AudioCodes™ Mediant™ Series

Enterprise Session Border Controller (E-SBC)

Interoperability Laboratory

Configuration Note

Connecting Microsoft® Lync™ Server 2013 with HOT SIP Trunk using AudioCodes E-SBC

March 2013

Document #: LTRT-12215

Table of Contents

List of Figures

List of Tables

Notice

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

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

Date Published: March 6, 2013

Trademarks

WEEE EU Directive

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

Customer Support

Customer technical support and 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. Your valuable feedback is highly appreciated.

Reader's Notes

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between HOT'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 HOT Partners who are responsible for installing and configuring HOT'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

The table below describes the 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 (to the HOT SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 HOT SIP Trunking Version

The table below describes the HOT SIP Trunking Version.

Table 2-2: HOT Version

Vendor/Service Provider	HOT
SSW Model/Service	GenBand (Nortel)
Software Version	10.0.B
Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Server 2013 Version

The table below describes the 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

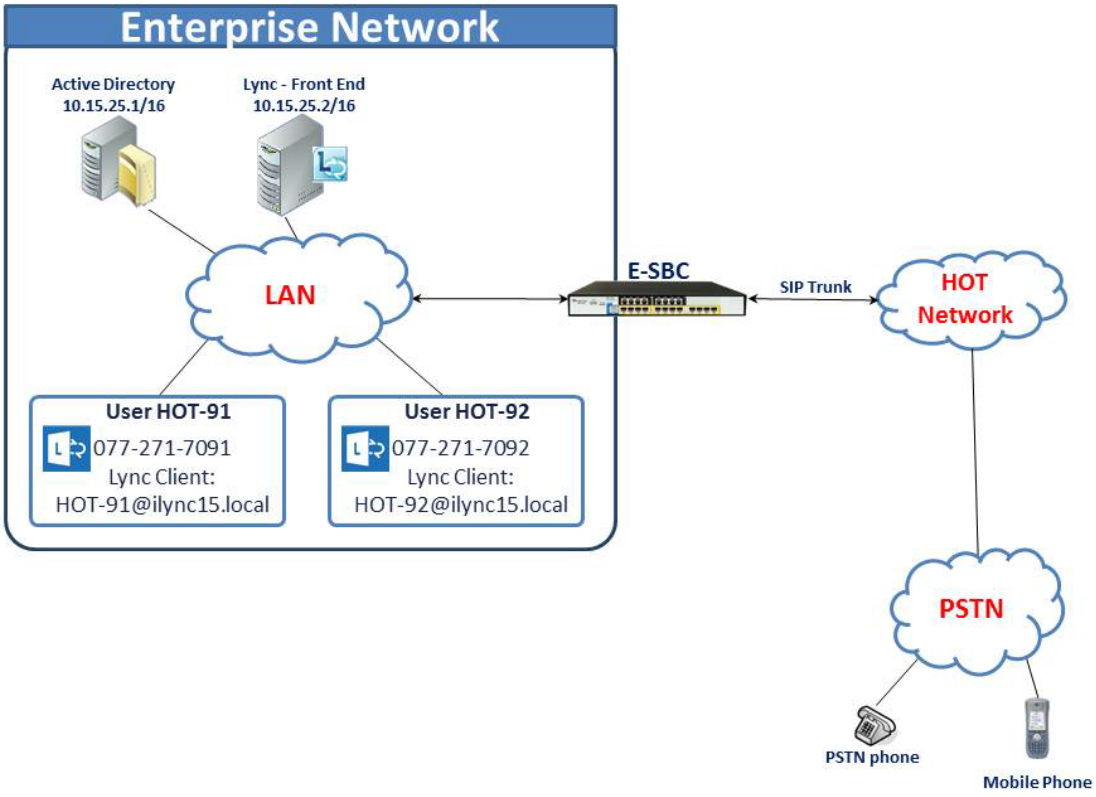
2.4 Interoperability Test Topology

The procedures in this document describe how to deploy the E-SBC using the following example scenario:

- 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 HOT'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 Lync Server 2013 network in the Enterprise LAN and HOT's SIP Trunk located in the public network.

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

Figure 2-1: E-SBC Interworking Microsoft Lync and HOT SIP Trunk Topology Example



2.4.1 Environment Setup

The example scenario 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 • HOT SIP Trunk is located on the WAN
Signaling Transcoding	• Microsoft Lync Server 2013 functions with SIP-over-TLS transport type • HOT SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	• Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders • HOT SIP Trunk supports G.711A-law and G.711U-law coders
Media Transcoding	• Microsoft Lync Server 2013 operates with the SRTP media type • HOT SIP trunk operates with the RTP media type

2.4.2 Known Limitations

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

Reader's Notes

3 Configuring Lync Server 2013

This section 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.

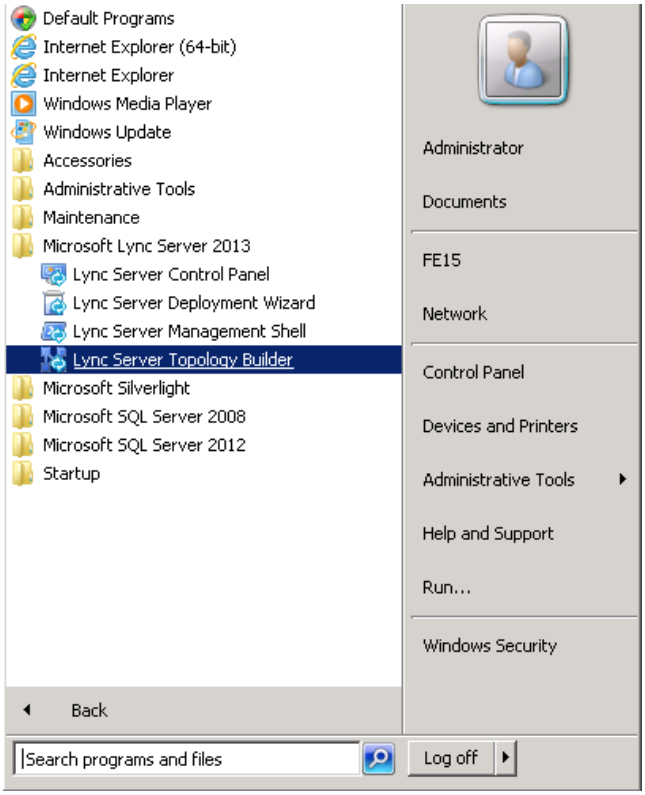
3.1 Configure the E-SBC as an IP / PSTN Gateway

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 a Mediation Server:**

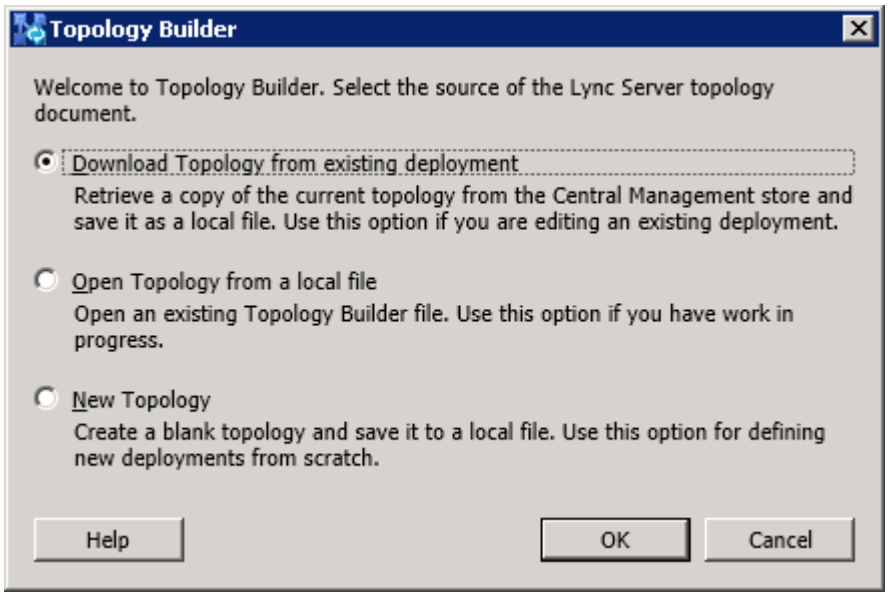
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**).

Figure 3-1: Starting the Lync Server Topology Builder



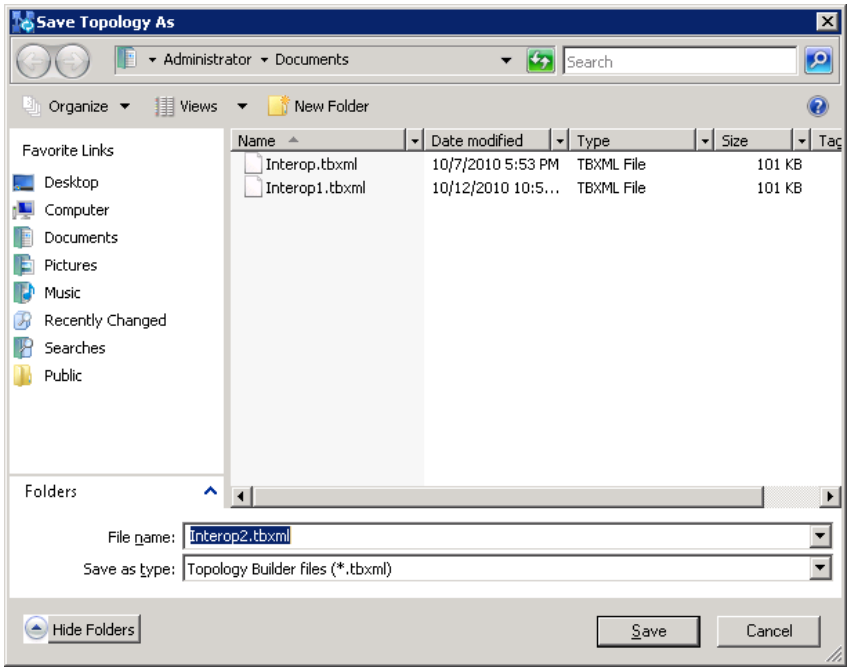
The following screen is displayed:

Figure 3-2: Topology Builder Options



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

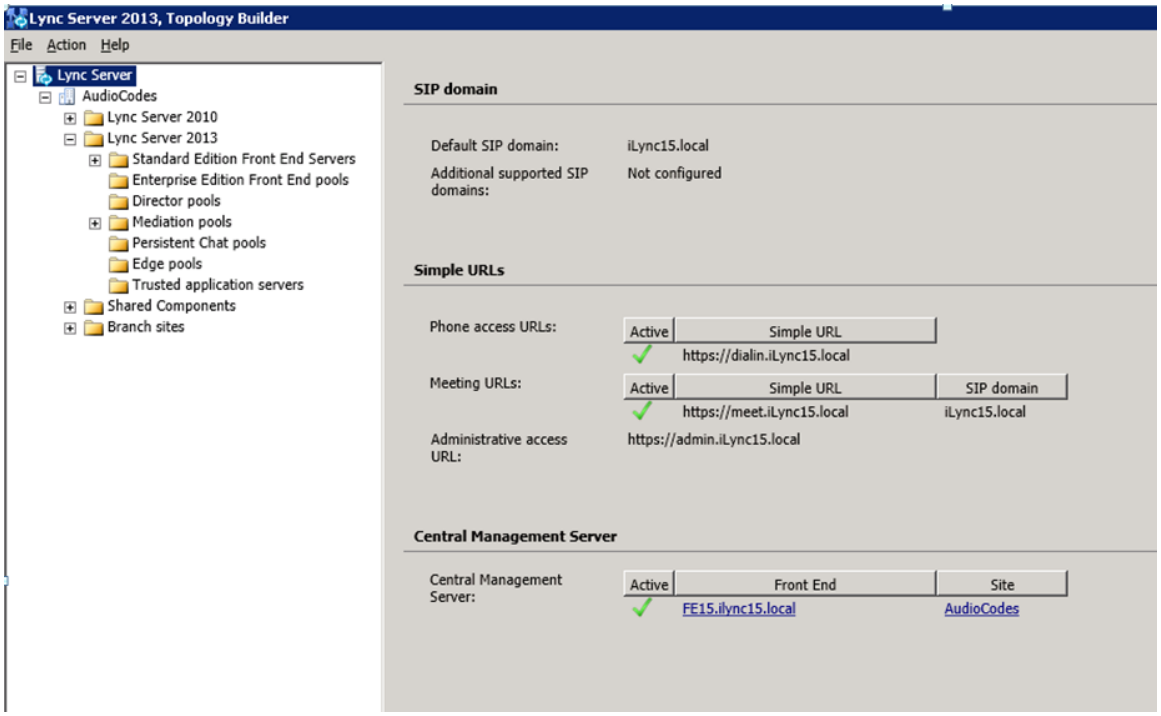
Figure 3-3: Saving the Topology



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

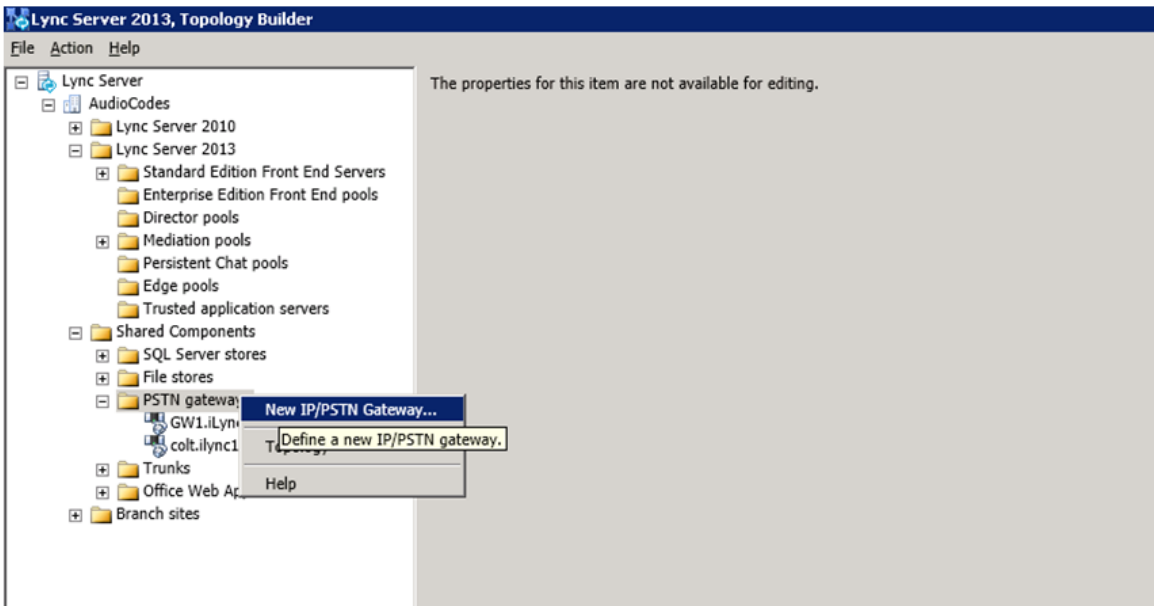
The Topology Builder screen with the downloaded topology is displayed.

Figure 3-4: Downloaded Topology



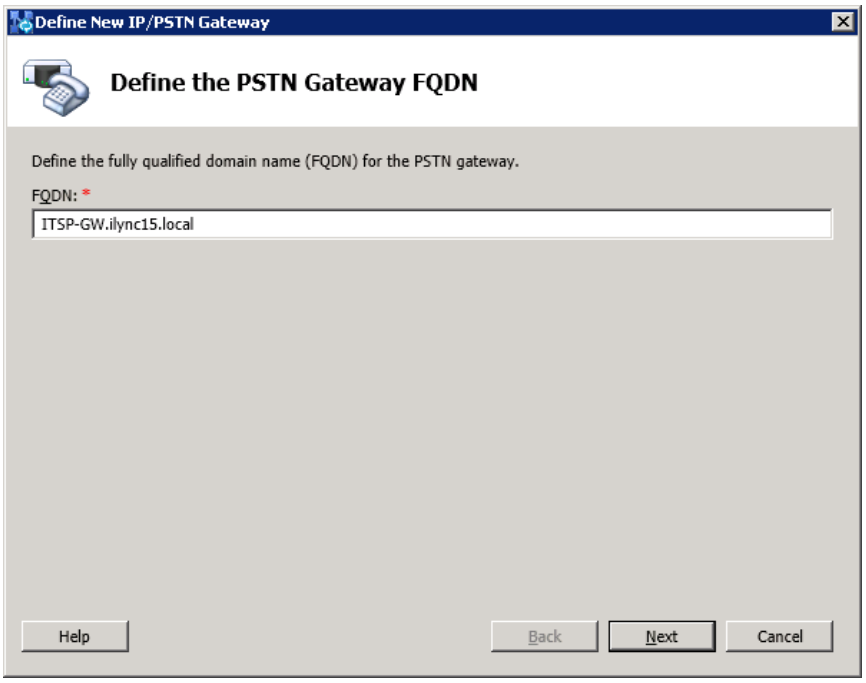
4. Under Lync Server 2013, your site name, Shared Components, right-click the **PSTN Gateways** node, and then click **New PSTN Gateway**.
5. Right-click the **PSTN gateways** folder, and then choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



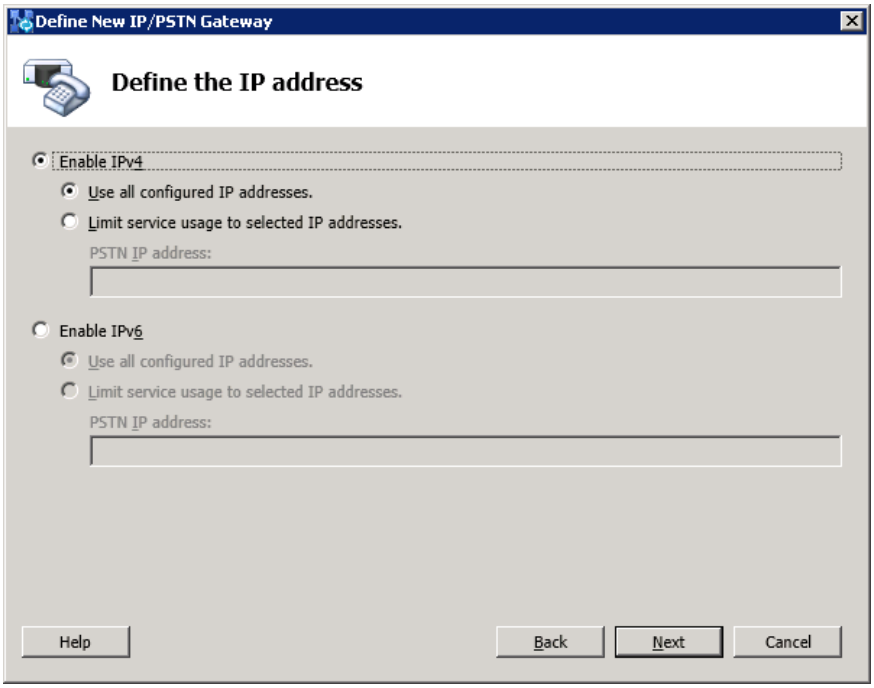
The following dialog box appears:

Figure 3-6: Defining the New IP/PSTN Gateway



6. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., "ITSP-GW.ilync15.local"). This FQDN should be updated 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 then click **Next**.

Figure 3-7: Defining the IP Address



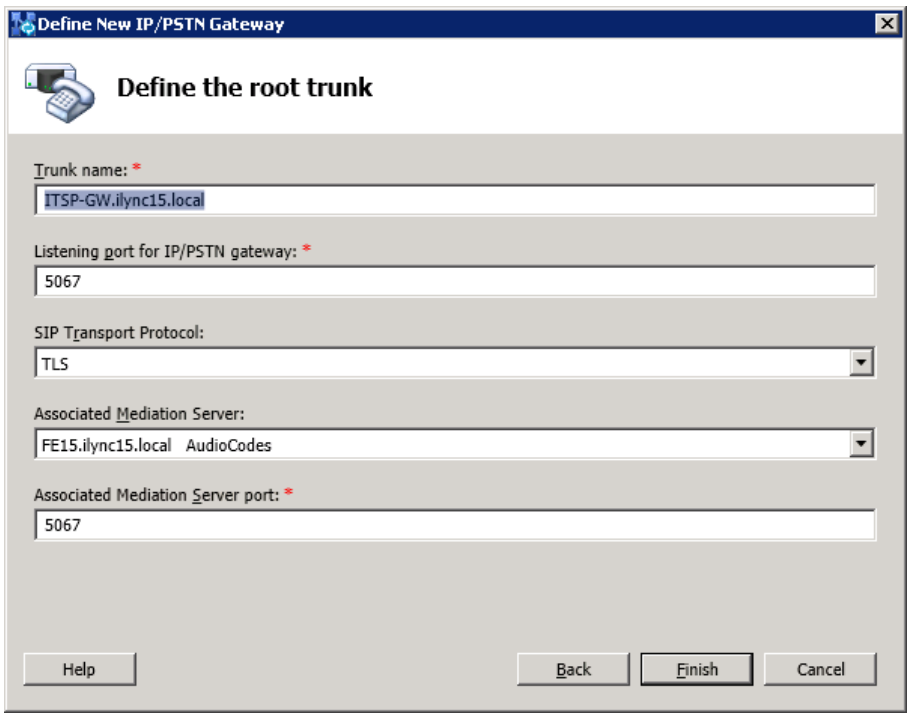
8. Click **Next**.

