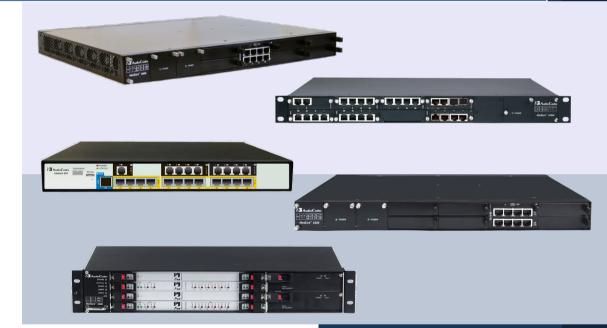
AudioCodes[™] Mediant[™] Series

Enterprise Session Border Controller (E-SBC)

Interoperability Laboratory

Configuration Note

Connecting Microsoft[®] Lync[™] Server 2013 with ITSP SIP Trunk using AudioCodes E-SBC







L 🕽 Lync



Version 6.6 December 2013 Document #: LTRT-54006

Table of Contents

1	1 Introduction				
	1.1	Intended Audience	9		
	1.2	About AudioCodes E-SBC Product Series			
2	Component Information				
	2.1	AudioCodes E-SBC Version	11		
	2.2	Microsoft Lync Server 2013 Version			
	2.3	Deploying the E-SBC			
		2.3.1 Example Environment			
		2.3.2 Environment Setup			
3	Con	figuring Microsoft Lync Server 2013	.15		
	3.1	Configuring the E-SBC as an IP / PSTN Gateway	15		
	3.2	Configuring 'Route' on Lync Server 2013			
4	Con	figuring AudioCodes E-SBC	.35		
	4.1	Step 1: Configuring the E-SBC's Network Interfaces	36		
		4.1.1 Configuring IP Network Interfaces for LAN and WAN			
		4.1.2 Configuring the Native VLAN ID	38		
	4.2	Step 2: Enabling the SBC Application	39		
	4.3	Step 3: Configuring SRDs			
		4.3.1 Configuring Media Realms			
		4.3.2 Configuring SRDs4.3.3 Configuring SIP Signaling Interfaces			
	4.4	Step 4: Configuring Proxy Sets			
	4.5	Step 5: Configuring IP Groups			
	4.6	Step 6: Configuring IP Profiles			
	4.7	Step 7: Configuring Coders			
	4.8	Step 8: Configuring a SIP TLS Connection			
		4.8.1 Configuring the NTP Server Address			
		4.8.2 Configuring a Certificate			
	4.9	Step 9: Configuring SRTP			
		Step 10: Configuring IP Media			
		Step 11: Configuring IP-to-IP Call Routing Rules			
		Step 12: Configuring IP-to-IP Outbound Manipulation			
		Step 13: Configuring SIP Message Manipulation Rules			
		Step 14: Configuring a Registration Account			
		Step 15: Configuring Miscellaneous E-SBC Functionalities			
	4.16	Step 16: Resetting the E-SBC	73		
Α	Con	figuring E-SBC to Send 414 Request-URI Too Long Response	.75		

List of Figures

Figure 2-1: E-SBC Interworking Lync 2013 and a SIP Trunk in an Example Environment	12
Figure 3-1: Starting the Lync Server Topology Builder	
Figure 3-2: Topology Builder Options.	
Figure 3-3: Save Topology	
Figure 3-4: Topology Builder Displaying Downloaded Topology	17
Figure 3-5: Selecting New IP/PSTN Gateway	
Figure 3-6: Define New IP/PSTN Gateway	
Figure 3-7: Define the IP Address	
Figure 3-8: Define the Root Trunk	20
Figure 3-9: E-SBC Added as an IP/PSTN Gateway and Trunk Created	
Figure 3-10: Selecting 'Publish Topology' from the 'Action' Menu	21
Figure 3-11: Publish Topology	22
Figure 3-12: Publish Topology Progress Screen	23
Figure 3-13: Publish Topology Successfully Completed	24
Figure 3-14: Opening the Lync Server Control Panel	25
Figure 3-15: Lync Server Credentials	
Figure 3-16: Microsoft Lync Server 2013 Control Panel	26
Figure 3-17: Voice Routing	
Figure 3-18: Route Option	
Figure 3-19: Adding New Voice Route	
Figure 3-20: Adding New Trunk	
Figure 3-21: List of Deployed Trunks	
Figure 3-22: Selected E-SBC Trunk	
Figure 3-23: Associating PSTN Usage with the Route	
Figure 3-24: Confirmation of New Voice Route	
Figure 3-25: Committing Voice Routes	
Figure 3-26: Uncommitted Voice Configuration Settings	
Figure 3-27: Confirmation of a Successful Voice Routing Configuration	
Figure 3-28: Voice Routing Screen Displaying Committed Routes	
Figure 4-1: Network Interfaces	
Figure 4-2: IP Interfaces Table	
Figure 4-3: Ports Native VLAN	
Figure 4-4: Applications Enabling	
Figure 4-5: Configuring a LAN Media Realm	
Figure 4-6: Configuring a WAN Media Realm	
Figure 4-7: Required Media Realm Table	41
Figure 4-8: Configuring the LAN SRD	
Figure 4-9: Configuring the WAN SRD	
Figure 4-10: Required SIP Interface Table	43
Figure 4-11: Proxy Set for Microsoft Lync Server 2013	45
Figure 4-12: Configuring a Proxy Set for the SIP Trunk	
Figure 4-13: Configured IP Group Table	
Figure 4-14: Configured IP Profile for Lync Server 2013	
Figure 4-15: Configured IP Profile for SIP Trunk	
Figure 4-16: Configured Coder Group for Lync Server 2013	53
Figure 4-17: Configured Coder Group for the SIP Trunk	
Figure 4-18: Allowed Coders Group for SIP Trunk	
Figure 4-19: Configuring the NTP Server IP Address	
Figure 4-20: Certificates Page - Creating CSR	
Figure 4-21: Microsoft Certificate Services Web Page	
Figure 4-22: Request a Certificate Page	
Figure 4-23: Advanced Certificate Request Page	
Figure 4-24: Submit a Certificate Request or Renewal Request Page	
Figure 4-25: Certificate Issued Page	
Figure 4-26: Download a CA Certificate, Certificate Chain, or CRL	
Figure 4-27: Certificates Page (Uploading Certificate)	
Figure 4-28: Media Security Page	

Figure 4-29: IP Media Settings	.62
Figure 4-30: Configured IP-to-IP Routing Rule to Terminate SIP OPTIONS Messages Received fron	n
the LAN	.64
Figure 4-31: IP-to-IP Routing Rule for LAN to WAN	.65
Figure 4-32: Configured IP-to-IP Routing Rule to Route Calls from WAN to LAN	.66
Figure 4-33: IP-to-IP Routing Table	.66
Figure 4-34: IP-to-IP Outbound Manipulation Rule – Rule Tab	.67
Figure 4-35: Configured IP-to-IP Outbound Manipulation Rule - Action Tab	.68
Figure 4-36: IP-to-IP Outbound Manipulation	.68
Figure 4-37: Message Manipulations Page	.69
Figure 4-38: Configured SIP Message Manipulation Rule	
Figure 4-39: Assigning a Manipulation Rule to IP Group 2	.70
Figure 4-40: Configuring a SIP Registration Account	.71
Figure 4-41: Configuring Forking Mode	.72
Figure 4-42: Resetting the E-SBC	.73
Figure A-1: Configuring a Condition for the Route	.75
Figure A-2: IP-to-IP Routing Rule for Long-URI Calls	.76
Figure A-3: Manipulation Rule to Set a Variable to '1' in Case of Long-URI Call	.77
Figure A-4: Manipulation Rule to Convert 408 to '414'	.77
Figure A-5: Message Manipulations Page	.78
Figure A-6: Assigning Manipulation Rule to IP Group 1	.78



Reader's Notes

Notice

This Configuration Note shows how to connect Microsoft Lync Server 2013 and a 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 software files bv reaistered well as can be viewed customers at http://www.audiocodes.com/downloads.

© Copyright 2013 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: December-8-2013

Trademarks

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

WEEE EU Directive

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

Customer Support

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



Reader's Notes

1 Introduction

This Configuration Note shows how to configure AudioCodes' Enterprise Session Border Controller (E-SBC) for interworking between an ITSP (Internet Telephony Service Provider's) SIP (Session Initiation Protocol) Trunking service and Microsoft's Lync communication platform (Lync Server 2013).

The Note shows how to connect Microsoft Lync Server 2013 and a SIP Trunk using AudioCodes Mediant E-SBC product series, which includes the Mediant 1000B Gateway & E-SBC, Mediant 800 Gateway & E-SBC, Mediant 2600 E-SBC, Mediant 4000 E-SBC and Mediant 3000 Gateway & E-SBC.

1.1 Intended Audience

The Configuration Note is intended for engineers or AudioCodes and Partners who are responsible for installing and configuring SIP Trunking and Microsoft's Lync communication platform for enabling VoIP calls using AudioCodes' E-SBC.

1.2 About AudioCodes E-SBC Product Series

AudioCodes' family of E-SBC devices enables reliable connectivity and security between an enterprise's VoIP network and the ITSP's VoIP network.

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

Designed as a cost-effective appliance, the E-SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability.

The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

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



Reader's Notes

2 Component Information

2.1 AudioCodes E-SBC Version

SBC Vendor	AudioCodes		
Models	 Mediant 800 Gateway & E-SBC Mediant 1000B Gateway & E-SBC Mediant 2600 E-SBC Mediant 3000 Gateway & E-SBC Mediant 4000 E-SBC 		
Software Version	SIP_6.60A or later		
Protocol	SIP/UDP (to the ITSP's SIP Trunk)SIP/TCP or TLS (to the Lync Front End Server)		
Additional Notes	None		

2.2 Microsoft Lync Server 2013 Version

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

2.3 Deploying the E-SBC

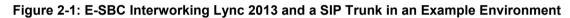
2.3.1 Example Environment

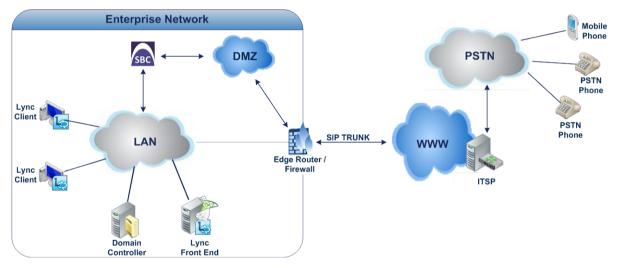
The example scenario below is referred to throughout this document in order to show how to deploy the E-SBC.

