



# **Application Notes for Configuring Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 to support Telnyx SIP Trunking Service – Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service on an enterprise solution consisting of Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 to interoperate with Telnyx SIP Trunking service.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

The Telnyx SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the Telnyx network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	6
2.3.	Support .....	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated .....	10
5.	Configure Avaya Aura® Communication Manager .....	11
5.1.	Licensing and Capacity .....	11
5.2.	System Features.....	12
5.3.	IP Node Names.....	14
5.4.	Codecs .....	14
5.5.	IP Network Regions .....	16
5.6.	Signaling Group .....	17
5.7.	Trunk Group .....	19
5.8.	Calling Party Information.....	23
5.9.	Inbound Routing.....	23
5.10.	Outbound Routing .....	24
6.	Configure Avaya Aura® Session Manager .....	27
6.1.	System Manager Login and Navigation.....	28
6.2.	SIP Domain .....	30
6.3.	Locations .....	31
6.4.	Adaptations.....	33
6.5.	SIP Entities .....	35
6.6.	Entity Links .....	38
6.7.	Routing Policies .....	39
6.8.	Dial Patterns .....	40
7.	Configure Avaya Session Border Controller for Enterprise .....	42
7.1.	System Access.....	42
7.2.	Device Management.....	44
7.3.	TLS Management.....	45
7.3.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise .....	46
7.3.2.	Server Profiles.....	47
7.3.3.	Client Profiles .....	49
7.4.	Network Management.....	51
7.5.	Media Interfaces .....	52
7.6.	Signaling Interfaces.....	53
7.7.	Server Interworking.....	55
7.7.1.	Server Interworking Profile – Enterprise .....	55
7.7.2.	Server Interworking Profile – Service Provider.....	57
7.8.	Server Configuration .....	59
7.8.1.	Server Configuration Profile – Enterprise .....	59
7.8.2.	Server Configuration Profile – Service Provider .....	61
7.9.	Routing .....	63

7.9.1.	Routing Profile – Enterprise .....	63
7.9.2.	Routing Profile – Service Provider .....	65
7.10.	Topology Hiding.....	66
7.10.1.	Topology Hiding Profile – Enterprise.....	66
7.10.2.	Topology Hiding Profile – Service Provider.....	68
7.11.	Domain Policies.....	69
7.11.1.	Media Rules.....	69
7.12.	End Point Policy Groups .....	72
7.12.1.	End Point Policy Group – Enterprise .....	72
7.12.2.	End Point Policy Group – Service Provider.....	73
7.13.	End Point Flows.....	74
7.13.1.	End Point Flow – Service Provider .....	75
7.13.2.	End Point Flow – Session Manager .....	76
8.	Telnyx SIP Trunking Service Configuration .....	77
9.	Verification and Troubleshooting .....	78
9.1.	General Verification Steps .....	78
9.2.	Communication Manager Verification.....	78
9.3.	Session Manager Verification .....	79
9.4.	Avaya SBCE Verification .....	81
10.	Conclusion .....	85
11.	References.....	85

# 1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Telnyx network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 10.1 (Communication Manager), Avaya Aura® Session Manager 10.1 (Session Manager), Avaya Session Border Controller for Enterprise 10.1 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Telnyx SIP Trunking service referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

The terms “Service Provider” or “Telnyx” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the network via a broadband connection to the public Internet.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

## 2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability, the following features and functionality were covered during the interoperability compliance test:

- SIP Trunk Authentication.
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by Telnyx. Incoming PSTN calls were terminated to the following endpoints: Avaya J189 IP Deskphones (SIP), Avaya 96x1 IP Deskphones (H.323), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Workplace client for Windows (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya Workplace client for Windows (SIP).
- Outgoing calls to the PSTN were routed via Telnyx network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.729, G.711A and G.711MU.
- No matching codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833:
  - Outbound call to PSTN application requiring DTMF (e.g., an IVR or voice mail system).
  - Inbound call from PSTN to Avaya CPE application requiring DTMF (e.g., Aura® Messaging, Avaya vector digit collection steps).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Routing inbound vector call to call center agent queues.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- Fax transmission using T.38 and G.711 pass-through.

**Note** – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in

these Application Notes. Consult reference [9] in the **References** section for additional information on this topic.

The following items were not tested:

- The “0” calls (Operator), 0+10 digits calls (Operator Assisted) and local directory assistance calls were not tested.

## 2.2. Test Results

Interoperability testing of the Telnyx SIP Trunking Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **Fax support:** Fax calls using the T.38 protocol worked properly during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay.
- **Caller ID display on EC500 extension to cellular:** For EC500 extension to cellular calls the Caller ID display at the Mobile/cellular station was always of the range DID numbers assigned to the trunk, regardless of the PSTN number being used to originate the call.
- **SIP OPTION Messages:** During the compliance test Telnyx did not send SIP OPTION messages to Avaya, Session Manager did send SIP OPTION messages to Telnyx and Telnyx responds back with 200 OK Keepalive SIP message, this was sufficient to keep the SIP trunk up in-service.
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider’s network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider’s network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location (**Section 6.4**).
- **Call transfer using REFER:** The regular call transfer from enterprise extension was working properly however the call transfer from Vector Directory Number (VDN) requires the Refer-To header having Telnyx SIP domain to work. This can be accomplished by overwrite the Telnyx SIP domain in the Refer-To header in the topology hiding profile for Telnyx as configured in **Section 7.10.2**.

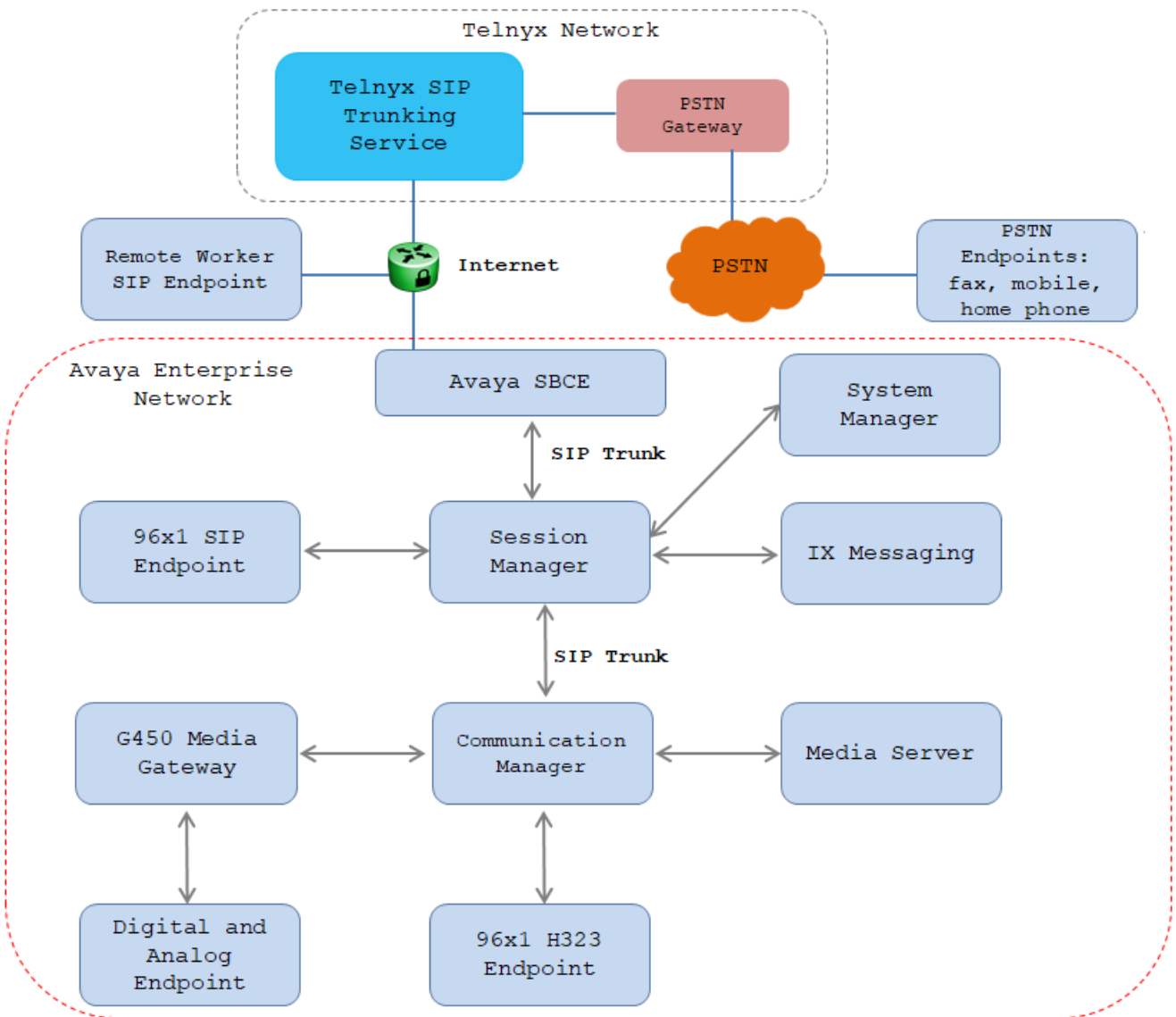
## 2.3. Support

For support of Telnyx SIP Trunking Service visit the corporate Web page at: <https://telnyx.com/>

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>

### 3. Reference Configuration

**Figure 1** illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Telnyx SIP Trunking Service through a public Internet WAN connection.



**Figure 1: Avaya SIP Enterprise Solution connected to Telnyx SIP Trunking Service**

The Avaya components used to create the simulated enterprise customer site included:

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya IX Messaging™
- Avaya Aura® Media Server.
- Avaya G450 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya J189 IP Deskphones (SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Workplace Client for Windows softphone (SIP).
- Avaya Agent for Desktop (SIP).
- Avaya digital and analog telephones.
- Ventafax fax software.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya Workplace Client for Windows (SIP). Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult reference [9] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (Communication Manager) and on which link to send the call.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Telnyx network.



A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

Communication Manager incorporates the ability to use the Avaya Aura® Media Server (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G430 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the **References** section.

The Avaya IX Messaging™ was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for IX Messaging™ are not directly related to the interoperability tests with the Telnyx network SIP Trunking service, they are not included in these Application Notes.

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya Aura® Communication Manager	10.1.0.0.0 Service Pack 0.1 (01.0.974.0-27293)
Avaya Aura® Session Manager	10.1.0.0 (10.1.0.0.1010019)
Avaya Aura® System Manager	10.1.0.0 Build No. 10.1.0.0.537353 Software Update Rev. No. 10.1.0.0.0614119
Avaya Session Border Controller for Enterprise	ASBCE 10.1 10.1.1.0-35-21872
Avaya IX Messaging™	11.0.0.3204 (IXM-11.0.0.3204)
Avaya Aura® Media Server	8.0.2.218_2022.01.05
Avaya G430 Media Gateway	g430_sw_42.7.0
Avaya J189 IP Deskphones (SIP)	Version 4.0.10.3.2
Avaya 9641G Deskphones (SIP and H.323)	7.1.9.0.8 (SIP) 6.8.304 (H.323)
Avaya one-X® Communicator (H.323, SIP)	6.2.14.15-SP14-Patch7
Avaya Workplace Client for Windows (SIP)	3.25.0.73
Avaya Agent for Desktop (Windows) (SIP)	2.0.6.19.3004
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
<b>Telnyx (Not Applicable)</b>	

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Servers and Media Gateway platforms running similar versions of Communication Manager and Session Manager. Telnyx prefers not to show their SIP trunk systems and software release.

**Note** – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.7.0) platforms. Consult the installation documentation on the **References** section for more information.

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the Telnyx SIP Trunking Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and the Avaya Media Server has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens capture will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

### 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **40000** licenses are available and **20** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
	Maximum Administered H.323 Trunks:	12000	10
	Maximum Concurrently Registered IP Stations:	18000	10
	Maximum Administered Remote Office Trunks:	12000	0
Max	Concurrently Registered Remote Office Stations:	18000	0
	Maximum Concurrently Registered IP eCons:	414	0
	Max Concur Reg Unauthenticated H.323 Stations:	100	0
	Maximum Video Capable Stations:	41000	2
	Maximum Video Capable IP Softphones:	18000	13
	<b>Maximum Administered SIP Trunks:</b>	<b>40000</b>	<b>20</b>
Max	Administered Ad-hoc Video Conferencing Ports:	24000	0
	Max Number of DS1 Boards with Echo Cancellation:	999	0
(NOTE: You must logoff & login to effect the permission changes.)			

