

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

Version 7.0



Microsoft Partner
Gold Communications



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	Twilio SIP Trunking Version	9
2.3	Microsoft Lync Server 2013 Version	9
2.4	Interoperability Test Topology.....	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring Lync Server 2013	13
3.1	Configuring the E-SBC as an IP / PSTN Gateway.....	13
3.2	Configuring the "Route" on Lync Server 2013	21
4	Configuring AudioCodes E-SBC.....	31
4.1	Step 1: Configure IP Network Interfaces.....	32
4.1.1	Step 1a: Configure VLANs	33
4.1.2	Step 1b: Configure Network Interfaces.....	34
4.2	Step 2: Enable the SBC Application.....	36
4.3	Step 3: Configure Media Realms	37
4.4	Step 4: Configure SIP Signaling Interfaces.....	39
4.5	Step 5: Configure Proxy Sets.....	41
4.6	Step 6: Configure IP Profiles.....	45
4.7	Step 7: Configure IP Groups	51
4.8	Step 8: Configure Allowed Coder.....	53
4.9	Step 9: Configure the SIP TLS Connection.....	54
4.9.1	Step 9a: Configure the NTP Server Address.....	54
4.9.2	Step 9b: Configure a Certificate for Operation with Microsoft Lync Server 2013....	55
4.9.3	Step 9c: Configure a Certificate for work with Twilio SIP Trunk.....	60
4.10	Step 10: Configure SRTP.....	61
4.11	Step 11: Configure Maximum IP Media Channels	62
4.12	Step 12: Configure IP-to-IP Call Routing Rules	63
4.13	Step 13: Configure Message Manipulation Rules	70
4.14	Step 14: Configure Miscellaneous Settings	75
4.14.1	Step 14a: Configure Classification Table	75
4.14.2	Step 14b: Configure Call Forking Mode	78
4.14.3	Step 14c: Disable Lifetime in Crypto Line of SDP	79
4.15	Step 15: Reset the E-SBC	80
A	AudioCodes INI File for UDP/RTP	81
B	AudioCodes INI File for TLS/SRTP	91

This page is intentionally left blank.

Notice

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

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

© Copyright 2015 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: Nov-17-2015

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX and One Box 365 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 services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Document Revision Record

LTRT	Description
12410	Initial document release for Version 7.0.
12411	Miscellaneous formatting.
12412	TLS/SRTP configuration for Twilio added.

Documentation Feedback

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

1 Introduction

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

1.1 Intended Audience

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

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	§ Mediant 500 E-SBC § Mediant 800 Gateway & E-SBC § Mediant 1000B Gateway & E-SBC § Mediant 3000 Gateway & E-SBC § Mediant 2600 E-SBC § Mediant 4000 E-SBC
Software Version	§ SIP_F7.00A.013.015 § SIP_F7.00A.043.004
Protocol	§ SIP/UDP (to the Twilio SIP Trunk) § SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 Twilio SIP Trunking Version

Table 2-2: Twilio Version

Vendor/Service Provider	Twilio
SSW Model/Service	Twilio
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Server 2013 Version

Table 2-3: Microsoft Lync Server 2013 Version

Vendor	Microsoft
Model	Microsoft Lync
Software Version	Release 2013 5.0.8308.872
Protocol	SIP
Additional Notes	None

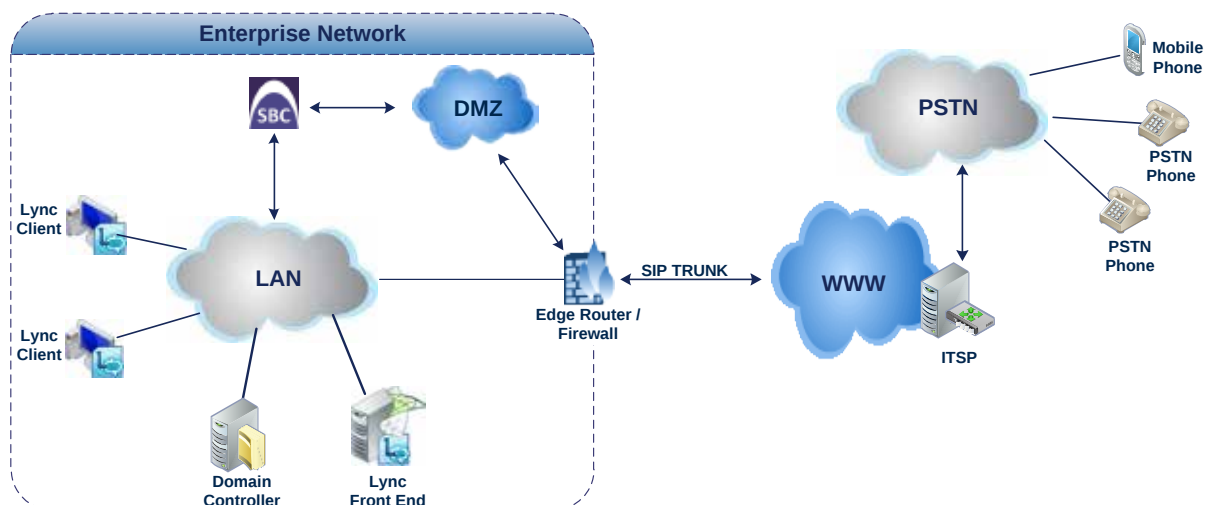
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Twilio SIP Trunk with Lync 2013 was done using the following topology setup:

- n Enterprise deployed with Microsoft Lync Server 2013 in its private network for enhanced communication within the Enterprise.
- n Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Twilio's SIP Trunking service.
- n 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 Twilio's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

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



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	§ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN § Twilio SIP Trunk is located on the WAN
Signaling Transcoding	§ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type § Twilio SIP Trunk operates with SIP-over-UDP or SIP-over-TLS transport types
Codecs Transcoding	§ Microsoft Lync Server 2013 supports a wide range of coders § Twilio SIP Trunk supports G.711U-law coder only
Media Transcoding	§ Microsoft Lync Server 2013 operates with SRTP media type § Twilio SIP Trunk operates with RTP or SRTP media types

2.4.2 Known Limitations

The following limitation was observed in the Interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and Twilio's SIP Trunk:

- n There is a 120 seconds broken connection timeout defined on the Twilio SIP Trunk. Consequently, the SIP trunk always expects to receive RTP packets. When a call is muted or placed on Hold, no packets are sent from the Microsoft Lync Server 2013 side. To resolve this issue, Force Transcoding should be enabled in the E-SBC IP Profile (see Section 4.6 on page 45).

This page is intentionally left blank.

3 Configuring Lync Server 2013

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



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

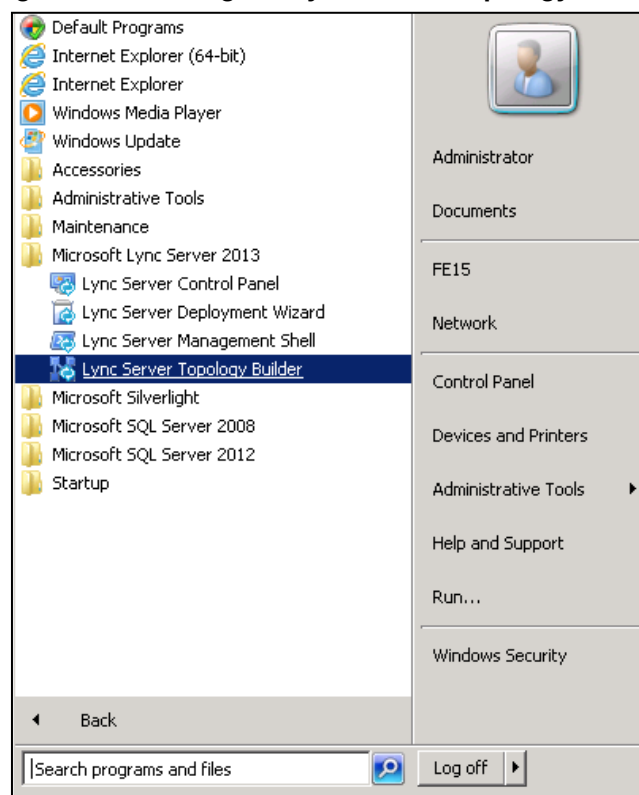
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

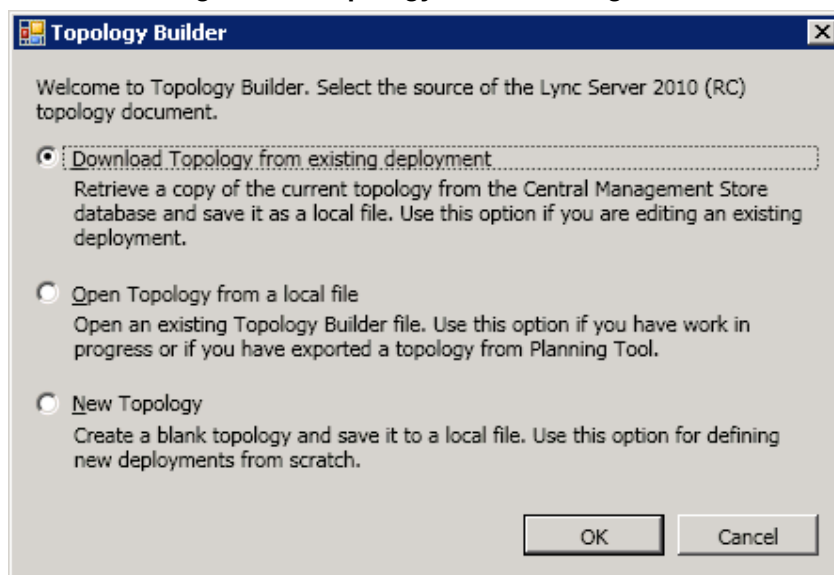
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



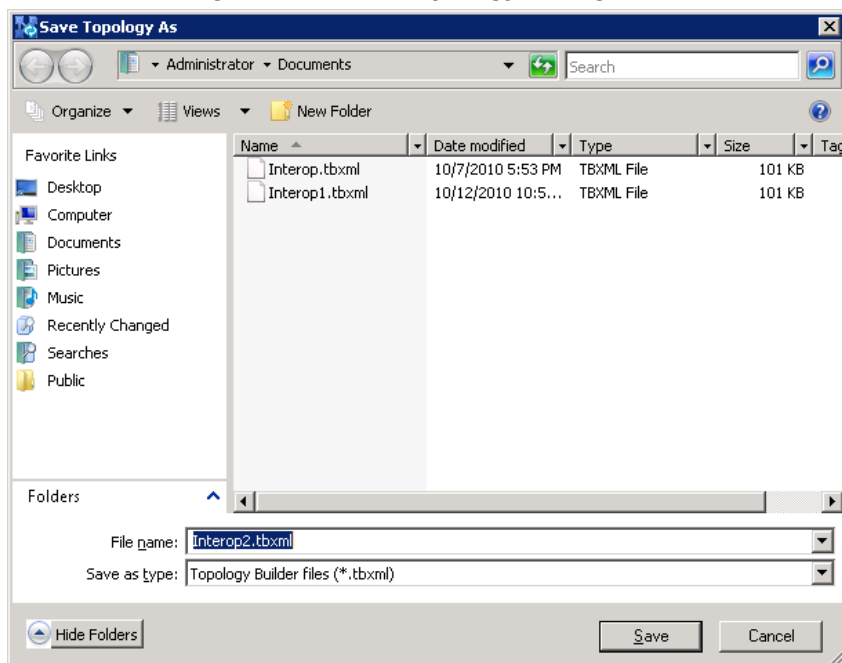
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

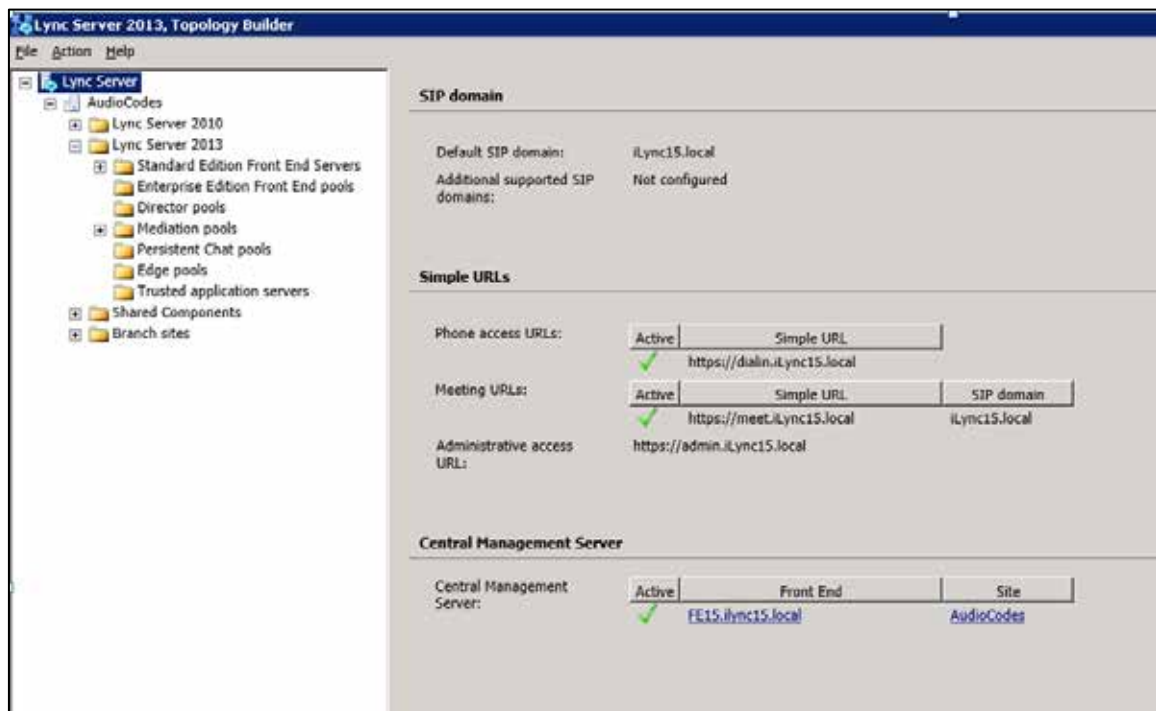
Figure 3-3: Save Topology Dialog Box



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

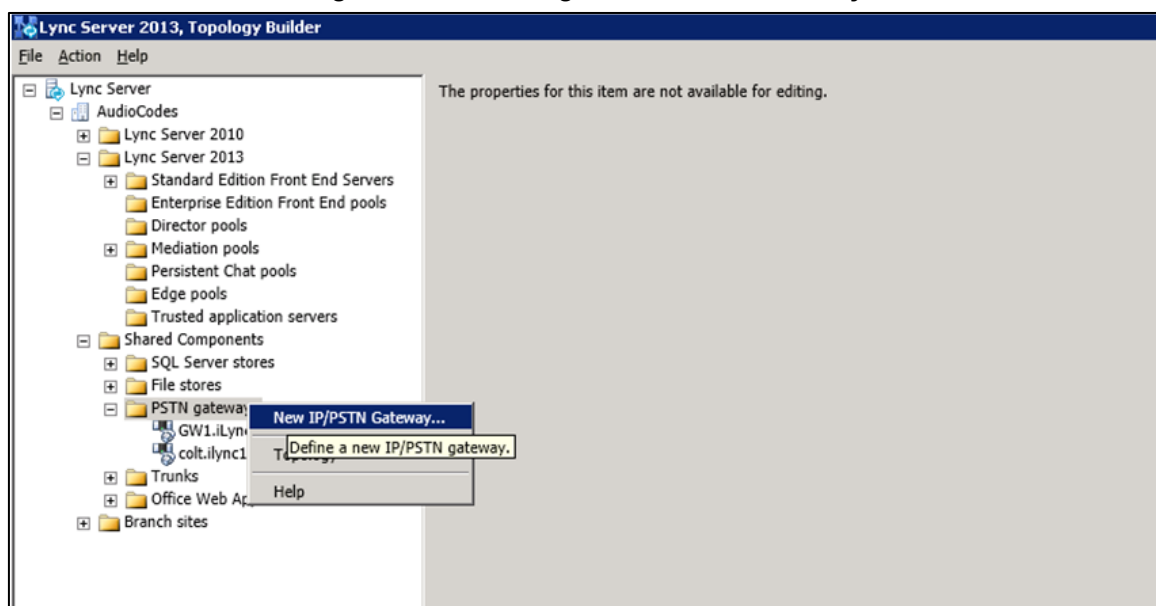
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



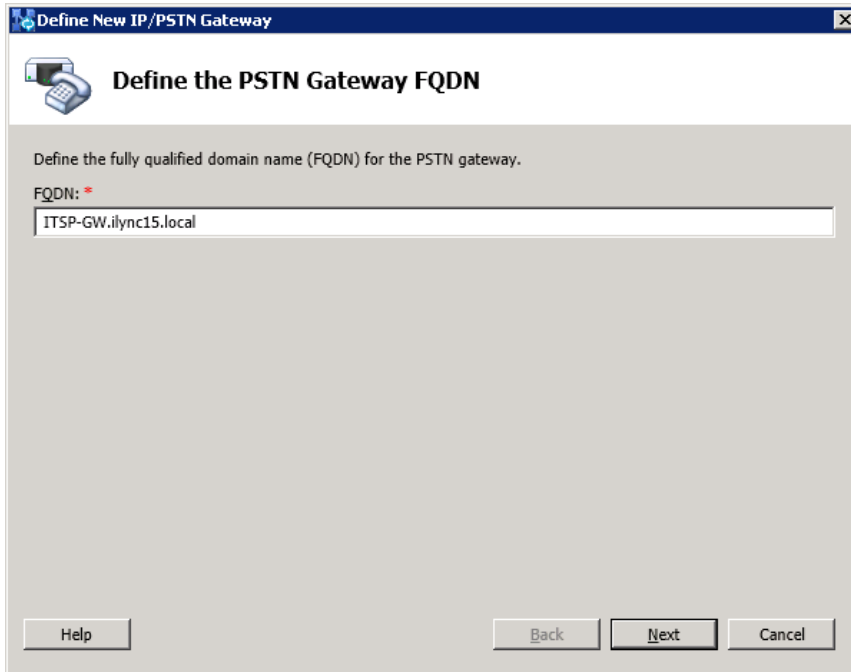
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

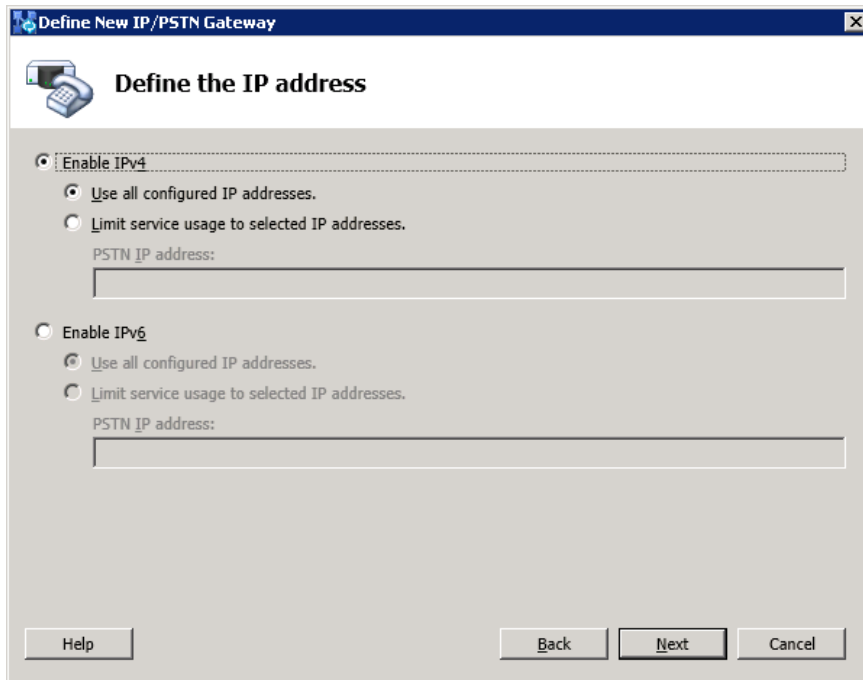
Figure 3-6: Define the PSTN Gateway FQDN



The screenshot shows a window titled "Define New IP/PSTN Gateway" with a sub-header "Define the PSTN Gateway FQDN". Below the sub-header is a text box labeled "FQDN: *" containing the text "ITSP-GW.ilync15.local". At the bottom of the window are three buttons: "Help", "Back", and "Next", and a "Cancel" button.