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



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

b. From the 'SIP Transport Protocol' drop-down list, select the Transport Type that the trunk uses (i.e., **TLS**).

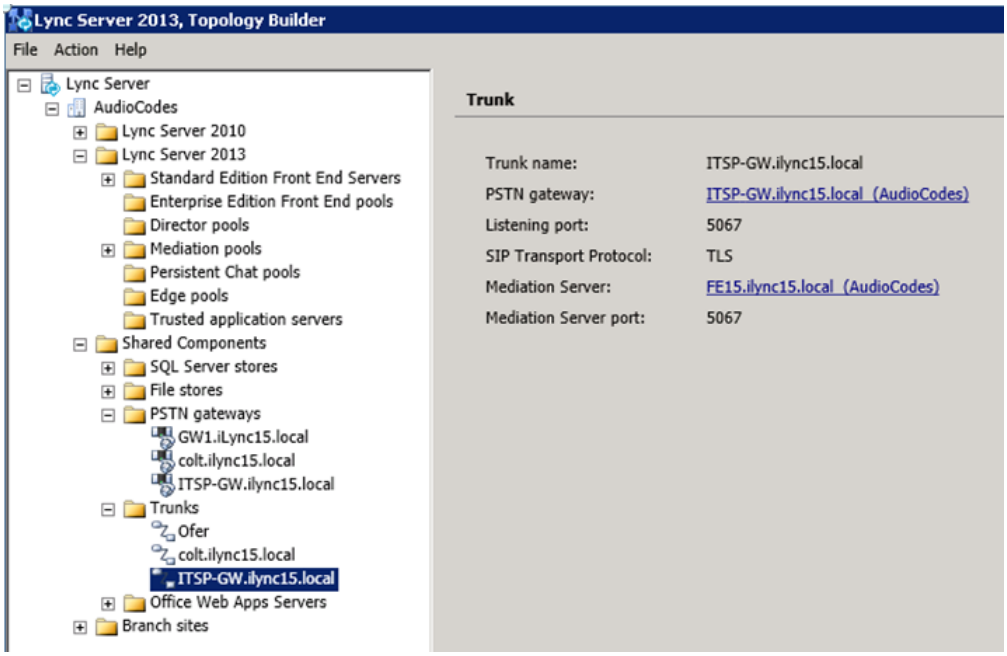
c. From the 'Associated Mediation Server' drop-down list, select the Mediation Server pool to associate with the root trunk of this PSTN Gateway.

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**.

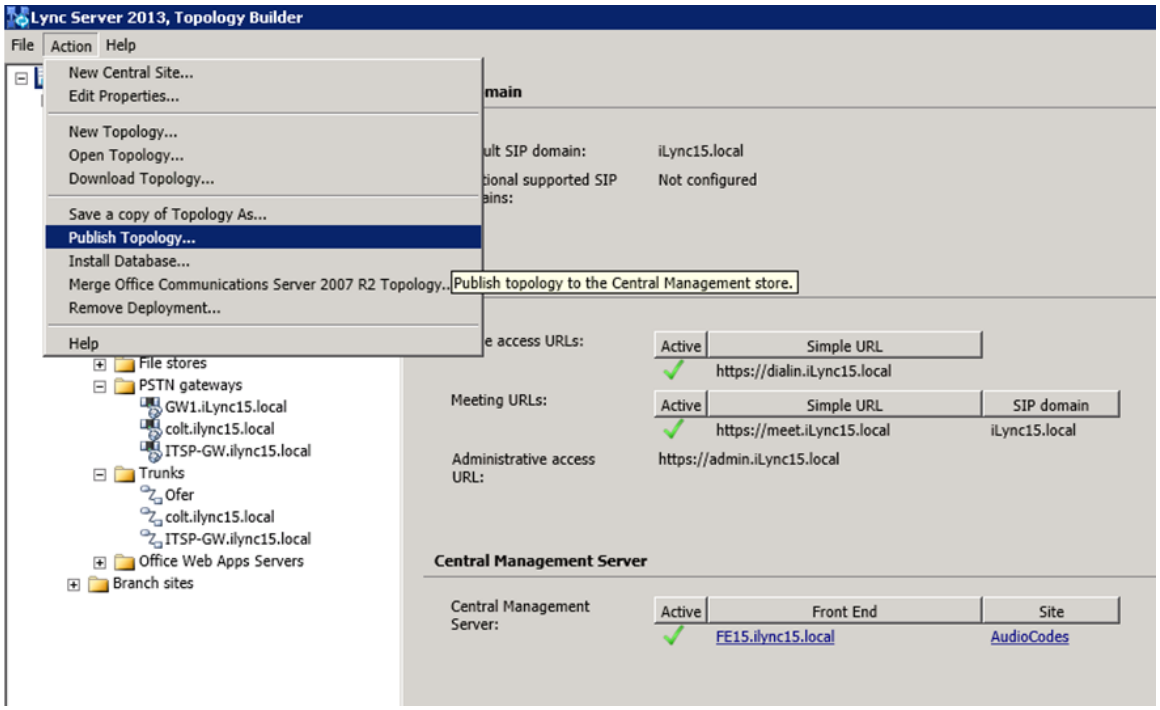
The SBC is added as a PSTN Gateway and a trunk is created as shown below:

Figure 3-9: Adding SBC as an IP/PSTN Gateway and Creating a Trunk



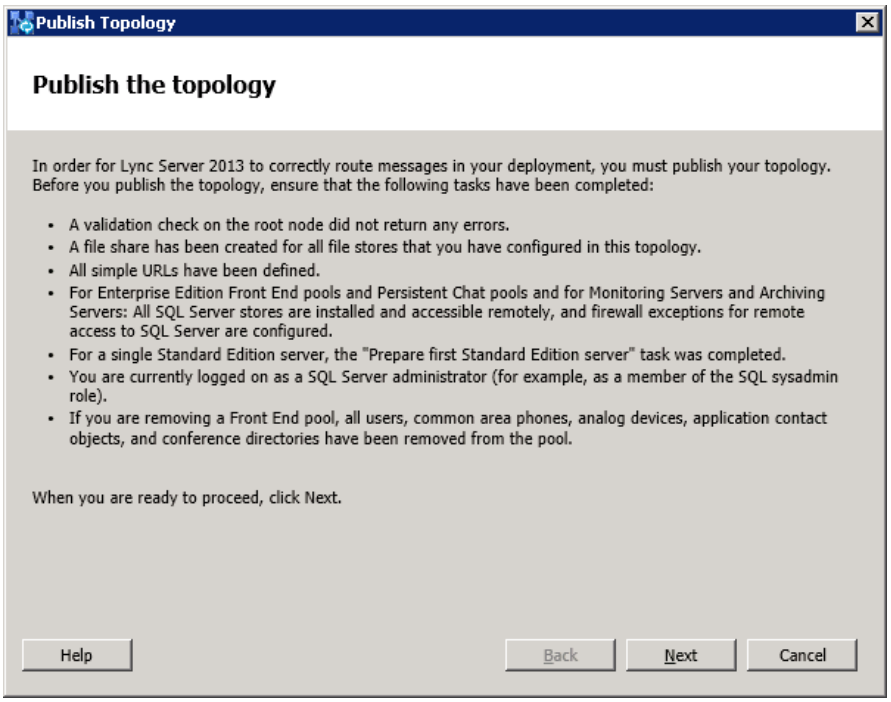
10. Publish the Topology by selecting the root item **Lync Server** > **Action** menu > **Publish Topology**, as shown below:

Figure 3-10: Selecting 'Publish Topology' from the 'Action' Menu



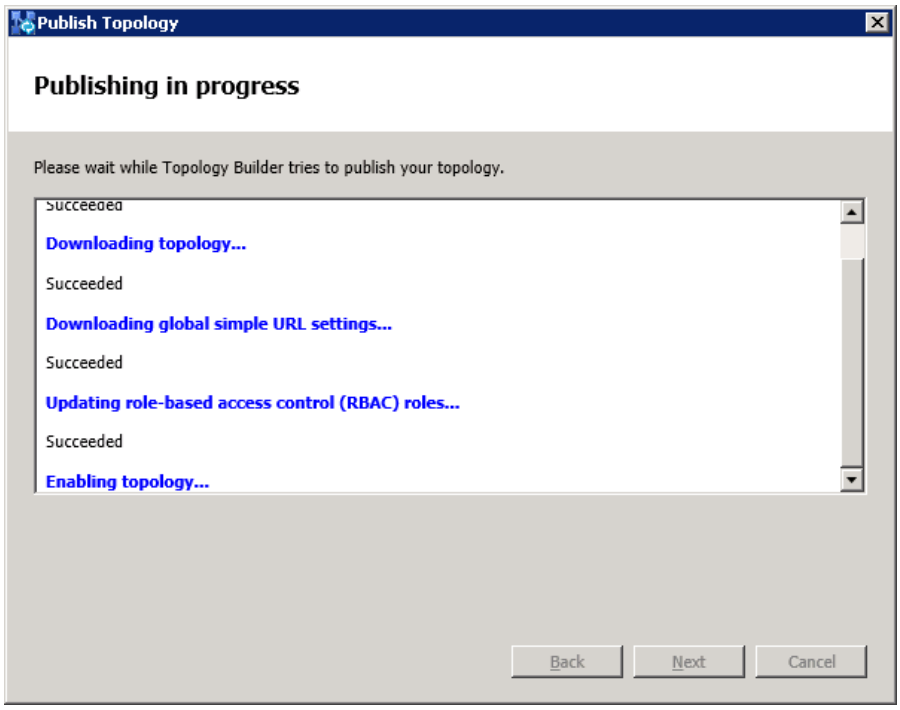
The Publish Topology screen is displayed in the screen below:

Figure 3-11: Publishing Topology



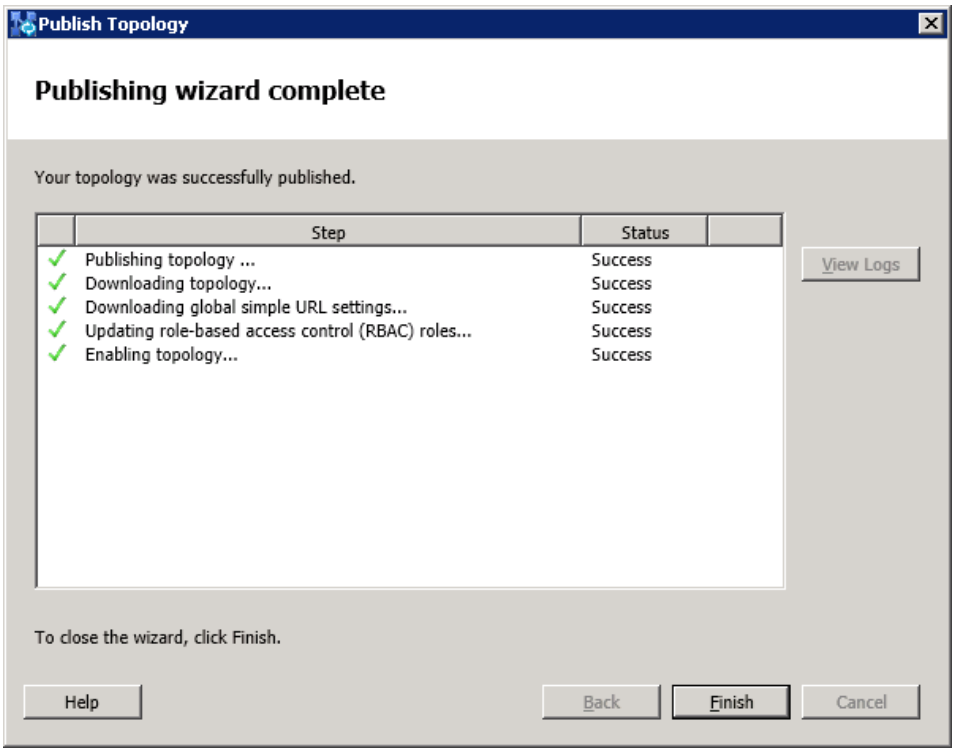
11. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing the Topology in Progress



12. Wait until the Publishing Topology process completes successfully, as shown below:

Figure 3-13: Publishing Topology Successfully Completed



13. Click **Finish**.

3.2 Configure the Route on Lync Server 2013

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

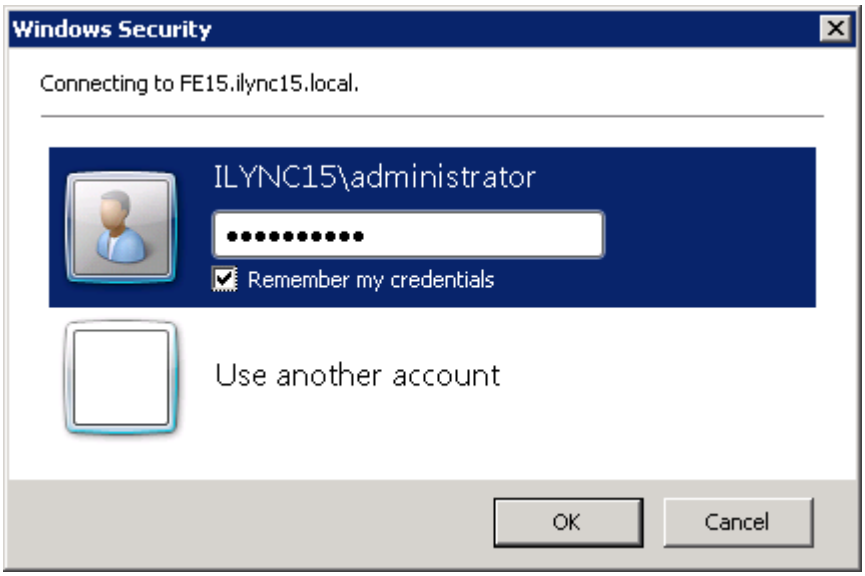
➢ **To configure the "route" on Lync Server 2013:**

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

Figure 3-14: Opening the Lync Server Control Panel

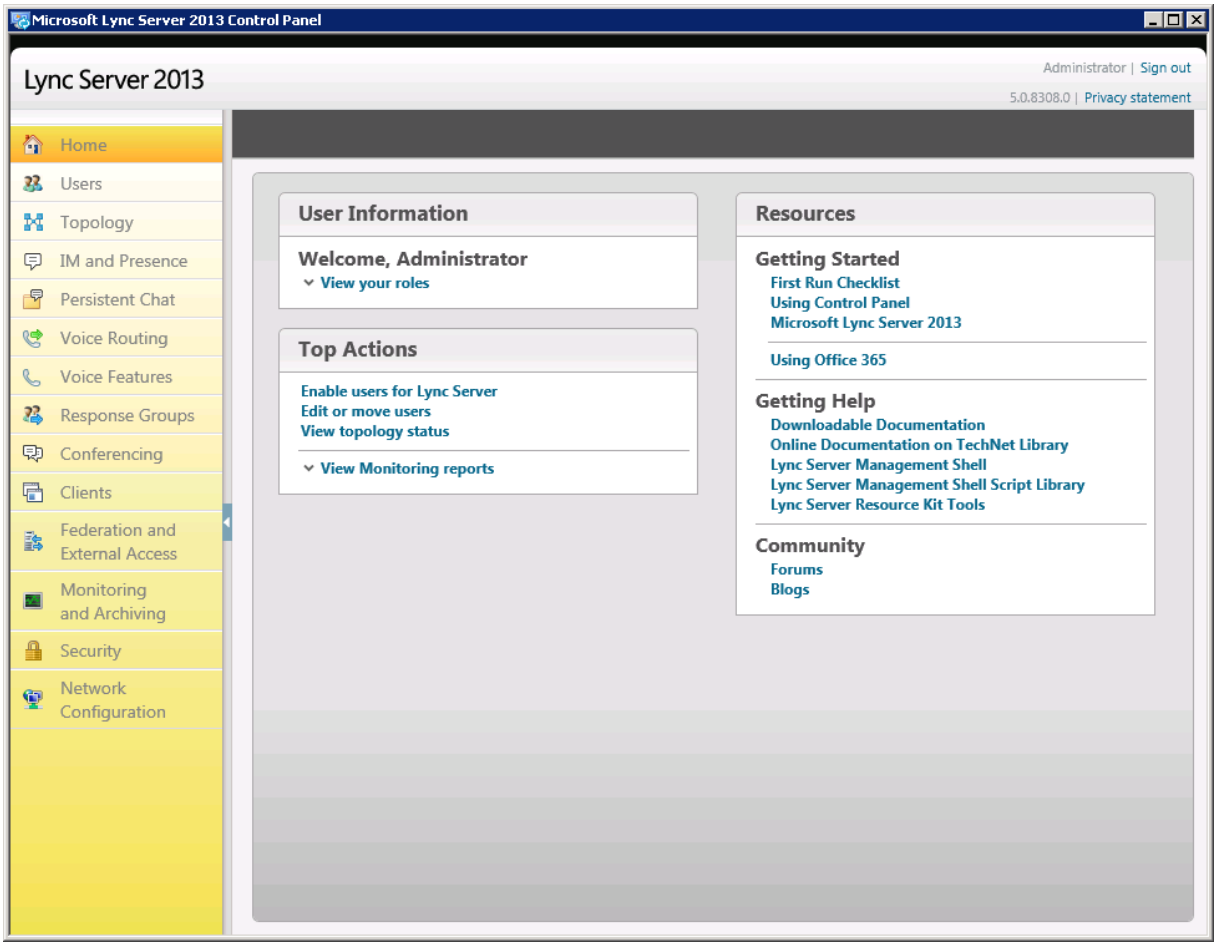
2. Enter your login credentials.

