AudioCodes Professional Services – Interoperability Lab

# Cisco Unified Communications Manager Ver.12 and Amazon Chime Voice Connector using AudioCodes Mediant<sup>™</sup> SBC

Version 7.2







### **Table of Contents**

1	Intro	duction	7
	1.1	Intended Audience	7
	1.2	About AudioCodes SBC Product Series	7
2	Com	ponent Information	9
	2.1	AudioCodes SBC Version	9
	2.2	AWS Chime Voice Connector Version	9
	2.3	IP-PBX Version	9
	2.4	Interoperability Test Topology	.10
		2.4.1 Environment Setup	.11
		2.4.2 Known Limitations	.11
3	Con	figuring Cisco CUCM	13
	3.1	Log in to Cisco Unified Communications Manager	.13
	3.2	Create a New Trunk	.13
	3.3	Create a New Route Pattern	.15
4	Con	figuring Amazon Chime Voice Connector	19
5	Con	figuring AudioCodes SBC	21
	5.1	Step 1: IP Network Interfaces Configuration	.22
		5.1.1 Step 1a: Configure VLANs	.23
		5.1.2 Step 1b: Configure Network Interfaces	.23
	5.2	Step 2: Configure Media Realms	.25
	5.3	Step 3: Configure SIP Signaling Interfaces	.28
	5.4	Step 4: Configure Proxy Sets	.30
	5.5	Step 5: Configure Coders	.34
	5.6	Step 6: Configure IP Profiles	.35
	5.7	Step 7: Configure IP Groups	.37
	5.8	Step 8: SIP ILS Connection Configuration (optional)	.39
		5.8.1 Step 8a: Configure the TLS version	.39
		5.8.3 Step 8c: Deploy Amazon Trusted Root Certificate	.41
	5.9	Step 9: Configure SRTP (optional)	.42
	5.10	Step 10: Configure IP-to-IP Call Routing Rules	.43
	5.11	Step 11: Configure IP-to-IP Manipulation Rules	.48
	5.12	Step 12: Configure Message Manipulation Rules	.53
	5.13	Step 13: Configure Account for Authentication	.55
	5.14	Step 14: Miscellaneous Configuration	.56
		5.14.1 Step 14a: Configure SBC Alternative Routing Reasons	.56
	5.15	Step 15: Reset the SBC	.57
Α	Aud	ioCodes INI File	59



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

This document is subject to change without notice.

Date Published: May-26-2019

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

### Stay in the Loop with AudioCodes



### Abbreviations and Terminology

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

### **Document Revision Record**

LTRT	Description
29320	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 website at <a href="https://online.audiocodes.com/documentation-feedback">https://online.audiocodes.com/documentation-feedback</a>.



This page is intentionally left blank.

# **1** Introduction

This Configuration Note describes how to set up the AudioCodes Session Border Controller (hereafter, referred to as *SBC*) for interworking between AWS Chime's Voice Connector and Cisco CUCM environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the 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 <u>https://www.audiocodes.com/partners/sbc-interoperability-list</u>.

### 1.1 Intended Audience

The document is intended for engineers, or AudioCodes and AWS Chime Partners who are responsible for installing and configuring AWS Chime's Voice Connector and Cisco CUCM for enabling VoIP calls using AudioCodes SBC.

### **1.2 About AudioCodes SBC Product Series**

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

The 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 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 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 SBC Version

### Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	<ul> <li>Mediant 500 Gateway &amp; 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, VE and CE)</li> </ul>
Software Version	7.20A.252.011
Protocol	<ul> <li>SIP/UDP or SIP/TCP or SIP/TLS (to the AWS Chime Voice Connector)</li> <li>SIP/TCP (to the Cisco CUCM)</li> </ul>
Additional Notes	None

## 2.2 AWS Chime Voice Connector Version

### Table 2-2: AWS Chime Version

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

## 2.3 IP-PBX Version

### Table 2-3: IP-PBX Version

Vendor	Cisco
Model	CUCM
Software Version	12.0.1
Protocol	SIP
Additional Notes	None

# 2.4 Interoperability Test Topology

The interoperability testing between AudioCodes SBC and AWS Chime Voice Connector with CUCM v12 was done using the following topology setup:

- Enterprise deployed with Cisco CUCM IP-PBX 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 AWS Chime's Voice Connector service.
- AudioCodes SBC is implemented to interconnect between the Enterprise LAN and the Voice Connector.
  - Session: Real-time voice session using the IP-based Session Initiation Protocol.
  - **Border:** IP-to-IP network border between IP-PBX network in the Enterprise LAN and AWS Chime's Voice Connector located in the public network.

The figure below illustrates this interoperability test topology:

#### Figure 2-1: Interoperability Test Topology between SBC and Cisco CUCM with AWS Chime Voice Connector



### 2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	<ul> <li>Cisco CUCM environment is located on the Enterprise's LAN</li> <li>AWS Chime Voice Connector is located on the WAN</li> </ul>
Signaling Transcoding	<ul> <li>Cisco CUCM operates with SIP-over-TCP transport type</li> <li>AWS Chime Voice Connector operates with SIP-over-UDP or SIP-over-TCP or SIP-over-TLS transport types</li> </ul>
Codecs Transcoding	<ul> <li>Cisco CUCM supports G.711A-law and G.711U-law coders</li> <li>AWS Chime Voice Connector supports G.711U-law coder</li> </ul>
Media Transcoding	<ul> <li>Cisco CUCM operates with RTP media type</li> <li>AWS Chime Voice Connector operates with RTP or SRTP media types</li> </ul>

### 2.4.2 Known Limitations

The following limitation was observed in the interoperability tests done for the AudioCodes SBC interworking between Cisco CUCM v.12 and AWS Chime's Voice Connector:

For inbound calling from AWS Chime Voice Connector to an IP-PBX, where the phone number being called isn't assigned an origination route, a busy/announcement should be heard however is not heard.

Amazon Chime Team is working on fixing this issue in the next release.



This page is intentionally left blank.

# **3 Configuring Cisco CUCM**

This section describes how to configure the Cisco Unified Communications Manager.

# 3.1 Log in to Cisco Unified Communications Manager

The procedure below describes how to log in to the Cisco CUCM Administration interface.

### > To log in to the Cisco Unified CM Administration interface:

1. Log in to the Cisco Unified CM Administration by entering the IP address of the Cisco Unified Communications Manager (CUCM) in the Web browser address field.

#### Figure 3-1: Cisco Unified CM Administration

India, Cisco Unified CM Administration     For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration Y Go
Cisco Unified CM Administration	Username Password Login Reset
Copyright © 1999 - 2017 Cisco Systems, Inc. All rights reserved.	
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Deliv	rery of Cisco cryptographic products does not imply third-party authority to import, export,

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distributes and even are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our <u>Expert Compliance Product Report</u> web site. For information about Cisco Unified Communications Manager please visit our <u>Unified Communications System Documentation</u> web site. For Cisco Technical Support please visit our <u>Technical Support</u> web site.

- 2. In the 'Username' field, enter the user name.
- 3. In the 'Password' field, enter the password.
- 4. Click Login.

## 3.2 Create a New Trunk

This section describes how to create a new trunk.

- To create a new trunk:
- 1. From the **Device** menu drop-down list, select **Trunk**.
- 2. Click Add New.

### Figure 3-2: Trunk page

վովո Cisco Unified CM Administration							Navigation Cisco Unified CM Administration 👻 GO										
cisco	For Cisco U	Unified Communio	ations Solutions										admin	Search Docume	ntation	About	Logout
System -	Call Routing 👻	Media Resources 👻	Advanced Features 👻	Device 👻	Application -	User Managemen	t <del>v</del> E	Bulk Administration	- Hel	ip 🔻							
Find and L	ist Trunks.																
Add Ne	ew																
Trunks																	
Find Trunk	s where Devic	ce Name	→ begins with     →	 Select iten	n or enter sear	Find Cl	ear Filt	er 🕂 📼									
					No a	ctive query. Plea	se ente	er your search crit	teria us	sing the op	tions above.						
Add Nev	v																

- **3.** Select Trunk Type **SIP Trunk**.
- 4. Click Next.



