



**Amazon Chime Voice Connector**

**SIP Trunking Configuration Guide:**

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

**September 2022**

## Document History

| <b>Rev. No.</b> | <b>Date</b>       | <b>Description</b>                      |
|-----------------|-------------------|---|
| 1.0             | Oct-24-2019       | SIP Trunk Configuration Guide           |
| 1.1             | Feb-6-2020        | Minor edits based on feedback           |
| 2.0             | September-19-2022 | Updated for Avaya CM 10.1 and SBCe 10.1 |

## Table of Contents

|       |  |    |
|-------|--|----|
| 1     | Audience .....                                 | 7  |
| 1.1   | Amazon Chime Voice Connector .....             | 7  |
| 2     | SIP Trunking Network Components .....          | 8  |
| 2.1   | Hardware Components .....                      | 9  |
| 2.2   | Software Requirements .....                    | 9  |
| 3     | Features .....                                 | 10 |
| 3.1   | Features Supported .....                       | 10 |
| 3.2   | Features Not Supported .....                   | 11 |
| 3.3   | Features Not Tested .....                      | 11 |
| 3.4   | Caveats and Limitations.....                   | 11 |
| 4     | Configuration .....                            | 12 |
| 4.1   | Configuration Checklist .....                  | 12 |
| 4.2   | Avaya Aura CM Configuration .....              | 12 |
| 4.2.1 | Avaya Aura CM Login .....                      | 12 |
| 4.2.2 | IP Node Name.....                              | 14 |
| 4.2.1 | IP Codec Set.....                              | 15 |
| 4.2.2 | IP Network Region .....                        | 16 |
| 4.2.3 | Signaling Group .....                          | 17 |
| 4.2.4 | Trunk Groups .....                             | 18 |
| 4.2.5 | Route Pattern .....                            | 22 |
| 4.2.6 | Outbound Call Routing .....                    | 23 |
| 4.2.7 | Outbound Caller ID .....                       | 24 |
| 4.2.8 | Inbound Call Routing .....                     | 25 |
| 4.3   | Avaya Aura Session Manager Configuration ..... | 26 |
| 4.3.1 | Avaya Aura SM login.....                       | 26 |
| 4.3.2 | Domain .....                                   | 27 |
| 4.3.3 | Locations.....                                 | 28 |
| 4.3.4 | Adaptations .....                              | 30 |
| 4.3.5 | SIP Entities and Entity Links .....            | 31 |
| 4.3.6 | Routing Policies .....                         | 37 |

|        |                                |    |
|--------|--------------------------------|----|
| 4.3.7  | Dial Patterns.....             | 40 |
| 4.4    | Avaya SBCE Configuration ..... | 42 |
| 4.4.1  | Avaya SBCE login .....         | 42 |
| 4.4.2  | Server Interworking.....       | 43 |
| 4.4.3  | SIP Servers .....              | 45 |
| 4.4.4  | Topology Hiding .....          | 50 |
| 4.4.5  | Routing .....                  | 52 |
| 4.4.6  | Signaling Rules.....           | 54 |
| 4.4.7  | Media Interface .....          | 60 |
| 4.4.8  | Signaling Interface .....      | 61 |
| 4.4.9  | TLS Configuration.....         | 65 |
| 4.4.10 | SIP Authentication.....        | 78 |

## 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.....               | 18 |
| Figure 8  | Trunk Group Continuation ..... | 19 |
| 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 | Inbound call routing.....      | 25 |
| Figure 15 | Avaya Aura SM login .....      | 26 |
| Figure 16 | Routing .....                  | 27 |
| Figure 17 | Add Domain.....                | 27 |
| Figure 18 | Domain .....                   | 28 |
| Figure 19 | Locations .....                | 28 |
| Figure 20 | Locations continuation.....    | 29 |
| Figure 21 | Locations continuation.....    | 29 |

|   |    |
|---|----|
| Figure 22 Digit Conversion to Avaya CM .....                          | 30 |
| Figure 23 Digit Conversion to Amazon .....                            | 30 |
| Figure 24 Adaptation for Amazon.....                                  | 31 |
| Figure 25 SIP Entity for Avaya SM .....                               | 33 |
| Figure 26 SIP Entity and Entity Links for Avaya CM.....               | 34 |
| Figure 27 SIP Entity and Entity Links for Avaya CM continuation ..... | 34 |
| Figure 28 SIP Entity and Entity Link for Avaya CM continuation.....   | 35 |
| Figure 29 SIP Entity and Entity Link for Avaya SBCE .....             | 35 |
| Figure 30 SIP Entity and Entity Link for Avaya SBCE continuation..... | 36 |
| Figure 31 SIP Entity and Entity Link for Avaya SBCE continuation..... | 36 |
| Figure 32 Routing Policy for Avaya CM .....                           | 37 |
| Figure 33 Routing Policy for Avaya CM continuation.....               | 37 |
| Figure 34 Routing Policy for Avaya CM continuation.....               | 38 |
| Figure 35 Routing Policy for Avaya SBCE .....                         | 38 |
| Figure 36 Routing Policy for Avaya SBCE continuation.....             | 39 |
| Figure 37 Routing Policy for Avaya SBCE continuation.....             | 39 |
| Figure 38 Dial Pattern to Avaya CM.....                               | 40 |
| Figure 39 Dial Pattern to Amazon via Avaya SBCE.....                  | 41 |
| Figure 40 Avaya SBCE Login.....                                       | 42 |
| Figure 41 Selection of Avaya SBCE Device .....                        | 43 |
| Figure 42 Server Interworking profile for Avaya SM.....               | 43 |
| Figure 43 Server Interworking profile for Avaya SM continuation ..... | 44 |
| Figure 44 Server Interworking profile for Amazon.....                 | 45 |
| Figure 45 SIP Server for Avaya SM .....                               | 45 |
| Figure 46 SIP Server for Avaya SM Continuation .....                  | 46 |
| Figure 47 SIP Server for Avaya SM Continuation .....                  | 47 |
| Figure 48 SIP Server for Amazon.....                                  | 48 |
| Figure 49 SIP Server for Amazon continuation.....                     | 48 |
| Figure 50 SIP Server for Amazon continuation.....                     | 49 |
| Figure 51 Topology Hiding Profile for Avaya SM.....                   | 50 |
| Figure 52 Topology Hiding Profile for Avaya SM continuation .....     | 50 |
| Figure 53 Topology Hiding Profile for Amazon.....                     | 51 |
| Figure 54 Routing for Avaya SM.....                                   | 52 |
| Figure 55 Routing for Avaya SM continuation .....                     | 53 |
| Figure 56 Routing for Avaya SM continuation .....                     | 53 |
| Figure 57 Routing for Amazon .....                                    | 54 |
| Figure 58 Signaling Rules for Avaya SM.....                           | 54 |
| Figure 59 Signaling Rules for Avaya SM continuation.....              | 55 |
| Figure 60 Signaling Rules for Avaya SM continuation.....              | 56 |
| Figure 61 Signaling Rules for Avaya SM continuation.....              | 56 |

|   |    |
|---|----|
| Figure 62 End Point Policy Group for Avaya SM .....               | 57 |
| Figure 63 End Point Policy Group for Avaya SM Continuation .....  | 58 |
| Figure 64 End Point Policy Group for Amazon .....                 | 59 |
| Figure 65 Media Interface facing Avaya SM .....                   | 60 |
| Figure 66 Media Interface facing Amazon .....                     | 60 |
| Figure 67 Signaling Interface facing Avaya SM .....               | 61 |
| Figure 68 Signaling Interface facing Amazon .....                 | 62 |
| Figure 69 Server Flow for Avaya SM .....                          | 63 |
| Figure 70 Server Flow for Amazon .....                            | 64 |
| Figure 71 Upload Amazon Root CA .....                             | 65 |
| Figure 72 Client Profile facing Amazon .....                      | 66 |
| Figure 73 Client Profile facing Amazon Continuation .....         | 67 |
| Figure 74 Server Profile facing Amazon .....                      | 68 |
| Figure 75 Server Profile facing Amazon Continuation .....         | 69 |
| Figure 76 SIP Server Profile – Amazon.....                        | 70 |
| Figure 77 Media Rule – Amazon.....                                | 71 |
| Figure 78 Media Rule – Amazon Continuation.....                   | 72 |
| Figure 79 Edit End Point policy Group – Amazon .....              | 73 |
| Figure 80 Edit End Point policy Group – Amazon Continuation ..... | 74 |
| Figure 81 Edit Signaling Interface – Amazon .....                 | 74 |
| Figure 82 Edit Signaling Interface – Amazon continuation.....     | 75 |
| Figure 83 Edit Server Flow – Amazon .....                         | 76 |
| Figure 84 Edit Server Flow – Amazon continuation .....            | 77 |
| Figure 85 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.

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 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

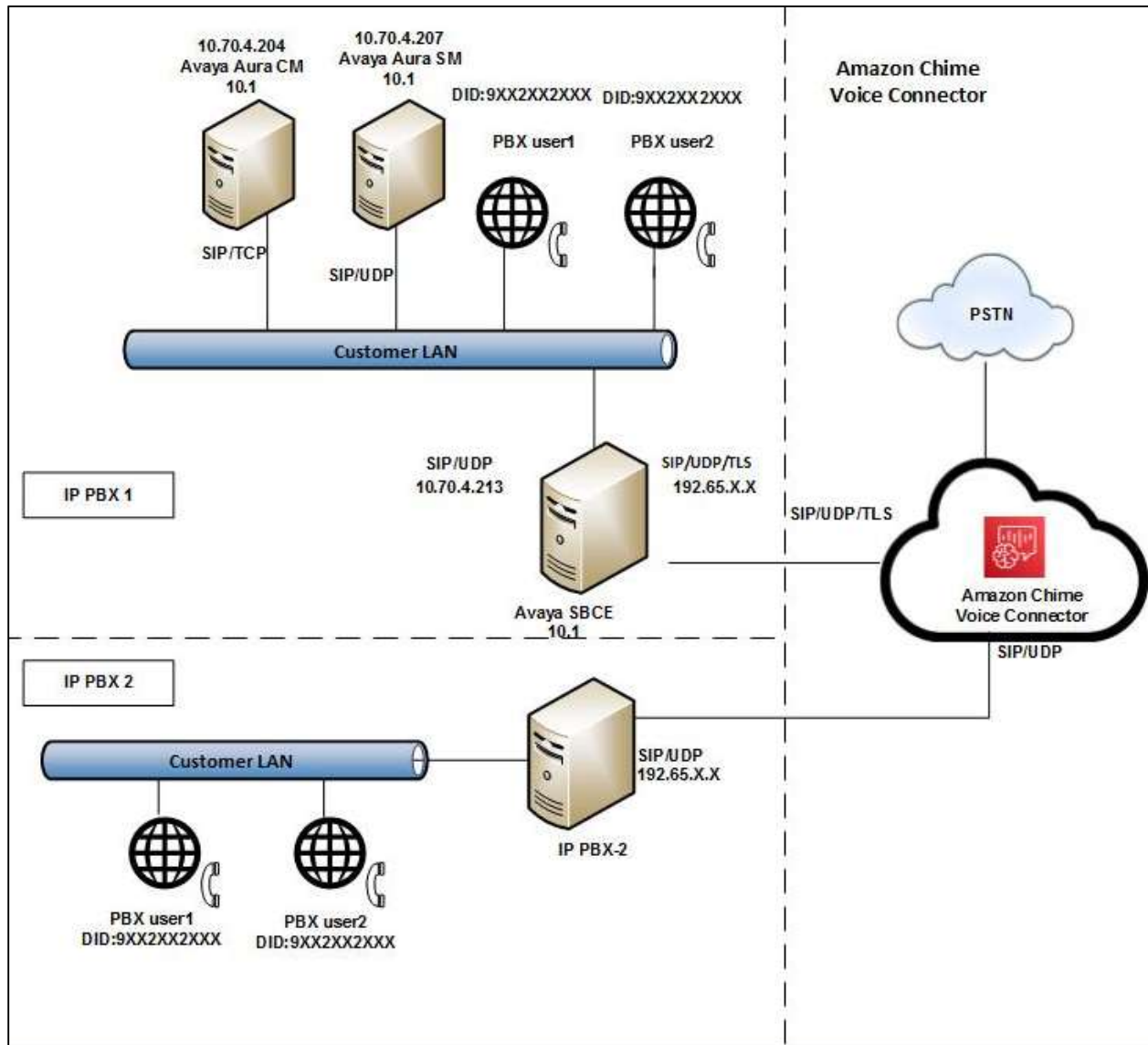


Figure 1 Network Topology

## 2.1 Hardware Components

- UCS-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)– 9630G

## 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

- 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

- 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

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 Voice Connector**.

