

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

Version 7.2



Microsoft Partner

Gold Communications



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	Rogers IP 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.....	33
4.2	Step 2: Enable the SBC Application	35
4.3	Step 3: Configure Media Realms	36
4.4	Step 4: Configure SIP Signaling Interfaces.....	39
4.5	Step 5: Configure Proxy Sets	41
4.6	Step 6: Configure Coders	47
4.7	Step 7: Configure IP Profiles	50
4.8	Step 8: Configure IP Groups.....	55
4.9	Step 9: SIP TLS Connection Configuration.....	57
4.9.1	Step 9a: Configure the NTP Server Address.....	57
4.9.2	Step 9b: Configure the TLS version	57
4.9.3	Step 9c: Configure a Certificate.....	58
4.10	Step 10: Configure SRTP	64
4.11	Step 11: Configure Maximum IP Media Channels	65
4.12	Step 12: Configure IP-to-IP Call Routing Rules	66
4.13	Step 13: Configure IP-to-IP Manipulation Rules.....	73
4.14	Step 14: Miscellaneous Configuration.....	75
4.14.1	Step 14a: Configure Call Forking Mode	75
4.14.2	Step 14b: Configure SBC Alternative Routing Reasons	75
4.15	Step 15: Reset the E-SBC	77
A	AudioCodes INI File	79
B	Configuring Analog Devices (ATAs) for Fax Support.....	91
B.1	Step 1: Configure the Endpoint Phone Number Table	91
B.2	Step 2: Configure Tel to IP Routing Table	92
B.3	Step 3: Configure Coders Table	92
B.4	Step 4: Configure SIP UDP Transport Type and Fax Signaling Method.....	93

This page is intentionally left blank.

Notice

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

© Copyright 2017 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: March-21-2017

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
39135	Initial document release for Version 7.2.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

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

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

1.1 Intended Audience

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

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ▪ Mediant 500 E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (SE and VE)
Software Version	SIP_7.20A.002
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP (to the Rogers SIP Trunk) ▪ SIP/TCP or SIP/TLS (to the S4B FE Server)
Additional Notes	None

2.2 Rogers IP Trunking Version

Table 2-2: Rogers Version

Vendor/Service Provider	Rogers
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Skype for Business Server 2015 Version

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

Vendor	Microsoft
Model	Skype for Business
Software Version	Release 2015 6.0.9319.259
Protocol	SIP
Additional Notes	None

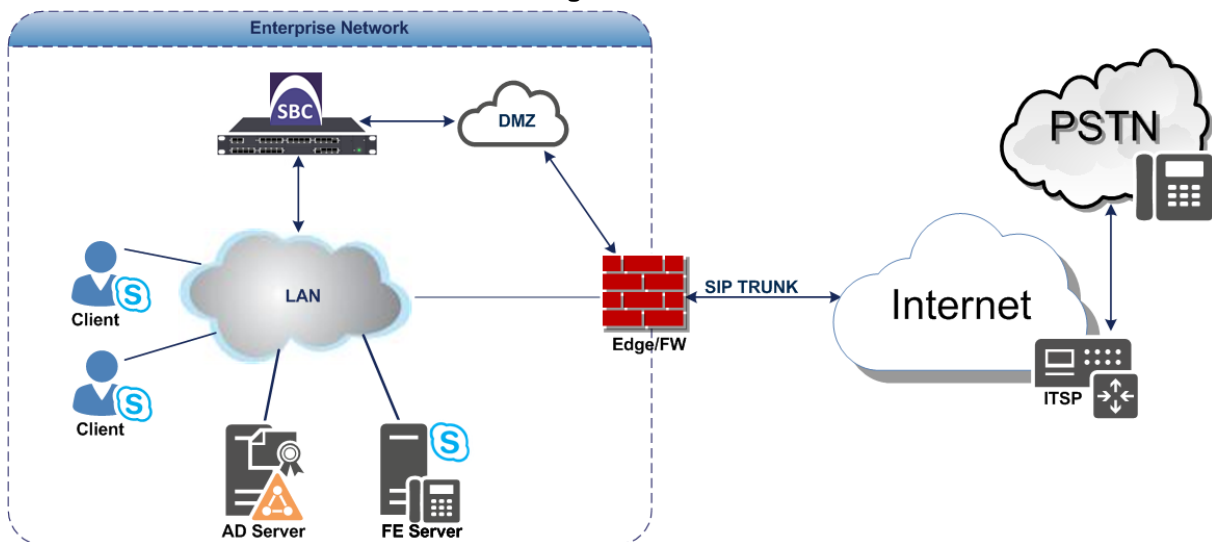
2.4 Interoperability Test Topology

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



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

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

2.4.2 Known Limitations

The following limitations were observed during interoperability tests performed for AudioCodes' E-SBC interworking between Microsoft Skype for Business Server 2015 and Rogers SIP Trunk:

- Early Media is not supported by Rogers
- Music on Hold is not supported by Rogers

This page is intentionally left blank.

3 Configuring Skype for Business Server 2015

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



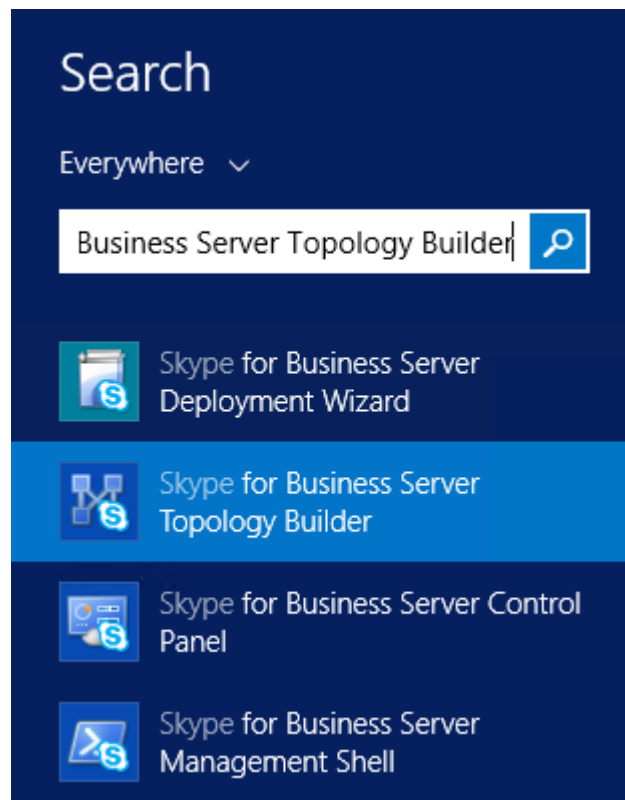
Note: Dial plans, voice policies, and PSTN usages are also necessary for Enterprise voice deployment; however, they are beyond the scope of this document.

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

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

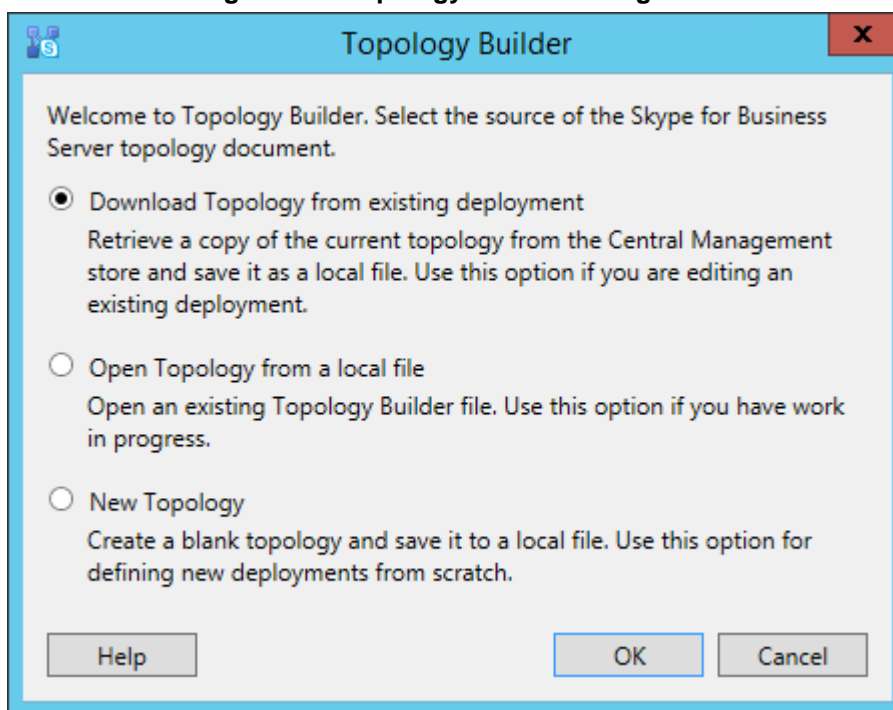
- **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**
- 1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

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



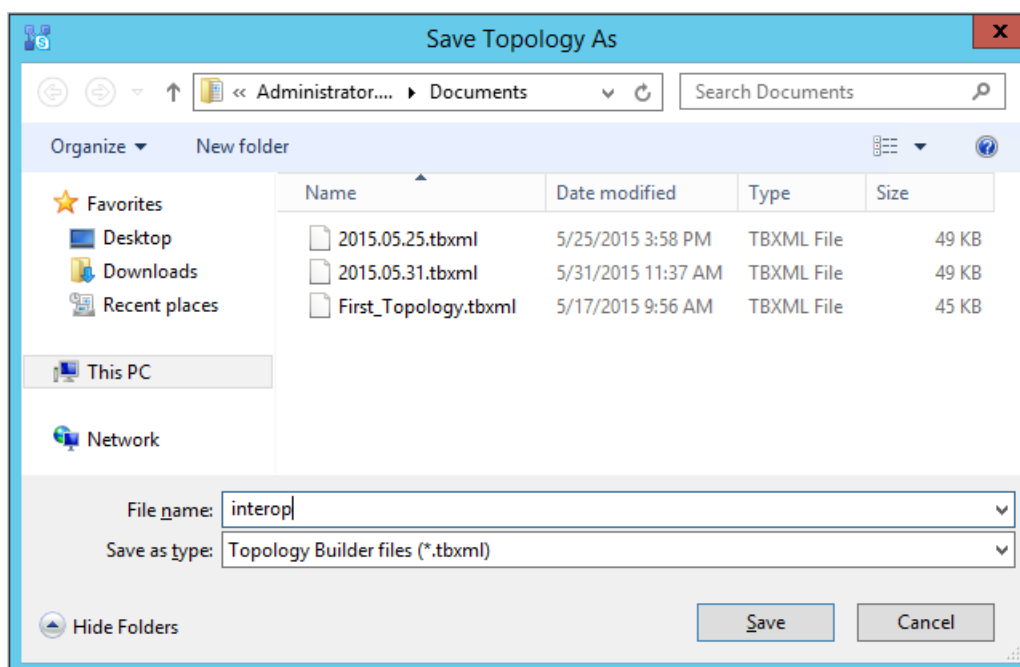
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

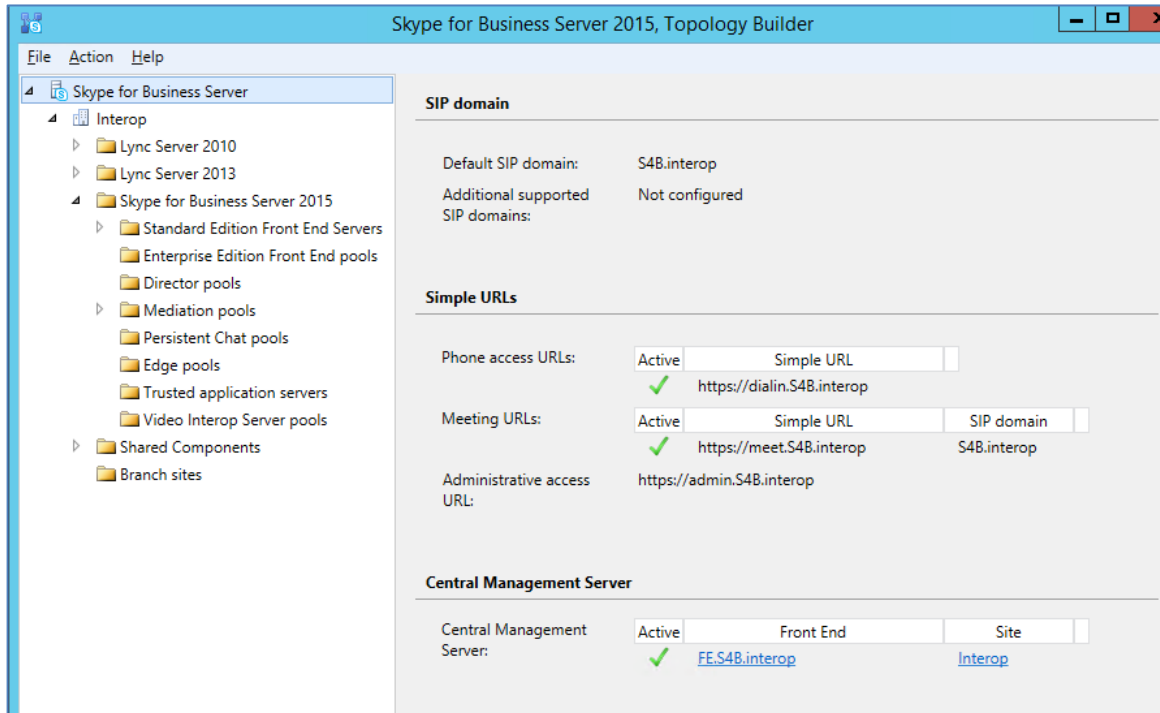
Figure 3-3: Save Topology Dialog Box



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

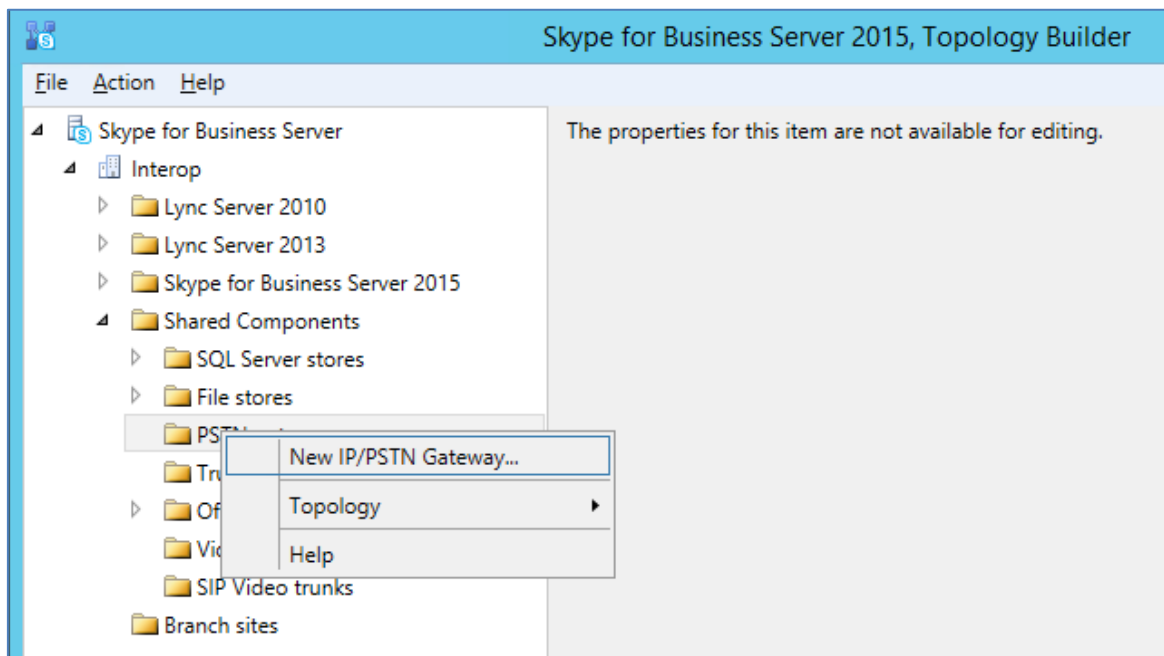
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



