

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Allstream SIP Trunk with Avaya Aura[®] Communication Manager 8.0, Avaya Aura[®] Session Manager 8.0 and Avaya Session Border Controller for Enterprise 8.0 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Allstream and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 8.0, Avaya Aura[®] Communication Manager 8.0, Avaya Session Border Controller for Enterprise 8.0 and various Avaya endpoints.

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.

Allstream is a member of the Avaya DevConnect Service Provider program. 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.	INT	RODUCTION	4		
2.	2. GENERAL TEST APPROACH AND TEST RESULTS4				
	2.1.	INTEROPERABILITY COMPLIANCE TESTING	5		
	2.2.	TEST RESULTS	5		
	2.3.	SUPPORT	6		
3.	RE	FERENCE CONFIGURATION	7		
4.	EQ	UIPMENT AND SOFTWARE VALIDATED	8		
5.	CO	NFIGURE AVAYA AURA [®] COMMUNICATION MANAGER	10		
	5.1.	LICENSING AND CAPACITY	10		
	5.2.	System Features			
	5.3.	IP NODE NAMES	13		
	5.4.	CODECS	13		
	5.5.	IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER	15		
	5.6.	CONFIGURE IP INTERFACE FOR PROCR			
	5.7.	SIGNALING GROUP			
	5.8.	TRUNK GROUP			
	5.9.	CALLING PARTY INFORMATION			
	5.10.	OUTBOUND ROUTING			
	5.11.	INCOMING CALL HANDLING TREATMENT			
	5.12.	CONTACT CENTER CONFIGURATION			
		2.1. Announcements			
		2.2. ACD Configuration for Call Queued for Handling by Agent			
	5.13.	AVAYA AURA® COMMUNICATION MANAGER STATIONS			
	5.14.	SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES			
6.	CO	NFIGURE AVAYA AURA® SESSION MANAGER			
	6.1.	AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION			
	6.2.	SPECIFY SIP DOMAIN			
	6.3.	ADD LOCATION	40		
	6.4.	ADD SIP ENTITIES			
		1. Configure Session Manager SIP Entity			
		2. Configure Communication Manager SIP Entity			
		3. Configure Avaya Session Border Controller for Enterprise SIP Entity			
	6.5.	ADD ENTITY LINKS			
	6.6.	CONFIGURE TIME RANGES			
	6.7.	ADD ROUTING POLICIES	•••••••••••••••••••••••••••••••		
	6.8.	ADD DIAL PATTERNS			
7.	CO	NFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	53		
	7.1.	LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	53		
	7.2.	GLOBAL PROFILES	56		
		1. Configure Server Interworking Profile - Avaya Site			
		2. Configure Server Interworking Profile – Allstream SIP Trunk Site			
		3. Configure Signaling Manipulation			
		4. Configure Server – Avaya Site			
		5. Configure Server – Allstream SIP Trunk			
		6. Configure Routing – Avaya Site			
		7. Configure Routing – Allstream SIP Trunk Site			
	7.2.	8. Configure Topology Hiding	68		

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

,	7.3.	DOMAIN POLICIES	70
	7.3.1	. Create Application Rules	
	7.3.2	. Create Media Rules	71
	7.3.3	. Create Signaling Rules	73
	7.3.4	Create Endpoint Policy Groups	
,	7.4.	DEVICE SPECIFIC SETTINGS	76
	7.4.1	. Manage Network Settings	76
		. Create Media Interfaces	
		Create Signaling Interfaces	
		. Configuration Server Flows	81
		4.4.1 Create End Point Flows – SMVM Flow	
	7.	4.4.2 Create End Point Flows – Allstream SIP Trunk Flow	
8.	ALL	STREAM SIP TRUNK CONFIGURATION	85
9.	VER	IFICATION STEPS	85
10.	CON	ICLUSION	86
11.	REF	ERENCES	87
12.	APP	ENDIX A – REMOTE WORKER CONFIGURATION	
	12.1.	NETWORK MANAGEMENT ON AVAYA SBCE	
	12.2.	MEDIA INTERFACE ON AVAYA SBCE	91
	12.3.	SIGNALING INTERFACE ON AVAYA SBCE	92
	12.4.	ROUTING PROFILE ON AVAYA SBCE	93
	12.5.	USER AGENT ON AVAYA SBCE	95
	12.6.	APPLICATION RULES ON AVAYA SBCE	
	12.7.	END POINT POLICY GROUPS ON AVAYA SBCE	
	12.8.	END POINT FLOWS ON AVAYA SBCE	
		1. Subscriber Flow	
		2. Server Flow on Avaya SBCE	
		2.8.2.1 Remote Worker Server Flow	
		2.8.2.2 Trunking Server Flow	
	12.9.	SYSTEM MANAGER	
		1. Modify Session Manager Firewall: Elements \rightarrow Session Manager \rightarrow Network Configuration	
		vall	
	12.9. 12.10.	2. Disable PPM Limiting: Elements 7 Session Manager 7 Session Manager Administration REMOTE WORKER CLIENT CONFIGURATION	
		Global Settings Screen	
13.	APP	ENDIX B - SIGMA SCRIPT	

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Allstream and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 8.0, Avaya Aura[®] Communication Manager 8.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 8.0 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Allstream SIP Trunk are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Allstream SIP Trunk via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Avaya SBCE with various types of Avaya phones.

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. 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 Allstream SIP Trunk Service did not include use of any specific encryption features as requested by Allstream.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test.

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider
- Outgoing PSTN calls from various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used in testing: Avaya one-X[®] Communicator (1XC) and Avaya EquinoxTM for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya EquinoxTM for Windows was used in testing as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using UDP, port 5060, between the Avaya enterprise and Allstream
- Direct IP-to-IP Media (also known as "Shuffling") over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway or Avaya Media Server
- Various call types including: local call, international call, inbound toll-free call, outbound toll-free, operator assisted call, local directory assistance call 411, emergency call 911
- Codec G.729, G.711MU
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call transfer, conference, off-net call forwarding, forwarding to Avaya Aura[®] Messaging and EC500 mobility (extension to cellular)
- SIP re-Invite/Update and REFER in off-net call transfer
- SIP Diversion header in off-net call forward
- Call Center scenarios
- Fax T.38 mode
- DTMF RFC2833
- Remote Worker

2.2. Test Results

Interoperability testing of Allstream was completed with successful results with limitation and observation below:

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	5 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

• For the outbound calls originated from the enterprise to PSTN, the Called Party number on the Avaya deskphones showed "Received by calling number" instead of "Received by called PSTN number" after the call was answered by PSTN - This issue is related to the URI.USER in the CONTACT header of "180 Ringing" and "183 Session Progress" and "200 OK" responded by Allstream. In the compliance testing, Allstream sent the URI.USER in the CONTACT headers as the provided DID number or invalid number instead of called PSTN number to the enterprise. As designed intent, Session Manager uses the URI.USER in the CONTACT headers to populate in the PAI header and sent it to Communication Manager. Then, Communication Manager/SIP phone used the URI.USER in the PAI header for the display purpose. Since Allstream cannot fix this issue, Avaya provide a fix by using a sigma script on Avaya SBCE to manipulate the URI.USER in the CONTACT header of "180 Ringing" and "183 Session Progress" and "200 OK " coming from Allstream (See Section 7.2.3 in details).

2.3. Support

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

For technical support on Allstream SIP Trunking, contact Allstream at https://allstream.com/solutions/sip-trunking/

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Allstream SIP Trunk. This is the configuration used for compliance testing.

For confidentiality and privacy purposes, actual public IP Addresses used in this testing have been masked out and replaced with fictitious IP Addresses throughout the document.

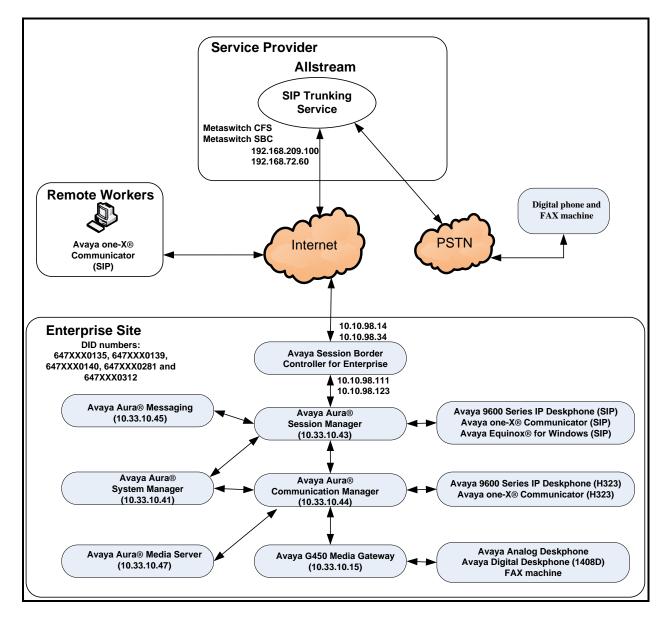


Figure 1: Avaya IP Telephony Network and Allstream SIP Trunk

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components			
Equipment/Software	Release/Version		
Avaya Aura [®] Communication Manager	8.0.0.1.2.822.25183		
running on VMware [®] -based Avaya appliance			
Avaya G450 Media Gateway	HW2 FW40.25		
– MM711AP Analog	HW46 FW096		
 MM712AP Digital 	HW10 FW014		
– MM710AP	HW5 FW020		
Avaya Aura [®] Session Manager	8.0.1.1.801103		
running on VMware [®] -based Avaya appliance			
Avaya Aura [®] System Manager	8.0.1.1		
running on VMware [®] -based Avaya appliance	Build-8.0.0.931077		
	Revision 8.0.1.1.039340		
Avaya Aura [®] Messaging	7.1.0.1.532.002.0 (SP1)		
running on VMware [®] -based Avaya appliance			
Avaya Aura [®] Media Server	8.0.0.183		
running on VMware [®] -based Avaya appliance			
Avaya Session Border Controller for Enterprise	8.0.0.19-16991		
running on Dell R210 V2 Server			
Avaya 9621G IP Deskphone (SIP)	Avaya [®] Deskphone SIP 7.1.5.0.11		
Avaya 9621G IP Deskphone (H.323)	Avaya [®] IP Deskphone		
	6.8.003		
Avaya 9641 IP Deskphone (H.323)	Avaya [®] IP Deskphone		
	6.8.003		
Avaya Digital Deskphone (1408D)	R48		
Avaya Equinox [™] for Windows	3.5.5.113.24		
Avaya one-X [®] Communicator (H.323 & SIP)	6.2.13.2-SP13 Patch 1		
Avaya Analog Deskphone	N/A		
HP Officejet 4500 Fax	N/A		
Allstream SIP Tr			
Equipment/Software	Release/Version		
Metaswitch CFS	rel 9.4.30		
Metaswitch SBC	rel 4.3.40		

Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	8 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

Note: It is assumed the general installation of VMware[®]- based Avaya Appliance Virtualization Platform, Avaya Aura[®] Communication Manager, Avaya Aura[®] System Manager, Avaya Aura[®] Session Manager, Avaya Aura[®] Messaging, Avaya Aura[®] Media Server and Avaya Media Gateway has been previously completed and is not discussed in this document.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Allstream SIP Trunk.

