Configuration Note

AudioCodes Professional Services – Interoperability Lab

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

Version 7.2

Table of Contents

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: October-18-2018

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
39234	Initial document release for Version 7.2.
39235	Fix for workaround for call muting issue.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

This page is intentionally left blank.

1 Introduction

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

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (SE and VE)
Software Version	SIP_7.20A.001.501
Protocol	▪ SIP/UDP (to the Bell Canada SIP Trunk) ▪ SIP/TCP or TLS (to the S4B FE Server)
Additional Notes	None

2.2 Bell Canada SIP Trunking Version

Table 2-2: Bell Canada Version

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

2.3 Microsoft Skype for Business Server 2015 Version

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

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

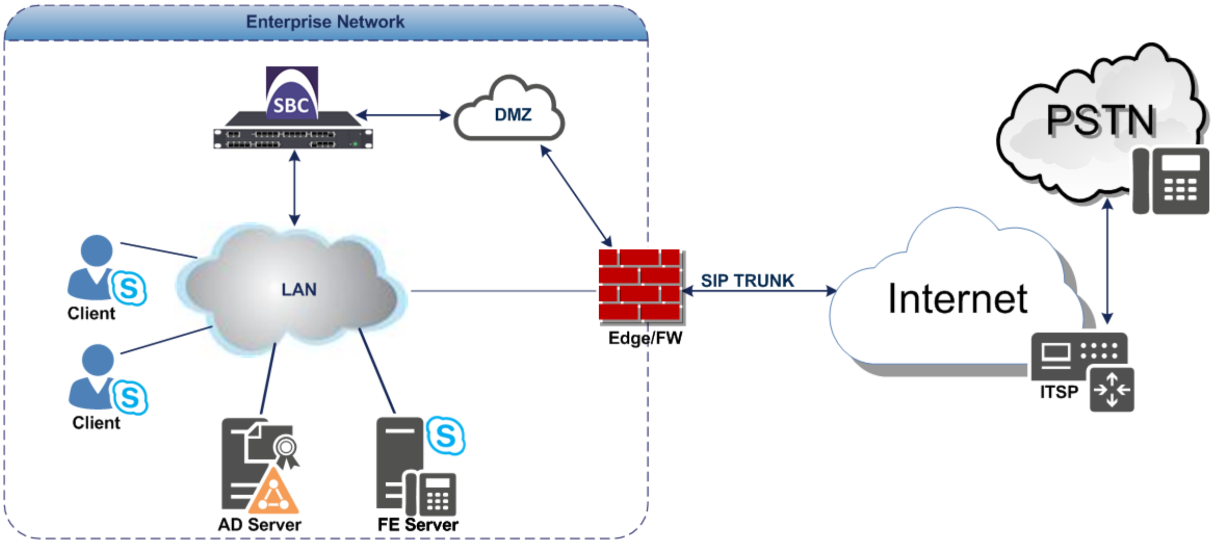
2.4 Interoperability Test Topology

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
Network	▪ Microsoft Skype for Business Server 2015 environment is located on the Enterprise's LAN ▪ Bell Canada SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SIP-over-TLS transport type ▪ Bell Canada SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders ▪ Bell Canada SIP Trunk supports G.711U-law and G.729 coders
Media Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SRTP media type ▪ Bell Canada SIP Trunk operates with RTP media type

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).

- When a Skype for Business user mutesthe call, Skype for Business server stops sending RTP packets. This causes the Bell Canada SIP Trunk to drop the call. To overcome this issue, the SBC needs to send RTP packets instead of Skype for Business. In order to achieve this, Force Transcoding needs to be configured in the IP Profile towards the Bell Canada SIP Trunk (see Section 4.7 on page 49).

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.

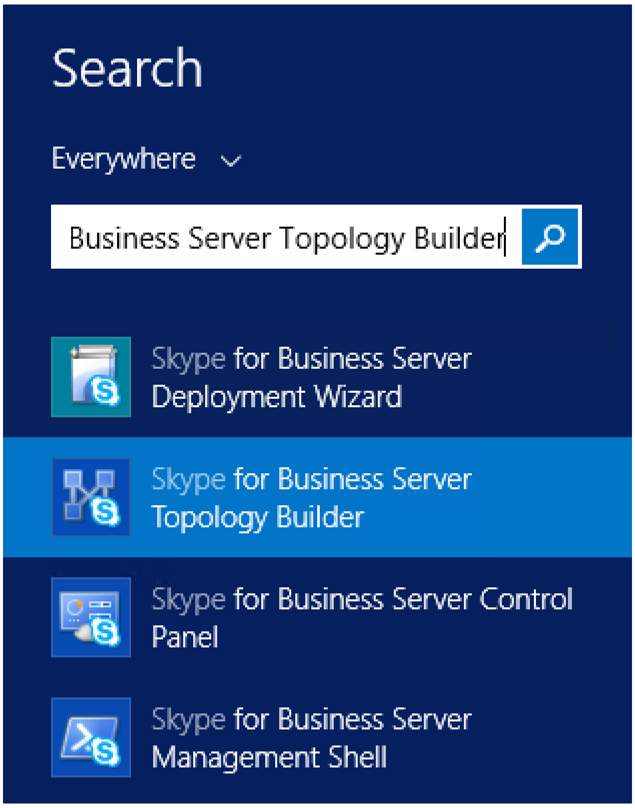
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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:**

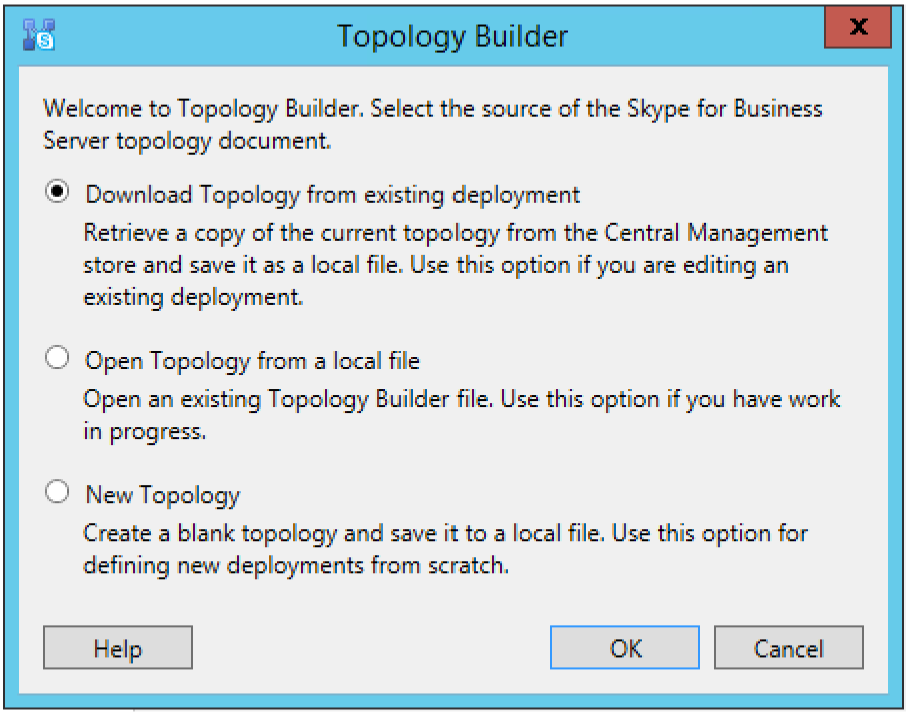
1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

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


Search
Everywhere
Business Server Topology Builder
Skype for Business Server Deployment Wizard
Skype for Business Server Topology Builder
Skype for Business Server Control Panel
Skype for Business Server Management Shell

The following is displayed:

Figure 3-2: Topology Builder Dialog Box



Welcome to Topology Builder. Select the source of the Skype for Business Server topology document.

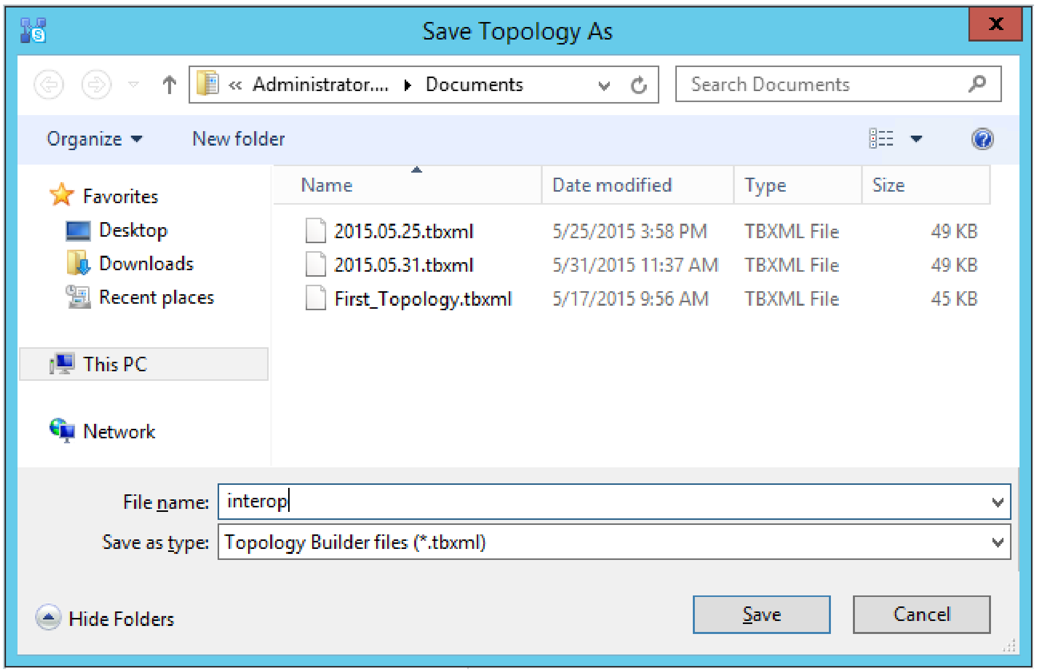
● Download Topology from existing deployment
Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.

○ Open Topology from a local file
Open an existing Topology Builder file. Use this option if you have work in progress.

○ New Topology
Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.

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



Name	Date modified	Type	Size
2015.05.25.tbxml	5/25/2015 3:58 PM	TBXML File	49 KB
2015.05.31.tbxml	5/31/2015 11:37 AM	TBXML File	49 KB
First_Topology.tbxml	5/17/2015 9:56 AM	TBXML File	45 KB

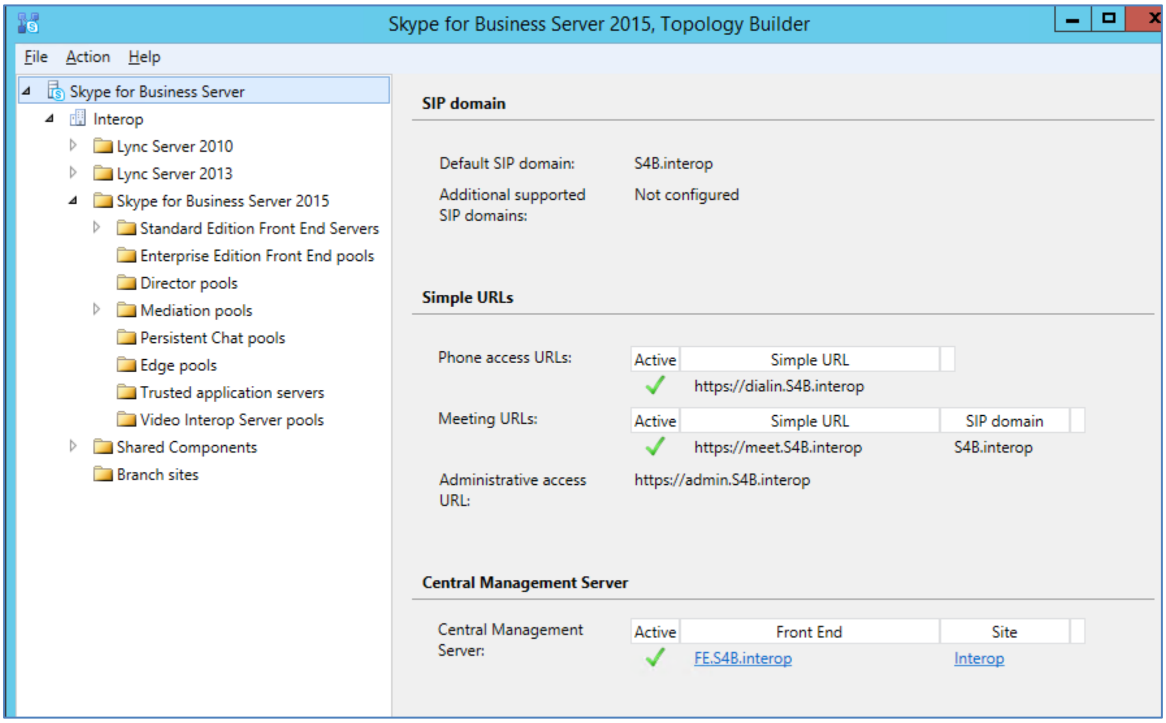
File name: interop

Save as type: Topology Builder files (*.tbxml)

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


Skype for Business Server 2015, Topology Builder
File Action Help
Skype for Business Server
Interop
Lync Server 2010
Lync Server 2013
Skype for Business Server 2015
Standard Edition Front End Servers
Enterprise Edition Front End pools
Director pools
Mediation pools
Persistent Chat pools
Edge pools
Trusted application servers
Video Interop Server pools
Shared Components
Branch sites

SIP domain

Default SIP domain: S4B.interop

Additional supported SIP domains: Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://dialin.S4B.interop

Meeting URLs:

Active	Simple URL	SIP domain
✓	https://meet.S4B.interop	S4B.interop

Administrative access URL: https://admin.S4B.interop

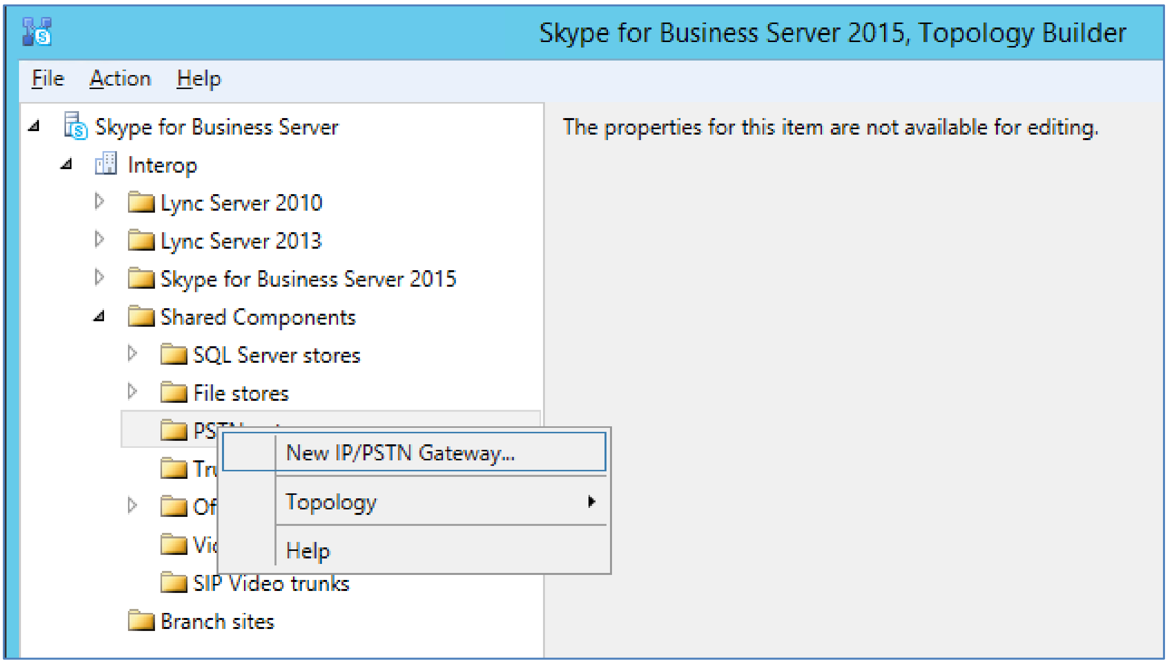
Central Management Server

Central Management Server:

Active	Front End	Site
✓	FE.S4B.interop	Interop

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:

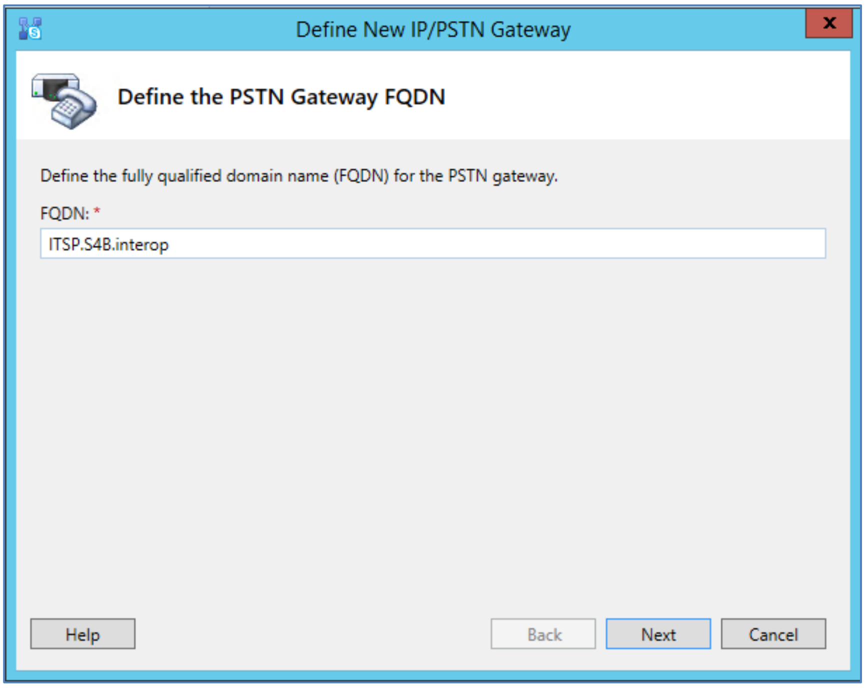
Figure 3-5: Choosing New IP/PSTN Gateway



The properties for this item are not available for editing.

The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



Define New IP/PSTN Gateway

Define the PSTN Gateway FQDN

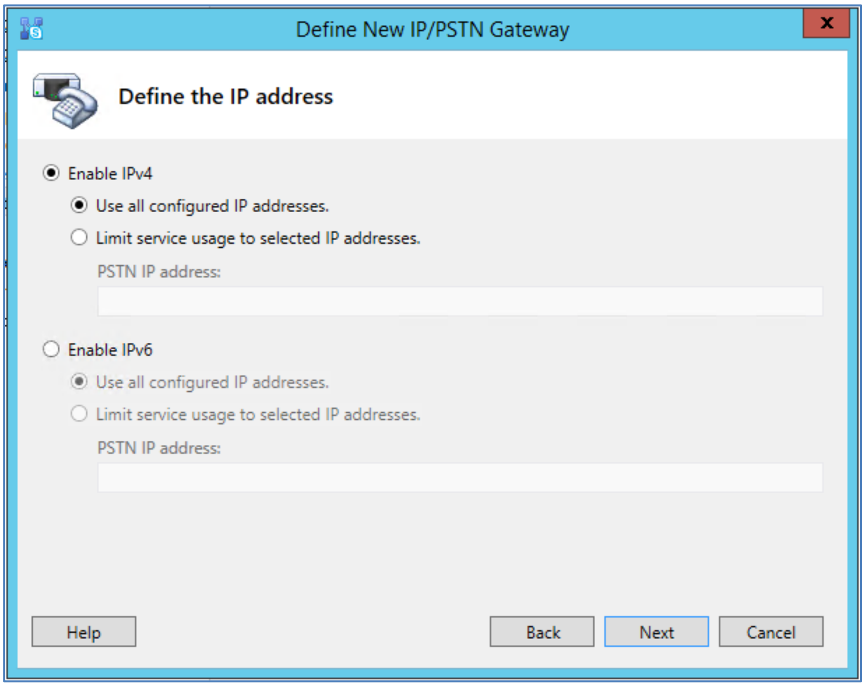
Define the fully qualified domain name (FQDN) for the PSTN gateway.

FQDN: *

ITSP.S4B.interop

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



Define New IP/PSTN Gateway

Define the IP address

● Enable IPv4

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

○ Enable IPv6

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

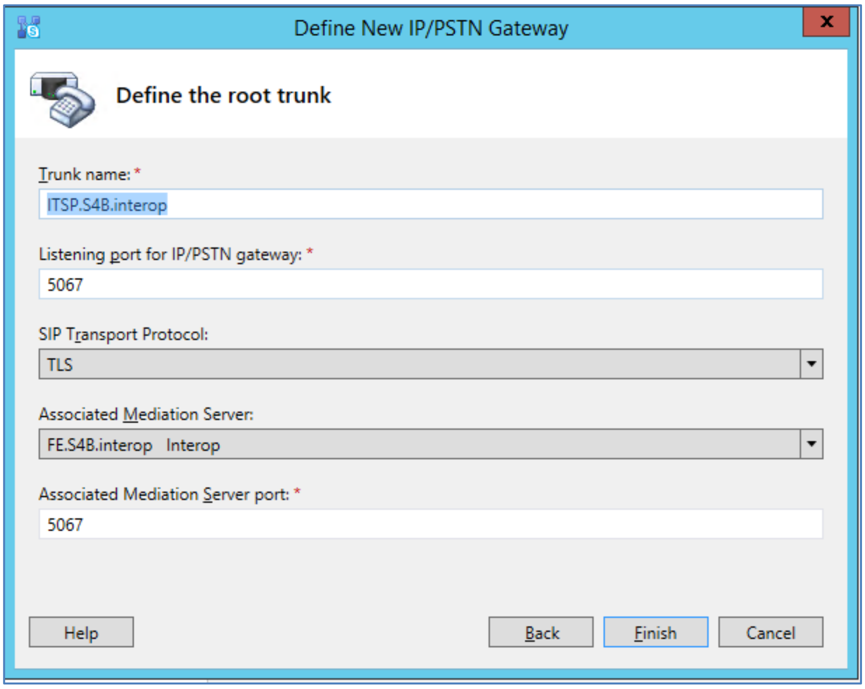
7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.
8. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server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



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

a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**). This parameter is later configured in the SIP Interface table (see Section 4.3 on page 37).

b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses. This parameter is later configured in the SIP Interface table (see Section 4.3 on page 37).

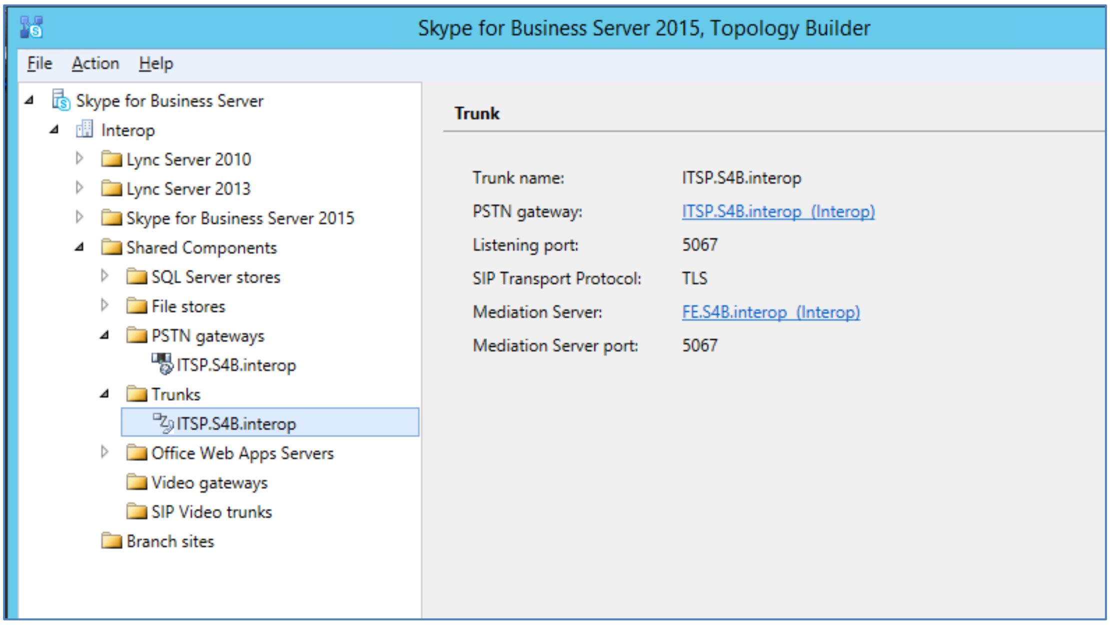
c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.

d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).

e. Click **Finish**.

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

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

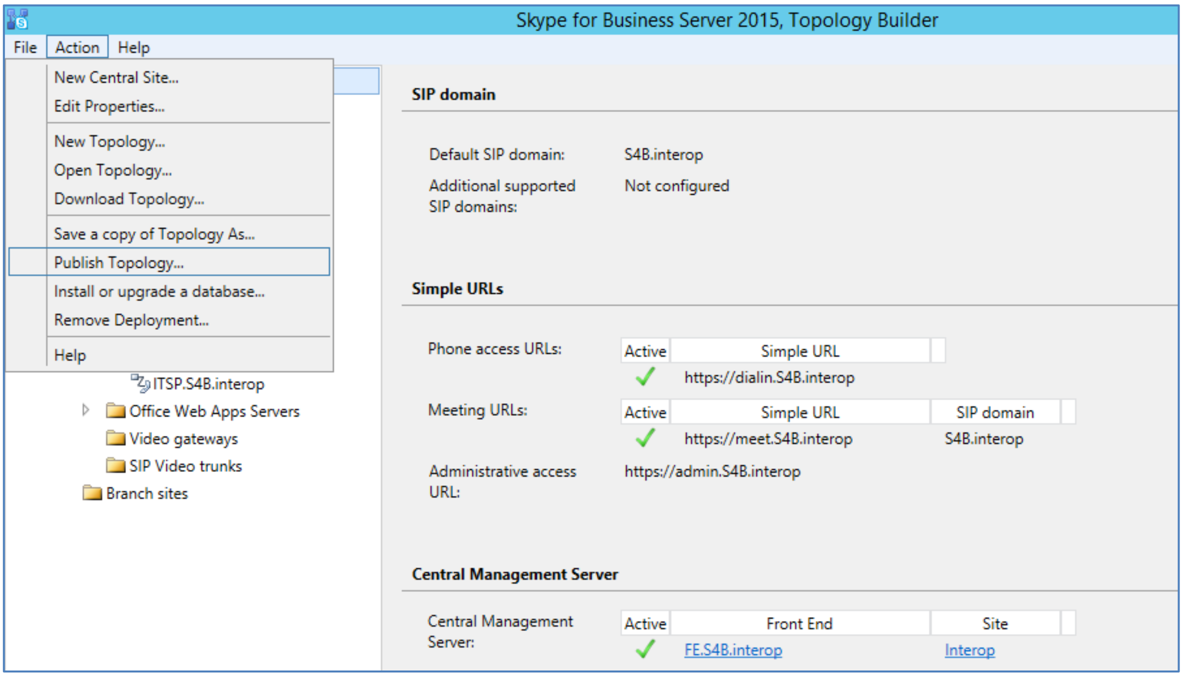


Trunk

Trunk name:	ITSP.S4B.interop
PSTN gateway:	ITSP.S4B.interop (Interop)
Listening port:	5067
SIP Transport Protocol:	TLS
Mediation Server:	FE.S4B.interop (Interop)
Mediation Server port:	5067

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



SIP domain

Default SIP domain:	S4B.interop
Additional supported SIP domains:	Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://dialin.S4B.interop

Meeting URLs:

Active	Simple URL	SIP domain
✓	https://meet.S4B.interop	S4B.interop

Administrative access URL: https://admin.S4B.interop

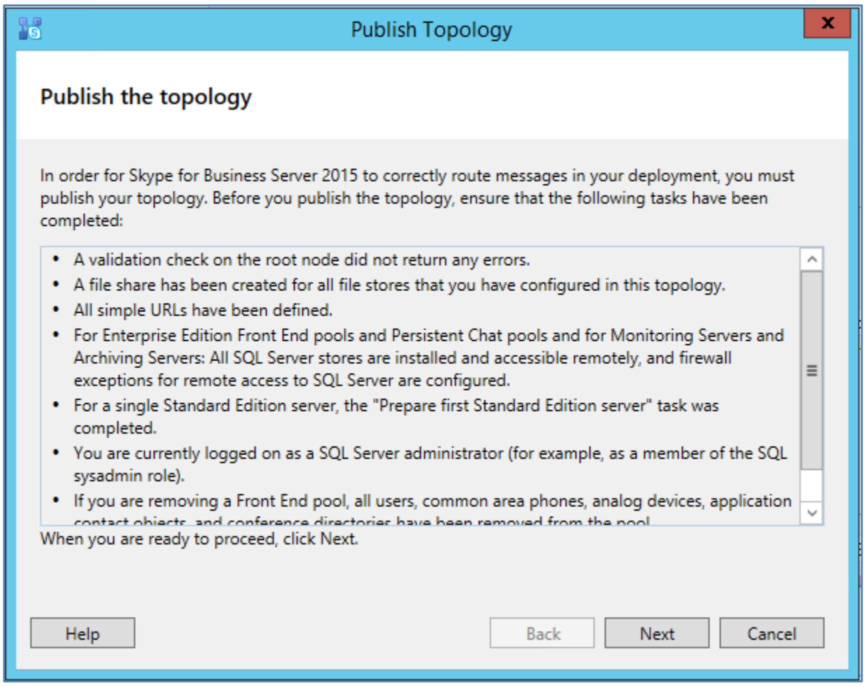
Central Management Server

Central Management Server:

Active	Front End	Site
✓	FE.S4B.interop	Interop

The following is displayed:

Figure 3-11: Publish the Topology



Publish Topology

Publish the topology

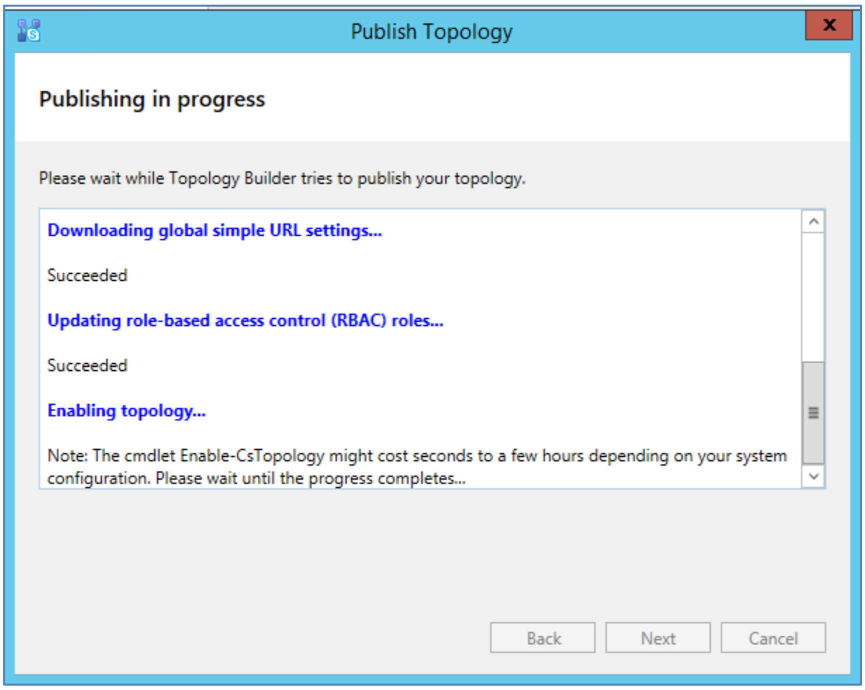
In order for Skype for Business Server 2015 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:

- A validation check on the root node did not return any errors.
- A file share has been created for all file stores that you have configured in this topology.
- All simple URLs have been defined.
- For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured.
- For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.
- You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).
- If you are removing a Front End pool, all users, common area phones, analog devices, application contact objects, and conference directories have been removed from the pool.