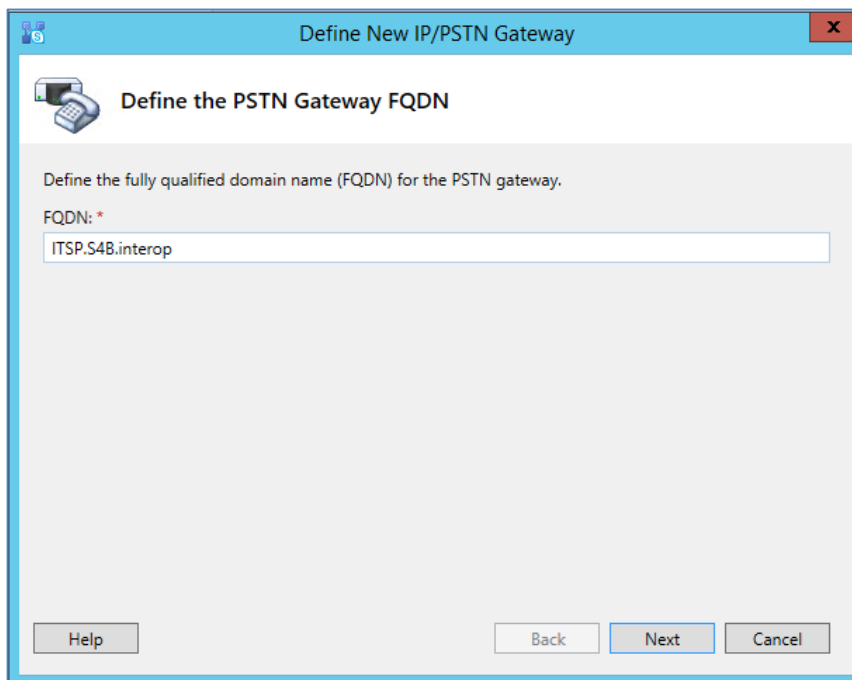
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



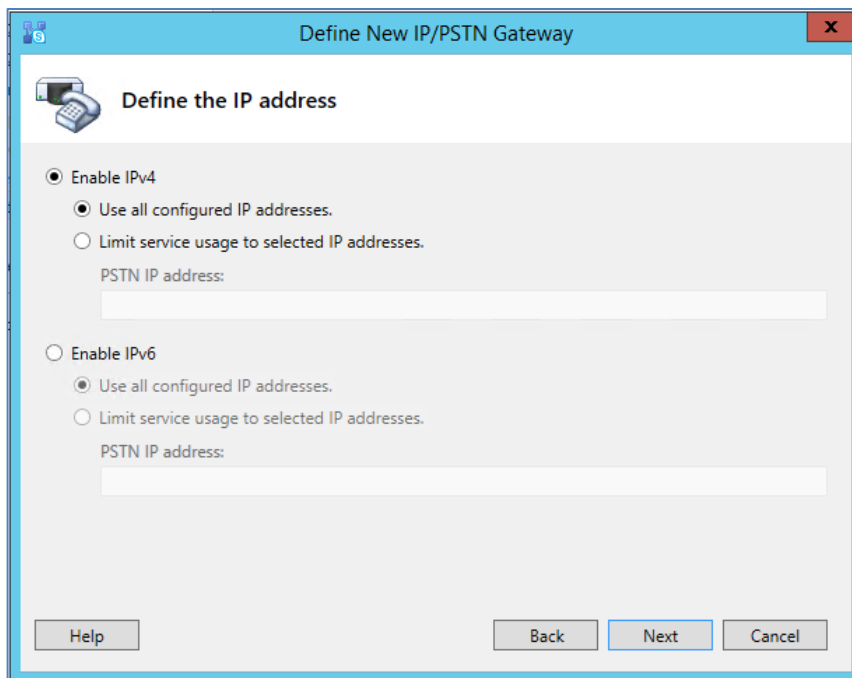
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP.S4B.interop**). This FQDN should be equivalent to the configured Subject Name (CN) in the TLS Certificate Context (see Section 4.9.3 on page 58).
6. Click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



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

and FQDN, and gateway listening port.

**Notes:**

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

Figure 3-8: Define the Root Trunk

Define New IP/PSTN Gateway

Define the root trunk

Trunk name: *
ITSP.S4B.interop

Listening port for IP/PSTN gateway: *
5067

SIP Transport Protocol:
TLS

Associated Mediation Server:
FE.S4B.interop Interop

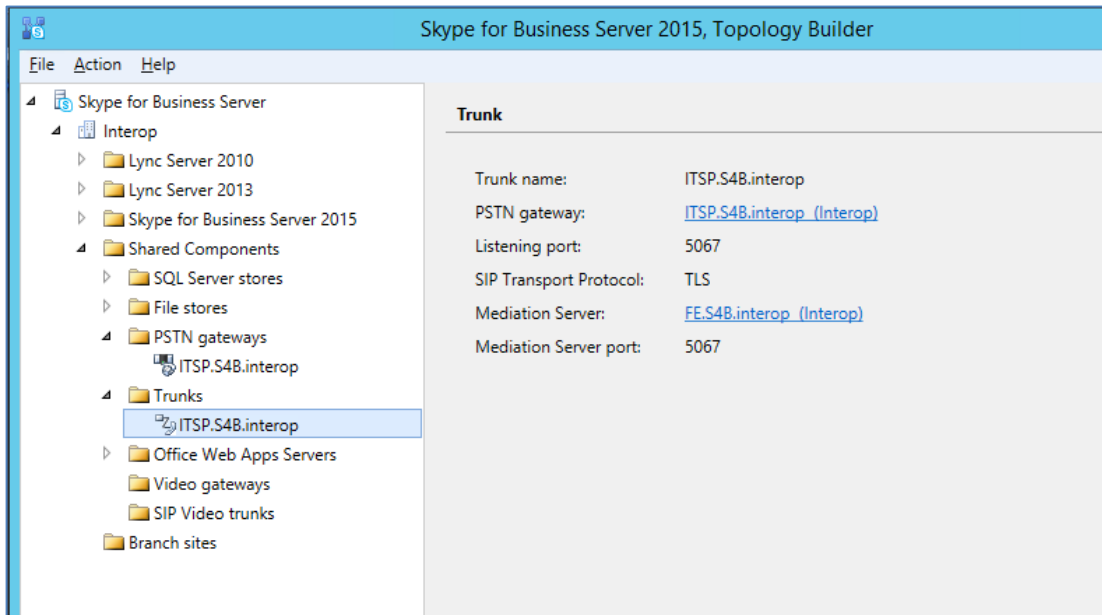
Associated Mediation Server port: *
5067

Help Back Finish Cancel

- a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**). This parameter is later configured in the SIP Interface table (see Section 4.3 on page 36).
- b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses. This parameter is later configured in the SIP Interface table (see Section 4.3 on page 36).
- c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
- d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
- e. Click **Finish**.

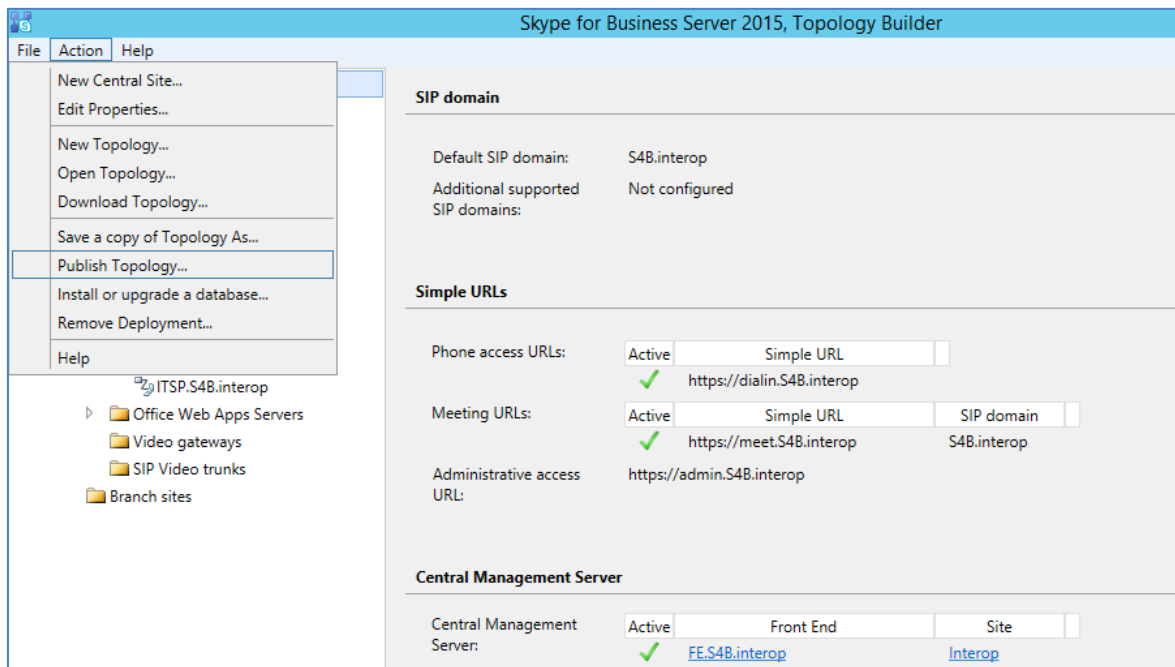
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



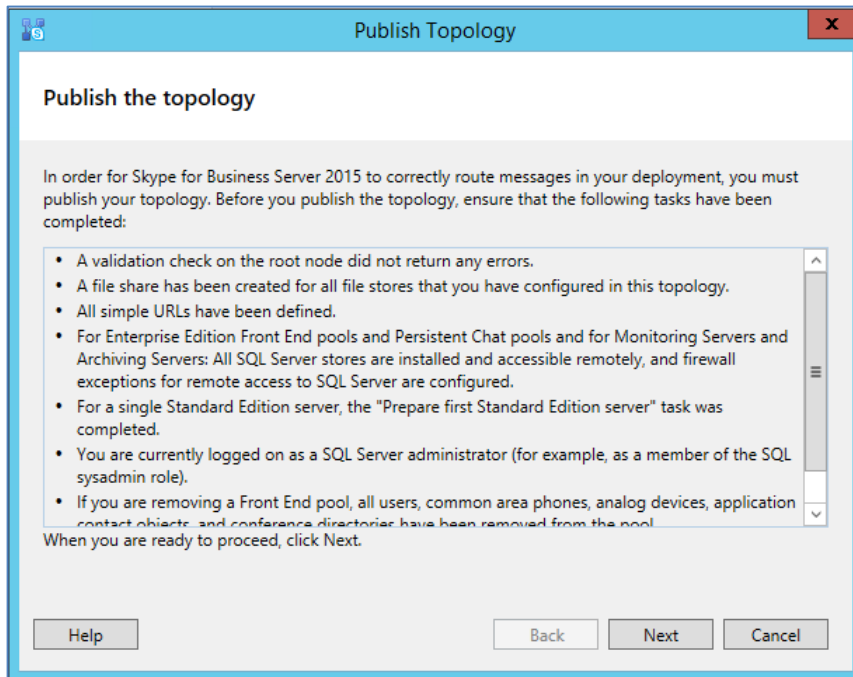
9. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



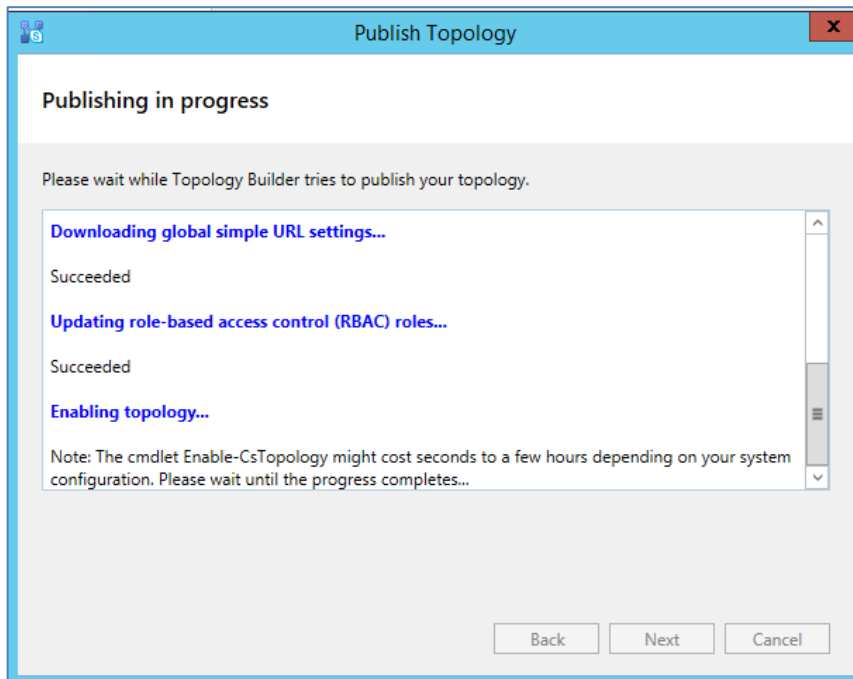
The following is displayed:

Figure 3-11: Publish the Topology



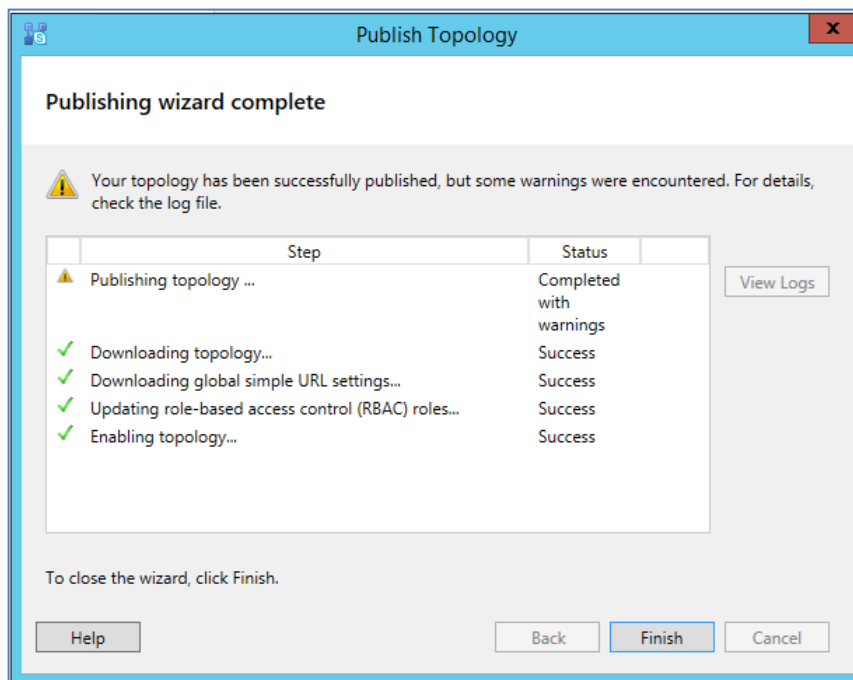
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



- Click **Finish**.

