AudioCodes Professional Services – Interoperability Lab

# Microsoft<sup>®</sup> Skype for Business Server 2015 and Virgin Media SIP Trunk using AudioCodes Mediant<sup>™</sup> E-SBC

Version 7.2





Gold Communications



## Table of Contents

1	Introduction7				
	1.1	Intended Audience			
	1.2	About AudioCodes E-SBC Product Series	7		
2	Com	ponent Information			
	2.1	AudioCodes E-SBC Version			
	2.2	Virgin Media SIP Trunking Version	9		
	2.3	Microsoft Skype for Business Server 2015 Version	9		
	2.4	Interoperability Test Topology			
		2.4.1 Environment Setup			
		2.4.2 Known Limitations			
3	Con	figuring Skype for Business Server 2015			
	3.1	Configuring the E-SBC as an IP / PSTN Gateway			
	3.2	Configuring the "Route" on Skype for Business Server 2015			
4		figuring AudioCodes E-SBC			
÷.,	4.1	Step 1: IP Network Interfaces Configuration			
	7.1	4.1.1 Step 1a: Configure VLANs			
		4.1.2 Step 1b: Configure Network Interfaces	.33		
	4.2	Step 2: Configure Media Realms			
	4.3	Step 3: Configure SIP Signaling Interfaces	.38		
	4.4	Step 4: Configure Proxy Sets			
	4.5	Step 5: Configure IP Profiles			
	4.6	Step 6: Configure IP Groups			
	4.7	Step 7: Configure Coders			
	4.8	Step 8: SIP TLS Connection Configuration			
		4.8.1 Step 8a: Configure the NTP Server Address			
		4.8.2 Step 8b: Configure the TLS version			
		4.8.3 Step 8c: Configure a Certificate	.55		
	4.9	Step 9: Configure SRTP	.61		
	4.10	Step 10: Configure Maximum IP Media Channels			
	4.11	Step 11: Configure IP-to-IP Call Routing Rules	.63		
	4.12	Step 12: Configure IP-to-IP Manipulation Rules	.72		
	4.13	Step 13: Configure Message Manipulation Rules	.74		
	4.14	Step 14: Configure Registration Accounts	.82		
	4.15	Step 15: Miscellaneous Configuration	.84		
		4.15.1 Step 15a: Configure Call Forking Mode	.84		
		4.15.2 Step 15b: Configure SBC Alternative Routing Reasons			
		4.15.3 Step 15c: Configure SBC Max Retransmission Time			
		4.15.4 Step 15d: Configure Broken Connection Behavior			
		4.15.5 Step 15e: Configuration Needed for Manipulating SIP OPTIONS			
		Step 16: Reset the E-SBC			
Α		ioCodes INI File			
В		figuring Analog Devices (ATAs) for Fax Support1			
	B.1	Step 1: Configure the Endpoint Phone Number Table1			
	<b>B</b> .2	Step 2: Configure Tel to IP Routing Table1			
	B.3	Step 3: Configure Coders Table1			
	B.4	Step 4: Configure SIP UDP Transport Type and Fax Signaling Method1	03		

This document is intentionally left blank.

## Notice

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 can be downloaded from <a href="https://www.audiocodes.com/library/technical-documents">https://www.audiocodes.com/library/technical-documents</a>.

This document is subject to change without notice.

Date Published: April-24-2018

## 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 <a href="https://www.audiocodes.com/services-support/maintenance-and-support">https://www.audiocodes.com/services-support/maintenance-and-support</a>.

## **Document Revision Record**

LTRT	Description
39339	Initial document release for Version 7.2.
39343	Re-Certification with new firmware release 7.2.200

## **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 <a href="https://online.audiocodes.com/documentation-feedback">https://online.audiocodes.com/documentation-feedback</a>.

## **Abbreviations and Terminology**

Each abbreviation, unless widely used, is spelled out in full when first used.



This page is intentionally left blank.

# **1** Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between Virgin Media's SIP Trunk and Microsoft's Skype for Business Server 2015 environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the E-SBC based on this interoperability setup. However, it is recommended to read through this document in order to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including download option, visit AudioCodes Web site at https://www.audiocodes.com/partners/sbc-interoperability-list.

## 1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Virgin Media Partners who are responsible for installing and configuring Virgin Media's SIP Trunk and Microsoft's Skype for Business Server 2015 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	<ul> <li>Mediant 500 E-SBC</li> <li>Mediant 500L Gateway &amp; E-SBC</li> <li>Mediant 800B Gateway &amp; E-SBC</li> <li>Mediant 1000B Gateway &amp; E-SBC</li> <li>Mediant 2600 E-SBC</li> <li>Mediant 4000 SBC</li> <li>Mediant 4000B SBC</li> <li>Mediant 9000 SBC</li> <li>Mediant Software SBC (SE and VE)</li> </ul>	
Software Version	7.20A.200.055	
Protocol	<ul><li>SIP/UDP (to Virgin Media SIP Trunk)</li><li>SIP/TCP or TLS (to the S4B FE Server)</li></ul>	
Additional Notes	None	

## 2.2 Virgin Media SIP Trunking Version

### Table 2-2: Virgin Media Version

Vendor/Service Provider	Virgin Media
SSW Model/Service	GENBAND
Software Version	C20
Protocol	SIP
Additional Notes	None

## 2.3 Microsoft Skype for Business Server 2015 Version

### Table 2-3: Microsoft Skype for Business Server 2015 Version

Vendor	Microsoft
Model	Skype for Business
Software Version	Release 2015 6.0.9319.259
Protocol	SIP
Additional Notes	None

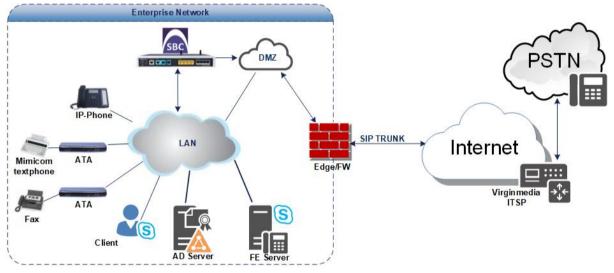
## 2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Virgin Media SIP Trunk with Skype for Business 2015 was done using the following topology setup:

- Enterprise deployed with Microsoft Skype for Business Server 2015 in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Virgin Media's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between Skype for Business Server 2015 network in the Enterprise LAN and Virgin Media'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 Skype for Business with Virgin Media SIP Trunk



## 2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	<ul> <li>Microsoft Skype for Business Server 2015 environment is located on the Enterprise's LAN</li> </ul>
	<ul> <li>Virgin Media SIP Trunk is located on the WAN</li> </ul>
Signaling Transcoding	<ul> <li>Microsoft Skype for Business Server 2015 operates with SIP- over-TLS transport type</li> </ul>
	<ul> <li>Virgin Media SIP Trunk operates with SIP-over-UDP transport type</li> </ul>
Codecs Transcoding	<ul> <li>Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders</li> </ul>
	<ul> <li>Virgin Media SIP Trunk supports both G711 A-Law and G711 U- law. The testing was only conducted using G711 A-law as this is Virgin Media SIP Trunk preferred codec for interoperability testing</li> </ul>
Media Transcoding	<ul> <li>Microsoft Skype for Business Server 2015 operates with SRTP media type</li> </ul>
	<ul> <li>Virgin Media SIP Trunk operates with RTP media type</li> </ul>

## 2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Skype for Business Server 2015 and Virgin Media 's SIP Trunk.

This page is intentionally left blank.

# 3 Configuring Skype for Business Server 2015

This chapter describes how to configure Microsoft Skype for Business Server 2015 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.



**Note:** For the intention of sending a proper address string for call establishment, it was agreed that a full E.164 number format be preceded by a leading '+' symbol. Therefore, you should ensure you configure Microsoft Skype for Business Server 2015 dial plan to work in full E.164 number format.

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

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

- > To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:
- On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows Start menu > search for Skype for Business Server Topology Builder), as shown below:
  - Figure 3-1: Starting the Skype for Business Server Topology Builder



The following is displayed:

### Figure 3-2: Topology Builder Dialog Box

Topology Builder	x			
Welcome to Topology Builder. Select the source of the Skype for Business Server topology document.				
<ul> <li>Download Topology from existing deployment Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.</li> </ul>				
<ul> <li>Open Topology from a local file</li> <li>Open an existing Topology Builder file. Use this option if you have work in progress.</li> </ul>				
<ul> <li>New Topology Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.</li> </ul>				
Help OK Cancel	]			

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

15	Save Topo	ogy As		x
🔄 🕘 🔻 🕇 📳 « Ad	ministrator > Documents	∨ Ċ Searc	ch Documents	م
Organize 👻 New folde	r			∷ • @
🔆 Favorites	Name	Date modified	Туре	Size
🛄 Desktop	2015.05.25.tbxml	5/25/2015 3:58 PM	TBXML File	49 KB
🗼 Downloads	2015.05.31.tbxml	5/31/2015 11:37 AM	TBXML File	49 KB
🔚 Recent places	First_Topology.tbxml	5/17/2015 9:56 AM	TBXML File	45 KB
I툎 This PC 역 Network				
File <u>n</u> ame: interop				
Save as <u>t</u> ype: Topol	ogy Builder files (*.tbxml)			~
) Hide Folders			<u>S</u> ave	Cancel

**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

S S	kype for Business Server	r 2015, Topology Builder 📃 🗖
<u>File</u> <u>A</u> ction <u>H</u> elp		
▲ Ls Skype for Business Server	SIP domain	
<ul> <li>Interop</li> <li>Lync Server 2010</li> <li>Lync Server 2013</li> <li>Skype for Business Server 2015</li> <li>Standard Edition Front End Servers</li> <li>Enterprise Edition Front End pools</li> <li>Director pools</li> </ul>	Default SIP domain: Additional supported SIP domains: Simple URLs	S4B.interop Not configured
Mediation pools	Shiple OKES	
Persistent Chat pools Edge pools Trusted application servers	Phone access URLs:	Active Simple URL https://dialin.S4B.interop
🚞 Video Interop Server pools	Meeting URLs:	Active Simple URL SIP domain
<ul> <li>Image: Shared Components</li> <li>Image: Branch sites</li> </ul>	Administrative access URL:	https://meet.S4B.interop S4B.interop https://admin.S4B.interop
	Central Management Serv	rver
	Central Management	Active Front End Site
	Server:	✓ FE.S4B.interop Interop

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

Figure 3-5: Choosing New IP/PSTN Gateway

10	Skype for Business Server 2015, Topology Builder
<u>File Action H</u> elp	
<ul> <li>Skype for Business Server</li> <li>Interop</li> <li>Lync Server 2010</li> <li>Lync Server 2013</li> <li>Skype for Business Server 2015</li> <li>Skype for Business Server 2015</li> <li>Shared Components</li> <li>SQL Server stores</li> <li>File stores</li> <li>File stores</li> <li>PS</li> <li>Trr</li> <li>New IP/PSTN Gateway</li> <li>Of</li> <li>Topology</li> <li>Vic</li> <li>Help</li> <li>SIP Video trunks</li> </ul>	The properties for this item are not available for editing.
Branch sites	

The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN

9	Define New IP/PSTN Gateway
5	Define the PSTN Gateway FQDN
Define th FQDN: *	he fully qualified domain name (FQDN) for the PSTN gateway.
	B.interop
Help	Back Next Cancel

- 5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP.S4B.interop**). This FQDN should be equivalent to the configured Subject Name (CN) in the TLS Certificate Context (see Section 4.8.3 on page 55).
- 6. Click **Next**; the following is displayed:

Figure 3-7: Define the IP Address

15	Define New IP/PSTN Gateway	х			
5	Define the IP address				
● Enab	le IPv4				
🔍 🔍 U	se all configured IP addresses.				
O Li	imit service usage to selected IP addresses.				
P	STN IP address:				
O Enab	le IPv6				
• U	se all configured IP addresses.				
O Li	mit service usage to selected IP addresses.				
P	PSTN IP address:				
Help	Back Next Cancel				

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

8. 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

8	Define New IP/PSTN Gateway	X
5	Define the root trunk	
<u>T</u> runk nam	ne: *	
ITSP.S4B.	interop	
Listening g	port for IP/PSTN gateway: *	
5067		
SIP T <u>r</u> ansp	port Protocol:	
TLS		•
Associated	d <u>M</u> ediation Server:	
FE.S4B.int	terop Interop	-
Associated	d Mediation <u>S</u> erver port: *	
5067		
Help	<u>B</u> ack <u>Einish</u> Cancel	

- a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**). This parameter is later configured in the SIP Interface table (see Section 4.2 on page 35).
- **b.** In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses. This parameter is later configured in the SIP Interface table (see Section 4.2 on page 35).
- **c.** In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
- **d.** In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
- e. Click Finish.