In the example environment:

- Microsoft Lync Server 2013 is deployed in an enterprise's private network for enhanced communication within the enterprise.
- The enterprise wants to offer its employees enterprise-voice capabilities and to connect the enterprise to the PSTN network using a SIP Trunking service provided by the enterprise's ITSP.
- AudioCodes' E-SBC is implemented to interconnect between the enterprise's LAN and the SIP Trunk.
 - Session: Real-time voice session using IP-based SIP
 - Border: IP-to-IP network border between Lync Server 2013 network in the enterprise LAN and the SIP Trunk located in the public network.

The figure below illustrates AudioCodes' E-SBC interworking between Microsoft Lync Server 2013 and an ITSP's SIP Trunking site.





2.3.2 Environment Setup

The example scenario includes the following environment setup:

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



Reader's Notes

3 Configuring Microsoft Lync Server 2013

This section shows 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 but are beyond the scope of this document.

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

This section shows how to configure the E-SBC as an IP / PSTN Gateway.

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



Figure 3-1: Starting the Lync Server Topology Builder



This screen is displayed:

Figure 3-2: Topology Builder Options

🔜 Topology Builder 🛛 🔀						
Welcome to Topology Builder. Select the source of the Lync Server 2010 (RC) topology document.						
 Download Topology from existing deployment Retrieve a copy of the current topology from the Central Management Store database and save it as a local file. Use this option if you are editing an existing deployment. 						
Open Topology from a local file Open an existing Topology Builder file. Use this option if you have work in progress or if you have exported a topology from Planning Tool.						
New Topology Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.						
OK Cancel						

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

Figure 3-3: Save Topology

Save Topology As 🛛 🗙					
Administ	rator 🔻 Documents	👻 🛃 Search			
🕘 Organize 🔻 📗 Views	👻 📑 New Folder		0		
Favorite Links Image: Desktop Image: Computer Image: Documents Image: Pictures Image: Music Image: Recently Changed Image: Searches Image: Public	Name	▼ Date modified ▼ Type 10/7/2010 5:53 PM TBXML File 10/12/2010 10:5 TBXML File			
	op2.tbxml logy Builder files (*.tbxm	0	• •		
Hide Folders		<u>S</u> a	Cancel		

3. Enter a name for the Topology file and 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:

Lync Server 2013, Topology Builder			×
File Action Help			
E kunc Server	SIP domain	•	
AudioCodes Lync Server 2010	Jir domain		_
E Durc Server 2013	Default SIP domain:	iLync15.local	
Enterprise Edition Front End Servers	Additional supported SIP	Not configured	
Director pools	domains:		
H Mediation pools			
Persistent Chat pools Edge pools	Simple URLs		
Trusted application servers	Simple URLs	_	<u> </u>
Components Define the second	Phone access URLs:	Active Simple URL	
	mone access ones.	Active Simple URL thtps://dialin.il.ync15.local	
	Meeting URLs:	Active Simple URL SIP domain	
		V https://met.ityneit.itynet.itynet.itynet.itynet.itynet.itynet.itynet.itynet.itynet.i	
	Administrative access	https://admin.iLync15.local	
	URL:		
	Central Management Serve	<i>ч</i>	
		•	-
	Central Management Server:	Active Front End Site	
	Server	FELSubmetS-local AudioCodes	

- **4.** In the tree, expand Lync Server 2013 > your site name > Shared Components.
- 5. Right-click the **PSTN Gateways** folder and select **New IP/PSTN Gateway** from the popup menu:



🔀 Lync Server 2013, Topology Builder		_ 8 ×
File Action Help		
🖃 🛃 Lync Server	The properties for this item are not available for editing.	
🖃 🚮 AudioCodes	The properties for any feat of end of endings	
E Lync Server 2010		
Lync Server 2013		
E Standard Edition Front End Servers		
Enterprise Edition Front End pools		
Director pools		
Mediation pools		
Persistent Chat pools		
Care Edge pools		
Instead application servers Shared Components		
SQL Server stores		
File stores		
PSTN gateway New ID/0CTN Colored		
GW1.iLyn	3 /	
PSTN gateway New IP/PSTN Gatewa GW1.iLyn Colt.ilync1 Colt.ilync1 Colt.ilync1	TN gateway.	
🕂 🧰 Trunks		
Branch sites		
🍂 Start 🐁 🍞 🔯		🏱 🐑 🎝 12:45 PM 📃



This dialog opens:

Figure 3-6: Define New IP/PSTN Gateway

🔀 Define N	ew IP/PSTN Gateway			×
-	Define the PSTN Gateway FQDN			
FQDN: *	e fully qualified domain name (FQDN) for the PSTN gat	eway.		
1151 01				
11.1		nut I	Next	count 1
Help		<u>B</u> ack	Next	Cancel

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

Figure 3-7: Define the IP Address

🔀 Define New IP/PSTN Gateway 🛛 🔀
Define the IP address
Enable IPv4
Use all configured IP addresses.
<u>Limit service usage to selected IP addresses.</u>
PSTN <u>I</u> P address:
C Enable IPv <u>6</u>
Use all configured IP addresses.
C Limit service usage to selected IP addresses.
PSTN <u>I</u> P address:
J
Help <u>B</u> ack <u>N</u> ext Cancel

- 8. Click Next.
- 9. Define a root trunk for the PSTN gateway. A trunk is a logical connection between a Mediation Server and a gateway, uniquely identified by the combination {Mediation Server FQDN, Mediation Server listening port (TLS or TCP): gateway IP and FQDN, gateway listening port}
 - When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
 - The root trunk cannot be removed until the associated PSTN gateway is removed.



Figure 3-8: Define the Root Trunk

💑 Define New IP/PSTN Gateway	×
Solution Define the root trunk	
Trunk name: *	
ITSP-GW.ilync15.local	
Listening port for IP/PSTN gateway: *	
5067	
SIP T <u>r</u> ansport Protocol:	
TLS	•
Associated Mediation Server:	
FE15.ilync15.local AudioCodes	•
Associated Mediation Server port: *	
5067	
Help <u>B</u> ack <u>F</u> inish	Cancel

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

Click Finish; the SBC is added as a PSTN Gateway and a trunk is created:

Image: Second Secon	😽 Lync Server 2013, Topology Builder			_ <u>-</u>
Image: Comparison of the compar	File Action Help			
Image: Source 2000 Tank Image: Source 2000 Image: Source 2000 Tank and tank Image: S	😑 🛃 Lync Server			
Image: Norme 2013 Table 4 datases Image: Norme 2014 Statuse 4 datases </td <td>🖃 🚮 AudioCodes</td> <td>Trunk</td> <td></td> <td>^</td>	🖃 🚮 AudioCodes	Trunk		^
Image: Standard Edition Front End Starves First Warter Starves Image: Starves Holdston Starves Image: Starves Holdstore Starves Image: Starves Holdstore Starves Image: Starves Holdstore Starves Image: Starves				
Image: Statute Science	Lync Server 2013	Trunk name:	ITSP-GW.ilvnc15.local	
Control points Control	E Standard Edition Front End Servers			
SP Transport Photoes: T.S. G ge pool G Se pool Total splic for an energy Soft Soft Server pool Soft Server pool Soft Server pool Soft Server po				
Provident Chargools Mediation Server: Provident Chargools				
Bege pois Mediation Server pot: Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Comparents Barde Solution Barde Sol	Persistent Chat nools	SIP Transport Protocol:		
In Traded application servers Mediation Server port: 567 In State State Components In State St	Edge pools	Mediation Server:	FE15.ilync15.local (AudioCodes)	
Image: A start of Comparets Image: A start of Comparets		Mediation Server port:	5067	
I Get does	🖃 🚞 Shared Components			
STR gateways Str Will Aprice State Str Will Aprice Str Will Aprice Str Will Aprice April 100 Str Will Aprice Str Will April 100 Str Will April 1	E SQL Server stores			
WWILHANDSHOL	🗉 🚞 File stores			
Control of the second	PSTN gateways			
Control of the second	GW1.iLync15.local			
Control of the second	TTCP.CW iterats local			
© offerred states © Offer Web Apps Servers © ■ Branch states				
Control Social Control Social Control Web Appe Servers Control Web	°Z_Ofer			
Office Web Appe Servers Branch sites	Colt.ilync15.local			
The set of	TTSP-GW.ilync15.local			
	Office Web Apps Servers			
	Branch sites			
Stat 🚠 🕞 🐹				
Tran in The Instance in the In				
Stat 🚠 🕞 🕅				
Tstar 🚠 🏹 🕅				
Start 🚠 🕞 🐹				
Tstat 🚠 🏹 🔣				
27 Start 🚠 🏹 🔯				
Tstart 🚠 🏹 🔣				
27 Start 🚠 🏹 🔯				
🏹 Start 🚠 🏹 🔣				
🎦 Start 🚠 🏹 🔯				
🏧 🕄 🚵 🌍 🙀				
🎦 Start 🚠 🏹 🔣				
27 Start 🚠 😂 🔯				
🎦 Start 🚠 🍃 🙀				
27 Start 🚠 😂 😼				
🎦 Start 🚠 🍃 🔣				
27 Start 🚠 🌍 😼				
🌆 🐨 🕅 🕼 🖉 🕅				
27start 🚠 🎯 🙀				
🖉 💱 🤹 🙀				
🖉 Start 🚠 🙀 🔣				
	🖉 Start 🐁 🍞 🔀			P 🐑 🕼 1:51 PM 💻

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

 Publish the Topology: In the main tree, select the root item Lync Server and from the Action menu, select Publish Topology:



1	Lync S	Server 2013, Topology Builder			_ 8 ×
Fi	le Acti	on Help			
15	N	lew Central Site			
	Έ E	dit Properties	main		^
	0 D S	iew Topology Jpen Topology Jownload Topology iave a copy of Topology As Wikish Topology	ult SIP domain: tional supported SIP ains:	ILync15.local Not configured	
		nstall Database	_		
	1	Arge Office Communications Server 2007 R2 Topology	Publish topology to the Cen	tral Management store.	
		temove Deployment	an abilit topology to the cen		
	н	ielp File stores	e access URLs:	Active Simple URL	
		Destores Destores Destores Destores		https://dialin.it.ync15.local	
		GW1.il vnc15.local	Meeting URLs:	Active Simple URL SIP domain	
		GW1.iLync15.local		https://meet.il.ync15.local iLync15.local	
		ITSP-GW.ilync15.local	Administrative access	https://admin.il.ync15.local	
		Trunks	URL:	nepsi/administricts.com	
		°Z_ Ofer			
		2 colt.ilync15.local			
		CITSP-GW.ilync15.local			•
		Branch sites	entral Management Serve	۲ ۲	^
	±		Central Management		
			Server:	Active Front End Site	
				FE15.ilvnc15.local AudioCodes	
	Trank	i 🐁 🍃 😿		De c	🗐 👍 1:55 PM 📃
<u>^</u>	, scart	i 📾 词 i 🚧			🖂 🕼 тарыны 📷



The Publish Topology screen is displayed:

Figure 3-11: Publish Topology

Publish the topology
 In order for Lync Server 2013 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed: A validation check on the root node did not return any errors. A file share has been created for all file stores that you have configured in this topology. All simple URLs have been defined. For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured. For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed. You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role). If you are removing a Front End pool, all users, common area phones, analog devices, application contact objects, and conference directories have been removed from the pool.
When you are ready to proceed, click Next. Help Back Next Cancel

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

Figure 3-12: Publish Topology Progress Scree	Figure	3-12:	Publish	Topology	Progress	Screen
--	--------	-------	---------	----------	----------	--------

Þ	Publish Topology
	Publishing in progress
I	Please wait while Topology Builder tries to publish your topology.
	Succeeded
	Downloading topology
	Succeeded
	Downloading global simple URL settings
	Succeeded
	Updating role-based access control (RBAC) roles
	Succeeded
	Enabling topology
	<u>B</u> ack <u>N</u> ext Cancel

12. Wait for the publishing topology process to successfully complete:



Figure 3-13: Publish Topology Successfully Completed

🔀 Publish Topology		×
Publishing wizard complete		
Your topology was successfully published.		
Step	Status	
Publishing topology Developed instances	Success Success	<u>V</u> iew Logs
 Downloading topology Downloading global simple URL settings 	Success	
 Updating role-based access control (RBAC) roles 	Success	
 Enabling topology 	Success	
To close the wizard, click Finish.		
Help	<u>B</u> ack <u>F</u> inish	Cancel

13. Click Finish.

3.2 Configuring 'Route' on Lync Server 2013

This section shows how to configure a 'Route' on the Lync Server 2013 and to associate it with the E-SBC PSTN gateway.

- To configure a 'route' on Lync Server 2013:
- Start the Microsoft Lync Server 2013 Control Panel: Click Start > All Programs > Microsoft Lync Server 2013 and then click Lync Server Control Panel:

Figure 3-14: Opening the Lync Server Control Panel

 Default Programs Internet Explorer (64-bit) Internet Explorer Windows Media Player Windows Update Accessories Administrative Tools Maintenance Microsoft Lync Server 2013 Lync Server Control Panel Lync Server Management Shell Lync Server Topology Builder Microsoft SQL Server 2012 Startup 	Administrator Documents FE15 Network Control Panel Devices and Printers Administrative Tools Help and Support Run Windows Security
 ● Back 	
Search programs and files	Log off

You're prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials

Connect to FE-Ly	nc.Lync.local	? ×
Connecting to FE	-Lync.Lync.local.	
<u>U</u> ser name:	🛃 Lync\Administra	tor 💌 💷
Password:	•••••	
	Remember my pa	issword
	ОК	Cancel

2. Enter your domain 'User name' and 'Password' and click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Alicrosoft Lync Server 2013 Control Panel _ 🗆 🗵 Administrator | Sign out Lync Server 2013 5.0.8308.0 | Privacy statement 🟠 Home 3 Users **User Information** Resources Topology IM and Presence Welcome, Administrator Getting Started First Run Checklist View your roles Persistent Chat Using Control Panel Microsoft Lync Server 2013 😢 Voice Routing **Top Actions** Using Office 365 📞 Voice Features Enable users for Lync Server Getting Help Edit or move users Response Groups Downloadable Documentation View topology status Online Documentation on TechNet Library Lync Server Management Shell Conferencing View Monitoring reports Lync Server Management Shell Script Library Clients Lync Server Resource Kit Tools Federation and 許 Community External Access Forums Blogs Monitoring and Archiving Security Network Ð Configuration

Figure 3-16: Microsoft Lync Server 2013 Control Panel

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

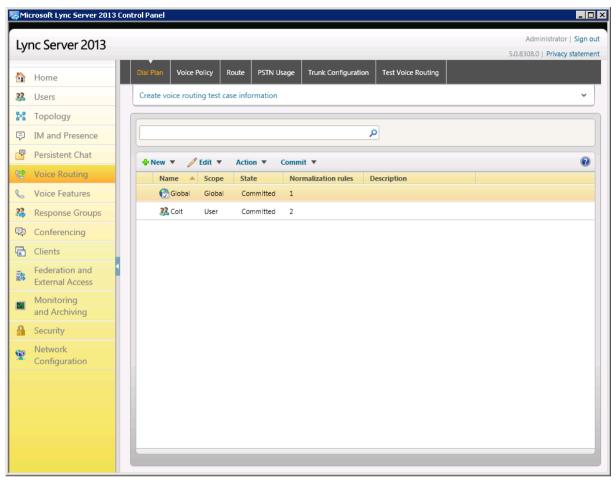


Figure 3-17: Voice Routing



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

Figure 3-18: Route Option

ync Server 20'	5					5.0.8308.0 Privacy statem
Home	Dial Plan	Voice Policy Ro	ute PSTN Usage T	runk Configuration Te	t Voice Routing	
Users	Create vo	ice routing test case	information			~
Topology						
IM and Presence				م		
Persistent Chat	4 New	🥖 Edit 🔻 🔺	Move up 🛛 👃 Move d	own Action v C	ommit 🔻	
Voice Routing	Nai	-	State	PSTN usage	Pattern to mat	
, Voice Features	Loc	alRoute	Committed	Internal, Local, Long Di	stance ^(\+1[0-9]{10})	5
Response Group	SBA	001	Committed	Internal, Local, Long Di	tance ^\+972355555	
Conferencing	COL	.т	Committed	Internal, Local, Long Di	tance ^\+00972	
Clients						
Federation and External Access						
Monitoring and Archiving						
Security						
Network Configuration						

5. Click **New**; the New Voice Route dialog opens:

Figure 3-19: Adding New Voice Route

OK Cancel	w Voice Route	
SiP Trunk Route escription: Build a Pattern to Match Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit. Starting digits for numbers that you want to allow: * Add Exceptions Remove Match this pattern:* ^5	OK X Cancel	
- Build a Pattern to Match - Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit. Starting digits for numbers that you want to allow: * Add Exceptions Remove Match this pattern:* ^	lame:*	
- Build a Pattern to Match Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit. Starting digits for numbers that you want to allow: * Add Exceptions Remove Match this pattern:* ^	SIP Trunk Route	
Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit. Starting digits for numbers that you want to allow:	Description:	
Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit. Starting digits for numbers that you want to allow: * Add Exceptions Remove Match this pattern:* ^		
Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit. Starting digits for numbers that you want to allow: * Add Exceptions Remove Match this pattern:* ^	Build a Pattern to Match	
Starting digits for numbers that you want to allow:		
* Add Exceptions Remove Match this pattern:*	the expression manually by clicking Edit.	
Match this pattern:*	Starting digits for numbers that you want to allow:	
Exceptions Remove		
Match this pattern:*		
^\$	Remove	
^\$		
^\$		
^\$		
Edit Reset	^\$	
	Edit Reset ?	

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

👸 Mio	rosoft Lync Server 2013	3 Control Panel	
1.0	ac Sonvor 2012		Administrator Sign out
Lyi	nc Server 2013		5.0.8308.0 Privacy statement
	Home	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
33	Users	Create voice routing test case information	~
М	Topology		
Ģ	IM and Presence	New Voice Route	
P	Persistent Chat	✓ OK X Cancel	0
Ç	Voice Routing	Exceptions	•
C	Voice Features	Remove	
23	Response Groups		
Ŗ	Conferencing	Match this pattern: *	
6	Clients	*	
1	Federation and External Access	Edit Reset	
	Monitoring and Archiving	Suppress caller ID	
1	Security	Alternate caller ID:	
9	Network Configuration	Associated trunks:	
		Add Remove	

Figure 3-20: Adding New Trunk

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



Home	Dial Plan Voi	ce Policy Route PSTN Usage Trunk (Configuration Test Voice Routing		
Users Users		outing test case information		0	
Тороlоду	S	elect Trunk		23 9	
IM and Presence	New Vo		٩		
Persistent Chat			, ,	_	0
		Service PstnGateway:GA001.ilync15.local	Site SBA001		
Voice Features		PstnGateway:GW1.iLync15.local	AudioCodes		
Response Groups		PstnGateway:SBA-GW.ilync15.local	SBA-test.ilync15.local		
Conferencing		PstnGateway:colt.ilync15.local	AudioCodes		
Clients	Ma .*	PstnGateway:ITSP-GW.ilync15.local	AudioCodes		
Federation and External Access					
Monitoring and Archiving	Si				
Security	A				
Network Configuration	Assoc			_	
			OK Car	ncel	
			KEINOYC		

