

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

Version 7.0



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	TELUS SIP Trunking Version	9
2.3	Microsoft Skype for Business Server 2015 Version	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring Skype for Business Server 2015.....	13
3.1	Configuring the E-SBC as an IP / PSTN Gateway	13
3.2	Configuring the "Route" on Skype for Business Server 2015.....	21
4	Configuring AudioCodes E-SBC.....	31
4.1	Step 1: IP Network Interfaces Configuration	32
4.1.1	Step 1a: Configure VLANs.....	33
4.1.2	Step 1b: Configure Network Interfaces.....	34
4.2	Step 2: Enable the SBC Application	36
4.3	Step 3: Configure Media Realms	37
4.4	Step 4: Configure SIP Signaling Interfaces	39
4.5	Step 5: Configure Proxy Sets	41
4.6	Step 6: Configure IP Profiles	47
4.7	Step 7: Configure IP Groups.....	55
4.8	Step 8: Configure Coders	57
4.9	Step 9: SIP TLS Connection Configuration	59
4.9.1	Step 9a: Configure the NTP Server Address.....	59
4.9.2	Step 9b: Configure the TLS version 1.0	60
4.9.3	Step 9c: Configure a Certificate.....	61
4.10	Step 10: Configure SRTP	66
4.11	Step 11: Configure Maximum IP Media Channels	67
4.12	Step 12: Configure IP-to-IP Call Routing Rules	68
4.13	Step 13: Configure IP-to-IP Manipulation Rules.....	80
4.14	Step 14: Configure Message Manipulation Rules	84
4.15	Step 15: Miscellaneous Configuration.....	94
4.15.1	Step 15a: Configure Call Forking Mode	94
4.15.2	Step 15b: Configure SBC Alternative Routing Reasons	95
4.15.3	Step 15c: Configure Registration Accounts.....	96
4.16	Step 16: Reset the E-SBC	97
A	AudioCodes INI file for VPN-based Configuration	99
B	AudioCodes INI file for Internet Registration-based Configuration.....	111
C	Configuring ATAs for FAX Support.....	123
C.1	Step 1: Configure the Endpoint Phone Number Table	123
C.2	Step 2: Configure Tel to IP Routing Table	124

C.3	Step 3: Configure Coders Table	124
C.4	Step 4: Configure SIP UDP Transport Type and Fax Signaling Method.....	125

Notice

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

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

© Copyright 2019 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: August-28-2019

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>.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
12224	Initial document release for Version 7.0 and Microsoft Skype for Business 2015.
12227	TELUS SIP Trunking product changed to IP Trunking Release 2; corporate formatting updates

Documentation Feedback

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

1 Introduction

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

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and TELUS Partners who are responsible for installing and configuring TELUS'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 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_7.00A.047.007
Protocol	▪ SIP/UDP (to the TELUS SIP Trunk) ▪ SIP/TCP or TLS (to the S4B FE Server)
Additional Notes	None

2.2 TELUS SIP Trunking Version

Table 2-2: TELUS Version

Vendor/Service Provider	TELUS
SSW Model/Service	Oracle AP6300 Session Border Controller GENBAND's EXPERIUS™ Application Server
Software Version	SBC: Oracle AP6300 Session Border Controller 7.1.2 MR 4 GENBAND's EXPERIUS Application Server MCP-17.0.22.12
Protocol	SIP
Additional Notes	IP Trunking Release 2

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

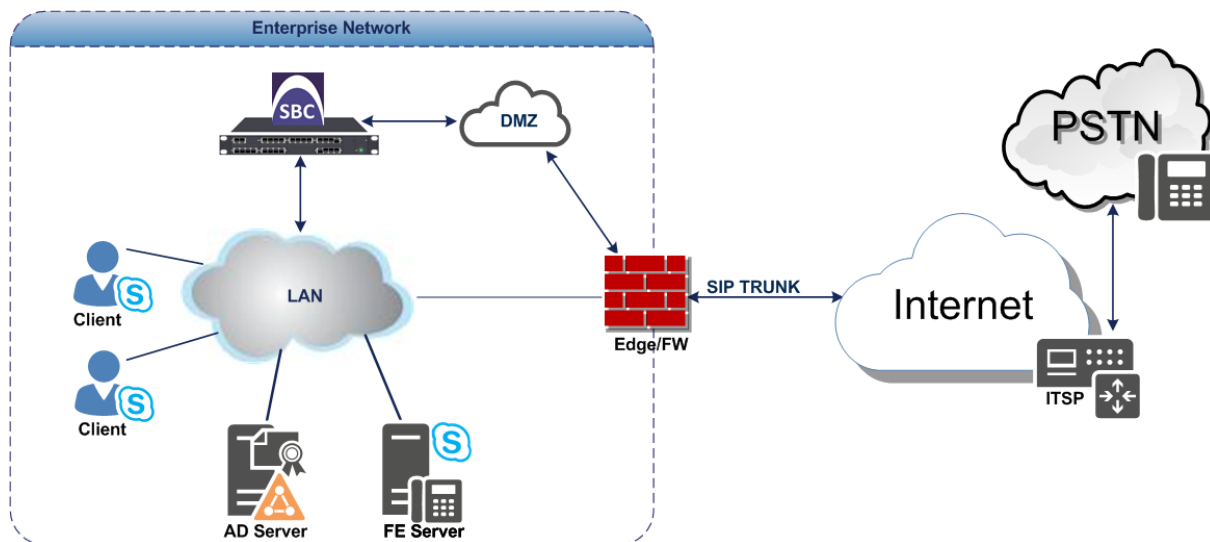
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and TELUS 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 TELUS'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 TELUS'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 TELUS SIP Trunk



Note: The topology can be based on two different TELUS connectivity methods - VPN-based or Internet registration-based. Throughout this document, where configuration depends on the specific connectivity method, the required configuration is indicated.

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 ▪ TELUS SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SIP-over-TLS transport type ▪ TELUS 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 ▪ TELUS SIP Trunk supports G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SRTP media type ▪ TELUS SIP Trunk operates with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Skype for Business Server 2015 and TELUS 's SIP Trunk.

This page is intentionally left blank.

3 Configuring Skype for Business Server 2015

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



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

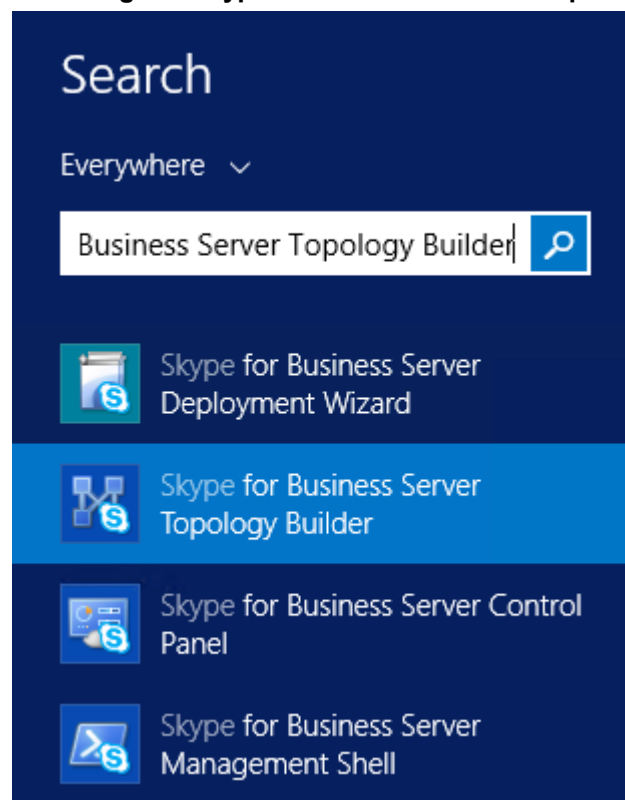
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

➤ **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**

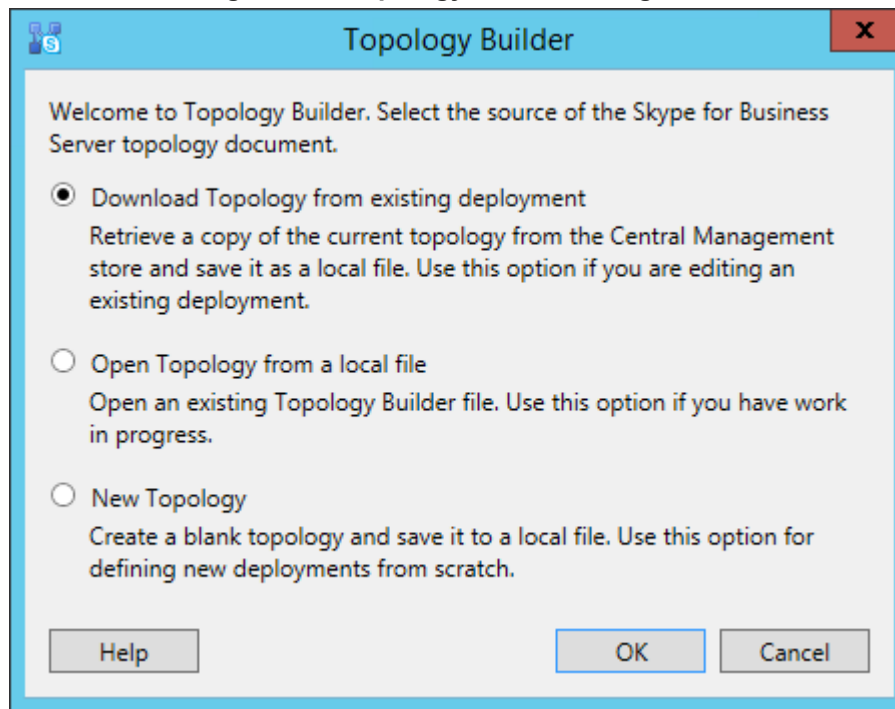
1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

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



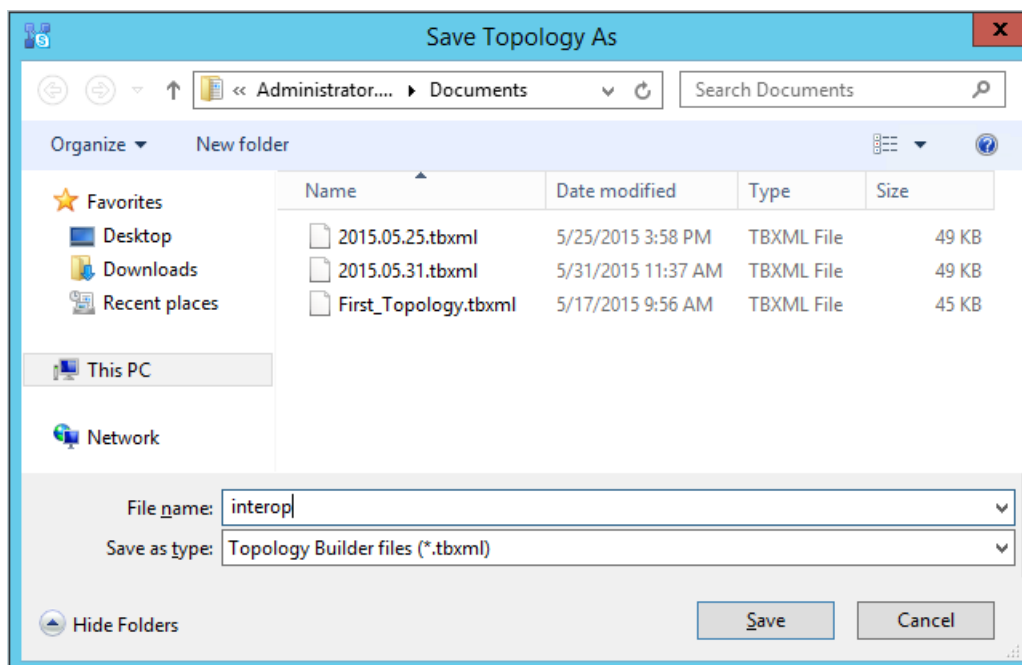
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

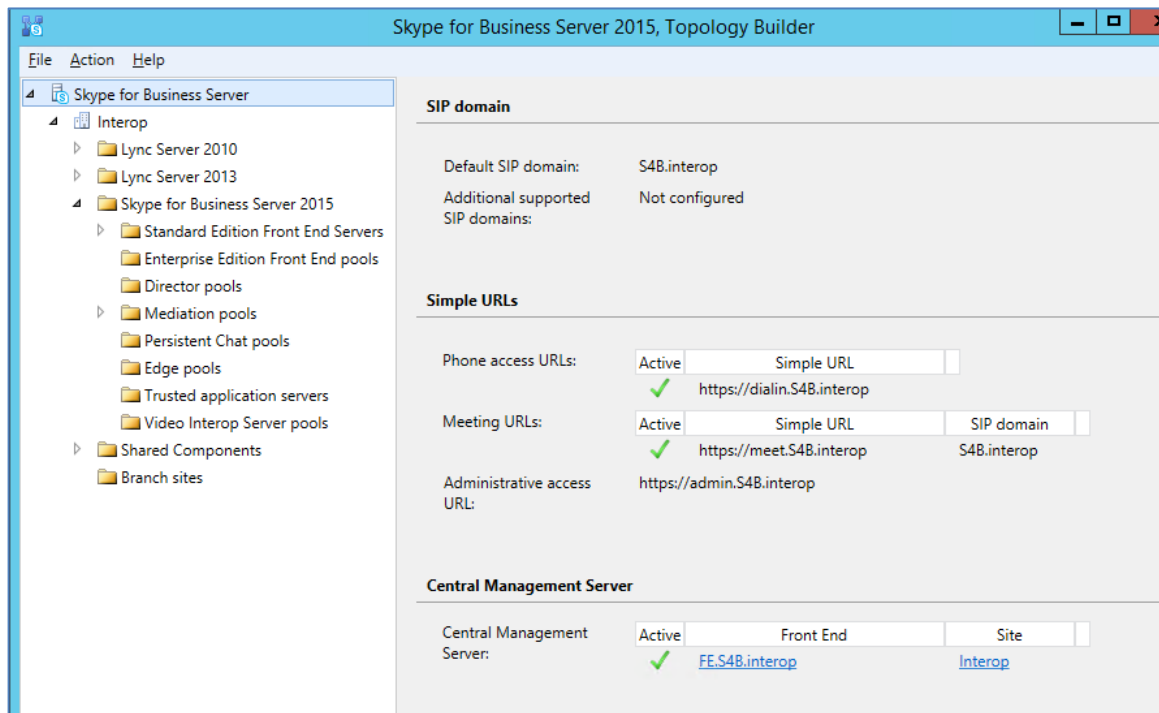
Figure 3-3: Save Topology Dialog Box



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

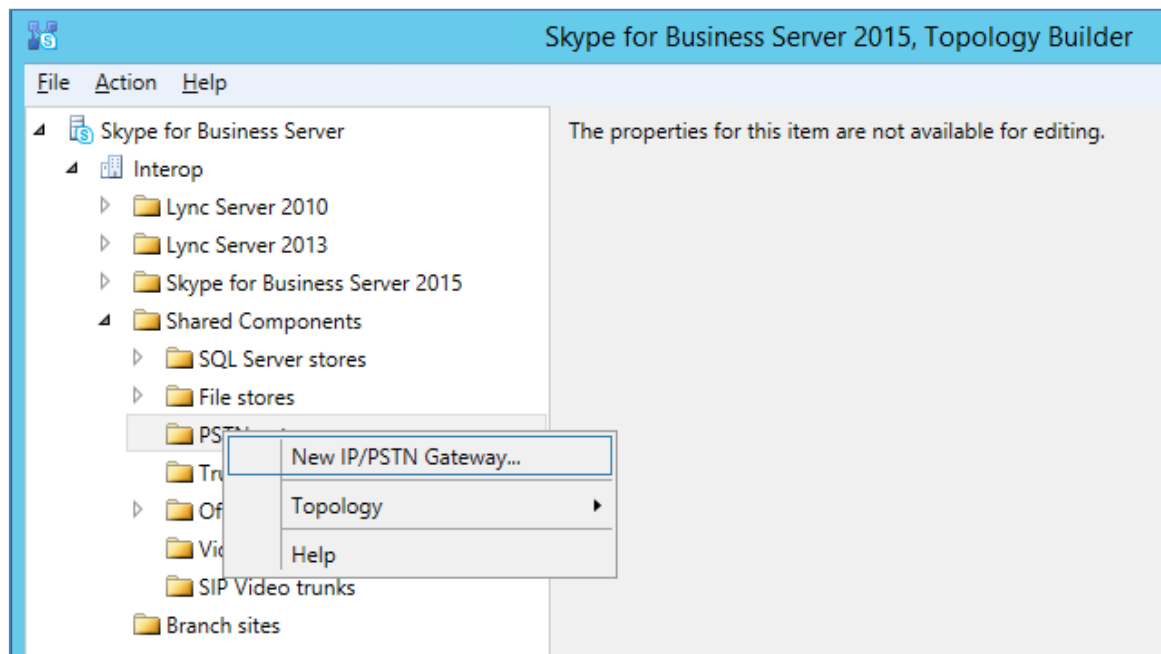
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



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

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN

The screenshot shows a dialog box titled "Define New IP/PSTN Gateway" with a close button (X) in the top right corner. The main heading is "Define the PSTN Gateway FQDN" next to a telephone icon. Below the heading, it says "Define the fully qualified domain name (FQDN) for the PSTN gateway." There is a text input field labeled "FQDN: *" containing the text "ITSP.S4B.interop". At the bottom, there are three buttons: "Help", "Back", and "Next" (which is highlighted in blue), and a "Cancel" button.