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

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

S S	kype for Business Server 2	2015, Topology Builder	
<u>File</u> <u>A</u> ction <u>H</u> elp			
<ul> <li>Skype for Business Server</li> <li>Interop</li> <li>Lync Server 2010</li> <li>Lync Server 2013</li> <li>Skype for Business Server 2015</li> <li>Shared Components</li> <li>SQL Server stores</li> <li>File stores</li> <li>File stores</li> <li>PSTN gateways</li> <li>ITSP.S4B.interop</li> <li>Trunks</li> <li>Trunks</li> <li>Office Web Apps Servers</li> <li>Video gateways</li> <li>SIP Video trunks</li> <li>Branch sites</li> </ul>	Trunk name: PSTN gateway: Listening port: SIP Transport Protocol: Mediation Server: Mediation Server port:	ITSP.S48.interop ITSP.S48.interop (Interop) 5067 TLS FE.S48.interop (Interop) 5067	

9. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology

16	Skype for Business Server 2015, Topology Builder					uilder	
File	Action	Help					
	New Ce	ntral Site					
	Edit Pro	perties		SIP domain			
	New Top	oology		Default SIP domain:	S4B.int	aron	
	Open To	pology					
	Downloa	ad Topology		Additional supported SIP domains:	Not co	nfigured	
	Save a c	opy of Topology As					
	Publish	Гороlоду					
	Install o	upgrade a database		Simple URLs			
	Remove	Deployment					
	Help			Phone access URLs:	Active	Simple URL	
<sup>™</sup> Zy ITSP.S4B.interop		,		<ul><li>✓</li></ul>	https://dialin.S4B.interop		
	Þ	Office Web Apps Servers		Meeting URLs:	Active	Simple URL	SIP domain
	ſ	📜 Video gateways			$\sim$	https://meet.S4B.interop	S4B.interop
	ſ	SIP Video trunks	Administrative acces		https://admin.S4B.interop		
	Ē 6	Branch sites		URL:			
				C			
				Central Management Serv	ver		
				Central Management	Active	Front End	Site
				Server:	$\checkmark$	FE.S4B.interop	Interop

The following is displayed:

Figure 3-11: Publish the Topology

8	Publish Topology	x
Publish the topo	ology	
	Business Server 2015 to correctly route messages in your deployment, you must y. Before you publish the topology, ensure that the following tasks have been	
<ul> <li>A file share has b</li> <li>All simple URLs h</li> <li>For Enterprise Ed Archiving Servers exceptions for ref</li> <li>For a single Stand completed.</li> <li>You are currently sysadmin role).</li> <li>If you are removit contact objects a</li> </ul>	ik on the root node did not return any errors. een created for all file stores that you have configured in this topology. have been defined. ition Front End pools and Persistent Chat pools and for Monitoring Servers and and Server stores are installed and accessible remotely, and firewall mote access to SQL Server are configured. dard Edition server, the "Prepare first Standard Edition server" task was a logged on as a SQL Server administrator (for example, as a member of the SQL ing a Front End pool, all users, common area phones, analog devices, application and conference directories have been removed from the pool to proceed, click Next.	
Help	Back Next Cancel	

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

Figure 3-12: Publishing in Progress

2	Publish Topology	x
	Publishing in progress	
	Please wait while Topology Builder tries to publish your topology.	
	Downloading global simple URL settings	^
	Succeeded	
	Updating role-based access control (RBAC) roles	
	Succeeded	
	Enabling topology	≡
	Note: The cmdlet Enable-CsTopology might cost seconds to a few hours depending on your system configuration. Please wait until the progress completes	~
	Back Next Cancel	

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

Figure 3-13: Publishing Wizard Complete

😽 Pub	lish Topology		×					
Publishing wizard complete								
Your	topology was successfully published.		_					
	Step	Status	1					
****	Publishing topology Downloading topology Downloading global simple URL settings Updating role-based access control (RBAC) roles Enabling topology	Success Success Success Success Success	View Logs					
To d	lose the wizard, click Finish.							
H	Help	Back Finish	Cancel					

12. Click Finish.

## 3.2 Configuring the "Route" on Skype for Business Server 2015

The procedure below describes how to configure a "Route" on the Skype for Business Server 2015 and to associate it with the E-SBC PSTN gateway.

- > To configure the "route" on Skype for Business Server 2015:
- Start the Microsoft Skype for Business Server 2015 Control Panel (Start > search for Microsoft Skype for Business Server Control Panel), as shown below:

Figure 3-14: Opening the Skype for Business Server Control Panel

Search						
Everywhere 🗸						
for Business Server Control Pane						
Skype for Business Server Deployment Wizard						
Skype for Business Server Topology Builder						
Skype for Business Server Control Panel						
Skype for Business Server Management Shell						

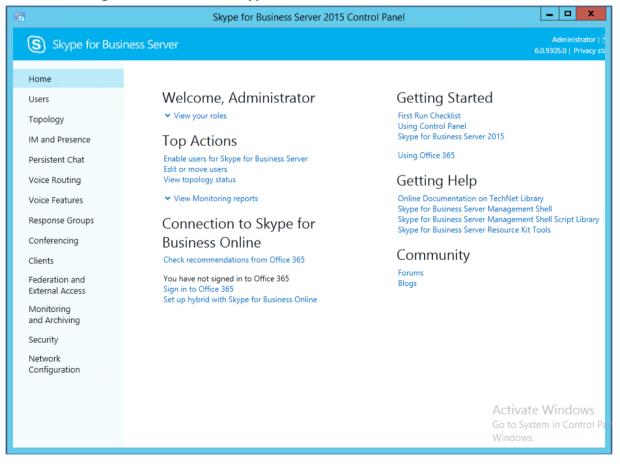
2. You are prompted to enter your login credentials:

Figure 3-15: Skype for Business Server Credentials

	Windows Security	x
AdminUIH Connecting to	ost o FE.S4B.interop.	
P	Administrator    Administrator    Domain: S4B  Remember my credentials	
	Connect a smart card	
	OK Cancel	

3. Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed:

Figure	3-16:	Microsoft	Skype	for E	Business	Server	2015	Control	Panel



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

	Figure 3-17: Voice Routing Page	
5	Skype for Business Server 2015 Control Panel	_ <b>D</b> X
Skype for Busine	ess Server	Administrator   Sign out 6.0.9305.0   Privacy statement
Home Users Topology	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTIN	G •
IM and Presence Persistent Chat	٩	
Voice Routing	🗣 New 🔻 🧪 Edit 🔻 Action 🔻 Commit 💌	0
Voice Features Response Groups	Name         Scope         State         Normalization rules         Description           Global         Global         Committed         1	
Conferencing Clients		
Federation and External Access		
Monitoring and Archiving		
Security Network Configuration		
		ate Windows System in Control Panel to a WS.

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

### Figure 3-18: Route Tab

<b>8</b>	Skype for B	usiness Server 2015 Control Panel	
Skype for Busine	ess Server		Administrator   Sign out 6.0.9305.0   Privacy statement
Home	DIAL PLAN VOICE POLICY ROUT	E PSTN USAGE TRUNK CONFIGURATION	TEST VOICE ROUTING
Users Topology	Create voice routing test case inf	ormation	~
IM and Presence Persistent Chat		٩	
Voice Routing	🗣 New 🧪 Edit 🔻 👚 Move up		Ø
Voice Features Response Groups	Name LocalRoute	State PSTN usage	Pattern to match ^(\+1[0-9](10))\$
Conferencing	Locarkoute	Commeed	(+ i(+)(+)))
Clients Federation and External Access			
Monitoring and Archiving			
Security Network Configuration			
			Activate Windows Go to System in Control Panel to a Windows.

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

Figure 3-19: Adding New Voice Route

Skype for Busi	ness Server	Administrator   Sign out 6.0.9305.0   Privacy statement
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING	
Users Topology	Create voice routing test case information	~
IM and Presence		
Persistent Chat	New Voice Route	Ø
Voice Routing	Scope:	•
Voice Features	Name: *	
Response Groups	ITSP	
Conferencing	Description:	
Clients		
Federation and External Access	<ul> <li>Build a Pattern to Match</li> <li>Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.</li> </ul>	
Monitoring and Archiving	Starting digits for numbers that you want to allow:	
Security	Type a valid number and then click Add. Add	
Network	Exceptions	
Configuration	Remove	
	Match this pattern: *	
	.*	
	Edit Reset	•

- 7. In the 'Name' field, enter a name for this route (e.g., ITSP).
- 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**.
- 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 3-20: List of Deployed Trunks

Skype for Busin				
Home	DIAL PLAN VOICE P	OLICY ROUTE PSTN USAGE	TRUNK CONFIGURATIO	N TEST VOICE ROUTING
Users	_			
Topology	Create voice r Se	lect Trunk		23
IM and Presence				Q
Persistent Chat	New Voice Routi			~
Voice Routing	√ ок 🗙	Service	Site	
Voice Features		PstnGateway:ITSP.S4B.interop	Interop	
Response Groups	Edit			
Conferencing	Suppress cal			
Clients	Alternate ca			
Federation and External Access	Associated trun			
Monitoring and Archiving	Associated truin			
Security				
Network Configuration				
	Associated PSTN		ОК	Cancel
	Select			Cancer
	PSTN usage record	Associated voice polic	ies	

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

Skype for Busin	ess Server
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING
Users Topology	Create voice routing test case information
IM and Presence Persistent Chat	New Voice Route
Voice Routing	Match this pattern: *
Voice Features Response Groups Conferencing	Edit Reset ?
Clients Federation and External Access	Suppress caller ID Atternate caller ID:
Monitoring and Archiving	Associated trunks:
Security Network Configuration	PstnGateway:ITSP.S4B.interop Add Remove

Figure 3-21: Selected E-SBC Trunk

### **10.** Associate a PSTN Usage to this route:

a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

### Figure 3-22: Associating PSTN Usage to Route

Skype for Busine	ess Server					
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING					
Users						
Topology	Create voice routing test case information					
IM and Presence	New Voice Route					
Persistent Chat						
Voice Routing						
Voice Features						
Response Groups	Associated trunks:					
Conferencing	PstnGateway:ITSP.S4B.interop Add					
Clients	Remove					
Federation and						
External Access	Associated PSTN Usages					
Monitoring and Archiving	🔚 Select Remove 🏫 🦺					
Security	PSTN usage record Associated voice policies					
Network	Internal					
Configuration	Local					
	Long Distance					

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

Skype for Busine	ess Server						
Home	DIAL PLAN VOICE POLICY	ROUTE PSTN USAGE	TRUNK CONFIGURATION	TEST VOICE ROUTING			
Users							
Topology	Create voice routing test o	Create voice routing test case information					
IM and Presence							
Persistent Chat			Q				
Voice Routing							
Voice Features	🖶 New 🧪 Edit 🔻 👚 M	love up 🕹 Move down		Pattern to match			
Response Groups	LocalRoute	Committed	PSTN usage	^(\+1[0-9]{10})\$			
Conferencing	ITSP	1 Uncommitted	Internal	^((\+66) (66))			

Figure 3-23: Confirmation of New Voice Route

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

Figure 3-24: Committing Voice Routes

Skype for Business Server							
Home	DIAL PLAN VOICE POLICY ROU	TE PSTN USAGE TRUNK CO	ONFIGURATION TEST VOICE ROUTING				
Users							
Topology	Create voice routing test case information						
IM and Presence							
Persistent Chat			<b>Q</b>				
Voice Routing							
Voice Features	🕂 New 🧪 Edit 🔻 👚 Move up	÷	Commit  Review uncommitted changes match				
Response Groups	Name LocalRoute	State PSTN usa Committed	Commit all (10))\$				
Conferencing	ITSP	1 Uncommitted Internal	Cancel selected changes 6))				
Clients			Cancel all uncommitted changes				

The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings

Uncommitted Voice Confi	iguration Settin	igs		2
Routes				^
Identity	Action	New value (pattern to match)	Old value (pattern to match)	
ITSP	Added	^((\+66) (66))		
			OK	Iancel

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

Figure 3-26: Confirmation of Successful Voice Routing Configuration

Skype for Busine							
Home	DIAL PLAN VOICE POLICY RO	UTE PSTN USAGE	TRUNK CONFIGURATION	TEST VOICE ROUTING			
Users Topology	Create voice routing test case information						
IM and Presence							
Persistent Chat			Q				
Voice Routing							
Voice Features	Hew Zedit - Move Name	up 🔸 Move down State	Action  Commit	Pattern to match			
Response Groups	LocalRoute						
Conferencing	ITSP						
Clients		O Successfully	y published voice routing o	configuration.			
Federation and External Access				Close			
Monitoring and Archiving							
Security							
Network Configuration							

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

Skype for Business Server						
Home	DIAL PLAN VOICE POLICY	ROUTE PSTN USAGE	TRUNK CONFIGURATION	TEST VOICE ROUTING		
Users						
Тороlоду	Create voice routing test ca	se information			*	
IM and Presence						
Persistent Chat			Q			
Voice Routing		_				
Voice Features	🖶 New 🧪 Edit 🔻 👚 Mo		Action 🔻 Commit 🔻		0	
Barran Garran	Name	State	PSTN usage	Pattern to match		
Response Groups	LocalRoute	Committed		^(\+1[0-9]{10})\$		
Conferencing	ITSP	Committed	Internal	^((\+66) (66))		
Clients						
Federation and External Access						
Monitoring and Archiving						
Security						
Network Configuration						

### Figure 3-27: 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 Skype for Business user number). This ID is required by Virgin Media 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 4.5 on page 47).

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.

