AudioCodes Mediant™ Series

Enterprise Session Border Controllers (E-SBC)

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2013 with XO Communications SIP Trunk using AudioCodes Mediant E-SBC

Version 1.0

May 2013

Document # LTRT-40821

Table of Contents

List of Figures

List of Tables

Notice

This document describes how to connect the Microsoft Lync Server 2013 and XO Communications SIP Trunk using AudioCodes Mediant E-SBC product series, which includes the Mediant 800 Gateway & E-SBC, Mediant 1000B Gateway & E-SBC, Mediant 3000 Gateway & E-SBC, and Mediant 4000 E-SBC.

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.

This document is subject to change without notice.

Date Published: May-26-2013

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, 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.

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 XO Communication's SIP Trunk and Microsoft's Lync Server 2013 environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and XO Communications Partners who are responsible for installing and configuring XO Communication'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

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.60A.228.002
Protocol	▪ SIP/UDP (to the XO Communications SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 XO Communications SIP Trunking Version

Table 2-2: XO Communications Version

Vendor/Service Provider	XO Communications
SSW Model/Service	Sonus SBC
Software Version	
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 5.0.8308.291 CU1
Protocol	SIP
Additional Notes	None

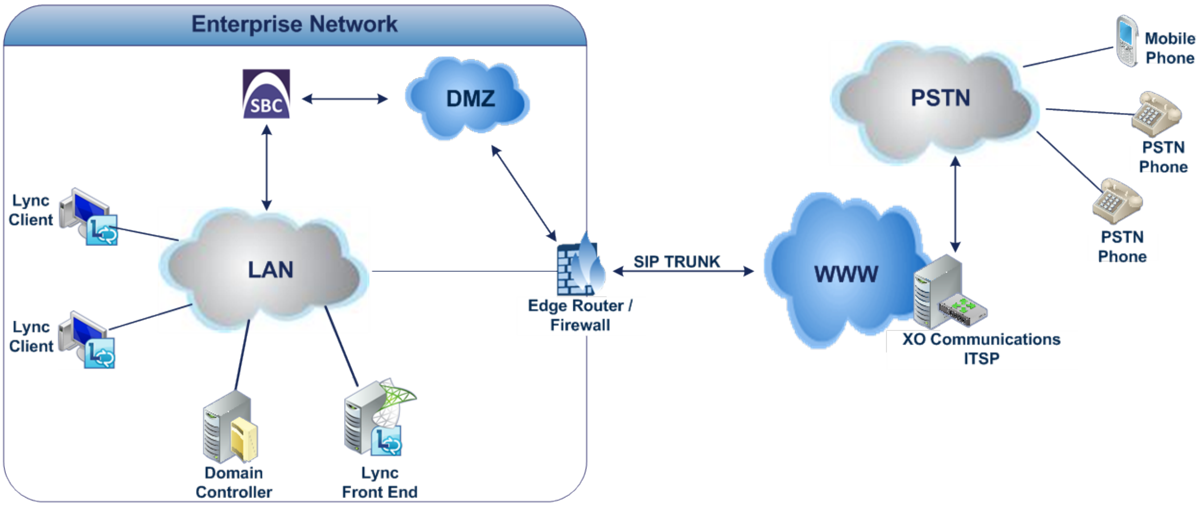
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and XO Communications 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 XO Communication'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 XO Communication'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 XO Communications SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

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

2.4.2 Known Limitations

XO Communications SIP Trunk doesn’t send early media DTMF.

When the Lync client is configured to have a call forward to an early media IVR, the PSTN user is unable to navigate the IVR menu using DTMF.

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.

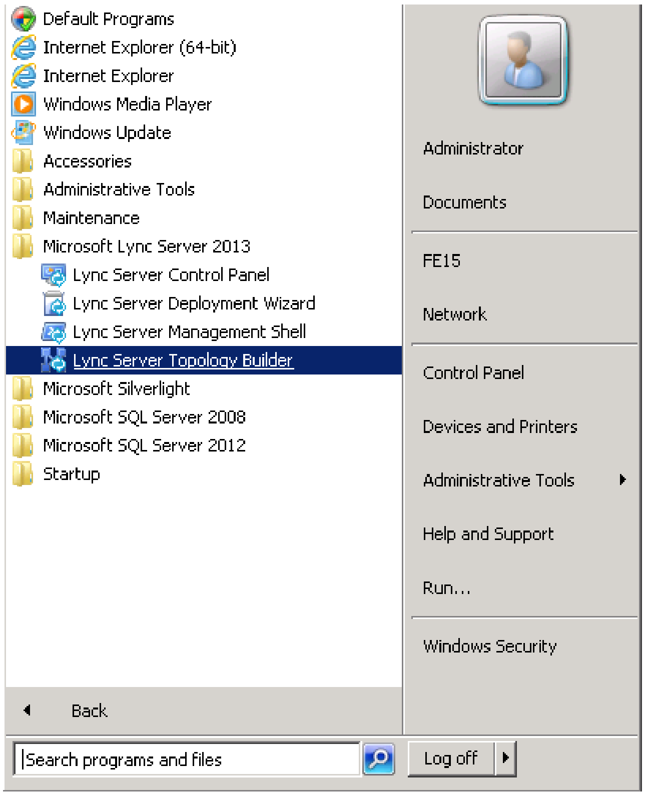
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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:**

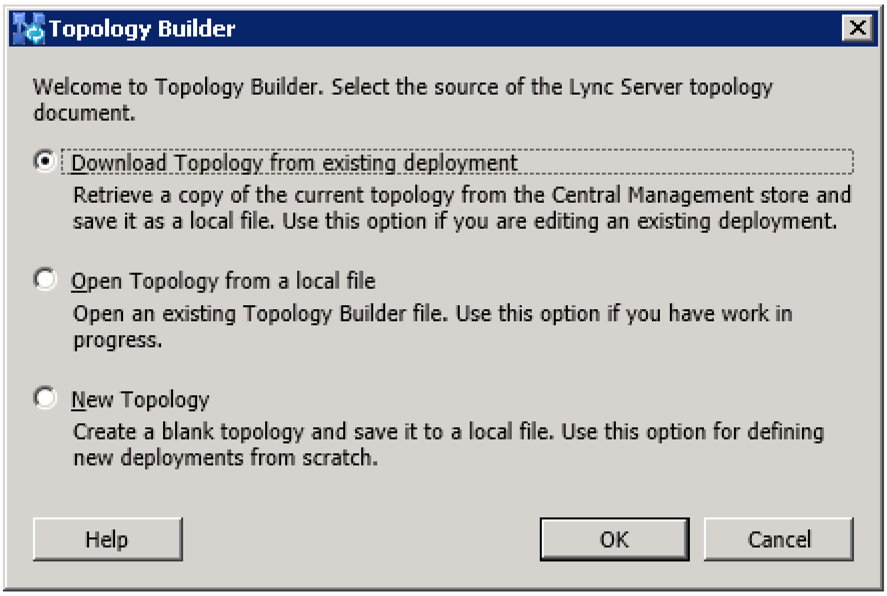
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



The following is displayed:

Figure 3-2: Topology Builder Dialog Box



Welcome to Topology Builder. Select the source of the Lync Server topology document.

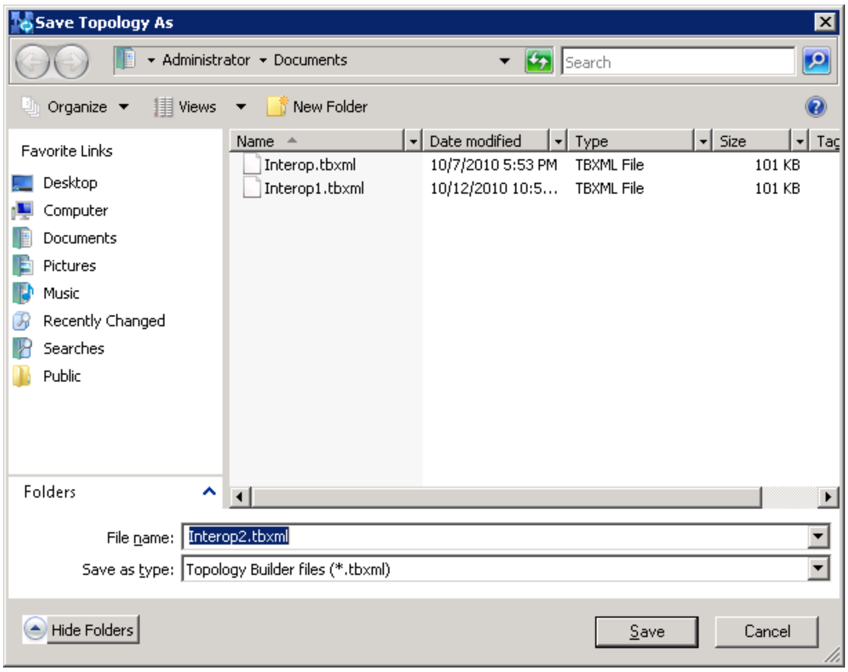
● Download Topology from existing deployment
Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.

○ Open Topology from a local file
Open an existing Topology Builder file. Use this option if you have work in progress.

○ New Topology
Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.

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



Name	Date modified	Type	Size	Tag
Interop.tbxml	10/7/2010 5:53 PM	TBXML File	101 KB	
Interop1.tbxml	10/12/2010 10:5...	TBXML File	101 KB	

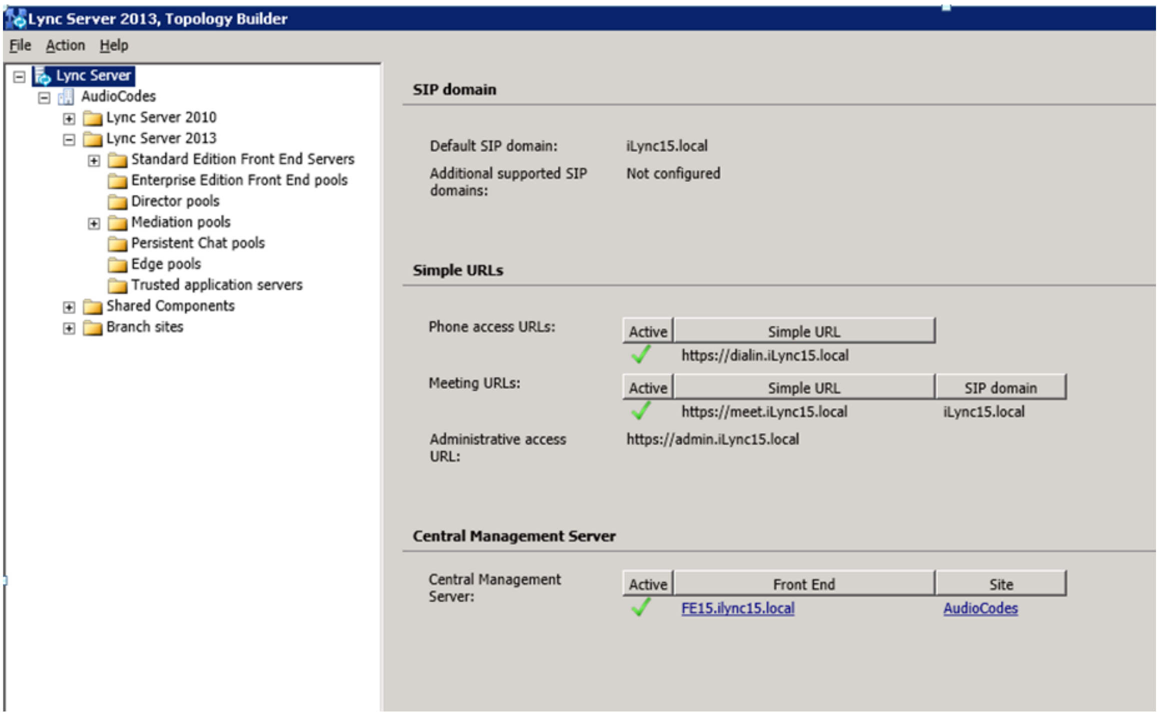
File name: Interop2.tbxml

Save as type: Topology Builder files (*.tbxml)

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



SIP domain

Default SIP domain: iLync15.local

Additional supported SIP domains: Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://dialin.iLync15.local

Meeting URLs:

Active	Simple URL	SIP domain
✓	https://meet.iLync15.local	iLync15.local

Administrative access URL: https://admin.iLync15.local

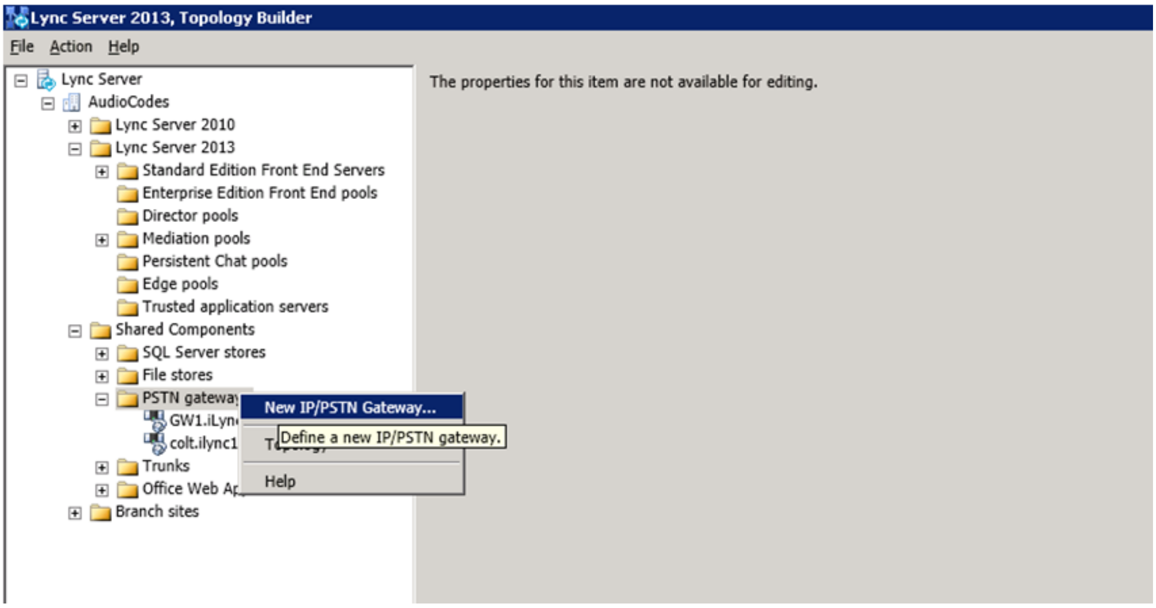
Central Management Server

Central Management Server:

Active	Front End	Site
✓	FE15.ilync15.local	AudioCodes

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:

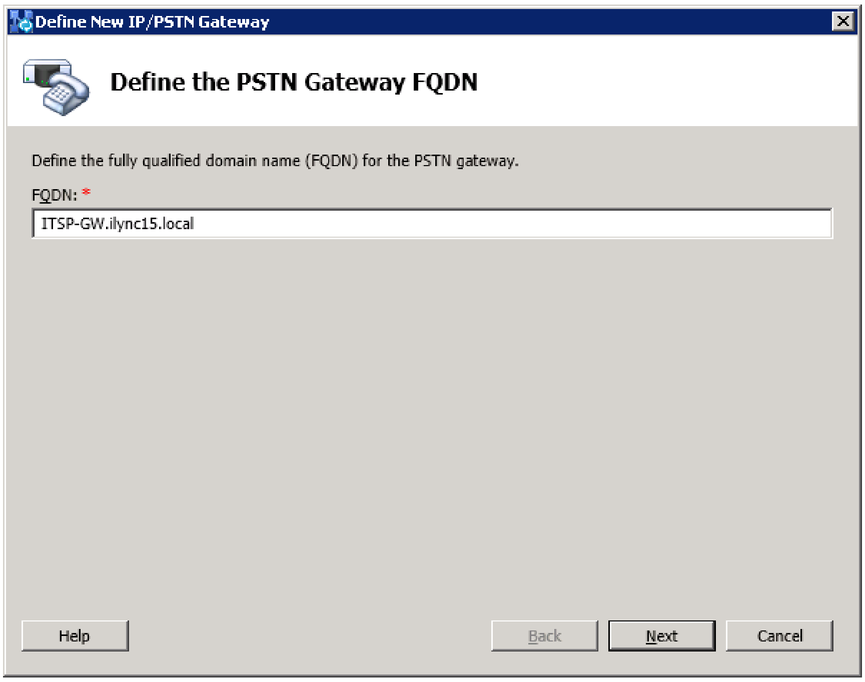
Figure 3-5: Choosing New IP/PSTN Gateway



The properties for this item are not available for editing.

The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



Define New IP/PSTN Gateway

Define the PSTN Gateway FQDN

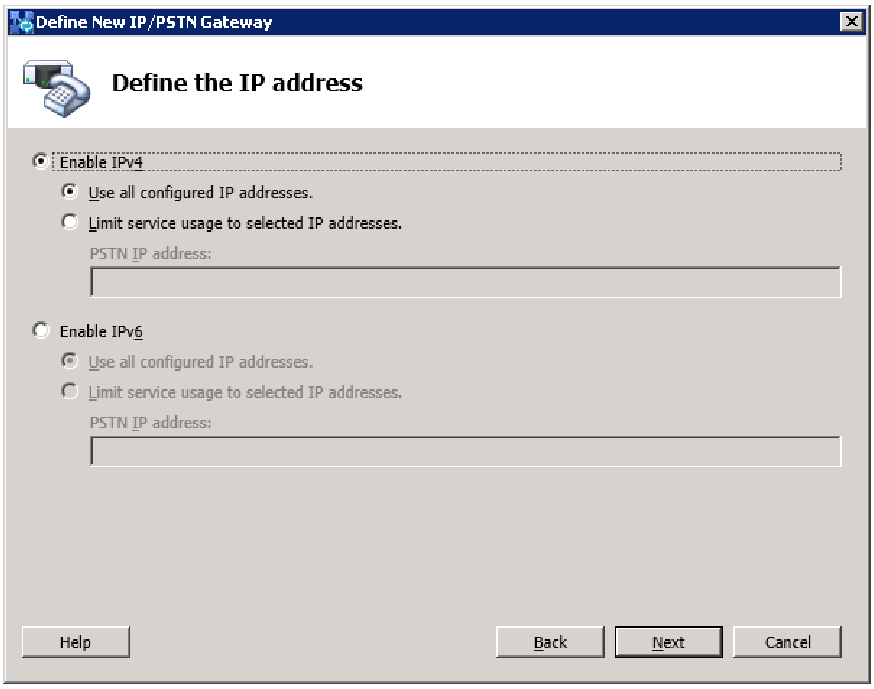
Define the fully qualified domain name (FQDN) for the PSTN gateway.

FQDN: *

ITSP-GW.ilync15.local

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



Define New IP/PSTN Gateway

Define the IP address

● Enable IPv4

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

○ Enable IPv6

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

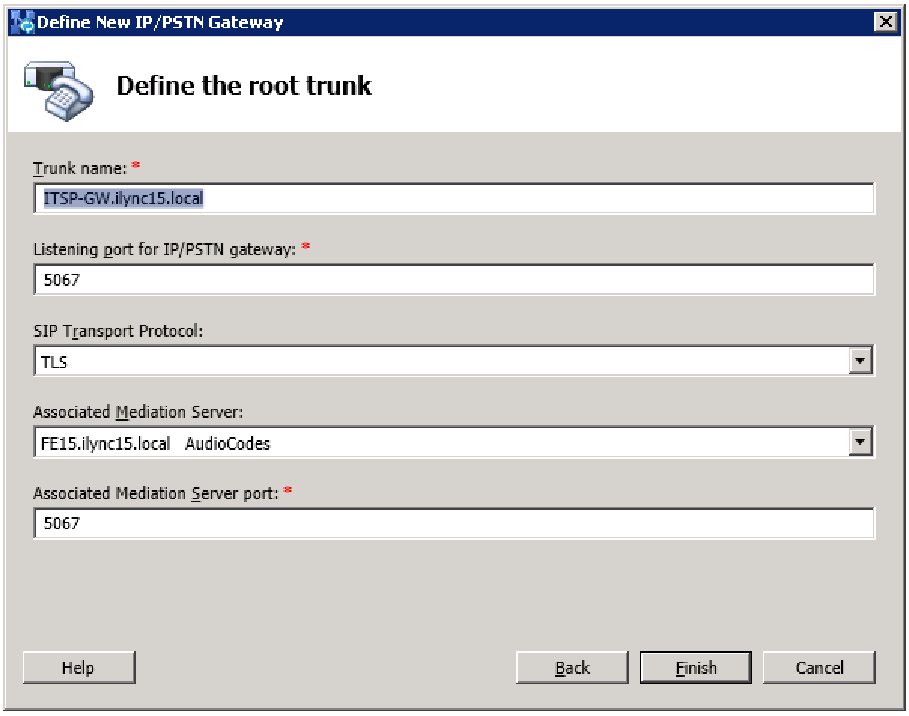
6. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

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



Define New IP/PSTN Gateway

Define the root trunk

Trunk name: * ITSP-GW.ilync15.local

Listening port for IP/PSTN gateway: * 5067

SIP Transport Protocol: TLS

Associated Mediation Server: FE15.ilync15.local AudioCodes

Associated Mediation Server port: * 5067

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.

