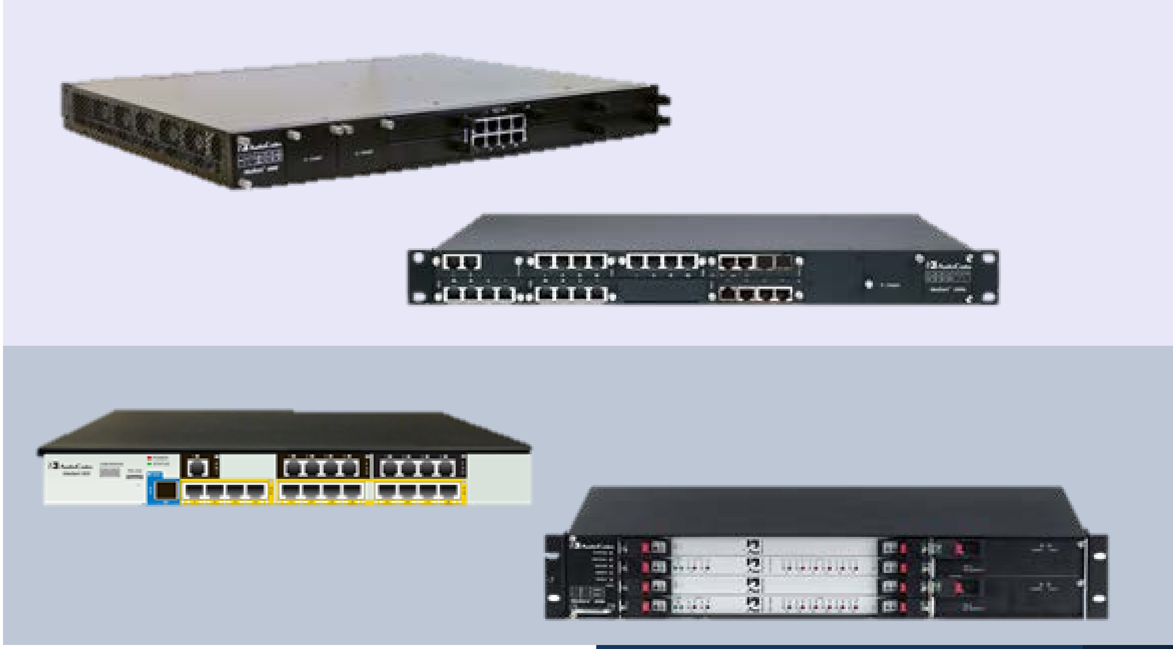
AudioCodes™ Mediant™ Series

Enterprise Session Border Controllers

Interoperability Lab

Configuration Note

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



March 2013

Document #: LTRT-12230

Table of Contents

Reader's Notes

Notice

This note shows how to connect Microsoft Lync Server 2013 and Colt 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: March-03-2013

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.

Note: Throughout this document, unless otherwise specified, the term *E-SBC* refers to any of the following AudioCodes products:

- Mediant 800 Gateway & E-SBC
- Mediant 1000B Gateway & E-SBC
- Mediant 3000 Gateway & E-SBC
- Mediant 4000 E-SBC

1 Introduction

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

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Colt Partners responsible for installing and configuring Colt's SIP Trunking and Microsoft's Lync Communication platform 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 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.216.006
Protocol	▪ SIP/UDP or TCP (to the Colt SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 Colt SIP Trunking Version

Table 2-2: Colt Version

Vendor/Service Provider	Colt
SSW Model/Service	Sonus
Software Version	8.4.4
Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Server 2013 Version

Table 2-3: Microsoft Lync Server 2013 Version

Vendor	Microsoft
Model	Microsoft Lync
Software Version	Release 2013 5.0.8308.0
Protocol	SIP
Additional Notes	None

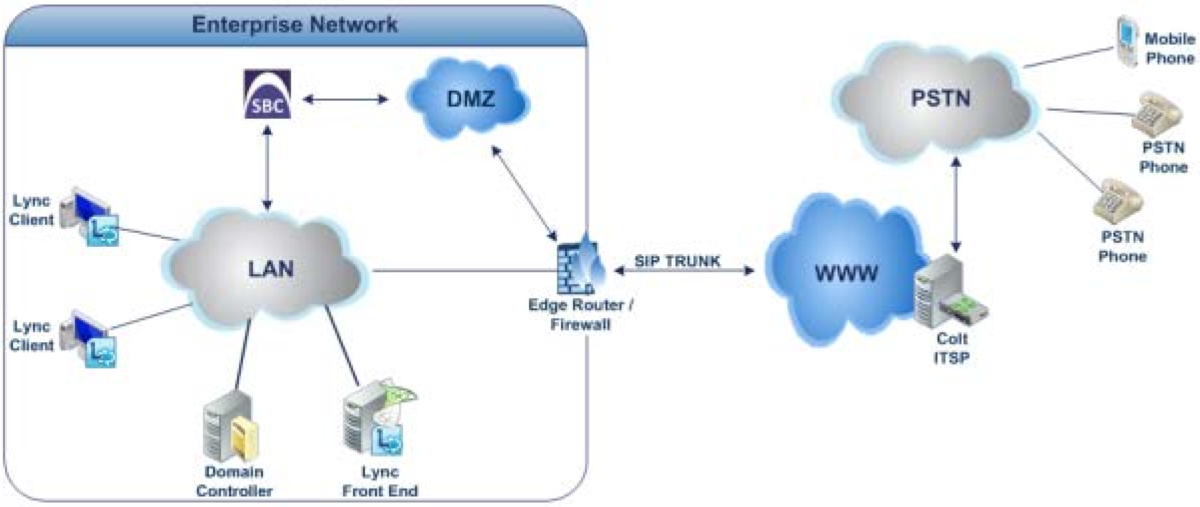
2.4 Interoperability Test Topology

Interoperability between AudioCodes E-SBC and Colt SIP trunk with Lync 2013 was tested using the following topology setup:

- The enterprise is deployed with Microsoft Lync Server 2013 in its private network for enhanced communication within the enterprise.
- The enterprise wants to offer its employees enterprise-voice capabilities and to connect the enterprise to the PSTN network using Colt's SIP Trunking service (Internet Telephony Service Provider / ITSP).
- 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 the Lync Server 2013 network in the enterprise LAN and Colt's SIP Trunk located in the public network.

The figure below illustrates E-SBC interworking between Lync Server 2013 and Colt's SIP Trunking site.

Figure 2-1: Interoperability Test Topology between E-SBC and Colt SIP Trunk with Lync 2013



2.4.1 Environment Setup

The example scenario includes this environment setup:

Table 2-4: Environment Setup

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

2.4.2 Known Limitations

- Colt SIP Trunk does not send RTCP packets in active call and in hold call.
- In some cases, Lync 2013 will terminate the call with network problems as the cause. To overcome this issue, disable the RTCPActiveCalls and RTCPCallsOnHold parameters on the Lync 2013 trunk configuration. However, when RTCP active calls or RTCP calls on hold is false, it is recommended to enable the session timer to periodically verify that the call is still active.

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, these are beyond the scope of this document.

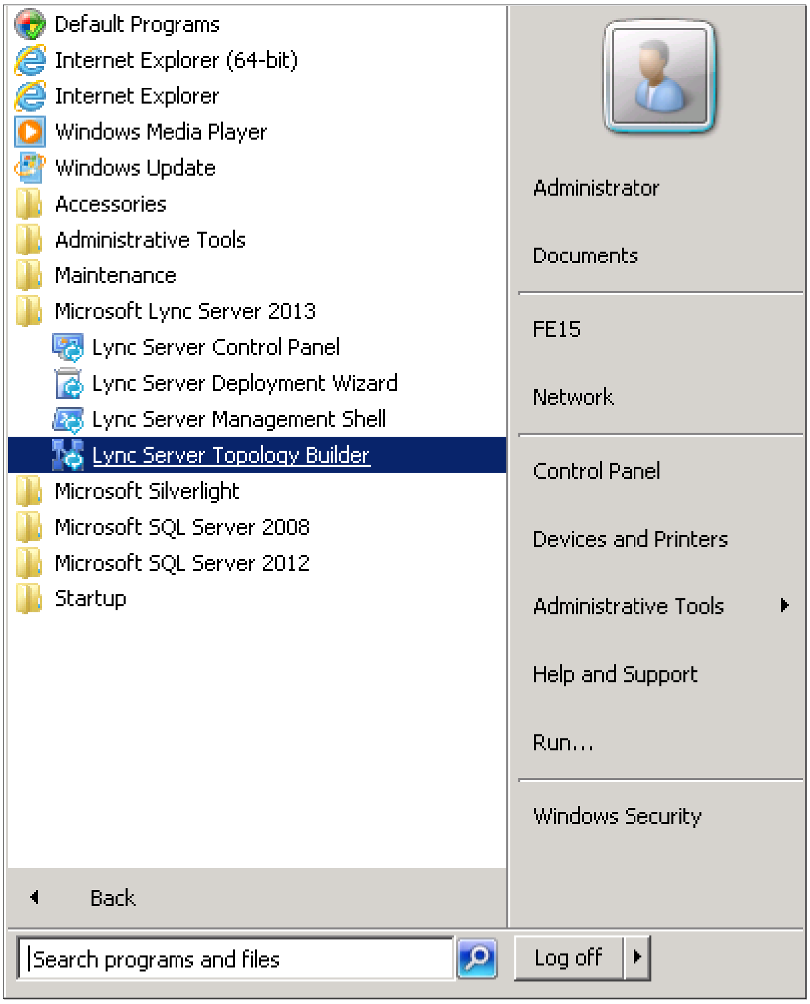
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

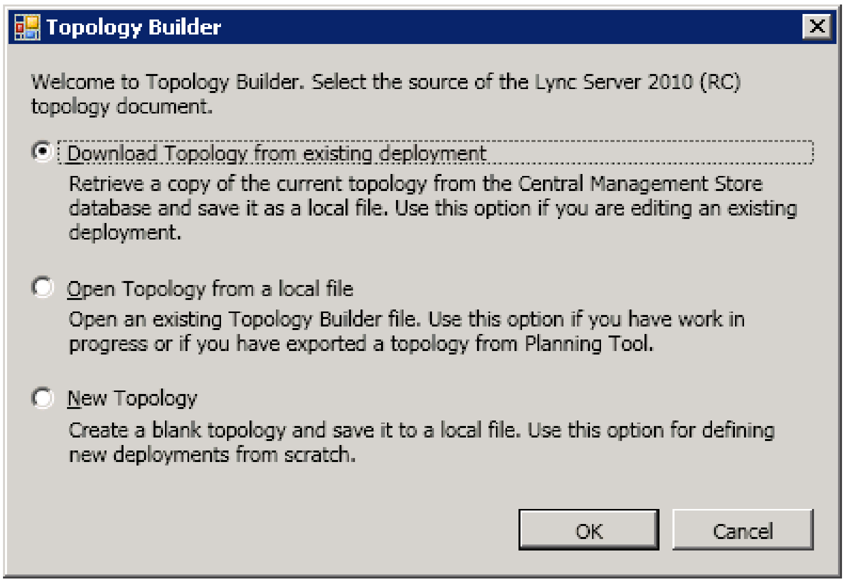
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder by doing the following: Click the Windows **Start** menu, click **All Programs**, and then click **Lync Server Topology Builder**.

Figure 3-1: Starting the Lync Server Topology Builder



The following screen is displayed:

Figure 3-2: Topology Builder Options



Topology Builder

Welcome to Topology Builder. Select the source of the Lync Server 2010 (RC) topology document.

● Download Topology from existing deployment

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

○ Open Topology from a local file

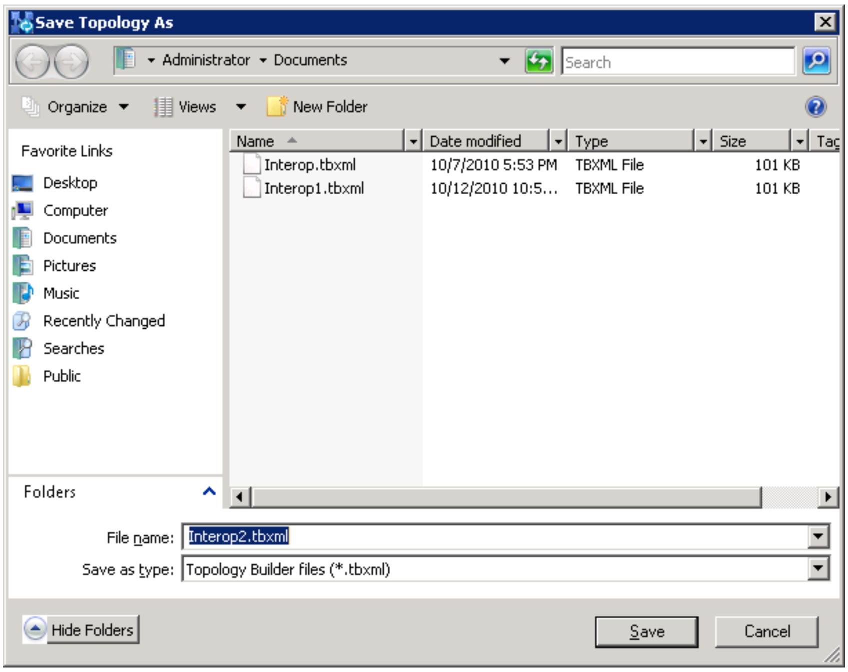
Open an existing Topology Builder file. Use this option if you have work in progress or if you have exported a topology from Planning Tool.

○ 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



Save Topology As

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	

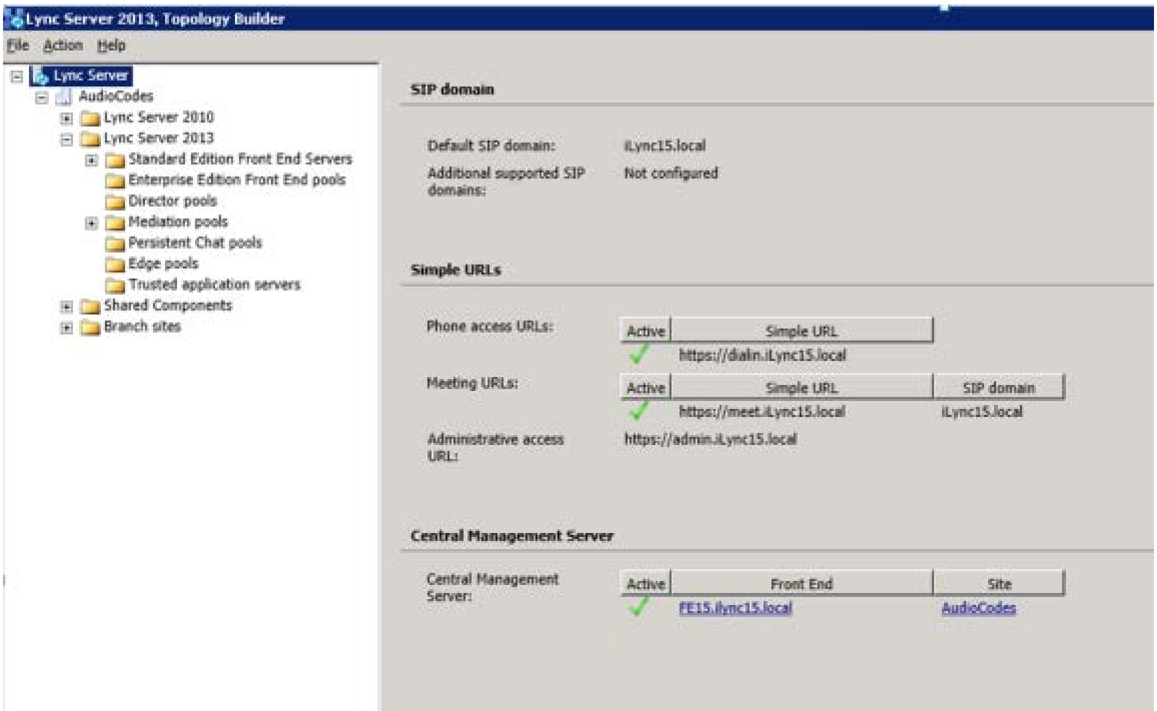
File name: Interop2.tbxml

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

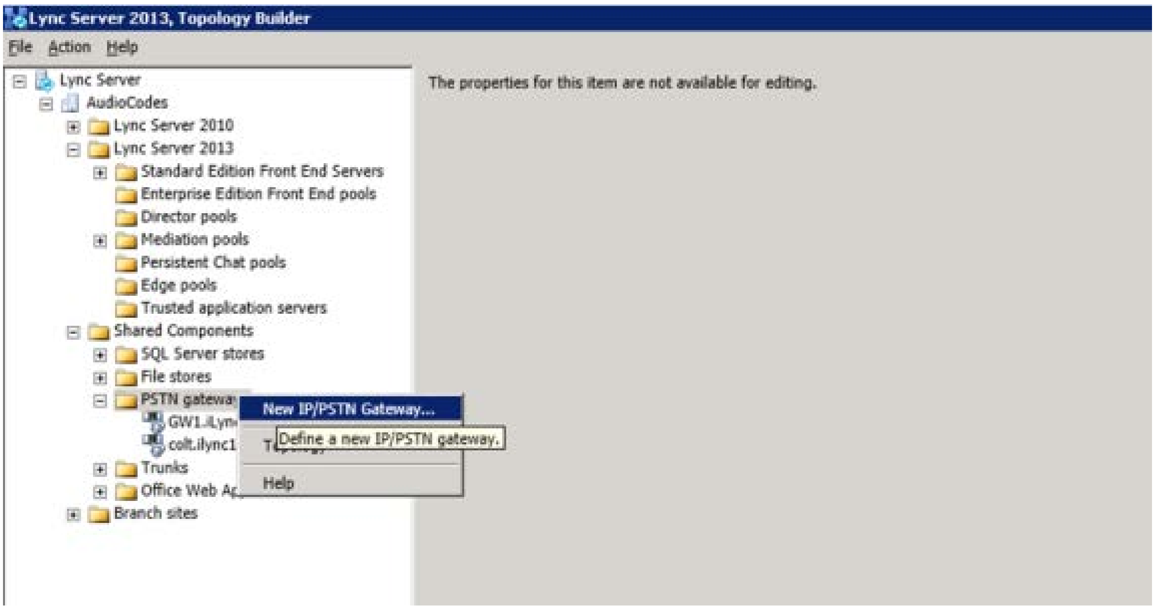
Central Management Server:

Active	Front End	Site
✓	FE15.ilync15.local	AudioCodes

4. Under Lync Server 2013, your site name, Shared Components, right-click the **PSTN Gateways** node, and then click **New PSTN Gateway**.

5. Right-click the **PSTN gateways** folder, and then choose **New IP/PSTN Gateway**, as shown below:

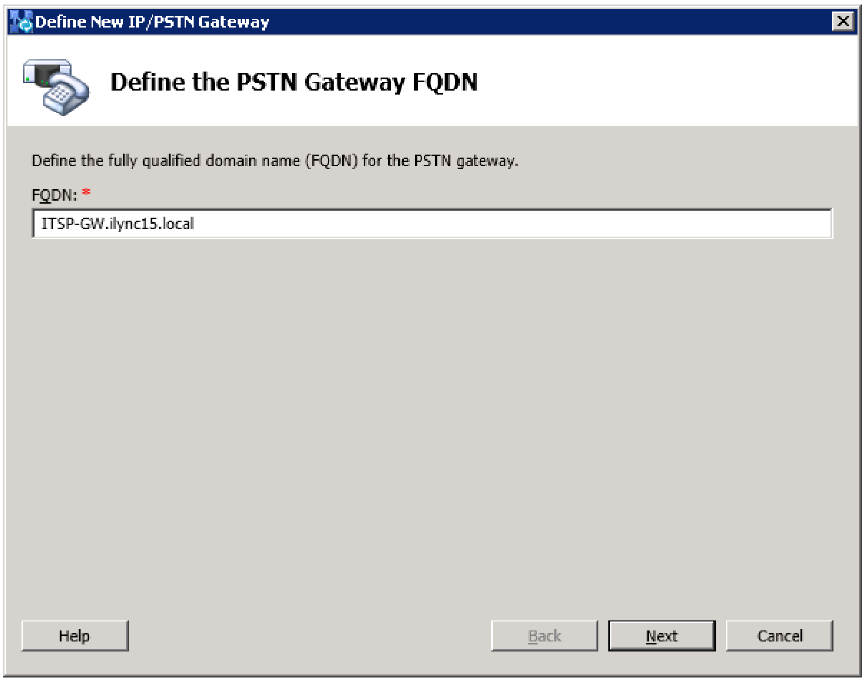
Figure 3-5: Choosing New IP/PSTN Gateway



The properties for this item are not available for editing.

