Configuration Note

AudioCodes Professional Services - Interoperability Lab

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

Version 7.0

Table of Contents

This page is intentionally left blank.

Notice

This document describes how to connect the Microsoft Skype for Business Server 2015 and Polkomtel 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.

Date Published: June-29-2015

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 One Box 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
12420	Initial document release for Version 7.0.

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 Polkomtel's SIP Trunk and Microsoft's Skype for Business Server 2015 environment.

1.1 Intended Audience

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

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_7.00A.021.013
Protocol	▪ SIP/UDP (to the Polkomtel SIP Trunk) ▪ SIP/TCP or TLS (to the S4B FE Server)
Additional Notes	None

2.2 Polkomtel SIP Trunking Version

Table 2-2: Polkomtel Version

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

2.3 Microsoft Skype for Business Server 2015 Version

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

Vendor	Microsoft
Model	Skype for Business
Software Version	Release 2015 6.0.9305.0
Protocol	SIP
Additional Notes	None

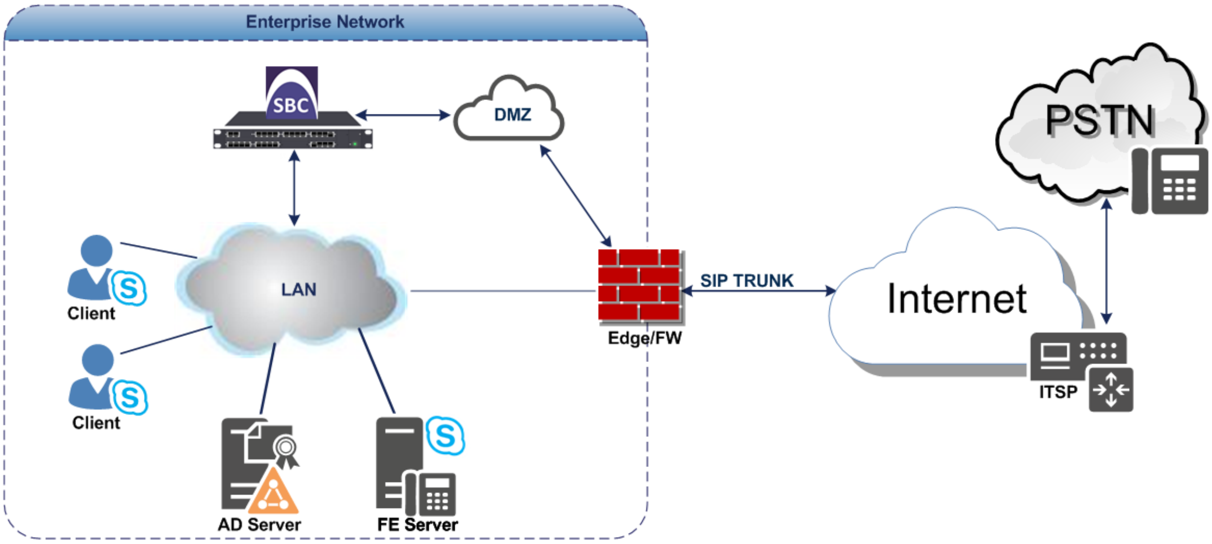
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Polkomtel 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 Polkomtel'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 Polkomtel'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 Polkomtel 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 ▪ Polkomtel SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SIP-over-TLS transport type ▪ Polkomtel SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders ▪ Polkomtel SIP Trunk supports G.711A-law and G.711U-law coders
Media Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SRTP media type ▪ Polkomtel SIP Trunk operates with RTP media type

2.4.2 Known Limitations

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

- For all outgoing calls from Microsoft Skype for Business Server 2015 through AudioCodes E-SBC towards the Polkomtel SIP Trunk, SIP INVITE messages from Microsoft immediately responded with 100 TRYING and 200 OK SIP messages. As a result, the remote ringback tone and early media cannot be heard.
- In Hold scenarios, even when Microsoft Skype for Business Client sends “a=sendonly” in the SDP part of SIP message (in order to play Music on Hold), Polkomtel SIP Trunk always responds with “a=inactive”. As a result, Music on Hold cannot be played. But Polkomtel SIP Trunk always plays Music on Hold by itself. The only problem, which may be here, if the customer (the owner of Microsoft Skype for Business Server 2015) will request to play its own music.
- If the Microsoft Skype for Business Server 2015 sends one of the following error Responses:
    - 480 Temporarily Unavailable
    - 488 Not Acceptable Here
    - 503 Service Unavailable
    - 603 Decline

  Polkomtel SIP Trunk still sends re-INVITEs and does not disconnect the call. To disconnect the call, a message manipulation rule is used to replace the above error response with the “486 Busy Here” response (see Section 4.14 on page 78).

This page is intentionally left blank.

3 Configuring Skype for Business Server 2015

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

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

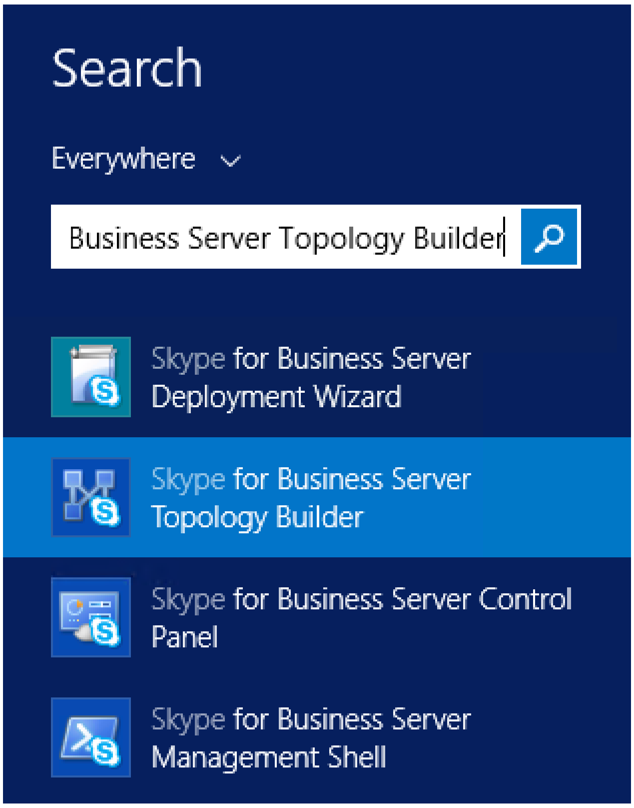
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

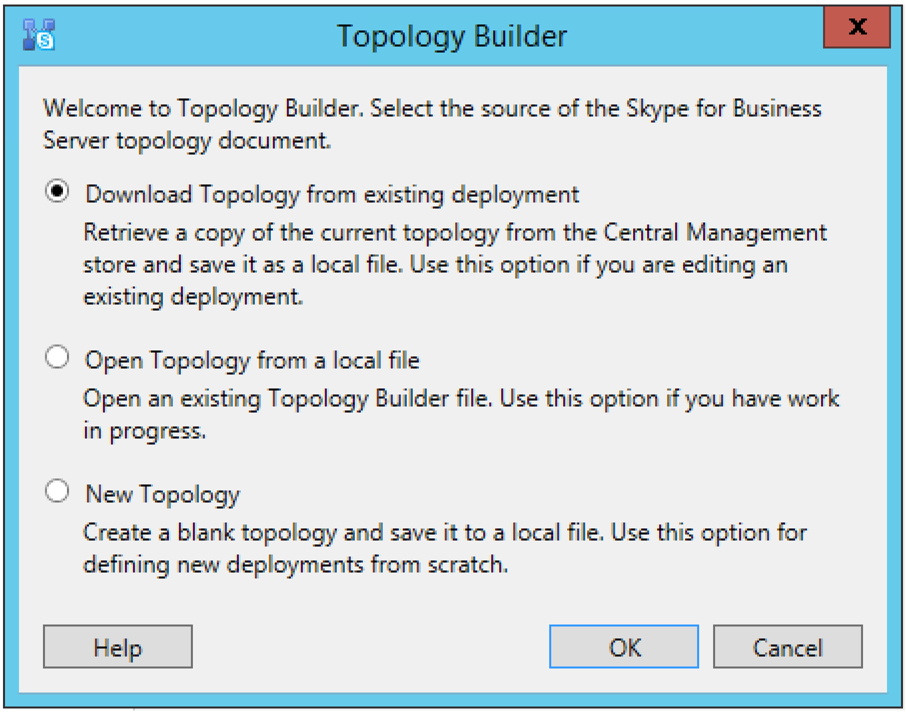
1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

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



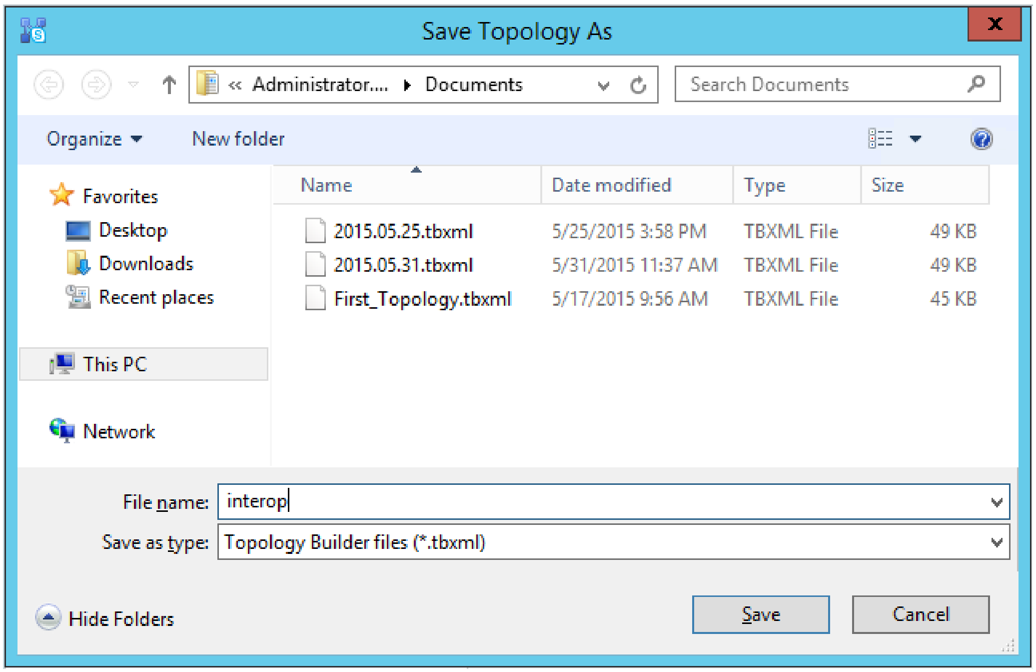
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

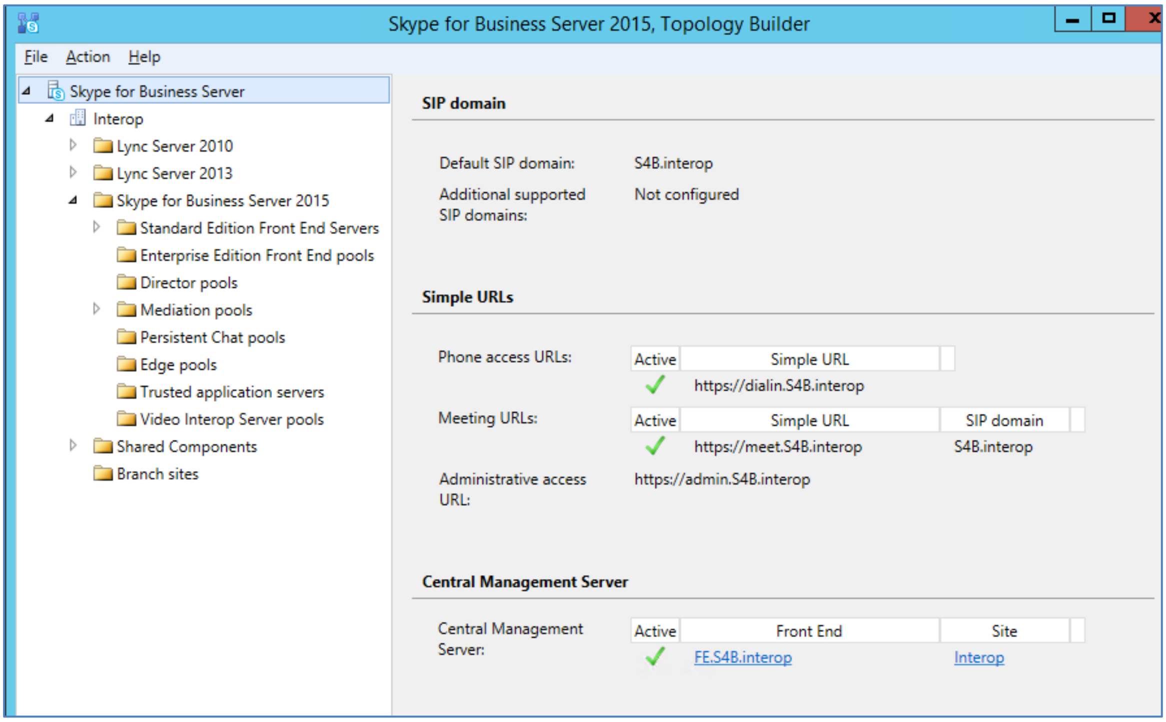
Figure 3-3: Save Topology Dialog Box



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

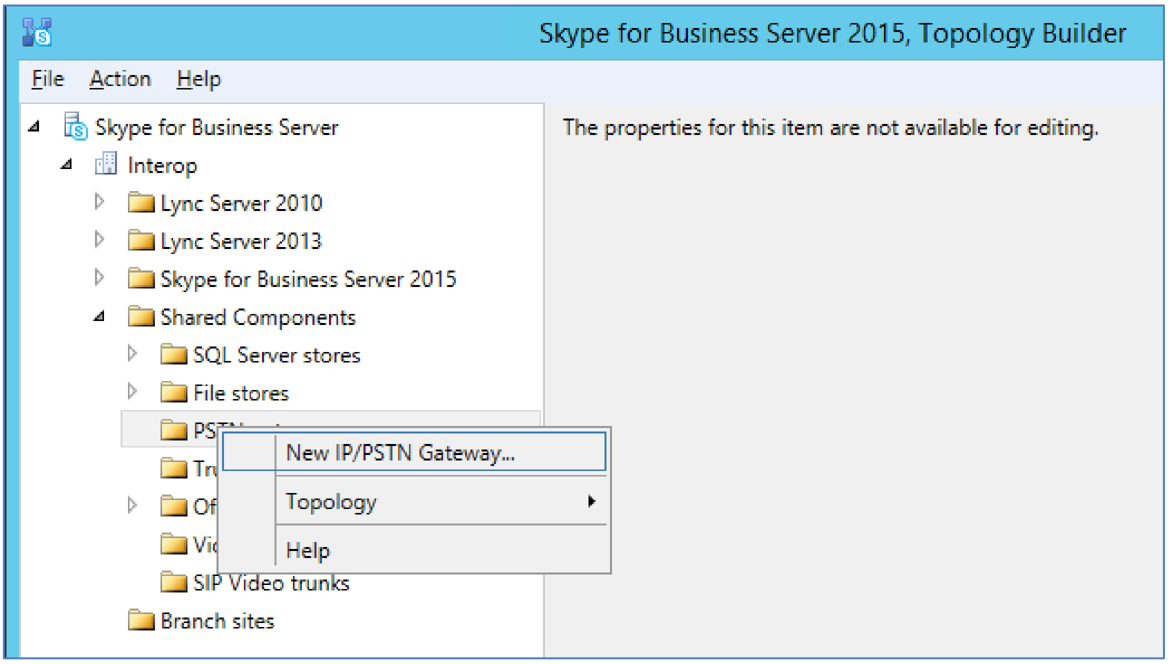
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



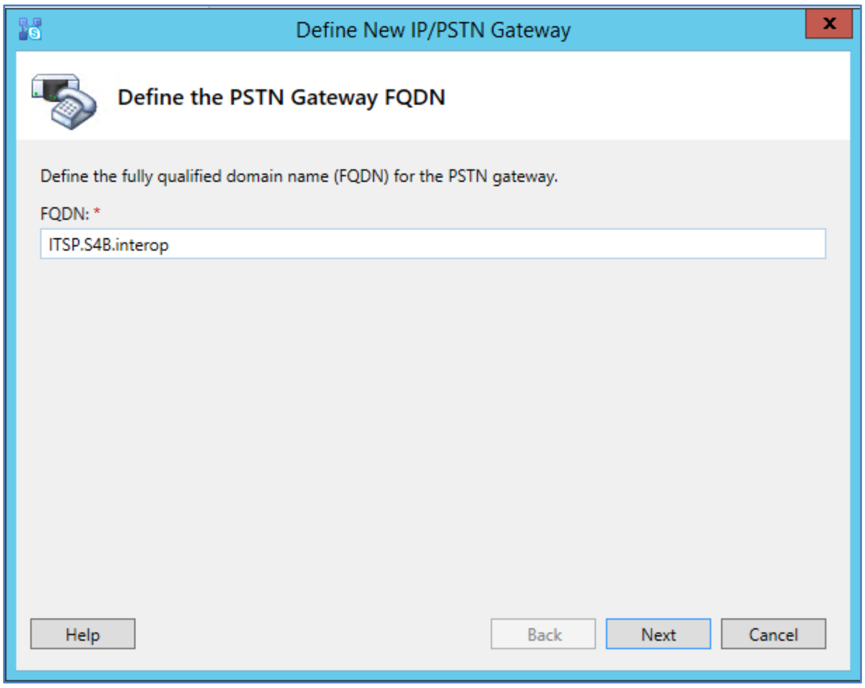
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



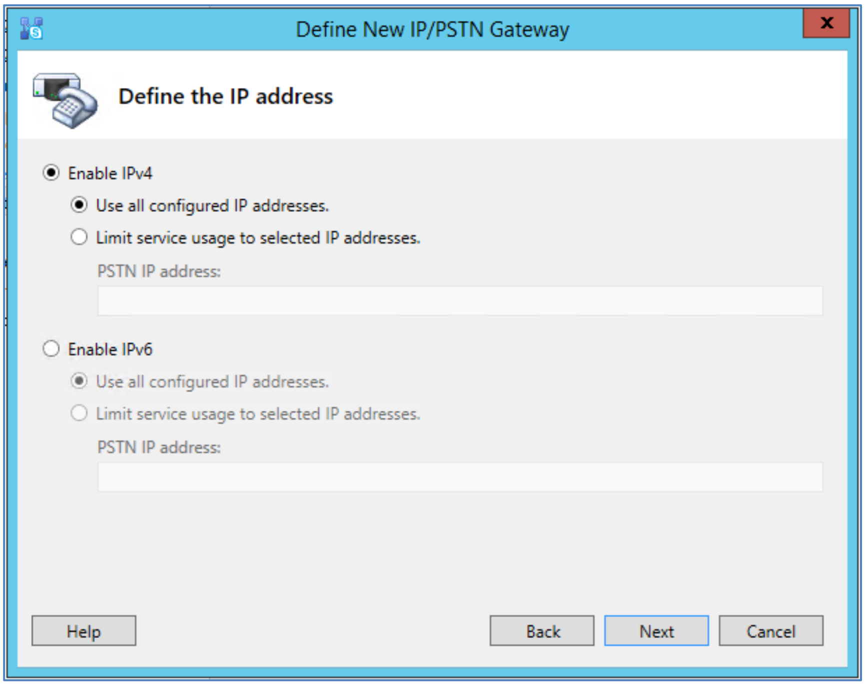
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP.S4B.interop**). Update this FQDN in the relevant DNS record, and then click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



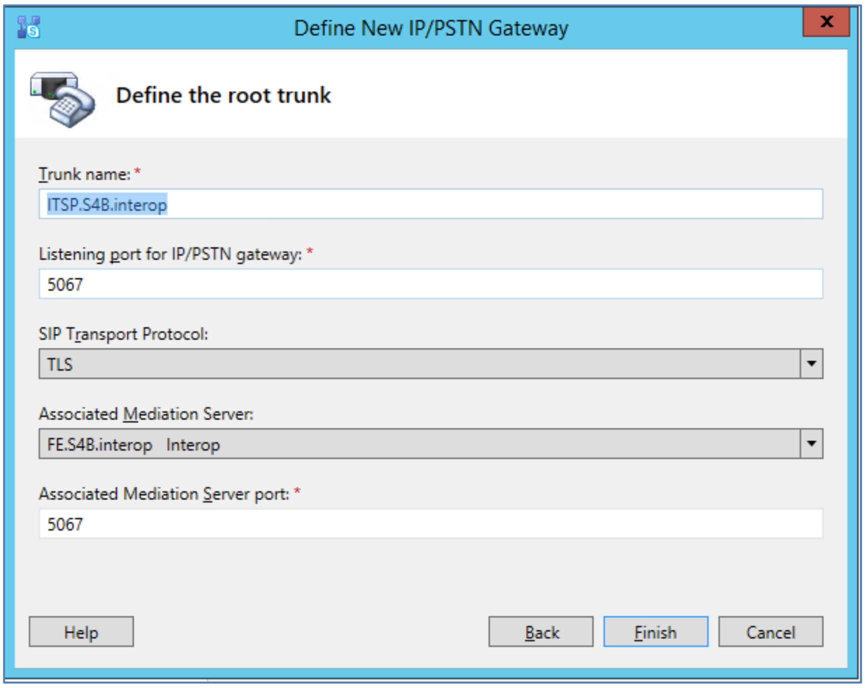
6. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

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

Notes:

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

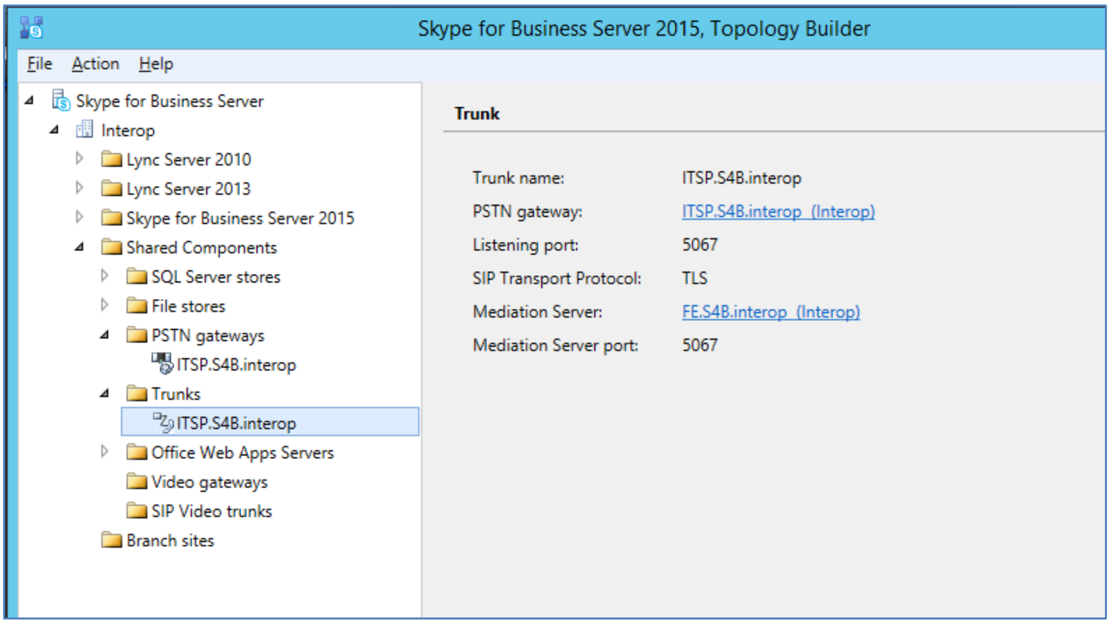
Figure 3-8: Define the Root Trunk



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

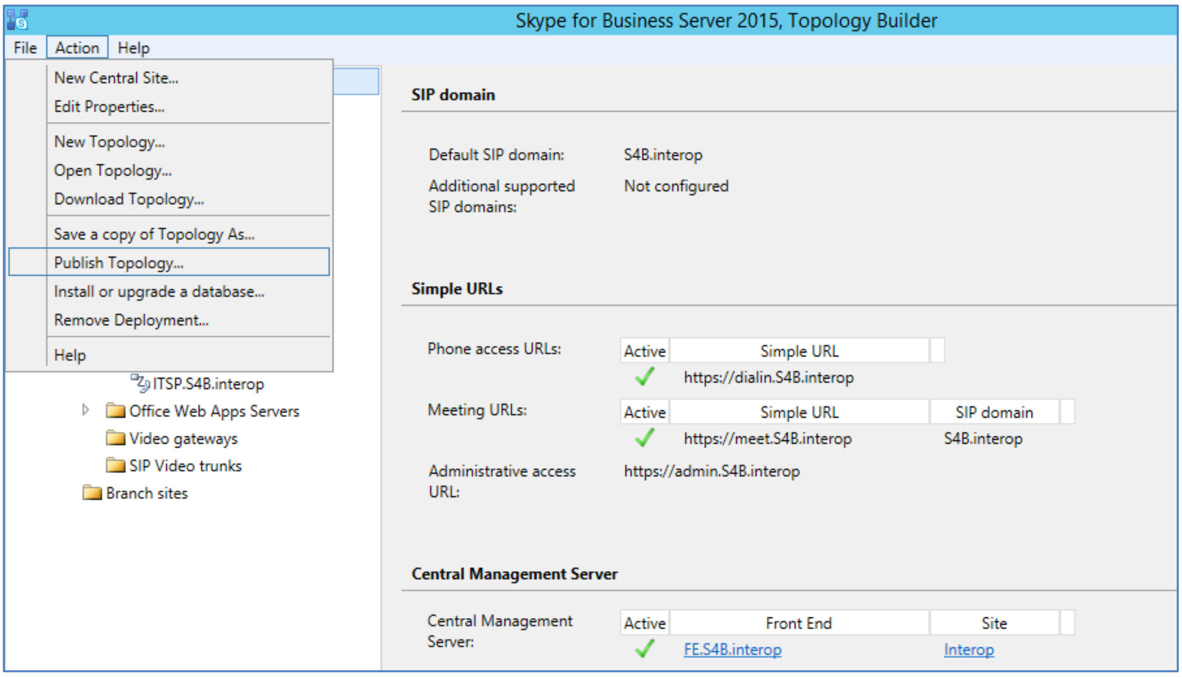
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



