



Application Notes for Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.0 with G12 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 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.0 to interoperate with G12 SIP Trunking service. These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

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 G12 SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the G12 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	15
5.5.	IP Network Regions	17
5.6.	Signaling Group	18
5.7.	Trunk Group	20
5.8.	Calling Party Information.....	24
5.9.	Inbound Routing.....	25
5.10.	Outbound Routing	26
6.	Configure Avaya Aura® Experience Portal	30
6.1.	Background	30
6.2.	Logging in and Licensing.....	31
6.3.	VoIP Connection	32
6.4.	Speech Servers	35
6.5.	Application References	36
6.6.	MPP Servers and VoIP Settings.....	38
6.7.	Configuring RFC2833 Event Value Offered by Experience Portal	41
7.	Configure Avaya Aura® Session Manager	42
7.1.	System Manager Login and Navigation.....	43
7.2.	SIP Domain	45
7.3.	Locations	45
7.4.	Adaptations.....	48
7.5.	SIP Entities	50
7.6.	Entity Links	53
7.7.	Routing Policies	55
7.8.	Dial Patterns	57
8.	Configure Avaya Session Border Controller for Enterprise	59
8.1.	System Access.....	59
8.2.	Device Management.....	61
8.3.	TLS Management.....	63
8.4.	Network Management	63
8.5.	Media Interfaces.....	65
8.6.	Signaling Interfaces.....	66

8.7.	Server Interworking.....	68
8.7.1.	Server Interworking Profile – Enterprise.....	68
8.7.2.	Server Interworking Profile – Service Provider.....	70
8.8.	Signaling Manipulation.....	72
8.9.	Server Configuration.....	73
8.9.1.	Server Configuration Profile – Enterprise	73
8.9.2.	Server Configuration Profile – Service Provider	75
8.10.	Routing	77
8.10.1.	Routing Profile – Enterprise.....	77
8.10.2.	Routing Profile – Service Provider	78
8.11.	Topology Hiding.....	79
8.11.1.	Topology Hiding Profile – Enterprise	79
8.11.2.	Topology Hiding Profile – Service Provider.....	81
8.12.	Domain Policies.....	82
8.12.1.	Application Rules.....	82
8.12.2.	Media Rules.....	83
8.12.3.	Signaling Rules	86
8.13.	End Point Policy Groups	87
8.13.1.	End Point Policy Group – Enterprise	87
8.13.2.	End Point Policy Group – Service Provider.....	88
8.14.	End Point Flows.....	89
8.14.1.	End Point Flow – Enterprise	90
8.14.2.	End Point Flow – Service Provider	91
9.	G12 SIP Trunking Service Configuration.....	92
10.	Verification and Troubleshooting.....	92
10.1.	General Verification Steps.....	92
10.2.	Communication Manager Verification.....	92
10.3.	Session Manager Verification	93
10.4.	Avaya SBCE Verification	95
11.	Conclusion	100
12.	References.....	100

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the G12 network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 8.1 (Communication Manager), Avaya Aura® Session Manager 8.1 (Session Manager), Avaya Aura® Experience Portal 7.2 (Experience Portal), Avaya Session Border Controller for Enterprise 8.0 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The G12 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 connection through the public Internet 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 “G12” 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.

For the testing associated with this Application Note, the interface between Avaya systems and the G12 SIP Trunking service did not include the use of any specific encryption features. Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible.

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 using IP Address.
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by G12. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 9408 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Equinox softphone (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 Deskphones (SIP).
- Outgoing calls to the PSTN were routed via G12 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 codec G.711MU.
- No matching codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- 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.
- T.38 and G711 pass through fax calls.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold).
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agents and extensions.
- Call and two-way talk path establishment between callers and Communication Manager agents and extensions following redirection from Experience Portal.
- 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.

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 [11] in the **References** section for additional information on this topic.

Items that are supported and that were not tested includes the following:

- Inbound toll free calls were not tested.
- 0, 0+10 digits, 911 Emergency and international calls were not tested.
- SIP NCR using SIP 302 Re-direction message. (Redirect before answer) was not supported.

2.2. Test Results

Interoperability testing of the G12 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:

- **OPTIONS** – G12 does not send OPTIONS messages to the Avaya enterprise network, but it does respond to OPTIONS messages it receives from the Avaya enterprise. This was enough to maintain the SIP trunk link 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-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector, AV-Global-Session-ID and P-Location (Refer to **Section 7.4**). To help reduce the packet size further, the Avaya SBCE can remove the “*gsid*” and “*epv*” parameters that may be included within the Contact header by applying a Sigma script to the G12 server configuration. Refer to **Section 8.8** and **13**.
- **Network call redirection** – Call transfer, call forward and EC500 off-net calling. G12 supports both SIP Re-INVITE and SIP REFER methods for the network call redirection but the SIP REFER method was used for the testing, due to the SIP Re-INVITE method had a no audio issue with the call redirection and EC500 off-net calling. This is a known issue and it is being investigated by the Avaya SBCE team.

2.3. Support

For support of G12 SIP Trunking Service visit the corporate Web page at:

<https://www.g12com.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 G12 SIP Trunking Service through the public Internet.

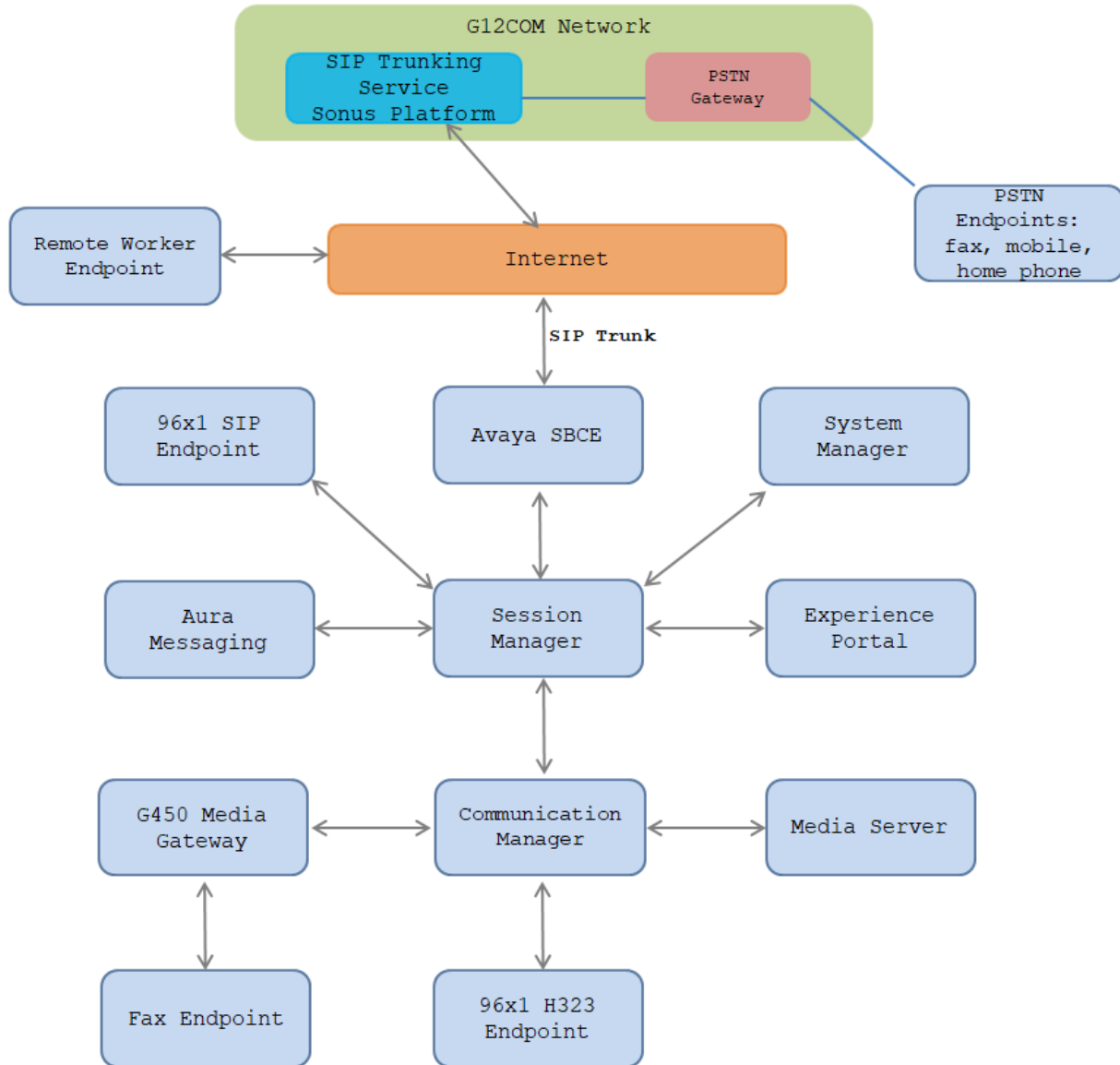


Figure 1: Avaya SIP Enterprise Solution connected to G12 SIP Trunking Service

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 Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya Aura® Experience Portal.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Equinox™ for Windows softphone (SIP).
- Avaya digital and analog telephones.

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 96x1 SIP Deskphones. For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on Avaya 96x1 SIP Deskphones used to test remote worker functionality. 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 [11] 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 or Experience Portal) 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 G12 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.

As part of the Avaya Aura® version 8.0 release, 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.

Avaya Aura® 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 Messaging are not directly related to the interoperability tests with the G12 network SIP Trunking service, they are not included in these Application Notes.

Avaya Aura® Experience Portal was also used during the compliance test to verify various SIP call flow scenarios with G12 SIP trunking service.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	8.1.0.1.1 (01.0.890.0-25517)
Avaya Aura® Session Manager	8.1.0.0 (8.1.0.0.810007)
Avaya Aura® System Manager	8.1.0.0 Build No. 8.1.0.0.733078 Software Update Rev. No. 8.1.0.0.079880
Avaya Session Border Controller for Enterprise	ASBCE 8.0 8.0.0.0-19-16991
Avaya Aura® Messaging	7.1 Service Pack 1 (MSG-01.0.532.0-0100)
Avaya Aura® Media Server	8.0.1.121_2019.04.29
Avaya G430 Media Gateway	g430_sw_41_9_0
Avaya Aura® Experience Portal	7.2.2.0.2118
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.5.0.11
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.8202
Avaya one-X® Communicator (H.323, SIP)	6.2.14.1-SP14
Avaya Equinox for Windows (SIP)	3.5.7.30.1
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
G12 SIP Trunking	
Sonus SBC	Version 6.2

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.

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 6.0.0) 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 G12 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 **68** 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	20
Maximum Concurrently Registered IP Stations:		18000	7
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	1
Maximum Video Capable IP Softphones:		18000	14
Maximum Administered SIP Trunks:		40000	68
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 (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
  CPN/ANI/ICLID Replacement for Restricted Calls: Restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: Unavailable