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 61).
6. Click **Next**; the following is displayed:

Figure 3-7: Define the IP Address

The screenshot shows the same dialog box titled "Define New IP/PSTN Gateway" with a close button (X) in the top right corner. The main heading is "Define the IP address" next to a telephone icon. Below the heading, there are two radio button options: "Enable IPv4" (which is selected) and "Enable IPv6". Under "Enable IPv4", there are two sub-options: "Use all configured IP addresses." (selected) and "Limit service usage to selected IP addresses." Below these is a text input field labeled "PSTN IP address:". The "Enable IPv6" section has the same sub-options and input field. At the bottom, there are three buttons: "Help", "Back", and "Next" (which is highlighted in blue), and a "Cancel" button.

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:**

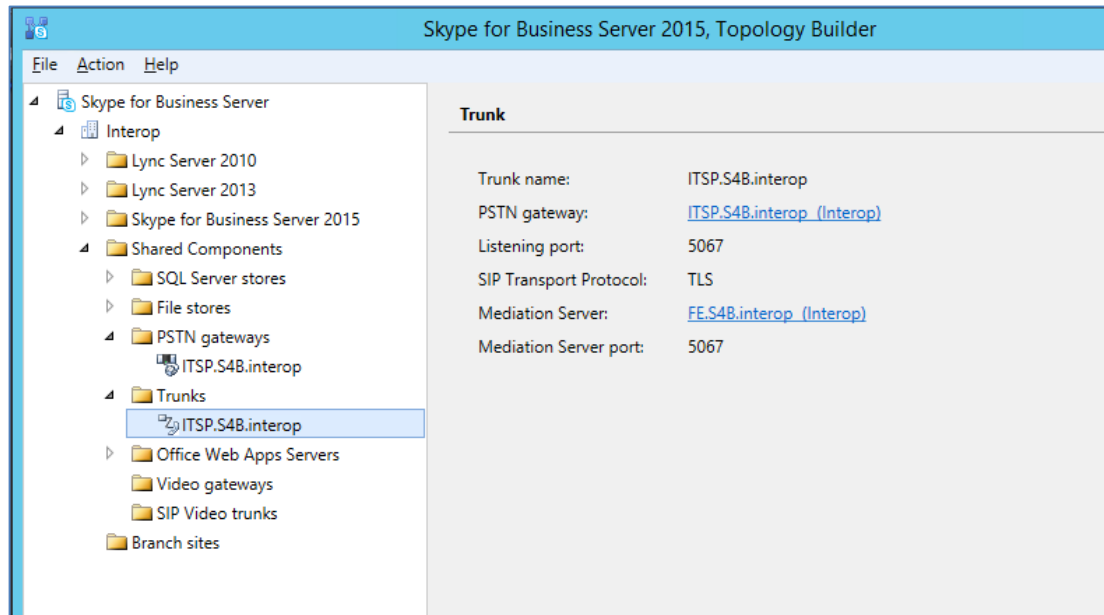
- When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
- The root trunk cannot be removed until the associated PSTN gateway is removed.

Figure 3-8: Define the Root Trunk

- 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 4.4 on page 39).
- 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 4.4 on page 39).
- c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
- d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
- e. Click **Finish**.

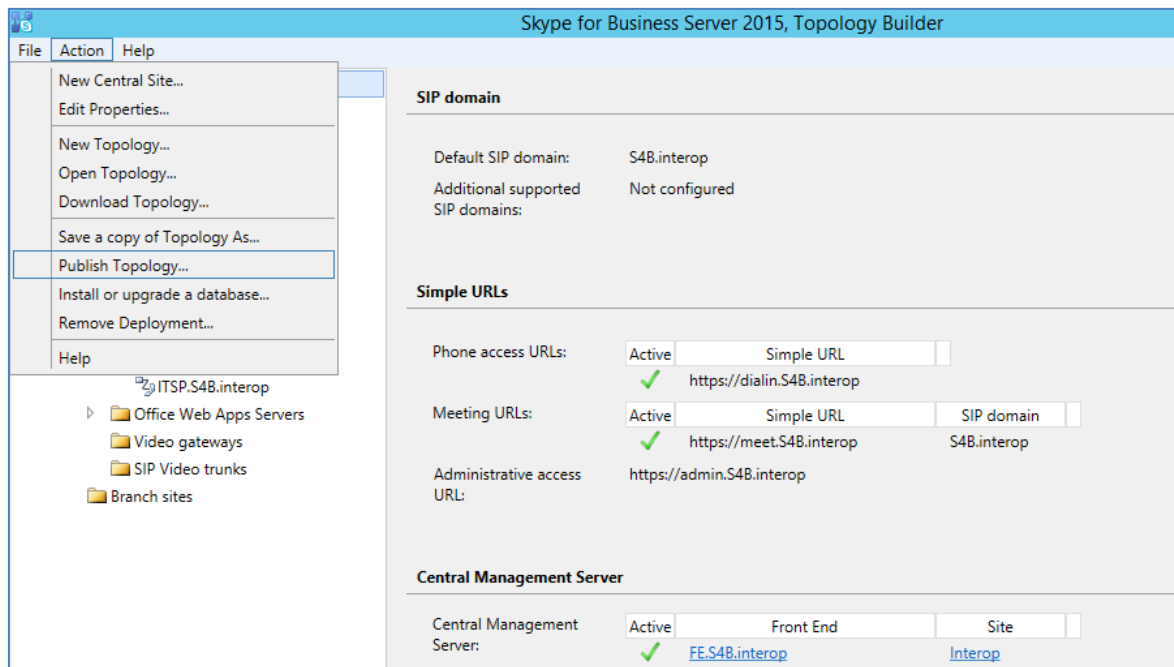
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



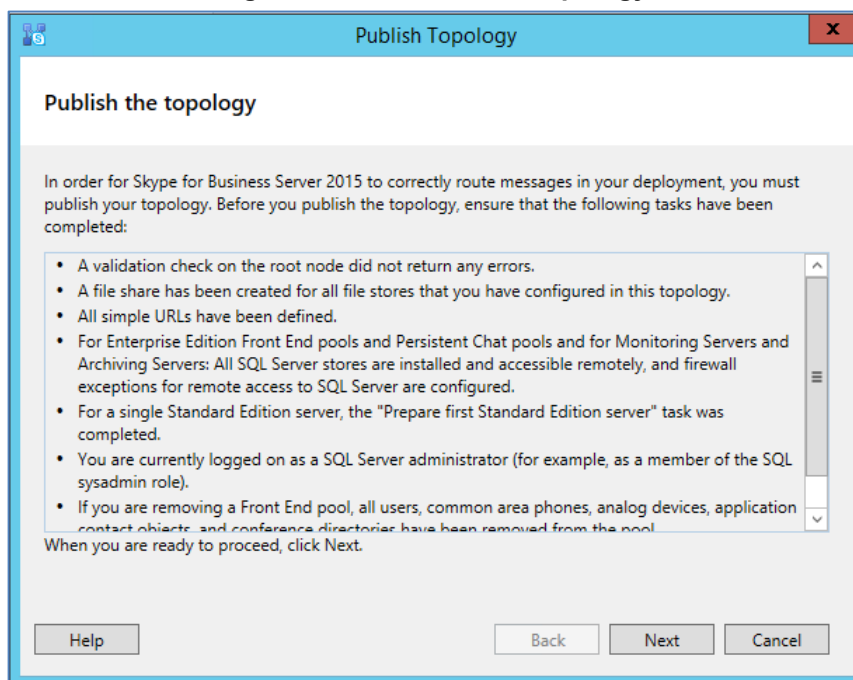
9. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



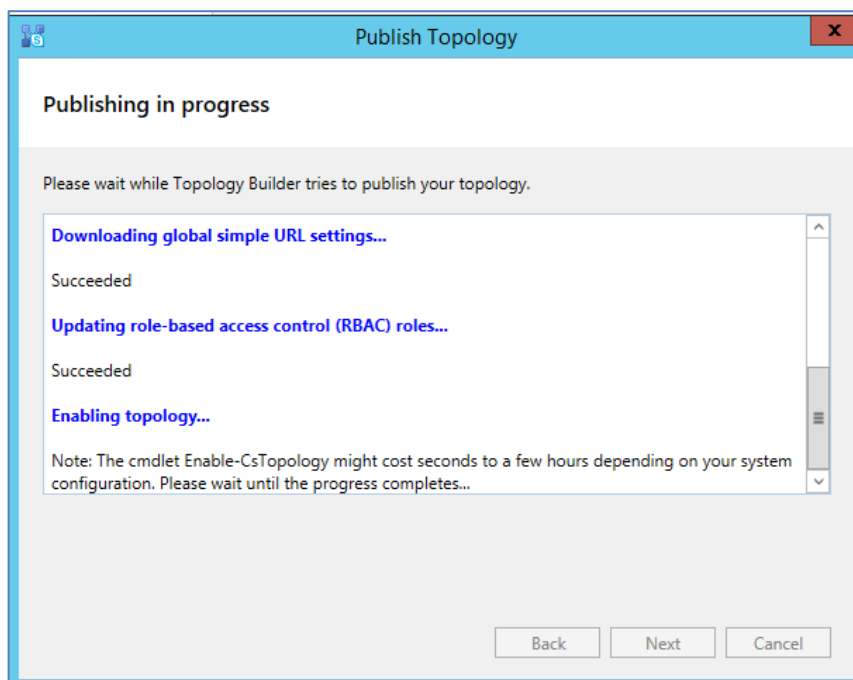
The following is displayed:

Figure 3-11: Publish the Topology



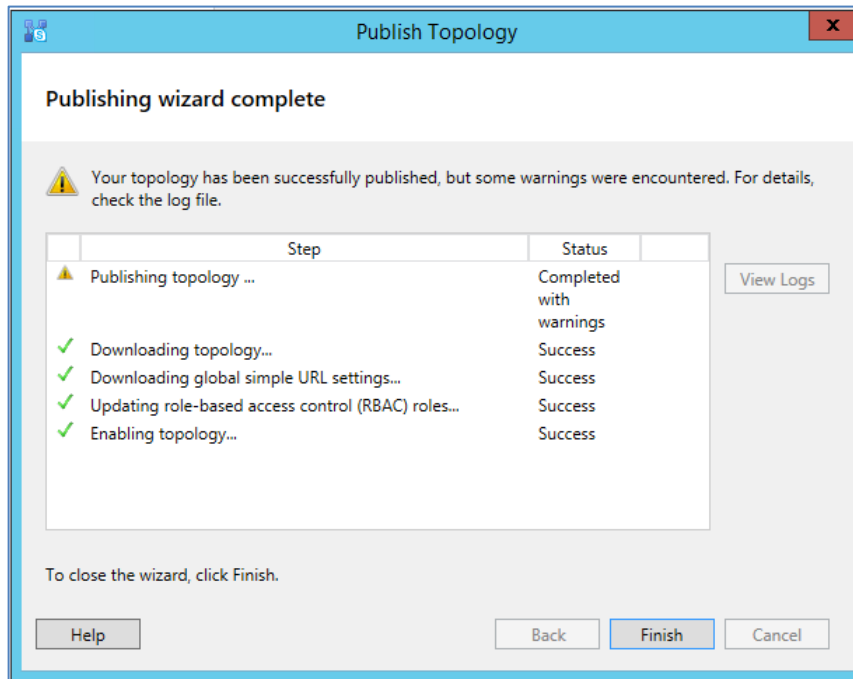
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



12. Click **Finish**.

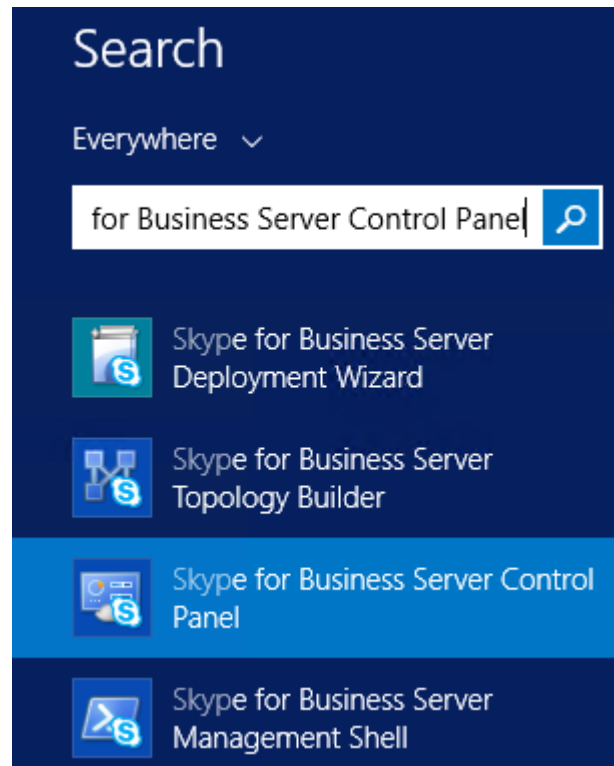
3.2 Configuring the "Route" on Skype for Business Server 2015

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:**

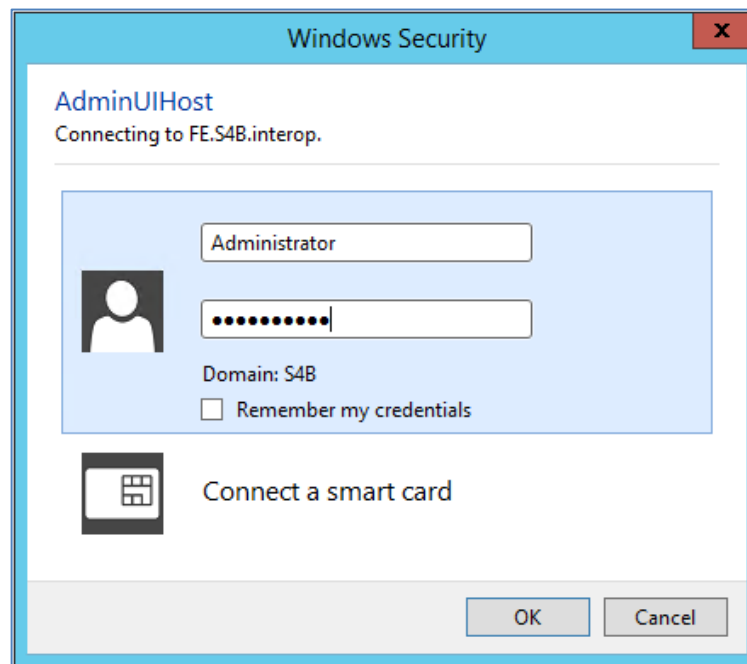
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