Skype for Business Server         Administrator   Sign out           6.0.9305.0   Privacy statement						
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING					
Users Topology	Create voice routing test case information					
IM and Presence						
Persistent Chat	٩					
Voice Routing		0				
Voice Features		s Called number rules				
Response Groups	💮 Global Global Committed 0	0				

### Figure 3-28: Voice Routing Screen – Trunk Configuration Tab

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

Figure	3-29:Edit	Trunk	Configuration	n Page
inguic	0 20.Eul	I I MIIIN	ooningunution	i i ugo

Skype for Busin	ess Server	Administrator   Sign out 6.0.9305.0   Privacy statement
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING	
Users		
Topology	Create voice routing test case information	~
IM and Presence		
Persistent Chat	New Trunk Configuration - PstnGateway:ITSP.S4B.interop	
Voice Routing	J OK X Cancel	•
Voice Features	Scope: Pool Name: *	
Response Groups	PstnGateway:ITSP.S4B.interop	
Conferencing	Description:	
Clients		
Federation and	Maximum early dialogs supported:	
External Access		
Monitoring and Archiving	Encryption support level: Required	
Security	Refer support:	
Network	Enable sending refer to the gateway	
Configuration	✓ Enable media bypass	
	✓ Centralized media processing	
	Enable RTP latching	
	✓ Enable forward call history	
	Enable forward P-Asserted-Identity data	
	$  \vec{\checkmark}  $ Enable outbound routing failover timer	-

- c. Select the Enable forward call history check box, and then click OK.
- d. Repeat Steps 11 through 13 to commit your settings.
- **16.** Use the following command on the Skype for Business Server Management Shell after reconfiguration to verify correct values:
  - Get-CsTrunkConfiguration

Identity	:	
Service:PstnGateway:ITSP.S4B.interop		
OutboundTranslationRulesList	:	
SipResponseCodeTranslationRulesList	:	{ }
OutboundCallingNumberTranslationRulesList	:	{ }
PstnUsages	:	{ }
Description	:	
ConcentratedTopology	:	True
EnableBypass	:	True
EnableMobileTrunkSupport	:	False
EnableReferSupport	:	True
EnableSessionTimer	:	True
EnableSignalBoost	:	False
MaxEarlyDialogs	:	20
RemovePlusFromUri	:	False
RTCPActiveCalls	:	True
RTCPCallsOnHold	:	True
SRTPMode	:	Required
EnablePIDFLOSupport	:	False

EnableRTPLatching	: False
EnableOnlineVoice	: False
ForwardCallHistory	: True
Enable3pccRefer	: False
ForwardPAI	: False
EnableFastFailoverTimer	: True
EnableLocationRestriction	: False
NetworkSiteID	:

# 4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Skype for Business Server 2015 and the Virgin Media 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:

- E-SBC WAN interface Virgin Media SIP Trunking environment
- E-SBC LAN interface Skype for Business Server 2015 environment

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

### Notes:

- For implementing Microsoft Skype for Business and Virgin Media SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a License Key that includes the following software features:
  - 🔸 Microsoft
  - √ SBC
  - ✓ Security
  - 🗸 DSP
  - 🗸 RTP
  - √ SIP

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

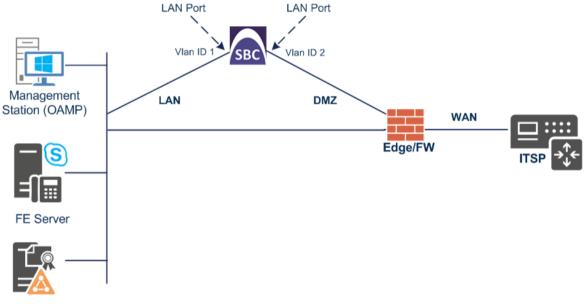
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at <a href="https://www.audiocodes.com/library/technical-documents">https://www.audiocodes.com/library/technical-documents</a>.
- IP addresses used in this Configuration Note are for example purposes only and do not reflect the live environment.

## 4.1 Step 1: IP Network Interfaces Configuration

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

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

### Figure 4-1: Network Interfaces in Interoperability Test Topology



DC+DNS+Cert Server

## 4.1.1 Step 1a: Configure VLANs

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

- LAN VoIP (assigned the name "LAN\_IF")
- WAN VoIP (assigned the name "WAN\_IF")
- **To configure the VLANs:**
- Open the Ethernet Device table (Setup menu > IP Network tab > Core Entities folder > Ethernet Devices).
- 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

Ethernet De	vices (2)		
+ New Edit		I⊲ ≪ Page 1 of 1 → ►I Show 10 ▼	] records per page
INDEX 🗢	VLAN ID	UNDERLYING INTERFACE N	IAME TAGGING
0	1	GROUP_1 vl	an 1 Untagged
1	2	GROUP_2 vli	an 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:

- LAN VoIP (assigned the name "LAN\_IF")
- WAN VoIP (assigned the name "WAN\_IF")
- > To configure the IP network interfaces:
- Open the IP Interfaces table (Setup menu > IP Network tab > Core Entities folder > IP Interfaces).
- 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	10.15.77.10 (LAN 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	LAN_IF (arbitrary descriptive name)
Primary DNS Server IP Address	10.15.27.1
Underlying Device	vlan 1

- 3. Add a network interface for the WAN side:
  - a. Click New.
  - **b.** Configure the interface as follows:

Parameter	Value
Application Type	Media + Control
IP Address	195.189.192.154 (DMZ IP address of E-SBC)
Prefix Length	25 (subnet mask in bits for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
Interface Name	WAN_IF
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.

The configured IP network interfaces are shown below:

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

IP Interfa	aces (2)								
+ New E	dit 📄 🗌 🟛		🛯 <	1of1 ⊨> ► S	ihow 10 🔻 recor	ds per page			Q
INDEX 🗢	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.77.10	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.154	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

## 4.2 Step 2: Configure Media Realms

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

### > To configure Media Realms:

- 1. Open the Media Realms table (Setup menu > Signaling & Media tab > Core Entities folder > Media Realms).
- 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	LAN_IF
Port Range Start	<b>6000</b> (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

### Figure 4-4: Configuring Media Realm for LAN

Media Realms [MRLan]			- x
GENERAL		QUALITY OF EXPERIENC	CE
Index	0	QoE Profile	v View
Name	MRLan	Bandwidth Profile	View
Topology Location	Down <b>v</b>		
IPv4 Interface Name	● #0 [LAN_IF] ▼ Vie	w	
Port Range Start	• 6000		
Number Of Media Session Leg	gs • 100		
Port Range End	6999		
Default Media Realm	No 🔻		
	Cancel	APPLY	

3. Click **New** to configure a Media Realm for WAN traffic:

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

### Figure 4-5: Configuring Media Realm for WAN

lia Realms <b>[MRWan]</b>				-
GENERAL		QUALITY OF EXPERIENC	:E	
Index Name	1 MRWan	QoE Profile Bandwidth Profile	<b>Y</b>	View View
Topology Location IPv4 Interface Name Port Range Start	<ul> <li>Up </li> <li>#1 [WAN_IF] </li> <li>7000</li> </ul>	2W		
Number Of Media Session Legs	<ul> <li>100</li> <li>7999</li> </ul>			
Default Media Realm	No 🔻			
	Cancel	APPLY		

The configured Media Realms are shown in the figure below:

+ New Ec	dit 🛛 🗌 面	I <	of 1 🕨 🕨 Show	10 🔻 records per pa	ge	Q
NDEX 🗢	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MRLan	LAN_IF	6000	100	6999	No
1	MRWan	WAN_IF	7000	100	7999	No

# 4.3 Step 3: Configure SIP Signaling Interfaces

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

- To configure SIP Interfaces:
- 1. Open the SIP Interfaces table (Setup menu > Signaling & Media tab > Core Entities folder > SIP Interfaces).
- 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	S4B (see note at the end of this section)
Network Interface	LAN_IF
Application Type	SBC
UDP Port (for supporting Fax ATA device)	5060 (if required)
ТСР	0
TLS Port	5067 (see note below)
Media Realm	MRLan



**Note:** The TLS port parameter must be identically configured in the Skype for Business Topology Builder (see Section 3.1 on page 13).

3. Click **New** to configure a SIP Interface for the WAN:

Parameter	Value
Index	1
Interface Name	VM
Network Interface	WAN_IF
Application Type	SBC
UDP Port	5060
TCP and TLS	0
Media Realm	MRWan

The configured SIP Interfaces are shown in the figure below:

+ New Edit and the set of the se					Q				
INDEX 🗢	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATIN PROTOCOL	MEDIA REALM
0	S4B	DefaultSRD	LAN_IF	SBC	5060	0	5067	No encapsulati	MRLan
1	VM	DefaultSRD	WAN_IF	SBC	5060	0	0	No encapsulation	MRWan



**Note:** Current software releases uses the string **names** of the configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups). Therefore, it is recommended to configure each configuration entity with meaningful names for easy identification.

# 4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Skype for Business Server 2015
- Virgin Media SIP Trunk A
- Virgin Media SIP Trunk B
- Fax supporting ATA device (optional)

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

#### > To configure Proxy Sets:

- 1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets).
- 2. Add a Proxy Set for the Skype for Business Server 2015 as shown below:

Parameter	Value
Proxy Set ID	1
Proxy Name	S4B
SBC IPv4 SIP Interface	S4B
Proxy Keep Alive	Using Options
Redundancy Mode	Homing
Proxy Hot Swap	Enable
Load Balancing Method	Round Robin

		SRD #0 [Default	tSRD]	T		
GENERAL				REDUNDANCY		
Index		1		Redundancy Mode	<ul> <li>Homing</li> </ul>	•
Name	L	64D		2		•
Name	•	S4B		Proxy Hot Swap	<ul> <li>Enable</li> </ul>	_
Gateway IPv4 SIP Interface		*	View	Proxy Load Balancing Method	<ul> <li>Round Rc</li> </ul>	۳
SBC IPv4 SIP Interface	•	#0 [S4B] 🔻	<ul> <li>View</li> </ul>	Min. Active Servers for Load Balancing	1	
TLS Context Name	[	•	View			
				ADVANCED		
KEEP ALIVE				Classification Input IP Address on	V	Ŧ
Proxy Keep-Alive		Using OPTIONS	•	DNS Resolve Method	-	Ŧ
Proxy Keep-Alive Time [sec]		60				
Keep-Alive Failure Responses						

Figure 4-8: Configuring Proxy Set for Microsoft Skype for Business Server 2015

a. Select the index row of the Proxy Set that you added, and then click the Proxy Address link located below the table; the Proxy Address table opens.
b. Click New; the following dialog box appears:

## Figure 4-9: Configuring Proxy Address for Microsoft Skype for Business Server 2015

Proxy A	Address		– x
	GENERAL		
	Index	0	
	Proxy Address	FE.S4B.interop:5067	
	Transport Type	TLS 🔻	
			^

- **c.** Configure the address of the Proxy Set according to the parameters described in the table below.
- d. Click Apply.

Parameter	Value
Index	0
Proxy Address	<b>FE.S4B.interop:5067</b> (Skype for Business Server 2015 IP address / FQDN and destination port)
Transport Type	TLS

3. Configure a Proxy Set for the Virgin Media SIP Trunk A:

Parameter	Value
Proxy Set ID	2
Proxy Name	VM Trunk A
SBC IPv4 SIP Interface	VM
Proxy Keep-Alive	Using Options
Proxy Keep-Alive Time [sec]	30
Keep-Alive Failure Responses	503

### Figure 4-10: Configuring Proxy Set for Virgin Media SIP Trunk A

Proxy S	oxy Sets [VM Trunk A] – x							
		SRD	ultSRD]	•				
	GENERAL		REDUNDANCY					
	Index	2		Redundancy Mode			•	
	Name •	VM Trunk A		Proxy Hot Swap Proxy Load Balancing Method		Disable	۲	
	Gateway IPv4 SIP Interface		View			Disable	•	
	SBC IPv4 SIP Interface	● #1 [VM] ▼		Min. Active Servers for Load Balancing		1		
	TLS Context Name		View					
				ADVANCED				
	KEEP ALIVE			Classification Input	IP Addre	ss only	Ŧ	
	Proxy Keep-Alive	Using OPTIONS	Ŧ	DNS Resolve Method	i		Ŧ	
	Proxy Keep-Alive Time [sec]	• 30						
	Keep-Alive Failure Responses	• 503						
			Cancel	PPLY				

- a. Select the index row of the Proxy Set that you added, and then click the Proxy Address link located below the table; the Proxy Address table opens.
   b. Click News the following dialog have apprecised.
- **b.** Click **New**; the following dialog box appears:

Proxy Address		– x
GENERAL		
Index	0	
Proxy Address	• 213.106.222.186:5060	
Transport Type	• UDP	•

### Figure 4-11: Configuring Proxy Address for Virgin Media SIP Trunk A

- **c.** Configure the address of the Proxy Set according to the parameters described in the table below.
- ParameterValueIndex0Proxy Address213.106.222.186:5060 ( IP address / FQDN and destination port)Transport TypeUDP
- 4. Configure a Proxy Set for the Virgin Media SIP Trunk B:

Parameter	Value
Proxy Set ID	3
Proxy Name	VM Trunk B
SBC IPv4 SIP Interface	VM
Proxy Keep-Alive	Using Options
Proxy Keep-Alive Time [sec]	30
Keep-Alive Failure Responses	503

oxy Sets [VM Trunk B]					-
	SRD	#0 [De	faultSRD]		
GENERAL			REDUNDANCY		
Index	3		Redundancy Mode		٣
Name	VM Trunk B		Proxy Hot Swap	Disable	•
Gateway IPv4 SIP Interface		View	Proxy Load Balancing Method	Disable	•
SBC IPv4 SIP Interface	• #1 [VM] 🔻	View	Min. Active Servers for Load Balancing	1	
TLS Context Name		View			
			ADVANCED		
KEEP ALIVE			Classification Input IP A	Address only	Ŧ
Proxy Keep-Alive	Using OPTIONS	•	DNS Resolve Method		•
Proxy Keep-Alive Time [sec]	• 30				
Keep-Alive Failure Responses	• 503				
	C	ancel	APPLY		

Figure 4-12: Configuring Proxy Set for Virgin Media SIP Trunk B

- a. Select the index row of the Proxy Set that you added, and then click the **Proxy** Address link located below the table; the Proxy Address table opens.
- **b.** Click **New**; the following dialog box appears:

Figure 4-13: Configuring Proxy Address for Virgin Media SIP Trunk B

Proxy A	ddress		– x
	GENERAL		
	Index	0	
	Proxy Address	<ul> <li>82.14.171.234:5060</li> </ul>	
	Transport Type	• UDP •	
	c. Configure	he address of the Proxy Set according to the parameters de	scribed in

- c. Configure the address of the Proxy Set according to the parameters described in the table below.
- d. Click Apply.