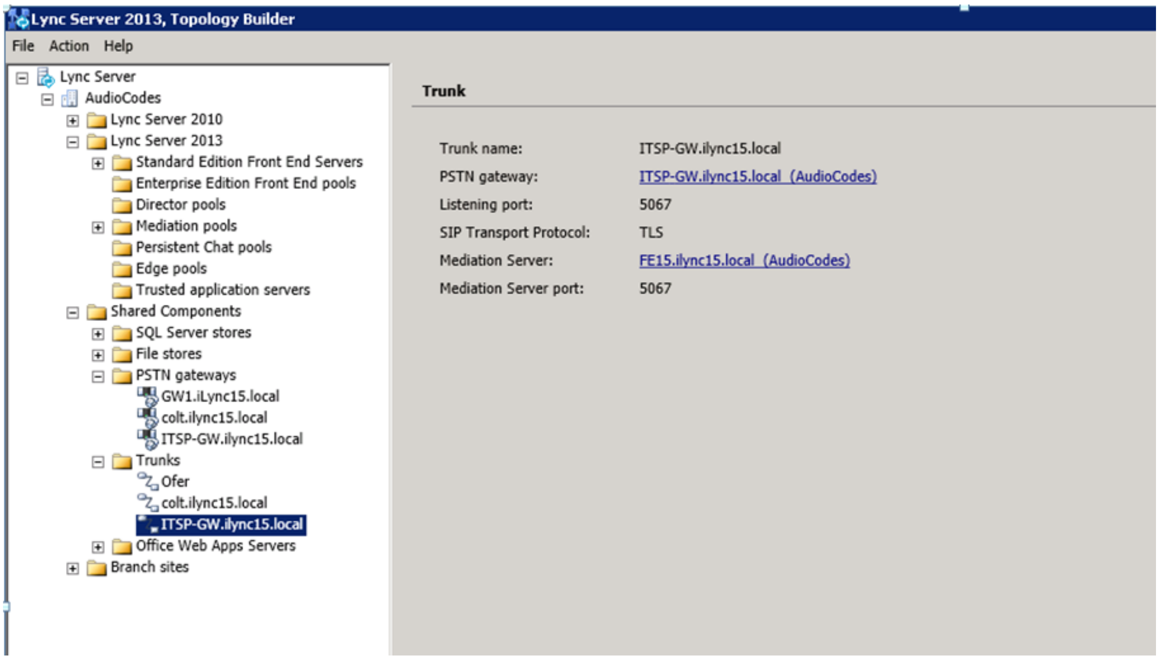
c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.

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:

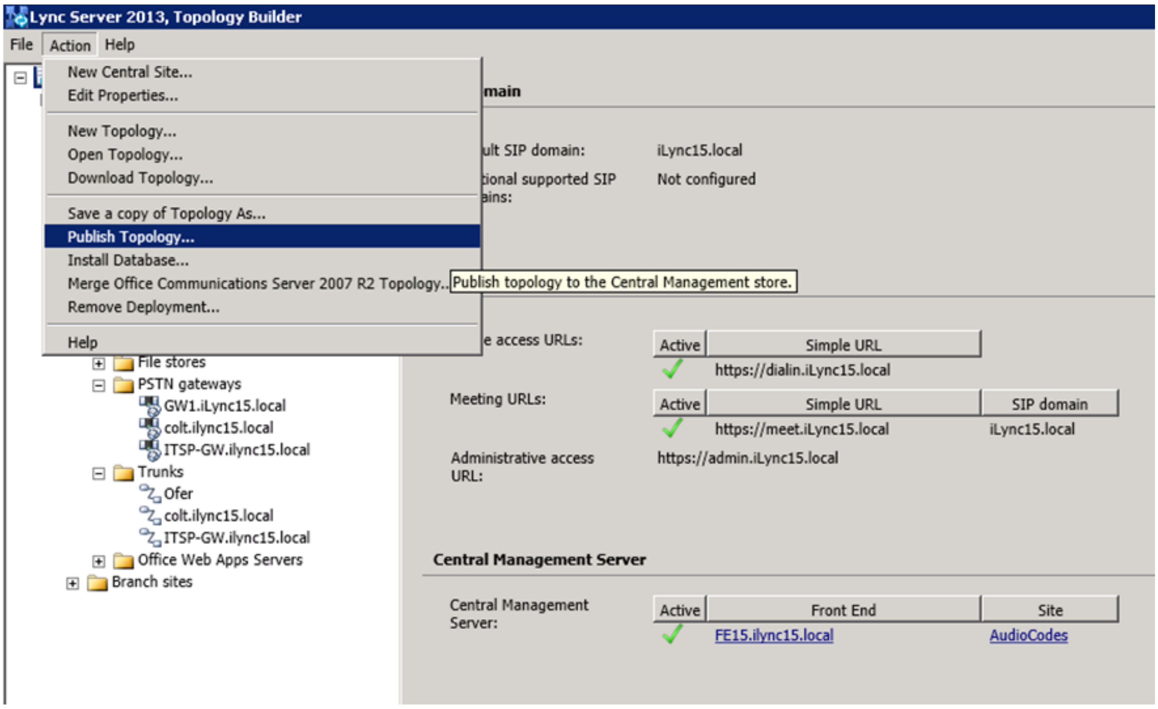
Figure 3-9: E-SBC added as IP/PSTN Gateway and Trunk Created



Trunk name: ITSP-GW.ilync15.local
PSTN gateway: ITSP-GW.ilync15.local (AudioCodes)
Listening port: 5067
SIP Transport Protocol: TLS
Mediation Server: FE15.ilync15.local (AudioCodes)
Mediation Server port: 5067

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



ult SIP domain: iLync15.local
tional supported SIP ains: Not configured

e access URLs:

Active	Simple URL
✓	https://dialin.iLync15.local

Meeting URLs:

Active	Simple URL	SIP domain
✓	https://meet.iLync15.local	iLync15.local

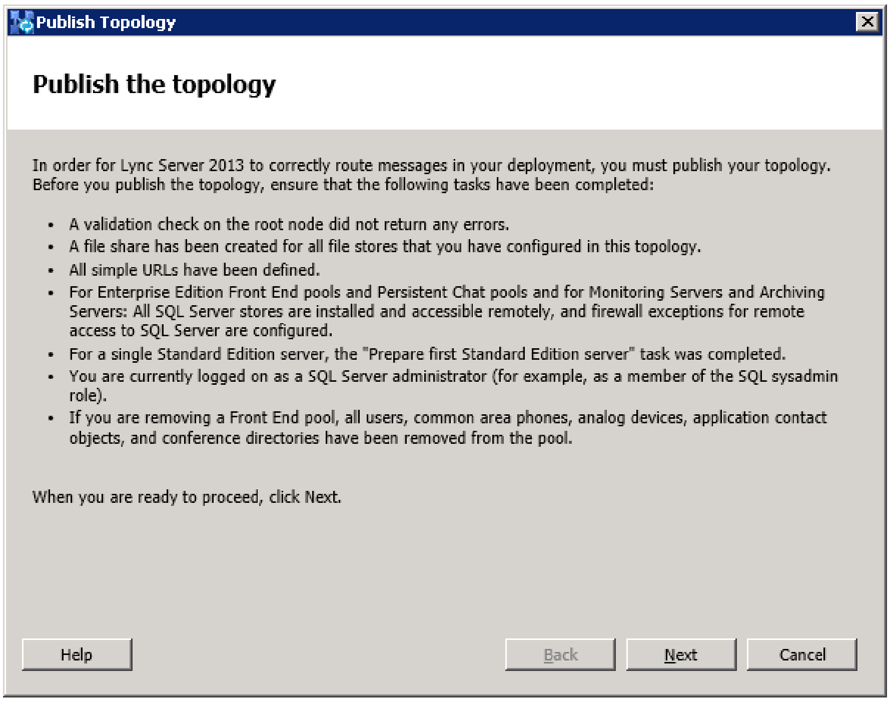
Administrative access URL: https://admin.iLync15.local

Central Management Server:

Active	Front End	Site
✓	FE15.ilync15.local	AudioCodes

The following is displayed:

Figure 3-11: Publish the Topology



Publish Topology

Publish the topology

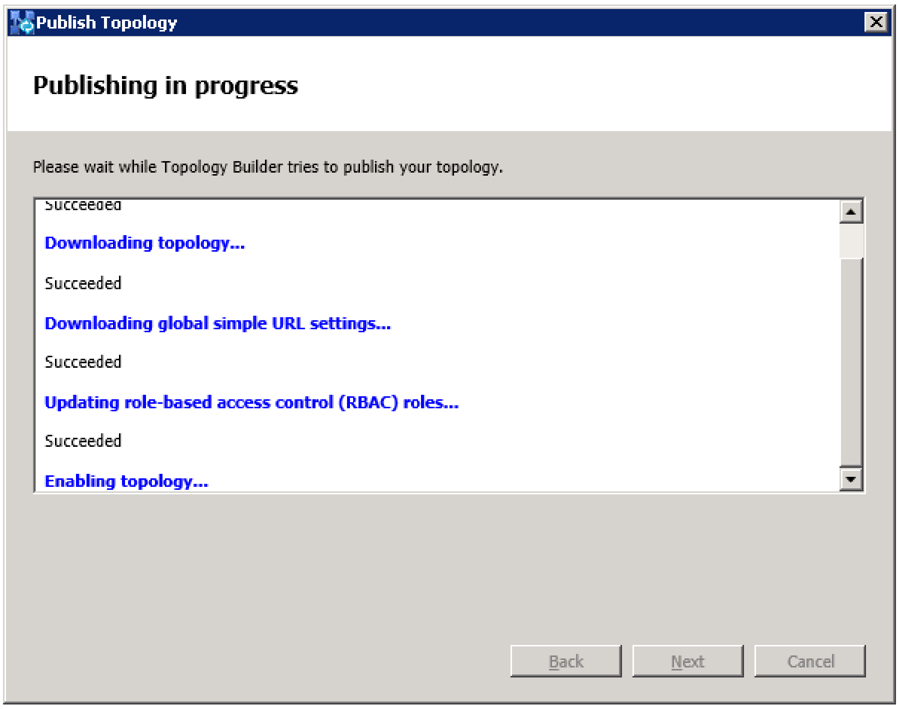
In order for Lync Server 2013 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:

- A validation check on the root node did not return any errors.
- A file share has been created for all file stores that you have configured in this topology.
- All simple URLs have been defined.
- For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured.
- For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.
- You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).
- If you are removing a Front End pool, all users, common area phones, analog devices, application contact objects, and conference directories have been removed from the pool.

When you are ready to proceed, click Next.

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

Figure 3-12: Publishing in Progress



Publish Topology

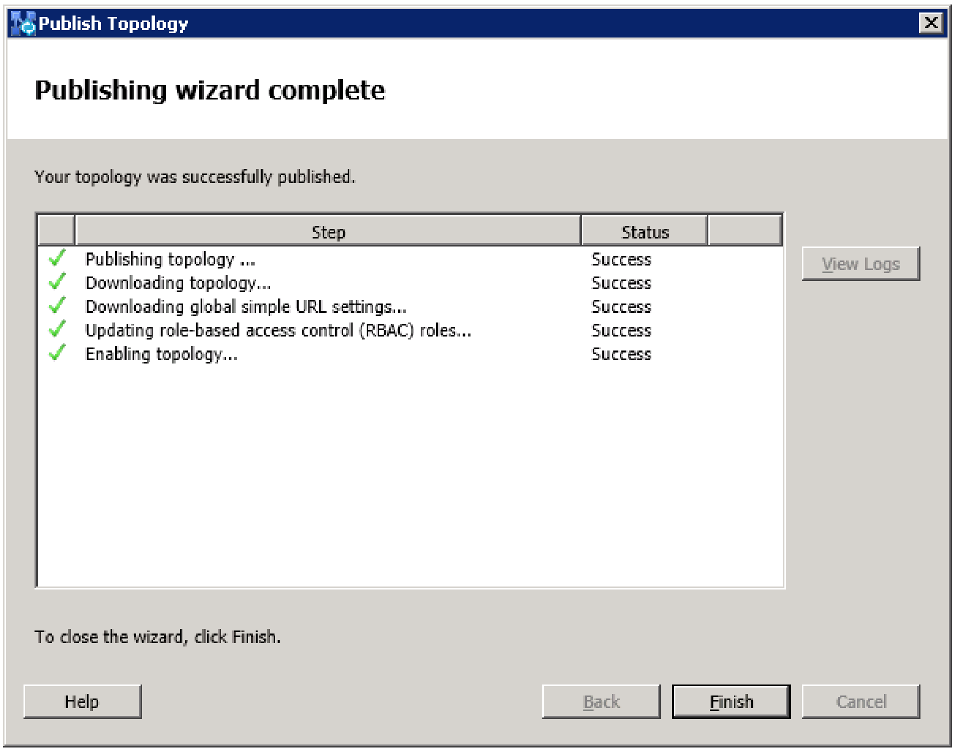
Publishing in progress

Please wait while Topology Builder tries to publish your topology.

```
Succeeded
Downloading topology...
Succeeded
Downloading global simple URL settings...
Succeeded
Updating role-based access control (RBAC) roles...
Succeeded
Enabling topology...
```

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

Figure 3-13: Publishing Wizard Complete



Publish Topology

Publishing wizard complete

Your topology was successfully published.

	Step	Status
✓	Publishing topology ...	Success
✓	Downloading topology...	Success
✓	Downloading global simple URL settings...	Success
✓	Updating role-based access control (RBAC) roles...	Success
✓	Enabling topology...	Success

To close the wizard, click Finish.

11. Click **Finish**.

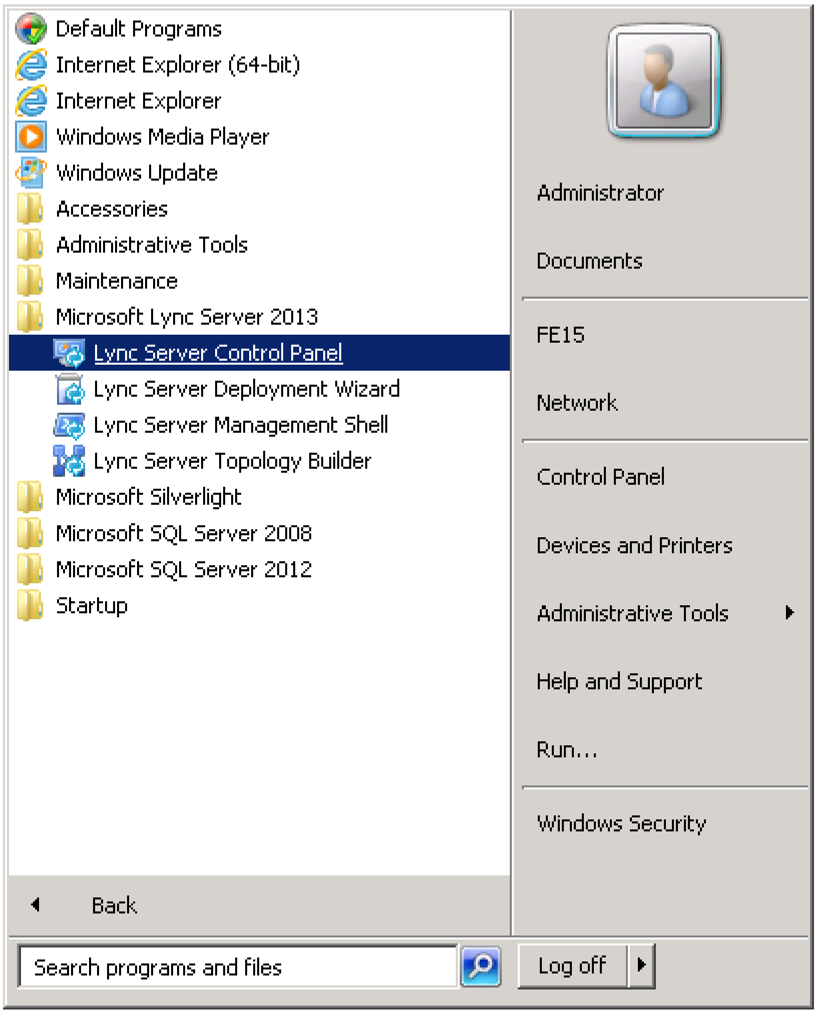
3.2 Configuring the "Route" on Lync Server 2013

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:**

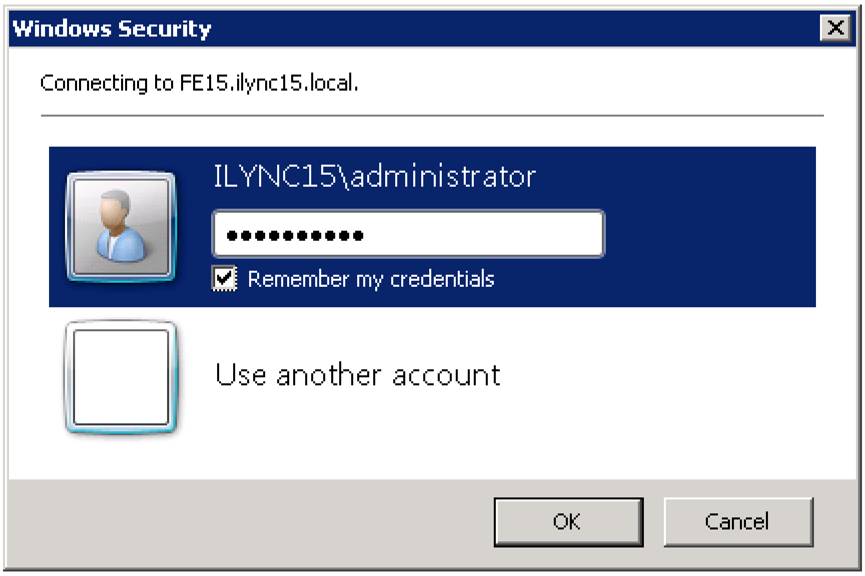
1. Start the Microsoft Lync Server 2013 Control Panel (**Start** > **All Programs** > **Microsoft Lync Server 2013** > **Lync Server Control Panel**), as shown below:

Figure 3-14: Opening the Lync Server Control Panel



You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



Windows Security

Connecting to FE15.ilync15.local.