Figure 3-21: List of Deployed Trunks

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

								_
er 2013							Adm	inistrator Si
				_			5.0.8308.0	Privacy stat
	Dial Plan	Voice Policy	Route	PSTN Usage	Trunk Configuration	Test Voice Routing	9	
	Create vo	pice routing tes	t case info	rmation				
/								
resence								
t Chat	-	OK 🗙 Can	cel					0
uting						Exceptions		Î
atures						Remove		
Groups								
cing		Match this patte	rn: *					
		*						
on and Access	-	Edit	Reset	?				
ng iving		Suppress caller	ID					
		Alternate caller	ID:					
ation	Asso	ociated trunks:						
		PstnGateway:[rsp			Add		
						Remove		
/ ree att att ci iv	Chat ing ures Groups ng and ccess	sence Chat ing and ccess ing	and seess and and and and and and and and	and teses and teses and teses bion Dial Plan Voice Policy Route Create voice routing test case info New Voice Route Vew Voice Route Vew Voice Route Vew Voice Route Vew Voice Route Chat Match this pattern: * * Buppress caller ID Alternate caller ID: PstnGateway:ITSP	Dial Plan Voice Policy Route PSTN Usage Create voice routing test case information Sence Chat ing Match this pattern: * * and tcsess ing Butternate caller ID Atternate caller ID: Associated trunks: PstnGateway:ITSP	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Create voice routing test case information Sence Chat ing Match this pattern: * * and creas Groups ing Suppress caller ID Atternate caller ID: Associated trunks: PstnGateway:ITSP	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing create voice routing test case information sence Chat ing ures Groups ng and create voice caller ID Atternate caller ID: ion PstnGatewayITSP Add Remove	Source Total Plan Voice Policy Roads PSTN Usage Trunk Configuration Test Voice Routing Create voice routing test case information Create voice Route New Voice Route New Voice Route Remove Remo

Figure 3-22: Selected E-SBC Trunk



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

licrosoft Lync Server 2013 Cor	trol Panel]
nc Server 2013		Administrator Sign
		5.0.8308.0 Privacy statem
Home	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
Users	Create voice routing test case information	*
Тороlоду		
IM and Presence	New Voice Route	
Persistent Chat	V X Cancel	0
Voice Routing		•
Voice Features	Associated trunks:	
Response Groups	PstnGateway:ITSP Add	
Conferencing	Remove	
Clients		
Federation and External Access	Associated PSTN Usages	
Monitoring	Select Remove 👚 🦊	
and Archiving	PSTN usage record Associated voice policies	
Security	Internal Global	
Network	Local Global	
Configuration	Long Distance Global	
	Translated number to test:	
		•

Figure 3-23: Associating PSTN Usage with the Route

11. Click **OK** (located under the New Voice Route section); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route

			٩	
🗣 New 🧪 Edit 🔻 👚 Move u	p 👆 Move down	Action 🔻 Com	nit 🔻	6
Name	State	PSTN usage	Pattern to match	
SIP Trunk Route	1 Uncommitted	Local, Internal	^/*	

12. From the Commit drop-down list, choose Commit all:

Figure 3-25: Committing Voice Routes

			٩	
🕈 New 🧪 Edit 🔻 👚 Move up	Hove down	Action 🔻	Commit 🔻	
Name	State	PSTN usa	Review uncommitted changes	
SIP Trunk Route	뛸 Uncommitted	Local, Inte	Commit all	

The Uncommitted Voice Configuration Settings dialog opens:

Uncor	mmitted Voice Config	guration Setting	5		0	×
Ro	outes				*	
	Identity	Action	New value (pattern to match)	Old value (pattern to match)		
	SIP Trunk Route	Added	^/*			
				C	ommit Canc	el .

Figure 3-26: Uncommitted Voice Configuration Settings

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

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

Home	Dial Plan Voice Policy	Route PSTN Usage Trur	nk Configuration Test Voice Routing		
Users	Create voice routing test ca	ase information			~
Тороlоду					
IM and Presence			Q		
Persistent Chat	P New / Edit ▼	Move up 🔒 Move dow	vn Action v Commit v		C
	Name	State	PSTN usage	Pattern to match	
Voice Features	LocalRoute	Committed	Internal, Local, Long Distance	^(\+1[0-9]{10})\$	
Response Groups	SBA001 Microsof	t Lync Server 2013 Con	trol Panel 🔞 🛛	^\+972355555	
Conferencing	COLT	sfully published voice ro		^\+00972	
] Clients	SIP Trun	sing published voice ro	uting configuration.	*	
Federation and External Access			Close		
Monitoring and Archiving					
Security					
Network Configuration					



14. Click **Close**; the newly committed Route is displayed in the Voice Routing screen:

Figure 3-28: Voice Routing Screen Displaying Committed Routes

Home	Dial Plan	Voice Policy	Route PS	TN Usage Trunk	Configuration	Test Voice Routing		
B Users	Create	voice routing tes	t case informat	ion				
Topology								
IM and Presence					م			
Persistent Chat	A New	🧪 Edit 🔻	1 Move up	👆 Move down	Action v	Commit 🔻		
Voice Routing	N	ame		State	PSTN usage		Pattern to match	
, Voice Features	Lo	ocalRoute		Committed	Internal, Loca	al, Long Distance	^(\+1[0-9]{10})\$	
Response Groups	SE	3A001		Committed	Internal, Loca	l, Long Distance	^\+972355555	
Conferencing	C	DLT		Committed	Internal, Loca	l, Long Distance	^\+00972	
Clients	SI	P Trunk Route		Committed	Internal, Loca	al, Long Distance	*	
Federation and External Access	•							
Monitoring and Archiving								
Security								
P Network Configuration								

4 Configuring AudioCodes E-SBC

This section shows how to configure AudioCodes' E-SBC for interworking between Microsoft Lync Server 2013 and an ITSP's SIP Trunk:

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

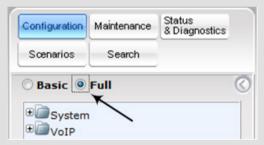
Configure the E-SBC using the Web-based management interface (embedded Web server).

Notes:

- The E-SBC must be installed with a Software Feature Key that includes the following items:
 - ✓ Microsoft
 - √ SBC
 - **√** Security
 - V DSP
 - **√** RTP
 - √ SIP

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

- The scope of this document does *not* cover security aspects of connecting a SIP Trunk to the Microsoft Lync environment. Security measures should be implemented in accordance with your organization's security policies. For basic security guidelines, see the *Recommended Security Guidelines Technical Note*.
- The E-SBC must be installed with SIP firmware version 6.6 or later.
- Before beginning to configure the E-SBC, select the **Full** option in the Web interface to display the full Navigation tree:



When the E-SBC is reset, the Web interface reverts to **Basic** display.

This document applies to Microsoft Lync 2013 and to Microsoft Lync 2010.

4.1 Step 1: Configuring the E-SBC's Network Interfaces

The subsections below show how to configure the E-SBC's network interfaces. Several methods can be used. The scenario exemplified in this document uses this method:

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

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

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

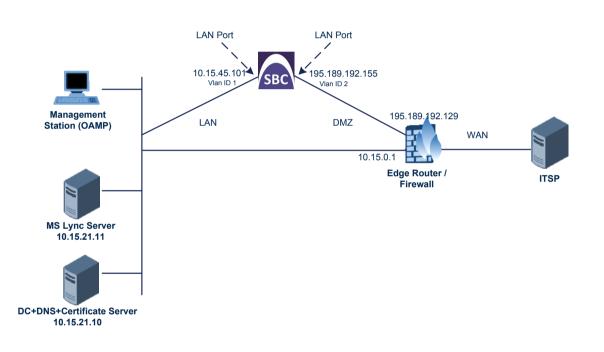


Figure 4-1: Network Interfaces

4.1.1 Configuring IP Network Interfaces for LAN and WAN

This subsection shows how to configure IP network interfaces for:

- LAN VoIP (Voice)
- WAN VoIP (WANSP)
- To configure the interfaces:
- Open the IP Interfaces Table page (Configuration tab > VoIP > Network Settings > IP Interfaces Table).



F	IP Interfaces Table										
	Note: Select row index to modify the relevant row.										
	1 Add index Done										
Ir	dex	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	0	OAMP + Media + Control	IPv4 Manual	10.15.21.15	16	10.15.0.1	1	O+M+C	0.0.0.0	0.0.0.0	GROUP_1
1	0	Media + Control	IPv4 Manual	10.15.2.1	16	10.15.2.22	1	XX1	0.0.0.0	0.0.0.0	GROUP_1
				-							
				IP Interfa	e Statu	s Table					

- 2. Modify the existing LAN network interface:
 - a. Select the 'Index' radio button adjacent to Application Type **OAMP + Media + Control** and click **Edit**.
 - **b.** Configure like this:

Parameter	Example Setting for IPv4	Example Setting for IPv6
Application Type	OAMP + Media + Control (application)	Media + Control . The OAMP application can be configured only with IPv4.
Interface Mode	See IPv4 in the E-SBC documentation.	See IPv6 in the E-SBC documentation.
IP Address	"10.15.45.101" (E-SBC IP address)	"2001::101" (only a global address can be entered)
Prefix Length	"16" for 255.255.0.0 (Subnet mask, in bits)	"64" (only 64 is supported)
Gateway	Default Gateway "10.15.0.1"	"2001::1"
VLAN ID	VLAN ID. "1".	"1"
Interface Name	Arbitrary descriptive name "Voice"	"IP6Voice"
Primary DNS Server IP Address	DNS IP address "10.15.21.10"	"2001::10"
Underlying Interface	GROUP_1 (Ethernet port group)	GROUP_1



- **3.** Add another network interface for the WAN side:
 - a. Enter 1 and click Add Index.
 - **b.** Configure like this:

Parameter	Example Setting for IPv4	Example Setting for IPv6
Application Type	Media + Control (application)	Media + Control
Interface Mode	See IPv4 in the E-SBC documentation.	See IPv6 in the E-SBC documentation.
IP Address	"195.189.192.155" (WAN IP address)	"2002::155"
Prefix Length	"16" for 255.255.0.0	"64" (only 64 is supported)
Gateway	"195.189.192.129" (Default Gateway - router's IP address)	"2002::129"
VLAN ID	"2" (WAN VLAN ID)	"2"
Interface Name	"WANSP" (arbitrary descriptive name of WAN interface)	"IP6WANSP"
Primary DNS Server IP Address	"80.179.52.100" (DNS IP address)	2001:4860:4860::8888
Secondary DNS Server IP Address	"80.179.55.100" (DNS IP address)	2001:4860:4860::8844
Underlying Interface	GROUP_2 (Ethernet port group)	GROUP_2

4. Click **Apply** and **Done**.

4.1.2 Configuring the Native VLAN ID

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

- > To configure the Native VLAN ID for the LAN and WAN interfaces:
- 1. Open the Physical Ports Settings page (Configuration tab> VoIP > Network > Physical Ports Table).
- 2. In the **GROUP_1** member ports, set the 'Native Vlan' field to 1; this VLAN is assigned to network interface Voice.
- 3. In the **GROUP_2** member ports, set the 'Native Vlan' field to 2; this VLAN is assigned to network interface WANSP.

