Configuration Note

AudioCodes Professional Services - Interoperability Lab

Microsoft® Lync™ Server 2013 and Telus' SIP Trunk using AudioCodes Mediant™ E-SBC

Version 7.0

Table of Contents

This page is intentionally left blank.

Notice

This document describes how to connect the Microsoft Lync Server 2013 and Telus' SIP Trunk using AudioCodes Mediant E-SBC product series.

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

Date Published: September-03-2015

Trademarks

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
12222	Initial document release for Version 7.0.
12223	Update for Internet registration-based connection method.

Documentation Feedback

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

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between Telus' SIP Trunk and Microsoft's Lync Server 2013 environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Telus' Partners who are responsible for installing and configuring Telus' SIP Trunk and Microsoft's Lync Server 2013 for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_7.00A.017.012
Protocol	▪ SIP/UDP (to the Telus SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 Telus SIP Trunking Version

Table 2-2: Telus Version

Vendor/Service Provider	Telus
SSW Model/Service	Oracle AP6300 Session Border Controller GENBAND's EXPERiUS™ Application Server
Software Version	SBC: Oracle AP6300 Session Border Controller 7.1.2 MR 4 GENBAND's EXPERiUS Application Server MCP-17.0.18.4
Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Server 2013 Version

Table 2-3: Microsoft Lync Server 2013 Version

Vendor	Microsoft
Model	Microsoft Lync
Software Version	Release 2013 5.0.8308.556
Protocol	SIP
Additional Notes	None

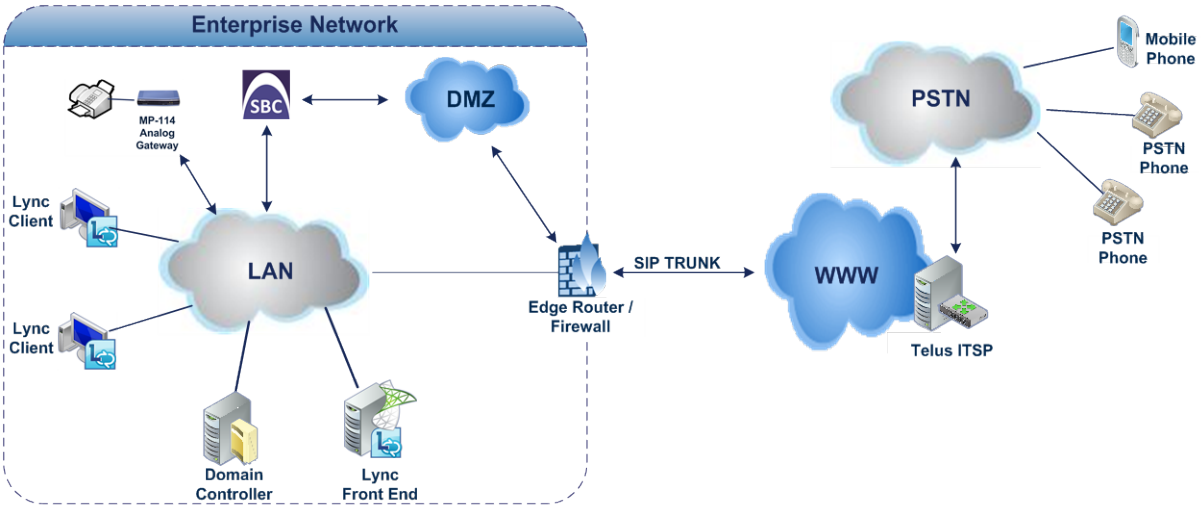
2.4 Interoperability Test Topology

Interoperability testing between AudioCodes E-SBC and Telus' SIP Trunk with Lync 2013 was performed using the following topology setup:

- Enterprise deployed with Microsoft Lync Server 2013 in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Telus' SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between Lync Server 2013 network in the Enterprise LAN and Telus' SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Lync with Telus SIP Trunk



Note: The topology can be based on two different Telus connectivity methods - VPN-based or Internet registration-based. Throughout this document, where configuration depends on the specific connectivity method, the required configuration will be indicated.

2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN ▪ Telus' SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type ▪ 7BTelus SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ Telus' SIP Trunk supports G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2013 operates with SRTP media type ▪ Telus' SIP Trunk operates with RTP media type

2.4.2 Known Limitations

One limitation was observed in the interoperability tests performed for the AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and Telus' SIP Trunk.

The interworking is related to the NPA-555-1212 operator-assisted answer service not being supported in a Microsoft Lync environment. The call flow for the specific call scenario is a pre-answer (pre 200-OK) operator assist, in which a caller then speaks with an operator/attendant to complete the intended call. Microsoft Lync does not open the talk path bi-directionally until a 200-OK is received, thus a one-way talk path is observed. This call type is not supported by the Microsoft Lync environment.

Although not a limitation, an interaction was observed in which the Telus infrastructure initiates a call scenario hold/resume using the UPDATE method. This was also observed when the call was originated from the HSPA (High Speed Packet Access) environment of the Telus infrastructure to the enterprise Microsoft Lync deployment.

This page is intentionally left blank.

3 Configuring Lync Server 2013

This chapter describes how to configure Microsoft Lync Server 2013 to operate with AudioCodes E-SBC.

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

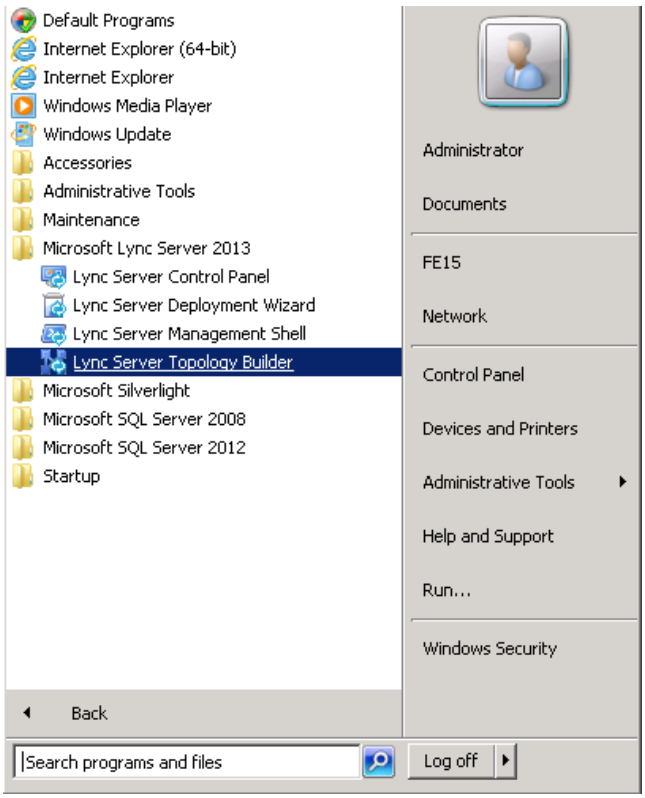
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

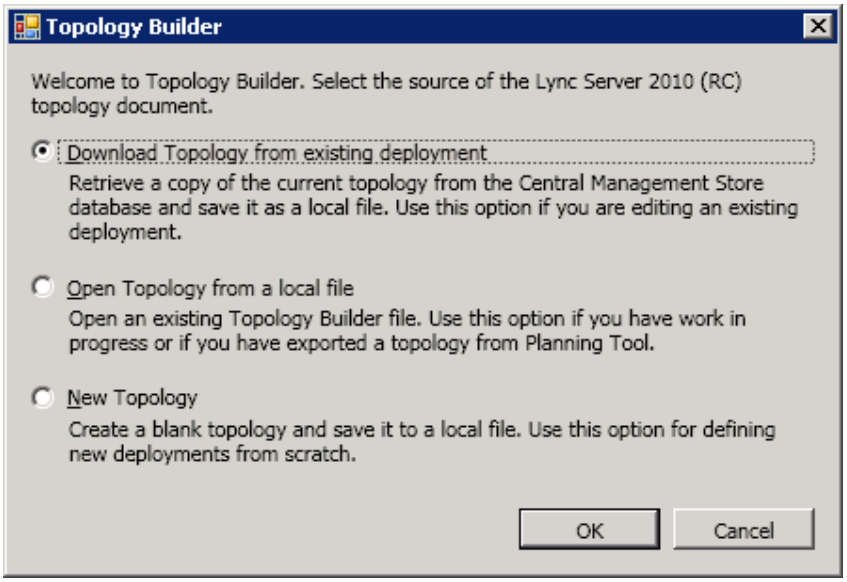
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



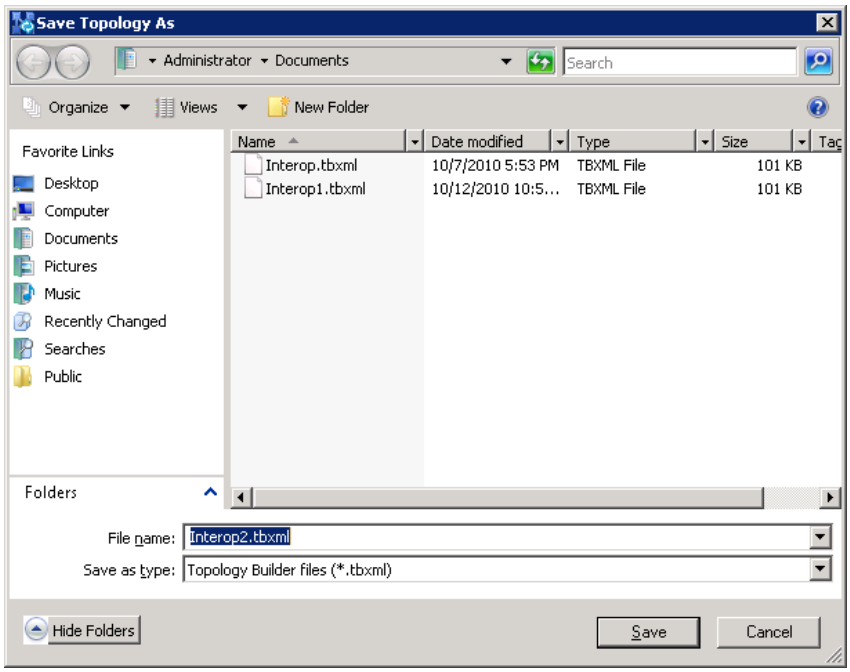
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

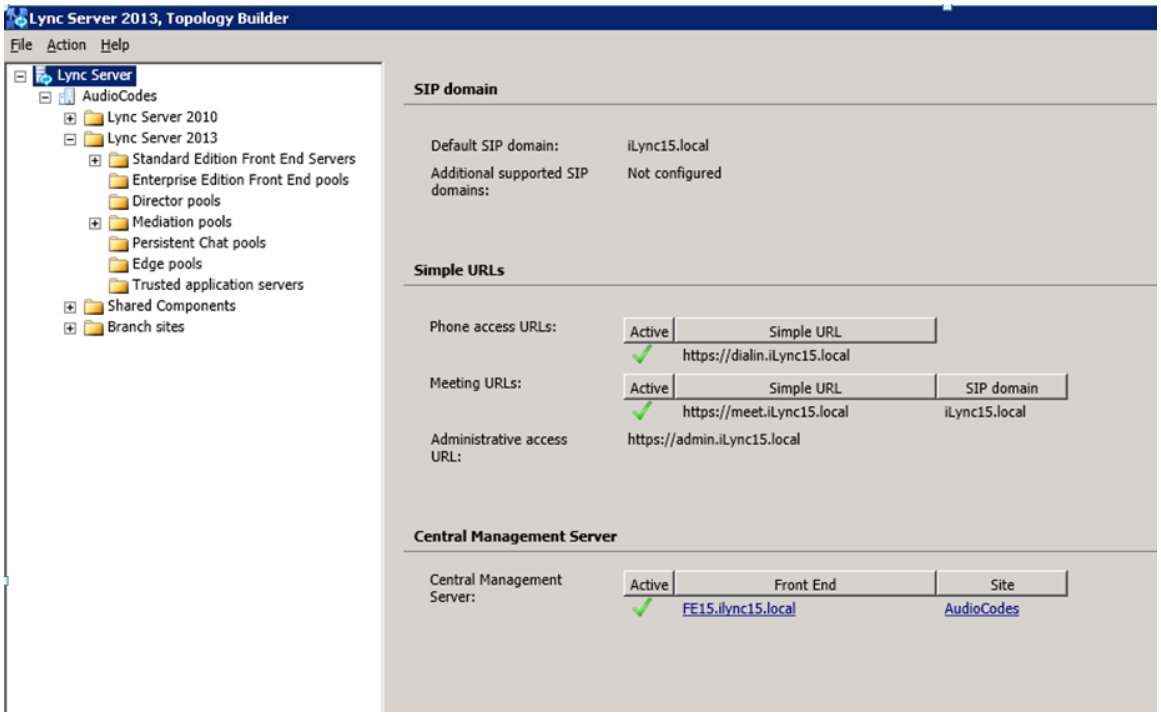
Figure 3-3: Save Topology Dialog Box



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

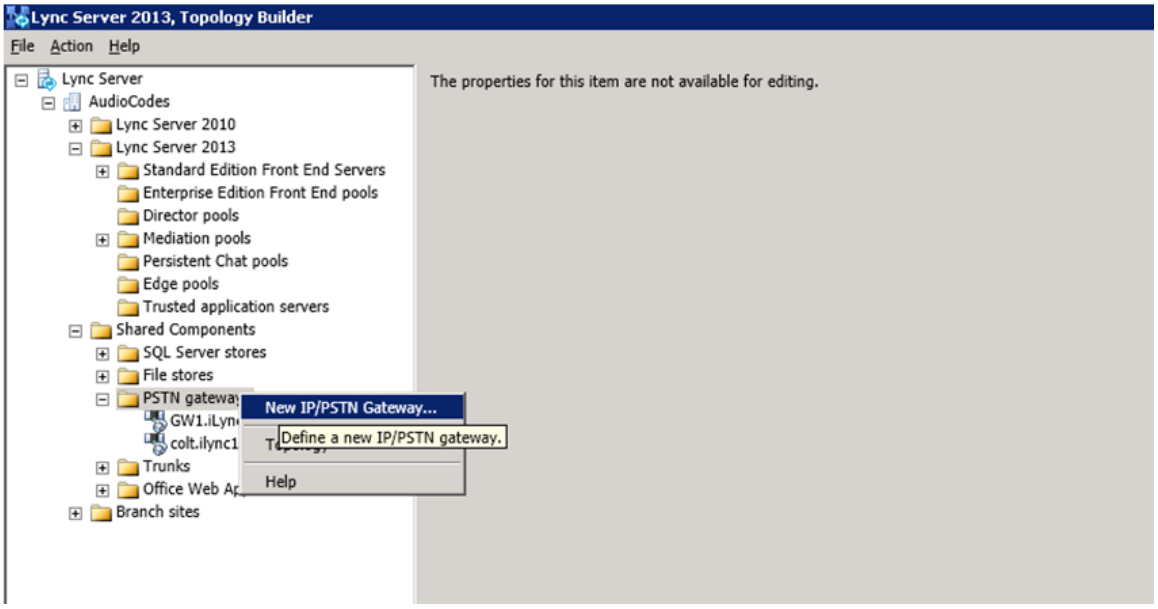
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



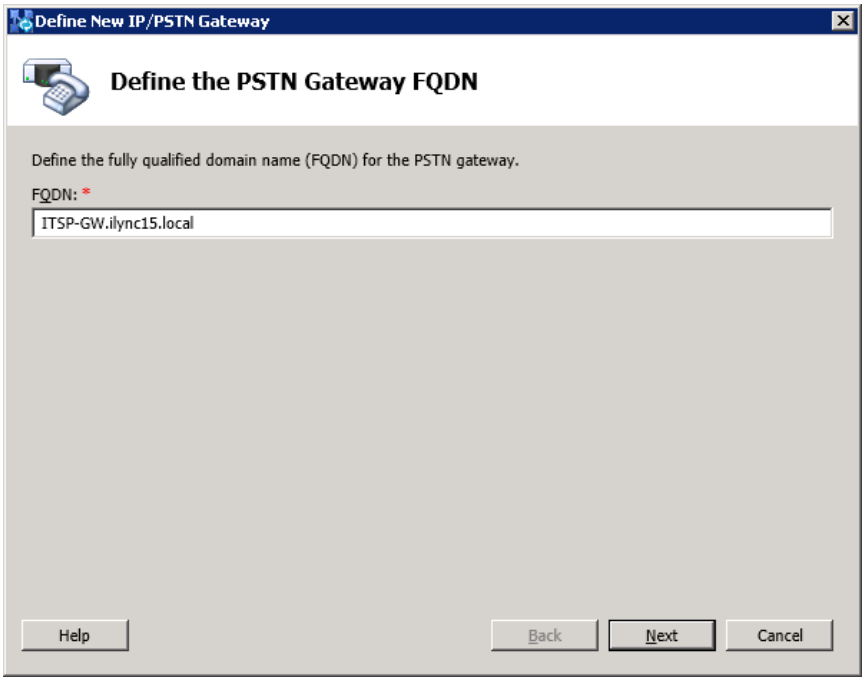
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



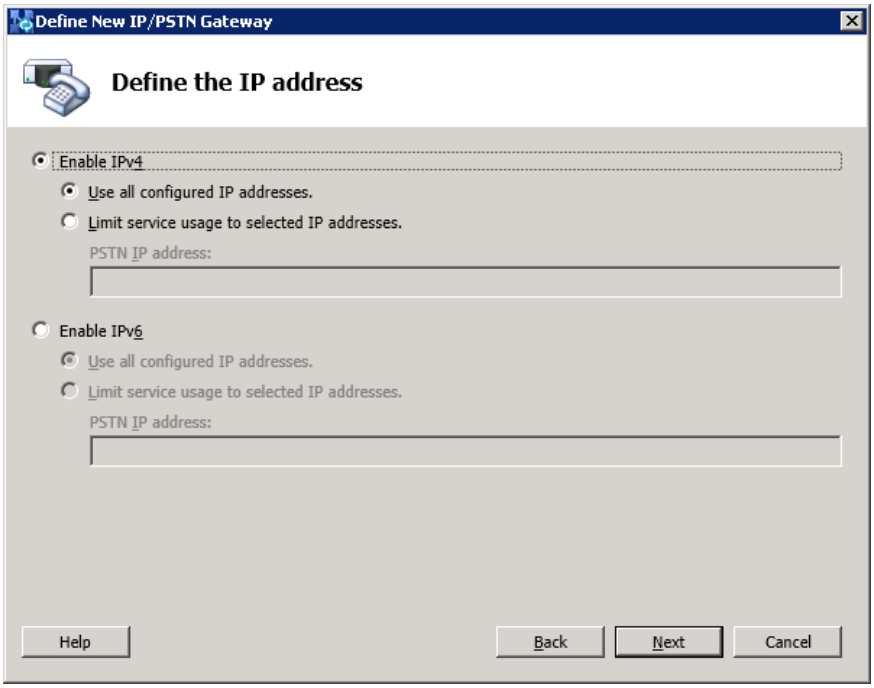
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP-GW.ilync15.local**). Update this FQDN in the relevant DNS record, and then click **Next**; the following is displayed:

Figure 3-7: Define the IP Address

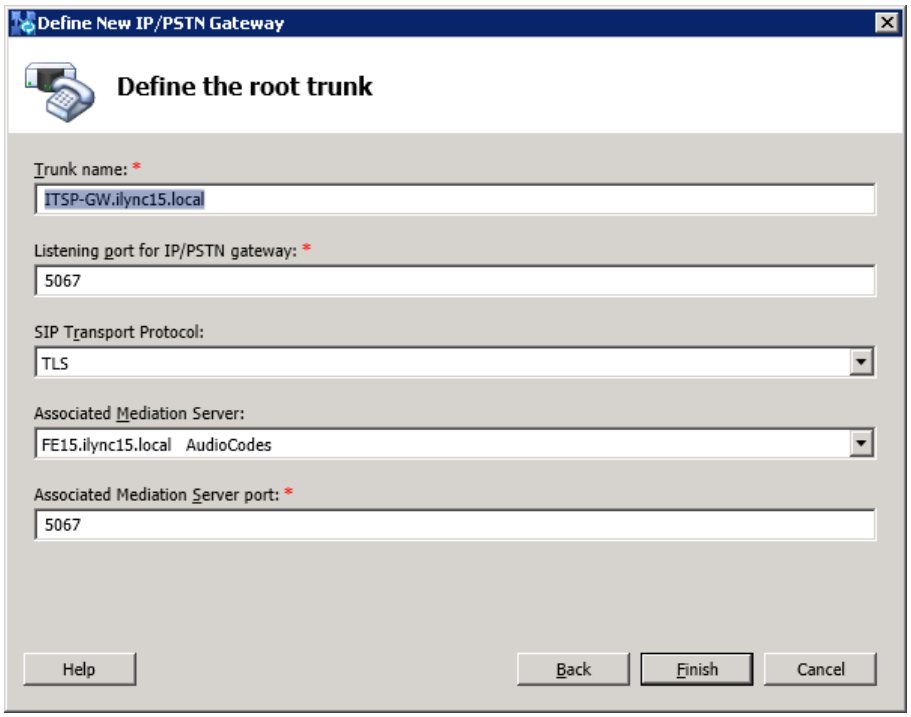


6. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.
7. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server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

Notes:

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

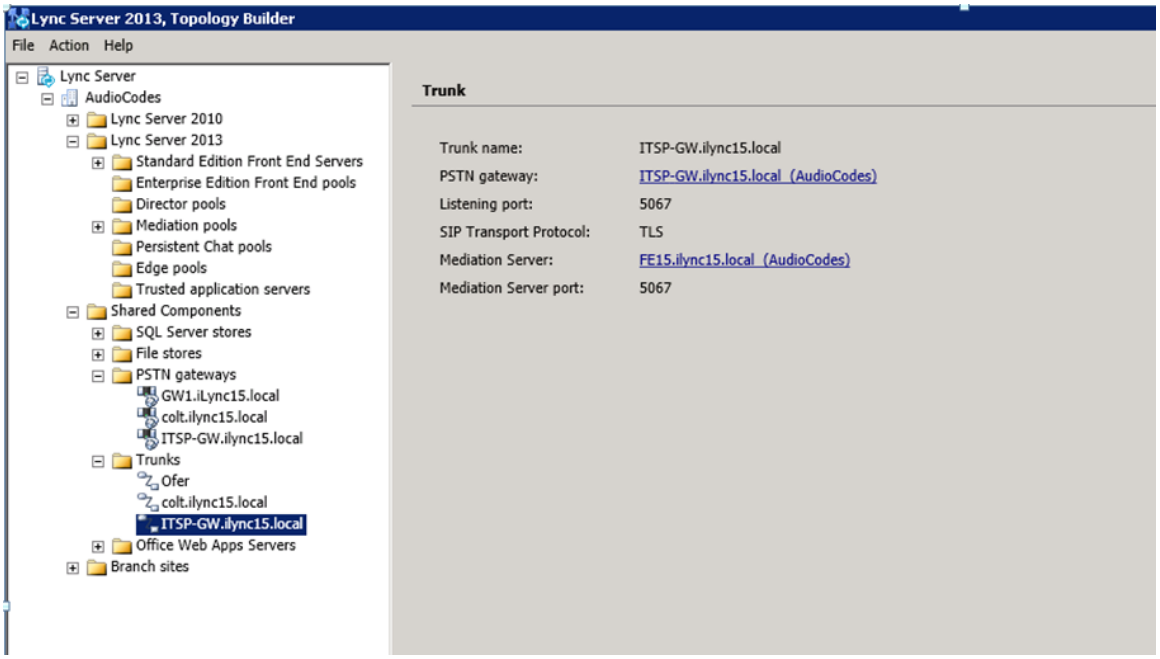
Figure 3-8: Define the Root Trunk



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

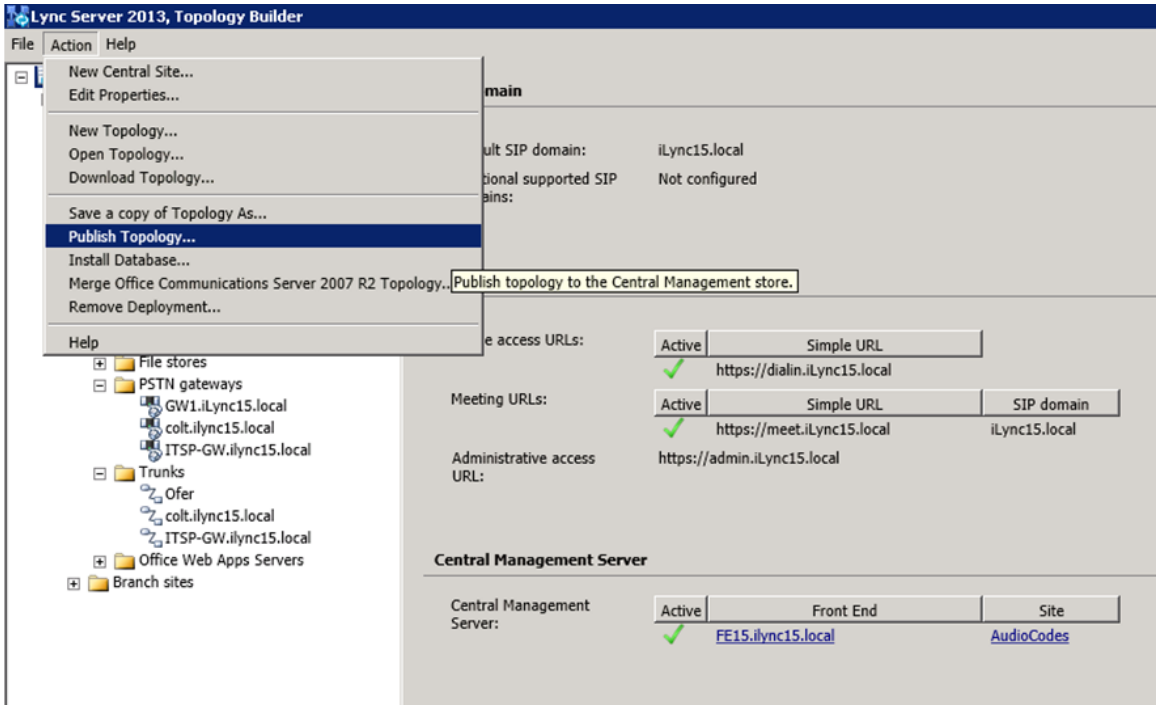
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



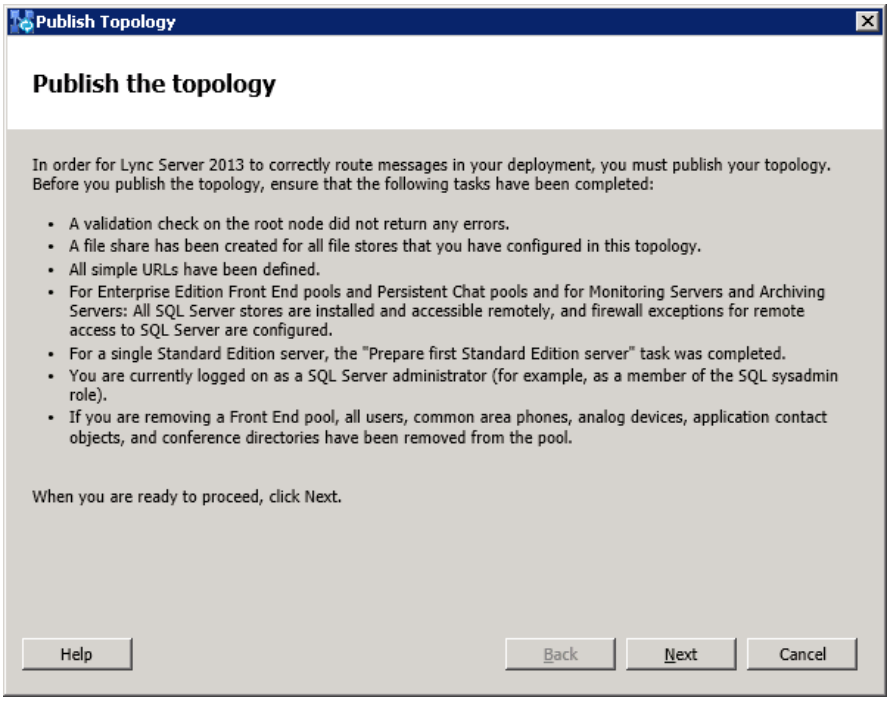
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



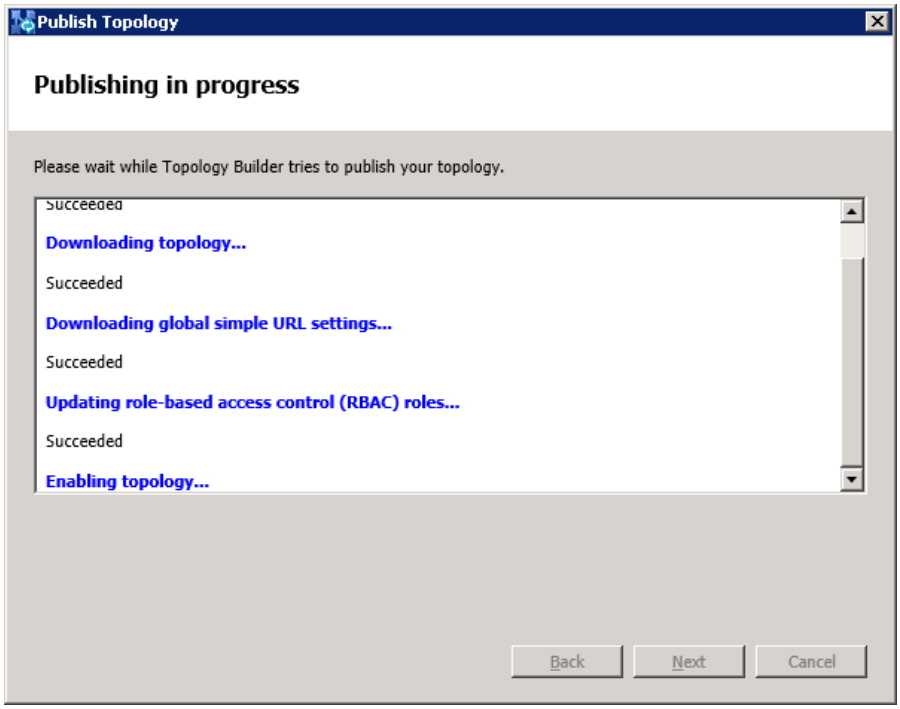
The following is displayed:

Figure 3-11: Publish the Topology



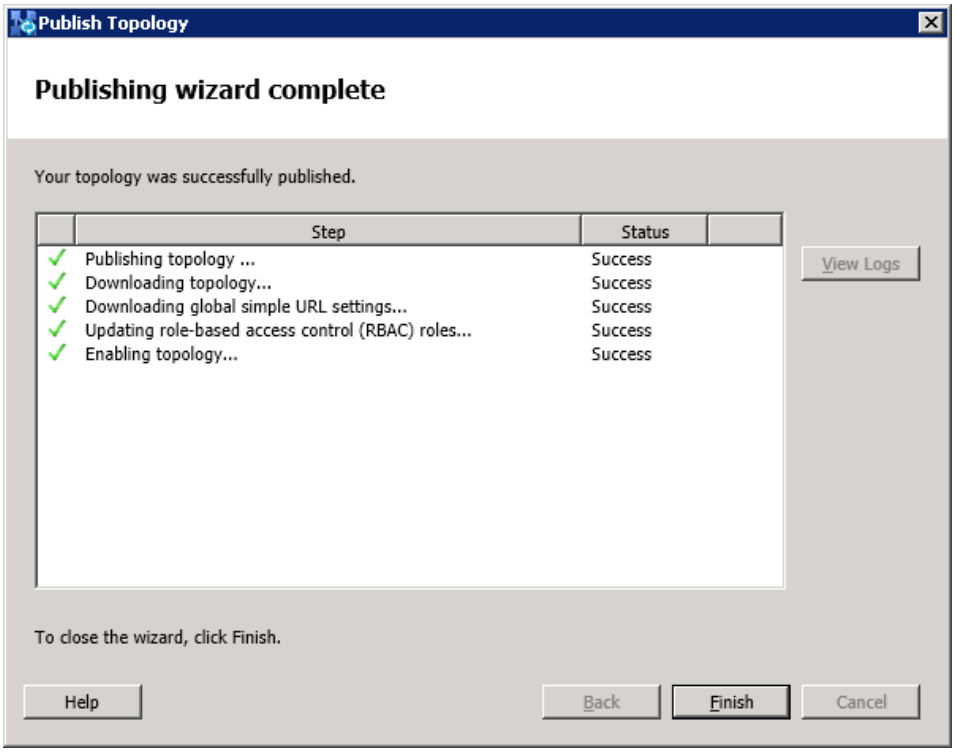
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. Click **Finish**.

3.2 Configuring the "Route" on Lync Server 2013

The procedure below describes how to configure a "Route" on the Lync Server 2013 and to associate it with the E-SBC PSTN gateway.