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.

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 the service provider. The example shows that 30000 SIP trunks are available and 100 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 to add additional capacity.

display system-parameters customer-options OPTIONAL FEATURES		Page	2 of 12
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	12000	0	
Maximum Concurrently Registered IP Stations:	18000	2	
Maximum Administered Remote Office Trunks:	12000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	414	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	41000	0	
Maximum Video Capable IP Softphones:	18000	5	
Maximum Administered SIP Trunks:	30000	100	
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	688	0	

Figure 2: System-Parameters Customer-Options Form – Page 2

On Page 4, verify that ARS is set to y.

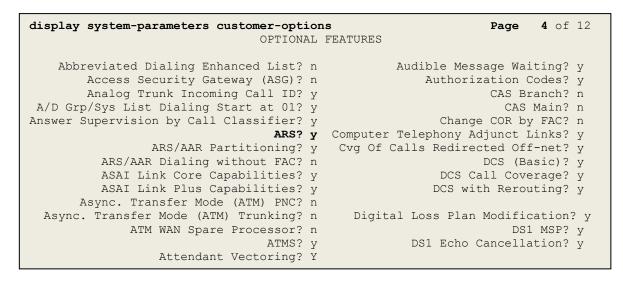


Figure 3: System-Parameters Customer-Options Form – Page 4

On Page 6, verify that Private Networking and Processor Ethernet are set to y.

```
6 of 12
display system-parameters customer-options
                                                               Page
                               OPTIONAL FEATURES
               Multinational Locations? n
                                                     Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n
                                             Station as Virtual Extension? y
                    Multiple Locations? n
                                            System Management Data Transfer? n
         Personal Station Access (PSA)? y
                                                        Tenant Partitioning? y
                                                Terminal Trans. Init. (TTI)? y
                       PNC Duplication? n
                                                       Time of Day Routing? y
                  Port Network Support? n
                                              TN2501 VAL Maximum Capacity? y
                       Posted Messages? y
                                                       Uniform Dialing Plan? y
                    Private Networking? y
                                             Usage Allocation Enhancements? y
              Processor and System MSP? y
                    Processor Ethernet? y
                                                         Wideband Switching? y
                                                                   Wireless? n
                         Remote Office? y
         Restrict Call Forward Off Net? y
                 Secondary Data Module? y
```

Figure 4: System-Parameters Customer-Options Form – Page 6

5.2. System Features

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

```
change system-parameters featuresPage1 of19FEATURE-RELATED SYSTEM PARAMETERS<br/>Self Station Display Enabled? nImage: Constraint of the system of the syste
```

Figure 5: System-Parameters Features Form – Page 1

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 **anonymous** for both. The value of **anonymous** is replaced for restricted numbers and unavailable numbers (refer to **Section 5.8**).

```
Page 9 of 19
change system-parameters features
                       FEATURE-RELATED SYSTEM PARAMETERS
CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous
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
```

Figure 6: System-Parameters Features Form – Page 9

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 as below:

- Messaging: Name: AAMVM, IP Address: 10.33.10.45
- Media Server: Name: AMS, IP Address: 10.33.10.47
- Session Manager: Name: bvwasm2, IP Address: 10.33.10.43
- Communication Manager: Name: procr, IP Address: 10.33.10.44

These node names will be needed for defining the service provider signaling group in **Section 5.7**.

change node-na	mes ip		Page	1 of	2
		IP NODE NAMES			
Name	IP Address				
AAMVM	10.33.10.45				
AMS	10.33.10.47				
bvwasm2	10.33.10.43				
default	0.0.0.0				
procr	10.33.10.44				
procr6	::				

Figure 7: Node-Names IP Form

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. In the compliance test, **ip-codec-set 1** was used for this purpose. Allstream supports the **G.729**, and **G.711MU** codecs. Default values can be used for all other fields.

```
        change ip-codec-set 1
        Page
        1 of
        2

        IP CODEC SET

        Codec Set: 1

        Audio
        Silence
        Frames
        Packet
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
```

Figure 8: IP-Codec-Set Form – Page 1

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. On Page 2, set the FAX Mode to t.38-standard. Allstream supports T.38 mode.

change ip-codec-set 1				Page	2 of	2
	IP CODEC SET					
	Allow Direc	t-IP Multimedia	? n			
	Mode	Redundancy		Pa	acket S	Size(ms)
FAX	t.38-standard	0	ECM:	У		
Modem	off	0				
TDD/TTY	US	3				
H.323 Clear-channel	n	0				
SIP 64K Data	n	0			20	

Figure 9: IP-Codec-Set Form – Page 2

5.5. IP Network Region for Media Gateway, Media Server

Network region provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, both Avaya G450 Media Gateway and Avaya Media Server were tested and used region 1. For the compliance test, IP network region 1 was chosen for the service provider trunk.

Use the **change ip-network-region 1** command to configure region 1 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**. This name appears in the From header of SIP messages originating from this IP region
- Enter a descriptive name in the **Name** field
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. Set both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes**. Shuffling can be further restricted at the trunk level on the Signaling Group form in **Section 5.7**
- Set the Codec Set field to the IP codec set defined in Section 5.4
- Default values can be used for all other fields

change ip-network-region 1 Page 1 of 20					
IP	NETWORK REGION				
Region: 1					
Location: 1 Authoritative	Domain: bvwdev.com				
Name: procr S	Stub Network Region: n				
MEDIA PARAMETERS I	ntra-region IP-IP Direct Audio	: yes			
Codec Set: 1 In	nter-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 RESERVATIO	N PARAM	IETERS		
H.323 IP ENDPOINTS	RSVP E	nabled?	'n		
H.323 Link Bounce Recovery? y					
Idle Traffic Interval (sec): 20					
Keep-Alive Interval (sec): 5					
Keep-Alive Count: 5					

Figure 10: IP-Network-Region Form

HV; Reviewed: SPOC 7/10/2019

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for Network Region 1. It can also be observed that the Controller IP Address is the Avaya Processor Ethernet (10.33.10.44), and that the gateway MGP IPv4 Address is 10.33.10.15. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```
display media-gateway 1
                                                              Page 1 of
                                                                           2
                           MEDIA GATEWAY 1
                   Type: g450
                  Name: g450
             Serial No: 12TGXXX00244
   Link Encryption Type: any-ptls/tls Enable CF? n
        Network Region: 1
                                           Location: 1
                                          Site Data:
          Recovery Rule: none
             Registered? y
  FW Version/HW Vintage: 40 .25 .0 /2
       MGP IPV4 Address: 10.33.10.15
       MGP IPV6 Address:
  Controller IP Address: 10.33.10.44
            MAC Address: 3c:4a:73:6b:c5:a8
  Mutual Authentication? optional
```

Figure 11: Media Gateway – Page 1

The following screen shows Page 2 for Media Gateway 1. The gateway has an MM712 media module supporting Avaya digital phones in slot V1, an MM711 supporting analog phones on slot V2, and the capability to provide announcements and music on hold via "gatewayannouncements" in logical slot V9.

```
Page 2 of 2
display media-gateway 1
                             MEDIA GATEWAY 1
                                  Type: g450
Slot Module Type
V1: MM712
                                                       DSP Type FW/HW version
MP80 170 7
                              Name
                              DCP MM
 V2: MM711
                              ANA MM
 V3:
 V4:
 V5:
 V6:
 V7:
 V8:
                                                     Max Survivable IP Ext: 8
 V9:
       gateway-announcements ANN VMM
```

Figure 12: Media Gateway – Page 2

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	16 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined in **Section 5.3**) and the **Signaling Group: 11** (Defined in **Section 5.7**) have been used. These fields are not configured in this screen, but just display the current information for the Media Server.

display media-server 1 MEI	DIA SERVER
Media Server ID:	1
Signaling Group: Voip Channel License Limit: Dedicated Voip Channel Licenses:	10
Node Name: Network Region: Location: Announcement Storage Area:	1

Figure 13: Media Server

5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**.

```
      change ip-interface procr
      IP INTERFACES

      Type: PROCR
      Target socket load: 19660

      Enable Interface? y
      Allow H.323 Endpoints? y

      Network Region: 1
      Allow H.248 Gateways? y

      IPV4 PARAMETERS
      Subnet Mask: /24
```

Figure 14: IP-Interface Form

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups.

For the compliance test, signaling group **20** was used for the signaling group between Communication Manager and Session Manager. It was used for outbound and inbound calls between the service provider and the enterprise. It was configured using the parameters highlighted below. Note: The signaling group between Communication Manager and Session Manager used for SIP phones is not mentioned in these Application Notes.

- 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 Session Manager
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager
- 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 as a Session Manager
- Set the Near-end Node Name to procr. This node name maps to the IP Address of Communication Manager as defined in Section 5.3
- Set the **Far-end Node Name** to **bvwasm2**. 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 for TLS, such as 5061

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	18 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

- 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**, the enterprise domain
- Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will re-route media traffic directly between the SIP trunk and the enterprise endpoint. Note that the Avaya G450 Media Gateway or Avaya Media Server will not remain in the media path of all calls between the SIP trunk and the endpoint
- Set the Alternate Route Timer (sec) to 6. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval
- Default values may be used for all other fields

Page 1 of 2 add signaling-group 20 SIGNALING GROUP Group Number: 20 Group Type: sig IMS Enabled? n Transport Method: tls Group Type: sip Q-SIP? n IP Video? n Enforce SIPS URI for SRTP? y Peer Detection Enabled? y Peer Server: SM Prepend '+'to Outgoing Calling/Alerting/Diverting/connected Public Numbers? y Remove '+' from Incoming Called/Calling/Alerting/Diverting/connected Numbers? n Near-end Node Name: procr Far-end Node Name: bywasm2 Near-end Listen Port: 5061 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Secondary Node Name: Far-end Domain: bvwdev.com Bypass If IP Threshold Exceeded? n Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Session Establishment Timer(min): 3 Enable Layer 3 Test? y Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Enable Layer 3 Test? y Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload IP-IP Audio Connections? y IP Audio Hairpinning? n Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6

Figure 15: Signaling-Group 20

For the compliance test, signaling group **11** was used for the signaling group between Communication Manager and Media Server. It was configured using the parameters highlighted below.

- Set the Group Type field to sip
- Set the **Transport Method** to the value of **tls** (Transport Layer Protocol). The transport method specified here is used between Communication Manager and Media Server
- Set the **Peer Detection Enabled** field to **n** and **Peer Server** to **AMS**
- Set the Near-end Node Name to procr. This node name maps to the IP Address of Communication Manager as defined in Section 5.3

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	19 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

- Set the **Far-end Node Name** to **AMS**. This node name maps to the IP Address of Media Server as defined in **Section 5.3**
- Set the Near-end Listen Port to 9061 and Far-end Listen Port to a valid unused port for TLS, such as 5071
- 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 10.33.10.47 (This is Media Server IP Address)