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

Figure 4-3: Ports Native VLAN

4.2 Step 2: Enabling the SBC Application

This step shows how to enable the SBC application.

- To enable the SBC application:
- 1. Open the Applications Enabling page (Configuration tab > VolP > Applications Enabling > Applications Enabling).

Figure 4-4: Applications Enabling

~		
🗲 SAS Application	Disable 👻	
🗲 SBC Application	Enable 👻	
🗲 IP to IP Application	Disable 👻	

- 2. From the 'SBC Application' drop-down list, select **Enable**.
- **3.** Reset the E-SBC with a **burn to flash** for this setting to take effect (see Section 4.16 on page 73).

4.3 Step 3: Configuring SRDs

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

4.3.1 Configuring Media Realms

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

Simplest is to configure one Media Realm for internal (LAN) traffic and another for external (WAN) traffic as shown below, applied to the example scenario.

To configure Media Realms:

- 1. Open the Media Realm Table page (**Configuration** tab > **VolP** > **Media** > **Media Realm Table**).
- 2. Add a Media Realm for the LAN traffic:
 - a. Click Add.
 - Parameter **Example Setting** "1" Index "MRLan" (an arbitrary name) Media Realm Name IPv4 Interface Name Voice (the interface name) IPv6 Interface Name IP6Voice (the interface name). Note: Only applicable if using IPv6. "6000" (a number representing the lowest UDP port Port Range Start number to be used for media on the LAN) "10" (the number of media sessions assigned with the Number of Media Session Legs port range)
 - **b.** Configure like this:

Figure 4-5: Configuring a LAN Media Realm

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

c. Click Submit.

- **3.** Add a Media Realm for the external traffic (WAN):
 - a. Click Add.
 - **b.** Configure like this:

Parameter	Example Setting
Index	"2"
Media Realm Name	"MRWan" (an arbitrary name)
IPv4 Interface Name	WANSP (the interface name)
IPv6 Interface Name	IP6WANSP (the interface name) Note: Only applicable if using IPv6.
Port Range Start	"7000" (a number representing the lowest UDP port number to be used for media on the WAN)
Number of Media Session Legs	"10" (the number of media sessions assigned with the port range)

Figure 4-6: Configuring a WAN Media Realm

Add Record	×
Index	2
Media Realm Name	MRWan
IPv4 Interface Name	WANSP 👻
IPv6 Interface Name	None 👻
Port Range Start	7000
Number Of Media Session Legs	10
Port Range End	7090
Default Media Realm	No 👻
	Submit ★ Cancel

c. Click Submit.

The configured Media Realm table is shown below:

Figure 4-7: Required Media Realm Table

Media	a Realm Table		
Add 4	+)		
Index (Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
1	MRLan	Voice	None
2	MRWan	WANSP	None
•		III	
	ia ka Page 1	of 1 🕞 🕞 Show 10 👻 records p	er page View 1 - 2 of

4.3.2 Configuring SRDs

This subsection shows how to configure the SRDs.

- To configure the SRDs:
- Open the SRD Table page (Configuration tab > VolP > Control Network > SRD Table).
- 2. Add an SRD for the E-SBC's internal interface (toward Lync Server 2013):
 - **a.** Configure these parameters:

Parameter	Example Setting
SRD Index	1
SRD Name	"SRDLan" (descriptive name for the SRD)
Media Realm	"MRLan" (associates the SRD with a Media Realm)

Figure 4-8: Configuring the LAN SRD

SRD Index		1 - SRDLan	-	
▼ Common Parameters				
SRD Name		SRDLan		
Media Realm		MRLan		
▲ SBC Parameters				
IP Group Status Table		Sets Status Table		

b. Click Submit.

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

Parameter	Example Setting
SRD Index	2
SRD Name	"SRDWan" (descriptive name for the SRD)
Media Realm	"MRWan" (associates the SRD with a Media Realm)

Figure 4-9: Configuring the WAN SRD

SRD Index	2 - SRDWan
 Common Parameters 	
SRD Name	SRDWan
Media Realm	MRWan
▲ SBC Parameters	
▲ IP Group Status Table	 Proxy Sets Status Table

b. Click Submit.

4.3.3 Configuring SIP Signaling Interfaces

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

The procedure below shows how to add SIP interfaces. In the example scenario, an internal and external SIP interface must be added for the E-SBC.

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

Parameter	Example Setting
Index	"1"
Network Interface	"Voice" (for IPv4) / "IP6Voice" (for IPv6)
Application Type	SBC
TLS Port	"5067"
TCP and UDP	"0"
SRD	"1"

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

Parameter	Example Setting
Index	"2"
Network Interface	"WANSP" (for IPv4) / "IP6WANSP" (for IPv6)
Application Type	SBC
UDP Port	"5060"
TCP and TLS	"O"
SRD	"2"

c. Click Submit.

The configured SIP Interface table is shown below:

Figure 4-10: Required SIP Interface Table

SIP I	nterface Table						
Add 4	•]						
Index 4	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	Voice	SBC	0	0	5067	1	None
2	WANSP	SBC	5060	0	0	2	None
•				III			
			🗔 😽 Page 1 of 1 🕨	> ► Show 10 💽 records p	er page		View 1 - 2 of

4.4 Step 4: Configuring Proxy Sets

This step shows how to configure the Proxy Sets. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). In the example scenario, two Proxy Sets must be configured for:

- Microsoft Lync Server 2013
- SIP Trunk

These Proxy Sets will later be associated with IP Groups.

- > To add Proxy Sets:
- Open the Proxy Sets Table page (Configuration tab > VolP > Control Network > Proxy Sets Table).
- 2. Add a Proxy Set for Lync Server 2013:
 - **a.** Configure these parameters:

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

Ŧ

E

Proxy Se	et ID		1				-
		Proxy Address		Tra	nspor	t Type	
	1	FE15.ilync15.local:5067			TLS	•	
	2					•	
	3		_			•	
	4		_		[•	
			_			<u> </u>	
	5					•	
Enable F	roxy	Keep Alive	Using	g Options			•
Proxy Keep Alive Time		60					
Proxy Lo	ad Ba	alancing Method	Round Robin 🗸				
Is Proxy	Hot S	Swap	Yes				-
Proxy Re	edund	lancy Mode	Not C	onfigured	ł		•

1

IP only

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

b. Click Subr	nit.
---------------	------

✓SRD Index

Classification Input

3. Add a Proxy Set for the SIP Trunk:

a. Configure these parameters:

Parameter	Example Setting
Proxy Set ID	2
Proxy Address	"SIPTrunk.Company.com:5060" (SIP Trunk IP address or FQDN and destination port)
Transport Type	UDP
Enable Proxy Keep Alive	Using Options
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Homing
SRD Index	"2" (enables classification by Proxy Set for this SRD in the IP Group belonging to the SIP Trunk)

Proxy Set	ID		2		
		Proxy Address	Transport Type		
	1	SIPTrunk.Company.com:5060)	UDP 👻	
	2			•	
	3			· ·	
	4			•	
	5			•	
,					
Enable Pr	оху	Keep Alive	Using	g Options	
Proxy Kee	ep Al	ive Time	60		
Proxy Loa	id Ba	alancing Method	Disable		
Is Proxy H	lot S	Swap	Yes		
Proxy Rec	lund	ancy Mode	Not Configured		
	x		2		
SRD Inde	index ification Input				

Figure 4-12: Configuring a Proxy Set for the SIP Trunk

b. Click Submit.

4.5 Step 5: Configuring IP Groups

This step shows how to create IP Groups. An IP Group represents a SIP entity behavior in the E-SBC's network. In the example scenario, IP Groups are created for:

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

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

- To configure IP Groups:
- Open the IP Group Table page (Configuration tab > VoIP > Control Network > IP Group Table).
- 2. Add an IP Group for the Lync Server 2013 Mediation Server:
 - a. Click Add.
 - **b.** Configure the parameters like this:

Parameter	Example Setting
Index	"1"
Туре	Server
Description	"Lync Server" (a descriptive name)
Proxy Set ID	"1"
SRD	"1"
Media Realm Name	"MRLan"
IP Profile ID	"1"

c. Click Submit.

3. Add an IP Group for the SIP Trunk:

a. Click Add.

b. Configure the parameters like this:

Parameter	Example Setting
Index	"2"
Туре	Server
Description	"SIP Trunk" (a descriptive name)
Proxy Set ID	"2"
SRD	"2"
Media Realm Name	"MRWan"
IP Profile ID	"2"

c. Click Submit.



The figure below shows the configured IP Group table:

Figure 4-13: Configured IP Group Table

IP Gr	oup Table								
Index :	Туре	Description	Proxy Set ID	SIP Group Name	Contact User	Local Host Name	SRD	Media Realm Name	IP Profile ID
	Server	Lync	1				1	LanMR	1
	Server	SIP Trunk	2				2	WanMR	2

4.6 Step 6: Configuring IP Profiles

This step shows how to configure IP Profiles. In the example scenario, the IP Profiles are used to configure the SRTP / TLS modes and other parameters that differ between the two entities - Lync Server 2013 and SIP Trunk.

Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.5 on page 47).

