



SIPREC Configuration Guide

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

December 2022

Document History

Rev. No.	Date	Description
1.0	December 19, 2022	SIPREC- Configuration Guide

Table of Contents

1	Audience	8
1.1	Amazon Chime SDK Voice Connector.....	8
2	SIP Trunking Network Components.....	9
2.1	Hardware Components	10
2.2	Software Requirements	10
3	Features	11
3.1	Features Supported.....	11
3.2	Features Not Supported.....	11
3.3	Features Not Tested	11
3.4	Caveats and Limitations.....	11
4	Configuration	11
4.1	Configuration Checklist	11
4.2	Avaya Aura CM Configuration	12
4.2.1	Avaya Aura CM Login.....	12
4.2.2	IP Node Name.....	13
4.2.1	IP Codec Set.....	14
4.2.2	IP Network Region	15
4.2.3	Signaling Group	16
4.2.4	Trunk Groups	17
4.2.5	Route Pattern.....	20
4.2.6	Outbound Call Routing	21
4.2.7	Outbound Caller ID	22
4.2.8	Inbound Call Routing	23
4.3	Avaya Aura Session Manager Configuration	24
4.3.1	Avaya Aura SM login.....	24
4.3.2	Domain	25
4.3.3	Locations.....	26
4.3.4	Adaptations	28
4.3.5	SIP Entities and Entity Links	29
4.3.6	Routing Policies	34

4.3.7	Dial Patterns.....	37
4.4	Avaya SBCE Configuration.....	39
4.4.1	Avaya SBCE login	39
4.4.2	Server Interworking.....	40
4.4.3	SIP Servers	43
4.4.4	Topology Hiding	49
4.4.5	Routing.....	51
4.4.6	Recording Profile.....	54
4.4.7	Session Policies	54
4.4.8	Session Flows	55
4.4.9	Signaling Rules.....	56
4.4.10	End Point Policy Groups	59
4.4.11	Media Interface	61
4.4.12	Signaling Interface	63
4.4.13	End Point Flows.....	66
4.4.14	TLS Configuration.....	70
4.4.15	Signaling Manipulation	76

Table of Figures

Figure 1 Network Topology	9
Figure 2: Avaya Aura CM login	12
Figure 3 IP Node Name	13
Figure 4 IP Codec Set	14
Figure 5 IP Network Region	15
Figure 6 Signaling Group	16
Figure 7 Trunk Group	17
Figure 8 Trunk Group Continuation	18
Figure 9 Trunk Group Continuation	19
Figure 10 Trunk Group Continuation	19
Figure 11 Route Pattern	20
Figure 12 Outbound Call Routing	21
Figure 13 Outbound Caller ID	22
Figure 14 Inbound call routing	23
Figure 15 Avaya Aura SM login	24
Figure 16 Routing	25
Figure 17 Add Domain	25
Figure 18 Domain	26
Figure 19 Locations	26
Figure 20 Locations continuation	27
Figure 21 Locations continuation	27
Figure 22 Digit Conversion to Avaya CM	28
Figure 23 Digit Conversion to Amazon	28
Figure 24 Adaptation for Amazon	29
Figure 25 SIP Entity for Avaya SM	30
Figure 26 SIP Entity and Entity Links for Avaya CM	31
Figure 27 SIP Entity and Entity Links for Avaya CM continuation	31
Figure 28 SIP Entity and Entity Link for Avaya CM continuation	32
Figure 29 SIP Entity and Entity Link for Avaya SBCE	32
Figure 30 SIP Entity and Entity Link for Avaya SBCE continuation	33
Figure 31 SIP Entity and Entity Link for Avaya SBCE continuation	33
Figure 32 Routing Policy for Avaya CM	34
Figure 33 Routing Policy for Avaya CM continuation	34
Figure 34 Routing Policy for Avaya CM continuation	35
Figure 35 Routing Policy for Avaya SBCE	35
Figure 36 Routing Policy for Avaya SBCE continuation	36
Figure 37 Routing Policy for Avaya SBCE continuation	36
Figure 38 Dial Pattern to Avaya CM	37
Figure 39 Dial Pattern to Amazon via Avaya SBCE	38

Figure 40 Avaya SBCE Login.....	39
Figure 41 Selection of Avaya SBCE Device	40
Figure 42 Server Interworking profile for Avaya SM.....	40
Figure 43 Server Interworking profile for Avaya SM continuation	41
Figure 44 Server Interworking profile for PSTN.....	42
Figure 45 Server Interworking profile for Amazon.....	42
Figure 46 SIP Server for Avaya SM	43
Figure 47 SIP Server for Avaya SM Continuation	43
Figure 48 SIP Server for Avaya SM Continuation	44
Figure 49 SIP Server for PSTN.....	45
Figure 50 SIP Server for PSTN continuation.....	45
Figure 51 SIP Server for PSTN continuation.....	46
Figure 52 SIP Server for Amazon.....	47
Figure 53 SIP Server for Amazon continuation.....	47
Figure 54 SIP Server for Amazon continuation.....	48
Figure 55 Topology Hiding Profile for Avaya SM.....	49
Figure 56 Topology Hiding Profile for Avaya SM continuation	49
Figure 57 Topology Hiding Profile for PSTN.....	50
Figure 58 Topology Hiding Profile for Amazon.....	50
Figure 59 Routing for Avaya SM.....	51
Figure 60 Routing for Avaya SM continuation	51
Figure 61 Routing for Avaya SM continuation	52
Figure 62 Routing for PSTN	52
Figure 63 Routing for Amazon	53
Figure 64 Recording Profile for Amazon	54
Figure 65 Recording Profile continuation for Amazon.....	54
Figure 66 Session Profile for Amazon.....	55
Figure 67 Session Profile Continuation for Amazon	55
Figure 68 Session Flow for Amazon	56
Figure 69 Signaling Rules for Avaya SM.....	56
Figure 70 Signaling Rules for Avaya SM continuation.....	57
Figure 71 Signaling Rules for Avaya SM continuation.....	57
Figure 72 Signaling Rules for Avaya SM continuation.....	58
Figure 73 End Point Policy Group for Avaya SM	59
Figure 74 End Point Policy Group for Avaya SM Continuation	59
Figure 75 End Point Policy Group for PSTN	60
Figure 76 End Point Policy Group for Amazon	60
Figure 77 Media Interface facing Avaya SM	61
Figure 78 Media Interface facing PSTN	61
Figure 79 Media Interface facing Amazon	62

Figure 80 Signaling Interface facing Avaya SM	63
Figure 81 Signaling Interface facing PSTN	64
Figure 82 Signaling Interface facing Amazon	65
Figure 83 Server Flow for Avaya SM	66
Figure 84 Server Flow for PSTN	67
Figure 85 Server Flow for Amazon	68
Figure 86 Server Flow for Amazon Continuation	69
Figure 87 Upload Amazon Root CA	70
Figure 88 Client Profile facing Amazon	71
Figure 89 Client Profile facing Amazon Continuation	72
Figure 90 Server Profile facing Amazon	73
Figure 91 Server Profile facing Amazon Continuation	74
Figure 92 Media Rule – Amazon.....	74
Figure 93 Media Rule – Amazon Continuation.....	75
Figure 94 Edit End Point policy Group – Amazon	76
Figure 95 Signaling Manipulation Rule for Amazon	76

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 **SIPREC** 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 SDK Voice Connector** for streaming audio to Amazon Kinesis Video Streams (KVS).

The information in this document is for informational purposes only. AWS does not guarantee the accuracy of this document and AWS has no responsibility or liability for errors or omissions related to this document. The document is subject to change without notice and should not be construed as a commitment by AWS.

1.1 Amazon Chime SDK Voice Connector

Amazon Chime SDK 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 SDK Voice Connector uses the industry-standard Session Initiation Protocol (SIP). Amazon Chime SDK 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 SDK Voice Connector offers cost-effective rates for inbound and outbound calls. Calls into Amazon Chime meetings, as well as calls to other Amazon Chime SDK Voice Connector customers are at no additional cost. With Amazon Chime SDK 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.

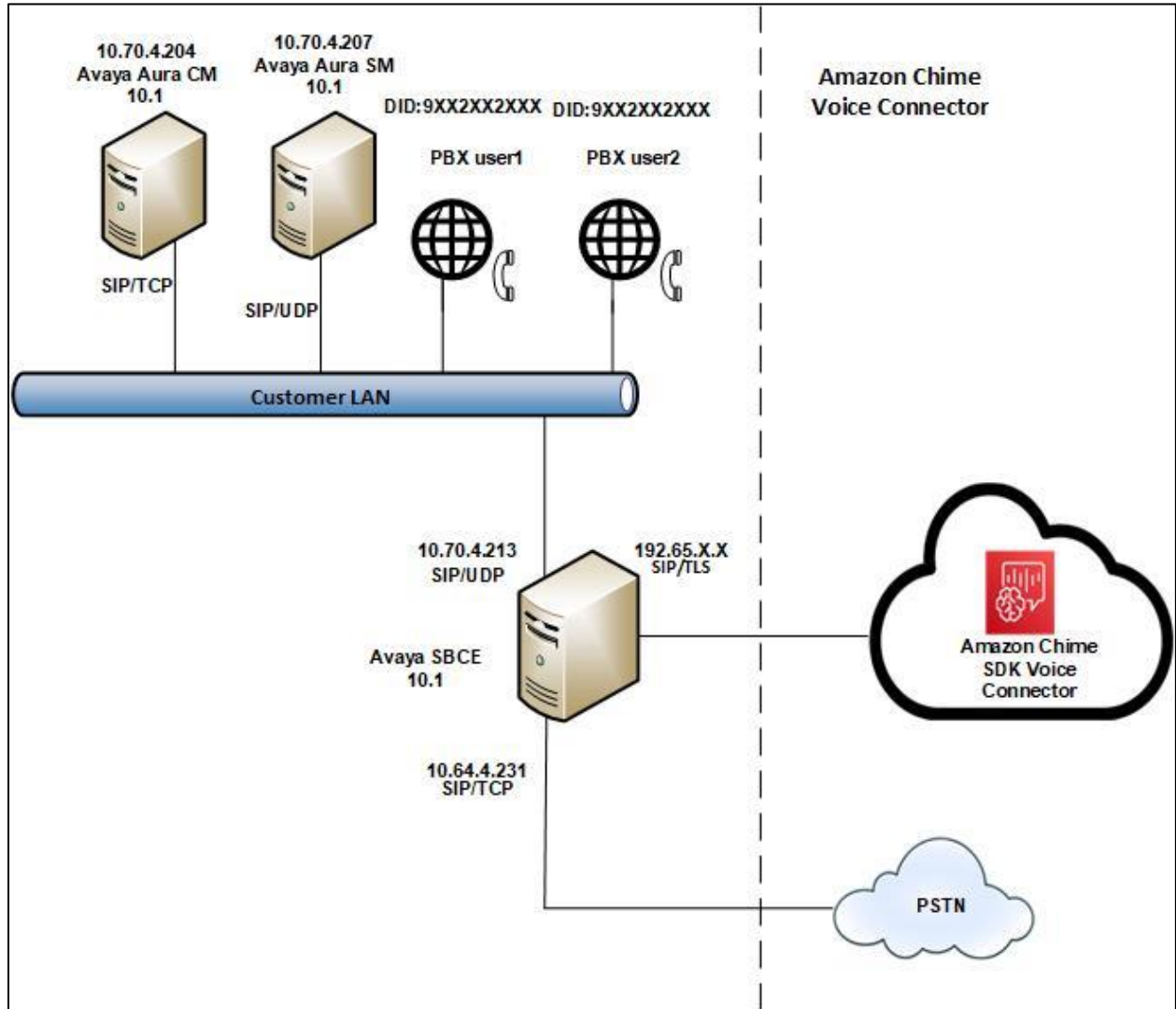


Figure 1 Network Topology

2.1 Hardware Components

- UCS-C240 VMWare server running ESXi 6.0 or later used for the following virtual machines
 - Avaya Aura
 - Communication Manager
 - Session Manager
- Avaya SBCE running on UCS-C240-Virtual Machine
- Avaya one-X IP Phone(s)– 9641G

2.2 Software Requirements

- Avaya Aura
 - Communication Manager: 10.1
 - Session Manager: 10.1
 - System Manager: 10.1
- Avaya Session Border Controller for Enterprise : 10.1.0.0-32-21432

3 Features

3.1 Features Supported

- SIPREC

3.2 Features Not Supported

- None

3.3 Features Not Tested

- None

3.4 Caveats and Limitations

- Amazon Chime SDK Voice Connector uses E164 numbering format for SIP Trunking Service, Signaling Manipulation rule is used to modify the Request URI towards SIP recorder.
- Avaya SBCE is violating the RFC while constructing the UPDATE and BYE towards the SIP Recorder, Avaya provided the Hotfix (sbce-10.1.0.0-34-21958-hotfix-05192022) to resolve the issue.

4 Configuration

The specific values listed in this guide are used in the lab configuration described in this document and are for illustrative purposes only. You must obtain and use the appropriate values for your deployment. Encryption is always recommended if supported.

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 SDK Voice Connector**.

Steps	Description	Reference
Step 1	Avaya Aura CM Configuration	Section 4.2
Step 2	Avaya Aura SM Configuration	Section 4.3
Step 3	Avaya SBCE Configuration	Section 4.4

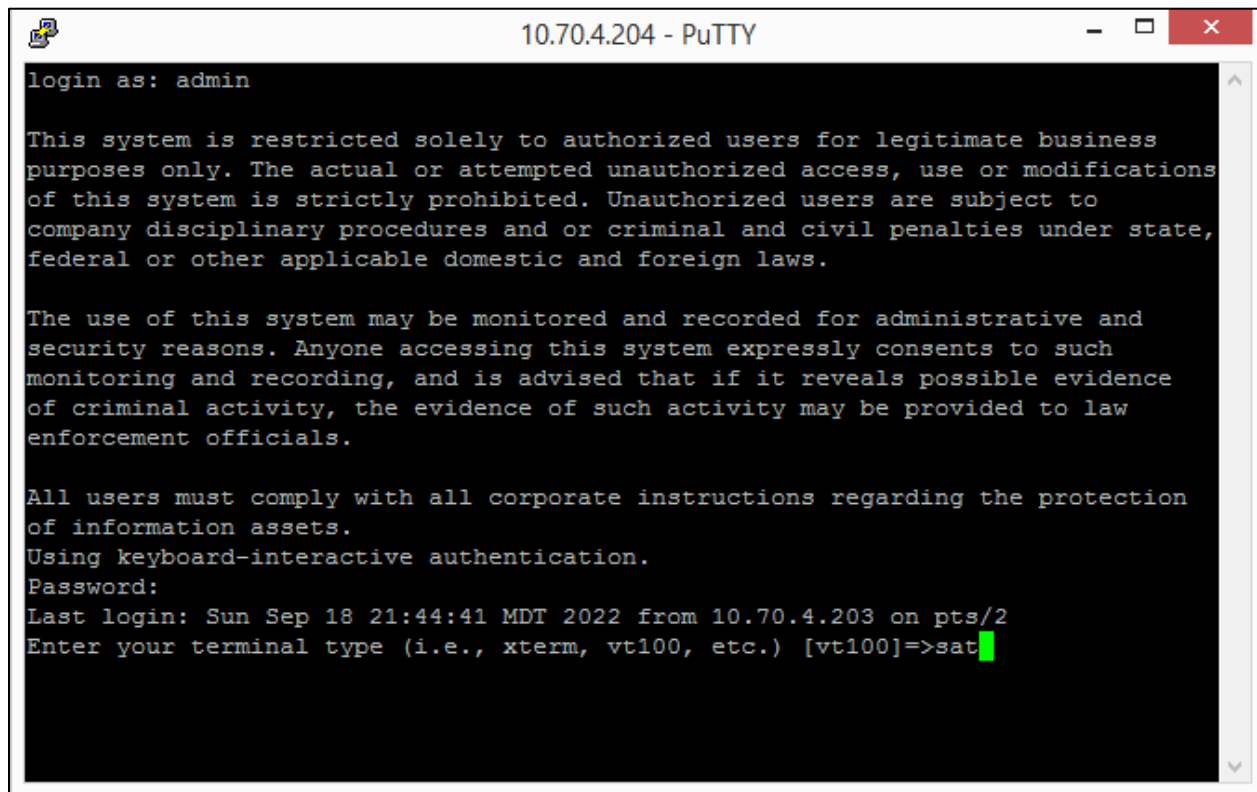
Table 1 – PBX Configuration Steps

4.2 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.