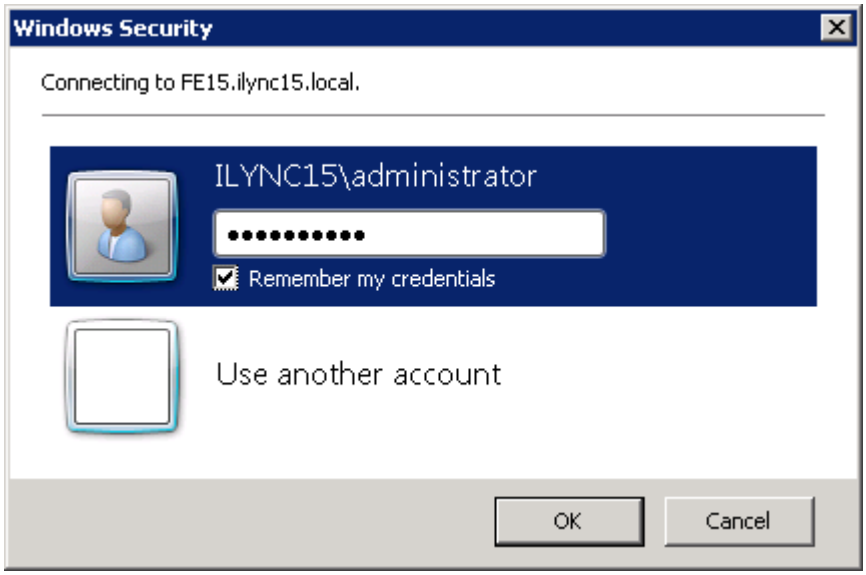
➢ **To configure the "route" on Lync Server 2013:**

1. Start the Microsoft Lync Server 2013 Control Panel (**Start** > **All Programs** > **Microsoft Lync Server 2013** > **Lync Server Control Panel**), as shown below:

Figure 3-14: Opening the Lync Server Control Panel

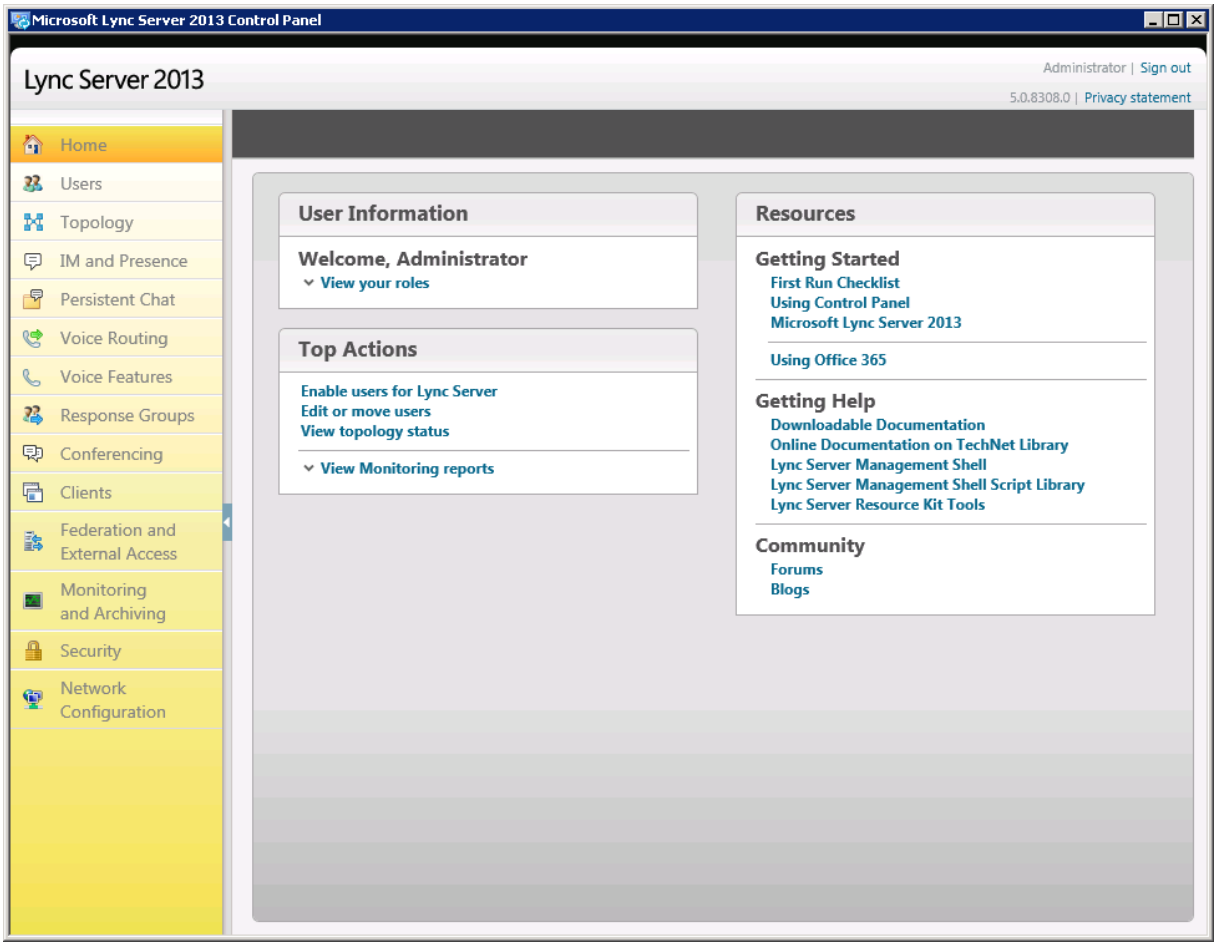
2. You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



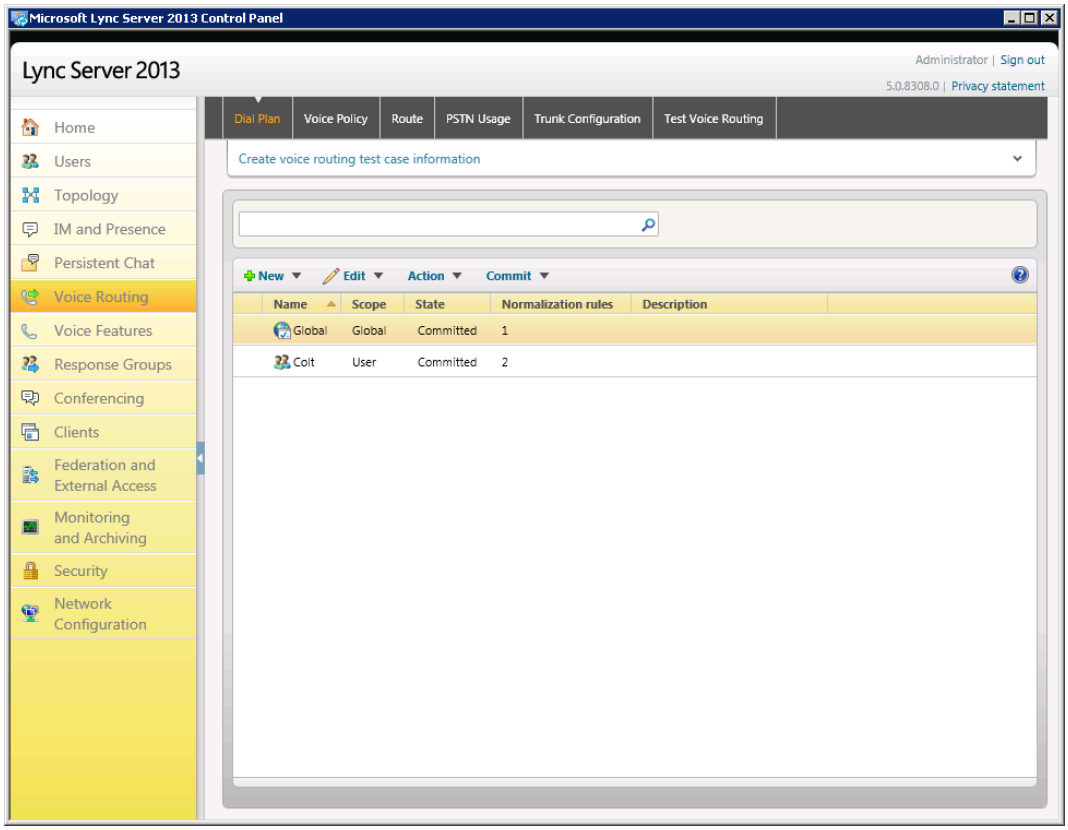
3. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



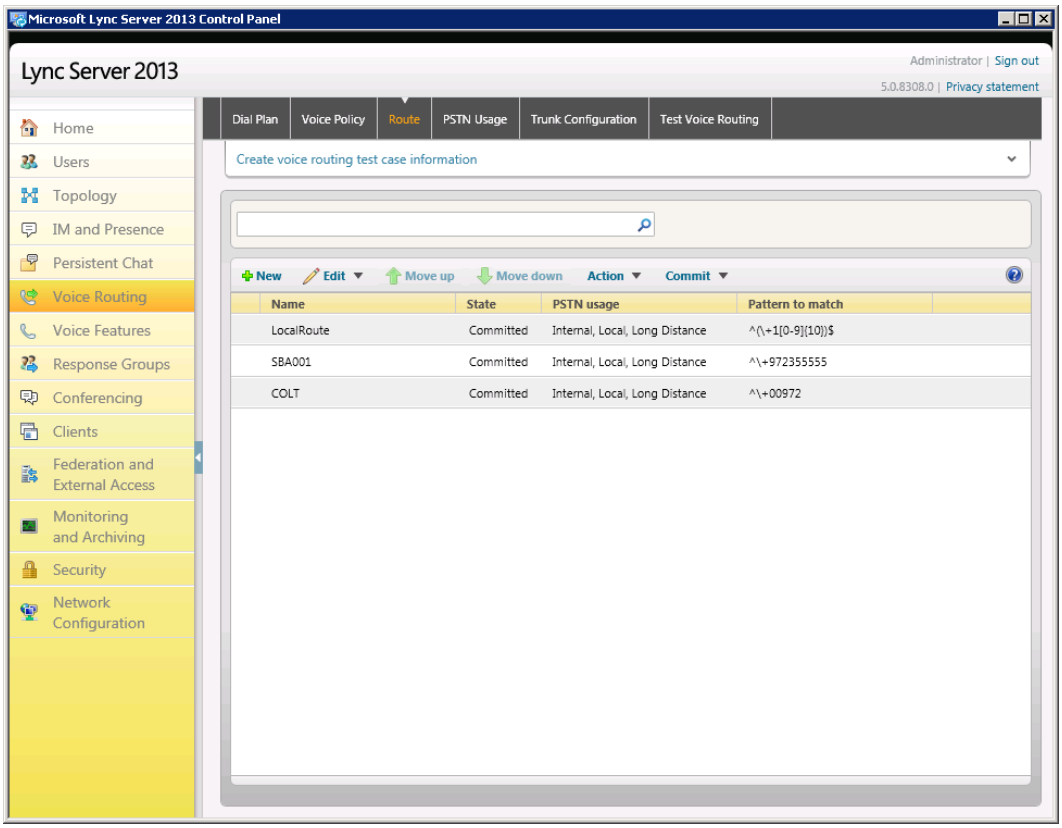
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



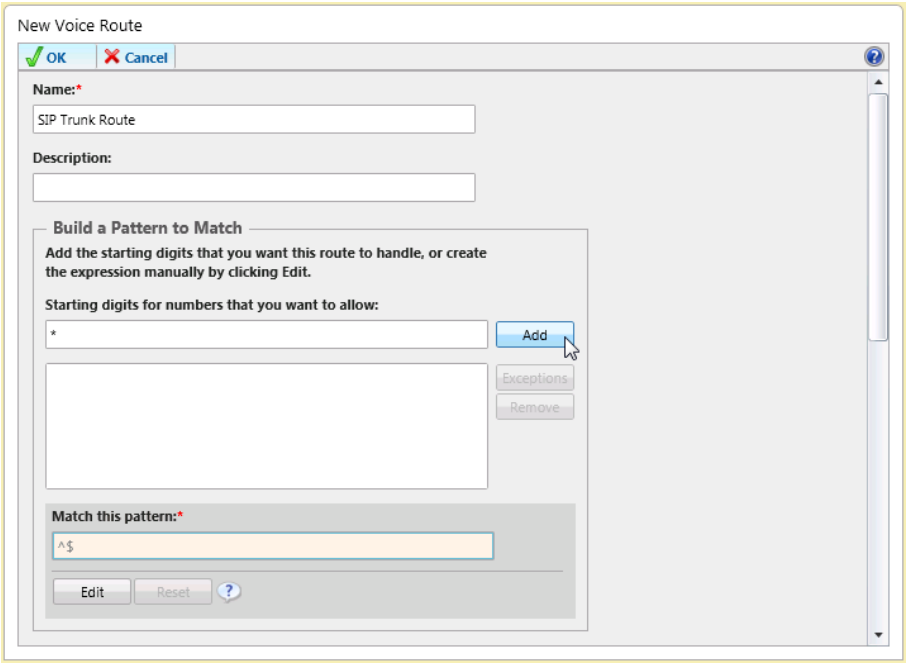
5. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



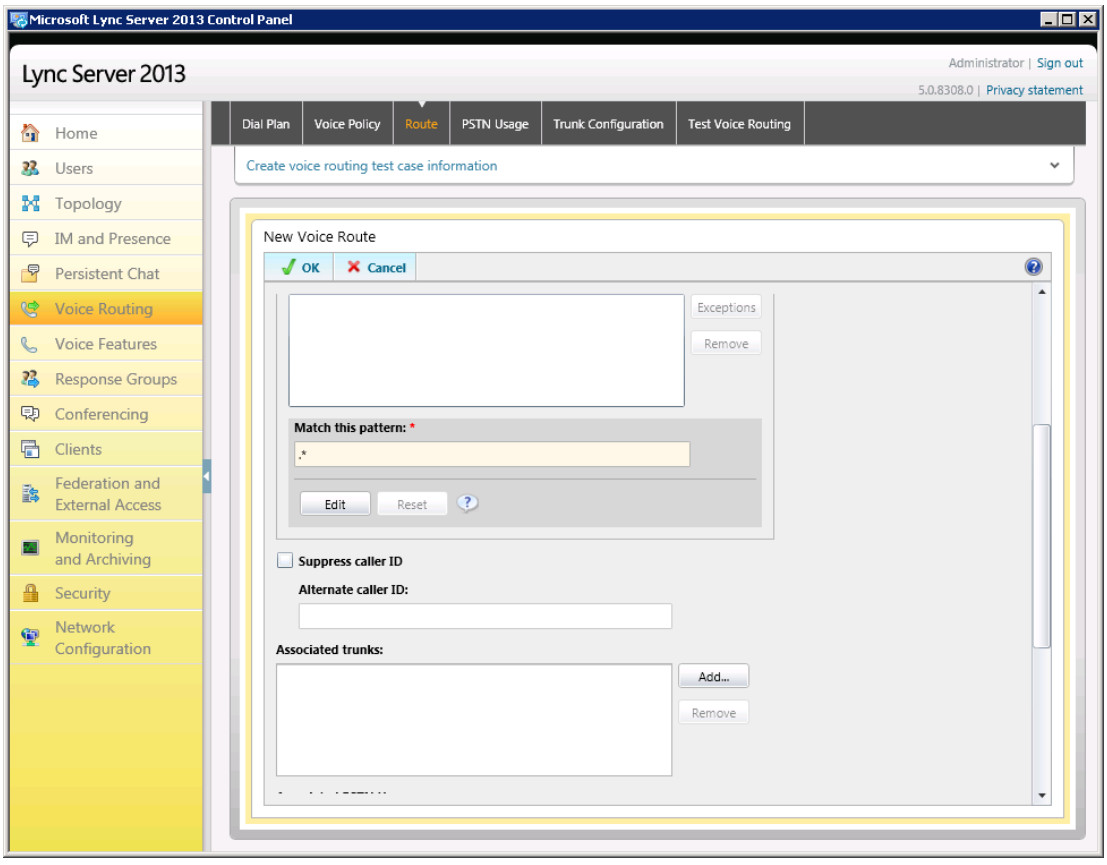
6. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



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

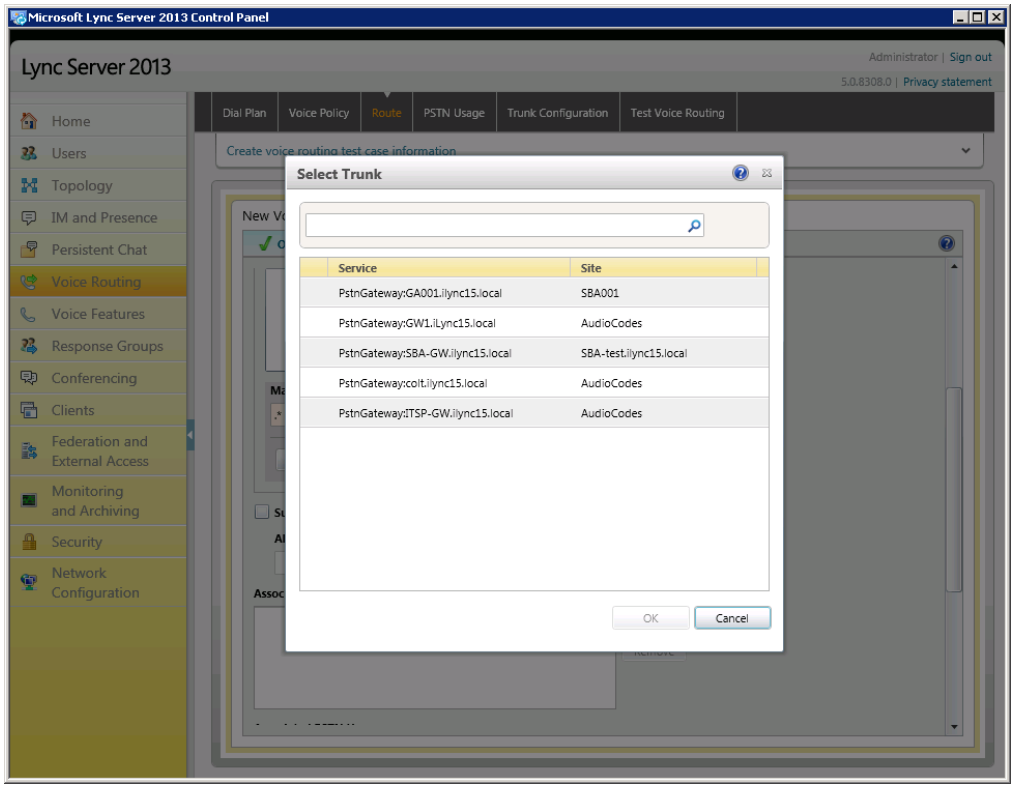
Figure 3-20: Adding New Trunk



9. Associate the route with the E-SBC Trunk that you created:

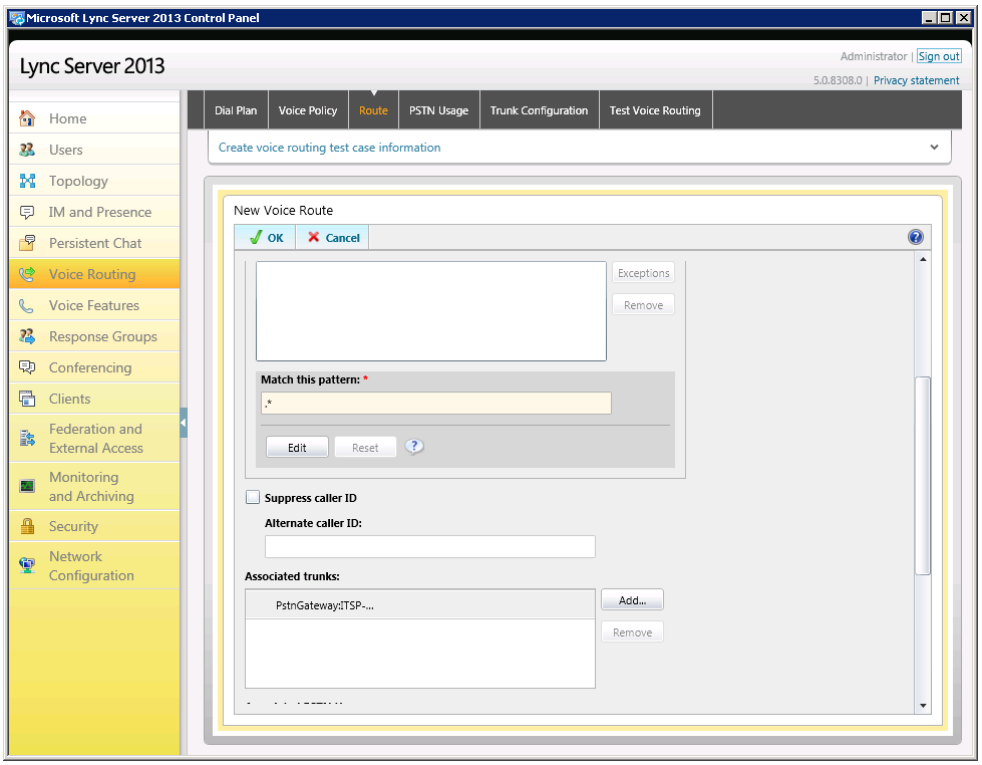
a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



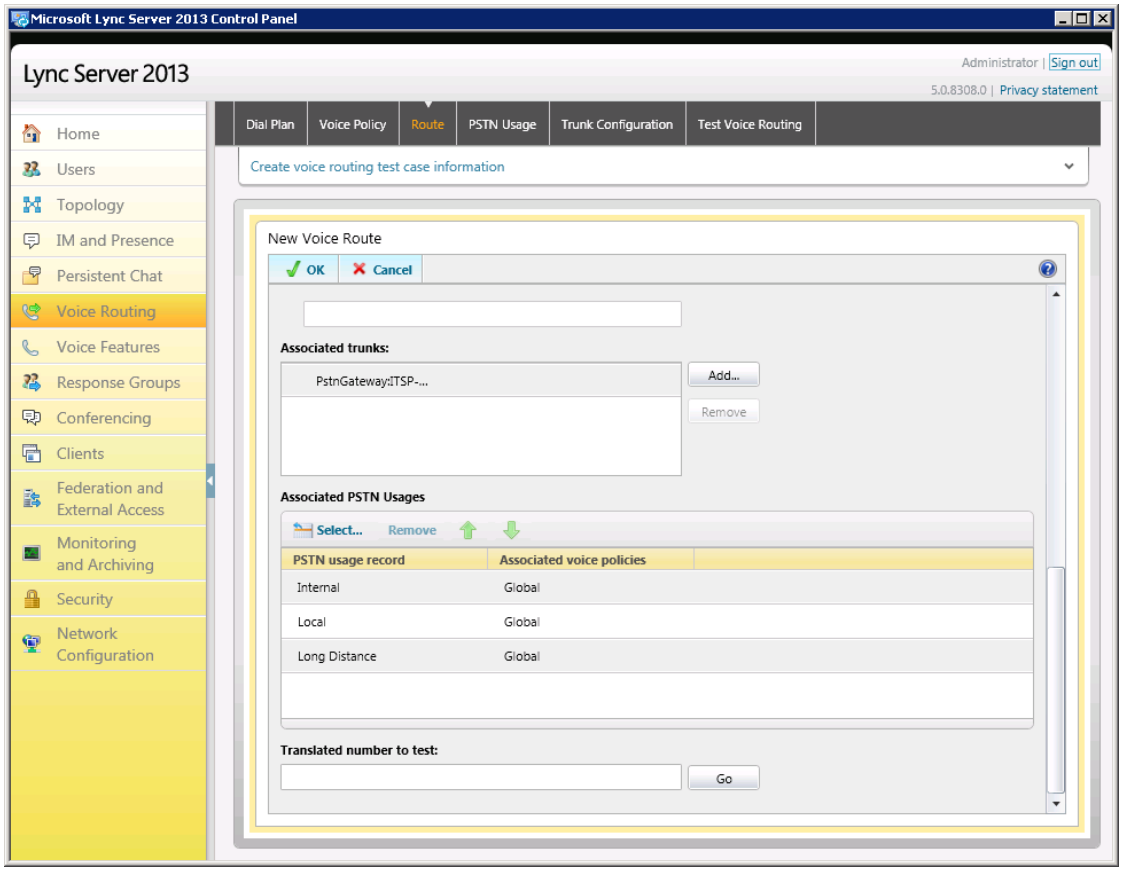
b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



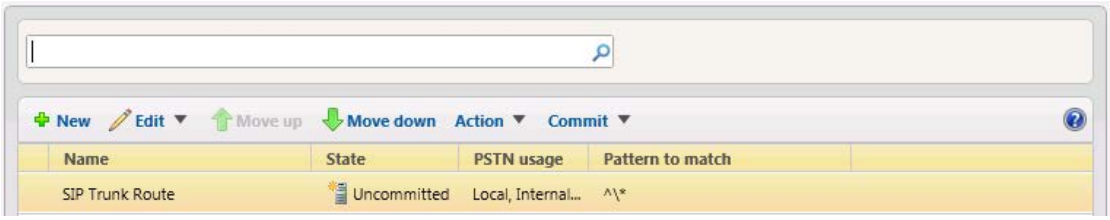
10. Associate a PSTN Usage to this route:
    a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



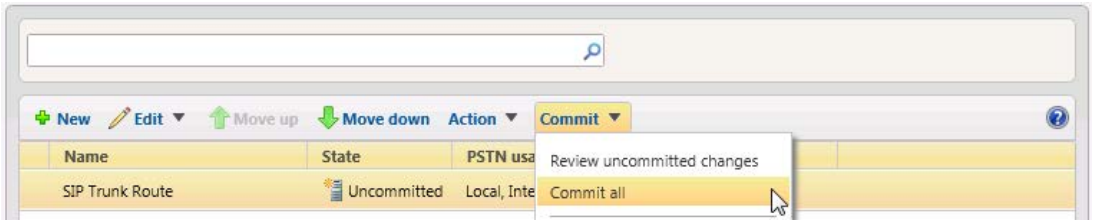
11. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



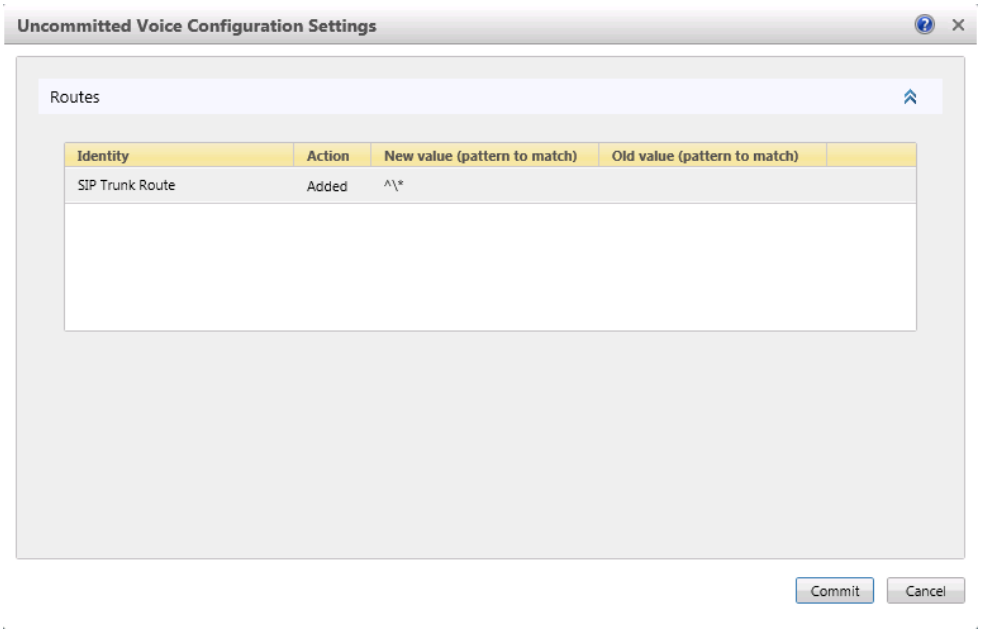
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



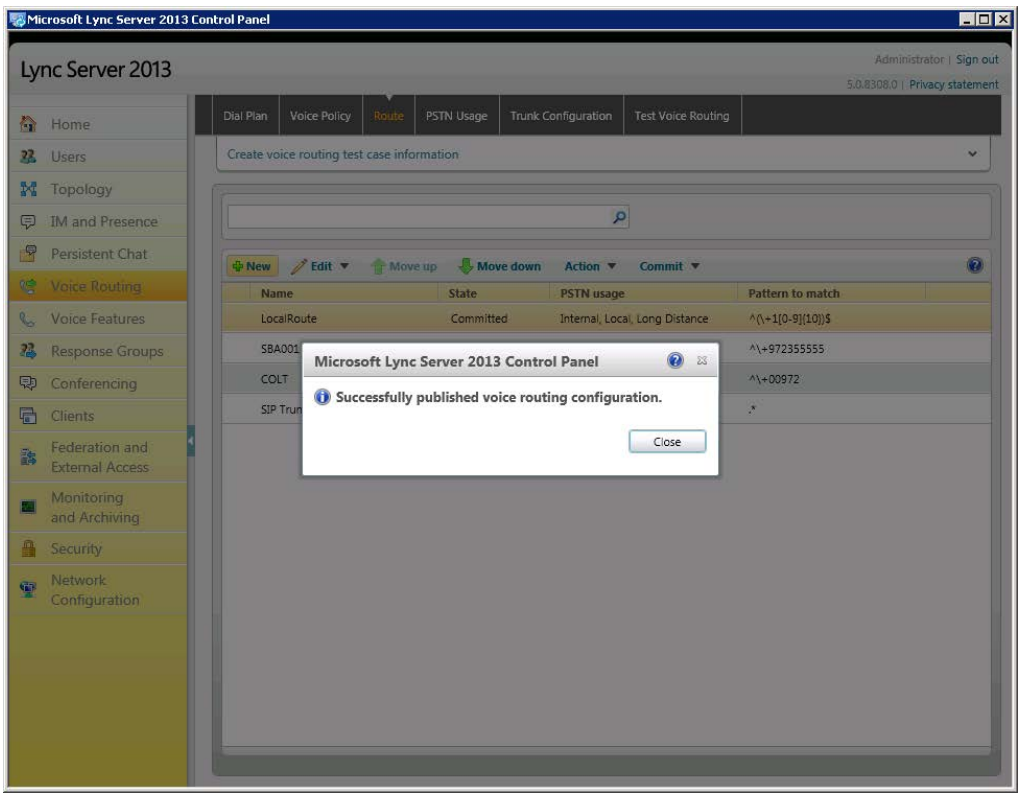
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



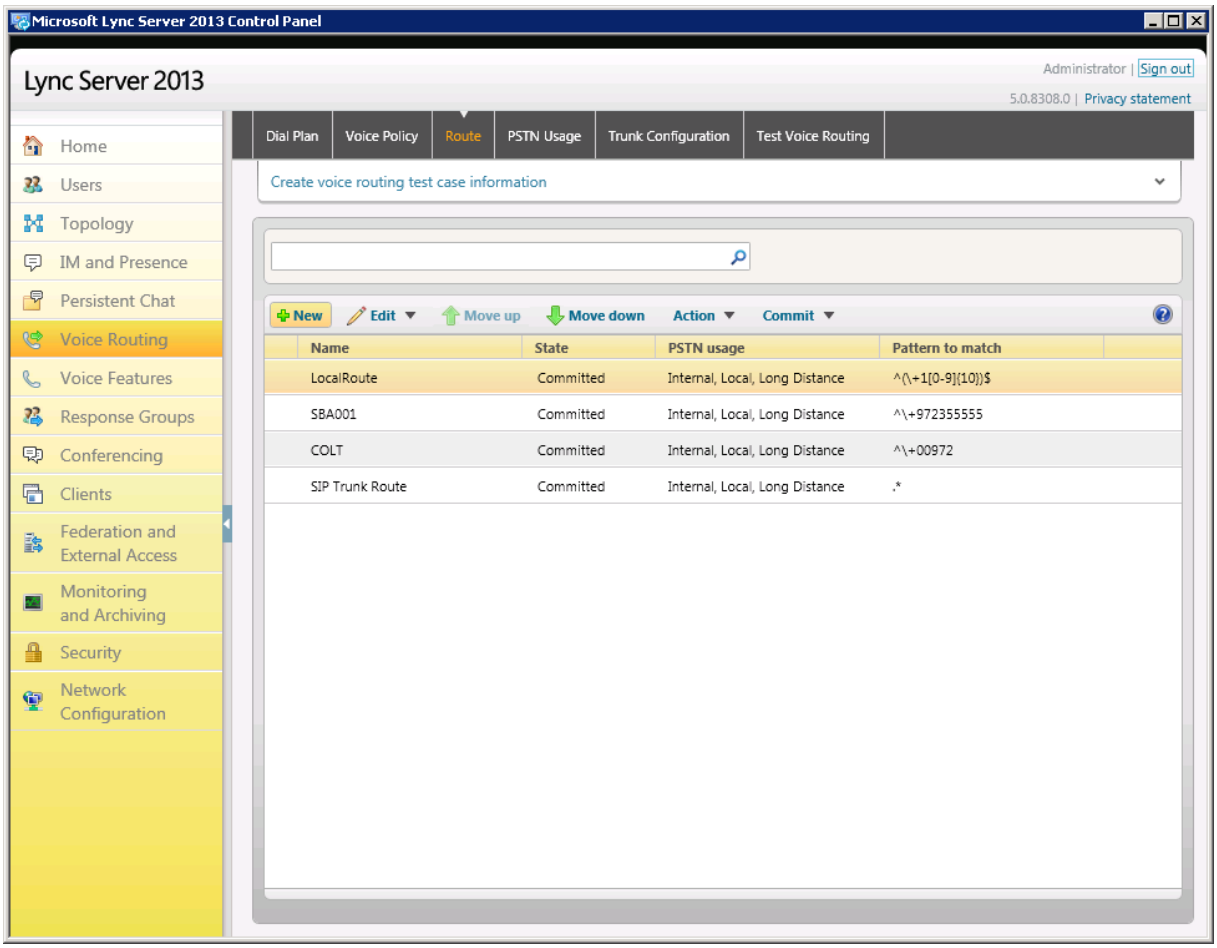
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirmation of Successful Voice Routing Configuration