| Steps  | Description                 | Reference                   |
|--------|-----------------------------|-----------------------------|
| Step 1 | Avaya Aura CM Configuration | <a href="#">Section 4.3</a> |
| Step 2 | Avaya Aura SM Configuration | <a href="#">Section 4.4</a> |
| Step 3 | Avaya SBCE Configuration    | <a href="#">Section 4.5</a> |

*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.

```
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-srtp
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 4.3.1
- *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.tekvizion.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
UDP Port Min: 2048    IP Audio Hairpinning? n
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                                           Group Type: sip
IMS Enabled? n                                           Transport Method: tcp
Q-SIP? n
IP Video? n
Peer Detection Enabled? y Peer Server: SM                Enforce SIPS URI for SRTP? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y Clustering? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                               Far-end Node Name: AASM10
Near-end Listen Port: 5060                             Far-end Listen Port: 5060
Far-end Network Region: 2
Far-end Domain: lab.tekvizion.com
Incoming Dialog Loopbacks: eliminate                    Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                               Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
Enable Layer 3 Test? y
Alternate Route Timer(sec): 6
"2" Must demand maintenance busy the signaling group first
```

Figure 6 Signaling Group

## 4.2.4 Trunk Groups

- Trunk group **5** is used for trunk to Avaya SM. Command **add trunk group 1** was used to create Trunk Group. Use **change trunk group 1** to modify existing trunk group.
- Set *Group Type*: **sip**
- Set *Group Name*: **AmazonAvaya**
- Set *TAC*: **#001**
- Set *Direction*: **two-way**
- Set *Service Type*: **public-ntwrk**
- Set *Member Assignment Method*: **auto**
- Set *Signaling Group*: **1** (created in section 4.3.3)
- 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: AmazonAvaya                                COR: 1              TN: 1              TAC: #001
Direction: two-way                                     Outgoing Display? n
Dial Access? n                                         Night Service: _____
Queue Length: 0
Service Type: public-ntwrk                             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? m                                     Measured: none
                                                         Maintenance Tests? y

  Suppress # Outpulsing? n Numbering Format: public
                                                         UII 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? n
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*: **AvAASM10**
- Set *Grp No*: **1** (created in Section 4.3.4)
- 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: Co AASM10
SCCAN? n   Secure SIP? n   Used for SIP stations? n

  Grp FRL
  No  No
1: 1  0
2:
3:
4:
5:
6:

  BCC VALUE   TSC CA-TSC   ITC BCIE Service/Feature PARM Sub   Numbering LAR
  0 1 2 M 4 W   Request Request
1: y y y y y n n   rest
2: y y y y y n n   rest
3: y y y y y n n   rest
4: y y y y y n n   rest
5: y y y y y n n   rest
6: y y y y y n n   rest

  DCS/ IXC
  QSIG Intw
  n user
  n user
  n user
  n user
  n user
  n user
  unk-unk none
  none
  none
  none
  none
  none
```

Figure 11 Route Pattern

## 4.2.6 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*: **1** (created in section 4.3.5)
- 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        |
| 21424259      | 10        | 12        | 1             | natl      | ---      | n        |
| 214242!       | 10        | 12        | 1             | natl      | ---      | n        |
| 325           | 3         | 12        | 1             | natl      | ---      | n        |
| 729           | 3         | 16        | 1             | intl      | ---      | n        |
| 18            | 3         | 12        | 1             | natl      | ---      | n        |
| 866           | 3         | 10        | 1             | natl      | ---      | n        |
| 91            | 10        | 12        | 1             | natl      | ---      | n        |
| 9725980       | 7         | 12        | 1             | natl      | ---      | n        |
| 19            | 3         | 12        | 1             | natl      | ---      | n        |
|               |           |           |               |           |          | n        |
|               |           |           |               |           |          | n        |
|               |           |           |               |           |          | n        |
|               |           |           |               |           |          | n        |
|               |           |           |               |           |          | n        |
|               |           |           |               |           |          | n        |

Figure 12 Outbound Call Routing

## 4.2.7 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*: **4**
- Set *EXT Code*: **2923**
- Set *Trk Grp*: **1** (created in section 4.3.4)
- Set *CPN Prefix*: **91XXXXXXXX**. (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        10      10
4  2005      1        10      10
4  2923      1        919xxxxxxx 10
4  5992      1        10      10
-----
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.
```

Figure 13 Outbound Caller ID

#### 4.2.8 Inbound Call Routing

- For Inbound call to Avaya PBX from PSTN through Amazon Chime Voice Connector SIP trunking, inc-call-handling-trmt-trunk-group is used. Use command **change inc-call-handling-trmt trunk-group x** to configure the routing table.
- Set *Number Len*: 10
- Set *Number Digits*:919XXXXXXXX
- Set *Del*: 10

```
change inc-call-handling-trmt trunk-group 1 Page 1 of 3
```

| INCOMING CALL HANDLING TREATMENT |               |                  |     |        |
|----------------------------------|---------------|------------------|-----|--------|
| Service/<br>Feature              | Number<br>Len | Number<br>Digits | Del | Insert |
| public-ntwrk                     | 10            | 04326            | 10  | 2632   |
| public-ntwrk                     | 10            | 04326            | 10  | 2003   |
| public-ntwrk                     | 10            | 04326            | 10  | 2005   |
| public-ntwrk                     | 10            | 91927            | 10  | 5992   |
| public-ntwrk                     | 10            | 919xxxxxxxx      | 10  | 2923   |
| public-ntwrk                     | 7             | 2952923          | 7   | 2923   |
| public-ntwrk                     | 4             | 2631             | 4   | 2631   |
| public-ntwrk                     | 4             | 2632             | 4   | 2632   |
| public-ntwrk                     | 4             | 2923             | 4   | 2923   |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |
| public-ntwrk                     | —             | —                | —   | —      |

