AudioCodes Professional Services – Interoperability Lab

# Mediant<sup>™</sup> E-SBC for BroadCloud SIP Trunk with Microsoft<sup>®</sup> Skype for Business Server 2015

Version 7.2





Gold Communications





## **Table of Contents**

1	Intro	duction	7
	1.1	Intended Audience	7
	1.2	About AudioCodes E-SBC Product Series	
2	Com	ponent Information	9
	2.1	AudioCodes E-SBC Version	
	2.2	BroadCloud SIP Trunking Version	
	2.3	Microsoft Skype for Business Server 2015 Version	
	2.4	Interoperability Test Topology	
		2.4.1 Environment Setup	
		2.4.2 Known Limitations	11
3	Con	figuring Skype for Business Server 2015	.13
	3.1	Configuring the E-SBC as an IP / PSTN Gateway	.13
	3.2	Configuring the "Route" on Skype for Business Server 2015	.21
4	Con	figuring AudioCodes E-SBC	.31
	4.1	Step 1: IP Network Interfaces Configuration	.32
		4.1.1 Step 1a: Configure VLANs	
		4.1.2 Step 1b: Configure Network Interfaces	
	4.2	Step 2: Enable the SBC Application	
	4.3	Step 3: Configure Media Realms	
	4.4	Step 4: Configure SIP Signaling Interfaces	
	4.5	Step 5: Configure Proxy Sets	
	4.6	Step 6: Configure Coders	
	4.7	Step 7: Configure IP Profiles	
	4.8	Step 8: Configure IP Groups	
	4.9	Step 9: SIP TLS Connection Configuration	
		<ul><li>4.9.1 Step 9a: Configure the NTP Server Address</li></ul>	
		4.9.2 Step 95: Configure a Certificate for Operation with Microsoft Skype for Business	
		Server 2015	57
		4.9.4 Step 9d: Configure a Certificate for Operation with the BroadCloud SIP Trunk	
		Step 10: Configure SRTP	
	4.11	Step 11: Configure Maximum IP Media Channels	
		Step 12: Configure IP-to-IP Call Routing Rules	
		Step 13: Configure IP-to-IP Manipulation Rules	
		Step 14: Configure Message Manipulation Rules	
		Step 15: Configure Registration Accounts	
	4.10	Step 16: Miscellaneous Configuration	
		4.16.1 Step 16a: Configure Call Forking Mode	
	4.17	Step 17: Reset the E-SBC	
Α		ioCodes INI File	



This page 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 and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

#### Date Published: May-14-2017

### 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 <u>www.audiocodes.com/support</u>.

### **Document Revision Record**

LTRT	Description	
12381	Initial document release for Version 7.2.	

### **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="http://www.audiocodes.com/downloads">http://www.audiocodes.com/downloads</a>.



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 BroadCloud'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 <a href="http://www.audiocodes.com/sbc-wizard">http://www.audiocodes.com/sbc-wizard</a> (login required).

# 1.1 Intended Audience

The document is intended for engineers, or AudioCodes and BroadCloud Partners who are responsible for installing and configuring BroadCloud'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	SIP_7.20A.002	
Protocol	<ul> <li>SIP/UDP or SIP/TLS (to the BroadCloud SIP Trunk)</li> <li>SIP/TCP or SIP/TLS (to the S4B FE Server)</li> </ul>	
Additional Notes	None	

# 2.2 BroadCloud SIP Trunking Version

#### Table 2-2: BroadCloud Version

Vendor/Service Provider	BroadCloud
SSW Model/Service	
Software Version	
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

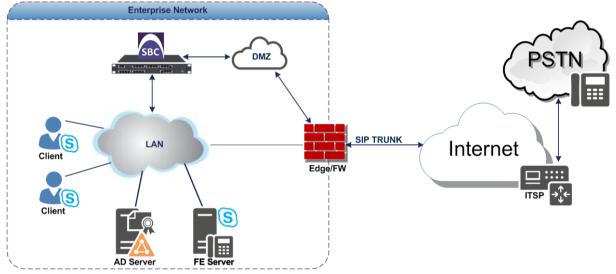
# 2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and BroadCloud 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 BroadCloud'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 BroadCloud's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:





### 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> <li>BroadCloud SIP Trunk is located on the WAN</li> </ul>
Signaling Transcoding	<ul> <li>Both, Microsoft Skype for Business Server 2015 and BroadCloud SIP Trunk, operates with SIP-over-TLS transport type</li> </ul>
Codecs Transcoding	<ul> <li>Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders</li> <li>BroadCloud SIP Trunk supports G.729, G.711A-law and G.711U-law coders</li> </ul>
Media Transcoding	<ul> <li>Both, Microsoft Skype for Business Server 2015 and BroadCloud SIP Trunk, operates with SRTP media type</li> </ul>

### 2.4.2 Known Limitations

The following limitation was observed during interoperability tests performed for the AudioCodes E-SBC interworking between Microsoft Skype for Business Server 2015 and BroadCloud 's SIP Trunk:

If the Microsoft Skype for Business Server 2015 sends the '503 Service Unavailable' error response, the BroadCloud SIP Trunk still sends re-INVITEs and does not disconnect the call. To disconnect the call, a message manipulation rule is used to replace the above error response with the '480 Temporarily Unavailable' response (see Section 4.14).



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.

# 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

Search				
Everywhere $\checkmark$				
Business Server Topology Builder				
Skype for Business Server Deployment Wizard				
Skype for Business Server Topology Builder				
Skype for Business Server Control Panel				
Skype for Business Server Management Shell				

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	logy As		x
🔄 🔄 🔻 👔 « Ac	Iministrator > Documents	✓ C Searce	ch Documents	م
Organize 🔻 New folde	er			∷ • @
🔆 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
I팊 This PC functional This PC				
File <u>n</u> ame: interc	p			~
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

File       Action       Help         Image: Skype for Business Server       SIP domain         Image: Skype for Business Server 2010       Default SIP domain:       S4B.interop         Image: Skype for Business Server 2013       Default SIP domain:       S4B.interop         Image: Skype for Business Server 2015       Default SIP domain:       S4B.interop         Image: Skype for Business Server 2015       Default SIP domain:       S4B.interop         Image: Skype for Business Server 2015       Default SIP domain:       S4B.interop         Image: Skype for Business Server 2015       Default SIP domain:       S4B.interop         Image: Skype for Business Server 2015       Default SIP domain:       S4B.interop         Image: Branch sites       Mediation pools       Simple URLs       Not configured         Image: Branch sites       Phone access URLs:       Active       Simple URL       SIP domain         Image: Branch sites       Meeting URLs:       Active       Simple URL       SIP domain         Image: Branch sites       Meting URLs:       Active       Simple URL       SIP domain         Image: Branch sites       Meting URLs:       Active       Front End       Site         Image: Branch sites       Enterprise Administrative access       https://admin.S4B.interop       S4B.interop </th <th>S</th> <th>kype for Business Server</th> <th>r 2015, Topology Builder 📃 🗖</th>	S	kype for Business Server	r 2015, Topology Builder 📃 🗖
<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> <li>Mediation pools</li> <li>Edge pools</li> <li>Trusted application servers</li> <li>Video Interop Server pools</li> <li>Shared Components</li> <li>Branch sites</li> <li>Shared Components</li> <li>Branch sites</li> <li>Standard Edition Structure</li> <li>Central Management Active Front End Site</li> </ul>	<u>File</u> <u>A</u> ction <u>H</u> elp		
▶ Lync Server 2013       Default SIP domain:       S4B.interop         ▲ Skype for Business Server 2015       Additional supported       Not configured         ▶ Standard Edition Front End Servers       Enterprise Edition Front End pools       Simple URLs         ■ Mediation pools       Persistent Chat pools       Phone access URLs:       Active         ■ Shared Components       Video Interop Server pools       Meeting URLs:       Active         ■ Branch sites       Administrative access       https://admin.S4B.interop         ✓       https://admin.S4B.interop         ✓       https://admin.S4B.interop         ✓       https://admin.S4B.interop         ✓       https://admin.S4B.interop         ✓       https://admin.S4B.interop		SIP domain	
P       Mediation pools         Persistent Chat pools       Edge pools         Trusted application servers       ✓         Video Interop Server pools       Meeting URLs:         Active       Simple URL         Shared Components       ✓         Branch sites       Administrative access         Multiplication Server       Meeting URLs:         Central Management       Active         Front End       Site	<ul> <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> </ul>	Additional supported SIP domains:	
Edge pools       Phone access URLs:       Active       Simple URL         Trusted application servers       Video Interop Server pools       Meeting URLs:       Active       Simple URL       SIP domain         Shared Components       Meeting URLs:       Active       Simple URL       SIP domain         Branch sites       Administrative access       https://admin.S4B.interop       S4B.interop         Central Management       Active       Front End       Site		Simple UKLS	
<ul> <li>Administrative access</li> <li>Branch sites</li> <li>Administrative access</li> <li>https://admin.S4B.interop</li> <li>Central Management</li> <li>Active</li> <li>Front End</li> <li>Site</li> </ul>	Edge pools	Phone access URLs:	
Administrative access       https://admin.S4B.interop         URL:       Central Management Server         Central Management       Active       Front End       Site	Video Interop Server pools	Meeting URLs:	
Central Management Active Front End Site			
Server Land Land Land		Central Management Ser	rver
Server:			Active Front End Site
V FE.34B.Interop Interop		Server:	✓ <u>FE.S4B.interop</u> 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

100 C	Skype for Business Server 2015, Topology Builder
<u>F</u> ile <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> </ul>	The properties for this item are not available for editing.
SQL Server stores     SQL Server stores     SQL Server stores     SPST     SPST     STr     New IP/PSTN Gateway     Tr     Of Topology     Vic Help     SIP Video trunks	
🚞 Branch sites	



The following is displayed:

#### Figure 3-6: Define the PSTN Gateway FQDN

S	Define New IP/PSTN Gateway	x
5	Define the PSTN Gateway FQDN	
Define ti FQDN: *	he fully qualified domain name (FQDN) for the PSTN gateway.	
	IB.interop	
Help	Back Next Cancel	

- 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 4.9.3 on page 57).
- 6. Click **Next**; the following is displayed:

#### Figure 3-7: Define the IP Address

Define New IP/PSTN Gateway
Define the IP address
Enable IPv4
<ul> <li>Use all configured IP addresses.</li> </ul>
<ul> <li>Limit service usage to selected IP addresses.</li> </ul>
PSTN IP address:
○ Enable IPv6
Use all configured IP addresses.
<ul> <li>Limit service usage to selected IP addresses.</li> </ul>
PSTN IP address:
Help Back Next Cancel

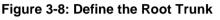
7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

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.