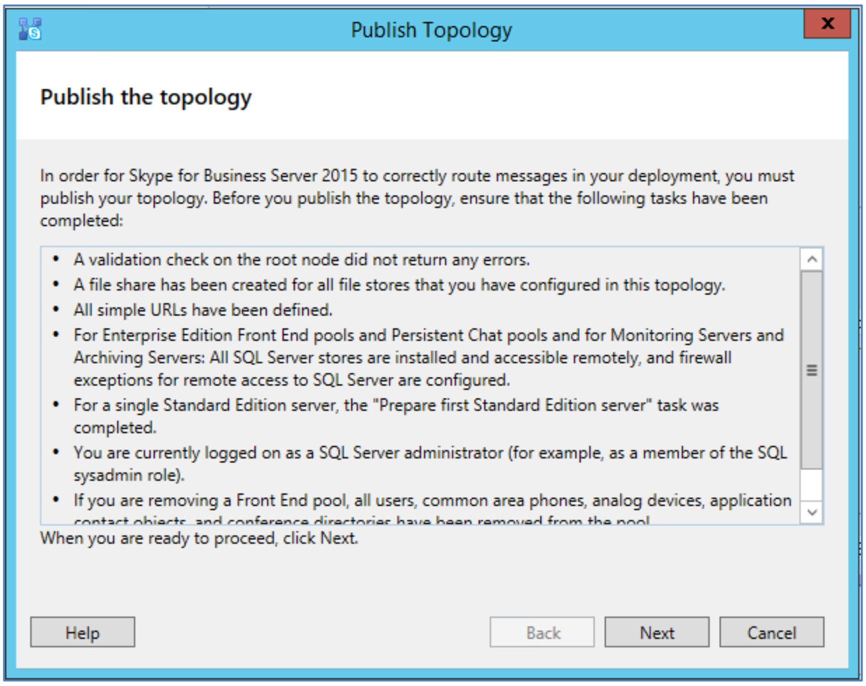
8. Publish the Topology In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



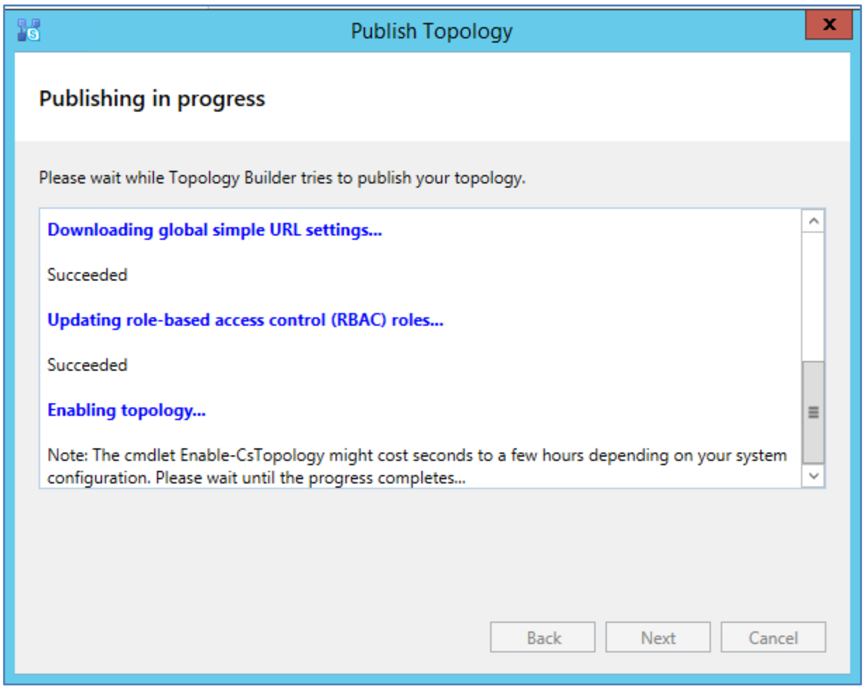
The following is displayed:

Figure 3-11: Publish the Topology



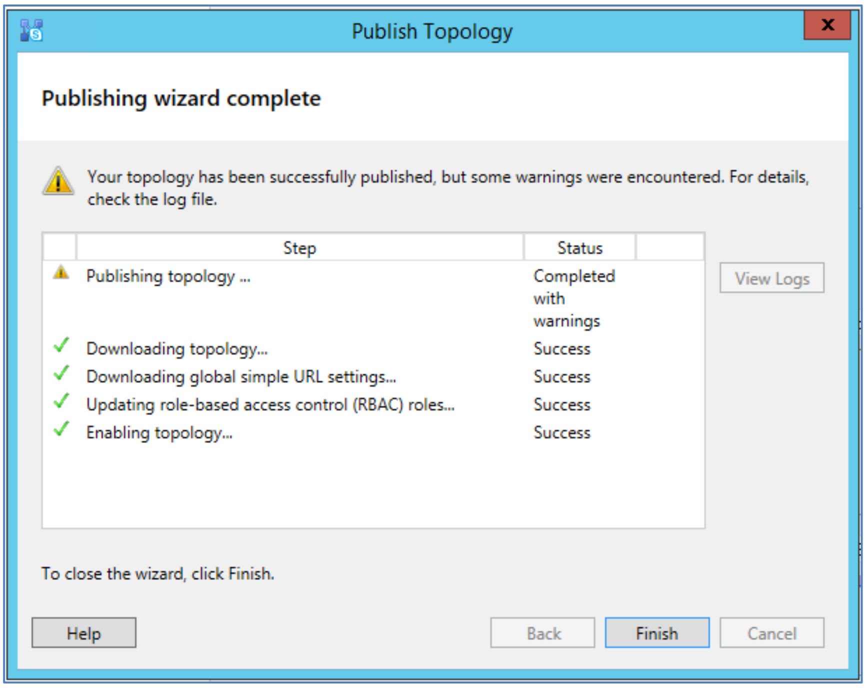
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. Click **Finish**.

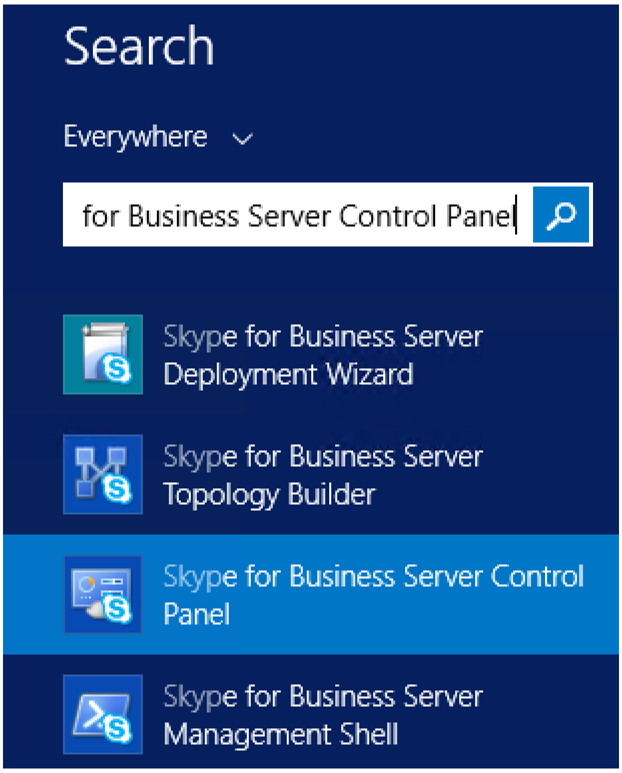
3.2 Configuring the "Route" on Skype for Business Server 2015

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:**

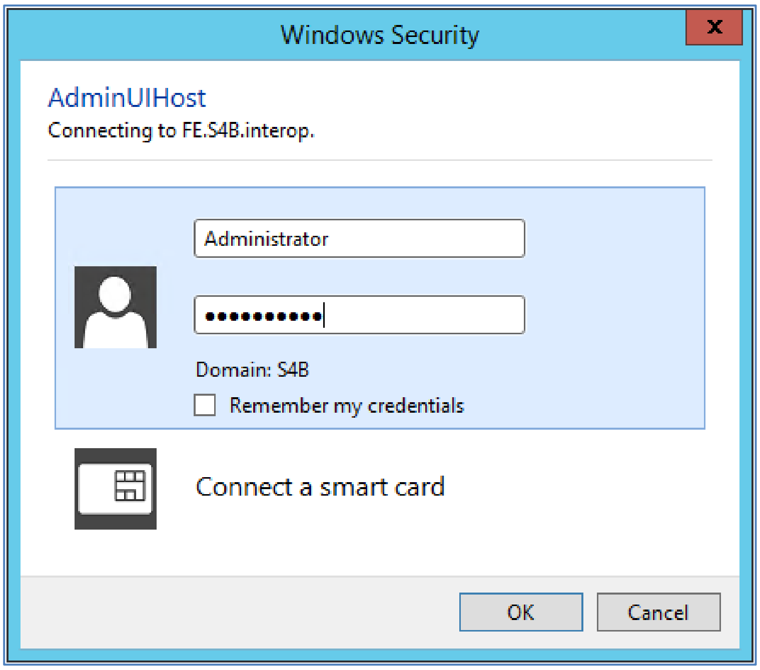
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

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



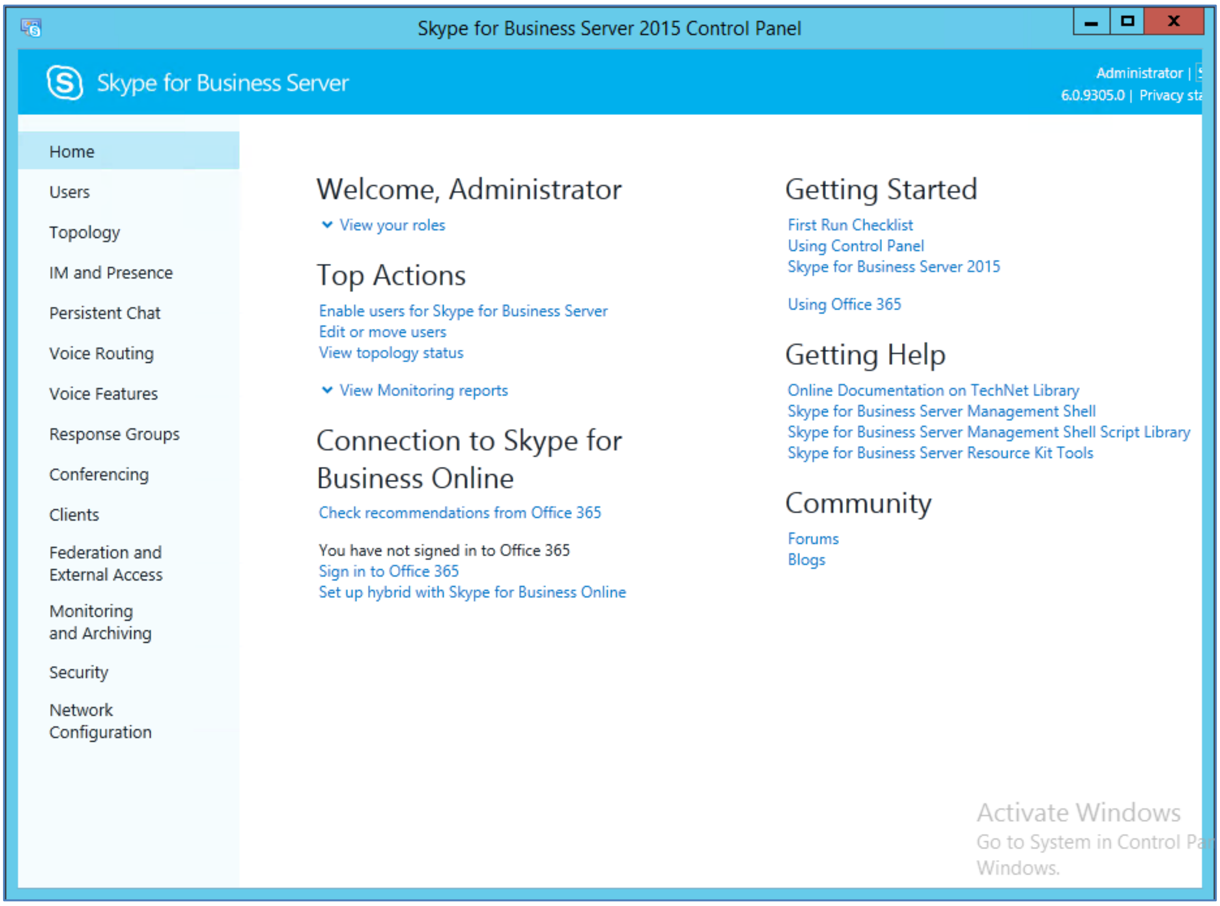
2. You are prompted to enter your login credentials:

Figure 3-15: Skype for Business Server Credentials



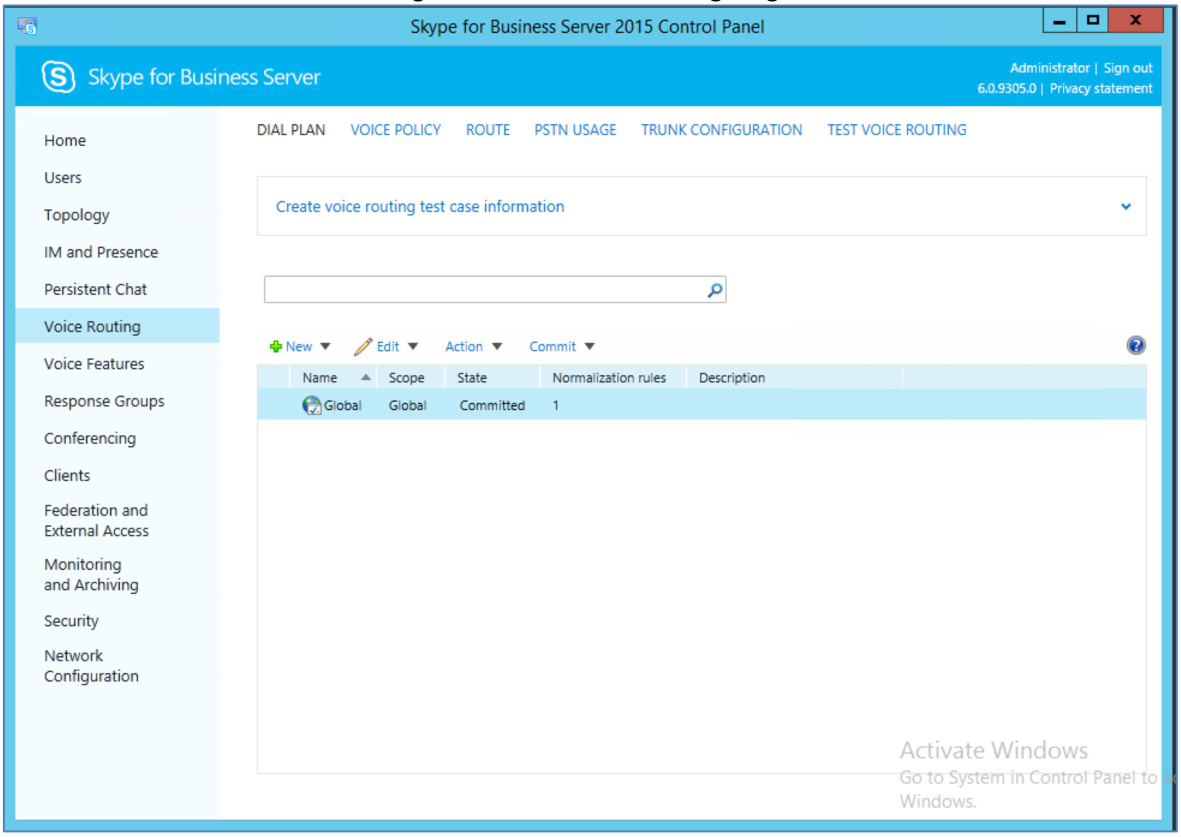
3. Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

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



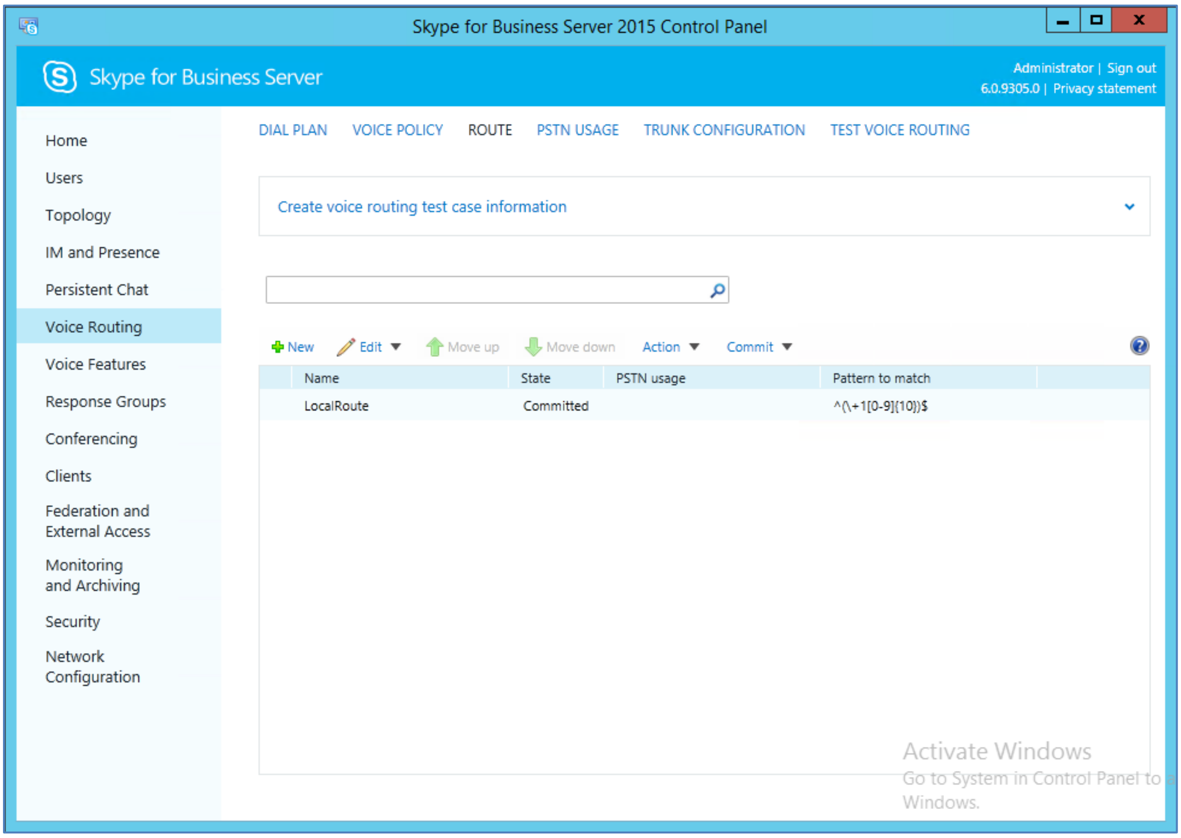
4. In the left navigation pane, select **Voice Routing**.

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



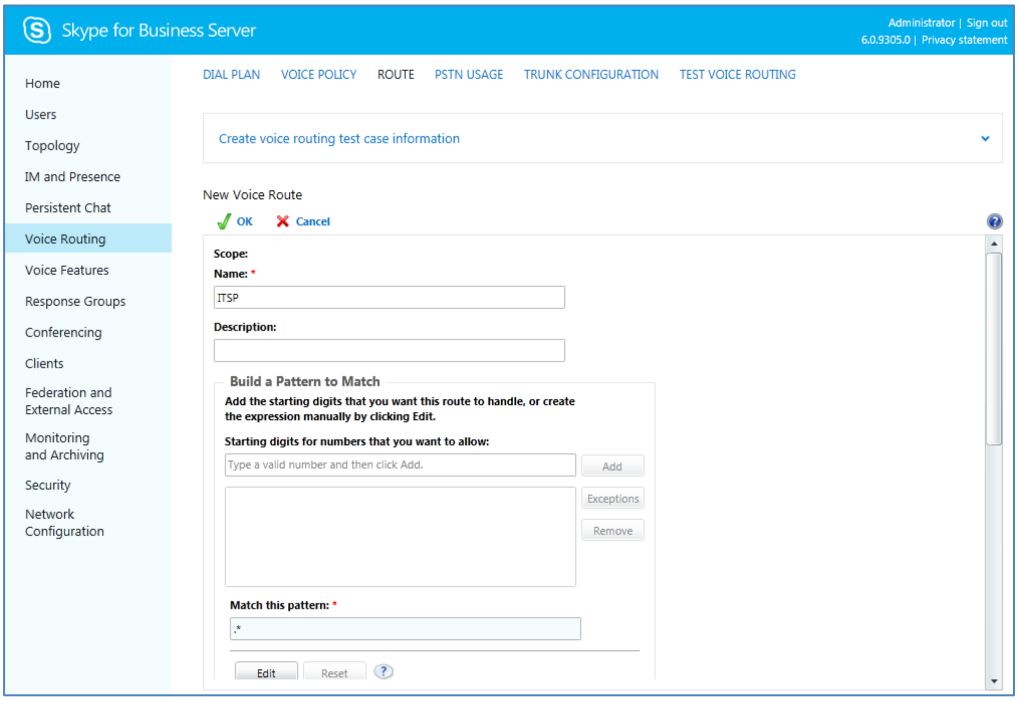
5. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



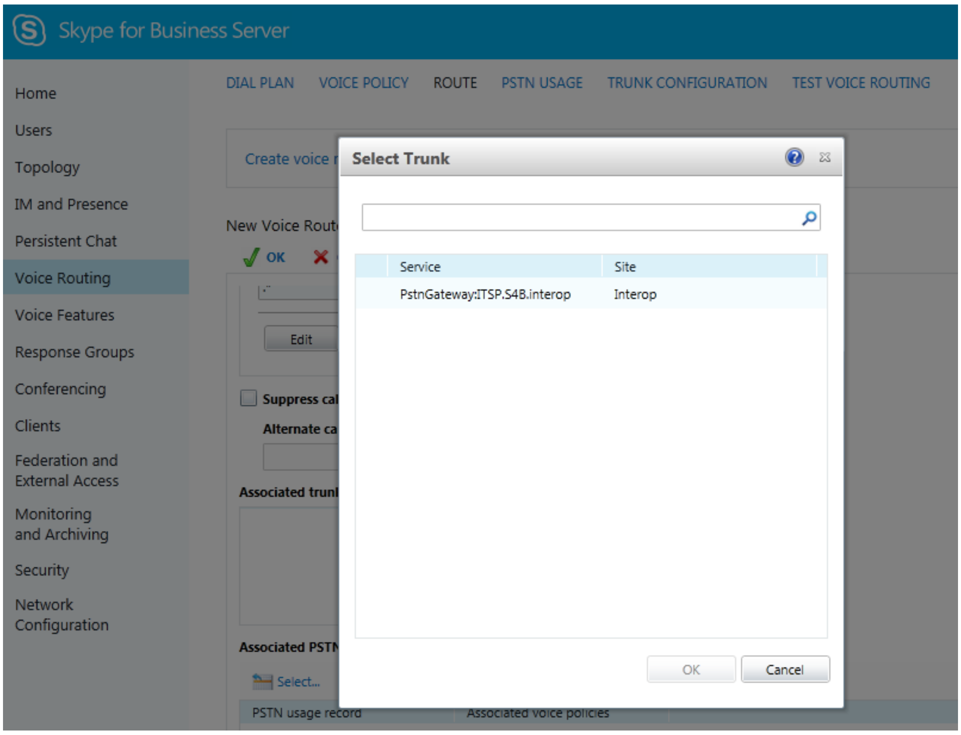
6. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



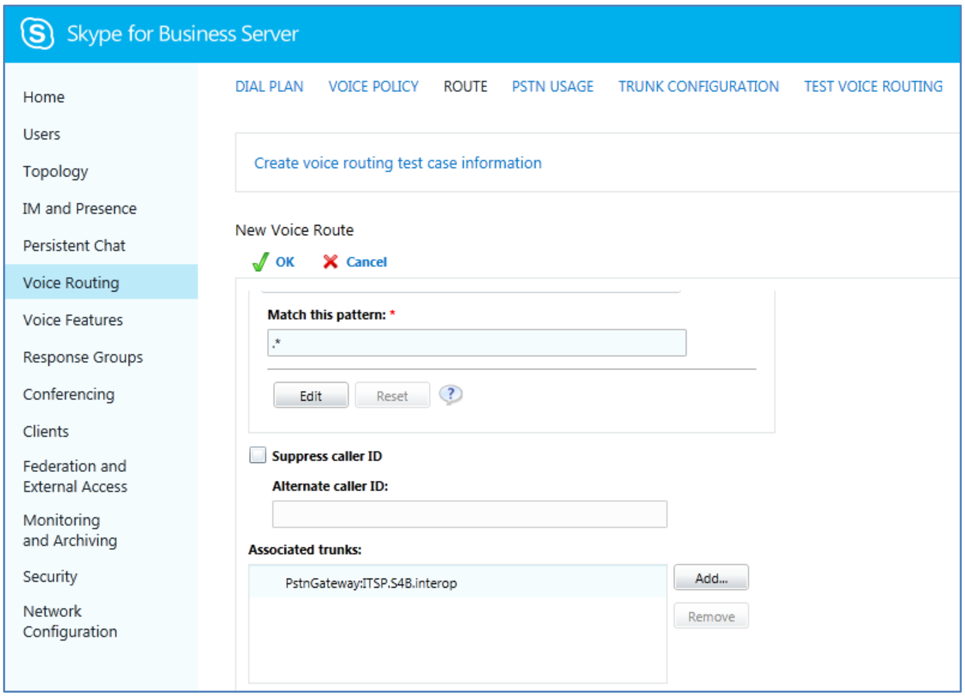
7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).
8. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.
9. Associate the route with the E-SBC Trunk that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