In the example, an IP Profile is added for each entity:

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

> To add IP Profiles:

- Open the IP Profile Settings page (Configuration tab > VoIP > Coders and Profiles > IP Profile Settings).
- 2. Add an IP Profile for Lync Server 2013:
 - a. Configure the parameters like this:

Parameter	Example Setting
Profile ID	1
Media IP Version Preference	Only IPv4 / Only IPv6
Reset SRTP State Upon Re-key	Enable
Extension Coders Group ID	Coders Group 1
Media Security Behavior	SRTP
SBC Remote Early Media RTP	Delayed (mandatory because the Lync Server 2013 does not immediately send RTP to the remote side if it sends a SIP 18x response)
RFC 2833 Behavior	Extend (in case the SIP Trunk does not send RFC 2833 in SDP)
SBC Remote Update Support	Supported Only After Connect
SBC Remote Re-Invite Support	Supported Only With SDP
SBC Remote Refer Behavior	Handle Locally (mandatory because Lync Server 2013 does not support receive Refer)
SBC Remote 3xx Behavior	Handle Locally (mandatory because Lync Server 2013 does not support receive 3xx)
SBC Remote Hold Format	Inactive



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

Profile ID	1	•	
Profile Name	Lync		
Media IP Version Preference	Only IPv4	•	
Reset SRTP State Upon Re-key	Enable 👻		
SBC			
Franscoding Mode	Only if Required	•	
Extension Coders Group ID	Coders Group 1	•	2
Allowed Coders Group ID	None	•	
Allowed Coders Mode	Restriction	•	
SBC Preferences Mode	Doesn't Include Extensions	•	
Diversion Mode	Don't Care	•	
listory Info Mode	Don't Care	•	2
Media Security Behavior	SRTP	•	
RFC 2833 Behavior	Extend	•	
Alternative DTMF Method	Don't Care	•	
P-Asserted-Identity	Don't Care	•	
SBC Fax Coders Group ID	None	•	
SBC Fax Behavior	0		
SBC Fax Offer Mode	0		
BC Fax Answer Mode	1		
SBC Session Expires Mode	Transparent	•	
SBC Remote Early Media RTP	Delayed	•	
BC Remote Can Play Ringback	Yes	•	
BC Remote Supports RFC 3960	Not Supported	•	
BC Multiple 18x Support	supported	•	
BC Early Media Response Type	Transparent	•	
BC Remote Update Support	Supported Only After Connect	•	2
BC Remote Re-Invite Support	Supported only with SDP	•	2
BC Remote Refer Behavior	Handle Locally	•	2
BC Remote Early Media Support	supported	•	
BC Remote 3xx Behavior	Handle Locally	•	2
BC Remote Delayed Offer Support	Not Supported	•	
SBC PRACK Mode	Transparent	•	
BC Enforce MKI Size	do-not-enforce	•	
BC User Registration Time	-1		

b. Click Submit.

- 3. Add an IP Profile for the SIP Trunk:
 - a. Configure the parameters like this:

Parameter	Example Setting
Profile ID	2
Media IP Version Preference	Only IPv4 / Only IPv6
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 2
Allowed Coders Mode	Preference (enables the received SDP offer to list Allowed coders first and then the original coders received in the SDP).
Media Security Behavior	RTP
SBC Remote Refer Behavior	Handle Locally (the E-SBC handles the incoming REFER request itself, without forwarding the REFER towards the SIP Trunk)



Note: The SIP Trunk's IP Profile depends on the SIP Trunk behavior. Refer to the explanations of the IP Profile parameters in the *E-SBC User's Manual* in order to configure the profile according to SIP Trunk behavior.



Profile ID	2	-	
Profile Name	SIP Trunk		Z
ledia IP Version Preference	Only IPv4	•	
BC			
ranscoding Mode	Only if Required	•	
xtension Coders Group ID	Coders Group 2	•	2
llowed Coders Group ID	Coders Group 2	•	2
llowed Coders Mode	Preference	•	2
BC Preferences Mode	Include Extensions	•	2
iversion Mode	Don't Care	•	
listory Info Mode	Don't Care	•	2
1edia Security Behavior	RTP	-	
FC 2833 Behavior	As Is	•	
lternative DTMF Method	Don't Care	•	
-Asserted-Identity	Don't Care	•	
BC Fax Coders Group ID	None	•	
BC Fax Behavior	0		
BC Fax Offer Mode	0		
BC Fax Answer Mode	1		
BC Session Expires Mode	Transparent	•	
BC Remote Early Media RTP	Immediate	•	
BC Remote Can Play Ringback	Yes	•	
BC Remote Supports RFC 3960	Not Supported	•	
BC Multiple 18x Support	supported	•	
BC Early Media Response Type	Transparent	•	
BC Remote Update Support	Supported	-	
BC Remote Re-Invite Support	Supported	-	
BC Remote Refer Behavior	Handle Locally	-	2
BC Remote Early Media Support	supported	-	
BC Remote 3xx Behavior	Transparent	-	
BC Remote Delayed Offer Support	Supported	•	
BC PRACK Mode	Transparent	•	

Figure 4-15: Configured IP Profile for SIP Trunk

b. Click Submit.

4.7 Step 7: Configuring Coders

This step shows how to configure coders (termed *Coder Groups*). You can configure up to four different Coder Groups. As Lync Server 2013 supports the G.711 coder while the network connection to SIP Trunk may restrict you to operate with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.711 coders for Lync Server 2013, and Coder Group with the G.729 coder for the SIP Trunk.

Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 49).

To configure coders:

- 1. Add a Coder Group for Lync Server 2013.
 - a. Configure the parameters like this:

Parameter	Example Setting
Coder Group ID	1
Coder Name	G.711 U-law
Coder Name	G.711 A-law
Silence Suppression	Enable

Figure 4-16: Configured Coder Group for Lync Server 2013

-								
Coder Group ID				1 👻				
Coder Name	2	Packetiza	ition Time	Rate	2	Payload Type	Silence Supp	ression
Coder Name G.711U-law	⊇ ▼	Packetiza 20	ation Time	Rate	•	Payload Type	Silence Supp Enable	ression +

b. Click Submit.

- 2. Add a Coder Group for SIP Trunk:
 - a. Configure the parameters like this:

Parameter	Example Setting
Coder Group ID	2
Coder Name	G.729

Figure 4-17: Configured Coder Group for the SIP Trunk

Coder Group ID			2 💌		
Coder N	Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.729	•	20 💌	8	18	Disabled 💌

b. Click Submit.

The step below adds an Allowed Coders Group to ensure that voice sent to the SIP Trunk uses the G.729 coder whenever possible.

Note that this Allowed Coders Group ID (and its preference) was assigned to the IP Profile belonging to the SIP Trunk in the previous step (see Section 4.6 on page 49).

- > To set a preferred coder for the SIP Trunk:
- 1. Open the Allowed Coders Group page (Configuration tab > VoIP > SBC > Allowed Coders Group).
- 2. From the 'Allowed Coders Group ID' drop-down list, select 2.
- 3. From the 'Coder Name' drop-down list, select **G.729**.

Figure 4-18: Allowed Coders Group for SIP Trunk

Allowed Coders Group ID	2 💌	
	Coder Name	
	G.729 💌	

4. Click Submit.

4.8 Step 8: Configuring a SIP TLS Connection

This step shows how to configure the E-SBC to use a TLS connection with the Lync Server 2013 Mediation Server. This step is mandatory for a secure SIP TLS connection.

4.8.1 Configuring the NTP Server Address

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

- > To configure the NTP server address:
- 1. Open the Application Settings page (Configuration tab > System > Application Settings).
- 2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., 10.15.21.10).

Figure 4-19: Configuring the NTP Server IP Address

▼ NTP Settings	
NTP Server IP Address	10.15.21.10
NTP UTC Offset Ho	urs: 2 Minutes: 0
NTP Updated Interval Ho	urs: 24 Minutes: 0
NTP Secondary Server IP	

3. Click Submit.

4.8.2 Configuring a Certificate

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

- To configure a certificate:
- 1. Open the Certificates page (Configuration tab > System > Certificates).

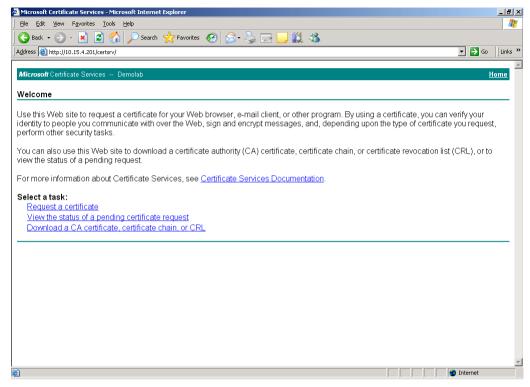
Figure 4-20: Certificates Page - Creating CSR

▼ Certificate Signing Request					
Subject Name [CN]	ITSP-GW.ilync15.local				
Organizational Unit [OU] (optional)					
Company name [O] (optional)					
Locality or city name [L] (optional)					
State [ST] (optional)					
Country code [C] (optional)					
Create CSR After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.					

- 2. In the 'Subject Name' field, enter the media gateway name (e.g., ITSP-GW.ilync15.local). This name must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 15).
- 3. Click **Create CSR**; a certificate request is generated.
- 4. Copy the CSR (from the line ----BEGIN CERTIFICATE to the line END CERTIFICATE REQUEST----) to a text file (such as Notepad) and save it to a folder on your computer with the file name *certreq.txt*.