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 (**interopASM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip interopASM                                     Page 1 of 2
```

IP NODE NAMES	
Name	IP Address
interopASM	10.33.1.12
interopASMB	10.33.1.22
loopback	10.33.1.6
lsp	10.33.1.7
procr	10.33.1.6
procr6	::

(7 of 17 administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

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 2 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. G12 supports audio codecs **G.711MU**. The codec G.729 was selected as the second codec but was not used during the testing.

change ip-codec-set 3

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 3

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1:	G.711MU	n	2	20
2:	G.729	n	2	20
3:				
4:				
5:				
6:				
7:				

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1:	1-srtp-aescm128-hmac80
2:	10-srtp-aescm256-hmac80
3:	none
4:	
5:	

On **Page 2**, set the **Fax Mode** to either **T.38-Standard** or **pass-through**. G12 supports both.

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-	Packet
		dancy	Size (ms)
FAX	pass-through	0	
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			

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 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwdev.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: bvwdev.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											
7											
8											
9											
10											
11											
12											
13											
14											
15											

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 *interopASM*. 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 *bvwdev.com*.
- 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*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- 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	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y			
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n			
Alert Incoming SIP Crisis Calls? n			
Near-end Node Name: procr		Far-end Node Name: interopASM	
Near-end Listen Port: 5067		Far-end Listen Port: 5067	
		Far-end Network Region: 3	
Far-end Domain:bvwdev.com			
		Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3		IP Audio Hairpinning? n	
Enable Layer 3 Test? y		Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n		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 2 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: y	
Group Name: OUTSIDE CALL	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 *private*. This field specifies the format of the calling party number (CPN) sent to the far-end.
- 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: none	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private	UI Treatment: service-provider
	Replace Restricted Numbers? y	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? 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 (Refer to **Section 2.2** for issues related to Experience Portal).
- Set the **Send Diversion Header** field to **y** and **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101**, the value preferred by G12.
- 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	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
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 private-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, three 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 private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
4	33	1		4	Total Administered: 14
4	34	1		4	Maximum Entries: 540
4	3301	3	2068098323	10	
4	3401	3	2068098325	10	
4	3312	3	2068098327	10	

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 G12 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/ Feature	Number Len	Number Digits	Del Insert				
public-ntwrk	10	2068098323	10	3301			
public-ntwrk	10	2068098325	10	3406			
public-ntwrk	10	2068098327	10	4800			

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							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 5		
	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0		3	fac	35	4	udp	*	3	dac
1		4	ext	4	4	aar	#	3	dac
1		11	udp	43	4	aar			
13		5	aar	44	4	udp			
14		5	aar	45	4	aar			
20		3	aar	46	4	aar			
23		5	aar	50	4	aar			
24		5	aar	52	4	udp			
25		4	aar	54	4	udp			
28		5	aar	546	5	aar			
30		4	aar	56	5	udp			
33		4	ext	60	5	udp			
33		5	aar	608	10	udp			
34		4	ext	8	1	fac			
34		5	aar	9	1	fac			

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

change feature-access-codes	Page 1 of 11
FEATURE ACCESS CODE (FAC)	
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: 8	
Auto Route Selection (ARS) - Access Code 1: 9	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 3, which contains the SIP trunk group to the service provider.

To make international call from the U.S. (e.g., dialing: 9011 + country code + number):

change ars analysis 01							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	
01	9	17	deny	iop		n	
011	10	18	3	intl		n	
1	11	14	3	pubu		n	
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	

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 **unk-unk**. All calls using this route pattern will use the private 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				unk-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® Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [9] in the **References** section for further details if necessary.

6.1. Background

Experience Portal consists of one or more Media Processing Platform (MPP) servers and an Experience Portal Manager (EPM) server. A single “server configuration” was used in the reference configuration. This consisted of a single MPP and EPM, running on a VMware environment, including an Apache Tomcat Application Server (hosting the Voice XML (VXML) and/or Call Control XML (CCXML) application scripts), that provide the directives to Experience Portal for handling the inbound calls.

References to the Voice XML and/or Call Control XML applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party DID number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match is found, Experience Portal informs the caller that the call cannot be handled and disconnects the call¹.

For the sample configuration described in these Application Notes, a simple VXML test application was used to exercise various SIP call flow scenarios with G12 SIP Trunking service. In production, enterprises can develop their own VXML and/or CCXML applications to meet specific customer self-service needs or consult Avaya Professional Services and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes.

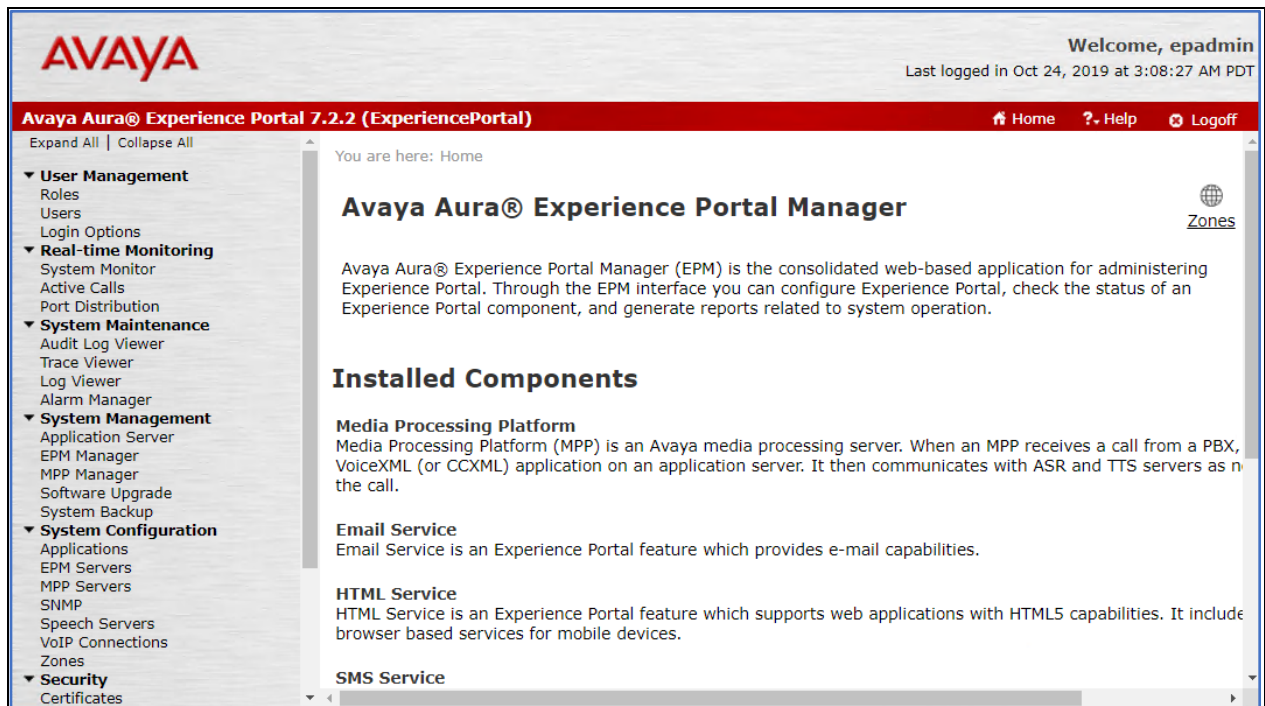
¹ An application may be configured with “inbound default” as the called number, to process all inbound calls that do not match any other application references.

6.2. Logging in and Licensing

This section describes the steps on Experience Portal for administering a SIP connection to the Session Manager.

Step 1 - Launch a web browser, enter `http://<IP address of the Avaya EPM server>/` in the URL, log in with the appropriate credentials and the following screen is displayed.

Note – All page navigation described in the following sections will utilize the menu shown on the left pane of the screenshot below.



Step 2 - In the left pane, navigate to **Security**→**Licensing**. On the **Licensing** page, verify that Experience Portal is properly licensed. If required licenses are not enabled, contact an authorized Avaya account representative to obtain the licenses.

AVAYA Welcome, epadmin
Last logged in Oct 24, 2019 at 3:08:27 AM PDT

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal) Home ? Help Logoff

You are here: [Home](#) > [Security](#) > [Licensing](#)

Licensing

This page displays the Experience Portal license information that is currently in effect. Experience Portal uses Avaya License Manager (WebLM) to control the number of telephony ports that are used.

License Server Information

License Server URL:	https://10.33.1.10:52233/WebLM/LicenseServer
Last Updated:	Jul 26, 2019 4:11:07 AM PDT
Last Successful Poll:	Oct 26, 2019 3:08:41 PM PDT

Licensed Products

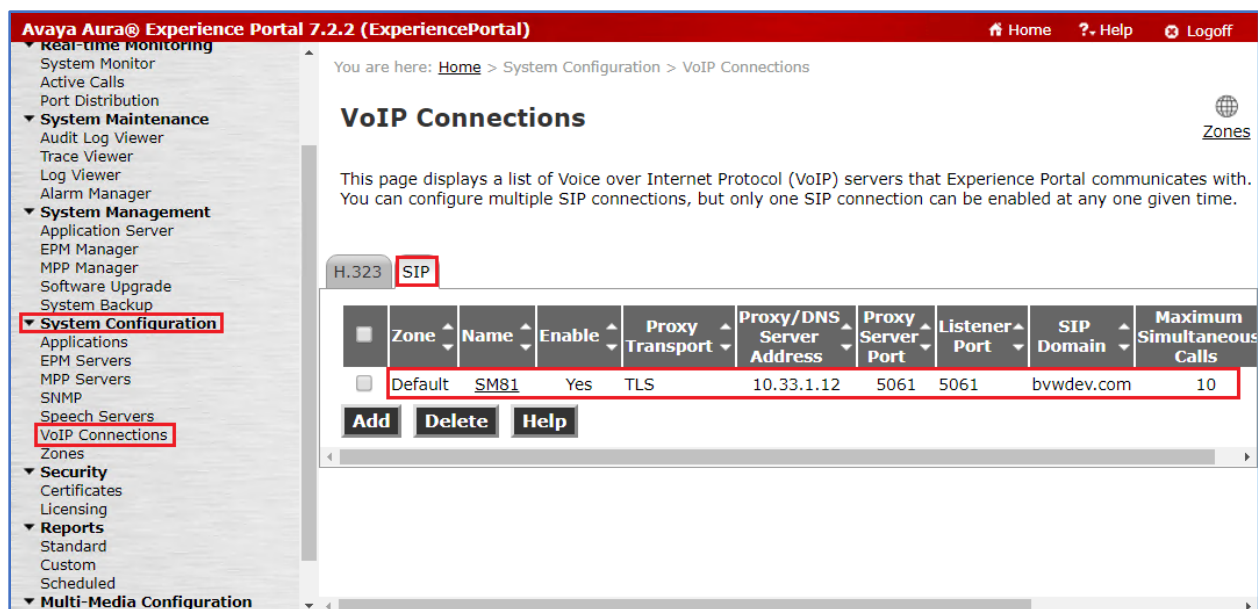
Experience Portal	
Announcement Ports:	100
ASR Connections:	250
Email Units:	50
Enable Media Encryption:	250
Enhanced Call Classification:	250
Google ASR Connections:	10
HTML Units:	100
SIP Signaling Connections:	100
SMS Units:	100

6.3. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager (**Sections 7.5 and 7.6**).

Step 1 - In the left pane, navigate to **System Configuration**→**VoIP Connections**. On the **VoIP Connections** page, select the **SIP** tab and click **Add** to add a SIP trunk.

Note – Only *one* SIP trunk can be active at any given time on Experience Portal.



Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **EP_SIP**).
- **Enable** – Set to **Yes**. mnvv
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
 - **Proxy Server Address** = **10.33.1.12** (the IP address of the Session Manager signaling interface defined in **Section 7.5**).
 - **Port** = **5061**
 - **Priority** = **0** (default)
 - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **bvwddev.com** (see **Section 7.2**).
- **Consultative Transfer** – Select **REFER**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **100** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES_CM_128**
- **Authentication Algorithm** = **HMAC_SHA1_80**
- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- Click on **Add** to add SRTP settings to the **Configured SRTP List**
- Use default values for all other fields.
- Click **Save**.

You are here: [Home](#) > [System Configuration](#) > [VoIP Connections](#) > [Change SIP Connection](#)

Change SIP Connection

Use this page to change the configuration of a SIP connection.

Zone:

Name:

Enable: ☒ Yes ☐ No

Proxy Transport:

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
<input type="text" value="10.33.1.12"/>	<input type="text" value="5061"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Remove

[Additional Proxy Server](#)

Listener Port:

SIP Domain:

P-Asserted-Identity:

Maximum Redirection Attempts:

Consultative Transfer: ☐ INVITE with REPLACES ☒ REFER

SIP Reject Response Code: ☒ ASM (503) ☐ SES (480) ☐ Custom

SIP Timers

T1: milliseconds

T2: milliseconds

B and F: milliseconds

Call Capacity

Maximum Simultaneous Calls:

- ☒ All Calls can be either inbound or outbound
☐ Configure number of inbound and outbound calls allowed

SRTP

Enable: ☒ Yes ☐ No

Encryption Algorithm: ☒ AES_CM_128 ☐ NONE

Authentication Algorithm: ☒ HMAC_SHA1_80 ☐ HMAC_SHA1_32

RTCP Encryption Enabled: ☐ Yes ☒ No

RTP Authentication Enabled: ☒ Yes ☐ No

Add

Configured SRTP List

SRTP-Yes,AES_CM_128,HMAC_SHA1_80,RTCP Encryption-No,RTP Authentication-Yes

Rem

6.4. Speech Servers

The installation and administration of the ASR and TSR Speech Servers are beyond the scope of this document. Some of the values shown below were defined during the Speech Server installations. Note that in the reference configuration the ASR and TTS servers used the same IP address.

ASR speech server:

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)

You are here: [Home](#) > System Configuration > Speech Servers

Speech Servers

This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.

ASR **TTS**

	Zone	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
<input type="checkbox"/>	Default	Nuance	Yes	10.33.1.61	Nuance	MRCP V2 TCP	5060	4	English(USA) en-US

Add **Delete** **Customize** **Help**

TTS speech server:

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)

You are here: [Home](#) > System Configuration > Speech Servers

Speech Servers

This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.

ASR **TTS**

	Zone	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed TTS Resources	Voices
<input type="checkbox"/>	Default	Nuance	Yes	10.33.1.61	Nuance	MRCP V2 TCP	5060	4	English(USA) en-US Allison F, English(USA) en-US Ava F, English(USA) en-US Nathan M, English(USA) en-US Zoe F

Add **Delete** **Customize** **Help**

6.5. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.33.1.3.

Step 1 - In the left pane, navigate to **System Configuration→Applications**. On the **Applications** page (not shown), click **Add** to add an application and configure as follows:

- **Name** – Set to a descriptive name (e.g., **Test2_APP**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type.
- **VoiceXML** and/or **CCXML URL** – Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Experience Portal test application on a single server is referenced.
- **Speech Servers ASR** and **TTS** – Select the appropriate ASR and/or TTS servers as necessary.
- **Application Launch** – Set to **Inbound**.
- **Called Number** – Enter the number to match against an inbound SIP INVITE message and click **Add**. In the sample configuration illustrated in these Application Notes, the local number 4800 was used. Repeat to define additional called party numbers as needed. Inbound calls with these called party numbers will be handled by the application defined in this section.

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of an application.

Zone: Default
Name: Test_VoiceXML
Enable: ☒ Yes ☐ No
Type:
Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum
Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL:

Mutual Certificate Authentication: ☒ Yes ☐ No

Basic Authentication: ☐ Yes ☒ No

ASR Speech Servers

Engine Types	Selected Engine Types
ASR: <input type="text" value="<None>"/>	Nuance

Nuance

Languages	Selected Languages
<input type="text" value="<None>"/>	English(USA) en-US

Resources:

N Best List Length:

Speech Complete Timeout: milliseconds

Speech Incomplete Timeout: milliseconds

Vendor Parameters:

TTS Speech Servers

Voices	Selected Voices
TTS: <input type="text" value="Nuance"/> English(USA) en-US Ava F English(USA) en-US Nathan M English(USA) en-US Zoe F	English(USA) en-US Allison F

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number:

Add

4800

Remove

Speech Parameters

Reporting Parameters

Advanced Parameters

Save

Apply

Cancel

Help

6.6. MPP Servers and VoIP Settings

This section illustrates the procedure for viewing or changing the MPP Settings. In the sample configuration, the MPP Server is co-resident on a single server with the Experience Portal Management server (EPM).

Step 1 - In the left pane, navigate to **System Configuration**→**MPP Servers** and the following screen is displayed. Click **Add**.

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)

You are here: [Home](#) > [System Configuration](#) > [MPP Servers](#)

MPP Servers

This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, it invokes a VoiceXML application on an application server and communicates with ASR and TTS servers as necessary to process the call.

	Zone	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Ca
<input type="checkbox"/>	Default	aep72	10.33.1.3	<Default>	<Default>	<Default>	15

Add **Delete**

MPP Settings **Browser Settings** **Video Settings** **VoIP Settings** **Help**

Step 2 - Enter any descriptive name in the **Name** field (e.g., **aep72**) and the IP address of the MPP server in the **Host Address** field and click **Continue** (not shown). Note that the Host Address used is the same IP address assigned to Experience Portal.

Step 3 - The certificate page will open. Check the **Trust this certificate** box (not shown). Once complete, click **Save**.

You are here: [Home](#) > System Configuration > [MPP Servers](#) > Change MPP Server

Change MPP Server

Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels to Finest if your Experience Portal system has heavy call traffic. The system might experience performance issues if Trace Levels are set to Finest. Set Trace Levels to Finest only when you are troubleshooting the system.

Zone: Default
Name: aep72
Host Address: 10.33.1.3
Network Address (VoIP): <Default>
Network Address (MRCP): <Default>
Network Address (AppSvr): <Default>
Maximum Simultaneous Calls: 15
Restart Automatically: ☒ Yes ☐ No

MPP Certificate