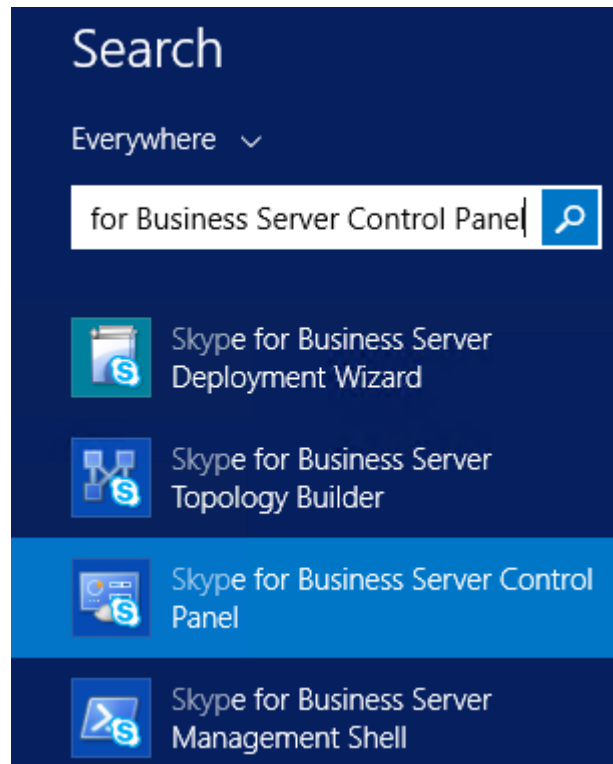
3.2 Configuring the "Route" on Skype for Business Server 2015

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

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

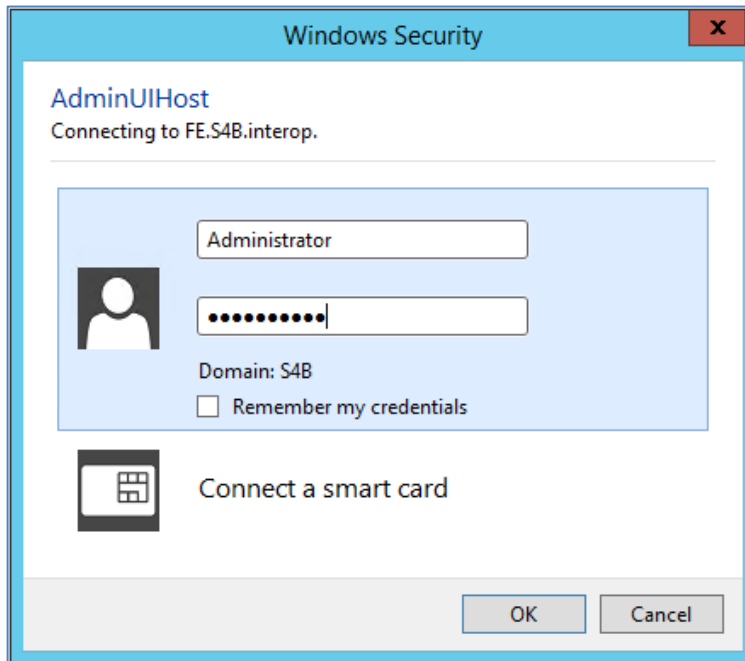
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

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



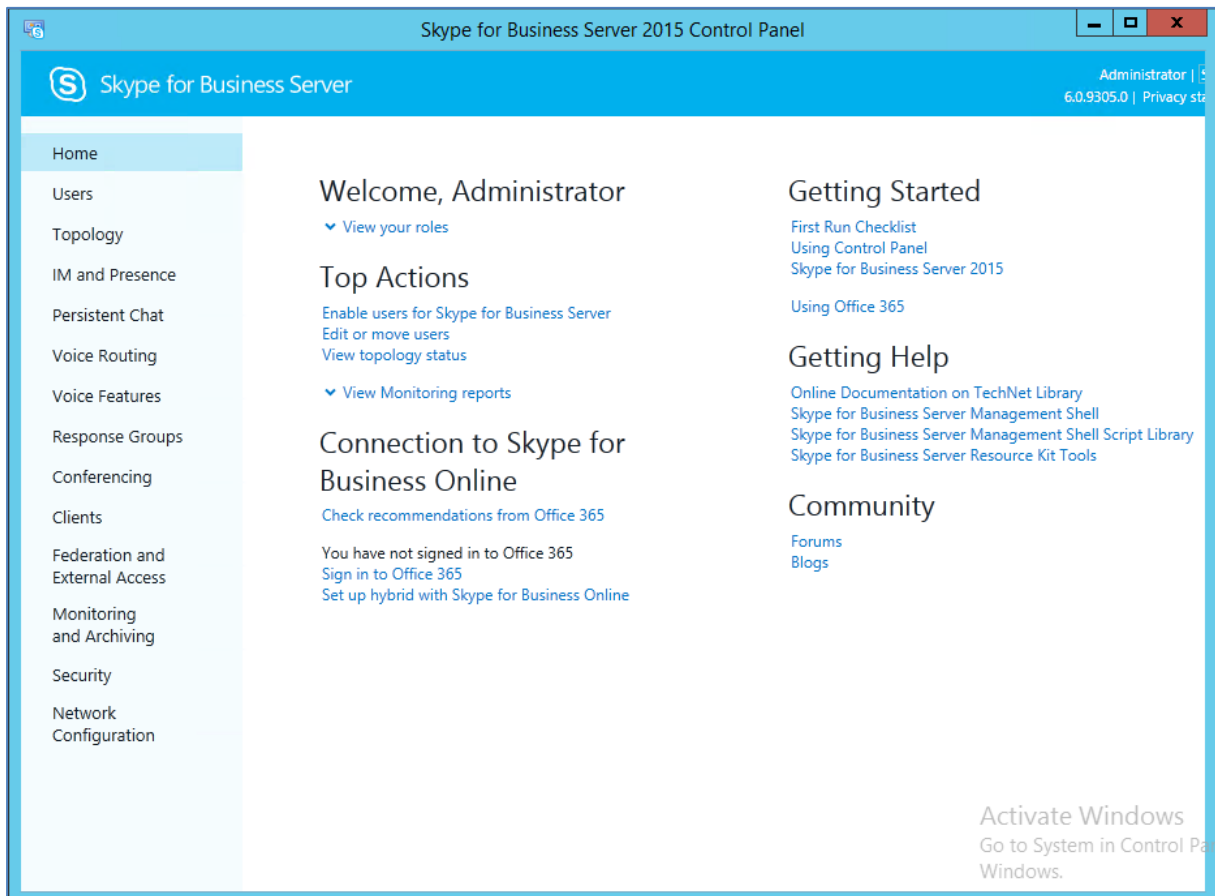
- You are prompted to enter your login credentials:

Figure 3-15: Skype for Business Server Credentials



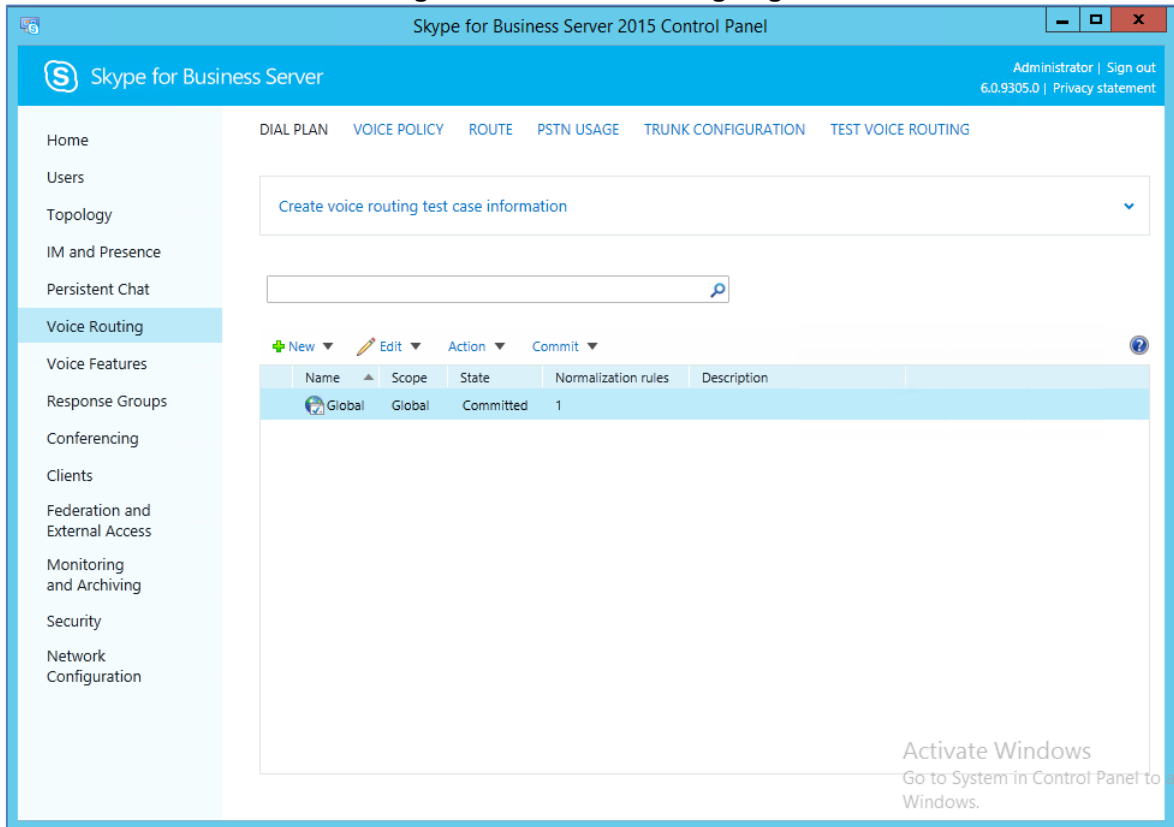
- Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

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



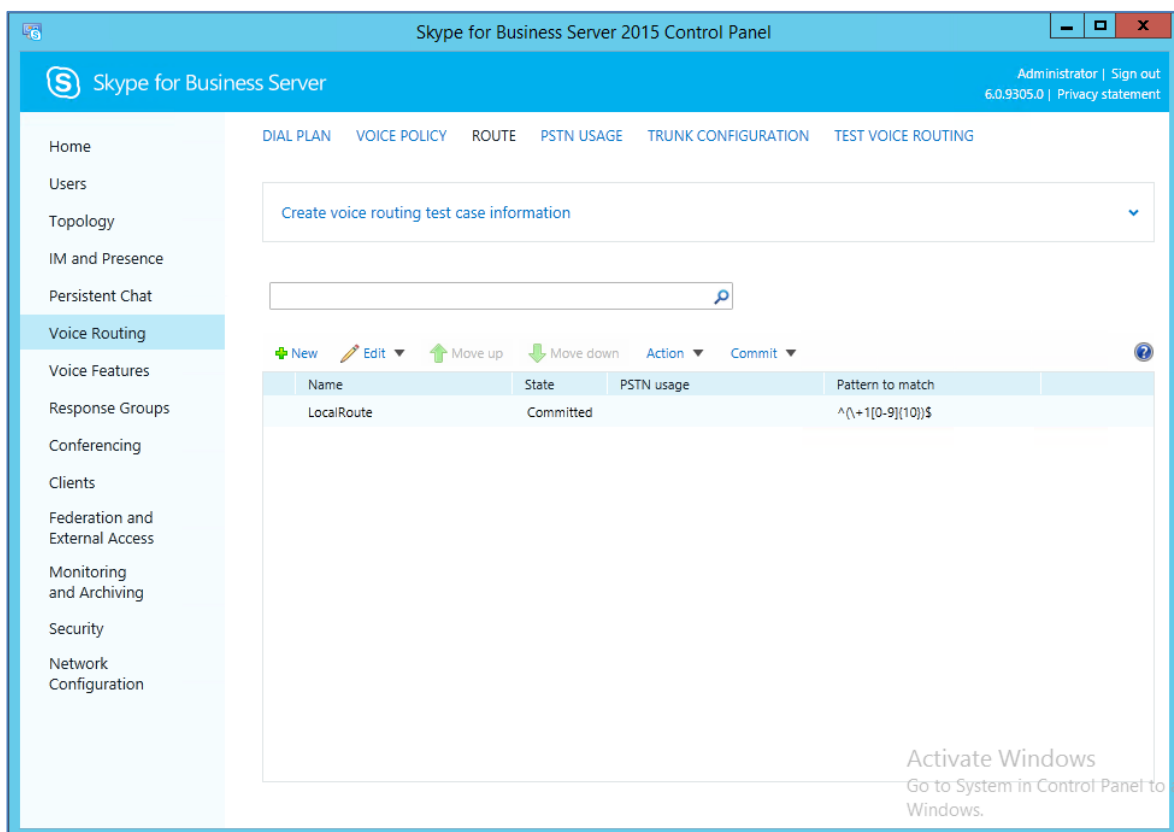
- In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



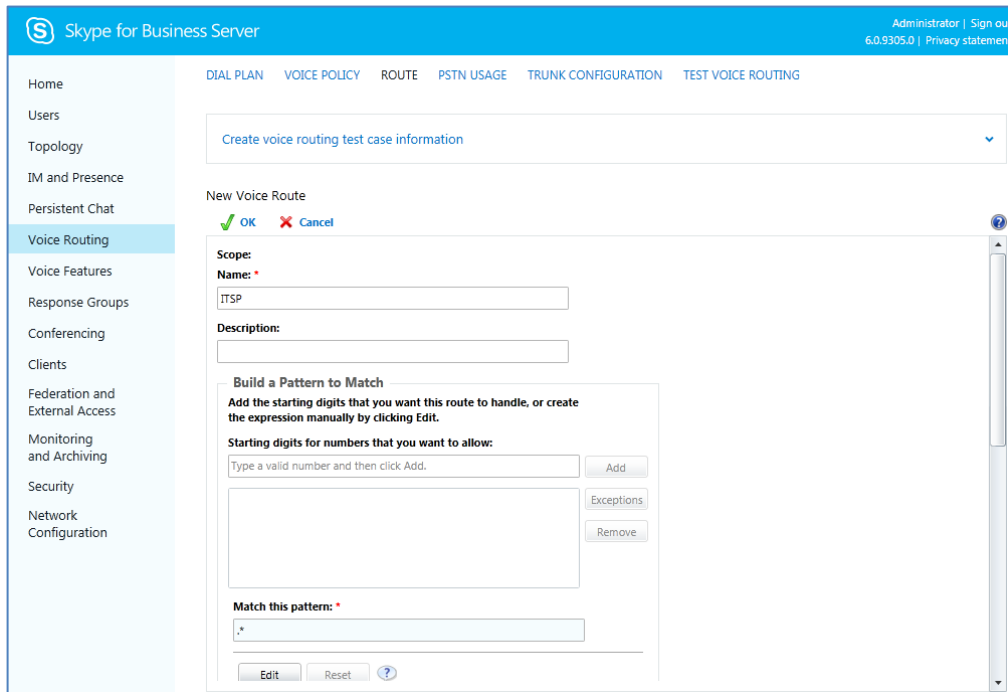
- In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



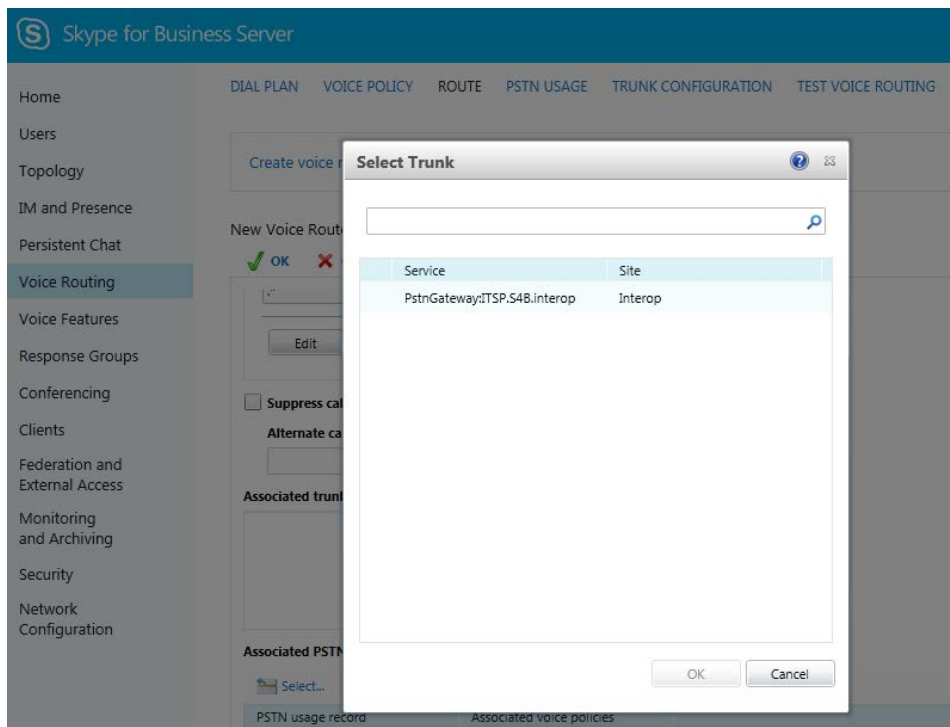
6. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