Figure 14 Inbound call routing

## 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**

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

Figure 15 Avaya Aura SM login

## 4.3.2 Domain

- Navigate to **Elements > Routing**

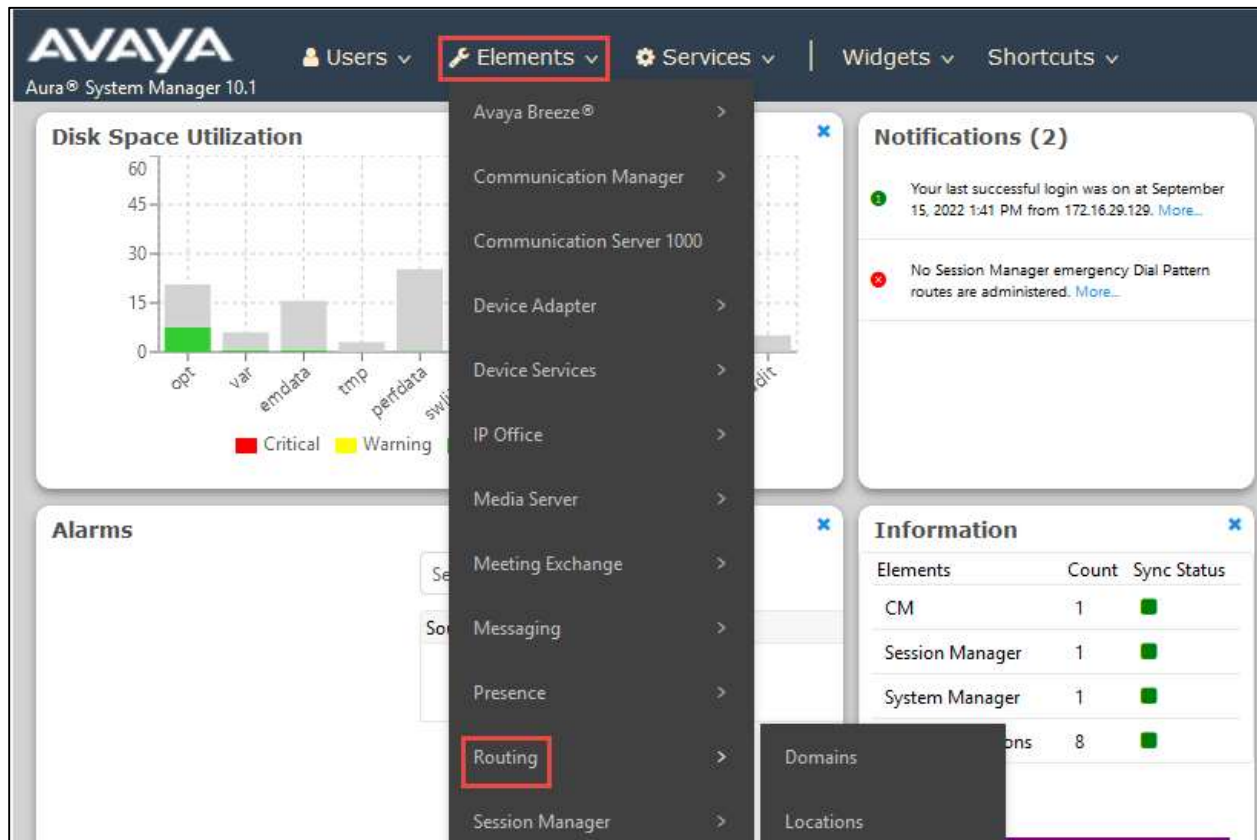


Figure 16 Routing

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

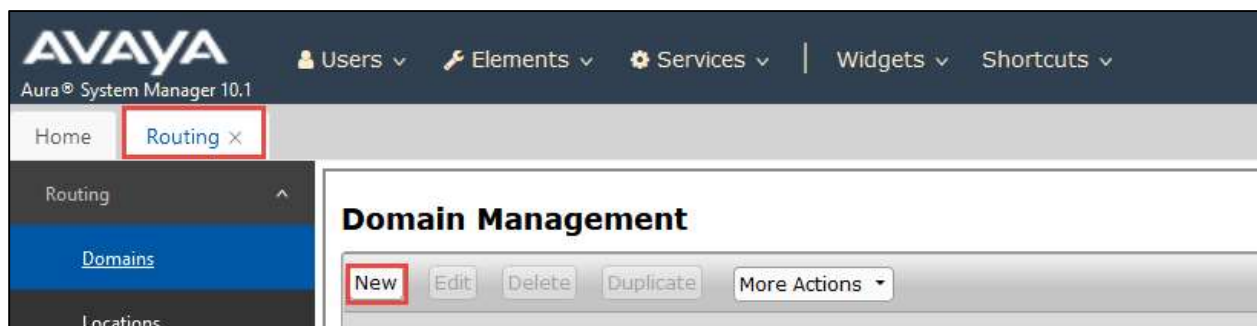


Figure 17 Add Domain

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

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

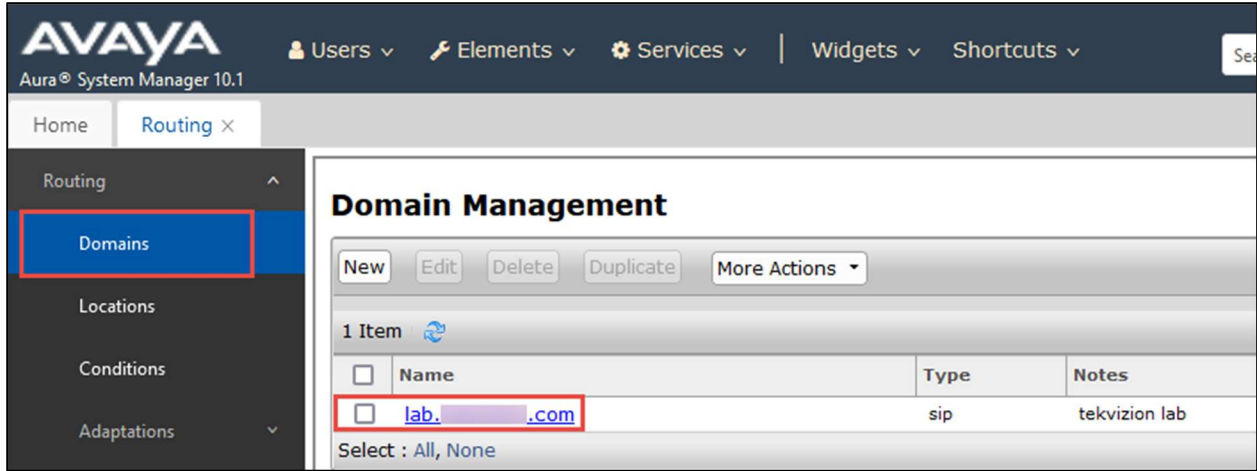


Figure 18 Domain

### 4.3.3 Locations

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

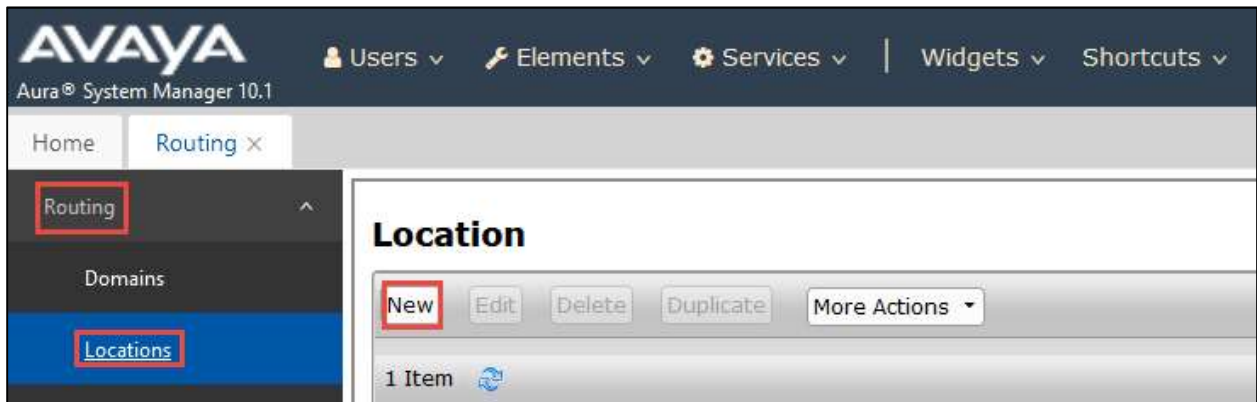


Figure 19 Locations

- Set Name: **Plano**

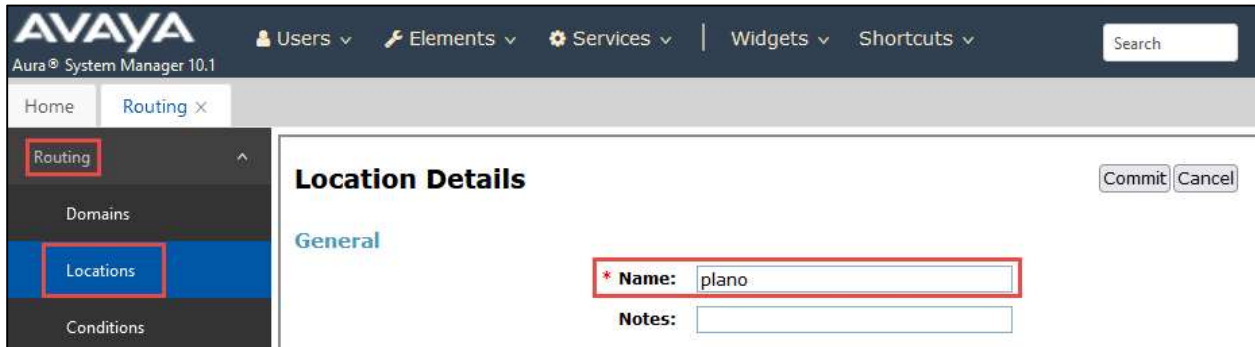


Figure 20 Locations continuation

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

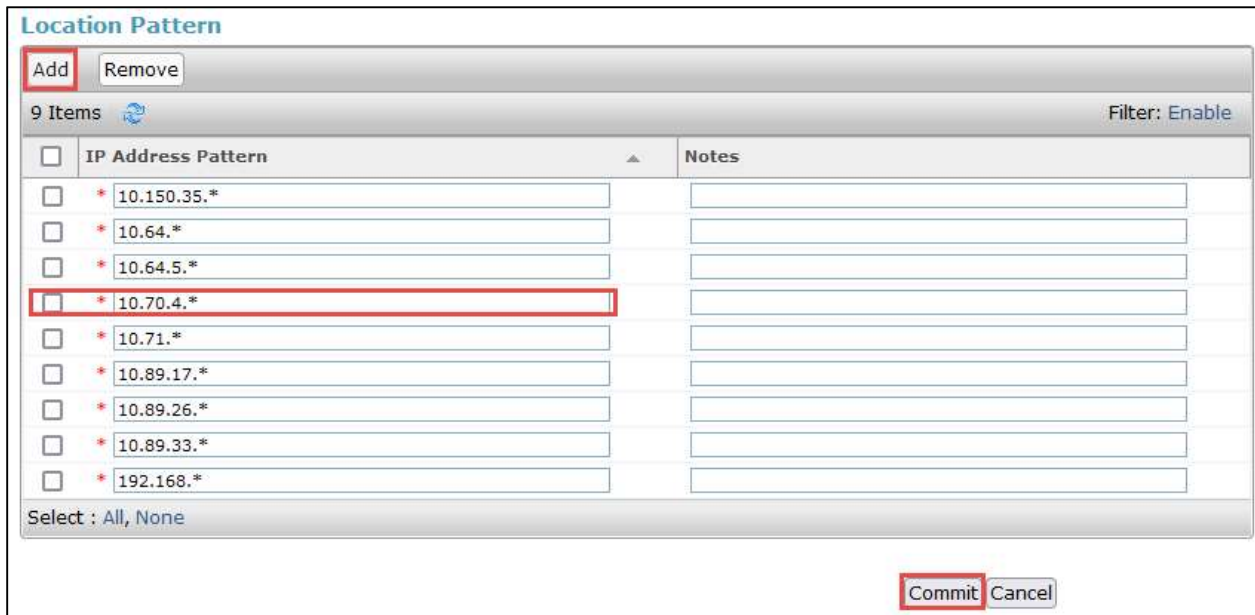


Figure 21 Locations continuation

#### 4.3.4 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*: **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   | Address to Modify  |
|------------------|--------------|---|--|
| <b>+191929</b>   | <b>11/36</b> | <b>5</b> – Deletes <b>+1919</b> from +191929 patterns | Destination – Modifies digits in <b>TO</b> 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  |
|------------------|--------------|--|--|--|
| <b>214242</b>    | <b>10/36</b> | <b>0</b>   | <b>+1</b> – Insert <b>+1</b> in front of 214242 patterns | Destination – Modifies the digits in <b>TO</b> header and sends it to Amazon |
| <b>+91929</b>    | <b>11/36</b> | <b>1</b> – Deletes <b>+</b> from +91929 patterns | <b>+1</b> – Inserts <b>+1</b> in front of 91929 patterns | Origination – Modifies digits in <b>FROM</b> 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

Commit
Cancel
Help ?

### Adaptation Details

**General**

\* **Adaptation Name:** Adapter for SBC

**Notes:** DigitConversionAdapter

\* **Module Name:** DigitConversionAdapter

**Type:** digit

**State:** enabled

**Module Parameter Type:** Name-Value Parameter

|                          | 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 |
|--------------------------|------------------|------|------|---------------|---------------|---------------|-------------------|------------|
| <input type="checkbox"/> | * +19192         | * 12 | * 36 |               | * 5           |               | destination       |            |

Select : All, None

#### Digit Conversion for Outgoing Calls from SM

Add Remove
Filter: Enable

7 Items

| <input type="checkbox"/> | Matching Pattern | Min  | Max  | Phone Context | Delete Digits | Insert Digits | Address to modify | Adaptation Da |
|--------------------------|------------------|------|------|---------------|---------------|---------------|-------------------|---------------|
| <input type="checkbox"/> | * +91929         | * 11 | * 36 |               | * 1           | +1            | origination       |               |
| <input type="checkbox"/> | * 18             | * 11 | * 36 |               | * 0           | +             | destination       |               |
| <input type="checkbox"/> | * 214242         | * 10 | * 36 |               | * 0           | +1            | destination       |               |
| <input type="checkbox"/> | * 325            | * 10 | * 36 |               | * 0           | +1            | destination       |               |
| <input type="checkbox"/> | * 729            | * 10 | * 36 |               | * 0           | +91           | destination       |               |
| <input type="checkbox"/> | * 91             | * 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)
- Under *Listen Port*:
- 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 x

**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 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 Filter: Enable

| <input type="checkbox"/> | Response Code & Reason Phrase | Mark Entity Up/Down | Notes |
|--------------------------|-------------------------------|---------------------|-------|
| 0 Items                  |                               |                     |       |

[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**

**AVAYA** Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search

Home Routing ×

Routing

- Domains
- Locations
- Conditions
- Adaptations ▾
- SIP Entities**
- Entity Links

**SIP Entity Details** Commit Cancel

**General**

\* Name: AACM10

\* FQDN or IP Address: 10.70.4.204

Type: CM ▾

Notes:

Adaptation: ▾

Location: plano ▾

Time Zone: America/Chicago ▾

Figure 26 SIP Entity and Entity Links for Avaya CM

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

**AVAYA** Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search admin

Home Routing ×

Routing

- Domains
- Locations
- Conditions
- Adaptations ▾
- SIP Entities
- Entity Links**

**Entity Links** Help ?

New Edit Delete Duplicate More Actions ▾

2 Items Filter: Enable

| <input type="checkbox"/> | Name                                | SIP Entity 1 | Protocol | Port | SIP Entity 2      | Port | DNS Override                        | Connection Policy | Deny New Service         | Notes |
|--------------------------|-------------------------------------|--------------|----------|------|-------------------|------|-------------------------------------|-------------------|--------------------------|-------|
| <input type="checkbox"/> | <a href="#">SM10_CM_SIP Trunk</a>   | AASM10       | TCP      | 5060 | AACM10            | 5060 | <input checked="" type="checkbox"/> | trusted           | <input type="checkbox"/> |       |
| <input type="checkbox"/> | <a href="#">ToAmazonVCAvaya SBC</a> | AASM10       | UDP      | 5060 | AmazonVC_AvayaSBC | 5060 | <input checked="" type="checkbox"/> | trusted           | <input type="checkbox"/> |       |

Select : All, None

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**

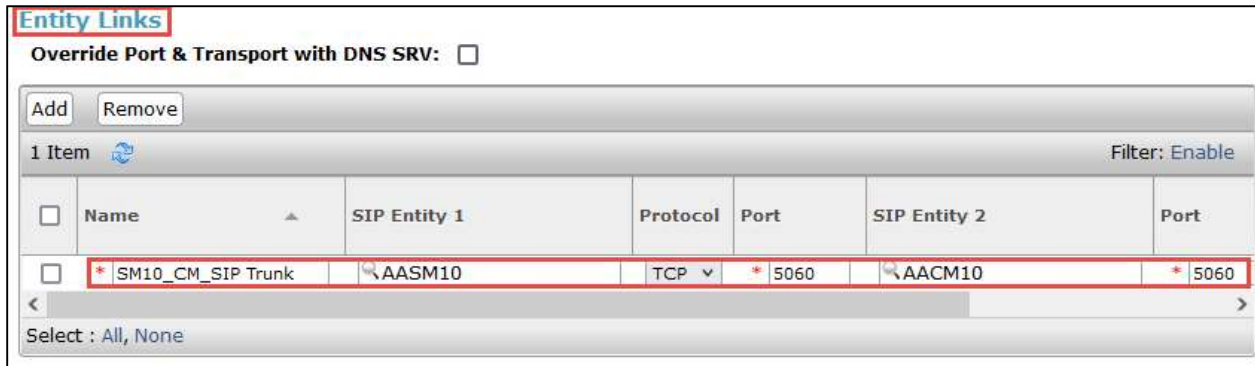


Figure 28 SIP Entity and Entity Link for Avaya CM continuation

## 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 4.4.4
- Set Location: Select the **location** created in Section 4.4.3
- Click **Commit**