```
      change signaling-group 11
      Page 1 of 2

      SIGNALING GROUP
      SIGNALING GROUP

      Group Number: 11
      Group Type: sip<br/>Transport Method: tls

      Peer Detection Enabled? n Peer Server: AMS

      Near-end Node Name: procr<br/>Near-end Listen Port: 9061

      Far-end Node Name: procr<br/>Far-end Listen Port: 5071<br/>Far-end Network Region: 1

      Far-end Domain: 10.33.10.47
```

Figure 16: Signaling-Group 11

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group for Session Manager created in **Section 5.7**.

For the compliance test, trunk group **20** was used for both outbound and inbound calls to the service provider. It 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. (e.g., ***020**). Note: Refer to **Section 5.10** for adding * in dialing plan
- Set Class of Restriction (COR) to 1
- Set **Direction** to **two-way** for trunk group **20**
- Set the **Service Type** field to **public-ntwrk**
- Set Member Assignment Method to auto
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**. Trunk group 20 was associated to signaling group 20
- 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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	20 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

add trunk-group 20	Page 1	of 4
	TRUNK GROUP	
Group Number: 20	Group Type: sip CDR Repo:	rts: y
Group Name: SIP Trunks	COR: 1 TN: 1	FAC: *020
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method	: auto
	Signaling Group	: 20
	Number of Members	: 50

Figure 17: Trunk-Group – Page 1

On Page 2, set the Redirect On OPTIM Failure timer to the same amount of time as the Alternate Route Timer on the signaling group form in Section 5.7. Note that the Redirect On OPTIM Failure timer is defined in milliseconds. Verify that the Preferred Minimum Session Refresh Interval (sec) is set to a value acceptable to the service provider. This value defines the interval that UPDATEs must be sent to keep the active session alive. For the compliance test, the value of 1200 seconds was used.

add trunk-group 20 Group Type: sip TRUNK PARAMETERS Unicode Name: auto Redirect On OPTIM Failure: 6000 SCCAN? n Digital Loss Group: 18 Preferred Minimum Session Refresh Interval (sec): 1200 Disconnect Supervision - In? y Out? y XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n

Figure 18: Trunk-Group – Page 2

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end (refer to **Section 5.9** for the public-unknown-numbering format). The compliance test used 10-digit numbering format. Thus, **Numbering Format** was set to **public** and the **Numbering Format** field in the route pattern was set to **public** unk (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to y. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2** if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if an enterprise user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

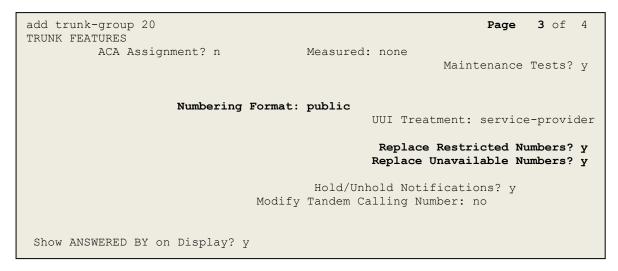


Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **y** so that CM will send SIP Refer in redirected calls or **n** so that CM will not send SIP Refer. Note: In the compliance test, Allstream supports both SIP Refer and SIP re-Invite/Update in redirected calls.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **y**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been redirected. Note: For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya Aura Messaging. The **Diversion Header** is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

add trunk-group 20 **4** of 4 Page 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? y 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

Figure 20: Trunk-Group – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "P-Asserted-Identity" headers. Since public numbering was selected to define the format of this number (**Section 5.8**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs), and it is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single public-unknown-numbering entry can be applied for all extensions. In the compliance test, stations with a 4-digit extension beginning with **01** or **02** or **03** will send the calling party number as the **CPN Prefix** plus the extension number.

Note: The entry applies to SIP connection to Session Manager, therefore the resulting number must be a complete E.164 number. Communication Manager automatically inserts a '+' in front of user number in From, P-Asserted-Identity, Contact, and Diversion headers. This plus sign will be removed by using the SIP manipulation on Avaya SBCE (See Session 7.2.3).

change public-unknown-numbering 0 NUMBERING - PUBLIC/UNKNOWN FORMAT			Page IAT	1 of	2	
Ext Ext Len Code	Trk Grp(s)	CPN Prefix	Total CPN Len			
4 01 4 02 4 03	20 20 20	647xxx 647xxx 647xxx	10 10 10			

Figure 21: Public-Unknown-Numbering Form

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 configuration is illustrated below. Use the **change dialplan analysis** command to define the **Dialed String** as following:

- Dialed String beginning with 01 or 02 or 03 for extension (ext)
- **Dialed String** beginning with **9** for feature access code (**fac**)
- **Dialed String** beginning with * for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk Group 20 in **Section 5.8**

change dialpl	lan analysi:			Page	1 of	12
		DIAL PLAN ANALYSIS TABLE Location: all	1	Percent Fi	ıll: 2	
	TotalCallLengthType4ext4ext4ext4ext4ext4ext4ext4ext4ext4ext4date	String Length Type	Dialed String			

Figure 22: Dialplan–Analysis Form

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)	2		
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialin3g List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code: *111			
Answer Back Access Code:			
Attendant Access code:			
Auto Alternate Routing (AAR) Access Code:			
Auto Route Selection (ARS) - Access Code 1: 9 Access C	ode 2:		
Automatic Callback Activation: Deactivati	on:		
Call Forwarding Activation Busy/DA: All: Deactivati	on:		
Call Forwarding Enhanced Status: Act: Deactivati	on:		
Call Park Access Code:			
Call Pickup Access Code:			
CAS Remote Hold/Answer Hold-Unhold Access Code:			
CDR Account Code Access Code:			
Change COR Access Code:			
Change Coverage Access Code:			
Conditional Call Extend Activation: Deactiv	ation:		
Contact Closure Open Code: Close C	ode:		

Figure 23: Feature–Access-Codes Form

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 20** which contains the SIP trunk group to the service provider (as defined next).

ARS DIGIT ANALYSIS TABLE Location: all Percent Full: 1 Dialed Total Route Call Node ANI	
Dialed Total Route Call Node ANI	
String Min Max Pattern Type Num Reqd	
0 1 13 20 pubu	
1613 11 11 20 pubu n	
1800 11 11 20 pubu n	
411 3 3 20 svcl n	
613 10 10 20 pubu n	
911 3 3 20 svcl n	

Figure 24: ARS–Analysis Form

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 in route pattern **20** for the compliance test.

- **Pattern Name**: Enter a descriptive name
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **20** was used
- **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 this field to **pub-unk** since public-unknown-numbering format should be used for this route (see **Section 5.8**)

change route-pattern 20 Page 1 of 3 Pattern Number: 5 Pattern Name: SP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC Mrk Lmt List Del Digits OSIG No Dqts Intw 1: 20 0 n user 2: n user 3: user n 4: n user 5: n user 6: n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts Format Subaddress 1: yyyyyn n rest pub-unk none 2: yyyyyn n rest none 3: y y y y y n n rest none 4: y y y y y n n rest none 5: ууууул п rest none 6: ууууул п rest none

Figure 25: Route–Pattern Form

Use the **change cor 1** command to change the Class of Restriction (COR) for the outbound call over SIP trunk. Set **Calling Party Restriction**: **none**. This setting allows the outbound call using feature access code (fac) 9 over SIP trunks.

1 of 23 change cor 1 Page CLASS OF RESTRICTION COR Number: 1 COR Description: FRL: 0 APLT? y Can Be Service Observed? n Calling Party Restriction: none Called Party Restriction: none Can Be A Service Observer? n Time of Day Chart: 1 Forced Entry of Account Codes? n Priority Queuing? n Direct Agent Calling? n Restriction Override: none Facility Access Trunk Test? n Restricted Call List? n Can Change Coverage? n Access to MCT? y Fully Restricted Service? n Group II Category For MFC: 7 Hear VDN of Origin Annc.? n Send ANI for MFE? n Add/Remove Agent Skills? n MF ANI Prefix: Automatic Charge Display? n Hear System Music on Hold? y PASTE (Display PBX Data on Phone)? n Can Be Picked Up By Directed Call Pickup? n Can Use Directed Call Pickup? n Group Controlled Restriction: inactive

Figure 26: Class of Restriction Form

HV; Reviewed: SPOC 7/10/2019

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

5.11. Incoming Call Handling Treatment

In general, the incoming call handling treatment 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, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by the service provider is 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 **20**. Use the **change inc-call-handling-trmt trunk-group 20** to convert incoming DID numbers as follows:

- The incoming DID number **647XXX0312** to **8000** by deleting **10** of the incoming digits for voicemail testing purpose. (8000 is voice mail pilot number)
- The incoming DID number **647XXX** to 4-digit extension by deleting **6** of the incoming digits for inbound call testing purpose

change inc-call-handling-trmt trunk-group 20 INCOMING CALL HANDLING TREATMENT				Page	1 of	3
Service/	Number	Number	Del Insert			
Feature	Len	Digits	Der Insert			
public-ntwrk	10	647xxx0312	10 8000			
-			10 8000			
public-ntwrk	10	647XXX	6			

Figure 27: Inc-Call-Handling-Trmt Form

5.12. Contact Center Configuration

This section describes the basic commands used to configure Announcements, Hunt-Groups, Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke Communication Manager to perform various call-related functions.

5.12.1. Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command "add announcement <extension>". The extension is an unused extension number.

list announcement				
Announcement	ANNO	JNCEMENTS/AUDIO SOURCES		Num of
				Num of
Extension	Туре	Name	Source	Files
1898	integrated	d SP2	001V9	1
1899	integrated	d SP1	001V9	1

Figure 28: Announcement Configuration

5.12.2. ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt-group, and agent-loginID used to queue inbound calls for handling by an agent.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