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

Figure 3-7: Define the IP Address



The screenshot shows a window titled "Define New IP/PSTN Gateway" with a sub-header "Define the IP address". Below the sub-header are two radio button options: "Enable IPv4" (selected) and "Enable IPv6". Each option has two sub-options: "Use all configured IP addresses." and "Limit service usage to selected IP addresses.". Below each sub-option is a text box labeled "PSTN IP address:". At the bottom of the window are three buttons: "Help", "Back", and "Next", and a "Cancel" button.

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

**Notes:**

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

Figure 3-8: Define the Root Trunk

Define 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

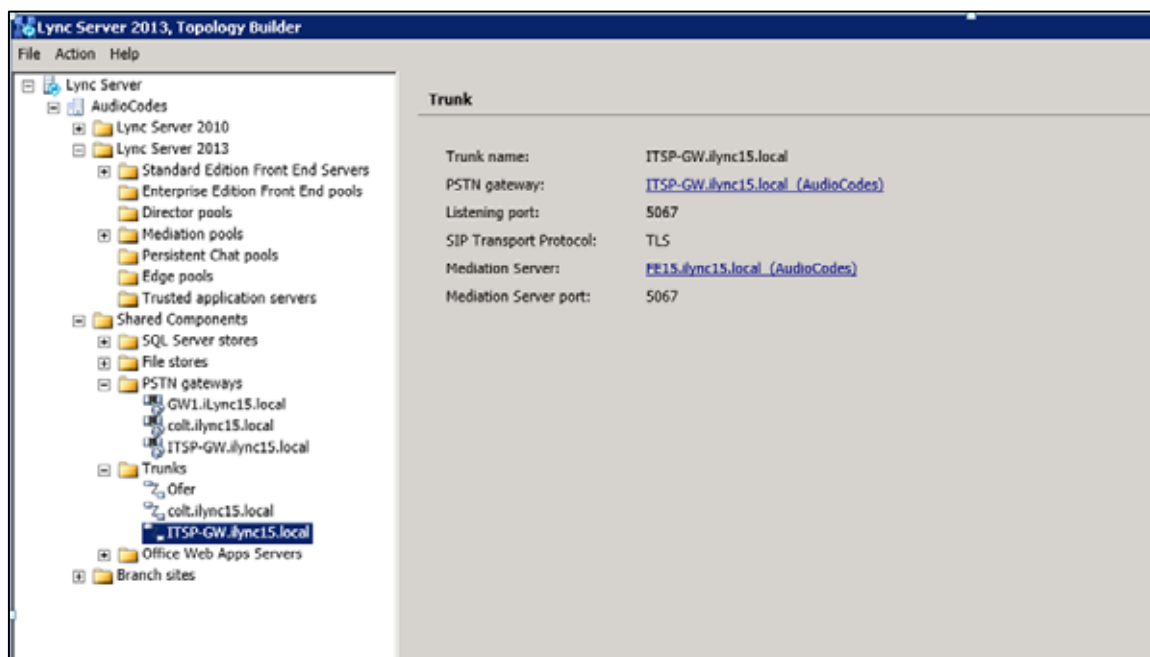
Associated Mediation Server port: *
5067

Help Back Finish Cancel

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

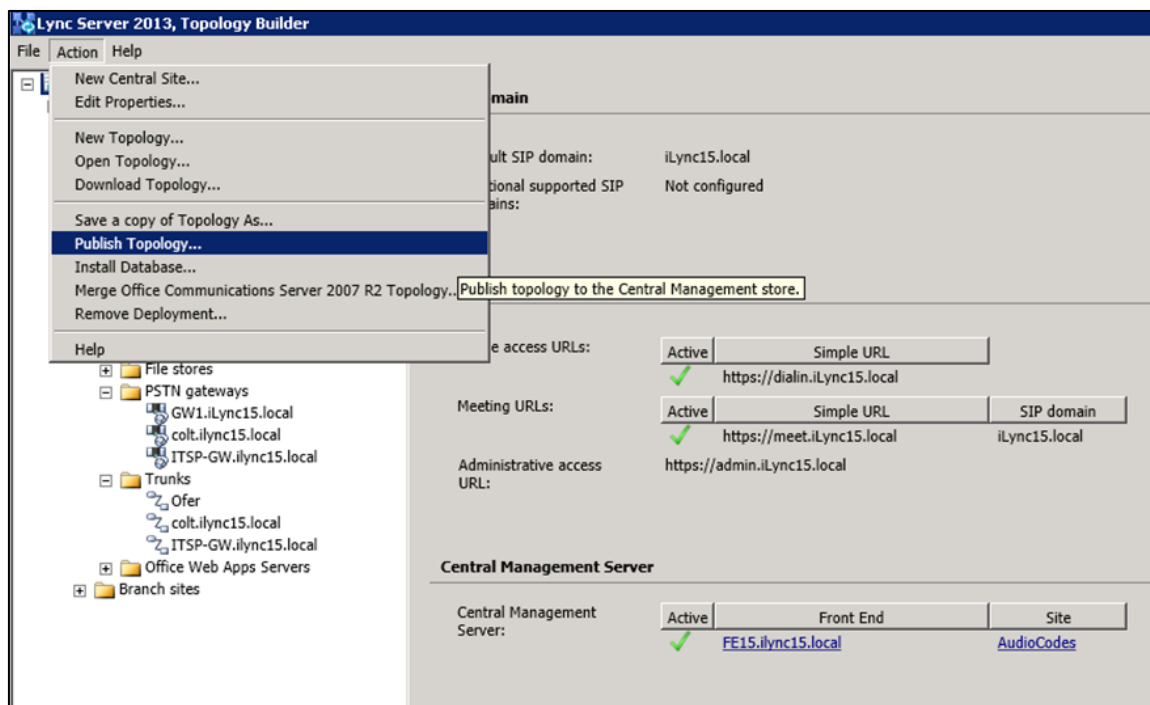
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



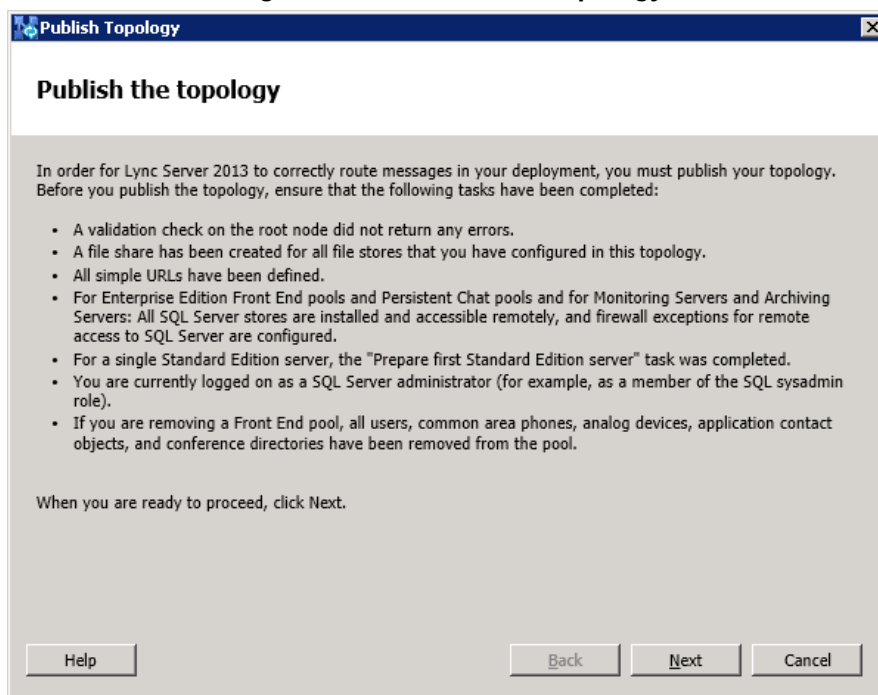
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



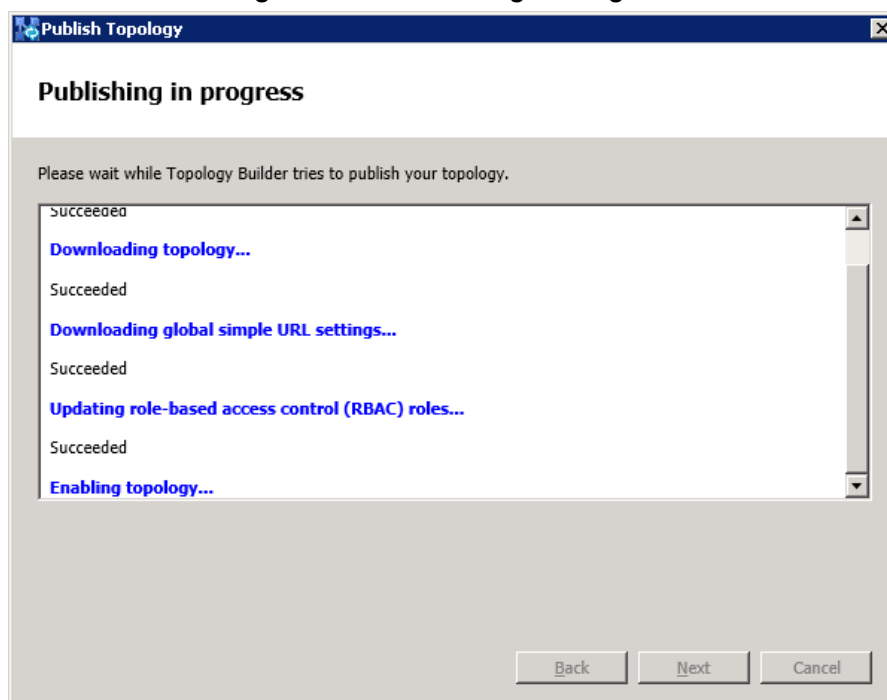
The following is displayed:

Figure 3-11: Publish the Topology



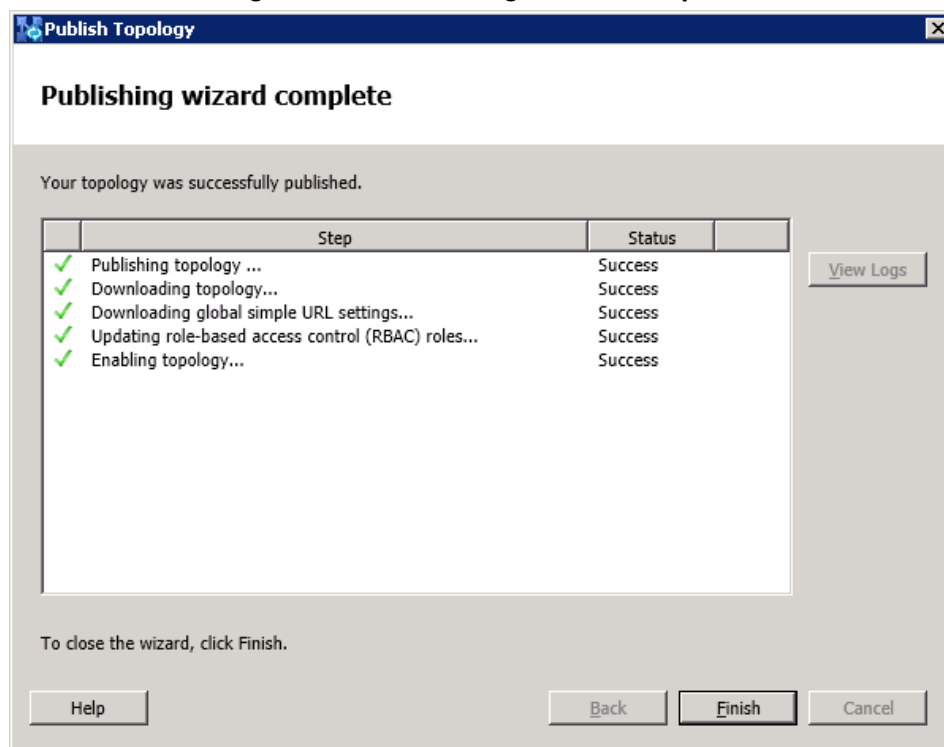
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. Click **Finish**.

3.2 Configuring the "Route" on Lync Server 2013

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

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

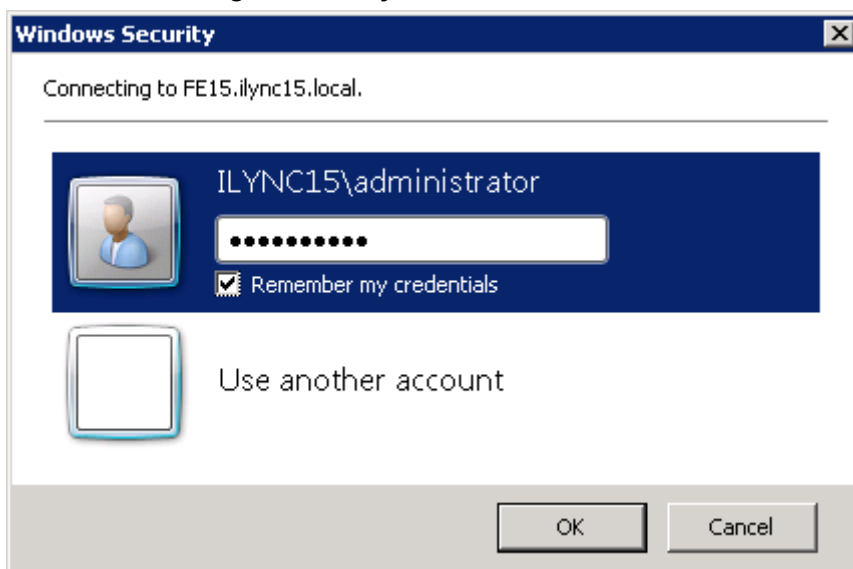
1. Start the Microsoft Lync Server 2013 Control Panel (**Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel**), as shown below:

Figure 3-14: Opening the Lync Server Control Panel



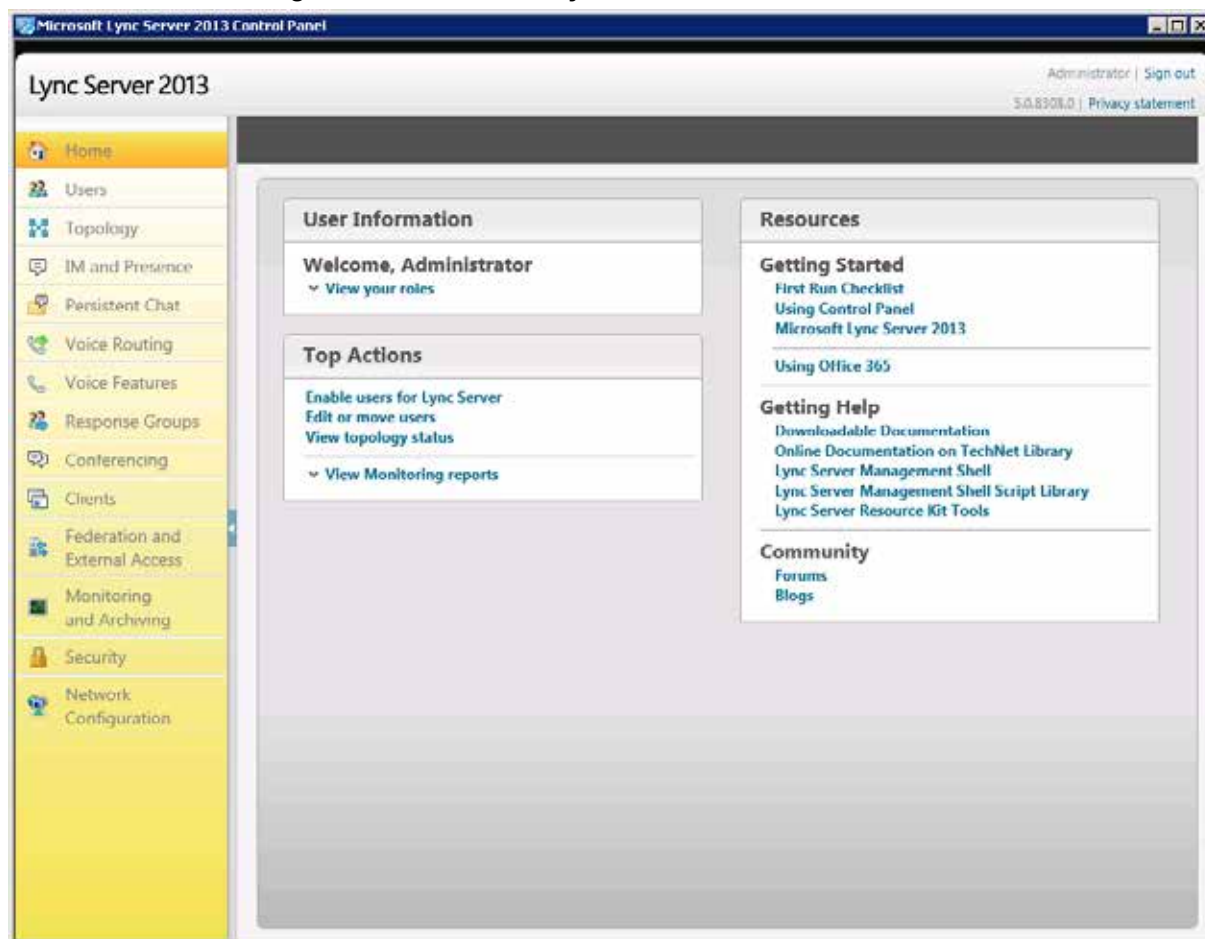
2. You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