4.2.1 Avaya Aura CM Login

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



```
10.70.4.204 - PuTTY
login as: admin

This system is restricted solely to authorized users for legitimate business
purposes only. The actual or attempted unauthorized access, use or modifications
of this system is strictly prohibited. Unauthorized users are subject to
company disciplinary procedures and or criminal and civil penalties under state,
federal or other applicable domestic and foreign laws.

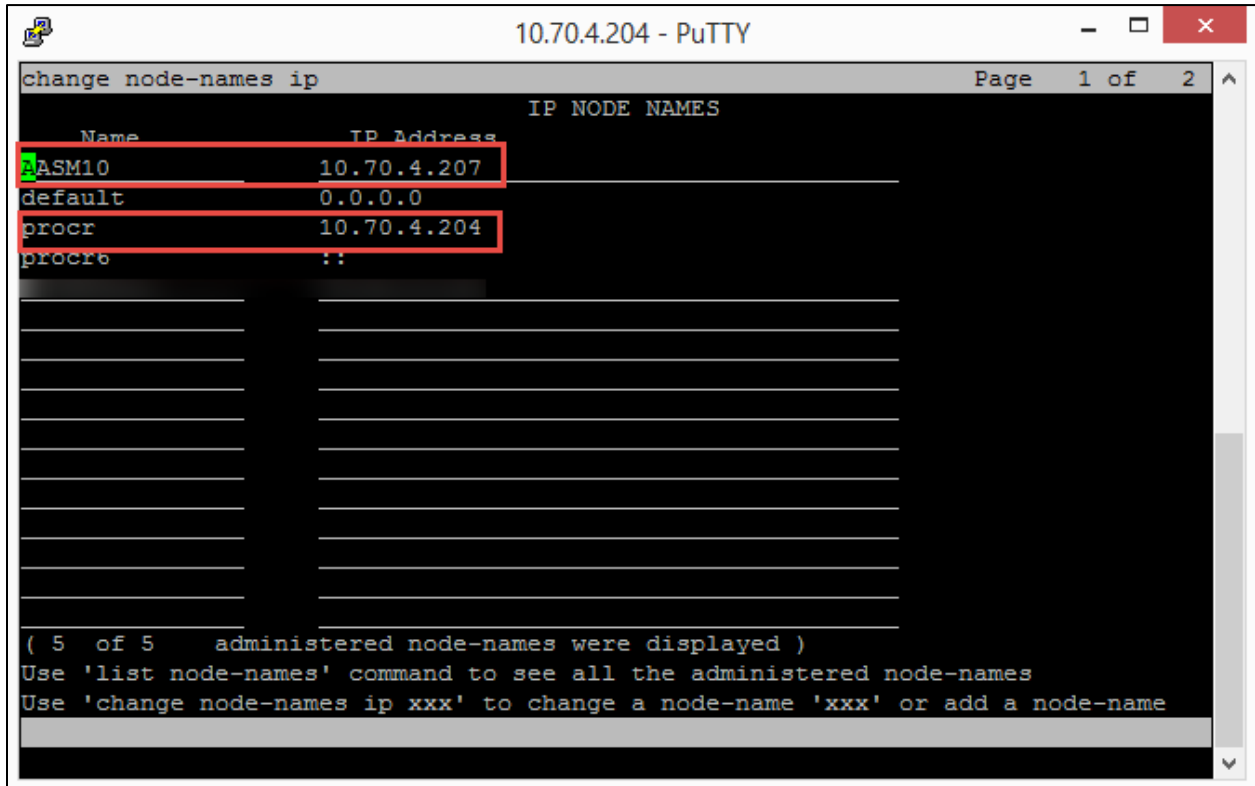
The use of this system may be monitored and recorded for administrative and
security reasons. Anyone accessing this system expressly consents to such
monitoring and recording, and is advised that if it reveals possible evidence
of criminal activity, the evidence of such activity may be provided to law
enforcement officials.

All users must comply with all corporate instructions regarding the protection
of information assets.
Using keyboard-interactive authentication.
Password:
Last login: Sun Sep 18 21:44:41 MDT 2022 from 10.70.4.203 on pts/2
Enter your terminal type (i.e., xterm, vt100, etc.) [vt100]=>sat
```

Figure 2: Avaya Aura CM login

4.2.2 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 (**AASM10**). The node names are needed for configuring the Signaling Group.



```
10.70.4.204 - PuTTY
change node-names ip Page 1 of 2
IP NODE NAMES
Name IP Address
AASM10 10.70.4.207
default 0.0.0.0
procr 10.70.4.204
procr6 ::

( 5 of 5 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Figure 3 IP Node Name

4.2.1 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                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 2

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size (ms)
1: G.711MU      n              2           20
2: _____  -              -
3: _____  -              -
4: _____  -              -
5: _____  -              -
6: _____  -              -
7: _____  -              -

Media Encryption                                Encrypted SRTP: enforce-unenc-srtcp
1: none
2: _____
3: _____
4: _____
5: _____
```

Figure 4 IP Codec Set

4.2.2 IP Network Region

- Use **change ip-network-region 2** to define the network region
- *Authoritative Domain*: Domain name **lab.XXXXXXXXXX.com**
- *Codec Set*: Enter codec set **2** created in Section 4.2.1
- *Intra-region IP-IP Direct Audio*: **yes**
- *Intra-region IP-IP Direct Audio*: **yes**

```
change ip-network-region 2                                     Page 1 of 20
IP NETWORK REGION
Region: 2             NR Group: 2
Location: 1          Authoritative Domain: lab. .com
Name: AmazonAvaya   Stub Network Region: n
MEDIA PARAMETERS
Codec Set: 2        Intra-region IP-IP Direct Audio: yes
                    Inter-region IP-IP Direct Audio: yes
                    IP Audio Hairpinning? n
UDP Port Min: 2048
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.lp Priority: 6
Audio 802.lp Priority: 6
Video 802.lp Priority: 5
AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
RSVP Enabled? n
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 5 IP Network Region

4.2.3 Signaling Group

- Command **add signaling group 1** was used to create Signaling Group. Use **change signaling group 1** 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*: **AASM10**
- Set *Far-end Listen Port*: **5060**
- Set *Far-end Network Region*: **2**
- Set *Far-end Domain*: **lab.xxxxxxxxx.com**
- Set *DTMF over IP*: **rtp-payload**
- Set *Direct IP-IP Audio Connections*: **n**
- Leave other fields to default value

```
change signaling-group 1                                     Page 1 of 2
                                     SIGNALING GROUP
Group Number: 1
IMS Enabled? n
Q-SIP? n
IP Video? n
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr
Near-end Listen Port: 5060
Far-end Node Name: AASM10
Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: lab.xxxxxxxxx.com
Incoming Dialog Loopbacks: eliminate
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
Enable Layer 3 Test? y
H.323 Station Outgoing Direct Media? y
Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n
Initial IP-IP Direct Media? n
Alternate Route Timer(sec): 6
F1=Cancel F2=Refresh F3=Submit F4=Clr F1d F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 6 Signaling Group

4.2.4 Trunk Groups

- Trunk group **1** is used for trunk to Avaya SM. Command **add trunk group 1** is used to create Trunk Group. Use **change trunk group 1** to modify existing trunk group.
- Set *Group Type*: **sip**
- Set *Group Name*: **SIP Trunk**
- Set *TAC*: **#001**
- Set *Direction*: **two-way**
- Set *Service Type*: **tie**
- Set *Member Assignment Method*: **auto**
- Set *Signaling Group*: **1** (created in section 4.2.3)
- Set *Number of Members*: **10**

```
change trunk-group 1                                     Page 1 of 4
TRUNK GROUP
Group Number: 1                                         Group Type: sip          CDR Reports: y
Group Name: SIP Trunk                                  COR: 1                  TN: 1              TAC: #001
Direction: two-way                                     Outgoing Display? n
Dial Access? n                                         Night Service:
Queue Length: 0
Service Type: tie                                       Auth Code? n
Member Assignment Method: auto
Signaling Group: 1
Number of Members: 10
```

Figure 7 Trunk Group

- Set Preferred Minimum Session Refresh Interval (sec): **900**

```
change trunk-group 1                                     Page 2 of 4
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
  SCCAN? n                               Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 900
  Disconnect Supervision - In? y  Out? y
  XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
Caller ID for Service Link Call to H.323 1xC: station-extension
```

Figure 8 Trunk Group Continuation

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

```
change trunk-group 1 Page 3 of 4
TRUNK FEATURES
  ACA Assignment?  Measured: none Maintenance Tests? y

  Suppress # Outpulsing? n Numbering Format: public
                               UI Treatment: service-provider
                               Replace Restricted Numbers? y
                               Replace Unavailable Numbers? y

  Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y
```

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 1 Page 4 of 4
PROTOCOL VARIATIONS
  Mark Users as Phone? 
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
  Send Transferring Party Information? y
  Network Call Redirection? n

  Send Diversion Header? y
  Support Request History? y
  Telephone Event Payload Type: 101

  Convert 180 to 183 for Early Media? n
  Always Use re-INVITE for Display Updates? n
  Resend Display UPDATE Once on Receipt of 481 Response? 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-have-extra-digits
```

Figure 10 Trunk Group Continuation

4.2.5 Route Pattern

- Use **change-route-pattern x** command to specify the routing preference. Route pattern **1** is used for SIP trunk to Avaya SM.
- Set *Pattern Name*: **to AASM10**
- Set *Grp No*: **1** (created in Section 4.2.4)
- Set *FRL*: **0**
- Set *Numbering Format*: **unk-unk**
- Leave all other fields to default values

```
change route-pattern 1
```

Page 1 of 4

Pattern Number: 1		Pattern Name: AASM10							
SCCAN? n	Secure SIP? n	Used for SIP stations? n							
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG Intw	IXC
1: 1	0							n	user
2:								n	user
3:								n	user
4:								n	user
5:								n	user
6:								n	user

BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	Sub Dgts	Numbering Format	LAR
0	1	2	M	4	W	Request				
1:	y	y	y	y	n	n		rest	unk-unk	none
2:	y	y	y	y	n	n		rest		none
3:	y	y	y	y	n	n		rest		none
4:	y	y	y	y	n	n		rest		none
5:	y	y	y	y	n	n		rest		none
6:	y	y	y	y	n	n		rest		none

Figure 11 Route Pattern

4.2.6 Outbound Call Routing

- For outbound call to PSTN through Amazon Chime SDK 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*: **1** (created in section 4.2.5)
- Set *Call Type*: **natl**

```
change ars analysis 2                                     Page 1 of 2
```

ARS DIGIT ANALYSIS TABLE							
Location: all							
Percent Full: 2							
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
214242	10	12	1	natl		n	
214	10	12	1	natl		n	
214	10	12	1	natl		n	
325	3	12	1	natl		n	
729	3	16	1	intl		n	
8	3	10	1	natl		n	
866	3	10	1	natl		n	
91	10	12	1	natl		n	
972	7	12	1	natl		n	
*69	3	3	1	natl		n	
						n	
						n	
						n	
						n	
						n	
						n	

```
F1=Cancel F2=Refresh F3=Submit F4=Clr F1d F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 12 Outbound Call Routing

4.2.7 Outbound Caller ID

- Amazon Chime SDK 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*: **4**
- Set *EXT Code*: **2923**
- Set *Trk Grp*: **1** (created in section 4.2.4)
- Set *CPN Prefix*: **97XXXXXXXX**. (Replace XXXXXXXX with the numbers to be prefixed)
- Set *Total CPN Len*: **10**

```

change public-unknown-numbering 1                                     Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT
Ext  Ext      Trk      CPN      Total
Len  Code      Grp(s)   Prefix   CPN
-----
4    2000        5        97259    10
4    2005        1        04320    10
4    2501        1        97259    10
4    2923        1        97259    10
4    5992        1        91927    10
-----
Total Administered: 5
Maximum Entries: 240
Note: If an entry applies to
a SIP connection to Avaya
Aura (R) Session Manager,
the resulting number must
be a complete E.164 number.
Communication Manager
automatically inserts
a '+' digit in this case.
-----
F1=Cancel F2=Refresh F3=Submit F4=Clr F5=Help F6=Update F7=Nxt Pg F8=Prv Pg