```
display hunt-group 13
                                                             Page 1 of
                                                                          3
                                HUNT GROUP
      GROUP NUMBER: 13
                                                       ACD? y
               Group Name: SP
                                                    Queue? y
           GROUP EXTENSION: 3211
                                                    Vector? y
                GROUP TYPE: UCD-MIA
                       TN: 1
                       COR: 1
                                                  MM Early Answer? n
      SECURITY CODE: 1234
                                  Local Agent Preference? n
ISDN/SIP Caller Display:
                  Queue Limit: unlimited
            Calls Warning Threshold: Port:
            Time Warning Threshold:
                                        Port:
```

Figure 29: Hunt Group Configuration – Page 1

HV; Reviewed: SPOC 7/10/2019

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note that **Skill** is set to **y**.

display hunt-group 13	HUNT GROUP	Page	2 of	3
Skill? y AAS? n	Expected Call Handling Time (sec) Service Level Target (% in sec):		0	

Figure 30: Hunt Group Configuration – Page 2

VDN 0281, shown below, is associated with vector 3

display vdn 0281			Page	1 of	3
	VECTOR DIRECTOR	Y NUMBER			
	EXTENSION: 028	1			
	Name*: Conta	act Center			
	DESTINATION: VEC	TOR NUMBER 3	3		
	Attendant Vectoring? n				
	Meet-me Conferencing? n				
	Allow VDN Override? n				
	COR: 1				
	TN*: 1				
	Measured: none	e			

Figure 31: VDN Configuration

In this simple example, vector 3 briefly plays ring back, then plays announcement 1899 (Step 02). This is an announcement heard when the call is first answered before the call is queued to the skill 13 (Step 03). If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear announcement 1898 (Step 05). Once an agent becomes available, the call will be delivered to the agent.

display vector 3 Page 1 of 6 CALL VECTOR

Number: 3 Name: Contact Center
Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y

01 wait-time 2 secs hearing ringback
02 announcement 1899
03 queue-to skill 13 pri m
04 wait-time 2 secs hearing silence
05 announcement 1898
06 goto step 3 if unconditionally

Figure 32: Vector 3 Configuration

The following screen illustrates an example agent-loginID 3311. In the sample configuration, an Avaya IP Deskphone logged in using agent-loginID 3311 and the configured password to staff and take a call for skill 13.

```
add agent-loginID 3311
                                                             Page 1 of
                                                                            2
                                 AGENT LOGINID
                Login ID: 3311
                                                                  AAS? n
                    Name: SP
                                    LWC Reception. .
LWC Log External Calls? n
AUDIX Name for Messaging:
                                                                AUDIX? n
                      TN: 1
                                                        LWC Reception: spe
                     COR: 1
           Coverage Path:
           Security Code: 1234
                                        LoginID for ISDN/SIP Display? n
                                                             Password: 1234
                                               Password (enter again): 1234
                                                         Auto Answer: station
                                                    MIA Across Skills: system
                                            ACW Agent Considered Idle: system
                                            Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time: :
```

Figure 33: Agent-loginID Configuration – Page 1

Solution & Interoperability Test Lab Application Notes33 of 111©2019 Avaya Inc. All Rights Reserved.ASCMSMSBCE80

HV; Reviewed: SPOC 7/10/2019

The following abridged screen shows Page 2 for agent-loginID 3311. Note that the Skill Number (SN) has been set to 13.

```
Display agent-loginID 3311

AGENT LOGINID

Direct Agent Skill:

Call Handling Preference: skill-level

SN RL SL SN RL SL

1: 13 1 16:

2: 17:
```

Figure 34: Agent LoginID Configuration – Page 2

Page 2 of

Page 11 of 19

Service Objective? n

Local Call Preference? n

2

To enable a telephone or one- X^{\otimes} Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to **y** as shown in the screen below.