Define New IP/PSTN Gateway	x
fine the root trunk	
erop	
t for IP/PSTN gateway: *	
Protocol:	•
ediation Server:	
p Interop ediation <u>S</u> erver port: *	•
Back Einish Cancel	
	rop  t for IP/PSTN gateway: *  Protocol:  ediation Server:  p Interop  ediation <u>S</u> erver port: *

- 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 4.3 on page 36).
- **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 4.3 on page 36).
- **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	kype for Business Server 2	2015, Topology Builder	
<u>File</u> <u>A</u> ction <u>H</u> elp			
<ul> <li>A B Skype for Business Server</li> <li>A B Skype for Business Server</li> <li>A D Lync Server 2010</li> <li>A Lync Server 2013</li> <li>A Skype for Business Server 2015</li> <li>A Shared Components</li> <li>A SQL Server stores</li> <li>A File stores</li> <li>A File stores</li> <li>A PSTN gateways</li> <li>B Trunks</li> <li>P Office Web Apps Servers</li> <li>A Video gateways</li> <li>SIP Video trunks</li> <li>B ranch sites</li> </ul>	Trunk name: PSTN gateway: Listening port: SIP Transport Protocol: Mediation Server: Mediation Server port:	ITSP.S4B.interop ITSP.S4B.interop (Interop) 5067 TLS FE.S4B.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

9	Skype for Business Server 2015, Topology Builder						
File	Action	Help	_				
	New Ce	ntral Site					
	Edit Pro	perties		SIP domain			
	New Top	oology		Default SIP domain:	C 40 ( )		
	Open To	pology			S4B.int		
	Downloa	ad Topology		Additional supported SIP domains:	Not co	nfigured	
	Save a c	opy of Topology As					
	Publish	Topology					
	Install o	r upgrade a database		Simple URLs			
	Remove	Deployment	-				
	Help			Phone access URLs:	Active	Simple URL	
		<sup>™</sup> Zy ITSP.S4B.interop	1		$\sim$	https://dialin.S4B.interop	
Office Web Apps Servers			Meeting URLs:	Active	Simple URL	SIP domain	
	ſ	📜 Video gateways			$\checkmark$	https://meet.S4B.interop	S4B.interop
	ſ	SIP Video trunks	Administrative access	Administrative access	https://	/admin.S4B.interop	
🚞 Branch sites			URL:				
				Central Management Serv			
				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

Publish Topology	x
Publish the topology	
In order for Skype for Business Server 2015 to correctly route messages in your deployment, yo publish your topology. Before you publish the topology, ensure that the following tasks have be completed:	
<ul> <li>A validation check on the root node did not return any errors.</li> <li>A file share has been created for all file stores that you have configured in this topology.</li> <li>All simple URLs have been defined.</li> <li>For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Server Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured.</li> <li>For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.</li> <li>You are currently logged on as a SQL Server administrator (for example, as a member of th sysadmin role).</li> <li>If you are removing a Front End pool, all users, common area phones, analog devices, applicant objects and conference directories have been removed from the pool.</li> <li>When you are ready to proceed, click Next.</li> </ul>	≡ ne SQL
Help Back Next	Cancel

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

Figure 3-12: Publishing in Progress

ł	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

9	Publish Topol	оду	X
Puk	plishing wizard complete		
Â	Your topology has been successfully published, but s check the log file.	ome warnings were encou	untered. For details,
	Step	Status	
^	Publishing topology	Completed with warnings	View Logs
✓	Downloading topology	Success	
✓	Downloading global simple URL settings	Success	
<ul> <li>✓</li> </ul>	Updating role-based access control (RBAC) roles	Success	
~	Enabling topology	Success	
To cl	lose the wizard, click Finish.		
H	ielp	Back Finis	h 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				



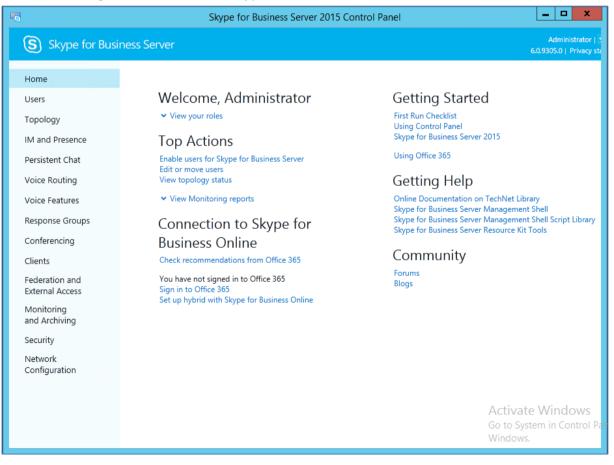
2. You are prompted to enter your login credentials:

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:





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

Figure 3-17: Voice Routing Page					
5	Skype for Business Server 2015 Control Panel	_ <b>□</b> ×			
Skype for Busine	iess Server 6	Administrator   Sign out 0.9305.0   Privacy statement			
Home Users Topology	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING Create voice routing test case information	•			
IM and Presence Persistent Chat					
Voice Routing	P ♣ New ▼ P Edit ▼ Action ▼ Commit ▼	0			
Voice Features Response Groups	Name Scope State Normalization rules Description				
Conferencing Clients					
Federation and External Access					
Monitoring and Archiving					
Security Network Configuration					
		Windows em in Control Panel to a			

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

#### Figure 3-18: Route Tab

3	Skype for E	Business Server 2015 Control Panel	
Skype for Busir	ness Server		Administrator   Sign out 6.0.9305.0   Privacy statement
Home	DIAL PLAN VOICE POLICY ROU	TE PSTN USAGE TRUNK CONFIGURATION	TEST VOICE ROUTING
Users Topology	Create voice routing test case in	formation	~
IM and Presence Persistent Chat		م	
Voice Routing	🗣 New 🧪 Edit 🔻 🔺 Move up	→	Ø
Voice Features	Name	State PSTN usage	Pattern to match
Response Groups	LocalRoute	Committed	^(\+1[0-9](10))\$
Conferencing			
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 Busin	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	<b>*</b>
IM and Presence		
Persistent Chat	New Voice Route	۵
Voice Routing		▲
Voice Features	Scope: Name: *	
Response Groups	ITSP	
Conferencing	Description:	
Clients		
Federation and External Access	Build a Pattern to Match Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.	
Monitoring	Starting digits for numbers that you want to allow:	
and Archiving	Type a valid number and then click Add. Add	
Security	Exceptions	
Network Configuration	Remove	
2		
	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 Busine				
Home	DIAL PLAN VOICE P	OLICY ROUTE PSTN USA	GE TRUNK CONFIGURATION	TEST VOICE ROUTING
Users				
Topology	Create voice r Sel	lect Trunk		<b>@</b> #
IM and Presence				
Persistent Chat	New Voice Rout			9
Voice Routing	√ ок 🗙	Service	Site	
Voice Features		PstnGateway:ITSP.S4B.interop	o Interop	
Response Groups	Edit			
Conferencing	Suppress cal			
Clients	Alternate ca			
Federation and External Access				
Monitoring and Archiving	Associated trun			
Security				
Network Configuration				
<u></u>	Associated PSTN			
	Select		OK	Cancel
	PSTN usage record	Associated voice	policies	

**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	
Voice Features	Match this pattern: *
Response Groups	*
Conferencing Clients	Edit Reset ?
Federation and External Access	Suppress caller ID Alternate caller ID:
Monitoring and Archiving	Associated trunks:
Security	PstnGateway:ITSP.S4B.interop Add
Network Configuration	Remove

Figure 3-21: Selected E-SBC Trunk

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

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

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

Skype for Busine	ss 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 Business Server								
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	ce							
Persistent Chat			Q					
Voice Routing								
Voice Features	🖶 New 🧪 Edit 🔻 👚 Move u		Action  Commit					
Baspansa Crouns	Name	State	PSTN usage	Pattern to match				
Response Groups	LocalRoute	Committed		^(\+1[0-9]{10})\$				
Conferencing	ITSP	뛸 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 Busin	less Server							
Home	DIAL PLAN VOICE POLICY ROL	TE PSTN USAGE TRUNK CO	ONFIGURATION TEST VOICE ROUTING					
Users								
Topology	Create voice routing test case in	Create voice routing test case information						
IM and Presence								
Persistent Chat			٩					
Voice Routing	• · · · • • • • · ·							
Voice Features	New / Edit < A Move up Name	State PSTN usag	Commit  Commit					
Response Groups	LocalRoute	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 C	onfiguration Settin	ıgs		٤ 🕥
Routes				^
Identity	Action	New value (pattern to match)	Old value (pattern to match)	
ITSP	Added	^((\+66) (66))		
			ОК	Tancel

**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 ROL	JTE 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	New 🖉 Edit 🔻 👚 Move u	Move down State	Action  Commit	Pattern to match			
Response Groups	LocalRoute	Skype for Business Server 2015 Control Panel 🕡 🚳					
Conferencing	ΠΣΡ	_	published voice routing c				
Clients		U Successiony	published voice routing c	omguration.			
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:

S Skype for Business Server 6								Administrator   Sign out 6.0.9305.0   Privacy statement
Home	DIAL PLAN	VOICE POLICY	ROUTE	PSTN USAGE	TRUNK COM	NFIGURATION	TEST VOICE ROUTING	
Users								
Тороlоду	Create vo	pice routing test	case infor	rmation				*
IM and Presence								
Persistent Chat					\$	0		
Voice Routing		A						0
Voice Features	New Name	-	Move up	Move down	Action  PSTN usage	Commit 🔻	Pattern to match	0
Response Groups	Local			Committed	PSTN Usage	:	^(\+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 BroadCloud SIP Trunk in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 4.6 on page 45).