```

Figure 13 Outbound Caller ID

4.3 Avaya Aura Session Manager Configuration

4.3.1 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**

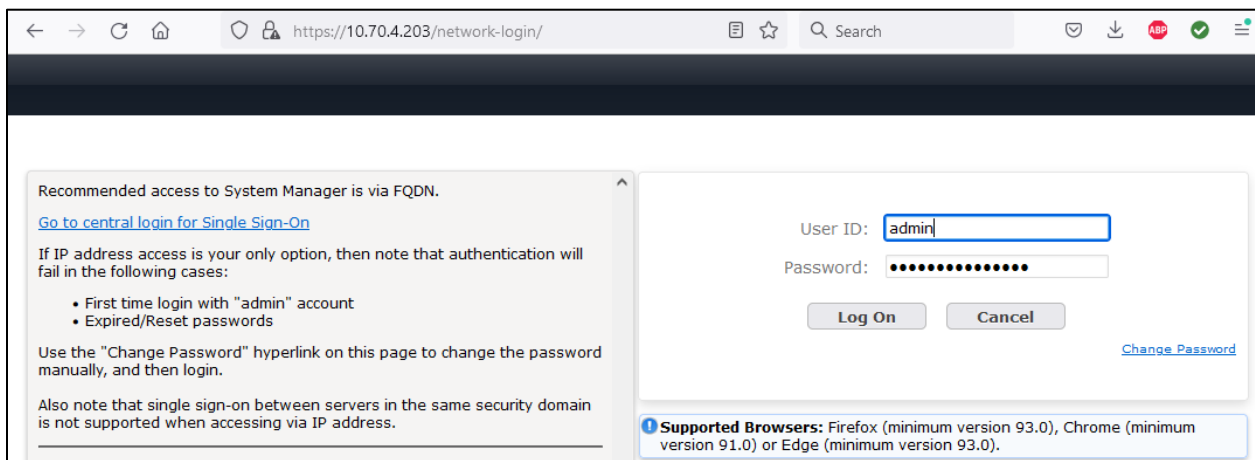


Figure 15 Avaya Aura SM login

4.3.2 Domain

- Navigate to **Elements > Routing**

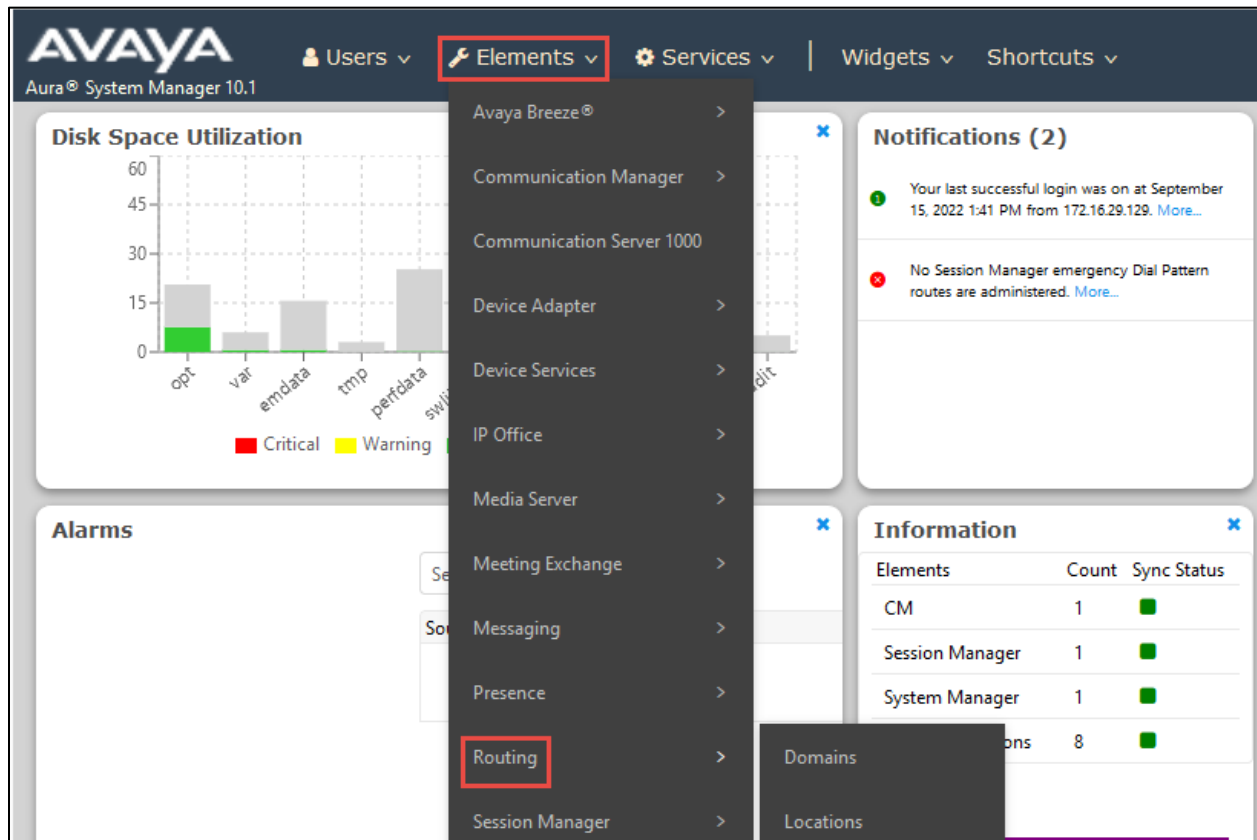


Figure 16 Routing

- Navigate to **Routing > Domains**
- Click **New**

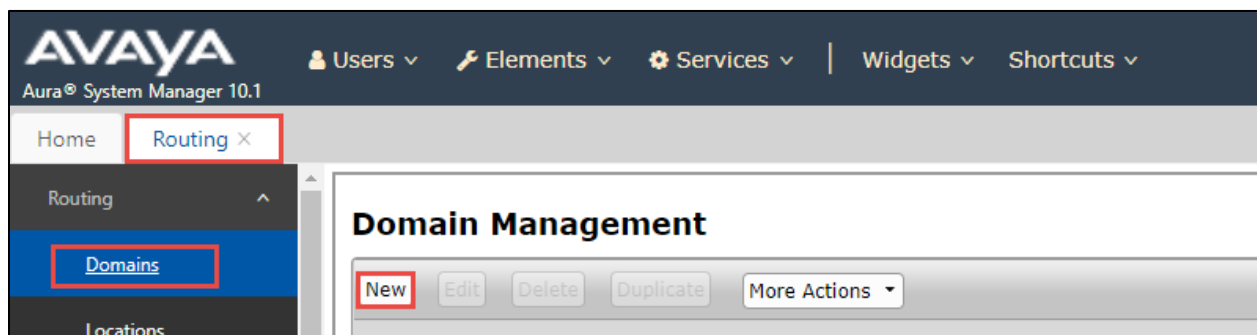


Figure 17 Add Domain

Set *Name*: Enter the domain name of Avaya Aura PBX, **lab.XXXXXXX.com**

- Set *Type*: **sip**
- Click **Commit**

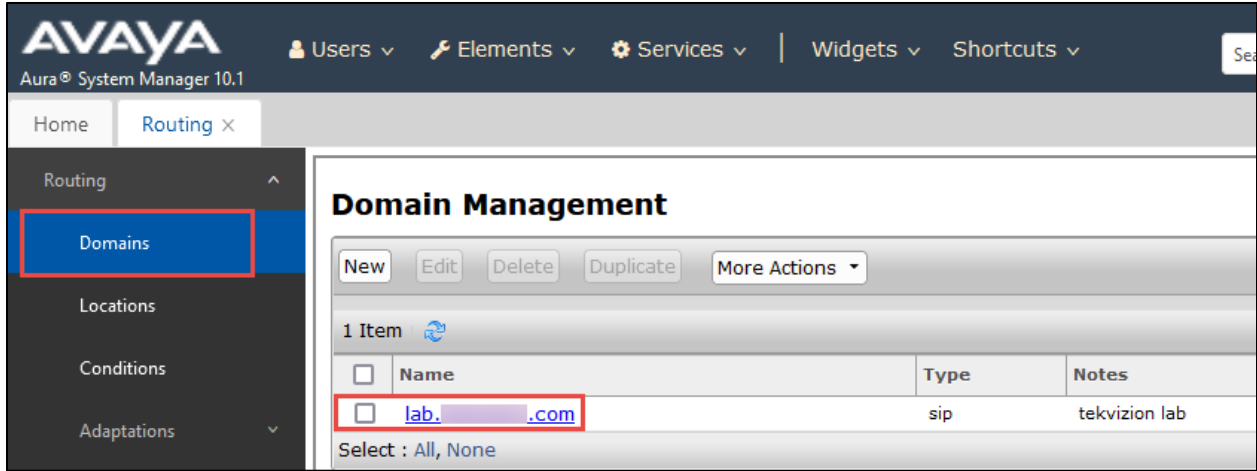


Figure 18 Domain

4.3.3 Locations

- Navigate to **Routing > Locations**
- Select **New**

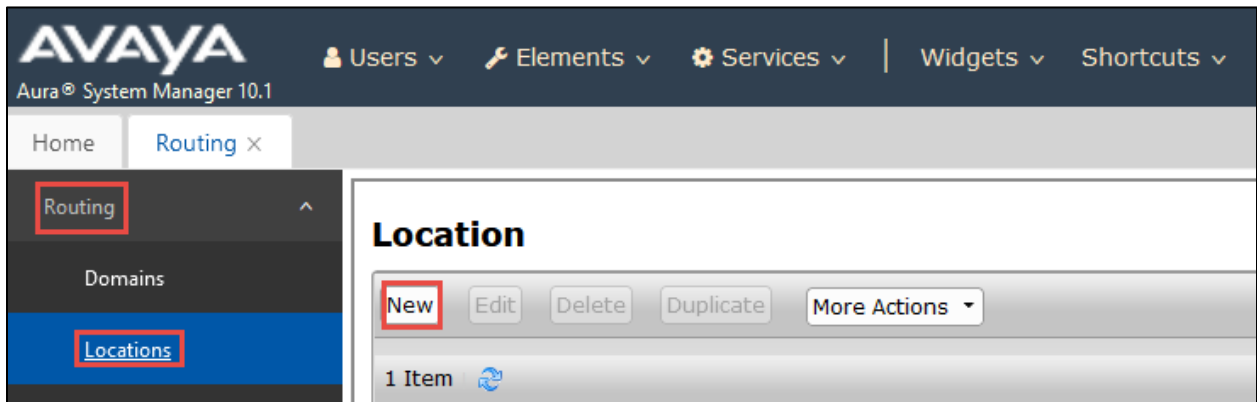


Figure 19 Locations

- Set Name: **Plano**

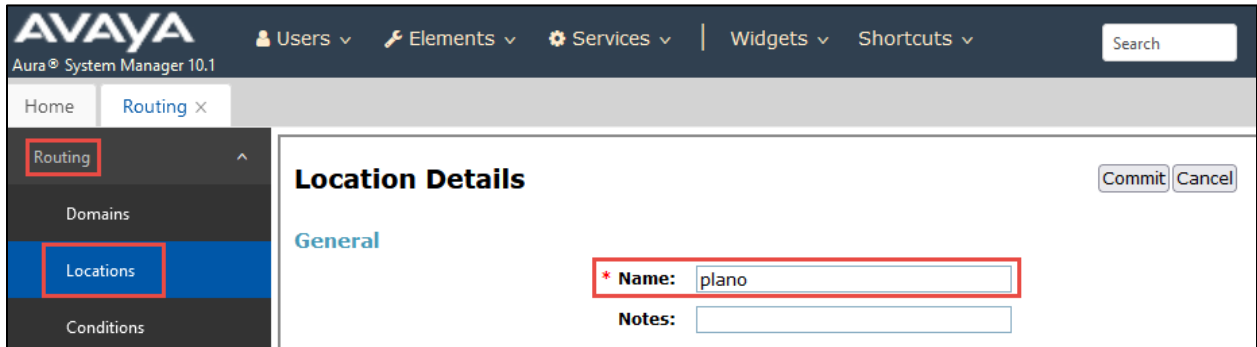


Figure 20 Locations continuation

- Under *Location Pattern*, select **Add** to add **IP Address** Patterns for different networks that communicates within the location
- Set *IP Address Pattern*: **10.70.4.***
- Leave all other fields to default values
- Click **Commit**

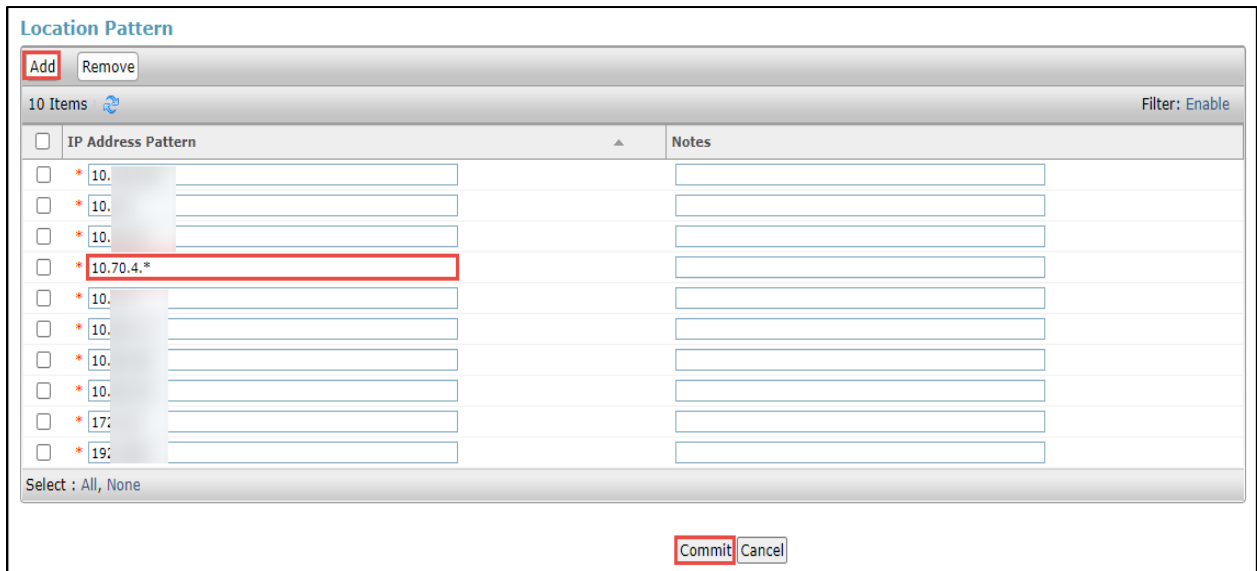


Figure 21 Locations continuation

4.3.4 Adaptations

- Amazon Chime SDK 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*: **Adapter 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/10.70.4.213** (Avaya SBCE LAN IP is entered)
- Set *Name/Value*: **osrcd/10.70.4.207** (Avaya Aura SM IP is entered)
- Under **Digit Conversion for Incoming Calls to SM**, click **Add**

Matching Pattern	Min/Max	Delete Digits	Insert Digits	Address to Modify
972598	10/36	10 – Deletes	2923	Destination – Modifies digits in TO header and sends it to Avaya CM

Figure 22 Digit Conversion to Avaya CM

- Under **Digit Conversion for Outgoing Calls from SM**, click **Add**

Matching Pattern	Min/Max	Delete Digits	Insert Digits	Address to Modify
214242	10/36	0	+1 – Insert +1 in front of 214242 patterns	Destination – Modifies the digits in TO header and sends it to Amazon

Figure 23 Digit Conversion to Amazon

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

- Routing
- Domains
- Locations
- Conditions
- Adaptations
- Adaptations
- Regular Expression ...
- Device Mappings
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns

Adaptation Details

Commit
Cancel
Help ?

General

* **Adaptation Name:**

Notes:

* **Module Name:**

Type:

State:

Module Parameter Type:

	Name	Value
<input type="checkbox"/>	fromto	true
<input type="checkbox"/>	odrcd	10.70.4.207
<input type="checkbox"/>	odstd	10.70.4.213

Select : All, None

Digit Conversion for Incoming Calls to SM

Add Remove
Filter: Enable

1 Item

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 972598	* 10	* 36		* 10	2923	destination		

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add Remove
Filter: Enable

2 Items

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 214242	* 10	* 36		* 0	+1	destination		
<input type="checkbox"/>	* 9725980	* 7	* 36		* 0	+1	destination		

Select : All, None

Commit
Cancel

Figure 24 Adaptation for Amazon

4.3.5 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, **AASM10**
- 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)
- Set *TCP/TLS Failover Port*: **5060/5061**
- Click **Add** to assign Domain **lab.xxxxxxxx.com** for the following Ports and Protocols
- Port **5060** and Protocol **TCP/UDP**
- Port **5061** and Protocol **TLS**
- Click **Commit**

AVAYA
Aura® System Manager 10.1

Users | Elements | Services | Widgets | Shortcuts | Search

Home | Routing

SIP Entity Details [Commit] [Cancel]

General

* Name: AASM10
 * IP Address: 10.70.4.207
 SIP FQDN:
 Type: Session Manager
 Notes:
 Location: plano
 Outbound Proxy:
 Time Zone: America/Chicago
 Minimum TLS Version: Use Global Setting
 Credential name:

Failover Ports

TCP Failover port: 5060
 TLS Failover port: 5061

Listen Ports

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	lab. .com	<input type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	lab. .com	<input type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	lab. .com	<input type="checkbox"/>	

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

[Commit] [Cancel]

Figure 25 SIP Entity for Avaya SM

SIP Entity and Entity Links for Avaya Aura Communication Manager

- Set Name: **AACM10**
- Set FQDN or IP Address: Enter the **IP address** of **Avaya Aura Communication Manager**
- Set Type: **CM**
- Click **Commit**

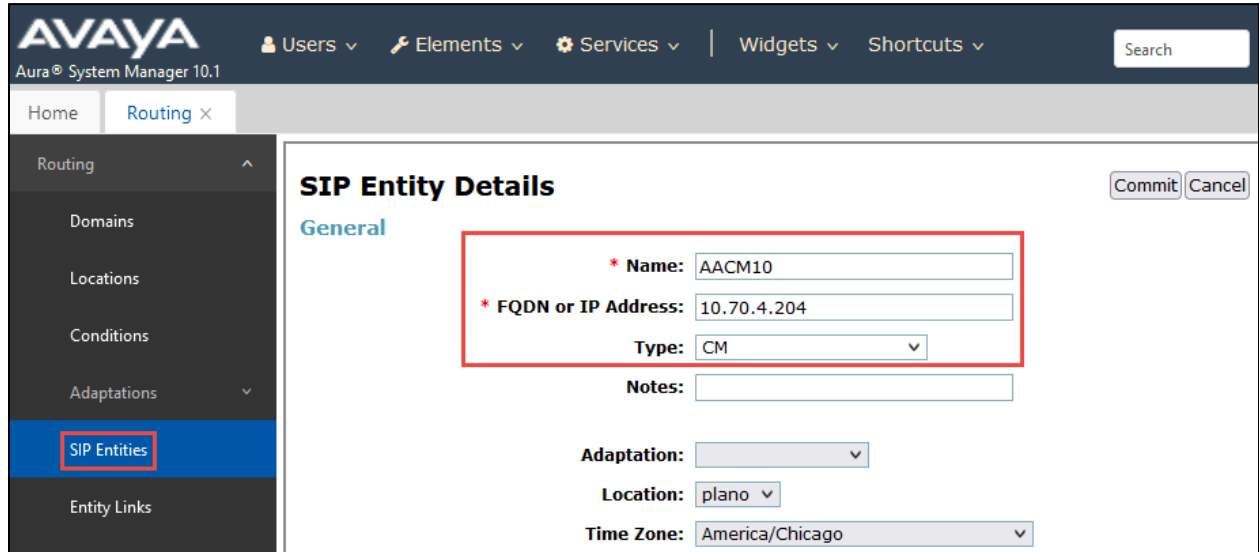


Figure 26 SIP Entity and Entity Links for Avaya CM

- Under *Entity Links*, Click **New**

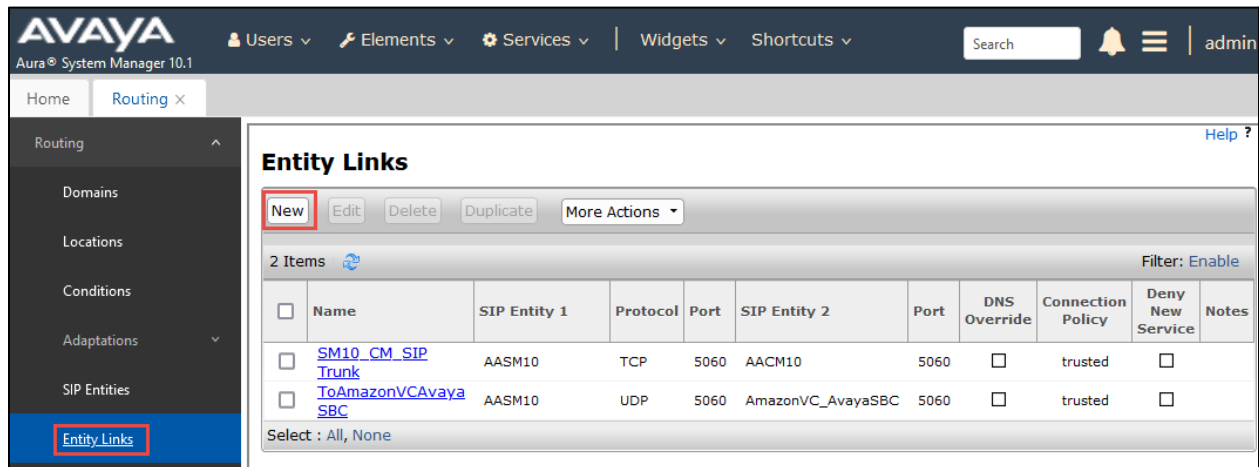


Figure 27 SIP Entity and Entity Links for Avaya CM continuation

- Set Name: **SM10_CM_SIP Trunk**
- Set SIP Entity 1: Select the SIP entity **AASM10**
- Set SIP Entity 2: **AACM10**
- Set Protocol: **TCP**
- Set Ports: **5060**
- Set Connection Policy: **trusted**
- Leave all other fields to default values
- Click **Commit**

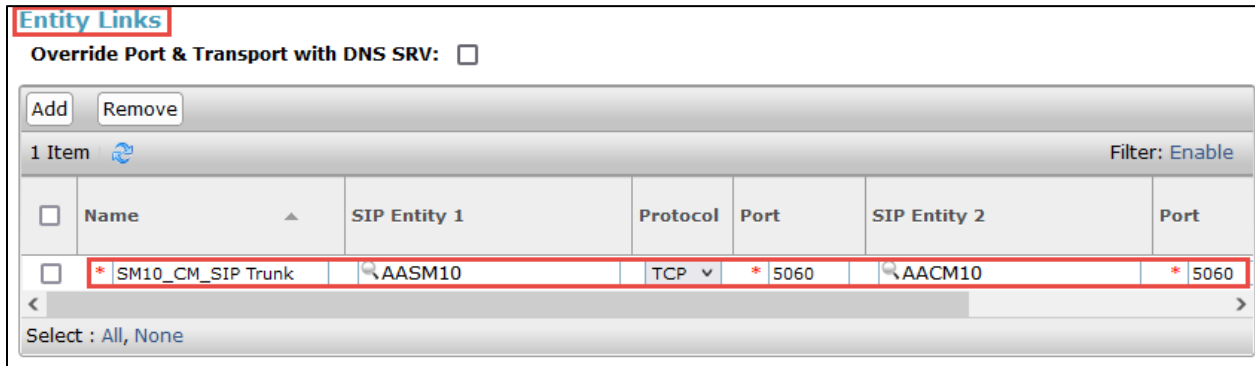


Figure 28 SIP Entity and Entity Link for Avaya CM continuation

SIP Entity and Entity Links for Avaya SBCE

- Set Name: **AmazonVC_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 4.3.4
- Set Location: Select the **location** created in Section 4.3.3
- Click **Commit**

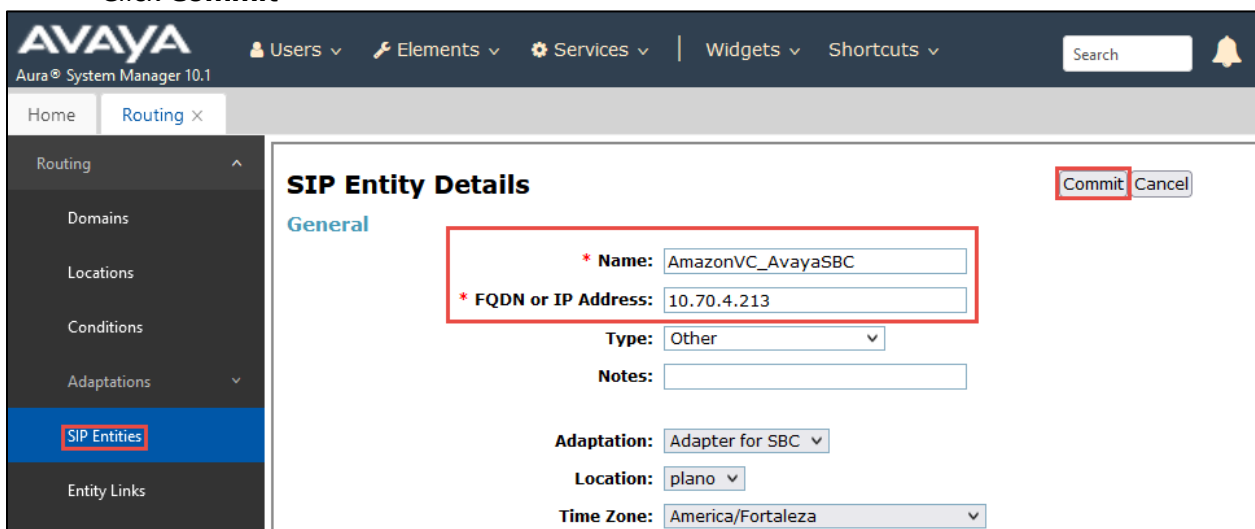


Figure 29 SIP Entity and Entity Link for Avaya SBCE

- Under *Entity Links*, Click **New**

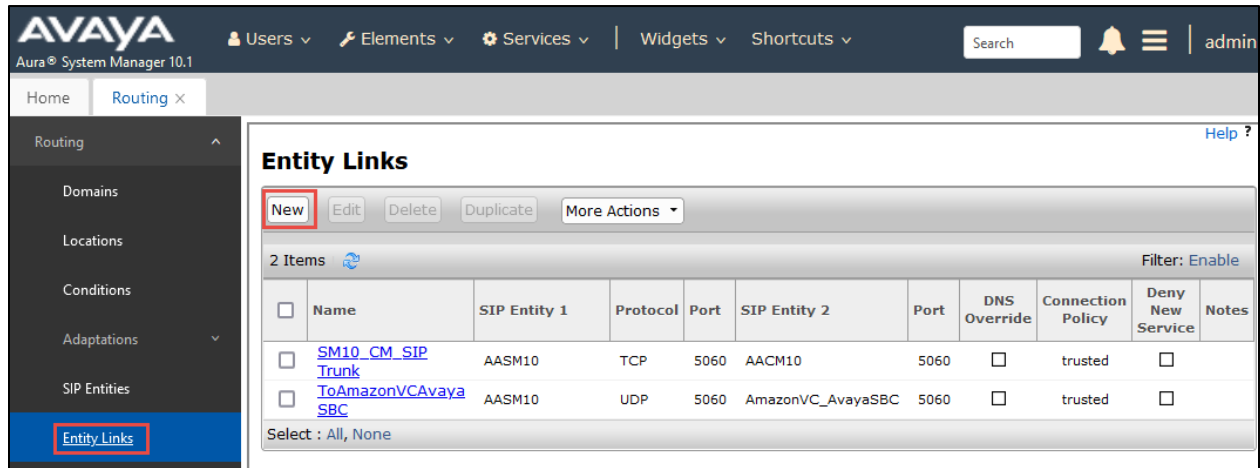


Figure 30 SIP Entity and Entity Link for Avaya SBCE continuation

- Set Name: **ToAmazonVCAvayaSBC**
- Set SIP Entity 1: Select the SIP Entity **AASM10**
- Set SIP Entity 2: **AmazonVC_AvayaSBC**
- Set Protocol: **UDP**
- Set Ports: Set both Ports to **5060**
- Set Connection Policy: **trusted**
- Leave all other fields to default values
- Click **Commit**

