

Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

# Configuration Note

## Microsoft® Lync™ Server 2013 and Telavox SIP Trunk using Mediant E-SBC



**Microsoft Partner**

Gold Communications



November 2013

Document # LTRT-39330





---

## Table of Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	Intended Audience .....	7
1.2	About AudioCodes E-SBC Product Series.....	7
<b>2</b>	<b>Component Information.....</b>	<b>9</b>
2.1	AudioCodes E-SBC Version .....	9
2.2	Telavox SIP Trunking Version .....	9
2.3	Microsoft Lync Server 2013 Version .....	9
2.4	Interoperability Test Topology .....	10
2.4.1	Environment Setup .....	11
2.4.2	Known Limitations.....	11
<b>3</b>	<b>Configuring Lync Server 2013 .....</b>	<b>13</b>
3.1	Configuring the E-SBC as an IP / PSTN Gateway .....	13
3.2	Configuring the "Route" on Lync Server 2013.....	21
<b>4</b>	<b>Configuring AudioCodes E-SBC.....</b>	<b>29</b>
4.1	Step 1: IP Network Interfaces Configuration .....	30
4.1.1	Step 1a: Configure VLANs.....	31
4.1.2	Step 1b: Configure Network Interfaces.....	32
4.1.3	Step 1c: Configure the Native VLAN ID.....	34
4.2	Step 2: Enable the SBC Application .....	35
4.3	Step 3: Signaling Routing Domains Configuration .....	36
4.3.1	Step 3a: Configure Media Realms.....	36
4.3.2	Step 3b: Configure SRDs .....	38
4.3.3	Step 3c: Configure SIP Signaling Interfaces .....	39
4.4	Step 4: Configure Proxy Sets .....	41
4.5	Step 5: Configure IP Groups.....	43
4.6	Step 6: Configure IP Profiles .....	45
4.7	Step 7: Configure Coders .....	51
4.8	Step 8: SIP TLS Connection Configuration.....	52
4.8.1	Step 8a: Configure the NTP Server Address.....	52
4.8.2	Step 8b: Configure a Certificate .....	53
4.9	Step 9: Configure SRTP .....	58
4.10	Step 10: Configure Maximum IP Media Channels .....	59
4.11	Step 11: Configure IP-to-IP Call Routing Rules .....	60
4.12	Step 12: Configure IP-to-IP Manipulation Rules.....	65
4.13	Step 13: Configure Message Manipulation Rules .....	67
4.14	Step 14: Miscellaneous Configuration.....	69
4.14.1	Step 14a: Configure Call Forking Mode .....	69
4.15	Step 15: Reset the E-SBC .....	70
<b>A</b>	<b>AudioCodes INI File .....</b>	<b>71</b>

**Reader's Notes**

## Notice

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

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

**© Copyright 2013 AudioCodes Ltd. All rights reserved.**

This document is subject to change without notice.

Date Published: November-19-2013

## Trademarks

AudioCodes, AC, AudioCoded, Ardit, CTI2, CTI<sup>2</sup>, CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

## WEEE EU Directive

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

## Customer Support

Customer technical support and service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact [support@audiocodes.com](mailto:support@audiocodes.com).

## 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>.

**Reader's Notes**

# 1 Introduction

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

## 1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Telavox Partners who are responsible for installing and configuring Telavox's 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.

**Reader's Notes**

## 2 Component Information

### 2.1 AudioCodes E-SBC Version

**Table 2-1: AudioCodes E-SBC Version**

<b>SBC Vendor</b>	AudioCodes
<b>Models</b>	<ul style="list-style-type: none"> <li>▪ Mediant 800 Gateway &amp; E-SBC</li> <li>▪ Mediant 1000B Gateway &amp; E-SBC</li> <li>▪ Mediant 3000 Gateway &amp; E-SBC</li> <li>▪ Mediant 2600 E-SBC</li> <li>▪ Mediant 4000 E-SBC</li> </ul>
<b>Software Version</b>	SIP_6.80A.004.004
<b>Protocol</b>	<ul style="list-style-type: none"> <li>▪ SIP/UDP (to the Telavox SIP Trunk)</li> <li>▪ SIP/TCP or TLS (to the Lync FE Server)</li> </ul>
<b>Additional Notes</b>	None

### 2.2 Telavox SIP Trunking Version

**Table 2-2: Telavox Version**

<b>Vendor/Service Provider</b>	Telavox
<b>SSW Model/Service</b>	
<b>Software Version</b>	
<b>Protocol</b>	SIP
<b>Additional Notes</b>	None

### 2.3 Microsoft Lync Server 2013 Version

**Table 2-3: Microsoft Lync Server 2013 Version**

<b>Vendor</b>	Microsoft
<b>Model</b>	Microsoft Lync
<b>Software Version</b>	Release 2013 5.0.8308.0
<b>Protocol</b>	SIP
<b>Additional Notes</b>	None

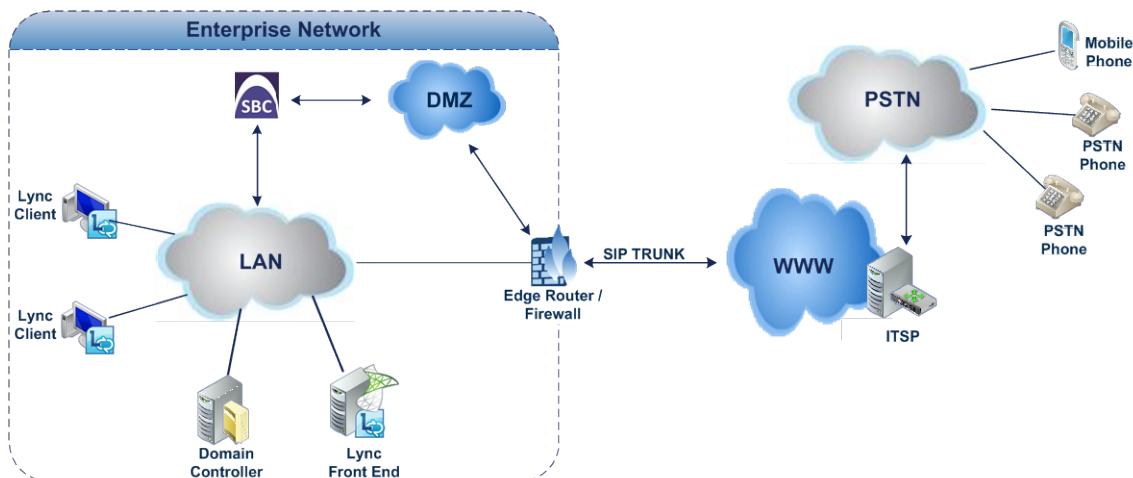
## 2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Telavox SIP Trunk with Lync 2013 was done 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 Telavox's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between Lync Server 2013 network in the Enterprise LAN and Telavox's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

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



## 2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

**Table 2-4: Environment Setup**

Area	Setup
<b>Network</b>	<ul style="list-style-type: none"><li>▪ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN</li><li>▪ Telavox SIP Trunk is located on the WAN</li></ul>
<b>Signaling Transcoding</b>	<ul style="list-style-type: none"><li>▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type</li><li>▪ Telavox SIP Trunk operates with SIP-over-UDP transport type</li></ul>
<b>Codecs Transcoding</b>	<ul style="list-style-type: none"><li>▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders</li><li>▪ Telavox SIP Trunk supports G.711A-law, G.711U-law, and GSM Full Rate coders</li></ul>
<b>Media Transcoding</b>	<ul style="list-style-type: none"><li>▪ Microsoft Lync Server 2013 operates with SRTP media type</li><li>▪ Telavox SIP Trunk operates with RTP media type</li></ul>

## 2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and Telavox's SIP Trunk.

**Reader's Notes**

## 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.

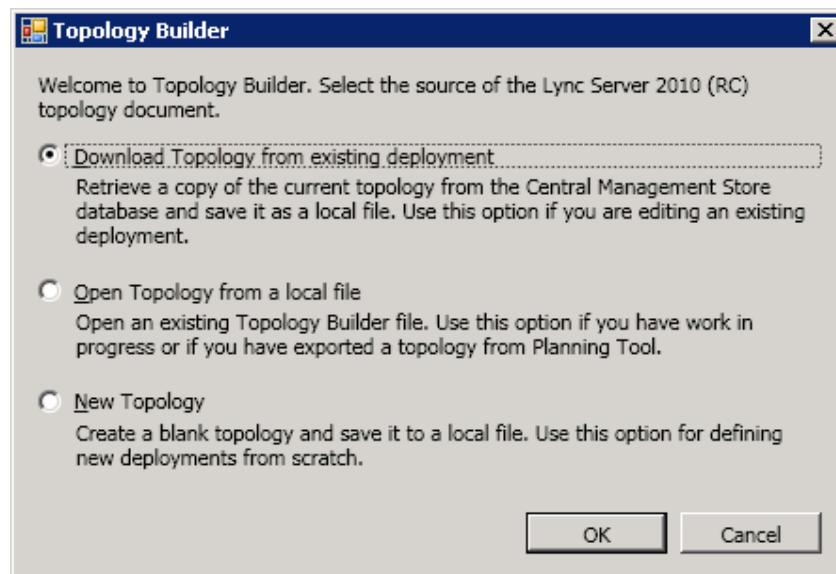
- **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows Start menu > All Programs > Lync Server Topology Builder), as shown below:

**Figure 3-1: Starting the Lync Server Topology Builder**



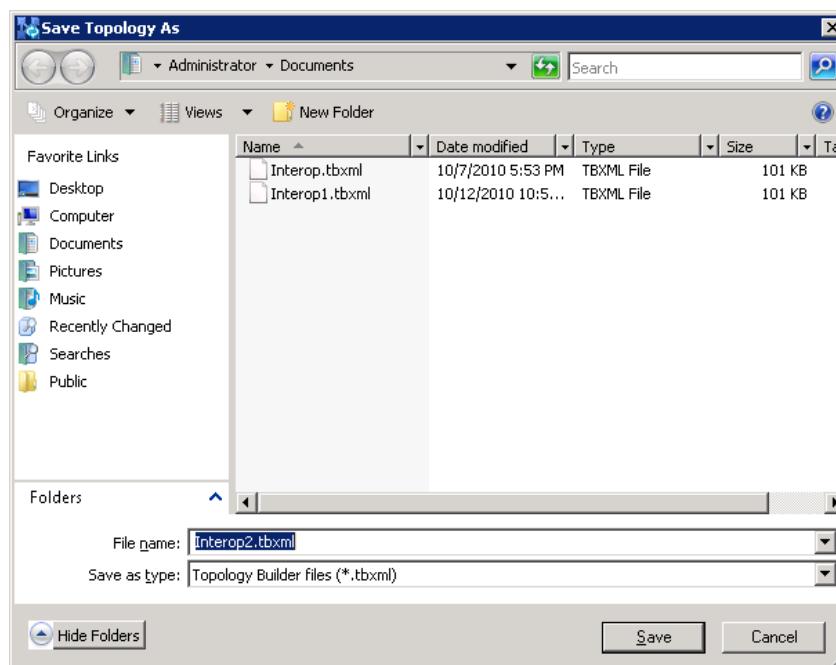
The following is displayed:

**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:

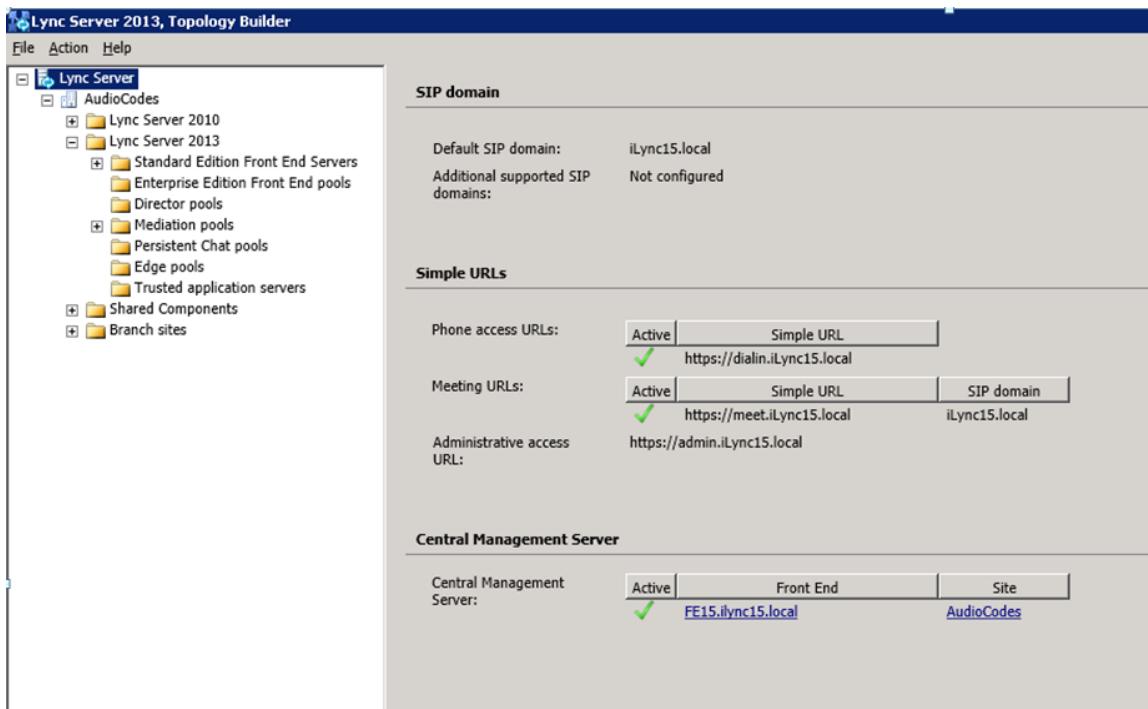
**Figure 3-3: Save Topology Dialog Box**



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.

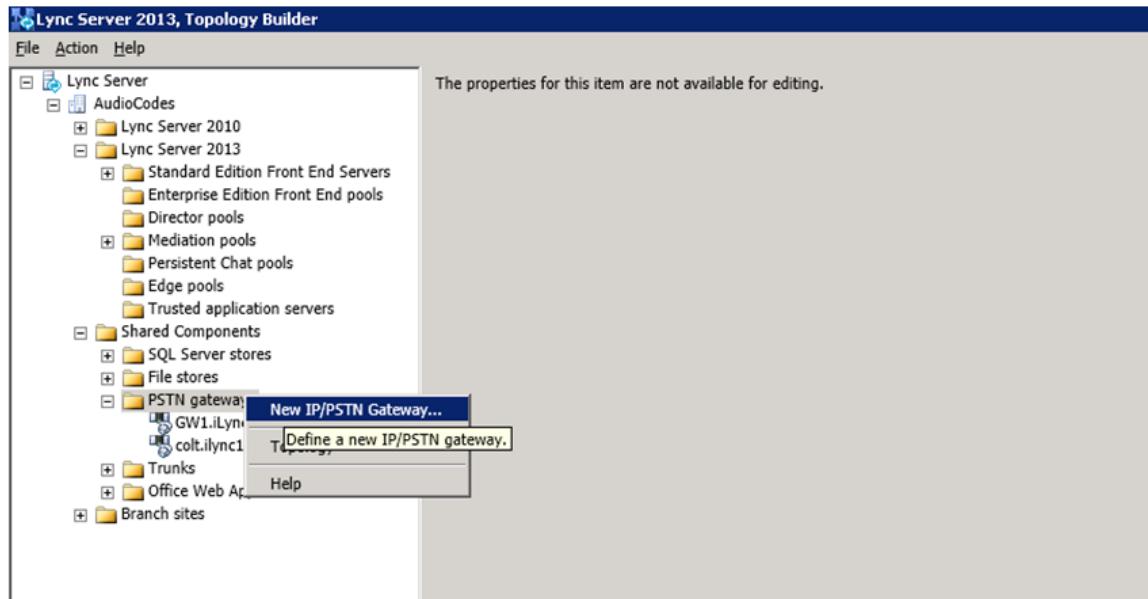
The Topology Builder screen with the downloaded Topology is displayed:

**Figure 3-4: Downloaded Topology**



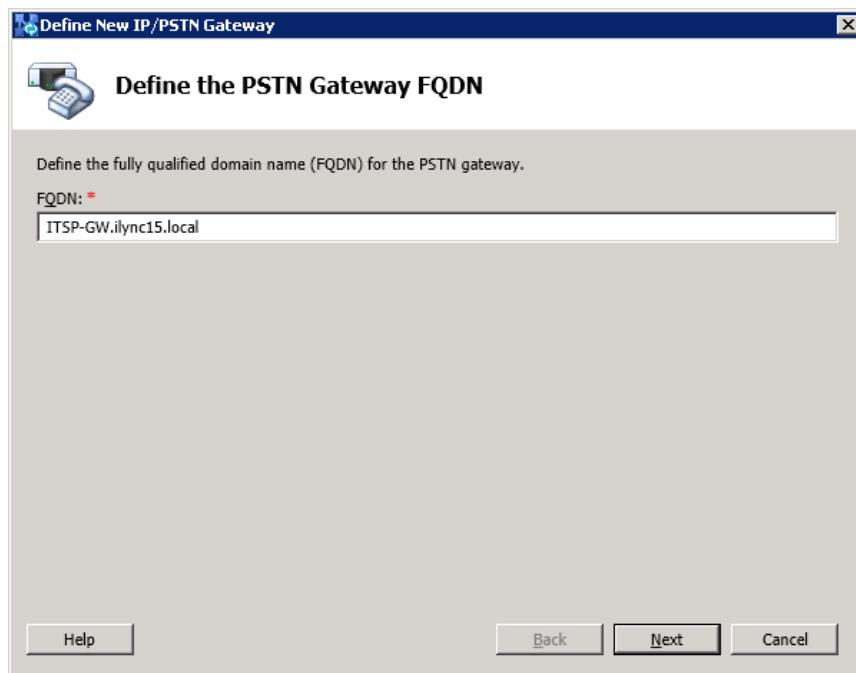
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

**Figure 3-5: Choosing New IP/PSTN Gateway**



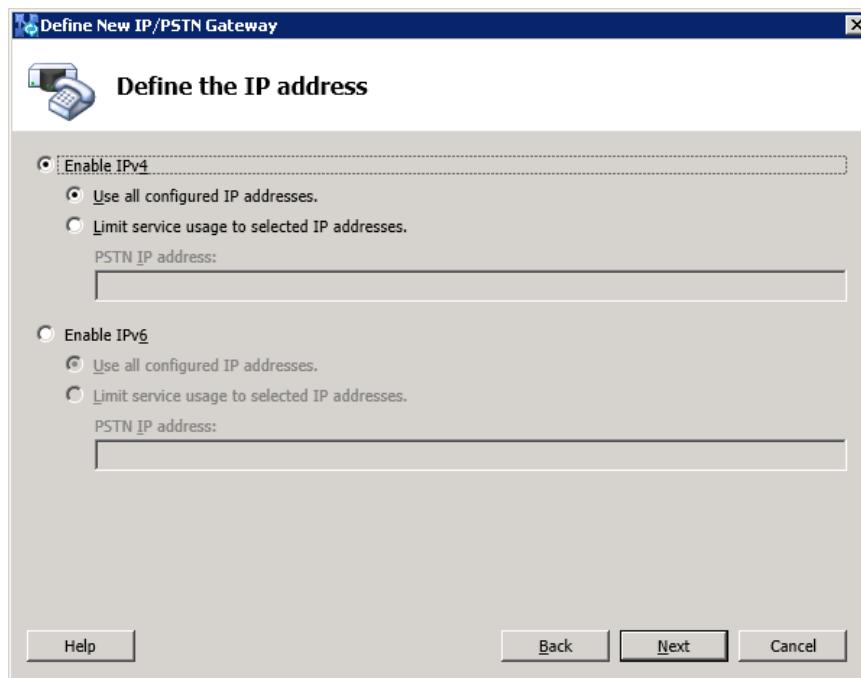
The following is displayed:

**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:

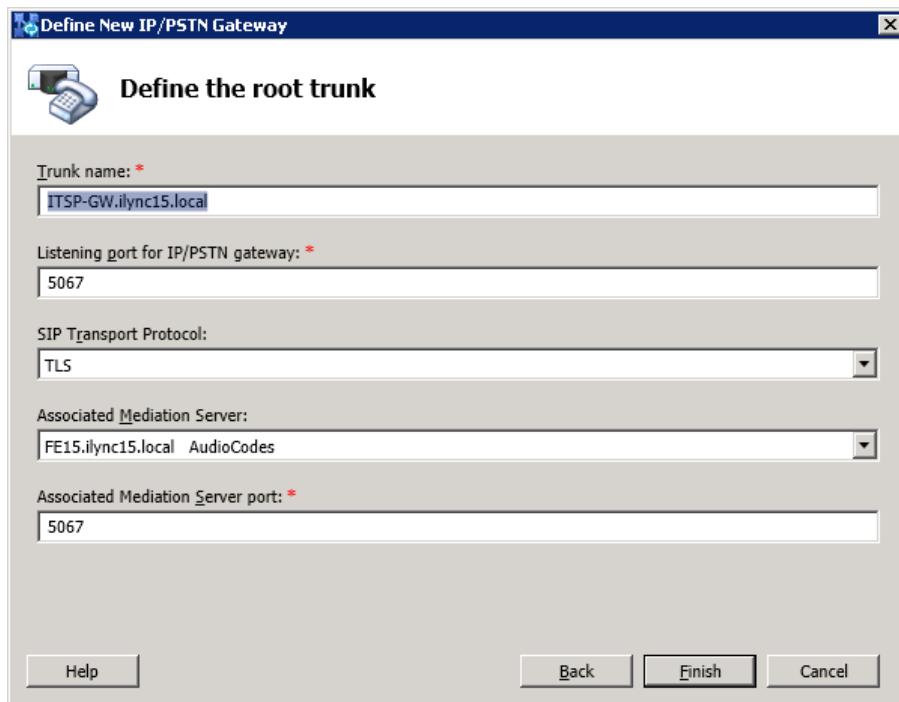
**Figure 3-7: Define the IP Address**



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:**

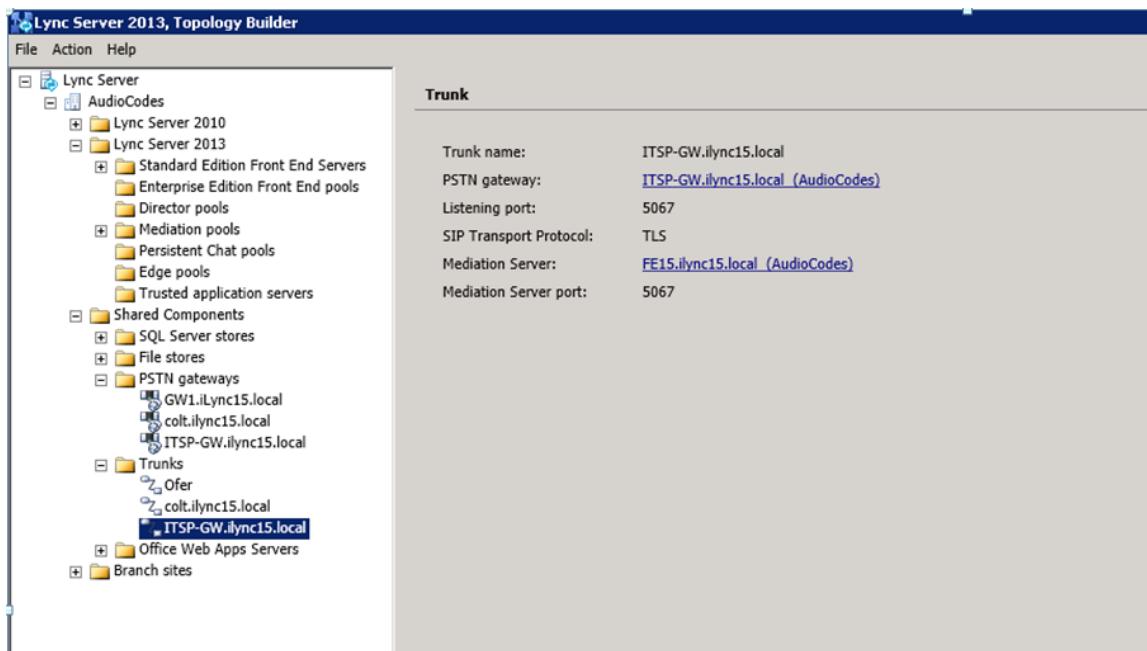
- When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
- The root trunk cannot be removed until the associated PSTN gateway is removed.

**Figure 3-8: Define the Root Trunk**

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

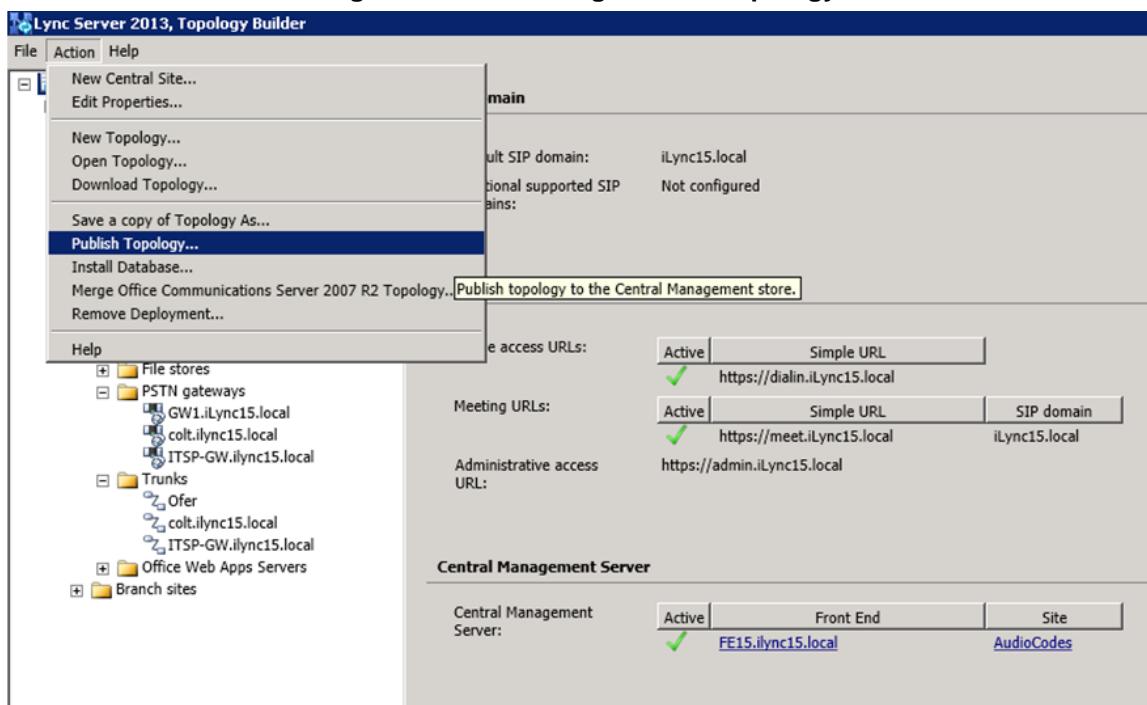
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



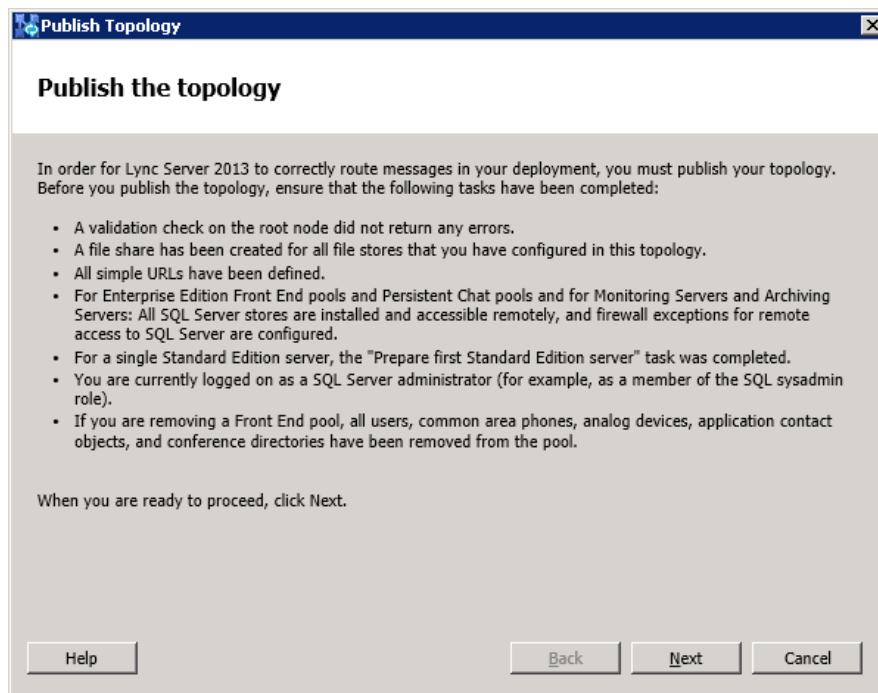
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

**Figure 3-10: Choosing Publish Topology**



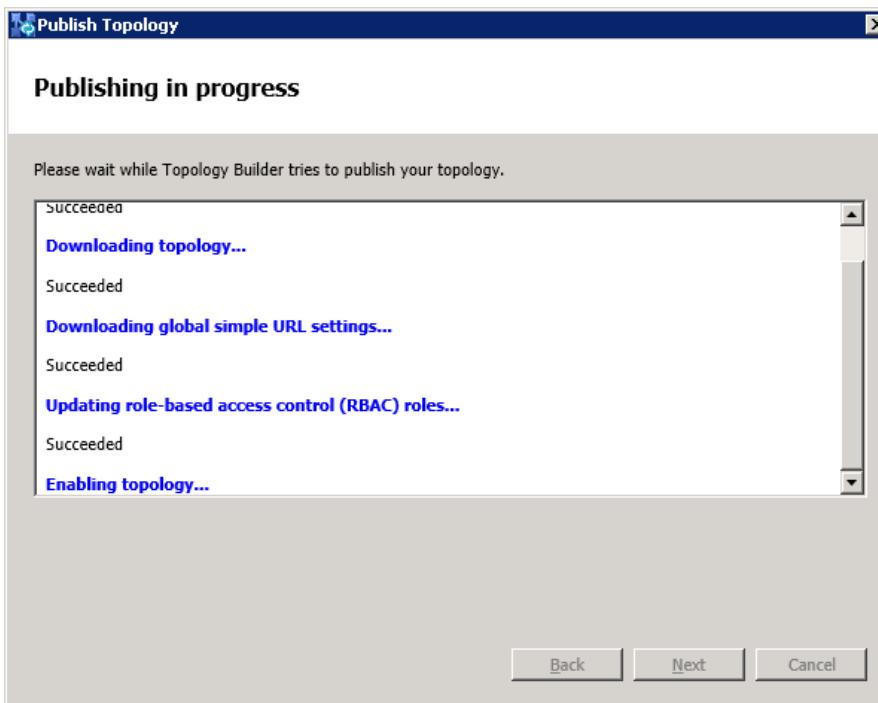
The following is displayed:

**Figure 3-11: Publish the Topology**



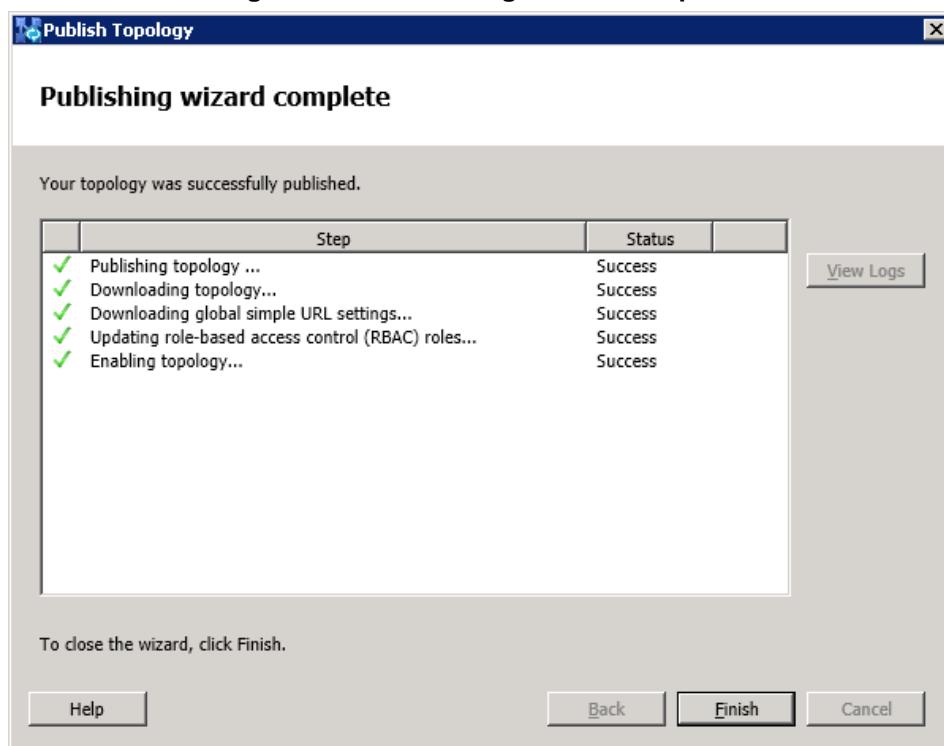
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