Figure 3-15: Entering Lync Server Credentials



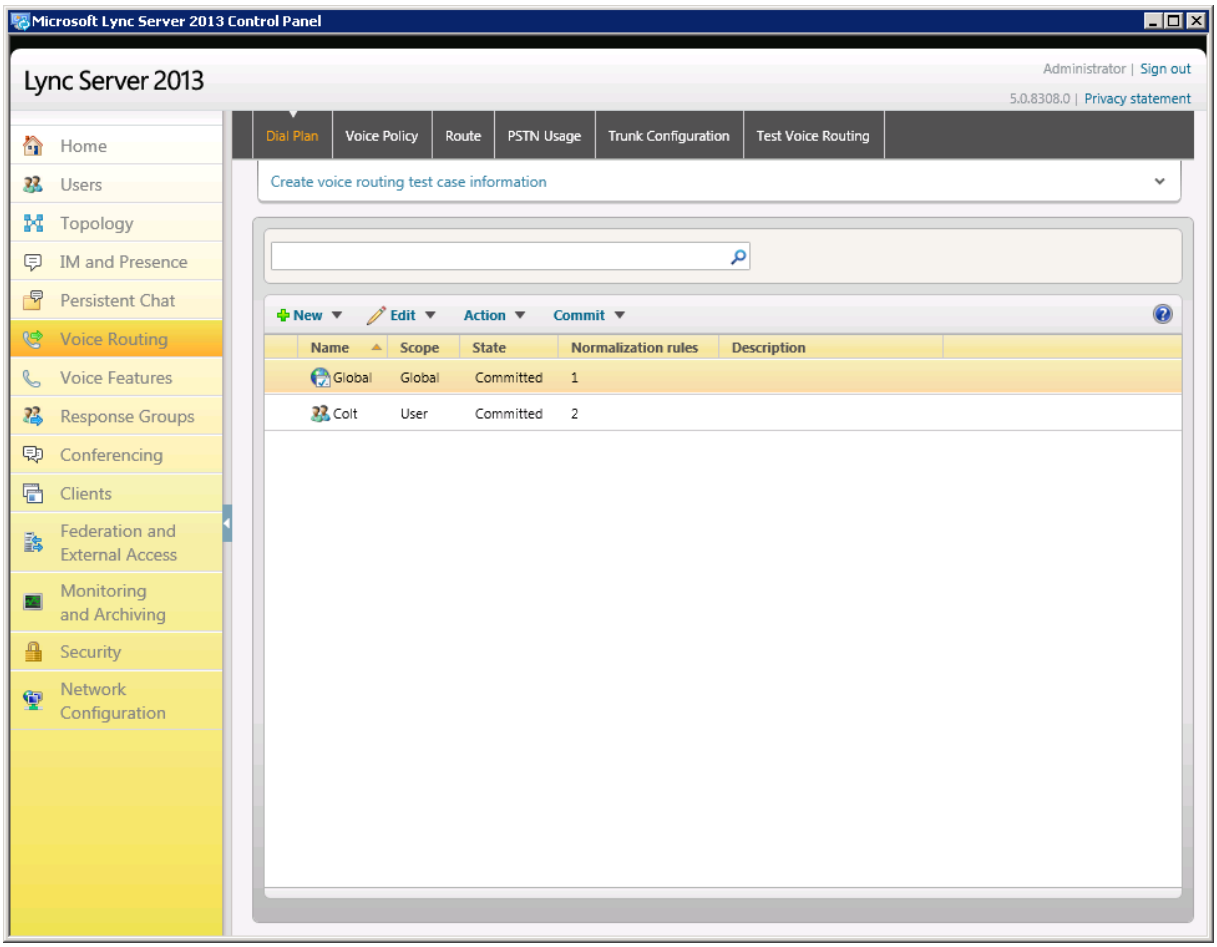
3. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed below:

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



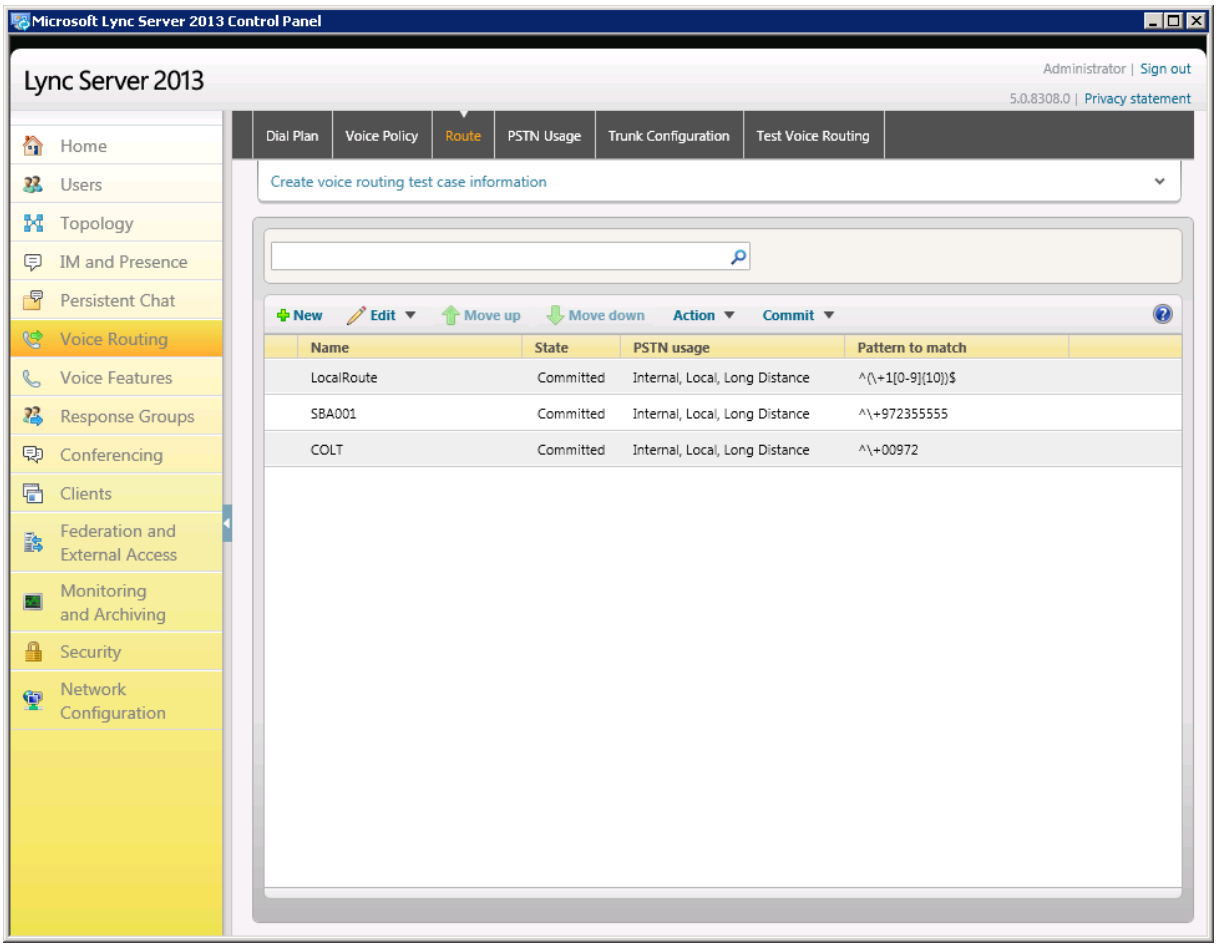
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Selecting Voice Routing



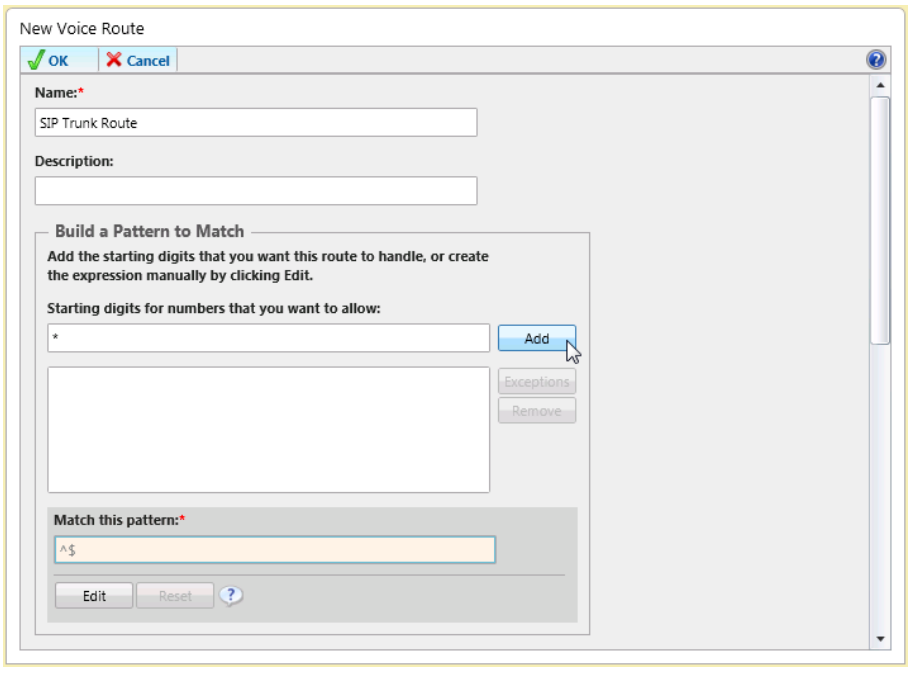
5. In the Voice Routing page, click the **Route** tab.

Figure 3-18: Selecting the Route Option



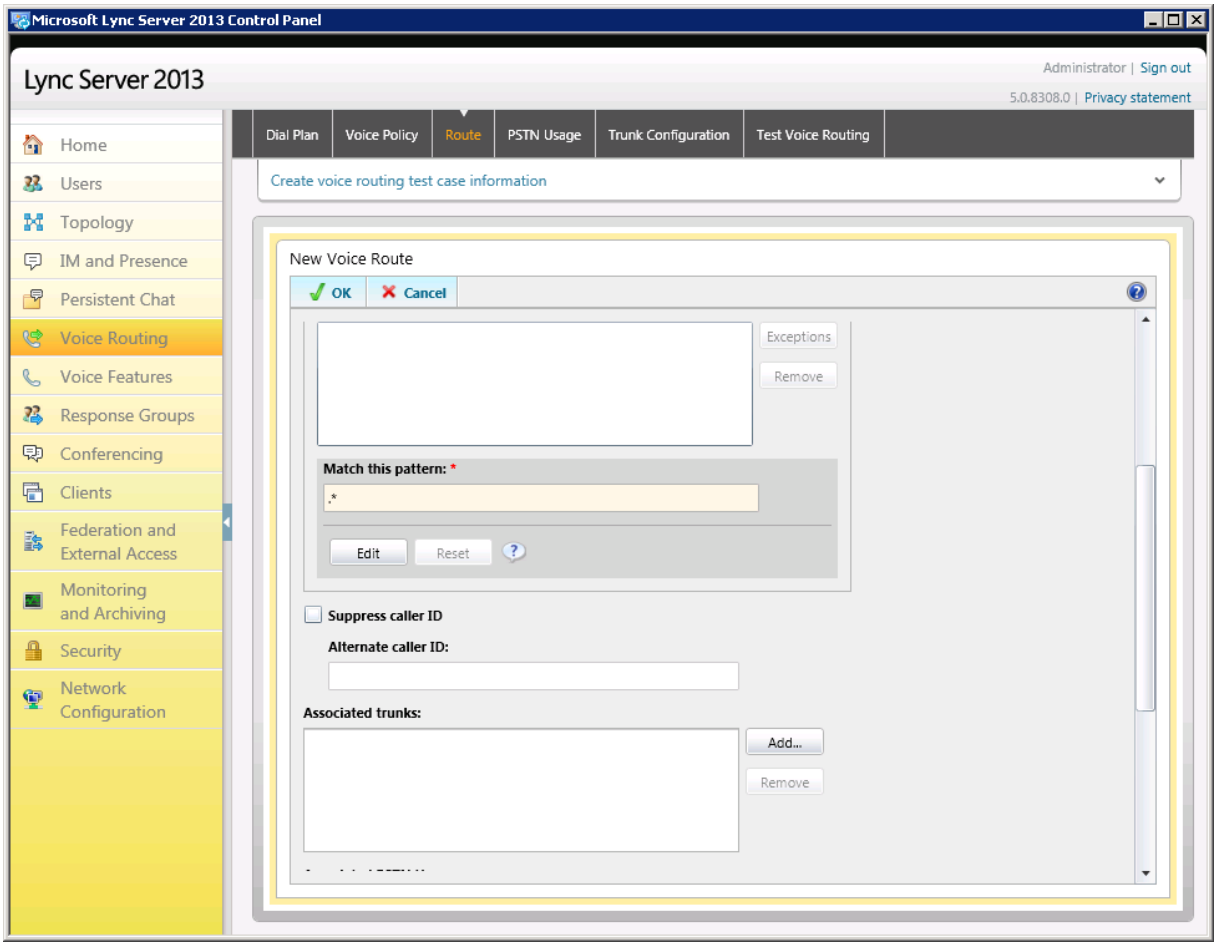
6. Click **New**; the New Voice Route dialog box appears:

Figure 3-19: Adding a New Voice Route



7. In the 'Name' field, enter a name for this route (e.g., "SIP Trunk Route").
8. In the 'Build a Pattern to Match' field, enter the starting digits you want this route to handle (e.g., "*", which means to match all numbers).
9. Click **Add**.

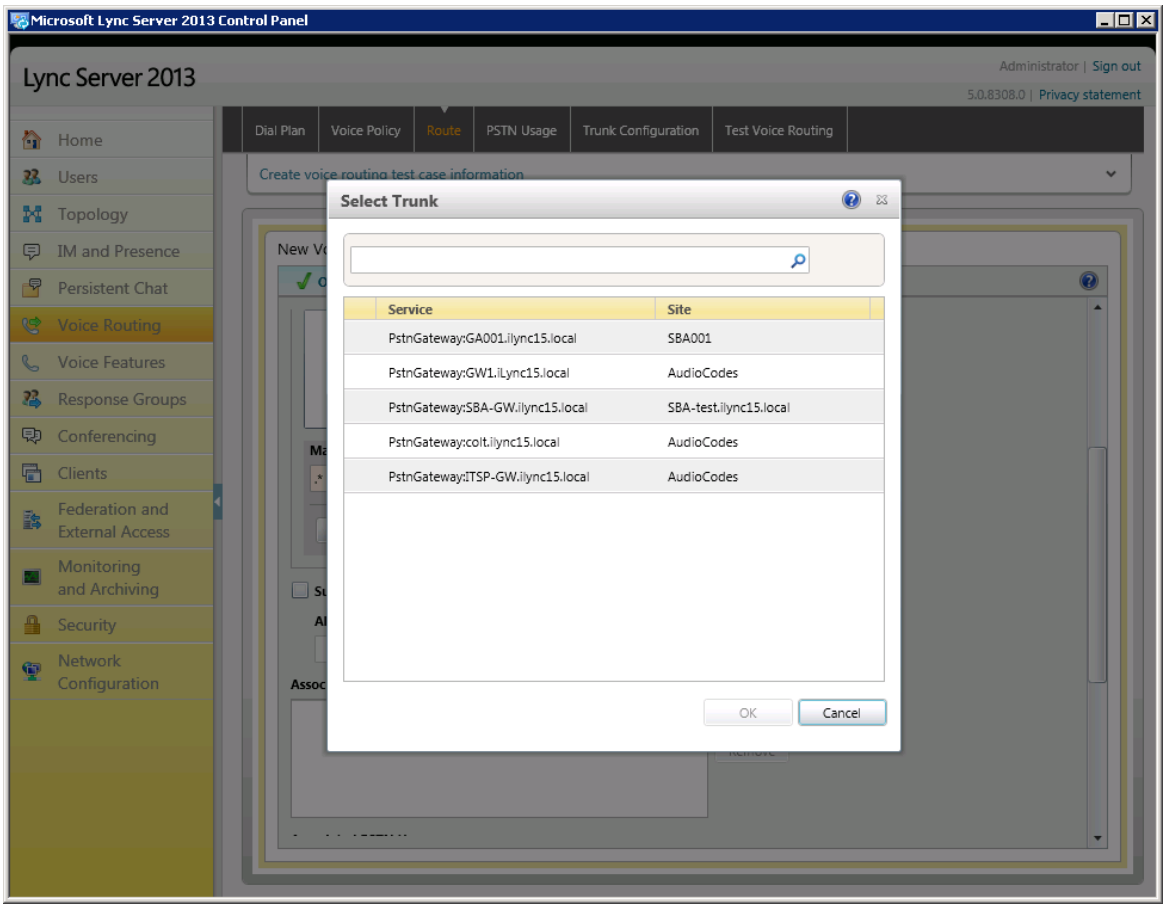
Figure 3-20: Adding a New Trunk



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

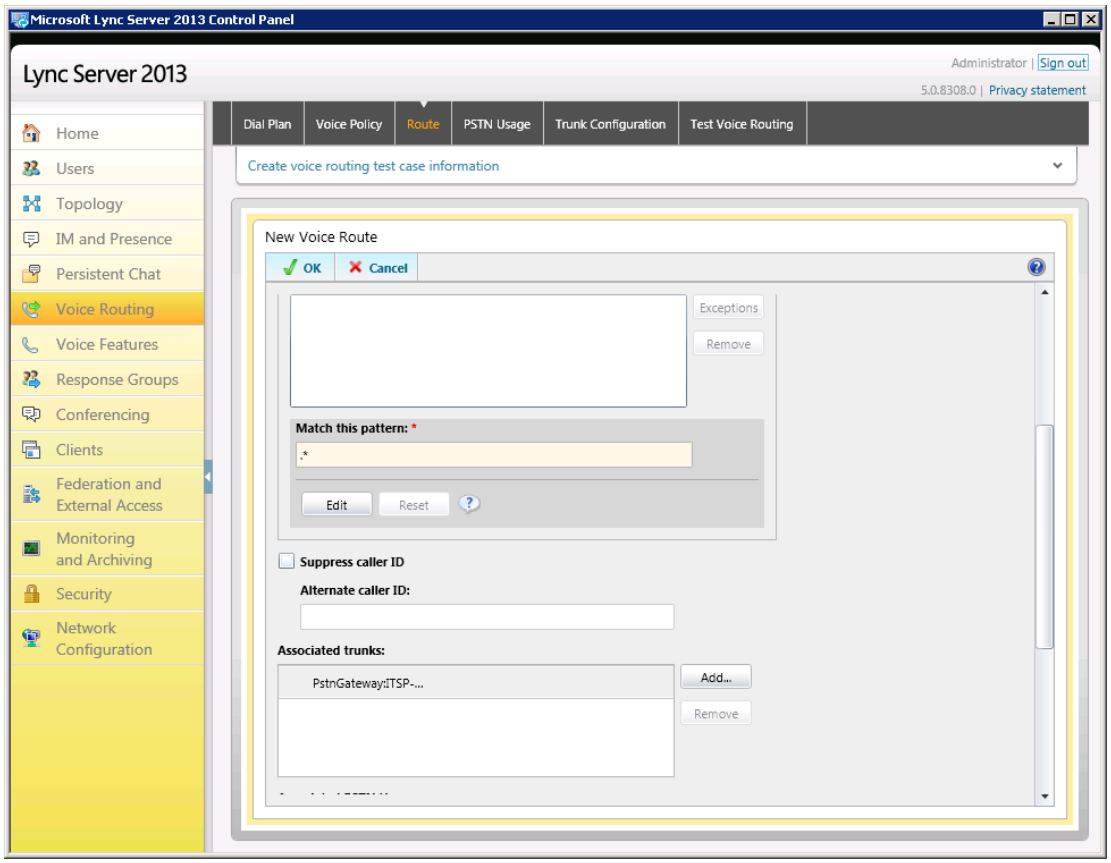
a. In the Associated Trunks pane, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: Displaying Deployed Trunks



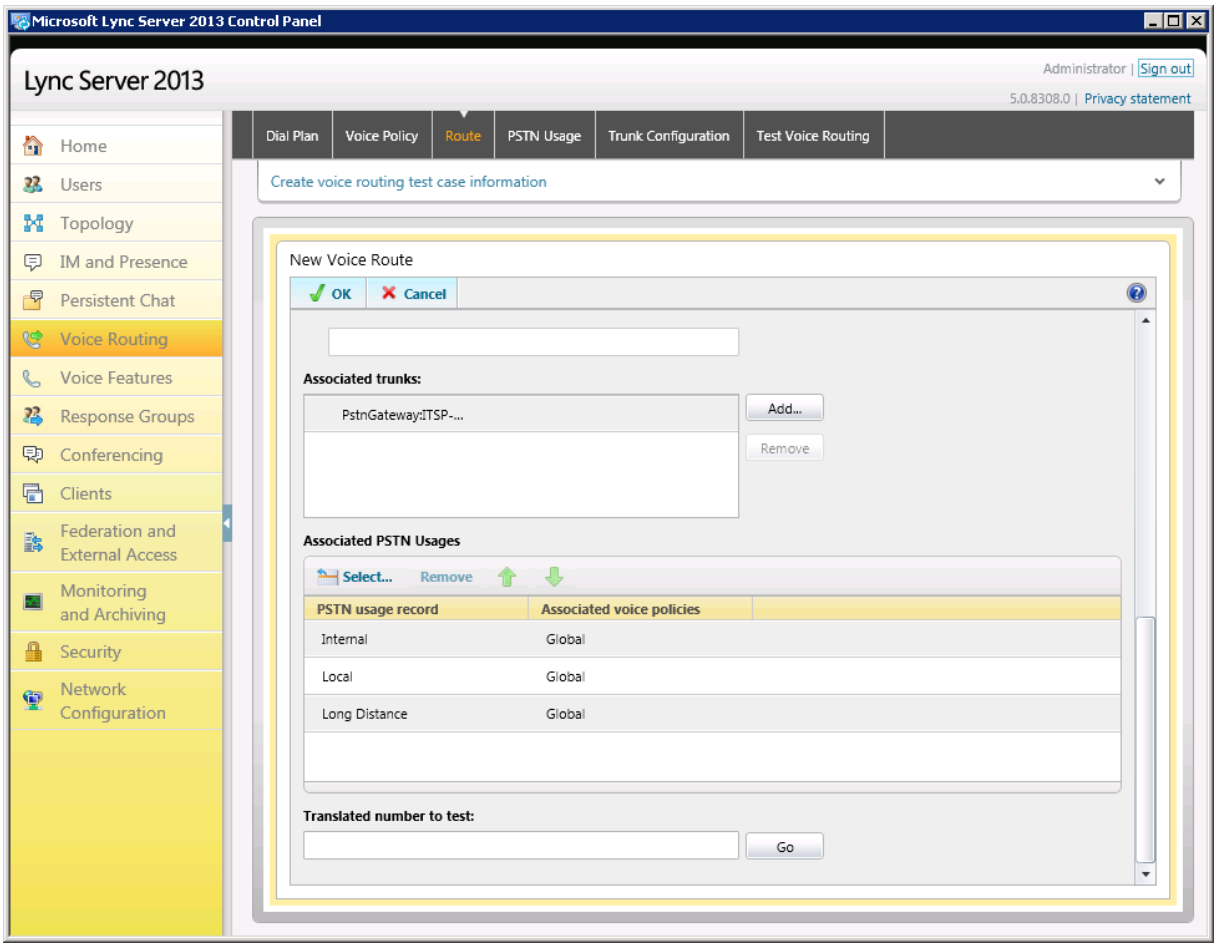
b. Select the E-SBC Trunk you created, and then click **OK**.