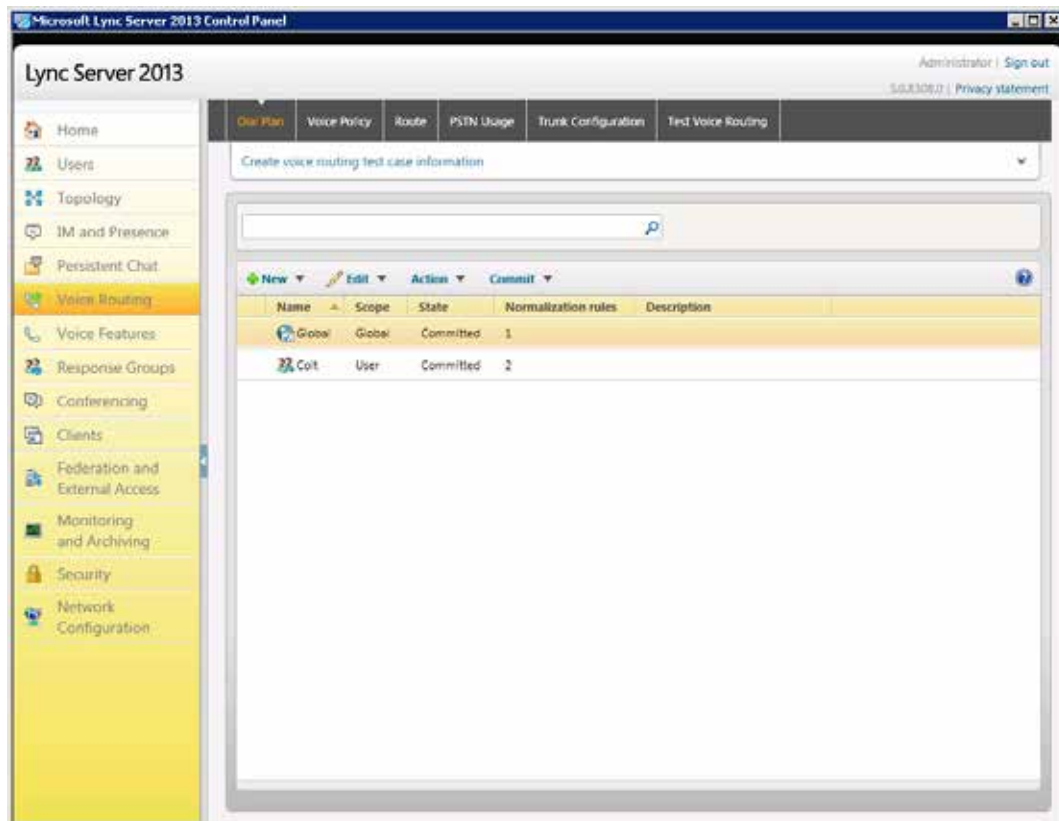
3. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



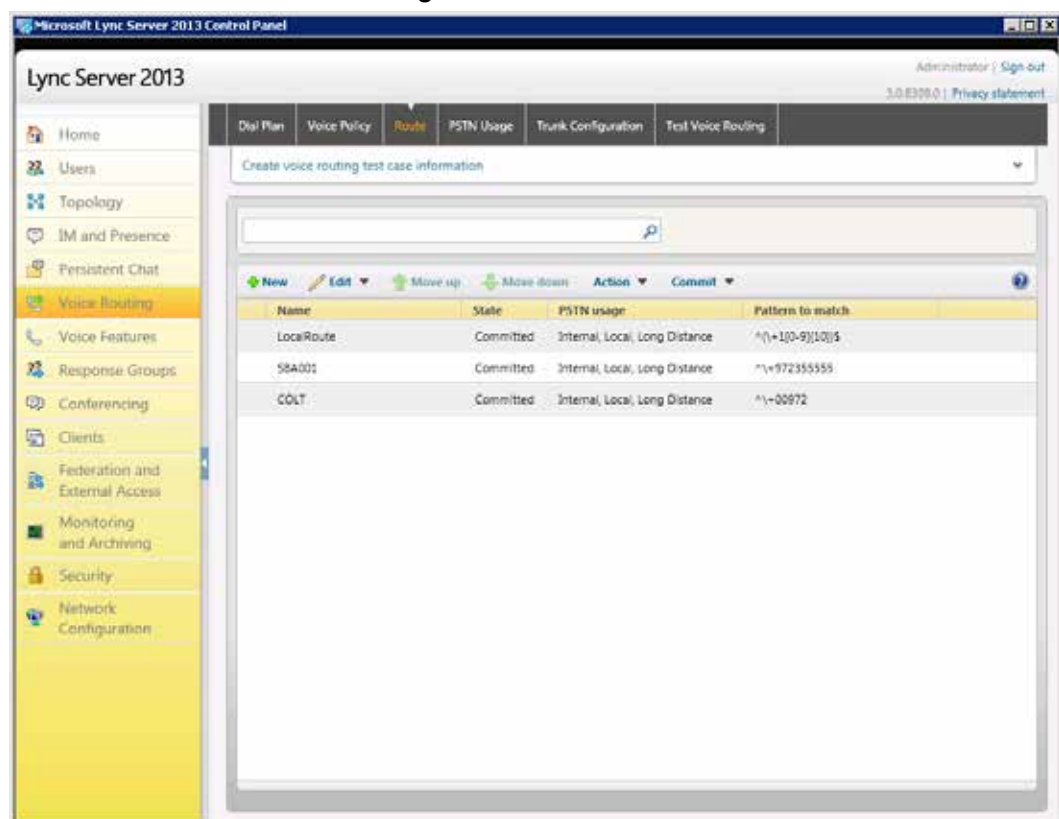
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



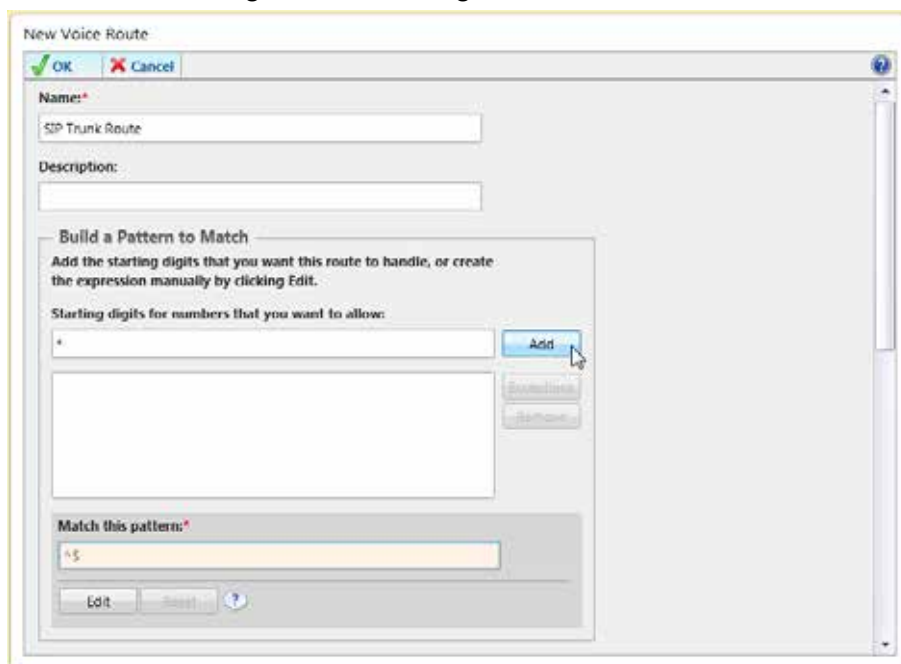
5. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



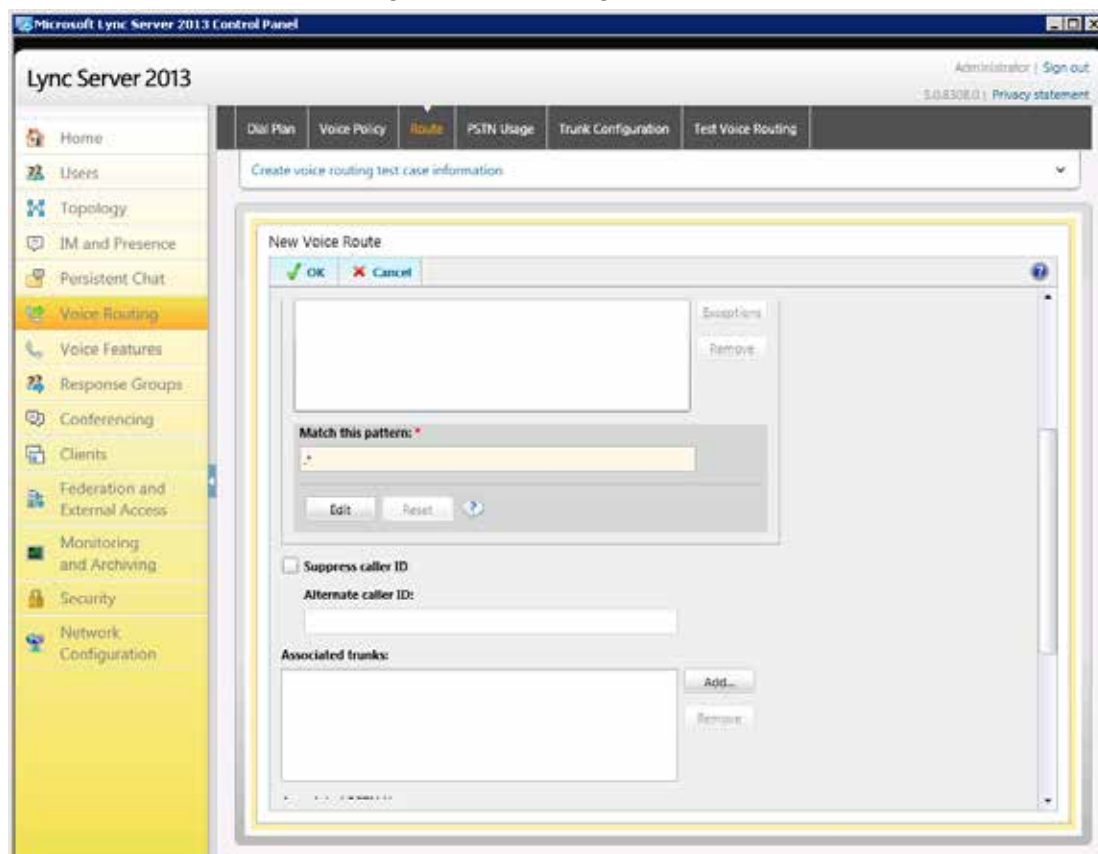
6. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



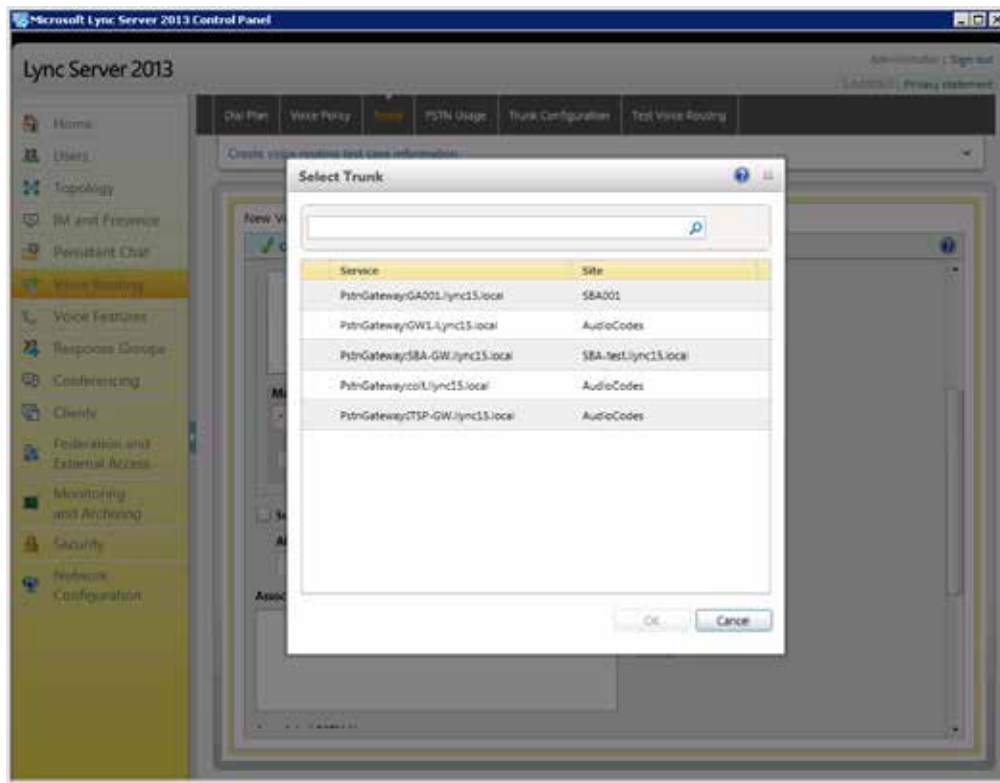
7. In the 'Name' field, enter a name for this route (e.g., **SIP Trunk Route**).
8. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.

Figure 3-20: Adding New Trunk



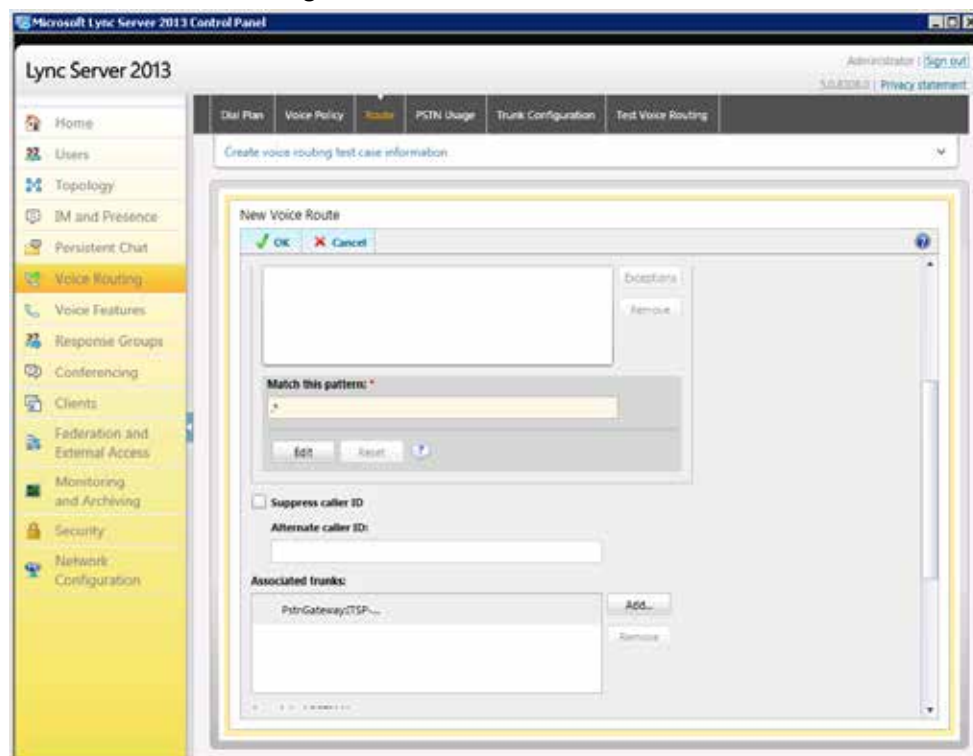
9. Associate the route with the E-SBC Trunk that you created:
 - a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



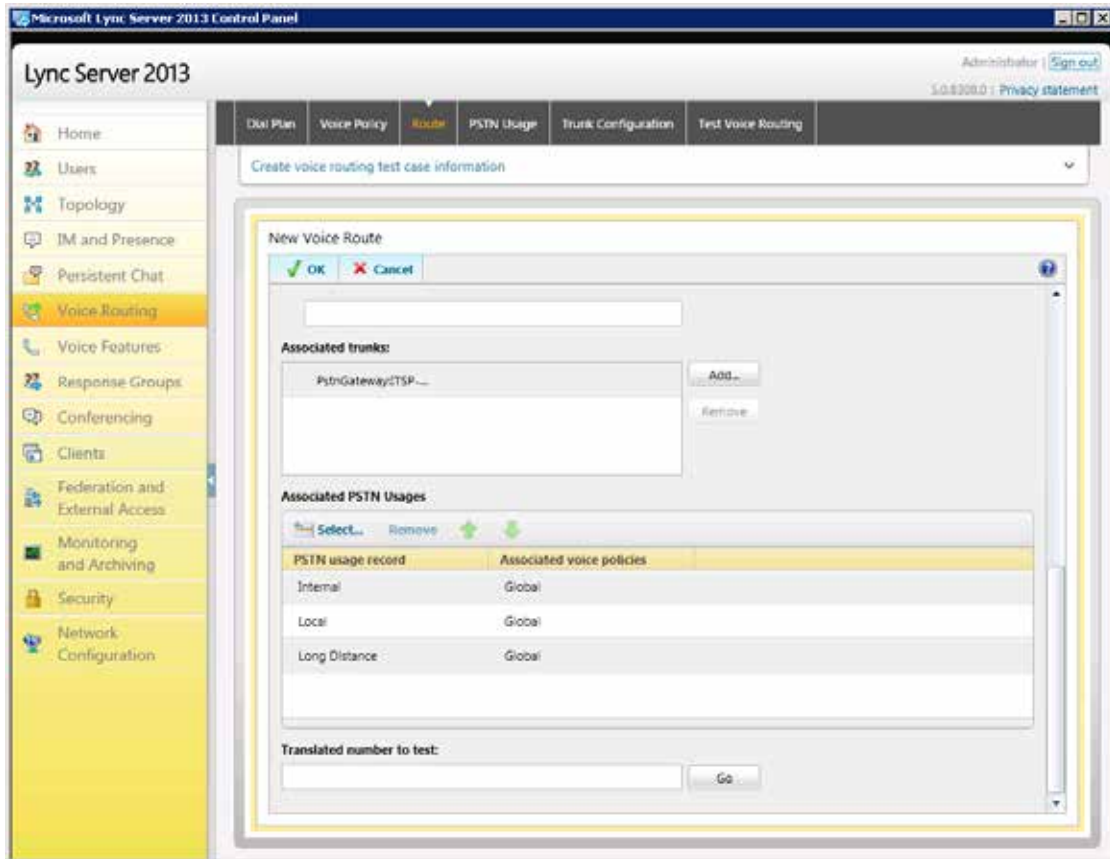
- b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