ILYNC15\administrator

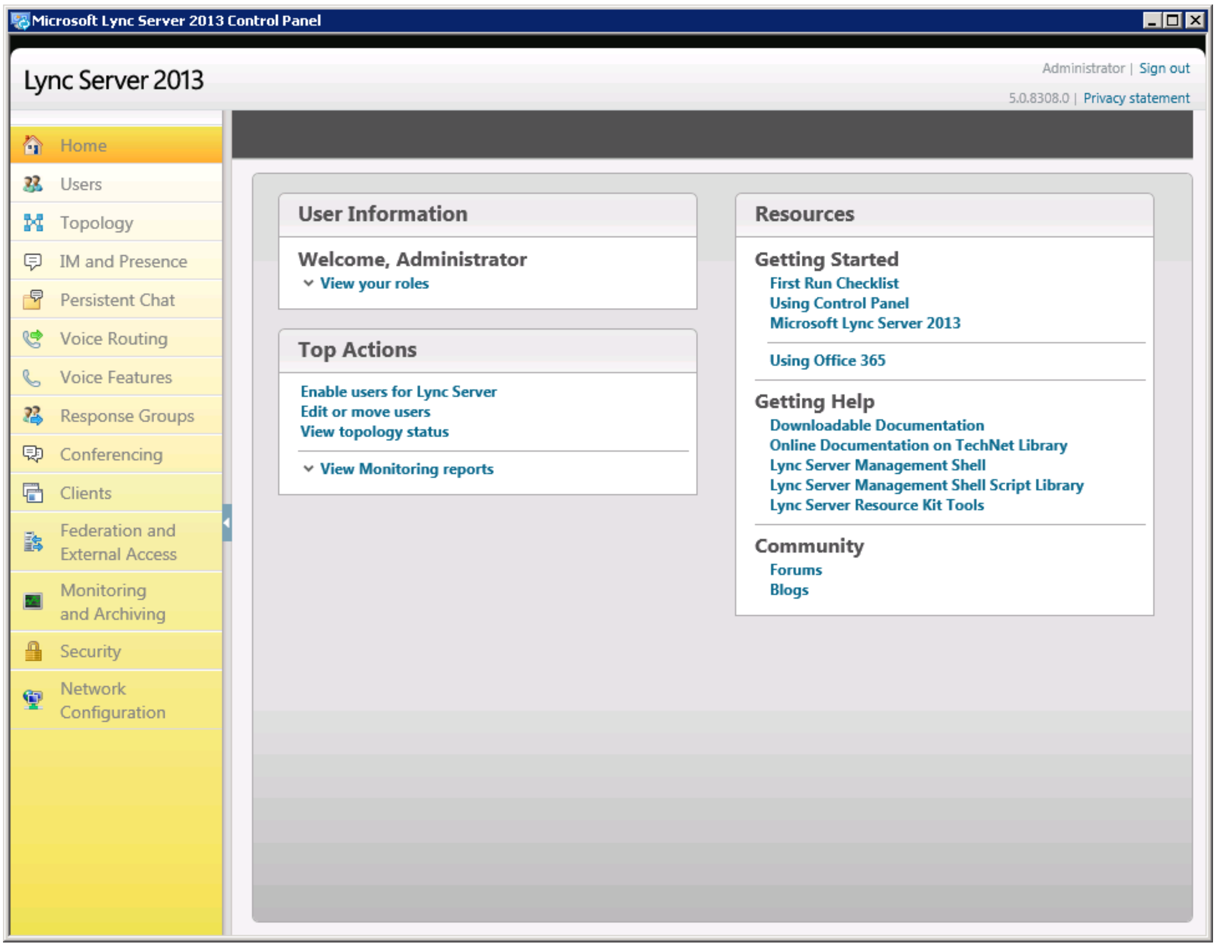
●●●●●●●●●●●

☑ Remember my credentials

Use another account

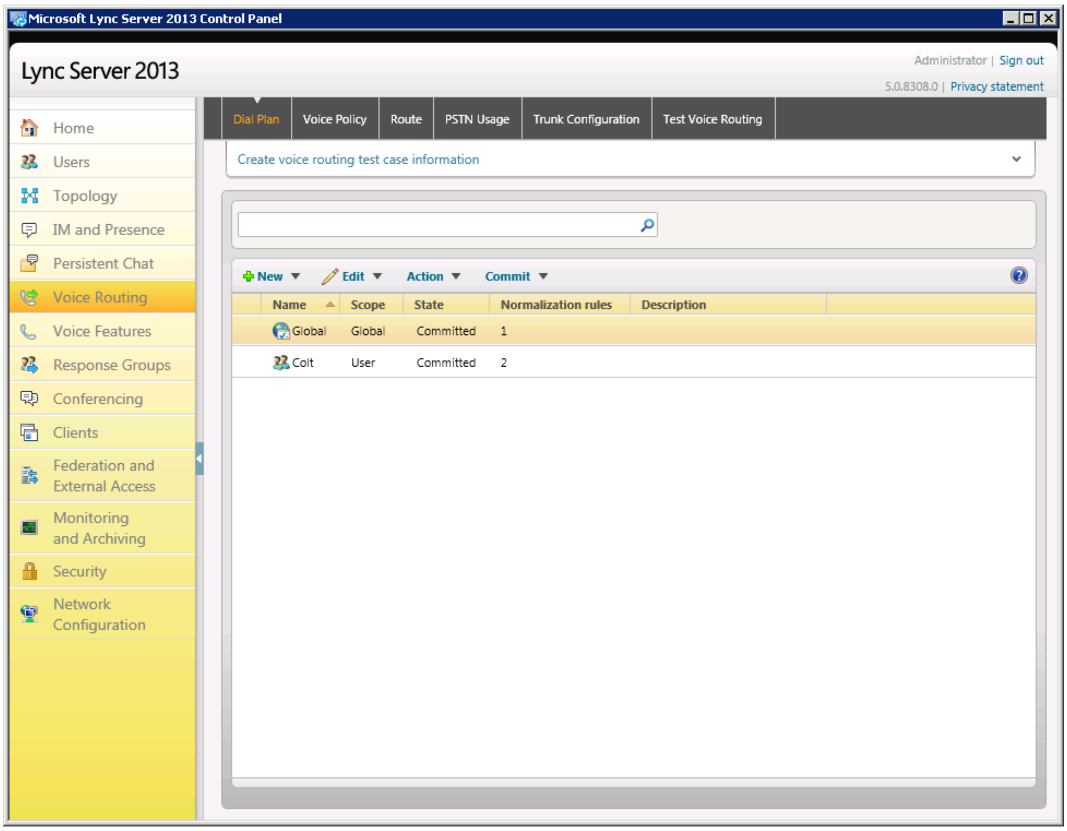
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



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

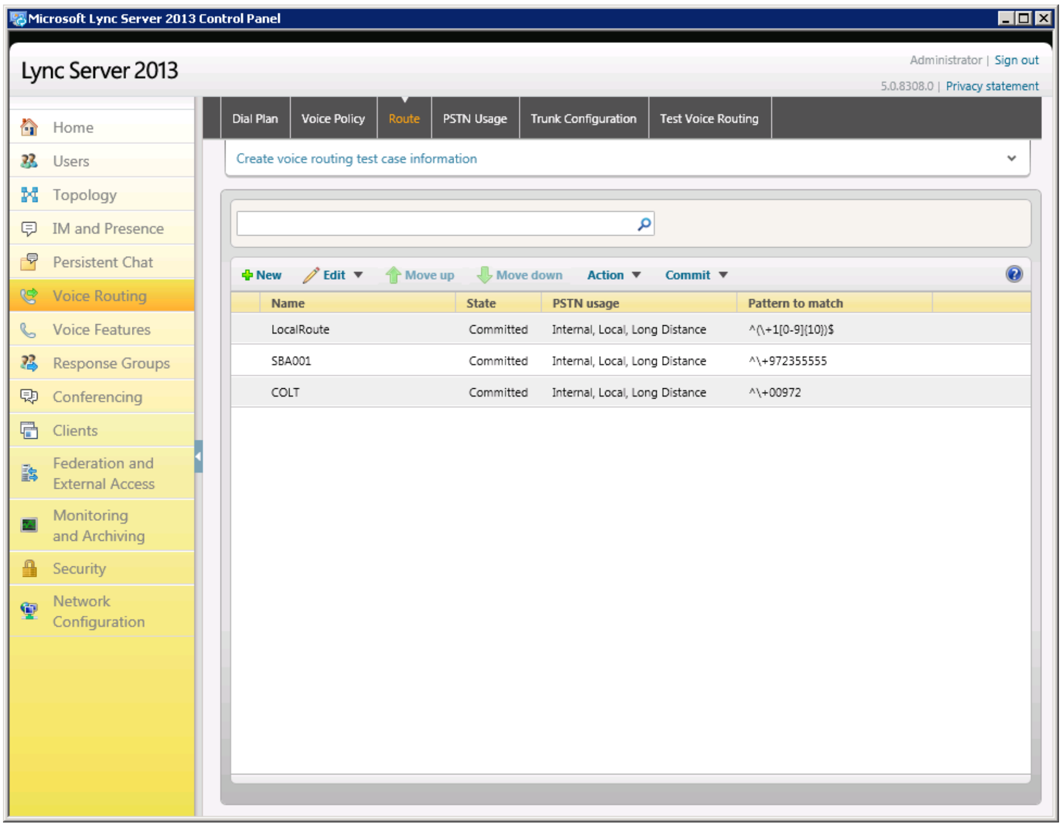
Figure 3-17: Voice Routing Page



Name	Scope	State	Normalization rules	Description
Global	Global	Committed	1	
Colt	User	Committed	2	

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

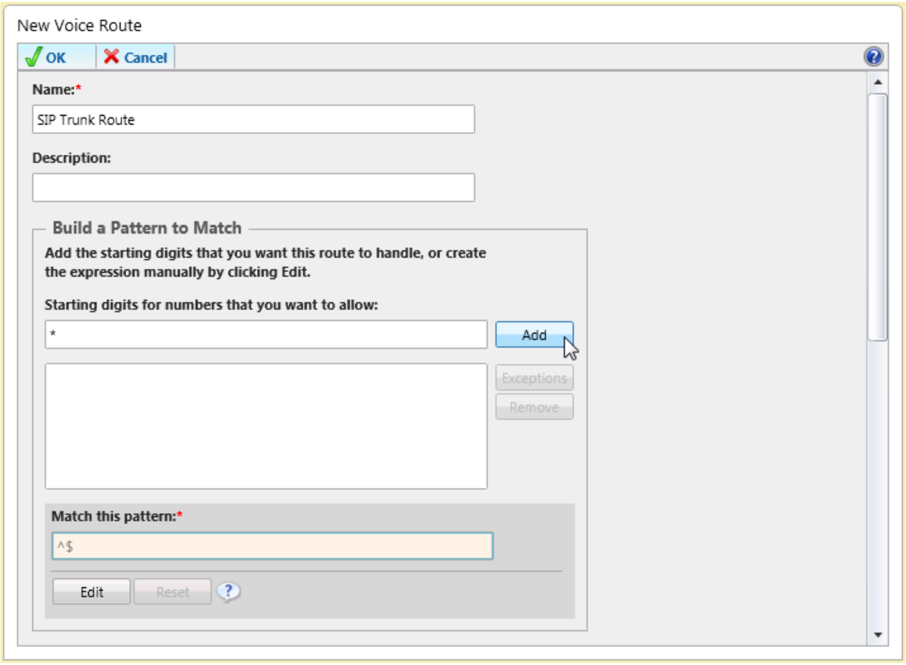
Figure 3-18: Route Tab



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

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

Figure 3-19: Adding New Voice Route



New Voice Route

Name:* SIP Trunk Route

Description:

Build a Pattern to Match

Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.

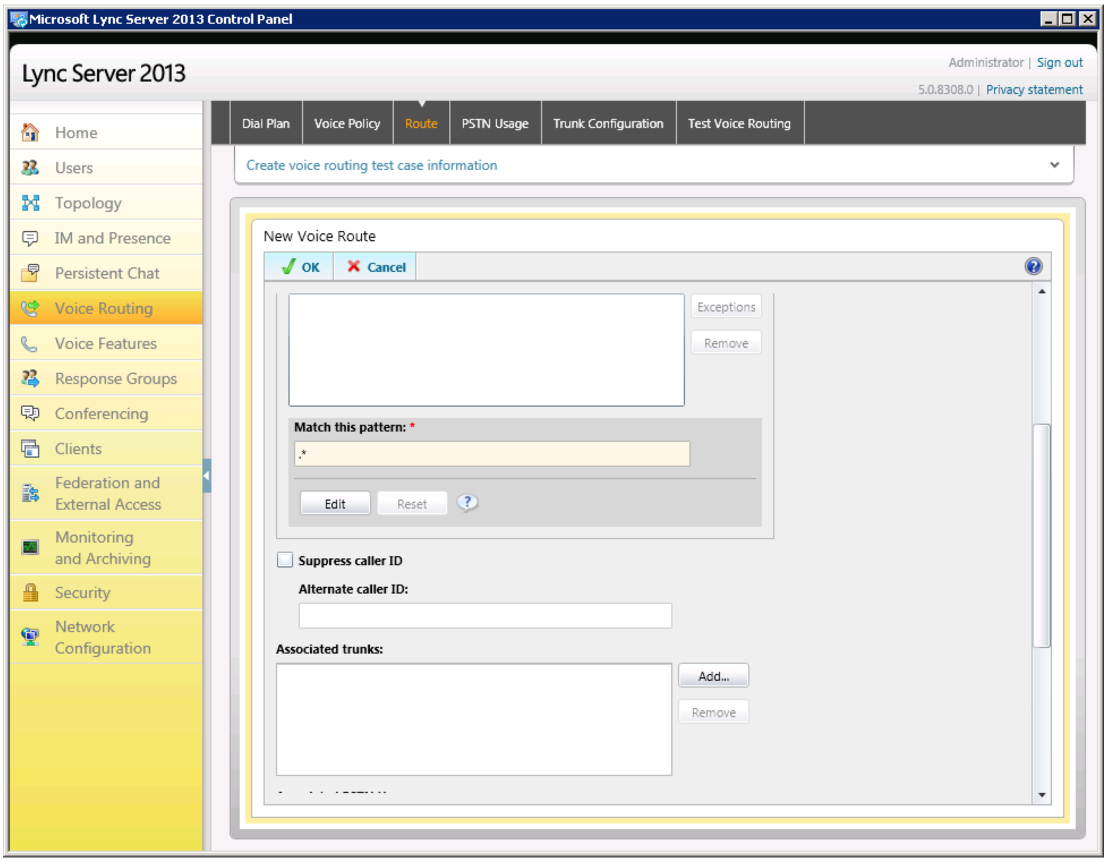
Starting digits for numbers that you want to allow: *

Match this pattern:* ^$

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



Microsoft Lync Server 2013 Control Panel

Lync Server 2013

Administrator | Sign out

5.0.8308.0 | Privacy statement

Create voice routing test case information

New Voice Route

Match this pattern: * .*

□ Suppress caller ID

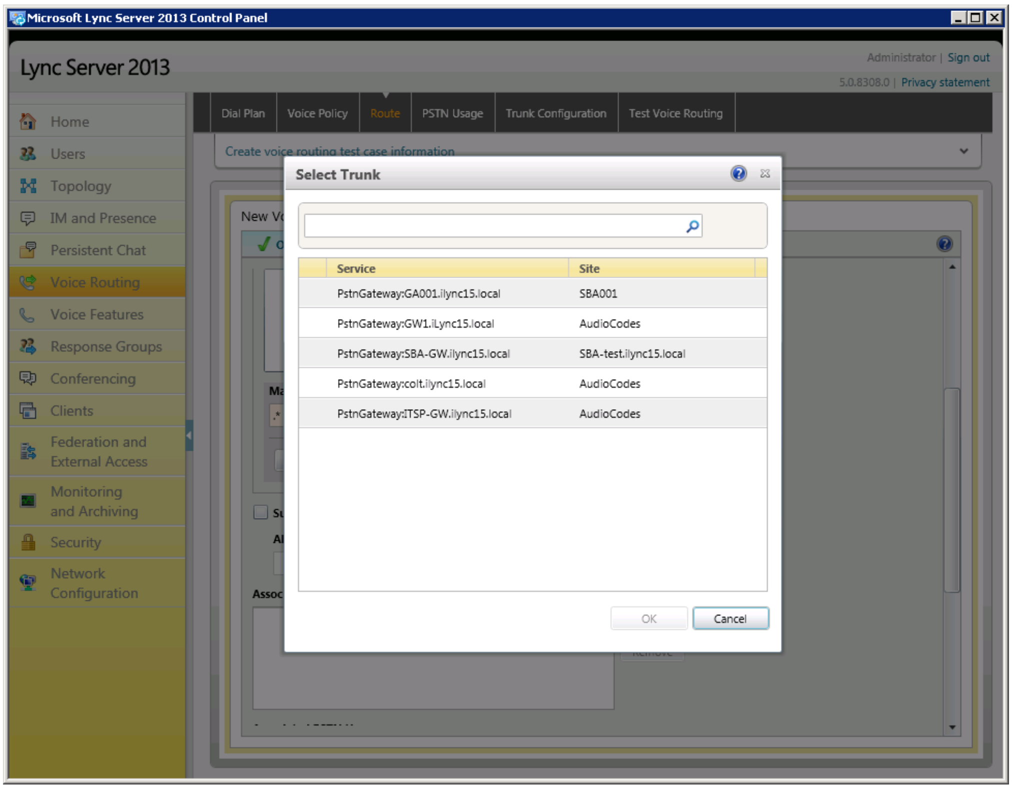
Alternate caller ID:

Associated trunks:

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:

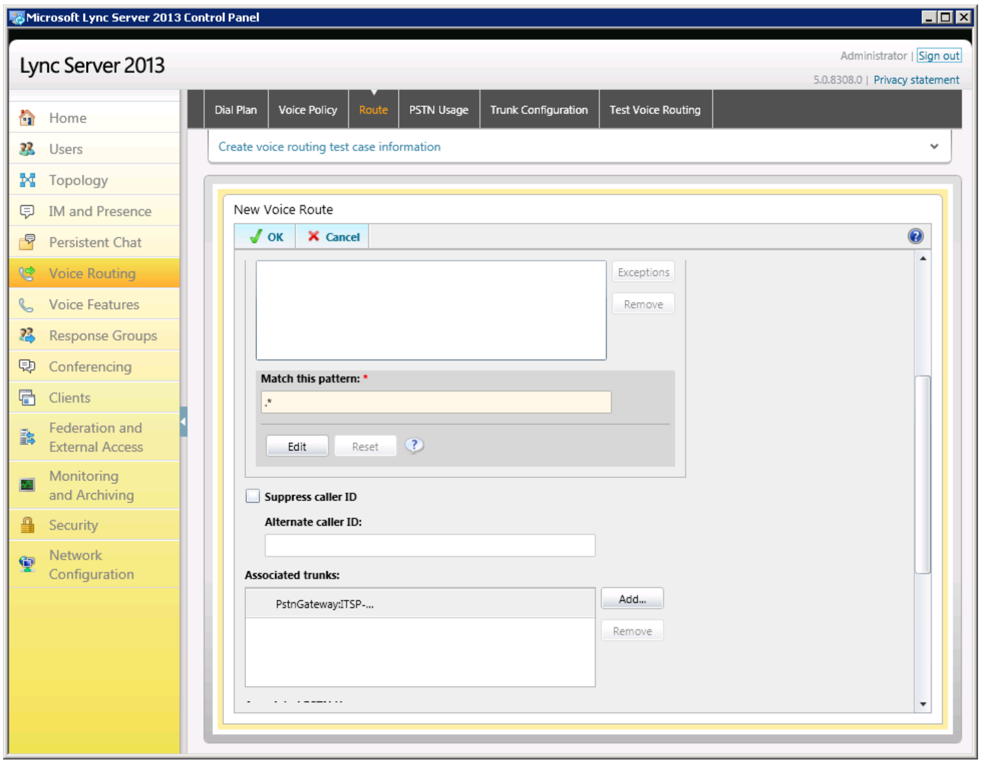
Figure 3-21: List of Deployed Trunks



Service	Site
PstnGateway:GA001.ilync15.local	SBA001
PstnGateway:GW1.iLync15.local	AudioCodes
PstnGateway:SBA-GW.ilync15.local	SBA-test.ilync15.local
PstnGateway:colt.ilync15.local	AudioCodes
PstnGateway:ITSP-GW.ilync15.local	AudioCodes

   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



Match this pattern: *
.*

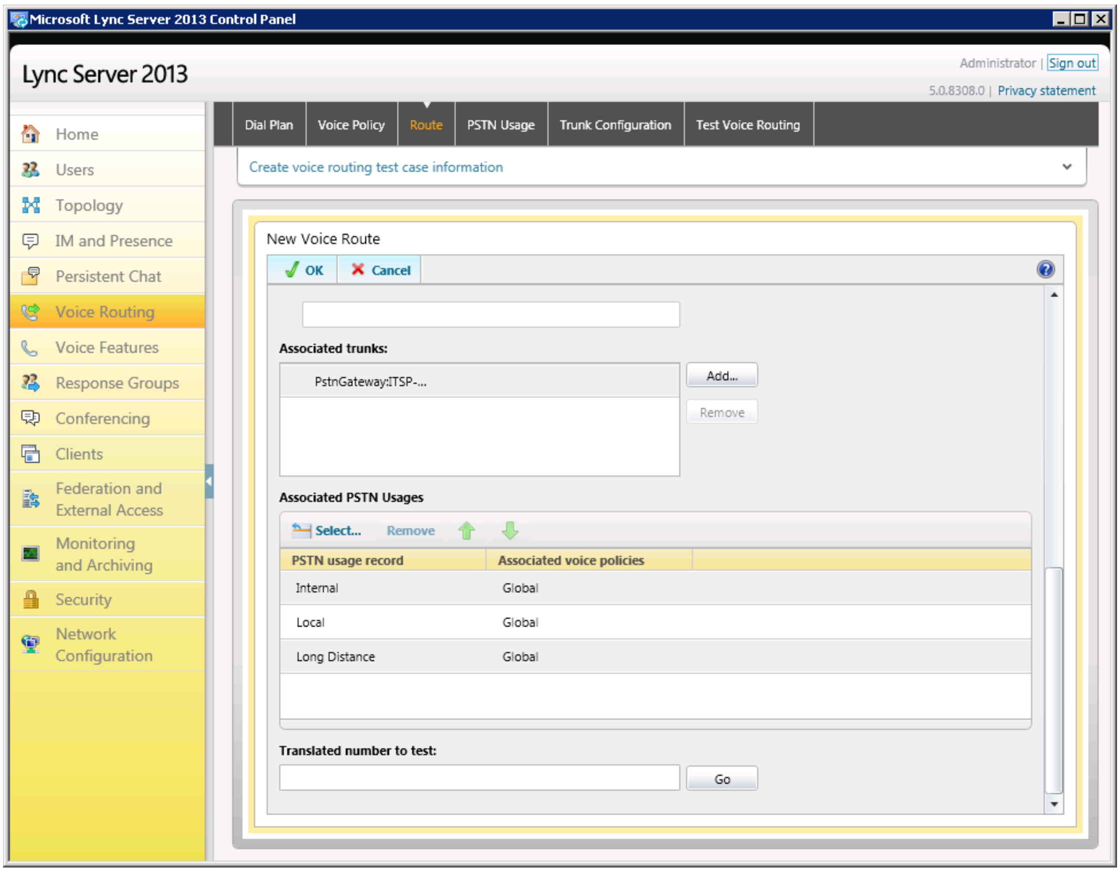
□ Suppress caller ID

Alternate caller ID:

Associated trunks:
PstnGateway:ITSP-...

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

Figure 3-23: Associating PSTN Usage to Route



Associated trunks:

PstnGateway:ITSP-...

