Configuration Note

AudioCodes Professional Services – Interoperability Lab

Microsoft® Skype for Business Server and EWE TEL SIP Trunk using AudioCodes Mediant™ SBC

Version 7.2

Table of Contents

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: July-09-2018

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
12895	Initial document release for Version 7.2.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

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

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

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and EWE TEL Partners who are responsible for installing and configuring EWE TEL's SIP Trunk and Microsoft's Skype for Business Server 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 SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (SE and VE)
Software Version	7.20A.202.112
Protocol	▪ SIP/UDP (to the EWE TEL SIP Trunk) ▪ SIP/TCP or SIP/TLS (to the S4B FE Server)
Additional Notes	None

2.2 EWE TEL SIP Trunking Version

Table 2-2: EWE TEL Version

Vendor/Service Provider	EWE TEL
SSW Model/Service	Cirpack SBC/MGC
Software Version	-
Protocol	SIP
Additional Notes	None

2.3 Microsoft Skype for Business Server Version

Table 2-3: Microsoft Skype for Business Server Version

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

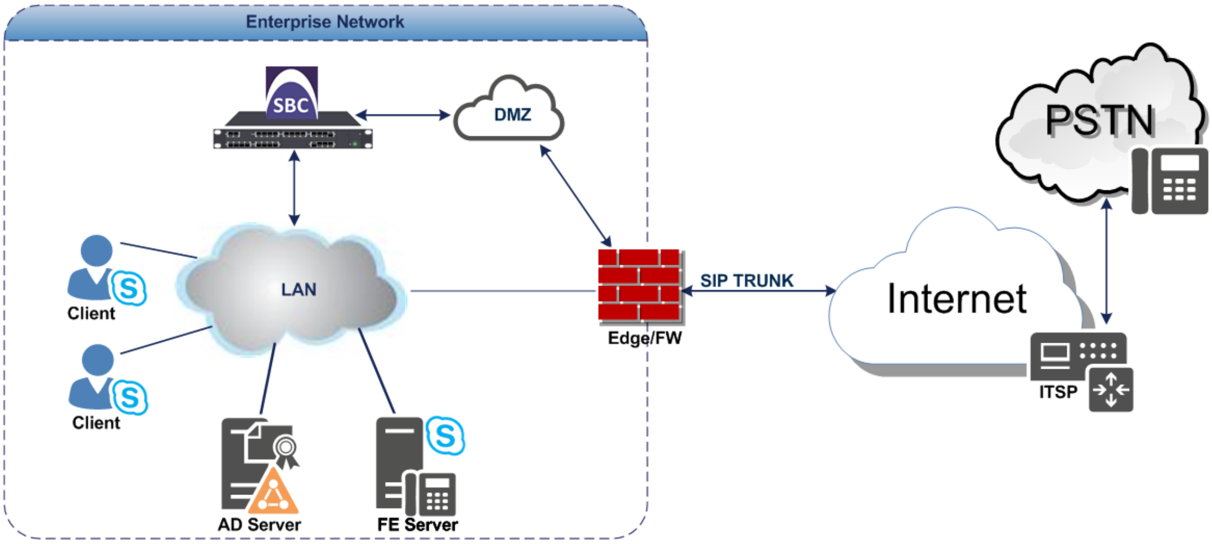
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and EWE TEL SIP Trunk with Skype for Business 2015 was done using the following topology setup:

- Enterprise deployed with Microsoft Skype for Business Server 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 EWE TEL'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 network in the Enterprise LAN and EWE TEL'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 EWE TEL 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 environment is located on the Enterprise's LAN ▪ EWE TEL SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Skype for Business Server operates with SIP-over-TLS transport type ▪ EWE TEL SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Skype for Business Server supports G.711A-law and G.711U-law coders ▪ EWE TEL SIP Trunk supports G.711A-law coder
Media Transcoding	▪ Microsoft Skype for Business Server operates with SRTP media type ▪ EWE TEL SIP Trunk operates with RTP media type

2.4.2 Known Limitations

The following limitation was observed during interoperability tests performed for the AudioCodes SBC interworking between Microsoft Skype for Business Server and EWE TEL 's SIP Trunk:

- Due to multiple interconnectivity networks, the usual ring-back tone is not playback. Therefore, the SBC was configured to generate a local ring-back tone and Early Media tests were performed, however, not verified.

This page is intentionally left blank.

3 Configuring Skype for Business Server

This chapter describes how to configure Microsoft Skype for Business Server 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.

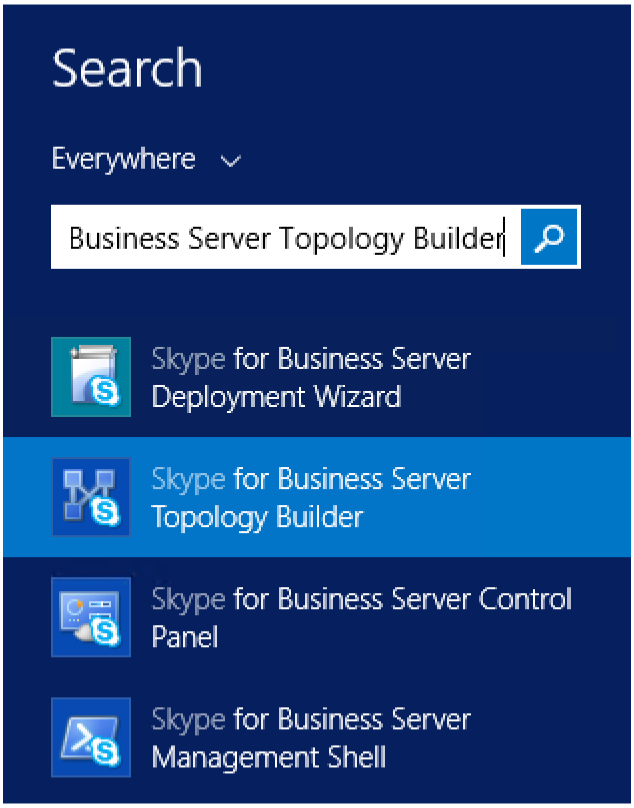
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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:**

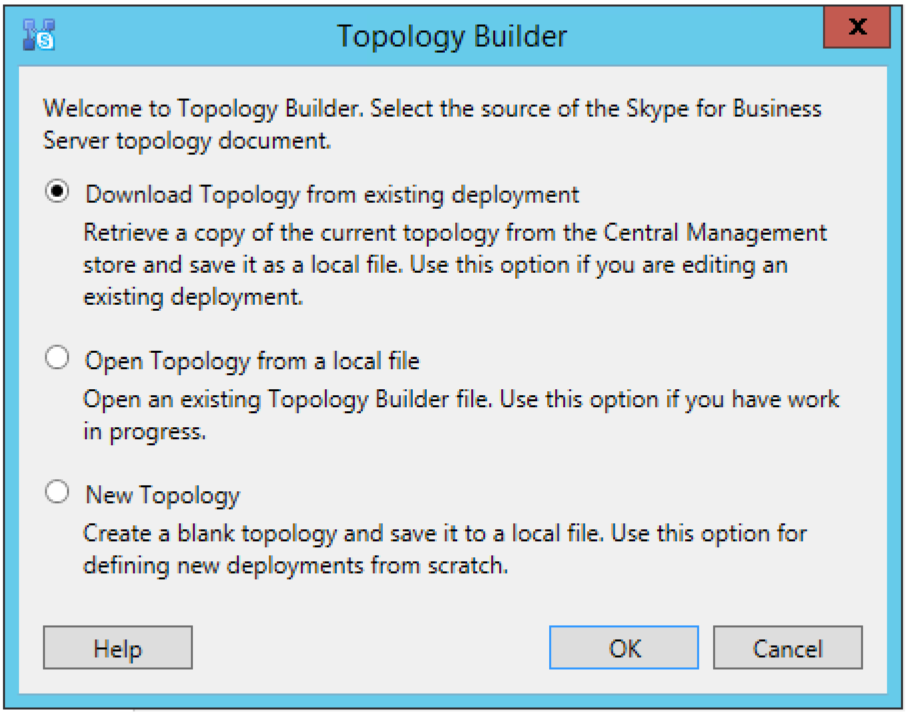
1. On the server where the Topology Builder is installed, start the Skype for Business Server Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

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



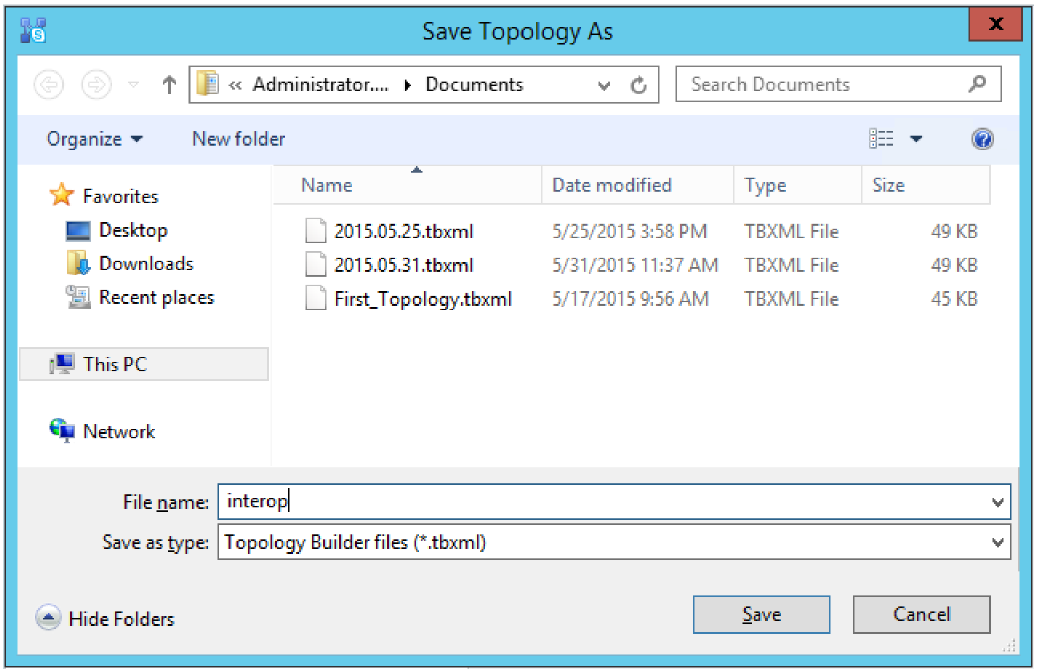
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

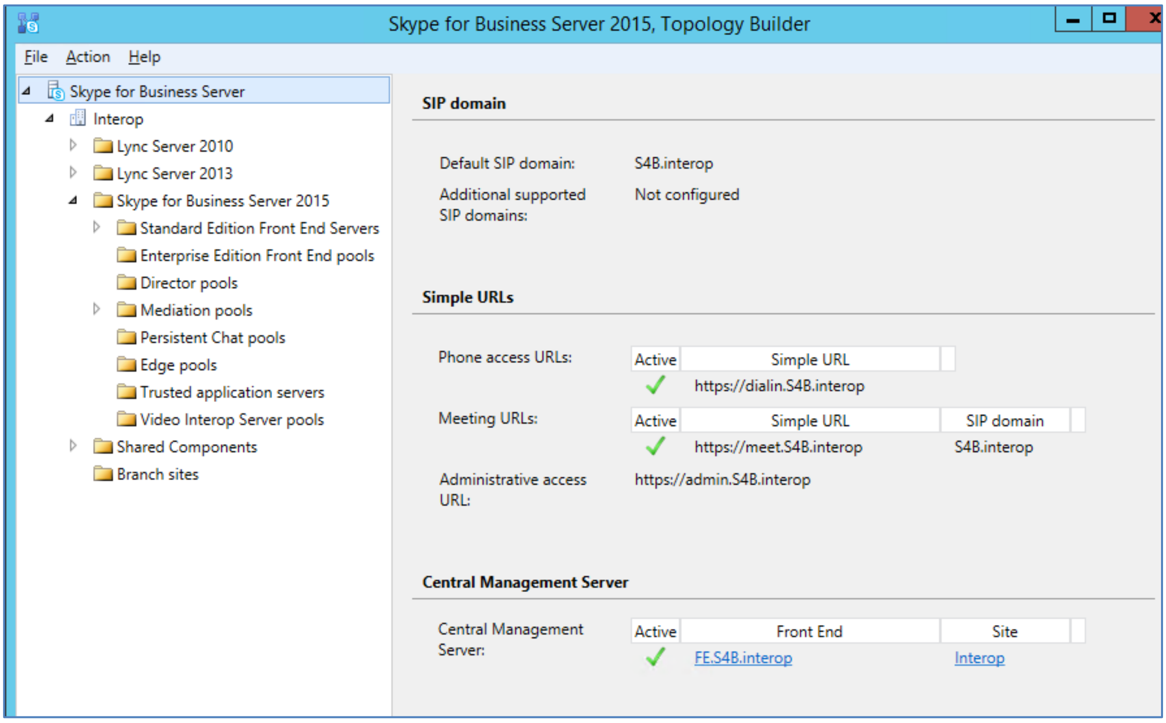
Figure 3-3: Save Topology Dialog Box



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

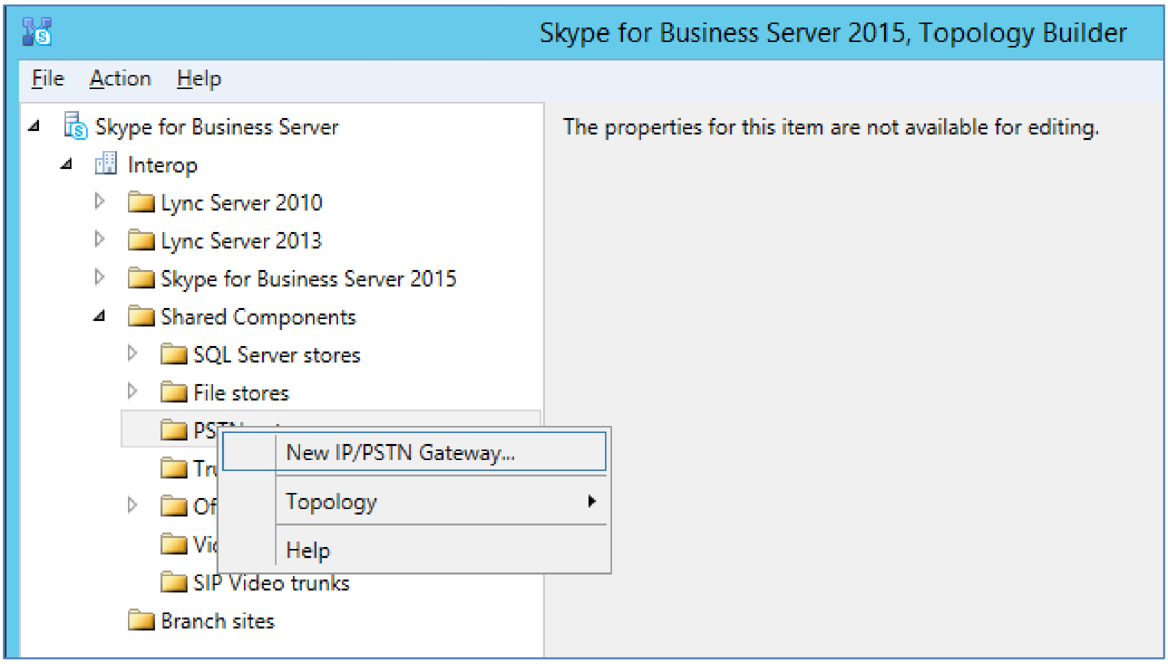
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



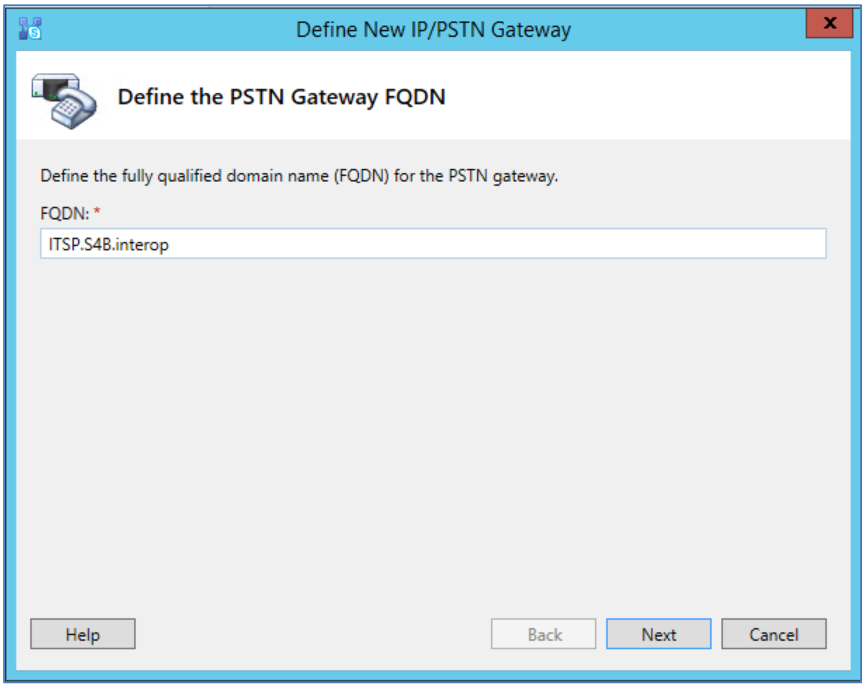
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



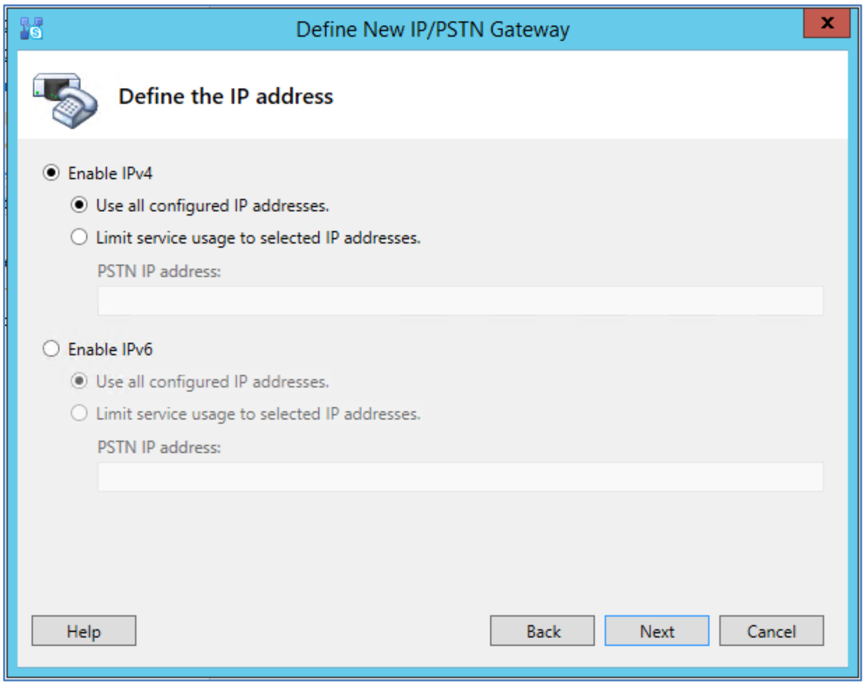
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP.S4B.interop**). This FQDN should be equivalent to the configured Subject Name (CN) in the TLS Certificate Context (see Section 4.8.3 on page 57).
6. Click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



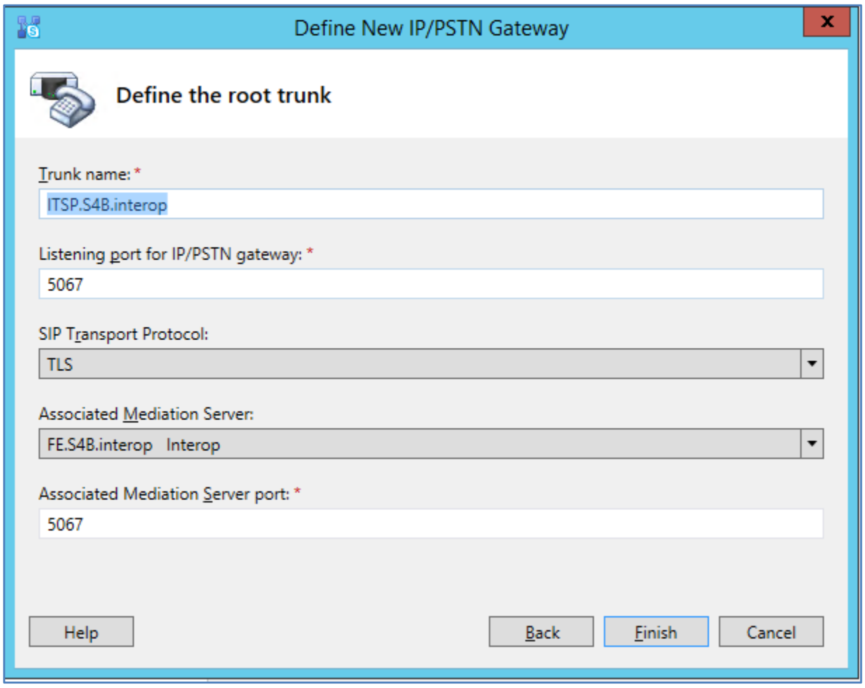
7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

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

Notes:

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

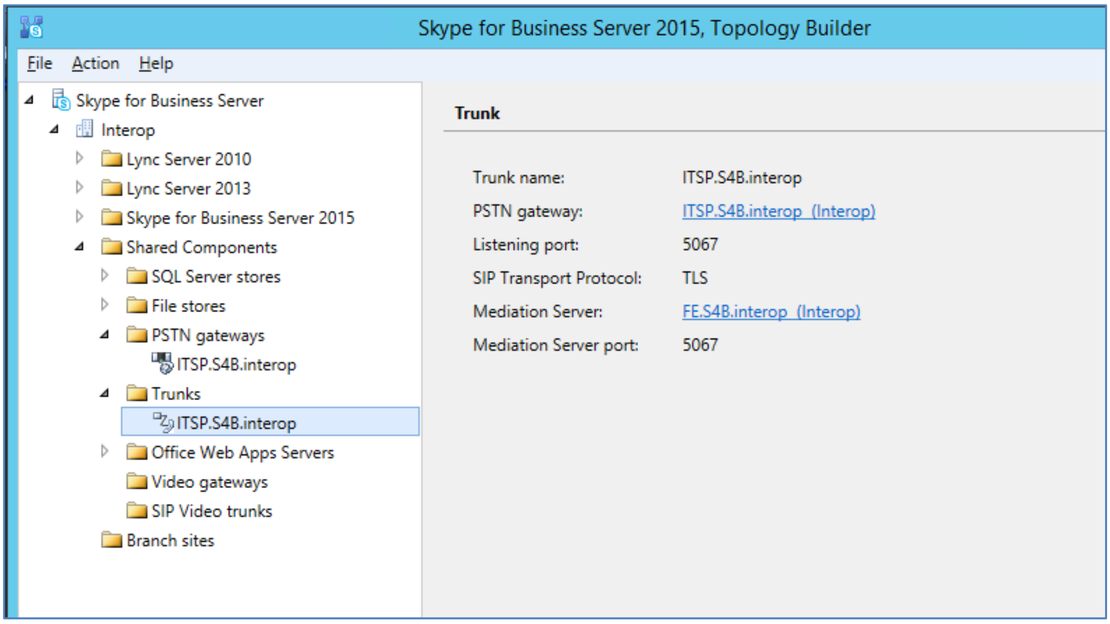
Figure 3-8: Define the Root Trunk



a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**). This parameter is later configured in the SIP Interface table (see Section 4.2 on page 35).
b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses. This parameter is later configured in the SIP Interface table (see Section 4.2 on page 35).
c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
e. Click **Finish**.

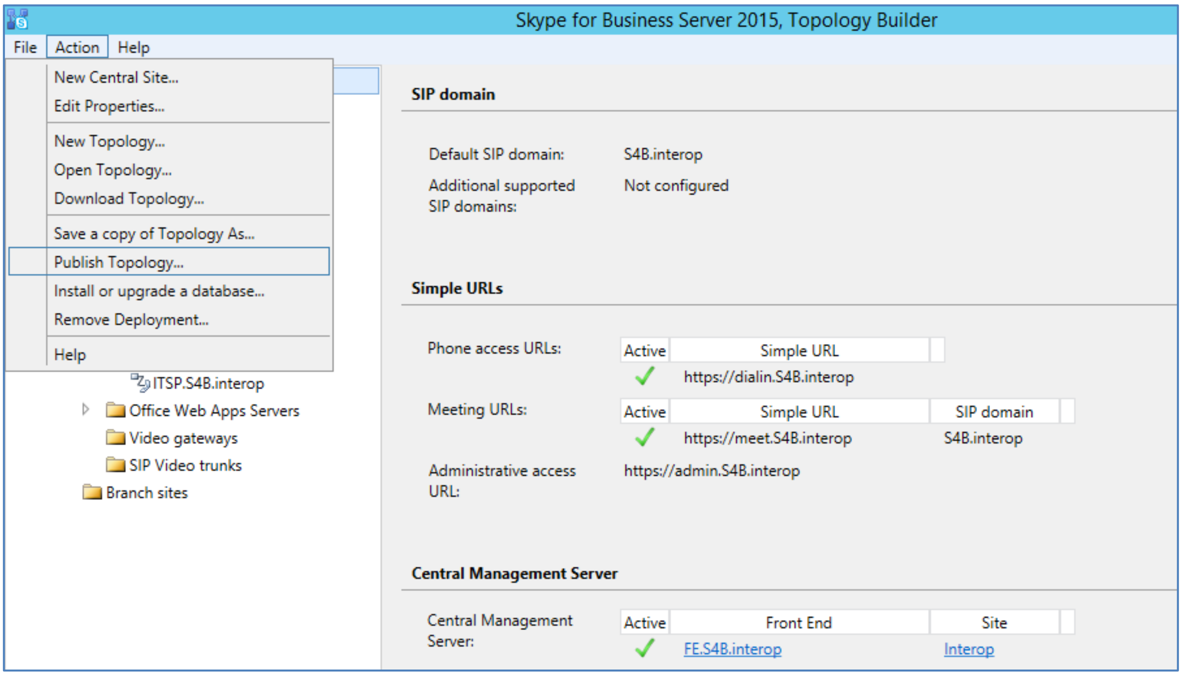
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



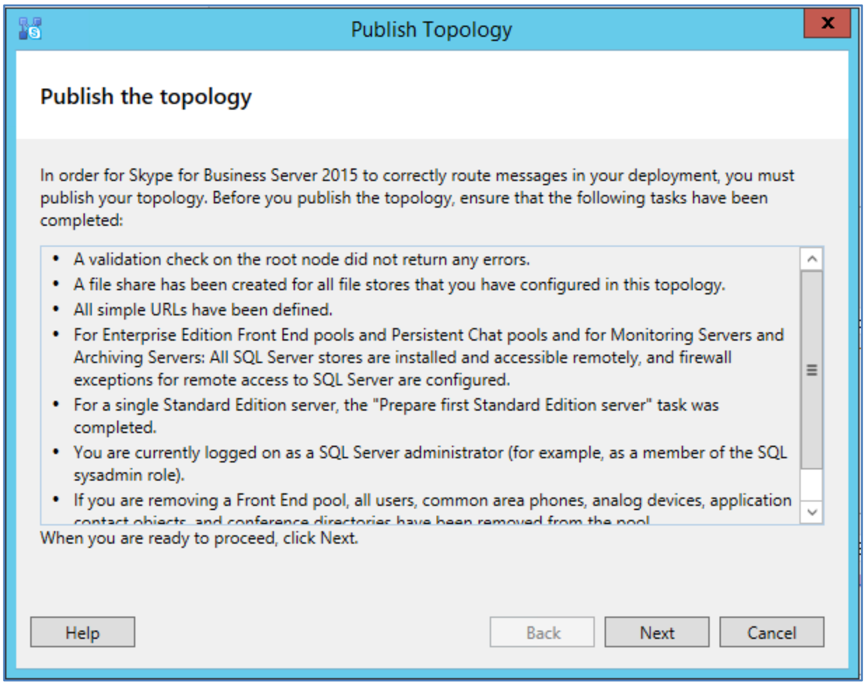
9. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



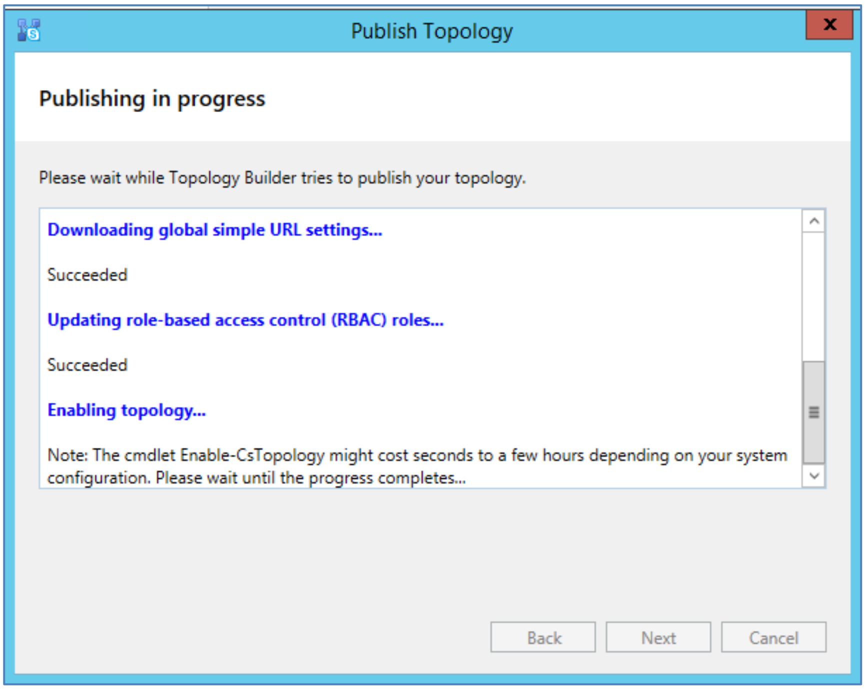
The following is displayed:

Figure 3-11: Publish the Topology



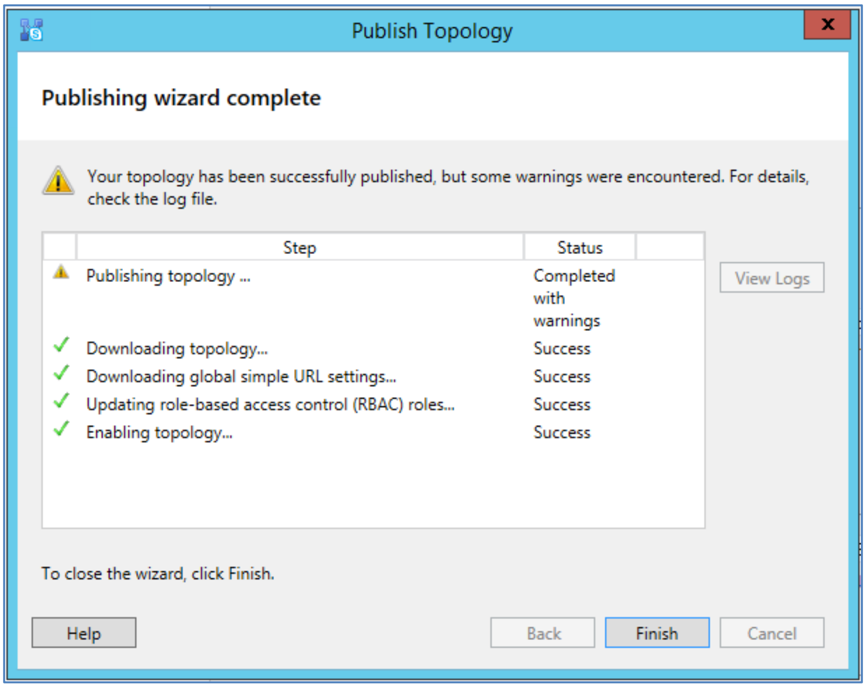
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



12. Click **Finish**.

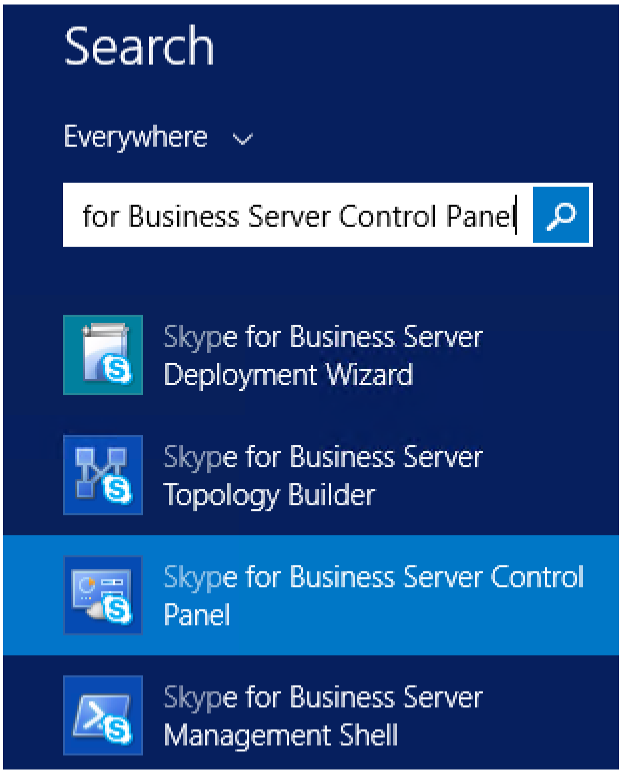
3.2 Configuring the "Route" on Skype for Business Server

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

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

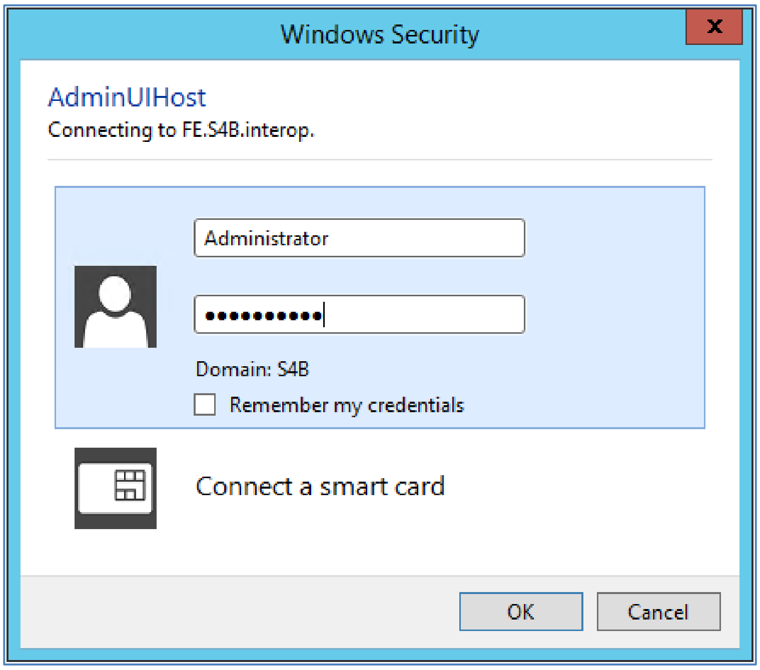
1. Start the Microsoft Skype for Business Server Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

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



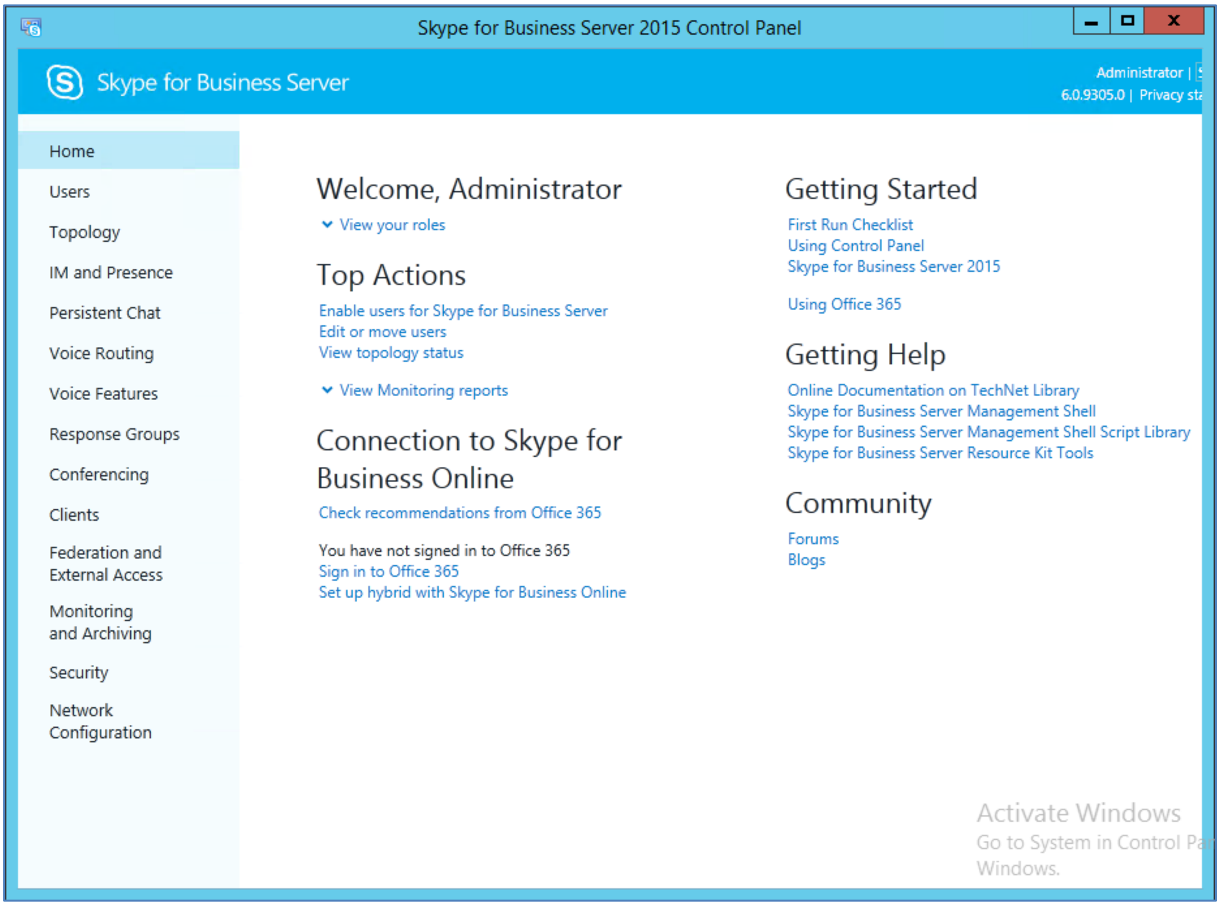
2. You are prompted to enter your login credentials:

Figure 3-15: Skype for Business Server Credentials



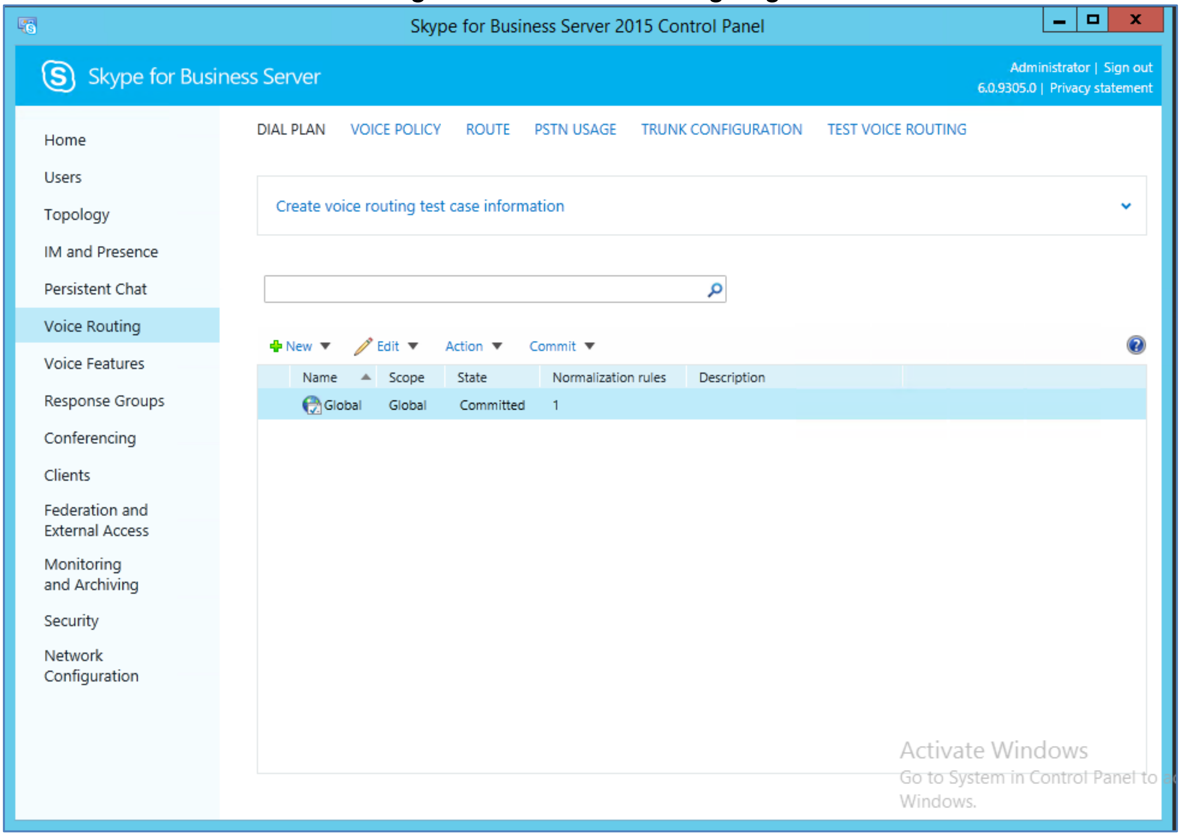
3. Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server Control Panel is displayed:

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



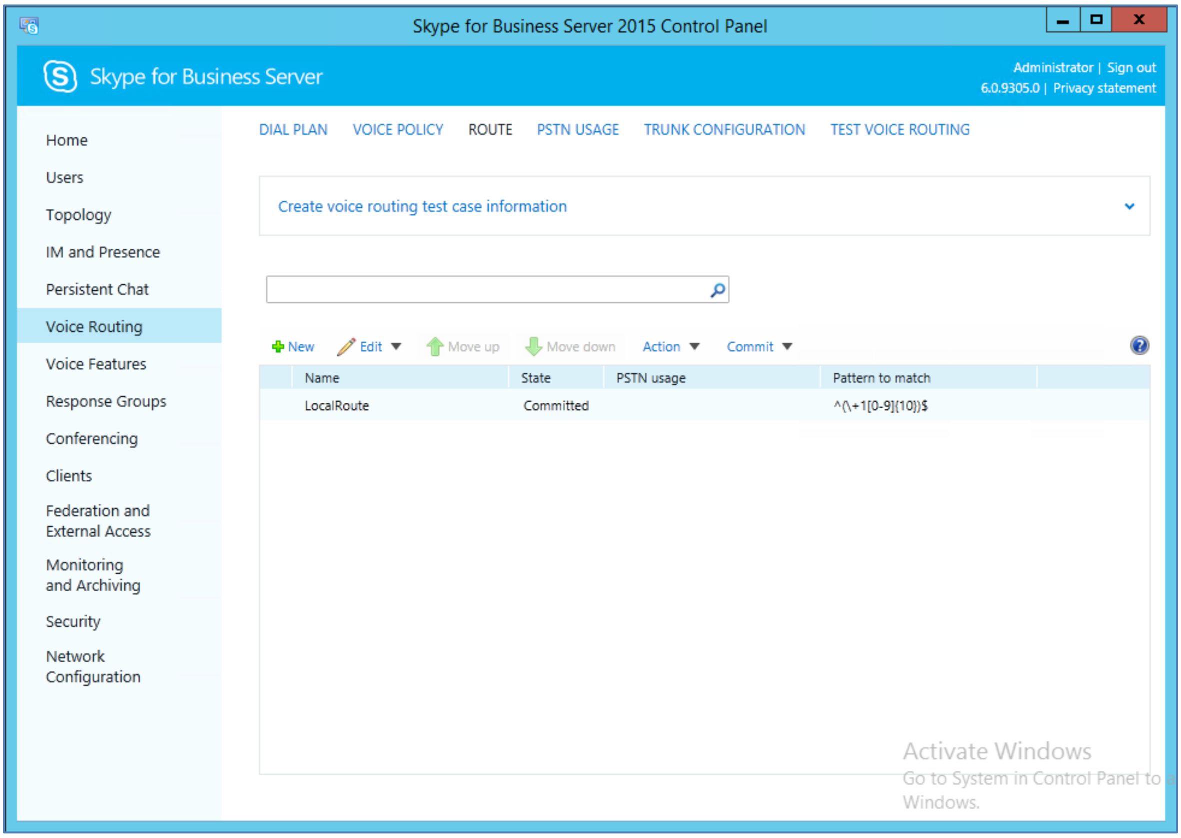
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



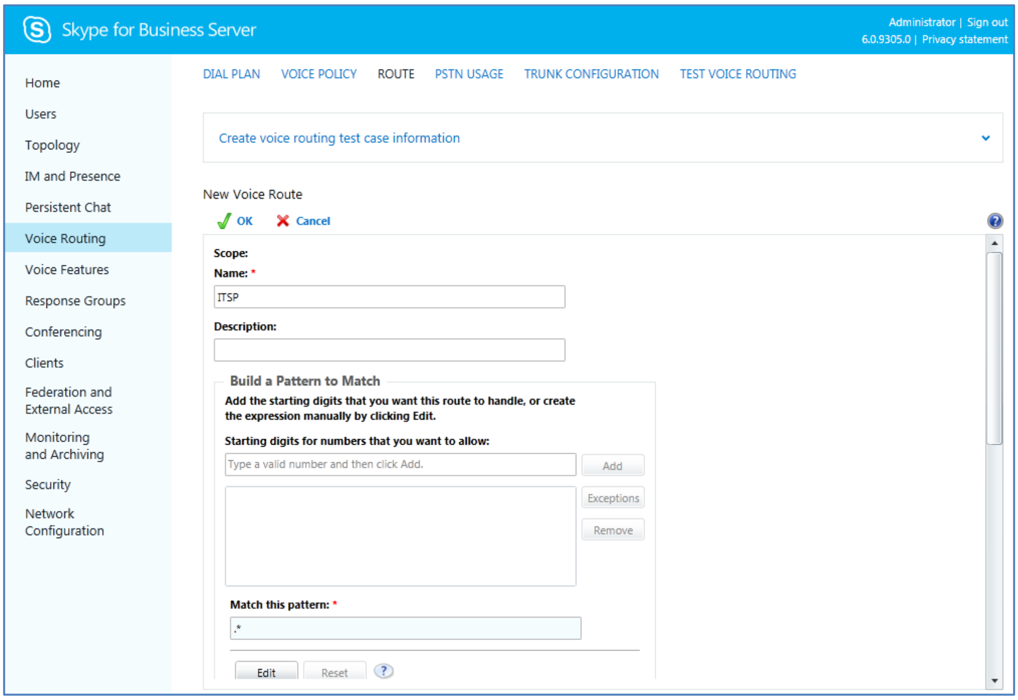
5. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



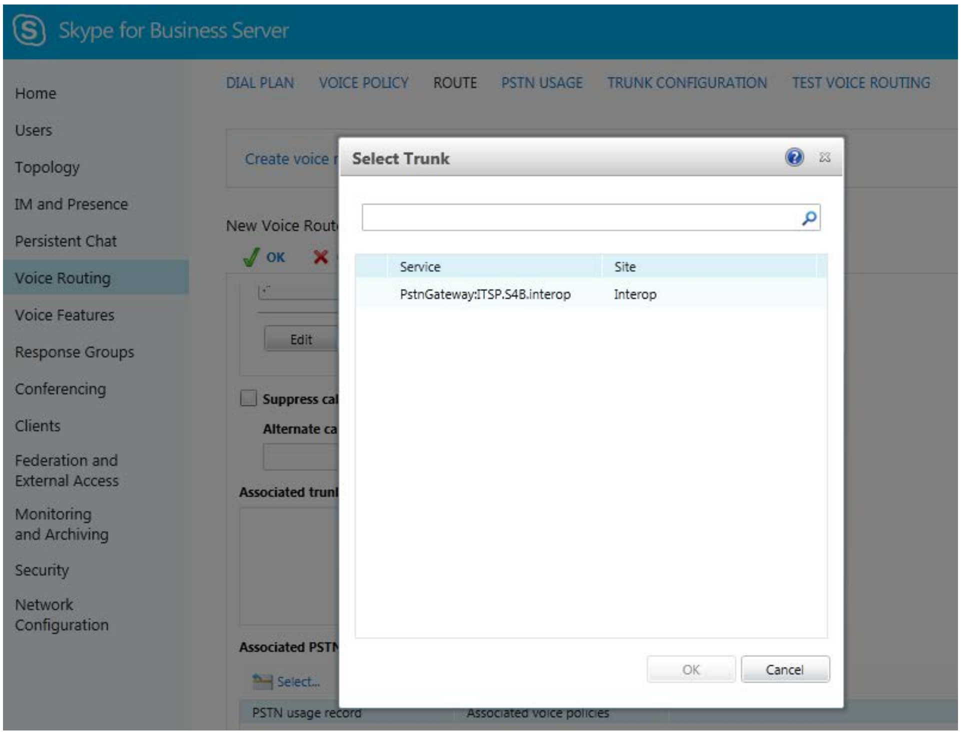
6. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



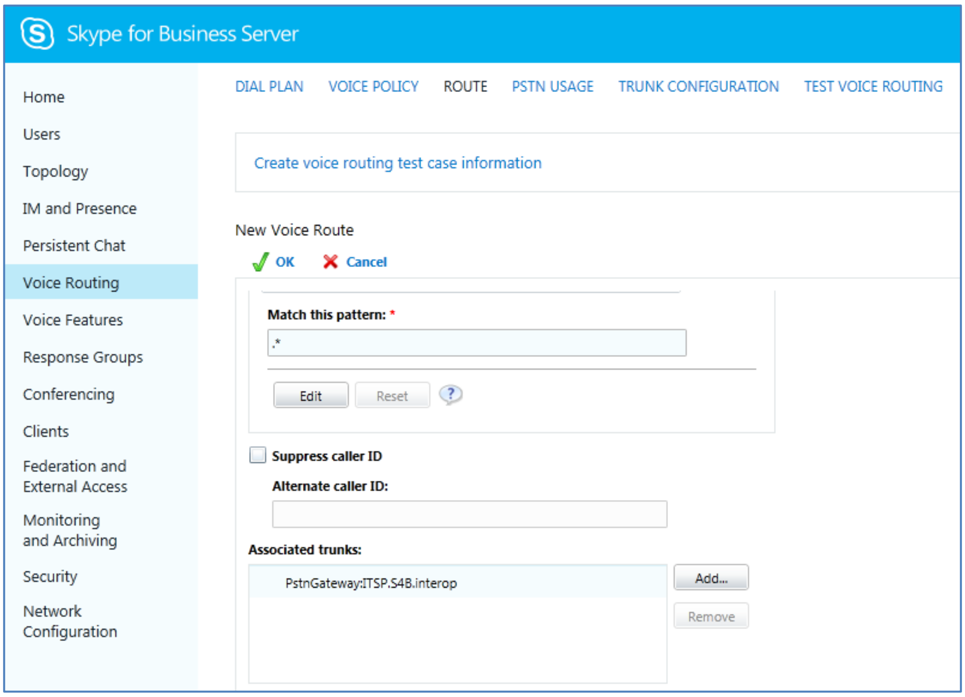
7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).
8. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.
9. Associate the route with the E-SBC Trunk that 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:

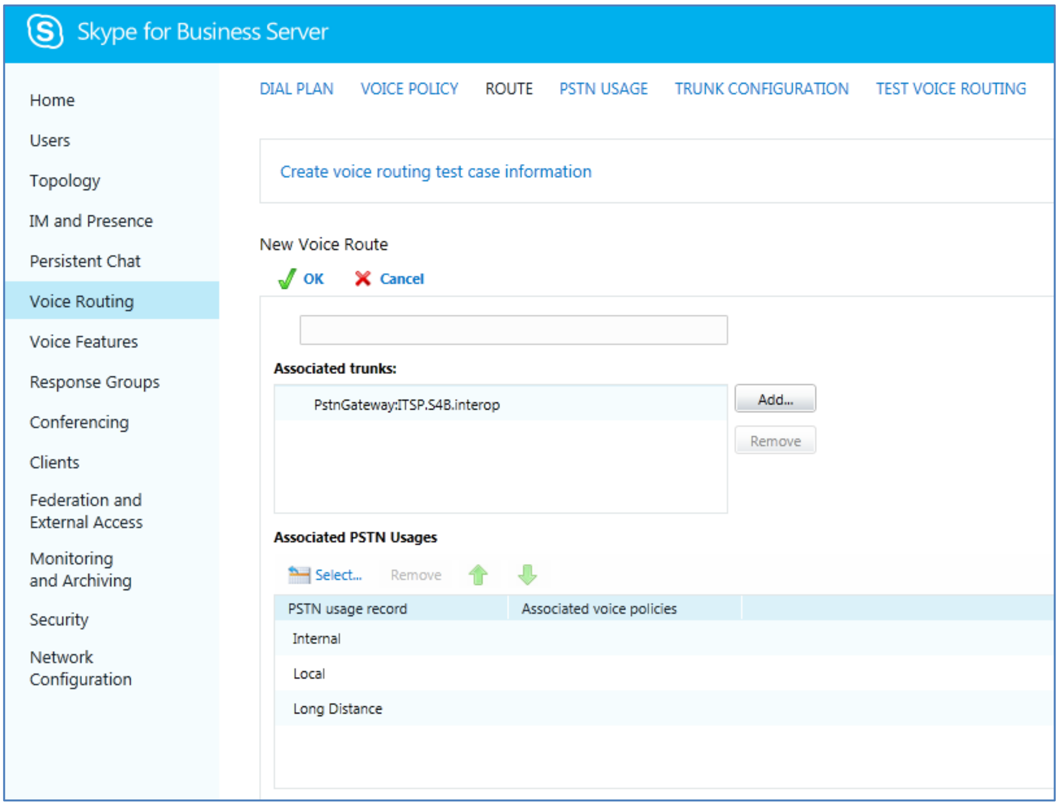
Figure 3-21: Selected E-SBC Trunk



10. Associate a PSTN Usage to this route:

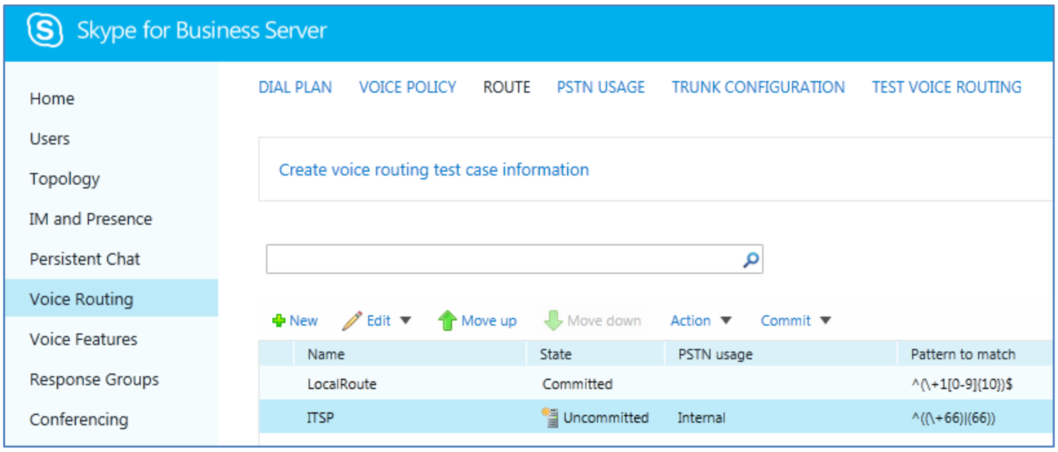
– Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-22: Associating PSTN Usage to Route



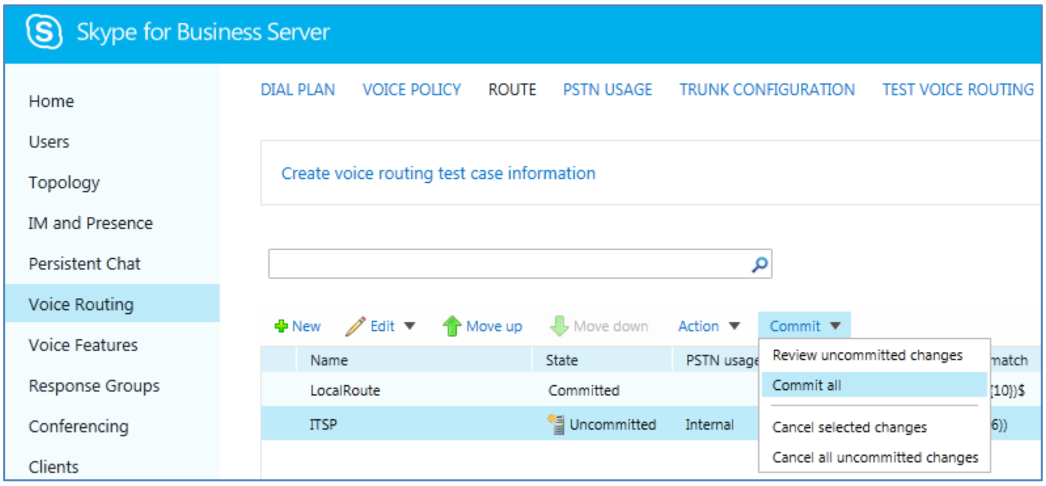
11. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-23: Confirmation of New Voice Route



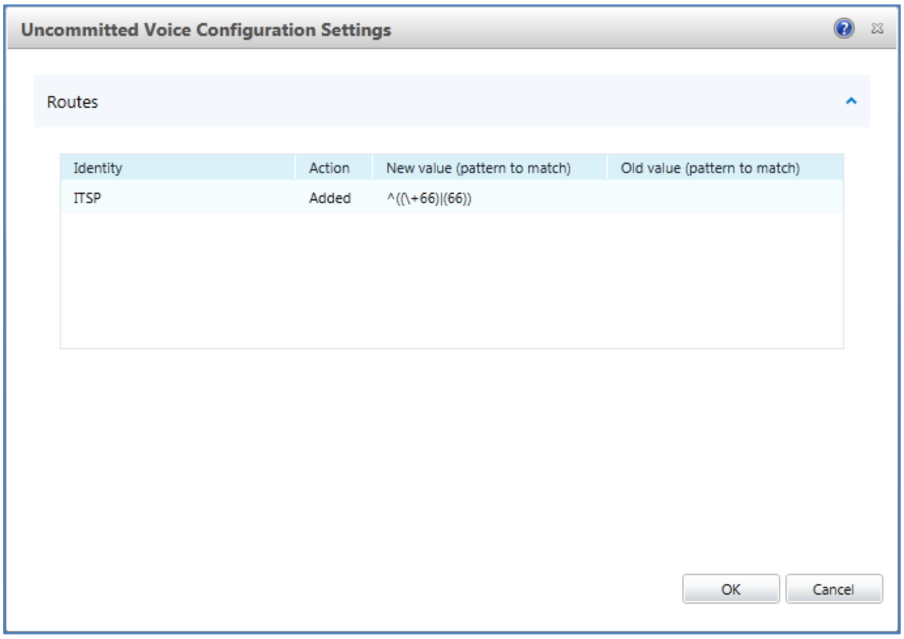
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-24: Committing Voice Routes