Figure 3-22: Selecting the E-SBC Trunk



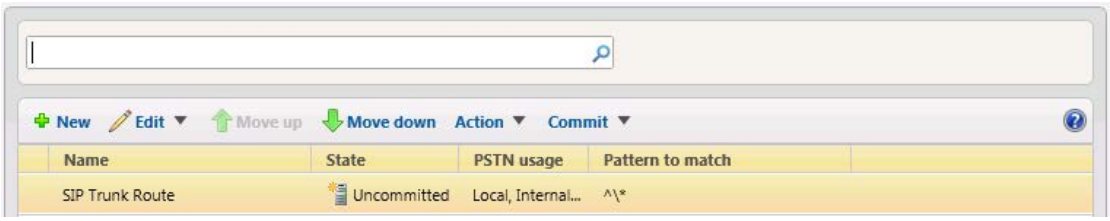
11. Associate a PSTN Usage to this route:
    a. In the Associated PSTN Usages group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



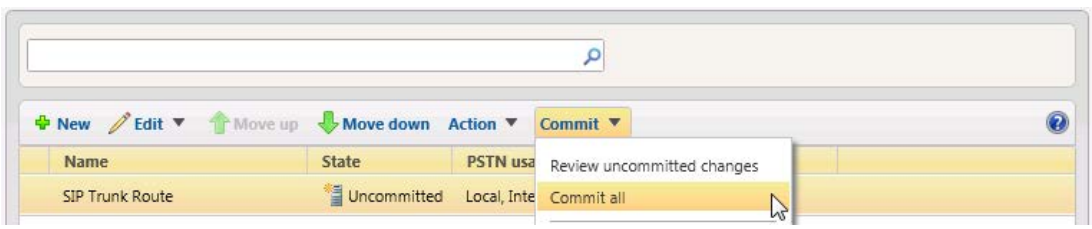
12. Click **OK** (located on the top of the New Voice Route dialog box); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



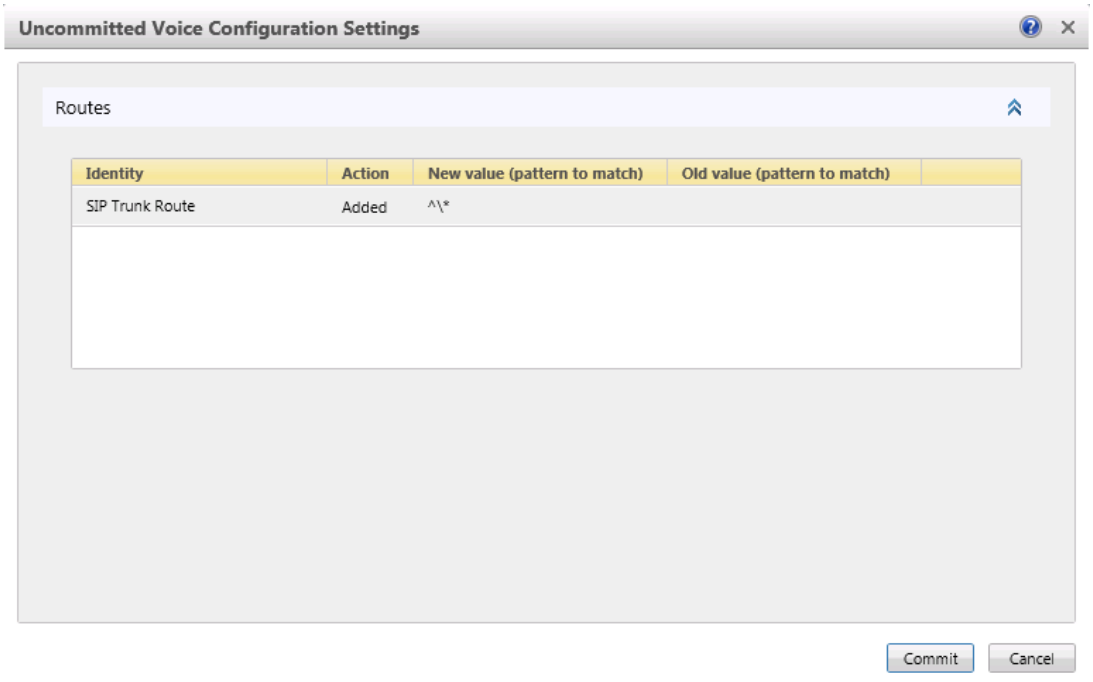
13. From the **Commit** drop-down list, choose **Commit all**, as shown below.

Figure 3-25: Committing Voice Routes



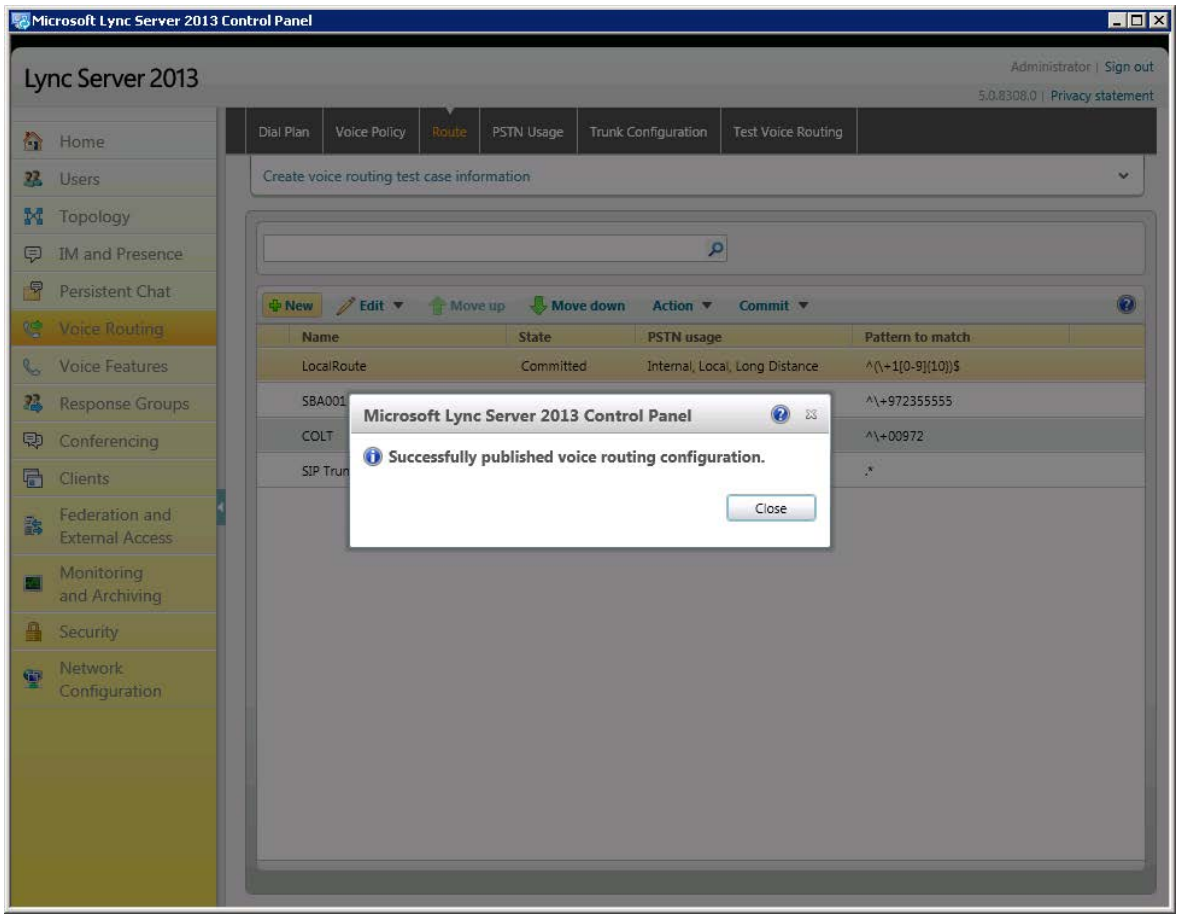
The Uncommitted Voice Configuration Settings dialog box appears:

Figure 3-26: Uncommitted Voice Configuration Settings



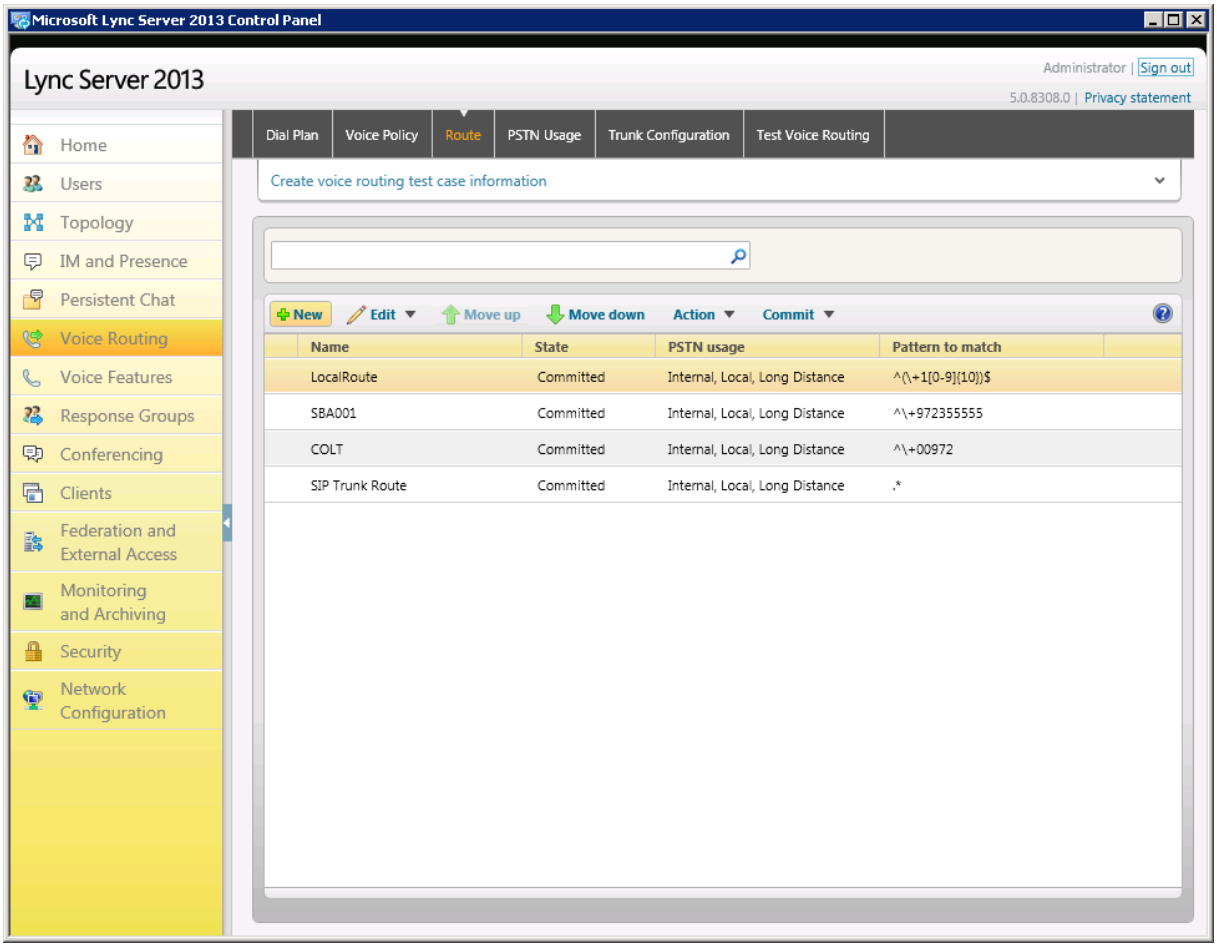
14. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirming Successful Voice Routing Configuration



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

Figure 3-28: Displaying Voice Routing Committed Routes



4 Configuring AudioCodes E-SBC

This section provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and HOT SIP Trunk:

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

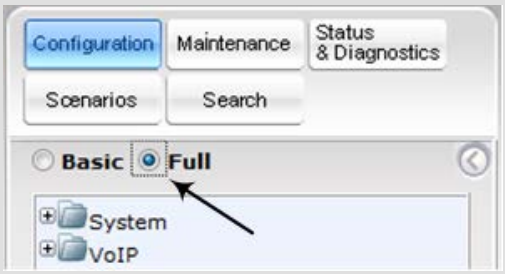
This section is applicable to both Microsoft Lync 2013 and Microsoft Lync 2010.

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

Notes:

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

  For more information about the Software Upgrade Feature Key, please 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 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: Network Interface Configuration

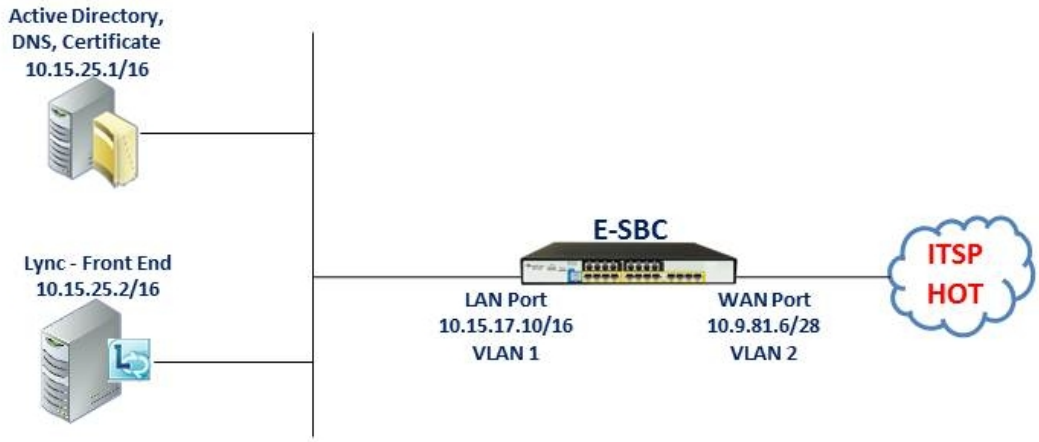
This step describes how to configure the E-SBC's network interfaces. There are several ways to deploy the E-SBC. However, the example scenario in this document uses the following deployment method:

- The E-SBC interfaces are between the Lync servers located on the LAN and the HOT SIP Trunk located on the WAN.
- The E-SBC directly connects to the WAN.

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: Configuring Network Interfaces



4.1.1 Step 1a: Configure Network Interfaces

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

- LAN VoIP ("LAN-Lync")
- WAN VoIP ("WAN-HOT")

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

1. Open the Multiple Interface Table page (**Configuration** tab > **Network Settings** > **IP Settings**).
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**.
   b. Set the interface as follows:

Parameter	Settings
IP Address	**10.15.17.10**
Prefix Length	**16** This is the Subnet mask in bits for 255.255.0.0.
Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**LAN-Lync** This is an arbitrary descriptive name.
Primary DNS Server IP Address	**10.15.25.1**
Underlying Interface	**GROUP_1** This is the 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	**10.9.81.1**
Prefix Length	**28** This is the Prefix Length for 255.255.255.128.
Gateway	**10.9.81.1** This is the default gateway - router's IP address.
VLAN ID	**2**
Interface Name	**WAN-HOT** This is the arbitrary descriptive name of the WAN interface.
Primary DNS Server IP Address	**0.0.0.0**
Underlying Interface	**GROUP_2** This is the Ethernet port group.

4. Click **Apply**, and then **Done**; the configured Multiple Interface Table appears.

Figure 4-2: Configured Multiple Interface Table

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
0	OAMP + Media + Control	IPv4 Manual	10.15.17.10	16	10.15.0.1	1	LAN-Lync	10.15.25.1	0.0.0.0	GROUP_1
1	Media + Control	IPv4 Manual	10.9.81.6	28	10.9.81.1	2	WAN-HOT	0.0.0.0	0.0.0.0	GROUP_2

4.1.2 Step 1b: Configure the Native VLAN ID

The procedure below 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 Table**).
2. For **GROUP_1** member ports, set the 'Native Vlan' field to "1". This VLAN was assigned to network interface "Voice".
3. For **GROUP_2** member ports, set the 'Native Vlan' field to "2". This VLAN was assigned to network interface "WANSP".
4. Click **Apply**; the Native VLAN ID is configured.

Figure 4-3: Configured 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

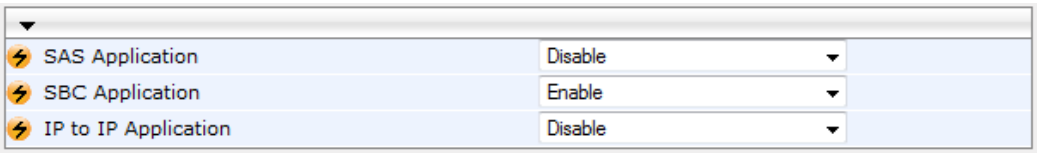
4.2 Step 2: Enable the SBC Application

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: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a **burn to flash** for this setting to take effect (see Section 4.16 on page 76).

4.3 Step 3: Signaling Routing Domains Configuration

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: Configure 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.

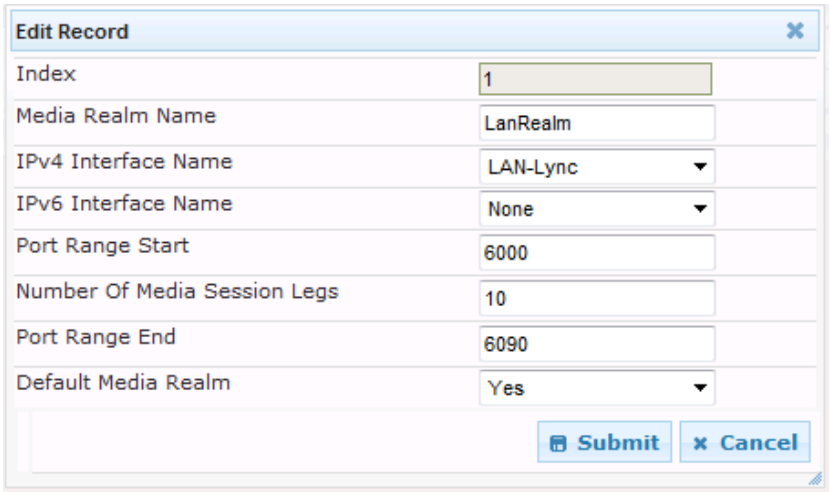
The simplest configuration is to create one Media Realm for internal (LAN) traffic and another for external (WAN) traffic, which is described in the procedure below for our example scenario.

➢ **To configure Media Realms:**

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

Parameter	Settings
Index	**1**
Media Realm Name	**LanRealm** This is an arbitrary Media Realm name.
IPv4 Interface Name	**LAN-Lync**
Port Range Start	**6000** This is the lowest UDP port number that will be used for media on the LAN.
Number of Media Session Legs	**10** This is the number of media sessions that are assigned with the port range.

Figure 4-5: Configuring LAN Media Realms

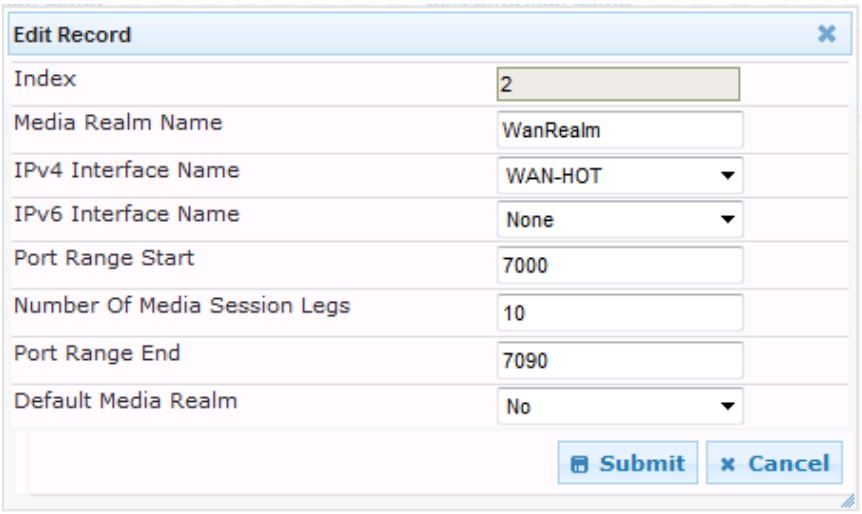


   c. Click **Submit**.

3. Add a Media Realm for the external traffic (WAN):
   a. Click **Add**.
   b. Configure the Media Realm as follows:

Parameter	Settings
Index	**2**
Media Realm Name	**WanRealm** This is an arbitrary name.
IPv4 Interface Name	**WAN-HOT**
Port Range Start	**7000** This is the lowest UDP port number that will be used for media on the WAN.
Number of Media Session Legs	**10** Enter the number of media sessions that are assigned with the port range.