When you are ready to proceed, click Next.

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

Figure 3-12: Publishing in Progress



Publish Topology

Publishing in progress

Please wait while Topology Builder tries to publish your topology.

Downloading global simple URL settings...

Succeeded

Updating role-based access control (RBAC) roles...

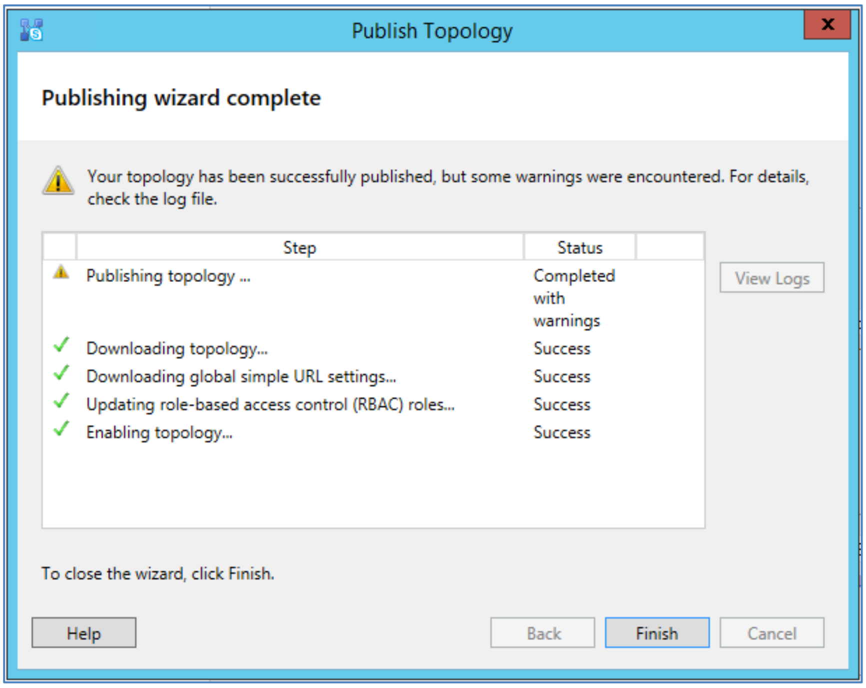
Succeeded

Enabling topology...

Note: The cmdlet Enable-CsTopology might cost seconds to a few hours depending on your system configuration. Please wait until the progress completes...

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

Figure 3-13: Publishing Wizard Complete



Publishing wizard complete

Your topology has been successfully published, but some warnings were encountered. For details, check the log file.

	Step	Status
⚠	Publishing topology ...	Completed with warnings
✓	Downloading topology...	Success
✓	Downloading global simple URL settings...	Success
✓	Updating role-based access control (RBAC) roles...	Success
✓	Enabling topology...	Success

To close the wizard, click Finish.

12. Click **Finish**.

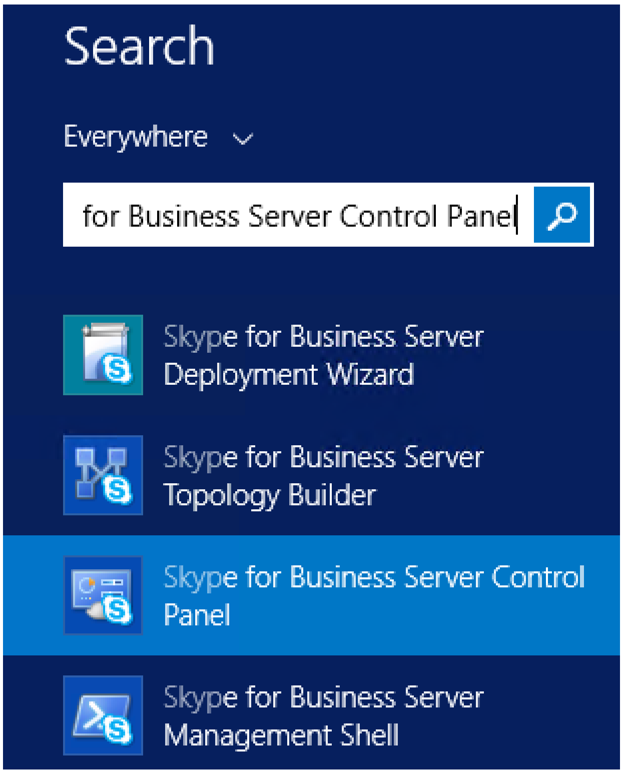
3.2 Configuring the "Route" on Skype for Business Server 2015

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:**

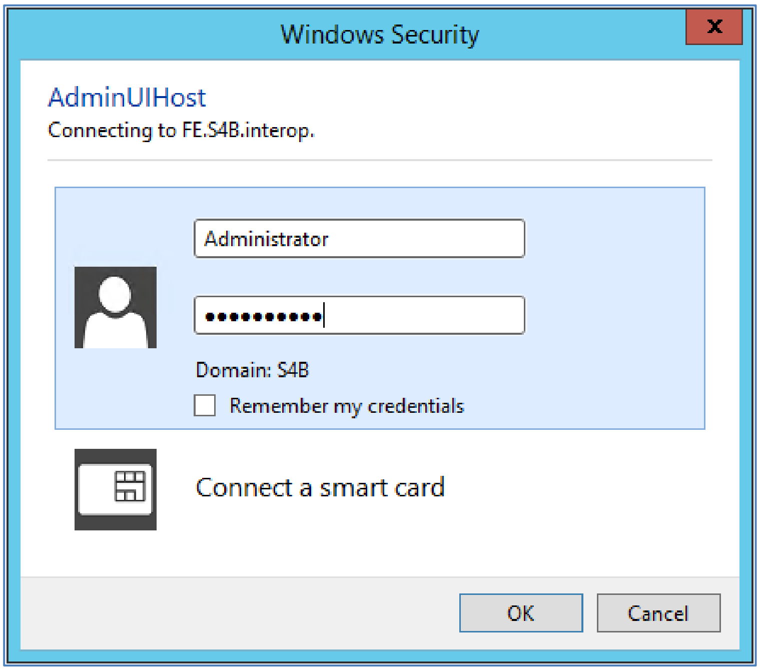
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

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


Search
Everywhere
for Business Server Control Panel
Skype for Business Server Deployment Wizard
Skype for Business Server Topology Builder
Skype for Business Server Control Panel
Skype for Business Server Management Shell

2. You are prompted to enter your login credentials:

Figure 3-15: Skype for Business Server Credentials



Windows Security

AdminUIHost

Connecting to FE.S4B.interop.

Administrator

••••••••••

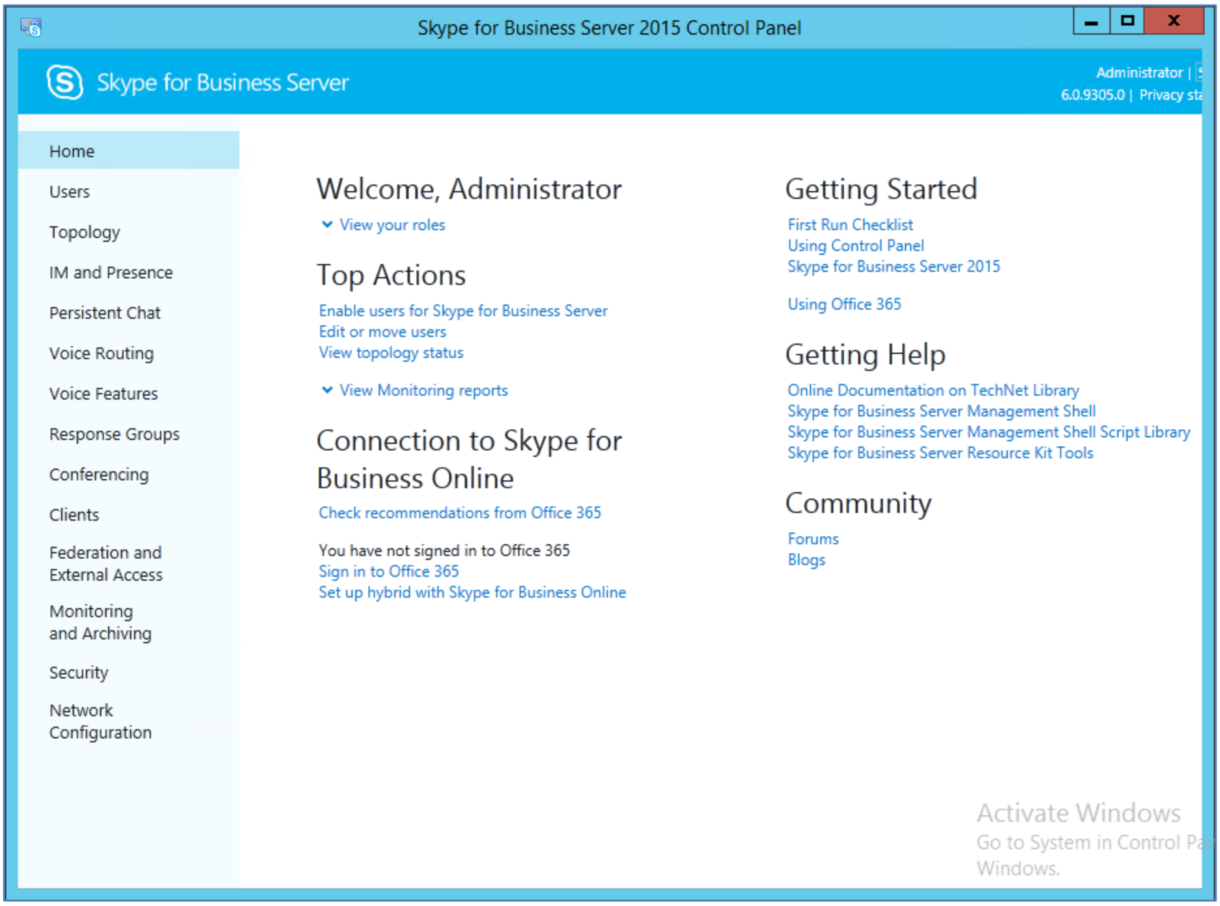
Domain: S4B

☐ Remember my credentials

Connect a smart card

3. 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



Skype for Business Server 2015 Control Panel

Skype for Business Server

Administrator | S
6.0.9305.0 | Privacy sta

Welcome, Administrator

View your roles

Top Actions

Enable users for Skype for Business Server
Edit or move users
View topology status

View Monitoring reports

Connection to Skype for Business Online

Check recommendations from Office 365

You have not signed in to Office 365
Sign in to Office 365
Set up hybrid with Skype for Business Online

Getting Started

First Run Checklist
Using Control Panel
Skype for Business Server 2015

Using Office 365

Getting Help

Online Documentation on TechNet Library
Skype for Business Server Management Shell
Skype for Business Server Management Shell Script Library
Skype for Business Server Resource Kit Tools

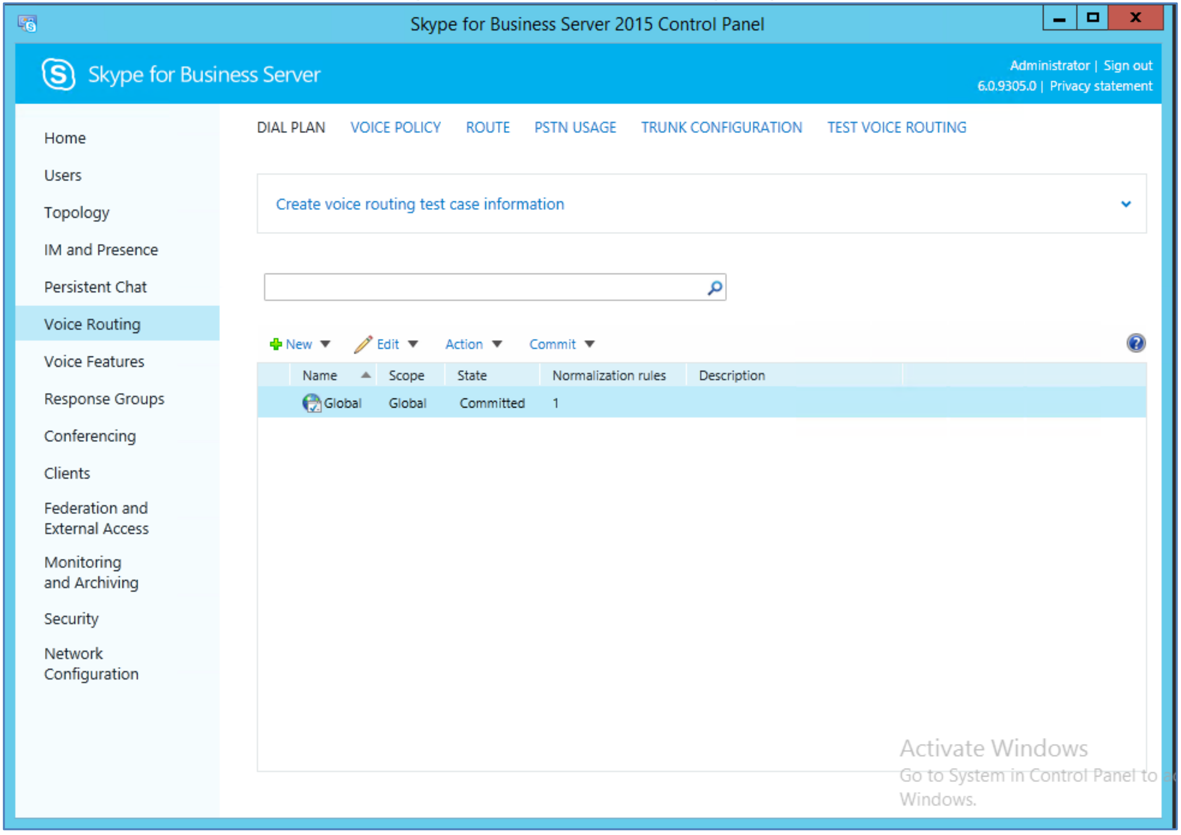
Community

Forums
Blogs

Activate Windows
Go to System in Control Pa
Windows.

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

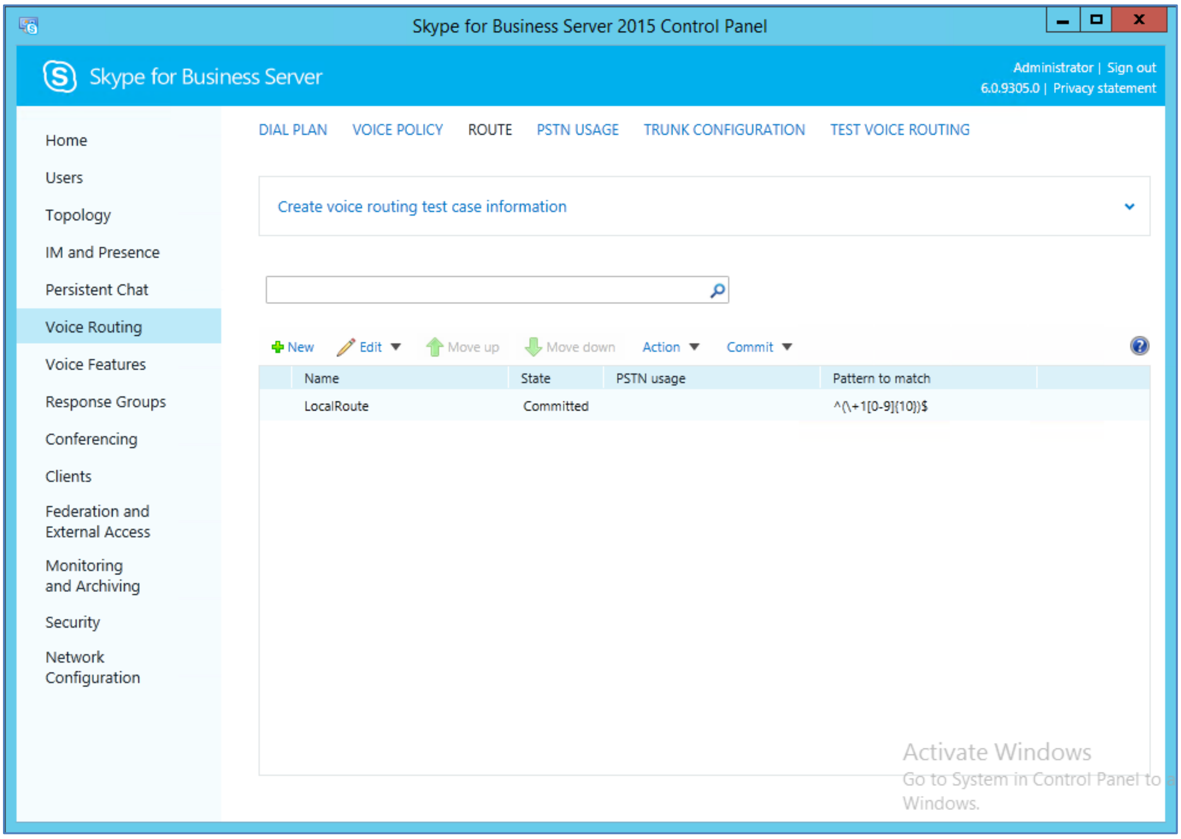
Figure 3-17: Voice Routing Page



Name	Scope	State	Normalization rules	Description
Global	Global	Committed	1	

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

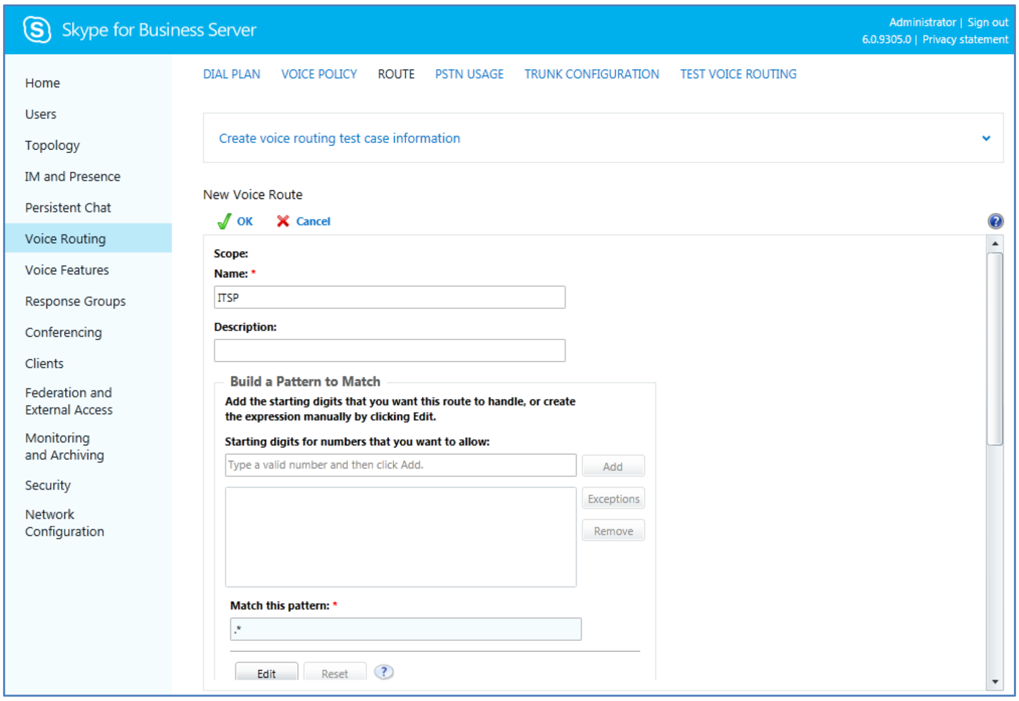
Figure 3-18: Route Tab



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

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

Figure 3-19: Adding New Voice Route



New Voice Route

Scope:

Name: * ITSP

Description:

Build a Pattern to Match

Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.

Starting digits for numbers that you want to allow: Type a valid number and then click Add.

Match this pattern: * .*

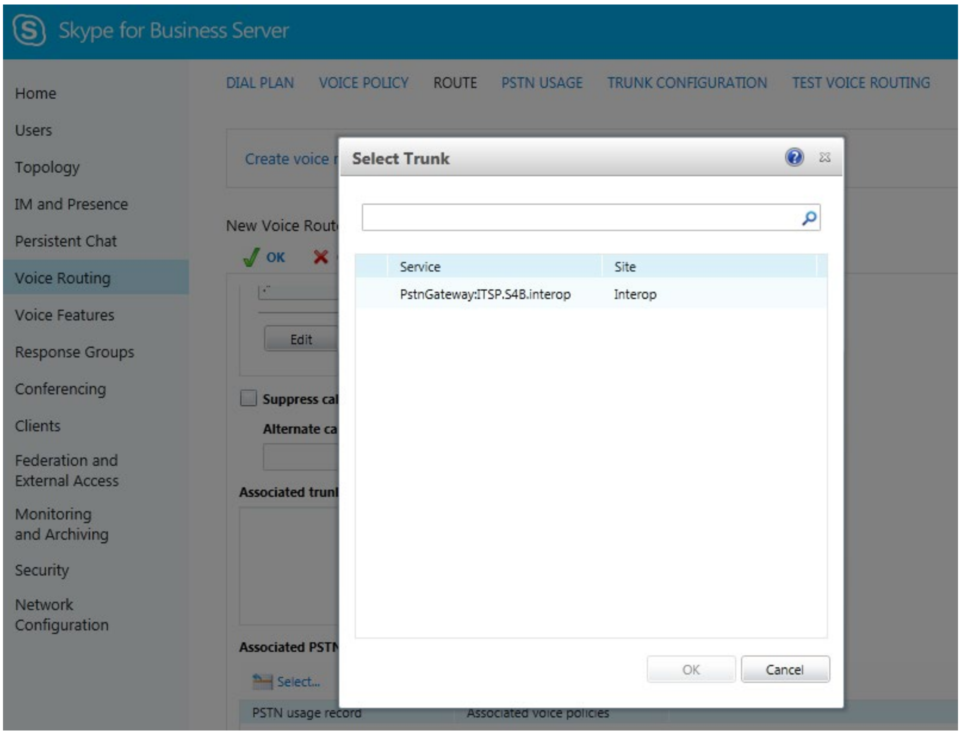
7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).

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

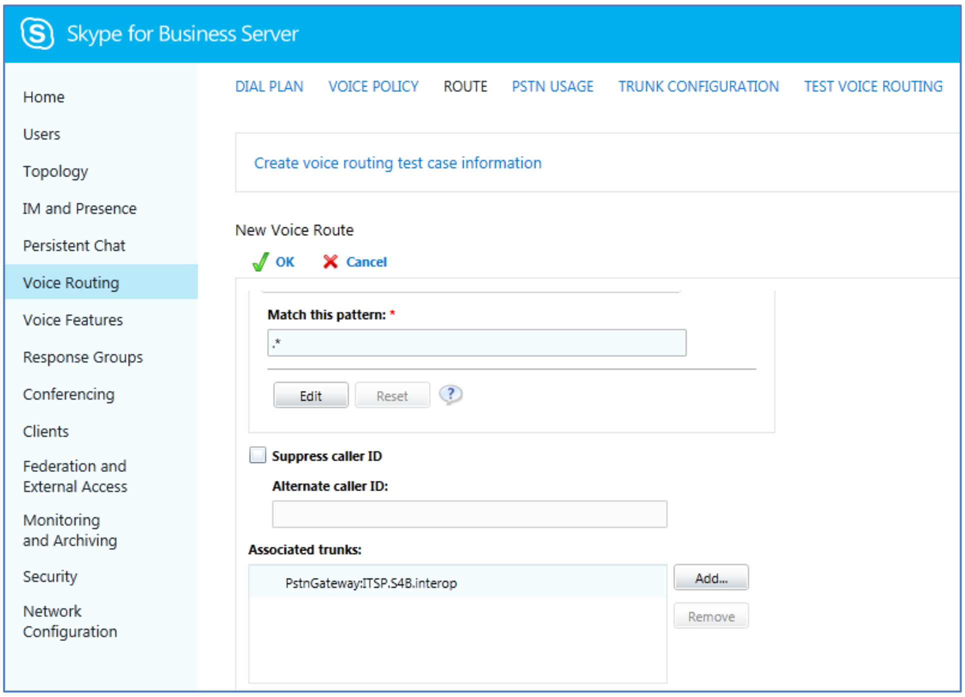


Select Trunk

Service	Site
PstnGateway:ITSP.S4B.interop	Interop

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



New Voice Route

Match this pattern: * .*

□ Suppress caller ID

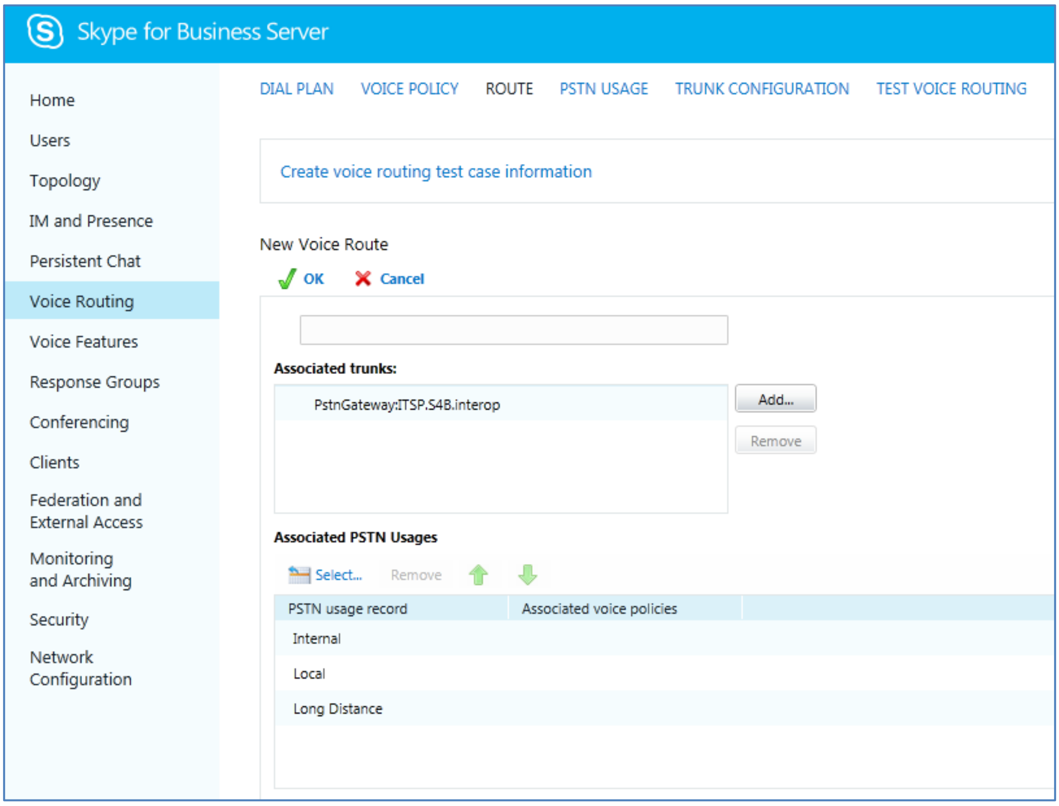
Alternate caller ID:

Associated trunks: PstnGateway:ITSP.S4B.interop

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



New Voice Route

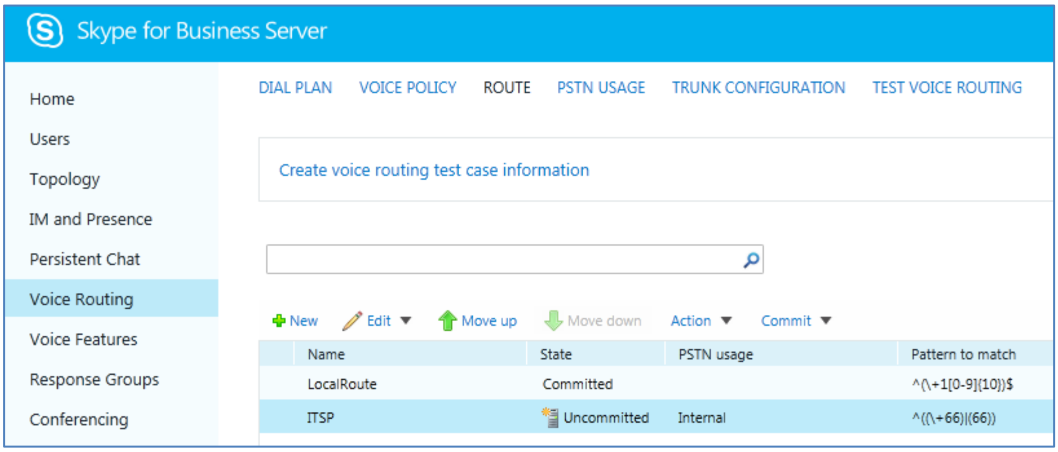
Associated trunks: PstnGateway:ITSP.S4B.interop

Associated PSTN Usages

PSTN usage record	Associated voice policies
Internal	
Local	
Long Distance	

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

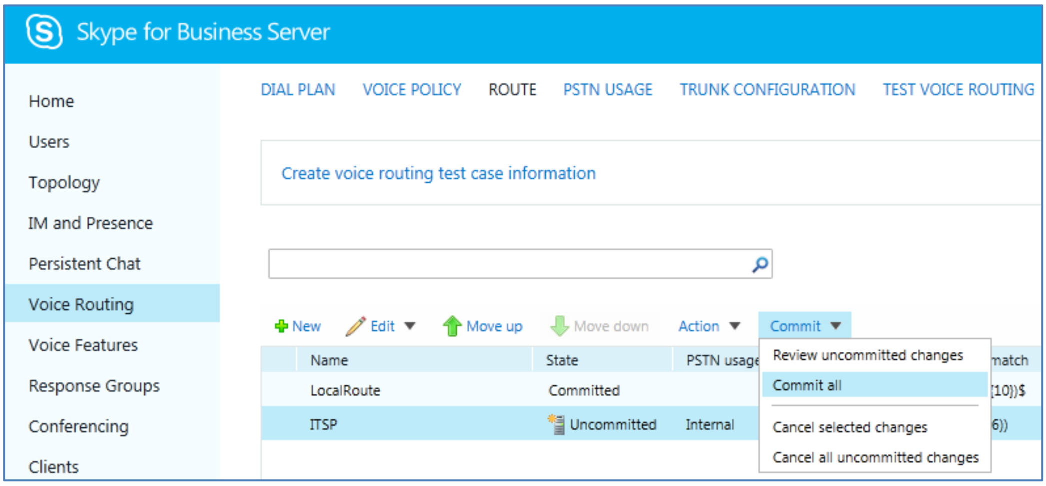
Figure 3-23: Confirmation of New Voice Route



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

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

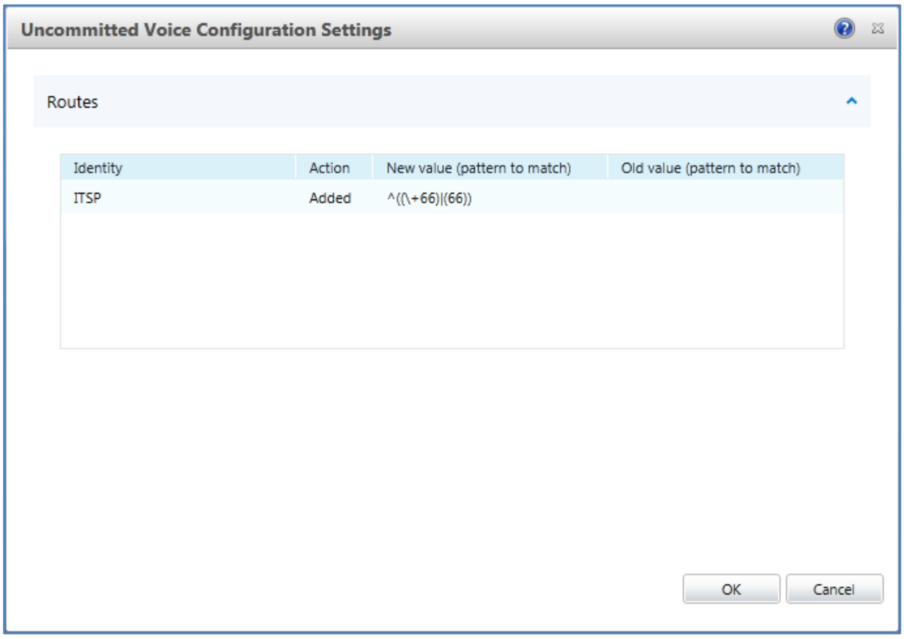
Figure 3-24: Committing Voice Routes



Name	State	PSTN usage	match
LocalRoute	Committed		{10})$
ITSP	Uncommitted	Internal	6))

The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



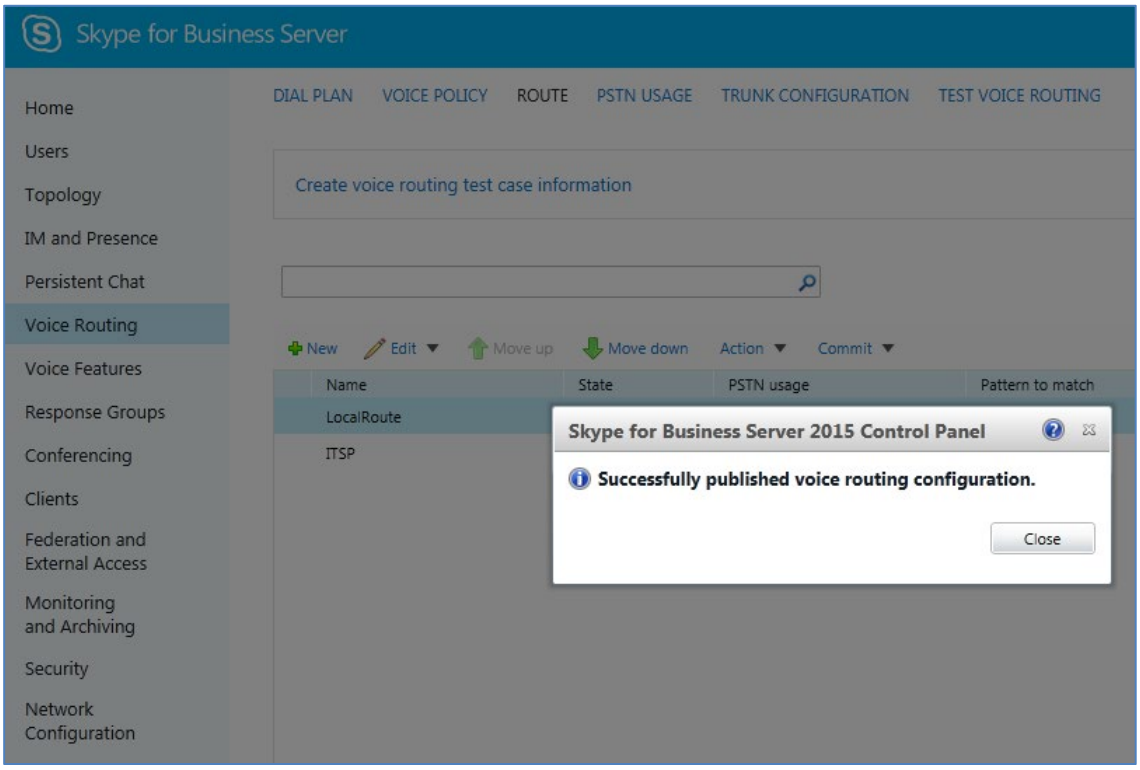
Uncommitted Voice Configuration Settings

Routes

Identity	Action	New value (pattern to match)	Old value (pattern to match)
ITSP	Added	^((\+66)|(66))	

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

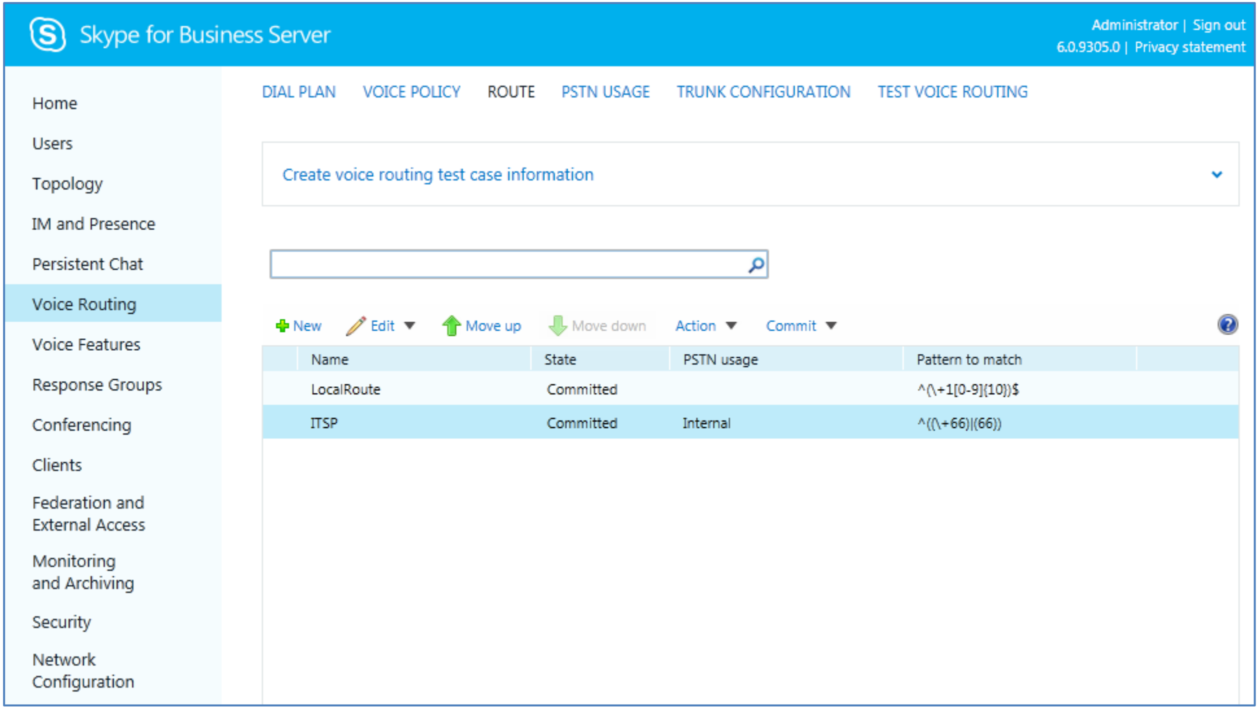


Skype for Business Server 2015 Control Panel

Successfully published 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



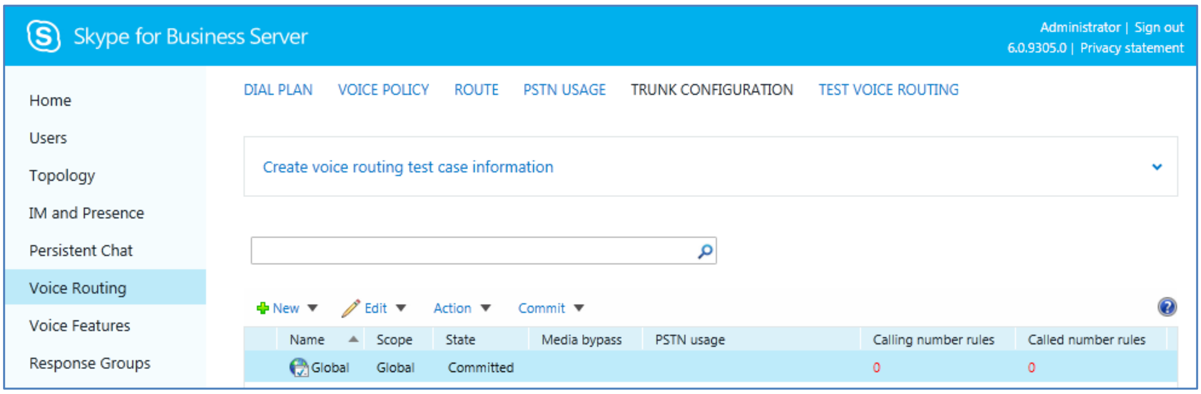
Name	State	PSTN usage	Pattern to match
LocalRoute	Committed		^(\+1[0-9]{10})$
ITSP	Committed	Internal	^((\+66)|(66))

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.

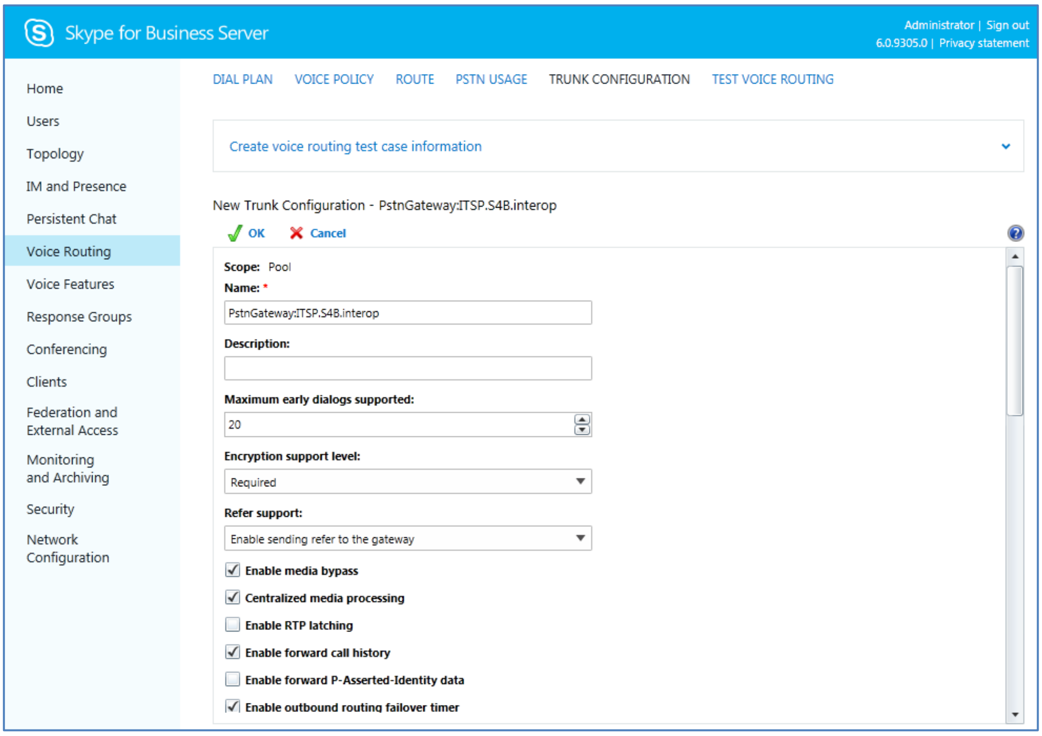
Figure 3-28: Voice Routing Screen – Trunk Configuration Tab



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



New Trunk Configuration - PstnGateway:ITSP.S4B.interop

Scope: Pool

Name: *

PstnGateway:ITSP.S4B.interop

Description:

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**

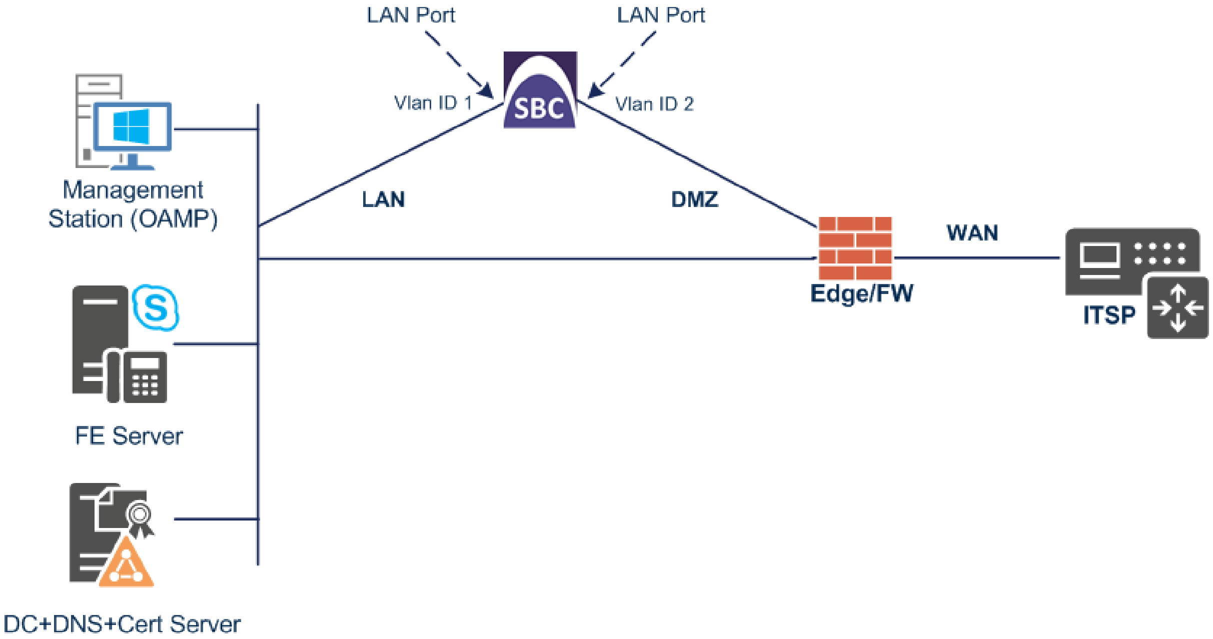
  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should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

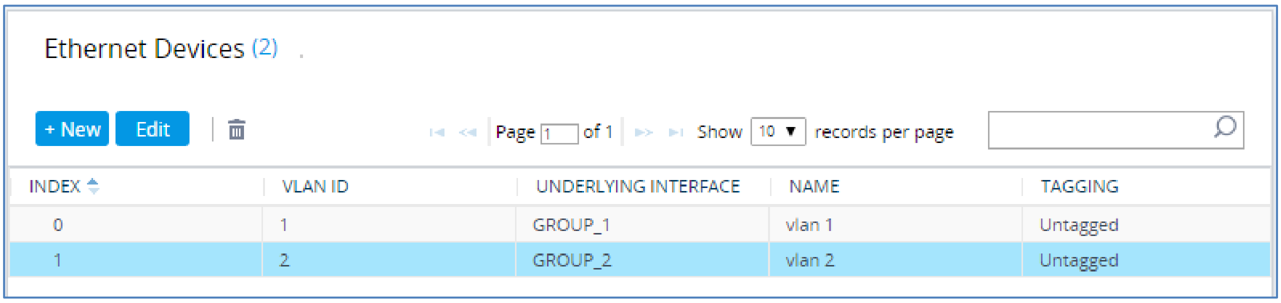
- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **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	**1**
VLAN ID	**2**
Underlying Interface	**GROUP_2** (Ethernet port group)
Name	**vlan 2**
Tagging	**Untagged**

Figure 4-2: Configured VLAN IDs in Ethernet Device



Ethernet Devices (2)

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

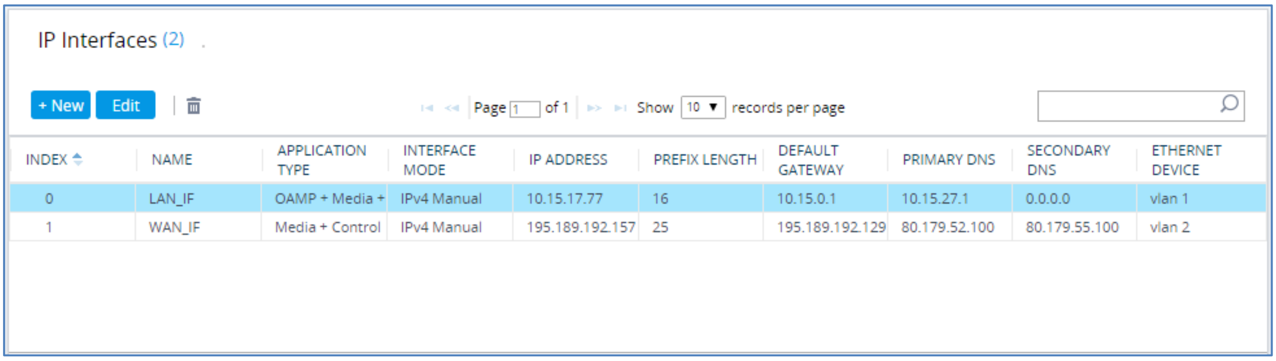
3. Add a network interface for the WAN side:
   a. Click **New**.
   b. Configure the interface as follows:

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

4. Click **Apply**.

The configured IP network interfaces are shown below:

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



IP Interfaces (2)

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

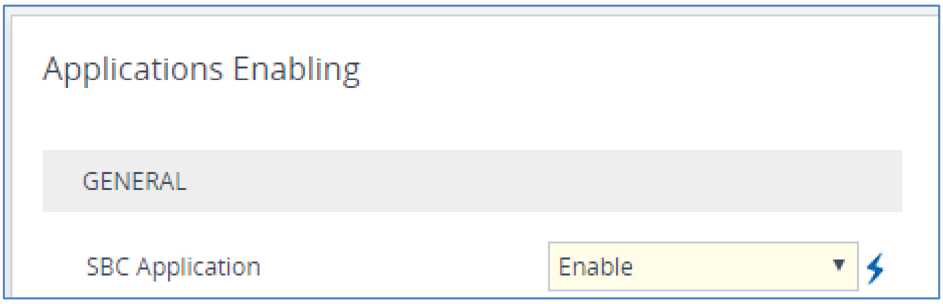
4.2 Step 2: Enable the SBC Application

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



Applications Enabling

GENERAL

SBC Application: Enable

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

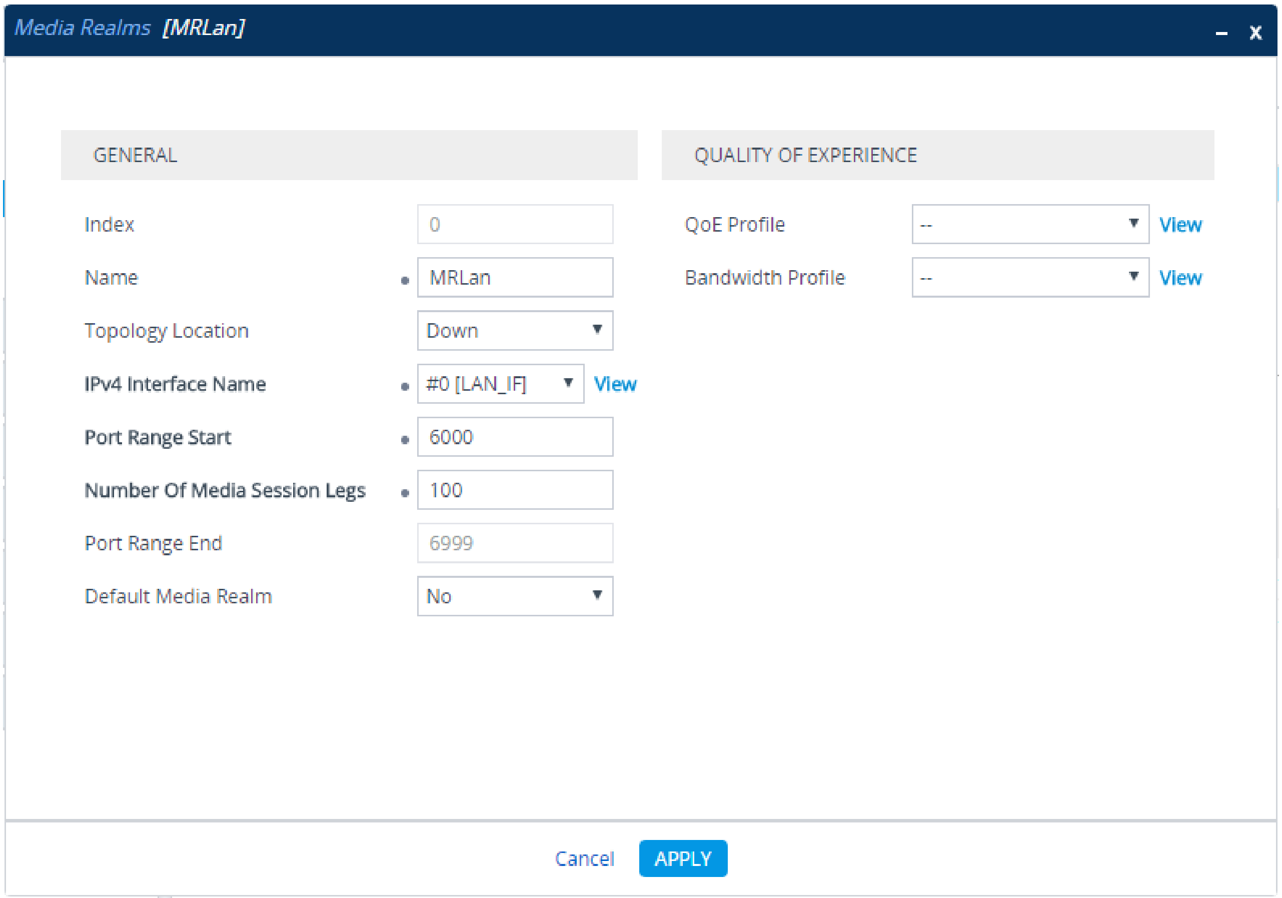
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **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	**0**
Name	**MRLan** (descriptive name)
IPv4 Interface Name	**LAN_IF**
Port Range Start	**6000** (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-5: Configuring Media Realm for LAN



Media Realms *[MRLan]*

GENERAL

Index	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

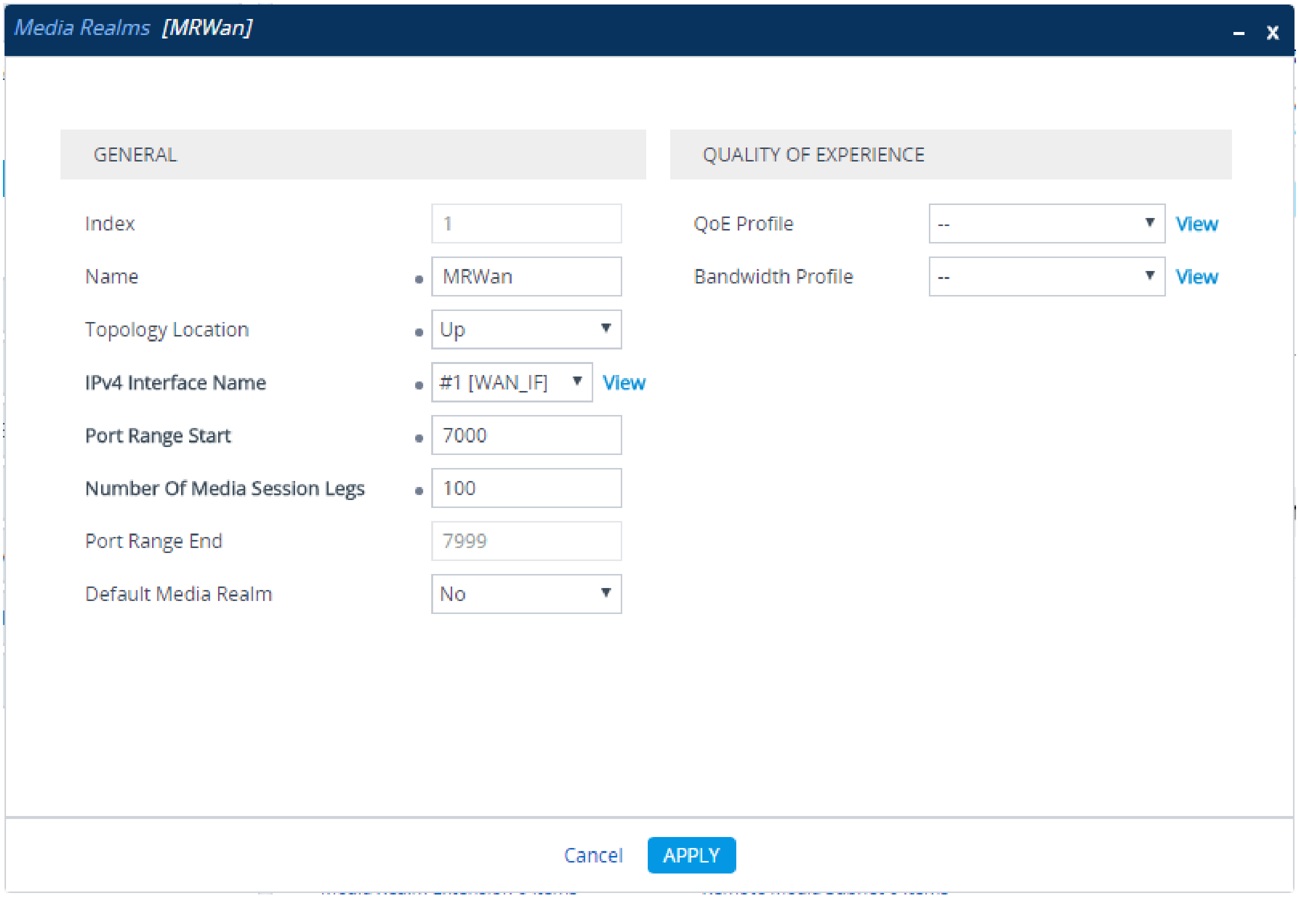
QUALITY OF EXPERIENCE

QoE Profile	--
Bandwidth Profile	--

3. Configure a Media Realm for WAN traffic:

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

Figure 4-6: Configuring Media Realm for WAN



Media Realms [MRWan]