The following dialog box appears:

Figure 3-6: Define New IP/PSTN Gateway



Define New IP/PSTN Gateway

Define the PSTN Gateway FQDN

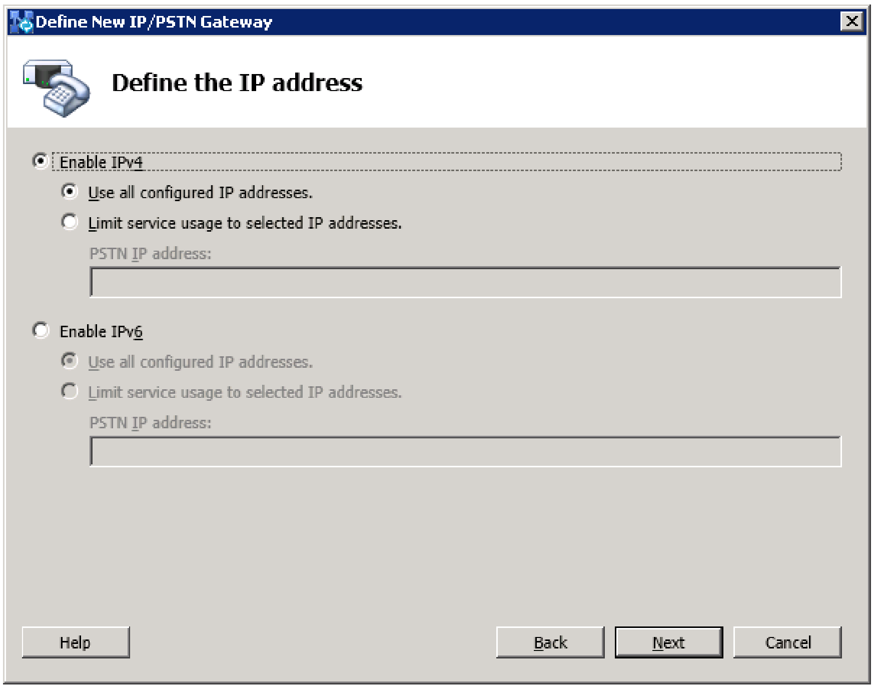
Define the fully qualified domain name (FQDN) for the PSTN gateway.

FQDN: *

ITSP-GW.ilync15.local

6. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., "ITSP-GW.ilync15.local"). This FQDN should be update in the relevant DNS record, and then click **Next.**
7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and click **Next**.

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.

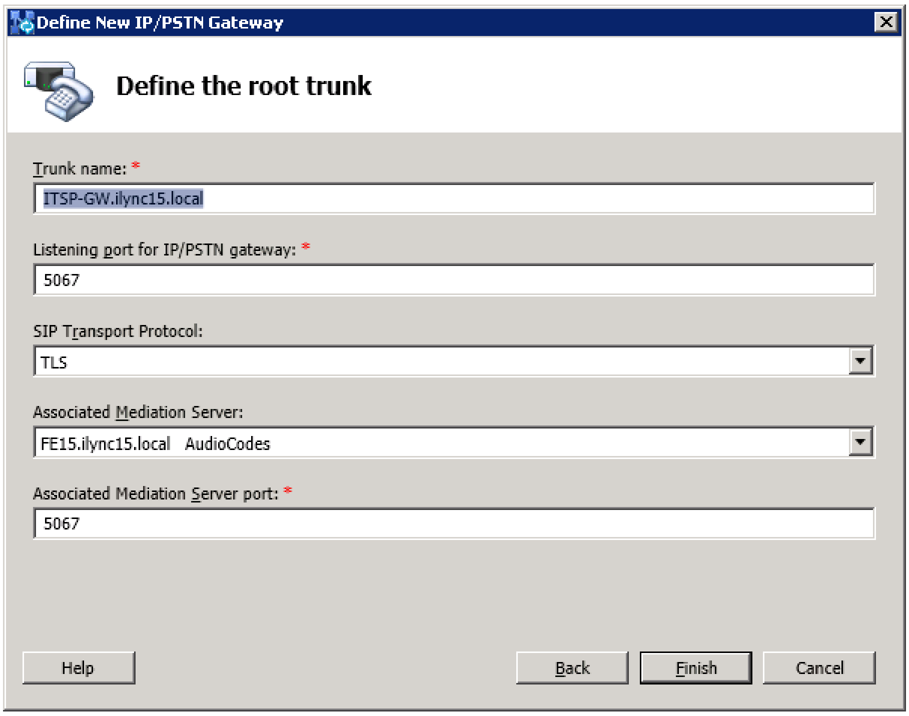
PSTN IP address:

8. Click **Next**.

9. 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.

Note: When defining a PSTN gateway in Topology Builder, 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 (i.e., **5067**).

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

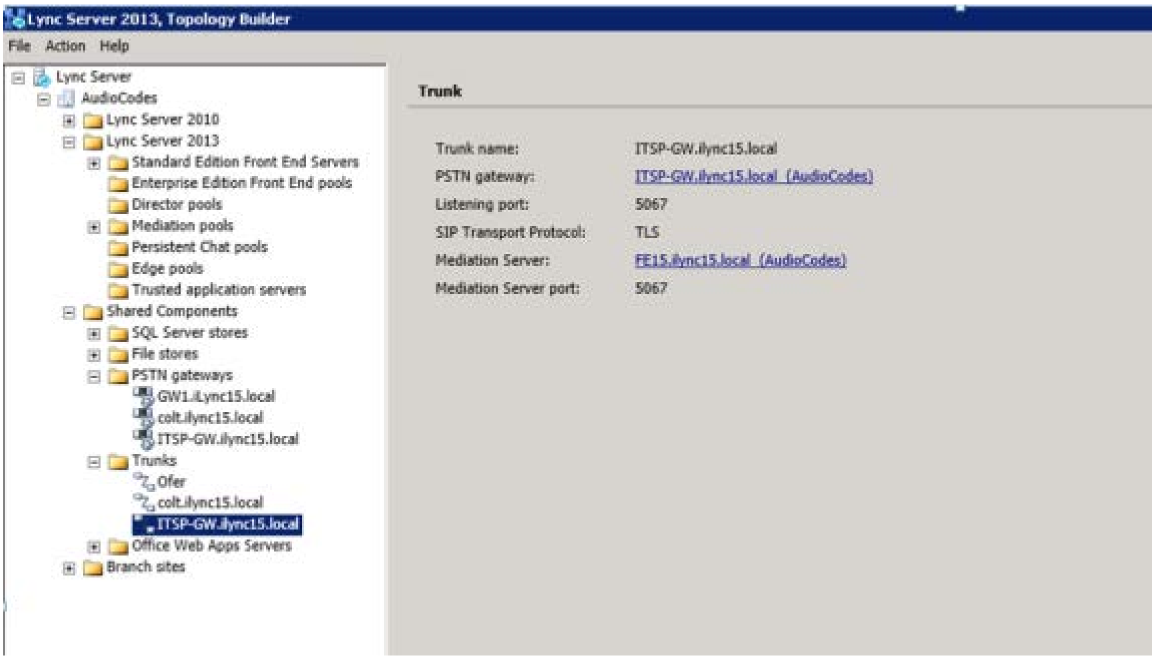
c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.

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

e. Click **Finish**.

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

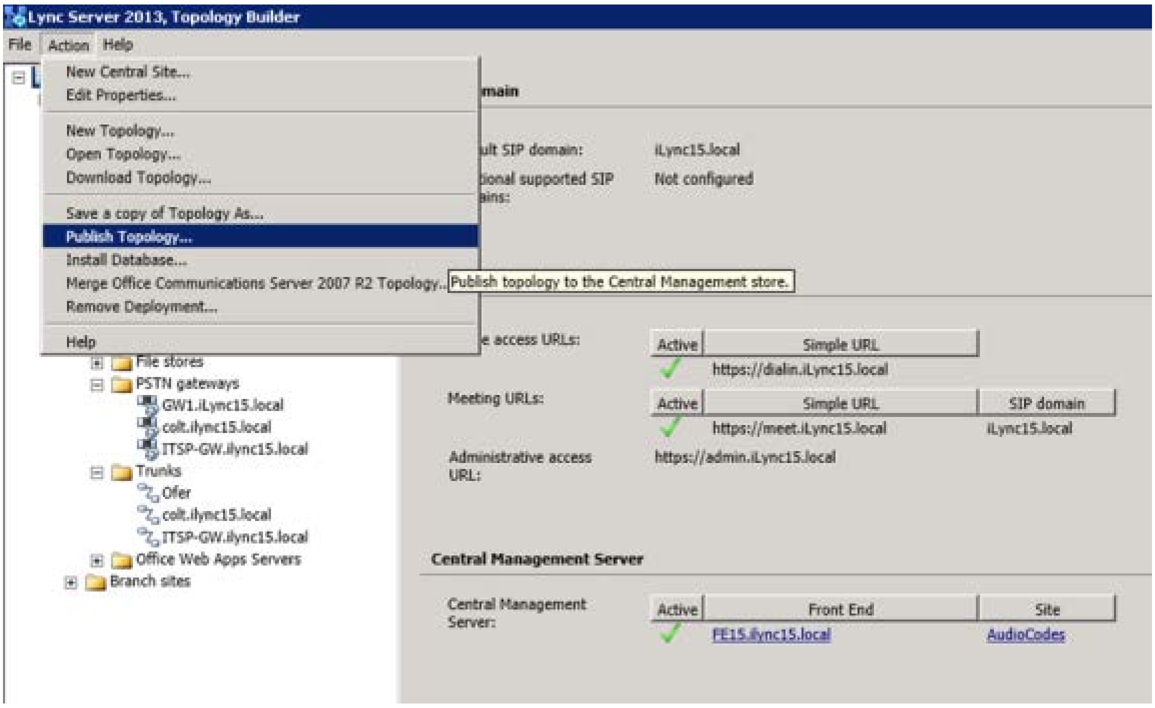
Figure 3-9: E-SBC Added as an IP/PSTN Gateway and Trunk Created



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

10. Publish the Topology: In the main tree, select the root item 'Lync Server', and then from the **Action** menu on the menu bar, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



ult SIP domain: iLync15.local

ional 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

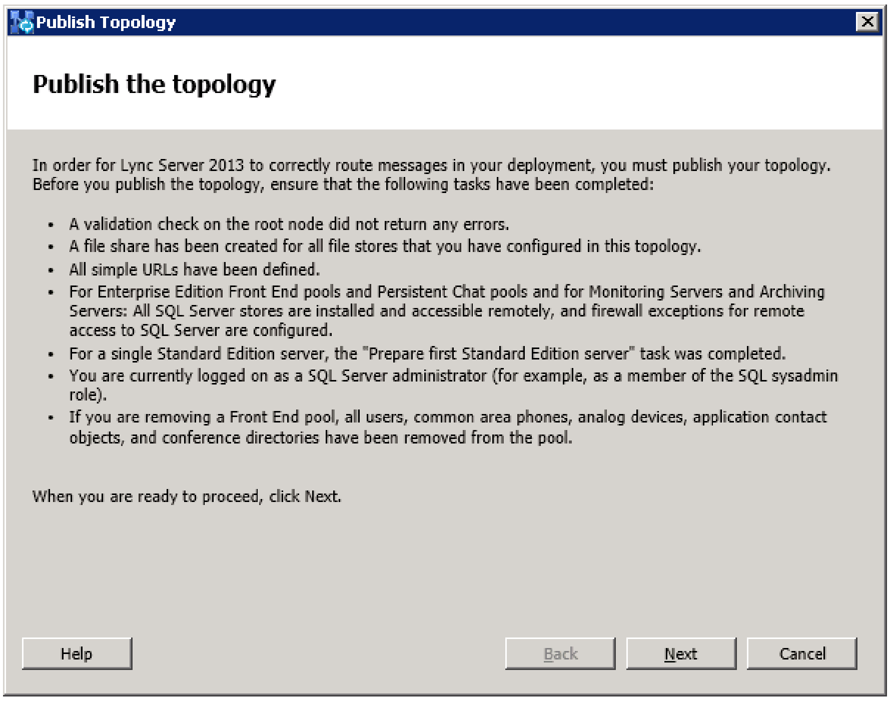
Administrative access URL: https://admin.iLync15.local

Central Management Server:

Active	Front End	Site
✓	FE15.ilync15.local	AudioCodes

The Publish Topology screen is displayed:

Figure 3-11: Publish Topology Screen



Publish the topology

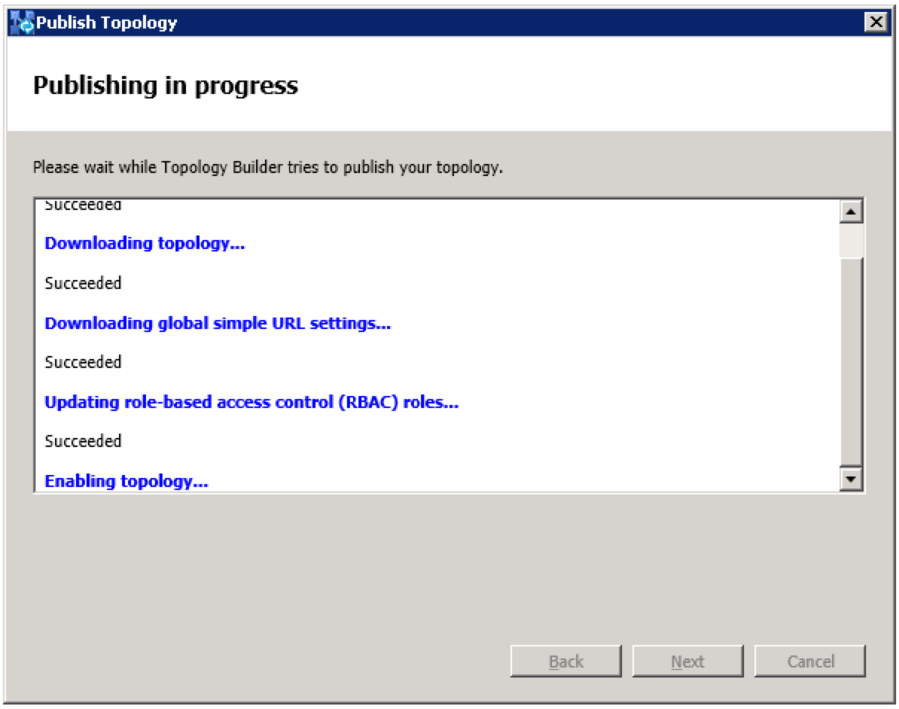
In order for Lync Server 2013 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:

- 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.