## 5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to **none**.

```
change system-parameters features                                     Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
      Music/Tone on Hold: music Type: ext 1103
      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **restricted** for restricted calls and **unavailable** for unavailable calls.

change system-parameters features	Page 9 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
CPN/ANI/ICLID PARAMETERS	
<b>CPN/ANI/ICLID Replacement for Restricted Calls: Restricted</b>	
<b>CPN/ANI/ICLID Replacement for Unavailable Calls: Unavailable</b>	
DISPLAY TEXT	
	Identity When Bridging: principal
	User Guidance Display? n
Extension only label for Team button on 96xx H.323 terminals? n	
INTERNATIONAL CALL ROUTING PARAMETERS	
	Local Country Code:
	International Access Code:
SCCAN PARAMETERS	
Enable Enbloc Dialing without ARS FAC? n	
CALLER ID ON CALL WAITING PARAMETERS	
Caller ID on Call Waiting Delay Timer (msec): 200	

### 5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and the Session Manager security module (**SM10**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AMS1	10.33.1.30	
AMS2	10.33.1.44	
CMS19	10.33.1.18	
RDTT	10.33.100.16	
<b>SM10</b>	<b>10.33.1.42</b>	
<b>procr</b>	<b>10.33.1.43</b>	
default	0.0.0.0	

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 3 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. Telnyx supports audio codecs **G.729**, **G.711A** and **G.711MU**. In the **Media Encryption** section, enter “1-srtp-aescm128-hmac80” as the encryption for secure media.

change ip-codec-set 3		Page 1 of 2
IP MEDIA PARAMETERS		
Codec Set: 3		
Audio Codec	Silence Suppression	Frames Per Pkt Size (ms)
1: G.711MU	n	2 20
2: G.711A	n	2 20
3: G.729	n	2 20
4:		
5:		
6:		
7:		
Media Encryption		Encrypted SRTP: best-effort
1:	1-srtp-aescm128-hmac80	
2:	none	
3:		

On **Page 2**, set the **Fax Mode** to **t.38-standard**.

change ip-codec-set 3		Page 2 of 2	
IP MEDIA PARAMETERS			
Allow Direct-IP Multimedia? y			
Maximum Call Rate for Direct-IP Multimedia:		384:Kbits	
Maximum Call Rate for Priority Direct-IP Multimedia:		384:Kbits	
	Mode	Redun- dancy	Packet Size (ms)
<b>FAX</b>	<b>t.38-standard</b>	0 ECM: y	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20
Media Connection IP Address Type Preferences			
1: IPv4			
2:			

## 5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avayalab.com** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes**, the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

```
change ip-network-region 3                                     Page 1 of 20
                                                                IP NETWORK REGION
  Region: 3           NR Group: 3
Location: 1           Authoritative Domain: avayalab.com
    Name: public      Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
    Codec Set: 3      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 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5
```



On **Page 4**, define the IP codec set to be used for traffic between region 3 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **3** will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 3										Page 4 of 20
Source Region: 3 Inter Network Region Connection Management										I S M
										G A y t
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	n	c
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	c e
1	3	y	NoLimit						n	all y t
2										
3	3									all
4										
5										
6										

## 5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, **tls** was used.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer is a Session Manager.

**Note:** Once the **Peer-Server** field is updated to **SM**, the system changes the default values of the following fields, setting them to display-only:

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to **y**.
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to **n**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM10**. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is

necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5067**.

- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**.
- Set **Initial IP-IP Direct Media** to **y**.
- Default values may be used for all other fields.

change signaling-group 3		Page 1 of 2
SIGNALING GROUP		
Group Number: 3	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
<b>Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y</b>		
<b>Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n</b>		
Alert Incoming SIP Crisis Calls? n		
<b>Near-end Node Name: procr</b>	<b>Far-end Node Name: SM10</b>	
<b>Near-end Listen Port: 5067</b>	<b>Far-end Listen Port: 5067</b>	
	<b>Far-end Network Region: 3</b>	
<b>Far-end Domain: avayalab.com</b>		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	<b>Direct IP-IP Audio Connections? y</b>	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	<b>Initial IP-IP Direct Media? y</b>	
	Alternate Route Timer(sec): 6	

## 5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 3 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.

Default values were used for all other fields.

change trunk-group 3		Page 1 of 4	
TRUNK GROUP			
Group Number: 3	Group Type: sip	CDR Reports: n	
Group Name: To-ServiceProvider	COR: 1	TN: 1	TAC: #03
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 3	
		Number of Members: 10	

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. The default value of **600** seconds was used.

```
change trunk-group 3                                     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): 600

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
```

On Page 3:

- Set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end. When **public** format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. The **Numbering Format** was set to **public** and the **Numbering Format** in the route pattern was set to **pub-unk** (see **Section 5.10**).
- Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

```
change trunk-group 3                                     Page 3 of 4
TRUNK FEATURES
    ACA Assignment? n                                     Measured: both
                                                         Maintenance Tests? y

    Suppress # Outpulsing? n   Numbering Format: public
                                                         UUI Treatment: service-provider

                                                         Replace Restricted Numbers? y
                                                         Replace Unavailable Numbers? y

