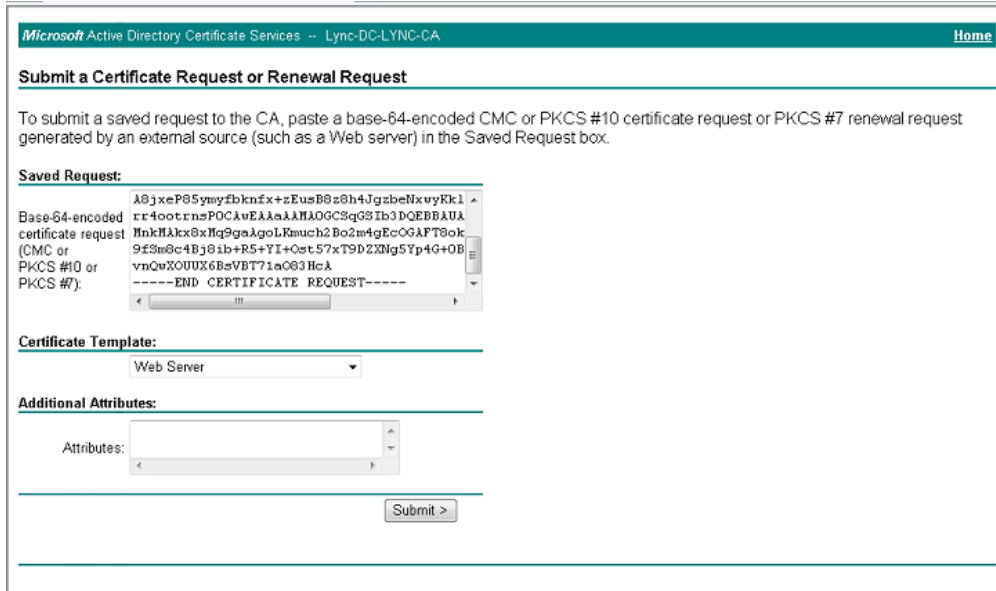
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-27: Advanced Certificate Request Page

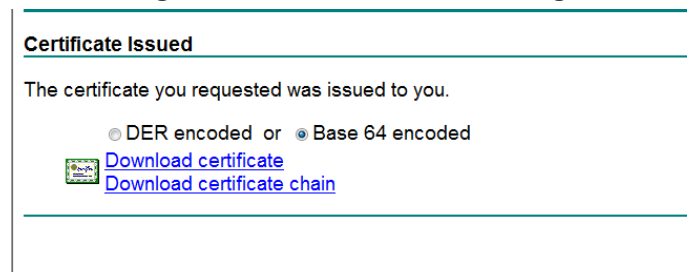


The screenshot shows a web page titled "Advanced Certificate Request" from Microsoft Certificate Services. The page has a green header bar with "Microsoft Certificate Services -- Demolab" on the left and "Home" on the right. Below the header, the title "Advanced Certificate Request" is followed by a horizontal line. The main content area contains the text "The policy of the CA determines the types of certificates you can request. Click one of the following options to:" followed by two blue links: "Create and submit a request to this CA." and "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.". A horizontal line is positioned below the second link.

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

**Figure 4-28: 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 4-29: 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 4-30: 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 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 4-31: 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 4-32: 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 88).

## 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 46).

➤ **To configure media security:**

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

Figure 4-33: Configuring SRTP

GENERAL		AUTHENTICATION & ENCRYPTION	
<b>Media Security</b>	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	
<b>Master Key Identifier (MKI) Size</b>	0	Enable Rekey After 181	Disable
<b>Symmetric MKI</b>	Disable		

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 88).

## 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.

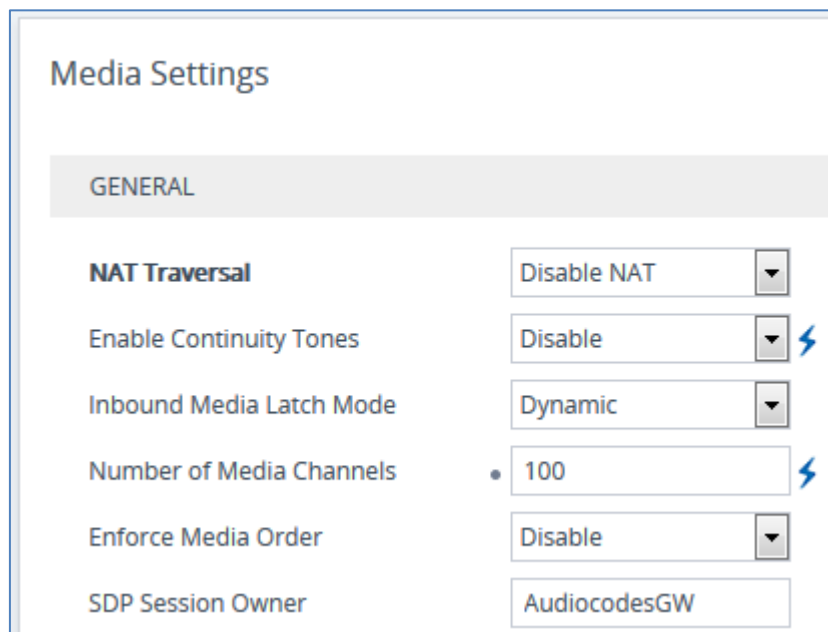


**Note:** This step is required **only** if transcoding is required.

➤ **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 4-34: Configuring Number of Media Channels**



The screenshot shows the 'Media Settings' page with the 'GENERAL' tab selected. The 'Number of Media Channels' field is highlighted with a blue lightning bolt icon and an arrow pointing to it from the right. The field contains the value '100'. Other settings include 'NAT Traversal' (Disable NAT), 'Enable Continuity Tones' (Disable), 'Inbound Media Latch Mode' (Dynamic), 'Enforce Media Order' (Disable), and 'SDP Session Owner' (AudiocodesGW).

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 88).



## 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 45,) to denote the source and destination of the call.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business Server 2015 (LAN) and Bell Canada 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 Bell Canada SIP Trunk
- Calls from Bell Canada 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	<b>0</b>
Name	<b>Terminate OPTIONS</b> (arbitrary descriptive name)
Source IP Group	<b>Any</b>
Request Type	<b>OPTIONS</b>
Destination Type	<b>Dest Address</b>
Destination Address	<b>internal</b>

**Figure 4-35: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS**

The screenshot shows a configuration window titled "IP-to-IP Routing [Terminate OPTIONS]". At the top, there is a "Routing Policy" dropdown menu set to "#0 [Default\_SBCRoutingPolicy]". The window is divided into two main sections: "GENERAL" and "ACTION".

**GENERAL Section:**

- Index:** 0
- Name:** Terminate OPTIONS
- Alternative Route Options:** Route Row
- MATCH Section:**
  - Source IP Group:** Any
  - Request Type:** OPTIONS
  - Source Username Prefix:** \*
  - Source Host:** \*
  - Source Tags:** (empty)

**ACTION Section:**

- Destination Type:** Dest Address
- Destination IP Group:** --
- Destination SIP Interface:** --
- Destination Address:** internal
- 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.