11. Click **Next**; the Topology Builder starts to publish your topology:

Figure 3-12: Publish Topology Progress Screen



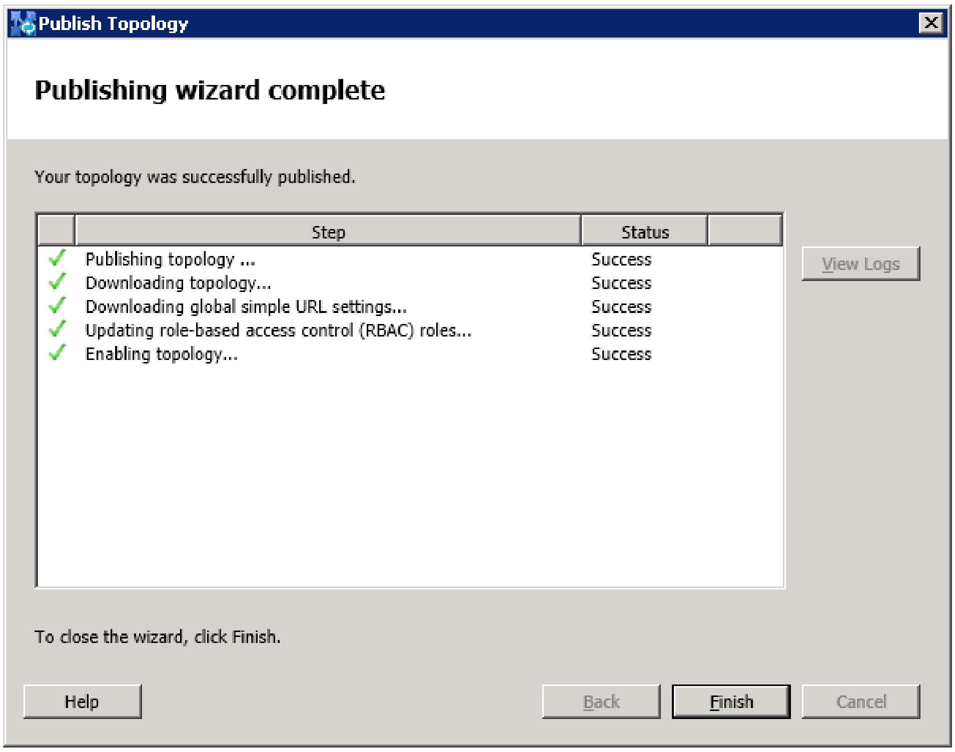
Publishing in progress

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...
```

12. Wait until the publishing topology process completes successfully:

Figure 3-13: Publish Topology Successfully Completed



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.

13. Click **Finish**.

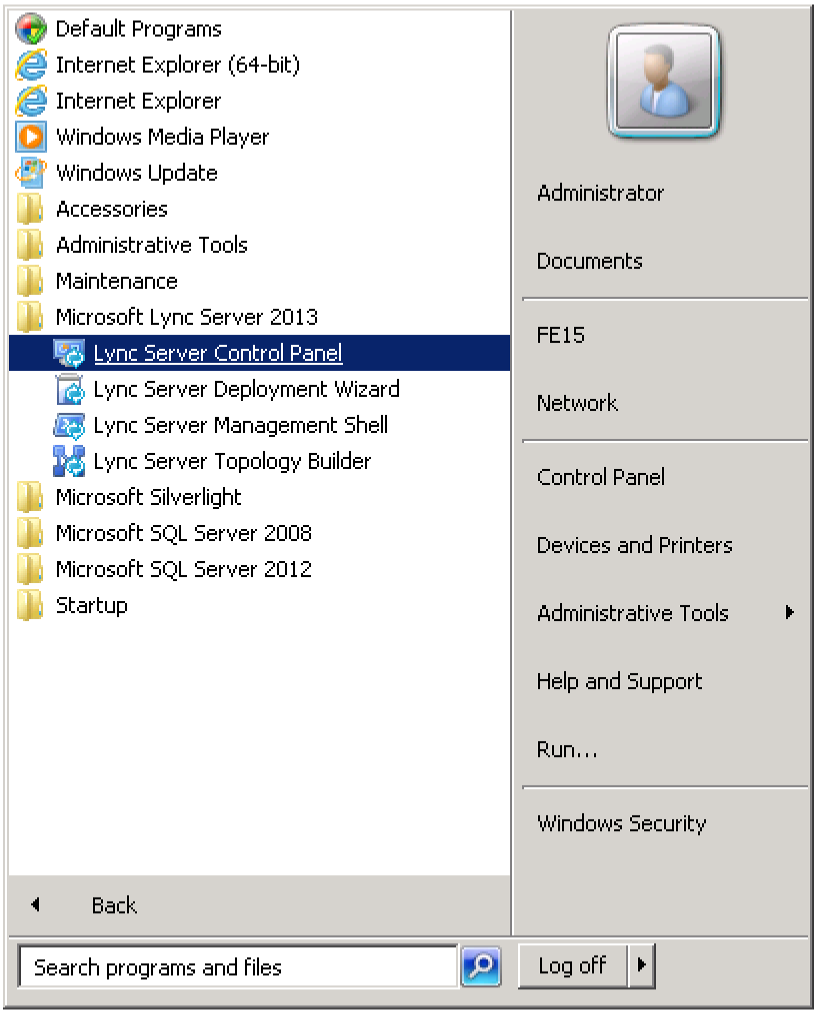
3.2 Configuring the "Route" on Lync Server 2013

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:

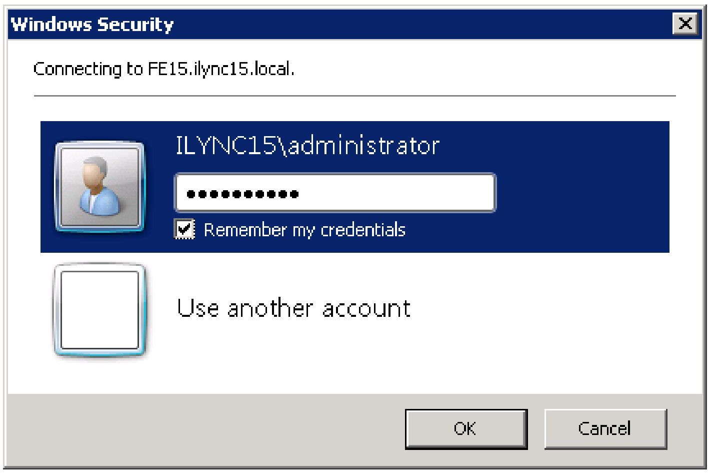
1. Start the Microsoft Lync Server 2013 Control Panel: click **Start**, click **All Programs**, click **Microsoft Lync Server 2013**, and then click **Lync Server Control Panel**, as shown below:

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.

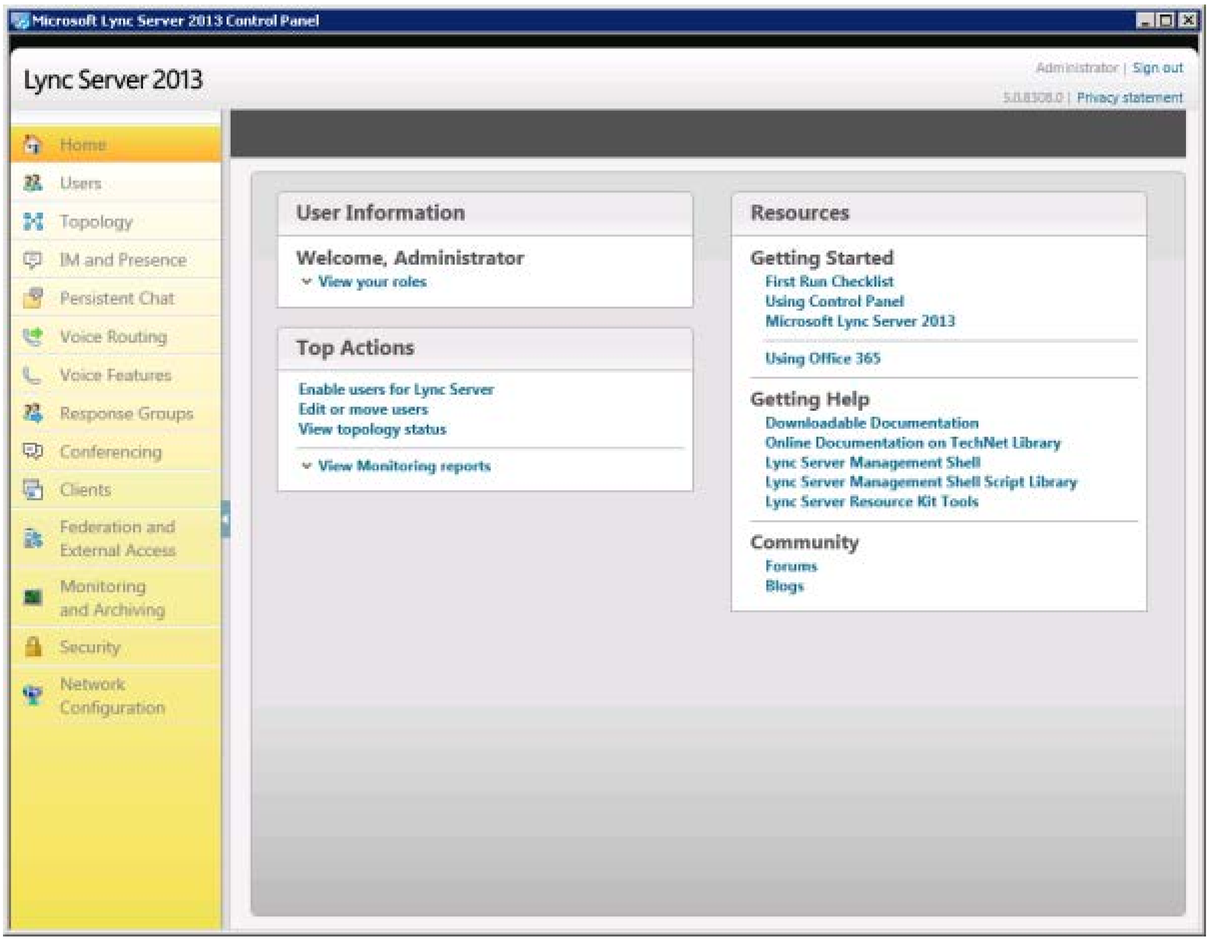
ILYNC15\administrator

••••••••••

☑ Remember my credentials

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



Microsoft Lync Server 2013 Control Panel

Lync Server 2013

Administrator | Sign out
5.0.8308.0 | Privacy statement

User Information

Welcome, Administrator

View your roles

Top Actions

Enable users for Lync Server
Edit or move users
View topology status

View Monitoring reports

Resources

Getting Started
First Run Checklist
Using Control Panel
Microsoft Lync Server 2013

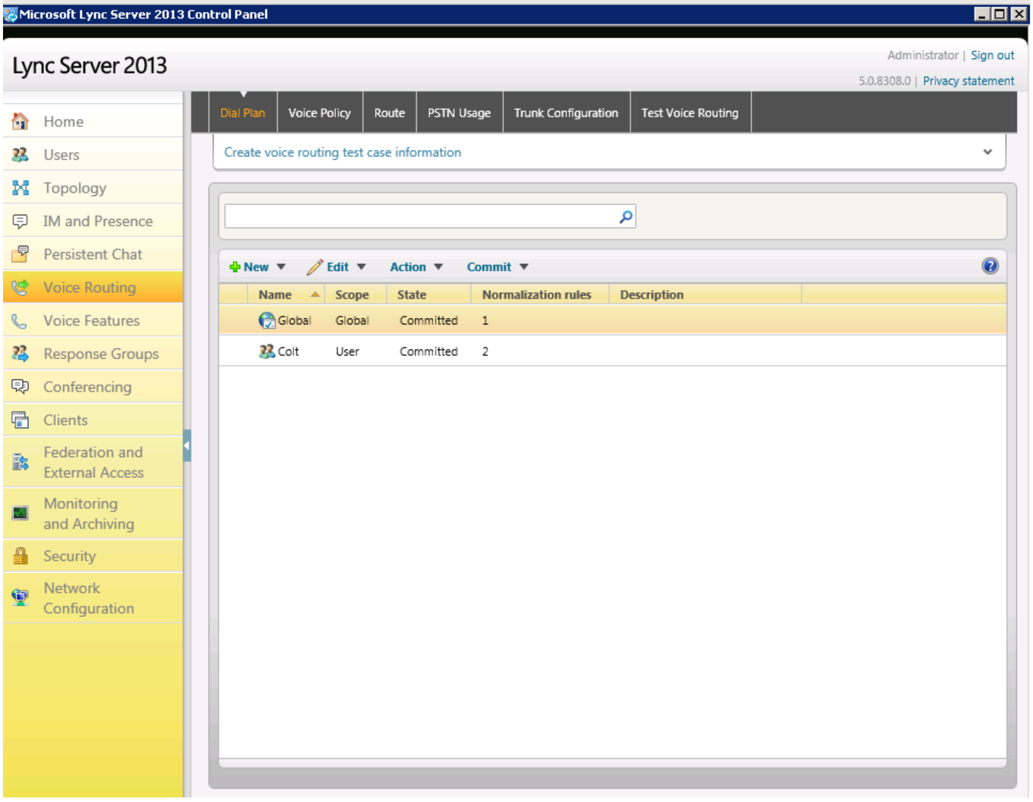
Using Office 365

Getting Help
Downloadable Documentation
Online Documentation on TechNet Library
Lync Server Management Shell
Lync Server Management Shell Script Library
Lync Server Resource Kit Tools

Community
Forums
Blogs

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

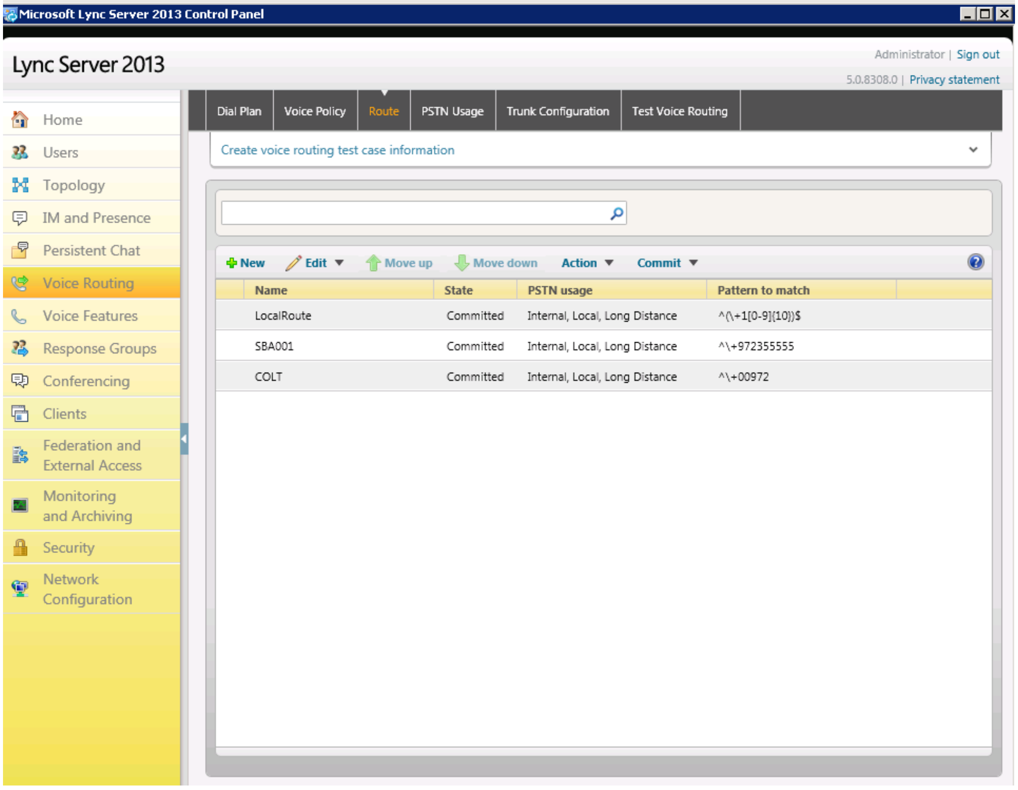
Figure 3-17: Voice Routing Page



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

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

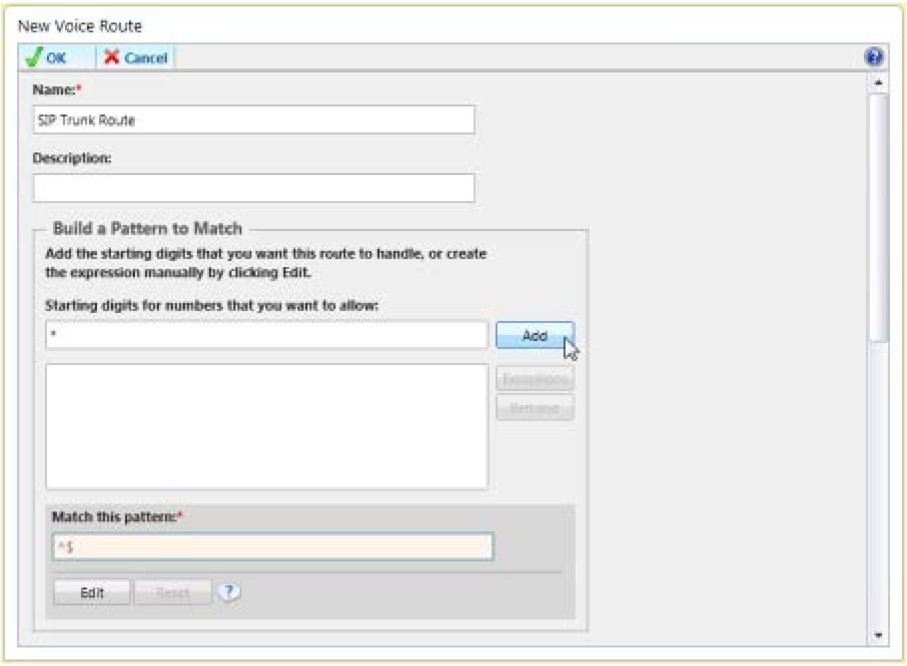
Figure 3-18: Route Option



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 dialog box appears:

Figure 3-19: Adding New Voice Route



Name:* SIP Trunk Route

Description:

Build a Pattern to Match

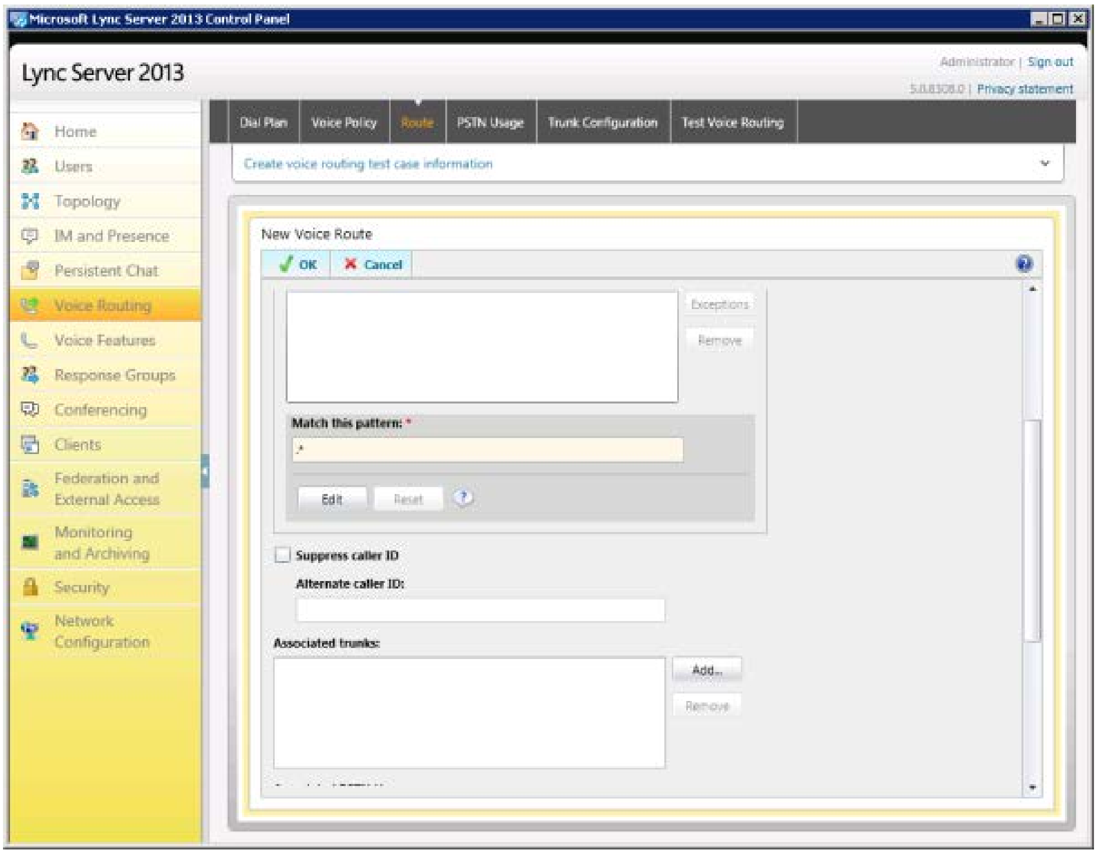
Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.

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. Under the 'Build a Pattern to Match' group, enter the starting digits you want this route to handle (e.g., **"*"**, which means to match all numbers).
8. Click **Add**.

Figure 3-20: Adding New Trunk



Match this pattern: * .*

□ Suppress caller ID

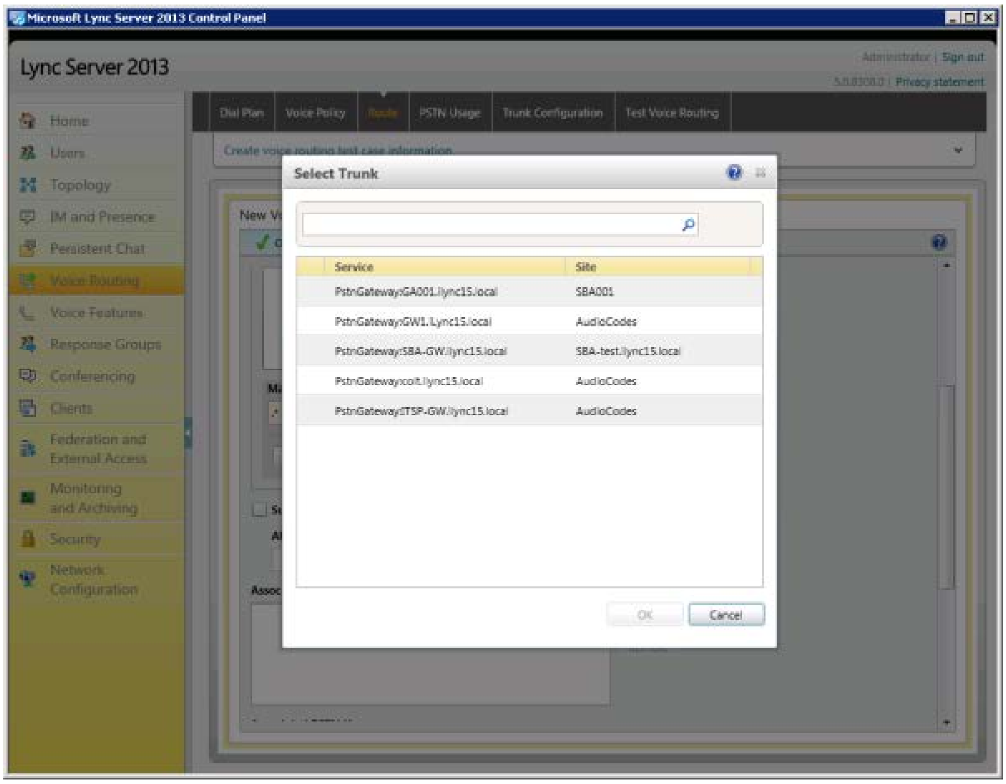
Alternate caller ID:

Associated trunks:

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

   a. In the Associated Trunks pane, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks

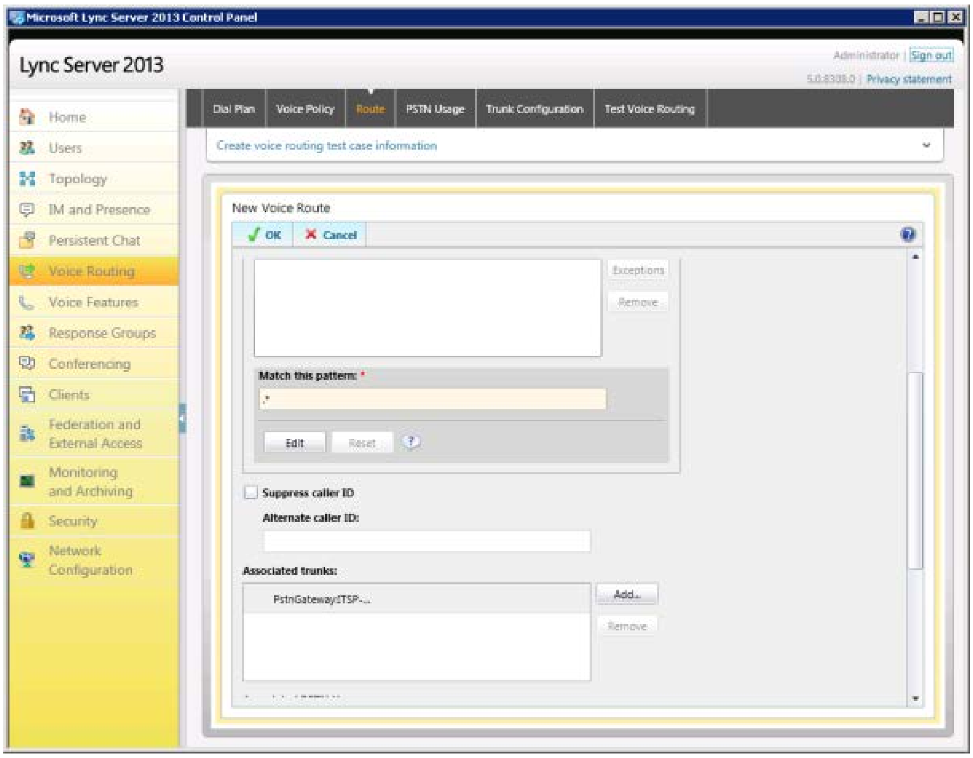


Select Trunk

Service	Site
PstnGateway:GA001.lync15.local	SBA001
PstnGateway:GW1.Lync15.local	AudioCodes
PstnGateway:SBA-GW.lync15.local	SBA-test.lync15.local
PstnGateway:colt.lync15.local	AudioCodes
PstnGateway:ITSP-GW.lync15.local	AudioCodes

   b. Select the E-SBC Trunk you created, and then click **OK**.

Figure 3-22: Selected E-SBC Trunk



Match this pattern: * .*

☐ Suppress caller ID

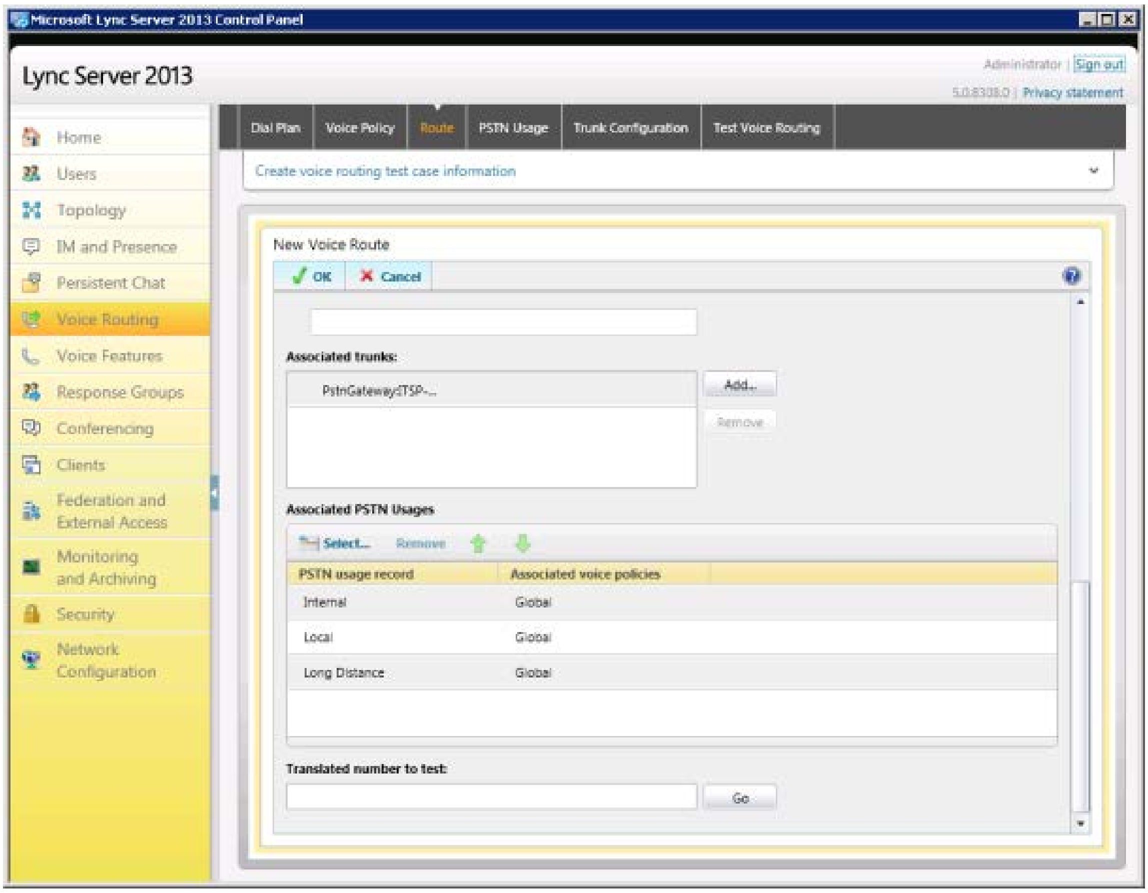
Alternate caller ID:

Associated trunks:

PstnGateway:ITSP-...

10. Associate a PSTN Usage to this route: In 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:TSP-...

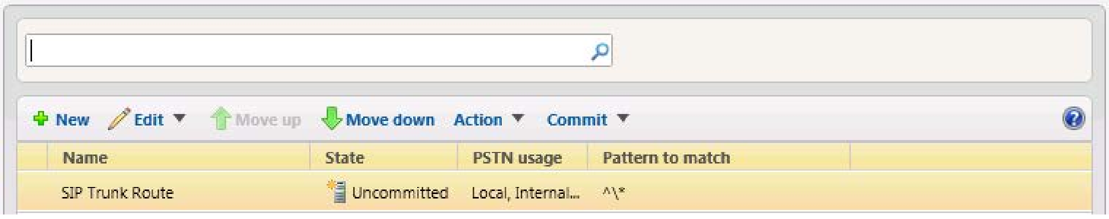
Associated PSTN Usages

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

Translated number to test:

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

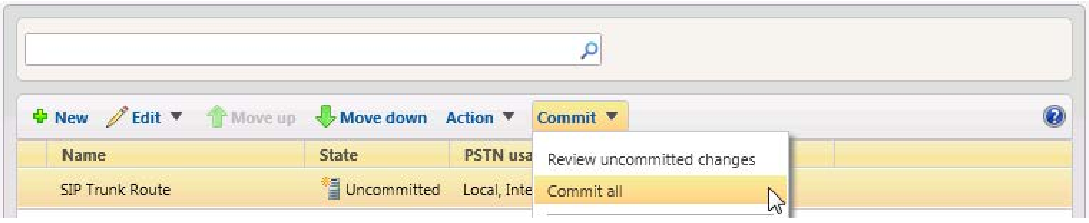
Figure 3-24: Confirmation of New Voice Route



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

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

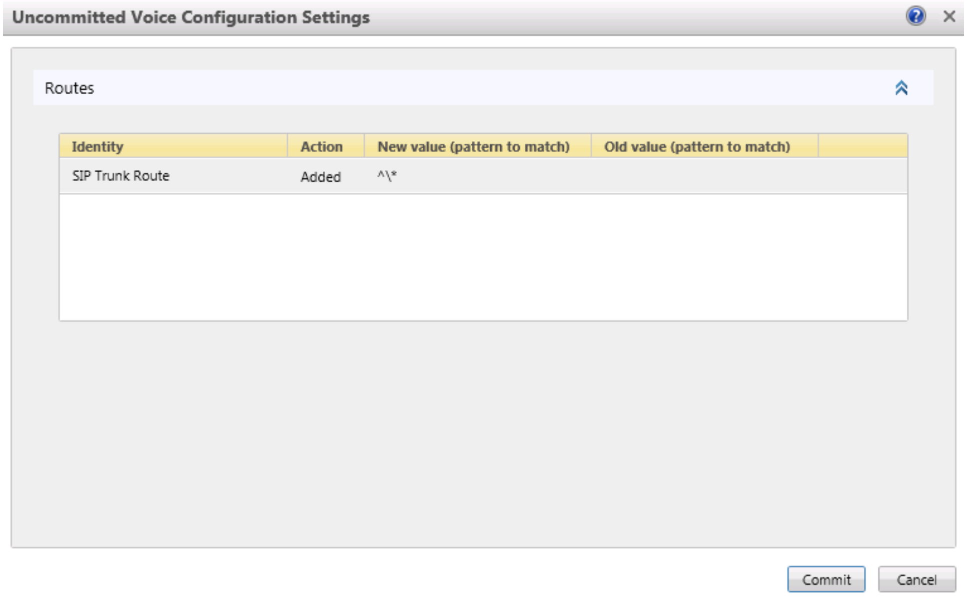
Figure 3-25: Committing Voice Routes



Name	State	PSTN usa
SIP Trunk Route	Uncommitted	Local, Inte

The Uncommitted Voice Configuration Settings dialog box appears:

Figure 3-26: Uncommitted Voice Configuration Settings



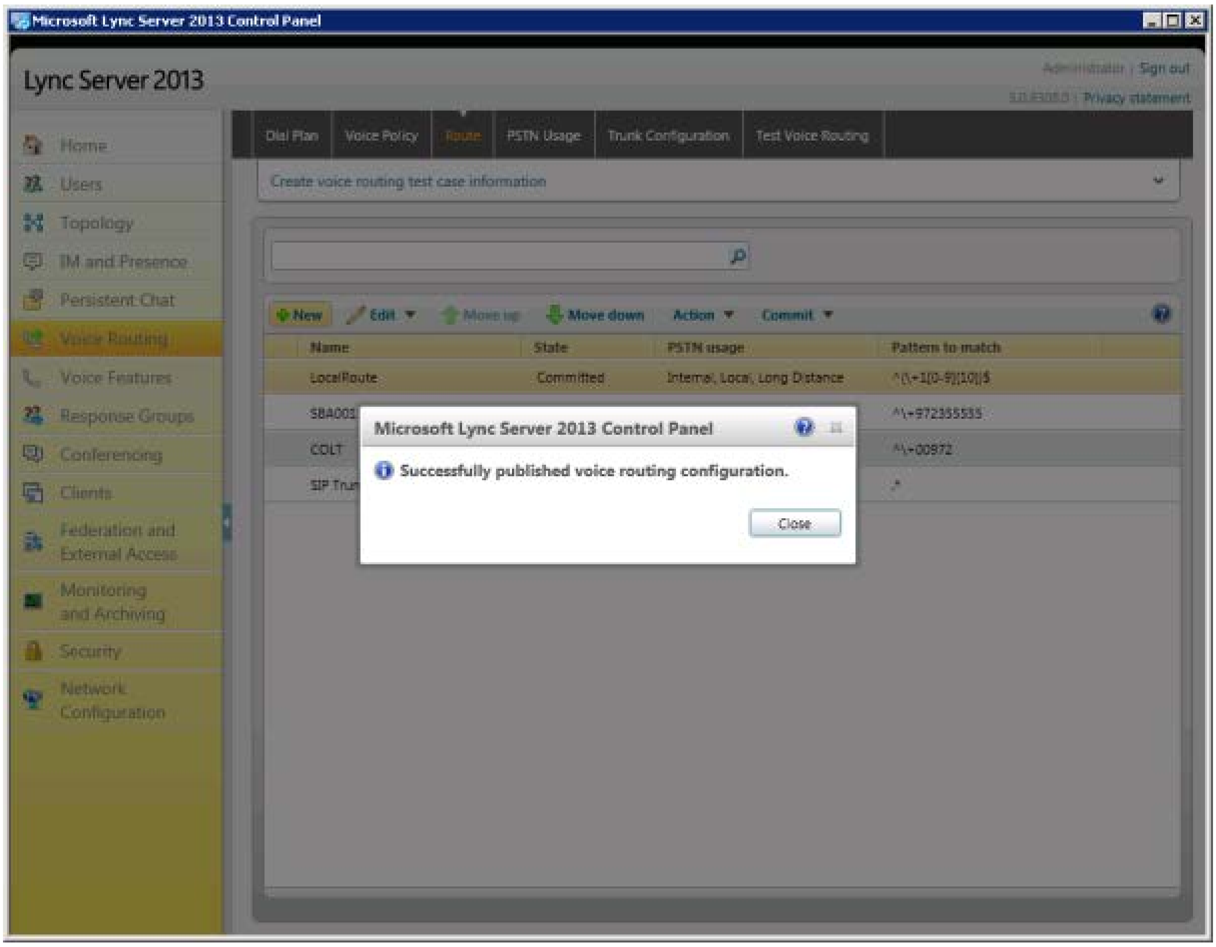
Uncommitted Voice Configuration Settings

Routes

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

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

Figure 3-27: Confirmation of Successful Voice Routing Configuration



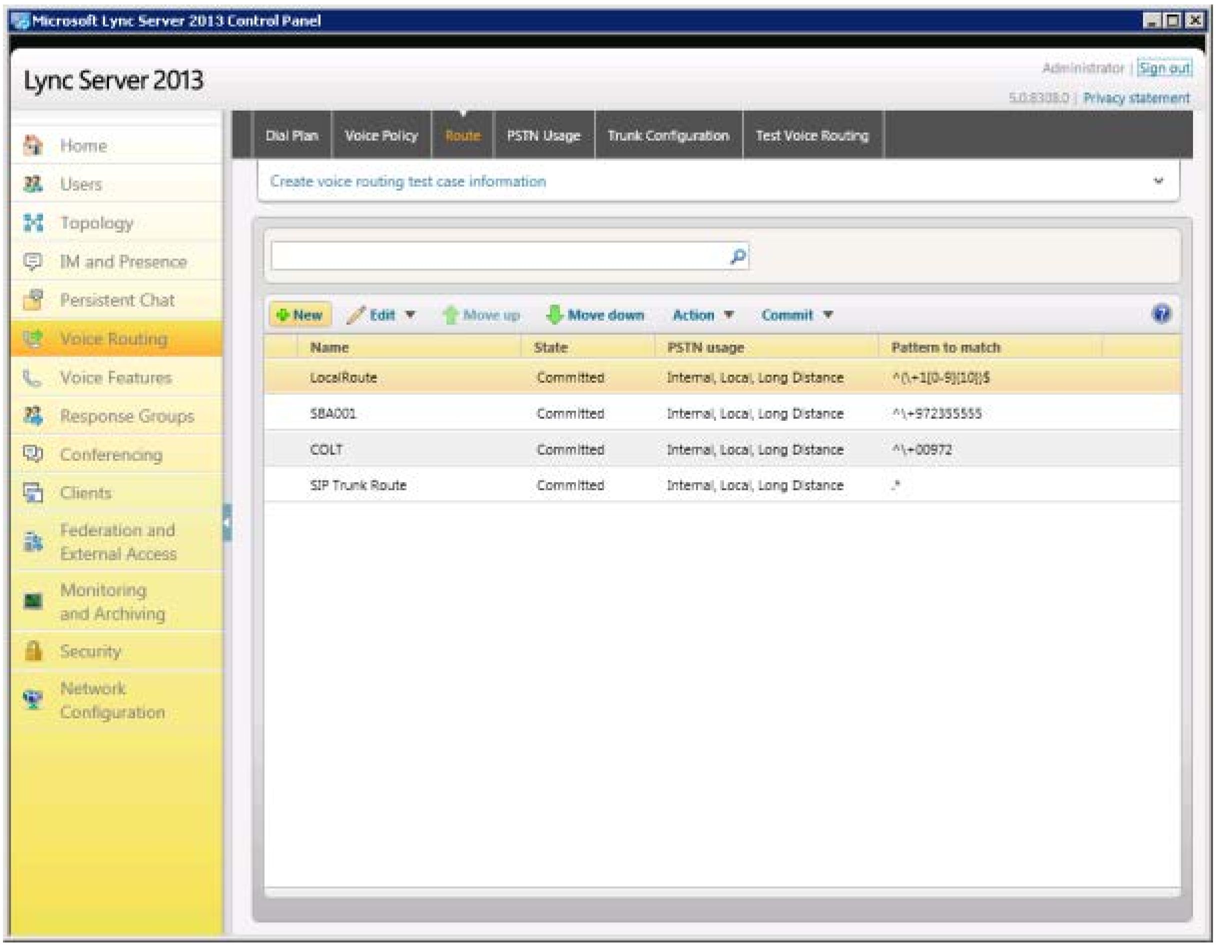
Microsoft Lync Server 2013 Control Panel

Successfully published voice routing configuration.

Name	State	PSTN usage	Pattern to match
LocalRoute	Committed	Internal, Local, Long Distance	^(\+1[0-9]{10})$
SBA001			^\+972355535
COLT			^\+00972
SIP Trun			.*

14. Click **Close**; the new committed Route is displayed in the Voice Routing screen, 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 Configure 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 Colt SIP Trunk:

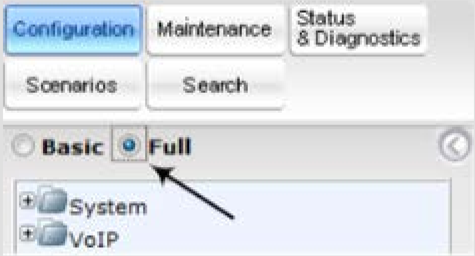
- E-SBC WAN interface: Colt SIP Trunking environment
- E-SBC LAN interface: Lync Server 2013 environment

This configuration is done using the E-SBC's Web-based management tool (embedded Web server).

Notes:

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

  For more information about the Software Feature key, contact your AudioCodes 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 Technical Note* 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 displayed below:



When the E-SBC is reset, the Web GUI reverts to Basic-menu display.