### Figure 3-3: Create Trunk Page

cisco	Cisco Unified CM Administration For Cisco Unified Communications Solutions		Navigation Cisco Unified CM Administration 🚽 Go admin Search Documentation About Logout
System - C	all Routing 👻 Media Resources 👻 Advanced Features 💌	Nevice ▼ Application ▼ User Management ▼ Bulk Administration ▼ Help ▼	
Trunk Confi	guration		Related Links: Back To Find/List 🔹 Go
Next			
Status (i) Status:	Ready		
Trunk Info	rmation		
Trunk Type Device Prote Trunk Servi	* SIP Trunk bool* SIP ce Type* None(Default)	•	
Next			

(i) \*- indicates required item.

- 5. In the **Device Name** field, enter a unique SIP Trunk name and optionally provide a description.
- 6. From the **Device Pool** drop-down list, select a device pool.

#### Figure 3-4: SIP Trunk Settings Page

System 👻 Call Routing 🗸 Media Resources 👻 Advanced Features 💌 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻

Trunk Configuration	_		Related Links: Back To Find/List	▼ Go
🔚 Save 🗶 Delete 🎱 Reset 🕂 Add New				
Status				<b>^</b>
(1) Status: Ready				
SIP Trunk Status				
Service Status: Unknown				
Duration: Time In Full Service: 1 day 5 hours 28 minutes				
- Davice Information				
Device Information	CID Truck			
Product: Device Protocol:	SIP			
Trunk Service Type	None(Default)			
Device Name*	SBC		]	
Description	10 15 77 55		]	
Device Pool*	Default	•		
Common Device Configuration	c None a	•		
Call Classification*	Lice System Default	•		
Media Resource Group List	ose system belaut	-		
Lesties*	< None >	-		
AAB Crown	Hub_None	-		
AAR Group	< None >	·		
	None	•		
QSIG Variant "	No Changes	Ŧ		
ASN.1 ROSE OID Encoding*	No Changes	T		
Packet Capture Mode*	None	•		
Packet Capture Duration	0			

7. Select the 'Redirecting Diversion Header Delivery – Outbound' check box.

#### Figure 3-5: Redirecting Diversion Header Delivery

Redirecting Diversion Header Delivery - Outbound							
Redirecting Party Transformation CSS	< None >	7					

8. Enter the Destination Address and Destination Port of the AudioCodes SBC.

### Figure 3-6: SIP Information Section

- SID Information				
Destination				
Destination Address is an SRV				
Destination Ad	ldress	Destination Address IPv6	Destination Port	Status
1* 10.15.77.55			5060	N/A
MTP Preferred Originating Codec*	711ulaw	•		
BLF Presence Group*	Standard Presence group	•		
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile	•		
Rerouting Calling Search Space	< None >	•		
Out-Of-Dialog Refer Calling Search Space	< None >	•		
SUBSCRIBE Calling Search Space	< None >	•		
SIP Profile*	MP1xx-SIP Profile	View Details		
DTMF Signaling Method*	No Preference	······		
	L			

- 9. From the SIP Trunk Security drop-down list, select a profile.
- **10.** From the **SIP Profile** drop-down list, select a profile.
- 11. Click Save.

### 3.3 Create a New Route Pattern

This section describes how to create a new route pattern.

- **To create new Route Pattern:**
- 1. From the **Call Routing** menu drop-down list, go to the **Route/Hunt** menu and select **Route Pattern**.

Figure 3-7: Route Pattern page

cisco	Cisco Unified CM Adr For Cisco Unified Communications	ninistration s Solutions	
System 👻	Call Routing 👻 Media Resources 👻	Advanced Features - Device - Application	👻 Us
Find and	AAR Group Dial Rules Route Filter		
Servers	Route/Hunt SIP Route Pattern	Route Group Local Route Group Names	
Find Serve	Intercom Class of Control	Route List Route Pattern	Find er your s
Add Nev	Client Matter Codes Forced Authorization Codes	Line Group	
	Translation Pattern Call Park	Hunt List Hunt Pilot	
	Directed Call Park Call Pickup Group		
	Directory Number Dial Plan Installer		

- 2. Click Add New.
- 3. Enter a Route Pattern according to schema (optionally provide a description).
- 4. From the **Gateway/Route List** drop-down list, select the SIP Trunk device name.

### Figure 3-8: Create Route Pattern Page

CISCO Unified CM Ad For Cisco Unified Communication	ministration ns Solutions	
System ▼ Call Routing ▼ Media Resources ▼	Advanced Features - Device - Application - User Managemen	t 👻 🛛 Bulk Ad
Route Pattern Configuration		
🔜 Save 🗙 Delete 🗋 Copy 🕂 Add N	lew	
Status Status: Ready		
Pattern Definition		
Route Pattern*	4XXX	
Route Partition	< None >	
Description	To SBC	
Numbering Plan	Not Selected 🔻	
Route Filter	< None > T	
MLPP Precedence*	Default 🔻	
Apply Call Blocking Percentage		
Resource Priority Namespace Network Domain	< None >	
Route Class*	Default	
Gateway/Route List*	SBC	(Edit)
Route Option	Route this pattern	
	Block this pattern No Error	
Call Classification * OffNet	τ	
External Call Control Profile < None >	<b></b>	
🗆 Allow Device Override 🗹 Provide Outside D	Dial Tone 🔲 Allow Overlap Sending 🔲 Urgent Priority	
Require Forced Authorization Code		
Authorization Level*		
Require Client Matter Code		

#### 5. Click Save.

### Figure 3-9: Added Route Pattern

abab	Cisco Ur	ified CM Administration	٢	lavigation Cisc	o Unified CM Administratio	on 🔻 Go
cisco	For Cisco Uni	fied Communications Solutions	admin	Search Do	cumentation About	Logout
System -	Call Routing 👻	Media Resources • Advanced Features • Device • Application • User Manageme	ent 👻 🛛 Bulk Adm	iinistration 👻	Help 👻	
Find and	l List Route Pat	erns				
🕂 Add	New Select	All Clear All 💥 Delete Selected				
Status-	ecords found					
Route	Patterns (1 - 7	of 7)			Rows per Pag	e 50 🔻
Find Rou	te Patterns where	Pattern 🔻 begins with 🔻 Find Clear Fi	ilter 🕂 📼			
	Pattern *	Description Part	ition Rou	ite Filter	Associated Device	Сору
	<u>1!</u>	National Calls to AT_T through AudioCodes SBC		5	BC-ATT	ß
	<u>1!#</u>	dial # to indicate end of dialing		5	BC-ATT	ß
	<u>1!9</u>	US Numbers		5	BC-ATT	ß
	<u>4XXX</u>	To SBC		5	BC	ß
	<u>972!</u>	to israel		5	BC-ATT	ß
	<u>972!#</u>	to israel		5	BC-ATT	ß
	<u>9XXX</u>	to Lync		L	<u>vnc</u>	6
Add Ne	w Select All	Clear All Delete Selected				

### Figure 3-10: Added Trunk

cisco	Cisco U	nified (	CM Administratio	on								N admin	lavigation Cisco Unified CM	Administration T GO
Sustam -	Call Bouting -	Modia Doa		a – Davias –	Applicatio	n – Unor	Managomo	at Dui	lk Adminic	tration -	Holp -			
System +	Call Routing •	Wedia Res	ources • Advanced realure	s • Device •	Applicatio	Jil 🔹 Osei	wanageme	n • Du	ik Auminis		ineip •	_		
Find and	List Trunks													
Add N	lew Selec		lear All 🕂 Delete Selecter	d 💁 Reset Se	elected									
-														
-Status-														
(1) 7 rec	cords found													
Trunks	(1 - 7 of 7)												Ro	ws per Page 50 🔻
Find Trunk	ks where Devic	e Name	▼ begins with ▼	1		Find	Clear Filt	er 🕂	-					
				Select item or	r enter sea	rch text 🔻	]							
		Name *	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status		SIP Trunk Duration	SIP Trunk Security Profile
		<u>Lync</u>	Lync Mediation Server		<u>Default</u>	<u>9XXX</u>				SIP	Full Service	Time	In Full Service: 1 day 5	Lync Security Profile
•		<u>SBC</u>	10.15.77.55		<u>Default</u>	<u>4XXX</u>				SIP	Full Service	Time	In Full Service: 1 day 5 40 minutes	Non Secure SIP Trunk Profile
		SBC-ATT			<u>Default</u>	<u>119</u>				SIP Trunk	Full Service	Time	In Full Service: 1 day 5 40 minutes	Non Secure SIP Trunk Profile
		SBC-ATT			<u>Default</u>	<u>1!</u>				SIP Trunk	Full Service	Time hours	In Full Service: 1 day 5 40 minutes	Non Secure SIP Trunk Profile
- 4		SBC-ATT			<u>Default</u>	<u>972!#</u>				SIP Trunk	Full Service	Time hours	In Full Service: 1 day 5 40 minutes	Non Secure SIP Trunk Profile
		SBC-ATT			<u>Default</u>	<u>972!</u>				SIP Trunk	Full Service	Time hours	In Full Service: 1 day 5 40 minutes	Non Secure SIP Trunk Profile
- 🖀		SBC-ATT			<u>Default</u>	<u>1!#</u>				SIP Trunk	Full Service	Time hours	In Full Service: 1 day 5 : 40 minutes	<u>Non Secure SIP</u> <u>Trunk Profile</u>
Add Nev	v Select All	Clear All	Delete Selected Reset S	elected										



Note: An '\*' indicates a mandatory field.