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

Skype for Busin	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					
Voice Features		les Called number rules			
Response Groups	Global Global Committed	0			

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

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

Skype for Busine	ss 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	Ø
Voice Routing	√ OK X Cancel	<ul> <li>Image: Second sec</li></ul>
Voice Features	Scope: Pool Name: *	
Response Groups	PstnGateway:ITSP.548.interop	
Conferencing	Description:	
Clients		
Federation and External Access	Maximum early dialogs supported:	
Monitoring	Encryption support level:	
and Archiving	Required T	
Security	Refer support:	
Network Configuration	Enable sending refer to the gateway	
	Enable media bypass	
	Centralized media processing	
	Enable RTP latching	
	Enable forward call history	
	Enable forward P-Asserted-Identity data	
	✓ Enable outbound routing failover timer	-

- 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 BroadCloud 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 BroadCloud 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 BroadCloud 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 configuring this topology. 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.

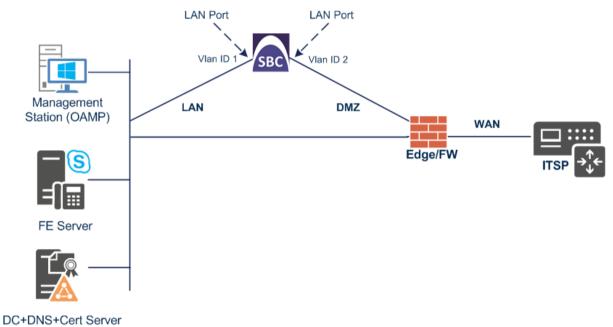


# 4.1 Step 1: IP Network Interfaces Configuration

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
  - BroadCloud 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



### 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	evices (2)			
+ New Edit		<ul> <li>Page 1 of 1 &gt;&gt; &gt;&gt; Show</li> </ul>	10 <b>v</b> records per page	Q .
INDEX 🗢	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

### 4.1.2 Step 1b: Configure Network Interfaces

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

- 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
Name	LAN_IF (arbitrary descriptive name)
Ethernet Device	vlan 1
IP Address	10.15.17.77 (LAN IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Default Gateway	10.15.0.1
Primary DNS	10.15.27.1

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

Parameter	Value
Name	WAN_IF
Application Type	Media + Control
Ethernet Device	vlan 2
IP Address	195.189.192.157 (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)
Primary DNS	80.179.52.100
Secondary DNS	80.179.55.100

4. Click Apply.

The configured IP network interfaces are shown below:

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

	+ New Edit and A Rege 1 of 1 and A Rege 1 of 1 and A Rege 2 A Rege								
NDEX 🗢	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

# 4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

- > To enable the SBC application:
- Open the Applications Enabling page (Setup menu > Signaling & Media tab > Core Entities folder > Applications Enabling).

Figure 4-4: Enabling SBC Application

Applications Enabling		
GENERAL		
SBC Application	Enable	<b>* \$</b>

- 2. From the 'SBC Application' drop-down list, select **Enable**.
- 3. Click Apply.
- 4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.17 on page 86).

# 4.3 Step 3: Configure Media Realms

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

#### 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
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 4-5: Configuring Media Realm for LAN

Media Re	ealms <b>[MRLan]</b>				- x
C	GENERAL		QUALITY OF EXPERIENC	E	
In	ndex	0	QoE Profile	•	View
N	lame •	MRLan	Bandwidth Profile	•	View
Тс	opology Location	Down 🔻			
IP	• • • • •	#0 [LAN_IF] View			
Po	ort Range Start 🔹	6000			
N	lumber Of Media Session Legs •	100			
Po	ort Range End	6999			
D	efault Media Realm	No 🔻			
		Cancel	APPLY		

**3.** Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
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)

Figuro 4-6.	Configuring	Modia	Poolm	for WAN
i iguie 4-0.	conniguning	weula	Neann	

GENERAL		QUALITY OF EXPER	RIENCE	
Index	1	QoE Profile		<ul> <li>Viev</li> </ul>
Name	MRWan	Bandwidth Profile		<ul> <li>View</li> </ul>
Topology Location	• Up	7		
IPv4 Interface Name	● #1 [WAN_IF] ▼	View		
Port Range Start	• 7000			
Number Of Media Session Legs	• 100			
Port Range End	7999			
Default Media Realm	No	•		



The configured Media Realms are shown in the figure below:

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

+ New Ed	lit 🗌	14 <4 Page 1	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

### 4.4 Step 4: Configure SIP Signaling Interfaces

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

#### 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
Name	<b>SIPInterface_LAN</b> (see note at the end of this section)
Network Interface	LAN_IF
Application Type	SBC
UDP Port	0
TCP Port	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. Configure a SIP Interface for the WAN:

Parameter	Value
Index	1
Name	SIPInterface_WAN
Network Interface	WAN_IF
Application Type	SBC
UDP Port	0
TCP Port	0
TLS Port	5061
Media Realm	MRWan



The configured SIP Interfaces are shown in the figure below:

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

+ New Ec	dit 📄 🗍 💼		🛯 <	of 1 🕨 🖭 Sho	ow 10 🔻 records	per page			Q
NDEX 🗢	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SIPInterface_LAN	DefaultSRD (#0	Voice	SBC	0	0	5067	No encapsulation	MRLan
1	SIPInterface_WAN	DefaultSRD (#0	WANSP	SBC	0	0	5061	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.

### 4.5 Step 5: Configure Proxy Sets

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

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

- Microsoft Skype for Business Server 2015
- BroadCloud SIP Trunk

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

#### **To configure Proxy Sets:**

- 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
Index	1
Name	S4B
SBC IPv4 SIP Interface	SIPInterface_LAN
TLS Context Name	default
Proxy Keep-Alive	Using Options
Redundancy Mode	Homing
Proxy Hot Swap	Enable
Proxy Load Balancing Method	Round Robin



oxy Sets <b>[S4B]</b>							-
		SRD #0 [Defaul	tSRD]	¥			
GENERAL				REDUNDANCY			
Index	1			Redundancy Mode		• Homing	•
Name	• S4B			Proxy Hot Swap		• Enable	•
Gateway IPv4 SIP Interface		٣	View	Proxy Load Balancing Method	ł	Round R	obin 🔻
SBC IPv4 SIP Interface	• #0 [S	Pinterface_LAN] 🔻	View	Min. Active Servers for Load E	Balancing	1	
TLS Context Name	• #0 [d	efault] 🔹	View				
				ADVANCED			
KEEP ALIVE				Classification Input	IP Address o	only	•
Proxy Keep-Alive		Disable	Ŧ	DNS Resolve Method			Ŧ
Proxy Keep-Alive Time [sec]		60					
Keep-Alive Failure Responses							
		С	ancel 🛛	NPPLY			

Figure 4-9: 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 4-10: Configuring Proxy Address for Microsoft Skype for Business Server 2015

Proxy	Address		– x
	GENERAL		
	Index	0	
	Proxy Address	FE.S4B.interop:5067	
	Transport Type	TLS	T
			~

**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 BroadCloud SIP Trunk:

Parameter	Value
Index	2
Name	BroadCloud
SBC IPv4 SIP Interface	SIPInterface_WAN
TLS Context Name	default
Proxy Keep-Alive	Using Options
Redundancy Mode	Homing
Proxy Hot Swap	Enable
DNS Resolve Method	SRV

#### Figure 4-11: Configuring Proxy Set for BroadCloud SIP Trunk

Proxy	Sets [BroadCloud]										– x
			SRD #0 [Defai	ultSRD]		Ŧ					
	GENERAL					REDUNDANCY					
	Index	2				Redundancy Mode		•	Homing	•	
	Name	Broad	dCloud			Proxy Hot Swap		•	Enable	•	
	Gateway IPv4 SIP Interface		,	View	,	Proxy Load Balancing Method			Disable	•	
	SBC IPv4 SIP Interface	#1 [SI	PInterface_WAN]	View	,	Min. Active Servers for Load Balar	ncing		1		
	TLS Context Name	#0 [de	efault]	View	,						
						ADVANCED					
	KEEP ALIVE					Classification Input	Address or	nly		•	
	Proxy Keep-Alive		Using OPTIONS	•		DNS Resolve Method • SR	RV			•	
	Proxy Keep-Alive Time [sec]		60								
	Keep-Alive Failure Responses	 									
				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 4-12: Configuring Proxy Address for BroadCloud SIP Trunk

Proxy Address							
	GENERAL						
	Index	0					
	Proxy Address •	hs2.fedsipt1.broadcloudgov.us					
	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	hs2.fedsipt1.broadcloudgov.us (IP address / FQDN and destination port)
Transport Type	TLS

The configured Proxy Sets are shown in the figure below:

Figure 4-13: Configured Proxy Sets in Proxy Sets Table

Proxy Sets	(2) .						
+ New Edit		14 « P	age 1 of 1 🕨 🕨	Show 10 ▼ records	per page		Q
INDEX 🗢	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
1	S4B	DefaultSRD (#0)		SIPInterface_LAN	60	Homing	Enable
2	BroadCloud	DefaultSRD (#0)		SIPInterface_WAN	60	Homing	Enable
2	BroadCloud	DefaultSRD (#0)		SIPInterface_WAN	60	Homing	Enable

### 4.6 Step 6: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Skype for Business Server 2015 supports the G.711 coder while the network connection to BroadCloud SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the BroadCloud SIP Trunk.