4.1 Step 1: Configure Network Interfaces

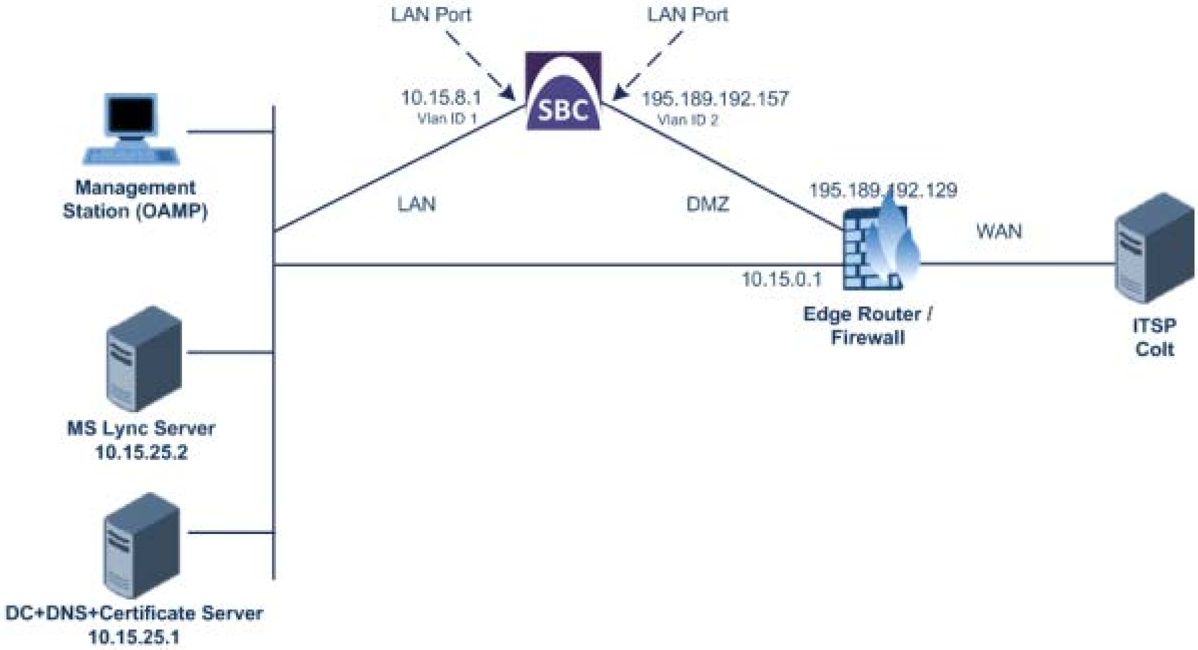
This step describes how to configure the E-SBC's network interfaces. There are several ways to deploy the E-SBC. However, the example scenario in this document uses the following deployment method:

- The E-SBC interfaces are between the Lync servers located on the LAN and the Colt SIP Trunk located on the WAN.
- The E-SBC connects to the WAN through a DMZ network.

The type of physical LAN connection depends on the method used to connect to the enterprise's network. In this example, E-SBC connects to the LAN and WAN using dedicated LAN ports, i.e., two ports and network cables.

In addition, the E-SBC uses two logical network interfaces; one to the LAN (VLAN ID 1) and one to the WAN (VLAN ID 2).

Figure 4-1: Network Interfaces



4.1.1 Step 1a: Configure IP Network Interfaces

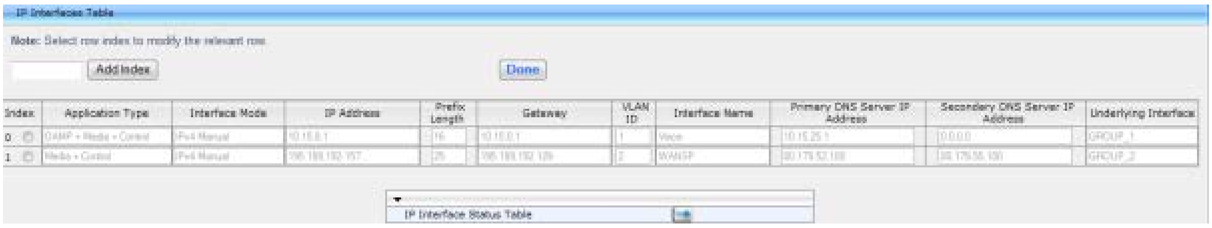
The procedure below describes how to configure the IP network interfaces for each of the following interfaces:

- LAN VoIP ("Voice")
- WAN VoIP ("WANSP")

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

1. Open the Multiple Interface Table page (**Configuration** tab > **Network Settings** > **IP Settings**).

Figure 4-2: Multiple Interface Table



IP Interfaces Table

Note: Select row index to modify the relevant row

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0 ○	OAMP + Media + Control	IPv4 Manual	10.15.8.1	16	10.15.0.1	1	Voice	10.15.25.1	0.0.0.0	GROUP_1
1 ○	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	2	WANSP	80.179.52.100	80.179.55.100	GROUP_2

2. Modify the existing LAN network interface:

   a. Select the 'Index' radio button corresponding to the Application Type, "OAMP + Media + Control", and then click **Edit**.

   a. Set the interface as follows:

Parameter	Example Setting
IP Address	**10.15.8.1** E-SBC IP address
Prefix Length	**16** for 255.255.0.0 Subnet mask in bits
Gateway	**10.15.0.1** Default Gateway
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 another network interface for the WAN side:

   a. Enter "1", and then click **Add Index**.

   b. Set the interface as follows:

Parameter	Settings
Application Type	**Media + Control**
IP Address	**195.189.192.157**
Prefix Length	**25** for 255.255.255.128
Gateway	**195.189.192.129** Default Gateway - router's IP address

Parameter	Settings
VLAN ID	**2**
Interface Name	**WANSP** Arbitrary descriptive name for the WAN interface
Primary DNS Server IP Address	**80.179.52.100**
Secondary DNS Server IP Address	**80.179.55.100**
Underlying Interface	**GROUP_2** Ethernet port group

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

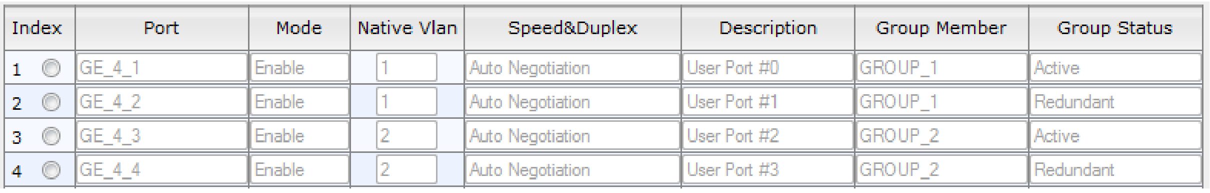
4.1.2 Step 1b: Configure the Native VLAN ID

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

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

1. Open the Physical Ports Settings page (**Configuration** tab> **VoIP** > **Network** > **Physical Ports Settings**).
2. In the **GROUP_1** member ports, set the 'Native Vlan' field to "1". This VLAN was assigned to network interface "Voice".
3. In the **GROUP_2** member ports, set the 'Native Vlan' field to "2". This VLAN was assigned to network interface "WANSP".

Figure 4-3: Ports 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

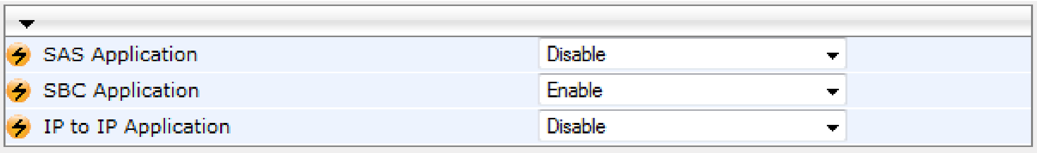
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-4: Applications Enabling



SAS Application	Disable
SBC Application	Enable
IP to IP Application	Disable

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.14 on page 63).

4.3 Step 3: Configure SRDs

This step describes how to configure Signaling Routing Domains (SRD). An SRD is a set of definitions comprising IP interfaces, E-SBC resources, SIP behaviors, and Media Realms.

4.3.1 Step 3a: Add Media Realms

A Media Realm represents a set of ports, associated with an IP interface, which are used by the E-SBC to transmit or receive media (RTP or SRTP). Media Realms are associated with SRDs or IP Groups.

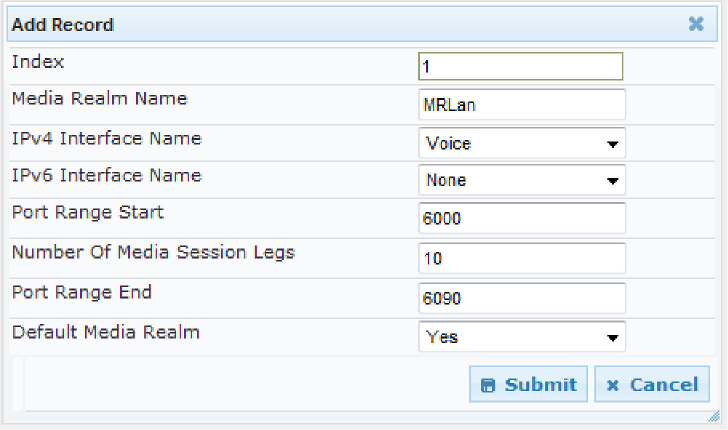
The simplest configuration is to create one Media Realm for internal (LAN) traffic and another for external (WAN) traffic, which is described in the procedure below for our example scenario.

➢ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** > **Media** > **Media Realm Configuration**).
2. Add a Media Realm for the LAN traffic:
   a. Click **Add**.
   b. Configure the Media Realm as follows:

Parameter	Example Setting
Index	**1**
Media Realm Name	**MRLan** An arbitrary name
IPv4 Interface Name	**Voice**
Port Range Start	**6000** Number representing the lowest UDP port number to be used for media on the LAN
Number of Media Session Legs	**10** The number of media sessions assigned with the port range

Figure 4-5: LAN Media Realm Configuration



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

   c. Click **Submit**.

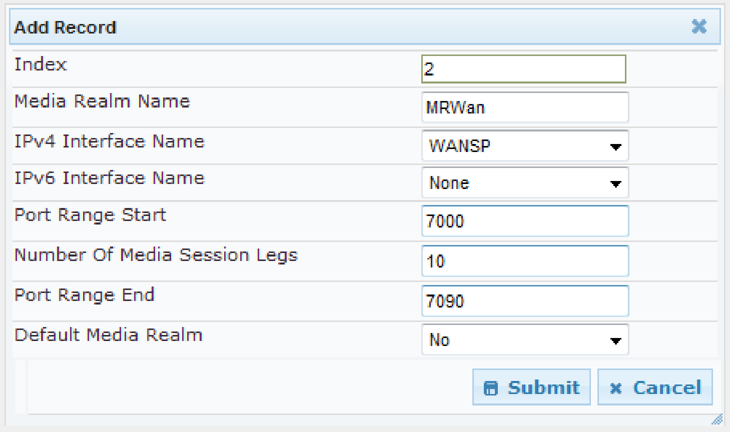
3. Add a Media Realm for the external traffic (WAN):

   a. Click **Add**.

   b. Configure the Media Realm as follows:

Parameter	Example Setting
Index	**2**
Media Realm Name	**MRWan** An arbitrary name
IPv4 Interface Name	**WANSP**
Port Range Start	**7000** Number representing the lowest UDP port number to be used for media on the WAN
Number of Media Session Legs	**10** The number of media sessions assigned with the port range

Figure 4-6: WAN Media Realm Configuration



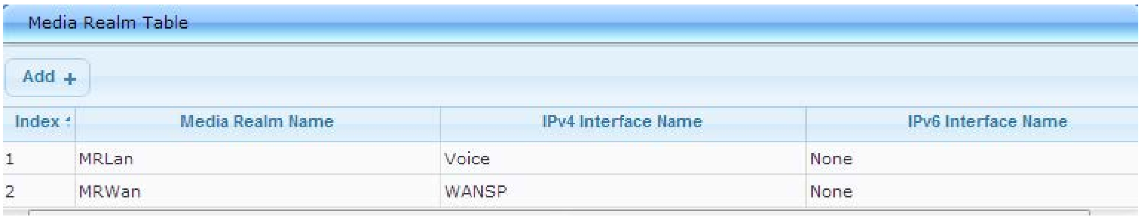
Add Record

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