```
Owner: C=US,O=AVAYA,OU=SDP,CN=aep72
Issuer: O=AVAYA,OU=MGMT,CN=SystemManager CA
Serial Number: 352dbbbde22c8aa8
Signature Algorithm: SHA256withRSA
Valid from: June 28, 2019 4:38:19 AM PDT until September 26, 2022 4:38:19 AM PDT
Certificate Fingerprints
MD5: f1:f8:92:8d:de:20:c0:df:df:66:7d:a1:cf:fa:7a:8a
SHA: 07:10:e8:86:15:3d:07:28:09:c1:24:71:de:f0:bb:3a:4e:c6:5b:74
SHA-256: f7:f0:92:25:18:eb:9c:65:58:7e:95:53:27:e9:4b:37:25:63:d7:18:22:6e:5e:4d:59:d8:5e:28:1a:4b:b2:bd
Subject Alternative Names
DNS Name: aep72
DNS Name: aep72.bvwddev.com
IP Address: 10.33.1.3
```

Categories and Trace Levels ▶

Save **Apply** **Cancel** **Help**

Step 4 - Click **VoIP Settings** tab on the screen displayed in **Step 1**.

- In the Port Ranges section, default ports were used.
- In the Codecs section set:
 - Set **Packet Time** to **20**.
 - Verify Codecs **G729**, **G711uLaw** and **G711aLaw** are enabled (check marks). Set the **Offer** and Answer **Order** as shown. In the sample configuration **G729** is the preferred codec, with **Order 1**, followed by **G711uLaw** with **Order 2** and **G711aLaw** with **Order 3**.
 - On the codec Offer set **G729 Discontinuous Transmission** to **No** (for G.729A).
- Use default values for all other fields.

Step 5 - Click on **Save** (not shown).

You are here: [Home](#) > [System Configuration](#) > [MPP Servers](#) > [VoIP Settings](#)

VoIP Settings

Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.

Port Ranges ▾

	Low	High
UDP:	<input type="text" value="11000"/>	<input type="text" value="30999"/>
TCP:	<input type="text" value="31000"/>	<input type="text" value="33499"/>
MRCP:	<input type="text" value="34000"/>	<input type="text" value="36499"/>
H.323 Station:	<input type="text" value="37000"/>	<input type="text" value="39499"/>

RTCP Monitor Settings ▾

Host Address:

Port:

VoIP Audio Formats ▾

MPP Native Format:

Codecs ▾

Offer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G711uLaw	<input type="text" value="1"/>
<input checked="" type="checkbox"/>	G711aLaw	<input type="text" value="2"/>
<input checked="" type="checkbox"/>	G729	<input type="text" value="3"/>

Packet Time: milliseconds

G729 Discontinuous Transmission: ☐ Yes ☒ No

Answer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G711uLaw	<input type="text" value="1"/>
<input checked="" type="checkbox"/>	G711aLaw	<input type="text" value="2"/>
<input checked="" type="checkbox"/>	G729	<input type="text" value="3"/>

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☒ Yes ☐ No

QoS Parameters ▸

Out of Service Threshold (% of VoIP Resources) ▸

Call Progress ▸

Miscellaneous ▸

6.7. Configuring RFC2833 Event Value Offered by Experience Portal

The configuration change example noted in this section was not required for any of the call flows illustrated in these Application Notes. For incoming calls from G12 to Experience Portal, G12 specifies the value 101 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Experience Portal answers, the SDP from Experience Portal matches this G12 offered value.

When Experience Portal sends an INVITE with SDP as part of an INVITE-based transfer (e.g., bridged transfer), Experience Portal offers the SDP. By default, Experience Portal specifies the value 127 for the RFC2833 telephone-events. Optionally, the value that is offered by Experience Portal can be changed, and this section outlines the procedure that can be performed by an Avaya authorized representative.

- Access Experience Portal via the command line interface.
- Navigate to the following directory: /opt/Avaya/ExperiencePortal/MPP/config
- Edit the file mppconfig.xml.
- Search for the parameter “mpp.sip.rfc2833.payload”. If there is no such parameter specified add a line such as the following to the file, where the value 101 is the value to be used for the RFC2833 events. If the parameter is already specified in the file, simply edit the value assigned to the parameter.
<parameter name="mpp.sip.rfc2833.payload">101</parameter>
- In the verification of these Application Notes, the line was added directly above the line where the sip.session.expires parameter is configured.

After saving the file with the change, restart the MPP server for the change to take effect. As shown below, the MPP may be restarted using the **Restart** button available via the Experience Portal GUI at **System Management → MPP Manager**.

Note that the **State** column shows when the MPP is running after the restart.

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (Oct 27, 2019 2:49:27 AM PDT)

This page displays the current state of each MPP in the Experience Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: Oct 27, 2019 2:49:20 AM PDT

Zone	Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
						Today	Recurring	In	Out
<input type="checkbox"/>	Default aep72	Online	Running	Restart needed	Yes	No	None	0	0

State Commands

Mode Commands

Restart/Reboot Options

☒ One server at a time
☐ All servers

7. Configure Avaya Aura® Session Manager

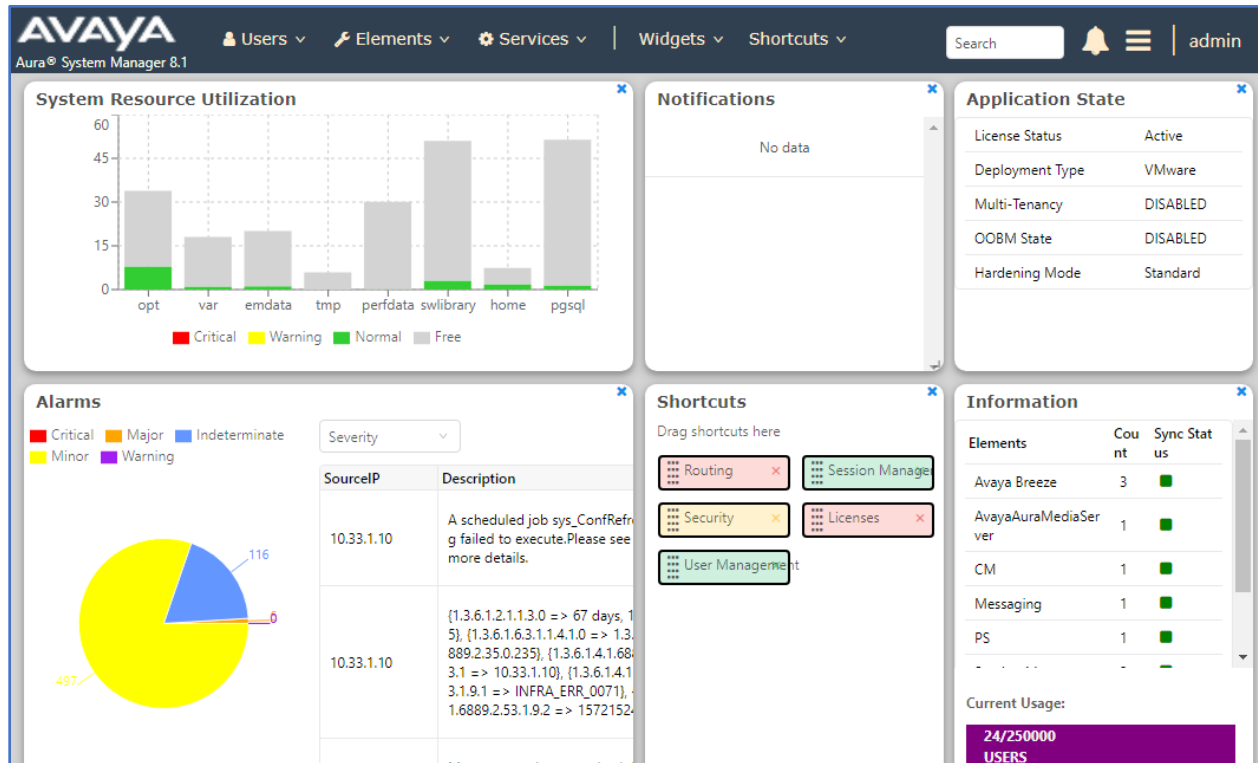
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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, Experience Portal 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.

7.1. 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 shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, version information, and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile (admin) are also present. The left navigation pane is expanded to the 'Routing' section, which is highlighted with a red box. The 'Routing' section contains a list of items: Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Domains' item is selected. The main content area displays the 'Domain Management' page, which includes a table with 2 items. The table has columns for Name, Type, and Notes. The items are 'bvwddev.com' (SIP Domain) and 'presence.bvwddev.com' (presence domain). The table also includes a 'Filter: Enable' button and a 'Select: All, None' option.

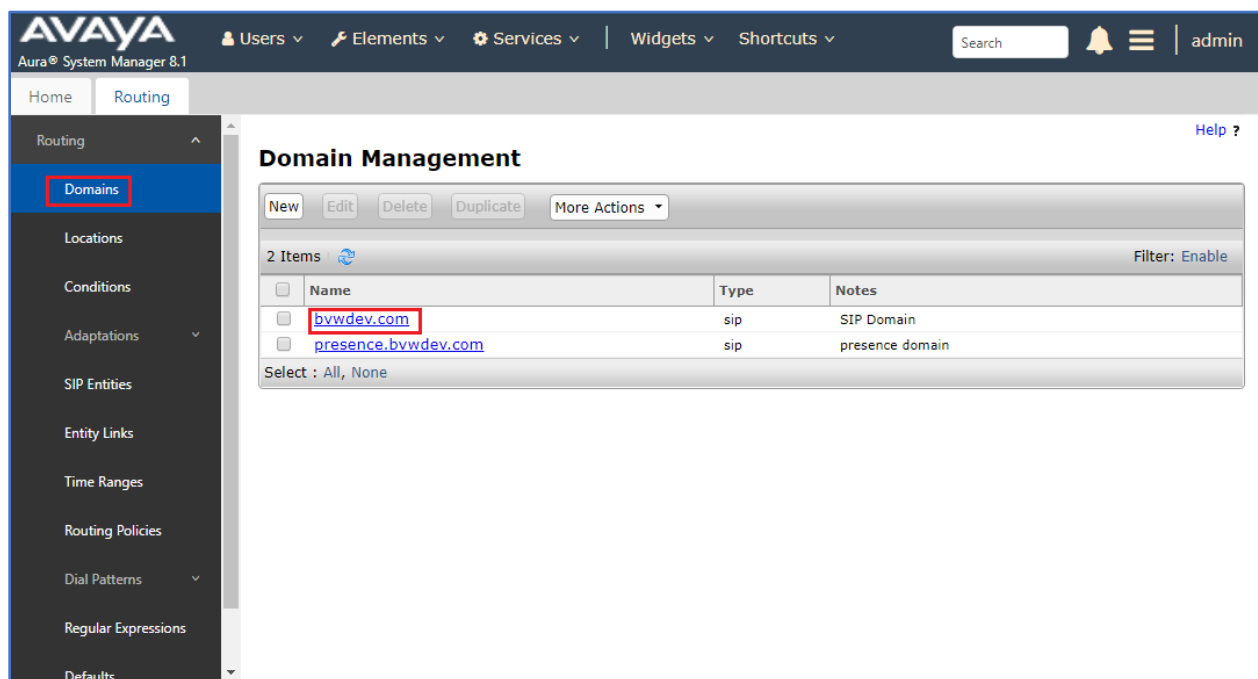
Name	Type	Notes
bvwddev.com	sip	SIP Domain
presence.bvwddev.com	sip	presence domain

7.2. 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, **avaya.lab.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.

The screen below shows the entry for the enterprise domain.



7.3. 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 **InteropASM**. 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 8.1 interface. The left sidebar shows the 'Locations' menu item highlighted. The main content area is titled 'Location Details' and contains the following fields:

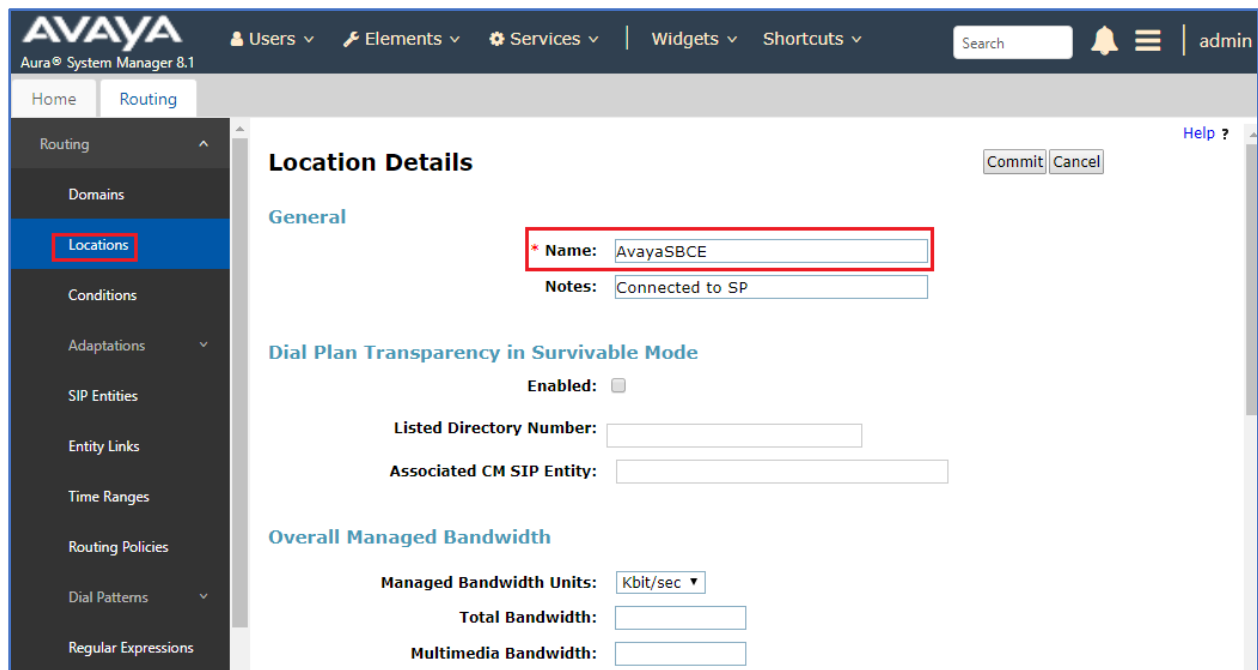
- General**
 - Name:** InteropASM (highlighted with a red box)
 - Notes:** Session Manager
- Dial Plan Transparency in Survivable Mode**
 - Enabled:** ☐
 - Listed Directory Number:**
 - Associated CM SIP Entity:**
- Overall Managed Bandwidth**
 - Managed Bandwidth Units:** Kbit/sec
 - Total Bandwidth:**
 - Multimedia Bandwidth:**
 - Audio Calls Can Take Multimedia Bandwidth:** ☒

The following screen shows the location details for the location named **InteropCM**. 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 displays the Avaya Aura System Manager 8.1 interface. The left sidebar shows the 'Locations' menu item highlighted. The main content area is titled 'Location Details' and contains the following fields:

- General**
 - Name:** InteropCM (highlighted with a red box)
 - Notes:** Communication Manager
- Dial Plan Transparency in Survivable Mode**
 - Enabled:** ☐
 - Listed Directory Number:**
 - Associated CM SIP Entity:**
- Overall Managed Bandwidth**
 - Managed Bandwidth Units:** Kbit/sec
 - Total Bandwidth:**
 - Multimedia Bandwidth:**
 - Audio Calls Can Take Multimedia Bandwidth:** ☒

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

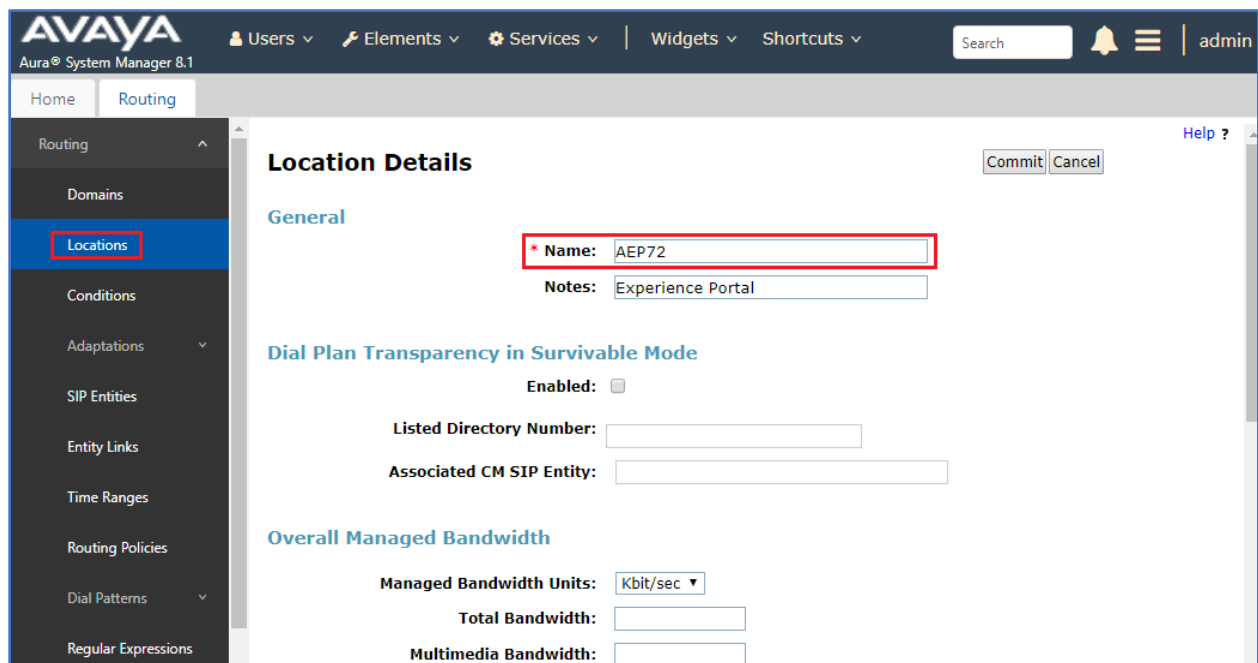


The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar has a menu with 'Locations' highlighted. The main content area is titled 'Location Details' and contains the following sections:

- General**: The 'Name' field is set to 'AvayaSBCE' and is highlighted with a red box. The 'Notes' field contains 'Connected to SP'.
- Dial Plan Transparency in Survivable Mode**: The 'Enabled' checkbox is unchecked. The 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty.
- Overall Managed Bandwidth**: The 'Managed Bandwidth Units' dropdown is set to 'Kbit/sec'. The 'Total Bandwidth' and 'Multimedia Bandwidth' fields are empty.

Buttons for 'Commit' and 'Cancel' are located in the top right corner of the form area.

The following screen shows the location details for the location named **AEP72**. Later, this location will be assigned to the SIP Entity corresponding to the Experience Portal. Other location parameters (not shown) retained the default values.



The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar has a menu with 'Locations' highlighted. The main content area is titled 'Location Details' and contains the following sections:

- General**: The 'Name' field is set to 'AEP72' and is highlighted with a red box. The 'Notes' field contains 'Experience Portal'.
- Dial Plan Transparency in Survivable Mode**: The 'Enabled' checkbox is unchecked. The 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty.
- Overall Managed Bandwidth**: The 'Managed Bandwidth Units' dropdown is set to 'Kbit/sec'. The 'Total Bandwidth' and 'Multimedia Bandwidth' fields are empty.

Buttons for 'Commit' and 'Cancel' are located in the top right corner of the form area.

7.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 8.1 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 ***HeadersRemoval*** was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location. 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 8.1

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

Home Routing

Routing
Domains
Locations
Conditions
Adaptations
Adaptations
