

# Amazon Chime Voice Connector

# SIP Trunking Configuration Guide:

Avaya Aura Communication Manager and Session Manager with Avaya Session Border Controller for Enterprise

October 2019

# **Document History**

Rev. No.	Date	Description
1.0	Oct-24-2019	SIP Trunk Configuration Guide
1.1	Feb-6-2020	Minor edits based on feedback

# Table of Contents

1	Auc	lience	7		
	1.1	Amazon Chime Voice	Connector7		
2	SIP	Trunking Network Components			
	2.1	Hardware Component	s9		
	2.2	Software Requirement	.s9		
3	Fea	tures	10		
	3.1	Features Supported			
	3.2	Features Not Supporte	ed11		
	3.3	Features Not Tested	11		
	3.4	Caveats and Limitatio	าร11		
4	Cor	figuration			
	4.1	Configuration Checklis	t12		
	4.2	IP Address Worksheet			
	4.3	Avaya Aura CM Config	uration13		
	4.3	1 Avaya Aura CM Lo	gin13		
	4.3	2 IP Node Name	14		
	4.3	1 IP Codec Set	15		
	4.3	2 IP Network Regior	۱16		
	4.3	3 Signaling Group			
	4.3	4 Trunk Groups			
	4.3	5 Route Pattern			
	4.3	6 Outbound Call Rou	ıting23		
	4.3	7 Outbound Caller I	D24		
	4.4	Avaya Aura Session M	anager Configuration25		
	4.4	1 Avaya Aura SM log	Jin25		
	4.4	2 Domain			
	4.4	3 Locations			
	4.4	4 Adaptations			
	4.4	5 SIP Entities and E	ntity Links31		
	4.4	.6 Routing Policies			
	4.4	7 Dial Patterns			
	4.5	Avaya SBCE Configura	ition41		

4.5.1	Avaya SBCE login	41
4.5.2	Server Interworking	42
4.5.3	SIP Servers	44
4.5.4	Topology Hiding	50
4.5.5	Routing	52
4.5.6	Signaling Rules	54
4.5.7	End Point Policy Groups	57
4.5.8	Media Interface	60
4.5.9	Signaling Interface	61
4.5.10	TLS Configuration	65
4.5.11	SIP Authentication	77

# Table of Figures

Figure 1 Network Topology	8
Figure 2: Avaya Aura CM login	13
Figure 3 IP Node Name	14
Figure 4 IP Codec Set	15
Figure 5 IP Network Region	16
Figure 6 Signaling Group	17
Figure 7 Trunk Group	
Figure 8 Trunk Group Continuation	
Figure 9 Trunk Group Continuation	20
Figure 10 Trunk Group Continuation	21
Figure 11 Route Pattern	22
Figure 12 Outbound Call Routing	23
Figure 13 Outbound Caller ID	24
Figure 14 Avaya Aura SM login	25
Figure 15 Routing	26
Figure 16 Add Domain	26
Figure 17 Domain	27
Figure 18 Locations	27
Figure 19 Locations continuation	28
Figure 20 Locations continuation	28
Figure 21 Digit Conversion to Avaya CM	29
Figure 22 Digit Conversion to Amazon	29
Figure 23 Adaptation for Amazon	
Figure 24 SIP Entity for Avaya SM	
Figure 25 SIP Entity and Entity Links for Avaya CM	33

Figure	26 SIP Entity and Entity Links for Avaya CM continuation	.33
Figure	27 SIP Entity and Entity Link for Avaya CM continuation	.34
Figure	28 SIP Entity and Entity Link for Avaya SBCE	.34
Figure	29 SIP Entity and Entity Link for Avaya SBCE continuation	.35
Figure	30 SIP Entity and Entity Link for Avaya SBCE continuation	.35
Figure	31 Routing Policy for Avaya CM	.36
Figure	32 Routing Policy for Avaya CM continuation	.36
Figure	33 Routing Policy for Avaya CM continuation	. 37
Figure	34 Routing Policy for Avaya SBCE	. 37
Figure	35 Routing Policy for Avaya SBCE continuation	. 38
Figure	36 Routing Policy for Avaya SBCE continuation	. 38
Figure	37 Dial Pattern to Avaya CM	. 39
Figure	38 Dial Pattern to Amazon via Avaya SBCE	.40
Figure	39 Avaya SBCE Login	.41
Figure	40 Selection of Avaya SBCE Device	. 42
Figure	41 Server Interworking profile for Avaya SM	. 42
Figure	42 Server Interworking profile for Avaya SM continuation	.43
Figure	43 Server Interworking profile for Amazon	.44
Figure	44 SIP Server for Avaya SM	. 44
Figure	45 SIP Server for Avaya SM Continuation	.45
Figure	46 SIP Server for Avaya SM Continuation	.46
Figure	47 SIP Server for Amazon	.47
Figure	48 SIP Server for Amazon continuation	.48
Figure	49 SIP Server for Amazon continuation	.49
Figure	50 Topology Hiding Profile for Avaya SM	.50
Figure	51 Topology Hiding Profile for Avaya SM continuation	. 50
Figure	52 Topology Hiding Profile for Amazon	.51
Figure	53 Routing for Avaya SM	.52
Figure	54 Routing for Avaya SM continuation	.53
Figure	55 Routing for Avaya SM continuation	53
Figure	56 Routing for Amazon	54
Figure	57 Signaling Rules for Avaya SM	54
Figure	58 Signaling Rules for Avaya SM continuation	55
Figure	59 Signaling Rules for Avaya SM continuation	56
Figure	60 Signaling Rules for Avaya SM continuation	56
Figure	61 End Point Policy Group for Avaya SM	57
Figure	62 End Point Policy Group for Avaya SM Continuation	.58
Figure	63 End Point Policy Group for Amazon	.59
Figure	64 Media Interface facing Avaya SM	60
Figure	65 Media Interface facing Amazon	60
Figure	66 Signaling Interface facing Avaya SM	61
Figure	67 Signaling Interface facing Amazon	62
Figure	68 Server Flow for Avaya SM	.63

Figure 69 Server Flow for Amazon	64
Figure 70 Upload Amazon Root CA	65
Figure 71 Client Profile facing Amazon	66
Figure 72 Client Profile facing Amazon Continuation	67
Figure 73 Server Profile facing Amazon	68
Figure 74 Server Profile facing Amazon Continuation	69
Figure 75 SIP Server Profile – Amazon	70
Figure 76 Media Rule – Amazon	71
Figure 77 Media Rule – Amazon Continuation	72
Figure 78 Edit End Point policy Group – Amazon	73
Figure 79 Edit End Point policy Group – Amazon Continuation	74
Figure 80 Edit Signaling Interface – Amazon	74
Figure 81 Edit Signaling Interface – Amazon continuation	75
Figure 82 Edit Server Flow – Amazon	76
Figure 83 Edit Server Flow – Amazon continuation	77
Figure 84 SIP Authentication – Amazon	78

# **1** Audience

This document is intended for technical staff and Value Added Resellers (VAR) with installation and operational responsibilities. This configuration guide provides steps for configuring SIP trunks using **Avaya Aura Communication Manager (Avaya Aura CM)**, **Avaya Aura Session Manager (Avaya Aura SM) with Avaya Session Border Controller for Enterprise (Avaya SBCE)** to connect to **Amazon Chime Voice Connector** for inbound and/or outbound telephony capabilities.

## **1.1 Amazon Chime Voice Connector**

Amazon Chime Voice Connector is a pay-as-you-go service that enables companies to make or receive secure phone calls over the internet or AWS Direct Connect using their existing telephone system or session border controller (SBC). The service has no upfront fees, elastically scales based on demand, supports calling both landline and mobile phone numbers in over 100 countries, and gives customers the option to enable inbound calling, outbound calling, or both.

Amazon Chime Voice Connector uses the industry-standard Session Initiation Protocol (SIP). Amazon Chime Voice Connector does not require dedicated data circuits. A company can use their existing Internet connection or AWS Direct Connect public virtual interface for SIP connectivity to AWS. Voice connectors can be configured in minutes using the AWS Management Console or Amazon Chime API. Amazon Chime Voice Connector offers cost-effective rates for inbound and outbound calls. Calls into Amazon Chime meetings, as well as calls to other Amazon Chime Voice Connector customers are at no additional cost. With Amazon Chime Voice Connector, companies can reduce their voice calling costs without having to replace their on-premises phone system.

# **2 SIP Trunking Network Components**

The network for the SIP trunk reference configuration is illustrated below and is representative of Avaya Aura CM and Avaya Aura SM with Avaya SBCE configuration.

IP PBX-2 is used as a secondary PBX in the topology to perform call failover and call distribution



Figure 1 Network Topology

## **2.1 Hardware Components**

- UCS-B200 VMWare server running ESXi 6.0 or later used for the following virtual machines
  - o Avaya Aura
    - Communication Manager
    - Session Manager
    - Modular Messaging
- Avaya SBCE running on Dell CAD 208 hardware appliance
- Avaya one-X IP Phone(s)- 9630G

### **2.2 Software Requirements**

- Avaya Aura
  - Session Manager: 8.0.1.1
  - Communication Manager: 8.0.1.1
  - System Manager: 8.0.1.1
  - Communication Manager Messaging: 7.0.0.1
- Avaya Session Border Controller for Enterprise : 8.0.0.0-19-16991

# **3 Features**

## **3.1 Features Supported**

- Calls to and from non-Toll Free number
- Calls to Toll Free number
- Calls to Premium Telephone number
- Calling Party Number Presentation
- Calling Party Number Restriction
- Inbound Calls to an IVR
- International Calls
- Call Authentication
- Anonymous call
- Secure Inbound and Outbound calls with Media Encryption
- DTMF-RFC 2833
- Long duration calls
- Calls to conference scheduled by Amazon Chime user
- Calls to Amazon Chime Business number
- Call Distribution
- Call Failover

## **3.2 Features Not Supported**

- The following are not supported by Amazon Chime Voice Connector,
  - Keep Alive SIP OPTIONS
  - Keep Alive Double CRLF

#### **3.3 Features Not Tested**

• None

#### **3.4 Caveats and Limitations**

- When an outbound call is made from Avaya Aura to PSTN endpoint, there is no two-way audio between Avaya Aura and PSTN endpoint. The issue is caused due to the following,
  - Avaya Aura sends re-INVITE to Amazon Chime Voice Connector for media re-negotiation with an incremented audio port number.
  - Amazon Chime Voice Connector does not re-negotiate with the incremented audio port number causing no way audio.