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

Figure 3-28: Voice Routing Screen Displaying Committed Routes

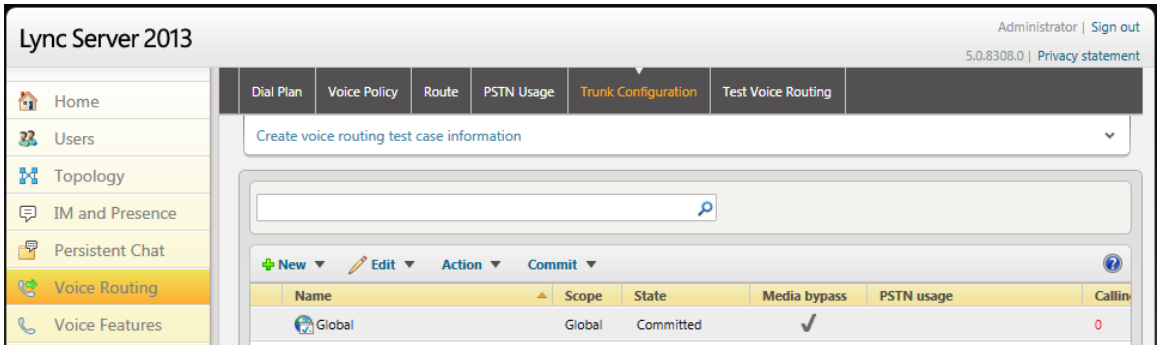


15. For ITSPs that implement a call identifier, continue with the following steps:

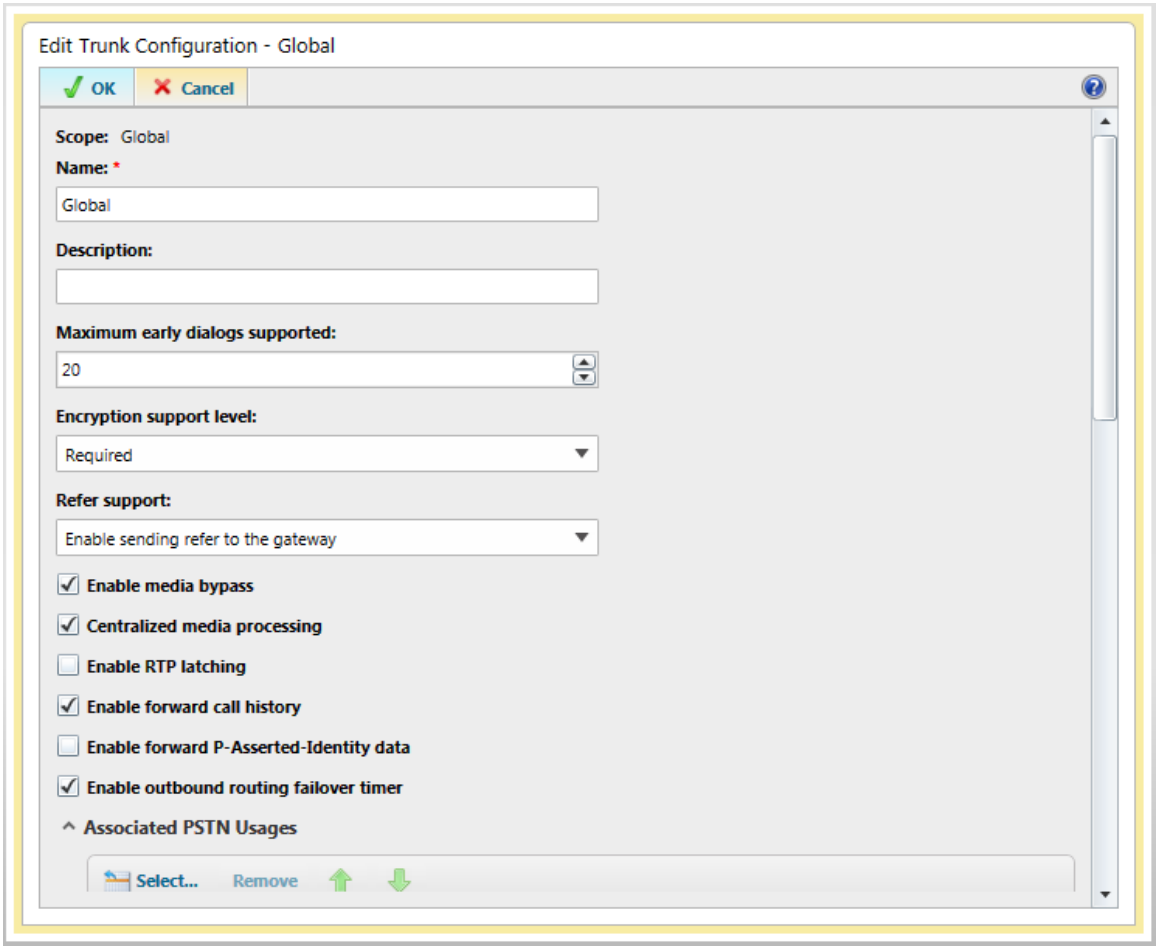
Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Lync user number). This ID is required by the SIP Trunk in the P-Asserted-Identity header. Using a Message Manipulation rule (see Section 4.14), the device adds this ID to the P-Asserted-Identity header in the sent INVITE message.

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

Figure 3-29: Voice Routing Screen – Trunk Configuration Tab



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



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

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

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and the SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

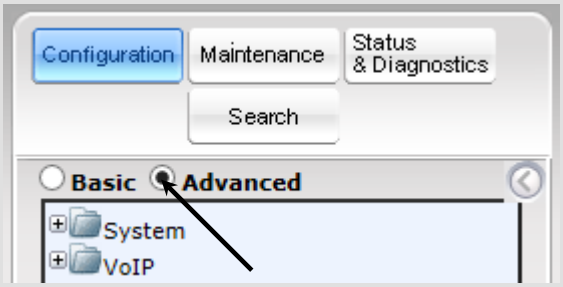
- E-SBC WAN interface - SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

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

Notes:

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

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



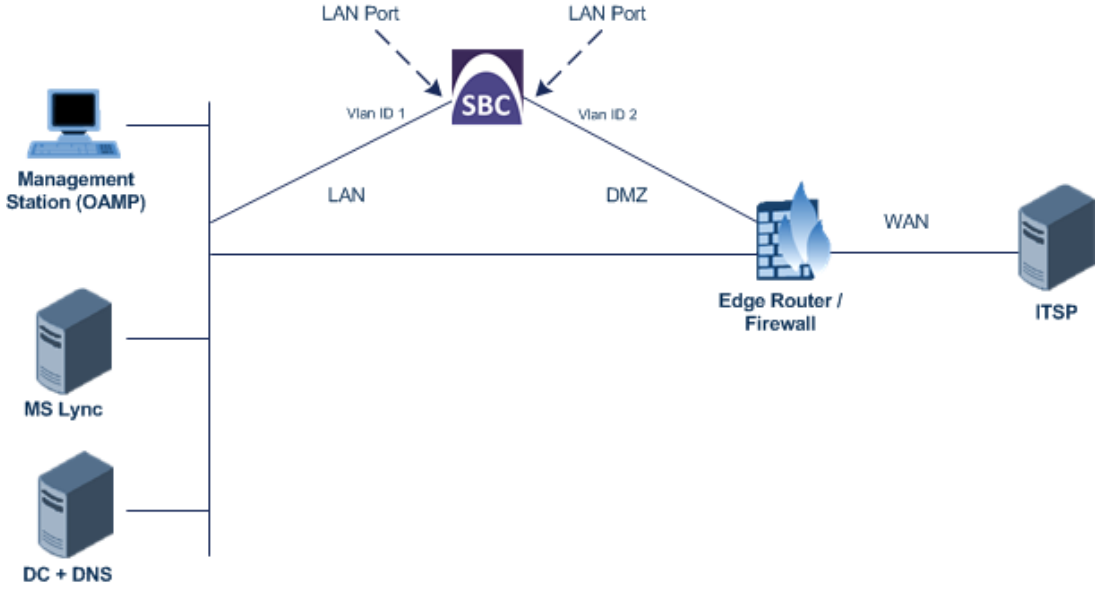
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: Configure IP Network Interfaces

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

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

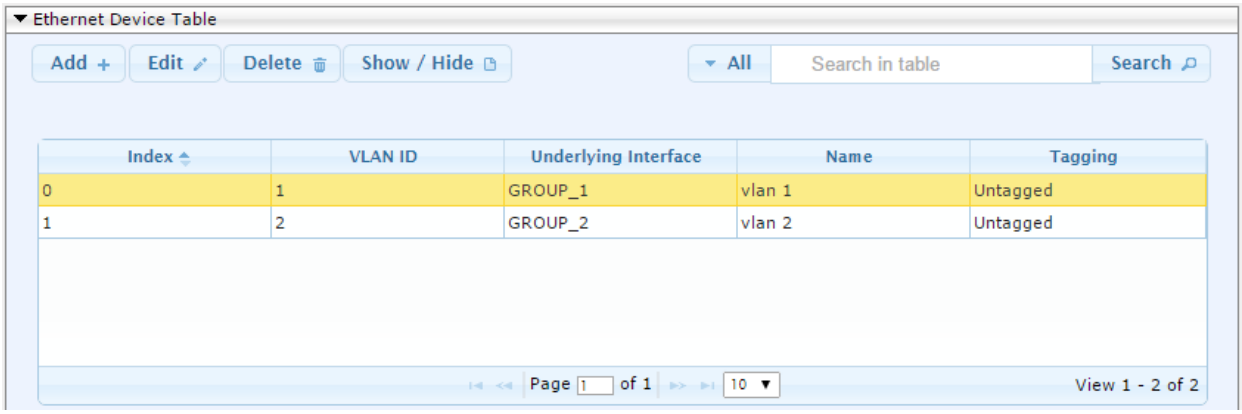
- LAN VoIP (assigned the name "Voice")
- WAN VoIP (assigned the name "Telus")

➢ **To configure the VLANs:**

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

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

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



4.1.2 Step 1b: Configure Network Interfaces

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

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

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

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Modify the existing LAN network interface:

a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
b. Configure the interface as follows:

Parameter	Value
IP Address	**10.15.45.32** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Default Gateway	**10.15.0.1**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.25.1**
Underlying Device	**vlan 1**

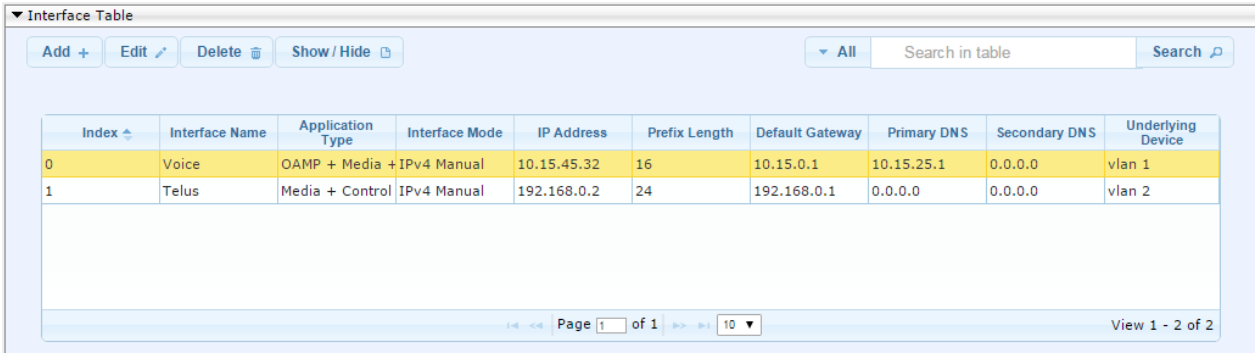
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**195.168.0.2** (WAN IP address)
Prefix Length	**24** (for 255.255.255.0)
Default Gateway	**192.168.0.1** (router's IP address)
Interface Name	**Telus**
Primary DNS Server IP Address	**0.0.0.0**
Secondary DNS Server IP Address	**0.0.0.0**
Underlying Device	**vlan 2**

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

The configured IP network interfaces are shown below:

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



4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-4: Enabling SBC Application

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.16).

4.3 Step 3: Configure Media Realms

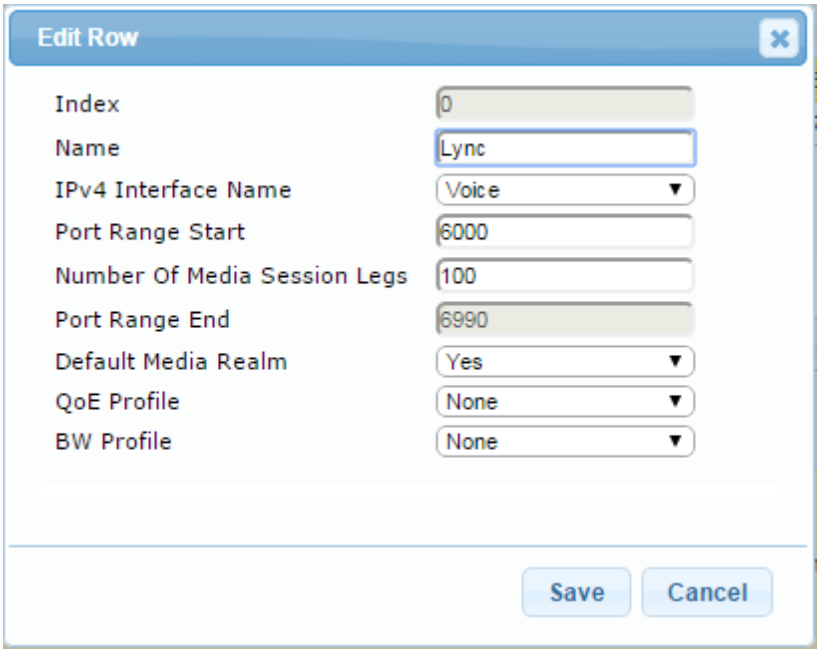
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

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

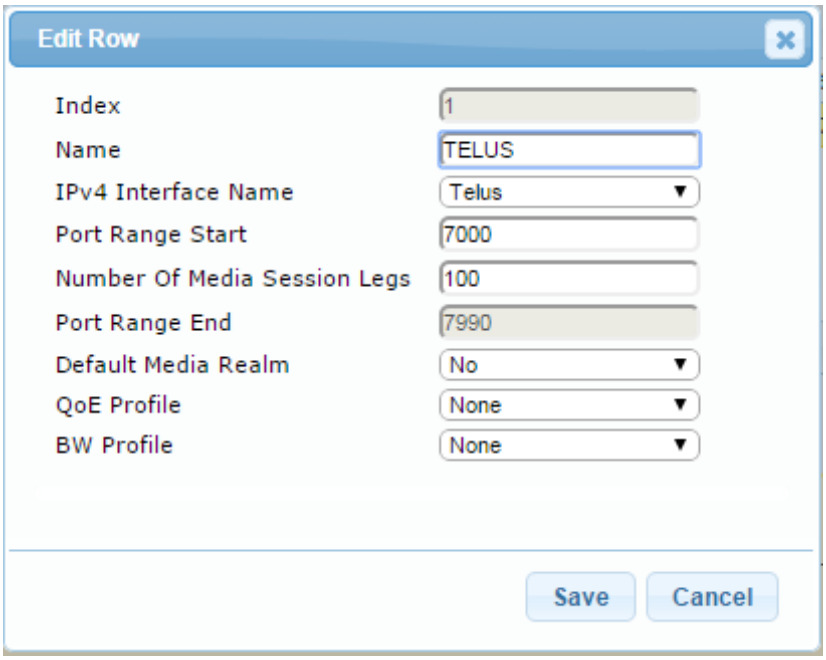
Figure 4-5: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

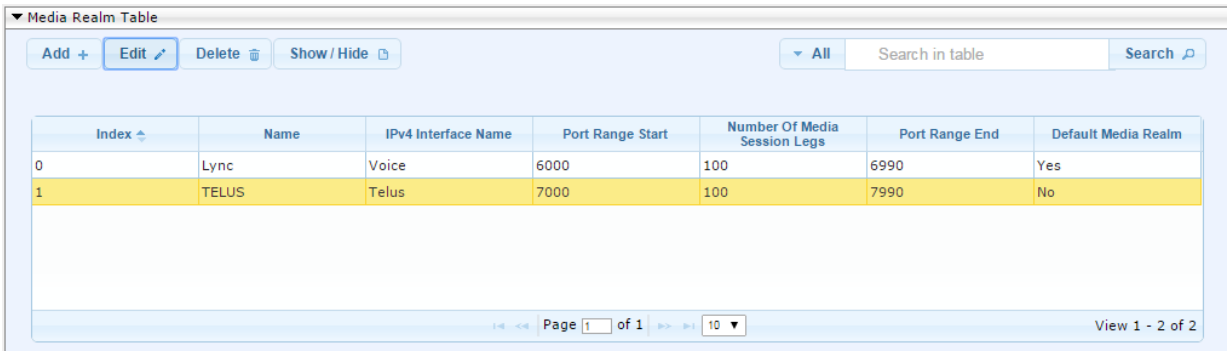
Parameter	Value
Index	**1**
Media Realm Name	**TELUS** (arbitrary name)
IPv4 Interface Name	**Telus**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

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



4.4 Step 4: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

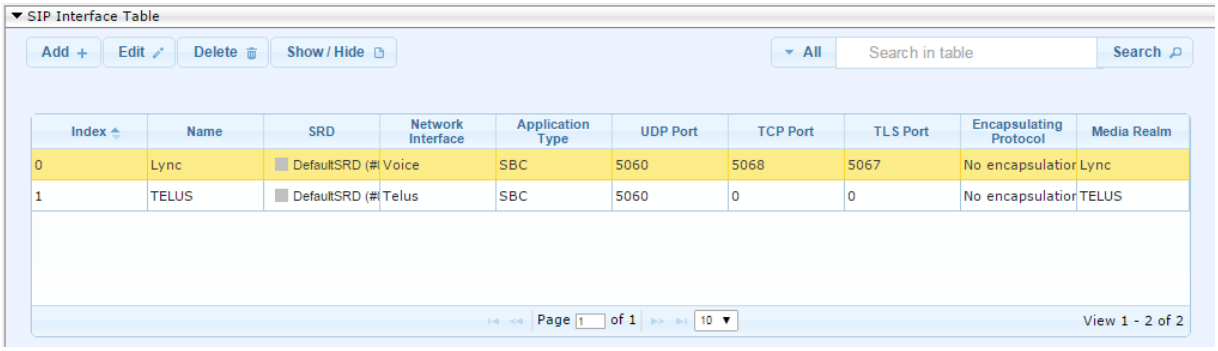
Parameter	Value
Index	**0**
Interface Name	**Lync** (see Note below)
Network Interface	**Voice**
Application Type	**SBC**
UDP Port (supporting FAX ATA)	**5060**
TCP Port (set to 0 if using TLS)	**5068**
TLS Port (set to 0 if using TCP)	**5067**
Media Realm	**Lync**

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	**1**
Interface Name	**TELUS** (see Note below)
Network Interface	**Telus**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	**0 or 5061** (For Internet Registration-based configuration)
Media Realm	**TELUS**

The configured SIP Interfaces are shown in the figure below:

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



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

4.5 Step 5: Configure Proxy Sets

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

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

- Microsoft Lync Server 2013
- Telus' SIP Trunk

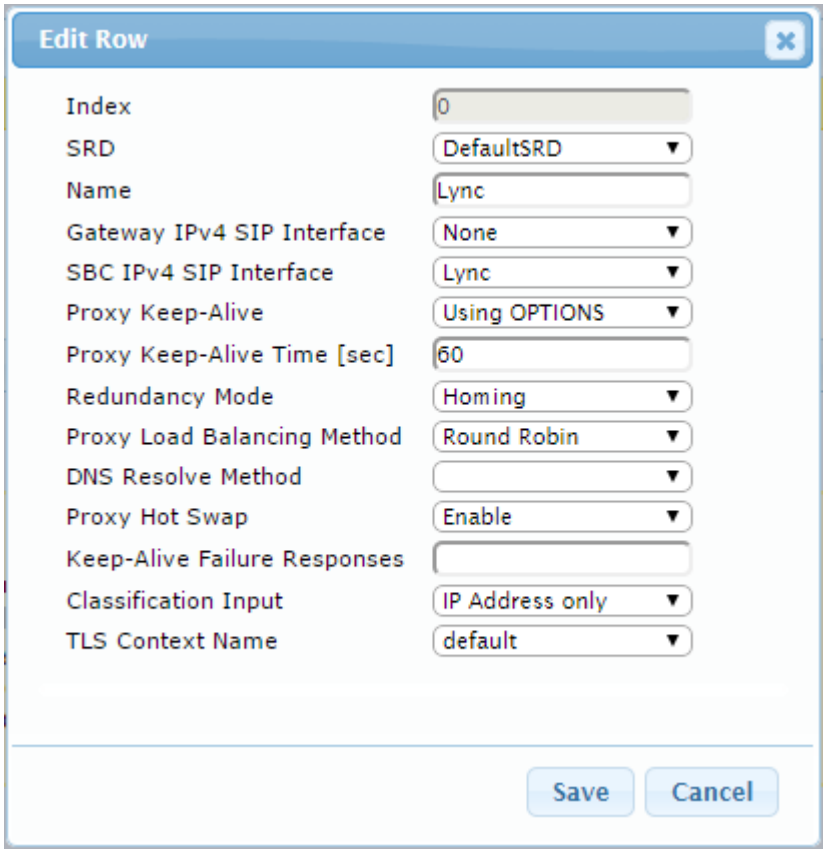
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the Lync Server 2013. You can use the default Proxy Set (Index 0), but modify it as shown below:

Parameter	Value
Proxy Set ID	**0**
Proxy Name	**Lync** (see Note on page 38)
SBC IPv4 SIP Interface	**Lync**
Proxy Keep Alive	**Using Options**
Redundancy Mode	**Homing**
Load Balancing Method	**Round Robin**
Proxy Hot Swap	**Enable**
TLS Context Name	**default**

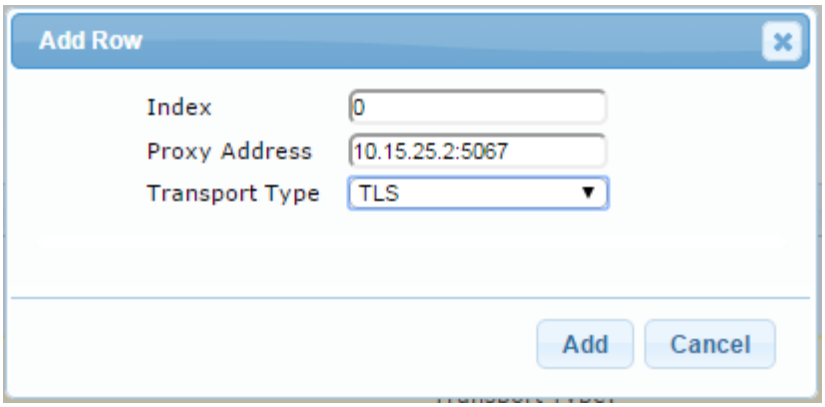
Figure 4-9: Configuring Proxy Set for Microsoft Lync Server 2013



3. Configure a Proxy Address Table for Proxy Set for Lync Server 2013:
   a. Go to Configuration tab > VoIP menu > VoIP Network > Proxy Sets Table > Proxy Address Table.

Parameter	Value
Index	**0**
Proxy Address	**10.15.25.2:5067** (Lync Server 2013 IP address / FQDN and destination port)
Transport Type	**TLS**

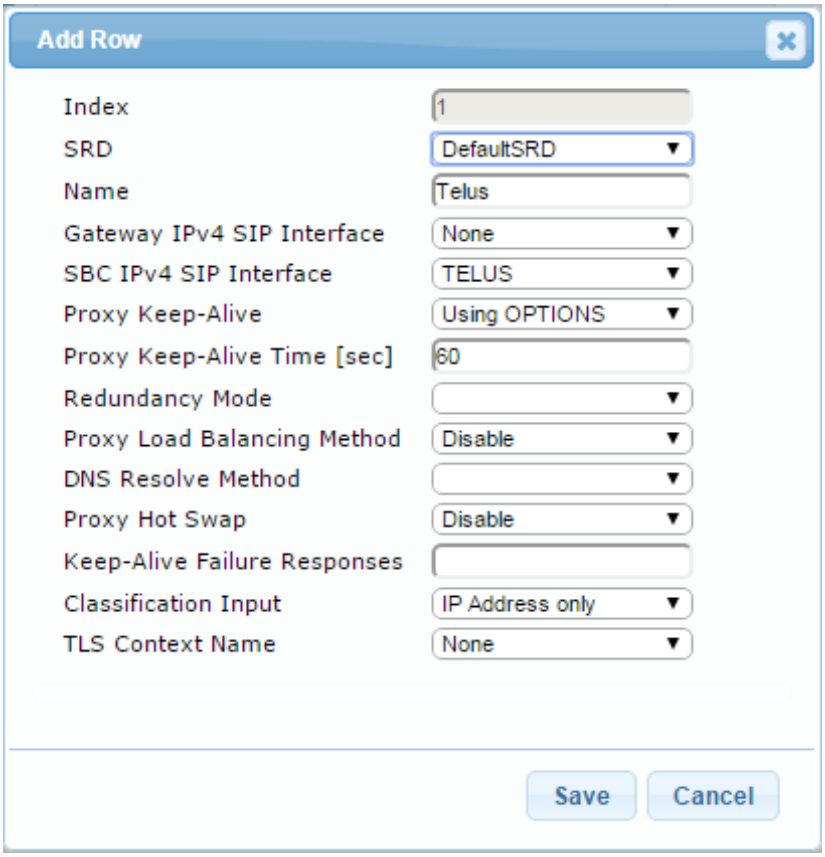
Figure 4-10: Configuring Proxy Address for Microsoft Lync Server 2013



4. Configure a Proxy Set for the SIP Trunk:

Parameter	Value
Proxy Set ID	**1**
Proxy Name	**Telus** (see Note on page 38)
SBC IPv4 SIP Interface	**TELUS**
Proxy Keep Alive	**Using Options**

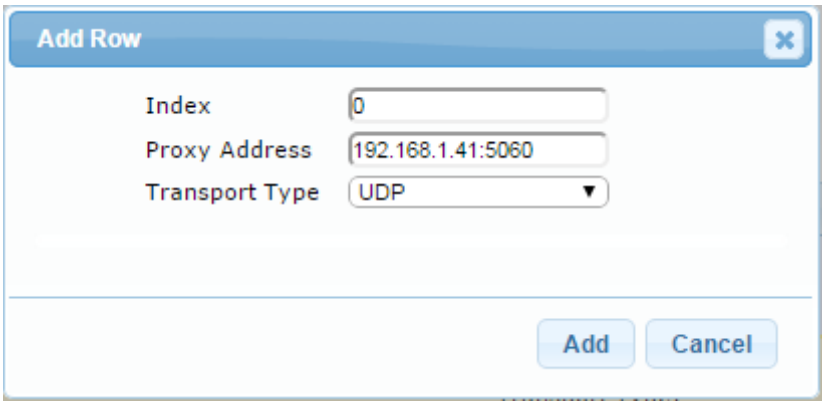
Figure 4-11: Configuring Proxy Set for Telus' SIP Trunk



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	**192.168.1.41:5060** (IP address / FQDN and destination port)
Transport Type	**UDP** (or TCP or TLS according to ITSP requirement)

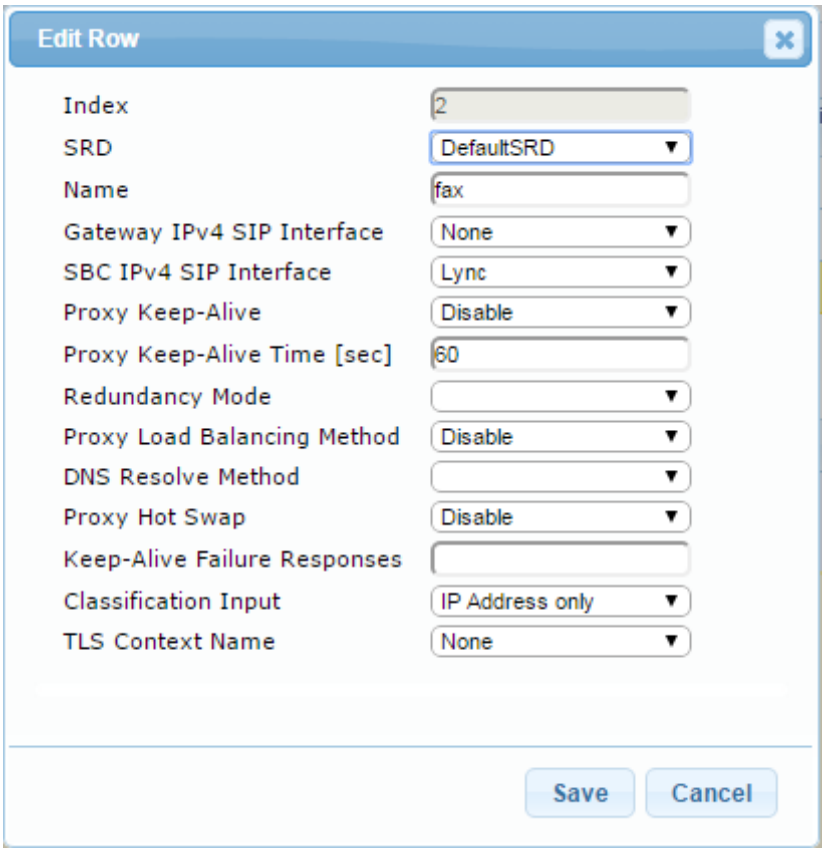
Figure 4-12: Configuring Proxy Address for



5. Configure a Proxy Set for the FAX supporting ATA:

Parameter	Value
Proxy Set ID	**2**
Proxy Name	**fax** (see Note on page 38)
SBC IPv4 SIP Interface	**Lync**

Figure 4-13: Configuring Proxy Set for SIP Trunk



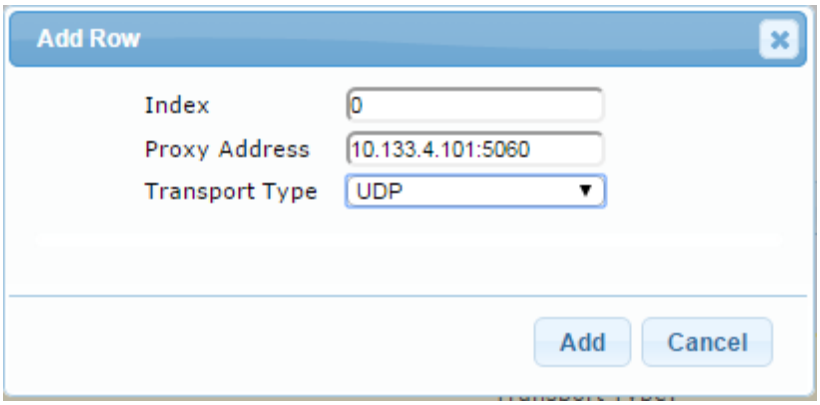
c. Configure a Proxy Address Table for Proxy Set 2:

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

Parameter	Value

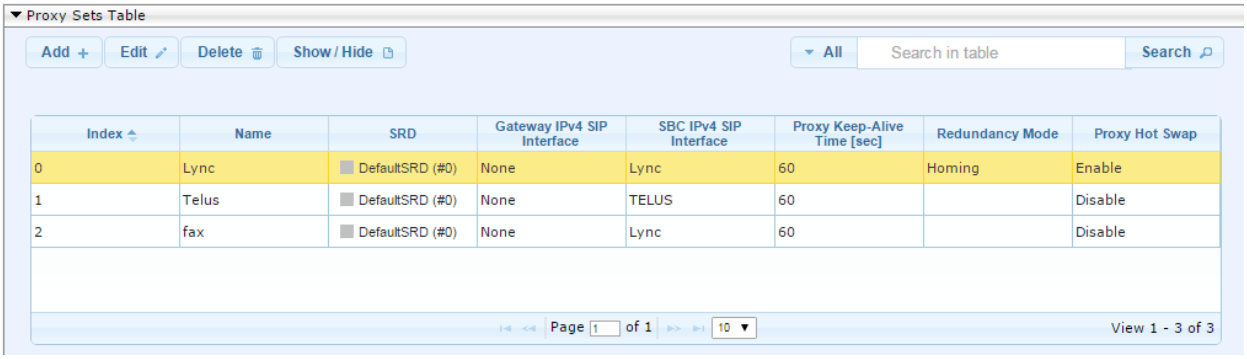
Index	**0**
Proxy Address	**10.133.4.101:5060** (IP address / FQDN and destination port)
Transport Type	**UDP**