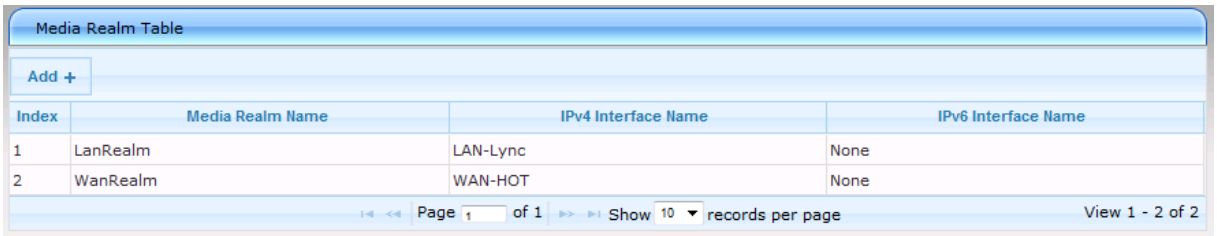
Figure 4-6: Configuring WAN Media Realm



   c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-7: Configured Media Realm Table



4.3.2 Step 3b: Configure SRDs

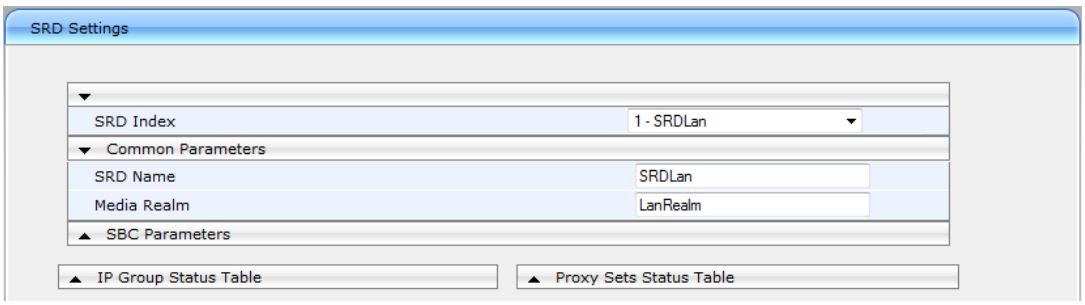
The procedure below describes how to configure the SRDs.

➢ **To configure 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	Settings
SRD Index	**1-SRDLan**
SRD Name	**SRDLan** This is the descriptive name for the SRD.
Media Realm	**LanRealm** This associates the SRD with a Media Realm**.**

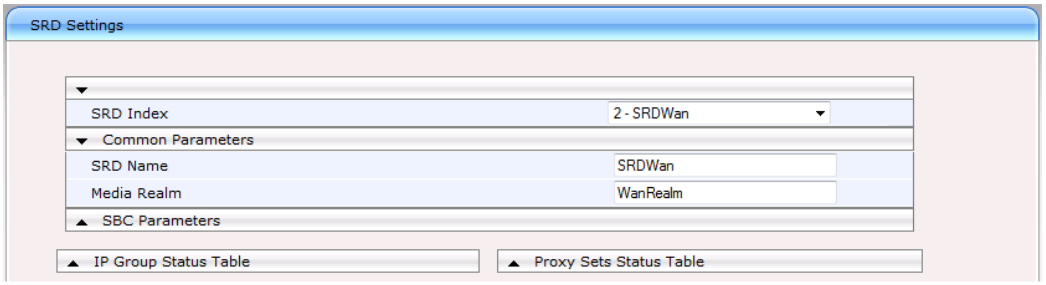
Figure 4-8: Configuring LAN SRDs



   b. Click **Submit**.
3. Add an SRD for the E-SBC's external interface (toward the HOT SIP Trunk):
   a. Configure the following parameters:

Parameter	Settings
SRD Index	**2-SRDWan**
SRD Name	**SRDWan** This is the descriptive name for the SRD.
Media Realm	**WanRealm** This associates the SRD with a Media Realm**.**

Figure 4-9: Configuring WAN SRDs



   b. Click **Submit**.

4.3.3 Step 3c: Configure 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.

The procedure below describes how to add SIP interfaces. In our example scenario, you need to 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	Settings
Index	**1**
Network Interface	**LAN-Lync**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
SRD	**1**

   c. Click **Submit**.

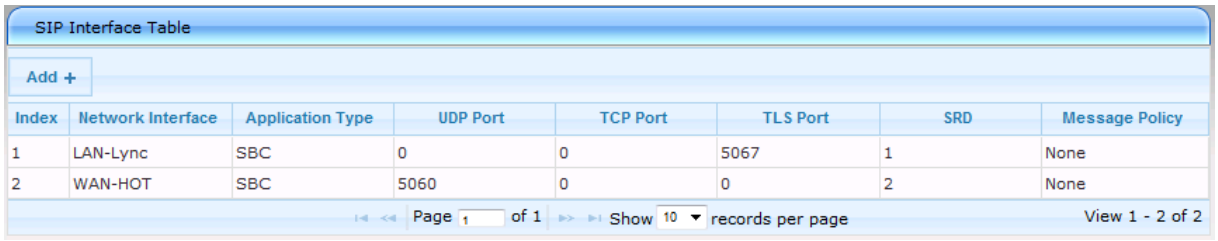
3. Add a SIP interface for the WAN:
   a. Click **Add**.
   b. Configure the following parameters:

Parameter	Settings
Index	**2**
Network Interface	**WAN-HOT**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	**0**
SRD	**2**

   c. Click **Submit**.

The configured SIP Interface table is shown below:

Figure 4-10: Required SIP Interface Table



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
- HOT SIP Trunk

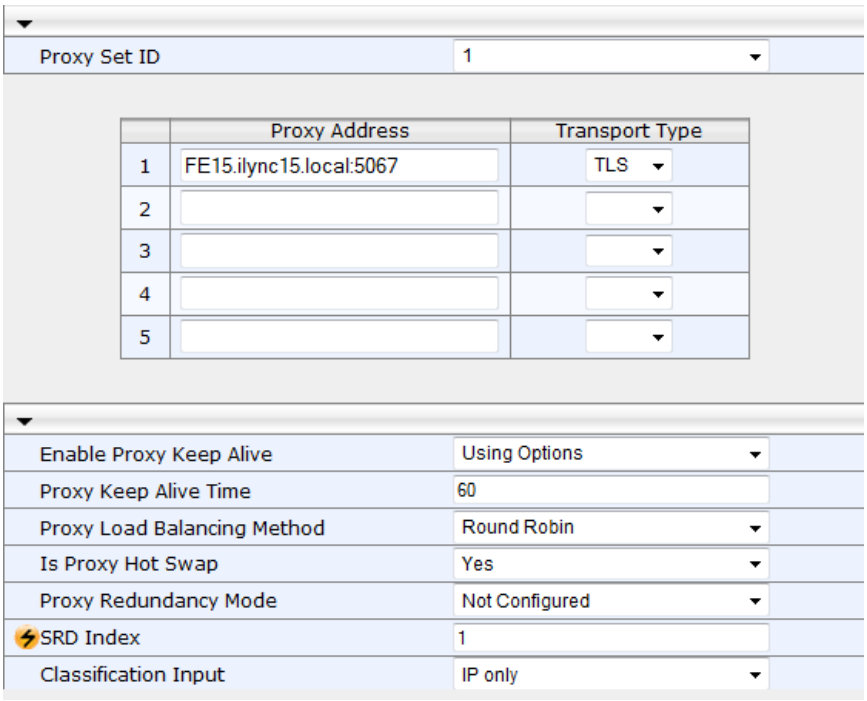
These Proxy Sets will later be associated with IP Groups.

➢ **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	Settings
Proxy Set ID	**1**
Proxy Address	**FE15.ilync15.local:5067** This is the 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

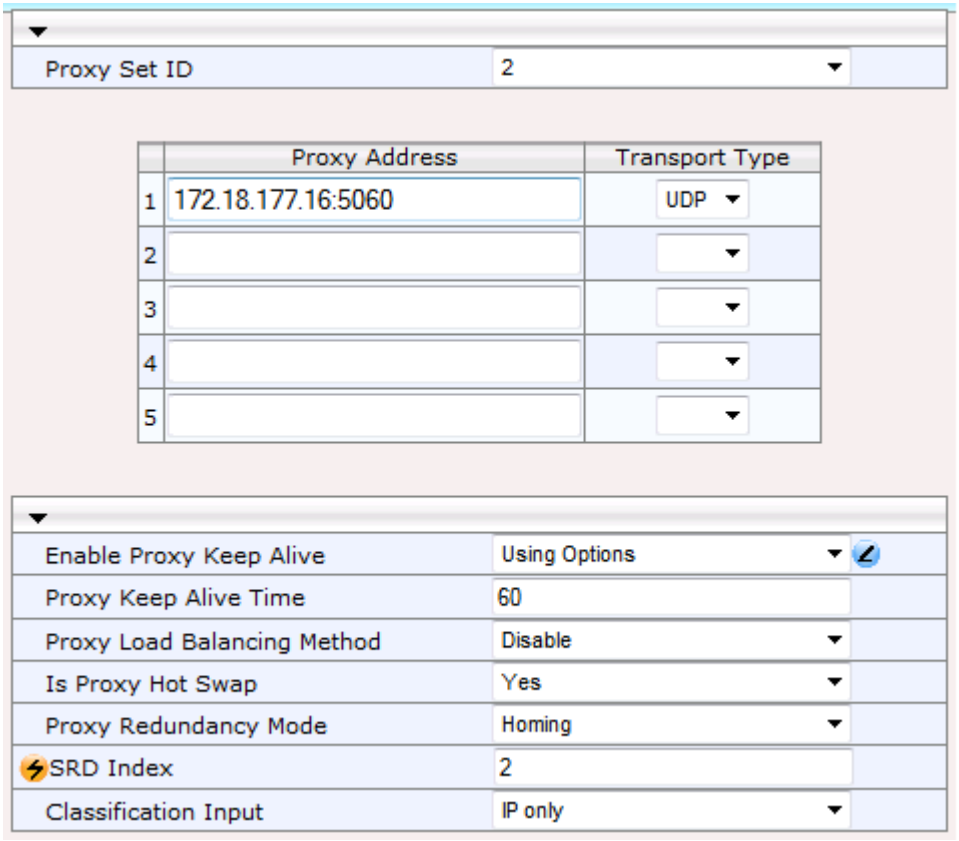


   b. Click **Submit**.

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

Parameter	Settings
Proxy Set ID	**2**
Proxy Address	**172.18.177.16:5060** This is the HOT 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** This enables classification by Proxy Set for this SRD in the IP Group belonging to the HOT SIP Trunk.

Figure 4-12: Proxy Set for HOT SIP Trunk



c. 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 our example scenario, you need to create IP Groups for the following entities:

- Lync Server 2013 (Mediation Server) on the LAN
- HOT 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	Settings
Index	**1**
Type	**Server**
Description	**Lync Server**
Proxy Set ID	**1**
SRD	**1**
Media Realm Name	**LanRealm**
IP Profile ID	**1**

   c. Click **Submit**.

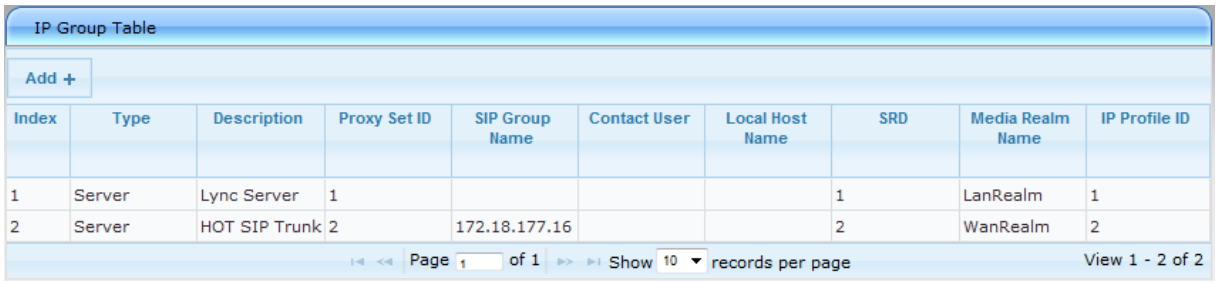
3. Add an IP Group for the HOT SIP Trunk:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**2**
Type	**Server**
Description	**HOT SIP Trunk**
Proxy Set ID	**2**
SIP Group Name	**172.18.177.16** This is the IP of HOT SIP Proxy.
SRD	**2**
Media Realm Name	**WanRealm**
IP Profile ID	**2**

   c. Click **Submit**.

The configured IP Group table is shown below:

Figure 4-13: Configured IP Group Table



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 HOT SIP Trunk. Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.5 on page 46).

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

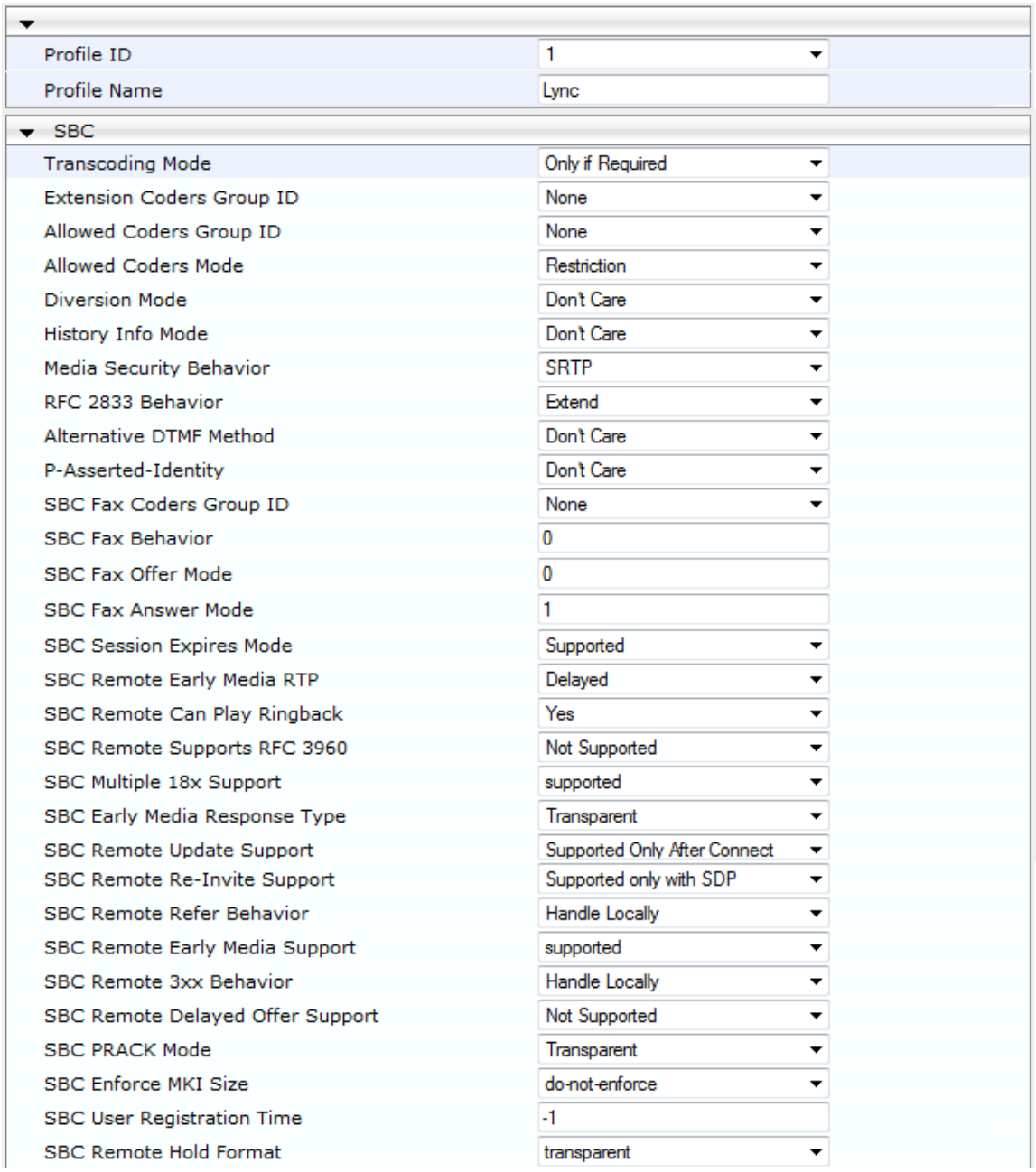
- Microsoft Lync Server 2013 - to operate in secure mode using SRTP and TLS
- HOT SIP trunk - to operate in non-secure mode using RTP and UDP

➢ **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	Settings
Profile ID	**1**
Media Security Behavior	**SRTP**
SBC RFC2833 Behavior	**Extend** This field is required, in case the SIP Trunk does not send an RFC 2833 in the SDP.
SBC Session Expires Mode	**Supported** SBC enables the session timer with Lync Server 2013 even if the HOT SIP Trunk does not support this capability.
SBC Remote Early Media RTP	**Delayed** This field is required, when the Lync Server 2013 sends a SIP 18x response. It does not immediately send an 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** This field is required since the Lync Server 2013 does not support receive REFER SIP messages.
SBC Remote 3xx Behavior	**Handle Locally** This field is required since Lync Server 2013 does not support receive 3xx SIP messages.
SBC Remote Delayed Offer Support	*Not Supported*

Figure 4-14: IP Profile for Lync Server 2013



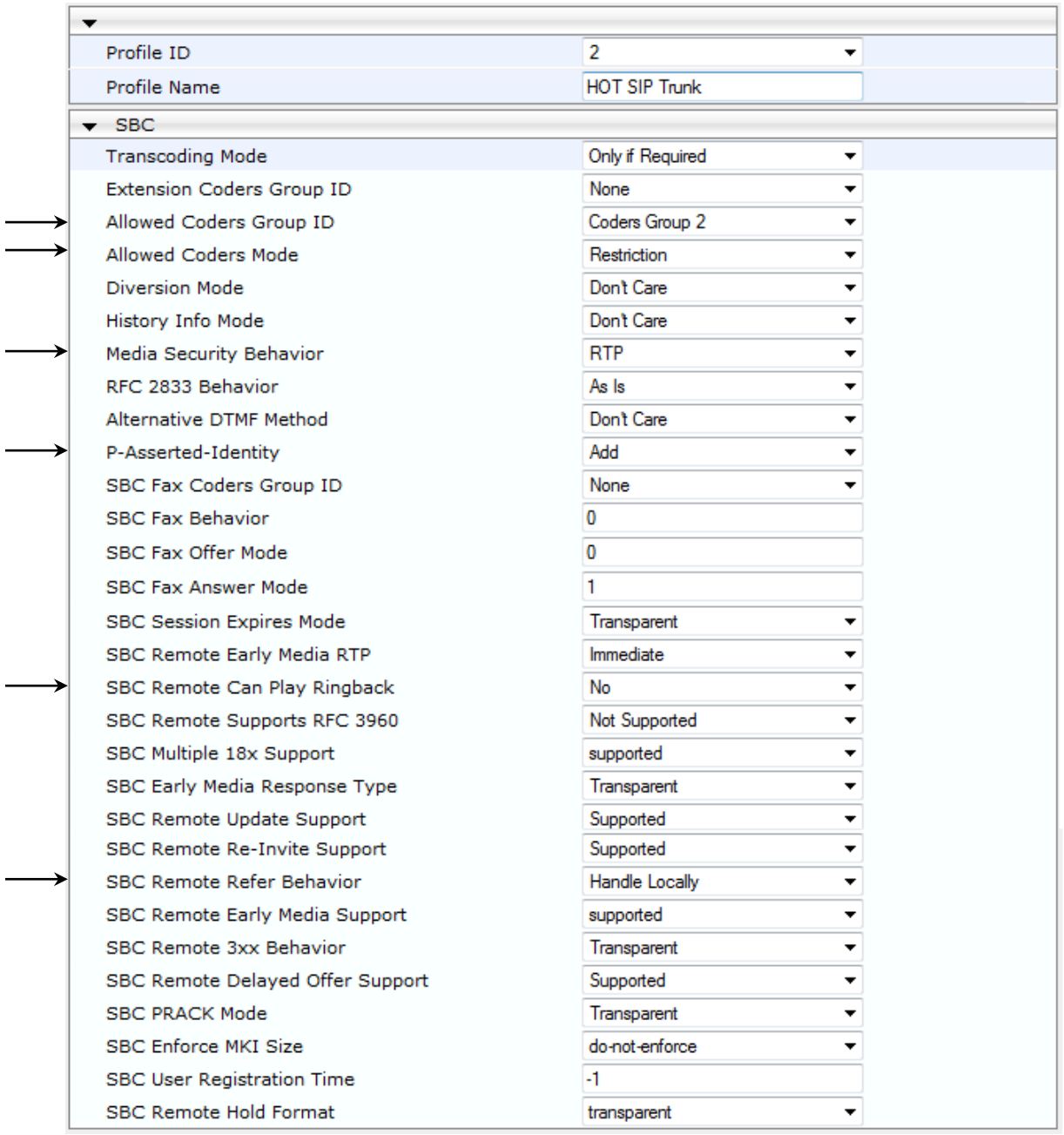
Profile ID	1
Profile Name	Lync
SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	None
Allowed Coders Group ID	None
Allowed Coders Mode	Restriction
Diversion Mode	Don't Care
History Info Mode	Don't Care
Media Security Behavior	SRTP
RFC 2833 Behavior	Extend
Alternative DTMF Method	Don't 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 HOT SIP Trunk:
   a. Configure the parameters as follows:

Parameter	Settings
Profile ID	**2**
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Restriction** Only coders common between SDP offered coders and Allowed Coders Group will be used.
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** This is required for anonymous calls.
SBC Remote Can Play Ringback	**No** This field is required as the Lync Server 2013 does not provide a Ringback tone for incoming calls.
SBC Remote Refer Behavior	**Handle Locally** E-SBC handles the incoming REFER request itself without forwarding the REFER towards the SIP Trunk.