   c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-7: Required Media Realm Table



Media Realm Table

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

4.3.2 Step 3b: Add SRDs

The procedure below describes how to add SRDs.

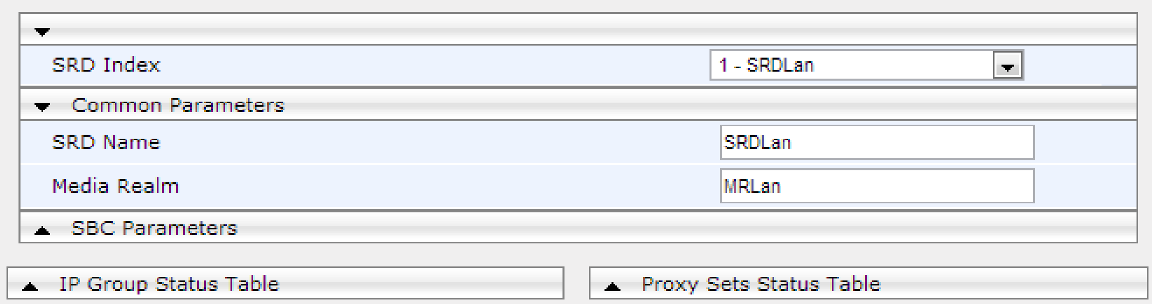
➢ **To add SRDs:**

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

   a. Configure the following parameters:

Parameter	Example Setting
SRD Index	**1**
SRD Name	**SRDLan** Descriptive name for the SRD
Media Realm	**MRLan** Associates the SRD with a Media Realm

Figure 4-8: LAN SRD Configuration



SRD Index: 1 - SRDLan

Common Parameters

SRD Name: SRDLan

Media Realm: MRLan

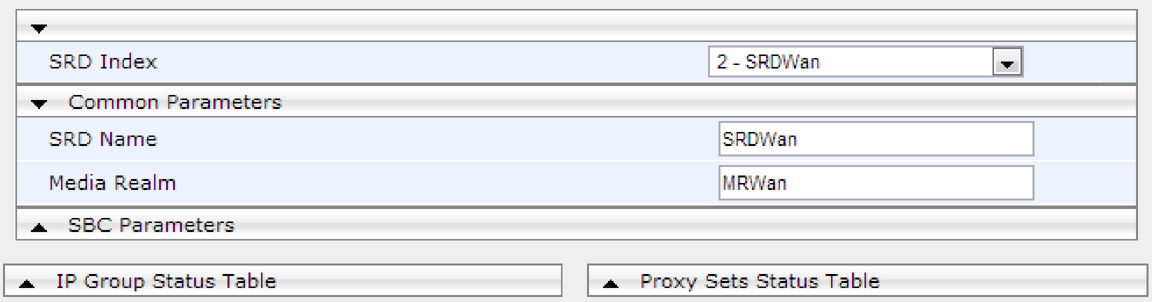
   b. Click **Submit**.

3. Add an SRD for the E-SBC’s external interface (toward the Colt SIP Trunk):

   a. Configure the following parameters:

Parameter	Example Setting
SRD Index	**2**
SRD Name	**SRDWan** Descriptive name for the SRD
Media Realm	**MRWan** Associates the SRD with a Media Realm

Figure 4-9: WAN SRD Configuration



SRD Index: 2 - SRDWan

Common Parameters

SRD Name: SRDWan

Media Realm: MRWan

   b. Click **Submit**.

4.3.3 Step 3c: Add SIP Signaling Interfaces

A SIP Interface consists of a combination of ports (UDP, TCP, and TLS) associated with a specific IP network interface. The SIP Interface is associated with an SRD.

This step describes how to add SIP interfaces. In the example scenario, you must add an internal and external SIP interface for the E-SBC.

➢ **To add SIP interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** > **Control Network** > **SIP Interface Table**).
2. Add a SIP interface for the LAN:
   a. Click **Add**.
   b. Configure the following parameters:

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

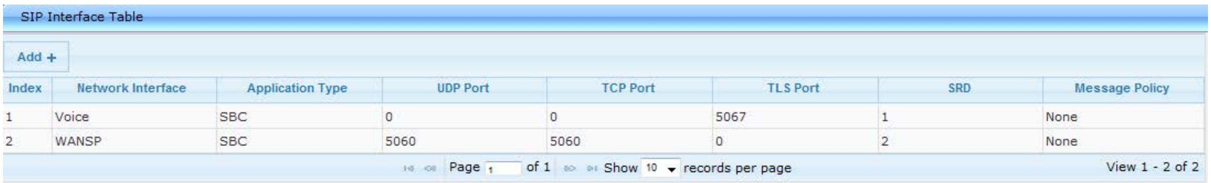
   c. Click **Submit**.
3. Add a SIP interface for the WAN:
   a. Click **Add**.
   b. Configure the following parameters:

Parameter	Example Setting
Index	**2**
Network Interface	**WANSP**
Application Type	**SBC**
UDP Port	**5060**
TCP Port	**5060**
TLS Port	**0**
SRD	**2**

   c. Click **Submit**.

The configured SIP Interface table is shown below:

Figure 4-10: Required SIP Interface Table



SIP Interface Table

Add +

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	5060	0	2	None

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

4.4 Step 4: Configure Proxy Sets

This step describes how to configure the Proxy Sets. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). In the example scenario, you need to configure two Proxy Sets for the following entities:

- Microsoft Lync Server 2013
- Colt SIP Trunk

These Proxy Sets will later be associated with IP Groups.

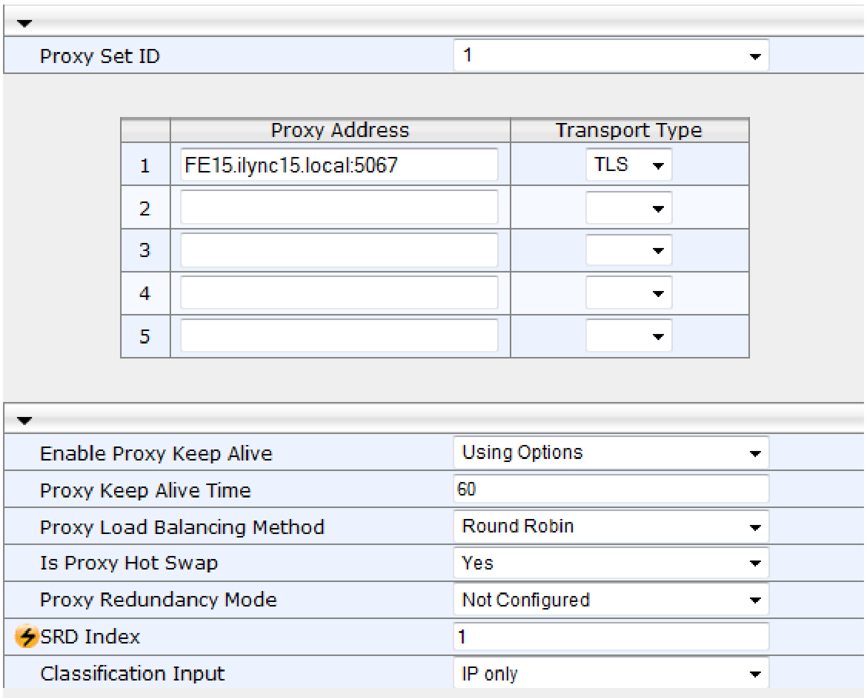
➢ **To add Proxy Sets:**

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

   a. Configure the following parameters:

Parameter	Example Setting
Proxy Set ID	**1**
Proxy Address	**FE15.ilync15.local:5067** Lync Server 2013 SIP Trunking IP address or 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: 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		

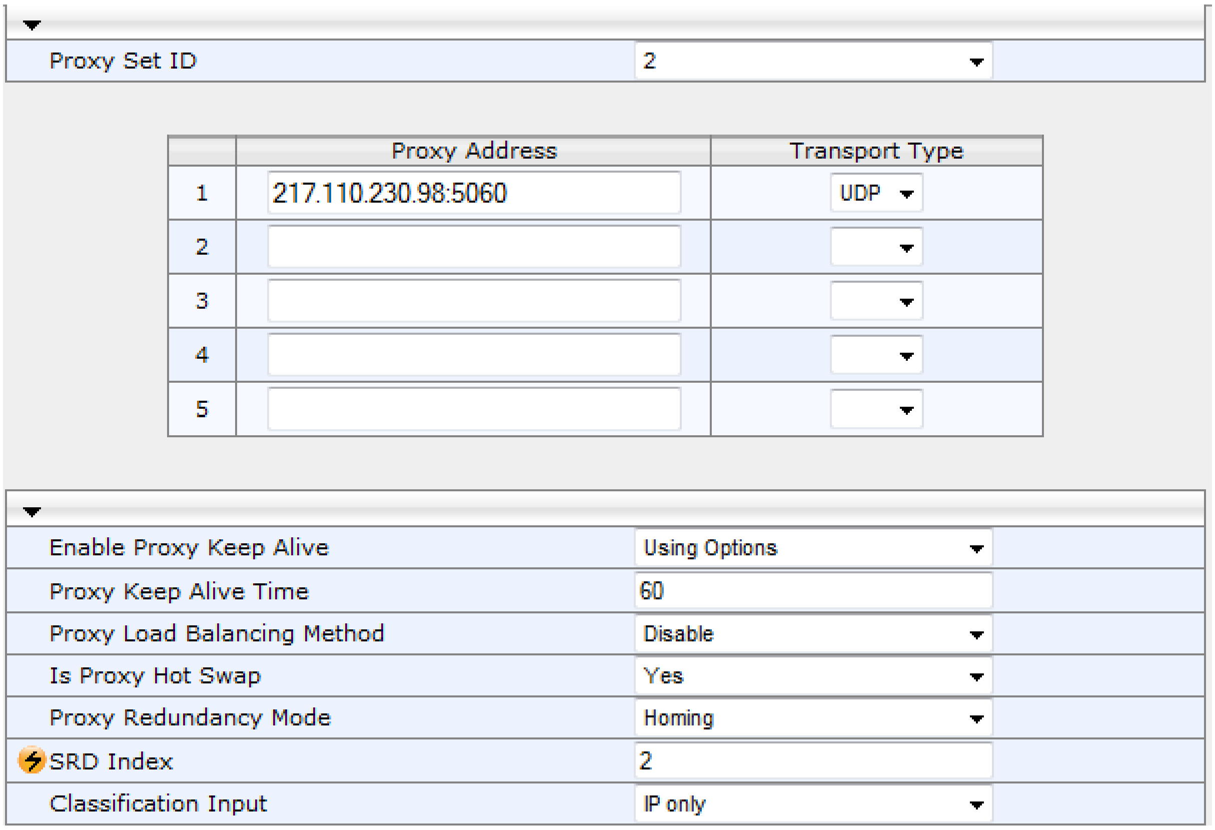
Enable Proxy Keep Alive: Using Options
Proxy Keep Alive Time: 60
Proxy Load Balancing Method: Round Robin
Is Proxy Hot Swap: Yes
Proxy Redundancy Mode: Not Configured
SRD Index: 1
Classification Input: IP only

   b. Click **Submit**.

3. Add a Proxy Set for the Colt SIP Trunk:

Parameter	Example Setting
Proxy Set ID	**2**
Proxy Address	**217.110.230.98:5060** Colt IP address or FQDN and destination port
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
Is Proxy Hot Swap	**Yes**
Proxy Redundancy Mode	**Homing**
SRD Index	**2** Enables classification by Proxy Set for this SRD in the IP Group belonging to the Colt SIP Trunk

Figure 4-12: Proxy Set for Colt SIP Trunk



Proxy Set ID	2

	Proxy Address	Transport Type
1	217.110.230.98:5060	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	Homing
SRD Index	2
Classification Input	IP only

4. Click **Submit**.

4.5 Step 5: Configure IP Groups

This step describes how to create IP Groups. An IP Group represents a SIP entity behavior in the E-SBC's network. In the example scenario, you need to create IP Groups for the following entities:

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

These IP Groups are later used by the SBC application for routing calls.

➢ To configure IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group for the Lync Server 2013 Mediation Server:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Example Setting
Index	**1**
Type	**Server**
Description	**Lync Server**
Proxy Set ID	**1**
SIP Group Name	**FE15.iLync15.Local**
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

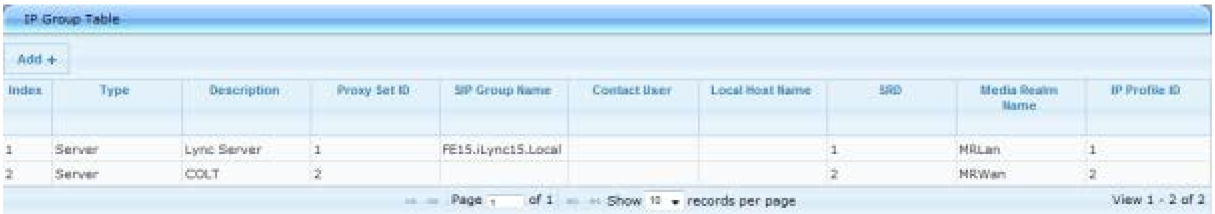
   c. Click **Submit**.
3. Add an IP Group for the Colt SIP Trunk:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Example Setting
Index	**2**
Type	**Server**
Description	**Colt** Descriptive name
Proxy Set ID	**2**
SRD	**2**
Media Realm Name	**MRWan**
IP Profile ID	**2**

   c. Click **Submit**.

The configured IP Group table is shown below:

Figure 4-13: Configured IP Group Table



IP Group Table

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	FE15.iLync15.Local			1	MRLan	1
2	Server	COLT	2				2	MRWan	2

4.6 Step 6: Configure IP Profiles

This step describes how to configure IP Profiles. In our example scenario, the IP Profiles are used to configure the SRTP / TLS modes and other parameters that differ between the two entities - Lync Server 2013 and Colt SIP Trunk. Note that the IP Profiles were assigned to the relevant IP Group in the previous step in the previous section.