The issue is resolved by configuring Avaya Aura CM with Direct IP-IP Media

*Connection* set to *No* to stop sending re-INVITE to Amazon Chime Voice Connector.

- Amazon Chime Voice Connector,
  - does not support SIP NOTIFY or SIP INFO for DTMF
  - does not send SIP session refresher for long duration calls
- When the WAN link is down and a call is in progress, the PSTN call leg is not disconnected automatically after a period of inactivity. The call has to be cleared manually.

# **4** Configuration

# 4.1 Configuration Checklist

In this section we present an overview of the steps that are required to configure **Avaya Aura CM**, **Avaya Aura SM and Avaya SBCE** for SIP Trunking with **Amazon Chime Voice Connector.** 

Steps	Description	Reference
Step 1	Avaya Aura CM Configuration	Section 4.3
Step 2	Avaya Aura SM Configuration	Section 4.4
Step 3	Avaya SBCE Configuration	Section 4.5

Table 1 – PBX Configuration Steps

## 4.2 IP Address Worksheet

The specific values listed in the table below and in subsequent sections are used in the lab configuration described in this document and are for **illustrative purposes only**. The customer must obtain and use the values for your deployment.

Component	Lab Value			
Avaya	SBCE			
LAN IP Address	10.89.33.13			
LAN Subnet Mask	255.255.255.0			
Avaya Aura CM				
IP Address 10.80.33.4				
Subnet Mask	255.255.255.0			
Avaya A	Aura SM			
IP Address	10.80.33.3			
Subnet Mask	255.255.255.0			
T-61- 2				

Table 2 – IP Addresses

## 4.3 Avaya Aura CM Configuration

This section with screen shots taken from Avaya Aura CM used for the interoperability testing gives a general overview of the PBX configuration.

#### 4.3.1 Avaya Aura CM Login

- Avaya Aura CM configuration is done via SAT simulator through PuTTY.
- Log in using an appropriate User ID and Password.

֎ 10.89.33.4 - PuTTY	_		×
login as: admin			
This system is restricted solely to authorized users for legitimat purposes only. The actual or attempted unauthorized access, use or of this system is strictly prohibited. Unauthorized users are subj company disciplinary procedures and or criminal and civil penaltie federal or other applicable domestic and foreign laws.	e busi modif ect to s unde	iness ficati o er sta	ons te,
The use of this system may be monitored and recorded for administr security reasons. Anyone accessing this system expressly consents monitoring and recording, and is advised that if it reveals possib of criminal activity, the evidence of such activity may be provide enforcement officials.	ative to suc le evi d to l	and ch idence Law	
All users must comply with all corporate instructions regarding th of information assets. Using keyboard-interactive authentication. Password: Last login: Thu Oct 17 23:32:45 MDT 2019 from 172.16.31.137 on pts Enter your terminal type (i.e., xterm, vt100, etc.) [vt100]=> 32308: old priority 0, new priority 0	e prot /l	tectio	n
admin@lab133-cm80> sat			

Figure 2: Avaya Aura CM login

#### 4.3.2 IP Node Name

• Use the **Change node-names ip** command to verify that node names are defined for Avaya Aura CM (**procr**) and Session Manager (**Lab133-SM80**). The node names are needed for configuring the Signaling Group.

🛃 10.89.33.4 - PuTTY		_		Х
change node-name	s ip	Page	l of	2 ^
	IP NODE NAMES			
Name	IP Address			
ab133-SM80	10.89.33.7			
a cmm	10.89.26.25			
default	0.0.0.0			
gateway	10.89.33.1			
procr	10.89.33.4			
procr6	::			
(8 of 8 adm	inistered node-names were displayed )			
Use 'list node-n	ames' command to see all the administered node-	names		
Use 'change node	-names ip xxx' to change a node-name 'xxx' or a	dd a no	de-name	2

Figure 3 IP Node Name

## 4.3.1 IP Codec Set

• Use **change ip-codec-set 2** to define list of codecs for calls between Avaya Aura CM and SM.

change ip-codec-	set 2				Pag	je 1	of	2
Codec Set: 2	IP	MEDIA PAR	AMETERS					
Audio Codec 1: G.711MU 2: G.711A 3: 4: 5: 6: 7:	Silence Suppression <u>n</u> - - - - - - -	Frames Per Pkt 2     	Packet Size(ms) 20 20					
Media Encry 1: none 2: 3: 4: 5:	ption		Encrypted   	SRTCP:	enforce-ur	ienc-s	rtcp	
Fl=Cancel F2=Ref	resh F3=Submi	t F4=Clr	Fld F5=Help	F6=Upd	ate F7=Nxt	Pg F8	=Prv	Pg

Figure 4 IP Codec Set

#### 4.3.2 IP Network Region

- Use change ip-network-region 2 to define the network region
- Authoritative Domain: Provide Domain Name
- Codec Set: Enter codec set **2** created in Section 4.3.1
- Intra-region IP-IP Direct Audio: **yes**
- Intra-region IP-IP Direct Audio: **yes**

change ip-network-region 2		Page	l of	20
	IP NETWORK REGION			
Region: 2 NR Group: 2				
Location: 1 Authoritative	Domain: .com			
Name: AmazonAvaya	Stub Network Region: n	_		
MEDIA PARAMETERS	Intra-region IP-IP Direct Au	dio: <mark>y</mark> es		
Codec Set: 2	Inter-region IP-IP Direct Au	dio: yes		
UDP Port Min: 2048	IP Audio Hairpinn	ing? <u>n</u>		
UDP Port Max: 3329				
DIFFSERV/TOS PARAMETERS				
Call Control PHB Value: 46				
Audio PHB Value: 46				
Video PHB Value: 26				
802.1P/Q PARAMETERS				
Call Control 802.1p Priority:	6			
Audio 802.1p Priority:	6			
Video 802.1p Priority:	5 AUDIO RESOURCE RESERVA	TION PARAM	ETERS	
H.323 IP ENDPOINTS	RSV	'P Enabled?	n	
H.323 Link Bounce Recovery? y				
Idle Traffic Interval (sec): 2	0			
Keep-Alive Interval (sec): 5				
Keep-Alive Count: 5				
Fl=Cancel F2=Refresh F3=Submit	F4=Clr Fld F5=Help F6=Update	F7=Nxt Pg	F8=Prv	Pg

Figure 5 IP Network Region

#### 4.3.3 Signaling Group

- Command **add signaling group 5** was used to create Signaling Group. Use **change signaling group 5** to modify existing signaling group.
- Set Group Type: **sip**
- Set Transport Method: tcp
- Set Peer Detection Enable: y
- Set Near-end Node Name: procr
- Set Near-end Listen Port: 5060
- Set Far-end Node Name: Lab133-SM80
- Set Far-end Listen Port: **5060**
- Set Far-end Network Region: 2
- Set Far-end Domain: Provide Domain Name
- Set *DTMF over IP*: **rtp-payload**
- Set Direct IP-IP Audio Connections: n (This test is done with Direct IP-IP Audio Connections set to No)
- Leave other fields to default value

change signaling-group	5		Page	l of	2	
	SIGNALING	GROUP				
Group Number: 5 IMS Enabled? n	Group Type: Transport Method:	sip tcp				
IP Video? n		Enforce S	IPS URI fo	or SRTP	? <u>y</u>	
Peer Detection Enabled? y Peer Server: SM Clustered? <u>n</u> Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n						
Alert Incoming SIP Cris Near-end Node Name: p Near-end Listen Port: b	is Calls? <u>n</u> procr 5060 F	Far-end Node Na Far-end Listen Po ar-end Network Regi	me: <u>Lab133</u> ort: <u>5060</u> .on: <u>2</u>	3-SM80		
Far-end Domain:	.com					
Incoming Dialog Loopbac DTMF over IP: :	ks: eliminate rtp-payload	Bypass If IP Th RFC 33 Direct IP-IP A	reshold Ex 89 Comfort udio Conne	ceeded? Noise? Ections?	? <u>n</u> ? n ? n	
Session Establishment T Enable Layer 3	imer(min): <u>3</u> Test? <u>y</u>	IP A	udio Hairp	pinning?	? <u>n</u>	
		Alteinate	Koute Tille	1 (360)		
Fl=Cancel F2=Refresh F3:	=Submit F4=Clr Fld	F5=Help F6=Update	F7=Nxt Pg	F8=Prv	Pg	

Figure 6 Signaling Group

#### 4.3.4 Trunk Groups

- Trunk group **5** is used for trunk to Avaya SM. Command **add trunk group 5** was used to create Trunk Group. Use **change trunk group 5** to modify existing trunk group.
- Set Group Type: **sip**
- Set Group Name: AmazonAvaya
- Set *TAC*: **#005**
- Set *Direction*: **two-way**
- Set Service Type: public-ntwrk
- Set Member Assignment Method: auto
- Set *Signaling Group*: **5** (created in section 4.3.3)
- Set Number of Members: 5

change trunk-group 5				Page	1 of	4
	TRU	UNK GROUP				
Group Number: 5		Group Type:	sip	CDR Repo	rts: y	
Group Name: AmazonAv	vaya	COR:	1 TN:	1	TAC: <u>#00</u>	)5
Direction: two-way	Outgo:	ing Display?	n			
Dial Access? n			Night Ser	vice:		
Queue Length: 0						
Service Type: <u>public-</u>	ntwrk	Auth Code?	n			
		1	Member Assign	ment Metho	d: auto	
			Sigr	naling Grou	p: <u>5</u>	
			Number	of Member	s: 5	
FleCencel FleDefinish I	E2-Submit E4-		- la EGelladata	EZ-Nut Da	E0-Dura	Der
ri-Cancel f2=Refresh h	rs-submit 14=0	JIT FIG F5=H	eip ro=Update	e r/-NXt Pg	ro-Prv	Fg

Figure 7 Trunk Group

• Set Preferred Minimum Session Refresh Internal (sec): 900



Figure 8 Trunk Group Continuation

- Set Numbering Format: Public
- Set Replace Restricted Numbers: yes

change trunk-group 5	Page 3 of 4
TRUNK FEATURES ACA Assignment? <mark>n</mark> Measured: <u>none</u>	Maintenance Tests? <u>y</u>
Suppress # Outpulsing? <u>n</u> Numbering Format: <u>public</u> UUI Treat	ment: <u>service-provider</u>
Replace Replace U	Restricted Numbers? <u>y</u> Navailable Numbers? <u>y</u>
Hold/Un Modify Tandem Calling Num	hold Notifications? <u>y</u> ber: <u>no</u>
Show ANSWERED BY on Display? v	
Fl=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Upda	te F7=Nxt Pg F8=Prv Pg