GENERAL

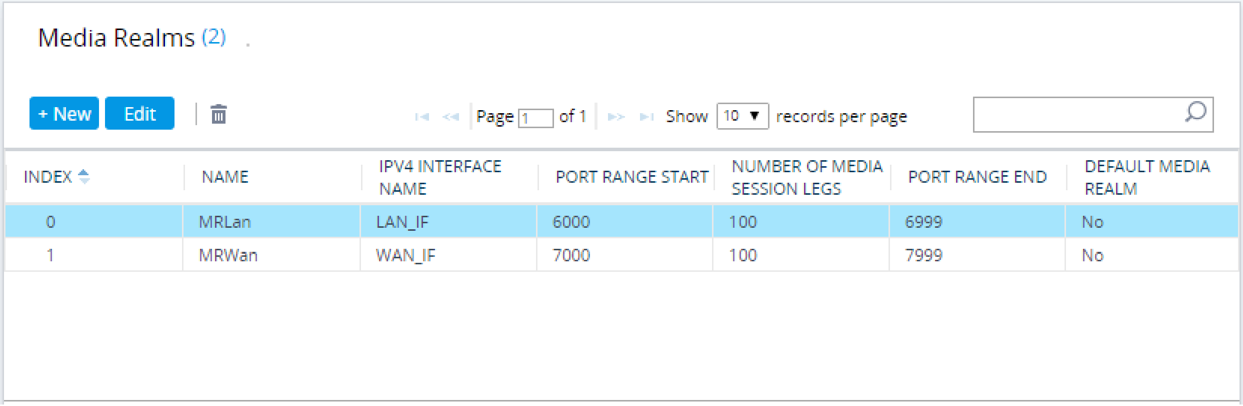
Index	1
Name	MRWan
Topology Location	Up
IPv4 Interface Name	#1 [WAN_IF]
Port Range Start	7000
Number Of Media Session Legs	100
Port Range End	7999
Default Media Realm	No

QUALITY OF EXPERIENCE

QoE Profile	--
Bandwidth Profile	--

The configured Media Realms are shown in the figure below:

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



Media Realms (2)

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

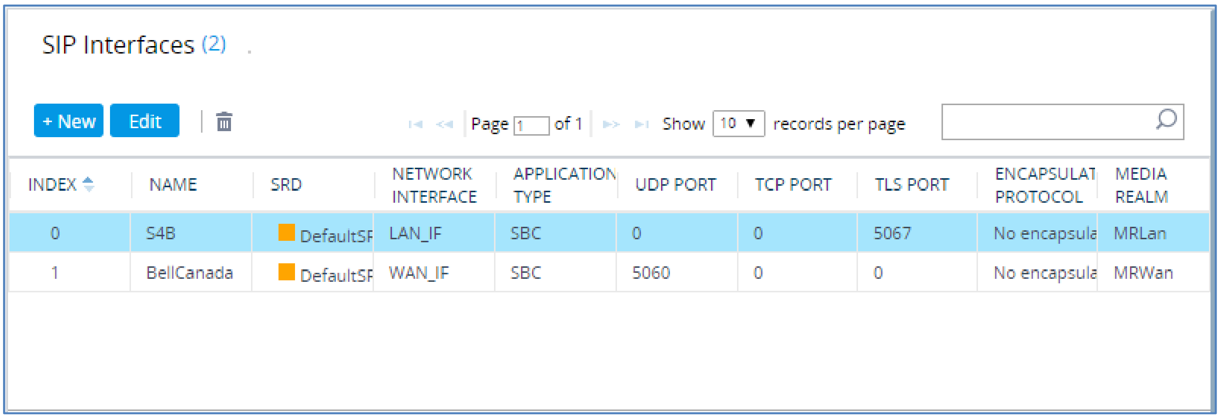
Note: The TLS port parameter must be identically configured in the Skype for Business Topology Builder (see Section 3.1 on page 13).

3. Configure a SIP Interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

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



INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULAT 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

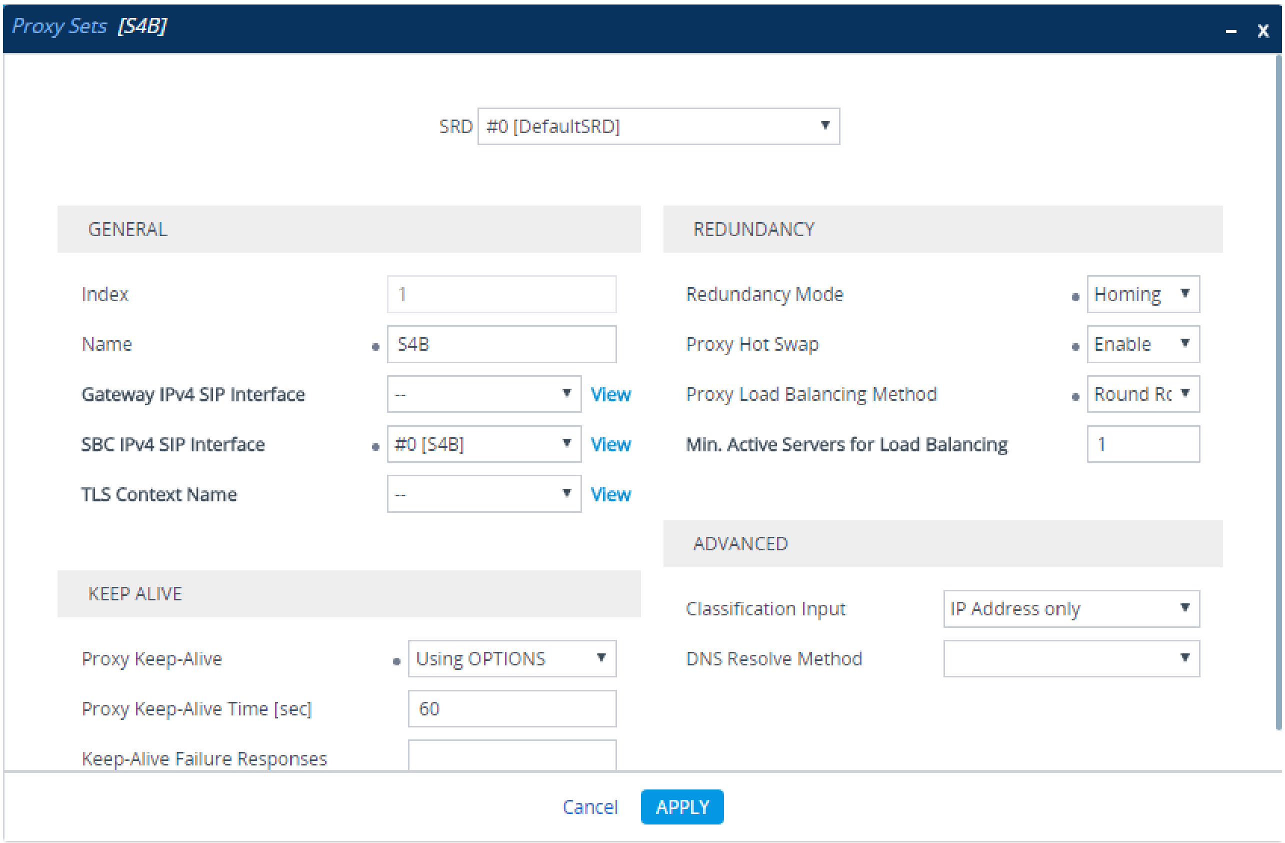
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

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

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



Proxy Sets [S4B]

SRD: #0 [DefaultSRD]

GENERAL

Index	1
Name	S4B
Gateway IPv4 SIP Interface	--
SBC IPv4 SIP Interface	#0 [S4B]
TLS Context Name	--

KEEP ALIVE

Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Keep-Alive Failure Responses	

REDUNDANCY

Redundancy Mode	Homing
Proxy Hot Swap	Enable
Proxy Load Balancing Method	Round Rc
Min. Active Servers for Load Balancing	1

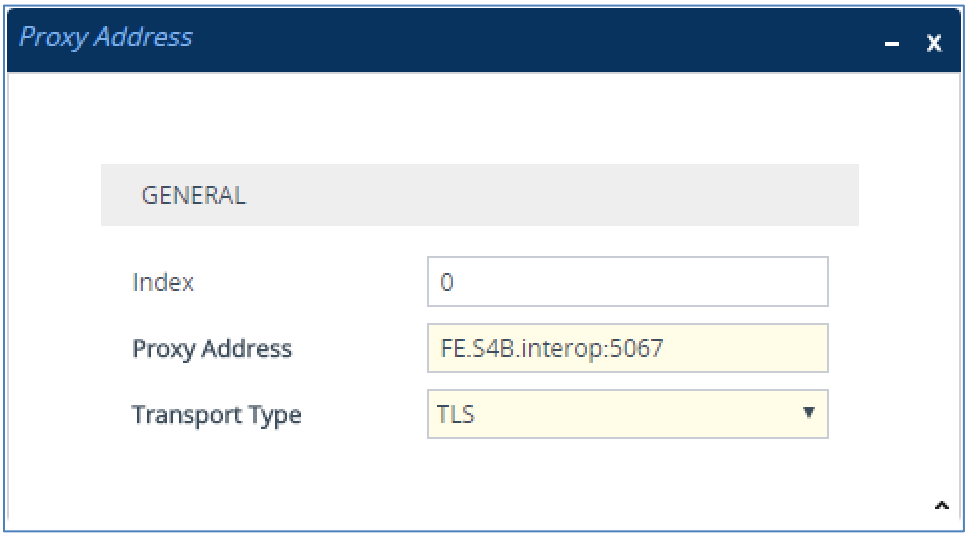
ADVANCED

Classification Input	IP Address only
DNS Resolve Method	

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



Proxy Address

GENERAL

Index	0
Proxy Address	FE.S4B.interop:5067
Transport Type	TLS

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

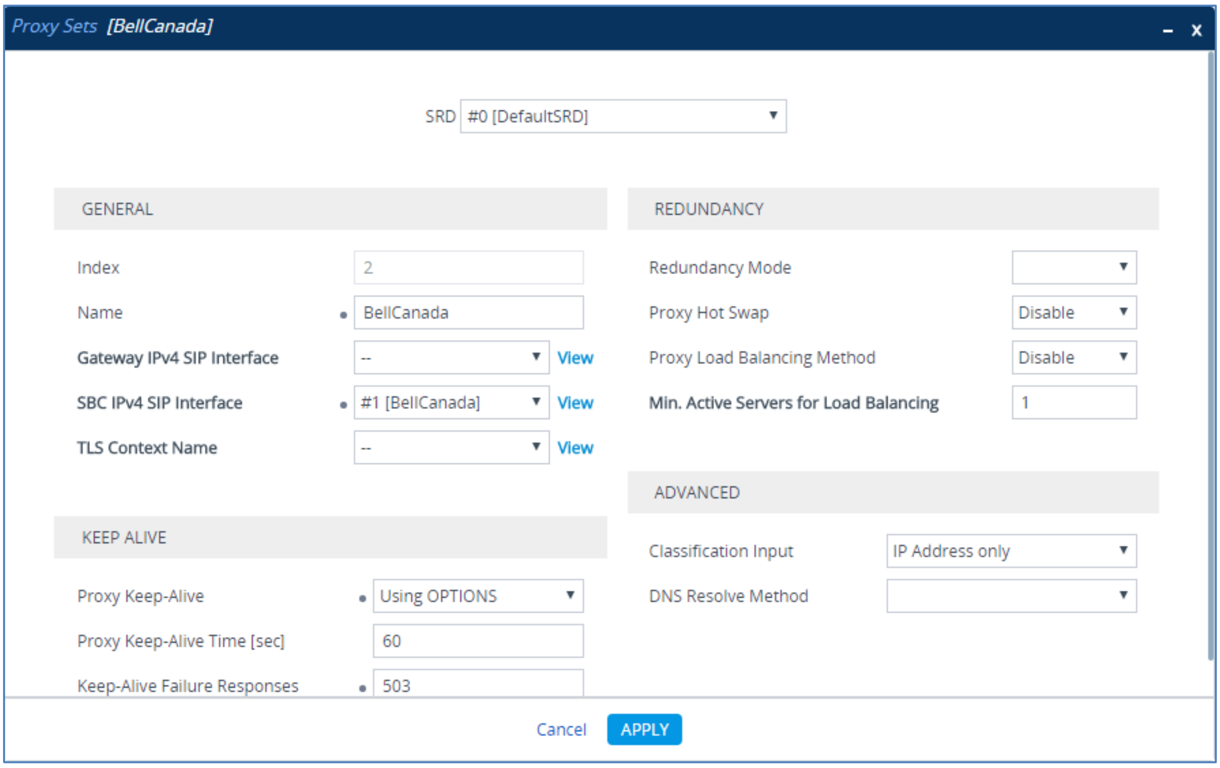
d. Click **Apply**.

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

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

Parameter	Value
Index	**2**
Name	**BellCanada**
SBC IPv4 SIP Interface	**BellCanada**
Proxy Keep-Alive	**Using Options**
Keep-Alive Failure Responses	**503**

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



Proxy Sets [BellCanada]

SRD: #0 [DefaultSRD]

GENERAL

Index: 2

Name: BellCanada

Gateway IPv4 SIP Interface: --

SBC IPv4 SIP Interface: #1 [BellCanada]

TLS Context Name: --

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Responses: 503

REDUNDANCY

Redundancy Mode:

Proxy Hot Swap: Disable

Proxy Load Balancing Method: Disable

Min. Active Servers for Load Balancing: 1

ADVANCED

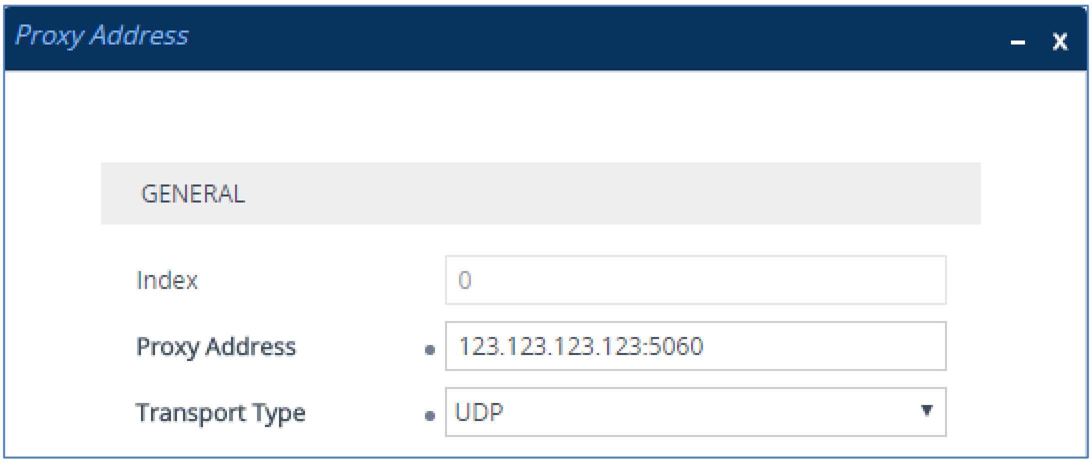
Classification Input: IP Address only

DNS Resolve Method:

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



Proxy Address

GENERAL

Index	0
Proxy Address ●	123.123.123.123:5060
Transport Type ●	UDP

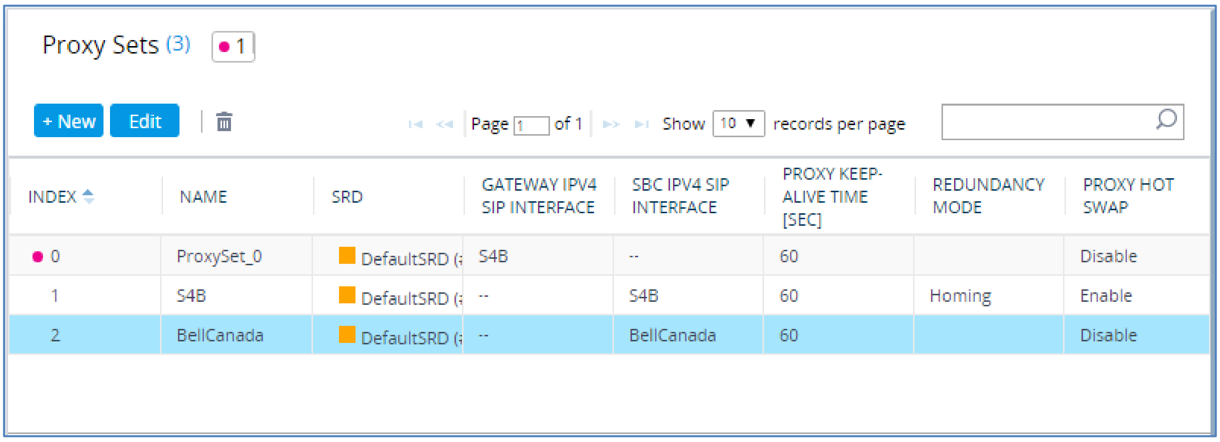
c. Configure the address of the Proxy Set according to the parameters described in the table below.

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

d. Click **Apply**.

The configured Proxy Sets are shown in the figure below:

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



Proxy Sets (3) ● 1

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.

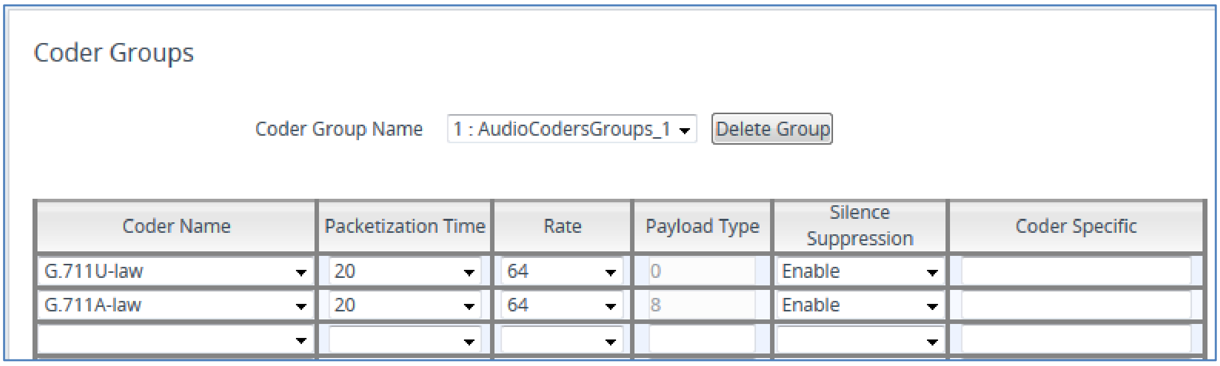
Note that the Coder Group ID for this entity will be assign to its corresponding IP Profile in the next step.

➢ **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	**AudioCodersGroups_1**
Coder Name	▪ **G.711 U-law** ▪ **G.711 A-law**
Silence Suppression	**Enable** (for both coders)

Figure 4-14: Configuring Coder Group for Skype for Business Server 2015



Coder Groups

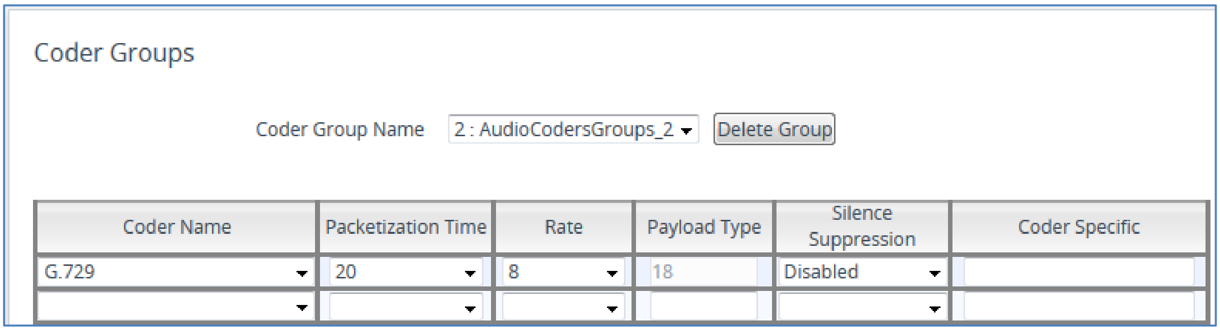
Coder Group Name: 1 : AudioCodersGroups_1

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	**AudioCodersGroups_2**
Coder Name	**G.729**

Figure 4-15: Configuring Coder Group for Bell Canada SIP Trunk



Coder Groups

Coder Group Name: 2 : AudioCodersGroups_2

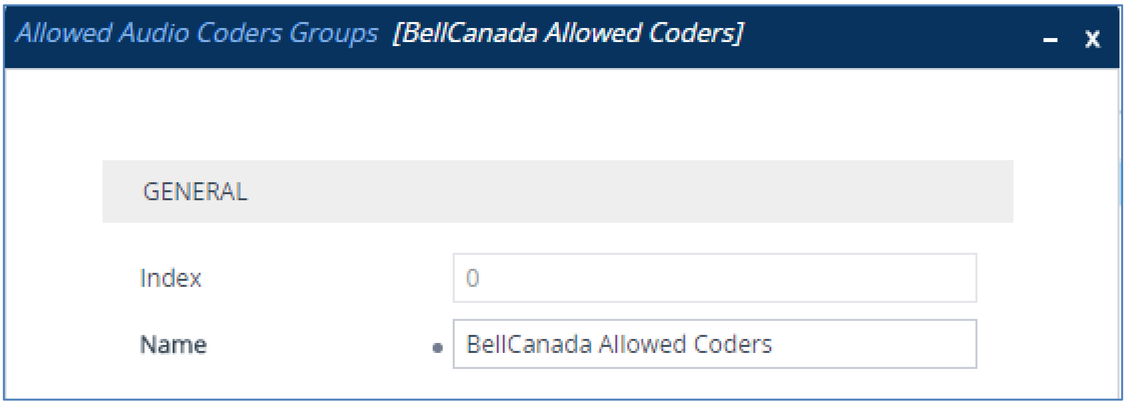
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.729	20	8	18	Disabled	

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



Allowed Audio Coders Groups [BellCanada Allowed Coders]

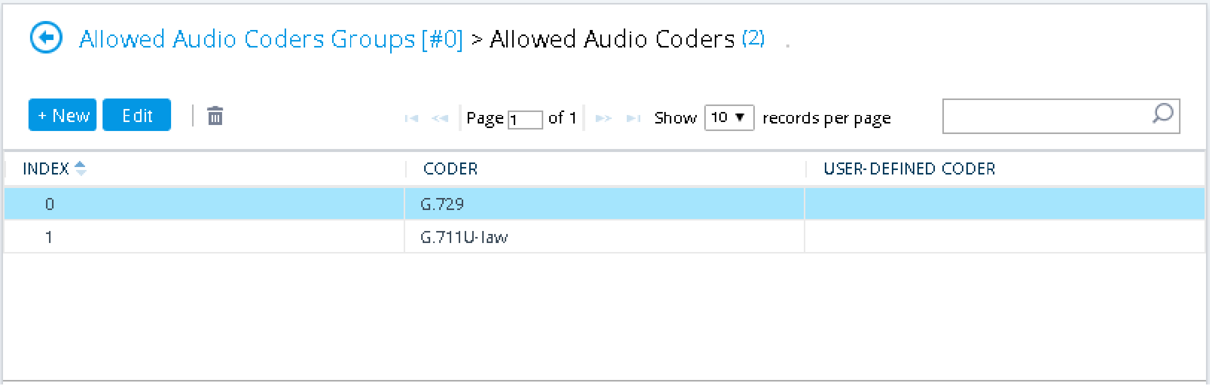
GENERAL

Index	0
Name ●	BellCanada Allowed Coders

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	**G.729**
Coder	**G.711 U-law**

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

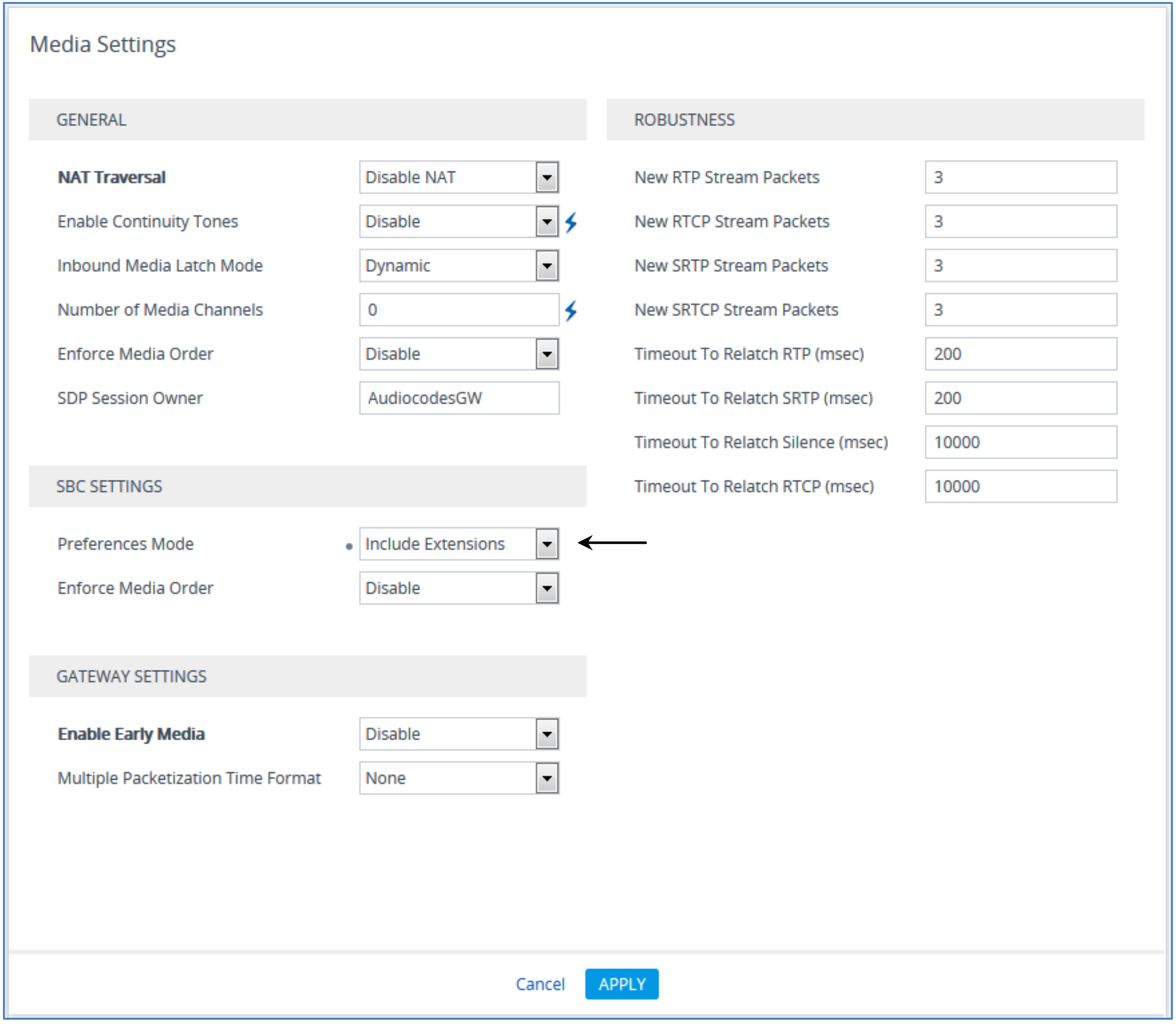


Allowed Audio Coders Groups [#0] > Allowed Audio Coders (2)

INDEX	CODER	USER-DEFINED CODER
0	G.729	
1	G.711U-law	

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

Figure 4-18: SBC Preferences Mode



Media Settings

GENERAL

NAT Traversal	Disable NAT
Enable Continuity Tones	Disable
Inbound Media Latch Mode	Dynamic
Number of Media Channels	0
Enforce Media Order	Disable
SDP Session Owner	AudiocodesGW

ROBUSTNESS

New RTP Stream Packets	3
New RTCP Stream Packets	3
New SRTP Stream Packets	3
New SRTCP Stream Packets	3
Timeout To Relatch RTP (msec)	200
Timeout To Relatch SRTP (msec)	200
Timeout To Relatch Silence (msec)	10000
Timeout To Relatch RTCP (msec)	10000

SBC SETTINGS

Preferences Mode	Include Extensions
Enforce Media Order	Disable

GATEWAY SETTINGS

Enable Early Media	Disable
Multiple Packetization Time Format	None

7. From the '**Preferences Mode**' drop-down list, select **Include Extensions**.
8. 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