Regular Expressi...
SIP Entities
Entity Links
Time Ranges

Adaptation Details

Commit Cancel Help ?

General

* Adaptation Name: HeadersRemoval

* Module Name: DigitConversionAdapter ▾

Module Parameter Type: Name-Value Parameter ▾

	Name	Value
<input type="checkbox"/>	eRHdrs	"Endpoint-View, P-Charging-Vector, P-Location, Alert-Info, Max-Breadth, P-AV-Message-Id, Accept-Language"

Select : All, None

Egress URI Parameters:

Notes: To be applied in other destinationSIP e

7.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager, Avaya SBCE and Experience Portal. 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, *SIP Trunk* (or *Other*) for the Avaya SBCE and *Voice Portal* for the Experience Portal.
- **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 7.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

The following screen shows the addition of the *ASM70A* 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 8.1 interface. The left navigation pane shows the 'SIP Entities' menu item selected. The main content area is titled 'SIP Entity Details' and includes a 'General' section. The 'General' section contains the following fields:

- Name:** ASM70A
- IP Address:** 10.33.1.12
- SIP FQDN:**
- Type:** Session Manager
- Notes:**
- Location:** InteroASM
- Outbound Proxy:**
- Time Zone:** America/Denver
- Minimum TLS Version:** Use Global Setting
- Credential name:**

The 'Monitoring' section at the bottom contains the following fields:

- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

The following screen shows the addition of the **ACM-Trunk3-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**. Select the location that applies to the SIP Entity being created, defined in **Section 7.3**. Select the **Time Zone**.

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 (see **Figure 1**).
- On the **Adaptation** field, the adaptation module **HeadersRemoval** previously defined in **Section 7.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- Select the **Time Zone**.

AVAYA
Aura® System Manager 8.1

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

Home Session Manager **Routing**

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

SIP Entity Details Commit Cancel [Help ?](#)

General

* Name: SBCE-A1

* FQDN or IP Address: 10.33.1.54

Type: SIP Trunk ▾

Notes:

Adaptation: HeadersRemoval ▾

Location: AvayaSBCE ▾

Time Zone: America/Denver ▾

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

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: egress ▾

The following screen shows the addition of the **AEP72** SIP Entity:

- The **FQDN or IP Address** field is set to the IP address of the Experience Portal (see **Figure 1**).
- Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- Select the **Time Zone**.

AVAYA
Aura® System Manager 8.1

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

Home **Routing**

Routing
Domains
Locations
Conditions
Adaptations ▾
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns ▾

SIP Entity Details Commit Cancel [Help ?](#)

General

* Name: AEP72

* FQDN or IP Address: 10.33.1.3

Type: Voice Portal ▾

Notes: AEP System 10.33.1.3

Adaptation: ▾

Location: AEP72 ▾

Time Zone: America/Denver ▾

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

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

7.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Three Entity Links were created; an entity link to Communication Manager for use only by service provider traffic, an entity link to the Avaya SBCE and an entity link to Experience Portal. To add an Entity Link, navigate to **Routing** → **Entity Links** 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 7.5**).
- **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 7.5**).
- **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.

Entity Links

Commit Cancel

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connect Policy
<input type="checkbox"/>	* ASM70A-ACM-Trunk3-5067	* Q ASM70A	TLS	* 5067	* Q ACM-Trunk3-Public	* 5067	<input type="checkbox"/>	trusted

Select : All, None

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 navigation tabs: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are on the right. Below the tabs, the page title 'Entity Links' is displayed with 'Commit' and 'Cancel' buttons. A 'Filter: Enable' button is on the right. The main table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Conn Po. A single item is listed with a red border around the row: Name is '*ASM70A_ASBC-A1_5061', SIP Entity 1 is '*QASM70A', Protocol is 'TLS', Port is '*5061', SIP Entity 2 is '*QASBCE-A1', Port is '*5061', DNS Override is unchecked, and Conn Po is 'truste'. Below the table, there is a 'Select: All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Conn Po
*ASM70A_ASBC-A1_5061	*QASM70A	TLS	*5061	*QASBCE-A1	*5061	<input type="checkbox"/>	truste

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

The screenshot shows the 'Entity Links' configuration page. At the top, there are navigation tabs: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are on the right. Below the tabs, the page title 'Entity Links' is displayed with 'Commit' and 'Cancel' buttons. A 'Filter: Enable' button is on the right. The main table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Conn Po. A single item is listed with a red border around the row: Name is '*SM70A_AEP71_5061_TLS', SIP Entity 1 is '*QASM70A', Protocol is 'TLS', Port is '*5061', SIP Entity 2 is '*QAEP72', Port is '*5061', DNS Override is unchecked, and Conn Po is 'truste'. Below the table, there is a 'Select: All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Conn Po
*SM70A_AEP71_5061_TLS	*QASM70A	TLS	*5061	*QAEP72	*5061	<input type="checkbox"/>	truste

7.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 7.5**. Three routing policies were added; an incoming policy with Communication Manager as the destination, an outbound policy with the Avaya SBCE as the destination and an incoming policy with Experience Portal 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 7.5**) 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 screen shows the Routing Policy for Communication Manager:

The screenshot displays the Avaya Aura System Manager 8.1 interface. The left navigation pane shows 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Name:** To-CM-Trunk3 (highlighted with a red box)
- Disabled:** ☐
- * Retries:** 0
- Notes:** Public SIP Trunk

The 'SIP Entity as Destination' section features a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
ACM-Trunk3-Public (highlighted with a red box)	10.33.1.6 (highlighted with a red box)	CM	Public SIP Trunk

The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows 1 item with the following details:

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

At the bottom, it says 'Select : All, None'.

The following screen shows the Routing Policies for the Avaya SBCE.

The screenshot displays the 'Routing Policy Details' page in the Avaya Aura System Manager 8.1 interface. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields:

- Name:** To-SBCE-A1 (highlighted with a red box)
- Disabled:** ☐
- Retries:** 0
- Notes:** (empty text box)

The 'SIP Entity as Destination' section features a 'Select' dropdown and a table with the following data:

Name	FQDN or IP Address	Type	Notes
SBCE-A1	10.33.1.54	SIP Trunk	

The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below these is a table with 1 item, filtered by 'Filter: Enable'.

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

The following screen shows the Routing Policies for Experience Portal.

The screenshot displays the 'Routing Policy Details' page in the Avaya Aura System Manager 8.1 interface, specifically for the 'To-AEP72' policy. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields:

- Name:** To-AEP72 (highlighted with a red box)
- Disabled:** ☐
- Retries:** 0
- Notes:** Route to EP 10.33.1.3

The 'SIP Entity as Destination' section features a 'Select' dropdown and a table with the following data:

Name	FQDN or IP Address	Type	Notes
AEP72	10.33.1.3	Voice Portal	AEP System 10.33.1.3

The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below these is a table with 1 item, filtered by 'Filter: Enable'.

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

At the bottom, there is a 'Select : All, None' option.

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. Also, a dial pattern was created to route calls from service provider to Experience Portal. 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:

- **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 7.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 7.7**). Click **Select** (not shown).
- Click **Commit** to save.

AVAYA
Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | Help ? | admin

Home Routing

- Routing
 - Domains
 - Locations
 - Conditions
 - Adaptations
 - SIP Entities
 - Entity Links
 - Time Ranges
 - Routing Policies**
 - Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-CM-Trunk3	0	<input type="checkbox"/>	ACM-Trunk3-Public	Public SIP Trunk

Select : All, None

AVAYA

Aura® System Manager 8.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Session Manager

Avaya Breeze®

Routing

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Dial Patterns

Origination Dial...

Regular Expressions

Defaults

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern:

1

* Min:

10

* Max:

14

Emergency Call:

☐

SIP Domain:

bvwdev.com

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-SBCE-A1	0	<input type="checkbox"/>	SBCE-A1	

Select : All, None

Aura® System Manager 8.1

- Users ▾
- Elements ▾
- Services ▾
- | Widgets ▾
- Shortcuts ▾

 Search 🔔 📑 admin

Home | Routing

Adaptations ▾

 SIP Entities

 Entity Links

 Time Ranges

 Routing Policies

 Dial Patterns ▲

Dial Pattern Details

[Help ?](#)

Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