- b. Click **Apply**.

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

Parameter	Value
Index	1
Route Name	<b>S4B to ITSP</b> (arbitrary descriptive name)
Source IP Group	<b>S4B</b>
Destination Type	<b>IP Group</b>
Destination IP Group	<b>BellCanada</b>
Destination SIP Interface	<b>BellCanada</b>

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

The screenshot shows a configuration window titled "IP-to-IP Routing [S4b to ITSP]". At the top, there is a "Routing Policy" dropdown menu set to "#0 [Default\_SBCRoutingPolicy]". The configuration is divided into three main sections: GENERAL, MATCH, and ACTION.

- GENERAL:**
  - Index: 1
  - Name: S4b to ITSP
  - Alternative Route Options: Route Row
- MATCH:**
  - Source IP Group: #1 [S4B] (with a "View" link)
  - Request Type: All
  - Source Username Prefix: \*
  - Source Host: \*
  - Source Tag: (empty)
- ACTION:**
  - Destination Type: IP Group
  - Destination IP Group: #2 [BellCanada] (with a "View" link)
  - Destination SIP Interface: #1 [BellCanada] (with a "View" link)
  - Destination Address: (empty)
  - Destination Port: 0
  - Destination Transport Type: (empty)
  - Call Setup Rules Set ID: -1
  - Group Policy: Sequential
  - Cost Group: -- (with a "View" link)

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

- b. Click **Apply**.

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

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

**Figure 4-37: Configuring IP-to-IP Routing Rule for ITSP to S4B**

- b. Click **Apply**.

The configured routing rules are shown in the figure below:

**Figure 4-38: 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	BellCanada	BellCanada	
2	ITSP to S4B	Default_SBC	Route Row	BellCanada	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 45) to denote the source and destination of the call.



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

For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from the Bell Canada 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	<b>0</b>
Name	<b>Add + toward S4B</b>
Source IP Group	<b>BellCanada</b>
Destination IP Group	<b>S4B</b>
Destination Username Prefix	* (asterisk sign)
Manipulated Item	<b>Destination URI</b>
Prefix to Add	<b>+ (plus sign)</b>

Figure 4-39: 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 Bell Canada SIP Trunk IP Group:

Figure 4-40: Example of Configured IP-to-IP Outbound Manipulation Rules

INDEX	NAME	ROUTING POLICY	ADDITION MANIPUL	SOURCE IP GROUP	DESTINAT IP GROUP	SOURCE USERNAM PREFIX	DESTINAT USERNAM PREFIX	MANIPUL ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Add + tow	Default_S	No	BellCanad	S4B	*	*	Destination	0	0	255	+	
1	Remove +	Default_S	No	S4B	Any	*	+	Destination	1	0	255		
2	Remove +	Default_S	No	S4B	Any	+	*	Source UF	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.

➤ **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 Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group. This removes the 'ms-opaque' parameter from the Contact Header.

Parameter	Value
Index	0
Name	Remove ms-opaque
Manipulation Set ID	4
Message Type	any.request
Action Subject	header.contact.url.param.ms-opaque
Action Type	Remove

**Figure 4-41: Configuring SIP Message Manipulation Rule 0 (for Bell Canada SIP Trunk)**

The screenshot shows a configuration window titled "Message Manipulations [Remove ms-opaque]". It is divided into three sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
  - Index: 0
  - Name: Remove ms-opaque
  - Manipulation Set ID: 4
  - Row Role: Use Current Condition
- ACTION:**
  - Action Subject: header.contact.url.param.ms-opaque
  - Action Type: Remove
  - Action Value: (empty)
- MATCH:**
  - Message Type: any.request
  - Condition: (empty)

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



- Configure another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk, which will be executed if the manipulation rule Index 0 (above) is executed. This rule is applied to response messages sent to the Bell Canada SIP Trunk IP Group. This rule normalizes the SIP Contact Header according to the Bell Canada requirements.

Parameter	Value
Index	1
Name	<b>Add tgrp to contact</b>
Manipulation Set ID	4
Row Role	<b>Use Previous Condition</b>
Action Subject	<b>header.contact.url.user</b>
Action Type	<b>Modify</b>
Action Value	<b>header.from.url.user+';tgrp=customer;trunk-context=siptrunking.bell.ca'</b>

**Figure 4-42: Configuring SIP Message Manipulation Rule 1 (for Bell Canada SIP Trunk)**

*Message Manipulations [Add tgrp to contact]*

**GENERAL**

Index: 1

Name: Add tgrp to contact

Manipulation Set ID: 4

Row Role: Use Previous Condition

**ACTION**

Action Subject: header.contact.url.user

Action Type: Modify

Action Value: header.from.url.user+';tgrp=vsa

**MATCH**

Message Type:

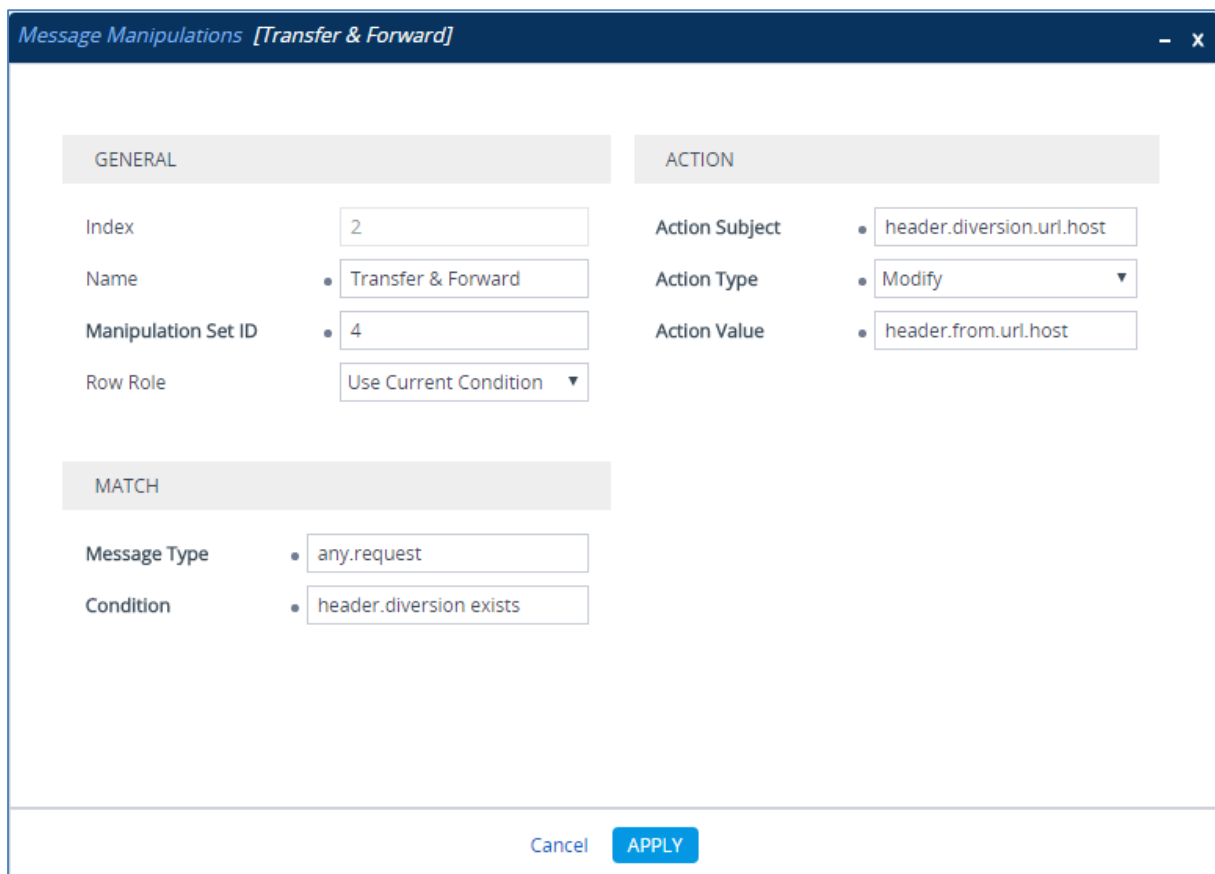
Condition:

Cancel APPLY

4. Configure another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer or Forward initiated by the Microsoft Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Diversion Header with the value from the SIP From Header, in case the SIP Diversion Header exists.

Parameter	Value
Index	<b>2</b>
Name	<b>Transfer &amp; Forward</b>
Manipulation Set ID	<b>4</b>
Message Type	<b>any.request</b>
Condition	<b>header.diversion exists</b>
Action Subject	<b>header.diversion.url.host</b>
Action Type	<b>Modify</b>
Action Value	<b>header.from.url.host</b>

**Figure 4-43: Configuring SIP Message Manipulation Rule 2 (for Bell Canada SIP Trunk)**



*Message Manipulations [Transfer & Forward]*

**GENERAL**

Index: 2

Name: Transfer & Forward

Manipulation Set ID: 4

Row Role: Use Current Condition

**ACTION**

Action Subject: header.diversion.url.host

Action Type: Modify

Action Value: header.from.url.host

**MATCH**

Message Type: any.request

Condition: header.diversion exists

Cancel APPLY

- Configure another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer initiated by the Microsoft Skype for Business Server 2015 IP Group. This adds the SIP Diversion Header with the value from the SIP Referred-By Header, in case the SIP Referred-By Header exists.

Parameter	Value
Index	3
Name	Call Transfer
Manipulation Set ID	4
Message Type	any.request
Condition	header.referred-by exists
Action Subject	header.diversion
Action Type	Add
Action Value	header.referred-by

Figure 4-44: Configuring SIP Message Manipulation Rule 3 (for Bell Canada SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Call Transfer]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

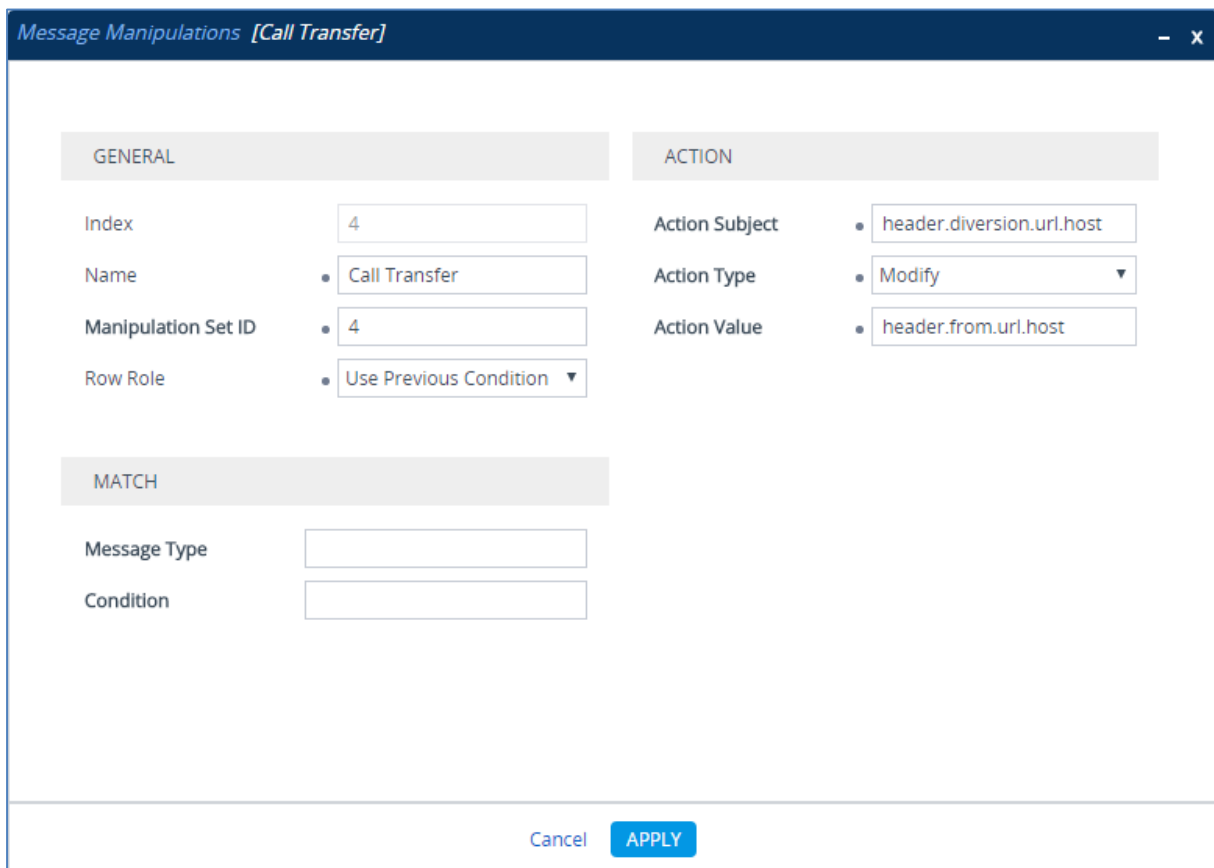
- GENERAL:**
  - Index: 3
  - Name: Call Transfer
  - Manipulation Set ID: 4
  - Row Role: Use Current Condition
- ACTION:**
  - Action Subject: header.diversion
  - Action Type: Add
  - Action Value: header.referred-by
- MATCH:**
  - Message Type: any.request
  - Condition: header.referred-by exists

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

6. Configure another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk, which will be executed if the manipulation rule Index 3 (above) is executed. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer initiated by the Microsoft Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Diversion Header with the value from the SIP From Header.