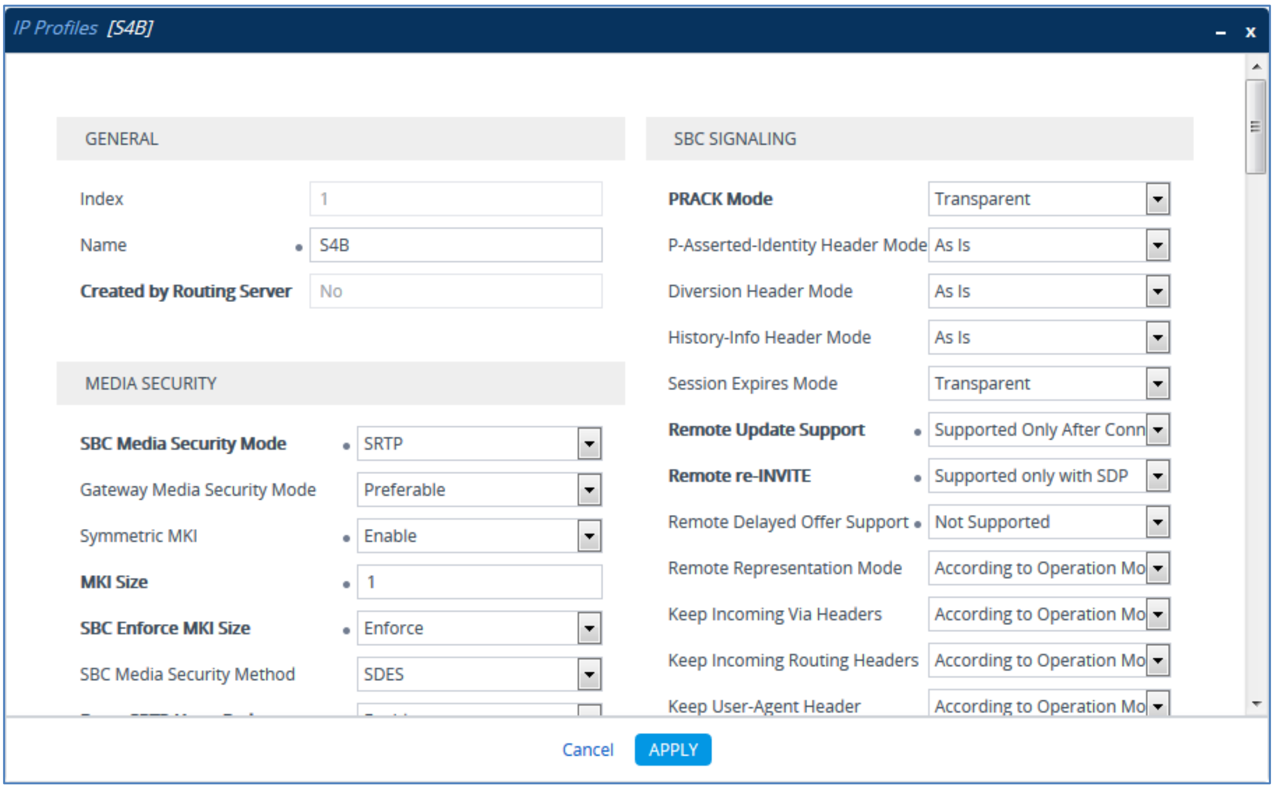
➢ **To configure IP Profile for the Skype for Business Server 2015:**

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

Remote 3xx Mode	**Handle Locally** (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)
SBC Hold	
Remote Hold Format	**Inactive** (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



IP Profiles [S4B]

GENERAL

Index	1
Name •	S4B
Created by Routing Server	No

MEDIA SECURITY

SBC Media Security Mode •	SRTP
Gateway Media Security Mode	Preferable
Symmetric MKI •	Enable
MKI Size •	1
SBC Enforce MKI Size •	Enforce
SBC Media Security Method	SDES

SBC SIGNALING

PRACK Mode	Transparent
P-Asserted-Identity Header Mode	As Is
Diversion Header Mode	As Is
History-Info Header Mode	As Is
Session Expires Mode	Transparent
Remote Update Support •	Supported Only After Conn
Remote re-INVITE •	Supported only with SDP
Remote Delayed Offer Support •	Not Supported
Remote Representation Mode	According to Operation Mo
Keep Incoming Via Headers	According to Operation Mo
Keep Incoming Routing Headers	According to Operation Mo
Keep User-Agent Header	According to Operation Mo

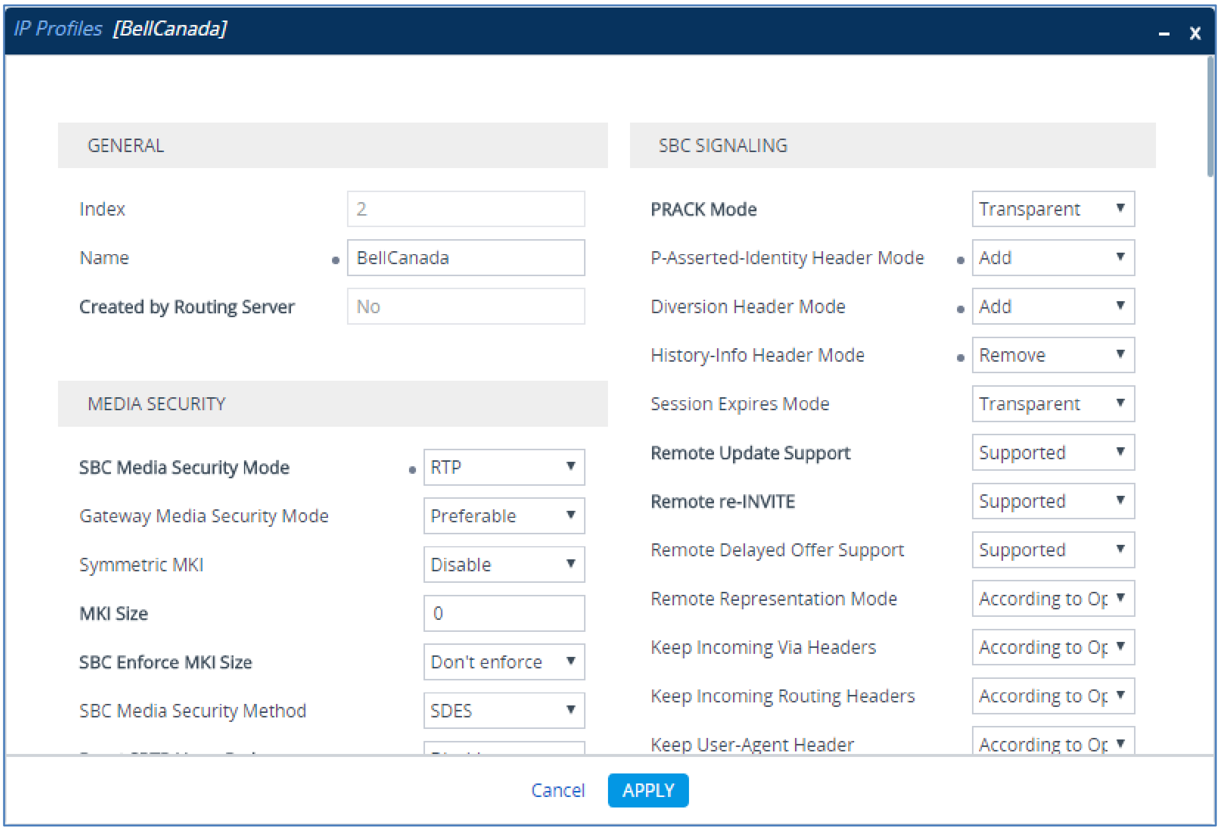
3. Click **Apply**.

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

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

Parameter	Value
General	
Index	**2**
Name	**BellCanada**
Media Security	
SBC Media Security Mode	**RTP**
SBC Media	
Mediation Mode	**Force Transcoding** (required for workaround issue, when a Skype for Business user mutes a call and the SBC needs to send RTP packets in order to prevent dropping the call from the Bell Canada SIP Trunk).
Extension Coders Group	**AudioCodersGroups_2**
Allowed Audio Coders	**BellCanada Allowed Coders**
Allowed Coders Mode	**Restriction and Preference** (lists Allowed Coders first and then original coders in received SDP offer)
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Diversion Header Mode	**Add** (required for transferred calls)
History-Info Header Mode	**Remove**
Session Expires Mode	**Not Supported**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally** (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	**Yes**

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



IP Profiles [BellCanada]

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 Op
Keep Incoming Via Headers	According to Op
Keep Incoming Routing Headers	According to Op
Keep User-Agent Header	According to Op

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:

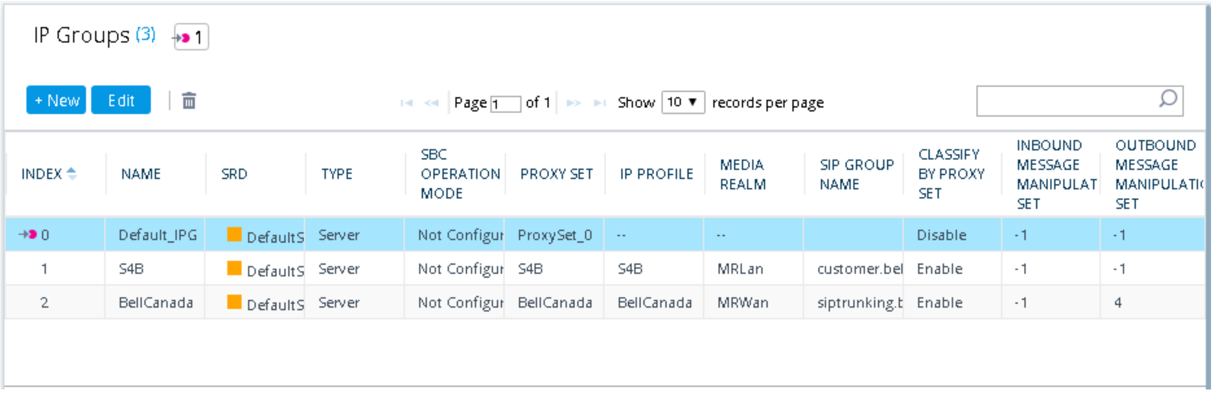
Parameter	Value
Index	**1**
Name	**S4B**
Type	**Server**
Proxy Set	**S4B**
IP Profile	**S4B**
Media Realm	**MRLan**
SIP Group Name	**customer.bell.ca** (according to ITSP requirement)

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

Parameter	Value
Index	**2**
Name	**BellCanada**
Topology Location	**Up**
Type	**Server**
Proxy Set	**BellCanada**
IP Profile	**BellCanada**
Media Realm	**MRWan**
SIP Group Name	**siptrunking.bell.ca** (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 MANIPULAT SET	OUTBOUND MESSAGE MANIPULATI SET
0	Default_IPG	🟧 DefaultS	Server	Not Configur	ProxySet_0	--	--		Disable	-1	-1
1	S4B	🟧 DefaultS	Server	Not Configur	S4B	S4B	MRLan	customer.bel	Enable	-1	-1
2	BellCanada	🟧 DefaultS	Server	Not Configur	BellCanada	BellCanada	MRWan	siptrunking.b	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.

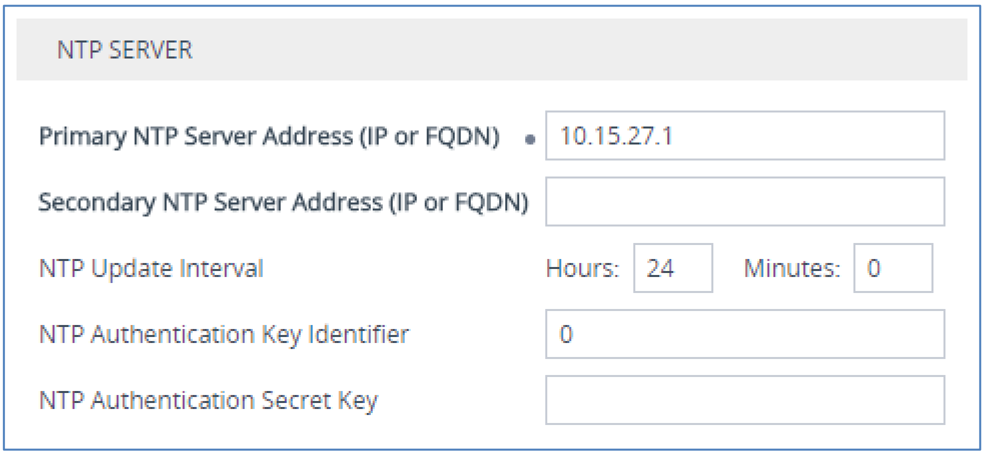
4.9.1 Step 9a: Configure the NTP Server Address

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) •	10.15.27.1
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

3. Click **Apply**.

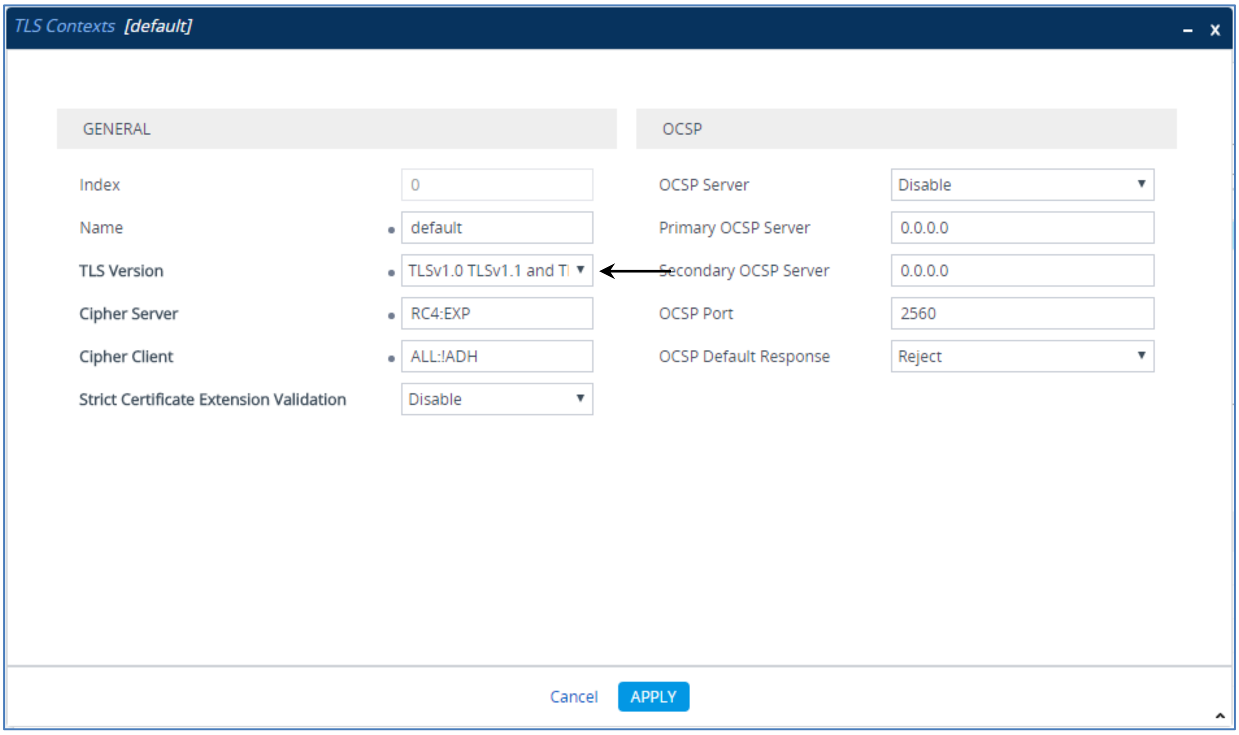
4.9.2 Step 9b: Configure the TLS version

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



TLS Contexts ***[default]***

GENERAL

Index: 0

Name: default

TLS Version: TLSv1.0 TLSv1.1 and Tl

Cipher Server: RC4:EXP

Cipher Client: ALL:!ADH

Strict Certificate Extension Validation: Disable

OCSP

OCSP Server: Disable

Primary OCSP Server: 0.0.0.0

Secondary OCSP Server: 0.0.0.0

OCSP Port: 2560

OCSP Default Response: Reject

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.

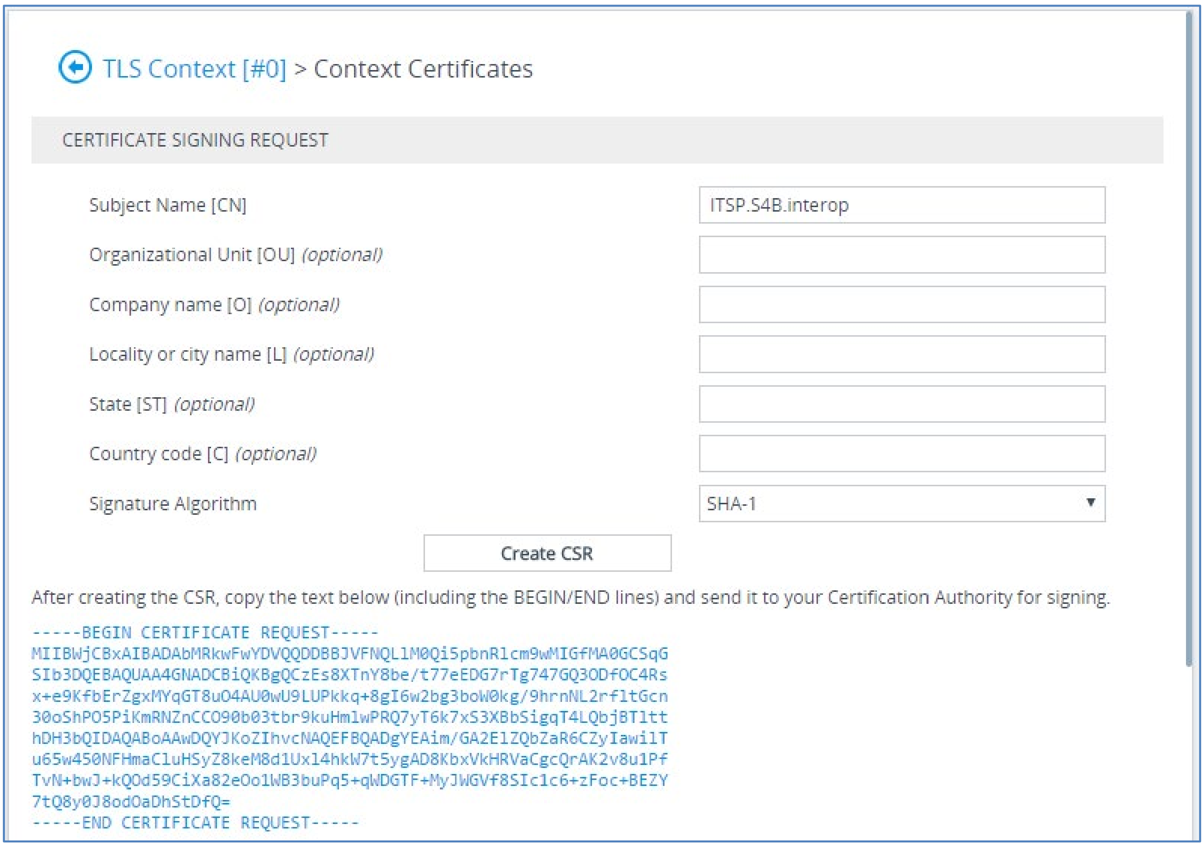
d. Deploying Device and Trusted Root Certificates on E-SBC.

> **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

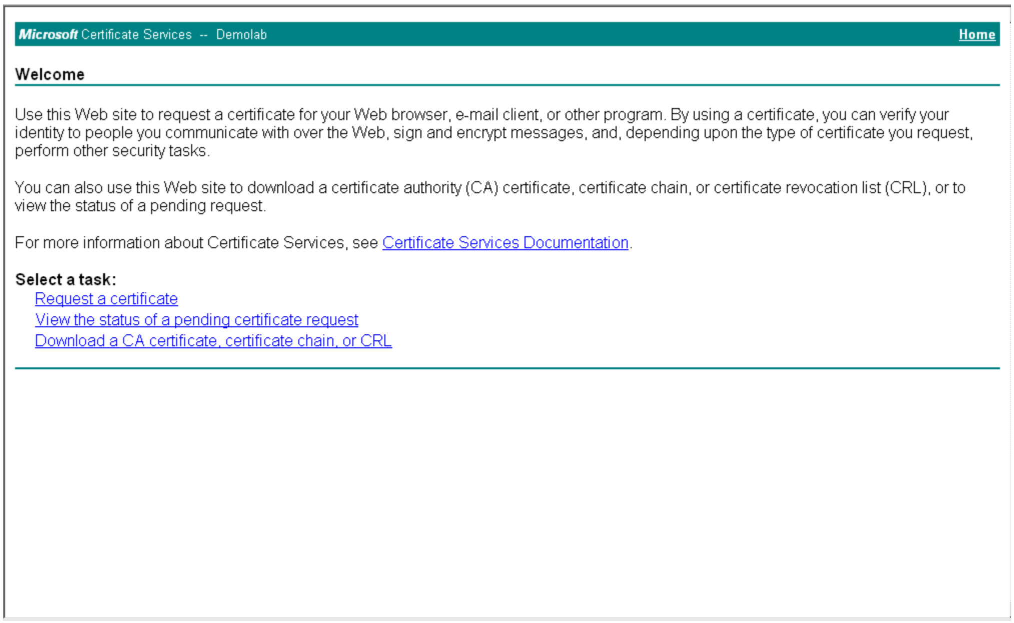
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAIBADAbMRkwFwYDVQQDDBBJVFNQL1M0Qi5pbnRlcm9wMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCzEs8XTnY8be/t77eEDG7rTg747GQ3ODfOC4Rs
x+e9KfbErZgxMYqGT8uO4AU0wU9LUPkkq+8gI6w2bg3boW0kg/9hrnNL2rfltGcn
30oShPO5PiKmRNZnCCO90b03tbr9kuHmlwPRQ7yT6k7xS3XBbSigqT4LQbjBTltt
hDH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAim/GA2ElZQbZaR6CZyIawilT
u65w450NFHmaCluHSyZ8keM8d1Uxl4hkW7t5ygAD8KbxVkHRVaCgcQrAK2v8u1Pf
TvN+bwJ+kQOd59CiXa82eOo1WB3buPq5+qWDGTF+MyJWGVf8SIc1c6+zFoc+BEZY
7tQ8y0J8odOaDhStDfQ=
-----END CERTIFICATE REQUEST-----
```

4. 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*.

5. 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



Welcome

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

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

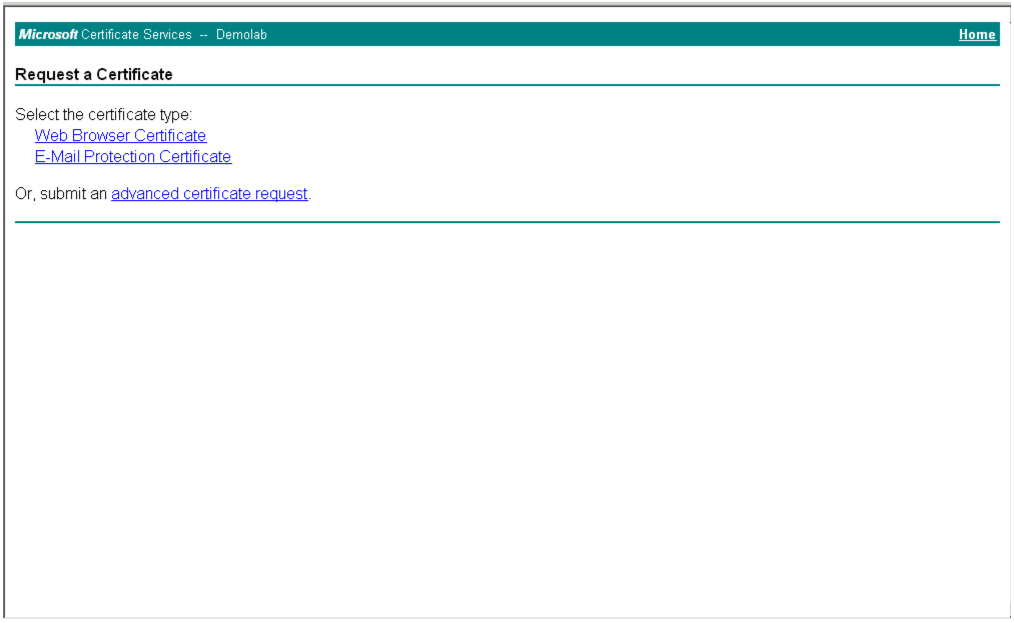
For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

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

6. Click **Request a certificate**.

Figure 4-26: Request a Certificate Page



Microsoft Certificate Services -- Demolab

Home

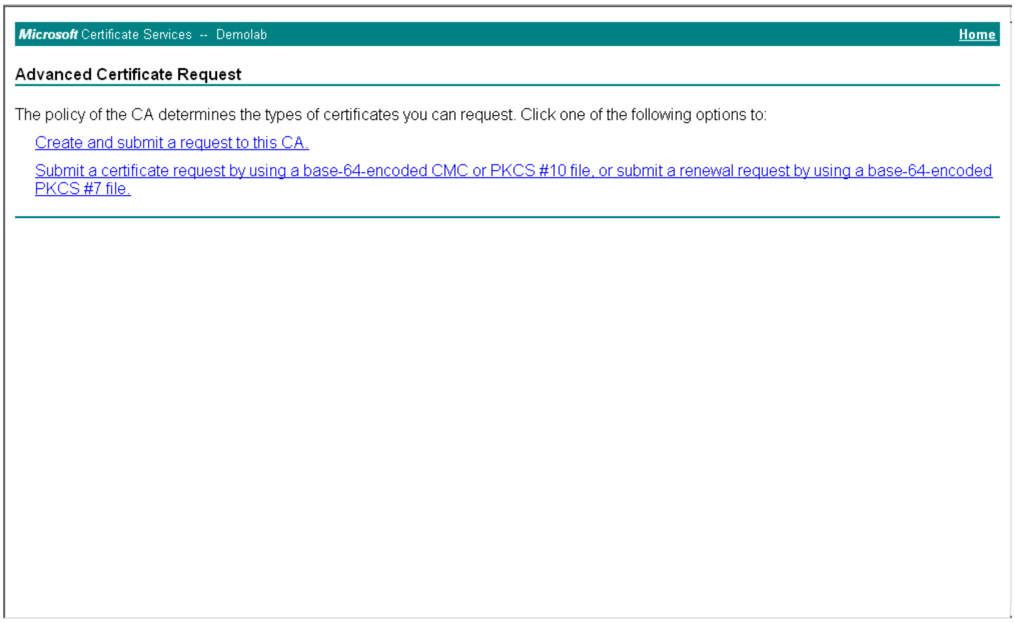
Request a Certificate

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

Or, submit an advanced certificate request.

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

Figure 4-27: Advanced Certificate Request Page



Microsoft Certificate Services -- Demolab

Home

Advanced Certificate Request

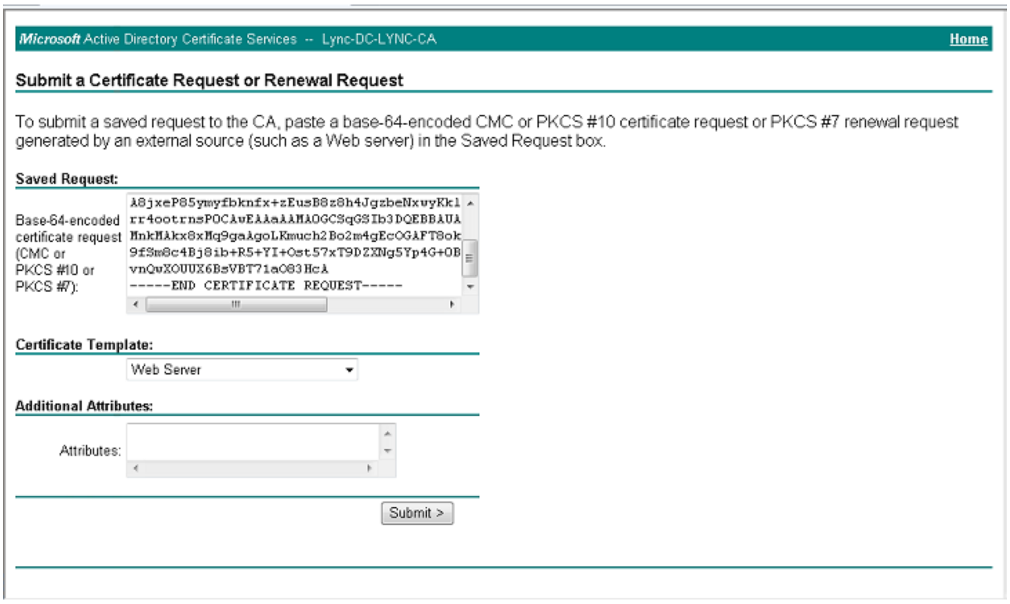
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

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

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

Figure 4-28: Submit a Certificate Request or Renewal Request Page



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

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
A8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxuyKkl
rr4ootrnsPOCAuEAAaAAMAOGCSqGSIb3DQEBBAUA
MnkMAkx8xMq9gaAgoLKmuch2Bo2m4gEcOGAFT8ok
9fSm8c4Bj8ib+R5+YI+Ost57xT9DZXNg5Yp4G+OB
vnQuXOUUX6BsVBT71a083HcA
-----END CERTIFICATE REQUEST-----
```