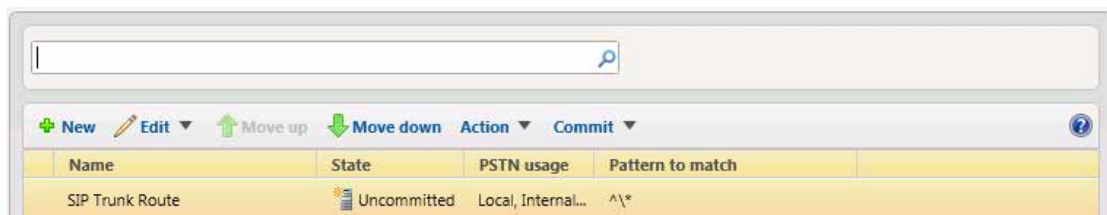
10. Associate a PSTN Usage to this route: Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



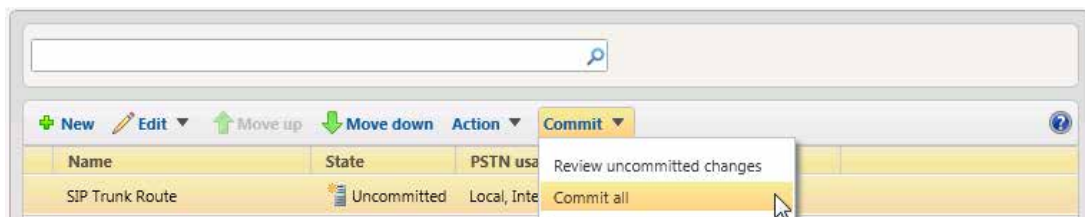
11. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



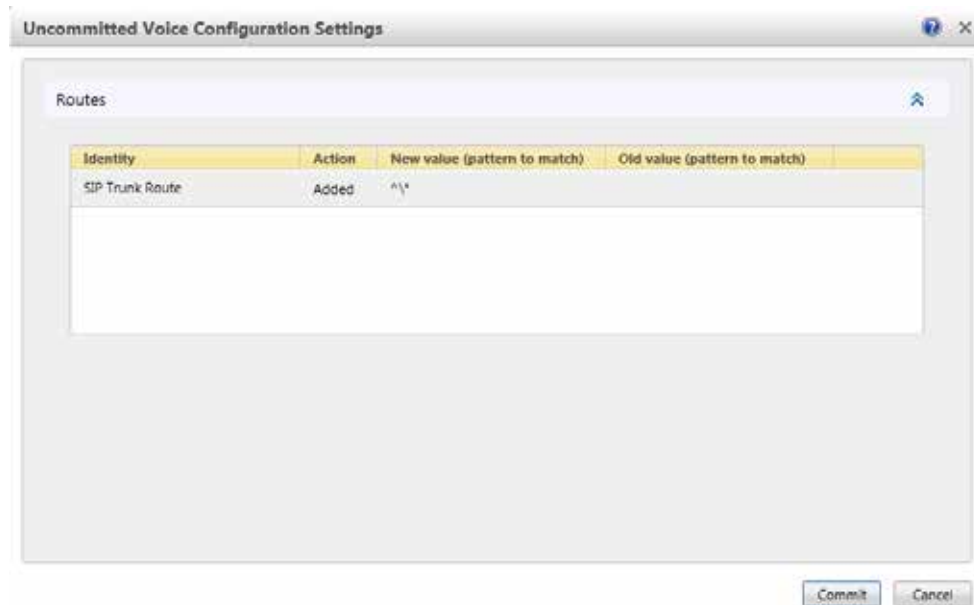
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



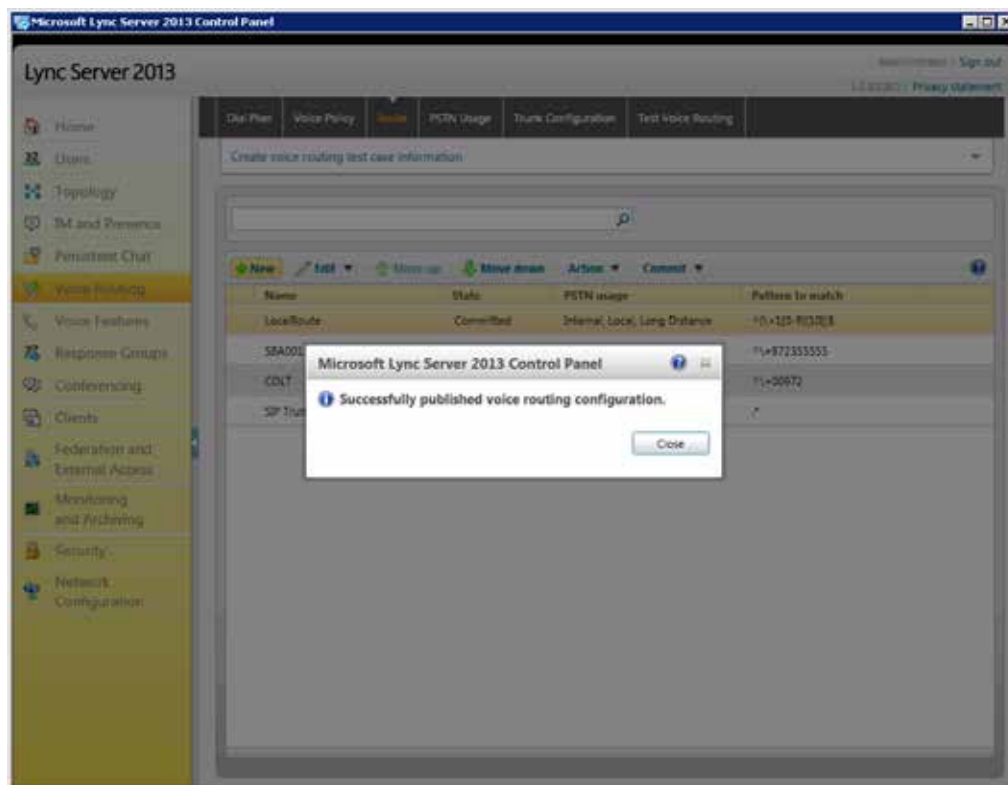
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



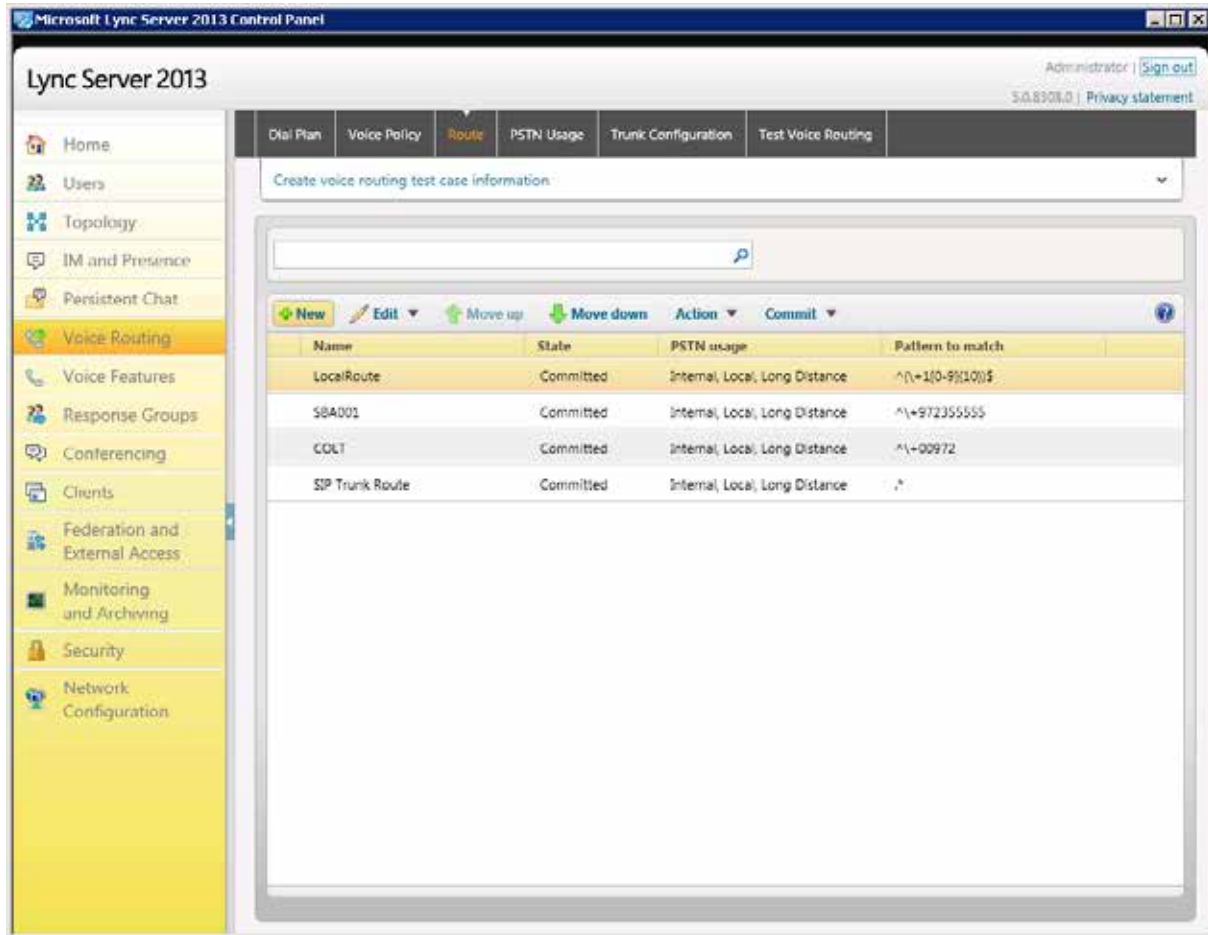
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirmation of Successful Voice Routing Configuration



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

Figure 3-28: Voice Routing Screen Displaying Committed Routes



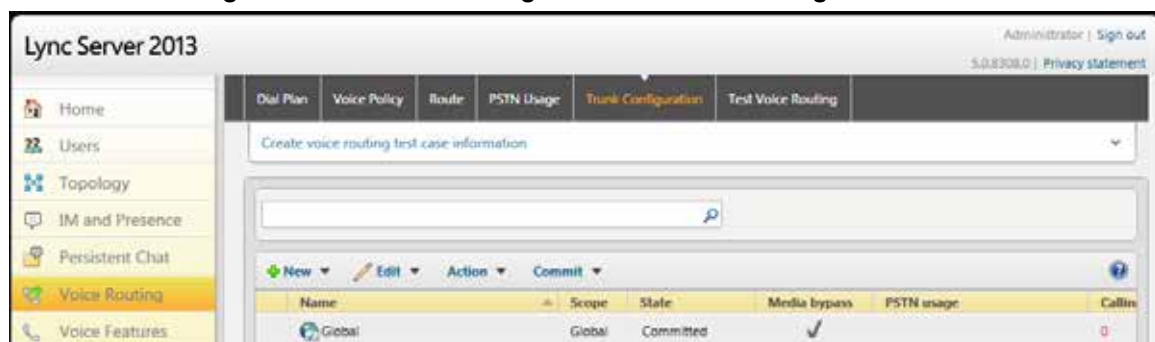
15. For ITSPs that implement a call identifier, continue with the following steps:



Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Lync user number). This ID is required by the Twilio SIP Trunk in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 4.6 on page 45).

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

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



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

Figure 3-30: Voice Routing Screen – Trunk Configuration - Edit

Edit Trunk Configuration - Global

OK Cancel

Scope: Global

Name: *

Global

Description:

Maximum early dialogs supported:

20

Encryption support level:

Required

Refer support:

Enable sending refer to the gateway

☒ Enable media bypass

☒ Centralized media processing

☐ Enable RTP latching

☒ Enable forward call history

☐ Enable forward P-Asserted-Identity data

☒ Enable outbound routing failover timer

^ Associated PSTN Usages

Select... Remove Up Down

- c. Select the **Enable forward call history** check box, and then click **OK**.
- d. Repeat Steps 11 through 13 to commit your settings.

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

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

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

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

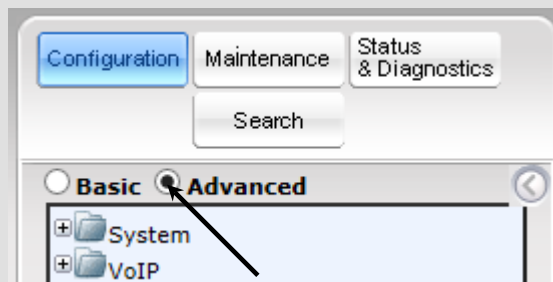
Notes:

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

- ✓ **Microsoft**
- ✓ **SBC**
- ✓ **Security**
- ✓ **DSP**
- ✓ **RTP**
- ✓ **SIP**

For more information about the Software License Key, contact your AudioCodes sales representative.

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



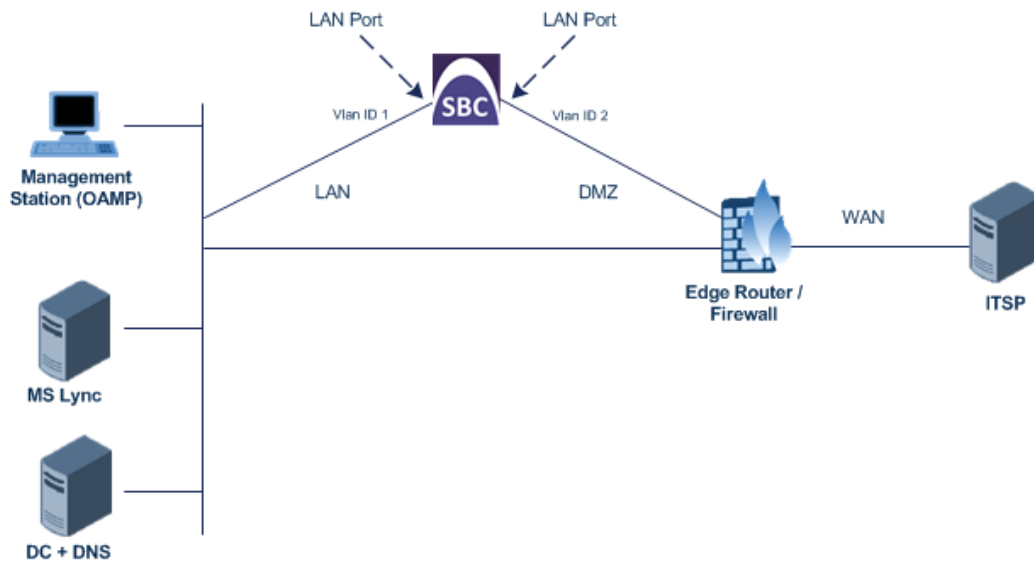
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: Configure IP Network Interfaces

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

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

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

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

Ø To configure the VLANs:

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

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

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

The screenshot shows the 'Ethernet Device Table' interface. At the top, there are buttons for 'Add +', 'Edit', 'Delete', and 'Show / Hide'. Below these is a search bar with a dropdown set to 'All' and a 'Search' button. The table has five columns: 'Index', 'VLAN ID', 'Underlying Interface', 'Name', and 'Tagging'. There are two rows of data. The first row has Index 0, VLAN ID 1, Underlying Interface GROUP_1, Name vlan 1, and Tagging Untagged. The second row has Index 1, VLAN ID 2, Underlying Interface GROUP_2, Name vlan 2, and Tagging Untagged. At the bottom, there is a pagination bar showing 'Page 1 of 1' and a 'View 1 - 2 of 2' indicator.

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

4.1.2 Step 1b: Configure Network Interfaces

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

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

Ø To configure the IP network interfaces:

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

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

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

Parameter	Value
Application Type	Media + Control
IP Address	195.189.192.158 (WAN IP address)
Prefix Length	25 (for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
Interface Name	WANSP
Primary DNS Server IP Address	80.179.52.100
Secondary DNS Server IP Address	80.179.55.100
Underlying Device	vlan 2

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

The configured IP network interfaces are shown below:

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

▼ Interface Table

Add +

Edit 

Delete 

Show / Hide 

▼ All

Search in table

Search 

Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	Voice	OAMP + Medi	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.25.1	0.0.0.0	vlan 1
1	WANSP	Media + Cont	IPv4 Manual	195.189.192.158	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2



Page 1 of 1



10 ▼

View 1 - 2 of 2

4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

Ø To enable the SBC application:

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

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.15 on page 80).

