APPLICATION NOTE: TC-16030

Integrating ShoreTel with Microsoft Skype for Business via AudioCodes E-SBC (SIP)

Microsoft Skype for Business and AudioCodes Mediant E-SBC Family

Contents

ST Doc Number	TC - 15010
Version	2.0
Date	October, 2015

960 Stewart Drive, Sunnyvale, CA 94085, USA +1 (800) 425-9385 Toll Free +1 (408) 331-3300 Tel.
ShoreTel.com

1 Overview

The purpose of this application note is to illustrate integrating the ShoreTel UC system with Microsoft (MS) Skype for Business for delivering voice calls between the two systems. This integration allows Skype for Business audio conferencing calls to and from external callers via trunks on the ShoreTel system. The same steps are required to enable users on either system to place voice calls to one another (extension to extension dialing).

This application note **does not** provide details on the following integration features:

- MS Outlook Voicemail integration for client-side unified messaging
- MS Outlook Calendar integration for automated call handling mode changes
- MS Outlook Calendar integration for automated conference bridge details within appointments
- MS Outlook Contact importing for easy dial-by-name and dial-by-company
- TAPI integration for dialing directly from within Outlook contacts
- MS Exchange integration for server-side unified messaging
- MS Skype for Business integration for IM, presence, or remote call control

This document focuses exclusively on the integration of MS Skype for Business “Enterprise Voice” capabilities with the ShoreTel UC system via the AudioCodes Mediant E-SBC products. Refer to other application notes and product documentation for details on all of the other integration methods. Please see the ‘References and Resources” section at the end of this document for a complete listing of related documentation and other configuration resources.

MS Skype for Business enterprise voice access to the public switched telephony network (PSTN) can be delivered via ShoreTel voice switches and the AudioCodes Mediant family of session border controllers. Microsoft Skype for Business audio conferencing users and ShoreTel IP phone users can place, transfer, and conference calls between the two systems.

1.1 Required Components

1. Any of the following AudioCodes Mediant E-SBC products
   - Mediant 500 E-SBC
   - Mediant 800 Gateway & E-SBC
   - Mediant 1000B Gateway & E-SBC
   - Mediant 2600 E-SBC
   - Mediant 3000 Gateway & E-SBC
   - Mediant 4000 SBC
   - Mediant 9000 SBC
   - Mediant Software SBC (Server Edition and Virtual Edition)
2. Microsoft Skype for Business Server 2015 with Mediation Server configured
3. One or more ShoreTel Voice physical or Virtual Switches with available SIP trunk capacity

Test were performed to ensure direct call, transfer, forward, hold/resume, Music on Hold, long call, long hold, pre-answer abandon, pre-transfer abandon, and other similar features and functionality were integrated properly and fully functional between the Microsoft Skype for Business environment and the ShoreTel environment.

Observed limitations: No limitations were observed when using ShoreTel Virtual or hardware switch and the default SIP Trunk Profile 'Default ITSP' was used for SIP Trunks between the AudioCodes device and the ShoreTel switch

1.2 Supported and Tested Versions

This document is written based on testing with the following versions of software:

- ShoreTel 14.2_Build_19.45.8701.0
- Microsoft Skype for Business Server Release 2015 6.0.9319.0
- AudioCodes Mediant 800 version 7.00A.035.012

Functionality differences based on future software updates from ShoreTel, AudioCodes, and Microsoft will be reflected as needed via updates to this document and other supporting resources. See the 'References and Resources" section at the end of this document.

1.3 Important Disclaimer

This document is for informational purposes only and is provided "AS IS". Microsoft and its partners cannot verify the accuracy of this information and take no responsibility for the content of this document. To the extent permitted by law, **Microsoft makes no warranties of any kind, disclaims all express, implied and statutory warranties, and assumes no liability to you for any damages of any type in connection with the content of this document.**

1.4 Intended Audience

The information provided in this document has been provided by Microsoft Partners or equipment manufactures and is provided "AS IS". This document contains information about how to modify the configuration of your PBX or VoIP gateway. Improper configuration may result in the loss of service of the PBX or gateway. Microsoft is unable to provide support or assistance with the configuration or troubleshooting of components described within. Microsoft recommends readers to engage the service of a Microsoft Skype for Business specialist or the manufacturers of the equipment described within to assist with the planning and deployment of Skype for Business 2015.

1.5 AudioCodes Mediant Products

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.

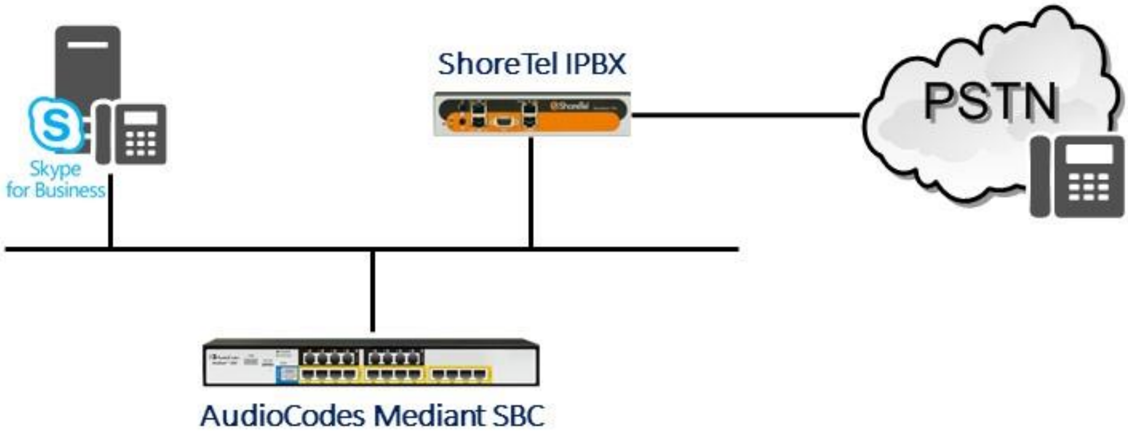


Figure 1 – Microsoft Skype for Busines and ShoreTel Interconnected via AudioCodes

1.6 Initial Configuration

The configuration information described in this document shows examples for configuring ShoreTel and the AudioCodes E-SBC. Even though configuration requirements can vary from setup to setup, the information provided in these steps, along with that found in the *ShoreTel Planning and Installation Guide* and the documentation provided by AudioCodes and Microsoft, should prove to be sufficient. However every design can vary and some may require more planning than others.

2 ShoreTel Configuration

This section describes the ShoreTel system configuration to support SIP Trunking. The section is divided into general system settings and trunk configurations (both group and individual) needed to support SIP Trunking.

2.1 ShoreTel System Settings – General

The first settings to address within the ShoreTel system are the general system settings. These configurations include the Call Control, the Site and the Switch settings. If these items have already been configured on your system, skip this section and go on to the “ShoreTel System Settings – Trunk Groups” section below.

2.2 Call Control Settings

The first settings to configure within ShoreTel Director are the Call Control Options. To configure these settings for the ShoreTel system, log into ShoreTel Director and select “Administration” then “Call Control” followed by “Options” – the “Call Control Options” screen will then appear (**Figure 2**).

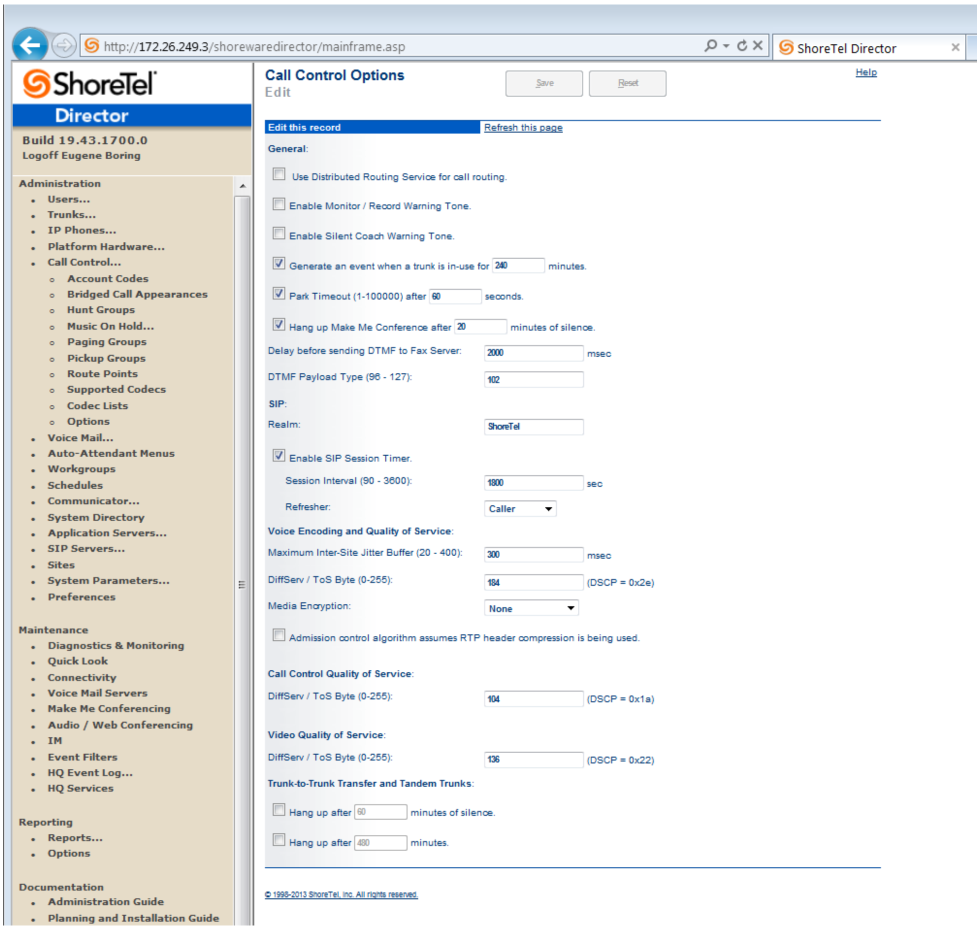


Figure 2 – Call Control Options Screen

Within the “Call Control Options” SIP parameters; confirm that the appropriate settings are made for the “Realm” and “Enable SIP Session Timer”.

The “Realm” parameter is used in authenticating all SIP devices. It is typically a description of the computer or system being accessed. Changing this value will require a reboot of all ShoreTel switches serving SIP extensions. It is not necessary to modify this parameter to get the ShoreTel IP PBX system functional with AudioCodes gateway.

Step 1 Verify that the “Enable SIP Session Timer” box is checked (enabled).

Step 2 Set the Session Interval Time to the recommended setting of 3600 seconds.

Step 3 Select the appropriate refresher (from the pull down menu) for the SIP Session Timer. The “Refresher” field will be set either to “Caller (UAC)” [User Agent Client] or to “Callee (UAS)” [User Agent Server]. If the “Refresher” field is set to “Caller (UAC)”, the Caller’s device will be in control of the session timer refresh. If “Refresher” is set to “Callee (UAS)”, the device of the person called will control the session timer refresh.

Step 4 Verify the “Voice Encoding and Quality of Service”, specifically the “Media Encryption” parameter. Make sure this parameter is set to “None”; otherwise you may experience one-way audio issues. Please refer to *ShoreTel Administration Guide* for additional details on media encryption and the other parameters in the “Voice Encoding and Quality of Service” area.

Step 5 Disable (uncheck) the “Always Use Port 5004 for RTP” parameter if checked; it is required for implementing SIP trunks between ShoreTel systems only. For SIP configurations, Dynamic User Datagram Protocol (UDP) must be used for RTP Traffic. If the parameter is disabled, Media Gateway Control Protocol (MGCP) will no longer use UDP port 5004; MGCP and SIP traffic will use dynamic UDP ports **(Figure 3)**.

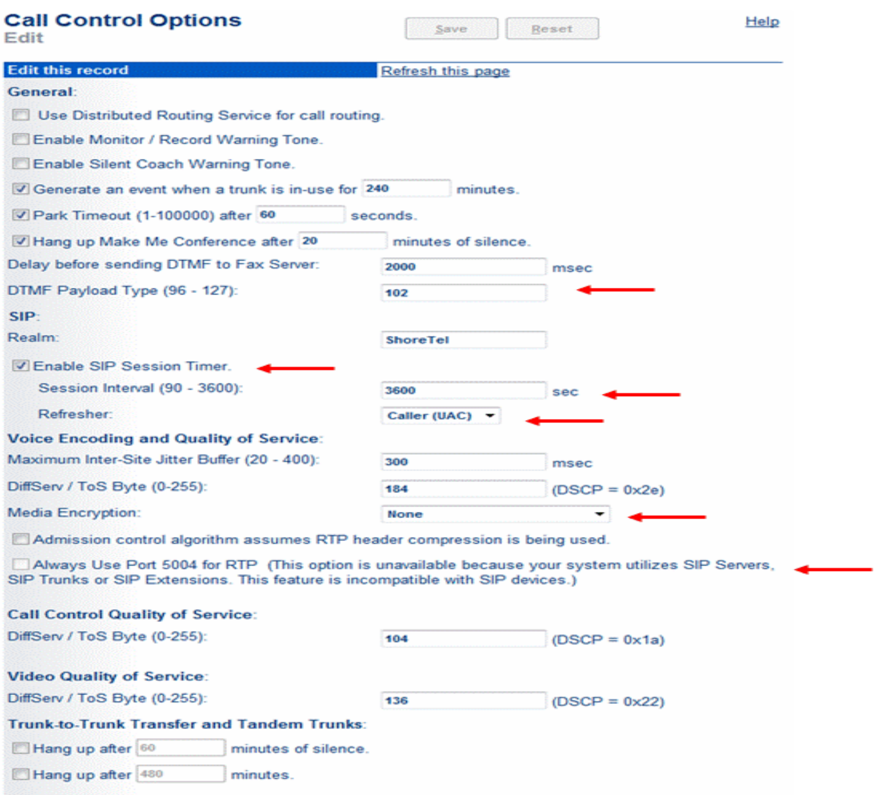


Figure 3 – Call Control Options Settings

Once this parameter is unchecked, make sure that “everything” (IP Phones, ShoreTel Voice Switches, ShoreTel Server, Distributed Voice Mail Servers / Remote Servers, Conference Bridges and Contact Centers) is “fully” rebooted – this is a “one time only” item. By not performing a full system reboot after changing this setting, one-way audio may occur during initial testing.

Step 6 Be sure to save your changes before leaving this screen by clicking Save at the top of the page.

2.3 Sites Settings

The next settings to address are the administration of sites. These settings are modified under the ShoreTel Director by selecting “Administration” then “Sites”.

This selection brings up the “Sites” screen.

Step 1 Within the “Sites” screen select the name of the site to configure. The “Edit Site” screen will then appear.

The only changes required to the “Edit Site” screen are to the “Admission Control Bandwidth” and “Intra-Site / Inter-Site Calls” parameters (**Figure 4**).

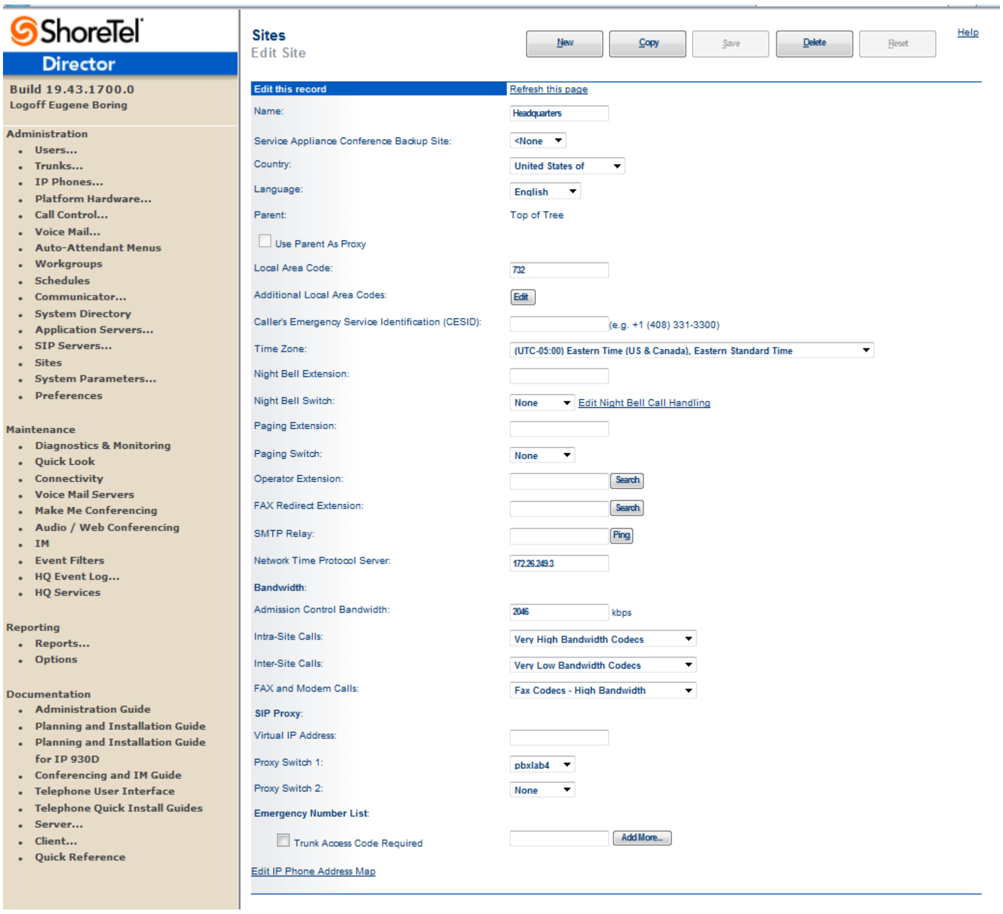


Figure 4 – Site Bandwidth settings

Step 2 Set the appropriate Admission Control Bandwidth for your network. Please refer to the *ShoreTel Planning and Installation Guide* for additional information on setting Admission Control Bandwidth for your network. Admission Control Bandwidth defines the bandwidth available to and from the site. This is important as SIP trunk calls will be counted against the site bandwidth.

Note: Bandwidth of 2046 kbps is just an example.

Step 3 Configure the "Inter-Site Calls" option for "Very Low Bandwidth Codecs." By default, "Very Low Bandwidth Codecs" contains four codecs, with G.729 being the primary codec of choice. The “Inter-Site Calls” parameter defines which codecs will be used when establishing a call with AudioCodes – the preferred codec choice is G.729.

Step 4 Save changes before leaving this screen by clicking **Save** at the top of the page.

2.4 Switch Settings - Allocating Ports for SIP Trunks

The final general settings to configure are the ShoreTel switch settings. These changes are modified by selecting “Administration” then “Switches” followed by “Primary” in ShoreTel Director (**Figure 5)**.

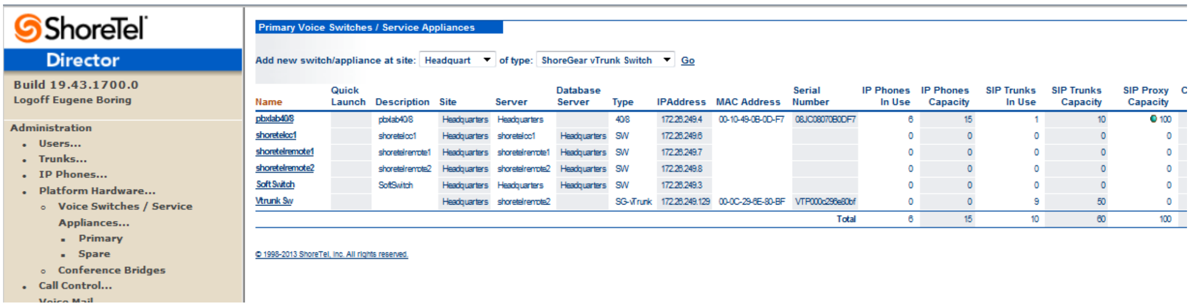


Figure 5 – Administration Switches

This action brings up the “Switches” screen. From the “Switches” screen, choose the name of the switch to configure for SIP trunks. The “Edit ShoreTel Switch” screen will appear.

Step 1 Within the “Edit ShoreTel Switch” screen, select the desired number of SIP Trunks from the ports available (**Figure 6**).

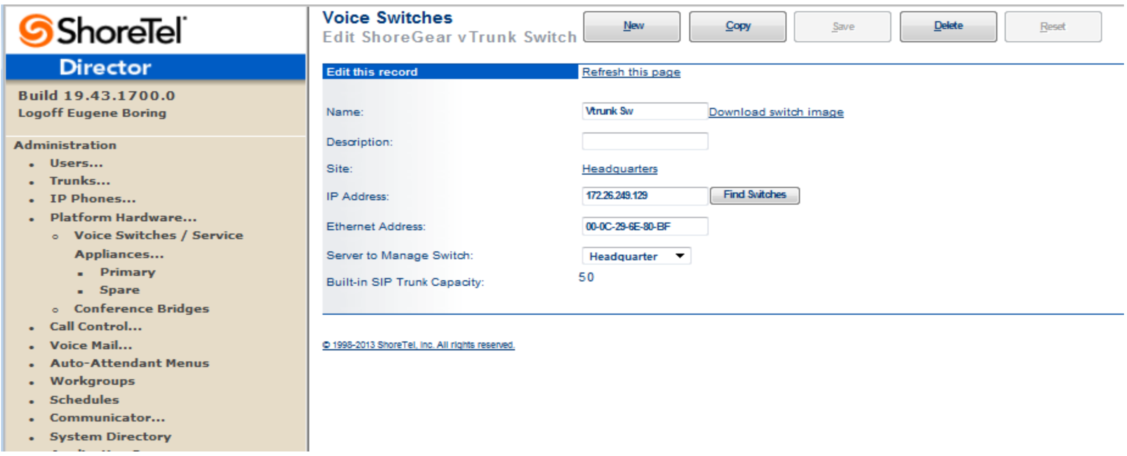


Figure 6 – ShoreTel Switch Settings

Each port designated as a Port Type of “SIP Trunk with Media Proxy” enables the support for five individual SIP trunks. The AudioCodes Mediant 1000 can be configured for up to 120 SIP trunks. Each trunk can support one concurrent call between the ShoreTel system and the Microsoft Skype for Business 2015 system. Determine the desired capacity of the interconnection between the two systems and configure the necessary resources as required, then proceed to the next section.

Step 2 Be sure to save your changes before leaving this screen by clicking Save at the top of the page.

2.5 ShoreTel System Settings – Trunk Groups

ShoreTel Trunk Groups only support Static IP Addresses for Individual Trunks.

In trunk planning, the following needs to be considered. AudioCodes gateway interfaces should always be configured to use a “static” IP Address.

The settings for Trunk Groups are changed by selecting “Administration”, then “Trunks” followed by “Trunk Groups” within ShoreTel Director (**Figure 7**).

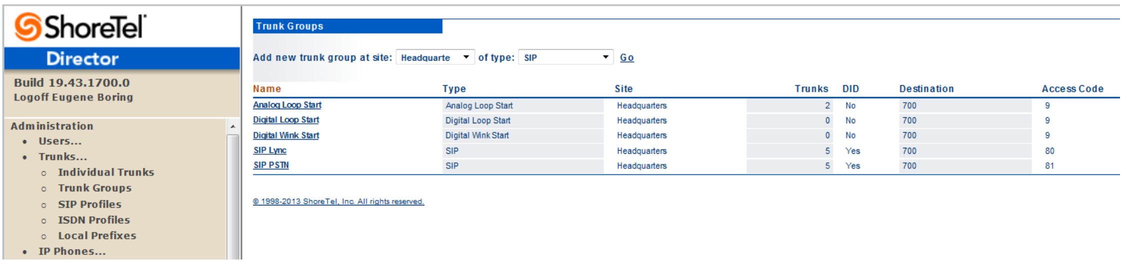


Figure 7 – Administration Trunk Groups

2.6 ShoreTel System Settings – SIP Trunks Configuration

For our test configuration, two trunk groups will be created:

First trunk group called “SIP PSTN” is to connect ShoreTel PBX to a simulated SIP Trunk Provider.

Second trunk group called “SIP Lync” is to connect ShoreTel PBX to the Skype for Business.

The configuration steps identical for both trunk groups.

Step 1 From the pull down menus on the “Trunk Groups” screen, select the site desired and select the “SIP” trunk type to configure.

Step 2 Click on the “Go” link from “Add new trunk group at site”. The “Edit SIP Trunk Group” screen will appear.

Step 3 Enter your preferred name for the new trunk group. In the example in Figure 8, the name “SIP PSTN” has been created.

Step 4 The “Enable SIP Info for G.711 DTMF Signaling” parameter should not be enabled (checked). Enabling SIP info is currently only used with SIP tie trunks between ShoreTel systems.

Step 5 The “Profile:” parameter is should be left at a default setting of “Default ITSP”; It is not necessary to modify this parameter when connecting to the AudioCodes gateway.

Step 6 The “Enable Digest Authentication” parameter defaults to “<None>” and modification is not required when connecting to the AudioCodes gateway

Step 7 Within the “Inbound:” settings, ensure the “Number of Digits from CO” is set to match what the ShoreTel SIP trunk switch will be receiving from AudioCodes gateway and ensure the “DNIS” or “DID” box is enabled (checked), along with the Extension parameter.

Step 8 We recommend that the Tandem Trunking parameter be enabled (checked) otherwise transfers to external telephone numbers will fail via SIP trunks. For additional information on this parameter, please refer to the *ShoreTel Planning and Installation Guide*.

The next item to change in the “Edit SIP Trunks Group” screen is to make the appropriate settings for the “Outbound:” parameters

Step 9 Enable (check) the “Outbound” parameter and define a Trunk “Access Code” and “Local Area Code” as appropriate.

In the “Trunk Services:” area, make sure the appropriate services are enabled or disabled based on your needs. In general, we are only using this trunk group to dial the off system extensions to reach the Skype for Business audio conferencing bridge or softphone users.

The last parameter determines if the call is sent out as <unknown> or with caller information (Caller ID). User DID will impact how information is passed out to the SIP Trunk group.

The final parameters for configuration in the Trunk Group are “Trunk Digit Manipulation”

ShoreTel
Brilliantly simple

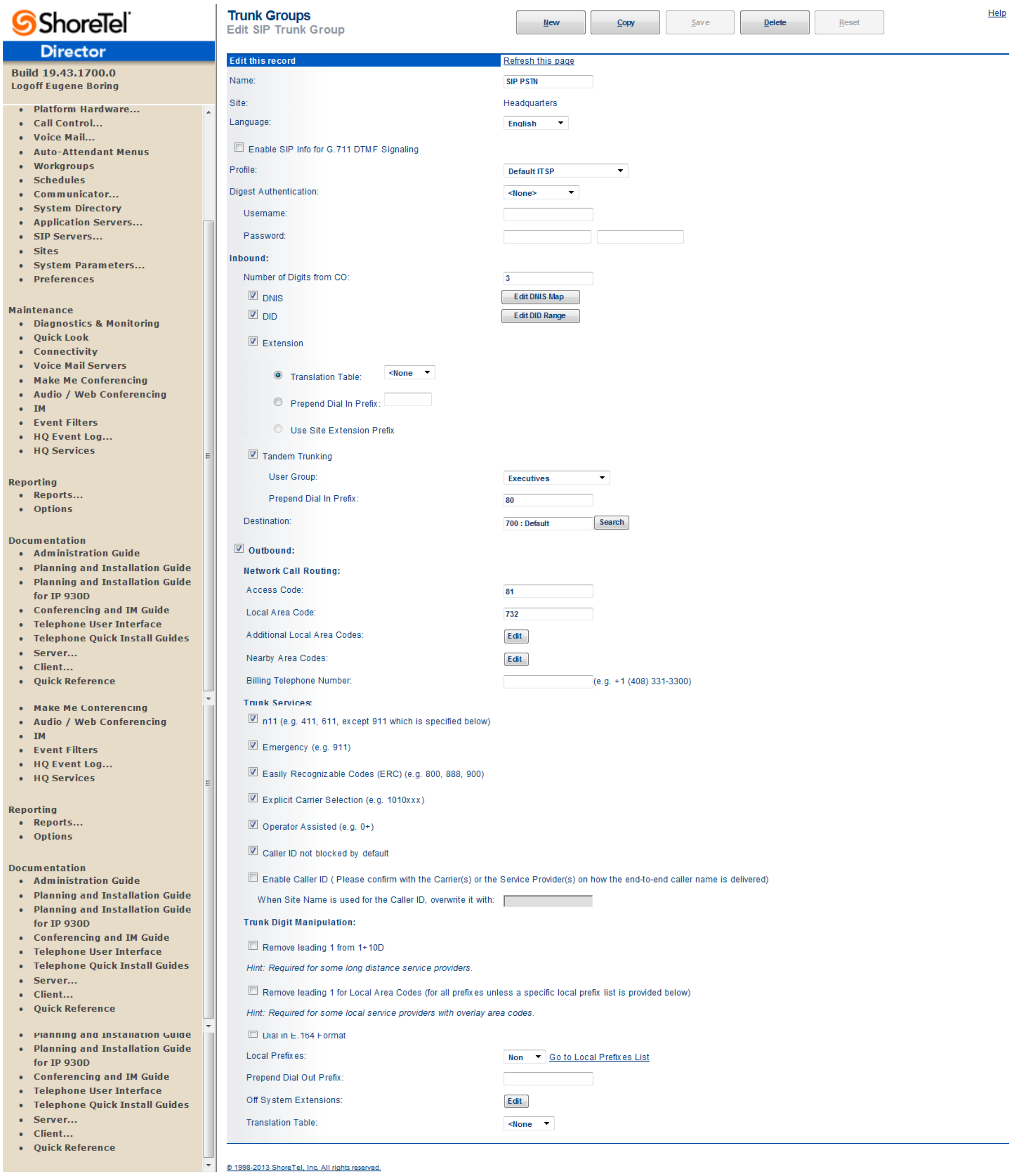


Figure 8 – SIP PSTN Trunk Group

Next you must create the Off System Extension (OSE) range that will be used to represent Skype for Business softphone users or simulated SIP PSTN phone numbers. An OSE is required for every Skype for Business enterprise voice endpoint that will be using the ShoreTel system.