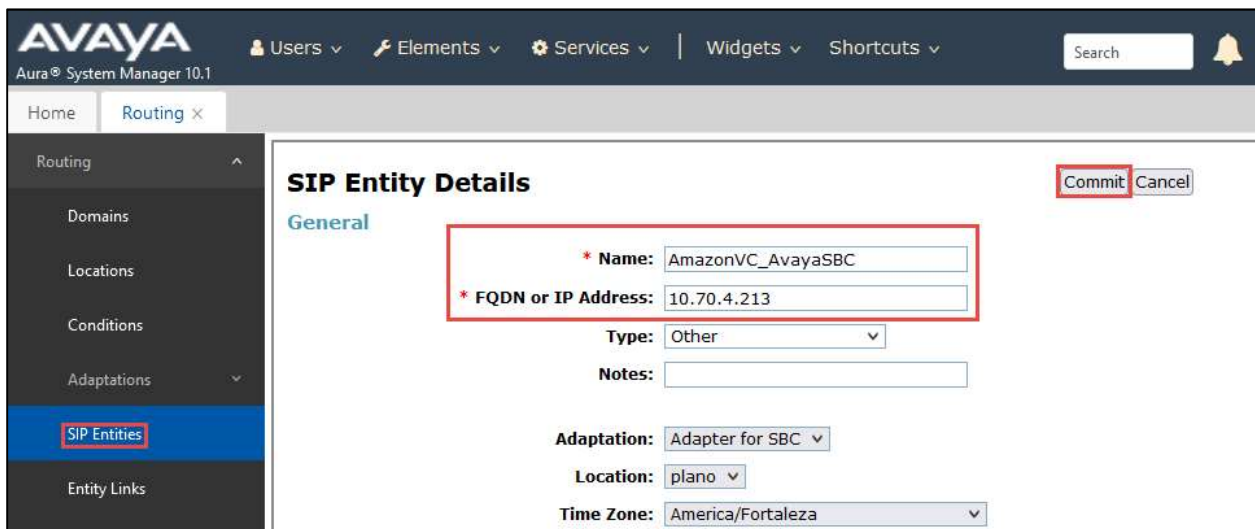


Figure 29 SIP Entity and Entity Link for Avaya SBCE

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

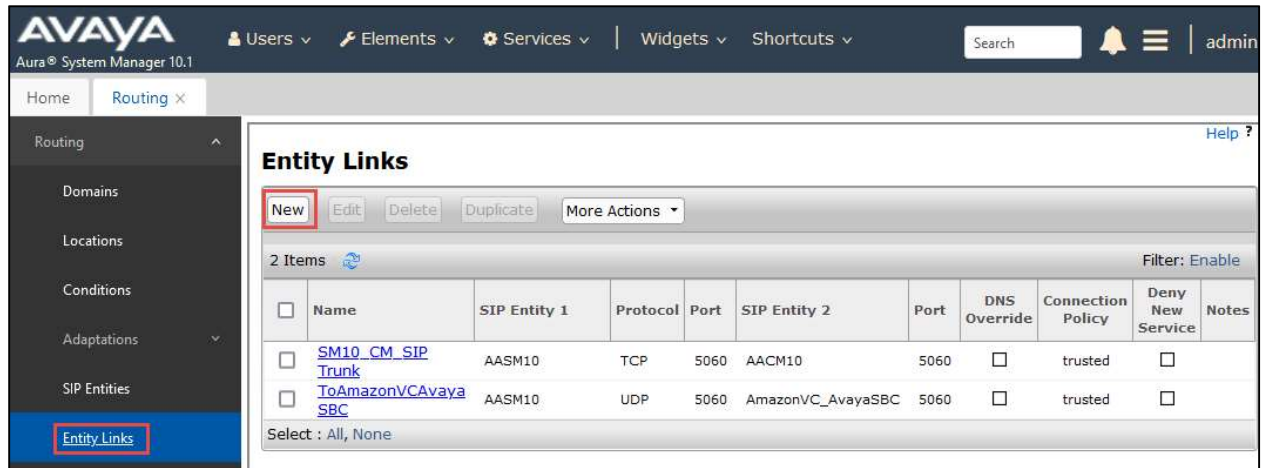


Figure 30 SIP Entity and Entity Link for Avaya SBCE continuation

- 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**

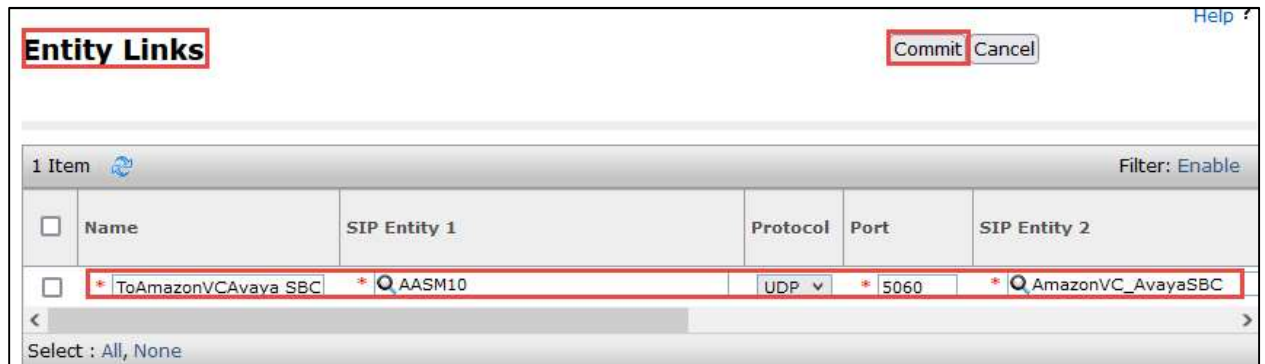


Figure 31 SIP Entity and Entity Link for Avaya SBCE continuation

## 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: SM to CM

Disabled:

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Figure 32 Routing Policy for Avaya CM

- Check the radio button beside **AACM10** as destination SIP Entity (configured in Section 4.4.5)
- 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"/> | <a href="#">AACM10</a>            | 10.70.4.204        | CM              |       |
| <input type="checkbox"/> | <a href="#">AASM10</a>            | 10.70.4.207        | Session Manager |       |
| <input type="checkbox"/> | <a href="#">AmazonVC_AvayaSBC</a> | 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 contains 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 contains 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 4.4.5)
- Click **Select** and return back to **Routing Policy Details** page

[Help ?](#)

### SIP Entities

New Edit Delete Duplicate More Actions ▾

3 Items [Refresh](#) Filter: Enable

| <input type="checkbox"/> | Name                              | FQDN or IP Address | Type            | Notes |
|--------------------------|-----------------------------------|--------------------|-----------------|-------|
| <input type="checkbox"/> | <a href="#">AACM10</a>            | 10.70.4.204        | CM              |       |
| <input type="checkbox"/> | <a href="#">AASM10</a>            | 10.70.4.207        | Session Manager |       |
| <input type="checkbox"/> | <a href="#">AmazonVC_AvayaSBC</a> | 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**

[Help ?](#)

### Routing Policy Details

Commit Cancel

**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*: **919**
- 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 **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 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 divided into two sections: 'General' and 'Originating Locations and Routing Policies'. In the 'General' section, the 'Pattern' field is set to '214242', 'Min' is '10', and 'Max' is '12'. The 'Emergency Call' checkbox is unchecked, and the 'SIP Domain' is set to '-ALL-'. The 'Notes' field is empty. In the 'Originating Locations and Routing Policies' section, there is an 'Add' button and a table with one item. The table has the following columns: 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The table contains one row with the following data: 'plano', empty, 'AmazonVCAvayaSBC', '0', unchecked, 'AmazonVC\_AvayaSBC'. Below the table, there is a 'Select' dropdown menu set to 'All, None'. At the top right of the page, there are 'Commit' and 'Cancel' buttons.

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

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**

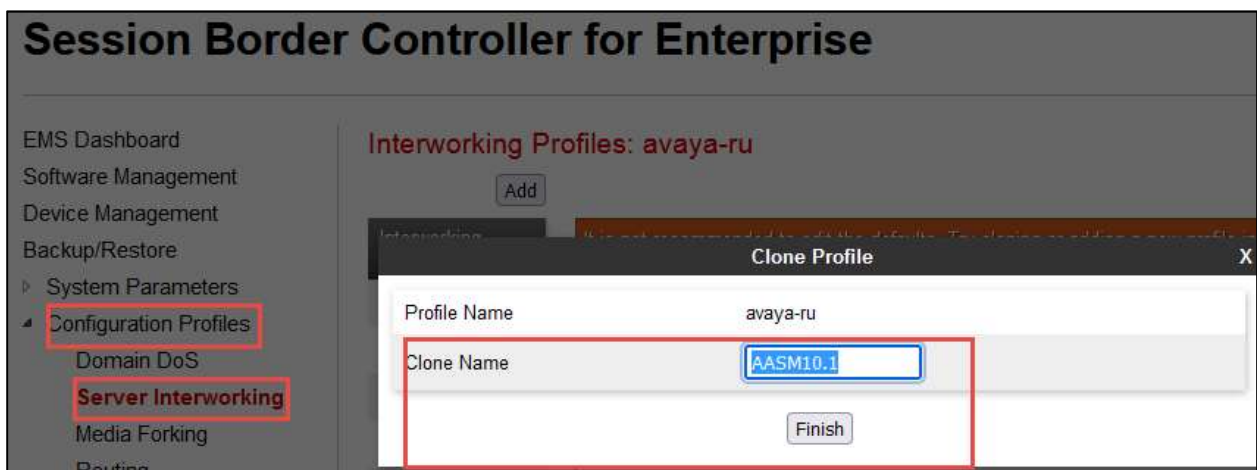


Figure 42 Server Interworking profile for Avaya SM

**Interworking Profiles: AASM.10.1**

Interworking Profiles

- cs2100
- avaya-ru
- AmazonVC
- AASM.10.1

Click here to add a description.

| 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      |
| Mediasec                 | No      |