4.3 Step 3: Configure Media Realms

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

Ø **To configure Media Realms:**

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

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

Figure 4-5: Configuring Media Realm for LAN

The screenshot shows a web-based configuration interface titled "Edit Row" with a close button (X) in the top right corner. The interface contains several input fields and dropdown menus for configuring a Media Realm. The fields are as follows:

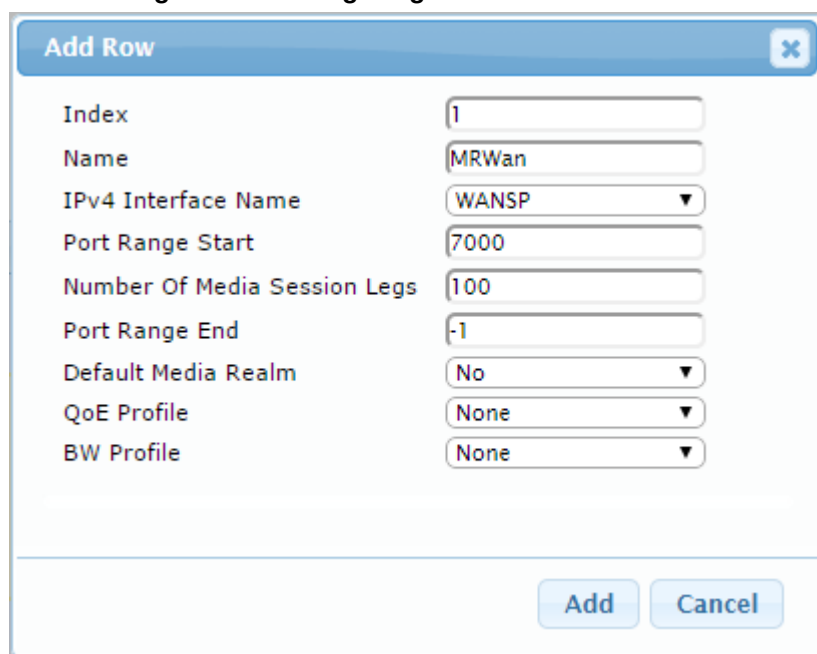
- Index:** A text input field containing the value "0".
- Name:** A text input field containing the value "MRLan".
- IPv4 Interface Name:** A dropdown menu with "Voice" selected.
- Port Range Start:** A text input field containing the value "6000".
- Number Of Media Session Legs:** A text input field containing the value "100".
- Port Range End:** A text input field containing the value "6990".
- Default Media Realm:** A dropdown menu with "No" selected.
- QoE Profile:** A dropdown menu with "None" selected.
- BW Profile:** A dropdown menu with "None" selected.

At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

3. Configure a Media Realm for WAN traffic:

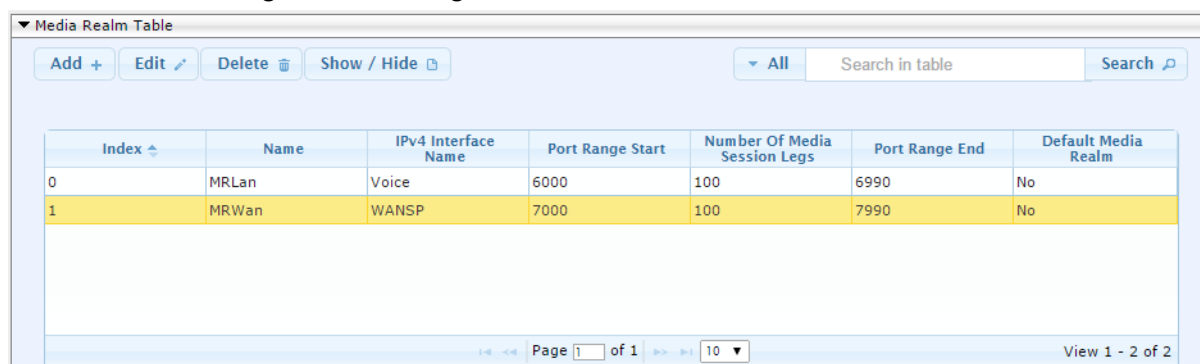
Parameter	Value
Index	1
Media Realm Name	MRWan (arbitrary name)
IPv4 Interface Name	WANSP
Port Range Start	7000 (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

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



Index	Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End	Default Media Realm
0	MRLan	Voice	6000	100	6990	No
1	MRWan	WANSP	7000	100	7990	No

4.4 Step 4: Configure SIP Signaling Interfaces

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

Ø To configure SIP Interfaces:

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

Parameter	Value
Index	0
Interface Name	Lync (see Note below)
Network Interface	Voice
Application Type	SBC
TLS Port	5067
TCP and UDP	0
Media Realm	MRLan

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	1
Interface Name	Twilio (see Note below)
Network Interface	WANSP
Application Type	SBC
UDP Port	5060
TLS Port	5061
TCP	0
Media Realm	MRWan

The configured SIP Interfaces are shown in the figure below:

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

SIP Interface Table

Add +

Edit

Delete

Show / Hide

All

Search in table

Search

Index	Name	SRD	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Encapsulating Protocol	Media Realm
0	Lync	 DefaultSRD	Voice	SBC	0	0	5067	No encapsulat	MRLan
1	Twilio	 DefaultSRD	WANSP	SBC	5060	0	5061	No encapsulat	MRWan

<<

>>

Page 1 of 1

10

View 1 - 2 of 2



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

4.5 Step 5: Configure Proxy Sets

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

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

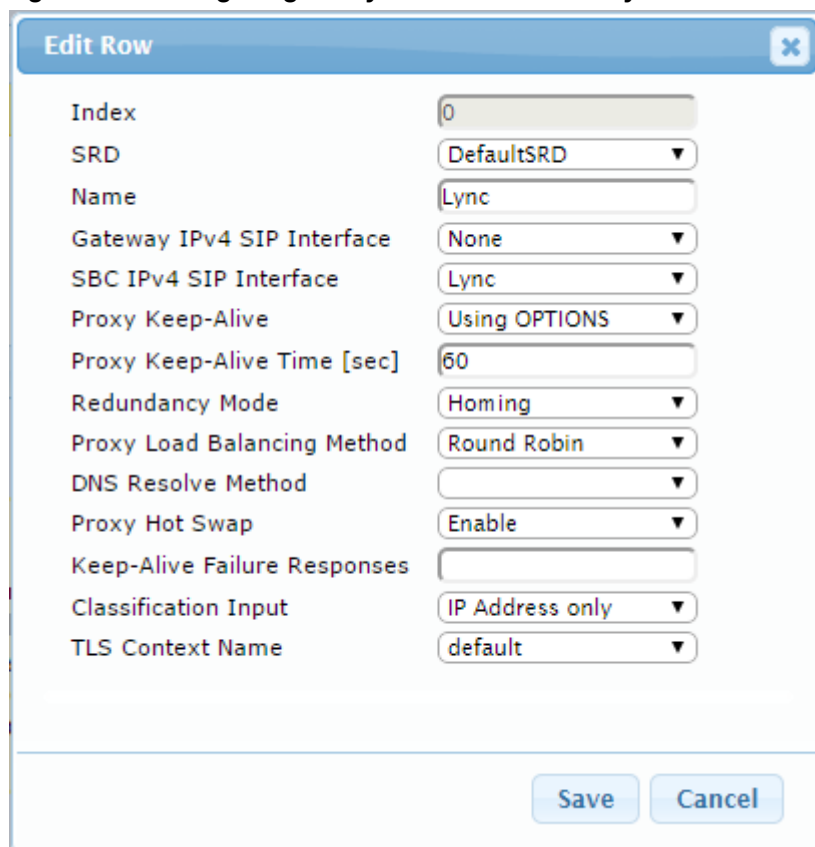
- n Microsoft Lync Server 2013
- n Twilio SIP Trunk

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

Ø To configure Proxy Sets:

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

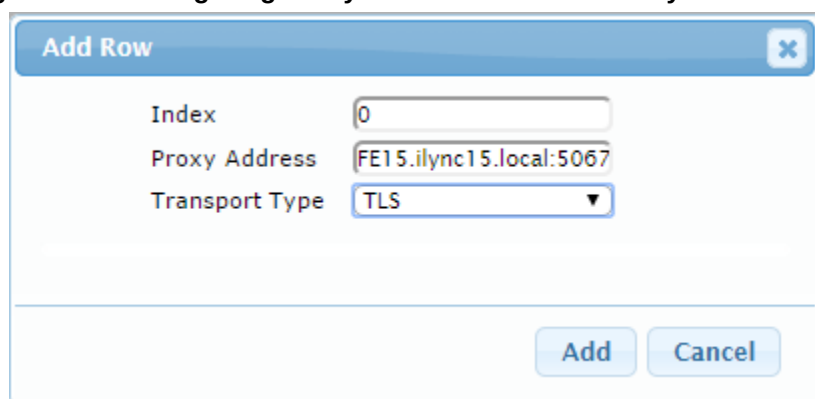
Parameter	Value
Proxy Set ID	0
Proxy Name	Lync
SBC IPv4 SIP Interface	Lync
Proxy Keep Alive	Using Options
Redundancy Mode	Homing
Load Balancing Method	Round Robin
Proxy Hot Swap	Enable
TLS Context Name	default

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


Parameter	Value
Index	0
SRD	DefaultSRD
Name	Lync
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	Lync
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Redundancy Mode	Homing
Proxy Load Balancing Method	Round Robin
DNS Resolve Method	
Proxy Hot Swap	Enable
Keep-Alive Failure Responses	
Classification Input	IP Address only
TLS Context Name	default

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

Parameter	Value
Index	0
Proxy Address	FE15.ilync15.local:5067 (Lync Server 2013 IP address / FQDN and destination port)
Transport Type	TLS

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


Parameter	Value
Index	0
Proxy Address	FE15.ilync15.local:5067
Transport Type	TLS

4. Configure a Proxy Set for the Twilio SIP Trunk:

Parameter	Value
Proxy Set ID	1
Proxy Name	Twilio
SBC IPv4 SIP Interface	Twilio
Proxy Keep Alive	Using Options
DNS Resolve Method	SRV

Figure 4-11: Configuring Proxy Set for Twilio SIP Trunk

Parameter	Value
Index	1
SRD	DefaultSRD
Name	Twilio
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	Twilio
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Redundancy Mode	None
Proxy Load Balancing Method	Disable
DNS Resolve Method	SRV
Proxy Hot Swap	Disable
Keep-Alive Failure Responses	None
Classification Input	IP Address only
TLS Context Name	None

- a. Configure a Proxy Address Table for Twilio Proxy Set:
- b. Go to **Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table** > **Proxy Address Table**.
 - i. To configure UDP transport:

Parameter	Value
Index	0
Proxy Address	ilync15.pstn.twilio.com:5060 (FQDN and destination port)
Transport Type	UDP

Figure 4-12: Configuring Proxy Address for Twilio SIP Trunk

Edit Row
✕

Index

Proxy Address

Transport Type

UDP ▼

Save

Cancel

ii. To configure TLS transport:

Parameter	Value
Index	0
Proxy Address	ilync15.pstn.twilio.com:5061 (FQDN and destination port)
Transport Type	TLS

Figure 4-13: Configuring Proxy Address for Twilio SIP Trunk

Edit Row
✕

Index

Proxy Address

Transport Type

TLS ▼

Save

Cancel

The configured Proxy Sets are shown in the figure below:

Figure 4-14: Configured Proxy Sets in Proxy Sets Table

▼ Proxy Sets Table

Add +

Edit ✎

Delete ✖

Show / Hide ☑

▼ All

Search in table

Search 🔍

Index	Name	SRD	Gateway IPv4 SIP Interface	SBC IPv4 SIP Interface	Proxy Keep-Alive Time [sec]	Redundancy Mode	Proxy Hot Swap
0	Lync	☐ DefaultSRD (#C None	Lync	Lync	60	Homing	Enable
1	Twilio	☐ DefaultSRD (#C None	Twilio	Twilio	60		Disable

Page 1 of 1
10 ▼

View 1 - 2 of 2

4.6 Step 6: Configure IP Profiles

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

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

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

Ø To configure IP Profile for the Lync Server 2013:

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

Parameter	Value
Index	1
Name	Lync
Symmetric MKI	Enable
MKI Size	1
Reset SRTP State Upon Re-key	Enable
Generate SRTP keys mode:	Always

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

The screenshot shows the 'Add Row' dialog box with the 'Common' tab selected. The 'Index' field is set to 1. The 'Name' field is set to 'Lync'. The following parameters are configured:

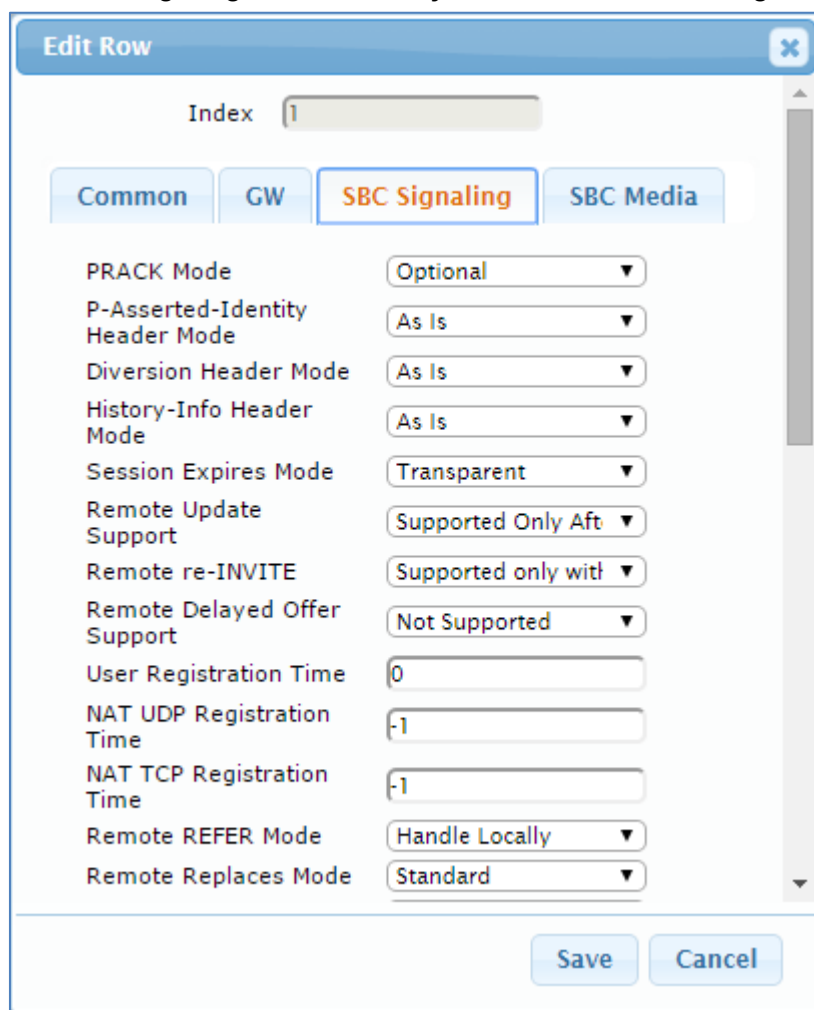
- Dynamic Jitter Buffer Minimum Delay [msec]: 10
- Dynamic Jitter Buffer Optimization Factor: 10
- Jitter Buffer Max Delay [msec]: 300
- RTP IP DiffServ: 46
- Signaling DiffServ: 40
- Silence Suppression: Disable
- RTP Redundancy Depth: 0
- Echo Canceler: Line
- Disconnect on Broken Connection: Enable
- Input Gain (-32 to 31 dB): 0
- Voice Volume (-32 to 31 dB): 0
- Media IP Version: Only IPv4

The 'Add' button is highlighted at the bottom right of the dialog.

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

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

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



Index: 1

Common GW **SBC Signaling** SBC Media

PRACK Mode: Optional

P-Asserted-Identity Header Mode: As Is

Diversion Header Mode: As Is

History-Info Header Mode: As Is

Session Expires Mode: Transparent

Remote Update Support: Supported Only Aft

Remote re-INVITE: Supported only with

Remote Delayed Offer Support: Not Supported

User Registration Time: 0

NAT UDP Registration Time: -1

NAT TCP Registration Time: -1

Remote REFER Mode: Handle Locally

Remote Replaces Mode: Standard

Save Cancel

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

Parameter	Value
Allowed Audio Coders	Coders Group 0 (in order to ensure that voice sent to the Twilio SIP Trunk uses the G.711U-law coder only)
SBC Media Security Mode	SRTP
Enforce MKI Size	Enforce
RTCP Mode	Generate Always (required, as Twilio SIP Trunk does not send RTCP packets in active and in hold calls, and in these cases, Microsoft Lync 2013 will terminate the call with network problems as the cause)

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

The screenshot shows the 'Edit Row' dialog box with the 'SBC Media' tab selected. The 'Index' is set to 1. The 'SBC Media' tab is highlighted in orange. The following parameters are visible:

- Transcoding Mode: Only If Required
- Extension Coders: None
- Allowed Audio Coders: Coders Group 0
- Allowed Coders Mode: Restriction
- Allowed Video Coders: None
- Allowed Media Types: (empty field)
- SBC Media Security Mode: SRTP
- Media Security Method: SDES
- Enforce MKI Size: Enforce
- SDP Remove Crypto Lifetime: No
- RFC 2833 Mode: As Is
- Alternative DTMF Method: As Is
- RFC 2833 DTMF Payload Type: 0
- Fax Coders: None

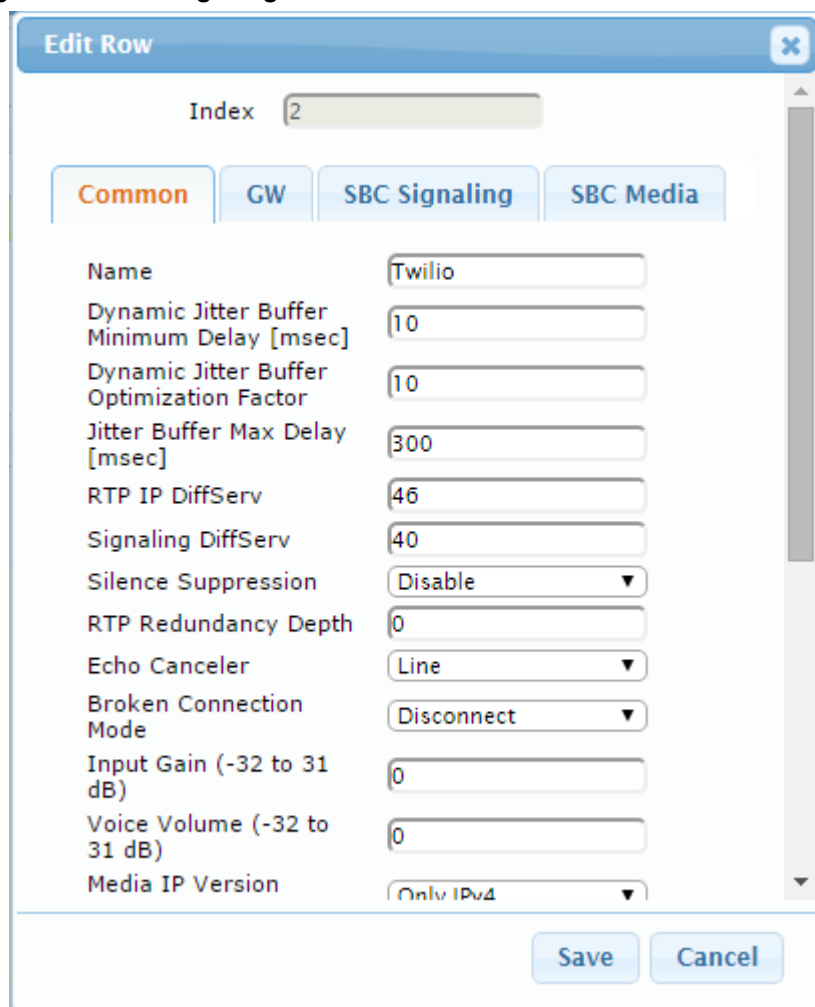
At the bottom right, there are 'Save' and 'Cancel' buttons.