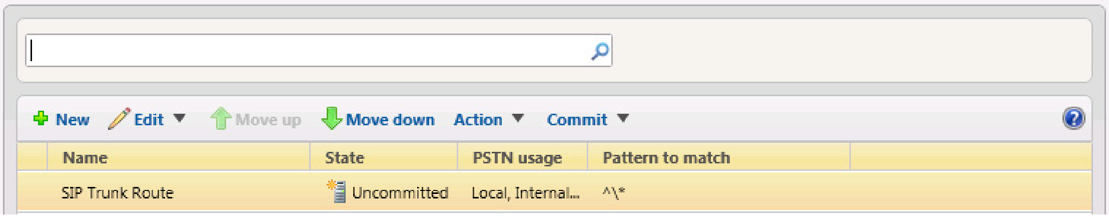
Associated PSTN Usages

PSTN usage record	Associated voice policies
Internal	Global
Local	Global
Long Distance	Global

Translated number to test:

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

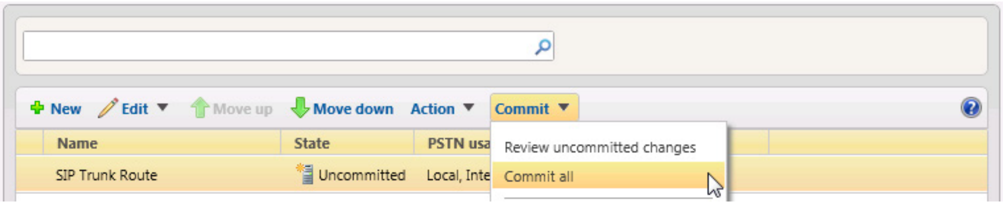
Figure 3-24: Confirmation of New Voice Route



Name	State	PSTN usage	Pattern to match
SIP Trunk Route	Uncommitted	Local, Internal...	^*

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

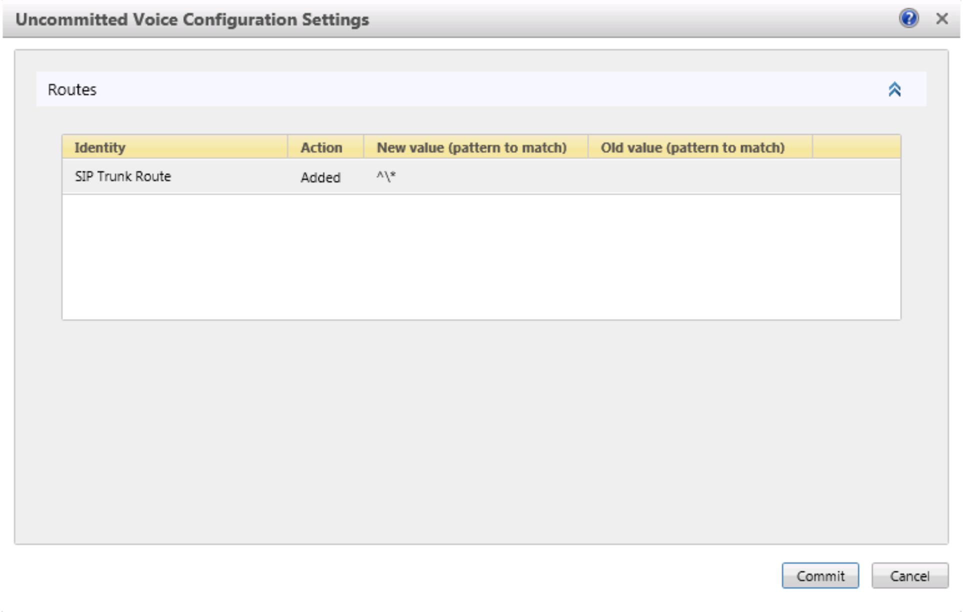
Figure 3-25: Committing Voice Routes



Name	State	PSTN usa
SIP Trunk Route	Uncommitted	Local, Inte

The Uncommitted Voice Configuration Settings page appears:

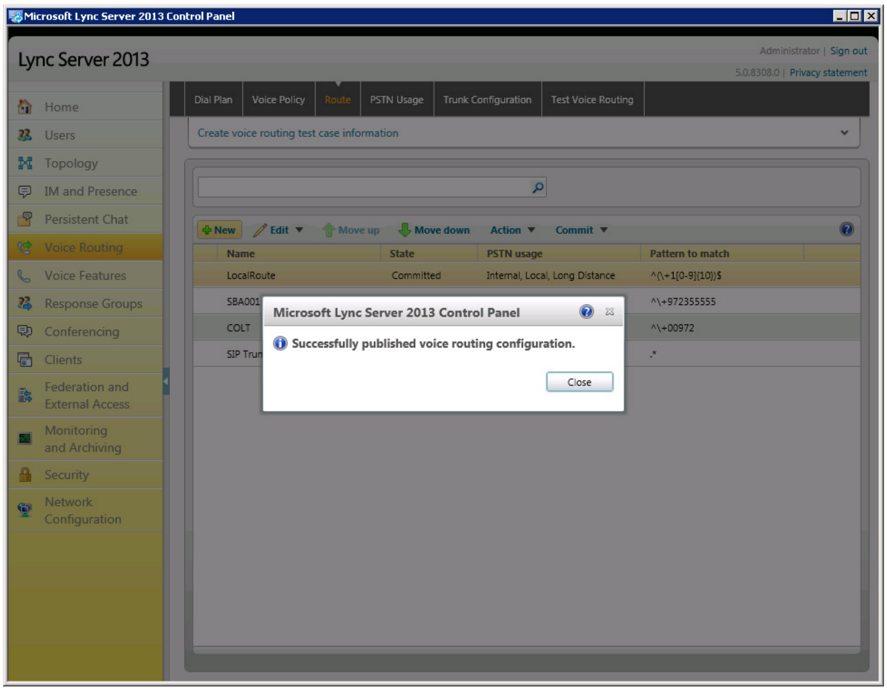
Figure 3-26: Uncommitted Voice Configuration Settings



Identity	Action	New value (pattern to match)	Old value (pattern to match)
SIP Trunk Route	Added	^*	

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

Figure 3-27: Confirmation of Successful Voice Routing Configuration



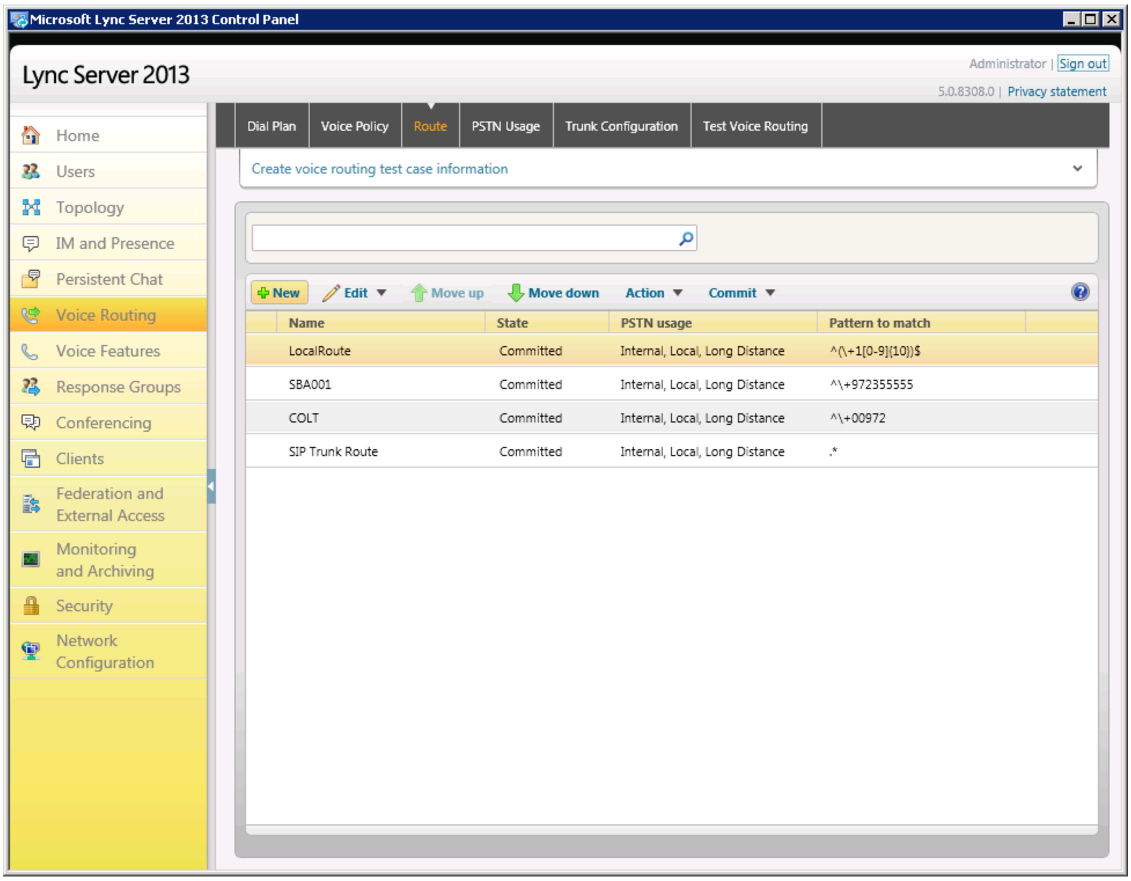
Name	State	PSTN usage	Pattern to match
LocalRoute	Committed	Internal, Local, Long Distance	^(\+1[0-9]{10})$
SBA001			^\+972355555
COLT			^\+00972
SIP Trun			.*

Microsoft Lync Server 2013 Control Panel

Successfully published 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	^(\+1[0-9]{10})$
SBA001	Committed	Internal, Local, Long Distance	^\+972355555
COLT	Committed	Internal, Local, Long Distance	^\+00972
SIP Trunk Route	Committed	Internal, Local, Long Distance	.*

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 XO Communications SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 12, and includes the following main areas:

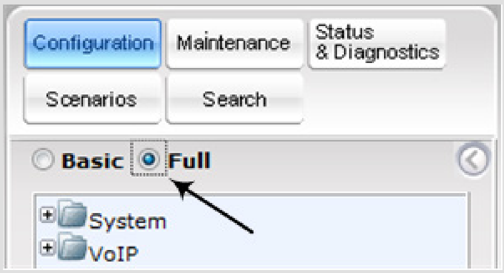
- E-SBC WAN interface - XO Communications SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

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

Notes:

- For implementing Microsoft Lync and XO Communications 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:



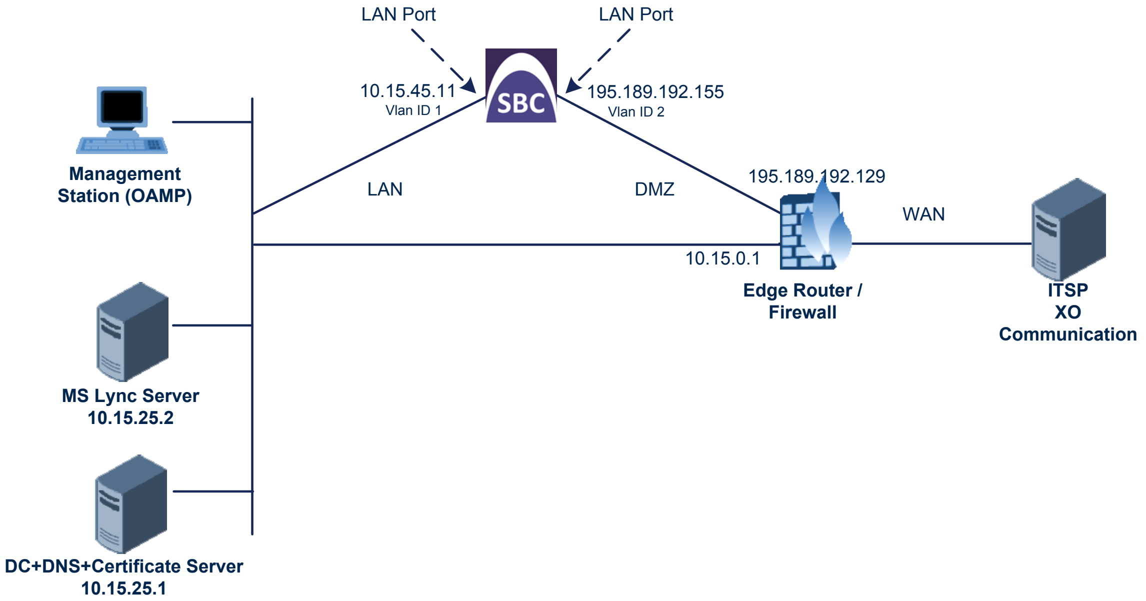
  Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

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
  - XO Communications 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 Network Interfaces

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

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

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

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

Parameter	Value
IP Address	**10.15.45.11** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.25.1**
Underlying Interface	**GROUP_1** (Ethernet port group)

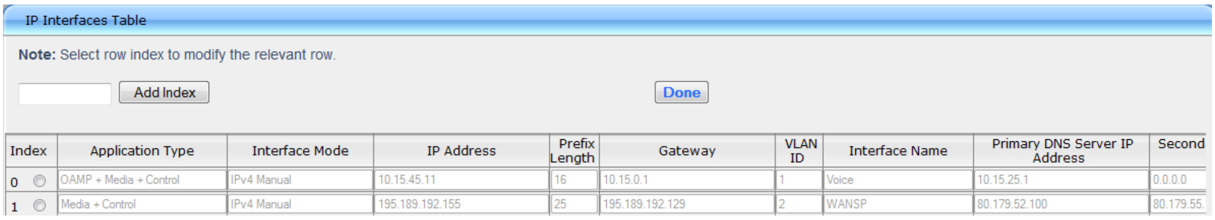
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**195.189.192.155** (WAN IP address)
Prefix Length	**16** (for 255.255.0.0)
Gateway	**195.189.192.129** (router's IP address)
VLAN ID	**2**
Interface Name	**WANSP**
Primary DNS Server IP Address	**80.179.52.100**
Secondary DNS Server IP Address	**80.179.55.100**
Underlying Interface	**GROUP_2**

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

The configured IP network interfaces are shown below:

Figure 4-2: Configured Network Interfaces in IP Interfaces Table



IP Interfaces Table

Note: Select row index to modify the relevant row.

Add Index   Done

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Second
0 ○	OAMP + Media + Control	IPv4 Manual	10.15.45.11	16	10.15.0.1	1	Voice	10.15.25.1	0.0.0.0
1 ○	Media + Control	IPv4 Manual	195.189.192.155	25	195.189.192.129	2	WANSP	80.179.52.100	80.179.55.

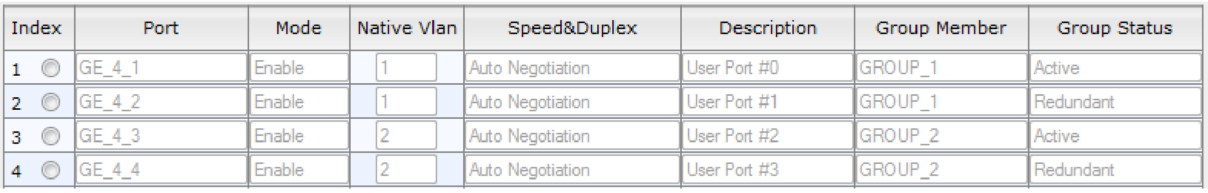
4.1.2 Step 1b: Configure the Native VLAN ID

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".
3. For the **GROUP_2** member ports, set the 'Native Vlan' field to **2**. This VLAN was assigned to network interface "WANSP".

Figure 4-3: Configured Port Native VLAN



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

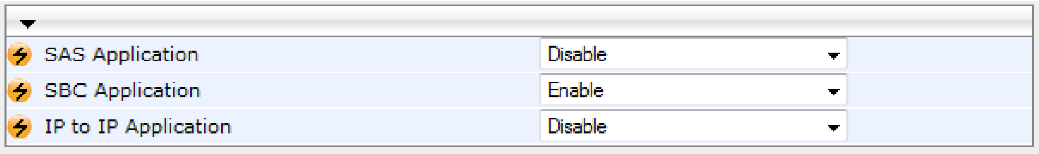
4.2 Step 2: Enable the SBC Application

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 4-4: Enabling SBC Application



SAS 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

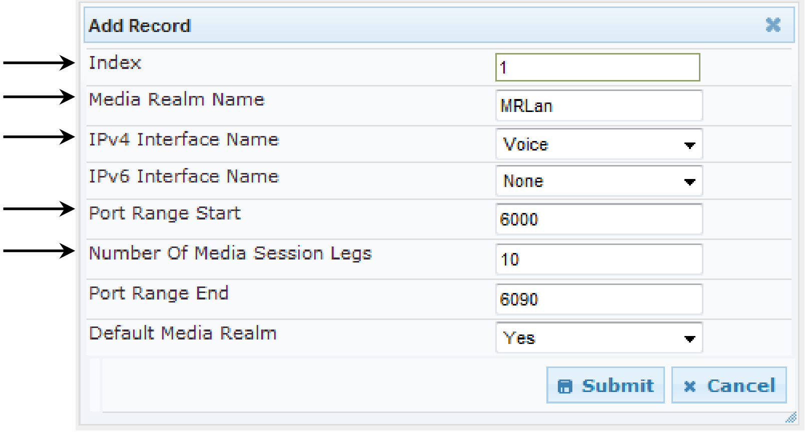
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

Parameter	Value
Index	**1**
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 4-5: Configuring Media Realm for LAN



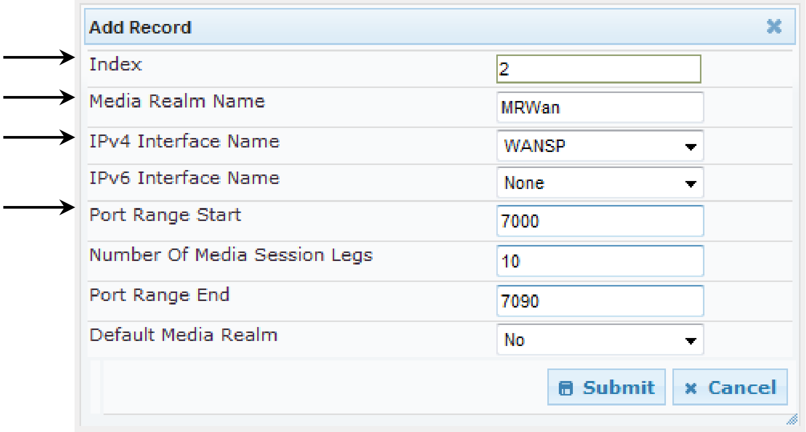
Add Record

Index	1
Media Realm Name	MRLan
IPv4 Interface Name	Voice
IPv6 Interface Name	None
Port Range Start	6000
Number Of Media Session Legs	10
Port Range End	6090
Default Media Realm	Yes

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	**2**
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 4-6: Configuring Media Realm for WAN

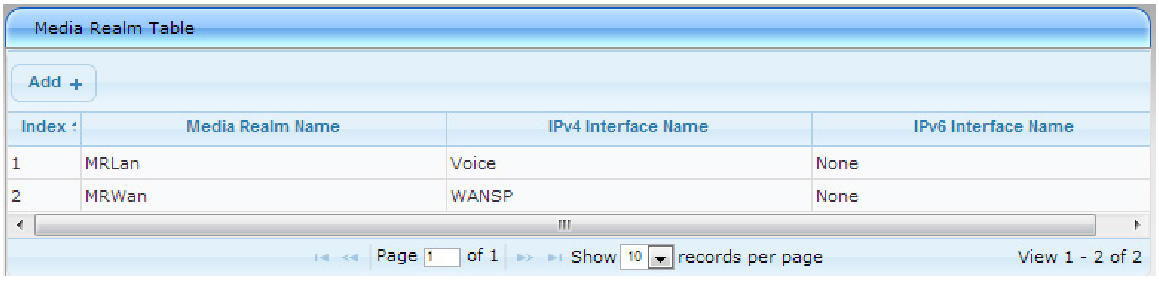


Add Record

Index	2
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	7090
Default Media Realm	No

The configured Media Realms are shown in the figure below:

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



Media Realm Table

Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
1	MRLan	Voice	None
2	MRWan	WANSP	None

Page 1 of 1 Show 10 records per page View 1 - 2 of 2

4.3.2 Step 3b: Configure SRDs

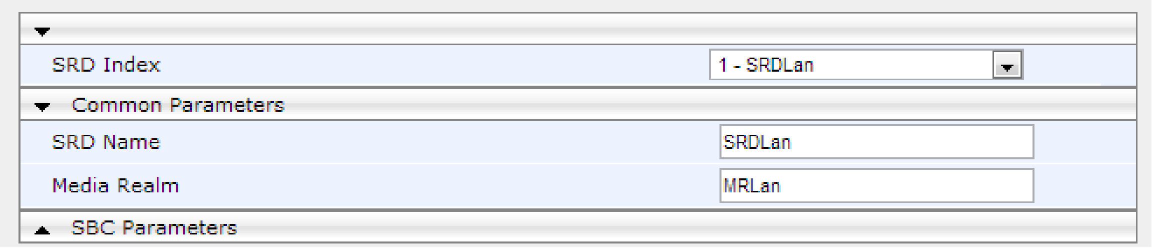
This step describes how to configure the SRDs.