Figure 3-20: List of Deployed Trunks



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

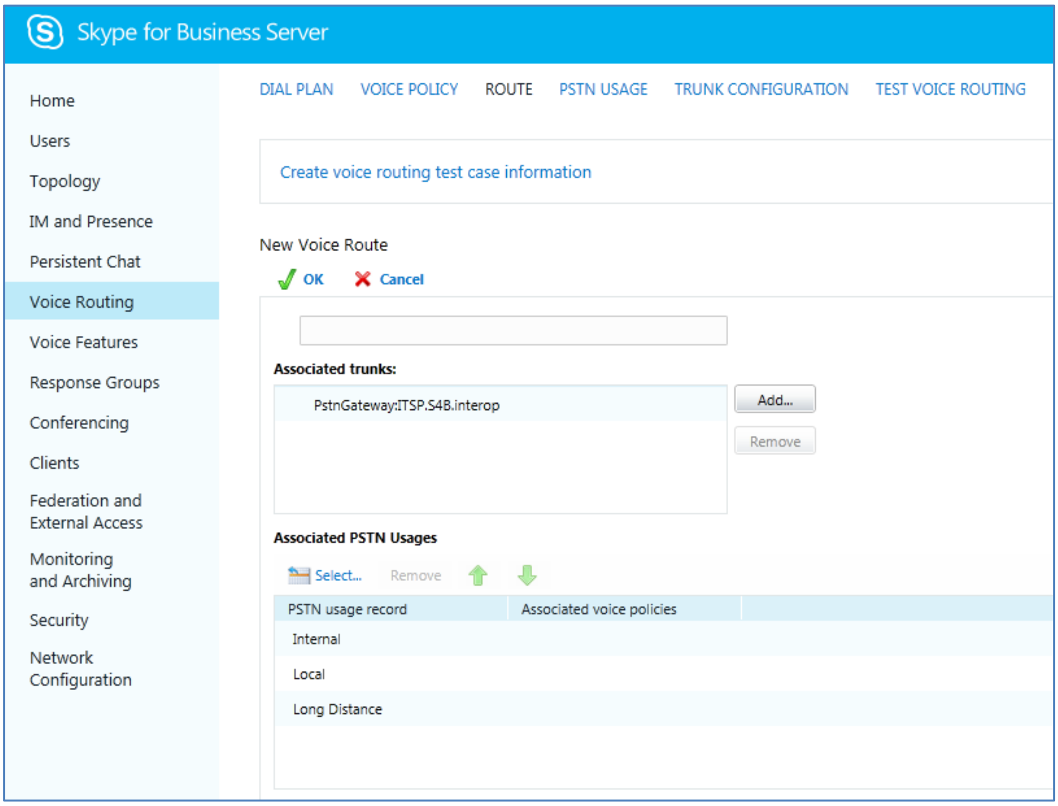
Figure 3-21: Selected E-SBC Trunk



10. Associate a PSTN Usage to this route:

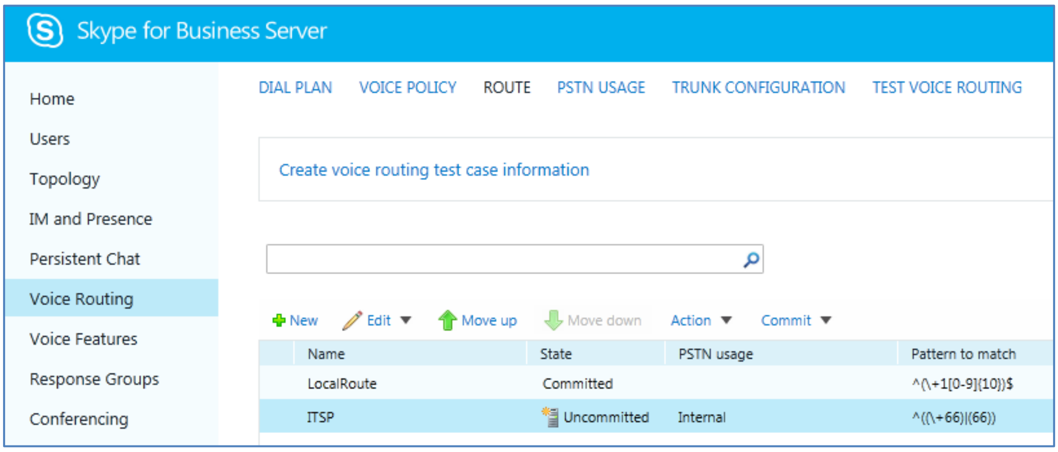
a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-22: Associating PSTN Usage to Route



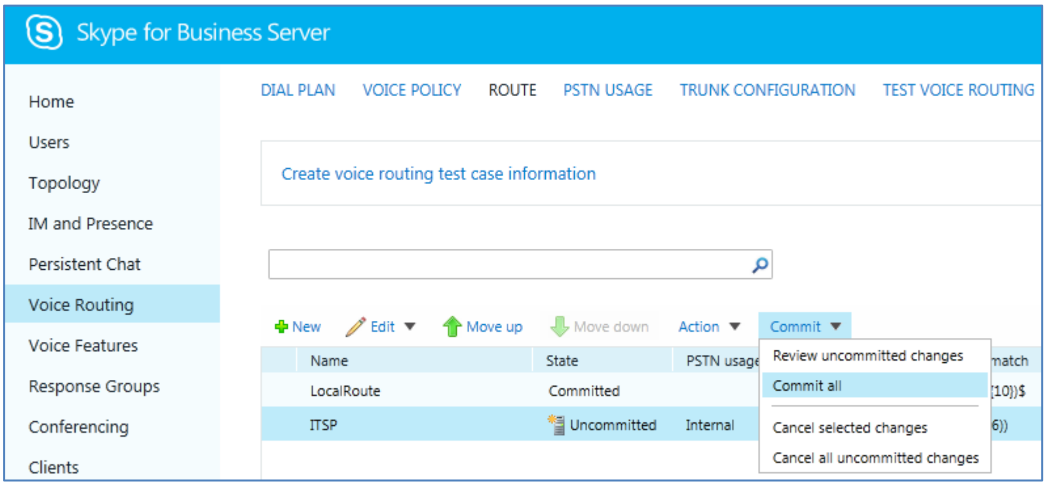
11. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-23: Confirmation of New Voice Route



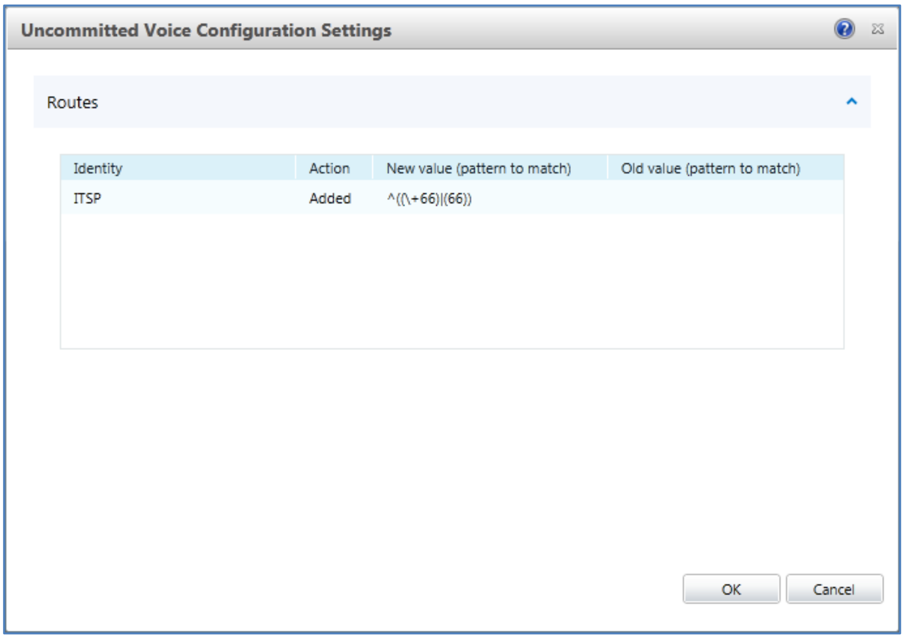
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-24: Committing Voice Routes



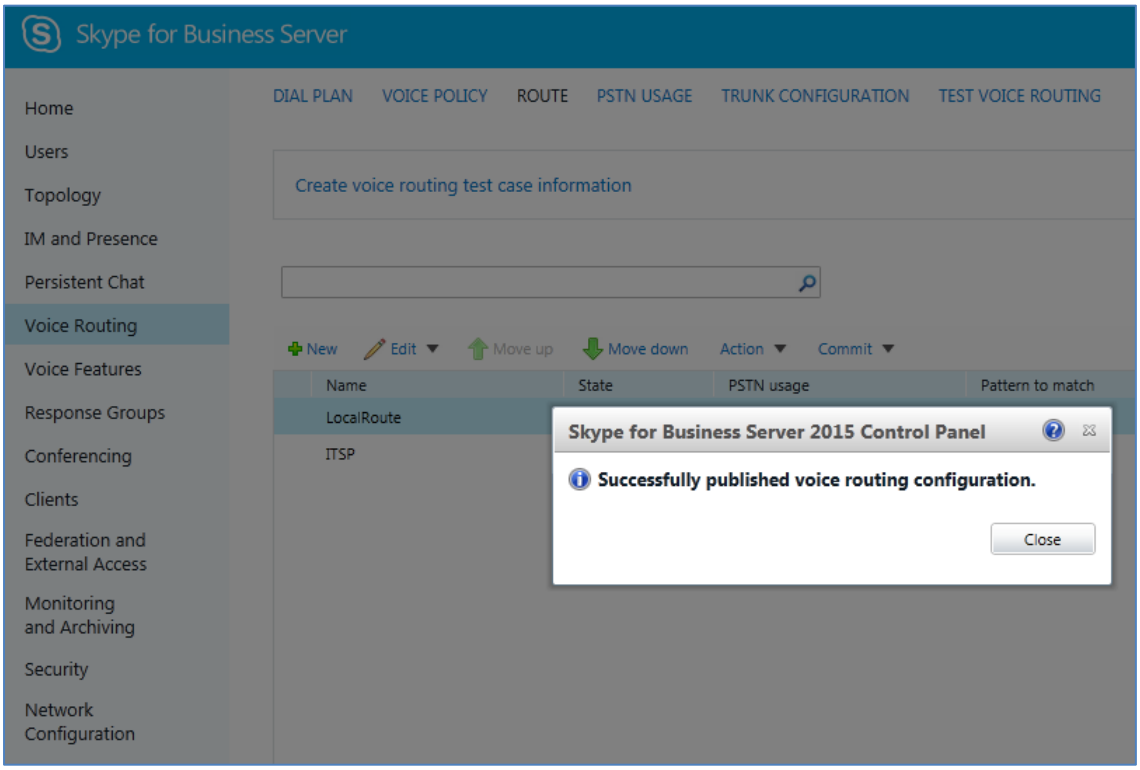
The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



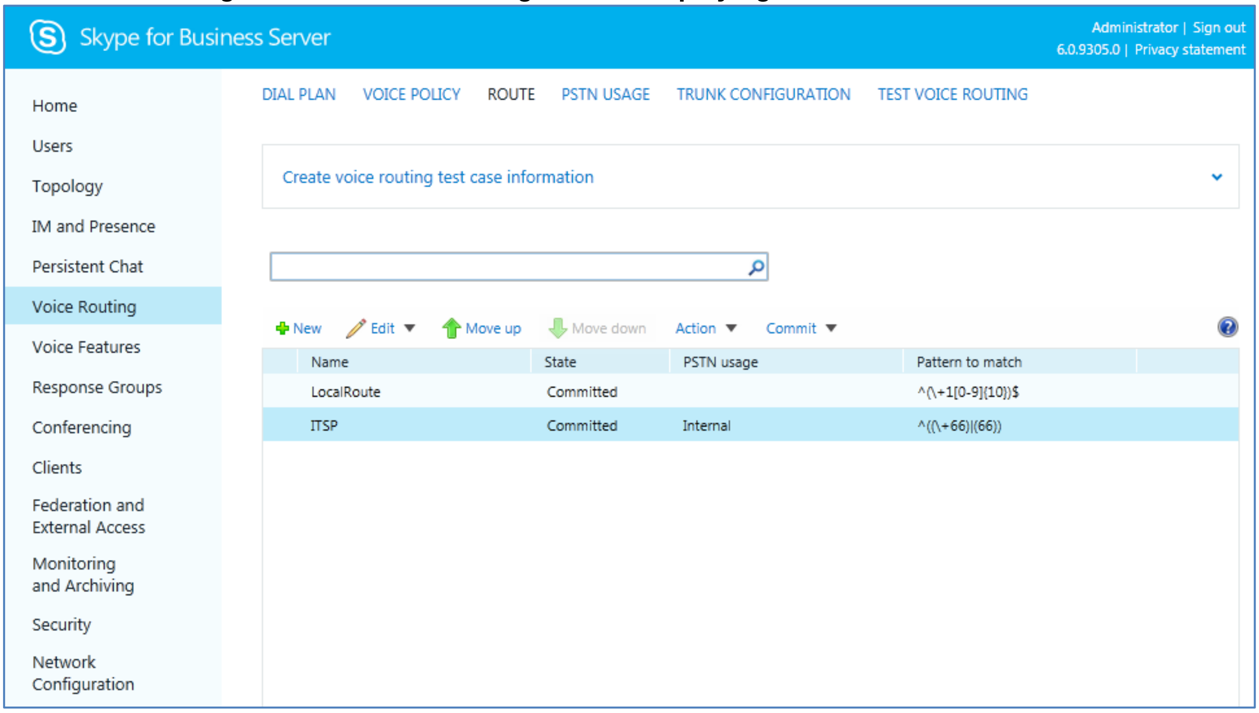
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-26: Confirmation of Successful Voice Routing Configuration



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

Figure 3-27: Voice Routing Screen Displaying Committed Routes

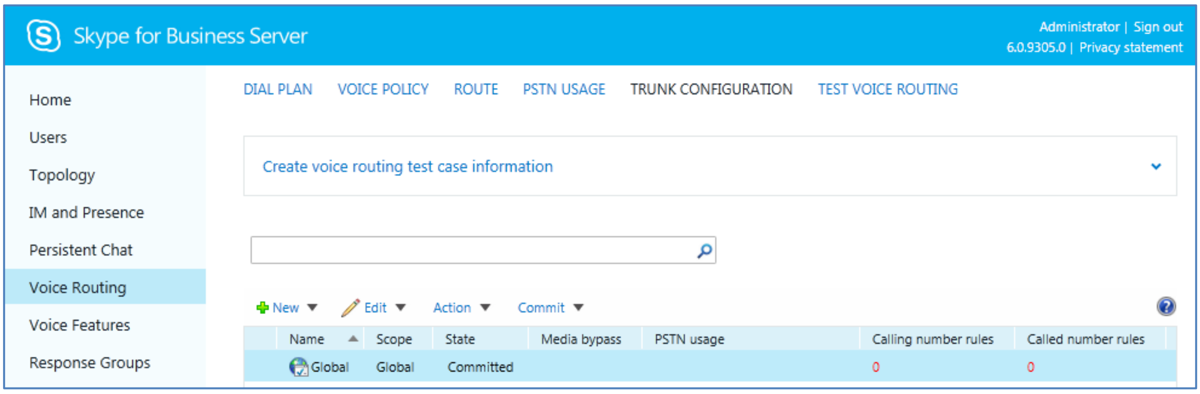


15. For ITSPs that implement a call identifier, continue with the following steps:

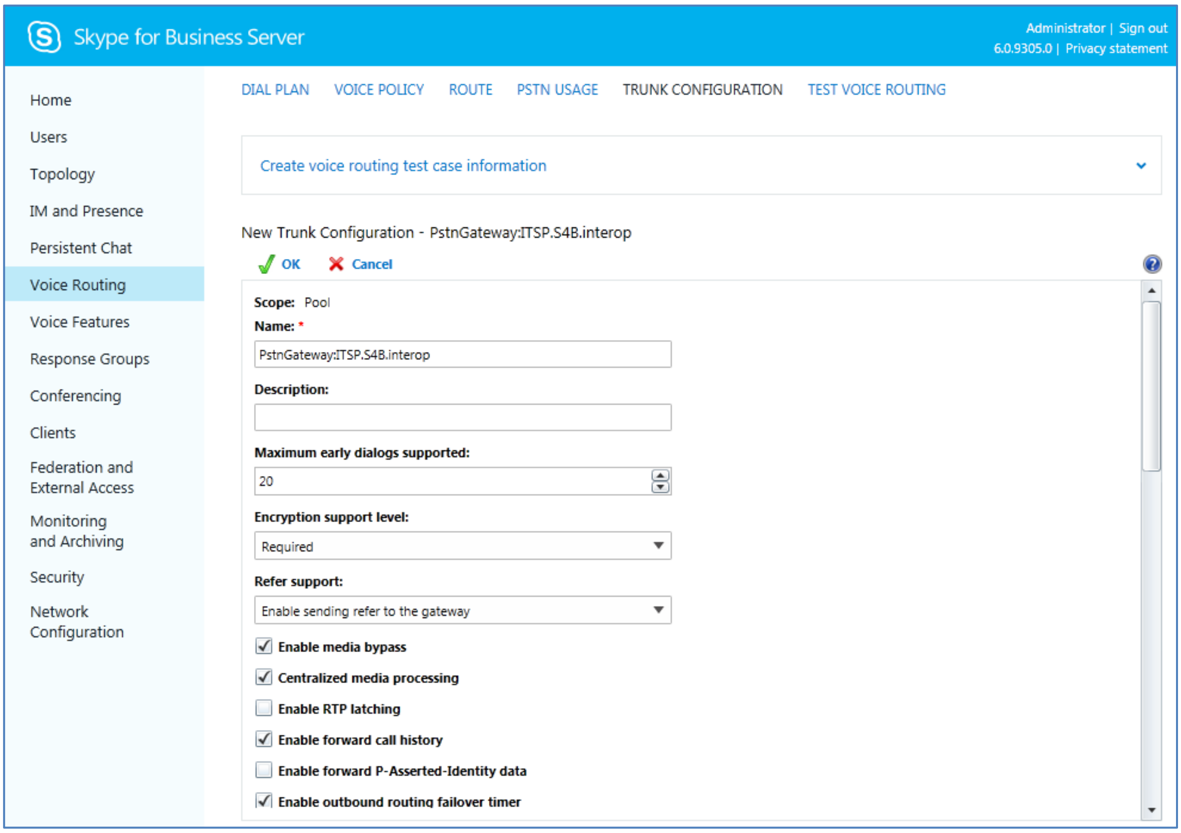
> **Note:** The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the S4B user number). This ID is required by Polkomtel SIP Trunk in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 4.6 on page 45).

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



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



c. Select the **Enable forward call history** check box, and then click **OK**.

d. Repeat Steps 11 through 13 to commit your settings.

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Skype for Business Server 2015 and the Polkomtel SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

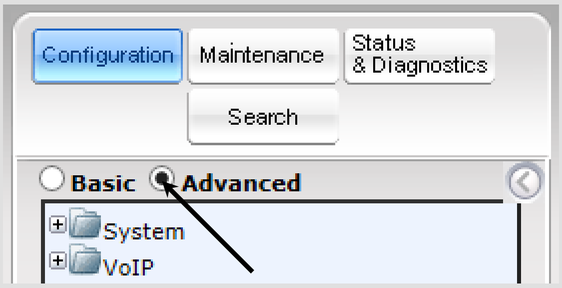
- E-SBC WAN interface - Polkomtel SIP Trunking environment
- E-SBC LAN interface - Skype for Business Server 2015 environment

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 Polkomtel SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
  - √ **Microsoft**
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

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



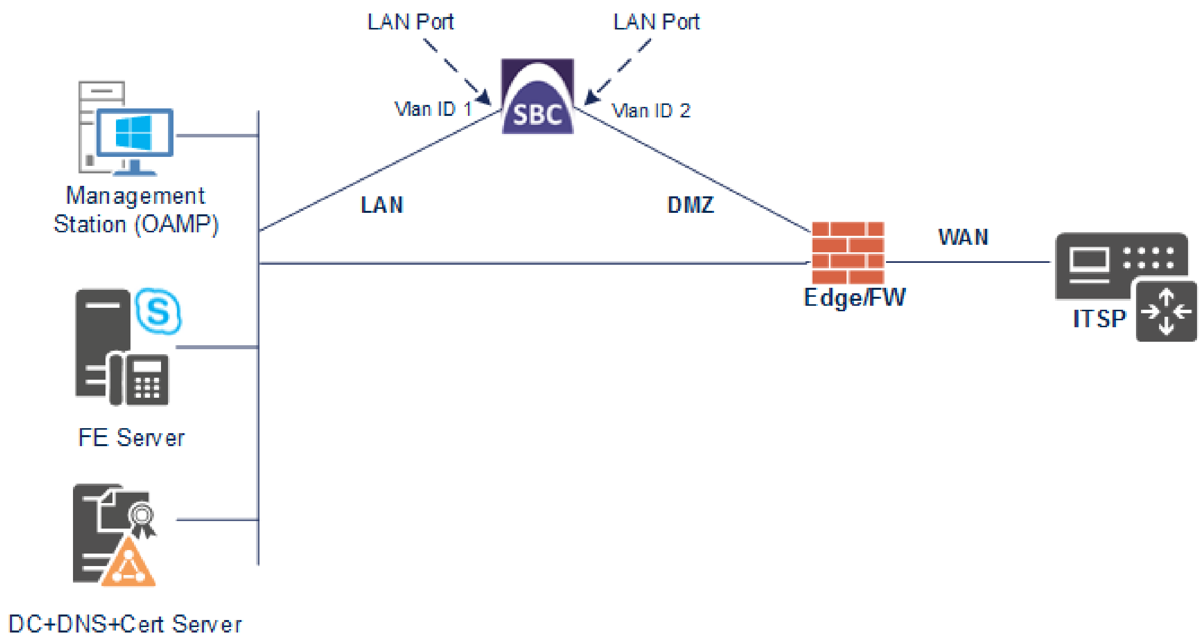
- Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

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

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

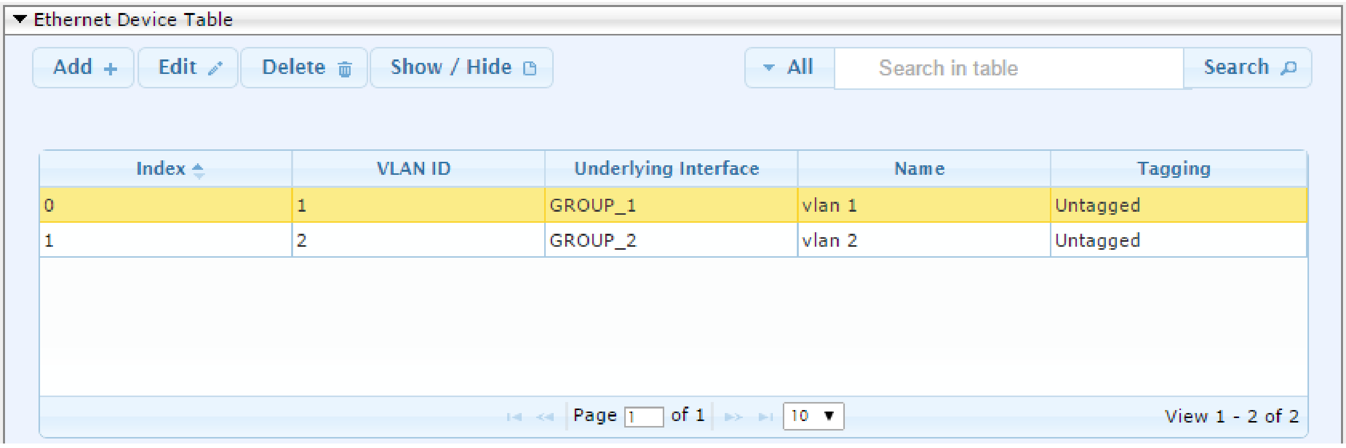
- LAN VoIP (assigned the name "Voice")
- WAN VoIP (assigned the name "WANSP")

➢ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side as follows:

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

Figure 4-2: Configured VLAN IDs in Ethernet Device Table



4.1.2 Step 1b: Configure Network Interfaces

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

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

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

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

Parameter	Value
IP Address	**10.15.17.55** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Default Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.27.1**
Underlying Device	**vlan 1**

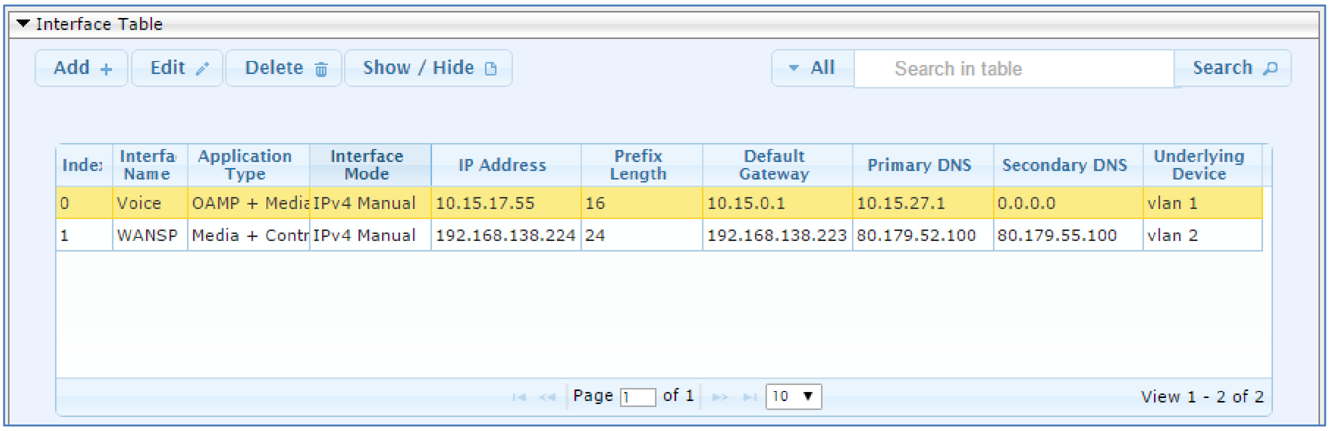
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**192.168.138.223** (WAN IP address)
Prefix Length	**25** (for 255.255.255.128)
Default Gateway	**192.168.138.224** (router's IP address)
VLAN ID	**2**
Interface Name	**WANSP**
Primary DNS Server IP Address	**80.179.52.100**
Secondary DNS Server IP Address	**80.179.55.100**
Underlying Device	**vlan 2**

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

The configured IP network interfaces are shown below:

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



Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	Voice	OAMP + Media	IPv4 Manual	10.15.17.55	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WANSP	Media + Contr	IPv4 Manual	192.168.138.224	24	192.168.138.223	80.179.52.100	80.179.55.100	vlan 2

4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-4: Enabling SBC Application

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.17 on page 88).