Ø To configure an IP Profile for the Twilio SIP Trunk:

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

Parameter	Value
Index	2
Profile Name	Twilio
MKI Size	0 (MKI isn't supported by Twilio SIP Trunk)

Figure 4-18: Configuring IP Profile for Twilio SIP Trunk – Common Tab



The screenshot shows the 'Edit Row' dialog box for configuring an IP Profile. The 'Index' is set to 2. The 'Common' tab is selected, showing the following parameters:

- Name: Twilio
- Dynamic Jitter Buffer Minimum Delay [msec]: 10
- Dynamic Jitter Buffer Optimization Factor: 10
- Jitter Buffer Max Delay [msec]: 300
- RTP IP DiffServ: 46
- Signaling DiffServ: 40
- Silence Suppression: Disable
- RTP Redundancy Depth: 0
- Echo Canceler: Line
- Broken Connection Mode: Disconnect
- Input Gain (-32 to 31 dB): 0
- Voice Volume (-32 to 31 dB): 0
- Media IP Version: Only IPv4

Buttons for 'Save' and 'Cancel' are at the bottom right.

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

Parameter	Value
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
Remote Update Support	Not Supported
Remote re-INVITE Support	Not Supported
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Play RBT To Transferee	Yes
Remote Hold Format	Not Supported

Figure 4-19: Configuring IP Profile for Twilio SIP Trunk – SBC Signaling Tab

Edit Row

Index: 2

Common | GW | **SBC Signaling** | SBC Media

PRACK Mode: Transparent

P-Asserted-Identity Header Mode: Add

Diversion Header Mode: As Is

History-Info Header Mode: As Is

Session Expires Mode: Transparent

Remote Update Support: Not Supported

Remote re-INVITE: Not Supported

Remote Delayed Offer Support: Supported

User Registration Time: 0

NAT UDP Registration Time: -1

NAT TCP Registration Time: -1

Remote REFER Mode: Handle Locally

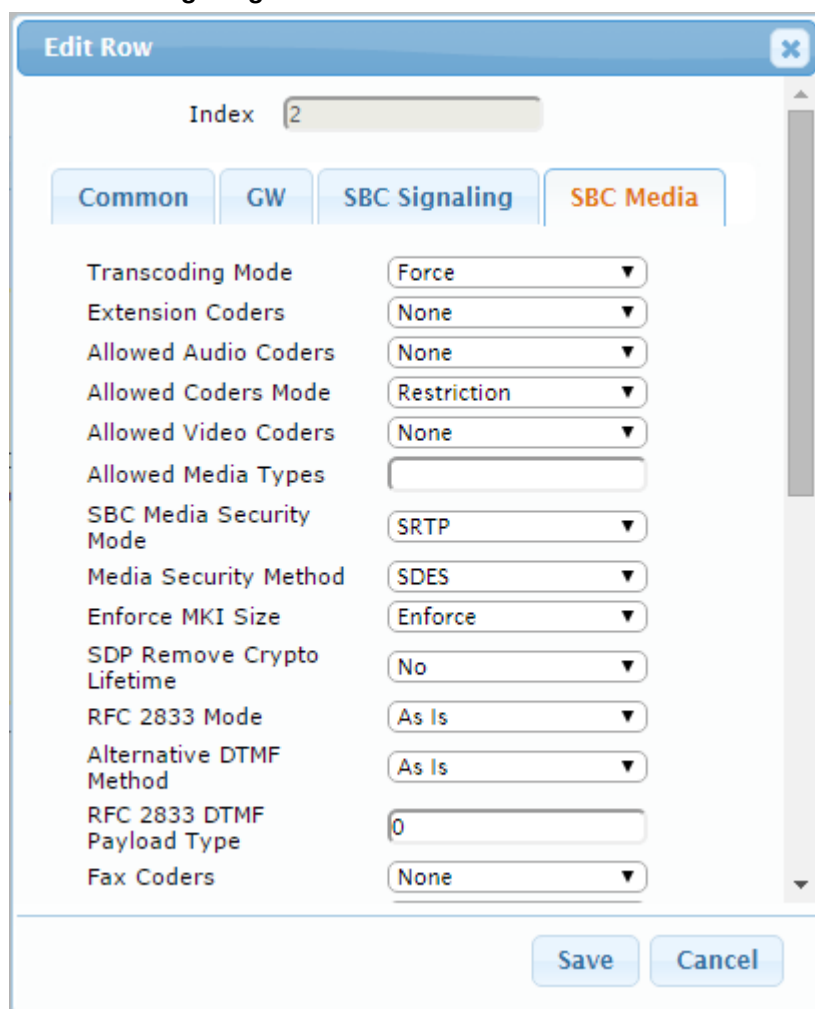
Remote Replaces Mode: Standard

Save Cancel

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

Parameter	Value
Transcoding Mode	Force (required as there is a 120 seconds broken connection timeout defined on the Twilio SIP Trunk. Consequently, the SIP trunk always expects to receive RTP packets. When a call is muted or placed on Hold, no packets are sent from the Microsoft Lync Server 2013 side).
Enforce MKI Size	Enforce

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



The screenshot shows the 'Edit Row' dialog box for configuring the SBC Media tab. The 'Index' is set to 2. The 'SBC Media' tab is selected. The parameters and their values are as follows:

Parameter	Value
Transcoding Mode	Force
Extension Coders	None
Allowed Audio Coders	None
Allowed Coders Mode	Restriction
Allowed Video Coders	None
Allowed Media Types	
SBC Media Security Mode	SRTP
Media Security Method	SDS
Enforce MKI Size	Enforce
SDP Remove Crypto Lifetime	No
RFC 2833 Mode	As Is
Alternative DTMF Method	As Is
RFC 2833 DTMF Payload Type	0
Fax Coders	None

Buttons: Save, Cancel

4.7 Step 7: Configure IP Groups

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

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

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

Ø To configure IP Groups:

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

Parameter	Value
Index	0
Name	Lync
Type	Server
Proxy Set	Lync
IP Profile	Lync
Media Realm	MRLan
SIP Group Name	ilync15.pstn.twilio.com (according to ITSP requirement)

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

Parameter	Value
Index	1
Name	Twilio
Type	Server
Proxy Set	Twilio
IP Profile	Twilio
Media Realm	MRWan
SIP Group Name	ilync15.pstn.twilio.com (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-21: Configured IP Groups in IP Group Table

▼ IP Group Table

Add +

Edit ✎

Delete 🗑

Show / Hide 📄

▼ All

Search in table

Search 🔍

Index ↕	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulation Set	Outbound Message Manipulation Set
0	Lync	Default	Server	Not Configured	Lync	Lync	MRLan	ilync15.pstn	Enable	-1	-1
1	Twilio	Default	Server	Not Configured	Twilio	Twilio	MRWan	ilync15.pstn	Enable	-1	-1

Page 1 of 1

10 ▼

View 1 - 2 of 2

4.8 Step 8: Configure Allowed Coder

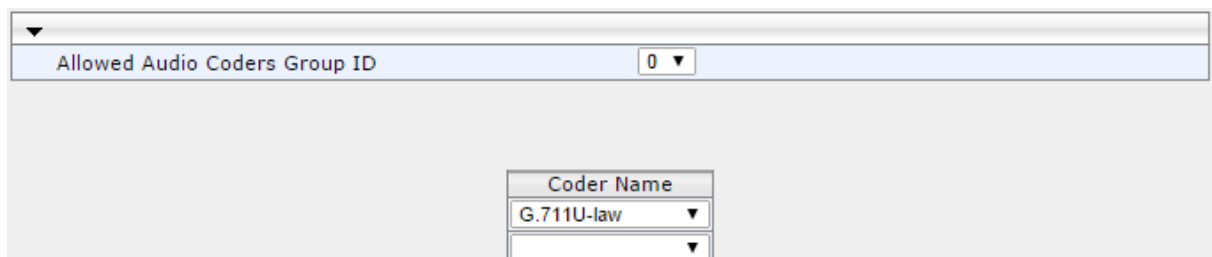
This step describes how to configure an Allowed Coders Group to ensure that voice sent to the Twilio SIP Trunk uses the G.711U-law coder only. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Twilio SIP Trunk (see Section 4.6 on page 45).

Ø To set a preferred coder for the SIP Trunk:

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

Parameter	Value
Allowed Audio Coders Group ID	0
Coder Name	G.711

Figure 4-22: Configuring Allowed Coders Group for SIP Trunk



The screenshot shows a web interface for configuring an Allowed Audio Coders Group. At the top, there is a dropdown menu labeled 'Allowed Audio Coders Group ID' with the value '0' selected. Below this, there is a section for 'Coder Name' with a dropdown menu showing 'G.711U-law' selected. The interface is clean and professional, with a light gray background and blue accents.

3. Click **Submit**.

4.9 Step 9: Configure the SIP TLS Connection

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

4.9.1 Step 9a: Configure the NTP Server Address

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

Ø To configure the NTP server address:

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

Figure 4-23: Configuring NTP Server Address

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

3. Click **Submit**.

4.9.2 Step 9b: Configure a Certificate for Operation with Microsoft Lync Server 2013

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

The procedure involves the following main steps:

- a. Generating a Certificate Signing Request (CSR).
- b. Requesting Device Certificate from CA.
- c. Obtaining Trusted Root Certificate from CA.
- d. Deploying Device and Trusted Root Certificates on E-SBC.

Ø To configure a certificate:

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click the **TLS Context Certificates**  button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **ITSP-2.ilync15.local**).
 - b. Fill in the rest of the request fields according to your security provider's instructions.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-24: Certificate Signing Request – Creating CSR

Certificate Signing Request	
Subject Name [CN]	ITSP-GW.ilync15.local
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	
Create CSR	
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.	
<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBXzCBYQIBADAgMR4wHAYDVQQDExVJVFNFQlUdXlMlseW5jMTUubG9jYVwwZ8w DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioo0LVrwNsC1 3TMgnoMVxdp9/BCXyvgT2W1vz0NGUsypa7w2DKKxr8xA9sGLXwy0ZCyB49U1pDF DJV8IldUfT8qL9d9V64f3Z004I1hweZSn4hHdAfGy0S6e91JhFw/USUD6/bNygQz 5z203jtjXKmdAgMBAAAGgADANBgkqhkiG9w0BAQQFAAQBqBLqe880JGrmEzPu5Q1 pRGiOuEQ4Pr6PL+JKghii6UpLmHEwixTedayzNh7b2yQgFYxiVWmX2JwrvXaCp5Y 8z8hOCZXV/E4MrR2s8bYb6bqxeteAXs+VwxgKObb4pSFfGLc82+dZUcODAB0wZFv nxSEoPACKnZittF/GgW+A4AoMQ== -----END CERTIFICATE REQUEST----- </pre>	



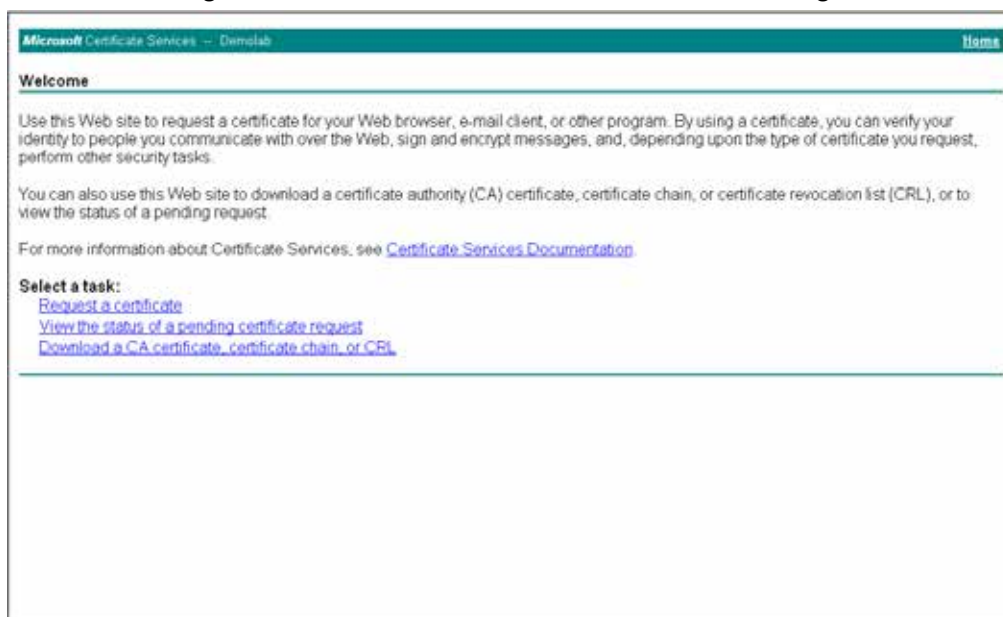
Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13).

5. Copy the CSR from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE"

REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.

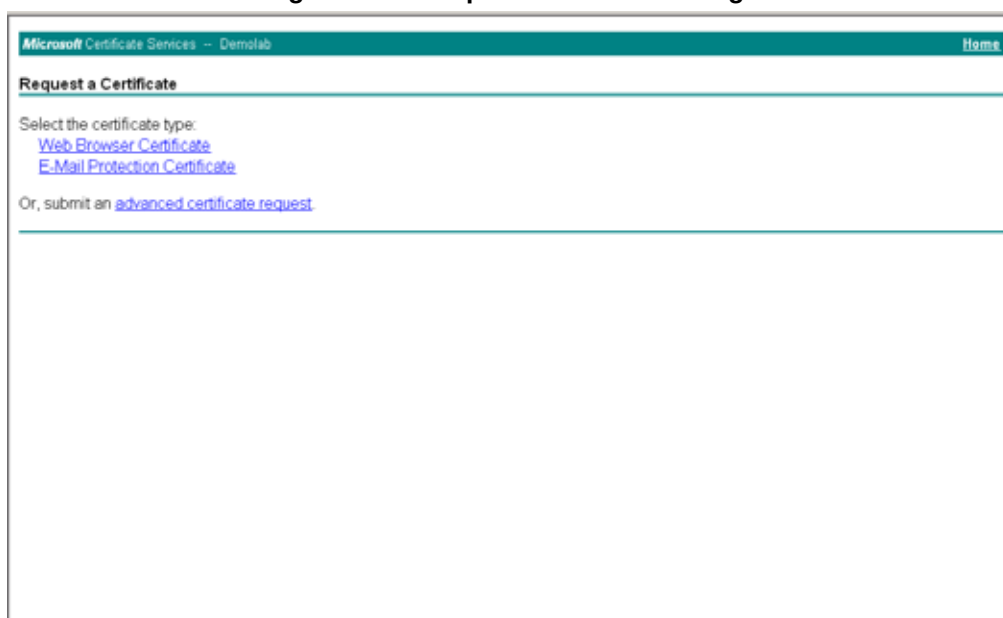
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

Figure 4-25: Microsoft Certificate Services Web Page



7. Click **Request a certificate**.

Figure 4-26: Request a Certificate Page



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

Figure 4-27: Advanced Certificate Request Page

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

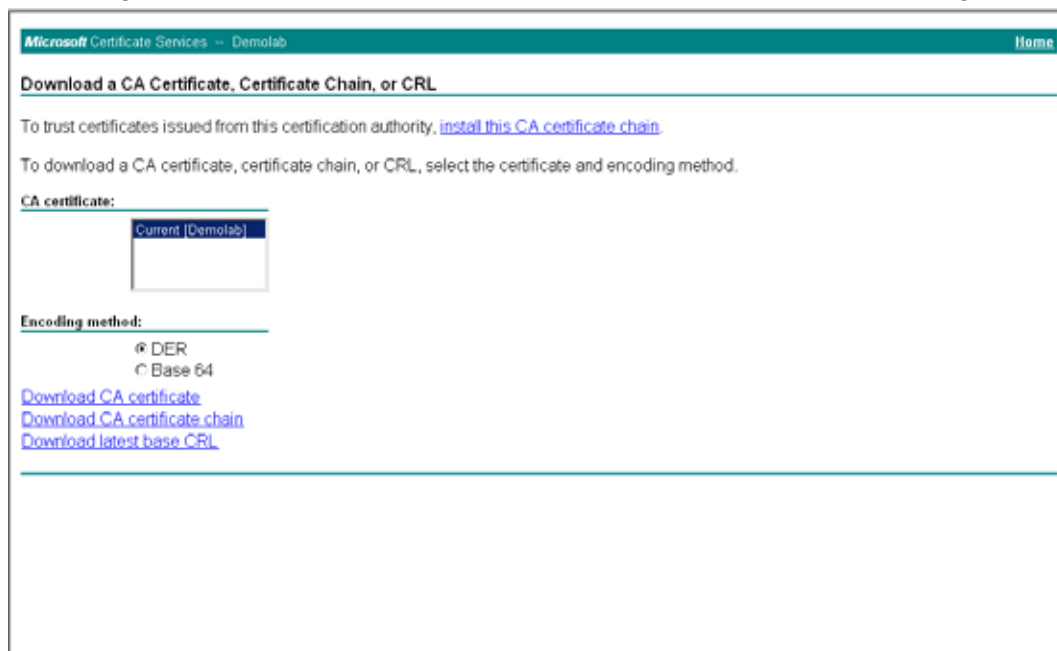
Figure 4-28: Submit a Certificate Request or Renewal Request Page

10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**.