Figure 9 Trunk Group Continuation

- Set Telephone Event payload Type: **101**
- Set Identity for calling Party Display: From
- Leave all other fields to default values

change trunk-group 5	Page 4 of 4
PROTOCOL VARIATIONS	
Mark Users as Phone?	n
Prepend '+' to Calling/Alerting/Diverting/Connected Number?	n
Send Transferring Party Information?	n
Network Call Redirection?	 n
	—
Send Diversion Header?	У
Support Request History?	n
Telephone Event Payload Type:	101
Convert 180 to 183 for Early Media?	n
Always Use re-INVITE for Display Updates?	n
Identity for Calling Party Display:	From
Block Sending Calling Party Location in INVITE?	n
Accept Redirect to Blank User Destination?	n
Enable Q-SIP?	n
	—
Interworking of ISDN Clearing with In-Band Tones:	keep-channel-active
Request URI Contents: may-ha	ve-extra-digits

Figure 10 Trunk Group Continuation

### 4.3.5 Route Pattern

- Use **change-route-pattern x** command to specify the routing preference. Route pattern **5** is used for SIP trunk to Avaya SM.
- Set Pattern Name: Avaya SBC
- Set Grp No: 5 (created in Section 4.3.4)
- Set *FRL*: **0**
- Set Numbering Format: unk-unk
- Leave all other fields to default values

change route-pa	ttern 5	Page 1 of 4
	Pattern Number: 5 Pattern Name:	Avaya SBC
SCCAN? n	Secure SIP? n Used for SIP stations? n	
Grp FRL NPA	Pfx Hop Toll No. Inserted	DCS/ IXC
No	Mrk Lmt List Del Digits	QSIG
	Dgts	Intw
1:5 0		<u>n</u> <u>user</u>
2:		<u>n</u> <u>user</u>
3:		<u>n</u> <u>user</u>
4:		<u>n</u> <u>user</u>
5:		<u>n</u> <u>user</u>
6:		<u>n</u> user
BCC VALUE	ISC CA-ISC IIC BCIE Service/Feature PARM	I Sub Numbering LAR
0 I 2 M 4 W	Request	Dgts Format
1: <u>y y y y y n</u>	<u>n</u> <u>rest</u>	unk-unk none
2: <u>y y y y y n</u>	<u>n</u> <u>rest</u>	none
<u>3: y y y y y n</u>	<u>n</u> <u>rest</u>	none
4: <u>y y y y y n</u>	<u>n</u> <u>rest</u>	none
5: <u>y y y y y n</u>	<u>n</u> <u>rest</u>	none
<u>6: y y y y y n</u>	n rest	none
Fl=Cancel F2=Re:	fresh F3=Submit F4=Clr Fld F5=Help F6=Update	e F7=Nxt Pg F8=Prv Pg

Figure 11 Route Pattern

#### 4.3.6 Outbound Call Routing

- For outbound call to PSTN through Amazon Chime Voice Connector SIP trunking, Automatic Route Selection (ARS) is used. Use command **change ars analysis x** to configure the routing table.
- Set Dialed String: 214242
- Set *Min*: **10**
- Set *Max*: **12**
- Set *Route Pattern*: **5** (created in section 4.3.5)
- Set Call Type: natl

change ars analysis 21						Page	l of	2
	A	RS DI	GIT ANALY	SIS TABI	LE			
Location: all							Full: 3	
Dialed	Tot	al	Route	Call	Node	ANI		
String	Min	Max	Pattern	Type	Num	Reqd		
<mark>2</mark> 140009999	10	10	5	natl		n		
214242	10	11	7	natl		<u>n</u>		
214242	10	12	5	natl		n		
214242	10	11	9	natl		<u>n</u>		
214242	10	12	5	natl		<u>n</u>		
3	/	/	2	nnpa		<u>n</u>		
3202	10	10	5	natl		<u>n</u>		
3252:	10	10	5	natl		<u>n</u>		
4026	10	10	9	natl		<u>n</u>		
411	3	3	deny	svcl		<u>n</u>		
469	10	10	1	natl		<u>n</u>		
5	7	7	2	hnpa		<u>n</u>		
5551212	7	7	9	natl		<u>n</u>		
6	7	7	2	hnpa		<u>n</u>		
611	3	3	1	svcl		<u>n</u>		
Fl=Cancel F2=Refresh F	3=Submit	F4=C	lr Fld F5:	=Help F6	5=Updat	e F7=Nxt P	g F8=Prv	Pg

Figure 12 Outbound Call Routing

### 4.3.7 Outbound Caller ID

- Amazon Chime Voice Connector SIP Trunk requires E164 Caller ID for outbound calls. Command **change public-unknown-number x** is used to configure the outbound caller ID for Extensions.
- Set *EXT Len*: **7**
- Set EXT Code: 2137429
- Set *Trk Grp*: **5** (created in section 4.3.4)
- Set *CPN Prefix*: **91XXXXXXX**. (Replace XXXXXXX with the numbers to be prefixed)
- Set Total CPN Len: 10

char	nge public-unknown	n-numbering	g 7	Page 1 of 2					
	NUMBERING - PUBLIC/UNKNOWN FORMAT								
				Total					
Ext	Ext	Trk	CPN	CPN					
Len	Code	Grp(s)	Prefix	Len					
				Total Administered: 18					
7	2000	5		7 Maximum Entries: 240					
4	2654	3	043:	10					
4	3000	12	856:	10 Note: If an entry applies to					
4	3001	12	856	10 a SIP connection to Avaya					
4	3003	12	856	10 Aura(R) Session Manager,					
4	5000	5		4 the resulting number must					
4	6614	12	856	10 be a complete E.164 number.					
7	2137429	5	91xxxxxxxx	10					
7	2149177	9	919	10 Communication Manager					
				automatically inserts					
				a '+' digit in this case.					

Figure 13 Outbound Caller ID

## 4.4 Avaya Aura Session Manager Configuration

#### 4.4.1 Avaya Aura SM login

- Avaya Aura Session Manager Configuration is accomplished through the Avaya Aura System Manager
- Access Avaya Aura System Manager Web login screen via https://<IP Address/FQDN>
- Enter the login credentials
- Click Log On

← → C ▲ Not secure   10.89.33.3/network-login/	\$
Recommended access to System Manager is via FQDN.	
Go to central login for Single Sign-On	User ID: admin
If IP address access is your only option, then note that authentication will fail in the following cases:	Password: •••••
<ul> <li>First time login with "admin" account</li> <li>Expired/Reset passwords</li> </ul>	Log On Cancel
Use the "Change Password" hyperlink on this page to change the password manually, and then login.	Change Password
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.	Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

Figure 14 Avaya Aura SM login

#### 4.4.2 Domain



Navigate to Elements > Routing

Figure 15 Routing

- Navigate to Routing > Domains
- Click New



Figure 16 Add Domain

- Set Name: Enter the domain name of Avaya Aura PBX
- Set Type: sip
- Click Commit

AVAYA Nura® System Manager 8.0	🛔 Users 🗸 🎤 Elements 🗸 🌣 Services 🗸   Widgets	∽ Shortcuts ∽		Search				
Home Routing								
Routing ^	Domain Management							
Domains	New Edit Delete Duplicate More Actions -							
Locations	Locations							
Conditions	Name	Туре	Notes					
Adapted in a	.com	sip	Lab113					
Adaptations *	Select : All, None							

Figure 17 Domain

### 4.4.3 Locations

- Navigate to Routing > Locations
- Select New

Routing ^	Location
Domains	New Edit Delete Duplicate More Actions -
Locations	1 Item - 2

Figure 18 Locations

#### • Set Name: Lab133-Plano

Home	Routing					
Routing		^	Location Details			Commit Cancel
Dom	nains		General			
Loca	ations		ocherur	* Name:	Lab133-Plano	
Con	ditions			Notes:	Lab133	

Figure 19 Locations continuation

- Under *Location Pattern*, select **Add** to add **IP Address** Patterns for different networks that communicates within the location
- Set IP Address Pattern: 10.80.33.x
- Leave all other fields to default values
- Click **Commit**

Loca	ntion Pattern							
Add	Remove							
7 Ite	7 Items : 🥭 Filter: Enabl							
	IP Address Pattern	*	Notes					
	* 10.64.x.x		·					
	* 10.75.214.x							
	* 10.89.17.x							
	* 10.89.26.x		Lab126					
	* 10.89.27.x							
	* 10.89.33.x		Lab133					
	* 172.16.x.x							
Sele	t : All, None							
			Commit Cancel					

Figure 20 Locations continuation

#### 4.4.4 Adaptations

- Amazon Chime Voice Connector uses E164 numbering format for SIP Trunking Service. Adaptation was created at the Session Manager to manipulate the digits sent to Amazon network via Avaya Session Border Controller for Enterprise (Avaya SBCE).
- Navigate to Routing > Adaptations. Click New
- Set Adaptation Name: Adaptation\_For\_sbc
- Set Module Name: DigitConversionAdapter
- Set *Module Parameter Type*: **Name-Value Parameter** is selected from the drop down, Click **Add**
- Set Name/Value: fromto/true
- Set *Name/Value*: **odstd/10.89.33.13** (Avaya SBCE LAN IP is entered)
- Set Name/Value: osrcd/10.89.33.7 (Avaya Aura SM IP is entered)
- Under Digit Conversion for Incoming Calls to SM, click Add

Matching Pattern	Min/Max	Delete Digits	Address to Modify
+191921	11/36	<b>5</b> – Deletes + <b>1919</b> from +191921 patterns	Destination – Modifies digits in <b>TO</b> header and sends it to Avaya CM

Figure 21 Digit Conversion to Avaya CM

• Under Digit Conversion for Outgoing Calls from SM, click Add

Matching	Min/Max	Delete	Insert Digits	Address to
Pattern		Digits		Modify
214242	10/36	0	+1 – Insert +1 in front of 214242 patterns	Destination – Modifies the digits in <b>TO</b> header and sends it to Amazon
+91921	11/36	<ul> <li>1 – Deletes</li> <li>+ from</li> <li>+91921</li> <li>patterns</li> </ul>	+1 – Inserts +1 in front of 91921 patterns	Origination – Modifies digits in <b>FROM</b> header and sends it to Amazon