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



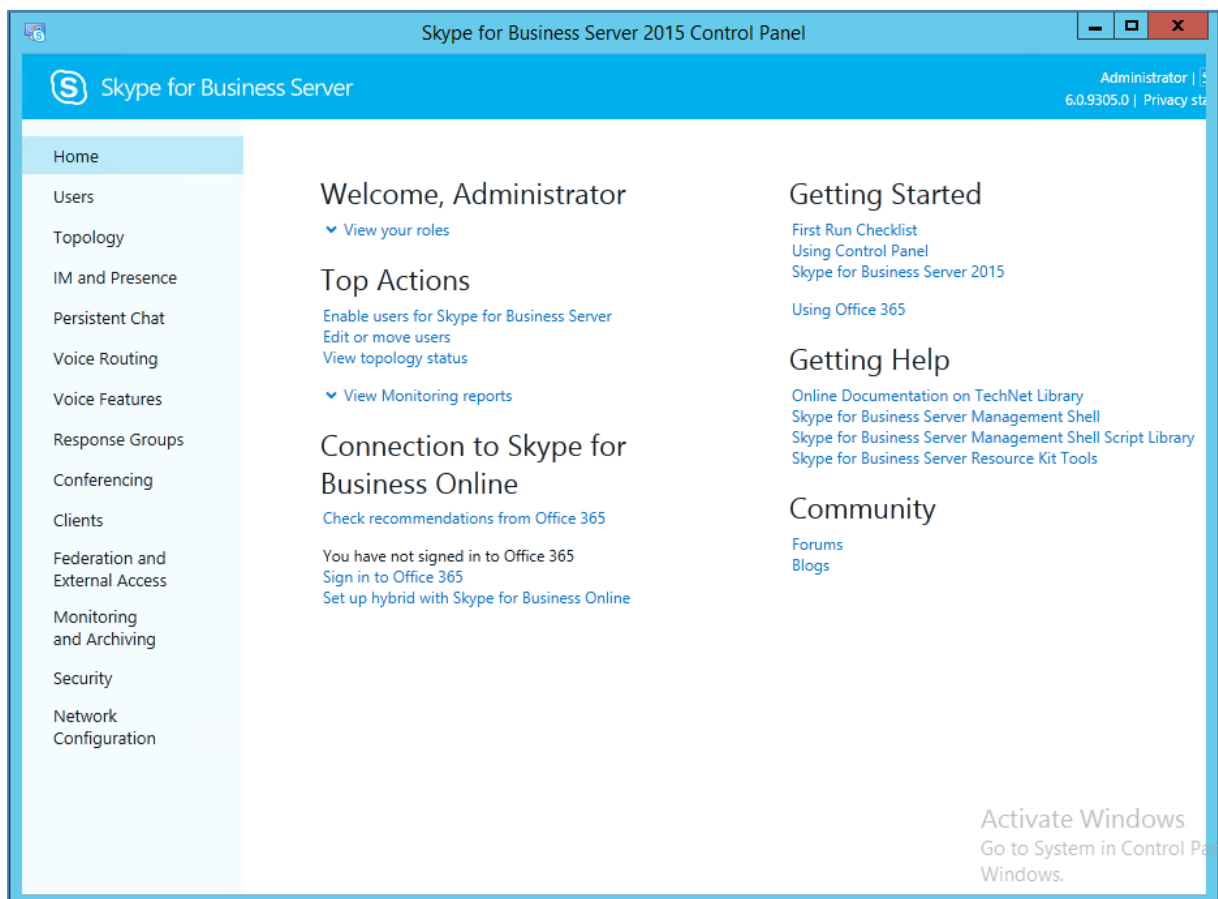
2. You are prompted to enter your login credentials:

Figure 3-15: Skype for Business Server Credentials



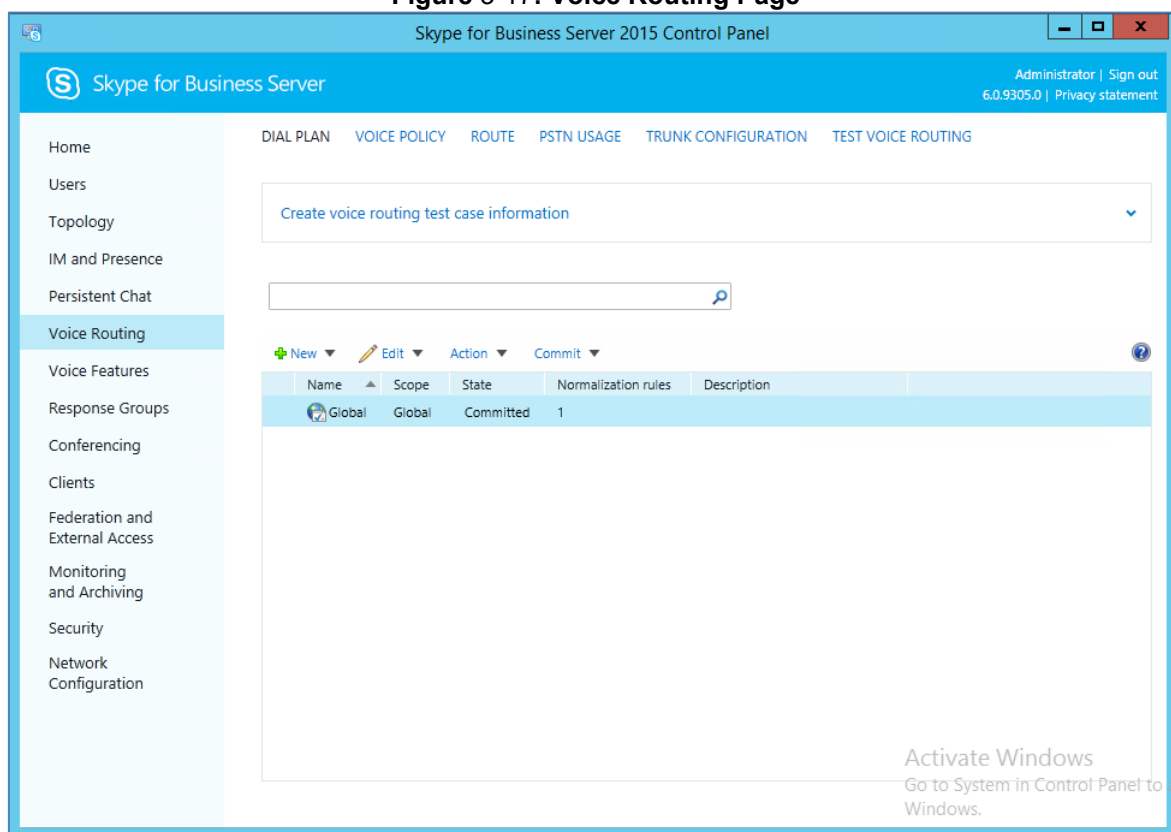
3. Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

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



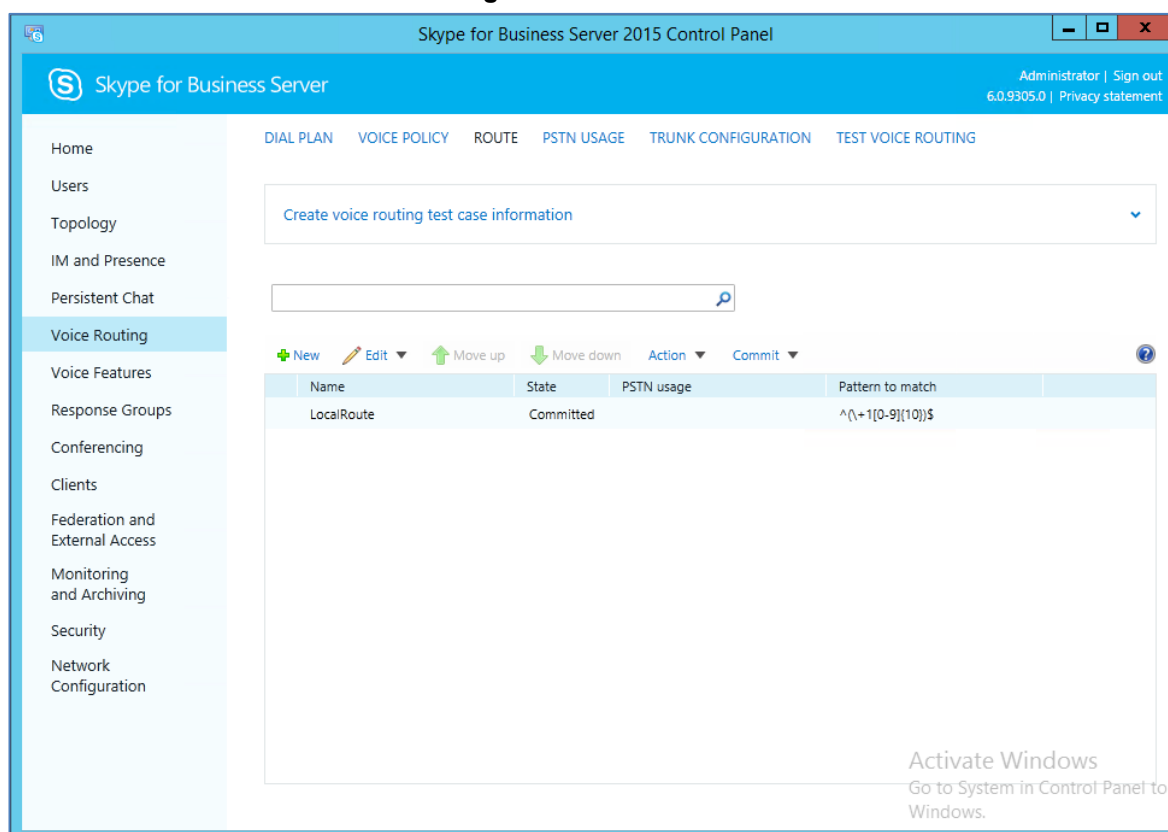
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



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

Figure 3-18: Route Tab



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

Figure 3-19: Adding New Voice Route

Skype for Business Server Administrator | Sign out 6.0.9305.0 | Privacy statement

Home DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Home Users Topology IM and Presence Persistent Chat **Voice Routing** Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network Configuration

Create voice routing test case information

New Voice Route OK Cancel

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. Add

Exceptions
Remove

Match this pattern: * *.* Edit Reset ?

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

Skype for Business Server

Home DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

New Voice Route OK Cancel

Match this pattern: * *.* Edit Reset ?

Suppress call transfer

Alternate call transfer

Associated trunk

Associated PSTN

PSTN usage record Associated voice policies

Select Trunk

Service	Site
PstnGateway:ITSP.S4B.interop	Interop

OK Cancel

- 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

Skype for Business Server

Home Users Topology IM and Presence Persistent Chat **Voice Routing** Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network Configuration

DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

New Voice Route

OK Cancel

Match this pattern: *

Edit Reset ?

☐ Suppress caller ID

Alternate caller ID:

Associated trunks:

PstnGateway:ITSP.S4B.interop Add... Remove

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

Figure 3-22: Associating PSTN Usage to Route

Skype for Business Server

Home Users Topology IM and Presence Persistent Chat **Voice Routing** Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network Configuration

DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

New Voice Route

OK Cancel

Associated trunks:

PstnGateway:ITSP.S4B.interop Add... Remove

Associated PSTN Usages

Select... Remove ↑ ↓

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

Skype for Business Server

DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

Search

+ New Edit Move up Move down Action Commit

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

Skype for Business Server

DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

Search

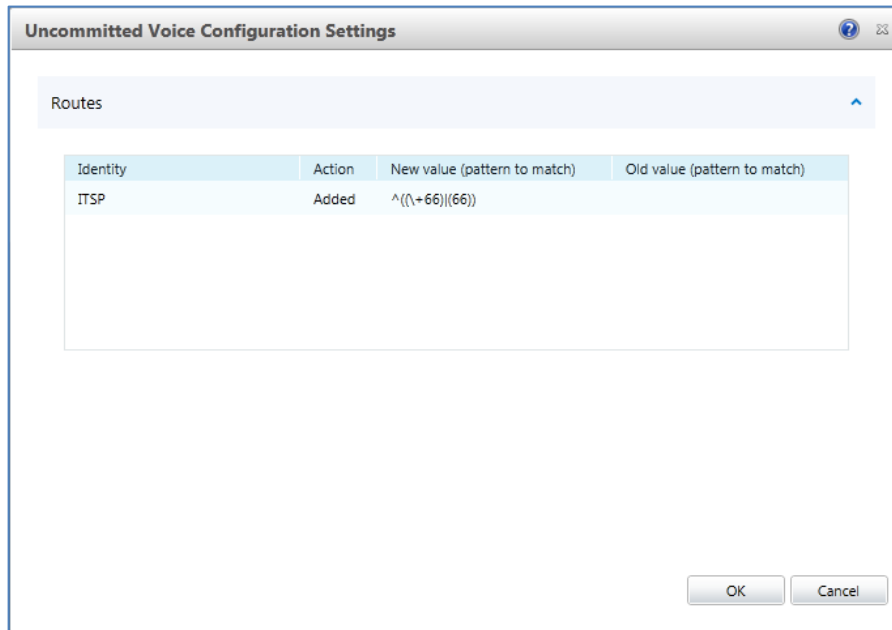
+ New Edit Move up Move down Action Commit

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

Review uncommitted changes
Commit all
Cancel selected changes
Cancel all uncommitted changes

The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



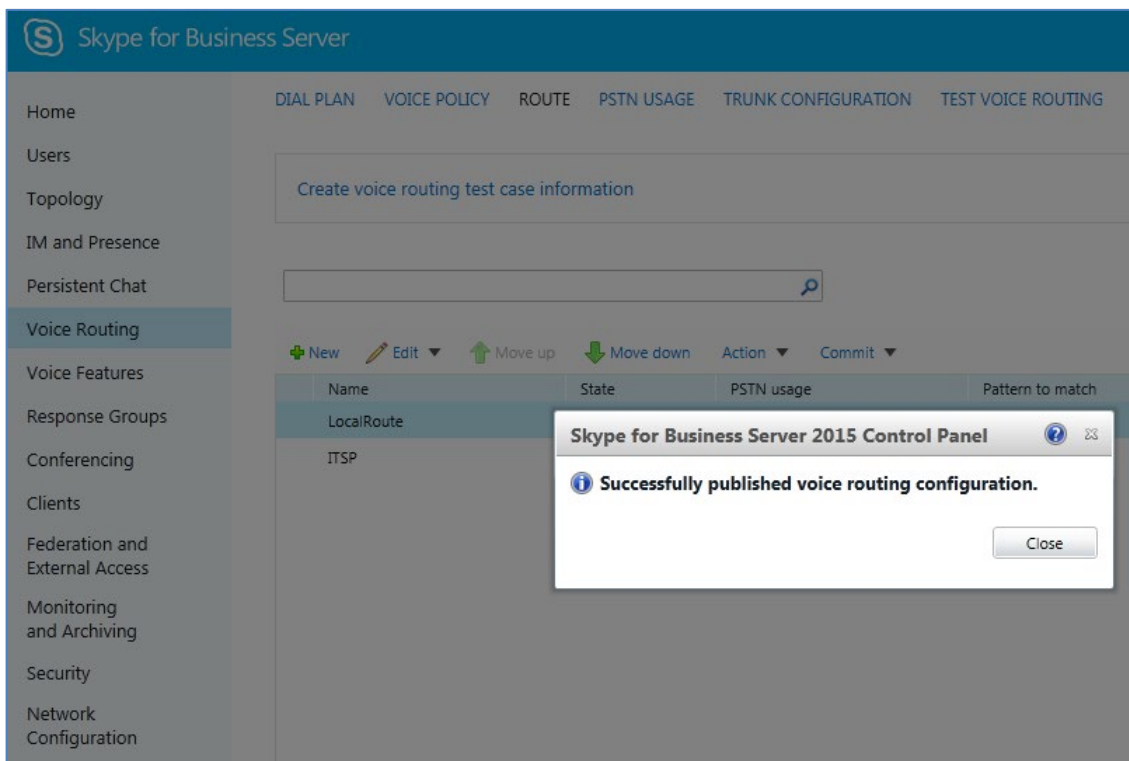
The dialog box titled "Uncommitted Voice Configuration Settings" contains a section labeled "Routes". Inside this section is a table with the following data:

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

At the bottom right of the dialog box are "OK" and "Cancel" buttons.

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



The screenshot shows the Skype for Business Server 2015 Control Panel. The left sidebar lists various configuration areas, with "Voice Routing" selected. The main area displays a table of voice routing configurations. A modal dialog box is overlaid on the table, displaying the message: "Successfully published voice routing configuration." with a "Close" button.

Name	State	PSTN usage	Pattern to match
LocalRoute			
ITSP			

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

Figure 3-27: Voice Routing Screen Displaying Committed Routes

The screenshot shows the Skype for Business Server administration interface. The left sidebar lists various configuration areas, with 'Voice Routing' selected. The top navigation bar includes tabs for DIAL PLAN, VOICE POLICY, ROUTE, PSTN USAGE, TRUNK CONFIGURATION, and TEST VOICE ROUTING. The main content area displays a table of 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 TELUS 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 47).

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

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

The screenshot shows the Skype for Business Server administration interface with the 'Trunk Configuration' tab selected. The left sidebar is the same as in Figure 3-27. The top navigation bar highlights the 'TRUNK CONFIGURATION' tab. The main content area displays a table of trunk configurations.