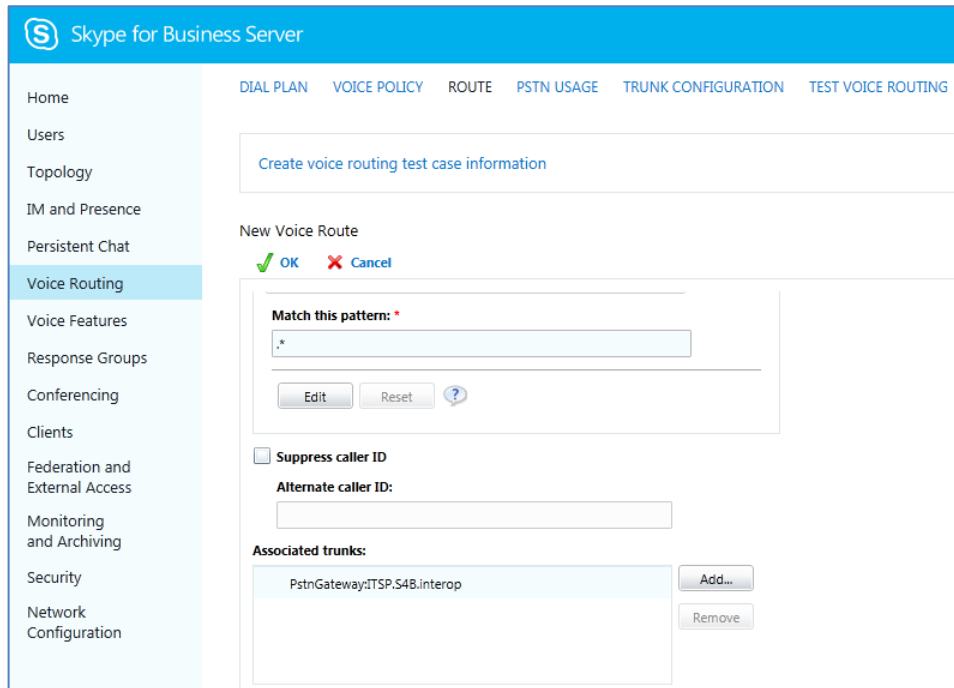
7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).
8. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.
9. Associate the route with the E-SBC Trunk that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

Figure 3-20: List of Deployed Trunks



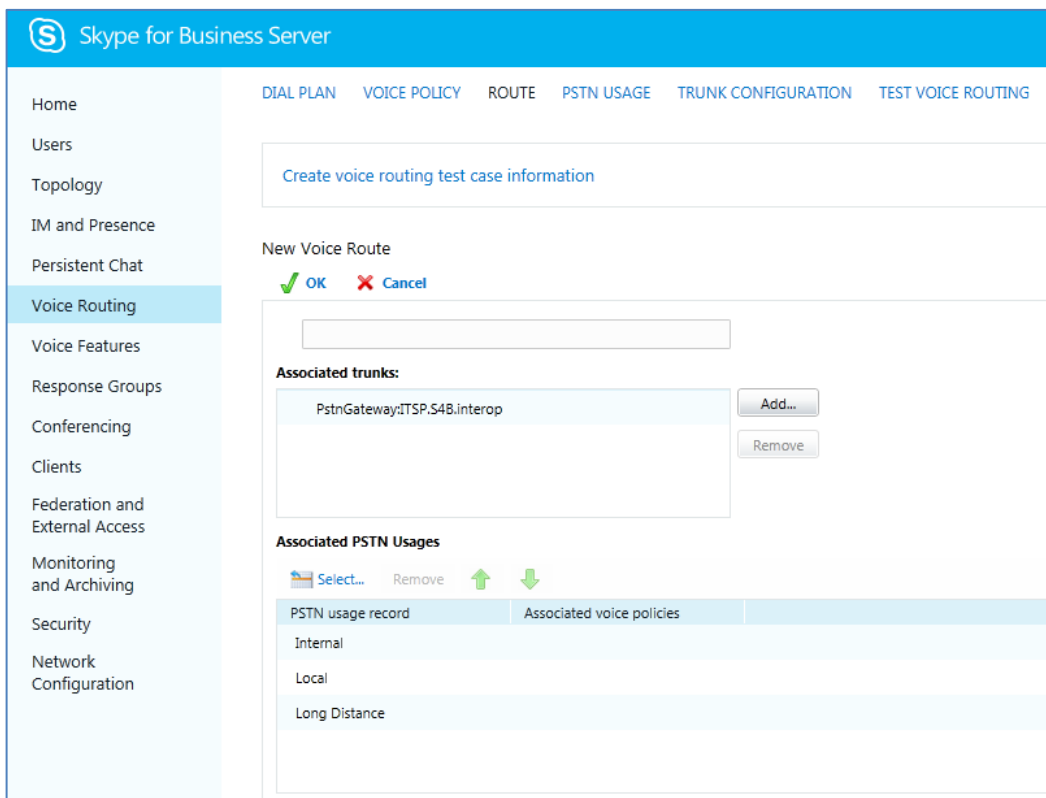
- b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-21: Selected E-SBC Trunk



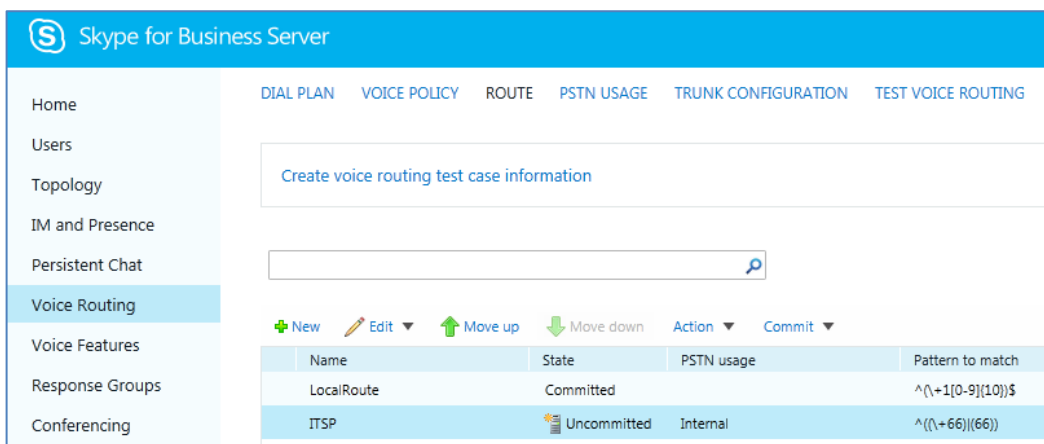
- 10. Associate a PSTN Usage to this route:
 - Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-22: Associating PSTN Usage to Route



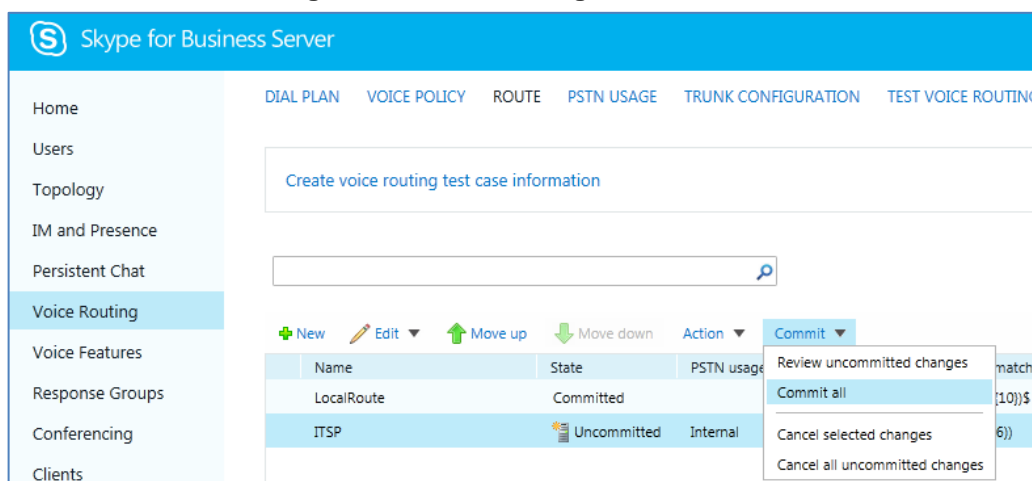
- Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-23: Confirmation of New Voice Route



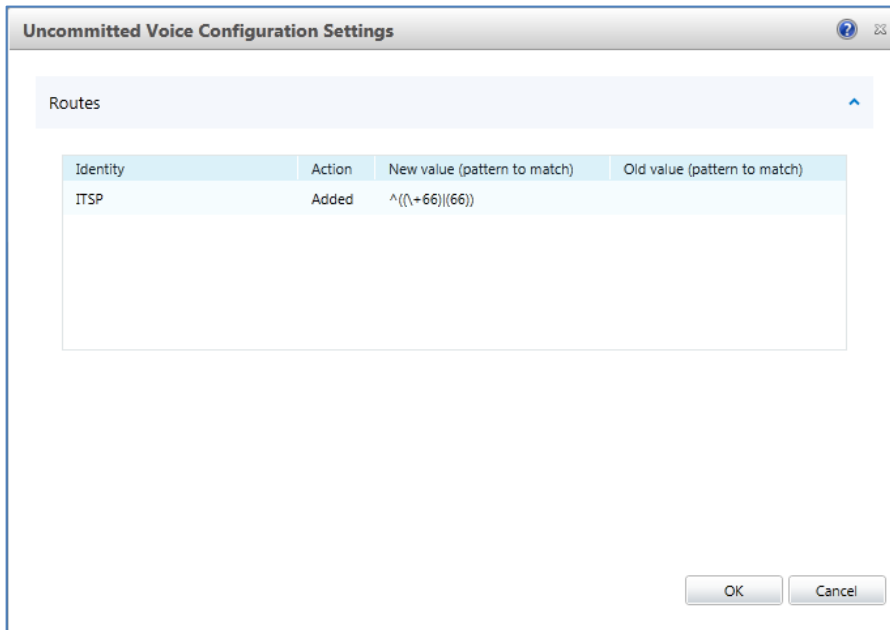
- From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-24: Committing Voice Routes



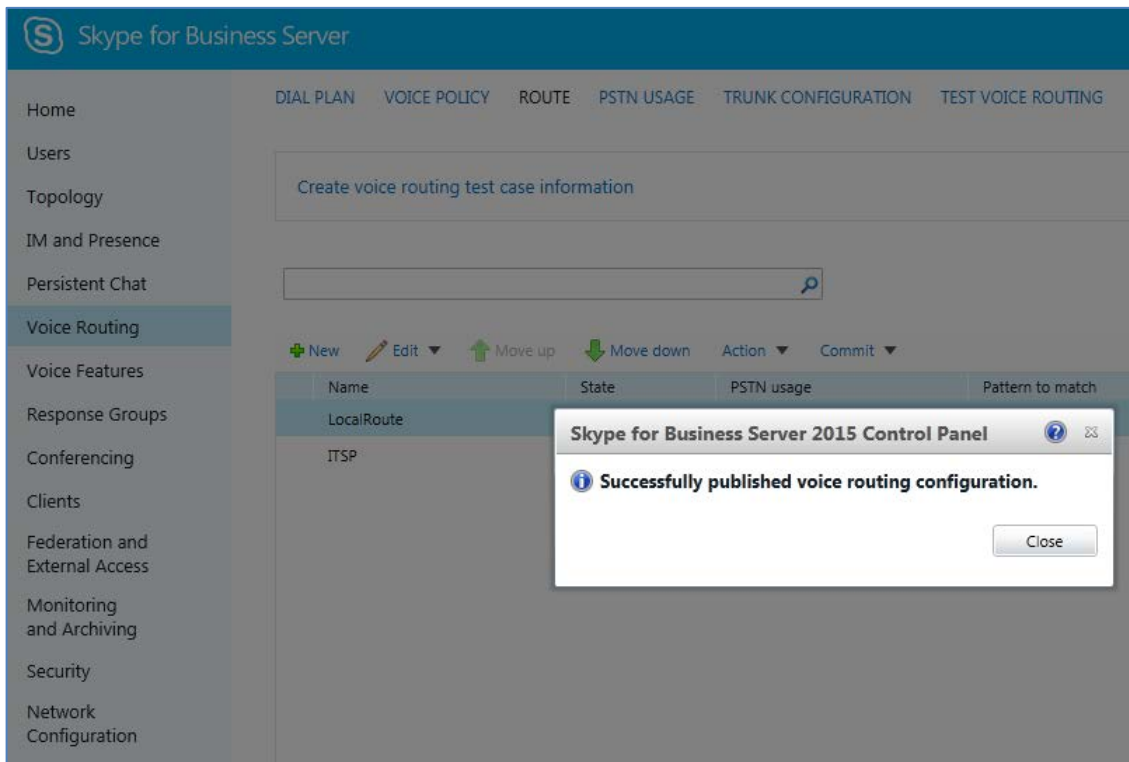
The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



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

Figure 3-26: Confirmation of Successful Voice Routing Configuration



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

Figure 3-27: Voice Routing Screen Displaying Committed Routes

The screenshot shows the 'Voice Routing' section of the Skype for Business Server administration console. The 'ROUTE' tab is selected. A table displays the following routes:

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

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



Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Skype for Business user number). This ID is required by Rogers 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).

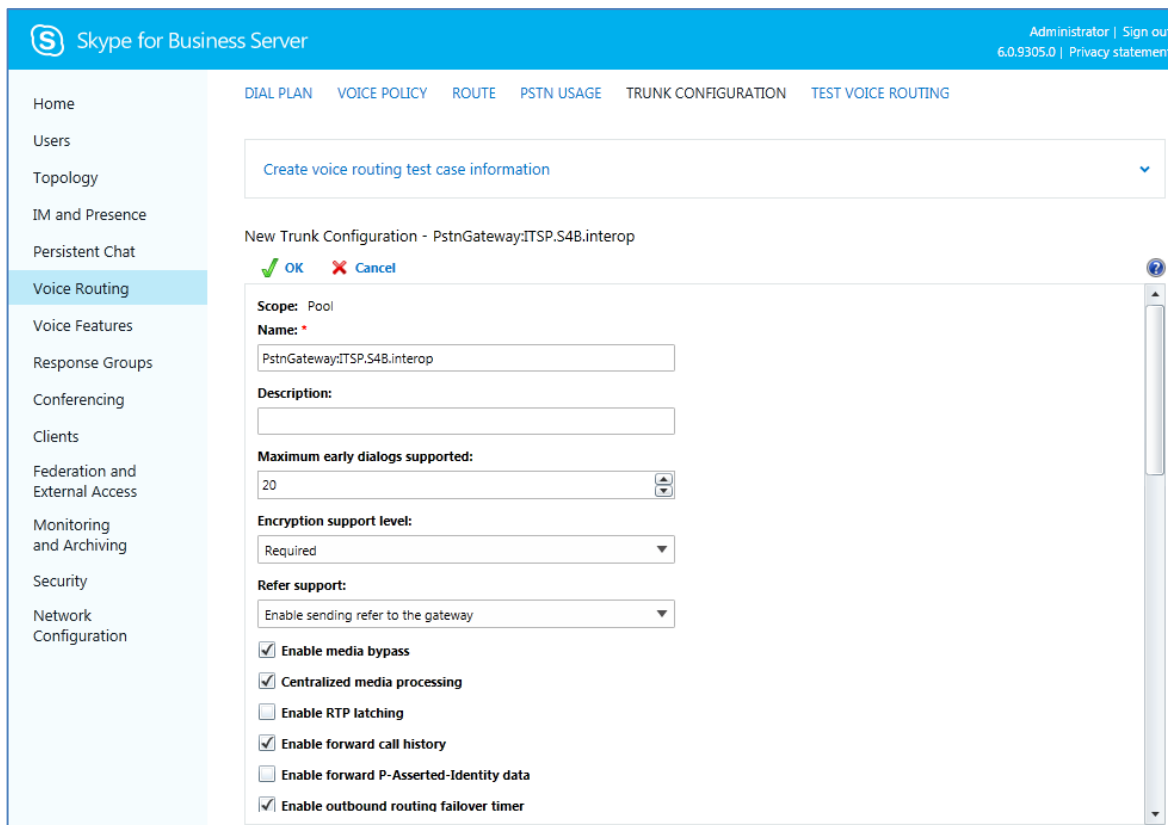
- a. In the Voice Routing page, select the **Trunk Configuration** tab. Note that you can add and modify trunk configuration by site or by pool.

