

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

Version 6.8



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 MSBR E-SBC Version.....	9
2.2	Telecom Liechtenstein SIP Trunking Version	9
2.3	Microsoft Skype for Business Server 2015 Version	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring Skype for Business Server 2015.....	13
3.1	Configuring the E-SBC as an IP / PSTN Gateway	13
3.2	Configuring the "Route" on Skype for Business Server 2015.....	21
4	Configuring AudioCodes E-SBC.....	31
4.1	Step 1: IP Network Interfaces Configuration	32
4.1.1	Step 1a: Configure Network Interface	33
4.2	Step 2: Enable the SBC Application	34
4.3	Step 3: Signaling Routing Domains Configuration	35
4.3.1	Step 3a: Configure Media Realms.....	35
4.3.2	Step 3b: Configure SRDs	37
4.3.3	Step 3c: Configure SIP Signaling Interfaces	38
4.4	Step 4: Configure Proxy Sets	41
4.5	Step 5: Configure IP Groups.....	44
4.6	Step 6: Configure IP Profiles	46
4.7	Step 7: Configure Coders	53
4.8	Step 8: SIP TLS Connection Configuration	54
4.8.1	Step 8a: Configure the NTP Server Address.....	54
4.8.2	Step 8b: Configure the TLS version	54
4.8.3	Step 8c: Configure a Certificate for Operation with Microsoft Skype for Business Server 2015	56
4.8.4	Step 8d: Configure a Certificate for work with Telecom Liechtenstein SIP Trunk.....	61
4.9	Step 9: Configure SRTP	62
4.10	Step 10: Configure IP-to-IP Call Routing Rules	63
4.11	Step 11: Configure IP-to-IP Manipulation Rules.....	69
4.12	Step 12: Configure Message Manipulation Rules	71
4.13	Step 13: Configure Registration Accounts	76
4.14	Step 14: Miscellaneous Configuration.....	77
4.14.1	Step 14a: Configure Call Forking Mode	77
4.14.2	Step 14b: Loading Prerecorded Tones File.....	78
4.14.3	Step 14c: Configure RTP Port for T.38 Fax.....	79
4.15	Step 15: Reset the E-SBC	80
A	AudioCodes INI File	81
B	AudioCodes CLI Script File	89

This page is intentionally left blank.

Notice

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

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

© Copyright 2016 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: June-26-2016

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
13040	Initial document release for Version 6.8.

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 Telecom Liechtenstein'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 Telecom Liechtenstein Partners who are responsible for installing and configuring Telecom Liechtenstein'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 MSBR E-SBC Version

Table 2-1: AudioCodes MSBR E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500L MSBR & E-SBC ▪ Mediant 500 MSBR & E-SBC ▪ Mediant 800 MSBR & E-SBC
Software Version	SIP_6.80A.308.003
Protocol	▪ SIP/UDP or SIP/TCP or SIP/TLS (to the Telecom Liechtenstein SIP Trunk) ▪ SIP/TCP or TLS (to the S4B FE Server)
Additional Notes	None

2.2 Telecom Liechtenstein SIP Trunking Version

Table 2-2: Telecom Liechtenstein Version

Vendor/Service Provider	Teles
SSW Model/Service	C5-Proxy
Software Version	5.08.33
Protocol	SIP
Additional Notes	None

2.3 Microsoft Skype for Business Server 2015 Version

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

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

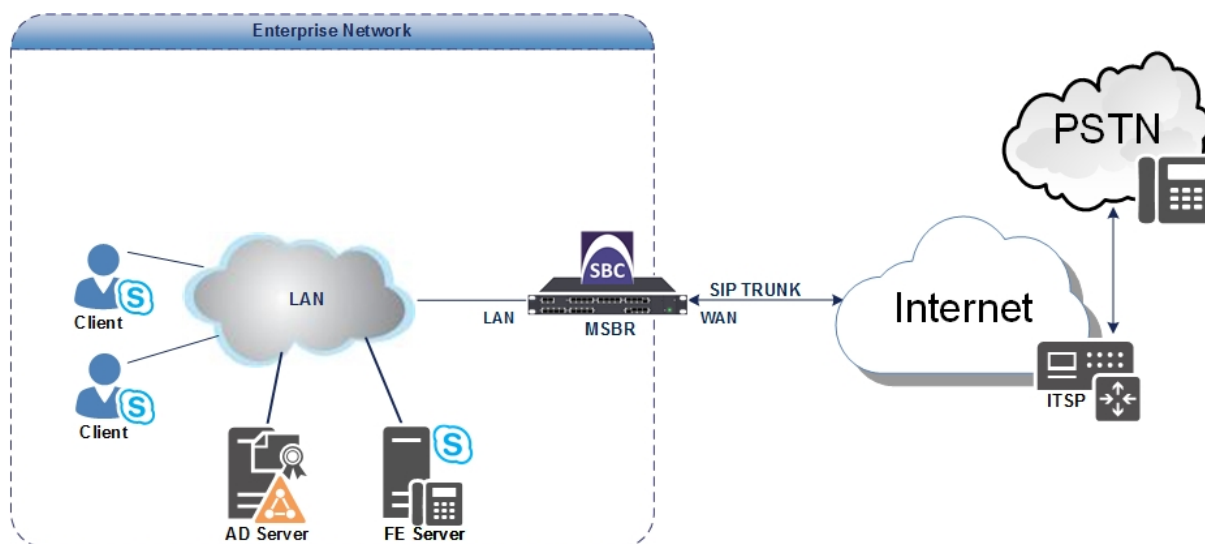
2.4 Interoperability Test Topology

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



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	- Microsoft Skype for Business Server 2015 environment is located on the Enterprise's LAN - Telecom Liechtenstein SIP Trunk is located on the WAN
Signaling Transcoding	- Microsoft Skype for Business Server 2015 can operates with SIP-over-TCP or SIP-over-TLS transport types - Telecom Liechtenstein SIP Trunk can operates with SIP-over-UDP or SIP-over-TCP or SIP-over-TLS transport types
Codecs Transcoding	- Microsoft Skype for Business Server 2015 support G.711A-law and G.711U-law coders - Telecom Liechtenstein SIP Trunk support G.711A-law, G.711U-law and G.729 coders
Media Transcoding	Both, Microsoft Skype for Business Server 2015 and Telecom Liechtenstein SIP Trunk can operates with RTP or SRTP media types

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 Telecom Liechtenstein 's SIP Trunk:

- In Call Forwarding scenarios, when a Skype for Business user forwards a call to a PSTN user, RTP packets need to be sent to open a pinhole in the firewall. To overcome this problem with the first incoming RTP packet in this scenario, instead of generating Ringback Tone as Call Progress Tone (CPT), which requires DSP we decided to use a Prerecorded Tones (PRT) file for ringback tones.

This page is intentionally left blank.

3 Configuring Skype for Business Server 2015

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



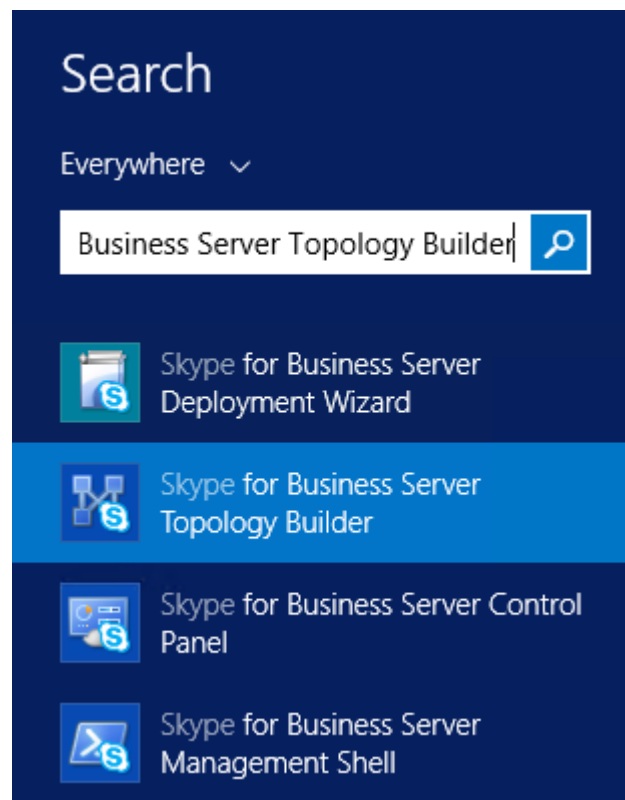
Note: Dial plans, voice policies, and PSTN usages are also necessary for Enterprise voice deployment; however, they are beyond the scope of this document.

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

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

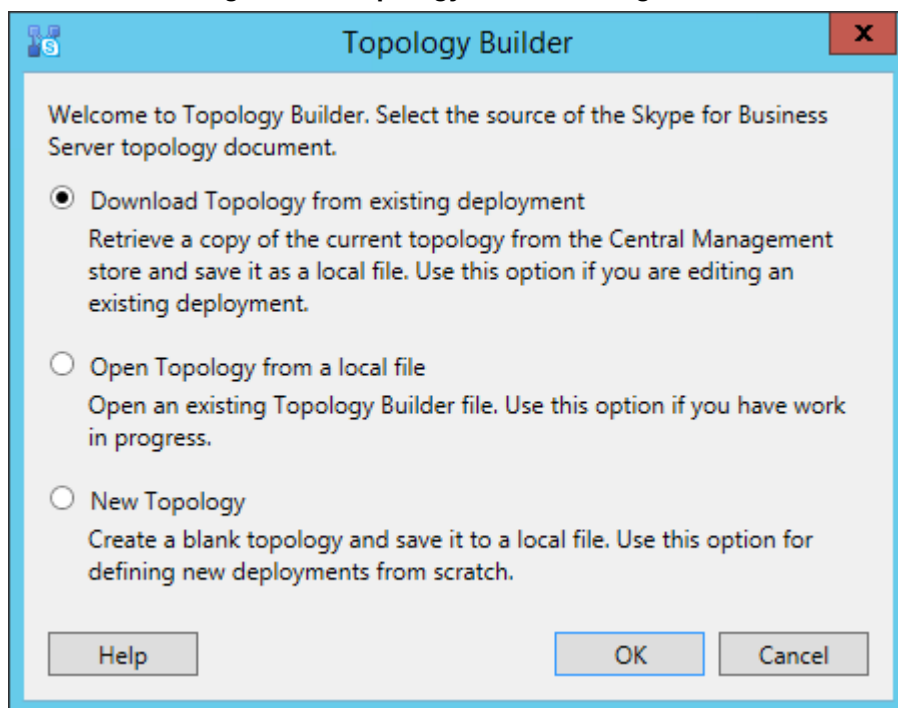
- **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**
- 1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

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



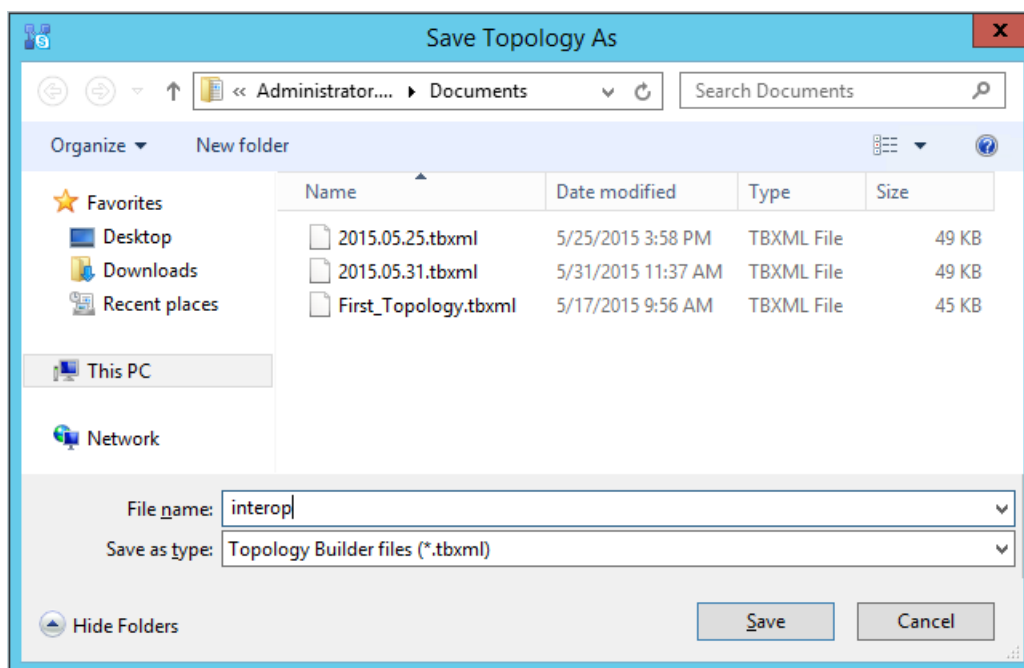
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

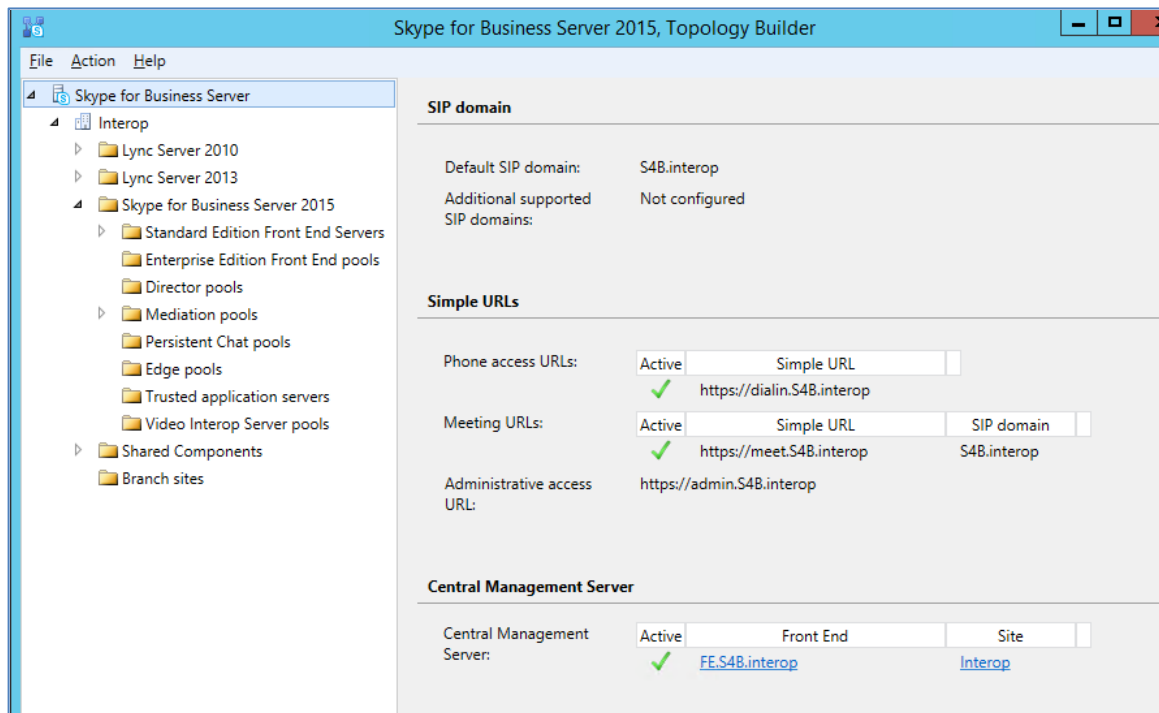
Figure 3-3: Save Topology Dialog Box



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

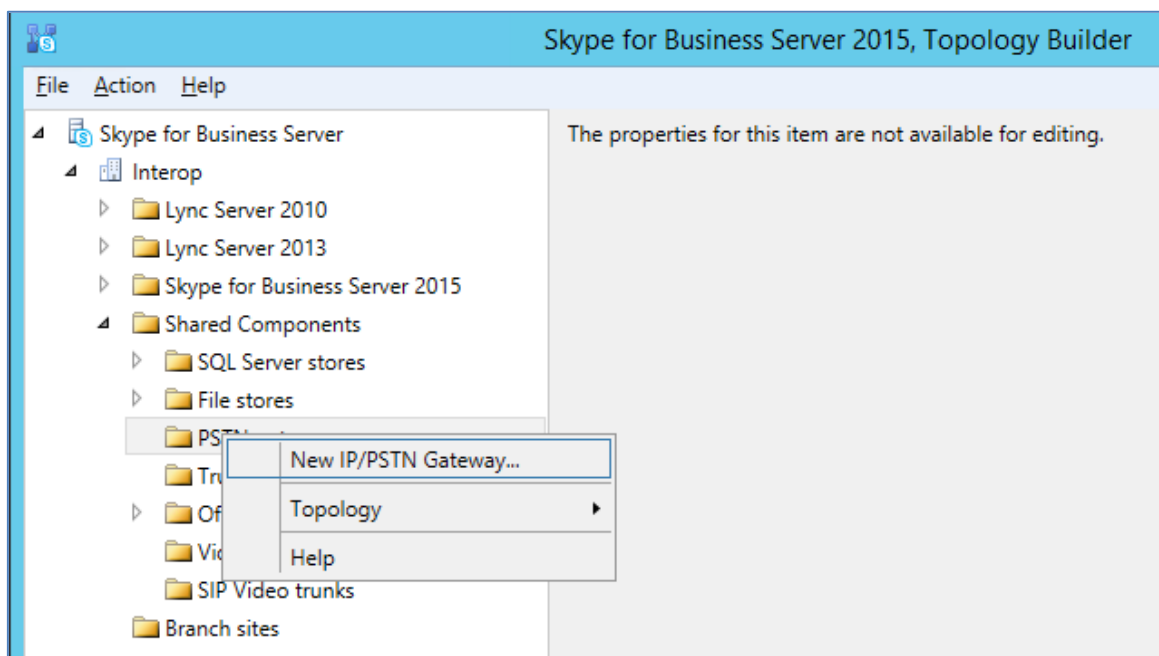
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



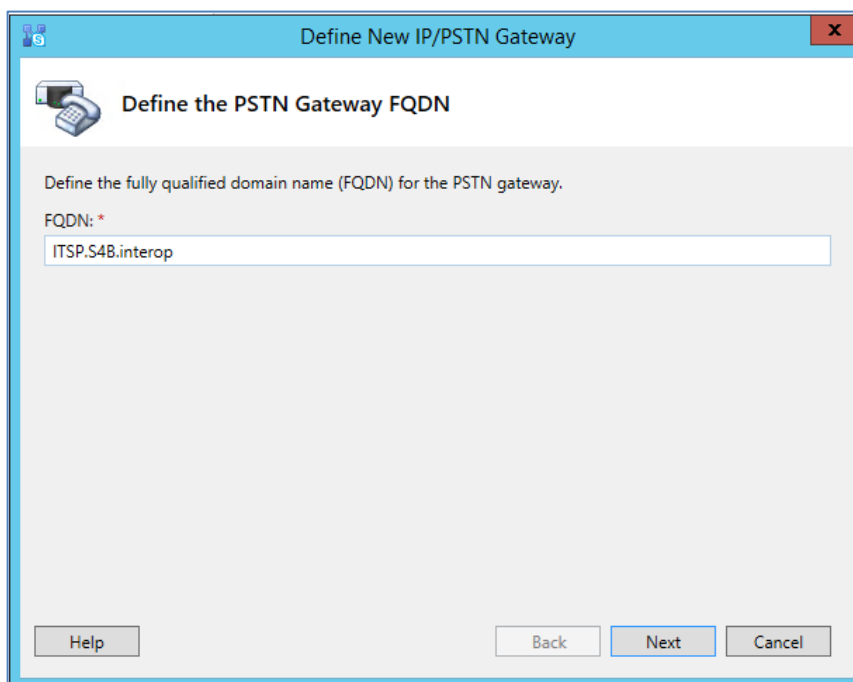
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

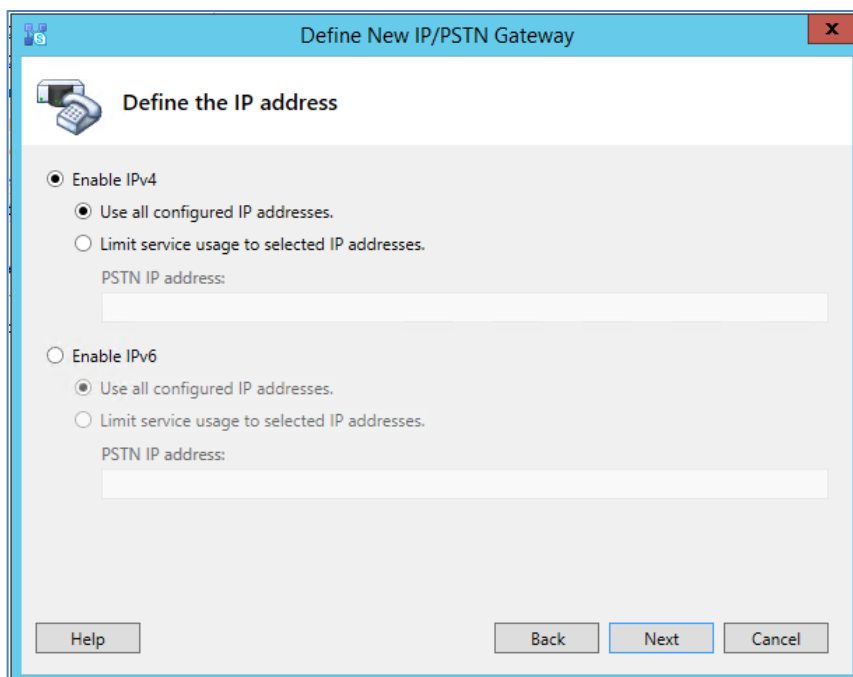
Figure 3-6: Define the PSTN Gateway FQDN



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

5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP.S4B.interop**). This FQDN should be equivalent to the configured Subject Name (CN) in the TLS Certificate Context (see Section 4.8.3 on page 56).
6. Click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



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

7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

8. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server FQDN, Mediation Server listening port (TLS or TCP), gateway IP and FQDN, and gateway listening port.