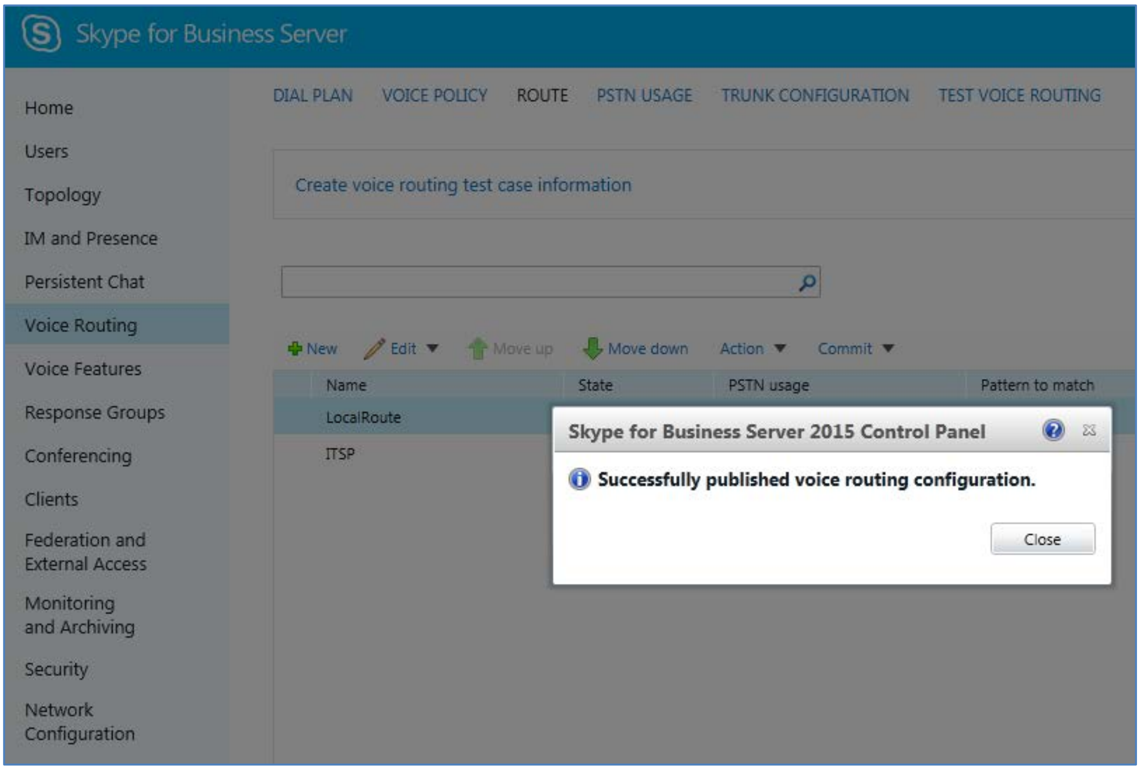
The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



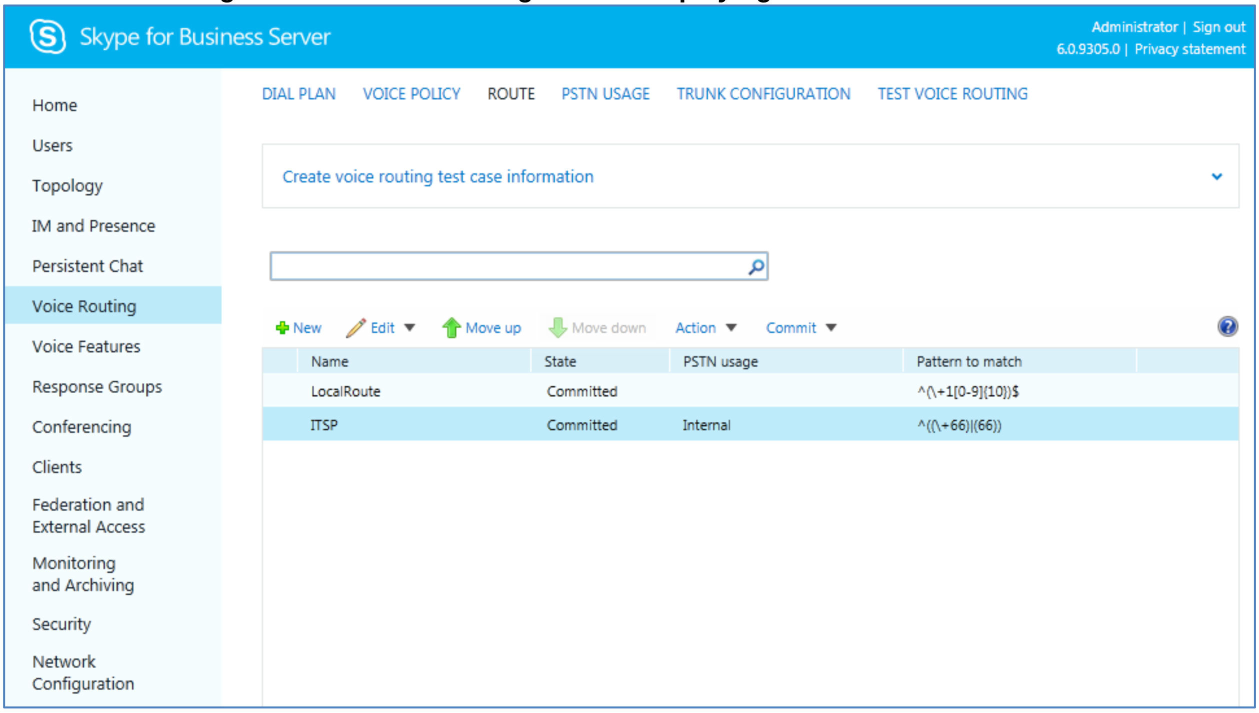
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

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

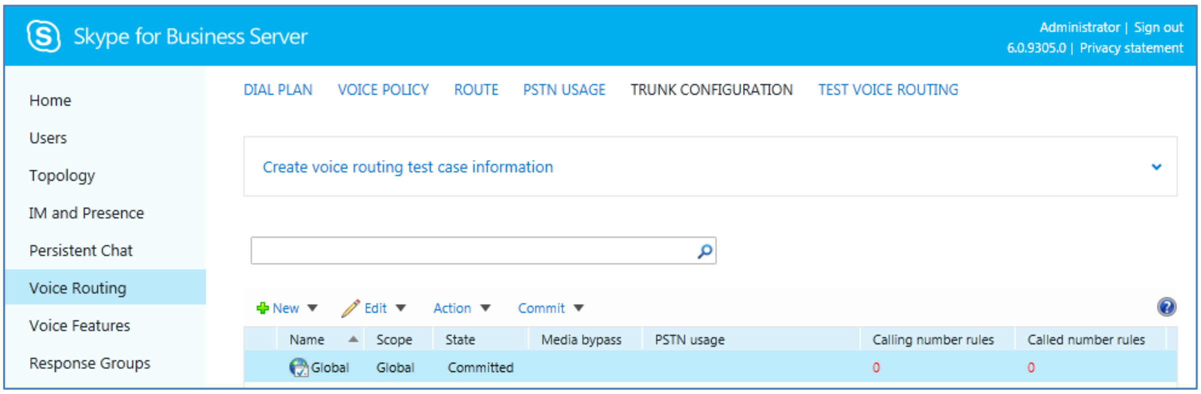


15. For ITSPs that implement a call identifier, continue with the following steps:

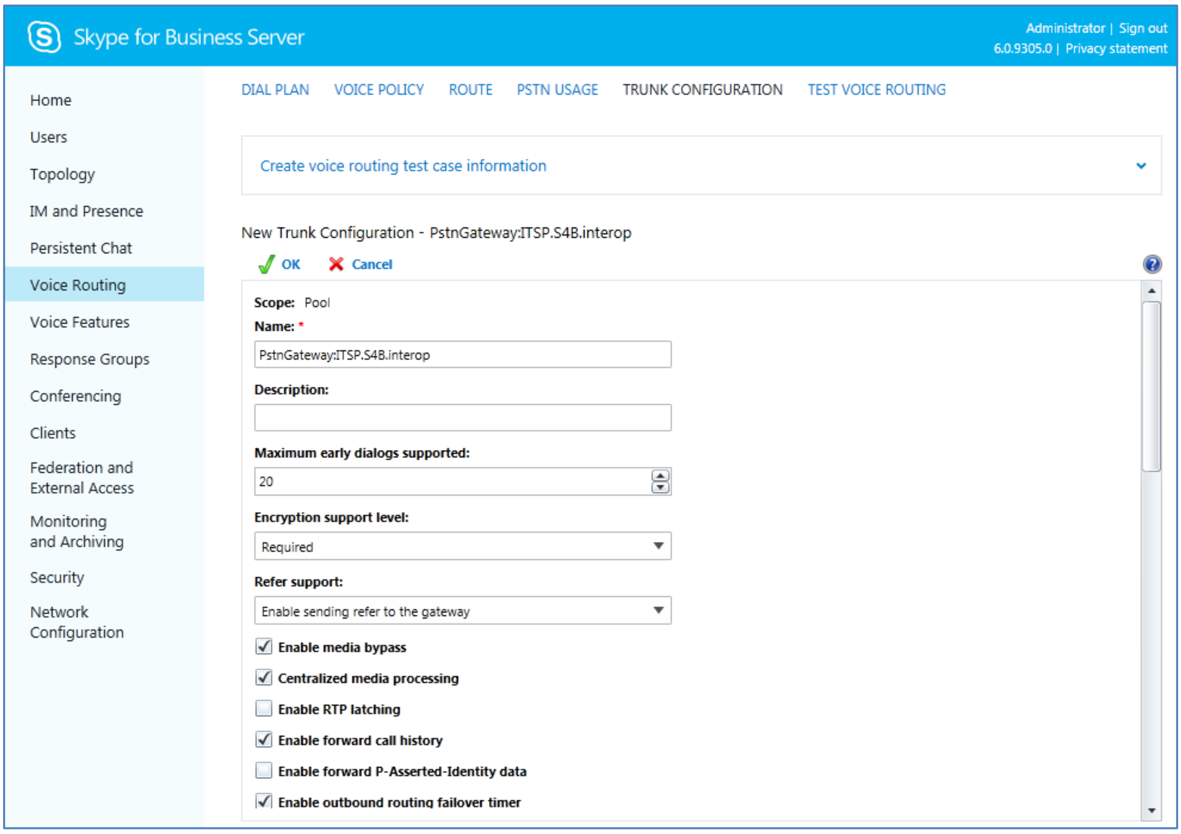
> **Note:** The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Skype for Business user number). This ID is required by EWE TEL SIP Trunk in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 4.5 on page 46).

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

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



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



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

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

16. Use the following command on the Skype for Business Server Management Shell after reconfiguration to verify correct values:

- **Get-CsTrunkConfiguration**

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

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

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Skype for Business Server and the EWE TEL 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 - EWE TEL SIP Trunking environment
- E-SBC LAN interface - Skype for Business Server 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 EWE TEL SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a License Key that includes the following software features:
  - √ **Microsoft**
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

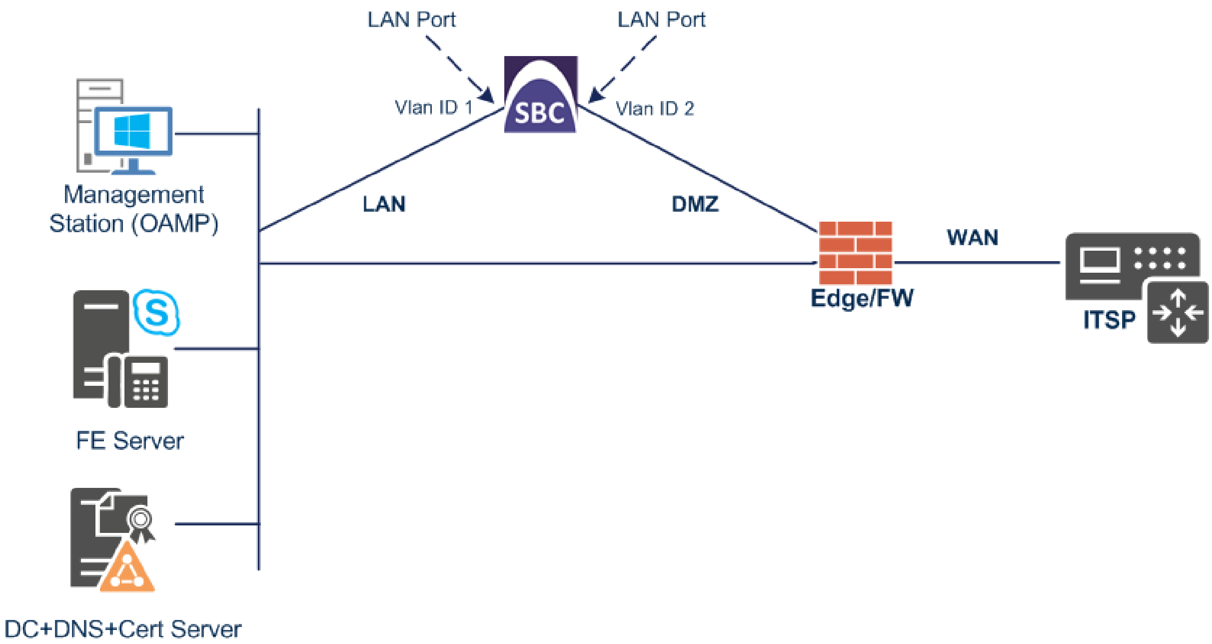
  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site

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

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

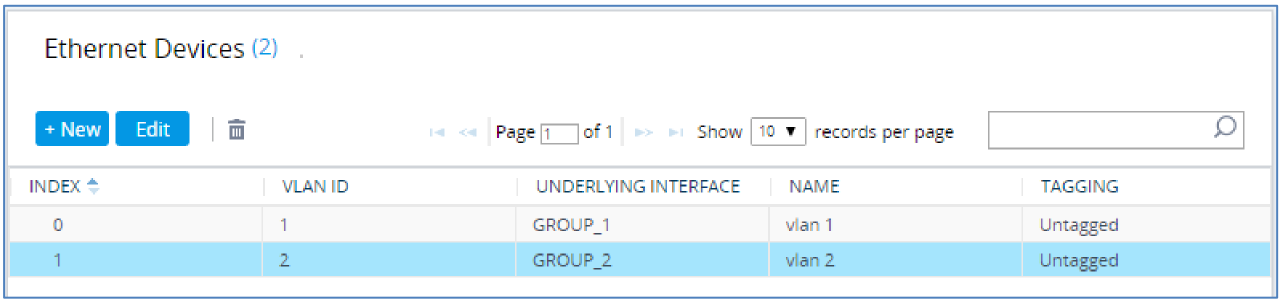
- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **To configure the VLANs:**

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

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

Figure 4-2: Configured VLAN IDs in Ethernet Device



4.1.2 Step 1b: Configure Network Interfaces

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

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

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

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

Parameter	Value

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

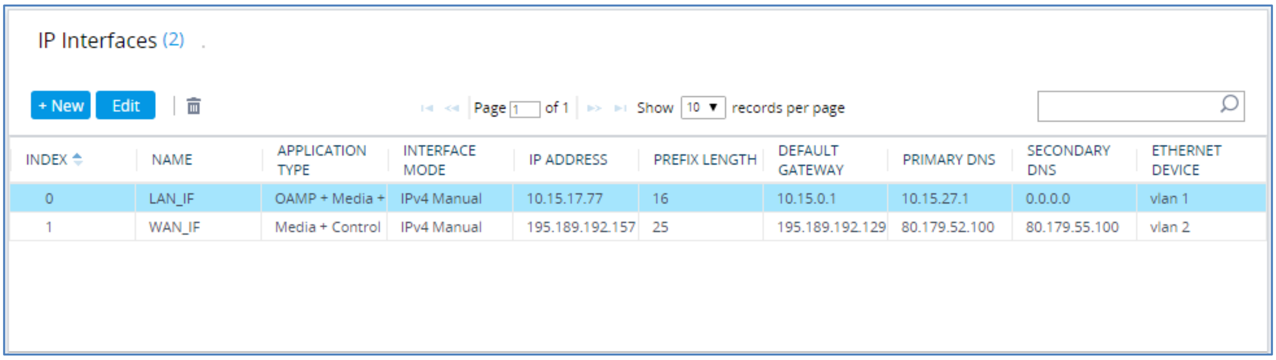
3. Add a network interface for the WAN side:
   a. Click **New**.
   b. Configure the interface as follows:

Parameter	Value
Name	**WAN_IF**
Application Type	**Media + Control**
Ethernet Device	**vlan 2**
IP Address	**195.189.192.157** (DMZ IP address of E-SBC)
Prefix Length	**25** (subnet mask in bits for 255.255.255.128)
Default Gateway	**195.189.192.129** (router's IP address)
Primary DNS	**80.179.52.100**
Secondary DNS	**80.179.55.100**

4. Click **Apply**.

The configured IP network interfaces are shown below:

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


IP Interfaces (2)

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

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

4.2 Step 2: Configure Media Realms

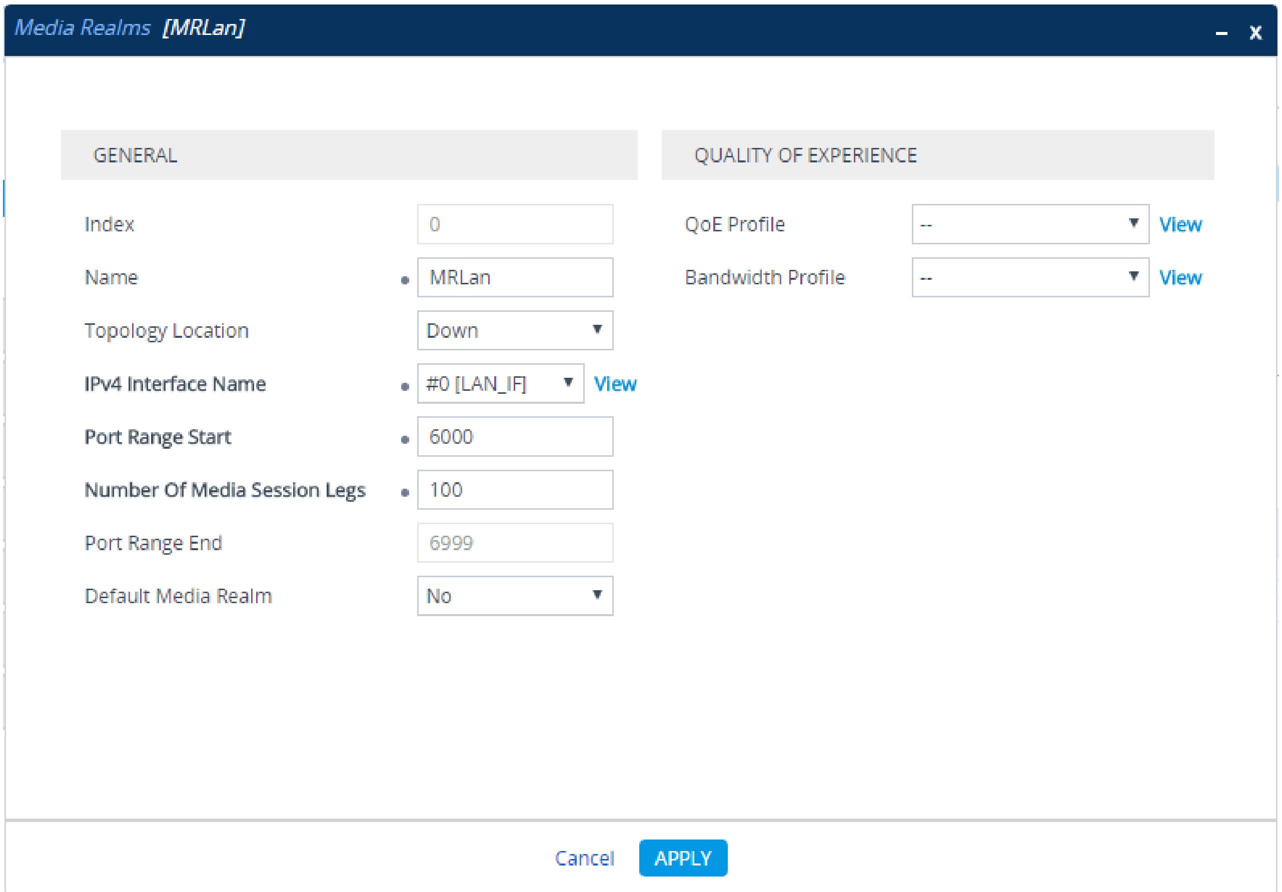
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

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

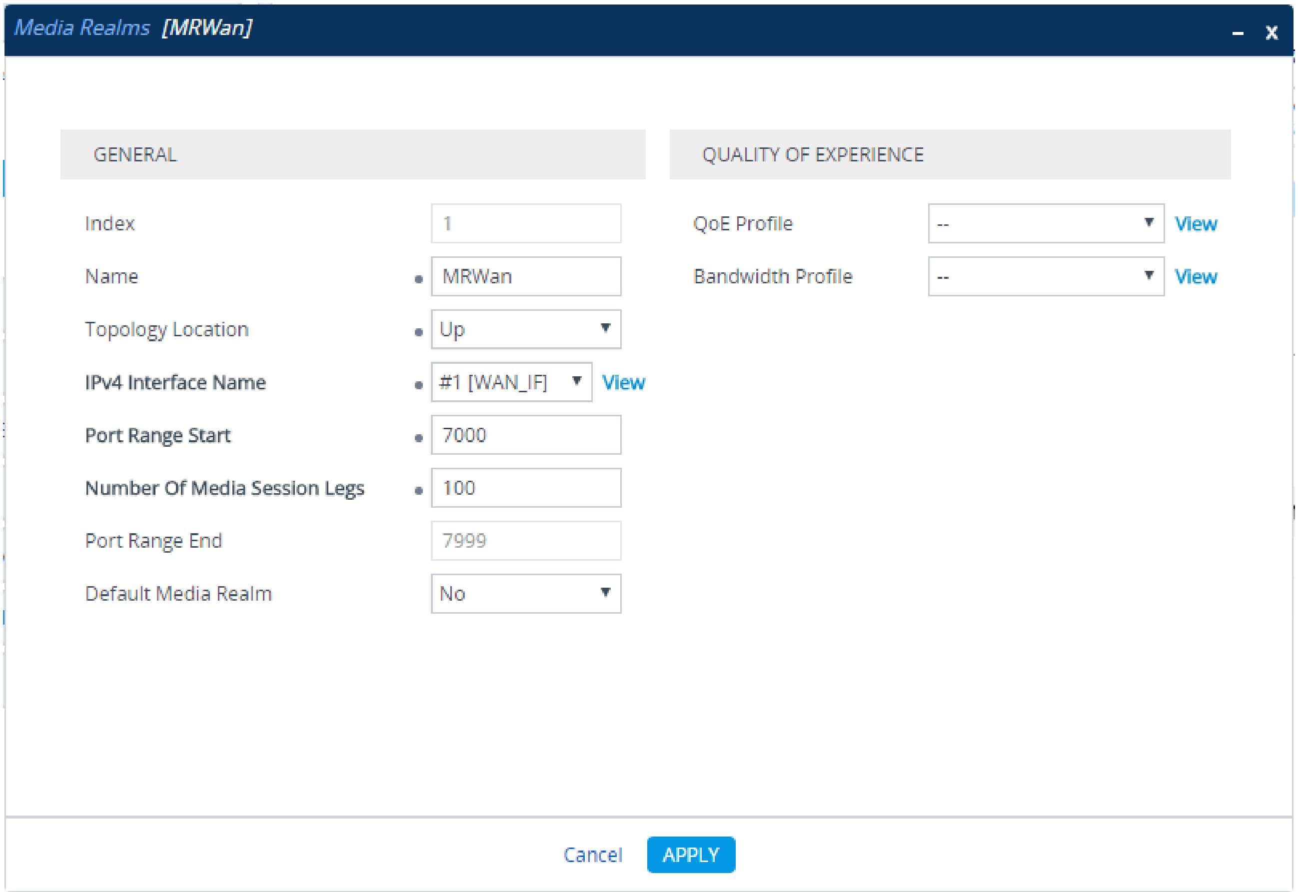
Figure 4-4: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

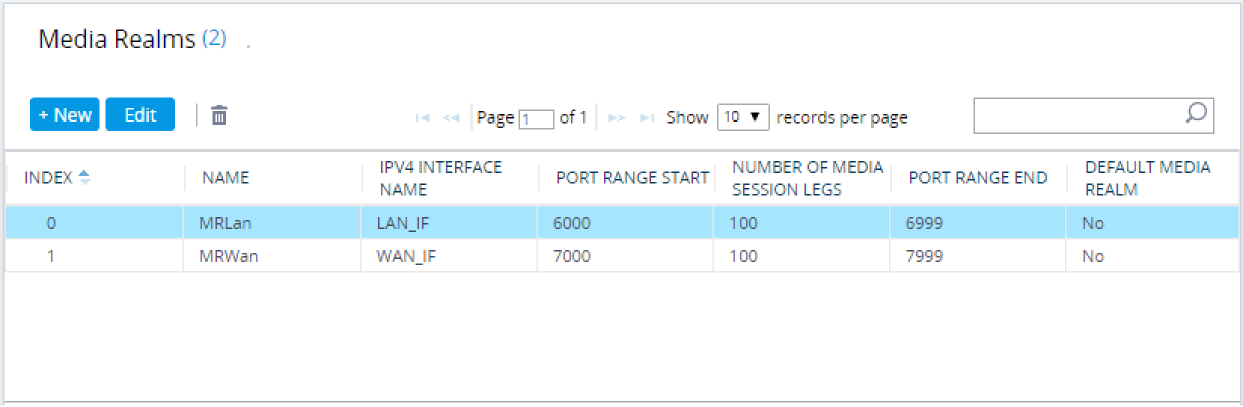
Parameter	Value
Index	**1**
Name	**MRWan** (arbitrary name)
Topology Location	**Up**
IPv4 Interface Name	**WAN_IF**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-5: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

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



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

4.3 Step 3: Configure SIP Signaling Interfaces

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

➤ **To configure SIP Interfaces:**

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

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

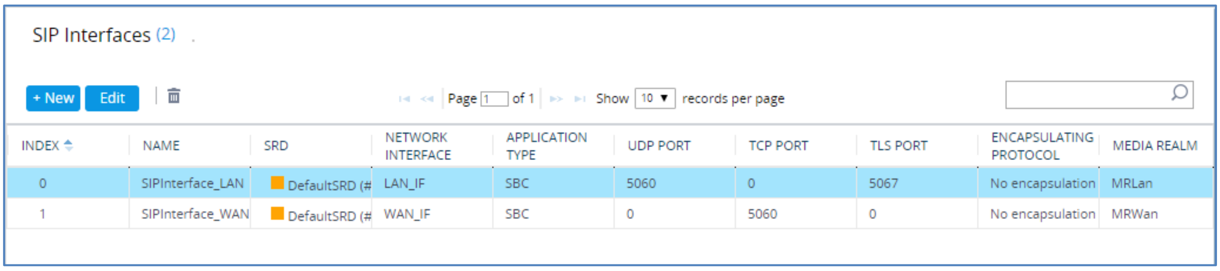
Note: The TLS port parameter must be identically configured in the Skype for Business Topology Builder (see Section 3.1 on page 13).

3. Configure a SIP Interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

Figure 4-7: Configured SIP Interfaces in SIP Interface Table



INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SIPInterface_LAN	DefaultSRD (#	LAN_IF	SBC	5060	0	5067	No encapsulation	MRLan
1	SIPInterface_WAN	DefaultSRD (#	WAN_IF	SBC	0	5060	0	No encapsulation	MRWan

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

4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Skype for Business Server
- EWE TEL SIP Trunk
- Fax supporting ATA device (optional)

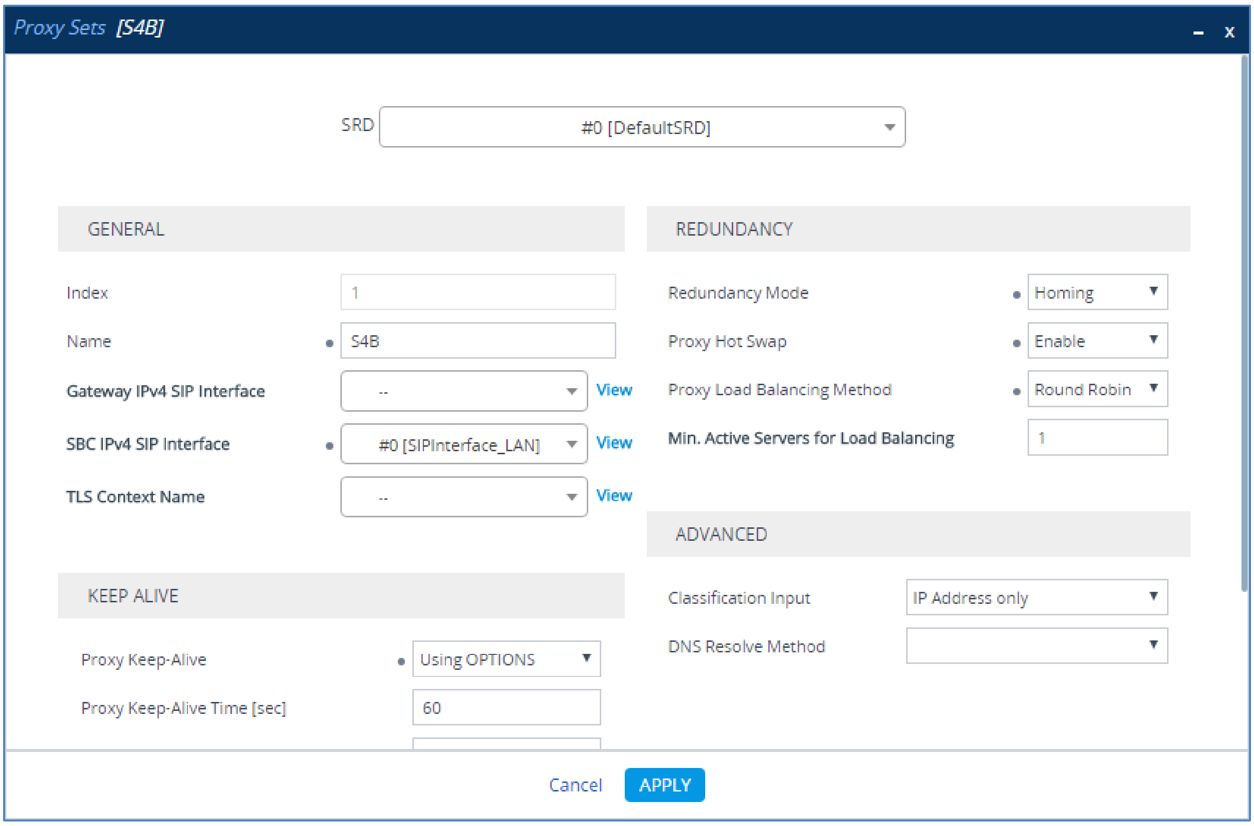
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).
2. Add a Proxy Set for the Skype for Business Server as shown below:

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

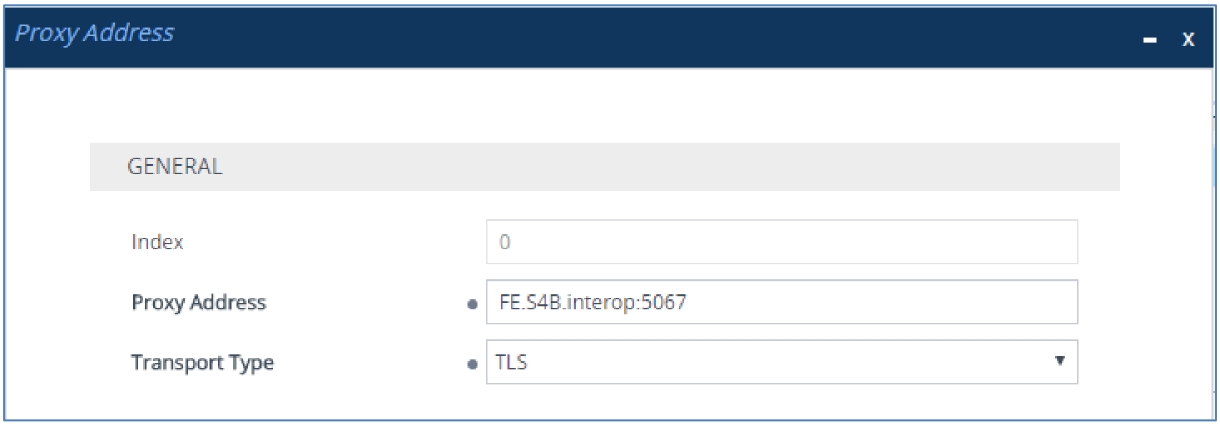
Figure 4-8: Configuring Proxy Set for Microsoft Skype for Business Server



a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.

b. Click **New**; the following dialog box appears:

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



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

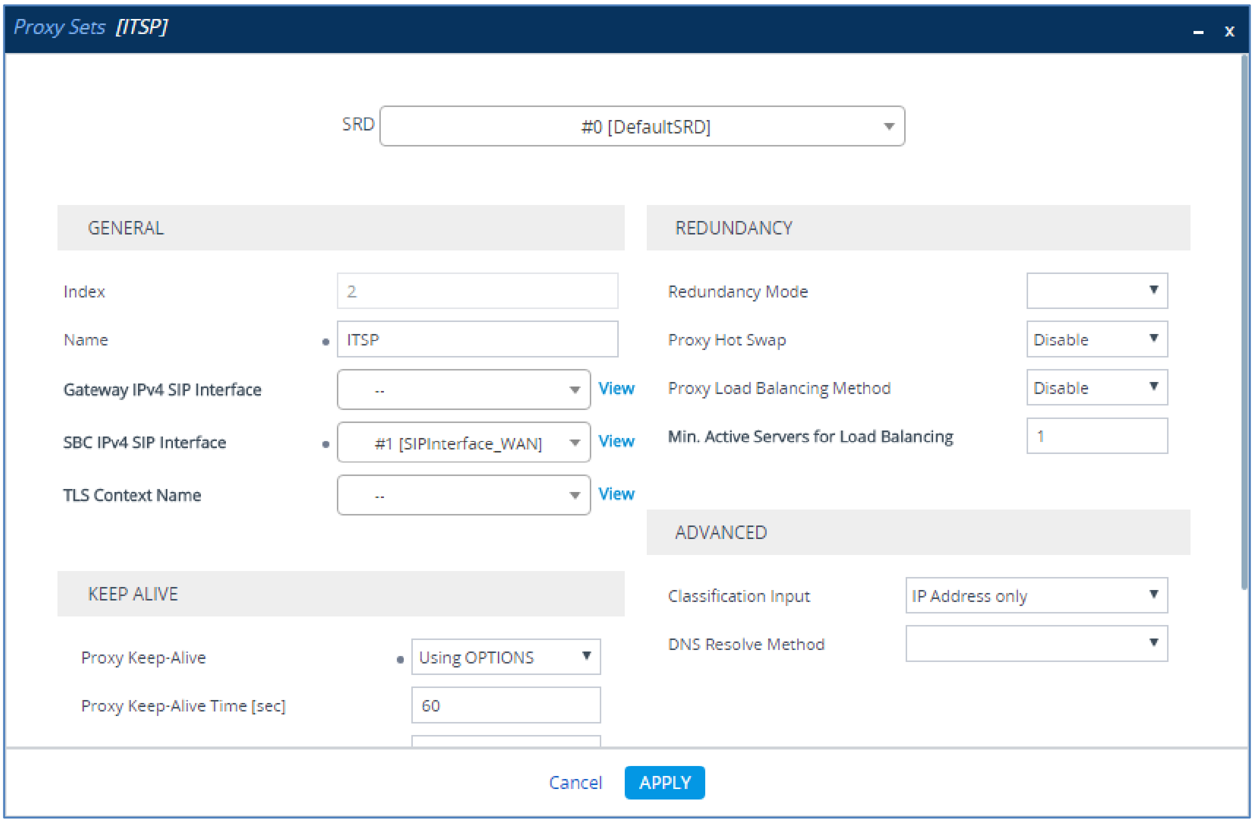
d. Click **Apply**.