In our example, you need to add an IP Profile for each entity:

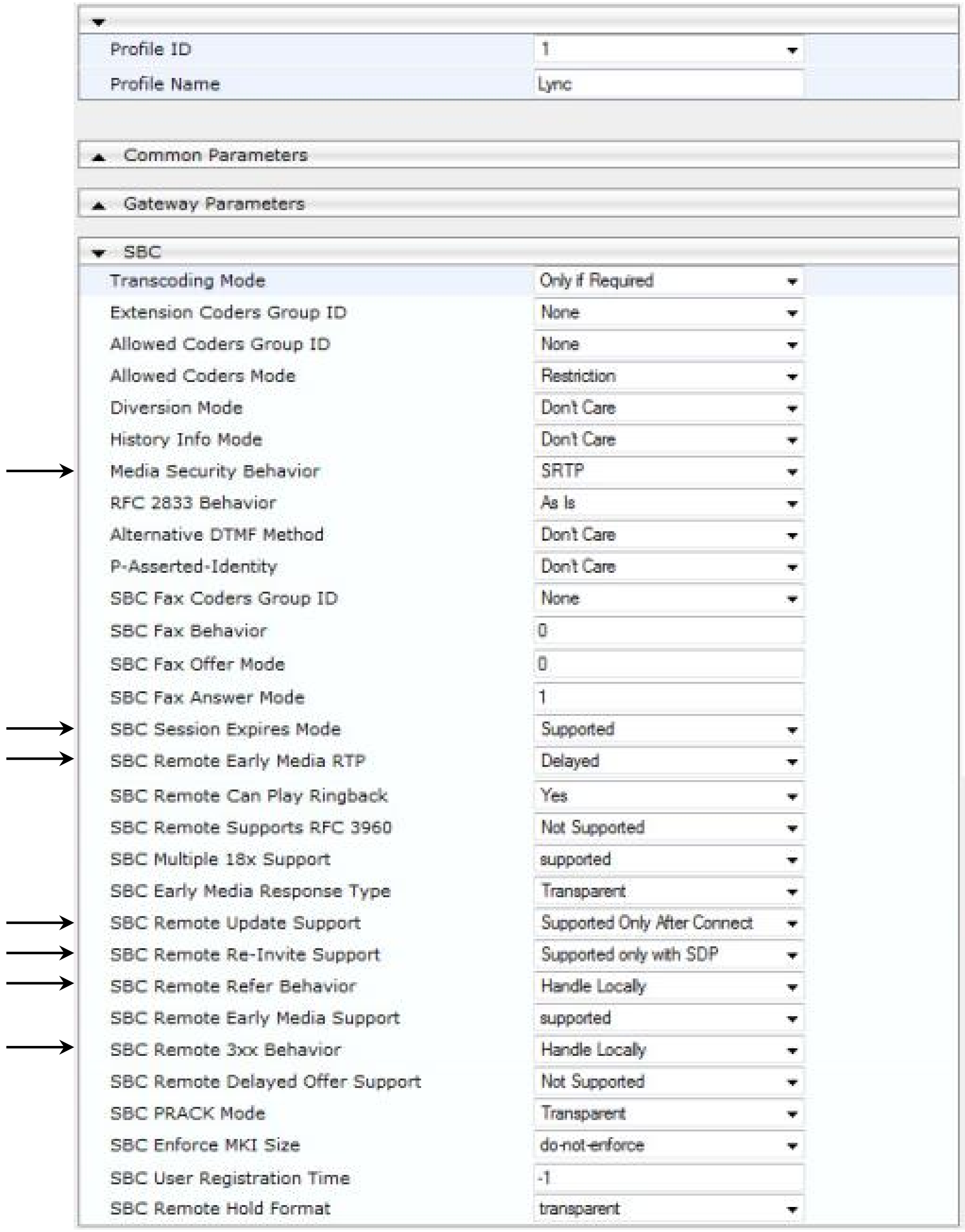
- Microsoft Lync Server 2013 - to operate in secure mode using SRTP and TLS
- Colt SIP trunk - to operate in non-secure mode using RTP and UDP

➢ **To add IP Profiles:**

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

Parameter	Example Setting
Profile ID	**1**
Media Security Behavior	**SRTP**
SBC Session Expires Mode	**Supported**
SBC Remote Early Media RTP	**Delayed** Required, as when the Lync Server 2013 sends a SIP 18x response, it does not immediately send the RTP to the remote side
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 messages (in the case of call transfer), the E-SBC handles the REFER locally and sends a re-INVITE to the Lync server
SBC Remote 3xx Behavior	**Handle Locally** Required Lync Server 2013 does not support receipt of SIP 3xx
SBC Remote Delayed Offer Support	**Not Supported**

Figure 4-14: IP Profile for Lync Server 2013



Profile ID	1
Profile Name	Lync

Transcoding Mode	Only if Required
Extension Coders Group ID	None
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	Supported
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	Handle Locally
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	transparent

b. Click **Submit**.

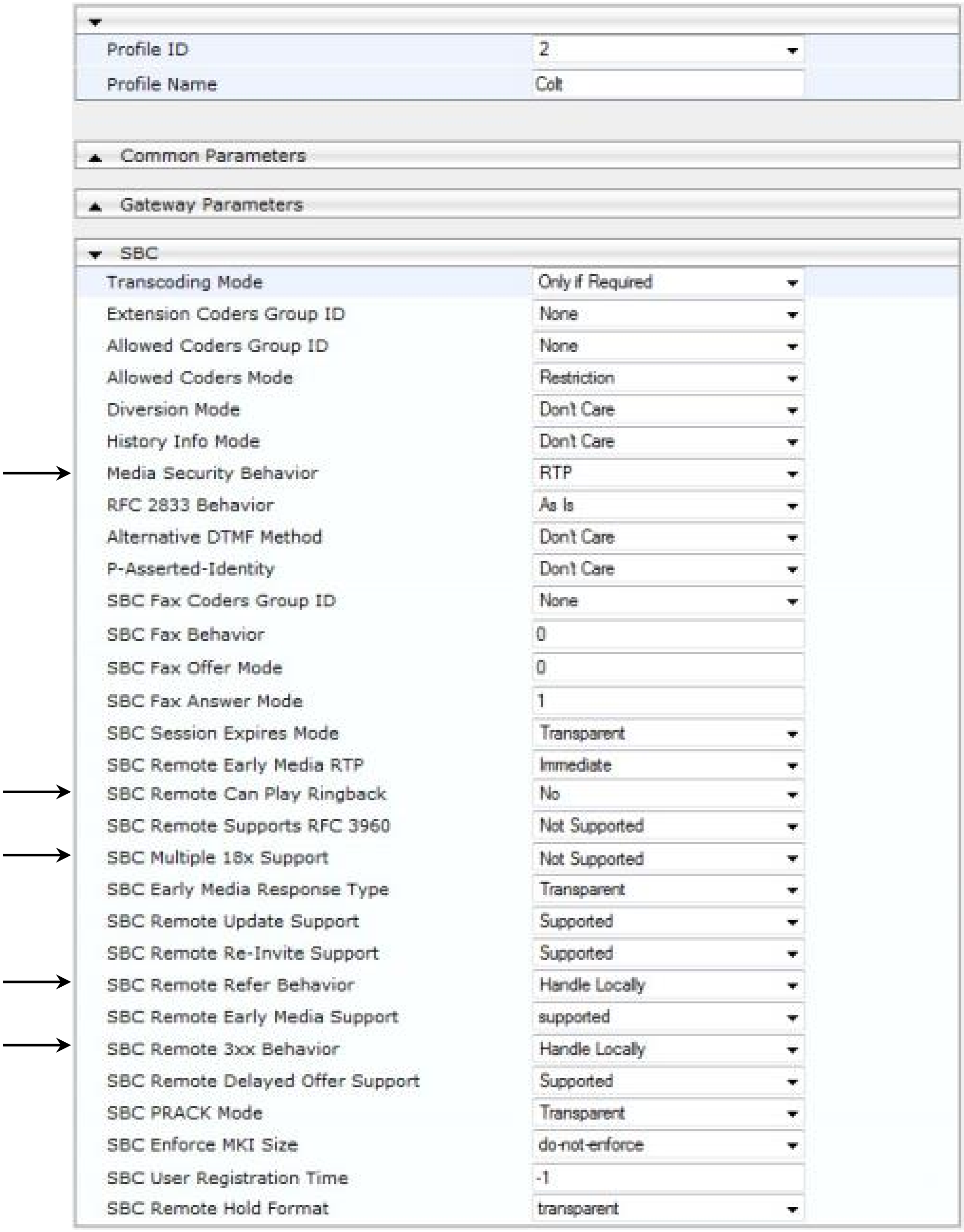
3. Add an IP Profile for the Colt SIP Trunk:

a. Configure the parameters as follows:

Parameter	Example Setting
Profile ID	**2**
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** If a SIP Trunk receives an 18x with SDP and

Parameter	Example Setting
	immediately after that, an 18x without SDP, it will play a local ringback, though in a Lync environment, there is a need to play a remote ringback
SBC Remote Refer Behavior	**Handle Locally** Required, SIP Trunk does not support receipt of REFER
SBC Remote 3xx Behavior	**Handle Locally** Required, as SIP Trunk does not support receipt of SIP 3xx

Figure 4-15: IP Profile for Colt SIP Trunk



Profile ID	2
Profile Name	Colt

Transcoding Mode	Only if Required
Extension Coders Group ID	None
Allowed Coders Group ID	None
Allowed Coders Mode	Restriction
Diversion Mode	Don't Care
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	Handle Locally
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

b. Click **Submit**.

4.7 Step 7: Configure a Secure SIP TLS Connection

This step 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.

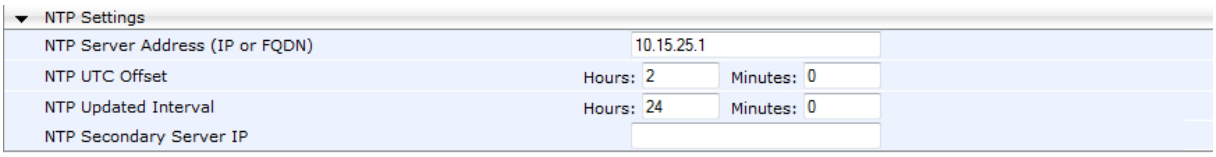
4.7.1 Step 7a: Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or third-party server) to ensure that the E-SBC receives 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 4-16: Configuring NTP Server Address



▾ NTP Settings

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

3. Click **Submit**.

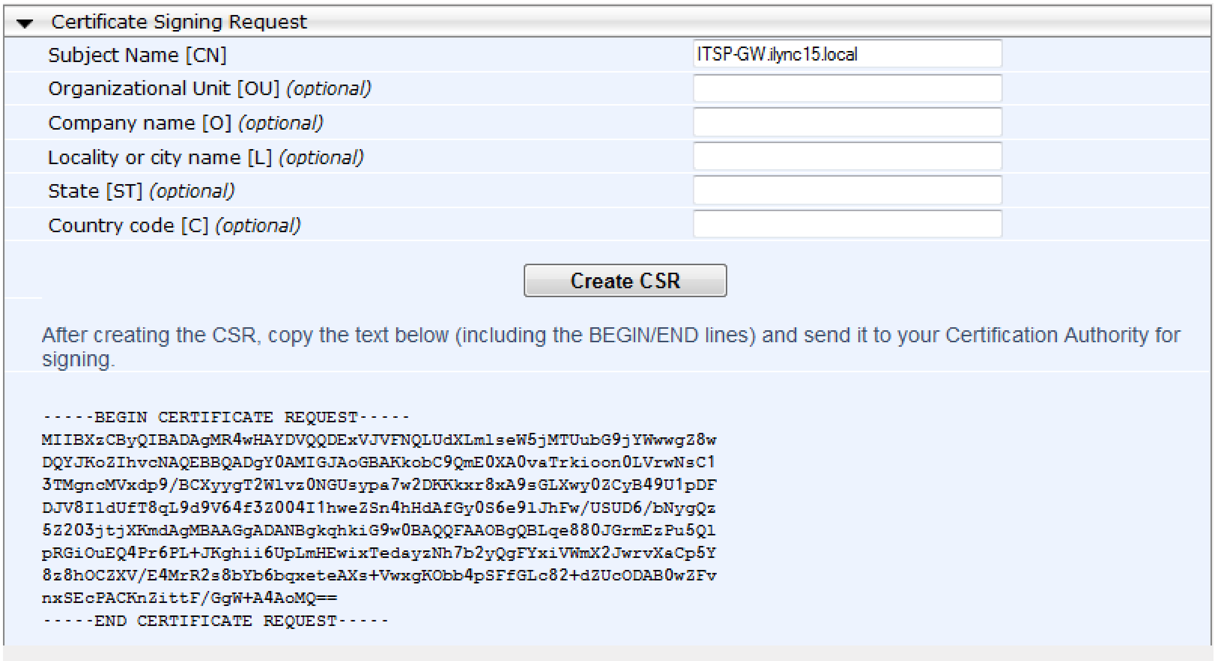
4.7.2 Step 7b: Configure a Certificate

This step describes how to exchange a certificate with the Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with the management station, i.e., the computer used to manage the E-SBC through its embedded Web server.

➢ **To configure a certificate:**

1. Open the Certificates page (**Configuration** tab > **System** > **Certificates**).

Figure 4-17: Certificates Page - Creating CSR



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)*	

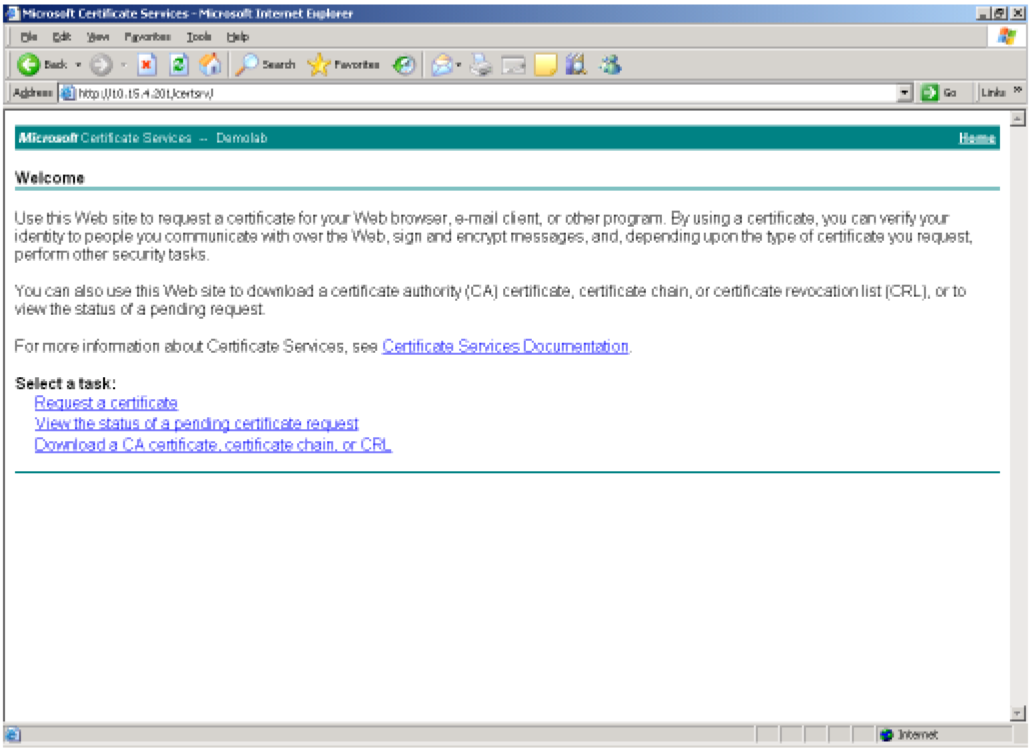
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBXzCByQIBADAgMR4wHAYDVQQDExVJVFNQLUdXLmlseW5jMTUubG9jYWwwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgncMVxdp9/BCXyygT2Wlvz0NGUsypa7w2DKKkxr8xA9sGLXwy0ZCyB49U1pDF
DJV8IldUfT8qL9d9V64f3Z004I1hweZSn4hHdAfGy0S6e91JhFw/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"). This name must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13).
3. Click **Create CSR**; a certificate request is generated.
4. Copy the CSR (from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----") to a text file (such as Notepad) and then save it to a folder on your computer with the file name *certreq.txt*.

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

Figure 4-18: Microsoft Certificate Services Web Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/
Go Links
Internet

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.

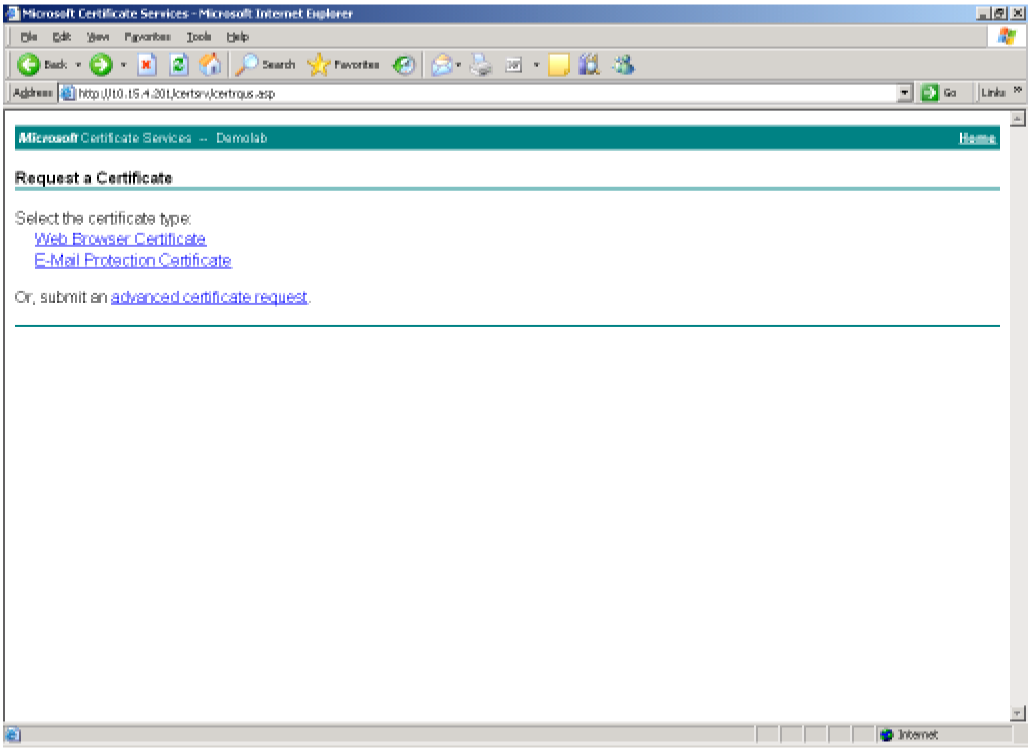
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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 4-19: Request a Certificate Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/certrqus.asp
Go Links
Internet

Microsoft Certificate Services -- Demolab Home

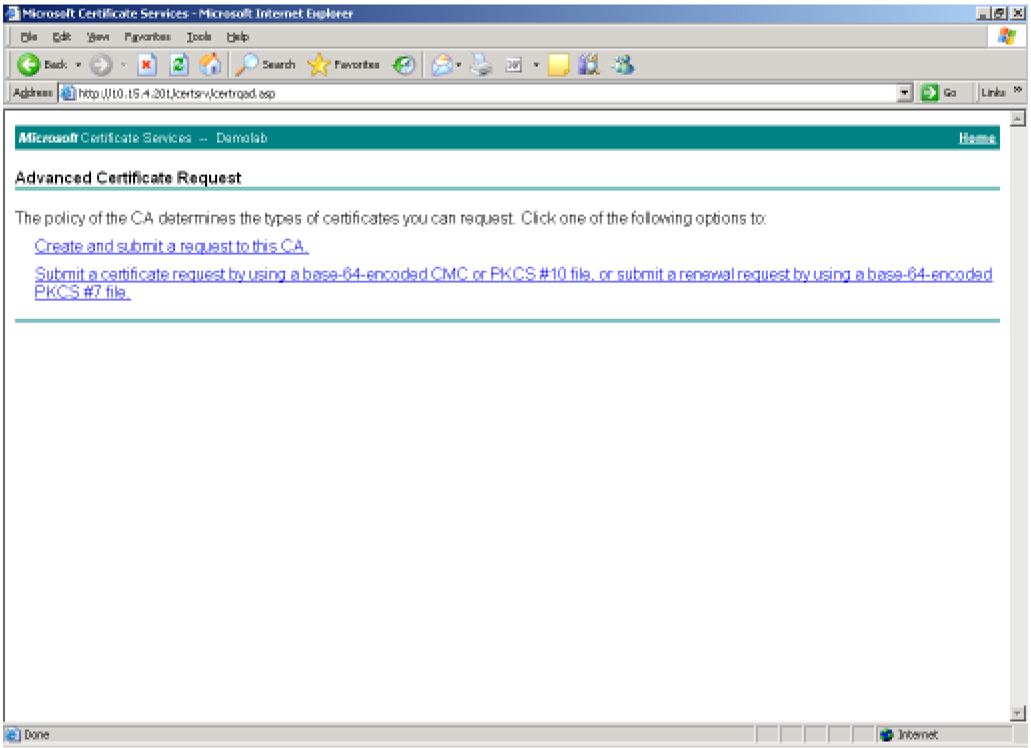
Request a Certificate

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 4-20: Advanced Certificate Request Page



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://10.15.4.201/certsrv/certrqad.asp
Go
Links
Done
Internet

Microsoft Certificate Services -- Demolab

Home

Advanced Certificate Request

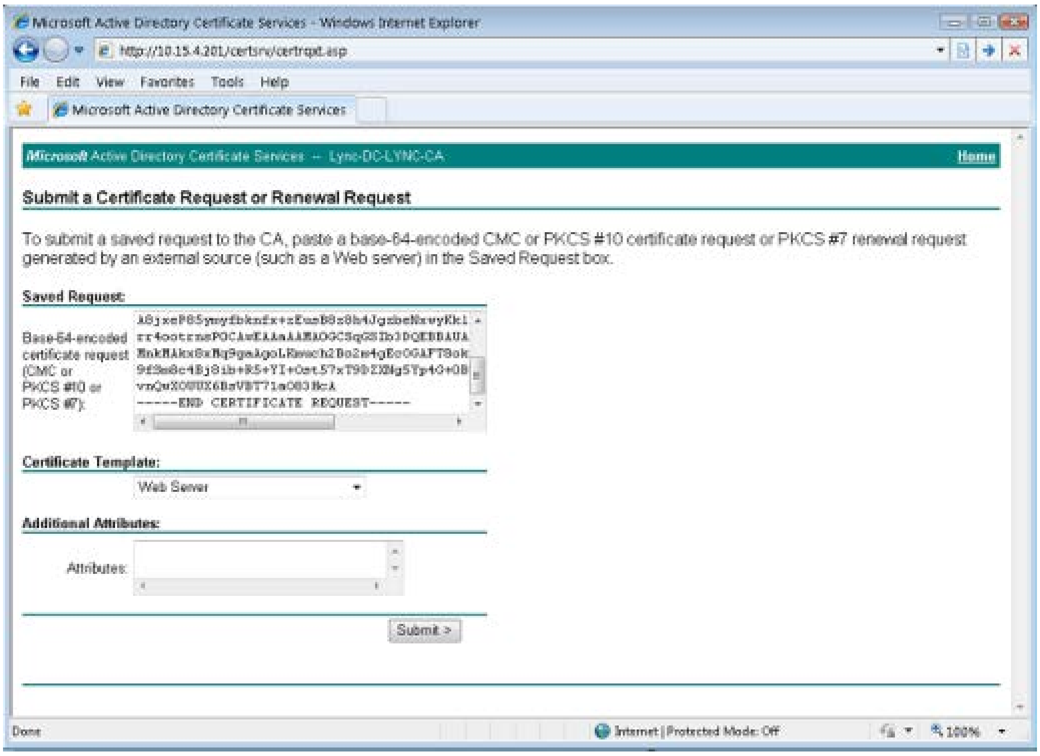
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

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 4-21: Submit a Certificate Request or Renewal Request Page



Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://10.15.4.201/certsrv/certrqxt.asp
File Edit View Favorites Tools Help
Microsoft Active Directory Certificate Services
Done
Internet | Protected Mode: Off
100%

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):