								Filter: Enable
<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes	
<input checked="" type="checkbox"/>	-ALL-	To-AEP72		0	<input type="checkbox"/>	AEP72	Route to EP 10.33.1.3	

Select : All, None

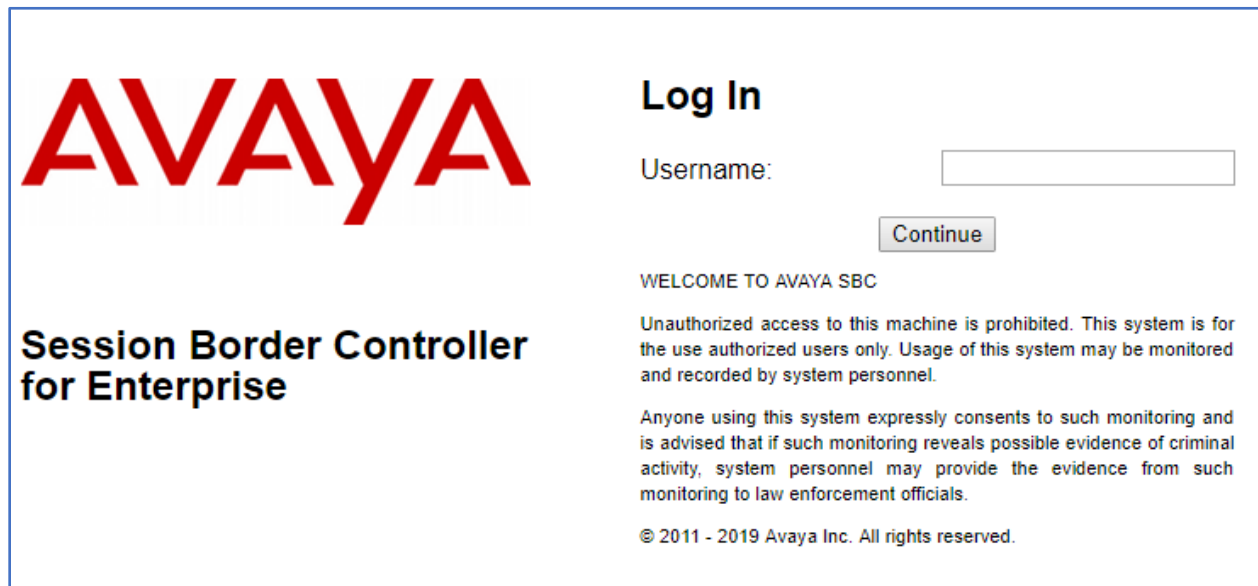
8. Configure Avaya Session Border Controller for Enterprise

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.

Note - The configuration tasks required to support TLS transport for signaling and SRTP for media are beyond the scope of these Application Notes; hence it's not discussed in detail in this document. Consult reference [8] in the **References** section for additional information on this topic.

8.1. 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 screenshot shows the login interface 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, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a warning about unauthorized access, a consent statement, and a copyright notice: "© 2011 - 2019 Avaya Inc. All rights reserved."

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **SBCE100** in the sample configuration.

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

EMS
SBCE100

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

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

Dashboard

Information	
System Time	12:23:37 AM MDT Refresh
Version	8.0.0.0-19-16991
Build Date	Sat Jan 26 21:58:11 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	10/28/2019 00:10:58 MDT
Failed Login Attempts	0

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS
SBCE100

Incidents (past 24 hours)

SBCE100: Ucid is not enabled. Dropping the Invite request towards recorder

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: SBCE100 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging

Dashboard

Information	
System Time	12:24:58 AM MDT Refresh
Version	8.0.0.0-19-16991
Build Date	Sat Jan 26 21:58:11 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	10/28/2019 00:10:58 MDT
Failed Login Attempts	0

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS
SBCE100

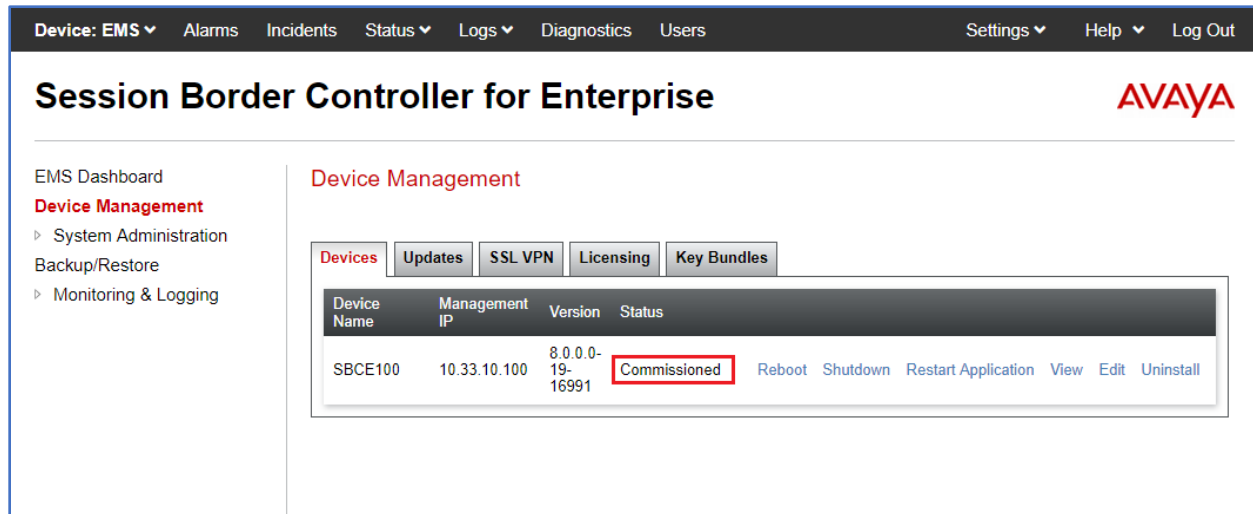
Incidents (past 24 hours)

SBCE100: Ucid is not enabled. Dropping the Invite request towards recorder

SBCE100: Ucid is not enabled. Dropping the Invite request towards recorder

8.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **SBCE100** 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.



The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: EMS, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main heading is "Session Border Controller for Enterprise" with the Avaya logo. The left sidebar shows the navigation menu with "Device Management" selected. The main content area is titled "Device Management" and contains a tabbed interface with "Devices" selected. Below the tabs is a table listing the device SBCE100. The table columns are Device Name, Management IP, Version, and Status. The status "Commissioned" is highlighted with a red box. To the right of the status are links for Reboot, Shutdown, Restart Application, View, Edit, and Uninstall.

Device Name	Management IP	Version	Status	Actions
SBCE100	10.33.10.100	8.0.0.0-19-16991	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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.

System Information: SBCE100

General Configuration

Appliance Name	SBCE100
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions	512
Requested: 512	
Advanced Sessions	512
Requested: 512	
Scopia Video Sessions	512
Requested: 512	
CES Sessions	512
Requested: 512	
Transcoding Sessions	512
Requested: 512	
CLID	---
Encryption	<input checked="" type="checkbox"/>
Available: Yes	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.1.51	10.33.1.51	255.255.255.0	10.33.1.1	A1
10.33.1.52	10.33.1.52	255.255.255.0	10.33.1.1	A1
10.33.1.53	10.33.1.53	255.255.255.0	10.33.1.1	A1
10.33.1.54	10.33.1.54	255.255.255.0	10.33.1.1	A1
10.207.80.90	10.207.80.90	255.255.255.128	10.207.80.1	B1
10.207.80.107	10.207.80.107	255.255.255.128	10.207.80.1	B1
50.207.80.108	10.207.80.108	255.255.255.128	10.207.80.1	B1
10.207.80.109	10.207.80.109	255.255.255.128	10.207.80.1	B1

DNS Configuration

Primary DNS	10.33.100.60
Secondary DNS	8.8.8.8
DNS Location	DMZ
DNS Client IP	10.33.1.51

Management IP(s)

IP #1 (IPv4)	10.33.10.100
--------------	--------------

The highlighted IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to G12 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 (10.33.1.54) was used to connect to the enterprise network, while its public interface (10.207.80.90) 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.

8.3. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

It is assumed that generation and installation of certificates and the creation of TLS Profiles on the Avaya SBCE have been previously completed, as it's not discussed in this document. Refer to item [8] in **Section 12**.

8.4. 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 (**10.33.1.54**) and public (**10.207.80.90**) sides of the Avaya SBCE are the ones relevant to these Application Notes.

Device: SBCE100
Alarms
Incidents
Status
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

AVAYA

Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
SIP Servers
LDAP
RADIUS
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface

Network Management

Interfaces

Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Private_A1	10.33.1.1	255.255.255.0	A1	10.33.1.51, 10.33.1.52, 10.33.1.53, 10.33.1.54	Edit Delete
Public_B1	10.207.80.1	255.255.255.128	B1	10.207.80.90, 10.207.80.107, 10.207.80.108, 10.207.80.109	Edit Delete

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.

Device: SBCE100
Alarms
Incidents
Status
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Advanced Options
DMZ Services
Monitoring & Logging

Network Management

Interfaces

Networks

Add VLAN

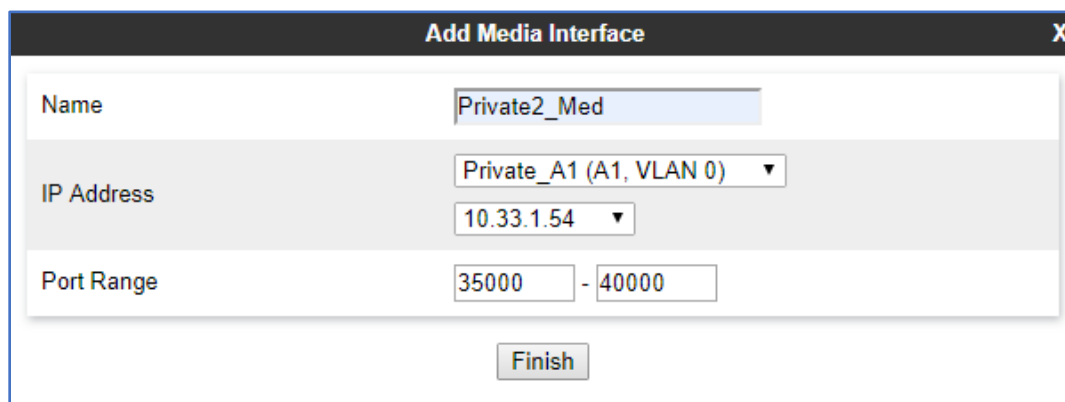
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

8.5. 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**.

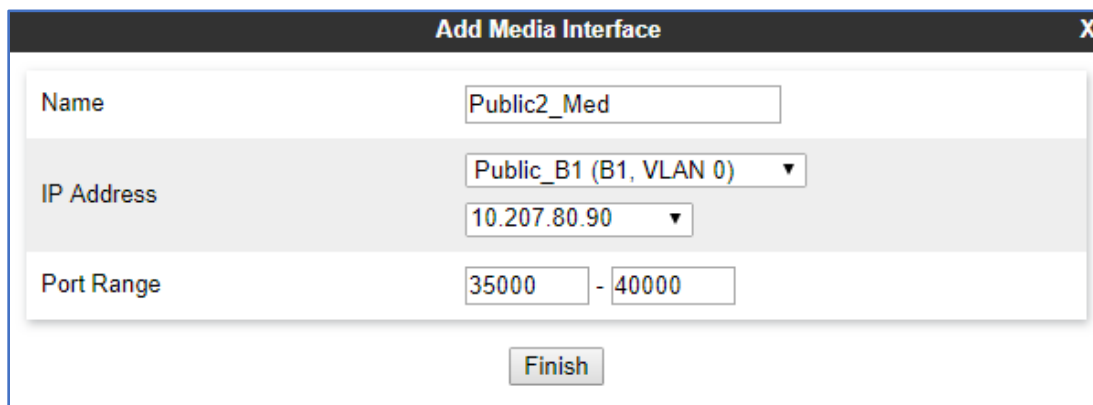


The screenshot shows the 'Add Media Interface' dialog box with the following fields:

- Name:** Private2_Med
- IP Address:** Private_A1 (A1, VLAN 0) (selected from a dropdown menu), 10.33.1.54 (selected from a dropdown menu)
- Port Range:** 35000 - 40000
- Finish** button

A Media Interface facing the public side was similarly created with the name **Public2_Med**, 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.
- Click **Finish**.



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

- Name:** Public2_Med
- IP Address:** Public_B1 (B1, VLAN 0) (selected from a dropdown menu), 10.207.80.90 (selected from a dropdown menu)
- Port Range:** 35000 - 40000
- Finish** button

8.6. 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 7.6**.
- Select a **TLS Profile**.
- Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' configuration window. The fields are as follows:

Field	Value
Name	Private2_Sig
IP Address	Private_A1 (A1, VLAN 0) 10.33.1.54
TCP Port	5060
UDP Port	
TLS Port	5061
TLS Profile	TLS_Server_Profile
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

A second Signaling Interface with the name **Public2_Sig** 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 G12 in the sample configuration.
- Click **Finish**.

Name	Public2_Sig
IP Address	Public_B1 (B1, VLAN 0) 10.207.80.90
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	

8.7. 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).

8.7.1. 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**.

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

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

Profile Name	avaya-ru
Clone Name	SM_ServerInter

Finish

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries.

The **General** tab settings are shown on the screen below. Make sure **T.38 Support** is checked and keep other fields at default.

The screenshot shows a dialog box titled "Editing Profile: SM_ServerInter" with a close button (X) in the top right corner. The "General" tab is selected. The settings are as follows:

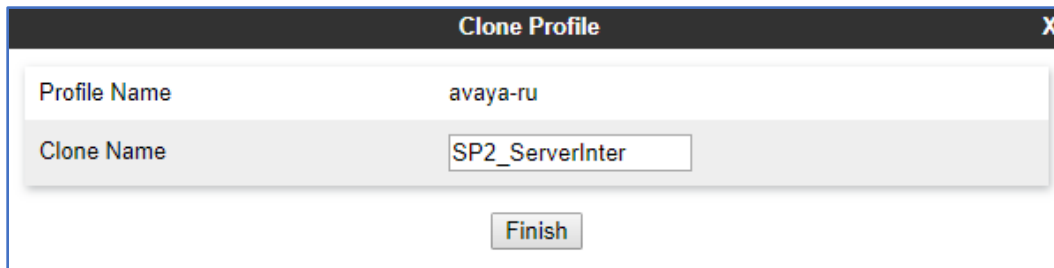
Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> 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

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

8.7.2. 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 **Configuration Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown).

- Enter a descriptive name for the new profile.
- Click **Next**.



Clone Profile	
Profile Name	avaya-ru
Clone Name	SP2_ServerInter
Finish	

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

The **Timers**, **Privacy**, **URI Manipulation**, **Header Manipulation** and **Advance** tabs contain no entries.

The **General** tab settings are shown on the screen below. Make sure **T.38 Support** is checked and keep other fields at default.

Editing Profile: SP2_ServerInter

X

General

Hold Support

☒ None
☐ RFC2543 - c=0.0.0.0
☐ RFC3264 - a=sendonly

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

Finish

8.8. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult reference [8] in the **References** section for more information on this topic.

A Sigma script was created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- Remove unwanted “gsid” and “epv” parameter from being sent to G12 in the Contact header.
- Remove the P-Location parameter from being sent to G12.

The scripts will later be applied to the Server Configuration Profiles corresponding the Service Provider (toward G12) in **Section 8.9.2**.

To create the SigMa script to be applied to the Server Configuration Profile corresponding to the Service Provider (G12), on the left navigation pane, select **Configuration Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name *G12Sigma* was chosen in this example.
- Copy and paste the script shown below or from Appendix A.
- Click **Save**.