    Modify Tandem Calling Number: no

    Show ANSWERED BY on Display? y
```

On Page 4:

- Set the **Network Call Redirection** field to **y**. With this setting, Communication Manager will use the SIP REFER method for the redirection of PSTN calls that are transferred back to the SIP trunk and SIP trunks related in the transferred call in CM will be released.
- Set the **Send Diversion Header** field to **Y** and **Support Request History** to **Y**.
- Set the **Telephone Event Payload Type** to **101**, the value preferred by Telnyx.
- Verify that **Identity for Calling Party Display** is set to **P-Asserted-Identity**.
- Default values were used for all other fields.

change trunk-group 3	Page 4 of 4
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
<b>Network Call Redirection? y</b>	
Build Refer-To URI of REFER From Contact For NCR? n	
<b>Send Diversion Header? y</b>	
<b>Support Request History? y</b>	
<b>Telephone Event Payload Type: 101</b>	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? y	
Identity for Calling Party Display: <b>P-Asserted-Identity</b>	
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	

## 5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, two DID numbers assigned by the service provider are shown. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
4	3302	3	12012700516	11	Total Administered: 2
4	3402	3	12012700527	11	Maximum Entries: 9999
					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.

## 5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Telnyx is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 3					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del	Insert	
Feature	Len	Digits			
public-ntwrk	12	+12012700516	12	3302	
public-ntwrk	12	+12012700527	12	3402	

## 5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1**, as a feature access code (**fac**).

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 6		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	udp	40	4	aar	8	1	fac
0	3	fac	411	3	udp	<b>9</b>	<b>1</b>	<b>fac</b>
1	4	ext	43	4	aar	*	3	dac
1	11	udp	44	4	udp	#	3	dac

Use the change feature-access-codes command to configure 9 as the Auto Route Selection (ARS) – Access Code 1.

change feature-access-codes			FEATURE ACCESS CODE (FAC)			Page 1 of 11		
Abbreviated Dialing List1 Access Code:								
Abbreviated Dialing List2 Access Code:								
Abbreviated Dialing List3 Access Code:								
Abbreviated Dial - Prgm Group List Access Code:								
Announcement Access Code: *05								
Answer Back Access Code: 007								
Attendant Access Code:								
Auto Alternate Routing (AAR) Access Code:								
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>						Access Code 2:		
Automatic Callback Activation:						Deactivation:		
Call Forwarding Activation Busy/DA: *07 All: *06						Deactivation: *16		
Call Forwarding Enhanced Status: Act:						Deactivation:		
Call Park Access Code: 008								
Call Pickup Access Code: *09								
CAS Remote Hold/Answer Hold-Unhold Access Code: *10								
CDR Account Code Access Code: *11								
Change COR Access Code:								
Change Coverage Access Code:								
Conditional Call Extend Activation:						Deactivation:		
Contact Closure Open Code:						Close Code:		



Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2, which contains the SIP trunk group to the service provider.

For international call to the U.S. (e.g., dialing: 912012701234):

change ars analysis 1

Page 1 of 2

ARS DIGIT ANALYSIS TABLE

Location: all

Percent Full: 1

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
<b>1</b>	<b>11</b>	<b>14</b>	<b>3</b>	<b>pubu</b>		<b>n</b>
101xxxx0	8	8	deny	op		n
101xxxx0	18	18	deny	op		n
101xxxx01	16	24	deny	iop		n
101xxxx011	17	25	deny	intl		n
101xxxx1	18	18	deny	fnpa		n
10xxx0	6	6	deny	op		n
10xxx0	16	16	deny	op		n
10xxx01	14	22	deny	iop		n
10xxx011	15	23	deny	intl		n
10xxx1	16	16	deny	fnpa		n
1200	11	11	deny	fnpa		n
121	11	11	3	pubu		n
123	10	11	3	natl		n
124	11	11	deny	fnpa		n

For local calls within same area code 201 (e.g., dialing: 2012701234):

change ars analysis 201						Page	1 of	2
ARS DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 1		
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
201		10	10	3	hnpa		n	
343		10	10	3	fnpa		n	
411		3	3	3	svcl		n	
423		10	10	3	pubu		n	
5		7	7	2	hnpa		n	
600		11	15	1	pubu		n	
608		10	10	3	pubu		n	

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 in the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** Set to **pub-unk**. All calls using this route pattern will use the public numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

change route-pattern 3										Page	1 of	4
Pattern Number: 3										Pattern Name: Public		
SCCAN? n		Secure SIP? n		Used for SIP stations? n								
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC				
No			Mrk	Lmt	List	Del	Digits	QSIG				
							Dgts	Intw				
1:	3	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	Numbering	LAR
	0	1	2	M	4	W	Request			Dgts	Format	
1:	y	y	y	y	y	n	n	rest			pub-unk	none
2:	y	y	y	y	y	n	n	rest				none
3:	y	y	y	y	y	n	n	rest				none
4:	y	y	y	y	y	n	n	rest				none
5:	y	y	y	y	y	n	n	rest				none
6:	y	y	y	y	y	n	n	rest				none

**Note** - Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.

## 6. Configure Avaya Aura® Session Manager

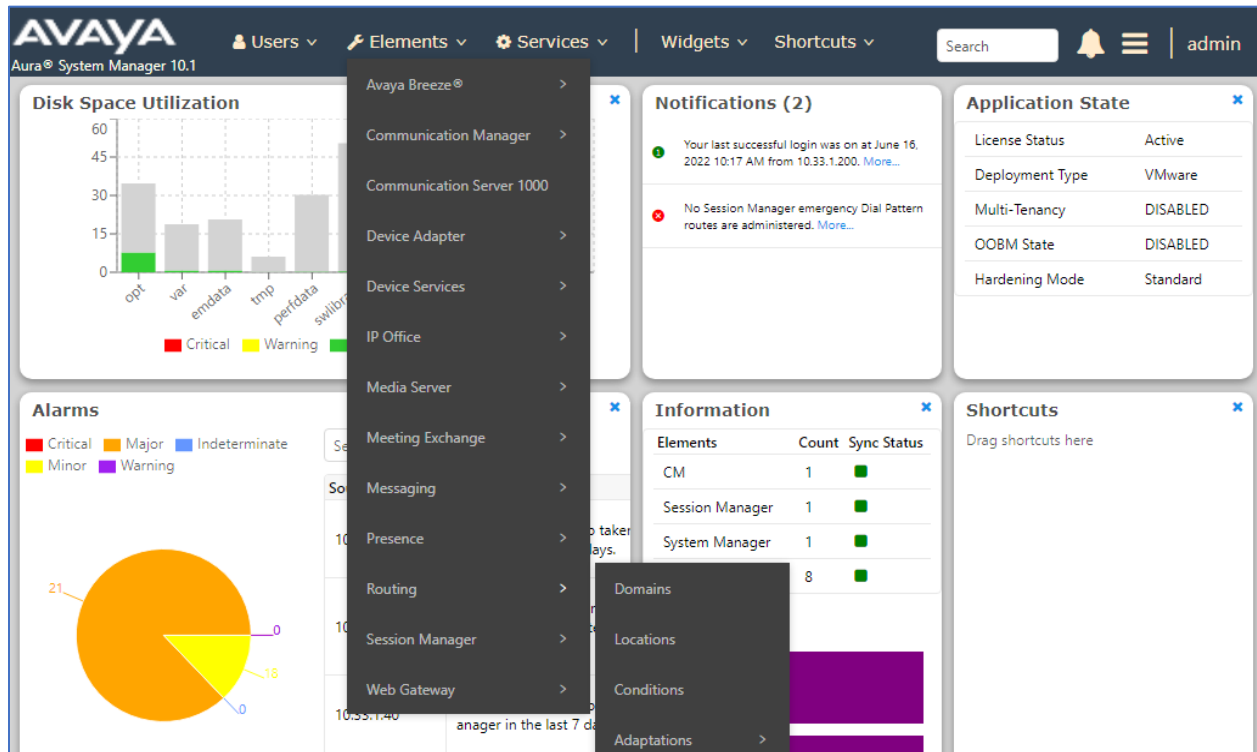
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

## 6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed; under **elements** select **Routing** → **Domains**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, version information, and links for Users, Elements, Services, Widgets, and Shortcuts. A search bar and user profile are also present. The left-hand navigation pane shows a tree structure with 'Routing' selected, which has expanded to show sub-items: Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Administration of Session Manager Routing Policies' and contains the following text:

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as follows:

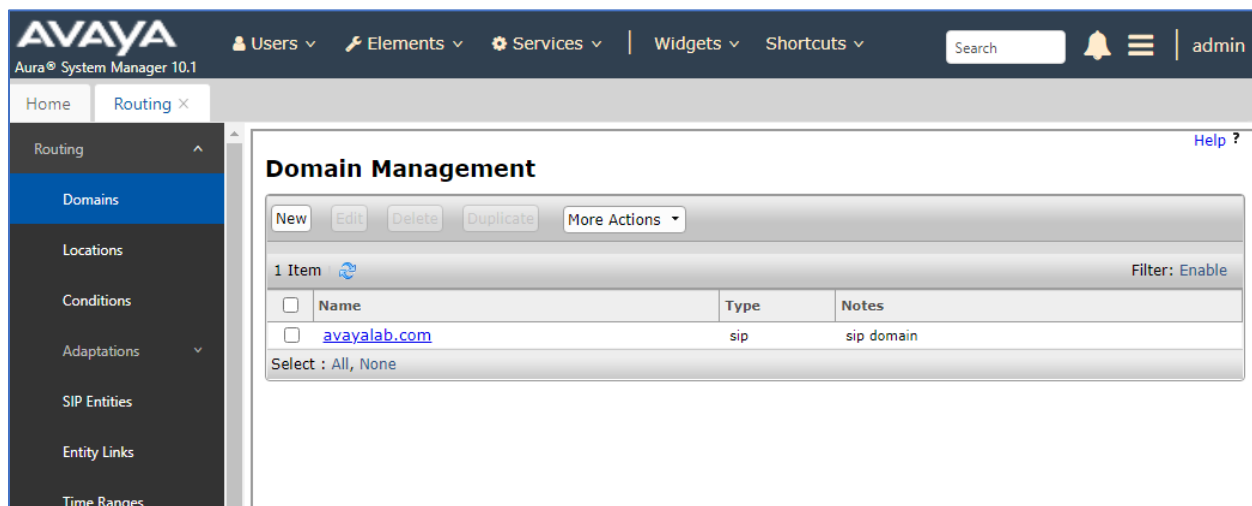
- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)
- Step 4: Create "Adaptations"
- Step 5: Create "SIP Entities"
  - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
  - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
  - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 6: Create the "Entity Links"
  - Between Session Managers
  - Between Session Managers and "other SIP Entities"
- Step 7: Create "Time Ranges"
  - Align with the tariff information received from the Service Providers
- Step 8: Create "Routing Policies"
  - Assign the appropriate "Routing Destination" and "Time Of Day"

## 6.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, **avayalab.com**. Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).
- Click **Commit** to save (not shown).

The screen below shows the entry for the enterprise domain.



## 6.3. Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management, call admission control and location-based routing. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).
- Click **Commit** to save.

The following screen shows the location details for the location named **Session Manager**. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Location Details' and contains the following sections:

- General**:
  - Name:** Session Manager
  - Notes:** Session Manager Location in VMware
- Dial Plan Transparency in Survivable Mode**:
  - Enabled:** ☐
  - Listed Directory Number:** [Empty text box]
  - Associated CM SIP Entity:** [Empty text box]
- Overall Managed Bandwidth**:
  - Managed Bandwidth Units:** Kbit/sec
  - Total Bandwidth:** [Empty text box]
  - Multimedia Bandwidth:** [Empty text box]
  - Audio Calls Can Take Multimedia Bandwidth:** ☒

At the top right of the 'Location Details' section, there are 'Commit' and 'Cancel' buttons. The user's name 'admin' is visible in the top right corner of the interface.

The following screen shows the location details for the location named **Communication Manager**. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options: Home, Routing (selected), Domains, Locations (highlighted), Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The form is divided into three sections: 'General', 'Dial Plan Transparency in Survivable Mode', and 'Overall Managed Bandwidth'. In the 'General' section, the 'Name' field is set to 'Communication Manager' and the 'Notes' field is set to 'Communication Manager Location in VI'. In the 'Dial Plan Transparency in Survivable Mode' section, the 'Enabled' checkbox is unchecked, and the 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty. In the 'Overall Managed Bandwidth' section, the 'Managed Bandwidth Units' dropdown is set to 'Kbit/sec', and the 'Total Bandwidth', 'Multimedia Bandwidth', and 'Audio Calls Can Take Multimedia Bandwidth' fields are empty. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked.