Figure 4-14: Configuring Proxy Address for



The configured Proxy Sets are shown in the figure below:

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



4.6 Step 6: Configure IP Profiles

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

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

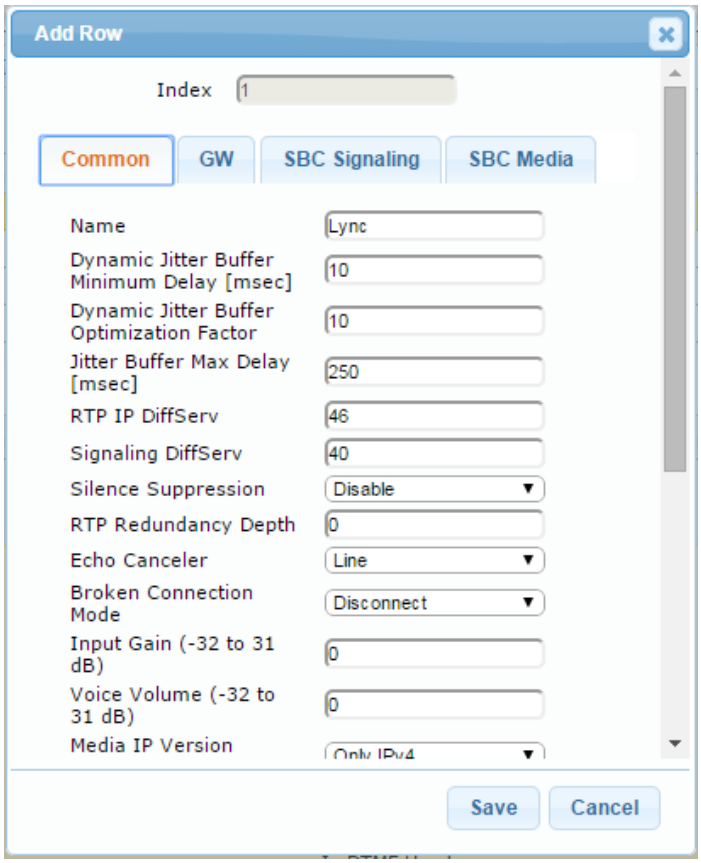
- Microsoft Lync Server 2013 - to operate in secure mode using SRTP and TLS
- SIP trunk - to operate in non-secure mode using RTP and UDP

➢ **To configure IP Profile for the Lync Server 2013:**

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	**Lync** (see Note on page 38)
Symmetric MKI	**Enable**
MKI Size	**1**
Reset SRTP State Upon Re-key	**Enable**
Generate SRTP keys mode:	**Always**

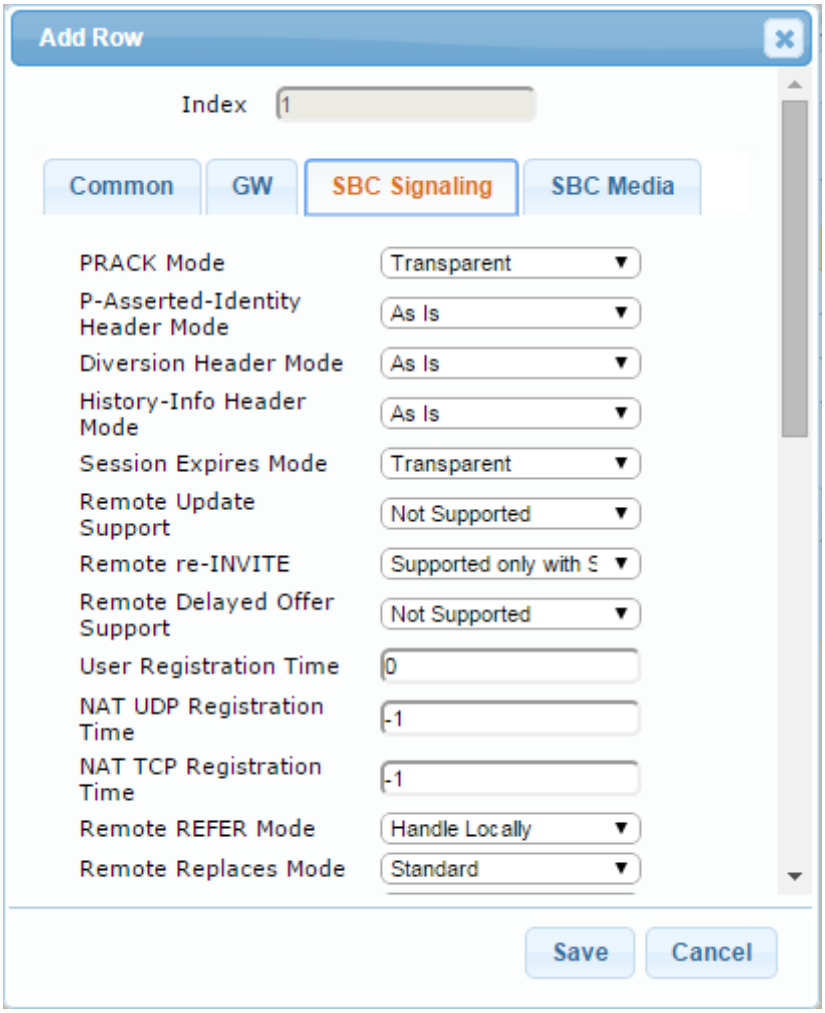
Figure 4-16: Configuring IP Profile for Lync Server 2013 – Common Tab



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

Parameter	Value
Remote Update Support	**Not Supported**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
Remote REFER Mode	**Handle Locally** (required, as Lync Server 2013 does not support receipt of SIP REFER)
Remote 3xx Mode	**Handle Locally** (required, as Lync Server 2013 does not support receipt of SIP 3xx responses)
Remote Early Media RTP Detection Behavior	**By Media** (required, as Lync Server 2013 does not send RTP immediately to remote side when it sends a SIP 18x response)
Remote Hold Format	**Send Only**

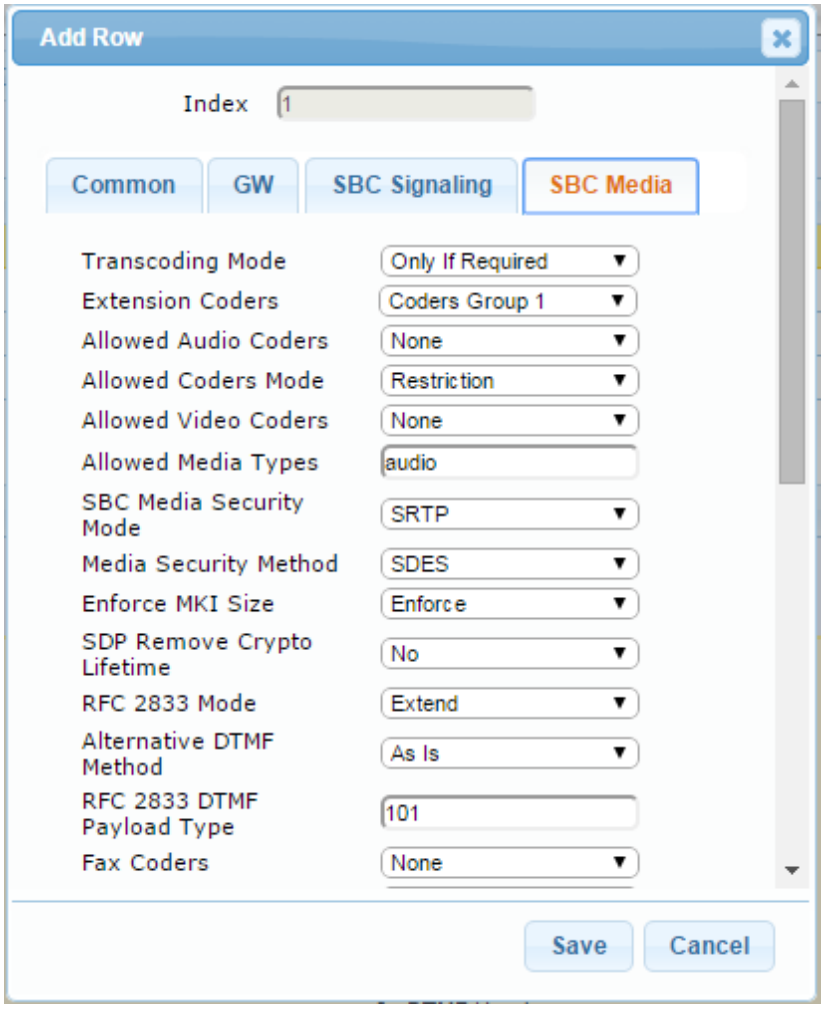
Figure 4-17: Configuring IP Profile for Lync Server 2013 – SBC Signaling Tab



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

Parameter	Value
Extension Coders Group ID	**Coders Group 1**
Allowed Media Types	**audio**
SBC Media Security Mode	**SRTP**
Enforce MKI Size	**Enforce**
RFC 2833 Mode	**Extend**
RFC 2833 DTMF Payload Type	**101**

Figure 4-18: Configuring IP Profile for Lync Server 2013 – SBC Media Tab

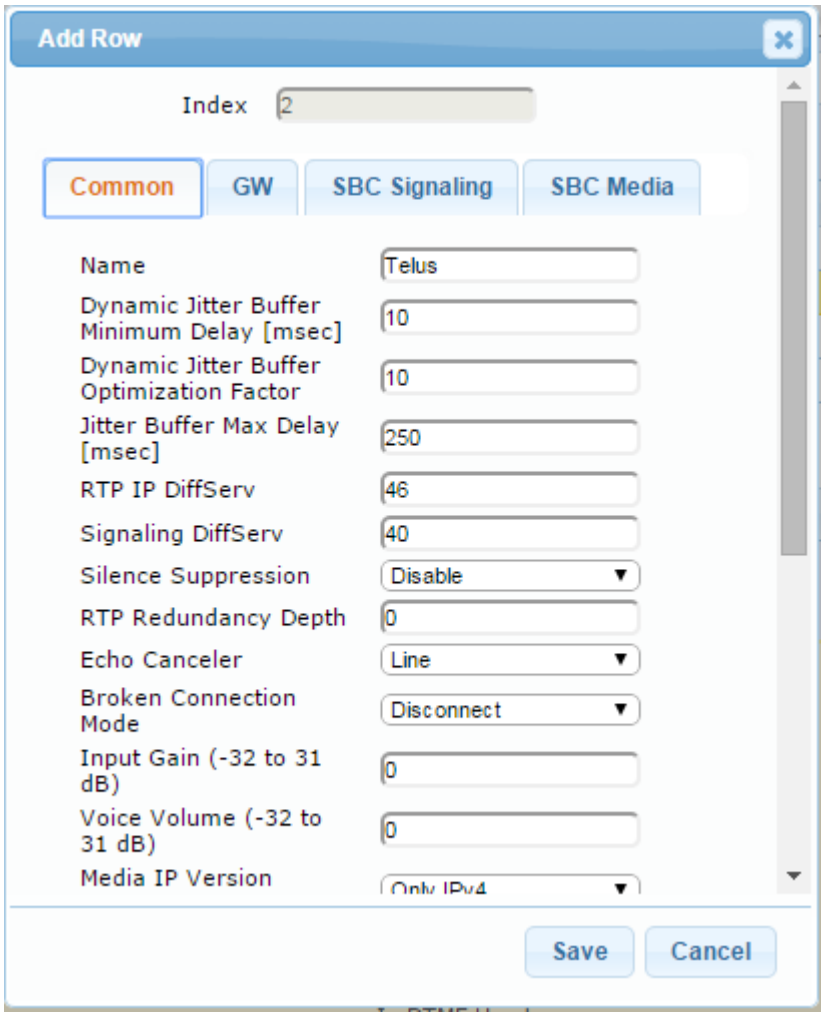


➢ **To configure an IP Profile for the SIP Trunk:**

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

Parameter	Value
Index	**2**
Profile Name	**Telus** (see Note on page 37)

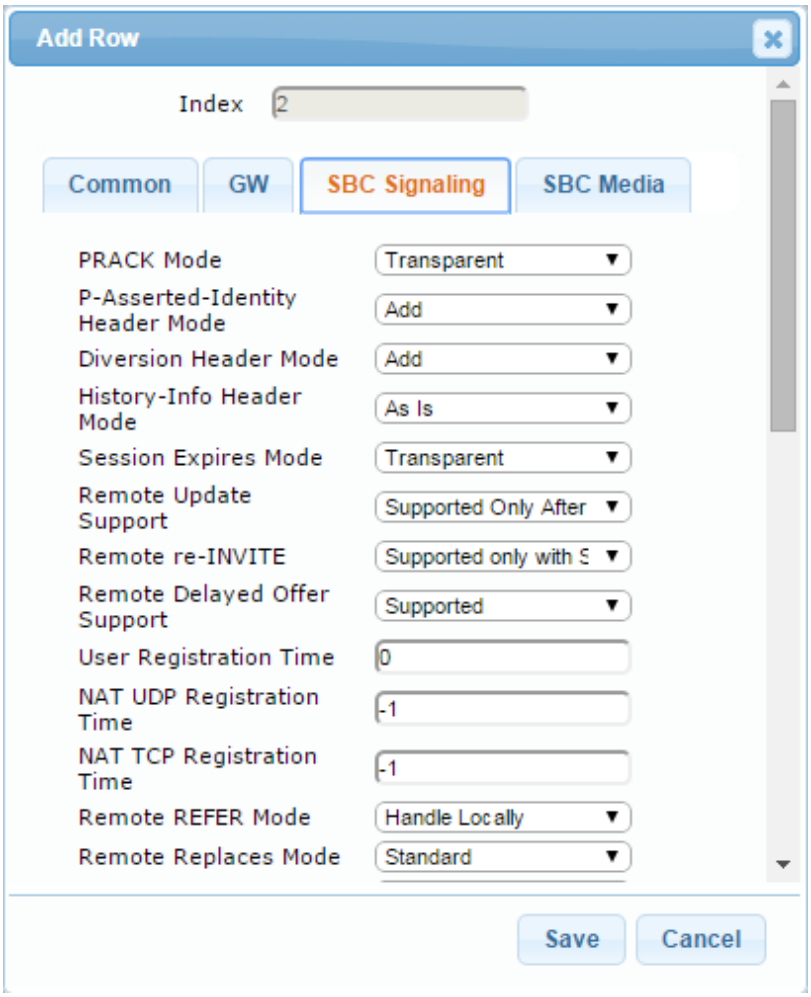
Figure 4-19: Configuring IP Profile for SIP Trunk – Common Tab



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

Parameter	Value
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Diversion Header Mode	**Add**
Remote Update Support	**Supported Only After Answer**
Remote re-INVITE	**Supported only with SDP**
Remote REFER Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Play RBT To Transferee	**Yes**
Remote Can Play Ringback	**No** (required, as Lync Server 2013 does not provide a ringback tone for incoming calls)
Remote Hold Format	**Send Only** (Telus initiates with the UPDATE method but supports this method when initiated by a Lync environment)

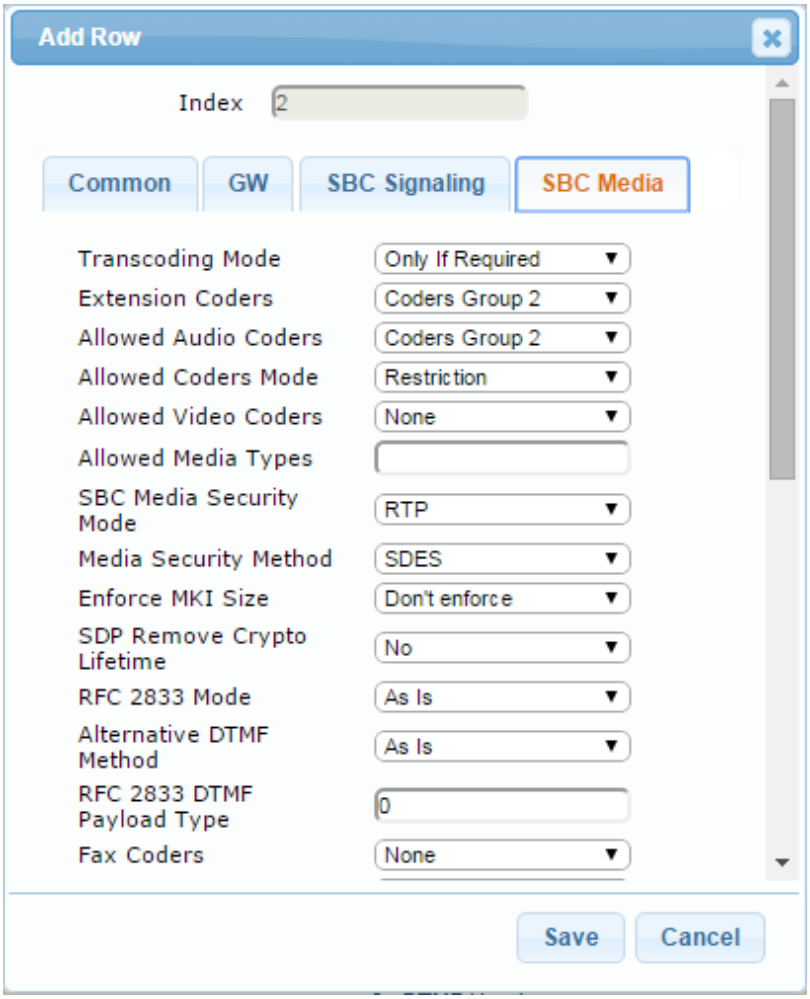
Figure 4-20: Configuring IP Profile for SIP Trunk – SBC Signaling Tab



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**
Allowed Coders Mode	**Restriction**
Media Security Behavior	**RTP**

Figure 4-21: Configuring IP Profile for SIP Trunk – SBC Media Tab

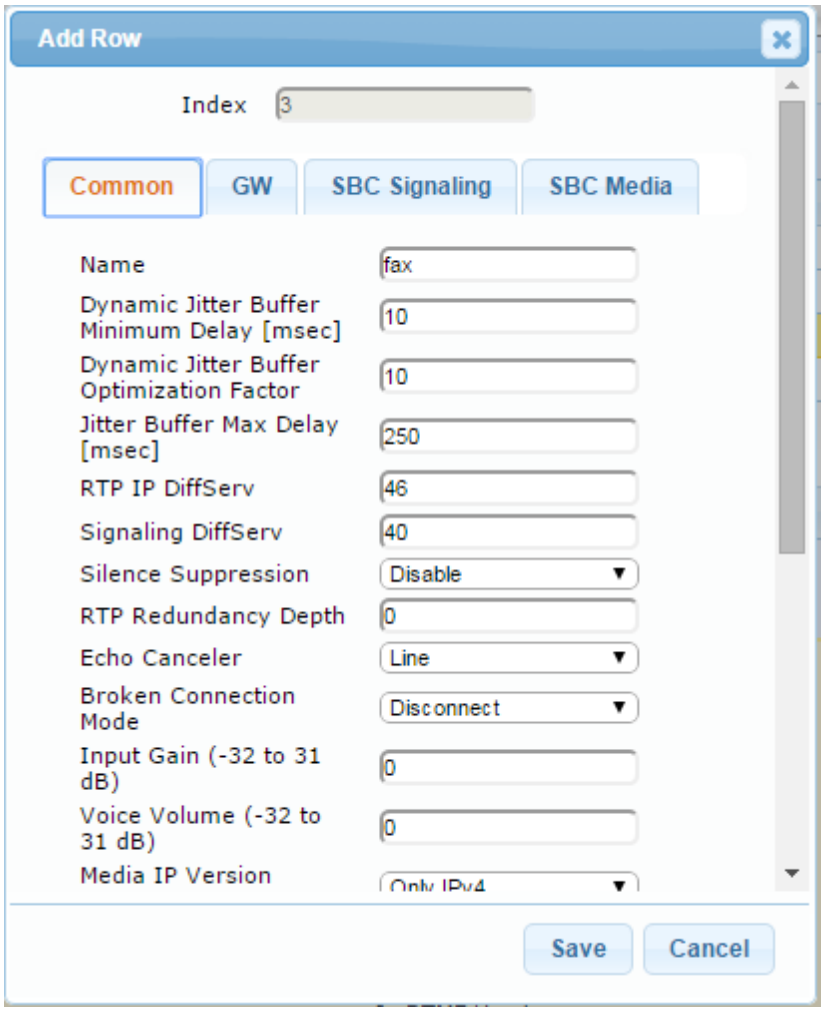


➢ **To configure an IP Profile for the FAX supporting ATA:**

5. Click **Add**.
6. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**3**
Profile Name	**fax** (see Note on page 37)

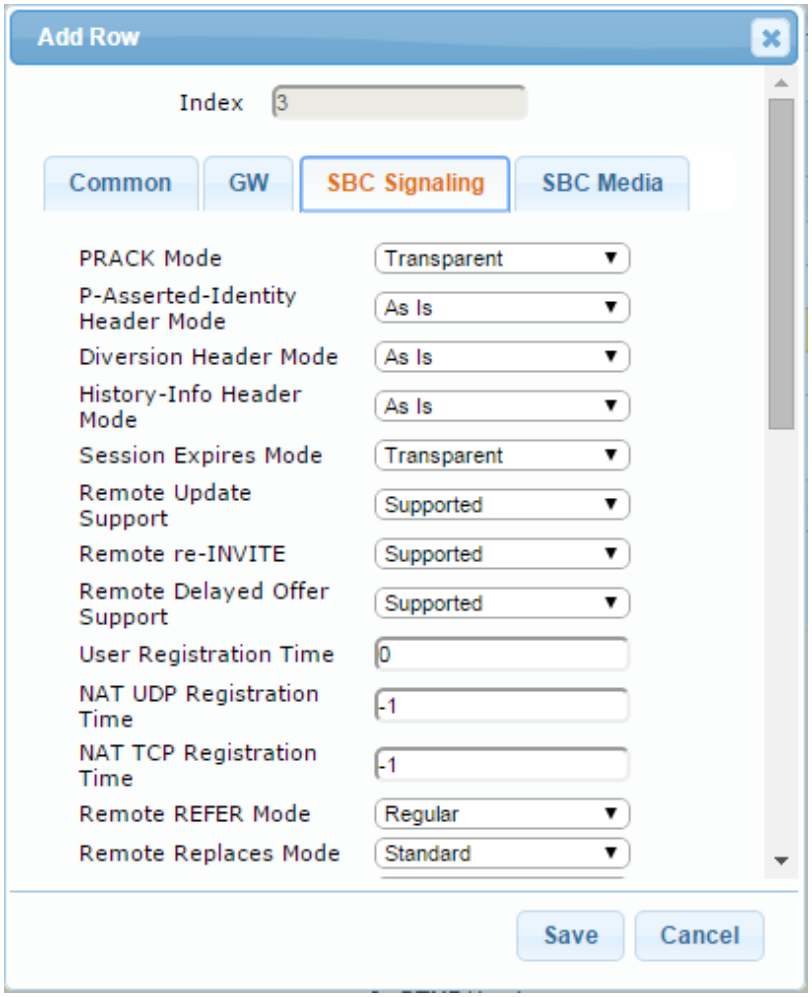
Figure 4-22: Configuring IP Profile for FAX ATA – Common Tab



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

Parameter	Value
All Parameters	**Leave as Default**

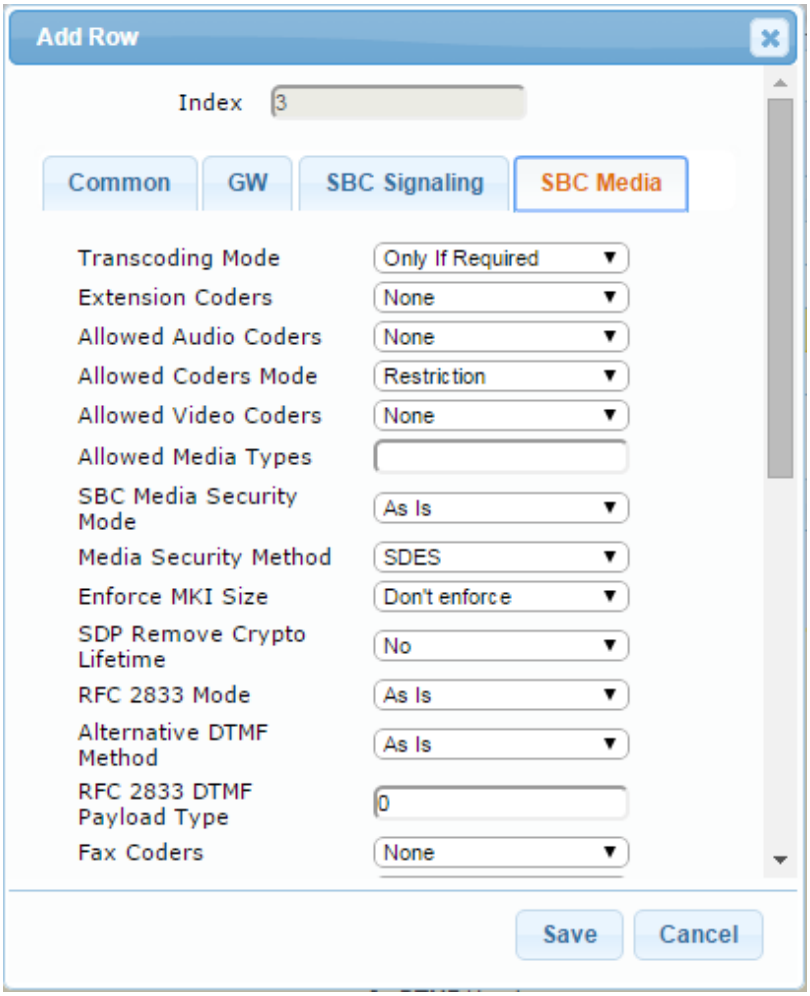
Figure 4-23: Configuring IP Profile for FAX ATA – SBC Signaling Tab



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

Parameter	Value
All Parameters	**Leave as default**

Figure 4-24: Configuring IP Profile for FAX ATA – SBC Media Tab



4.7 Step 7: Configure IP Groups

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

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

- Lync Server 2013 (Mediation Server) located on LAN
- SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the Lync Server 2013. You can use the default IP Group (Index 0), but modify it as shown below:

Parameter	Value
Index	**0**
Name	**Lync** (see Note on page 38)
Type	**Server**
Proxy Set	**Lync**
IP Profile	**Lync**
Media Realm	**Lync**
SIP Group Name	AC.test (according to ITSP requirement)

3. Configure an IP Group for the SIP Trunk:

Parameter	Value
Index	**1**
Name	**Telus** (see Note on page 38)
Type	**Server**
Proxy Set	**Telus**
IP Profile	**Telus**
Media Realm	**TELUS**
SIP Group Name	ITSP.test (according to ITSP requirement)
Local Host Name	ipnet.com (according to ITSP requirement for Internet Registration-based configuration).

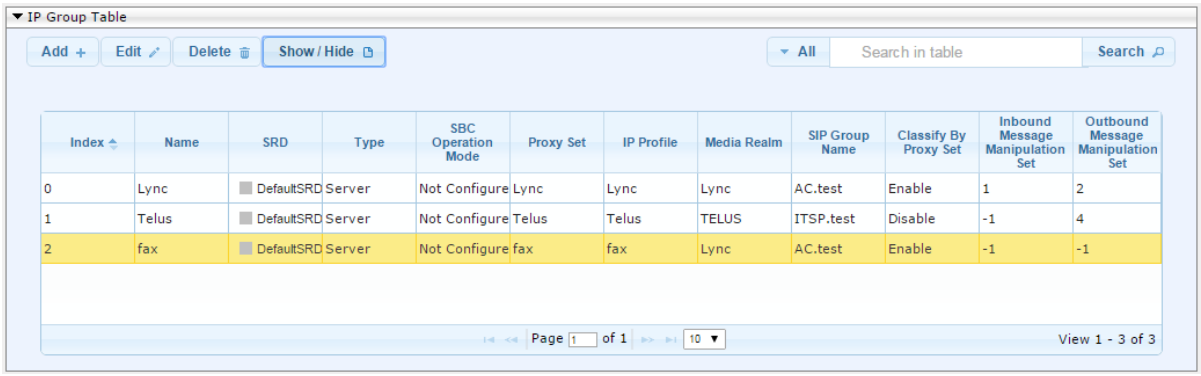
4. Configure an IP Group for the FAX supporting ATA:

Parameter	Value
Index	**2**

Name	**fax** (see Note on page 38)
Type	**Server**
Proxy Set	**fax**
IP Profile	**fax**
Media Realm	**Lync**
SIP Group Name	AC.test (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-25: Configured IP Groups in IP Group Table



4.8 Step 8: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Lync Server 2013 supports the G.711 coder while the network connection to SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the SIP Trunk.

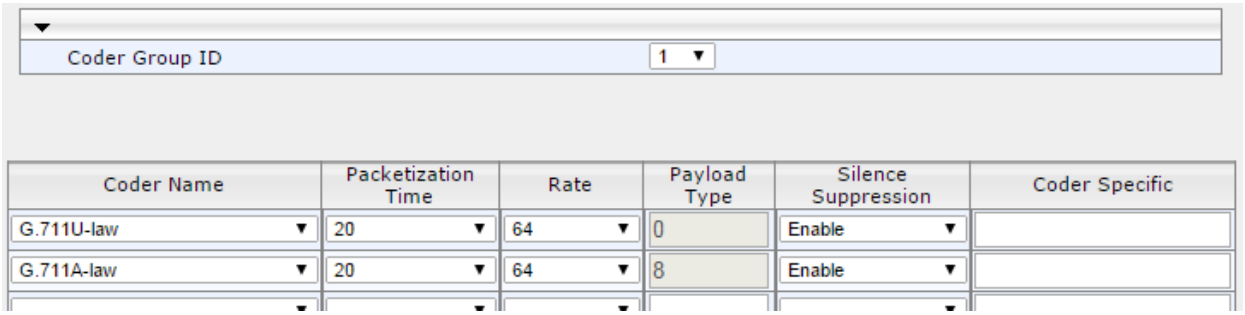
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6).

➢ **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 Lync Server 2013:

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

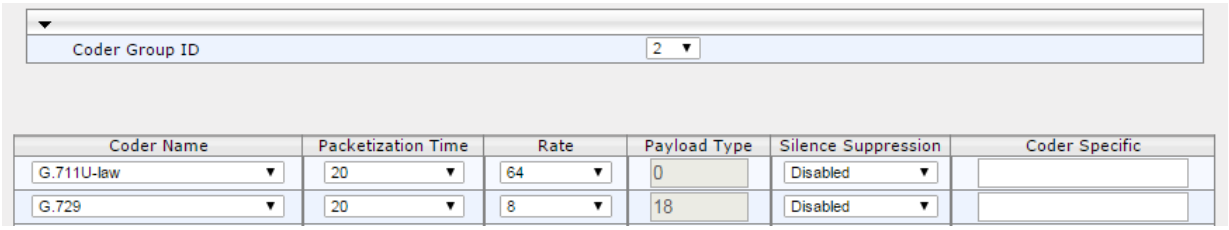
Figure 4-26: Configuring Coder Group for Lync Server 2013



3. Configure a Coder Group for SIP Trunk:

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

Figure 4-27: Configuring Coder Group for SIP Trunk



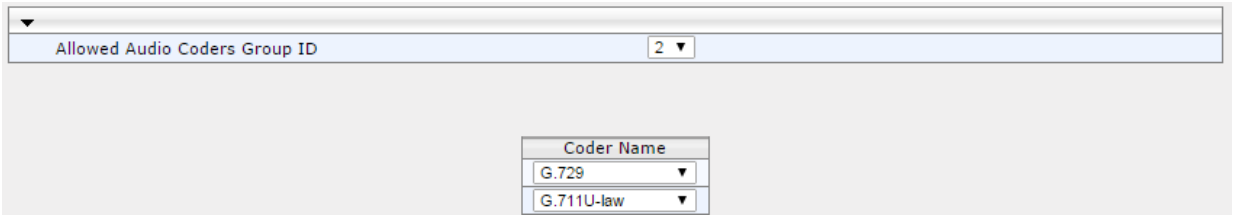
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the SIP Trunk (see Section 4.6).