This page is intentionally left blank.

# 4 Configuring Amazon Chime Voice Connector

To configure Amazon Chime Voice Connector please refer to the following link: <u>https://docs.aws.amazon.com/chime/latest/ag/voice-connectors.html</u>



This page is intentionally left blank

# 5 Configuring AudioCodes SBC

This chapter provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Cisco CUCM and the AWS Chime Voice Connector. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and include the following main areas:

- SBC WAN interface AWS Chime Voice Connector environment
- SBC LAN interface CUCM environment

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

### Notes:

- For implementing CUCM and AWS Chime Voice Connector based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
  - √ 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, which can be found at AudioCodes web site



## 5.1 Step 1: IP Network Interfaces Configuration

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

- SBC interfaces with the following IP entities:
  - Cisco CUCM, located on the LAN
  - AWS Chime Voice Connector, located on the WAN
- 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, SBC connects to the LAN and DMZ using dedicated LAN ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

#### Figure 5-1: Network Interfaces in Interoperability Test Topology



### 5.1.1 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 5-2: Configured VLAN IDs in Ethernet Device

Ethernet Devices	; (2)			
+ New Edit 🕅	i	I≪ < Page 1 of 1 → ►I Show	10 🔻 records per pa	ge D
INDEX 🗢	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

### 5.1.2 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
-----------	-------

Nama	I AN IE (arbitrary descriptive name)
Name	<b>LAN_IF</b> (arbitrary descriptive name)
Ethernet Device	vlan 1
IP Address	10.15.17.77 (LAN IP address of SBC)
Prefix Length	<b>16</b> (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 SBC)
Prefix Length	<b>25</b> (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 5-3: Configured Network Interfaces in IP Interfaces Table

faces (2)								
Edit		🛯 < Page	1of1   ▶> ▶ S	Show 10 ▼ recor	rds per page			Q
NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
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
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
	faces (2) . Edit = ==================================	faces (2) .  Edit  NAME APPLICATION TYPE LAN_IF OAMP + Media + WAN_IF Media + Control	Edit       Image: Control of the second	Edit       Image I of 1       Image I	Edit       Image 1 of 1       Image 1 of 1       Image	Edit       Image:	Edit       Image       Image <th< th=""><th>Edit       Image       Page       of 1       Image       Tecords per page         NAME       APPLICATION TYPE       INTERFACE MODE       IP ADDRESS       PREFIX LENGTH       DEFAULT GATEWAY       PRIMARY DNS       SECONDARY DNS         LAN_IF       OAMP + Media +       IPV4 Manual       10.15.17.77       16       10.15.0.1       10.15.27.1       0.0.00         WAN_IF       Media + Control       IPV4 Manual       195.189.192.157       25       195.189.192.129       80.179.52.100       80.179.55.100</th></th<>	Edit       Image       Page       of 1       Image       Tecords per page         NAME       APPLICATION TYPE       INTERFACE MODE       IP ADDRESS       PREFIX LENGTH       DEFAULT GATEWAY       PRIMARY DNS       SECONDARY DNS         LAN_IF       OAMP + Media +       IPV4 Manual       10.15.17.77       16       10.15.0.1       10.15.27.1       0.0.00         WAN_IF       Media + Control       IPV4 Manual       195.189.192.157       25       195.189.192.129       80.179.52.100       80.179.55.100

## 5.2 Step 2: Configure Media Realms

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

### > To configure Media Realms:

- 1. Open the Media Realms table (Setup menu > Signaling & Media tab > Core Entities folder > Media Realms).
- 2. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

Parameter	Value
Index	0
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	<b>100</b> (media sessions assigned with port range)

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

ledia Realms [MRLan]				– x
GENERAL		QUALITY OF EXPERIENC	ΞE	
Index	0	QoE Profile	•	View
Name	• MRLan	Bandwidth Profile	•	View
Topology Location	Down 🔻			
IPv4 Interface Name	• #0 [LAN_IF] Vie	2W		
Port Range Start	• 6000			
Number Of Media Session Legs	• 100			
Port Range End	6999			
Default 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)

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

GENERAL					QUALITY OF EXPERIEN	NCE			
Index		1			QoE Profile	-	-	•	View
Name	•	MRWan			Bandwidth Profile	-	-	•	View
Topology Location		Up	۳						
IPv4 Interface Name	•	#1 [WAN_IF] •	Vi	ew					
Port Range Start	•	7000							
Number Of Media Session Legs	•	100							
Port Range End		7999							
Default Media Realm		No	۳						

The configured Media Realms are shown in the figure below:

Media Realn	וא (2) .					
+ New Edit	Ē	🛯 🛹 🏾 Page 👔	of 1 🕨 🕨 Show	10 🔻 records per pa	ge	Q
INDEX 🗢	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

# 5.3 Step 3: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the 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 and TCP Ports	5060
TLS Port	0
Media Realm	MRLan

**3.** Configure a SIP Interface for the WAN:

Parameter	Value
Index	1
Name	SIPInterface_WAN
Network Interface	WAN_IF
Application Type	SBC
UDP Port	5060
TCP Port	0
TLS Port	5061
Media Realm	MRWan

The configured SIP Interfaces are shown in the figure below:

Figure 5-7: Configured SIP Interfaces in SIP Interface Table

SIP Interf	aces (2)								
+ New Ec	dit 🛛 🗍 面		🔫 🛹 Page	e 1 of 1 🔛	► Show 10 ¥	records per pag	e		Q
INDEX 🗢	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATIN PROTOCOL	MEDIA REALM
0	SIPInterface_LA	DefaultSRD	LAN_IF	SBC	5060	5060	0	No encapsulation	MRLan
1	SIPInterface_W/	DefaultSRD	WAN_IF	SBC	0	5060	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.

## 5.4 Step 4: Configure Proxy Sets

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

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

- Cisco CUCM
- AWS Chime Voice Connector

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

### > To configure Proxy Sets:

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

Parameter	Value
Index	1
Name	CUCM12 (arbitrary name)
SBC IPv4 SIP Interface	SIPInterface_LAN
Proxy Keep-Alive	Using Options

#### Figure 5-8: Configuring Proxy Set for Cisco CUCM

Proxy	Sets [CUCM12]										– x
			SRD		#0 [	Defa	ultSRD]				
	GENERAL						REDUNDANCY				
	Index		1				Redundancy Mode			•	
	Name	•	CUCM12				Proxy Hot Swap		Disable	•	
	Gateway IPv4 SIP Interface			,	View		Proxy Load Balancing Method		Disable	•	
	SBC IPv4 SIP Interface	•	#0 [SIPInterface_LAN]	,	View		Min. Active Servers for Load Ba	alancing	1		
	TLS Context Name			,	View						
							ADVANCED				
	KEEP ALIVE						Classification Input	IP Address o	nly	•	
	Proxy Keep-Alive		Using OPTIONS		•		DNS Resolve Method			•	
	Proxy Keep-Alive Time [sec]		60								
	Keep-Alive Failure Responses										
				(	Cancel	A	APPLY				

- 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:

Proxy /	Address			-	x
	GENERAL				
	Index		0		
	Proxy Address	•	10.15.28.101:5060		
	Transport Type	•	TCP v		
	Proxy Priority		0		
	Proxy Random Weight		0		

Figure 5-9: Configuring Proxy Address for Cisco CUCM

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

Parameter	Value
Index	0
Proxy Address	<b>10.15.28.101:5060</b> (IP-PBX IP address / FQDN and destination port)
Transport Type	ТСР

d. Click Apply.