Parameter	Value
Index	4
Name	Call Transfer
Manipulation Set ID	4
Row Role	Use Previous Condition
Action Subject	header.diversion.url.host
Action Type	Modify
Action Value	header.from.url.host

**Figure 4-45: Configuring SIP Message Manipulation Rule 4 (for Bell Canada SIP Trunk)**



*Message Manipulations [Call Transfer]*

**GENERAL**

Index: 4

Name: Call Transfer

Manipulation Set ID: 4

Row Role: Use Previous Condition

**ACTION**

Action Subject: header.diversion.url.host

Action Type: Modify

Action Value: header.from.url.host

**MATCH**

Message Type:

Condition:

Cancel **APPLY**

- Configure another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer or Forward initiated by the Microsoft Skype for Business Server 2015 IP Group. This removes the '+' prefix from the user part of the SIP Diversion Header.

Parameter	Value
Index	5
Name	Transfer & Forward
Manipulation Set ID	4
Message Type	any.request
Action Subject	header.diversion.url.user
Action Type	Remove Prefix
Action Value	'+'

Figure 4-46: Configuring SIP Message Manipulation Rule 5 (for Bell Canada SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Transfer & Forward]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
  - Index: 5
  - Name: Transfer & Forward
  - Manipulation Set ID: 4
  - Row Role: Use Current Condition
- ACTION:**
  - Action Subject: header.diversion.url.user
  - Action Type: Remove Prefix
  - Action Value: '+'
- MATCH:**
  - Message Type: any.request
  - Condition: (empty field)

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

8. Configure another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer initiated by the Microsoft Skype for Business Server 2015 IP Group. This removes the SIP Referred-By Header.

Parameter	Value
Index	6
Name	Call Transfer
Manipulation Set ID	4
Message Type	any.request
Condition	header.referred-by exists
Action Subject	header.referred-by
Action Type	Remove

**Figure 4-47: Configuring SIP Message Manipulation Rule 6 (for Bell Canada SIP Trunk)**

*Message Manipulations [Call Transfer]*

**GENERAL**

Index: 6

Name: Call Transfer

Manipulation Set ID: 4

Row Role: Use Current Condition

**ACTION**

Action Subject: header.referred-by

Action Type: Remove

Action Value:

**MATCH**

Message Type: any.request

Condition: header.referred-by exists

Cancel APPLY

9. Configure another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule is applied to response messages sent to the Bell Canada SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method type '603' with the value '486', because Bell Canada SIP Trunk not recognizes '603' method type.

Parameter	Value
Index	7
Name	Reject Cause
Manipulation Set ID	4
Message Type	any.response.603
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'486'

**Figure 4-48: Configuring SIP Message Manipulation Rule 7 (for Bell Canada SIP Trunk)**

The screenshot shows a configuration window titled "Message Manipulations [Reject Cause]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
  - Index: 7
  - Name: Reject Cause
  - Manipulation Set ID: 4
  - Row Role: Use Current Condition
- ACTION:**
  - Action Subject: header.request-uri.methodtype
  - Action Type: Modify
  - Action Value: '486'
- MATCH:**
  - Message Type: any.response.603
  - Condition: (empty)

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

**Figure 4-49: Example of Configured SIP Message Manipulation Rules**

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Remove ms-opaque	4	any.request		header.contact.ur	Remove		Use Current Condit
1	Add tgrp to contac	4			header.contact.ur	Modify	header.from.url.u	Use Previous Cond
2	Transfer & Forwar	4	any.request	header.diversion €	header.diversion.t	Modify	header.from.url.h	Use Current Condit
3	Call Transfer	4	any.request	header.referred-by	header.diversion	Add	header.referred-b	Use Current Condit
4	Call Transfer	4			header.diversion.t	Modify	header.from.url.h	Use Previous Cond
5	Transfer & Forwar	4	any.request		header.diversion.t	Remove Prefix	‘+’	Use Current Condit
6	Call Transfer	4	any.request	header.referred-b	header.referred-b	Remove		Use Current Condit
7	Reject Cause	4	any.response.603		header.request-ur	Modify	‘486’	Use Current Condit

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to the Bell Canada SIP Trunk IP Group. These rules are specifically required to enable proper interworking between Bell Canada SIP Trunk and Skype for Business Server 2015. Refer to the *User’s Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages sent to the Bell Canada SIP Trunk IP Group. This removes the ‘ms-opaque’ parameter from the Contact Header.	SIP Messages normalization according to the Bell Canada Specification.
1	If the manipulation rule Index 0 (above) is executed, then the following rule is also executed. It normalizes the SIP Contact Header according to the Bell Canada requirements.	
2	This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer or Forward initiated by the Microsoft Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Diversion Header with the value from the SIP From Header, in case the SIP Diversion Header exists.	For Call Transfer or Forward scenarios, the Bell Canada SIP Trunk needs that the Host part in the SIP Diversion Header is predefined. In order to do this, the Host part of the SIP Diversion Header is replaced with the value from the SIP From Header.
3	This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer initiated by the Microsoft Skype for Business Server 2015 IP Group. This adds the SIP Diversion Header with the value from the SIP Referred-By Header, in case the SIP Referred-By Header exists.	Bell Canada SIP Trunk does not support “Referred-By” Header. So in Call Transfer scenarios, the SIP Diversion Header with the value from the SIP Referred-By Header, is added.
4	If the manipulation rule Index 3 (above) is executed, the following rule is also executed. It applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer initiated by the Microsoft Skype for Business Server 2015 IP Group. This replaces the Host part of the SIP Diversion Header with the value from the SIP From Header.	For Call Transfer scenarios, Bell Canada SIP Trunk needs that Host part in SIP Diversion Header will be predefined. To do this, the Host part of the SIP Diversion Header is replaced with the value from SIP From Header.



<b>Rule Index</b>	<b>Rule Description</b>	<b>Reason for Introducing Rule</b>
5	This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer or Forward initiated by the Microsoft Skype for Business Server 2015 IP Group. This removes the '+' prefix from the user part of the SIP Diversion Header.	Bell Canada SIP Trunk does not support E.164 number format in SIP messages, so it is necessary to remove '+' in each user part.
6	This rule applies to messages sent to the Bell Canada SIP Trunk IP Group for Call Transfer initiated by the Microsoft Skype for Business Server 2015 IP Group. This removes the SIP Referred-By Header.	Bell Canada SIP Trunk does not support the "Referred-By" Header in SIP INVITE messages, so it is necessary to remove them.
7	This rule is applied to response messages sent to the Bell Canada SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method type '603' with the value '486', because Bell Canada SIP Trunk not recognizes '603' method type.	Bell Canada SIP Trunk does not recognize the '603' method type.

10. Assign Manipulation Set ID 4 to the Bell Canada 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 Bell Canada SIP trunk IP Group, and then click **Edit**.
  - c. Set the 'Outbound Message Manipulation Set' field to **4**.