The following screen shows the location details for the location named **Avaya SBCE**. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options: Home, Routing (selected), Domains, Locations (highlighted), Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The form is divided into three sections: 'General', 'Dial Plan Transparency in Survivable Mode', and 'Overall Managed Bandwidth'. In the 'General' section, the 'Name' field is set to 'Avaya SBCE' and the 'Notes' field is set to 'Avaya SBCE Location in VMware'. In the 'Dial Plan Transparency in Survivable Mode' section, the 'Enabled' checkbox is unchecked, and the 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty. In the 'Overall Managed Bandwidth' section, the 'Managed Bandwidth Units' dropdown is set to 'Kbit/sec', and the 'Total Bandwidth', 'Multimedia Bandwidth', and 'Audio Calls Can Take Multimedia Bandwidth' fields are empty. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked.



## 6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 10.1 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named **Remove-Headers** was created to block the headers listed below before they were forwarded to the Avaya SBCE. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name:** Enter an appropriate name.
- **Module Name:** Select the **DigitConversionAdapter** option.
- **Module Parameter Type:** Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters, as follows:

- **Name:** Enter **eRHdrs**. This parameter will remove the specified headers from messages in the egress direction.
- **Value:** Enter “**Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View**”.
- Click **Commit** to save.

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left at their default values.

**AVAYA** Aura® System Manager 10.1

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

Home Routing ×

Routing Domains Locations Conditions Adaptations Adaptations Regular Expressions Device Mappings SIP Entities Entity Links Time Ranges Routing Policies

### Adaptation Details

Commit Cancel Help ?

**General**

\* **Adaptation Name:** Remove-Headers

**Notes:**

\* **Module Name:** DiversionTypeAdapter ▾

**Type:** digit

**State:** enabled ▾

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

Add Remove		
<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	eRHdrs	"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View"

Select : All, None

**Egress URI Parameters:**

## 6.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling (see **Figure 1**).
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** (or **Other**) for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

The following screen shows the addition of the **Session Manager** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left navigation pane shows the 'Routing' section expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'Monitoring'. In the 'General' section, the 'Name' field is set to 'SM10', the 'IP Address' field is set to '10.33.1.42', the 'Type' dropdown is set to 'Session Manager', and the 'Location' dropdown is also set to 'Session Manager'. The 'Time Zone' dropdown is set to 'America/Denver'. The 'Minimum TLS Version' dropdown is set to 'Use Global Setting'. The 'Credential name' field is empty. In the 'Monitoring' section, both 'SIP Link Monitoring' and 'CRLF Keep Alive Monitoring' dropdowns are set to 'Use Session Manager Configuration'. The 'Commit' and 'Cancel' buttons are visible at the top right of the form.

The following screen shows the addition of the **CM10-Public** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**. For **Type** Select **CM** for Communication Manager. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**. Select the **Time Zone**. Click **Commit** to save.

**AVAYA**  
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing ×

Routing  
Domains  
Locations  
Conditions  
Adaptations ▾  
**SIP Entities**  
Entity Links  
Time Ranges  
Routing Policies  
Dial Patterns ▾  
Regular Expressions  
Defaults <

**SIP Entity Details** Commit Cancel Help ?

**General**

\* Name: CM10-Public

\* FQDN or IP Address: 10.33.1.43

Type: CM ▾

Notes:

Adaptation: ▾

Location: Communication Manager ▾

Time Zone: America/Denver ▾

\* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: none ▾

**Loop Detection**

Loop Detection Mode: On ▾

The following screen shows the addition of the **Avaya SBCE** SIP Entity for the Avaya SBCE:

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface.
- For **Type** Select **SIP Trunk**.
- On the **Adaptation** field, the adaptation module **Remove-Headers** previously defined in **Section 6.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- Select the **Time Zone**.
- Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Name:** Avaya SBCE
- FQDN or IP Address:** 10.33.1.35
- Type:** SIP Trunk (dropdown)
- Notes:** SBCE v10 Signaling 1
- Adaptation:** Remove-Headers (dropdown)
- Location:** Avaya SBCE (dropdown)
- Time Zone:** America/Denver (dropdown)
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress (dropdown)

The 'Loop Detection' section at the bottom shows:

- Loop Detection Mode:** On (dropdown)

## 6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; an entity link to Communication Manager for use only by service provider traffic and an entity link to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** (not shown) in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link (**Section 5.6**).
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2:** Select the name of the other system from the drop-down menu (**Section 6.5**).
- **Port:** Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. **TLS** transport and port **5067** were used.

The screenshot shows the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. The first row contains the following data: Name: SM10\_CM10-Public\_5067, SIP Entity 1: SM10, Protocol: TLS, Port: 5067, SIP Entity 2: CM10-Public, Port: 5067, DNS Override: unchecked, and Connection Policy: trusted. At the bottom, there is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
SM10_CM10-Public_5067	SM10	TLS	5067	CM10-Public	5067	<input type="checkbox"/>	trusted

The Entity Link to the Avaya SBCE is shown below; **TLS** transport and port **5061** were used.

The screenshot shows the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. The first row contains the following data: Name: SM10\_Avaya SBCE\_5061, SIP Entity 1: SM10, Protocol: TLS, Port: 5061, SIP Entity 2: Avaya SBCE, Port: 5061, DNS Override: unchecked, and Connection Policy: trusted. At the bottom, there is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
SM10_Avaya SBCE_5061	SM10	TLS	5061	Avaya SBCE	5061	<input type="checkbox"/>	trusted

## 6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: An incoming policy with Communication Manager as the destination and an outbound policy with the Avaya SBCE as the destination. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager.

**AVAYA**  
Aura® System Manager 10.1

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

Home Routing ×

Routing Policies

**Routing Policy Details** [Commit] [Cancel] Help ?

**General**

\* Name: To-CM10-Public

Disabled: ☐

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM10-Public	10.33.1.43	CM	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

The following screens show the Routing Policies for the Avaya SBCE.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left navigation pane is expanded to 'Routing Policies'. The main content area displays the 'Routing Policy Details' for a policy named 'To-Avaya SBCE'. The 'General' section includes fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section shows a table with one entry: 'Avaya SBCE' with FQDN or IP Address '10.33.1.35', Type 'SIP Trunk', and Notes 'SBCE v10 Signaling 1'. The 'Time of Day' section shows a table with one item: '24/7' with a time range from '00:00' to '23:59'.

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.33.1.35	SIP Trunk	SBCE v10 Signaling 1

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

## 6.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select “**ALL**” to route incoming calls to all SIP domains.
- **Notes:** Add a brief description (optional).
- In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria (**Section 6.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 6.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to Communication Manager. In the examples, calls to 12-digit numbers starting with **+1201**



arriving from location **Avaya SBCE**, used route policy **To-CM10-Public** to Communication Manager. The SIP Domain was set to **avayalab.com**.