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

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

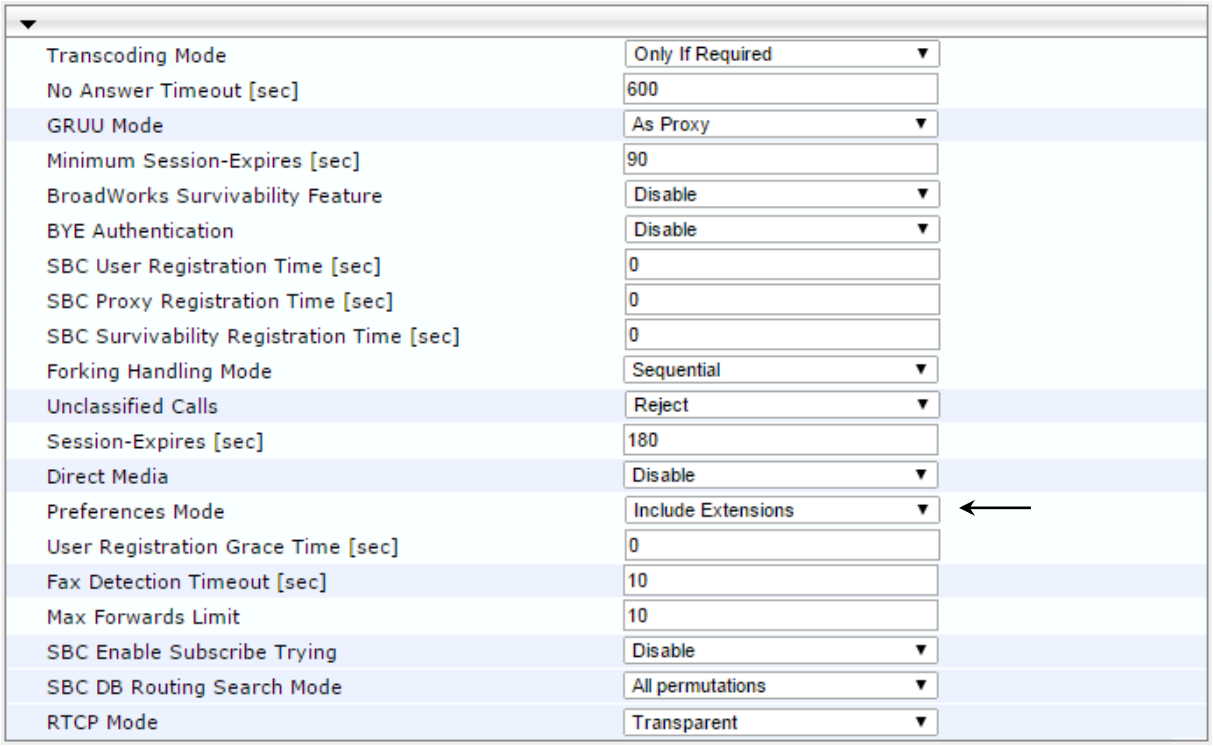
Parameter	Value
Allowed Audio Coders Group ID	**2**
Coder Name	**G.729** **G.711 U-law**

Figure 4-28: Configuring Allowed Coders Group for SIP Trunk



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

Figure 4-29: SBC Preferences Mode



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

4.9 Step 9: Configure SIP TLS Connection

This section describes how to configure the E-SBC for using a TLS connection with the Lync Server 2013 Mediation Server. This is essential for a secure SIP TLS connection.

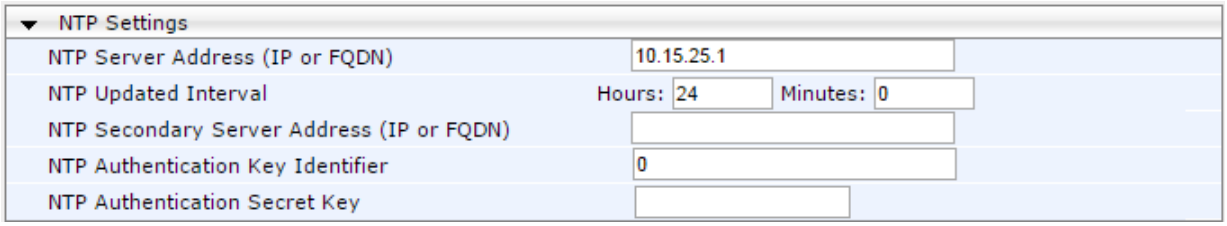
4.9.1 Step 9a: Configure the NTP Server Address

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

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

1. Open the Application Settings page (**Configuration** tab > **System** > **Application Settings**).
2. In the 'NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.25.1**).

Figure 4-30: Configuring NTP Server Address



3. Click **Submit**.

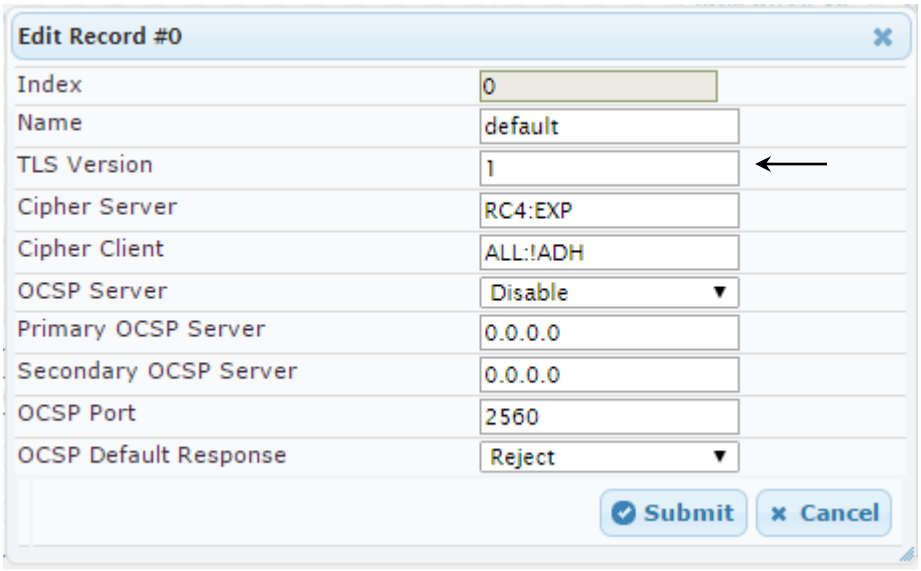
4.9.2 Step 9b: Configure the TLS version 1.0

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

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

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

Figure 4-31: Configuring TLS version 1.0



4. Click **Submit**.

4.9.3 Step 9c: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Lync Server 2013.

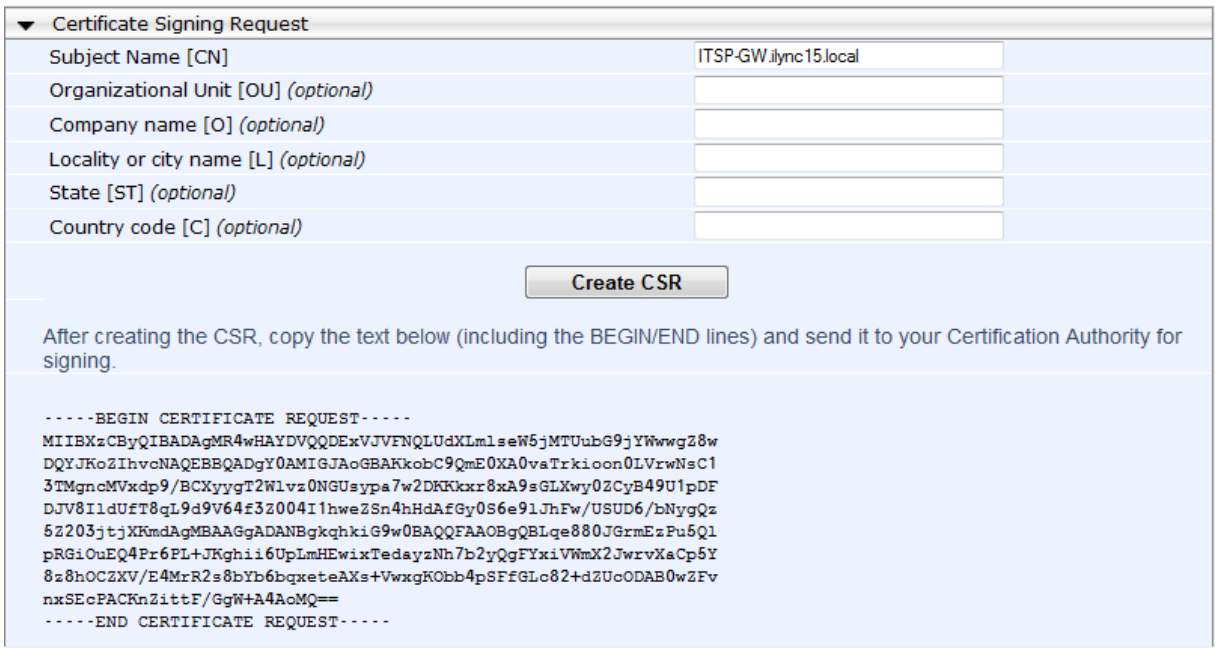
The procedure involves the following main steps:

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-2.ilync15.local**).
   b. Fill in the rest of the request fields according to your security provider's instructions.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-32: Certificate Signing Request – Creating CSR

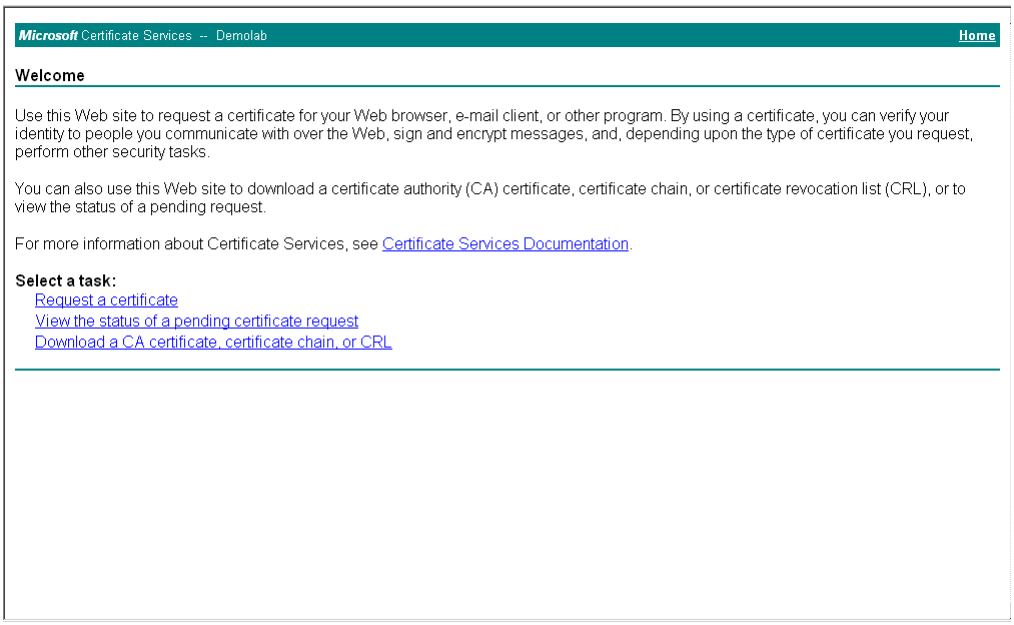


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1).

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

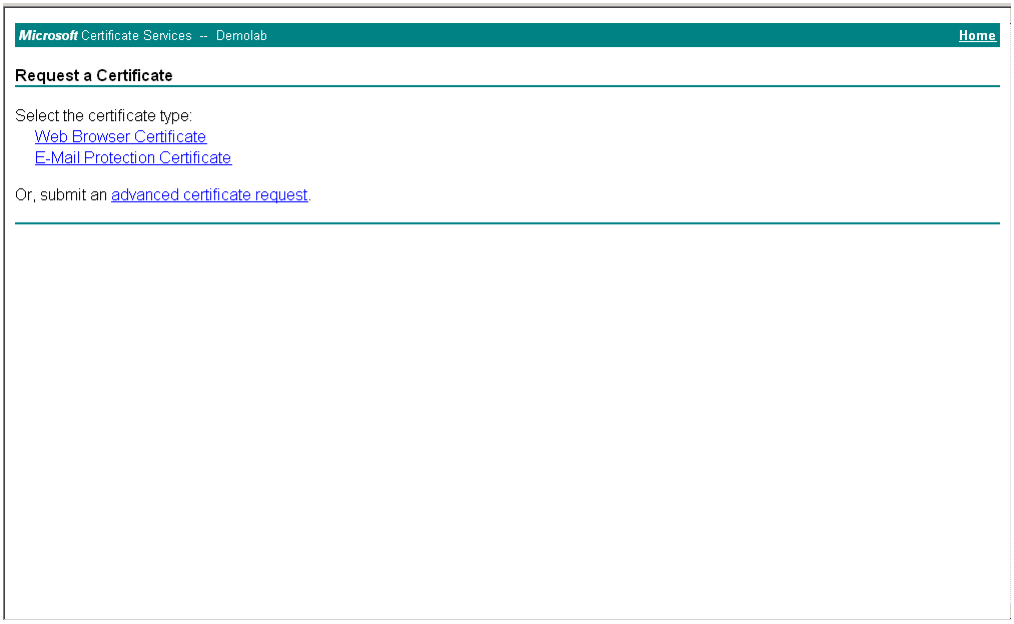
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-33: Microsoft Certificate Services Web Page



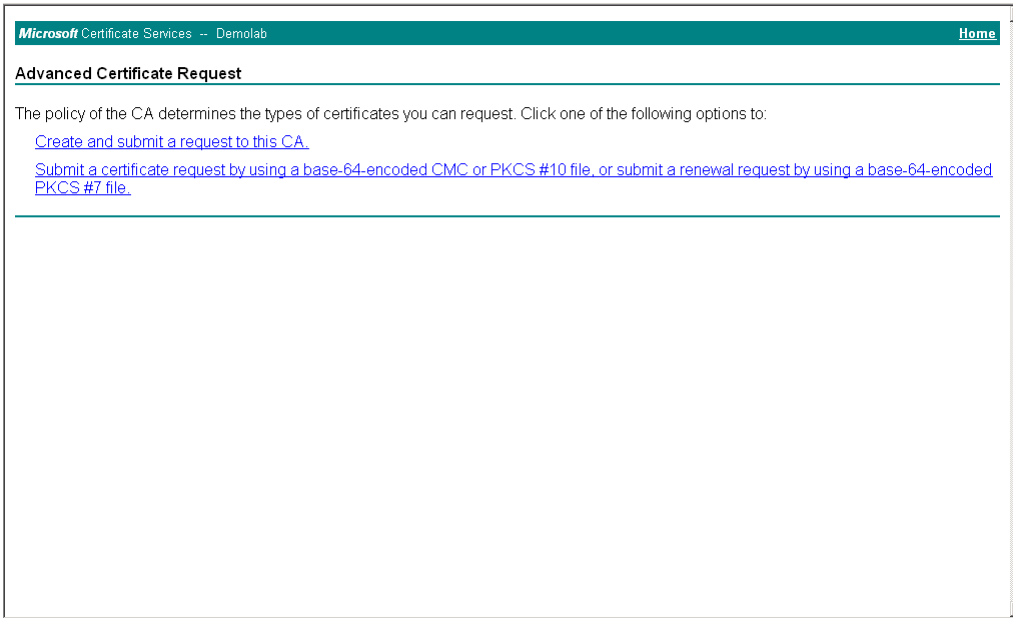
7. Click **Request a certificate**.

Figure 4-34: Request a Certificate Page



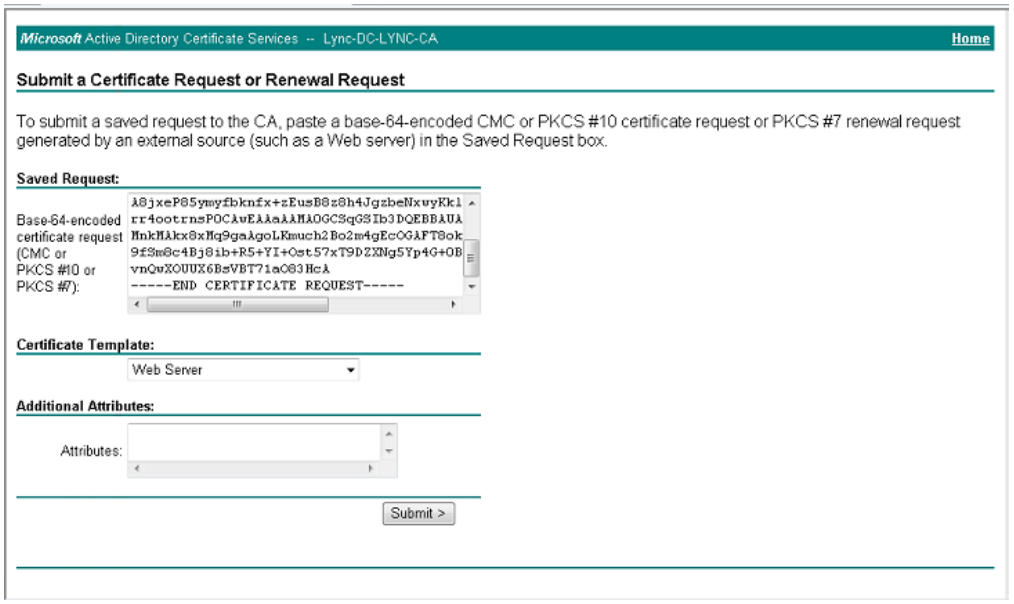
8. Click **advanced certificate request**, and then click **Next**.

Figure 4-35: Advanced Certificate Request Page



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

Figure 4-36: Submit a Certificate Request or Renewal Request Page

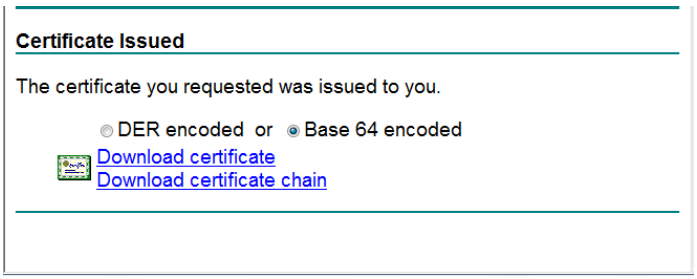


10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.

11. From the 'Certificate Template' drop-down list, select **Web Server**.

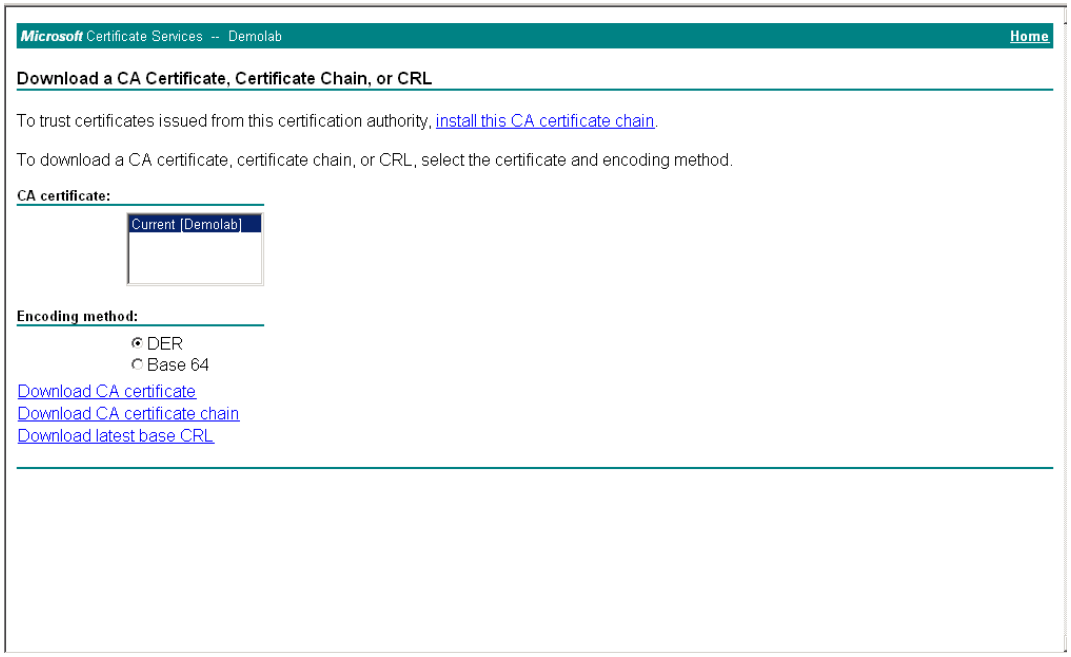
12. Click **Submit**.

Figure 4-37: Certificate Issued Page



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

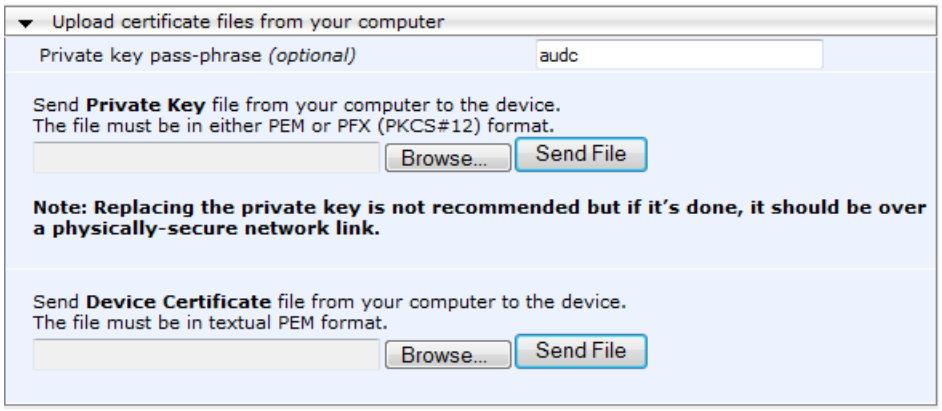
Figure 4-38: Download a CA Certificate, Certificate Chain, or CRL Page



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.

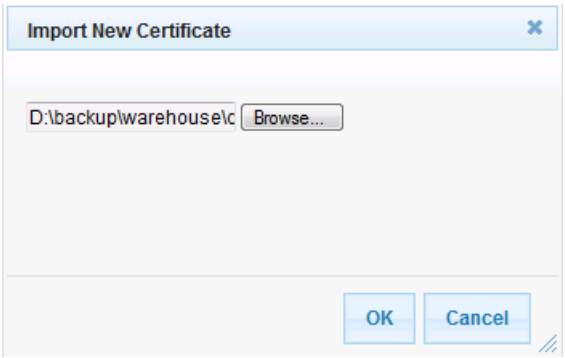
20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
    a. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-39: Upload Device Certificate Files from your Computer Group



    b. In the E-SBC's Web interface, return to the **TLS Contexts** page.
    c. 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.
    d. Click the **Import** button, and then select the certificate file to load.

Figure 4-40: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16).

4.10 Step 10: Configure SRTP

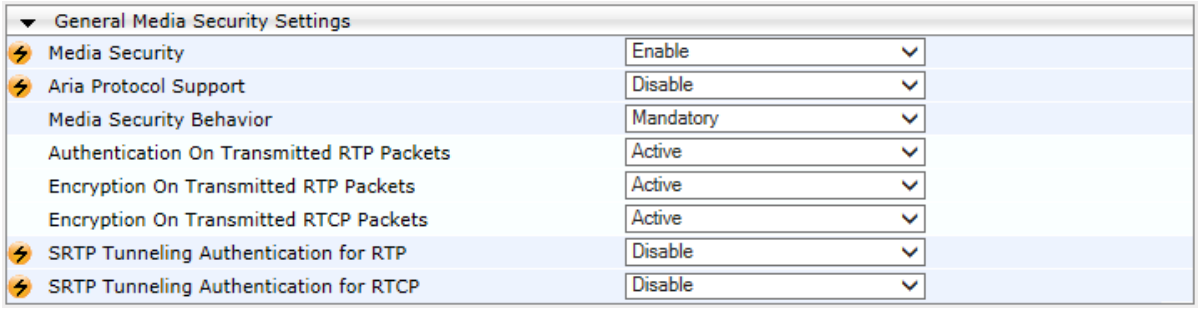
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6).

➢ **To configure media security:**

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

Parameter	Value
Media Security	**Enable**

Figure 4-41: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16).

4.11 Step 11: Configure Maximum IP Media Channels

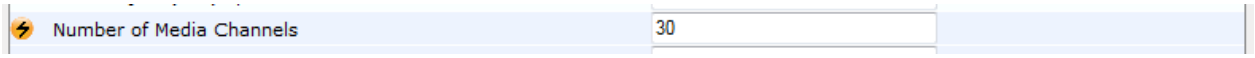
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

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

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

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

Figure 4-42: Configuring Number of Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.7 on page 44, IP Group 1 represents Lync Server 2013, and IP Group 2 represents SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Lync Server 2013 (LAN), SIP Trunk (WAN), and the FAX supporting ATA (LAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from any direction
- Calls from Lync Server 2013 to SIP Trunk
- Calls from SIP Trunk specifically for FAX
- Calls from SIP Trunk to Lync Server 2013
- Calls from FAX supporting ATA to SIP Trunk

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

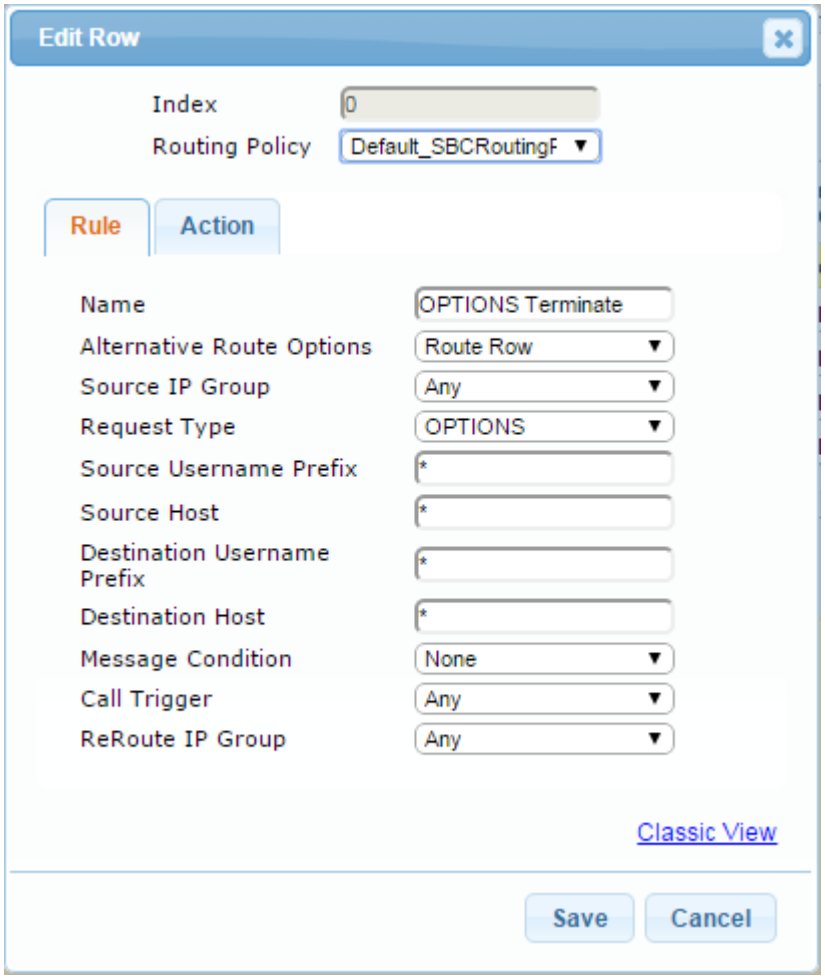
1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:

a. Click **Add**.

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

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

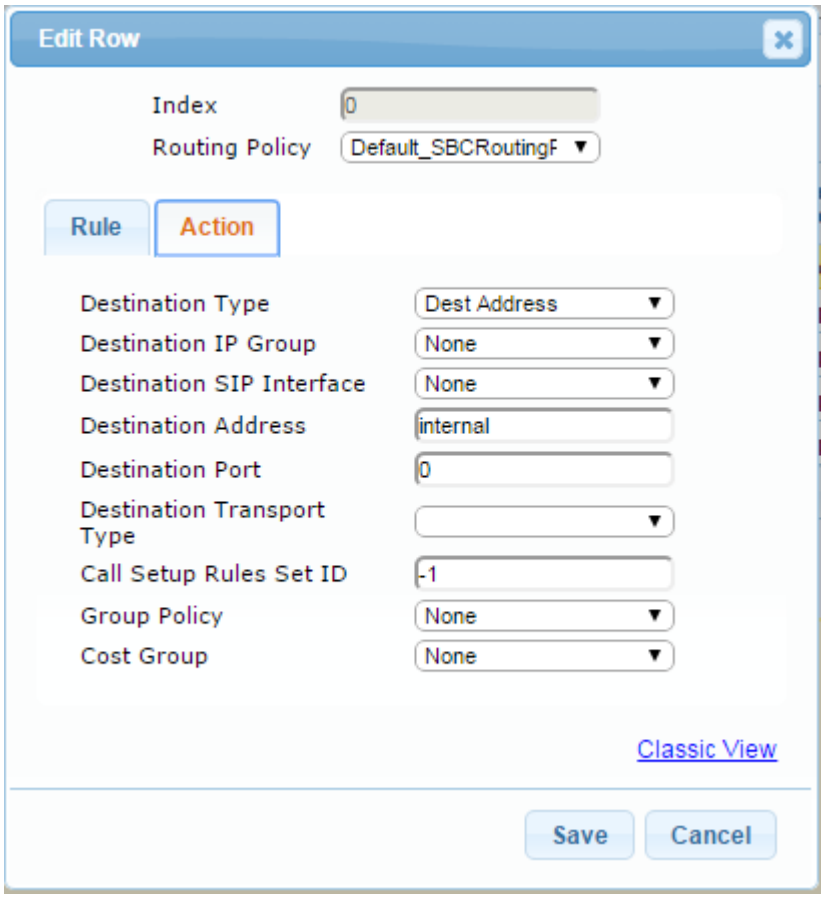
Figure 4-43: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab



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

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

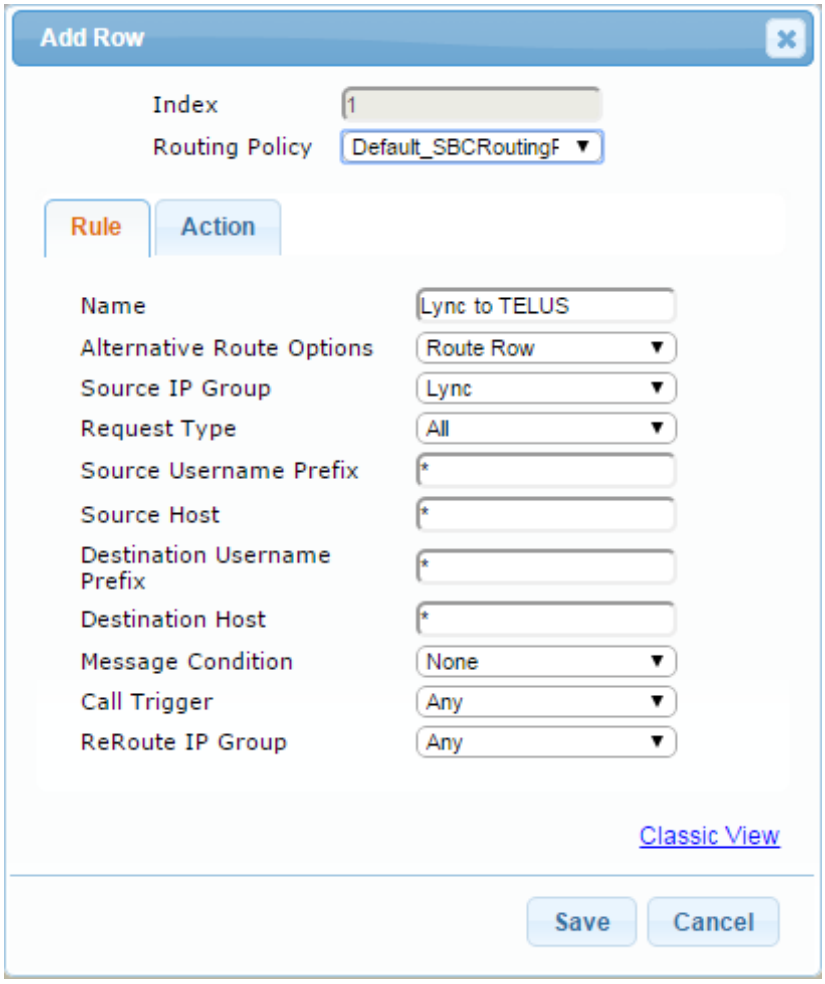
Figure 4-44: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab



3. Configure a rule to route calls from Lync Server 2013 to SIP Trunk:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

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

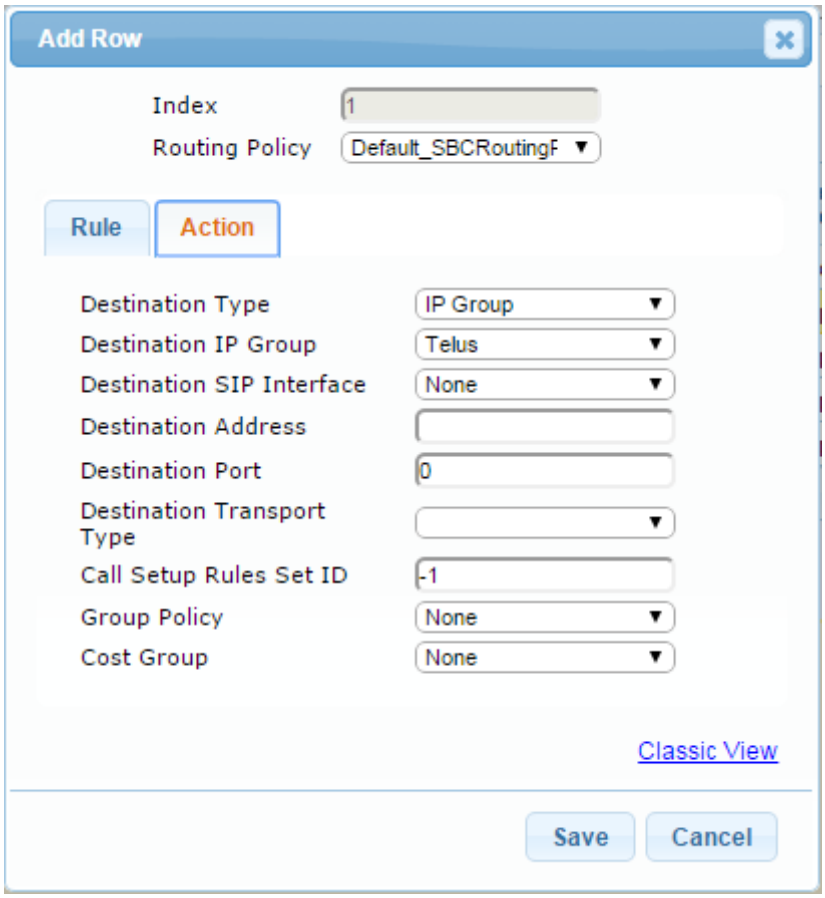
Figure 4-45: Configuring IP-to-IP Routing Rule for Lync to Telus – Rule tab



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

Parameter	Value
Destination Type	**IP Group**
Destination IP Group	**Telus**

Figure 4-46: Configuring IP-to-IP Routing Rule for Lync to Telus – Action tab



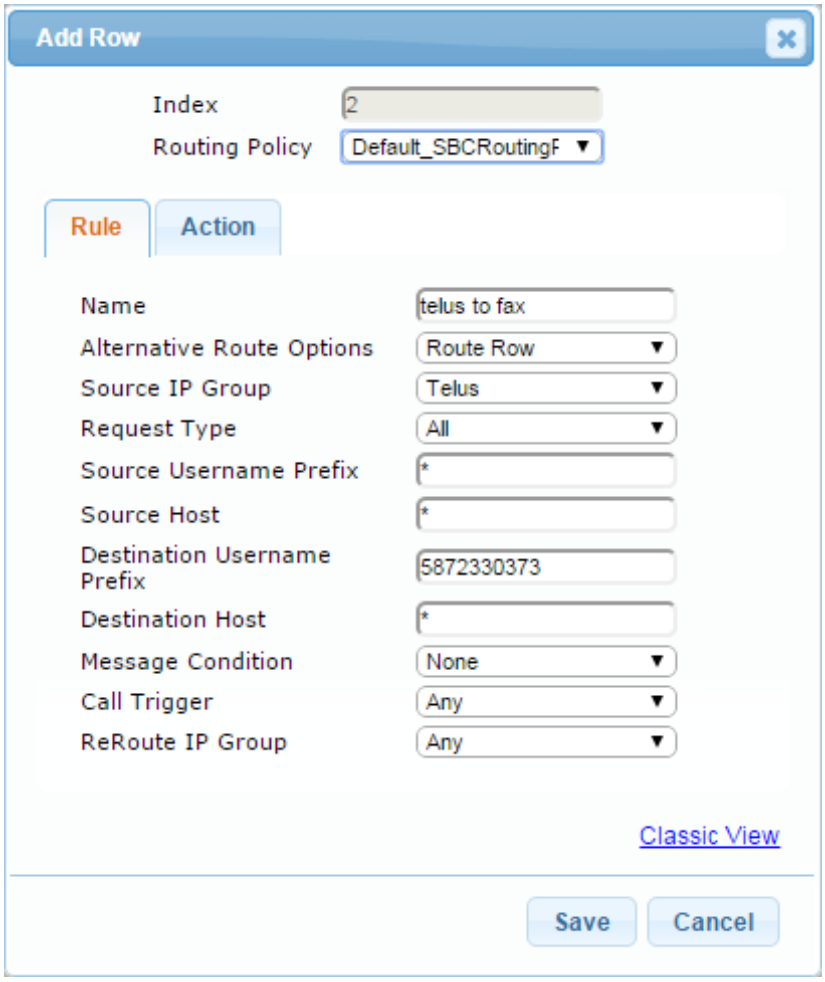
4. To configure rule to route calls from SIP Trunk to FAX supporting ATA:

a. Click **Add**.