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

The screenshot shows the 'Trunk Configuration' tab selected in the Voice Routing section. A table displays the following configuration:

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

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



- c. Select the **Enable forward call history** check box, and then click **OK**.
 - d. Repeat Steps 11 through 13 to commit your settings.
16. Use the following command on the Skype for Business Server Management Shell after reconfiguration to verify correct values:

■ **Get-CsTrunkConfiguration**

```

Identity :
Service:PstnGateway:ITSP.S4B.interop
OutboundTranslationRulesList :
SipResponseCodeTranslationRulesList : {}
OutboundCallingNumberTranslationRulesList : {}
PstnUsages : {}
Description :
ConcentratedTopology : True
EnableBypass : True
EnableMobileTrunkSupport : False
EnableReferSupport : True
EnableSessionTimer : True
EnableSignalBoost : False
MaxEarlyDialogs : 20
RemovePlusFromUri : False
RTCPActiveCalls : True
RTCPCallsOnHold : True
SRTPMode : Required
EnablePIDFLOSupport : False
EnableRTPLatching : False
EnableOnlineVoice : False
ForwardCallHistory : True
    
```

Enable3pccRefer	: False
ForwardPAI	: False
EnableFastFailoverTimer	: True
EnableLocationRestriction	: False
NetworkSiteID	:

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Skype for Business Server 2015 and the Rogers 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 - Rogers 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 Rogers SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a License Key that includes the following software features:

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

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

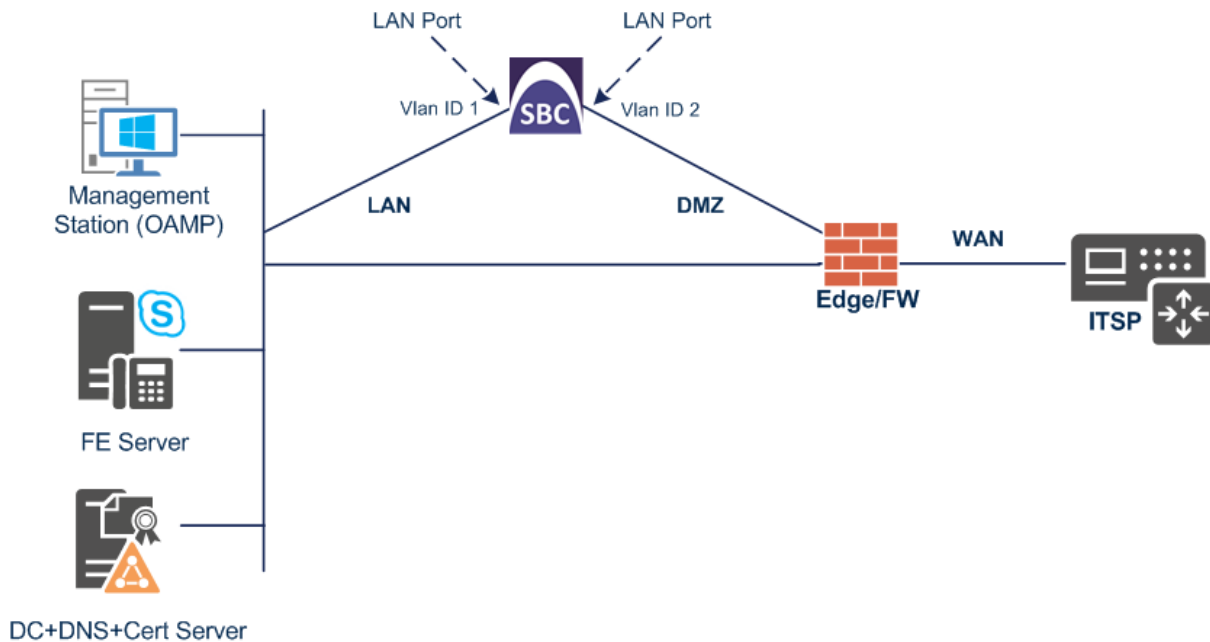
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on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

4.1 Step 1: IP Network Interfaces Configuration

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

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

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

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

➤ **To configure the VLANs:**

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

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

Figure 4-2: Configured VLAN IDs in Ethernet Device

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

4.1.2 Step 1b: Configure Network Interfaces

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

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

➤ **To configure the IP network interfaces:**

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

Parameter	Value
Name	LAN_IF (arbitrary descriptive name)
Ethernet Device	vlan 1
IP Address	10.15.17.77 (LAN IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Default Gateway	10.15.0.1
Primary DNS	10.15.27.1

3. Add a network interface for the WAN side:

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

Parameter	Value
Name	WAN_IF
Application Type	Media + Control
Ethernet Device	vlan 2
IP Address	195.189.192.153 (DMZ IP address of E-SBC)
Prefix Length	25 (subnet mask in bits for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
Primary DNS	80.179.52.100
Secondary DNS	80.179.55.100

4. Click **Apply**.

The configured IP network interfaces are shown below:

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

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

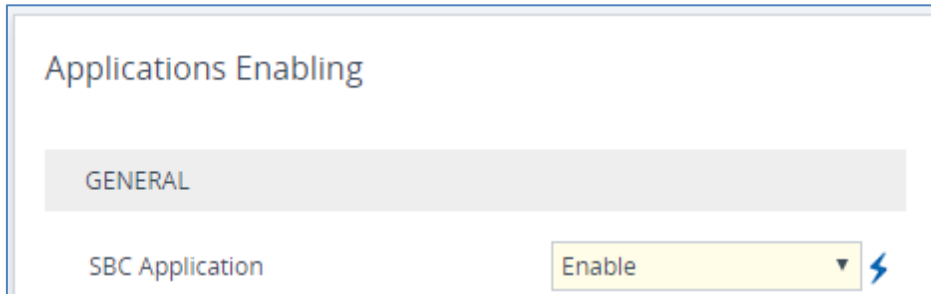
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.15 on page 77).

4.3 Step 3: Configure Media Realms

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

➤ **To configure Media Realms:**

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

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

Figure 4-5: Configuring Media Realm for LAN

Media Realms [MRLan]
- x

GENERAL

Index

Name

Topology Location

IPv4 Interface Name [View](#)

Port Range Start

Number Of Media Session Legs

Port Range End

Default Media Realm

QUALITY OF EXPERIENCE

QoE Profile [View](#)

Bandwidth Profile [View](#)

Cancel APPLY

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Name	MRWan (arbitrary name)
Topology Location	Up
IPv4 Interface Name	WAN_IF
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 screenshot shows the configuration interface for a Media Realm named 'MRWan'. The 'GENERAL' tab is active, showing the following settings:

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

The 'QUALITY OF EXPERIENCE' tab is also visible, showing:

- QoS Profile: --
- Bandwidth Profile: --

Buttons for 'Cancel' and 'APPLY' are located at the bottom of the window.

The configured Media Realms are shown in the figure below:

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

Media Realms (2)

+ New
Edit
|
🗑

⏪ << Page 1 of 1 >> ⏩ Show 10 records per page

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

4.4 Step 4: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the E-SBC.

➤ **To configure SIP Interfaces:**

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

Parameter	Value
Index	0
Name	S4B (see note at the end of this section)
Network Interface	LAN_IF
Application Type	SBC
UDP Port (for supporting Fax ATA device)	5060 (if required)
TCP	0
TLS Port	5067 (see note below)
Media Realm	MRLan



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

3. Configure a SIP Interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

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

SIP Interfaces (2)

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

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATION PROTOCOL	MEDIA REALM
0	S4B	DefaultSRD	Voice	SBC	5060	0	5067	No encapsulation	MRLan
1	SP	DefaultSRD	DMZ	SBC	5060	0	0	No encapsulation	MRWan



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

4.5 Step 5: Configure Proxy Sets

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

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

- Microsoft Skype for Business Server 2015
- Rogers SIP Trunk
- Fax supporting 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 (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Add a Proxy Set for the Skype for Business Server 2015 as shown below:

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

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

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

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

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

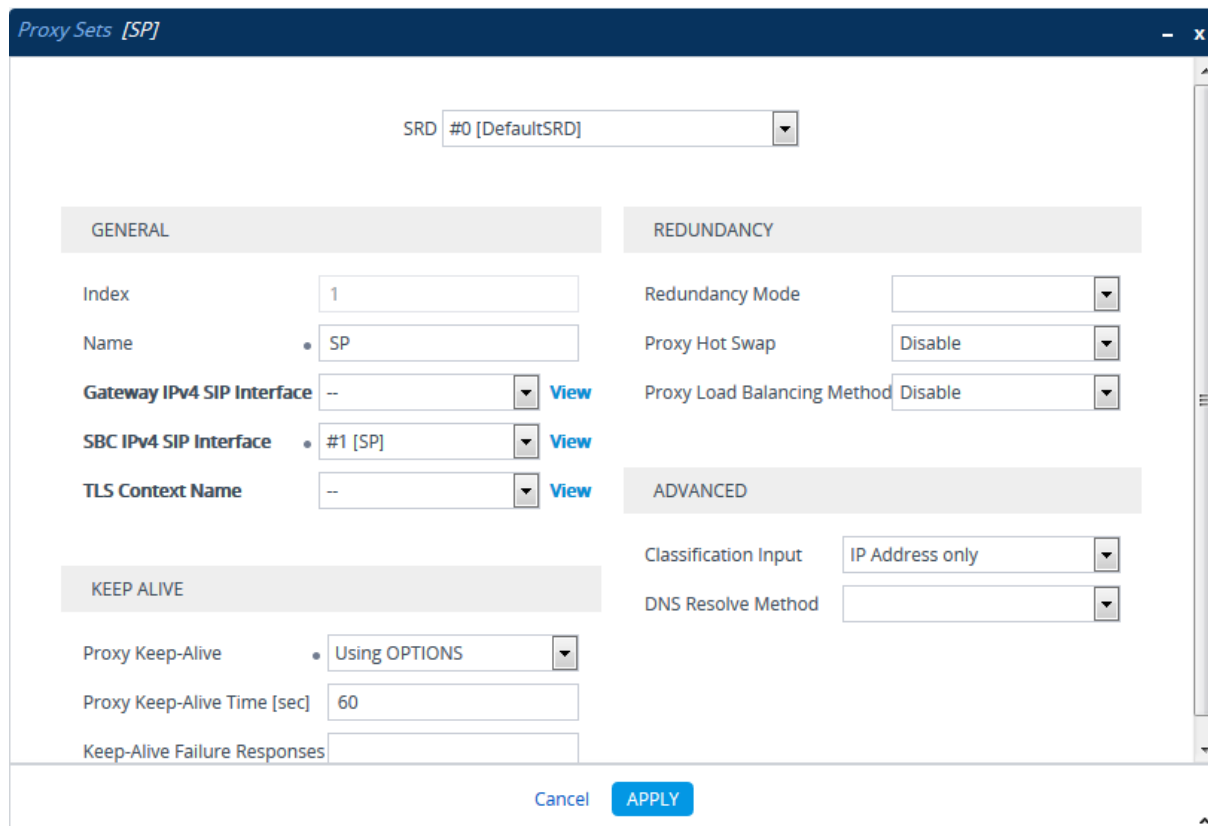
d. Click **Apply**.

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

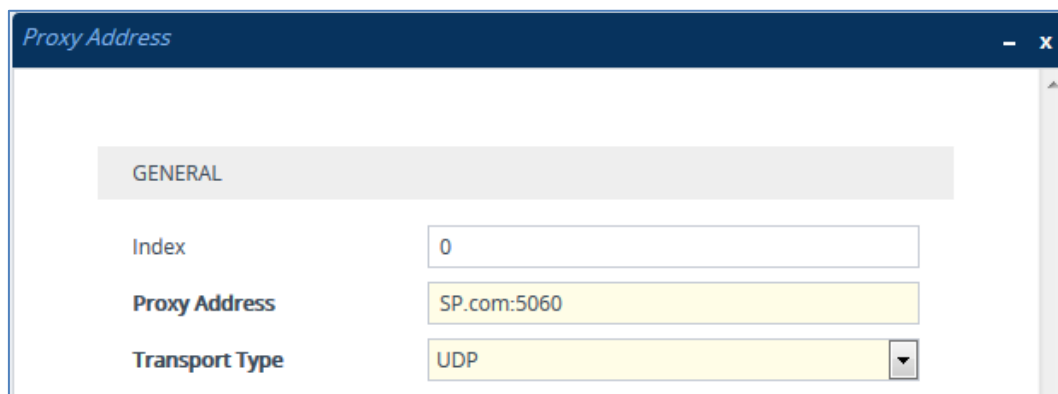
3. Configure a Proxy Set for the Rogers SIP Trunk:

Parameter	Value
Index	2
Name	SP
SBC IPv4 SIP Interface	SP
Proxy Keep-Alive	Using Options

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



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

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


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

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

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

Parameter	Value
Index	3
Name	Fax
SBC IPv4 SIP Interface	S4B

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

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

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

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

d. Click **Apply**.

Parameter	Value
Index	0
Proxy Address	10.15.17.12:5060 (IP address / FQDN and destination port)
Transport Type	UDP

The configured Proxy Sets are shown in the figure below:

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

Proxy Sets (3)

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

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

4.6 Step 6: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Skype for Business Server 2015 supports the G.711 coder while the network connection to Rogers 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 Rogers SIP Trunk.

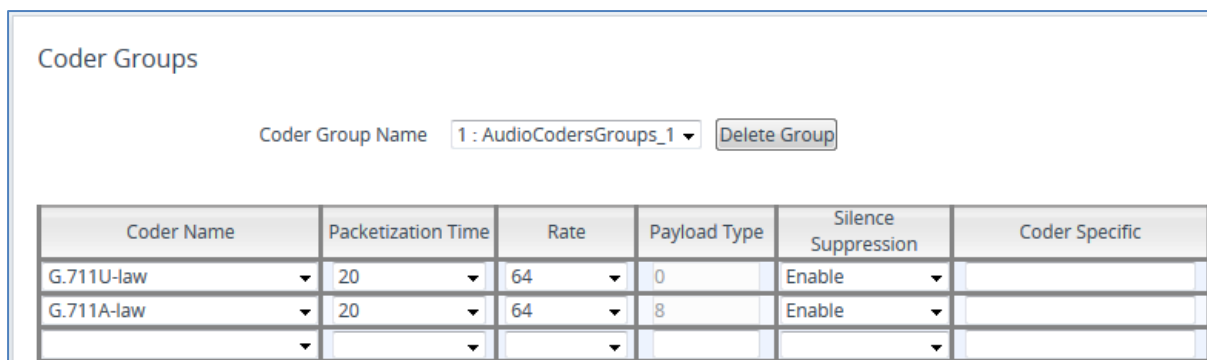
Note that the Coder Group ID for this entity will be assign to its corresponding IP Profile in the next step.

➤ **To configure coders:**

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

Parameter	Value
Coder Group Name	AudioCodersGroups_1
Coder Name	<ul style="list-style-type: none"> ▪ G.711 U-law ▪ G.711 A-law
Silence Suppression	Enable (for both coders)

Figure 4-16: Configuring Coder Group for Skype for Business Server 2015



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

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

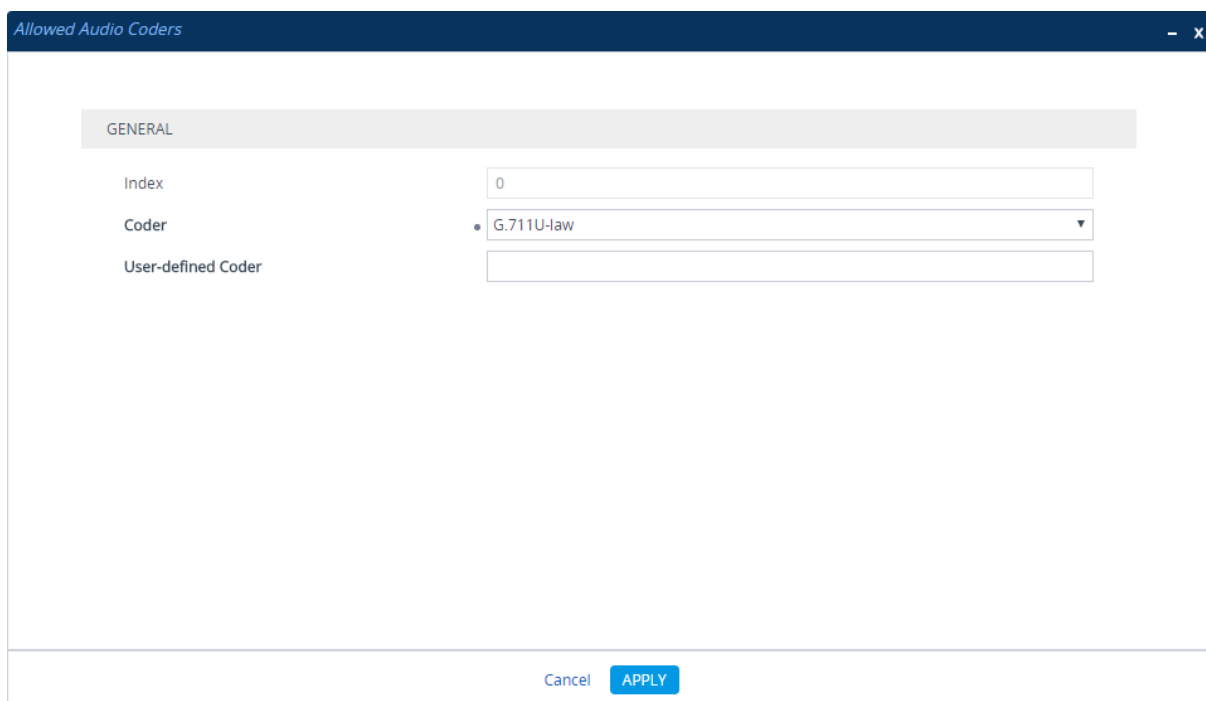
Figure 4-17: Configuring Allowed Coders Group for Rogers SIP Trunk



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

Parameter	Value
Index	0
Coder	G.711U-law

Figure 4-18: Configuring Allowed Coders for Rogers SIP Trunk



The screenshot shows a configuration window titled "Allowed Audio Coders". Inside, there is a "GENERAL" section with the following fields:

- Index:** A text input field containing the value "0".
- Coder:** A dropdown menu with "G.711U-law" selected.
- User-defined Coder:** An empty text input field.