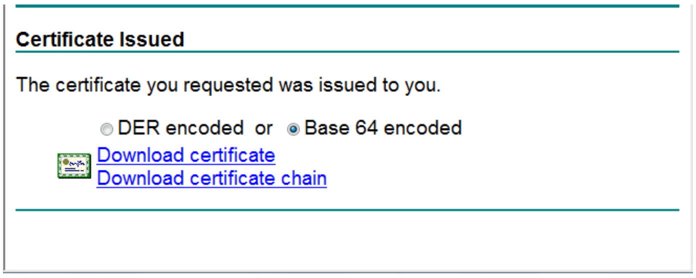
Certificate Template: Web Server

Additional Attributes:

Attributes:

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



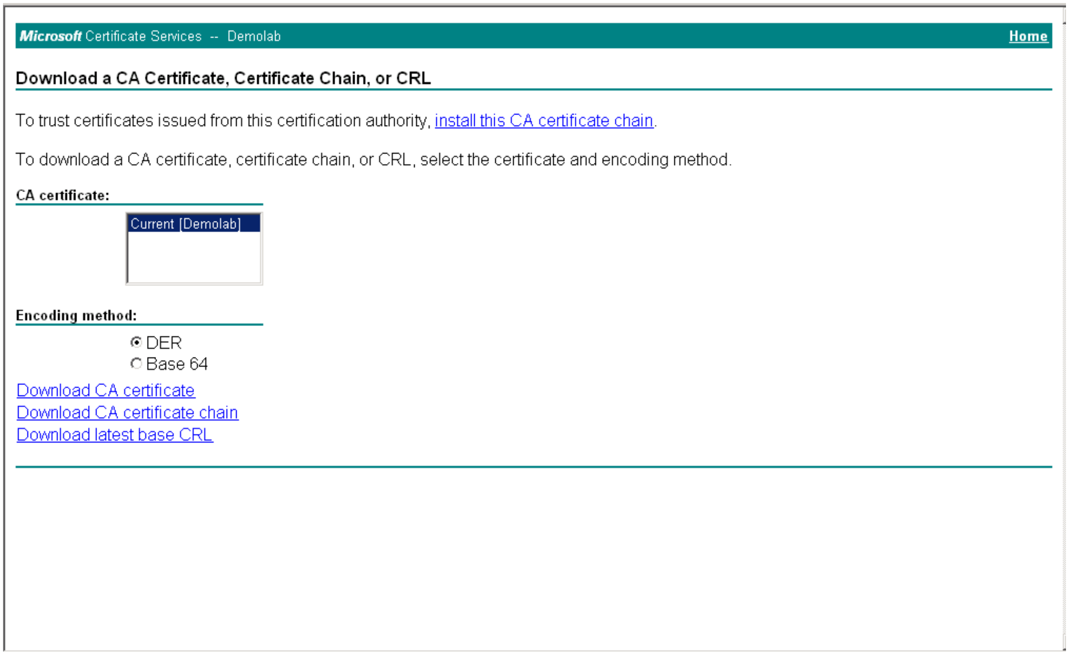
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

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



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:

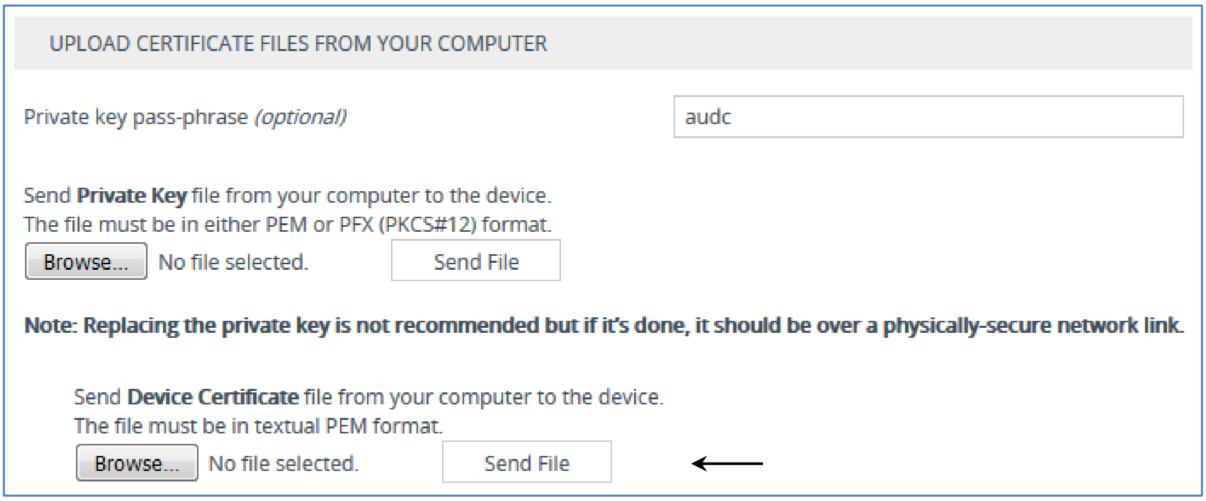
● DER
○ Base 64

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



UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*: audc

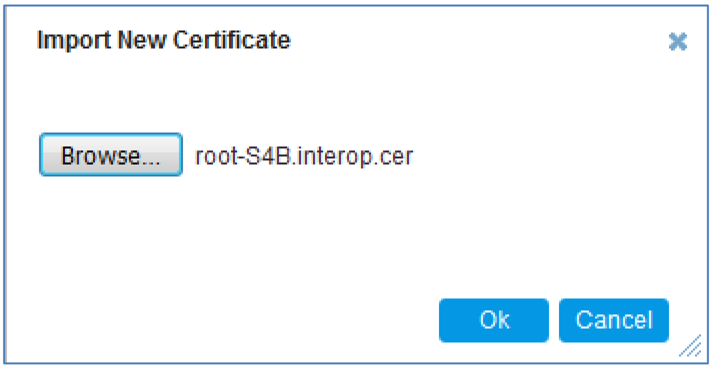
Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

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

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



Import New Certificate

root-S4B.interop.cer

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).

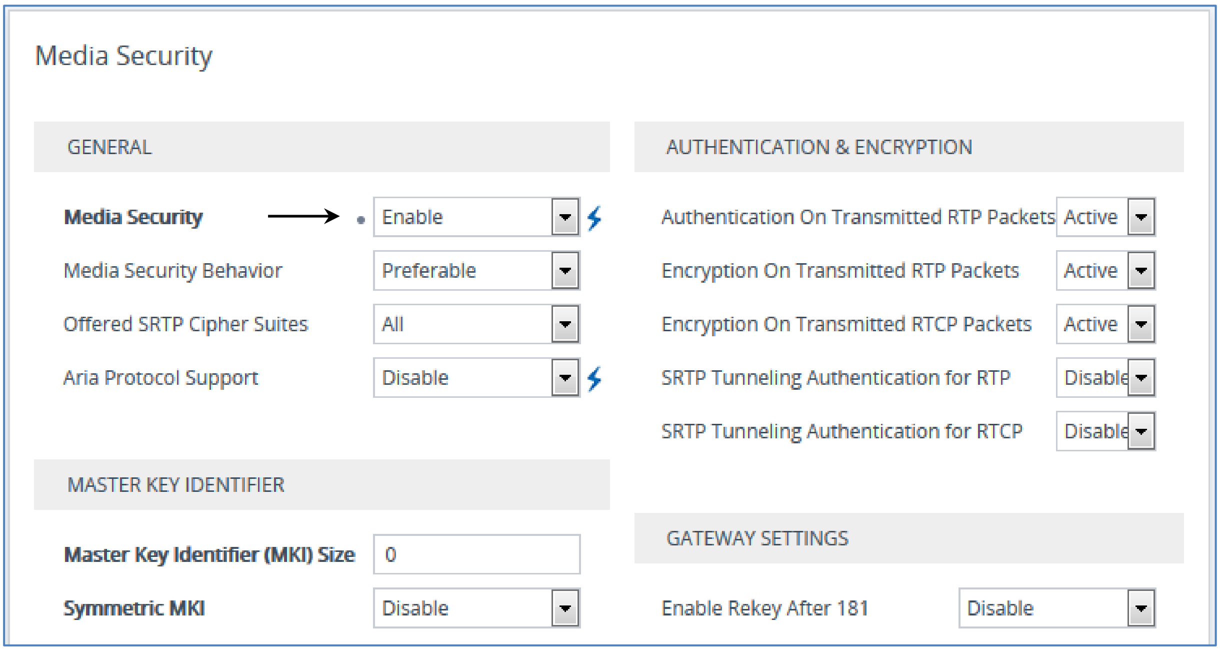
4.10 Step 10: Configure SRTP

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



Media Security

GENERAL

Media Security	Enable
Media Security Behavior	Preferable
Offered SRTP Cipher Suites	All
Aria Protocol Support	Disable

MASTER KEY IDENTIFIER

Master Key Identifier (MKI) Size	0
Symmetric MKI	Disable

AUTHENTICATION & ENCRYPTION

Authentication On Transmitted RTP Packets	Active
Encryption On Transmitted RTP Packets	Active
Encryption On Transmitted RTCP Packets	Active
SRTP Tunneling Authentication for RTP	Disable
SRTP Tunneling Authentication for RTCP	Disable

GATEWAY SETTINGS

Enable Rekey After 181	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

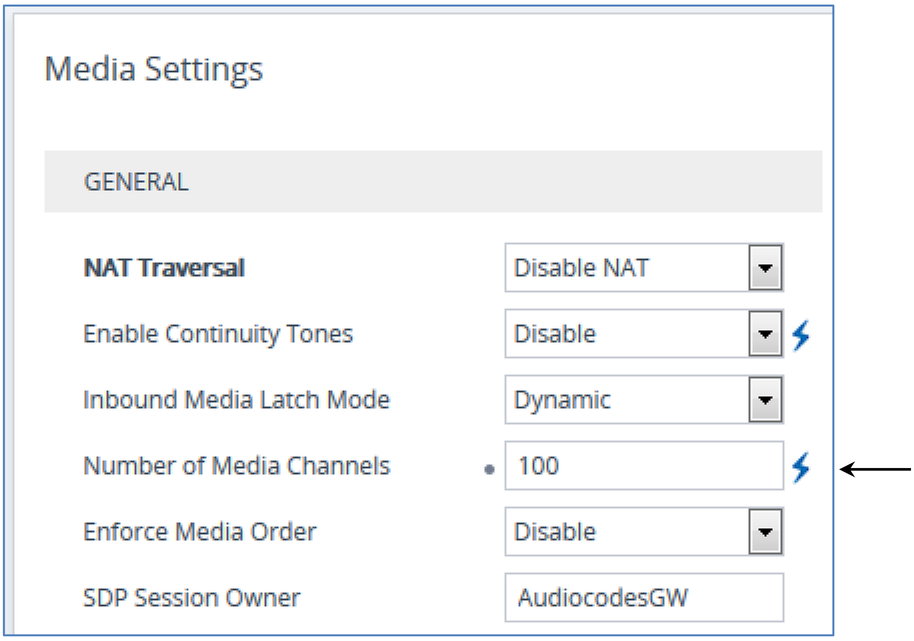
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

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



Media Settings

GENERAL

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

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., 10**0**).
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):

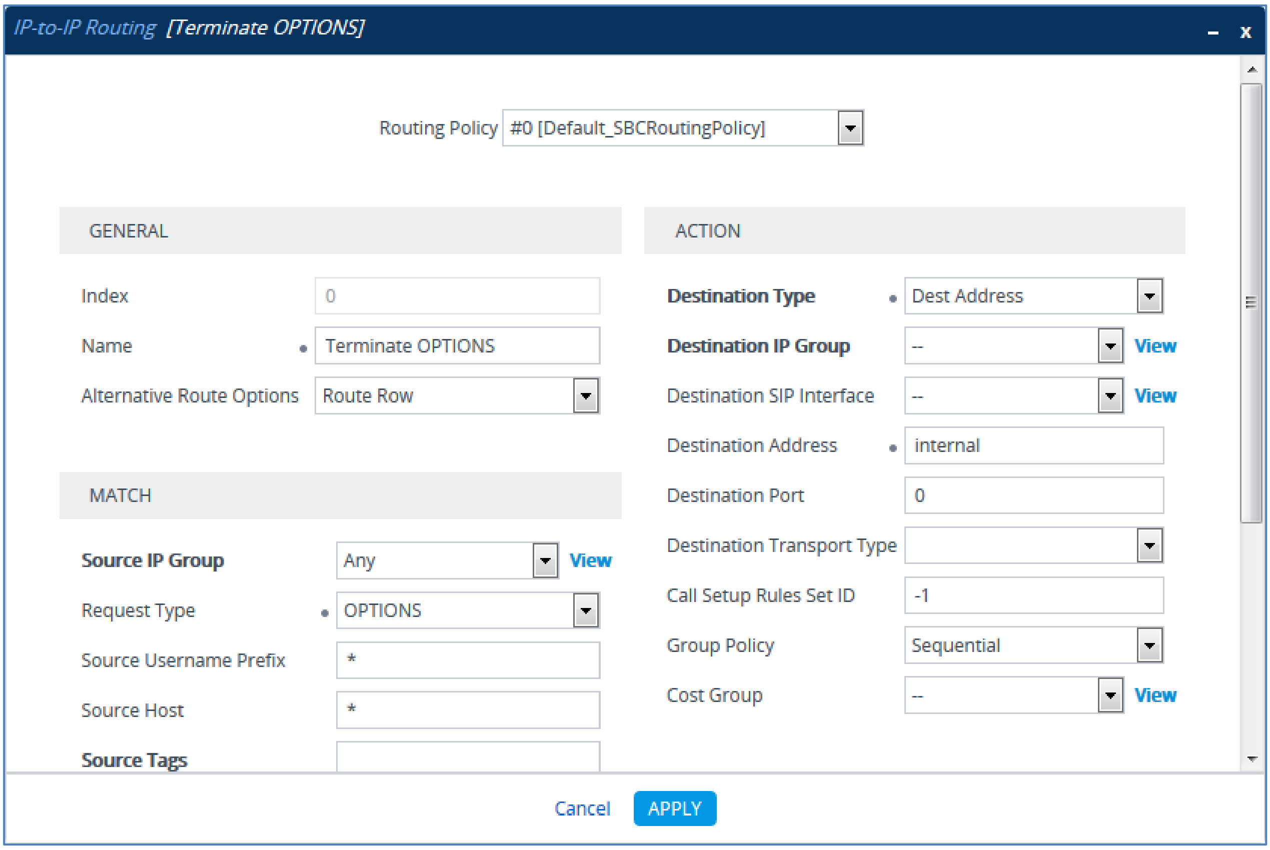
- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
- Calls from Skype for Business Server 2015 to Bell Canada SIP Trunk
- Calls from Bell Canada SIP Trunk to Skype for Business Server 2015

➢ 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	**0**
Name	**Terminate OPTIONS** (arbitrary descriptive name)
Source IP Group	**Any**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

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



IP-to-IP Routing [Terminate OPTIONS]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index	0
Name	Terminate OPTIONS
Alternative Route Options	Route Row

MATCH

Source IP Group	Any
Request Type	OPTIONS
Source Username Prefix	*
Source Host	*
Source Tags	

ACTION

Destination Type	Dest Address
Destination IP Group	--
Destination SIP Interface	--
Destination Address	internal
Destination Port	0
Destination Transport Type	
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	--

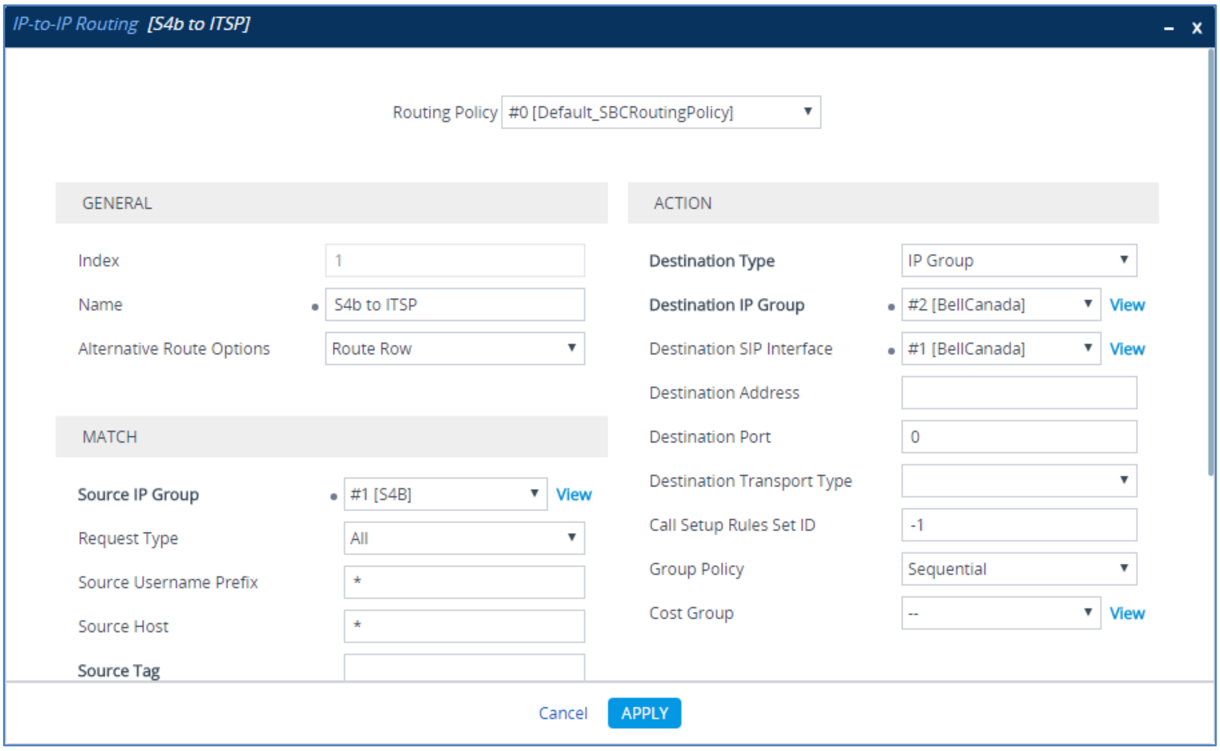
   b. Click **Apply**.

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	**S4B to ITSP** (arbitrary descriptive name)
Source IP Group	**S4B**
Destination Type	**IP Group**
Destination IP Group	**BellCanada**
Destination SIP Interface	**BellCanada**

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



IP-to-IP Routing [S4b to ITSP]

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL

Index	1
Name	S4b to ITSP
Alternative Route Options	Route Row

MATCH

Source IP Group	#1 [S4B]
Request Type	All
Source Username Prefix	*
Source Host	*
Source Tag	

ACTION

Destination Type	IP Group
Destination IP Group	#2 [BellCanada]
Destination SIP Interface	#1 [BellCanada]
Destination Address	
Destination Port	0
Destination Transport Type	
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	--

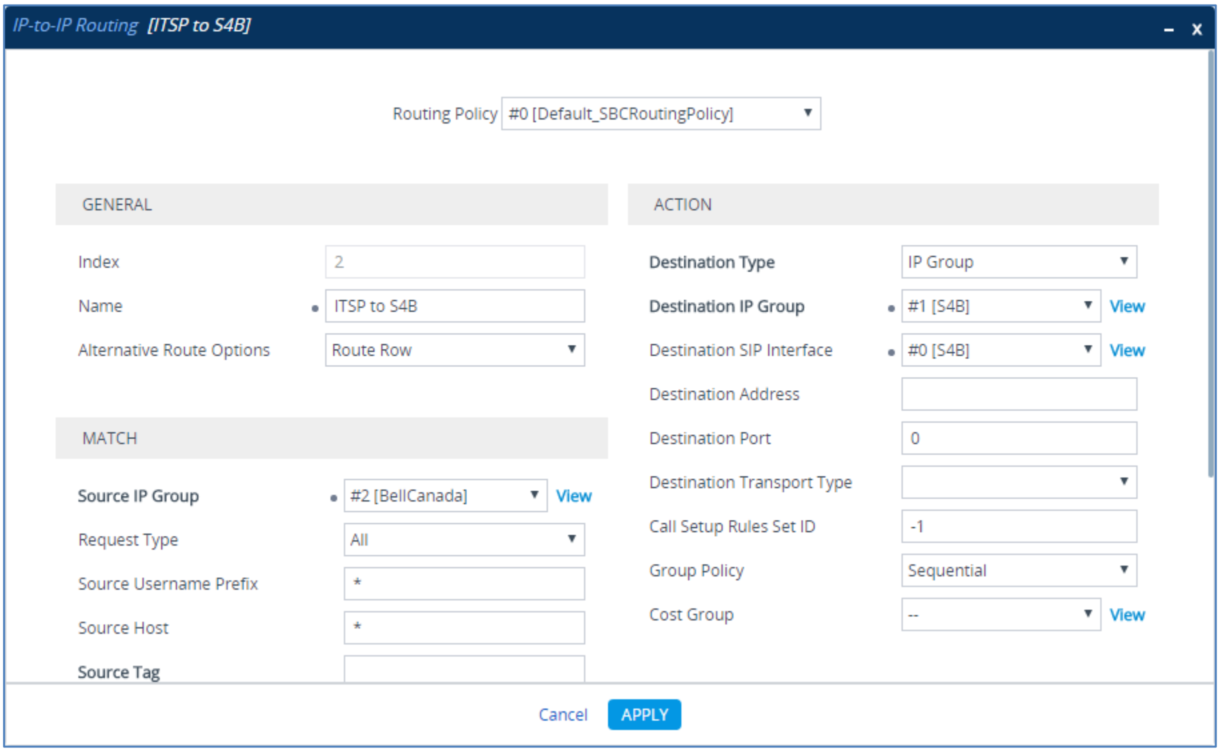
   b. Click **Apply**.

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



IP-to-IP Routing [ITSP to S4B]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index: 2

Name: ITSP to S4B

Alternative Route Options: Route Row

MATCH

Source IP Group: #2 [BellCanada]

Request Type: All

Source Username Prefix: *

Source Host: *

Source Tag:

ACTION

Destination Type: IP Group

Destination IP Group: #1 [S4B]

Destination SIP Interface: #0 [S4B]

Destination Address:

Destination Port: 0

Destination Transport Type:

Call Setup Rules Set ID: -1

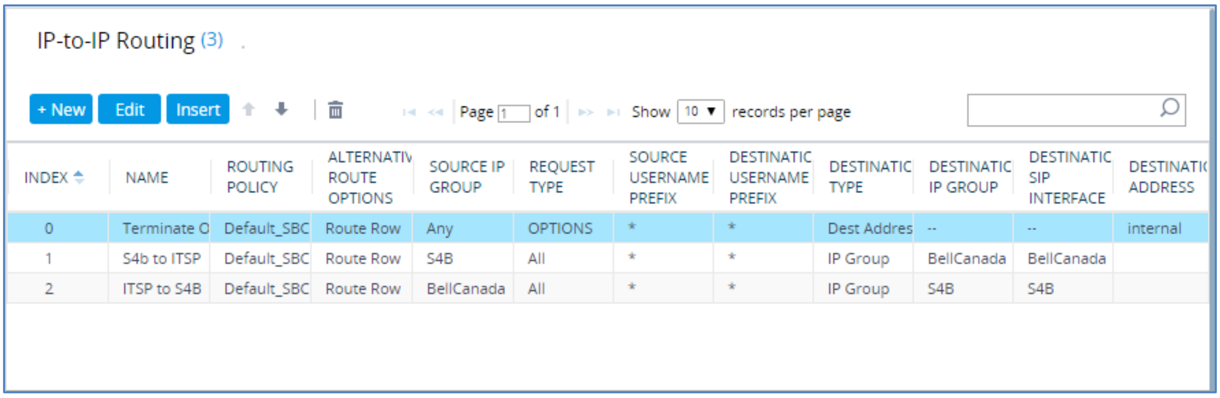
Group Policy: Sequential

Cost Group: --

   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



INDEX	NAME	ROUTING POLICY	ALTERNATIV ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATIC USERNAME PREFIX	DESTINATIC TYPE	DESTINATIC IP GROUP	DESTINATIC SIP INTERFACE	DESTINATI(ADDRESS
0	Terminate O	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Addres	--	--	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.

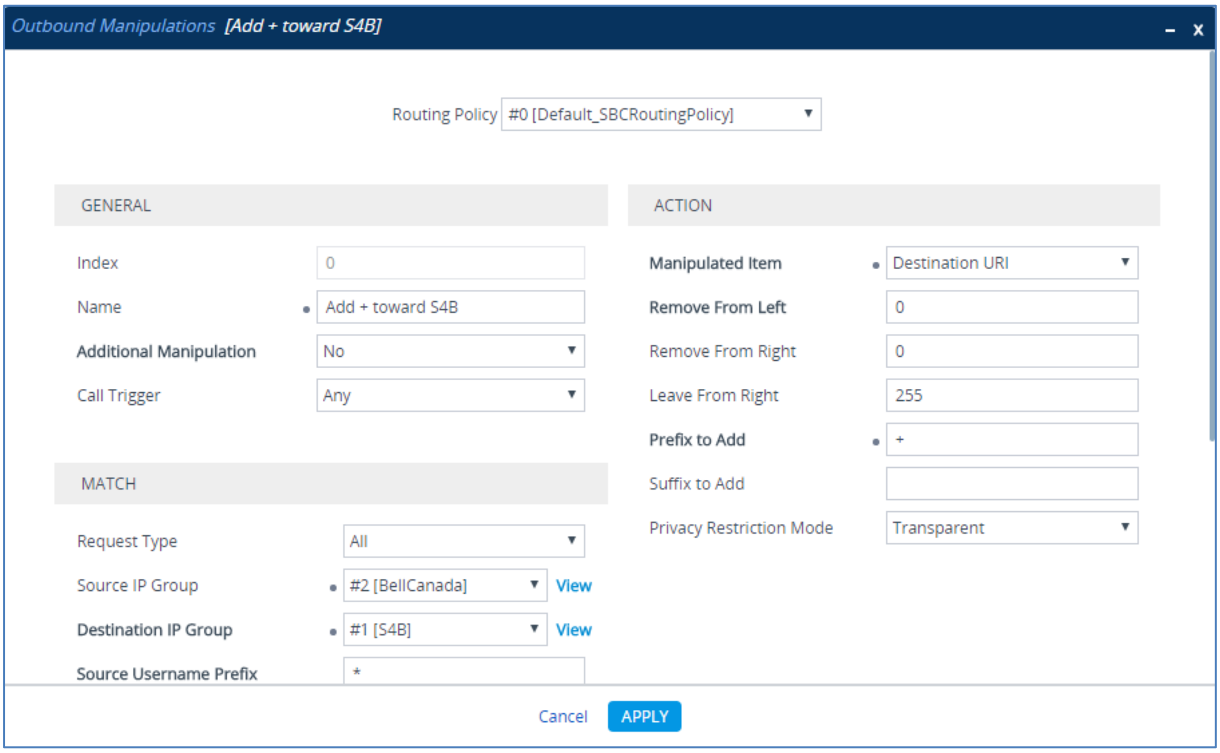
For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from the Bell Canada SIP Trunk IP Group to the Skype for Business Server 2015 IP Group for any destination username prefix.

➢ **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	**0**
Name	**Add + toward S4B**
Source IP Group	**BellCanada**
Destination IP Group	**S4B**
Destination Username Prefix	***** (asterisk sign)
Manipulated Item	**Destination URI**
Prefix to Add	**+** (plus sign)

Figure 4-39: Configuring IP-to-IP Outbound Manipulation Rule



Outbound Manipulations [Add + toward S4B]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index	0
Name	Add + toward S4B
Additional Manipulation	No
Call Trigger	Any

MATCH

Request Type	All
Source IP Group	#2 [BellCanada]
Destination IP Group	#1 [S4B]
Source Username Prefix	*

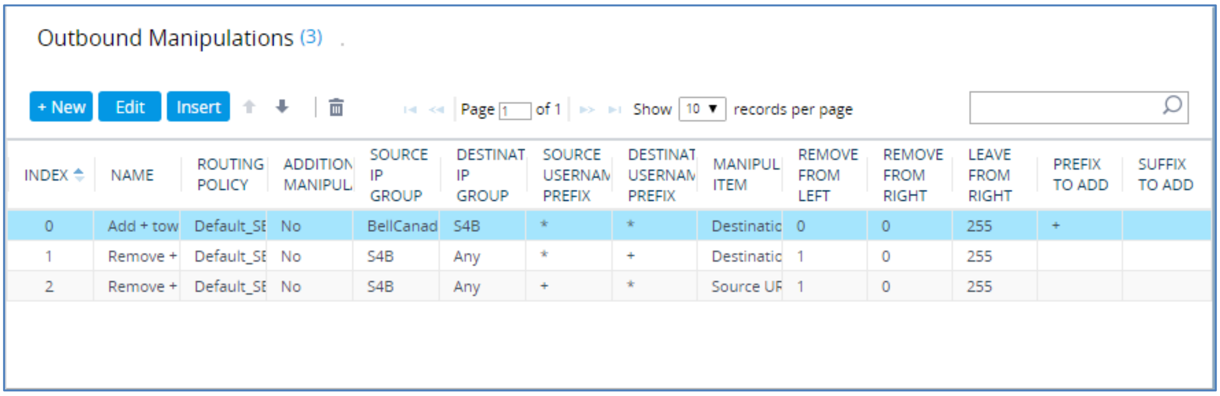
ACTION

Manipulated Item	Destination URI
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	
Privacy Restriction Mode	Transparent

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



Outbound Manipulations (3)

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_SE	No	BellCanad	S4B	*	*	Destinatic	0	0	255	+	
1	Remove +	Default_SE	No	S4B	Any	*	+	Destinatic	1	0	255		
2	Remove +	Default_SE	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).