Note that the Coder Group ID for this entity will be assign to its corresponding IP Profile in the next step.

- > To configure coders:
- 1. Open the Coder Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Coder Groups).
- 2. Configure a Coder Group for Skype for Business Server 2015:

Parameter	Value
Coder Group Name	AudioCodersGroups_0
Coder Name	<ul><li>G.711 U-law</li><li>G.711 A-law</li></ul>
Silence Suppression	Enable (for both coders)

#### Figure 4-14: Configuring Coder Group for Skype for Business Server 2015

Coder Groups										
Coder Group Name 0 : AudioCodersGroups_0 V Delete Group										
Coder Name		Packetization	Time	Rate		Payload Type	Silence Suppression		Coder Specific	
G.711U-law	•	20	•	<b>6</b> 4 <b>v</b>		0	Enable 🔹			
G.711A-law	•	20	•	<b>6</b> 4 <b>v</b>		8	Enable 🔻			
	•		T	T			•			

#### 3. Configure a Coder Group for BroadCloud SIP Trunk:

Parameter	Value
Coder Group Name	AudioCodersGroups_1
Coder Name	<ul> <li>G.729</li> <li>G.711 A-law</li> <li>G.711 U-law</li> </ul>

#### Figure 4-15: Configuring Coder Group for BroadCloud SIP Trunk

Coder Groups											
	Coder Group Name 1 : AudioCodersGroups_1  Delete Group										
	Coder Name		Packetization Time	e	Rate	Payload Type	1	Silence Suppression		Coder Specific	1
	G.729	Ŧ	20 🔻	Π	8 🔻	18	T	Disabled •			1
	G.711A-law	•	20 🔻		<b>6</b> 4 <b>v</b>	8	Ī	Disabled 🔻			1
	G.711U-law	•	20 🔻		<b>6</b> 4 <b>v</b>	0	Ι	Disabled 🔻			]
		۳	•		•		I	•			]

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the BroadCloud SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID will be assign to the IP Profile belonging to the BroadCloud SIP Trunk in the next step.

- **>** To set a preferred coder for the Skype for Business Server 2015:
- 1. 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 Audio Coders Group Skype for Business Server 2015.

#### Figure 4-16: Configuring Allowed Coders Group for Skype for Business Server 2015

Allowed	l Audio Coders Group	os [S4B Allowed Coders]	– x
	GENERAL		
	Index	0	
	Name	S4B Allowed Coders	

- 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 Audio Coders table opens.
- 5. Click **New** and configure an Allowed Coders as follows:

Parameter	Value
Index	0
Coder	G.711 A-law
Index	1
Coder	G.711 U-law

#### Figure 4-17: Configuring Allowed Coders the Skype for Business Server 2015

Allowed Audio Coders Groups [#0] > Allowed Audio Coders (2)								
+ New Edit 🗐 🗑	I < <   Page 1 of 1   ⇒ ⇒ Show 10 ▼ records per	page 🔎						
INDEX 🗢	CODER	USER-DEFINED CODER						
0	G.711A-law							
1	G.711U-law							

- To set a preferred coder for the BroadCloud 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 Audio Coders Group for BroadCloud SIP Trunk.

#### Figure 4-18: Configuring Allowed Coders Group for BroadCloud SIP Trunk

Allowed	l Audio Coders Grou	Ips [BroadCloud Allowed Coders]	– x
	GENERAL		
	Index	1	
	Name	BroadCloud Allowed Coders	

- 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 Audio Coders table opens.
- 5. Click **New** and configure an Allowed Coders as follows:

Parameter	Value
Index	0
Coder	G.729
Index	1
Coder	G.711 A-law
Index	2
Coder	G.711 U-law

#### Figure 4-19: Configuring Allowed Coders for BroadCloud SIP Trunk

Allowed Audio Coders     New Edit	Groups [#1] > Allowed Audio Co		Q
INDEX 🗢	CODER	USER-DEFINED CODER	
0	G.729		
1	G.711A-law		
2	G.711U-law		



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

Media Settings			
GENERAL		ROBUSTNESS	
NAT Traversal	Disable NAT	New RTP Stream Packets	3
Enable Continuity Tones	Disable 💌 🗲	New RTCP Stream Packets	3
Inbound Media Latch Mode	Dynamic 💌	New SRTP Stream Packets	3
Number of Media Channels	0	New SRTCP Stream Packets	3
Enforce Media Order	Disable 🔻	Timeout To Relatch RTP (msec)	200
SDP Session Owner	AudiocodesGW	Timeout To Relatch SRTP (msec)	200
		Timeout To Relatch Silence (msec)	10000
SBC SETTINGS		Timeout To Relatch RTCP (msec)	10000
Preferences Mode	• Include Extensions	←	
Enforce Media Order	Disable 🔻		
GATEWAY SETTINGS			
Enable Early Media	Disable 💌		
Multiple Packetization Time Format	None 🔻		
	Cancel	APPLY	

Figure 4-20: SBC Preferences Mode

- 7. From the 'Preferences Mode' drop-down list, select Include Extensions.
- 8. Click Apply.

### 4.7 Step 7: 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 SIP over TLS
- BroadCloud SIP trunk to operate in secure mode using SRTP and SIP over TLS
- > To configure IP Profile for the Skype for Business Server 2015:
- 1. 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 Media	
Extension Coders Group	AudioCodersGroups_0
Allowed Audio Coders	S4B Allowed Coders
RFC 2833 Mode	Extend
RFC 2833 DTMF Payload Type	101
SBC Signaling	
Remote Update Support	Supported Only After Connect
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	

# AudioCodes

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)
SBC Hold	
Remote Hold Format	Inactive
Media	
Broken Connection Mode	Ignore

#### Figure 4-21: Configuring IP Profile for Skype for Business Server 2015

IP Profi	iles [S4B]						– x
							<b>^</b>
	GENERAL				SBC SIGNALING		E
	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 •	Supported Only After Conn	
	Gateway Media Security Mode		Preferable	•	Remote re-INVITE •	Supported only with SDP	•
	Symmetric MKI		Enable	•	Remote Delayed Offer Support •	Not Supported	•
	MKI Size		1		Remote Representation Mode	According to Operation Mo	-
	SBC Enforce MKI Size		Enforce	•	Keep Incoming Via Headers	According to Operation Mo	-
	SBC Media Security Method		SDES	•	Keep Incoming Routing Headers	According to Operation Mo	-
					Keep User-Agent Header	According to Operation Mo	<b>•</b> •
				Cancel	APPLY		

3. Click Apply.

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

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

Parameter	Value
General	
Index	2
Name	BroadCloud
Media Security	
SBC Media Security Mode	SRTP
Symmetric MKI	Enable
SBC Enforce MKI Size	Enforce
SBC Remove Crypto Lifetime in SDP	Yes
SBC Early Media	
Remote Can Play Ringback	<b>No</b> (required, as Skype for Business Server 2015 does not provide a ringback tone for incoming calls)
SBC Media	
Extension Coders Group	AudioCodersGroups_1
Allowed Audio Coders	BroadCloud Allowed Coders
Allowed Coders Mode	<b>Restriction and Preference</b> (lists Allowed Coders first and then original coders in received SDP offer)
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Play RBT To Transferee	Yes
Remote 3xx Mode	Handle Locally
Media	
Broken Connection Mode	Ignore



IP Profiles [BroadCloud]					– x
GENERAL				SBC SIGNALING	
Index	2			PRACK Mode	Transparent 🔻
Name	• Broa	adCloud		P-Asserted-Identity Header Mode	• Add •
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	Ŧ	Remote Update Support	Supported 🔻
Gateway Media Security Mod	e	Preferable	•	Remote re-INVITE	Supported 🔻
Symmetric MKI		<ul> <li>Enable</li> </ul>	•	Remote Delayed Offer Support	Supported 🔻
MKI Size		0		Remote Representation Mode	According to Or ▼
SBC Enforce MKI Size		<ul> <li>Enforce</li> </ul>	•	Keep Incoming Via Headers	According to Or ▼
SBC Media Security Method		SDES		Keep Incoming Routing Headers	According to Or ▼
		<b>_</b> · · ·		Keep User-Agent Header	According to Or 🔻
		(	Cancel	APPLY	

Figure 4-22: Configuring IP Profile for BroadCloud SIP Trunk

2. Click Apply.

### 4.8 Step 8: 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
- BroadCloud SIP Trunk located on WAN

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

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

Parameter	Value
Index	1
Name	S4B
Туре	Server
Proxy Set	S4B
IP Profile	S4B
Media Realm	MRLan
SIP Group Name	<b>interop.adpt-tech.com</b> (according to ITSP requirement)

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

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

Parameter	Value
Index	2
Name	BroadCloud
Topology Location	Up
Туре	Server
Proxy Set	BroadCloud
IP Profile	BroadCloud
Media Realm	MRWan
SIP Group Name	<b>interop.adpt-tech.com</b> (according to ITSP requirement)