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

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

Figure 4-19: SBC Preferences Mode

The screenshot shows the 'Media Settings' page with several sections:

- GENERAL**
 - NAT Traversal: Disable NAT
 - Enable Continuity Tones: Disable
 - Inbound Media Latch Mode: Dynamic
 - Number of Media Channels: 0
 - Enforce Media Order: Disable
 - SDP Session Owner: AudiocodesGW
- ROBUSTNESS**
 - New RTP Stream Packets: 3
 - New RTCP Stream Packets: 3
 - New SRTP Stream Packets: 3
 - New SRTCP Stream Packets: 3
 - Timeout To Relatch RTP (msec): 200
 - Timeout To Relatch SRTP (msec): 200
 - Timeout To Relatch Silence (msec): 10000
 - Timeout To Relatch RTCP (msec): 10000
- SBC SETTINGS**
 - Preferences Mode: **Include Extensions** (indicated by an arrow)
 - Enforce Media Order: Disable
- GATEWAY SETTINGS**
 - Enable Early Media: Disable
 - Multiple Packetization Time Format: None

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

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

4.7 Step 7: Configure IP Profiles

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

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

- Microsoft Skype for Business Server 2015 – to operate in secure mode using SRTP and SIP over TLS
- Rogers SIP trunk – to operate in non-secure mode using RTP and SIP over UDP
- Fax ATA device – to operate in non-secure mode using RTP and SIP over UDP

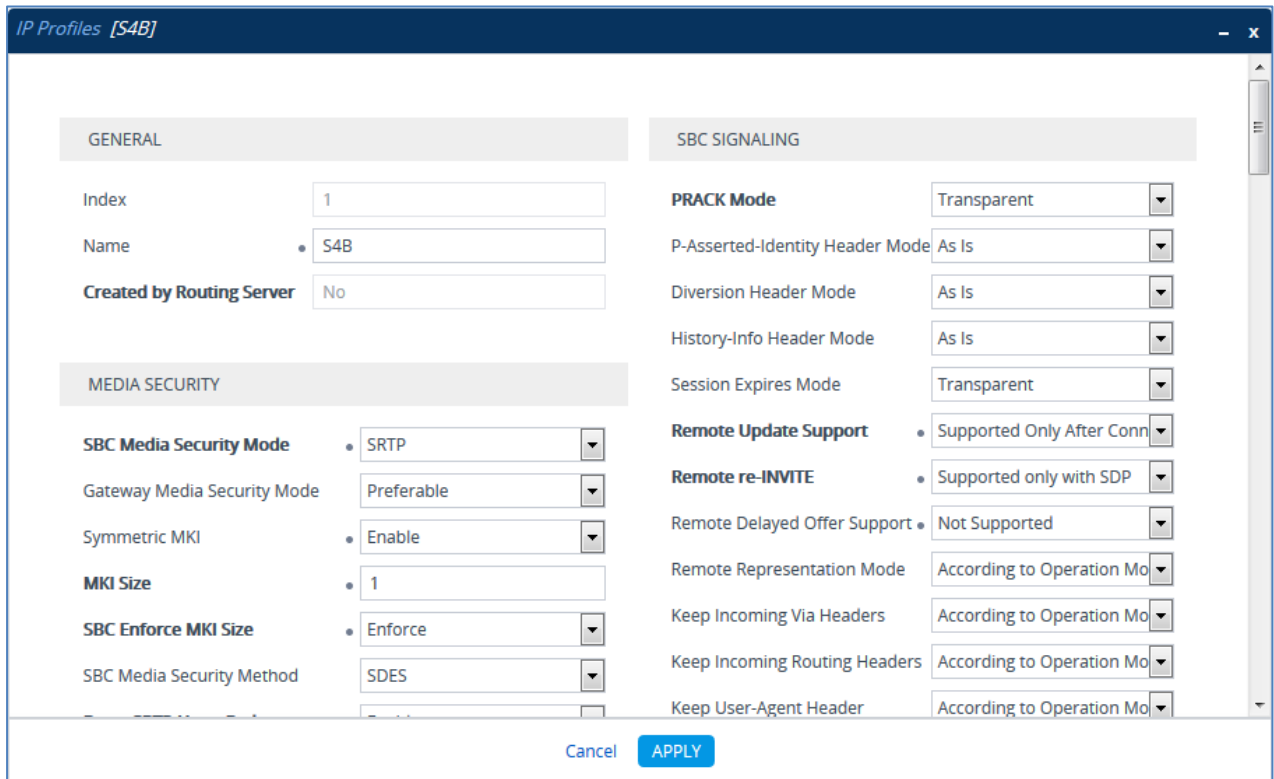
➤ **To configure IP Profile for the Skype for Business Server 2015:**

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

Parameter	Value
General	
Index	1
Name	S4B
Media Security	
SBC Media Security Mode	SRTP
Symmetric MKI	Enable
MKI Size	1
Enforce MKI Size	Enforce
Reset SRTP State Upon Re-key	Enable
Generate SRTP Keys Mode:	Always
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	AudioCodersGroups_1
RTCP Mode	Generate Always
SBC Signaling	
Remote Update Support	Supported Only After Connect
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	

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

Figure 4-20: Configuring IP Profile for Skype for Business Server 2015



3. Click **Apply**.

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

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

Parameter	Value
General	
Index	2
Name	SP
Media Security	
SBC Media Security Mode	RTP
SBC Early Media	
Remote Can Play Ringback	Yes (required, as Skype for Business Server 2015 does not provide a Ringback tone for incoming calls)
SBC Media	
Extension Coders Group	
Allowed Audio Coders	SP Allowed Coders
Allowed Coders Mode	Restriction
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Play RBT To Transferee	Yes
SBC Hold	
Remote Hold Format	Not Supported

Figure 4-21: Configuring IP Profile for Rogers SIP Trunk

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

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

2. Click **Apply**.

➤ **To configure an IP Profile for the FAX supporting ATA (if required):**

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

Parameter	Value
Index	3
Profile Name	Fax

Figure 4-22: Configuring IP Profile for FAX ATA

The screenshot shows the configuration interface for an IP Profile named 'Fax'. It is divided into two main sections: GENERAL and SBC SIGNALING. The GENERAL section contains the following parameters:

- Index:** 3
- Name:** Fax
- Created by Routing Server:** No

The SBC SIGNALING section contains the following parameters:

- PRACK Mode:** Transparent
- P-Asserted-Identity Header Mode:** As Is
- Diversion Header Mode:** As Is
- History-Info Header Mode:** As Is
- Session Expires Mode:** Transparent
- Remote Update Support:** Supported
- Remote re-INVITE:** Supported
- Remote Delayed Offer Support:** Supported
- Remote Representation Mode:** According to Operation Mod
- Keep Incoming Via Headers:** According to Operation Mod
- Keep Incoming Routing Headers:** According to Operation Mod
- Keep User-Agent Header:** According to Operation Mod

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

2. All other parameters leave as Default.
3. Click **Apply**.

4.8 Step 8: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

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

- Skype for Business Server 2015 (Mediation Server) located on LAN
- Rogers SIP Trunk located on WAN
- Fax supporting ATA device located on LAN (if required)

➤ To configure IP Groups:

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

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

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

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

4. Configure an IP Group for the Fax supporting 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

IP Groups (3)

+ New Edit

Page 1 of 1 Show 10 records per page

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

4.9 Step 9: SIP TLS Connection Configuration

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

4.9.1 Step 9a: Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or a third-party server) to ensure that the E-SBC receives the accurate and current date and time. This is necessary for validating certificates of remote parties.

➤ **To configure the NTP server address:**

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

Figure 4-24: Configuring NTP Server Address

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

3. Click **Apply**.

4.9.2 Step 9b: Configure the TLS version

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

➤ **To configure the TLS version:**

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

Figure 4-25: Configuring TLS version

4. Click **Apply**.

4.9.3 Step 9c: Configure a Certificate

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

The procedure involves the following main steps:

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



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

➤ **To configure a certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **ITSP.S4B.interop**).
 - b. Fill in the rest of the request fields according to your security provider's instructions.

- c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-26: Certificate Signing Request – Creating CSR

← TLS Context [#0] > Context Certificates

CERTIFICATE SIGNING REQUEST

Subject Name [CN]