Figure 4-15: IP Profile for HOT SIP Trunk



b. Click **Submit**.

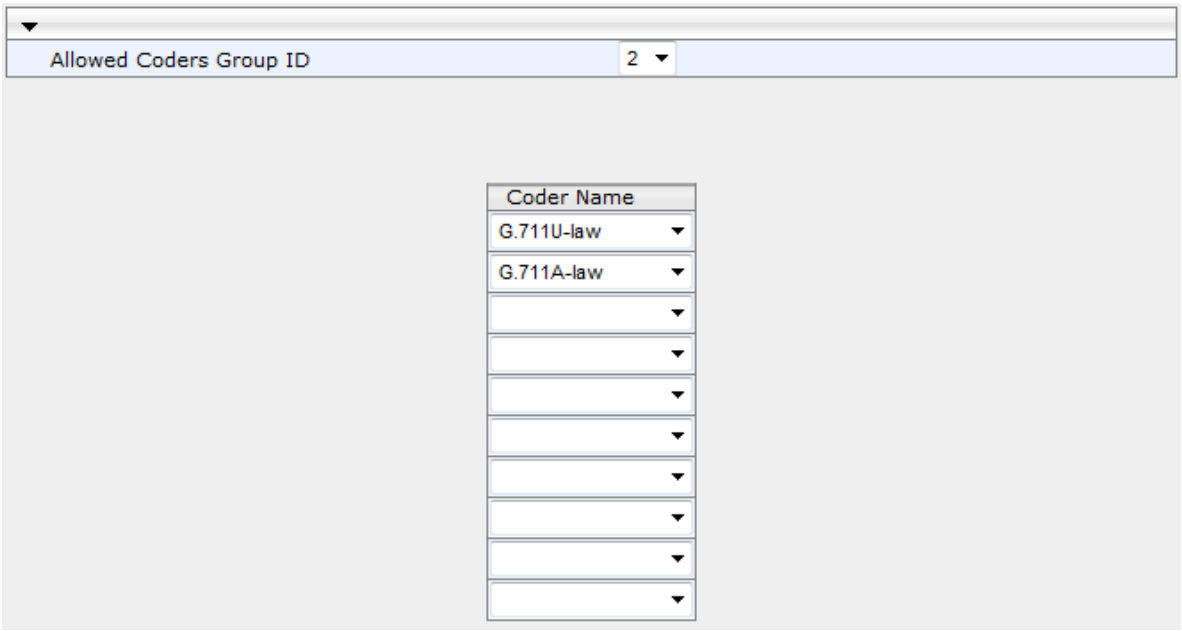
4.7 Step 7: Configure Allowed Coders

This step describes the procedure to add an Allowed Coders Group to ensure that voice sent to the HOT SIP Trunk uses the G.711 U-law and G.711 A-law coders only. Note that this Allowed Coders Group ID (and its preference) was assigned to the IP Profile belonging to the HOT SIP Trunk in the previous step (see Section 4.6 on page 48).

➢ **To configure a allowed coders for the HOT SIP Trunk:**

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).
2. From the 'Allowed Coders Group ID' drop-down list, select **2**.
3. From the 'Coder Name' drop-down list, select **G.711 U-law** and **G.711 A-law** coders.

Figure 4-16: Configuring Allowed Coders Group for HOT SIP Trunk



4. Click **Submit**.

4.8 Step 8: SIP TLS Connection Configuration

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.

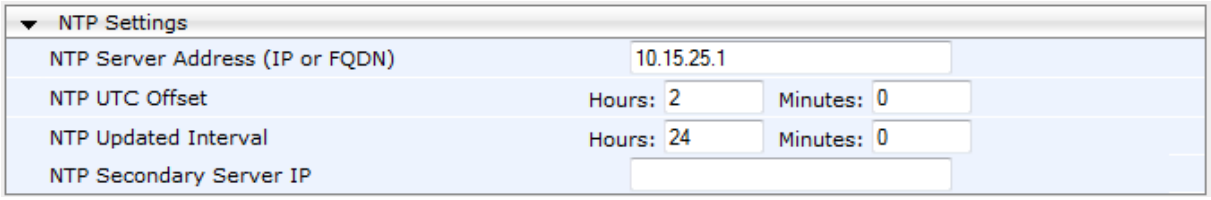
4.8.1 Step 8a: Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or 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 Address (IP or FQDN)' field, enter the IP address of the NTP server (e.g., "10.15.9.10").

Figure 4-17: Configuring NTP Server Address



3. Click **Submit**.

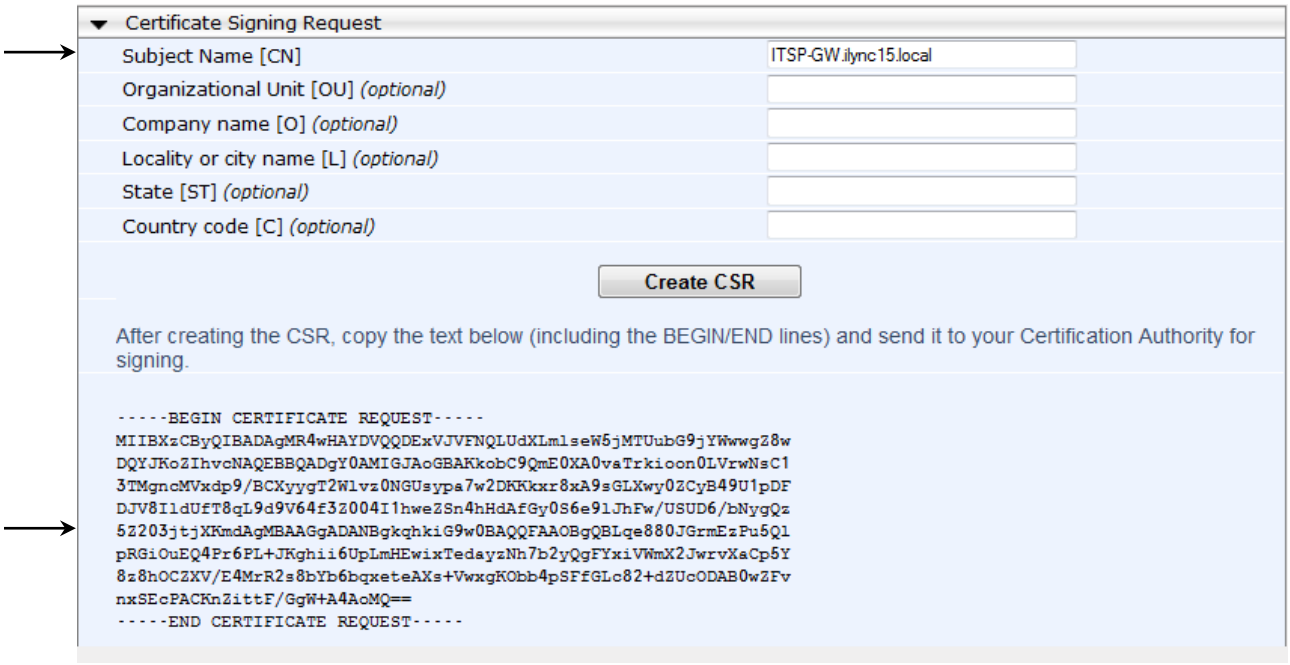
4.8.2 Step 8b: Configure a Certificate

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**).

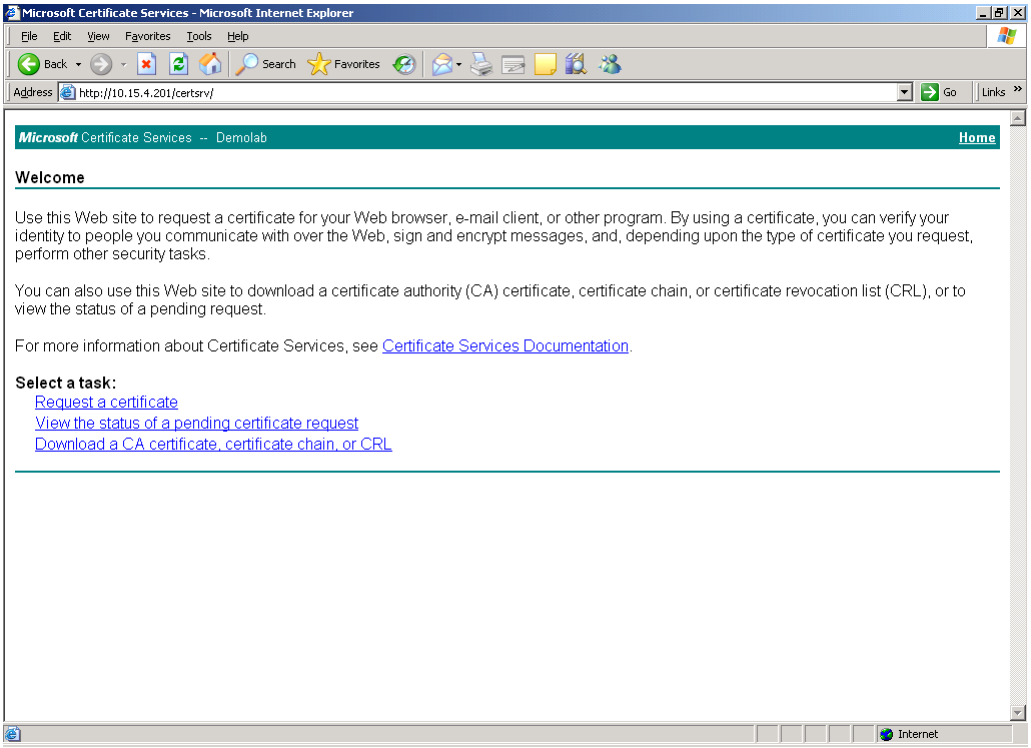
Figure 4-18: Configuring a Certificate - Creating CSR



2. In the Subject Name field, enter the media gateway name (e.g., "ITSP-GW.ilync15.local"). This name must be equivalent 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***.

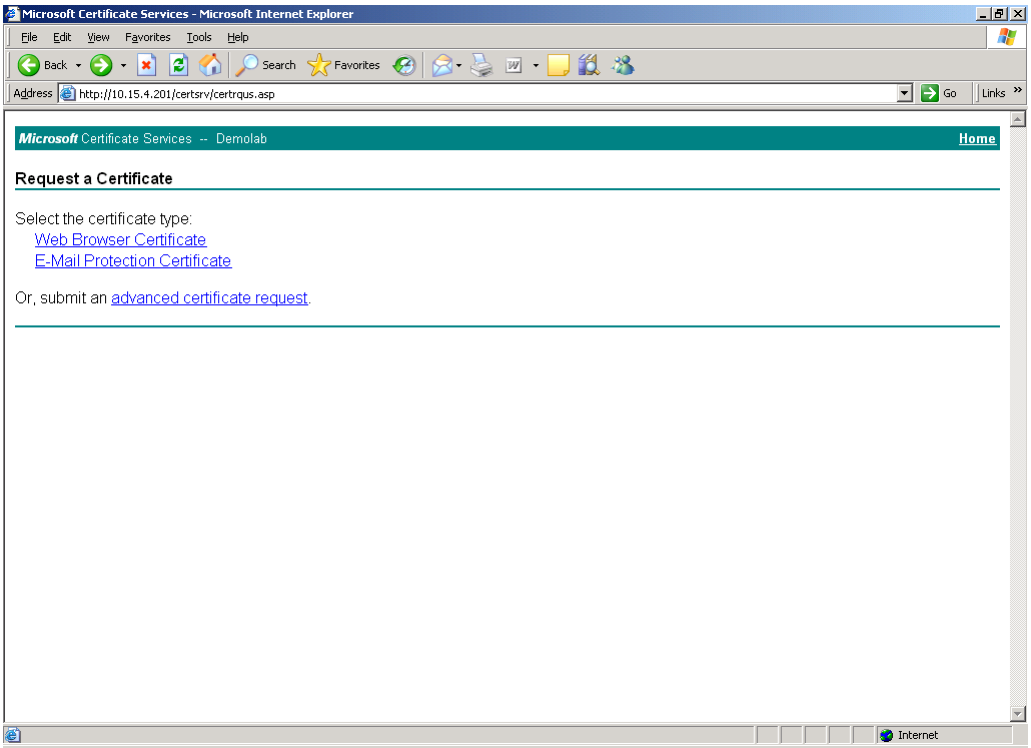
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-19: Displaying Microsoft Certificate Services Web Page



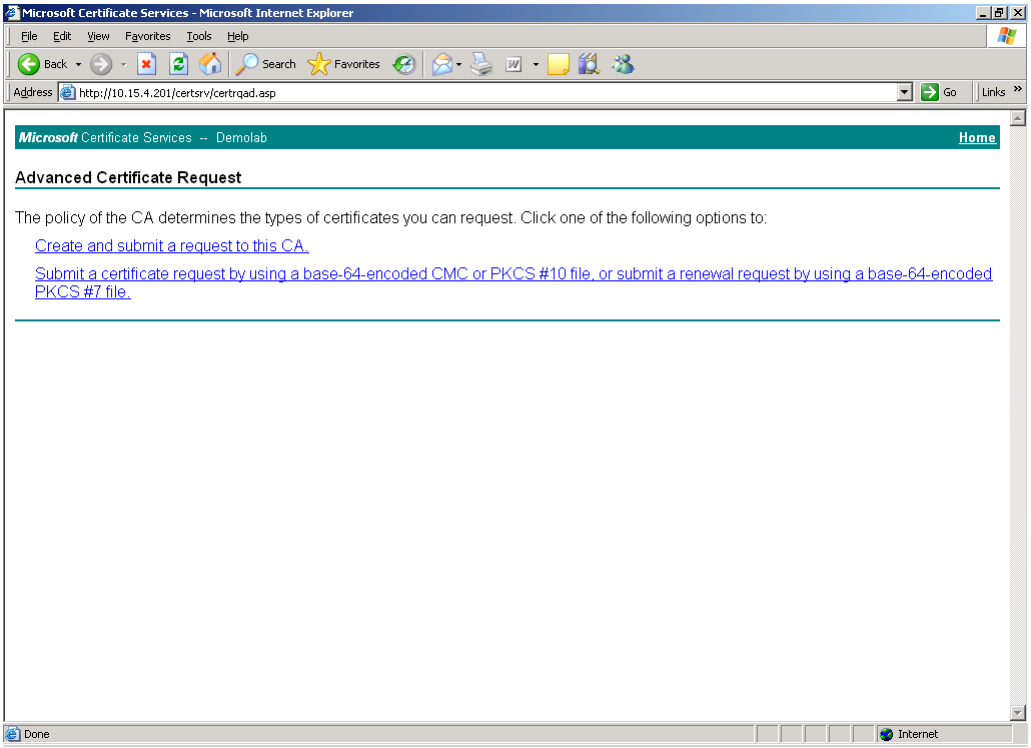
6. Click **Request a certificate**.

Figure 4-20: Requesting a Certificate



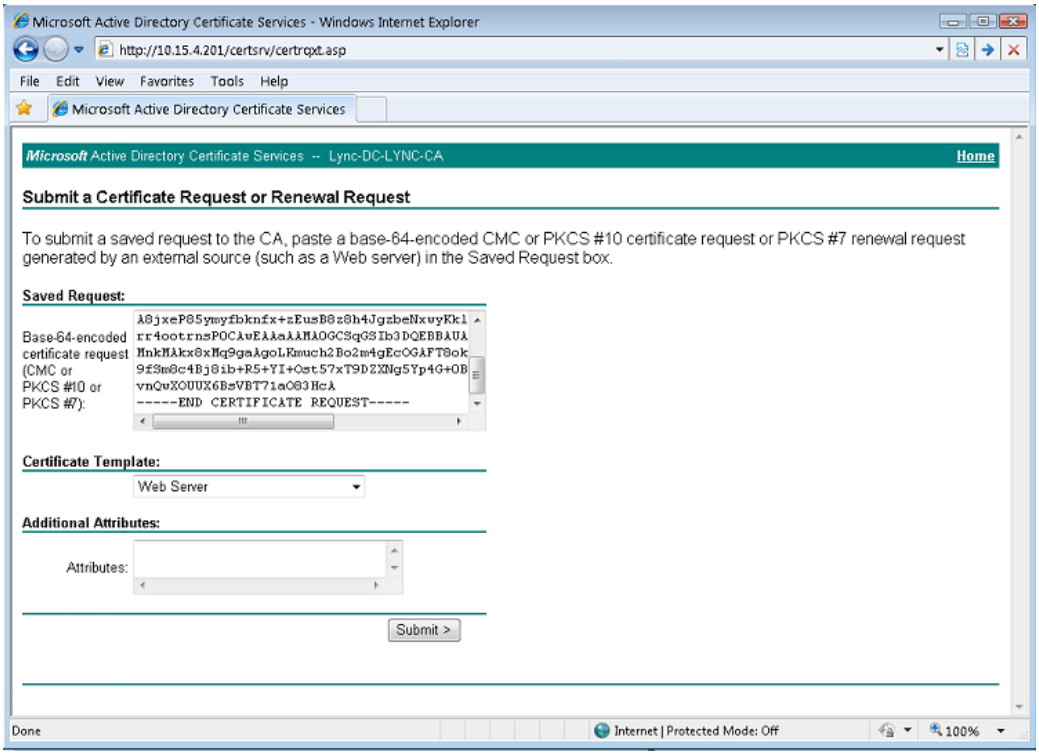
7. Click **advanced certificate request**, and then click **Next**; the following screen appears:

Figure 4-21: Requesting an Advanced Certificate



8. Click **Submit a certificate request ...**, and then click **Next**; the following screen appears:

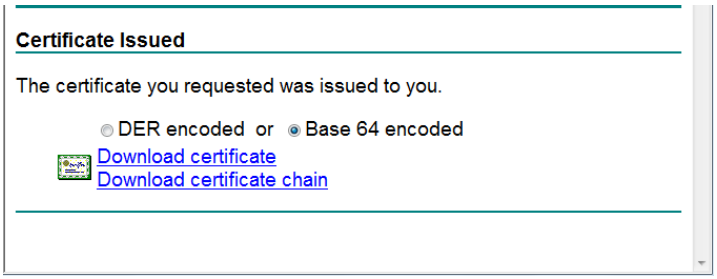
Figure 4-22: Submitting a Certificate Request or Renewal Request Page



9. Open the *certreq.txt* file that you created and saved in Step 4 on page 54, and then copy its contents to the 'Base64 Encoded Certificate Request' field.