3. Configure a Proxy Set for the AWS Chime Voice Connector:

Parameter	Value
Index	2
Name	AWS-Chime
SBC IPv4 SIP Interface	SIPInterface_WAN
Proxy Keep-Alive	Using Options



	SRD	#0 [Def	faultSRD]			
GENERAL			REDUNDANCY			
Index	2		Redundancy Mode			•
Name	AWS-Chime		Proxy Hot Swap		Disable	•
Gateway IPv4 SIP Interface	<b>v</b>	ïew	Proxy Load Balancing Method		Disable	•
SBC IPv4 SIP Interface	• #1 [SIPInterface_WAN] 🔻 V	ïew	Min. Active Servers for Load Ba	llancing	1	
TLS Context Name	V	ïew				
			ADVANCED			
KEEP ALIVE			Classification Input	IP Address o	nly	•
Proxy Keep-Alive	Using OPTIONS	•	DNS Resolve Method			•
Proxy Keep-Alive Time [sec]	60					
Keep-Alive Failure Responses						

Figure 5-10: Configuring Proxy Set for AWS Chime Voice Connector

- 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 5-11: Configuring Proxy Address for AWS Chime Voice Connector

Proxy A	ddress		– x
	GENERAL		
	Index	0	
	Proxy Address	• dt3ynfnrl41vhejg9rtlfz.voiceconnector.chime.aws:5060	
	Transport Type	• TCP •	
	Proxy Priority	0	
	Proxy Random Weight	0	

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

Parameter	Value
Index	0
Proxy Address	dt3ynfnrl41vhejg9rtlfz.voiceconnector.chime.aws: 5060 (FQDN and destination port of your enterprise voice connector ID)
Transport Type	TCP or TLS (according to connection requirement)
d. Click Apply.	

The configured Proxy Sets are shown in the figure below:

Ciaura	E 49.	Configu	unad Dra	Way Cata	in Dro	Way Cata	Tabla
ridure.	<b>D-1Z</b>	Connat	irea Pro	xv Sels	III Pro	xv Sels	rable

Proxy Sets	(3)						
+ New Edit		14 <4	Page 1 of 1 🔛	► Show 10 ▼ re	cords per page		Q
INDEX 🗢	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP- ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)		SIPInterface_LAN	60		Disable
1	CUCM12	DefaultSRD (#0)		SIPInterface_LAN	60		Disable
2	AWS-Chime	DefaultSRD (#0)		SIPInterface_WAN	60		Disable

# 5.5 Step 5: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Cisco CUCM may support different coders while the AWS Chime Voice Connector supports only G.711 U-law coder, you need to add a Coder Group with the G.711 U-law coder for the AWS Chime Voice Connector.

Note that the Coder Group ID for this entity will be assigned 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 AWS Chime Voice Connector:

Parameter	Value
Coder Group Name	AudioCodersGroups_0
Coder Name	G.711 U-law

#### Figure 5-13: Configuring Coder Group for AWS Chime Voice Connector

(	Coder Groups									
	Coder Group Name 0 : AudioCodersGroups_0   Delete Group									
	Coder Name		Packetization	Time	Rate		Payload Type	Silence Suppression	Coder Specific	
	G.711U-law	•	20	•	64	•	0	Disabled 🔹		
		•		T		•		<b>.</b>		

### 5.6 Step 6: Configure IP Profiles

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

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

- Cisco CUCM to operate in non-secure mode using RTP and SIP over TCP
- AWS Chime Voice Connector to operate in non-secure mode using RTP and SIP over UDP
- > To configure IP Profile for CISCO CUCM:
- 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	CUCM12
Media Security	
SBC Media Security Mode	RTP

#### Figure 5-14: Configuring IP Profile for Cisco CUCM

files [CUCM12]					
GENERAL			SBC SIGNALING		
Index 1			PRACK Mode	Transparent	•
Name • CU(	CM12		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	RTP	•	Remote Update Support	Supported	•
Gateway Media Security Mode	Preferable	•	Remote re-INVITE	Supported	۳
Symmetric MKI	Disable	•	Remote Delayed Offer Support	Supported	•
MKI Size	0		Remote Representation Mode	According to Operation Mode	•
SBC Enforce MKI Size	Don't enforce	•	Keep Incoming Via Headers	According to Operation Mode	•
SBC Media Security Method	SDES	•	Keep Incoming Routing Headers	According to Operation Mode	•
Reset SRTP Upon Re-key	Disable	•	Keep User-Agent Header	According to Operation Mode	•
		Cancel	ΑΡΡΙΥ		

### > To configure an IP Profile for the AWS Chime Voice Connector:

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

Parameter	Value		
General			
Index	2		
Name	AWS-Chime		
Media Security			
SBC Media Security Mode	<b>RTP</b> or <b>SRTP</b> (according to connection requirement)		
SBC Media			
Extension Coders Group	AudioCodersGroups_0		
RFC 2833 Mode	<b>Extended</b> (in case CUCM is configured without support for RFC 2833)		
SBC Signaling			
P-Asserted-Identity Header Mode	Add (required for anonymous calls)		
Remote Delayed Offer Support	Not Supported		

### Figure 5-15: Configuring IP Profile for AWS Chime Voice Connector

IP Profi	IP Profiles [AWS-Chime] – x								
	GENERAL					SBC SIGNALING			
	Index	2				PRACK Mode	Transparent	•	
	Name •	AWS	5-Chime			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	•	RTP	•		Remote Update Support	Supported	•	
	Gateway Media Security Mode		Preferable	•		Remote re-INVITE	Supported	•	
	Symmetric MKI		Disable	•		Remote Delayed Offer Support •	Not Supported	•	
	MKI Size		0			Remote Representation Mode	According to Operation Mode	•	
	SBC Enforce MKI Size		Don't enforce	•		Keep Incoming Via Headers	According to Operation Mode	•	
	SBC Media Security Method		SDES	•		Keep Incoming Routing Headers	According to Operation Mode	•	
	Reset SRTP Upon Re-key		Disable	•		Keep User-Agent Header	According to Operation Mode	•	
			C	ancel	AF	PPLY			

# 5.7 Step 7: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the 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:

- Cisco CUCM located on LAN
- AWS Chime Voice Connector located on WAN
- > To configure IP Groups:
- Open the IP Groups table (Setup menu > Signaling & Media tab > Core Entities folder > IP Groups).
- 2. Add an IP Group for the Cisco CUCM:

Parameter	Value
Index	1
Name	CUCM12
Туре	Server
Proxy Set	CUCM12
IP Profile	CUCM12
Media Realm	MRLan
SIP Group Name	(FQDN of your enterprise AWS Chime Voice Connector ID)

3. Configure an IP Group for the AWS Chime Voice Connector:

Parameter	Value
Index	2
Name	AWS-Chime
Topology Location	Up
Туре	Server
Proxy Set	AWS-Chime
IP Profile	AWS-Chime
Media Realm	MRWan
SIP Group Name	(FQDN of your enterprise AWS Chime voice connector ID)



The configured IP Groups are shown in the figure below:

### Figure 5-16: Configured IP Groups in IP Group Table

IP Grou	ups (3)										
+ New	Edit 🗌 🖬			🛯 < Page 1	of 1 🕨	► Show 10	<ul> <li>records p</li> </ul>	oer page			Q
INDEX 🗢	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
0	Default_IPG	DefaultSF	Server	Not Configur	ProxySet_0				Disable	-1	-1
1	CUCM12	DefaultSF	Server	Not Configur	CUCM12	CUCM12	MRLan	dt3ynfnrl41v	Enable	-1	2
2	AWS-Chime	DefaultSF	Server	Not Configur	AWS-Chime	AWS-Chime	MRWan	dt3ynfnrl41v	Enable	-1	-1

## 5.8 Step 8: SIP TLS Connection Configuration (optional)

This section describes how to configure the SBC for using a TLS connection with the AWS Chime Voice Connector. This is essential for a secure SIP TLS connection and highly recommended by Amazon.

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

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or a third-party server) to ensure that the 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., **8.8.8.8**).