Figure 22 Digit Conversion to Amazon

- Leave all other fields at default values
- Click Commit

Routing ^ Adapta	ation Det	ails					Commit Cancel	Help ?
Domains								
Locations * Adaptation Name: Adaptation_for_SBC								
Conditions * Modu	le Name: Dig	itConversionA	Adapter 🔻					
Adaptations ^	Parameter Type:	me-Value Para	ameter 🔻					
Adaptations	Ad	ld Remove						
Danu dan Evranani		Name		<u>۱</u>	/alue			
Regular Expressi		fromto			true			
SIP Entities		odstd			10.89.33.	.13		
Entity Links		osrcd			10.89.33.	.7		
<b>_</b>	Sel	lect : All, Non	e					
<b>Digit Conversion for Inco</b>	ming Cal	ls to SM	I					
Add Remove								
				_			Filter	Enable
							Filter:	Enable
Matching Pattern 🔺 M	in Ma	x Pho	one Context	Delete	e In	sert Digits	Address to modify	Adapt
* +191921	* 11 *	36		* 5			destination <b>v</b>	
								•
Select : All, None								
Digit Conversion for Ou	utgoing	Calls fro	om SM					
Add Remove								
11 Items 🛛 🍣								Filter:
Matching Pattern	Min	Мах	Phone Context	De Dig	lete jits	Insert Digits	Address modify	s to
* +91921	* 11	* 36		*	1	+1	origina	tion 🔻
* 18	* 11	* 36		*	0	+	destina	ation 🔻
* 206	* 10	* 36		*	0	+1	destina	ation 🔻
* 214000	* 10	* 36		*	0	+1	destina	ation 🔻
* 214242	* 10	* 36		*	0	+1	destina	ation 🔻

Figure 23 Adaptation for Amazon

#### 4.4.5 SIP Entities and Entity Links

#### SIP Entity for Avaya Aura Session Manager

- Navigate to: Routing > SIP Entities. Click New
- Set Name: Enter name of the host, Lab133\_SM80
- Set FQDN or IP Address: Enter the SIP address of the Session Manager
- Set *Type*: **Session Manager** is selected from the drop down
- Set *Location*: Select the **location** (created in Section 4.4.3)
- Under *Listen Port*:
- Set TCP/TLS Failover Port: 5060/5061
- Click Add to assign Domain for the following Ports and Protocols

- Port 5060 and Protocol TCP/UDP
- Port 5061 and Protocol TLS
- Click **Commit**

Home	Routing	Rout	ing					
Routing Dom	nains	^	SIP Entity Det	ails				Commit Cancel
Loca	ntions			* Name: * IP Address:	Lab133-SM	180		]
Cone	ditions			SIP FQDN:				]
Adaj	ptations	^		Туре:	Session Ma	nager 🔻		]
	Adaptations			Notes:	Lab133			
	Regular Expres	si		Location:	Lab133-Pla	no 🔻	_	J
SIP E	Intities			Outbound Proxy: Time Zone:	America/Ch	nicago	▼	
Entit	ty Links	•	Minin	rum TLS Version: Credential name:	Use Global	Setting •		
Co	nditions		Failover Ports TCP Failover port: 5060 TLS Failover port: 5061					
Ad	Adaptations	î	Listen Ports					
	Regular Expres	si	Add Remove 3 Items 🚓					Filter: Enable
SIF	Entities		Listen Ports	Protocol Default D	omain	Endpoint	Notes	
En	tity Links		\$060 \$060 \$061	UDP TLS	com * com *			
	<		Select : All, None					

Figure 24 SIP Entity for Avaya SM

#### SIP Entity and Entity Links for Avaya Aura Communication Manager

- Set Name: Lab133CM\_SIP\_TCP
- Set FQDN or IP Address: Enter the IP address of Avaya Aura Communication Manager
- Set Type: CM
- Click Commit

Routing	SIP Entity Details
Domains	General
Locations	* Name: Lab133CM_SIP_TCP
Conditions	* FQDN or IP Address: 10.89.33.4
Conditions	Type: CM T
Adaptations	Notes:
SIP Entities	Adaptation: 🔹 🔻
Entity Links	Location: V
	Time Zone: America/Fortaleza

Figure 25 SIP Entity and Entity Links for Avaya CM

• Under Entity Links, Click New

Routing	^	Entity Links		
Domains		New Edit Delete Duplicate More Action	ons 🔹	
Locations		9 Items I 🍣		
Conditions		Name	SIP Entity 1	Protocol
Adaptations	~	AMM AMM 5060 TCP	Lab133-SM80	ТСР
		Lab133-SM80 Corp GW 5060 UDP	Lab133-SM80	UDP
SIP Entities		Lab133-SM80 IPC 5061 TLS	Lab133-SM80	TLS
	_	Lab133-SM80 Lab126 SBCE 5060 TCP	Lab133-SM80	TLS
Entity Links		Lab133- SM80 Lab133CM SIP Phone 5061 TLS	Lab133-SM80	TLS
Time Ranges		Lab133- SM80 Lab133CM SIP TCP 5060 TCP	Lab133-SM80	ТСР

Figure 26 SIP Entity and Entity Links for Avaya CM continuation

- Set Name: Lab133-SM80\_Lab133CM\_SIP\_TCP\_5060\_TCP
- Set SIP Entity 1: Select the SIP entity Lab133-SM80
- Set SIP Entity 2: Lab133CM\_SIP\_TCP
- Set Protocol: **TCP**
- Set *Ports*: **5060**
- Set Connection Policy: trusted
- Leave all other fields to default values
- Click Commit

Ent	ity Links			Commi	t Cancel	
1 Ite	m I					Filter
	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
	* Lab133-SM80_Lab133CM	* Q Lab133-SM80	TCP 🔻	* 5060	* Q Lab133CM_SIP_TCP	* 5060

Figure 27 SIP Entity and Entity Link for Avaya CM continuation

#### SIP Entity and Entity Links for Avaya SBCE

- Set Name: AmazonCVC\_AvayaSBC
- Set FQDN or IP Address: Enter the **IP address** of **Avaya SBCE** interface facing Avaya Aura SM
- Set *Adaptation*: Select the **Adaptation** for Avaya SBCE configured in Section 4.4.4
- Set Location: Select the location created in Section 4.4.3
- Click Commit

ura® System Manager 8.0	<b>≗</b> U	sers 🗸 🎾	elements 🗸 🔅 Services 🖞	<ul> <li>Widgets &lt; Shortcuts</li> </ul>	~	Search
Home Routing						
Routing	^	SIP En	tity Details			Commit Cancel
Domains		General	* Name:	AmazonCVC_AvayaSBC		
Conditions			* FQDN or IP Address:	10.89.33.13		
Adaptations	~		Type: Notes:	Other •		
SIP Entities			Adaptation:	Adaptation_for_SBC V		
Entity Links			Location:	Lab133-Plano 🔻		
			Time Zone:	America/Fortaleza	•	

Figure 28 SIP Entity and Entity Link for Avaya SBCE

• Under *Entity Links*, Click **New** 

Routing	^	Ent	ity Links							
Domains		New	New Edit Delete Duplicate More Actions  9 Items							
Locations		9 Ite								
Conditions			Name	SIP Entity 1	Protocol					
Adaptations			AMM AMM 5060 TCP	Lab133-SM80	тср					
			Lab133-SM80 Corp GW 5060 UDP	Lab133-SM80	UDP					
SIP Entities			Lab133-SM80 IPC 5061 TLS	Lab133-SM80	TLS					
	_		Lab133-SM80 Lab126 SBCE 5060 TCP	Lab133-SM80	TLS					
Entity Links			Lab133- SM80 Lab133CM SIP Phone 5061 TLS	Lab133-SM80	TLS					
Time Ranges			<u>Lab133-</u> <u>SM80 Lab133CM SIP TCP 5060 TCP</u>	Lab133-SM80	тср					

Figure 29 SIP Entity and Entity Link for Avaya SBCE continuation

- Set Name: ToAmazonCVCAvayaSBC
- Set SIP Entity 1: Select the SIP Entity Lab133-SM80
- Set SIP Entity 2: AmazonCVC\_AvayaSBC
- Set Protocol: UDP
- Set Ports: Set both Ports to 5060
- Set Connection Policy: trusted
- Leave all other fields to default values
- Click Commit

E	nti	ity Links			Commi	Cancel	
1	Iter	n I 🍣					Filter
		Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
I		* ToAmazonCVCAvayaSBC	* Q Lab133-SM80	UDP V	* 5060	* Q AmazonCVC_AvayaSBC	* 5060

Figure 30 SIP Entity and Entity Link for Avaya SBCE continuation

#### 4.4.6 Routing Policies

#### Routing policy to Avaya Aura CM

- Navigate to: Routing > Routing Policies. Click New
- Set Name: To\_CM(TCP)
- Click Select under SIP Entity as Destination and the SIP Entities window is displayed

<b>Routing Policy Details</b>	Commit Cancel
General	
	* Name: to_CM(TCP)
	Disabled:
	* Retries: 0
	Notes:
SIP Entity as Destination	
Select	

Figure 31 Routing Policy for Avaya CM

- Check the radio button beside **Lab133CM\_SIP\_TCP** as destination SIP Entity (configured in Section 4.4.5)
- Click **Select** and return back to **Routing Policy** Details page

SIP Entities	Select Cancel		
SIP Entities			
9 Items 🗉 🍣			
Name	FQDN or IP Address	Туре	Notes
AmazonCVC_AvayaSBC	10.89.33.13	Other	
AMM	10.89.26.25	Messaging	
Corp_GW	10.64.1.72	SIP Trunk	Corp PRI gateway
IPC	10.64.2.114	SIP Trunk	to IPC Zone 1
Lab126_SBCE	10.89.26.13	SIP Trunk	
Lab133CM_SIP_Phone	10.89.33.4	CM	
Lab133CM_SIP_TCP	10.89.33.4	CM	
Lab133CM_SIP_TLS	10.89.33.4	CM	
Nokia_SBC	10.75.214.115	SIP Trunk	Nokia SBC
Select : None			

Figure 32 Routing Policy for Avaya CM continuation
Leave all other fields at default values

Click Commit

Routing Policy Details	Commit Cancel	
General * Nam Disable * Retrie Note	e: to_CM(TCP) d: s: 0 s: 0	
SIP Entity as Destination		
Name	FQDN or IP Address	Туре
Lab133CM_SIP_TCP	10.89.33.4	CM

Figure 33 Routing Policy for Avaya CM continuation

#### **Routing policy to Avaya SBCE**

- Set Name: AmazonCVCAvayaSBC
- Click Select under SIP Entity as Destination and SIP Entities window is displayed.