4.3 Step 3: Configure Media Realms

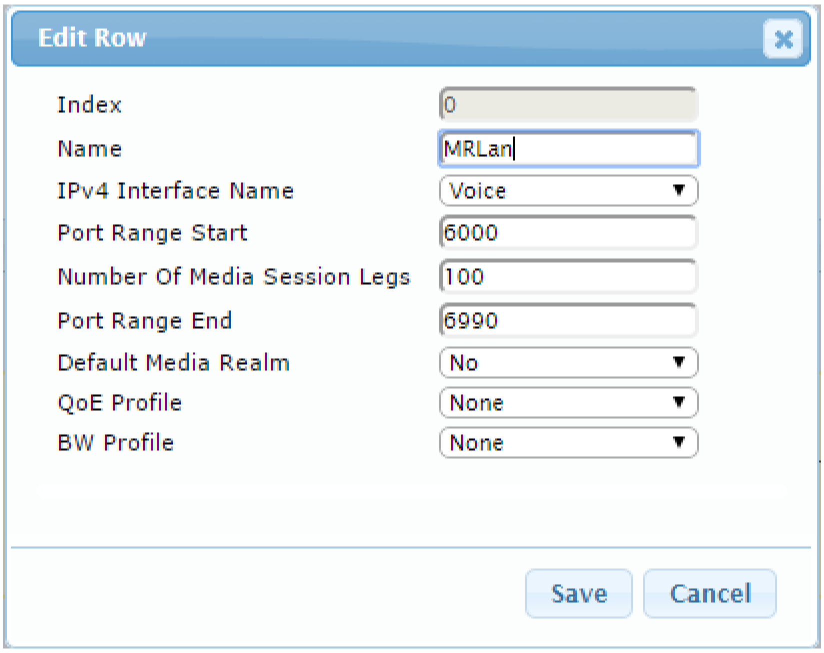
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

Parameter	Value
Index	**0**
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)

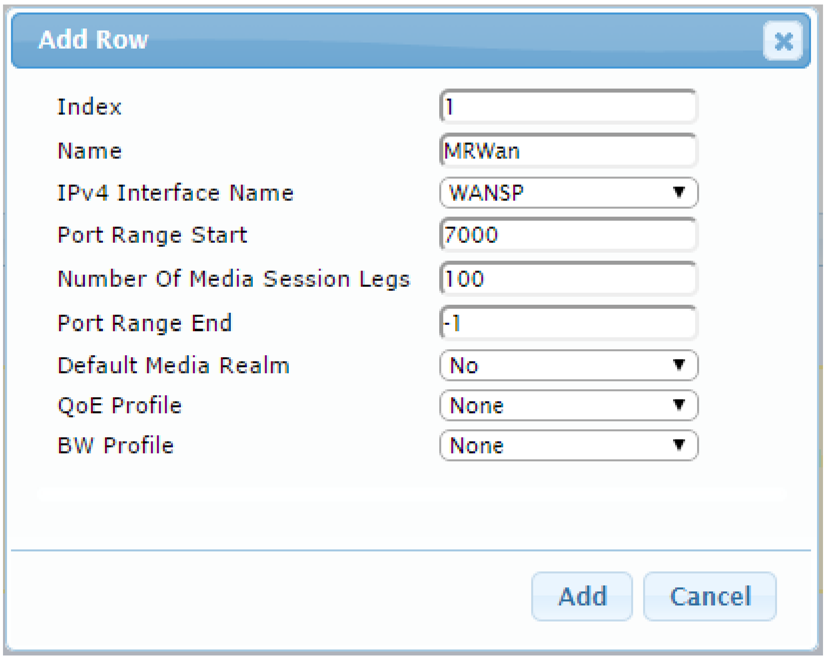
Figure 4-5: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

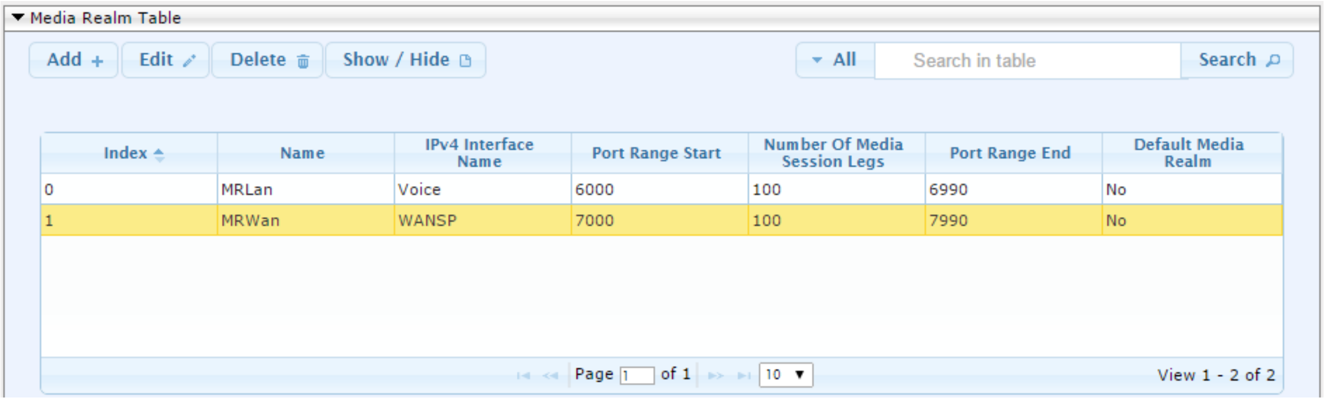
Parameter	Value
Index	**1**
Media Realm Name	**MRWan** (arbitrary name)
IPv4 Interface Name	**WANSP**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

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



4.4 Step 4: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Add a SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

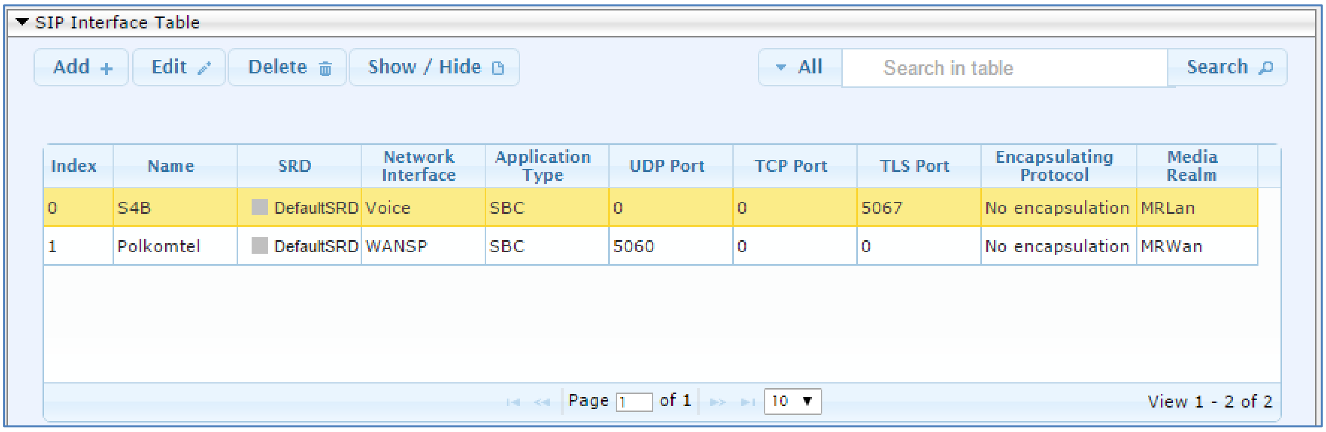
Parameter	Value
Index	**0**
Interface Name	**S4B** (see Note below)
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
Media Realm	**MRLan**

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	**1**
Interface Name	**Polkomtel** (see Note below)
Network Interface	**WANSP**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	**0**
Media Realm	**MRWan**

The configured SIP Interfaces are shown in the figure below:

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


SIP Interface Table

Add + | Edit | Delete | Show / Hide | All | Search in table | Search

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

Page 1 of 1 | 10 | View 1 - 2 of 2

Note: Unlike in previous software releases where configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups) were associated with each other using table row indices, Version 7.0 uses the string **names** of the configuration entities. Therefore, it is recommended to configure each configuration entity with meaningful names for easy identification.

4.5 Step 5: Configure Proxy Sets

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

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

- Microsoft Skype for Business Server 2015
- Polkomtel SIP Trunk

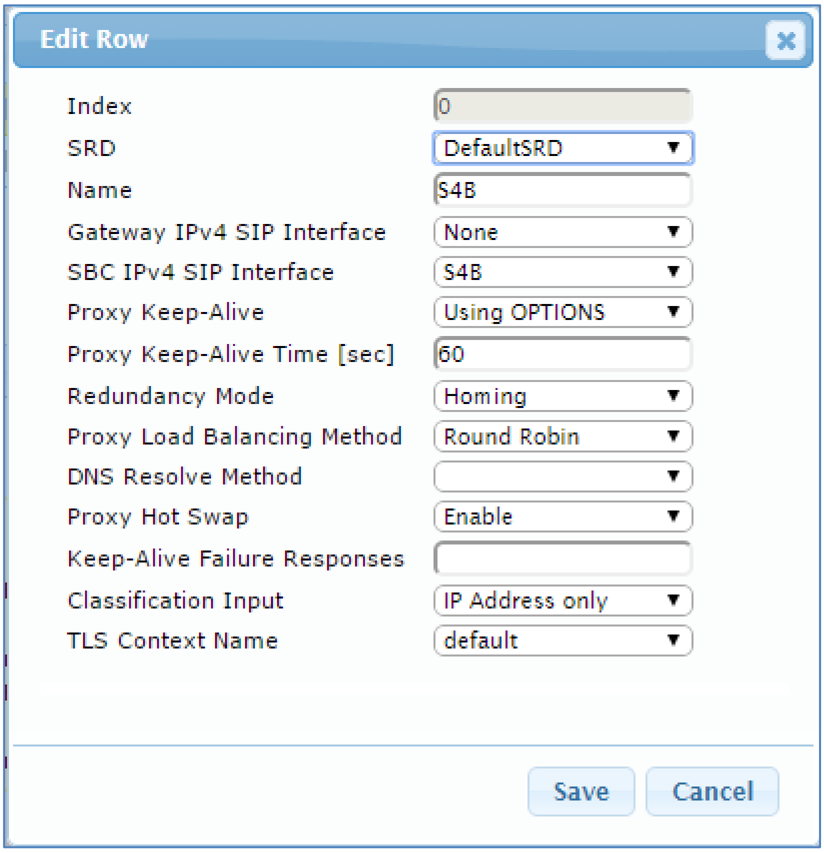
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➢ **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. You can use the default Proxy Set (Index 0), but modify it as shown below:

Parameter	Value
Proxy Set ID	**0**
Proxy Name	**S4B** (see Note on page 40)
SBC IPv4 SIP Interface	**S4B**
Proxy Keep Alive	**Using Options**
Redundancy Mode	**Homing**
Load Balancing Method	**Round Robin**
Proxy Hot Swap	**Enable**
TLS Context Name	**default**

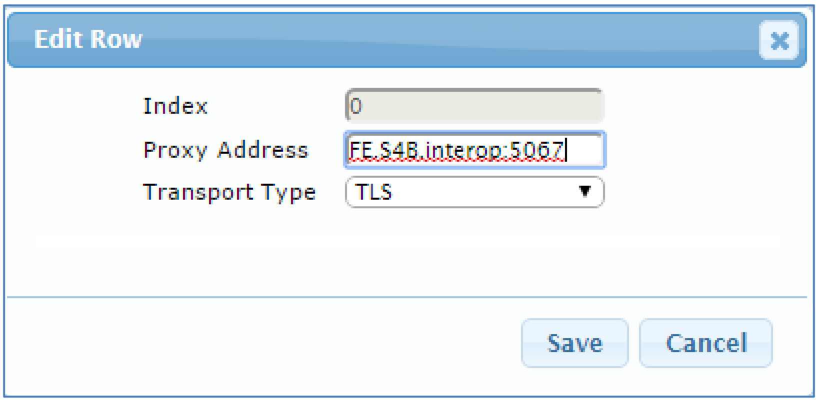
Figure 4-9: Configuring Proxy Set for Microsoft Skype for Business Server 2015



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

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

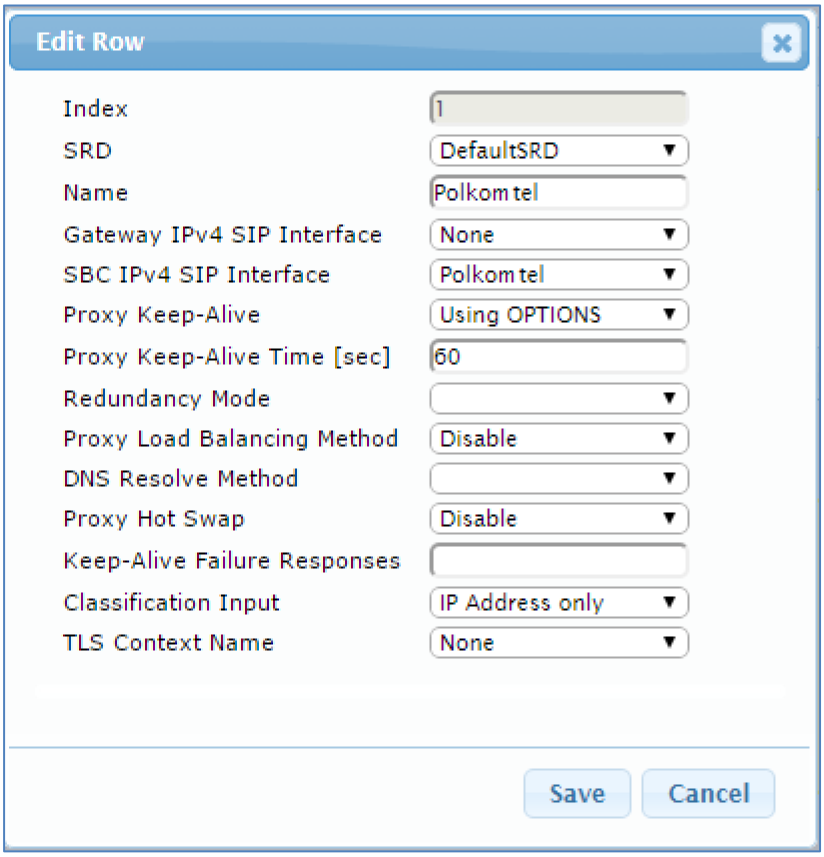
Figure 4-10: Configuring Proxy Address for Microsoft Skype for Business Server 2015



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

Parameter	Value
Proxy Set ID	**1**
Proxy Name	**Polkomtel** (see Note on page 40)
SBC IPv4 SIP Interface	**Polkomtel**
Proxy Keep Alive	**Using Options**

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

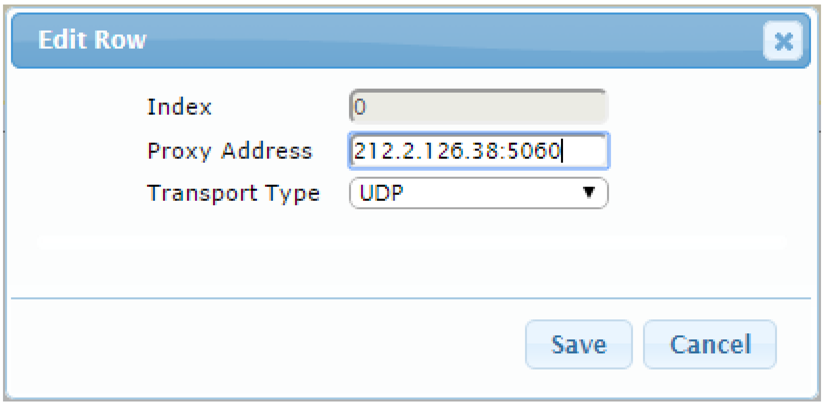


a. Configure a Proxy Address Table for Proxy Set 1:

b. Navigate to **Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table** > **Proxy Address Table**.

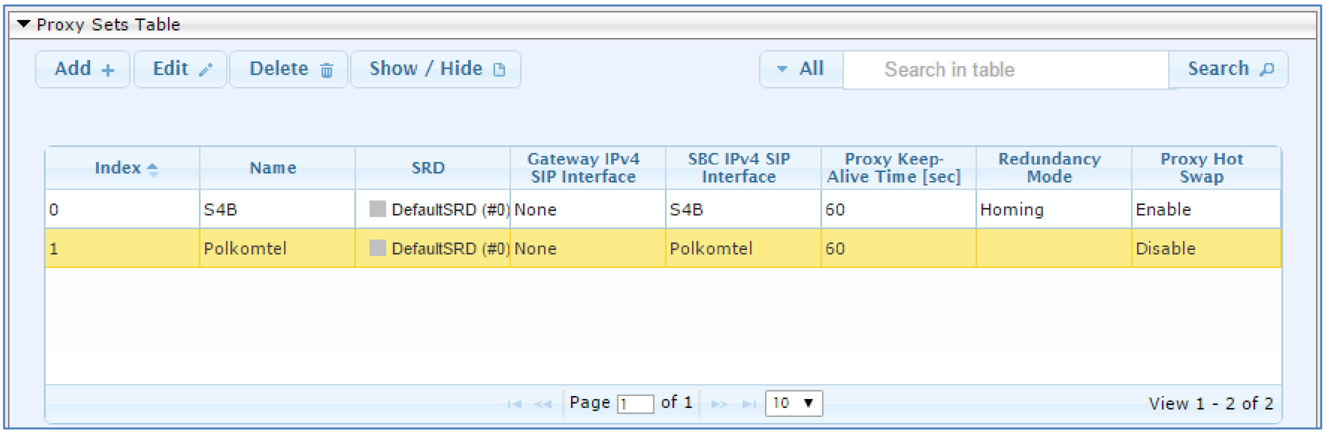
Parameter	Value
Index	**0**
Proxy Address	**212.2.126.38:5060** (IP address / FQDN and destination port)
Transport Type	**UDP**

Figure 4-12: Configuring Proxy Address for



The configured Proxy Sets are shown in the figure below:

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



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:

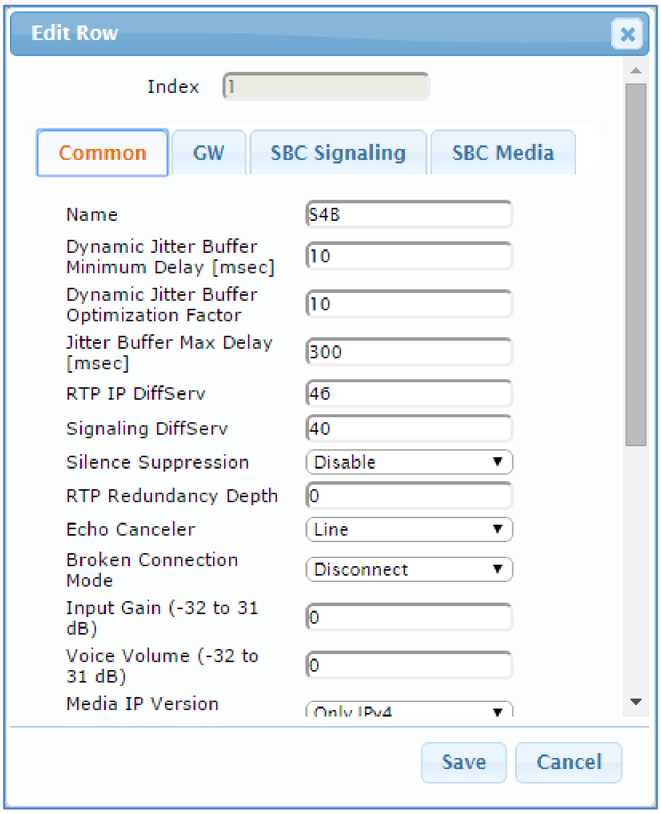
- **Microsoft Skype for Business Server 2015** - to operate in secure mode using SRTP and TLS
- **Polkomtel SIP trunk** - to operate in non-secure mode using RTP and UDP

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

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

Parameter	Value
Index	**1**
Name	**S4B** (see Note on page 40)
Symmetric MKI	**Enable**
MKI Size	**1**
Reset SRTP State Upon Re-key	**Enable**
Generate SRTP keys mode:	**Always**

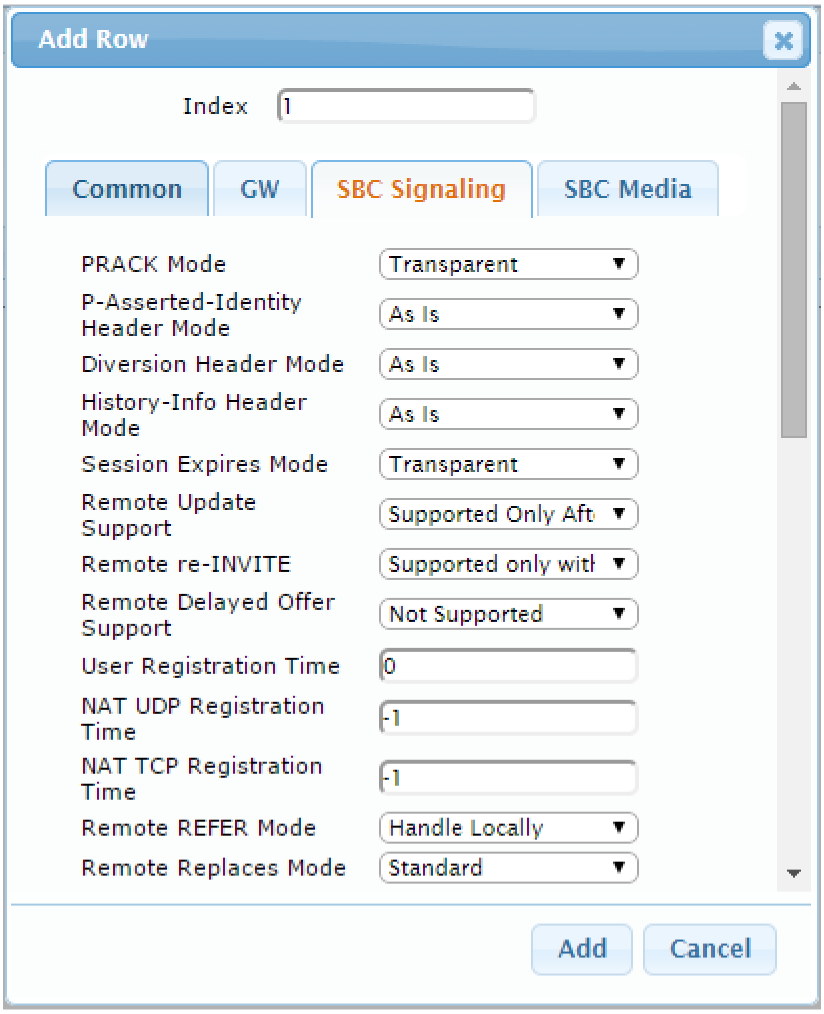
Figure 4-14: Configuring IP Profile for Skype for Business Server 2015 – Common Tab



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

Parameter	Value
Remote Update Support	**Supported Only After Connect**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
Remote REFER Mode	**Handle Locally** (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Remote 3xx Mode	**Handle Locally** (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)
Remote Early Media RTP Detection Behavior	**By Media** (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)

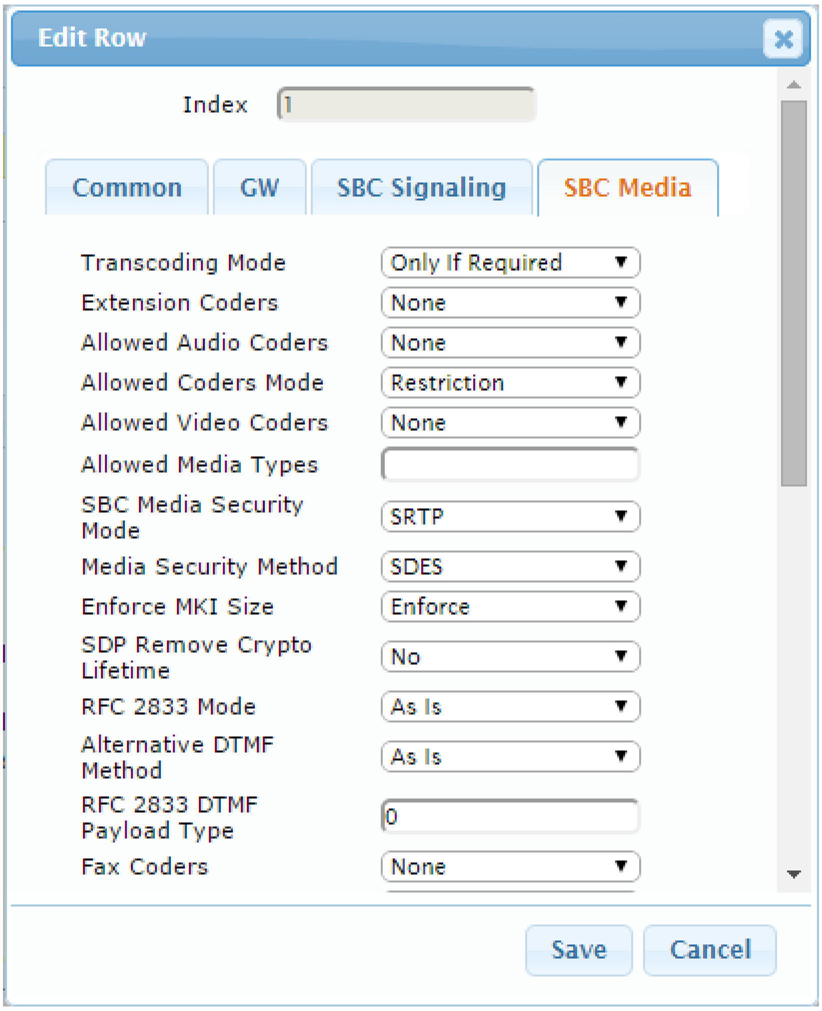
Figure 4-15: Configuring IP Profile for Skype for Business Server 2015 – SBC Signaling Tab