Step 10 Click the Edit button next to Off System Extensions:. The Off Systems Extension Range dialog is displayed (Figure 8a)

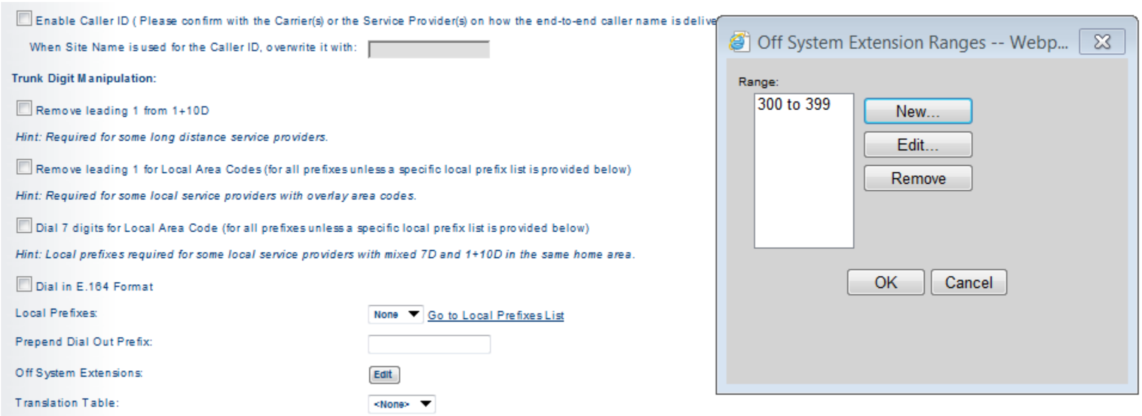


Figure 8a – SIP PSTN Trunk Group with off system extensions

Step 11 Click "New" and define the first range for the extensions that will represent the Skype for Business enterprise voice endpoints on ShoreTel system or simulated SIP PSTN phone numbers.

Step 12 Click "OK" to save the first range and repeat if necessary.

Step 13 After all your setting changes are made to the "Edit SIP Trunk Group" screen, click the "Save" button at the top of the page.

ShoreTel
Brilliantly simple

2.7 SIP Skype for Business Trunk Group

Second trunk group called “SIP Lync” is to connect ShoreTel PBX to Skype for Business. The configuration steps identical for both trunk groups

Step 1 From the pull down menus on the “Trunk Groups” screen, select the site desired and select the “SIP” trunk type to configure.

Step 2 Click on the “Go” link from “Add new trunk group at site”. The “Edit SIP Trunk Group” screen will appear.

Step 3 Enter your preferred name for the new trunk group. In the example in Figure 9, the name “SIP Lync” has been created.

Step 4 The “Enable SIP Info for G.711 DTMF Signaling” parameter should not be enabled (checked). Enabling SIP info is currently only used with SIP tie trunks between ShoreTel systems.

Step 5 The “Profile:” parameter is should be left at a default setting of “Default ITSP”; It is not necessary to modify this parameter when connecting to the AudioCodes gateway.

Step 6 The “Enable Digest Authentication” parameter defaults to “<None>” and modification is not required when connecting to the AudioCodes gateway

Step 7 Within the “Inbound:” settings, ensure the “Number of Digits from CO” is set to match what the ShoreTel SIP trunk switch will be receiving from AudioCodes gateway and ensure the “DNIS” or “DID” box is enabled (checked), along with the Extension parameter.

Step 8 We recommend that the Tandem Trunking parameter be enabled (checked) otherwise transfers to external telephone numbers will fail via SIP trunks. For additional information on this parameter, please refer to the *ShoreTel Planning and Installation Guide*.

The next item to change in the “Edit SIP Trunks Group” screen is to make the appropriate settings for the “Outbound:” parameters.

Step 9 Enable (check) the “Outbound” parameter and define a Trunk “Access Code” and “Local Area Code” as appropriate.

In the “Trunk Services:” area, make sure the appropriate services are enabled or disabled based on your needs. In general, we are only using this trunk group to dial the off system extensions to reach the Skype for Business audio conferencing bridge or softphone users.

The last parameter determines if the call is sent out as <unknown> or with caller information (Caller ID). User DID will impact how information is passed out to the SIP Trunk group.

The final parameters for configuration in the Trunk Group are “Trunk Digit Manipulation”

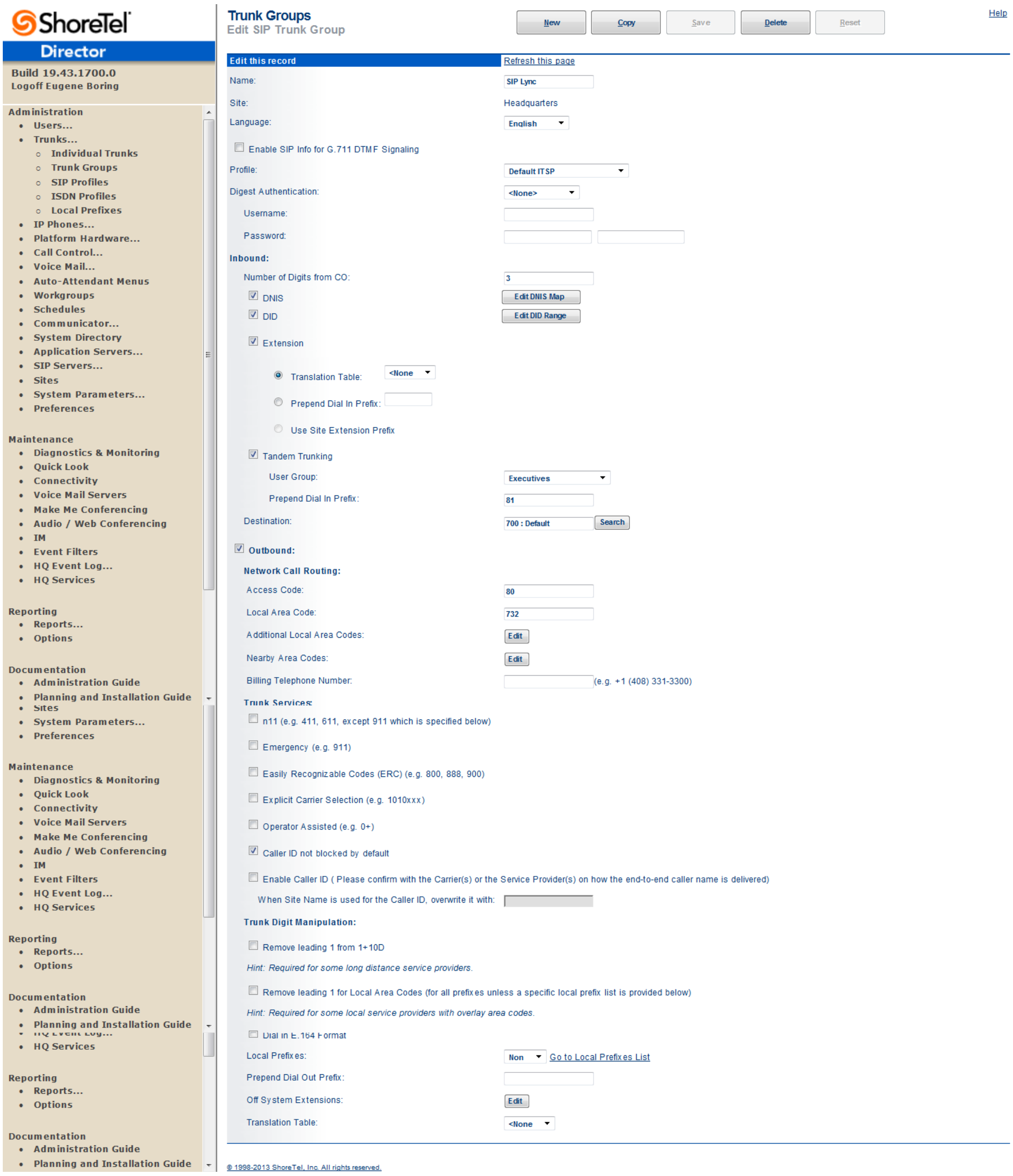


Figure 9 – SIP Lync Trunk Group

Step 10 Click the "Edit" button next to "Off System Extensions:". The Off Systems Extension Range dialog is displayed (Figure 9a)

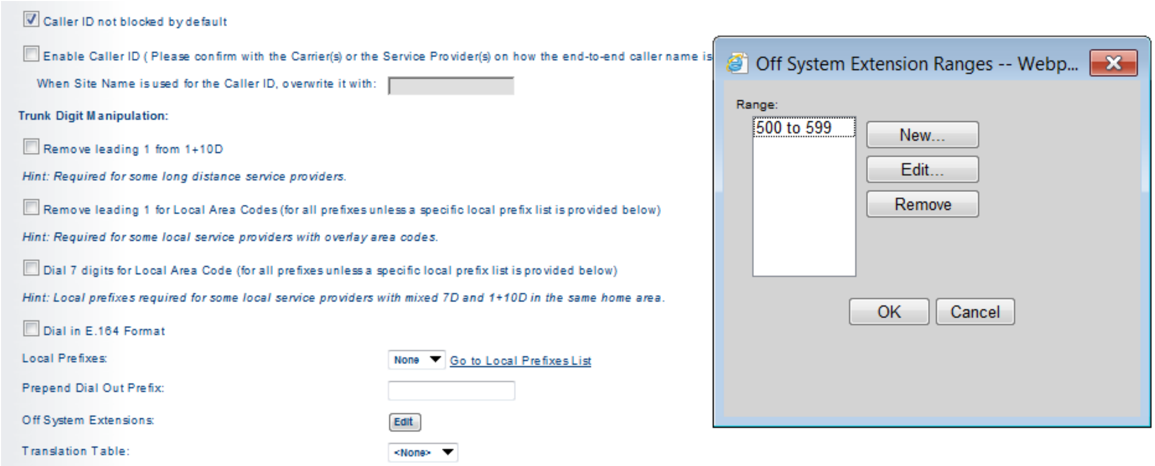


Figure 9a – SIP PSTN Trunk Group with off system extensions

Step 11 Click "New" and define the first range for the extensions that will represent the Skype for Business enterprise voice endpoints on ShoreTel system or simulated SIP PSTN phone numbers

Step 12 Click "OK" to save the first range and repeat if necessary.

Step 13 After all your setting changes are made to the "Edit SIP Trunk Group" screen, click the "Save" button at the top of the page.

2.8 ShoreTel System Settings – Individual Trunks

Before starting individual trunks configuration, verify that ShoreTel switch for new trunks is available.

Select “Administration”, then “Platform Hardware”, then “Voice Switches”, then “Primary“.

In our configuration switch, “SG30” is present.

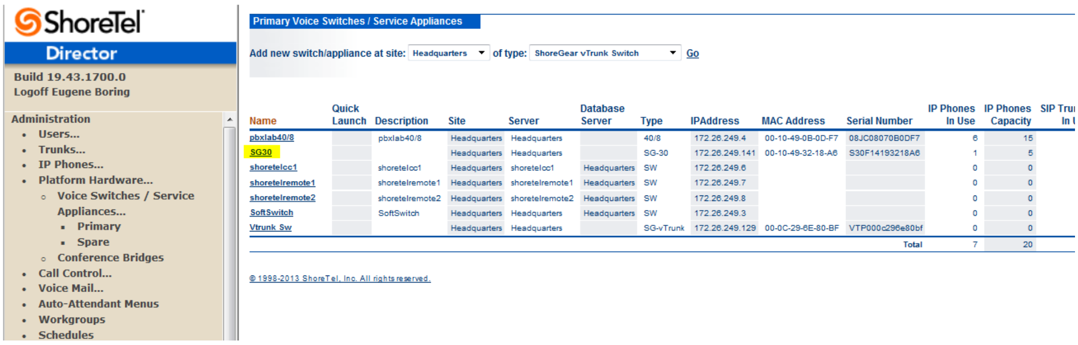


Figure 10 – Administration Switches (SG30)

This section covers the configuration of the individual trunks. Select “Administration”, then “Trunks” followed by “Individual Trunks” to configure the individual trunks.

Step 1 Select the site for the new individual trunk(s) to be added and select the appropriate trunk group from the pull down menu in the “Add new trunk at site” area as shown in **Figure 11**. In this example, the site is “Headquarters” and the trunk group is “SIP PSTN”, as created above.

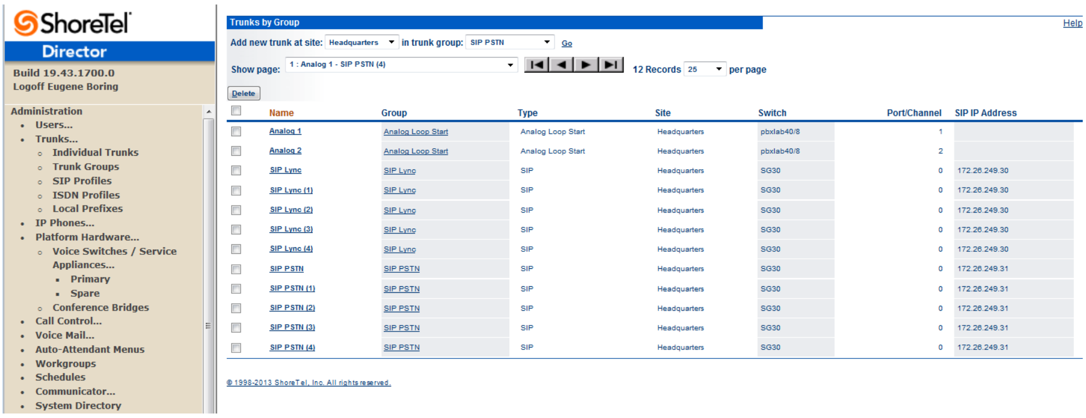


Figure 11 – Trunks by Group (trunks are using SG30 switch)

Step 2 Click on the “Go” button to bring up the “Edit Trunk” screen.

Step 3 From the individual trunks “Edit Trunk” screen, input a name for the individual trunks. When selecting a name, the recommendation is to name the individual trunks the same as the name of the trunk group so that the trunk type can easily be tracked.

Step 4 For the “Switch:” select the switch upon which the individual trunk will be created. For the “IP Address”, enter the IP address of the AudioCodes gateway or simulated SIP trunk provider.

Step 5 Select the number of individual trunks desired (each one supports “one” audio path – for example if 10 is configured, then 10 audio paths can be active at one time).

Step 6 Click Save

Step 7 Repeat steps 1-6 for creating SIP PSTN Trunks as shown in Figure 14.

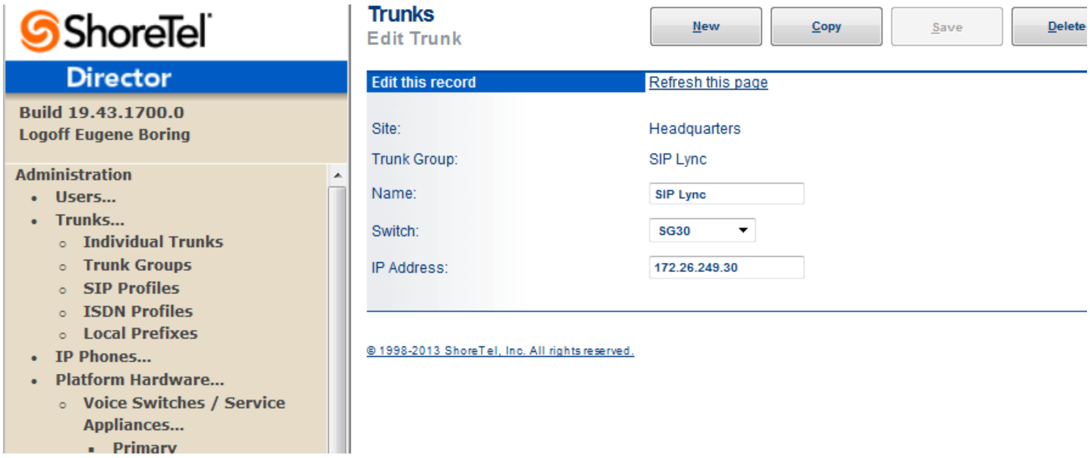


Figure 12 – Individual trunk setting (SG30 switch) for Skype for Business Trunk group

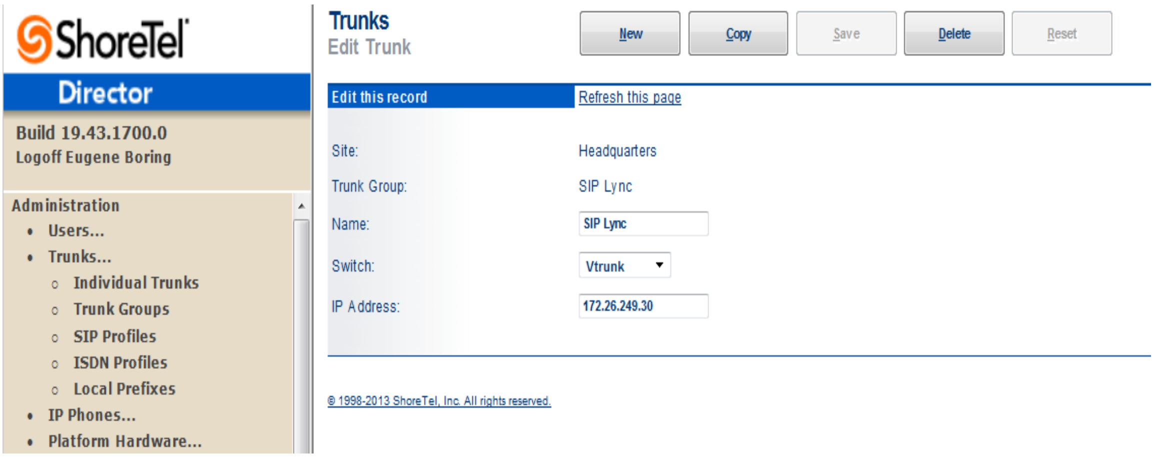


Figure 13 – Individual trunk setting (virtual switch) for Skype for Business trunk group

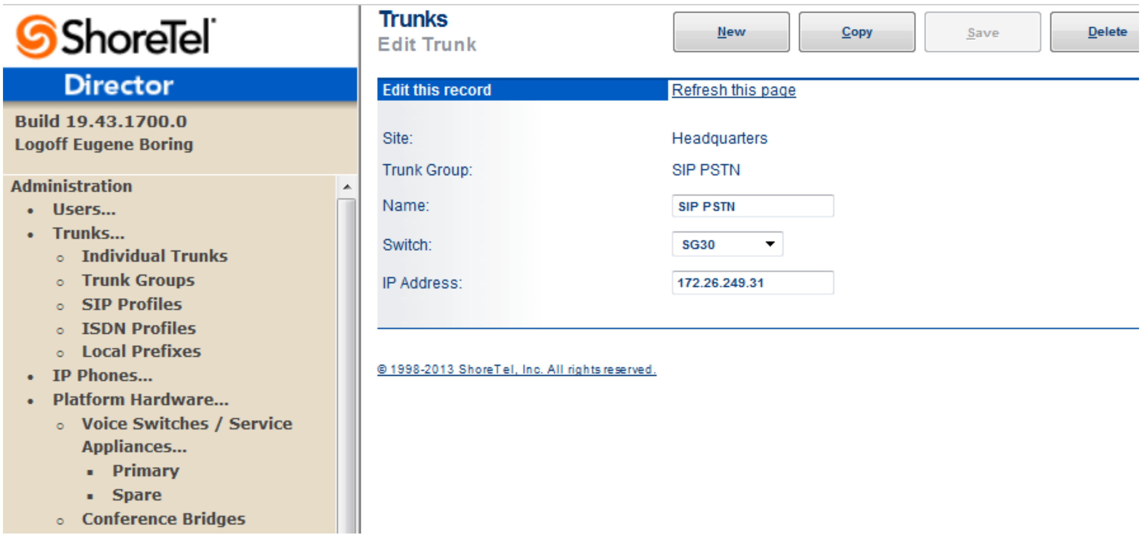


Figure 14 – Individual trunk setting (SG30 switch) for PSTN trunk group

After setting up the trunk groups and individual trunks, refer to the *ShoreTel Planning and Installation Guide* to make the appropriate changes for the User Group settings. This completes the settings for the ShoreTel system side.

2.9 ShoreTel Technical Support

In the event that you have problems with the ShoreTel system, you may contact ShoreTel Technical Assistance Center at +1 (800) 742-2348 (Toll Free) or +1 (408) 331-3313 (International). A support contract must be in place before any assistance will be provided.

3 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Skype for Business Server 2015 and the ShoreTel UC system. These configuration procedures are based on the interoperability test topology and includes the following main areas:

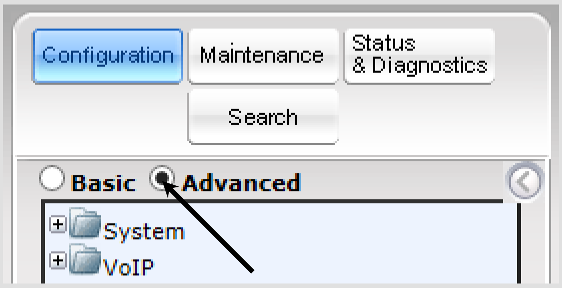
- E-SBC WAN interface - ShoreTel UC system environment
- E-SBC LAN interface - Skype for Business Server 2015 environment

This configuration is done using the E-SBC's embedded Web server (hereafter, referred to as *Web interface*).

Notes:

- For implementing Microsoft Skype for Business and ShoreTel UC system based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
  - √ **Microsoft**
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

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



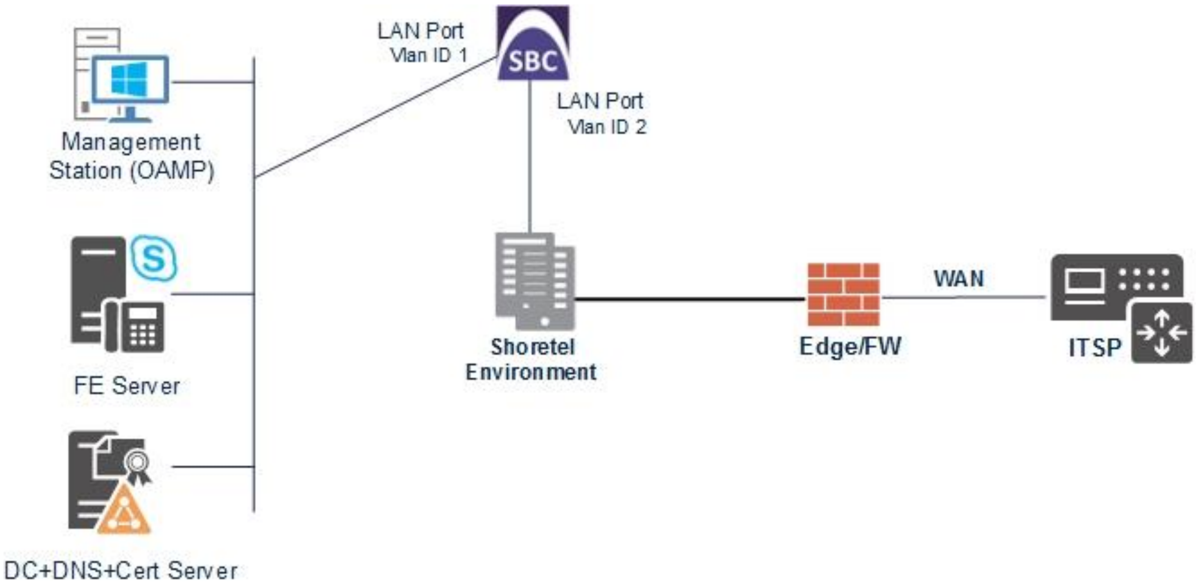
  Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

3.1 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
  - ShoreTel UC system, located on the 'WAN'
- ShoreTel UC system connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, E-SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - WAN (VLAN ID 2)

Figure 3-1: Network Interfaces in Interoperability Test Topology



3.1.1 Step 1a: Configure VLANs

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

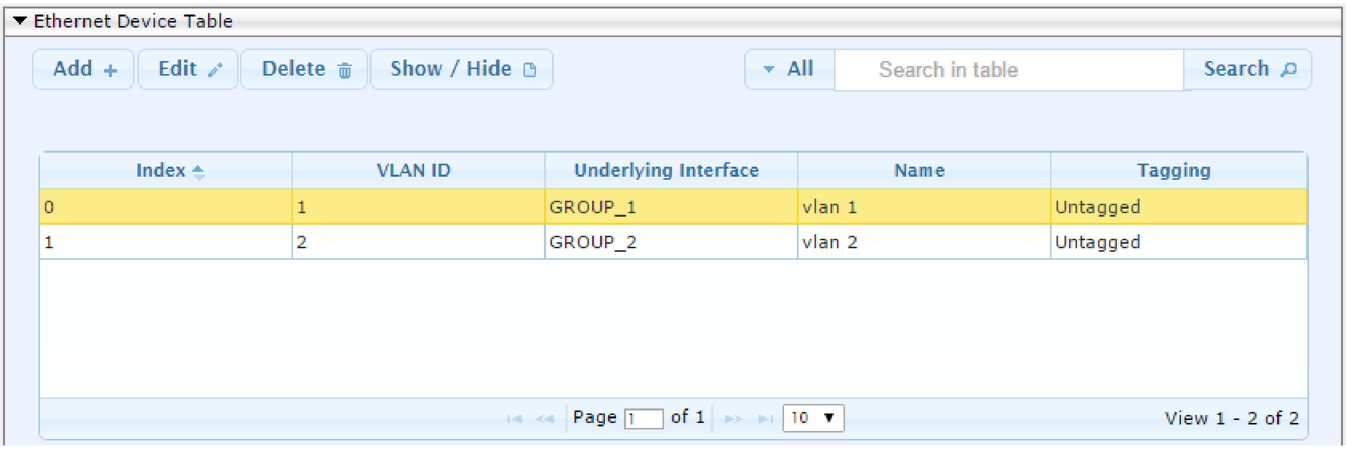
- LAN VoIP (assigned the name "Voice")
- WAN VoIP (assigned the name "WANSP")

➢ To configure the VLANs:

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

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

Figure 3-2: Configured VLAN IDs in Ethernet Device Table



3.1.2 Step 1b: Configure Network Interfaces

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

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

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

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

Parameter	Value
IP Address	**172.21.128.28** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Default Gateway	**172.21.1.1**
VLAN ID	**1**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**172.21.0.20**
Underlying Device	**vlan 1**

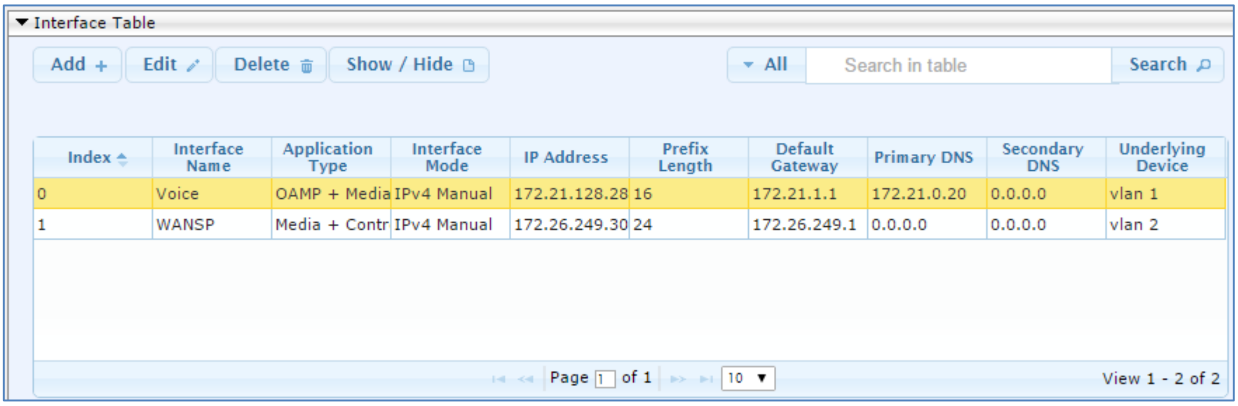
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**172.26.249.30** (WAN IP address)
Prefix Length	**24** (for 255.255.255.0)
Default Gateway	**172.26.249.1** (router's IP address)
VLAN ID	**2**
Interface Name	**WANSP**
Primary DNS Server IP Address	According to customer network requirement
Underlying Device	**vlan 2**

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

The configured IP network interfaces are shown below:

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



Interface Table

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

Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	Voice	OAMP + Media	IPv4 Manual	172.21.128.28	16	172.21.1.1	172.21.0.20	0.0.0.0	vlan 1
1	WANSP	Media + Contr	IPv4 Manual	172.26.249.30	24	172.26.249.1	0.0.0.0	0.0.0.0	vlan 2

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

3.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 3-4: Enabling SBC Application

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 3.16 on page 77).