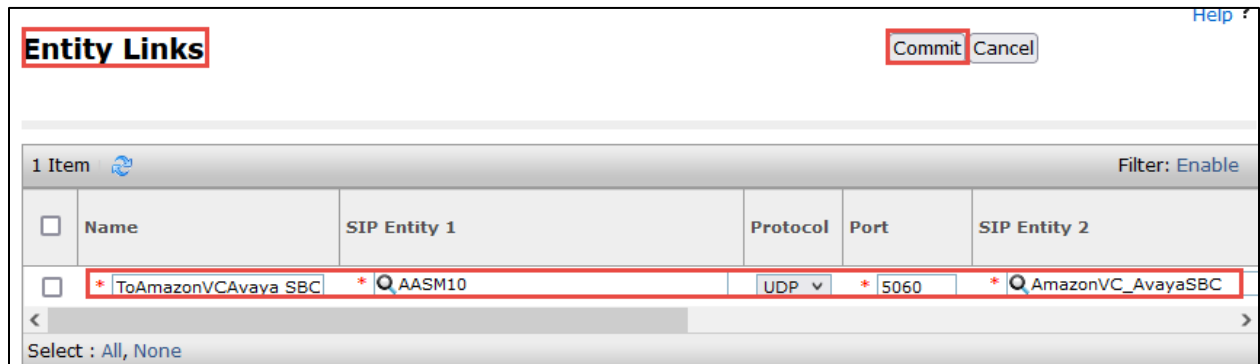
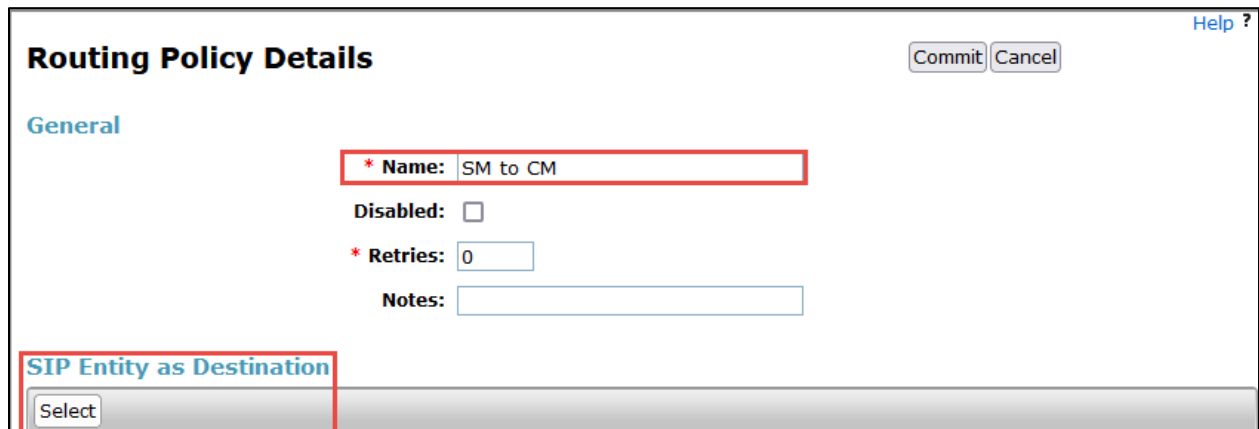


Figure 31 SIP Entity and Entity Link for Avaya SBCE continuation

4.3.6 Routing Policies

Routing policy to Avaya Aura CM

- Navigate to: **Routing > Routing Policies**. Click **New**
- Set *Name*: **SM to CM**
- Click **Select** under **SIP Entity as Destination** and the **SIP Entities** window is displayed



Routing Policy Details Commit Cancel [Help ?](#)

General

* **Name:**

Disabled:


* **Retries:**

Notes:

SIP Entity as Destination

Figure 32 Routing Policy for Avaya CM

- Check the radio button beside **AACM10** as destination SIP Entity (configured in Section 4.3.5)
- Click **Select** and return back to **Routing Policy** Details page



SIP Entities [Help ?](#)

3 Items Filter: [Enable](#)

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	AACM10	10.70.4.204	CM	
<input type="checkbox"/>	AASM10	10.70.4.207	Session Manager	
<input type="checkbox"/>	AmazonVC_AvayaSBC	10.70.4.213	Other	

Select : All, None

Figure 33 Routing Policy for Avaya CM continuation

Leave all other fields at default values

- Click Commit

The screenshot shows the 'Routing Policy Details' configuration page. The 'General' section has the following fields: '* Name: SM to CM', 'Disabled: ', '* Retries: 0', and 'Notes:'. The 'SIP Entity as Destination' section features a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
AACM10	10.70.4.204	CM	

Figure 34 Routing Policy for Avaya CM continuation

Routing policy to Avaya SBCE

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

The screenshot shows the 'Routing Policy Details' configuration page. The 'General' section has the following fields: '* Name: AmazonVCAvayaSBC', 'Disabled: ', '* Retries: 0', and 'Notes:'. The 'SIP Entity as Destination' section features a 'Select' button.

Figure 35 Routing Policy for Avaya SBCE

- Check the radio button beside **AmazonVC_AvayaSBC** as destination SIP Entity (configured in Section 4.3.5)
- Click **Select** and return back to **Routing Policy Details** page

SIP Entities Help ?

New Edit Delete Duplicate More Actions ▾

3 Items Filter: Enable

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	AACM10	10.70.4.204	CM	
<input type="checkbox"/>	AASM10	10.70.4.207	Session Manager	
<input type="checkbox"/>	AmazonVC_AvayaSBC	10.70.4.213	Other	

Select : All, None

Figure 36 Routing Policy for Avaya SBCE continuation

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

Routing Policy Details Commit Cancel Help ?

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AmazonVC_AvayaSBC	10.70.4.213	Other	

Figure 37 Routing Policy for Avaya SBCE continuation

4.3.7 Dial Patterns

Dial Pattern for Avaya Aura CM

- Navigate to: **Routing > Dial Patterns**. Click **New**
- Set *Pattern*: **972598**
- Set *Min*: **6**
- Set *Max*: **36**
- Under **Originating Locations and Routing Policies**, Click **Add**, at the new window
- *Originating Location*: Select **Plano** (created in Section 4.3.3)
- *Routing Policies*: Select **SM to CM** under Routing Policies
- Click **Select** to return to **Dial Pattern Details** page
- Leave all other fields to default values.
- Click **Commit**

Dial Pattern Details Commit Cancel [Help ?](#)

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	plano		SM to CM	0	<input type="checkbox"/>	AACM10	

Select : All, None

Figure 38 Dial Pattern to Avaya CM

Dial Pattern to Amazon Chime SDK 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 **Plano** (created in Section 4.4.3)
- *Routing Policies*: Select **AmazonVCAvayaSBC** under **Routing Policies**
- Click **Select** to return to **Dial Pattern Details** page
- Leave all other fields to default values.
- Click **Commit**

The screenshot displays the 'Dial Pattern Details' configuration page. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'Commit' button. The 'General' section contains the following fields:

- * Pattern: 214242
- * Min: 10
- * Max: 12
- Emergency Call:
- SIP Domain: -ALL-
- Notes: (empty text box)

The 'Originating Locations and Routing Policies' section features an 'Add' button and a table with one item:

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	plano		AmazonVCAvayaSBC	0	<input type="checkbox"/>	AmazonVC_AvayaSBC	

Below the table, it says 'Select : All, None'.

Figure 39 Dial Pattern to Amazon via Avaya SBCE

4.4 Avaya SBCE Configuration

4.4.1 Avaya SBCE login

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



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

Figure 40 Avaya SBCE Login

- Under Device, select **ASBCE10** from drop down to expand the configuration for Avaya SBCE.

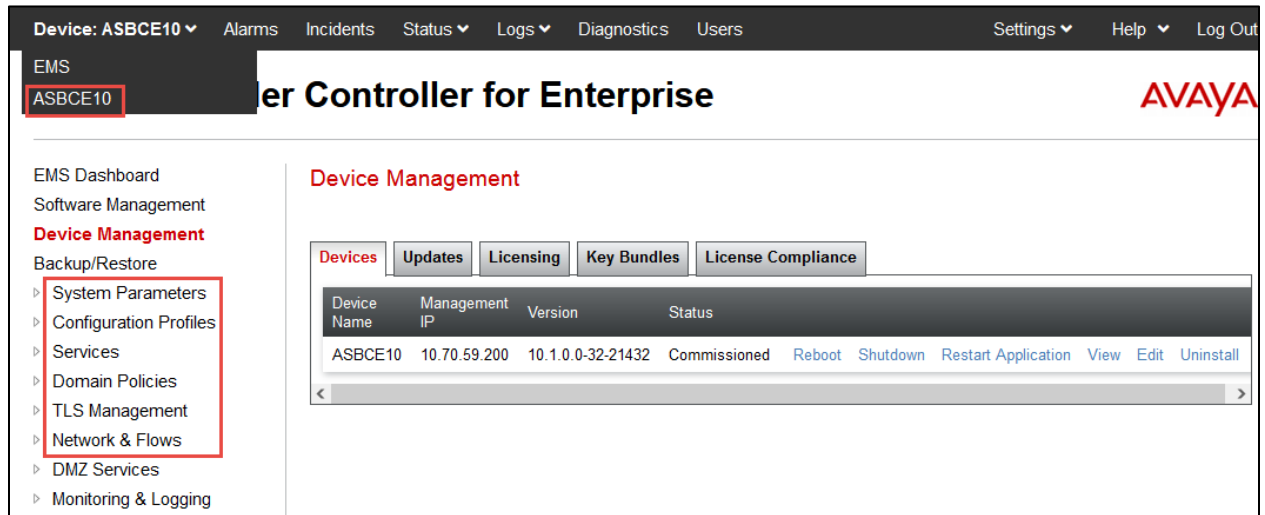


Figure 41 Selection of Avaya SBCE Device

4.4.2 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: **AASM10.1**
- Click **Finish**

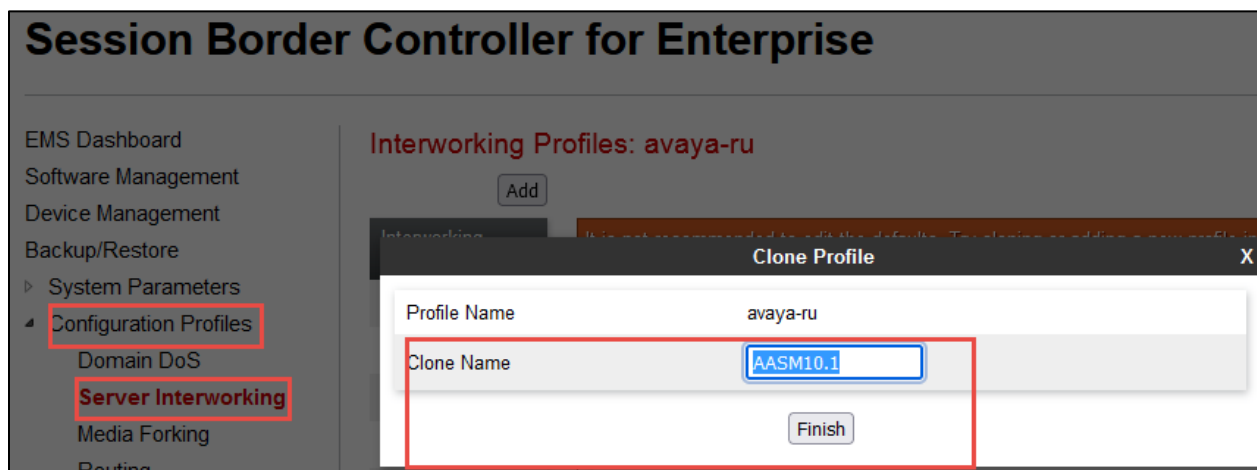


Figure 42 Server Interworking profile for Avaya SM

Interworking Profiles: AASM.10.1

Interworking Profiles

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediassec	No

Interworking Profiles

AASM.10.1

Figure 43 Server Interworking profile for Avaya SM continuation

Server Interworking for PSTN

- Repeat the same procedure to create the Interworking Profile to PSTN

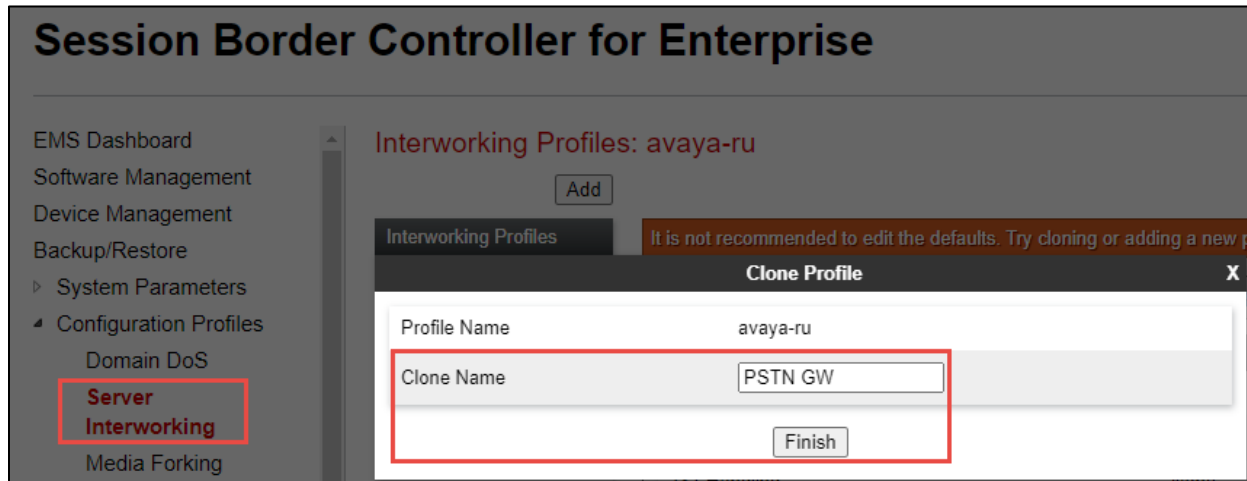


Figure 44 Server Interworking profile for PSTN

Server Interworking for Amazon Chime SDK Voice Connector

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

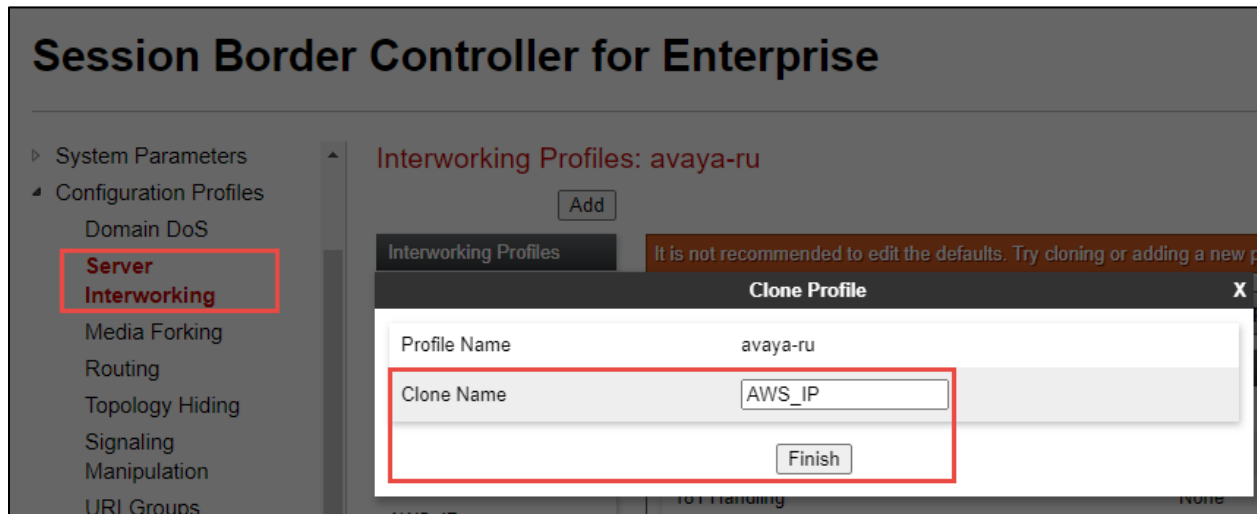


Figure 45 Server Interworking profile for Amazon

4.4.3 SIP Servers

SIP Server for Avaya SM

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



Figure 46 SIP Server for Avaya SM

Set *Server Type*: Select **Trunk 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**

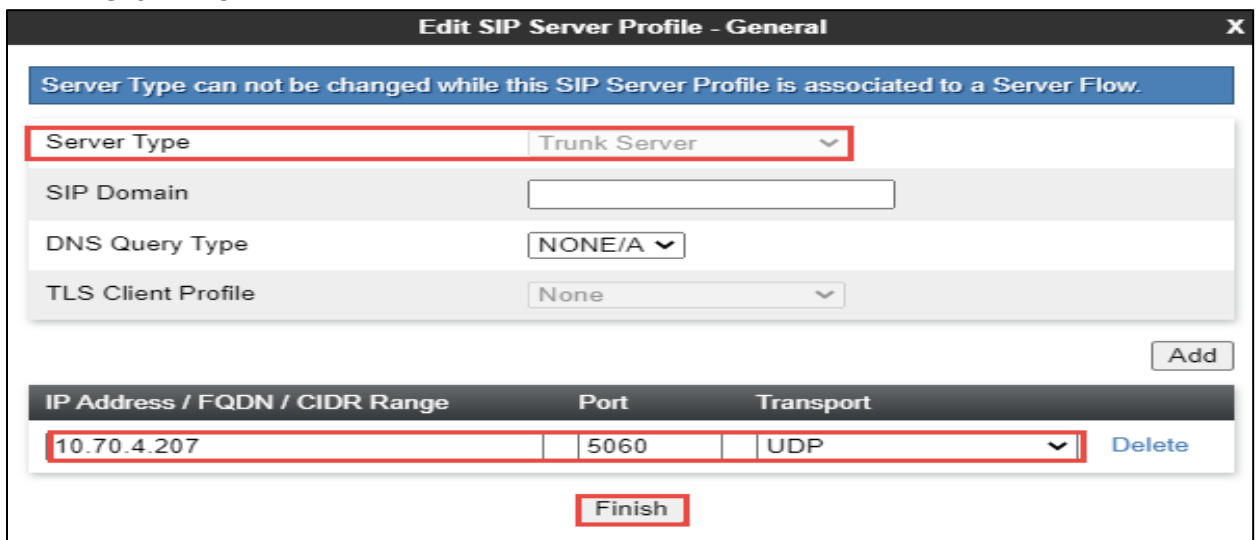


Figure 47 SIP Server for Avaya SM Continuation

- Navigate to **Advanced** tab
- Set *Enable Grooming*: **Checked**
- Set *Interworking Profile*: Select **AASM 10.1** (created in section 4.4.2)
- Click **Finish**

The screenshot shows a configuration window titled "Edit SIP Server Profile - Advanced". The window contains several settings:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	AASM.10.1 ▾
Signaling Manipulation Script	None ▾
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▾
NG911 Support	<input type="checkbox"/>

At the bottom center of the window is a button labeled "Finish".