<b>Routing Policy Details</b>	Commit
General	
	* Name: AmazonCVCAvayaSBC
	Disabled:
	* Retries: 0
	Notes:
SIP Entity as Destination	
Select	

Figure 34 Routing Policy for Avaya SBCE

- Check the radio button beside **AmazonCVC\_AvayaSBC** as destination SIP Entity (configured in Section 4.4.5)
- Click **Select** and return back to **Routing Policy Details** page

SIP	' Entities	Sel	lect Cancel	
SIP	Entities			
9 Ite	ms 🛛 💝			
	Name	FQDN or IP Address	Туре	Notes
$\odot$	AmazonCVC_AvayaSBC	10.89.33.13	Other	
0	АММ	10.89.26.25	Messaging	
	Corp_GW	10.64.1.72	SIP Trunk	Corp PRI gateway
	IPC	10.64.2.114	SIP Trunk	to IPC Zone 1
	Lab126_SBCE	10.89.26.13	SIP Trunk	
	Lab133CM_SIP_Phone	10.89.33.4	СМ	
	Lab133CM_SIP_TCP	10.89.33.4	CM	
	Lab133CM_SIP_TLS	10.89.33.4	СМ	
-	Nalva CDC	10 75 214 115	SID Truck	Nakia SBC

Figure 35 Routing Policy for Avaya SBCE continuation

- Leave all other fields to default values
- Click **Commit**

Routing Policy Details	Commit Cancel		Help ?
General			
* Name: Amaz	onCVCAvayaSBC		
Disabled: 📃			
* Retries: 0			
Notes:			
SIP Entity as Destination			
Name	FQDN or IP Address	Туре	Notes
AmazonCVC_AvayaSBC	10.89.33.13	Other	

Figure 36 Routing Policy for Avaya SBCE continuation

## 4.4.7 Dial Patterns

#### **Dial Pattern for Avaya Aura CM**

- Navigate to: Routing > Dial Patterns. Click New
- Set *Pattern*: **2137**
- Set *Min*: **4**
- Set *Max*: **12**
- Under **Originating Locations and Routing Policies**, Click **Add**, at the new window
- Originating Location: Select Lab133-Plano (created in Section 4.4.3)
- Routing Policies: Select to\_CM(TCP) under Routing Policies
- Click Select to return to Dial Pattern Details page
- Leave all other fields to default values.
- Click **Commit**

Home Routing									
Routing	^	Dial Pattern Deta	ails					Commit Cancel	Help ?
Domains		General						_	
Locations			* Pat	ttern: 2137					
Conditions			*	Min: 4					
Adaptations	~	Em	ergency	/ Call:				1	
SIP Entities			SIP Do	main: -ALL-	٣				
Entity Links			N	lotes:					
Time Ranges		Add Remove	and F	Routing Polici	es				
Routing Policies		1 Item						Filt	ter: Enable
Dial Patterns	^ •	Originating Location I	Name 🔺	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<		Lab133-Plano		Lab133	to_CM(TCP)	0		Lab133CM_SIP_TCP	
		Select : All, None							

Figure 37 Dial Pattern to Avaya CM

#### Dial Pattern to Amazon Chime Voice Connector via Avaya SBCE

- Navigate to: Routing > Dial Patterns. Click New
- Set Pattern: **214242**
- Set *Min*: **10**
- Set *Max*: **12**
- Under **Originating Locations and Routing Policies**, Click **Add**, at the new window
- Originating Location: Select Lab133-Plano (created in Section 4.4.3)
- Routing Policies: Select AmazonCVCAvayaSBC under Routing Policies
- Click Select to return to Dial Pattern Details page
- Leave all other fields to default values.
- Click **Commit**

Home Routing	
Routing ^	Dial Pattern Details
Domains	General
Locations	* Pattern: 214242
Conditions	* Min: 10
Adaptations 🗸 🗸	Emergency Call:
SIP Entities	SIP Domain: lab.tekvizion.com ▼
Entity Links	Notes:
Time Ranges	Originating Locations and Routing Policies Add Remove
Routing Policies	1 Item 🖓 Filter:
Dial Patterns ^	Originating Location Name     Originating Location Name     Originating Location Name     Routing Policy Name     Rank     Routing Policy Disabled     Routing Policy Destination
<	Lab133-Plano Lab133 AmazonCVCAvayaSBC 0 AmazonCVC_AvayaSBC
	Select : All, None

Figure 38 Dial Pattern to Amazon via Avaya SBCE

# 4.5 Avaya SBCE Configuration

#### 4.5.1 Avaya SBCE login

- Log into Avaya Session Border Controller for Enterprise (SBCE) web interface by typing "https://X.X.X.Sbc".
- Enter the Username and Password
- Click Log In



Figure 39 Avaya SBCE Login

• Under Device, select **Lab126-ASBCE** from drop down to expand the configuration for Avaya SBCE.

Device: Lab126-ASBCE V EMS Lab126-ASBCE	Alarms Incidents Status	Logs v Diagnostics Users Enterprise			Settings 🗸	Help Y Log Our
EMS Dashboard Device Management Backup/Restore	Dashboard Information			Installed Devices		
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> <li>Services</li> </ul>	System Time Version Build Date	07:15:57 AM CDT 8.0.0.0-19-16991 Sat Jan 26 21:58:11 UTC 2019	Refresh	EMS Lab126-ASBCE		
Domain Policies     TLS Management	License State Aggregate Licensing Overages	⊘ ОК 0				
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>	Peak Licensing Overage Count Last Logged in at Failed Login Attempts	0 10/18/2019 07:07:07 CDT 0				

Figure 40 Selection of Avaya SBCE Device

# 4.5.2 Server Interworking

### Server Interworking for Avaya SM

- Navigate to: Configuration Profiles > Server Interworking
- Select the predefined Interworking Profile avaya-ru, click Clone
- Set Clone Name: Lab126ASM
- Click Finish



Figure 41 Server Interworking profile for Avaya SM

Interworking Profiles:	: Lab126ASM	
Add		
Interworking Profiles		Click here to add a description.
cs2100	General Timers Privacy URI Maniput	lation Header Manipulation Advanced
avaya-ru		
Avaya_SM_Comcast	General	
Comcast	Hold Support	NONE
Avava SM to GENBA	180 Handling	None
Vadafana NI	181 Handling	None
Vodalone_NL	182 Handling	None
Vodatone	183 Handling	None
Lab126ASM	Refer Handling	No
To_AmazonCVC	URI Group	None
AudioCodes_Ser_Int	Send Hold	No
	Delayed Offer	No
	3xx Handling	No
	Diversion Header Support	No
	Delayed SDP Handling	No

Figure 42 Server Interworking profile for Avaya SM continuation

## Server Interworking for Amazon Chime Voice Connector

• Repeat the same procedure to create the Interworking Profile to Amazon Chime Voice Connector

EMS Dashboard Device Management Backup/Restore		Interworking Profil	es: avaya-ru	
<ul> <li>System Parameters</li> </ul>		Interworking Profiles	It is not recommended to edit the defaults. T	ry cloning or adding a new profile instead.
<ul> <li>Configuration Profiles</li> </ul>		cs2100	General Timers Privacy URI Man	ioulation Header Manipulation Advanced
Domain DoS		avaya-ru		
Server Interworking			General Clone Profile	x
Media Forking		Profile Name	avaya-ru	
Routing Topology Hiding		Clone Name	To_AmazonCVC	
Signaling Manipulation			Finish	
URI Groups	-	Lab126ASM		

Figure 43 Server Interworking profile for Amazon

## 4.5.3 SIP Servers

#### SIP Server for Avaya SM

- Navigate to Services > SIP Servers
- Click Add
- Set Profile Name: Avaya\_SM
- Click Next

Session B	order (	Controller for	Enterprise				
EMS Dashboard Device Management Backup/Restore	5	SIP Servers: Avaya_ Add	SM	Heartheat	Pagietration	Ping	Advancod
<ul> <li>System Parameters</li> <li>Configuration Profile</li> <li>Services</li> <li>SIP Servers</li> </ul>	es	QFlex VoV CNoIP	Server Type DNS Query Type	Tieartbeat	Registration	Call Sen	ver
LDAP RADIUS		-	Address / FODN Add Server Configuration Pr	ofile		x	Port 5060
<ul> <li>Domain Policies</li> <li>TLS Management</li> <li>Network &amp; Flows</li> <li>DMZ Services</li> </ul>		Profile Name	Avaya_SM			-	Edit
<ul> <li>Monitoring &amp; Loggir</li> </ul>	ıg	Avaya_SM					

Figure 44 SIP Server for Avaya SM

Set Server Type: Select Call Server from the drop down

- Set *IP Address/FQDN*: Enter the **Avaya Aura Session Manager SIP IP** Address
- Set Port: **5060**
- Set Transport: **UDP**
- Click Finish

Edit SIP Server Profile - General X					
Server Type can not be changed w	hile this SIP Server Profile is associated to a Se	rver Flow.			
Server Type	Call Server 🔻				
SIP Domain		_			
DNS Query Type	NONE/A *				
TLS Client Profile	None 🔻				
		Add			
IP Address / FQDN	Port Transport				
10.89.33.7	5060 UDP	▼ Delete			
	Finish				

Figure 45 SIP Server for Avaya SM Continuation

- Navigate to **Advanced** tab
- Set *Enable Grooming*: Checked
- Set Interworking Profile: Select Lab126ASM (created in section 4.5.2)
- Click Finish

Edit Sl	P Server Profile - Advanced	X
Enable DoS Protection		
Enable Grooming		7
Interworking Profile	Lab126ASM V	
Signaling Manipulation Script	None T	-
Securable		
Enable FGDN		
TCP Failover Port		
TLS Failover Port		
Tolerant		
URI Group	None T	
	Finish	

Figure 46 SIP Server for Avaya SM Continuation

## SIP Server for Amazon Chime Voice Connector

- Navigate to Services > SIP Servers
- Click Add
- Set Profile Name: AmazonCVC
- Click **Next**