**Figure 4-50: Assigning Manipulation Set 4 to the Bell Canada SIP Trunk IP Group**

The screenshot shows the 'IP Groups [BellCanada]' configuration window. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this are two main sections: 'GENERAL' and 'QUALITY OF EXPERIENCE'. The 'GENERAL' section includes fields for Index (2), Name (BellCanada), Topology Location (Up), Type (Server), Proxy Set (#2 [BellCanada]), IP Profile (#2 [BellCanada]), Media Realm (#1 [MRWan]), Contact User, SIP Group Name (siptrunking.bell.ca), and Created By Routing Server (No). The 'QUALITY OF EXPERIENCE' section includes QoE Profile and Bandwidth Profile, both set to '--'. Below these is the 'MESSAGE MANIPULATION' section, which is expanded to show 'Inbound Message Manipulation Set' (-1) and 'Outbound Message Manipulation Set' (4). There are also two empty text boxes for 'Message Manipulation User-Defined String 1' and 'Message Manipulation User-Defined String 2'. At the bottom, there is a 'SBC REGISTRATION AND AUTHENTICATION' section which is currently collapsed. At the very bottom of the window 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 Bell Canada SIP Trunk on behalf of Skype for Business Server 2015. The Bell Canada 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 Bell Canada 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	<b>S4B</b>
Application Type	<b>SBC</b>
Serving IP Group	<b>BellCanada</b>
Host Name	As provided by the SIP Trunk provider
Register	<b>No</b>
Contact User	<b>123123123123</b> (trunk main line)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

**Figure 4-51: 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 tabs: "GENERAL" and "CREDENTIALS".

**GENERAL Tab:**

- Index: 0
- Served Trunk Group: -1
- Application Type: SBC
- Serving IP Group: #2 [BellCanada] (with a "View" link)
- Host Name: 123.123.123.123
- Register: No
- Contact User: 123123123123

**CREDENTIALS Tab:**

- User Name: 123123123123
- Password: (empty field)

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

4. Click **Apply**.

**This page is intentionally left blank.**

## 4.16 Step 16: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

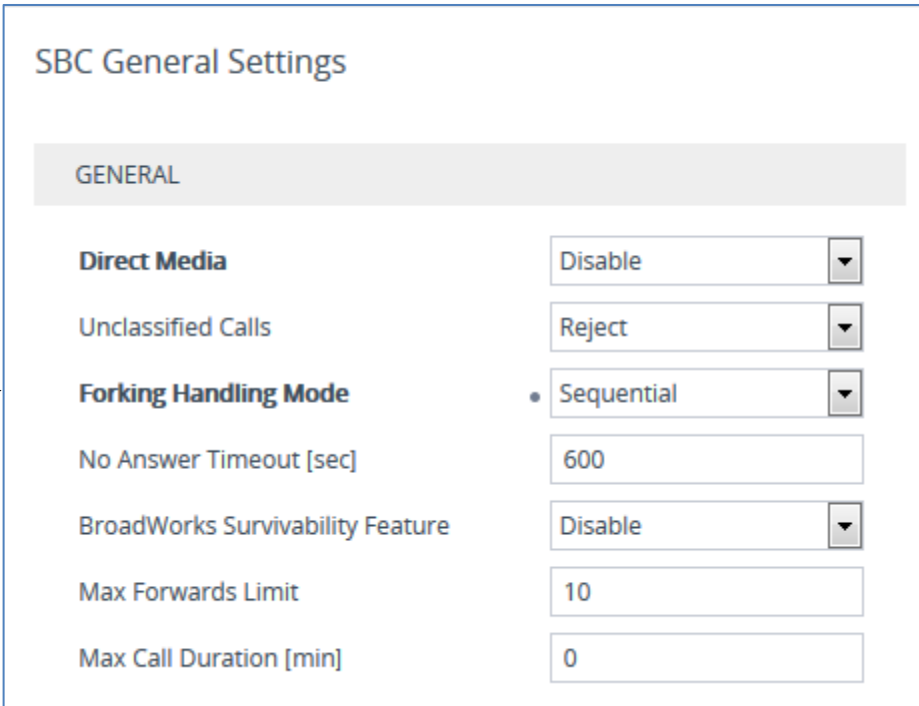
### 4.16.1 Step 16a: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, 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 4-52: Configuring Forking Mode**



The screenshot shows the 'SBC General Settings' page. A grey bar at the top is labeled 'GENERAL'. Below it, several settings are listed in a table-like format. The 'Forking Handling Mode' setting is highlighted with a black arrow pointing to its dropdown menu, which is currently set to 'Sequential'. Other settings include 'Direct Media' (Disable), 'Unclassified Calls' (Reject), 'No Answer Timeout [sec]' (600), 'BroadWorks Survivability Feature' (Disable), 'Max Forwards Limit' (10), and 'Max Call Duration [min]' (0).

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

3. Click **Apply**.

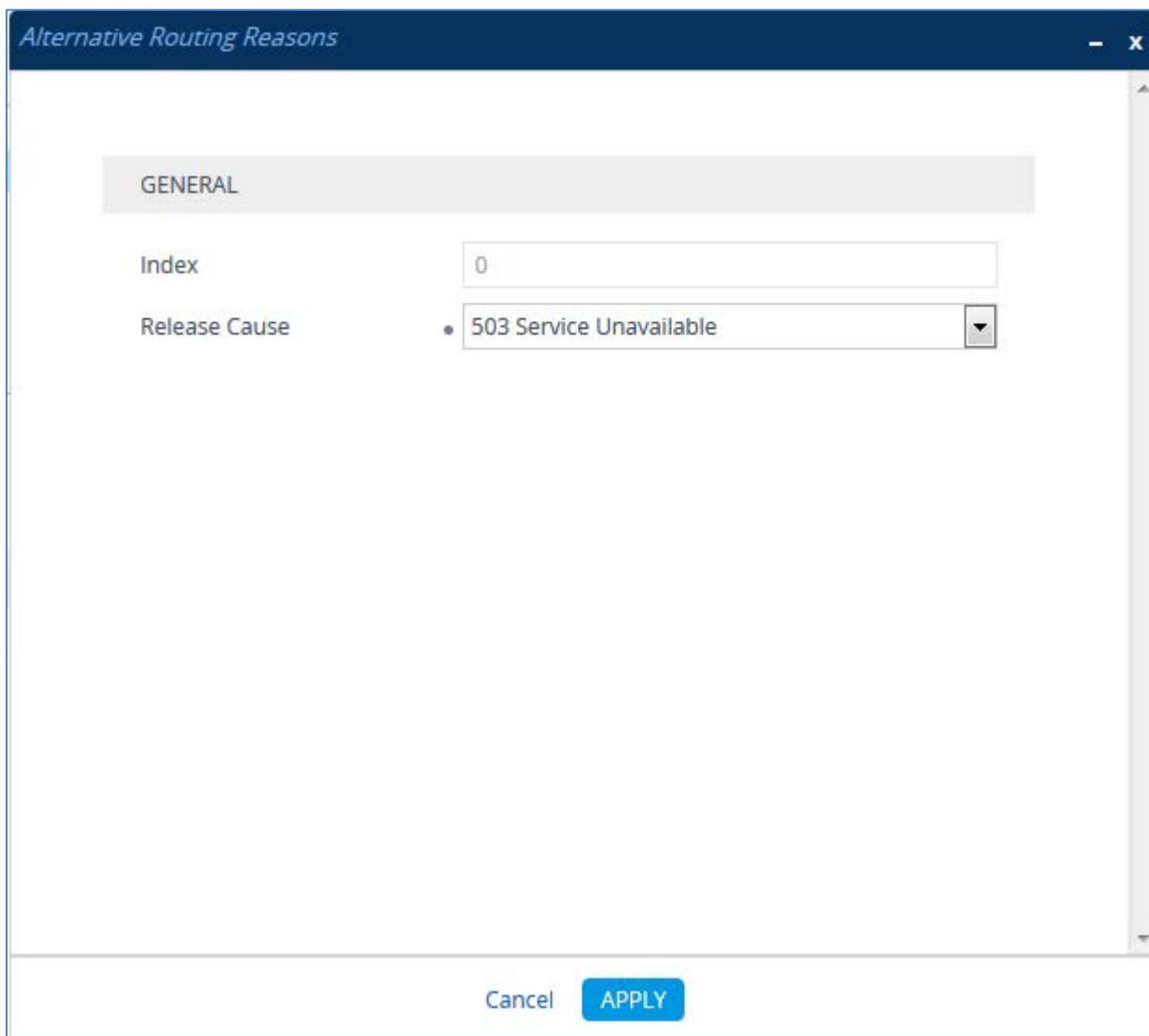
## 4.16.2 Step 16b: Configure SBC Alternative Routing Reasons