Figure 48 SIP Server for Avaya SM Continuation

SIP Server for PSTN

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



Figure 49 SIP Server for PSTN

Set *Server Type*: Select **Trunk Server** from the drop down

- Set *IP Address/FQDN*: Enter the **PSTN IP Address**
- Set *Port*: **5060**
- Set *Transport*: **TCP**
- Click **Finish**

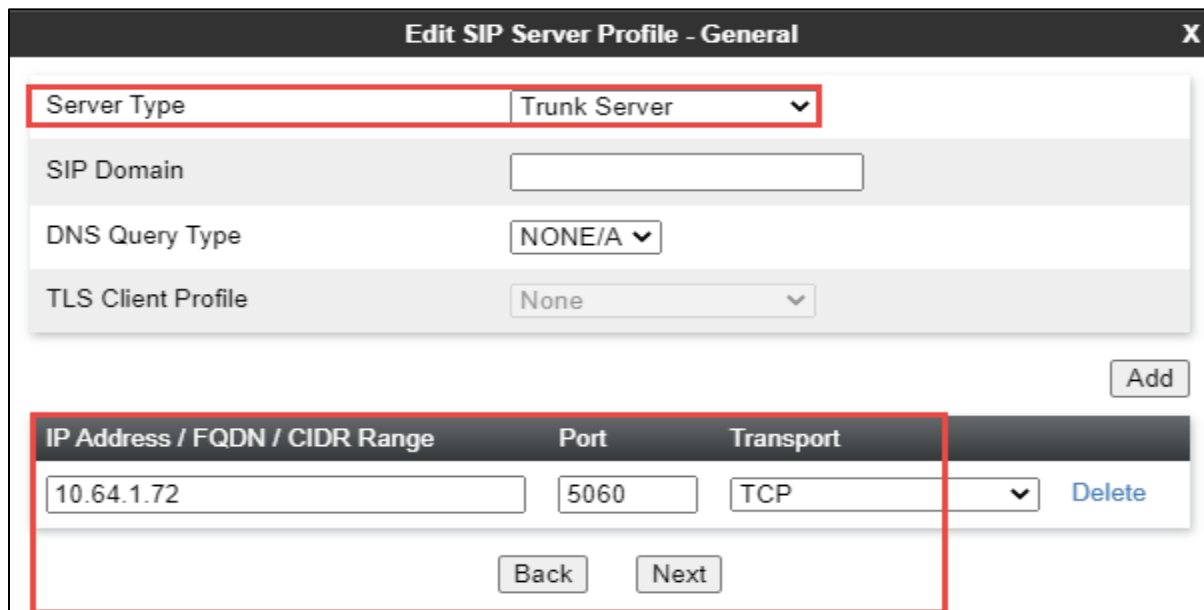


Figure 50 SIP Server for PSTN continuation

Navigate to **Advanced** tab

- Set *Interworking Profile*: Select **PSTN GW** (created in section 4.4.2)
- Click **Finish**

The screenshot shows a configuration window titled "Edit SIP Server Profile - Advanced". The window contains several settings:

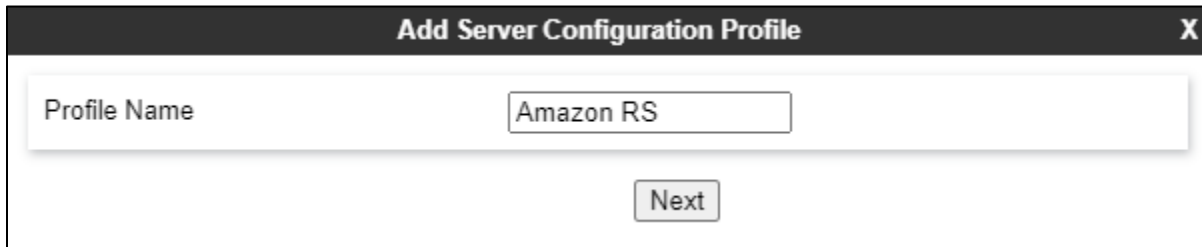
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	PSTN GW ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼
NG911 Support	<input type="checkbox"/>

At the bottom of the window, there is a button labeled "Finish".

Figure 51 SIP Server for PSTN continuation

SIP Server for Amazon Chime SDK Voice Connector

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

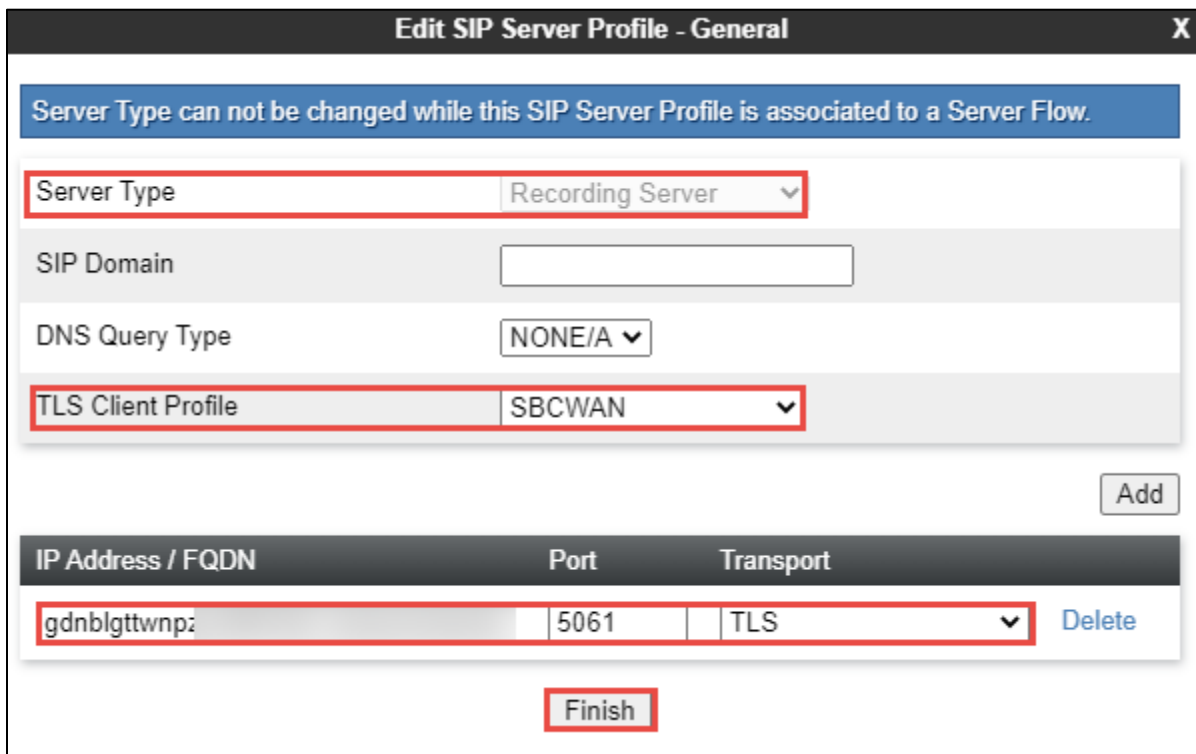


The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Amazon RS". Below the input field is a "Next" button.

Figure 52 SIP Server for Amazon

Set *Server Type*: Select **Recording Server** from the drop down

- TLS Client Profile: SBCWAN (created in section 4.4.13)
- Set *IP Address/FQDN*: Enter the **Amazon Chime SDK voice Connector Outbound Host Name**
- Set *Port*: **5061**
- Set *Transport*: **TLS**
- Click **Finish**



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. A blue banner at the top reads "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several configuration fields:

- Server Type**: Recording Server (dropdown menu)
- SIP Domain**: (empty text input field)
- DNS Query Type**: NONE/A (dropdown menu)
- TLS Client Profile**: SBCWAN (dropdown menu)

An "Add" button is located to the right of the TLS Client Profile field. Below these fields is a table with three columns: "IP Address / FQDN", "Port", and "Transport".

IP Address / FQDN	Port	Transport
gdnblgtwnp:	5061	TLS

A "Delete" button is located to the right of the table row. At the bottom of the dialog is a "Finish" button.

Figure 53 SIP Server for Amazon continuation

Navigate to **Advanced** tab

- Set *Interworking Profile*: Select **AWS_IP** (created in section 4.4.2)
- Set *Signaling Manipulation Script*: Select **AMZURI** (Created in Section 4.4.15)
- Click **Finish**

The screenshot shows a configuration window titled "Edit SIP Server Profile - Advanced". The window contains several settings:

- Enable Grooming:
- Interworking Profile:
- Signaling Manipulation Script:
- Securable:
- Enable FGDN:
- TCP Failover Port:
- TLS Failover Port:
- Tolerant:
- URI Group:
- NG911 Support:

A red box highlights the "Interworking Profile" and "Signaling Manipulation Script" fields. Another red box highlights the "Finish" button at the bottom center of the window.

Figure 54 SIP Server for Amazon continuation

4.4.4 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**

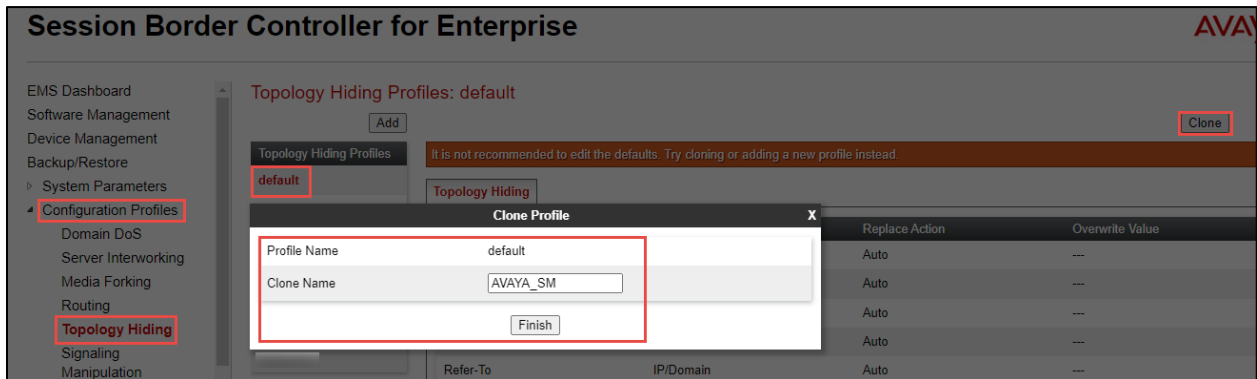


Figure 55 Topology Hiding Profile for Avaya SM

- 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*: **lab.xxxxxxxx.com**

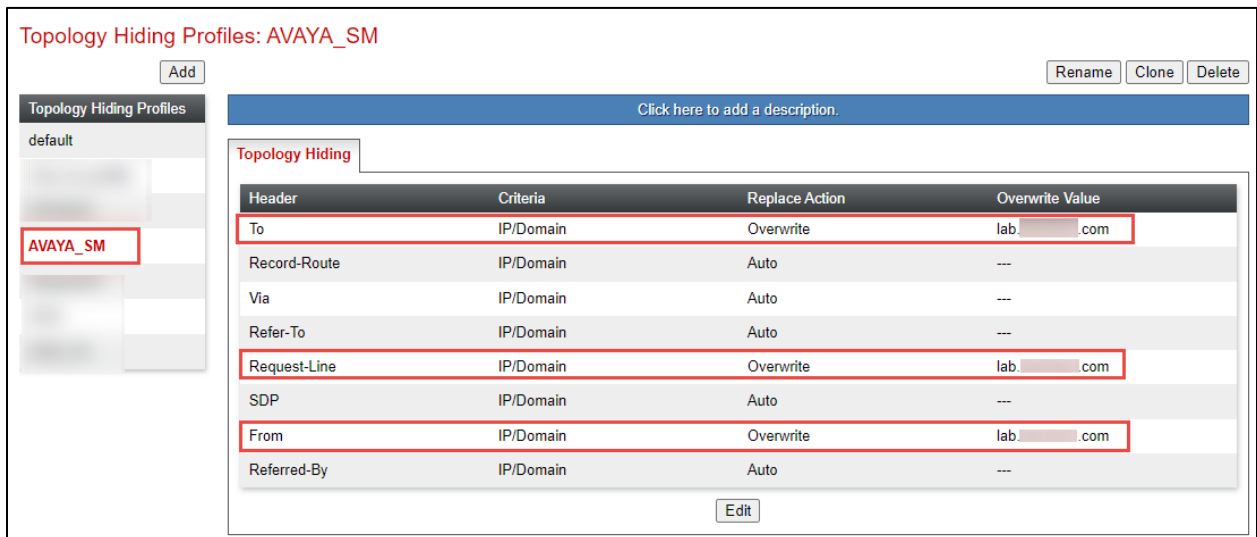


Figure 56 Topology Hiding Profile for Avaya SM continuation

Topology hiding profile for PSTN

- Repeat the same procedure to create the profile for **PSTNGW**
- *Overwrite Value:* Replace the **To** header and **Request-Line** header with **IP address of PSTN**
- Click **Finish**

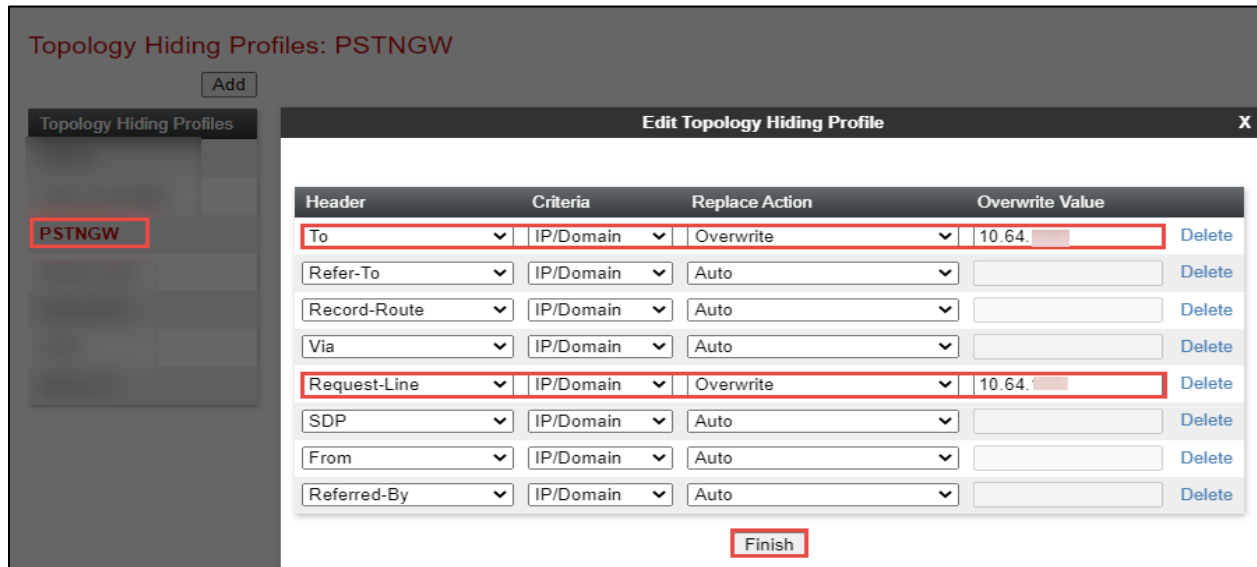


Figure 57 Topology Hiding Profile for PSTN

Topology hiding profile for Amazon Chime SDK Voice connector

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

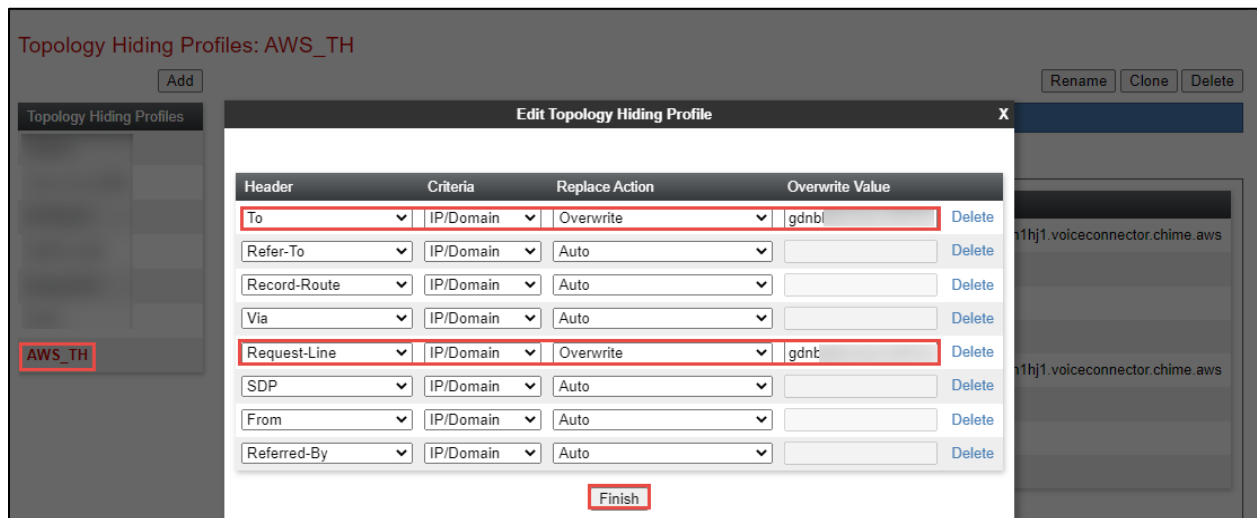


Figure 58 Topology Hiding Profile for Amazon

4.4.5 Routing

Routing for Avaya SM

- Navigate to: **Configuration Profiles > Routing**
- Click **Add**
- Set *Profile Name*: **Avaya_SM**
- Click **Next**