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

Parameter	Value
Index	**2**
Route Name	**telus to fax** (arbitrary descriptive name)
Source IP Group	**Telus**
Destination Username Prefix	**5872330373** (specific number to route to ATA)

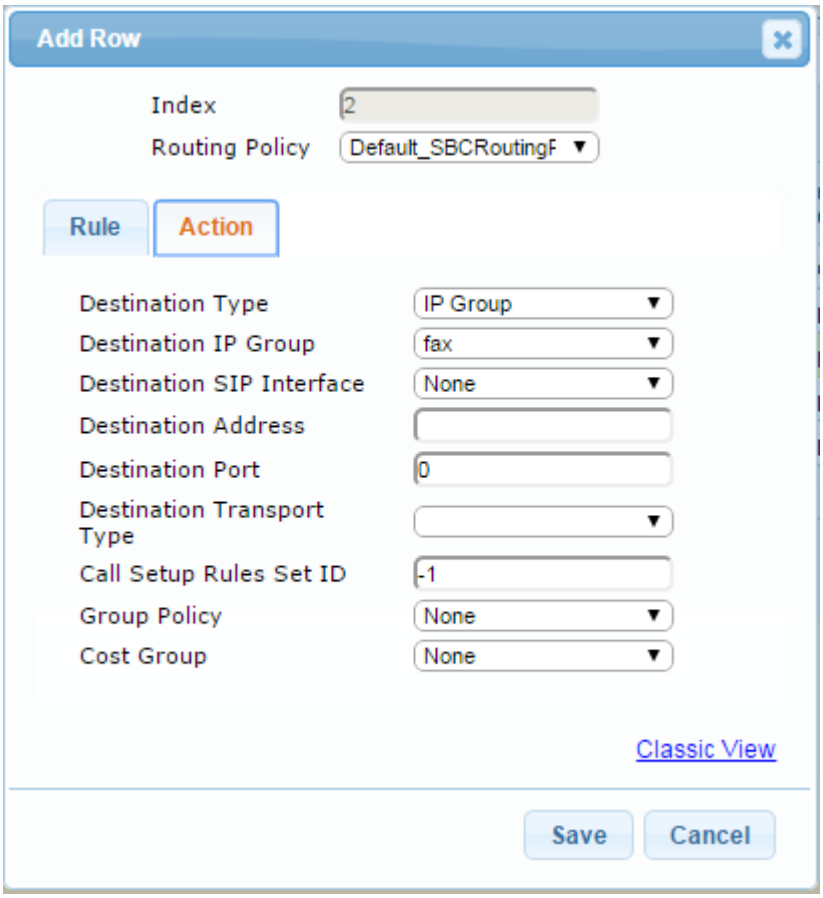
Figure 4-47: Configuring IP-to-IP Routing Rule for Telus to fax – Rule tab



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

Parameter	Value
Destination Type	**IP Group**
Destination IP Group	**fax**

Figure 4-48: Configuring IP-to-IP Routing Rule for Telus to fax – Action tab



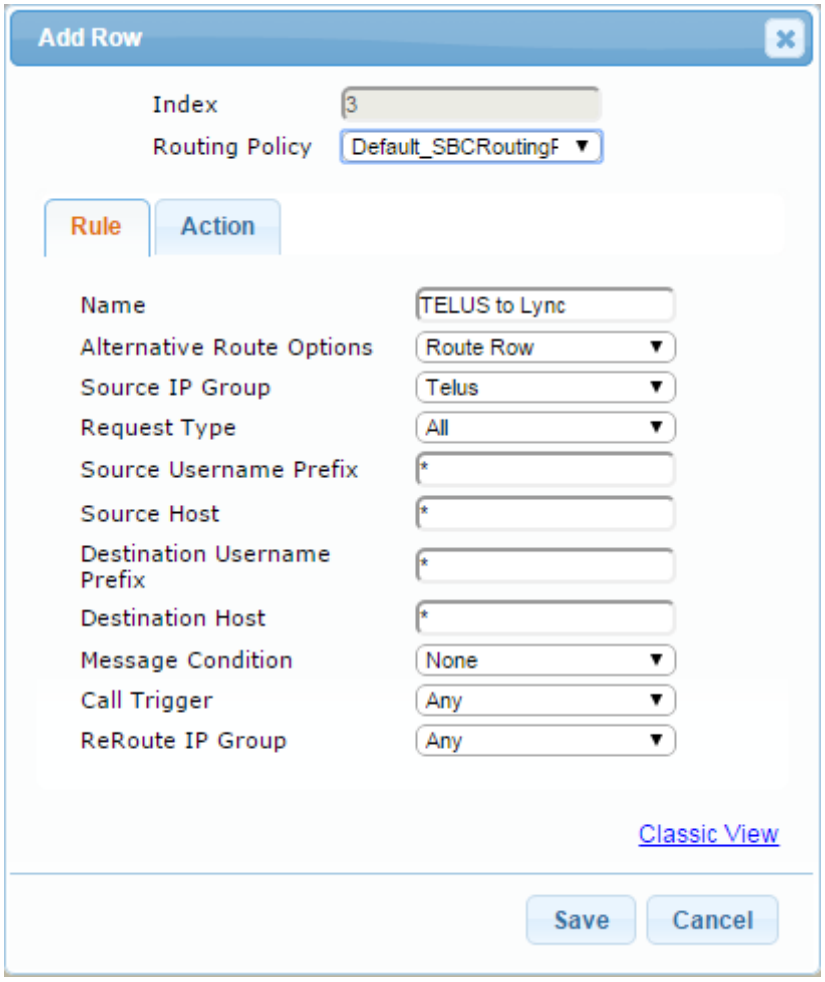
5. To configure rule to route calls from SIP Trunk to Lync Server 2013:

a. Click **Add**.

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

Parameter	Value
Index	**3**
Route Name	**Telus to Lync** (arbitrary descriptive name)
Source IP Group	**Telus**

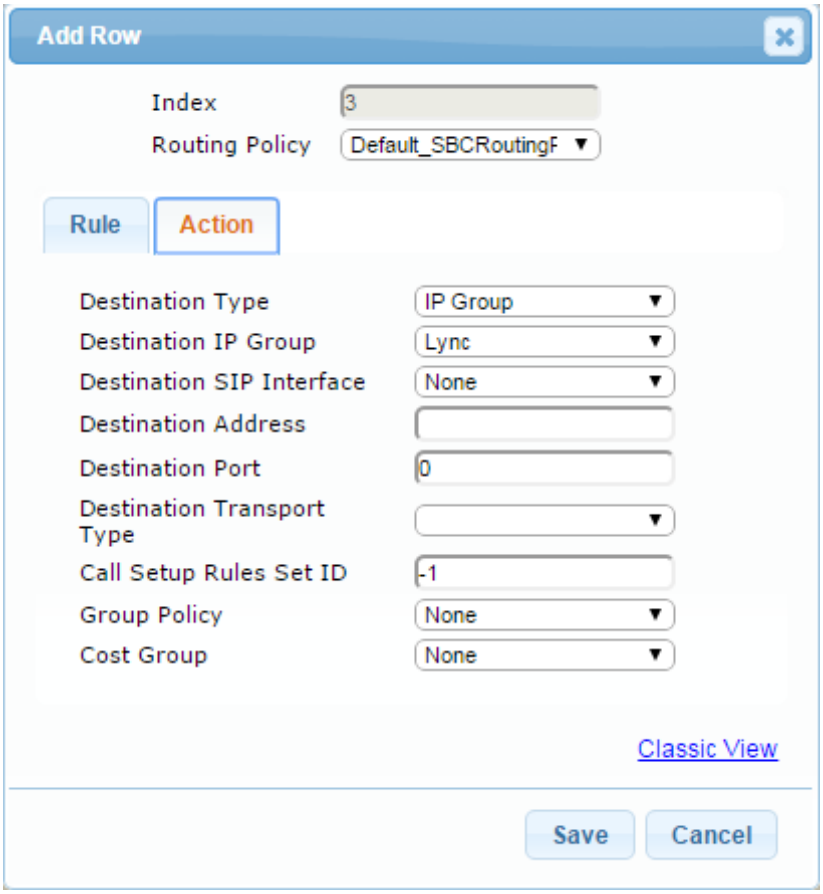
Figure 4-49: Configuring IP-to-IP Routing Rule for Telus to Lync – Rule tab



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

Parameter	Value
Destination Type	**IP Group**
Destination IP Group	**Lync**

Figure 4-50: Configuring IP-to-IP Routing Rule for Telus to Lync – Action tab



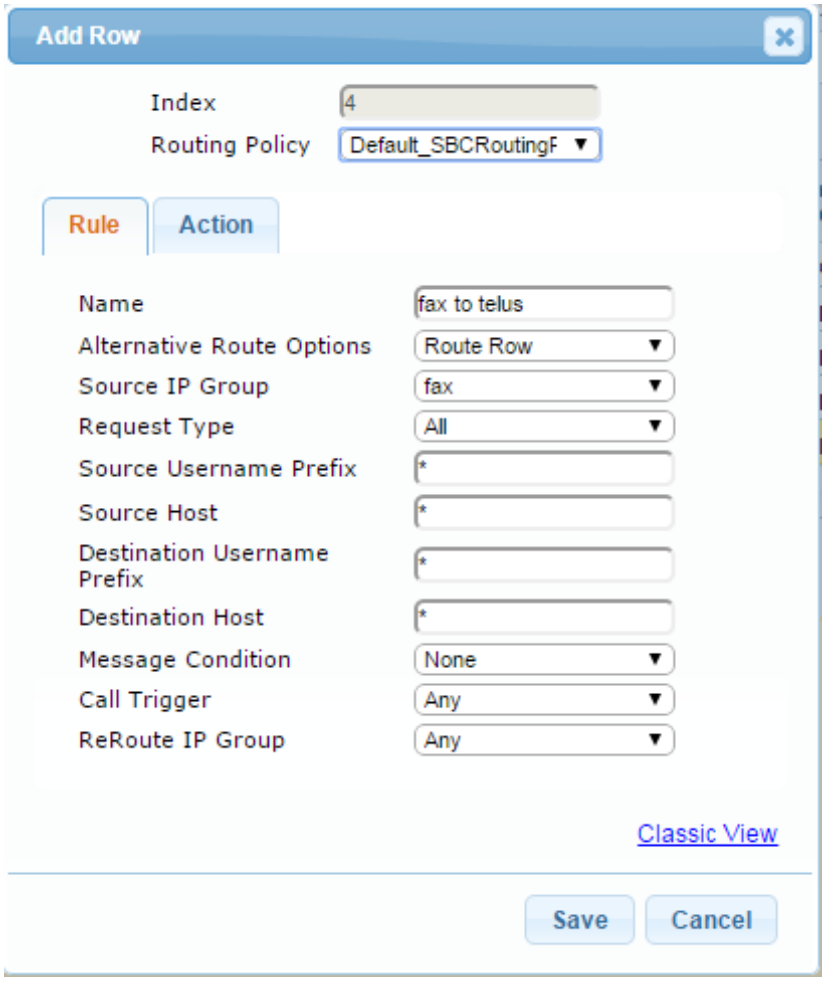
6. To configure rule to route calls from Fax ATA to Telus:

a. Click **Add**.

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

Parameter	Value
Index	**4**
Route Name	**fax to Telus** (arbitrary descriptive name)
Source IP Group	**fax**

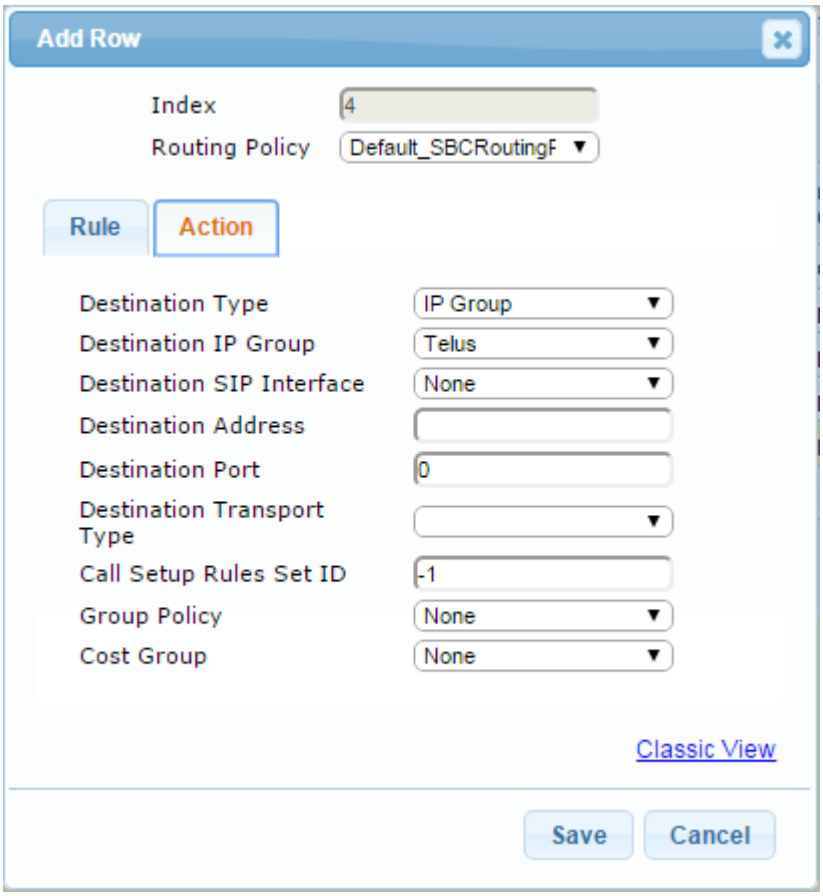
Figure 4-51: Configuring IP-to-IP Routing Rule for fax to Telus – Rule tab



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

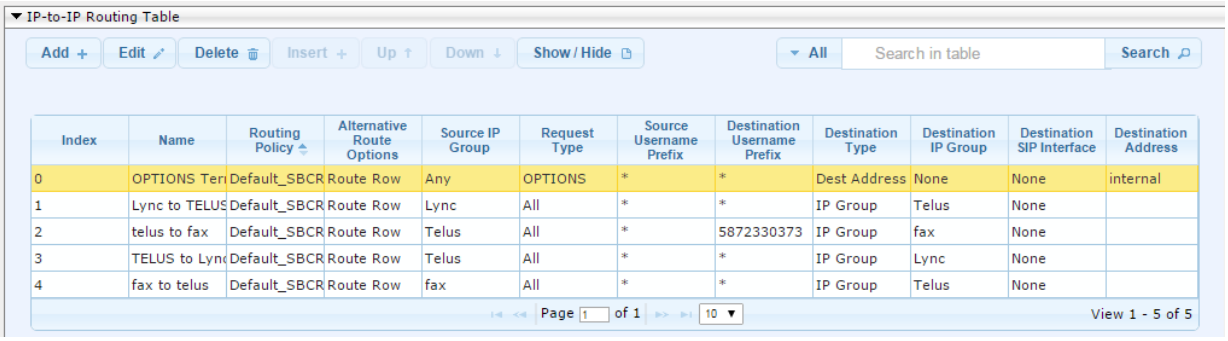
Parameter	Value
Destination Type	**IP Group**
Destination IP Group	**Telus**

Figure 4-52: Configuring IP-to-IP Routing Rule for fax to Telus – Action tab



The configured routing rules are shown in the figure below:

Figure 4-53: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



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

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.7 on page 44, IP Group 0 represents Lync Server 2013, and IP Group 1 represents SIP Trunk.

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

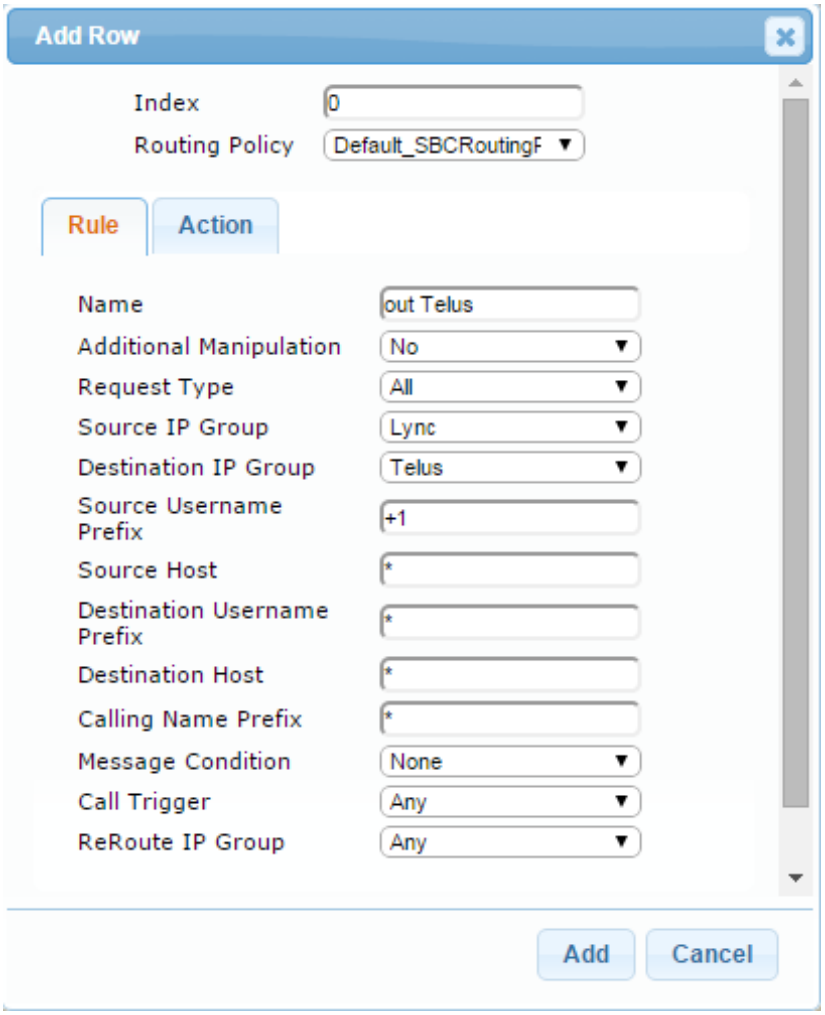
For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from the SIP Trunk IP Group to the Lync Server 2013 IP Group for any destination username prefix.

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

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

Parameter	Value
Index	**0**
Name	**Out Telus**
Source IP Group	**Lync**
Destination IP Group	**Telus**
Source Username Prefix	**+1**
Destination Username Prefix	***** (asterisk sign)

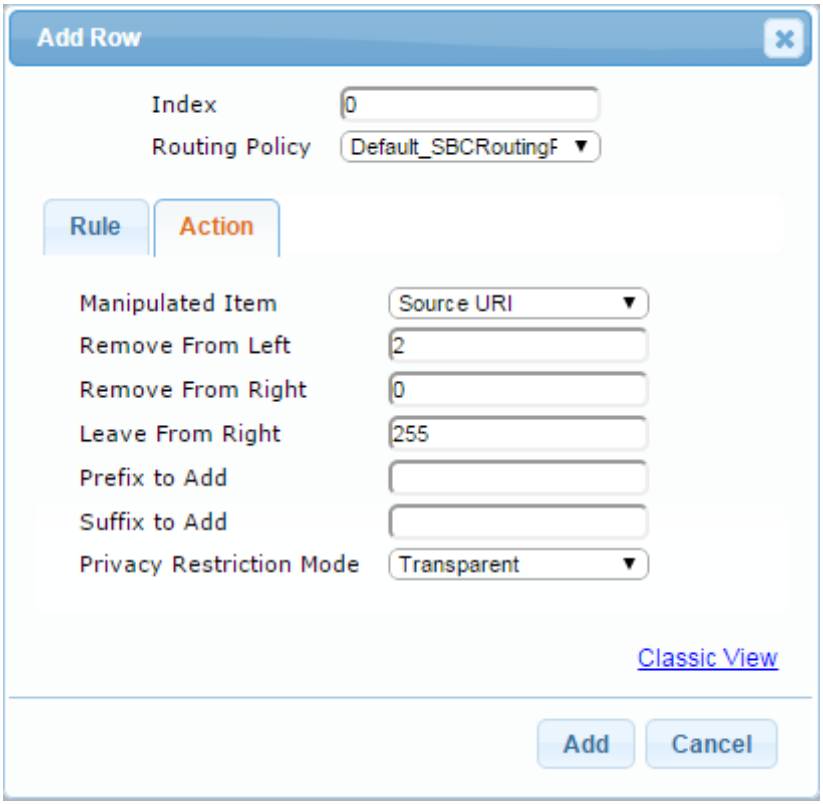
Figure 4-54: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Value
Manipulated Item	**Source URI**
Remove from left	**2**

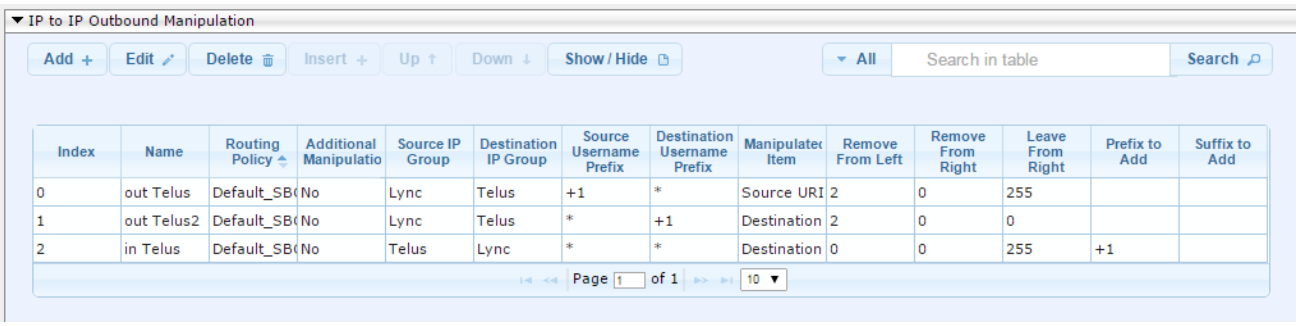
Figure 4-55: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between Lync Server 2013 IP Group and Telus IP Group:

Figure 4-56: Example of Configured IP-to-IP Outbound Manipulation Rules



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

4.14 Step 14: Configure Message Manipulation Rules

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

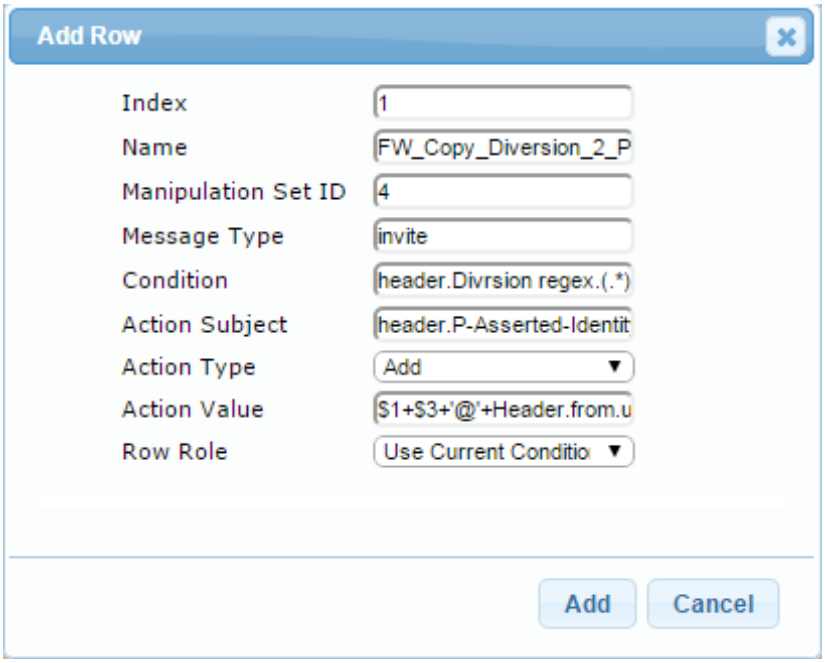
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for SIP Trunk. This rule applies to messages sent to the SIP Trunk IP Group in a call forward scenario. This adds a P-Asserted-Identity header to outgoing invite which is derived from the Diversion header which was created when a History header was originally sent the MS Lync environment for a Forward call. The URL Host part of the SIP From Header is used to populate the value of the P-Asserted-Identity Header. This works in concert with the Telus IP Profile parameter for adding a Diversion header.

Parameter	Value
Index	**1**
Name	**FW_Copy_Diversion_2_P-Asserted**
Manipulation Set ID	**4**
Message Type	**invite**
Condition	**header.Diversion regex.(.*)(\+1)(.*)(@)(.*)**
Action Subject	**header.P-Asserted-Identity**
Action Type	**Add**
Action Value	**$1+$3+'@'+Header.from.url.host+';user=phone>'**

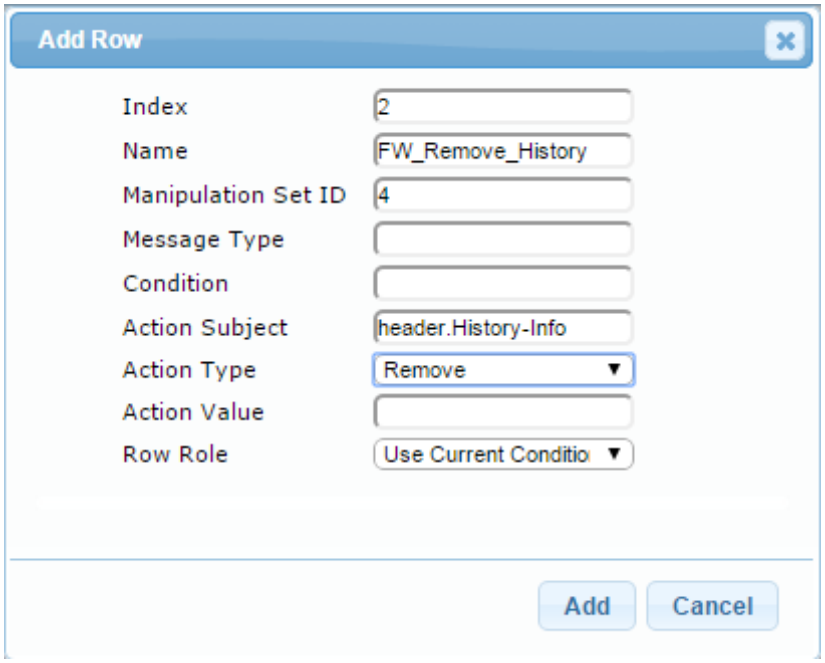
Figure 4-57: Configuring SIP Message Manipulation Rule 1 (for Telus SIP Trunk)



3. Configure a new manipulation rule (Manipulation Set 4) for SIP Trunk. This rule applies to messages sent to the SIP Trunk IP Group in a call forward scenario. This removes the History-Info header from the outgoing invite which was originally received from the Lync environment. It was used to generate a Diversion header which was then used to create the P-Asserted-Identity header for a Forward call. This is clearing the Telus unsupported header for proper interworking.

Parameter	Value
Index	**2**
Name	**FW_Remove_History**
Manipulation Set ID	**4**
Action Subject	**header.History-Info**
Action Type	**Remove**

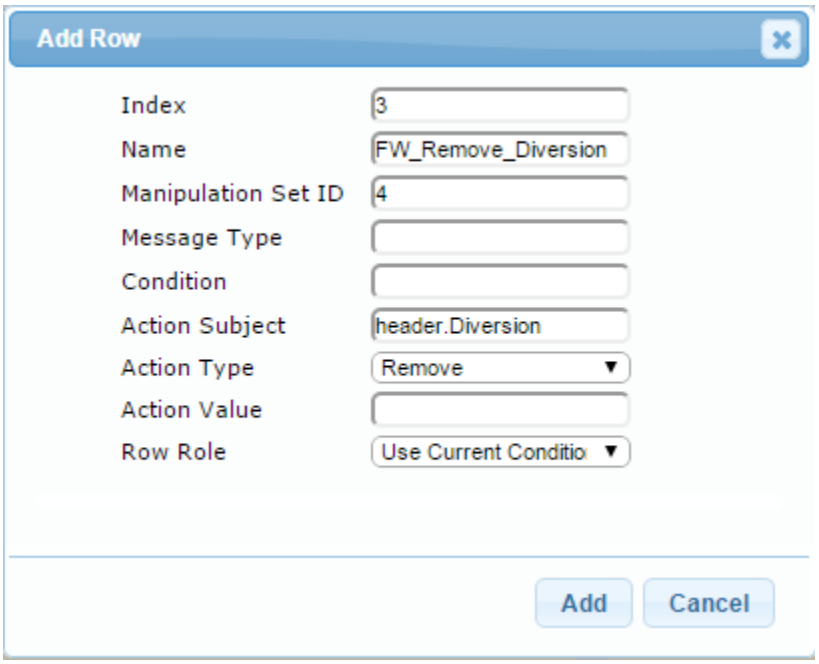
Figure 4-58: Configuring SIP Message Manipulation Rule 2 (for Telus' SIP Trunk)



4. Configure a new manipulation rule (Manipulation Set 4) for SIP Trunk. This rule applies to messages sent to the SIP Trunk IP Group in a call forward scenario. This removes the Diversion header from the outgoing invite which was temporarily created based off of the History-Info header originally received from the Lync environment. It was used to generate a P-Asserted-Identity header for a Forward call. This is clearing the Telus unsupported header for proper interworking.