Figure 43 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

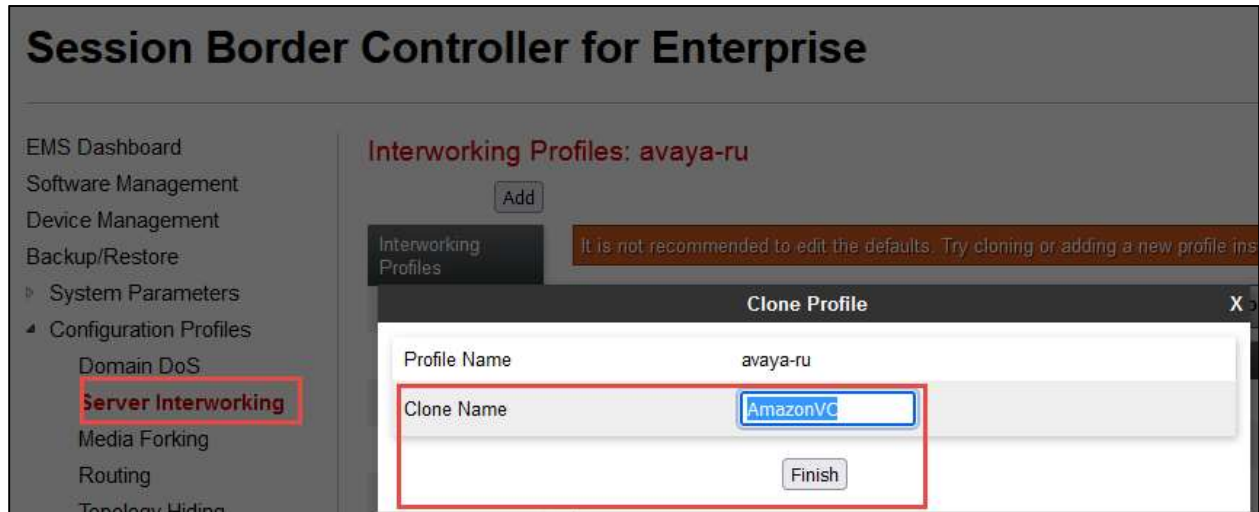


Figure 44 Server Interworking profile for Amazon

### 4.4.3 SIP Servers

#### SIP Server for Avaya SM

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

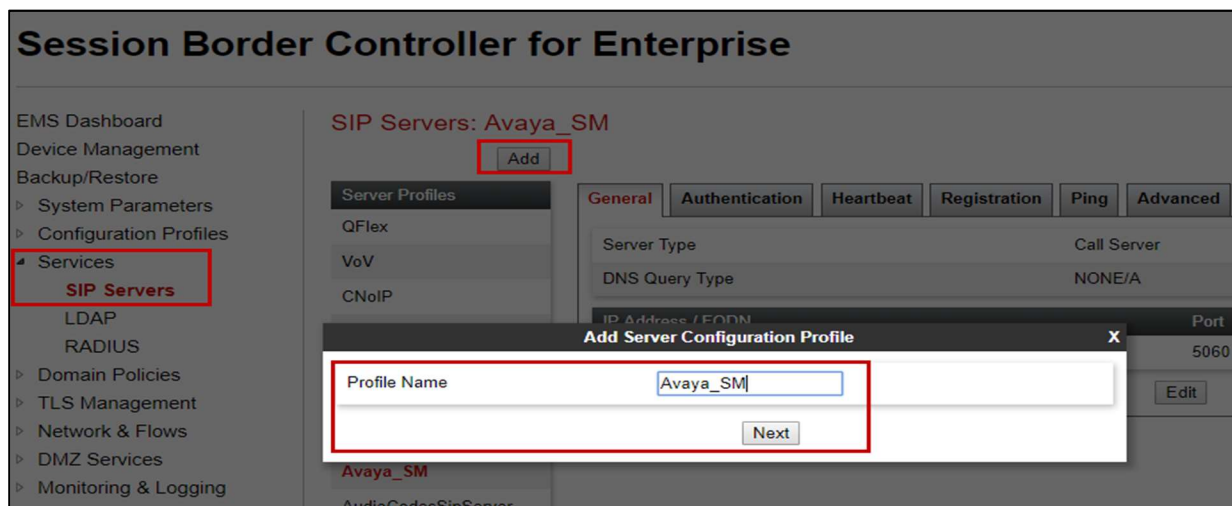


Figure 45 SIP Server for Avaya SM

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**

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type: Call Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

| IP Address / FQDN | Port | Transport |        |
|-------------------|------|-----------|--------|
| 10.70.4.207       | 5060 | UDP       | Delete |

Finish

Figure 46 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**

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

- Enable DoS Protection:
- Enable Grooming:
- Interworking Profile: AASM.10.1 (highlighted with a red box)
- Signaling Manipulation Script: None
- Securable:
- Enable FGDN:
- TCP Failover Port: [Empty text box]
- TLS Failover Port: [Empty text box]
- Tolerant:
- URI Group: None
- NG911 Support:

At the bottom center of the window, there is a button labeled "Finish" which is also highlighted with a red box.

Figure 47 SIP Server for Avaya SM Continuation

## SIP Server for Amazon Chime Voice Connector

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



Figure 48 SIP Server for Amazon

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

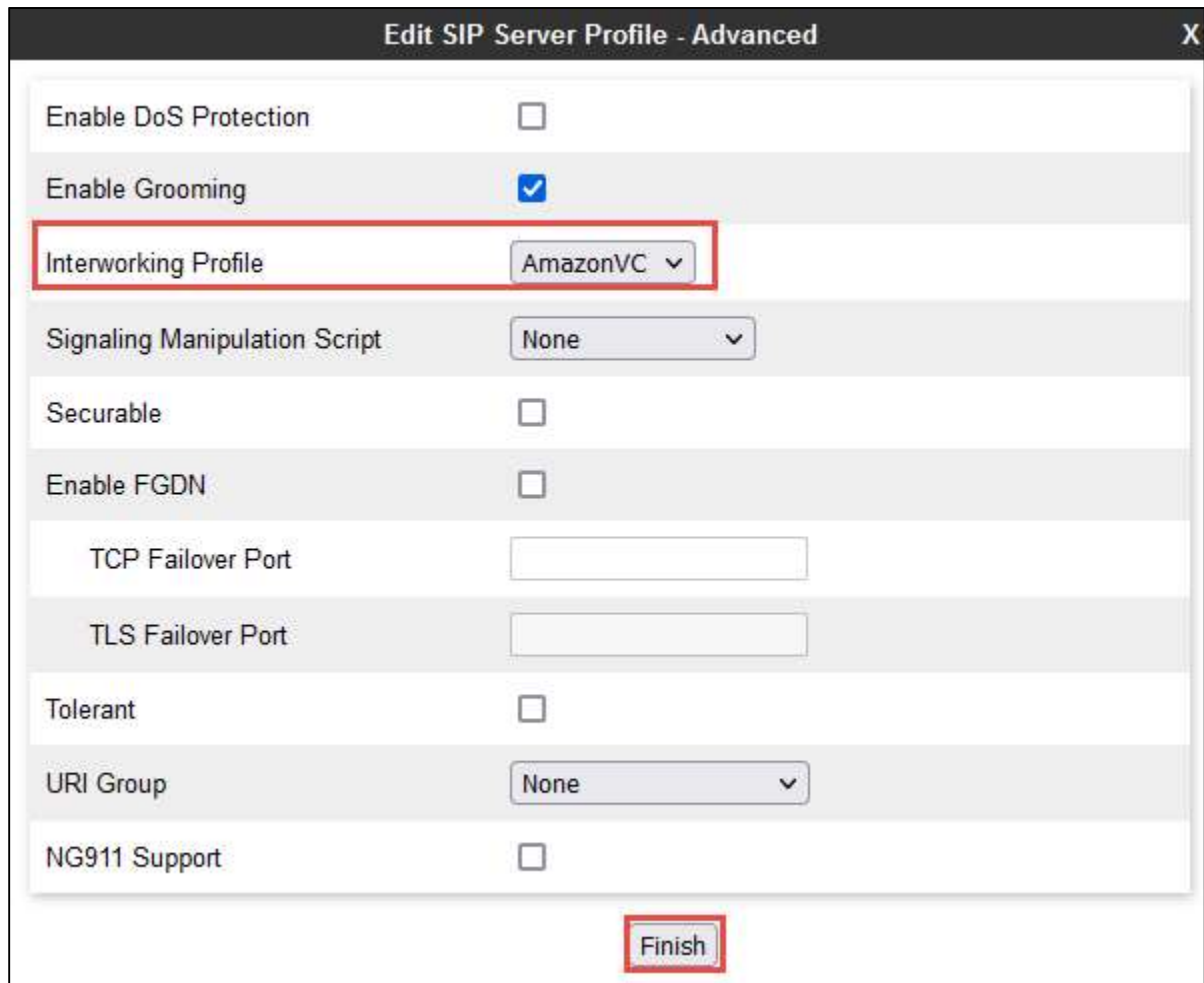
- Set *IP Address/FQDN*: Enter the **Amazon Chime voice Connector Outbound Host Name**
- Set *Port*: **5060**
- Set *Transport*: **UDP**
- Click **Finish**



Figure 49 SIP Server for Amazon continuation

Navigate to **Advanced** tab

- Set *Interworking Profile*: Select **To\_AmazonVC** (created in section 4.5.2)
- Click **Finish**



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

- Enable DoS Protection:
- Enable Grooming:
- Interworking Profile: AmazonVC (highlighted with a red box)
- Signaling Manipulation Script: None
- Securable:
- Enable FGDN:
- TCP Failover Port: [Empty text box]
- TLS Failover Port: [Empty text box]
- Tolerant:
- URI Group: None
- NG911 Support:

The "Finish" button at the bottom center is highlighted with a red box.