➢ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **Control 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	**SRDLan** (descriptive name for SRD)
Media Realm	**MRLan** (associates SRD with Media Realm)

Figure 4-8: Configuring LAN SRD



SRD Index: 1 - SRDLan

Common Parameters

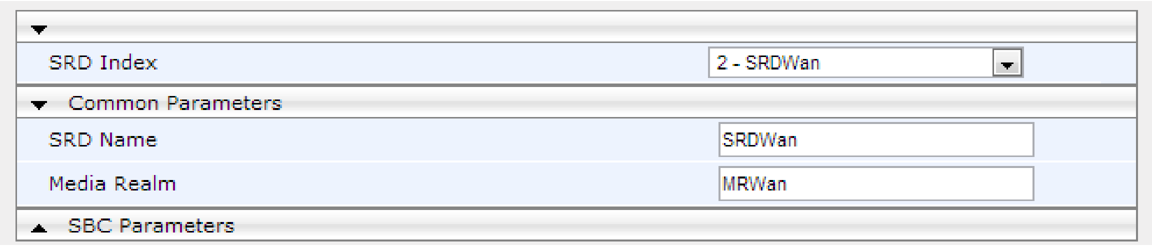
SRD Name: SRDLan

Media Realm: MRLan

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

Parameter	Value
SRD Index	**2**
SRD Name	**SRDWan**
Media Realm	**MRWan**

Figure 4-9: Configuring WAN SRD



SRD Index: 2 - SRDWan

Common Parameters

SRD Name: SRDWan

Media Realm: MRWan

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 > **Control Network** > **SIP Interface Table**).
2. Configure a SIP interface for the LAN:

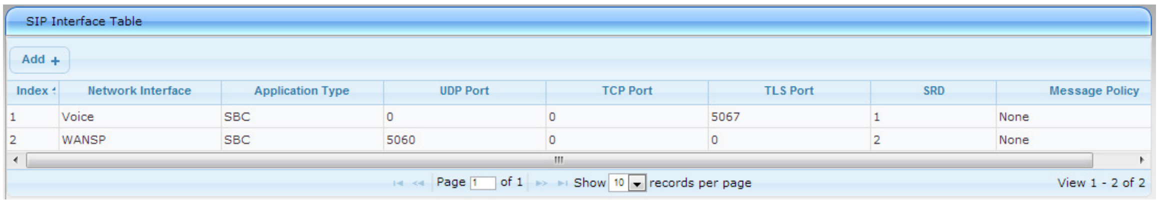
Parameter	Value
Index	**1**
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
SRD	**1**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**2**
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 4-10: Configured SIP Interfaces in SIP Interface Table



SIP Interface Table

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	Voice	SBC	0	0	5067	1	None
2	WANSP	SBC	5060	0	0	2	None

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
- XO Communications SIP Trunk

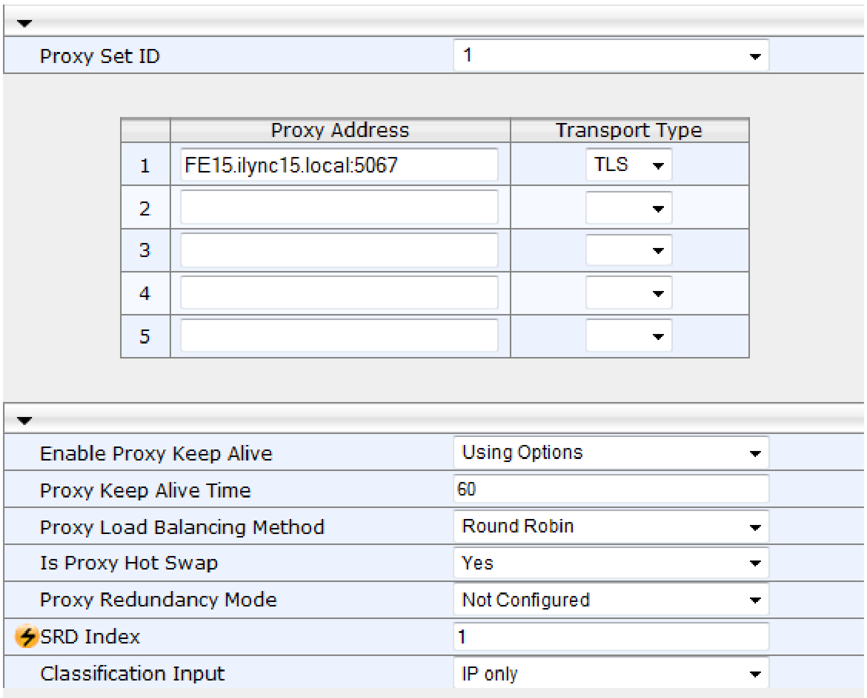
These Proxy Sets will later be associated with IP Groups.

➢ To configure Proxy Sets:

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

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

Figure 4-11: Configuring Proxy Set for Microsoft Lync Server 2013



Proxy Set ID	1

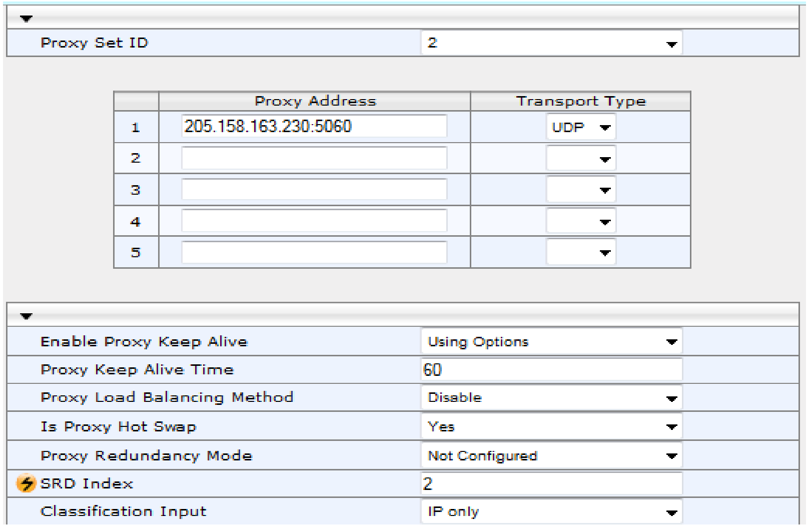
	Proxy Address	Transport Type
1	FE15.ilync15.local:5067	TLS
2		
3		
4		
5		

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 XO Communications SIP Trunk:

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**205.158.163.230:5060** (XO Communications IP address / FQDN and destination port)
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
Is Proxy Hot Swap	**Yes**
SRD Index	**2** (enables classification by Proxy Set for SRD of IP Group belonging to XO Communications SIP Trunk)

Figure 4-12: Configuring Proxy Set for XO Communications SIP Trunk



Proxy Set ID	2

	Proxy Address	Transport Type
1	205.158.163.230:5060	UDP
2		
3		
4		
5		

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
- XO Communications SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Configure an IP Group for the Lync Server 2013 Mediation Server:

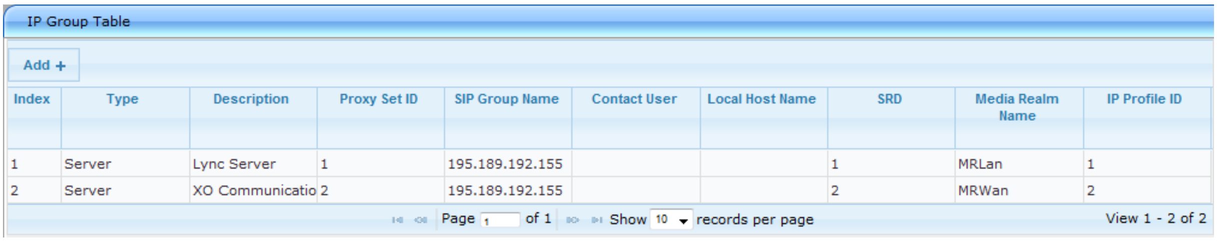
Parameter	Value
Index	**1**
Type	**Server**
Description	**Lync Server** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**195.189.192.155**
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

3. Configure an IP Group for the XO Communications SIP Trunk:

Parameter	Value
Index	**2**
Type	**Server**
Description	**XO Communications** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**195.189.192.155**
SRD	**2**
Media Realm Name	**MRWan**
IP Profile ID	**2**

The configured IP Groups are shown in the figure below:

Figure 4-13: Configured IP Groups in IP Group Table



IP Group Table

Add +

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	Local Host Name	SRD	Media Realm Name	IP Profile ID
1	Server	Lync Server	1	195.189.192.155			1	MRLan	1
2	Server	XO Communicatio	2	195.189.192.155			2	MRWan	2

Page 1 of 1 Show 10 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
- XO Communications 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 42).

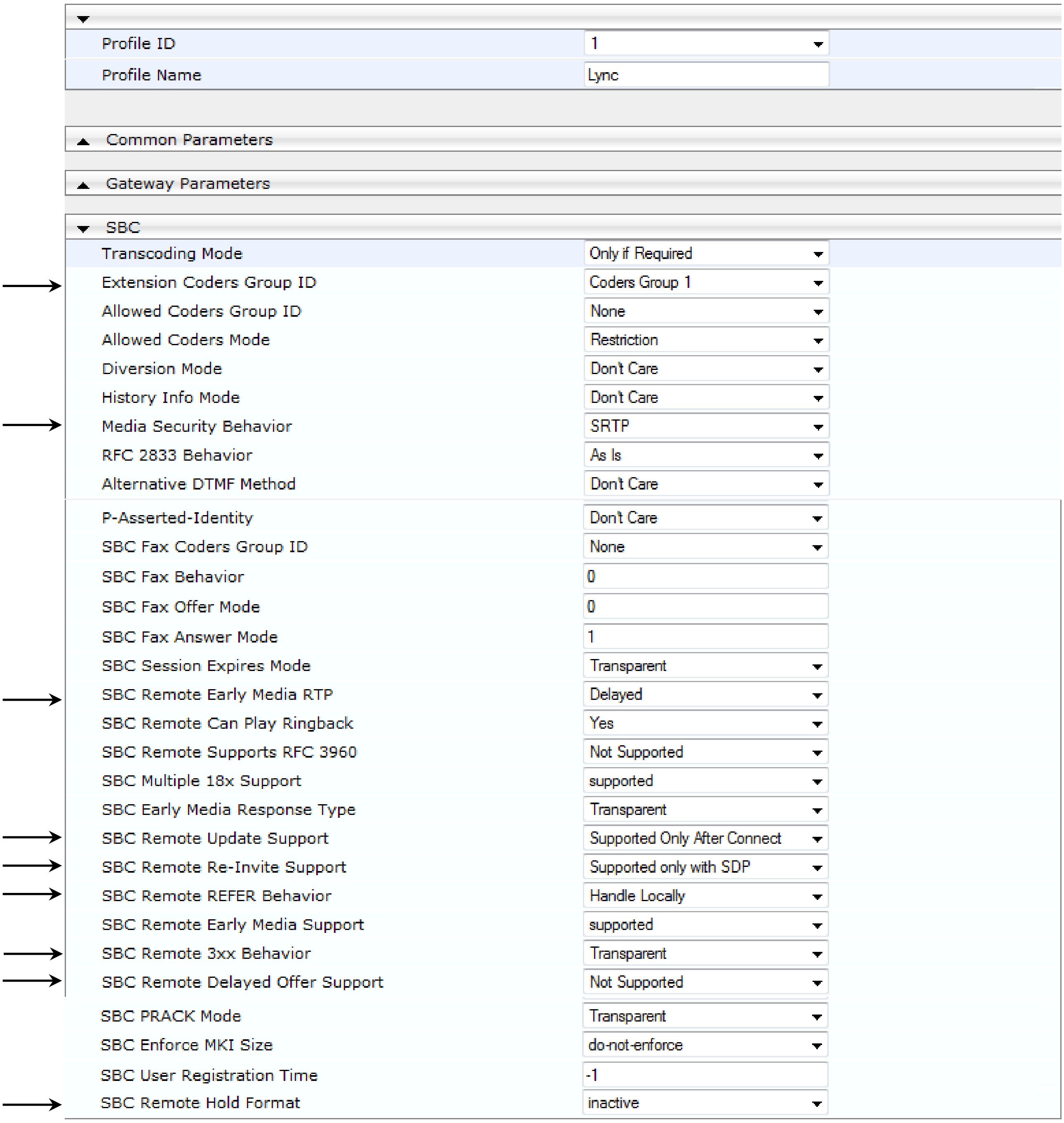
➢ To configure IP Profiles:

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Configure an IP Profile for Lync Server 2013:

Parameter	Value
Profile ID	**1**
Extension Coders Group ID	**Coders Group 1**
Media Security Behavior	**SRTP**
SBC Remote Early Media RTP	**Delayed** (required, as Lync Server 2013 does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Remote Update Support	**Supported Only After Connect**
SBC Remote Re-Invite Support	**Supported Only With SDP**
SBC Remote Refer Behavior	**Handle Locally** (required, as Lync Server 2013 does not support receipt of SIP REFER)
SBC Remote 3xx Behavior	**Handle Locally** (required, as Lync Server 2013 does not support receipt of SIP 3xx responses)
SBC Remote Delayed Offer Support	**Not Supported**

Reset SRTP State Upon Rekey	**Enable** **Note:** Currently, you cannot configure this parameter through the Web-based management tool. As an alternative, use the *ini* configuration file, as follows: 1 When you have completed **all** configuration, save the configuration to an ini file (see Appendix A on page 71). 2 Open the file and search for "IpProfile 1". 3 For this IP Profile, set the *IpProfile_ResetSRTPStateUponRekey* parameter to 1. This value is located sixth from the end of the line (i.e., semicolon): "**1**, 0, 1, 0, 3, 0;" 4 Save the file and load it to the device.
SBC Remote Hold Format	**Inactive**

Figure 4-14: Configuring IP Profile for Lync Server 2013



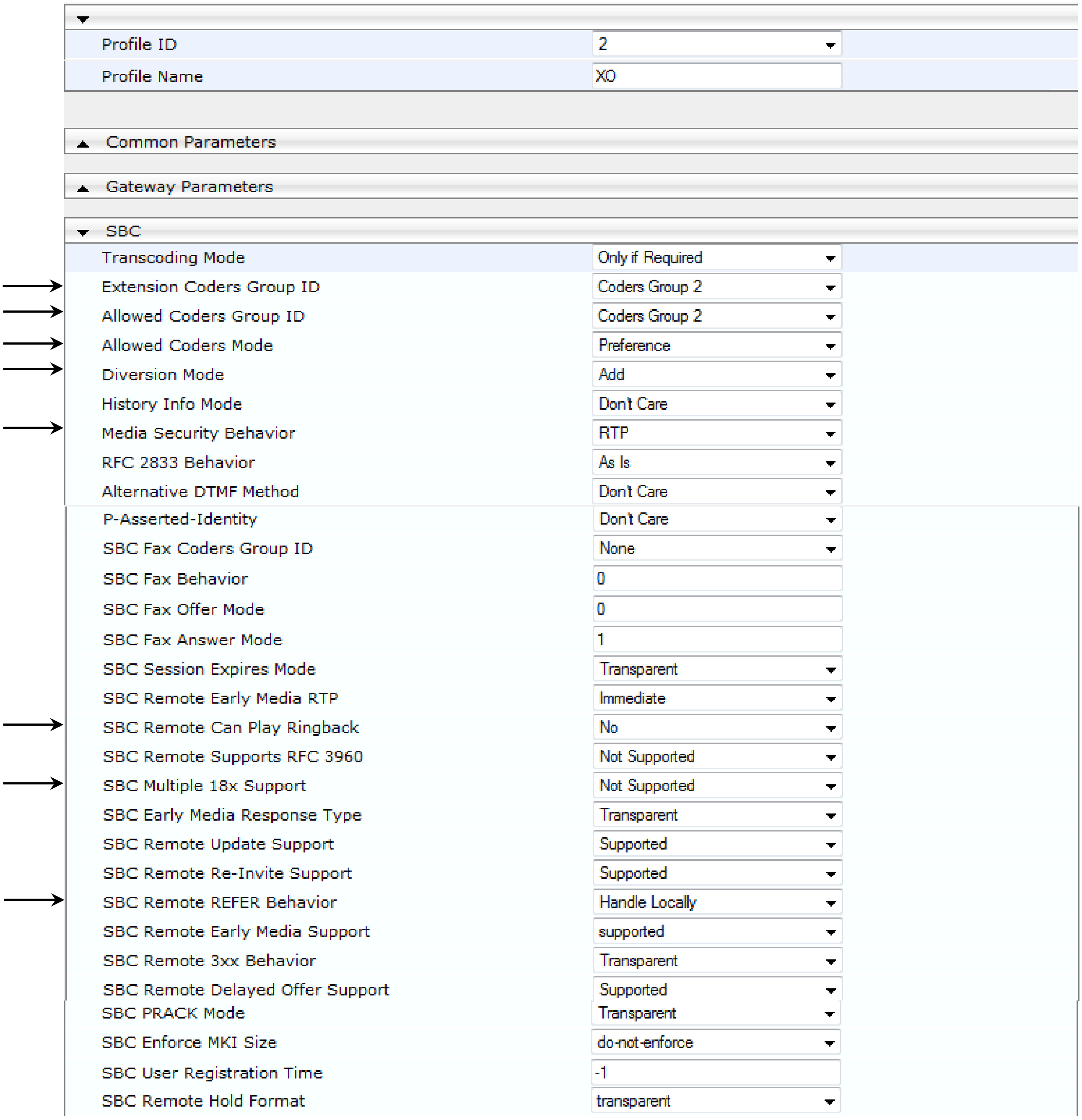
Profile ID	1
Profile Name	Lync

Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 1
Allowed Coders Group ID	None
Allowed Coders Mode	Restriction
Diversion Mode	Don't Care
History Info Mode	Don't Care
Media Security Behavior	SRTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	Don't Care
P-Asserted-Identity	Don't Care
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent
SBC Remote Early Media RTP	Delayed
SBC Remote Can Play Ringback	Yes
SBC Remote Supports RFC 3960	Not Supported
SBC Multiple 18x Support	supported
SBC Early Media Response Type	Transparent
SBC Remote Update Support	Supported Only After Connect
SBC Remote Re-Invite Support	Supported only with SDP
SBC Remote REFER Behavior	Handle Locally
SBC Remote Early Media Support	supported
SBC Remote 3xx Behavior	Transparent
SBC Remote Delayed Offer Support	Not Supported
SBC PRACK Mode	Transparent
SBC Enforce MKI Size	do-not-enforce
SBC User Registration Time	-1
SBC Remote Hold Format	inactive

3. Configure an IP Profile for the XO Communications SIP Trunk:

Parameter	Value
Profile ID	**2**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Preference** (lists Allowed Coders first and then original coders in received SDP offer)
Diversion Mode	**Add** (required for Call Forward calls)
Media Security Behavior	**RTP**
SBC Remote Can Play Ringback	**No** (required, as Lync Server 2013 does not provide a ringback tone for incoming calls)
SBC Multiple 18x Support	**Not Supported**
SBC Remote Refer Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)

Figure 4-15: Configuring IP Profile for XO Communications SIP Trunk



Profile ID	2
Profile Name	XO

▲ Common Parameters

▲ Gateway Parameters

▼ SBC

Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 2
Allowed Coders Mode	Preference
Diversion Mode	Add
History Info Mode	Don't Care
Media Security Behavior	RTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	Don't Care
P-Asserted-Identity	Don't Care
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent
SBC Remote Early Media RTP	Immediate
SBC Remote Can Play Ringback	No
SBC Remote Supports RFC 3960	Not Supported
SBC Multiple 18x Support	Not Supported
SBC Early Media Response Type	Transparent
SBC Remote Update Support	Supported
SBC Remote Re-Invite Support	Supported
SBC Remote REFER Behavior	Handle Locally
SBC Remote Early Media Support	supported
SBC Remote 3xx Behavior	Transparent
SBC Remote Delayed Offer Support	Supported
SBC PRACK Mode	Transparent
SBC Enforce MKI Size	do-not-enforce
SBC User Registration Time	-1
SBC Remote Hold Format	transparent

4.7 Step 7: 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 XO Communications 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 XO Communications SIP Trunk.

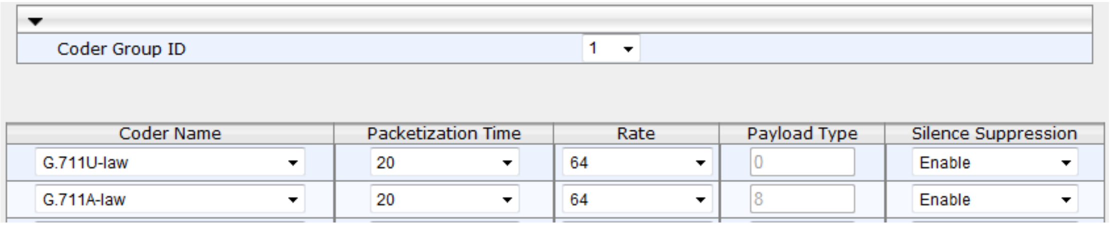
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 44).