3.3 Step 3: Configure Media Realms

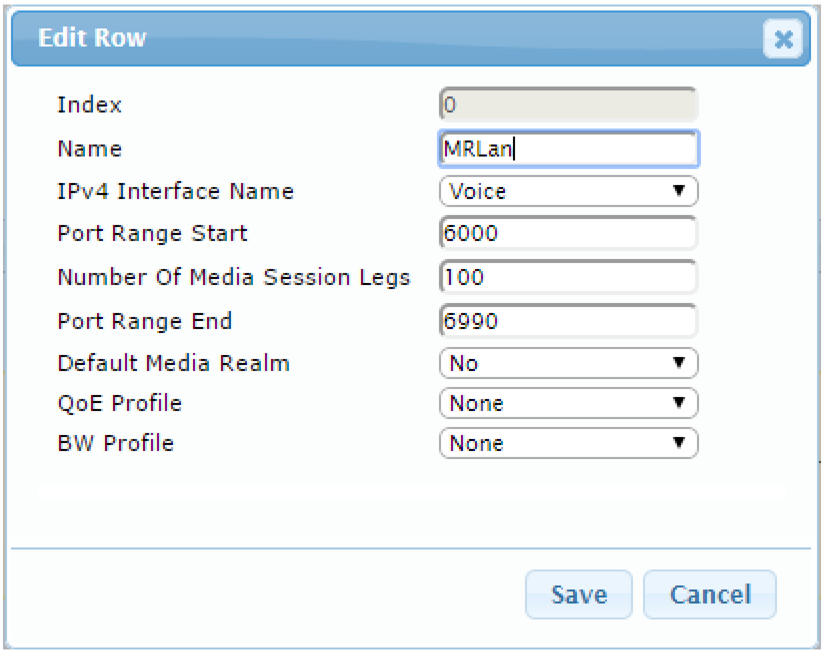
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

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

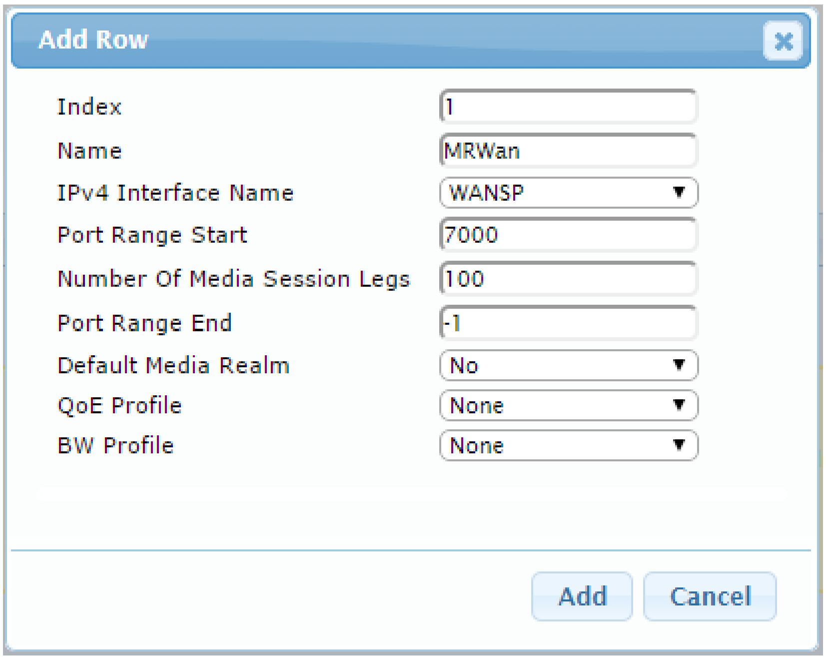
Figure 3-5: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

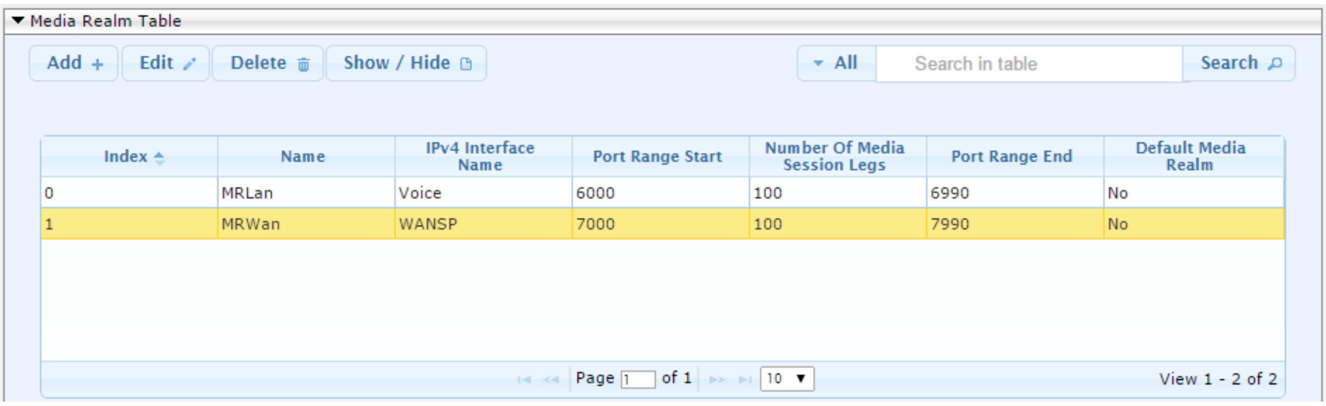
Parameter	Value
Index	**1**
Media Realm Name	**MRWan** (arbitrary name)
IPv4 Interface Name	**WANSP**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 3-6: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 3-7: Configured Media Realms in Media Realm Table



3.4 Step 4: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

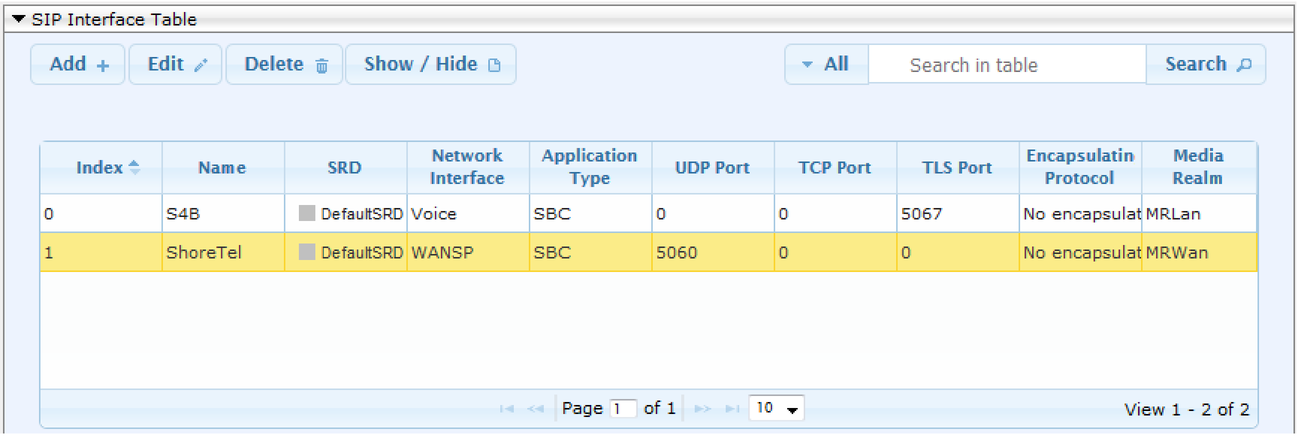
Parameter	Value
Index	**0**
Interface Name	**S4B**
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
Media Realm	**MRLan**

3. Configure a SIP Interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

Figure 3-8: Configured SIP Interfaces in SIP Interface Table



3.5 Step 5: Configure Proxy Sets

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

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

- Microsoft Skype for Business Server 2015
- ShoreTel UC system

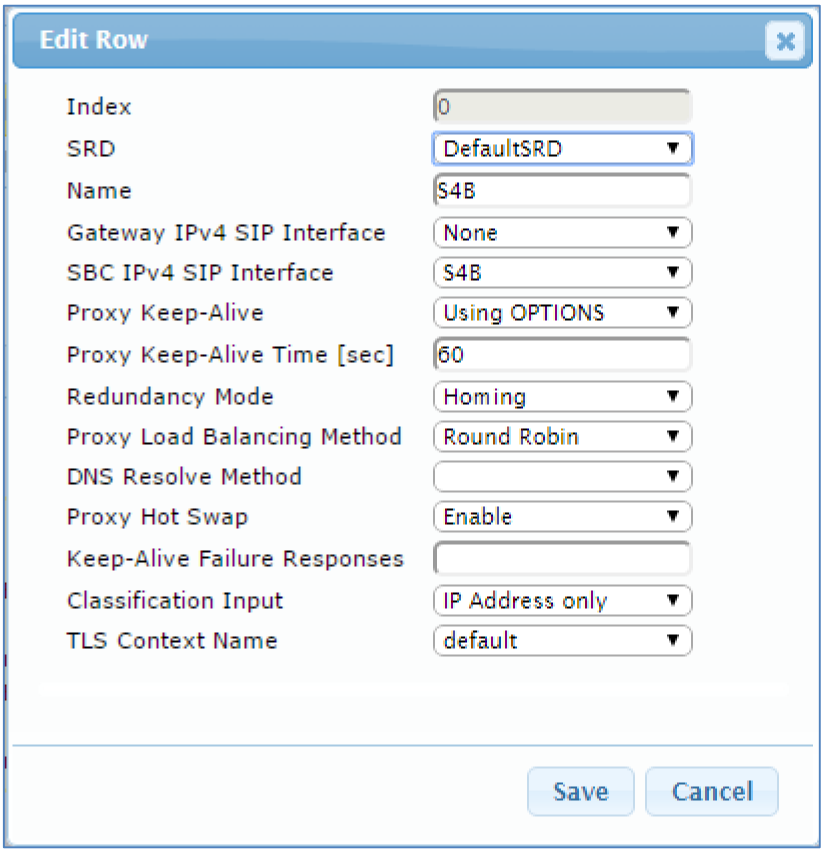
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➢ **To configure Proxy Sets:**

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

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

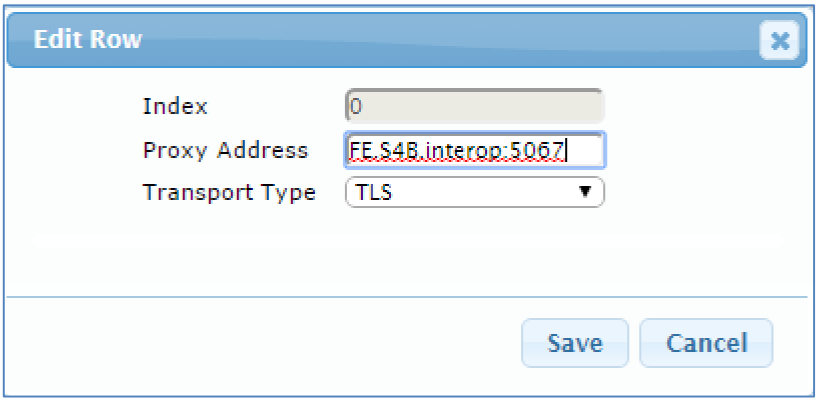
Figure 3-9: Configuring Proxy Set for Microsoft Skype for Business Server 2015



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

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

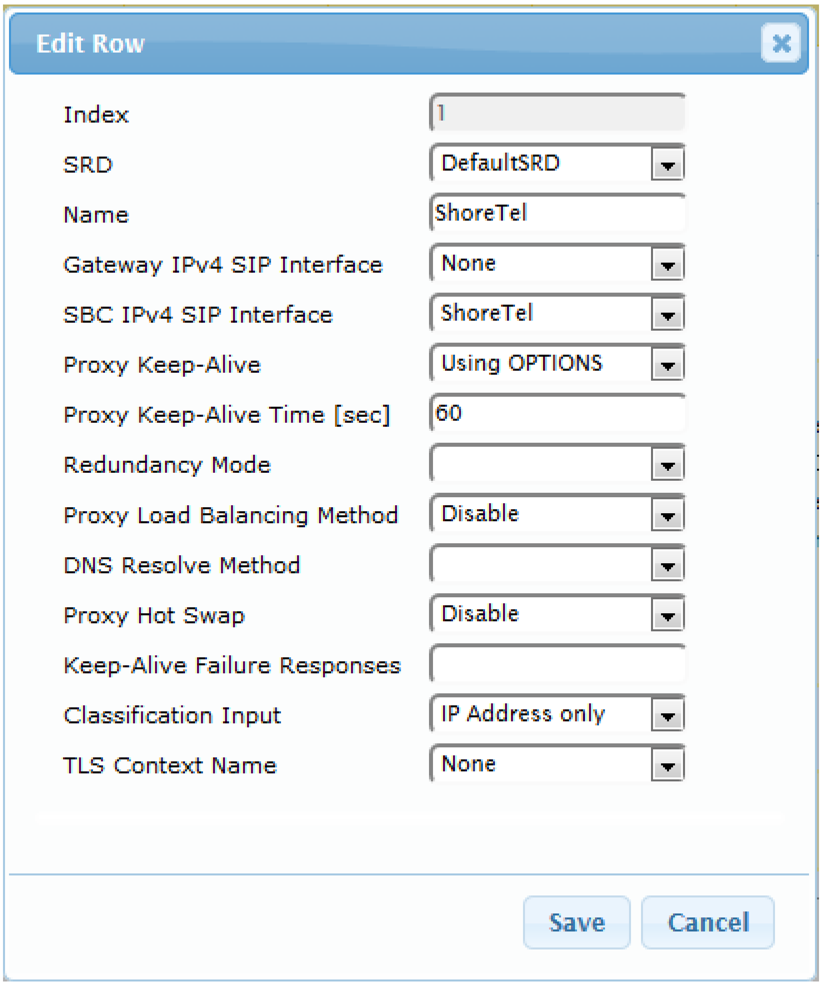
Figure 3-10: Configuring Proxy Address for Microsoft Skype for Business Server 2015



4. Configure a Proxy Set for the ShoreTel UC system:

Parameter	Value
Proxy Set ID	**1**
Proxy Name	**ShoreTel**
SBC IPv4 SIP Interface	**ShoreTel**
Proxy Keep Alive	**Using Options**

Figure 3-11: Configuring Proxy Set for ShoreTel UC system

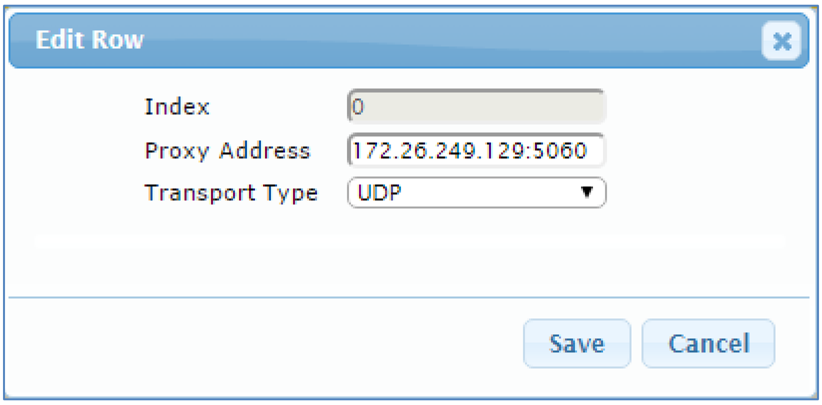


a. Configure a Proxy Address Table for Proxy Set 1:

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

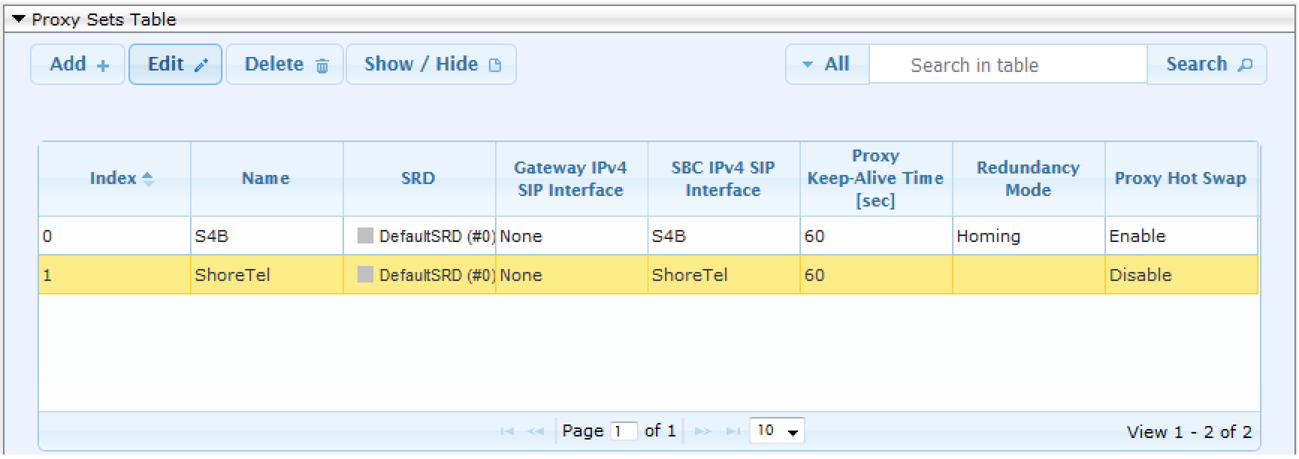
Parameter	Value
Index	**0**
Proxy Address	**172.26.249.129:5060** (IP address / FQDN and destination port)
Transport Type	**UDP**

Figure 3-12: Configuring Proxy Address for ShoreTel UC system



The configured Proxy Sets are shown in the figure below:

Figure 3-13: Configured Proxy Sets in Proxy Sets Table



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

3.6 Step 6: Configure IP Profiles

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

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

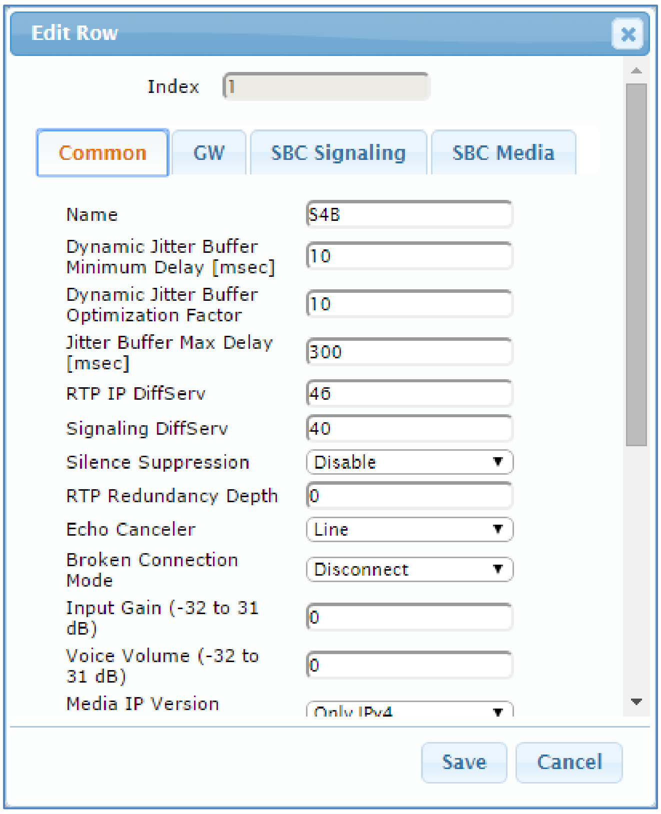
- Microsoft Skype for Business Server 2015 - to operate in secure mode using SRTP and TLS
- ShoreTel UC system - to operate in non-secure mode using RTP and UDP

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

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

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

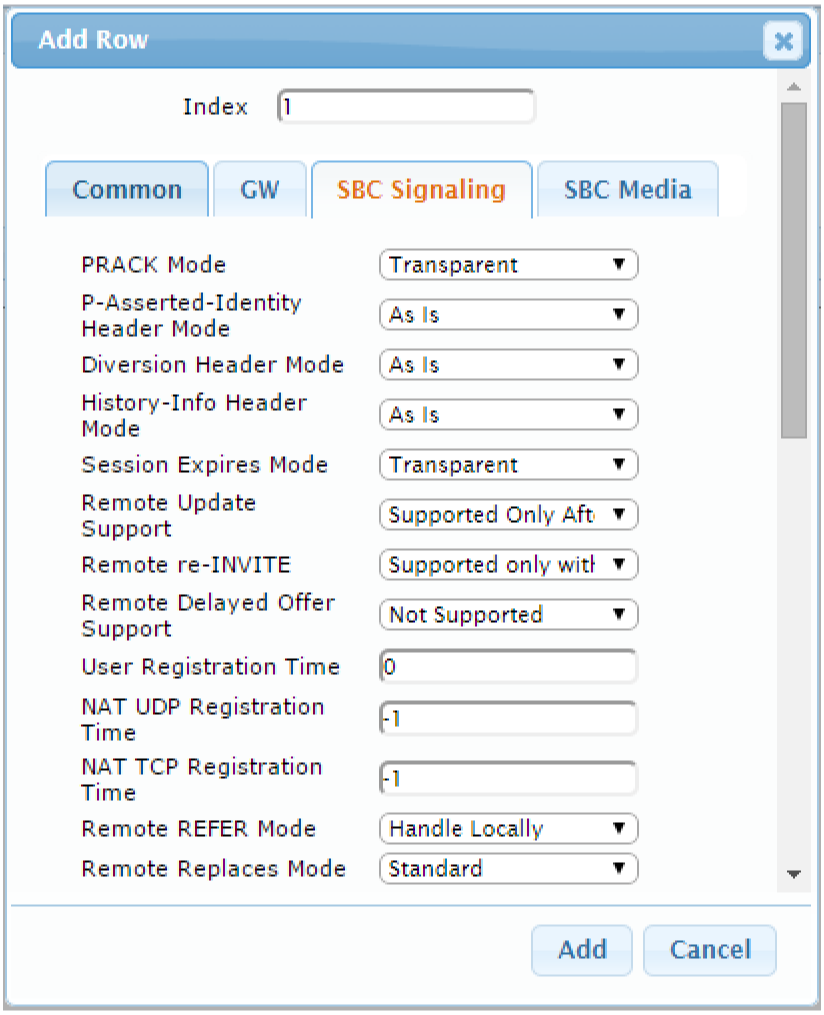
Figure 3-14: Configuring IP Profile for Skype for Business Server 2015 – Common Tab



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

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

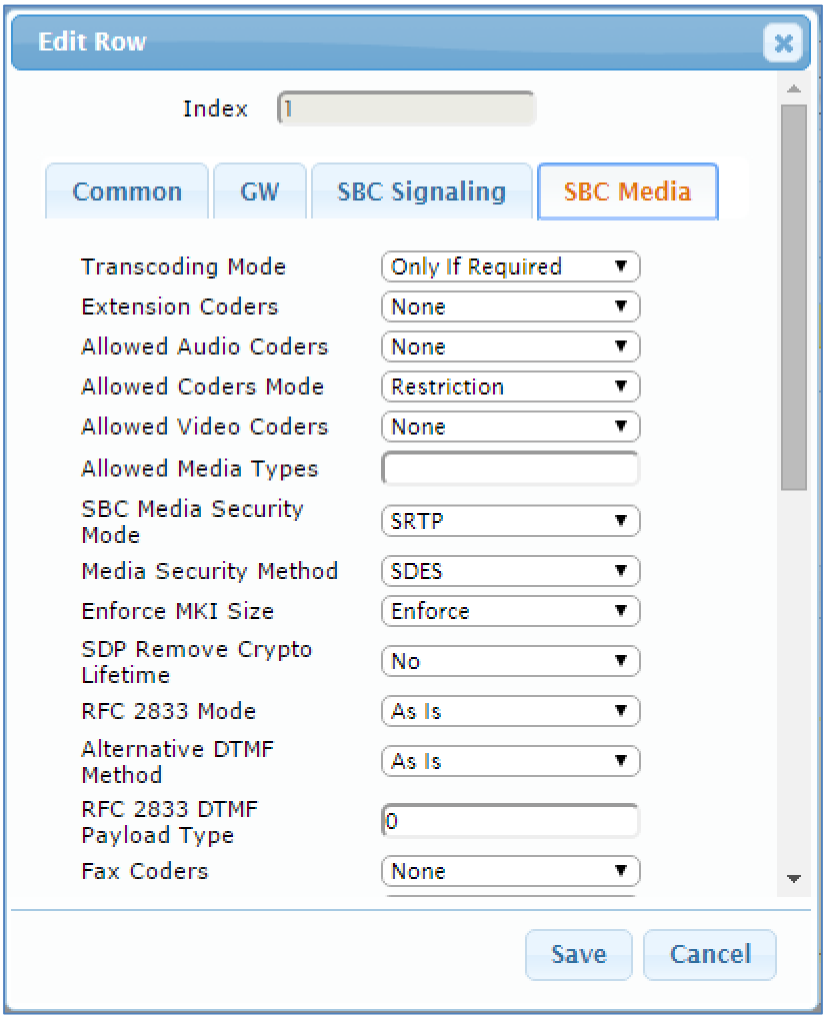
Figure 3-15: Configuring IP Profile for Skype for Business Server 2015 – SBC Signaling Tab



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

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

Figure 3-16: Configuring IP Profile for Skype for Business Server 2015 – SBC Media Tab

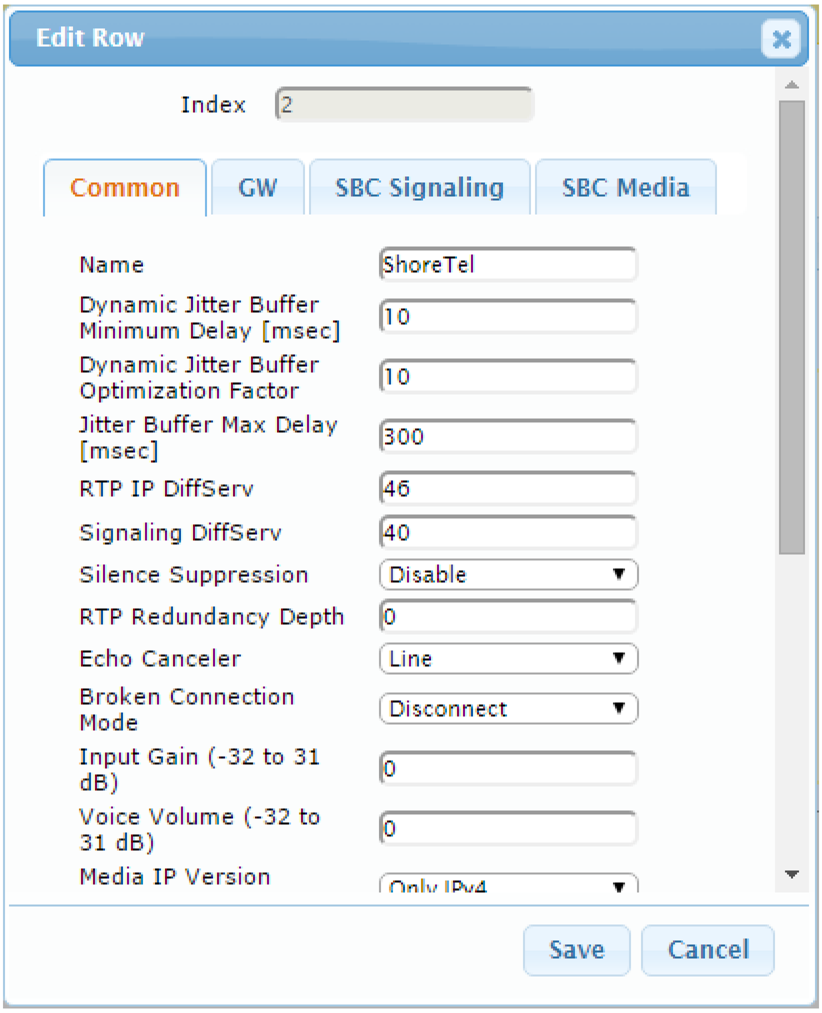


➢ To configure an IP Profile for the ShoreTel UC system:

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

Parameter	Value
Index	**2**
Profile Name	**ShoreTel**

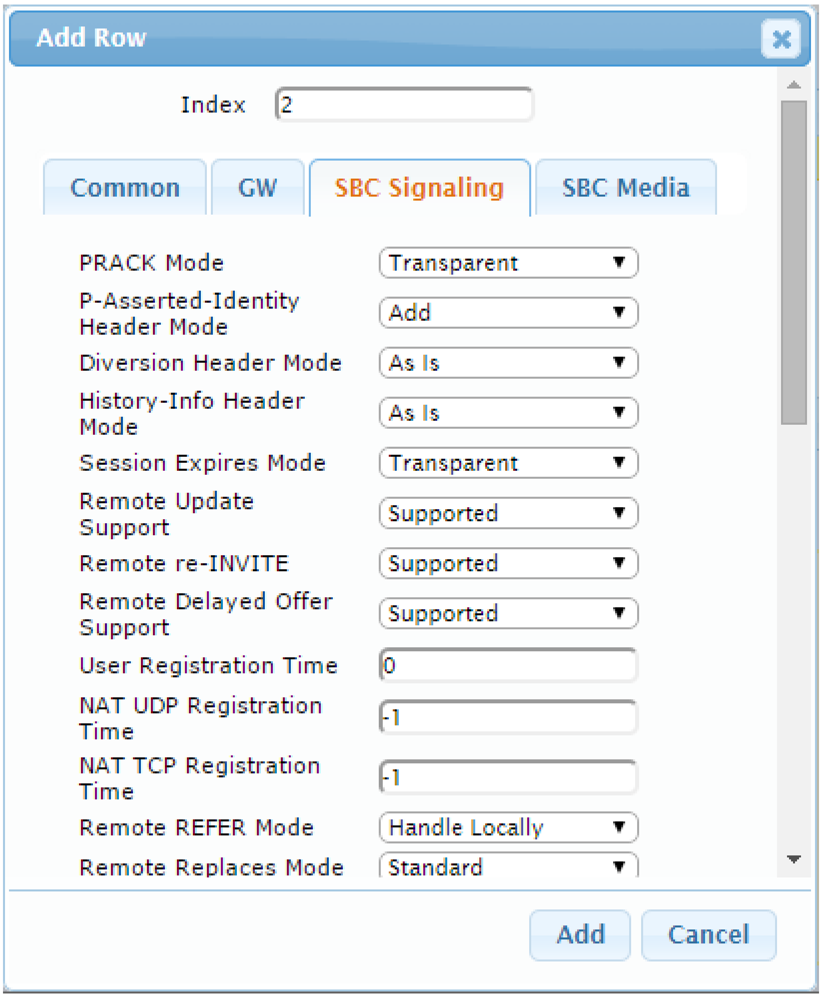
Figure 3-17: Configuring IP Profile for ShoreTel UC system – Common Tab



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

Parameter	Value
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Remote REFER Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to UC system)
Play RBT To Transferee	**Yes** (required for playing ring back tone for transferred calls)

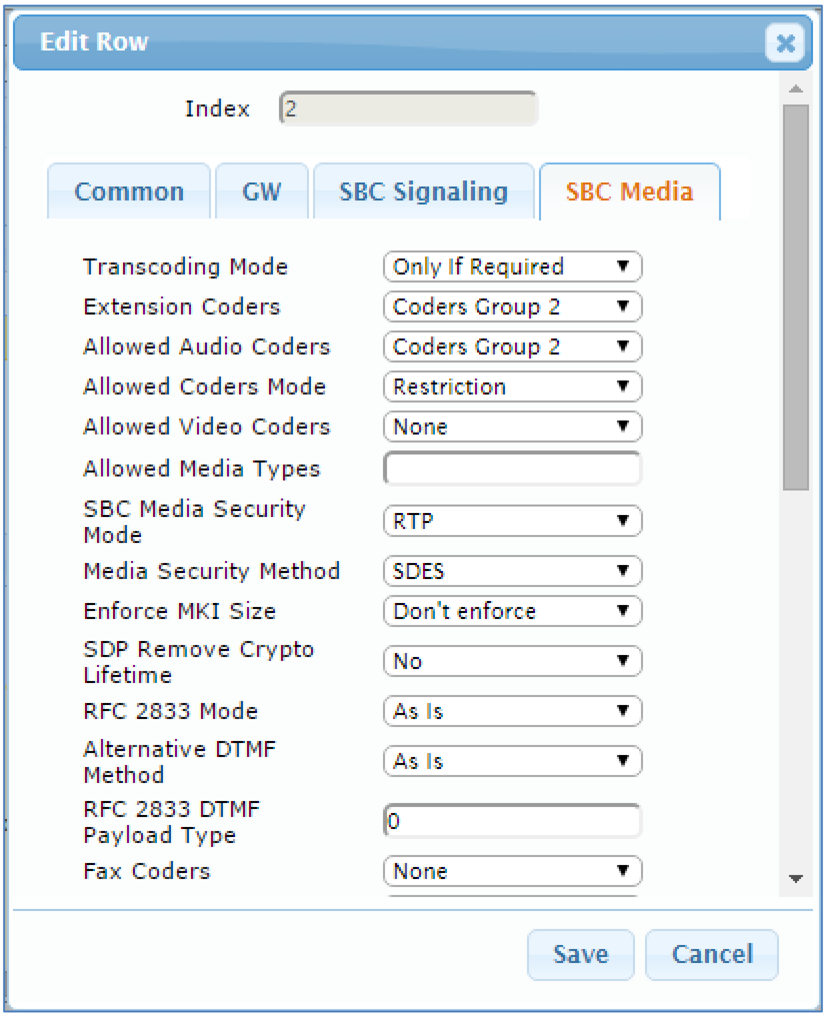
Figure 3-18: Configuring IP Profile for ShoreTel UC system – SBC Signaling Tab