Parameter	Value
Index	0
Proxy Address	82.14.171.234:5060 (IP address / FQDN and destination port)
Transport Type	UDP

**5.** Configure a Proxy Set for Fax supporting ATA device (if required):

Parameter	Value
Proxy Set ID	4
Proxy Name	MP-Fax
SBC IPv4 SIP Interface	S4B

### Figure 4-14: Configuring Proxy Set for Fax ATA device

Proxy	/Sets [MP-Fax]										– x
			SRD		#0	[Defa	ultSRD]				
	GENERAL						REDUNDANCY				
	Index		4				Redundancy Mode			•	
	Name	•	MP-Fax				Proxy Hot Swap		Disable	•	
	Gateway IPv4 SIP Interface			•	View		Proxy Load Balancing Method	l	Disable	•	
	SBC IPv4 SIP Interface	•	#0 [S4B]	•	View		Min. Active Servers for Load B	alancing	1		
	TLS Context Name			•	View						_
							ADVANCED				
	KEEP ALIVE						Classification Input	IP Address or	nly	•	
	Proxy Keep-Alive		Disable		•		DNS Resolve Method			•	
	Proxy Keep-Alive Time [sec]		60								
	Keep-Alive Failure Responses										
				C	Cancel	A	PPLY				

a. Select the index row of the Proxy Set that you added, and then click the Proxy Address link located below the table; the Proxy Address table opens.
b. Click New; the following dialog box appears:

Figure 4-15: Configuring Proxy Address for Fax ATA device

Proxy Address		– x
GENERAL		
Index	0	
Proxy Address	• 10.15.77.12:5060	
Transport Type	• UDP •	

**c.** Configure the address of the Proxy Set according to the parameters described in the table below.

### d. Click Apply.

Parameter	Value
Index	0
Proxy Address	<b>10.15.17.12:5060</b> (IP address / FQDN and destination port)
Transport Type	UDP

The configured Proxy Sets are shown in the figure below:

### Figure 4-16: Configured Proxy Sets in Proxy Sets Table

Proxy Se	ets (5)						
+ New	Edit 🛛 🗍 面	14 <4	Page 1 of 1	▶> ► Show 10	▼ records per p	age	Q
INDEX 🗢	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP- ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD		S4B	60		Disable
1	S4B	DefaultSRD		S4B	60	Homing	Enable
2	VM Trunk A	DefaultSRD		VM	30		Disable
3	VM Trunk B	DefaultSRD		VM	30		Disable
4	MP-Fax	DefaultSRD		S4B	60		Disable

# 4.5 Step 5: Configure IP Profiles

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

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

- Microsoft Skype for Business Server 2015 to operate in secure mode using SRTP and TLS
- Virgin Media SIP trunk to operate in non-secure mode using RTP and UDP
- Fax ATA device to operate in non-secure mode using RTP and UDP
- > To configure IP Profile for the Skype for Business Server 2015:
- Open the IP Profiles table (Setup menu > Signaling & Media tab > Coders & Profiles folder > IP Profiles).
- 2. Click New, and then configure the parameters as follows:

Parameter	Value
General	
Index	1
Name	S4B
Media Security	
SBC Media Security Mode	SRTP
Symmetric MKI	Enable
MKI Size	1
Enforce MKI Size	Enforce
Reset SRTP State Upon Re-key	Enable
Generate SRTP Keys Mode:	Always
SBC Early Media	
Remote Early Media RTP Detection Mode	<b>By Media</b> (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Signaling	
Remote Update Support	Not Supported
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Remote 3xx Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)

GENERAL				SBC SIGNALING		
Index	1			PRACK Mode		Transparent 🔹
Name	S4B			P-Asserted-Identity Header Mode		As Is
Created by Routing Server	No			Diversion Header Mode		As Is
				History-Info Header Mode		As Is
MEDIA SECURITY				Session Expires Mode		Transparent •
SBC Media Security Mode		SRTP	•	Remote Update Support	•	Not Supported
Gateway Media Security Mode		Preferable	Ŧ	Remote re-INVITE	٠	Supported only with SE 🔻
Symmetric MKI		Enable	•	Remote Delayed Offer Support	٠	Not Supported
MKI Size		1		Remote Representation Mode		According to Operation <b>v</b>
SBC Enforce MKI Size		Enforce	Ŧ	Keep Incoming Via Headers		According to Operation 🔻
SBC Media Security Method		SDES	•	Keep Incoming Routing Headers		According to Operation 🔻
				Keep User-Agent Header		According to Operation <b>•</b>

### Figure 4-17: Configuring IP Profile for Skype for Business Server 2015

#### 3. Click Apply.

#### > To configure an IP Profile for the Virgin Media SIP Trunk:

1. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	2
Name	VM
Media Security	
SBC Media Security Mode	RTP
SBC Media	
Allowed Audio Coders	VM
SBC Signaling	
Remote Update Support	Not Supported
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	<b>Handle Locally</b> (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
SBC Hold	
Remote Hold Format	<b>Send Only</b> (required, as Virgin Media work is in Send Only mode)

GENERAL				SBC SIGNALING			
Index	2	2		PRACK Mode		Transparent	Ŧ
Name	• \	/M		P-Asserted-Identity Header Mode	•	Add	Ŧ
Created by Routing Server	1	No		Diversion Header Mode		As Is	۳
				History-Info Header Mode		As Is	۳
MEDIA SECURITY				Session Expires Mode		Transparent	۳
SBC Media Security Mode		RTP	Ŧ	Remote Update Support	•	Not Supported	٣
Gateway Media Security Mode		Preferable	•	Remote re-INVITE		Supported	۳
Symmetric MKI		Disable	•	Remote Delayed Offer Support		Supported	٣
MKI Size		0		Remote Representation Mode		According to Operation Mod	٣
SBC Enforce MKI Size		Don't enforce	•	Keep Incoming Via Headers		According to Operation Mod	٣
SBC Media Security Method		SDES	•	Keep Incoming Routing Headers		According to Operation Mod	۳
				Keep User-Agent Header		According to Operation Mod	v

Figure 4-18: Configuring IP Profile for Virgin Media SIP Trunk

# 4.6 Step 6: 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:

- Skype for Business Server 2015 (Mediation Server) located on LAN
- Virgin Media SIP Trunk located on WAN
- Fax supporting ATA device located on LAN (if required)

### **To configure IP Groups:**

 Open the IP Groups table (Setup menu > Signaling & Media tab > Core Entities folder > IP Groups).

Parameter	Value
Index	1
Name	S4B
Topology Location	Down
Туре	Server
Proxy Set	S4B
IP Profile	S4B
Media Realm	MRLan
SIP Group Name	213.106.222.186 (according to ITSP requirement)
Classify By Proxy Set	Enable

2. Add an IP Group for the Skype for Business Server 2015 as shown below:

**3.** Configure an IP Group for the Virgin Media SIP Trunk A:

Parameter	Value
Index	2
Name	VM Trunk A
Topology Location	Up
Туре	Server
Proxy Set	VM Trunk A
IP Profile	VM
Media Realm	MRWan
SIP Group Name	213.106.222.186 (according to ITSP requirement)

4. Configure an IP Group for the Virgin Media SIP Trunk B:

Parameter	Value
Index	3
Name	VM Trunk B
Topology Location	Up
Туре	Server
Proxy Set	VM Trunk B
IP Profile	VM
Media Realm	MRWan
SIP Group Name	82.14.171.234 (according to ITSP requirement)

5. Configure an IP Group for the Fax supporting ATA device:

Parameter	Value
Index	3
Name	MP-Fax
Туре	Server
Proxy Set	MP-Fax
Media Realm	MRLan
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-19: Configured IP Groups in IP Group Table

IP Grou	ıps (5)										
+ New	Edit 🗌 💼		14	e 🛹 Page 1	of1   ►> ► 5	5how 10 ▼ re	cords per page				Q
INDEX 🗢	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATI( SET	OUTBOUND MESSAGE MANIPULATI SET
0	Default_IPG	DefaultSR	Server	Not Configure					Disable	-1	-1
1	S4B	DefaultSR	Server	Not Configure	S4B	S4B	MRLan	213.106.222.1	Enable	-1	-1
2	VM Trunk A	DefaultSR	Server	Not Configure	VM Trunk A	VM	MRWan	213.106.222.1	Enable	-1	4
3	VM Trunk B	DefaultSR	Server	Not Configure	VM Trunk B	VM	MRWan	82.14.171.234	Enable	-1	4
4	MP-Fax	DefaultSR	Server	Not Configure	MP-Fax			213.106.222.1	Enable	-1	-1

# 4.7 Step 7: Configure Coders

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Virgin Media SIP Trunk uses the G.711A-law coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Virgin Media SIP Trunk (see Section 4.5 on page 47).

- To set a preferred coder for the Virgin Media SIP Trunk:
- Open the Allowed Audio Coders Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Allowed Audio Coders Groups).
- 2. Click **New** and configure a name for the Allowed Video Coders Group for Virgin Media SIP Trunk.

#### Figure 4-20: Configuring Allowed Coders Group for Virgin Media SIP Trunk

Allowed	Audio Coders Groups [VM]		– x
	GENERAL		
		-	
	Index	0	
	Name	• VM	

- 3. Click Apply.
- 4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Video Coders table opens.
- 5. Click **New** and configure an Allowed Coders as follows:

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

#### Figure 4-21: Configuring Allowed Coders for Virgin Media SIP Trunk

Allowed	l Audio Coders		– x
	GENERAL		
	Index	0	
	Coder	• G.711A-law	
	User-defined Coder		

# 4.8 **Step 8: SIP TLS Connection Configuration**

This section describes how to configure the E-SBC for using a TLS connection with the Skype for Business Server 2015 Mediation Server. This is essential for a secure SIP TLS connection.

## 4.8.1 Step 8a: Configure the NTP Server Address

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

- > To configure the NTP server address:
- 1. Open the Time & Date page (Setup menu > Administration tab > Time & Date).
- 2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.27.1**).

#### Figure 4-22: Configuring NTP Server Address

NTP SERVER	
Primary NTP Server Address (IP or FQDN) •	10.15.27.1
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

## 4.8.2 Step 8b: Configure the TLS version

This step describes how to configure the E-SBC to use TLS only. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

- To configure the TLS version:
- Open the TLS Contexts table (Setup menu > IP Network tab > Security folder > 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 'Edit'.
- 3. From the 'TLS Version' drop-down list, select 'TLSv1.0 TLSv1.1 and TLSv1.2'.

Contexts [default]			-
GENERAL		OCSP	
Index	0	OCSP Server	Disable <b>•</b>
Name	default	Primary OCSP Server	0.0.0.0
TLS Version	TLSv1.0 TLSv1.1 and Tl 🔻	Secondary OCSP Server	0.0.0.0
Cipher Server	RC4:EXP	OCSP Port	2560
Cipher Client	ALL: ADH	OCSP Default Response	Reject 🔻
Strict Certificate Extension Validation	Disable <b>v</b>		

#### Figure 4-23: Configuring TLS Version

## 4.8.3 Step 8c: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Skype for Business Server 2015.

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.



**Note:** The Subject Name (CN) field parameter should be identically configured in the DNS Active Directory and Topology Builder (see Section 3.1 on page 13).

### To configure a certificate:

- Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
- In the TLS Contexts page, select the required TLS Context index row, and then click the Change Certificate link located below the table; 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.S4B.interop**).
  - **b.** Fill in the rest of the request fields according to your security provider's instructions.
  - **c.** Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

ERTIFICATE SIGNING REQUEST	
Subject Name [CN]	ITSP.S4B.interop
Organizational Unit [OU] (optional)	
Company name [O] <i>(optional)</i>	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] <i>(optional)</i>	
Signature Algorithm	SHA-1
Create CSR	
creating the CSR, copy the text below (including the BEGIN/EN	D lines) and send it to your Certification Authority for signing.
-BEGIN CERTIFICATE REQUEST WjCBxAIBADAbMRkwFwYDV00DDBBJVFN0L1M00i5pbnRlcm9wMIGfM	MARCEAG
DOEBAOUAA4GNADCBiOKBgOCzEs8XTnY8be/t77eEDG7rTg747G030	

- 4. Copy the CSR from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
- 5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

#### Figure 4-25: Microsoft Certificate Services Web Page

licrosoft Certificate Services Demolab Ho
elcome
se this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your entity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, enform other security tasks.
ou can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to aw the status of a pending request.
or more information about Certificate Services, see Certificate Services Documentation.
elect a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

### 6. Click Request a certificate.

Figure 4-26: Request a Certificate Page

Microsoff Certificate Services Demolab	<u>Home</u>
Request a Certificate	
Select the certificate type: <u>Web Browser Certificate</u> <u>E-Mail Protection Certificate</u>	
Or, submit an <u>advanced certificate request</u>	

7. Click advanced certificate request, and then click Next.



Microsoft Certificate Services Demolab Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

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

Microsoft Active	e Directory Certificate Services Lync-DC-LYNC-CA	<u>Home</u>
Submit a Certi	tificate Request or Renewal Request	
	aved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal re an external source (such as a Web server) in the Saved Request box.	equest
Saved Request:	1	
certificate request (CMC or	A8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxuyKk1 tr4ootrnsP0CAUEAAAAMAOCC3qG3Ib5D02BBAUA IMnKHAksMag9aAgoLKmuch2b2CMqECGAFTBok 95Sm8c4Bj8ib+R5+YI+Ost57xT9D2XNg5Yp4G+OB vnQuXOUUX6BsVBT71aO83BcA END CERTIFICATE REQUEST	
Certificate Temp	plate:	
	Web Server 👻	
Additional Attrib	butes:	
Attributes:	K	
	Submit >	

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

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

Figure 4-29: Certificate Issued Page

Certificate Issue	d
The certificate yo	u requested was issued to you.
Downloa	encoded or ⊚Base 64 encoded ad certificate ad certificate chain

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

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:	
© DER © Base 64	
Download CA certificate Download CA certificate chain Download latest base CRL	

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

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

- 19. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
  - a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; 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 13, 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 <i>(optional)</i>	audc
Send <b>Private Key</b> file from your computer to the device. The file must be in either PEM or PFX (PKCS#12) format. Browse No file selected. Send File Note: Replacing the private key is not recommended but if it's dor	ne, 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.	
Browse No file selected. Send File	—

- 20. In the E-SBC's Web interface, return to the TLS Contexts page.
  - a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
  - **b.** Click the **Import** button, and then select the certificate file to load.