Figure 50 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**

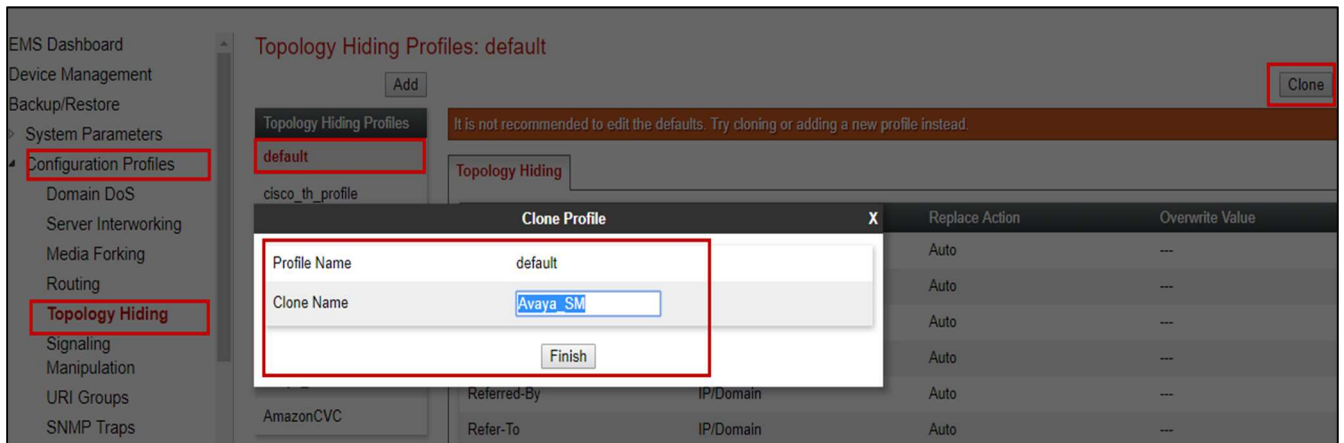


Figure 51 Topology Hiding Profile for Avaya SM

- 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**
- Click **Finish**

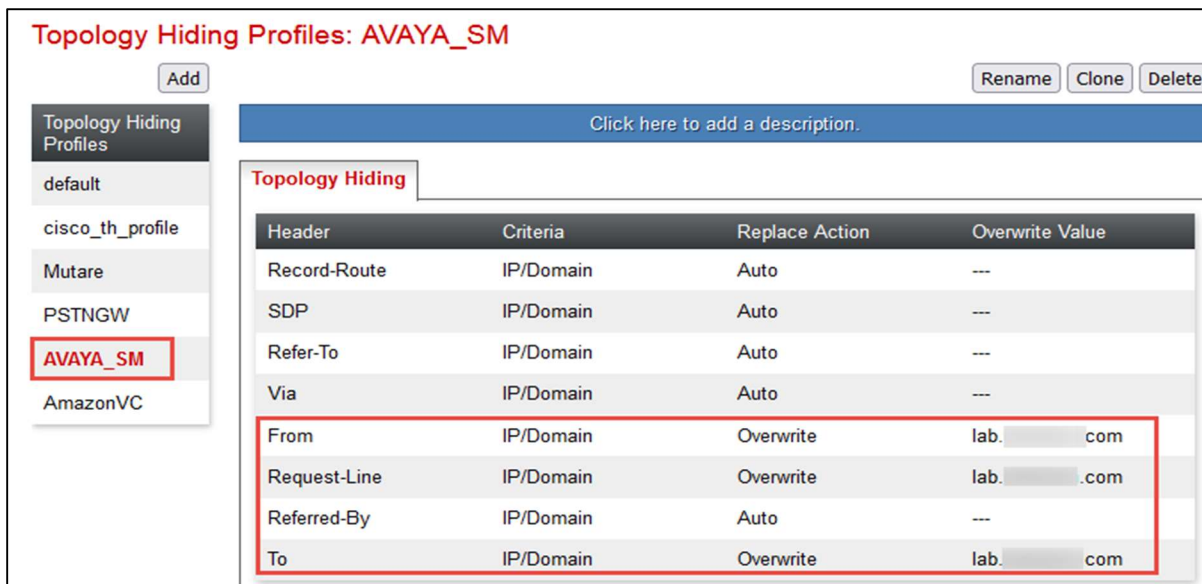


Figure 52 Topology Hiding Profile for Avaya SM continuation

## Topology hiding profile for Amazon Chime Voice Connector

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

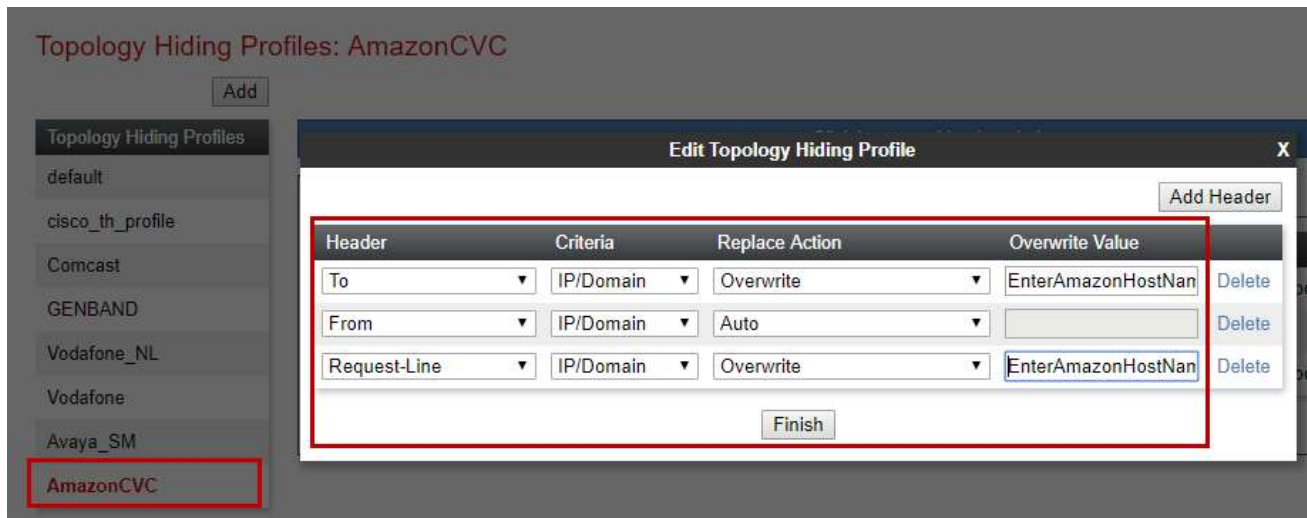


Figure 53 Topology Hiding Profile for Amazon

## 4.4.5 Routing

### Routing for Avaya SM

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

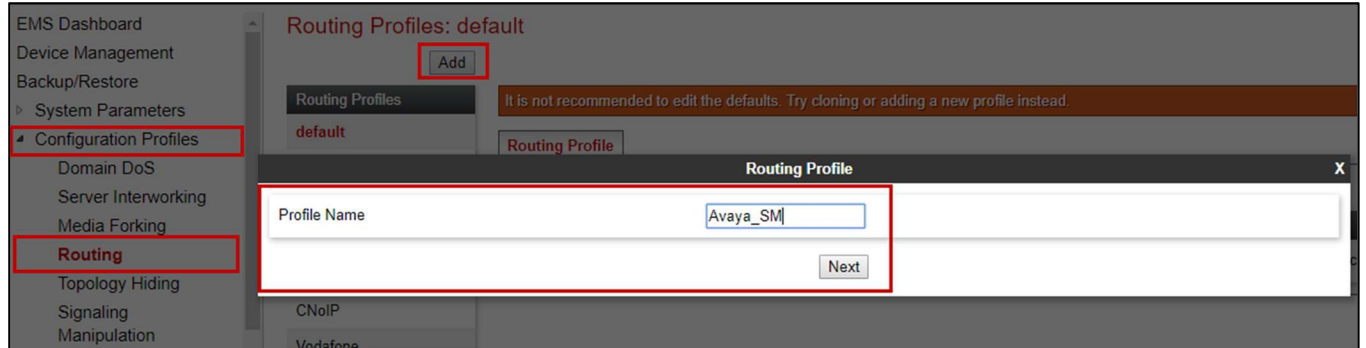


Figure 54 Routing for Avaya SM

- 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**

Profile : AVAYA\_SM - Edit Rule

|                            |                          |                       |                          |
|----------------------------|--------------------------|-----------------------|--------------------------|
| 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 type="checkbox"/> | Next Hop In-Dialog    | <input type="checkbox"/> |
| Ignore Route Header        | <input type="checkbox"/> |                       |                          |
| ENUM                       | <input type="checkbox"/> | ENUM Suffix           |                          |

**Add**

| Priority / Weight | LDAP Search Attribute | LDAP Search Regex Pattern | LDAP Search Regex Result | SIP Server Profile | Next Hop Address       | Transport |        |
|-------------------|-----------------------|---------------------------|--------------------------|--------------------|------------------------|-----------|--------|
| 1                 |                       |                           |                          | Avaya_SM           | 10.70.4.207:5060 (UDF) | None      | Delete |

**Finish**

Figure 55 Routing for Avaya SM continuation

**Routing Profiles: AVAYA\_SM**

**Add**    **Rename**    **Clone**    **Delete**

Click here to add a description.

**Routing Profile**    **Update Priority**    **Add**

| Priority | URI Group | Time of Day | Load Balancing | Next Hop Address | Transport |             |
|----------|-----------|-------------|----------------|------------------|-----------|-------------|
| 1        | *         | default     | Priority       | 10.70.4.207:5060 | UDP       | Edit Delete |

Routing Profiles: default, PSTN\_ROUTE, Mutare Inbound, Mutare Outbound, **AVAYA\_SM**, AmazonVC

Figure 56 Routing for Avaya SM continuation

## Routing for Amazon

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

| Priority / Weight | LDAP Search Attribute | LDAP Search Regex Pattern | LDAP Search Regex Result | SIP Server Profile | Next Hop Address    | Transport |        |
|-------------------|-----------------------|---------------------------|--------------------------|--------------------|---------------------|-----------|--------|
|                   |                       |                           |                          | AmazonVC           | hydpgl6qdjye6dcwdnh | None      | Delete |

Figure 57 Routing for Amazon

## 4.4.6 Signaling Rules

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

Signaling Rules: default

Clone

Signaling Rules

default

General Requests Responses Request Headers Response Headers Signaling QoS UCID

Clone Rule

Rule Name default

Clone Name Avaya\_SM

Finish

Outbound

Requests Allow

Figure 58 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**

The screenshot shows a dialog box titled "Edit Header Control" with a close button "X" in the top right corner. The dialog contains the following fields and controls:

- Proprietary Request Header**: A checkbox that is checked.
- Header Name**: A text input field containing the value "AV-Global-Session-ID".
- Method Name**: A dropdown menu with "ALL" selected.
- Header Criteria**: Three radio buttons: "Forbidden" (selected), "Mandatory", and "Optional".
- Presence Action**: A dropdown menu with "Remove header" selected.
- 486 Busy Here**: A button located below the Presence Action dropdown.
- Finish**: A button located at the bottom center of the dialog.

Figure 59 Signaling Rules for Avaya SM continuation

- Repeat the same steps for all other required headers

**Signaling Rules: Avaya SM**

Buttons: Add, Rename, Clone, Delete

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          | Method Name | Header Criteria | Action        | Proprietary | Direction | Edit | Delete |
|-----|----------------------|-------------|-----------------|---------------|-------------|-----------|------|--------|
| 1   | Alert-Info           | ALL         | Forbidden       | Remove Header | No          | IN        | Edit | Delete |
| 2   | Reason               | ALL         | Forbidden       | Remove Header | No          | IN        | Edit | Delete |
| 3   | AV-Global-Session-ID | ALL         | Forbidden       | Remove Header | Yes         | IN        | Edit | Delete |
| 4   | Endpoint-View        | ALL         | Forbidden       | Remove Header | Yes         | IN        | Edit | Delete |
| 5   | P-AV-Message-Id      | ALL         | Forbidden       | Remove Header | Yes         | IN        | Edit | Delete |
| 6   | P-Charging-Vector    | ALL         | Forbidden       | Remove Header | Yes         | IN        | Edit | Delete |
| 7   | P-Location           | ALL         | Forbidden       | Remove Header | Yes         | IN        | Edit | Delete |

Figure 60 Signaling Rules for Avaya SM continuation

- Repeat the same steps for Response Headers

**Signaling Rules: Avaya\_SM**

Buttons: Add, Rename, Clone, Delete

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 | Edit | Delete |
|-----|----------------------|---------------|-------------|-----------------|---------------|-------------|-----------|------|--------|
| 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 61 Signaling Rules for Avaya SM continuation

## 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**

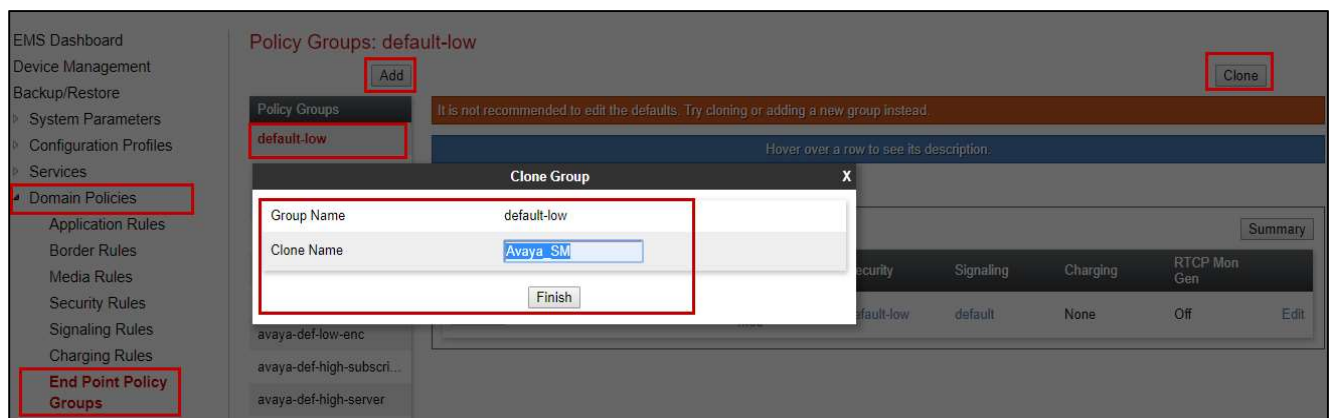
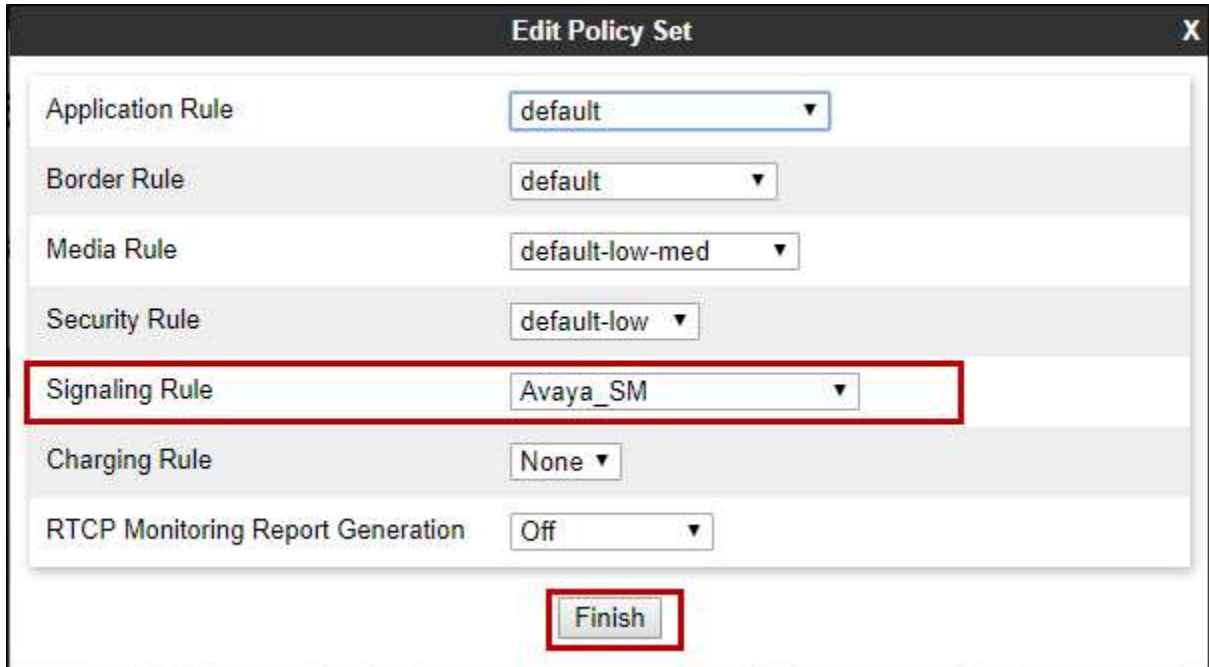