➢ **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 4-16: Configuring Coder Group for Lync Server 2013



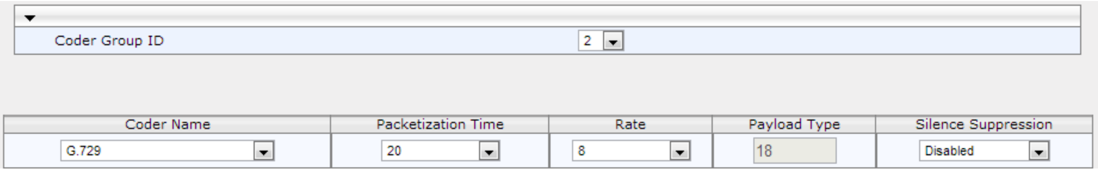
Coder Group ID 1

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

3. Configure a Coder Group for XO Communications SIP Trunk:

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

Figure 4-17: Configuring Coder Group for XO Communications SIP Trunk



Coder Group ID 2

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.729	20	8	18	Disabled

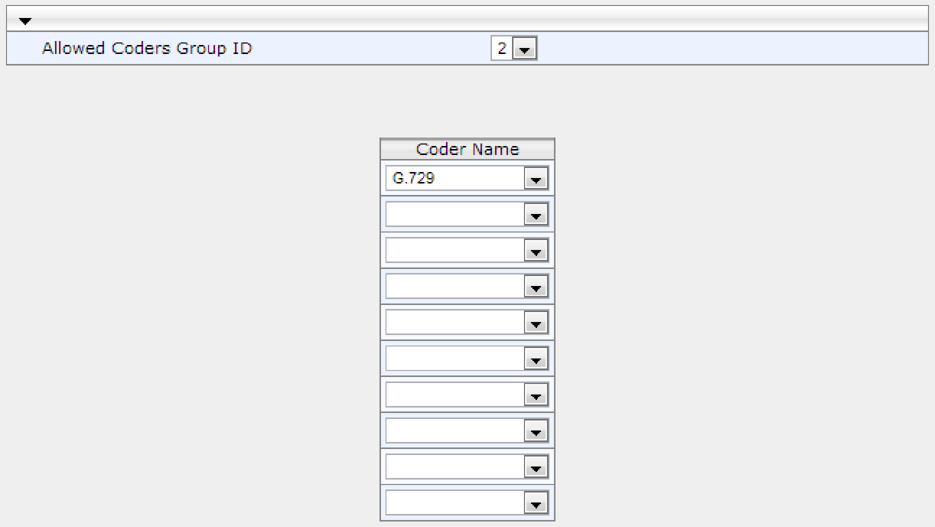
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the XO Communications SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the XO Communications SIP Trunk in the previous step (see Section 4.6 on page 44).

➢ To set a preferred coder for the XO Communications 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	**2**
Coder Name	**G.729**

Figure 4-18: Configuring Allowed Coders Group for XO Communications SIP Trunk

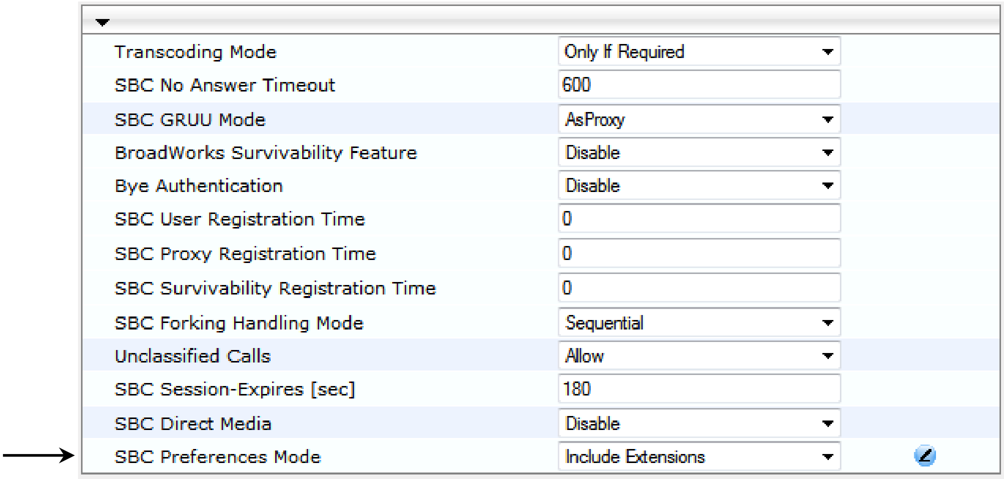


Allowed Coders Group ID: 2

Coder Name: G.729

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

Figure 4-19: SBC Preferences Mode



Transcoding Mode	Only If Required
SBC No Answer Timeout	600
SBC GRUU Mode	AsProxy
BroadWorks Survivability Feature	Disable
Bye Authentication	Disable
SBC User Registration Time	0
SBC Proxy Registration Time	0
SBC Survivability Registration Time	0
SBC Forking Handling Mode	Sequential
Unclassified Calls	Allow
SBC Session-Expires [sec]	180
SBC Direct Media	Disable
SBC Preferences Mode	Include Extensions

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

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.

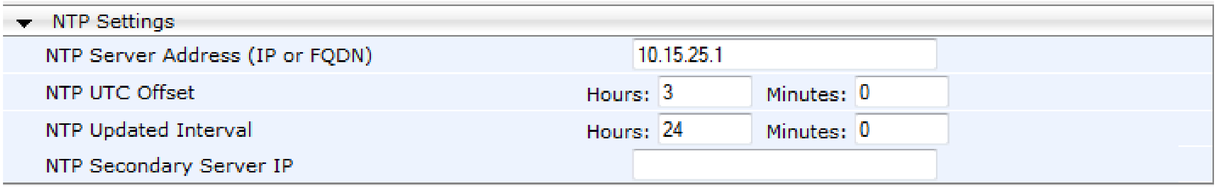
4.8.1 Step 8a: Configure the NTP Server Address

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: 3	Minutes: 0
NTP Updated Interval	Hours: 24	Minutes: 0
NTP Secondary Server IP		

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.

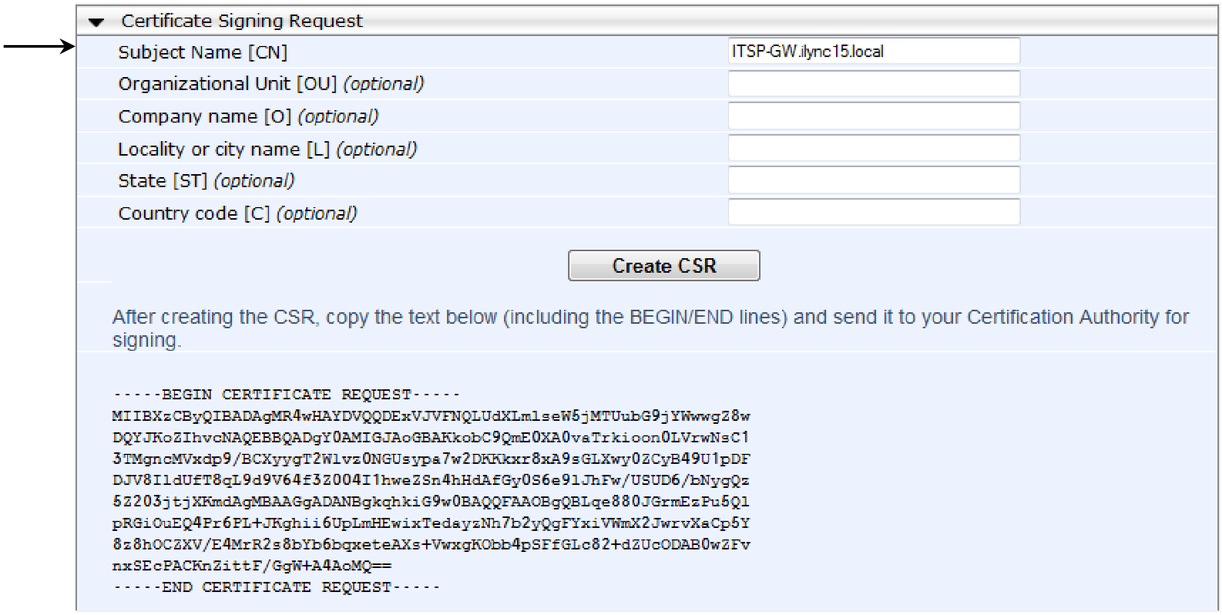
c. Obtaining Trusted Root Certificate from CA.