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



- **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 4.16 on page 89).

# 4.9 Step 9: Configure SRTP

This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 4.5 on page 47).

#### > To configure media security:

 Open the Media Security page (Setup menu > Signaling & Media tab > Media folder > Media Security).

Media Security						
GENERAL		AUTHENTICATION & ENCRYPTION				
Media Security	• Enable	•	Authentication On Transmitte	d RTP Packets	Active	•
Media Security Behavior	Preferable	•	Encryption On Transmitted RT	P Packets	Active	•
Offered SRTP Cipher Suites	All	•	Encryption On Transmitted RT	CP Packets	Active	•
Aria Protocol Support	Disable	•	SRTP Tunneling Authentication	n for RTP	Disable	•
			SRTP Tunneling Authentication	n for RTCP	Disable	•
MASTER KEY IDENTIFIER						
Master Key Identifier (MKI) Size	Master Key Identifier (MKI) Size 0		GATEWAY SETTINGS			
Symmetric MKI	Disable	v	Enable Rekey After 181	Disable		•

#### Figure 4-33: Configuring SRTP

- 2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
- 3. Click Apply.
- 4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 89).

# 4.10 Step 10: Configure Maximum IP Media Channels

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



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

#### > To configure the maximum number of IP media channels:

 Open the Media Settings page (Setup menu > Signaling & Media tab > Media folder > Media Settings).

	Figure 4-34: Configuring Number of Media Channels						
	Media Settings						
	GENERAL						
	NAT Traversal	Disable NAT 💌					
	Enable Continuity Tones	Disable 🗾 🗲					
	Inbound Media Latch Mode	Dynamic 🔹					
$\longrightarrow$	Number of Media Channels	• 100 5					
	Enforce Media Order	Disable 💌					
	SDP Session Owner	AudiocodesGW					

- 2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., 100).
- 3. Click Apply.
- 4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 89).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.6 on page46) to denote the source and destination of the call.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business Server 2015 (LAN) and Virgin Media SIP Trunks (DMZ):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and WAN interfaces.
- Calls from Skype for Business Server 2015 to Virgin Media SIP Trunk A
- Calls from Skype for Business Server 2015 to Virgin Media SIP Trunk B as an alternative route if SIP Trunk A fails
- Calls from Fax / Minicom supporting ATA device to Virgin Media SIP Trunk A (if required)
- Calls from Fax / Minicom supporting ATA device to Virgin Media SIP Trunk B as an alternative route if SIP Trunk A fails (if required)
- Calls from Virgin Media SIP Trunk A or B to Fax / Minicom supporting ATA device (if required)
- Calls from Virgin Media SIP Trunk A or B to Skype for Business Server 2015

#### **To configure IP-to-IP routing rules:**

- 1. Open the IP-to-IP Routing table (Setup menu > Signaling & Media tab > SBC folder > Routing > IP-to-IP Routing).
- 2. Configure a rule to terminate SIP OPTIONS messages received from the both LAN and WAN:
  - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	<b>OPTIONS termination</b> (arbitrary descriptive name)
Source IP Group	Any
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

#### Figure 4-35: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

IP-to-IP Routing [OPTIONS termination] _ x					
Routing Policy #0 [Default_SBCRoutingPolicy]					
GENERAL		ACTION			
Index	0	Destination Type	Dest Address	v	
Name	OPTIONS termination	Destination IP Group		View	
Alternative Route Options	Route Row 🔻	Destination SIP Interface		View	
		Destination Address	internal		
MATCH		Destination Port	0		
Source IP Group	Any View	Destination Transport Type		Y	
Request Type	OPTIONS     T	IP Group Set	<b>v</b>	View	
Source Username Pattern	*	Call Setup Rules Set ID	-1		
Source Host	*	Group Policy	Sequential	*	
Source Tag		Cost Group		View	
	Canc	el APPLY			

- 3. Configure a rule to route calls from Skype for Business Server 2015 to Virgin Media SIP Trunk A:
  - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	1
Route Name	<b>S4B to VM Trunk A</b> (arbitrary descriptive name)
Source IP Group	S4B
Destination Type	IP Group
Destination IP Group	VM Trunk A

### Figure 4-36: Configuring IP-to-IP Routing Rule for S4B to VM Trunk A

-to-IP Routing [S4B to VM Trunk A]				- ×
	Routing Policy #0 [	Default_SBCRoutingPolicy]		
GENERAL		ACTION		
Index	1	Destination Type	IP Group 🔻	
Name •	S4B to VM Trunk A	Destination IP Group	● #2 [VM Trunk A]    View	
Alternative Route Options	Route Row 🔻	Destination SIP Interface	View	
		Destination Address		
MATCH		Destination Port	0	
Source IP Group	• #1 [S4B] • View	Destination Transport Type	¥	
Request Type	All	IP Group Set	View	
Source Username Pattern	*	Call Setup Rules Set ID	-1	
Source Host	*	Group Policy	Sequential 🔻	
Source Tag		Cost Group	View	
	Cance	APPLY		

- 4. Configure a rule to route calls from Skype for Business Server 2015 to Virgin Media SIP Trunk B as alternative routing if the connection with SIP Trunk A fails:
  - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	<b>S4B to VM Trunk B</b> (arbitrary descriptive name)
Alternative Route Options	Alternative Route Ignore Inputs
Source IP Group	S4B
Destination Type	IP Group
Destination IP Group	VM Trunk B

#### Figure 4-37: Configuring IP-to-IP Routing Rule for S4B to VM Trunk B

IP-to-IP Routing [S4B to VM Trunk B]					– x
	Routing Policy	#0 [Defaul	t_SBCRoutingPolicy]		
GENERAL			ACTION		
Index	2		Destination Type	IP Group	v
Name	S4B to VM Trunk B		Destination IP Group	#3 [VM Trunk B]	View
Alternative Route Options	Alternative Route Ignore Inputs	•	Destination SIP Interface		View
			Destination Address		
MATCH			Destination Port	0	
Source IP Group	• #1 [S4B]	View	Destination Transport Type		v
Request Type	All	•	IP Group Set		View
Source Username Pattern	*		Call Setup Rules Set ID	-1	
Source Host	*		Group Policy	Sequential	•
Source Tag			Cost Group		View
	(	Cancel A	PPLY		

- 5. Configure a rule to route calls from Fax / Minicom supporting ATA device to Virgin Media SIP Trunk A:
  - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	3
Route Name	Fax to VM Trunk A (arbitrary descriptive name)
Source IP Group	MP-Fax
Destination Type	IP Group
Destination IP Group	VM Trunk A

### Figure 4-38: Configuring IP-to-IP Routing Rule for Fax / Minicom to VM Trunk A

IP-to-IP Routing [Fax to VM Trunk A]					– x
	Routing Policy #	#0 [Default	_SBCRoutingPolicy]		
GENERAL			ACTION		
Index	3		Destination Type	IP Group	v
Name	Fax to VM Trunk A		Destination IP Group	• #2 [VM Trunk A]	View
Alternative Route Options	Route Row	•	Destination SIP Interface		View
			Destination Address		
MATCH			Destination Port	0	
Source IP Group	• #4 [MP-Fax]   V	iew	Destination Transport Type		•
Request Type	All	v	IP Group Set		View
Source Username Pattern	*		Call Setup Rules Set ID	-1	
Source Host	*		Group Policy	Sequential	•
Source Tag			Cost Group		View
	Ca	incel Al	PPLY		

- 6. Configure a rule to route calls from the Fax / Minicom supporting the ATA device to Virgin Media SIP Trunk B, as alternative routing if the connection with the SIP Trunk A fails:
  - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	4
Route Name	Fax to VM Trunk B (arbitrary descriptive name)
Alternative Route Options	Alternative Route Ignore Inputs
Source IP Group	MP-Fax
Destination Type	IP Group
Destination IP Group	VM Trunk B

Figure 4-39: Configuring IP-to-IP Routing Rule for Fax / Minicom to VM Trunk B

P Routing [Fax to VM Trunk E			
	Routing Policy #	[Default_SBCRoutingPolicy]	
GENERAL		ACTION	
GENERAL		ACTION	
Index	4	Destination Type	IP Group
Name	Fax to VM Trunk B	Destination IP Group	• #3 [VM Trunk B] View
Alternative Route Options	Alternative Route Ignore Inputs	Destination SIP Interface	<b>v</b> iew
		Destination Address	
MATCH		Destination Port	0
Source IP Group	• #4 [MP-Fax]   Vie	N Destination Transport Type	T
Request Type	All	IP Group Set	<b>v</b> iew
Source Username Pattern	*	Call Setup Rules Set ID	-1
Source Host	*	Group Policy	Sequential 🔻
Source Tag		Cost Group	View
	Car	cel APPLY	

b. Click Apply.

+441183374147 (dedicated fax line)

7. Configure a rule to route calls from Virgin Media SIP Trunk A or B to the Fax /Minicom ATA Device:

an eller nem, and aler conligate the par	
Parameter	Value
Index	5
Route Name	VM to Fax (arbitrary descriptive name)
Source IP Group	Any

IP Group MP-Fax

a. Click **New**, and then configure the parameters as follows:

**Destination Username Prefix** 

**Destination Type** 

**Destination IP Group** 

#### Figure 4-40: Configuring IP-to-IP Routing Rule for VM Trunk to Fax / Minicom ATA Device

IP-to-IP Routing [VM to Fax]				– x
	Routing Policy #0	0 [Default_SBCRoutingPolicy]		
GENERAL		ACTION		
Index	5	Destination Type	IP Group	v
Name •	VM to Fax	Destination IP Group	• #4 [MP-Fax]	▼ View
Alternative Route Options	Route Row 🔻	Destination SIP Interface		▼ View
		Destination Address		
MATCH		Destination Port	0	
Source IP Group	Any 👻 View	Destination Transport Type		v
Request Type	All	<ul> <li>IP Group Set</li> </ul>		▼ View
Source Username Pattern	*	Call Setup Rules Set ID	-1	
Source Host	*	Group Policy	Sequential	•
Source Tag		Cost Group		▼ View
	Cano	APPLY		

- 8. Configure a rule to route calls from Virgin Media SIP Trunk A or B to Skype for Business Server 2015:
  - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	6
Route Name	VM to S4B (arbitrary descriptive name)
Source IP Group	Any
Destination Type	IP Group
Destination IP Group	S4B

#### Figure 4-41: Configuring IP-to-IP Routing Rule for VM to S4B

IP-to-IP	to-IP Routing [VM to S4B]x						
		Routing Policy #	#0 [Default	SBCRoutingPolicy]			
	GENERAL			ACTION			
	Index	5		Destination Type	IP Group	•	
	Name • V	/M to S4B		Destination IP Group	#1 [S4B]	View	
	Alternative Route Options	loute Row	•	Destination SIP Interface		View	
				Destination Address			
	MATCH			Destination Port	0		
	Source IP Group	Any 💌 V	iew	Destination Transport Type		•	
	Request Type	All	•	IP Group Set		View	
	Source Username Pattern	*		Call Setup Rules Set ID	-1		
	Source Host	*		Group Policy	Sequential	•	
	Source Tag			Cost Group		View	
		Ca	ncel AF	PPLY			

The configured routing rules are shown in the figure below:

Figure 4-42: Configured IP-to-II	P Routing Rules in IP-to-IP	Routing Table
----------------------------------	-----------------------------	---------------

IP-to-IF	IP-to-IP Routing (7) .										
+ New	+ New Edit Insert 🛊 🖡 💼 🛤 eq Page 1 of 1 🔛 🖬 Show 10 🗸 records per page										
INDEX 🗢	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	OPTIONS tern	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address			internal
1	S4B to VM Tru	Default_SBCR	Route Row	S4B	All	*	*	IP Group	VM Trunk A		
2	S4B to VM Tru	Default_SBCR	Alternative Rc	S4B	All	*	*	IP Group	VM Trunk B		
3	Fax to VM Tru	Default_SBCR	Route Row	MP-Fax	All	*	*	IP Group	VM Trunk A		
4	Fax to VM Tru	Default_SBCR	Alternative Rc	MP-Fax	All	*	*	IP Group	VM Trunk B		
5	VM to Fax	Default_SBCR	Route Row	Any	All	*	+4411833741	IP Group	MP-Fax		
6	VM to S4B	Default_SBCR	Route Row	Any	All	*	*	IP Group	S4B		



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

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.6 on page 46) to denote the source and destination of the call.