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

3. Configure a Proxy Set for the EWE TEL SIP Trunk:

Parameter	Value
Index	**2**
Name	**ITSP**
SBC IPv4 SIP Interface	**SIPInterface_WAN**
Proxy Keep-Alive	**Using Options**

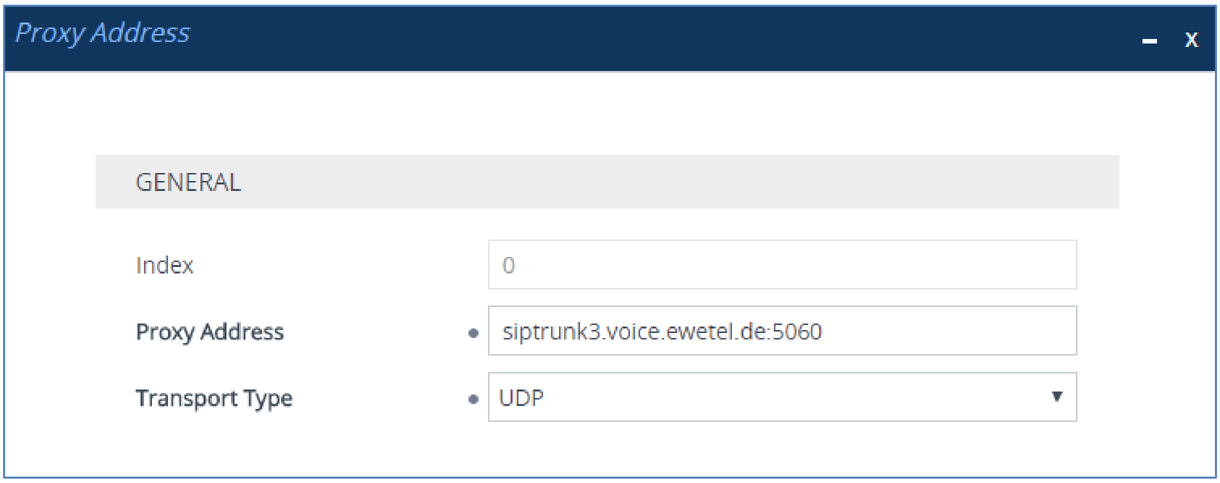
Figure 4-10: Configuring Proxy Set for EWE TEL SIP Trunk



a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.

b. Click **New**; the following dialog box appears:

Figure 4-11: Configuring Proxy Address for EWE TEL SIP Trunk



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

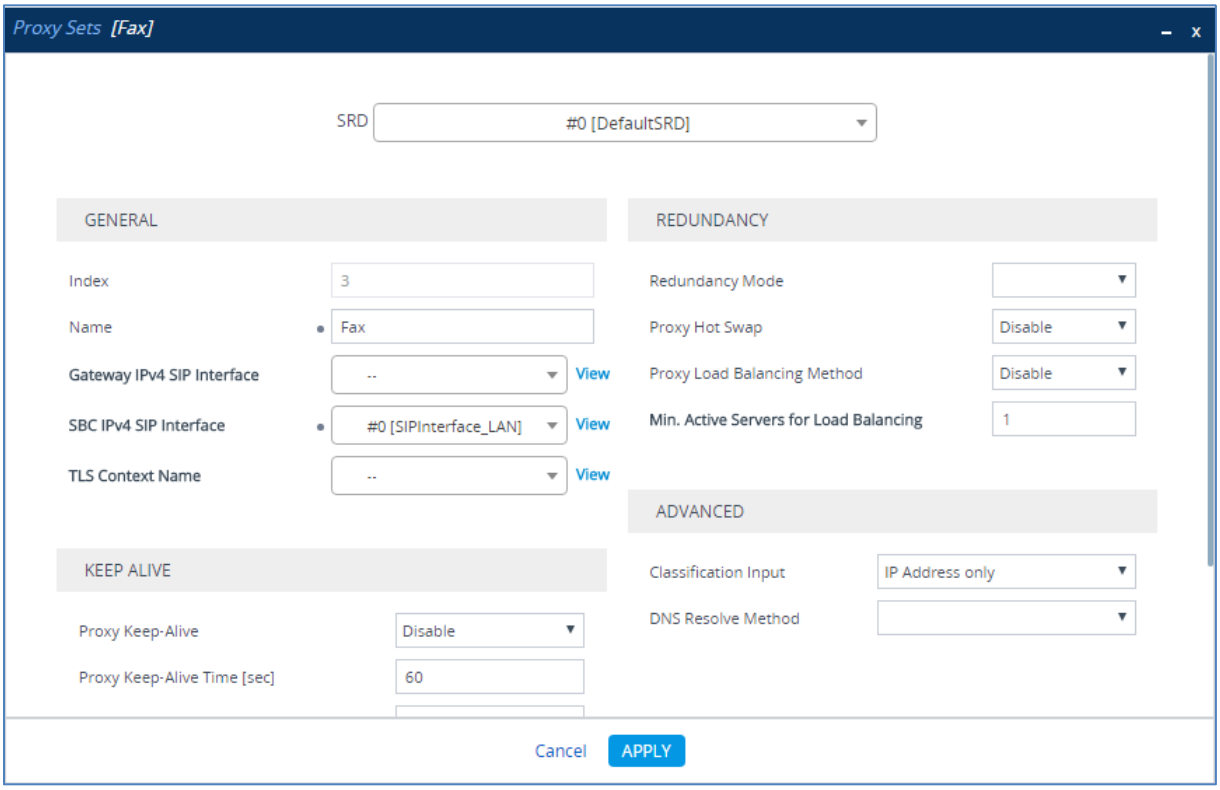
d. Click **Apply**.

Parameter	Value
Index	**0**
Proxy Address	**siptrunk3.voice.ewetel.de:5060** (FQDN and destination port)
Transport Type	**UDP**

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

Parameter	Value
Index	**3**
Name	**Fax**
SBC IPv4 SIP Interface	**SIPInterface_LAN**

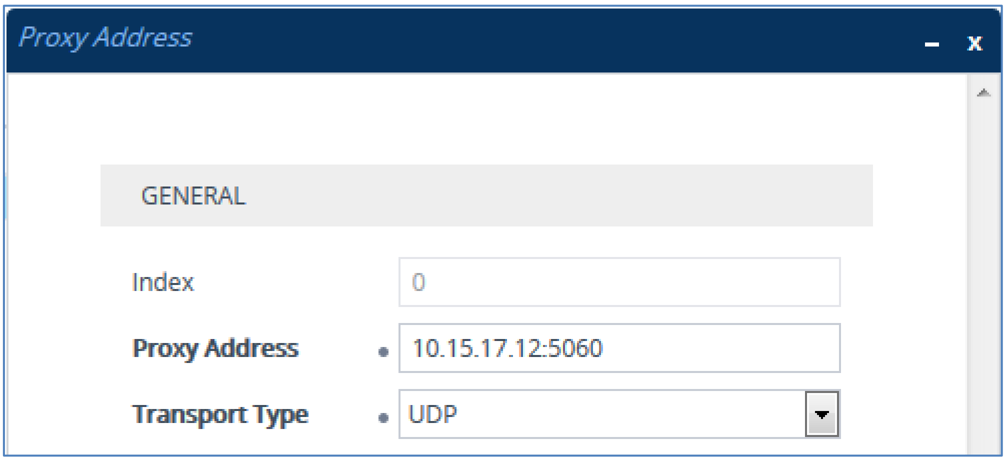
Figure 4-12: Configuring Proxy Set for Fax ATA device



a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.

b. Click **New**; the following dialog box appears:

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



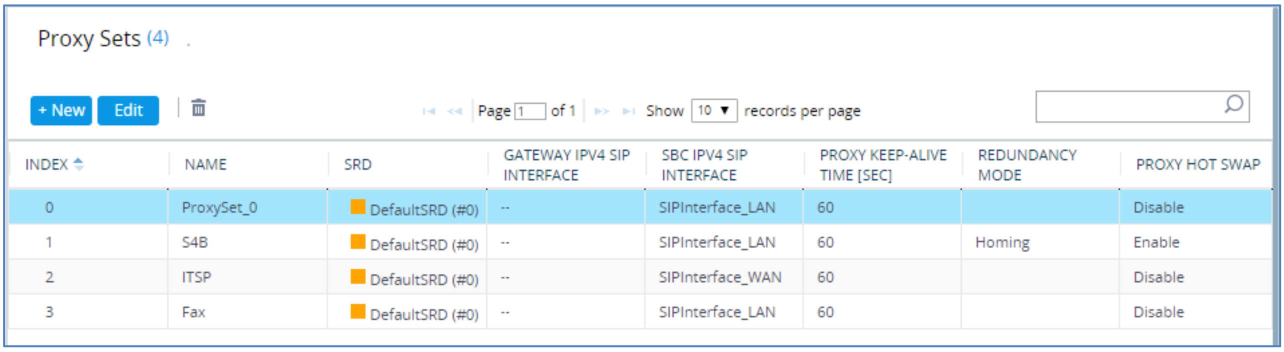
c. Configure the address of the Proxy Set according to the parameters described in the table below.

d. Click **Apply**.

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

The configured Proxy Sets are shown in the figure below:

Figure 4-14: Configured Proxy Sets in Proxy Sets Table



Proxy Sets (4)

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

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	SIPInterface_LAN	60		Disable
1	S4B	DefaultSRD (#0)	--	SIPInterface_LAN	60	Homing	Enable
2	ITSP	DefaultSRD (#0)	--	SIPInterface_WAN	60		Disable
3	Fax	DefaultSRD (#0)	--	SIPInterface_LAN	60		Disable

4.5 Step 5: Configure Coders

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

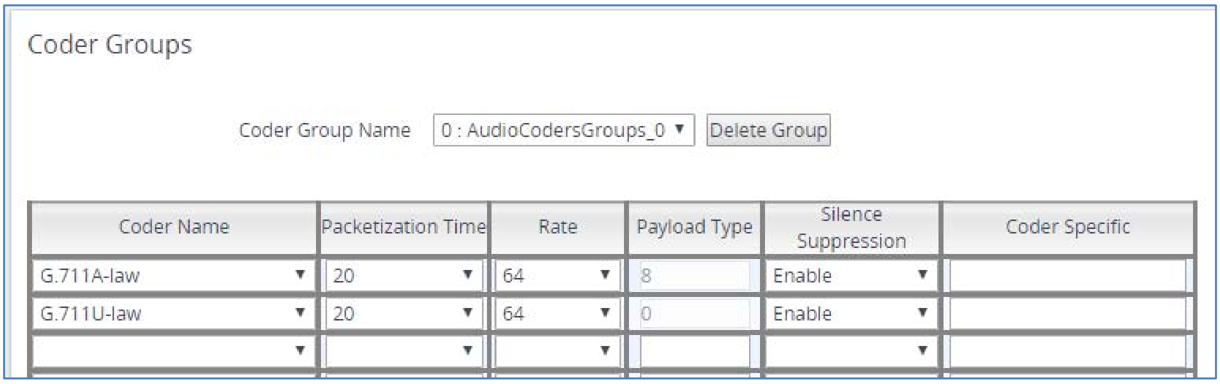
Note that the Coder Group ID for this entity will be assign to its corresponding IP Profile in the next step.

➢ **To configure coders:**

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

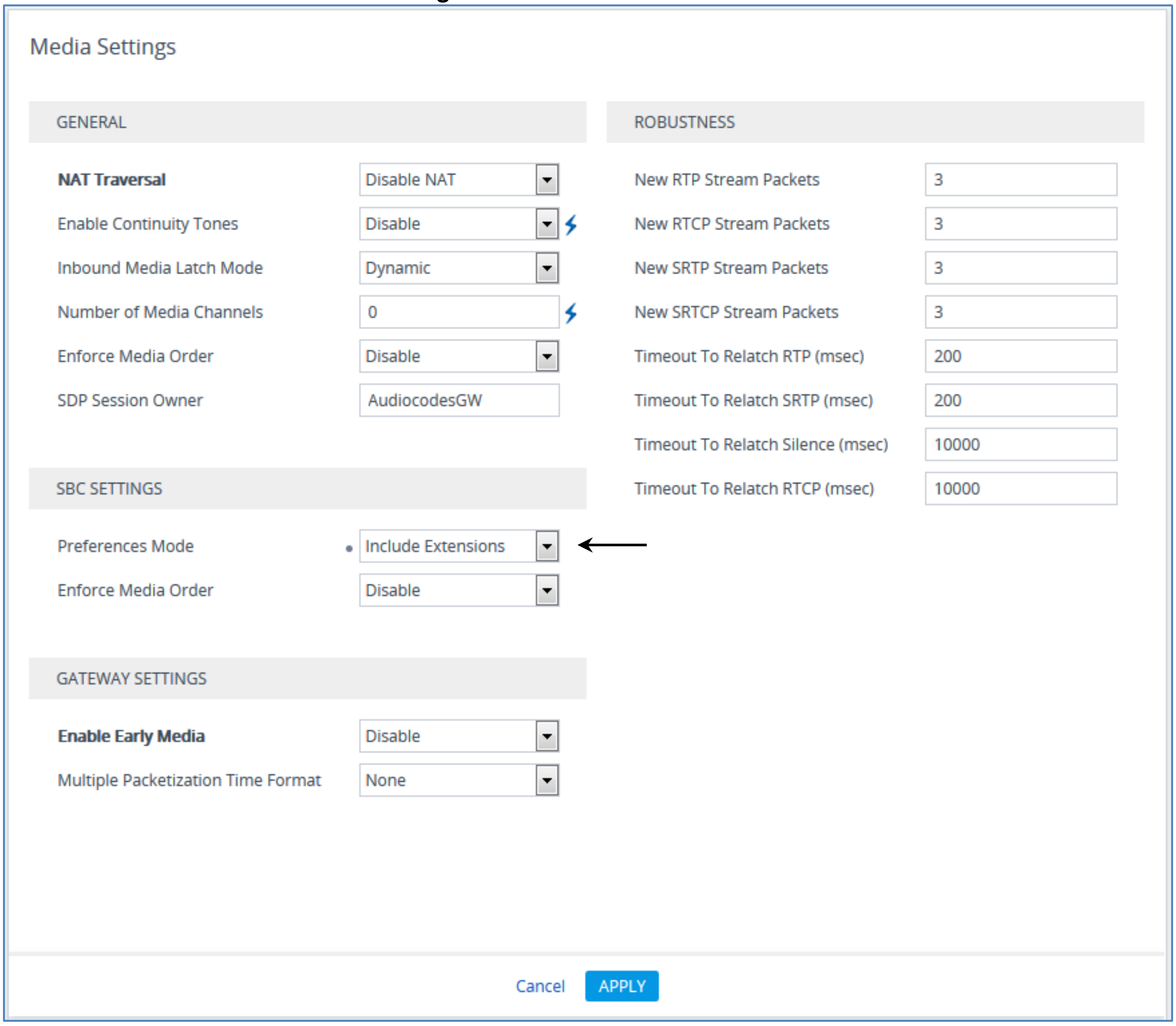
Parameter	Value
Coder Group Name	**AudioCodersGroups_0**
Coder Name	▪ **G.711 A-law** ▪ **G.711 U-law**
Silence Suppression	**Enable** (for both coders)

Figure 4-15: Configuring Coder Group for Skype for Business Server



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

Figure 4-16: SBC Preferences Mode



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

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 – to operate in secure mode using SRTP and SIP over TLS
- EWE TEL SIP trunk – to operate in non-secure mode using RTP and SIP over UDP
- Fax ATA device – to operate in non-secure mode using RTP and SIP over UDP

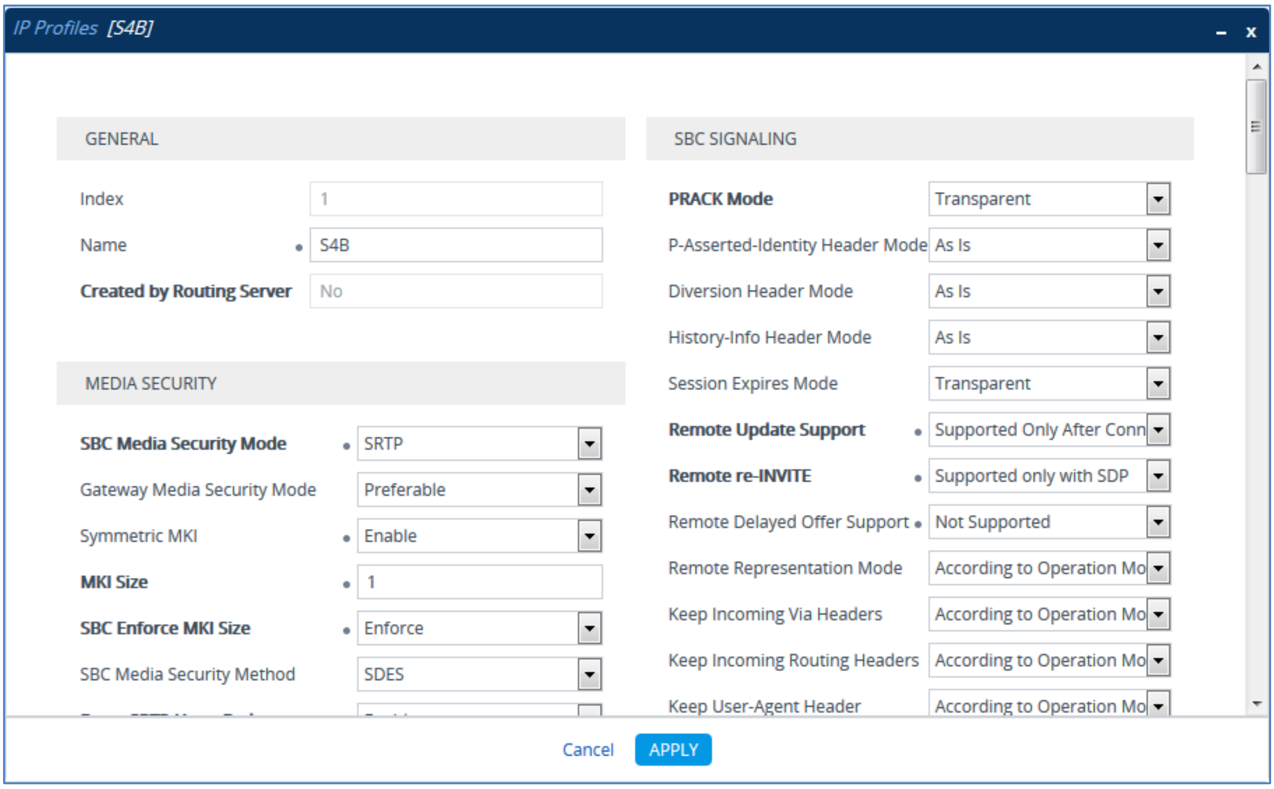
➢ **To configure IP Profile for the Skype for Business Server:**

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

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

SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally** (required, as Skype for Business Server does not support receipt of SIP REFER)
Remote 3xx Mode	**Handle Locally** (required, as Skype for Business Server does not support receipt of SIP 3xx responses)

Figure 4-17: Configuring IP Profile for Skype for Business Server



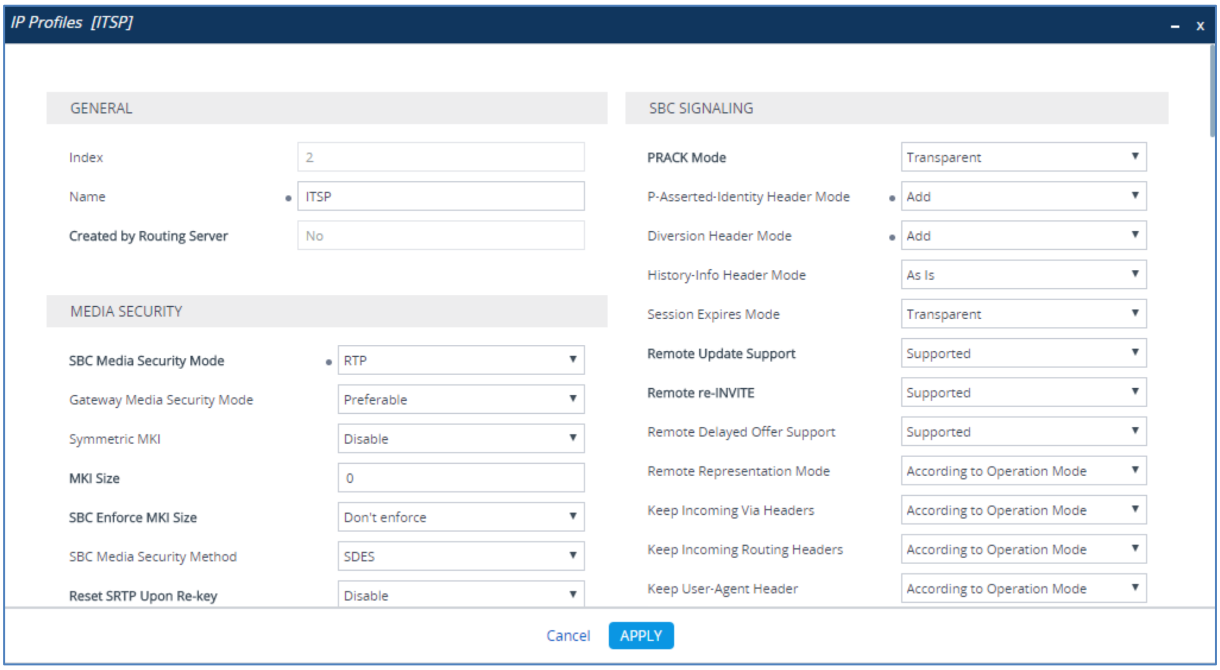
3. Click **Apply**.

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

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

Parameter	Value
General	
Index	**2**
Name	**ITSP**
Media Security	
SBC Media Security Mode	**RTP**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media** (required to overcome a problem when a ringback tone is not sent from the ITSP)
Remote Can Play Ringback	**No** (required, as Skype for Business Server does not provide a ringback tone for incoming calls)
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Diversion Header Mode	**Add** (required for call forwarding)
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally** (required, as Skype for Business Server does not support receipt of SIP REFER)
Play RBT To Transferee	**Yes** (required for call transfer)
Remote 3xx Mode	**Handle Locally**

Figure 4-18: Configuring IP Profile for EWE TEL SIP Trunk



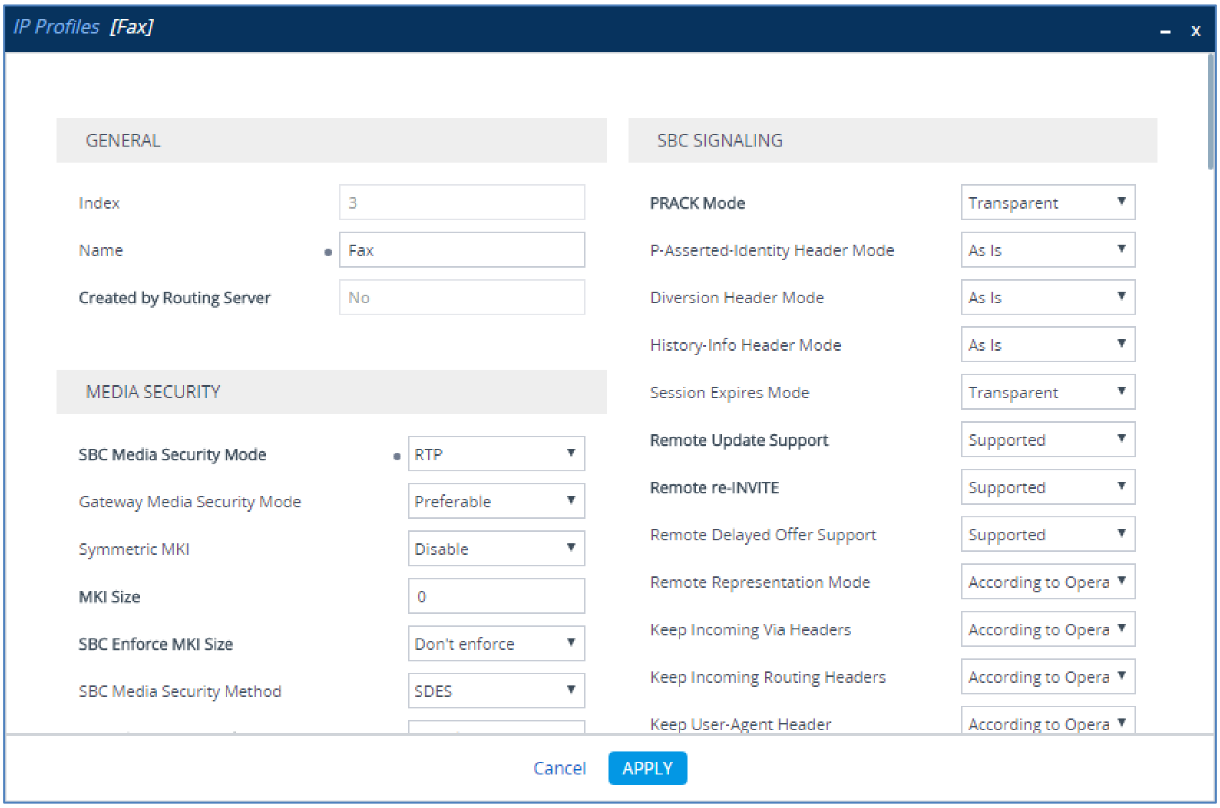
2. Click **Apply**.