**Notes:**

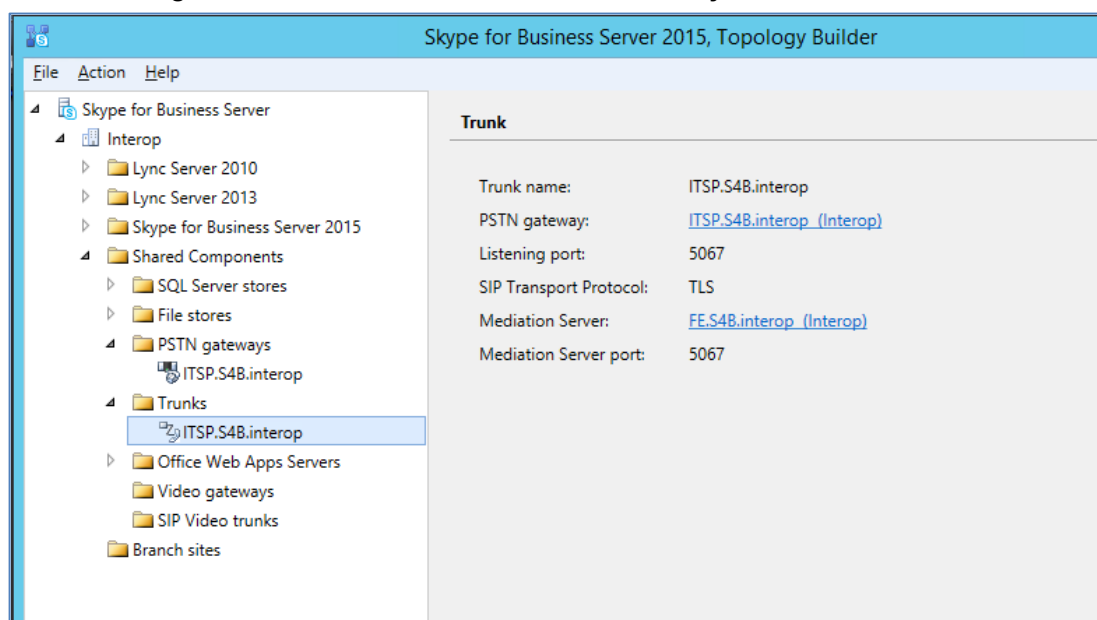
- When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
- The root trunk cannot be removed until the associated PSTN gateway is removed.

Figure 3-8: Define the Root Trunk

- 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**).
- In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses.
- In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
- In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
- Click **Finish**.

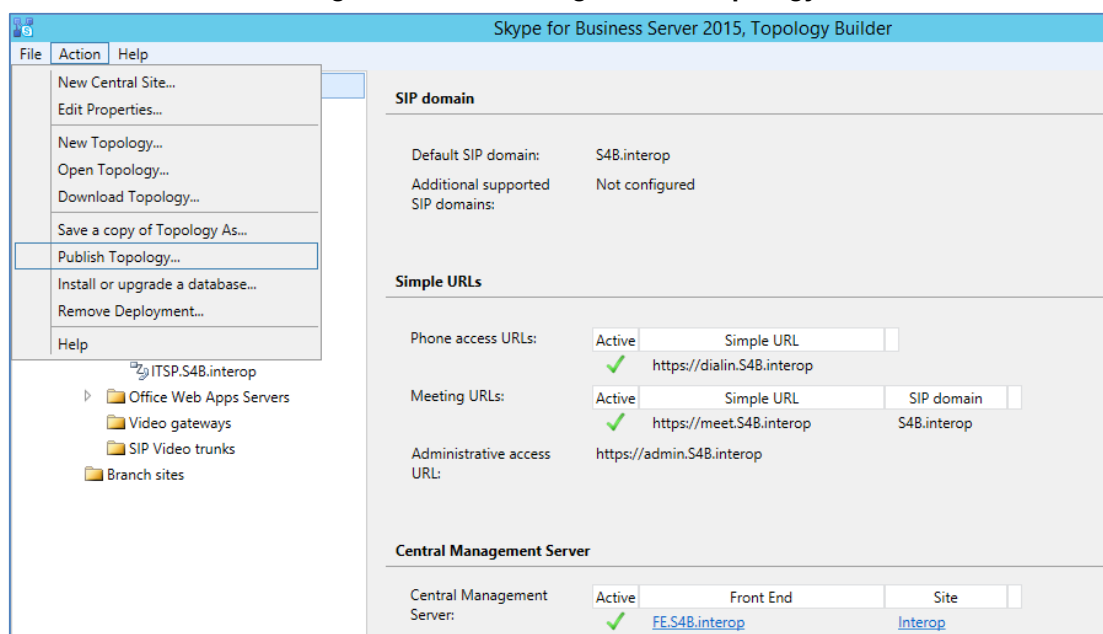
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



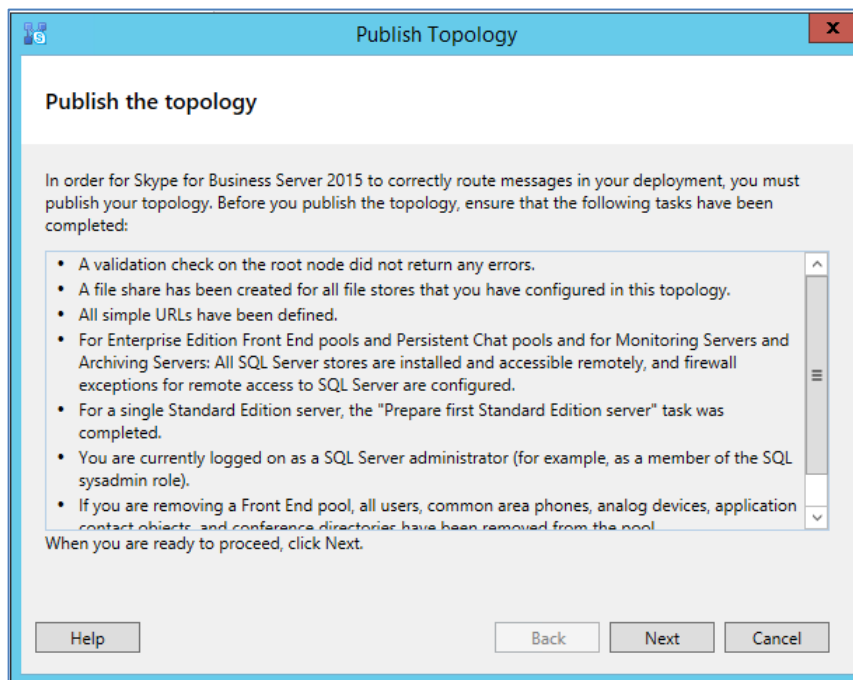
- Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



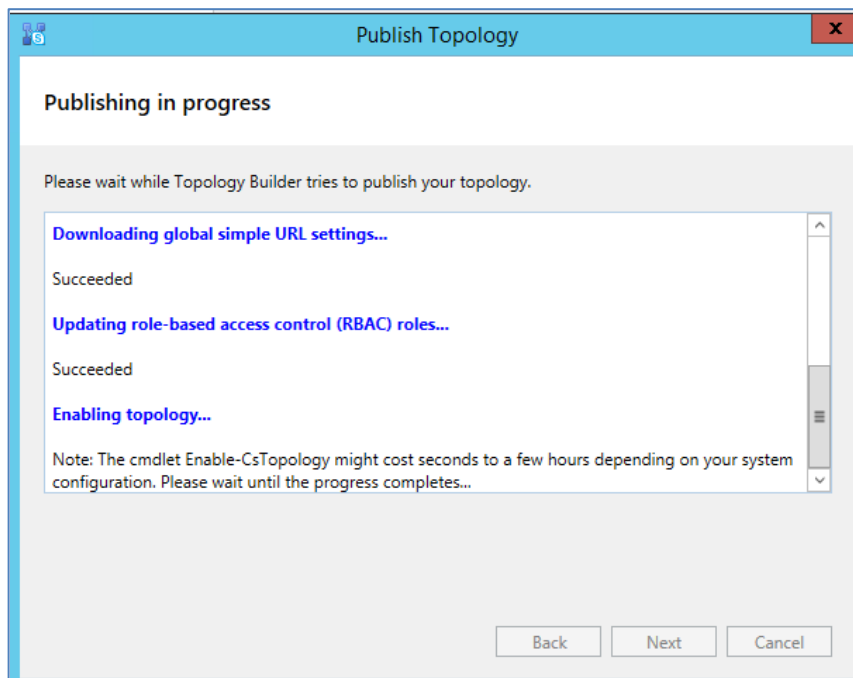
The following is displayed:

Figure 3-11: Publish the Topology



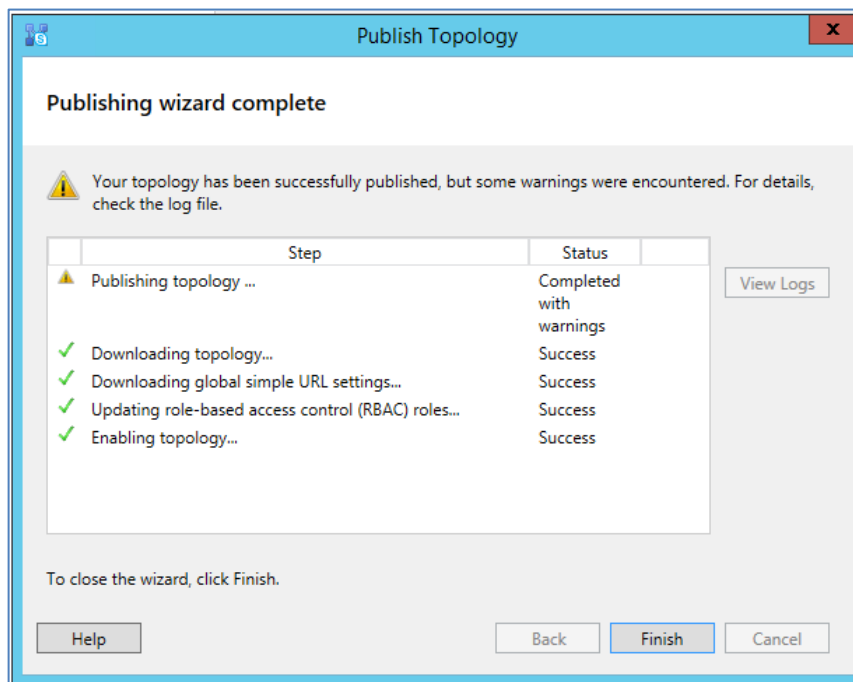
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



12. Click **Finish**.

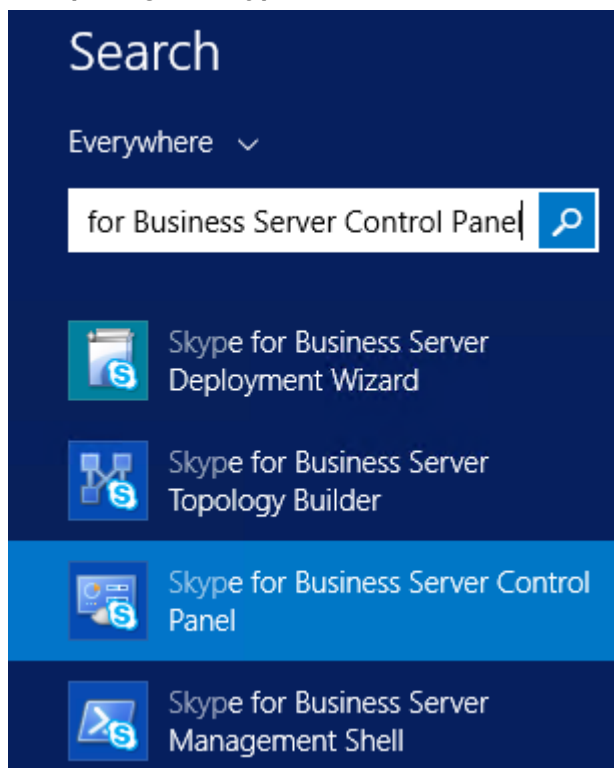
3.2 Configuring the "Route" on Skype for Business Server 2015

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

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

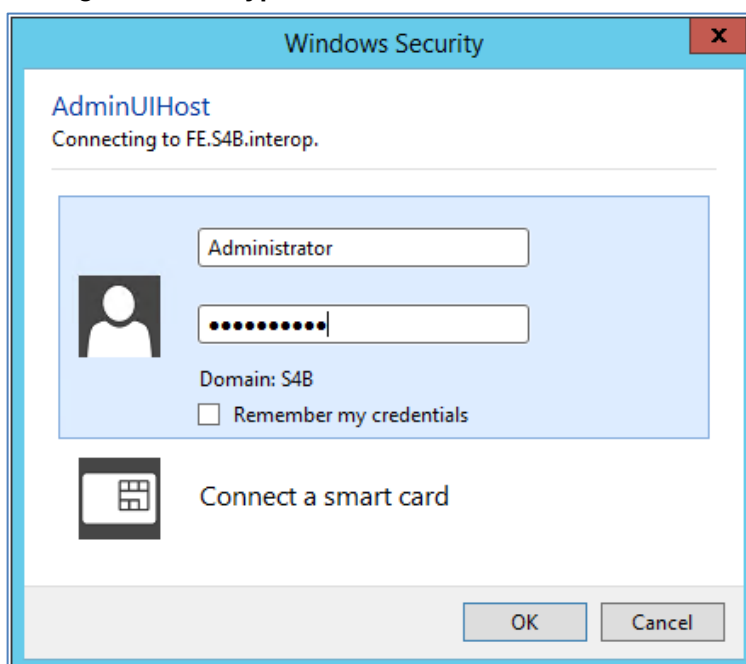
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

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



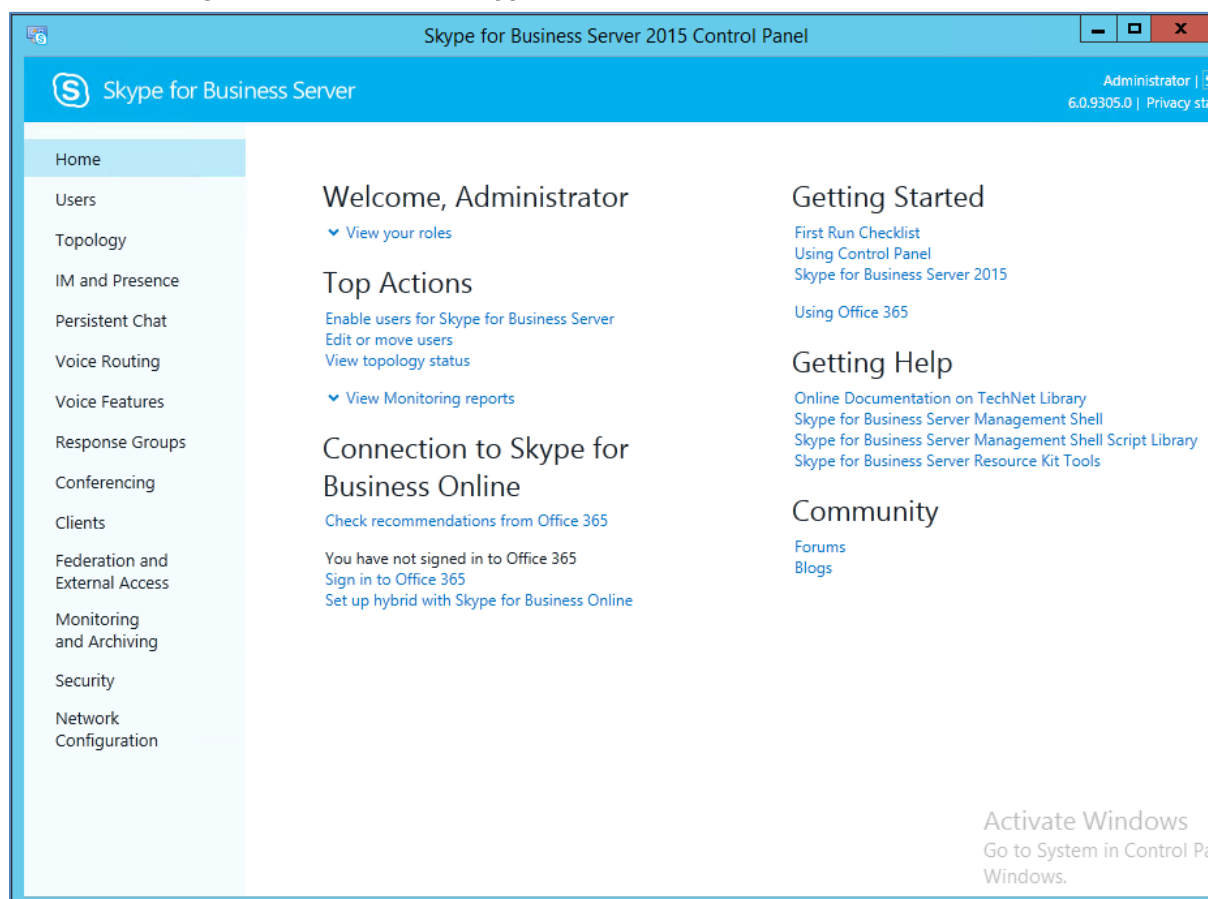
2. You are prompted to enter your login credentials.