The configured IP Groups are shown in the figure below:

ups (2) .										
Edit			🛯 << Page 1	of 1 🕟 🕨	Show 10 V	records pe	r page			Q
NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULAT SET	OUTBOUN MESSAGE MANIPULA SET
S4B	Defaults	Server	Not Configu	S4B	S4B	MRLan	interop.adp1	Enable	-1	-1
BroadCloud	Defaults	Server	Not Configu	BroadCloud	BroadCloud	MRWan	interop.adp1	Enable	-1	4
	Edit in the second seco	Edit 🗐 🏛 NAME SRD S4B 📕 DefaultS	Edit NAME SRD TYPE S4B  Default Server	Edit Harris Page 1 NAME SRD TYPE S4B Default: Server Not Configu	Edit     Image     Page     of 1     Image       NAME     SRD     TYPE     SBC OPERATION MODE     PROXY SET       S4B     Default     Server     Not Configu     S4B	Edit     Image: Total and the set of the	Edit     Image: The set of th	Edit       Image: Total and the server of the	Edit       Image:	Edit       Image: Type       Page: Tof 1       Image: Type       Show 10       records per page         NAME       SRD       Type       SBC OPERATION MODE       IP PROFILE       MEDIA REALM       SIP GROUP SET       INBOUND MESSAGE MANIPULAT SET         S4B       Defaults       Server       Not Configu       S4B       S4B       MRLan       interop.adpl       Enable       -1

### 4.9 Step 9: SIP TLS Connection Configuration

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

### 4.9.1 Step 9a: Configure the NTP Server Address

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

- > 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**).

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	

#### Figure 4-24: Configuring NTP Server Address

3. Click Apply.

### 4.9.2 Step 9b: 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'

TLS Co	ntexts [default]						- x
	GENERAL				OCSP		
	Index		0		OCSP Server	Disable 🔻	
	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 🔻				
			Canco				
_			Cance		PPLY		^

Figure 4-25: Configuring TLS version

4. Click Apply.

# 4.9.3 Step 9c: Configure a Certificate for Operation with Microsoft Skype for Business Server 2015

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).
- 2. 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:



• TLS Context [#0] > Context Certificates	
CERTIFICATE SIGNING REQUEST	
Subject Name [CN]	ITSP.S4B.interop
Organizational Unit [OU] (optional)	
Company name [O] <i>(optional)</i>	
Locality or city name [L] <i>(optional)</i>	
State [ST] <i>(optional)</i>	
Country code [C] <i>(optional)</i>	
Signature Algorithm	SHA-1
Create CSR	
ter creating the CSR, copy the text below (including the BEGIN/END lines) a	nd send it to your Certification Authority for signing.
BEGIN CERTIFICATE REQUEST IIBWJCBxAIBADAbMRkwFwyDVQQDDBBJVFNQL1M0Qi5pbnRlcm9wMIGfMA0GCSqG Ib3DQEBAQUAA4GNADCBiQKBgQCzEs8XTnY8be/t77eEDG7rTg747GQ3ODfOC4Rs +e9KfbErZgxMYqGT8u04AU0wU9LUPkkq+8gI6w2bg3boW0kg/9hrnNL2rfltGcn 3oShP05PiKmRNZnCC090b03tbr9kuHmlwPRQ7yT6k7xS3XBb5igqT4LQbjBTltt DH3bQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAim/GA2E1ZQbZaR6CZyIawiIT 55w450NFHmaCluH5yZ8keM8d1Ux14hkW7t5ygAD8KbxVKHRVaCgcQrAK2v8u1Pf /N+bwJ+kQOd59CiX882e001WB3buPq5+qWDGTF+MyJWGVf8SIc1c6+zFoc+BEZY tQ8y0J8od0aDhStDfQ= END CERTIFICATE REOUEST	

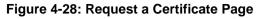
Figure 4-26: Certificate Signing Request – Creating CSR

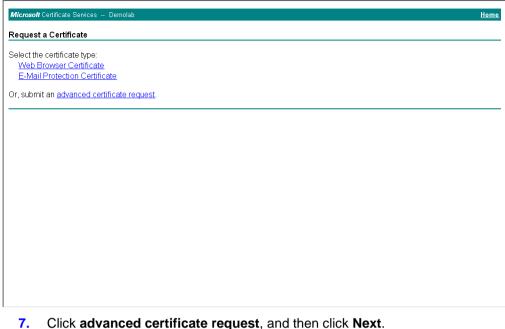
- 4. Copy the CSR from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
- 5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate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

#### Figure 4-27: Microsoft Certificate Services Web Page

Microsoft Certificate Services Demolab	<u>Hon</u>
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other identity to people you communicate with over the Web, sign and encrypt messages, ar perform other security tasks.	
You can also use this Web site to download a certificate authority (CA) certificate, cert view the status of a pending request.	tificate chain, or certificate revocation list (CRL), or to
For more information about Certificate Services, see Certificate Services Documenta	<u>ation</u> .
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	

6. Click Request a certificate.





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

#### Figure 4-29: Advanced Certificate Request Page

Microsoft Certificate Services Demolab Hon
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-encode PKCS #7 file.

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



Figure 4-30: Submit a Certificate Request or Renewal Request Page

Microsoft Active	Directory Certificate Services Lync-DC-LYNC-CA Hom
Submit a Certi	ificate Request or Renewal Request
generated by a	ved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request n external source (such as a Web server) in the Saved Request box.
certificate request (CMC or	A8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxuyKk1       rr4ootrnsPOCAWEAAAAHAOGCSqOSIbsDQEBBAUA       HnkHAkx8xHq9gaAgoLKmuch2B02m4gEcOGAFT8ok       9fSm8c4Bj9ib+R8+YI+Ost57xT9DZXNg5Yp4G+OB      END CERTIFICATE REQUEST          III
	Web Server
Additional Attribu	utes:
Attributes:	▲ ► ►
	Submit >

- 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 4-31: Certificate Issued Page

The ce	ertificate you requested	was issued to you.		
9			əd	

- 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.

<i>Microsoft</i> 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:	
Encoding method: © DER © Base 64 Download CA certificate Download CA certificate chain Download latest base CRL	

Figure 4-32: 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.



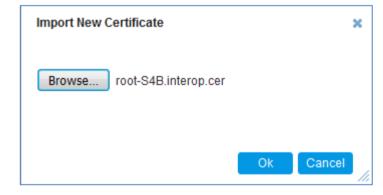
- **19.** In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
  - a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
  - b. Scroll down 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 4-33: 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 <b>Device Certificate</b> file from your computer to the device. The file must be in textual PEM format. <b>Browse</b> 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 4-34: 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 4.17 on page 86).

#### 4.9.4 Step 9d: Configure a Certificate for Operation with the BroadCloud SIP Trunk

This step describes how to load the BroadCloud Root Certificate as a Trusted Root Certificate. This certificate is used by the E-SBC to authenticate the connection with the BroadCloud SIP Trunk.

The procedure involves the following main steps:

- a. Obtaining a Trusted Root Certificate from the BroadCloud.
- b. Deploying the BroadCloud Root Certificate as Trusted Root Certificates on the E-SBC.
- To load 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 (usually default index 0 will be used), and then click the Trusted Root Certificates link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
- 3. Click the **Import** button, and then select the certificate file to load.

#### Figure 4-35: Importing the BroadCloud Root Certificate into Trusted Certificates Store

Import New Certificate		×
Choose File Geotrust_root.cer		
	Ok	Cancel

- 4. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
- 5. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 86).

### 4.10 Step 10: Configure SRTP

This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 4.6 on page 45).

#### > To configure media security:

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

Media Security					
GENERAL			AUTHENTICATION & ENCRYPT	ION	
Media Security $\longrightarrow$	Enable	- 5	Authentication On Transmitted	RTP Packet	s Active 💌
Media Security Behavior	Preferable	•	Encryption On Transmitted RTF	Packets	Active 💌
Offered SRTP Cipher Suites	All	•	Encryption On Transmitted RT	CP Packets	Active 💌
Aria Protocol Support	Disable	- 5	SRTP Tunneling Authentication	for RTP	Disable 💌
			SRTP Tunneling Authentication	for RTCP	Disable 🔻
MASTER KEY IDENTIFIER					
Master Key Identifier (MKI) Size	0		GATEWAY SETTINGS		
Symmetric MKI	Disable	•	Enable Rekey After 181	Disable	•

#### Figure 4-36: 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 4.17 on page 86).

### 4.11 Step 11: Configure Maximum IP Media Channels

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



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

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

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

Media Settings	
GENERAL	
NAT Traversal	Disable NAT 💌
Enable Continuity Tones	Disable 💌 🗲
Inbound Media Latch Mode	Dynamic 💌
Number of Media Channels	• 100 5 -
Enforce Media Order	Disable 💌
SDP Session Owner	AudiocodesGW

#### Figure 4-37: Configuring Number of Media Channels

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **100**).