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

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

Parameter	Value
General	
Index	**3**
Name	**Fax**
Media Security	
SBC Media Security Mode	**RTP**
Media	
Broken Connection Mode	**Ignore**

Figure 4-19: Configuring IP Profile for FAX ATA



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

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 (Mediation Server) located on LAN
- EWE TEL SIP Trunk located on WAN
- Fax supporting ATA device located on LAN (if required)

➢ **To configure IP Groups:**

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

Parameter	Value
Index	**1**
Name	**S4B**
Type	**Server**
Proxy Set	**S4B**
IP Profile	**S4B**
Media Realm	**MRLan**
SIP Group Name	**siptrunk3.voice.ewetel.de** (according to ITSP requirement)

3. Configure an IP Group for the EWE TEL SIP Trunk:

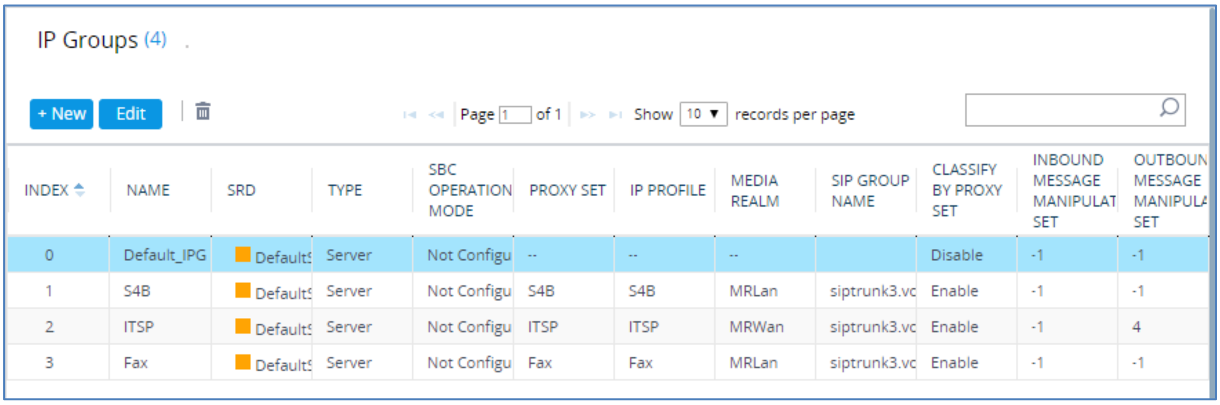
Parameter	Value
Index	**2**
Name	**ITSP**
Topology Location	**Up**
Type	**Server**
Proxy Set	**ITSP**
IP Profile	**ITSP**
Media Realm	**MRWan**
SIP Group Name	**siptrunk3.voice.ewetel.de** (according to ITSP requirement)

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

Parameter	Value
Index	**2**
Name	**Fax**
Type	**Server**
Proxy Set	**Fax**
IP Profile	**Fax**
Media Realm	**MRLan**
SIP Group Name	**siptrunk3.voice.ewetel.de** (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

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



4.8 Step 8: SIP TLS Connection Configuration

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

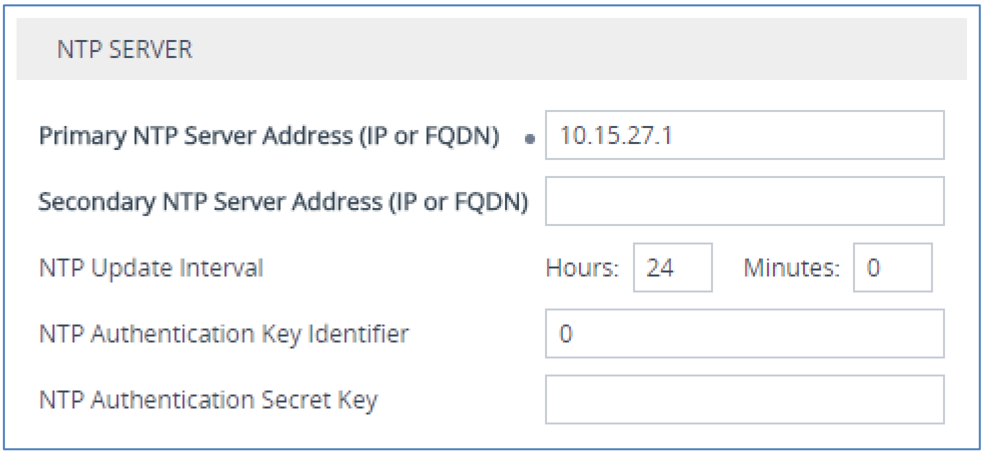
4.8.1 Step 8a: Configure the NTP Server Address

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

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

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

Figure 4-21: Configuring NTP Server Address



3. Click **Apply**.

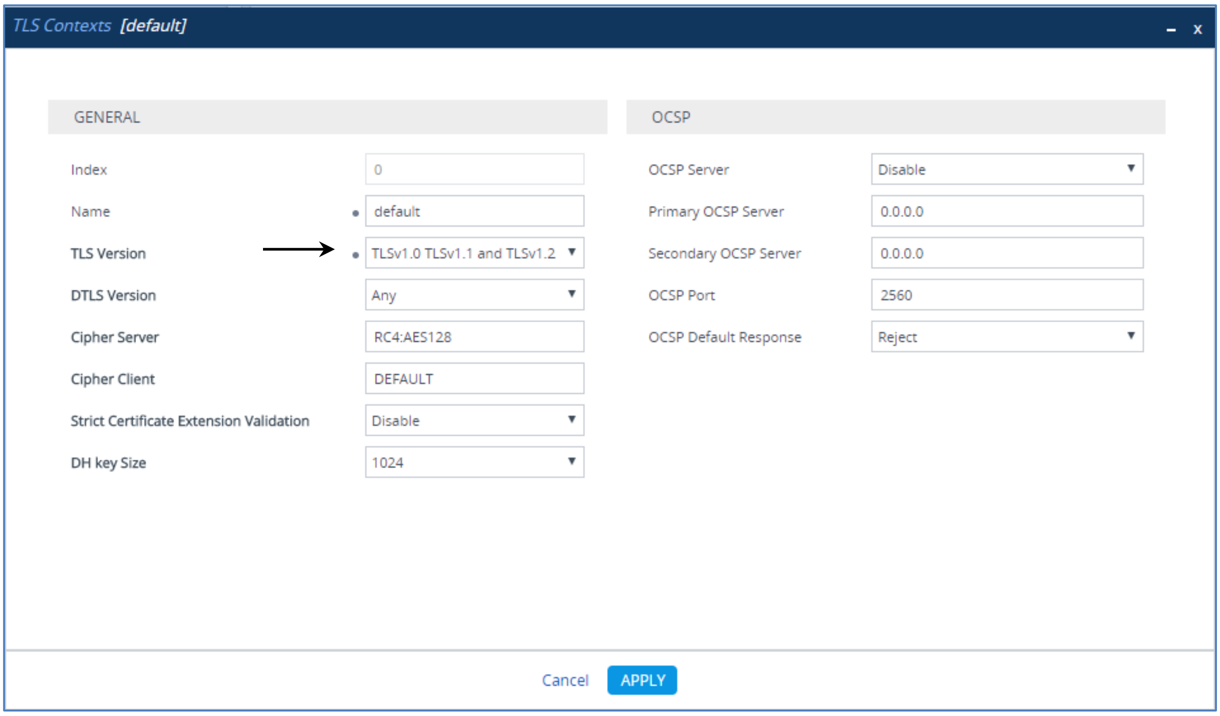
4.8.2 Step 8b: Configure the TLS version

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

➢ **To configure the TLS version:**

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

Figure 4-22: Configuring TLS version



4. Click **Apply**.

4.8.3 Step 8c: 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.

The procedure involves the following main steps:

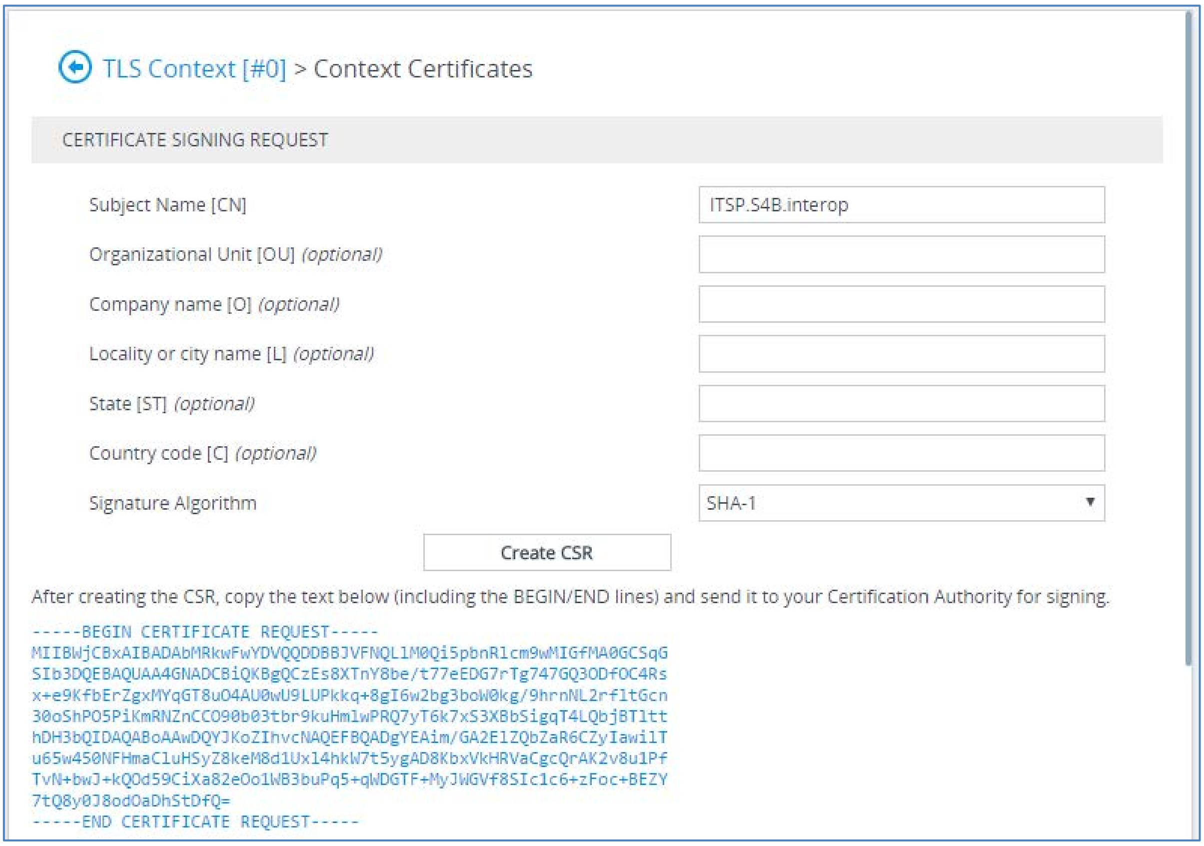
a. Generating a Certificate Signing Request (CSR).
b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root Certificate from CA.
d. Deploying Device and Trusted Root Certificates on E-SBC.

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

➢ **To configure a certificate:**

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

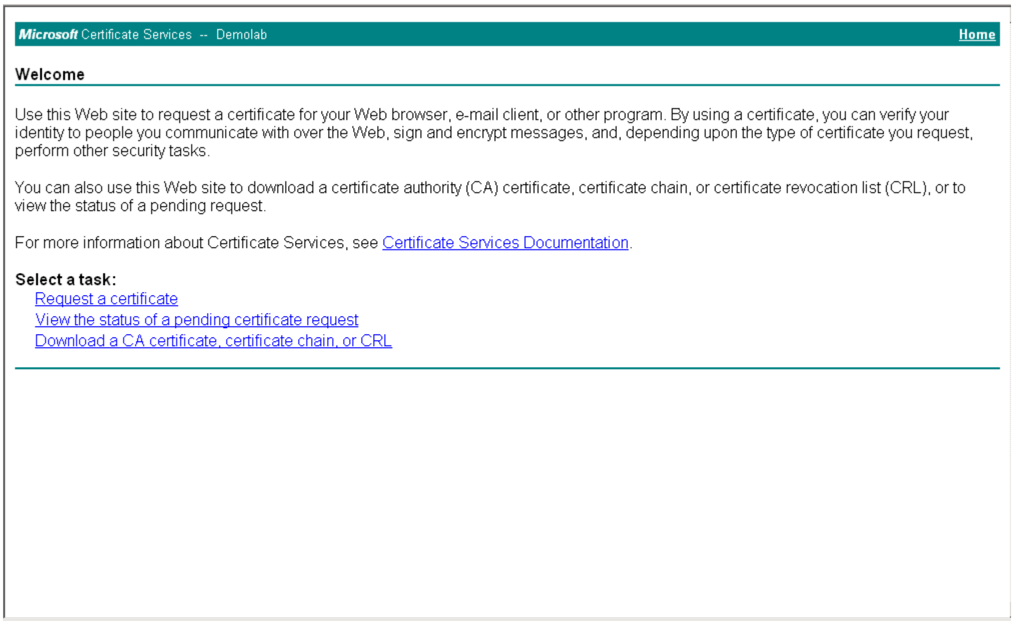
Figure 4-23: Certificate Signing Request – Creating CSR



4. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----"** to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.

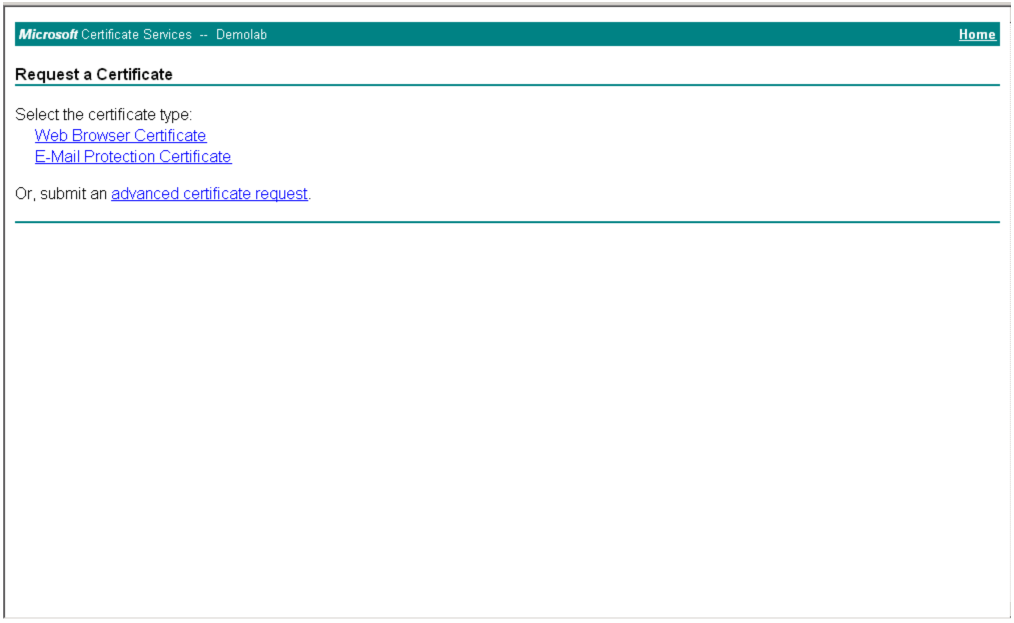
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-24: Microsoft Certificate Services Web Page



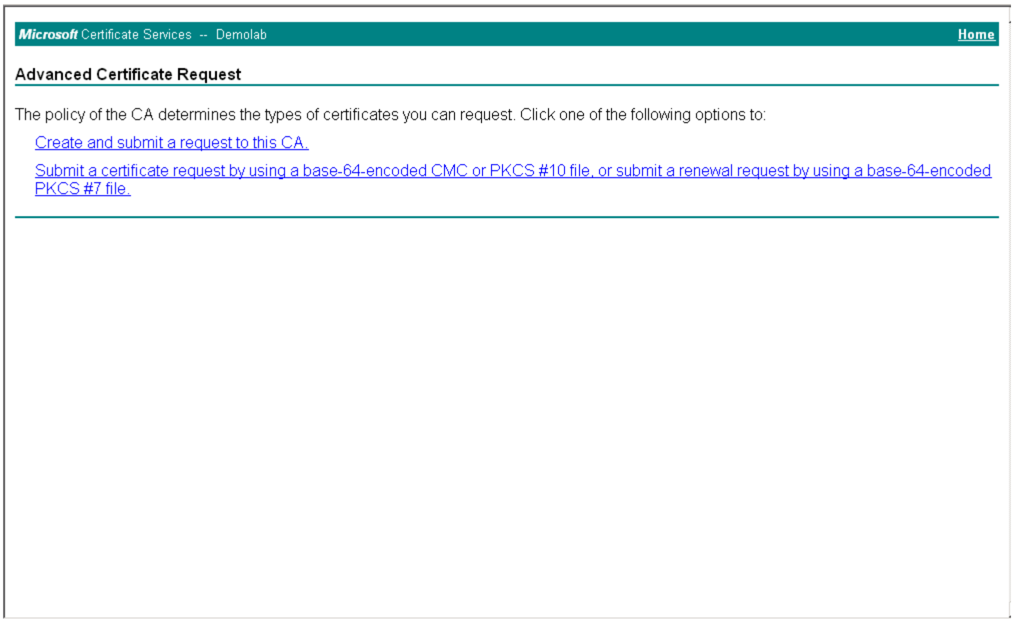
6. Click **Request a certificate**.

Figure 4-25: Request a Certificate Page



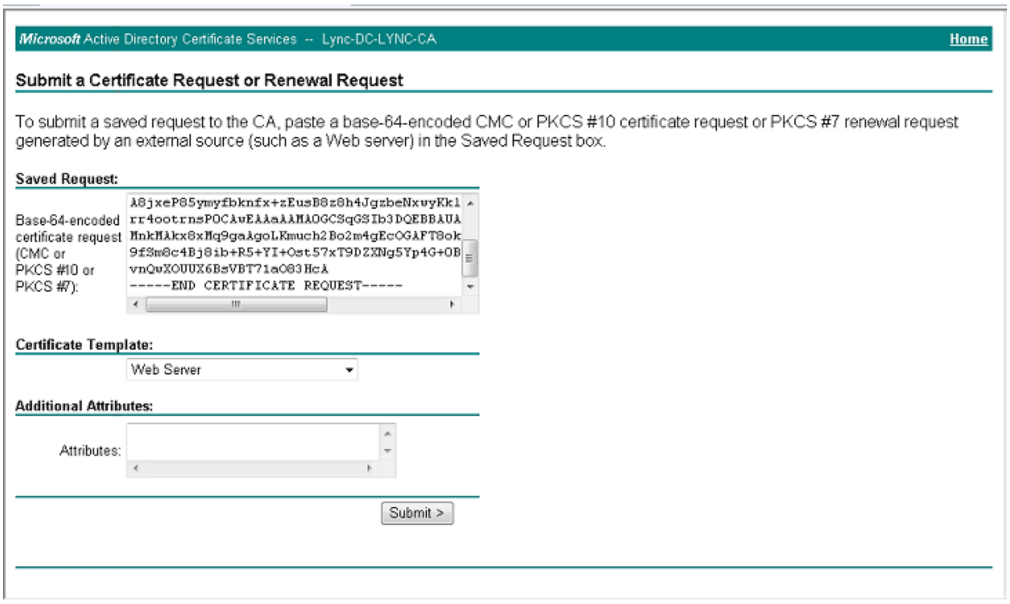
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-26: Advanced Certificate Request Page



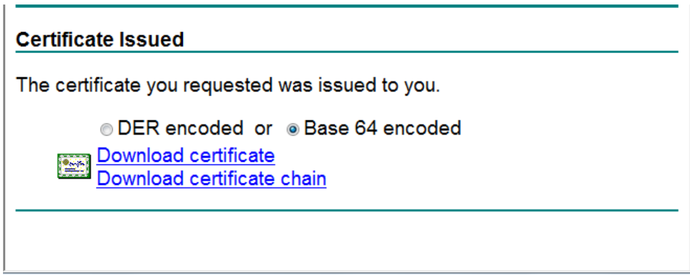
8. Click **Submit a certificate request ...**, and then click **Next**.

Figure 4-27: Submit a Certificate Request or Renewal Request Page



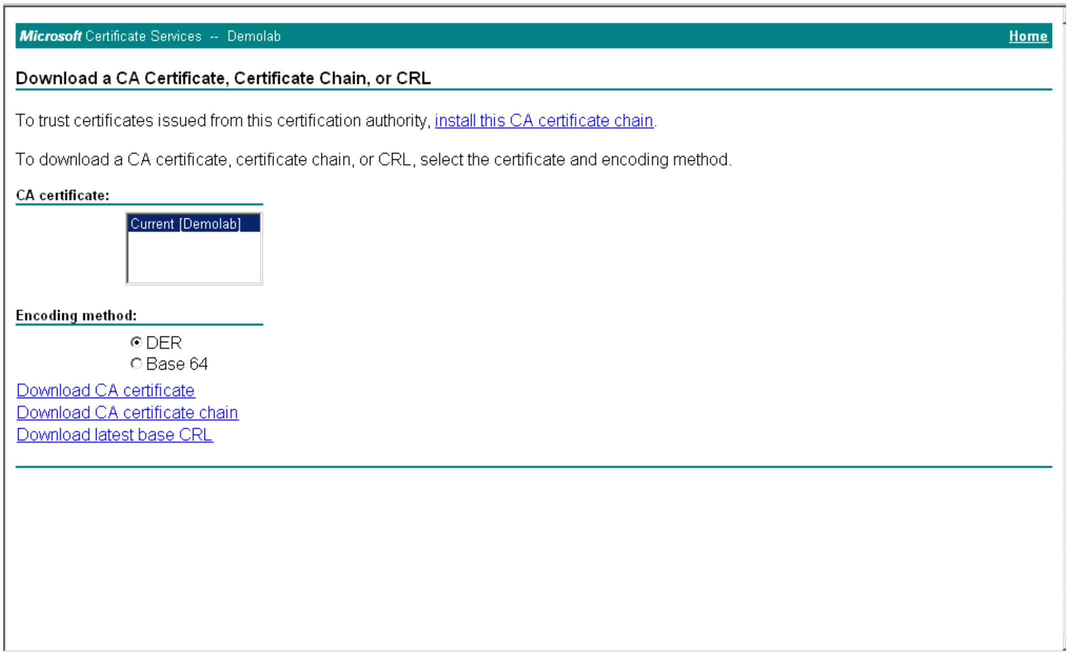
9. Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the 'Saved Request' field.
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-28: Certificate Issued Page



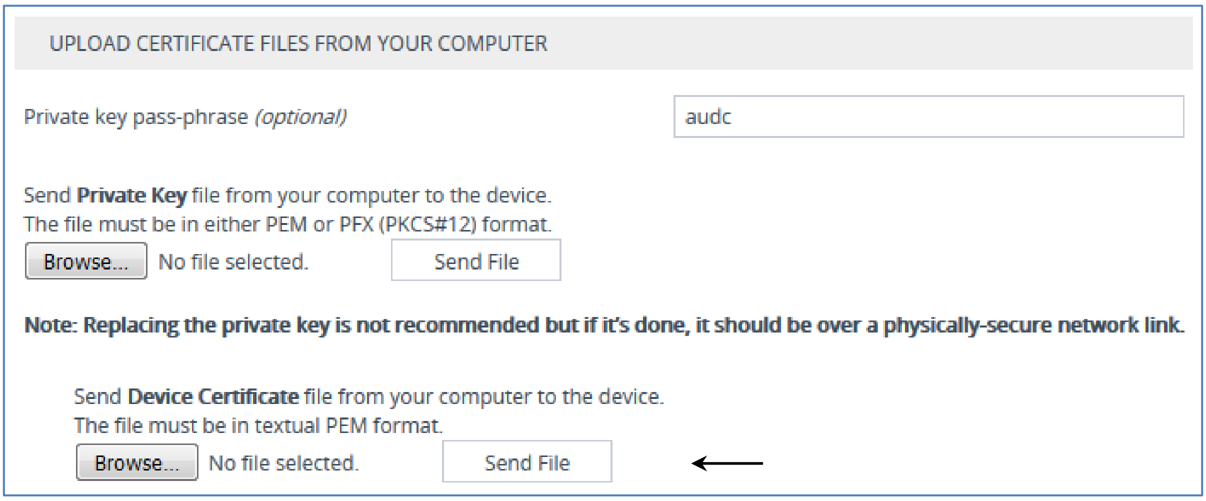
12. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.
13. Save the file as *gateway.cer* to a folder on your computer.
14. Click the **Home** button or navigate to the certificate server at http://<Certificate Server>/CertSrv.
15. Click **Download a CA certificate**,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

Figure 4-29: Download a CA Certificate, Certificate Chain, or CRL Page



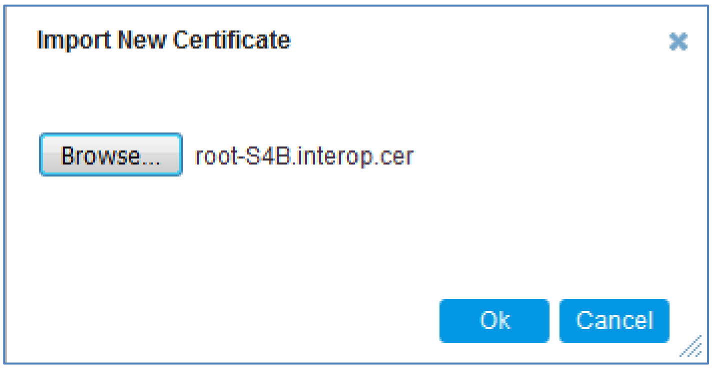
16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file as *certroot.cer* to a folder on your computer.
19. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
    a. In the TLS Contexts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

Figure 4-30: Upload Device Certificate Files from your Computer Group



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

Figure 4-31: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 87).

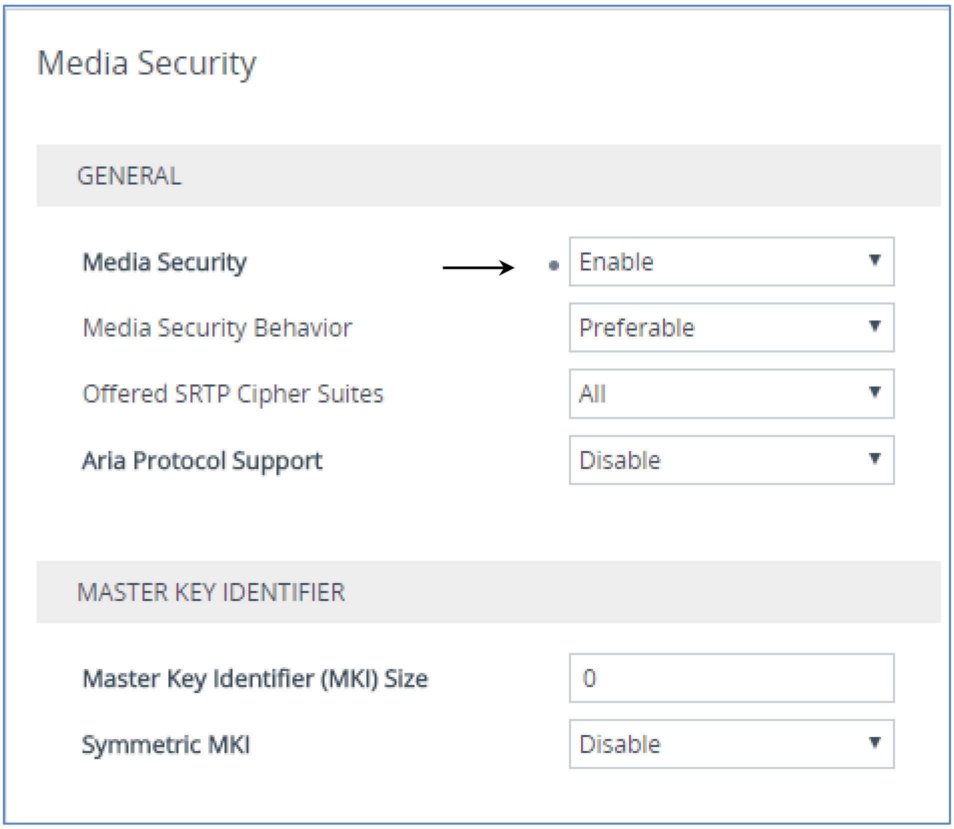
4.9 Step 9: Configure SRTP

This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server when you configured an IP Profile for Skype for Business Server (see Section 4.5 on page 46).

➢ **To configure media security:**

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

Figure 4-32: Configuring SRTP



2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.7 on page 45,) to denote the source and destination of the call.