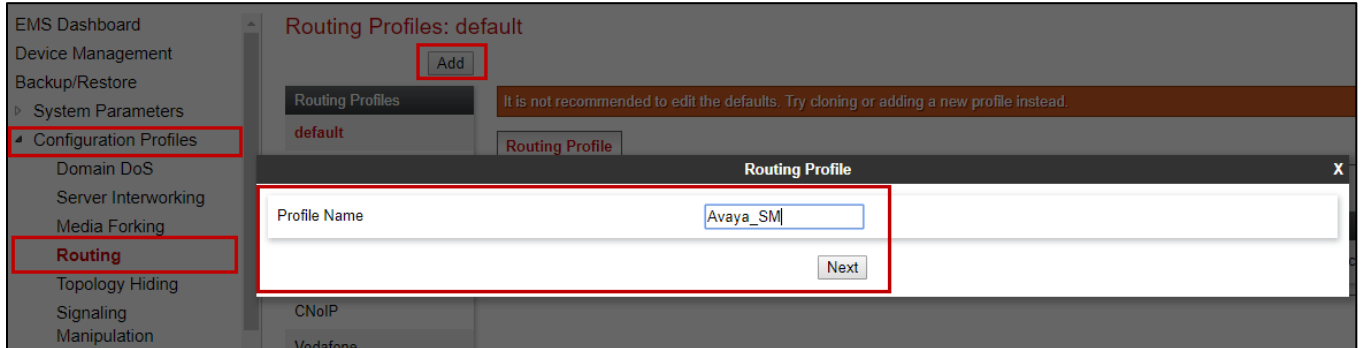


Figure 59 Routing for Avaya SM

- At Routing Profile Window, Click **Add**
- Set *Priority/Weight*: **1**
- Set *Server Configuration*: **Avaya_SM** (configured in section 4.4.3)
- The **Server IP, Port** and **Transport Protocol** populates automatically
- Click **Finish**

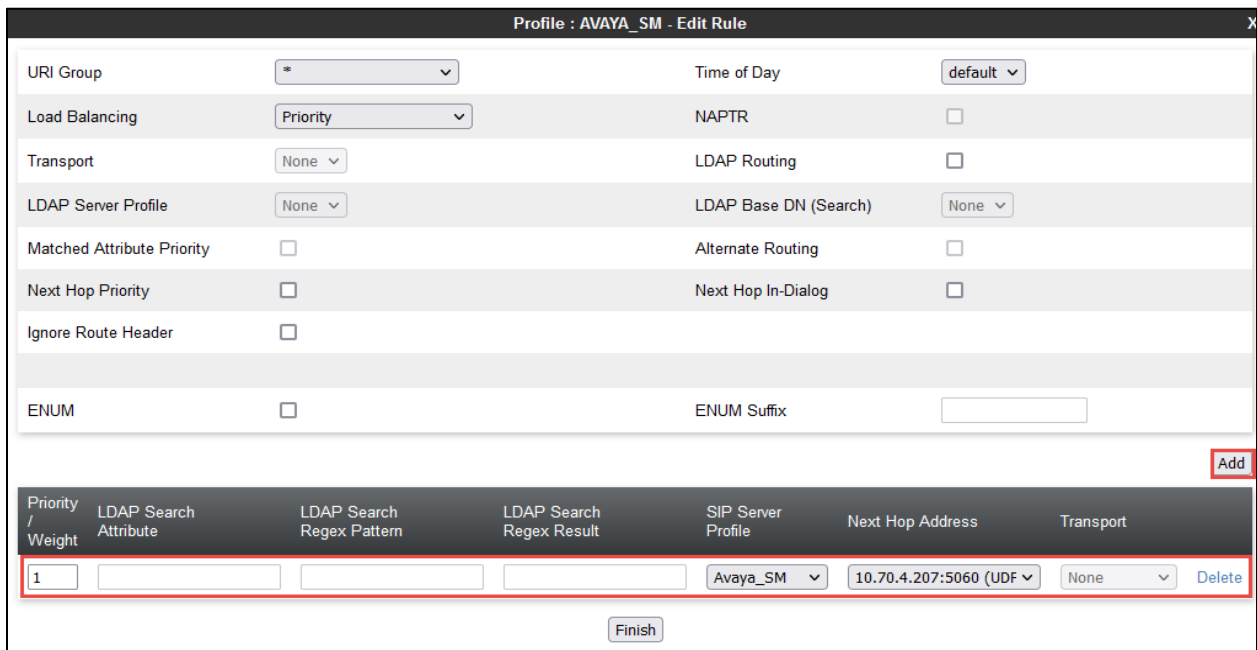


Figure 60 Routing for Avaya SM continuation

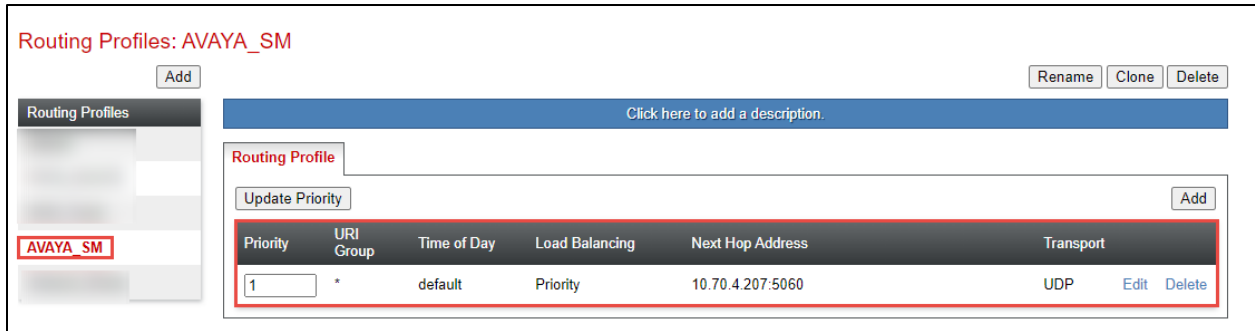


Figure 61 Routing for Avaya SM continuation

Routing for PSTN

- Repeat the same steps to create the Routing Profile for **PSTN**
- Set *Priority/Weight*: **1**
- Set *Server Configuration*: **PSTN GW** (configured in section 4.4.3)
- The **Server IP, Port** and **Transport Protocol** populates automatically
- Click **Finish**

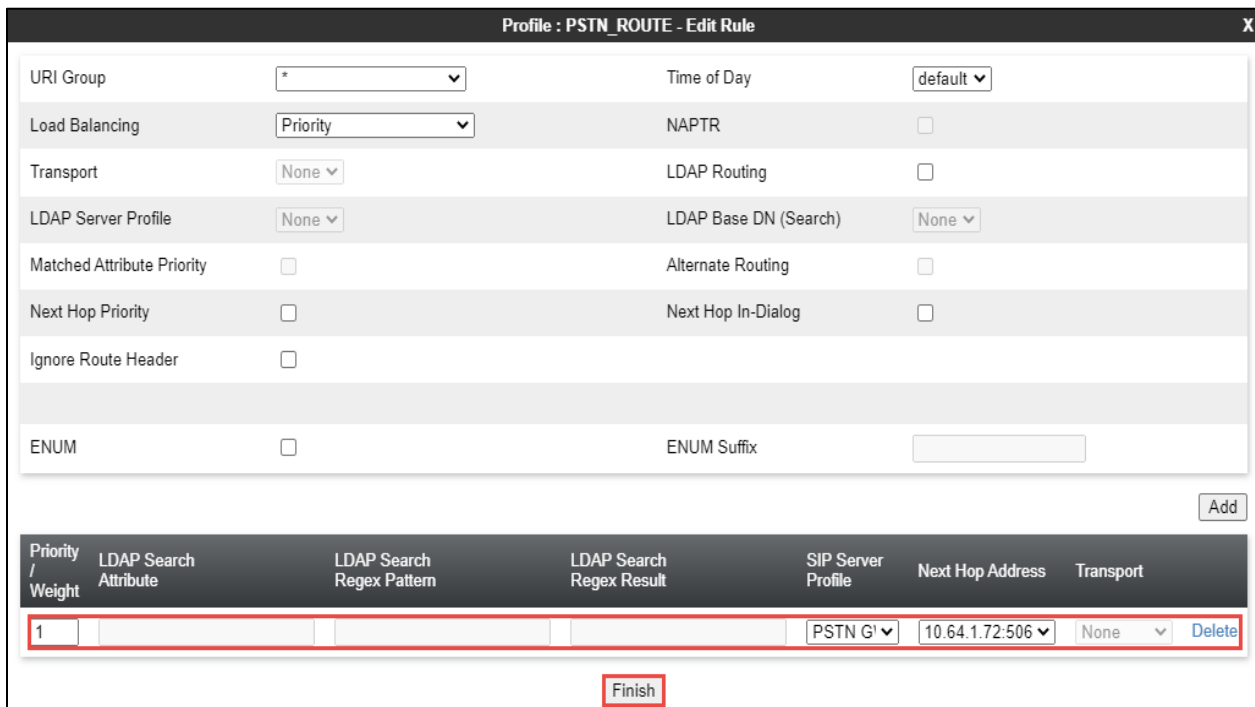


Figure 62 Routing for PSTN

Routing for Amazon

- Repeat the same steps to create the Routing Profile **Amazon_Route** for Amazon
- Set *Priority/Weight*: **1**
- Set *Server Configuration*: **Amazon RS** (configured in section 4.4.3)
- The **Server IP/FQDN, Port** and **Transport Protocol** populates automatically
- Click **Finish**

Profile : Amazon_Route - Edit Rule X

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Amazon		None	Delete

Figure 63 Routing for Amazon

4.4.6 Recording Profile

- Navigate to: **Configuration > Recording Profile**
- Click **Add**
- Set *Profile Name*: **Amazon_RP**
- Click **Next**

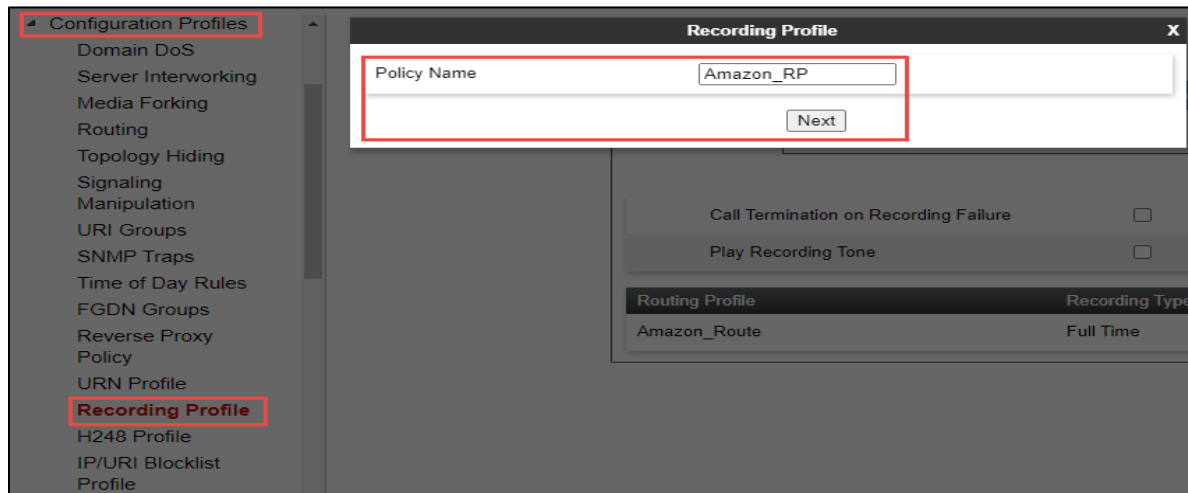


Figure 64 Recording Profile for Amazon

- Set Routing Profile: Select **Amazon_Route** (configured in section 4.4.5)
- Set Recording Type: Select **Full Time** from the dropdown
- Click **Finish**

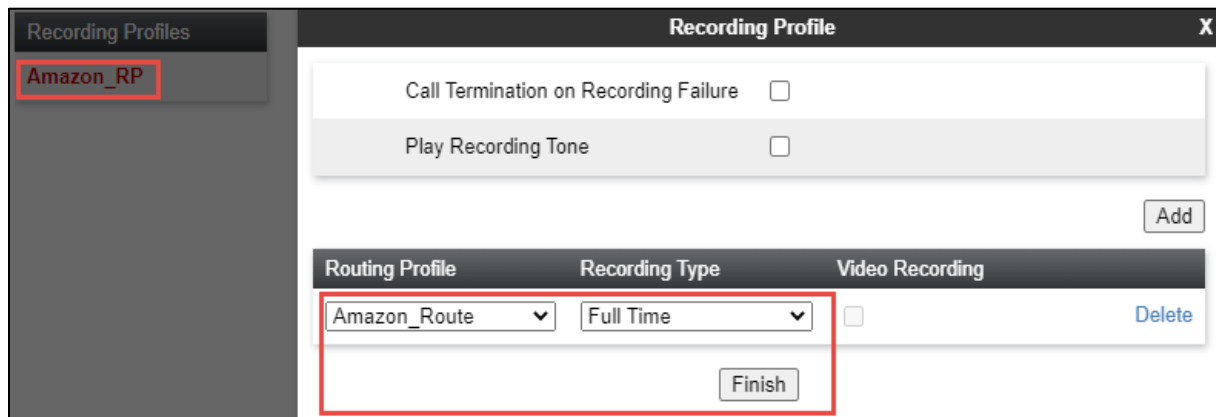


Figure 65 Recording Profile continuation for Amazon

4.4.7 Session Policies

- Navigate to: **Domain Policies > Session Policies**

- Select **default** under Session Policies, Click **Clone**
- Set *Profile Name*: **Amazon_SP**
- Click **Next**

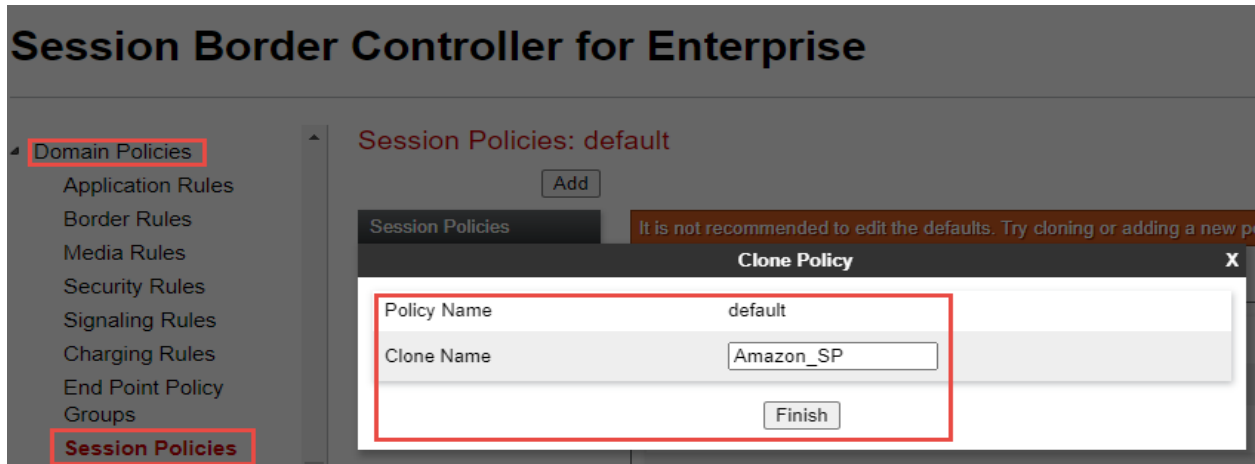


Figure 66 Session Profile for Amazon

- Media Anchoring: **Checked**
- Recording Server: **Checked**
- Set Routing Profile: Select the route profile **Amazon_RP** (configured in section 4.4.6)
- Click **Finish**

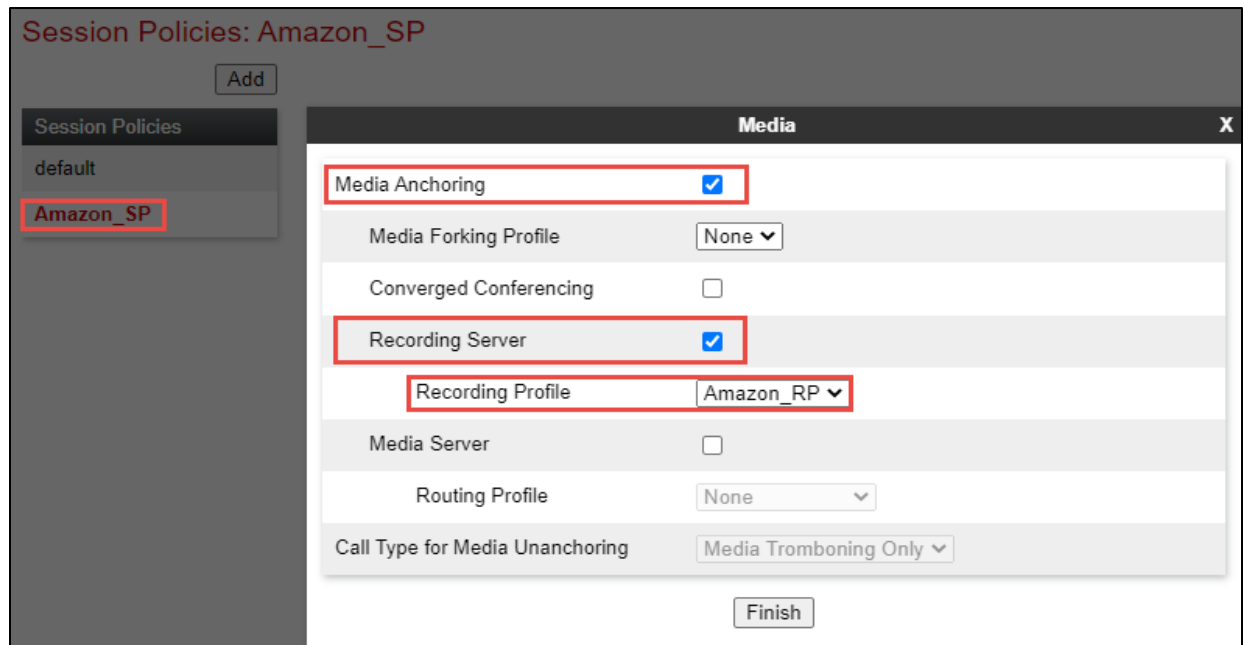


Figure 67 Session Profile Continuation for Amazon

4.4.8 Session Flows

- Navigate to: **Network and Flows > Session Flows**

- Click **ADD**
- Set *Name*: **Amazon_SF**
- Select Session Policy: **Amazon_SP** (configured in section 4.4.7)
- Click **Finish**