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

For example, for this interoperability test topology, a manipulation is configured to strip the "+" (plus sign) from the destination number for Emergency calls to the Virgin Media SIP Trunk IP Group if the plus sign exists and to not perform any action for all other emergency calls.

#### **To configure a number manipulation rule:**

- Open the Outbound Manipulations table (Setup menu > Signaling & Media tab > SBC folder > Manipulation > Outbound Manipulations).
- 2. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	To Emergency do nothing
Source IP Group	Any
Destination IP Group	Any
Destination Username Pattern	[999,112,18000]
Manipulated Item	Destination URI

und Manipulations <b>[To E</b>	mergel	ncy do nothing]					
		Routing Policy	#0 [D	efaul	t_SBCRoutingPolicy]		
GENERAL					ACTION		
Index	C				Manipulated Item	Destination URI	Ŧ
Name	• 1	o Emergency do nothing			Remove From Left	0	
Additional Manipulation	N	0	•		Remove From Right	0	
Call Trigger	A	ny	•		Leave From Right	255	
					Prefix to Add		
MATCH					Suffix to Add		
Request Type		All	•		Privacy Restriction Mode	Transparent	•
Source IP Group		Any	▼ View				
Destination IP Group		Any	<ul> <li>View</li> </ul>				
Source Username Pattern		*					
			Cancel		PPLY		

#### Figure 4-43: Configuring IP-to-IP Outbound Manipulation Rule

#### 3. Click Apply.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between Skype for Business Server 2015 IP Group and Virgin Media SIP Trunk IP Groups:

Figure 4-44	: Example of	<b>Configured IP-to-IF</b>	Outbound Manipulation Rules

+ New	Edit Insert	↑ ↓ 🗎 🖻		ia <a< th=""><th>Page 1 of 1</th><th>▶&gt; ► Show</th><th>10 🔻 records p</th><th>er page</th><th></th><th></th><th></th><th></th><th>Q</th></a<>	Page 1 of 1	▶> ► Show	10 🔻 records p	er page					Q
INDEX 🗢	NAME	ROUTING POLICY	ADDITIONAL MANIPULATI(		DESTINATION IP GROUP	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	MANIPULATE ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX T ADD
0	To Emergency	Default_SBCR	No	Any	Any	*	[999,112,1800	Destination U	0	0	255		
1	To Emergency	Default_SBCR	No	Any	Any	*	[+999,+112,+1	Destination U	1	0	255		
2	Do nothing	Default_SBCR	No	Any	Any	*	+	Destination U	0	0	255		
3	Add + toward	Default_SBCR	No	Any	Any	*	*	Destination U	0	0	255	+	

Rule Index	Description
0	Calls from any (S4B or MP Fax) IP Group with destination number 999 or 112 or 18000, do not perform any action for the destination number.
1	Calls from any (S4B or MP Fax) IP Group with destination number +999 or +112 or +18000. Remove "+" from this numbers.
2	Calls from any (S4B or MP Fax) IP Group with the prefix destination number "+", do not perform any action for the destination number.
3	Calls from any (S4B or MP Fax) IP Group with any destination number (*), add "+" prefix to the destination number.

## 4.13 Step 13: Configure Message Manipulation Rules

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

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

- > To configure SIP message manipulation rule:
- 1. Open the Message Manipulations page (Setup menu > Signaling & Media tab > Message Manipulation folder > Message Manipulations).
- 2. Configure a new manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule applies to response messages sent to Virgin Media SIP Trunk A or B and consist method type '410 Gone'. This replaces the method type '410' with the value '480', according to Virgin Media request.

Parameter	Value
Index	0
Name	Change Failure Response 410 to 480
Manipulation Set ID	4
Message Type	any.response
Condition	header.request-uri.methodtype=='410'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'480'

Message	Manipulations [Change F	ailure Response 410 to 480]			- x
	GENERAL		ACTION		
1		0 Change Failure Response 410 to 480 ● 4 Use Current Condition ▼	Action Subject • Action Type • Action Value •	Modify V	
	MATCH				
		any.response header.request-uri.methodtype=='410'			
		Cancel	APPLY		

3. Configure another manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule is applied on SIP INVITE request messages sent to the Virgin Media SIP Trunk IP Group. This add OPTIONS method to the SIP Allow header.

Parameter	Value
Index	1
Name	Add Options to Allow Header
Manipulation Set ID	4
Message Type	invite.request
Condition	header.allow regex (.*)
Action Subject	header.allow regex
Action Type	Modify
Action Value	\$1+',OPTIONS'

#### Figure 4-46: Configuring SIP Message Manipulation Rule 1 (for Virgin Media SIP Trunk)

Messag	e Manipulations [Add Optio	ns to Allow Header]			– ×
	GENERAL		ACTION		
	Index	1	Action Subject	header.allow	Editor
	Name	Add Options to Allow Header	Action Type	Modify	*
	Manipulation Set ID	• 4	Action Value	\$1+',OPTIONS'	Editor
	Row Role	Use Current Condition			
	MATCH				
	Message Type	invite.request     Editor			
	Condition	header.allow regex (.*)     Editor			
		Cancel	APPLY		

4. Configure another manipulation rule (Manipulation Set 10) for Virgin Media SIP Trunk. This rule is applied on SIP OPTIONS messages sent to the Virgin Media SIP Trunk IP Group. This replaces the host part of the SIP Request-Uri header with the destination address.

Parameter	Value
Index	2
Name	Change Dest in R-URI
Manipulation Set ID	10
Message Type	Options
Action Subject	Header.Request-URI.URL.Host
Action Type	Modify
Action Value	Param.Message.Address.Dst.Address

#### Figure 4-47: Configuring SIP Message Manipulation Rule 2 (for Virgin Media SIP Trunk)

Message Manipulations [Chan	- x					
GENERAL		ACTION				
Index	2	Action Subject	Header.Request-URI.URL.Host	Editor		
Name	Change Dest in R-URI	Action Type	Modify	•		
Manipulation Set ID	• 10	Action Value	Param.Message.Address.Dst.Address	Editor		
Row Role MATCH	Use Current Condition	•				
Message Type	Options	Editor				
Condition		Editor				
		Cancel APPLY				

5. Configure another manipulation rule (Manipulation Set 10) for Virgin Media SIP Trunk. This rule is applied on SIP OPTIONS messages sent to the Virgin Media SIP Trunk IP Group. This replaces the host part of the SIP To header with the destination address.

Parameter	Value
Index	3
Name	Change Dest in To
Manipulation Set ID	10
Message Type	Options
Action Subject	Header.To.URL.Host
Action Type	Modify
Action Value	Param.Message.Address.Dst.Address

### Figure 4-48: Configuring SIP Message Manipulation Rule 3 (for Virgin Media SIP Trunk)

Messag	e Manipulations [Change	Dest in To]			– ×
	GENERAL		ACTION		
	Index	3	Action Subject	Header.To.URL.Host	Editor
	Name	Change Dest in To	Action Type	Modify	•
	Manipulation Set ID	• 10	Action Value	Param.Message.Address.Dst.Address	Editor
	Row Role	Use Current Condition 🔹			
	MATCH				
	Message Type	Options     Editor			
	Condition	Editor			
		Cancel	APPLY		

6. Configure another manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule is applied on all SIP request messages with SIP P-Asserted-Identity header, sent to the Virgin Media SIP Trunk IP Group. This replaces the user part of the SIP P-Asserted-Identity header with the pre-defined 'pilot' number.



**Note:** Adapt the pre-defined 'pilot' number according to your environment dial plan.

Parameter	Value
Index	4
Name	For test 27
Manipulation Set ID	4
Message Type	Any.Request
Condition	Header.P-Asserted-Identity exists
Action Subject	Header.P-Asserted-Identity.URL.User
Action Type	Modify
Action Value	'+441183374142'

#### Figure 4-49: Configuring SIP Message Manipulation Rule 4 (for Virgin Media SIP Trunk)

Message Manipulations [Fo	r test 27]			– ×
GENERAL		ACTION		
Index Name Manipulation Set ID Row Role	4 • For test 27 • 14 Use Current Condition ▼	Action Subject Action Type Action Value	<ul> <li>Header:P-Asserted-Identity.URL.User</li> <li>Modify</li> <li>'+441183374142'</li> </ul>	Editor  Editor Editor
МАТСН				
Message Type Condition	Any.Request     Editor     Header.P-Asserted-Identity exists     Editor			
	Cancel	APPLY		

Message	Manipulation	s (5) .						
+ New E	dit Insert 🛧	<b>↓   亩 →</b>	🛛 🔜 🛛 Page 🔟 d	of1   🏎 💌 Show	10 🔻 records p	er page		Q
INDEX 🗢	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Change Failure F	4	any.response	header.request-	header.request-	Modify	'480'	Use Current Cor
1	Add Options to A	4	invite.request	header.allow reg	header.allow	Modify	\$1+',OPTIONS'	Use Current Cor
2	Change Dest in F	10	Options		Header.Request	Modify	Param.Message.	Use Current Cor
3	Change Dest in 1	10	Options		Header.To.URL.H	Modify	Param.Message.	Use Current Cor
4	For test 27	14	Any.Request	Header.P-Assert	Header.P-Assert	Modify	'+441183374142	Use Current Cor

#### Figure 4-50: Example of Configured SIP Message Manipulation Rules

The table below includes a SIP message manipulation rule which is executed for messages sent to Virgin Media SIP Trunk IP Groups. This rule is specifically required to enable proper interworking between Virgin Media SIP Trunk and Skype for Business Server 2015. Refer to the *User's Manual* for further details regarding the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule		
0	This rule applies to response messages sent to Virgin Media SIP Trunk A or B and consist method type '410 Gone'. This replaces the method type '410' with the value '480', according to the Virgin Media request.	Virgin Media request to change '410' method type to '480'.		
1	This rule is applied on SIP INVITE request messages sent to the Virgin Media SIP Trunk IP Group. This adds the OPTIONS method to the SIP Allow header.	According to Virgin Media request, SIP Allow Header of Invite messages should contain OPTIONS method.		
2	This rule is applied on SIP OPTIONS messages sent to the Virgin Media SIP Trunk IP Group. This replaces the host part of the SIP Request-Uri header with the destination address.	Virgin Media request that SIP OPTIONS messages from the SBC sent with destination address of appropriated trunk (Trunk A or Trunk B) in the Request-Uri and To headers.		
3	This rule is applied on SIP OPTIONS messages sent to the Virgin Media SIP Trunk IP Group. This replaces the host part of the SIP To header with the destination address.			
4	This rule is applied on all SIP request messages with SIP P-Asserted-Identity header, sent to the Virgin Media SIP Trunk IP Group. This replaces the user part of the SIP P-Asserted-Identity header with the pre-defined 'pilot' number.	According to Virgin Media request, the customer should have the ability to configure a pre- defined number which will be displayed as CLI instead of a real caller number.		

- 7. Assign Manipulation Set ID 4 to the Virgin Media SIP trunk IP Group:
  - a. Open the IP Groups table (Setup menu > Signaling & Media tab > Core Entities folder > IP Groups).
  - **b.** Select the row of Virgin Media SIP trunk IP Group, and then click **Edit**.
  - c. Set the 'Outbound Message Manipulation Set' field to 4.

#### Figure 4-51: Assigning Manipulation Set 4 to the Virgin Media SIP Trunk IP Group

IP Grou	ups [SP]		-	x
		SRD #0 [DefaultSRD]	•	*
	GENERAL		QUALITY OF EXPERIENCE	E
	Index	1	QoE Profile View	
	Name	• SP	Bandwidth Profile View	
	Topology Location	• Up		
	Туре	Server 💌	MESSAGE MANIPULATION	
	Proxy Set	• #1 [SP]	Inbound Message Manipulation Set -1	
	IP Profile	• #2 [SP] View	Outbound Message Manipulation Set • 4	
	Media Realm	• #1 [MRWan]	Message Manipulation User-Defined String 1	
	SIP Group Name		Message Manipulation User-Defined String 2	
	Created By Routing Server	No		
	Used By Routing Server	Not Used 💌	SBC REGISTRATION AND AUTHENTICATION	-
		Cance	APPLY	

## 4.14 Step 14: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the Virgin Media SIP Trunk on behalf of Skype for Business Server 2015. The Virgin Media SIP Trunk requires registration and authentication to provide service. In the interoperability test topology, the Served IP Group is Skype for Business Server 2015 IP Group and the Serving IP Group is Virgin Media SIP Trunk IP Group.