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:

The screenshot shows the Skype for Business Server administration console. The left-hand navigation pane is expanded to 'Voice Routing'. The main content area displays the 'New Trunk Configuration' page for the configuration 'PstnGateway:ITSP.S4B.interop'. At the top of the main area, there is a blue bar with the Skype logo and the text 'Skype for Business Server'. To the right of this bar, the user is logged in as 'Administrator' with a 'Sign out' link and the version '6.0.9305.0' and a 'Privacy statement' link. Below the blue bar, there are several tabs: 'DIAL PLAN', 'VOICE POLICY', 'ROUTE', 'PSTN USAGE', 'TRUNK CONFIGURATION' (which is selected), and 'TEST VOICE ROUTING'. The 'New Trunk Configuration' page has a title bar with 'OK' and 'Cancel' buttons. The configuration details are as follows: 'Scope: Pool', 'Name: PstnGateway:ITSP.S4B.interop', 'Description: ' (empty), 'Maximum early dialogs supported: 20', 'Encryption support level: Required', 'Refer support: Enable sending refer to the gateway', and several checkboxes: 'Enable media bypass' (checked), 'Centralized media processing' (checked), 'Enable RTP latching' (unchecked), 'Enable forward call history' (checked), 'Enable forward P-Asserted-Identity data' (unchecked), and 'Enable outbound routing failover timer' (checked).

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

This page is intentionally left blank.

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 TELUS 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 - TELUS 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*).

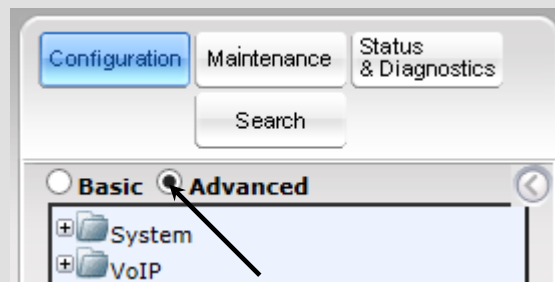
Notes:

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

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

For more information about the Software 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.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Advanced-menu display mode. To do this, select the **Advanced** option, as shown below:



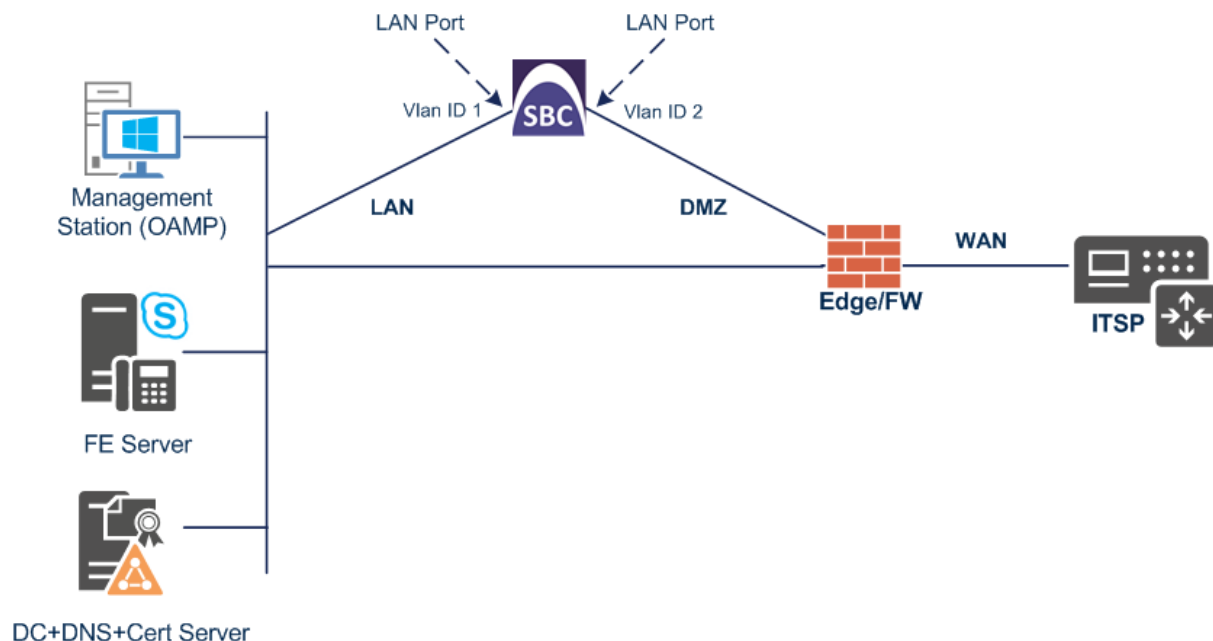
- When the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

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
 - TELUS 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 WAN 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)
 - WAN (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 "Voice")
- WAN VoIP (assigned the name "WANSP")

➤ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).
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 Table

The screenshot shows the 'Ethernet Device Table' interface. At the top, there are buttons for 'Add +', 'Edit', 'Delete', and 'Show / Hide'. Below these is a search bar with a dropdown menu set to 'All' and a 'Search' button. The table itself has five columns: 'Index', 'VLAN ID', 'Underlying Interface', 'Name', and 'Tagging'. There are two rows of data. The first row has Index 0, VLAN ID 1, Underlying Interface GROUP_1, Name vlan 1, and Tagging Untagged. The second row has Index 1, VLAN ID 2, Underlying Interface GROUP_2, Name vlan 2, and Tagging Untagged. At the bottom of the table, there is a pagination bar showing 'Page 1 of 1' and a 'View 1 - 2 of 2' indicator.

Ethernet Device Table				
Add + Edit Delete Show / Hide All Search in table Search				
Index	VLAN ID	Underlying Interface	Name	Tagging
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged
Page 1 of 1 10 View 1 - 2 of 2				

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 "Voice")
- WAN VoIP (assigned the name "WANSP")

➤ To configure the IP network interfaces:

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
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
IP Address	10.15.17.55 (IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Default Gateway	10.15.0.1
VLAN ID	1
Interface Name	Voice (arbitrary descriptive name)
Primary DNS Server IP Address	10.15.27.1
Underlying Device	vlan 1

3. Add a network interface for the WAN side:
 - a. Enter **1**, and then click **Add Index**.
 - b. Configure the interface as follows:

Parameter	Value
Application Type	Media + Control
IP Address	195.189.192.158 Note: For Internet registration-based topology, use a public IP address. For VPN-based topology, use a private IP address.
Prefix Length	25 (for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
VLAN ID	2
Interface Name	WANSP
Primary DNS Server IP Address	80.179.52.100
Secondary DNS Server IP Address	80.179.55.100
Underlying Device	vlan 2

4. Click **Apply**, and then **Done**.

The configured IP network interfaces are shown below:

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

▼ Interface Table

Add +

Edit ✎

Delete 🗑

Show / Hide 📄

▼ All

Search in table

Search 🔍

Index ↕	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	Voice	OAMP + Media +	IPv4 Manual	10.15.17.55	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WANSP	Media + Control	IPv4 Manual	195.189.192.158	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

⏪ ⏩

Page 1 of 1

10 ▼

View 1 - 2 of 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 (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.16 on page 97).

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 Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
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	Voice
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

The screenshot shows the 'Edit Row' dialog box for configuring a Media Realm. The dialog has a title bar with 'Edit Row' and a close button. The fields and their values are:

- Index: 0
- Name: MRLan
- IPv4 Interface Name: Voice
- Port Range Start: 6000
- Number Of Media Session Legs: 100
- Port Range End: 6990
- Default Media Realm: No
- QoE Profile: None
- BW Profile: None

At the bottom of the dialog are 'Save' and 'Cancel' buttons. Five arrows on the left point to the Index, Name, IPv4 Interface Name, Port Range Start, and Number Of Media Session Legs fields.

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Name	MRWan (arbitrary name)
IPv4 Interface Name	WANSP
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

The 'Add Row' dialog box contains the following fields and values:

- Index: 1
- Name: MRWan
- IPv4 Interface Name: WANSP
- Port Range Start: 7000
- Number Of Media Session Legs: 100
- Port Range End: -1
- Default Media Realm: No
- QoE Profile: None
- BW Profile: None

Buttons at the bottom: Add, Cancel.

The configured Media Realms are shown in the figure below:

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

Media Realm Table

Add + Edit Edit Delete Delete Show / Hide Show / Hide

All Search in table Search

Index	Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End	Default Media Realm
0	MRLan	Voice	6000	100	6990	No
1	MRWan	WANSP	7000	100	7990	No

Page 1 of 1 10 View 1 - 2 of 2

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 Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
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
Interface Name	S4B
Network Interface	Voice
Application Type	SBC
UDP Port (supporting FAX Analog Telephone Adaptor - ATA)	5060
TCP Port (set to 0 if using TLS)	5060
TLS Port (set to 0 if using TCP)	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
Interface Name	TELUS
Network Interface	WANSP
Application Type	SBC
UDP Port	5060
TCP and TLS	0 or 5061 (For Internet Registration-based configuration)
Media Realm	MRWan

The configured SIP Interfaces are shown in the figure below:

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

SIP Interface Table

Add +

Edit ✎

Delete 🗑

Show / Hide 📄

▼ All

Search in table

Search 🔍

Index ⬆	Name	SRD	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Encapsulating Protocol	Media Realm
0	S4B	DefaultSRD	Voice	SBC	5060	0	5067	No encapsulat	MRLan
1	TELUS	DefaultSRD	WANSP	SBC	5060	0	0	No encapsulat	MRWan

⏪

⏴

Page 1 of 1

⏵

⏩

10 ▼

View 1 - 2 of 2



Note: Unlike previous software releases where configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups) were associated with each other using table row indices, Version 7.0 uses the string **names** of the configuration entities. 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
- TELUS SIP Trunk
- Fax supporting Analog Telephony Adapter (ATA) device (optional)

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 page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the Skype for Business Server 2015. You can use the default Proxy Set (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	S4B
SBC IPv4 SIP Interface	S4B
Proxy Keep Alive	Using Options
Redundancy Mode	Homing
Proxy Load Balancing Method	Round Robin
Proxy Hot Swap	Enable

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

Parameter	Value
Index	0
SRD	DefaultSRD
Name	S4B
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	S4B
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Redundancy Mode	Homing
Proxy Load Balancing Method	Round Robin
DNS Resolve Method	
Proxy Hot Swap	Enable
Keep-Alive Failure Responses	
Classification Input	IP Address only
TLS Context Name	default

Buttons: Save, Cancel

3. Configure a Proxy Address Table for Proxy Set for Skype for Business Server 2015:
 - a. Go to **Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table** > **Proxy Address Table**.

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

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

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

Buttons: Save, Cancel

4. Configure a Proxy Set for the TELUS SIP Trunk:

Parameter	Value
Index	1
Name	TELUS
SBC IPv4 SIP Interface	TELUS
Proxy Keep Alive	Using Options

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

The screenshot shows the 'Edit Row' configuration window for a Proxy Set. The window has a title bar 'Edit Row' with a close button. The main area contains a list of parameters and their values, each with a dropdown arrow. The parameters are:

- Index: 1
- SRD: DefaultSRD
- Name: TELUS
- Gateway IPv4 SIP Interface: None
- SBC IPv4 SIP Interface: TELUS
- Proxy Keep-Alive: Using OPTIONS
- Proxy Keep-Alive Time [sec]: 60
- Redundancy Mode: (empty)
- Proxy Load Balancing Method: Disable
- DNS Resolve Method: (empty)
- Proxy Hot Swap: Disable
- Keep-Alive Failure Responses: (empty)
- Classification Input: IP Address only
- TLS Context Name: None

At the bottom right, there are 'Save' and 'Cancel' buttons. Five arrows point to the first five rows of the configuration list.

- a. Configure a Proxy Address Table for Proxy Set 1:
- b. Navigate to **Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table** > **Proxy Address Table**.

Parameter	Value
Index	0
Proxy Address	209.115.158.100:5060 (IP address / FQDN and destination port)
Transport Type	UDP

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

The screenshot shows a dialog box titled "Edit Row" with a close button (X) in the top right corner. Inside the dialog, there are three input fields:

- Index:** A text box containing the value "0".
- Proxy Address:** A text box containing the value "209.115.158.100:5060".
- Transport Type:** A dropdown menu with "UDP" selected.

At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

5. Configure a Proxy Set for Fax supporting an ATA device (if required):

Parameter	Value
Index	2
Name	Fax
SBC IPv4 SIP Interface	S4B

Figure 4-13: Configuring Proxy Set for Fax ATA Device

The screenshot shows the 'Edit Row' configuration window for a Proxy Set. The window has a title bar with 'Edit Row' and a close button. The main area contains a list of parameters and their values:

- Index: 2
- SRD: DefaultSRD
- Name: Fax
- Gateway IPv4 SIP Interface: None
- SBC IPv4 SIP Interface: S4B
- Proxy Keep-Alive: Disable
- Proxy Keep-Alive Time [sec]: 60
- Redundancy Mode: (empty)
- Proxy Load Balancing Method: Disable
- DNS Resolve Method: (empty)
- Proxy Hot Swap: Disable
- Keep-Alive Failure Responses: (empty)
- Classification Input: IP Address only
- TLS Context Name: None

At the bottom right, there are 'Save' and 'Cancel' buttons. Three arrows on the left side of the window point to the 'Index', 'Name', and 'SBC IPv4 SIP Interface' fields respectively.

- c. Configure a Proxy Address Table for Proxy Set 2:
- d. Navigate to **Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table** > **Proxy Address Table**.

Parameter	Value
Index	0
Proxy Address	10.15.17.12 (IP address / FQDN and destination port)
Transport Type	UDP

Figure 4-14: Configuring Proxy Address for Fax ATA Device

Edit Row

Index: 0

Proxy Address: 10.15.17.12

Transport Type: UDP

Save Cancel

The configured Proxy Sets are shown in the figure below:

Figure 4-15: Configured Proxy Sets in Proxy Sets Table

▼ Proxy Sets Table

Add + Edit Delete Show / Hide

▼ All Search in table Search

Index	Name	SRD	Gateway IPv4 SIP Interface	SBC IPv4 SIP Interface	Proxy Keep-Alive Time [sec]	Redundancy Mode	Proxy Hot Swap
0	S4B	DefaultSRD (#0)	None	S4B	60	Homing	Enable
1	TELUS	DefaultSRD (#0)	None	TELUS	60		Disable
2	Fax	DefaultSRD (#0)	None	S4B	60		Disable

Page 1 of 1 10 View 1 - 3 of 3

4.6 Step 6: 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
- TELUS 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 Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Name	S4B
Symmetric MKI	Enable
MKI Size	1
Reset SRTP State Upon Re-key	Enable
Generate SRTP keys mode:	Always

Figure 4-16: Configuring IP Profile for Skype for Business Server 2015 – Common Tab

The screenshot shows the 'Edit Row' dialog box for configuring an IP Profile. The 'Common' tab is selected. The 'Index' is 1. The 'Name' is S4B. Other parameters include Dynamic Jitter Buffer Minimum Delay [msec] (10), Dynamic Jitter Buffer Optimization Factor (10), Jitter Buffer Max Delay [msec] (300), RTP IP DiffServ (46), Signaling DiffServ (40), Silence Suppression (Disable), RTP Redundancy Depth (0), Echo Canceled (Line), Broken Connection Mode (Disconnect), Input Gain (-32 to 31 dB) (0), Voice Volume (-32 to 31 dB) (0), and Media IP Version (Only IPv4). The 'Save' and 'Cancel' buttons are at the bottom right.

4. Click the **SBC Signaling** tab, and then configure the parameters as follows:

Parameter	Value
Remote Update Support	Not Supported
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
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)
Remote Early Media RTP Detection Behavior	By Media (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)

Figure 4-17: Configuring IP Profile for Skype for Business Server 2015 – SBC Signaling Tab

The screenshot shows the 'Edit Row' dialog box with the 'SBC Signaling' tab selected. The 'Index' is set to 1. The parameters and their values are as follows:

Parameter	Value
PRACK Mode	Optional
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	Not Supported
Remote re-INVITE	Supported only with
Remote Delayed Offer Support	Not Supported
User Registration Time	0
NAT UDP Registration Time	-1
NAT TCP Registration Time	-1

Buttons at the bottom: Save, Cancel.