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

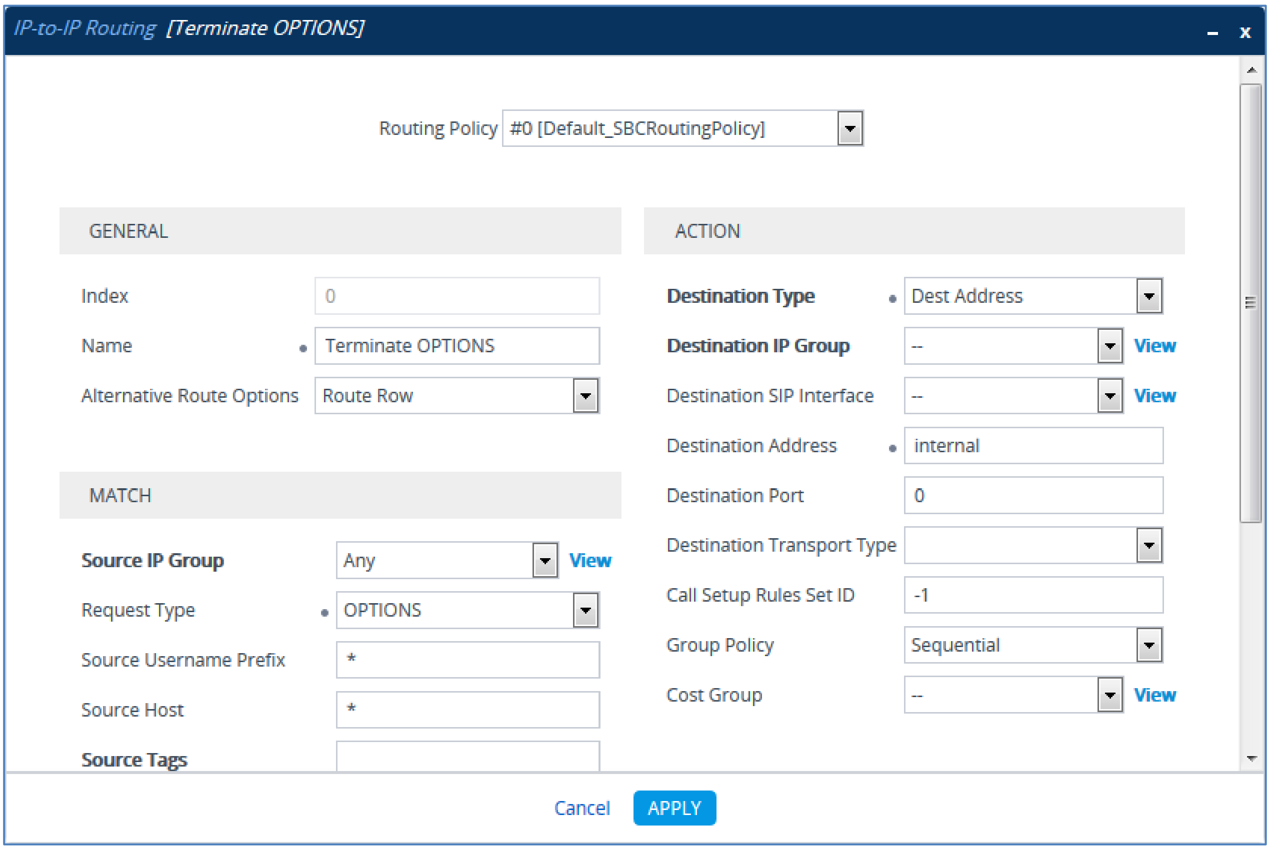
- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
- Terminate REFER messages to Skype for Business Server
- Calls from Skype for Business Server to EWE TEL SIP Trunk
- Calls from EWE TEL SIP Trunk to Fax supporting ATA device (if required)
- Calls from EWE TEL SIP Trunk to Skype for Business Server
- Calls from Fax supporting ATA device to EWE TEL SIP Trunk (if required)

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

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure a rule to terminate SIP OPTIONS messages received from the both LAN and DMZ:
   a. Click **New**, and then configure the parameters as follows:

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

Figure 4-33: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS



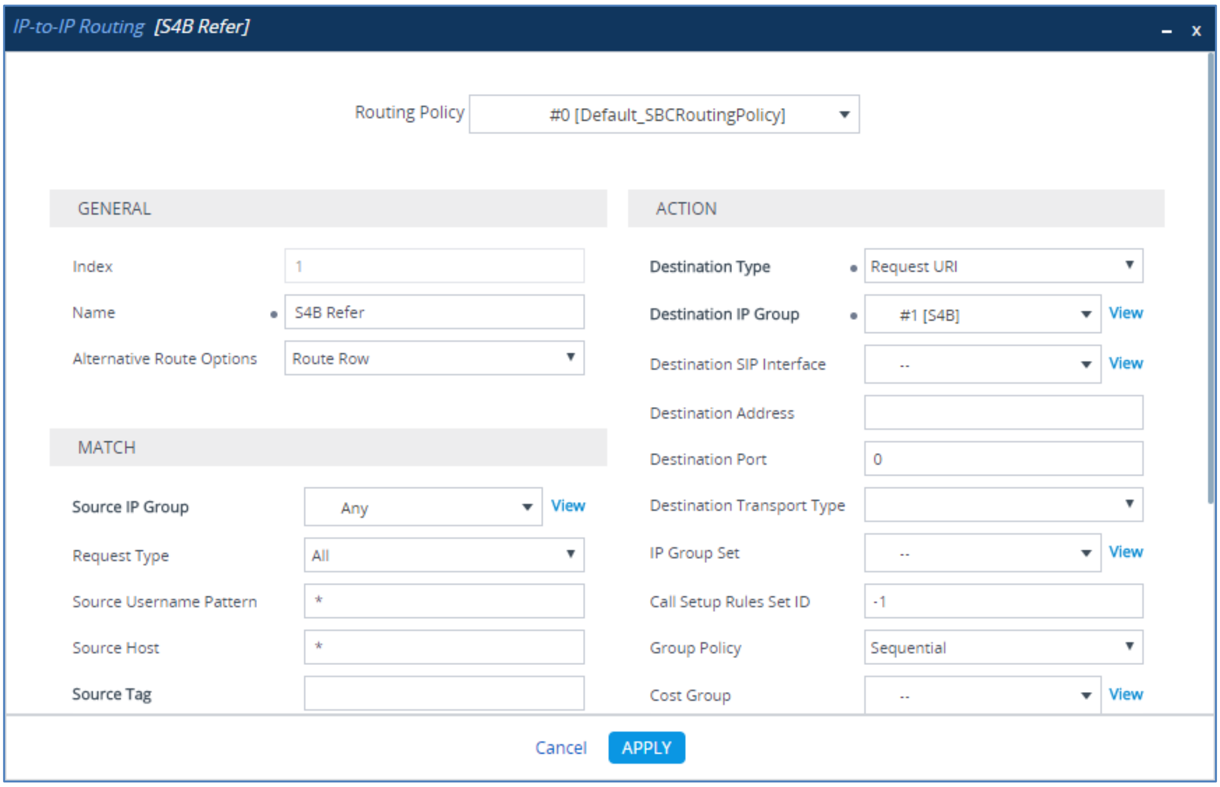
b. Click **Apply**.

3. Configure a rule to terminate REFER messages to Skype for Business Server 2015:

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

Parameter	Value
Index	**1**
Route Name	**S4B Refer** (arbitrary descriptive name)
Source IP Group	**Any**
Call Triger	**REFER**
ReRoute IP Group	**S4B**
Destination Type	**Request URI**
Destination IP Group	**S4B**

Figure 4-34: Configuring IP-to-IP Routing Rule for Terminating REFER



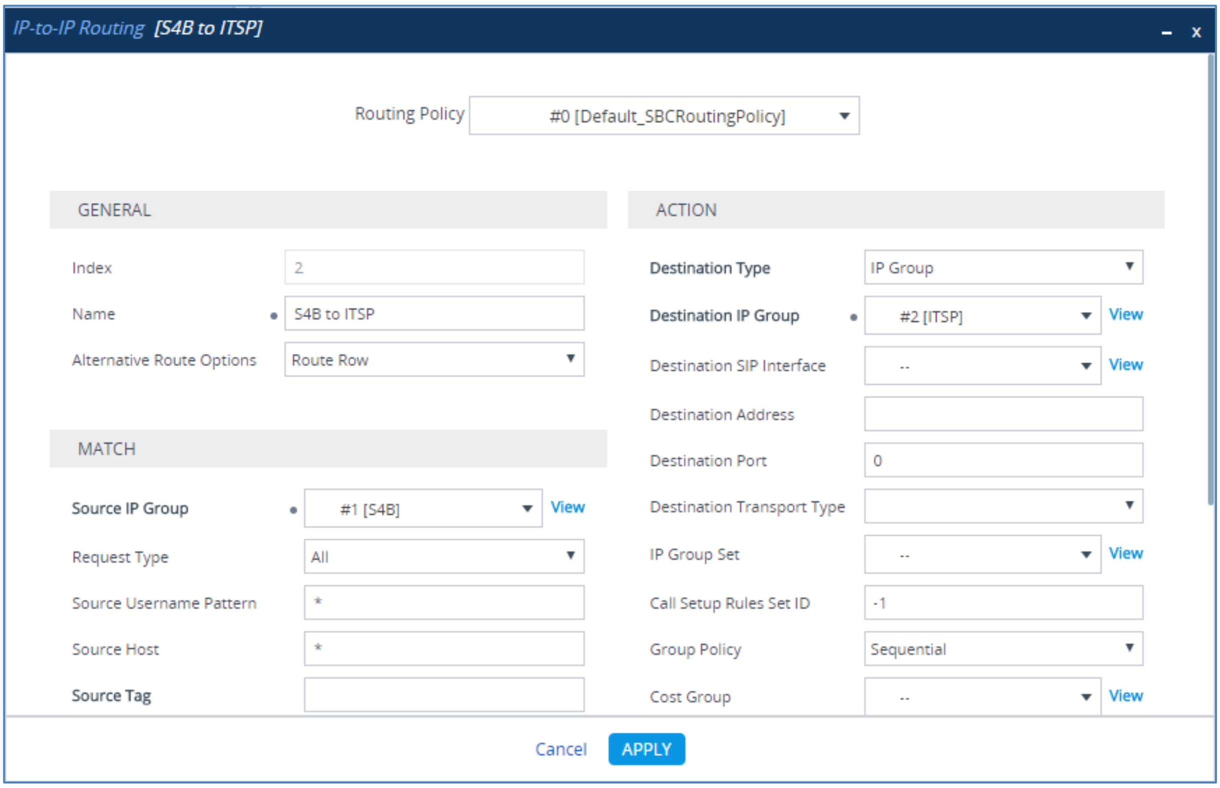
b. Click **Apply**.

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

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

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

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



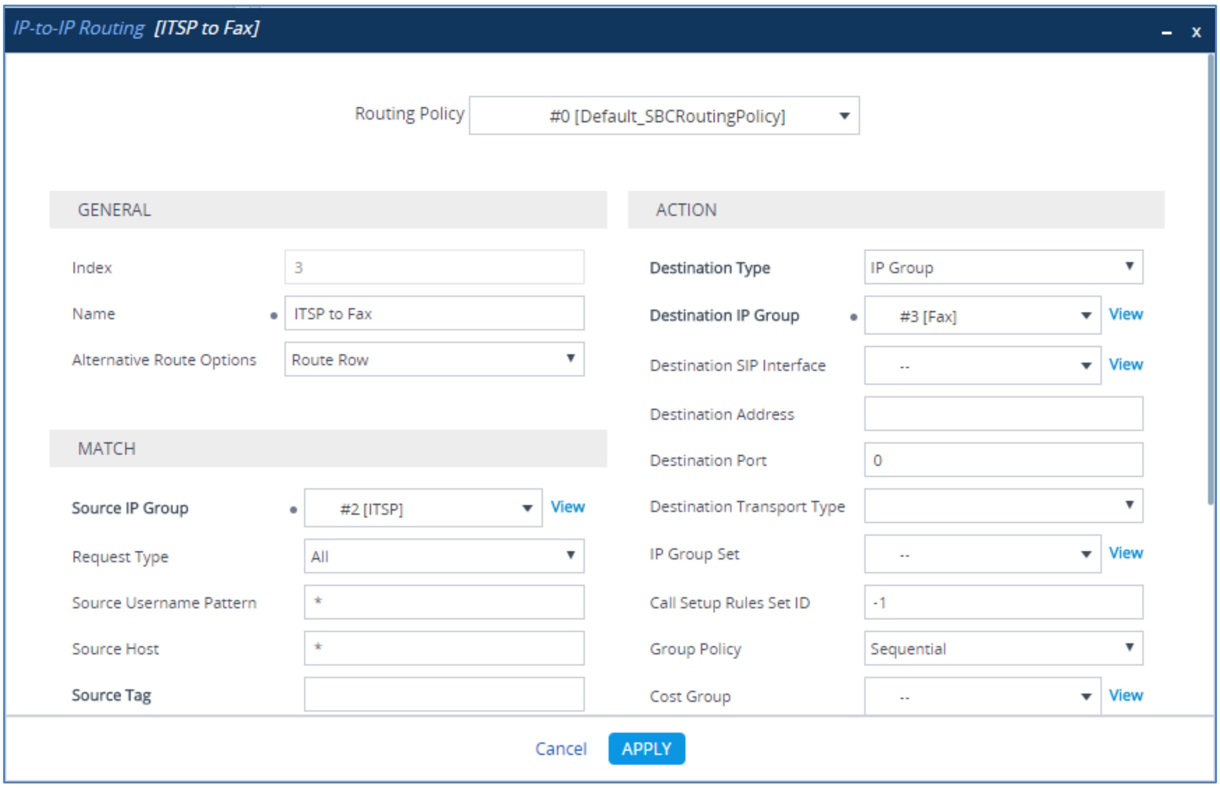
b. Click **Apply**.

5. Configure rule to route calls from EWE TEL SIP Trunk to Fax supporting ATA device:

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

Parameter	Value
Index	**3**
Route Name	**ITSP to Fax** (arbitrary descriptive name)
Source IP Group	**Swisscom**
Destination Username Prefix	**+1234567890** (dedicated FAX number)
Destination Type	**IP Group**
Destination IP Group	**Fax**

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



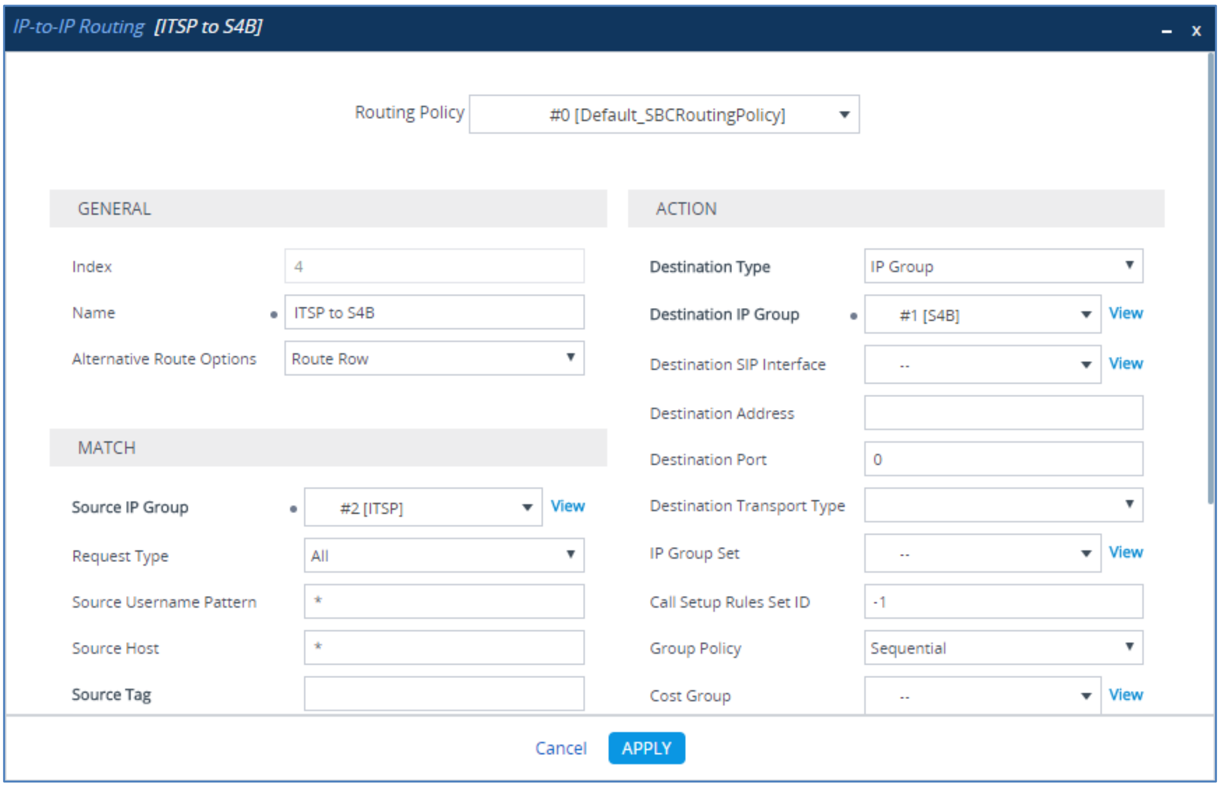
b. Click **Apply**.

6. Configure rule to route calls from EWE TEL SIP Trunk to Skype for Business Server 2015:

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

Parameter	Value
Index	**4**
Route Name	**ITSP to S4B** (arbitrary descriptive name)
Source IP Group	**ITSP**
Destination Type	**IP Group**
Destination IP Group	**S4B**

Figure 4-37: Configuring IP-to-IP Routing Rule for ITSP to S4B



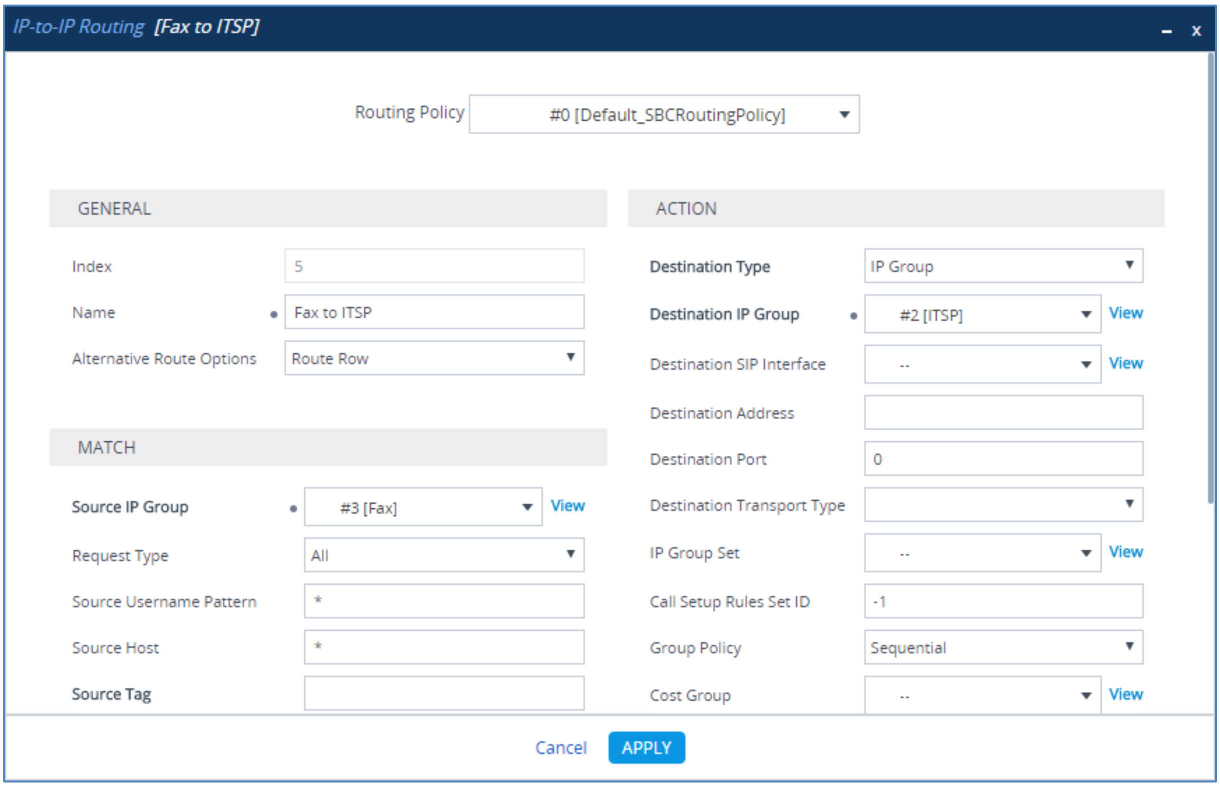
b. Click **Apply.**

7. Configure a rule to route calls from Fax supporting ATA device to EWE TEL SIP Trunk:

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

Parameter	Value
Index	**5**
Route Name	**Fax to ITSP** (arbitrary descriptive name)
Source IP Group	**Fax**
Destination Type	**IP Group**
Destination IP Group	**ITSP**

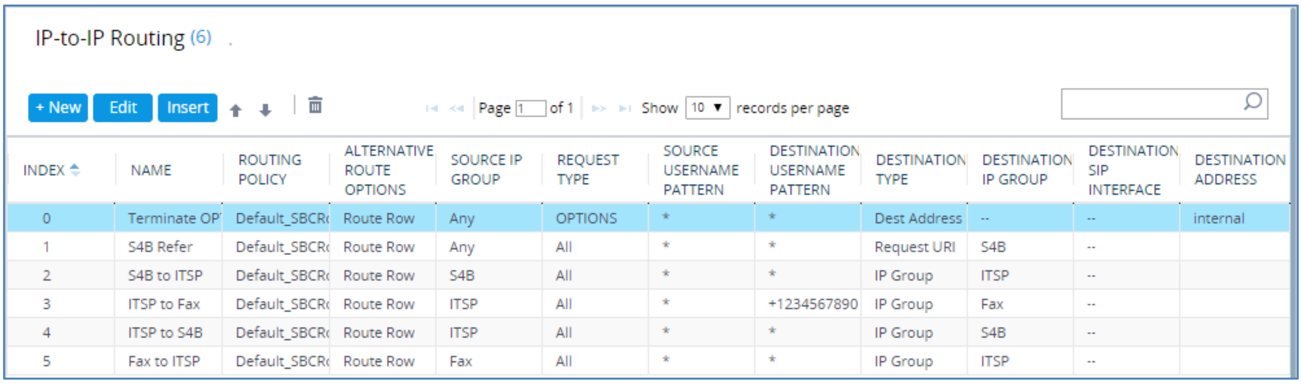
Figure 4-38: Configuring IP-to-IP Routing Rule for Fax to ITSP



b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 4-39: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



IP-to-IP Routing (6)

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

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate OP	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	S4B Refer	Default_SBCR	Route Row	Any	All	*	*	Request URI	S4B	--	
2	S4B to ITSP	Default_SBCR	Route Row	S4B	All	*	*	IP Group	ITSP	--	
3	ITSP to Fax	Default_SBCR	Route Row	ITSP	All	*	+1234567890	IP Group	Fax	--	
4	ITSP to S4B	Default_SBCR	Route Row	ITSP	All	*	*	IP Group	S4B	--	
5	Fax to ITSP	Default_SBCR	Route Row	Fax	All	*	*	IP Group	ITSP	--	

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

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.7 on page 45) to denote the source and destination of the call.

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

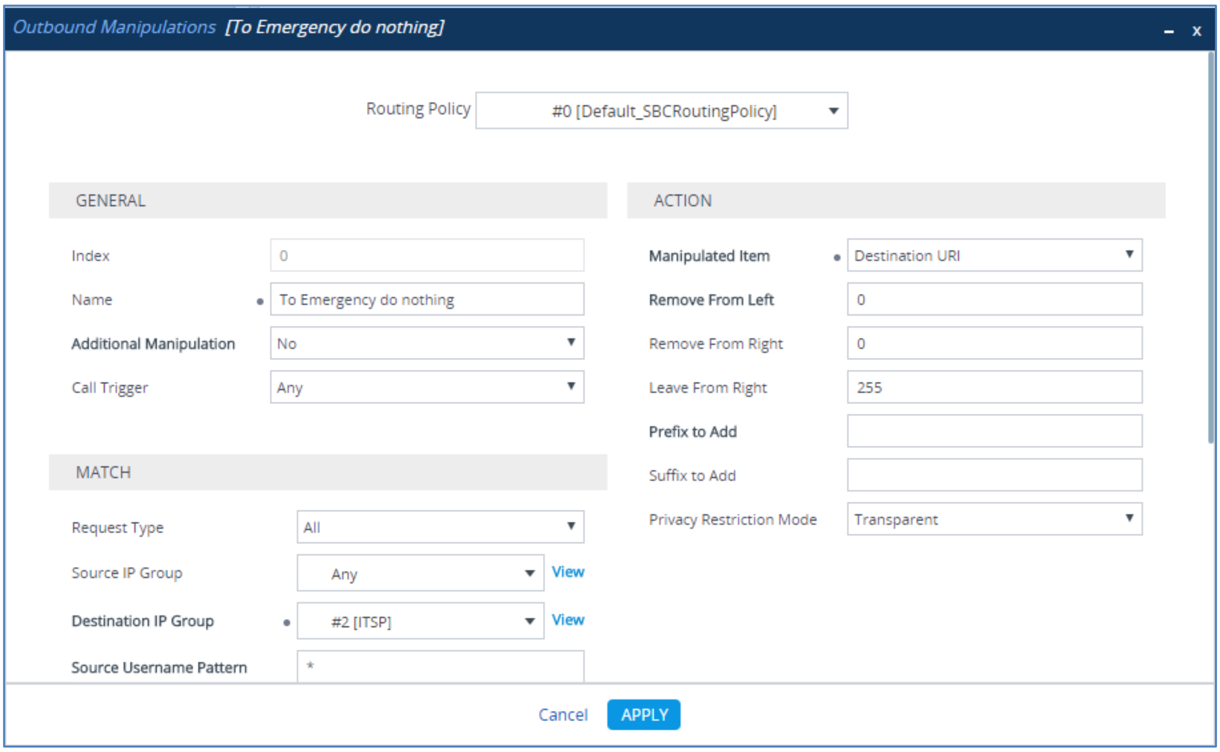
For example, for this interoperability test topology, a manipulation is configured to strip the "+" (plus sign) from the destination number for Emergency calls to the EWE TEL SIP Trunk IP Group if the plus sign exists and to not perform any action for all other emergency calls.

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

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

Parameter	Value
Index	**0**
Name	**To Emergency do nothing**
Source IP Group	**Any**
Destination IP Group	**Any**
Destination Username Pattern	**[110,112]**
Manipulated Item	**Destination URI**

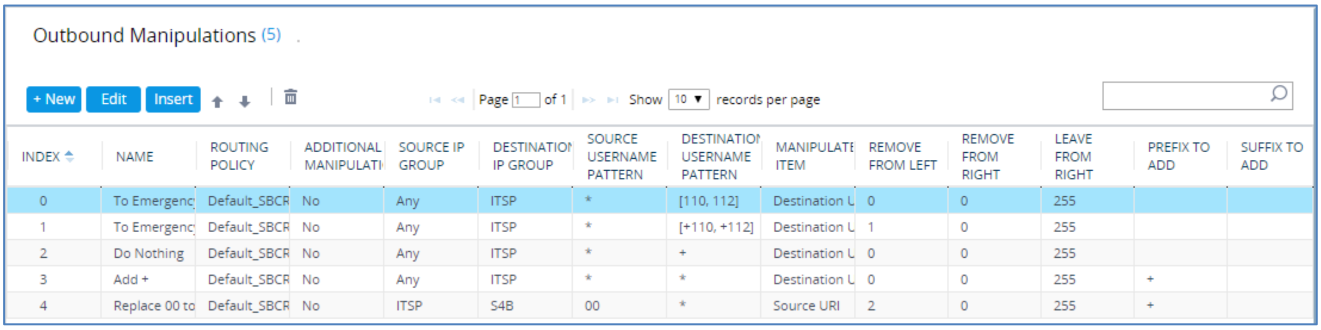
Figure 4-40: Configuring IP-to-IP Outbound Manipulation Rule



3. Click **Apply**.

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

Figure 4-41: Example of Configured IP-to-IP Outbound Manipulation Rules


Outbound Manipulations (5)

INDEX	NAME	ROUTING POLICY	ADDITIONAL MANIPULATI	SOURCE IP GROUP	DESTINATION IP GROUP	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	MANIPULATE ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	To Emergenc	Default_SBCR	No	Any	ITSP	*	[110, 112]	Destination U	0	0	255		
1	To Emergenc	Default_SBCR	No	Any	ITSP	*	[+110, +112]	Destination U	1	0	255		
2	Do Nothing	Default_SBCR	No	Any	ITSP	*	+	Destination U	0	0	255		
3	Add +	Default_SBCR	No	Any	ITSP	*	*	Destination U	0	0	255	+	
4	Replace 00 to	Default_SBCR	No	ITSP	S4B	00	*	Source URI	2	0	255	+	

Rule Index	Description
0	Calls from any (S4B or MP Fax) IP Group with destination number 110 or 112, do not perform any action for the destination number.
1	Calls from any (S4B or MP Fax) IP Group with destination number +110 or +112. Remove "+" from this numbers.
2	Calls from any (S4B or MP Fax) IP Group with the prefix destination number "+", do not perform any action for the destination number.
3	Calls from any (S4B or MP Fax) IP Group with any destination number (*), add "+" prefix to the destination number.

4.12 Step 12: Configure Message Manipulation Rules

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

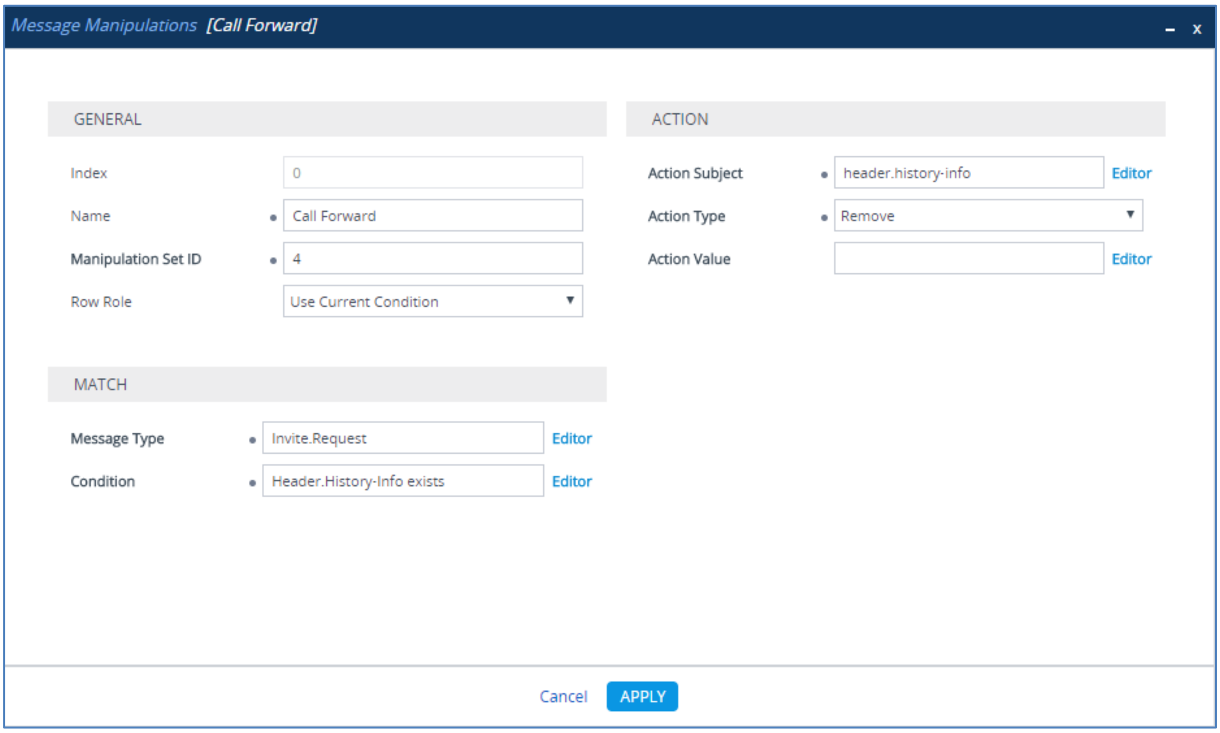
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for EWE TEL SIP Trunk. This rule applies to messages sent to the EWE TEL SIP Trunk IP Group in a call forward scenario. This removes the SIP History-Info Header.