### Figure 5-17: Configuring NTP Server Address

NTP SERVER	
Enable NTP	Enable •
Primary NTP Server Address (IP or FQDN) •	8.8.8.8
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

### 5.8.2 Step 8b: Configure the TLS version

This step describes how to configure the SBC to use TLS version 1.2 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 'TLSv1.2'

TLS Contexts [default]							– x
GENERAL				OCSP			
Index		0		OCSP Server	Disable	•	
Name	•	default		Primary OCSP Server	0.0.0.0		
TLS Version	•	TLSv1.2	]	Secondary OCSP Server	0.0.0.0		
DTLS Version		Any 🔻		OCSP Port	2560		
Cipher Server		DEFAULT		OCSP Default Response	Reject	•	
Cipher Client		DEFAULT					
Strict Certificate Extension Validation		Disable •					
DH key Size		1024 🔻					
		Canc	el	APPLY			

#### Figure 5-18: Configuring TLS version

### 5.8.3 Step 8c: Deploy Amazon Trusted Root Certificate

This step describes how to import the Amazon Chime root certificate. Currently the Amazon Chime Voice Connector service uses a wildcard certificate (\*.voiceconnector.chime.aws). To trust this certificate, your SBC *must* import this certificate to its Trusted Certificates storage. Download the certificate from <a href="https://s3.amazonaws.com/voice-connector-certs/combined-ca-bundle.pem">https://s3.amazonaws.com/voice-connector-certs/combined-ca-bundle.pem</a>. Follow the steps below to import the certificate to the Trusted Root storage.

- > To configure a certificate:
- 1. 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 **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 5-19: Importing Root Certificate into Trusted Certificates Store

Import New Certificate	×
Choose File combined-ca-bundle.pem	
Ok Cancel	

4. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

# 5.9 Step 9: Configure SRTP (optional)

This step describes how to configure media security. If the AWS Chime Voice Connector requires SRTP, configure the SBC to operate in the same manner. Note that SRTP is enabled for the AWS Chime Voice Connector when you configure an IP Profile (see Section 5.5 on page 34).

- > To configure media security:
- Open the Media Security page (Setup menu > Signaling & Media tab > Media folder > Media Security).

Media Security			
GENERAL			
Media Security	• En	able	•
Media Security Behavior	Pre	eferable	•
Offered SRTP Cipher Suites	All		•
Aria Protocol Support	Dis	sable	•
MASTER KEY IDENTIFIER			
Master Key Identifier (MKI) Size	0		
Symmetric MKI	Dis	sable	•

Figure 5-20: Configuring SRTP

- 2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
- 3. Click Apply.

# 5.10 Step 10: 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 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 5.7 on page 33,) 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 Cisco CUCM (LAN) and AWS Chime Voice Connector (DMZ):

- Terminate SIP OPTIONS messages on the SBC that are received from the both LAN and DMZ
- Calls from Cisco CUCM to AWS Chime Voice Connector
- Calls from AWS Chime Voice Connector to Cisco CUCM
- **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	Internal
Internal Action	Reply (Response='200')



	D D II				
	Routing Policy	#0 [Defa	ult_SBCRoutingPolicy]		
GENERAL			ACTION		
Index	0		Destination Type	<ul> <li>Internal</li> </ul>	•
Name	Terminate OPTIONS		Destination IP Group		▼ View
Alternative Route Options	Route Row	Ŧ	Destination SIP Interface		▼ View
			Destination Address		
MATCH			Destination Port	0	
Source IP Group	Any	▼ View	Destination Transport Type		•
Request Type	OPTIONS	•	IP Group Set		✓ View
Source Username Pattern	*		Call Setup Rules Set ID	-1	
Source Host	*		Group Policy	Sequential	٣
Source Tag			Cost Group		▼ View

Figure 5-21: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

- 4. Configure a rule to route calls from Cisco CUCM to AWS Chime Voice Connector:
  - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	<b>CUCM12 to AWS-Chime</b> (arbitrary descriptive name)
Source IP Group	CUCM12
Destination Type	IP Group
Destination IP Group	AWS-Chime

### Figure 5-22: Configuring IP-to-IP Routing Rule for Cisco CUCM to AWS-Chime

IP-to-IP Routing [CUCM12 to AWS-Chime] x							
	Routing Policy #0 [D	efault_SBCRoutingPolicy]					
GENERAL		ACTION					
Index	1	Destination Type	IP Group				
Name •	CUCM12 to AWS-Chime	Destination IP Group	• #2 [AWS-Chime] • View				
Alternative Route Options	Route Row 🔻	Destination SIP Interface	View				
		Destination Address					
MATCH		Destination Port	0				
Source IP Group	• #1 [CUCM12]	Destination Transport Type	v				
Request Type	All	IP Group Set	• View				
Source Username Pattern	*	Call Setup Rules Set ID	-1				
Source Host	*	Group Policy	Sequential 🔻				
Source Tag		Cost Group	<b>v</b> iew				
	Cance	APPLY					

b. Click Apply.

- 5. Configure rule to route calls from AWS Chime Voice Connector to Cisco CUCM:
  - **a.** Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	4
Route Name	<b>AWS-Chime to CUCM12</b> (arbitrary descriptive name)
Source IP Group	AWS-Chime
Destination Type	IP Group
Destination IP Group	CUCM12

### Figure 5-23: Configuring IP-to-IP Routing Rule for AWS-Chime to Cisco CUCM Server

IP-to-IP Routing [AWS-Chime to CUCM12] – x							
Routing Policy	#0 [De	fault_SBCRoutingPolicy]					
GENERAL		ACTION					
Index 2		Destination Type	IP Group	•			
Name • AWS-Chime to CUCM12		Destination IP Group	#1 [CUCM12]	View			
Alternative Route Options Route Row	•	Destination SIP Interface	•	View			
		Destination Address					
MATCH		Destination Port	0				
Source IP Group • #2 [AWS-Chime]	▼ View	Destination Transport Type		•			
Request Type All	•	IP Group Set	•	View			
Source Username Pattern *		Call Setup Rules Set ID	-1				
Source Host *		Group Policy	Sequential	•			
Source Tag		Cost Group		View			
	Cancel	APPLY					

The configured routing rules are shown in the figure below:

IP-to-IP Routing (3) .											
+ New	Edit Insert	±.∓.1	<b>i</b> 14	e 🛹 Page 1	of 1 🔛	► Show 10	<ul> <li>records per</li> </ul>	page			Q
INDEX 🗢	NAME	ROUTING POLICY	ALTERNATIV ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATIO USERNAME PATTERN	DESTINATIO TYPE	DESTINATIO	DESTINATIO SIP INTERFACE	DESTINATIC ADDRESS
0	OPTIONS Ter	Default_SBCI	Route Row	Any	OPTIONS	*	*	Internal			
1	CUCM12 to A	Default_SBCF	Route Row	CUCM12	All	*	*	IP Group	AWS-Chime		
2	AWS-Chime t	Default_SBCF	Route Row	AWS-Chime	All	*		IP Group	CUCM12		



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

# 5.11 Step 11: 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 5.7 on page 33) to denote the source and destination of the call.



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

For example, the AWS Chime requires that the dialed number be displayed in E.164 format. However the Cisco CUCM doesn't support the "+" (plus sign) in the phone number. So, for the interoperability, a manipulation is configured to add the "+" (plus sign) to the destination number (if it does not exist) for calls from the CUCM Server IP Group to the AWS Chime Voice Connector IP Group for any destination username pattern. In the opposite direction, strip the "+" (plus sign) from the phone number for calls from the AWS Chime Voice Connector IP Group to the CUCM Server IP Group.

### > To configure a number manipulation rule:

Open the Outbound Manipulations table (Setup menu > Signaling & Media tab > SBC folder > Manipulation > Outbound Manipulations).