The screenshot shows the 'Dial Pattern Details' form in the Avaya Aura System Manager 10.1 interface. The 'General' tab is active. The 'Pattern' field is set to '+1201', 'Min' is '12', and 'Max' is '12'. The 'Emergency Call' checkbox is unchecked. The 'SIP Domain' dropdown is set to 'avayalab.com'. The 'Notes' field is empty. Below the 'General' tab, the 'Originating Locations and Routing Policies' section shows a table with one item: '-ALL-' with a rank of 0 and a routing policy of 'CM10-Public'. The 'Routing Policy Destination' is also 'CM10-Public'. The 'Routing Policy Disabled' checkbox is unchecked. The 'Select' dropdown is set to 'All, None'.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		To-CM10-Public	0	<input type="checkbox"/>	CM10-Public	

The example in this screen shows the 11-digit dialed numbers for outbound calls, beginning with **1**, arriving from the **Communication Manager** location, will use route policy **Avaya SBCE**, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP trunk. The SIP Domain was set to **avayalab.com**.

The screenshot shows the 'Dial Pattern Details' form in the Avaya Aura System Manager 10.1 interface. The 'General' tab is active. The 'Pattern' field is set to '1', 'Min' is '11', and 'Max' is '11'. The 'Emergency Call' checkbox is unchecked. The 'SIP Domain' dropdown is set to 'avayalab.com'. The 'Notes' field is empty. Below the 'General' tab, the 'Originating Locations and Routing Policies' section shows a table with one item: '-ALL-' with a rank of 0 and a routing policy of 'Avaya SBCE'. The 'Routing Policy Destination' is also 'Avaya SBCE'. The 'Routing Policy Disabled' checkbox is unchecked. The 'Select' dropdown is set to 'All, None'.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		To-Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	

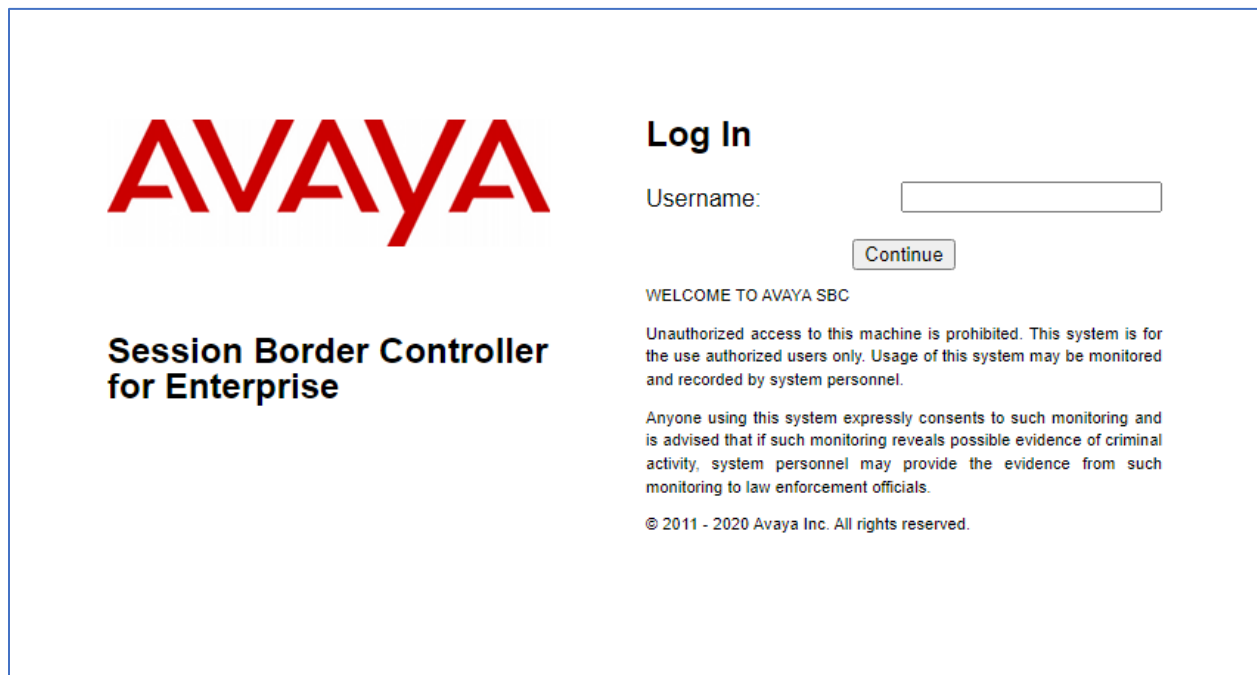
Repeat the above procedures as needed to define additional dial patterns.

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **References** section.

### 7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The image shows the login page of the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, the text "WELCOME TO AVAYA SBC" is shown, followed by a disclaimer: "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." Below this is a consent statement: "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." At the bottom, the copyright notice "© 2011 - 2020 Avaya Inc. All rights reserved." is displayed.

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **SBCEv10** in the sample configuration.

Device: EMS ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

EMS  
SBCEv10

## Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Software Management  
**Device Management**  
▸ System Administration  
▸ Templates  
Backup/Restore  
▸ Monitoring & Logging

### Device Management

Devices Updates Licensing Key Bundles

Device Name	Management IP	Version	Status	
SBCEv10	10.33.10.101	10.1.1.0-35-21872	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

Device: SBCEv10 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

## Session Border Controller for Enterprise

AVAYA

**EMS Dashboard**  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
▸ DMZ Services  
▸ Monitoring & Logging

### Dashboard

**Information**

System Time	09:59:27 AM MDT	<a href="#">Refresh</a>
Version	10.1.1.0-35-21872	
GUI Version	10.1.1.0-21872	
Build Date	Mon Apr 18 07:57:04 UTC 2022	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/01/2022 09:47:41 MDT	
Failed Login Attempts	0	

**Installed Devices**

EMS
SBCEv10

**Active Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

None found.

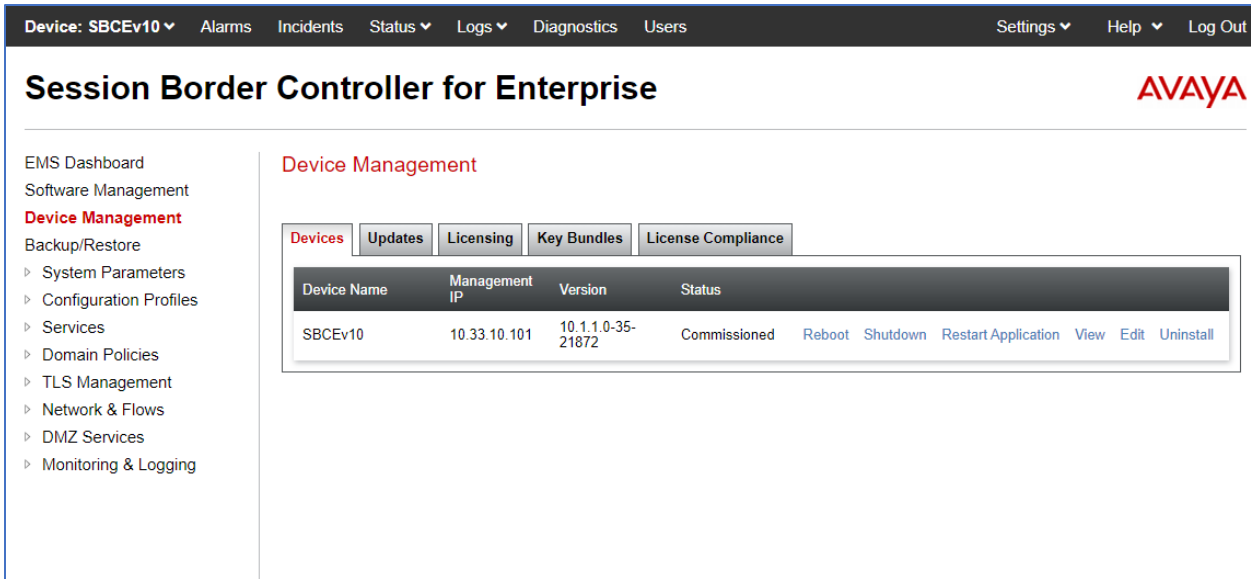
[Add](#)

**Notes**

No notes found.

## 7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **SBCEv10** is shown. The management IP address that was configured during installation is blurred out for security reasons; the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings. Note that **DNS configuration** is required for this solution. The highlighted IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to Telnyx and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (10.33.1.35) was used to connect to the enterprise network, while its public interface (50.xxx.xxx.109) was used to connect to the public network. See **Figure 1**.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

System Information: SBCEv10

General Configuration

Appliance NameSBCEv10

Box TypeSIP

Deployment ModeProxy

Device Configuration

HA ModeNo

Two Bypass ModeNo

License Allocation

Standard Sessions512  
Requested: 250

Advanced Sessions512  
Requested: 250

Scopia Video Sessions512  
Requested: 250

CES Sessions512  
Requested: 250

Transcoding Sessions512  
Requested: 250

AMR☐

Premium Sessions0  
Requested: 0

CLID---

EncryptionAvailable: Yes☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.1.35	10.33.1.35	255.255.255.0	10.33.1.1	A1
10.33.1.36	10.33.1.36	255.255.255.0	10.33.1.1	A1
50. .108	50. .108	255.255.255.128	50. .1	B1
50. .109	50. .109	255.255.255.128	50. .1	B1

DNS Configuration

Primary DNS10.33.100.60

Secondary DNS8.8.8.8

DNS LocationDMZ

DNS Client IP10.33.1.35

Management IP(s)

IP #1 (IPv4)10.33.10.101

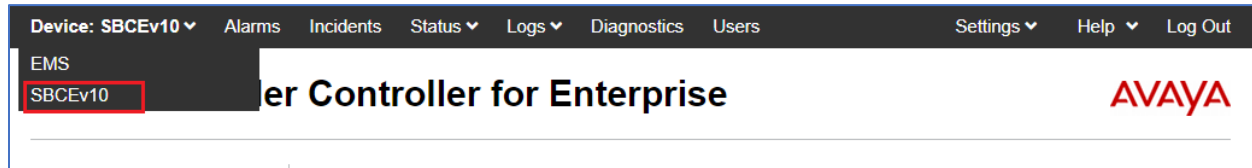
## 7.3. TLS Management

**Note** – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between Session Manager and Avaya SBCE. The following procedures show how to create the client and server profiles to support the TLS connection.

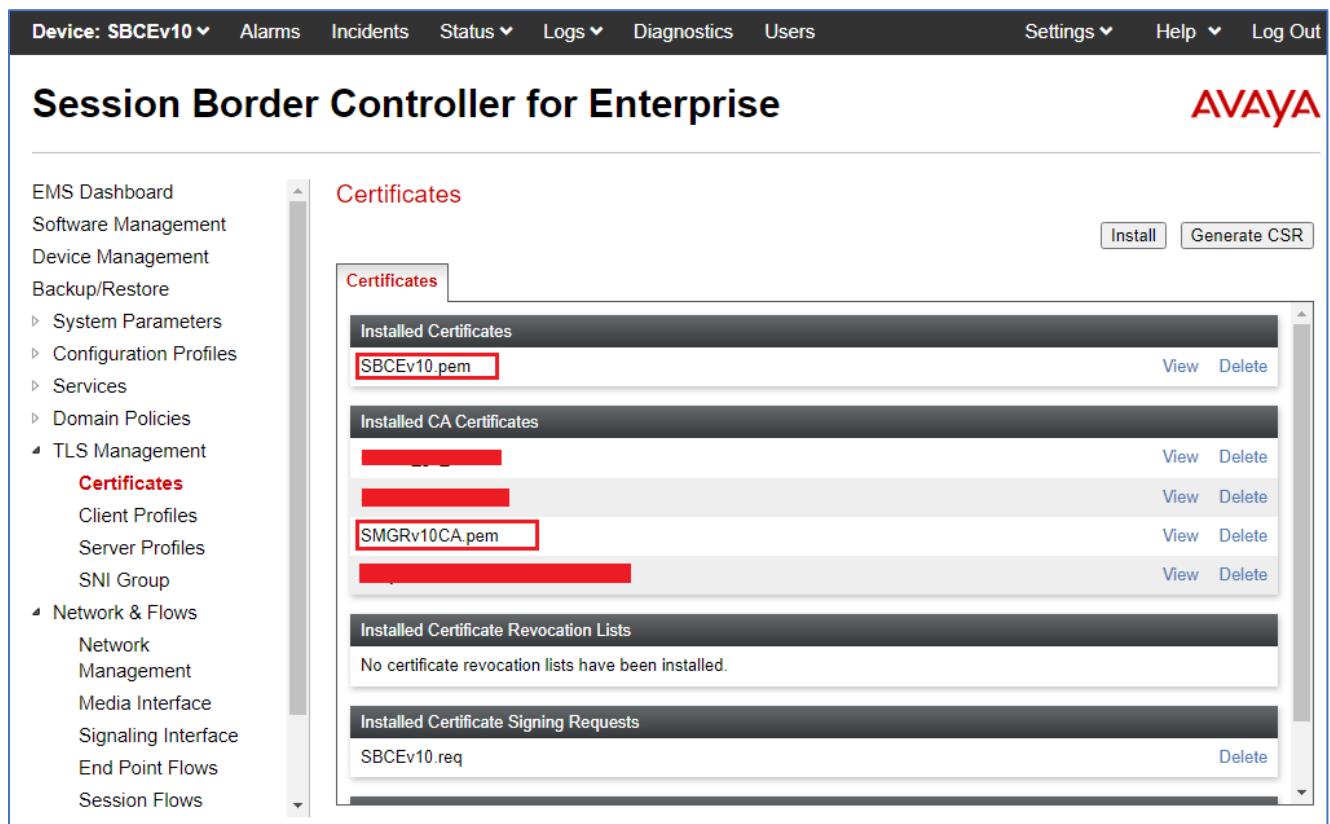
### 7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **SBCEv10** in the sample configuration.



**Step 1 - Select TLS Management → Certificates** from the left-hand menu. Verify the following:

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area (not shown).



### 7.3.2. Server Profiles

**Step 1** - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **SBCEv10.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

**Step 2** - Accept default values for the next screen (not shown) and click **Finish**.

**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	<input type="text" value="Server_TLS"/>
Certificate	<input type="text" value="SBCEv10.pem"/>
SNI Options	<input type="text" value="None"/>
SNI Group	<input type="text" value="None"/>

Certificate Verification	
Peer Verification	<input type="text" value="None"/>
Peer Certificate Authorities	<div><div></div><div></div><div>SMGRv10CA.pem</div><div></div></div>
Peer Certificate Revocation Lists	<div></div>
Verification Depth	<input type="text" value="0"/>

Next

The following screen shows the completed TLS **Server Profile** form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCEv10, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management options, with "Server Profiles" highlighted under the "TLS Management" section. The main content area is titled "Server Profiles: Server\_TLS" and features an "Add" button and a "Delete" button. Below this, a "Server TLS Profile Page" tab is active, showing the "Server Profile" configuration form. The form is divided into three sections: "TLS Profile", "Certificate Verification", and "Renegotiation Parameters".

TLS Profile	
Profile Name	Server_TLS
Certificate	SBCEv10.pem
SNI Options	None

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0



### 7.3.3. Client Profiles

**Step 1** - Select **TLS Management** → **Client Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **SBCEv10.pem**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SMGRv10CA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

**Step 2** - Accept default values for the next screen (not shown) and click **Finish**.

**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	<input type="text" value="Client_TLS"/>
Certificate	<input type="text" value="SBCEv10.pem"/>
SNI	<input type="checkbox"/> Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	<div><div></div><div></div><div>SMGRv10CA.pem</div><div></div></div>
Peer Certificate Revocation Lists	<div></div>
Verification Depth	<input type="text" value="1"/>
Extended Hostname Verification	<input type="checkbox"/>
Server Hostname	<input type="text"/>

Next

The following screen shows the completed TLS **Client Profile** form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCEv10, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo.

On the left, a sidebar menu lists various management options, with 'TLS Management' expanded to show 'Client Profiles'.

The main content area is titled 'Client Profiles: Client\_TLS'. It features an 'Add' button and a 'Delete' button. Below the title, there is a blue bar with the text 'Click here to add a description.'.

The 'Client Profile' form is displayed, showing the following details:

TLS Profile	
Profile Name	Client_TLS
Certificate	SBCEv10.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SMGRv10CA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