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 4-53: 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 window control icons. Below the header is a light gray bar with the word "GENERAL" in bold. The main area contains two fields: "Index" with a text input field containing the number "0", and "Release Cause" with a dropdown menu showing "503 Service Unavailable". At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

4. Click **Apply**.

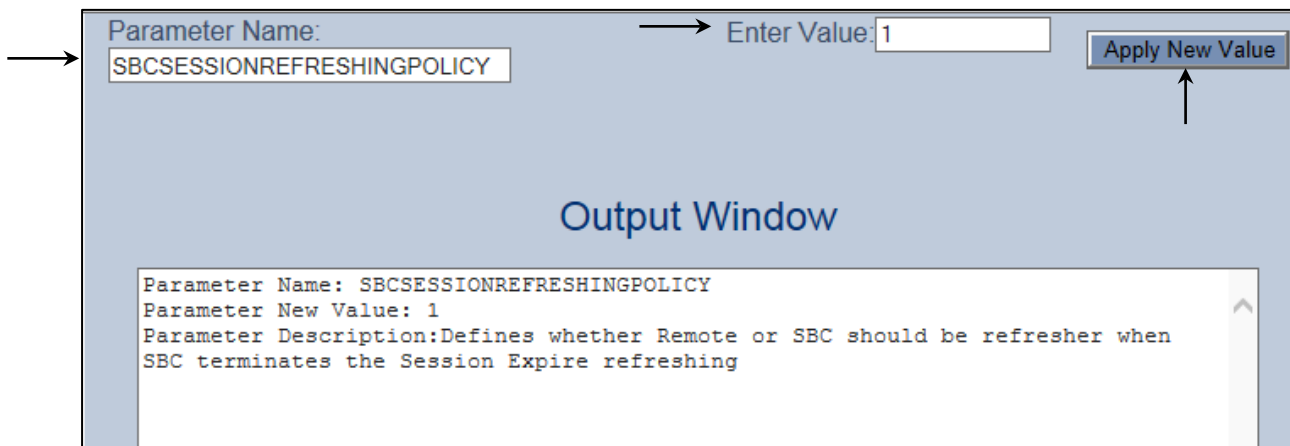
### 4.16.3 Step 16c: Configure SBC Session Refreshing Policy

This step shows how to configure the 'SBC Session Refreshing Policy' parameter. In some cases, Microsoft Skype for Business does not perform a refresh of Session Timer even when it confirms that it will be refresher. To resolve this issue, the SBC is configured as Session Expire refresher.

➤ **To configure SBC Session Refreshing Policy:**

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., <http://10.15.17.10/AdminPage>).
2. In the left pane of the page that opens, click *ini* Parameters.

**Figure 4-54: Configuring SBC Session Refreshing Policy in AdminPage**



3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
SBCSESSIONREFRESHINGPOLICY	1 (enables SBC as refresher of Session Timer)

4. Click the **Apply New Value** button for each field.

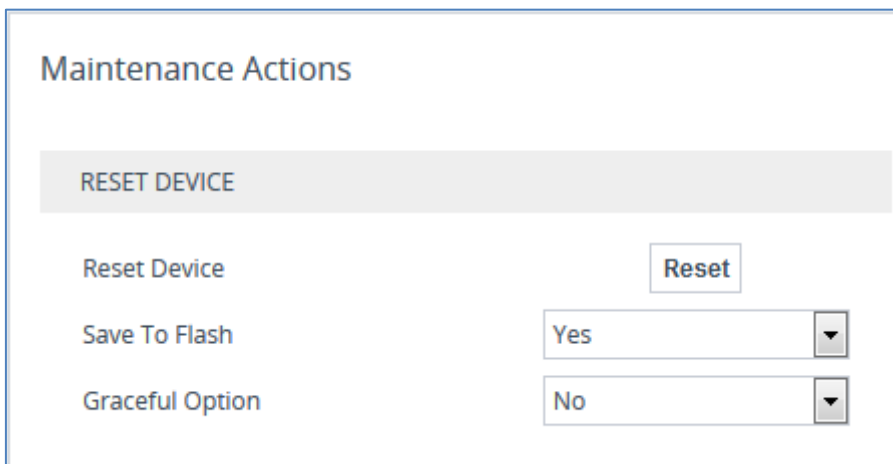
## 4.17 Step 17: Reset the E-SBC

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 4-55: Resetting the E-SBC**



The screenshot shows the 'Maintenance Actions' 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 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 AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 31, is shown below:



**Note:** To load or save an *ini* file, use the Configuration File page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**).

```

;*****
;** Ini File **
;*****

;Board: Mediant 500
;HW Board Type: 69  FK Board Type: 77
;Serial Number: 4965606
;Slot Number: 1
;Software Version: 7.20A.001.501
;DSP Software Version: 5014AE3_R => 720.23
;Board IP Address: 10.15.77.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M  Flash size: 64M  Core speed: 500Mhz
;Num of DSP Cores: 1  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features:;Board Type: Mediant 500 ;DATA features: ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;Channel Type: DspCh=30
IPMediaDspCh=30 ;HA ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;IP Media: Conf VXML ;DSP Voice features: RTCP-XR
;PSTN FALLBACK Supported ;FXSPorts=3 ;FXOPorts=1 ;Coders: G723 G729 G728
NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711
MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB
;Control Protocols: MGCP SIP SASurvivability SBC=60 MSFT FEU=100
TestCall=100 ;Default features:;Coders: G711 G726;

;----- HW components-----
;
; Slot # : Module type : # of ports
;-----
;      2 : FXS          : 3
;      3 : FXO          : 1
;-----

[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
NTPServerIP = '0.0.0.0'

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10