```
A8jxeP85ymyfbkndx+zEuzB8z8h4JgzbeNxvyKkl
rr4ootrnsPOCAwEAAaAAMAOGCSqGSIb3DQEBBAUA
MnkMAkx8xMq9gmAgoLKmuch2Bo2m4gEoOGAFT8ok
9f8m8c4Bj8ib+R5+YI+Oet57xT9DZXNg5Yp4O+OB
vnQuXOUUX6BsVBT71aO03HcA
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

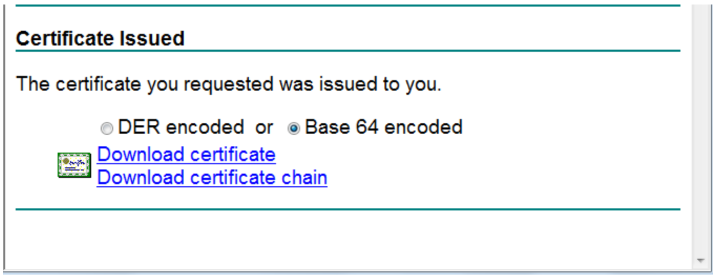
Additional Attributes:

Attributes:

Submit >

9. Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the ‘Base64 Encoded Certificate Request’ field.
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-22: Certificate Issued Page



Certificate Issued

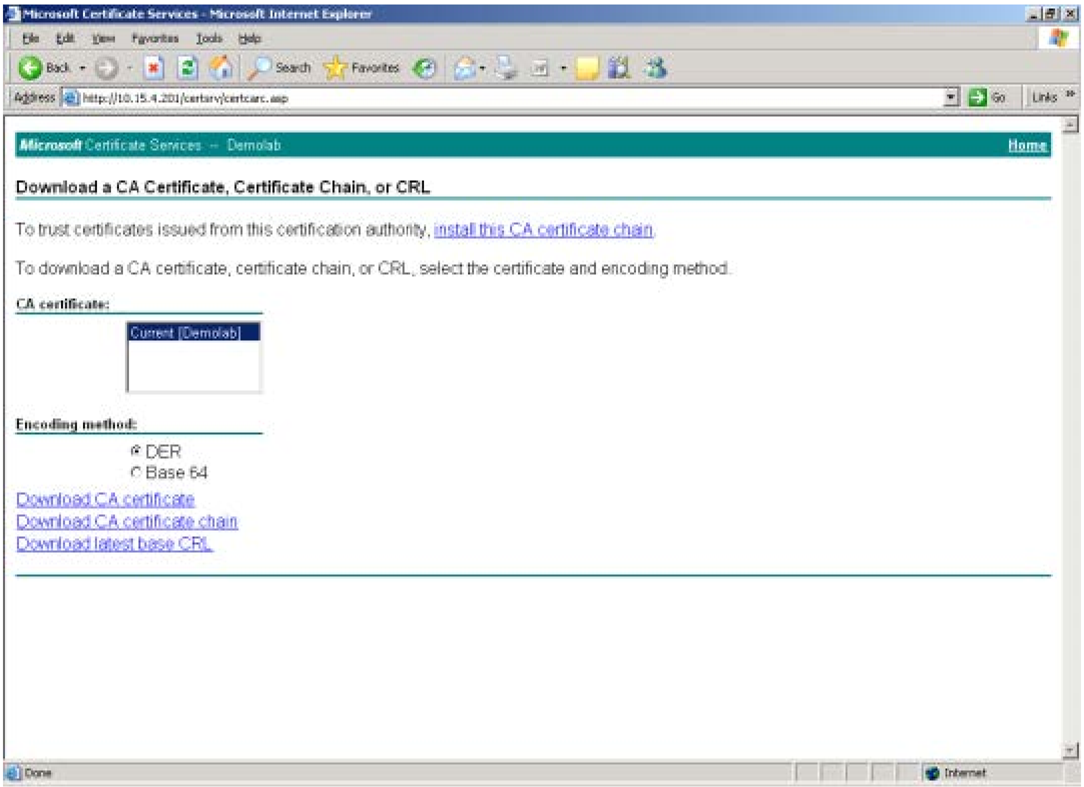
The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

12. Select the **Base 64 encoded** option for encoding, and then click **Download CA certificate**.
13. Save the file with the name *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 the **Download a CA certificate**, **certificate chain, or CRL**.

Figure 4-23: Download a CA Certificate, Certificate Chain, or CRL Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/certcarc.asp
Go Links
Done
Internet

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

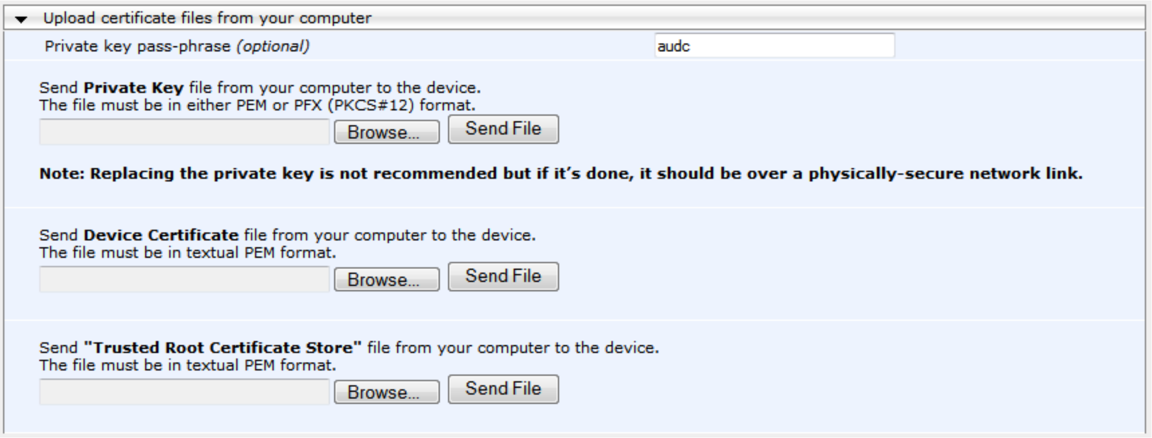
16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file with the name *certroot.cer* to a folder on your computer.

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 4-24: 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 4.14 on page 63).

4.8 Step 8: Configure SRTP

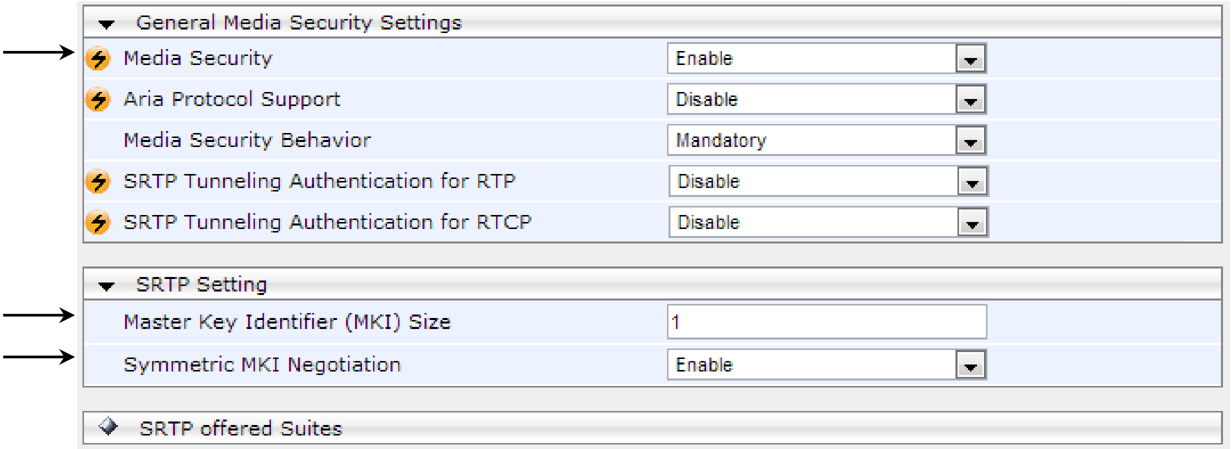
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), you need to configure the E-SBC to operate in the same manner.

Note that SRTP was enabled for Lync Server 2013 when you added an IP Profile for Lync Server 2013 (see Section 4.6 on page 42).

➢ To configure media security:

1. Open the Media Security page (**Configuration** tab > **Media** > **Media Security**).

Figure 4-25: Media Security Page



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

SRTP offered Suites

2. Configure the parameters as follows:

Parameter	Example Setting
Media Security	**Enable**
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 4.14 on page 63).

4.9 Step 9: Configure Maximum IP Media Channels

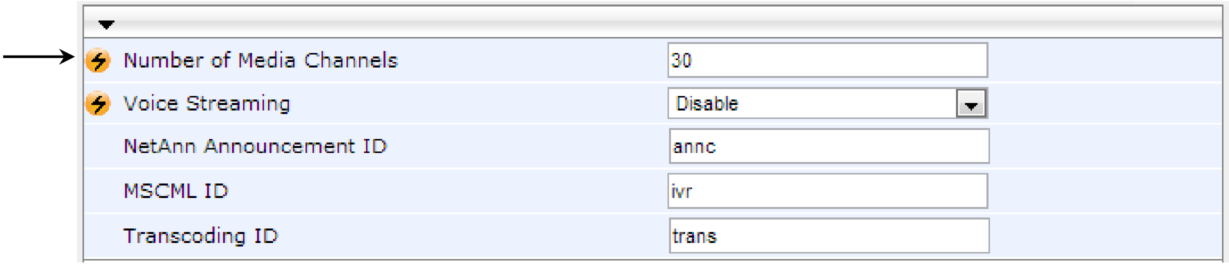
This step describes how to configure the number of media channels for IP-based media. To perform coder transcoding, define digital signaling processors (DSP) channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to sessions.

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

➢ **To configure IP media:**

1. Open the IP Media Settings page (**Configuration** tab > **VoIP** > **IP Media** > **IP Media Settings**).

Figure 4-26: Configuring Media Channels



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

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g.,"30").
3. Click **Submit**.

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

This step describes how to configure IP-to-IP call routing rules in the IP-to-IP Routing table. These rules define the route for forwarding SIP messages (e.g., INVITE) received on one IP interface to another.

The SIP message is routed according to a rule whose configured input characteristics (e.g., Source IP Group) match those of the message. If the characteristics of an incoming message do not match the first rule in the table, they are then compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

In the example scenario, you need to add the following IP-to-IP routing rules to route calls between Lync Server 2013 (LAN) and Colt SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from LAN to WAN
- Calls from WAN to LAN

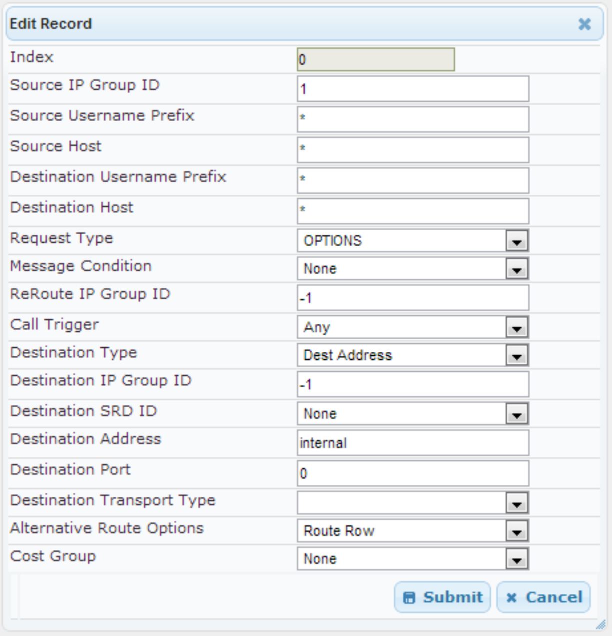
The routing rules use IP Groups to denote the source and destination of the call. As configured in Step 5 (see Section 4.5 on page 40), IP Group ID 1 was assigned to Lync Server 2013, and IP Group ID 2 to Colt SIP Trunk.

➢ To add IP-to-IP routing rules:

1. Open the IP2IP Routing Table page (**Configuration** > **VoIP** > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to terminate SIP OPTIONS messages received from the LAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

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

Figure 4-27: IP-to-IP Routing Rule for LAN to WAN

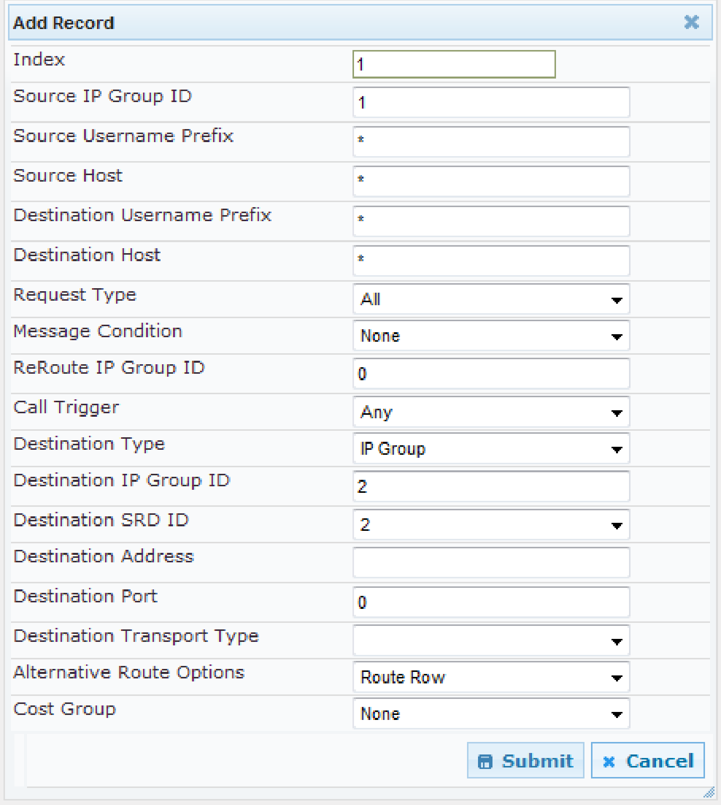


Index	0
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Destination Type	Dest Address
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	internal
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Cost Group	None

3. Add a rule to route calls from LAN to WAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

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

Figure 4-28: 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

c. Click **Submit**.

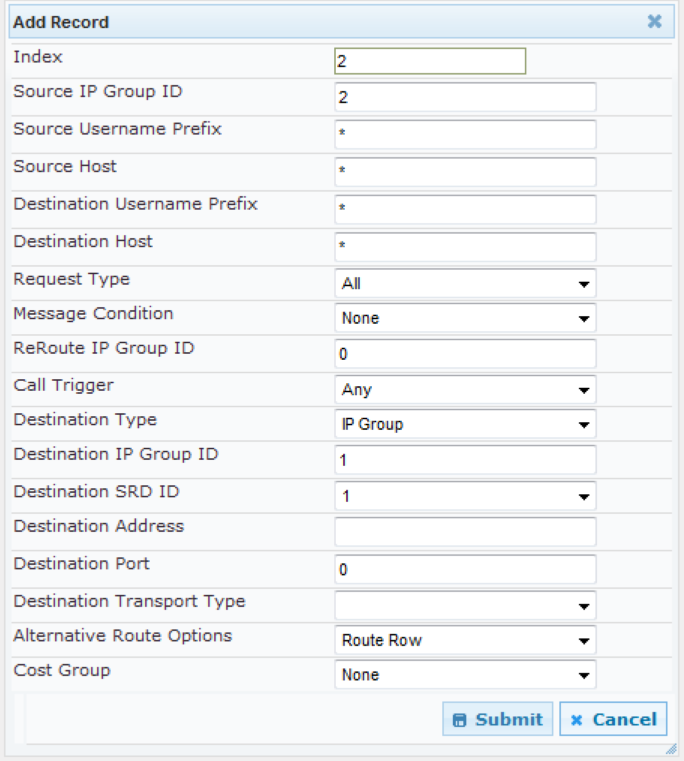
4. Add a rule to route calls from WAN to LAN:

   a. Click **Add**.

   b. Configure the parameters as follows:

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

Figure 4-29: IP-to-IP Routing Rule for WAN to LAN



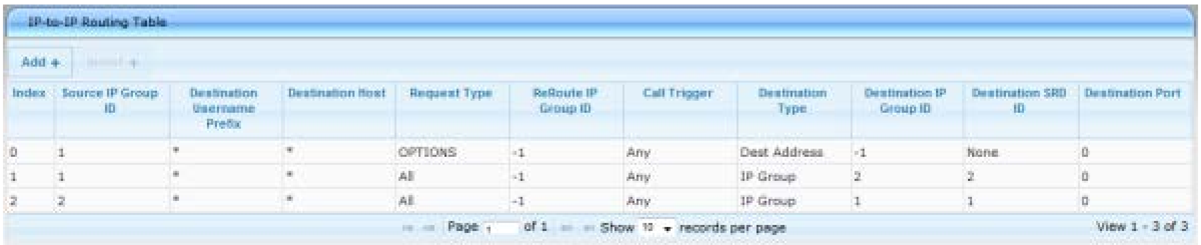
Add Record

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

   c. Click **Submit**.

The figure below shows the above configured routing rules in the IP-to-IP Routing Table:

Figure 4-30: 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

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

Note: The routing configuration may change according to the local deployment topology.

4.11 Step 11: Configure IP-to-IP Manipulation

This step describes how to configure IP-to-IP manipulation rules. These rules concern number manipulation of the source and / or destination number. The manipulation rules use IP Groups to denote the source and destination of the call. As configured in Step 5, IP Group ID 1 was assigned to Lync Server 2013 and IP Group ID 2 to the Colt SIP Trunk.