5. Click the **SBC Media** tab, and then configure the parameters as follows:

Parameter	Value
Extension Coders Group ID	Coders Group 1
SBC Media Security Mode	SRTP
Enforce MKI Size	Enforce
RFC 2833 Mode	Extend
RFC 2833 DTMF Payload Type	101

Figure 4-18: Configuring IP Profile for Skype for Business Server 2015 – SBC Media Tab

The screenshot shows the 'Edit Row' configuration window for the SBC Media tab. The window has a title bar 'Edit Row' with a close button. Below the title bar is an 'Index' field with the value '1'. There are four tabs: 'Common', 'GW', 'SBC Signaling', and 'SBC Media' (which is selected and highlighted in orange). The 'SBC Media' tab contains the following parameters and their values:

- Transcoding Mode: Only If Required
- Extension Coders: Coders Group 1
- Allowed Audio Coders: None
- Allowed Coders Mode: Restriction
- Allowed Video Coders: None
- Allowed Media Types: (empty field)
- SBC Media Security Mode: SRTP
- Media Security Method: SDES
- Enforce MKI Size: Enforce
- SDP Remove Crypto Lifetime: No
- RFC 2833 Mode: Extend
- Alternative DTMF Method: As Is

At the bottom right of the window are 'Save' and 'Cancel' buttons.

➤ To configure an IP Profile for the TELUS SIP Trunk:

1. Click **Add**.
2. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Name	TELUS

Figure 4-19: Configuring IP Profile for TELUS SIP Trunk – Common Tab

The screenshot shows a configuration window titled "Edit Row" with a close button (X) in the top right corner. At the top, there is a field for "Index" with the value "2". Below this are four tabs: "Common" (highlighted in orange), "GW", "SBC Signaling", and "SBC Media". Under the "Common" tab, there is a list of parameters, each with a corresponding input field or dropdown menu:

- Name: TELUS
- Dynamic Jitter Buffer Minimum Delay [msec]: 10
- Dynamic Jitter Buffer Optimization Factor: 10
- Jitter Buffer Max Delay [msec]: 300
- RTP IP DiffServ: 46
- Signaling DiffServ: 40
- Silence Suppression: Disable (dropdown menu)
- RTP Redundancy Depth: 0
- Echo Canceler: Line (dropdown menu)
- Broken Connection Mode: Ignore (dropdown menu)
- Input Gain (-32 to 31 dB): 0

At the bottom right of the window are "Save" and "Cancel" buttons. Two arrows on the left side of the image point to the "Index" field and the "Common" tab.

3. Click the **SBC Signaling** tab, and then configure the parameters as follows:

Parameter	Value
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Play RBT To Transferee	Yes
Remote Can Play Ringback	No (required, as Skype for Business Server 2015 does not provide a ringback tone for incoming calls)

Figure 4-20: Configuring IP Profile for TELUS SIP Trunk – SBC Signaling Tab

The screenshot shows the 'Edit Row' dialog box with the 'SBC Signaling' tab selected. The 'Index' is set to 2. The parameters and their values are as follows:

Parameter	Value
PRACK Mode	Transparent
P-Asserted-Identity Header Mode	Add
Diversion Header Mode	As Is
History-Info Header Mode	As Is
Session Expires Mode	Transparent
Remote Update Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Supported
User Registration Time	0
NAT UDP Registration Time	-1
NAT TCP Registration Time	-1

Buttons: Save, Cancel

4. Click the **SBC Media** tab, and then configure the parameters as follows:

Parameter	Value
Extension Coders	Coders Group 2
Allowed Coders	Coders Group 2
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer)
SBC Media Security Mode	RTP

Figure 4-21: Configuring IP Profile for TELUS SIP Trunk – SBC Media Tab

The screenshot shows the 'Add Row' dialog box for configuring the SBC Media tab. The 'Index' is set to 2. The 'SBC Media' tab is selected. The parameters and their values are as follows:

- Transcoding Mode: Only If Required
- Extension Coders: Coders Group 2
- Allowed Coders: Coders Group 2
- Allowed Coders Mode: Preference
- Allowed Video: None
- Allowed Media Types: (empty)
- SBC Media Security Mode: RTP
- Media Security Method: SDES
- Enforce MKI Size: Don't enforce
- SDP Remove Crypto LifeTime: No
- RFC 2833 Mode: As Is
- Alternative DTMF Method: As Is
- RFC 2833 DTMF Payload Type: 0
- Fax Coders: None

Arrows point to the following parameters: Transcoding Mode, Extension Coders, Allowed Coders, Allowed Coders Mode, and SBC Media Security Mode.

➤ To configure an IP Profile for the FAX supporting ATA:

1. Click **Add**.
2. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	3
Name	Fax

Figure 4-22: Configuring IP Profile for FAX ATA – Common Tab

The screenshot shows the 'Edit Row' dialog box with the following configuration:

- Index:** 3
- Tabs:** Common (selected), GW, SBC Signaling, SBC Media
- Name:** Fax
- Dynamic Jitter Buffer Minimum Delay [msec]:** 10
- Dynamic Jitter Buffer Optimization Factor:** 10
- Jitter Buffer Max Delay [msec]:** 300
- RTP IP DiffServ:** 46
- Signaling DiffServ:** 40
- Silence Suppression:** Disable
- RTP Redundancy Depth:** 0
- Echo Canceler:** Line
- Broken Connection Mode:** Disconnect
- Input Gain (-32 to 31 dB):** 0
- Voice Volume (-32 to 31 dB):** 0
- Media IP Version:** Only IPv4

Buttons at the bottom: Save, Cancel.

3. Click the **SBC Signaling** tab, and then configure the parameters as follows:

Parameter	Value
All Parameters	Leave as Default

4. Click the **SBC Media** tab, and then configure the parameters as follows:

Parameter	Value
All Parameters	Leave as default

4.7 Step 7: 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 the LAN
- TELUS SIP Trunk located on the WAN
- Fax supporting the ATA device located on the LAN (if required)

➤ To configure IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the Skype for Business Server 2015. You can use the default IP Group (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	S4B
Type	Server
Proxy Set	S4B
IP Profile	S4B
Media Realm	MRLan
SIP Group Name	(according to ITSP requirement)

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

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

4. Configure an IP Group for Fax supporting the ATA device.

Parameter	Value
Index	2
Name	Fax
Type	Server
Proxy Set	Fax
IP Profile	Fax
Media Realm	MRLan
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-23: Configured IP Groups in IP Group Table

The screenshot shows a web interface titled "IP Group Table". At the top, there are buttons for "Add +", "Edit", "Delete", and "Show / Hide". Below these is a search bar with a dropdown menu set to "All" and a "Search" button. The main area contains a table with the following data:

Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulation Set	Outbound Message Manipulation Set
0	S4B	DefaultSR Server	Server	Not Configured	S4B	S4B	MRLan	195.189.192.158	Enable	-1	-1
1	TELUS	DefaultSR Server	Server	Not Configured	TELUS	TELUS	MRWan	ipinet4.com	Enable	-1	4
2	Fax	DefaultSR Server	Server	Not Configured	Fax	Fax	MRLan	195.189.192.158	Enable	-1	-1

At the bottom of the table, there is a pagination bar showing "Page 1 of 1" and a "View 1 - 3 of 3" indicator.

4.8 Step 8: 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 TELUS 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 TELUS SIP Trunk.

Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 47).

➤ **To configure coders:**

1. Open the Coder Group Settings (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders Group Settings**).
2. Configure a Coder Group for Skype for Business Server 2015:

Parameter	Value
Coder Group ID	1
Coder Name	▪ G.711 U-law ▪ G.711 A-law
Silence Suppression	Enable (for both coders)

Figure 4-24: Configuring Coder Group for Skype for Business Server 2015

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 TELUS SIP Trunk:

Parameter	Value
Coder Group ID	2
Coder Name	▪ G.711 U-law ▪ G.729

Figure 4-25: Configuring Coder Group for TELUS SIP Trunk

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711U-law	20	64	0	Disabled	
G.729	20	8	18	Disabled	

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the TELUS SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the TELUS SIP Trunk (see Section 4.6 on page 47).

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

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Audio Coders Group**).
2. Configure an Allowed Coder as follows:

Parameter	Value
Allowed Audio Coders Group ID	2
Coder Name	▪ G.711 U-law ▪ G.729

Figure 4-26: Configuring Allowed Coders Group for TELUS SIP Trunk

3. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).

Figure 4-27: SBC Preferences Mode

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

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 Application Settings page (**Configuration** tab > **System** > **Time And Date**).
2. In the 'NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.27.1**).

Figure 4-28: 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

3. Click **Submit**.

4.9.2 Step 9b: Configure the TLS version 1.0

This step describes how to configure the E-SBC to use TLS version 1.0 only. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➤ **To configure the TLS version 1.0:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **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. In the 'TLS Version' field, enter 1.

Figure 4-29: Configuring TLS version 1.0

Edit Record #0	
Index	0
Name	default
TLS Version	1
Cipher Server	RC4:EXP
Cipher Client	ALL:!ADH
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject
Submit Cancel	

4. Click **Submit**.

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 (**Configuration** tab > **System** menu > **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 the **TLS Context Certificates**  button, located at the bottom of the TLS Contexts page; 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.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-30: Certificate Signing Request – Creating CSR

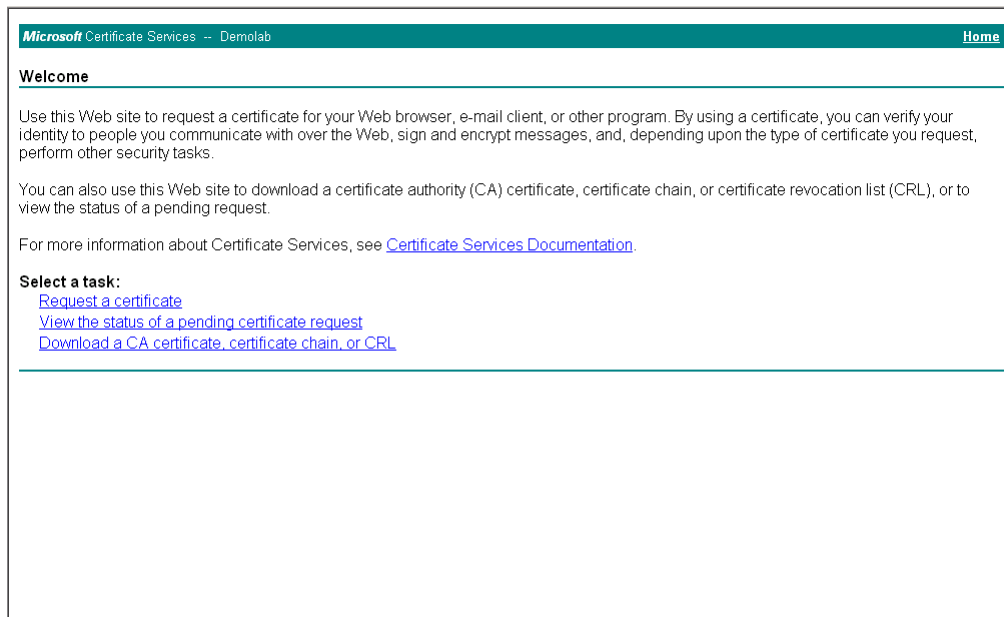
Certificate Signing Request	
Subject Name [CN]	ITSP.S4B.interop
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	
Create CSR	
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.	
<pre>-----BEGIN CERTIFICATE REQUEST----- MIIBwJCBAIBADABMRkwFwYDVQDDBBJVFNQLM0Q15pbmR1cm9wMIGfMA0GC5qG SIB3DQEBAAUAA4GNADCBiQK8gQCzEs8XTnY8be/t77eEDG7rTg747GQ3ODFOC4R5 x+e9KfberZgxMYqGT8u04AU0wU9LUPkkq+8gI6w2bg3bol0kg/9hrnNL2rftGcn 300ShP05PikmRNZnCC090b03tbr9kuHm1wPRQ7yT6k7x53XBbsigqT4LQbj8T1tt dH3bQIDAQABAAwDQY3K0ZiHvCNAQEFBQADgYEAIm/GA2E1ZQbZaR6CZyIaw1lt u65w450NFHmaC1uHSyZ8keM8d1Ux14hkiw7t5ygAD8KbXVkhRvACgcQrAK2v8u1Pf TVN+bwJ+kQ0d59C1x82e0o1wB3buPq5+qMDGTF+MyJWGVf85Ic1c6+zFoc+BEZY 7tQ8y0J8od0aDhStDFQ= -----END CERTIFICATE REQUEST-----</pre>	



Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Skype for Business Server 2015 (see Section 3.1 on page 13).

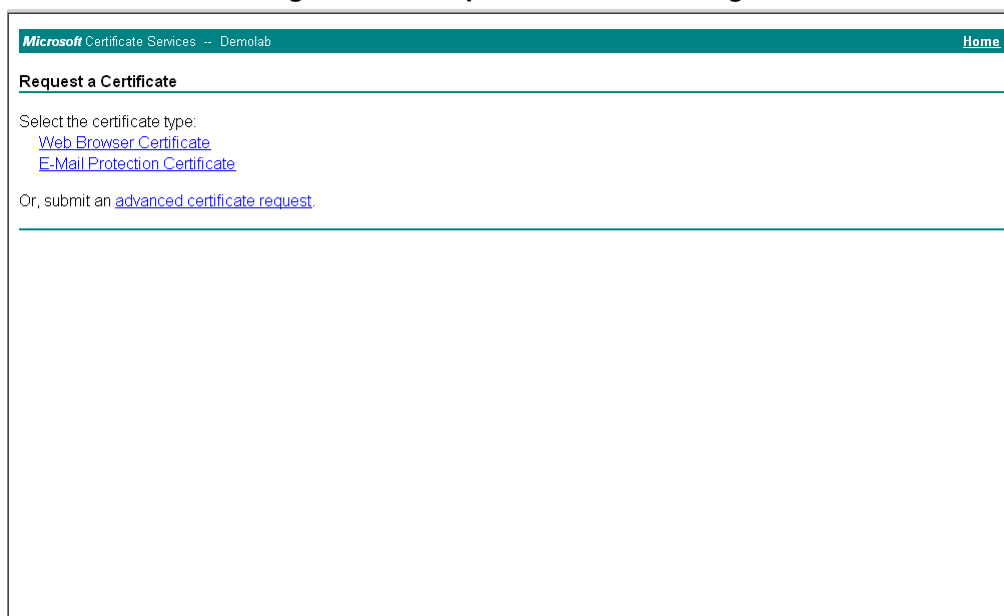
5. Copy the CSR from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate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

Figure 4-31: Microsoft Certificate Services Web Page



7. Click **Request a certificate**.

Figure 4-32: Request a Certificate Page



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

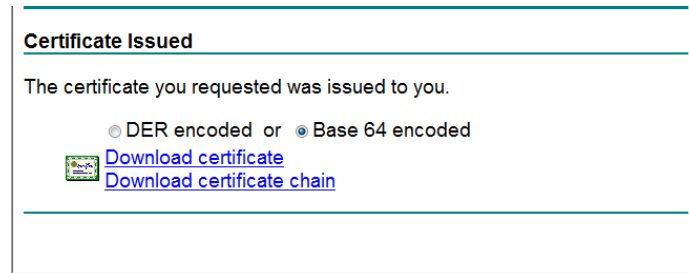
Figure 4-33: Advanced Certificate Request Page

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

Figure 4-34: Submit a Certificate Request or Renewal Request Page

10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**.