```

```
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

ENABLEMEDIASECURITY = 1

[WEB Params]

LogoWidth = '145'

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SBCSESSIONREFRESHINGPOLICY = 1

[SCTP Params]

[IPsec Params]

[Audio Staging Params]
```

```
[SNMP Params]

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0;

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.10, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.160, 25, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]
```

```

[ DspTemplates ]

;
; *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$KhNPHB5LGQlQVwoCAw5TXQ1fAwVYXw93eXsncHx0f354eC8qKC8tYGB1Zm0xNWA8bmk6Z
Wlt01zTVwcGV15RCQg=", 1, 0, 5, 15, 60, 200,
"6d6b6fed6c859d76e9bd3f2ddac9fa42";
WebUsers 1 = "User",
"$1$X29RB1MFV1ECBFkLWg4JD1YNQkcXQUZBREUcHBtPHRhPT7e2uua9seCxse296bru6r3xp
aDy8POnoaugo6z4qKs=", 1, 0, 2, 15, 60, 50,
"8a7afee729111917232021f993b9ba02";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_RequireStrictCert, TLSContexts_OcspEnable,
TLSContexts_OcspServerPrimary, TLSContexts_OcspServerSecondary,
TLSContexts_OcspServerPort, TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 7, "RC4:AES128", "ALL:!ADH", 0, 0, , , 2560,
0;

[ \TLSContexts ]

[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";
AudioCodersGroups 1 = "AudioCodersGroups_1";
AudioCodersGroups 2 = "AudioCodersGroups_2";

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]

FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "BellCanada Allowed Coders";

[ \AllowedAudioCodersGroups ]
    
```

```

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_CNGmode,
IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia,
IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller,
IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour,
IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupName,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarlyl183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPptimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWTtoVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCMaxCallDuration,
IpProfile_SBCGenerateRTP, IpProfile_SBCISUPBodyHandling,
IpProfile_SBCISUPVariant, IpProfile_SBCVoiceQualityEnhancement,
IpProfile_SBCMaxOpusBW;

IpProfile 1 = "S4B", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "",

```

```

"AudioCodersGroups_1", 0, 0, "", "", "", 0, 1, 1, 0, 0, 0, 8, 300, 400,
0, 0, 0, "", 0, 0, 1, 3, 0, 1, 1, 0, 3, 2, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0,
0, 0, 0, 1, 0, 1, 1, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0,
0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0;
IpProfile 2 = "BellCanada", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24,
0, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_2", 0, 0, "", "BellCanada Allowed Coders", "", 2, 2,
0, 0, 1, 0, 8, 300, 400, 1, 2, 0, "", 0, 0, 1, 3, 2, 2, 2, 1, 3, 0, 1, 0,
1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0,
0, 0, 0, 0, 0, 0;

[ \IpProfile ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile,
CpMediaRealm_TopologyLocation;
CpMediaRealm 0 = "MRLan", "LAN_IF", "", 6000, 100, 6999, 1, "", "", 0;
CpMediaRealm 1 = "MRWan", "WAN_IF", "", 7000, 100, 7999, 0, "", "", 1;

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "";

[ \SRD ]

[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;
    
```

```

[ \MessagePolicy ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation;
SIPInterface 0 = "S4B", "LAN_IF", 2, 0, 0, 5067, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0, 0;
SIPInterface 1 = "BellCanada", "WAN_IF", 2, 5060, 0, 0, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1, 0, 1;

[ \SIPInterface ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB;
!ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"S4B", "", "", "", "", 1;
ProxySet 1 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "", 1, -1, "", "",
"S4B", "", "", "", 1;
ProxySet 2 = "BellCanada", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1,
"503", "", "BellCanada", "", "", 1;

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWPProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,

```

```

IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1;
IPGroup 1 = 0, "S4B", "S4B", "customer.bell.ca", "", -1, 0,
"DefaultSRD", "MRLan", 1, "S4B", -1, -1, -1, 0, 0, "", 0, -1, -1, "",
"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 0, "", -1;
IPGroup 2 = 0, "BellCanada", "BellCanada", "siptrunking.bell.ca", "", -1,
0, "DefaultSRD", "MRWan", 1, "BellCanada", -1, -1, 4, 0, 0, "", 0, -1, -
1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0,
0, -1, 0, 0, 1, "", -1;

[ \IPGroup ]

[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "1", 0, "FE.S4B.interop:5067", 2;
ProxyIp 1 = "2", 0, "123.123.123.123:5060", 0;

[ \ProxyIp ]

[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "S4B", "BellCanada", "123123123123", "Password",
"123.123.123.123", 0, "123123123123", 2;

[ \Account ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
    
```



```

IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"", "", "", "", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "";
IP2IPRouting 1 = "S4B to ITSP", "Default_SBCRoutingPolicy", "S4B", "",
"", "", "", 0, "", "Any", 0, -1, 0, "BellCanada", "BellCanada", "", 0,
-1, 0, 0, "", "", "";
IP2IPRouting 2 = "ITSP to S4B", "Default_SBCRoutingPolicy", "BellCanada",
"", "", "", "", 0, "", "Any", 0, -1, 0, "S4B", "S4B", "", 0, -1, 0,
0, "", "", "";

[ \IP2IPRouting ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "Add + toward S4B",
"Default_SBCRoutingPolicy", 0, "BellCanada", "S4B", "", "", "", "",
"", "", 0, "Any", 0, 1, 0, 0, 255, "+", "", 0, "", "";
IPOutboundManipulation 1 = "Call Abroad", "Default_SBCRoutingPolicy", 0,
"S4B", "Any", "", "", "+9", "", "", "", 0, "Any", 0, 1, 1, 0, 255,
"011", "", 0, "", "";
IPOutboundManipulation 2 = "Call to US", "Default_SBCRoutingPolicy", 0,
"S4B", "Any", "", "", "7", "", "", "", 0, "Any", 0, 1, 0, 0, 255,
"1", "", 0, "", "";
IPOutboundManipulation 3 = "Remove + from Source",
"Default_SBCRoutingPolicy", 0, "S4B", "Any", "+", "", "", "", "", "",
0, "Any", 0, 0, 1, 0, 255, "", "", 0, "", "";

[ \IPOutboundManipulation ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Remove ms-opaque", 4, "any.request", "",
"header.contact.url.param.ms-opaque", 1, "", 0;