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

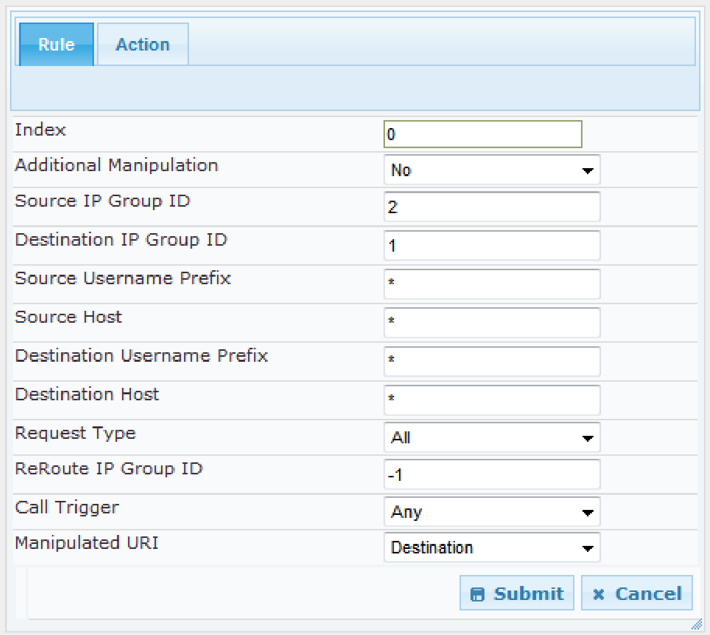
The procedure below provides an example of configuring a manipulation rule that adds the plus sign "+" to the destination number for calls from IP Group 2 (Colt SIP Trunk) destined to IP Group 1 (i.e., Lync Server 2013), when the destination number prefix is any number ("*").

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

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

Parameter	Example Setting
Index	**0**
Source IP Group	**2**
Destination IP Group	**1**
Destination Username Prefix	*****
Manipulated URI	**Destination**

Figure 4-31: IP-to-IP Outbound Manipulation Rule – Rule Tab

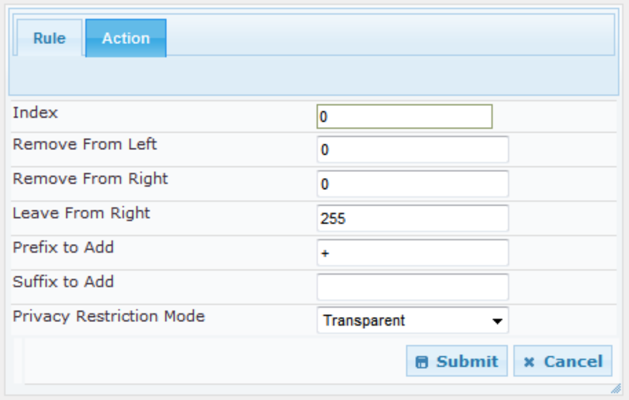


Index	0
Additional Manipulation	No
Source IP Group ID	2
Destination IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
ReRoute IP Group ID	-1
Call Trigger	Any
Manipulated URI	Destination

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

Parameter	Example Setting
Prefix to Add	**+**

Figure 4-32: IP-to-IP Outbound Manipulation Rule - Action Tab

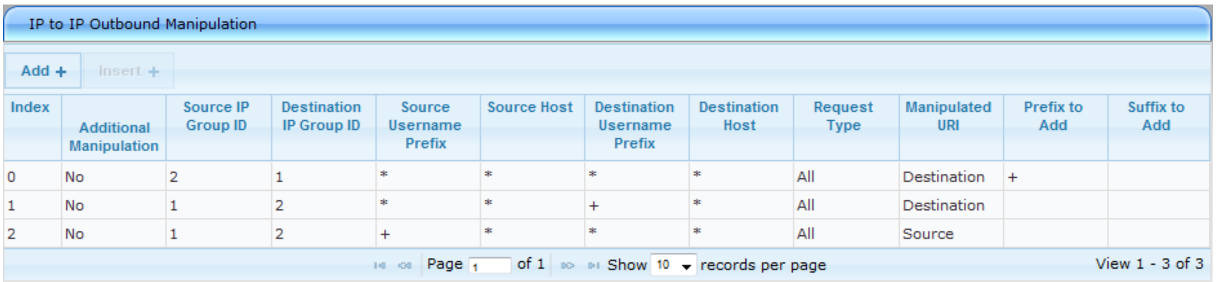


Index	0
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	
Privacy Restriction Mode	Transparent

5. Click **Submit**.

The IP to IP Outbound Manipulation table below includes manipulation rules for calls between IP Group 1 (i.e., Lync Server 2013) and IP Group 2 (i.e., Colt SIP Trunk):

Figure 4-33: IP to IP Outbound Manipulation Table - Example



IP to IP Outbound Manipulation

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		

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

- **Index 0:** Calls received from IP Group 2 and destined to IP Group 1 that have any destination number (*), add "+" to the prefix of the destination number.
- **Index 1:** Calls received from IP Group 1 and destined to IP Group 2 that have a prefix destination number of "+", remove "+" from this prefix.
- **Index 2:** Calls received from IP Group 1 and destined to IP Group 2 with source number prefix of "+", remove the "+" from this prefix source number.

4.12 Step 12: Configure Message Manipulation Rules

This step describes how to configure SIP message manipulation rules (done in the Message Manipulations table). SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message. 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.

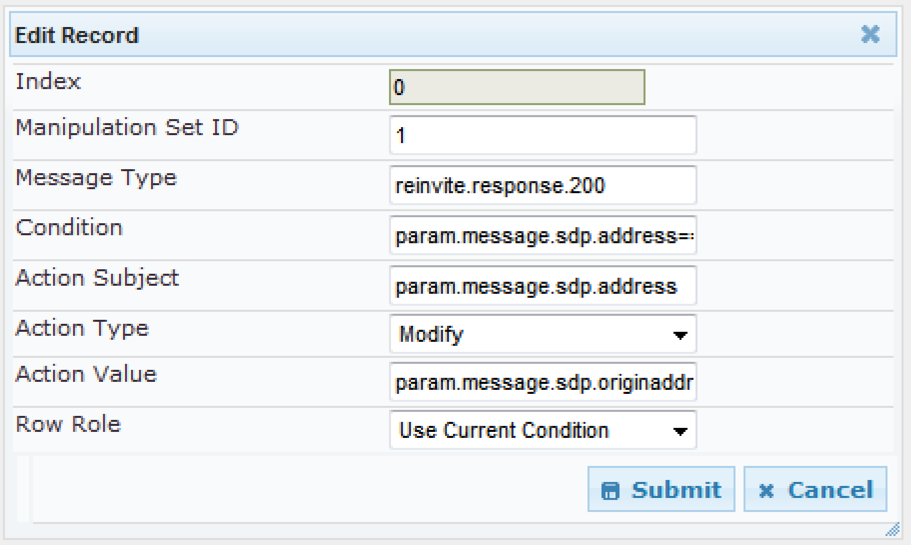
In the example scenario, a manipulation is configured for SIP 200OK response for re-INVITE that in the SDP the IP address is ’0.0.0.0’ (hold) the manipulation change the IP address to the SBC IP address.

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

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rule for Manipulation Set ID 0:

Rule Index	Setting
Index	**0**
Manipulation Set ID	**1**
Message Type	**reinvite.response.200**
Condition	**param.message.sdp.address=='0.0.0.0'**
Action Subject	**param.message.sdp.address**
Action Type	**Modify**
Action Value	**param.message.sdp.originaddress**

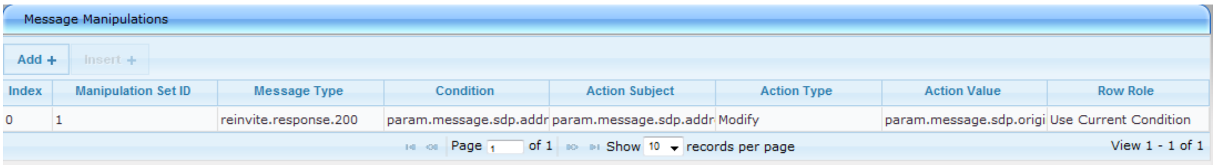
Figure 4-34: SIP Message Manipulation – Index 0



Edit Record

Index	0
Manipulation Set ID	1
Message Type	reinvite.response.200
Condition	param.message.sdp.address=:
Action Subject	param.message.sdp.address
Action Type	Modify
Action Value	param.message.sdp.originaddr
Row Role	Use Current Condition

Figure 4-35: SIP Message Manipulation – Example

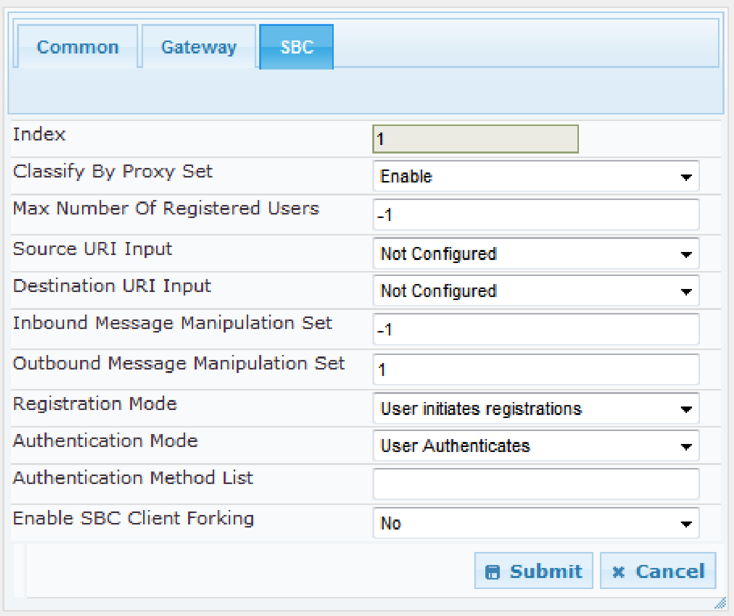


Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	1	reinvite.response.200	param.message.sdp.addr	param.message.sdp.addr	Modify	param.message.sdp.origi	Use Current Condition

SIP 200 OK responses that contain in its SDP the IP address 0.0.0.0 (hold), is changed to the IP address of the E-SBC.

3. Assign the Manipulation Set ID 1 to IP Group 1:
   a. Open the IP Group Table page (**Configuration** > **VoIP** > **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 ‘Outbound Message Manipulation Set’ field to "1".

Figure 4-36: Assigning Manipulation Rule 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	-1
Outbound Message Manipulation Set	1
Registration Mode	User initiates registrations
Authentication Mode	User Authenticates
Authentication Method List	
Enable SBC Client Forking	No

   e. Click **Submit**.

4.13 Step 13: Miscellaneous Configuration

This step describes miscellaneous E-SBC configuration.

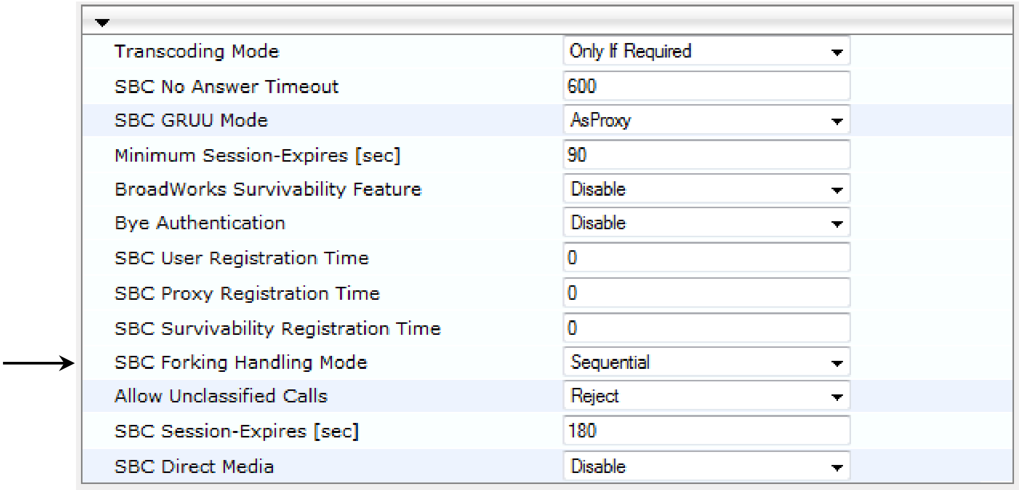
4.13.1 Step 13a: Configure Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received due to call forking of an INVITE. In the example scenario, if an 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC reopens the stream according to subsequently received 18x responses with SDP, or plays a ringback tone if a 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** > **SBC** > **General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.

Figure 4-37: 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**.

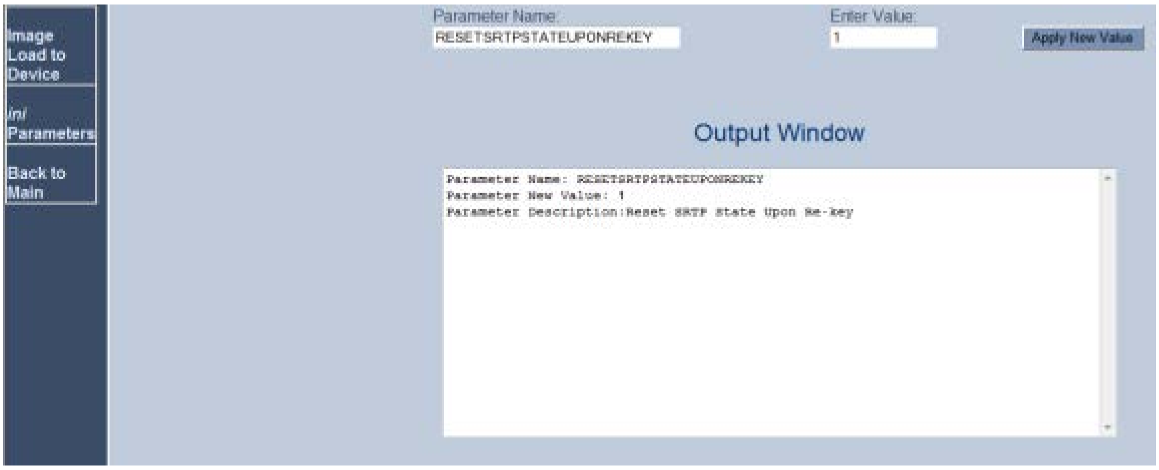
4.13.2 Step 13b: Configure SRTP Behavior upon Rekey Mode

This step describes how to configure SRTP upon re-key generation.

➢ **To configure SRTP upon re-key:**

1. Open the Admin page, by appending the suffix "AdminPage" (case-sensitive) to the device's IP address in the Web browser's URL field (e.g., http://10.15.45.101/AdminPage).
2. In the left pane, click ***ini* Parameters**.

Figure 4-38: AdminPage



Parameter Name: RESETSRTPSTATEUPONREKEY
Enter Value: 1

```
Parameter Name: RESETSRTPSTATEUPONREKEY
Parameter New Value: 1
Parameter Description:Reset SRTP State Upon Re-key
```

3. In the 'Parameter Name' and 'Enter Value' fields, enter the following values:

Parameter Name	Enter Value
RESETSRTPSTATEUPONREKEY	**1** Enables resetting SRTP State Upon Re-key

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

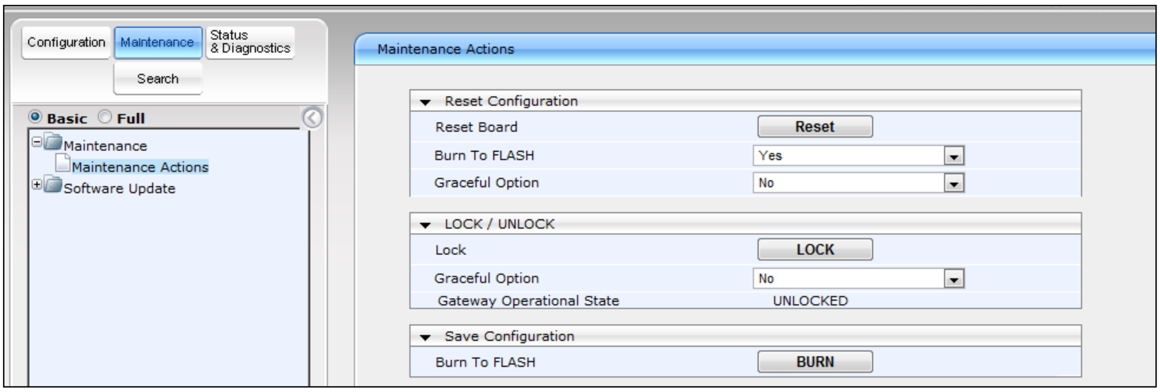
4.14 Step 14: Reset the E-SBC

After completing E-SBC configuration as described in the previous steps, 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 with a reset:**

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

Figure 4-39: 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.

Reader's Notes

A AudioCodes ini File

The *ini* file configuration of the E-SBC, corresponding to the configuration using the Web interface described above, is shown below:

```
;**************
;** Ini File **
;**************
;Board: Mediant 800
;Board Type: 69
;Serial Number: 3489490
;Slot Number: 1
;Software Version: 6.60A.216.006
;DSP Software Version: 5014AE3_R_LD => 660.22
;Board IP Address: 10.15.8.1
;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 ;Coders: G723 G729 G728
NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB
G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB
;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;E1Trunks=4 ;T1Trunks=4 ;FXSPorts=4
;FXOPorts=4 ;Channel Type: RTP DspCh=30 IPMediaDspCh=30 ;DSP Voice
features: ;Control Protocols: MSFT FEU=20 TestCall=120 MGCP SIP
SASurvivability SBC=120 ;Default features:;Coders: G711 G726;
;------ Mediant 800 HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
; 1 : FALC56 : 1
; 2 : FXS : 4
; 3 : Empty
;----------------------------------------------
[SYSTEM Params]
SyslogServerIP = 10.15.45.200
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
DebugRecordingDestIP = 10.15.2.8
;VpFileLastUpdateTime is hidden but has non-default value
DebugRecordingStatus = 1
NTPServerIP = '10.15.25.1'
LDAPSEARCHDNSINPARALLEL = 0
OAMPDEFAULTNETWORKSOURCE = 1
[BSP Params]
PCMLawSelect = 3
[Analog Params]
[ControlProtocols Params]
```

```
AdminStateLockControl = 0
[MGCP Params]
[MEGACO Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
[PSTN Params]
[SS7 Params]
[Voice Engine Params]
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
CallProgressTonesFilename = 'usa_tones_13.dat'
[WEB Params]
LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value
[SIP Params]
MEDIACHANNELS = 20
GWDEBUGLEVEL = 5
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLESYMMETRICMKI = 1
SBCFORKINGHANDLINGMODE = 1
RESETSRTPSTATEUPONREKEY = 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, 1, 4, "User Port #2",
"GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 1, 4, "User Port #3",
"GROUP_2", "Redundant";
PhysicalPortsTable 4 = "FE_5_1", 1, 1, 4, "User Port #4",
"GROUP_3", "Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 1, 4, "User Port #5",
"GROUP_3", "Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 1, 4, "User Port #6",
"GROUP_4", "Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 1, 4, "User Port #7",
"GROUP_4", "Redundant";
```

```
PhysicalPortsTable 8 = "FE_5_5", 1, 1, 4, "User Port #8",
"GROUP_5", "Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 1, 4, "User Port #9",
"GROUP_5", "Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 2, 4, "User Port #10",
"GROUP_6", "Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 2, 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, 10.15.8.1, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 195.189.192.157, 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 = "217.110.230.98", 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, 46, 40, 0, 0, 0, 0, 2, 0,
0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, -1,
0, 1, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 3, 1, 1,
0, 3, 2, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, -1, 0, 0, 1, 0, 0, 0;
IpProfile 2 = "Colt", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0,
0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, 1,
0, 2, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2,
1, 3, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 1, 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, 0, 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, "to Lync", 1, "FE15.iLync15.Local", "", 0, -1, -1,
0, -1, 1, "MRLan", 1, 1, -1, -1, 1, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "to COLT", 2, "", "", 0, -1, -1, 0, -1, 2, "MRWan",
1, 2, -1, 1, -1, 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, , "", 0,
-1, 0, ;
IP2IPRouting 2 = 2, "*", "*", "*", "*", 0, , -1, 0, 0, 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, 5060, 0, 2, , -1, 0, 500;
[ \SIPInterface ]
[ IPOutboundManipulation ]
```

```
FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix,
IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID,
IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight,
IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = 0, 2, 1, "*", "*", "*", "*", 0, -1, 0,
1, 0, 0, 255, "+", "", 0;
IPOutboundManipulation 1 = 0, 1, 2, "*", "*", "+", "*", 0, -1, 0,
1, 1, 0, 255, "", "", 0;
IPOutboundManipulation 2 = 0, 1, 2, "+", "*", "*", "*", 0, -1, 0,
0, 1, 0, 255, "", "", 0;
[ \IPOutboundManipulation ]
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0;
[ \CodersGroup0 ]
[ MessageManipulations ]
FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 0 = 1, "reinvite.response.200",
"param.message.sdp.address=='0.0.0.0'",
"param.message.sdp.address", 2, "param.message.sdp.originaddress",
0;
[ \MessageManipulations ]
[ RoutingRuleGroups ]
FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength,
RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;
[ \RoutingRuleGroups ]
[ LoggingFilters ]
FORMAT LoggingFilters_Index = LoggingFilters_FilterType,
LoggingFilters_Value, LoggingFilters_Syslog,
LoggingFilters_CaptureType;
LoggingFilters 0 = 1, "", 1, 2;
[ \LoggingFilters ]
[ 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 ]
```

Configuration Note

www.audiocodes.com