Parameter	Value
Index	0
Name	Do Nothing
Source IP Group	CUCM12
Destination IP Group	AWS-Chime
Destination Username Pattern	+ (plus sign)
Manipulated Item	Destination URI

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

	Routing Policy	#0 [Defa	ult_SBCRoutingPolicy]	
GENERAL			ACTION	
Index	0		Manipulated Item	Destination URI
Name	Do Nothing		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	Ŧ	Privacy Restriction Mode	Transparent <b>•</b>
Source IP Group	• #1 [CUCM12]	▼ View		
Destination IP Group	• #2 [AWS-Chime]	▼ View		
Source Username Pattern	*			

Figure 5-25: Configuring IP-to-IP Outbound Manipulation Rule

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

Parameter	Value
Index	1
Name	Add +
Source IP Group	CUCM12
Destination IP Group	AWS-Chime
Destination Username Pattern	* (asterisk sign)
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

### Figure 5-26: Configuring IP-to-IP Outbound Manipulation Rule

Outbound Manipulations [Add	+]			- x
	Routing Policy	#0 [Defa	ault_SBCRoutingPolicy]	•
GENERAL			ACTION	
Index	1		Manipulated Item	Destination URI
Name •	Add +		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	• #1 [CUCM12]	▼ View		
Destination IP Group	• #2 [AWS-Chime]	▼ View		
Source Username Pattern	*			
		Cancel	APPLY	

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

Parameter	Value
Index	2
Name	Strip + towards CUCM12
Source IP Group	AWS-Chime
Destination IP Group	CUCM12
Destination Username Pattern	+ (plus sign)
Manipulated Item	Destination URI
Remove From Left	1

### Figure 5-27: Configuring IP-to-IP Outbound Manipulation Rule

Outbound Manipulations [Stri	p + towards CUCM12]			- x
	Routing Policy	#0 [Defa	ult_SBCRoutingPolicy]	<b>r</b>
GENERAL			ACTION	
Index	2		Manipulated Item	Destination URI
Name •	Strip + towards CUCM12		Remove From Left	1
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 [AWS-Chime]	▼ View		
Destination IP Group	• #1 [CUCM12]	▼ View		
Source Username Pattern	*			
		Cancel	APPLY	

**C**audiocodes

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between CUCM Server IP Group and AWS Chime Voice Connector IP Group:

Figure 5-28: Example of Configured IP-to-IP Outbound Manipulation Rules

Outbo	Outbound Manipulations (3)												
+ New	Edit Inser	t ± ∓	Ê	14 <4	Page 1	of1 🌬 🖬 S	Show 10 ▼ r	ecords per pag	;e				Q
INDEX ≑	NAME	ROUTING POLICY	ADDITIONAI MANIPULAT	SOURCE IP GROUP	DESTINATIO	SOURCE USERNAME PATTERN	DESTINATIC USERNAME PATTERN	MANIPULAT ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Do Nothing	Default_SBC	No	CUCM12	AWS-Chime	*	+	Destination	0	0	255		
1	Add +	Default_SBC	No	CUCM12	AWS-Chime	*	*	Destination	0	0	255	+	
2	Strip + towa	Default_SBC	No	AWS-Chime	CUCM12	*	+	Destination	1	0	255		

Rule Index	Description
0	Calls from CUCM12 IP Group to AWS-Chime IP Group with the prefix destination number "+", do nothing.
1	Calls from CUCM12 IP Group to AWS-Chime IP Group with any destination number (*), add "+" to the prefix of the destination number.
2	Calls from AWS-Chime IP Group to CUCM12 IP Group with the prefix destination number "+", remove one character from the left (remove "+").

# 5.12 Step 12: 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).
- Configure a manipulation rule (Manipulation Set 2) for the Cisco CUCM server. This rule applies to messages sent to the CUCM Server IP Group. This replaces the host part of the SIP Request-URI Header with the CUCM Server IP address.

Parameter	Value
Index	0
Name	Change R-URI host toward CUCM12
Manipulation Set ID	2
Message Type	Any.Request
Action Subject	Header.Request-URI.URL.Host
Action Type	Modify
Action Value	Param.Message.Address.Dst.Address

#### Figure 5-29: Configuring SIP Message Manipulation Rule 0 (for CUCM12)

Message Manipulations [Chang	ge RUI host toward CUCM12]			– ×
GENERAL		ACTION		
Index Name <b>Manipulation Set ID</b> Row Role	0       • Change RUI host toward CUCM12       • 2       Use Current Condition	Action Subject Action Type Action Value	header.request-uri.url.host     Modify     param.message.address.dst.address	Editor • Editor
MATCH				
Message Type 🔹	Any Editor			
Condition	Editor			
	Cancel	APPLY		



**Note:** Due to fact that Cisco CUCM can be configured in different ways (e.g. to use SIP REFER Message or Re-INVITE for Call Transfer scenarios), different Message Manipulation Rules may needrequired to be configured.

- 3. Assign Manipulation Set ID 2 to the CUCM Server IP Group:
  - Open the IP Groups table (Setup menu > Signaling & Media tab > Core Entities folder > IP Groups).
  - b. Select the row of the CUCM Server IP Group, and then click Edit.
  - c. Set the 'Outbound Message Manipulation Set' field to 2.

IP Groups [CUCM12] – x								
		SRD	#0 [D	efaultSRD]				
GENERAL				QUALITY OF EXPERIENCE				
Index		1		QoE Profile			•	View
Name	•	CUCM12		Bandwidth Profile			•	View
Topology Location		Down	•					
Туре		Server	•	MESSAGE MANIPULATION				
Proxy Set	•	#1 [CUCM12]	View	Inbound Message Manipulation	on Set	-1		
IP Profile	•	#1 [CUCM12]	View	Outbound Message Manipulat	tion Set •	2		
Media Realm	•	#0 [MRLan]	View	Message Manipulation User-De	efined String 1			
Contact User				Message Manipulation User-De	efined String 2			
SIP Group Name	•	dt3ynfnrl41vhejg9rtlfz.voiceconnector.chime	.aws	Proxy Keep-Alive using IP Grou	up settings	Disable		Ŧ
Created By Routing Ser	/er	No						
Cancel APPLY								

## 5.13 Step 13: Configure Account for Authentication

This step describes how to configure the SIP account for authentication purposes. Amazon Chime Voice Connector requires IP-based whitelisting for outbound calling. Consequently, the SBC needs to be configured with the appropriate credentials using the Accounts Table. In the interoperability test topology, the Served IP Group is CUCM Server and the Serving IP Group is AWS Chime Voice Connector.

#### > To configure a SIP account for authentication:

- 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
Name	AWS Chime Authentication (arbitrary descriptive name)
Application Type	SBC
Served IP Group	CUCM12
Serving IP Group	AWS-Chime
Contact User	audiocodes (per Chime Voice Connector configuration)
Username	According to Chime Voice Connector configuration
Password	According to Chime Voice Connector configuration

#### Figure 5-31: Configuring a SIP Authentication Account

ccounts [AWS Chime Authenticati	on]	- >
GENERAL	CREDENTIALS	
Index	0 User Name audiocodes	
Name	AWS Chime Authentication     Password     ·	
Served Trunk Group	-1	
Application Type	• SBC •	
Served IP Group	• #1 [CUCM12] • View	
Serving IP Group	• #2 [AWS-Chime] View	
Host Name		
Contact User	audiocodes	
Register	No	
Registrar Stickiness	Disable •	
Registrar Search Mode	Current Working Server	
Re-REGISTER on INVITE Failure	Disable •	
	Cancel APPLY	

4. Click Apply.

### 5.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

### 5.14.1 Step 14a: Configure SBC Alternative Routing Reasons

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

- > To configure SIP reason codes for alternative IP routing:
- Open the Alternative Routing Reasons table (Setup menu > Signaling & Media tab > SBC folder > Routing > Alternative Reasons).
- 2. Click New.
- 3. From the 'Release Cause' drop-down list, select **503 Service Unavailable**.

#### Figure 5-32: SBC Alternative Routing Reasons Table

Alternativ	e Routing Reasons		- x
	GENERAL	0	*
	Release Cause	• 503 Service Unavailable	
		Cancel APPLY	

## 5.15 Step 15: Reset the SBC

After you have completed the configuration of the SBC described in this chapter, save ("burn") the configuration to the 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 5-33: Resetting the SBC

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

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



This page is intentionally left blank.