```
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{

//Remove gsid and epv parameters from Contact header.
remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

//Remove P-Location parameter.
remove(%HEADERS["P-Location"][1]);

}
}
```

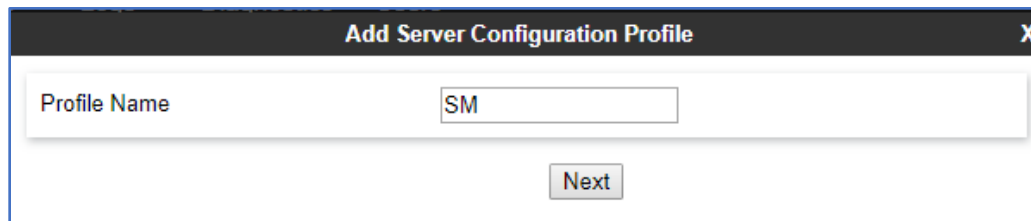

8.9. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and G12 SIP Proxy (Trunk Server).

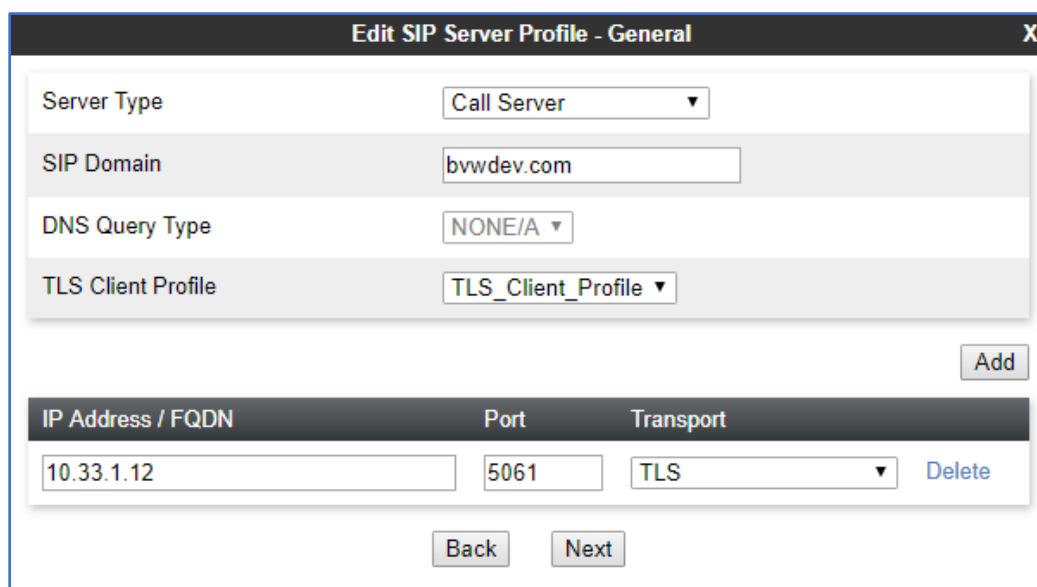
8.9.1. Server Configuration Profile – Enterprise

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**.



- On the **Edit SIP Server Profile – General** tab select *Call Server* from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 7.5**).
- 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 7.6**.
- Select a **TLS Profile**.
- Click **Next**.



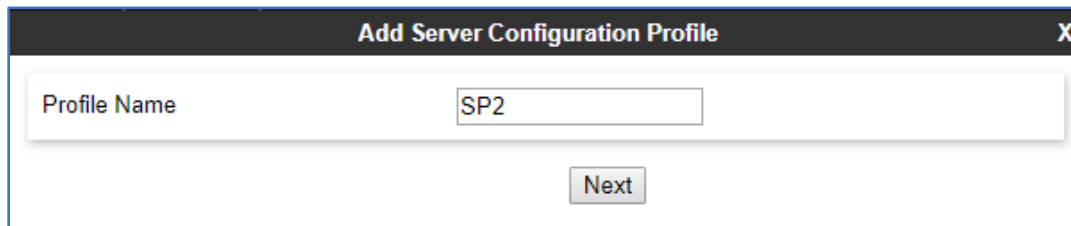
- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
 - Check **Enable Grooming**.
 - Select **SM_ServerInter** from the **Interworking Profile** drop-down menu (**Section 8.7.1**).
- Click **Finish**.

Edit SIP Server Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SM_ServerInter ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼
Finish	

8.9.2. 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 (*SP2* was used).
- Click **Next**.

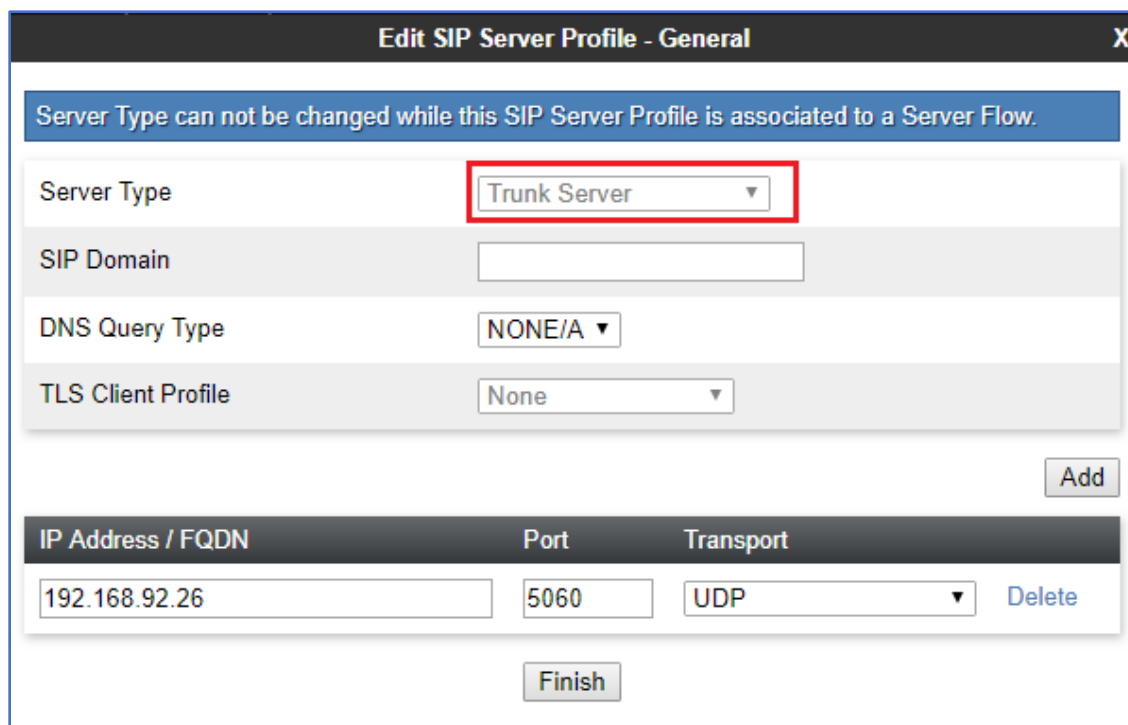


Add Server Configuration Profile X

Profile Name

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 *192.168.92.26* (G12's SIP proxy server IP address). This information was provided by G12.
- 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

SIP Domain

DNS Query Type

TLS Client Profile

Add

IP Address / FQDN	Port	Transport	
<input type="text" value="192.168.92.26"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	Delete

Finish

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

- Check **Enable Grooming**.
- Select **SP2_ServerInter** from the **Interworking Profile** drop-down menu (**Section 8.7.2**).
- Select the **Remove_Header** from the **Signaling Manipulation Script** drop down menu (**Sections 8.8** and **Section 13**).
- Click **Finish**.

The screenshot shows a window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options, each with a label and a control element:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SP2_ServerInter ▼
Signaling Manipulation Script	Remove_Header ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

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

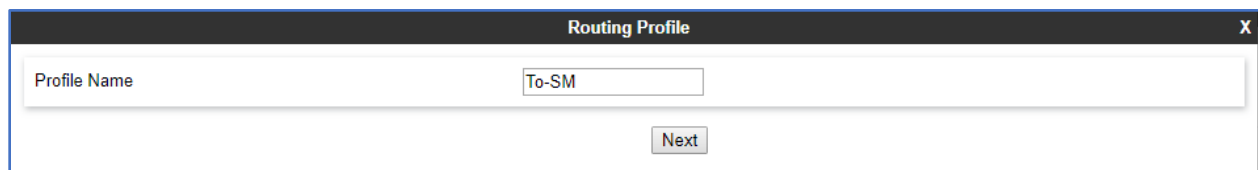
8.10.Routing

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.

8.10.1. Routing Profile – Enterprise

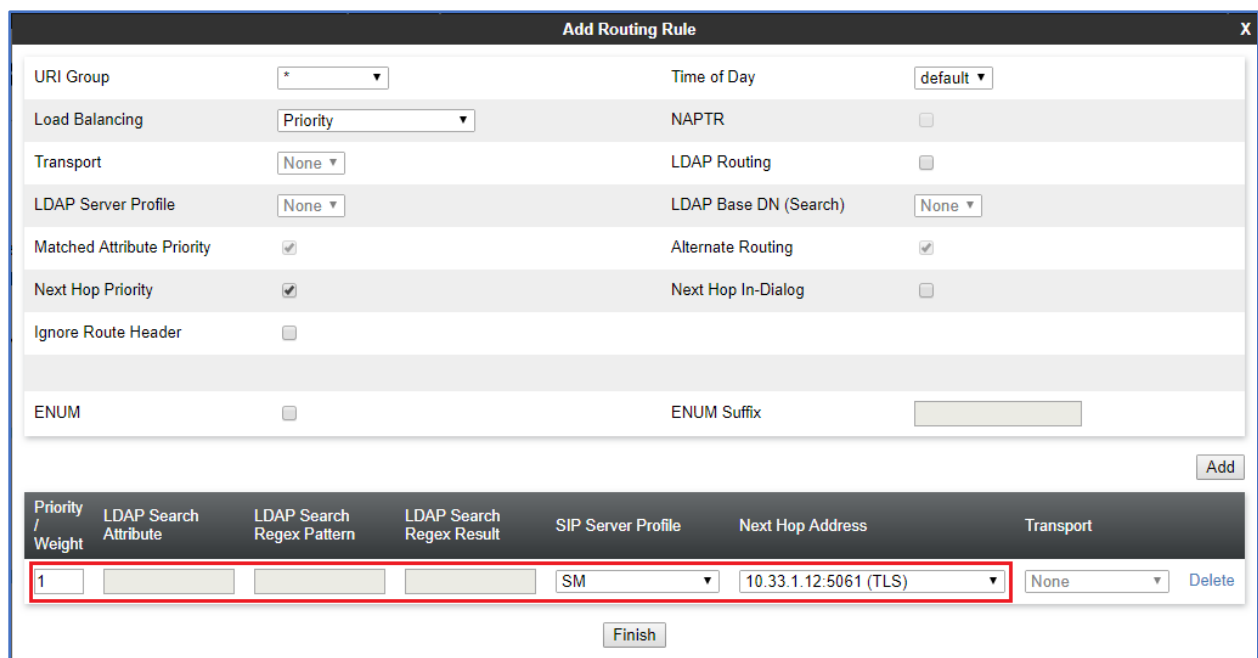
To create the inbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

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



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "To-SM". Below this field is a button labeled "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 **SM**. 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 8.9.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



The screenshot shows a window titled "Add Routing Rule" with a close button (X) in the top right corner. The window contains several configuration fields and a table at the bottom.

Configuration fields include:

- 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: (empty)

An "Add" button is located at the bottom right of the configuration area.

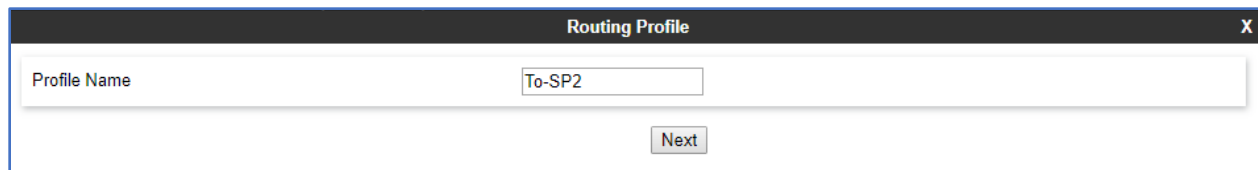
Below the configuration area is a table with the following columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. The first row of the table is highlighted with a red box and contains the following values: 1, (empty), (empty), (empty), SM, 10.33.1.12:5061 (TLS), and None. A "Delete" button is located to the right of the last cell in the first row.

A "Finish" button is located at the bottom center of the window.

8.10.2. Routing Profile – Service Provider

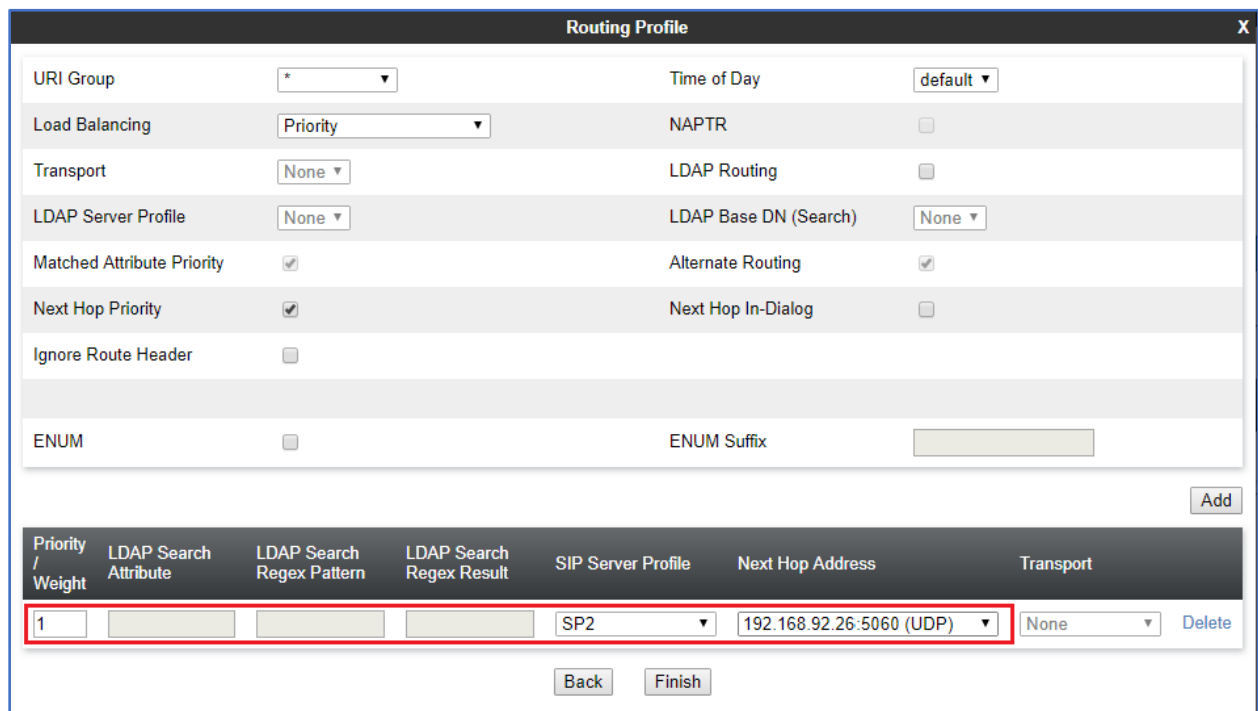
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below (*To-SP2* was used).
- Click **Next**.



The screenshot shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text field labeled 'Profile Name' containing the text 'To-SP2'. Below the text field is a button labeled 'Next'.

- Click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter *1*.
- Under **SIP Server Profile**, select *SP2*.
- The **Next Hop Address** is populated automatically with *192.168.92.26:5060 (UDP)* G12's SIP Proxy IP address, Port and Transport, Server Configuration Profile defined in **Section 8.9.2**.
- Click **Finish**



The screenshot shows a 'Routing Profile' dialog box with various configuration options and a table of routing entries.

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:

Routing Entries Table:

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SP2	192.168.92.26:5060 (UDP)	None	Delete

Buttons: Back, Finish, Add

8.11.Topology Hiding

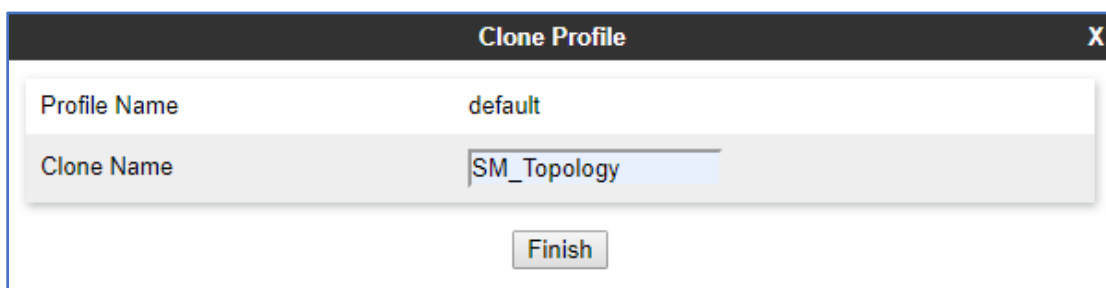
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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.

8.11.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise 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).

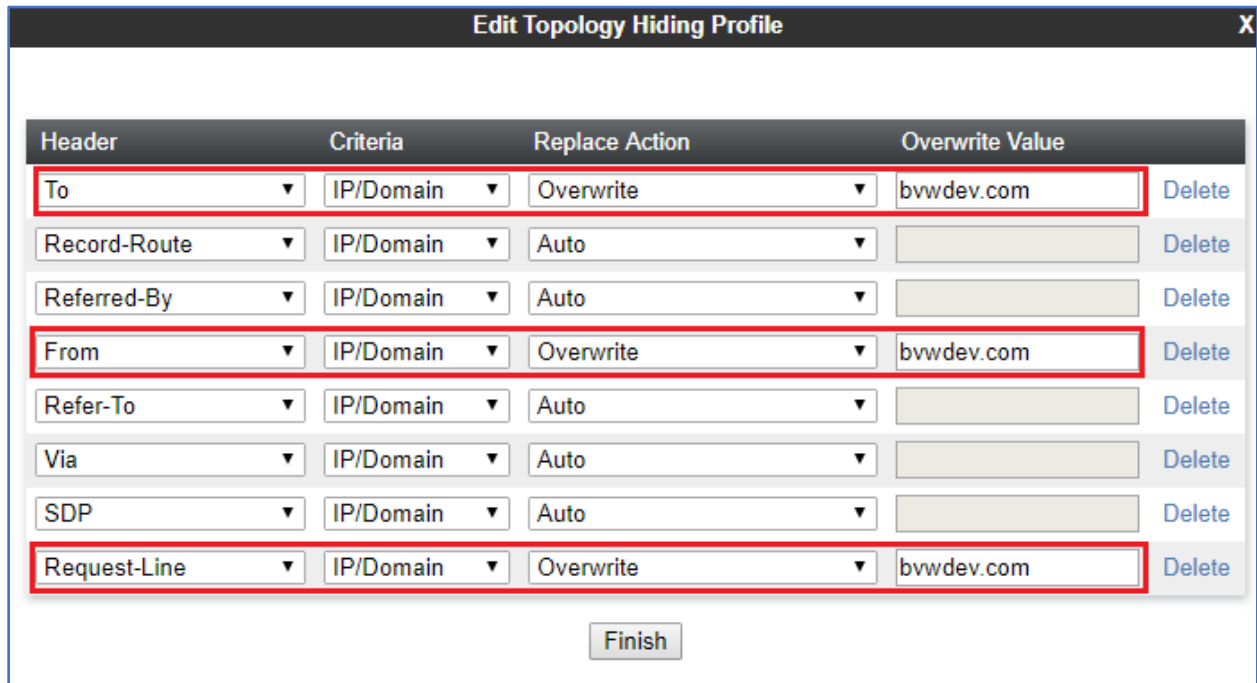
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The screenshot shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. Below the header, there are two input fields. The first field is labeled 'Profile Name' and contains the text 'default'. The second field is labeled 'Clone Name' and contains the text 'SM_Topology'. At the bottom center of the dialog, there is a button labeled 'Finish'.

On the newly cloned *SM_Topology* 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 *bvwdev.com*, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 7.2**.
- Default values were used for all other fields.
- Click **Finish**.



The screenshot shows a window titled "Edit Topology Hiding Profile" with a close button (X) in the top right corner. Inside the window is a table with four columns: "Header", "Criteria", "Replace Action", and "Overwrite Value". There are eight rows in the table. The first, fourth, and eighth rows are highlighted with red borders. In these highlighted rows, the "Header" column contains "To", "From", and "Request-Line" respectively. The "Criteria" column for all rows contains "IP/Domain". The "Replace Action" column for the highlighted rows contains "Overwrite", while for the other rows it contains "Auto". The "Overwrite Value" column for the highlighted rows contains "bvwdev.com", while for the other rows it is empty. To the right of each row is a "Delete" button. Below the table is a "Finish" button.

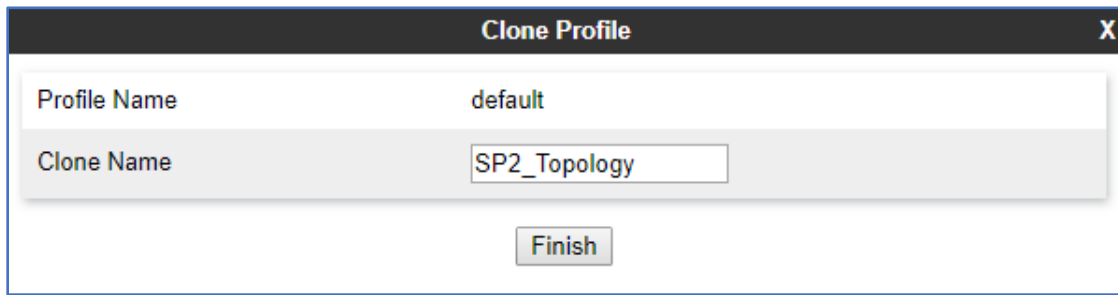
Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Overwrite	bvwdev.com	Delete
Record-Route	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	bvwdev.com	Delete
Refer-To	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Request-Line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

Finish

8.11.2. Topology Hiding Profile – Service Provider

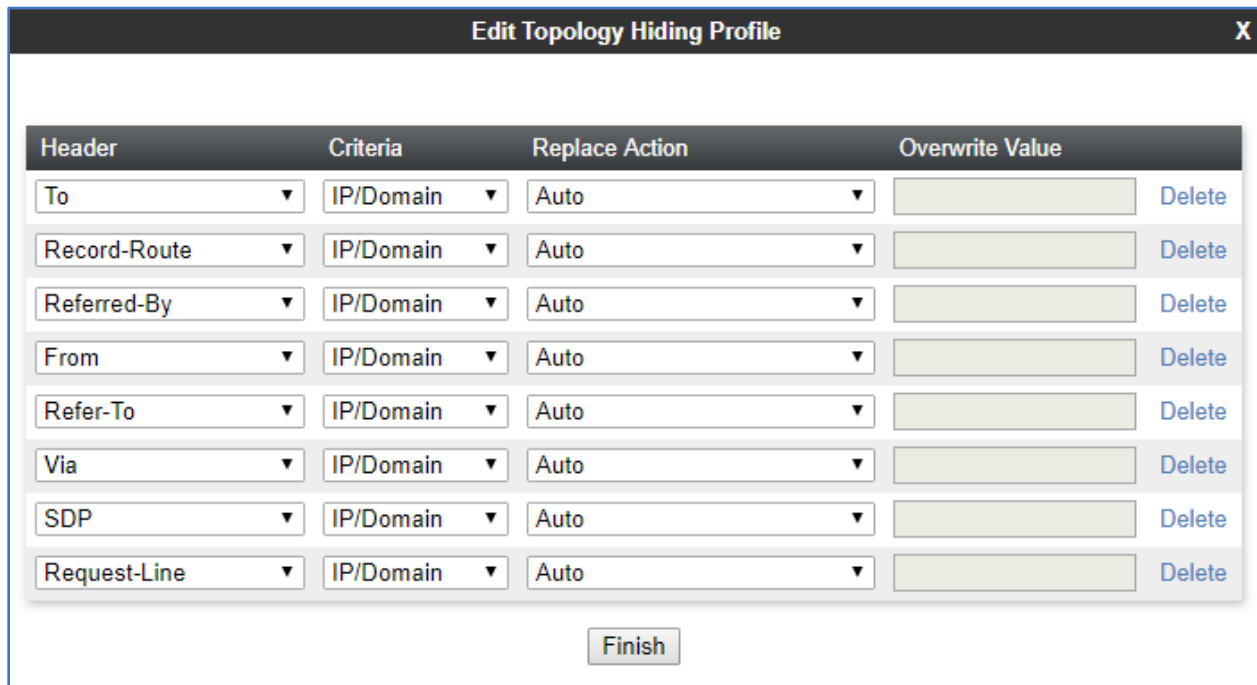
To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select *default* from the list of pre-defined profiles and click the **Clone** button (not shown).

- 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 'SP2_Topology'. Below these fields is a 'Finish' button.

- Click **Edit** on the newly created **SP2_Topology** Topology Hiding profile and leave all fields at default.
- 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 the following data:

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

Below the table is a 'Finish' button.

8.12.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.

8.12.1.Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**, click on the **Add** button to add a new rule.

In the testing, the **default-trunk** application rule was used as shown below.

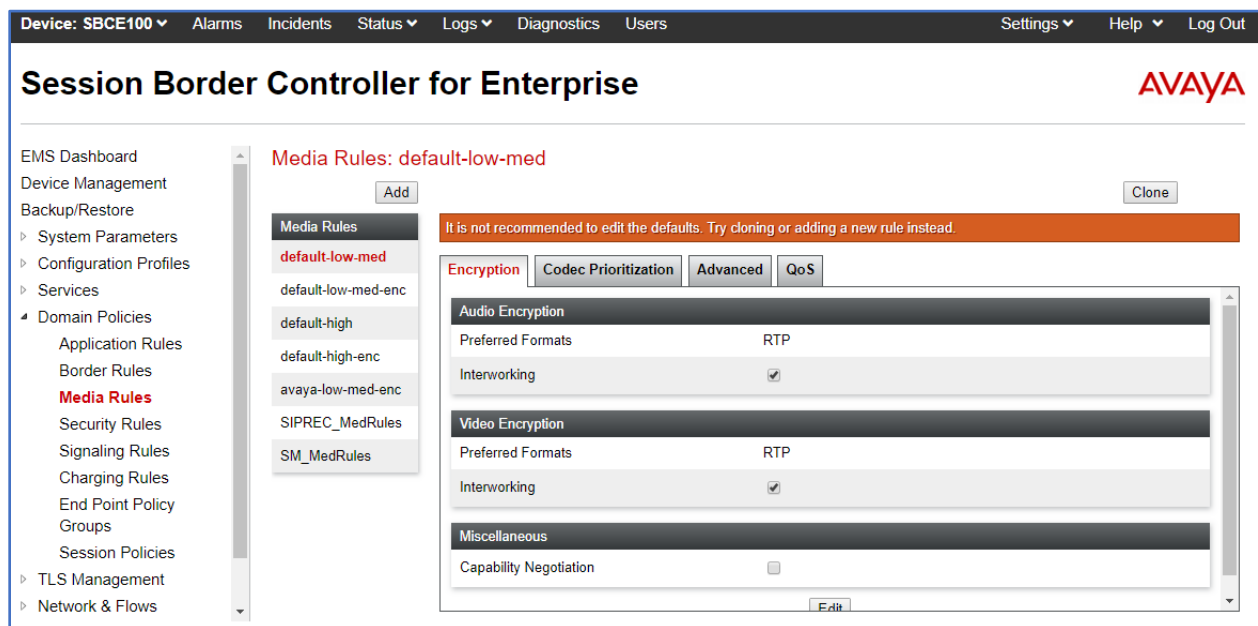
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	<input checked="" type="radio"/> Off <input type="radio"/> RADIUS <input type="radio"/> CDR Adjunct
RADIUS Profile	None ▼
Media Statistics Support	<input type="checkbox"/>
Call Duration	<input checked="" type="radio"/> Setup <input type="radio"/> Connect
RTCP Keep-Alive	<input type="checkbox"/>

Finish

8.12.2. 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 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.
- Under **Rule Name** enter **SM_MedRules**.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Leave all fields at default under Video Encryption.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Click **Next**.

Media Encryption
X

Audio Encryption

Preferred Format #1	S RTP_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"/>

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"/>

Miscellaneous

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

Finish

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

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

Media Encryption

Audio Encryption

Preferred Format #1

RTP

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☒

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Video Encryption

Preferred Format #1

RTP

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Miscellaneous

Capability Negotiation

☐

Finish

8.12.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE100, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various configuration areas, with 'Signaling Rules' highlighted under 'Domain Policies'. The main content area is titled 'Signaling Rules: default' and features an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'General' tab is active, showing a table with the following data:

UCID	Requests
	Allow
	Non-2XX Final Responses
	Allow
	Optional Request Headers
	Allow
	Optional Response Headers
	Allow

Below the table, there is a 'Content-Type Policy' section with a checkbox for 'Enable Content-Type Checks' which is checked. Below this, there is a table with the following data:

Action	Allow	Multipart Action	Allow
Exception List		Exception List	

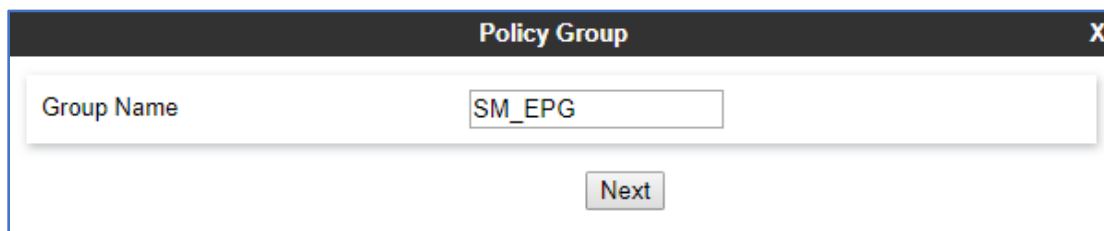
8.13.End Point Policy Groups

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.

8.13.1. 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).

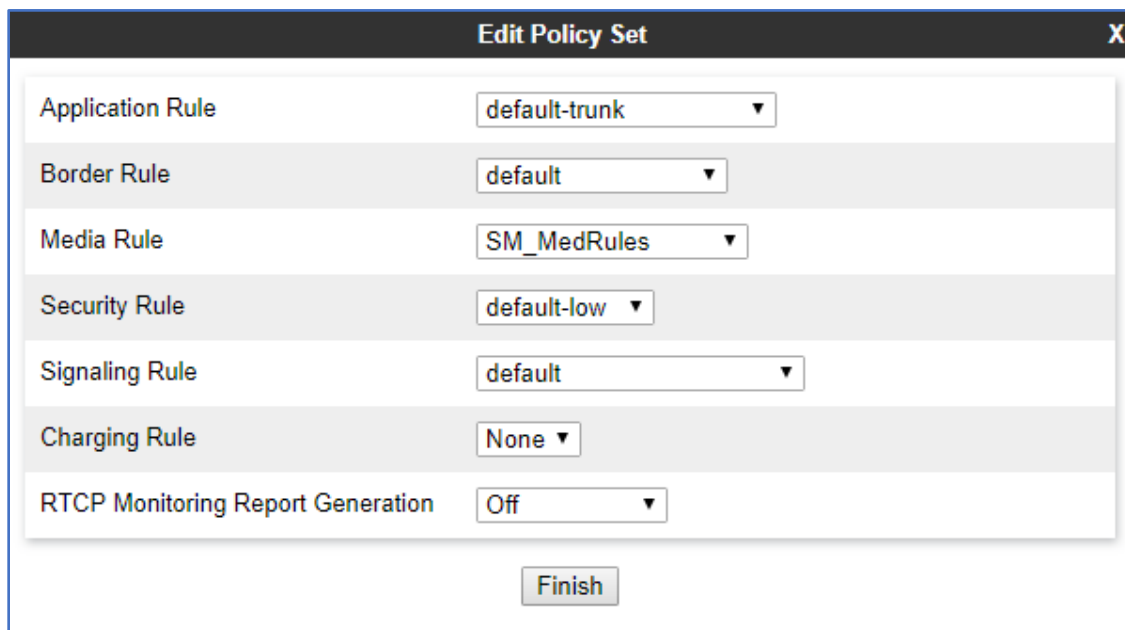
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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 "SM_EPG". Below the input field, there is a button labeled "Next".

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

- **Application Rule:** *default-trunk* (Section 8.12.1).
- **Border Rule:** *default*.
- **Media Rule:** *SM_MedRules* (Section 8.12.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 8.12.3).
- 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:

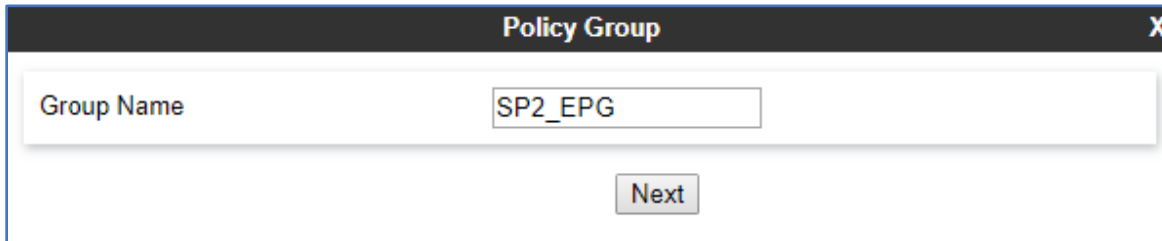
Label	Value
Application Rule	default-trunk
Border Rule	default
Media Rule	SM_MedRules
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

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

8.13.2. 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).

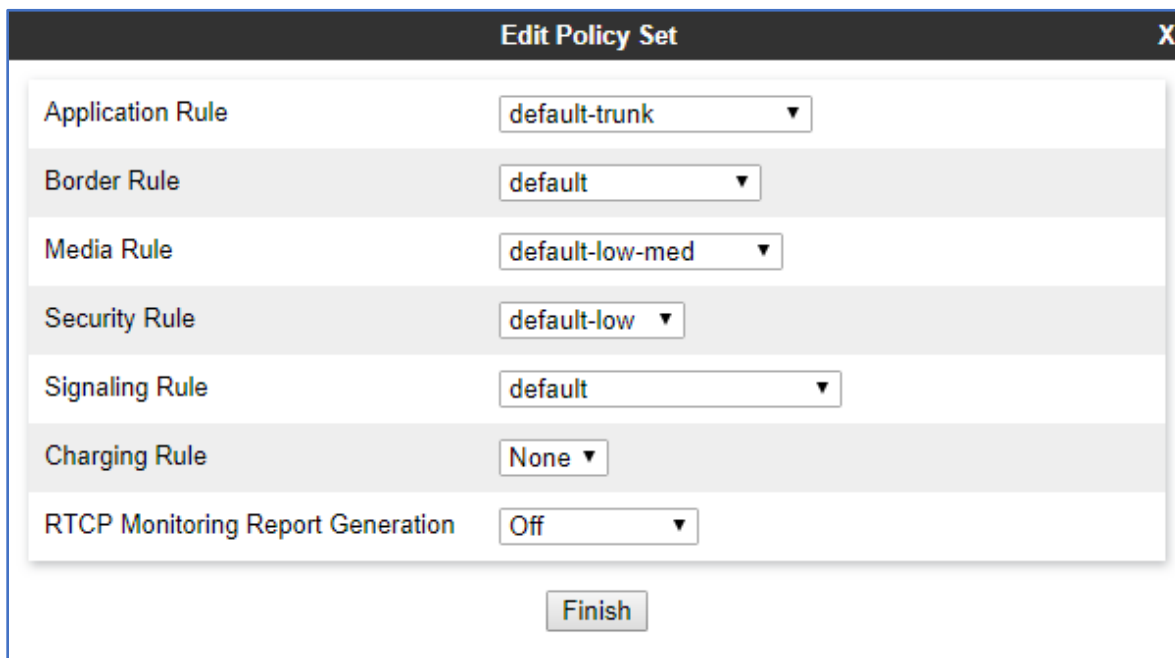
- Enter an appropriate name in the **Group Name** field (*SP2_EPG* was used).
- Click **Next**.



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 "SP2_EPG". Below the input field, there is a button labeled "Next".

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

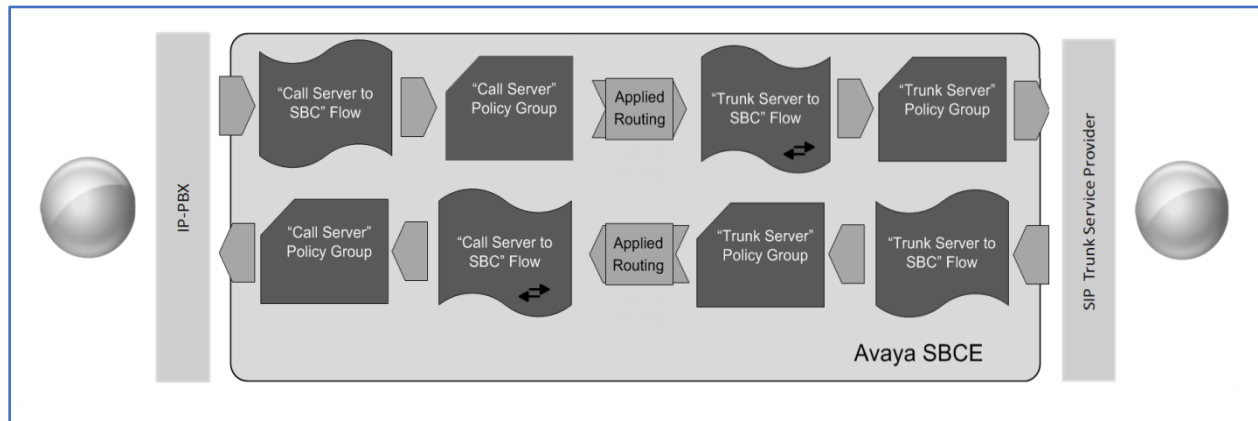
- **Application Rule:** *default-trunk* (Section 8.12.1).
- **Border Rule:** *default*.
- **Media Rule:** *default-low-med* (Section 8.12.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 8.12.3).
- Click **Finish**.



The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. Inside the dialog, there are several rows, each with a label on the left and a dropdown menu on the right. The labels and their corresponding dropdown values are: "Application Rule" (default-trunk), "Border Rule" (default), "Media Rule" (default-low-med), "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".

8.14.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.

8.14.1. End Point Flow – Enterprise

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). The screen below shows the flow named *Session Manager Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 8.10.2**, which is the reverse route of the flow. Click **Finish**.

Flow Name	Session Manager Flow
SIP Server Profile	SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public2_Sig
Signaling Interface	Private2_Sig
Media Interface	Private2_Med
Secondary Media Interface	None
End Point Policy Group	SM_EPG
Routing Profile	To-SP2
Topology Hiding Profile	SM_Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

Finish

8.14.2. End Point Flow – Service Provider

A second Server Flow with the name *Service Provider Flow* was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 8.10.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.

The screenshot shows the 'Edit Flow: Service Provider Flow' configuration window. The fields and their values are as follows:

Field	Value
Flow Name	Service Provider Flow
SIP Server Profile	SP2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private2_Sig
Signaling Interface	Public2_Sig
Media Interface	Public2_Med
Secondary Media Interface	None
End Point Policy Group	SP2_EPG
Routing Profile	To-SM
Topology Hiding Profile	SP2_Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

At the bottom of the window is a 'Finish' button.

9. G12 SIP Trunking Service Configuration

To use G12 SIP Trunking Service, a customer must request the service from G12 using the established sales processes. The process can be started by contacting G12 via the corporate web site at: <https://www.g12com.com/>

During the signup process, G12 and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to G12 network.

G12 will provide the following information:

- SIP Trunk IP address.
- Domain name.
- DID numbers.
- Etc.

10. 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.

10.1.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.

10.2.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.

10.3.Session Manager Verification

The Session Manager configuration may be verified via System Manager.

Step 1 - Using the procedures described in **Section 7**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**, then select **Dashboard** (not shown).

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

In the **Entity Monitoring** column, Session Manager shows that there are **3** alarms out of the **18** Entities defined.

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: Shutdown System: EASG: As of 9:53 AM

2 Items Show All Filter: Enable

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
ASM70A	Core	✓	0/0/0	Up	Accept New Service	3/18	0	2/2	✓	✓	Normal	Enabled	8.1.0.0
ASM70B	Core	No Connection	---	---	---	---	---	---	---	---	Normal	---	---

Select : All, None

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.

Avaya Aura System Manager 8.1

Home Session Manager