Parameter	Value
Index	**3**
Name	**FW_Remove_Diversion**
Manipulation Set ID	**4**
Action Subject	**header.Diversion**
Action Type	**Remove**

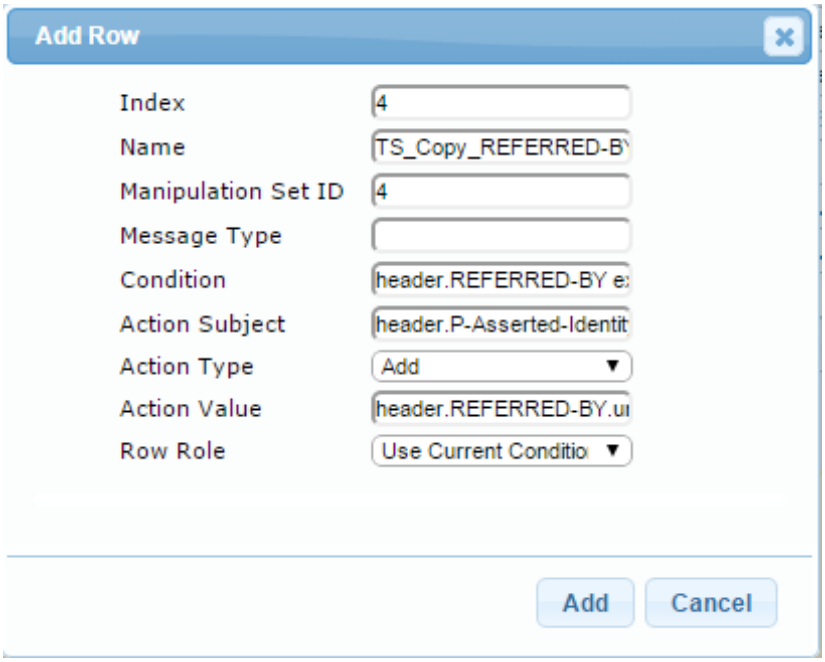
Figure 4-59: Configuring SIP Message Manipulation Rule 3 (for Telus' SIP Trunk)



5. Configure a new manipulation rule (Manipulation Set 4) for SIP Trunk. This rule applies to messages sent to the SIP Trunk IP Group in a call transfer scenario. This adds a P-Asserted-Identity header to outgoing invite which is derived from the Referred-By header which was originally sent from the MS Lync environment for a Transfer call. The URL Host part of the SIP Referred-By Header is used to populate the value of the P-Asserted-Identity Header.

Parameter	Value
Index	**4**
Name	**TS_Copy_REFERRED-BY_2_P-Asserted**
Manipulation Set ID	**4**
Condition	**header.REFERRED-BY exists**
Action Subject	**header.P-Asserted-Identity**
Action Type	**Add**
Action Value	**header.REFERRED-BY.url**

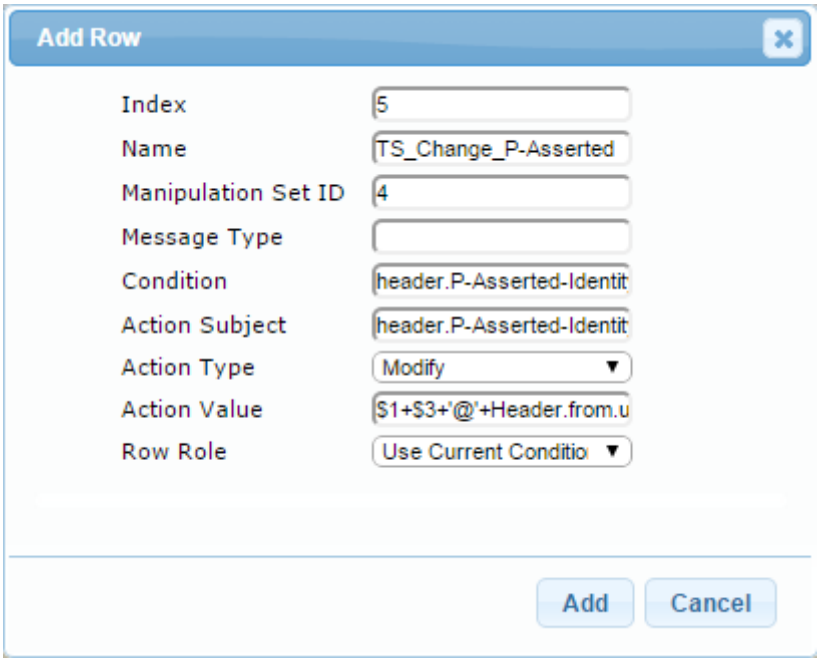
Figure 4-60: Configuring SIP Message Manipulation Rule 4 (for Telus' SIP Trunk)



6. Configure a new manipulation rule (Manipulation Set 4) for SIP Trunk. This rule applies to messages sent to the SIP Trunk IP Group in a call transfer scenario. This modifies the P-Asserted-Identity header of the outgoing invite which is derived from the Referred-By header which was originally sent from the MS Lync environment for a Transfer call. This rule removes the '+1' prefix and the URL Host part of the SIP From Header is used to populate the value of the P-Asserted-Identity Header URL Host value.

Parameter	Value
Index	**5**
Name	**TS_Change_P-Asserted**
Manipulation Set ID	**4**
Condition	**header.P-Asserted-Identity regex.(.*)(\+1)(.*)(@)(.*)**
Action Subject	**header.P-Asserted-Identity**
Action Type	**Modify**
Action Value	**$1+$3+'@'+Header.from.url.host+';user=phone>'**

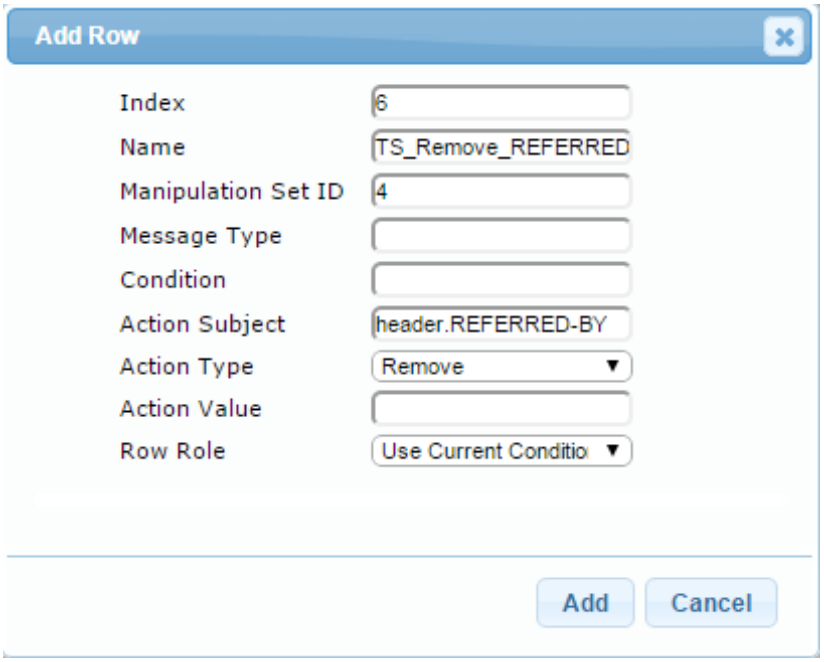
Figure 4-61: Configuring SIP Message Manipulation Rule 5 (for Telus' SIP Trunk)



7. Configure a new manipulation rule (Manipulation Set 4) for SIP Trunk. This rule applies to messages sent to the SIP Trunk IP Group in a call transfer scenario. This removes the Referred-By header from the outgoing invite to support the interworking between MS Lync and Telus for the unsupported header.

Parameter	Value
Index	**6**
Name	**TS_Remove_REFERRED-BY**
Manipulation Set ID	**4**
Action Subject	**header.REFERRED-BY**
Action Type	**Remove**

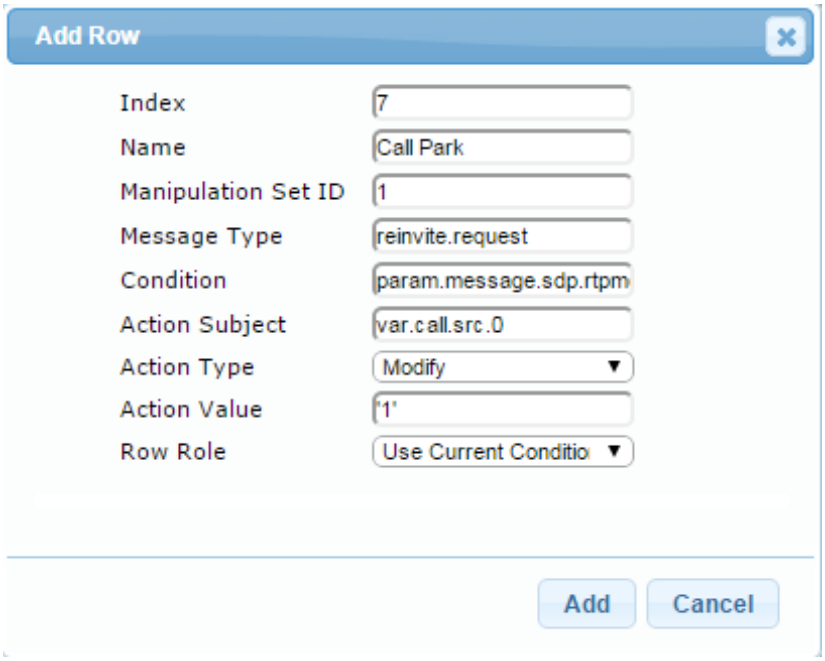
Figure 4-62: Configuring SIP Message Manipulation Rule 6 (for Telus' SIP Trunk)



8. Configure a new manipulation rule (Manipulation Set 1) for inbound processing from the Lync environment. This rule applies to messages received from the MS Lync environment in a call park scenario and hold scenarios (when music on hold is enabled). This interworking is used to identify a call state change when 'sendonly' is received within the SDP of a re-invite request. The handling will create a variable and set it to a value of '1' for further processing.

Parameter	Value
Index	**7**
Name	**Call Park**
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'**

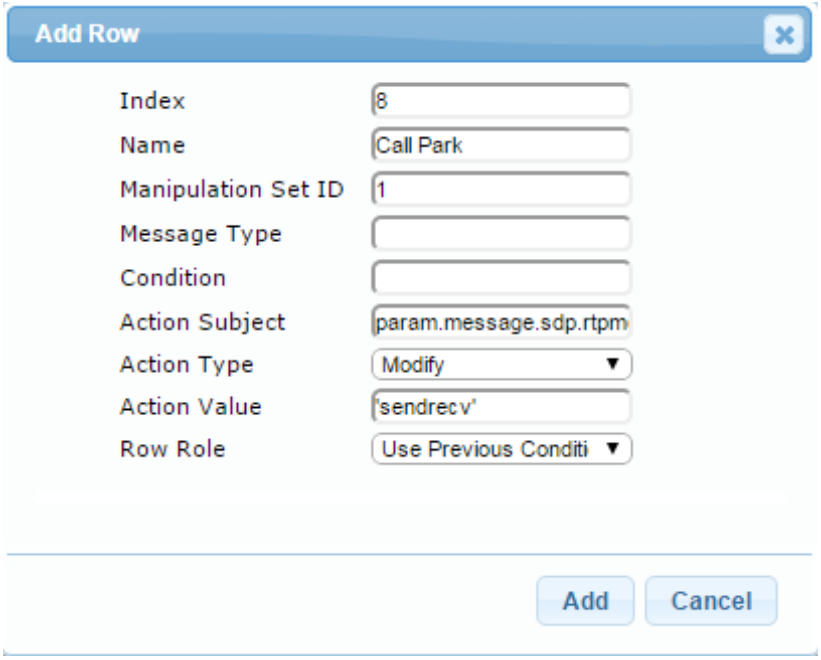
Figure 4-63: Configuring SIP Message Manipulation Rule 7 (inbound from MS Lync)



9. Configure a new manipulation rule (Manipulation Set 1) for inbound processing from the Lync environment. This rule applies to the previous rule. If the previous rule applies, then this rule continues the specific processing. This is bound by the Row Rule "Use Previous Connection'. This specific interworking sets within the SDP the 'sendrecv' for proper handling and interworking with the Telus SIP Trunk.

Parameter	Value
Index	**8**
Name	**Call Park**
Manipulation Set ID	**1**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**'sendrecv'**
Row Rule	**Use Previous Condition**

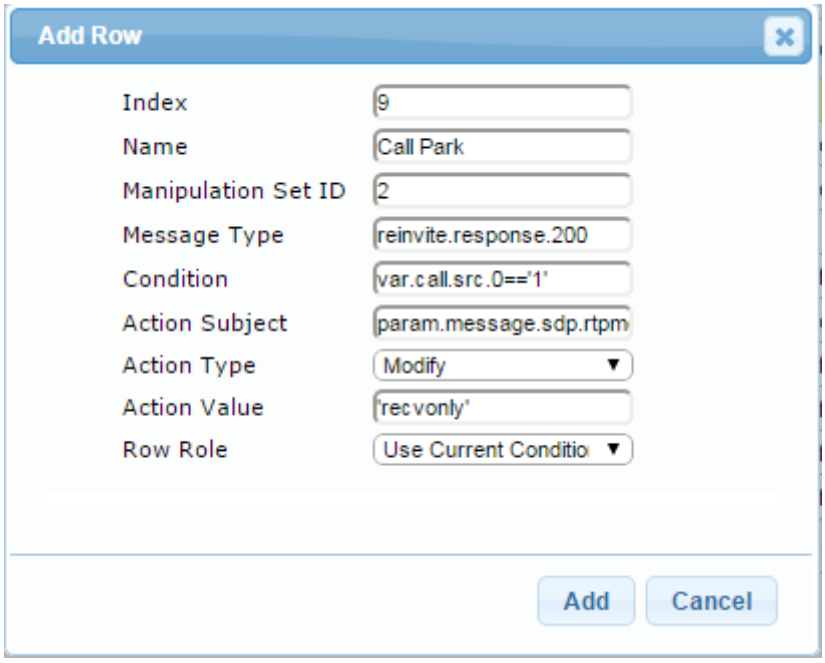
Figure 4-64: Configuring SIP Message Manipulation Rule 8 (inbound from MS Lync)



10. Configure a new manipulation rule (Manipulation Set 2) for processing towards the Lync environment. This rule applies to messages which are about to be routed to the Lync environment for Call Park and hold scenarios (when Music on Hold is enabled). This interworking specifically looks at the re-invite response (SIP 200 OK message) and checks if there was a previous variable declared and if so, if it was set to the value of **'1'**. If this scenario is a match, the SDP RTP mode is modified to 'recvonly' as the message is sent towards the Lync environment. This allows for the interworking of sendonly/rcvonly on the Lync side with the sendrcv mode on the Telus side to support Music on Hold.

Parameter	Value
Index	**9**
Name	**Call Park**
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'**

Figure 4-65: Configuring SIP Message Manipulation Rule 9 (outbound to Lync)



11. Configure a new manipulation rule (Manipulation Set 2) for outbound processing to the Lync environment. This rule applies to the previous rule. If the previous rule applies, then this rule continues the specific processing. This is bound by the Row Rule 'Use Previous Connection'. This specific interworking sets the call state variable, which was previously associated with the call scenario, to a value of **'0'** for correct handling and interworking between the Lync environment and the Telus SIP Trunk to support call park/unpark and call hold/resume scenarios.

Parameter	Value
Index	**10**
Name	**Call Park**
Manipulation Set ID	**2**
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'0'**
Row Rule	**Use Previous Condition**

Figure 4-66: Configuring SIP Message Manipulation Rule 10 (Outbound to Lync)

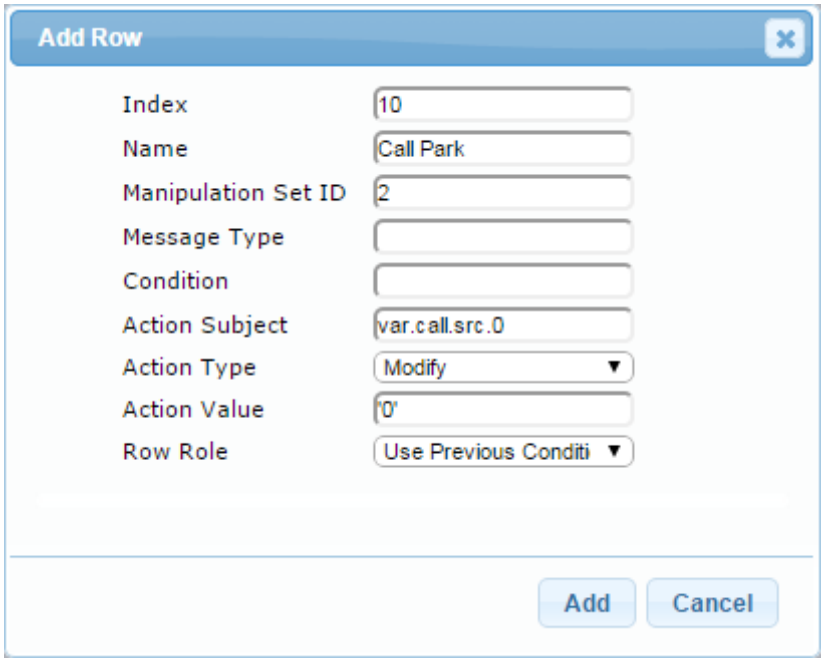
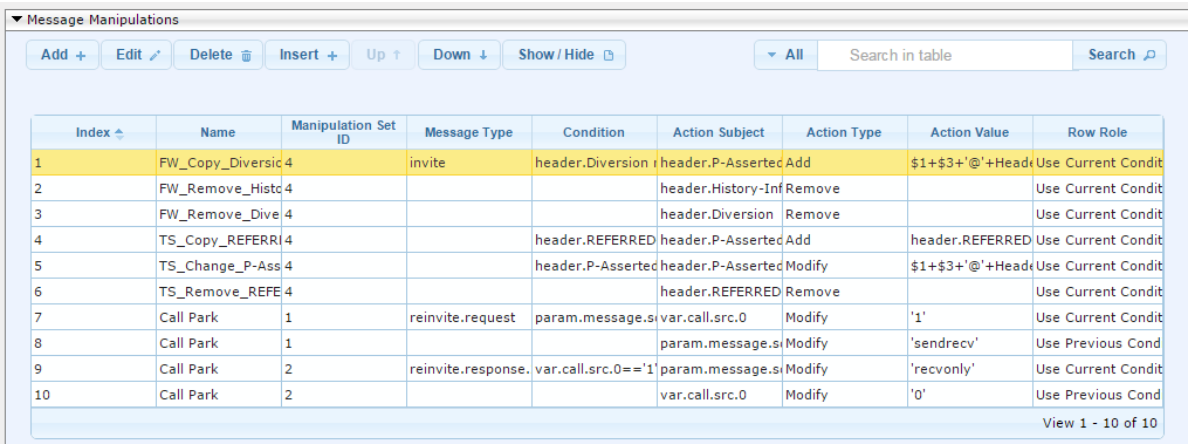


Figure 4-67: Example of Configured SIP Message Manipulation Rules



The table displayed below includes SIP message manipulation rules bound together by commonality via the Manipulation Set IDs (1, 2, and 4), executed for messages sent to and from the SIP Trunk IP Group as well as the Lync Server 2013 IP Group.

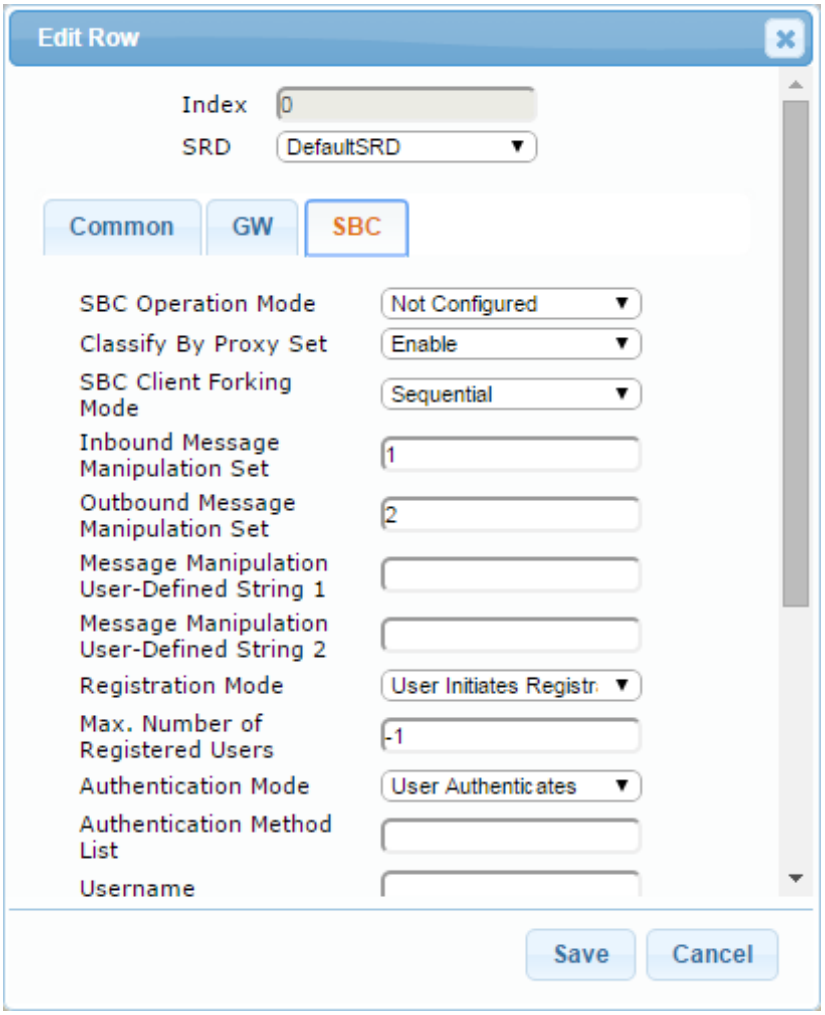
These rules are specifically required to enable correct interworking between SIP Trunk and Lync Server 2013. The specific items are needed to support Call Park and Music on Hold (rules 7-10). Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
1	This rule applies to messages sent to the SIP Trunk IP Group in a call forward scenario. This rule uses the Diversion Header to create a P-Asserted-Identity Header. It also removes the '+1' prefix and it replaces the URL Host part of the P-Asserted-Identity Header with the URL Host from the SIP From Header value.	For Call Forward scenarios, the SIP Trunk requires the User part in the SIP P-Asserted-Identity Header to be a known/defined number. To do this, the User part of the SIP Diversion Header is used to create a P-Asserted-Identity Header, while replacing the value of the URL Host with that of the From Header URL Host.
2	This rule applies to messages sent to the SIP Trunk IP Group in a call forward scenario. It removes the History-Info Header.	
3	This rule applies to messages sent to the SIP Trunk IP Group in a call forward scenario. It removes the Diversion Header.	
4	This rule applies to messages sent to Telus' SIP Trunk IP Group. If a Referred-By Header exists because of a transfer scenario, then copy the Referred-By Header URL to a newly created P-Asserted-Identity Header.	For Call Transfer initiated by Lync Server 2013, the SIP Trunk supports a P-Asserted-Identity header for transfer call scenarios. The Referred-By header received from the Lync environment needs to be used to generate the P-Asserted-Identity Header. The '+1' prefix is removed and the URL Host of the new P-Asserted-Identity header is changed to that of the From Header.
5	This rule removes prefix '+1' from the Referred-By Header and replaces the **host** part of the P-Asserted-Identity Header with the value from the SIP From Header.	
6	This rule applies to messages sent to the SIP Trunk IP Group. This rule removes the Referred-By Header from the message.	
7	For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Lync 2013-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.).	In the Call Park scenario, Microsoft Lync sends Re-INVITE messages twice. The first message is sent with the SDP, where the RTP mode is set to

Rule Index	Rule Description	Reason for Introducing Rule
8	If the previous manipulation rule (Index 0) 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".	"a=inactive". The second message is sent with "a=sendonly". The SIP Trunk has a problem recognizing two sequential Re-INVITE messages with different RTP modes. This causes the loss of the Music On Hold functionality in the Call Park scenario. These four rules are applied to work around this limitation.
9	This rule attempts to normalize the call processing state back to Lync 2013 for the correct reply to the initially received "sendonly". For every SIP Re-INVITE Response message with the variable set to **'1'**, change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent back to the Lync-initiated Hold.	
10	If the manipulation rule Index 2 (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. Lync now sends Music on Hold to the SIP Trunk even without the SIP Trunk knowing how to receive MoH. The call is now truly on hold with MoH and calls can be Park/unParked or Held/Resumed repeatedly while maintaining control of the call scenario.	

12. Assign Manipulation Set IDs 1 and 2 to the Lync 2013 IP Group:
    a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
    b. Select the row of the Lync 2013 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**.

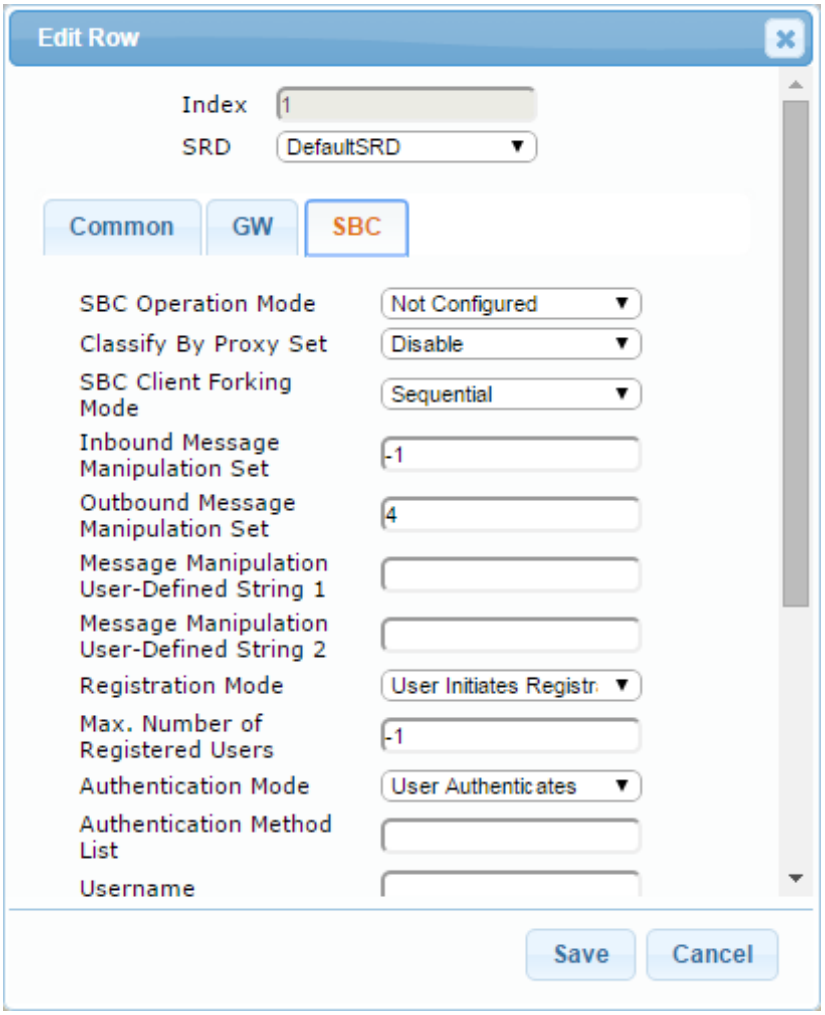
Figure 4-68: Assigning Manipulation Set to the Lync 2013 IP Group



    f. Click **Submit**.

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

Figure 4-69: Assigning Manipulation Set 4 to the SIP Trunk IP Group



    e. Click **Submit**.

4.15 Step 15: Configure Miscellaneous Settings

This section describes configuring miscellaneous E-SBC settings.

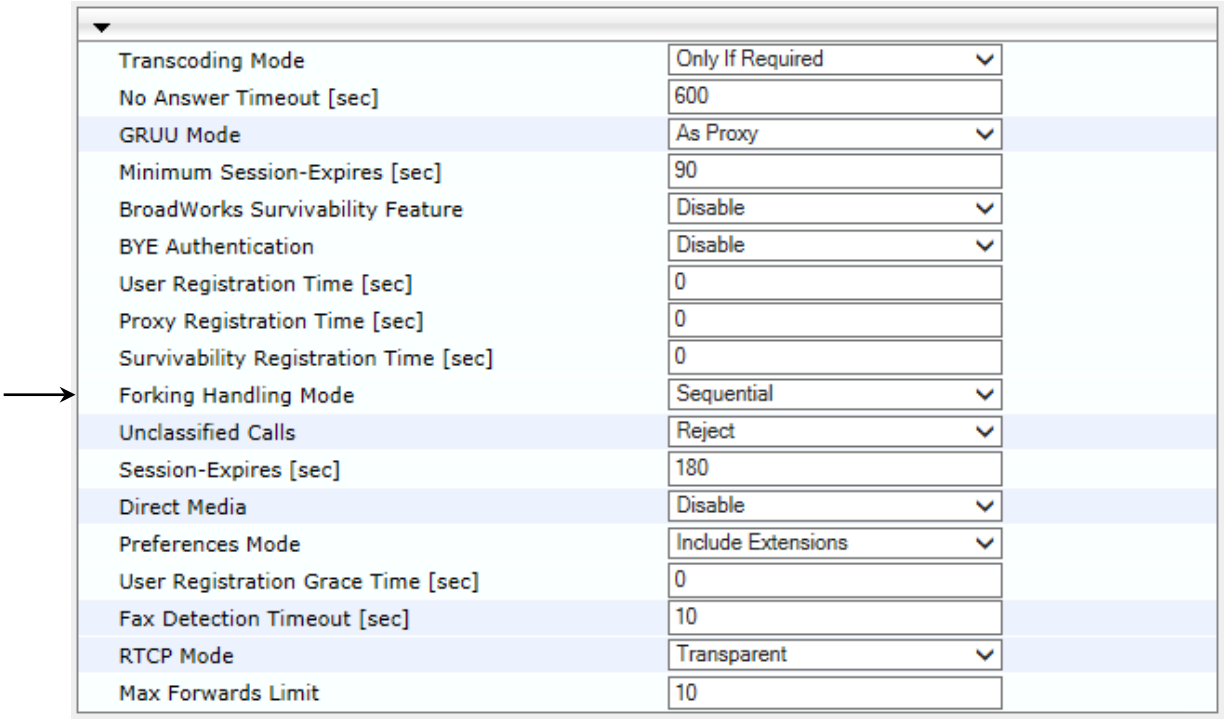
4.15.1 Step 15a: Configure Call Forking Mode

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 Lync Server 2013 environment.

➢ **To configure call forking:**

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

Figure 4-70: Configuring Forking Mode



3. Click **Submit**.

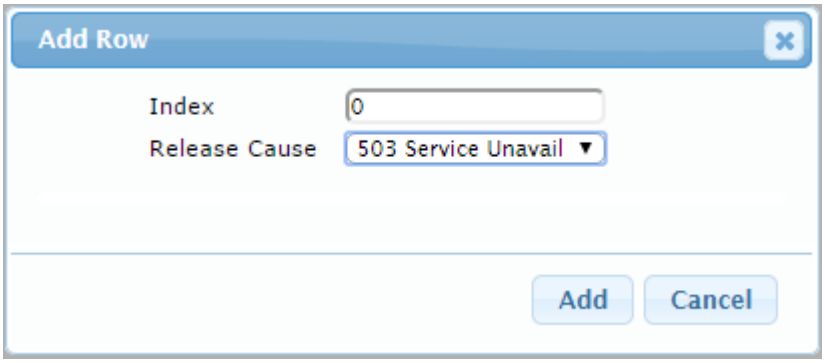
4.15.2 Step 15b: Configure SBC Alternative Routing Reasons

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 4-71: SBC Alternative Routing Reasons Table - Add Record



3. Click **Submit**.

4.15.3 Step 15c: Configure Registration Accounts

Note: Following step applicable only for internet registration based topology.

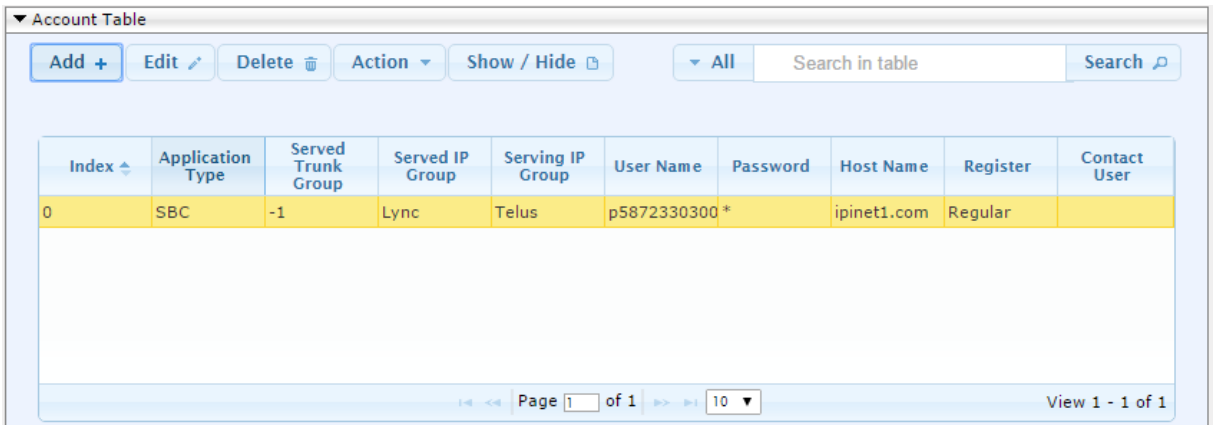
This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the Telus SIP Trunk on behalf of Lync Server 2013. The Telus SIP Trunk requires registration and authentication to provide service in the internet registration-based topology.