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)*	

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-----
MIIBXzCByQIBADAgMR4wHAYDVQQDExVJVFNQLUdXLmlseW5jMTUubG9jYWwwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgncMVxdp9/BCXyygT2Wlvz0NGUsypa7w2DKKkxr8xA9sGLXwy0ZCyB49U1pDF
DJV8IldUfT8qL9d9V64f3Z004I1hweZSn4hHdAfGy0S6e9lJhFw/USUD6/bNygQz
5Z203jtjXKmdAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQBLqe880JGrmEzPu5Ql
pRGiOuEQ4Pr6PL+JKghii6UpLmHEwixTedayzNh7b2yQgFYxiVWmX2JwrvXaCp5Y
8z8hOCZXV/E4MrR2s8bYb6bqxeteAXs+VwxgKObb4pSFfGLc82+dZUcODAB0wZFv
nxSEcPACKnZittF/GgW+A4AoMQ==
-----END CERTIFICATE REQUEST-----
```

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

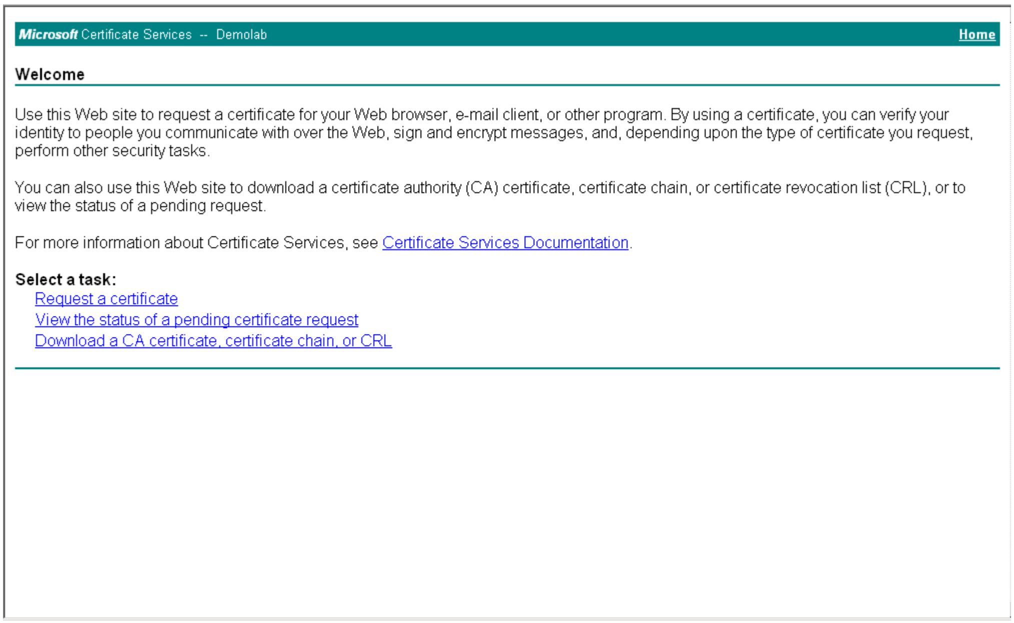
> **Note:** The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 15.

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



Microsoft Certificate Services -- Demolab **Home**

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.

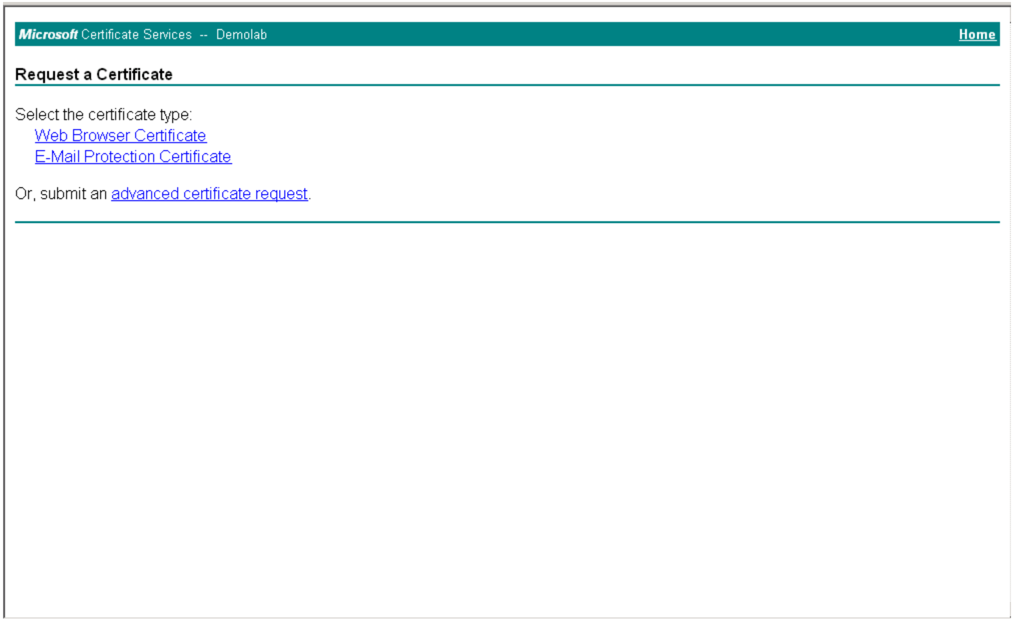
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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



Microsoft Certificate Services -- Demolab **Home**

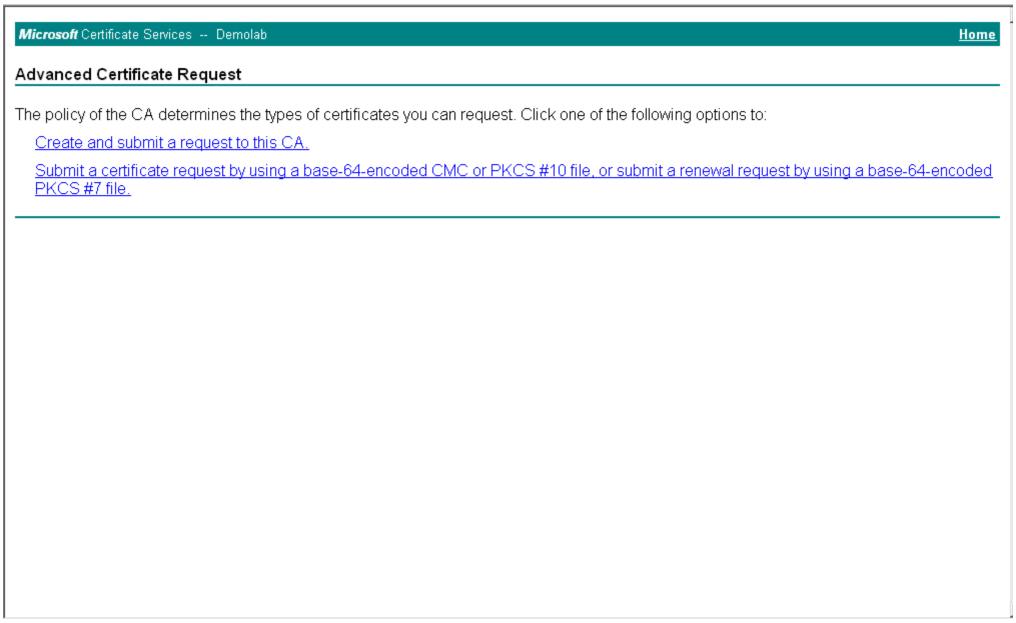
Request a Certificate

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



Advanced Certificate Request

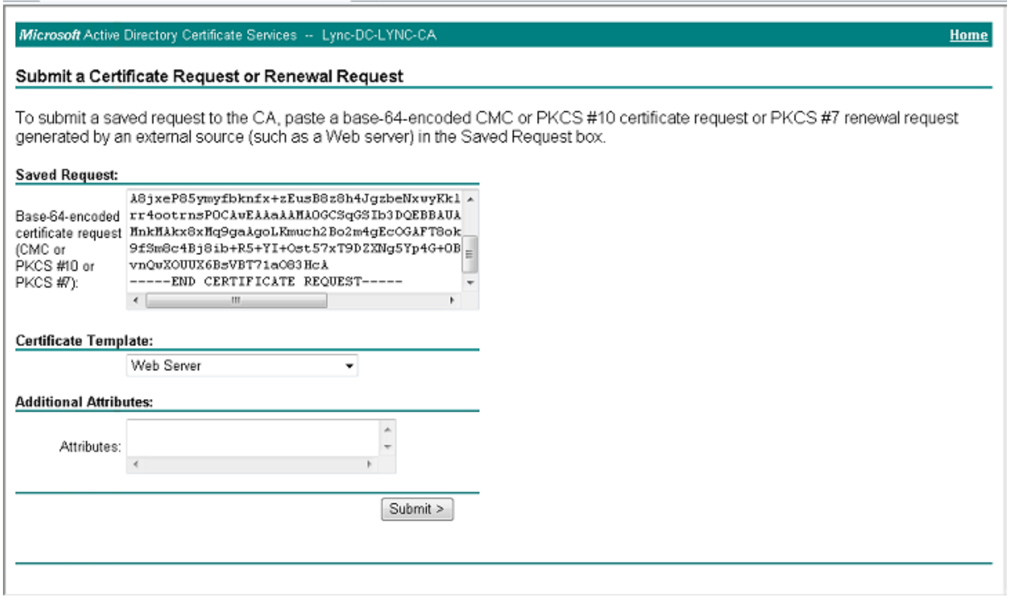
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

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

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



Microsoft Active Directory Certificate Services -- Lync-DC-LYNC-CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
A8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxuyKkl
rr4ootrnsPOCAuEAAaAAMAOGCSqGSIb3DQEBBAUA
MnkMAkx8xMq9gaAgoLKmuch2Bo2m4gEcOGAFT8ok
9fSm8c4Bj8ib+R5+YI+Ost57xT9DZXNg5Yp4G+OB
vnQuXOUUX6BsVBT71aO83HcA
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

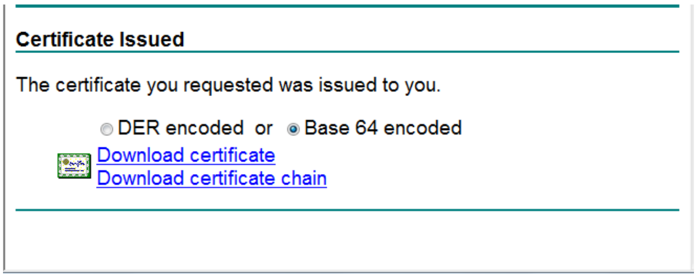
Web Server

Additional Attributes:

Attributes:

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



Certificate Issued

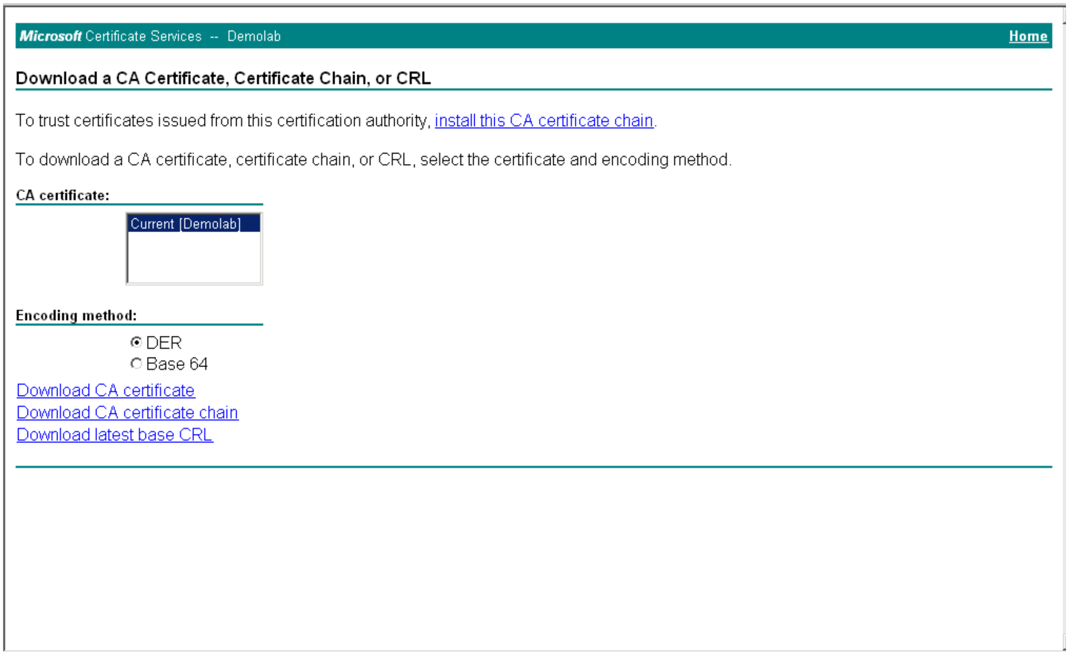
The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

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



Microsoft Certificate Services -- Demolab

Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Demolab]

Encoding method:

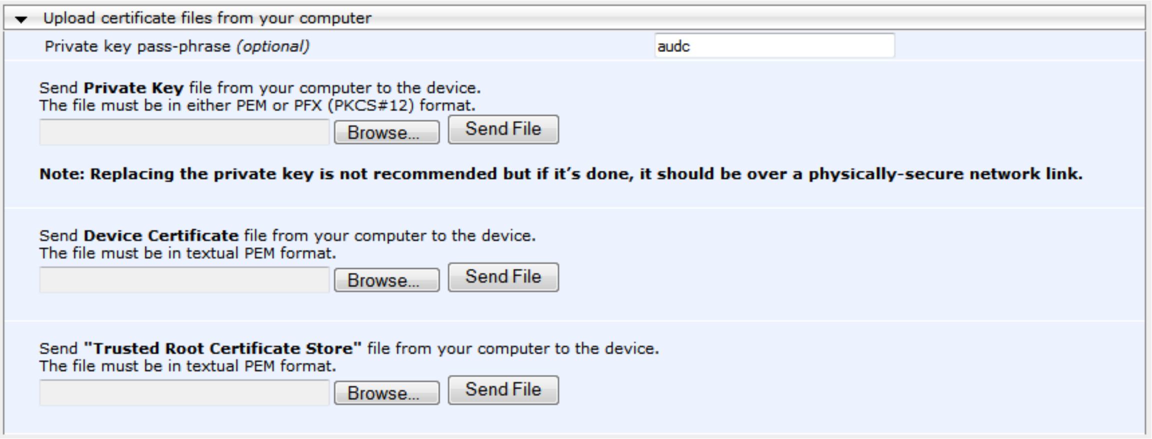
● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL

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:
    a. 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.
    b. 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)



Upload certificate files from your computer

Private key pass-phrase *(optional)*: audc

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

Send **"Trusted Root Certificate Store"** file from your computer to the device.
The file must be in textual PEM format.

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

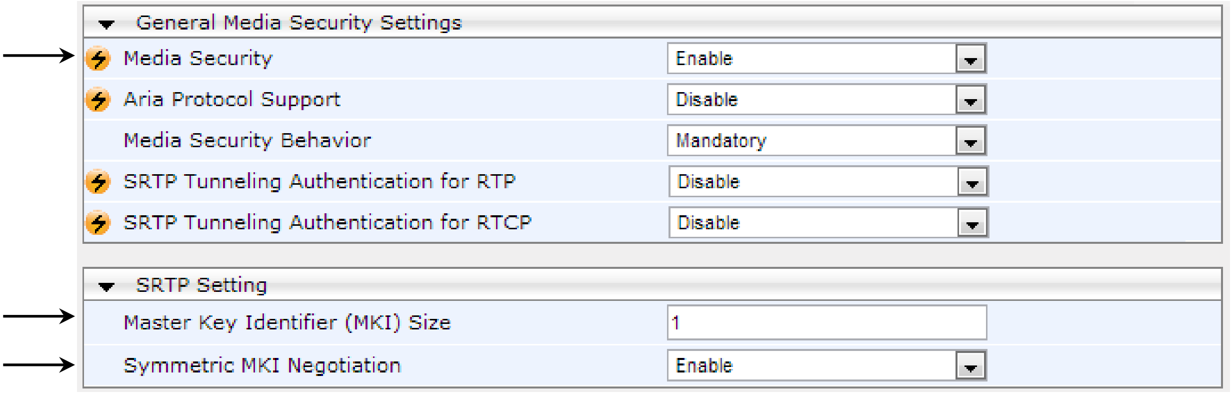
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 44).

➢ **To configure media security:**

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

Parameter	Value
Media Security	**Enable**
Master Key Identifier (MKI) Size	**1**
Symmetric MKI Negotiation	**Enable**

Figure 4-29: Configuring SRTP



General Media Security Settings

Media Security	Enable
Aria Protocol Support	Disable
Media Security Behavior	Mandatory
SRTP Tunneling Authentication for RTP	Disable
SRTP Tunneling Authentication for RTCP	Disable

SRTP Setting

Master Key Identifier (MKI) Size	1
Symmetric MKI Negotiation	Enable

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).

4.10 Step 10: Configure Maximum IP Media Channels

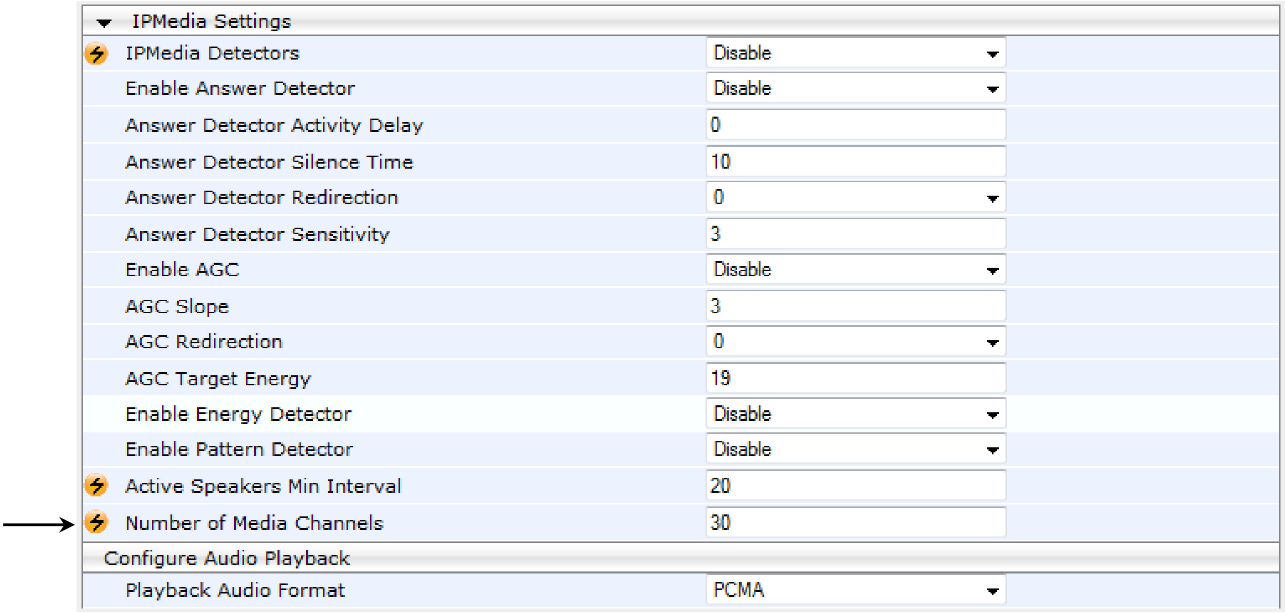
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

> **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



IPMedia Settings

IPMedia Detectors	Disable
Enable Answer Detector	Disable
Answer Detector Activity Delay	0
Answer Detector Silence Time	10
Answer Detector Redirection	0
Answer Detector Sensitivity	3
Enable AGC	Disable
AGC Slope	3
AGC Redirection	0
AGC Target Energy	19
Enable Energy Detector	Disable
Enable Pattern Detector	Disable
Active Speakers Min Interval	20
Number of Media Channels	30

Configure Audio Playback

Playback Audio Format	PCMA

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 42, IP Group 1 represents Lync Server 2013, and IP Group 2 represents XO Communications 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 XO Communications SIP Trunk (WAN):

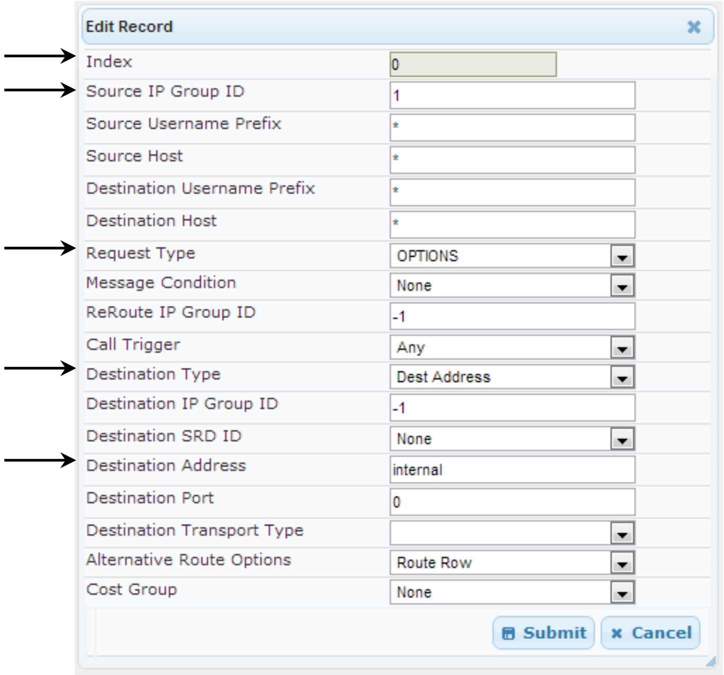
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to XO Communications SIP Trunk
- Calls from XO Communications SIP Trunk to Lync Server 2013

➢ 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:

Parameter	Value
Index	**0**
Source IP Group ID	**1**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

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



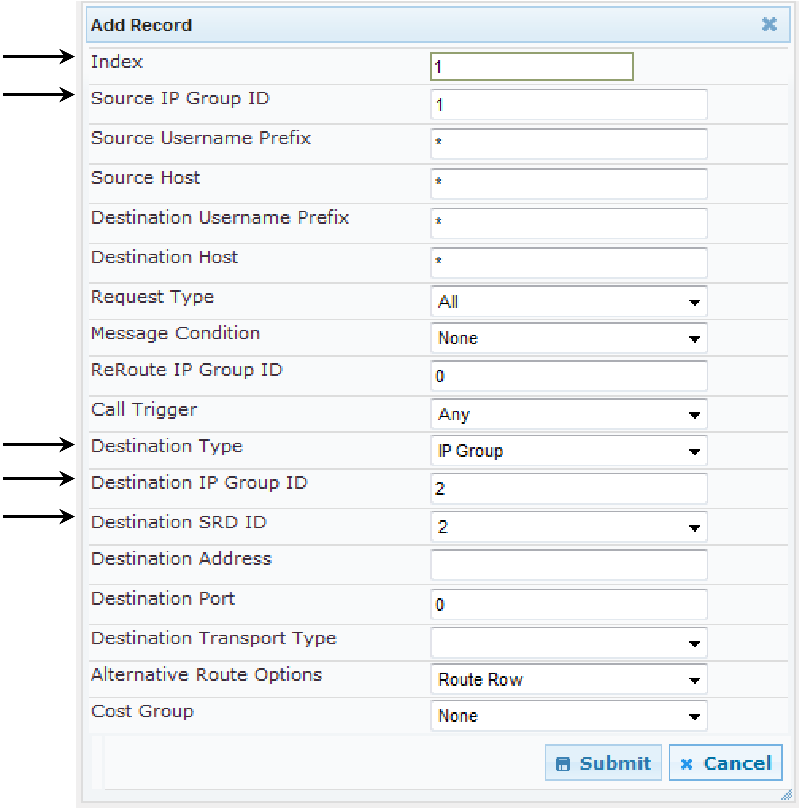
Edit Record

Index	0
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
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
Cost Group	None

3. Configure a rule to route calls from Lync Server 2013 to XO Communications SIP Trunk:

Parameter	Value
Index	**1**
Source IP Group ID	**1**
Destination Type	**IP Group**
Destination IP Group ID	**2**
Destination SRD ID	**2**

Figure 4-32: Configuring IP-to-IP Routing Rule for LAN to WAN



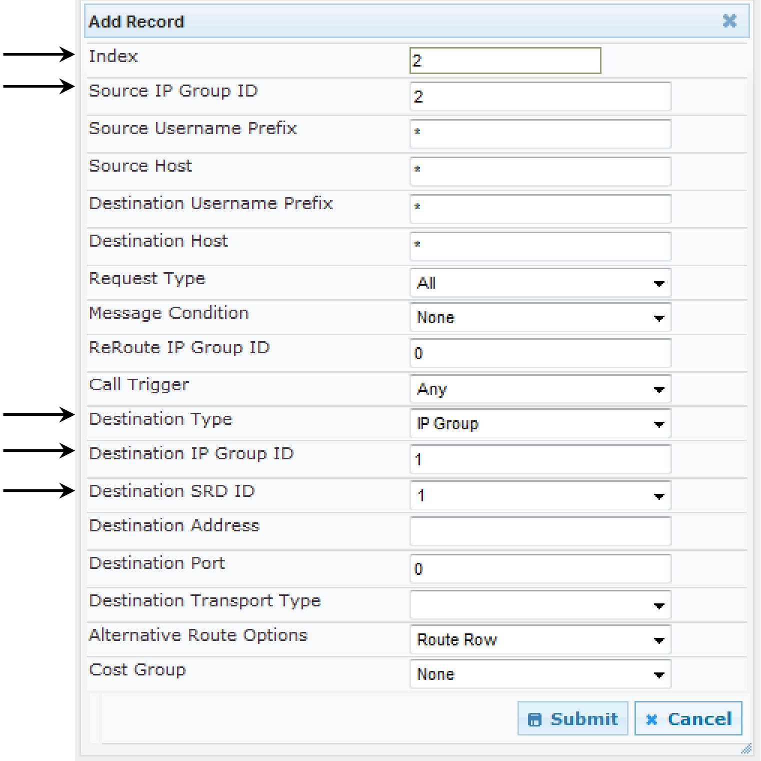
Add Record

Index	1
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	0
Call Trigger	Any
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
Cost Group	None

4. Configure a rule to route calls from XO Communications SIP Trunk to Lync Server 2013:

Parameter	Value
Index	**2**
Source IP Group ID	**2**
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 4-33: Configuring IP-to-IP Routing Rule for WAN to LAN

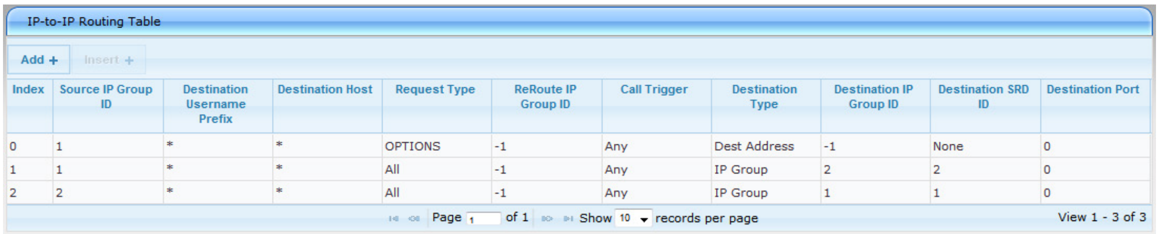


Add Record

Index	2
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	0
Call Trigger	Any
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
Cost Group	None

The configured routing rules are shown in the figure below:

Figure 4-34: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



IP-to-IP Routing Table

Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	ReRoute IP Group ID	Call Trigger	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Port
0	1	*	*	OPTIONS	-1	Any	Dest Address	-1	None	0
1	1	*	*	All	-1	Any	IP Group	2	2	0
2	2	*	*	All	-1	Any	IP Group	1	1	0

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 42, IP Group 1 represents Lync Server 2013, and IP Group 2 represents XO Communications SIP Trunk.

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

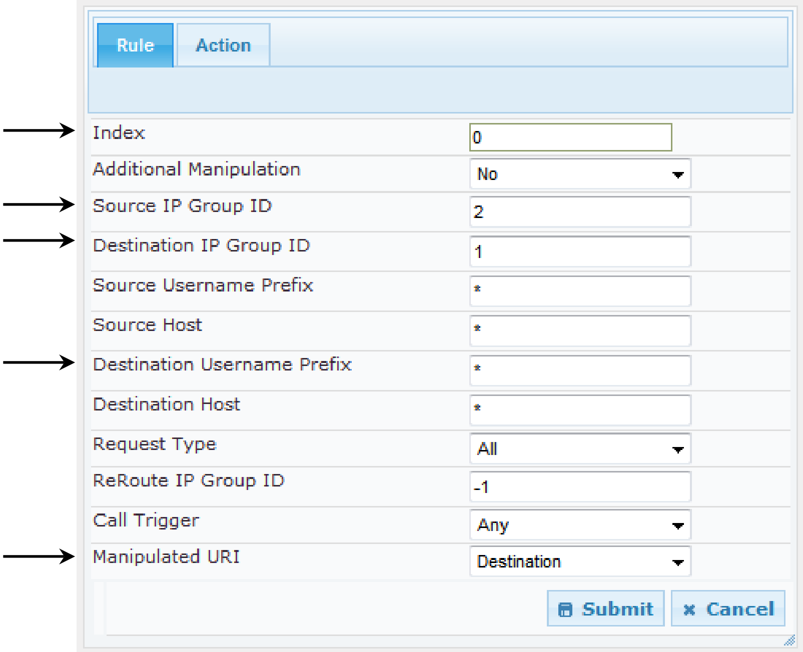
For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from IP Group 2 (XO Communications SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

➢ **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	**0**
Source IP Group	**2**
Destination IP Group	**1**
Destination Username Prefix	* (asterisk sign)
Manipulated URI	**Destination**

Figure 4-35: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

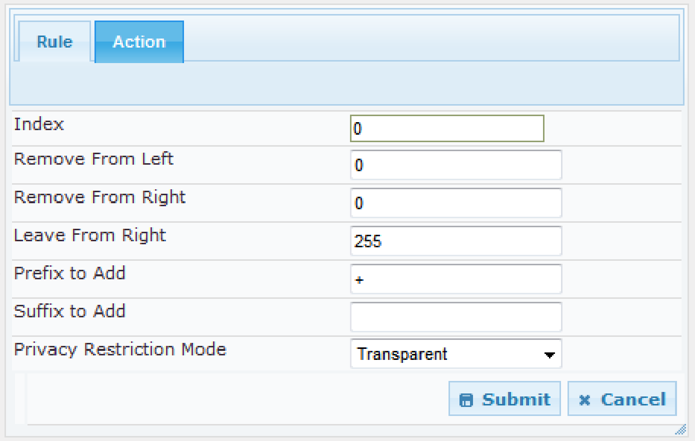


Index	0
Additional Manipulation	No
Source IP Group ID	2
Destination IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
ReRoute IP Group ID	-1
Call Trigger	Any
Manipulated URI	Destination

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

Parameter	Value
Prefix to Add	**+** (plus sign)

Figure 4-36: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

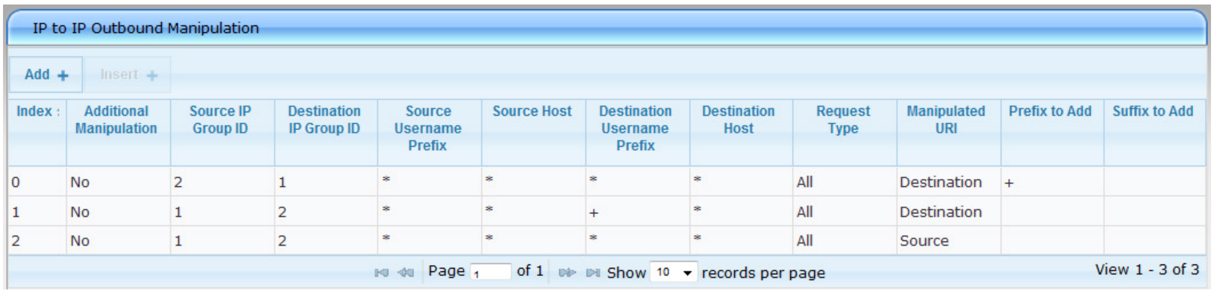


Index	0
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	
Privacy Restriction Mode	Transparent

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., XO Communications SIP Trunk):

Figure 4-37: Example of Configured IP-to-IP Outbound Manipulation Rules



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

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

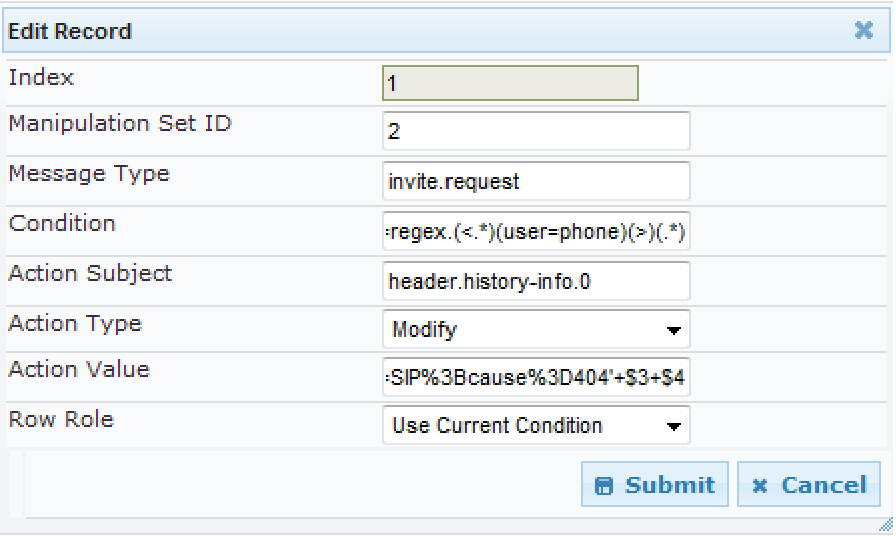
This step describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

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 2) for Lync Server 2013. This rule applies to messages sent to the XO Communications SIP Trunk (IP Group 2), for simultaneous ringing initiated by the Lync Server 2013 (IP Group 1). This adds an Action Value containing the Reason for the History-Info header, causing the E-SBC to add a diversion header towards the SIP Trunk.

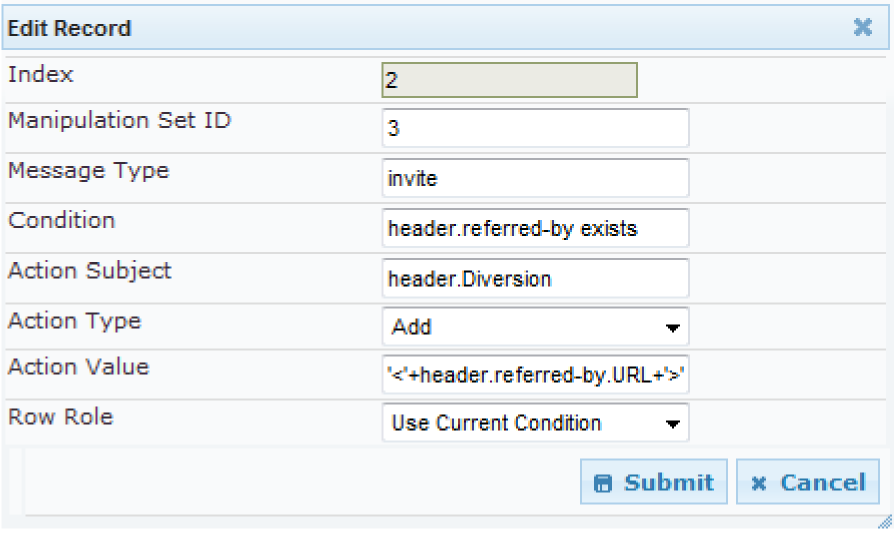
Parameter	Value
Index	**1**
Manipulation Set ID	**2**
Message Type	**invite.request**
Condition	**header.history-info.0==regex.(<.*)(user=phone)(>)(.*)**
Action Subject	**header.history-info.0**
Action Type	**Modify**
Action Value	**$1+$2+'?Reason=SIP%3Bcause%3D404'+$3+$4**



Index	1
Manipulation Set ID	2
Message Type	invite.request
Condition	:regex.(<.*)(user=phone)(>)(.*)
Action Subject	header.history-info.0
Action Type	Modify
Action Value	:SIP%3Bcause%3D404'+$3+$4
Row Role	Use Current Condition

3. Configure a new manipulation rule (Manipulation Set 3) for XO Communications SIP Trunk. This rule is applied to messages sent to the XO Communications SIP Trunk (IP Group 2) for Call Transfer initiated by the Lync Server 2013 (IP Group 1). This replaces the Referred-by header with the Diversion header.

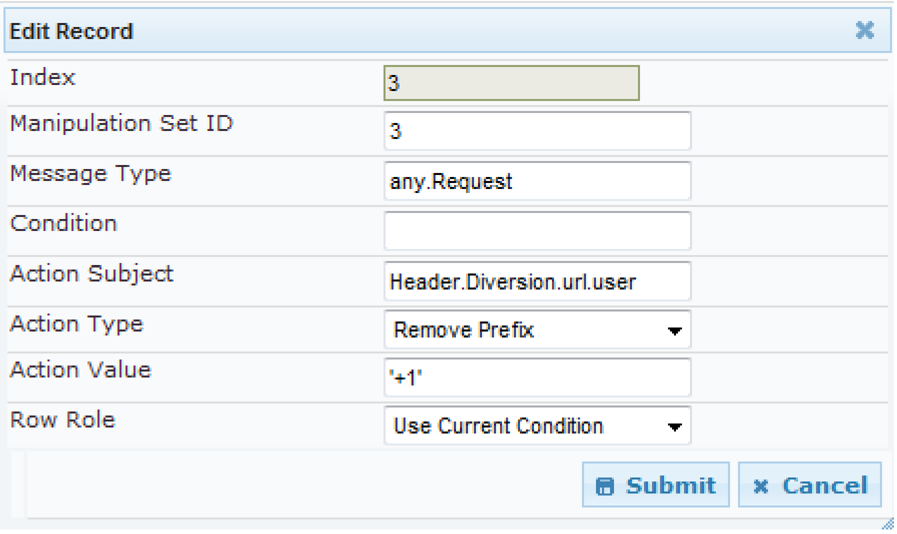
Parameter	Value
Index	**2**
Manipulation Set ID	**3**
Message Type	**invite**
Condition	**header.referred-by exists**
Action Subject	**header.Diversion**
Action Type	**Add**
Action Value	**'<'+header.referred-by.URL+'>'**


Edit Record

Index	2
Manipulation Set ID	3
Message Type	invite
Condition	header.referred-by exists
Action Subject	header.Diversion
Action Type	Add
Action Value	'<'+header.referred-by.URL+'>'
Row Role	Use Current Condition

4. Configure another manipulation rule (Manipulation Set 3) for XO Communications SIP Trunk. This rule applies to messages sent to the XO Communications SIP Trunk (IP Group 2) for the Diversion header. This removes the '+1' from the user part of the Diversion header.

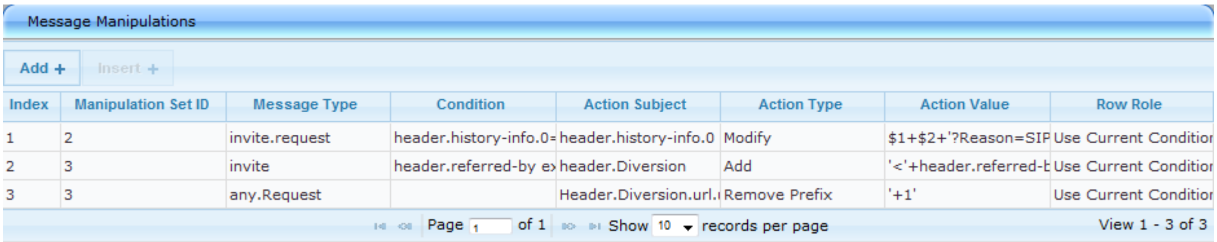
Parameter	Value
Index	**3**
Manipulation Set ID	**3**
Message Type	**any.Request**
Action Subject	**Header.Diversion.url.user**
Action Type	**Remove Prefix**
Action Value	**'+1'**



Edit Record

Index	3
Manipulation Set ID	3
Message Type	any.Request
Condition	
Action Subject	Header.Diversion.url.user
Action Type	Remove Prefix
Action Value	'+1'
Row Role	Use Current Condition

Figure 4-38: Example of Configured SIP Message Manipulation Rules



Message Manipulations

Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
1	2	invite.request	header.history-info.0=	header.history-info.0	Modify	$1+$2+'?Reason=SIP	Use Current Conditior
2	3	invite	header.referred-by e›	header.Diversion	Add	'<'+header.referred-k	Use Current Conditior
3	3	any.Request		Header.Diversion.url.ı	Remove Prefix	'+1'	Use Current Conditior

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

5. Assign Manipulation Set ID 2 to IP Group 1:

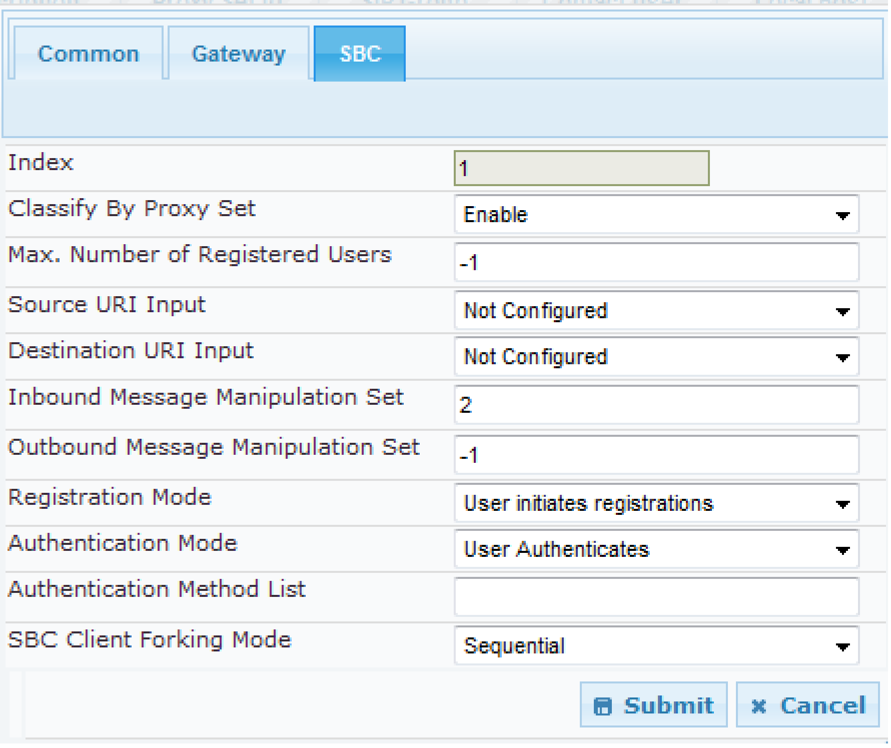
    a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).

    b. Select the row of IP Group 1, and then click **Edit**.

    c. Click the **SBC** tab.

    d. Set the 'Inbound Message Manipulation Set' field to **2**.

Figure 4-39: Assigning Manipulation Set to IP Group 1

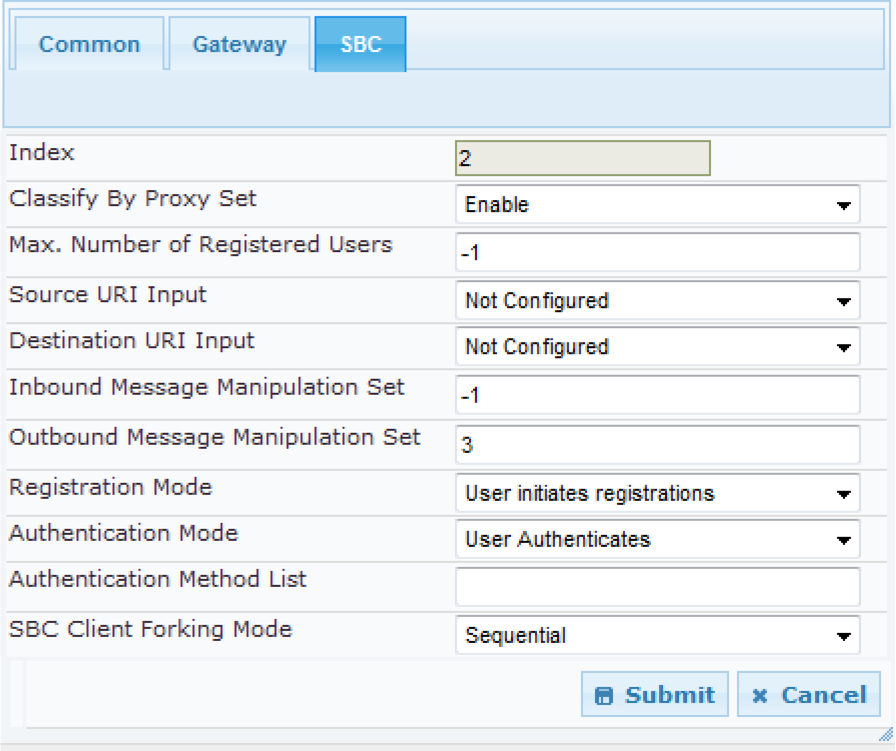


Index	1
Classify By Proxy Set	Enable
Max. Number of Registered Users	-1
Source URI Input	Not Configured
Destination URI Input	Not Configured
Inbound Message Manipulation Set	2
Outbound Message Manipulation Set	-1
Registration Mode	User initiates registrations
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential

e. Click **Submit**.

6. Assign Manipulation Set ID 3 to IP Group 2:
   a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control 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 **3**.

Figure 4-40: Assigning Manipulation Set 2 to IP Group 2



Index	2
Classify By Proxy Set	Enable
Max. Number of Registered Users	-1
Source URI Input	Not Configured
Destination URI Input	Not Configured
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	3
Registration Mode	User initiates registrations
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential

   e. Click **Submit**.

4.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

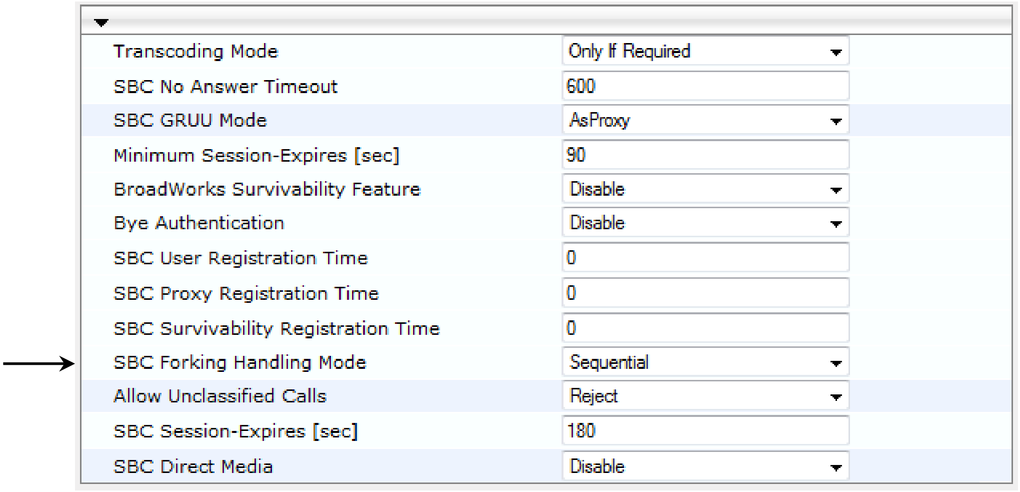
4.14.1 Step 14: Configure Call Forking Mode

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 4-41: Configuring Forking Mode



Transcoding Mode	Only If Required
SBC No Answer Timeout	600
SBC GRUU Mode	AsProxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
Bye Authentication	Disable
SBC User Registration Time	0
SBC Proxy Registration Time	0
SBC Survivability Registration Time	0
SBC Forking Handling Mode	Sequential
Allow Unclassified Calls	Reject
SBC Session-Expires [sec]	180
SBC Direct Media	Disable

3. Click **Submit**.

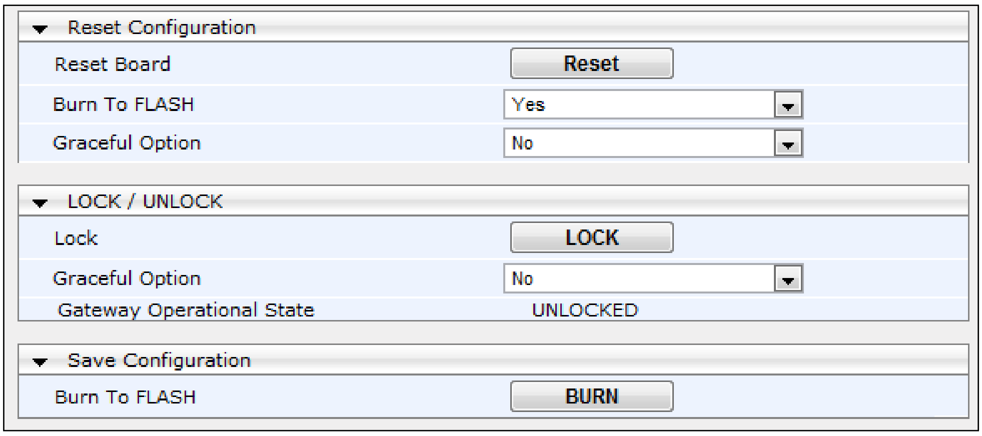
4.15 Step 15: Reset the E-SBC

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 4-42: Resetting the E-SBC



Reset Configuration

Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No

LOCK / UNLOCK

Lock	LOCK
Graceful Option	No
Gateway Operational State	UNLOCKED

Save Configuration

Burn To FLASH	BURN

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

A AudioCodes INI File

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

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