Figure 62 End Point Policy Group for Avaya SM

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



The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several configuration options, each with a dropdown menu:

|                                   |                 |
|-----------------------------------|-----------------|
| Application Rule                  | default         |
| Border Rule                       | default         |
| Media Rule                        | default-low-med |
| Security Rule                     | default-low     |
| Signaling Rule                    | Avaya_SM        |
| Charging Rule                     | None            |
| RTCP Monitoring Report Generation | Off             |

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

*Figure 63 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

The screenshot displays the 'Policy Groups: AmazonVC' configuration page. On the left, a sidebar lists various policy groups, with 'AmazonVC' highlighted. The main area shows a table with the following data:

| Order | Application | Border  | Media      | Security    | Signaling | Charging | RTCP Mon Gen |      |
|-------|-------------|---------|------------|-------------|-----------|----------|--------------|------|
| 1     | default     | default | Amazon-enc | default-low | default   | None     | Off          | Edit |

Figure 64 End Point Policy Group for Amazon

#### 4.4.7 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**

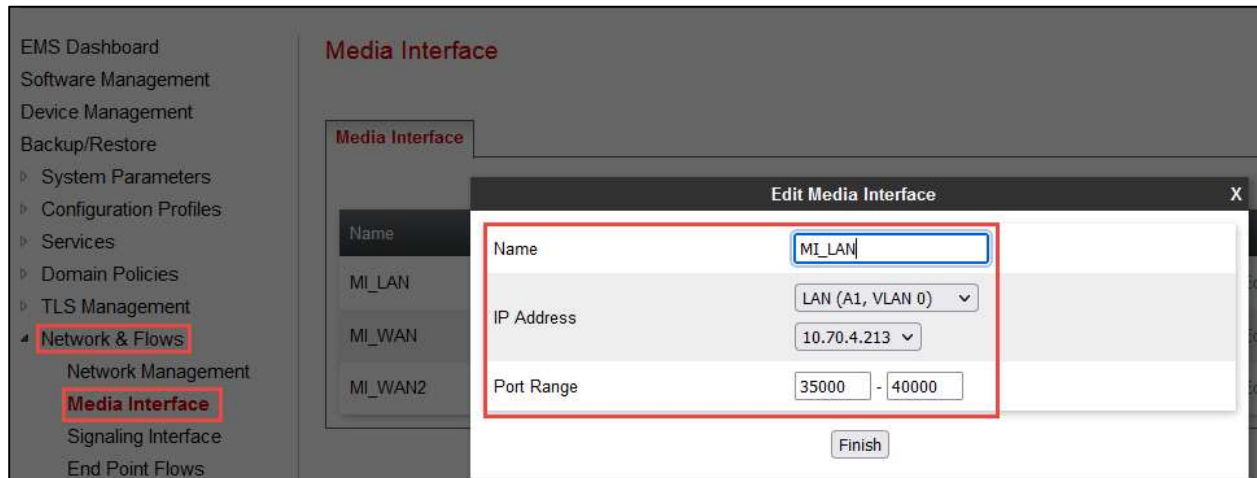


Figure 65 Media Interface facing Avaya SM

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

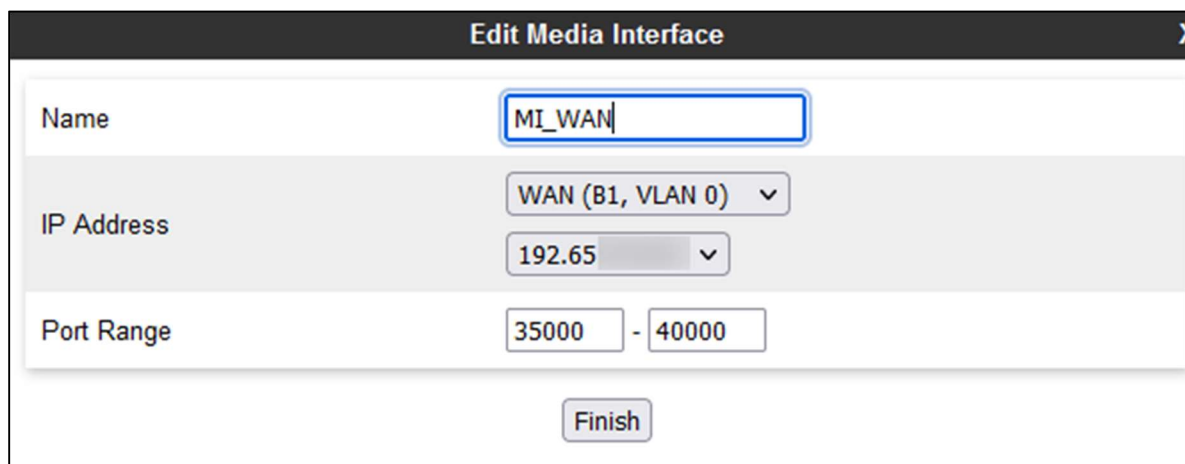


Figure 66 Media Interface facing Amazon

## 4.4.8 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**
- Set **UDP Port**: **5060**
- Click **Finish**

The screenshot shows the EMS Dashboard with the 'Signaling Interface' configuration window open. The window is titled 'Edit Signaling Interface' and contains the following fields:

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

The 'Finish' button is located at the bottom right of the window. The left sidebar of the dashboard shows the navigation menu with 'Network & Flows' and 'Signaling Interface' highlighted.

Figure 67 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.

The screenshot displays the EMS Dashboard with a sidebar on the left containing navigation options like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'Network Management', 'Media Interface', 'Signaling Interface', 'End Point Flows', 'Session Flows', 'Advanced Options', 'DMZ Services', and 'Monitoring & Logging'. The main area is titled 'Signaling Interface' and shows a list of interfaces: SI\_PSTN, SI\_LAN, and SI\_WAN. The 'SI\_WAN' interface is selected, and an 'Edit Signaling Interface' dialog box is open. The dialog has the following fields: 'Name' (SI\_WAN), 'IP Address' (WAN (B1, VLAN 0) 192.65), 'TCP Port' (Leave blank to disable), 'UDP Port' (5060), 'TLS Port' (Leave blank to disable), 'TLS Profile' (None), 'Enable Shared Control' (checkbox), and 'Shared Control Port'. A 'Finish' button is located at the bottom of the dialog.

Figure 68 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*: **SI\_WAN** (created in section 4.5.10)
- Set *Signaling Interface*: **SI\_LAN** (section 4.5.10)
- Set *Media Interface*: **Mi\_LAN** (section 4.5.9)
- Set *End Point Policy Group*: **Avaya\_SM** (section 4.5.8)
- Set *Routing Profile*: **AmazonVC** (section 4.5.6)

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

Edit Flow: Avaya SM X

|                               |                                       |
|-------------------------------|---------------------------------------|
| Flow Name                     | <input type="text" value="Avaya SM"/> |
| SIP Server Profile            | <input type="text" value="Avaya_SM"/> |
| URI Group                     | <input type="text" value="*"/>        |
| Transport                     | <input type="text" value="UDP"/>      |
| Remote Subnet                 | <input type="text" value="*"/>        |
| Received Interface            | <input type="text" value="SI_WAN"/>   |
| Signaling Interface           | <input type="text" value="SI_LAN"/>   |
| Media Interface               | <input type="text" value="MI_LAN"/>   |
| Secondary Media Interface     | <input type="text" value="None"/>     |
| End Point Policy Group        | <input type="text" value="Avaya SM"/> |
| Routing Profile               | <input type="text" value="AmazonVC"/> |
| Topology Hiding Profile       | <input type="text" value="AVAYA_SM"/> |
| Signaling Manipulation Script | <input type="text" value="None"/>     |
| Remote Branch Office          | <input type="text" value="Any"/>      |
| Link Monitoring from Peer     | <input type="checkbox"/>              |
| FQDN Support                  | <input type="checkbox"/>              |
| FQDN                          | <input type="text"/>                  |

Figure 69 Server Flow for Avaya SM

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

**Edit Flow: AmazonVC**

|                               |                          |
|-------------------------------|--------------------------|
| Flow Name                     | AmazonVC                 |
| SIP Server Profile            | AmazonVC                 |
| URI Group                     | *                        |
| Transport                     | UDP                      |
| Remote Subnet                 | *                        |
| Received Interface            | SI_LAN                   |
| Signaling Interface           | SI_WAN                   |
| Media Interface               | MI_WAN                   |
| Secondary Media Interface     | None                     |
| End Point Policy Group        | AmazonVC                 |
| Routing Profile               | AVAYA_SM                 |
| Topology Hiding Profile       | AmazonVC                 |
| Signaling Manipulation Script | None                     |
| Remote Branch Office          | Any                      |
| Link Monitoring from Peer     | <input type="checkbox"/> |
| FQDN Support                  | <input type="checkbox"/> |
| FQDN                          |                          |

**Finish**

Figure 70 Server Flow for Amazon

#### 4.4.9 TLS Configuration

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

Amazon Chime Voice Connector Root Certificate can be downloaded from Amazon Chime Voice Connector account

- 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**

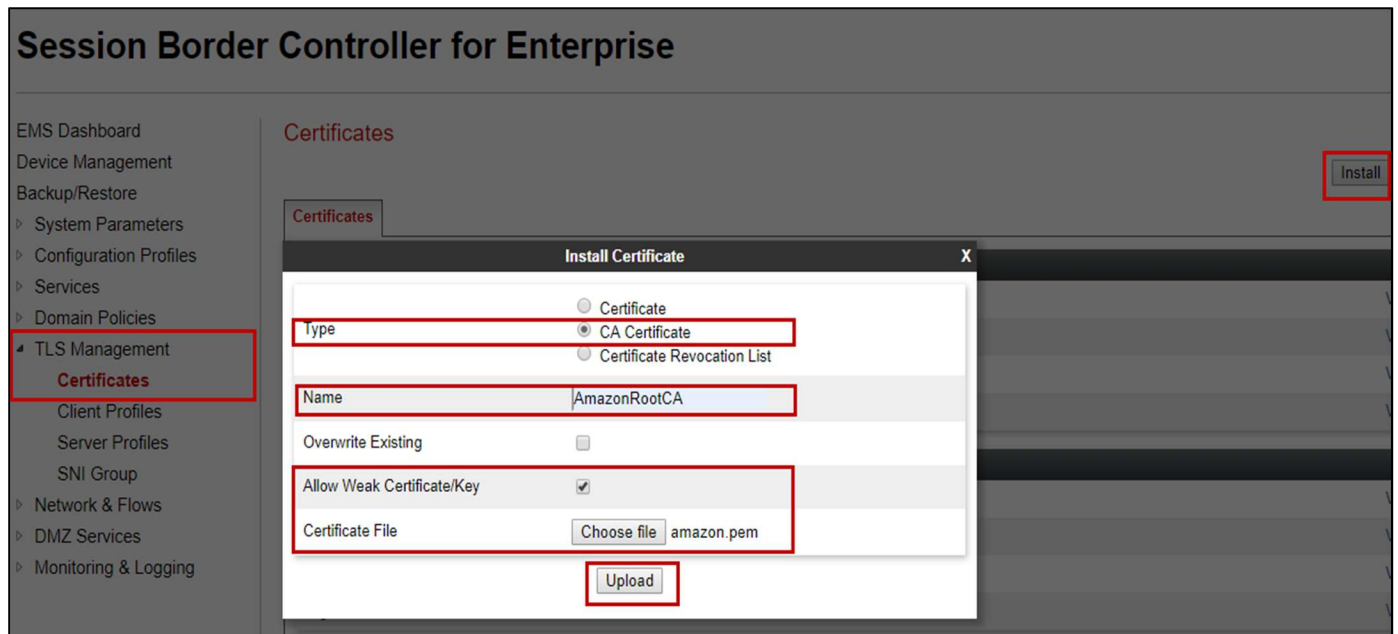


Figure 71 Upload Amazon Root CA

## 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 **asbce10.crt** for Avaya SBCE interface facing Amazon Chime Voice Connector
- Set *Peer Certificate Authorities*: Select **amazon.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 72 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 73 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 **asbce10.crt** for Avaya SBCE interface facing Amazon Chime 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**

**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 Options:

SNI Group:

**Certificate Verification**

Peer Verification:

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

**Next**

Figure 74 Server Profile facing Amazon

- Set *Version*: Check 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 75 Server Profile facing Amazon Continuation

## Edit SIP Server

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

The screenshot displays the 'Edit SIP Server Profile - General' configuration window. The left sidebar shows the navigation menu with 'SIP Servers' highlighted. The main window contains the following configuration details:

- Server Type:** Trunk Server (dropdown menu)
- SIP Domain:** (empty text field)
- DNS Query Type:** NONE/A (dropdown menu)
- TLS Client Profile:** SBCWAN (dropdown menu)
- IP Address / FQDN:** EnterAmazonOutboundHostName (text field)
- Port:** 5061 (text field)
- Transport:** TLS (dropdown menu)

Buttons for 'Add', 'Delete', and 'Finish' are also visible.