**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:**

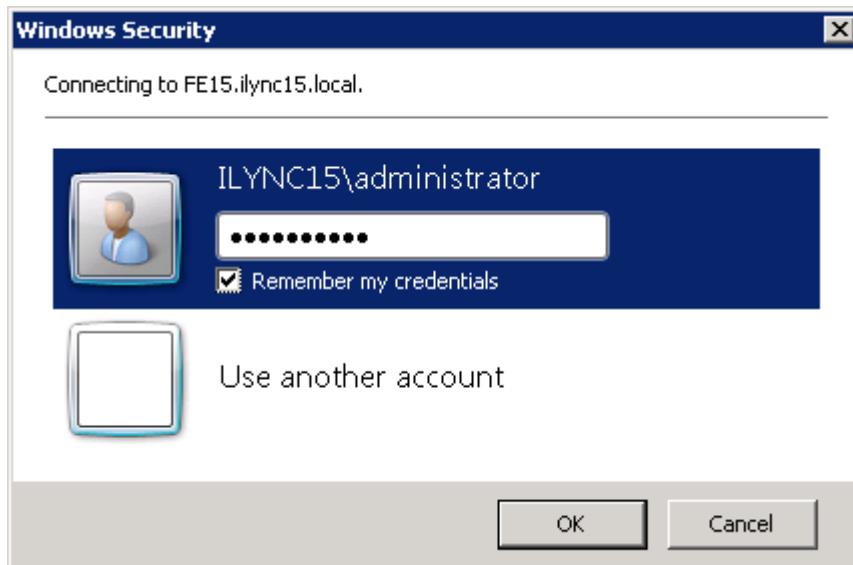
1. Start the Microsoft Lync Server 2013 Control Panel (**Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel**), as shown below:

**Figure 3-14: Opening the Lync Server Control Panel**



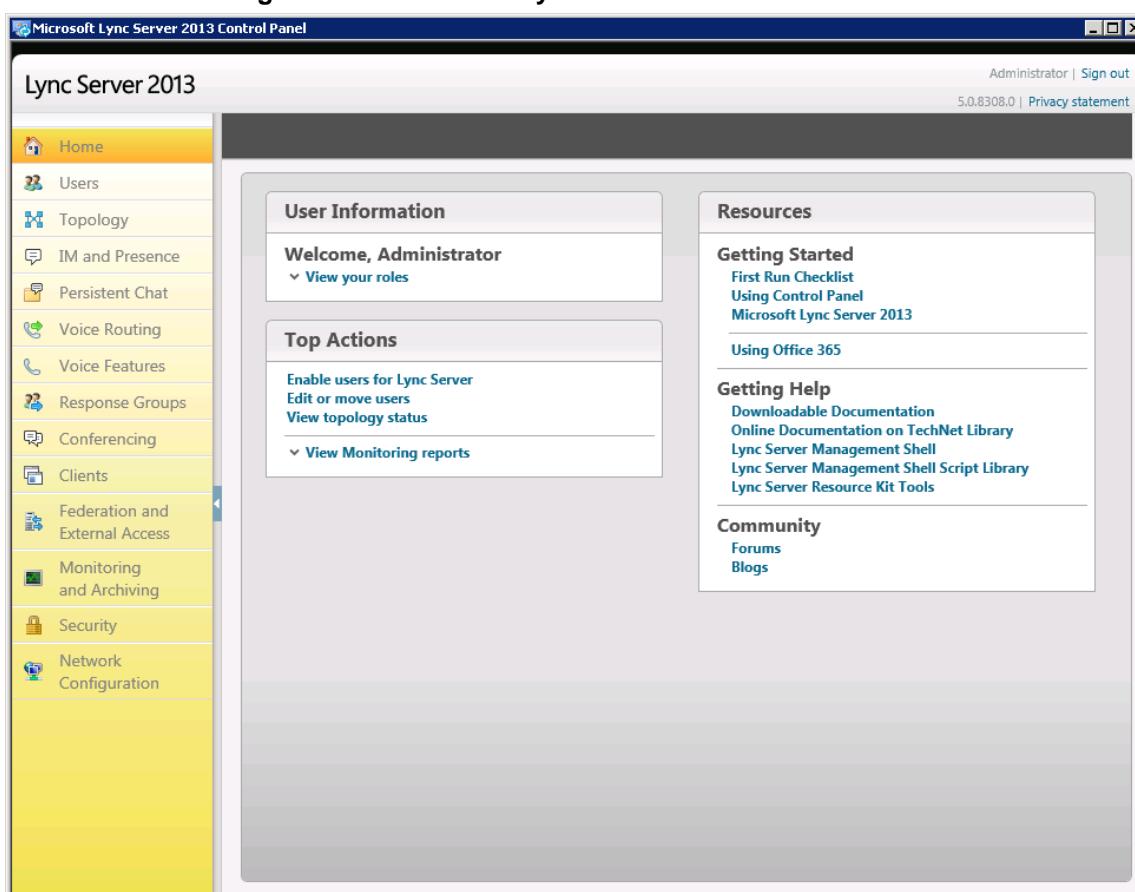
You are prompted to enter your login credentials:

**Figure 3-15: Lync Server Credentials**

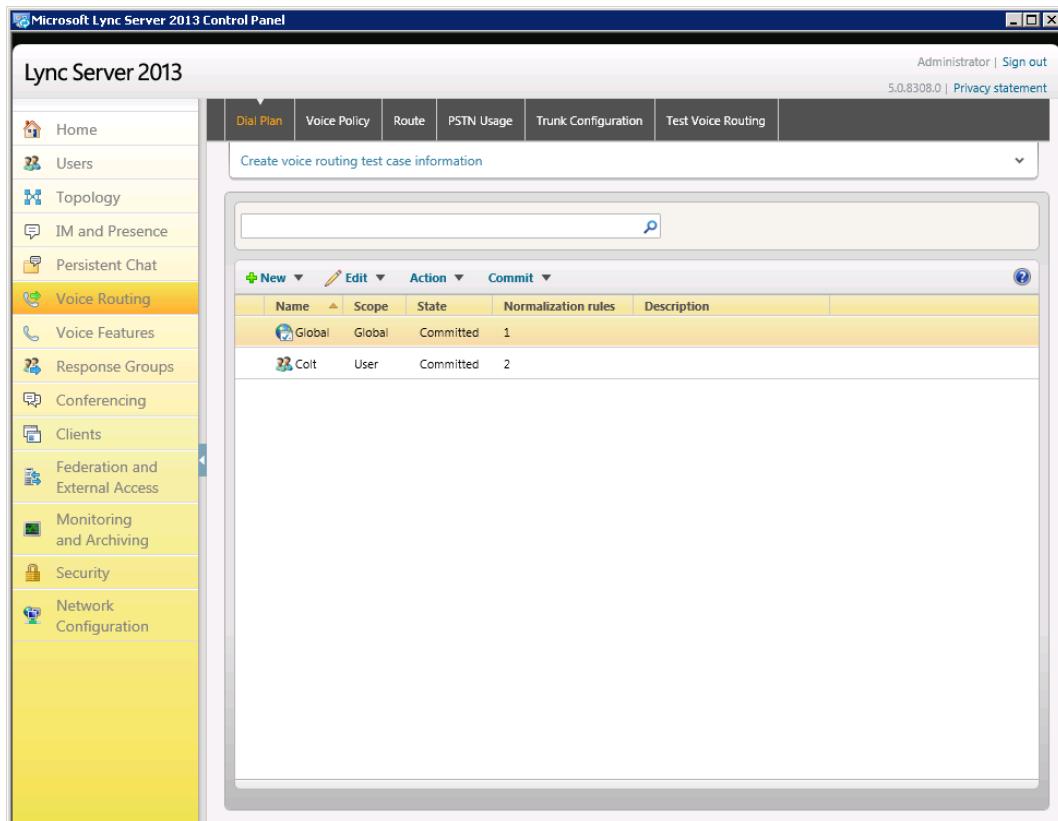


2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

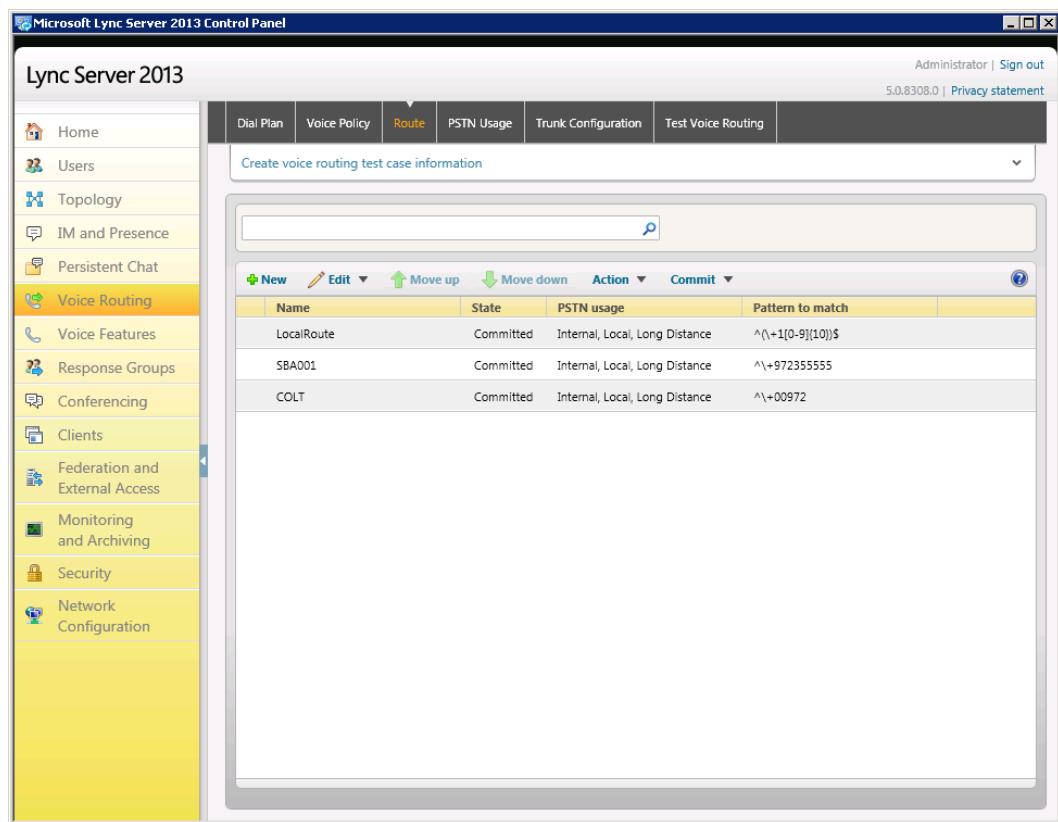
**Figure 3-16: Microsoft Lync Server 2013 Control Panel**



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

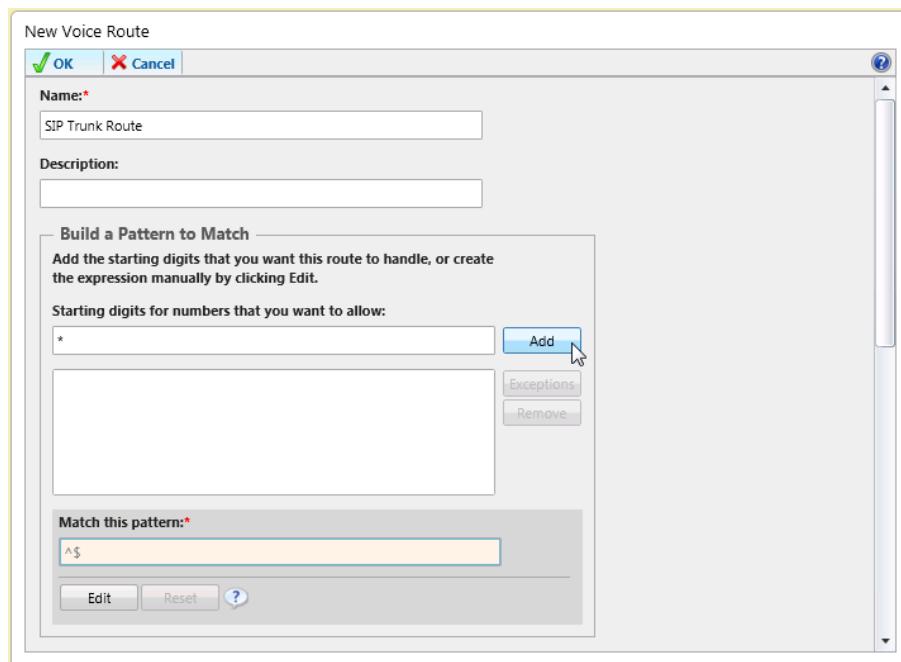
**Figure 3-17: Voice Routing Page**

- 4.** In the Voice Routing page, select the **Route** tab.

**Figure 3-18: Route Tab**

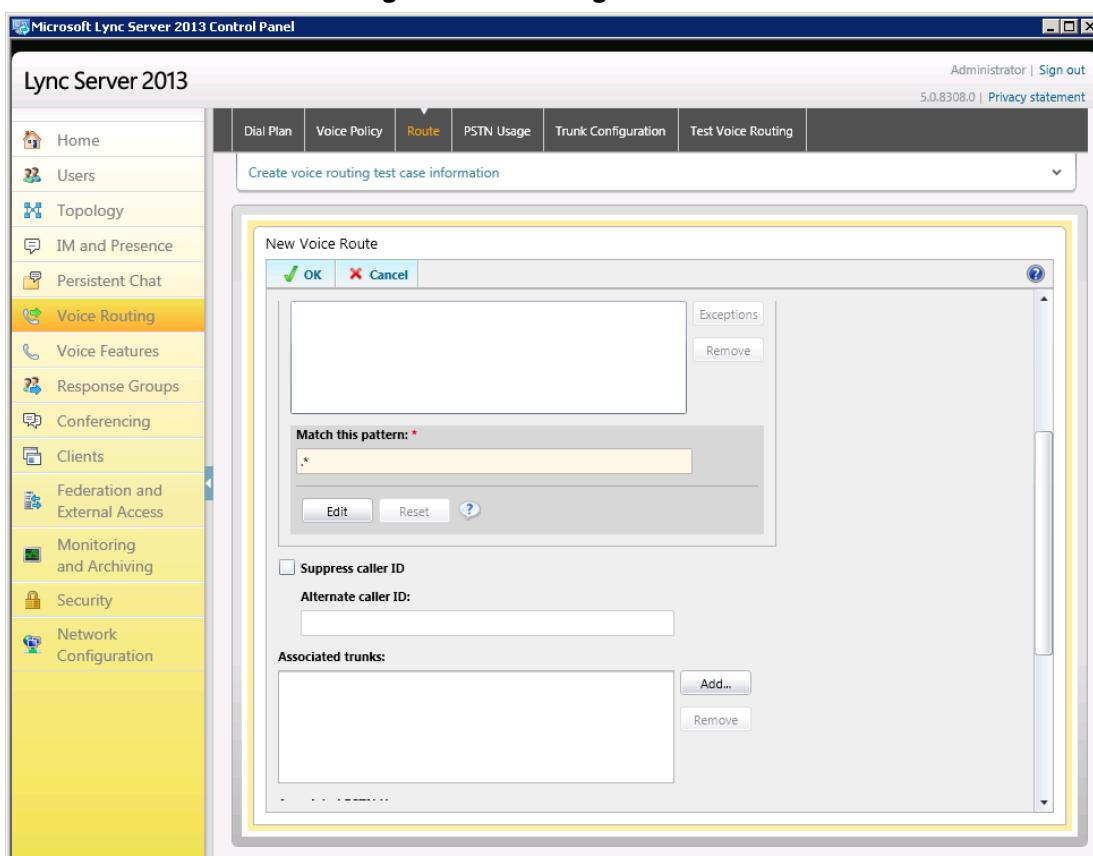
5. Click **New**; the New Voice Route page appears:

**Figure 3-19: Adding New Voice Route**



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

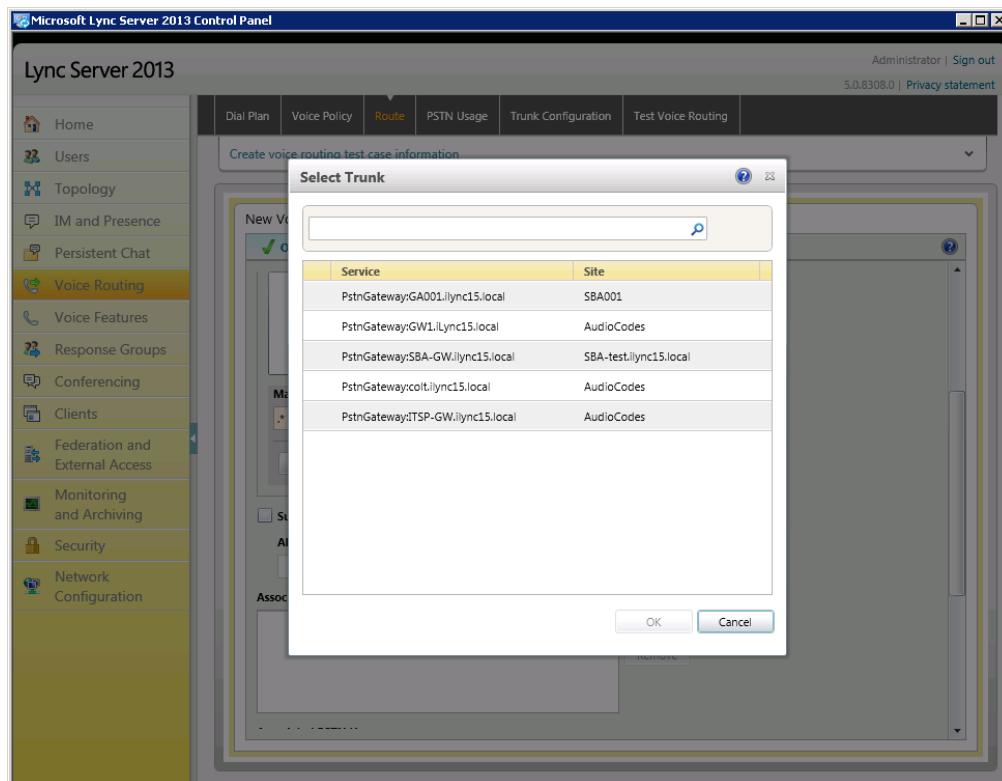
**Figure 3-20: Adding New Trunk**



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

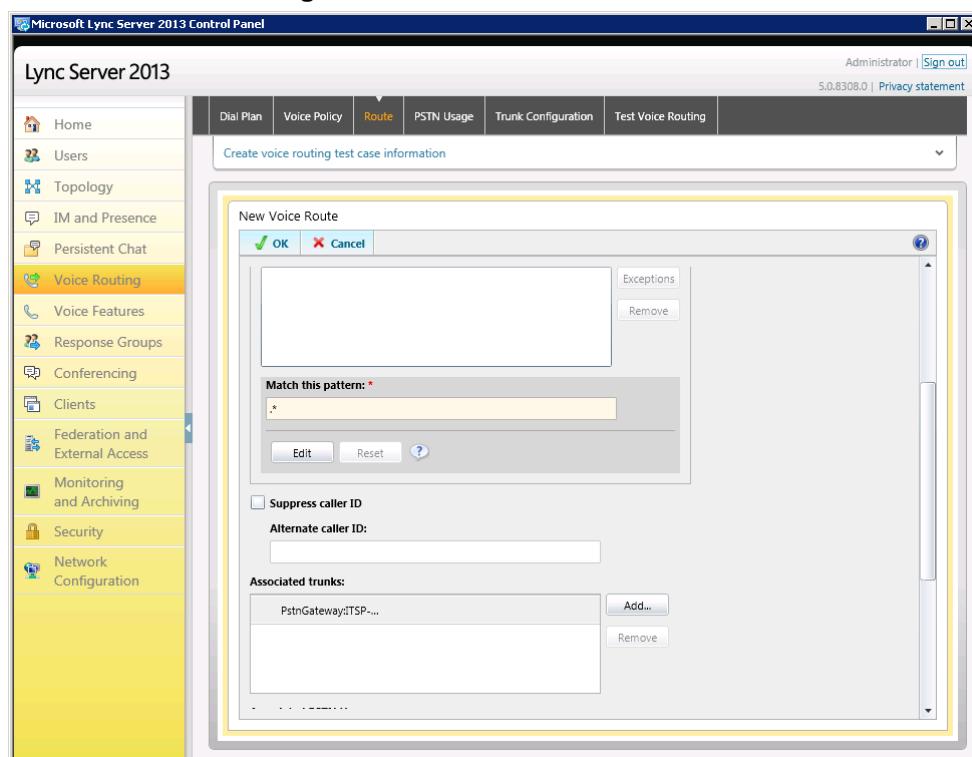
- a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

**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:

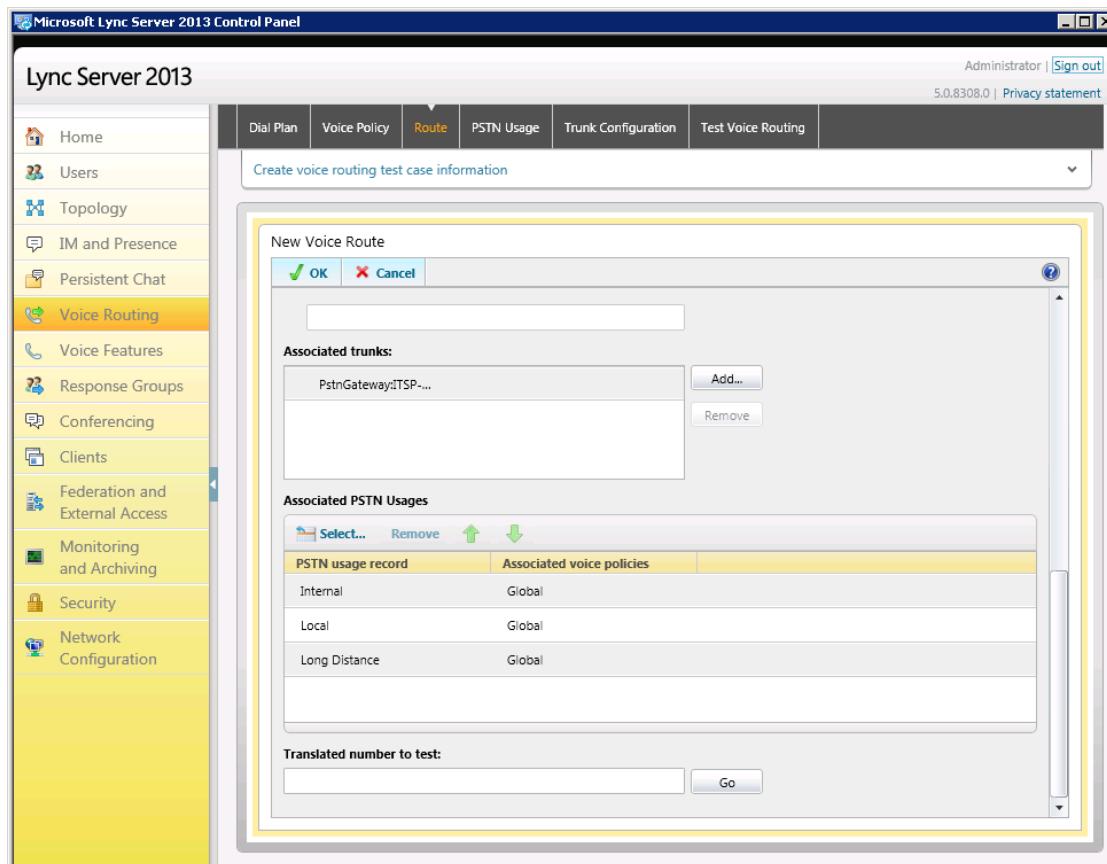
**Figure 3-22: Selected E-SBC Trunk**



9. 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**



10. 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**

<span style="color: green;">+</span> <b>New</b> <span style="color: blue;">Edit</span> <span style="color: green;">Move up</span> <span style="color: green;">Move down</span> <span style="color: blue;">Action</span> <span style="color: blue;">Commit</span>				
Name	State	PSTN usage	Pattern to match	
SIP Trunk Route	<span style="color: blue;">Uncommitted</span>	Local, Internal...	$\wedge\backslash*$	

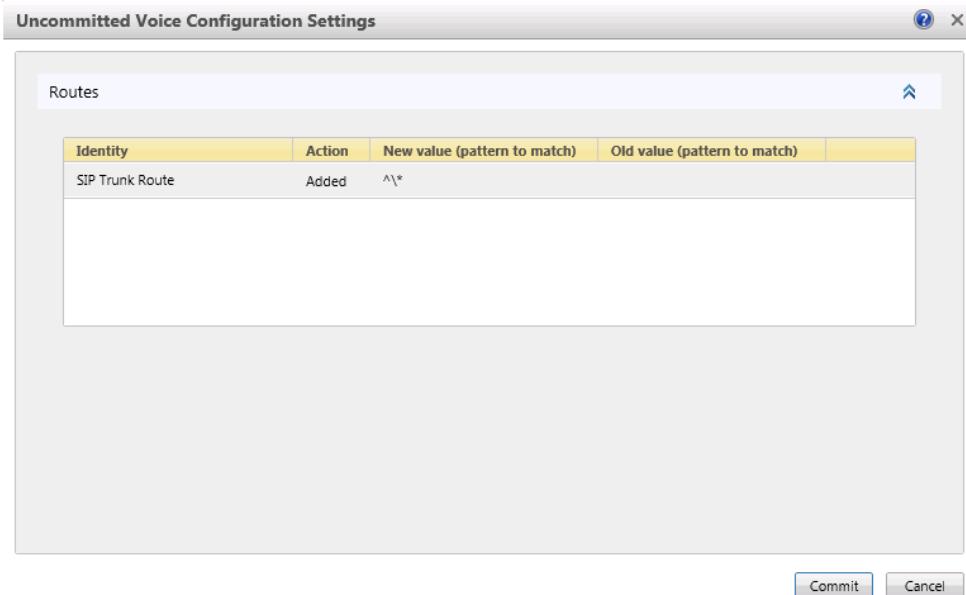
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

**Figure 3-25: Committing Voice Routes**

<span style="color: green;">+</span> <b>New</b> <span style="color: blue;">Edit</span> <span style="color: green;">Move up</span> <span style="color: green;">Move down</span> <span style="color: blue;">Action</span> <span style="color: blue;">Commit</span>				
Name	State	PSTN usa	Review uncommitted changes	
SIP Trunk Route	<span style="color: blue;">Uncommitted</span>	Local, Inte	Commit all	

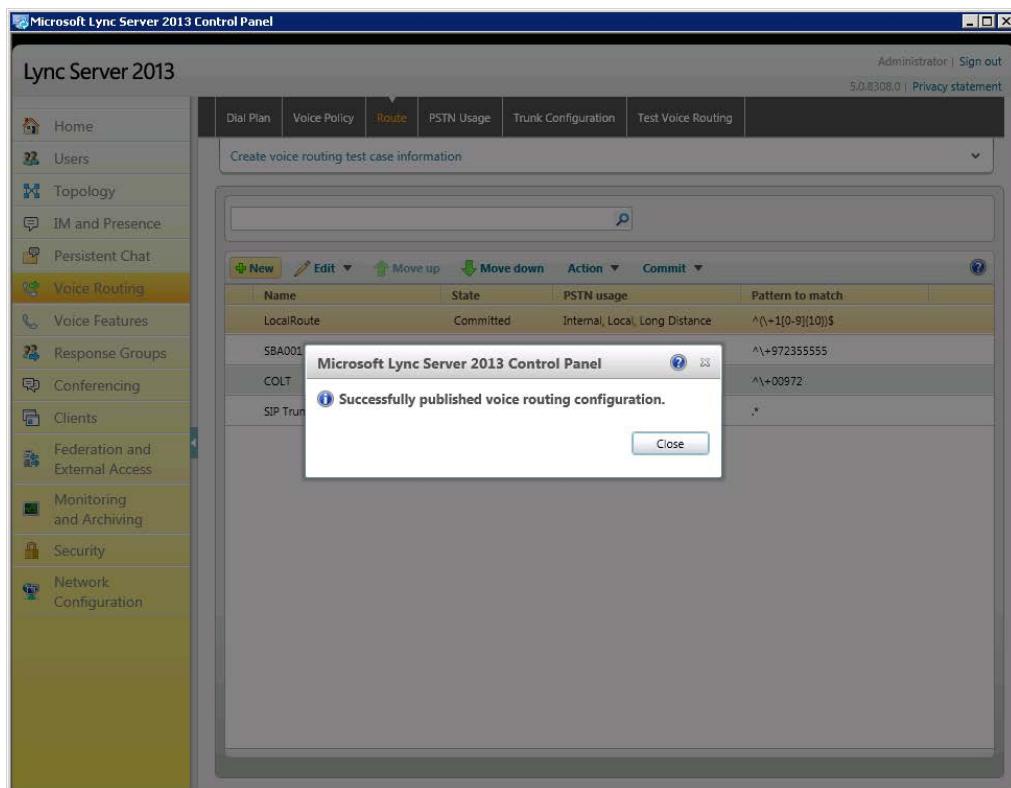
The Uncommitted Voice Configuration Settings page appears:

**Figure 3-26: Uncommitted Voice Configuration Settings**



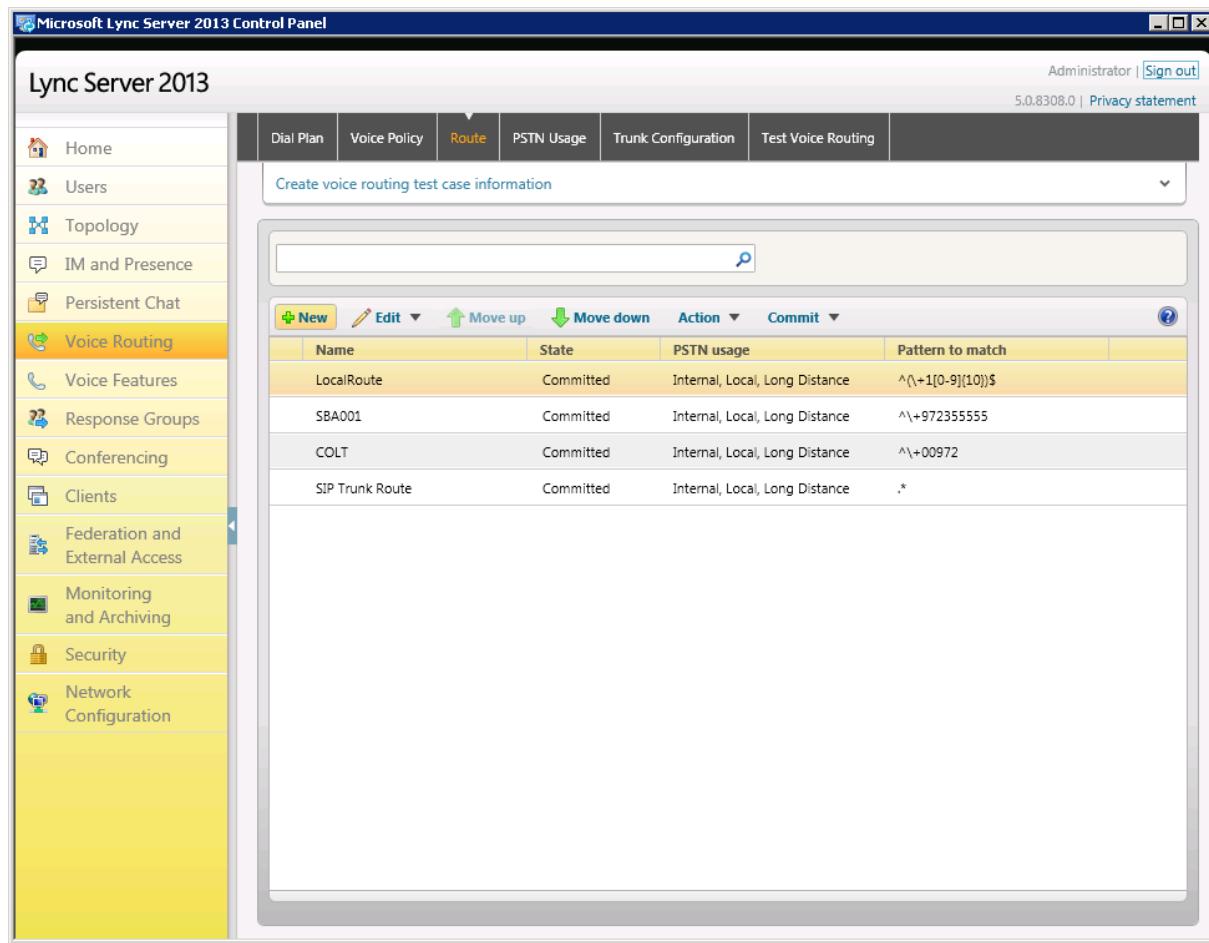
- Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

**Figure 3-27: Confirmation of Successful Voice Routing Configuration**



13. 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**



Name	State	PSTN usage	Pattern to match
LocalRoute	Committed	Internal, Local, Long Distance	<code>^(\\+1[0-9]{10})\$</code>
SBA001	Committed	Internal, Local, Long Distance	<code>^\\+972355555</code>
COLT	Committed	Internal, Local, Long Distance	<code>^\\+00972</code>
SIP Trunk Route	Committed	Internal, Local, Long Distance	<code>*</code>