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

Parameter	Value
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 2**
Media Security Behavior	**RTP**

Figure 3-19: Configuring IP Profile for ShoreTel UC system – SBC Media Tab



3.7 Step 7: Configure IP Groups

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

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

- Skype for Business Server 2015 (Mediation Server) located on LAN side of E-SBC
- ShoreTel UC system located on WAN side of E-SBC

➤ **To configure IP Groups:**

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

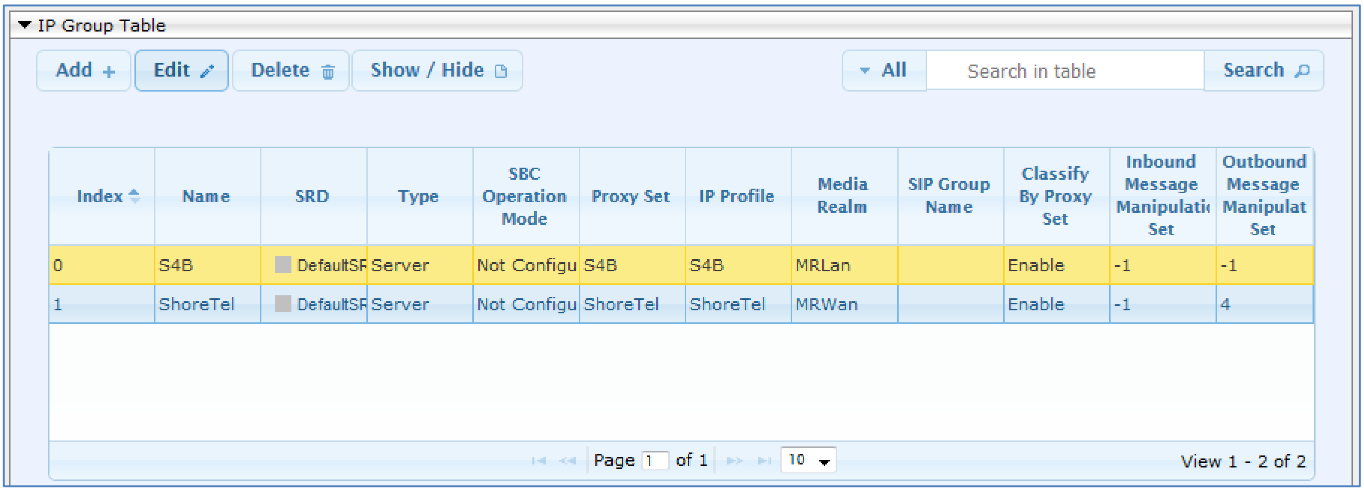
Parameter	Value
Index	**0**
Name	**S4B**
Type	**Server**
Proxy Set	**S4B**
IP Profile	**S4B**
Media Realm	**MRLan**
SIP Group Name	**172.26.249.129** (according to ITSP requirement)

3. Configure an IP Group for the ShoreTel UC system:

Parameter	Value
Index	**1**
Name	**ShoreTel**
Type	**Server**
Proxy Set	**ShoreTel**
IP Profile	**ShoreTel**
Media Realm	**MRWan**
SIP Group Name	**172.26.249.129** (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 3-20: Configured IP Groups in IP Group Table



Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulatio Set	Outbound Message Manipulat Set
0	S4B	DefaultSR	Server	Not Configu	S4B	S4B	MRLan		Enable	-1	-1
1	ShoreTel	DefaultSR	Server	Not Configu	ShoreTel	ShoreTel	MRWan		Enable	-1	4

3.8 Step 8: Configure Coders

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

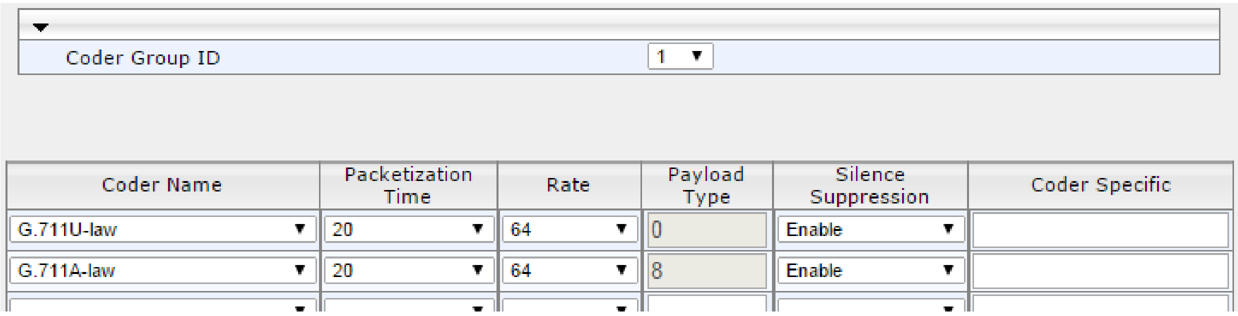
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 3.6 on page 33).

➢ **To configure coders:**

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

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

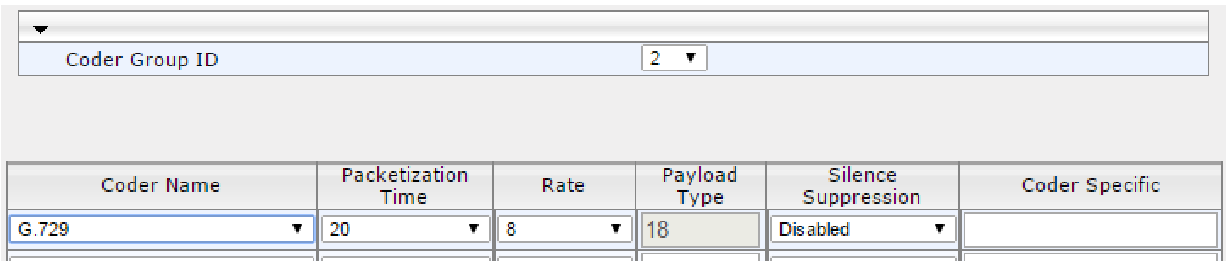
Figure 3-21: Configuring Coder Group for Skype for Business Server 2015



3. Configure a Coder Group for ShoreTel UC system:

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

Figure 3-22: Configuring Coder Group for ShoreTel UC system



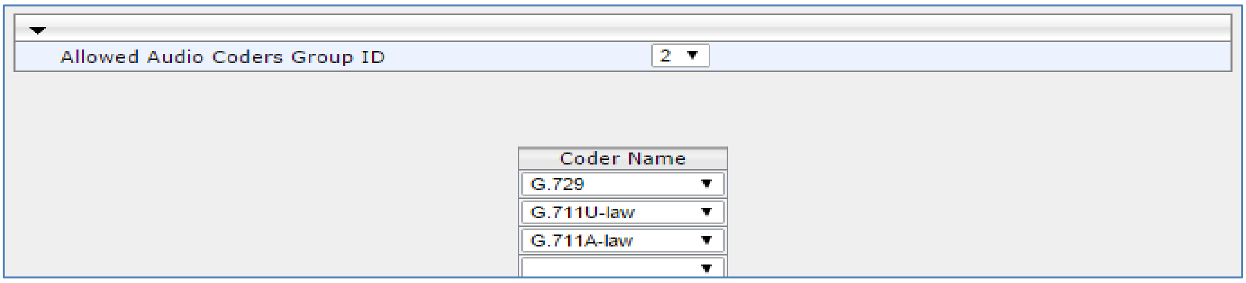
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the ShoreTel UC system uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the ShoreTel UC system (see Section 3.6 on page 33).

➢ **To set a preferred coder for the ShoreTel UC system:**

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

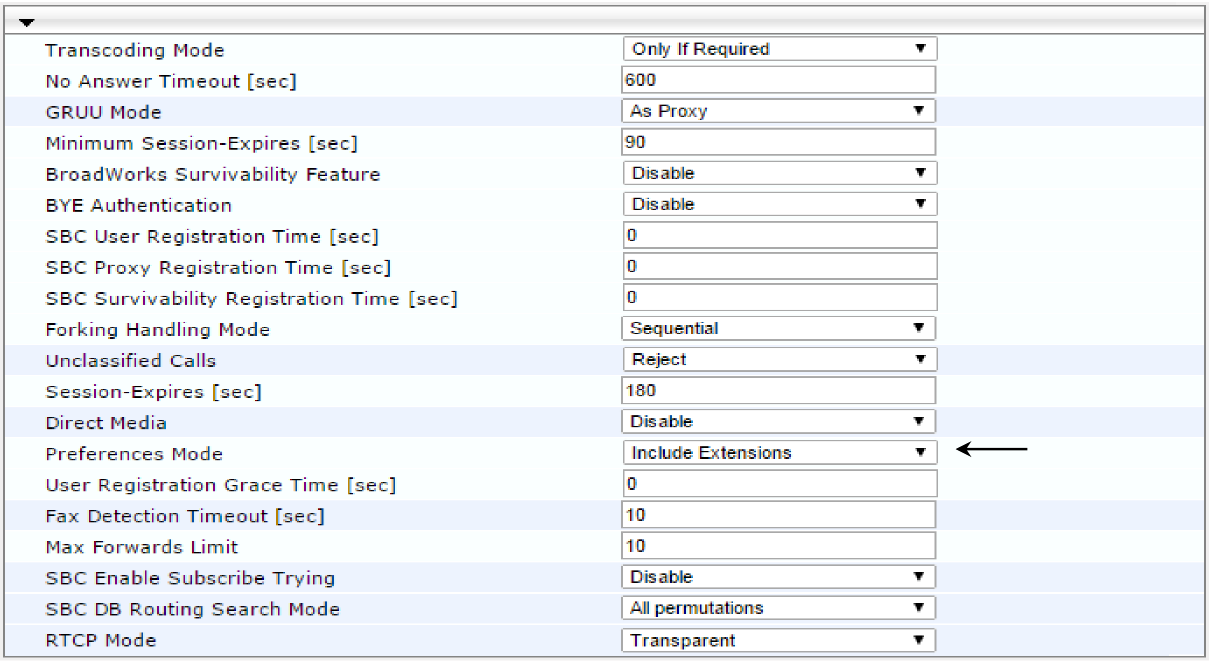
Parameter	Value
Allowed Audio Coders Group ID	**2**
Coder Name	▪ **G.729** ▪ **G.711 U-law** ▪ **G.711 A-law**

Figure 3-23: Configuring Allowed Coders Group for ShoreTel UC system



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

Figure 3-24: SBC Preferences Mode



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

3.9 Step 9: SIP TLS Connection Configuration

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

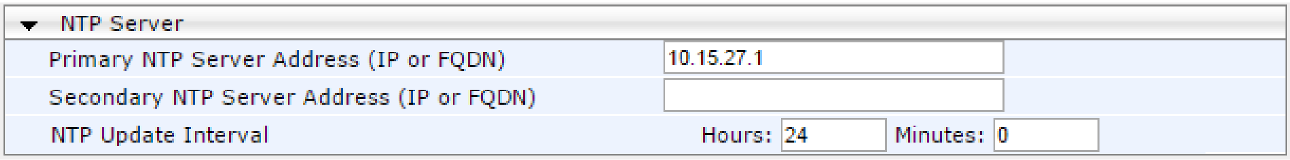
3.9.1 Step 9a: Configure the NTP Server Address

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

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

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

Figure 3-25: Configuring NTP Server Address



3. Click **Submit**.

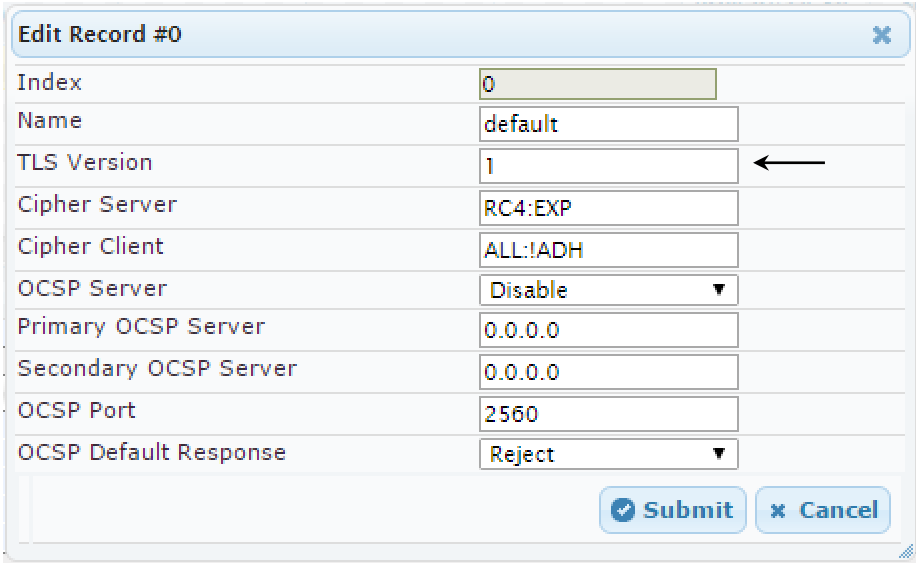
3.9.2 Step 9b: Configure the TLS version 1.0

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

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

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

Figure 3-26: Configuring TLS version 1.0



4. Click **Submit**.

3.9.3 Step 9c: Configure a Certificate

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

The procedure involves the following main steps:

a. Generating a Certificate Signing Request (CSR).

b. Requesting Device Certificate from CA.

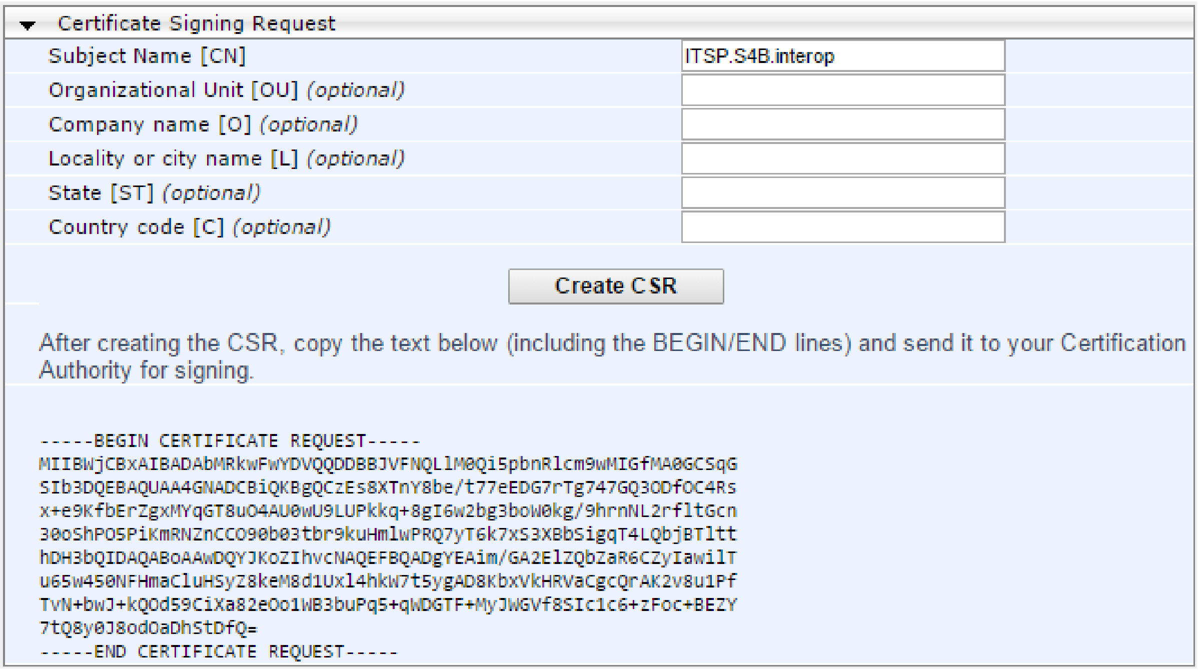
c. Obtaining Trusted Root Certificate from CA.

d. Deploying Device and Trusted Root Certificates on E-SBC.

➢ **To configure a certificate:**

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

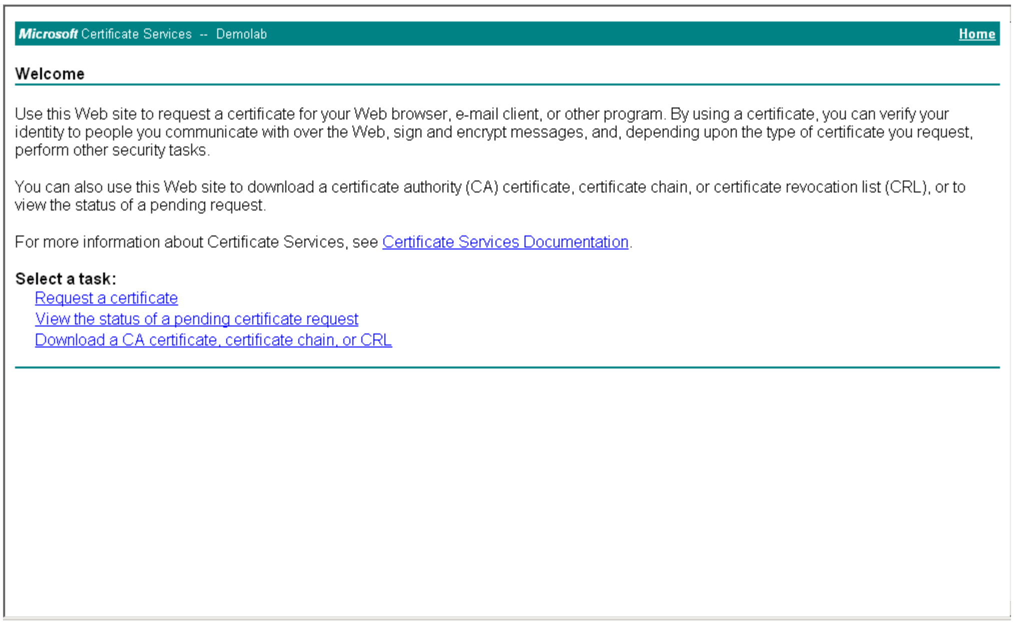
Figure 3-27: Certificate Signing Request – Creating CSR



> **Note:** The value entered in this field must be identical to the gateway name configured in the Topology Builder for Skype for Business Server 2015 (see Section 4.1 on page 78).

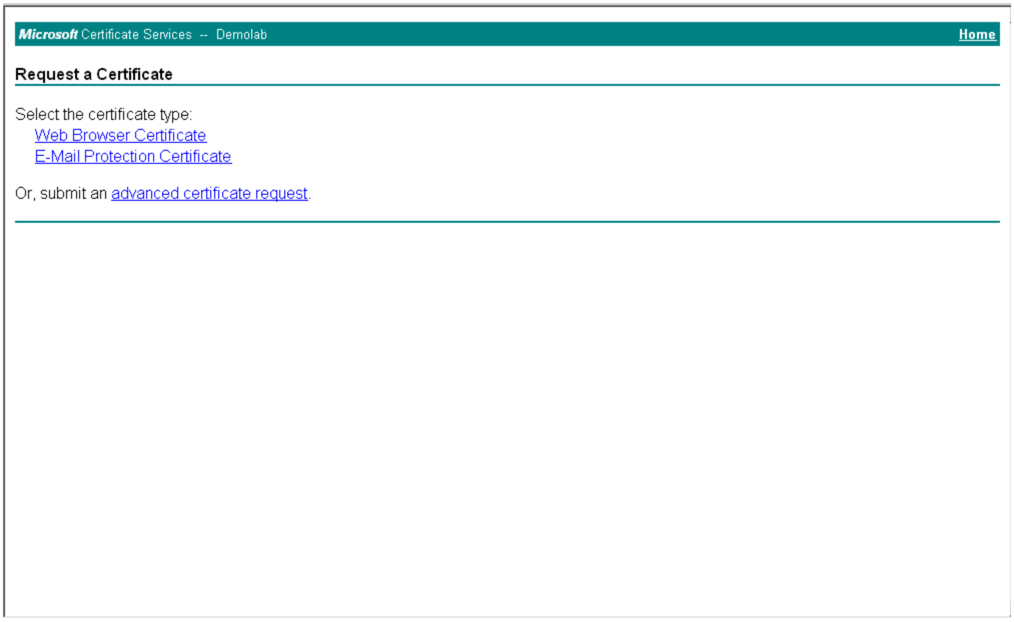
5. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----**" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate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

Figure 3-28: Microsoft Certificate Services Web Page



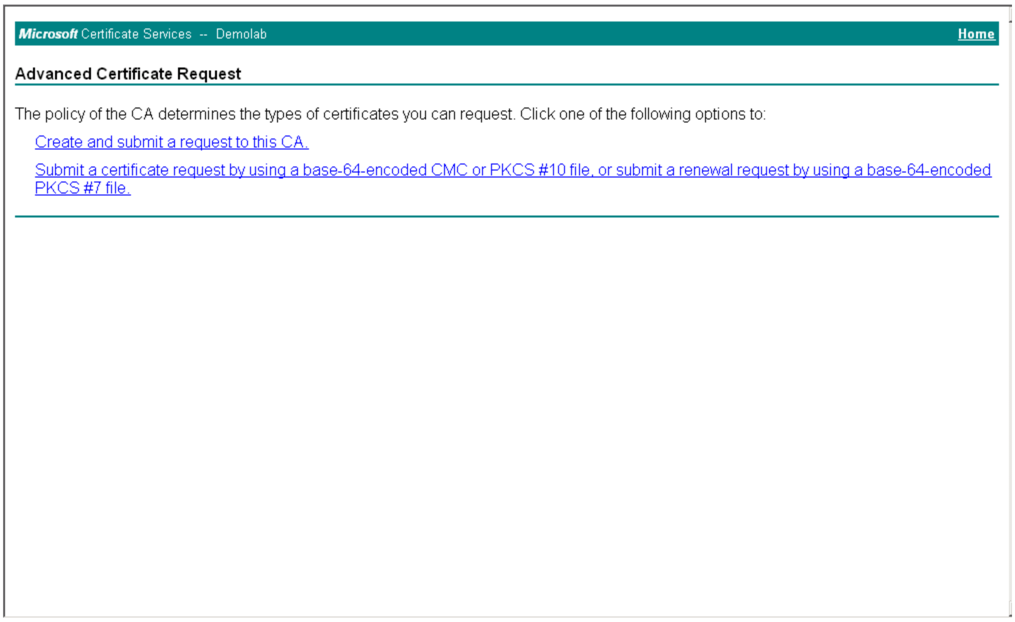
7. Click **Request a certificate**.

Figure 3-29: Request a Certificate Page



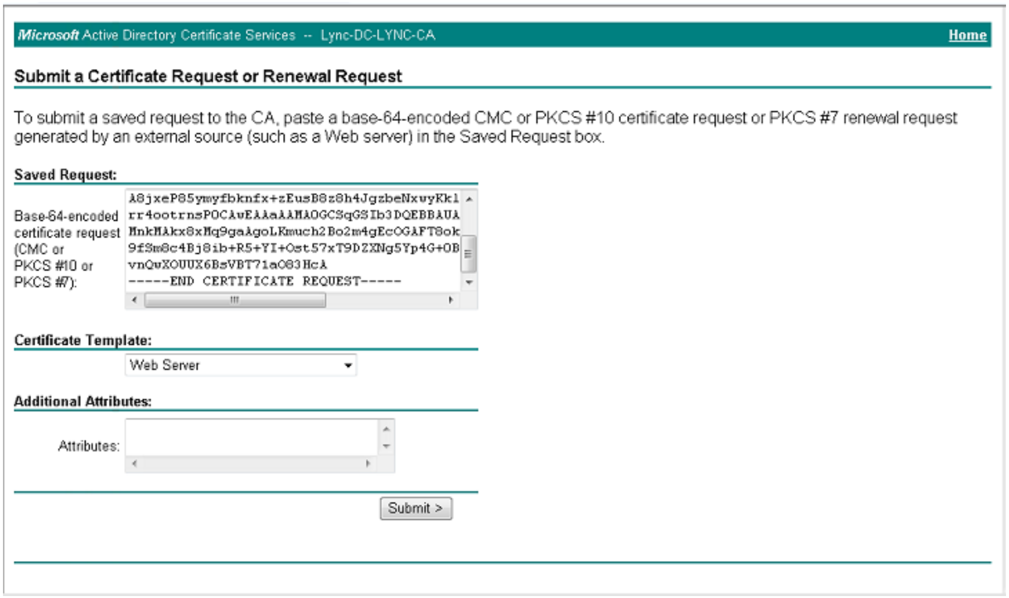
8. Click **advanced certificate request**, and then click **Next**.

Figure 3-30: Advanced Certificate Request Page



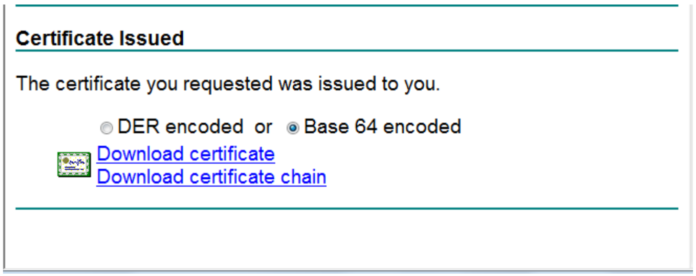
9. Click **Submit a certificate request ...**, and then click **Next**.

Figure 3-31: Submit a Certificate Request or Renewal Request Page



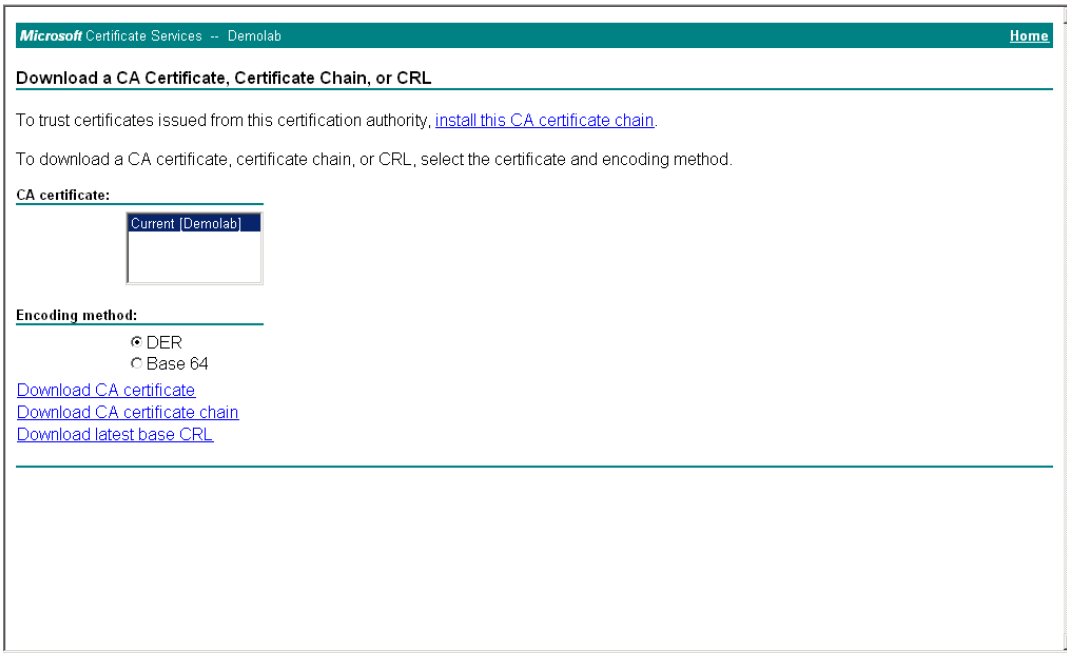
10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**.

Figure 3-32: Certificate Issued Page



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

Figure 3-33: Download a CA Certificate, Certificate Chain, or CRL Page



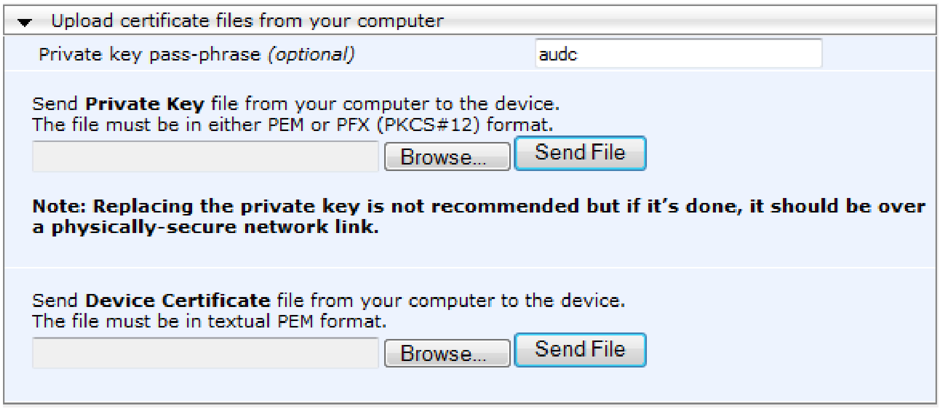
17. Under the 'Encoding method' group, select the **Base 64** option for encoding.
18. Click **Download CA certificate**.
19. Save the file as *certroot.cer* to a folder on your computer.

20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:

   a. In the TLS Contexts table, select the required TLS Context index row (typically, the default TLS Context at Index 0 is used), and then click the **TLS Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.

   b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 3-34: Upload Device Certificate Files from your Computer Group

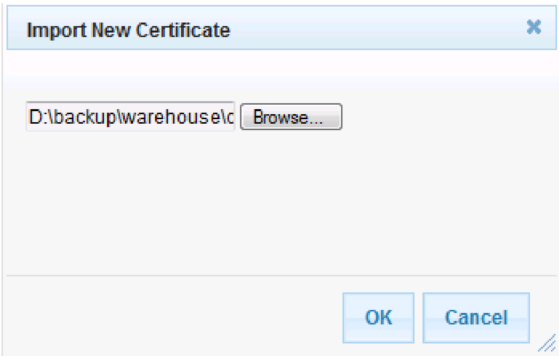


   c. In the E-SBC's Web interface, return to the **TLS Contexts** page.

   d. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates** button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.

   e. Click the **Import** button, and then select the certificate file to load.

Figure 3-35: Importing Root Certificate into Trusted Certificates Store



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

22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 3.16 on page 77).