Figure 3-15: Skype for Business Server Credentials



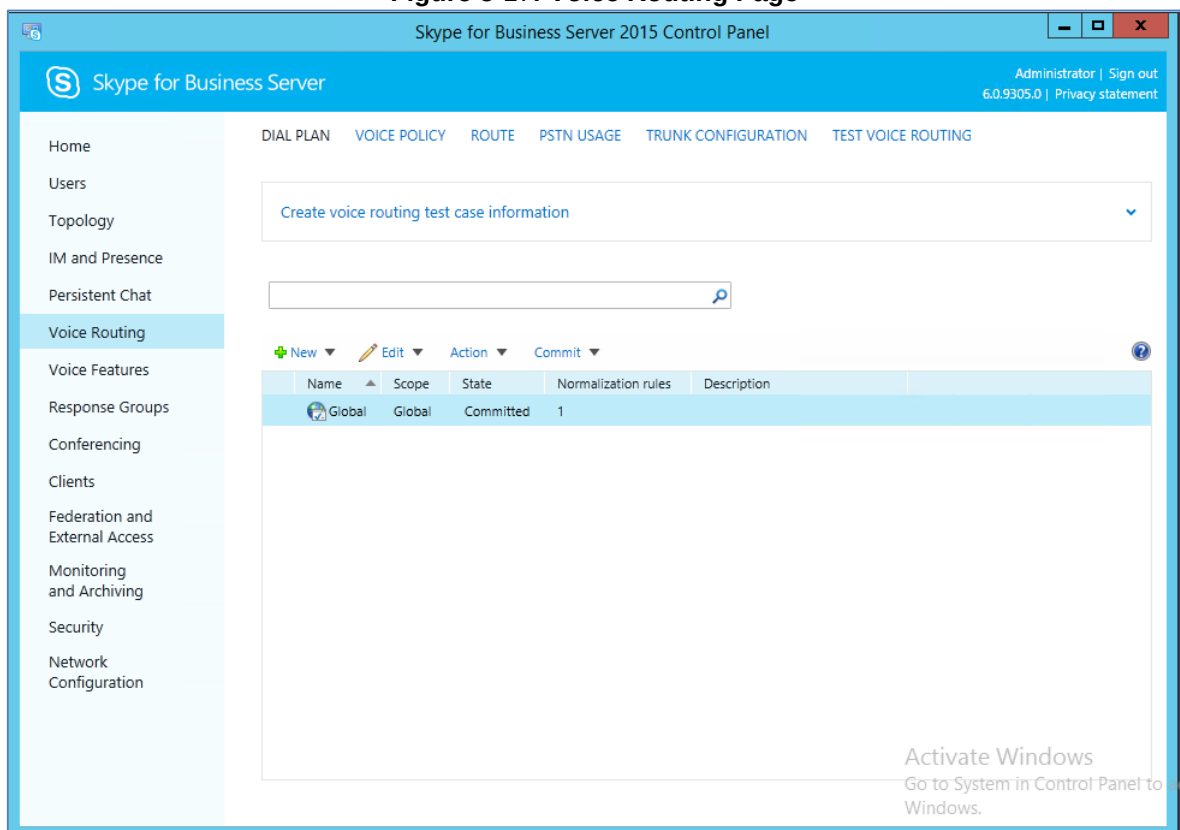
3. Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed.

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



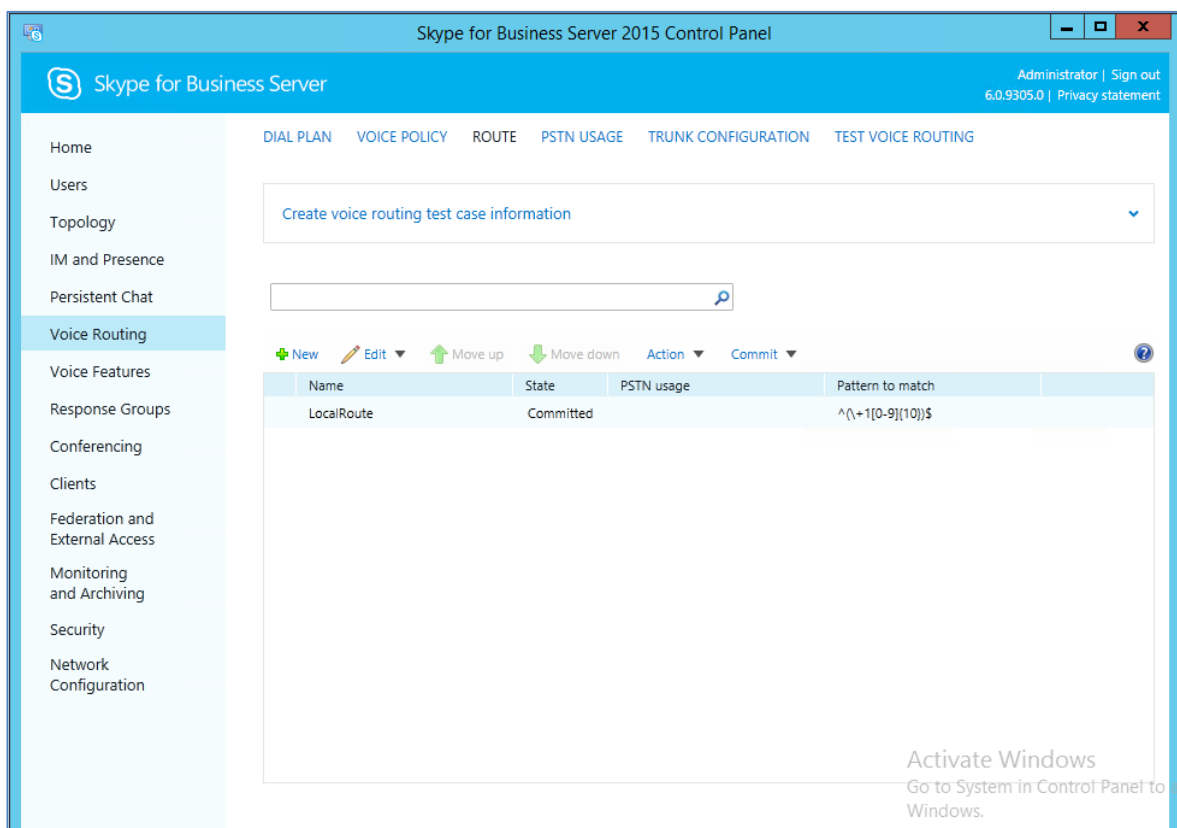
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



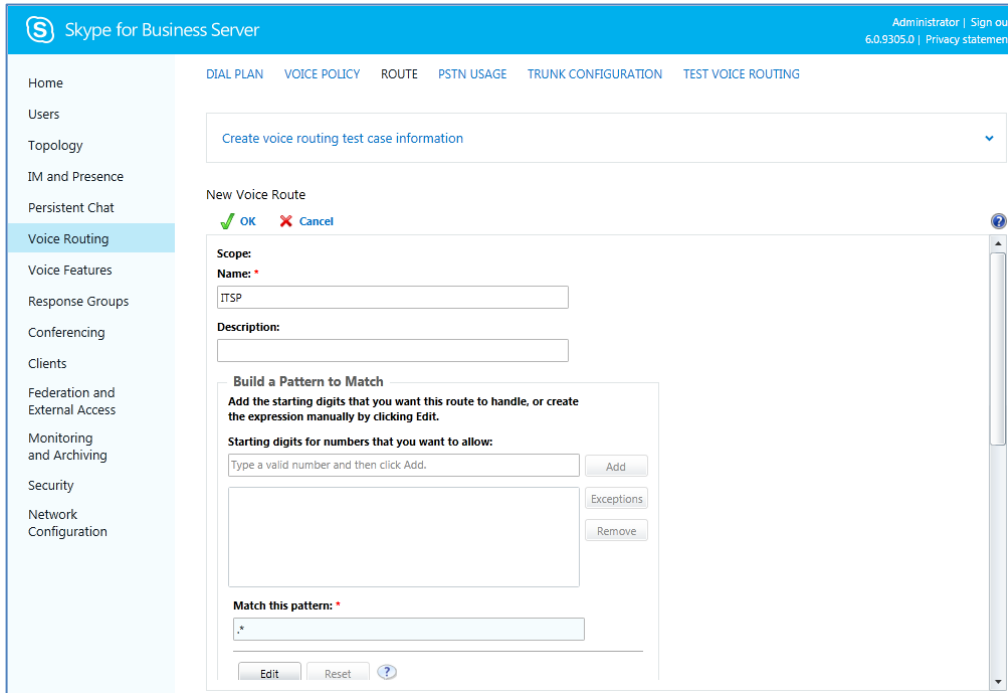
5. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



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

Figure 3-19: Adding New Voice Route



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

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

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

Create voice routing test case information

New Voice Route

OK Cancel

Scope:

Name: * ITSP

Description:

Build a Pattern to Match

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

Starting digits for numbers that you want to allow:

Type a valid number and then click Add.

Add

Exceptions

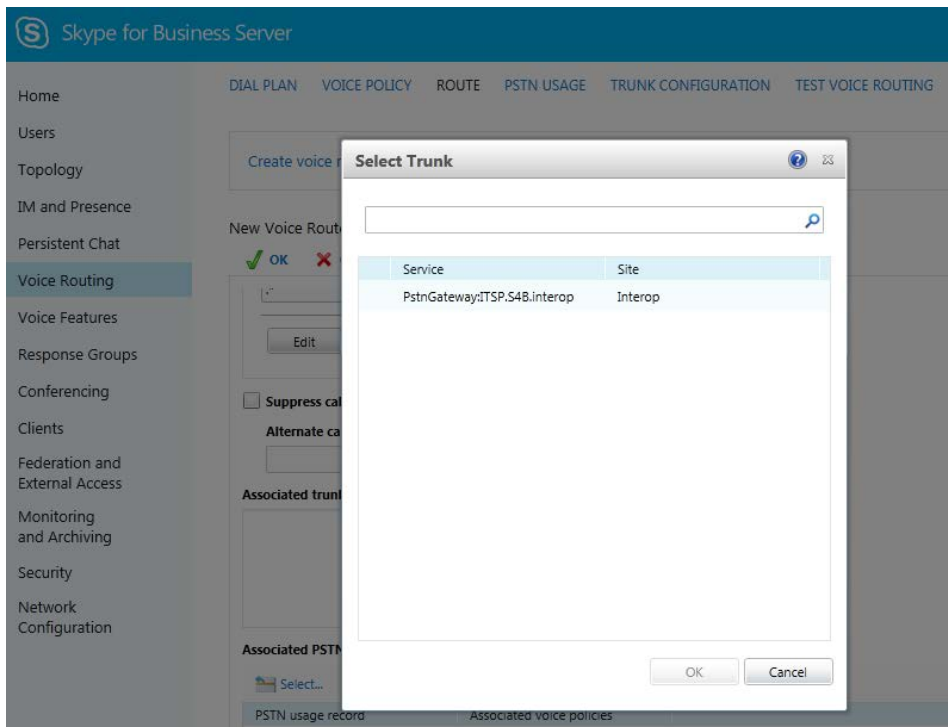
Remove

Match this pattern: *

Edit Reset ?

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

Figure 3-20: List of Deployed Trunks



Skype for Business Server

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

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

Create voice routing test case information

New Voice Route

OK Cancel

.*

Edit

Suppress call transfer

Alternate call transfer

Associated trunk

Associated PSTN

Select...

PSTN usage record

Associated voice policies

Select Trunk

Service	Site
PstnGateway:ITSP.S4B.interop	Interop

OK Cancel

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

Figure 3-21: Selected E-SBC Trunk

Skype for Business Server

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

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

Create voice routing test case information

New Voice Route

OK Cancel

Match this pattern: *

Edit Reset ?

☐ Suppress caller ID

Alternate caller ID:

Associated trunks:

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

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

Figure 3-22: Associating PSTN Usage to Route

Skype for Business Server

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

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

Create voice routing test case information

New Voice Route

OK Cancel

Associated trunks:

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

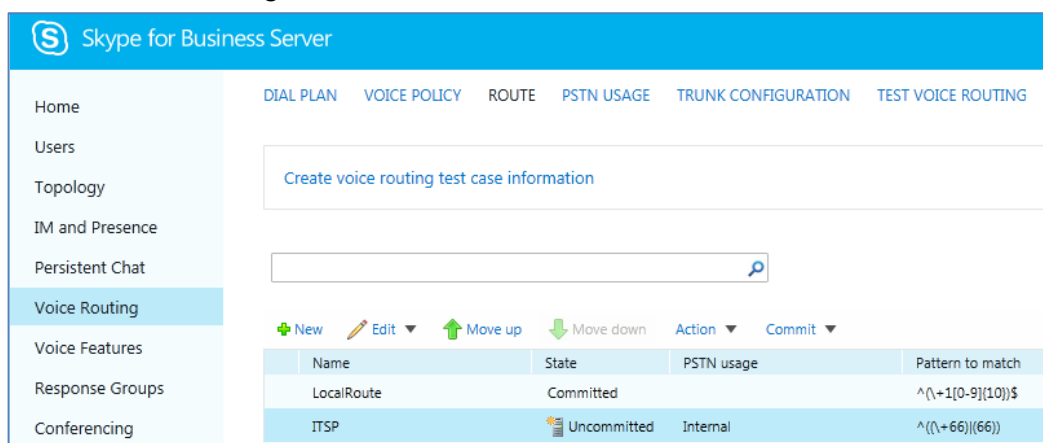
Associated PSTN Usages

Select... Remove ↑ ↓

PSTN usage record	Associated voice policies
Internal	
Local	
Long Distance	

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

Figure 3-23: Confirmation of New Voice Route



Skype for Business Server

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

Create voice routing test case information

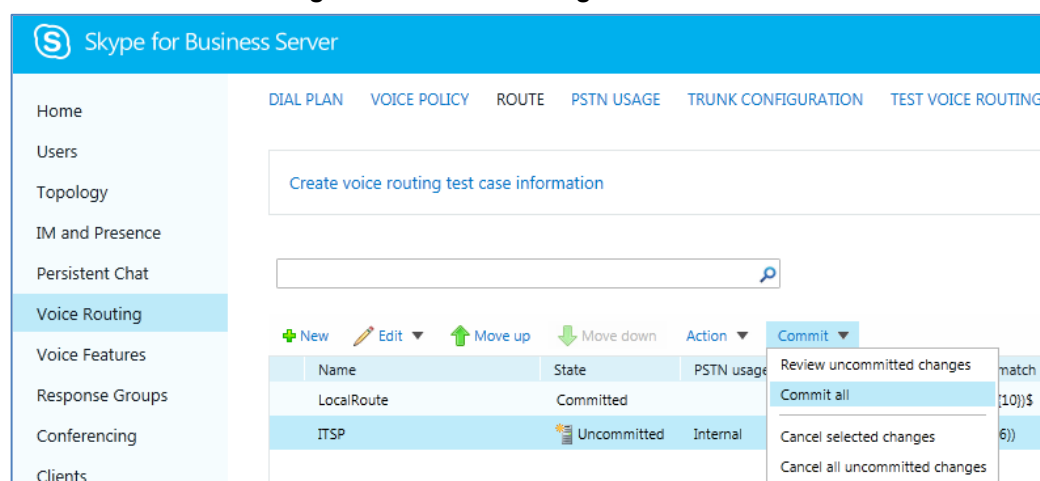
Search

+ New Edit Move up Move down Action Commit

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

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

Figure 3-24: Committing Voice Routes



Skype for Business Server

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

Create voice routing test case information

Search

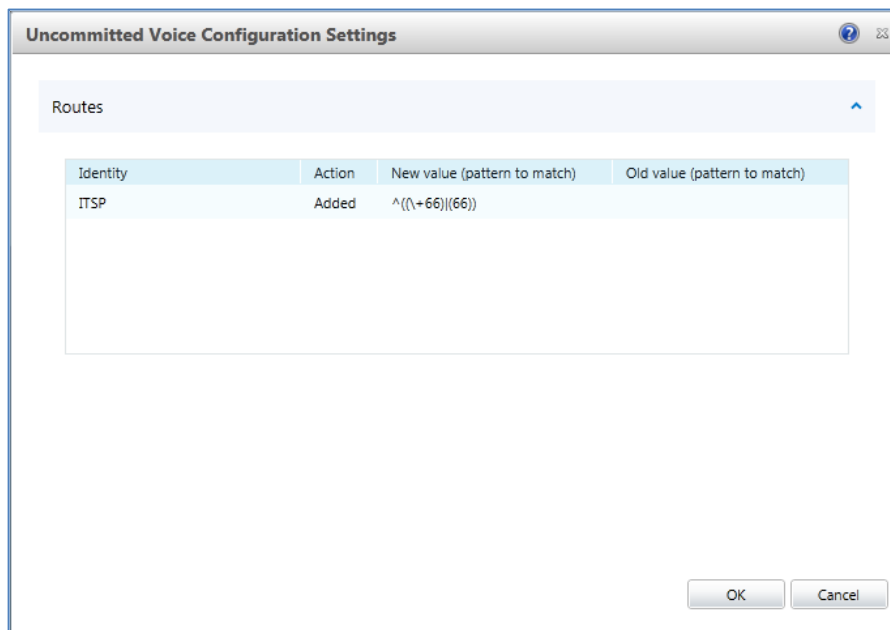
+ New Edit Move up Move down Action Commit

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

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

The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



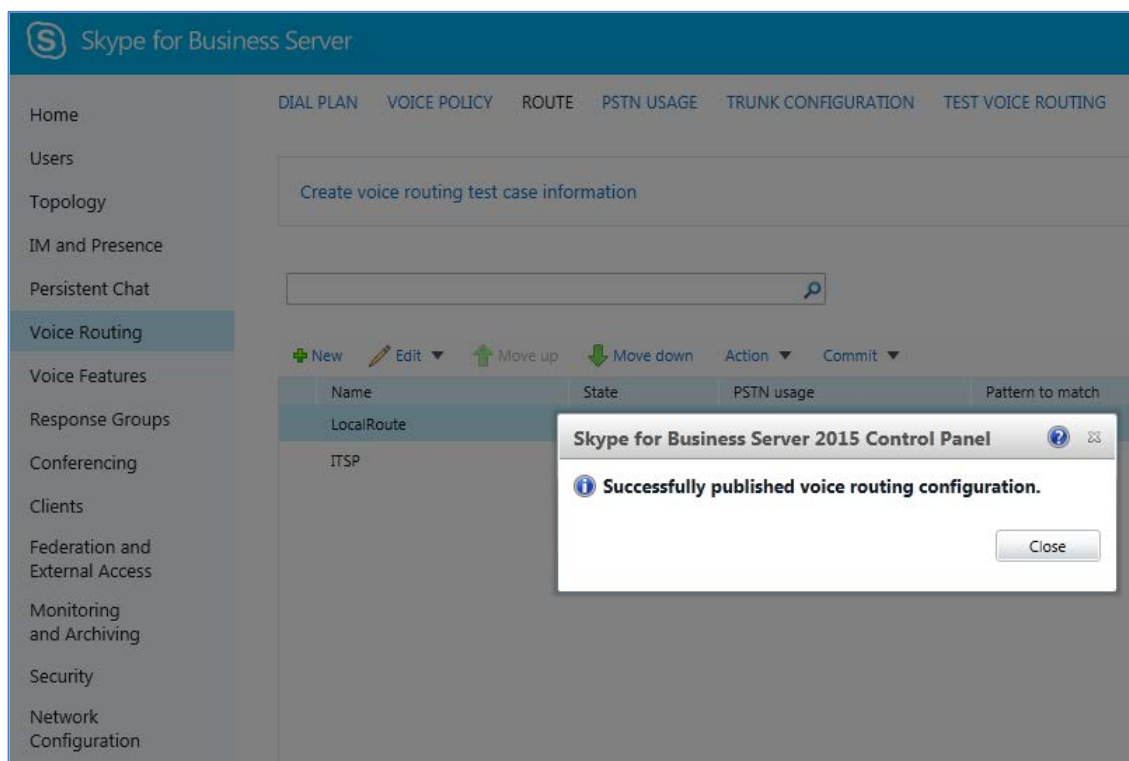
The dialog box titled "Uncommitted Voice Configuration Settings" contains a section labeled "Routes". Inside this section is a table with the following data:

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

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

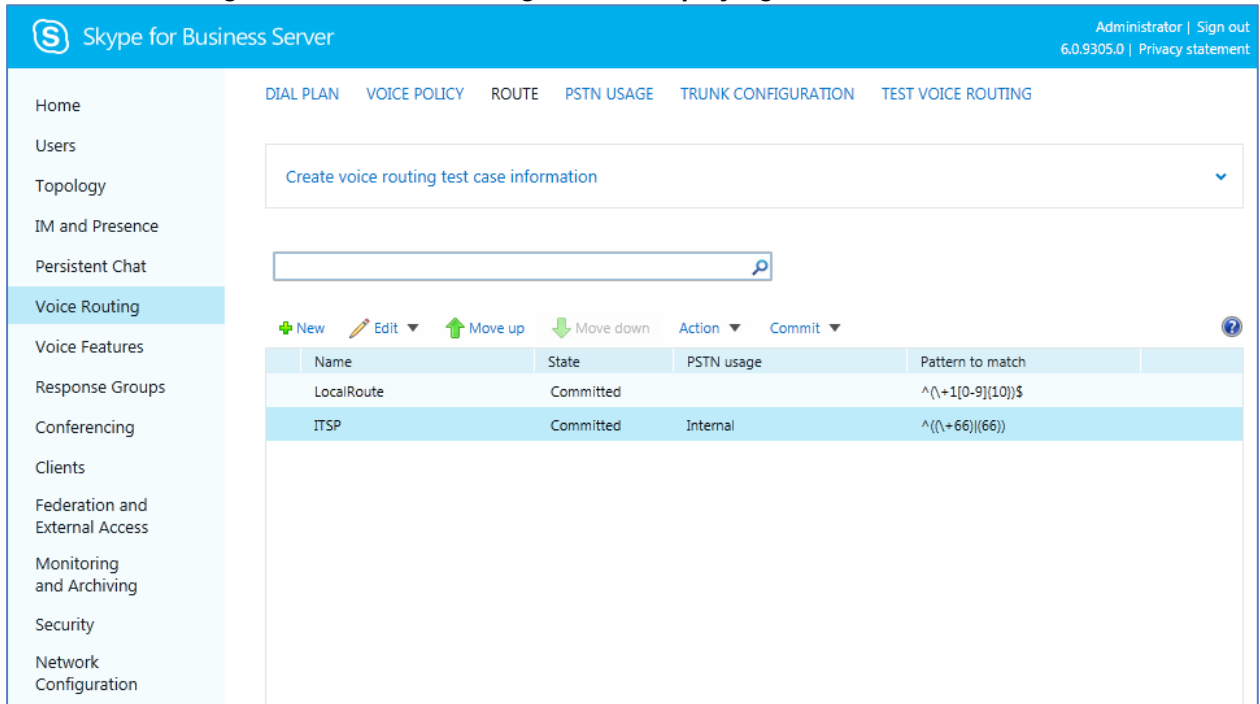
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-26: Confirmation of Successful Voice Routing Configuration



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

Figure 3-27: Voice Routing Screen Displaying Committed Routes



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

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

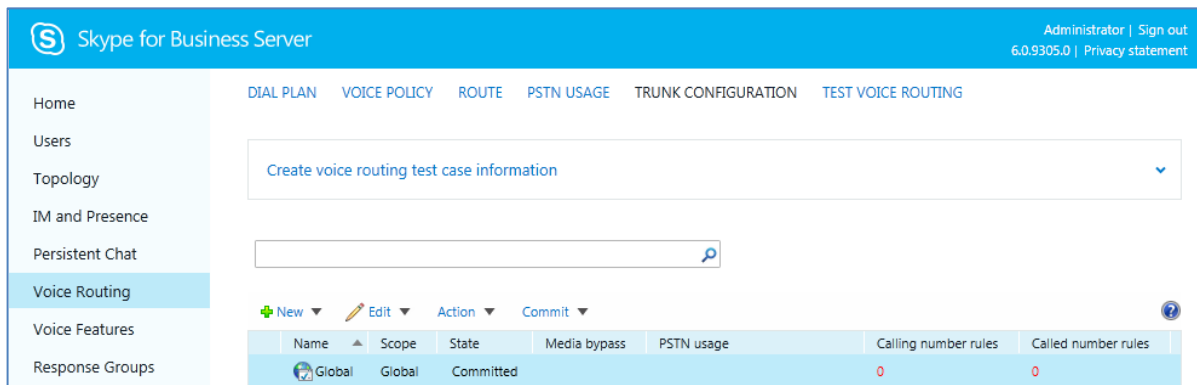
15. For ITSPs that implement a call identifier, continue with the following steps:



Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Skype for Business user number). This ID is required by Telecom Liechtenstein 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 4.5 on page 44).

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

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



The screenshot shows the Skype for Business Server interface with the 'Trunk Configuration' tab selected. The left sidebar remains the same. The top navigation bar includes tabs for DIAL PLAN, VOICE POLICY, ROUTE, PSTN USAGE, TRUNK CONFIGURATION, and TEST VOICE ROUTING. The main content area displays a table of trunk configurations.

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

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

The screenshot shows the Skype for Business Server Admin Center interface. The top navigation bar includes 'DIAL PLAN', 'VOICE POLICY', 'ROUTE', 'PSTN USAGE', 'TRUNK CONFIGURATION', and 'TEST VOICE ROUTING'. The left sidebar lists various configuration areas, with 'Voice Routing' selected. The main content area displays the 'New Trunk Configuration' page for 'PstnGateway:ITSP.S4B.interop'. The page includes a 'Scope' dropdown set to 'Pool', a 'Name' field with the value 'PstnGateway:ITSP.S4B.interop', and a 'Description' field. Below these are several settings: 'Maximum early dialogs supported' (set to 20), 'Encryption support level' (set to 'Required'), and 'Refer support' (set to 'Enable sending refer to the gateway'). At the bottom, there are several checkboxes: 'Enable media bypass' (checked), 'Centralized media processing' (checked), 'Enable RTP latching' (unchecked), 'Enable forward call history' (checked), 'Enable forward P-Asserted-Identity data' (unchecked), and 'Enable outbound routing failover timer' (checked). The page also features 'OK' and 'Cancel' buttons at the top left of the configuration area.

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

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes MSBR E-SBC for interworking between Microsoft Skype for Business Server 2015 and the Telecom Liechtenstein 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 MSBR WAN interface - Telecom Liechtenstein 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:

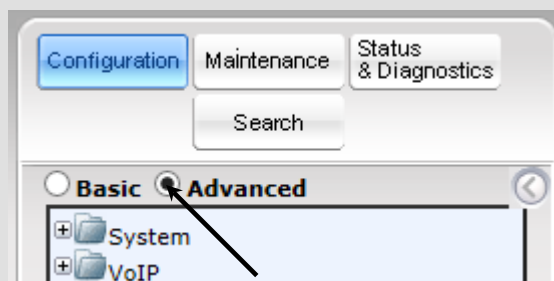
- For implementing Microsoft Skype for Business and Telecom Liechtenstein SIP Trunk based on the configuration described in this section, AudioCodes MSBR E-SBC must be installed with a Software License Key that includes the following software features:

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

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



- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Advanced-menu display mode. To do this, select the Advanced option, as shown below:



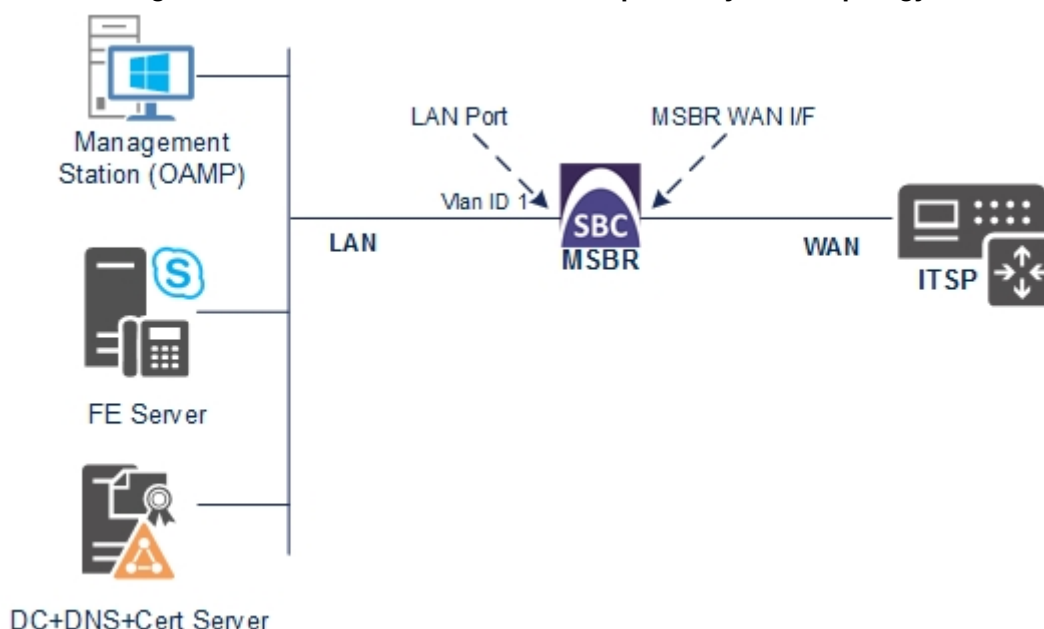
- When the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: IP Network Interfaces Configuration

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

- E-SBC interfaces with the following IP entities:
 - Skype for Business servers, located on the LAN
 - Telecom Liechtenstein SIP Trunk, located on the WAN
- 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 using dedicated LAN port and to the WAN using MSBR's WAN interface.

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure Network Interface

This step describes how to configure the IP network interface for LAN VoIP interface (assigned the name "Voice"). Configuration of WAN data interface depends on physical interface, that's why it is out of the scope of this document.

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

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

Parameter	Value
IP Address	10.15.17.10 (LAN IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Default Gateway	10.15.17.11 (MSBR Data vlan 1 IP address)
Interface Name	Voice (arbitrary descriptive name)
Primary DNS Server IP Address	10.15.27.1
Underlying Device	vlan 1

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

The configured IP network interface is shown below:

Figure 4-2: Configured Network Interface in IP Interfaces Table

Interface Table									
Add +		Edit ↗		Delete 🗑		Show/Hide 📄			
Index ↕	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media	IPv4 Manual	10.15.17.10	16	10.15.17.11	Voice	10.15.27.1	0.0.0.0	vlan 1

4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).

Figure 4-3: Enabling SBC Application

⚡ SAS Application	Disable
⚡ SBC Application	Enable
⚡ IP to IP Application	Disable

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.15 on page 80).

4.3 Step 3: Signaling Routing Domains Configuration

This step describes how to configure Signaling Routing Domains (SRD). The SRD represents a logical VoIP network. Each logical or physical connection requires an SRD, for example, if the E-SBC interfaces with both the LAN and WAN, a different SRD would be required for each one.

The SRD is composed of the following:

- **Media Realm:** Defines a UDP port range for RTP/SRTP (media) traffic on a specific logical IP network interface of the E-SBC.
- **SIP Interface:** Defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface of the E-SBC.

4.3.1 Step 3a: Configure Media Realms

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

➤ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Modify the existing Media Realm for LAN traffic:

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

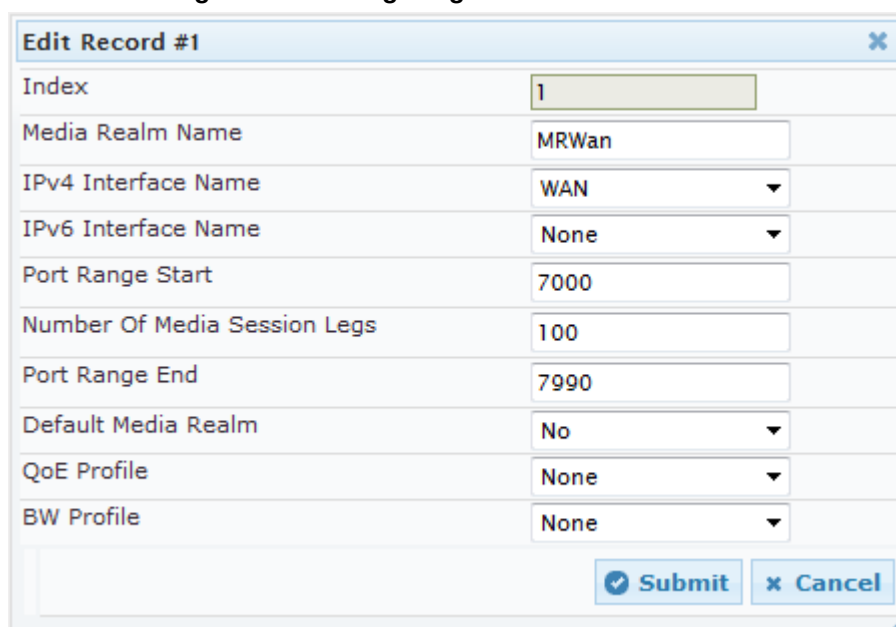
Figure 4-4: Configuring Media Realm for LAN

Edit Record #0	
Index	0
Media Realm Name	MRLan
IPv4 Interface Name	Voice
IPv6 Interface Name	None
Port Range Start	6000
Number Of Media Session Legs	100
Port Range End	-1
Default Media Realm	No
QoE Profile	None
BW Profile	None
Submit Cancel	

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Media Realm Name	MRWan (arbitrary name)
IPv4 Interface Name	WAN (a reserved word for MSBR WAN I/F)
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 4-5: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 4-6: Configured Media Realms in Media Realm Table

Media Realm Table			
Add +			
Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
0	MRLan	Voice	None
1	MRWan	WAN	None
Page 1 of 1 Show 10 records per page View 1 - 2 of 2			

4.3.2 Step 3b: Configure SRDs

This step describes how to configure the SRDs.

➤ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SRD Table**).
2. Configure an SRD for the E-SBC's internal interface (toward Skype for Business):

Parameter	Value
Index	0
Name	SRDLan (descriptive name for SRD)
Media Realm Name	MRLan (associates SRD with Media Realm)

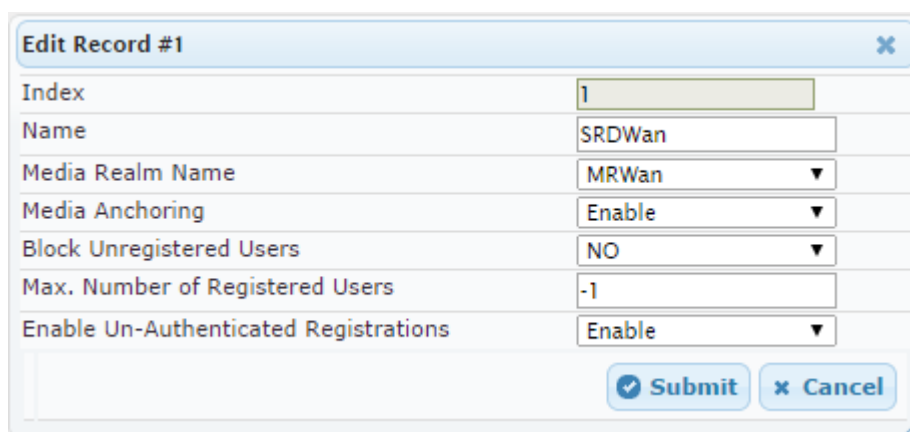
Figure 4-7: Configuring LAN SRD

The screenshot shows a web-based configuration window titled "Edit Record #0". It contains several input fields and dropdown menus. The "Index" field is set to 0. The "Name" field contains "SRDLan". The "Media Realm Name" dropdown is set to "MRLan". The "Media Anchoring" dropdown is set to "Enable". The "Block Unregistered Users" dropdown is set to "NO". The "Max. Number of Registered Users" field is set to "-1". The "Enable Un-Authenticated Registrations" dropdown is set to "Enable". At the bottom right, there are two buttons: "Submit" (with a checkmark icon) and "Cancel" (with an 'x' icon).

3. Configure an SRD for the E-SBC's external interface (toward the Telecom Liechtenstein SIP Trunk):

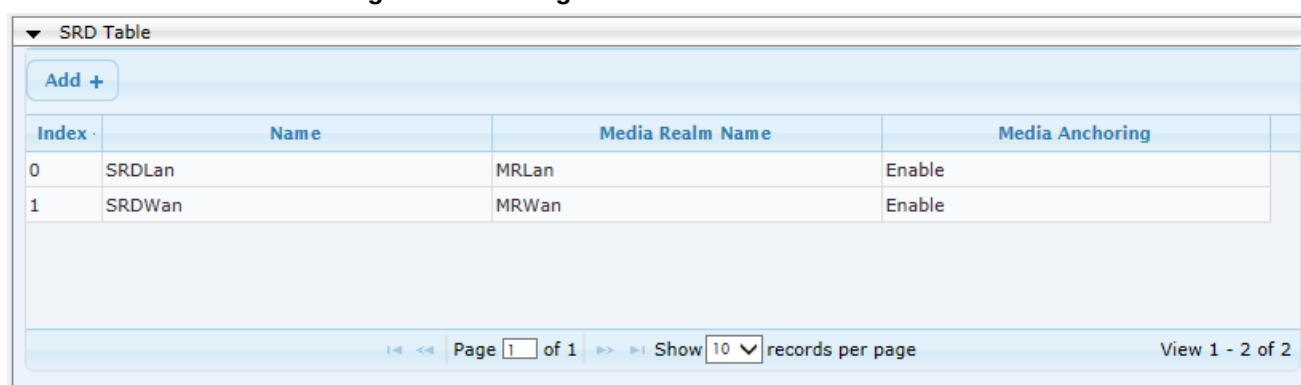
Parameter	Value
Index	1
Name	SRDWan
Media Realm Name	MRWan

Figure 4-8: Configuring WAN SRD



The configured SRDs are shown in the figure below:

Figure 4-9: Configured SRDs in SRD Table



Index	Name	Media Realm Name	Media Anchoring
0	SRDLan	MRLan	Enable
1	SRDWan	MRWan	Enable

4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➤ To configure SIP Interfaces:

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Configure a SIP interface for the LAN:

Parameter	Value
Index	0
Interface Name	S4B (arbitrary descriptive name)
Network Interface	Voice
Application Type	SBC
TLS Port	5067
TCP and UDP	0
SRD	0

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	1
Interface Name	TLI (arbitrary descriptive name)
Network Interface	WAN
Application Type	SBC
UDP Port	5060
TCP and TLS	5060 and 5061
SRD	1

The configured SIP Interfaces are shown in the figure below:

Figure 4-10: Configured SIP Interfaces in SIP Interface Table

SIP Interface Table							
Add +							
Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
0	S4B	Voice	SBC	0	0	5067	0
1	TLI	WAN	SBC	5060	5060	5061	1
Page 1 of 1 Show 10 records per page View 1 - 2 of 2							



Note: The TLS port parameter (for S4B SIP Interface) must be identically configured in the Skype for Business Topology Builder (see Section 3.1 on page 13).