Figure 4-35: Certificate Issued Page



Certificate Issued

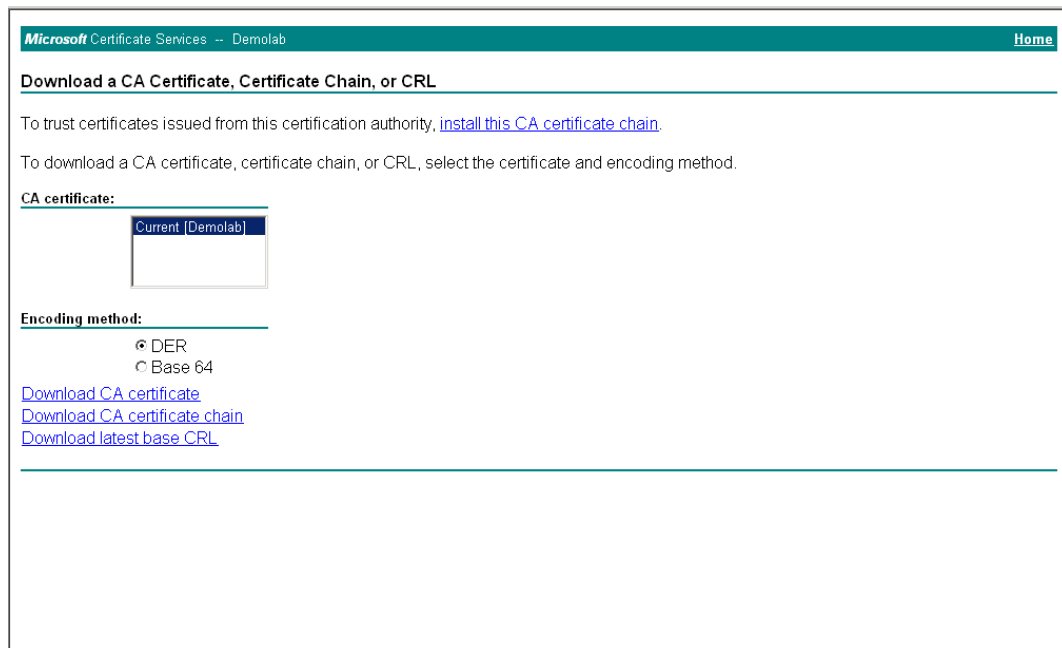
The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

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

Figure 4-36: Download a CA Certificate, Certificate Chain, or CRL Page



Microsoft Certificate Services -- Demolab Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

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

CA certificate:

Current [Demolab]

Encoding method:

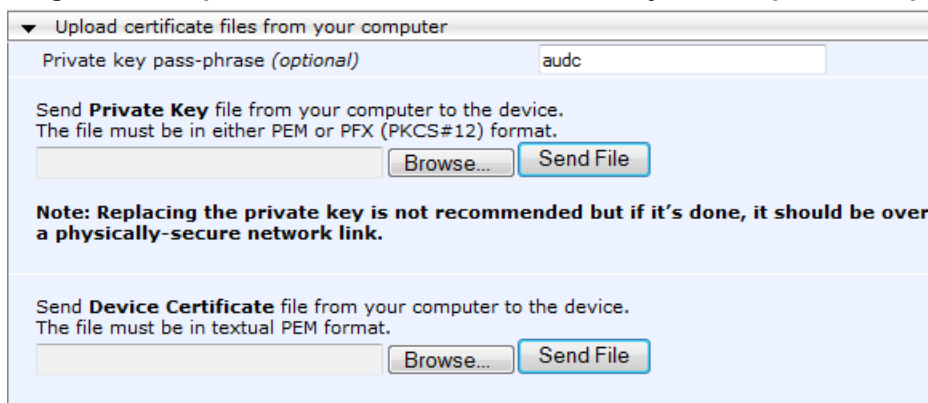
☒ DER
☐ Base 64

[Download CA certificate](#)
[Download CA certificate chain](#)
[Download latest base CRL](#)

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

20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts table, select the required TLS Context index row (typically, the default TLS Context at Index 0 is used), and then click the **TLS Context Certificates**  button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
 - b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-37: Upload Device Certificate Files from your Computer Group



▼ Upload certificate files from your computer

Private key pass-phrase (optional)

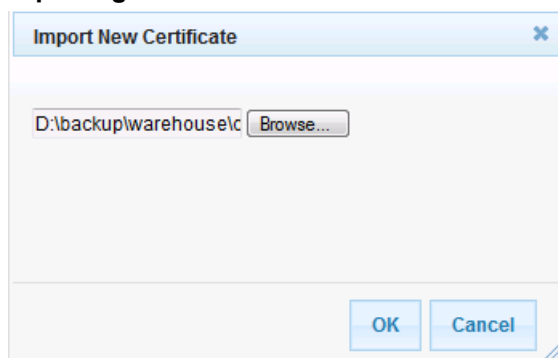
Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

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.

- c. In the E-SBC's Web interface, return to the **TLS Contexts** page.
- d. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates**  button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
- e. Click the **Import** button, and then select the certificate file to load.

Figure 4-38: Importing Root Certificate into Trusted Certificates Store



Import New Certificate ✕

D:\backup\warehouse\c

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 4.16 on page 97).

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 47).

➤ **To configure media security:**

1. Open the Media Security page (**Configuration** tab > **VoIP** menu > **Media** menu > **Media Security**).
2. Configure the parameters as follows:

Parameter	Value
Media Security	Enable

Figure 4-39: Configuring SRTP

General Media Security Settings	
Media Security	Enable
Aria Protocol Support	Disable
Media Security Behavior	Mandatory
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

3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 97).

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 IP Media Settings page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).

Figure 4-40: Configuring Number of Media Channels

⚡ Number of Media Channels	30
----------------------------	----

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section [4.16](#) on page [97](#)).

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 to denote the source and destination of the call. As configured in Section 4.7 on page 46, IP Group 1 represents Skype for Business Server 2015, and IP Group 2 represents TELUS SIP Trunk.

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 TELUS SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from any direction.
- Calls from Skype for Business Server 2015 to TELUS SIP Trunk
- Calls from TELUS SIP Trunk specifically for Fax (if required)
- Calls from TELUS SIP Trunk to Skype for Business Server 2015
- Calls from Fax supporting the ATA device to TELUS SIP Trunk (if required)

➤ To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from any destination:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

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

Figure 4-41: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab

Edit Row

Index: 0

Routing Policy: Default_SBCRouting ▼

Rule | **Action**

Name: OPTIONS termination

Alternative Route Options: Route Row ▼

Source IP Group: Any ▼

Request Type: OPTIONS ▼

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: *

Destination Host: *

Destination Tags:

Message Condition: None ▼

Call Trigger: Any ▼

ReRoute IP Group: Any ▼

Save Cancel

- c. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-42: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

Add Row

Index: 0
Routing Policy: Default_SBCRouting

Rule | **Action**

Destination Type: Dest Address
Destination IP Group: None
Destination SIP Interface: None
Destination Address: internal
Destination Port: 0
Destination Transport Type:
Call Setup Rules Set ID: -1
Group Policy: None
Cost Group: None

[Classic View](#)

Add Cancel

3. Configure the rule to route calls from TELUS SIP Trunk to Fax supporting the ATA device by doing the following:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Name	ITSP to Fax (arbitrary descriptive name)
Source IP Group	TELUS

Figure 4-43: Configuring IP-to-IP Routing Rule for ITSP to Fax – Rule tab

Edit Row

Index: 1

Routing Policy: Default_SBCRouting

Rule | Action

Name: ITSP to Fax

Alternative Route Options: Route Row

Source IP Group: TELUS

Request Type: All

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: 5872330307

Destination Host: *

Destination Tags:

Message Condition: None

Call Trigger: Any

ReRoute IP Group: Any

Save Cancel

- c. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group	Fax
Destination SIP Interface	S4B

Figure 4-44: Configuring IP-to-IP Routing Rule for ITSP to Fax – Action tab

Edit Row [X]

Index: 1
Routing Policy: Default_SBCRouting

Rule **Action**

Destination Type: IP Group
Destination IP Group: Fax
Destination SIP Interface: S4B
Destination Address:
Destination Port: 0
Destination Transport Type:
Call Setup Rules Set ID: -1
Group Policy: None
Cost Group: None

[Classic View](#)

Save Cancel

4. Configure a rule to route calls from Fax supporting the ATA device to TELUS SIP Trunk:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Name	Fax to ITSP (arbitrary descriptive name)
Source IP Group	Fax

Figure 4-45: Configuring IP-to-IP Routing Rule for Fax to ITSP – Rule tab

Edit Row

Index: 2

Routing Policy: Default_SBCRouting

Rule | Action

Name: Fax to ITSP

Alternative Route Options: Route Row

Source IP Group: Fax

Request Type: All

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: *

Destination Host: *

Destination Tags:

Message Condition: None

Call Trigger: Any

ReRoute IP Group: Any

Save Cancel

- c. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group	TELUS
Destination SIP Interface	TELUS

Figure 4-46: Configuring IP-to-IP Routing Rule for Fax to ITSP – Action tab

The screenshot shows the 'Edit Row' dialog box with the 'Action' tab selected. The 'Index' is set to 2 and the 'Routing Policy' is 'Default_SBCRouting'. The 'Destination Type' is 'IP Group', 'Destination IP Group' is 'TELUS', and 'Destination SIP Interface' is 'TELUS'. Other fields like 'Destination Address', 'Destination Port', 'Destination Transport Type', 'Call Setup Rules Set ID', 'Group Policy', and 'Cost Group' are also visible. Three arrows point to the 'Destination Type', 'Destination IP Group', and 'Destination SIP Interface' fields.

Parameter	Value
Index	2
Routing Policy	Default_SBCRouting
Destination Type	IP Group
Destination IP Group	TELUS
Destination SIP Interface	TELUS
Destination Address	
Destination Port	0
Destination Transport Type	
Call Setup Rules Set ID	-1
Group Policy	None
Cost Group	None

[Classic View](#)

Save Cancel

5. Configure a rule to route calls from Skype for Business Server 2015 to TELUS SIP Trunk:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	3
Name	S4B to ITSP (arbitrary descriptive name)
Source IP Group	S4B

Figure 4-47: Configuring IP-to-IP Routing Rule for S4B to ITSP – Rule tab

Edit Row

Index: 3

Routing Policy: Default_SBCRouting

Rule | Action

Name: S4B to ITSP

Alternative Route Options: Route Row

Source IP Group: S4B

Request Type: All

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: *

Destination Host: *

Destination Tags:

Message Condition: None

Call Trigger: Any

ReRoute IP Group: Any

Save Cancel

- c. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group	TELUS
Destination SIP Interface	TELUS

Figure 4-48: Configuring IP-to-IP Routing Rule for S4B to ITSP – Action tab

The screenshot shows the 'Edit Row' dialog box with the 'Action' tab selected. The 'Index' is set to 3 and the 'Routing Policy' is 'Default_SBCRouting'. The 'Destination Type' is 'IP Group', 'Destination IP Group' is 'TELUS', and 'Destination SIP Interface' is 'TELUS'. Other fields like 'Destination Address', 'Destination Port', 'Destination Transport Type', 'Call Setup Rules Set ID', 'Group Policy', and 'Cost Group' are also visible. Three arrows point to the 'Destination Type', 'Destination IP Group', and 'Destination SIP Interface' fields.

Parameter	Value
Index	3
Routing Policy	Default_SBCRouting
Destination Type	IP Group
Destination IP Group	TELUS
Destination SIP Interface	TELUS
Destination Address	
Destination Port	0
Destination Transport Type	
Call Setup Rules Set ID	-1
Group Policy	None
Cost Group	None

Classic View

Save Cancel

6. Configure a rule to route calls from TELUS SIP Trunk to Skype for Business Server 2015 by doing the following:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	4
Name	ITSP to S4B (arbitrary descriptive name)
Source IP Group	TELUS

Figure 4-49: Configuring IP-to-IP Routing Rule for ITSP to S4B – Rule tab

Edit Row

Index: 4

Routing Policy: Default_SBCRouting

Rule | Action

Name: ITSP to S4B

Alternative Route Options: Route Row

Source IP Group: TELUS

Request Type: All

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: *

Destination Host: *

Destination Tags:

Message Condition: None

Call Trigger: Any

ReRoute IP Group: Any

Save Cancel

- c. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group	S4B
Destination SIP Interface	S4B

Figure 4-50: Configuring IP-to-IP Routing Rule for ITSP to S4B – Action tab

Index: 4
Routing Policy: Default_SBCRouting

Rule **Action**

Destination Type: IP Group
Destination IP Group: S4B
Destination SIP Interface: S4B
Destination Address:
Destination Port: 0
Destination Transport Type:
Call Setup Rules Set ID: -1
Group Policy: None
Cost Group: None

[Classic View](#)

Save Cancel

The configured routing rules are shown in the figure below:

Figure 4-51: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing Table											
Add + Edit Edit Delete Delete Insert + Up ↑ Down ↓ Show / Hide ▢ ▾ All Search in table Search 🔍											
Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destination SIP Interface	Destination Address
0	OPTIONS to	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Address	None	None	internal
1	ITSP to Fax	Default_SBC	Route Row	TELUS	All	*	5872330307	IP Group	Fax	S4B	
2	Fax to ITSP	Default_SBC	Route Row	Fax	All	*	*	IP Group	TELUS	TELUS	
3	S4B to ITSP	Default_SBC	Route Row	S4B	All	*	*	IP Group	TELUS	TELUS	
4	ITSP to S4B	Default_SBC	Route Row	TELUS	All	*	*	IP Group	S4B	S4B	

Page 1 of 1 10 View 1 - 5 of 5



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 source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.7 on page 46, IP Group 0 represents Skype for Business Server 2015, and IP Group 1 represents TELUS SIP Trunk.



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

For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from the TELUS 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 IP-to-IP Outbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC > Manipulations SBC > IP-to-IP Outbound**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Add +1 toward S4B
Source IP Group	TELUS
Destination IP Group	S4B
Destination Username Prefix	* (asterisk sign)

Figure 4-52: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

Edit Row

Index: 0

Routing Policy: Default_SBCRouting

Rule | **Action**

Name: Add +1 toward S4B

Additional Manipulation: No

Request Type: All

Source IP Group: TELUS

Destination IP Group: S4B

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: *

Destination Host: *

Destination Tags:

Calling Name Prefix: *

Message Condition: None

Call Trigger: Any

Save Cancel

4. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Manipulated Item	Destination URI
Prefix to Add	+1 (plus sign)

Figure 4-53: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

Edit Row

Index: 0
Routing Policy: Default_SBCRouting

Rule **Action**

Manipulated Item: Destination URI

Remove From Left: 0

Remove From Right: 0

Leave From Right: 255

Prefix to Add: +1

Suffix to Add:

Privacy Restriction Mode: Transparent

[Classic View](#)

Save Cancel

5. Click **Submit**.

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 TELUS SIP Trunk IP Group:

Figure 4-54: Example of Configured IP-to-IP Outbound Manipulation Rules

▼ IP to IP Outbound Manipulation													
Add +		Edit	Delete	Insert +	Up ↑	Down ↓	Show / Hide	▼ All	Search in table		Search		
Index	Name	Routing Policy	Addition: Manipula	Source IP Group	Destinati IP Group	Source Usernam Prefix	Destinati Usernam Prefix	Manipulated Item	Remove From Left	Remove From Right	Leave From Right	Prefix to Add	Suffix to Add
0	Add +1 to	Default_SENo		TELUS	S4B	*	*	Destination URI	0	0	255	+1	
1	Change +	Default_SENo		S4B	TELUS	*	+	Destination URI	1	0	255	011	
2	Remove +	Default_SENo		S4B	TELUS	+1	*	Source URI	2	0	255		

Rule Index	Description
1	Calls from ITSP IP Group to S4B IP Group with any destination number (*). Add "+1" to the prefix of the destination number.
2	Calls from S4B IP Group to ITSP IP Group with the prefix destination number "+". Replace prefix "+" with prefix "011" (for international dialing for example).
3	Calls from S4B IP Group to ITSP IP Group with source number prefix "+1". Remove the "+1" 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 (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. This rule applies to messages sent to the TELUS SIP Trunk IP Group. This adds OPTIONS to the SIP Allow Header.

Parameter	Value
Index	0
Name	Add OPTIONS to Allow Header
Manipulation Set ID	4
Condition	header.allow regex(.*)
Action Subject	header.allow
Action Type	Modify
Action Value	\$1+',OPTIONS'

Figure 4-55: Configuring SIP Message Manipulation Rule 0 (for TELUS SIP Trunk)

The screenshot shows a web-based configuration interface for SIP message manipulation rules. The 'Edit Row' dialog box is open, displaying the following fields and values:

- Index:** 0
- Name:** Add OPTIONS to Allow Header
- Manipulation Set ID:** 4
- Message Type:** (empty)
- Condition:** header.allow regex(.*)
- Action Subject:** header.allow
- Action Type:** Modify
- Action Value:** \$1+',OPTIONS'
- Row Role:** Use Current Condit

At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

3. Configure another manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. This rule applies to messages sent to the TELUS SIP Trunk IP Group in a call forward scenario. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP History-Info Header.

Parameter	Value
Index	1
Name	Call Forward
Manipulation Set ID	4
Condition	header.history-info.0 regex (<sip:)(.)(.*)(@)(.)*
Action Subject	header.p-asserted-identity.url.user
Action Type	Modify
Action Value	\$3

Figure 4-56: Configuring SIP Message Manipulation Rule 1 (for TELUS SIP Trunk)

Edit Row

Index

1

Name

Call Forward

Manipulation Set ID

4

Message Type

Condition

header.history-info.0 re

Action Subject

header.p-asserted-ident

Action Type

Modify

Action Value

\$3

Row Role

Use Current Condit

Save

Cancel

4. Configure another manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. If the manipulation rule Index 1 (above) is executed, then the following rule is also executed. This rule removes SIP History-Info Header.