Figure 4-29: Certificate Issued Page

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

Figure 4-30: Download a CA Certificate, Certificate Chain, or CRL Page



Microsoft Certificate Services - Demolab Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

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

CA certificate:

Encoding method:

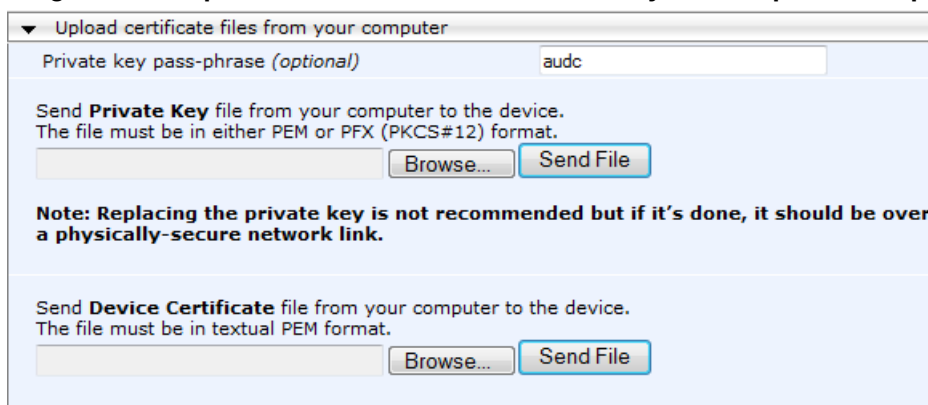
☒ DER
☐ Base 64

[Download CA certificate](#)
[Download CA certificate chain](#)
[Download latest base CRL](#)

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

20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click the **TLS Context Certificates**  button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
 - b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-31: Upload Device Certificate Files from your Computer Group



▼ Upload certificate files from your computer

Private key pass-phrase (optional)

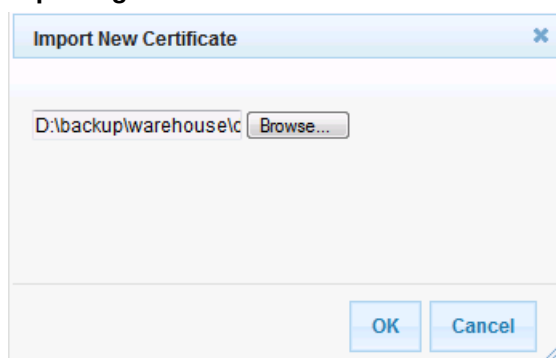
Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

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.

- c. In the E-SBC's Web interface, return to the **TLS Contexts** page.
- d. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates**  button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
- e. Click the **Import** button, and then select the certificate file to load.

Figure 4-32: Importing Root Certificate into Trusted Certificates Store



Import New Certificate

D:\backup\warehouse\c

21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 80).

4.9.3 Step 9c: Configure a Certificate for work with Twilio SIP Trunk

This step describes how to exchange a certificate with Twilio Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Twilio SIP Trunk.

The procedure involves the following main steps:

- a. Generating a Private Key and Self-Signed Certificate.
- b. Obtaining Trusted Root Certificate from Twilio CA.
- c. Deploying Trusted Root Certificates on E-SBC.

Ø To configure a certificate:

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. Click **Add** and configure new record in the TLS Contexts table (with name e.g., **Twilio**).
3. Click the **TLS Context Certificates**  button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
4. Under the **Certificate Signing Request** group, enter the E-SBC name (e.g., **audc**).
5. Under the **Generate new private key and self-signed certificate** group, do the following:
 - a. Click the **Generate Private Key** button.
 - b. Click the **Generate Self-Signed Certificate** button.
6. In the E-SBC's Web interface, return to the **TLS Contexts** page.
7. In the TLS Contexts table, select the **Twilio** TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates**  button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
8. Click the **Import** button, and then select the certificate file to load. Twilio's root certificate can be loaded from the following link:
<https://www.twilio.com/docs/api/sip-trunking/getting-started#rootCA>.
9. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
10. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 80).

4.10 Step 10: Configure SRTP

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

Ø **To configure media security:**

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

Parameter	Value
Media Security	Enable

Figure 4-33: Configuring SRTP

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

3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 80).

4.11 Step 11: Configure Maximum IP Media Channels

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



Note: This step is required **only** if transcoding is required. For Interoperability with Twilio SIP Trunk it is required because forced transcoding enabled in order to deal with Broken Connection Timeout on Twilio SIP trunk issue.

Ø To configure the maximum number of IP media channels:

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

Figure 4-34: Configuring Number of Media Channels

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section [4.15](#) on page [80](#)).

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

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

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

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

Ø To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
 - a.** Click **Add**.
 - b.** Click the **Rule** tab, and then configure the parameters as follows:

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

Figure 4-35: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab

Edit Row

Index
0
Routing Policy
Default_SBCRouting

Rule

Action

Name
Terminate OPTIONS
Alternative Route Options
Route Row
Source IP Group
Lync
Request Type
OPTIONS
Source Username Prefix
*
Source Host
*
Destination Username Prefix
*
Destination Host
*
Message Condition
None
Call Trigger
Any
ReRoute IP Group
Any

[Classic View](#)

Save

Cancel

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-36: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

Add Row

Index: 0

Routing Policy: Default_SBCRouting

Rule | **Action**

Destination Type: Dest Address

Destination IP Group: None

Destination SIP Interface: None

Destination Address: internal

Destination Port: 0

Destination Transport Type:

Call Setup Rules Set ID: -1

Group Policy: None

Cost Group: None

[Classic View](#)

Add Cancel

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

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

Figure 4-37: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab

Add Row
✕

Index

Routing Policy

Default_SBCRouting ▼

Rule
Action

Name

Alternative Route Options

Route Row ▼

Source IP Group

Lync ▼

Request Type

All ▼

Source Username Prefix

Source Host

Destination Username Prefix

Destination Host

Message Condition

None ▼

Call Trigger

Any ▼

ReRoute IP Group

Any ▼

[Classic View](#)

Add

Cancel

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

Parameter	Value
Destination Type	IP Group
Destination IP Group	Twilio
Destination SIP Interface	Twilio

Figure 4-38: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab

Edit Row

Index: 1

Routing Policy: Default_SBCRouting

Rule | **Action**

Destination Type: IP Group

Destination IP Group: Twilio

Destination SIP Interface: Twilio

Destination Address:

Destination Port: 0

Destination Transport Type:

Call Setup Rules Set ID: -1

Group Policy: None

Cost Group: None

[Classic View](#)

Save Cancel

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

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

Figure 4-39: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab

Edit Row

Index
2
Routing Policy
Default_SBCRouting

Rule

Action

Name
ITSP to Lync
Alternative Route Options
Route Row
Source IP Group
Twilio
Request Type
All
Source Username Prefix
*
Source Host
*
Destination Username Prefix
*
Destination Host
*
Message Condition
None
Call Trigger
Any
ReRoute IP Group
Any

[Classic View](#)

Save
Cancel

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

Parameter	Value
Destination Type	IP Group
Destination IP Group	Lync
Destination SIP Interface	Lync

Figure 4-40: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab

Edit Row

Index: 2
Routing Policy: Default_SBCRouting

Rule | **Action**

Destination Type: IP Group
Destination IP Group: Lync
Destination SIP Interface: Lync
Destination Address:
Destination Port: 0
Destination Transport Type:
Call Setup Rules Set ID: -1
Group Policy: None
Cost Group: None

[Classic View](#)

Save Cancel

The configured routing rules are shown in the figure below:

Figure 4-41: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

▼ IP-to-IP Routing Table

Add + Edit Edit Delete Delete Insert + Up ↑ Down ↓ Show / Hide ▢ ▾ All Search in table Search 🔍

Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destination SIP Interface	Destination Address
0	OPTIONS to Lync	Default_SBC	Route Row	Lync	OPTIONS	*	*	Dest Address	None	None	internal
1	Lync to ITSP	Default_SBC	Route Row	Lync	All	*	*	IP Group	Twilio	Twilio	
2	ITSP to Lync	Default_SBC	Route Row	Twilio	All	*	*	IP Group	Lync	Lync	

Page 1 of 1 10 View 1 - 3 of 3



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

4.13 Step 13: Configure Message Manipulation Rules

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

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

Ø To configure SIP message manipulation rule:

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for Twilio SIP Trunk. This rule applies to messages sent to the Twilio SIP Trunk IP Group in a call forwarding scenario. This rule replaces the host part of the SIP History-Info Header with the value that was configured in the Twilio SIP Trunk IP Group.

Parameter	Value
Index	0
Name	Change Host of History-Info.0
Manipulation Set ID	4
Message Type	invite.request
Condition	header.history-info.0 regex (.*)(@)(.*)((user=phone)(.*))
Action Subject	header.history-info.0
Action Type	Modify
Action Value	\$1+\$2+param.ipg.dst.host+\$4+\$5

Figure 4-42: Configuring SIP Message Manipulation Rule 0 (for Twilio SIP Trunk)

The screenshot shows a web-based configuration interface for SIP message manipulation rules. The 'Edit Row' dialog box is open, displaying the following fields and values:

- Index: 0
- Name: Change Host of History-Info.0
- Manipulation Set ID: 4
- Message Type: invite.request
- Condition: header.history-info.0 re
- Action Subject: header.history-info.0
- Action Type: Modify (selected from a dropdown)
- Action Value: \$1+\$2+param.ipg.dst.h
- Row Role: Use Current Condit (selected from a dropdown)

At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

3. Configure another manipulation rule (Manipulation Set 4) for the Twilio SIP Trunk. This rule also applies to messages sent to the Twilio SIP Trunk IP Group in a call forwarding scenario. This rule removes SIP History-Info.1 Header.

Parameter	Value
Index	1
Name	Remove History-Info.1
Manipulation Set ID	4
Message Type	invite.request
Action Subject	header.history-info.1
Action Type	Remove

Figure 4-43: Configuring SIP Message Manipulation Rule 1 (for Twilio SIP Trunk)

The screenshot shows a web-based configuration interface for SIP message manipulation rules. The 'Edit Row' dialog is open, displaying the following configuration details:

- Index:** 1
- Name:** Remove History-Info.1
- Manipulation Set ID:** 4
- Message Type:** invite.request
- Condition:** (empty field)
- Action Subject:** header.history-info.1
- Action Type:** Remove (selected from a dropdown menu)
- Action Value:** (empty field)
- Row Role:** Use Current Condit (selected from a dropdown menu)

At the bottom right of the dialog, there are two buttons: 'Save' and 'Cancel'.

4. Configure another manipulation rule (Manipulation Set 4) for the Twilio SIP Trunk. This rule applies to messages sent to the Twilio SIP Trunk IP Group in a call transfer scenario. This rule replaces the host part of the SIP Referred-by Header with the value that was configured in the Twilio SIP Trunk IP Group.

Parameter	Value
Index	2
Name	Change Referred-by Host
Manipulation Set ID	4
Message Type	invite.request
Condition	header.referred-by exists
Action Subject	header.referred-by.url.host
Action Type	Modify
Action Value	param.ipg.dst.host

Figure 4-44: Configuring SIP Message Manipulation Rule 2 (for Twilio SIP Trunk)

Edit Row

Index

2

Name

Change Referred-by Host

Manipulation Set ID

4

Message Type

invite.request

Condition

header.referred-by exists

Action Subject

header.referred-by.url.h

Action Type

Modify

Action Value

param.ipg.dst.host

Row Role

Use Current Condit

Save

Cancel

Figure 4-45: Configured SIP Message Manipulation Rules

▼ Message Manipulations								
Add + Edit ✎ Delete 🗑️ Insert + Up ↑ Down ↓ Show / Hide 📄 ▼ All Search in table Search 🔍								
Index	Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	Change Host of History-Info.0	4	invite.request	header.history-info.	header.history-in	Modify	\$1+\$2+param.ip	Use Current Conc
1	Remove History-Info.1	4	invite.request		header.history-in	Remove		Use Current Conc
2	Change Referred-by Host	4	invite.request	header.referred-by	header.referred-	Modify	param.ipg.dst.hc	Use Current Conc
Page 1 of 1 View 1 - 3 of 3								

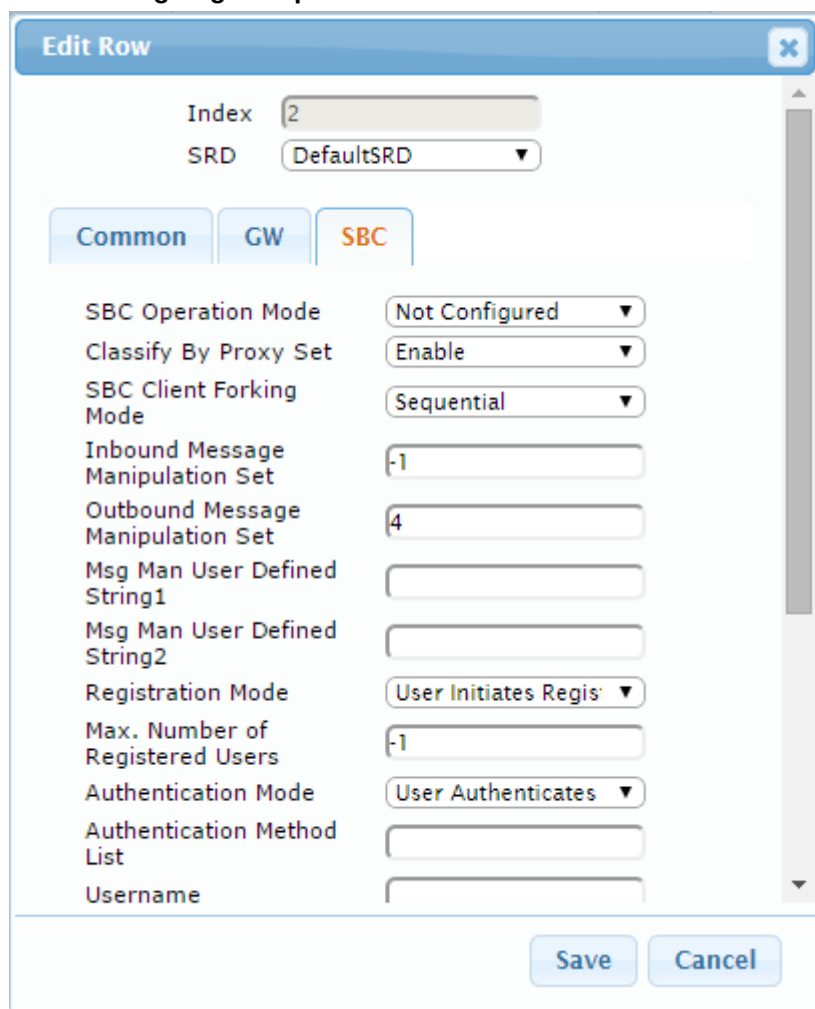
The table displayed below includes SIP message manipulation rules, which Manipulation Set ID 4 groups together and which are executed for messages sent to the Twilio SIP Trunk IP Group. These rules are specifically required to enable proper interworking between Twilio SIP Trunk and Lync Server 2013. Refer to the *User's Manual* for further details on the full capabilities of header manipulation.

SIP Message Manipulation Rules

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages sent to the SIP Trunk IP Group in a call forwarding scenario. This rule replaces the host part of the SIP History-Info Header with the value, configured in the Twilio SIP Trunk IP Group.	To introduce Topology Hiding in the Call Forward scenarios, the host part of the SIP History-Info Header should be replaced with the value that was configured in the SIP Trunk IP Group.
1	This rule also applies to messages sent to the SIP Trunk IP Group in a call forwarding scenario. This rule removes the SIP History-Info.1 Header.	To introduce Topology Hiding in the Call Forward scenarios, the SIP History-Info.1 Header should be removed.
2	This rule applies to messages sent to the SIP Trunk IP Group in a call transfer scenario. This replaces the host part of the SIP Referred-by Header with the value, configured in the Twilio SIP Trunk IP Group.	To introduce Topology Hiding in the Call Transfer scenarios, the host part of the SIP Referred-by Header should be replaced with the value that was configured in the SIP Trunk IP Group.

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

Figure 4-46: Assigning Manipulation Set 4 to the Twilio SIP Trunk IP Group



The screenshot shows the 'Edit Row' dialog box with the following fields and values:

Field	Value
Index	2
SRD	DefaultSRD
Common	
GW	
SBC	
SBC Operation Mode	Not Configured
Classify By Proxy Set	Enable
SBC Client Forking Mode	Sequential
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	4
Msg Man User Defined String1	
Msg Man User Defined String2	
Registration Mode	User Initiates Regis
Max. Number of Registered Users	-1
Authentication Mode	User Authenticates
Authentication Method List	
Username	

Buttons: Save, Cancel

- e. Click **Submit**.

4.14 Step 14: Configure Miscellaneous Settings

This section describes the configuration of miscellaneous E-SBC settings.

4.14.1 Step 14a: Configure Classification Table

This step shows how to configure the E-SBC Classification Table. For the interoperability test topology with the Twilio SIP Trunk, the **Proxy** FQDN Address is configured in the Proxy Set Table and all outgoing calls are routed to this **Proxy** FQDN Address. However incoming calls from Twilio may arrive from different global locations (Twilio has local servers in main global regions). Consequently, it's necessary to also allow SIP messages to be received from these different local Twilio servers.