4.4 Step 4: 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
- Telecom Liechtenstein SIP Trunk

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

➤ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the Skype for Business Server 2015 as shown below:

Parameter	Value
Proxy Set ID	1
Proxy Address	FE.S4B.interop:5067 (Skype for Business Server 2015 IP address / FQDN and destination port)
Transport Type	TLS
Proxy Name	S4B (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Homing
SRD Index	0
TLS Context Index	0

Figure 4-11: Configuring Proxy Set for Microsoft Skype for Business Server 2015

Proxy Set ID		1
--------------	--	---

	Proxy Address	Transport Type
1	FE.S4B.interop:5067	TLS
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name		S4B
Enable Proxy Keep Alive		Using Options
Proxy Keep Alive Time		60
KeepAlive Failure responses		
DNS Resolve Method		Not Configured
Proxy Load Balancing Method		Round Robin
Is Proxy Hot Swap		Yes
Proxy Redundancy Mode		Homing
SRD Index		0
Classification Input		IP only
TLS Context Index		-1

3. Configure a Proxy Set for the Telecom Liechtenstein SIP Trunk:

Parameter	Value
Proxy Set ID	2
Proxy Address	sip-proxy.fl1.li:5083 (for unsecure connection) sip-proxy2.fl1.li:5081 (for secure connection)
Transport Type	TCP or UDP (for unsecure connection) TLS (for secure connection)
Proxy Name	TLI (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
DNS Resolve Method	SRV
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Homing
SRD Index	1
TLS Context Index	1 (only for secure connection it is needed to differentiate TLS Contexts, used for connection with Skype for Business and SIP Trunk)

Figure 4-12: Configuring Proxy Set for Telecom Liechtenstein SIP Trunk

Proxy Set ID

2

	Proxy Address	Transport Type
1	sip-proxy.fl1.li:5083	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name

TLI

Enable Proxy Keep Alive

Using Options

Proxy Keep Alive Time

60

KeepAlive Failure responses

DNS Resolve Method

SRV

Proxy Load Balancing Method

Disable

Is Proxy Hot Swap

Yes

Proxy Redundancy Mode

Homing

SRD Index

1

Classification Input

IP only

TLS Context Index

-1

4.5 Step 5: 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. A typical deployment consists of multiple IP Groups associated with the same SRD. For example, you can have two LAN IP PBXs sharing the same SRD, and two ITSPs / SIP Trunks sharing the same SRD. 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)
- Telecom Liechtenstein SIP Trunk

➤ To configure IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the Skype for Business Server 2015 as shown below:

Parameter	Value
Index	1
Type	Server
Description	S4B (arbitrary descriptive name)
Proxy Set ID	1
SIP Group Name	t100000f.convoip.ch (according to ITSP requirement for Switzerland numbers) or t100000g.convoip.li (for Liechtenstein numbers)
SRD	0
Media Realm Name	MRLan
IP Profile ID	1

3. Configure an IP Group for the Telecom Liechtenstein SIP Trunk:

Parameter	Value
Index	2
Type	Server
Description	TLI (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	t100000f.convoip.ch (according to ITSP requirement for Switzerland numbers) or t100000g.convoip.li (for Liechtenstein numbers)
SRD	1
Media Realm Name	MRWan
IP Profile ID	2

The configured IP Groups are shown in the figure below:

Figure 4-13: Configured IP Groups in IP Group Table

▼ IP Group Table								
Add +								
Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
1	Server	S4B	1	t100000f.convoip.ch			No	0
2	Server	TLI	2	t100000f.convoip.ch			No	1
Page 1 of 1 Show 10 records per page View 1 - 2 of 2								

4.6 Step 6: Configure IP Profiles

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

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

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

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

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

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

Figure 4-14: Configuring IP Profile for Skype for Business Server 2015 – Common Tab

Common	GW	SBC
Index	1	
Profile Name	S4B	
Profile Preference	1	
Dynamic Jitter Buffer Minimum Delay [msec]	10	
Dynamic Jitter Buffer Optimization Factor	10	
RTP IP DiffServ	46	
Signaling DiffServ	40	
Silence Suppression	Disable ▼	
RTP Redundancy Depth	0	
Echo Canceler	Line ▼	
Broken Connection Mode	Ignore ▼	
Input Gain (-32 to 31 dB)	0	
Voice Volume (-32 to 31 dB)	0	
Media IP Version Preference	Only IPv4 ▼	
Symmetric MKI	Enable ▼	
MKI Size	1	
Reset SRTP Upon Re-key	Enable ▼	
Generate SRTP keys mode	Always ▼	
Jitter Buffer Max Delay [msec]	300	
Submit Cancel		

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

Parameter	Value
Allowed Coders Group ID	Coders Group 0
Allowed Coders Mode	Preference (re-arranges the order of the coders according to their order of appearance in the Allowed Coders Group Table)
SBC Media Security Behavior	SRTP
PRACK Mode	Optional
Remote Update Support	Supported Only After Connect
Remote re-INVITE	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
Remote REFER Behavior	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Remote 3xx Behavior	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)
Enforce MKI Size	Enforce
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)
Remote Can Play Ringback	No

Figure 4-15: Configuring IP Profile for Skype for Business Server 2015 – SBC Tab

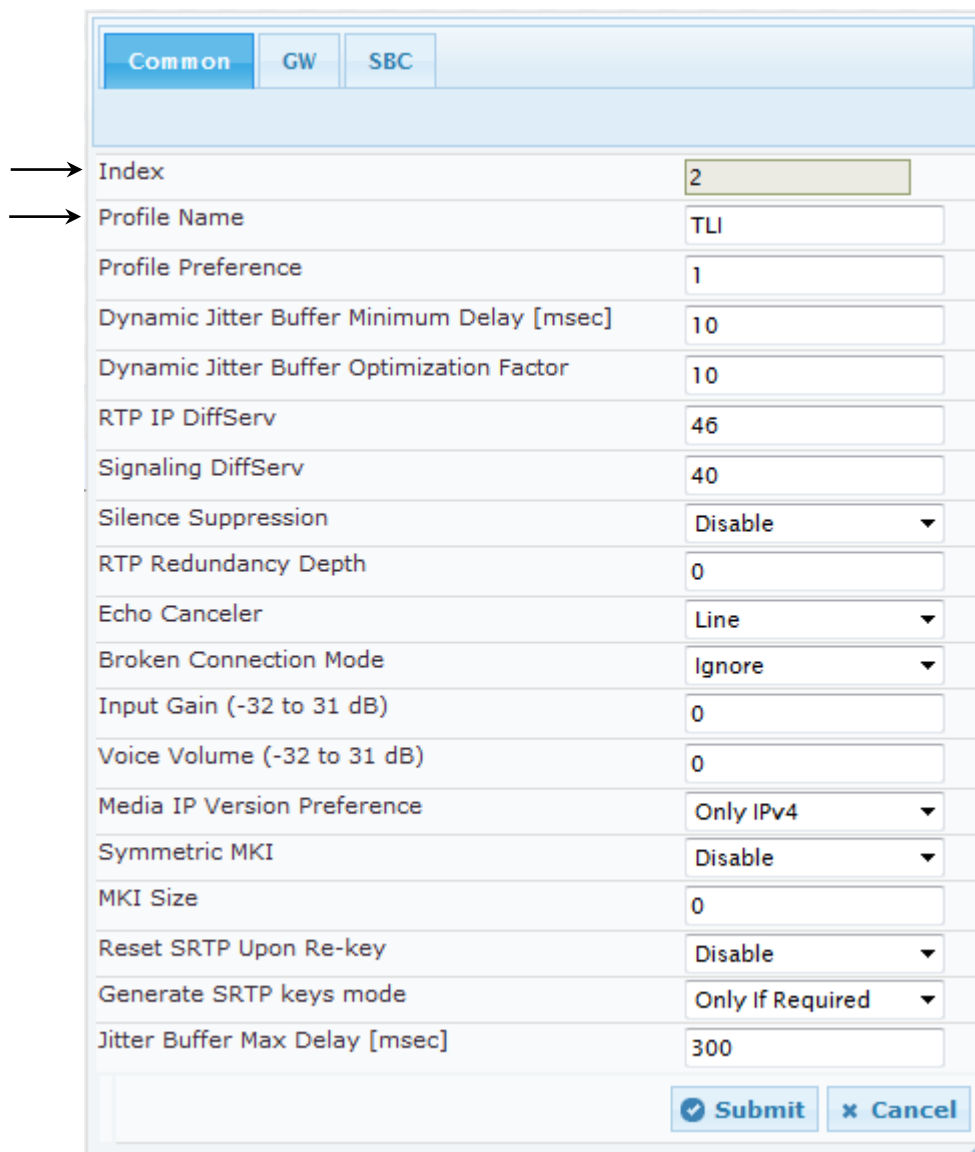
Common GW SBC	
Index	1
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
→ Allowed Coders Group ID	Coders Group 0
→ Allowed Video Coders Group ID	None
→ Allowed Coders Mode	Preference
→ SBC Media Security Behavior	SRTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	As Is
Diversion Mode	As Is
History-Info Mode	As Is
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
→ PRACK Mode	Optional
Session Expires Mode	Supported
→ Remote Update Support	Supported Only Aft
→ Remote re-INVITE	Supported only witl
→ Remote Delayed Offer Support	Not Supported
→ Remote REFER Behavior	Handle Locally
→ Remote 3xx Behavior	Handle Locally
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
→ Enforce MKI Size	Enforce
→ Remote Early Media RTP Detection Mode	By Media
Remote RFC 3960 Gateway Model Support	Not Supported
→ Remote Can Play Ringback	No
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Transparent
Remote Replaces Behavior	Standard
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Remove
RTP Redundancy Behavior	Disallow
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Transparent
Remote Multiple Answers Mode	Disabled
Keep VIA Headers	Not Configured
Keep User-Agent Header	Not Configured
User Behind NAT UDP Registration Time	-1
User Behind NAT TCP Registration Time	-1
Adapt RFC2833 BW to Voice coder BW	Disabled
Submit Cancel	

➤ To configure an IP Profile for the Telecom Liechtenstein SIP Trunk:

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

Parameter	Value
Index	2
Profile Name	TLI

Figure 4-16: Configuring IP Profile for Telecom Liechtenstein SIP Trunk – Common Tab



Parameter	Value
Index	2
Profile Name	TLI
Profile Preference	1
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceler	Line
Broken Connection Mode	Ignore
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required
Jitter Buffer Max Delay [msec]	300

Submit Cancel

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

Parameter	Value
Allowed Coders Group ID	Coders Group 0
Allowed Coders Mode	Restriction and Preference (use only Allowed Coders and re-arranges the order of the coders according to their order of appearance in the Allowed Coders Group Table)
SBC Media Security Behavior	RTP or SRTP (for secured connection)
Diversion Mode	Add (required for transferred calls)
History-Info Mode	Remove
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Remote Early Media RTP Detection Mode	By Media (required, in order to send pre-recorded ringback tone)
Remote Can Play Ringback	No
Remote Hold Format	Send Only

Figure 4-17: Configuring IP Profile for Telecom Liechtenstein SIP Trunk – SBC Tab

Common GW SBC	
Index	2
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
→ Allowed Coders Group ID	Coders Group 0
→ Allowed Video Coders Group ID	None
→ Allowed Coders Mode	Restriction and Pref
→ SBC Media Security Behavior	RTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	As Is
→ Diversion Mode	Add
→ History-Info Mode	Remove
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Transparent
Session Expires Mode	Transparent
Remote Update Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Supported
→ Remote REFER Behavior	Handle Locally
Remote 3xx Behavior	Transparent
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
→ Enforce MKI Size	Don't enforce
→ Remote Early Media RTP Detection Mode	By Media
→ Remote RFC 3960 Gateway Model Support	Not Supported
→ Remote Can Play Ringback	No
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
→ Remote Hold Format	Send Only
Remote Replaces Behavior	Standard
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Transparent
Remote Multiple Answers Mode	Disabled
Keep VIA Headers	Not Configured
Keep User-Agent Header	Not Configured
User Behind NAT UDP Registration Time	-1
User Behind NAT TCP Registration Time	-1
Adapt RFC2833 BW to Voice coder BW	Disabled

Submit Cancel

4.7 Step 7: Configure Coders

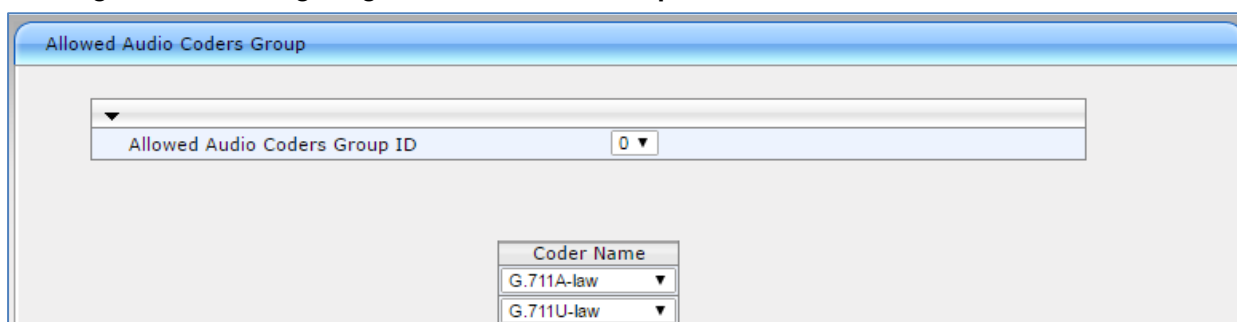
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Telecom Liechtenstein SIP Trunk uses the G.711A-law and G.711U-law coders only and in specific order. Note that this Allowed Coders Group ID was assigned to the IP Profiles (see Section 4.5 on page 44).

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

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

Parameter	Value
Allowed Audio Coders Group ID	0
Coder Name	G.711A-law
Coder Name	G.711U-law

Figure 4-18: Configuring Allowed Coders Group for Telecom Liechtenstein SIP Trunk



4.8 Step 8: 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 or the Telecom Liechtenstein SIP Trunk. This is essential for a secure SIP TLS connection.

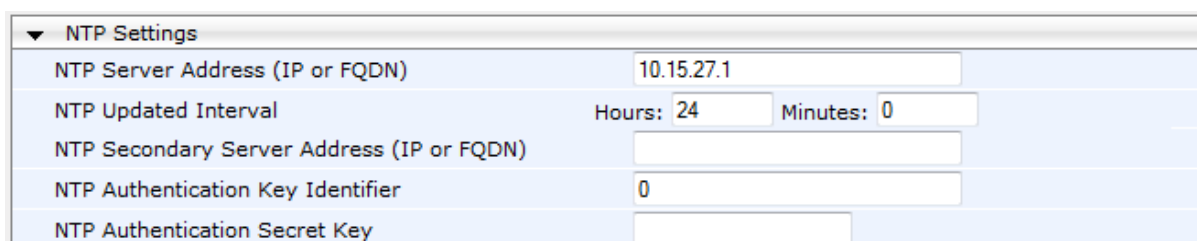
4.8.1 Step 8a: Configure the NTP Server Address

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

➤ To configure the NTP server address:

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

Figure 4-19: Configuring NTP Server Address



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

3. Click **Submit**.

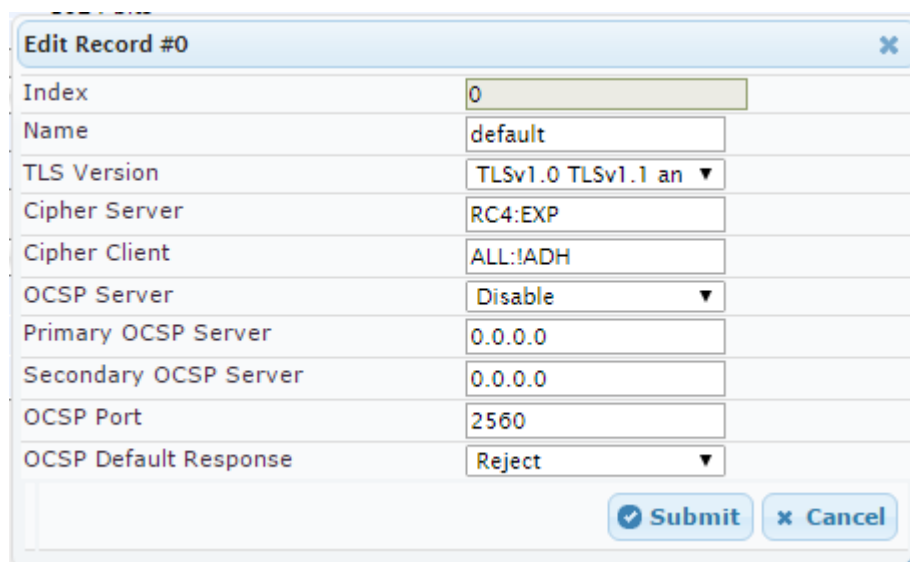
4.8.2 Step 8b: Configure the TLS version

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 page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click 'Edit'.
3. From the 'TLS Version' drop-down list, select 'TLSv1.0 TLSv1.1 and TLSv1.2'

Figure 4-20: Configuring TLS version



The screenshot shows a web-based configuration window titled "Edit Record #0". It contains a table of configuration parameters for TLS. The parameters and their values are as follows:

Parameter	Value
Index	0
Name	default
TLS Version	TLSv1.0 TLSv1.1 and
Cipher Server	RC4:EXP
Cipher Client	ALL:!ADH
OCSP Server	Disable
Primary OCSP Server	0.0.0.0
Secondary OCSP Server	0.0.0.0
OCSP Port	2560
OCSP Default Response	Reject

At the bottom right of the dialog, there are two buttons: "Submit" (with a checkmark icon) and "Cancel" (with an 'x' icon).

4. Click **Submit**.

4.8.3 Step 8c: Configure a Certificate for Operation with Microsoft Skype for Business Server 2015

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:

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

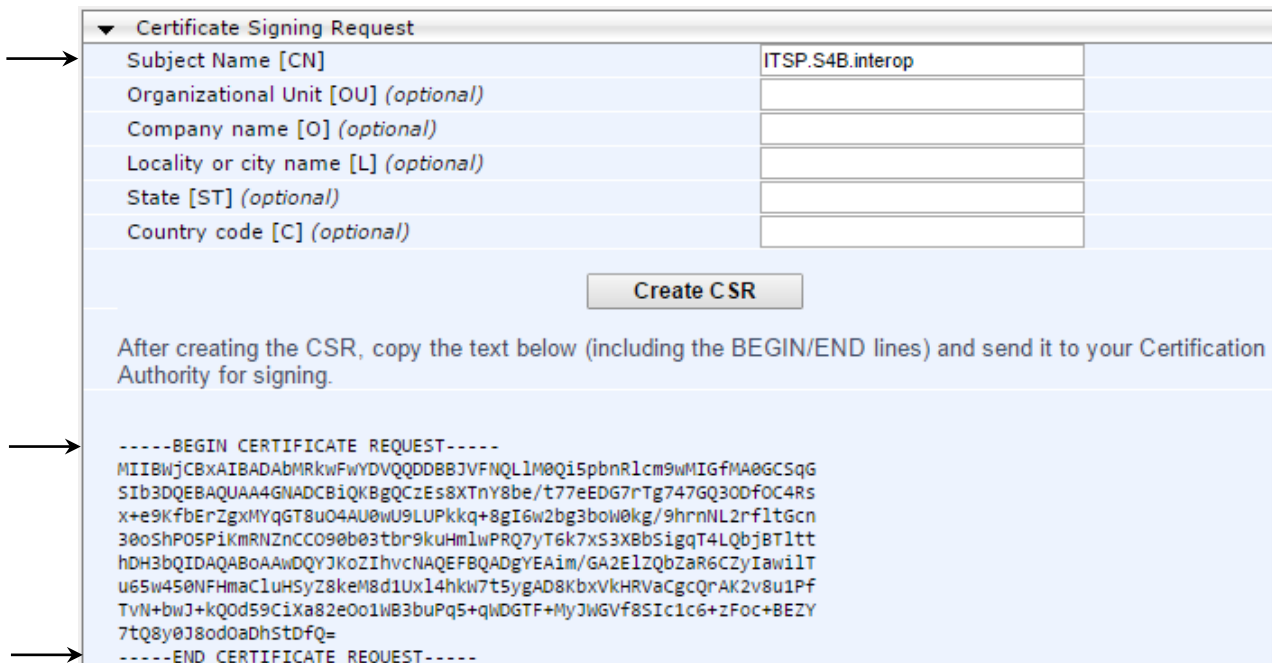


Note: The Subject Name (CN) field parameter should be identically configured in the DNS Active Directory and Topology Builder (see Section 3.1 on page 13).