EMS Dashboard Device Management Backup/Restore	SIP Servers: Avaya	SM	
<ul> <li>System Parameters</li> </ul>	A	Add Server Configuration Profile	x
Configuration Profiles	Profile Name	AmazonCVC	
<ul> <li>Services</li> </ul>			
SIP Servers		Next	
LDAP	GENBAND	Interworking Profile	LaDIZ
RADIUS	GENDAND	Olevalla e Masimulatian Osiat	News
Domain Policies	Comcast	Signaling Manipulation Script	ivone
TLS Management	Vodafone	Securable	

Figure 47 SIP Server for Amazon

- Set Server Type: Select Trunk Server from the drop down
- Set *IP Address/FQDN*: Enter the Amazon Chime voice Connector Outbound Host Name
- Set Port: **5060**
- Set Transport: UDP
- Click **Finish**

Edit SI	P Server Profile - General	X
Server Type	Trunk Server	
SIP Domain		
DNS Query Type	NONE/A 🔻	
TLS Client Profile	None <b>*</b>	
	A	.dd
IP Address / FQDN	Port Transport	
EnterAmazonOutboundHostName	5060 UDP    Delete	)
	Finish	

Figure 48 SIP Server for Amazon continuation

- Navigate to **Advanced** tab
- Set *Interworking Profile*: Select **To\_AmazonCVC** (created in section 4.5.2)
  Click **Finish**

Edit SIP	P Server Profile - Advanced	X
Enable DoS Protection		٦
Enable Grooming		
Interworking Profile	To_AmazonCVC	
Signaling Manipulation Script	None 🔻	
Securable		
Enable FGDN		
TCP Failover Port		
TLS Failover Port		
Tolerant		
URI Group	None	
	Finish	

Figure 49 SIP Server for Amazon continuation

# 4.5.4 Topology Hiding

#### Topology hiding profile for Avaya SM

- Topology Hiding profiles are added for Avaya SM to overwrite and hide certain headers
- Navigate to: Configuration Profiles > Topology Hiding
- Select the Profile **default**. Click **Clone**
- Set Clone Name: Avaya\_SM
- Click **Finish**

EMS Dashboard	Topology Hiding Pro	files: default				
Device Management Backup/Restore	Add					Clone
<ul> <li>System Parameters</li> </ul>	Topology Hiding Profiles	It is not recommended to edit the	e defaults. Try cloning or adding a	a new profil	e instead.	
<ul> <li>Configuration Profiles</li> </ul>	default	Topology Hiding				
Domain DoS Server Interworking	cisco_th_profile	Clone Profile		x	Replace Action	Overwrite Value
Media Forking	Profile Name	default			Auto	
Routing	Clone Name	Avava SM		- 8	Auto	
Topology Hiding Signaling				- 8	Auto	
Manipulation		Finish		- 88	Auto	
URI Groups	AmazonCVC	Referred-By	IP/Domain		Auto	
SNMP Traps		Refer-To	IP/Domain		Auto	

Figure 50 Topology Hiding Profile for Avaya SM

- Select the newly created profile Avaya\_SM and Click Edit
- Set Header: Request-Line, To, From are selected
- Set *Replace Action*: **Overwrite**
- Set Overwrite Value: Provide the appropriate value to be sent
- Click Finish

Topology Hiding Pro	ofiles: Avaya_SM					
Add						
Topology Hiding Profiles			Click h	ere to add a descri	ption.	
default		Ed	it Topology Hiding Prof	ile		X
cisco_th_profile					Add	Header
Comcast	Header	Criteria	Replace Action	Over	write Value	
GENBAND	То	IP/Domain •	Overwrite	•	.com	Delete
Vodafone_NL	From	IP/Domain •	Overwrite	•	.com	Delete
Vodafone	Request-Line •	IP/Domain •	Overwrite	•	.com	Delete
Avaya_SM			Finish			
AmazonCVC						

Figure 51 Topology Hiding Profile for Avaya SM continuation

## **Topology hiding profile for Amazon Chime Voice Connector**

- Repeat the same procedure to create the profile for AmazonCVC
- Overwrite Value: Replace the **To** header and **Request-Line** header with
- Amazon Chime Voice Connector Outbound Host Name
- Click Finish

Topology Hiding Profi	les: AmazonCV	C			
Add					
Topology Hiding Profiles			Edit Topology Hiding Profi	ile	x
default				Ad	ld Header
cisco_th_profile	Header	Criteria	Replace Action	Overwrite Value	
Comcast	То	▼ IP/Domain	▼ Overwrite	▼ EnterAmazonHostNa	n Delete
GENBAND	From	▼ IP/Domain	▼ Auto	▼	Delete
Vodafone_NL	Request-Line	▼ IP/Domain	▼ Overwrite	▼ EnterAmazonHostNa	n Delete
Vodafone			Finish		
Avaya_SM			1 mon		_
AmazonCVC					

Figure 52 Topology Hiding Profile for Amazon

# 4.5.5 Routing

## **Routing for Avaya SM**

- Navigate to: Configuration Profiles > Routing
- Click Add
- Set Profile Name: Avaya\_SM
- Click **Next**

EMS Dashboard Device Management Backup/Restore > System Parameters	Routing Profiles: d     Add     Routing Profiles     default	efault It is not recommended to edit the defaults. Try cloning or a	lding a new profile instead.
Domain DoS		Routing Profile Routing Profile	x
Server Interworking Media Forking	Profile Name	Avaya_SM	
Routing Topology Hiding		Next	
Signaling Manipulation	CNoIP		

Figure 53 Routing for Avaya SM

- At Routing Profile Window, Click Add
- Set Priority/Weight: 1
- Set Server Configuration: Avaya\_SM (configured in section 4.5.3)
- The Server IP, Port and Transport Protocol populates automatically
- Click Finish

	Prof	ile : Avaya_SM - Edit Rule	X
URI Group	*	Time of Day	default 🔻
Load Balancing	Priority •	NAPTR	
Transport	None *	LDAP Routing	
LDAP Server Profile	None *	LDAP Base DN (Search)	None *
Matched Attribute Priority		Alternate Routing	0
Next Hop Priority		Next Hop In-Dialog	
Ignore Route Header	0		
ENUM		ENUM Suffix	
			Add
Priority LDAP Search / Attribute Weight	LDAP Search Regex Pattern	LDAP Search SIP Server Regex Result Profile	Next Hop Address Transport
1		Avaya_S 🔻	10.89.33.7:5060 T None T Delete
		Finish	

Figure 54 Routing for Avaya SM continuation

Routing Profiles: Avaya_SM							
Add					Rename		
Routing Profiles			Clic	ck here to add a description.			
default	Routing Profile						
QFlex							
Comcast	Update Priority						
GENBAND	Priority URI Group	Time of Day	Load Balancing	Next Hop Address	Transport		
VoV	1 *	default	Priority	10.89.33.7:5060	UDP		

Figure 55 Routing for Avaya SM continuation

## **Routing for Amazon**

- Repeat the same steps to create the Routing Profile **AmazonCVC** for Amazon
- Next Hop Address: Enter Amazon Chime Voice Connector Outbound Host Name

	Profi	le : AmazonCVC - Edit Rule	x
URI Group	*	Time of Day	default <b>T</b>
Load Balancing	DNS/SRV V	NAPTR	
Transport	None •	LDAP Routing	
LDAP Server Profile	None <b>*</b>	LDAP Base DN (Search)	None V
Matched Attribute Priority		Alternate Routing	
Next Hop Priority		Next Hop In-Dialog	
Ignore Route Header			
ENUM		ENUM Suffix	
			Add
Priority LDAP Search / Attribute Weight	LDAP Search Regex Pattern	LDAP Search SIP Server Regex Result Profile	Next Hop Address Transport
0		Amazon( 🔻	dtndxrmmjlx1us:  None Delete
		Finish	

Figure 56 Routing for Amazon

## 4.5.6 Signaling Rules

- Navigate to: Domain Policies > Signaling Rules
- Select **default** under Signaling Rules, Click **Clone**
- Set *Name*: Avaya\_SM
- Click Finish

Reverse Proxy	<b>^</b>	Signaling Rules: de	fault			
Policy		Add				Clone
<ul> <li>Services</li> </ul>						
SIP Servers		Signaling Rules	It is not recommended to edit the defau	lts. Try cloning or adding a new rule instead.		
LDAP		default	General Requests Responses	Request Headers Response Headers	Signaling QoS UCID	
RADIUS			Clone Rule	x		
Domain Policies						
Application Rules		Rule Name	default			
Border Rules		Clone Name	Avaya_SM			
Media Rules						
Security Rules			Finish			
Signaling Rules	li k					
Charging Rules			Outbound			
End Point Policy Groups			Requests	Allow		

Figure 57 Signaling Rules for Avaya SM

• Select the newly cloned Signaling Rule **Avaya\_SM**, under tab Request Headers, Click **Add In Header Control** 

- Set Proprietary Request Header: Checked
- Set Header Name: AV-Global-Session-ID
- Set *Method Name*: Select **ALL** from the drop down
- Set *Header Criteria*: Forbidden
- Set *Presence Action*: **Remove header** is selected from the drop down
- Click Finish

	Edit Header Control	X
Proprietary Request Header		
Header Name	AV-Global-Session-ID	
Method Name	ALL 🔻	
Header Criteria	<ul> <li>Forbidden</li> <li>Mandatory</li> <li>Optional</li> </ul>	
Presence Action	Remove header       486       Busy Here	
	Finish	

Figure 58 Signaling Rules for Avaya SM continuation

Signaling Rules: Ava	aya_SN	1								
Add								Rename	Clone	Delet
Signaling Rules					Click here to add	a description.				
default	Genera	I Requests	Responses	Request Heade	ers Response Hea	ders Signaling Qo	S UCID			
No-Content-Type-Checks						4	Add In Header Con	trol Add Ou	ıt Headeı	r Control
Creatran	Row	Header Name		Method Name	Header Criteria	Action	Proprietary	Direction		
Crestron	1	AV-Global-Ses	sion-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
Avaya_Sivi	2	Endpoint-View		ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
test	3	P-AV-Message	⊦ld	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	4	P-Charging-Ve	ector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	5	P-Location		ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	6	Reason		ALL	Forbidden	Remove Header	No	IN	Edit	Delete
	7	Alert-Info		ALL	Forbidden	Remove Header	No	IN	Edit	Delete