## 4 Configuring AudioCodes E-SBC

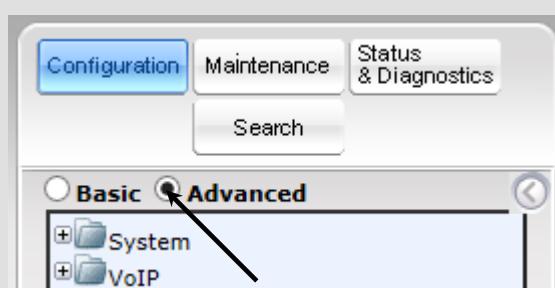
This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and the Telavox SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following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

- E-SBC WAN interface - Telavox 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 Telavox 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 document does **not** cover security aspects for connecting the SIP Trunk to the Microsoft Lync environment. Security measures should be implemented in accordance with your organization's security policies. For basic security guidelines, 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 Full-menu display mode. To do this, select the **Full** option, as shown below:



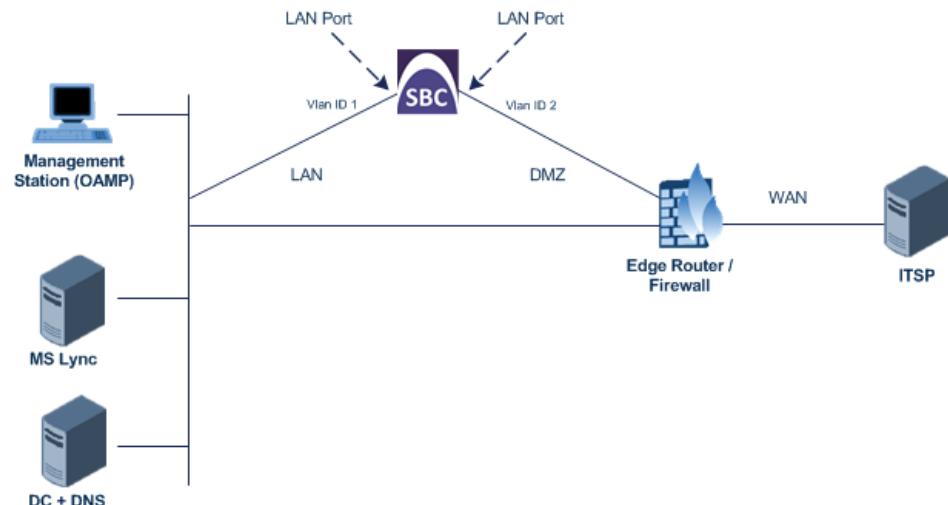
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

## 4.1 Step 1: IP Network Interfaces Configuration

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

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

**Figure 4-1: Network Interfaces in Interoperability Test Topology**



### 4.1.1 Step 1a: Configure VLANs

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

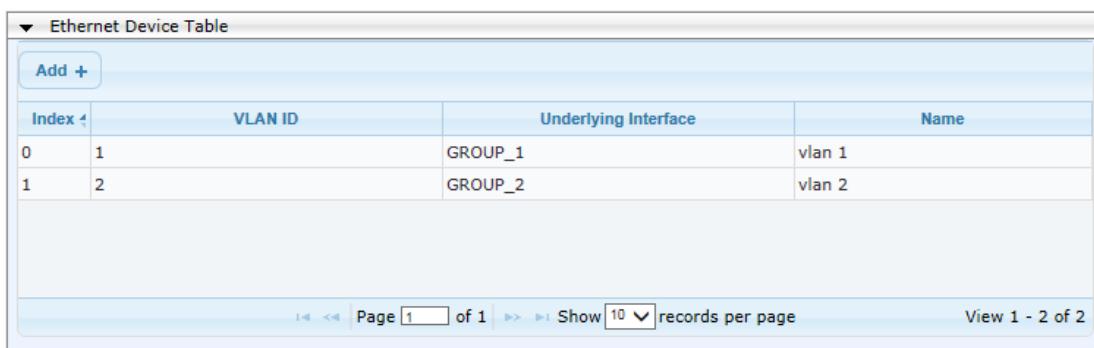
- LAN VoIP (assigned the name "Voice")
- WAN VoIP (assigned the name "WANSP")

➤ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).  
A row for VLAN ID 1 and underlying interface GROUP\_1 is displayed.
2. 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

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



The screenshot shows a web-based configuration interface for an Ethernet Device Table. At the top left, there is a dropdown menu labeled "Ethernet Device Table". Below it is a button labeled "Add +". The main area contains a table with four columns: "Index", "VLAN ID", "Underlying Interface", and "Name". There are two rows in the table. Row 0 has an index of 1, a VLAN ID of 1, an underlying interface of GROUP\_1, and a name of "vlan 1". Row 1 has an index of 1, a VLAN ID of 2, an underlying interface of GROUP\_2, and a name of "vlan 2". At the bottom of the table, there are navigation links for "Page 1 of 1", "Show 10 records per page", and "View 1 - 2 of 2".

Index	VLAN ID	Underlying Interface	Name
0	1	GROUP_1	vlan 1
1	2	GROUP_2	vlan 2

#### 4.1.2 Step 1b: Configure Network Interfaces

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

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

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

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

Parameter	Value
IP Address	<b>10.15.17.77</b> (IP address of E-SBC)
Prefix Length	<b>16</b> (subnet mask in bits for 255.255.0.0)
Gateway	<b>10.15.0.1</b>
VLAN ID	<b>1</b>
Interface Name	<b>Voice</b> (arbitrary descriptive name)
Primary DNS Server IP Address	<b>10.15.25.1</b>
Underlying Device	<b>vlan 1</b>

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	<b>Media + Control</b>
IP Address	<b>195.189.192.157</b> (WAN IP address)
Prefix Length	<b>25</b> (for 255.255.255.128)
Gateway	<b>195.189.192.129</b> (router's IP address)
VLAN ID	<b>2</b>
Interface Name	<b>WANSP</b>
Primary DNS Server IP Address	<b>80.179.52.100</b>
Secondary DNS Server IP Address	<b>80.179.55.100</b>
Underlying Device	<b>vlan 2</b>

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

The configured IP network interfaces are shown below:

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

Interface Table									
Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Devic
0	OAMP + Media + Control	IPv4 Manual	10.15.17.77	16	10.15.0.1	Voice	10.15.25.1	0.0.0.0	vlan 1
1	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	WANSP	80.179.52.100	80.179.55.100	vlan 2

### 4.1.3 Step 1c: Configure the Native VLAN ID

This step describes how to configure the Native VLAN ID for the LAN and WAN interfaces.

➤ **To configure the Native VLAN ID for the IP network interfaces:**

1. Open the Physical Ports Settings page (**Configuration** tab> **VoIP** menu > **Network > Physical Ports Table**).
2. For the **GROUP\_1** member ports, set the 'Native Vlan' field to **1**. This VLAN was assigned to network interface "Voice" in Section 4.1.2 above.
3. For the **GROUP\_2** member ports, set the 'Native Vlan' field to **2**. This VLAN was assigned to network interface "WANSP" in Section 4.1.2 above.

**Figure 4-4: Configured Port Native VLAN**

Physical Ports Settings							
Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_4_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_4_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

## 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 4-5: Enabling SBC Application**

SBC Application	Disable
SBC Application	Enable
IP to IP Application	Disable

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section [4.15](#) on page [70](#)).

## 4.3 Step 3: Signaling Routing Domains Configuration

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

The SRD is composed of the following:

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

### 4.3.1 Step 3a: Configure Media Realms

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

➤ **To configure Media Realms:**

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

Parameter	Value
Index	0
Media Realm Name	MRLan (descriptive name)
IPv4 Interface Name	Voice
Port Range Start	6000 (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	10 (media sessions assigned with port range)

**Figure 4-6: Configuring Media Realm for LAN**

**Edit Record #0** ×

Index	<input type="text" value="0"/>
Media Realm Name	<input type="text" value="MRLan"/>
IPv4 Interface Name	<input type="text" value="Voice"/>
IPv6 Interface Name	<input type="text" value="None"/>
Port Range Start	<input type="text" value="6000"/>
Number Of Media Session Legs	<input type="text" value="10"/>
Port Range End	<input type="text" value="6090"/>
Default Media Realm	<input type="text" value="Yes"/>
QOE Profile	<input type="text" value="None"/>
BW Profile	<input type="text" value="None"/>

Submit Cancel

**3.** Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Media Realm Name	MRWan (arbitrary name)
IPv4 Interface Name	WANSP
Port Range Start	7000 (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	10 (media sessions assigned with port range)

**Figure 4-7: Configuring Media Realm for WAN**

Add Record	
Index	1
Media Realm Name	MRWan
IPv4 Interface Name	WANSP
IPv6 Interface Name	None
Port Range Start	7000
Number Of Media Session Legs	10
Port Range End	-1
Default Media Realm	No
QOE Profile	None
BW Profile	None
<input checked="" type="button"/> <b>Submit</b> <input type="button"/> <b>Cancel</b>	

The configured Media Realms are shown in the figure below:

**Figure 4-8: Configured Media Realms in Media Realm Table**

Media Realm Table			
Add +	Index	Media Realm Name	IPv4 Interface Name
	0	MRLan	Voice
	1	MRWan	WANSP
Page 1 of 1 Show 10 records per page View 1 - 2 of 2			

### 4.3.2 Step 3b: Configure SRDs

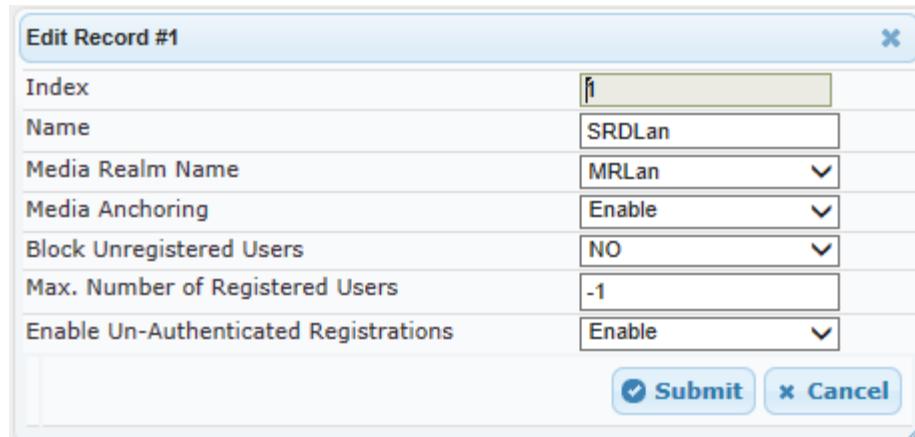
This step describes how to configure the SRDs.

➤ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SRD Table**).
2. Configure an SRD for the E-SBC's internal interface (toward Lync Server 2013):

Parameter	Value
SRD Index	1
SRD Name	<b>SRDLan</b> (descriptive name for SRD)
Media Realm	<b>MRLan</b> (associates SRD with Media Realm)

**Figure 4-9: Configuring LAN SRD**



The screenshot shows a software interface titled "Edit Record #1". It contains a table with the following data:

Index	1
Name	SRDLan
Media Realm Name	MRLan
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable

At the bottom right are two buttons: "Submit" and "Cancel".

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

Parameter	Value
SRD Index	2
SRD Name	<b>SRDWan</b>
Media Realm	<b>MRWan</b>

**Figure 4-10: Configuring WAN SRD**

Edit Record #2	
Index	2
Name	SRDWan
Media Realm Name	MRWan
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable
<input checked="" type="button"/> <b>Submit</b> <input type="button"/> <b>Cancel</b>	

### 4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➤ **To configure SIP Interfaces:**

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

Parameter	Value
Index	1
Interface Name	Lync (arbitrary descriptive name)
Network Interface	Voice
Application Type	SBC
TLS Port	5067
TCP and UDP	0
SRD	1

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	2
Interface Name	Telavox (arbitrary descriptive name)
Network Interface	WANSP
Application Type	SBC
UDP Port	5060
TCP and TLS	0
SRD	2

The configured SIP Interfaces are shown in the figure below:

**Figure 4-11: Configured SIP Interfaces in SIP Interface Table**

SIP Interface Table							
Index	Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	Lync	Voice	SBC	0	0	5067	1
2	Telavox	WANSP	SBC	5060	0	0	2
View 1 - 2 of 2							

## 4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Lync Server 2013
- Telavox SIP Trunk

These Proxy Sets will later be associated with IP Groups.

➤ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for Lync Server 2013:

Parameter	Value
Proxy Set ID	1
Proxy Address	<b>FE15.ilync15.local:5067</b> (Lync Server 2013 IP address / FQDN and destination port)
Transport Type	<b>TLS</b>
Proxy Name	<b>Lync</b> (arbitrary descriptive name)
Enable Proxy Keep Alive	<b>Using Options</b>
Proxy Load Balancing Method	<b>Round Robin</b>
Is Proxy Hot Swap	<b>Yes</b>
SRD Index	1

Figure 4-12: Configuring Proxy Set for Microsoft Lync Server 2013

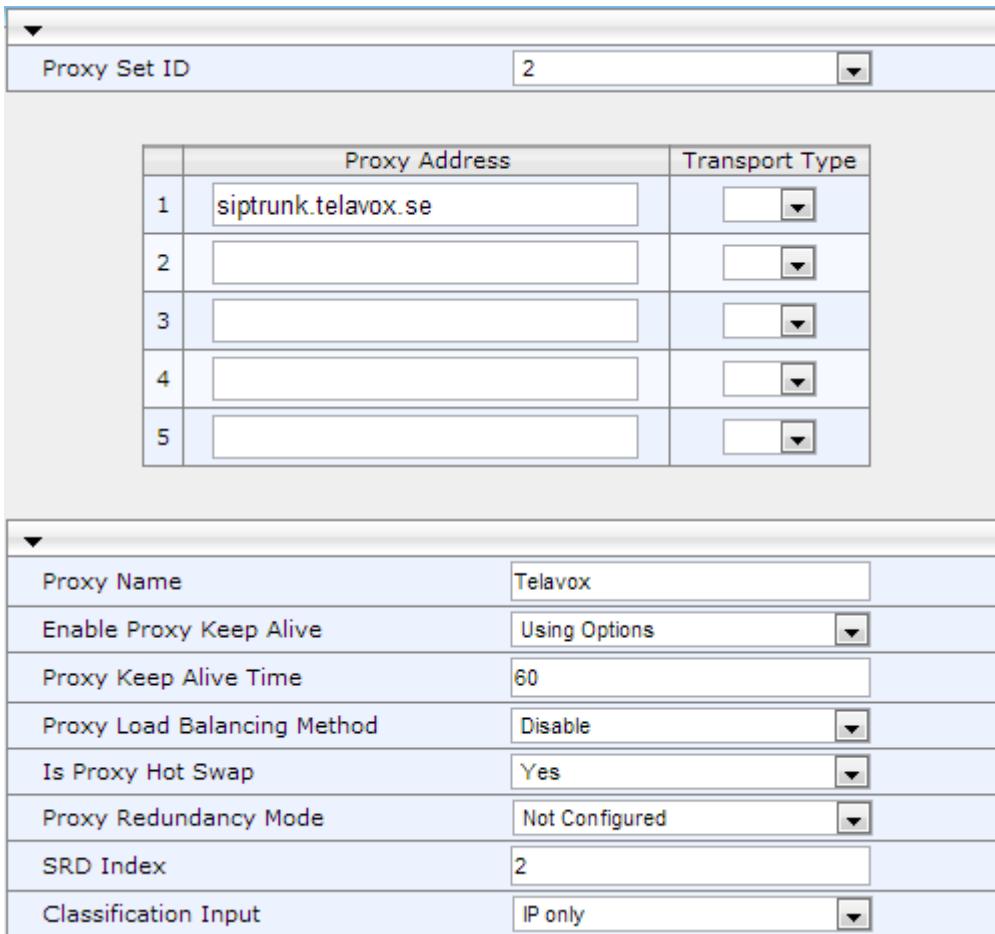
Proxy Address	Transport Type
1 FE15.ilync15.local:5067	TLS
2	
3	
4	
5	

Proxy Name	Lync
Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

3. Configure a Proxy Set for the Telavox SIP Trunk:

Parameter	Value
Proxy Set ID	<b>2</b>
Proxy Address	<b>siptrunk.telavox.se</b> (Telavox IP address / FQDN and destination port)
Transport Type	<b>UDP</b>
Proxy Name	<b>Telavox</b> (arbitrary descriptive name)
Enable Proxy Keep Alive	<b>Using Options</b>
Is Proxy Hot Swap	<b>Yes</b>
SRD Index	<b>2</b> (enables classification by Proxy Set for SRD of IP Group belonging to Telavox SIP Trunk)

Figure 4-13: Configuring Proxy Set for Telavox SIP Trunk



Index	Proxy Address	Transport Type
1	siptrunk.telavox.se	UDP
2		UDP
3		UDP
4		UDP
5		UDP

Proxy Name	Telavox
Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Not Configured
SRD Index	2
Classification Input	IP only

4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.15 on page 70).