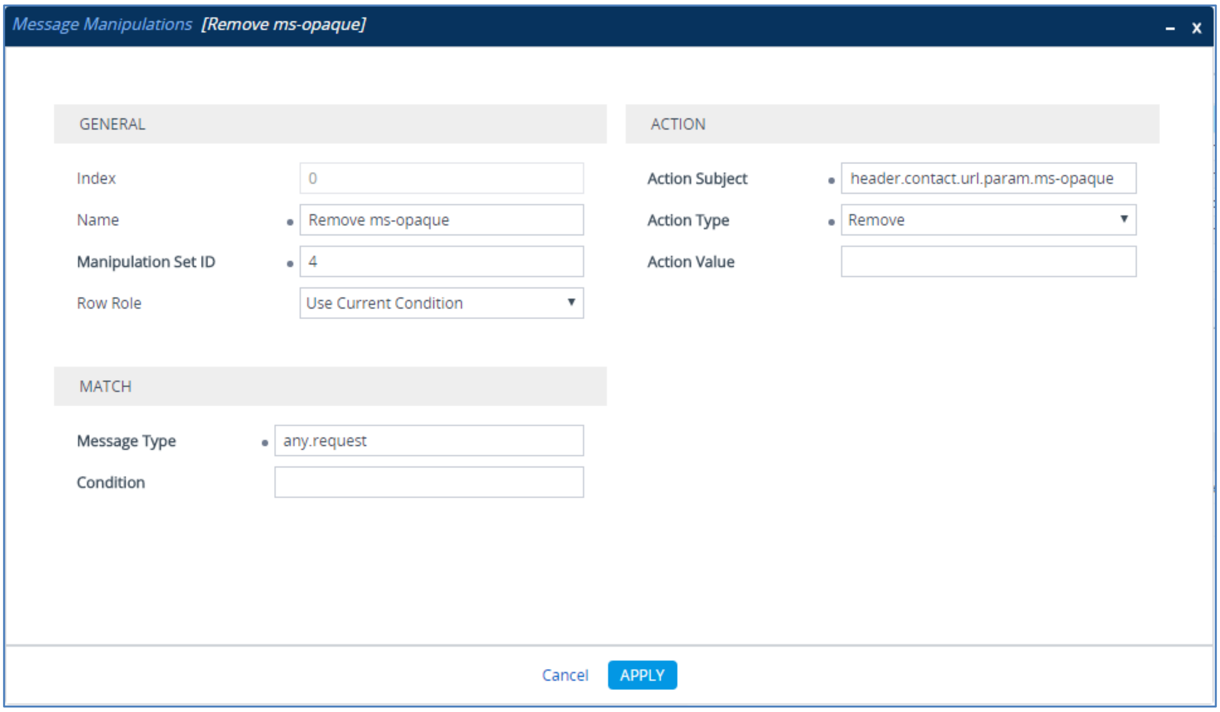
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➢ **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)


Message Manipulations [Remove ms-opaque]

GENERAL

Index: 0

Name: Remove ms-opaque

Manipulation Set ID: 4

Row Role: Use Current Condition

MATCH

Message Type: any.request

Condition:

ACTION

Action Subject: header.contact.url.param.ms-opaque

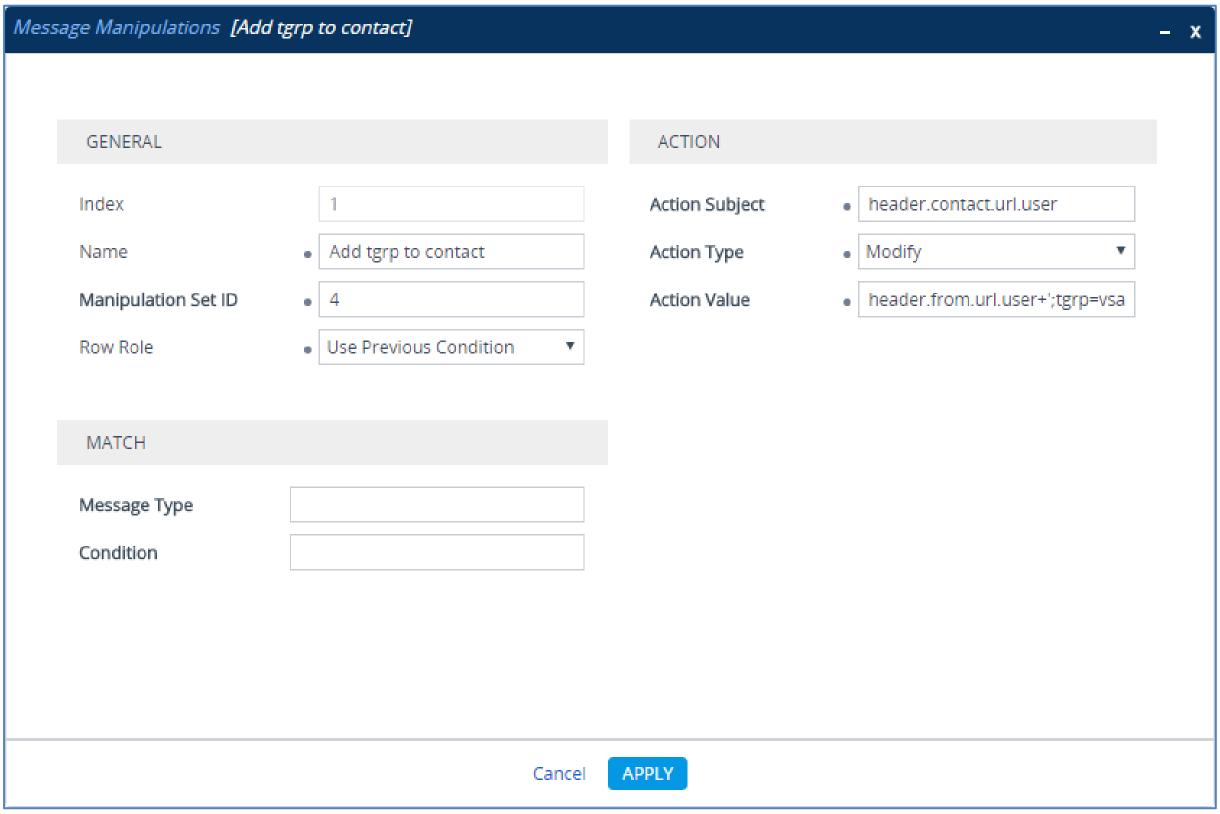
Action Type: Remove

Action Value:

3. 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	**Add tgrp to contact**
Manipulation Set ID	**4**
Row Role	**Use Previous Condition**
Action Subject	**header.contact.url.user**
Action Type	**Modify**
Action Value	**header.from.url.user+';tgrp=customer;trunk-context=siptrunking.bell.ca'**

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

MATCH

Message Type	
Condition	

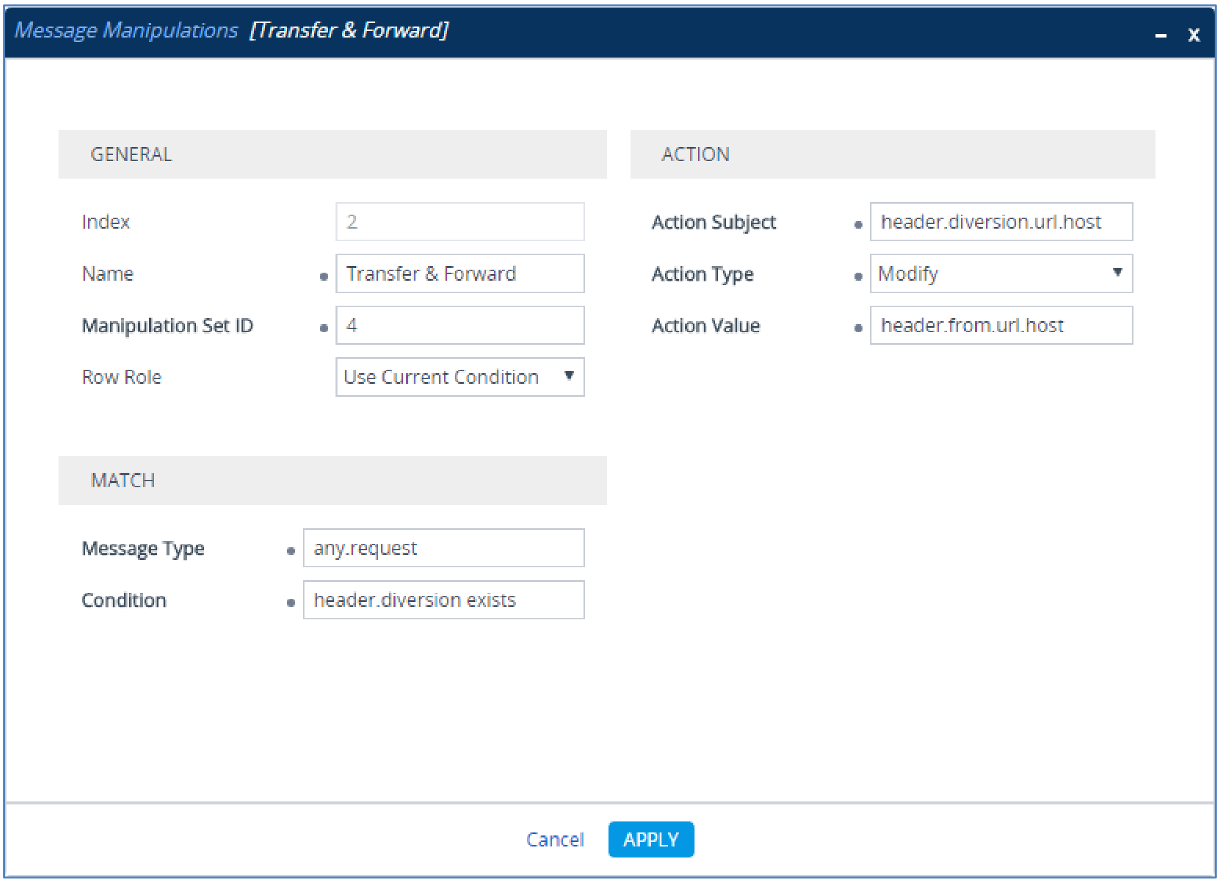
ACTION

Action Subject	header.contact.url.user
Action Type	Modify
Action Value	header.from.url.user+';tgrp=vsa

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	**2**
Name	**Transfer & Forward**
Manipulation Set ID	**4**
Message Type	**any.request**
Condition	**header. diversion exists**
Action Subject	**header.diversion.url.host**
Action Type	**Modify**
Action Value	**header.from.url.host**

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

MATCH

Message Type: any.request

Condition: header.diversion exists

ACTION

Action Subject: header.diversion.url.host

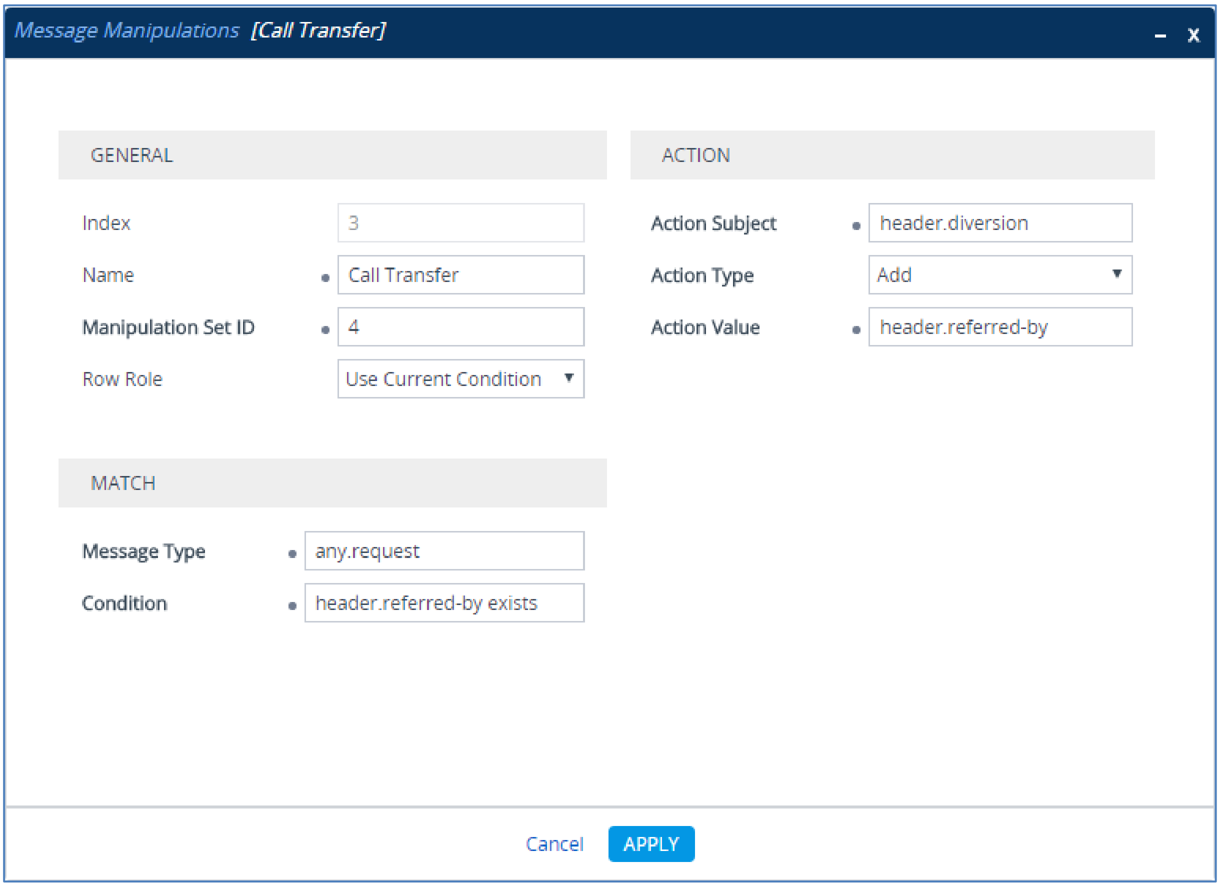
Action Type: Modify

Action Value: header.from.url.host

5. 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)



Message Manipulations *[Call Transfer]*

GENERAL

Index: 3

Name: Call Transfer

Manipulation Set ID: 4

Row Role: Use Current Condition

MATCH

Message Type: any.request

Condition: header.referred-by exists

ACTION

Action Subject: header.diversion

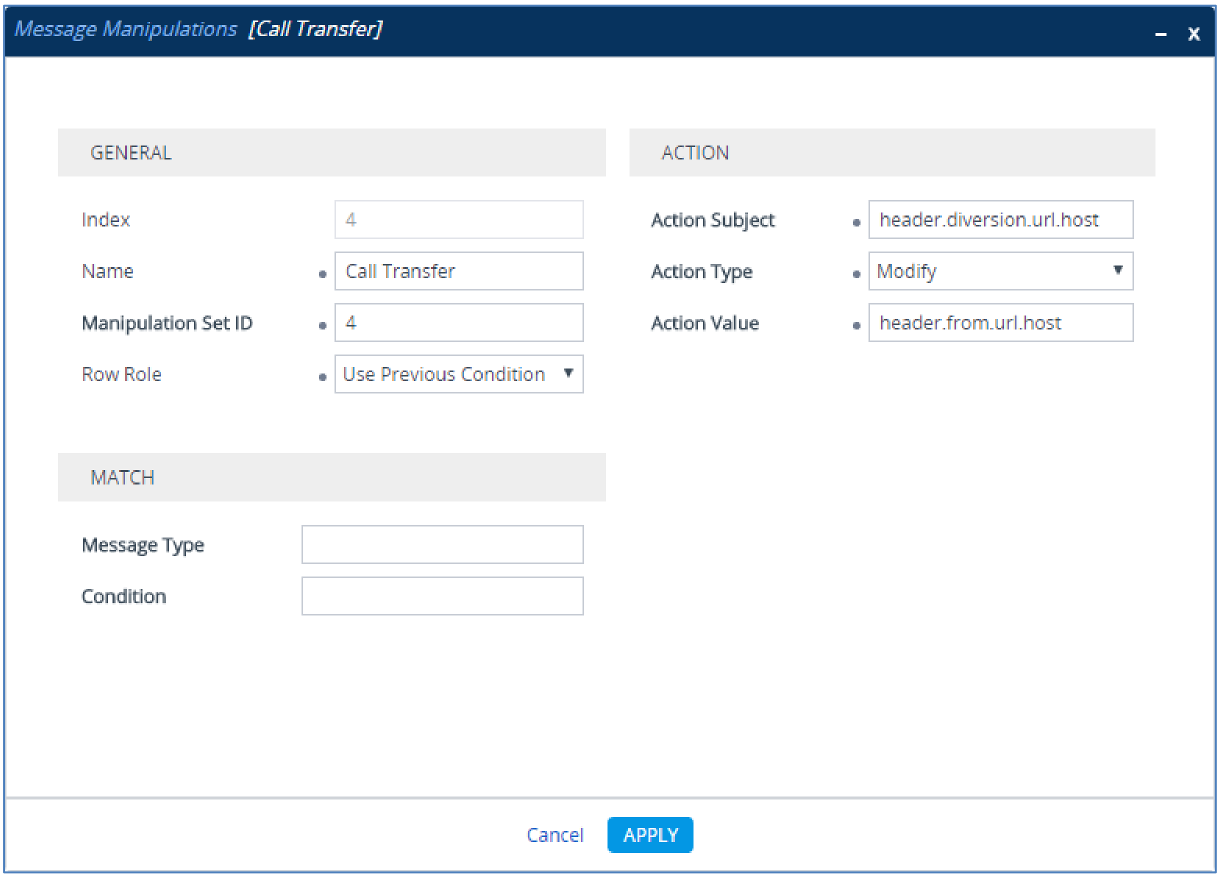
Action Type: Add

Action Value: header.referred-by

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

MATCH

Message Type	
Condition	

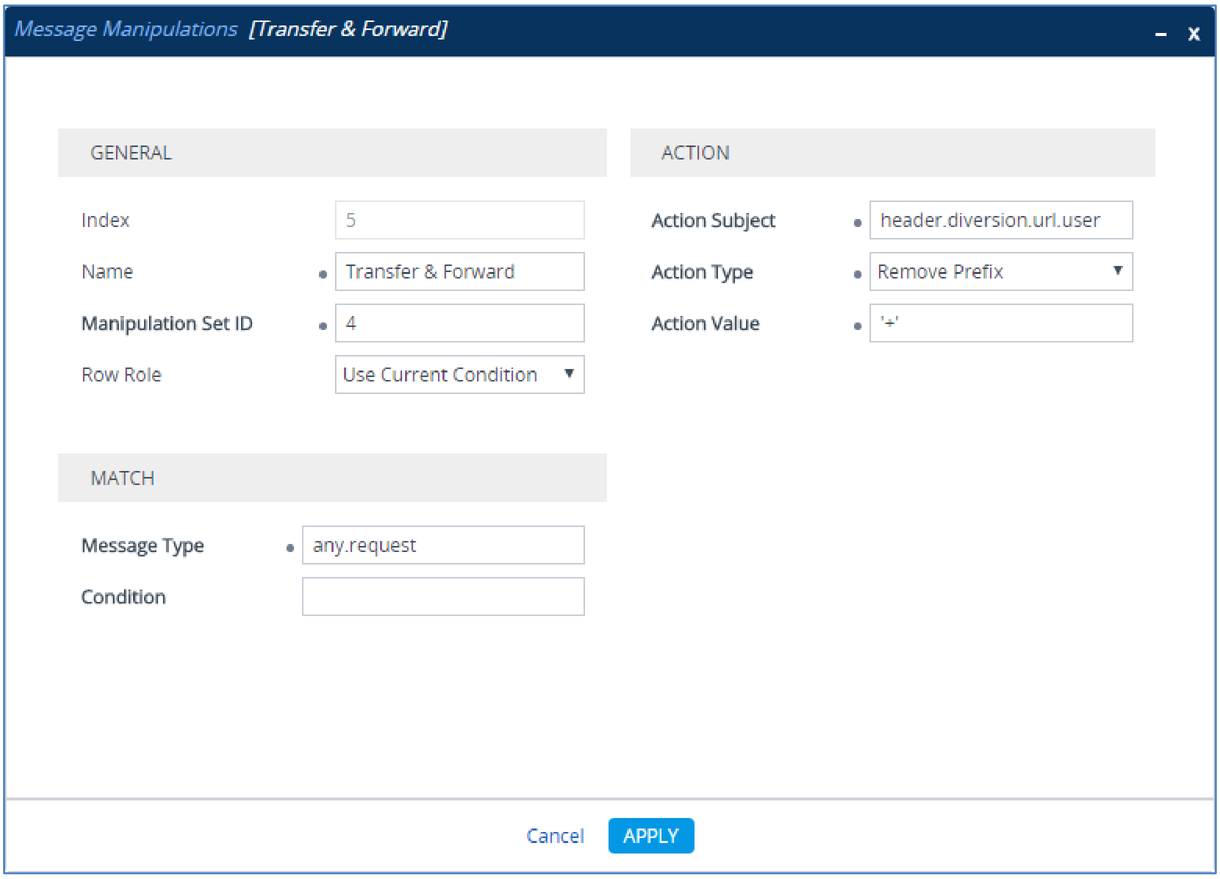
ACTION

Action Subject	header.diversion.url.host
Action Type	Modify
Action Value	header.from.url.host

7. 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)



Message Manipulations [Transfer & Forward]

GENERAL

Index	5
Name	Transfer & Forward
Manipulation Set ID	4
Row Role	Use Current Condition

MATCH

Message Type	any.request
Condition	

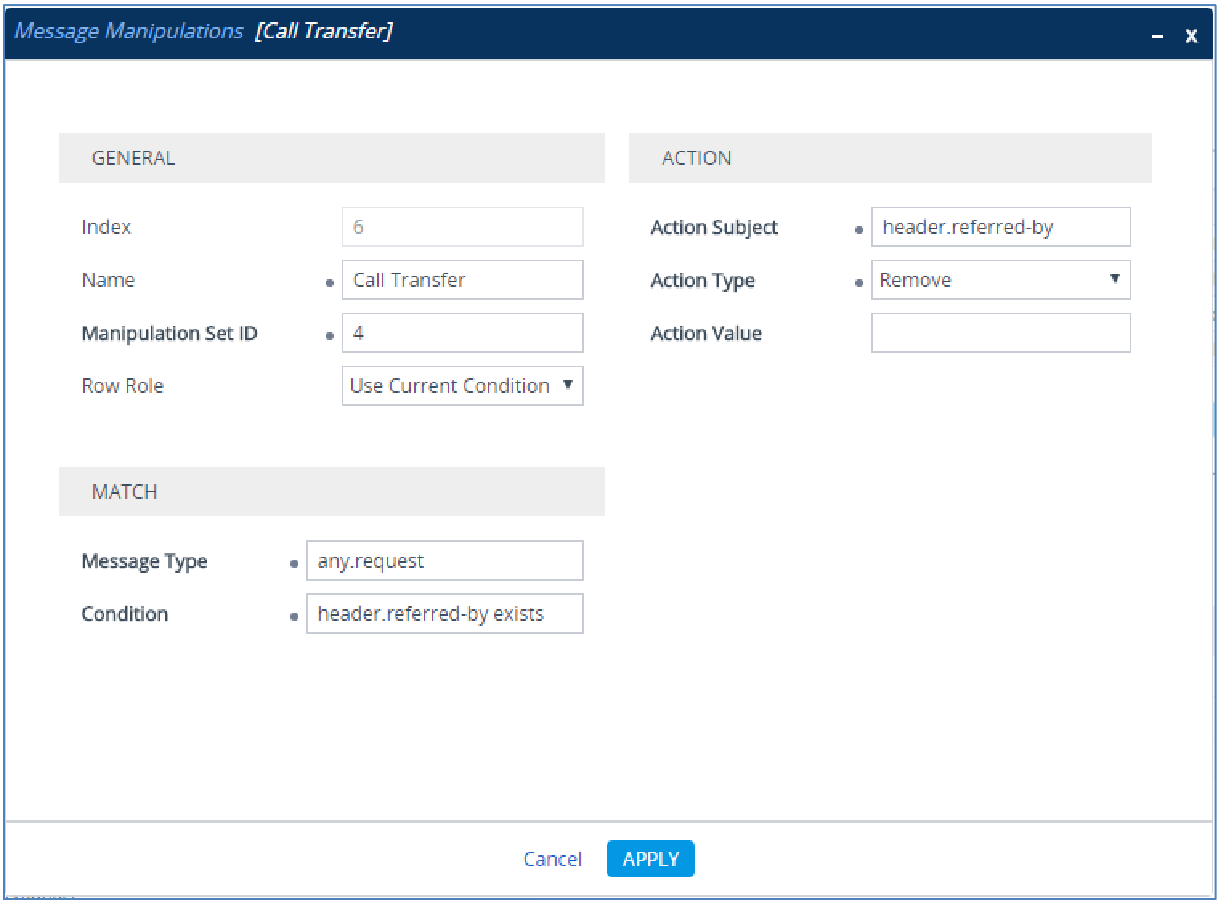
ACTION

Action Subject	header.diversion.url.user
Action Type	Remove Prefix
Action Value	'+'

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

MATCH

Message Type	any.request
Condition	header.referred-by exists

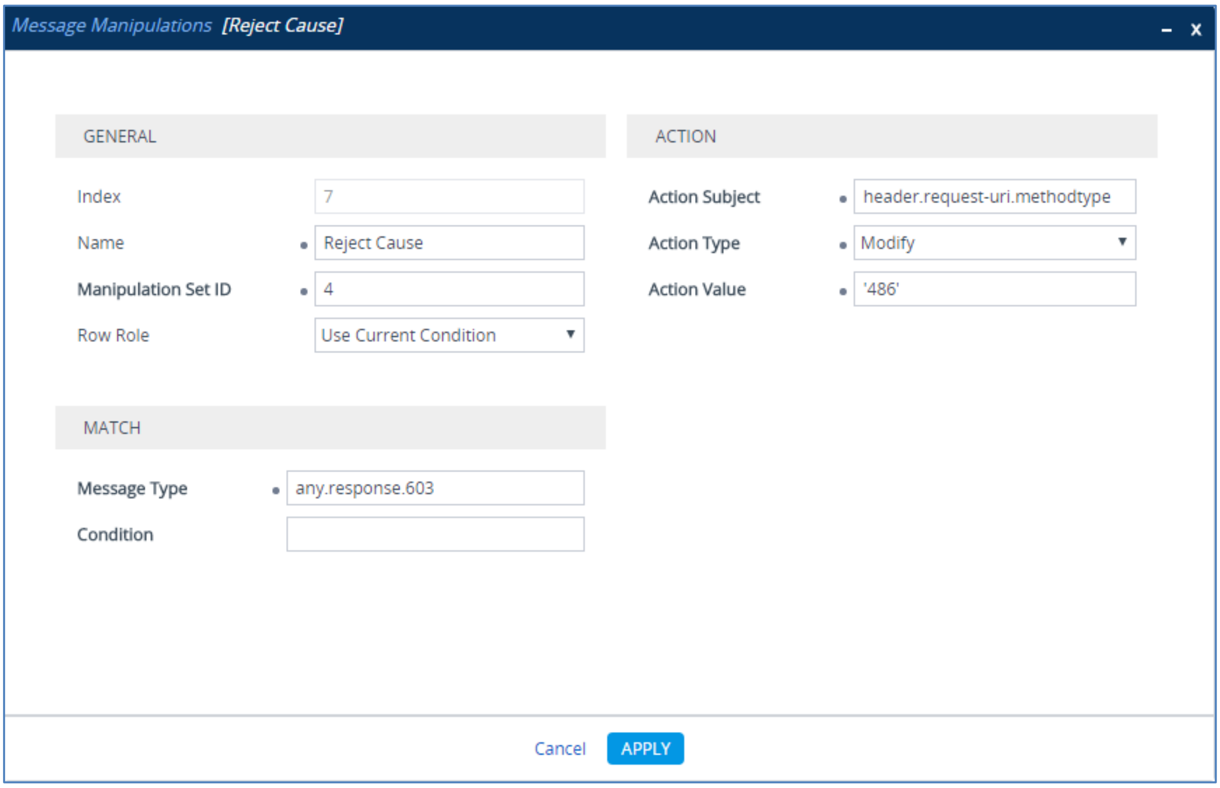
ACTION

Action Subject	header.referred-by
Action Type	Remove
Action Value	

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)