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

Parameter	Value
SBC Media Security Mode	**SRTP**
Enforce MKI Size	**Enforce**

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

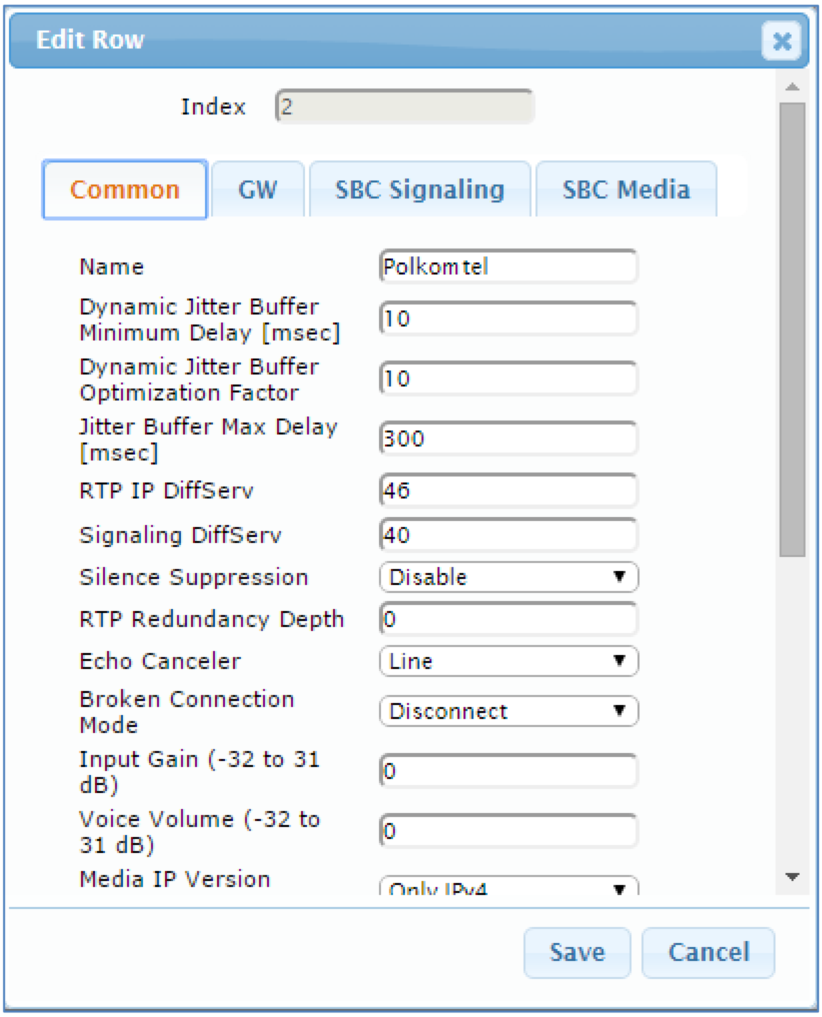


➢ **To configure an IP Profile for the Polkomtel SIP Trunk:**

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

Parameter	Value
Index	**2**
Profile Name	**Polkomtel** (see Note on page 40)

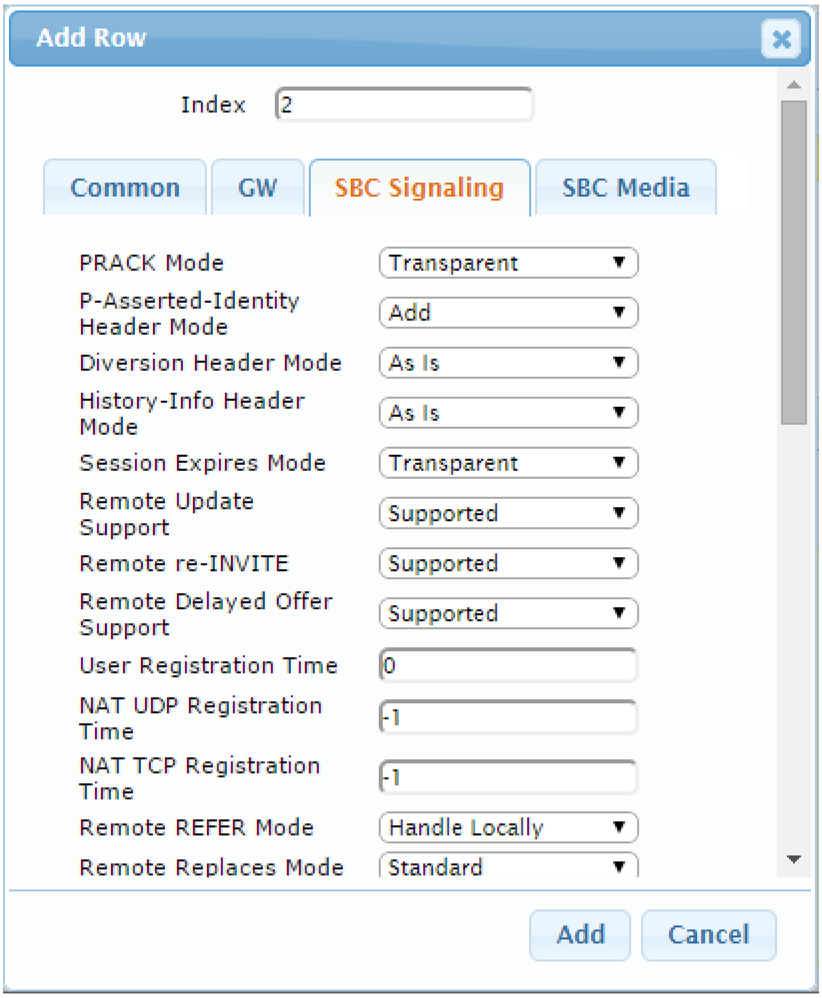
Figure 4-17: Configuring IP Profile for Polkomtel SIP Trunk – Common Tab



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

Parameter	Value
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Remote REFER Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)

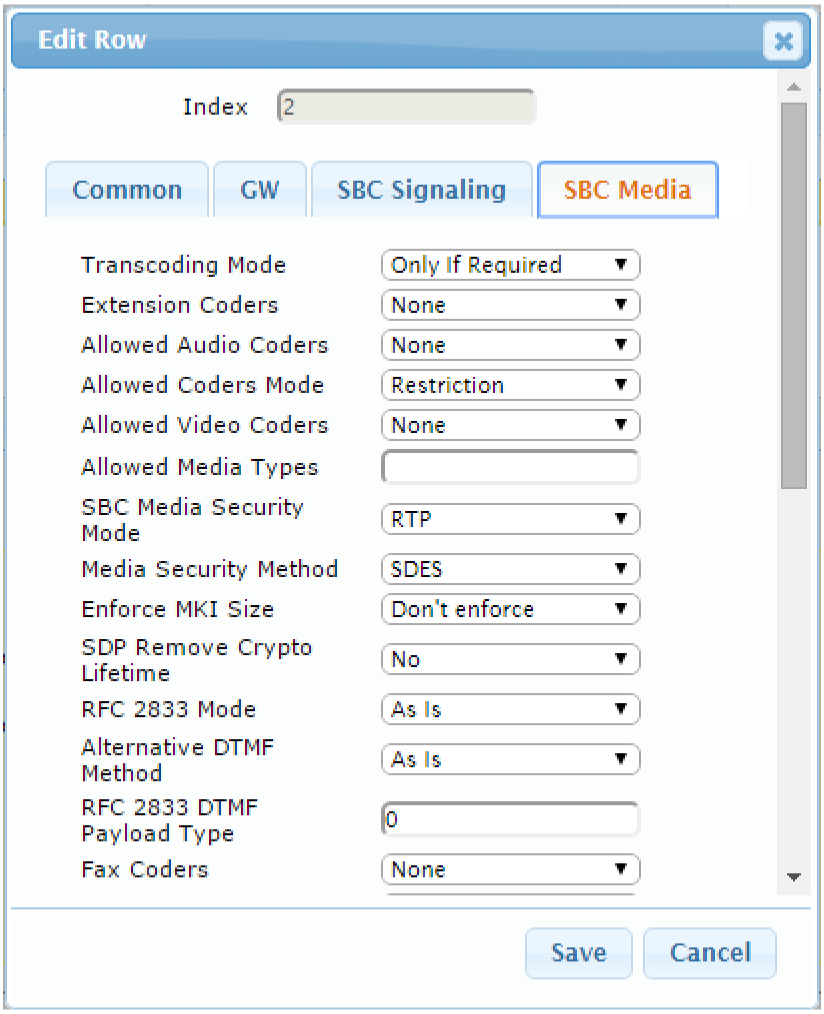
Figure 4-18: Configuring IP Profile for Polkomtel SIP Trunk – SBC Signaling Tab



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

Parameter	Value
Media Security Behavior	**RTP**

Figure 4-19: Configuring IP Profile for Polkomtel SIP Trunk – SBC Media Tab



4.7 Step 7: Configure IP Groups

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

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

- Skype for Business Server 2015 (Mediation Server) located on LAN
- Polkomtel SIP Trunk located on WAN

➢ **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 Skype for Business Server 2015. You can use the default IP Group (Index 0), but modify it as shown below:

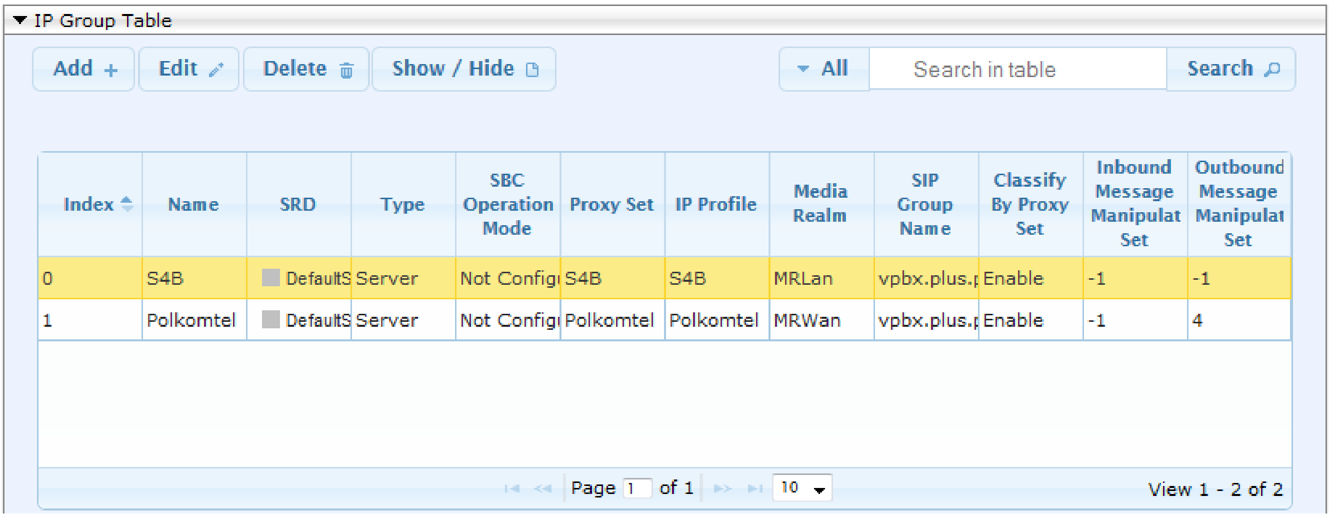
Parameter	Value
Index	**0**
Name	**S4B** (see Note on page 40)
Type	**Server**
Proxy Set	**S4B**
IP Profile	**S4B**
Media Realm	**MRLan**
SIP Group Name	**vpbx.plus.pl** (according to ITSP requirement)

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

Parameter	Value
Index	**1**
Name	**Polkomtel** (see Note on page 40)
Type	**Server**
Proxy Set	**Polkomtel**
IP Profile	**Polkomtel**
Media Realm	**MRWan**
SIP Group Name	**vpbx.plus.pl** (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-20: Configured IP Groups in IP Group Table



Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulat Set	Outbound Message Manipulat Set
0	S4B	DefaultS	Server	Not Confi	S4B	S4B	MRLan	vpbx.plus.	Enable	-1	-1
1	Polkomtel	DefaultS	Server	Not Confi	Polkomtel	Polkomtel	MRWan	vpbx.plus.	Enable	-1	4

4.8 Step 8: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Skype for Business Server 2015 supports the G.711 coder while the network connection to Polkomtel SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the Polkomtel SIP Trunk.

Note: This step is required **only** if specific coders are required.

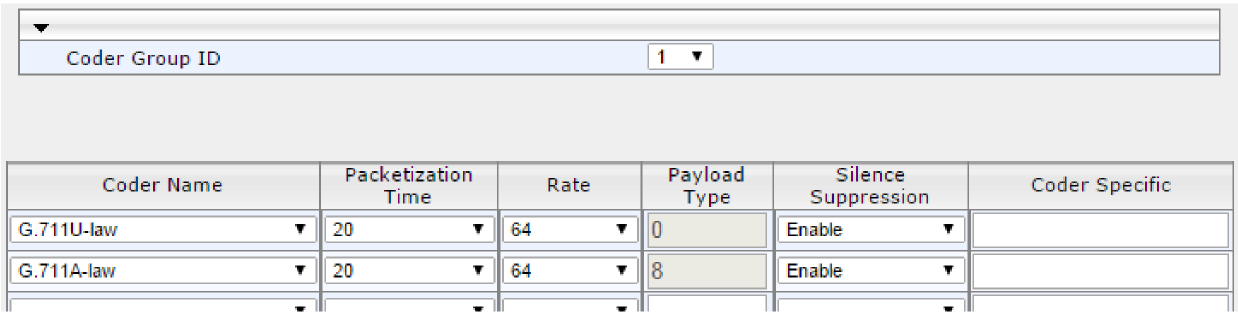
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 45).

➢ **To configure coders:**

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

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

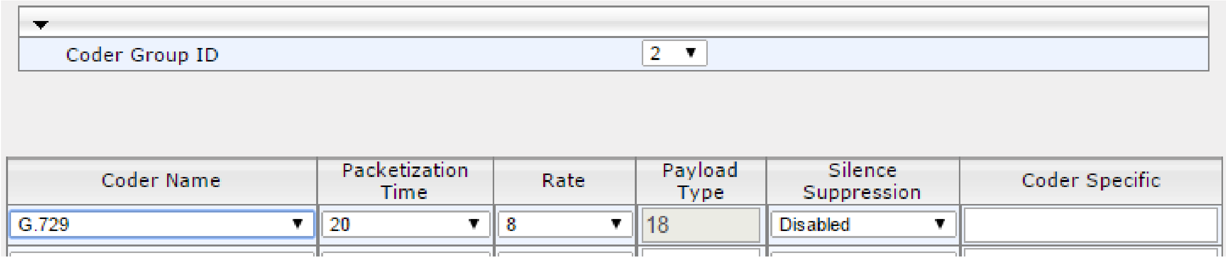
Figure 4-21: Configuring Coder Group for Skype for Business Server 2015



3. Configure a Coder Group for Polkomtel SIP Trunk:

Parameter	Value
Coder Group ID	**2**
Coder Name	**G.729**

Figure 4-22: Configuring Coder Group for Polkomtel SIP Trunk



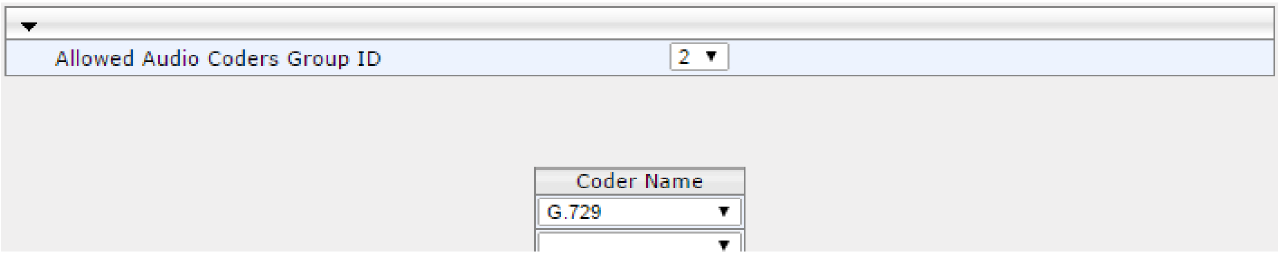
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Polkomtel SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Polkomtel SIP Trunk (see Section 4.6 on page 45).

➢ **To set a preferred coder for the Polkomtel SIP Trunk:**

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

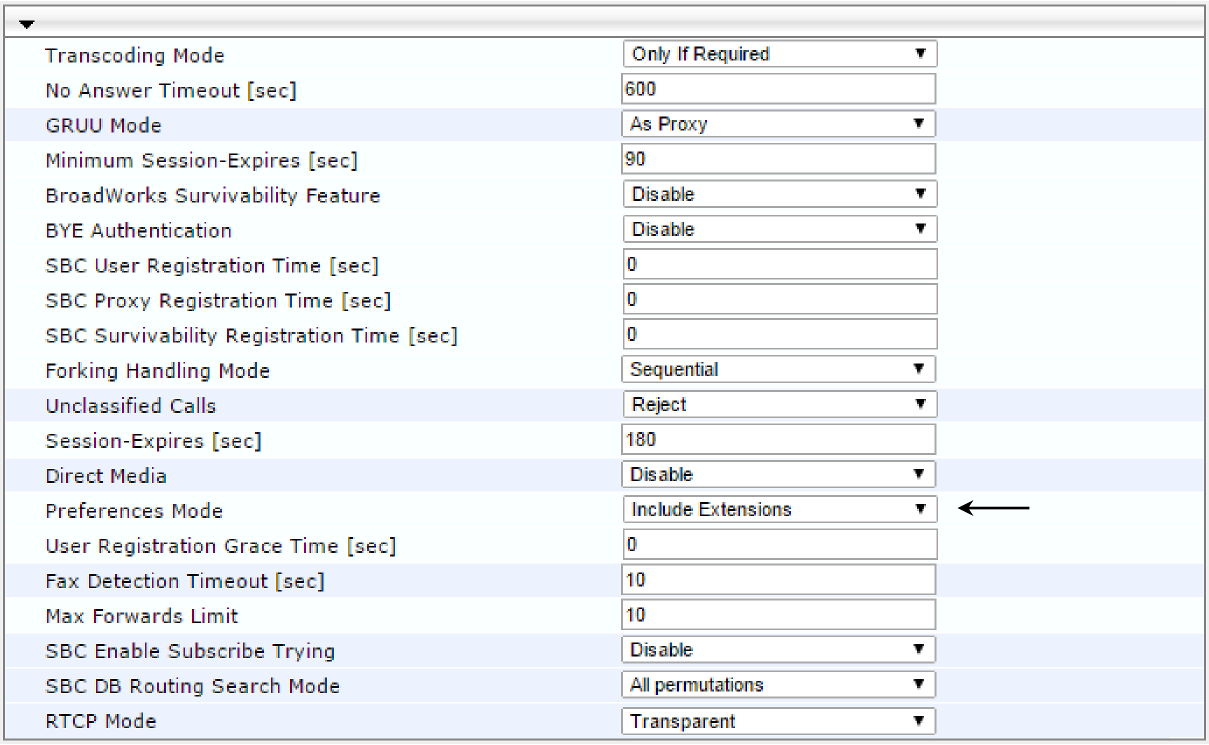
Parameter	Value
Allowed Audio Coders Group ID	**2**
Coder Name	**G.729**

Figure 4-23: Configuring Allowed Coders Group for Polkomtel SIP Trunk



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

Figure 4-24: SBC Preferences 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
SBC User Registration Time [sec]	0
SBC Proxy Registration Time [sec]	0
SBC 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
Max Forwards Limit	10
SBC Enable Subscribe Trying	Disable
SBC DB Routing Search Mode	All permutations
RTCP Mode	Transparent

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

4.9 Step 9: SIP TLS Connection Configuration

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

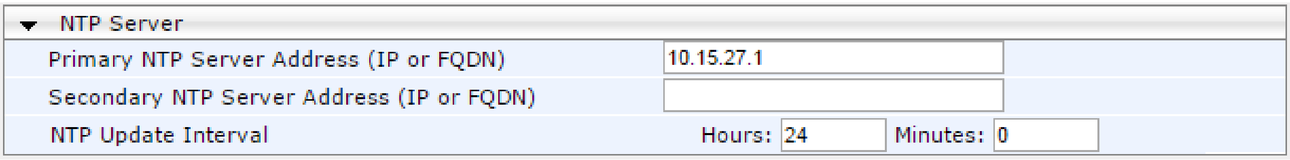
4.9.1 Step 9a: Configure the NTP Server Address

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

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

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

Figure 4-25: Configuring NTP Server Address



3. Click **Submit**.

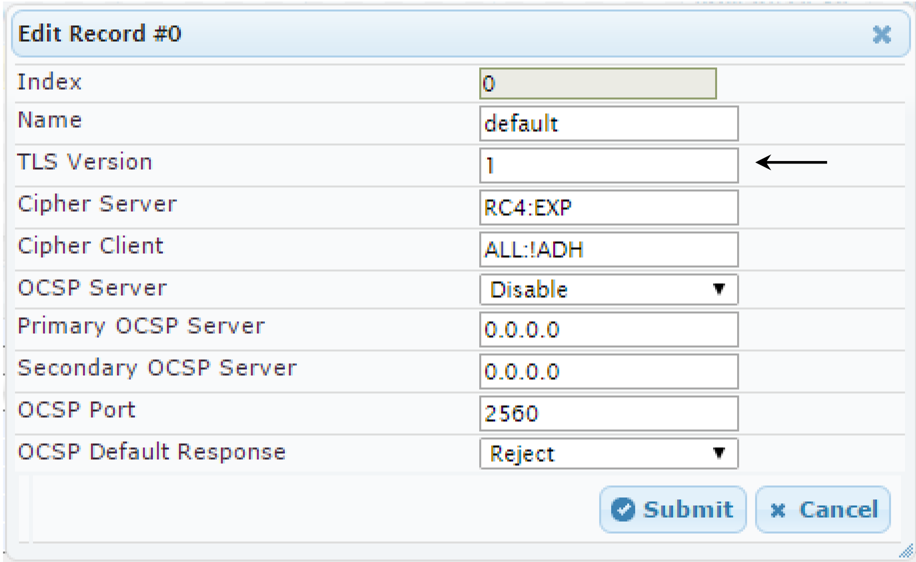
4.9.2 Step 9b: Configure the TLS version 1.0

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

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

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

Figure 4-26: Configuring TLS version 1.0



4. Click **Submit**.

4.9.3 Step 9c: Configure a Certificate

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

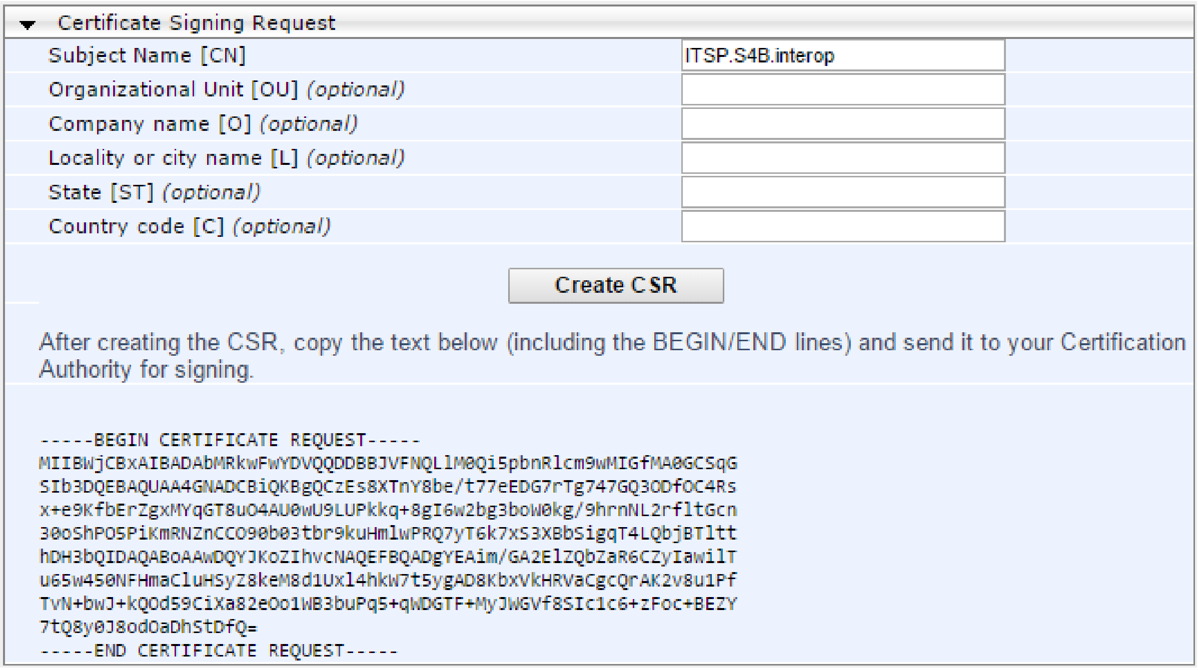
The procedure involves the following main steps:

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

➢ **To configure a certificate:**

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

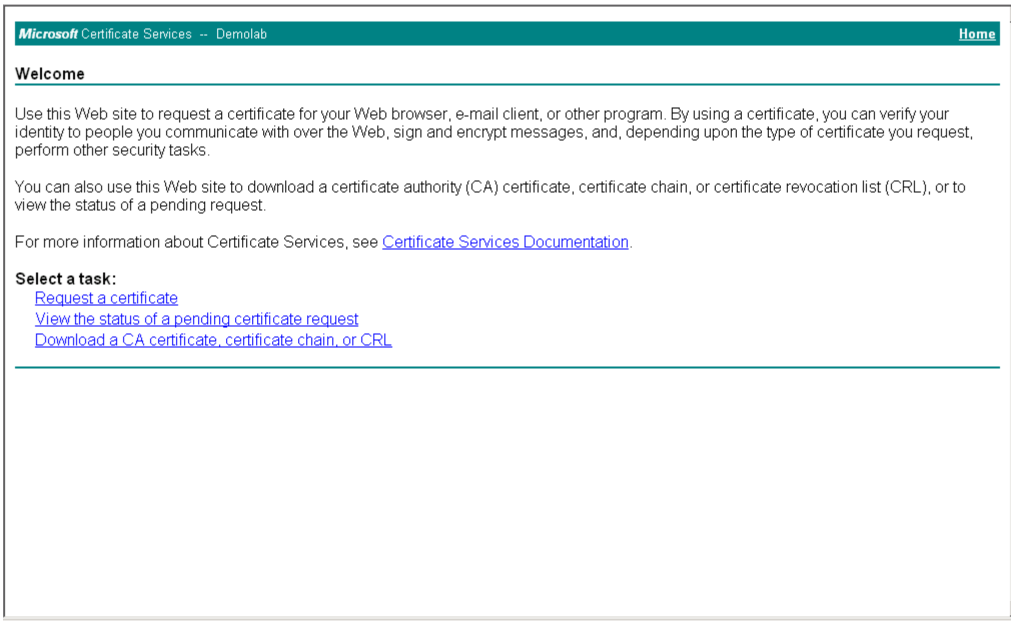
Figure 4-27: Certificate Signing Request – Creating CSR