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





6. Click Request a certificate.

Figure 4-22: Request a Certificate Page

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	×
Eile Edit View Favorites Iools Help	n
🕒 Back 🔹 🕤 🔹 😰 🏠 🔎 Search 🤺 Favorites 🤣 🎅 - چ 🔟 - 🛄 🏭 🦓	
Address 🕘 http://10.15.4.201/certsrv/certrqus.asp	🔽 🛃 Go 🛛 Links 🎽
	A
Microsoft Certificate Services Demolab	<u>Home</u>
Request a Certificate	
Select the certificate type:	
Web Browser Certificate	
E-Mail Protection Certificate	
Or, submit an advanced certificate request.	
	*
	Internet



7. Click advanced certificate request and click Next.

Figure 4-23: Advanced Certificate Request Page

🗿 Microsoft Certificate Services - Microsoft Internet Explorer			_ 8 ×
Elle Edit Yiew Favorites Iools Help			al an
🕒 😋 Back 🔹 🕥 🖌 📓 🏠 🔎 Search 👷 Favorites 🛛 🔗 😓 🦉 🔹 🛄 🔹 🛄 🆓			
Address 💩 http://10.15.4.201/certsrv/certrqad.asp		🛨 🔁 Go	Links ×
			4
Microsoft Certificate Services Demolab		Ë	ome
Advanced Certificate Request			
The policy of the CA determines the types of certificates you can request. Click one of the following options to:			
Create and submit a request to this CA.			
		. 64 open	dod
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by us PKCS #7 file.	sing a pase	<u>-64-erico</u>	<u>bed</u>
Č Done		Internet	

8. Click Submit a certificate request... and click Next.

Figure 4-24: Submit a Certificate Request or Renewal Request Page

🏉 Microsoft Active	Directory Certificate Services - Windows Internet Explorer	J 🔀
😋 🔾 🗢 🙋 htt	ttp://10.15.4.201/certsrv/certroxt.asp 🔹 🛛	→ ×
File Edit View	Favorites Tools Help	
🚖 🔏 Microsoft	Active Directory Certificate Services	
	Directory Certificate Services Lync-DC-LYNC-CA Hon	<u>e</u>
Submit a Certi	ificate Request or Renewal Request	-
	ved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request in external source (such as a Web server) in the Saved Request box.	
Saved Request:		
	A8jxeP85ymyfDbnfx+zEusB828h4JgzbeNkuyfKel rr4ootrmsPOCAuEAAaANAQGC3qGS1b3DQEBBAUA MnRHAkz6Xg4G3abaCkmuch2802amgEGC0APTBok 9f3m6c4Bj8ib+R5+YI+Ost57xT9D2XNg5Yp4G+OB wr0quXcOUX6B9VBT71ac08HcA END CERTIFICATE REQUEST	
Certificate Temp	late:	
	Web Server -	
Additional Attribu	utes:	
Attributes:	<	
	Submit >	
		_
Dana	😡 Internet Protected Mode: Off 🛛 🖓 💌 💐 100%	-
Done	😜 Internet Protected Mode: Off 🛛 🖓 💌 🔍 100%	•

- 9. Open the *certreq.txt* file that you created and saved in Step 4 and copy its contents to the 'Base-64-Encoded Certificate Request' field.
- **10.** From the 'Certificate Template' drop-down list, select **Web Server**.

11. Click Submit.

Figure 4-25: Certificate Issued Page



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

Figure 4-26: Download a CA Certificate, Certificate Chain, or CRL

🖉 Microsoft Certificate Services - Microsoft Internet Explorer	_ 8 ×
Eile Edit Yiew Favorites Iools Help	A.
🕒 Back 🔹 🕥 🖌 📓 🏠 🔎 Search 🤺 Favorites 🚱 🔗 - چ 🔟 🔹 🛄 🖓	
Address a http://10.15.4.201/certsrv/certcarc.asp	🔹 🔁 Go 🔤 Links 🎇
	*
Microsoft Certificate Services Demolab	<u>Home</u>
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Current (Demolab)	
Encoding method:	
© DER	
C Base 64	
Download CA certificate Download CA certificate chain	
Download Latest base CRL	
	•
a Done	Internet

- **16.** Under the 'Encoding method' group, select the **Base 64** option for encoding.
- **17.** Click **Download CA certificate**.



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

Figure 4-27: Certificates Page (Uploading Certificate)

•	 Upload certificate files from your computer 		
	Private key pass-phrase (optional)	audc	
	Send Private Key file from your computer to the device. The file must be in either PEM or PFX (PKCS#12) format. Choose File No file chosen Send File Note: Replacing the private key is not recommended but if it's done, it should be Send Device Certificate file from your computer to the device.	over a physically-secure network link.	
	The file must be in textual PEM format. Choose File No file chosen Send File		
	Send "Trusted Root Certificate Store" file from your computer to the device. The file must be in textual PEM format. Choose File No file chosen Send File		

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 73).

4.9 Step 9: Configuring SRTP

This step shows how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), configure the E-SBC to do so as well.

Note that SRTP was enabled for Lync Server 2013 when you added an IP Profile for Lync Server 2013 (see Section 4.6 on page 49).

> To configure media security:

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

Figure 4-28: Media Security Page

-	General Media Security Settings	
4	Media Security	Enable
9	Aria Protocol Support	Disable
	Media Security Behavior	Mandatory 💌
9	SRTP Tunneling Authentication for RTP	Disable
9	SRTP Tunneling Authentication for RTCP	Disable
-	SRTP Setting	
	Master Key Identifier (MKI) Size	1
	Symmetric MKI Negotiation	Enable

SRTP offered Suites

2. Configure the parameters like this:

Parameter	Example Setting
Media Security	Enable
Master Key Identifier (MKI) Size	"1"
Symmetric MKI Negotiation	Enable

3. Click Submit.

 Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 73).

4.10 Step 10: Configuring IP Media

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



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

To configure IP media:

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

4	Number of Media Channels	30
4	Voice Streaming	Disable
	NetAnn Announcement ID	annc
	MSCML ID	ivr
	Transcoding ID	trans
	Conference	
	Conference ID	conf
	Beep on Conference	Enable
	Enable Conference DTMF Clamping	Enable
	Enable Conference DTMF Reporting	Disable

Figure 4-29: IP Media Settings

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

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

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

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

In the example scenario, the following IP-to-IP routing rules must be added in order to route calls between Lync Server 2013 (LAN) and SIP Trunk (WAN):

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

The routing rules use IP Groups to denote the source and destination of the call.

As configured in Step 5 (see Section 4.5 on page 47), IP Group ID 1 was assigned to Lync Server 2013, and IP Group ID 2 to SIP Trunk.

- To add IP-to-IP routing rules:
- 1. Open the IP-to-IP Routing Table page (Configuration tab > VoIP > SBC > Routing SBC > IP-to-IP Routing Table).
- 2. Add a rule to terminate SIP OPTIONS messages received from the LAN:
 - a. Click Add.
 - **b.** Configure the parameters like this:

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



Figure 4-30: Configured IP-to-IP Routing Rule to Terminate SIP OPTIONS Messages Received from the LAN

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

c. Click Submit.

- 3. Add a rule to route calls from LAN to WAN:
 - a. Click Add.
 - b. Configure the parameters like this:

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

Add Record	×
Index	1
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None 👻
ReRoute IP Group ID	0
Call Trigger	Any 👻
Destination Type	IP Group 👻
Destination IP Group ID	2
Destination SRD ID	2 🔹
Destination Address	
Destination Port	0
Destination Transport Type	· · · · · · · · · · · · · · · · · · ·
Alternative Route Options	Route Row 👻
Cost Group	None 👻
	🗟 Submit 🛛 🗙 Cancel

Figure 4-31: IP-to-IP Routing Rule for LAN to WAN

- c. Click Submit.
- 4. Add a rule to route calls from WAN to LAN:
 - a. Click Add.
 - **b.** Configure the parameters like this:

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

Figure 4-32: Configured IP-to-IP Routing Rule to Route Calls from WAN to LAN

Index	2
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None 👻
ReRoute IP Group ID	0
Call Trigger	Any 🗸
Destination Type	IP Group 👻
Destination IP Group ID	1
Destination SRD ID	1
Destination Address	
Destination Port	0
Destination Transport Type	·
Alternative Route Options	Route Row 👻
Cost Group	None 👻

c. Click Submit.

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

Figure 4-33: IP-to-IP Routing Table

IP-t	IP-to-IP Routing Table									
Add	Add + Insert +									
Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	ReRoute IP Group ID	Call Trigger	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Port
0	1	*	*	OPTIONS	-1	Апу	Dest Address	-1	None	0
1	1	*	*	All	-1	Any	IP Group	2	2	0
2	2	*	*	All	-1	Any	IP Group	1	1	0
				14 of Page 1	of 1 💀 💀 Sho	ow 10 👻 records p	ber page			View 1 - 3 of 3



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

4.12 Step 12: Configuring IP-to-IP Outbound Manipulation

This step shows how to configure IP-to-IP manipulation rules. They concern number manipulation of the source and / or destination number. They use IP Groups to denote the source and destination of the call. As configured in Step 5 (see Section 4.5 on page 47), IP Group ID 1 was assigned to Lync Server 2013 and IP Group ID 2 to the SIP Trunk.



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

The step below exemplifies configuring a manipulation rule which adds a plus sign + to the destination number for calls from IP Group 2 (SIP Trunk) destined to IP Group 1 (i.e., Lync Server 2013), when the destination number prefix is any number (*).

> To add a number manipulation rule:

- Open the IP to IP Outbound Manipulation page (Configuration tab > VoIP > SBC > Manipulations SBC > IP-to-IP Outbound).
- 2. Click Add.
- 3. Click the **Rule** tab and configure the parameters like this:

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

Figure 4-34: IP-to-IP Outbound Manipulation Rule – Rule Tab

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



4. Click the **Action** tab and configure the parameters like this:

Parameter	Example Setting
Prefix to Add	"+"

Figure 4-35: Configured IP-to-IP Outbound Manipulation Rule - Action Tab

Rule Action	
Index	1
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	
Privacy Restriction Mode	Transparent
	Submit × Cancel

5. Click Submit.

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

Figure 4-36: IP-to-IP Outbound Manipulation

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

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

4.13 Step 13: Configuring SIP Message Manipulation Rules

This step shows how to configure SIP message manipulation rules (configured in the Message Manipulations table).

SIP message manipulation rules can include insertion, removal and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message. After configuring the SIP message manipulation rules, assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

See an example below of a message manipulation rule configuration; use the *E-SBC User's Manual* for detailed instructions on how to configure message manipulation rules according to your requirements.

In the example scenario, the configured manipulation rule manipulates the P-Asserted-Identity user part of the header, and replaces it with the user part that appears on the Referred-By header.

To configure SIP message manipulation rules:

 Open the Message Manipulations page (Configuration tab > VoIP > SIP Definitions > Msg Policy & Manipulation > Message Manipulations).