Parameter	Value
Index	2
Name	Call Forward
Manipulation Set ID	4
Action Subject	header.history-info
Action Type	Remove
Row Role	Use Previous Condition

Figure 4-57: Configuring SIP Message Manipulation Rule 2 (for TELUS SIP Trunk)

The screenshot shows a web-based configuration interface for SIP message manipulation rules. The 'Edit Row' dialog is open, displaying the following configuration for Rule 2:

- Index:** 2
- Name:** Call Forward
- Manipulation Set ID:** 4
- Message Type:** (empty field)
- Condition:** (empty field)
- Action Subject:** header.history-info
- Action Type:** Remove (selected from a dropdown menu)
- Action Value:** (empty field)
- Row Role:** Use Previous Condi (selected from a dropdown menu)

At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

5. Configure another manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. This rule applies to messages sent to the TELUS SIP Trunk IP Group in a call forward scenario. This removes the prefix '1' from the user part of the SIP P-Asserted-Identity Header.

Parameter	Value
Index	3
Name	Call Forward
Manipulation Set ID	4
Action Subject	header.p-asserted-identity.url.user
Action Type	Remove Prefix
Action Value	'1'

Figure 4-58: Configuring SIP Message Manipulation Rule 3 (for TELUS SIP Trunk)

The screenshot shows a web-based configuration interface for SIP message manipulation rules. The 'Edit Row' dialog box is open, displaying the configuration for a rule with Index 3. The fields are as follows:

Index	3
Name	Call Forward
Manipulation Set ID	4
Message Type	
Condition	
Action Subject	header.p-asserted-ident
Action Type	Remove Prefix
Action Value	'1'
Row Role	Use Current Condit

At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

6. Configure another manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. This rule applies to messages sent to the TELUS SIP Trunk IP Group in a call transfer scenario. This removes prefix '+1' from the user part of the SIP Referred-By Header.

Parameter	Value
Index	4
Name	Call Transfer
Manipulation Set ID	4
Message Type	any.response
Condition	header.referred-by exists
Action Subject	header.referred-by.url.user
Action Type	Remove Prefix
Action Value	'+1'

Figure 4-59: Configuring SIP Message Manipulation Rule 4 (for TELUS SIP Trunk)

Edit Row

Index

4

Name

Call Transfer

Manipulation Set ID

4

Message Type

Condition

header.referred-by exists

Action Subject

header.referred-by.url.u

Action Type

Remove Prefix

Action Value

'+1'

Row Role

Use Current Condit

Save

Cancel

7. Configure another manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. If the manipulation rule Index 4 (above) is executed, then the following rule is also executed. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	5
Name	Call Transfer
Manipulation Set ID	4
Action Subject	header.p-asserted-identity.url.user
Action Type	Modify
Action Value	header.referred-by.url.user
Row Role	Use Previous Condition

Figure 4-60: Configuring SIP Message Manipulation Rule 5 (for TELUS SIP Trunk)

The screenshot shows a web-based configuration interface for SIP Message Manipulation Rules. The 'Edit Row' dialog is open, displaying the configuration for Rule 5. The fields are as follows:

Index	5
Name	Call Transfer
Manipulation Set ID	4
Message Type	
Condition	
Action Subject	header.p-asserted-ident
Action Type	Modify
Action Value	header.referred-by.url.u
Row Role	Use Previous Condi

At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

8. Configure another manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. If the manipulation rule Index 5 (above) is executed, then the following rule is also executed. This replaces the user part of the SIP From Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	6
Name	Call Transfer
Manipulation Set ID	4
Action Subject	header.from.url.user
Action Type	Modify
Action Value	header.referred-by.url.user
Row Role	Use Previous Condition

Figure 4-61: Configuring SIP Message Manipulation Rule 6 (for TELUS SIP Trunk)

The screenshot shows a 'Edit Row' dialog box with the following fields and values:

- Index: 6
- Name: Call Transfer
- Manipulation Set ID: 4
- Message Type: (empty)
- Condition: (empty)
- Action Subject: header.from.url.user
- Action Type: Modify
- Action Value: header.referred-by.url.u
- Row Role: Use Previous Condi

Buttons: Save, Cancel

9. Configure another manipulation rule (Manipulation Set 4) for TELUS SIP Trunk. If the manipulation rule Index 6 (above) is executed, then the following rule is also executed. This rule removes SIP Referred-By Header.

Parameter	Value
Index	7
Name	Call Transfer
Manipulation Set ID	4
Action Subject	header.referred-by
Action Type	Remove
Row Role	Use Previous Condition

Figure 4-62: Configuring SIP Message Manipulation Rule 7 (for TELUS SIP Trunk)

Figure 4-63: Configured SIP Message Manipulation Rules

Message Manipulations								
Add + Edit Delete Insert + Up ↑ Down ↓ Show / Hide All Search in table Search								
Index	Name	Manipulat Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	Add OPTIONS to Allow	4		header.allow regex(.*)	header.allow	Modify	\$1+',OPTIONS'	Use Current Cond
1	Call Forward	4		header.history-info.0 re	header.p-asserted-identity.url.u	Modify	\$3	Use Current Cond
2	Call Forward	4			header.history-info	Remove		Use Previous Condi
3	Call Forward	4			header.p-asserted-identity.url.u	Remove Prefix	'1'	Use Current Cond
4	Call Transfer	4		header.referred-by exis	header.referred-by.url.user	Remove Prefix	'1'	Use Current Cond
5	Call Transfer	4			header.p-asserted-identity.url.u	Modify	header.referred-by.ur	Use Previous Condi
6	Call Transfer	4			header.from.url.user	Modify	header.referred-by.ur	Use Previous Condi
7	Call Transfer	4			header.referred-by	Remove		Use Previous Condi

The table below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to the TELUS SIP Trunk IP Group. These rules are specifically required to enable proper interworking between TELUS 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 TELUS SIP Trunk IP Group. This adds OPTIONS to the SIP Allow Header.	TELUS SIP Trunk requirement.
1	This rule applies to messages sent to the TELUS SIP Trunk IP Group in a call forward scenario. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP History-Info Header.	For Call Forward scenarios, TELUS SIP Trunk needs the user part in the SIP P-Asserted-Identity Header to be from the numbers pool assigned to the customer. In order to do this, the user part of the SIP P-Asserted-Identity Header is replaced with the value from the History-Info Header. After performing this manipulation, the SIP History-Info Header is removed according to the TELUS SIP Trunk requirement.
2	If the manipulation rule Index 1 (above) is executed, then the following rule is also executed. This rule removes SIP History-Info Header.	
3	This rule applies to messages sent to the TELUS SIP Trunk IP Group in a call forward scenario. This removes prefix '1' from the user part of the SIP P-Asserted-Identity Header.	
4	This rule applies to messages sent to the TELUS SIP Trunk IP Group in a call transfer scenario. This removes prefix '+1' from the user part of the SIP Referred-By Header.	For Call Transfers initiated by Skype for Business Server 2015, TELUS SIP Trunk needs the user part in the SIP P-Asserted-Identity Header to be from the numbers pool assigned to the customer. In order to do this, the user part of the SIP P-Asserted-Identity and From Headers is replaced with the value from the SIP Referred-By Header. After performing these manipulations, the SIP Referred-By Header is removed according to the TELUS SIP Trunk requirement.
5	If the manipulation rule Index 4 (above) is executed, then the following rule is also executed. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP Referred-By Header.	
6	If the manipulation rule Index 5 (above) is executed, then the following rule is also executed. This replaces the user part of the SIP From Header with the value from the SIP Referred-By Header.	
7	If the manipulation rule Index 6 (above) is executed, then the following rule is also executed. This rule removes SIP Referred-By Header.	

10. Assign Manipulation Set ID 4 to the TELUS SIP trunk IP Group:
 - a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
 - b. Select the row of the TELUS SIP trunk IP Group, and then click **Edit**.
 - c. Click the **SBC** tab.
 - d. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-64: Assigning Manipulation Set 4 to the TELUS SIP Trunk IP Group

The screenshot shows the 'Edit Row' dialog box with the 'SBC' tab selected. The 'Index' is 1 and the 'SRD' is 'DefaultSRD'. The 'Outbound Message Manipulation Set' field is highlighted in yellow and contains the value '4'. An arrow points to this field from the left. The 'Save' and 'Cancel' buttons are at the bottom right.

Common	GW	SBC	GW Group Status
SBC Operation Mode: Not Configured			
Classify By Proxy Set: Enable			
SBC Client Forking Mode: Sequential			
Inbound Message Manipulation Set: -1			
Outbound Message Manipulation Set: 4			
Message Manipulation User-Defined String 1:			
Message Manipulation User-Defined String 2:			
Registration Mode: User Initiates Regis			
Max. Number of Registered Users: -1			
Authentication Mode: User Authenticates			
Authentication Method List:			
Username:			

- e. Click **Submit**.

4.15 Step 15: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

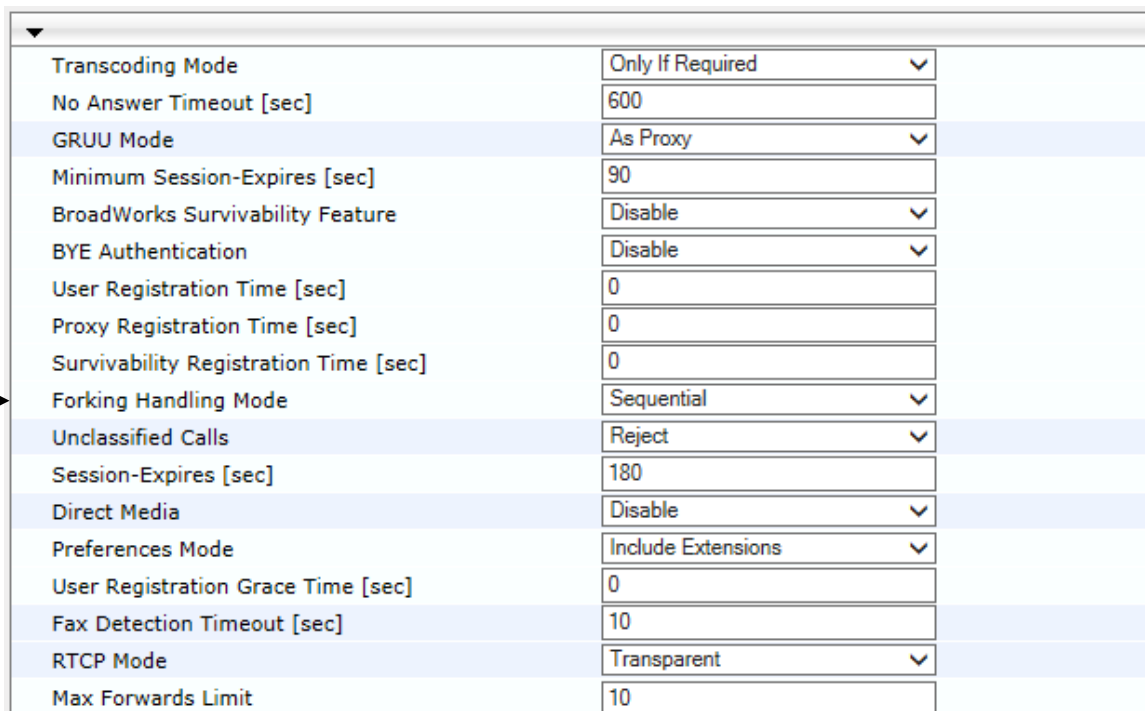
4.15.1 Step 15a: Configure Call Forking Mode

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 General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.

Figure 4-65: Configuring Forking Mode



Transcoding Mode	Only If Required
No Answer Timeout [sec]	600
GRUU Mode	As Proxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
BYE Authentication	Disable
User Registration Time [sec]	0
Proxy Registration Time [sec]	0
Survivability Registration Time [sec]	0
Forking Handling Mode	Sequential
Unclassified Calls	Reject
Session-Expires [sec]	180
Direct Media	Disable
Preferences Mode	Include Extensions
User Registration Grace Time [sec]	0
Fax Detection Timeout [sec]	10
RTCP Mode	Transparent
Max Forwards Limit	10

3. Click **Submit**.

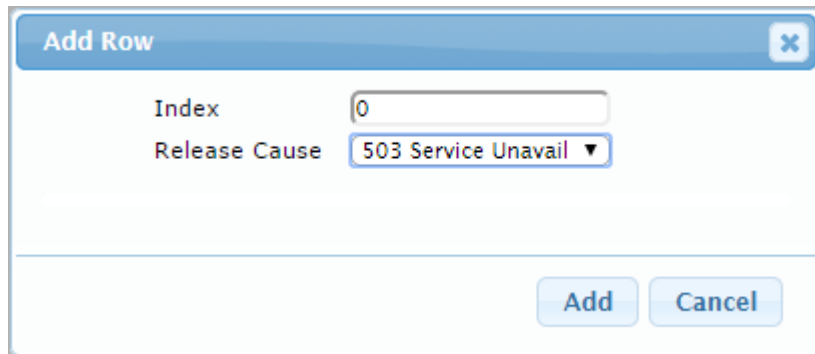
4.15.2 Step 15b: Configure SBC Alternative Routing Reasons

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 SBC Alternative Routing Reasons page (**Configuration** tab > **VoIP** menu > **SBC > Routing SBC > SBC Alternative Routing Reasons**).
2. Click **Add**; the following dialog box appears:

Figure 4-66: SBC Alternative Routing Reasons Table - Add Record



The screenshot shows a dialog box titled "Add Row" with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first field is labeled "Index" and contains the value "0". The second field is labeled "Release Cause" and has a dropdown menu with the selected option "503 Service Unavail". At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

3. Click **Submit**.

4.15.3 Step 15c: Configure Registration Accounts



Note: The following step is applicable only for Internet registration-based topology.

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

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

➤ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Enter an Index number (e.g., "0"), and then click **Add**.
3. Configure the account according to the provided information, for example:

Parameter	Value
Application Type	SBC
Served IP Group	S4B
Serving IP Group	TELUS
Username	As provided by TELUS
Password	As provided by TELUS
Host Name	ipinet4.com (as provided by TELUS)
Register	Regular
Contact User	p5872330306 (Trunk pilot user, as provided by TELUS)

4. Click **Apply**.

Figure 4-67: Configuring SIP Registration Account

Index	Application Type	Served Trunk Group	Served IP Group	Serving IP Group	User Name	Password	Host Name	Register	Contact User
0	SBC	-1	S4B	TELUS	p5872330306	*	ipinet4.com	Regular	p5872330306

4.16 Step 16: 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 save the configuration to flash memory:**

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

Figure 4-68: Resetting the E-SBC

The screenshot displays a web-based configuration interface for an E-SBC. It is divided into three main sections:

- Reset Configuration:** Contains a "Reset Board" button, a "Burn To FLASH" dropdown menu set to "Yes", and a "Graceful Option" dropdown menu set to "No".
- LOCK / UNLOCK:** Contains a "Lock" button, a "Graceful Option" dropdown menu set to "No", and a "Gateway Operational State" label showing "UNLOCKED".
- Save Configuration:** Contains a "Burn To FLASH" button labeled "BURN".

2. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).
3. Click the **Reset** button.

This page is intentionally left blank.