## 7.4. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from the **Network & Flows** on the left-side menu. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (**10.33.1.35**) and public (**50.xxx.xxx.109**) sides of the Avaya SBCE are the ones relevant to these Application Notes.

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B1** interfaces. Click the buttons under the **Status** column, if necessary, to enable the interfaces.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: SBCEv10', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar lists various management options, with 'Network Management' highlighted under the 'Network & Flows' section. The main content area is titled 'Network Management' and features two tabs: 'Interfaces' (selected) and 'Networks'. An 'Add VLAN' button is located in the top right of the interface table. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled). Each interface has a corresponding status button in the 'Status' column.

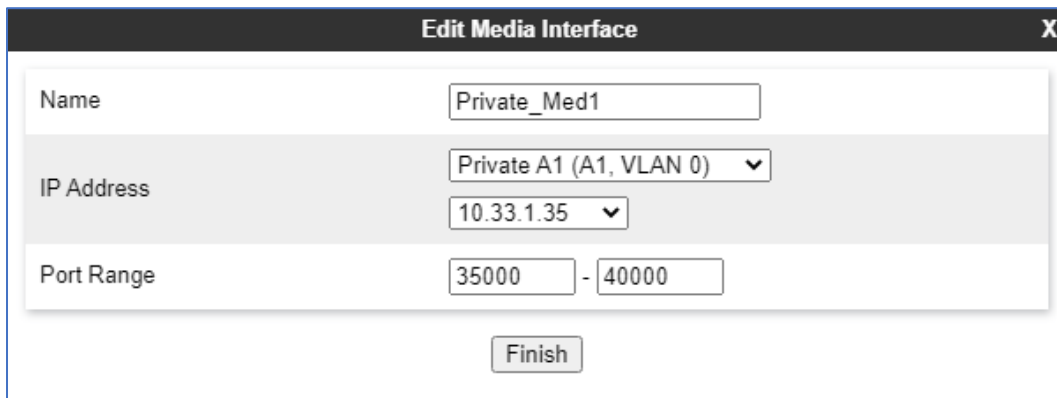
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

## 7.5. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

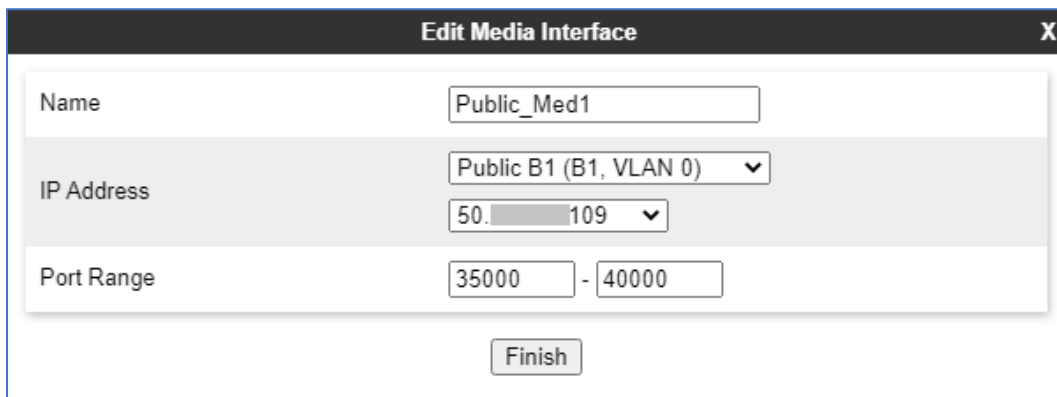


The screenshot shows the 'Edit Media Interface' dialog box with the following fields:

- Name:** Private\_Med1
- IP Address:** Private A1 (A1, VLAN 0) (selected from a dropdown menu)
- IP Address:** 10.33.1.35 (selected from a dropdown menu)
- Port Range:** 35000 - 40000
- Finish** button

A Media Interface facing the public side was similarly created with the name **Public\_Med1**, as shown below.

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.



The screenshot shows the 'Edit Media Interface' dialog box with the following fields:

- Name:** Public\_Med1
- IP Address:** Public B1 (B1, VLAN 0) (selected from a dropdown menu)
- IP Address:** 50.109 (selected from a dropdown menu)
- Port Range:** 35000 - 40000
- Finish** button

## 7.6. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**.
- Select a **TLS Profile** (**Section 7.3.2**).
- Click **Finish**.

The screenshot shows a web-based configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. The fields are as follows:

Field Label	Value / Selection
Name	Private_Sig1
IP Address	Private A1 (A1, VLAN 0) (dropdown) 10.33.1.35 (dropdown)
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	Server_TLS (dropdown)
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

A second Signaling Interface with the name **Public\_Sig1** was similarly created in the service provider's direction.

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5060** for **UDP Port**, since UDP port 5060 is used to listen for signaling traffic from Telnyx in the sample configuration.
- Click **Finish**.

**Edit Signaling Interface** X

Name	Public_Sig1
IP Address	Public B1 (B1, VLAN 0) ▼ 50. 109 ▼
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None ▼
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

## 7.7. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

### 7.7.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Configuration Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select **avaya-ru** from the list of pre-defined profiles. Click **Clone** (not shown).

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The top navigation bar includes 'Device: SBCEv10', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists various configuration options, with 'Configuration Profiles' expanded to show 'Server Interworking'. The main content area is titled 'Interworking Profiles: avaya-ru' and features a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, there are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, displaying a table of settings:

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
Disable Header Support	No

- Enter a descriptive name for the cloned profile.
- Click **Finish**.

The 'Clone Profile' dialog box is shown with the following fields:

- Profile Name:** avaya-ru
- Clone Name:** SM\_Interworking
- Finish** button

Click **Edit** on the newly cloned **Avaya-SM** interworking profile:

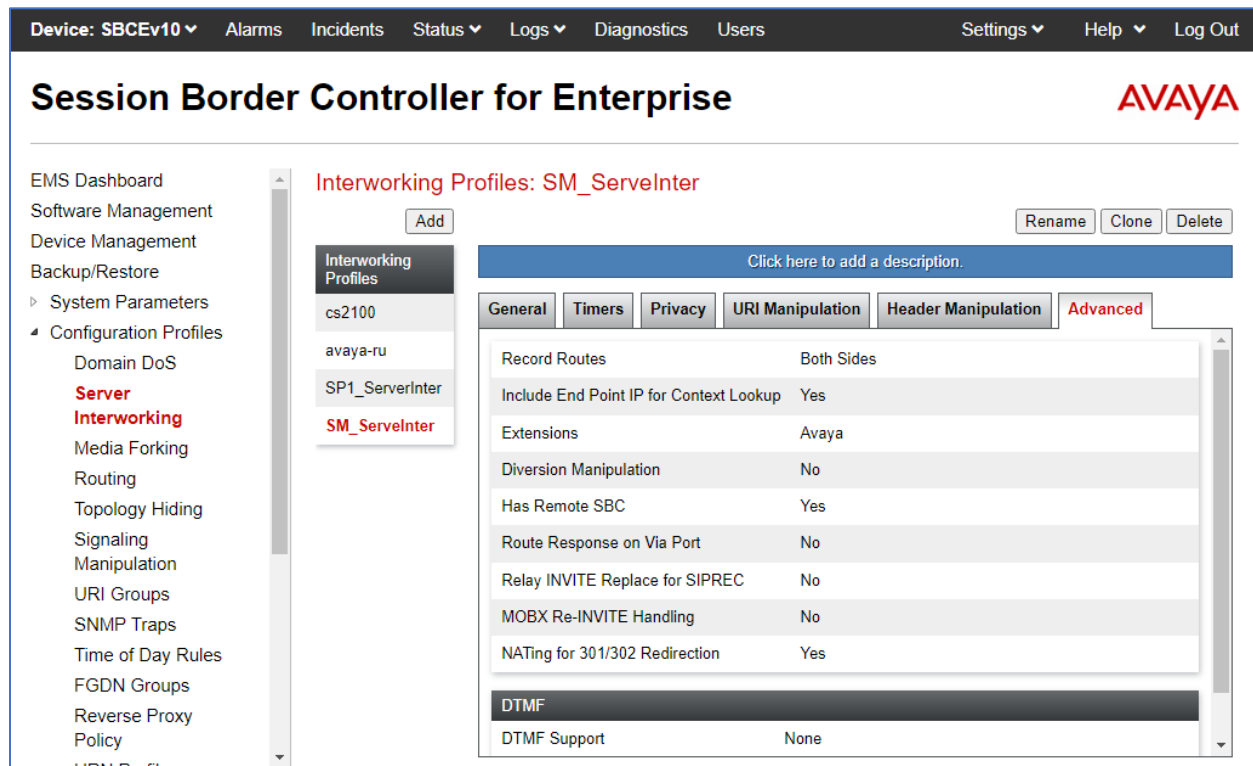
- On the **General** tab, set **T.38 Support** to **Yes** and **SIPS Required** to **No**.
- Leave remaining fields with default values.
- Click **Finish** (not shown).

The **General** tab settings are shown on the screen below:

Editing Profile: SM_ServeInter	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly <input type="radio"/> Microsoft Teams
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
SIPS Required	<input type="checkbox"/>
Mediasec Handling	<input type="checkbox"/>
<input type="button" value="Finish"/>	



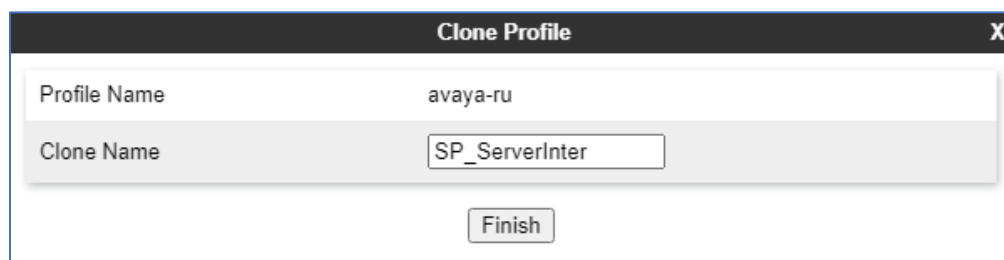
The **Advanced** tab settings are shown on the screen below:



### 7.7.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown).

- Enter a descriptive name for the new profile.
- Click **Next**.
- On the **General** tab, set **SIPS Required** to **No** and set T.38 Support to Yes.



- Click **Next** until the last tab is reached then click **Finish** on the last tab leaving remaining fields with default values (not shown).

The **General** tab settings are shown on the screen below:

Editing Profile: SP1\_ServerInter

X

General

Hold Support

None

RFC2543 - c=0.0.0.0

RFC3264 - a=sendonly

Microsoft Teams

180 Handling

None

SDP

No SDP

181 Handling

None

SDP

No SDP

182 Handling

None

SDP

No SDP

183 Handling

None

SDP

No SDP

Refer Handling

URI Group

None

Send Hold

Delayed Offer

3xx Handling

Diversion Header Support

Delayed SDP Handling

Re-Invite Handling

Prack Handling

Allow 18X SDP

T.38 Support

URI Scheme

SIP

TEL

ANY

Via Header Format

RFC3261

RFC2543

SIPS Required

Mediasec Handling

Finish

The **Advanced** tab settings are shown on the screen below:

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: SBCEv10, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar contains a navigation menu with categories like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, and various protocol-specific settings. The 'Configuration Profiles' section is expanded, showing a list of profiles: cs2100, avaya-ru, SP1\_ServerInter (highlighted), and SM\_ServerInter. The main content area is titled 'Interworking Profiles: SP1\_ServerInter' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a tabbed interface with tabs for General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced (selected). The Advanced tab displays a table of settings:

Setting	Value
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
<b>DTMF</b>	
DTMF Support	None

## 7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and Telnyx SIP Proxy (Trunk Server).

### 7.8.1. Server Configuration Profile – Enterprise

From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

- Enter an appropriate **Profile Name** similar to the screen below.
- 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 'SM10'. Below the input field is a 'Next' button.

- On the **Edit SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **SIP Domain** field, enter the SIP domain name as defined in **Section 6.2**.

- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.6**.
- Select a **TLS Profile** (**Section 7.3.3**).
- Click **Next**.

Edit SIP Server Profile - General
X

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

Server Type
Call Server

SIP Domain
avayalab.com

DNS Query Type
NONE/A

TLS Client Profile
Client\_TLS

Add

IP Address / FQDN	Port	Transport	
10.33.1.42	5061	TLS	Delete

Finish

- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
  - Check **Enable Grooming** (required for TLS transport).
  - Select **SM\_ServerInter** from the **Interworking Profile** drop-down menu (**Section 7.7.1**).
- Click **Finish**.

### 7.8.2. Server Configuration Profile – Service Provider

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below (**SP1** was used).
- Click **Next**.

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop-down menu for the **Server Type**.

- On the **IP Addresses / FQDN** field, enter 192.xxx.xxx.11 (Telnyx SIP proxy IP address). This information was provided by Telnyx.
- Enter **5060** under **Port** and select **UDP** for **Transport**.
- Click **Next**.

**Edit SIP Server Profile - General** X

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

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
192.11	5060	UDP

Delete

Finish

On the **Add SIP Server Profile - Advanced** window:

- Uncheck **Enable Grooming** (not required for UDP transport).
- Select **SP1\_ServerInter** from the **Interworking Profile** drop-down menu (**Section 7.7.2**).
- Click **Finish**.

## 7.9. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the service provider SIP trunk.

### 7.9.1. Routing Profile – Enterprise

To create the inbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select **SM10**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.8.1**.

- Defaults were used for all other parameters.
- Click **Finish**.

Profile : To-SM10 - Edit Rule

URI Group

\*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SM10	10.33.1.42:506	None	Delete

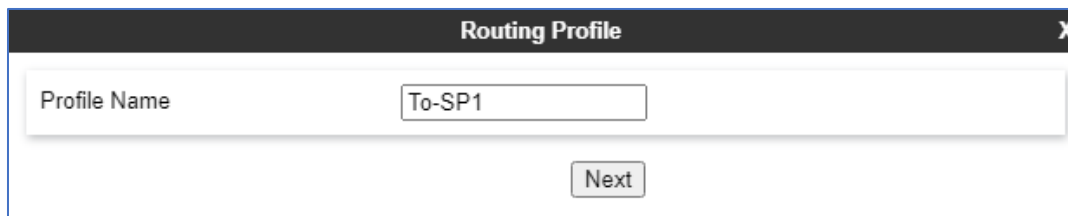
Finish



## 7.9.2. Routing Profile – Service Provider

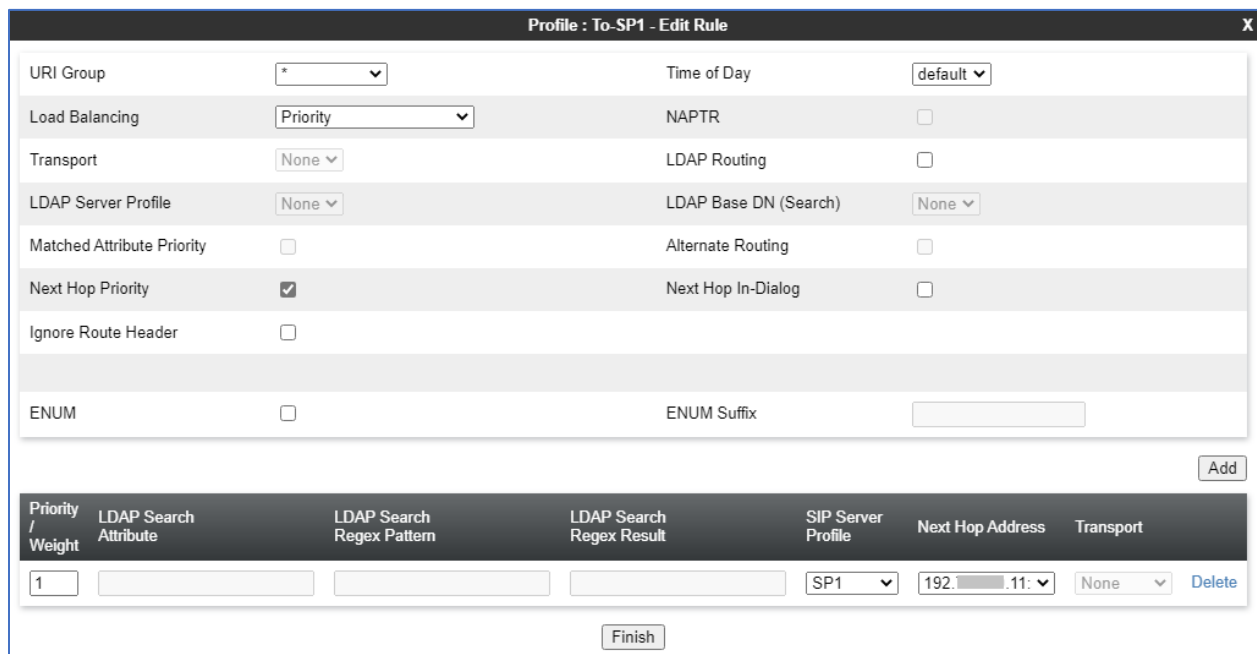