In the interoperability test topology, the Served IP Group is Lync Server 2013 (Lync IP Group) and the Serving IP Group is Telus SIP Trunk (Telus IP Group).

➢ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).

Figure 4-72: Configuring SIP Registration Account



2. Click **Add**.
3. Configure the account according to the provided information from Telus, for example:

Parameter	Value
Served IP Group	**Lync**
Serving IP Group	**Telus**
Username	As provided by ITSP
Password	As provided by ITSP
Host Name	**ipinet1.com** (as provided by ITSP)
Register	**Regular**
Contact User	**p5872330300** (trunk pilot user, as provided by ITSP)
Application Type	**SBC**

4. Click **Apply**.

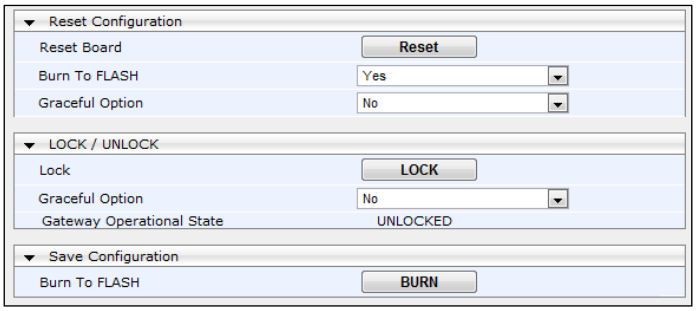
4.16 Step 16: Reset the E-SBC

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 4-73: Resetting the E-SBC



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

A AudioCodes INI file for VPN-based Configuration

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

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

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

;Board: Mediant 1000
;HW Board Type: 47  FK Board Type: 71
;Serial Number: 5702238
;Slot Number: 1
;Software Version: 7.00A.017.012
;DSP Software Version: 624AE3=> 660.13
;Board IP Address: 10.15.45.32
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 496M   Flash size: 64M
;Num of DSP Cores: 20  Num DSP Channels: 120
;Num of physical LAN ports: 3
;Profile: NONE
;;Key features:;Board Type: Mediant 1000 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;PSTN FALLBACK Supported
;E1Trunks=4 ;T1Trunks=4 ;FXSPorts=20 ;FXOPorts=20 ;IP Media: Conf ;DSP
Voice features: RTCP-XR ;Eth-Port=6 ;DATA features: ;Channel Type: RTP
DspCh=120 IPMediaDspCh=120 ;HA ;Coders: G723 G729 G728 NETCODER GSM-FR
GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB
MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB ;QOE
features: VoiceQualityMonitoring MediaEnhancement ;Control Protocols:
MSFT CLI TRANSCODING=120 FEU=120 TestCall=1000 SIPRec=120 CODER-
TRANSCODING=120 EMS SBC-SIGNALING=120 SBC-MEDIA=120 WebRTC ELIN MGCP SIP
SBC=120 ;Default features:;Coders: G711 G726;

;---------  HW components ---------
;
; Slot # : Module type : # of ports : # of DSPs
;-----------------------------------------------
;      1 : FALC56      :          4 :         5
;      2 : Empty
;      3 : Empty
;      4 : Empty
;      5 : Empty
;      6 : Empty
;-----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.133.4.105
```

```
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
DebugRecordingDestIP = 10.133.4.22
;VpFileLastUpdateTime is hidden but has non-default value
DebugRecordingStatus = 1
NTPServerIP = '10.15.25.1'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
DisableICMPRedirects = 1
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

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

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

WebLogoText = 'TELUS'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
HTTPSCipherString = 'RC4:EXP'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value
```

```
[SIP Params]

MEDIACHANNELS = 120
SECURECALLSFROMIP = 1
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
SIPTRANSPORTTYPE = 2
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLEEARLY183 = 1
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10485760
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]


[VXML Params]

[IPsec Params]


[Audio Staging Params]


[SNMP Params]

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_0_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 4, "User Port #1", "GROUP_2",
"Active";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 1, "GE_0_1", "";
EtherGroupTable 1 = "GROUP_2", 1, "GE_0_2", "";

[ \EtherGroupTable ]

[ DeviceTable ]

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

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

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.45.32, 16, 10.15.0.1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 192.168.0.2, 24, 192.168.0.1, "Telus", 0.0.0.0,
0.0.0.0, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

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

[ \DspTemplates ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$oMbDkJDAlZWSm8vOmcrLn5uCg9TR0dOFg4zdi4Pe39+NpfPw9/Xx9aP4/a78+Pv8+eG0t
uXh7eDh4ODt7eW86Lo=", 1, 0, 2, 15, 60, 200,
"653ca73b76fc550875e6d161e22a7eb3";
WebUsers 1 = "User",
"$1$K00cFB9OAQIBCgYDAgUJAQ1ZDQhYXXR3e3BwciJ+fit4KS96LC1kaGtnN2AyY2k8OTlvb
246BVlbUlNRA15aUFM=", 1, 0, 2, 15, 60, 50,
"fd54bdb898dd1b65a86d1f64483f4d57";

[ \WebUsers ]

[ TLSContexts ]

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

[ \TLSContexts ]

[ IpProfile ]
```

```
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "audio", -1, -1, 0,
1, 1, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 0, 1, 0, 3, 2, 1,
0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 101, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 250, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 2 = "Telus", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0,
0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, "", 2, -1, 0, 2,
0, 0, 1, 0, 8, 300, 400, 1, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1, 1, 3, 0, 1, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0,
0, 0, 250, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
```

```
IpProfile 3 = "fax", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 250, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;

[ \IpProfile ]

[ CpMediaRealm ]

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

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]

[ SRD ]

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

[ \SRD ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer;
SIPInterface 0 = "Lync", "Voice", 2, 5060, 5068, 5067, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "Lync", 0, -1, -1, -1, 0;
SIPInterface 1 = "TELUS", "Telus", 2, 5060, 0, 0, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "TELUS", 0, -1, -1, -1, 0;

[ \SIPInterface ]

[ ProxySet ]
```

```
FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "Lync", 1, 60, 1, 1, "DefaultSRD", 0, "default", 1, -1, "",
"", "Lync", "", "", "", "";
ProxySet 1 = "Telus", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"TELUS", "", "", "", "";
ProxySet 2 = "fax", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"Lync", "", "", "", "";

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 0 = 0, "Lync", "Lync", "AC.test", "", -1, 0, "DefaultSRD",
"Lync", 1, "Lync", -1, 1, 2, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0;
IPGroup 1 = 0, "Telus", "Telus", "ITSP.test", "", -1, 0, "DefaultSRD",
"TELUS", 0, "Telus", -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==",
0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0;
IPGroup 2 = 0, "fax", "fax", "AC.test", "", -1, 0, "DefaultSRD", "Lync",
1, "fax", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
"", 0, "", "", 0, 0, "", 0, 0, -1, 0;

[ \IPGroup ]

[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "10.15.25.2:5067", 2;
ProxyIp 1 = "1", 0, "192.168.1.41:5060", 0;
```

```
ProxyIp 2 = "2", 0, "10.133.4.101:5060", 0;

[ \ProxyIp ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS Terminate", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "";
IP2IPRouting 1 = "Lync to TELUS", "Default_SBCRoutingPolicy", "Lync",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "Telus", "", "", 0, -1, 0, 0,
"";
IP2IPRouting 2 = "telus to fax", "Default_SBCRoutingPolicy", "Telus",
"*", "*", "5872330373", "*", 0, "", "Any", 0, -1, 0, "fax", "", "", 0, -
1, 0, 0, "";
IP2IPRouting 3 = "TELUS to Lync", "Default_SBCRoutingPolicy", "Telus",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "Lync", "", "", 0, -1, 0, 0,
"";
IP2IPRouting 4 = "fax to telus", "Default_SBCRoutingPolicy", "fax", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "Telus", "", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]

[ Classification ]

FORMAT Classification_Index = Classification_ClassificationName,
Classification_MessageConditionName, Classification_SRDName,
Classification_SrcSIPInterfaceName, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePrefix, Classification_SrcHost,
Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupName,
Classification_DestRoutingPolicy, Classification_IpProfileName;
Classification 1 = "Telus", "", "DefaultSRD", "TELUS", "192.168.1.41",
5060, 0, "*", "*", "*", "*", 1, "Telus", "", "";

[ \Classification ]


[ IPOutboundManipulation ]

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

```
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = "out Telus", "Default_SBCRoutingPolicy", 0,
"Lync", "Telus", "+1", "*", "*", "*", "*", "", 0, "Any", 0, 0, 2, 0, 255,
"", "", 0;
IPOutboundManipulation 1 = "out Telus2", "Default_SBCRoutingPolicy", 0,
"Lync", "Telus", "*", "*", "+1", "*", "*", "", 0, "Any", 0, 1, 2, 0, 255,
"", "", 0;
IPOutboundManipulation 2 = "in Telus", "Default_SBCRoutingPolicy", 0,
"Telus", "Lync", "*", "*", "*", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255,
"+1", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0, "";
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup0 2 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup0 ]

[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 0, "";

[ \CodersGroup1 ]

[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce,
CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup2 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup2 ]

[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";
AllowedCodersGroup2 1 = "g711Ulaw64k";

[ \AllowedCodersGroup2 ]
```

```
[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 1 = "FW_Copy_Diversion_2_P-Asserted", 4, "invite",
"header.Diversion regex.(.*)(\+1)(.*)(@)(.*)", "header.P-Asserted-
Identity", 0, "$1+$3+'@'+Header.from.url.host+';user=phone>'", 0;
MessageManipulations 2 = "FW_Remove_History", 4, "", "", "header.History-
Info", 1, "", 0;
MessageManipulations 3 = "FW_Remove_Diversion", 4, "", "",
"header.Diversion", 1, "", 0;
MessageManipulations 4 = "TS_Copy_REFERRED-BY_2_P-Asserted", 4, "",
"header.REFERRED-BY exists", "header.P-Asserted-Identity", 0,
"header.REFERRED-BY.url", 0;
MessageManipulations 5 = "TS_Change_P-Asserted", 4, "", "header.P-
Asserted-Identity regex.(.*)(\+1)(.*)(@)(.*)", "header.P-Asserted-
Identity", 2, "$1+$3+'@'+Header.from.url.host+';user=phone>'", 0;
MessageManipulations 6 = "TS_Remove_REFERRED-BY", 4, "", "",
"header.REFERRED-BY", 1, "", 0;
MessageManipulations 7 = "Call Park", 1, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2, "'1'", 0;
MessageManipulations 8 = "Call Park", 1, "", "",
"param.message.sdp.rtpmode", 2, "'sendrecv'", 1;
MessageManipulations 9 = "Call Park", 2, "reinvite.response.200",
"var.call.src.0=='1'", "param.message.sdp.rtpmode", 2, "'recvonly'", 0;
MessageManipulations 10 = "Call Park", 2, "", "", "var.call.src.0", 2,
"'0'", 1;

[ \MessageManipulations ]


[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]
```

B AudioCodes INI file for Internet Registration-based Configuration

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

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

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

;Board: Mediant 1000
;HW Board Type: 47  FK Board Type: 71
;Serial Number: 5702238
;Slot Number: 1
;Software Version: 7.00A.019.010
;DSP Software Version: 624AE3=> 660.14
;Board IP Address: 10.15.45.32
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 496M   Flash size: 64M
;Num of DSP Cores: 20  Num DSP Channels: 120
;Num of physical LAN ports: 3
;Profile: NONE
;;Key features:;Board Type: Mediant 1000 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;PSTN FALLBACK Supported
;E1Trunks=4 ;T1Trunks=4 ;FXSPorts=20 ;FXOPorts=20 ;IP Media: Conf ;DSP
Voice features: RTCP-XR ;Eth-Port=6 ;DATA features: ;Channel Type: RTP
DspCh=120 IPMediaDspCh=120 ;HA ;Coders: G723 G729 G728 NETCODER GSM-FR
GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB
MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB ;QOE
features: VoiceQualityMonitoring MediaEnhancement ;Control Protocols:
MSFT CLI TRANSCODING=120 FEU=120 TestCall=1000 SIPRec=120 CODER-
TRANSCODING=120 EMS SBC-SIGNALING=120 SBC-MEDIA=120 WebRTC ELIN MGCP SIP
SBC=120 ;Default features:;Coders: G711 G726;

;---------  HW components ---------
;
; Slot # : Module type : # of ports : # of DSPs
;-----------------------------------------------
;      1 : FALC56      :          4 :         5
;      2 : Empty
;      3 : Empty
;      4 : Empty
;      5 : Empty
;      6 : Empty
;-----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.133.4.107
```

```
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
DebugRecordingDestIP = 10.133.4.107
;VpFileLastUpdateTime is hidden but has non-default value
DebugRecordingStatus = 1
NTPServerIP = '10.15.25.1'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
DisableICMPRedirects = 1
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

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

[PSTN Params]


[SS7 Params]


[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

WebLogoText = 'TELUS'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
```

```
HTTPSCipherString = 'RC4:EXP'
;HTTPSPkeyFileName is hidden but has non-default value
;HTTPSCertFileName is hidden but has non-default value

[SIP Params]

MEDIACHANNELS = 120
SECURECALLSFROMIP = 1
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
SIPTRANSPORTTYPE = 2
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLEEARLY183 = 1
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10485760
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]


[VXML Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_0_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 4, "User Port #1", "GROUP_2",
"Active";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 1, "GE_0_1", "";
EtherGroupTable 1 = "GROUP_2", 1, "GE_0_2", "";

[ \EtherGroupTable ]
```

```
[ DeviceTable ]

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

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.45.32, 16, 10.15.0.1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 192.168.0.2, 24, 192.168.0.1, "Telus", 0.0.0.0,
0.0.0.0, "vlan 2";

[ \InterfaceTable ]


[ DspTemplates ]

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

[ \DspTemplates ]


[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$oMbDkJDAlZWSm8vOmcrLn5uCg9TR0dOFg4zdi4Pe39+NpfPw9/Xx9aP4/a78+Pv8+eG0t
uXh7eDh4ODt7eW86Lo=", 1, 0, 2, 15, 60, 200,
"653ca73b76fc550875e6d161e22a7eb3";
WebUsers 1 = "User",
"$1$K00cFB9OAQIBCgYDAgUJAQ1ZDQhYXXR3e3BwciJ+fit4KS96LC1kaGtnN2AyY2k8OTlvb
246BVlbUlNRA15aUFM=", 1, 0, 2, 15, 60, 50,
"fd54bdb898dd1b65a86d1f64483f4d57";

[ \WebUsers ]


[ TLSContexts ]
```

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

[ \TLSContexts ]


[ IpProfile ]

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

```
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "audio", -1, -1, 0,
1, 1, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 0, 1, 0, 3, 2, 1,
0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 101, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 250, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 2 = "Telus", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0,
0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, "", 2, -1, 0, 2,
0, 0, 1, 0, 8, 300, 400, 1, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1, 1, 3, 0, 1, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0,
0, 0, 250, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 3 = "fax", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 250, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;

[ \IpProfile ]


[ CpMediaRealm ]

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

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]


[ SRD ]

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

[ \SRD ]


[ SIPInterface ]

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

```
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer;
SIPInterface 0 = "Lync", "Voice", 2, 5060, 5068, 5067, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "Lync", 0, -1, -1, -1, 0;
SIPInterface 1 = "TELUS", "Telus", 2, 5060, 0, 5061, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "TELUS", 0, -1, -1, -1, 0;

[ \SIPInterface ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "Lync", 1, 60, 1, 1, "DefaultSRD", 0, "default", 1, -1, "",
"", "Lync", "", "", "", "";
ProxySet 1 = "Telus", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"TELUS", "", "", "", "";
ProxySet 2 = "fax", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"Lync", "", "", "", "";
ProxySet 3 = "TELUS Internet", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1,
"", "", "TELUS", "", "", "", "";

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 0 = 0, "Lync", "Lync", "AC.test", "", -1, 0, "DefaultSRD",
"Lync", 1, "Lync", -1, 1, 2, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0;
IPGroup 1 = 0, "Telus", "Telus", "ITSP.test", "", -1, 0, "DefaultSRD",
"TELUS", 0, "Telus", -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==",
0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0;
```

```
IPGroup 2 = 0, "fax", "fax", "AC.test", "", -1, 0, "DefaultSRD", "Lync",
1, "fax", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
"", 0, "", "", 0, 0, "", 0, 0, -1, 0;
IPGroup 3 = 0, "TELUS Internet", "TELUS Internet", "ipinet1.com", "", -1,
0, "DefaultSRD", "TELUS", 1, "Telus", -1, -1, 4, 0, 0, "", 0, -1, -1,
"ipnet.com", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1,
0;

[ \IPGroup ]


[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "10.15.25.2:5067", 2;
ProxyIp 1 = "1", 0, "192.168.1.49:5060", 0;
ProxyIp 2 = "2", 0, "10.133.4.101:5060", 0;
ProxyIp 3 = "3", 0, "209.91.75.37", 0;

[ \ProxyIp ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "Lync", "TELUS Internet", "p5872330300",
"$1$pJWXlZOdyMjI", "ipinet1.com", 1, "p5872330300", 2;

[ \Account ]


[ IP2IPRouting ]

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

```
IP2IPRouting 1 = "Lync to TELUS", "Default_SBCRoutingPolicy", "Lync",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "Telus", "", "", 0, -1, 0, 0,
"";
IP2IPRouting 2 = "Lync to TELUS Internet", "Default_SBCRoutingPolicy",
"Lync", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "TELUS Internet", "",
"", 0, -1, 1, 0, "";
IP2IPRouting 3 = "telus to fax", "Default_SBCRoutingPolicy", "Telus",
"*", "*", "5872330374", "*", 0, "", "Any", 0, -1, 0, "fax", "", "", 0, -
1, 0, 0, "";
IP2IPRouting 4 = "TELUS to Lync", "Default_SBCRoutingPolicy", "Telus",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "Lync", "", "", 0, -1, 0, 0,
"";
IP2IPRouting 5 = "fax to telus", "Default_SBCRoutingPolicy", "fax", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "Telus", "", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]


[ Classification ]

FORMAT Classification_Index = Classification_ClassificationName,
Classification_MessageConditionName, Classification_SRDName,
Classification_SrcSIPInterfaceName, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePrefix, Classification_SrcHost,
Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupName,
Classification_DestRoutingPolicy, Classification_IpProfileName;
Classification 1 = "Telus", "", "DefaultSRD", "TELUS", "192.168.1.41",
5060, 0, "*", "*", "*", "*", 1, "Telus", "", "";

[ \Classification ]


[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = "out Telus", "Default_SBCRoutingPolicy", 0,
"Lync", "Telus", "+1587", "*", "*", "*", "*", "", 0, "Any", 0, 0, 2, 0,
255, "", "", 0;
IPOutboundManipulation 1 = "out Telus2", "Default_SBCRoutingPolicy", 0,
"Lync", "Telus", "*", "*", "+85551", "*", "*", "", 0, "Any", 0, 1, 0, 0,
0, "12142911029", "", 0;
```

```
IPOutboundManipulation 2 = "in Telus", "Default_SBCRoutingPolicy", 0,
"Telus", "Lync", "*", "*", "*", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255,
"+1", "", 0;
IPOutboundManipulation 3 = "in Telus2", "Default_SBCRoutingPolicy", 0,
"Telus", "Lync", "xxxxxxxxxxx", "*", "*", "*", "*", "", 0, "Any", 0, 0,
0, 0, 255, "+", "", 0;
IPOutboundManipulation 4 = "out Telus3", "Default_SBCRoutingPolicy", 0,
"Lync", "Telus", "*", "*", "+85557", "*", "*", "", 0, "Any", 0, 1, 5, 0,
255, "1732", "", 0;
IPOutboundManipulation 5 = "in Telus3", "Default_SBCRoutingPolicy", 0,
"Telus", "Lync", "*", "*", "*", "*", "*", "", 0, "Any", 0, 0, 0, 0, 255,
"", "", 0;
IPOutboundManipulation 6 = "out Telus forward",
"Default_SBCRoutingPolicy", 0, "Lync", "Telus", "*", "*", "+85551", "*",
"*", "", 0, "Any", 0, 1, 6, 0, 255, "", "", 0;
IPOutboundManipulation 7 = "out Telus Internet",
"Default_SBCRoutingPolicy", 0, "Lync", "TELUS Internet", "+1", "*", "*",
"*", "*", "", 0, "Any", 0, 0, 2, 0, 255, "", "", 0;
IPOutboundManipulation 8 = "out Telus Internet 2",
"Default_SBCRoutingPolicy", 0, "Lync", "TELUS Internet", "*", "*",
"+85551", "*", "*", "", 0, "Any", 0, 1, 6, 0, 255, "12142911029", "", 0;
IPOutboundManipulation 9 = "in Telus Internet",
"Default_SBCRoutingPolicy", 0, "TELUS Internet", "Lync", "*", "*", "*",
"*", "*", "", 0, "Any", 0, 1, 0, 0, 255, "+1", "", 0;

[ \IPOutboundManipulation ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0, "";
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup0 2 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup0 ]


[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 0, "";

[ \CodersGroup1 ]


[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce,
CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup2 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup2 ]
```

```
[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";
AllowedCodersGroup2 1 = "g711Ulaw64k";

[ \AllowedCodersGroup2 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 1 = "FW_Copy_Diversion_2_P-Asserted", 4, "invite",
"header.Diversion regex.(.*)(\+1)(.*)(@)(.*)", "header.P-Asserted-
Identity", 0, "$1+$3+'@'+Header.from.url.host+';user=phone>'", 0;
MessageManipulations 2 = "FW_Remove_History", 4, "", "", "header.History-
Info", 1, "", 0;
MessageManipulations 3 = "FW_Remove_Diversion", 4, "", "",
"header.Diversion", 1, "", 0;
MessageManipulations 4 = "TS_Copy_REFERRED-BY_2_P-Asserted", 4, "",
"header.REFERRED-BY exists", "header.P-Asserted-Identity", 0,
"header.REFERRED-BY.url", 0;
MessageManipulations 5 = "TS_Change_P-Asserted", 4, "", "header.P-
Asserted-Identity regex.(.*)(\+1)(.*)(@)(.*)", "header.P-Asserted-
Identity", 2, "$1+$3+'@'+Header.from.url.host+';user=phone>'", 0;
MessageManipulations 6 = "TS_Remove_REFERRED-BY", 4, "", "",
"header.REFERRED-BY", 1, "", 0;
MessageManipulations 7 = "Call Park", 1, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2, "'1'", 0;
MessageManipulations 8 = "Call Park", 1, "", "",
"param.message.sdp.rtpmode", 2, "'sendrecv'", 1;
MessageManipulations 9 = "Call Park", 2, "reinvite.response.200",
"var.call.src.0=='1'", "param.message.sdp.rtpmode", 2, "'recvonly'", 0;
MessageManipulations 10 = "Call Park", 2, "", "", "var.call.src.0", 2,
"'0'", 1;
MessageManipulations 11 = "Add C=1", 6, "invite",
"body.sdp==regex.(.*)(b=)(.*)", "body.sdp", 2, "$1+'c=IN IP4
10.15.45.32'+$2+$3", 0;
MessageManipulations 12 = "Add C=2", 6, "invite",
"body.sdp==regex.(.*)(\r\n)(b=)(.*)", "body.sdp", 2, "$1+$2+'c=IN IP4
10.15.45.32'+$2+$3+$4", 0;
MessageManipulations 13 = "flip_from", 7, "invite", "", "header.P-
Asserted-identity.url.user", 2, "'5872330373'", 0;
MessageManipulations 14 = "In_FW_Copy_Diversion_2_P-Asserted", 3,
"invite", "header.Diversion regex.(.*)(\+1)(.*)(@)(.*)", "header.P-
Asserted-Identity", 0, "$1+$3+'@ipnet.com;user=phone>'", 0;
MessageManipulations 15 = "In_FW_Remove_History", 3, "", "",
"header.History-Info", 1, "", 0;
MessageManipulations 16 = "In_FW_Remove_Diversion", 3, "", "",
"header.Diversion", 1, "", 0;
MessageManipulations 17 = "In_TS_Copy_REFERRED-BY_2_P-Asserted", 3, "",
"header.REFERRED-BY exists", "header.P-Asserted-Identity", 0,
"header.REFERRED-BY.url", 0;
```

```
MessageManipulations 18 = "In_TS_Change_P-Asserted", 3, "", "header.P-
Asserted-Identity regex.(.*)(\+1)(.*)(@)(.*)", "header.P-Asserted-
Identity", 2, "$1+$3+'@ipnet.com;user=phone>'", 0;
MessageManipulations 19 = "In_TS_Remove_REFERRED-BY", 3, "", "",
"header.REFERRED-BY", 1, "", 0;

[ \MessageManipulations ]


[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]


[ Test_Call ]

FORMAT Test_Call_Index = Test_Call_EndpointURI, Test_Call_CalledURI,
Test_Call_RouteBy, Test_Call_IPGroupName, Test_Call_DestAddress,
Test_Call_DestTransportType, Test_Call_SIPInterfaceName,
Test_Call_ApplicationType, Test_Call_AutoRegister, Test_Call_UserName,
Test_Call_Password, Test_Call_CallParty, Test_Call_MaxChannels,
Test_Call_CallDuration, Test_Call_CallsPerSecond, Test_Call_TestMode,
Test_Call_TestDuration, Test_Call_Play, Test_Call_ScheduleInterval,
Test_Call_QOEProfile, Test_Call_BWProfile;
Test_Call 0 = "6000", "+9001", 2, "", "10.15.25.2:5061", 2, "Lync", 0, 0,
"", "$1$gQ==", 0, 1, 20, 10, 0, 0, 0, 0, "", "";

[ \Test_Call ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

C Configuring Analog Devices (ATAs) for FAX Support

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

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

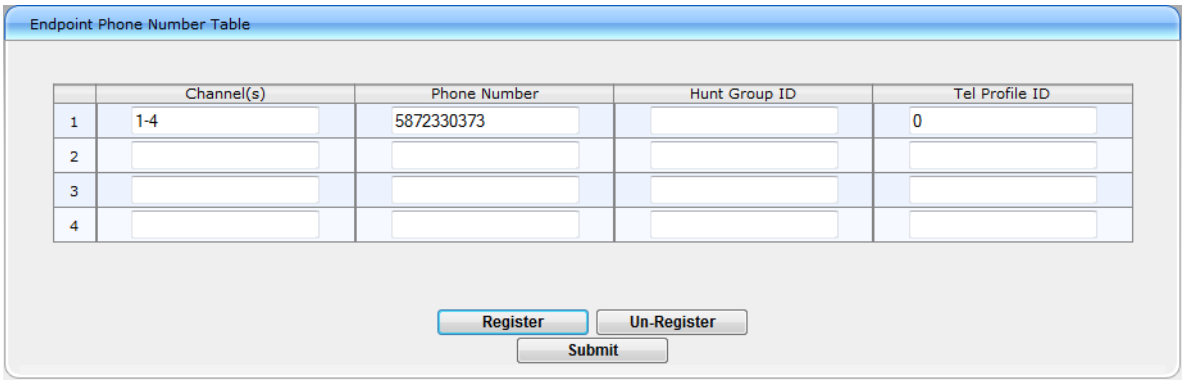
C.1 Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints) by defining telephone numbers. The configuration below uses the example of ATA destination phone number "5872330373" (IP address 10.133.4.101) with all routing directed to the SBC device (10.15.45.32).

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

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

Figure C-1: Endpoint Phone Number Table Page



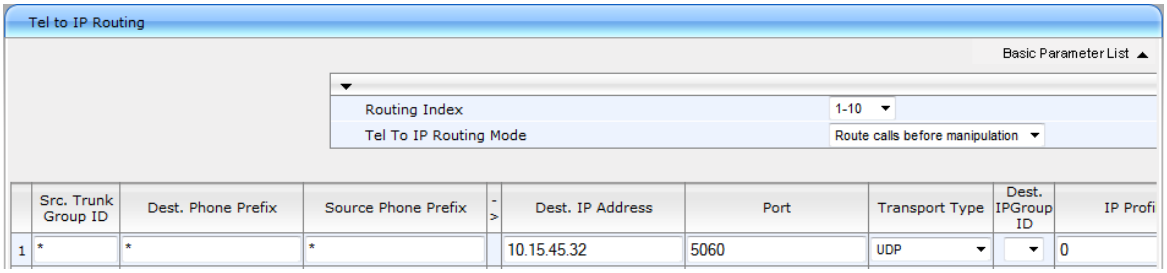
C.2 Step 2: Configure Tel to IP Routing Table

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

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

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

Figure C-2: Tel to IP Routing Page



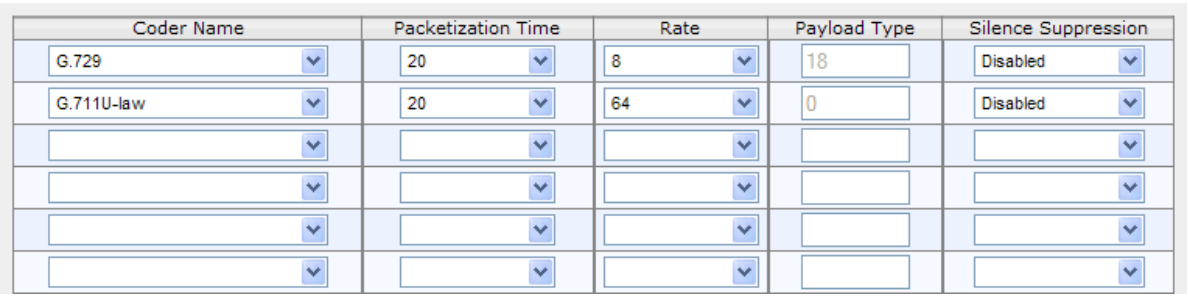
C.3 Step 3: Configure Coders Table

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

➢ **To configure MP-11x coders:**

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

Figure C-3: Coders Table Page



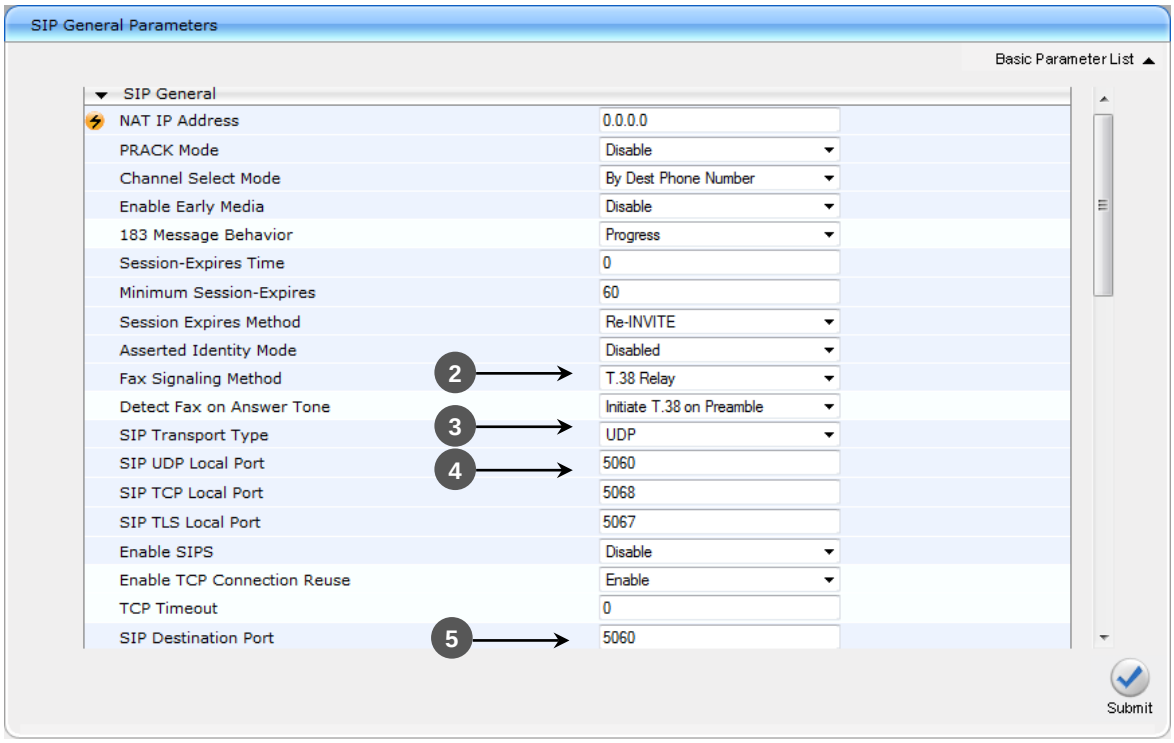
C.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

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

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

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

Figure C-4: SIP General Parameters Page



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

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

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

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-12222

AudioCodes