• Repeat the same steps for all other required headers

Figure 59 Signaling Rules for Avaya SM continuation

• Repeat the same steps for Response Headers

Signaling Rules: Avay	ya_SM										
Add								[	Rename	Clone	Delete
Signaling Rules					Click here to	add a descriptio	on.				
default	General	Requests	Responses	Request Hea	ders Respons	e Headers Si	gnaling QoS UC	D			
No-Content-Type-Checks							Add In He	ader Control	Add Out	Hoador (	Control
Comcast				0			Add III He		Add Odd	Teader	Control
Crestron	Row	Header Name		Response Code	Method Name	Header Criteri	a Action	Proprietary	Direction		
Avaya_SM	1	P-Location		1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
test	2	Endpoint-View		1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	3	P-Location		2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	4	AV-Global-Ses	sion-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	5	AV-Global-Ses	sion-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	6	P-AV-Message	⊦ld	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	7	P-AV-Message	⊦ld	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
	8	Endpoint-View		2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Figure 60 Signaling Rules for Avaya SM continuation

## 4.5.7 End Point Policy Groups

#### End Point Policy Group for Avaya SM

- A new End Point Policy Group is created for Avaya Aura Session Manager.
- The **default-low** policy group is used for the Amazon Chime Voice Connector.
- Navigate to: **Domain Policies > End Point Policy Groups**
- Select **default-low** under Policy Groups
- Click Clone
- Set Clone Name: Avaya\_SM
- Click **Finish**

EMS Dashboard Device Management Backup/Restore	Policy Groups: defau	ult-low					Clone	]
System Parameters	Policy Groups	It is not recommended to edit the defaults. In	y cloning or adding a new group	o instead.				
Configuration Profiles	default-low							
Services		Clone Group	х					
Domain Policies     Application Rules	Group Name	default-low					Sur	mmary
Border Rules Media Rules	Clone Name	Avaya_SM	ecu	rity	Signaling	Charging	RTCP Mon Gen	
Security Rules Signaling Rules Charging Rules	avaya-def-low-enc		fau	llt-low	default	None	Off	Edit
End Point Policy Groups	avaya-def-high-server							

Figure 61 End Point Policy Group for Avaya SM

- Select the newly cleated Group Avaya\_SM, Click Edit
  Set Signaling Rule: Avaya\_SM
  Click Finish

	Edit Policy Set	X
Application Rule	default <b>v</b>	٦
Border Rule	default <b>v</b>	
Media Rule	default-low-med	
Security Rule	default-low <b>T</b>	
Signaling Rule	Avaya_SM 🔹	
Charging Rule	None <b>T</b>	
RTCP Monitoring Report Generation	Off •	
	Finish	

Figure 62 End Point Policy Group for Avaya SM Continuation

## End Point Policy Group for Amazon Chime Voice Connector

• Repeat the same steps to create End Policy Group for Amazon Chime Voice Connector

Policy Groups: Ama	azonCVC									
Add								Rename	Clone	Delete
Policy Groups				Click I	here to add a desc	ription.				
default-low				Click he	re to add a row de	scription.				
default-low-enc										
default-med	Policy Gro	bup								
default-med-enc									Summ	nary
default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Gen	Mon	
default-high-enc	1	default	default	default-low-	default-low	default	None	Off		Edit
avaya-def-low-enc				med						
avaya-def-high-subscri										
avaya-def-high-server										
Avaya_SM										
Vodafone										
Comcast										
IPC										
AmazonCVC										

Figure 63 End Point Policy Group for Amazon

## 4.5.8 Media Interface

- Navigate to: Network & Flows > Media Interface. Click Add
- Set *Name*: **Med\_LAN** is given here
- Set *IP Address*: Select **SBC\_LAN** from the drop down and the **IP address** populates automatically. The IP address for Interface facing Avaya Aura SM is 10.89.33.13
- Set Port Range: **35000-40000**
- Click Finish

Application Dulas	Media Interface			
Application Rules	Media Internace			
Media Rules				
Security Rules	Media Interface			
Signaling Rules				Add
Charging Rules		Edit Media Interface	X	
End Point Policy			ange	
Groups	Name	Med_LAN	- 40000	Edit Delete
Session Policies	10.4.11	LAN-A1 (A1, VLAN 0)	- 40000	Edit Delete
Network & Flows	IP Address	10.89.33.13 🔻		
Network	Port Range	35000 - 40000		
Management				
Media Interface		Finish		
Signaling Interface				
End Point Flows				
Session Flows				

Figure 64 Media Interface facing Avaya SM

• Repeat the same steps to create a Media Interface facing Amazon Chime Voice Connector

	X	
Name	Med_WAN	
IP Address	WAN-B1 (B1, VLAN 0)  192.6	
Port Range	35000 - 40000	
	Finish	

Figure 65 Media Interface facing Amazon

# 4.5.9 Signaling Interface

### Signaling Interface for Avaya SM

- Navigate to: Network & Flows > Signaling Interface. Click Add, new Add Signaling Interface window appears
- Set Name: SIG\_LAN is given for the interface facing Avaya Aura SM
  Set IP Address: Select LAN-A1
- Set UDP Port: **5060**
- Click **Finish**

Application Rules	Signaling Interface					
Media Rules		Edit Signaling Interface	v			
Security Rules		Eur signaling interface	^			
Signaling Rules	Name	SIG_LAN				Add
Charging Rules		LAN-A1 (A1, VLAN 0)		_		7100
End Point Policy Groups	IP Address	10.89.33.13 🔻		LS Profile		
Session Policies	TCP Port Leave blank to disable		4	one	Edit	Delete
TLS Management	UDP Port	5000	4	one	Edit	
Network & Flows	Leave blank to disable	5060				
Network Management	TLS Port Leave blank to disable					
Media Interface	TLS Profile	None 🔻				
Signaling Interface	Enable Shared Control					
End Point Flows		_				
Session Flows	Shared Control Port					
Advanced Options		Finish				
DMZ Services		Finish				
Monitoring & Logging						5

Figure 66 Signaling Interface facing Avaya SM

#### **Signaling Interface for Amazon Chime Voice Connector**

• Repeat the same steps to create the Signaling Interface facing Amazon. UDP is used between Avaya SBCE and Amazon Chime Voice Connector.

Edi	t Signaling Interface	x
Name	SIG_WAN	
IP Address	WAN-B1 (B1, VLAN 0)    Igen 192.65   Value	
TCP Port Leave blank to disable		
UDP Port Leave blank to disable	5060	
TLS Port Leave blank to disable		
TLS Profile	None •	
Enable Shared Control		
Shared Control Port		
	Finish	

Figure 67 Signaling Interface facing Amazon

- Navigate to: Network & Flows > End Point Flows > Server Flows. Click Add
- Set Flow Name: Avaya SM
- Set SIP Server Profile: Avaya\_SM created in section 4.5.3 is selected
- Set *Transport*: **UDP**
- Set Received Interface: **SIG\_WAN** (created in section 4.5.10)
- Set Signaling Interface: **SIG\_LAN** (section 4.5.10)
- Set *Media Interface*: **Med\_LAN** (section 4.5.9)
- Set End Point Policy Group: Avaya\_SM (section 4.5.8)
- Set *Routing Profile*: **AmazonCVC** (section 4.5.6)

- Set *Topology Hiding Profile*: Avaya\_SM (section 4.5.4)
  Click Finish

E	Edit Flow: Avaya SM
Flow Name	Avaya SM
SIP Server Profile	Avaya_SM 🔹
URI Group	*
Transport	UDP V
Remote Subnet	*
Received Interface	SIG_WAN V
Signaling Interface	SIG_LAN V
Media Interface	Med_LAN V
Secondary Media Interface	None •
End Point Policy Group	Avaya_SM 🔹
Routing Profile	AmazonCVC •
Topology Hiding Profile	Avaya_SM 🔻
Signaling Manipulation Script	None <b>v</b>
Remote Branch Office	Any <b>•</b>
Link Monitoring from Peer	
	Finish

Figure 68 Server Flow for Avaya SM

• Repeat the same steps to create a Server Flow for Amazon Chime Voice Connector.

Ed	lit Flow: AmazonCVC	X
Flow Name	AmazonCVC	
SIP Server Profile	AmazonCVC •	
URI Group	* •	٦
Transport	UDP V	
Remote Subnet	*	
Received Interface	SIG_LAN V	
Signaling Interface	SIG_WAN V	
Media Interface	Med_WAN ▼	
Secondary Media Interface	None •	
End Point Policy Group	AmazonCVC 🔹	
Routing Profile	Avaya_SM •	
Topology Hiding Profile	AmazonCVC •	
Signaling Manipulation Script	None	
Remote Branch Office	Any 🔻	
Link Monitoring from Peer		
	Finish	

Figure 69 Server Flow for Amazon

## 4.5.10TLS Configuration

The following are necessary steps to modify the configuration from protocol UDP to TLS between Avaya SBCE and Amazon Chime Voice Connector

- Navigate to: **TLS management > Certificates**. Click **Install**
- Set Type: Select CA Certificate
- Set *Name*: **AmazonRootCA**
- Set Allow weak Certificate/Key: Checked
- Set Certificate File: Click Choose File to select Amazon Root CA
- Click Upload

Session Border	Controller for E	nterprise		
EMS Dashboard Device Management Backup/Restore > System Parameters	Certificates			Install
<ul> <li>Configuration Profiles</li> <li>Services</li> <li>Domain Policies</li> <li>TLS Management Certificates</li> <li>Client Profiles</li> <li>Server Profiles</li> </ul>	Type Name Overwrite Existing	Install Certificate Certificate Certificate CA Certificate Certificate Certificate Revocation List AmazonRootCA	x   	
SNI Group ▶ Network & Flows ▶ DMZ Services ▶ Monitoring & Logging	Allow Weak Certificate/Key Certificate File	Choose file amazon.pem		

Figure 70 Upload Amazon Root CA

### **Client Profile for Amazon Chime Voice Connector**

- Navigate to: TLS management > Client Profiles. Click Add
- Set *Profile Name*: **SBCWAN** is given for interface facing Amazon Chime Voice Connector
- Set *Certificate*: select server certificate **Lab126SBCWAN.crt** for Avaya SBCE interface facing Amazon Chime Voice Connector
- Set *Peer Certificate Authorities*: Select **amazon.crt** which is uploaded in previous step
- Set Verification Depth: 5
- Click **Next**