Session Manager

Dashboard

Session Manager Ad...

Global Settings

Communication Prof...

Network Configur...

Device and Locati...

Application Confi...

System Status

SIP Entity Monit...

Managed Band...

All Entity Links for Session Manager: ASM70A

Summary View

19 Items Filter: Enable

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
	SIPAACC	IPv4	10.33.1.55	5061	TLS	FALSE	UP	200 OK	UP
	SBCE-A1	IPv4	10.33.1.54	5061	TLS	FALSE	UP	200 OK	UP
	Presence70	IPv4	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
	IPOSE110	IPv4	10.33.1.110	5061	TLS	FALSE	UP	200 OK	UP
	Dialogic	IPv4	10.33.1.200	5060	TCP	FALSE	UP	200 OK	UP
	Car2-cores	IPv4	10.33.1.81	5060	TCP	FALSE	UP	200 OK	UP
	Breeze2	IPv4	10.33.1.46	5061	TLS	FALSE	UP	200 OK	UP
	Breeze	IPv4	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
	ASBCE-A1	IPv4	10.33.1.51	5061	TLS	FALSE	UP	200 OK	UP
	AEP72	IPv4	10.33.1.3	5061	TLS	FALSE	UP	200 OK	UP
	ACM-Trunk3-Public	IPv4	10.33.1.6	5067	TLS	FALSE	UP	200 OK	UP
	ACM-Trunk1-Private	IPv4	10.33.1.6	5061	TLS	FALSE	UP	200 OK	UP
	AAM	IPv4	10.33.1.5	5061	TLS	FALSE	UP	200 OK	UP
	car2-mas	IPv4	Entity is not monitored	0	---	N.A.	DOWN		NOTMONITORED
	Breeze1	IPv4	Entity is not monitored	0	---	N.A.	DOWN		NOTMONITORED

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.

10.4.Ayaya 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.

Session Border Controller for Enterprise **AVAYA**

EMS Dashboard

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

Dashboard

Information	
System Time	10:13:48 AM MDT Refresh
Version	8.0.0.0-19-16991
Build Date	Sat Jan 26 21:58:11 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	10/29/2019 10:54:32 MDT
Failed Login Attempts	0

Installed Devices

- EMS
- SBCE100

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

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

Alarm Viewer **AVAYA**

Alarms

<input checked="" type="checkbox"/>	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 displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left, the 'EMS Dashboard' menu lists 'Device Management', 'System Administration', 'Backup/Restore', and 'Monitoring & Logging'. The central 'Dashboard' section contains several widgets: 'Information' (System Time: 10:16:07 AM MDT, Version: 8.0.0.0-19-16991, Build Date: Sat Jan 26 21:58:11 UTC 2019, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 10/29/2019 10:54:32 MDT, Failed Login Attempts: 0), 'Installed Devices' (listing EMS and SBCE100), 'Active Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (None found). An 'Add' button is located at the bottom right of the dashboard area.

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

The screenshot displays the 'Incident Viewer' page. The top navigation bar includes 'Help'. The main header shows 'Incident Viewer' and the 'AVAYA' logo. Below the header, there are filters for 'Device' (set to 'All') and 'Category' (set to 'Licensing'), along with a 'Clear Filters' button. To the right are 'Refresh' and 'Generate Report' buttons. The text 'Displaying results 0 to 0 out of 0.' is shown above a table. The table has columns for 'ID', 'Device', 'Date & Time', 'Category', 'Type', and 'Cause'. The table body contains the text 'No incidents found.' Below the table is a pagination control showing '<<' '<' '1' '>' '>>'.

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

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

Session Border Controller for Enterprise

EMS Dashboard

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

Dashboard

Information	
System Time	10:21:15 AM MDT Refresh
Version	8.0.0.0-19-16991
Build Date	Sat Jan 26 21:58:11 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	10/29/2019 10:54:32 MDT
Failed Login Attempts	0

Installed Devices

- EMS
- SBCE100

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

[Add](#)

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

Device: SBCE100 ▾ Help

Diagnostics

Full Diagnostic **Ping Test** [Start Diagnostic](#)

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (10.33.1.1)	Average ping from 10.33.1.51 [A1] to 10.33.1.1 is 0.703ms.
✓ Ping: SBC (A1) to Primary DNS (10.33.100.60)	Average ping from 10.33.1.51 [A1] to 10.33.100.60 is 0.306ms.
✓ Ping: SBC (A1) to Secondary DNS (8.8.8.8)	Average ping from 10.33.1.51 [A1] to 8.8.8.8 is 2.560ms.
✓ Ping: SBC (B1) to	

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 displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: SBCE100, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo. A left sidebar lists various management options, with "Monitoring & Logging" expanded to show "Trace" as the selected option. The main content area, titled "Trace: SBCE100", contains a "Packet Capture" tab and a "Captures" tab. The "Packet Capture Configuration" window is open, showing a form with the following fields: Status (Ready), Interface (Any), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (capture.pcap). A red rectangle highlights the Status, Interface, Local Address, Remote Address, and Protocol fields. At the bottom of the configuration window are "Start Capture" and "Clear" buttons.

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address <small>IP[:Port]</small>	All :
Remote Address <small>*, *:Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	capture.pcap

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 displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: SBCE100, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management options, with "Monitoring & Logging" expanded to show "Trace" in red. The main content area is titled "Trace: SBCE100" and features two tabs: "Packet Capture" and "Captures". The "Captures" tab is active, showing a table of captured files. A red box highlights the first entry in the table.

File Name	File Size (bytes)	Last Modified	
capture_20191031102756.pcap	983,040	October 31, 2019 10:28:29 AM MDT	Delete

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

11. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.0, to connect to the G12 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**.

12. 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 8.1.x, Issue 2, August 2019.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 3, August 2019.
- [3] *Administering Avaya Aura® System Manager for Release 8.1.x*, Issue 3, July 2019.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 8.1.x, Issue 2, July 2019.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 8.1., Issue 1, June 2019.
- [6] *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 1, June 2019.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 3, July 2019.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 1, February 2019.
- [9] *Administering Avaya Aura® Experience Portal*, Release 7.2.2, Issue 1, March 2019
- [10] *Implementing Avaya Aura® Experience Portal on a single server*, Release 7.2.2, Issue 1, July 2019
- [11] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0 - Issue 1.0*.
- [12] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 7, June 2019.
- [13] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0.x, Issue 5, June 2019.
- [14] *Planning for and Administering Avaya Equinox for Android, iOS, Mac, and Windows*. Release 3.6, Issue 1, July 2019.
- [15] *Administering Avaya one-X® Communicator*. Release 6.2, Feature Pack 10, November 2015.
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [17] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2019 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.