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

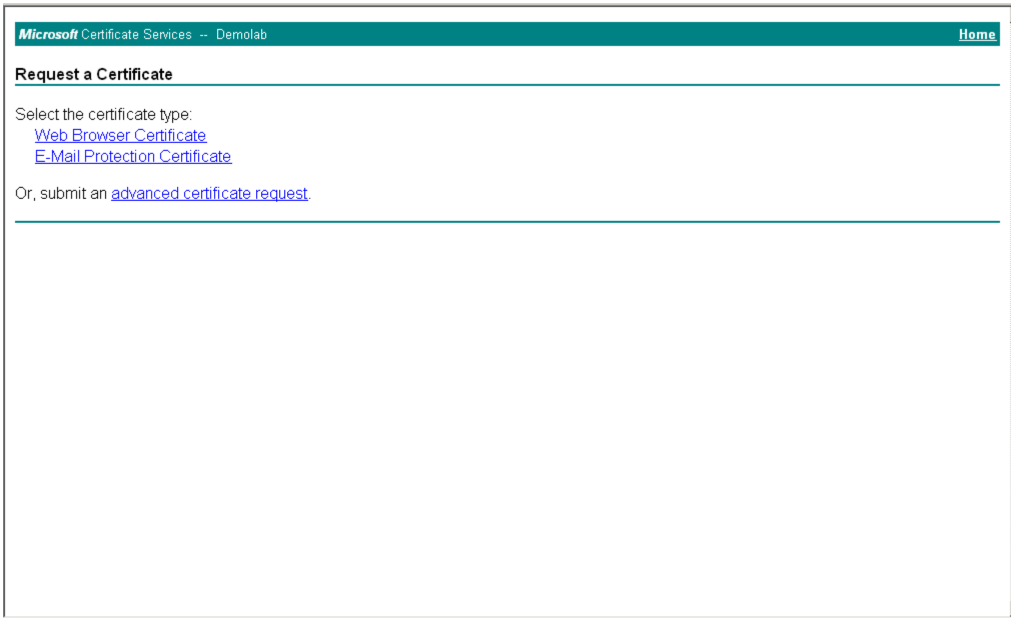
5. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----"** to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate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

Figure 4-28: Microsoft Certificate Services Web Page



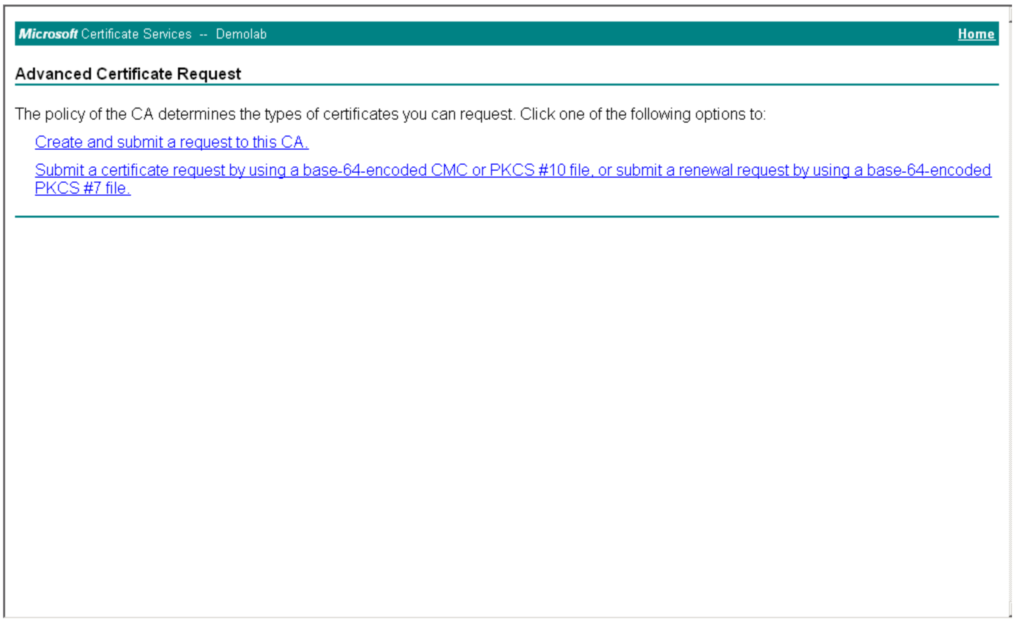
7. Click **Request a certificate**.

Figure 4-29: Request a Certificate Page



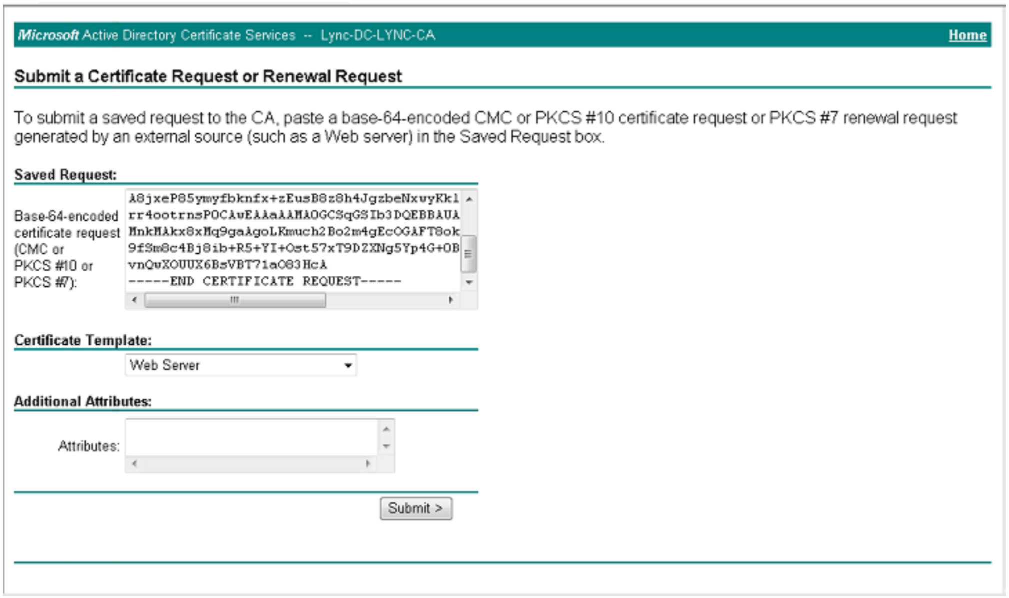
8. Click **advanced certificate request**, and then click **Next**.

Figure 4-30: Advanced Certificate Request Page



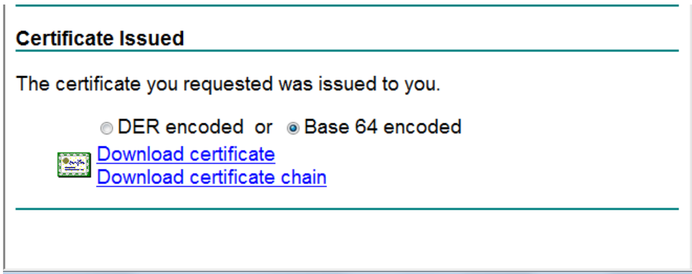
9. Click **Submit a certificate request ...**, and then click **Next**.

Figure 4-31: Submit a Certificate Request or Renewal Request Page



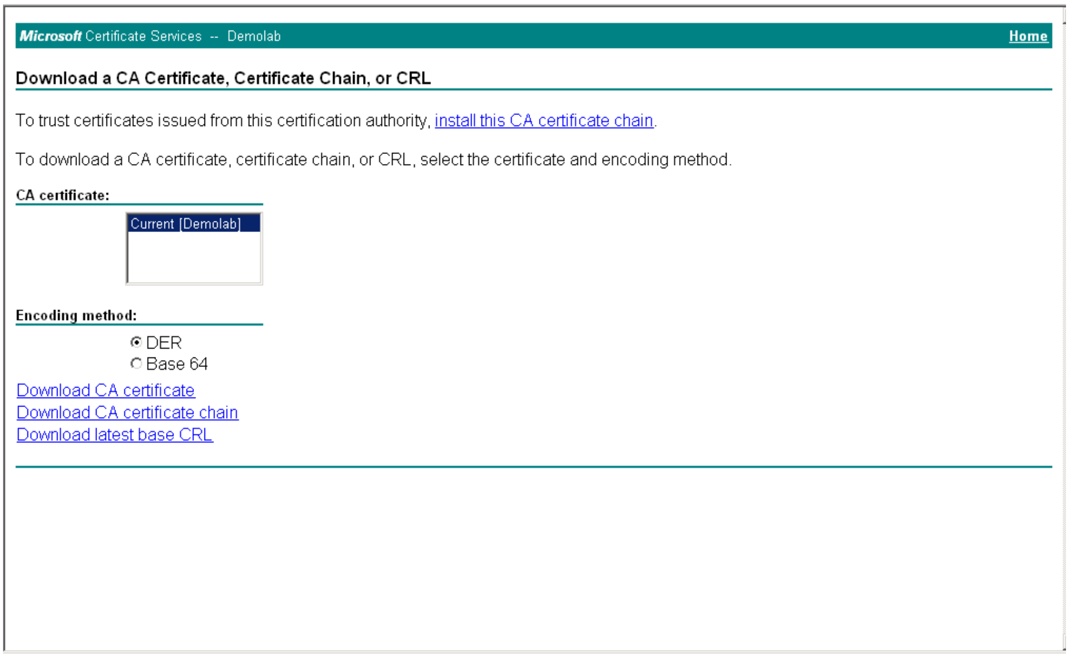
10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**.

Figure 4-32: 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 4-33: Download a CA Certificate, Certificate Chain, or CRL Page



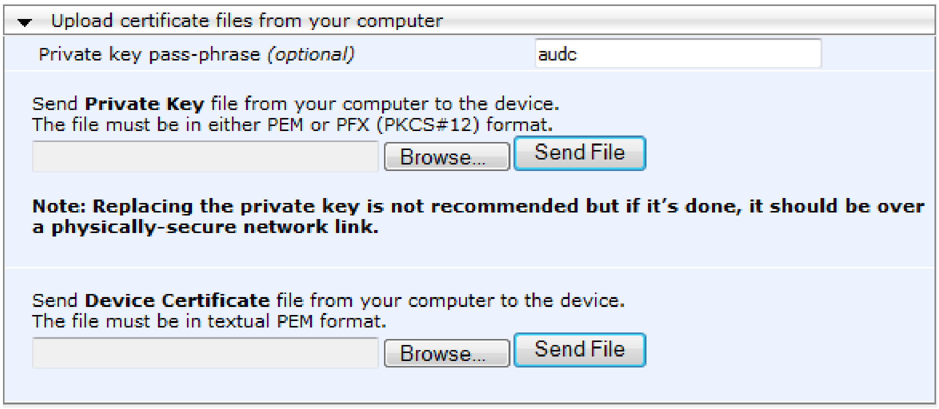
17. Under the 'Encoding method' group, select the **Base 64** option for encoding.
18. Click **Download CA certificate**.
19. Save the file as *certroot.cer* to a folder on your computer.

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 4-34: Upload Device Certificate Files from your Computer Group

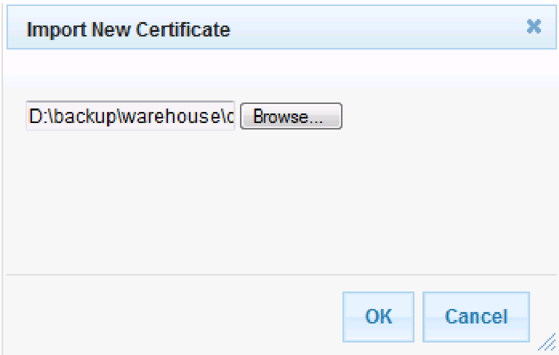


    c. In the E-SBC's Web interface, return to the **TLS Contexts** page.

    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 4-35: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 88).

4.10 Step 10: Configure SRTP

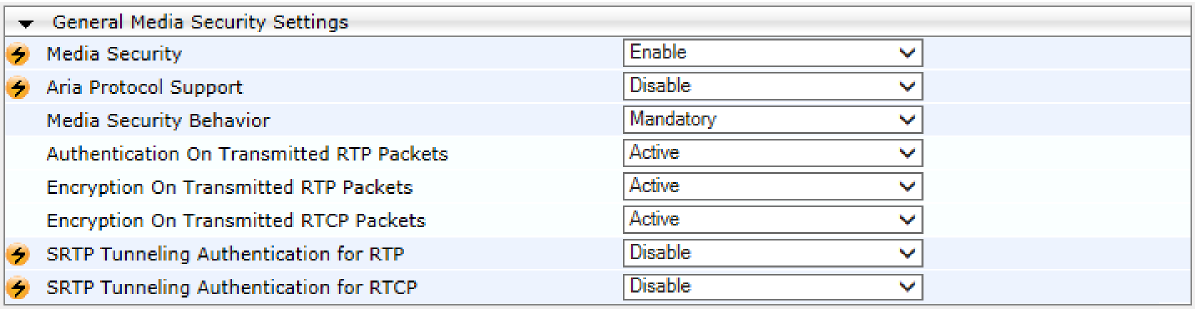
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 4.6 on page 45).

➢ **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 4-36: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 88).

4.11 Step 11: Configure Maximum IP Media Channels

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

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

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

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

Figure 4-37: Configuring Number of Media Channels

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 88).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.7 on page 44, IP Group 1 represents Skype for Business Server 2015, and IP Group 2 represents Polkomtel 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 Polkomtel SIP Trunk (WAN):

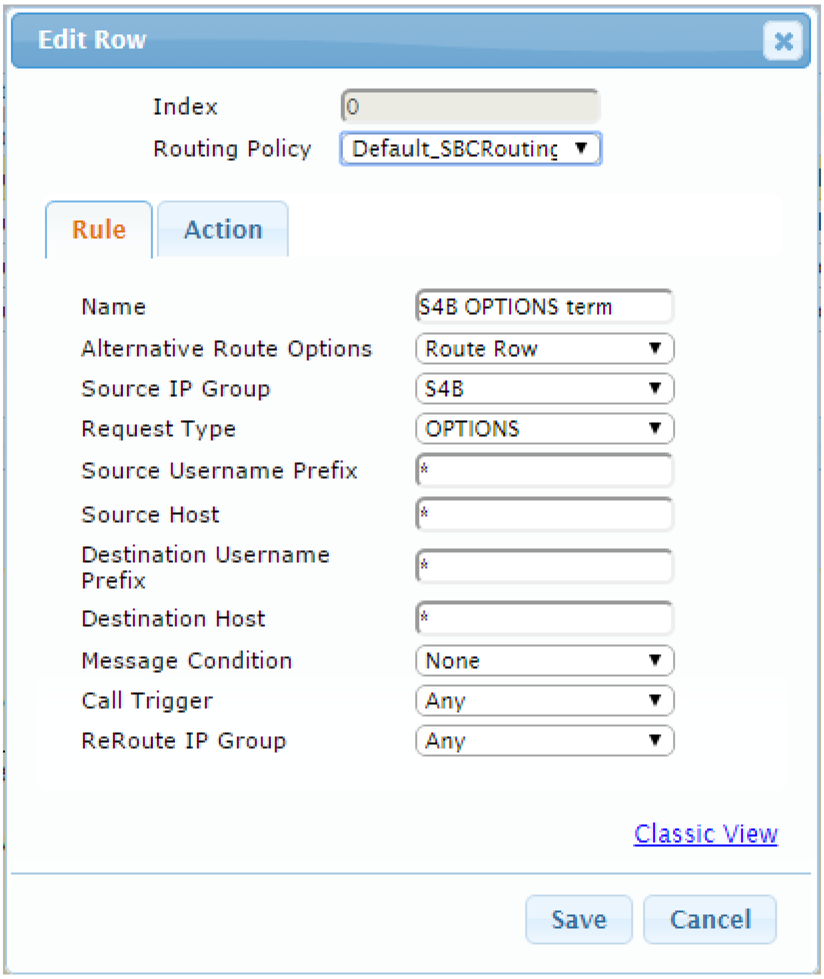
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Skype for Business Server 2015 to Polkomtel SIP Trunk
- Calls from Polkomtel SIP Trunk to Skype for Business Server 2015

➢ 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 Skype for Business Server 2015:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Name	**S4B OPTIONS term** (arbitrary descriptive name)
Source IP Group	**S4B**
Request Type	**OPTIONS**

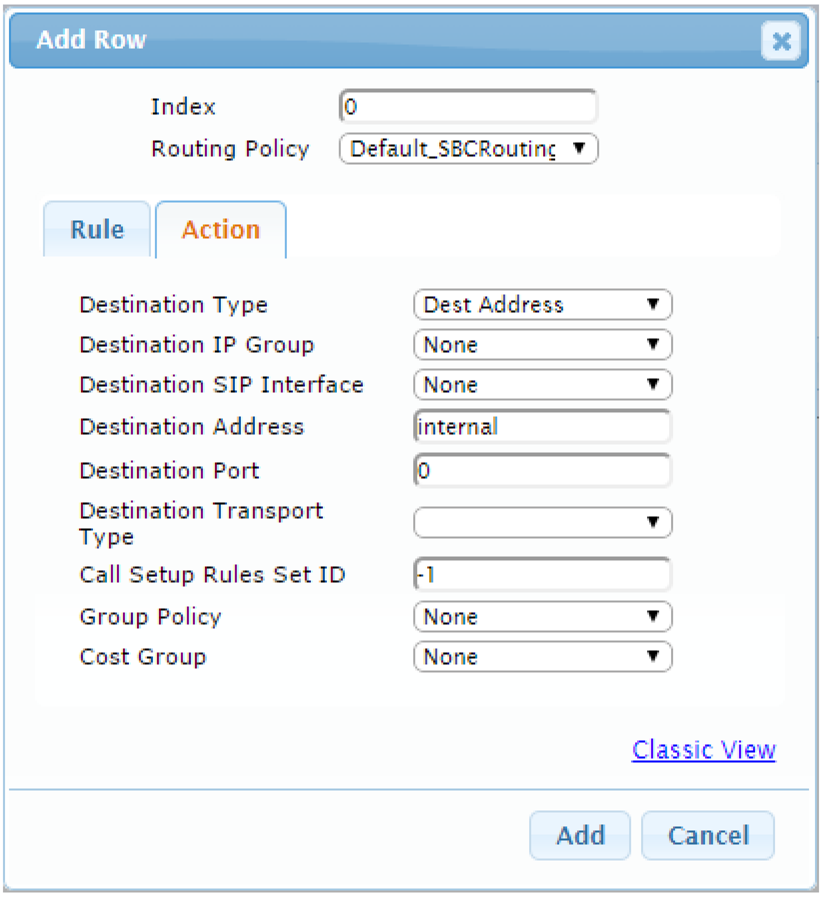
Figure 4-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from S4B – Rule Tab



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

Parameter	Value
Destination Type	**Dest Address**
Destination Address	**internal**

Figure 4-39: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from S4B – Action Tab



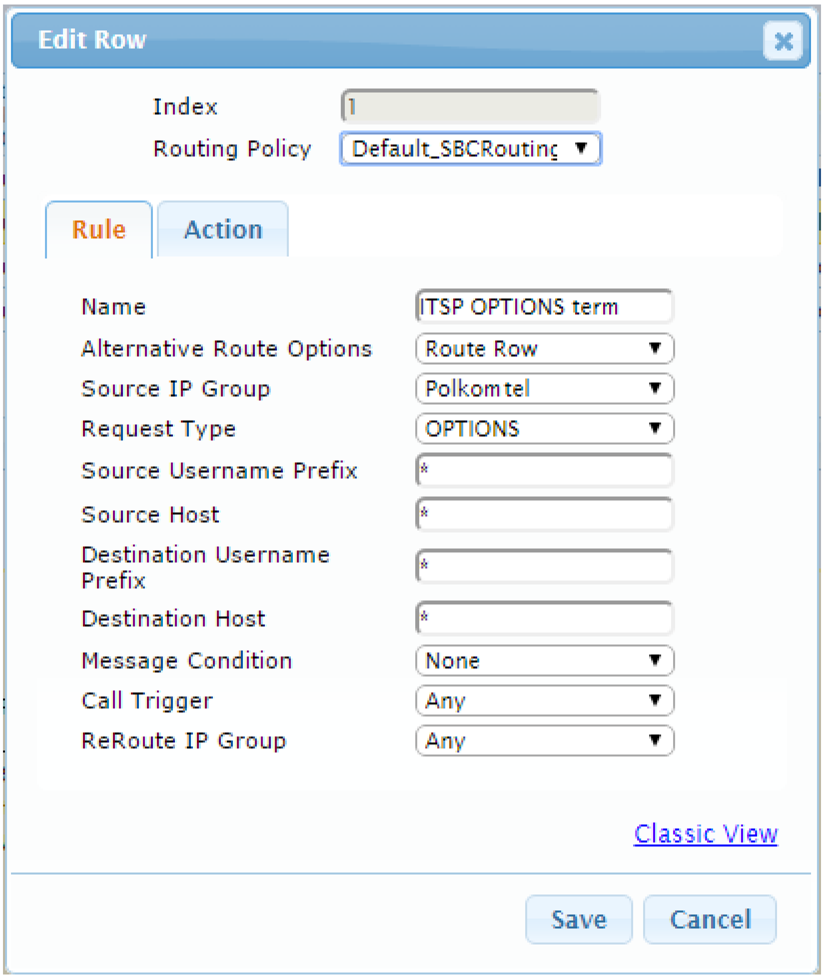
3. Configure a rule to terminate SIP OPTIONS messages received from the Polkomtel SIP Trunk:

   a. Click **Add**.

   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Name	**ITSP OPTIONS term** (arbitrary descriptive name)
Source IP Group	**Polkomtel**
Request Type	**OPTIONS**

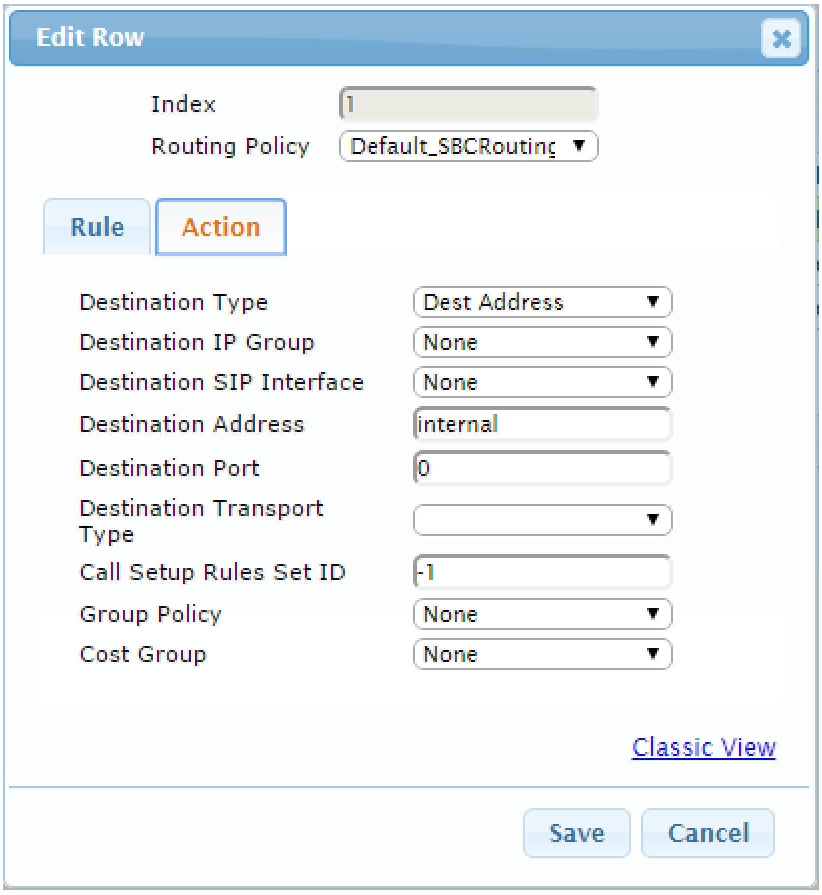
Figure 4-40: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Polkomtel – Rule Tab



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

Parameter	Value
Destination Type	**Dest Address**
Destination Address	**internal**

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



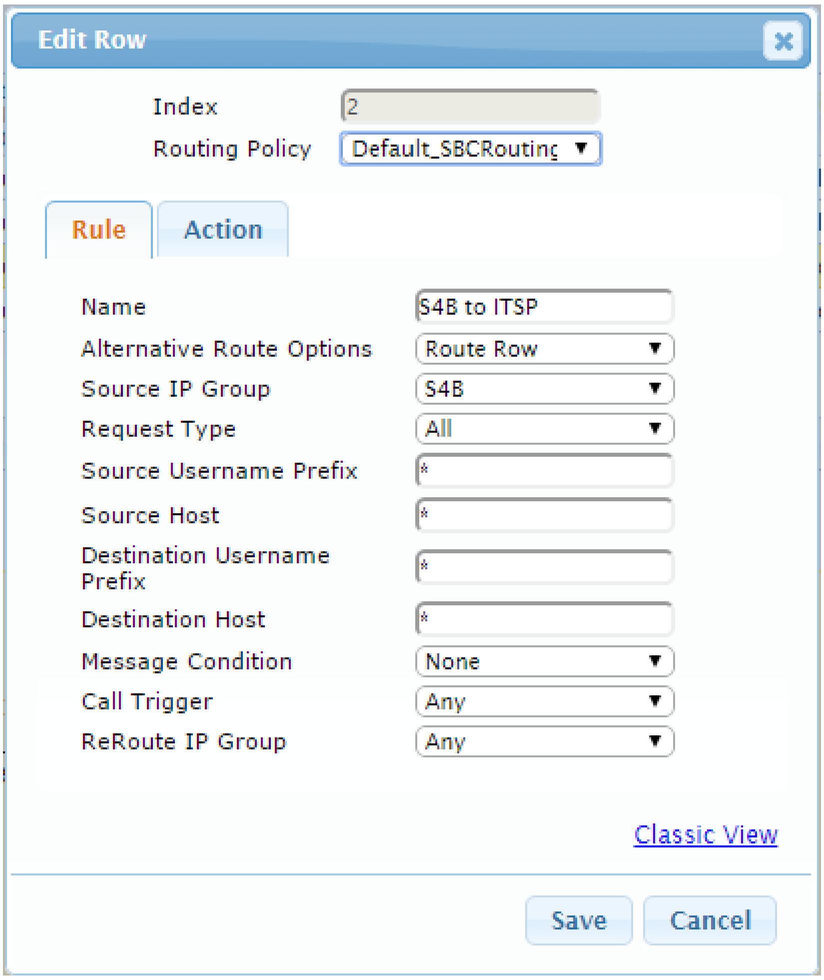
4. Configure a rule to route calls from Skype for Business Server 2015 to Polkomtel SIP Trunk:

a. Click **Add**.