```
change system-parameters features
FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
EAS
Expert Agent Selection (EAS) Enabled? y
Minimum Agent-LoginID Password Length: 4
```

Figure 35: Enable Expert Agent Selection

5.13. Avaya Aura[®] Communication Manager Stations

In the sample configuration, a 4-digit station extension was used with the format 0135. Use the **add station 0135** command to add an Avaya H.323 IP Deskphone.

- Enter Type: 9621, Name: H323-0135, Security Code: 1234, Coverage Path 1: 1, IP SoftPhone: y (if using this extension as a Softphone such as Avaya one-X[®] Communicator)
- Leave other values as default

Page 1 of 5 add station 0135 STATION Lock Messages? n Security Code: * Coverage Path 1: 1 Coverage Path 2: Extension: 0135 BCC: 0 TN: 1 Type: 9621 COR: 1 COS: 1 Port: S000055 Name: H323-0135 Tests? y Hunt-to Station: STATION OPTIONS Time of Day Lock Table: Loss Group: 19 Personalized Ringing Pattern: 1 Speakerphone: 2-way Display Language: English able GK Node Name: Display Language: English Button Modules: 0 Message Lamp Ext: 0135 Survivable GK Node Name: Survivable COR: internal Media Complex Ext: Survivable Trunk Dest? y IP SoftPhone? y IP Video softphone? n Short/Prefixed Registration Allowed: default Customizable Labels? Y

Figure 36: Add-Station Form

5.14. Save Avaya Aura[®] Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

6. Configure Avaya Aura® Session Manager

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

- SIP Domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Time Ranges, which define the time-based-routing
- Routing Policies, which define route destinations and control call routing between the SIP Entities
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call

It may not be necessary to create all the items above when configuring a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura[®] System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP Address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

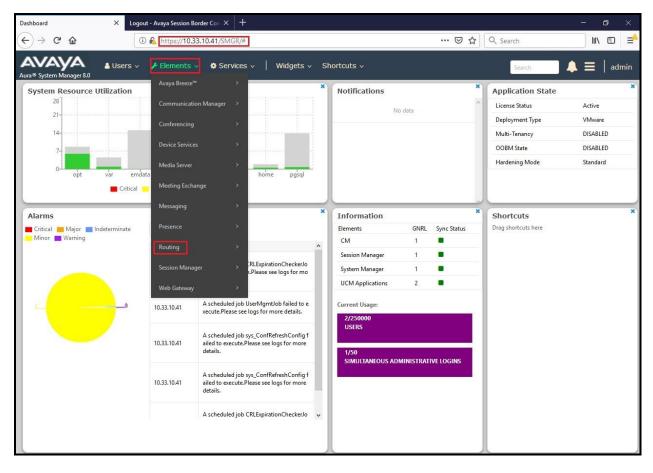


Figure 37: System Manager Home Screen

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

a® System Manager 8.0	Users v 🖌 Elements v 🌣 Services v Widgets v Shortcuts v Search 💄 🗮 adm
ome Routing	
Routing ^	Help ? Introduction to Network Routing Policy
Domains	Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.
Locations	The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:
	Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
Adaptations	Step 2: Create "Locations"
SIP Entities	Step 3: Create "Adaptations"
	Step 4: Create "SIP Entities"
Entity Links	- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
Time Ranges	- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
	- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
Routing Policies	Step 5: Create the "Entity Links"
Dial Patterns	- Between Session Managers
	- Between Session Managers and "other SIP Entities"
Regular Expressions	Step 6: Create "Time Ranges"
Defaults	- Align with the tariff information received from the Service Providers
	Step 7: Create "Routing Policies"
	- Assign the appropriate "Routing Destination" and "Time Of Day"
	(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
	Step 8: Create "Dial Patterns"
	- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"
	Step 9: Create "Regular Expressions"
	- Assign the appropriate "Routing Policies" to the "Regular Expressions"
	Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".
	IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

Figure 38: Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev.com**.

Navigate to **Routing** \rightarrow **Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), 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** (not shown) to save.

The screen below shows the existing entry for the enterprise domain.

Avra@ System Manager 8.0	Lusers ∨	Shortcuts v	Search 🔔 🚍 admin
Home Routing			
Routing	Domain Management		Help ?
Domains	New Edit Delete Duplicate More Actions •		
Locations	1 Item 🍣		Filter: Enable
Adaptations	Name	Type Notes	
SIP Entities	Select : All, None	sip	

Figure 39: Domain Management

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville-GSSCP**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing** \rightarrow **Locations** 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:

In the General section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name for the Location
- Notes: Add a brief description (optional)

Click Commit to save

AVAYA Aura © System Manager 8.0	Users 🗸 🎤 Elements 🗸 🌣 Services 🗸 Widg	jets v Shortcuts v	Search	🗌 🙏 🗮 admin
Home Routing				
Routing ^	Location Details	Commit	Canad	Help ? 🔺
Domains	Location Details	Commic	Cancel	
Locations	General			
	* Name Notes			
Adaptations	Notes			
SIP Entities	Dial Plan Transparency in Survivable Mode			
Entity Links	Enabled			
Time Ranges	Listed Directory Number			
Routing Policies	Associated CM SIP Entity			
Dial Patterns	Overall Managed Bandwidth			
Regular Expressions	Managed Bandwidth Units	Kbit/sec 🗸		
Defaults	Total Bandwidth			
Deraults	Multimedia Bandwidth			
	Audio Calls Can Take Multimedia Bandwidth			
	Per-Call Bandwidth Parameters			
	Maximum Multimedia Bandwidth (Intra-Location)	2000 Kbit/Sec		
	Maximum Multimedia Bandwidth (Inter-Location)	2000 Kbit/Sec		
	* Minimum Multimedia Bandwidth			
	* Default Audio Bandwidth	80 Kbit/sec 🗸		
<	Alarm Threshold			
	Overall Alarm Threshold	80 🗸 ‰		~

Figure 40: Location Configuration

HV; Reviewed: SPOC 7/10/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. In the Location Pattern section, click Add to enter IP Address Pattern. The following patterns were used in testing:

- IP Address Pattern: 10.33.10.*, 10.33.5.*, 10.10.98.*
- Click **Commit** to save

*	Notes	
	notes	

Figure 41: IP Ranges Configuration

Note: Call bandwidth management parameters should be set per customer requirement.

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager, which includes Communication Manager and Avaya SBCE.

Navigate to **Routing** \rightarrow **SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

Name: Enter a descriptive name FODN or IP Address: Enter the FODN or IP Address of the SIP Entity that is used for SIP signaling Select Session Manager for Session Manager, CM for Type: Communication Manager and SIP Trunk for Avaya SBCE This field is only present if **Type** is not set to **Session Manager**. Adaptation: Adaptation modules were not used in this configuration Select the Location that applies to the SIP Entity being created. For Location: the compliance test, all components were located in Location **Belleville-GSSCP** Time Zone: Select the time zone for the Location above

In this configuration, there are three SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **bvwasm2**. The IP Address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.43**. The user will need to select the specific values for the **Location** and **Time Zone**.

Avra® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🏟 Services 🗸 ╞ Widg	ets v Shortcuts v	Search 💄 🗮 🛛 admin
Home Routing			
Routing ^	SIP Entity Details	Commit Cancel	Help ? 🔨
Domains	General		
Locations		bvwasm2	
Adaptations	* IP Address: SIP FQDN:	10.33.10.43	
SIP Entities		Session Manager	
Entity Links	Notes:	SM	
Time Ranges	Location:	Belleville-GSSCP	
	Outbound Proxy:	~	
Routing Policies	Time Zone:	America/Toronto	
Dial Patterns	Minimum TLS Version:	Use Global Setting 🗸	
Regular Expressions	Credential name:		
N C (1)	Monitoring		
Defaults	SIP Link Monitoring:	Use Session Manager Configuration \checkmark	
	CRLF Keep Alive Monitoring:	CRLF Monitoring Disabled	

Figure 42: Session Manager SIP Entity

To define the ports used by Session Manager, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Listen Ports** section, click **Add** and enter the following values. Use default values for all remaining fields:

- Port: Port number on which Session Manager listens for SIP requests
- **Protocol**: Transport protocol to be used with this port
- **Default Domain**: The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain

Defaults can be used for the remaining fields. Click **Commit** (not shown) to save

The compliance test used port **5061** with **TLS** for connecting to Communication Manager and Avaya SBCE

Listen Ports TCP Failover port: TLS Failover port:				
Add Remove				
4 Items 🍣				Filter: Enable
Listen Ports	*	Protocol Default Domain	Notes	
5061		TLS bvwdev.com		
Select : All, None				

Figure 43: Session Manager SIP Entity Port

6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **CM8**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP Address of Communication Manager **10.33.10.44**. Note that **CM** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

Aura® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🗳	FServices ∨ Widge	ets v Shortcuts v Search 🌲 🗮 🛛 admin
Home Routing			
Routing ^	SIP Entity Details		Commit Cancel
Domains	General		
Locations		* Name:	CM8
Adaptations		* FQDN or IP Address:	
		Туре:	CM
SIP Entities		Notes:	
Entity Links		Adaptation:	×
Time Ranges		Location:	Belleville-GSSCP v
Routing Policies		L	America/Toronto
Routing Policies	* SIP	Timer B/F (in seconds):	
Dial Patterns		Minimum TLS Version:	Use Global Setting 🗸
Regular Expressions		Credential name: Securable:	
Defaults		Call Detail Recording:	
	Loop Detection	Loop Detection Mode:	Off
		Loop Detection Plote.	
	Monitoring	SIP Link Monitoring:	Link Monitoring Enabled

Figure 44: Communication Manager SIP Entity

6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **SBCE**. The **FQDN** or **IP Address** field is set to the IP Address of the SBCE's private network interface **10.10.98.111**. Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA Aura® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🕻	Services v Widge	gets v Shortcuts v Search 🗼 🚍 admin
Home Routing			
Routing ^	SIP Entity Details		Commit Cancel
Domains	General		
Locations		* Name:	
Adaptations		* FQDN or IP Address:	
SIP Entities		Type: Notes:	SIP Trunk
SIP Entities		notes.	
Entity Links		Adaptation:	
Time Ranges			Belleville-GSSCP v
Routing Policies			: America/Toronto
	* SIP	Timer B/F (in seconds): Minimum TLS Version:	
Dial Patterns		Credential name:	
Regular Expressions		Securable:	
Defaults		Call Detail Recording:	egress 🗸
	Loop Detection		
		Loop Detection Mode:	On v
		Loop Count Threshold:	5
	Loop Dete	ction Interval (in msec):	: 200
	Monitoring		
		SIP Link Monitoring:	Link Monitoring Enabled

Figure 45: Avaya SBCE SIP Entity

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by the service provider traffic and one to the Avaya SBCE.

To add an Entity Link, navigate to **Routing** \rightarrow Entity Links in the left-hand navigation pane and click on the New button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

- Name: Enter a descriptive name
- SIP Entity 1: Select the Session Manager being used
- **Protocol**: Select the transport protocol used for this link
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	45 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

- SIP Entity 2: Select the name of the other system as defined in Section 6.4
- **Port**: Port number on which the other system receives SIP requests from the Session Manager
- **Connection Policy**: Select **trusted**. **Note**: If **trusted** is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied

Click **Commit** to save

The following screen illustrates 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 5.7**.

AVAYA Aura® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🕴	Services 🗸 Widgets 🗸	Shortcuts v			Search		∃ admin
Home Routing								
Routing ^	Entity Links			Commi	t Cancel			Help ?
Domains	Linery Lines							