➤ To configure a certificate:

- Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
- In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click the **TLS Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
- Under the **Certificate Signing Request** group, do the following:
 - In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **ITSP.S4B.interop**).
 - Fill in the rest of the request fields according to your security provider's instructions.
- Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-21: Certificate Signing Request – Creating CSR



▼ Certificate Signing Request

Subject Name [CN]	ITSP.S4B.interop
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	

Create CSR

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

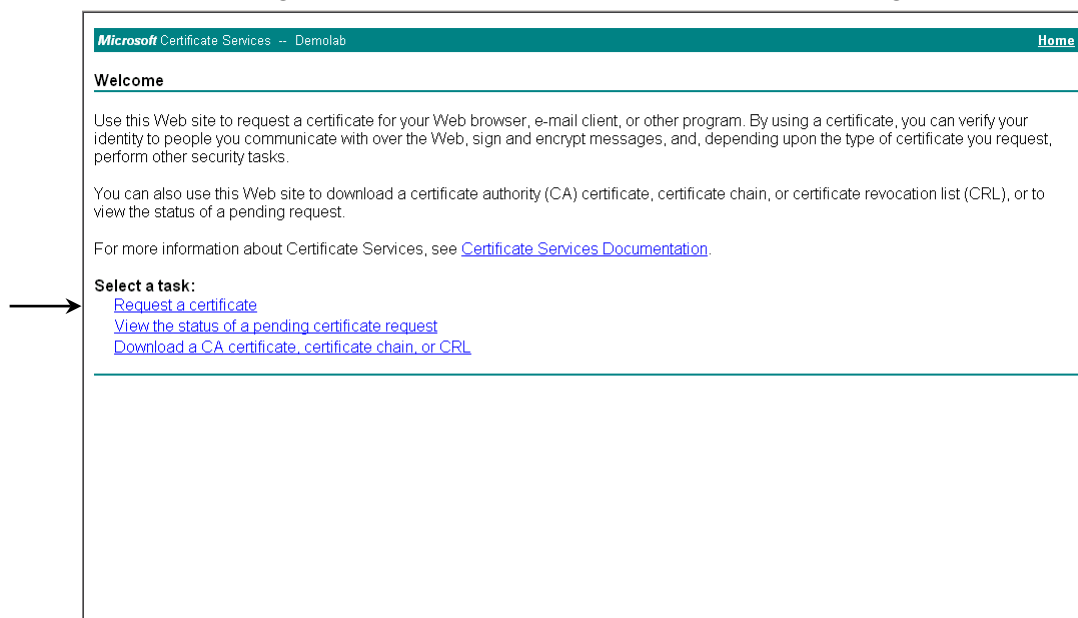
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAIBADAbMRkwFwYDVQQDDBBjVFNQL1M0Q1SpbnRlcm9wMIGfMA0GCSqG
S1B3DQEBAAQAGNADCBiQKBgQCzEs8XTnY8be/t77eEDG7rTg747GQ3ODfOC4Rs
x+e9KfberZgxMYqGT8u04AU0wU9LUPkq+8gI6w2bg3bow0kg/9hrnNL2rf1tGcn
30oShPO5PikmRNZnCC090b03tbr9kuHmlwPRQ7yT6k7xS3XBbsigqT4LQbj8T1tt
hDH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAim/GA2ELZQbZaR6CZyIaw1lt
u65w450NFHmaC1uHSyZ8keM8d1Ux14hkw7t5ygAD8KbxVkhRvACgcQrAK2v8u1Pf
TVN+bwJ+kQOd59CiXa82e0o1WB3buPq5+qWDGTF+MyJWGVf8S1c1c6+zFoc+BEZY
7tQ8y0J8od0aDhStdfQ=
-----END CERTIFICATE REQUEST-----
```



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

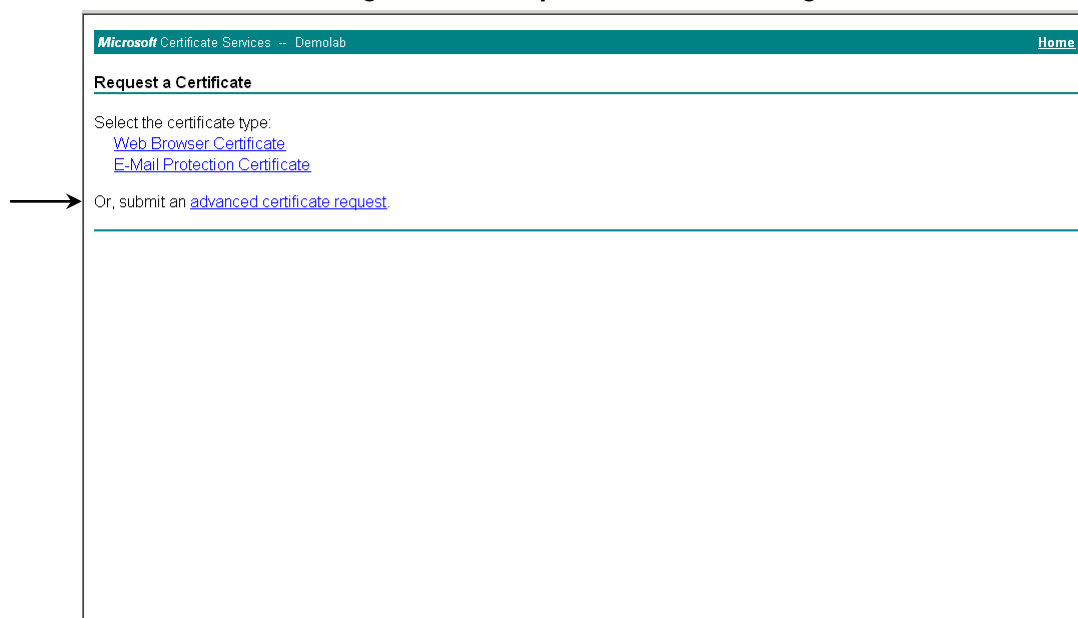
5. Copy the CSR from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate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

Figure 4-22: Microsoft Certificate Services Web Page



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

Figure 4-23: Request a Certificate Page



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

Figure 4-24: Advanced Certificate Request Page

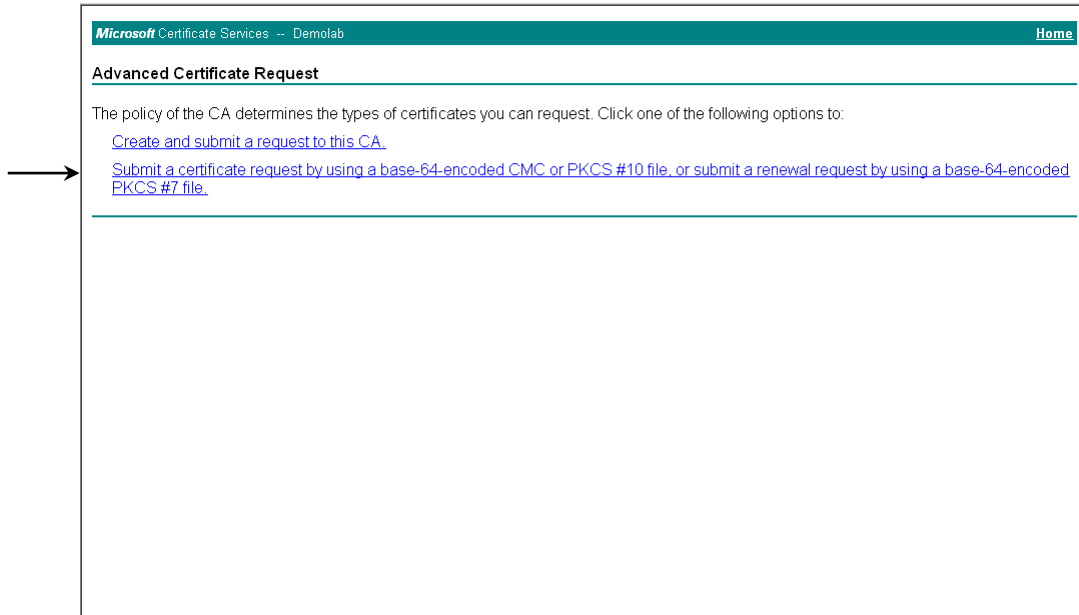
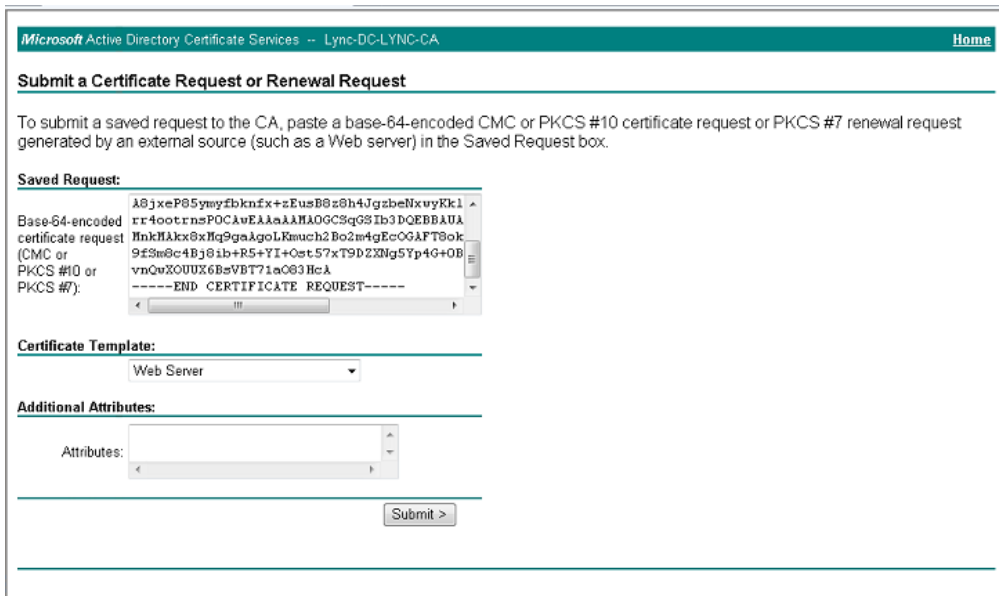
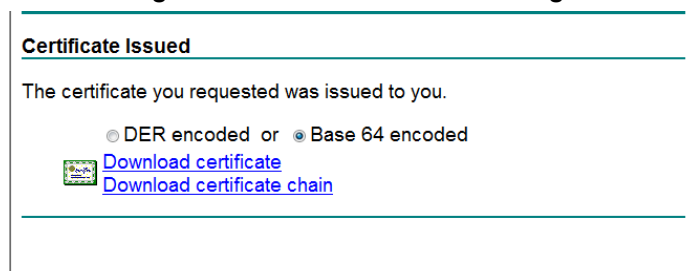


Figure 4-25: Submit a Certificate Request or Renewal Request Page



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

Figure 4-26: Certificate Issued Page



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

Figure 4-27: Download a CA Certificate, Certificate Chain, or CRL Page

Microsoft Certificate Services -- Demolab Home

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

Current [Demolab]

Encoding method:

☒ DER
☐ Base 64

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

17. Under the 'Encoding method' group, select the **Base 64** option for encoding.
18. Click **Download CA certificate**.
19. Save the file as *certroot.cer* to a folder on your computer.
20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts table, select the required TLS Context index row (typically, the default TLS Context at Index 0 is used), and then click the **TLS Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
 - b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-28: Upload Device Certificate Files from your Computer Group

▼ Upload certificate files from your computer

Private key pass-phrase (optional)

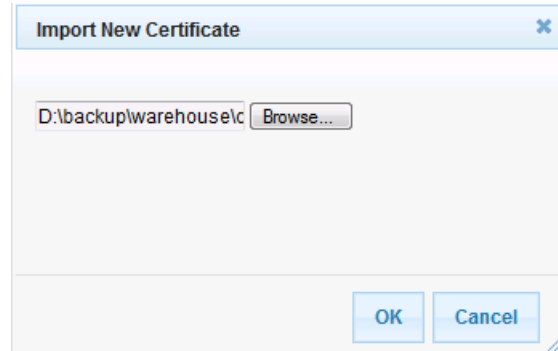
Send **Private Key** file from your computer to the device.
 The file must be in either PEM or PFX (PKCS#12) format.

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

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

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

Figure 4-29: 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 80).

4.8.4 Step 8d: Configure a Certificate for work with Telecom Liechtenstein SIP Trunk



Note: This step is only relevant for implementing a TLS connectivity to the Telecom Liechtenstein SIP trunk.

This step describes how to exchange a certificate with Telecom Liechtenstein Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with the Telecom Liechtenstein SIP Trunk.

The procedure involves the following main steps:

- a. Obtaining Trusted Root Certificate from Telecom Liechtenstein CA.
- b. Deploying Trusted Root Certificates on E-SBC.

➤ **To configure a certificate:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. Click **Add** and configure new record in the TLS Contexts table (with name e.g., **TLI**).
3. Click the **TLS Context Certificates**  button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
4. In the TLS Contexts table, select the **TLI** TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates**  button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
5. Click the **Import** button, and then select the certificate file to load Telecom Liechtenstein Trusted Root Certificate.
6. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
7. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 80).

4.9 Step 9: Configure SRTP

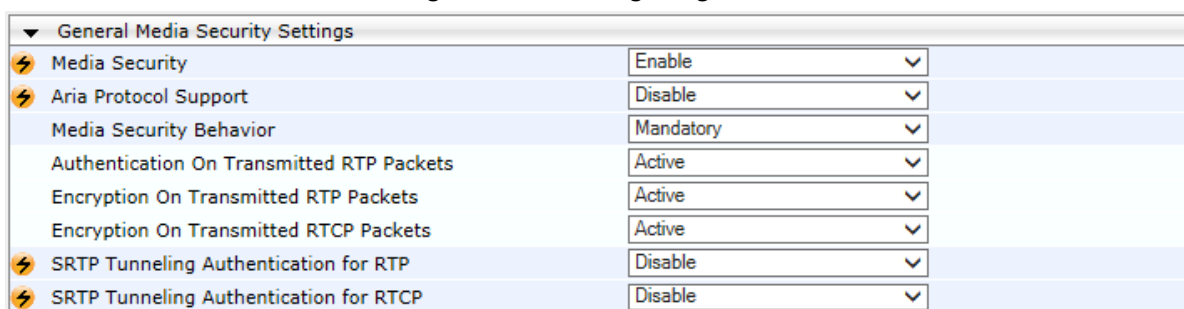
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 4.5 on page 44).

➤ **To configure media security:**

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

Parameter	Value
Media Security	Enable

Figure 4-30: Configuring SRTP



General Media Security Settings		
Media Security	Enable	▼
Aria Protocol Support	Disable	▼
Media Security Behavior	Mandatory	▼
Authentication On Transmitted RTP Packets	Active	▼
Encryption On Transmitted RTP Packets	Active	▼
Encryption On Transmitted RTCP Packets	Active	▼
SRTP Tunneling Authentication for RTP	Disable	▼
SRTP Tunneling Authentication for RTCP	Disable	▼

3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 80).

4.10 Step 10: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 44, IP Group 1 represents Skype for Business Server 2015, and IP Group 2 represents Telecom Liechtenstein SIP Trunk.

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

- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Skype for Business Server 2015 to Telecom Liechtenstein SIP Trunk
- Calls from Telecom Liechtenstein SIP Trunk to Skype for Business Server 2015

➤ **To configure IP-to-IP routing rules:**

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

Parameter	Value
Index	0
Route Name	Terminate OPTIONS (arbitrary descriptive name)
Request Type	OPTIONS

Figure 4-31: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS – Rule Tab

Rule	Action
Index	0
Route Name	Terminate OPTIONS
Source IP Group ID	-1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1
Submit Cancel	

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-32: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS – Action Tab

Rule	Action
Index	0
Destination Type	Dest Address
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	internal
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
Rules Set Id	-1
Submit Cancel	

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

Parameter	Value
Index	1
Route Name	S4B to ITSP (arbitrary descriptive name)
Source IP Group ID	1

Figure 4-33: Configuring IP-to-IP Routing Rule for S4B to ITSP – Rule tab

The screenshot shows a configuration window with two tabs: 'Rule' (selected) and 'Action'. The 'Rule' tab contains the following fields and values:

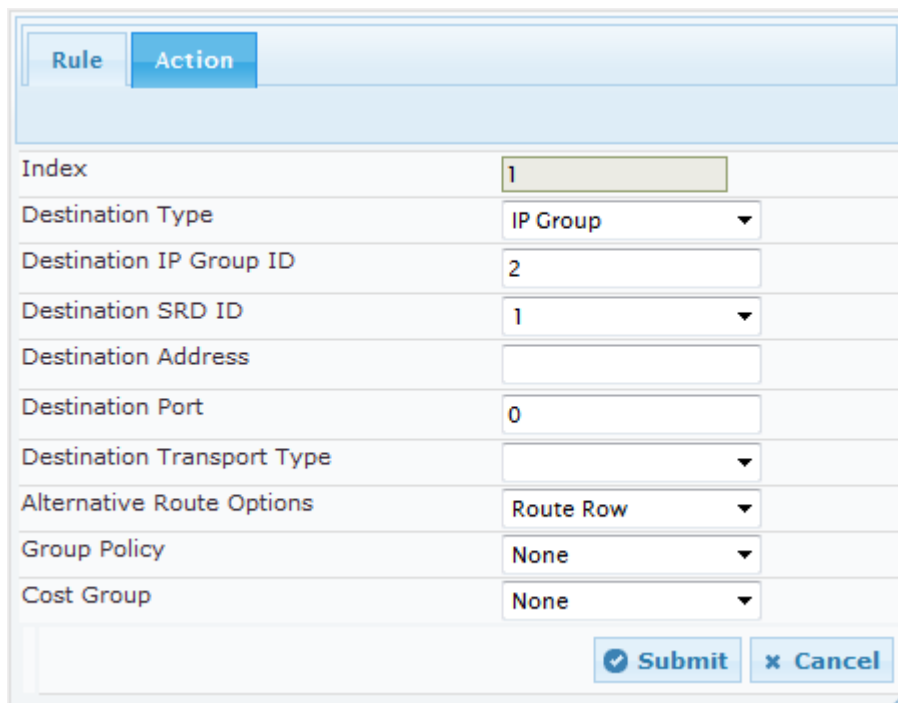
Index	1
Route Name	S4B to ITSP
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

At the bottom right of the window are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	1

Figure 4-34: Configuring IP-to-IP Routing Rule for S4B to ITSP – Action tab



Rule Action	
Index	1
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	1
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None

Submit Cancel

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

Parameter	Value
Index	2
Route Name	ITSP to S4B (arbitrary descriptive name)
Source IP Group ID	2

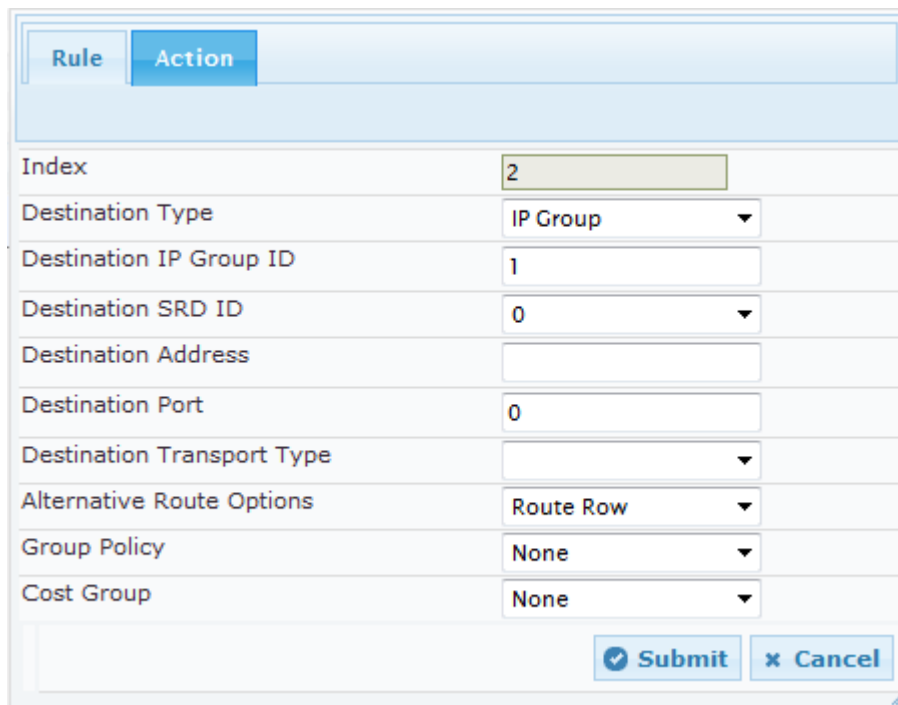
Figure 4-35: Configuring IP-to-IP Routing Rule for ITSP to S4B – Rule tab

Parameter	Value
Index	2
Route Name	ITSP to S4B
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

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

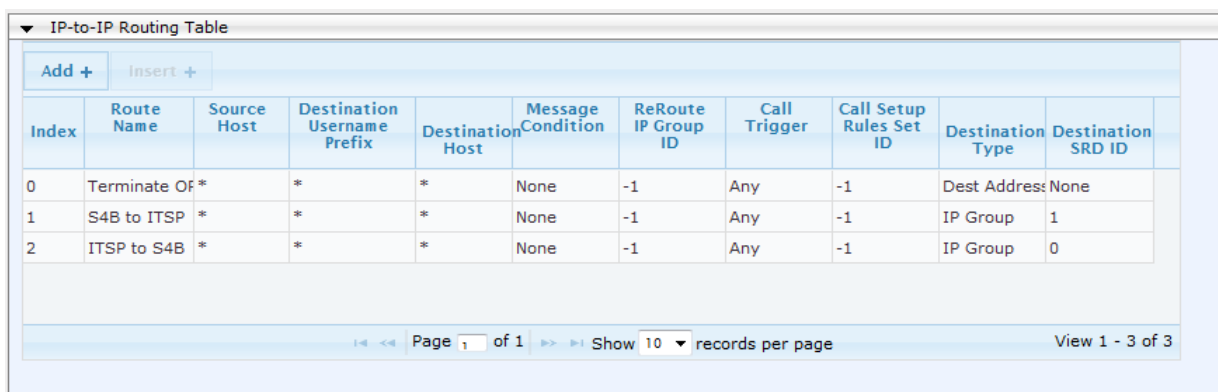
Parameter	Value
Destination Type	IP Group
Destination IP Group ID	1
Destination SRD ID	0

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



The configured routing rules are shown in the figure below:

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



Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination SRD ID
0	Terminate OF*	*	*	*	None	-1	Any	-1	Dest Address	None
1	S4B to ITSP *	*	*	*	None	-1	Any	-1	IP Group	1
2	ITSP to S4B *	*	*	*	None	-1	Any	-1	IP Group	0



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

4.11 Step 11: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 44, IP Group 0 represents Skype for Business Server 2015, and IP Group 1 represents Telecom Liechtenstein SIP Trunk.



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

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

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

1. Open the IP-to-IP Outbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC > Manipulations SBC > IP-to-IP Outbound**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Source IP Group	2
Destination IP Group	1
Destination Username Prefix	* (asterisk sign)

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

The screenshot shows the 'Rule' tab of the IP-to-IP Outbound Manipulation configuration form. The fields are as follows:

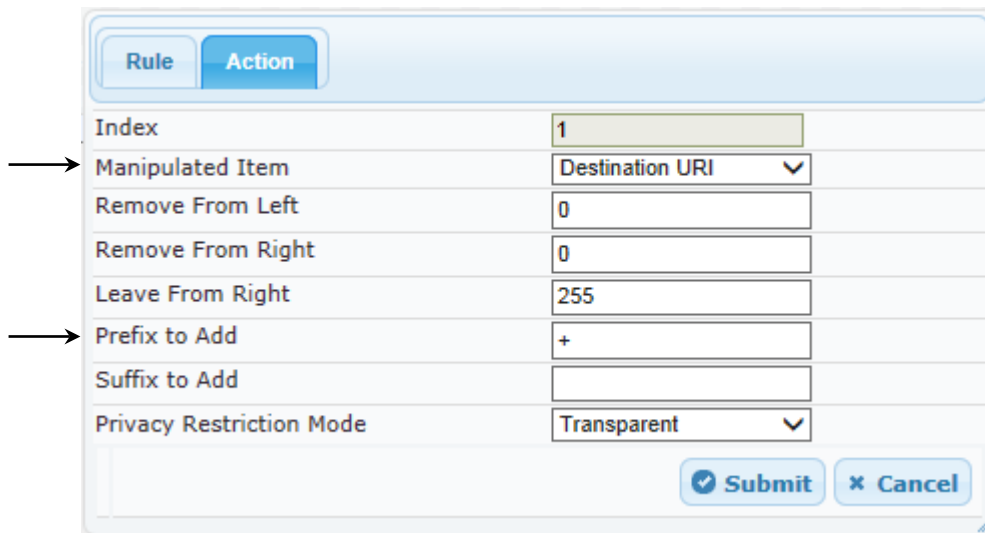
- Index:** 1
- Manipulation Name:** (empty text field)
- Additional Manipulation:** No (dropdown menu)
- Source IP Group ID:** 2
- Destination IP Group ID:** 1
- Source Username Prefix:** *
- Source Host:** *
- Destination Username Prefix:** *
- Destination Host:** *
- Calling Name Prefix:** *
- Message Condition:** None (dropdown menu)
- Request Type:** All (dropdown menu)
- ReRoute IP Group ID:** -1
- Call Trigger:** Any (dropdown menu)

At the bottom right, there are 'Submit' and 'Cancel' buttons.

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

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

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



5. Click **Submit**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between IP Group 1 (i.e., Skype for Business Server 2015) and IP Group 2 (i.e., Telecom Liechtenstein SIP Trunk):

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

IP to IP Outbound Manipulation												
Add + Insert +												
Index	Manipulation Name	Additional Manipulation	Source IP Group ID	Destination IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Manipulated Item	Prefix to Add	Suffix to Add
1		No	2	1	*	*	*	*	All	Destination	+	
2		No	1	2	*	*	+	*	All	Destination		
3		No	1	2	+	*	*	*	All	Source URI		

Page 1 of 1 Show 10 records per page View 1 - 3 of 3

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

4.12 Step 12: Configure Message Manipulation Rules

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

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

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for Telecom Liechtenstein SIP Trunk. This rule is applied to messages sent to the Telecom Liechtenstein SIP Trunk IP Group for Call Forward initiated by the Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Diversion Header with the value from the SIP From Header.

Parameter	Value
Index	0
Manipulation Name	Call Forward
Manipulation Set ID	4
Message Type	invite
Action Subject	header.diversion.url.host
Action Type	Modify
Action Value	header.from.url.host

Figure 4-41: Configuring SIP Message Manipulation Rule 0 (for Telecom Liechtenstein SIP Trunk)

The screenshot shows a web-based configuration interface for SIP Message Manipulation Rules. The 'Edit Record #0' dialog is open, displaying the following fields and values:

- Index:** 0
- Manipulation Name:** Call Forward
- Manipulation Set ID:** 4
- Message Type:** invite
- Condition:** (empty field)
- Action Subject:** header.diversion.url.ho
- Action Type:** Modify (dropdown menu)
- Action Value:** header.from.url.host