#### 3. Click Apply.

**4.** Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 86).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.8 on page 44,) 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 BroadCloud SIP Trunk (DMZ):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
- Calls from Skype for Business Server 2015 to BroadCloud SIP Trunk
- Calls from BroadCloud SIP Trunk to Skype for Business Server 2015

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

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

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

#### Figure 4-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

IP-to-IP Routing [Terminate OPTIC	ONS]			- x
	Routing Policy #0 [Default_	SBCRoutingPolicy]		<b>^</b>
GENERAL		ACTION		
Index	0	Destination Type •	Dest Address	<b>▼</b> =
Name •	Terminate OPTIONS	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		•
Request Type	• OPTIONS •	Call Setup Rules Set ID	-1	
Source Username Prefix	*	Group Policy	Sequential	-
Source Host	*	Cost Group		View
Source Tags				-
	Cancel	APPLY		

**b.** Click **Apply**.

## AudioCodes

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

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

#### Figure 4-39: Configuring IP-to-IP Routing Rule for S4B to BroadCloud

IP-to-I	P Routing [S4B to ITSP]			- x
		Routing Policy #0 [Default_S	BCRoutingPolicy]	
	GENERAL		ACTION	
	Index Name Alternative Route Options	1  S4B to ITSP  Route Row	Destination Type Destination IP Group Destination SIP Interface	IP Group   #2 [BroadCloud]  View  View
	MATCH		Destination Address Destination Port	0
	Source IP Group Request Type Source Username Prefix Source Host Source Tag	• #1 [54B] ▼ View All ▼ * 	Destination Transport Type IP Group Set Call Setup Rules Set ID Group Policy Cost Group	▼            ▼           -1           Sequential         ▼            ▼           View
		Cancel	APPLY	

b. Click Apply.

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

Parameter	Value
Index	2
Route Name	BroadCloud to S4B (arbitrary descriptive name)
Source IP Group	BroadCloud
Destination Type	IP Group
Destination IP Group	S4B

#### Figure 4-40: Configuring IP-to-IP Routing Rule for BroadCloud to S4B

IP-to-	IP Routing [ITSP to S4B]			- x
		Routing Policy #0 [Default_SBC	RoutingPolicy]	
	GENERAL		ACTION	
	Index	2	Destination Type	IP Group
	Name	ITSP to S4B	Destination IP Group	• #1 [S4B] <b>View</b>
	Alternative Route Options	Route Row 🔻	Destination SIP Interface	View
			Destination Address	
	MATCH		Destination Port	0
	Source IP Group	• #2 [BroadCloud] • View	Destination Transport Type	<b></b>
	Request Type	All	IP Group Set	View
	Source Username Prefix	*	Call Setup Rules Set ID	-1
	Source Host	*	Group Policy	Sequential 🔻
	Source Tag		Cost Group	View
		Cancel 🗾	APPLY	

b. Click Apply.



The configured routing rules are shown in the figure below:

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

+ New	Edit Inser	t 🕆 🕂	<b>İ</b>	<	of 1 🕨 🕨	Show 10 ¥	records per	page			Q
INDEX 🗢	NAME	ROUTING POLICY	ALTERNATIV ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATIC USERNAME PREFIX	DESTINATIC TYPE	DESTINATIC	DESTINATIC SIP INTERFACE	DESTINAT ADDRESS
0	Terminate O	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Addres			internal
1	S4B to ITSP	Default_SBC	Route Row	S4B	All	*	*	IP Group	BroadCloud		
2	ITSP to S4B	Default_SBC	Route Row	BroadCloud	All	*	*	IP Group	S4B		



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

### 4.13 Step 13: 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 4.8 on page 44) 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 add the "+" (plus sign) to the destination number for calls from the BroadCloud SIP Trunk IP Group to the Skype for Business Server 2015 IP Group for any destination username prefix.

#### > 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	Add + toward S4B
Source IP Group	BroadCloud
Destination IP Group	S4B
Destination Username Prefix	* (asterisk sign)
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)



bound Manipulations [Add -	+ toward S4B]		-
	Routing Policy #0 [Default_	SBCRoutingPolicy]	
GENERAL		ACTION	
Index	0	Manipulated Item	• Destination URI •
Name	• Add + toward S4B	Remove From Left	0
Additional Manipulation	No	Remove From Right	0
Call Trigger	Any 🔻	Leave From Right	255
		Prefix to Add	• +
MATCH		Suffix to Add	
Request Type	All	Privacy Restriction Mode	Transparent 🔻
Source IP Group	• #2 [BroadCloud] • View	1	
Destination IP Group	• #1 [S4B] • View	1	
Source Username Prefix	*		
	Cancel	APPLY	

Figure 4-42: 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 BroadCloud SIP Trunk IP Group:

Figure 4-43: Examp	ole of Configured IP-to-IP	Outbound Manipulation Rules	
I Iguio I Ior Examp			

+ New	Edit	nsert 🕇	+ │ 🖻	14 - 44	Page 1	]of 1   🕨 🕨	Show 10	▼ records	per page				Q
NDEX 🗢	NAME	ROUTING POLICY	ADDITION MANIPUL	SOURCE IP GROUP	DESTINAT IP GROUP	SOURCE USERNAN PREFIX	DESTINAT USERNAN PREFIX	MANIPUL ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFI) TO AD
0	Add + tow	Default_SE	No	BroadClou	S4B	*	*	Destinatio	0	0	255	+	
1	Change + r	Default_SE	No	S4B	BroadClou	*	+	Destinatic	1	0	255	011	
2	Remove +	Default_SE	No	S4B	BroadClou	+8	*	Source UF	1	0	255		

Rule Index	Description
1	Calls from BroadCloud IP Group to S4B IP Group with any <u>destination</u> number (*), add "+" to the prefix of the destination number.
2	Calls from S4B IP Group to BroadCloud IP Group with the prefix <u>destination</u> number "+", remove "+" from this prefix and add "011" to the prefix.
3	Calls from S4B IP Group to BroadCloud IP Group with <u>source</u> number prefix "+8", remove the "+" from this prefix.

### 4.14 Step 14: 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 BroadCloud SIP Trunk. This rule applies to messages sent to the BroadCloud SIP Trunk IP Group in a Call Forward scenario. This adds a SIP Diversion Header with the value from the SIP From Header only if the SIP History-Info Header exists.

Parameter	Value	
Index	0	
Name	Call Forward	
Manipulation Set ID	4	
Message Type	invite	
Condition	header.history-info exists	
Action Subject	header.diversion	
Action Type	Add	
Action Value	header.from	

#### Figure 4-44: Configuring SIP Message Manipulation Rule 0 (for BroadCloud SIP Trunk)

Message Manipulations [Ca	ll Forward]			- x
GENERAL		ACTION		
Index	0	Action Subject	• header.diversion	
Name	Call Forward	Action Type	Add	
Manipulation Set ID	• 4	Action Value	• header.from	
Row Role	Use Current Condition			
MATCH				
Message Type	invite			
Condition •	header.history-info exists			
	Cancel	APPLY		

**3.** Configure another manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk. This rule applies to messages sent to the BroadCloud SIP Trunk IP Group in a Call Forwarding scenario. This replaces the user part of the SIP From Header with the value from the SIP History-Info Header.

Parameter	Value
Index	1
Name	Call Forward
Manipulation Set ID	4
Message Type	invite
Condition	header.history-info.0 regex ( <sip:)(.)(.*)(@)(.*)< td=""></sip:)(.)(.*)(@)(.*)<>
Action Subject	header.from.url.user
Action Type	Modify
Action Value	\$3

#### Figure 4-45: Configuring SIP Message Manipulation Rule 1 (for BroadCloud SIP Trunk)

Message Manipulations [Call H	Forward]			– x
GENERAL		ACTION		
Index Name <b>Manipulation Set ID</b> Row Role	1         • Call Forward         • 4         Use Current Condition	Action Subject Action Type Action Value	<ul> <li>header.diversion.url.user</li> <li>Modify </li> <li>\$3</li> </ul>	
MATCH				
Message Type • Condition •	header.history-info.0 regex ( <sip:)(.)(.*< th=""><th></th><th></th><th></th></sip:)(.)(.*<>			
	Cancel	APPLY		

**4.** If the manipulation rule Index 1 (above) is executed, then the following rule is also executed to remove the SIP History-Info Header.

Parameter	Value
Index	2
Name	Call Forward
Manipulation Set ID	4
Row Role	Use Previous Condition
Message Type	
Condition	
Action Subject	header.history-info
Action Type	Remove
Action Value	

#### Figure 4-46: Configuring SIP Message Manipulation Rule 2 (for BroadCloud SIP Trunk)

Message Manipulations [Ca	all Forward]			– x
GENERAL		ACTION		
Index Name <b>Manipulation Set ID</b> Row Role	2  Call Forward  4 Use Previous Condition ▼	Action Subject Action Type Action Value	<ul> <li>header.history-info</li> <li>Remove</li> </ul>	V
МАТСН				
Message Type Condition				
	Cancel	APPLY		

5. Configure a manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk that applies to messages sent to the BroadCloud SIP Trunk IP Group in a Call Transfer scenario. This replaces the host part of the SIP Referred-By Header with the value from the SIP From Header.

Parameter	Value
Index	3
Name	Call Transfer
Manipulation Set ID	4
Message Type	invite
Condition	header.referred-by exists
Action Subject	header.referred-by.url.host
Action Type	Modify
Action Value	header.from.url.host

#### Figure 4-47: Configuring SIP Message Manipulation Rule 3 (for BroadCloud SIP Trunk)

Message Manipulations [Ca	ll Transfer]			– x
GENERAL		ACTION		
Index Name	3 Call Transfer	Action Subject Action Type	header.referred-by.url.host     Modify	
Manipulation Set ID Row Role	● 4 Use Current Condition ▼	Action Value	<ul> <li>header.from.url.host</li> </ul>	
МАТСН				
Message Type Generation Generatio Generation Generation Generation Generation Generation	header.referred-by exists			
	Cancel	APPLY		

6. Configure a manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk that applies to messages sent to the BroadCloud SIP Trunk IP Group in a Call Transfer scenario. This rule removes '+' prefix from the user part of the SIP Referred-By Header.