Locations	1 Item 🏾							Filter: Enable
Adaptations	□ Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
SIP Entities	SM_CM_TLS_5061	* Q bywasm2	TLS 🗸	* 5061	* Q СМ8	* 5061		trusted 🗸
Entity Links	< Select : All, None							>

Figure 46: Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4**, **7.2.6** and **7.4.3**.

© System Manager 8.0 me Routing	占 Users 🦄	🗸 🎤 Elements 🗸 🤹	Services v Widgets v	Shortcuts 🗸				Se	arch	▲ =	admin
uting ^ Domains		ity Links			Comm	t Cancel					He
	1 Ite	m @									Filter: Enal
Adaptations		Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
SIP Entities											

Figure 47: Avaya SBCE Entity Link

6.6. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a Time Range, select **Routing** \rightarrow **Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.

AVAYA Aura® System Manager 8.0	🛔 Users 🗸	🖌 🔑 Elem	ents v	Servic	es v	Wid	gets 🗸	Shorto	cuts v			Search	▲ ≡	admin
Home Routing														
Routing	Tim	e Rang	es											Help ?
Domains	New	Edit D	elete) (C	uplicate	More	Actions	•							
Locations	1 Ite	im											Filter	: Enable
Adaptations		Name	Мо	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes		
on r an		24/7	~	~	~	~	~	V	V	00:00	23:59	Time Range 2	4/7	
SIP Entities	Selec	t : All, None												
Entity Links														
Time Ranges														



6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added; one for Communication Manager and one for Avaya SBCE.

To add a Routing Policy, navigate to **Routing** \rightarrow **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	47 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

- Name: Enter a descriptive name
- Notes: Add a brief description (optional)

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies 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 Details** for the policy named **Allstream Inbound Calls** associated with incoming PSTN calls from Allstream to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM8**.

Aura® System	and the second se	🛓 Users 🗸 🎤 Elen	ients 🗸 🔅 Services 🔇	V Widgets V Shortcuts V		Si	earch	🕽 📃 admi
Home	Routing ×							
Routing			licy Details		Commit Cance	The second se		Help ?
Domai		General						
Locatio Condit				* Name: Allstream Inbound Ca	alls			
Condit				* Retries: 0				
SIP Ent				Notes:				
		SIP Entity as	Destination					
Entity	Links	Select	FQDN or IP Ad	ddrocs		Туре	Notes	
Time R	langes	СМ8	10.33.10.44	MI1532		CM	Hores	
		<						>

Figure 49: Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **Allstream Outbound Calls** associated with outgoing calls from Communication Manager to the PSTN via Allstream SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

AVAYA Aura® System Manager 8.0	🛓 Users 🗸 🍃 Elemer	its 🗸 🔅 Services 🗸	Widgets v Shortcuts v		Sea	arch	🔳 admin
Home Routing ×							
	Routing Poli	cy Details		Commit Cancel			Help ?
Domains Locations	General		* Name: Allstream Outbound C	alls			
Conditions		ſ	Disabled: * Retries: 0				
Adaptations	~		Notes:				
SIP Entities	SIP Entity as De	estination					
Entity Links	Select						
Time Ranges	Name	FQDN or IP A			Туре	Notes	
Routing Policies	SBCE	10.10.98.111	1		SIP Trunk		>

Figure 50: Routing to Allstream SIP Trunk

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to Allstream SIP Trunk through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing** \rightarrow **Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

٠	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
- 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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	49 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

Location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns were similarly defined.

The first example shows that outbound 11-digit dialed numbers that begin with **1613** and have a destination **SIP Domain** of **bvwdev.com** uses **Routing Policy Name** as **Allstream Outbound Calls** which is defined in **Section 6.7**.

Avra® System Manager 8.0	🛿 Users 🗸 🖌 Elements 🗸 🔷 Services 🗸 📔 Widgets 🗸 Shortcuts 🗸 💦 Search 🤇	≡ admin
Home Routing ×		
Routing ^	Dial Pattern Details	Help ?
Domains	General	
Locations	* Pattern: 1613	
Conditions	* Min: 4	
Adaptations v	Max: 11 Emergency Call:	
SIP Entities	SIP Domain: bvwdev.com	
Entity Links	Notes: Allstream Outbound Calls	
Time Ranges	Originating Locations and Routing Policies	
Routing Policies	Add Remove	
Routing Policies	1 Item 🍣	Filter: Enable
Dial Patterns ^	Originating Location Name Notes Routing Policy Name Rank Disabled Destination Note	iting Policy es
Dial Patterns	Allstream Outbound 0 SBCE	>
Outsingting Dist Des	Select : All, None	

Figure 51: Dial Pattern_1613

Note that with the above Dial Pattern, Allstream did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed back to the PSTN.

The second example shows that inbound 10-digit numbers that start with **647** use **Routing Policy Name** as **Allstream Inbound Calls** which is defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Allstream.

Aura® System Manager 8.0	Users v 🖌 Elements v 🌣 Services v 🛛 Widgets v Shortcuts v Search 🔰 🚊 🗍 admin
Home Routing ×	
Routing	Help ? Dial Pattern Details
Domains	General
Locations	* Pattern: 647
Conditions	* Min: 3 * Max: 36
Adaptations 🗸 🗸	Emergency Call:
SIP Entities	SIP Domain: bvwdev.com
Entity Links	Notes: Allstream Inbound Calls
Time Ranges	Originating Locations and Routing Policies
Routing Policies	Add Remove
Dial Patterns ^	Originating Location Name, Originating Location Notes Routing Policy Name Rank Routing Policy Disabled Routing Policy Destination Routing Policy Notes
Dial Patterns	-ALL- Allstream Inbound Calls 0 CM8
	Select : All, None

Figure 52: Dial Pattern_647

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

D 11										
me Routing ×										
outing	^		l Patte	rne						He
Domains			Falle	ins						
Domains		New	Edit	Delete		plicate More Actio	ns 🔹			
Locations			~							Filter: Ena
		-	ems 🍣 Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Filter: Ena
Conditions			Q	1	13		chiergency rype	Emergency Phoney	bywdey.com	Allstream Outbound Calls
Adaptations	~		011	3	36				bywdev.com	Allstream Outbound Calls
Adaptations			013	3	4				bywdev.com	Allstream SIP phones
SIP Entities			02	2	36				bywdey.com	Allstream SIP phones
			03	2	36				bywdey.com	Allstream SIP phones
Entity Links			1613	4	11				bywdev.com	Allstream Outbound Calls
			1800	4	36				bywdev.com	Allstream Outbound Calls
Time Ranges			411	3	36				bvwdev.com	Allstream Outbound Calls
			613	3	36				bvwdev.com	Allstream Outbound Calls
Routing Policies			647	3	36				bvwdev.com	Allstream Inbound Calls
			911	3	36				bywdey.com	Allstream Outbound Calls

Figure 53: Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

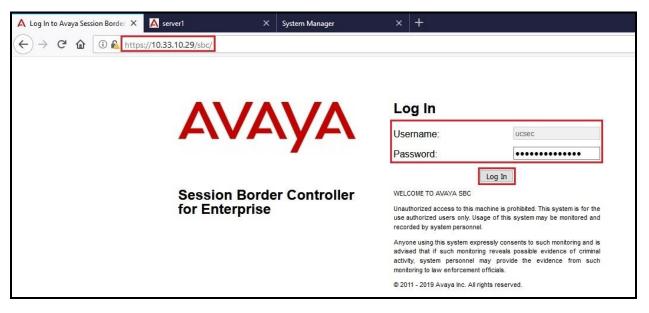
This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the Allstream.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Allstream system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, refer to the documentation listed in **Section 11** of these Application Notes.

7.1. Log in to Avaya Session Border Controller for Enterprise

Access the web interface by typing "**https://x.x.x/sbc/**" (where x.x.x.x is the management IP of the Avaya SBCE).



Enter the Username and Password and click on Log In button.

Figure 54: Avaya SBCE Login

Select **Device SBCE** and the **Dashboard** main page will appear as shown below.

Session Dorug	er Controller for	Enterprise			AVA	АУА
MS Dashboard	Dashboard					
evice Management	Information			Installed Devices		
ackup/Restore System Parameters	System Time	02:30:35 PM EDT	Refresh	EMS		
Configuration Profiles	Version	8.0.0.0-19-16991		SBCE		
Services	Build Date	Sat Jan 26 21:58:11 UTC 2019				
Domain Policies	License State	ØOK				
TLS Management	Aggregate Licensing Overages	0				
Network & Flows DMZ Services	Peak Licensing Overage Count	0				
Monitoring & Logging	Last Logged in at	04/30/2019 12:10:11 EDT				
	Failed Login Attempts	0				
	Active Alarms (past 24 hours)			Incidents (past 24 hours)		
	None found.			SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		

Figure 55: Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **SBCE** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

Device: SBCE 🗸 Alarms	Incidents Status 🛩 Lo	ogs♥ Diagnostics User	s		Se	ettings 🗸 🛛 I	lelp 🗸	Log Out
Session Bord	er Controller	for Enterprise	9				AV	AYA
EMS Dashboard Device Management	Device Managem	nent						
Backup/Restore System Parameters 	Devices Updates	SSL VPN Licensing Key	y Bundles					
Configuration Profiles	Device Name	Management IP Vers	ion Status					
 Services Domain Policies 	SBCE	10.33.10.29 8.0.0	0.0-19-16991 Commissioned	Reboot	Shutdown Restart Appl	ication View	Edit Un	install

Figure 56: Avaya SBCE Device Management

The System Information screen shows General Configuration, Device Configuration, Network Configuration, DNS Configuration and Management IP(s) information provided during installation and corresponds to Figure 1.

			System Info	rmation: SBCE			x
General Configu	ation		Device Configurat	ion	- Dynamic License Alloc	ation ——	
Appliance Name	SBCE		HA Mode	No		Min License Allocation	Max License Allocation
Box Type			Two Bypass Mode	NO		ShOod And Addition	and the second second
Deployment Mode	Proxy				Standard Sessions	0	0
		1.9			Advanced Sessions	0	0
					Scopia Video Sessions	0	0
					CES Sessions	0	0
					Transcoding Sessions	0	0
					CLID		
					Encryption Available: Yes		
Network Configu	ration						
IP		Public IP	Ne	twork Prefix or Subnet Mas	sk Gateway		Interface
10.10.98.111		10.10.98.111	25	5.255.255.224	10.10.98.97		B1
10.10.98.123		10.10.98.123	25	5.255.255.224	10.10.98.97		B1
10.10.98.14		10.10.98.14	25	5.255.255.192	10.10.98.1		A1
10.10.98.34		10.10.98.34	25	5.255.255.192	10.10.98.1		A1
DNS Configuration	'n		Management IP(s)				
Primary DNS	10.10.98.60		IP #1 (IPv4) 1	0.33.10.29			
Secondary DNS			1				
DNS Location	DMZ						
DNS Client IP	10.10.98.111						

Figure 57: Avaya SBCE System Information

7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Configure Server Interworking Profile - Avaya Site

Server Interworking profile allows administrator to configure and manage various SIP call server specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Configuration Profiles** \rightarrow **Server Interworking**

- Select avaya-ru in Interworking Profiles
- Click Clone
- Enter Clone Name: SMVM and click Finish (not shown)
- Select **SMVM** in **Interworking Profiles**
- Select General tab and click Edit button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that Session Manager server interworking profile (named: SMVM) was added.

evice: SBCE 	Incidents Status ✓ Logs	➤ Diagnostics Users		Settings 🗸 🛛 F	lelp 🖌 🛛 Log O
Session Borde	er Controller fo	or Enterprise			AVAYA
MS Dashboard Device Management	Interworking Profile	s: SMVM		Rename	Clone Delete
ackup/Restore	Interworking Profiles	ř.	Click here to add a description.	Kellallie	Clotte
System Parameters	cs2100		Click here to add a description.		
Configuration Profiles Domain DoS		General Timers Privacy URI Manip	ulation Header Manipulation Advance	ed	
Server Interworking	avaya-ru	General			
Media Forking	SMVM	Hold Support	NONE		
Routing		180 Handling	None		
Topology Hiding		181 Handling	None		
Signaling Manipulation		182 Handling	None		
URI Groups		-	None		
SNMP Traps		183 Handling			
Time of Day Rules FGDN Groups		Refer Handling	No		
Reverse Proxy Policy		URI Group	None		
Services		Send Hold	No		
Domain Policies		Delayed Offer	Yes		
TLS Management		3xx Handling	No		
Network & Flows		Diversion Header Support	No		
DMZ Services		Delayed SDP Handling	No		
Monitoring & Logging		Re-Invite Handling	No		
		Prack Handling	No		
		Allow 18X SDP	No		
		T.38 Support	Yes		