Message Manipulations *[Reject Cause]*

GENERAL

Index	7
Name	Reject Cause
Manipulation Set ID	4
Row Role	Use Current Condition

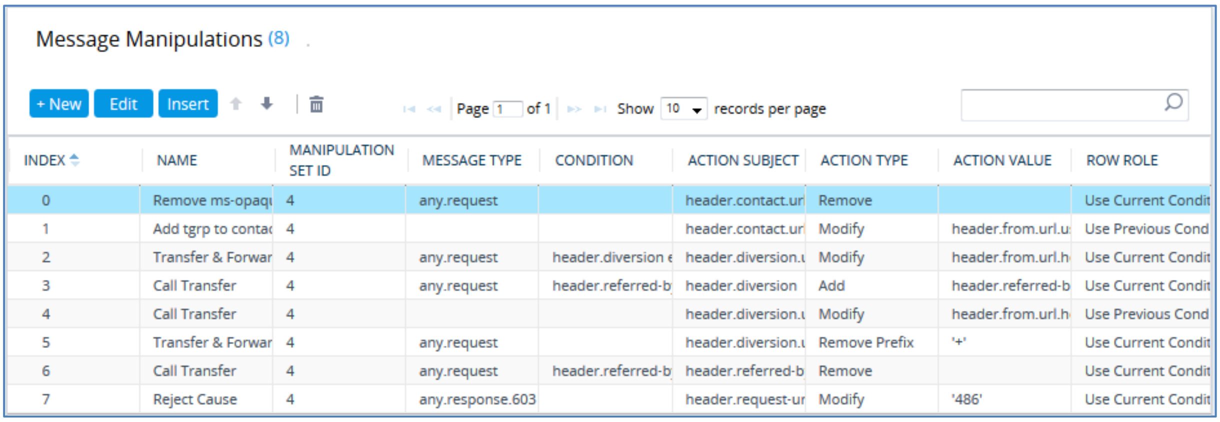
MATCH

Message Type	any.response.603
Condition	

ACTION

Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'486'

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



Message Manipulations (8)

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Remove ms-opaqu	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 e	header.diversion.u	Modify	header.from.url.h	Use Current Condit
3	Call Transfer	4	any.request	header.referred-b	header.diversion	Add	header.referred-b	Use Current Condit
4	Call Transfer	4			header.diversion.u	Modify	header.from.url.h	Use Previous Cond
5	Transfer & Forwar	4	any.request		header.diversion.u	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

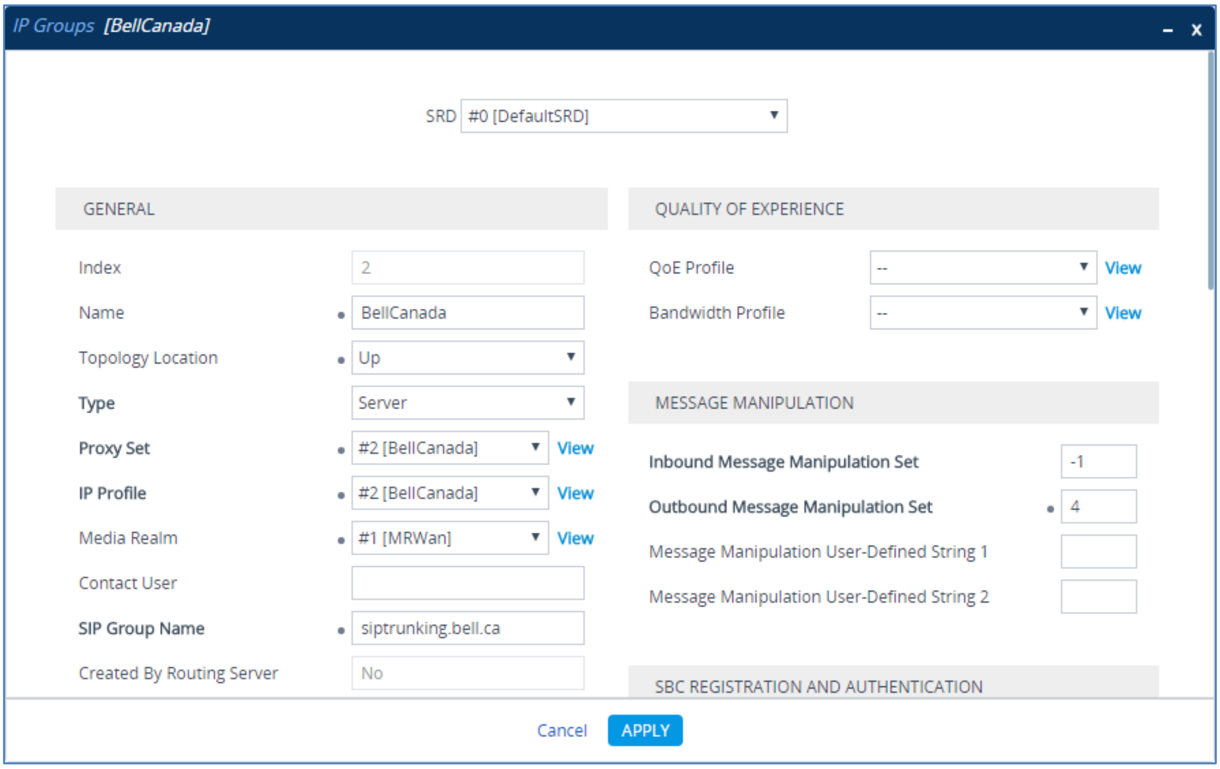
The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to the Bell Canada SIP Trunk IP Group. These rules are specifically required to enable proper interworking between Bell Canada SIP Trunk and 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.

Rule Index	Rule Description	Reason for Introducing Rule
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



IP Groups [BellCanada]

SRD #0 [DefaultSRD]

GENERAL

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
Created By Routing Server	No

QUALITY OF EXPERIENCE

QoE Profile	--
Bandwidth Profile	--

MESSAGE MANIPULATION

Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	4
Message Manipulation User-Defined String 1	
Message Manipulation User-Defined String 2	

SBC REGISTRATION AND AUTHENTICATION

    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.

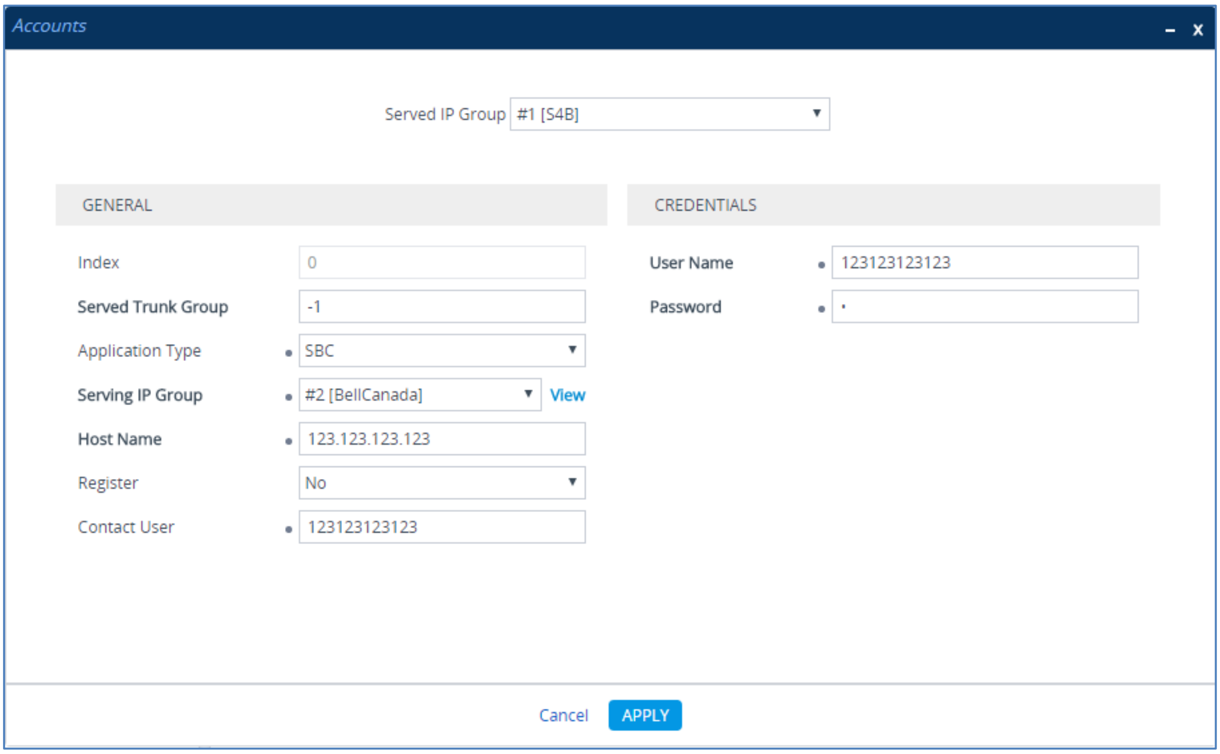
In the interoperability test topology, the Served IP Group is Skype for Business Server 2015 IP Group and the Serving IP Group is Bell Canada SIP Trunk IP Group.

➢ **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	**S4B**
Application Type	**SBC**
Serving IP Group	**BellCanada**
Host Name	As provided by the SIP Trunk provider
Register	**No**
Contact User	**123123123123** (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



Served IP Group: #1 [S4B]

GENERAL

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

CREDENTIALS

User Name: 123123123123
Password: •

4. Click **Apply**.

This page is intentionally left blank.

4.16 Step 16: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

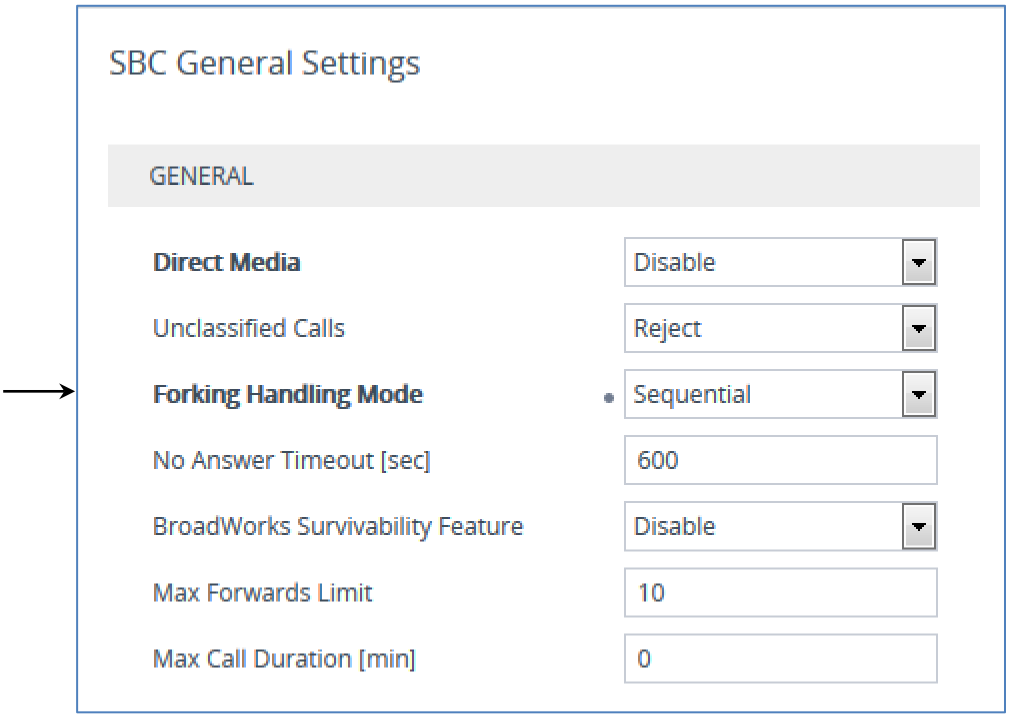
4.16.1 Step 16a: Configure Call Forking Mode

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



SBC General Settings

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**.

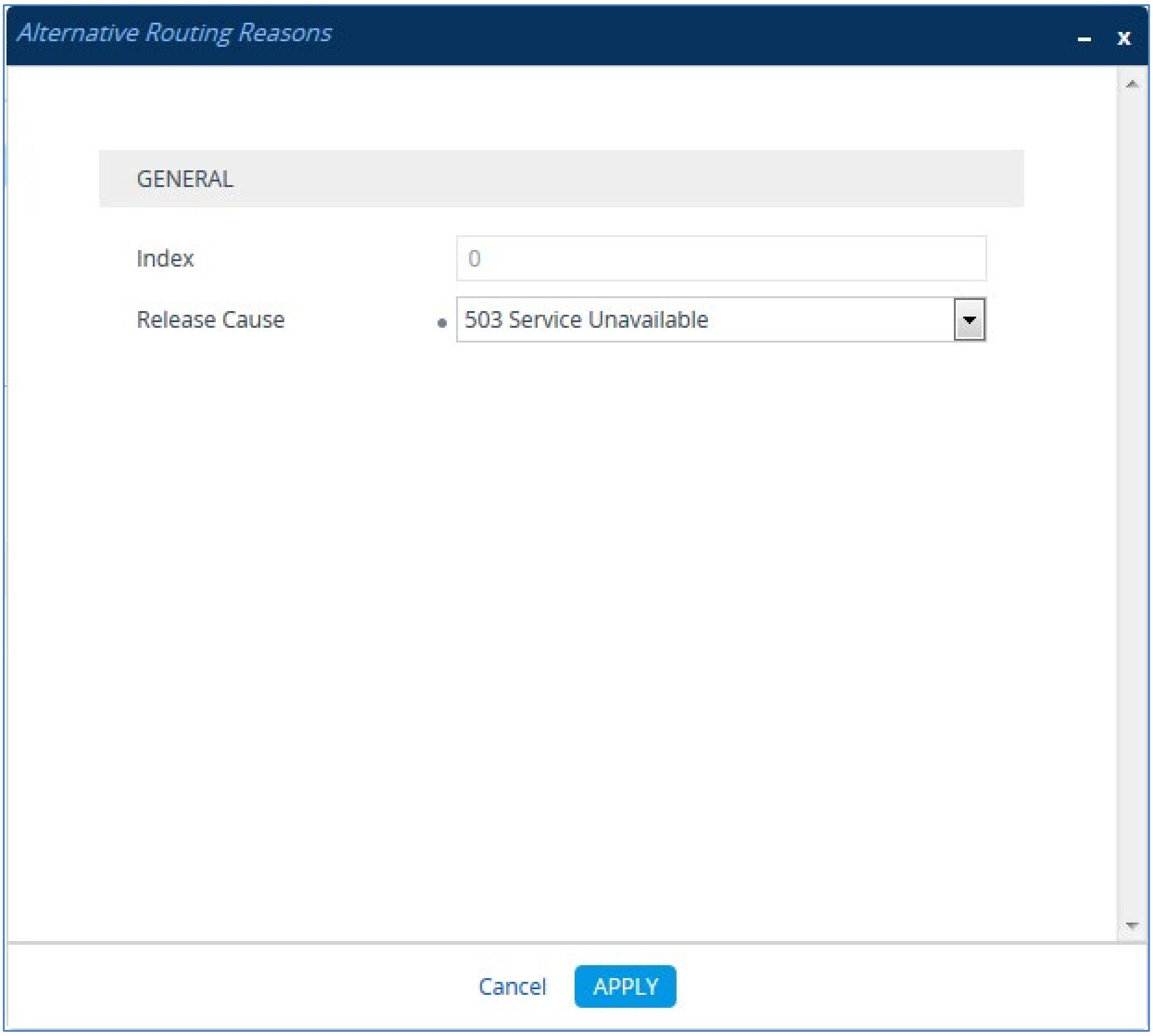
4.16.2 Step 16b: Configure SBC Alternative Routing Reasons

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



Index: 0

Release Cause: 503 Service Unavailable

4. Click **Apply**.

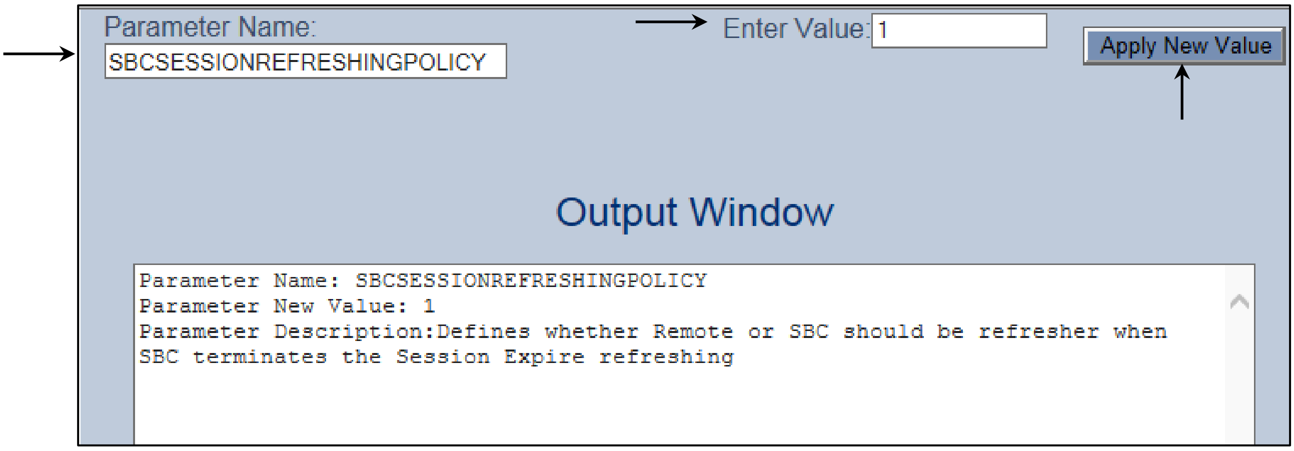
4.16.3 Step 16c: Configure SBC Session Refreshing Policy

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



Parameter Name: SBCSESSIONREFRESHINGPOLICY

Enter Value: 1

```
Parameter Name: SBCSESSIONREFRESHINGPOLICY
Parameter New Value: 1
Parameter Description:Defines whether Remote or SBC should be refresher when
SBC terminates the Session Expire refreshing
```

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.

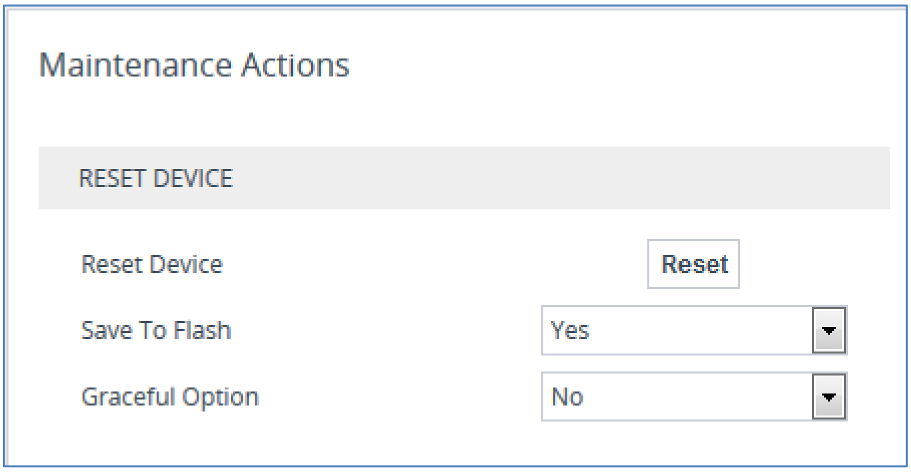
4.17 Step 17: Reset the E-SBC

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



Maintenance Actions

RESET DEVICE

Reset Device: Reset

Save To Flash: Yes

Graceful Option: 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'
SBCPREFERENCESMODE = 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",
"$1$KhNPHB5LGQlQVwoCAw5TXQ1fAwVYXw93eXsncHx0f354eC8qKC8tYGBlZm0xNWA8bmk6Z
WltO1ZTVwcGVl5RCQg=", 1, 0, 5, 15, 60, 200,
"6d6b6fed6c859d76e9bd3f2ddac9fa42";
WebUsers 1 = "User",
"$1$X29RB1MFVlECBFkLWg4JD1YNQkcXQUZBREUcHBtPHRhPT7e2uua9seCxse296bru6r3xp
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_SBCDiversionMode, 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_EnableEarly183,
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_SBCAdaptRFC2833BWToVoiceCoderBW,
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, 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, 1, 0, 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_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, 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

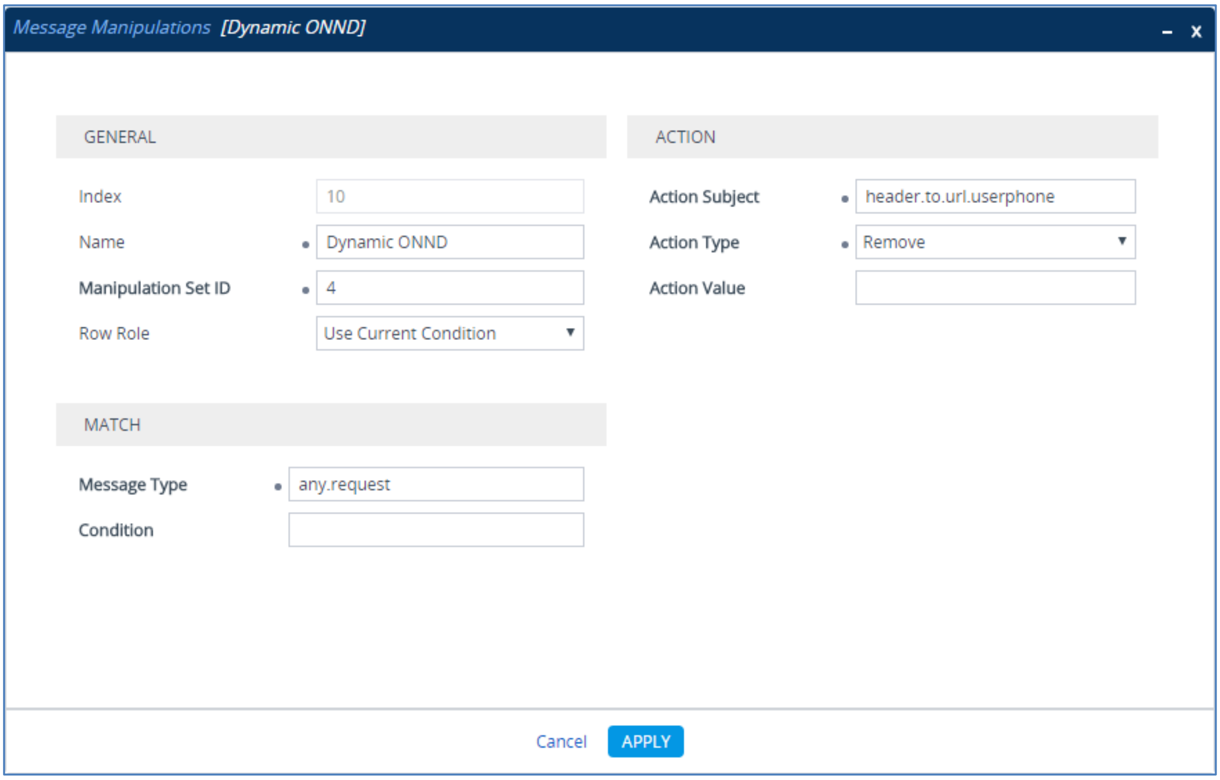
The following SIP message manipulation rules should be configured in order to work in Dynamic ONND mode.

➢ **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	**10**
Name	**Dynamic ONND**
Manipulation Set ID	**4**
Message Type	**any.request**
Action Subject	**header.to.url.userphone**
Action Type	**Remove**

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



Message Manipulations [Dynamic ONND]

GENERAL

Index	10
Name	Dynamic ONND
Manipulation Set ID	4
Row Role	Use Current Condition

MATCH

Message Type	any.request
Condition	

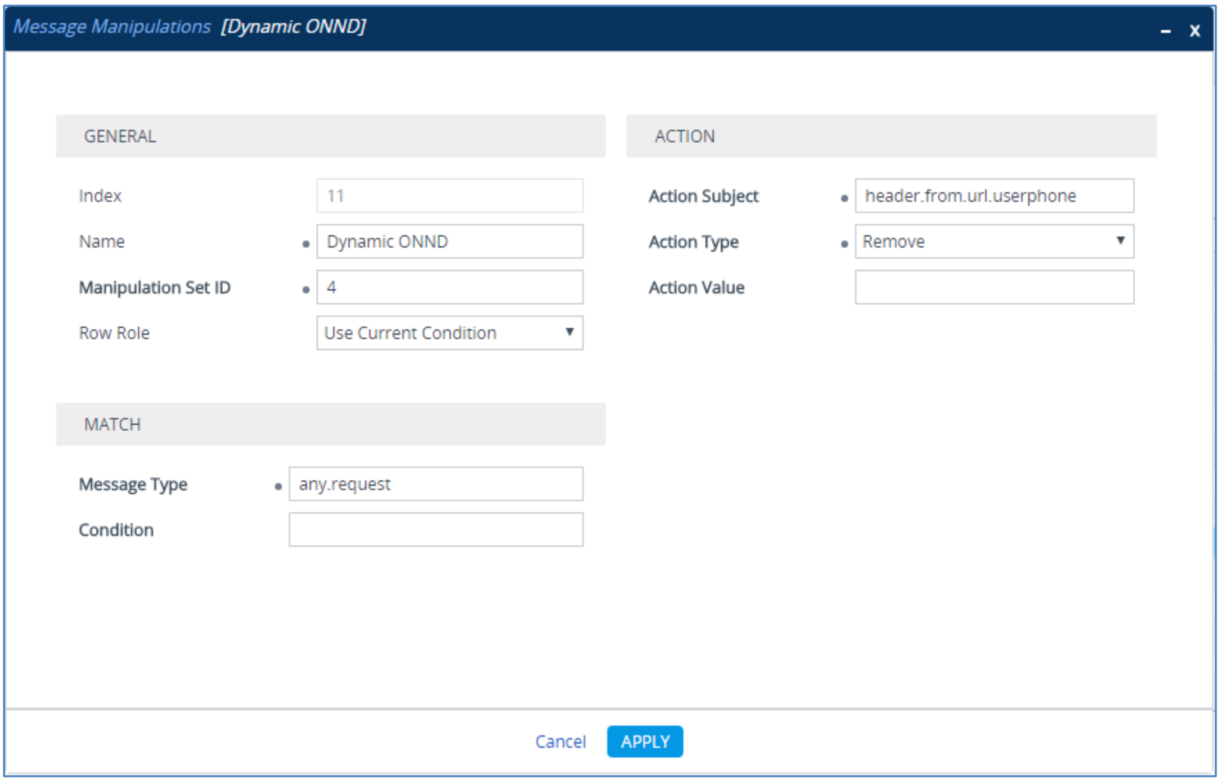
ACTION

Action Subject	header.to.url.userphone
Action Type	Remove
Action Value	

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

Index: 11

Name: Dynamic ONND

Manipulation Set ID: 4

Row Role: Use Current Condition

MATCH

Message Type: any.request

Condition:

ACTION

Action Subject: header.from.url.userphone

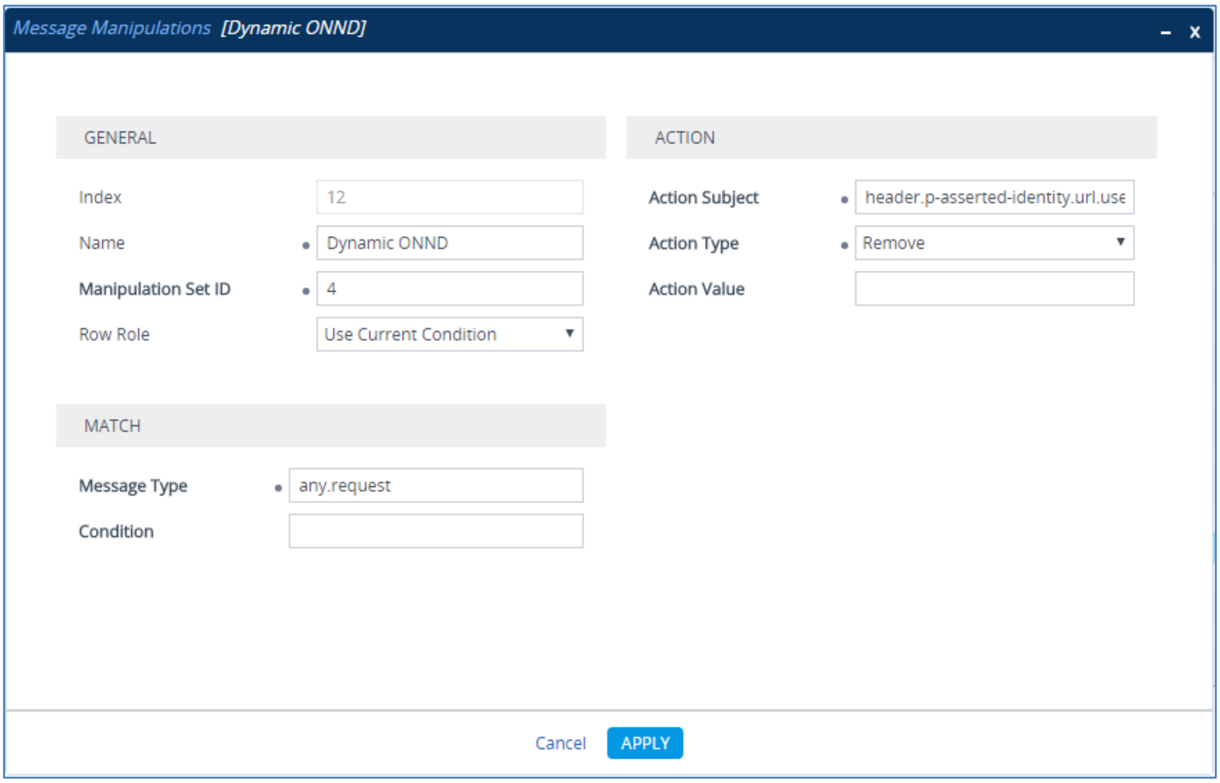
Action Type: Remove

Action Value:

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)



Message Manipulations *[Dynamic ONND]*

GENERAL

Index: 12

Name: Dynamic ONND

Manipulation Set ID: 4

Row Role: Use Current Condition

MATCH

Message Type: any.request

Condition:

ACTION

Action Subject: header.p-asserted-identity.url.use

Action Type: Remove

Action Value:

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

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

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

Document #: LTRT-39235