Device: Lab126-ASBCE V A	a Edit Profile X
Session Borde	WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.
EMS Dashboard	TLS Profile
Device Management	Profile Name SBCWAN
Backup/Restore	Certificate Lab126SBCWAN.crt
<ul> <li>Configuration Profiles</li> </ul>	SNI Enabled
<ul> <li>Services</li> <li>Demois Delisies</li> </ul>	Certificate Verification
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>	Peer Verification Required
Certificates	amazon.crt
Client Profiles	Peer Certificate Authorities Lab126SMGR.crt Lab133SMGR.crt
Server Profiles	DigiCertGlobalRootCA.crt 👻
SNI Group Network & Flows Network Management	Peer Certificate Revocation Lists
Media Interface	Verification Depth 5
Signaling Interface	Extended Hostname Verification
Session Flows	Server Hostname
Advanced Options	Next

Figure 71 Client Profile facing Amazon

- Set Version: Select all 3 TLS versions
- Click Finish

	Edit Profile	X
Renegotiation Parameters		
Renegotiation Time	0 seconds	
Renegotiation Byte Count	0	
Handshake Options		
Version	TLS 1.2 TLS 1.1 TLS 1.0	
Ciphers	🖲 Default 🔍 FIPS 🔍 Custom	
Value (What's this?)	HIGH:IDH:IADH:IMD5:IaNULL:IeNULL:@STRENGT	ł
	Back	

Figure 72 Client Profile facing Amazon Continuation

### Server Profile for Amazon Chime Voice Connector

- Navigate to: **TLS management > Server Profiles**. Click **Add**
- Set *Profile Name*: **SBCWAN** is given for interface facing Amazon Chime Voice Connector
- Set *Certificate*: Select server certificate **Lab126SBCWAN.crt** for Avaya SBCE interface facing Amazon Chime Voice Connector
- Set Peer Verification: None
- Click **Next**

Device: Lab126-ASBCE 🗸	Alarms Incidents Status V Lo	ogs v Diagnostics Users Edit Profile	x
Session Borde	WARNING: Due to the way OpenSSL pass even if one or more of the cipher sure to carefully check your entry as in may cause catastrophic problems. TLS Profile	handles cipher checking, Cipher Suite validation will s are invalid as long as at least one cipher is valid. Make walid or incorrectly entered Cipher Suite custom values	
Backup/Restore	Profile Name	SBCWAN	to be to
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> </ul>	Certificate	Lab126SBCWAN.crt •	i ux h
<ul> <li>Services</li> </ul>	SNI Options	None •	
Domain Policies	SNI Group	None *	one
TLS Management			1
Certificates	Certificate Verification		
Server Profiles	Peer Verification	None 🔻	
SNI Group     Network & Flows     DMZ Services	Peer Certificate Authorities	amazon.crt Ab126SMGR.crt Lab126SMGR.crt DigiCertGlobalRootCA.crt V	ł
Monitoring & Logging	Peer Certificate Revocation Lists	×	O TL
	Verification Depth	0	IGH:
		Next	

Figure 73 Server Profile facing Amazon

- Set Version: Check all 3 TLS versions
- Click Finish

	Edit Profile	X
Renegotiation Parameters		
Renegotiation Time	0 seconds	
Renegotiation Byte Count	0	
Handshake Options		
Version	🗹 TLS 1.2 🗹 TLS 1.1 🗹 TLS 1.0	
Ciphers	Default	
Value (What's this?)	HIGH:IDH:IADH:IMD5:IaNULL:IeNULL:@STRENG	Tł
	Back Finish	

Figure 74 Server Profile facing Amazon Continuation

### **Edit SIP Server**

- Navigate to: Services > SIP Servers
- Select Server Profile AmazonCVC
- Under General tab, Click **Edit**
- Set Transport: Select **TLS** from Dropdown
- Set Port: **5061**
- Set TLS Client Profile: Select Client Profile SBCWAN
- Click Finish

SIP Servers: Amazo	onCVC		
Add			
Server Profiles	Edit SI	P Server Profile - General	X
QFlex	Server Type	Trunk Server	
VoV	SIP Domain		ctor
CNoIP	DNS Query Type		
GENBAND	DNS Query Type	NONE/A V	
Comcast	TLS Client Profile	SBCWAN V	
Vodafone			Add
IPC	IP Address / FQDN	Port Transport	
Avaya_SM	EnterAmazonOutboundHostName	5061 TLS	▼ Delete
AudioCodesSipServer			
AmazonCVC		Finish	

Figure 75 SIP Server Profile – Amazon

# Configure SRTP

- Navigate to: **Domain Policies > Media Rules**
- Select Media Rule default-high-enc, Click Clone
- Set Clone Name: Amazon-enc
- Click Finish

Session Border	<b>Controller</b>	for Enterprise	Å
EMS Dashboard A Device Management Backup/Restore	Media Rules: def	fault-high-enc	Clone
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> <li>Services</li> <li>SIP Servers</li> </ul>	default-low-med default-low-me	It is not recommended to edit the defaults. Try clonin         Encryption       Codec Prioritization         Advanced         Audio Encryption	ng or adding a new rule instead.
LDAP RADIUS	default-high-enc	Preferred Formats SRTP	_AES_CM_128_HMAC_SHA1_80
Application Rules Border Rules	Rule Name	default-high-enc	_
Media Rules Security Rules Sianalina Rules		Finish	

Figure 76 Media Rule – Amazon

- Select newly created Media Rule Amazon-enc, Click Edit
- Set Preferred Format #1: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_32
- Set Interworking under Audio Encryption: **Unchecked**
- Click Finish

	Media Encryption
Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_32 V
Preferred Format #2	NONE <b>v</b>
Preferred Format #3	NONE v
Encrypted RTCP	
МКІ	
Lifetime Leave blank to match any value.	2^
Interworking	
Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 V
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	
МКІ	
Lifetime Leave blank to match any value.	2^
Interworking	
Miscellaneous	
Capability Negotiation	
	Finish

Figure 77 Media Rule – Amazon Continuation
## **Edit End Point Policy Groups**

- Navigate to: **Domain Policies > End Point Policy Groups**
- Select **AmazonCVC** under Policy Groups
- Click Edit

Policy Groups	Click here to add a description.									
default-low		Click here to add a row description.								
default-low-enc	Policy Grou	up.				-				
default-med	Policy Grou	чр								
default-med-enc									Summary	
default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen		
default-high-enc	1	default	default	default-low-	default-low	default	None	Off	Edit	
avaya-def-low-enc				mea						
avaya-def-high-subscri										
avaya-def-high-server										
Avaya_SM										
Vodafone										
Comcast										
IPC										
AmazonCVC										

Figure 78 Edit End Point policy Group – Amazon

- Set *Media Rule*: Select **Amazon-enc**
- Click Finish

	Edit Policy Set X
Application Rule	default <b>v</b>
Border Rule	default
Media Rule	Amazon-enc 🔻
Security Rule	default-low •
Signaling Rule	default <b>v</b>
Charging Rule	None <b>T</b>
RTCP Monitoring Report Generation	Off ▼
	Finish

Figure 79 Edit End Point policy Group – Amazon Continuation

## **Edit Signaling Interface**

- Navigate to: Network & Flows > Signaling Interface
- Select interface **SIG\_WAN**
- Click Edit

Signaling Rules Charging Rules	•	Signaling Interface						
End Point Policy Groups		Signaling Interface						
Session Policies								Add
<ul> <li>TLS Management</li> </ul>								
Certificates		Name	Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Client Profiles		SIG_LAN	10.89.33.13		5060		None	Edit Delete
Server Profiles			LANART (AT, VEAN 0)					
SNI Group		SIG_WAN	192.65. WAN-B1 (B1, VLAN 0)		5060		None	Edit Delete
<ul> <li>Network &amp; Flows</li> </ul>								
Network	1							
Management								
Media Interface								
Signaling Interface								
End Point Flows	1							
Session Flows								



• Set *TLS Port*: **5061** 

- Set TLS Profile: Select SBCWAN
- Set *TCP/UDP Port*: Delete the values as only TLS is used.
- Click Finish

	Edit Signaling Interface	X
Name	SIG_WAN	
IP Address	WAN-B1 (B1, VLAN 0) 192.65.	
TCP Port Leave blank to disable		
UDP Port Leave blank to disable		
TLS Port Leave blank to disable	5061	
TLS Profile	SBCWAN V	
Enable Shared Control		
Shared Control Port		
	Finish	

Figure 81 Edit Signaling Interface – Amazon continuation

## **Edit Server Flows**

- Navigate to: Network & Flows > End Point Flows > Server Flows
- Select Server Flow AmazonCVC, Click Edit



Figure 82 Edit Server Flow – Amazon

- Set Transport: **TLS**
- Set End Point Policy Group: Select AmazonCVC
- Click Finish

	Edit Flow: AmazonCVC
Flow Name	AmazonCVC
SIP Server Profile	AmazonCVC •
URI Group	* T
Transport	TLS V
Remote Subnet	*
Received Interface	SIG_LAN V
Signaling Interface	SIG_WAN V
Media Interface	Med_WAN •
Secondary Media Interface	None <b>v</b>
End Point Policy Group	AmazonCVC •
Routing Profile	Avaya_SM 🔻
Topology Hiding Profile	default 🔻
Signaling Manipulation Script	None •
Remote Branch Office	Any ▼
Link Monitoring from Peer	
	Finish

Figure 83 Edit Server Flow – Amazon continuation

## 4.5.11SIP Authentication

- Navigate to: Services > SIP Servers
- SIP Server: Select AmazonCVC, Click Edit
- Navigate to Authentication. Click Edit
- Enable Authentication: Checked
- Username: Enter Username configured in Amazon Chime Voice Connector
- *Password*: Enter **Password** configured in Amazon Chime Voice Connector
- Click Finish

Backup/Restore	-	SIP Servers: Amaz	onCVC								
System Parameters		Add									
Configuration Profiles		Server Profiles	General	Authentication	Heartheat	Registration	Ping	Advanced			
<ul> <li>Services</li> </ul>		OElex	General	Authentication	Tieartbeat	Registration	Ting	Auvanceu			
SIP Servers		QT IEX		Edit SIP Server Profile - Authentication X							
LDAP		VoV									
RADIUS		CNoIP	Enable	Enable Authentication User Name							
Domain Policies		GENBAND	Use								
Application Rules		Comcast	Rea	alm	enver challence)						
Media Rules		Vodafone	Rec	and a second	verver onanenge)					- 1	
Security Rules		IPC	(Lea	ssword ave blank to keep existing	g password)						
Signaling Rules		Avaya_SM	Cor	nfirm Password							
Charging Rules		AudioCodesSipServer									
End Point Policy Groups		AmazonCVC		_	_			_			
Session Policies									+19		

Figure 84 SIP Authentication – Amazon