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

Signature Algorithm

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAIBADAbMRkwFwYDVQQDDBBjVFNQL1M0Q15pbmR1cm9wMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCzEs8XTnY8be/t77eEDG7rTg747GQ30DFOC4Rs
x+e9KfbErZgxMYqGT8u04AU0wU9LUPkkq+8gI6w2bg3boW0kg/9hrnNL2rf1tGcn
30oShP05PiKmRNZnCC090b03tbr9kuHmlwPRQ7yT6k7xS3XBbSigqT4LQbjBT1tt
hDH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAim/GA2E1ZQbZaR6CZyIaw1T
u65w450NFHmaC1uHSyZ8keM8d1Ux14hkw7t5ygAD8KbxVkHRVaCgcQrAK2v8u1Pf
TvN+bwJ+kQ0d59CiXa82e0o1W83buPq5+qMDGTF+MyJwGVf8SIC1c6+zFoc+BEZY
7tQ8y0J8od0aDhStDFQ=
-----END CERTIFICATE REQUEST-----
```

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

Figure 4-27: Microsoft Certificate Services Web Page

Microsoft Certificate Services -- Demolab Home

Welcome

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

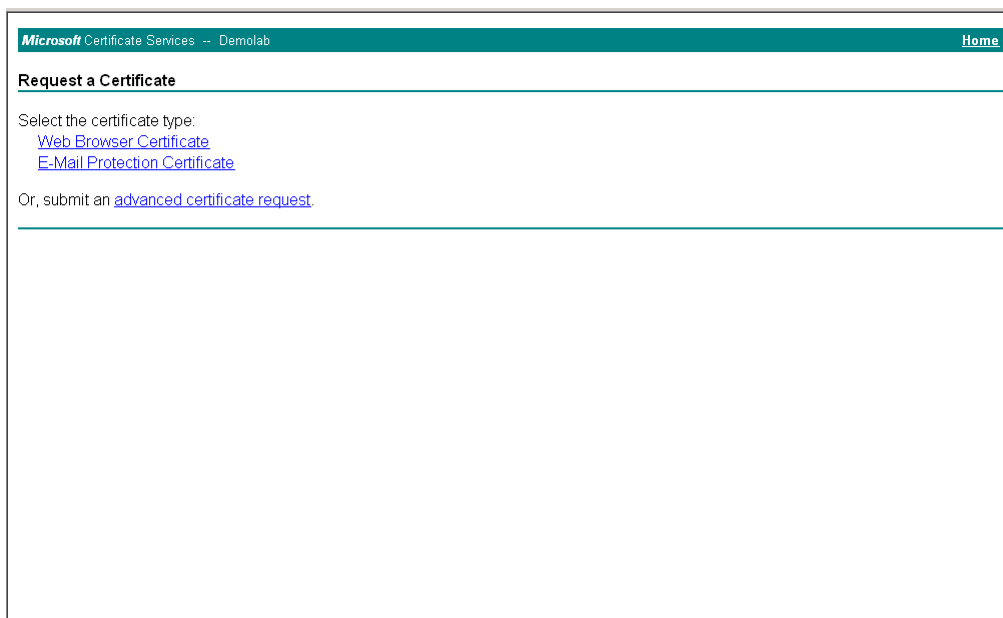
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- Click **Request a certificate**.

Figure 4-28: Request a Certificate Page


Microsoft Certificate Services -- Demolab Home

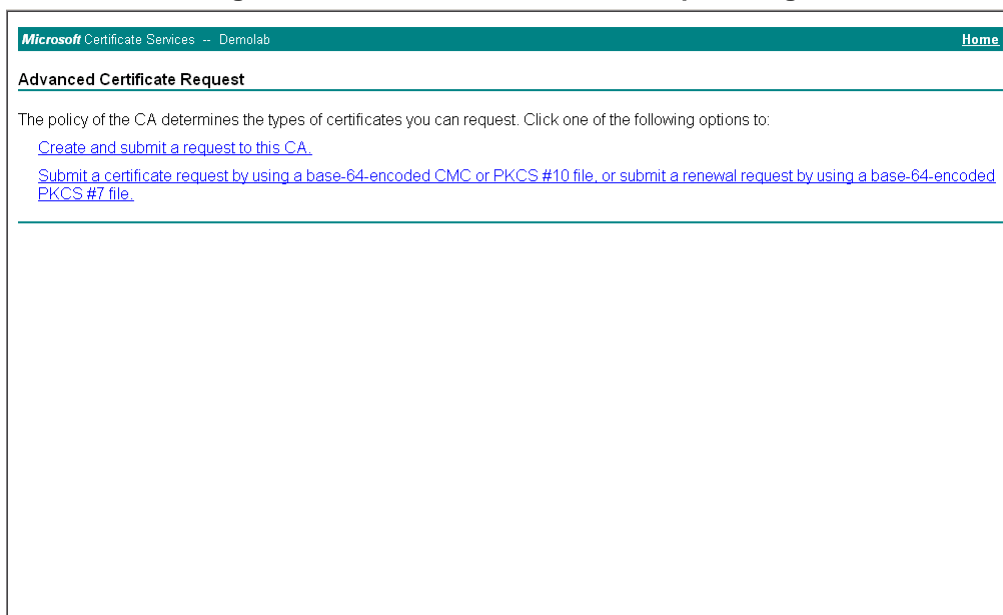
Request a Certificate

Select the certificate type:

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

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

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

Figure 4-29: Advanced Certificate Request Page


Microsoft Certificate Services -- Demolab Home

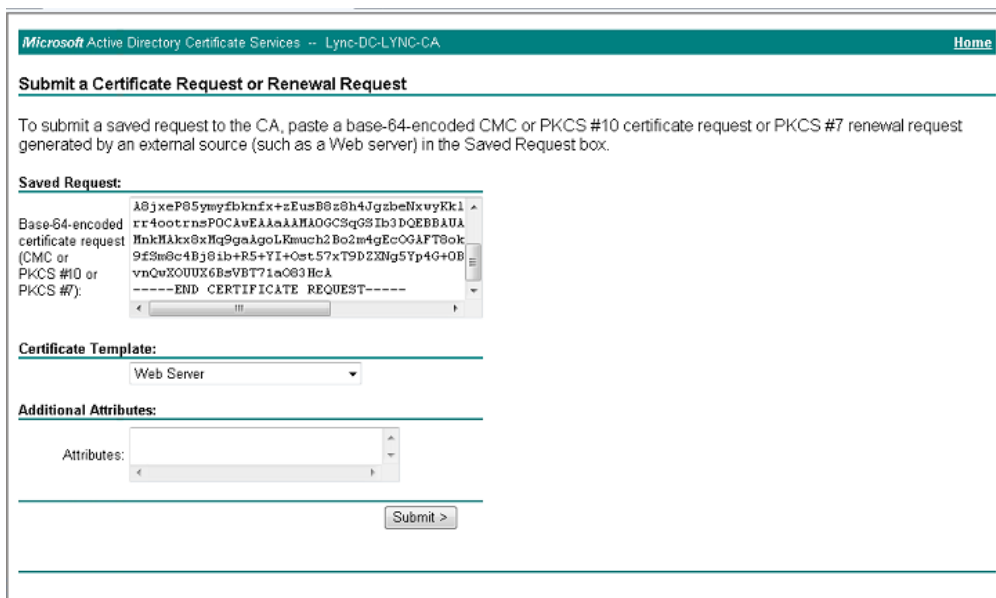
Advanced Certificate Request

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

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

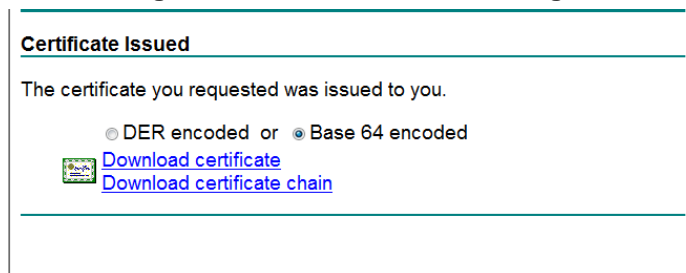
- Click **Submit a certificate request ...**, and then click **Next**.

Figure 4-30: Submit a Certificate Request or Renewal Request Page

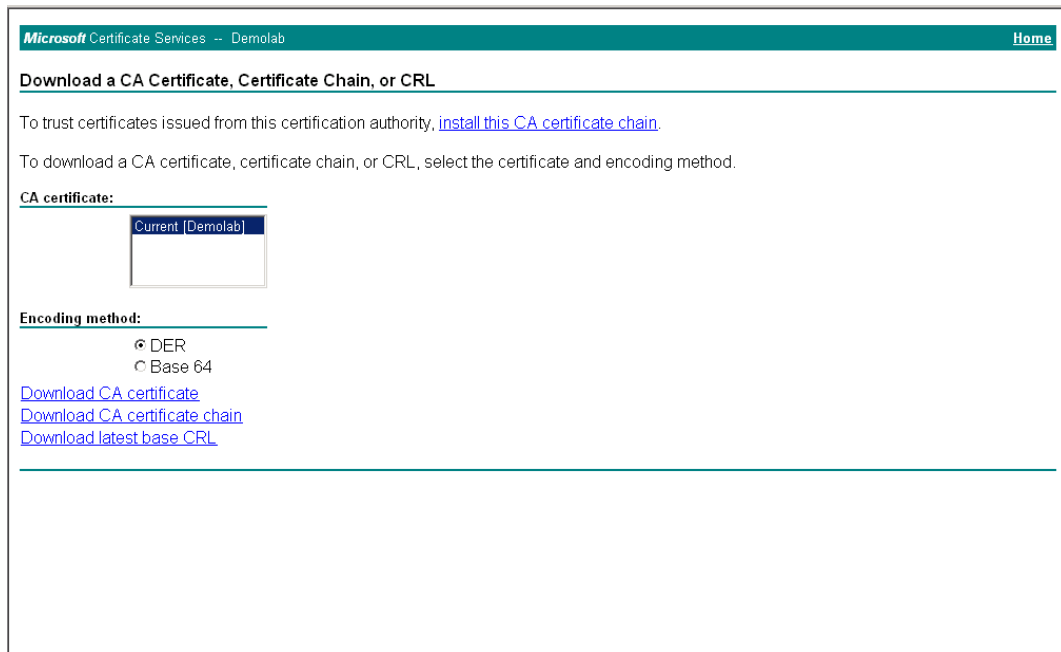


- Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the 'Saved Request' field.
- From the 'Certificate Template' drop-down list, select **Web Server**.
- Click **Submit**.

Figure 4-31: Certificate Issued Page



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

Figure 4-32: Download a CA Certificate, Certificate Chain, or CRL Page


Microsoft Certificate Services -- Demolab Home

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

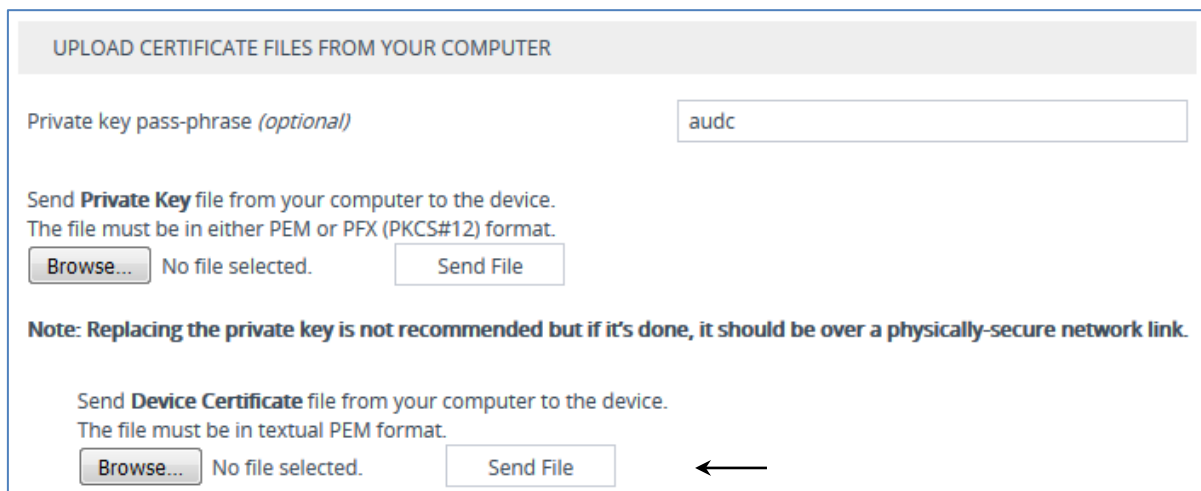
Current [Demolab]

Encoding method:

DER
 Base 64

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

16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file as *certroot.cer* to a folder on your computer.
19. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
 - b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 13, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-33: 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.

No file selected.

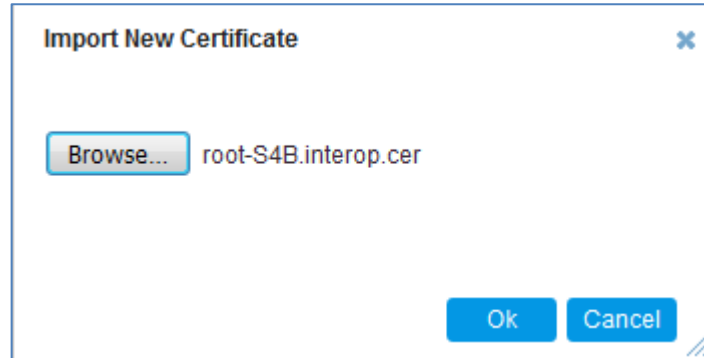
Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

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

No file selected. ←

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

Figure 4-34: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 77).

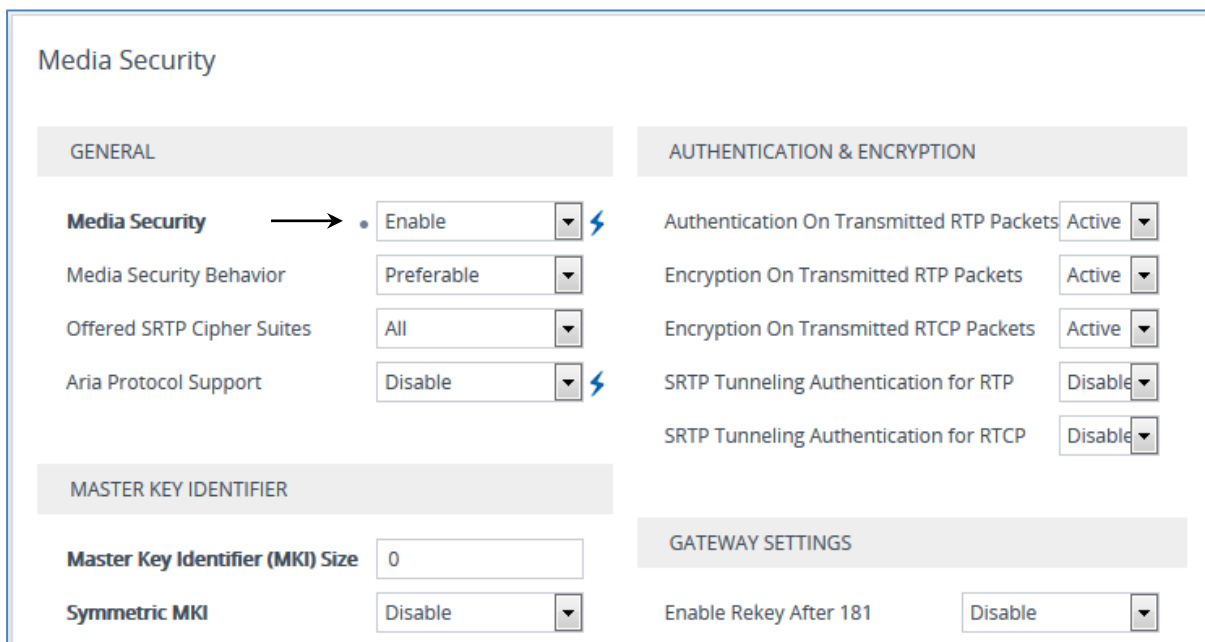
4.10 Step 10: Configure SRTP

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 (**Setup menu > Signaling & Media tab > Media folder > Media Security**).

Figure 4-35: Configuring SRTP



Media Security	
GENERAL	
Media Security	• Enable
Media Security Behavior	Preferable
Offered SRTP Cipher Suites	All
Aria Protocol Support	Disable
MASTER KEY IDENTIFIER	
Master Key Identifier (MKI) Size	0
Symmetric MKI	Disable
AUTHENTICATION & ENCRYPTION	
Authentication On Transmitted RTP Packets	Active
Encryption On Transmitted RTP Packets	Active
Encryption On Transmitted RTCP Packets	Active
SRTP Tunneling Authentication for RTP	Disable
SRTP Tunneling Authentication for RTCP	Disable
GATEWAY SETTINGS	
Enable Rekey After 181	Disable

2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 77).

4.11 Step 11: Configure Maximum IP Media Channels

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



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

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

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

Figure 4-36: Configuring Number of Media Channels

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

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **100**).
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section on page 77).

4.12 Step 12: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.8 on page 55) to denote the source and destination of the call.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business Server 2015 (LAN) and Rogers SIP Trunk (DMZ):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
 - Calls from Skype for Business Server 2015 to Rogers SIP Trunk
 - Calls from Rogers SIP Trunk to Fax supporting ATA device (if required)
 - Calls from Rogers SIP Trunk to Skype for Business Server 2015
 - Calls from Fax supporting ATA device to Rogers SIP Trunk (if required)
- **To configure IP-to-IP routing rules:**
1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
 2. Configure a rule to terminate SIP OPTIONS messages received from the both LAN and DMZ:
 - a. Click **New**, and then configure the parameters as follows:

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

Figure 4-37: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

- b. Click **Apply**.
- 3. Configure rule to route calls from Rogers SIP Trunk to Fax supporting ATA device:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	1
Route Name	ITSP to Fax (arbitrary descriptive name)
Source IP Group	SP
Destination Username Prefix	123456 (dedicated FAX number)
Destination Type	IP Group
Destination IP Group	Fax
Destination SIP Interface	S4B

Figure 4-38: Configuring IP-to-IP Routing Rule for ITSP to Fax

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL

Index: 1

Name: ITSP to Fax

Alternative Route Options: Route Row

MATCH

Source IP Group: #1 [SP] [View](#)

Request Type: All

Source Username Prefix: *

Source Host: *

Source Tags:

Destination Username Prefix: 123456

ACTION

Destination Type: IP Group

Destination IP Group: #2 [Fax] [View](#)

Destination SIP Interface: #0 [S4B] [View](#)

Destination Address:

Destination Port: 0

Destination Transport Type:

Call Setup Rules Set ID: -1

Group Policy: Sequential

Cost Group: -- [View](#)

Cancel **APPLY**

- b. Click **Apply**.

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

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

Figure 4-39: Configuring IP-to-IP Routing Rule for S4B to ITSP

The screenshot shows a configuration window titled "IP-to-IP Routing [S4B to ITSP]". At the top, there is a "Routing Policy" dropdown set to "#0 [Default_SBCRoutingPolicy]". The window is divided into two main sections: "GENERAL" and "ACTION".

GENERAL Section:

- Index: 2
- Name: S4B to ITSP
- Alternative Route Options: Route Row

MATCH Section:

- Source IP Group: #0 [S4B]
- Request Type: All
- Source Username Prefix: *
- Source Host: *
- Source Tags: (empty)

ACTION Section:

- Destination Type: IP Group
- Destination IP Group: #1 [SP]
- Destination SIP Interface: #1 [SP]
- Destination Address: (empty)
- Destination Port: 0
- Destination Transport Type: (empty)
- Call Setup Rules Set ID: -1
- Group Policy: Sequential
- Cost Group: --

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

- b. Click **Apply**.

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

Parameter	Value
Index	3
Route Name	ITSP to S4B (arbitrary descriptive name)
Source IP Group	SP
Destination Type	IP Group
Destination IP Group	S4B
Destination SIP Interface	S4B

Figure 4-40: Configuring IP-to-IP Routing Rule for ITSP to S4B

The screenshot shows a configuration window titled "IP-to-IP Routing [ITSP to S4B]". At the top, the "Routing Policy" is set to "#0 [Default_SBCRoutingPolicy]". The window is divided into three main sections: GENERAL, MATCH, and ACTION.

- GENERAL:**
 - Index: 3
 - Name: ITSP to S4B
 - Alternative Route Options: Route Row
- MATCH:**
 - Source IP Group: #1 [SP] (with a "View" link)
 - Request Type: All
 - Source Username Prefix: *
 - Source Host: *
 - Source Tags: (empty)
- ACTION:**
 - Destination Type: IP Group
 - Destination IP Group: #0 [S4B] (with a "View" link)
 - Destination SIP Interface: #0 [S4B] (with a "View" link)
 - Destination Address: (empty)
 - Destination Port: 0
 - Destination Transport Type: (empty)
 - Call Setup Rules Set ID: -1
 - Group Policy: Sequential
 - Cost Group: -- (with a "View" link)

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

- b. Click **Apply**.

- 6. Configure a rule to route calls from Fax supporting ATA device to Rogers SIP Trunk:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	4
Route Name	Fax to ITSP (arbitrary descriptive name)
Source IP Group	Fax
Destination Type	IP Group
Destination IP Group	SP
Destination SIP Interface	SP

Figure 4-41: Configuring IP-to-IP Routing Rule for Fax to ITSP – Rule tab

- b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 4-42: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (5)

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

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate OP	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	ITSP to Fax	Default_SBCR	Route Row	SP	All	*	123456	IP Group	Fax	S4B	
2	S4B to ITSP	Default_SBCR	Route Row	S4B	All	*	*	IP Group	SP	SP	
3	ITSP to S4B	Default_SBCR	Route Row	SP	All	*	*	IP Group	S4B	S4B	
4	Fax to ITSP	Default_SBCR	Route Row	Fax	All	*	*	IP Group	SP	SP	



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

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.8 on page 55) to denote the source and destination of the call.



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

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

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

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

Parameter	Value
Index	0
Name	Add + toward S4B
Source IP Group	SP
Destination IP Group	S4B
Destination Username Prefix	* (asterisk sign)
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 4-43: Configuring IP-to-IP Outbound Manipulation Rule

3. Click **Apply**.

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

Figure 4-44: Example of Configured IP-to-IP Outbound Manipulation Rules

INDEX	NAME	ROUTING POLICY	ADDITION MANIPUL	SOURCE IP GROUP	DESTINAT IP GROUP	SOURCE USERNAM PREFIX	DESTINAT USERNAM PREFIX	MANIPULATED ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Add + toward S	Default_SE	No	SP	S4B	*	*	Destination URI	0	0	255	+	
1	Remove + from	Default_SE	No	S4B	SP	*	+	Destination URI	1	0	255		
2	Remove + from	Default_SE	No	S4B	SP	+	*	Source URI	1	0	255		

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

4.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

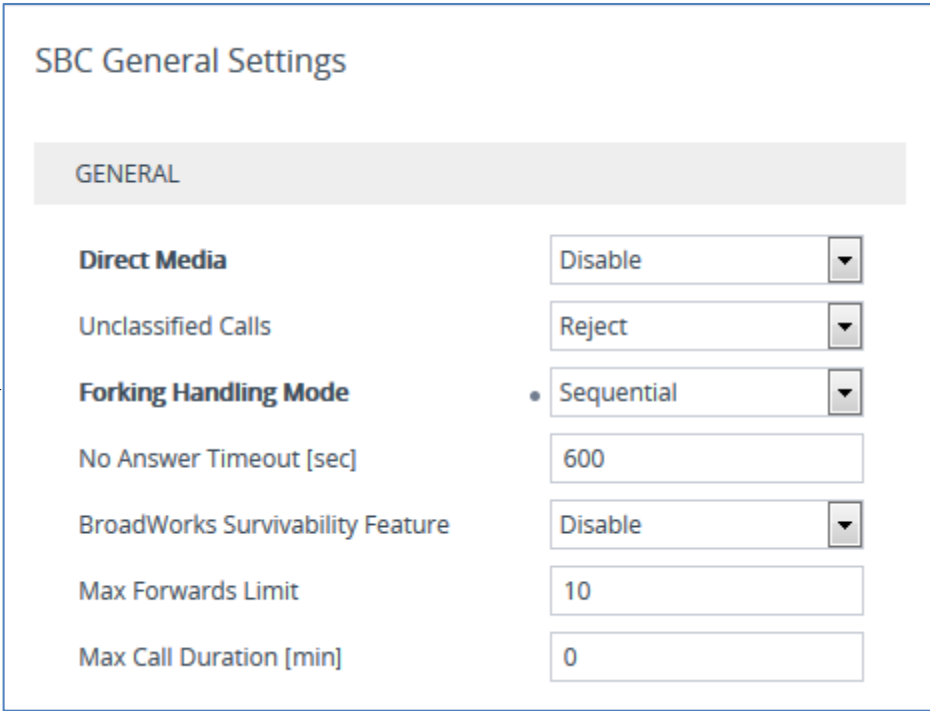
4.14.1 Step 14a: Configure Call Forking Mode

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

➤ **To configure call forking:**

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

Figure 4-45: Configuring Forking Mode



The screenshot shows the 'SBC General Settings' page. The 'GENERAL' tab is selected. The 'Forking Handling Mode' is set to 'Sequential', indicated by a radio button and a dropdown arrow. An arrow points to the 'Forking Handling Mode' label. Other settings include 'Direct Media' (Disable), 'Unclassified Calls' (Reject), 'No Answer Timeout [sec]' (600), 'BroadWorks Survivability Feature' (Disable), 'Max Forwards Limit' (10), and 'Max Call Duration [min]' (0).

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

3. Click **Apply**.

4.14.2 Step 14b: Configure SBC Alternative Routing Reasons

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

➤ **To configure SIP reason codes for alternative IP routing:**

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons**).

2. Click **New**.
3. From the 'Release Cause' drop-down list, select **503 Service Unavailable**.

Figure 4-46: SBC Alternative Routing Reasons Table

The screenshot shows a software dialog box titled "Alternative Routing Reasons". It features a "GENERAL" tab. Under this tab, there are two fields: "Index" which contains the number "0", and "Release Cause" which is a dropdown menu currently displaying "503 Service Unavailable". At the bottom of the dialog, there are two buttons: "Cancel" and "APPLY".

4. Click **Apply**.

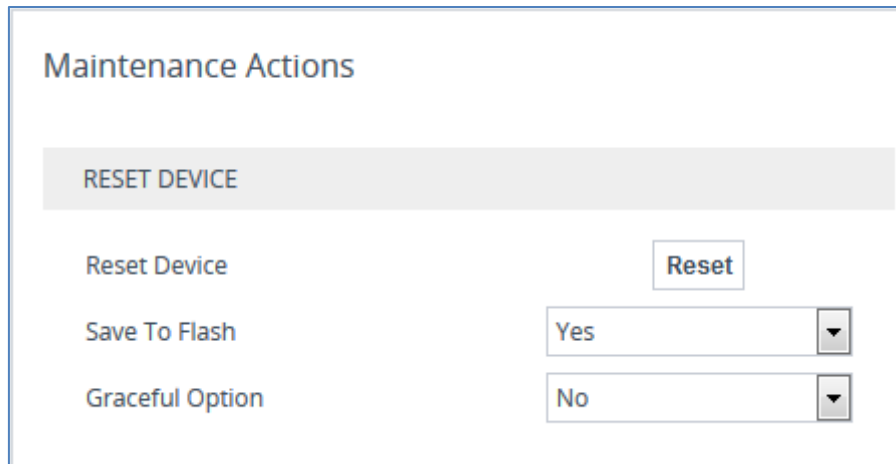
4.15 Step 15: Reset the E-SBC

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

➤ **To reset the device through Web interface:**

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

Figure 4-47: Resetting the E-SBC



The screenshot shows the 'Maintenance Actions' web interface. At the top, there is a header 'Maintenance Actions'. Below it, a grey bar contains the text 'RESET DEVICE'. Underneath, there are three rows of controls: 'Reset Device' with a 'Reset' button to its right; 'Save To Flash' with a dropdown menu showing 'Yes'; and 'Graceful Option' with a dropdown menu showing 'No'.

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

This page is intentionally left blank

A AudioCodes INI File

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



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