#### > To configure a registration account:

- Open the Accounts table (Setup menu > Signaling & Media tab > SIP Definitions folder > Accounts).
- 2. Click New.
- **3.** Configure the account according to the provided information from Virgin Media, for S4B, serving by VM Trunk A:

Parameter	Value
Served IP Group	S4B
Application Type	SBC
Serving IP Group	VM Trunk A
Register	Νο
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

#### 4. Click Apply.

5. Repeat for S4B, serving by Virgin Media Trunk B:

Parameter	Value
Served IP Group	S4B
Application Type	SBC
Serving IP Group	VM Trunk B
Register	Νο
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

- 6. Click Apply.
- 7. Repeat the same for Fax / Minicom ATA Device, serving by VM Trunk A:

Parameter	Value
Served IP Group	MP-Fax
Application Type	SBC
Serving IP Group	VM Trunk A
Register	Νο
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

- 8. Click Apply.
- 9. Repeat the same for Fax / Minicom ATA Device, serving by VM Trunk B:

Parameter	Value
Served IP Group	MP-Fax
Application Type	SBC
Serving IP Group	VM Trunk B
Register	No
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-52	Configuring a S	SIP Registration	Account
i iguie 4-52	. Configuring a C	nr negisilation	Account

+ New	Edit 🗍 💼 Action	n	🛯 🔜 Pag	e 1 of 1 🕨 🕨	Show 10 🔻 reco	rds per page			Q
INDEX ≑	APPLICATION TYPE	SERVED TRUNK GROUP	SERVED IP GROUP	SERVING IP GROUP	USER NAME	PASSWORD	HOST NAME	REGISTER	CONTACT USE
0	SBC	-1	S4B	VM Trunk A	virginpbx01_011	*		No	
1	SBC	-1	S4B	VM Trunk B	virginpbx01_011	*		No	
2	SBC	-1	MP-Fax	VM Trunk A	virginpbx01_011	*		No	
3	SBC	-1	MP-Fax	VM Trunk B	virginpbx01_011	*		No	

### 4.15 **Step 15: Miscellaneous Configuration**

This section describes miscellaneous E-SBC configuration.

### 4.15.1 Step 15a: 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 ringback tone if a 180 response without SDP is received. It is mandatory to set this field for the Skype for Business Server 2015 environment.

#### **To configure call forking:**

- 1. Open the SBC General Settings page (Setup menu > Signaling & Media tab > SBC folder > SBC General Settings).
- 2. From the 'SBC Forking Handling Mode' drop-down list, select Sequential.

#### Figure 4-53: Configuring Forking Mode

	SBC General Settings	
	GENERAL	
	Direct Media	Disable 💌
	Unclassified Calls	Reject 💌
→	Forking Handling Mode	Sequential 💌
	No Answer Timeout [sec]	600
	BroadWorks Survivability Feature	Disable 💌
	Max Forwards Limit	10
	Max Call Duration [min]	0

### 4.15.2 Step 15b: Configure SBC Alternative Routing Reasons

This step describes how to configure the E-SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case E-SBC attempts to locate an alternative route for the call.

#### > To configure SIP reason codes for alternative IP routing:

- Open the Alternative Routing Reasons table (Setup menu > Signaling & Media tab > SBC folder > Routing > Alternative Reasons).
- 2. Click New.
- 3. From the 'Release Cause' drop-down list, select **503 Service Unavailable**.

	Figure 4-54: SBC	Alternative	Routing	Reasons	Table
--	------------------	-------------	---------	---------	-------

Alternative Routing Reasons	– x
GENERAL	*
Index 0 Release Cause • 503 Service Unavailable •	-
Cancel APPLY	

### 4.15.3 Step 15c: Configure SBC Max Retransmission Time

This step describes how to configure the E-SBC's maximum retransmission attempts. In this case, E-SBC attempts to locate an alternative route for the call after three attempts.

- > To configure SIP SBC Max Retransmission Time:
- 1. Open the Transport Settings (Setup menu > Signaling & Media tab > SIP Definitions folder > Transport Settings).
- 2. Click New.
- 3. In the 'SIP Maximum RTX' field, enter 3 (retransmission will be stopped after 3 attempts).

Transport Settings					
GENERAL			TCP CONNECTION		
SIP NAT Detection	Enable •	,	TCP/TLS Connection Reuse	Enable	•
Enable SIPS	Disable •		TCP Timeout	0	
SIP Transport Type	UDP •		Reliable Connection Persistent Mode	Disable	•
ENUM Resolution	e164.arpa				
SIP 408 Response upon non-INVITE	Enable 🔻		RETRANSMISSION		
DNS Query Type	A-Record •		SIP T1 Retransmission Timer [msec]	500	
			SIP T2 Retransmission Timer [msec]	4000	
SBC SETTINGS	-		SIP Maximum RTX	3	
WebSocket Keep-Alive Period [sec]	0				

#### Figure 4-55: SBC Max Retransmission Time

### 4.15.4 Step 15d: Configure Broken Connection Behavior

This step describes how to configure the E-SBC to ignore broken connection. This is needed for proper behavior during fax transmission.

- > To configure SIP Broken Connection Behavior:
- Open the SIP Definitions General Settings (Setup menu > Signaling & Media tab > SIP Definitions folder > SIP Definitions General Settings).
- 2. Click New.
- 3. From the 'Broken Connection Mode' drop-down list, select **Ignore**.

SIP Definitions General Settings				
GENERAL			SBC SETTINGS	
Send Reject (503) upon Overload	Enable	•	Enable Subscribe Trying	Disable •
Retry-After Time	0		Minimum Session-Expires [sec]	90
Fake Retry After	0		Session-Expires [sec]	180
X-Channel Header	Disable	•		
			GATEWAY SESSION EXPIRES	
GATEWAY SETTINGS			Session-Expires Time	0
PRACK Mode	Supported	•	Minimum Session-Expires	90
Early 183	Disable	•	Session Expires Method	re-INVITE •
183 Message Behavlor	Progress	•	Session Expires Disconnect Time	32
3xx Behavior	Forward	•		
Call Transfer using re-INVITEs	Disable	•	DISCONNECT SUPERVISION	
First Call Ringback Tone ID	-1	$\rightarrow$	<ul> <li>Broken Connection Mode</li> </ul>	• Ignore •
Enable Delayed Offer	Disable	•	Broken Connection Timeout [100 msec]	100
Source Header For Called Number	use RequestURI header	•		
Verify Received VIA	Disable	•		
Reject Cancel after Connect	Disable	•		
	c	ancel AF	PPLY	

#### Figure 4-56: SBC Broken Connection Behavior

### 4.15.5 Step 15e: Configuration Needed for Manipulating SIP OPTIONS

This step describes how to configure the E-SBC's string name in SIP OPTIONS Keep-alive messages (host part of the Request-URI and To SIP headers).

#### To configure the Gateway Outbound Manipulation Set:

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

#### Figure 4-57: Configuring GW Outbound Manipulation Set via AdminPage

Image Lc <del>ad</del> to Device <i>ini</i> Parameters Back to	Parameter Name: GWOUTBOUNDMANIPULATIONSET	eutput Window	Apply New Value
Main	Parameter Name: GWOUTBOUNDMANI Parameter New Value: 10 Parameter Description:Outbound applies for all outgoing INVIT	manipulation set ID for GW - If c	onfigured,

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

Parameter	Value
GWOUTBOUNDMANIPULATIONSET	10

- 5. Click the Apply New Value button for each field.
- 6. Click on **Back to Main**. On the main page don't forget to save the configuration.

## 4.16 Step 16: Reset the E-SBC

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

- > To reset the device through Web interface:
- 1. Open the Maintenance Actions page (Setup menu > Administration tab > Maintenance folder > Maintenance Actions).

Figure 4-58: Resetting the E-SBC

Maintenance Actions	
RESET DEVICE	
Reset Device	Reset
Save To Flash	Yes
Graceful Option	No

- 2. Ensure that the ' Save To Flash' field is set to Yes (default).
- 3. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
- 4. Click **OK** to confirm device reset.

This page is intentionally left blank.

# A AudioCodes INI File

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



**Note:** To load or save an *ini* file, use the Configuration File page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**).

```
; * * * * * * * * * * * * * *
;** Ini File **
; * * * * * * * * * * * * * *
[SYSTEM Params]
SyslogServerIP = 10.10.10.10
EnableSyslog = 1
NTPServerUTCOffset = 10800
NTPServerIP = '10.15.27.1'
[BSP Params]
PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
[Analog Params]
[ControlProtocols Params]
AdminStateLockControl = 0
[Voice Engine Params]
BrokenConnectionEventTimeout = 1000
ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'
[WEB Params]
UseProductName = 1
FaviconCurrentVersion = 2
[SIP Params]
MEDIACHANNELS = 100
GWDEBUGLEVEL = 5
SIPMAXRTX = 3
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
GWOUTBOUNDMANIPULATIONSET = 10
```

```
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
[IPsec Params]
[SNMP Params]
[ DeviceTable ]
FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;
[ \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, 10.15.77.10, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.154, 25, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "vlan 2";
[ \InterfaceTable ]
[ WebUsers ]
FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_CliSessionLimit, WebUsers_SessionTimeout, WebUsers_BlockTime,
WebUsers_UserLevel, WebUsers_PwNonce, WebUsers_SSHPublicKey;
WebUsers 0 = "Admin",
"$1$bgtdFkgQREJNFRNJHUhDGRtPTuPju+bhteC1ubG4vby9t7fy9fbloqfyoKmt+KP5/qz9m
ZSTlpyUkpDNzMudz54=", 1, 0, 5, -1, 15, 60, 200,
"e4064f90b5b26631d46fbcdb79f2b7a0", ".fc";
WebUsers 1 = "User",
"$1$Cj46OmhtN3ElJiolcSQnfXh4Ii5+Jn4ZRBQRHR0fHx4bTB9ITE8aVqRQVQUGAAEPXVkCD
w0GWSEgIHN0dHB2LHE=", 1, 0, 5, -1, 15, 60, 50,
"c26a27dd91a886b99de5e81b9a736232", "";
[ \WebUsers ]
[ TLSContexts ]
FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert,
```

```
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "default", 7, 0, "RC4:EXP", "ALL:!ADH", 0, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;
[ \TLSContexts ]
[ AudioCodersGroups ]
FORMAT AudioCodersGroups Index = AudioCodersGroups Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";
[ \AudioCodersGroups ]
[ AllowedAudioCodersGroups ]
FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "VM";
[ \AllowedAudioCodersGroups ]
[ IpProfile ]
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,
IpProfile_RTPRedundancyDepth, 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_SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionMode,
IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling,
IpProfile_SBCFaxCodersGroupName, 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\_SBCAdaptRFC2833BWToVoiceCoderBW, IpProfile\_CreatedByRoutingServer, IpProfile\_SBCFaxReroutingMode, IpProfile\_SBCMaxCallDuration, IpProfile\_SBCGenerateRTP, IpProfile\_SBCISUPBodyHandling, IpProfile\_SBCISUPVariant, IpProfile\_SBCVoiceQualityEnhancement, IpProfile\_SBCMaxOpusBW, IpProfile\_SBCEnhancedPlc, IpProfile\_LocalRingbackTone, IpProfile\_LocalHeldTone, IpProfile\_SBCGenerateNoOp; IpProfile 1 = "S4B", 1, "AudioCodersGroups\_0", 0, 10, 10, 46, 24, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "audio", "", "", 0, 1, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 0, 1, 0, 3, 2, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0; IpProfile 2 = "VM", 1, "AudioCodersGroups\_0", 0, 10, 10, 46, 24, 0, 0, 2,  $0, \ 0, \ 0, \ 0, \ -1, \ 1, \ 0, \ 0, \ -1, \ 1, \ 1, \ 4, \ -1, \ 1, \ 1, \ 0, \ 0, \ "", \ "", \ 0, \ 0, \ "",$ "VM", "", 0, 2, 0, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0,  $0,\ 2,\ 1,\ 3,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 0,\ 1,$ [ \IpProfile ] [ CpMediaRealm ] FORMAT CpMediaRealm\_Index = CpMediaRealm\_MediaRealmName, CpMediaRealm\_IPv4IF, CpMediaRealm\_IPv6IF, CpMediaRealm\_RemoteIPv4IF, CpMediaRealm\_RemoteIPv6IF, CpMediaRealm\_PortRangeStart, CpMediaRealm\_MediaSessionLeg, CpMediaRealm\_PortRangeEnd, CpMediaRealm\_IsDefault, CpMediaRealm\_QoeProfile, CpMediaRealm\_BWProfile, CpMediaRealm\_TopologyLocation; CpMediaRealm 0 = "MRLan", "LAN\_IF", "", "", "", 6000, 100, 6999, 0, "", "", 0; CpMediaRealm 1 = "MRWan", "WAN\_IF", "", "", "", 7000, 100, 7999, 0, "", ", 1; [ \CpMediaRealm ] [ SBCRoutingPolicy ] FORMAT SBCRoutingPolicy\_Index = SBCRoutingPolicy\_Name, SBCRoutingPolicy\_LCREnable, SBCRoutingPolicy\_LCRAverageCallLength,