3.10 Step 10: Configure SRTP

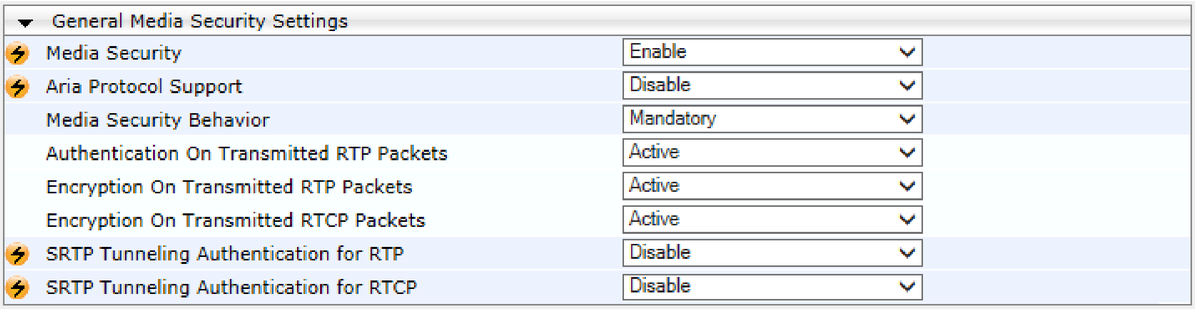
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 3.6 on page 33).

➢ **To configure media security:**

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

Parameter	Value
Media Security	**Enable**

Figure 3-36: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 3.16 on page 77).

3.11 Step 11: Configure Maximum IP Media Channels

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

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

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

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

Figure 3-37: Configuring Number of Media Channels

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 3.16 on page 77).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 3.7 on page 32, IP Group 1 represents Skype for Business Server 2015, and IP Group 2 represents ShoreTel UC system.

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

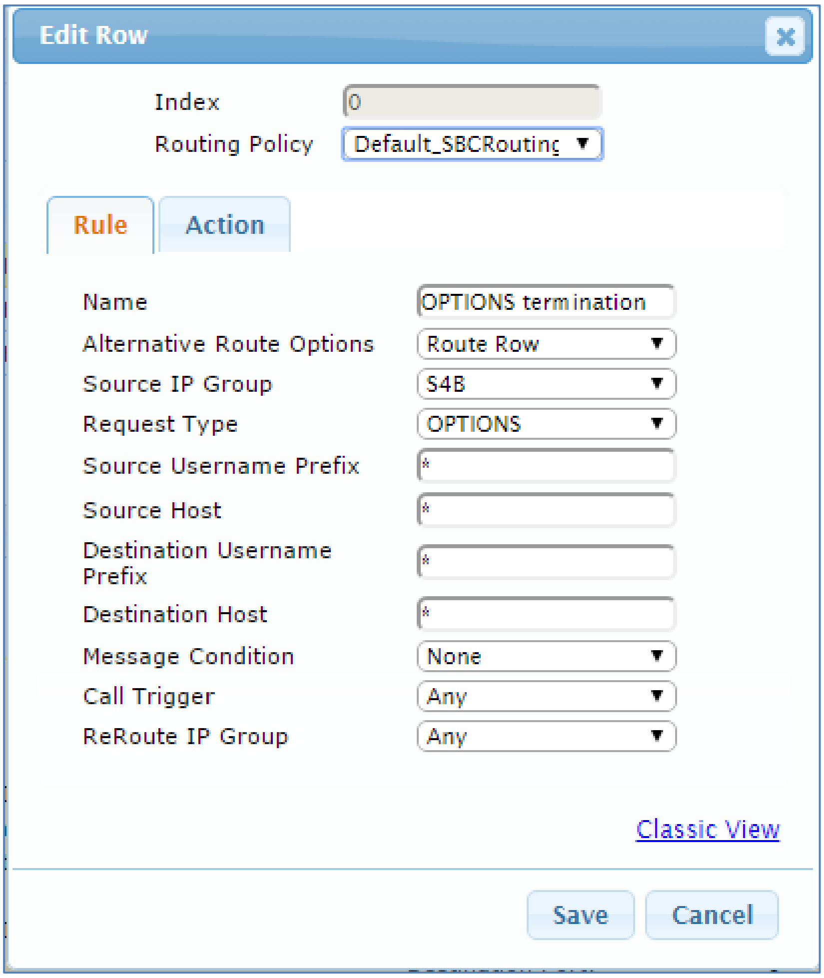
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Skype for Business Server 2015 to ShoreTel UC system
- Calls from ShoreTel UC system to Skype for Business Server 2015

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

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

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

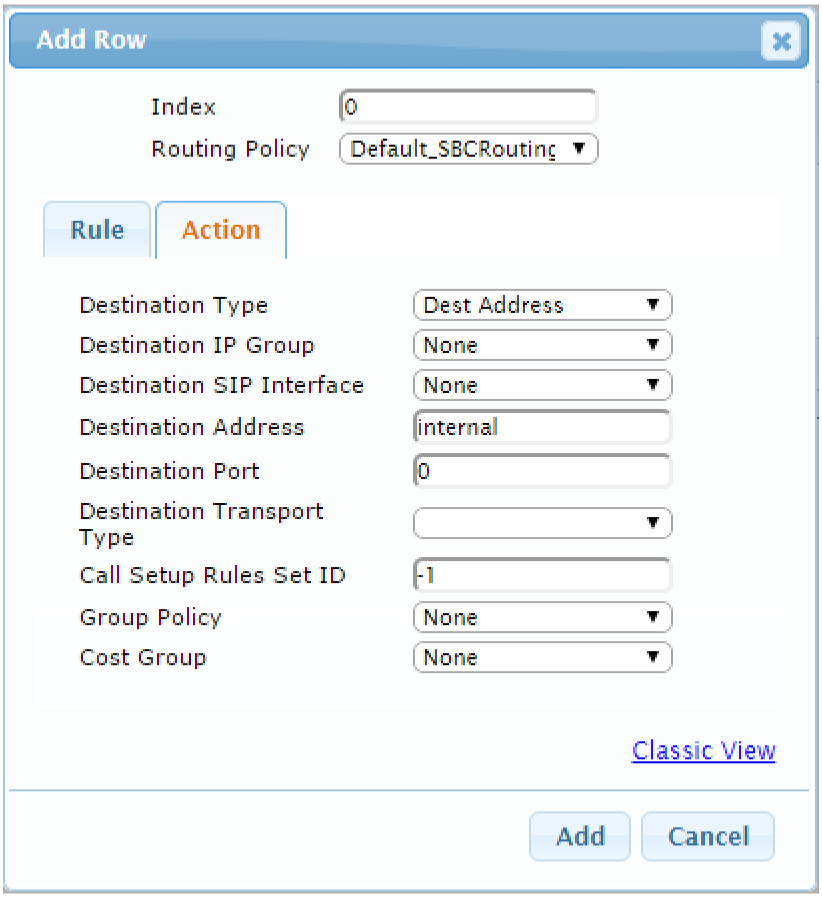
Figure 3-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab



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

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

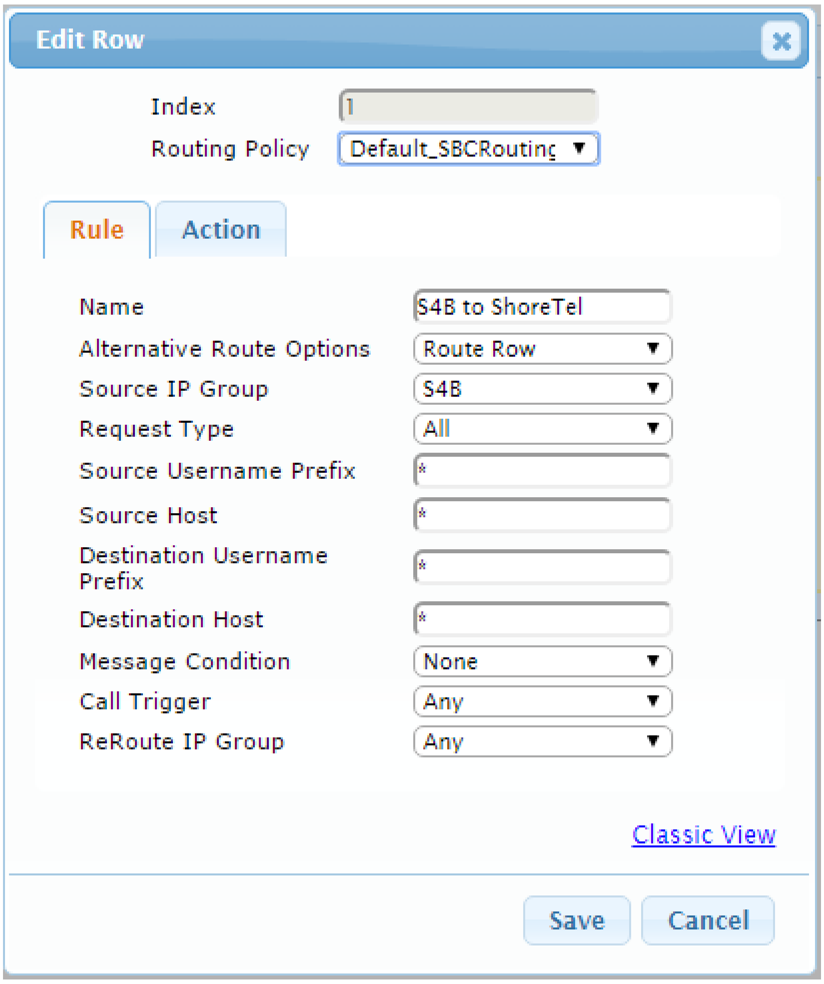
Figure 3-39: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab



3. Configure a rule to route calls from Skype for Business Server 2015 to ShoreTel UC system:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

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

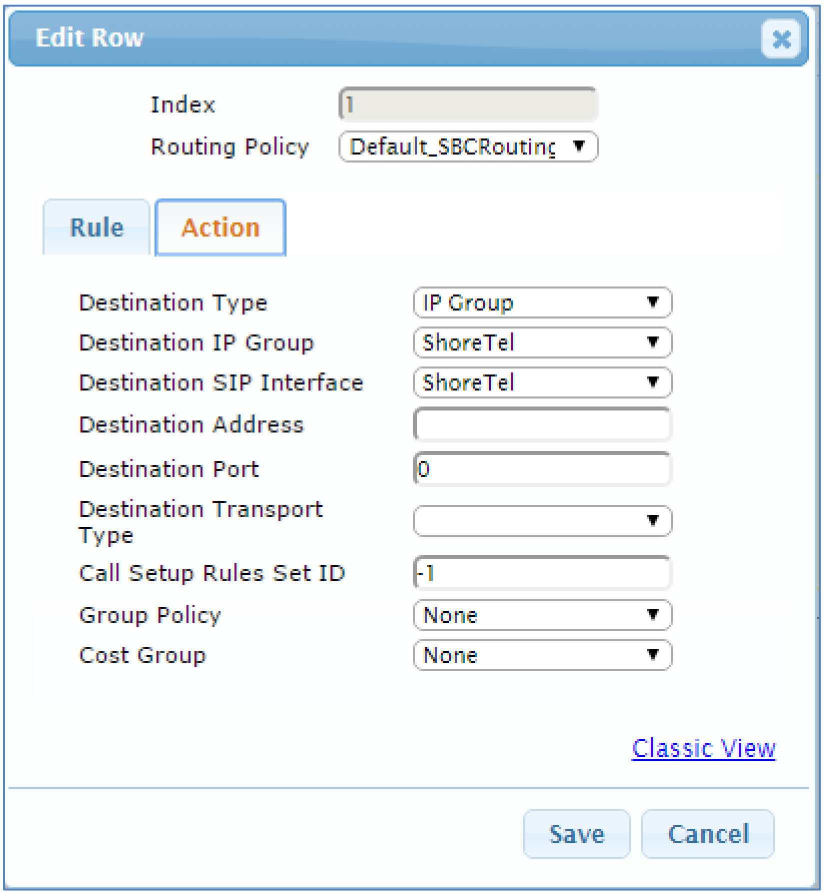
Figure 3-40: Configuring IP-to-IP Routing Rule for S4B to ShoreTel – Rule tab



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

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

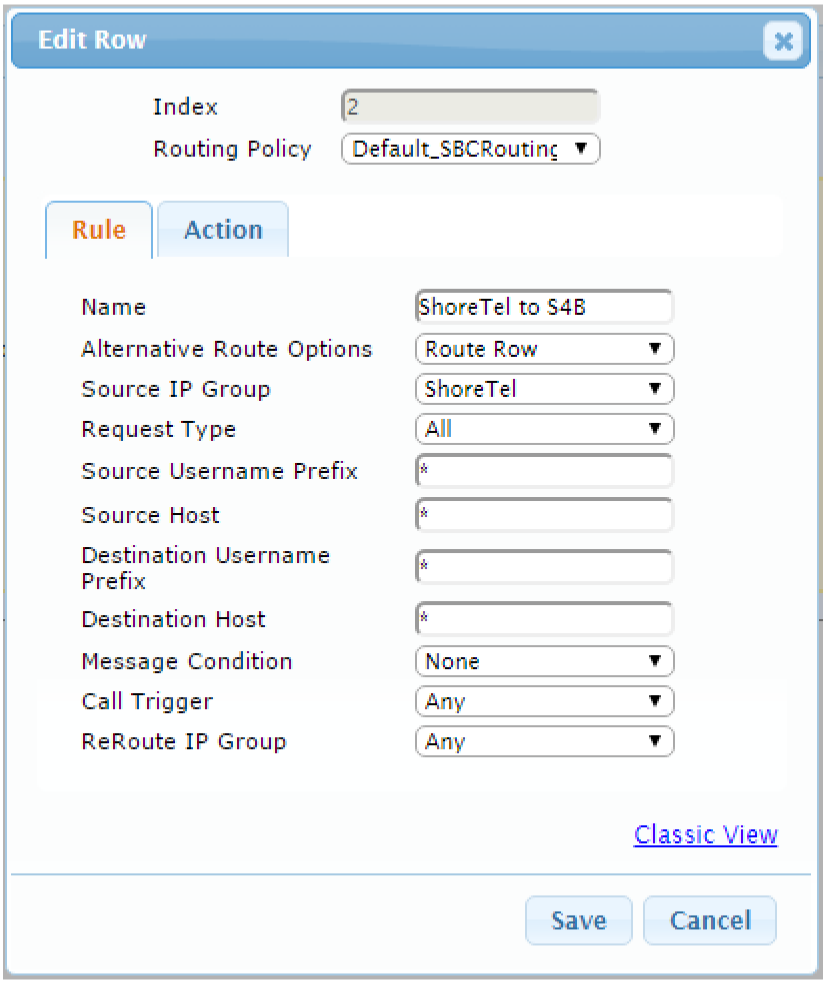
Figure 3-41: Configuring IP-to-IP Routing Rule for S4B to ShoreTel – Action tab



4. To configure rule to route calls from ShoreTel UC system to Skype for Business Server 2015:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

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

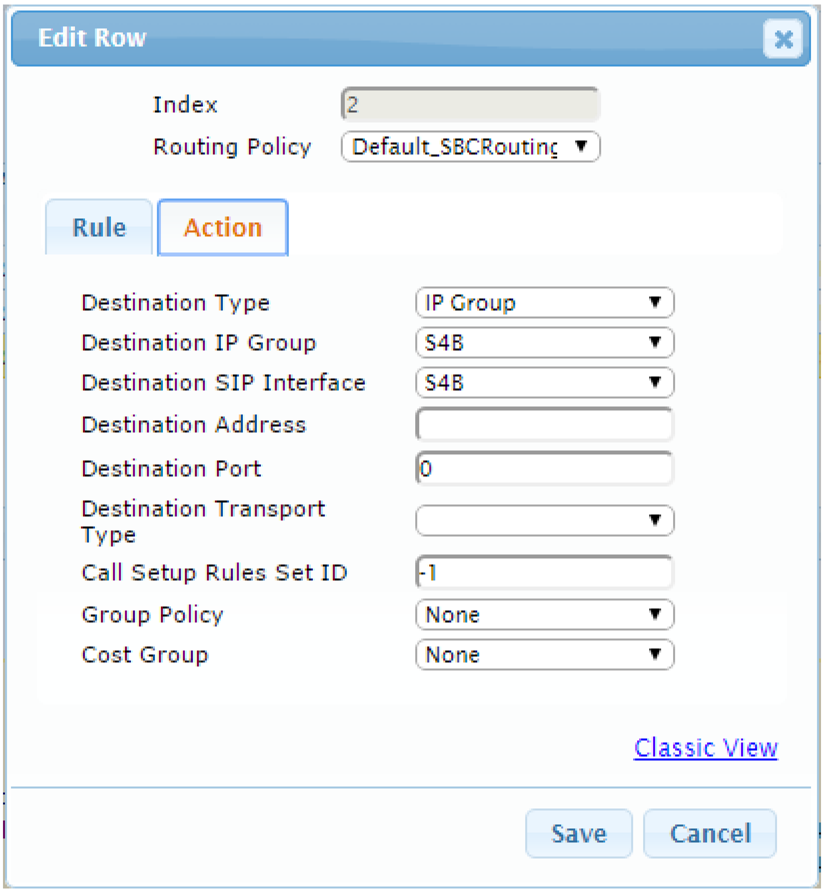
Figure 3-42: Configuring IP-to-IP Routing Rule for ShoreTel to S4B – Rule tab



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

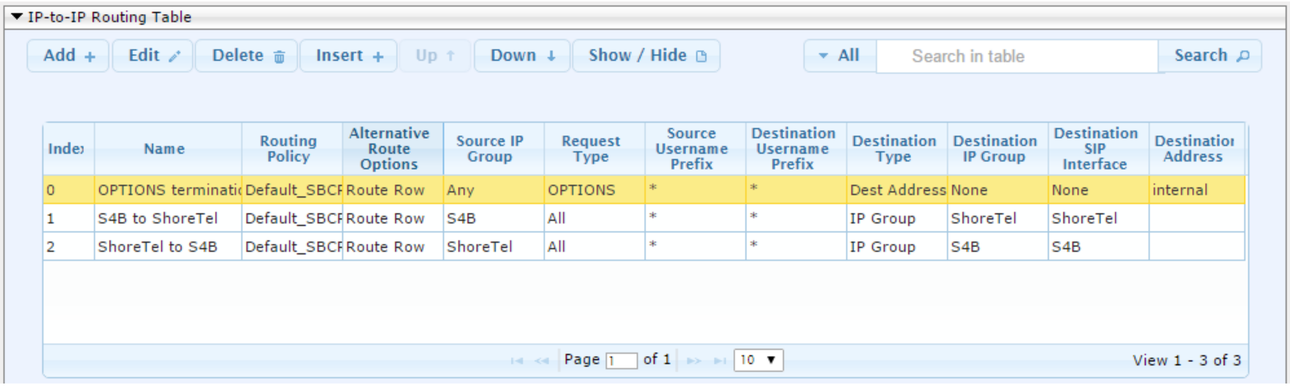
Parameter	Value
Destination Type	**IP Group**
Destination IP Group	**S4B**
Destination SIP Interface	**S4B**

Figure 3-43: Configuring IP-to-IP Routing Rule for ShoreTel to S4B – Action tab



The configured routing rules are shown in the figure below:

Figure 3-44: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destination SIP Interface	Destination Address
0	OPTIONS terminati	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address	None	None	internal
1	S4B to ShoreTel	Default_SBCR	Route Row	S4B	All	*	*	IP Group	ShoreTel	ShoreTel	
2	ShoreTel to S4B	Default_SBCR	Route Row	ShoreTel	All	*	*	IP Group	S4B	S4B	

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

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 3.7 on page 32, IP Group 0 represents Skype for Business Server 2015, and IP Group 1 represents ShoreTel UC system.

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

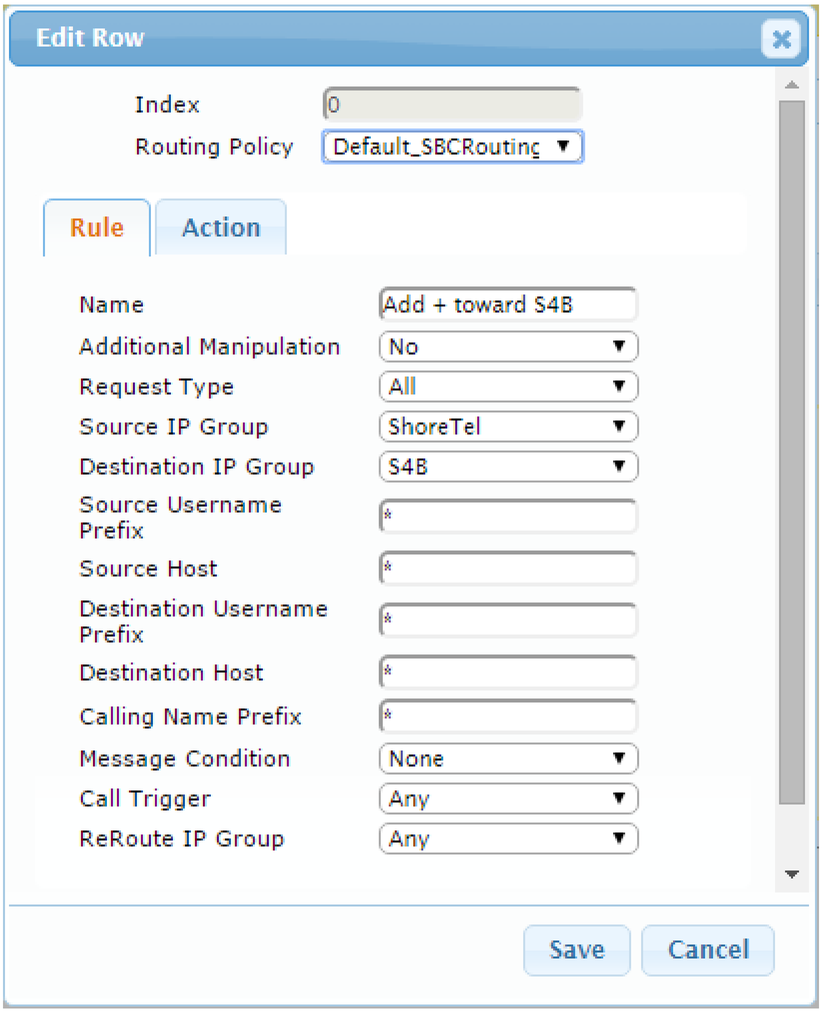
For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from the ShoreTel UC system IP Group to the Skype for Business Server 2015 IP Group for any destination username prefix and to remove the “+” from the Source and Destination numbers for calls from the Microsoft Skype for Business Server 2015 IP Group to the ShoreTel UC system IP Group.

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

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

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

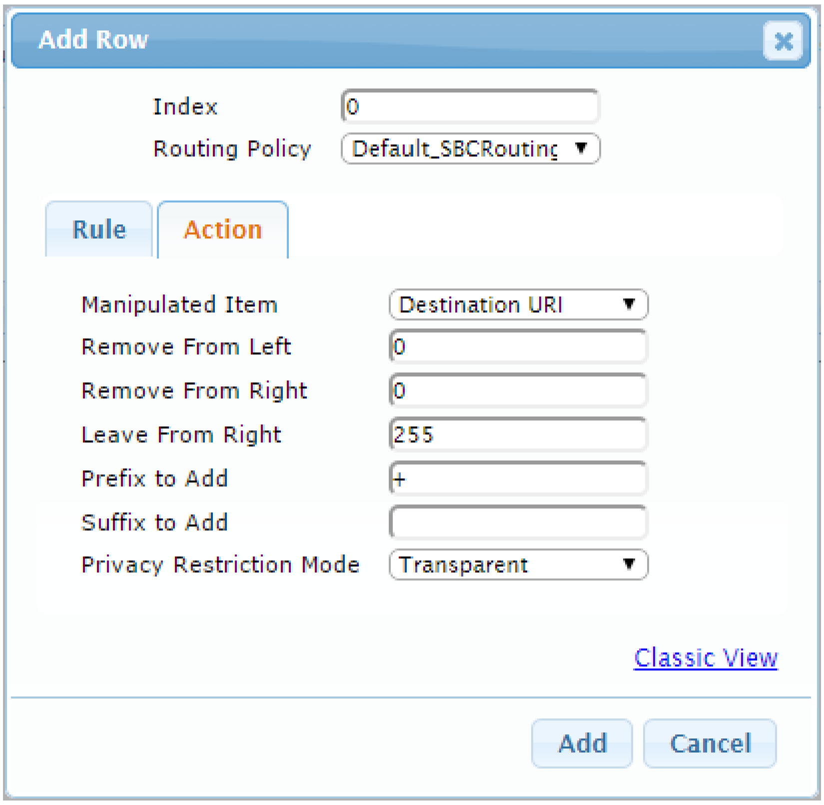
Figure 3-45: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

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

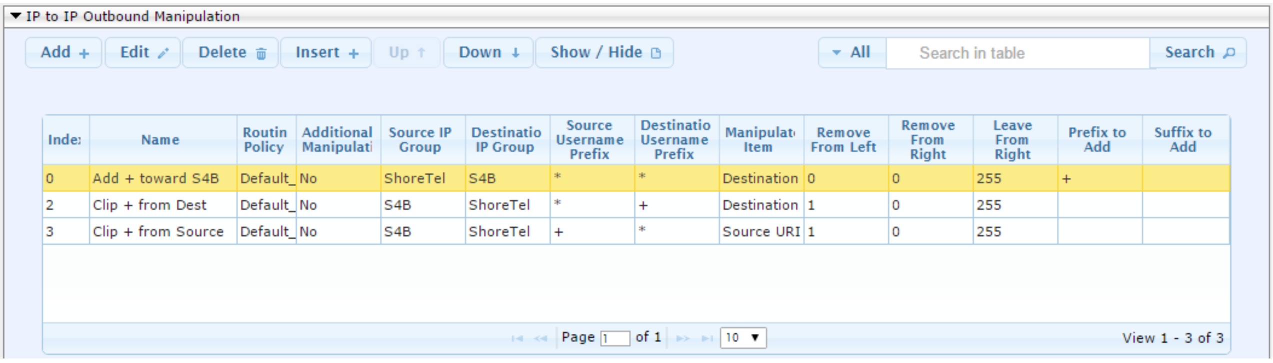
Figure 3-46: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

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

Figure 3-47: Example of Configured IP-to-IP Outbound Manipulation Rules



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

3.14 Step 14: Configure Message Manipulation Rules

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

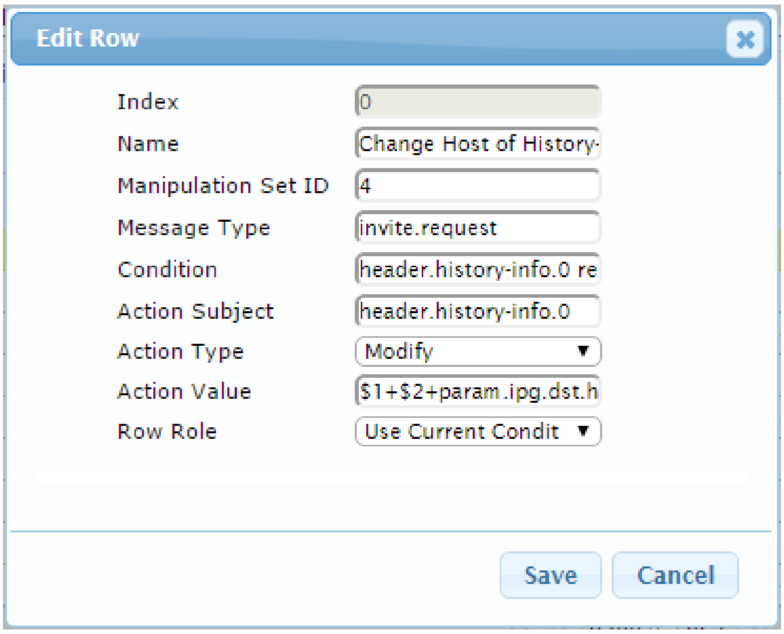
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for ShoreTel UC system. This rule applies to messages sent to the ShoreTel UC system IP Group calls initiated by the Skype for Business Server 2015 IP Group, which contain a PAI. This replace the host part of the P-Asserted Identity header with the destination host on the outgoing message towards the ShoreTel UC system.

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

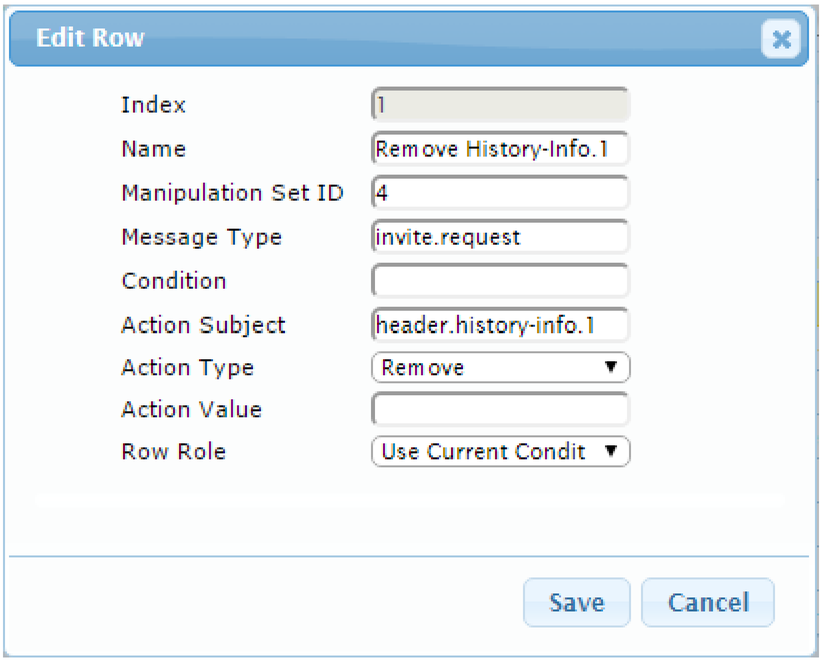
Figure 3-48: Configuring SIP Message Manipulation Rule 0 (for ShoreTel UC system)



3. Configure another manipulation rule (Manipulation Set 4) for ShoreTel UC system. This rule applies to messages sent to the ShoreTel UC system IP Group calls initiated by the Skype for Business Server 2015 IP Group, which contain a long PAI. The SBC separates the P-Asserted Identity header into two separate PAI headers. This removes the second P-Asserted Identity header on the outgoing message towards the ShoreTel UC system.

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

Figure 3-49: Configuring SIP Message Manipulation Rule 1 (for ShoreTel UC system)



4. Configure another manipulation rule (Manipulation Set 4) for ShoreTel UC system. This rule applies to messages sent to the ShoreTel UC system IP Group calls initiated by the Skype for Business Server 2015 IP Group in a call transfer scenario. This rule replaces the host part of the SIP Referred-by Header with the value that was configured in the ShoreTel UC system IP Group.