b. Click the **Rule** tab, and then configure the parameters as follows:

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

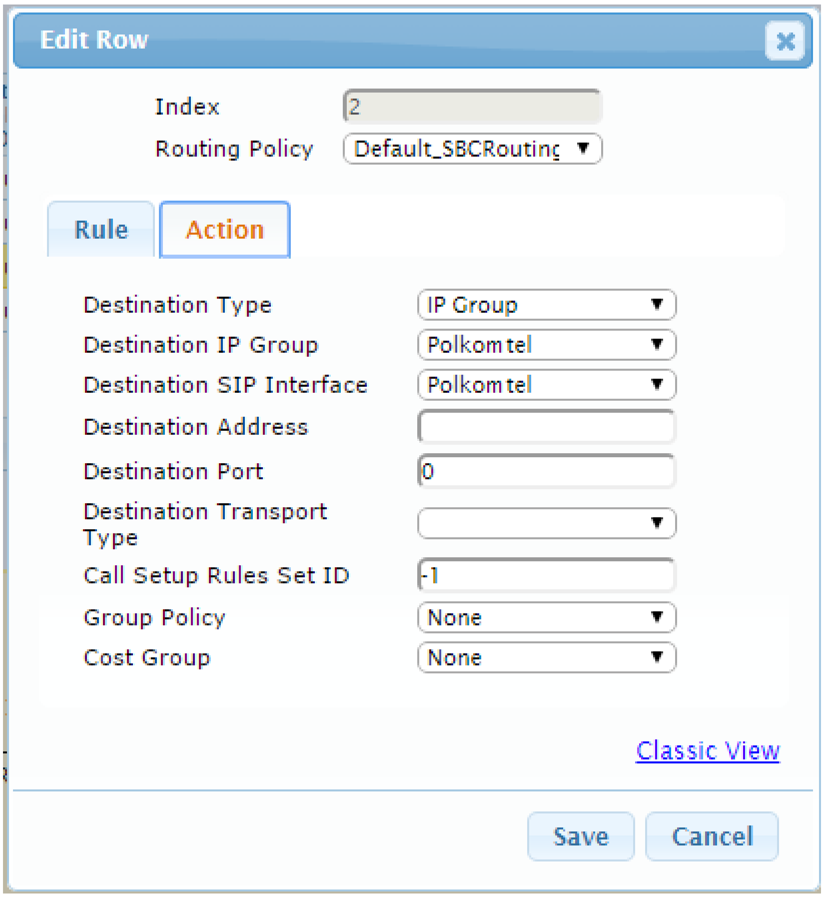
Figure 4-42: Configuring IP-to-IP Routing Rule for S4B to ITSP – Rule tab



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

Parameter	Value
Destination Type	**IP Group**
Destination IP Group	**Polkomtel**
Destination SIP Interface	**Polkomtel**

Figure 4-43: Configuring IP-to-IP Routing Rule for S4B to ITSP – Action tab



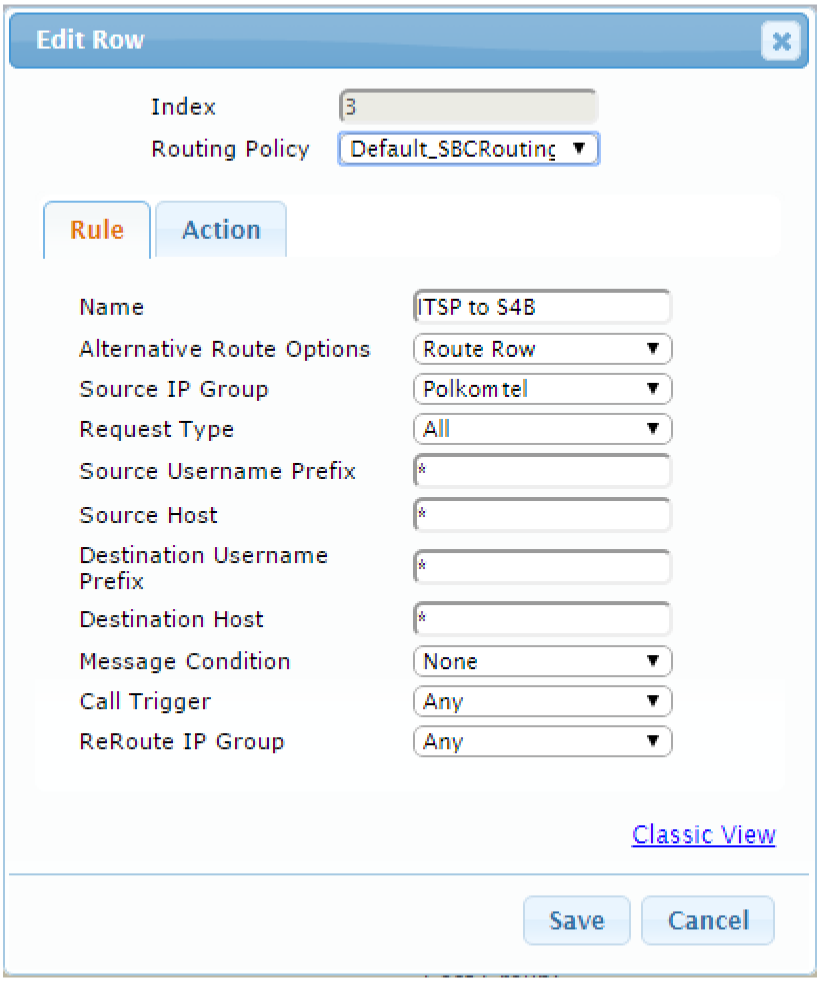
5. To configure rule to route calls from Polkomtel SIP Trunk to Skype for Business Server 2015:

a. Click **Add**.

b. Click the **Rule** tab, and then configure the parameters as follows:

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

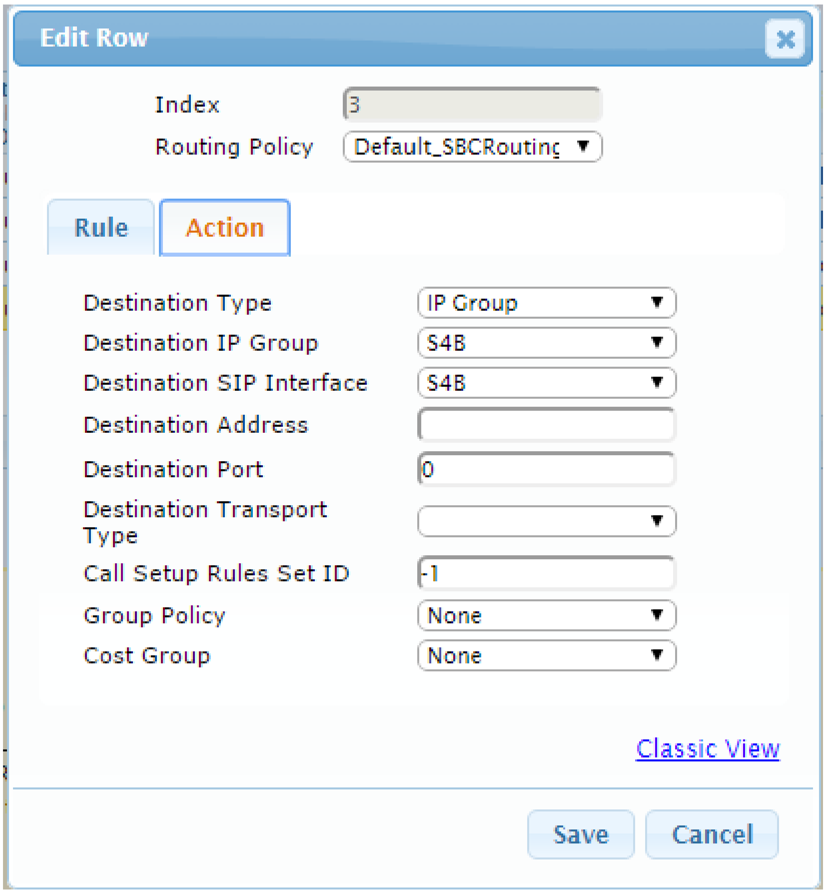
Figure 4-44: Configuring IP-to-IP Routing Rule for ITSP to S4B – Rule tab



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

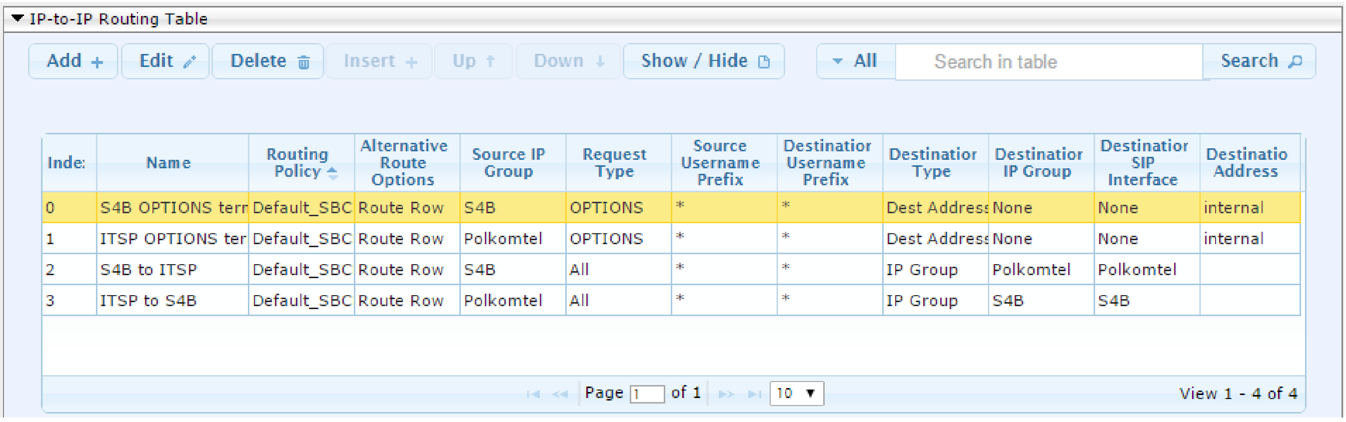
Parameter	Value
Destination Type	**IP Group**
Destination IP Group	**S4B**
Destination SIP Interface	**S4B**

Figure 4-45: Configuring IP-to-IP Routing Rule for ITSP to S4B – Action tab



The configured routing rules are shown in the figure below:

Figure 4-46: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



IP-to-IP Routing Table

Add + | Edit | Delete | Insert + | Up | Down | Show / Hide | All | Search in table | Search

Inde:	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destinatior Username Prefix	Destinatior Type	Destinatior IP Group	Destinatior SIP Interface	Destinatio Address
0	S4B OPTIONS terr	Default_SBC	Route Row	S4B	OPTIONS	*	*	Dest Addres:	None	None	internal
1	ITSP OPTIONS ter	Default_SBC	Route Row	Polkomtel	OPTIONS	*	*	Dest Addres:	None	None	internal
2	S4B to ITSP	Default_SBC	Route Row	S4B	All	*	*	IP Group	Polkomtel	Polkomtel	
3	ITSP to S4B	Default_SBC	Route Row	Polkomtel	All	*	*	IP Group	S4B	S4B	

Page 1 of 1 | 10 | View 1 - 4 of 4

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

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.7 on page 44, IP Group 0 represents Skype for Business Server 2015, and IP Group 1 represents Polkomtel SIP Trunk.

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

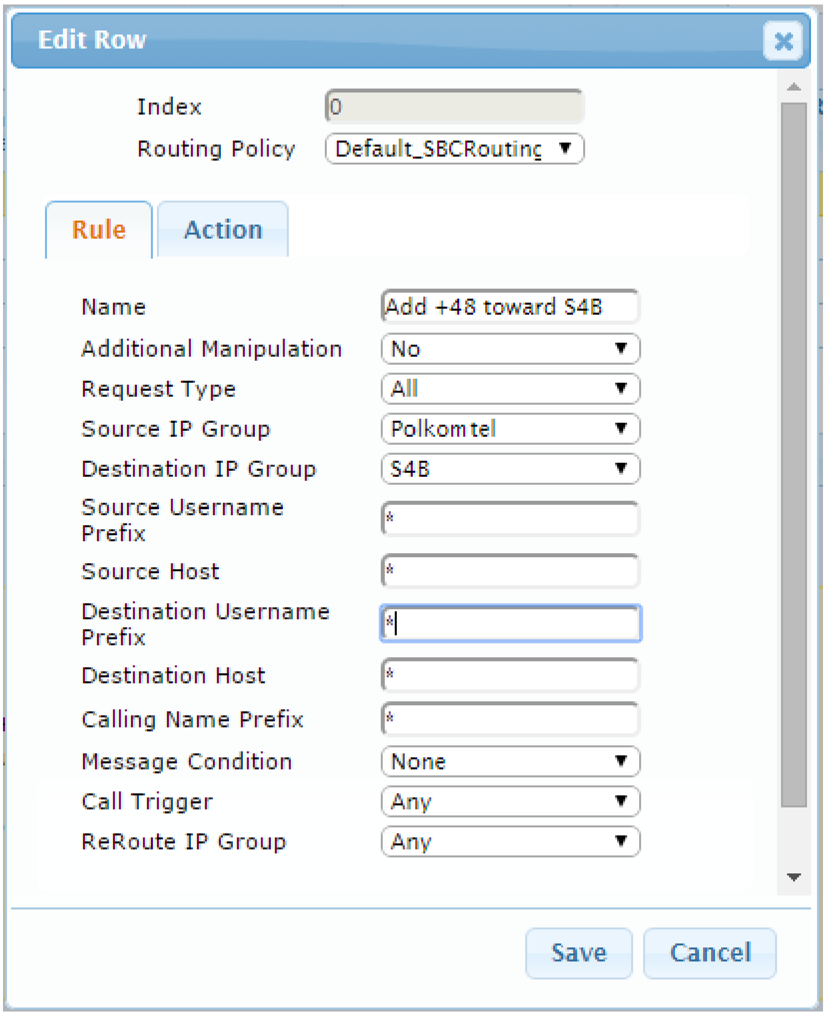
For this interoperability test topology, a manipulation is configured to add the "+48" (plus sign) to the destination number for calls from the Polkomtel SIP Trunk IP Group to the Skype for Business Server 2015 IP Group for any destination username prefix.

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

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

Parameter	Value
Index	**0**
Name	**Add +48 toward S4B**
Source IP Group	**SP**
Destination IP Group	**S4B**
Destination Username Prefix	***** (asterisk sign)

Figure 4-47: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

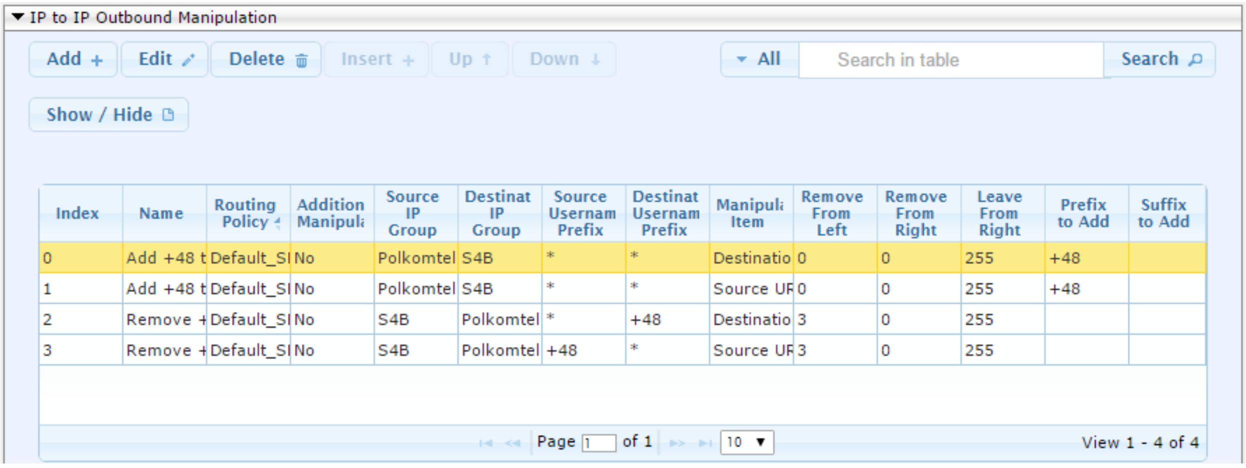
Parameter	Value
Manipulated Item	**Destination URI**
Prefix to Add	**+48** (plus sign)

Figure 4-48: 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 Skype for Business Server 2015 IP Group and Polkomtel SIP Trunk IP Group:

Figure 4-49: Example of Configured IP-to-IP Outbound Manipulation Rules



Index	Name	Routing Policy	Addition Manipul	Source IP Group	Destinat IP Group	Source Usernam Prefix	Destinat Usernam Prefix	Manipul Item	Remove From Left	Remove From Right	Leave From Right	Prefix to Add	Suffix to Add
0	Add +48 t	Default_SI	No	Polkomtel	S4B	*	*	Destinatio	0	0	255	+48	
1	Add +48 t	Default_SI	No	Polkomtel	S4B	*	*	Source UR	0	0	255	+48	
2	Remove +	Default_SI	No	S4B	Polkomtel	*	+48	Destinatio	3	0	255		
3	Remove +	Default_SI	No	S4B	Polkomtel	+48	*	Source UR	3	0	255		

Rule Index	Description
1	Calls from ITSP IP Group to S4B IP Group with any destination number (*), add "+48" to the prefix of the destination number.
2	Calls from ITSP IP Group to S4B IP Group with any destination number (*), add "+48" to the prefix of the source number.
3	Calls from S4B IP Group to ITSP IP Group with the prefix destination number "+48", remove "+48" from this prefix.
4	Calls from S4B IP Group to ITSP IP Group with source number prefix "+48", remove the "+48" from this prefix.

4.14 Step 14: Configure Message Manipulation Rules

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

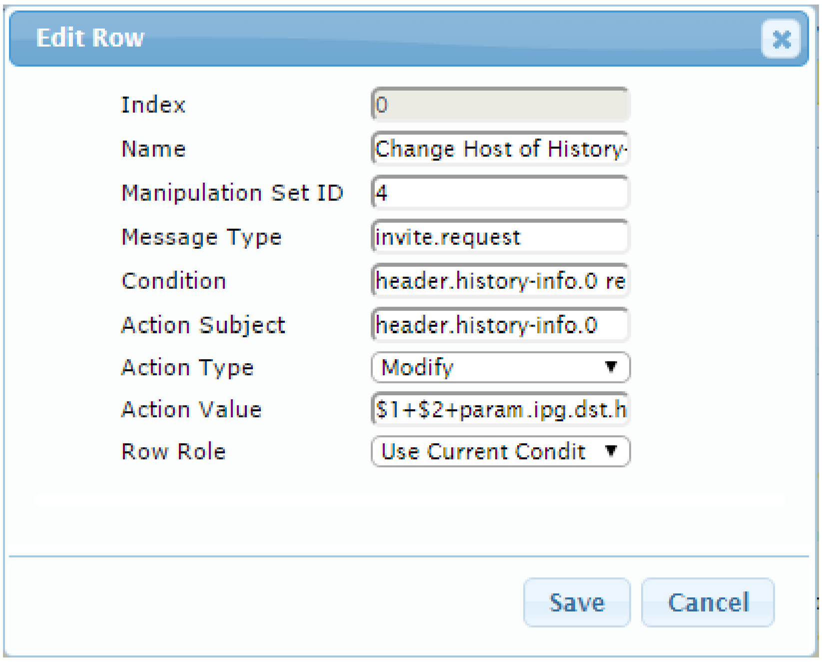
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for Polkomtel SIP Trunk. This rule applies to messages sent to the Polkomtel SIP Trunk IP Group in a call forwarding scenario. This rule replaces the host part of the SIP History-Info Header with the value that was configured in the Polkomtel SIP Trunk IP Group.

Parameter	Value
Index	**0**
Name	**Change Host of History-Info.0**
Manipulation Set ID	**4**
Message Type	**invite.request**
Condition	**header.history-info.0 regex (.*)(@)(.*)(;user=phone)(.*)**
Action Subject	**header.history-info.0**
Action Type	**Modify**
Action Value	**$1+$2+param.ipg.dst.host+$4+$5**

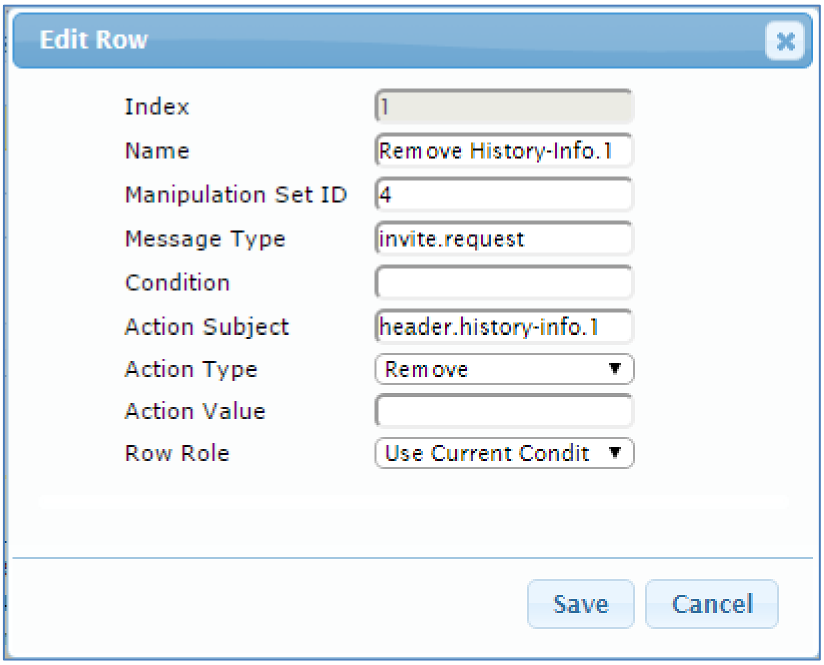
Figure 4-50: Configuring SIP Message Manipulation Rule 0 (for Polkomtel SIP Trunk)



3. Configure another manipulation rule (Manipulation Set 4) for the Polkomtel SIP Trunk. This rule also applies to messages sent to the Polkomtel SIP Trunk IP Group in a call forwarding scenario. This rule removes SIP History-Info.1 Header.

Parameter	Value
Index	**1**
Name	**Remove History-Info.1**
Manipulation Set ID	**4**
Message Type	**invite.request**
Action Subject	**header.history-info.1**
Action Type	**Remove**

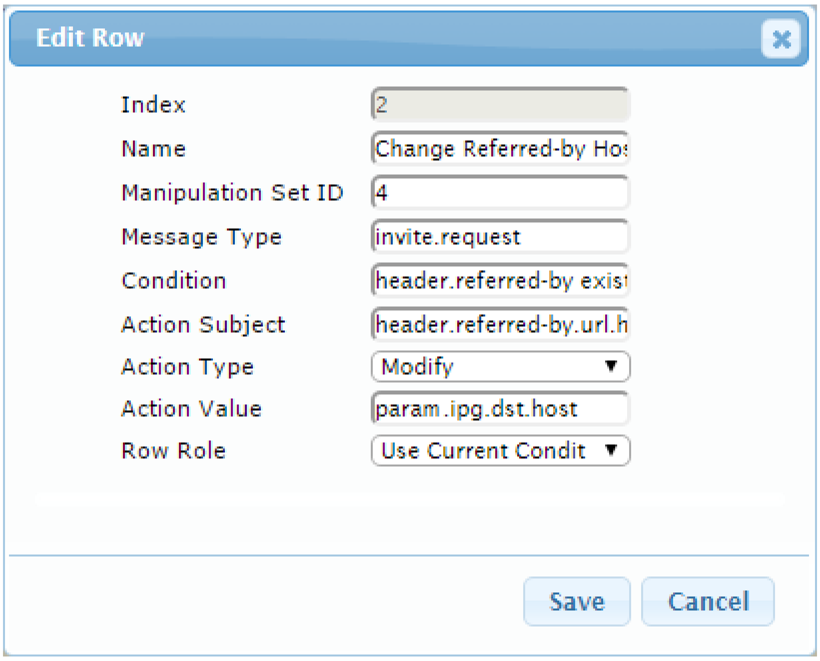
Figure 4-51: Configuring SIP Message Manipulation Rule 1 (for Polkomtel SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 4) for the Polkomtel SIP Trunk. This rule applies to messages sent to the Polkomtel SIP Trunk IP Group in a call transfer scenario. This rule replaces the host part of the SIP Referred-by Header with the value that was configured in the Polkomtel SIP Trunk IP Group.

Parameter	Value
Index	**2**
Name	**Change Referred-by Host**
Manipulation Set ID	**4**
Message Type	**invite.request**
Condition	**header.referred-by exists**
Action Subject	**header.referred-by.url.host**
Action Type	**Modify**
Action Value	**param.ipg.dst.host**

Figure 4-52: Configuring SIP Message Manipulation Rule 2 (for Polkomtel SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 4) for Polkomtel SIP Trunk. This rule is applied to response messages sent to the Polkomtel SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method type ‘480’ or ‘488’ or ‘503’ or ‘603’ with the value ‘486’, because Polkomtel SIP Trunk not recognizes these method types.