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below (**To-SP1** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Routing 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 "To-SP1". Below this field is a button labeled "Next".

- Under **Load Balancing** select **Priority**.
- Under **SIP Server Profile**, select **SP1**.
- The **Next Hop Address** is populated automatically with **192.xxx.xxx.11:5060 (UDP)**.  
Telnyx SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 7.8.2**.
- Click **Finish**



The screenshot shows a dialog box titled "Profile : To-SP1 - Edit Rule" with a close button (X) in the top right corner. The dialog contains several configuration options:

- URI Group: \*
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- LDAP Routing: ☐
- LDAP Server Profile: None
- LDAP Base DN (Search): None
- Matched Attribute Priority: ☐
- Alternate Routing: ☐
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐
- ENUM: ☐
- ENUM Suffix:

At the bottom right, there is an "Add" button. Below the configuration options is a table with the following columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, Transport, and a Delete button.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	Delete
1				SP1	192.xxx.xxx.11:5060	None	

At the bottom center, there is a "Finish" button.

## 7.10. Topology Hiding

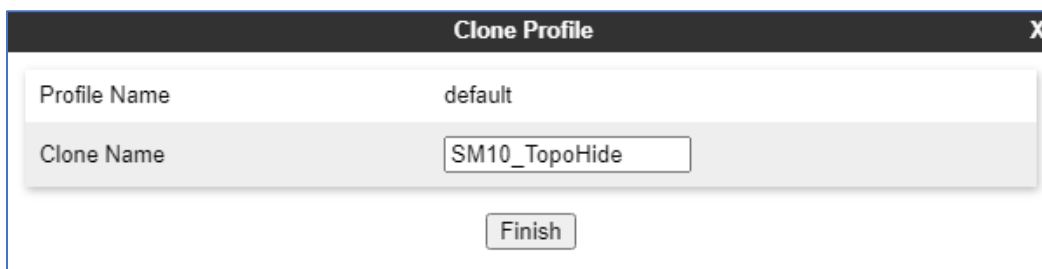
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

### 7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side, select **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The screenshot shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The dialog has two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'SM10\_TopoHide'. A 'Finish' button is located at the bottom center of the dialog.

On the newly cloned **SM10\_TopoHide** profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **avayalab.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**.
- Default values were used for all other fields.
- Click **Finish**.

Edit Topology Hiding Profile

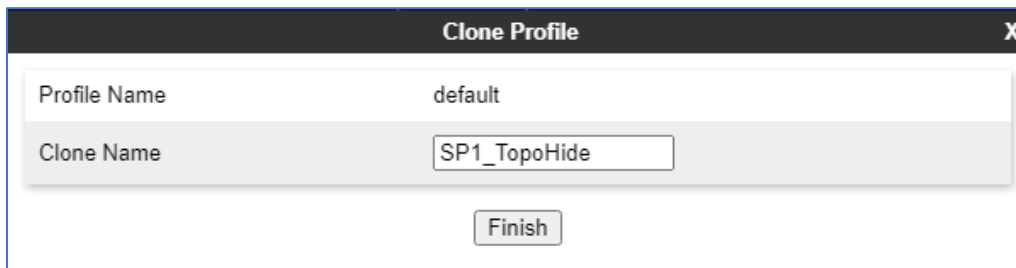
Header	Criteria	Replace Action	Overwrite Value	
Record-Route	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	avayalab.com	Delete
To	IP/Domain	Overwrite	avayalab.com	Delete
Referred-By	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	avayalab.com	Delete
SDP	IP/Domain	Auto		Delete

Finish

### 7.10.2. Topology Hiding Profile – Service Provider

To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

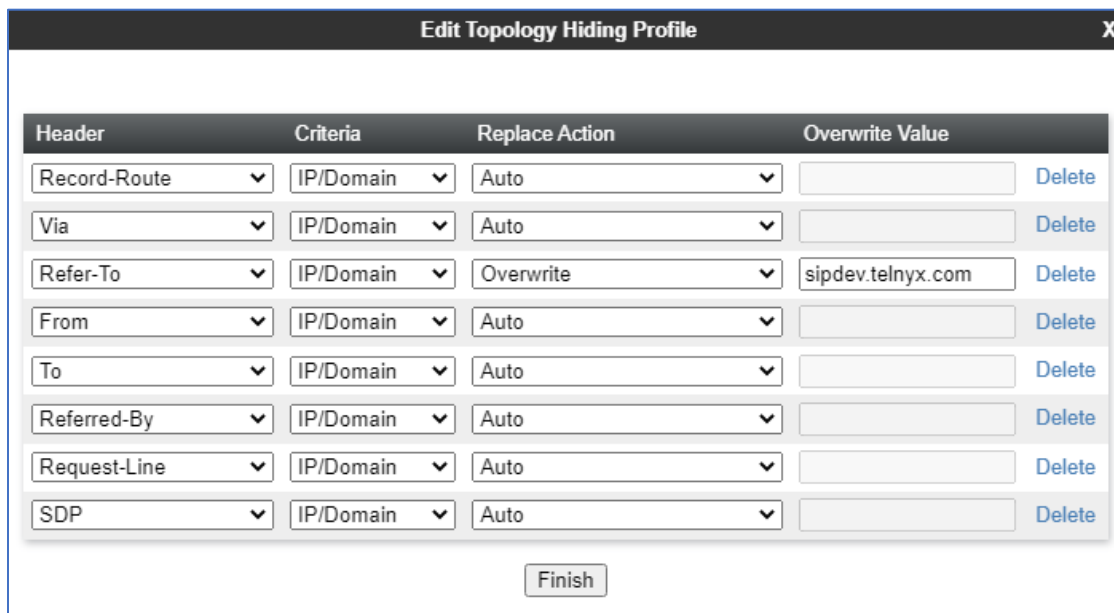
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The 'Clone Profile' dialog box has a title bar with 'Clone Profile' and a close button 'X'. It contains two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'SP1\_TopoHide'. Below these fields is a 'Finish' button.

On the newly cloned **SP1\_TopoHide** profile screen, click the **Edit** button (not shown).

- For the, **Refer-To** header, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **sipdev.telnyx.com**, in the **Overwrite Value** column of the header, as shown below. This is the service provider's domain name (refer **Section 2.2** for detail).
- Default values were used for all other fields.
- Click **Finish**.



The 'Edit Topology Hiding Profile' dialog box has a title bar with 'Edit Topology Hiding Profile' and a close button 'X'. It contains a table with four columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table has eight rows of headers. The 'Refer-To' row has 'Overwrite' selected in the 'Replace Action' column and 'sipdev.telnyx.com' entered in the 'Overwrite Value' column. All other rows have 'Auto' in the 'Replace Action' column and an empty 'Overwrite Value' field. Each row has a 'Delete' button to its right. Below the table is a 'Finish' button.

Header	Criteria	Replace Action	Overwrite Value	
Record-Route	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Overwrite	sipdev.telnyx.com	Delete
From	IP/Domain	Auto		Delete
To	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete

## 7.11. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

### 7.11.1. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, one media rule (shown below) was created toward Session Manager and a default media rule was used toward the Service Provider.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **SM10\_MedRule**.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, selects **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**.
- Under Audio Encryption, **Preferred Format #2**, selects **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption, if needed.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Click **Next**.

Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

Media Encryption
X

### Audio Encryption

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

### Video Encryption

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

### Miscellaneous

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

Finish

- For the compliance test, the **default-low-med** Media Rule was used in the Service Provider direction, shown below.

Media Encryption	
<b>Audio Encryption</b>	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>
<b>Video Encryption</b>	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>
<b>Miscellaneous</b>	
Capability Negotiation	<input checked="" type="checkbox"/>
Finish	

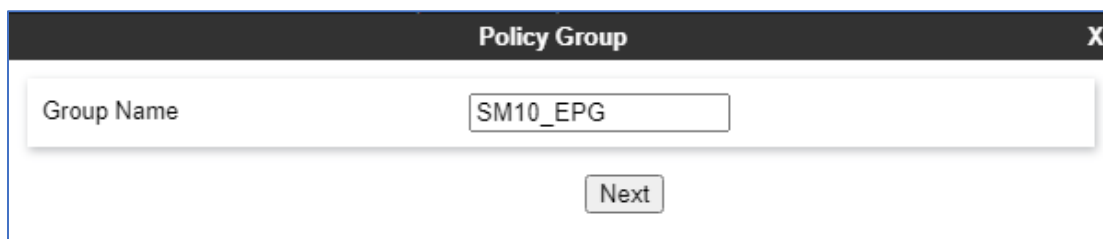
## 7.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

### 7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

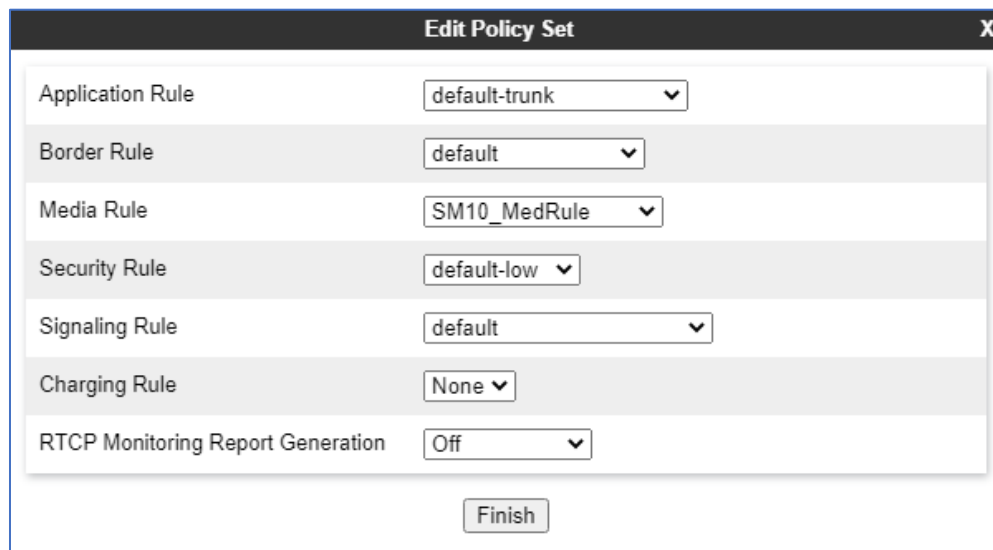
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "SM10\_EPG". Below the input field, there is a button labeled "Next".

Under the **Policy Group** tab enter the following:

- **Application Rule:** select **default-trunk**.
- **Border Rule:** select **default**.
- **Media Rule:** select **SM10\_MedRule** (Section 7.11.1).
- **Security Rule:** select **default-low**.
- **Signaling Rule:** select **default**.
- Click **Finish**.



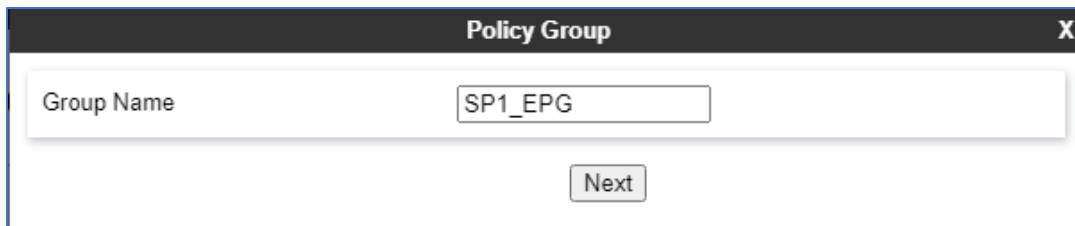
The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a rule name and a dropdown menu. The rules and their selected values are: Application Rule (default-trunk), Border Rule (default), Media Rule (SM10\_MedRule), Security Rule (default-low), Signaling Rule (default), Charging Rule (None), and RTCP Monitoring Report Generation (Off). At the bottom of the dialog, there is a button labeled "Finish".



### 7.12.2. End Point Policy Group – Service Provider

To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

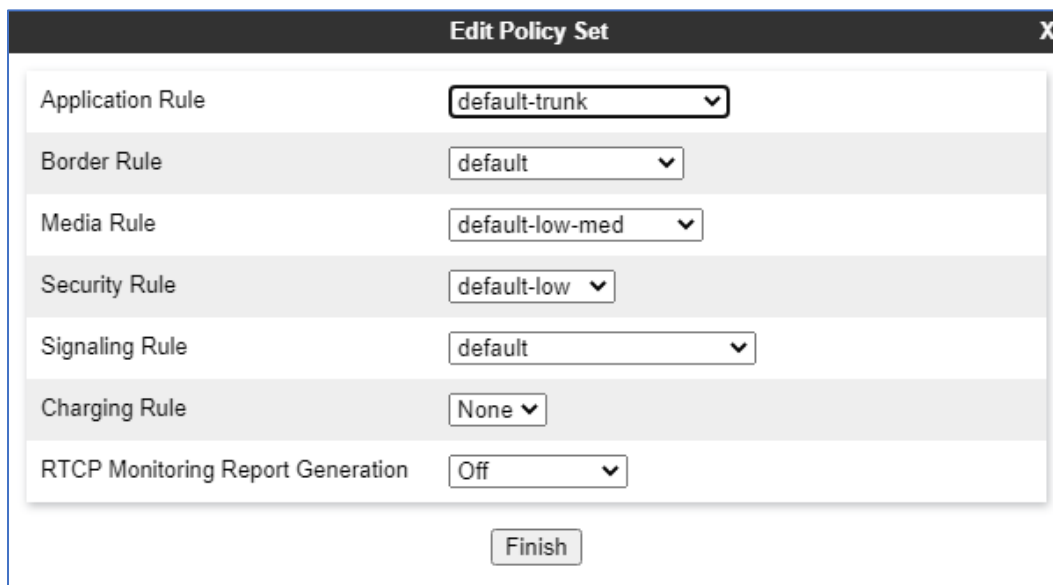
- Enter an appropriate name in the **Group Name** field (**Service Provider** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "SP1\_EPG". Below the input field, there is a button labeled "Next".

Under the **Policy Group** tab enter the following:

- **Application Rule:** select **default-trunk**.
- **Border Rule:** select **default**.
- **Media Rule:** select **default-low-med**.
- **Security Rule:** select **default-low**.
- **Signaling Rule:** select **default**.
- Click **Finish**.



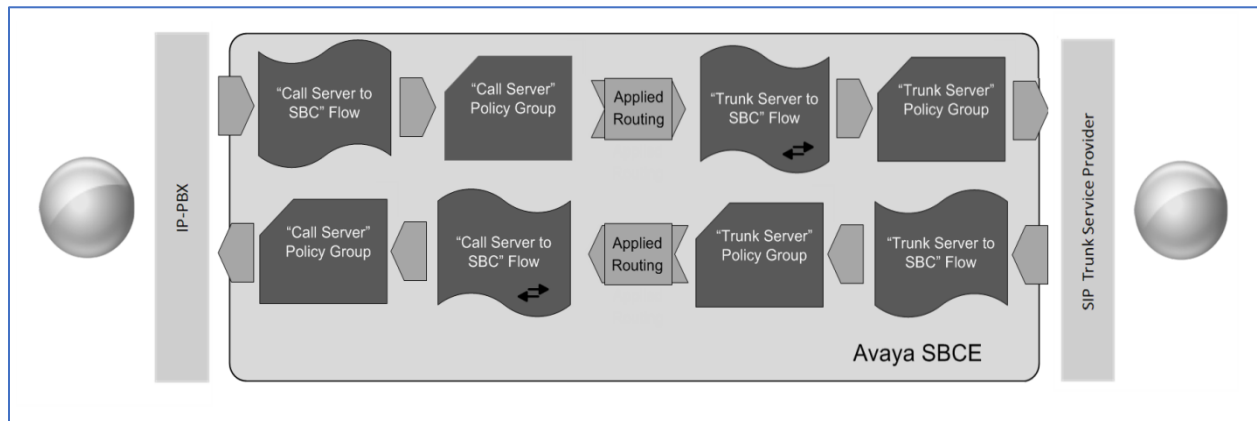
The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a label and a dropdown menu:

Label	Value
Application Rule	default-trunk
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

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

## 7.13. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

### 7.13.1. End Point Flow – Service Provider

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The screen below shows the flow named “**SP1 Flow To SM**” created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: SP1 Flow To SM	
Flow Name	SP1 Flow To SM
SIP Server Profile	SP1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_Sig1
Signaling Interface	Public_Sig1
Media Interface	Public_Med1
Secondary Media Interface	None
End Point Policy Group	SP1_EPG
Routing Profile	To-SM10
Topology Hiding Profile	SP1_TopoHide
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
Finish	

### 7.13.2. End Point Flow – Session Manager

A second Server Flow with the name “**SM Flow To SP1**” was similarly created in the Service Provider direction. To create the call flow toward the Service Provider, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: SM Flow To SP1		X
Flow Name	<input type="text" value="SM Flow To SP1"/>	
SIP Server Profile	<input type="text" value="SM10"/>	
URI Group	<input type="text" value="*/"/>	
Transport	<input type="text" value="*/"/>	
Remote Subnet	<input type="text" value="*/"/>	
Received Interface	<input type="text" value="Public_Sig1"/>	
Signaling Interface	<input type="text" value="Private_Sig1"/>	
Media Interface	<input type="text" value="Private_Med1"/>	
Secondary Media Interface	<input type="text" value="None"/>	
End Point Policy Group	<input type="text" value="SM10_EPG"/>	
Routing Profile	<input type="text" value="To-SP1"/>	
Topology Hiding Profile	<input type="text" value="SM10_TopoHide"/>	
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"/>	
<input type="button" value="Finish"/>		