- Row Role:** Use Current Condi (dropdown menu)

At the bottom right of the dialog, there are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

3. Configure another manipulation rule (Manipulation Set 4) for Telecom Liechtenstein SIP Trunk. This rule is applied to messages sent to the Telecom Liechtenstein SIP Trunk IP Group during Call Transfer initiated by the Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Referred-By Header with the value, configured in the 'SIP Group Name' parameter for the Telecom Liechtenstein SIP Trunk IP Group.

Parameter	Value
Index	1
Manipulation Name	Call Transfer
Manipulation Set ID	4
Message Type	invite
Condition	header.referred-by exists
Action Subject	header.referred-by.url.host
Action Type	Modify
Action Value	param.ipg.dst.host

Figure 4-42: Configuring SIP Message Manipulation Rule 1 (for Telecom Liechtenstein SIP Trunk)

Edit Record #1

Index	1
Manipulation Name	Call Transfer
Manipulation Set ID	4
Message Type	invite
Condition	header.referred-by exists
Action Subject	header.referred-by.url.h
Action Type	Modify
Action Value	param.ipg.dst.host
Row Role	Use Current Condit

Submit
Cancel

4. Configure another manipulation rule (Manipulation Set 4) for Telecom Liechtenstein SIP Trunk. This rule is applied to messages sent to the Telecom Liechtenstein SIP Trunk IP Group for Anonymous Calls initiated by the Skype for Business Server 2015. This rule adds a SIP Privacy Header with value 'id'.

Parameter	Value
Index	2
Manipulation Name	For Anonymous Calls
Manipulation Set ID	4
Message Type	invite
Condition	header.from.url contains 'anonymous'
Action Subject	header.privacy
Action Type	Add
Action Value	'id'

Figure 4-43: Configuring SIP Message Manipulation Rule 2 (for Telecom Liechtenstein SIP Trunk)

Edit Record #2

Index	2
Manipulation Name	For Anonymous Calls
Manipulation Set ID	4
Message Type	invite
Condition	header.from.url contain
Action Subject	header.privacy
Action Type	Add
Action Value	'id'
Row Role	Use Current Condit

Figure 4-44: Configured SIP Message Manipulation Rules

▼ Message Manipulations							
Add +		Insert +					
Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	Call Forward	4	invite		header.diversion.url.host	Modify	header.from.url.host
1	Call Transfer	4	invite	header.referred-by exists	header.referred-by.url	Modify	param.ipg.dst.host
2	For Anonymous Call	4	invite	header.from.url contains	header.privacy	Add	'id'
Page 1 of 1 Show 10 records per page View 1 - 3 of 3							

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

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule is applied to messages sent to the Telecom Liechtenstein SIP Trunk IP Group for Call Forward initiated by the Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Diversion Header with the value from the SIP From Header.	For Call Forward scenarios, Telecom Liechtenstein SIP Trunk needs that host part in SIP Diversion Header will be pre-defined.
1	This rule is applied to messages sent to the Telecom Liechtenstein SIP Trunk IP Group during Call Transfer initiated by the Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Referred-By Header with the value, configured in the 'SIP Group Name' parameter for the Telecom Liechtenstein SIP Trunk IP Group.	For Call Transfer scenarios, Telecom Liechtenstein SIP Trunk needs that host part in SIP Referred-By Header will be pre-defined.
2	This rule is applied to messages sent to the Telecom Liechtenstein SIP Trunk IP Group for Anonymous Calls initiated by the Skype for Business Server 2015. This rule adds a SIP Privacy Header with value 'id'.	For Anonymous Calls scenarios, Telecom Liechtenstein SIP Trunk required SIP Privacy Header with value 'id'.

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

Figure 4-45: Assigning Manipulation Set 4 to the Telecom Liechtenstein SIP Trunk IP Group

Common		GW		SBC	
Index	2				
Classify By Proxy Set	Enable				
Max. Number of Registered Users	-1				
Inbound Message Manipulation Set	-1				
Outbound Message Manipulation Set	4				
Registration Mode	User Initiates Regis				
Authentication Mode	User Authenticates				
Authentication Method List					
SBC Client Forking Mode	Sequential				
Source URI Input					
Destination URI Input					
Username	Admin				
Password	•				
Msg Man User Defined String1					
Msg Man User Defined String2					
SIP Connect	No				
Route Using Request URI Port	Disable				
Submit Cancel					

- e. Click **Submit**.

4.13 Step 13: Configure Registration Accounts

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

In the interoperability test topology, the Served IP Group is Skype for Business Server 2015 (IP Group 1) and the Serving IP Group is Telecom Liechtenstein SIP Trunk (IP Group 2).

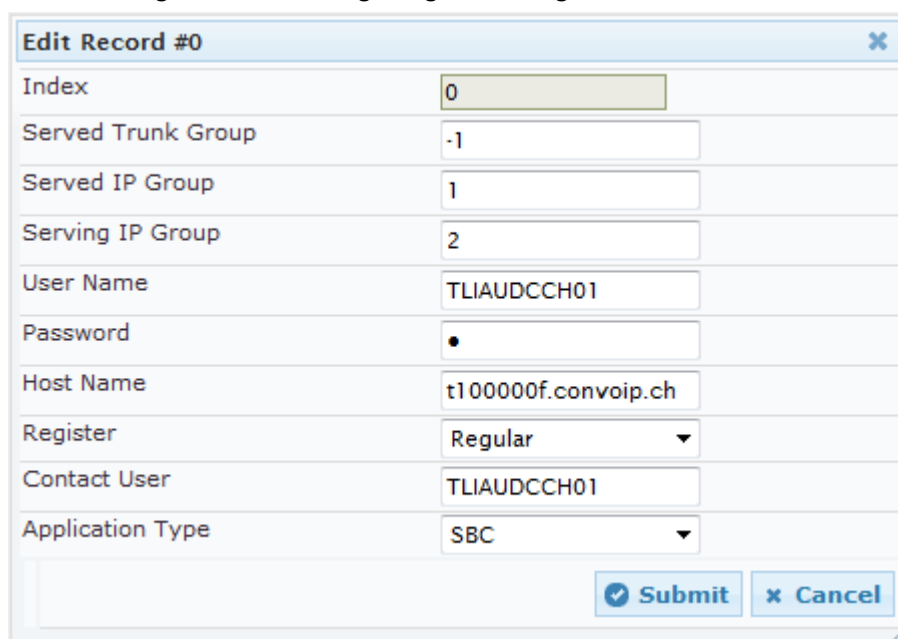
➤ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Click **Add**.
3. Configure the account according to the provided information from Telecom Liechtenstein, for example:

Parameter	Value
Served IP Group	1 (Skype for Business Server 2015)
Serving IP Group	2 (Telecom Liechtenstein SIP Trunk)
User Name	As provided by TLI
Password	As provided by TLI
Host Name	t100000f.convoip.ch (as provided by TLI)
Register	Regular
Contact User	TLIAUDCCH01 (as provided by TLI)
Application Type	SBC

4. Click **Add**.

Figure 4-46: Configuring a SIP Registration Account



Edit Record #0	
Index	0
Served Trunk Group	-1
Served IP Group	1
Serving IP Group	2
User Name	TLIAUDCCH01
Password	•
Host Name	t100000f.convoip.ch
Register	Regular
Contact User	TLIAUDCCH01
Application Type	SBC
Submit Cancel	

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

Figure 4-47: Configuring Forking Mode

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

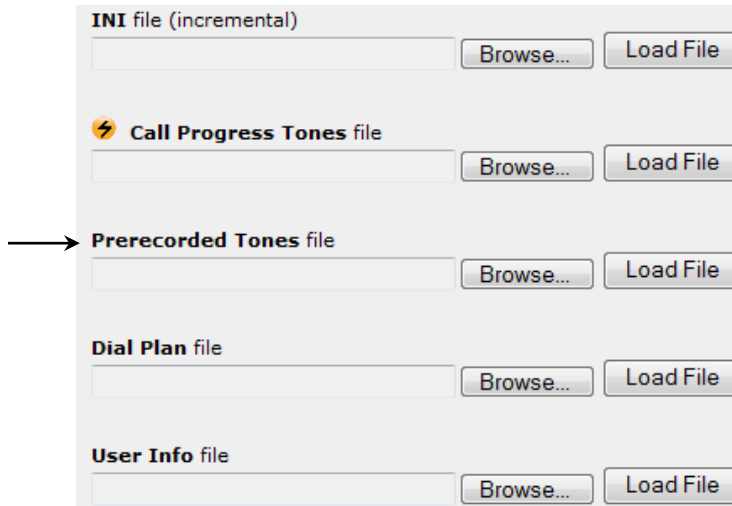
3. Click **Submit**.

4.14.2 Step 14b: Loading Prerecorded Tones File

This step describes how to load prerecorded tones file in order to overcome problem with first incoming RTP packet in call forwarding scenario, when Skype for Business user forward call to PSTN user. In this scenario, instead of generating Ringback Tone as Call Progress Tone (CPT), which requires DSP we decided to use Prerecorded Tones (PRT) file for ringback tones.

➤ To load PRT file to the device using the Web interface:

1. Open the Load Auxiliary Files page (**Maintenance** tab > **Software Update** menu > **Load Auxiliary Files**).




Note: The appearance of certain file load fields depends on the installed Software License Key.

2. Click the **Browse** button corresponding to the **Prerecorded Tones** file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
3. Click the **Load File** button corresponding to the file you want to load.
4. Save the loaded auxiliary files to flash memory.

4.14.3 Step 14c: Configure RTP Port for T.38 Fax

This step describes how to configure E-SBC to use the same RTP port for T.38 Fax for incoming fax.

➤ **To configure use RTP port for T.38 fax:**

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

Figure 4-48: Configuring SBC Session Refreshing Policy in AdminPage

The screenshot shows a web interface for configuring parameters. At the top, there are two input fields: 'Parameter Name:' and 'Enter Value:'. The 'Parameter Name' field contains 'T38USERTPPORT' and the 'Enter Value' field contains '1'. To the right of these fields is a button labeled 'Apply New Value'. Below these fields is a large area labeled 'Output Window'. Inside the 'Output Window', there is a text box containing the following information: 'Parameter Name: T38USERTPPORT', 'Parameter New Value: 1', and 'Parameter Description: T.38 packets will be received on RTP port'. Arrows point to the 'Parameter Name' field, the 'Enter Value' field, and the 'Apply New Value' button.

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

Parameter	Value
T38UseRTPPort	1

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

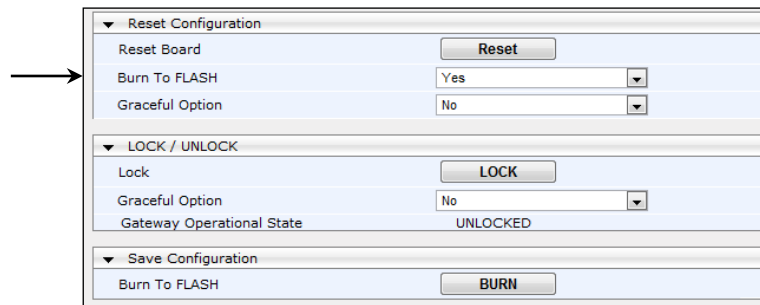
4.15 Step 15: Reset the E-SBC

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 save the configuration to flash memory:

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

Figure 4-49: Resetting the E-SBC



▼ Reset Configuration	
Reset Board	Reset
Burn To FLASH	Yes ▼
Graceful Option	No ▼
▼ LOCK / UNLOCK	
Lock	LOCK
Graceful Option	No ▼
Gateway Operational State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	BURN

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

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, relates to the SIP over TCP unsecured connection example with Liechtenstein numbers, is shown below:



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

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

;Board: Mediant 500 - MSBR
;HW Board Type: 69  FK Board Type: 77
;Serial Number: 4965606
;Slot Number: 1
;Software Version: 6.80A.308.003
;DSP Software Version: 5014AE3_R => 680.31
;Board IP Address: 10.15.17.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.17.11
;Ram size: 369M  Flash size: 64M  Core speed: 500Mhz
;Num of DSP Cores: 1  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;Key features:;Board Type: 77 ;IP Media: Conf VXML ;DSP Voice features:
RTCP-XR ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;Channel Type: DspCh=30 IPMediaDspCh=30 ;HA ;PSTN
FALLBACK Supported ;FXSPorts=3 ;FXOPorts=1 ;Coders: G723 G729 G728
NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711
MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB ;DATA features:
Routing FireWall&VPN WAN BGP Advanced-Routing 3G FTTX-WAN T1E1-Wan-
Trunks=2 ;Control Protocols: MSFT FEU=100 TestCall=100 MGCP SIP
SASurvivability SBC=60 ;Default features:;Coders: G711 G726;

;----- HW components-----
;
;
; Slot # : Module type : # of ports
;-----
;      2 : FXS          : 3
;      3 : FX0          : 1
;-----

[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
TelnetServerIdleDisconnect = 1000
;VpFileLastUpdateTime is hidden but has non-default value
TR069ACSPASSWORD = '$1$gQ=='
```

```
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.27.1'
LdapSearchServerMethod = 0
Tr069TLSContext = 0
;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]

NatMode = 0
PrerecordedTonesFileName = 'RingbackTone-Guitar-A-law.dat'
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1

[WEB Params]

SharedSecret = '$1$woS2sLC0opqIjoKZng=='
UserProductName = 'Mediant 500 - MSBR'
LogoWidth = '145'
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSPKeyFileName is hidden but has non-default value
```

```

[SIP Params]

REGISTRATIONTIME = 360
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
T38USERTPPOT = 1
USEGATEWAYNAMEFOROPTIONS = 1
;ENABLEPROXYSRVQUERY is hidden but has non-default value
;ENABLESRVQUERY is hidden but has non-default value
DNSQUERYTYPE = 1
PROXYDNSQUERYTYPE = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESENABLE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SCTP Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName;
DeviceTable 0 = 1, "", "vlan 1";

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.10, 16, 10.15.17.11, "Voice",
10.15.27.1, 0.0.0.0, "vlan 1";

[ \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 ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 100, 6990, 1, "", "";
CpMediaRealm 1 = "MRWan", "WAN", "", 7000, 100, 7990, 0, "", "";

[ \CpMediaRealm ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations;
SRD 0 = "SRDLan", "MRLan", 0, 0, -1, 1;
SRD 1 = "SRDWan", "MRWan", 0, 0, -1, 1;

[ \SRD ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE.S4B.interop:5067", 2, 1;
ProxyIp 1 = "sip-proxy.fl1.li:5083", 1, 2;

[ \ProxyIp ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
```

```

IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversiionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay, IpProfile_SBCRemoteMultipleAnswersMode,
IpProfile_SBCKeepVIAHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCAdaptRFC2833BWTToVoiceCoderBW;