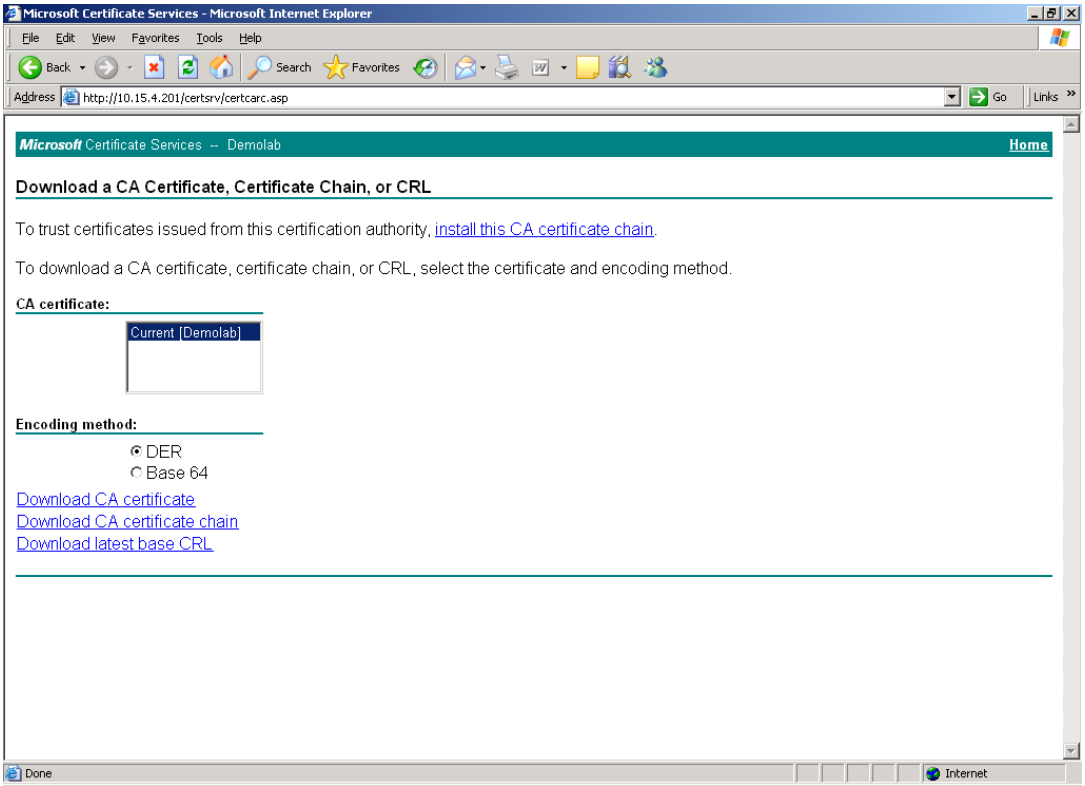
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-23: Displaying Issued Certificate



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 4-24: Downloading a CA Certificate, Certificate Chain, or CRL Page



16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file 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 Section 4.13 on page 69, 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 on page 57, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-25: Uploading a Certificate to E-SBC

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 76).

4.9 Step 9: Configure Media Security

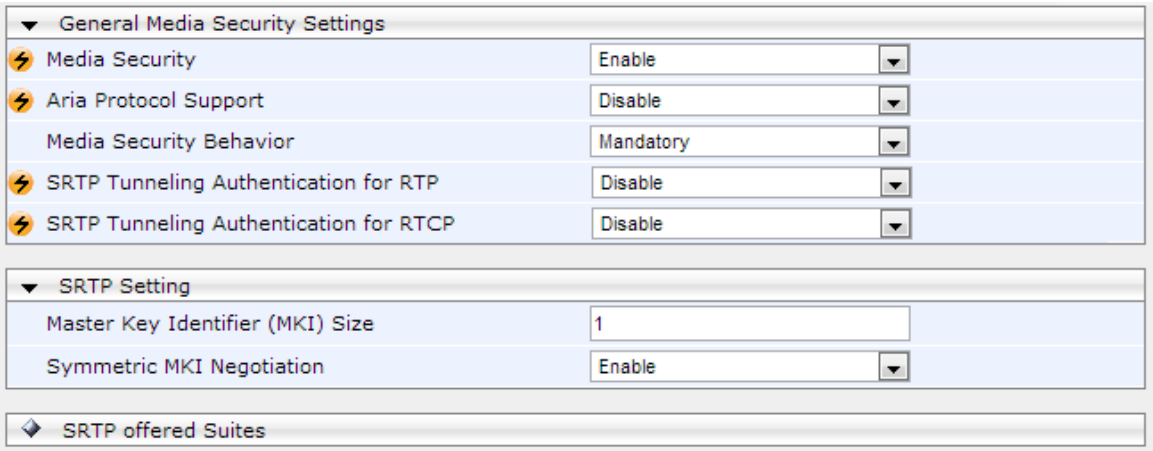
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), you need to configure the E-SBC to operate in the same manner.

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 48).

➢ **To configure media security:**

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

Figure 4-26: Configuring Media Security Settings



2. Configure the parameters as follows:

Parameter	Settings
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 4.16 on page 76).

4.10 Step 10: Configure Number of Media Channels

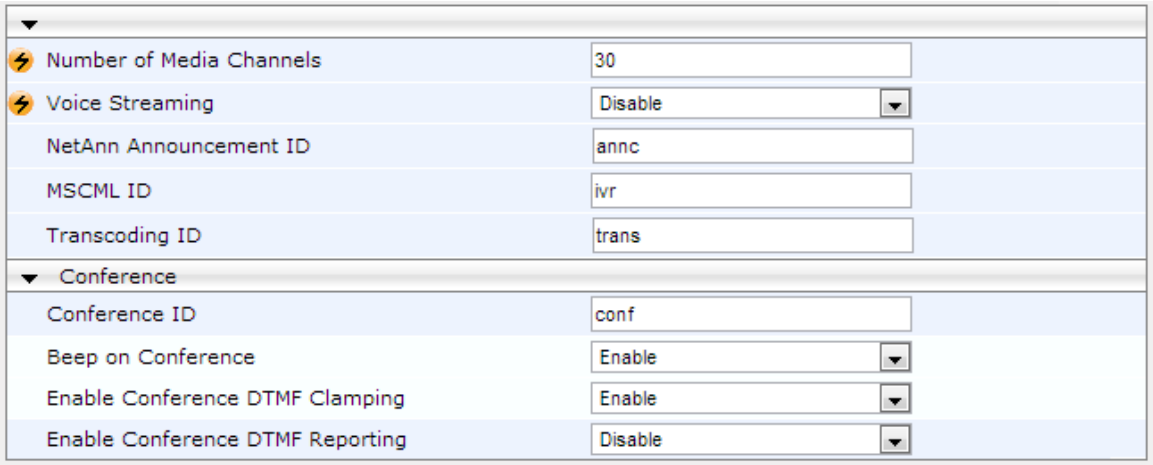
This step describes how to configure the number of media channels for IP-based media. To perform coder transcoding, define digital signaling processors (DSP) channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to sessions.

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

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

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

Figure 4-27: Configuring Number of Media Channels



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

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

This step describes how to configure IP-to-IP call routing rules (which are done 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 our example scenario, you need to add the following IP-to-IP routing rules to route calls between Lync Server 2013 (LAN) and HOT 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.

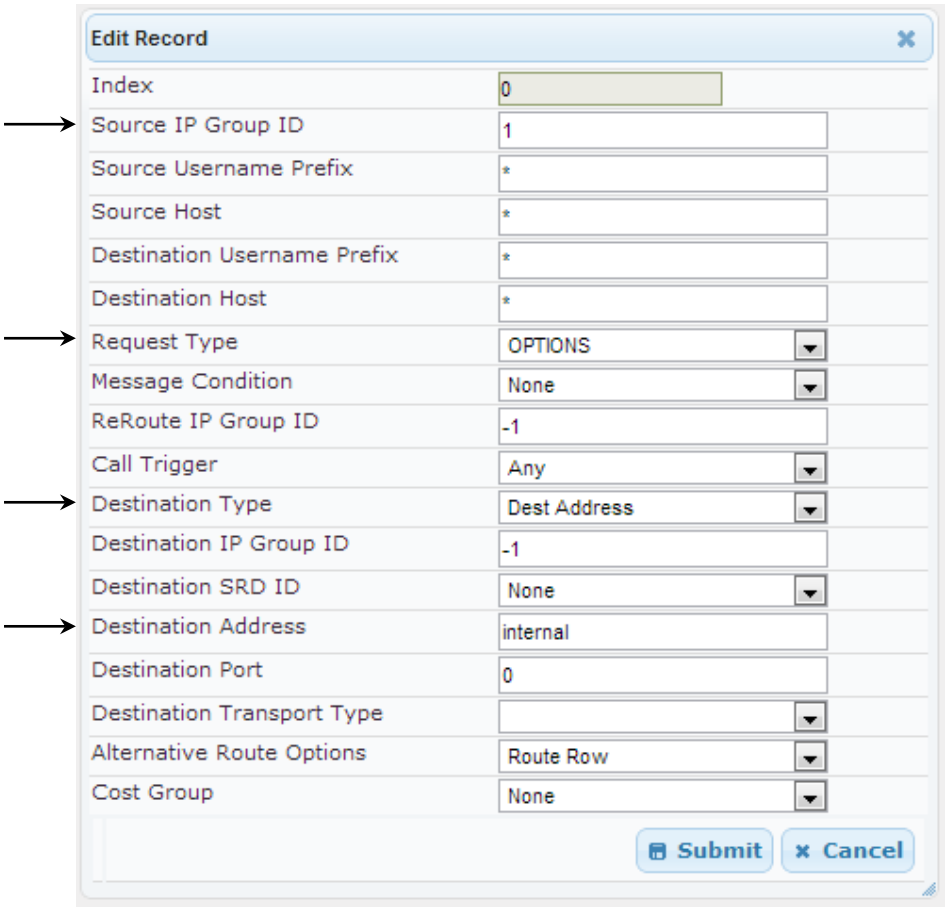
The routing rules use IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 46, IP Group ID 1 was assigned to Lync Server 2013, and IP Group ID 2 to HOT SIP Trunk.

➢ **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	Settings
Index	**0**
Source IP Group ID	**1**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**.

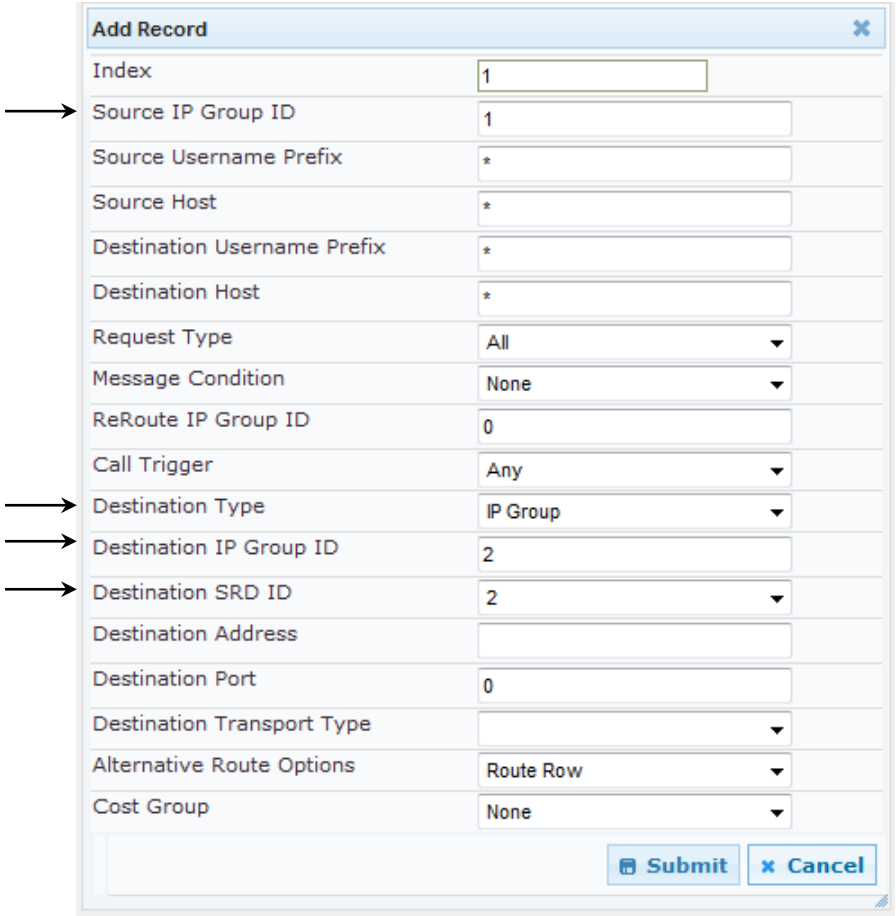
Figure 4-28: Edit Record



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

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

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

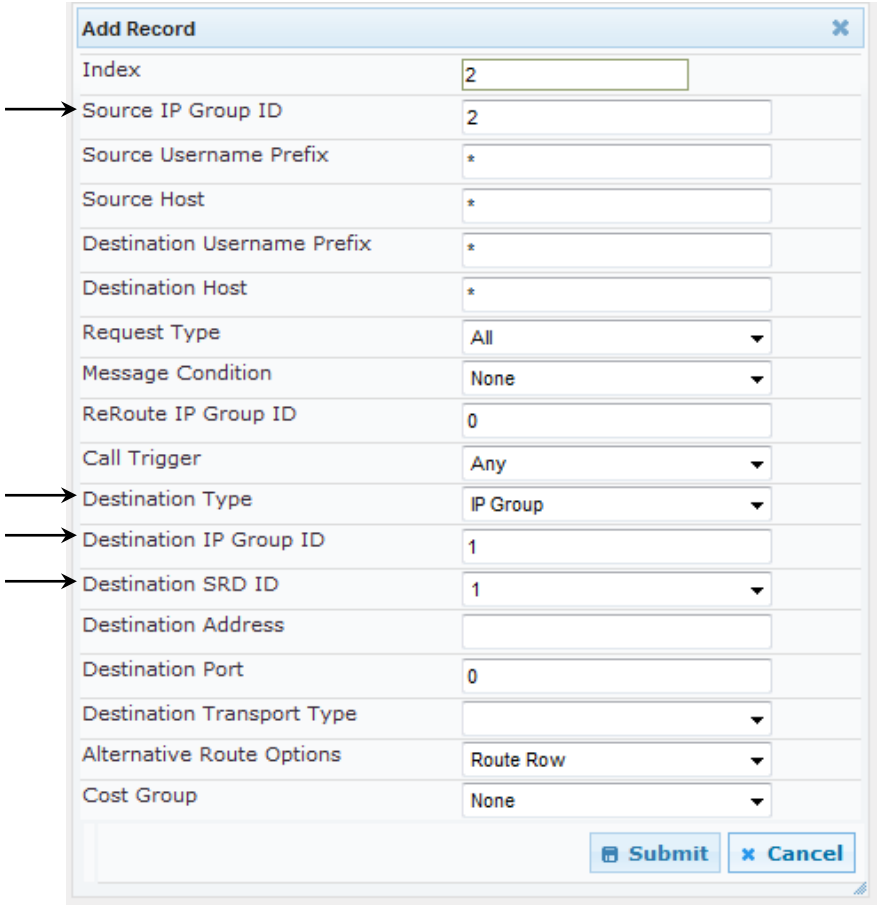


   c. Click **Submit**.

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

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

Figure 4-30: IP-to-IP Routing Rule for WAN to LAN



   c. Click **Submit**.

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

Figure 4-31: IP-to-IP Routing Table

IP-to-IP Routing Table

Add + Insert +

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.

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

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 Section 4.5 on page 46, IP Group ID 1 was assigned to Lync Server 2013 and IP Group ID 2 to the HOT SIP Trunk.

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

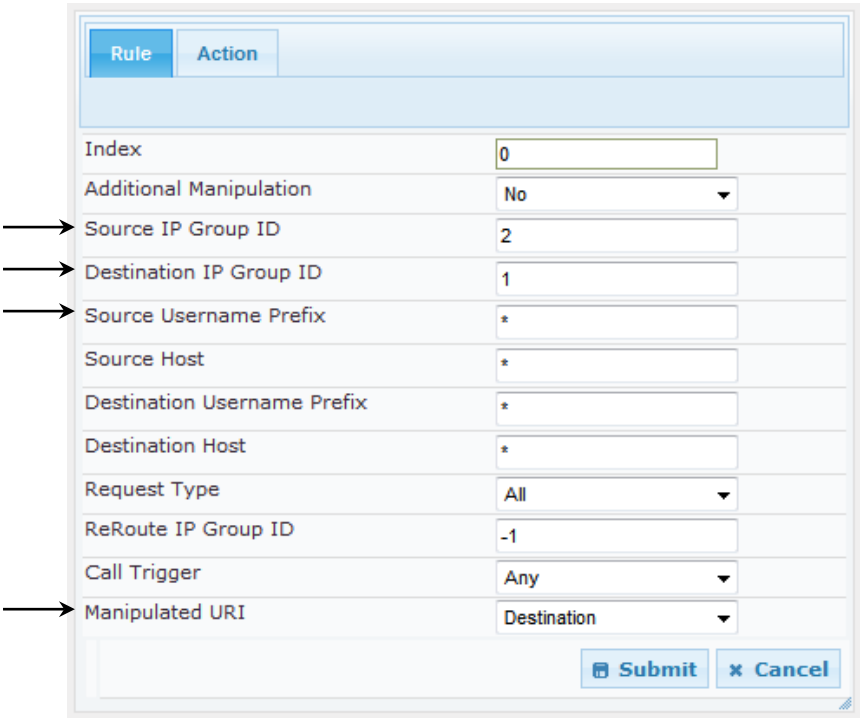
The procedure below provides an example of configuring a manipulation rule that adds the plus sign "+" to the destination number for calls from IP Group 2 (HOT SIP Trunk) destined to IP Group 1 (i.e., Lync Server 2013), when the destination number prefix is any number ("*").

➢ **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	Settings
Index	**0**
Source IP Group ID	**2**
Destination IP Group ID	**1**
Destination Username Prefix	*****
Manipulated URI	**Destination**

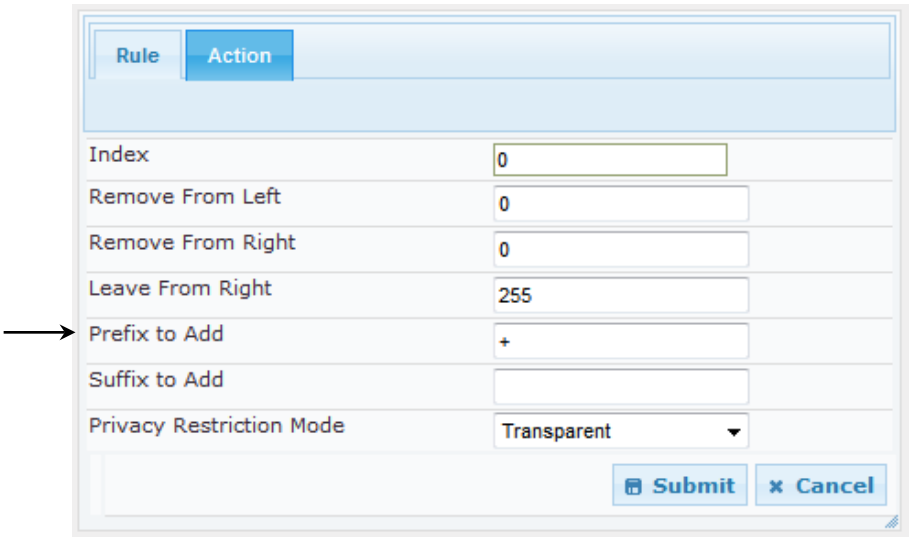
Figure 4-32: IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Prefix to Add	+

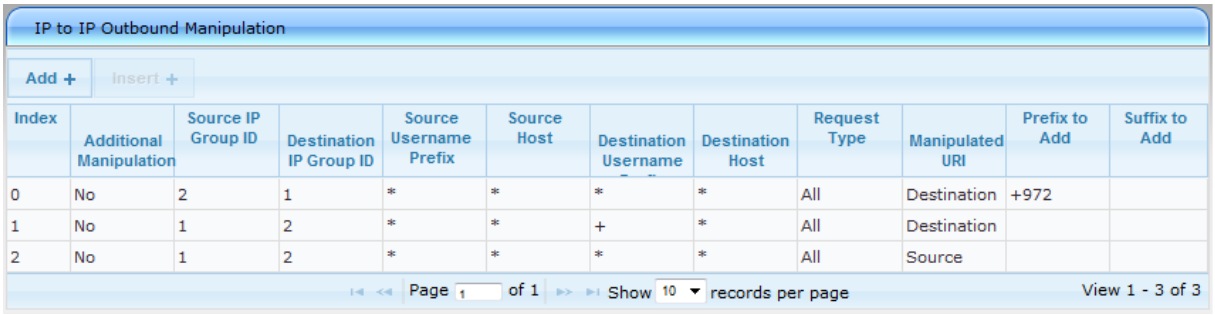
Figure 4-33: IP-to-IP Outbound Manipulation Rule - Action Tab



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., HOT SIP Trunk):

Figure 4-34: IP to IP Outbound Manipulation Table - Example


IP to IP Outbound Manipulation

Add + | Insert +

Index	Additional Manipulation	Source IP Group ID	Destination IP Group ID	Source Username Prefix	Source Host	Destination Username	Destination Host	Request Type	Manipulated URI	Prefix to Add	Suffix to Add
0	No	2	1	*	*	*	*	All	Destination	+972	
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

Rule Index	Description
0	Calls received from IP Group 2 and destined to IP Group 1 that have any destination number (*), remove 1 character and add "+972" to the prefix of the destination number.
1	Calls received from IP Group 1 and destined to IP Group 2 that have a prefix destination number of "+", remove 4 characters from this prefix.
2	Calls received from IP Group 1 and destined to IP Group 2 with any source number, remove 4 characters from this prefix source number.