Parameter	Value
Index	**0**
Name	**Call Forward**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.History-Info exists**
Action Subject	**Header.History-Info**
Action Type	**Remove**

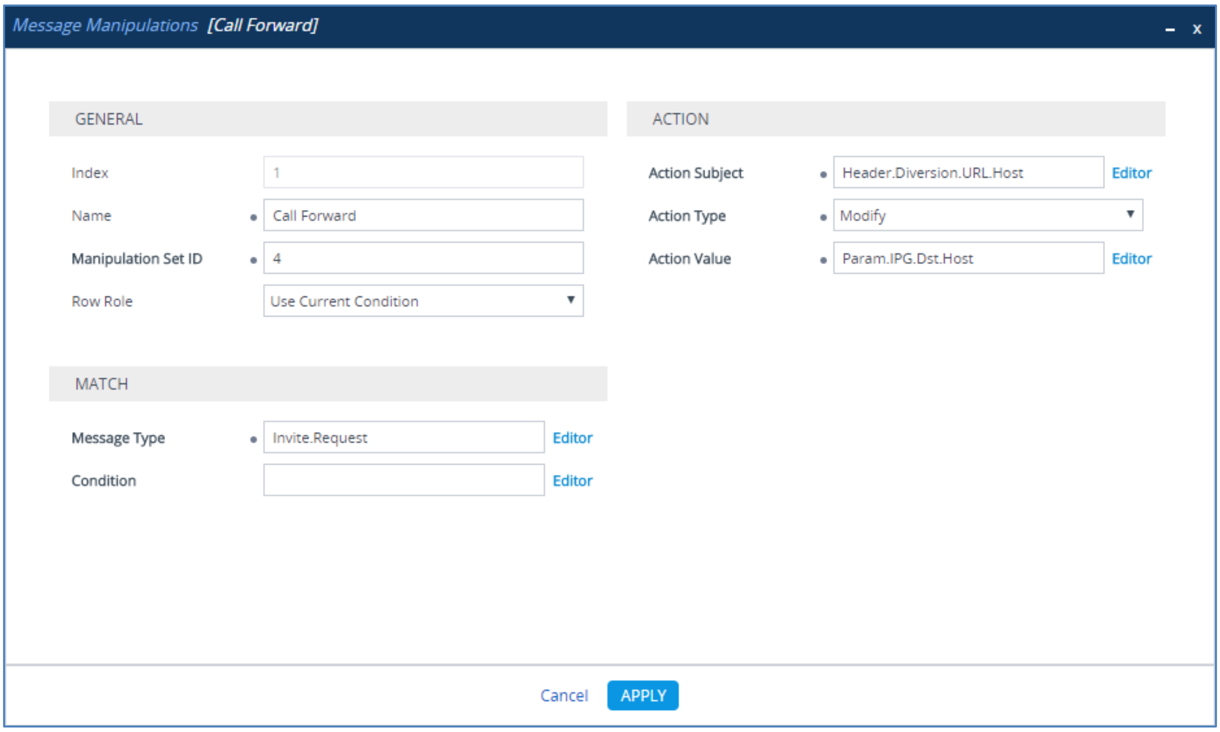
Figure 4-42: Configuring SIP Message Manipulation Rule 0 (for EWE TEL SIP Trunk)



3. Configure another manipulation rule (Manipulation Set 4) for EWE TEL SIP Trunk. This rule applies to messages sent to the EWE TEL SIP Trunk IP Group in a call forward scenario. This replaces the **host** part of the SIP Diversion Header with the value, configured in the EWE TEL SIP Trunk IP Group's 'SIP Group Name'.

Parameter	Value
Index	**1**
Name	**Call Forward**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Action Subject	**Header.Diversion.URL.Host**
Action Type	**Modify**
Action Value	**Param.IPG.Dst.Host**

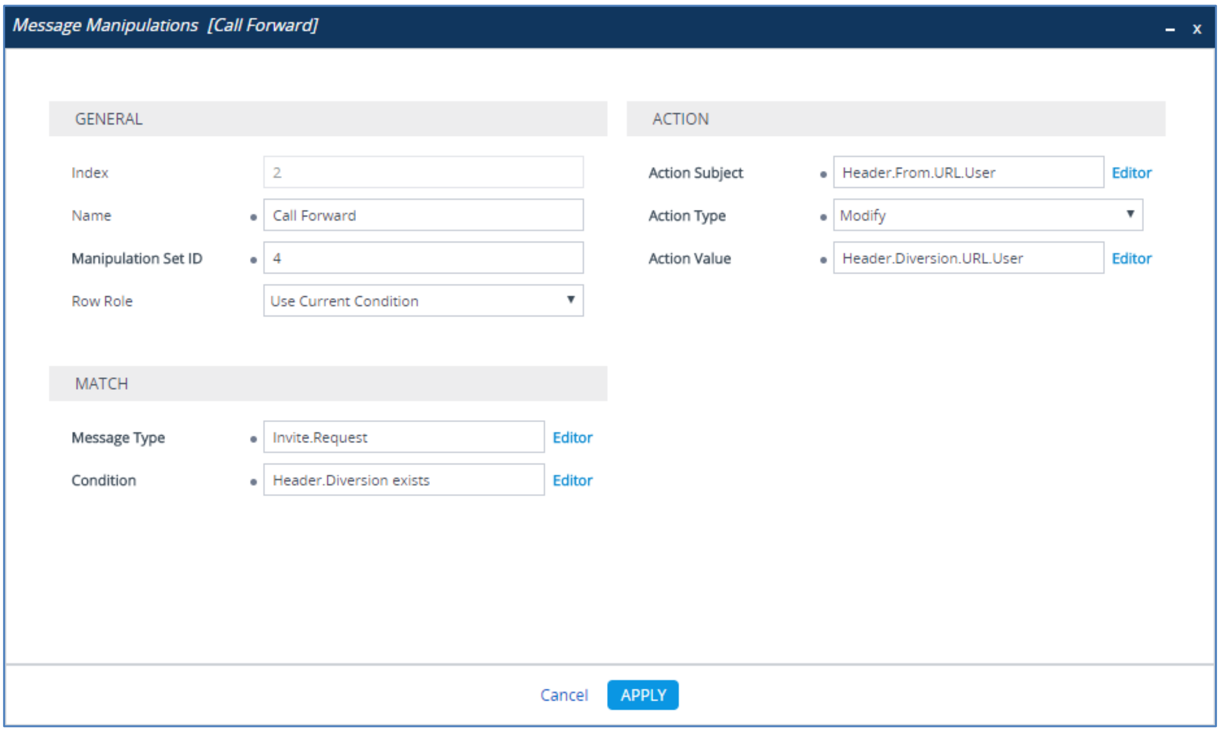
Figure 4-43: Configuring SIP Message Manipulation Rule 1 (for EWE TEL SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 4) for EWE TEL SIP Trunk. This rule applies to messages sent to the EWE TEL SIP Trunk IP Group in a call forwarding scenario. This replaces the **user** part of the SIP From Header with the value, from the SIP Diversion Header.

Parameter	Value
Index	**2**
Name	**Call Forward**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.Diversion exists**
Action Subject	**Header.From.URL.User**
Action Type	**Modify**
Action Value	**Header.Diversion.URL.User**

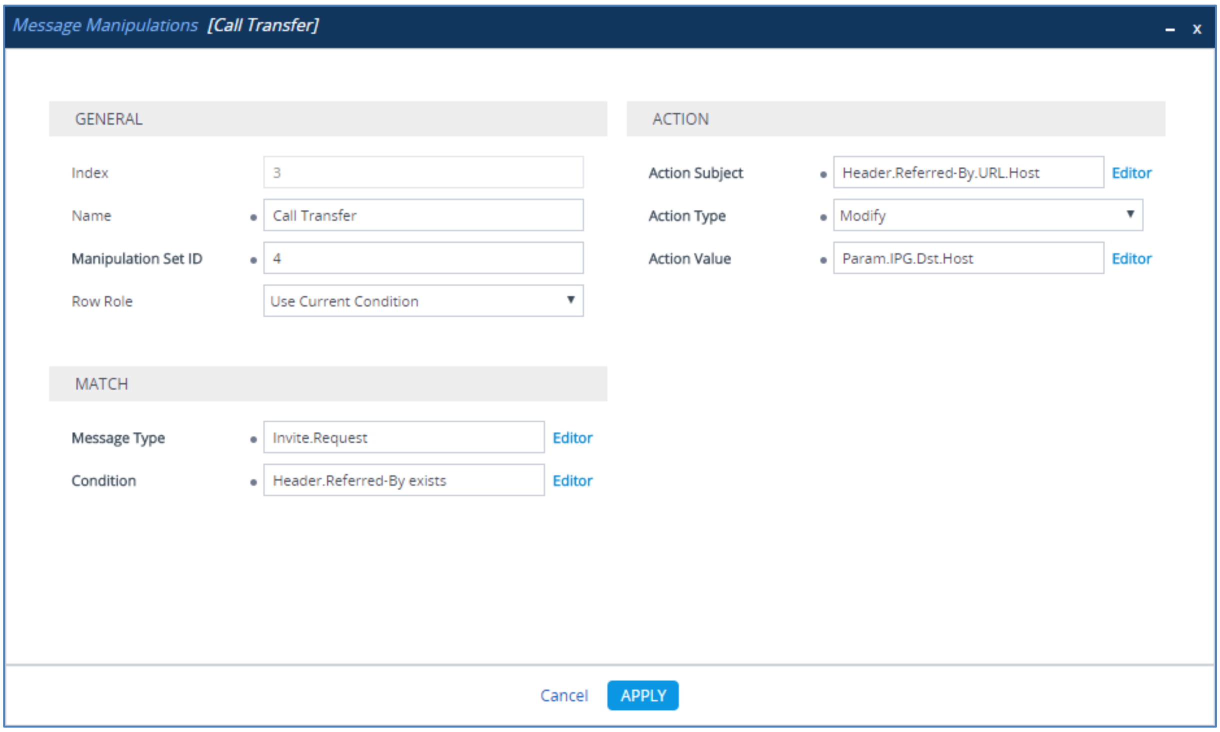
Figure 4-44: Configuring SIP Message Manipulation Rule 2 (for EWE TEL SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 4) for EWE TEL SIP Trunk. This rule applies to messages sent to the EWE TEL SIP Trunk IP Group in a call transfer scenario. This replace the **host** part of the SIP Referred-By Header with the value, configured in the EWE TEL SIP Trunk IP Group's 'SIP Group Name'.

Parameter	Value
Index	**3**
Name	**Call Transfer**
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**

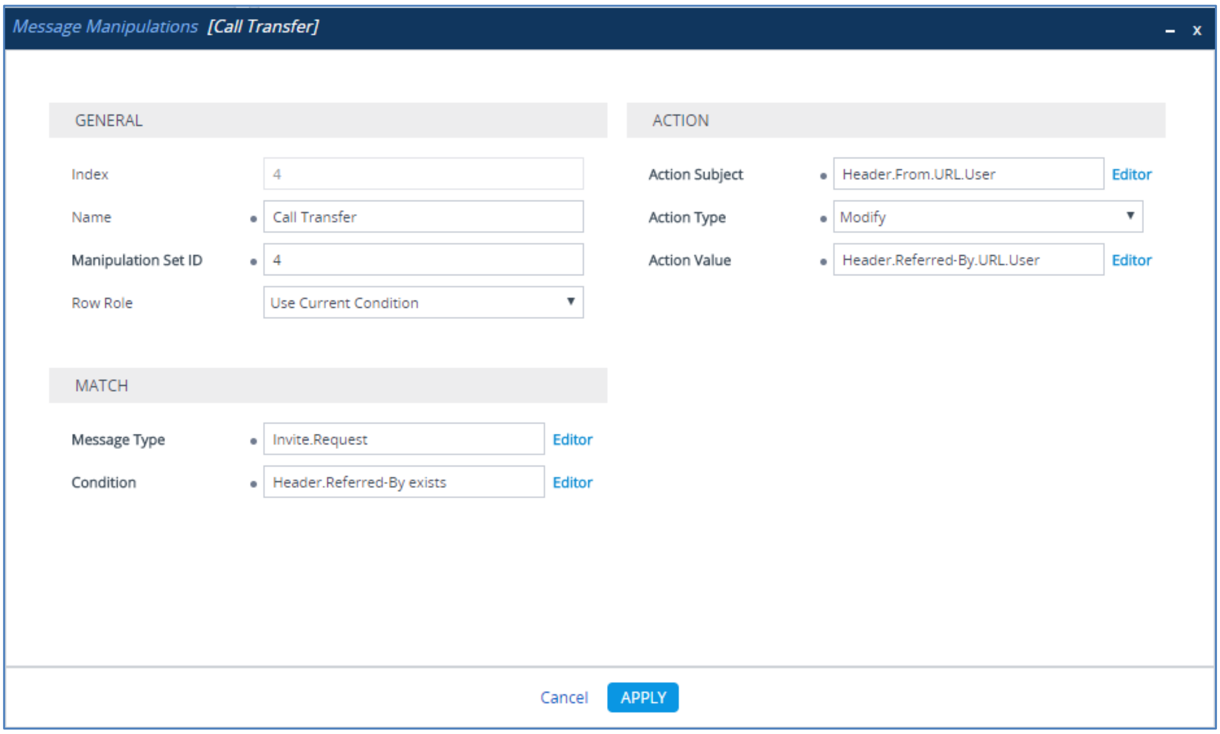
Figure 4-45: Configuring SIP Message Manipulation Rule 3 (for EWE TEL SIP Trunk)



6. Configure another manipulation rule (Manipulation Set 4) for EWE TEL SIP Trunk. This rule applies to messages sent to the EWE TEL SIP Trunk IP Group in a call transfer scenario. This replace the **user** part of the SIP From Header with the value, from the SIP Referred-By Header.

Parameter	Value
Index	**4**
Name	**Call Transfer**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.Referred-By exists**
Action Subject	**Header.From.URL.User**
Action Type	**Modify**
Action Value	**Header.Referred-By.URL.User**

Figure 4-46: Configuring SIP Message Manipulation Rule 4 (for EWE TEL SIP Trunk)



7. Configure another manipulation rule (Manipulation Set 4) for EWE TEL SIP Trunk. This rule is applied to response messages sent to the EWE TEL SIP Trunk IP Group for Error Responses initiated by the Skype for Business Server IP Group. This replaces the method types '480', '503' and '603' with the value '486', because EWE TEL SIP Trunk not recognizes these method types.

Parameter	Value
Index	**5**
Name	**Error Responses**
Manipulation Set ID	**4**
Message Type	**Any.Response**
Condition	**Header.Request-URI.MethodType == '480' 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 4-47: Configuring SIP Message Manipulation Rule 5 (for EWE TEL SIP Trunk)

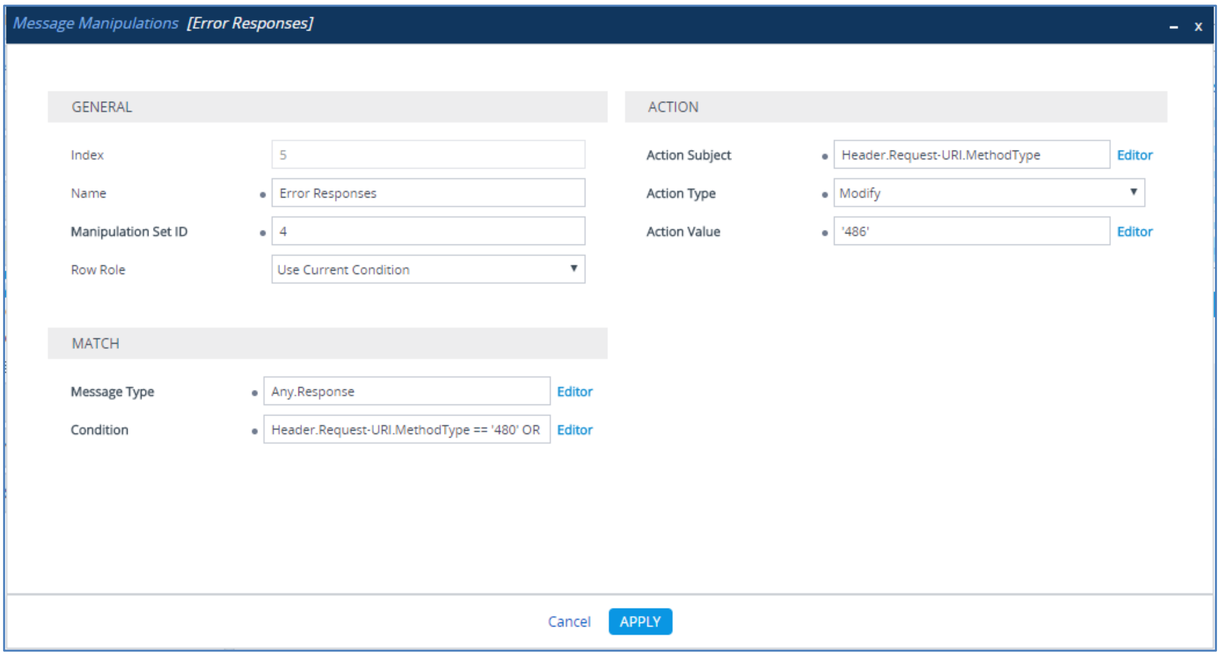
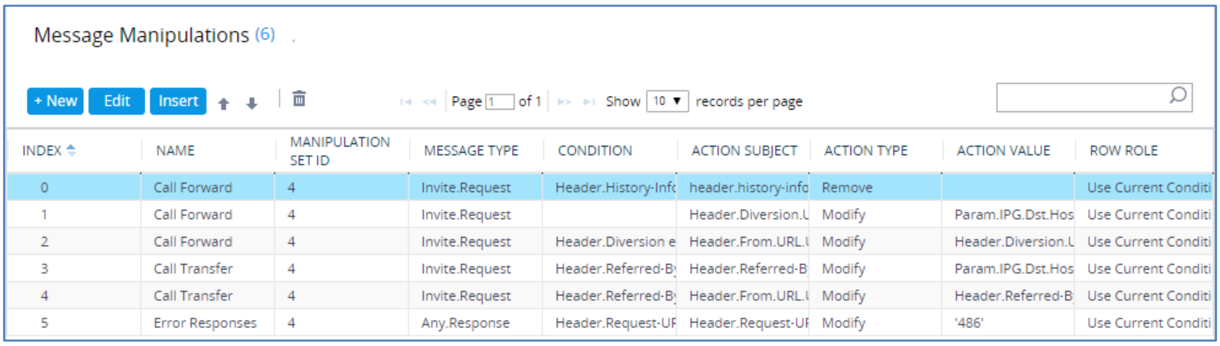


Figure 4-48: Example of Configured SIP Message Manipulation Rules


Message Manipulations (6)

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

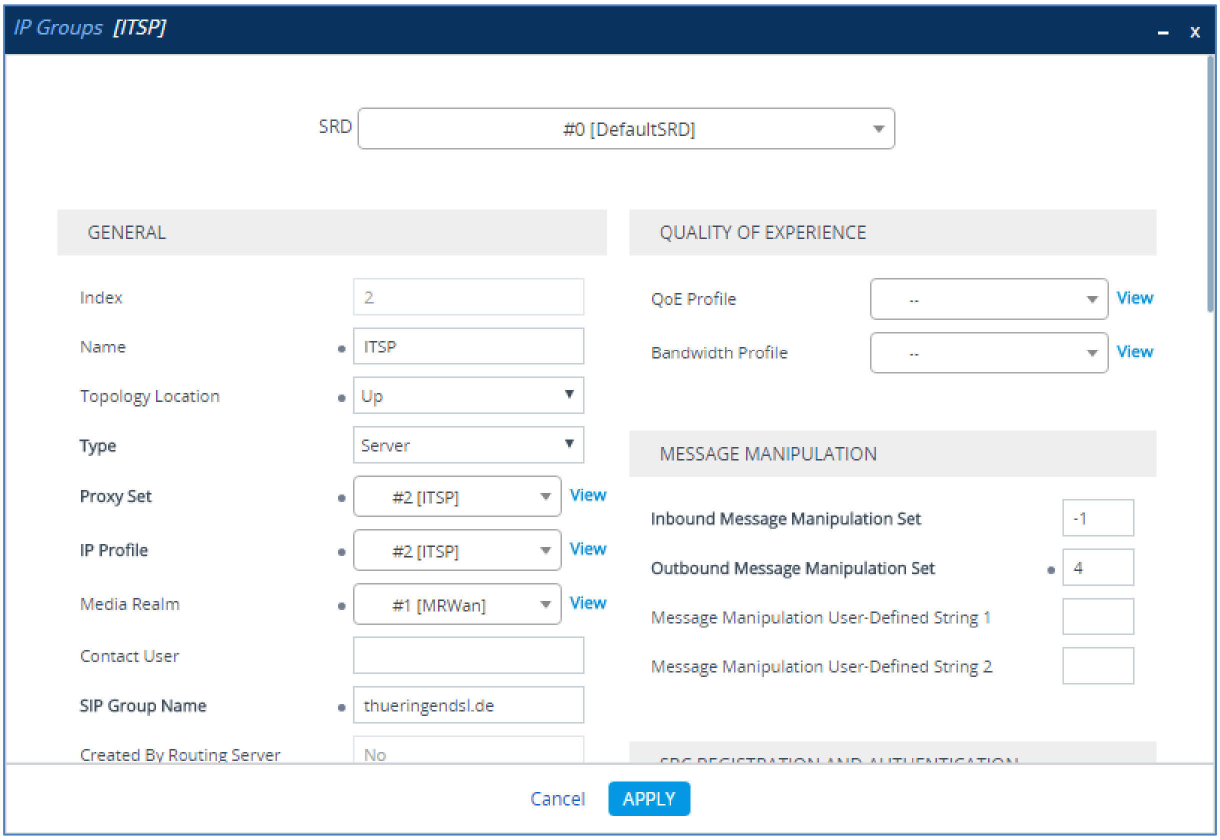
INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Call Forward	4	Invite.Request	Header.History-Infc	header.history-info	Remove		Use Current Conditi
1	Call Forward	4	Invite.Request		Header.Diversion.U	Modify	Param.IPG.Dst.Hos	Use Current Conditi
2	Call Forward	4	Invite.Request	Header.Diversion e	Header.From.URL.U	Modify	Header.Diversion.U	Use Current Conditi
3	Call Transfer	4	Invite.Request	Header.Referred-By	Header.Referred-B	Modify	Param.IPG.Dst.Hos	Use Current Conditi
4	Call Transfer	4	Invite.Request	Header.Referred-By	Header.From.URL.U	Modify	Header.Referred-B	Use Current Conditi
5	Error Responses	4	Any.Response	Header.Request-UF	Header.Request-UF	Modify	'486'	Use Current Conditi

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to the EWE TEL SIP Trunk IP Group as well as the Skype for Business Server IP Group. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This remove the SIP History-Info Header.	For Call Forward scenarios initiated by Skype for Business Server, EWE TEL SIP Trunk requires a SIP Diversion Header with a pre-defined host part and that the user part of the SIP From Header is identical to the SIP Diversion Header.
1	This replace the **host** part of the SIP Diversion Header with the value, configured in the EWE TEL SIP Trunk IP Group's 'SIP Group Name'.	
2	This replace the **user** part of the SIP From Header with the value from the SIP Diversion Header.	
3	This replace the **host** part of the SIP Referred-By Header with the value, configured in the EWE TEL SIP Trunk IP Group's 'SIP Group Name'.	For Call Transfer initiated by Skype for Business Server, EWE TEL SIP Trunk requires a SIP Referred-By Header with pre-defined host part and that the user part of the SIP From Header is identical to the SIP Referred-By Header.
4	This replaces the **user** part of the SIP From Header with the value, from the SIP Referred-By Header.	
5	This rule is applied to response messages sent to the EWE TEL SIP Trunk IP Group for Error Responses initiated by the Skype for Business Server IP Group. This replaces the method types '480', '503' and '603' with the value '486'.	EWE TEL SIP Trunk does not recognize these method types and continues to send INVITEs messages to the SBC.

8. Assign Manipulation Set ID 4 to the EWE TEL SIP trunk IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the EWE TEL SIP trunk IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-49: Assigning Manipulation Set 4 to the EWE TEL SIP Trunk IP Group



   d. Click **Apply**.

4.13 Step 13: Configure Registration Accounts

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

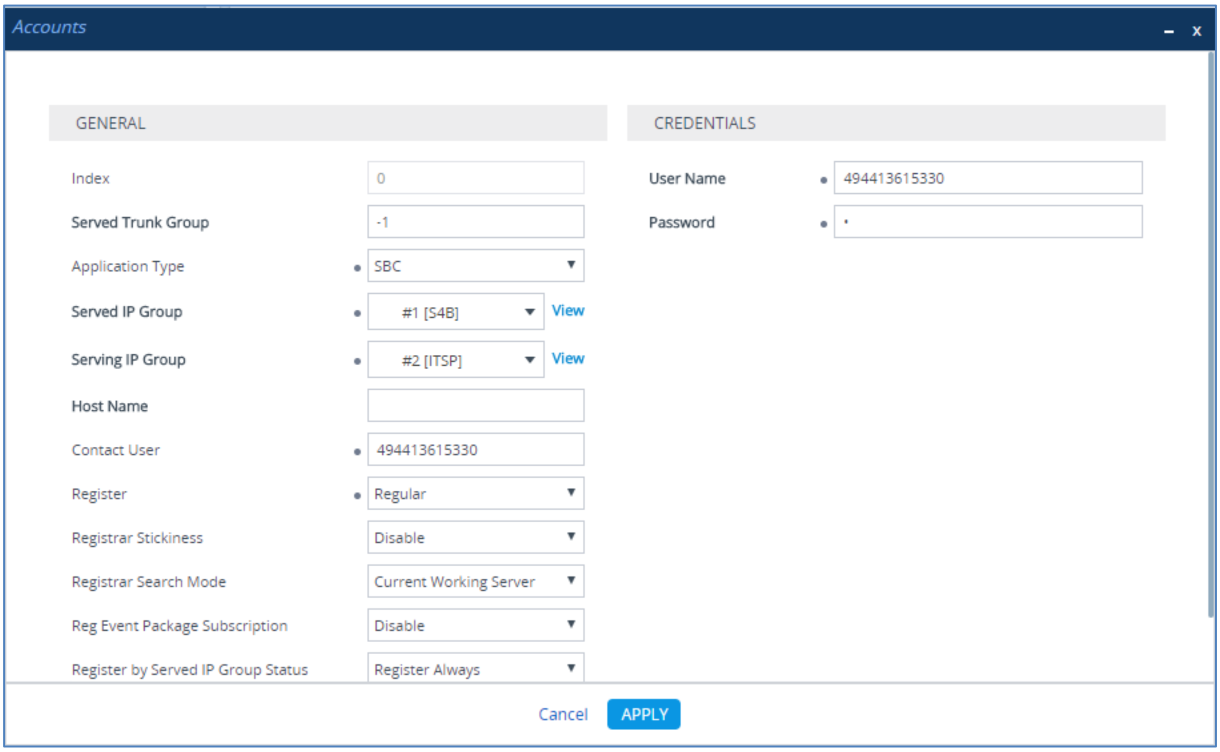
In the interoperability test topology, the Served IP Group is Skype for Business Server IP Group and the Serving IP Group is EWE TEL SIP Trunk IP Group.

➢ **To configure a registration account:**

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from, for example:

Parameter	Value
Served IP Group	**S4B**
Application Type	**SBC**
Serving IP Group	**ITSP**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	**1234567890** (trunk main line)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-50: Configuring a SIP Registration Account for S4B

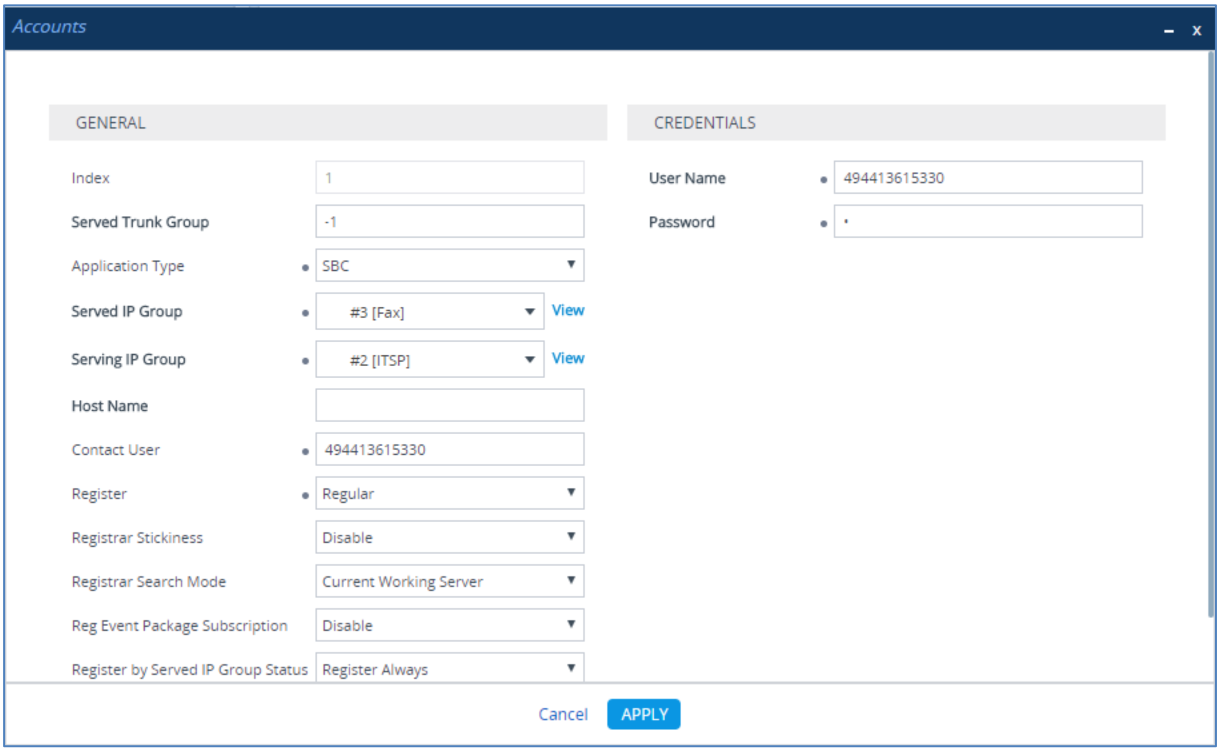


4. Click **Apply**.

5. Click **New**.
6. Configure another account for FAX IP Group according to the provided information from, for example:

Parameter	Value
Served IP Group	**Fax**
Application Type	**SBC**
Serving IP Group	**ITSP**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	**1234567890** (trunk main line)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-51: Configuring a SIP Registration Account for Fax ATA Device



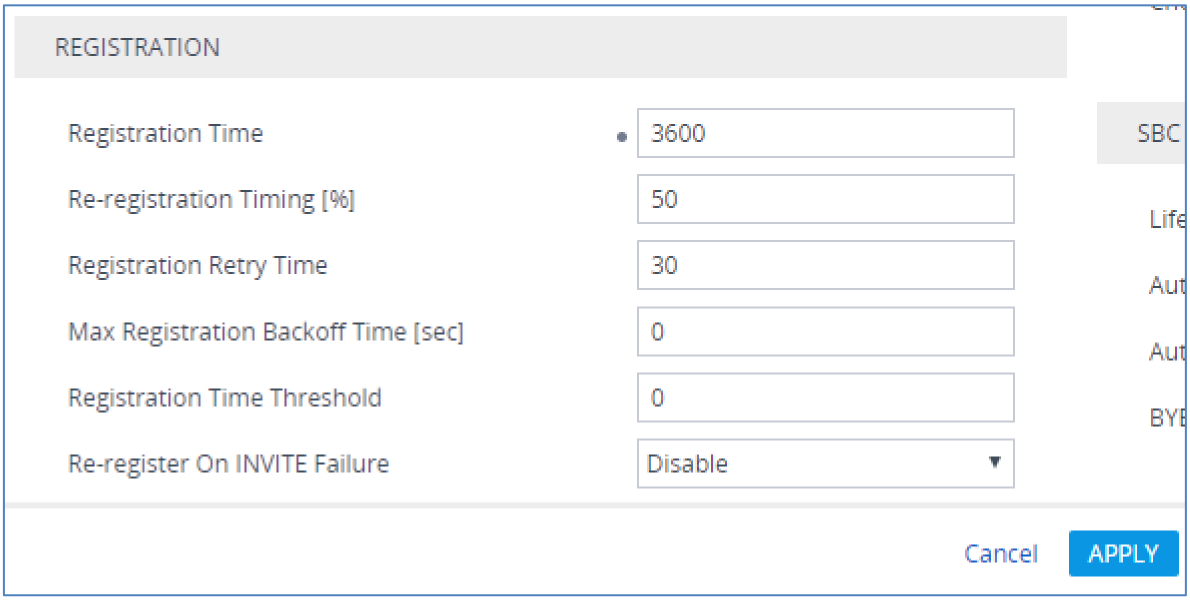
7. Click **Apply**.