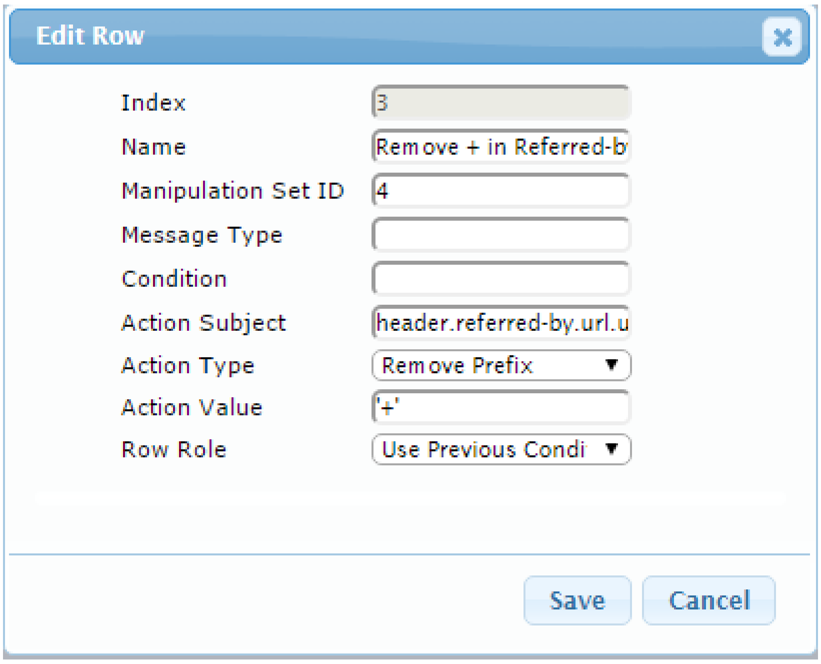
Parameter	Value
Index	**2**
Name	**Change Referred-By Host**
Manipulation Set ID	**4**
Message Type	**invite.request**
Condition	**header.referred-by exists**
Action Subject	**header.referred-by.url.host**
Action Type	**Modify**
Action Value	**param.ipg.dst.host**

Figure 3-50: Configuring SIP Message Manipulation Rule 2 (for ShoreTel UC system)

5. If manipulation rule index 2 (above) is executed, then the following rule is also executed. It removed '+' prefix from User part of the SIP Referred-by Header.

Parameter	Value
Index	**3**
Name	**Remove + in Referred-By**
Manipulation Set ID	**4**
Message Type	
Condition	
Action Subject	**header.referred-by.url.user**
Action Type	**Remove Prefix**
Action Value	**'+'**
Row Role	**Use Previous Condition**

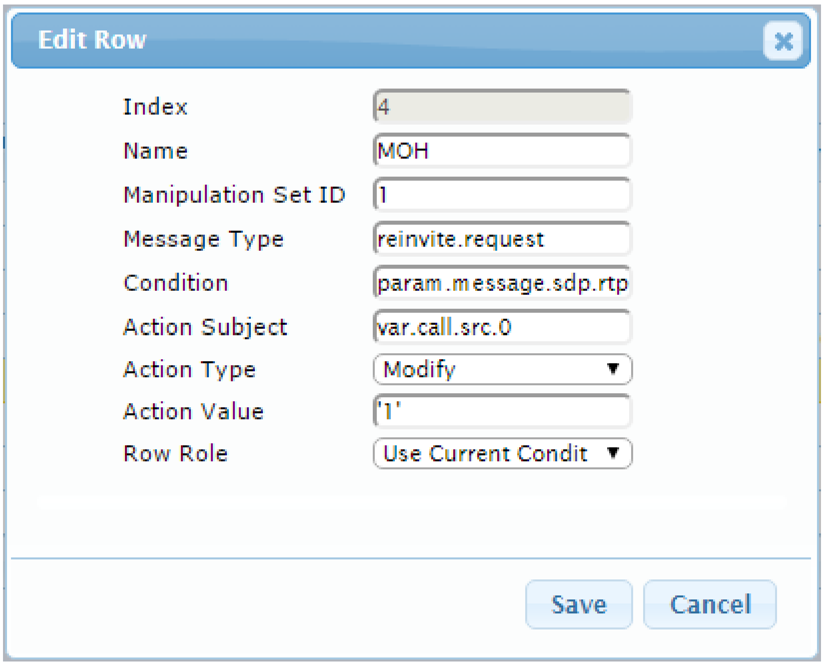
Figure 3-51: Configuring SIP Message Manipulation Rule 3 (for ShoreTel UC system)



6. For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Skype for Business-initiated Hold), create a variable and set it to **'1'**. This variable manages how the call will be handled in each state (answer, request, etc.).

Parameter	Value
Index	**4**
Manipulation Name	**MOH**
Manipulation Set ID	**1**
Message Type	**reinvite.request**
Condition	**param.message.sdp.rtpmode=='sendonly'**
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**‘1’**
Row Role	**Use Current Condition**

Figure 3-52: Configuring SIP Message Manipulation Rule 4 (for Microsoft Skype for Business)



7. If the manipulation rule Index 4 (above) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to “sendonly” change it to “sendrecv”.

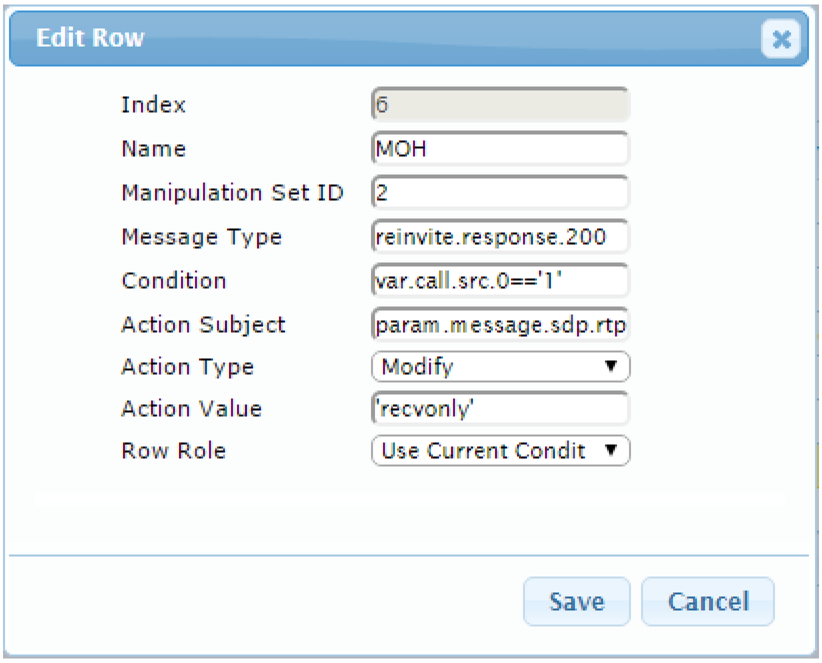
Parameter	Value
Index	**5**
Manipulation Name	**MOH**
Manipulation Set ID	**1**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**‘sendrecv’**
Row Role	**Use Previous Condition**

Figure 3-53: Configuring SIP Message Manipulation Rule 5 (for Microsoft Skype for Business)

8. The following rule attempts to normalize the call processing state back to Microsoft Skype for Business for the correct reply to the initially received “sendonly”. For every SIP Re-INVITE message with the variable set to **'1'**, change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent from the ShoreTel UC system to the Skype for Business initiated Hold.

Parameter	Value
Index	**6**
Manipulation Name	**MOH**
Manipulation Set ID	**2**
Message Type	**reinvite.response.200**
Condition	**var.call.src.0==”1”**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**‘recvonly’**
Row Role	**Use Current Condition**

Figure 3-54: Configuring SIP Message Manipulation Rule 6 (for Microsoft Skype for Business)



9. If the manipulation rule Index 6 (above) is executed, then the following rule is also executed. If the variable is determined to be set to **"1"** (in the previous manipulation rule), then set it to **"0"** in order to normalize the call processing state back. Skype for Business now sends Music on Hold to the ShoreTel UC system even without the ShoreTel UC system knowing how to receive Music on Hold. The call is now truly on hold with Music on Hold.

Parameter	Value
Index	**7**
Manipulation Name	**MOH**
Manipulation Set ID	**2**
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'0'**
Row Role	**Use Previous Condition**

Figure 3-55: Configuring SIP Message Manipulation Rule 7 (for Microsoft Skype for Business)

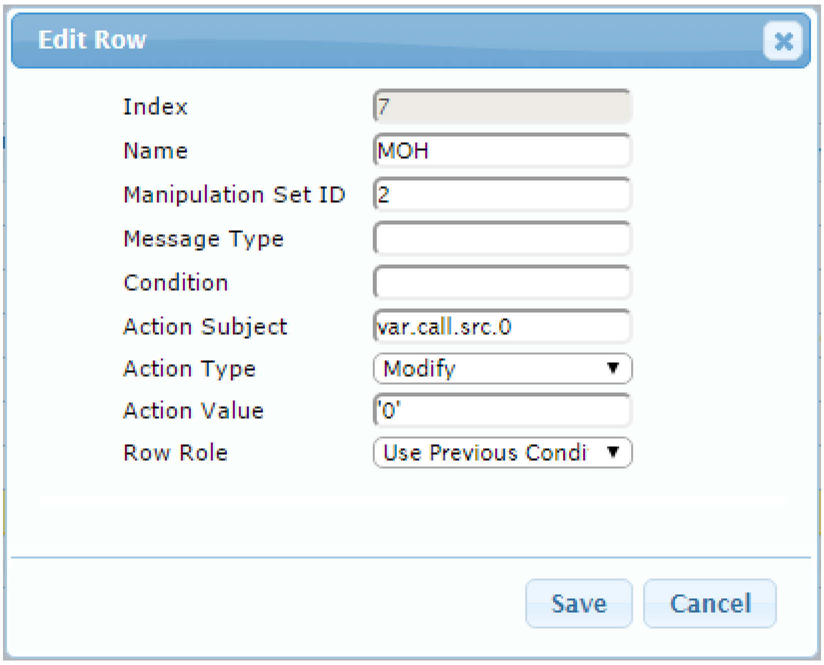


Figure 3-56: Example of Configured SIP Message Manipulation Rules

Message Manipulations

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

Show / Hide

Index	Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	Change Host of History-I	4	invite.request	header.history-inf	header.history-ir	Modify	$1+$2+param.ip	Use Current Con
1	Remove History-Info.1	4	invite.request		header.history-ir	Remove		Use Current Con
2	Change Referred-by Hos	4	invite.request	header.referred-b	header.referred-	Modify	param.ipg.dst.hc	Use Current Con
3	Remove + in Referred-b	4			header.referred-	Remove Prefix	'+'	Use Previous Co
4	MOH	1	reinvite.request	param.message.s	var.call.src.0	Modify	'1'	Use Current Con
5	MOH	1			param.message.	Modify	'sendrecv'	Use Previous Co
6	MOH	2	reinvite.response	var.call.src.0=='1'	param.message.	Modify	'recvonly'	Use Current Con
7	MOH	2			var.call.src.0	Modify	'0'	Use Previous Co

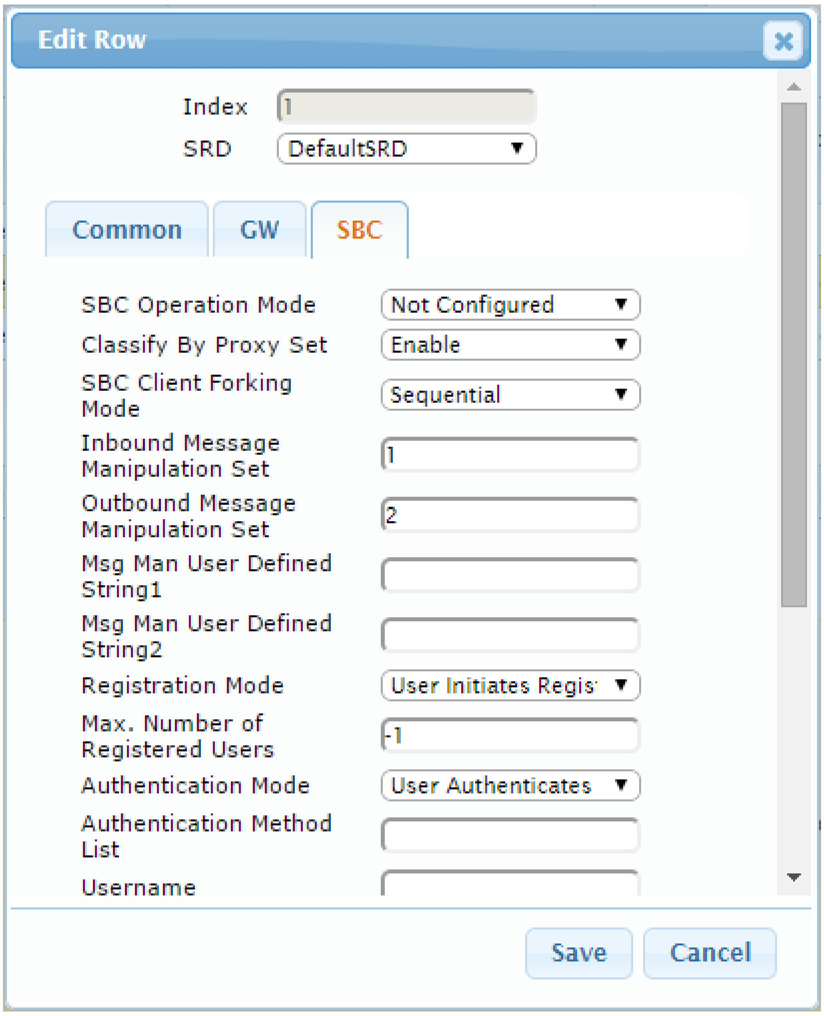
Page 1 of 1 | 10 | View 1 - 8 of 8

The table displayed below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs (Manipulation Set IDs 1, 2, and 4) which are executed for messages sent to and from the ShoreTel UC system IP Group as well as the Skype for Business Server 2015 IP Group. These rules are specifically required to enable proper interworking between ShoreTel UC system and Skype for Business Server 2015. The specific items are needed to support Music on Hold (rules 4-7). Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

<table>
<tr><th>Rule Index</th><th>Rule Description</th><th>Reason for Introducing Rule</th></tr>
<tr><td>0</td><td>This rule applies to messages sent to the ShoreTel UC system IP Group in a call forward scenario. This replaces the user part of the SIP From Header with the value from the SIP History-Info Header.</td><td>To introduce Topology Hiding in the Call Forward scenarios, the host part of the SIP History-Info Header should be replaced with the value that was configured in the SIP Trunk IP Group.</td></tr>
<tr><td>1</td><td>This rule applies to messages sent to the ShoreTel UC system IP Group in a call forward scenario. This rule removes the SIP History-Info.1 Header.</td><td>To introduce Topology Hiding in the Call Forward scenarios, the SIP History-Info.1 Header should be removed.</td></tr>
<tr><td>2</td><td>This rule applies to messages sent to ShoreTel UC system IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-by Header with the value, configured in the ShoreTel UC system IP Group.</td><td rowspan="2">To introduce Topology Hiding in the Call Transfer scenarios, the host part of the SIP Referred-by Header should be replaced with the value that was configured in the SIP Trunk IP Group.</td></tr>
<tr><td>3</td><td>If the manipulation rule Index 2 (above) is executed, then the following rule is also executed. It remove prefix ‘+’ from the Referred-By Header.</td></tr>
<tr><td>4</td><td>For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a S4B-initiated Hold), create a variable and set it to '1'. This variable manages how the call will be handled in each state (answer, request, etc.).</td><td rowspan="4">In the Hold scenario, Microsoft S4B sends Re-INVITE message with the SDP, where the RTP mode is set to “a= sendonly”. However, the ShoreTel UC system support only “a=inactive” RTP mode. This causes the loss of the Music On Hold functionality. These four rules are applied to work around this limitation.</td></tr>
<tr><td>5</td><td>If the previous manipulation rule (Index 4) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to “sendonly”, change it to “sendrecv”.</td></tr>
<tr><td>6</td><td>This rule attempts to normalize the call processing state back to S4B for the correct reply to the initially received “sendonly”. For every SIP Re-INVITE message with the variable set to '1', change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent from the ShoreTel UC system to the S4B-initiated Hold.</td></tr>
<tr><td>7</td><td>If the manipulation rule Index 6 (above) is executed, then the following rule is also executed. If the variable is determined to be set to "1" (in the previous manipulation rule), then set it to “0” to normalize the call processing state. S4B now sends Music on Hold to the ShoreTel UC system even without the ShoreTel UC system knowing how to receive MoH. The call is now truly on hold with MoH.</td></tr>
</table>

10. Assign Manipulation Set IDs 1 and 2 to the Skype for Business 2015 IP Group:
    a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
    b. Select the row of the Skype for Business 2015 IP Group, and then click **Edit**.
    c. Click the **SBC** tab.
    d. Set the 'Inbound Message Manipulation Set' field to **1**.
    e. Set the 'Outbound Message Manipulation Set' field to **2**.

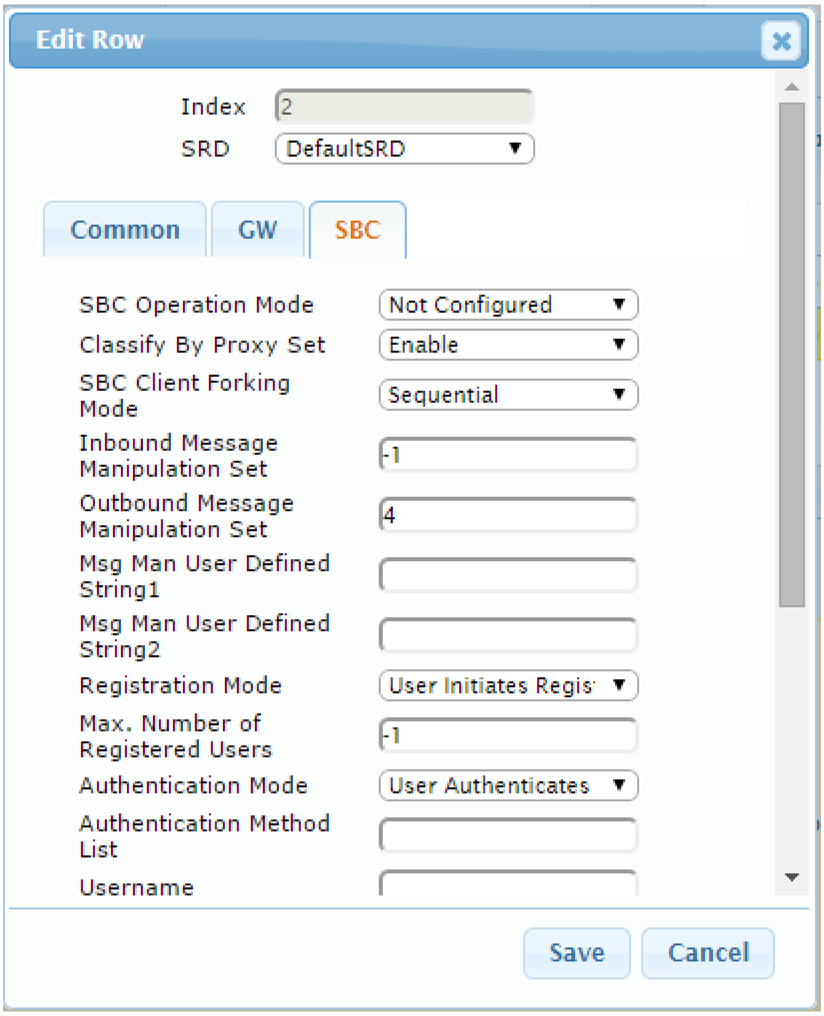
Figure 3-57: Assigning Manipulation Set to the Skype for Business 2015 IP Group



    f. Click **Submit**.

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

Figure 3-58: Assigning Manipulation Set 4 to the ShoreTel UC system IP Group



    e. Click **Submit**.

3.15 Step 15: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

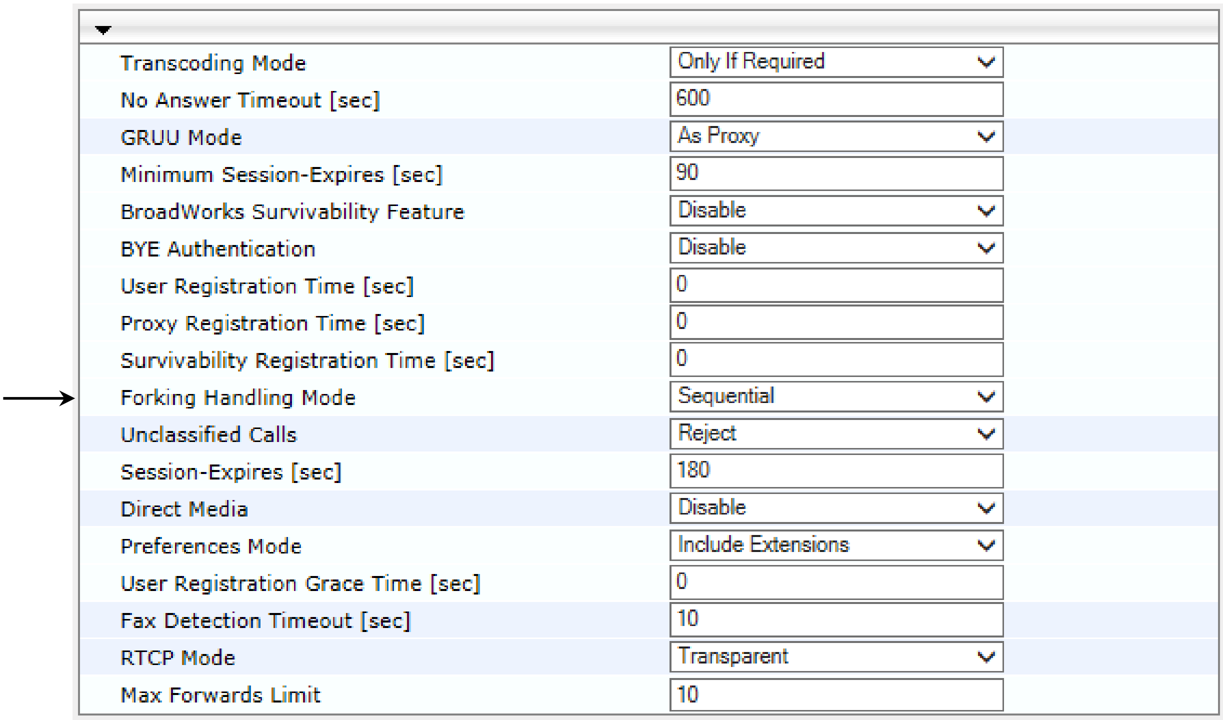
3.15.1 Step 15a: Configure Call Forking Mode

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

➢ **To configure call forking:**

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

Figure 3-59: Configuring Forking Mode



3. Click **Submit**.

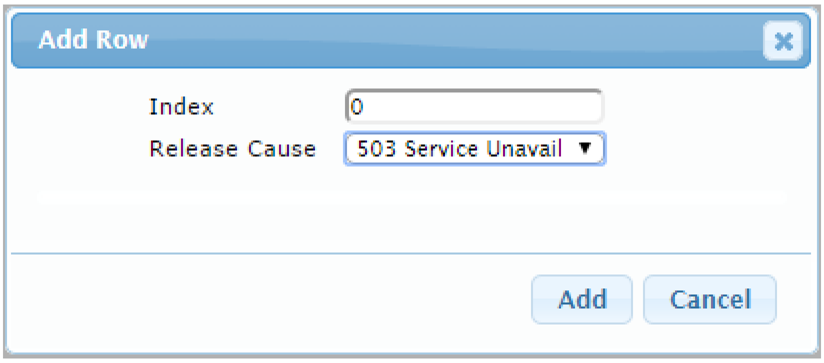
3.15.2 Step 15b: Configure SBC Alternative Routing Reasons

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

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

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

Figure 3-60: SBC Alternative Routing Reasons Table - Add Record



3. Click **Submit**.

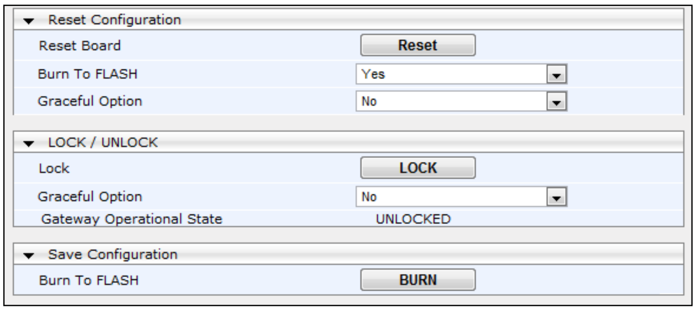
3.16 Step 16: Reset the E-SBC

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

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

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

Figure 3-61: Resetting the E-SBC



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

4 Configuring Microsoft Skype for Business Server 2015

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

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

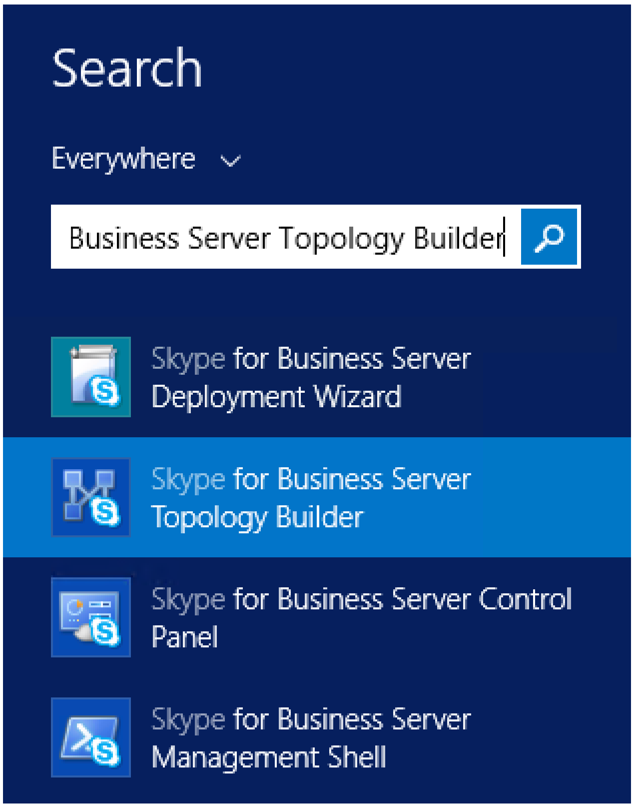
4.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

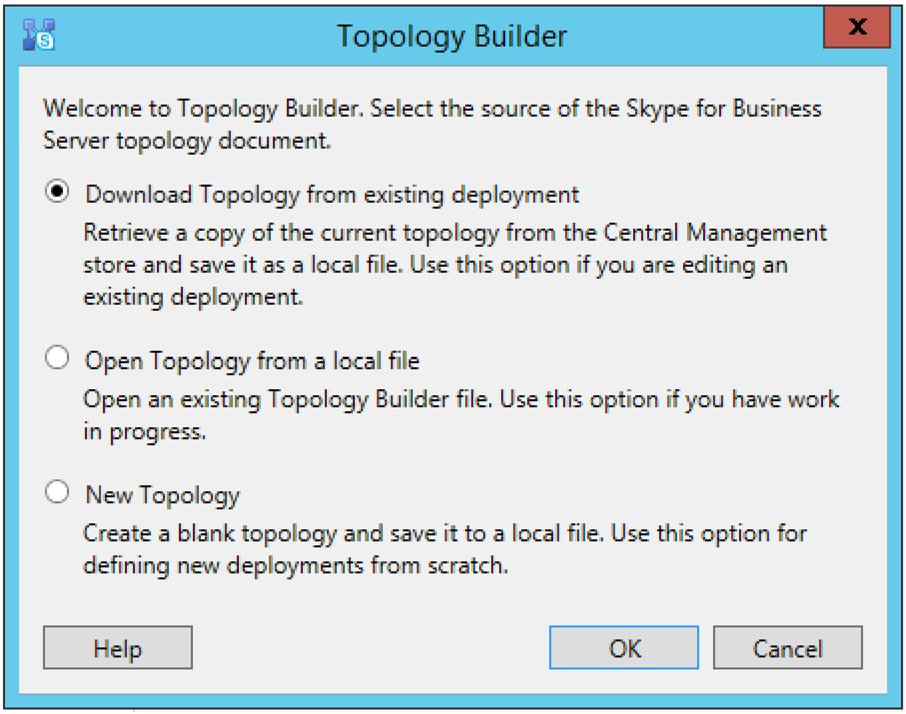
1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

Figure 4-1: Starting the Skype for Business Server Topology Builder



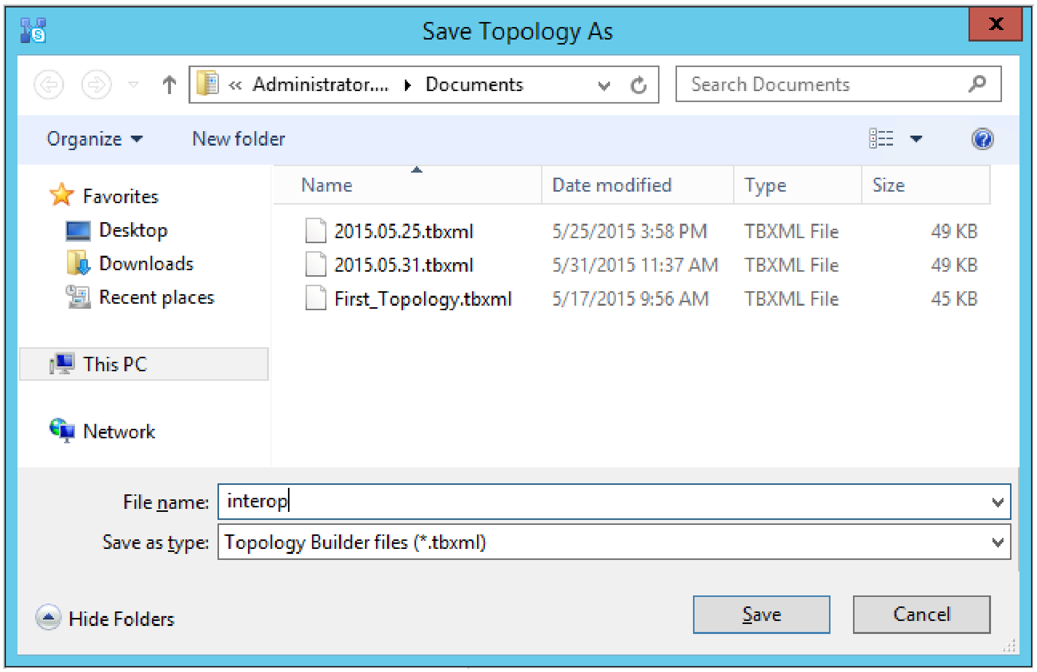
The following is displayed:

Figure 4-2: 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:

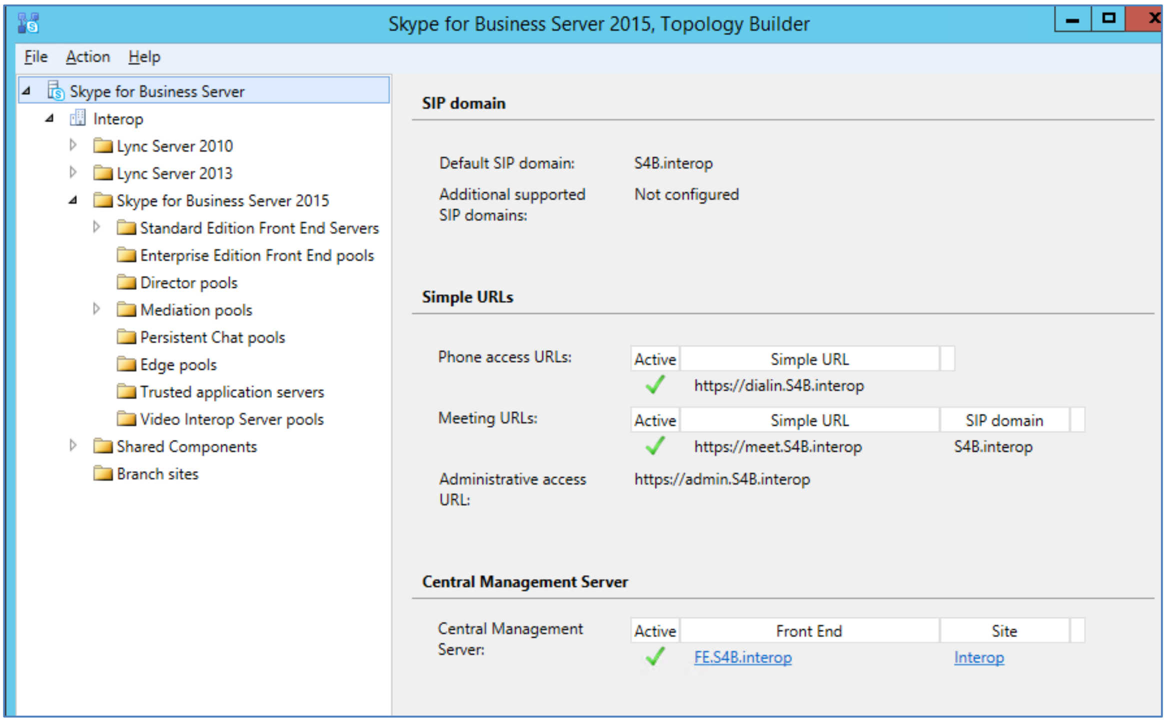
Figure 4-3: Save Topology Dialog Box



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.