Parameter	Value
Index	4
Name	Call Transfer
Manipulation Set ID	4
Message Type	invite
Condition	header.referred-by exists
Action Subject	header.referred-by.url.user
Action Type	Remove Prefix
Action Value	·+'

#### Figure 4-48: Configuring SIP Message Manipulation Rule 4 (for BroadCloud SIP Trunk)

Message Manipulations [C	[all Transfer]		- x
GENERAL		ACTION	
Index Name <b>Manipulation Set ID</b> Row Role	4 • Call Transfer • 4 Use Current Condition ▼	Action Subject Action Type Action Value	<ul> <li>header.referred-by.url.usei</li> <li>Remove Prefix </li> <li>'+'</li> </ul>
МАТСН			
0 51	invite     header.referred-by exists		
	Cancel	APPLY	

7. Configure a manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk that applies to messages sent to the BroadCloud SIP Trunk IP Group in a Call Transfer scenario. This replaces the user part of the SIP From Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	5
Name	Call Transfer
Manipulation Set ID	4
Message Type	invite
Condition	header.referred-by exists
Action Subject	header.from.url.user
Action Type	Modify
Action Value	header.referred-by.url.user

#### Figure 4-49: Configuring SIP Message Manipulation Rule 5 (for BroadCloud SIP Trunk)

Message Manipulations [C	Call Transfer]		– x
GENERAL		ACTION	
Index Name <b>Manipulation Set ID</b> Row Role	5     • Call Transfer     • 4     Use Current Condition ▼	Action Subject Action Type Action Value	<ul> <li>header.from.url.user</li> <li>Modify</li> <li>header.referred-by.url.user</li> </ul>
MATCH			
Message Type Condition	invite     header.referred-by exists		
	Cancel	APPLY	

8. Configure another manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk. This rule is applied to response messages sent to the BroadCloud SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method type '503' with the value '480', because BroadCloud SIP Trunk not recognizes '503' method type.

Parameter	Value
Index	6
Name	Reject Responses
Manipulation Set ID	4
Message Type	any.response
Condition	header.request-uri.methodtype=='503'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'480'

#### Figure 4-50: Configuring SIP Message Manipulation Rule 6 (for BroadCloud SIP Trunk)

Message Manipulations [Reject	Responses]			- x
GENERAL		ACTION		
Index Name <b>Manipulation Set ID</b> Row Role	6     • Reject Responses     • 4     Use Current Condition	Action Subject Action Type Action Value	<ul> <li>header.request-uri.methodtype</li> <li>Modify</li> <li>'480'</li> </ul>	] ]
MATCH				
Message Type • Condition •	any.response header.request-uri.methodtype=='503'			
	Cancel	APPLY		

Message N	Message Manipulations (7) .							
+ New Edi	t Insert 🕇 🖡	<b>İ</b>	<a 1="" 1<="" of="" page="" th=""><th>▶&gt; ▶ Show 10 ▼ re</th><th>ecords per page</th><th></th><th></th><th>Q</th></a>	▶> ▶ Show 10 ▼ re	ecords per page			Q
INDEX 🗢	NAME	MANIPULATION SET	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Call Forward	4	invite	header.history-info e	header.diversion	Add	header.from	Use Current Conditio
1	Call Forward	4	invite	header.history-info.0	header.diversion.url.	Modify	\$3	Use Current Conditio
2	Call Forward	4			header.history-info	Remove		Use Previous Conditi
3	Call Transfer	4	invite	header.referred-by e	header.referred-by.u	Modify	header.from.url.host	Use Current Conditio
4	Call Transfer	4	invite	header.referred-by e	header.referred-by.u	Remove Prefix	'+'	Use Current Conditio
5	Call Transfer	4	invite	header.referred-by e	header.from.url.user	Modify	header.referred-by.u	Use Current Conditio
6	Reject Responses	4	any.response	header.request-uri.n	header.request-uri.n	Modify	'480'	Use Current Conditio

#### Figure 4-51: Example of Configured SIP Message Manipulation Rules

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to and from the BroadCloud SIP Trunk IP Group. These rules are specifically required to enable proper interworking between BroadCloud SIP Trunk and Skype for Business Server 2015. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule			
0	This rule adds a SIP Diversion Header with the value from the SIP From Header only if the SIP History-Info Header exists.	For <b>Call Forward</b> scenarios, BroadCloud SIP Trunk needs the SIP Diversion Header. In order to			
1	This rule replaces the <b>user</b> part of the SIP From Header with the value from the SIP History-Info Header.	do this, a SIP Diversion Header is added with the value from SIP From Header and the User part of			
2	If the manipulation rule Index 1 (above) is executed, then the following rule is also executed. It removes the SIP History-Info Header.	the SIP Diversion Header is replaced with the value from History-Info Header.			
3	This rule replaces the <b>host</b> part of the SIP Referred-By Header with the value from the SIP From Header.	For <b>Call Transfer</b> initiated by Skype for Business Server 2015,			
4	This rule removes '+' prefix from the user part of the SIP Referred-By Header.	BroadCloud SIP Trunk needs to replace the <b>host</b> part of the SIP Referred-By Header with the			
5	This rule replaces the <b>user</b> part of the SIP From Header with the value from the SIP Referred-By Header.	value from the SIP From Header			
6	This rule replaces the method type '503' with the value '480', because BroadCloud SIP Trunk does not recognize the '503' method type.	BroadCloud SIP Trunk does not recognize the '503' method type and continues to send an INVITE message i.e.it tries to setup another call.			

- 9. Assign Manipulation Set ID 4 to the BroadCloud 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 the BroadCloud SIP trunk IP Group, and then click **Edit**.
  - c. Set the 'Outbound Message Manipulation Set' field to 4.

#### Figure 4-52: Assigning Manipulation Set 4 to the BroadCloud SIP Trunk IP Group

IP Groups [BroadCloud] – x						
	SRD #0 [DefaultS	RD]	v			
GENERAL			QUALITY OF EXPERIENCE	E		
Index Name	2  BroadCloud		QoE Profile Bandwidth Profile		<ul><li>View</li><li>View</li></ul>	
Topology Location	• Up	•				
Туре	Server	•	MESSAGE MANIPULATIO	N		
Proxy Set IP Profile		View View	Inbound Message Manipu		-1	
Media Realm	● #1 [MRWan] ▼	View	Outbound Message Mani Message Manipulation U		• 4	
Contact User SIP Group Name	interop.adpt-tech.com		Message Manipulation U	ser-Defined String 2		
Created By Routing Server	No		SBC REGISTRATION AND	AUTHENTICATION		
	Car	ncel 🛛	PPLY			

d. Click Apply.

### 4.15 Step 15: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the BroadCloud SIP Trunk on behalf of Skype for Business Server 2015. The BroadCloud 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 BroadCloud SIP Trunk IP Group.

- > To configure a registration account:
- 1. 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 , for example:

Parameter	Value
Served IP Group	S4B
Application Type	SBC
Serving IP Group	BroadCloud
Host Name	As provided by the SIP Trunk provider
Register	Regular
Contact User	1234567890 (trunk main line)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Accounts		- x
	Served IP Group #1 [S4B]	
GENERAL	CREDENTIALS	
Index Served Trunk Group Application Type Serving IP Group Host Name Register Contact User	0       User Name       1234567890         -1       Password       .         SBC       ▼         #2 [BroadCloud]       ▼         View       interop.adpt-tech.com         Regular       ▼         1234567890	
	Cancel APPLY	

Figure 4-53: Configuring a SIP Registration Account

4. Click Apply.

### 4.16 Step 16: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

### 4.16.1 Step 16a: 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**.

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

#### Figure 4-54: Configuring Forking Mode

3. Click Apply.

### 4.16.2 Step 16b: 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**.

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

Figure 4-55: SBC Alternative Routing Reasons Table

4. Click Apply.

## 4.17 Step 17: 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 4-56: 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.

## 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 **
; * * * * * * * * * * * * * *
;Board: Mediant 800
;HW Board Type: 69 FK Board Type: 72
;Serial Number: 2265355
;Slot Number: 1
;Software Version: 7.20A.002
;DSP Software Version: 5014AE3_R => 720.25
;Board IP Address: 10.15.77.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
               Flash size: 64M Core speed: 300Mhz
;Ram size: 512M
;Num of DSP Cores: 3 Num DSP Channels: 30
;Num of physical LAN ports: 12
;Profile: NONE
;;;Key features:;Board Type: Mediant 800 ;PSTN FALLBACK Supported
;BRITrunks=4 ;E1Trunks=1 ;T1Trunks=1 ;FXSPorts=4 ;FXOPorts=0 ;Channel
Type: DspCh=30 IPMediaDspCh=30 ;HA ;DATA features: ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;DSP Voice features: RTCP-XR
;Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC
EVRC-B AMR-WB G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB
SPEEX_WB OPUS_NB OPUS_WB ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ; IP Media: Conf VXML CALEA
TrunkTesting ;Control Protocols: MGCP SIP SASurvivability SBC=250 MSFT
FEU=100 TestCall=100 ;Default features:;Coders: G711 G726;
;----- HW components-----
;
; Slot # : Module type : # of ports
                             ------
;-----
     1 : BRI
;
                     : 4
      2 : FXS
                      : 4
;
     3 : FALC56
                     : 1
;
[SYSTEM Params]
SyslogServerIP = 10.15.77.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
```

TR069ACSPASSWORD = '\$1\$gQ=='

## AudioCodes

```
TR069CONNECTIONREQUESTPASSWORD = '$1$qQ=='
NTPServerIP = '10.15.27.1'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value
[BSP Params]
PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
[Analog Params]
[ControlProtocols Params]
AdminStateLockControl = 0
[MGCP Params]
[MEGACO Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
[PSTN Params]
[SS7 Params]
[Voice Engine Params]
ENABLEMEDIASECURITY = 1
[WEB Params]
LogoWidth = '145'
UseProductName = 1
;HTTPSPkeyFileName is hidden but has non-default value
[SIP Params]
MEDIACHANNELS = 200
SIPDESTINATIONPORT = 8934
GWDEBUGLEVEL = 5
ENABLESBCAPPLICATION = 1
```