```
;**************
;** Ini File **
;**************
;Board: Mediant 800 - MSBG
;Board Type: 69
;Serial Number: 3455586
;Slot Number: 1
;Software Version: 6.60A.224.004
;DSP Software Version: 5014AE3_R_LD => 660.22
;Board IP Address: 10.15.45.11
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 368M Flash size: 64M
;Num of DSP Cores: 3 Num DSP Channels: 30
;Num of physical LAN ports: 12
;Profile: NONE
;Key features:;Board Type: Mediant 800 - MSBG ;Channel Type: RTP DspCh=30
IPMediaDspCh=30 ;DSP Voice features: IpmDetector ;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 ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;DATA features: Eth-Port=12
;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;PSTN FALLBACK Supported ;E1Trunks=4 ;T1Trunks=4 ;IP Media: CALEA
TrunkTesting ;Control Protocols: MGCP MEGACO H323 SIP SASurvivability
SBC=120 MSFT CLI TestCall=10 ;Default features:;Coders: G711 G726;
;------ Mediant 800 - MSBG HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
; 1 : FALC56 : 1
; 2 : Empty
; 3 : Empty
;----------------------------------------------
[SYSTEM Params]
SyslogServerIP = 10.15.45.200
EnableSyslog = 1
NTPServerUTCOffset = 10800
DebugRecordingDestIP = 10.15.45.200
DebugRecordingStatus = 1
NTPServerIP = '10.15.25.1'
LDAPSEARCHDNSINPARALLEL = 0

[BSP Params]
PCMLawSelect = 3
ExtBootPReqEnable = 1
[Analog Params]
```

```
[ControlProtocols Params]
AdminStateLockControl = 0

[Voice Engine Params]
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1

[WEB Params]
LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'

[SIP Params]
MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
MEDIASECURITYBEHAVIOUR = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLESYMMETRICMKI = 1
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1

[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",
"Redundant";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Active";
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 ]

[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 6, 10, 10.15.45.11, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 195.189.192.155, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.55.100, GROUP_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 1 = "MRLan", Voice, , 6000, 10, 6090, 1;
CpMediaRealm 2 = "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 = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE15.ilync15.local:5067", 2, 1;
ProxyIp 1 = "205.158.163.230:5060", 0, 2;
[ \ProxyIp ]

[ 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_SBCAllowedCodersGroupID, 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_SBCPlayHeldTone, IpProfile_SBCRemoteHoldFormat,
IpProfile_DelayTimeForInvite;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 3, -1, 1, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, -1, 0, 1, 0, 0, 0, 0,
8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1, 0, 3, 0, 1, 0, 1, 1, 0, 0,
1, 0, 1, 0, 0, 0, -1, 1, 0, 1, 0, 3, 0;
IpProfile 2 = "XO", 1, 2, 0, 10, 10, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, -1,
1, 0, 3, -1, 1, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, 2, 1, 2, 0, 0, 0, 0, 8,
300, 400, 1, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 3, 0, 0, 0, 1, 1, 0, 0, 0,
0, 0, 0, 0, 0, -1, 0, 0, 1, 0, 0, 0;
[ \IpProfile ]

[ ProxySet ]
FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput,
ProxySet_ProxyRedundancyMode;
ProxySet 0 = 0, 60, 0, 0, 0, 0, -1;
ProxySet 1 = 1, 60, 1, 1, 1, 0, -1;
ProxySet 2 = 1, 60, 0, 1, 2, 0, -1;
[ \ProxySet ]

[ IPGroup ]
FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName;
IPGroup 1 = 0, "Lync Server", 1, "195.189.192.155", "", 0, -1, -1, 0, -1,
1, "MRLan", 1, 1, -1, 2, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "XO Communications", 2, "195.189.192.155", "", 0, -1, -1,
0, -1, 2, "MRWan", 1, 2, -1, -1, 3, 0, 0, "", 0, -1, -1, "";
[ \IPGroup ]

[ IP2IPRouting ]
FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_CostGroup;
IP2IPRouting 0 = 1, "*", "*", "*", "*", 6, , -1, 0, 1, -1, , "internal",
0, -1, 0, ;
IP2IPRouting 1 = 1, "*", "*", "*", "*", 0, , -1, 0, 0, 2, 2, "", 0, -1,
0, ;
IP2IPRouting 2 = 2, "*", "*", "*", "*", 0, , -1, 0, 0, 1, 1, "", 0, -1,
0, ;
[ \IP2IPRouting ]

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

[ IPInboundManipulation ]
FORMAT IPInboundManipulation_Index =
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose,
IPInboundManipulation_SrcIPGroupID,
IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost,
IPInboundManipulation_RequestType, IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft,
IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 0 = 0, 0, 1, "+", "*", "*", "*", 0, 0, 2, 0, 255,
"", "";
IPInboundManipulation 1 = 0, 0, 2, "", "*", "214", "*", 0, 1, 0, 0, 255,
"+1", "";
IPInboundManipulation 2 = 0, 0, 1, "*", "*", "+", "*", 0, 1, 1, 0, 255,
"", "";
[ \IPInboundManipulation ]

 [ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0;
[ \CodersGroup0 ]
[ CodersGroup1 ]
FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce;
CodersGroup1 0 = "g711Alaw64k", 20, 0, -1, 0;
CodersGroup1 1 = "g711Ulaw64k", 20, 0, -1, 0;
[ \CodersGroup1 ]

[ CodersGroup2 ]
FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = "g729", 20, 0, -1, 0;
[ \CodersGroup2 ]

[ AllowedCodersGroup1 ]
FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Ulaw64k";
AllowedCodersGroup1 1 = "eg711Alaw";
[ \AllowedCodersGroup1 ]

[ AllowedCodersGroup2 ]
FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";
[ \AllowedCodersGroup2 ]

[ MessageManipulations ]
FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 1 = 2, "invite.request", "header.history-
info.0==regex.(<.*)(user=phone)(>)(.*)", "header.history-info.0", 2,
"$1+$2+'?Reason=SIP%3Bcause%3D404'+$3+$4", 0;
MessageManipulations 2 = 3, "invite", "header.referred-by exists",
"header.Diversion", 0, "'<'+header.referred-by.URL+'>'", 0;
MessageManipulations 3 = 3, "any.Request", "",
"Header.Diversion.url.user", 6, "'+1'", 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

www.audiocodes.com