# A AudioCodes INI File

The *ini* configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 19, 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: M800B
;Board Type: 72
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 7.20A.252.011
;DSP Software Version: 5014AE3 R => 710.16
;Board IP Address: 10.15.77.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M Flash size: 64M Core speed: 500Mhz
;Num of DSP Cores: 3
;Num of physical LAN ports: 4
; Profile: NONE
;;;Key features:;Board Type: M800B ;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 ;DSP Voice
features: RTCP-XR ;DATA features: ;Channel Type: DspCh=30 IPMediaDspCh=30
;HA ;E1Trunks=1 ;T1Trunks=1 ;FXSPorts=4 ;FXOPorts=0 ;BRITrunks=4 ;IP
Media: Conf VXML ; QOE features: VoiceQualityMonitoring MediaEnhancement
;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;Control Protocols: MGCP SIP SBC=250 TEAMS MSFT FEU=100 TestCall=100
;Default features:;Coders: G711 G726;
;----- HW components -----
;
; Slot # : Module type : # of ports
                            _____
      ------
     1 : FALC56
                    : 1
;
      2 : FXS
                     : 4
;
     3 : BRI
                    : 4
;-----
[SYSTEM Params]
SyslogServerIP = 10.10.10.10
EnableSyslog = 0
NTPServerUTCOffset = 7200
HALocalMAC = '00908f50dcb2'
TR069ACSPASSWORD = '$1$qQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$qQ=='
NTPServerIP = '8.8.8.8'
```

# **C**audiocodes

```
SBCWizardFilename = 'templates4.zip'
[BSP Params]
PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
[Analog Params]
[ControlProtocols Params]
AdminStateLockControl = 0
[PSTN Params]
LineCode = 2
V5ProtocolSide = 0
[Voice Engine Params]
ENABLEMEDIASECURITY = 1
PLThresholdLevelsPerMille 0 = 5
PLThresholdLevelsPerMille 1 = 10
PLThresholdLevelsPerMille 2 = 20
PLThresholdLevelsPerMille 3 = 50
CallProgressTonesFilename = 'usa tones 13.dat'
[WEB Params]
[SIP Params]
GWDEBUGLEVEL = 5
SIPGATEWAYNAME = 'audiocodes@test'
USEGATEWAYNAMEFOROPTIONS = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
USEPINGPONGKEEPALIVE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
[ 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, 10.15.77.55, 16, 10.15.0.1, "LAN IF",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.150, 24, 195.189.192.129, "WAN IF",
80.179.52.100, 80.179.55.100, "vlan 2";
[ \InterfaceTable ]
[ 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", 4, 0, "DEFAULT", "DEFAULT", 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 ]
[ IpProfile ]
FORMAT IpProfile Index = IpProfile ProfileName, IpProfile IpPreference,
IpProfile CodersGroupName, IpProfile IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile IPDiffServ, IpProfile SigIPDiffServ,
IpProfile RTPRedundancyDepth, IpProfile CNGmode,
IpProfile VxxTransportType, IpProfile NSEMode, IpProfile IsDTMFUsed,
IpProfile PlayRBTone2IP, IpProfile EnableEarlyMedia,
IpProfile ProgressIndicator2IP, IpProfile EnableEchoCanceller,
IpProfile CopyDest2RedirectNumber, IpProfile MediaSecurityBehaviour,
IpProfile CallLimit, IpProfile DisconnectOnBrokenConnection,
IpProfile FirstTxDtmfOption, IpProfile SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile VoiceVolume, IpProfile AddIEInSetup,
IpProfile SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile SBCAllowedMediaTypes, IpProfile SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile SBCAlternativeDTMFMethod, IpProfile SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile AMDSensitivityLevel, IpProfile AMDMaxGreetingTime,
IpProfile AMDMaxPostSilenceGreetingTime, IpProfile SBCDiversionMode,
IpProfile SBCHistoryInfoMode, IpProfile EnableQSIGTunneling,
```

IpProfile SBCFaxCodersGroupName, IpProfile SBCFaxBehavior, IpProfile SBCFaxOfferMode, IpProfile SBCFaxAnswerMode, IpProfile SbcPrackMode, IpProfile SBCSessionExpiresMode, IpProfile SBCRemoteUpdateSupport, IpProfile SBCRemoteReinviteSupport, IpProfile\_SBCRemoteDelayedOfferSupport, IpProfile\_SBCRemoteReferBehavior, IpProfile SBCRemote3xxBehavior, IpProfile SBCRemoteMultiple18xSupport, IpProfile SBCRemoteEarlyMediaResponseType, IpProfile SBCRemoteEarlyMediaSupport, IpProfile EnableSymmetricMKI, IpProfile MKISize, IpProfile SBCEnforceMKISize, IpProfile\_SBCRemoteEarlyMediaRTP, IpProfile\_SBCRemoteSupportsRFC3960, IpProfile SBCRemoteCanPlayRingback, IpProfile EnableEarly183, IpProfile EarlyAnswerTimeout, IpProfile SBC2833DTMFPayloadType, IpProfile SBCUserRegistrationTime, IpProfile ResetSRTPStateUponRekey, IpProfile AmdMode, IpProfile SBCReliableHeldToneSource, IpProfile\_GenerateSRTPKeys, IpProfile\_SBCPlayHeldTone, IpProfile\_SBCRemoteHoldFormat, IpProfile\_SBCRemoteReplacesBehavior, IpProfile SBCSDPPtimeAnswer, IpProfile SBCPreferredPTime, IpProfile\_SBCUseSilenceSupp, IpProfile SBCRTPRedundancyBehavior, IpProfile SBCPlayRBTToTransferee, IpProfile SBCRTCPMode, IpProfile SBCJitterCompensation, IpProfile\_SBCRemoteRenegotiateOnFaxDetection, IpProfile JitterBufMaxDelay, IpProfile\_SBCUserBehindUdpNATRegistrationTime, IpProfile SBCUserBehindTcpNATRegistrationTime, IpProfile SBCSDPHandleRTCPAttribute, IpProfile\_SBCRemoveCryptoLifetimeInSDP, IpProfile\_SBCIceMode, IpProfile\_SBCRTCPMux, IpProfile\_SBCMediaSecurityMethod, IpProfile\_SBCHandleXDetect, IpProfile\_SBCRTCPFeedback, IpProfile SBCRemoteRepresentationMode, IpProfile SBCKeepVIAHeaders, IpProfile SBCKeepRoutingHeaders, IpProfile SBCKeepUserAgentHeader, IpProfile SBCRemoteMultipleEarlyDialogs, IpProfile\_SBCRemoteMultipleAnswersMode, IpProfile\_SBCDirectMediaTag, IpProfile SBCAdaptRFC2833BWToVoiceCoderBW, IpProfile\_CreatedByRoutingServer, IpProfile\_SBCFaxReroutingMode, IpProfile SBCMaxCallDuration, IpProfile SBCGenerateRTP, IpProfile SBCISUPBodyHandling, IpProfile SBCISUPVariant, IpProfile SBCVoiceQualityEnhancement, IpProfile SBCMaxOpusBW, IpProfile\_SBCEnhancedPlc, IpProfile\_LocalRingbackTone, IpProfile\_LocalHeldTone, IpProfile\_SBCGenerateNoOp, IpProfile SBCRemoveUnKnownCrypto; IpProfile 1 = "CUCM12", 1, "AudioCodersGroups\_0", 0, 10, 10, 46, 24, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "", "", "", 0, 2, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0,0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0; IpProfile 2 = "AWS-Chime", 1, "AudioCodersGroups\_0", 0, 10, 10, 46, 24, 

 Ipprofile 2 - Aws-chime , 1, AudiocodersGroups\_0 , 0, 10, 10, 40, 24,

 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",

 "AudioCodersGroups\_0", 0, 0, "", "", "", 0, 2, 1, 0, 0, 1, 0, 8, 300,

 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0,

 0, 0, -1, -1, 0, 0;[ \IpProfile ] [ CpMediaRealm ] FORMAT CpMediaRealm\_Index = CpMediaRealm\_MediaRealmName, CpMediaRealm\_IPv4IF, CpMediaRealm\_IPv6IF, CpMediaRealm\_RemoteIPv4IF, CpMediaRealm RemoteIPv6IF, CpMediaRealm PortRangeStart, CpMediaRealm\_MediaSessionLeg, CpMediaRealm\_PortRangeEnd, CpMediaRealm IsDefault, CpMediaRealm QoeProfile, CpMediaRealm BWProfile, CpMediaRealm\_TopologyLocation;

AudioCodes Mediant SBC