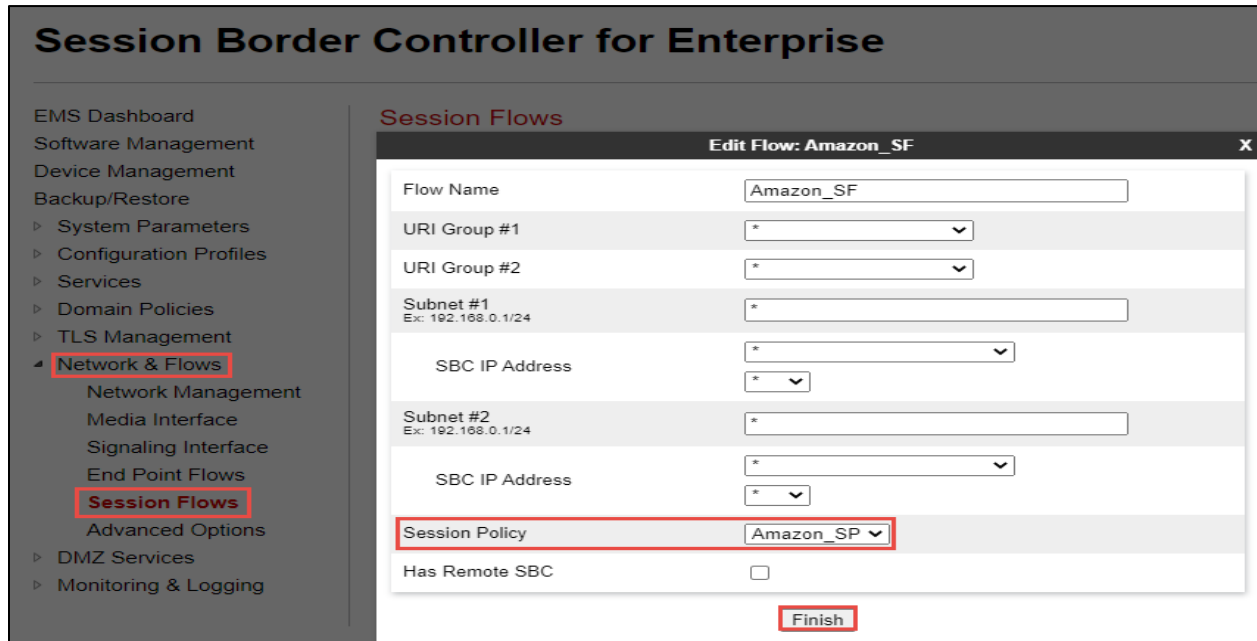


Figure 68 Session Flow for Amazon

4.4.9 Signaling Rules

Signaling rule for Avaya

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

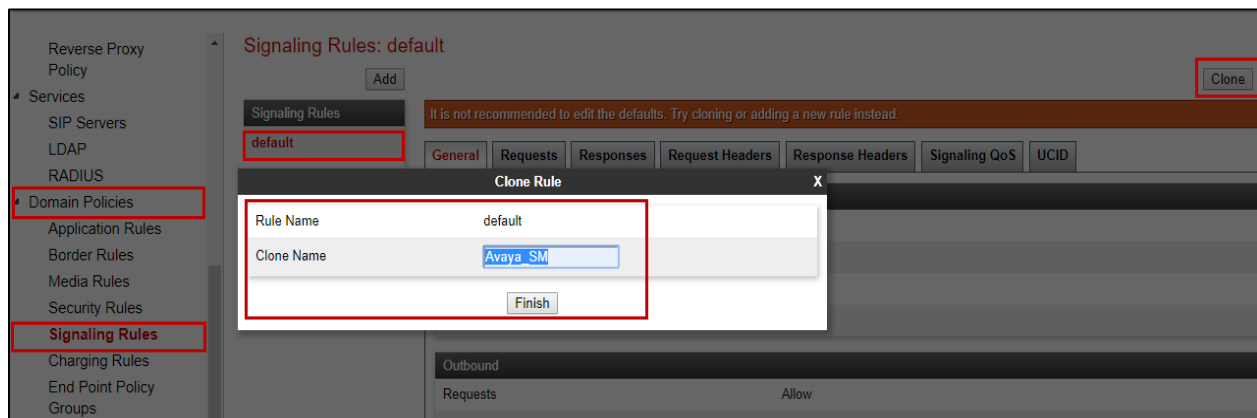


Figure 69 Signaling Rules for Avaya SM

- 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**

Figure 70 Signaling Rules for Avaya SM continuation

- Repeat the same steps for all other required headers

Figure 71 Signaling Rules for Avaya SM continuation

- Repeat the same steps for Response Headers

Signaling Rules: Avaya_SM

Rename Clone Delete

Add

Click here to add a description.

General Requests Responses Request Headers **Response Headers** Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
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-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Figure 72 Signaling Rules for Avaya SM continuation

4.4.10 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 SDK 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**

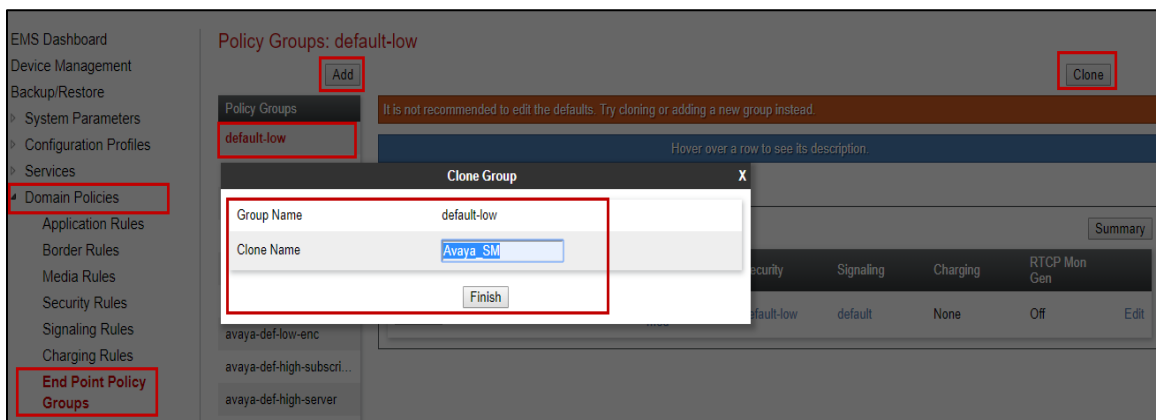


Figure 73 End Point Policy Group for Avaya SM

- Select the newly created Group **Avaya_SM**, Click **Edit**
- Set *Signaling Rule*: **Avaya_SM**
- Click **Finish**

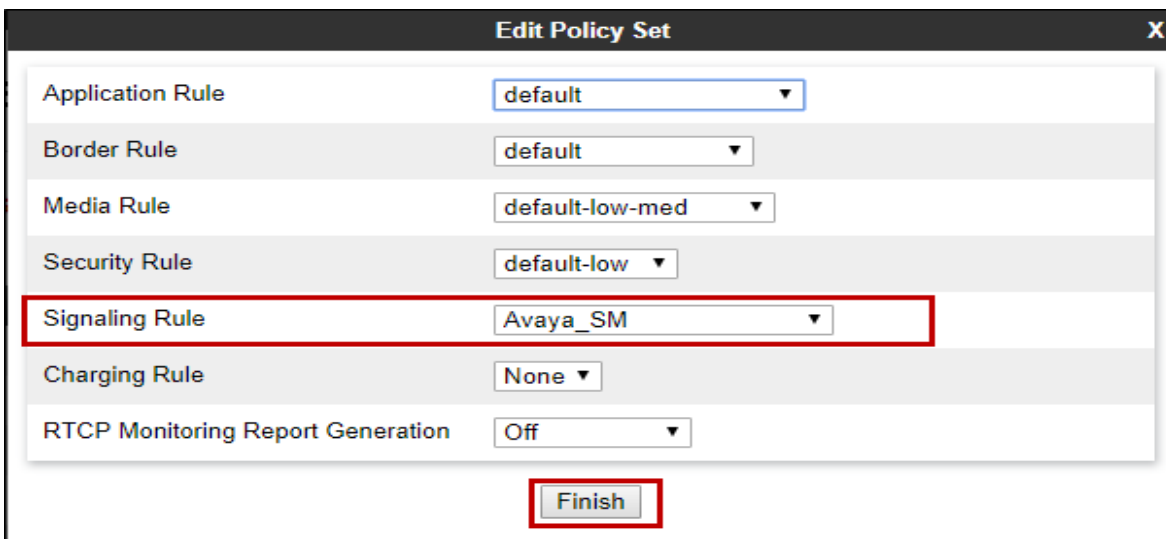


Figure 74 End Point Policy Group for Avaya SM Continuation

End Point Policy Group for PSTN

- Repeat the same steps to create End Policy Group for PSTN

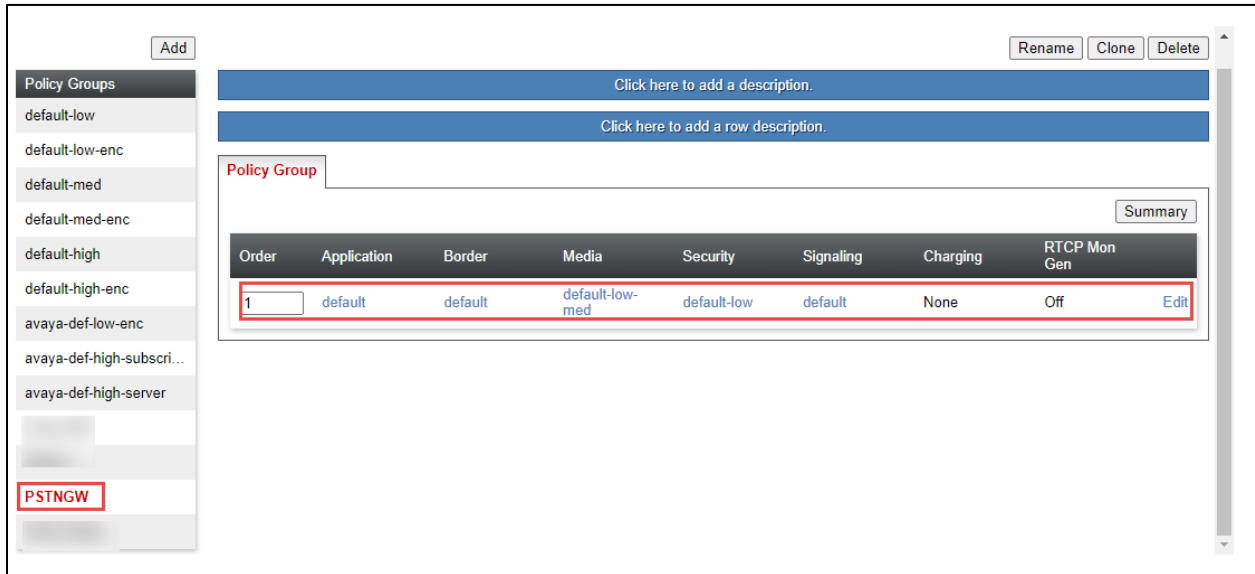


Figure 75 End Point Policy Group for PSTN

End Point Policy Group for Amazon

- Repeat the same steps to create End Policy Group for Amazon Chime SDK Voice Connector
- Select Media Rule: **AWS_MR** (configured in section 4.4.14)

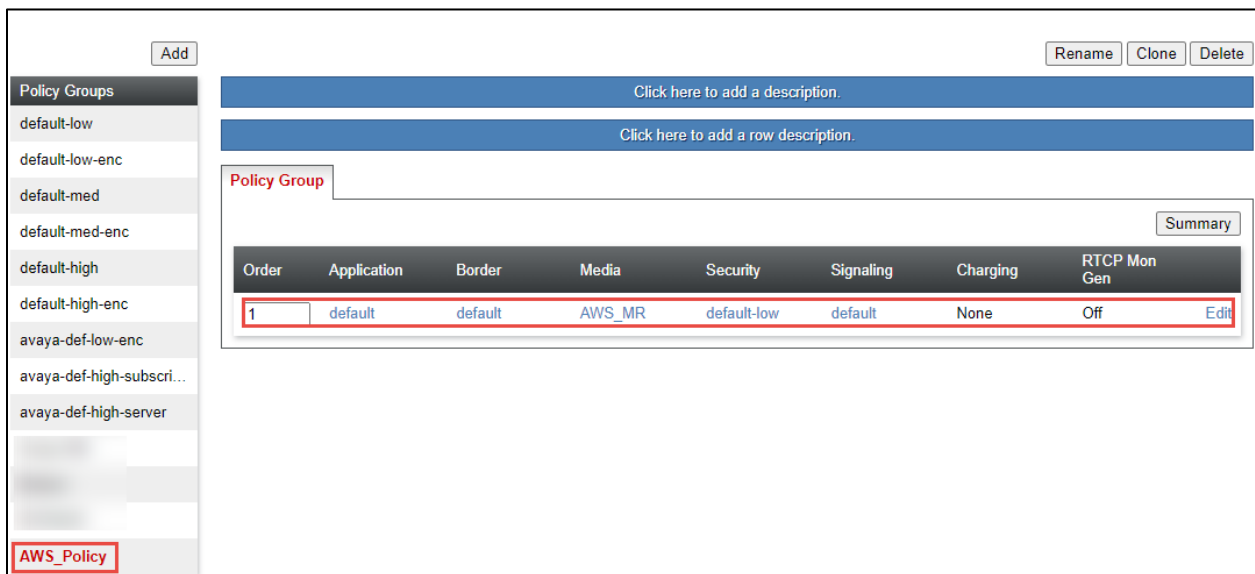


Figure 76 End Point Policy Group for Amazon

4.4.11 Media Interface

- Navigate to: **Network & Flows > Media Interface**. Click **Add**
- Set **Name**: **MI_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 10.70.4.213
- Set **Port Range**: **35000-40000**
- Click **Finish**

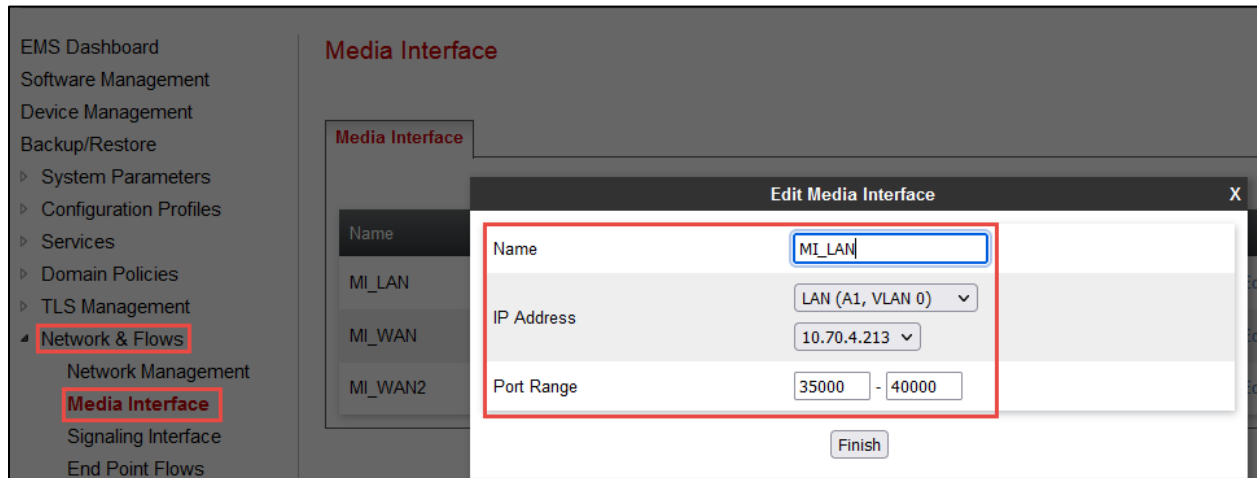


Figure 77 Media Interface facing Avaya SM

- Repeat the same steps to create a Media Interface facing PSTN

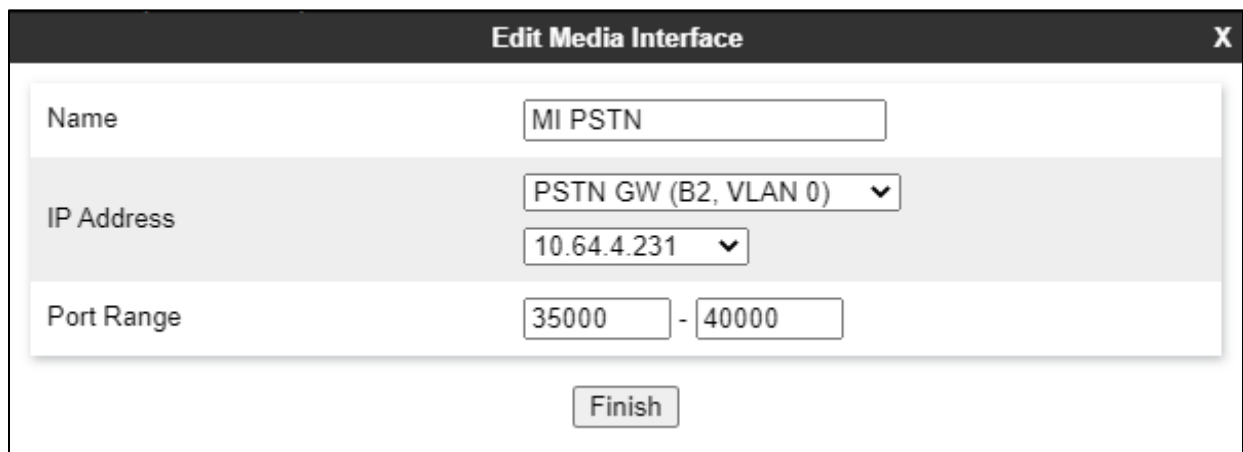


Figure 78 Media Interface facing PSTN

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

Name	<input type="text" value="MI_WAN"/>
IP Address	<input type="text" value="WAN (B1, VLAN 0)"/> <input type="text" value="192.65."/> <input type="text"/>
Port Range	<input type="text" value="48796"/> - <input type="text" value="48883"/>

Figure 79 Media Interface facing Amazon

4.4.12 Signaling Interface

Signaling Interface for Avaya SM

- Navigate to: **Network & Flows > Signaling Interface**. Click **Add**, new **Add Signaling Interface** window appears
- Set **Name**: **SI_LAN** is given for the interface facing Avaya Aura SM
- Set **IP Address**: Select **LAN (A1, VLAN 0)**
- Set **UDP Port**: **5060**
- Click **Finish**

The screenshot shows the 'Edit Signaling Interface' window in the EMS Dashboard. The left sidebar contains a navigation menu with 'Network & Flows' and 'Signaling Interface' highlighted. The main window displays the configuration for the 'SI_LAN' interface. The configuration fields are as follows:

Field	Value
Name	SI_LAN
IP Address	LAN (A1, VLAN 0)
IP Address	10.70.4.213
TCP Port	5060
UDP Port	5060
TLS Port	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

A red box highlights the Name, IP Address, TCP Port, and UDP Port fields. A 'Finish' button is located at the bottom right of the window.