This step describes how to configure SIP registration period. The EWE TEL SIP Trunk requires a registration period of 3600 seconds.

➢ To configure a registration time period:

1. Open the Proxy & Registration page (Setup menu > Signaling & Media tab > SIP Definitions folder > Proxy & Registration).
2. Configure **Registration Time** parameter with the value **3600**.

Figure 4-52: Configuring Registration Time



3. Click **Apply**.

4.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

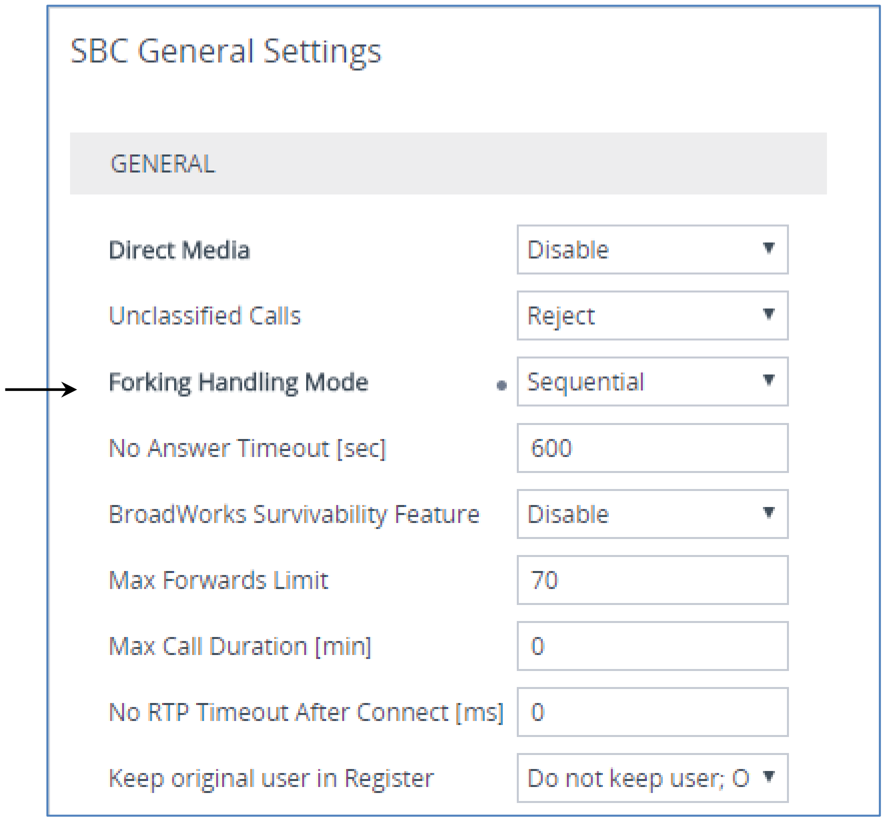
4.14.1 Step 14a: Configure Call Forking Mode

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

➢ **To configure call forking:**

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

Figure 4-53: Configuring Forking Mode



3. Click **Apply**.

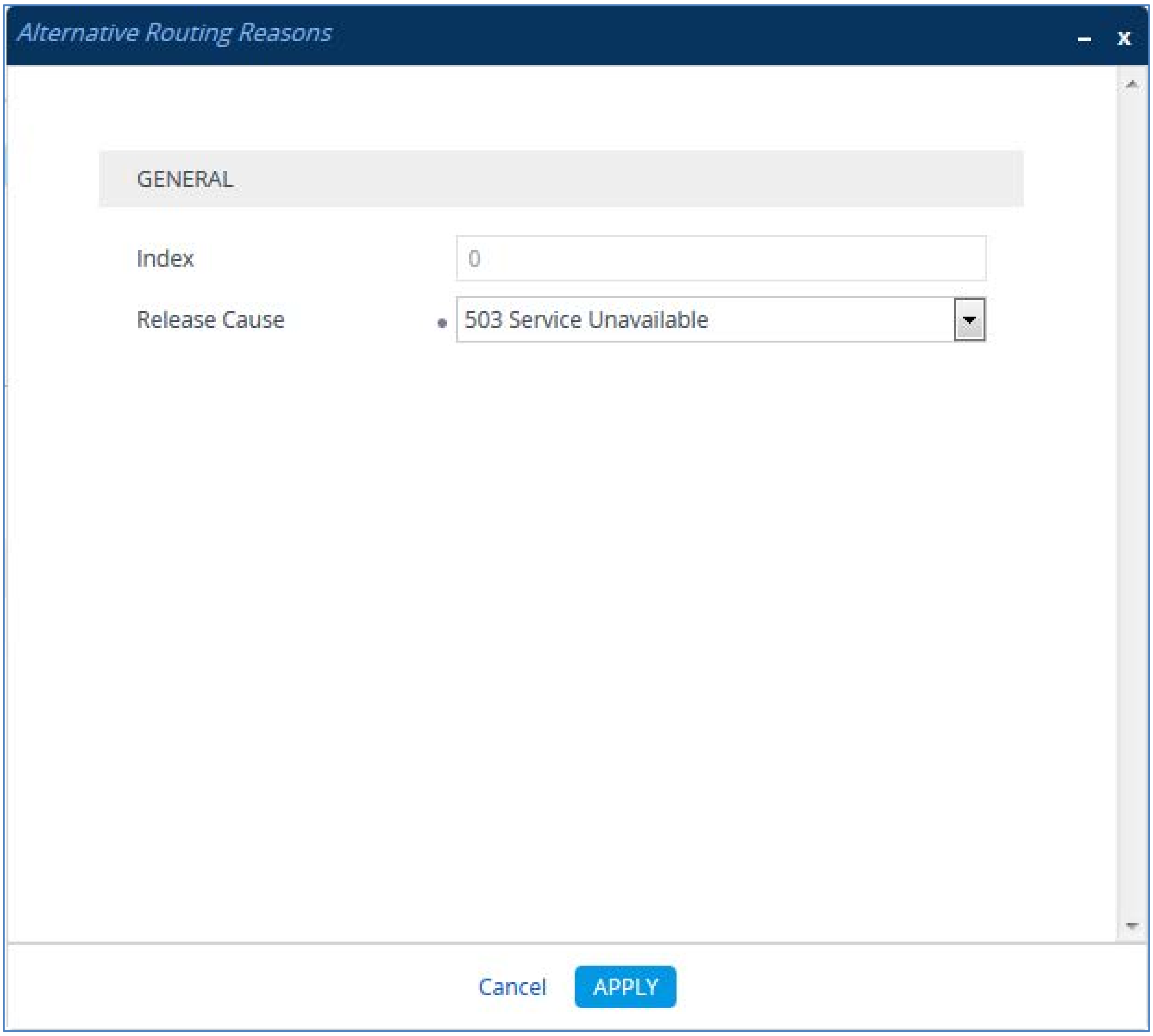
4.14.2 Step 14b: Configure SBC Alternative Routing Reasons

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

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

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons**).
2. Click **New**.
3. From the 'Release Cause' drop-down list, select **503 Service Unavailable**.

Figure 4-54: SBC Alternative Routing Reasons Table



4. Click **Apply**.

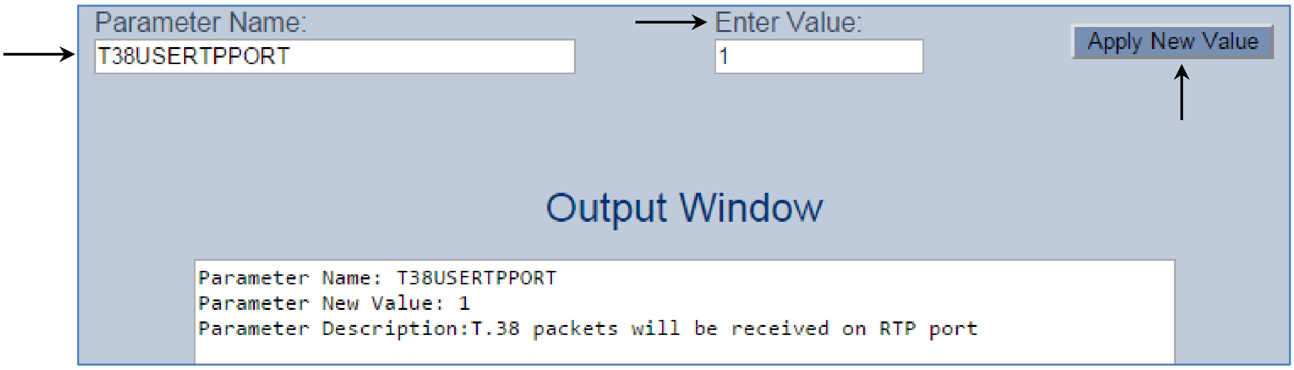
4.14.3 Step 14c: Configure RTP Port for T.38 Fax

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

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

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

Figure 4-55: Configuring SBC to use the same RTP port for T.38 Fax in AdminPage



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

Parameter	Value
T38UseRTPPort	**1**

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

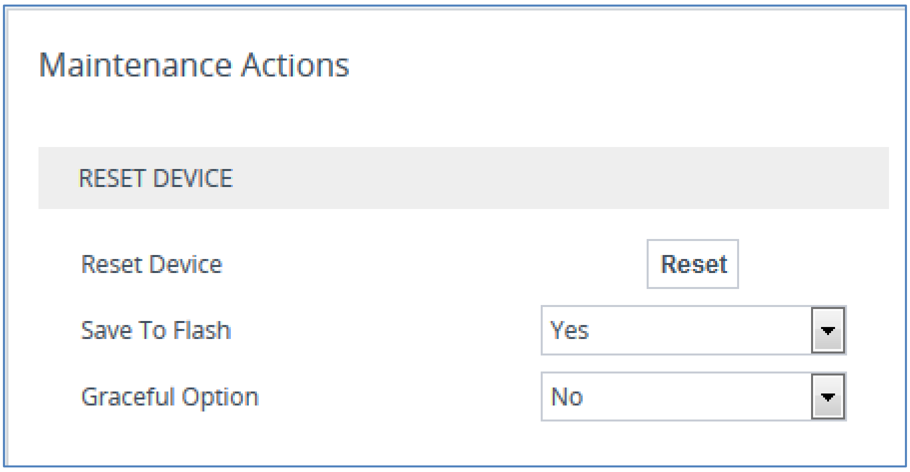
4.15 Step 15: Reset the E-SBC

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

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

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

Figure 4-56: Resetting the E-SBC



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

This page is intentionally left blank.

A AudioCodes INI File

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

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

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

;Board: M500
;HW Board Type: 69 FK Board Type: 77
;Serial Number: 4965606
;Slot Number: 1
;Software Version: 7.20A.202.112
;DSP Software Version: 5014AE3_R => 710.07
;Board IP Address: 10.15.77.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 1  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features:;Board Type: M500 ;Channel Type: DspCh=30 IPMediaDspCh=30
;HA ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;IP Media: VXML ;FXSPorts=3 ;FXOPorts=1 ;Coders: G723
G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB
G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB
OPUS_WB ;DSP Voice features: RTCP-XR ;Control Protocols: MSFT FEU=100
TestCall=100 MGCP SIP SBC=100 ;Default features:;Coders: G711 G726;

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


[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
;SSHAdminKey is hidden but has non-default value
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.27.1'
```

```
;LastConfigChangeTime is hidden but has non-default value
;BarrierFilename is hidden but has non-default value
;LocalTimeZoneName is hidden but has non-default value
PM_gwINVITEDialogs = '1,190,200,15'
PM_gwSUBSCRIBEDialogs = '1,3800,4000,15'
PM_gwSBCRegisteredUsers = '1,570,600,15'
PM_gwSBCMediaLegs = '1,190,200,15'
PM_gwSBCTranscodingSessions = '1,13,15,15'

[BSP Params]

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

[ControlProtocols Params]

AdminStateLockControl = 0

[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UseProductName = 1
;HTTPSPkeyFileName is hidden but has non-default value
FaviconCurrentVersion = 3
Languages = 'en-US', '', '', '', '', '', '', '', '', ''

[SIP Params]

REGISTRATIONTIME = 3600
GWDEBUGLEVEL = 5
T38USERTPPORT = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SBCSESSIONREFRESHINGPOLICY = 1
SBC100TRYINGUPONREINVITE = 0
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
```

```
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

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

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.10, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.157, 24, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]


[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_CliSessionLimit, WebUsers_SessionTimeout, WebUsers_BlockTime,
WebUsers_UserLevel, WebUsers_PwNonce, WebUsers_SSHPublicKey;
WebUsers 0 = "Admin",
"$1$bgtdFkgQREJNFRNJHUhDGRtPTuPju+bhteC1ubG4vby9t7fy9fb1oqfyoKmt+KP5/qz9m
```

```
ZSTlpyUkpDNzMudz54=", 1, 0, 5, -1, 15, 60, 200,
"e4064f90b5b26631d46fbcdb79f2b7a0", ".fc";
WebUsers 1 = "User",
"$1$Cj46OmhtN3ElJiolcSQnfXh4Ii5+Jn4ZRBQRHR0fHx4bTB9ITE8aVgRQVQUGAAEPXVkCD
w0GWSEgIHN0dHB2LHE=", 1, 0, 5, -1, 15, 60, 50,
"c26a27dd91a886b99de5e81b9a736232", "";

[ \WebUsers ]


[ TLSContexts ]

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

[ \TLSContexts ]


[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";

[ \AudioCodersGroups ]


[ AllowedAudioCodersGroups ]

FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "ITSP Allowed Coders";
AllowedAudioCodersGroups 1 = "G.711 Only";

[ \AllowedAudioCodersGroups ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,
IpProfile_RTPRedundancyDepth, IpProfile_CNGmode,
IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia,
IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller,
IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour,
IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
```

```
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionMode,
IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling,
IpProfile_SBCFaxCodersGroupName, IpProfile_SBCFaxBehavior,
IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCFaxReroutingMode,
IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP,
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW,
IpProfile_SBCEnhancedPlc, IpProfile_LocalRingbackTone,
IpProfile_LocalHeldTone, IpProfile_SBCGenerateNoOp,
IpProfile_SBCRemoveUnKnownCrypto;
IpProfile 1 = "S4B", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "", "", 0, 1, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, "", 0, 0, 1, 3, 0, 1, 1, 0, 3, 2, 1, 0, 1, 1, 1, 1, 1, 0,
1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 300, -1, -1,
0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, -1, -1, 0, 0;
IpProfile 2 = "ITSP", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "",
"", "", 0, 2, 0, 0, 0, 1, 0, 8, 300, 400, 1, 0, 0, "", 0, 0, 1, 3, 0, 2,
2, 1, 3, 2, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1,
-1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0;
IpProfile 3 = "Fax", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "",
"", "", 0, 2, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2,
2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1,
-1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0;

[ \IpProfile ]
```

```
[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_RemoteIPv4IF,
CpMediaRealm_RemoteIPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile,
CpMediaRealm_TopologyLocation;
CpMediaRealm 0 = "MRLan", "LAN_IF", "", "", "", 6000, 100, 6999, 0, "",
"", 0;
CpMediaRealm 1 = "MRWan", "WAN_IF", "", "", "", 7000, 100, 7999, 0, "",
"", 1;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]


[ SRD ]

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

[ \SRD ]


[ MessagePolicy ]

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

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
```

```
SIPInterface_AdditionalUDPPorts, SIPInterface_SRDName,
SIPInterface_MessagePolicyName, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation,
SIPInterface_PreParsingManSetName, SIPInterface_AdmissionProfile;
SIPInterface 0 = "SIPInterface_LAN", "LAN_IF", 2, 5060, 0, 5067, "",
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1,
0, 0, "", "";
SIPInterface 1 = "SIPInterface_WAN", "WAN_IF", 2, 5060, 0, 0, "",
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1,
0, 1, "", "";

[ \SIPInterface ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 1 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "", 1, -1, "", "",
"SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 2 = "ITSP", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, 1, "", "",
"SIPInterface_WAN", "", "", 1, 1, 10, -1;
ProxySet 3 = "Fax", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"SIPInterface_LAN", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId, IPGroup_Tags, IPGroup_SBCUserStickiness,
IPGroup_UserUDPPortAssignment, IPGroup_AdmissionProfile;
```

```
IPGroup 0 = 0, "Default_IPG", "", "", "", -1, 0, "DefaultSRD", "", 0, "",
-1, -1, -1, 0, 0, "", 0, -1, -1, "", "Admin", "$1$aCkNBwIC", 0, "", "",
0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "";
IPGroup 1 = 0, "S4B", "S4B", "siptrunk3.voice.ewetel.de", "", -1, 0,
"DefaultSRD", "MRLan", 1, "S4B", -1, -1, -1, 0, 0, "", 0, -1, -1, "",
"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 0, "", -1, "", 0, 0, "";
IPGroup 2 = 0, "ITSP", "ITSP", "siptrunk3.voice.ewetel.de", "", -1, 0,
"DefaultSRD", "MRWan", 1, "ITSP", -1, -1, 4, 0, 0, "", 0, -1, -1, "",
"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 1, "", -1, "", 0, 0, "";
IPGroup 3 = 0, "Fax", "Fax", "siptrunk3.voice.ewetel.de", "", -1, 0,
"DefaultSRD", "MRLan", 1, "Fax", -1, -1, -1, 0, 0, "", 0, -1, -1, "",
"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 0, "", -1, "", 0, 0, "";

[ \IPGroup ]


[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "1", 0, "FE.S4B.interop:5067", 2;
ProxyIp 1 = "2", 0, "siptrunk3.voice.ewetel.de:5060", 0;
ProxyIp 3 = "3", 0, "10.15.77.14:5060", 0;

[ \ProxyIp ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_ContactUser,
Account_Register, Account_RegistrarStickiness,
Account_RegistrarSearchMode, Account_RegEventPackageSubscription,
Account_ApplicationType, Account_RegByServedIPG,
Account_UDPPortAssignment;
Account 0 = -1, "S4B", "ITSP", "1234567890", "$1$aCkNBwIC", "",
"1234567890", 1, 0, 0, 0, 2, 0, 0;
Account 1 = -1, "Fax", "ITSP", "1234567890", "$1$aCkNBwIC", "",
"1234567890", 1, 0, 0, 0, 2, 0, 0;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
```

```
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName,
IP2IPRouting_RoutingTagName, IP2IPRouting_InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 1 = "S4B Refer", "Default_SBCRoutingPolicy", "Any", "*",
"*", "*", "*", 0, "", "S4B", 2, -1, 2, "S4B", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";
IP2IPRouting 2 = "S4B to ITSP", "Default_SBCRoutingPolicy", "S4B", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "ITSP", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";
IP2IPRouting 3 = "ITSP to Fax", "Default_SBCRoutingPolicy", "ITSP", "*",
"*", "+4944136153305", "*", 0, "", "Any", 0, -1, 0, "Fax", "", "", 0, -1,
0, 0, "", "", "", "", "default", "";
IP2IPRouting 4 = "ITSP to S4B", "Default_SBCRoutingPolicy", "ITSP", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "S4B", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";
IP2IPRouting 5 = "Fax to ITSP", "Default_SBCRoutingPolicy", "Fax", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "ITSP", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";

[ \IP2IPRouting ]


[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "To Emergency do nothing",
"Default_SBCRoutingPolicy", 0, "Any", "ITSP", "*", "*", "[110, 112]",
"*", "*", "", 0, "Any", 0, 1, 0, 0, 255, "", "", 0, "", "";
IPOutboundManipulation 1 = "To Emergency strip +",
"Default_SBCRoutingPolicy", 0, "Any", "ITSP", "*", "*", "[+110, +112]",
"*", "*", "", 0, "Any", 0, 1, 1, 0, 255, "", "", 0, "", "";
IPOutboundManipulation 2 = "Do Nothing", "Default_SBCRoutingPolicy", 0,
"Any", "ITSP", "*", "*", "+", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255,
"", "", 0, "", "";
```

```
IPOutboundManipulation 3 = "Add +", "Default_SBCRoutingPolicy", 0, "Any",
"ITSP", "*", "*", "*", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255, "+", "",
0, "", "";
IPOutboundManipulation 4 = "Replace 00 to + toward SfB",
"Default_SBCRoutingPolicy", 0, "ITSP", "S4B", "00", "*", "*", "*", "*",
"", 0, "Any", 0, 0, 2, 0, 255, "+", "", 0, "", "";

[ \IPOutboundManipulation ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Call Forward", 4, "Invite.Request",
"Header.History-Info exists", "header.history-info", 1, "", 0;
MessageManipulations 1 = "Call Forward", 4, "Invite.Request", "",
"Header.Diversion.URL.Host", 2, "Param.IPG.Dst.Host", 0;
MessageManipulations 2 = "Call Forward", 4, "Invite.Request",
"Header.Diversion exists", "Header.From.URL.User", 2,
"Header.Diversion.URL.User", 0;
MessageManipulations 3 = "Call Transfer", 4, "Invite.Request",
"Header.Referred-By exists", "Header.Referred-By.URL.Host", 2,
"Param.IPG.Dst.Host", 0;
MessageManipulations 4 = "Call Transfer", 4, "Invite.Request",
"Header.Referred-By exists", "Header.From.URL.User", 2, "Header.Referred-
By.URL.User", 0;
MessageManipulations 5 = "Error Responses", 4, "Any.Response",
"Header.Request-URI.MethodType == '480' 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, 0, "";

[ \GwRoutingPolicy ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

```
[ MaliciousSignatureDB ]

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

[ \MaliciousSignatureDB ]


[ AllowedAudioCoders ]

FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 0 = "ITSP Allowed Coders", 0, 1, "";
AllowedAudioCoders 2 = "G.711 Only", 0, 1, "";

[ \AllowedAudioCoders ]


[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 1, "";
AudioCoders 4 = "AudioCodersGroups_0", 1, 2, 2, 90, -1, 1, "";

[ \AudioCoders ]
```

This page is intentionally left blank.

B Configuring Analog Devices (ATAs) for Fax Support

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

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

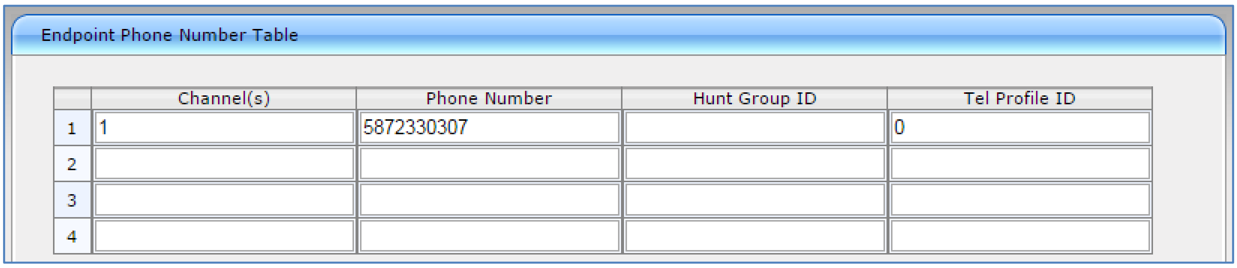
B.1 Step 1: Configure the Endpoint Phone Number Table

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

➢ **To configure the Endpoint Phone Number table:**

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

Figure B-1: Endpoint Phone Number Table Page



Endpoint Phone Number Table

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

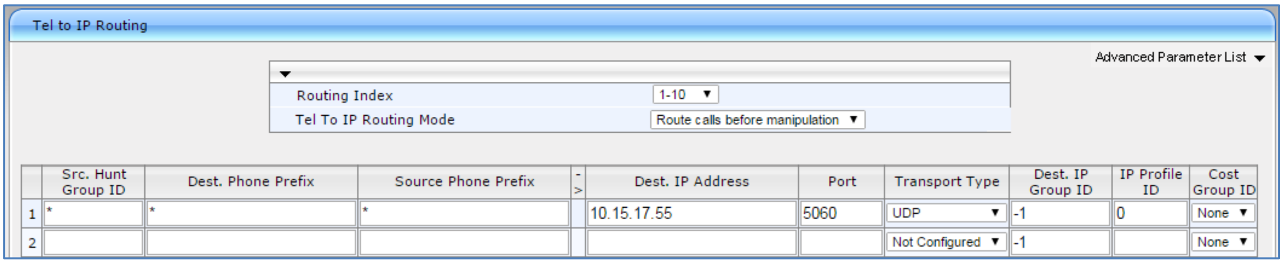
B.2 Step 2: Configure Tel to IP Routing Table

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

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

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

Figure B-2: Tel to IP Routing Page



Tel to IP Routing

Advanced Parameter List

Routing Index	1-10
Tel To IP Routing Mode	Route calls before manipulation

	Src. Hunt Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Port	Transport Type	Dest. IP Group ID	IP Profile ID	Cost Group ID
1	*	*	*		10.15.17.55	5060	UDP	-1	0	None
2							Not Configured	-1		None

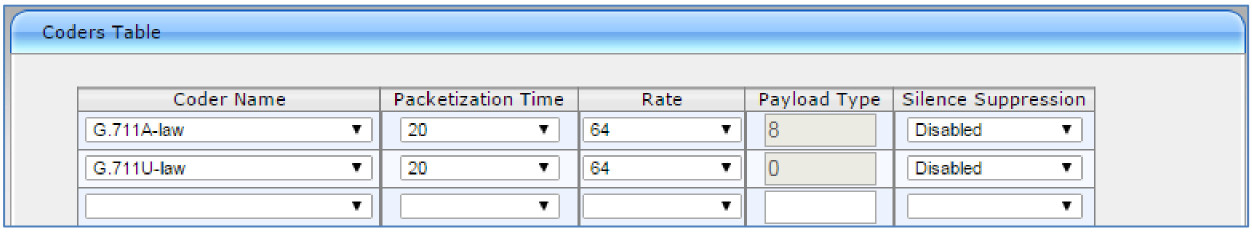
B.3 Step 3: Configure Coders Table

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

➢ **To configure MP-11x coders:**

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

Figure B-3: Coders Table Page



Coders Table

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

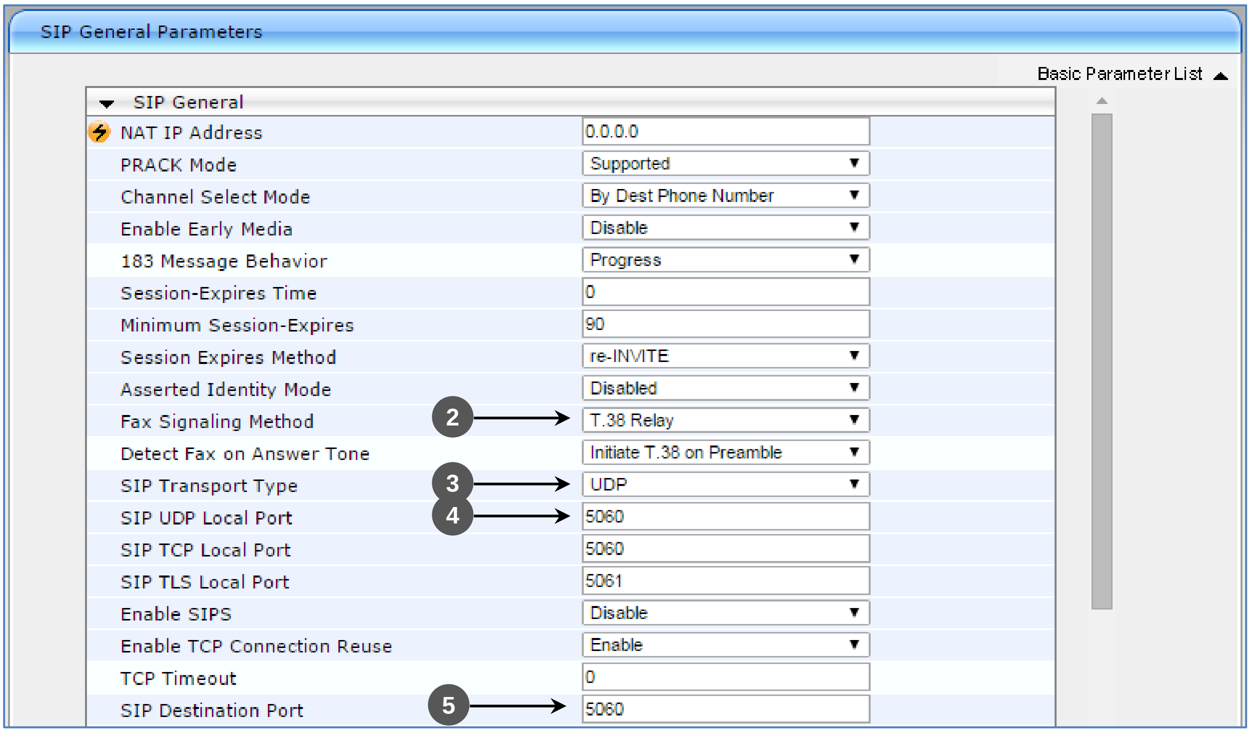
B.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

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

➢ **To configure the fax signaling method:**

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

Figure B-4: SIP General Parameters Page



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

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

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

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

Document #: LTRT-12895