```
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value
[SCTP Params]
[IPsec Params]
[Audio Staging Params]
[SNMP Params]
[ PhysicalPortsTable ]
FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 0, 4, "User Port #4", "None", "
                                                                   ";
PhysicalPortsTable 5 = "FE_5_2", 0, 4, "User Port #5", "None", "
                                                                   ";
PhysicalPortsTable 6 = "FE_5_3", 0, 4, "User Port #6", "None", "
                                                                   " :
PhysicalPortsTable 7 = "FE_5_4", 0, 4, "User Port #7", "None", "
                                                                   ";
PhysicalPortsTable 8 = "FE_5_5", 0, 4, "User Port #8", "None", "
                                                                   ";
PhysicalPortsTable 9 = "FE_5_6", 0, 4, "User Port #9", "None", " ";
PhysicalPortsTable 10 = "FE_5_7", 0, 4, "User Port #10", "None", "
                                                                    ";
PhysicalPortsTable 11 = "FE_5_8", 0, 4, "User Port #11", "None", " ";
[ \PhysicalPortsTable ]
[ EtherGroupTable ]
FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 0, "", "";
EtherGroupTable 5 = "GROUP_6", 0, "",
                                      "";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
```

## 

```
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP 10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";
[ \EtherGroupTable ]
[ DeviceTable ]
FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_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, 10.15.77.77, 16, 10.15.0.1, "Voice",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.153, 24, 195.189.192.129, "WANSP",
80.179.52.100, 80.179.55.100, "vlan 2";
[ \InterfaceTable ]
[ DspTemplates ]
  *** TABLE DspTemplates ***
;
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
[ \DspTemplates ]
[ WebUsers ]
FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$LE0VGBxUAQFSUAJXUQANXwoPDwtaeSNwInB2c3B+eihzKSgvfDIzMDI1YGc0YWhub2hlP
GpUVwdVBlNSBgpRXV4=", 1, 0, 2, 15, 60, 200,
"62cabed25276f6d59432fcaf295a1346";
WebUsers 1 = "User"
"$1$fRwcHLO4tOHmvOKy7Oiys7m5vrbzpqfyoKL0r6v7q/iv/P35kpmUwcXBkZWYy5iaz8+Wm
```

```
NGBgoPXhdTRi4yDj94=", 3, 0, 2, 15, 60, 50,
"e124fc45691a62316416e055a60edb6f";
[ \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 1 = "AudioCodersGroups_1";
[ \AudioCodersGroups ]
[ AllowedAudioCodersGroups ]
FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "S4B Allowed Coders";
AllowedAudioCodersGroups 1 = "BroadCloud Allowed Coders";
[ \AllowedAudioCodersGroups ]
[ IpProfile ]
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
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_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
```

# AudioCodes

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 1 = "S4B", 1, "AudioCodersGroups\_0", 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "AudioCodersGroups\_0", 0, 0, "", "S4B Allowed Coders", "", 0, 1, 1, 0, 0, 0, 0, 0, 0, 0; IpProfile 2 = "BroadCloud", 1, "AudioCodersGroups\_0", 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "AudioCodersGroups\_1", 0, 0, "", "BroadCloud Allowed Coders", "", 2, 1, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 3, 2, 1, 0,1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 300, -1, -1, 0, 1, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0; [ \IpProfile ] [ CpMediaRealm ] FORMAT CpMediaRealm\_Index = CpMediaRealm\_MediaRealmName, CpMediaRealm\_IPv4IF, CpMediaRealm\_IPv6IF, CpMediaRealm\_PortRangeStart, CpMediaRealm\_MediaSessionLeg, CpMediaRealm\_PortRangeEnd, CpMediaRealm\_IsDefault, CpMediaRealm\_QoeProfile, CpMediaRealm\_BWProfile, CpMediaRealm\_TopologyLocation; CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 250, 8499, 1, "", "", 0;

```
CpMediaRealm 1 = "MRWan", "WANSP", "", 6000, 250, 8499, 0, "", "", 1;
[ \CpMediaRealm ]
[ SBCRoutingPolicy ]
FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy LCREnable, SBCRoutingPolicy LCRAverageCallLength,
SBCRoutingPolicy LCRDefaultCost, SBCRoutingPolicy LdapServerGroupName;
SBCRoutingPolicy 0 = "Default SBCRoutingPolicy", 0, 1, 0, "";
[ \SBCRoutingPolicy ]
[ SRD ]
FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName;
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_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation;
SIPInterface 0 = "SIPInterface_LAN", "Voice", 2, 0, 0, 5067,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1,
0, 0;
SIPInterface 1 = "SIPInterface_WAN", "WANSP", 2, 0, 0, 5061,
"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 1 = "S4B", 1, 60, 1, 1, "DefaultSRD", 0, "default", 1, -1, "",
"", "SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 2 = "BroadCloud", 1, 60, 0, 1, "DefaultSRD", 0, "default", 1, 1,
"", "", "SIPInterface_WAN", "", "", 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 1 = 0, "S4B", "S4B", "interop.adpt-tech.com", "", -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;
IPGroup 2 = 0, "BroadCloud", "BroadCloud", "interop.adpt-tech.com", "", -
1, 0, "DefaultSRD", "MRWan", 1, "BroadCloud", -1, -1, 4, 0, 0, "", 0, -1,
-1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0,
0, -1, 0, 0, 1, "", -1;
[ \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, "hs2.fedsipt1.broadcloudgov.us", 2;
[ \ProxyIp ]
[ Account ]
FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "S4B", "BroadCloud", "8325624857",
"$1$jt/69vP78vC0ruL8uA==", "interop.adpt-tech.com", 1, "8325624857", 2;
[ \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 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "", "";
IP2IPRouting 1 = "S4B to ITSP", "Default_SBCRoutingPolicy", "S4B", "*"
"*", "*", "*", 0, "", "Any", 0, -1, 0, "BroadCloud", "", "", 0, -1, 0, 0,
"", "", "", "";
IP2IPRouting 2 = "ITSP to S4B", "Default_SBCRoutingPolicy", "BroadCloud",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "S4B", "", "", 0, -1, 0, 0,
"", "", "", "";
[ \IP2IPRouting ]
[ IPOutboundManipulation ]
FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation SrcUsernamePrefix, IPOutboundManipulation SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
```

# AudioCodes

```
IPOutboundManipulation CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
\label{eq:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:intro:
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "Add + toward S4B",
"Default_SBCRoutingPolicy", 0, "BroadCloud", "S4B", "*", "*", "*", "*",
"*", "", 0, "Any", 0, 1, 0, 0, 255, "+", "", 0, "", "";
IPOutboundManipulation 1 = "Change + to 011", "Default_SBCRoutingPolicy",
0, "S4B", "BroadCloud", "*", "*", "+", "*", "*", "", 0, "Any", 0, 1, 1,
0, 255, "011", "", 0, "", "";
IPOutboundManipulation 2 = "Remove + from Source",
"Default_SBCRoutingPolicy", 0, "S4B", "BroadCloud", "+8", "*", "*", "*", "*", "*", 0, "Any", 0, 0, 1, 0, 255, "", "", 0, "", "";
[ \IPOutboundManipulation ]
[ MessageManipulations ]
FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Call Forward", 4, "invite", "header.history-
info exists", "header.diversion", 0, "header.from", 0;
MessageManipulations 1 = "Call Forward", 4, "invite", "header.history-
info.0 regex (<sip:)(.)(.*)(@)(.*)", "header.diversion.url.user", 2,</pre>
"$3", 0;
MessageManipulations 2 = "Call Forward", 4, "", "header.history-
info", 1, "", 1;
MessageManipulations 3 = "Call Transfer", 4, "invite", "header.referred-
by exists", "header.referred-by.url.host", 2, "header.from.url.host", 0;
MessageManipulations 4 = "Call Transfer", 4, "invite", "header.referred-
by exists", "header.referred-by.url.user", 6, "'+'", 0;
MessageManipulations 5 = "Call Transfer", 4, "invite", "header.referred-
by exists", "header.from.url.user", 2, "header.referred-by.url.user", 0;
MessageManipulations 6 = "Reject Responses", 4, "any.response",
"header.request-uri.methodtype=='503'", "header.request-uri.methodtype",
2, "'480'", 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'"; 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 = "S4B Allowed Coders", 0, 1, ""; AllowedAudioCoders 1 = "S4B Allowed Coders", 1, 2, ""; AllowedAudioCoders 2 = "BroadCloud Allowed Coders", 0, 3, ""; AllowedAudioCoders 3 = "BroadCloud Allowed Coders", 1, 1, ""; AllowedAudioCoders 4 = "BroadCloud Allowed Coders", 2, 2, "";

```
[ \AllowedAudioCoders ]
```

[ AudioCoders ]

[ \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, 2, 2, 90, -1, 1, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 1, 2, 90, -1, 1, "";
AudioCoders 2 = "AudioCodersGroups_1", 0, 3, 2, 19, -1, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 1, 1, 2, 90, -1, 0, "";
AudioCoders 4 = "AudioCodersGroups_1", 2, 2, 2, 90, -1, 0, "";
```

This page is intentionally left blank.

#### **International Headquarters**

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

#### AudioCodes Inc.

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

Contact us: <u>www.audiocodes.com/contact</u> Website: <u>www.audiocodes.com</u>

©2017 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-12381