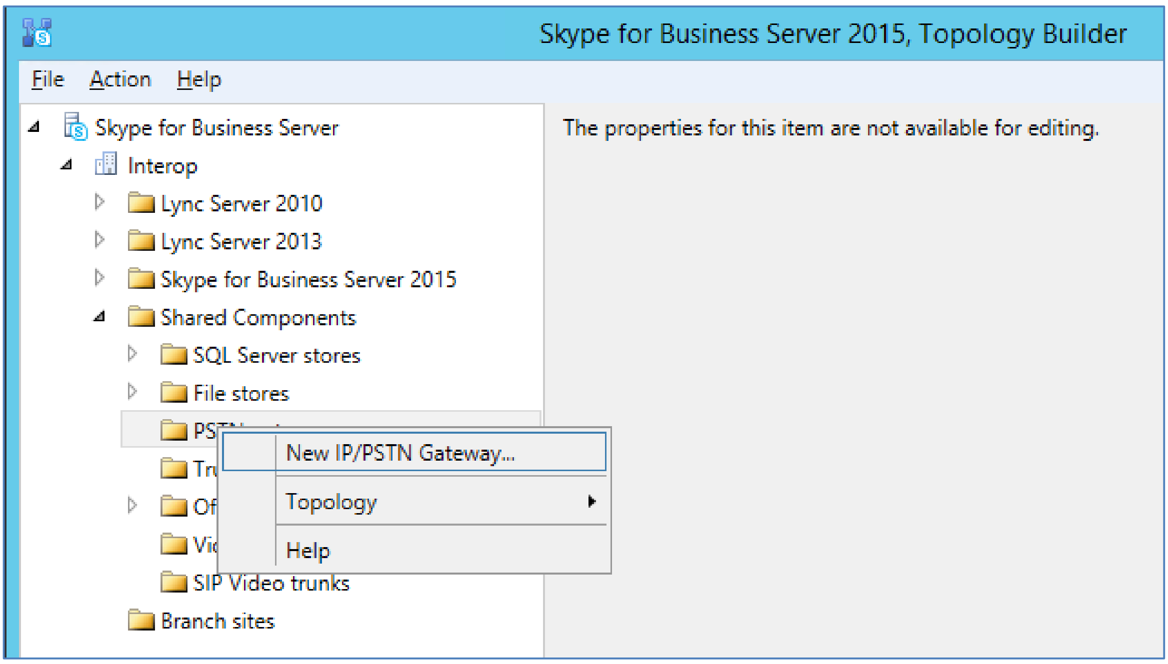
The Topology Builder screen with the downloaded Topology is displayed:

Figure 4-4: Downloaded Topology



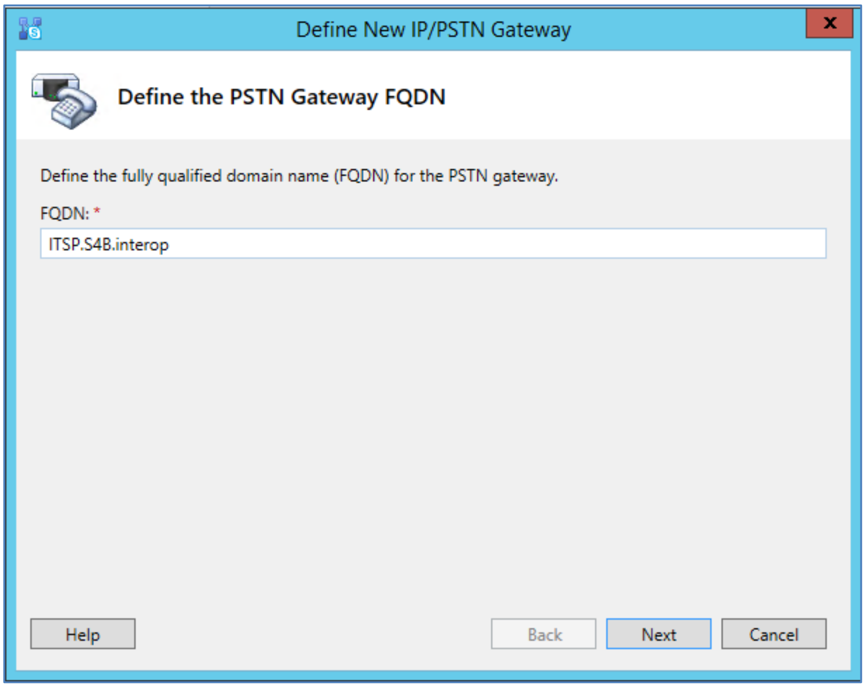
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 4-5: Choosing New IP/PSTN Gateway



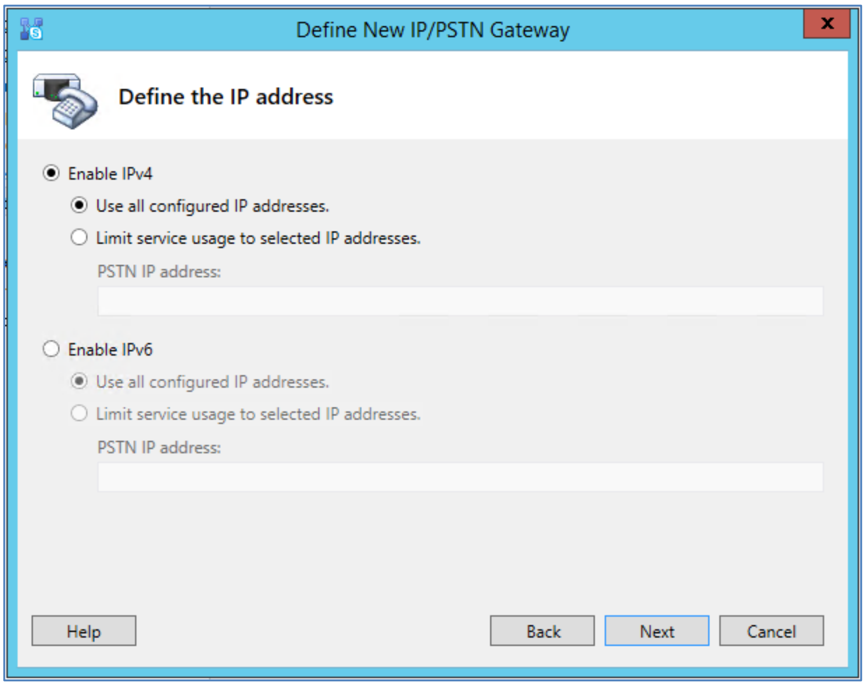
The following is displayed:

Figure 4-6: Define the PSTN Gateway FQDN



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

Figure 4-7: Define the IP Address



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

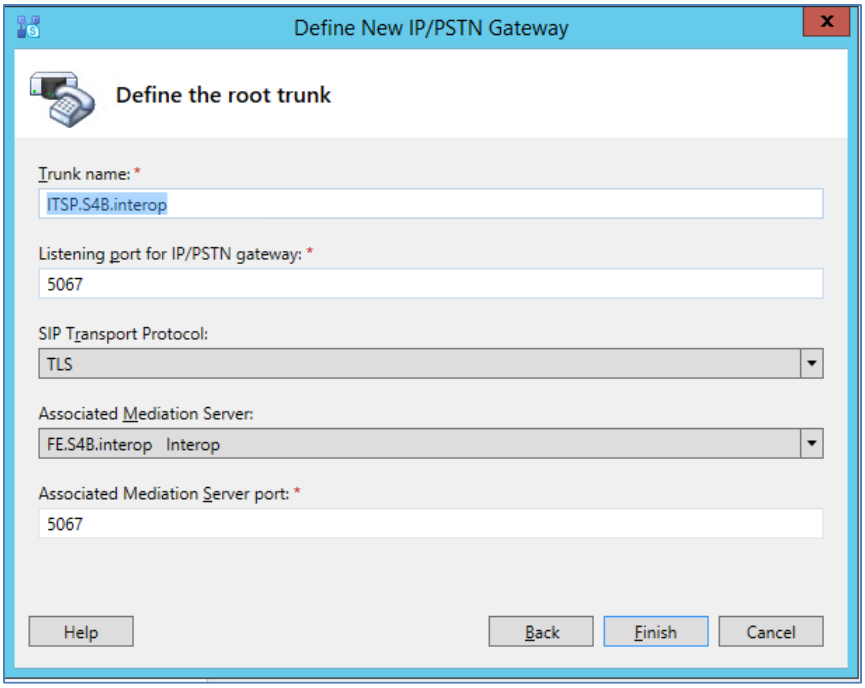
7. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server FQDN, Mediation Server listening port (TLS or TCP), gateway IP and

FQDN, and gateway listening port.

Notes:

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

Figure 4-8: Define the Root Trunk



a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**).

b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses.

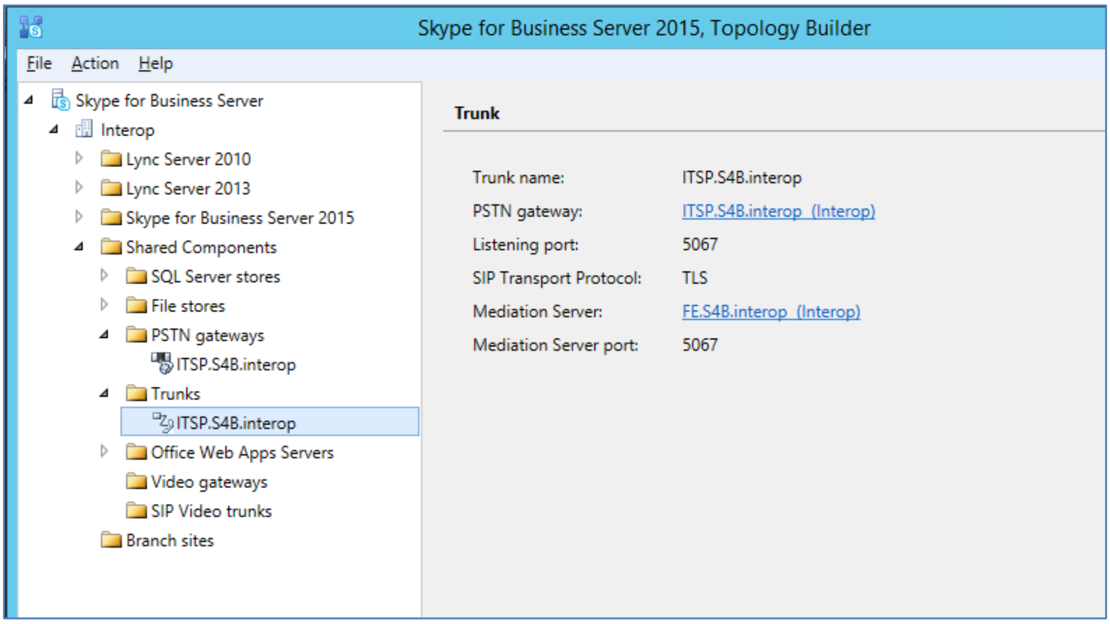
c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.

d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).

e. Click **Finish**.

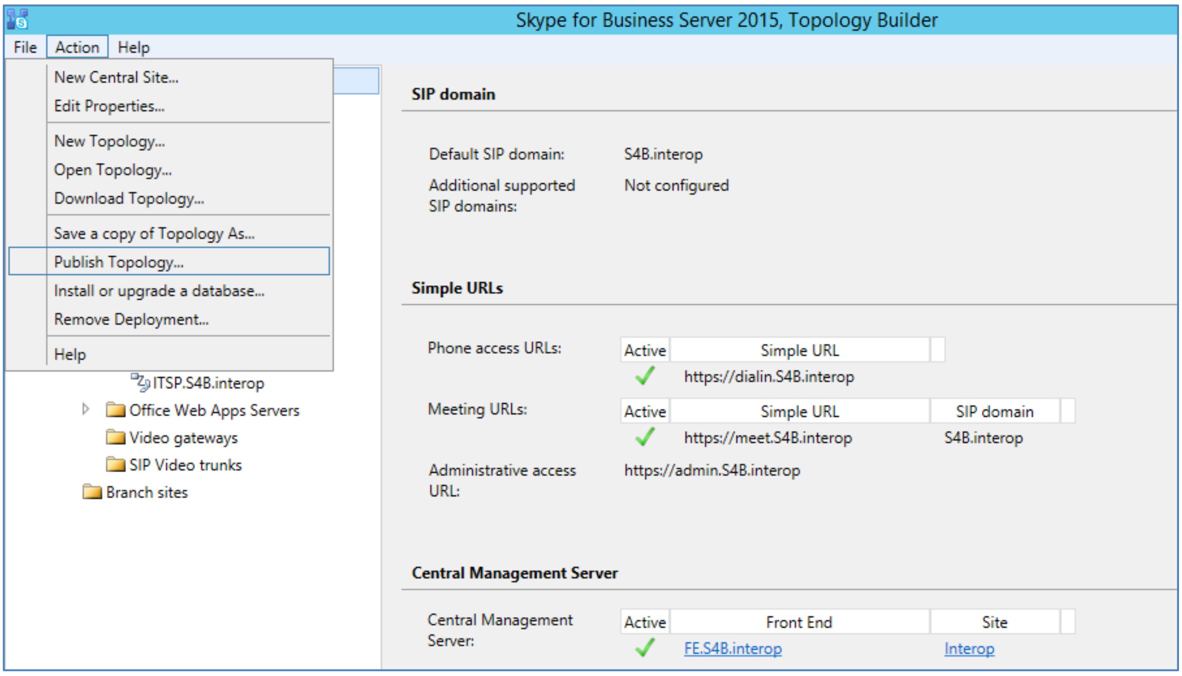
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

Figure 4-9: E-SBC added as IP/PSTN Gateway and Trunk Created



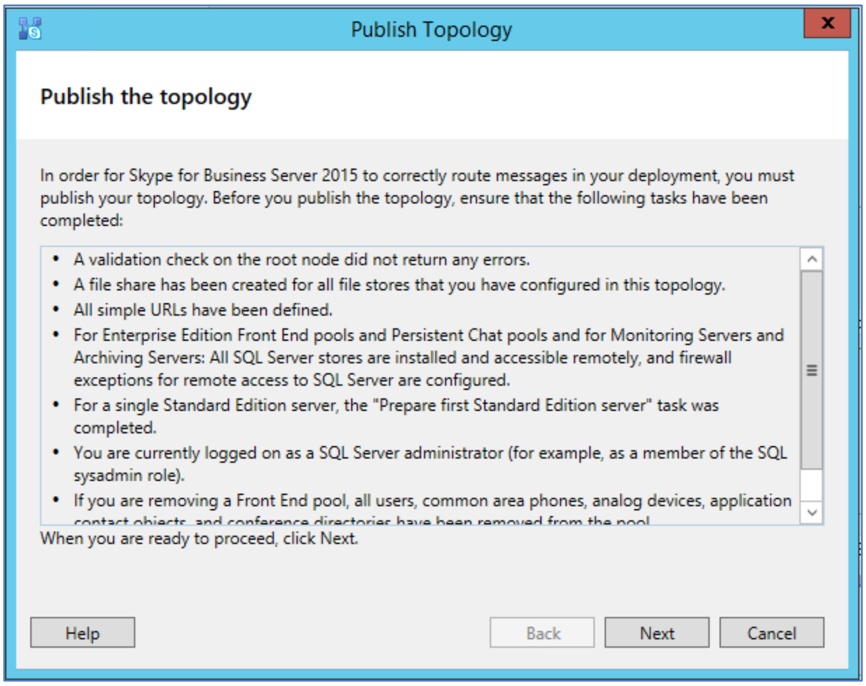
8. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 4-10: Choosing Publish Topology



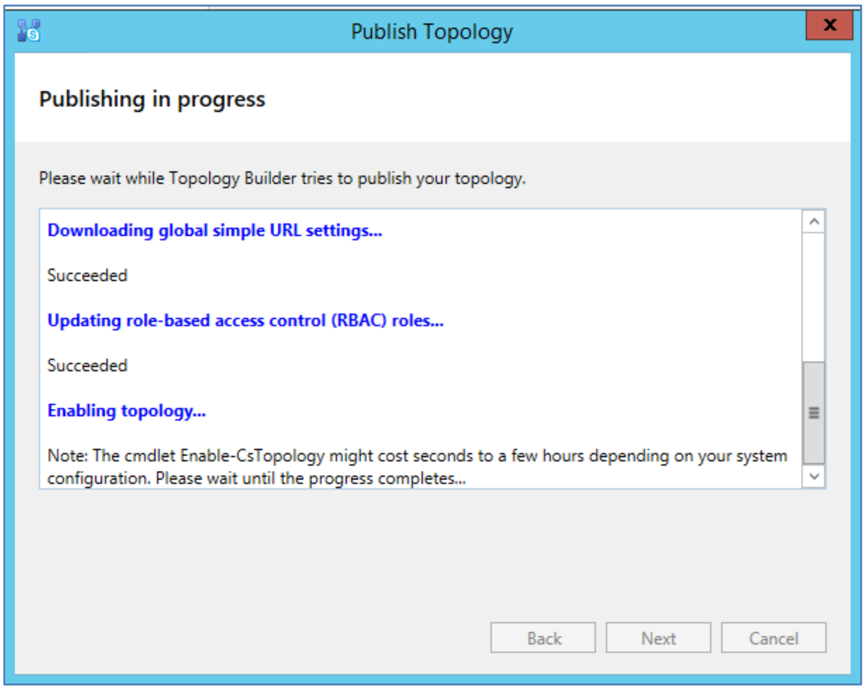
The following is displayed:

Figure 4-11: Publish the Topology



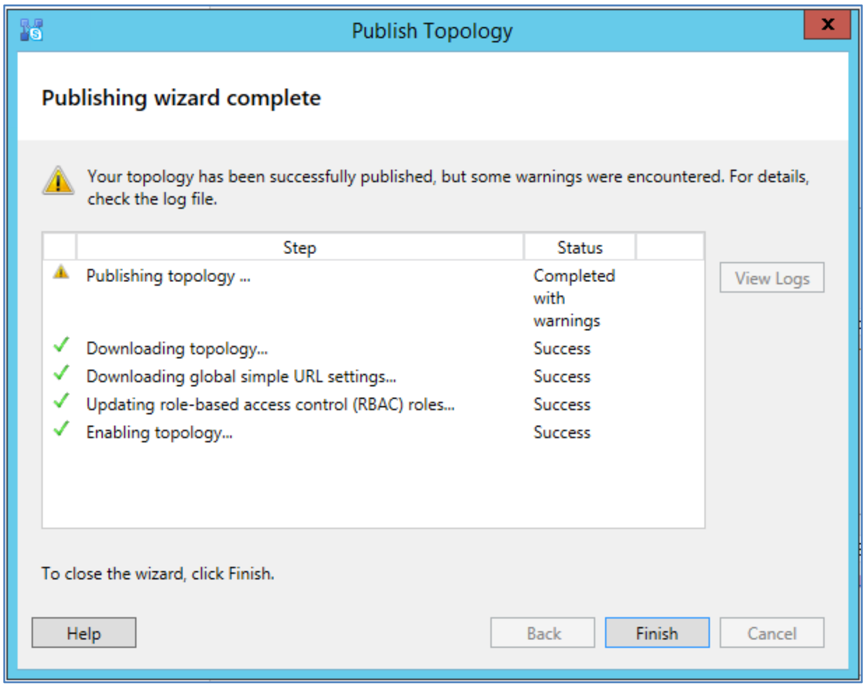
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 4-12: Publishing in Progress



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

Figure 4-13: Publishing Wizard Complete



11. Click **Finish**.

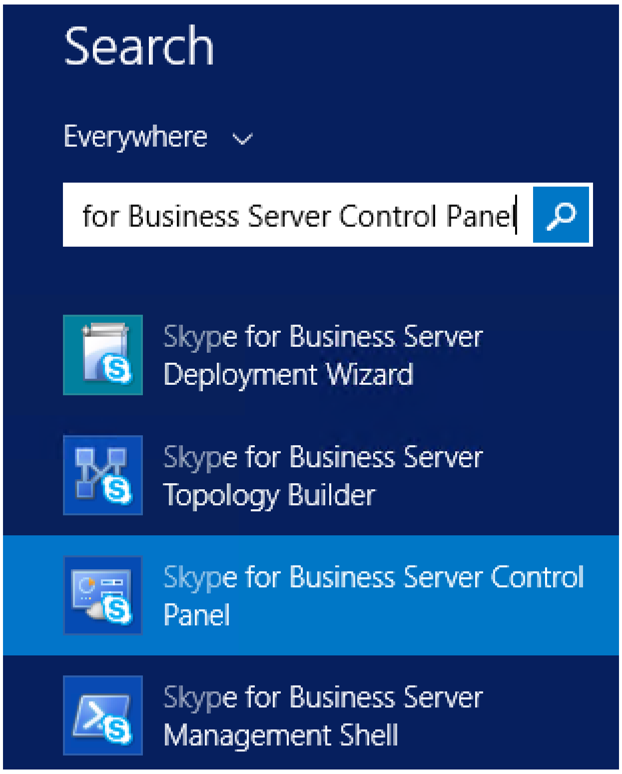
4.2 Configuring the "Route" on Skype for Business Server 2015

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

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

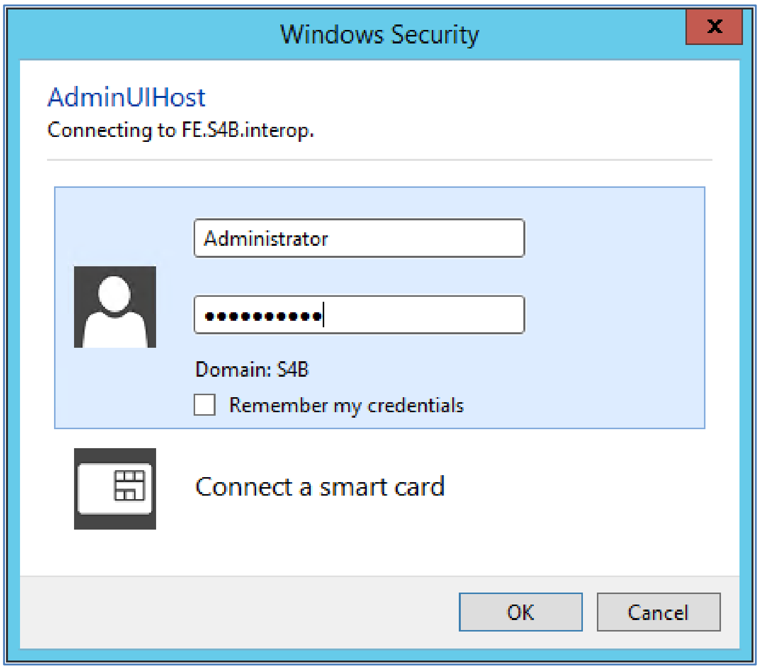
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

Figure 4-14: Opening the Skype for Business Server Control Panel



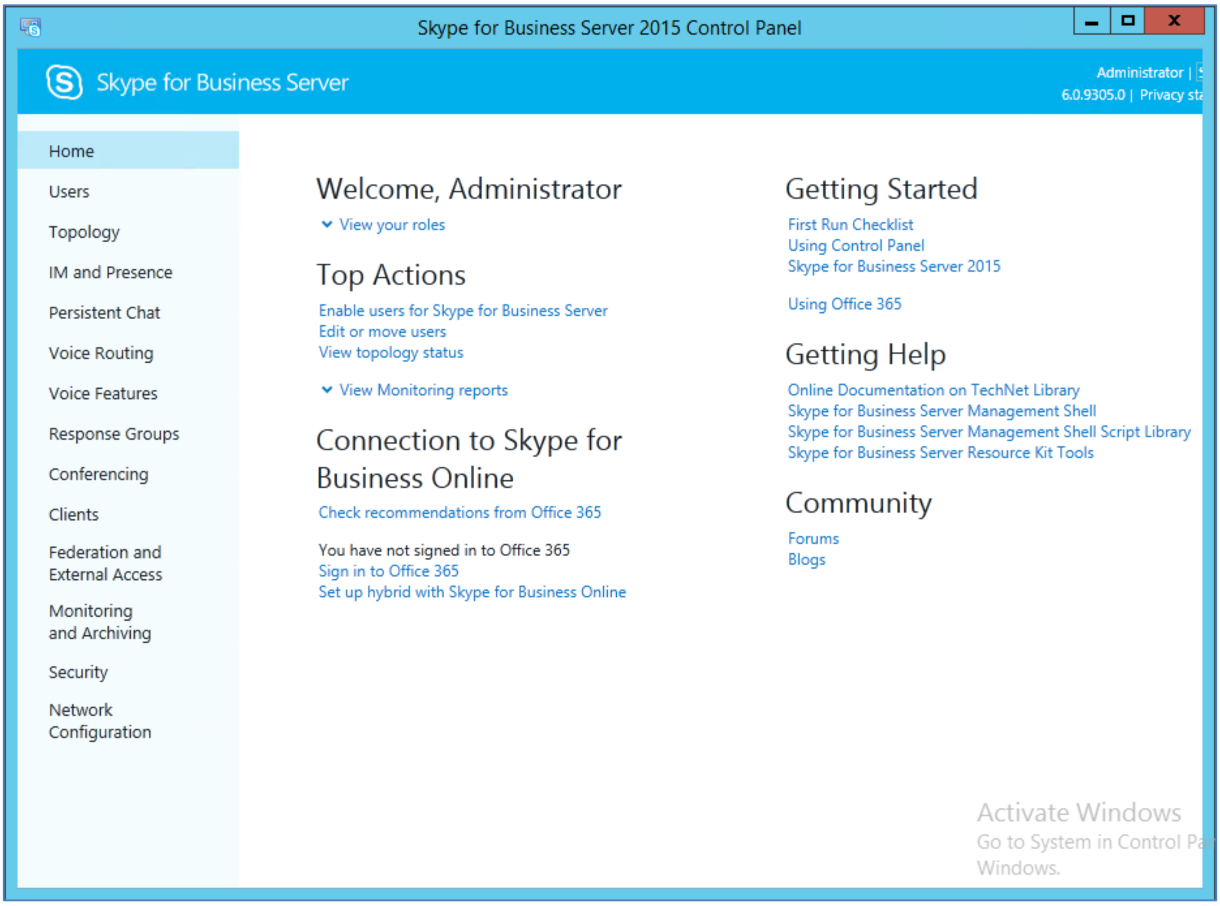
2. You are prompted to enter your login credentials:

Figure 4-15: Skype for Business Server Credentials



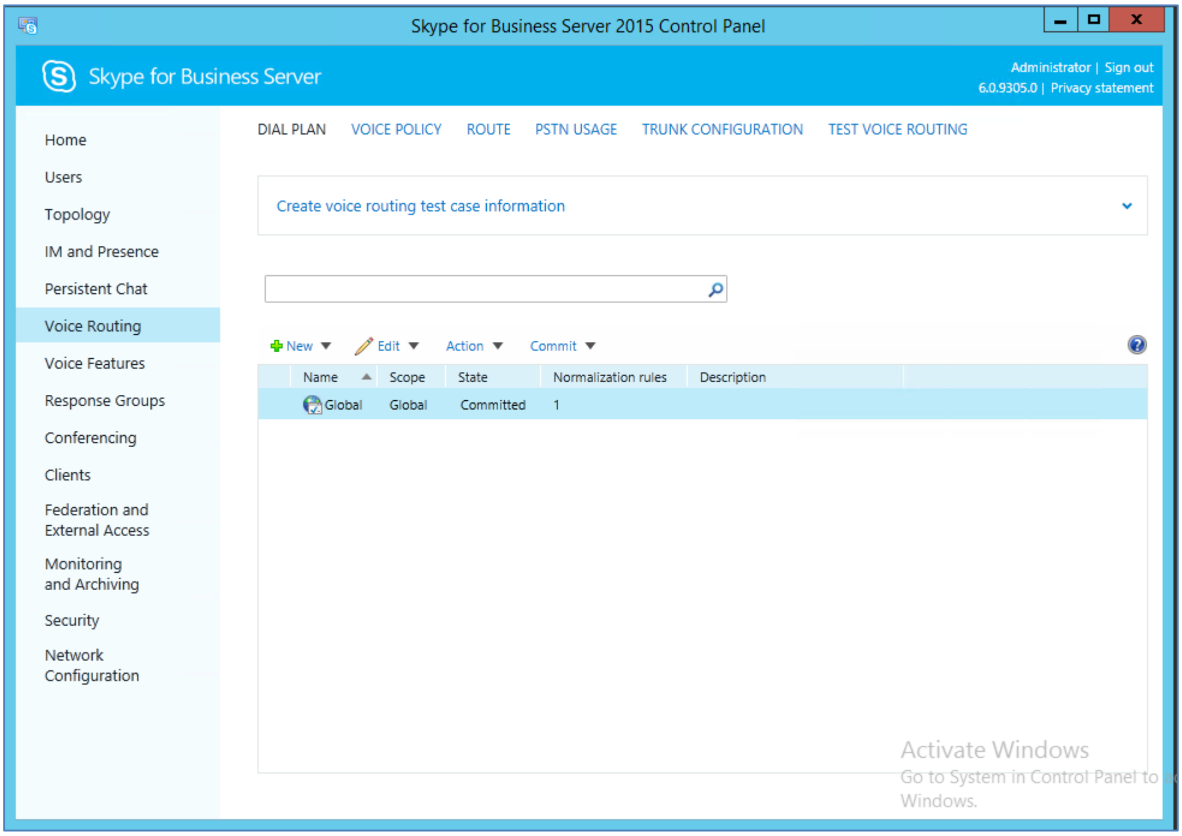
3. Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

Figure 4-16: Microsoft Skype for Business Server 2015 Control Panel



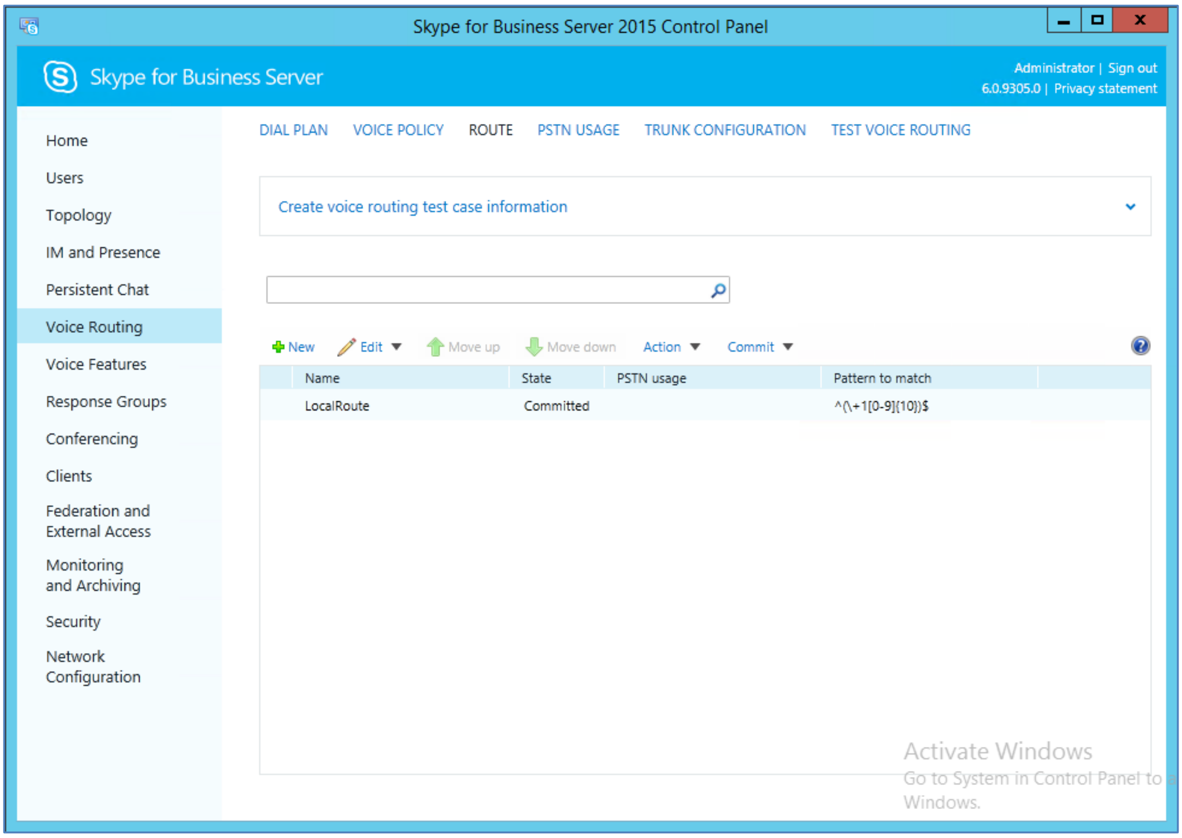
4. In the left navigation pane, select **Voice Routing**.

Figure 4-17: Voice Routing Page



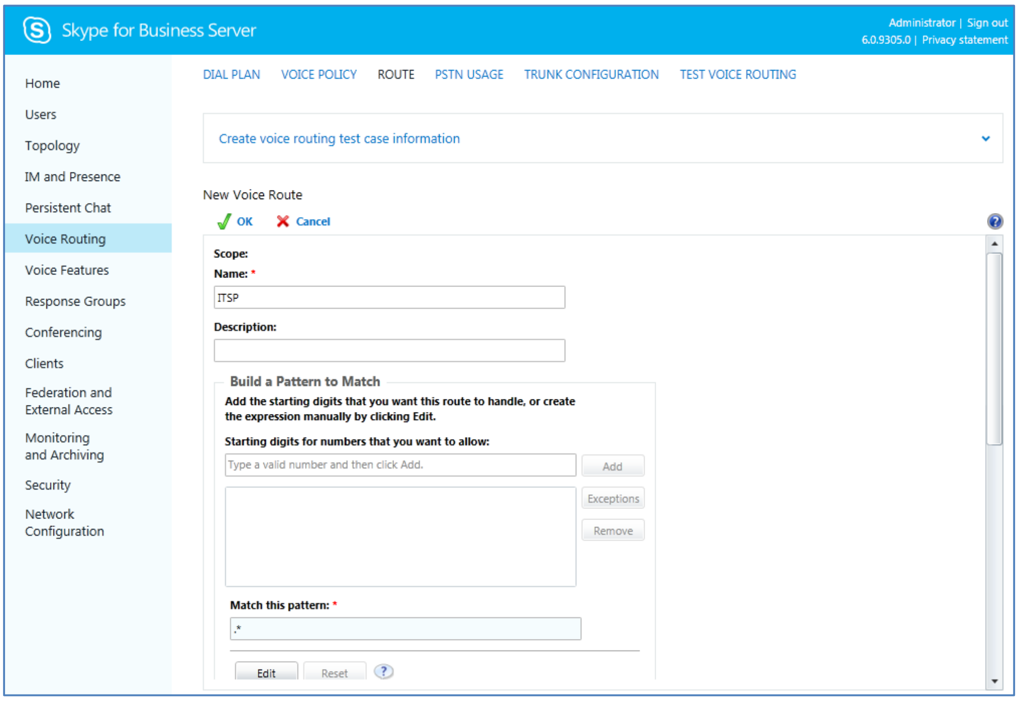
5. In the Voice Routing page, select the **Route** tab.

Figure 4-18: Route Tab



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

Figure 4-19: Adding New Voice Route



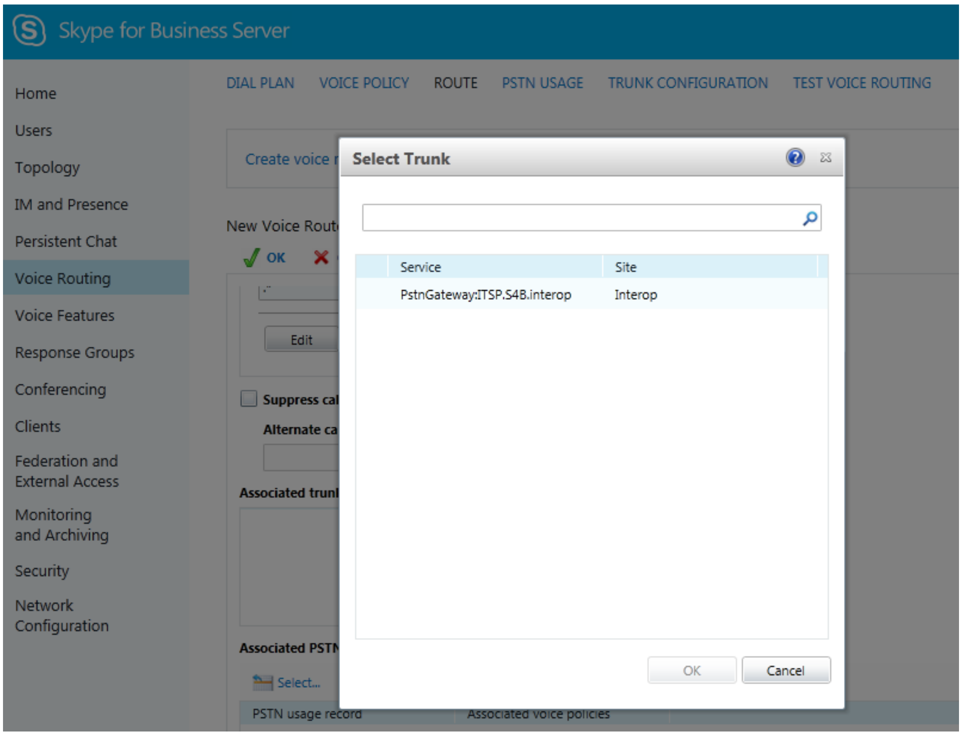
7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).

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:

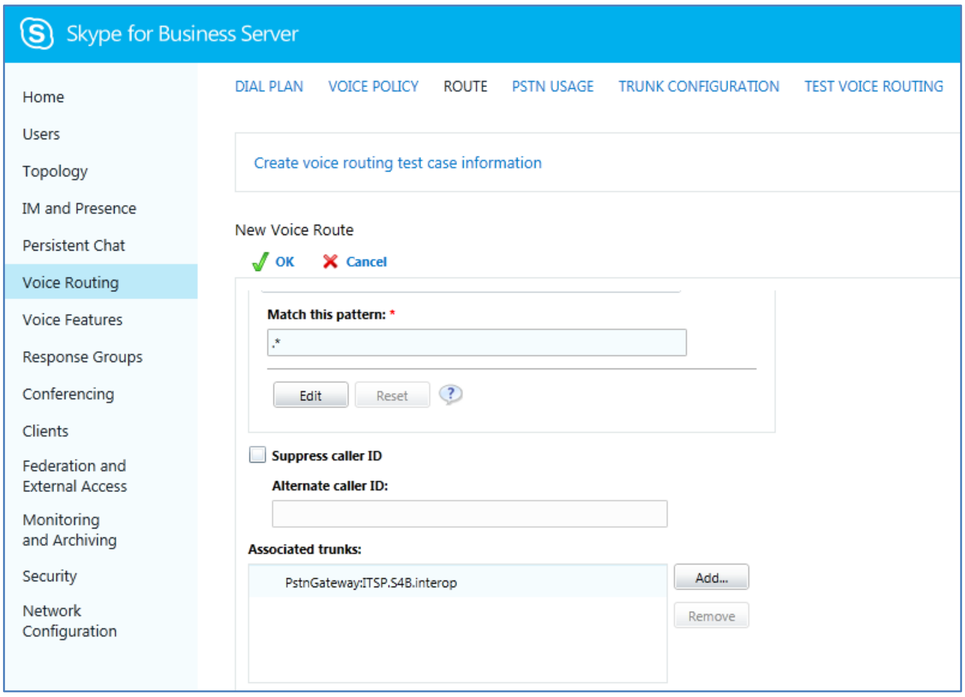
a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 4-20: 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:

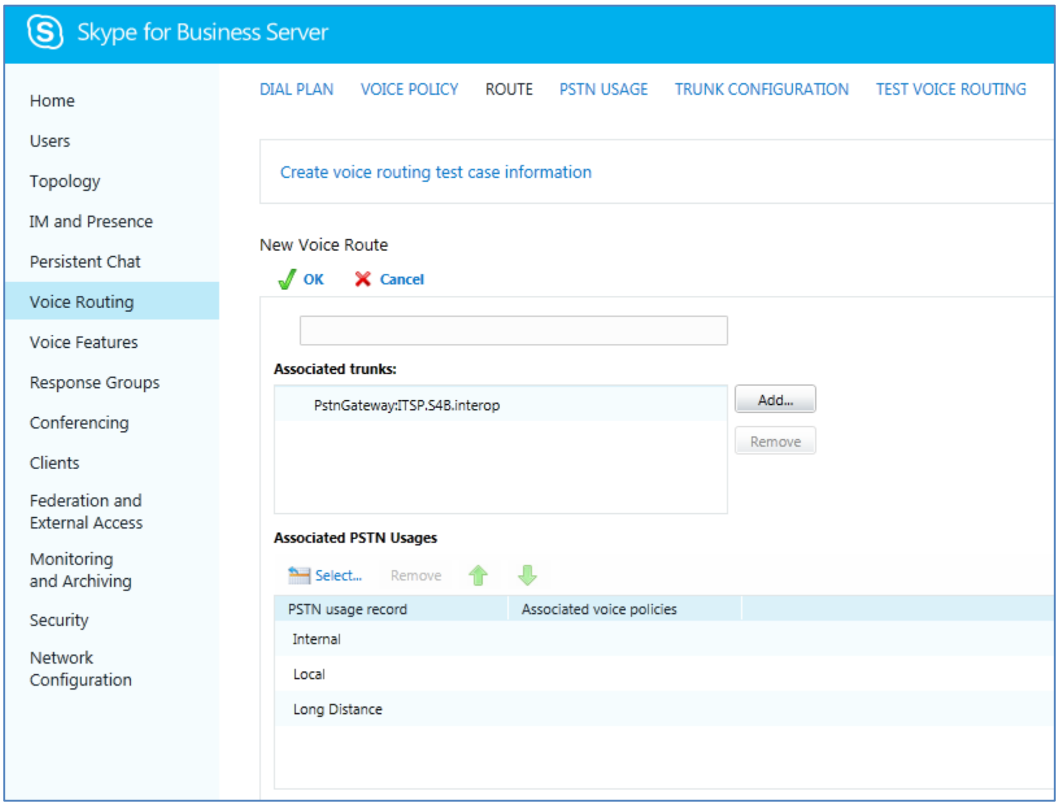
Figure 4-21: Selected E-SBC Trunk



10. Associate a PSTN Usage to this route:

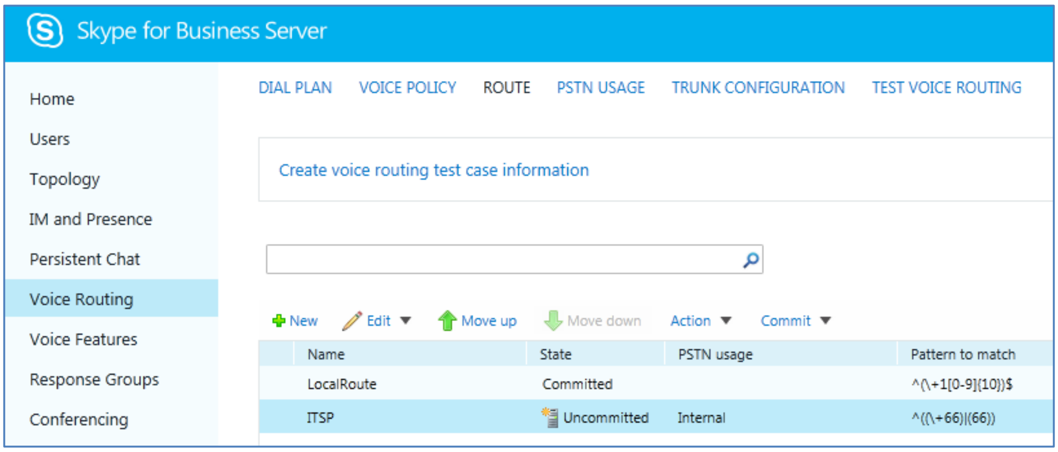
c. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 4-22: Associating PSTN Usage to Route



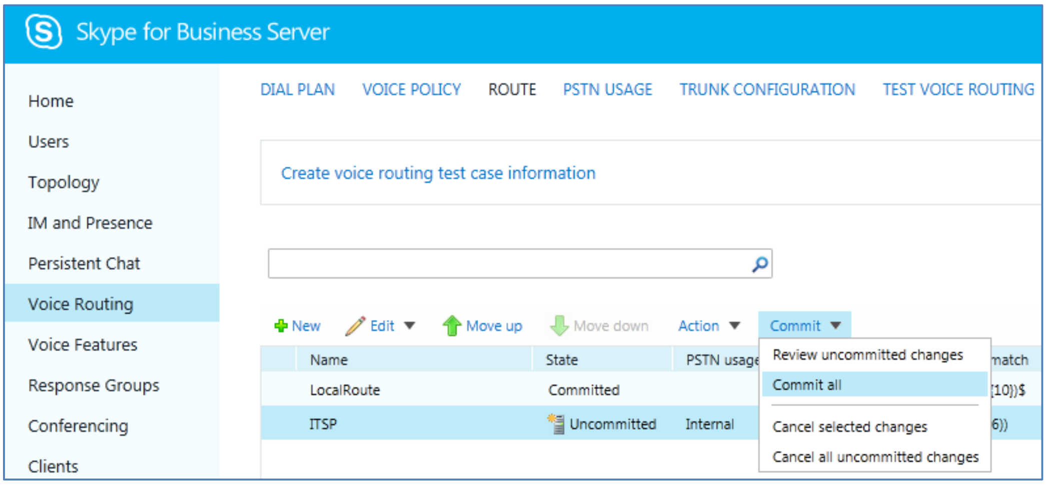
11. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 4-23: Confirmation of New Voice Route



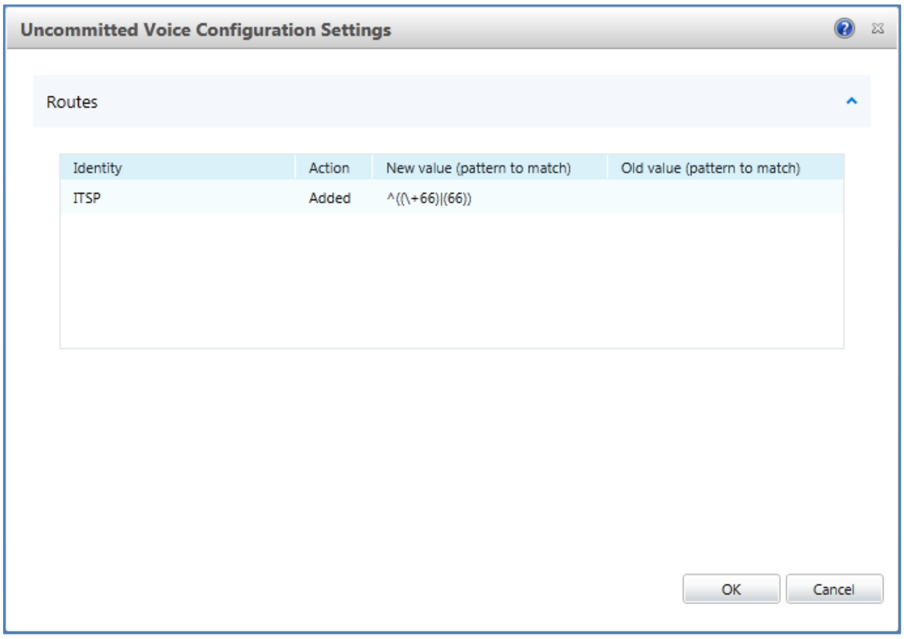
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 4-24: Committing Voice Routes



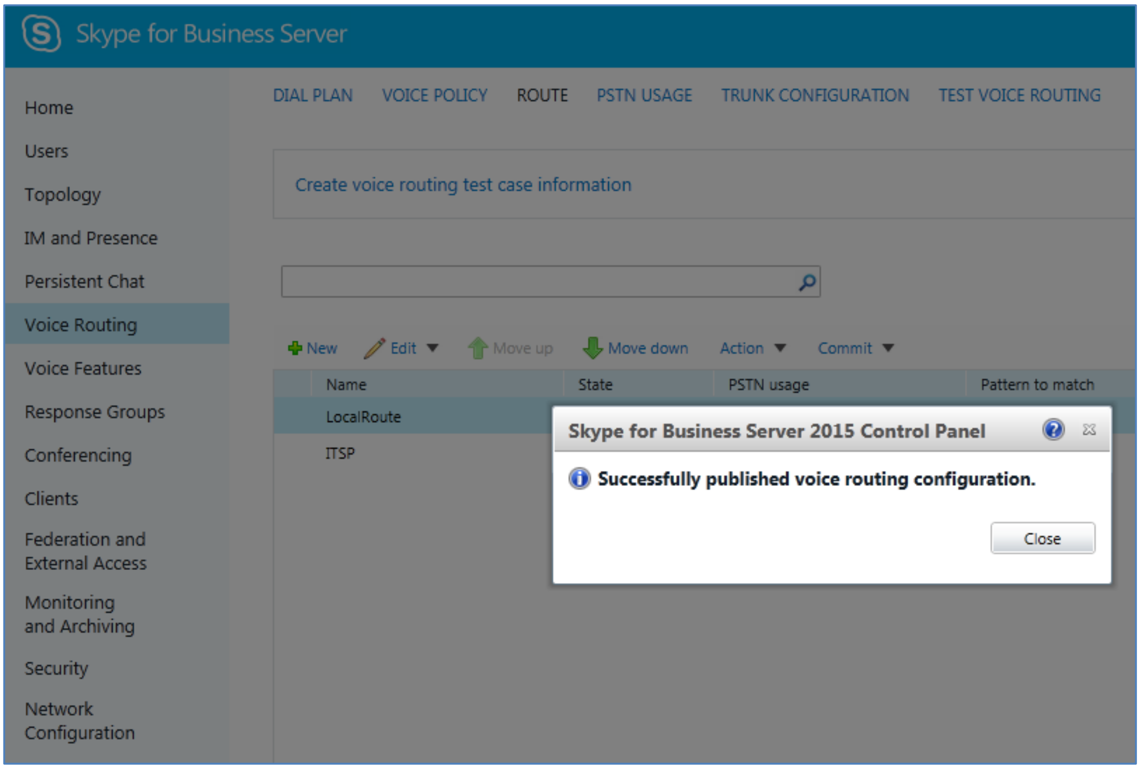
The Uncommitted Voice Configuration Settings page appears:

Figure 4-25: Uncommitted Voice Configuration Settings



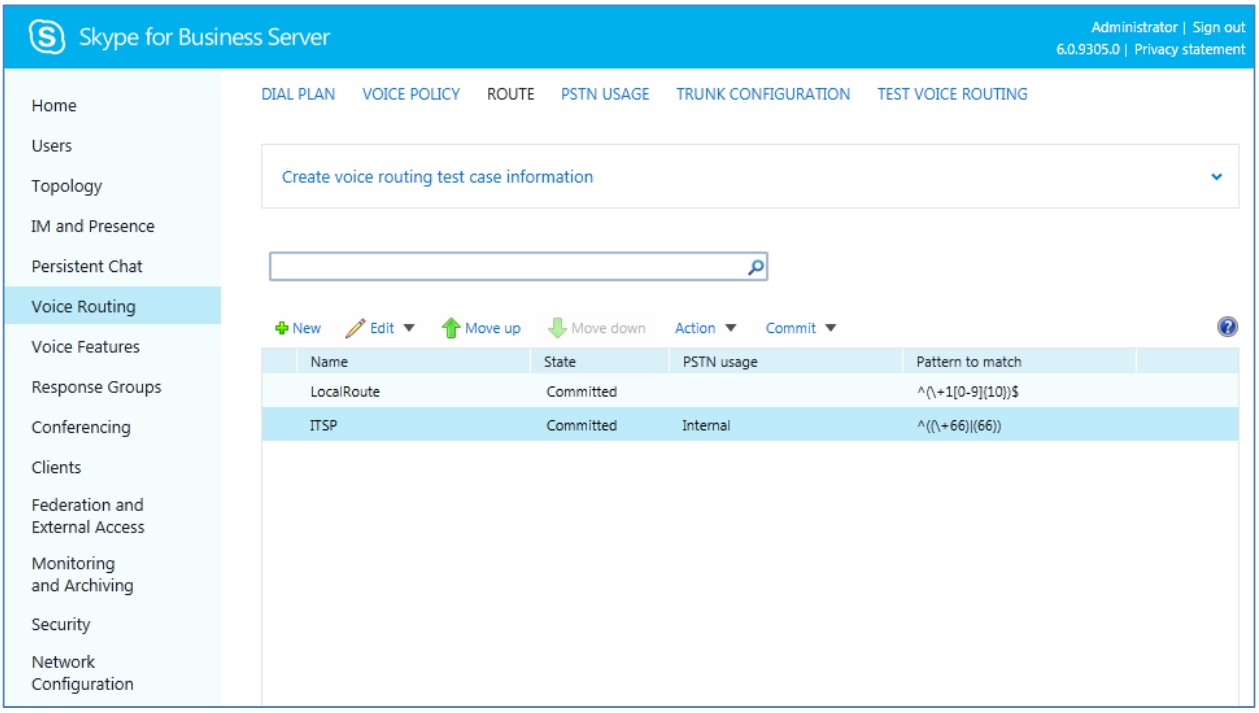
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 4-26: Confirmation of Successful Voice Routing Configuration



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

Figure 4-27: Voice Routing Screen Displaying Committed Routes

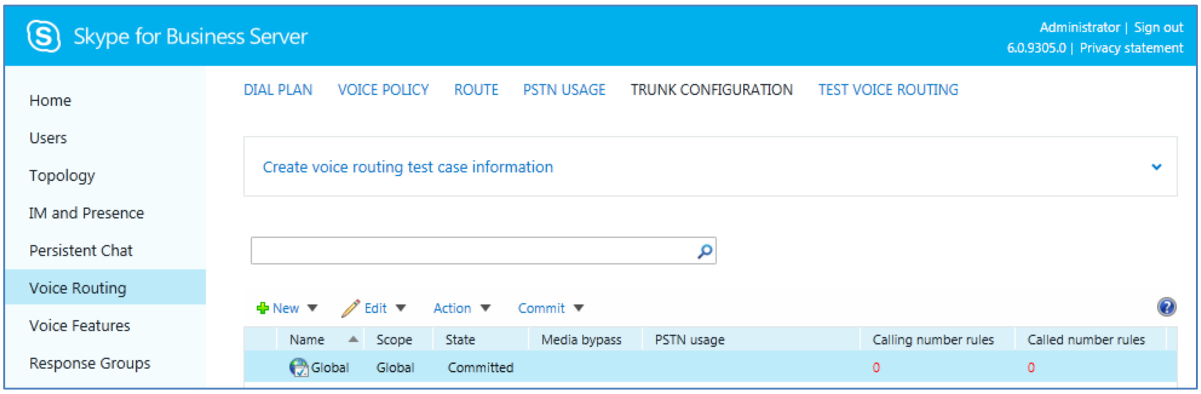


15. For ITSPs that implement a call identifier, continue with the following steps:

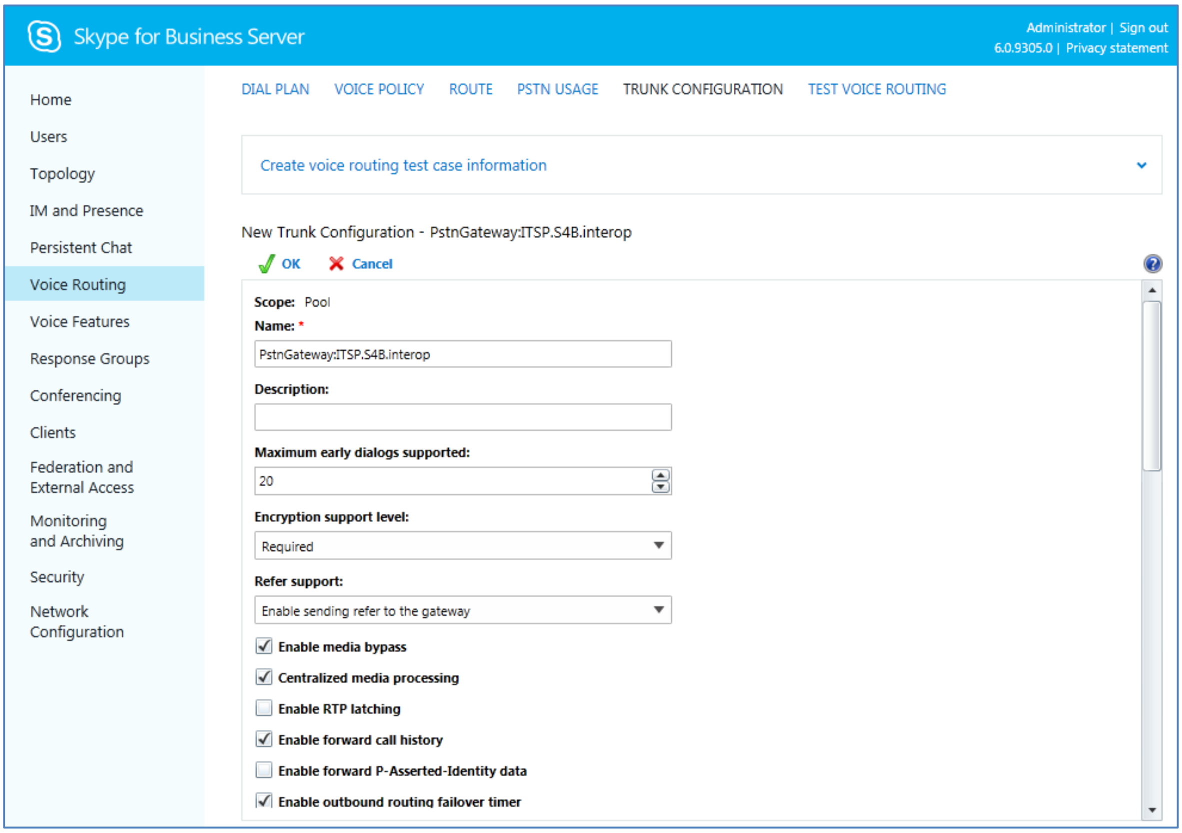
Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Skype for Business user number). This ID is required by ShoreTel UC system in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 3.6 on page 33).

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 4-28: 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.