## 4.5 Step 5: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. A typical deployment consists of multiple IP Groups associated with the same SRD. For example, you can have two LAN IP PBXs sharing the same SRD, and two ITSPs / SIP Trunks sharing the same SRD. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

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

- Lync Server 2013 (Mediation Server) located on LAN
- Telavox 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. Configure an IP Group for the Lync Server 2013 Mediation Server:

Parameter	Value
Index	1
Type	Server
Description	Lync (arbitrary descriptive name)
Proxy Set ID	1
SIP Group Name	Telavox (according to ITSP requirement)
SRD	1
Media Realm Name	MRLan
IP Profile ID	1

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

Parameter	Value
Index	2
Type	Server
Description	Telavox (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	Telavox (according to ITSP requirement)
SRD	2
Media Realm Name	MRWan
IP Profile ID	2

The configured IP Groups are shown in the figure below:

**Figure 4-14: Configured IP Groups in IP Group Table**

IP Group Table									
<b>Add +</b>									
Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD	
1	Server	Lync	1	195.189.192.157		Not Configured	No	1	
2	Server	Telavox	2	audiocodes.com		Not Configured	No	2	

Page  of 1 Show  records per page View 1 - 2 of 2

## 4.6 Step 6: Configure IP Profiles

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

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

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

Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 43).

➤ **To configure IP Profiles:**

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

Parameter	Value
Index	1
Profile Name	Lync (arbitrary descriptive name)
Symmetric MKI	Enable
MKI Size	1
Reset SRTP State Upon Re-key	Enable
Generate SRTP keys mode:	Always

Figure 4-15: Configuring IP Profile for Lync Server 2013 – Common Tab

The screenshot shows the 'IP Profile Settings' page with the 'Common' tab selected. The configuration parameters are as follows:

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

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

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

Parameter	Value
Media Security Behavior	<b>SRTP</b>
PRACK Mode	<b>Optional</b> (required, as Telavox does not support PRACK)
Remote Update Support	<b>Supported Only After Connect</b>
Remote Re-Invite Support	<b>Supported Only With SDP</b>
Remote Delayed Offer Support	<b>Not Supported</b>
Remote Refer Behavior	<b>Handle Locally</b> (required, as Lync Server 2013 does not support receipt of SIP REFER)
Remote 3xx Behavior	<b>Handle Locally</b> (required, as Lync Server 2013 does not support receipt of SIP 3xx responses)
Enforce MKI Size	<b>Enforce</b>
Remote Early Media RTP Behavior	<b>Delayed</b> (required, as Lync Server 2013 does not send RTP immediately to remote side when it sends a SIP 18x response)
RTCP Mode	<b>Generate Always</b> (required, as Telavox SIP Trunk does not send RTCP packets in active call and in hold call, and in these cases, Microsoft Lync 2013 will terminate the call with network problems as the cause)

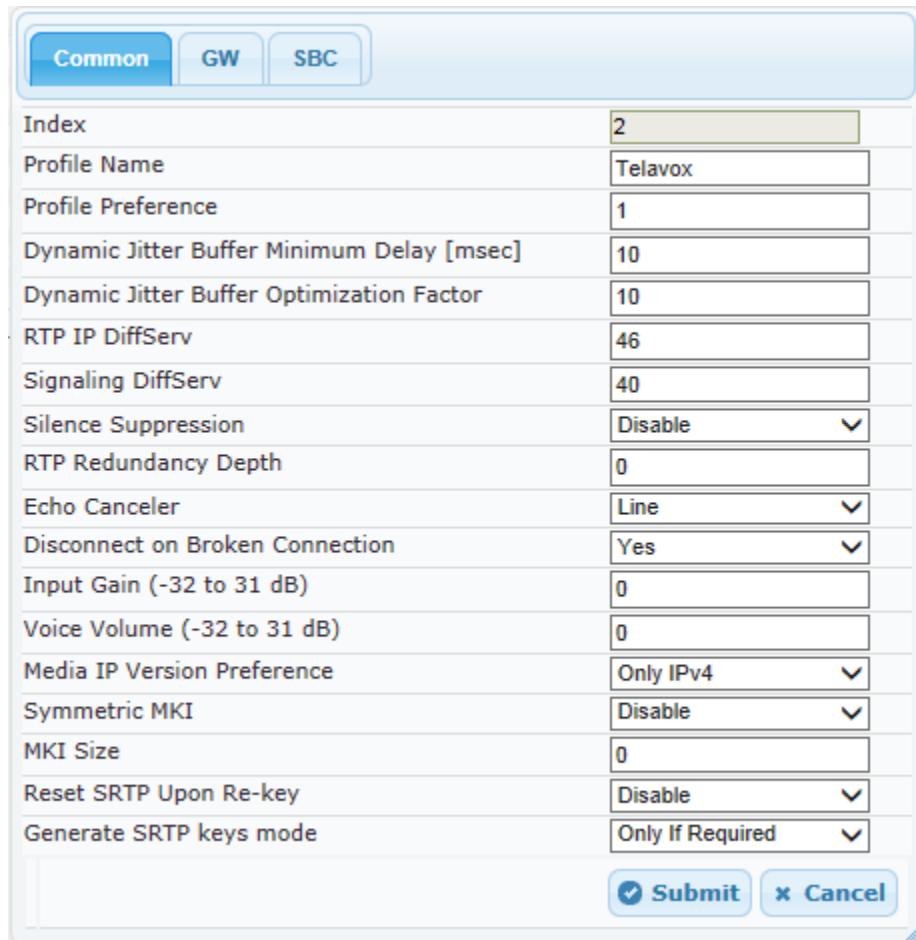
**Figure 4-16: Configuring IP Profile for Lync Server 2013 – SBC Tab**

		<b>SBC</b>
Index	1	
Extension Coders Group ID	None	
Transcoding Mode	Only If Required	
Allowed Media Types		
Allowed Coders Group ID	None	
Allowed Video Coders Group ID	None	
Allowed Coders Mode	Restriction	
SBC Media Security Behavior	SRTP	
RFC 2833 Behavior	As Is	
Alternative DTMF Method	As Is	
P-Asserted-Identity	As Is	
Diversion Mode	As Is	
History-Info Mode	As Is	
Fax Coders Group ID	None	
Fax Behavior	As Is	
Fax Offer Mode	All coders	
Fax Answer Mode	Single coder	
PRACK Mode	Optional	
Session Expires Mode	Transparent	
Remote Update Support	Supported Only After	
Remote re-INVITE	Supported only with S	
Remote Delayed Offer Support	Not Supported	
Remote REFER Behavior	Handle Locally	
Remote 3xx Behavior	Handle Locally	
Remote Multiple 18x	Supported	
Remote Early Media Response Type	Transparent	
Remote Early Media	Supported	
Enforce MKI Size	Enforce	
Remote Early Media RTP Behavior	Delayed	
Remote RFC 3960 Gateway Model Support	Not Supported	
Remote Can Play Ringback	Yes	
RFC 2833 DTMF Payload Type	0	
User Registration Time	0	
Reliable Held Tone Source	Yes	
Play Held Tone	No	
Remote Hold Format	Transparent	
Remote Replaces Behavior	Transparent	
SDP Ptime Answer	Remote Answer	
Preferred PTime	0	
Use Silence Suppression	Transparent	
RTP Redundancy Behavior	AS IS	
Play RBT To Transferee	No	
RTCP Mode	Generate Always	
Jitter Compensation	Disable	
Remote Renegotiate on Fax Detection	Don't Care	
<input checked="" type="button"/> <b>Submit</b> <input type="button"/> <b>Cancel</b>		

5. Configure an IP Profile for the Telavox SIP Trunk:
6. Click **Add**.
7. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Profile Name	Telavox (arbitrary descriptive name)

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



The screenshot shows the 'Common' tab selected in a configuration interface. The profile is named 'Telavox' and has an index of 2. Other settings include:

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

At the bottom are 'Submit' and 'Cancel' buttons.

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

Parameter	Value
Profile ID	<b>2</b>
Allowed Coders Group ID	<b>Coders Group 1</b>
Allowed Coders Mode	<b>Restricted</b> (lists Allowed Coders first and then original coders in received SDP offer)
Media Security Behavior	<b>RTP</b>
Remote REFER Behavior	<b>Handle Locally</b> (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Remote Can Play Ringback	<b>No</b> (required, as Lync Server 2013 does not provide a ringback tone for incoming calls)

**Figure 4-18: Configuring IP Profile for Telavox SIP Trunk – SBC Tab**

		SBC
Index	2	
Extension Coders Group ID	None	
Transcoding Mode	Only If Required	
Allowed Media Types		
Allowed Coders Group ID	Coders Group 1	
Allowed Video Coders Group ID	None	
Allowed Coders Mode	Restriction	
SBC Media Security Behavior	RTP	
RFC 2833 Behavior	As Is	
Alternative DTMF Method	As Is	
P-Asserted-Identity	As Is	
Diversion Mode	As Is	
History-Info Mode	As Is	
Fax Coders Group ID	None	
Fax Behavior	As Is	
Fax Offer Mode	All coders	
Fax Answer Mode	Single coder	
PRACK Mode	Transparent	
Session Expires Mode	Transparent	
Remote Update Support	Supported	
Remote re-INVITE	Supported	
Remote Delayed Offer Support	Not Supported	
Remote REFER Behavior	Handle Locally	
Remote 3xx Behavior	Transparent	
Remote Multiple 18x	Supported	
Remote Early Media Response Type	Transparent	
Remote Early Media	Supported	
Enforce MKI Size	Don't enforce	
Remote Early Media RTP Behavior	Immediate	
Remote RFC 3960 Gateway Model Support	Not Supported	
Remote Can Play Ringback	No	
RFC 2833 DTMF Payload Type	0	
User Registration Time	0	
Reliable Held Tone Source	Yes	
Play Held Tone	No	
Remote Hold Format	Transparent	
Remote Replaces Behavior	Transparent	
SDP Ptime Answer	Remote Answer	
Preferred PTime	0	
Use Silence Suppression	Transparent	
RTP Redundancy Behavior	AS IS	
Play RBT To Transferee	No	
RTCP Mode	Transparent	
Jitter Compensation	Disable	
Remote Renegotiate on Fax Detection	Don't Care	
<input checked="" type="button"/> <b>Submit</b> <input type="button"/> <b>Cancel</b>		

## 4.7 Step 7: Configure Coders

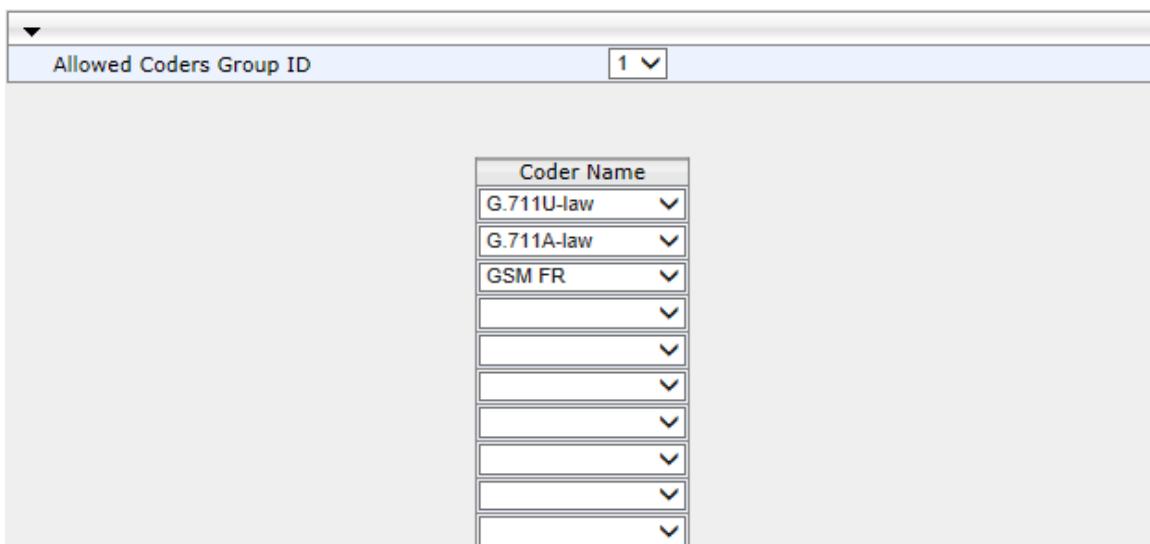
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Telavox SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Telavox SIP Trunk in the previous step (see Section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

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

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

Parameter	Value
Allowed Coders Group ID	1
Coder Name	<b>G.711 U-law</b>
Coder Name	<b>G.711 A-law</b>
Coder Name	<b>gsmFullRate</b>

Figure 4-19: Configuring Allowed Coders Group for Telavox SIP Trunk



## 4.8 Step 8: SIP TLS Connection Configuration

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

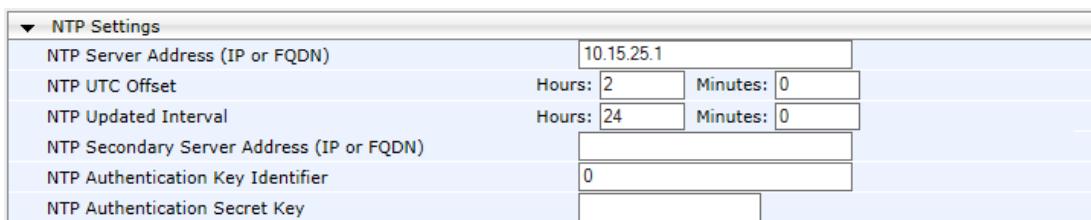
### 4.8.1 Step 8a: Configure the NTP Server Address

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

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

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

**Figure 4-20: Configuring NTP Server Address**



NTP Settings	
NTP Server Address (IP or FQDN)	10.15.25.1
NTP UTC Offset	Hours: 2 Minutes: 0
NTP Updated Interval	Hours: 24 Minutes: 0
NTP Secondary Server Address (IP or FQDN)	
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

3. Click **Submit**.

## 4.8.2 Step 8b: Configure 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 Certificates page (**Configuration tab > System > Certificates**).

**Figure 4-21: Certificates Page - Creating CSR**

Certificate Signing Request	
Subject Name [CN]	ITSP-GW.ilync15.local
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	
<b>Create CSR</b>	