Figure 80 Signaling Interface facing Avaya SM

Signaling Interface for PSTN

- Repeat the same steps to create the Signaling Interface facing PSTN. TCP is used between Avaya SBCE and PSTN.

The screenshot displays the 'Edit Signaling Interface' configuration window. The left sidebar contains a navigation menu with the following items: Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies, TLS Management, Network & Flows (highlighted), Network Management, Media Interface, Signaling Interface (highlighted), End Point Flows, Session Flows, Advanced Options, and DMZ Services. The main configuration area is titled 'Edit Signaling Interface' and contains the following fields:

Field	Value
Name	SI_PSTN
IP Address	PSTN GW (B2, VLAN 0) (dropdown showing 10.64.4.231)
TCP Port	5060
UDP Port	Leave blank to disable
TLS Port	Leave blank to disable
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

A 'Finish' button is located at the bottom right of the configuration area.

Figure 81 Signaling Interface facing PSTN

Signaling Interface for Amazon Chime SDK Voice Connector

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

The screenshot displays the 'Edit Signaling Interface' configuration window. The left sidebar shows the navigation menu with 'Network & Flows' and 'Signaling Interface' highlighted. The main configuration area includes the following fields:

Field	Value
Name	SI_WAN
IP Address	WAN (B1, VLAN 0) / 192
TCP Port	
UDP Port	
TLS Port	5061
TLS Profile	SBCWAN
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

A 'Finish' button is located at the bottom right of the configuration area.

Figure 82 Signaling Interface facing Amazon

4.4.13 End Point Flows

- Navigate to: **Network & Flows > End Point Flows > Server Flows**. Click **Add**
- Set *Flow Name*: **Avaya_SM**
- Set *SIP Server Profile*: **Avaya** created in section 4.4.3 is selected
- Set *Transport*: *
- Set *Received Interface*: **SI_PSTN**
- Set *Signaling Interface*: **SI_LAN**
- Set *Media Interface*: **MI_LAN**
- Set *End Point Policy Group*: **Avaya SM** (section 4.4.10)
- Set *Routing Profile*: **PSTN_ROUTE** (section 4.4.6)
- Set *Topology Hiding Profile*: **AVAYA_SM** (section 4.4.4)
- Click **Finish**

The screenshot shows the 'Edit Flow: Avaya_SM' configuration window. The window title is 'Edit Flow: Avaya_SM' with a close button 'X' in the top right corner. The configuration is organized into several sections, with three sections highlighted by red boxes:

- Section 1 (Top):** Flow Name: Avaya_SM; SIP Server Profile: Avaya (dropdown).
- Section 2 (Middle):** Received Interface: SI_PSTN (dropdown); Signaling Interface: SI_LAN (dropdown); Media Interface: MI_LAN (dropdown).
- Section 3 (Bottom):** End Point Policy Group: Avaya SM (dropdown); Routing Profile: PSTN_ROUTE (dropdown); Topology Hiding Profile: AVAYA_SM (dropdown).

Other visible fields include: URI Group: * (dropdown); Transport: * (dropdown); Remote Subnet: * (text field); Secondary Media Interface: None (dropdown); Signaling Manipulation Script: None (dropdown); Remote Branch Office: Any (dropdown); Link Monitoring from Peer: ; FQDN Support: ; FQDN: (text field). A 'Finish' button is located at the bottom center of the window.

Figure 83 Server Flow for Avaya SM

- Repeat the same steps to create a Server Flow for PSTN.

Edit Flow: PSTN GW	
Flow Name	PSTN GW
SIP Server Profile	PSTN GW
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	SI_LAN
Signaling Interface	SI_PSTN
Media Interface	MI PSTN
Secondary Media Interface	None
End Point Policy Group	PSTNGW
Routing Profile	AVAYA_SM
Topology Hiding Profile	PSTNGW
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
Finish	

Figure 84 Server Flow for PSTN

- Repeat the same steps to create a Server Flow for Amazon Chime SDK Voice Connector

Edit Flow: Amazon	
Flow Name	Amazon
SIP Server Profile	Amazon RS
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	SI_LAN
Signaling Interface	SI_WAN
Media Interface	MI_WAN
Secondary Media Interface	None
End Point Policy Group	AWS_Policy
Routing Profile	Amazon_Route
Topology Hiding Profile	AWS
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

Figure 85 Server Flow for Amazon

Edit Flow: Amazon1
✕

Flow Name	<input style="width: 90%;" type="text" value="Amazon1"/>
SIP Server Profile	<input style="width: 90%;" type="text" value="Amazon RS"/> ▼
URI Group	<input style="width: 90%;" type="text" value="*"/> ▼
Transport	<input style="width: 90%;" type="text" value="*"/> ▼
Remote Subnet	<input style="width: 90%;" type="text" value="*"/>
Received Interface	<input style="width: 90%;" type="text" value="SI_PSTN"/> ▼
Signaling Interface	<input style="width: 90%;" type="text" value="SI_WAN"/> ▼
Media Interface	<input style="width: 90%;" type="text" value="MI_WAN"/> ▼
Secondary Media Interface	<input style="width: 90%;" type="text" value="None"/> ▼
End Point Policy Group	<input style="width: 90%;" type="text" value="AWS_Policy"/> ▼
Routing Profile	<input style="width: 90%;" type="text" value="Amazon_Route"/> ▼
Topology Hiding Profile	<input style="width: 90%;" type="text" value="AWS"/> ▼
Signaling Manipulation Script	<input style="width: 90%;" type="text" value="None"/> ▼
Remote Branch Office	<input style="width: 90%;" type="text" value="Any"/> ▼
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input style="width: 90%;" type="text"/>

Figure 86 Server Flow for Amazon Continuation

4.4.14 TLS Configuration

The following are necessary steps to configure the protocol TLS between Avaya SBCE and Amazon Chime SDK 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**

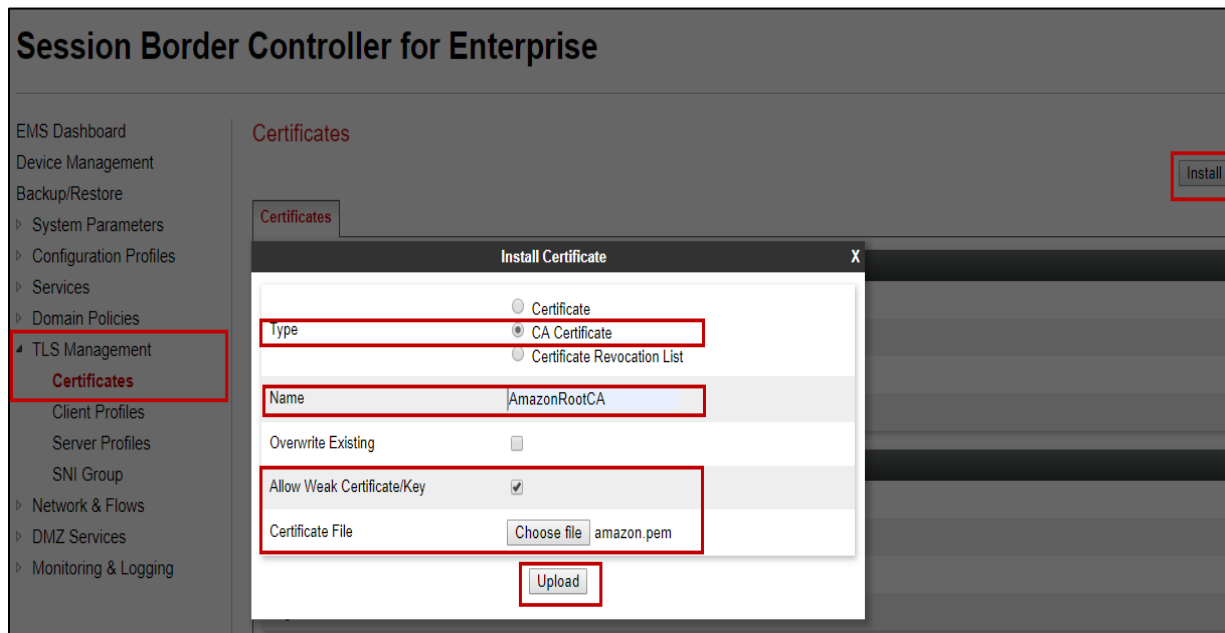


Figure 87 Upload Amazon Root CA

Client Profile for Amazon Chime SDK Voice Connector

- Navigate to: **TLS management > Client Profiles**. Click **Add**
- Set *Profile Name*: **SBCWAN** is given for interface facing Amazon Chime SDK Voice Connector
- Set *Certificate*: select server certificate **asbce10.crt** for Avaya SBCE interface facing Amazon Chime SDK Voice Connector
- Set *Peer Certificate Authorities*: Select **AmazonRootCA.Pem** which is uploaded in previous step
- Set *Verification Depth*: 5
- Click **Next**

Session Border

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▾ Services
 SIP Servers
 H248 Servers
 LDAP
 RADIUS
▸ Domain Policies
▾ TLS Management
 Certificates
 Client Profiles
 Server Profiles
 SNI Group
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Edit Profile

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.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name:

Certificate:

SNI: Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

Extended Hostname Verification:

Server Hostname:

Figure 88 Client Profile facing Amazon

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

Edit Profile X

Renegotiation Parameters

Renegotiation Time seconds

Renegotiation Byte Count

Handshake Options

Version TLS 1.2 TLS 1.1 TLS 1.0

Ciphers Default FIPS Custom

Value (What's this?)

Figure 89 Client Profile facing Amazon Continuation

Server Profile for Amazon Chime SDK Voice Connector

- Navigate to: **TLS management > Server Profiles**. Click **Add**
- Set *Profile Name*: **SBCWAN** is given for interface facing Amazon Chime SDK Voice Connector
- Set *Certificate*: Select server certificate **asbce10.crt** for Avaya SBCE interface facing Amazon Chime SDK Voice Connector
- Set *Peer Verification*: **None**
- Click **Next**

Session Border

EMS Dashboard
Software Management
Device Management
Backup/Restore
‣ System Parameters
‣ Configuration Profiles
‣ Services
 SIP Servers
 H248 Servers
 LDAP
 RADIUS
‣ Domain Policies
‣ TLS Management
 Certificates
 Client Profiles
 Server Profiles
 SNI Group
‣ Network & Flows
‣ DMZ Services
‣ Monitoring & Logging

Edit Profile X

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.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name: SBCWAN

Certificate: asbce10.crt

SNI Options: None

SNI Group: None

Certificate Verification

Peer Verification: None

Peer Certificate Authorities: AmazonRootCA.pem

Peer Certificate Revocation Lists:

Verification Depth: 0

Next

Figure 90 Server Profile facing Amazon

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

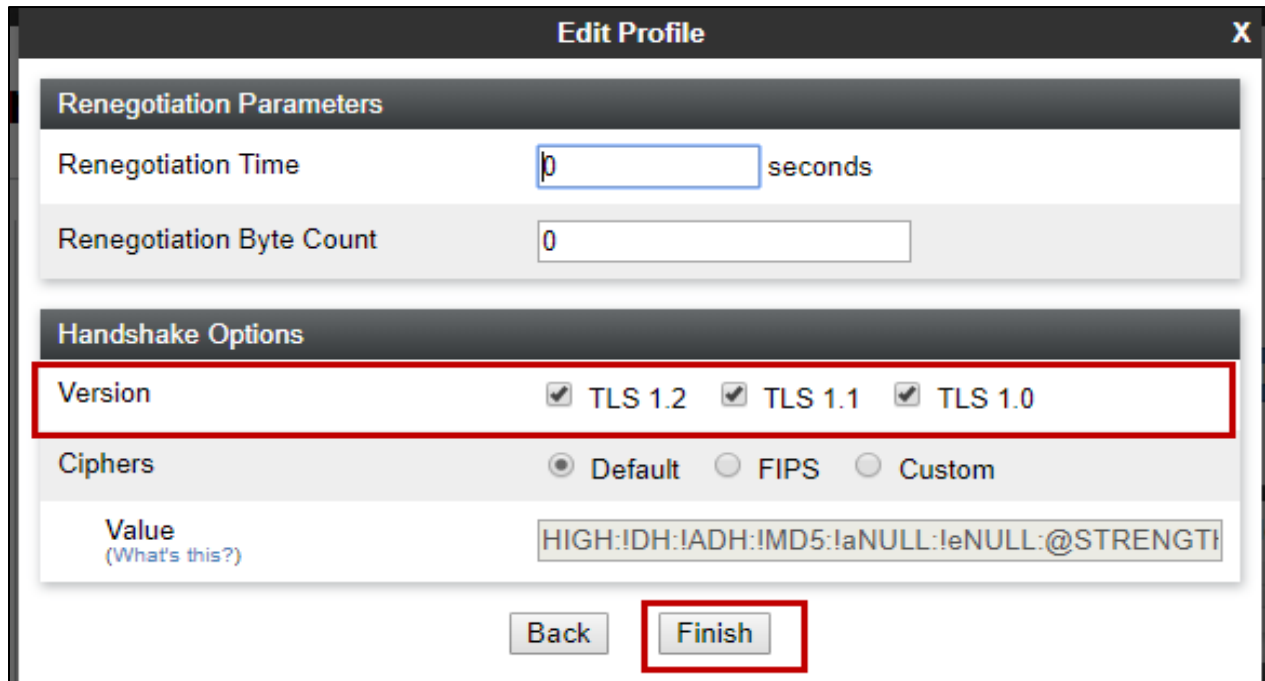


Figure 91 Server Profile facing Amazon Continuation

Configure SRTP

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

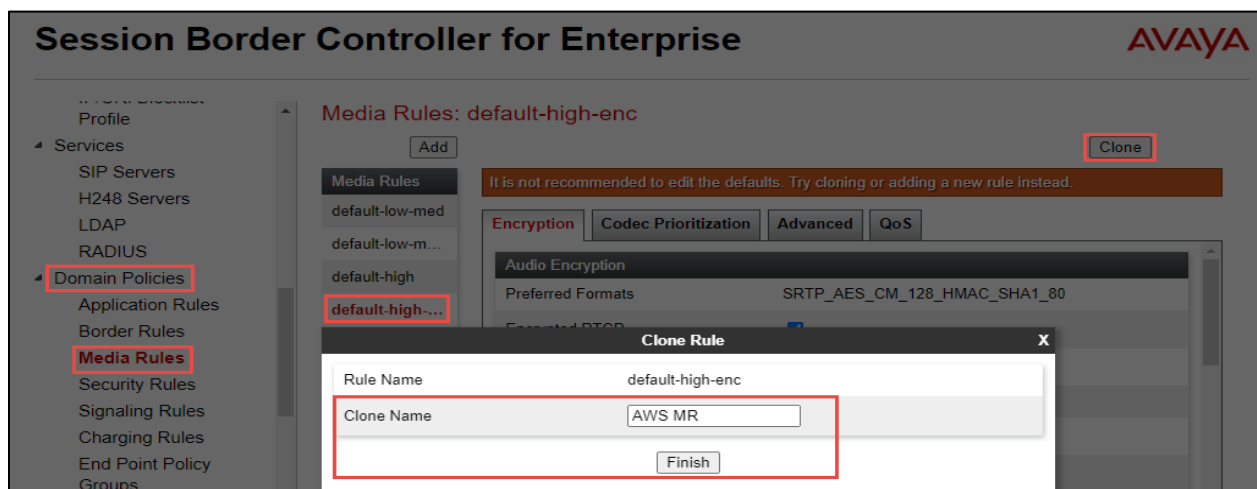


Figure 92 Media Rule – Amazon

- Select newly created Media Rule **AWS MR**, Click **Edit**
- Set Preferred Format #1: **SRTP_AES_CM_128_HMAC_SHA1_80**
- Set Interworking under Audio Encryption: **Unchecked**
- Click **Finish**

Media Encryption X

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	NONE ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
<u>MKI</u>	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input style="width: 50px;" type="text"/>
Interworking	<input type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	NONE ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
<u>MKI</u>	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input style="width: 50px;" type="text"/>
Interworking	<input type="checkbox"/>
Symmetric Context Reset	<input type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

Capability Negotiation	<input type="checkbox"/>
------------------------	--------------------------

Figure 93 Media Rule – Amazon Continuation

Edit End Point Policy Groups

- Navigate to: **Domain Policies > End Point Policy Groups**
- Select **AWS** under Policy Groups
- Set *Media Rule*: Select **AWS_MR**
- Click **Finish**

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
1	default	default	AWS_MR	default-low	default	None	Off

Figure 94 Edit End Point policy Group – Amazon

4.4.15 Signaling Manipulation

- Navigate to **Configuration Profiles>Signaling Manipulation**
- Click **ADD**
- Set *Title*: **AMZURI**
- Provide the required manipulation rule and Click **Save**

```
1 within session "INVITE"
2 {
3   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="INVITE"
4   {
5     %HEADERS["Request_Line"][1].URI.USER.regex_replace("^","+1972 ");
6   }
7 }
```

Figure 95 Signaling Manipulation Rule for Amazon