```

```

IpProfile 1 = "S4B", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 0, -1, 1, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 0, 1, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 2, 2, 0, 0, 0,
0, 300, 0, -1, -1, -1, -1, 0;
IpProfile 2 = "TLI", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 0, -1, 2, 2, 0,
0, 0, 0, 8, 300, 400, 1, 2, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 3, 0, 1, 0, 1,
0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300, 0, -1, -1, -1, -1, 0;

```

[\IpProfile]

[ProxySet]

```

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;

```

```

ProxySet 0 = "", 0, 60, 0, 0, 0, 0, "-1", -1, -1, "";

```

```

ProxySet 1 = "S4B", 0, 60, 1, 1, 0, 0, "-1", 1, -1, "";

```

```

ProxySet 2 = "TLI", 1, 60, 0, 1, 1, 0, "-1", 1, 1, "";

```

[\ProxySet]

[IPGroup]

```

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,

```

```

IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BwProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect,
IPGroup_SBCRouteUsingRequestURIPort;

IPGroup 1 = 0, "S4B", 1, "t100000g.convoip.li", "", 0, -1, -1, 0, -1, 0,
"MRlan", 1, 1, -1, -1, 2, 0, 0, "", 0, -1, -1, "", "Admin",
"$1$aCkNBwIC", 0, "", "", "", 0, "", "", 0, 0;

IPGroup 2 = 0, "TLI", 2, "t100000g.convoip.li", "", 0, -1, -1, 0, -1, 1,
"MRwan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "Admin",
"$1$aCkNBwIC", 0, "", "", "", 0, "", "", 0, 0;

[ \IPGroup ]

[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup,
Account_ServingIPGroup, Account_Username, Account_Password,
Account_HostName, Account_Register, Account_ContactUser,
Account_ApplicationType;
Account 0 = -1, 1, 2, "TLIAUDCFL01", "$1$IHlnFBRdAx9rUH0HUw==",
"t100000g.convoip.li", 1, "TLIAUDCFL01", 2;

[ \Account ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "Terminate OPTIONS", -1, "", "", "", "", 6, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "S4B to ITSP", 1, "", "", "", "", 0, "", -1, 0, -1,
0, 2, "1", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to S4B", 2, "", "", "", "", 0, "", -1, 0, -1,
0, 1, "0", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]

[ TLSContexts ]

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

```

```

TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 7, "RC4:EXP", "ALL:!ADH", 0, , , 2560, 0;
TLSContexts 1 = "TLI", 7, "RC4:AES128", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet;
SIPInterface 0 = "S4B", "Voice", 2, 0, 0, 5067, 0, "", "", -1, 0, 500, -
1;
SIPInterface 1 = "TLI", "WAN", 2, 5060, 5060, 5061, 1, "", "", -1, 0,
500, -1;

[ \SIPInterface ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = "Add + toward S4B", 0, 2, 1, "", "", "00",
"", "", "", 0, -1, 0, 1, 2, 0, 255, "+", "", 0;
IPOutboundManipulation 1 = "Change + to 00 Dest", 0, 1, 2, "", "", "+",
"", "", "", 0, -1, 0, 1, 1, 0, 255, "00", "", 0;
IPOutboundManipulation 2 = "Change + to 00 Sour", 0, 1, 2, "+", "", "",
"", "", "", 0, -1, 0, 0, 1, 0, 255, "00", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

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

```

```
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 0, "";

[ \CodersGroup0 ]

[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = "g711Alaw64k";
AllowedCodersGroup0 1 = "g711Ulaw64k";

[ \AllowedCodersGroup0 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Call Forward", 4, "invite", "",
"header.diversion.url.host", 2, "header.from.url.host", 0;
MessageManipulations 1 = "Call Transfer", 4, "invite", "header.referred-
by exists", "header.referred-by.url.host", 2, "param.ipg.dst.host", 0;
MessageManipulations 2 = "For Anonymous Calls", 4, "invite",
"header.from.url contains 'anonymous'", "header.privacy", 0, "'id'", 0;

[ \MessageManipulations ]

[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 1, 1;

[ \RoutingRuleGroups ]

[ 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 ]
```

B AudioCodes CLI Script File

Below shown example of AudioCodes MSBR CLI script file:

```
# Running Configuration Mediant 500 - MSBR

## VoIP Configuration
configure voip
  tls 0
    name default
    tls-version tls-v1.0_1.1_1.2
    ciphers-server "RC4:EXP"
    ciphers-client "ALL:!ADH"
    ocsp-server disable
    ocsp-port 2560
    ocsp-default-response reject
  exit
  tls 1
    name TLI
    tls-version tls-v1.0_1.1_1.2
    ciphers-server "RC4:AES128"
    ciphers-client "ALL:!ADH"
    ocsp-server disable
    ocsp-port 2560
    ocsp-server-primary 0.0.0.0
    ocsp-server-secondary 0.0.0.0
    ocsp-default-response reject
  exit
  appli-enabling
    enable-sbc on
    activate
  exit
  coders-and-profiles ip-profile 1
    profile-name "S4B"
    disconnect-on-broken-connection ignore
    sbc-allowed-coders-group-id coders-group-0
    sbc-allowed-coders-mode preference
    sbc-media-security-behaviour srtp
    sbc-prack-mode optional
    sbc-rmt-update-supp supported-only-after-connect
    sbc-rmt-re-invite-supp supported-only-with-sdp
    sbc-rmt-delayed-offer not-supported
    sbc-rmt-refer-behavior handle-locally
    sbc-rmt-3xx-behavior handle-locally
    enable-symmetric-mki enable
    sbc-enforce-mki-size enforce
    sbc-rmt-early-media-rtp by-media
    sbc-rmt-can-play-ringback no
    early-answer-timeout 0
    reset-srtp-upon-re-key enable
    generate-srtp-keys always
    sbc-use-silence-supp remove
    sbc-rtp-red-behav disallow
    activate
  exit
```

```
coders-and-profiles ip-profile 2
  profile-name "TLI"
  disconnect-on-broken-connection ignore
  sbc-allowed-coders-group-id coders-group-0
  sbc-allowed-coders-mode restriction-and-preference
  sbc-media-security-behaviour rtp
  sbc-diversion-mode add
  sbc-history-info-mode remove
  sbc-rmt-refer-behavior handle-locally
  mki-size 0
  sbc-rmt-early-media-rtp by-media
  sbc-rmt-can-play-ringback no
  early-answer-timeout 0
  reset-srtp-upon-re-key disable
  generate-srtp-keys only-if-required
  remote-hold-Format sendonly
  activate
exit
coders-and-profiles coders-group-0 0
  name "g711Alaw64k"
  p-time 20
  rate 0
  activate
exit
coders-and-profiles coders-group-0 1
  name "g711Ulaw64k"
  p-time 20
  rate 0
  activate
exit
interface network-dev 0
  name "vlan 1"
  activate
exit
interface network-if 0
  ip-address 10.15.17.10
  gateway 10.15.17.11
  name "Voice"
  primary-dns 10.15.27.1
  underlying-dev "vlan 1"
  activate
exit
voip-network realm 0
  name "MRLan"
  ipv4if "Voice"
  port-range-start 6000
  session-leg 100
  port-range-end 6990
  is-default true
  activate
exit
voip-network realm 1
  name "MRWan"
  ipv4if "WAN"
  port-range-start 7000
  session-leg 100
```

```
port-range-end 7990
activate
exit
voip-network srd 0
name "SRDLan"
media-realm-name "MRLan"
activate
exit
voip-network srd 1
name "SRDWan"
media-realm-name "MRWan"
activate
exit
voip-network sip-interface 0
interface-name "S4B"
network-interface "Voice"
application-type sbc
udp-port 0
tcp-port 0
tls-port 5067
activate
exit
voip-network sip-interface 1
interface-name "TLI"
network-interface "WAN"
application-type sbc
srd 1
activate
exit
voip-network proxy-set 0
proxy-name ""
activate
exit
voip-network proxy-set 1
proxy-name "S4B"
proxy-load-balancing-method round-robin
is-proxy-hot-swap yes
proxy-redundancy-mode homing
activate
exit
voip-network proxy-set 2
proxy-name "TLI"
proxy-enable-keep-alive using-options
is-proxy-hot-swap yes
srd-id 1
proxy-redundancy-mode homing
dns-resolve-method srv
activate
exit
voip-network ip-group 1
description "S4B"
proxy-set-id 1
sip-group-name "t100000g.convoip.li"
media-realm-name "MRLan"
ip-profile-id 1
outbound-msg-manipulation-set 2
```

```
username "Admin"
password aCkNBwIC obscured
activate
exit
voip-network ip-group 2
description "TLI"
proxy-set-id 2
sip-group-name "t100000g.convoip.li"
srd 1
media-realm-name "MRwan"
ip-profile-id 2
outbound-mesg-manipulation-set 4
username "Admin"
password aCkNBwIC obscured
activate
exit
gw digitalgw rp-network-domains 1
name "dsn"
activate
exit
gw digitalgw rp-network-domains 2
name "dod"
activate
exit
gw digitalgw rp-network-domains 3
name "drsn"
activate
exit
gw digitalgw rp-network-domains 5
name "uc"
activate
exit
gw digitalgw rp-network-domains 7
name "cuc"
activate
exit
gw digitalgw digital-gw-parameters
answer-detector-cmd 10486144
energy-detector-cmd 587202560
activate
exit
ldap
ldap-search-server-method sequentialy
activate
exit
media udp-port-configuration
udp-port-spacing 10
activate
exit
media security
media-security-enable on
srtp-tx-packet-mKi-size 1
activate
exit
media RTP-RTCP
disable-nat-traversal 0
```

```
    activate
  exit
  sbc routing ip2ip-routing 0
    route-name "Terminate OPTIONS"
    request-type options
    dst-type dst-address
    dst-address "internal"
    activate
  exit
  sbc routing ip2ip-routing 1
    route-name "S4B to ITSP"
    src-ip-group-id 1
    dst-ip-group-id 2
    dst-srd-id "1"
    activate
  exit
  sbc routing ip2ip-routing 2
    route-name "ITSP to S4B"
    src-ip-group-id 2
    dst-ip-group-id 1
    dst-srd-id "0"
    activate
  exit
  sbc manipulations ip-outbound-manipulation 0
    manipulation-name "Add + toward S4B"
    src-ip-group-id 2
    dst-ip-group-id 1
    dst-user-name-prefix "00"
    manipulated-uri destination
    remove-from-left 2
    prefix-to-add "+"
    activate
  exit
  sbc manipulations ip-outbound-manipulation 1
    manipulation-name "Change + to 00 Dest"
    src-ip-group-id 1
    dst-ip-group-id 2
    dst-user-name-prefix "+"
    manipulated-uri destination
    remove-from-left 1
    prefix-to-add "00"
    activate
  exit
  sbc manipulations ip-outbound-manipulation 2
    manipulation-name "Change + to 00 Sour"
    src-ip-group-id 1
    dst-ip-group-id 2
    src-user-name-prefix "+"
    remove-from-left 1
    prefix-to-add "00"
    activate
  exit
  sbc manipulations message-manipulations 0
    manipulation-name "Call Forward"
    manipulation-set-id 4
    message-type "invite"
```

```
    action-subject "header.diversion.url.host"
    action-type modify
    action-value "header.from.url.host"
    activate
  exit
  sbc manipulations message-manipulations 1
    manipulation-name "Call Transfer"
    manipulation-set-id 4
    message-type "invite"
    condition "header.referred-by exists"
    action-subject "header.referred-by.url.host"
    action-type modify
    action-value "param.ipg.dst.host"
    activate
  exit
  sbc manipulations message-manipulations 2
    manipulation-name "For Anonymous Calls"
    manipulation-set-id 4
    message-type "invite"
    condition "header.from.url contains 'anonymous'"
    action-subject "header.privacy"
    action-value "'id'"
    activate
  exit
  sbc general-setting
    sbc-forking-handling-mode sequential
    sbc-preferences with-extensions
    activate
  exit
  sbc allowed-coders-group group-0 0
    name "g711Alaw64k"
    activate
  exit
  sbc allowed-coders-group group-0 1
    name "g711Ulaw64k"
    activate
  exit
  services least-cost-routing routing-rule-groups 0
    lcr-default-cost highest-cost
    activate
  exit
  sip-definition proxy-and-registration
    dns-query srv
    proxy-dns-query srv
    registration-time 360
    use-gw-name-for-opt enable
    activate
  exit
  sip-definition general-settings
    t38-use-rtp-port on
    activate
  exit
  sip-definition advanced-settings
    set ldap-primary-key "telephoneNumber"
    activate
  exit
```

```
sip-definition account 0
  served-ip-group 1
  serving-ip-group 2
  user-name "TLIAUDCFL01"
  password IHlnFBRdAx9rUH0HUw== obscured
  host-name "t100000g.convoip.li"
  register reg
  contact-user "TLIAUDCFL01"
  application-type sbc
  activate
exit
tdm
  pcm-law-select mulaw
  activate
exit
voip-network proxy-ip 0
  proxy-address "FE.S4B.interop:5067"
  transport-type tls
  proxy-set-id 1
  activate
exit
voip-network proxy-ip 1
  proxy-address "sip-proxy.fl1.li:5083"
  transport-type tcp
  proxy-set-id 2
  activate
exit
exit

## System Configuration
configure system
  cli-terminal
    idle-timeout 1000
    activate
  exit
  cwp
    set acs-password $1$gQ== obscured
    set connection-request-password $1$gQ== obscured
    tls-context 0
    activate
  exit
  logging
    syslog on
    debug-level detailed
    syslog-ip 10.15.17.100
    activate
  exit
  ntp
    set primary-server "10.15.27.1"
    activate
  exit
  radius
    set shared-secret "$1$woS2sLC0opqIjoKZng== "
    activate
  exit
  snmp
```

```
no activate-keep-alive-trap
activate
exit
web
set https-cipher-string "RC4:EXP"
activate
exit
no packetsmart enable
hostname "Mediant 500 - MSBR"
configuration-version 0
exit
configure data
interface GigabitEthernet 0/0
ip address 195.189.192.160 255.255.255.128
mtu auto
desc "WAN Copper"
no ipv6 enable
speed auto
duplex auto
no service dhcp
ip dns server static
ip name-server 80.179.52.100 80.179.55.100
napt
firewall enable
no shutdown
exit
interface Fiber 0/1
no ip address
mtu auto
desc "WAN Fiber"
no ipv6 enable
no service dhcp
ip dns server static
no shutdown
exit
interface GigabitEthernet 1/1
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/2
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/3
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
```

```
interface GigabitEthernet 1/4
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface VLAN 1
  ip address 10.15.17.11 255.255.0.0
  mtu auto
  desc "LAN switch VLAN 1"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no napt
  no firewall enable
  no link-state monitor
  no shutdown
exit
interface VLAN 2
  no ip address
  mtu auto
  desc "LAN switch VLAN 2"
  no ipv6 enable
  no service dhcp
  ip dns server auto
  no link-state monitor
  shutdown
exit
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 3600
ip nat translation icmp-timeout 6
# Note: The following WAN ports are in use by system services,
#       conflicting rules should not be created:
#       Ports 82 - 82 --> TR069
#       Ports 7000 - 7990 --> RealmPortPool::MRWan
#       Ports 5060 - 5060 --> SIPUDP#1
#       Ports 5060 - 5060 --> SIPLISTENING#1
#       Ports 5061 - 5061 --> SIPLISTENING#1
# Note: The following NAT rules are in effect for system services,
#       conflicting rules should not be created:
#       RealmPortPool::MRWan: LAN ports 7000-7990 to WAN IP
195.189.192.160 ports 7000-7990, interface GigabitEthernet 0/0
#       SIPUDP#1: LAN ports 5060-5060 to WAN IP 195.189.192.160
ports 5060-5060, interface GigabitEthernet 0/0
#       SIPLISTENING#1: LAN ports 5060-5060 to WAN IP
195.189.192.160 ports 5060-5060, interface GigabitEthernet 0/0
#       SIPLISTENING#1: LAN ports 5061-5061 to WAN IP
195.189.192.160 ports 5061-5061, interface GigabitEthernet 0/0
ip route 0.0.0.0 0.0.0.0 195.189.192.129 GigabitEthernet 0/0 1
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
exit
```


International Headquarters

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

AudioCodes Inc.

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

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com



Document #: LTRT-13040