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBXzCBQIBADAgMR4wHAYDVQQDExVJVFNQLUdXLmlseW5jMTUubG9jYWwwg28w
DQYJKoZIhvvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgnMcMVxdp9/BCXyygT2W1vz0NGUsypa7w2DKKkxr8xA9sGLXwy02CyB49U1pDF
DJVB1ldUFT8qL9d9V64f3Z004I1hwe28n4hHdAfGy0S6e91JhFw/USUD6/bNygQz
5Z203jtjXKmdAgMBAAGgADANBgkqhkiG9w0BAQQFAOBgQBLe880JgrmEzPu5Q1
pRGiOuEQ4Pr6PL+JKghii6UpImHEwixTedayzNh7b2yQgFYxiVWmX2JwrvXaCp5Y
8z8hOCZXV/E4MrR2a8bYb6bxeteAXs+VwxgRObb4pSFFGLc82+dZUcODAB0wZFv
nxSEcPACKnZittF/GgW+A4AoMQ==
-----END CERTIFICATE REQUEST-----
```

2. In the 'Subject Name' field, enter the media gateway name (e.g., **ITSP-GW.ilync15.local**).

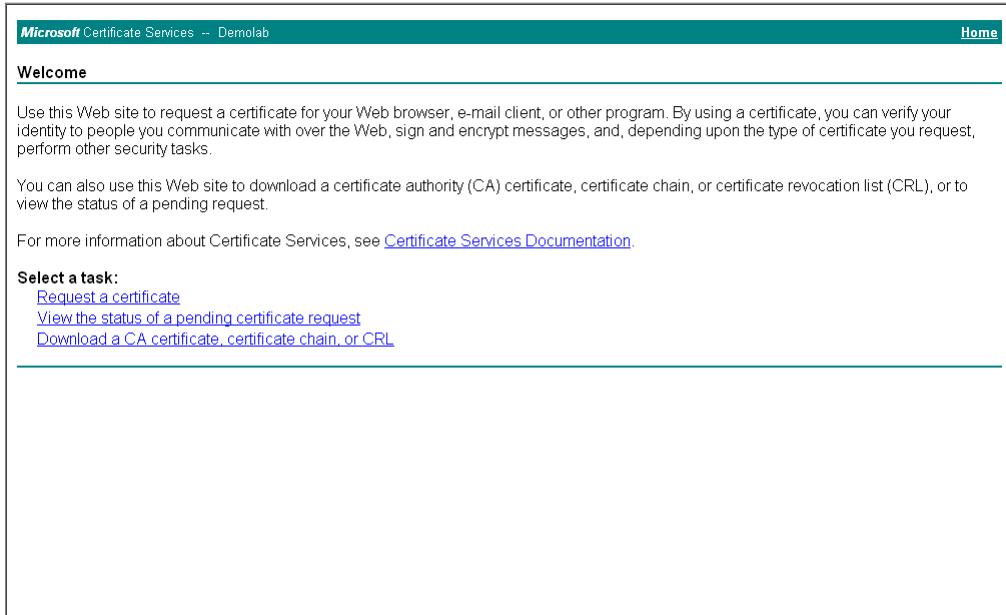


**Note:** The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13).

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

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

**Figure 4-22: Microsoft Certificate Services Web Page**



**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

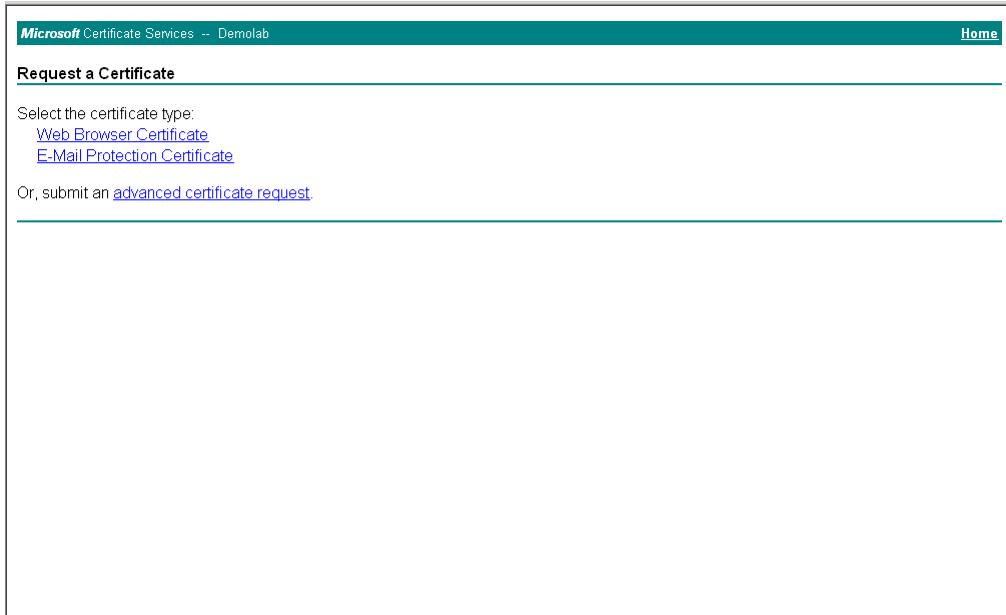
For more information about Certificate Services, see [Certificate Services Documentation](#).

**Select a task:**

[Request a certificate](#)  
[View the status of a pending certificate request](#)  
[Download a CA certificate, certificate chain, or CRL](#)

6. Click **Request a certificate**.

**Figure 4-23: Request a Certificate Page**



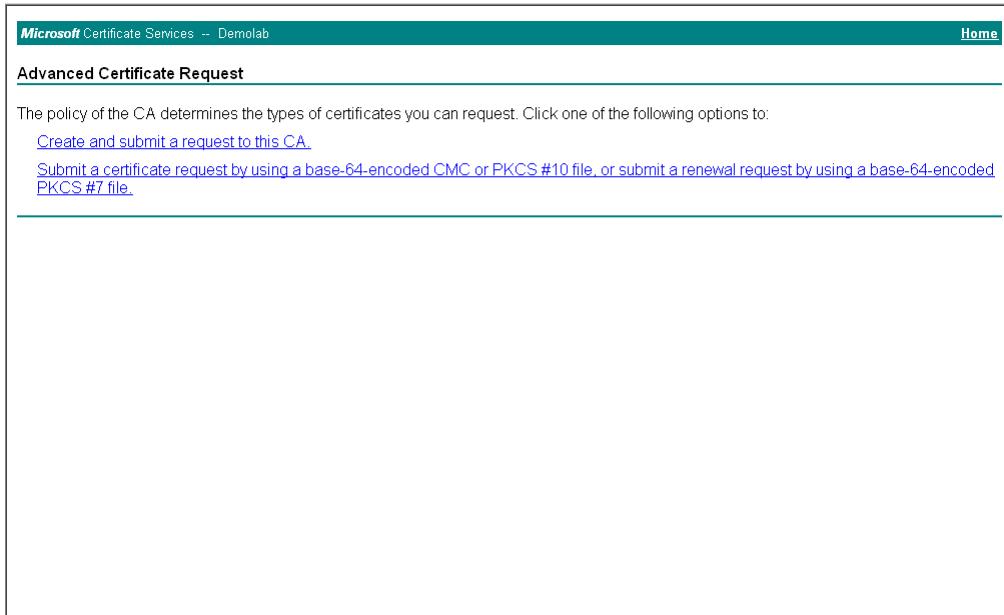
**Request a Certificate**

Select the certificate type:

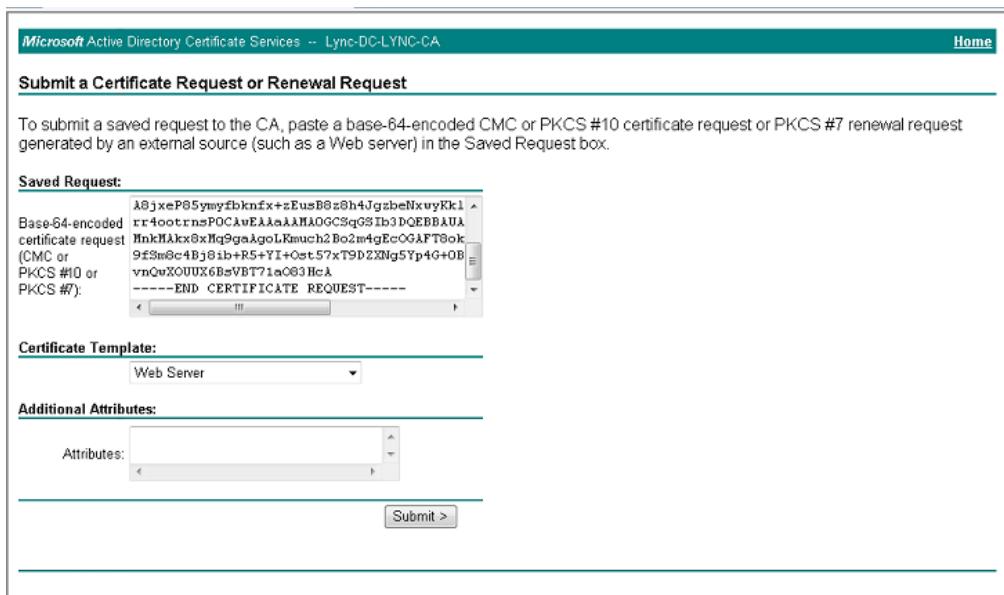
[Web Browser Certificate](#)  
[E-Mail Protection Certificate](#)

Or, submit an [advanced certificate request](#).

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

**Figure 4-24: Advanced Certificate Request Page**

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

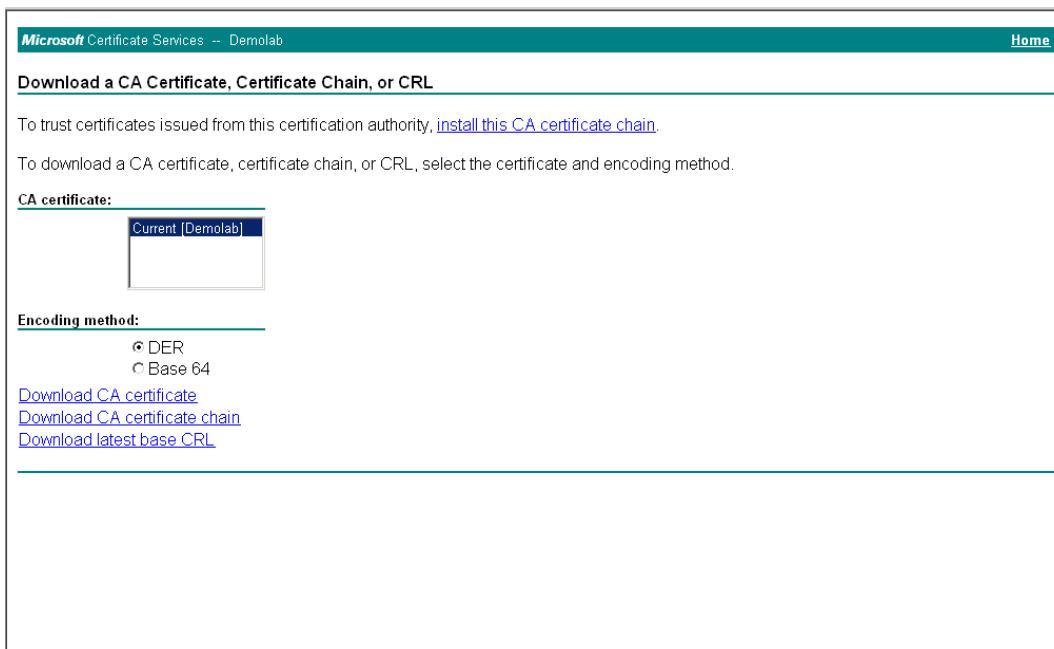
**Figure 4-25: Submit a Certificate Request or Renewal Request Page**

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

**Figure 4-26: Certificate Issued Page**

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

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



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

- 19.** In the E-SBC's Web interface, return to the Certificates page and do the following:
- In the 'Device Certificate' field, click **Browse** and select the *gateway.cer* certificate file that you saved on your computer in Step 13, and then click **Send File** to upload the certificate to the E-SBC.
  - In the 'Trusted Root Certificate Store' field, click **Browse** and select the *certroot.cer* certificate file that you saved on your computer in Step 18, and then click **Send File** to upload the certificate to the E-SBC.

**Figure 4-28: Certificates Page (Uploading Certificate)**

The screenshot shows the 'Certificates' page of the E-SBC's web interface. It has three main sections:

- Private key pass-phrase (optional):** A text input field containing 'audc'. Below it is a note: "Send **Private Key** file from your computer to the device. The file must be in either PEM or PFX (PKCS#12) format." With 'Browse...' and 'Send File' buttons.
- Note:** "Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link."
- Device Certificate:** A note: "Send **Device Certificate** file from your computer to the device. The file must be in textual PEM format." With 'Browse...' and 'Send File' buttons.
- Trusted Root Certificate Store:** A note: "Send **'Trusted Root Certificate Store'** file from your computer to the device. The file must be in textual PEM format." With 'Browse...' and 'Send File' buttons.

- 20.** Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 70).

## 4.9 Step 9: Configure SRTP

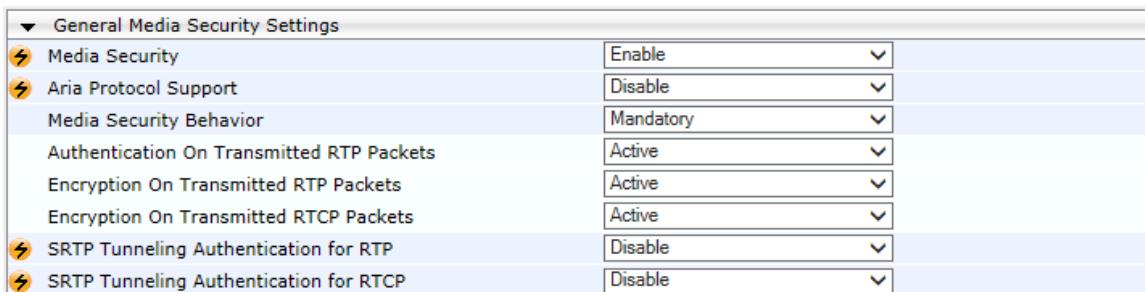
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 45).

➤ **To configure media security:**

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

Parameter	Value
Media Security	Enable

**Figure 4-29: Configuring SRTP**



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

2. Click **Submit**.
3. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 70).

## 4.10 Step 10: 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 > **IP Media** > **IP Media Settings**).

Figure 4-30: Configuring Number of IP Media Channels

Number of Media Channels	30
Voice Streaming	Disable
NetAnn Announcement ID	annc
MSCML ID	ivr
Transcoding ID	trans

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 4.15 on page 70).

## 4.11 Step 11: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 43, IP Group 1 represents Lync Server 2013, and IP Group 2 represents Telavox 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) and Telavox SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to Telavox SIP Trunk
- Calls from Telavox SIP Trunk to Lync Server 2013

➤ **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:
3. Click **Add**.
4. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	0
Route Name	<b>OPTIONS termination</b> (arbitrary descriptive name)
Source IP Group ID	1
Request Type	<b>OPTIONS</b>
Destination Type	<b>Dest Address</b>
Destination Address	<b>internal</b>

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

The screenshot shows a configuration interface for a routing rule. At the top, there are two tabs: 'Rule' (selected) and 'Action'. Below the tabs is a table with the following fields:

Index	0
Route Name	OPTIONS termination
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any

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

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

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

The screenshot shows a configuration interface for a routing rule. At the top, there are two tabs: 'Rule' (selected) and 'Action' (disabled). Below the tabs is a table with the following fields:

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

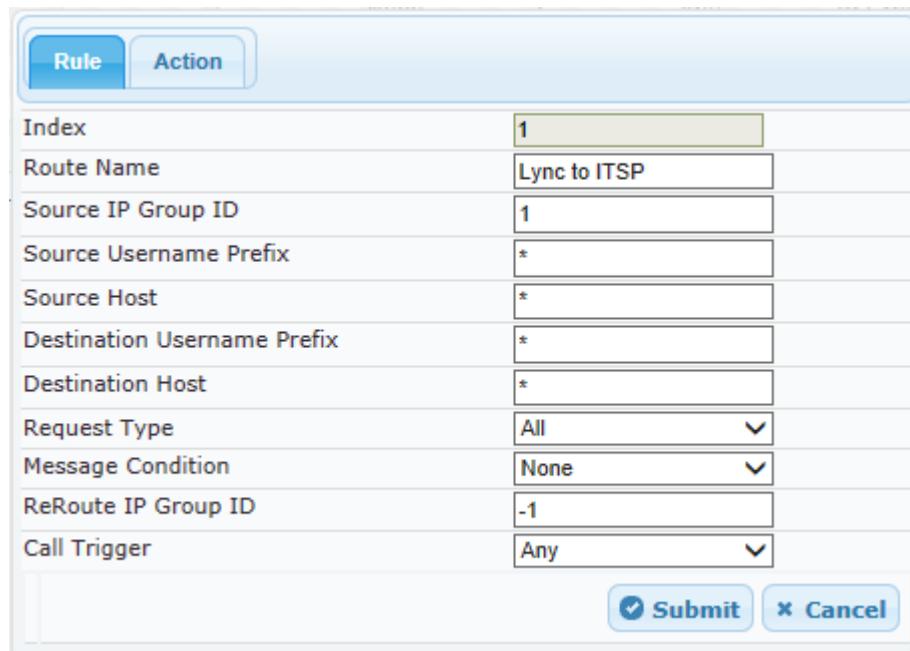
At the bottom right are 'Submit' and 'Cancel' buttons.

- Configure a rule to route calls from Lync Server 2013 to Telavox SIP Trunk:
- Click **Add**.

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

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

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



The screenshot shows the 'Rule' tab selected in a configuration interface. The form contains the following parameters and their values:

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

At the bottom right are two buttons: **Submit** (with a checkmark icon) and **Cancel**.

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

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

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

		<b>Action</b>
Index	1	
Destination Type	IP Group	
Destination IP Group ID	2	
Destination SRD ID	2	
Destination Address		
Destination Port	0	
Destination Transport Type		
Alternative Route Options	Route Row	
Group Policy	None	
Cost Group	None	
Rules Set Id	-1	
<input checked="" type="button"/> <b>Submit</b> <input type="button"/> <b>Cancel</b>		

**10.** Configure a rule to route calls from Telavox SIP Trunk to Lync Server 2013:

**11.** Click **Add**.

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

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

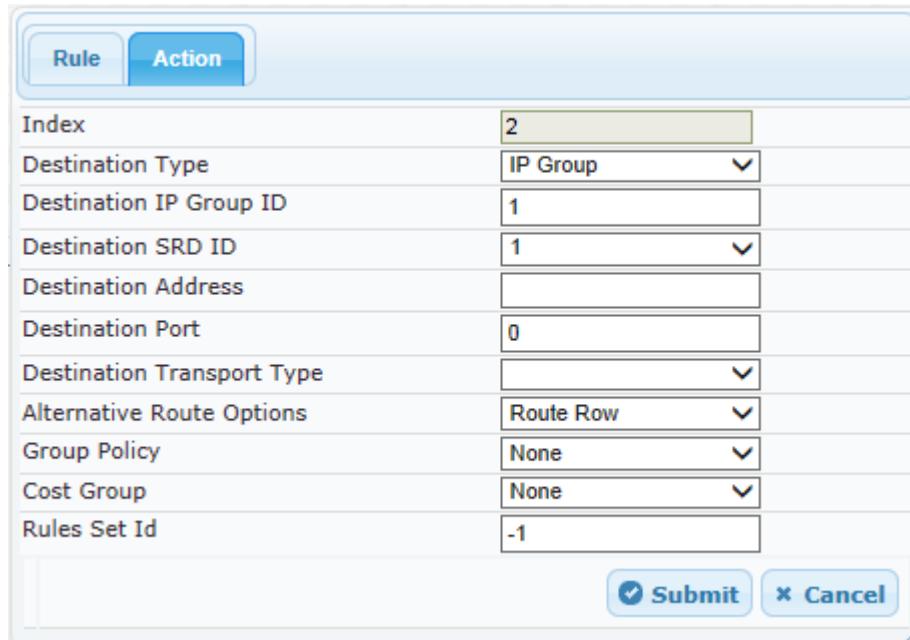
**Figure 4-35: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab**

		<b>Rule</b>	<b>Action</b>
Index	2		
Route Name	ITSP to Lync		
Source IP Group ID	2		
Source Username Prefix	*		
Source Host	*		
Destination Username Prefix	*		
Destination Host	*		
Request Type	All		
Message Condition	None		
ReRoute IP Group ID	-1		
Call Trigger	Any		
<input checked="" type="button"/> <b>Submit</b> <input type="button"/> <b>Cancel</b>			

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

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

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

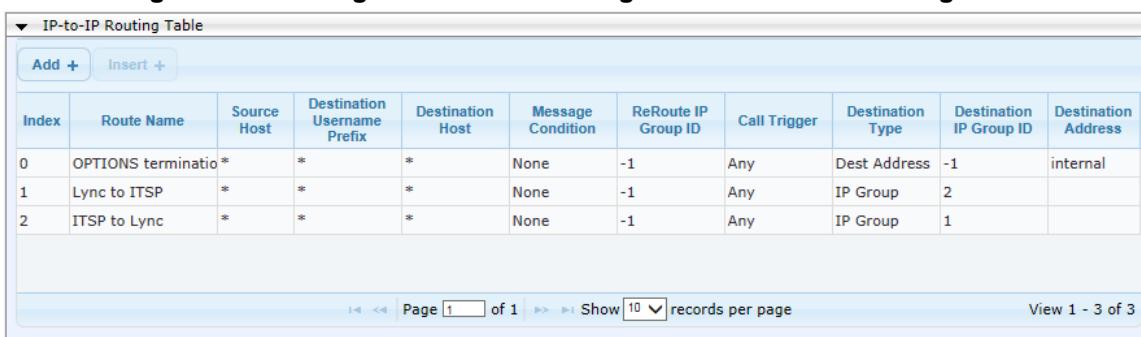


Index	2
Destination Type	IP Group
Destination IP Group ID	1
Destination SRD ID	1
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
Rules Set Id	-1

Submit     Cancel

The configured routing rules are shown in the figure below:

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



Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Destination Type	Destination IP Group ID	Destination Address
0	OPTIONS terminatio*	*	*	None	-1	Any	Dest Address	-1	internal	
1	Lync to ITSP	*	*	None	-1	Any	IP Group	2		
2	ITSP to Lync	*	*	None	-1	Any	IP Group	1		

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



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

## 4.12 Step 12: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 43, IP Group 1 represents Lync Server 2013, and IP Group 2 represents Telavox SIP Trunk.



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

For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from IP Group 2 (Telavox SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

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

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

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

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

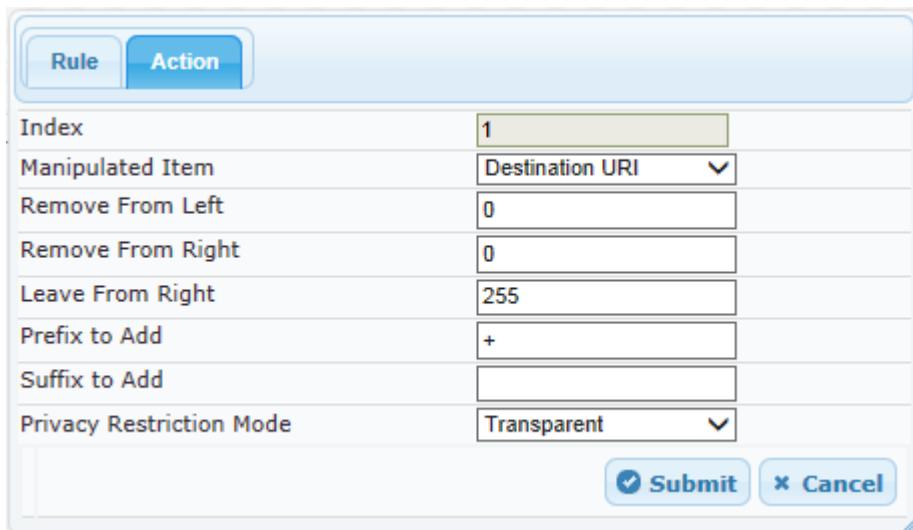
Index	1
Manipulation Name	
Additional Manipulation	No
Source IP Group ID	2
Destination IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Calling Name Prefix	*
Message Condition	None
Request Type	All
ReRoute IP Group ID	-1
Call Trigger	Any

**Submit** **Cancel**

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

Parameter	Value
Manipulated Item	<b>Destination URI</b>
Prefix to Add	<b>+</b> (plus sign)

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



Index	1
Manipulated Item	Destination URI
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	
Privacy Restriction Mode	Transparent

**Submit**     **Cancel**

5. Click **Submit**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between IP Group 1 (i.e., Lync Server 2013) and IP Group 2 (i.e., Telavox SIP Trunk):

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

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

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

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

## 4.13 Step 13: 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 the Telavox SIP Trunk. This rule is applied to response messages sent to the Telavox SIP Trunk (IP Group 2) for Rejected Calls initiated by the Lync Server 2013 (IP Group 1). This replaces the method type '603' with the value '486', because Telavox SIP Trunk does not recognize the '603' method type.

Parameter	Value
Index	0
Manipulation name	Reject Call
Manipulation Set ID	4
Message Type	any.response
Condition	header.request-uri.methodtype=='603'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'486'
Row Role	Use Current Condition

Figure 4-41: Configuring SIP Message Manipulation Rule 9 (for Telavox SIP Trunk)

The screenshot shows a configuration dialog titled 'Edit Record #0'. It contains the following fields:

Index	0
Manipulation Name	Reject Call
Manipulation Set ID	4
Message Type	any.response
Condition	header.request-uri.methodtype=='603'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'486'
Row Role	Use Current Condition

At the bottom right are two buttons: 'Submit' and 'Cancel'.

3. Assign Manipulation Set ID 4 to IP Group 2:
  - a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
  - b. Select the row of IP Group 2, and then click **Edit**.
  - c. Click the **SBC** tab.
  - d. Set the 'Outbound Message Manipulation Set' field to 4.

**Figure 4-42: Assigning Manipulation Set 4 to IP Group 2**

		<b>Common</b>	<b>GW</b>	<b>SBC</b>
Index	<input type="text" value="2"/>			
Classify By Proxy Set	<input type="text" value="Enable"/> 			
Max. Number of Registered Users	<input type="text" value="-1"/>			
Inbound Message Manipulation Set	<input type="text" value="-1"/>			
Outbound Message Manipulation Set	<input type="text" value="4"/>			
Registration Mode	<input type="text" value="User Initiates Registr."/> 			
Authentication Mode	<input type="text" value="User Authenticates"/> 			
Authentication Method List	<input type="text"/>			
SBC Client Forking Mode	<input type="text" value="Sequential"/> 			
Source URI Input	<input type="text" value="Not Configured"/> 			
Destination URI Input	<input type="text" value="Not Configured"/> 			
Username	<input type="text"/>			
Password	<input type="text"/>			
<input checked="" type="button" value="Submit"/>  <input type="button" value="Cancel"/>				

- e. Click **Submit**.

## 4.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

### 4.14.1 Step 14a: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if 18x 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 180 response without SDP is received. It's 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 4-43: Configuring Forking Mode**

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

3. Click **Submit**.

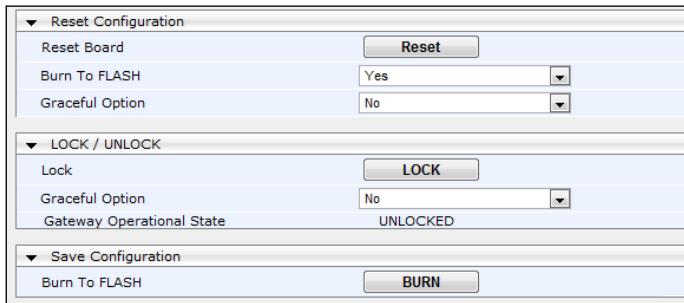
## 4.15 Step 15: Reset the E-SBC

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

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

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

**Figure 4-44: Resetting the E-SBC**



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

## A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 29, is shown below:



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