## 8. Telnyx SIP Trunking Service Configuration

To use Telnyx SIP Trunking Service, a customer must request the service from Telnyx using the established sales processes. The process can be started by contacting Telnyx via the corporate web site at: <https://telnyx.com/>

During the signup process, Telnyx and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Telnyx network.

Telnyx will provide the following information:

- SIP Proxy IP address and SIP domain name of the Telnyx SIP server.
- DID numbers.
- Supported codecs and order of preference.
- Any IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices (firewall).

## 9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of commands that can be used to troubleshoot the solution.

### 9.1. General Verification Steps

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

### 9.2. Communication Manager Verification

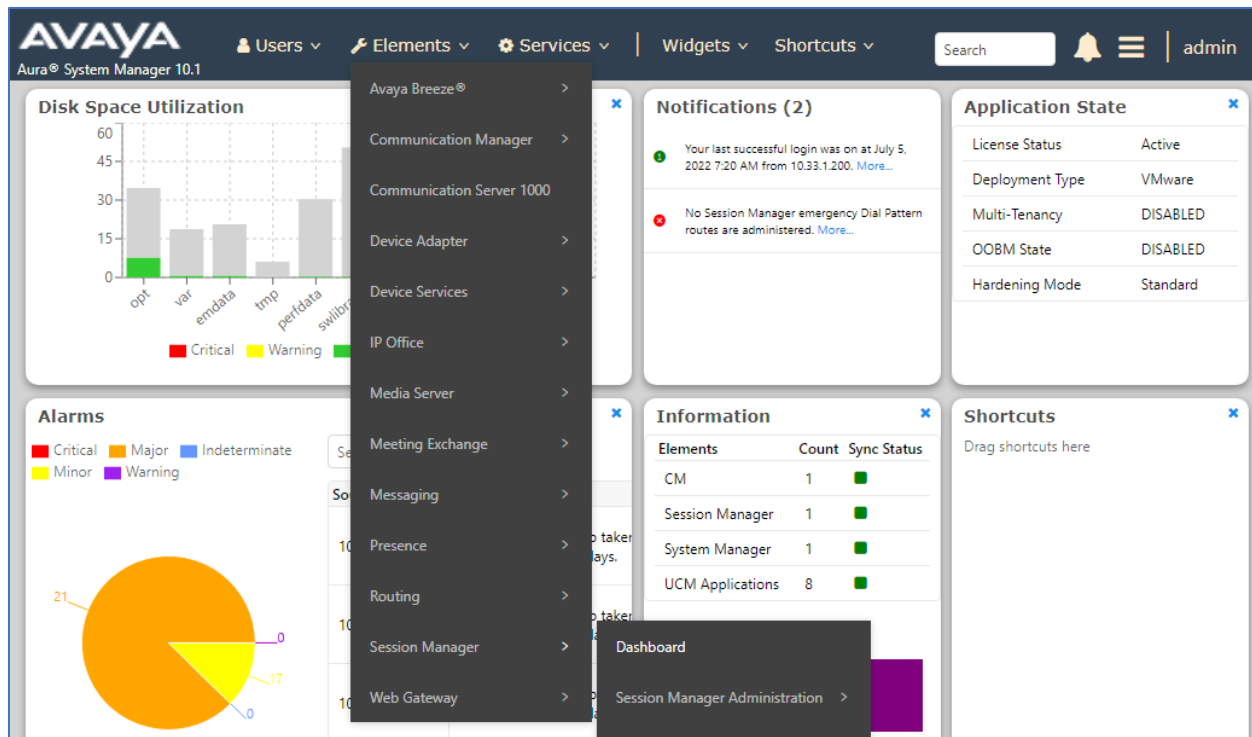
The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **list trace station** <extension number>  
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>  
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>  
Displays signaling group service state.
- **status trunk** <trunk group number>  
Displays trunk group service state.
- **status station** <extension number>  
Displays signaling and media information for an active call on a specific station.

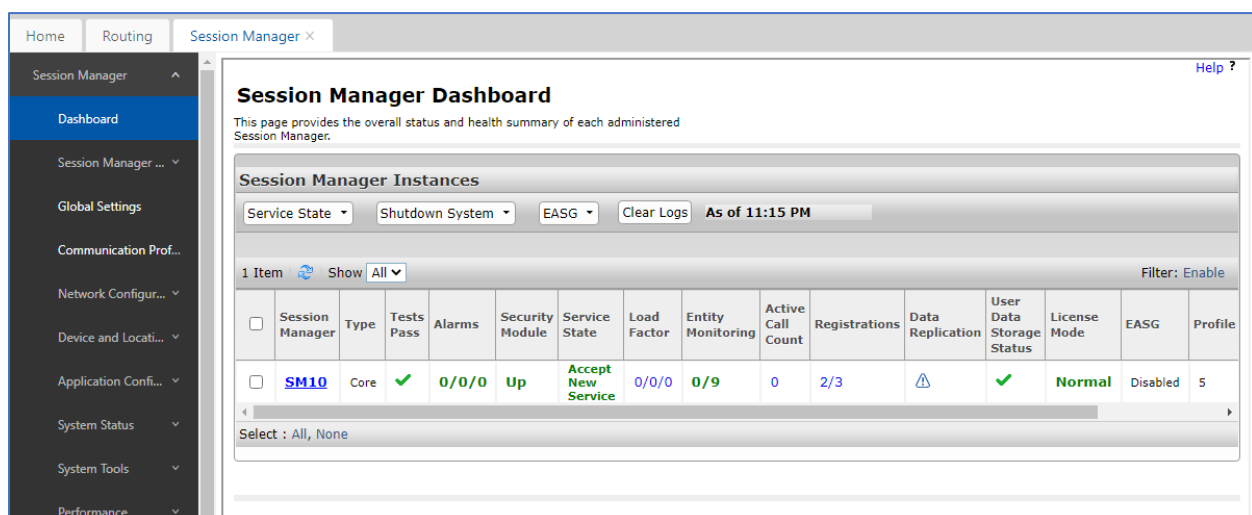
### 9.3. Session Manager Verification

The Session Manager configuration may be verified via System Manager.

**Step 1** - Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**, then select **Dashboard**.



**Step 2** - The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Security Module** and **Service State** columns all show good status.



Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns are **UP**, like shown on the screen below.

**Session Manager Entity Link Connection Status**  
This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

**All Entity Links for Session Manager: SM10**

Summary View

9 Items Filter: Enable

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">Avaya Messaging</a>	IPv4	10.33.1.25	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">Avaya SBCE</a>	IPv4	10.33.1.35	5061	TLS	FALSE	UP	200 Keepalive	UP
<input type="radio"/>	<a href="#">CM10</a>	IPv4	10.33.1.43	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM10-Public</a>	IPv4	10.33.1.43	5067	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">IPQ</a>	IPv4	10.33.1.110	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE8-A1</a>	IPv4	10.33.1.51	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">SBCE8-A2</a>	IPv4	10.33.1.54	5060	TCP	FALSE	UP	403 Forbidden	UP

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** – The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test.



## 9.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

**Alarms:** This screen provides information about the health of the SBC.

Device: EMS ▾ **Alarms** Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller for Enterprise

**EMS Dashboard**

- Software Management
- Device Management
  - System Administration
  - Templates
- Backup/Restore
- Monitoring & Logging

#### Dashboard

Information		
System Time	11:21:59 PM MDT	<a href="#">Refresh</a>
Version	10.1.1.0-35-21872	
GUI Version	10.1.1.0-21872	
Build Date	Mon Apr 18 07:57:04 UTC 2022	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/05/2022 11:31:34 MDT	
Failed Login Attempts	0	

Installed Devices
EMS
SBCEv10

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

[Add](#)

Notes
No notes found.

The following screen shows the **Alarm Viewer** page.

Device: EMS ▾ Help

### Alarm Viewer

**Alarms**

✓ ID	Details	State	Time	Device
No alarms found for this device.				

[Clear Selected](#) [Clear All](#)

**Incidents** : Provides detailed reports of anomalies, errors, policies violations, etc.

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The top navigation bar includes 'Device: EMS', 'Alarms', 'Incidents' (highlighted with a red box), 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo. On the left is the 'EMS Dashboard' menu with options like Software Management, Device Management, System Administration, Templates, Backup/Restore, and Monitoring & Logging. The central 'Dashboard' section contains an 'Information' table with system details, a table for 'Active Alarms (past 24 hours)' showing 'None found.', and a table for 'Incidents (past 24 hours)' also showing 'None found.'. On the right, the 'Installed Devices' section lists 'EMS' and 'SBCEv10'.

Information		
System Time	11:24:02 PM MDT	<a href="#">Refresh</a>
Version	10.1.1.0-35-21872	
GUI Version	10.1.1.0-21872	
Build Date	Mon Apr 18 07:57:04 UTC 2022	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/05/2022 11:31:34 MDT	
Failed Login Attempts	0	

Active Alarms (past 24 hours)	
None found.	

Incidents (past 24 hours)	
None found.	

The following screen shows the Incident Viewer page.

The screenshot shows the 'Incident Viewer' page for device 'SBCEv10'. It features a filter section with 'Category' set to 'All' and buttons for 'Clear Filters', 'Refresh', and 'Generate Report'. Below this is a 'Summary' tab and a table of incidents. The table indicates it is displaying entries 1 to 15 of 2000. The table has columns for ID, Date & Time, Category, Type, and Cause.

ID	Date & Time	Category	Type	Cause
827828947596619	Jun 19, 2022 10:58:15 AM	Media Anomaly Detection	Media Inactivity Detected From Both Parties	Call Audit Cleanup
827462798698553	Jun 10, 2022 11:33:17 PM	Media Anomaly Detection	Media Inactivity Detected From Both Parties	Call Audit Cleanup
827328025886784	Jun 7, 2022 8:40:51 PM	Policy	Message Dropped	No Subscriber Flow Matched
827327931822737	Jun 7, 2022 8:37:43 PM	Protocol Discrepancy	ACK Message Out of Dialog	General Method not allowed Out-Of-Dialog
827327931822187	Jun 7, 2022 8:37:43 PM	Policy	Call Denied	No Subscriber Flow Matched
827327605453450	Jun 7, 2022 8:26:50 PM	Policy	Message Dropped	No Subscriber Flow Matched
827327288588749	Jun 7, 2022 8:16:17 PM	Policy	Call Denied	No Server Flow Matched for Outgoing Message
827327279371774	Jun 7, 2022 8:15:58 PM	Policy	Call Denied	No Server Flow Matched for Outgoing Message
827327055502885	Jun 7, 2022 8:08:31 PM	Policy	Message Dropped	No Subscriber Flow Matched
827326652603200	Jun 7, 2022 7:55:05 PM	Policy	Message Dropped	No Subscriber Flow Matched

**Diagnostics:** This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

The following screen shows the Diagnostics page with the results of a ping test.

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as .pcap files. Navigate to **Monitor & Logging → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The top navigation bar includes 'Device: SBCEv10', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists various management options, with 'Monitoring & Logging' expanded to show 'Trace'. The main content area is titled 'Trace: SBCEv10' and contains a 'Packet Capture' tab. The 'Packet Capture Configuration' form is displayed with the following fields: Status (Ready), Interface (B1), Local Address (All), Remote Address (\*), Protocol (All), Maximum Number of Packets to Capture, and Capture Filename (BasicTestCall.pcap). 'Start Capture' and 'Clear' buttons are at the bottom.

Once the capture is stopped, click the **Captures** tab and select the proper .pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

The screenshot shows the 'Captures' tab in the 'Trace: SBCEv10' section. It displays a table with one captured file. A 'Refresh' button is in the top right corner of the table area.

File Name	File Size (bytes)	Last Modified	
BasicTestCall_20220705233847.pcap	227,255	July 5, 2022 at 11:39:19 PM MDT	Delete

Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBCE.

## 10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1, to connect to the Telnyx SIP Trunking service, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Sections 2.1** and **2.2**.

## 11. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Deploying Avaya Aura® Communication Manager in a Virtualized Environment*, Release 10.1, Issue 3, April 2022.
- [2] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021.
- [3] *Administering Avaya Aura® System Manager* for Release 10.1.x, Issue 5, April 2022.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 10.1.x, Issue 2, March 2022.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 10.1., Issue 2, March 2022.
- [6] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022.
- [7] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*, Release 10.1, Issue 1, December 2021.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, Issue 1, December 2021.
- [9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 10.1.x, Issue 1, April 2022.
- [10] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [11] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

---

**©2022 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).