```
CpMediaRealm 0 = "MRLan", "LAN IF", "", "", 6000, 50, 6499, 0, "",
"", 0;
CpMediaRealm 1 = "MRWan", "WAN IF", "", "", 7000, 50, 7499, 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 BlockUnReqUsers, SRD MaxNumOfReqUsers,
SRD EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD SBCDialPlanName, SRD AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default SBCRoutingPolicy", "",
"":
[\SRD]
[ MessagePolicy ]
FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy MaxMessageLength, MessagePolicy MaxHeaderLength,
MessagePolicy MaxBodyLength, MessagePolicy MaxNumHeaders,
MessagePolicy MaxNumBodies, MessagePolicy SendRejection,
MessagePolicy MethodList, MessagePolicy MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -
1, 1, "", 0, "", 0, 1;
[ \MessagePolicy ]
[ SIPInterface ]
FORMAT SIPInterface Index = SIPInterface InterfaceName,
SIPInterface NetworkInterface,
SIPInterface SCTPSecondaryNetworkInterface, SIPInterface ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface SCTPPort, SIPInterface AdditionalUDPPorts,
SIPInterface AdditionalUDPPortsMode, 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 PreParsingManSetName, SIPInterface AdmissionProfile,
SIPInterface CallSetupRulesSetId;
SIPInterface 0 = "SIPInterface_LAN", "LAN_IF", "", 2, 5060, 5060, 0, 0,
"", 0, "DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -
1, -1, 0, 0, "", "", -1;
SIPInterface 1 = "SIPInterface WAN", "WAN IF", "", 2, 0, 5060, 5061, 0,
"", 0, "DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1, 0, 1, "", "", -1;
[ \SIPInterface ]
[ ProxySet ]
FORMAT ProxySet Index = ProxySet ProxyName,
ProxySet EnableProxyKeepAlive, ProxySet ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet SRDName, ProxySet ClassificationInput, ProxySet TLSContextName,
ProxySet ProxyRedundancyMode, ProxySet DNSResolveMethod,
ProxySet KeepAliveFailureResp, ProxySet GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SIPInterface_LAN", "", ", 1, 1, 10, -1;
ProxySet 1 = "CUCM12", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 2 = "AWS-Chime", 1, 60, 0, 0, "DefaultSRD", 0, "", -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 SBCServerAuthType, IPGroup OAuthHTTPService,
IPGroup EnableSBCClientForking, IPGroup SourceUriInput,
IPGroup DestUriInput, IPGroup ContactName, IPGroup Username,
IPGroup Password, IPGroup UUIFormat, IPGroup QOEProfile,
IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup MsgManUserDef2, IPGroup SIPConnect, IPGroup SBCPSAPMode,
IPGroup DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup SBCRouteUsingRequestURIPort, IPGroup SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup CallSetupRulesSetId, IPGroup Tags, IPGroup SBCUserStickiness,
IPGroup UserUDPPortAssignment, IPGroup AdmissionProfile,
IPGroup ProxyKeepAliveUsingIPG;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0,
"", 0;
IPGroup 1 = 0, "CUCM12", "CUCM12",
"dt3ynfnrl41vhejg9rtlfz.voiceconnector.chime.aws", "", -1, 0,
"DefaultSRD", "MRLan", 1, "CUCM12", -1, -1, 2, 0, 0, "", -1, "", 0, -1, -
```

```
1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0;
IPGroup 2 = 0, "AWS-Chime", "AWS-Chime",
"dt3ynfnrl41vhejg9rtlfz.voiceconnector.chime.aws", "", -1, 0,
"DefaultSRD", "MRWan", 1, "AWS-Chime", -1, -1, -1, 0, 0, "", -1, "", 0, -
1, -1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default",
0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, "", 1;
[ \IPGroup ]
[ ProxyIp ]
FORMAT ProxyIp Index = ProxyIp ProxySetId, ProxyIp ProxyIpIndex,
ProxyIp IpAddress, ProxyIp TransportType, ProxyIp Priority,
ProxyIp Weight;
ProxyIp 0 = "1", 0, "10.15.28.101:5060", 1, 0, 0;
ProxyIp 1 = "2", 0,
"dt3ynfnrl41vhejg9rtlfz.voiceconnector.chime.aws:5060", 1, 0, 0;
[ \ProxyIp ]
[ Account ]
FORMAT Account Index = Account AccountName, Account ServedTrunkGroup,
Account ServedIPGroupName, Account ServingIPGroupName, Account Username,
Account Password, Account HostName, Account ContactUser,
Account Register, Account RegistrarStickiness,
Account RegistrarSearchMode, Account RegEventPackageSubscription,
Account_ApplicationType, Account_RegByServedIPG,
Account UDPPortAssignment, Account ReRegisterOnInviteFailure;
Account 0 = "AWS Chime Authentication", -1, "CUCM12", "AWS-Chime",
"audiocodes", "$1$S3p+fno=", "", "audiocodes", 0, 0, 0, 0, 2, 0, 0, 0;
[ \Account ]
[ IP2IPRouting ]
FORMAT IP2IPRouting Index = IP2IPRouting RouteName,
IP2IPRouting RoutingPolicyName, IP2IPRouting SrcIPGroupName,
IP2IPRouting SrcUsernamePrefix, IP2IPRouting SrcHost,
IP2IPRouting DestUsernamePrefix, IP2IPRouting DestHost,
IP2IPRouting RequestType, IP2IPRouting MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting CallSetupRulesSetId, IP2IPRouting DestType,
IP2IPRouting DestIPGroupName, IP2IPRouting DestSIPInterfaceName,
IP2IPRouting DestAddress, IP2IPRouting DestPort,
IP2IPRouting DestTransportType, IP2IPRouting AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName,
IP2IPRouting RoutingTagName, IP2IPRouting InternalAction;
IP2IPRouting 0 = "OPTIONS Termination", "Default_SBCRoutingPolicy",
"Any", "*", "*", "*", 6, "", "Any", 0, -1, 13, "", "", 0, -1, 0,
0, "", "", "", ", "default", "Reply(Response='200')";
IP2IPRouting 1 = "CUCM12 to AWS-Chime", "Default SBCRoutingPolicy",
"CUCM12", "*", "*", "*", 0, "", "Any", 0, -1, 0, "AWS-Chime",
"", 0, -1, 0, 0, "", "", "", "default", "";
IP2IPRouting 2 = "AWS-Chime to CUCM12", "Default_SBCRoutingPolicy", "AWS-Chime", "*", "*", ", "*", 0, "", "Any", 0, -1, 0, "CUCM12", "", "", 0, -1, 0, 0, "", "", "", ", "default", "";
```

```
[ \IP2IPRouting ]
[ IPOutboundManipulation ]
FORMAT IPOutboundManipulation Index =
IPOutboundManipulation ManipulationName,
IPOutboundManipulation RoutingPolicyName,
IPOutboundManipulation IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation SrcHost,
IPOutboundManipulation DestUsernamePrefix,
IPOutboundManipulation DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation MessageConditionName,
IPOutboundManipulation RequestType,
IPOutboundManipulation ReRouteIPGroupName,
IPOutboundManipulation Trigger, IPOutboundManipulation ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation RemoveFromRight,
IPOutboundManipulation LeaveFromRight, IPOutboundManipulation Prefix2Add,
IPOutboundManipulation Suffix2Add,
IPOutboundManipulation PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "Do Nothing", "Default SBCRoutingPolicy", 0,
"CUCM12", "AWS-Chime", "*", "*", "+", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255, "", "", 0, "", "";
IPOutboundManipulation 1 = "Add +", "Default SBCRoutingPolicy", 0,
"CUCM12", "AWS-Chime", "*", "*", "*", "*", "*", ", 0, "Any", 0, 1, 0, 0, 255, "+", "", 0, "", "";
IPOutboundManipulation 2 = "Strip + towards CUCM12",
"Default_SBCRoutingPolicy", 0, "AWS-Chime", "CUCM12", "*", "*", "+", "*",
"*", "", 0, "Any", 0, 1, 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 = "Change RUI host toward CUCM12", 2, "Any", "",
"header.request-uri.url.host", 2, "param.message.address.dst.address", 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
'STVuS'":
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 ]
[ 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, 0, "";
```

[ \AudioCoders ]

#### **International Headquarters**

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

#### AudioCodes Inc.

200 Cottontail Lane Suite A101E Somerset NJ 08873 Tel: +1-732-469-0880 Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide Website: https://www.audiocodes.com/

©2019 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-29320