Figure 4-37: Message Manipulations Page

Mes	Message Manipulations							
Add	Add + Insert +							
Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role	
0	0	any	header.referred-by exists	sheader.p-asserted-identit	Modify	'<'+header.referred-by.U	Use Current Condition	
	i∈ ∞ Page + of 1 ∞ ⊨ Show 10 → records per page View 1 - 1 of 1							

2. Add the following manipulation rules for Manipulation Set ID 0:

Parameter	Example Setting
Index	"O"
Manipulation Set ID	"O"
Message Type	any Note: Enter the value as is.
Condition	header.referred-by exists Note: Enter the value as is.
Action Subject	header.p-asserted-identity Note: Enter the value as is.
Action Type	Modify
Action Value	<pre>'<'+header.referred-by.URL+'>' Note: Enter the value as is.</pre>

Edit Record	×
Index	0
Manipulation Set ID	0
Message Type	any
Condition	header.referred-by exists
Action Subject	header.p-asserted-identity
Action Type	Modify 👻
Action Value	'<'+header.referred-by.URL+'>'
Row Role	Use Current Condition 👻
	🗟 Submit 🛛 🗙 Cancel

Figure 4-38: Configured SIP Message Manipulation Rule

- Click Submit.
- 3. Assign the Manipulation Set ID 0 to IP Group 2:
 - a. Open the IP Group Table page (Configuration tab > VoIP > Control Network > IP Group Table).
 - **b.** Select the row of IP Group 2 and click **Edit**.
 - c. Click the SBC tab.
 - d. Set the 'Outbound Message Manipulation Set' field to 0.

Figure 4-39: Assigning a Manipulation Rule to IP Group 2

Common Gateway SBC				
Index	2			
Classify By Proxy Set	Enable			
Max Number Of Registered Users	-1			
Source URI Input	Not Configured			
Destination URI Input	Not Configured			
Inbound Message Manipulation Set	-1			
Outbound Message Manipulation Set	0			
Registration Mode	User initiates registrations			
Authentication Mode	User Authenticates			
Authentication Method List				
Enable SBC Client Forking	No			
	Submit × Cancel			

e. Click Submit.

4.14 Step 14: Configuring a Registration Account

This step shows how to configure SIP registration accounts (in the Account Table page) so that the E-SBC can register with the SIP Trunk on behalf of Lync Server 2013.



Note: Not *all* SIP Trunks require registration (and authentication) to provide service. If your SIP Trunk doesn't require registration, skip this step.

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

- > To configure a registration account:
- 1. Open the Account Table page (Configuration tab > VolP > SIP Definitions > Account Table).

Figure 4-40: Configuring a SIP Registration Account

Accou	nt Table								
Note:	Note: Select row index to modify the relevant row.								
	Add		Compact						
Index	Served Trunk Group	Served IP Group	Serving IP Group	User Name	Password	Host Name	Register	Contact User	Application Type
1 0	-1	1	2	UserName	÷		Yes		SBC

- 2. Enter an index number (1) and click Add.
- **3.** Configure the account according to the information provided by the SIP Trunk provider, for example:

Parameter	Example Setting
Served IP Group	"1" (i.e., Lync Server 2013)
Serving IP Group	"2" (i.e., SIP Trunk)
Username	(Provided by the SIP Trunk provider)
Password	(Provided by the SIP Trunk provider)
Register	Yes
Application Type	SBC

4. Click Apply.

4.15 Step 15: Configuring Miscellaneous E-SBC Functionalities

This step shows how to configure the E-SBC's handling of SIP 18x responses received due to call forking of an INVITE.

In the example scenario, if an 18x with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC reopens the stream according to subsequently received 18x responses with SDP, or plays a ringback tone if a 180 response without SDP is received. It's mandatory to set this field for the Lync Server 2013 environment.

> To configure call forking:

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

General	General Settings				
	•				
	Transcoding Mode	Only If Required 👻			
	SBC No Answer Timeout	600]		
	SBC GRUU Mode	AsProxy -			
	Minimum Session-Expires [sec]	90]		
	BroadWorks Survivability Feature	Disable -	.]		
	Bye Authentication	Disable	•]		
	SBC User Registration Time	0]		
	SBC Proxy Registration Time	0]		
	SBC Survivability Registration Time	0]		
	SBC Forking Handling Mode	Sequential -	· 🖉		
	Unclassified Calls	Reject			
	SBC Session-Expires [sec]	180]		
	SBC Direct Media	Disable -			
	SBC Preferences Mode	Include Extensions			
	Max Forwards Limit	10]		

Figure 4-41: Configuring Forking Mode

- **3.** From the 'SBC Preferences Mode' drop-down list, select **Include Extensions** to ensure that Extension coders and Allowed coders are arranged according to their order of appearance in the Allowed Coders Group table.
- 4. Click Submit.

4.16 Step 16: Resetting the E-SBC

After completing the configuration of the E-SBC as described in the preceding steps, save (burn) the configuration to the E-SBC's flash memory with a reset; the settings will now take effect.

- > To save the configuration to flash memory with a reset:
- 1. Open the Maintenance Actions page (Maintenance tab > Maintenance > Maintenance Actions).

Configuration Maintenance Status 8 Diagnostics Search	Maintenance Actions			
				-
Basic O Full	Reset Board	Reset		
Maintenance	Burn To FLASH	Yes	-	
Contract Actions	Graceful Option	No	•	
	V LOCK / UNLOCK			
	Lock	LOCK		
	Graceful Option	No	•	
	Gateway Operational State	UNLOCKED		
	✓ Save Configuration			
	Burn To FLASH	BURN		

Figure 4-42: Resetting the E-SBC

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



Reader's Notes

A Configuring E-SBC to Send 414 Request-URI Too Long Response

This step shows how to configure the E-SBC to send a 414 Request-URI Too Long response when it encounters a Request URI it cannot handle due to excessive length.

When the E-SBC receives an INVITE with a long Request URI (a condition rule), it will route it to an unknown destination IP address (i.e., 1.1.1.1) and it will set a variable for this call to **1**. After a timeout, the E-SBC will generate an internal 408 Request Timeout response. Using message manipulation, the E-SBC will convert this response to a 414 Request-URI Too Long response (only if the variable value is **1**).

- > To configure a condition for this route:
- Open the Condition Table page (Configuration tab > VolP > SBC > Routing SBC > Condition Table).
- 2. Click the Add tab and configure the parameters like this:

Parameter	Example Setting
Index	"0"
Condition	header.request-uri.url.host.name len>'100' Note: You can choose the length of the Request-URI to process.

Figure A-1: Configuring a Condition for the Route

Add Record	х
Index	0
Condition	uri.url.host.name len>'100'
Description	
	🗃 Submit 🗙 Cancel

- 3. Click Submit.
- > To configure the route:
- Open the IP-to-IP Routing Table page (Configuration tab > VoIP > SBC > Routing SBC > IP-to-IP Routing Table).
- 2. Add a rule to route long-URI calls to unknown IP address:

a. Click Add.

b. Configure the parameters like this:

Parameter	Example Setting
Index	"0" (this rule should be the first rule in the table)
Message Condition	"0" (this number is the index of the condition configured above)
Destination Type	Dest address
Destination Address	"1.1.1.1" (unreachable IP address)

Add Record	×
Index	0
Source IP Group ID	-1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	0 •
ReRoute IP Group ID	-1
Call Trigger	Any 👻
Destination Type	Dest Address 👻
Destination IP Group ID	-1
Destination SRD ID	None -
Destination Address	1.1.1.1
Destination Port	0
Destination Transport Type	· · · · · · · · · · · · · · · · · · ·
Alternative Route Options	Route Row 👻
Cost Group	None -
	■ Submit × Cancel

Figure A-2: IP-to-IP Routing Rule for Long-URI Calls

> To configure a message manipulation rule:

- Open the Message Manipulations page (Configuration tab > VolP > SIP Definitions > Msg Policy & Manipulation > Message Manipulations).
- 2. Add a rule to set a variable to **1** in the case of a long-URI call:
 - a. Click Add.
 - **b.** Configure the parameters like this:

Parameter	Example Setting
Index	"0"
Manipulation Set ID	"1"
Message Type	invite.request
Condition	header.request-uri.url.host.name len>'100'
Action Subject	var.call.src.0
Action Type	Modify
Action Value	'1'

Figure A-3: Manipulation Rule to Set a Variable to '1' in Case of Long-URI Call

Edit Record	×
Index	0
Manipulation Set ID	1
Message Type	invite.request
Condition	uest-uri.url.host.name len>'100'
Action Subject	var.call.src.0
Action Type	Modify 👻
Action Value	۲ ^μ
Row Role	Use Current Condition 👻
	Submit X Cancel

- c. Click Submit.
- 3. Add a rule to convert 408 to '414':
 - a. Click Add.
 - **b.** Configure the parameters like this:

Parameter	Example Setting
Index	"1"
Manipulation Set ID	"2"
Message Type	invite.response.408
Condition	var.call.src.0 == '1'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'414'

Figure A-4: Manipulation Rule to Convert 408 to '414'

Edit Record	×
Index	1
Manipulation Set ID	2
Message Type	invite.response.408
Condition	var.call.src.0 == '1'
Action Subject	Header.request-uri.methodtype
Action Type	Modify 👻
Action Value	'414'
Row Role	Use Current Condition 👻
	B Submit × Cancel

c. Click Submit.



Figure A-5: Message Manipulations Page

Message Manipulations								
Add + Insert +								
Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role	
0	1	invite.request	header.request-ur	var.call.src.0	Modify	'1'	Use Current Cond	
1	2	invite.response.40	var.call.src.0 == '1	Header.request-ur	Modify	'414'	Use Current Cond	

4. Assign the Manipulation Set to IP Group 1 :

- a. Open the IP Group Table page (Configuration tab > VoIP > Control Network > IP Group Table).
- **b.** Select the row of IP Group 1 and click **Edit**.
- c. Click the SBC tab.
- d. Set the 'Inbound Message Manipulation Set' field to 1.
- e. Set the 'Outbound Message Manipulation Set' field to 2.

Figure A-6: Assigning Manipulation Rule to IP Group 1

Common Gateway SBC				
Index	1			
Classify By Proxy Set	Enable -			
Max Number Of Registered Users	-1			
Source URI Input	Not Configured 👻			
Destination URI Input	Not Configured 👻			
Inbound Message Manipulation Set	1			
Outbound Message Manipulation Set	2			
Registration Mode	User initiates registrations 🔹			
Authentication Mode	User Authenticates -			
Authentication Method List				
Enable SBC Client Forking	No			
	Submit × Cancel			

f. Click Submit.

Reader's Notes



Configuration Note

www.audiocodes.com