```

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

;Board: Mediant 800
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 3522531
;Slot Number: 1
;Software Version: 7.20A.002
;DSP Software Version: 5014AE3_R => 720.25
;Board IP Address: 10.15.70.101
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M  Flash size: 64M  Core speed: 300Mhz
;Num of DSP Cores: 1  Num DSP Channels: 59
;Num of physical LAN ports: 4
;Profile: NONE
;SBC Sessions Capability:;Local License: 68 SBC Sessions (up to 68 if all
legacy telephony interfaces are disabled);Pool License: 0 SBC Sessions
(from License Pool Manager);Total (Actual): 68 SBC Sessions (up to 68 if
all legacy telephony interfaces are disabled);;Key features:;Board Type:
Mediant 800 ;DSP Voice features: RTCP-XR ;Channel Type: RTP DspCh=60
IPMediaDspCh=60 ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;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 ;PSTN FALLBACK
Supported ;DATA features: ;QOE features: VoiceQualityMonitoring
;ElTrunks=2 ;FXSPorts=8 ;FXOPorts=8 ;IP Media: Conf ;Control Protocols:
TDMtoSBC MGCP SIP SBC=60 MSFT FEU=100 TestCall=1000 WebRTC ;Default
features:;Coders: G711 G726;

;----- HW components-----
;
; Slot # : Module type : # of ports
;-----
;      1 : FXO           : 4
;      2 : FXO           : 4
;      3 : Empty
;-----

[SYSTEM Params]

SyslogServerIP = 10.15.70.2
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value

```

```
NTPServerUTCOffset = 7200
DebugRecordingDestIP = 10.15.70.2
;VpFileLastUpdateTime is hidden but has non-default value
TLSPkeySize = 2048
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
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

LogoWidth = '145'

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
```



```

ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESEXMODE = 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_2",
"Active";
PhysicalPortsTable 2 = "GE_4_3", 0, 4, "User Port #2", "None", " ";
PhysicalPortsTable 3 = "GE_4_4", 0, 4, "User Port #3", "None", " ";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

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

[ \EtherGroupTable ]

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \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, 10.15.70.101, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.153, 25, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

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

[ \DspTemplates ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$0+qysO+zue3t67q+5u3ZgtvQ3d3Rg9CI097diNeOksfBkZbBlJHPy57JzZ+fzzkzOzI8M
DU0PTxumjlrNzsmdyQ=", 1, 0, 5, 30, 60, 200,
"f92053631e3f2e8796ae95f2322f1a63";
WebUsers 1 = "User",
"$1$lqHyqfqqo6+trqmQk5qVlpfElJyampubm8uWiIGF0tXWh9PajInZj4mKjKai8KCl/KL/r
PH+qf39//7n5+bm5uI=", 3, 0, 2, 15, 60, 50,
"a59ad6ef34de1997cbca580a804adde8";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "TLSContexts_0", 7, 0, "RC4:AES128", "ALL:!aNULL", 0, 0,
0.0.0.0, 0.0.0.0, 2560, 0, 1024;

[ \TLSContexts ]
    
```

```
[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 1 = "AudioCodersGroups_1";

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]

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

[ \AllowedAudioCodersGroups ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_CNGmode,
IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia,
IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller,
IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour,
IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupName,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_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_SBCAdaptRFC2833BWTtoVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCFaxReroutingMode,
IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP,
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW;
IpProfile 1 = "S4B", 1, "", 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "", "", "", 0, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 1, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0,
0, 0, 0, 0, 0, 0;
IpProfile 2 = "Rogers", 1, "", 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "", "Rogers Allowed
Coders", "", 0, 2, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0,
2, 2, 1, 3, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 5,
0, 0, 0, 0, 0, 1, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1,
-1, -1, 0, "", 0, 0, 0, 0, 0, 0;
IpProfile 3 = "Fax", 1, "", 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "", "", "", 0, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, "", 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, 0, 0,
0, 0, 0, 0, 0, 0;

[ \IpProfile ]

[ CpMediaRealm ]

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

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]

[ SRD ]
    
```

```

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

[ \SRD ]

[ MessagePolicy ]

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

[ \MessagePolicy ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPSPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation;
SIPInterface 0 = "S4B", "LAN_IF", 2, 5060, 0, 5067, "DefaultSRD", "",
"TLSContexts_0", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0, 0;
SIPInterface 1 = "Rogers", "WAN_IF", 2, 5060, 0, 0, "DefaultSRD", "",
"TLSContexts_0", -1, 0, 500, -1, 0, "MRwan", 0, -1, -1, -1, 0, 1;

[ \SIPInterface ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "", 1, -1, "", "",
"S4B", "", "", 1, 1, 10, -1;
ProxySet 1 = "Rogers", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"Rogers", "", "", 1, 1, 10, -1;

```

```

ProxySet 2 = "Fax", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"S4B", "", "", 1, 1, 10, -1;

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId;
IPGroup 0 = 0, "Default_IPG", "S4B", "", "", -1, 0, "DefaultSRD", "", 0,
"", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0, "",
"", 0, 0, "TLSContexts_0", 0, 0, -1, 0, 0, 0, "", -1;
IPGroup 1 = 0, "S4B", "S4B", "", "", -1, 0, "DefaultSRD", "MRLan", 1,
"S4B", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "Admin", "$1$aCkNBwIC", 0,
"", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, 0, "", -1;
IPGroup 2 = 0, "Rogers", "Rogers", "173.46.31.194", "", -1, 0,
"DefaultSRD", "MRWan", 1, "Rogers", -1, -1, -1, 0, 0, "", 0, -1, -1, "",
"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "TLSContexts_0", 0,
0, -1, 0, 0, 1, "", -1;
IPGroup 3 = 0, "Fax", "Fax", "", "", -1, 0, "DefaultSRD", "MRLan", 1,
"Fax", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "Admin", "$1$aCkNBwIC", 0,
"", "", 0, "", "", 0, 0, "TLSContexts_0", 0, 0, -1, 0, 0, 0, "", -1;

[ \IPGroup ]

[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "FE.S4B.interop:5067", 2;
ProxyIp 1 = "1", 0, "173.46.31.194:5060", 0;
ProxyIp 2 = "2", 0, "10.15.40.29:5060", 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_IPGroupSetName;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "S4B",
"**, **", "**", "**", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "", "";
IP2IPRouting 1 = "Fax to Rogers", "Default_SBCRoutingPolicy", "Fax",
"99+14033060094", "**", "**", "**", 0, "", "Any", 0, -1, 0, "Rogers",
"Rogers", "", 0, -1, 0, 0, "", "", "", "";
IP2IPRouting 2 = "Rogers to Fax", "Default_SBCRoutingPolicy", "Rogers",
"**, **", "99+14033060094", "**", 0, "", "Any", 0, -1, 0, "Fax", "S4B",
"", 0, -1, 0, 0, "", "", "", "";
IP2IPRouting 3 = "S4B to Rogers", "Default_SBCRoutingPolicy", "S4B", "**",
"**, **", "**", 0, "", "Any", 0, -1, 0, "Rogers", "Rogers", "", 0, -1, 0,
0, "", "", "", "";
IP2IPRouting 4 = "Rogers to S4B", "Default_SBCRoutingPolicy", "Rogers",
"**, **", "**", "**", 0, "", "Any", 0, -1, 0, "S4B", "S4B", "", 0, -1, 0,
0, "", "", "", "";

[ \IP2IPRouting ]

[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index =
IPInboundManipulation_ManipulationName,
IPInboundManipulation_RoutingPolicyName,
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose,
IPInboundManipulation_SrcIPGroupName,
IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost,
IPInboundManipulation_RequestType, IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft,
IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 1 = "", "Default_SBCRoutingPolicy", 0, 0, "Rogers",
"xxxxxxxxx#", "**", "**", "**", 0, 0, 0, 0, 255, "+1", "";
IPInboundManipulation 2 = "", "Default_SBCRoutingPolicy", 0, 0, "Rogers",
"[0-9]", "**", "**", "**", 0, 0, 0, 0, 255, "+", "";

[ \IPInboundManipulation ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,

```

```

IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "Add + toward S4B",
"Default_SBCRoutingPolicy", 0, "Rogers", "S4B", "*", "*", "*", "*", "*",
", 0, "Any", 0, 1, 0, 0, 255, "+1", "", 0, "", "";
IPOutboundManipulation 3 = "", "Default_SBCRoutingPolicy", 0, "S4B",
"Any", "*", "*", "+972", "*", "*", "", 0, "Any", 0, 1, 1, 0, 255, "011",
", 0, "", "";
IPOutboundManipulation 4 = "", "Default_SBCRoutingPolicy", 0, "S4B",
"Rogers", "*", "*", "1800", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255, "",
", 0, "", "";
IPOutboundManipulation 5 = "Remove + Dst", "Default_SBCRoutingPolicy", 0,
"S4B", "Rogers", "*", "*", "*", "*", "*", "", 0, "Any", 0, 1, 2, 0, 255,
", "", 0, "", "";
IPOutboundManipulation 6 = "Remove +1", "Default_SBCRoutingPolicy", 0,
"S4B", "Rogers", "*", "*", "*", "*", "*", "*", "", 0, "Any", 0, 0, 2, 0, 255,
", "", 0, "", "";

[ \IPOutboundManipulation ]

[ IDSRule ]

FORMAT IDSRule_Index = IDSRule_Policy, IDSRule_RuleID, IDSRule_Reason,
IDSRule_ThresholdScope, IDSRule_ThresholdWindow,
IDSRule_MinorAlarmThreshold, IDSRule_MajorAlarmThreshold,
IDSRule_CriticalAlarmThreshold, IDSRule_DenyThreshold,
IDSRule_DenyPeriod;
IDSRule 10 = "", 0, 1, 0, 3, 15, -1, -1, -1, -1;
IDSRule 11 = "", 1, 2, 0, 3, 50, -1, -1, -1, -1;
IDSRule 12 = "", 2, 3, 0, 5, 30, -1, -1, -1, -1;
IDSRule 13 = "", 3, 4, 0, 3, 50, -1, -1, -1, -1;
IDSRule 14 = "", 4, 5, 0, 3, 50, -1, -1, -1, -1;

[ \IDSRule ]

[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]
    
```



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

[ \ResourcePriorityNetworkDomains ]

[ MaliciousSignatureDB ]

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smapi", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 0 = "Rogers Allowed Coders", 0, 2, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]
```

```
FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,  
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,  
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,  
AudioCoders_CoderSpecific;  
AudioCoders 0 = "AudioCodersGroups_1", 0, 2, 2, 90, -1, 1, "";  
AudioCoders 1 = "AudioCodersGroups_1", 1, 1, 2, 90, -1, 1, "";  
\AudioCoders]
```

B Configuring Analog Devices (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.

B.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 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:**
- 1. 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 B-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				

B.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:**

1. 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 B-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	0	None
2						Not Configured	-1		None

B.3 Step 3: Configure Coders Table

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

➤ **To configure MP-11x coders:**

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

Figure B-3: Coders Table Page

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

B.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 B-4: SIP General Parameters Page

SIP General Parameters	
Basic Parameter List ▲	
▼ SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported ▼
Channel Select Mode	By Dest Phone Number ▼
Enable Early Media	Disable ▼
183 Message Behavior	Progress ▼
Session-Expires Time	0
Minimum Session-Expires	90
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	5060
SIP TLS Local Port	5061
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.

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

Contact us: www.audiocodes.com/contact

Website: www.audiocodes.com

©2017 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM, AudioCodes One Voice 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-39135