```

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69 FK Board Type: 77
;Serial Number: 2265355
;Slot Number: 1
;Software Version: 6.80A.006.004
;DSP Software Version: 5014AE3_R => 680.17
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M Flash size: 64M Core speed: 300Mhz
;Num of DSP Cores: 3 Num DSP Channels: 62
;Num of physical LAN ports: 12
;Profile: NONE
;Key features:;Board Type: 77 ;PSTN FALBACK Supported ;E1Trunks=2
;T1Trunks=2 ;FXSPorts=4 ;FXOPorts=4 ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;DSP Voice features:
IpmDetector RTCP-XR AMRPolicyManagement ;Channel Type: RTP DspCh=62
IPMediaDspCh=62 ;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 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;Control Protocols: MSFT CLI
TRANSCODING=60 FEU=100 TestCall=100 MGCP MEGACO H323 SIP TPNCP
SASurvivability SBC=60 ;Default features:;Coders: G711 G726;

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

[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '10.15.25.1'

```

```
[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10

[Analog Params]

FarEndDisconnectType = 7

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]

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

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UseRProductName = 'Mediant 800 E-SBC'
WebLogoText = 'Telavox'
UseWeblogo = 1
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
DNSQUERYTYPE = 1
PROXYDNSQUERYTYPE = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
```

```

[SCTP Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[PhysicalPortsTable]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 2, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 1, 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 1, 4, "User Port #7", "GROUP_4",
"Redundant";
PhysicalPortsTable 8 = "FE_5_5", 1, 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 1, 4, "User Port #11", "GROUP_6",
"Redundant";

[\PhysicalPortsTable]

[EtherGroupTable]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 2, "FE_5_1", "FE_5_2";
EtherGroupTable 3 = "GROUP_4", 2, "FE_5_3", "FE_5_4";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";

[\EtherGroupTable]

```

```

[ DeviceTable ]

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

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.77, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.157, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

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

[ \DspTemplates ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 10, 6090, 1, "", "";
CpMediaRealm 1 = "MRWan", "WANSP", "", 7000, 10, 7090, 0, "", "";

[ \CpMediaRealm ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "SRDLan", "MRLan", 0, 0, -1, 1;
SRD 2 = "SRDWan", "MRWan", 0, 0, -1, 1;

```

```
[ \SRD ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIpIpAddress, ProxyIpTransportType,
ProxyIpProxySetId;
ProxyIp 0 = "FE15.ilync15.local:5067", 2, 1;
ProxyIp 1 = "siptrunk.telavox.se", -1, 2;

[ \ProxyIp ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfileProfileName, IpProfileIpPreference,
IpProfileCodersGroupID, IpProfileIsFaxUsed,
IpProfileJitterBufMinDelay, IpProfileJitterBufOptFactor,
IpProfileIPDiffServ, IpProfileSigIPDiffServ, IpProfileSCE,
IpProfileRTPRedundancyDepth, IpProfileRemoteBaseUDPPort,
IpProfileCNGmode, IpProfileVxxTransportType, IpProfileNSEMode,
IpProfileIsDTMFUsed, IpProfilePlayRBTone2IP,
IpProfileEnableEarlyMedia, IpProfileProgressIndicator2IP,
IpProfileEnableEchoCanceller, IpProfileCopyDest2RedirectNumber,
IpProfileMediaSecurityBehaviour, IpProfileCallLimit,
IpProfileDisconnectOnBrokenConnection, IpProfileFirstTxDtmfOption,
IpProfileSecondTxDtmfOption, IpProfileRxDTMFOption,
IpProfileEnableHold, IpProfileInputGain, IpProfileVoiceVolume,
IpProfileAddIEInSetup, IpProfileSBCExtensionCodersGroupID,
IpProfileMediaIPVersionPreference, IpProfileTranscodingMode,
IpProfileSBCAllowedMediaTypes, IpProfileSBCAllowedCodersGroupID,
IpProfileSBCAllowedVideoCodersGroupID, IpProfileSBCAllowedCodersMode,
IpProfileSBCMediaSecurityBehaviour, IpProfileSBCRFC2833Behavior,
IpProfileSBCAlternativeDTMFMethod, IpProfileSBCAssertIdentity,
IpProfileAMDSensitivityParameterSuit, IpProfileAMDSensitivityLevel,
IpProfileAMDMaxGreetingTime, IpProfileAMDMaxPostSilenceGreetingTime,
IpProfileSBCDiversionMode, IpProfileSBCHistoryInfoMode,
IpProfileEnableQSIGTunneling, IpProfileSBCFaxCodersGroupID,
IpProfileSBCFaxBehavior, IpProfileSBCFaxOfferMode,
IpProfileSBCFaxAnswerMode, IpProfileSbcPrackMode,
IpProfileSBCSessionExpiresMode, IpProfileSBCRemoteUpdateSupport,
IpProfileSBCRemoteReinviteSupport,
IpProfileSBCRemoteDelayedOfferSupport, IpProfileSBCRemoteReferBehavior,
IpProfileSBCRemote3xxBehavior, IpProfileSBCRemoteMultiple18xSupport,
IpProfileSBCRemoteEarlyMediaResponseType,
IpProfileSBCRemoteEarlyMediaSupport, IpProfileEnableSymmetricMKI,
IpProfileMKISize, IpProfileSBCEnforceMKISize,
IpProfileSBCRemoteEarlyMediaRTP, IpProfileSBCRemoteSupportsRFC3960,
IpProfileSBCRemoteCanPlayRingback, IpProfileEnableEarly183,
IpProfileEarlyAnswerTimeout, IpProfileSBC2833DTMFPayloadType,
IpProfileSBCUserRegistrationTime, IpProfileResetSRTPStateUponRekey,
IpProfileAmdMode, IpProfileSBCReliableHeldToneSource,
IpProfileGenerateSRTPKeys, IpProfileSBCPlayHeldTone,
IpProfileSBCRemoteHoldFormat, IpProfileSBCRemoteReplacesBehavior,
IpProfileSBCSDPPTimeAnswer, IpProfileSBCPreferredPTime,
IpProfileSBCUseSilenceSupp, IpProfileSBCRTPRedundancyBehavior,
IpProfileSBCPlayRBTTToTransferee, IpProfileSBCRTCPMode,
IpProfileSBCJitterCompensation,
IpProfileSBCRemoteRenegotiateOnFaxDetection,
IpProfileJitterBufMaxDelay;
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, "", -1, -1, 0, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, -1, 0, 0, 1, 1, 0, 1, 0, 3, 2, 1, 0, 1,
```



```

IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS termination", 1, "*", "**", "**", "*", 6, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "Lync to ITSP", 1, "*", "**", "**", "**", 0, "", -1, 0, -1,
0, 2, "", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to Lync", 2, "*", "**", "**", "**", 0, "", -1, 0, -1,
0, 1, "", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType;
SIPInterface 1 = "Lync", "Voice", 2, 0, 0, 5067, 1, "", -1, 0, 500;
SIPInterface 2 = "Telavox", "WANSP", 2, 5060, 0, 0, 2, "", -1, 0, 500;

[ \SIPInterface ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 1 = "", 0, 2, 1, "*", "**", "**", "**", "*", "", 0, -1,
1, 0, 1, 0, 255, "+", "", 0;
IPOutboundManipulation 2 = "", 0, 1, 2, "*", "**", "+", "**", "**", "", 0, -1,
0, 1, 3, 0, 255, "00", "", 0;
IPOutboundManipulation 3 = "", 0, 1, 2, "+", "**", "**", "**", "**", "", 0, -1,
0, 0, 1, 0, 255, "", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

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

```

```
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 1;
[ \CodersGroup0 ]

[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Ulaw64k";
AllowedCodersGroup1 1 = "g711Alaw64k";
AllowedCodersGroup1 2 = "gsmFullRate";

[ \AllowedCodersGroup1 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Reject Call", 4, "any.response",
"header.request-uri.methodtype=='603'", "header.request-uri.methodtype",
2, "'486'", 0;

[ \MessageManipulations ]

[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]

[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]
```

**Reader's Notes**





## Configuration Note