```

```

MessageManipulations 1 = "Add tgrp to contact", 4, "", "",
"header.contact.url.user", 2,
"header.from.url.user+';tgrp=customer;trunk-
context=siptrunking.bell.ca'", 1;
MessageManipulations 2 = "Transfer & Forward", 4, "any.request",
"header.diversion.exists", "header.diversion.url.host", 2,
"header.from.url.host", 0;
MessageManipulations 3 = "Call Transfer", 4, "any.request",
"header.referred-by.exists", "header.diversion", 0, "header.referred-by",
0;
MessageManipulations 4 = "Call Transfer", 4, "", "",
"header.diversion.url.host", 2, "header.from.url.host", 1;
MessageManipulations 5 = "Transfer & Forward", 4, "any.request", "",
"header.diversion.url.user", 6, "'+'", 0;
MessageManipulations 6 = "Call Transfer", 4, "any.request",
"header.referred-by.exists", "header.referred-by", 1, "", 0;
MessageManipulations 7 = "Reject Cause", 4, "any.response.603", "",
"header.request-uri.methodtype", 2, "'486'", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]

[ MaliciousSignatureDB ]

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
    
```

```
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 0 = "BellCanada Allowed Coders", 0, 3, "";
AllowedAudioCoders 1 = "BellCanada Allowed Coders", 1, 2, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_1", 0, 2, 2, 90, -1, 1, "";
AudioCoders 2 = "AudioCodersGroups_1", 1, 1, 2, 90, -1, 1, "";
AudioCoders 3 = "AudioCodersGroups_2", 0, 3, 2, 19, -1, 0, "";

[ \AudioCoders ]
```

**This page is intentionally left blank.**

## B Configuring Dynamic ONND

The procedure below describes additional steps needed to configure Dynamic Outgoing Name & Number Display (ONND) presentation mode.

### B.1 Configure SIP Message Manipulation Rules

The following SIP message manipulation rules should be configured in order to work in Dynamic ONND mode.

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

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Add a manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group. This removes the 'userphone' parameter from the SIP To Header.

Parameter	Value
Index	<b>10</b>
Name	<b>Dynamic ONND</b>
Manipulation Set ID	<b>4</b>
Message Type	<b>any.request</b>
Action Subject	<b>header.to.url.userphone</b>
Action Type	<b>Remove</b>

**Figure B-1: Configuring SIP Message Manipulation Rule 10 (for Bell Canada SIP Trunk)**

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

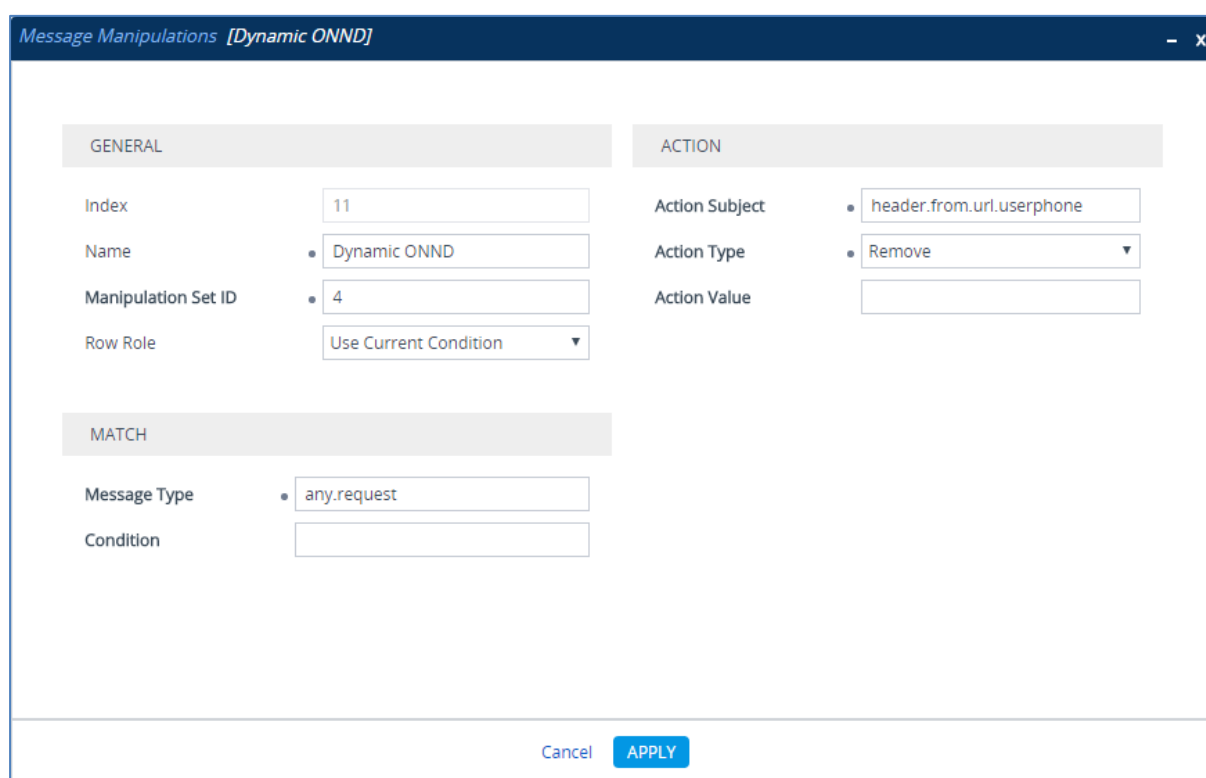
- GENERAL:**
  - Index: 10
  - Name: Dynamic ONND
  - Manipulation Set ID: 4
  - Row Role: Use Current Condition
- ACTION:**
  - Action Subject: header.to.url.userphone
  - Action Type: Remove
  - Action Value: (empty)
- MATCH:**
  - Message Type: any.request
  - Condition: (empty)

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

3. Add another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group. This removes the 'userphone' parameter from the SIP From Header.

Parameter	Value
Index	11
Name	Dynamic ONND
Manipulation Set ID	4
Message Type	any.request
Action Subject	header.from.url.userphone
Action Type	Remove

**Figure B-2: Configuring SIP Message Manipulation Rule 11 (for Bell Canada SIP Trunk)**



*Message Manipulations [Dynamic ONND]*

GENERAL		ACTION	
Index	11	Action Subject	header.from.url.userphone
Name	Dynamic ONND	Action Type	Remove
Manipulation Set ID	4	Action Value	
Row Role	Use Current Condition		

MATCH	
Message Type	any.request
Condition	

Cancel **APPLY**

4. Add another manipulation rule (Manipulation Set 4) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk IP Group. This removes the 'userphone' parameter from the SIP P-Asserted-Identity Header.

Parameter	Value
Index	12
Name	Dynamic ONND
Manipulation Set ID	4
Message Type	any.request
Action Subject	header.p-asserted-identity.url.userphone
Action Type	Remove

Figure B-3: Configuring SIP Message Manipulation Rule 11 (for Bell Canada SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Dynamic ONND]". It is organized into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL Section:**
  - Index: 12
  - Name: Dynamic ONND
  - Manipulation Set ID: 4
  - Row Role: Use Current Condition
- ACTION Section:**
  - Action Subject: header.p-asserted-identity.url.use
  - Action Type: Remove
  - Action Value: (empty field)
- MATCH Section:**
  - Message Type: any.request
  - Condition: (empty field)

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

**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](http://www.audiocodes.com/info)

**Website:** [www.audiocodes.com](http://www.audiocodes.com)



Document #: LTRT-39234