A AudioCodes INI file for VPN-based Configuration

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 431, is shown below:



Note: To load and save an ini file, use the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 7.00A.047.007
;DSP Software Version: 5014AE3_R => 700.44
;Board IP Address: 10.15.17.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 496M  Flash size: 64M  Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features;;Board Type: 72 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;DATA features: ;PSTN FALLBACK
Supported ;E1Trunks=1 ;T1Trunks=1 ;FXSPorts=8 ;FXOPorts=0 ;DSP Voice
features: RTCP-XR ;IP Media: Conf VXML ;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
;QOE features: VoiceQualityMonitoring MediaEnhancement ;Channel Type:
DspCh=30 IPMediaDspCh=30 ;HA ;Control Protocols: MGCP SIP SASurvivability
SBC=60 MSFT FEU=100 TestCall=100 ;Default features;;Coders: G711 G726;

;----- HW components-----
;
; Slot # : Module type : # of ports
;-----
;      1 : FALC56      : 1
;      2 : FXS         : 4
;      3 : BRI         : 4
;-----

[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
```

```

NTPServerIP = '10.15.27.1'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[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]

UserProductName = 'Mediant 800 E-SBC'
WebLogoText = 'TELUS'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSPkeyFileName is hidden but has non-default value
PacketSmartPlatform = 'M800'

[SIP Params]

```

```
MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESEXMODE = 1
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[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, 10.15.17.55, 16, 10.15.0.1, "Voice",
10.15.27.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.158, 25, 195.189.192.129, "WANSP",
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",
"$1$LE0VGBxUAQFSUAJXUQANXwoPDwtaeSNwInB2c3B+eihzKSgvfDIzMDI1YGc0YWhub2h1P
GpUVwdVBlNSBgPRXV4=", 1, 0, 2, 15, 60, 200,
"62cabed25276f6d59432fcaf295a1346";
WebUsers 1 = "User",
"$1$fRwcHLO4tOHmvOKy7OiyS7m5vrbzpqfyoKL0r6v7q/iv/P35kpmUwcXBkZWYy5iaz8+Wm
NGBgoPXhdTRi4yDj94=", 3, 0, 2, 15, 60, 50,
"e124fc45691a62316416e055a60edb6f";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,

```

```

TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 1, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
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_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
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 1 = "S4B", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "", -1, -1, 0, 1, 1,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 0, 0, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 0, 1, 0, 0, 101, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 2 = "TELUS", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0,
0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, "", 2, -1, 1, 2,
0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 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, 1, 0,
0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 3 = "Fax", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 2, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 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, 0, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 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 0 = "MRLan", "Voice", "", 6000, 100, 6999, 0, "", "";
CpMediaRealm 1 = "MRWan", "WANSP", "", 7000, 100, 7999, 0, "", "";

[ \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 ]

[ 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 0 = "S4B", "Voice", 2, 5060, 0, 5067, "DefaultSRD", "", "
default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0;
SIPInterface 1 = "TELUS", "WANSP", 2, 5060, 0, 0, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1, 0;

[ \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_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "", 1, -1, "", "",
"S4B", "", "", "", "", "";
ProxySet 1 = "TELUS", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"TELUS", "", "", "", "", "";
ProxySet 2 = "Fax", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"S4B", "", "", "", "", "";

[ \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_EnablesSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWPProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_SBCDialPlanName;
IPGroup 0 = 0, "S4B", "S4B", "192.168.0.2", "", -1, 0, "DefaultSRD",
"MRLan", 1, "S4B", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";
IPGroup 1 = 0, "TELUS", "TELUS", "192.168.0.2", "", -1, 0, "DefaultSRD",
"MRWan", 1, "TELUS", -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==",
0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";
IPGroup 2 = 0, "Fax", "Fax", "", "", -1, 0, "DefaultSRD", "MRLan", 1,
"Fax", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "",
0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";

[ \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 = "0", 0, "FE.S4B.interop:5067", 2;
ProxyIp 1 = "1", 0, "192.168.1.73:5060", 0;
ProxyIp 2 = "2", 0, "10.15.17.12", 0;

[ \ProxyIp ]

[ 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 = "OPTIONS termination", "Default_SBCRoutingPolicy",
"Any", "*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0,
-1, 0, 0, "", "", "";
IP2IPRouting 1 = "ITSP to Fax", "Default_SBCRoutingPolicy", "TELUS", "*",
"*, "5872330335", "*", 0, "", "Any", 0, -1, 0, "Fax", "S4B", "", 0, -1,
0, 0, "", "", "";
IP2IPRouting 2 = "Fax to ITSP", "Default_SBCRoutingPolicy", "Fax", "*",
"*, "*", 0, "", "Any", 0, -1, 0, "TELUS", "TELUS", "", 0, -1, 0, 0,
"", "", "";
IP2IPRouting 3 = "S4B to ITSP", "Default_SBCRoutingPolicy", "S4B", "*",
"*, "*", 0, "", "Any", 0, -1, 0, "TELUS", "TELUS", "", 0, -1, 0, 0,
"", "", "";
IP2IPRouting 4 = "ITSP to S4B", "Default_SBCRoutingPolicy", "TELUS", "*",
"*, "*", 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 +1 toward S4B",
"Default_SBCRoutingPolicy", 0, "TELUS", "S4B", "*", "*", "*", "*", "*",
"", 0, "Any", 0, 1, 0, 0, 255, "+1", "", 0, "", "";
IPOutboundManipulation 1 = "Change + to 011", "Default_SBCRoutingPolicy",
0, "S4B", "TELUS", "*", "*", "+", "*", "*", "", 0, "Any", 0, 1, 1, 0,
255, "011", "", 0, "", "";
IPOutboundManipulation 2 = "Remove +1 from Source",
"Default_SBCRoutingPolicy", 0, "S4B", "TELUS", "+1", "*", "*", "*", "*",
"", 0, "Any", 0, 0, 2, 0, 255, "", "", 0, "", "";

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0, "";

[ \CodersGroup0 ]

[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 0, "";

[ \CodersGroup1 ]

[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce,
CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup2 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup2 ]

```

```
[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Alaw64k";
AllowedCodersGroup1 1 = "g711Ulraw64k";

[ \AllowedCodersGroup1 ]


[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g711Ulraw64k";
AllowedCodersGroup2 1 = "g729";

[ \AllowedCodersGroup2 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Add OPTIONS to Allow Header", 4, "",
"header.allow regex(.*)", "header.allow", 2, "$1+',OPTIONS'", 0;
MessageManipulations 1 = "Call Forward", 4, "", "header.history-info.0
regex (<sip:)(.)(.*) (@)(.*)", "header.p-asserted-identity.url.user", 2,
"$3", 0;
MessageManipulations 2 = "Call Forward", 4, "", "", "header.history-
info", 1, "", 1;
MessageManipulations 3 = "Call Forward", 4, "", "", "header.p-asserted-
identity.url.user", 6, "'1'", 0;
MessageManipulations 4 = "Call Transfer", 4, "", "header.referred-by
exists", "header.referred-by.url.user", 6, "'+1'", 0;
MessageManipulations 5 = "Call Transfer", 4, "", "", "header.p-asserted-
identity.url.user", 2, "header.referred-by.url.user", 1;
MessageManipulations 6 = "Call Transfer", 4, "", "",
"header.from.url.user", 2, "header.referred-by.url.user", 1;
MessageManipulations 7 = "Call Transfer", 4, "", "", "header.referred-
by", 1, "", 1;

[ \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 ]
```

This page is intentionally left blank.

B AudioCodes INI file for Internet Registration-based Configuration

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 and save an *ini* file, use the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 7.00A.047.007
;DSP Software Version: 5014AE3_R => 700.44
;Board IP Address: 10.15.17.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 496M  Flash size: 64M  Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features;;Board Type: 72 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;DATA features: ;PSTN FALLBACK
Supported ;E1Trunks=1 ;T1Trunks=1 ;FXSPorts=8 ;FXOPorts=0 ;DSP Voice
features: RTCP-XR ;IP Media: Conf VXML ;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
;QOE features: VoiceQualityMonitoring MediaEnhancement ;Channel Type:
DspCh=30 IPMediaDspCh=30 ;HA ;Control Protocols: MGCP SIP SASurvivability
SBC=60 MSFT FEU=100 TestCall=100 ;Default features;;Coders: G711 G726;

;----- HW components-----
;
; Slot # : Module type : # of ports
;-----
;      1 : FALC56      : 1
;      2 : FXS         : 4
;      3 : BRI         : 4
;-----

[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
```

```

NTPServerIP = '10.15.27.1'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[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]

UserProductName = 'Mediant 800 E-SBC'
WebLogoText = 'TELUS'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSPkeyFileName is hidden but has non-default value
PacketSmartPlatform = 'M800'

[SIP Params]

```



```
MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESENABLEMODE = 1
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[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, 10.15.17.55, 16, 10.15.0.1, "Voice",
10.15.27.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.158, 25, 195.189.192.129, "WANSP",
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",
"$1$LE0VGBxUAQFSUAJXUQANXwoPDwtaeSNwInB2c3B+eihzKSgvfDIzMDI1YGc0YWhub2h1P
GpUVwdVBlNSBgPRXV4=", 1, 0, 2, 15, 60, 200,
"62cabed25276f6d59432fcaf295a1346";
WebUsers 1 = "User",
"$1$fRwcHLO4tOHmvOKy7OiyS7m5vrbzpqfyoKL0r6v7q/iv/P35kpmUwcXBkZWYy5iaz8+Wm
NGBgoPXhdTRi4yDj94=", 3, 0, 2, 15, 60, 50,
"e124fc45691a62316416e055a60edb6f";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,

```

```

TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 1, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
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_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
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_SBCSDPHandlerRTCPAttribute,
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 1 = "S4B", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "", -1, -1, 0, 1, 1,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 0, 0, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 0, 1, 0, 0, 101, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 2 = "TELUS", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0,
0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, "", 2, -1, 1, 2,
0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 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, 1, 0,
0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 3 = "Fax", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 2, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 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, 0, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 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 0 = "MRLan", "Voice", "", 6000, 100, 6999, 0, "", "";
CpMediaRealm 1 = "MRWan", "WANSP", "", 7000, 100, 7999, 0, "", "";

[ \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 ]

[ 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 0 = "S4B", "Voice", 2, 5060, 0, 5067, "DefaultSRD", "", "
default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0;
SIPInterface 1 = "TELUS", "WANSP", 2, 5060, 0, 0, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1, 0;

[ \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_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "", 1, -1, "", "",
"S4B", "", "", "", "", "";
ProxySet 1 = "TELUS", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"TELUS", "", "", "", "", "";
ProxySet 2 = "Fax", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"S4B", "", "", "", "", "";

[ \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_EnablesSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWPProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_SBCDialPlanName;
IPGroup 0 = 0, "S4B", "S4B", "195.189.192.158", "", -1, 0, "DefaultSRD",
"MRLan", 1, "S4B", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";
IPGroup 1 = 0, "TELUS", "TELUS", "ipinet4.com", "", -1, 0, "DefaultSRD",
"MRWan", 1, "TELUS", -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==",
0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";
IPGroup 2 = 0, "Fax", "Fax", "195.189.192.158", "", -1, 0, "DefaultSRD",
"MRLan", 1, "Fax", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";

[ \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 = "0", 0, "FE.S4B.interop:5067", 2;
ProxyIp 1 = "1", 0, "209.115.158.100:5060", 0;
ProxyIp 2 = "2", 0, "10.15.17.12", 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", "TELUS", "p5872330306", "$1$BjQ0Ozk5OzpsbGw=",
"ipinet4.com", 1, "p5872330306", 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 = "OPTIONS termination", "Default_SBCRoutingPolicy",
"Any", "*", "*", "*", "6", "", "Any", 0, -1, 1, "", "", "internal", 0,
-1, 0, 0, "", "", "";
IP2IPRouting 1 = "ITSP to Fax", "Default_SBCRoutingPolicy", "TELUS", "*",
"*, "5872330307", "0", "", "Any", 0, -1, 0, "Fax", "S4B", "", 0, -1,
0, 0, "", "", "";
IP2IPRouting 2 = "Fax to ITSP", "Default_SBCRoutingPolicy", "Fax", "*",
"*, "0", "", "Any", 0, -1, 0, "TELUS", "TELUS", "", 0, -1, 0, 0,
"", "", "";
IP2IPRouting 3 = "S4B to ITSP", "Default_SBCRoutingPolicy", "S4B", "*",
"*, "0", "", "Any", 0, -1, 0, "TELUS", "TELUS", "", 0, -1, 0, 0,
"", "", "";
```

```

IP2IPRouting 4 = "ITSP to S4B", "Default_SBCRoutingPolicy", "TELUS", "*",
"*, "*", "*", 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 +1 toward S4B",
"Default_SBCRoutingPolicy", 0, "TELUS", "S4B", "*", "*", "*", "*", "*",
"", 0, "Any", 0, 1, 0, 0, 255, "+1", "", 0, "", "";
IPOutboundManipulation 1 = "Change + to 011", "Default_SBCRoutingPolicy",
0, "S4B", "TELUS", "*", "*", "+", "*", "*", "", 0, "Any", 0, 1, 1, 0,
255, "011", "", 0, "", "";
IPOutboundManipulation 2 = "Remove +1 from Source",
"Default_SBCRoutingPolicy", 0, "S4B", "TELUS", "+1", "*", "*", "*", "*",
"", 0, "Any", 0, 0, 2, 0, 255, "", "", 0, "", "";

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0, "";

[ \CodersGroup0 ]

[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Ulau64k", 20, 0, -1, 0, "";
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 0, "";

[ \CodersGroup1 ]

```

```
[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce,
CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup2 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup2 ]

[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Alaw64k";
AllowedCodersGroup1 1 = "g711Ulaw64k";

[ \AllowedCodersGroup1 ]

[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g711Ulaw64k";
AllowedCodersGroup2 1 = "g729";

[ \AllowedCodersGroup2 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Add OPTIONS to Allow Header", 4, "",
"header.allow regex(.*)", "header.allow", 2, "$1+',OPTIONS'", 0;
MessageManipulations 1 = "Call Forward", 4, "", "header.history-info.0
regex (<sip:)(.)(.*)(@)(.*)", "header.p-asserted-identity.url.user", 2,
"$3", 0;
MessageManipulations 2 = "Call Forward", 4, "", "", "header.history-
info", 1, "", 1;
MessageManipulations 3 = "Call Forward", 4, "", "", "header.p-asserted-
identity.url.user", 6, "'1'", 0;
MessageManipulations 4 = "Call Transfer", 4, "", "header.referred-by
exists", "header.referred-by.url.user", 6, "'+1'", 0;
MessageManipulations 5 = "Call Transfer", 4, "", "", "header.p-asserted-
identity.url.user", 2, "header.referred-by.url.user", 1;
MessageManipulations 6 = "Call Transfer", 4, "", "",
"header.from.url.user", 2, "header.referred-by.url.user", 1;
MessageManipulations 7 = "Call Transfer", 4, "", "", "header.referred-
by", 1, "", 1;

[ \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 ]
```

This page is intentionally left blank.

C Configuring ATAs for FAX Support

This section describes how to configure the analog device entity to route its calls to the AudioCodes Media Gateway for supporting faxes. The analog device entity must be configured to send all calls to the AudioCodes SBC.



Note: The configuration described in this section is for ATA devices configured for AudioCodes MP-11x series.

C.1 Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints) by defining telephone numbers. The configuration below uses the example of the ATA destination phone number **5872330307** (IP address 10.15.17.12) with all routing directed to the SBC device (10.15.17.55).

- **To configure the Endpoint Phone Number table:**
 - Open the Endpoint Phone Number Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP submenu** > **Hunt Group** sub-menu > **Endpoint Phone Number**).

Figure C-1: Endpoint Phone Number Table Page

Endpoint Phone Number Table				
	Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID
1	1	5872330307		0
2				
3				
4				

C.2 Step 2: Configure Tel to IP Routing Table

This step describes how to configure the Tel-to-IP routing rules to ensure that the MP-11x device sends all calls to the AudioCodes central E-SBC device.

➤ **To configure the Tel to IP Routing table:**

- Open the Tel to IP Routing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Routing** sub-menu > **Tel to IP Routing**).

Figure C-2: Tel to IP Routing Page

	Src. Hunt Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IP Group ID	IP Profile ID	Cost Group ID
1	*	*	*	10.15.17.55	5060	UDP	-1		None
2						Not Configured	-1		None

C.3 Step 3: Configure Coders Table

This step describes how to configure the coders for the MP-11x device.

➤ **To configure MP-11x coders:**

- Open the Coders page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** sub-menu > **Coders**).

Figure C-3: Coders Table Page

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.729	20	8	18	Disabled
G.711U-law	20	64	0	Disabled

C.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

This step describes how to configure the fax signaling method for the MP-11x device.

➤ To configure the fax signaling method:

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).

Figure C-4: SIP General Parameters Page

SIP General Parameters	
NAT IP Address	0.0.0.0
PRACK Mode	Disable
Channel Select Mode	By Dest Phone Number
Enable Early Media	Disable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	60
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	T.38 Relay
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5068
SIP TLS Local Port	5067
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060

2. From the 'FAX Signaling Method' drop-down list, select **G.711 Transport** for G.711 fax support and select **T.38 Relay** for T.38 fax support.
3. From the 'SIP Transport Type' drop-down list, select **UDP**.
4. In the 'SIP UDP Local Port' field, enter **5060** (corresponding to the Central Gateway UDP transmitting port configuration).
5. In the 'SIP Destination Port', enter **5060** (corresponding to the Central Gateway UDP listening port configuration).

International Headquarters

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

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

website: <https://www.audiocodes.com>

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-12227