4.13 Step 13: 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.

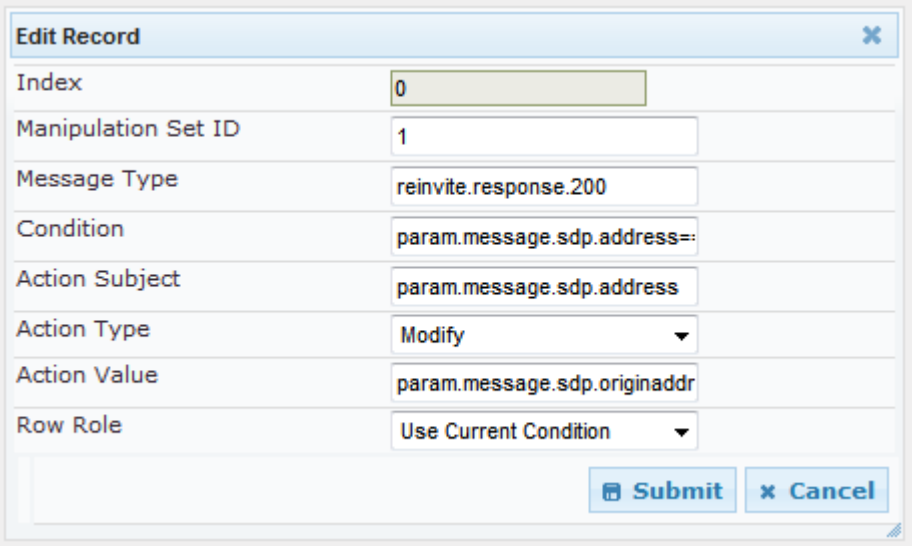
In our example scenario we set a manipulation for SIP 200 OK response for Re-INVITE that in the SDP the IP address is '0.0.0.0' (hold) the manipulation change the IP address to the SBC IP address and change RTP Mode to 'inactive'.

➢ **To configure SIP message manipulation rule for Index 0:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules 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 4-35: SIP Message Manipulation – Index 0

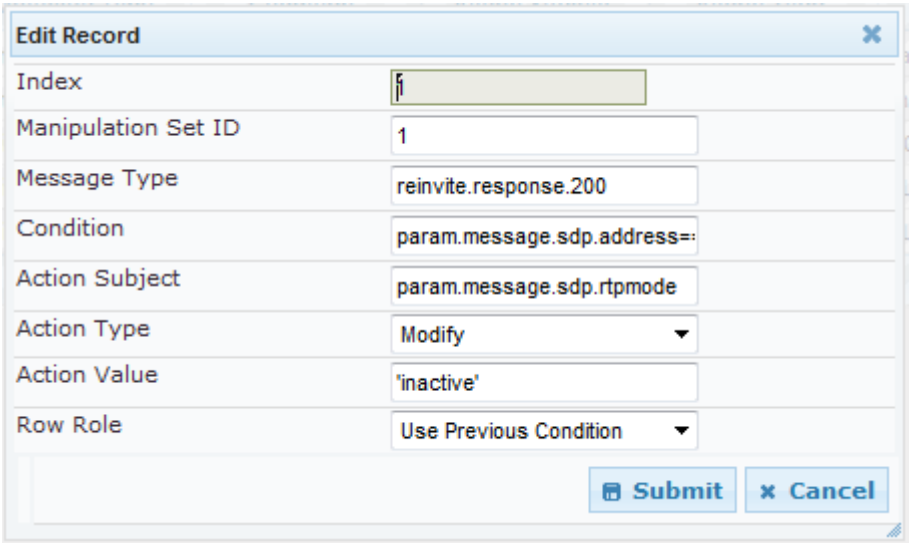


➢ **To configure SIP message manipulation rule for Index 1:**

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

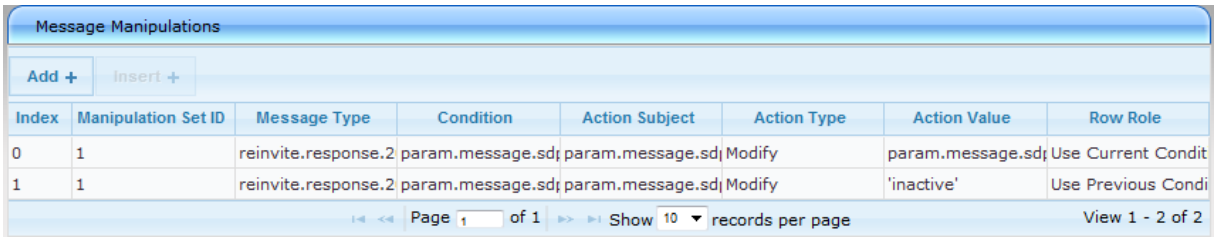
Rule Index	Setting
Index	**1**
Manipulation Set ID	**1**
Message Type	**reinvite.response.200**
Condition	**param.message.sdp.address=='0.0.0.0'**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**inactive**
Row Role	**Use Previous Condition**

Figure 4-36: SIP Message Manipulation – Index 1



The Message Manipulations table below includes SIP message manipulations for SIP 200 OK responses for Re-INVITE that has an IP address of '0.0.0.0' in the SDP. The manipulation (Index 0) changes the IP address to the SBC IP address and (Index 1) changes RTP Mode to 'inactive'.

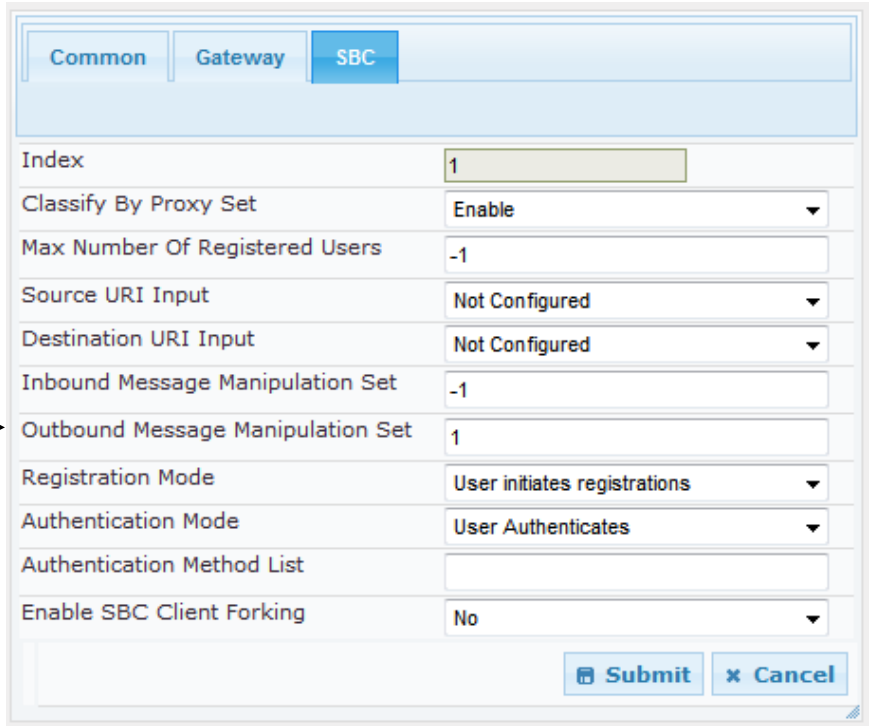
Figure 4-37: SIP Message Manipulation – Example



Rule Index	Description
0	SIP 200 OK response that contains IP address '0.0.0.0' in the SDP. It changes the IP address to the SBC IP address.
1	If the manipulation rule Index 0 (above) is executed, then the following rule is also executed on the same SIP message; the RTP mode is changed to 'inactive'.

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 2, and then click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Outbound Message Manipulation Set' field to "1".

Figure 4-38: Assigning Manipulation Rule to IP Group 1



   e. Click **Submit**.

Reader's Notes

4.14 Step 14: Configure Registration Accounts

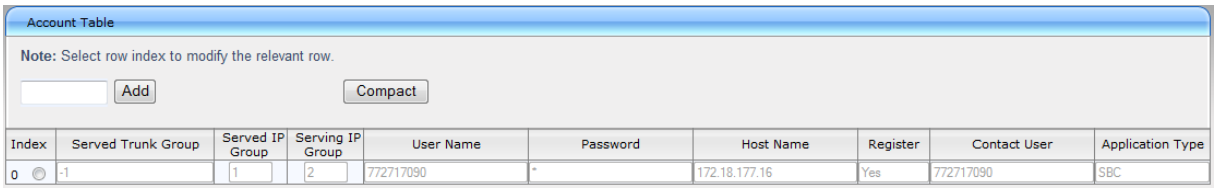
This step describes how to configure SIP registration accounts (in the Account table). This is required so that the E-SBC can register with the HOT SIP Trunk on behalf of Lync Server 2013. The HOT SIP Trunk requires registration and authentication to provide service.

In this example, the **Served** IP Group is Lync Server 2013 (IP Group 1) and the **Serving** IP Group is HOT SIP Trunk (IP Group 2).

➢ **To configure a registration account:**

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

Figure 4-39: Configuring SIP Registration Account



2. Enter an index number (e.g., "0"), and then click **Add**.
3. Configure the account according to the provided information from HOT, for example:

Parameter	Settings
Served IP Group	**1** This is for Lync Server 2013.
Serving IP Group	**2** This is for HOT SIP Trunk.
Username	Set the username as provided by HOT.
Password	Set the password as provided by HOT.
Host Name	**172.18.177.16** This is the Host Name as requested by HOT.
Register	**Yes**
Contact User	**772717090** Set to the trunk main line.
Application Type	**SBC**

4. Click **Apply**.

4.15 Step 15: Miscellaneous Configuration

This step describes miscellaneous E-SBC configuration.

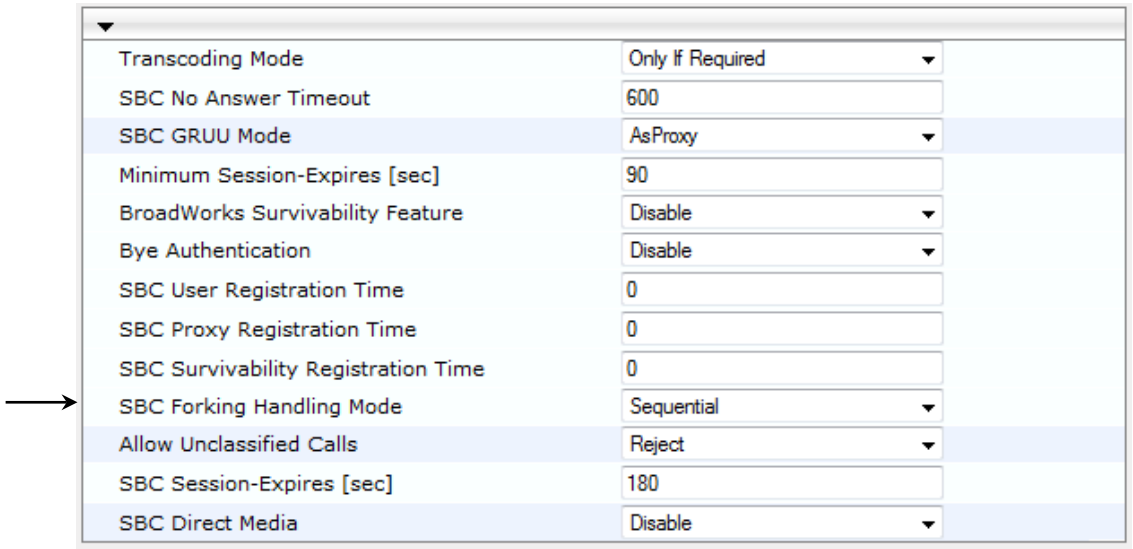
4.15.1 Step 15a: Configure Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received due to call forking of an INVITE. In our example scenario, if a SIP 18x 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 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 4-40: Configuring Forking Mode



3. Click **Submit**.

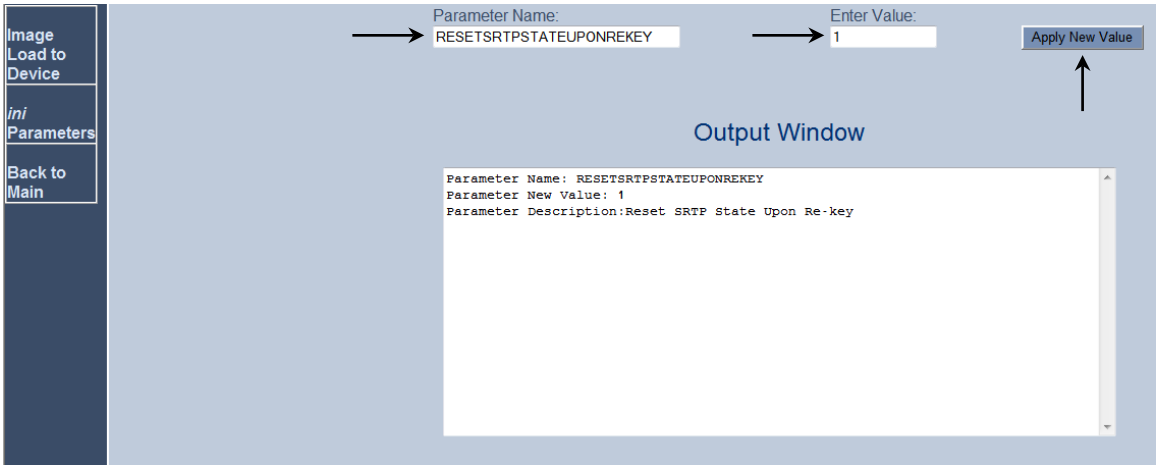
4.15.2 Step 15b: Configure SRTP Behavior upon Rekey Mode

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

➢ **To configure SRTP upon re-key:**

1. Open the Admin page: append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.15.17.10/AdminPage).
2. In the left pane, click ***ini* Parameters**.

Figure 4-41: Configuring SRTP Behavior upon Rekey Mode in AdminPage



3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
RESETSRTPSTATEUPONREKEY	**1** This enables Reset SRTP State Upon Re-key

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

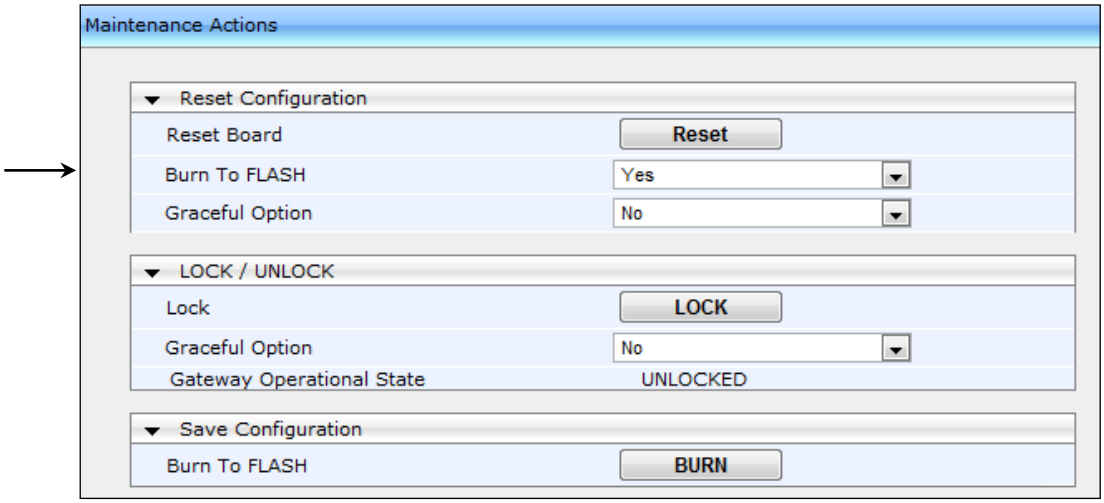
4.16 Step 16: Reset the E-SBC

After you have completed the E-SBC configuration as described in the previous steps, you need to 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 4-42: Resetting the E-SBC



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

A AudioCodes INI File

The *ini* file configuration of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 33, is shown below:

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

;Board: Mediant 800 - MSBG
;Board Type: 69
;Serial Number: 2542001
;Slot Number: 1
;Software Version: 6.60A.216.006
;DSP Software Version: 5014AE3_R_LD => 660.21
;Board IP Address: 10.15.17.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 368M   Flash size: 64M
;Num of DSP Cores: 1  Num DSP Channels: 22
;Num of physical LAN ports: 12
;Profile: NONE
;Key features:;Board Type: Mediant 800 - MSBG ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;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 ;PSTN FALLBACK Supported ;E1Trunks=1 ;T1Trunks=1
;Channel Type: RTP DspCh=30 IPMediaDspCh=30 ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;DSP Voice features:
IpmDetector RTCP-XR AMRPolicyManagement V150=50 ;IP Media: Conf
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;SS7 Links:
M3UA=1 ;PSTN Protocols: IUA=1 ;Control Protocols: MGCP MEGACO H323
SIP TPNCP SASurvivability SBC=50 MSFT CLI TRANSCODING=50 FEU=5
TestCall=5 ;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 = 10.15.2.9
EnableSyslog = 1
NTPServerUTCOffset = 7200
NTPServerIP = '10.15.25.1'
LDAPSEARCHDNSINPARALLEL = 0
```

```
[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

[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 = 30
REGISTRATIONTIME = 3600
GWDEBUGLEVEL = 0
MEDIASECURITYBEHAVIOUR = 1
ENABLESBCAPPLICATION = 1
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, 2, 4, "User Port #2",
"GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3",
"GROUP_2", "Redundant";
PhysicalPortsTable 4 = "FE_5_1", 1, 1, 4, "User Port #4",
"GROUP_3", "Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 1, 4, "User Port #5",
"GROUP_3", "Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 1, 4, "User Port #6",
"GROUP_4", "Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 1, 4, "User Port #7",
"GROUP_4", "Redundant";
PhysicalPortsTable 8 = "FE_5_5", 1, 1, 4, "User Port #8",
"GROUP_5", "Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 1, 4, "User Port #9",
"GROUP_5", "Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 1, 4, "User Port #10",
"GROUP_6", "Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 1, 4, "User Port #11",
"GROUP_6", "Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1,
EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, GE_4_1, GE_4_2;
EtherGroupTable 1 = "GROUP_2", 2, GE_4_3, GE_4_4;
EtherGroupTable 2 = "GROUP_3", 2, FE_5_1, FE_5_2;
```

```
EtherGroupTable 3 = "GROUP_4", 2, FE_5_3, FE_5_4;
EtherGroupTable 4 = "GROUP_5", 2, FE_5_5, FE_5_6;
EtherGroupTable 5 = "GROUP_6", 2, FE_5_7, FE_5_8;

[ \EtherGroupTable ]


[ 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, 10.15.17.10, 16, 10.15.0.1, 1, "LAN-
Lync", 10.15.25.1, 0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 10.9.81.6, 28, 10.9.81.1, 2, "WAN-HOT",
0.0.0.0, 0.0.0.0, GROUP_2;

[ \InterfaceTable ]



[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF,
CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault;
CpMediaRealm 1 = "LanRealm", LAN-Lync, , 6000, 10, 6090, 1;
CpMediaRealm 2 = "WanRealm", WAN-HOT, , 7000, 10, 7090, 0;

[ \CpMediaRealm ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm,
SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers,
SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "SRDLan", "LanRealm", 0, 0, -1, 1;
SRD 2 = "SRDWan", "WanRealm", 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 = "172.18.177.16:5060", 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 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, 1, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 3, 1, 1,
0, 3, 2, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, -1, 0, 0, 1, 0, 0;
IpProfile 2 = "HOT SIP Trunk", 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, 2, 0, 2, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3,
0, 2, 2, 1, 3, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, -1, 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 = 0, 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, "", "", 0, -1, -1, 0, -1, 1,
"LanRealm", 1, 1, -1, -1, 1, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "HOT SIP Trunk", 2, "172.18.177.16", "", 0, -1, -1,
0, -1, 2, "WanRealm", 1, 2, -1, -1, 2, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroup, Account_ServingIPGroup, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, 1, 2, "772717090", *, "172.18.177.16", 1,
"772717090", 2;

[ \Account ]


[ 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 = "LAN-Lync", 2, 0, 0, 5067, 1, , -1, 0, 500;
SIPInterface 2 = "WAN-HOT", 2, 5060, 0, 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, 1, 0, 255, "+972", "", 0;
IPOutboundManipulation 1 = 0, 1, 2, "*", "*", "+", "*", 0, -1, 0,
1, 4, 0, 255, "", "", 0;
IPOutboundManipulation 2 = 0, 1, 2, "*", "*", "*", "*", 0, -1, 0,
0, 4, 0, 255, "", "", 0;
```

```
[ \IPOutboundManipulation ]


 [ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g711Ulaw64k";
AllowedCodersGroup2 1 = "g711Alaw64k";

[ \AllowedCodersGroup2 ]


[ 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 1 = 1, "reinvite.response.200",
"param.message.sdp.address=='0.0.0.0'",
"param.message.sdp.rtpmode", 2, "'inactive'", 1;

[ \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

AudioCodes

Configuration Note

www.audiocodes.com