Ø To configure Classification Table:

1. Open the Classification Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Classification Name	Twilio Termination URI (arbitrary descriptive name)
Source SIP Interface	Twilio
Source Host	ilync15.pstn.twilio.com (Twilio FQDN)

Figure 4-47: Classification Table Page – Rule Tab

Edit Row

Index

0

SRD

DefaultSRD

Rule

Action

Name

Twilio Termination URI

Source SIP Interface

Twilio

Source IP Address

Source Transport Type

Any

Source Port

0

Source Username Prefix

*

Source Host

ilync15.pstn.twilio.com

Destination Username Prefix

*

Destination Host

*

Message Condition

None

[Classic View](#)

Save

Cancel

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

Parameter	Value
Action Type	Allow
Source IP Group	Twilio
IP Profile	Twilio

Figure 4-48: Classification Table Page – Action Tab

Edit Row

Index: 0
SRD: DefaultSRD

Rule **Action**

Action Type: Allow
Destination Routing Policy: None
Source IP Group: Twilio
IP Profile: Twilio

[Classic View](#)

Save Cancel

5. Click **Submit**.

Figure 4-49: Example of Classification Table

Classification Table

Add + Edit Edit Delete Delete Insert + Up ↑ Down ↓ Show / Hide Show

All Search in table Search

Index	Name	SRD	Source SIP Interface	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Action Type	Source IP Group
0	Twilio Termination URI	DefaultSRD	*	*	ilync15.pstn.twilio.com	*	*	Allow	Twilio

Page 1 of 1 10 View 1 - 1 of 1

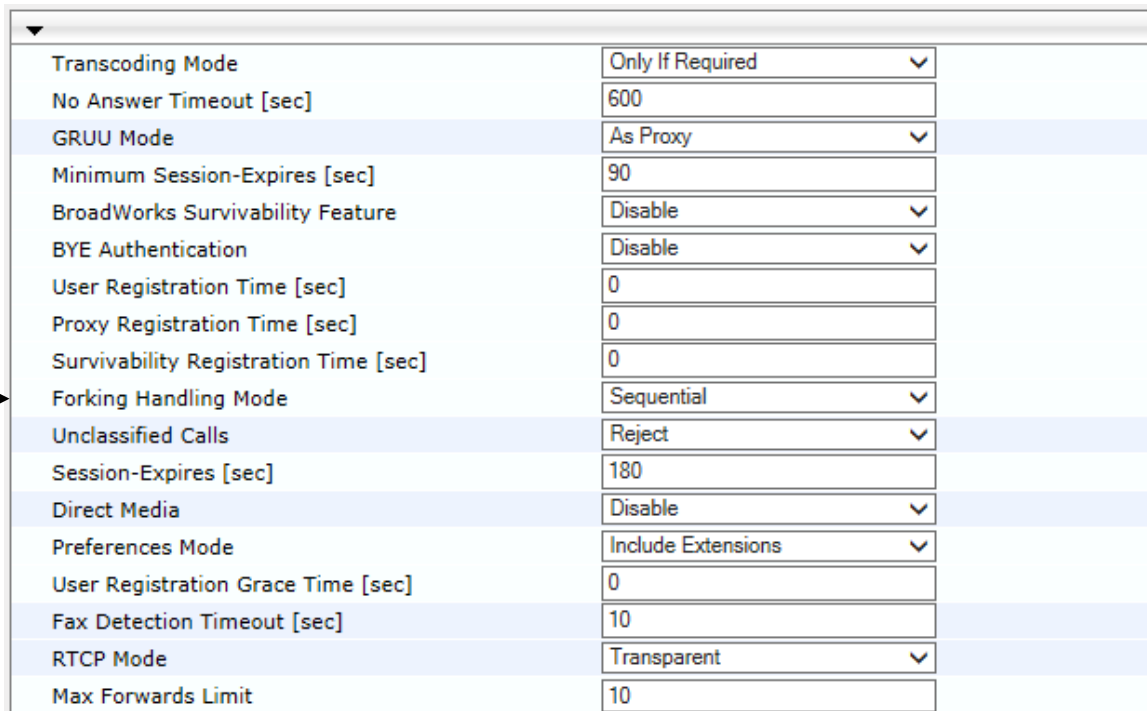
4.14.2 Step 14b: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if a SIP 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ring-back tone if a 180 response without SDP is received. It is mandatory to set this field for the Lync Server 2013 environment.

Ø To configure call forking:

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

Figure 4-50: Configuring Forking Mode



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

3. Click **Submit**.

4.14.3 Step 14c: Disable Lifetime in Crypto Line of SDP

This step describes how to disable sending lifetime value in the crypto line of SDP portion of SIP messages sent toward Twilio SIP Trunk.

Ø **To disable lifetime in crypto line of SDP:**

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://10.15.17.77/AdminPage>).
2. In the left pane, click **ini Parameters**.

Figure 4-51: Configuring SBC Media Sync in AdminPage

Parameter Name: Enter Value:

Output Window

```
Parameter Name: DISABLECRYPTOLIFETIMEINSDP
Parameter New Value: 1
Parameter Description: Disable Crypto Life Time In SDP
```

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

Parameter	Value
DisableCryptoLifeTimeInSDP	1 (This disable sending lifetime value in the crypto line of SDP portion of SIP messages)

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

4.15 Step 15: Reset the E-SBC

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

Ø To save the configuration to flash memory:

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

Figure 4-52: Resetting the E-SBC



The screenshot shows a web-based configuration interface for the E-SBC. It is divided into three main sections:

- Reset Configuration:** Contains a 'Reset Board' button, a 'Burn To FLASH' dropdown menu set to 'Yes', and a 'Graceful Option' dropdown menu set to 'No'.
- LOCK / UNLOCK:** Contains a 'Lock' button, a 'Graceful Option' dropdown menu set to 'No', and a 'Gateway Operational State' label showing 'UNLOCKED'.
- Save Configuration:** Contains a 'Burn To FLASH' button labeled 'BURN'.

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

A AudioCodes INI File for UDP/RTP

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



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

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 2265355
;Slot Number: 1
;Software Version: 7.00A.013.015
;DSP Software Version: 5014AE3_R => 700.32
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M  Flash size: 64M  Core speed: 300Mhz
;Num of DSP Cores: 3  Num DSP Channels: 60
;Num of physical LAN ports: 12
;Profile: NONE
;;Key features;;Board Type: 72 ;Channel Type: DspCh=60 IPMediaDspCh=60
;HA ;QOE features: VoiceQualityMonitoring MediaEnhancement ;DATA
features: ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;DSP Voice features: RTCP-XR ;Coders: G723 G729
G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722
EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB
OPUS_WB ;E1Trunks=2 ;T1Trunks=2 ;FXSPorts=4 ;FX0Ports=4 ;BRITrunks=4 ;IP
Media: Conf VXML ;Control Protocols: MGCP SIP SASurvivability SBC=60 MSFT
CLI TRANSCODING=60 FEU=100 TestCall=100 EMS LAD=20 ;Default
features;;Coders: G711 G726;

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

[SYSTEM Params]

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

```
[BSP Params]

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

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]

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

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UserProductName = 'Mediant 800 E-SBC'
WebLogoText = 'Twilio'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
```

```

SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_3", 1, 4, "User Port #2", "GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 0, 4, "User Port #4", "None", " ";
PhysicalPortsTable 5 = "FE_5_2", 0, 4, "User Port #5", "None", " ";
PhysicalPortsTable 6 = "FE_5_3", 0, 4, "User Port #6", "None", " ";
PhysicalPortsTable 7 = "FE_5_4", 0, 4, "User Port #7", "None", " ";
PhysicalPortsTable 8 = "FE_5_5", 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 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_1", "GE_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_3", "GE_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";

```

```

EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

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

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.77, 16, 10.15.0.1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.158, 25, 195.189.192.129, "WANSP",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

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

[ \DspTemplates ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$LE0VGBxUAQFSUAJXUQANXwoPDwtaeSNwInB2c3B+eihzKSgvfDIzMDI1YGc0YWhub2h1P
GpUVwdVBlnSBgpRXV4=", 1, 0, 2, 15, 60, 200,
"62cabed25276f6d59432fcac295a1346";
WebUsers 1 = "User",
"$1$FrWchL04t0HmvOKy70iys7m5vrzbzpqfyoKL0r6v7q/iv/P35kpmUwcXBkZWYy5iaz8+Wm
NGBgoPXhdTRi4yDj94=", 1, 0, 2, 15, 60, 50,
"e124fc45691a62316416e055a60edb6f";

```

```
[ \WebUsers ]
```

```
[ TLSContexts ]
```

```
FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts_0 = "default", 1, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;
```

```
[ \TLSContexts ]
```

```
[ IpProfile ]
```

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

```

IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandlerRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 0, -1, 0, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 0, 1, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 2 = "Twilio", 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, 1, "", -1, -1, 0, 2,
0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 0, 0, 1, 3, 0, 1, 0,
1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 5, 0, 0, 0, 0, 1, 0,
0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;

[ \IpProfile ]

[ CpMediaRealm ]

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

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]

[ SRD ]

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

[ \SRD ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,

```

```

SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer;
SIPInterface 0 = "Lync", "Voice", 2, 0, 0, 5067, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0;
SIPInterface 1 = "Twilio", "WANSP", 2, 5060, 0, 0, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1, 0;

[ \SIPInterface ]

[ ProxySet ]

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

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 0 = 0, "Lync", "Lync", "ilync15.pstn.twilio.com", "", -1, 0,
"DefaultSRD", "MRLan", 1, "Lync", -1, -1, -1, 0, 0, "", 0, -1, -1, "",
"", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, 0, 0, -1, 0;
IPGroup 1 = 0, "Twilio", "Twilio", "ilync15.pstn.twilio.com", "", -1, 0,
"DefaultSRD", "MRWan", 1, "Twilio", -1, -1, 4, 0, 0, "", 0, -1, -1, "",
"", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, 0, 0, -1, 0;

[ \IPGroup ]

```

```
[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "FE15.ilync15.local:5067", 2;
ProxyIp 1 = "1", 0, "ilync15.pstn.twilio.com:5060", 0;

[ \ProxyIp ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS termination", "Default_SBCRoutingPolicy",
"Lync", "*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal",
0, -1, 0, 0, "";
IP2IPRouting 1 = "Lync to ITSP", "Default_SBCRoutingPolicy", "Lync", "*",
"*, "*", "*", 0, "", "Any", 0, -1, 0, "Twilio", "Twilio", "", 0, -1, 0,
0, "";
IP2IPRouting 2 = "ITSP to Lync", "Default_SBCRoutingPolicy", "Twilio",
"*, "*", "*", "*", 0, "", "Any", 0, -1, 0, "Lync", "Lync", "", 0, -1, 0,
0, "";

[ \IP2IPRouting ]

[ Classification ]

FORMAT Classification_Index = Classification_ClassificationName,
Classification_MessageConditionName, Classification_SRDName,
Classification_SrcSIPInterfaceName, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePrefix, Classification_SrcHost,
Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupName,
Classification_DestRoutingPolicy, Classification_IpProfileName;
Classification 0 = " Twilio Termination URI", "", "DefaultSRD", "Twilio",
"", 0, -1, "", " ilync15.pstn.twilio.com", "*", "*", 1, "Twilio", "",
"Twilio";

[ \Classification ]

[ CodersGroup0 ]

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

```

[ \CodersGroup0 ]

[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = "g711Ulaw64k";

[ \AllowedCodersGroup0 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change Host of History-Info.0", 4,
"invite.request", "header.history-info.0 regex
(.*)(@)(.*)((user=phone)(.*)" , "header.history-info.0", 2,
"$1+$2+param.ipg.dst.host+$4+$5", 0;
MessageManipulations 1 = "Remove History-Info.1", 4, "invite.request",
"", "header.history-info.1", 1, "", 0;
MessageManipulations 2 = "Change Referred-by Host", 4, "invite.request",
"header.referred-by exists", "header.referred-by.url.host", 2,
"param.ipg.dst.host", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]

```

This page is intentionally left blank.

B AudioCodes INI File for TLS/SRTP

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



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

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 2265355
;Slot Number: 1
;Software Version: 7.00A.043.004
;DSP Software Version: 5014AE3_R => 700.40
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M  Flash size: 64M  Core speed: 300Mhz
;Num of DSP Cores: 3  Num DSP Channels: 60
;Num of physical LAN ports: 12
;Profile: NONE
;;;Key features;;Board Type: 72 ;Channel Type: DspCh=60 IPMediaDspCh=60
;HA ;QOE features: VoiceQualityMonitoring MediaEnhancement ;DATA
features: ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;DSP Voice features: RTCP-XR ;Coders: G723 G729
G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722
EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB
OPUS_WB ;E1Trunks=2 ;T1Trunks=2 ;FXSPorts=4 ;FX0Ports=4 ;BRITrunks=4 ;IP
Media: Conf VXML ;Control Protocols: MGCP SIP SASurvivability SBC=60 MSFT
CLI TRANSCODING=60 FEU=100 TestCall=100 EMS LAD=20 ;Default
features;;Coders: G711 G726;

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

[SYSTEM Params]

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

```
[BSP Params]

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

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]

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

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

ENABLEMEDIASEcurity = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UserProductName = 'Mediant 800 E-SBC'
WebLogoText = 'Twilio'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSPkeyFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value
PacketSmartPlatform = 'M800'

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
```

```

SBPPREFERENCESMODE = 1
DISABLECRYPTOLIFETIMEINSDP = 1
SBPFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_3", 1, 4, "User Port #2", "GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 0, 4, "User Port #4", "None", " ";
PhysicalPortsTable 5 = "FE_5_2", 0, 4, "User Port #5", "None", " ";
PhysicalPortsTable 6 = "FE_5_3", 0, 4, "User Port #6", "None", " ";
PhysicalPortsTable 7 = "FE_5_4", 0, 4, "User Port #7", "None", " ";
PhysicalPortsTable 8 = "FE_5_5", 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 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_1", "GE_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_3", "GE_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";
EtherGroupTable 6 = "GROUP_7", 0, "", "";

```

```

EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

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

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.77, 16, 10.15.0.1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.158, 25, 195.189.192.129, "WANSP",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

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

[ \DspTemplates ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$LE0VGBxUAQFSUAJXUQANXwoPDwtaeSNwInB2c3B+eihzKSgvfDIzMDI1YGc0YWhub2h1P
GpUVwdVB1NSBgprXV4=", 1, 0, 2, 15, 60, 200,
"62cabed25276f6d59432fcdf295a1346";
WebUsers 1 = "User",
"$1$FrWcHL04tOHmvOKy70iys7m5vrbzpqfyoKL0r6v7q/iv/P35kpmUwcXBkZWYy5iaz8+Wm

```

```

NGBgoPXhdTRi4yDj94=", 1, 0, 2, 15, 60, 50,
"e124fc45691a62316416e055a60edb6f";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 1, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;
TLSContexts 1 = "Twilio", 1, "AES:RC4", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPptimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,

```

```

IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWTToVoiceCoderBW;

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, "", 0, -1, 0, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 0, 1, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;
IpProfile 2 = "Twilio", 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, 1, "", -1, -1, 0, 1,
0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 0, 0, 1, 3, 0, 1, 0,
1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 5, 0, 0, 0, 0, 0, 1, 0,
0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;

[ \IpProfile ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 100, 6999, 1, "", "";
CpMediaRealm 1 = "MRwan", "WANSP", "", 7000, 100, 7999, 0, "", "";

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]

[ SRD ]

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

[ \SRD ]

```

[SIPInterface]

```

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer;
SIPInterface 0 = "Lync", "Voice", 2, 0, 0, 5067, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0;
SIPInterface 1 = "Twilio", "WANSP", 2, 5060, 0, 5061, "DefaultSRD", "",
"Twilio", -1, 0, 500, -1, 0, "MRwan", 0, -1, -1, -1, 0;

```

[\SIPInterface]

[ProxySet]

```

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

```

[\ProxySet]

[IPGroup]

```

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWPProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID;
IPGroup 0 = 0, "Lync", "Lync", "ilync15.pstn.twilio.com", "", -1, 0,
"defaultSRD", "MRLan", 1, "Lync", -1, -1, -1, 0, 0, "", -1, -1, "",
"", "$!$gQ==", 0, "", "", "", 0, "", "", 0, 0, 0, 0, -1, 0, 0;

```

```

IPGroup 1 = 0, "Twilio", "Twilio", "ilync15.pstn.twilio.com", "", -1, 0,
"DefaultSRD", "MRWan", 1, "Twilio", -1, -1, 4, 0, 0, "", 0, -1, -1, "",
"", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0;

[ \IPGroup ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "0", 0, "FE15.ilync15.local:5067", 2;
ProxyIp 1 = "1", 0, "ilync15.pstn.twilio.com:5061", 2;

[ \ProxyIp ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS termination", "Default_SBCRoutingPolicy",
"Lync", "", "", "", "", 6, "", "Any", 0, -1, 1, "", "", "internal",
0, -1, 0, 0, "";
IP2IPRouting 1 = "Lync to ITSP", "Default_SBCRoutingPolicy", "Lync", "",
"", "", "", 0, "", "Any", 0, -1, 0, "Twilio", "Twilio", "", 0, -1, 0,
0, "";
IP2IPRouting 2 = "ITSP to Lync", "Default_SBCRoutingPolicy", "Twilio",
"", "", "", "", 0, "", "Any", 0, -1, 0, "Lync", "Lync", "", 0, -1, 0,
0, "";

[ \IP2IPRouting ]

[ Classification ]

FORMAT Classification_Index = Classification_ClassificationName,
Classification_MessageConditionName, Classification_SRDName,
Classification_SrcSIPInterfaceName, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePrefix, Classification_SrcHost,
Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupName,
Classification_DestRoutingPolicy, Classification_IpProfileName;
Classification 0 = "Twilio Termination URI", "", "DefaultSRD", "Twilio",
"", 0, -1, "", "ilync15.pstn.twilio.com", "", "", 1, "Twilio", "",
"Twilio";

[ \Classification ]

[ IPOutboundManipulation ]

```

```

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 1 = "For Anonymous Test",
"Default_SBCRoutingPolicy", 0, "Lync", "Twilio", "*", "*", "*", "*", "*",
"", 0, "Any", 0, 0, 0, 0, 255, "", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

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

[ \CodersGroup0 ]

[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = "g711Ulaw64k";

[ \AllowedCodersGroup0 ]

[ IDSRule ]

FORMAT IDSRule_Index = IDSRule_Policy, IDSRule_RuleID, IDSRule_Reason,
IDSRule_ThresholdScope, IDSRule_ThresholdWindow,
IDSRule_MinorAlarmThreshold, IDSRule_MajorAlarmThreshold,
IDSRule_CriticalAlarmThreshold, IDSRule_DenyThreshold,
IDSRule_DenyPeriod;
IDSRule 10 = "", 0, 1, 0, 3, 15, -1, -1, -1, -1;
IDSRule 11 = "", 1, 2, 0, 3, 50, -1, -1, -1, -1;
IDSRule 12 = "", 2, 3, 0, 5, 30, -1, -1, -1, -1;
IDSRule 13 = "", 3, 4, 0, 3, 50, -1, -1, -1, -1;
IDSRule 14 = "", 4, 5, 0, 3, 50, -1, -1, -1, -1;

[ \IDSRule ]

```

```
[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change Host of History-Info.0", 4,
"invite.request", "header.history-info.0 regex
(.*)(@)(.*)((;user=phone)(.*)" , "header.history-info.0", 2,
"$1+$2+param.ipg.dst.host+$4+$5", 0;
MessageManipulations 1 = "Remove History-Info.1", 4, "invite.request",
"", "header.history-info.1", 1, "", 0;
MessageManipulations 2 = "Change Referred-by Host", 4, "invite.request",
"header.referred-by exists", "header.referred-by.url.host", 2,
"param.ipg.dst.host", 0;
MessageManipulations 3 = "Error Responses Test", 14, "any.response",
"header.request-uri.methodtype=='480'", "header.request-uri.methodtype",
2, "'503'", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

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

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com



Document #: LTRT-12412