		URI Scheme	SIP		
		Via Header Format	RFC3261		
			Edit		

Figure 58: Server Interworking – Avaya site

HV; Reviewed: SPOC 7/10/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. 56 of 111 ASCMSMSBCE80

7.2.2. Configure Server Interworking Profile – Allstream SIP Trunk Site

From the menu on the left-hand side, select Configuration Profiles \rightarrow Server Interworking \rightarrow Add

- Enter **Profile Name**: **SP4** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)
- Select **SP4** in **Interworking Profiles**
- Select **General** tab and click **Edit** button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that Allstream server interworking profile (named: SP4) was added.

Device: SBCE Υ Alarms Ir	ncidents Status 🛩 Log	gs♥ Diagnostics Users		Settings 🗸 Help 🖌 Lo	og Ou
Session Border	r Controller f	or Enterprise		AVA	٩
EMS Dashboard Device Management	Interworking Profi	es: SP4		Rename Clone De	elete
Backup/Restore System Parameters	Interworking Profiles		Click here to add a description.		
Configuration Profiles Domain DoS	cs2100 avaya-ru	General Timers Privacy URI Mani	ulation Header Manipulation Advance	d	
Server Interworking Media Forking	SMVM	General Hold Support	NONE		
Routing Topology Hiding Signaling Manipulation	SP5	180 Handling 181 Handling	None		
URI Groups SNMP Traps		182 Handling 183 Handling	None None		
Time of Day Rules FGDN Groups		Refer Handling URI Group	No None		
Reverse Proxy Policy Services		Send Hold	No		
Domain Policies TLS Management		Delayed Offer βxx Handling	Yes No		
Network & Flows DMZ Services		Diversion Header Support Delayed SDP Handling	No No		
Monitoring & Logging		Re-Invite Handling	No		
		Prack Handling Allow 18X SDP	No		
		T.38 Support URI Scheme	Yes		
		Via Header Format	RFC3261		
			Edit		

Figure 59: Server Interworking – Allstream SIP Trunk site

7.2.3. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

From the menu on the left-hand side, select Configuration Profiles \rightarrow Signaling Manipulation \rightarrow Add

- Enter script **Title**: **SP4**. In the script editing window, enter the text exactly as shown in the below screenshot to perform the following:
 - Manipulate the SIP headers for outbound calls
 - Remove un-wanted headers
 - Modify user of SIP URI in PAI header on off-net call forward
 - Modify the SIP OPTION
 - Manipulate URI.USER in Contact headers of "180 Ringing" and "183 Session Progress" and "200 OK" responded by Allstream. (See Section 2.2 for observation in detail)
 - Click Save (not shown)

Device: SBCE 🛩 Alarms	Incidents Status ❤ Logs	⊧♥ Diagnostics Users	Settings 🗸	Help 🗸	Log Out
Session Borde	r Controller f	or Enterprise		AV	AYA
EMS Dashboard Device Management Backup/Restore	Signaling Manipula	tion Scripts: SP4	Download	d Clone	Delete
 System Parameters Configuration Profiles Domain DoS Server Interworking Media Forking Routing Topology Hiding Signaling Manipulation URI Groups SMMP Traps 	Signaling Manipulation Scripts One-X Communicator SP4-1 SP4	Click here to add a description. Signaling Manipulation within session "ALL" { act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" { //Manipulate headers %HEADERS["-rnom"][1].URI.USER.regex_replace("(\+",""); %HEADERS["Outract"][1].URI.USER.regex_replace("(\+)",""); %HEADERS["Outract"][1].URI.USER.regex_replace("(\+)",""); %HEADERS["Outract"][1].URI.USER.regex_replace("(\+)",""); %HEADERS["Outract"][1].URI.USER.regex_replace("(\+)",""); %HEADERS["Untact"][1].URI.USER.regex_replace("(\+)",""); %HEADERS["Untact"][1].URI.USER.regex_replace("(\+)",""); %HEADERS["Untact"][1].URI.USER.regex_replace("(\+)",""); %HEADERS["History-Info"][3]); remove(%HEADERS["History-Info"][2]);			
Time of Day Rules FGDN Groups Reverse Proxy Policy Domain Policies TLS Management Network & Flows DMZ Services Monitoring & Logging		<pre>remove(%HEADERS["History-Info"][1]); //Modify user of SIP URI in PAI header on Call Forward Off-net if (%HEADERS["Diversion"][1].regex_match("reason")) then { act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" } //Modify the OPTIONS %HEADERS["Request_Line"][1].regex_replace("sip:metaswitch@10.10.98.14:5006 %HEADERS["Request_Line"][1].regex_replace("sip:metaswitch@10.10.98.14:5006 act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" { //Modify URI.USER in Contact header of 180 Ringing/183 Session Progress/2000 CK con act on response where %DIRECTION="108DUMD" and %ENTRY_POINT="AFTER_NETWORK" and or %RESP_CODE="183" or %RESP_CODE="200" { %HEADERS["Contact"][1].URI.USER = %HEADERS["To"][1].URI.USER; } }</pre>	0","sip:10.10.98 ming from Allstro	.14:5060"); eam	
) Edit			

Figure 60: Signaling Manipulation

Note: See **Appendix B** in **Section 13** for the reference of this signaling manipulation (SigMa) script.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	58 of 111
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.	ASCMSMSBCE80

7.2.4. Configure Server – Avaya Site

The **SIP Servers** screen contains six tabs: **General**, **Authentication**, **Heartbeat**, **Registration**, **Ping** and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server specific parameters such as port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select Services \rightarrow SIP Servers \rightarrow Add

Enter Profile Name: SMVM

On **General** tab, enter the following:

- Server Type: Select Call Server
- **TLS Client Profile**: Select **AvayaSBCClient**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
- IP Address/FQDN: 10.33.10.43 (Session Manager IP Address)
- Port: 5061
- Transport: TLS
- Click **Finish** (not shown)

Device: SBCE 🗸 Alarms	Incidents Status 🗸 Logs 🕯	 Diagnostics Users 		Settings 🗸 Help 🖌 Log Out
Session Bord	er Controller fo	r Enterprise		AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters	SIP Servers: SMVM Add Server Profiles	General Authentication Hearth	eat Registration Ping Advanced	Rename Clone Delete
 Configuration Profiles Services SIP Servers LDAP 	SMVM	Server Type TLS Client Profile DNS Query Type	Call Server AvayaSBCClient NONE/A	
RADIUS Domain Policies TLS Management Network & Flows 		IP Address / FQDN 10.33.10.43	Port 5061 Edit	Transport TLS

Figure 61: SIP Server – General - Avaya site

On the **Advanced** tab:

- Enable Grooming box is checked
- Select SMVM for Interworking Profile (see Section 7.2.1)
- Click **Finish** (not shown)

General Authentication	Heartbeat Registration Ping	Advanced	
Enable DoS Protection			
Enable Grooming			
Interworking Profile	SMVM		
Signaling Manipulation Script	None		
Securable			
Enable FGDN			
Tolerant			
URI Group	None		
	Ed	Jit	

Figure 62: SIP Server – Advanced - Avaya site

7.2.5. Configure Server – Allstream SIP Trunk

From the menu on the left-hand side, select Services \rightarrow SIP Servers \rightarrow Add There are 2 signaling servers on Allstream site for redundancy purposes. The signaling server IP addresses are 192.168.209.100 (Allstream site 1) and 192.168.72.60 (Allstream site 2)

Enter Profile Name: AS1

On General tab, enter the following:

- Server Type: Select Trunk Server
- IP Address/FQDN: 192.168.209.100 (Allstream signaling server 1 IP address)
- Port: 5060
- Transport: UDP
- Click **Finish** (not shown)



Figure 63: SIP Server – General – Allstream site 1

On **Heartbeat** tab, enter the following:

- Check Enable Heartbeat
- Select Method: OPTIONS
- Set Frequency: 60 seconds
- Input From URI: ping@10.10.98.14 (Avaya SBCE public interface IP address)
- Input To URI: ping@192.168.209.100 (Allstream signaling server 1 IP address)

e Heartbeat	
ethod	OPTIONS
requency	60 seconds
rom URI	ping@10.10.98.14
) URI	ping@192.168.209.100

Figure 64: SIP Server – Heartbeat – Allstream site 1

On the **Advanced** tab, enter the following:

- Interworking Profile: SP4 (see Section 7.2.2)
- Signaling Manipulation Script: SP4 (see Section 7.2.3)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping	Advanced			
Enable D	loS Protection							
Enable G	Grooming							
Interwork	ing Profile		SP4					
Signaling	Manipulation Scrip	t	SP4					
Securabl	e							
Enable F	GDN							
Tolerant								
URI Grou	iþ		Non	e				
				Ed	lit			

Figure 65: SIP Server – Advanced – Allstream site 1

Enter **Profile Name: AS2**

On **General** tab, enter the following:

- Server Type: Select Trunk Server
- IP Address/FQDN: 192.168.72.60 (Allstream signaling server 2 IP address)
- Port: 5060
- Transport: UDP
- Click **Finish** (not shown)

Session Bord	er Controller f	or Enterprise				AV	/AYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles < Services	SIP Servers: AS2 Add Server Profiles SMVM AS2	Server Type	Trunk St		Rename	Clone	Delete
SIP Servers LDAP RADIUS Domain Policies TLS Management	AS1	DNS Query Type IP Address / FQDN 192.168.72.60	NONE/A	Port 5060 Edit	Transport UDP		

Figure 66: SIP Server – General – Allstream site 2

HV; Reviewed: SPOC 7/10/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. On **Heartbeat** tab, enter the following:

- Check Enable Heartbeat
- Select Method: OPTIONS
- Set Frequency: 60 seconds
- Input From URI: ping@10.10.98.14 (Avaya SBCE public interface IP address)
- Input **To URI**: **ping@192.168.72.60** (Allstream signaling server 2 IP address)

eral Autho	entication	Heartbeat	Registration	Ping	Advanced
nable Heartbea	ıt				
Method			OP	TIONS	
Frequency			60 s	seconds	
From URI			ping	@10.10.	98.14
To URI			ping	@192.16	8.72.60
				Ec	lit

Figure 67: SIP Server – Heartbeat – Allstream site 2

On the **Advanced** tab, enter the following:

- Interworking Profile: SP4 (see Section 7.2.2)
- Signaling Manipulation Script: SP4 (see Section 7.2.3)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping Advanced
Enable D	loS Protection			
Enable G	rooming			
Interwork	ing Profile		SP4	
Signaling	Manipulation Script	t	SP4	
Securabl	e			
Enable F	GDN			
Tolerant				
URI Grou	p		None	e
				Edit

Figure 68: SIP Server – Advanced – Allstream site 2

7.2.6. Configure Routing – Avaya Site

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server Addresses and resolution methods, next hop routing information, and packet transport types.

From the menu on the left-hand side, select Configuration Profiles \rightarrow Routing and click Add as highlighted below.

Enter Profile Name: AS_To_SMVM and click Next button (Not Shown)

- Select Load Balancing: Priority
- Check Next Hop Priority
- Click Add button to add a Next-Hop Address
- Priority/Weight: 1
- SIP Server Profile: SMVM (see Section 7.2.4)
- Next Hop Address: 10.33.10.43:5061 (TLS) (Session Manager IP address)
- Click Finish

Device: SBCE - Alarms In	cidents Status 🛩 Logs	✓ Diagnostics	Users			Settings 🗸	Help 👻 Log Out
Session Border	Controller fo	or Enterpr	ise				AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters Configuration Profiles	Routing Profiles: AS Add Routing Profiles default	S_To_SMVM		Click h	ere to add a description.	Rena	me Clone Delete
Domain DoS Server Interworking	To SMVM RW	Roduing Provine	_	Add Routing Ru	ıle	_	x
Media Forking Routing	URI Group	* ~			Time of Day	default 🗸	
Topology Hiding	Load Balancing	Priority	~		NAPTR		
Signaling Manipulation URI Groups	Transport	None 🗸			LDAP Routing		
SNMP Traps	LDAP Server Profile	None 🖂			LDAP Base DN (Search)	None \vee	
Time of Day Rules	Matched Attribute Priority				Alternate Routing		
FGDN Groups Reverse Proxy Policy	Next Hop Priority				Next Hop In-Dialog		
Services	Ignore Route Header						
Domain Policies TLS Management Network & Flows	ENUM				ENUM Suffix		
 DMZ Services Monitoring & Logging 							Add
	Priority / Weight LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	e Next Hop Address	Trans	port
	1			SMVM	√ 10.33.10.43:5061 (TLS) ~ None	e v Delete
				Finish			

Figure 69: Routing to Session Manager

HV; Reviewed: SPOC 7/10/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. 66 of 111 ASCMSMSBCE80