Parameter	Value
Index	**3**
Name	**Reject Cause**
Manipulation Set ID	**4**
Message Type	**any.response**
Condition	**header.request-uri.methodtype=='480' OR header.request-uri.methodtype=='488' OR header.request-uri.methodtype=='503' OR header.request-uri.methodtype=='603'**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'486'**

Figure 4-53: Configuring SIP Message Manipulation Rule 3 (for Polkomtel SIP Trunk)

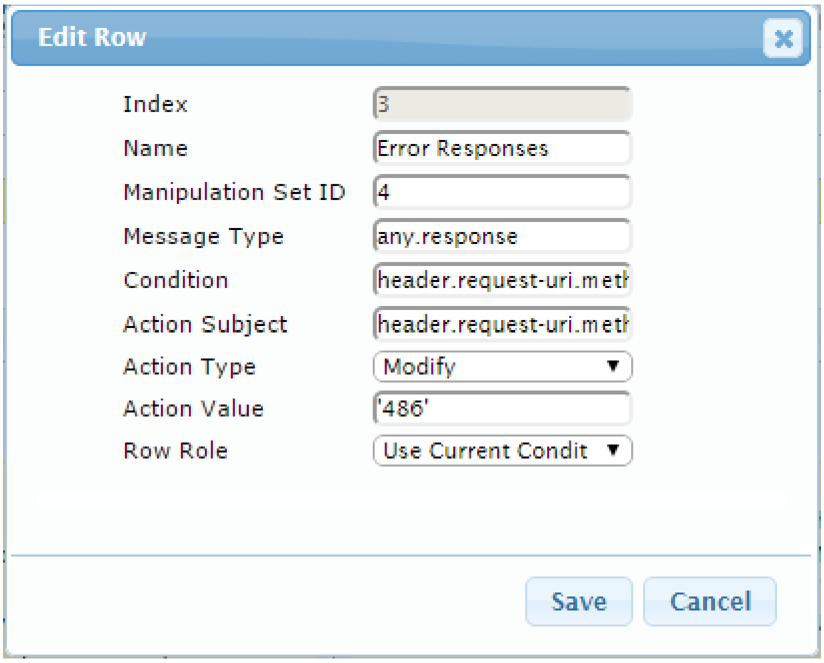
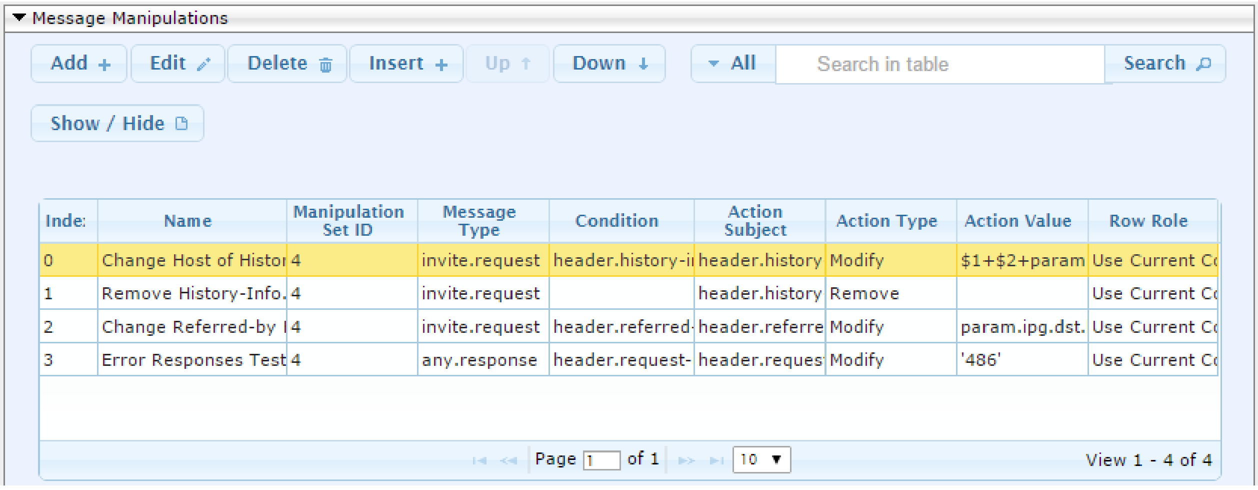


Figure 4-54: Configured SIP Message Manipulation Rules



Inde:	Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	Change Host of Histor	4	invite.request	header.history-i	header.history	Modify	$1+$2+param	Use Current C
1	Remove History-Info.	4	invite.request		header.history	Remove		Use Current C
2	Change Referred-by I	4	invite.request	header.referred-	header.referre	Modify	param.ipg.dst.	Use Current C
3	Error Responses Test	4	any.response	header.request-	header.reques	Modify	'486'	Use Current C

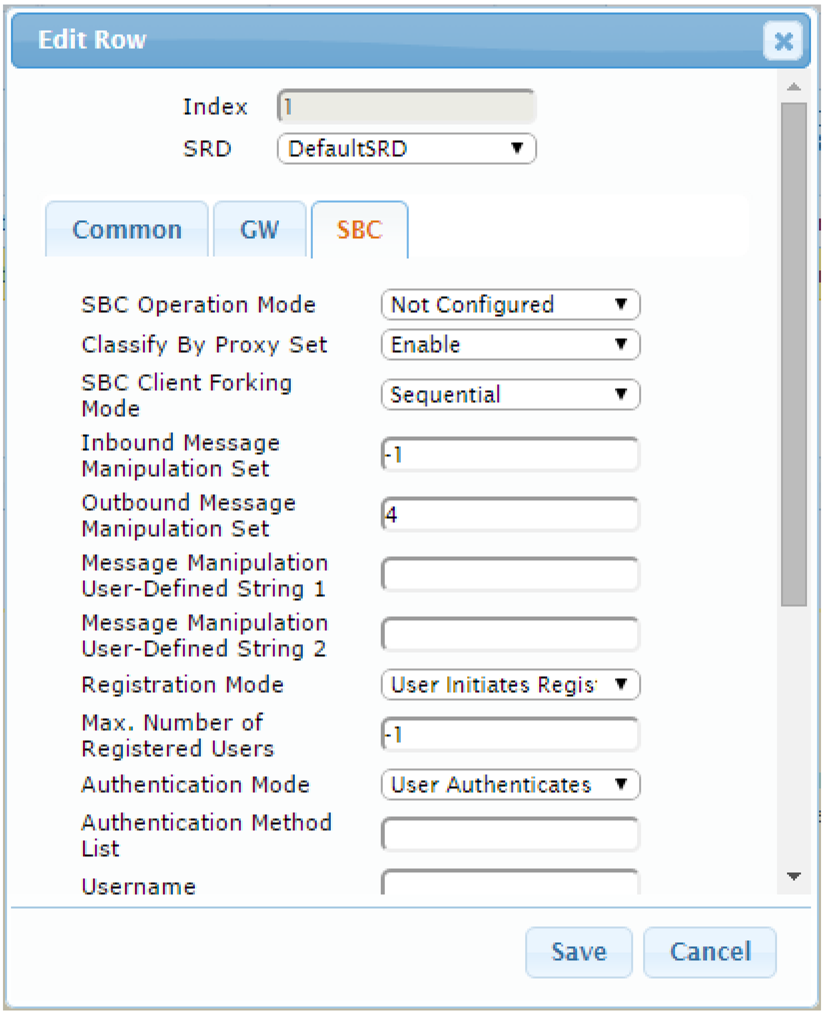
The table displayed below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set ID 4 which are executed for messages sent to the Polkomtel SIP Trunk IP Group. These rules are specifically required to enable proper interworking between Polkomtel SIP Trunk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

SIP Message Manipulation Rules

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages sent to the Polkomtel SIP Trunk IP Group in a call forwarding scenario. This rule replaces the host part of the SIP History-Info Header with the value, configured in the Polkomtel SIP Trunk IP Group.	To introduce Topology Hiding in the Call Forward scenarios, the host part of the SIP History-Info Header should be replaced with the value that was configured in the SIP Trunk IP Group.
1	This rule also applies to messages sent to the Polkomtel SIP Trunk IP Group in a call forwarding scenario. This rule removes the SIP History-Info.1 Header.	To introduce Topology Hiding in the Call Forward scenarios, the SIP History-Info.1 Header should be removed.
2	This rule applies to messages sent to the Polkomtel SIP Trunk IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-by Header with the value, configured in the Polkomtel SIP Trunk IP Group.	To introduce Topology Hiding in the Call Transfer scenarios, the host part of the SIP Referred-by Header should be replaced with the value that was configured in the SIP Trunk IP Group.
3	This rule is applied to response messages sent to the Polkomtel SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method type '480' or '488' or '503' or '603' with the value '486'.	Polkomtel SIP Trunk does not recognize these method types.

6. Assign Manipulation Set ID 4 to the Polkomtel 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 Polkomtel SIP trunk IP Group, and then click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-55: Assigning Manipulation Set 4 to the Polkomtel SIP Trunk IP Group



   e. Click **Submit**.

4.15 Step 15: Configure Registration Accounts

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

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

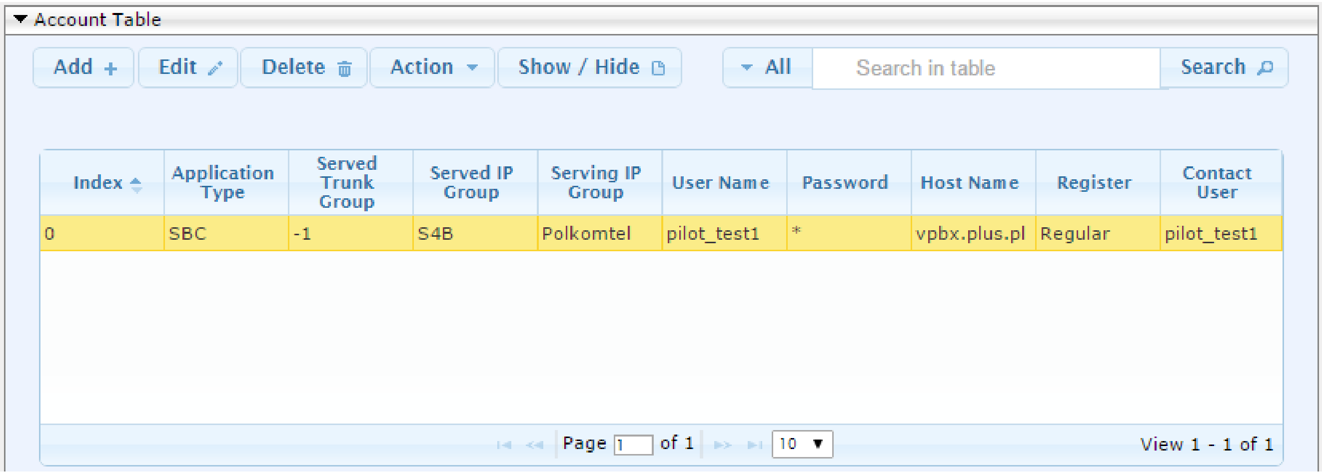
➢ **To configure a registration account:**

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

Parameter	Value
Application Type	**SBC**
Served IP Group	**S4B**
Serving IP Group	**Polkomtel**
Username	**pilot_test1**
Password	As provided by customer
Host Name	**vpbx.plus.pl**
Register	**Regular**
Contact User	**pilot_test1** (trunk main line)

4. Click **Apply**.

Figure 4-56: **Configuring SIP Registration Account**



4.16 Step 16: Miscellaneous Configuration

This section describes the configuration of miscellaneous E-SBC settings

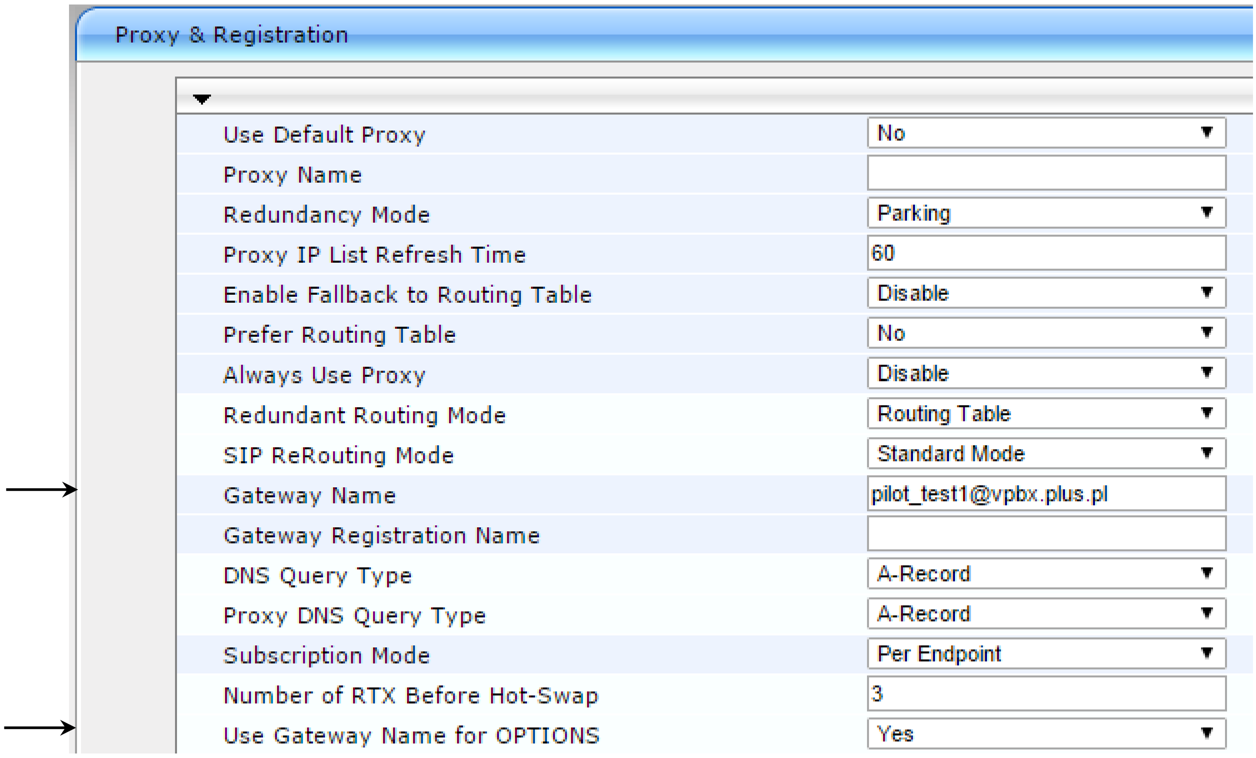
4.16.1 Step 16a: Configure String Name for SIP OPTIONS

This step describes how to configure the E-SBC's string name in keep-alive SIP OPTIONS messages (host part of the Request-URI).

➢ **To configure the string name for SIP OPTIONS:**

1. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).
2. In the 'Gateway Name' field, enter the name according to the ITSP requirement (e.g., **pilot_test1@vpbx.plus.pl**).
3. From the 'Use Gateway Name for OPTIONS' drop-down list, select **Yes**.

Figure 4-57: Configuring String Name for SIP OPTIONS



4. Click **Submit**.

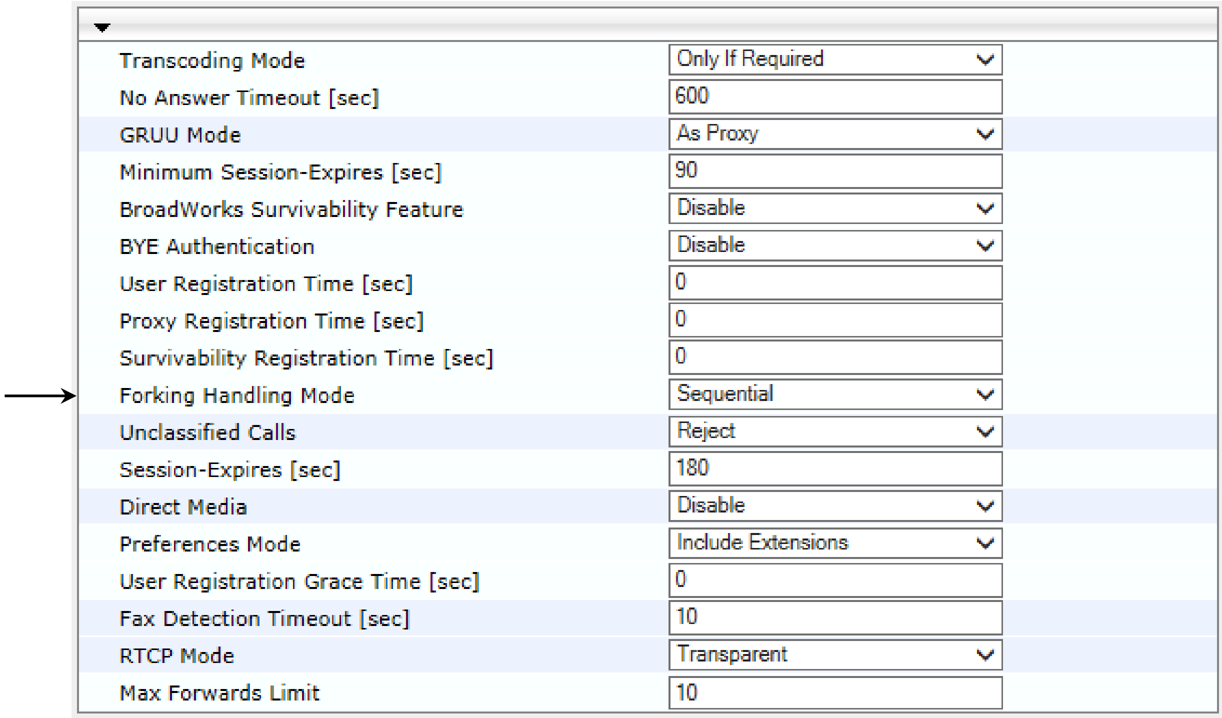
4.16.2 Step 16b: Configure Call Forking Mode

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 ring back 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 4-58: Configuring Forking Mode



3. Click **Submit**.

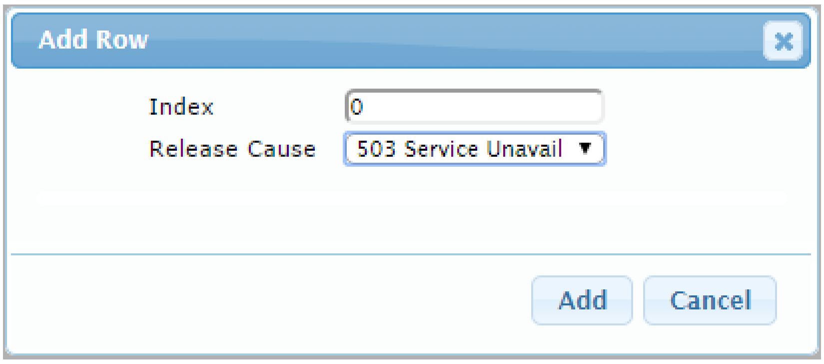
4.16.3 Step 16c: Configure SBC Alternative Routing Reasons

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

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

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

Figure 4-59: SBC Alternative Routing Reasons Table - Add Record



3. Click **Submit**.

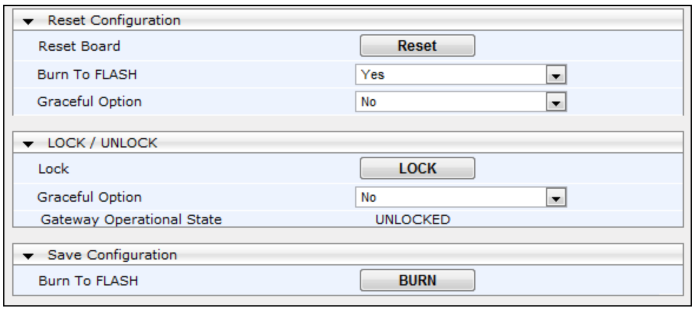
4.17 Step 17: Reset the E-SBC

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

➢ **To save the configuration to flash memory:**

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

Figure 4-60: Resetting the E-SBC



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, is shown below:

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

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 74
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 7.00A.021.013
;DSP Software Version: 5014AE3_R => 700.38
;Board IP Address: 10.15.17.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;Key features:;Board Type: 74 ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;Channel Type: DspCh=30
IPMediaDspCh=30 ;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 ;DSP Voice features: IpmDetector RTCP-XR
AMRPolicyManagement ;E1Trunks=1 ;FXSPorts=8 ;FXOPorts=0 ;BRITrunks=5
;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;DATA features: ;QOE features: VoiceQualityMonitoring MediaEnhancement
;Control Protocols: MSFT CLI TRANSCODING=30 FEU=100 TestCall=100 MGCP
MEGACO H323 SIP TPNCP SASurvivability SBC=50 ;Default features:;Coders:
G711 G726;

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


[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '10.15.27.1'
```

```
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

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

[PSTN Params]


[SS7 Params]


[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

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

[SIP Params]

REGISTRATIONTIME = 300
```

```
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
SIPGATEWAYNAME = 'pilot_test1@vpbx.plus.pl'
USEGATEWAYNAMEFOROPTIONS = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_3", 1, 4, "User Port #2", "GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_1", "GE_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_3", "GE_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

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

```
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0;

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.55, 16, 10.15.0.1, "Voice",
10.15.27.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 192.168.138.224, 24, 192.168.138.223, "WANSP",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]


[ DspTemplates ]

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

[ \DspTemplates ]


[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$LE0VGBxUAQFSUAJXUQANXwoPDwtaeSNwInB2c3B+eihzKSgvfDIzMDI1YGc0YWhub2hlP
GpUVwdVBlNSBgpRXV4=", 1, 0, 2, 15, 60, 200,
"62cabed25276f6d59432fcaf295a1346";
WebUsers 1 = "User",
"$1$fRwcHLO4tOHmvOKy7Oiys7m5vrbzpqfyoKL0r6v7q/iv/P35kpmUwcXBkZWYy5iaz8+Wm
NGBgoPXhdTRi4yDj94=", 3, 0, 2, 15, 60, 50,
"e124fc45691a62316416e055a60edb6f";

[ \WebUsers ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 1, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;
```

```
[ \TLSContexts ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW;
IpProfile 1 = "S4B", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
```

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

[ \IpProfile ]


[ CpMediaRealm ]

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

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]


[ SRD ]

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

[ \SRD ]


[ SIPInterface ]

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

```
[ \SIPInterface ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "S4B", 0, 60, 1, 1, "DefaultSRD", 0, "default", 1, -1, "",
"", "S4B", "", "", "", "";
ProxySet 1 = "Polkomtel", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "Polkomtel", "", "", "", "";

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 0 = 0, "S4B", "S4B", "vpbx.plus.pl", "", -1, 0, "DefaultSRD",
"MRLan", 1, "S4B", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0;
IPGroup 1 = 0, "Polkomtel", "Polkomtel", "vpbx.plus.pl", "", -1, 0,
"DefaultSRD", "MRWan", 1, "Polkomtel", -1, -1, 4, 0, 0, "", 0, -1, -1,
"", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0;

[ \IPGroup ]


[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]


[ ProxyIp ]
```

```
FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "FE.S4B.interop:5067", 2;
ProxyIp 1 = "1", 0, "212.2.126.38:5060", 0;

[ \ProxyIp ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "S4B", "Polkomtel", "pilot_test1", "$1$gQ==",
"vpbx.plus.pl", 1, "pilot_test1", 2;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "S4B OPTIONS term", "Default_SBCRoutingPolicy", "S4B",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "";
IP2IPRouting 1 = "ITSP OPTIONS term", "Default_SBCRoutingPolicy",
"Polkomtel", "*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "",
"internal", 0, -1, 0, 0, "";
IP2IPRouting 2 = "S4B to ITSP", "Default_SBCRoutingPolicy", "S4B", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "Polkomtel", "Polkomtel", "", 0, -
1, 0, 0, "";
IP2IPRouting 3 = "ITSP to S4B", "Default_SBCRoutingPolicy", "Polkomtel",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "S4B", "S4B", "", 0, -1, 0,
0, "";

[ \IP2IPRouting ]


[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
```

```
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = "Add +48 toward S4B",
"Default_SBCRoutingPolicy", 0, "Polkomtel", "S4B", "*", "*", "*", "*",
"*", "", 0, "Any", 0, 1, 0, 0, 255, "+48", "", 0;
IPOutboundManipulation 1 = "Add +48 to Source",
"Default_SBCRoutingPolicy", 0, "Polkomtel", "S4B", "*", "*", "*", "*",
"*", "", 0, "Any", 0, 0, 0, 0, 255, "+48", "", 0;
IPOutboundManipulation 2 = "Remove +48 from Dest",
"Default_SBCRoutingPolicy", 0, "S4B", "Polkomtel", "*", "*", "+48", "*",
"*", "", 0, "Any", 0, 1, 3, 0, 255, "", "", 0;
IPOutboundManipulation 3 = "Remove +48 from Source",
"Default_SBCRoutingPolicy", 0, "S4B", "Polkomtel", "+48", "*", "*", "*",
"*", "", 0, "Any", 0, 0, 3, 0, 255, "", "", 0;

[ \IPOutboundManipulation ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0, "";
CodersGroup1 1 = "g711Alaw64k", 20, 255, -1, 1, "";

[ \CodersGroup0 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change Host of History-Info.0", 4,
"invite.request", "header.history-info.0 regex
(.*)(@)(.*)(;user=phone)(.*)", "header.history-info.0", 2,
"$1+$2+param.ipg.dst.host+$4+$5", 0;
MessageManipulations 1 = "Remove History-Info.1", 4, "invite.request",
"", "header.history-info.1", 1, "", 0;
MessageManipulations 2 = "Change Referred-by Host", 4, "invite.request",
"header.referred-by exists", "header.referred-by.url.host", 2,
"param.ipg.dst.host", 0;
MessageManipulations 3 = "Error Responses Test", 4, "any.response",
"header.request-uri.methodtype=='480' OR header.request-
uri.methodtype=='488' OR header.request-uri.methodtype=='503' OR
header.request-uri.methodtype=='603'", "header.request-uri.methodtype",
2, "'486'", 0;

[ \MessageManipulations ]


[ GwRoutingPolicy ]
```

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

[ \GwRoutingPolicy ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

This page is intentionally left blank.

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-12420