```
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";
[ \SBCRoutingPolicy ]
[ SRD ]
FORMAT SRD_Index = SRD_Name, SRD_BlockUnReqUsers, SRD_MaxNumOfReqUsers,
SRD EnableUnAuthenticatedRegistrations, SRD SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName, SRD_AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "",
"";
[\SRD]
[ MessagePolicy ]
FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;
[ \MessagePolicy ]
[ SIPInterface ]
FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_AdditionalUDPPorts, SIPInterface_SRDName,
SIPInterface_MessagePolicyName, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
{\tt SIPInterface\_PreClassificationManSet, \ {\tt SIPInterface\_EncapsulatingProtocol, } }
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation,
SIPInterface_PreParsingManSetName, SIPInterface_AdmissionProfile;
SIPInterface 0 = "S4B", "LAN_IF", 2, 5060, 0, 5067, "", "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0, 0, "", "";
SIPInterface 1 = "VM", "WAN_IF", 2, 5060, 0, 0, "", "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1, 0, 1, "", "";
[ \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\_GWIPv6SIPInterfaceName, ProxySet\_SBCIPv6SIPInterfaceName, ProxySet\_MinActiveServersLB, ProxySet SuccessDetectionRetries, ProxySet SuccessDetectionInterval, ProxySet\_FailureDetectionRetransmissions; ProxySet 0 = "ProxySet\_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "", "S4B", "", "", 1, 1, 10, -1; ProxySet 1 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "", 1, -1, "", "", "S4B", "", "", 1, 1, 10, -1; ProxySet 2 = "VM Trunk A", 1, 30, 0, 0, "DefaultSRD", 0, "", -1, -1, "503", "", "VM", "", "", 1, 1, 10, -1; ProxySet 3 = "VM Trunk B", 1, 30, 0, 0, "DefaultSRD", 0, "", -1, -1, "503", "", "VM", "", "", 1, 1, 10, -1; ProxySet 4 = "MP-Fax", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "", "S4B", "", "", 1, 1, 10, -1; [ \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\_EnableSBCClientForking, IPGroup\_SourceUriInput, IPGroup\_DestUriInput, IPGroup\_ContactName, IPGroup\_Username, IPGroup\_Password, IPGroup\_UUIFormat, IPGroup\_QOEProfile, IPGroup\_BWProfile, IPGroup\_AlwaysUseSourceAddr, IPGroup\_MsgManUserDef1, IPGroup\_MsgManUserDef2, IPGroup\_SIPConnect, IPGroup\_SBCPSAPMode, IPGroup\_DTLSContext, IPGroup\_CreatedByRoutingServer, IPGroup\_UsedByRoutingServer, IPGroup\_SBCOperationMode, IPGroup SBCRouteUsingRequestURIPort, IPGroup SBCKeepOriginalCallID, IPGroup\_TopologyLocation, IPGroup\_SBCDialPlanName, IPGroup\_CallSetupRulesSetId, IPGroup\_Tags, IPGroup\_SBCUserStickiness, IPGroup\_UserUDPPortAssignment, IPGroup\_AdmissionProfile; IPGroup 0 = 0, "Default\_IPG", "", "", "", -1, 0, "DefaultSRD", "", 0, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "Admin", "\$1\$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, ""; IPGroup 1 = 0, "S4B", "S4B", "213.106.222.186", "", -1, 0, "DefaultSRD", "MRLan", 1, "S4B", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "Admin", "\$1\$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, ""; IPGroup 2 = 0, "VM Trunk A", "VM Trunk A", "213.106.222.186", "", -1, 0, "DefaultSRD", "MRWan", 1, "VM", -1, -1, 4, 0, 0, "", 0, -1, -1, "", "Admin", "\$1\$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, ""; IPGroup 3 = 0, "VM Trunk B", "VM Trunk B", "82.14.171.234", "", -1, 0, "DefaultSRD", "MRWan", 1, "VM", -1, -1, 4, 0, 0, "", 0, -1, -1, "", "Admin", "\$1\$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, ""; IPGroup 4 = 0, "MP-Fax", "MP-Fax", "213.106.222.186", "", -1, 0, "DefaultSRD", "", 1, "", -1, -1, 0, 0, "", 0, -1, -1, "", "Admin", "\$1\$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, ""; [ \IPGroup ]

[ SBCAlternativeRoutingReasons ]

```
FORMAT SBCAlternativeRoutingReasons Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;
[ \SBCAlternativeRoutingReasons ]
[ ProxyIp ]
FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "1", 0, "FE.S4B.interop:5067", 2;
ProxyIp 1 = "2", 0, "213.106.222.186:5060", 0;
ProxyIp 2 = "3", 0, "82.14.171.234:5060", 0;
ProxyIp 3 = "4", 0, "10.15.77.12:5060", 0;
[ \ProxyIp ]
[ Account ]
FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_ContactUser,
Account_Register, Account_RegistrarStickiness,
Account_RegistrarSearchMode, Account_RegEventPackageSubscription,
Account_ApplicationType, Account_RegByServedIPG,
Account_UDPPortAssignment;
Account 0 = -1, "S4B", "VM Trunk A", "virginpbx01_01183374140",
"$1$WWsfbG0bGmtTJCEmIiFeUSssK18q", "", "", 0, 0, 0, 0, 2, 0, 0;
Account 1 = -1, "S4B", "VM Trunk B", "virginpbx01_01183374140",
"$1$WWsfbG0bGmtTJCEmIiFeUSssK18q", "", "", 0, 0, 0, 0, 2, 0, 0;
Account 2 = -1, "MP-Fax", "VM Trunk A", "virginpbx01_01183374140",
"$1$WWsfbG0bGmtTJCEmIiFeUSssK18q", "", "", 0, 0, 0, 0, 2, 0, 0;
Account 3 = -1, "MP-Fax", "VM Trunk B", "virginpbx01_01183374140",
"$1$WWsfbG0bGmtTJCEmIiFeUSssK18q", "", "", 0, 0, 0, 0, 2, 0, 0;
[ \Account ]
[ 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_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName,
IP2IPRouting_RoutingTagName, IP2IPRouting_InternalAction;
IP2IPRouting 0 = "OPTIONS termination", "Default_SBCRoutingPolicy",
"Any", "*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0, 0, "", "", "", ", "default", "";
```

IP2IPRouting 1 = "S4B to VM Trunk A", "Default\_SBCRoutingPolicy", "S4B", "\*", "\*", "\*", "\*", 0, "", "Any", 0, -1, 0, "VM Trunk A", "", "", 0, -1, 0, 0, "", "", "", ", "", 0, -1, 0, 0, "", "", "", ", "default", ""; IP2IPRouting 2 = "S4B to VM Trunk B", "Default\_SBCRoutingPolicy", "S4B", "\*", "\*", "\*", "\*", 0, "", "Any", 0, -1, 0, "VM Trunk B", "", "", 0, -1, 1, 0, "", "", "", "default", ""; IP2IPRouting 3 = "Fax to VM Trunk A", "Default\_SBCRoutingPolicy", "MP-Fax", "\*", "\*", "\*", "\*", 0, "", "Any", 0, -1, 0, "VM Trunk A", "", "", 0, -1, 0, 0, "", "", "", "", "default", ""; IP2IPRouting 4 = "Fax to VM Trunk B", "Default\_SBCRoutingPolicy", "MP-Fax", "\*", "\*", "\*", "\*", 0, "", "Any", 0, -1, 0, "VM Trunk B", "", "", 0, -1, 1, 0, "", "", "", "default", ""; IP2IPRouting 5 = "VM to Fax", "Default\_SBCRoutingPolicy", "Any", "\*",
"\*", "+441183374147", "\*", 0, "", "Any", 0, -1, 0, "MP-Fax", "", "", 0, 1, 0, 0, "", "", "", "", "default", ""; IP2IPRouting 6 = "VM to S4B", "Default\_SBCRoutingPolicy", "Any", "\*", "\*", "\*", "\*", 0, "", "Any", 0, -1, 0, "S4B", "", "", 0, -1, 0, 0, "", "", "", "", "default", ""; [ \IP2IPRouting ] [ 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\_DestTags, IPOutboundManipulation\_SrcTags; IPOutboundManipulation 0 = "To Emergency do nothing", "Default\_SBCRoutingPolicy", 0, "Any", "Any", "\*", "\*", "[999,112,18000]", "\*", "\*", "", 0, "Any", 0, 1, 0, 0, 255, "", "", 0, "", ""; IPOutboundManipulation 1 = "To Emergency strip +" "Default\_SBCRoutingPolicy", 0, "Any", "Any", "\*", "\*", "[+999,+112,+18000]", "\*", "\*", "", 0, "Any", 0, 1, 1, 0, 255, "", "", 0, "", ""; IPOutboundManipulation 2 = "Do nothing", "Default\_SBCRoutingPolicy", 0, "Any", "Any", "\*", "\*", "+", "\*", "\*", ", 0, "Any", 0, 1, 0, 0, 255, "", "", 0, "", ""; IPOutboundManipulation 3 = "Add + toward VM", "Default\_SBCRoutingPolicy", 0, "Any", "Any", "\*", "\*", "\*", "\*", "\*", ", 0, "Any", 0, 1, 0, 0, 255, "+", "", 0, "", "", 0, ", ""; [ \IPOutboundManipulation ] [ MessageManipulations ]

```
FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change Failure Response 410 to 480", 4,
"any.response", "header.request-uri.methodtype=='410'", "header.request-
uri.methodtype", 2, "'480'", 0;
MessageManipulations 1 = "Add Options to Allow Header", 4,
"invite.request", "header.allow regex (.*)", "header.allow", 2,
"$1+',OPTIONS'", 0;
MessageManipulations 2 = "Change Dest in R-URI", 10, "Options", "",
"Header.Request-URI.URL.Host", 2, "Param.Message.Address.Dst.Address", 0;
MessageManipulations 3 = "Change Dest in To", 10, "Options", "",
"Header.To.URL.Host", 2, "Param.Message.Address.Dst.Address", 0;
MessageManipulations 4 = "For test 27", 14, "Any.Request", "Header.P-
Asserted-Identity exists", "Header.P-Asserted-Identity.URL.User", 2,
"'+441183374142'", 0;
[ \MessageManipulations ]
[ GwRoutingPolicy ]
FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";
[ \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 ]
[ MaliciousSignatureDB ]
FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'"
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
```

## **C**audiocodes

```
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";
[ \MaliciousSignatureDB ]
[ AllowedAudioCoders ]
FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 0 = "VM", 0, 1, "";
[ \AllowedAudioCoders ]
[ AudioCoders ]
FORMAT AudioCoders Index = AudioCoders AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
[ \AudioCoders ]
```

# B Configuring Analog Devices (ATAs) for Fax Support

This section describes how to configure the analog device entity to route its calls to the AudioCodes Media Gateway for supporting faxes or Minicoms. The analog device entity must be configured to send all calls to the AudioCodes SBC.



**Note:** The configuration described in this section is for ATA devices configured for AudioCodes MP-11x series.

## **B.1** Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints) by defining telephone numbers. The configuration below uses the example of ATA destination phone number "+441183374143" (IP address 10.15.17.12) with all routing directed to the SBC device (10.15.17.10).

> To configure the Endpoint Phone Number table:

 Open the Endpoint Phone Number Table page (Configuration tab > VolP menu > GW and IP to IP submenu > Hunt Group sub-menu > Endpoint Phone Number).

E	ndpoin	nt Phone Number Table				_
		Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID	
	1	1	+441183374143		0	
	2					
	3					

#### Figure B-1: Endpoint Phone Number Table Page

## **B.2** Step 2: Configure Tel to IP Routing Table

This step describes how to configure the Tel-to-IP routing rules to ensure that the MP-11x device sends all calls to the AudioCodes central E-SBC device.

#### > To configure the Tel to IP Routing table:

1. Open the Tel to IP Routing page (Configuration tab > VoIP menu > GW and IP to IP sub-menu > Routing sub-menu > Tel to IP Routing).

#### Figure B-2: Tel to IP Routing Page

		_						A	dvanced Par	ameter Lis
		Deutine I	ndau		1-10 ▼			-		
		Routing Ir						1		
		Tel To IP F	Routing Mode		Route calls before mani	ipulation 🔻		_		
Src. Hunt	Doct Bhon	Drofiv	Course Dhone Drefix	-	Doct ID Address	Dort	Transport Type	Dest. IP Group	IP Profile	Cost
Src. Hunt Group ID	Dest. Phon	e Prefix	Source Phone Prefix	>	Dest. IP Address	Port	Transport Type	Dest. IP Group ID		Cost Group II
	Dest. Phon	e Prefix	Source Phone Prefix	>	Dest. IP Address	Port 5060				

### **B.3** Step 3: Configure Coders Table

This step describes how to configure the coders for the MP-11x device.

- **To configure MP-11x coders:**
- 1. Open the Coders page (Configuration tab > VoIP menu > Coders And Profiles sub-menu > Coders).

#### Figure B-3: Coders Table Page

Cod	lers Table					
	Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	
	G.711A-law	20 🔻	64 🔻	8	Disabled V	
	G.711U-law	20 🔻	64 🔻	0	Disabled <b>v</b>	
	<b>T</b>	<b>T</b>	<b></b>		<b>T</b>	

### B.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

This step describes how to configure the fax signaling method for the MP-11x device.

- > To configure the fax signaling method:
- Open the SIP General Parameters page (Configuration tab > VoIP menu > SIP Definitions submenu > General Parameters).

		Basic Parameter
		<b>^</b>
🗲 NAT IP Address	0.0.0.0	
PRACK Mode	Supported T	
Channel Select Mode	By Dest Phone Number	
Enable Early Media	Disable 🔻	
183 Message Behavior	Progress V	
Session-Expires Time	0	
Minimum Session-Expires	90	
Session Expires Method	re-INVITE T	
Asserted Identity Mode	Disabled <b>v</b>	
Fax Signaling Method 2 -	T.38 Relay	
Detect Fax on Answer Tone	Initiate T.38 on Preamble	
SIP Transport Type 3		
SIP UDP Local Port 4	→ 5060	
SIP TCP Local Port	5060	
SIP TLS Local Port	5061	
Enable SIPS	Disable <b>v</b>	
Enable TCP Connection Reuse	Enable <b>v</b>	
TCP Timeout	0	

#### Figure B-4: SIP General Parameters Page

- 2. From the 'FAX Signaling Method' drop-down list, select **G.711 Transport** for G.711 fax support and select **T.38 Relay** for T.38 fax support.
- 3. From the 'SIP Transport Type' drop-down list, select **UDP**.
- **4.** In the 'SIP UDP Local Port' field, enter **5060** (corresponding to the Central Gateway UDP transmitting port configuration).
- 5. In the 'SIP Destination Port', enter **5060** (corresponding to the Central Gateway UDP listening port configuration).

#### **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: <u>https://www.audiocodes.com/corporate/offices-worldwide</u> Website: <u>https://www.audiocodes.com/</u>

©2018 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond 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.

Document #: LTRT-39343