Figure 76 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**

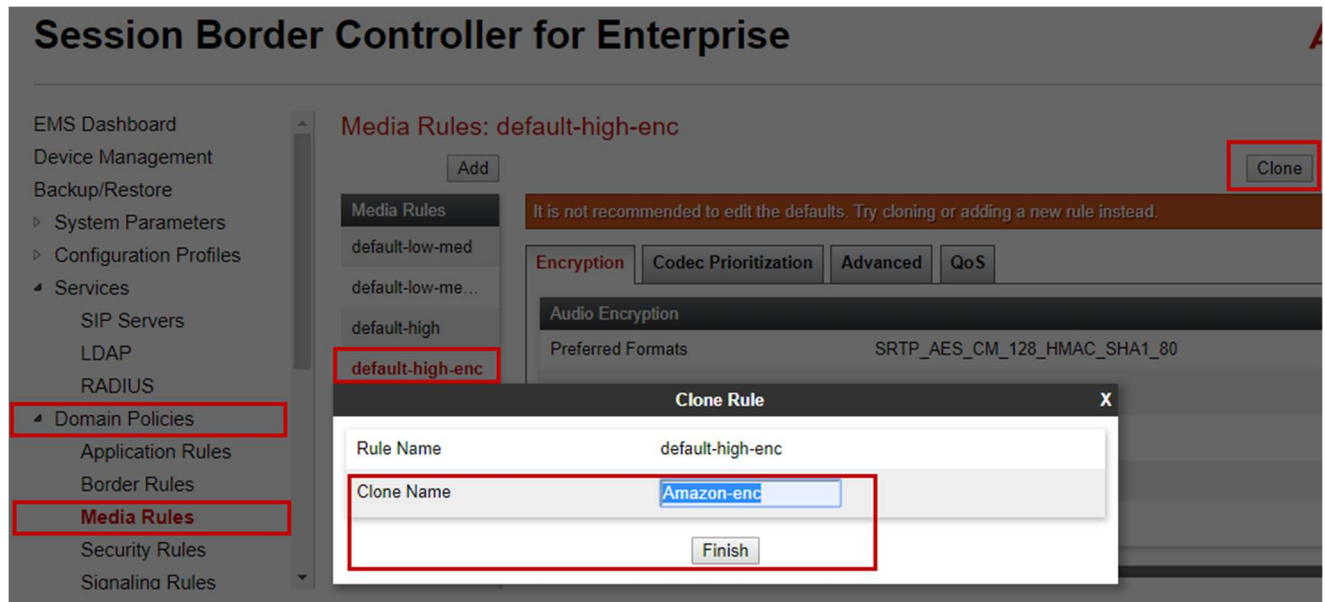


Figure 77 Media Rule – Amazon

- 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 ▾                           |
| Preferred Format #2  | NONE ▾   |
| Preferred Format #3  | NONE ▾   |
| Encrypted RTCP   | <input type="checkbox"/>                                 |
| MKI  | <input type="checkbox"/>                                 |
| Lifetime<br><small>Leave blank to match any value.</small> | 2 <sup>^</sup> <input style="width: 40px;" 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"/>                                 |
| MKI  | <input type="checkbox"/>                                 |
| Lifetime<br><small>Leave blank to match any value.</small> | 2 <sup>^</sup> <input style="width: 40px;" type="text"/> |
| Interworking   | <input checked="" type="checkbox"/>                      |
| Symmetric Context Reset                                    | <input checked="" type="checkbox"/>                      |
| Key Change in New Offer                                    | <input type="checkbox"/>                                 |

*Figure 78 Media Rule – Amazon Continuation*

## Edit End Point Policy Groups

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

The screenshot displays the 'Edit End Point Policy Group' interface. On the left, a sidebar lists various policy groups, with 'AmazonCVC' highlighted. The main area shows a table with columns for Order, Application, Border, Media, Security, Signaling, Charging, and RTP Mon Gen. The 'Edit' button is highlighted in red.

| Order | Application | Border  | Media           | Security    | Signaling | Charging | RTP Mon Gen |      |
|-------|-------------|---------|-----------------|-------------|-----------|----------|-------------|------|
| 1     | default     | default | default-low-med | default-low | default   | None     | Off         | Edit |

Figure 79 Edit End Point policy Group – Amazon

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

**Edit Policy Set**

Application Rule: default

Border Rule: default

**Media Rule: Amazon-enc**

Security Rule: default-low

Signaling Rule: default

Charging Rule: None

RTCP Monitoring Report Generation: Off

**Finish**

Figure 80 Edit End Point policy Group – Amazon Continuation

### Edit Signaling Interface

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

**Signaling Interface**

| Name          | Signaling IP Network             | TCP Port | UDP Port | TLS Port | TLS Profile |             |
|---------------|----------------------------------|----------|----------|----------|-------------|-------------|
| SI_PSTN       | 10.64.5.219<br>WAN2 (B2, VLAN 0) | 5060     | 5060     | ---      | None        | Edit Delete |
| SI_LAN        | 10.70.4.213<br>LAN (A1, VLAN 0)  | 5060     | 5060     | ---      | None        | Edit Delete |
| <b>SI_WAN</b> | 192.65<br>WAN (B1, VLAN 0)       | ---      | ---      | 5061     | SBCWAN      | Edit Delete |

Figure 81 Edit Signaling Interface – Amazon

- 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

IP Address

TCP Port  Leave blank to disable

UDP Port  Leave blank to disable

TLS Port  Leave blank to disable

TLS Profile

Enable Shared Control

Shared Control Port

**Finish**

Figure 82 Edit Signaling Interface – Amazon continuation

## Edit Server Flows

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

The screenshot displays the 'End Point Flows' configuration page in the EMS interface. The left sidebar shows the navigation menu with 'Network & Flows' and 'End Point Flows' highlighted. The main content area shows the 'Server Flows' tab selected, with a table listing the configured flows. The 'AmazonVC' flow is highlighted, and the 'Edit' button is visible for it.

| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |      |       |      |        |
|----------|-----------|-----------|--------------------|---------------------|------------------------|-----------------|------|-------|------|--------|
| 1        | AmazonVC  | *         | SI_LAN             | SI_WAN              | AmazonVC               | AVAYA_SM        | View | Clone | Edit | Delete |
| 1        | Avaya SM  | *         | SI_WAN             | SI_LAN              | Avaya SM               | AmazonVC        | View | Clone | Edit | Delete |

Figure 83 Edit Server Flow – Amazon

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

The screenshot shows a configuration window titled "Edit Flow: AmazonVC". The window contains several fields for configuring a flow. The "Transport" field is set to "TLS" and the "End Point Policy Group" field is set to "AmazonVC". Both of these fields are highlighted with red rectangular boxes. Other fields include "Flow Name" (AmazonVC), "SIP Server Profile" (AmazonVC), "URI Group" (\*), "Remote Subnet" (\*), "Received Interface" (SI\_LAN), "Signaling Interface" (SI\_WAN), "Media Interface" (MI\_WAN), "Secondary Media Interface" (None), "Routing Profile" (AVAYA\_SM), "Topology Hiding Profile" (AmazonVC), "Signaling Manipulation Script" (None), "Remote Branch Office" (Any), "Link Monitoring from Peer" (checkbox), "FQDN Support" (checkbox), and "FQDN" (text box). A "Finish" button is located at the bottom center of the window.

|                               |                          |
|-------------------------------|--------------------------|
| Flow Name                     | AmazonVC                 |
| SIP Server Profile            | AmazonVC                 |
| URI Group                     | *                        |
| Transport                     | TLS                      |
| Remote Subnet                 | *                        |
| Received Interface            | SI_LAN                   |
| Signaling Interface           | SI_WAN                   |
| Media Interface               | MI_WAN                   |
| Secondary Media Interface     | None                     |
| End Point Policy Group        | AmazonVC                 |
| Routing Profile               | AVAYA_SM                 |
| Topology Hiding Profile       | AmazonVC                 |
| Signaling Manipulation Script | None                     |
| Remote Branch Office          | Any                      |
| Link Monitoring from Peer     | <input type="checkbox"/> |
| FQDN Support                  | <input type="checkbox"/> |
| FQDN                          |                          |

**Finish**

Figure 84 Edit Server Flow – Amazon continuation

#### 4.4.10 SIP Authentication

- Navigate to: **Services > SIP Servers**
- *SIP Server*: Select **AmazonVC**, 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**

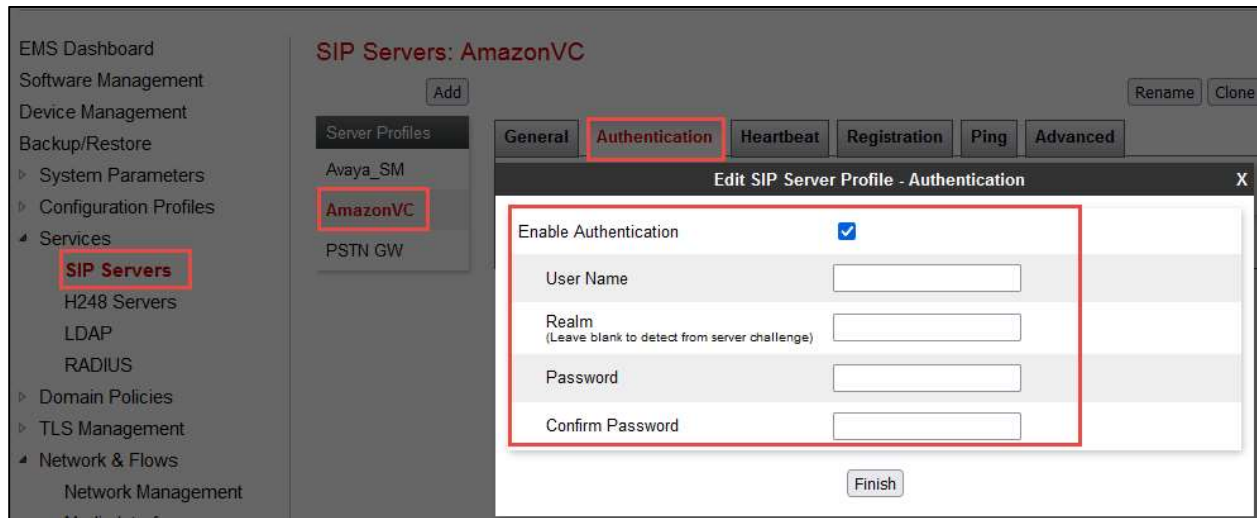


Figure 85 SIP Authentication – Amazon