7.2.7. Configure Routing – Allstream SIP Trunk Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select Configuration Profiles \rightarrow Routing and click Add as highlighted below.

Enter Profile Name: SMVM_To_AS and click Next button (not shown)

- Load Balancing: Priority
- Check Next Hop Priority
- Click **Add** button to add a Next-Hop Address
- Priority/Weight: 1; Server Configuration: AS1 (see Section 7.2.5); Next Hop Address: 192.168.209.100:5060 (UDP) (Allstream signaling server 1 IP address)
- Priority/Weight: 2; Server Configuration: AS2 (see Section 7.2.5); Next Hop Address: 192.168.72.60:5060 (UDP) (Allstream signaling server 2 IP address)
- Click **Finish**

Device: SBCE - Alarms Inc	cidents Status 🗸 Logs	 Diagnostics 	Users			Setting	gs 🗙 Help 👻 Log Out
Session Border	Controller fo	or Enterp	orise				AVAYA
EMS Dashboard Device Management Backup/Restore System Parameters	Routing Profiles: SN Add Routing Profiles	/VM_To_AS	_	Ci Routing Profile	ick here to add a description. e		Rename Clone Delete
Domain DoS Server Interworking	URI Group	* ~			Time of Day	default 🗸	Add
Media Forking Routing Topology Hiding	Load Balancing Transport	Priority None ~	~		NAPTR LDAP Routing		
Signaling Manipulation URI Groups	LDAP Server Profile Matched Attribute Priority	None 🗸			LDAP Base DN (Search) Alternate Routing	None 🗸	Delete
SNMP Traps Time of Day Rules FGDN Groups	Next Hop Priority Ignore Route Header				Next Hop In-Dialog		_
Reverse Proxy Policy Services Domain Policies 	ENUM				ENUM Suffix		
TLS Management Network & Flows DMZ Services	Priority / LDAP Search / Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	e Next Hop Address	Transport	Add
Monitoring & Logging	Veight Attribute			AS1 AS2	 192.168.209.100:5060 192.168.72.60:5060 (0) 		Delete Delete
				Back Fini	ish		

Figure 70: Routing to Allstream SIP Trunk

7.2.8. Configure Topology Hiding

The **Topology Hiding** screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select Configuration Profiles \rightarrow Topology Hiding

- Select default in Topology Hiding Profiles
- Click Clone
- Enter Clone Name: AS_To_SMVM and click Finish (not shown)
- Select **AS_To_SMVM** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **To**,
 - In the Criteria column select IP/Domain
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bvwdev.com**
- For the Header **Request-Line**,
 - In the Criteria column select IP/Domain
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bvwdev.com** Note: bvwdev.com is SIP Domain of enterprise
- For the Header **From**,
 - In the Criteria column select IP/Domain
 - In the **Replace Action** column select: **Overwrite** In the **Overwrite Value** column: **bvwdev.com**

Click **Finish** (not shown)

Session Borde	r Controller f	or Enterpris	e		AV	АУА
EMS Dashboard	Topology Hiding P	rofiles: AS To SMV	M			
Device Management	Add				Rename Clone	Delete
Backup/Restore System Parameters	Topology Hiding Profiles		Clici	where to add a description.		
Configuration Profiles Domain DoS	default	Topology Hiding				
Server Interworking	cisco_th_profile	Header	Criteria	Replace Action	Overwrite Value	
Media Forking	AS_To_SMVM	То	IP/Domain	Overwrite	bwwdev.com	
Routing		Referred-By	IP/Domain	Auto	-	
Topology Hiding		Request-Line	IP/Domain	Overwrite	bvwdev.com	
Signaling Manipulation		Via	IP/Domain	Auto		
URI Groups SNMP Traps		Refer-To	IP/Domain	Auto	<u></u>	
Time of Day Rules		Record-Route	IP/Domain	Auto		
FGDN Groups		SDP	IP/Domain	Auto		
Reverse Proxy Policy		From	IP/Domain	Overwrite	bwwdev.com	
Services			a vo striain	o to think	prinder.com	

Figure 71: Topology Hiding To Session Manager

From the menu on the left-hand side, select Configuration Profiles \rightarrow Topology Hiding

- Select default in Topology Hiding Profiles
- Click Clone
- Enter Clone Name: SMVM_To_AS and click Finish (not shown)

Session Borde	er Controller	for Enterprise	2		AVAYA
EMS Dashboard Device Management	Topology Hiding	Profiles: SMVM_To_A	S		Rename Clone Delete
Backup/Restore System Parameters 	Topology Hiding Profiles		Click	chere to add a description.	
Configuration Profiles	default	Topology Hiding			
Server Interworking	cisco_th_profile	Header	Criteria	Replace Action	Overwrite Value
Media Forking	SMVM_To_AS	То	IP/Domain	Auto	
Routing	AS_To_SMVM	Referred-By	IP/Domain	Auto	
Topology Hiding	-	Request-Line	IP/Domain	Auto	-
Signaling Manipulation URI Groups		Via	IP/Domain	Auto	-
SNMP Traps		Refer-To	IP/Domain	Auto	
Time of Day Rules		Record-Route	IP/Domain	Auto	
FGDN Groups		SDP	IP/Domain	Auto	-
Reverse Proxy Policy Services		From	IP/Domain	Auto	
Domain Policies				Edit	

Figure 72: Topology Hiding To Allstream

7.3. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

7.3.1. Create Application Rules

Application rules define the type of SBC-based Unified Communication (UC) applications Avaya SBCE protects. You can also determine the maximum number of concurrent voice and video sessions that your network can process before resource exhaustion.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Application Rules**

- Select **default** from **Application Rules** and click **Clone** button:
- Enter Clone Name (e.g., SIP-Trunk) and click Finish (not shown)
- Click on **SIP-Trunk** from **Application Rules**, then click **Edit** button:
- In the **Audio** field:
 - Check In and Out
 - Enter an appropriate value in the **Maximum Concurrent Sessions** field (e.g., **2000**), and the same value in the **Maximum Session Per Endpoint** field
 - Leave the **CDR Support** field at **Off** and the **RTCP Keep-Alive** field unchecked (**No**)

Device: SBCE - Alarms	Incidents Status 🛩 Logs	s♥ Diagnostics Users			Settings 🗸	Help 🖌 Log Out
Session Borde	er Controller f	or Enterprise				AVAYA
EMS Dashboard	Application Rules:	SIP-Trunk				
Device Management	Add				Renam	ne Clone Delete
Backup/Restore System Parameters	Application Rules		Click h	ere to add a description.		
Configuration Profiles	default	Application Rule				
Services	default-trunk					
Domain Policies	default-subscriber-low	Application Type	In	Out Maximum Concurrent Sess	ions Maximum Se	essions Per Endpoint
Application Rules	default-subscriber-high	Audio		2000	2000	
Border Rules	0	Video				
Media Rules	default-server-low					
Security Rules	default-server-high	Miscellaneous				
Signaling Rules	SIP-Trunk	CDR Support	Off			
Charging Rules		RTCP Keep-Alive	No			
End Point Policy	RW_AR	Teror receptance	110			
Groups				Edit		
Session Policies		L				

Click on **Finish** (not shown)

Figure 73: Application Rule

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

7.3.2. Create Media Rules

Media Rules allow one to define 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.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Media Rules**

- Select the **default-low-med-enc** rule, click **Clone**. Enter **Clone Name**: **SMVM** Click **Finish** (not shown)
- Select SMVM under Media Rules to Edit

The Encryption tab indicates that RTP and SRTP_AES_CM_128_HMAC_SHA1_80 encryption was used as **Preferred Formats** for Audio Encryption.

Device: SBCE - Alarms	Incidents Status V Logs	 Diagnostics Users 		Settings 🗸 Help 🖌 Log Out
Session Borde	er Controller fo	or Enterprise		AVAYA
EMS Dashboard Device Management Backup/Restore System Parameters	Media Rules: SMVM Add Media Rules	И	Click here to add a description.	Rename Clone Delete
 Configuration Profiles Services Domain Policies Application Rules 	default-low-med default-low-med-enc default-high	Encryption Codec Prioritization Audio Encryption Preferred Formats	RTP	
Border Rules Media Rules Security Rules Signaling Rules	default-high-enc avaya-low-med-enc	Encrypted RTCP MKI	SRTP_AES_CM_128_HMAC_SH	141_30
Charging Rules End Point Policy Groups Session Policies	SP4	Lifetime Interworking Video Encryption	Any	
TLS Management Network & Flows DMZ Services		Preferred Formats Interworking	RTP	
Monitoring & Logging		Miscellaneous Capability Negotiation	Edit	

Figure 74: Media Rule 1

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Media Rules**

• Select the **default-low-med** rule, click **Clone**. Enter **Clone Name**: **SP4** Click **Finish** (not shown)

Session Bord	er Controller f	or Enterprise		AVAYA
EMS Dashboard	Media Rules: SP4			
Device Management	Add			Rename Clone Delete
Backup/Restore	Media Rules		Click here to add a description.	
 System Parameters Configuration Profiles 	default-low-med			
 Services 	default-low-med-enc	Encryption Codec Priorit	tization Advanced QoS	
Domain Policies		Audio Encryption		
Application Rules	default-high	Preferred Formats	RTP	
Border Rules	default-high-enc	Interworking		
Media Rules	avaya-low-med-enc	Interworking		
Security Rules	SMVM	Video Encryption		
Signaling Rules	SP4	Preferred Formats	RTP	
Charging Rules	3F4	Interworking		
End Point Policy		Interworking	M	
Groups		Miscellaneous		
Session Policies		Capability Negotiation		
TLS Management		Oupublicy regenation		
Network & Flows			Edit	
 DMZ Services Monitoring & Logging 				

Figure 75: Media Rule 2

7.3.3. Create Signaling Rules

In the reference configuration, Signaling Rules are used to filter various SIP headers.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Signaling Rules**

- Select the **default** rule, click **Clone**. Enter **Clone Name**: **SIP-Trunk**. Click **Finish** (not shown)
- Select SIP-Trunk under Signaling Rules
- Select the Signaling QoS tab and click on Edit button
- Verify that **Enabled** is selected
- Select **DCSP**
- Select Value = EF
- Click Finish (not shown)

Device: SBCE - Alarms	Incidents Status 🗸 Log	js ❤ Diagnostics	Users			Sel	ttings 🗸	Help 🗸	Log Out
Session Bord	er Controller f	or Enterpr	ise					AV	/AYA
EMS Dashboard Device Management Backup/Restore	Signaling Rules: S Add Signaling Rules	IP-Trunk		Click b	ere to add a description		Rename	Clone	Delete
 System Parameters Configuration Profiles Services 	default No-Content-Type-Ch	General Reques	sts Responses	Request Headers	Response Headers		UCID		
Domain Policies Application Rules	SIP-Trunk	Signaling QoS QoS Type		⊠ DS0	P				
Border Rules Media Rules		DSCP		EF					
Security Rules Signaling Rules Charging Rules					Edit				

Figure 76: Signaling Rule

7.3.4. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): Application, Border, Media, Signaling, Security, Charging and RTCP Monitoring Report Generation, each of which was created using the procedures contained in the previous sections. A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **End Point Policy Groups**

- Select Add.
- Enter Group Name: SMVM
 - Application Rule: SIP-Trunk (See in Section 7.3.1)
 - Border Rule: default
 - Media Rule: SMVM (See in Section 7.3.2)
 - Security Rule: default-low
 - Signaling Rule: SIP-Trunk (See in Section 7.3.3)
- Select **Finish** (not shown)

Device: SBCE 🛩 Alarms	Incidents Status 🗸 Log		ostics Use					Settings	✔ He	lp 🗸 Log (
Session Bord	er Controller f	or Ent	erprise	e						AVAY	4
EMS Dashboard	Policy Groups: SN	IVM									
Device Management	Add							Re	name (Clone Delete	
Backup/Restore System Parameters	Policy Groups				Click	here to add a desc	ription.				
Configuration Profiles	default-low	-			Hover ov	er a row to see its o	description.				ή
Services	default-low-enc										
Domain Policies	default-med	Policy Gro	oup								_
Application Rules Border Rules	default-med-enc								_	Summary	
Media Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Gen	Mon	
Security Rules	default-high-enc	1	SIP-Trunk	default	SMVM	default-low	SIP-Trunk	None	Off	Edit	1
Signaling Rules	avaya-def-low-enc		-								
Charging Rules	avaya-def-high-subsc										
Groups	avaya-def-high-server										
Session Policies	SMVM										
 TLS Management Network & Flows 	SP4										
 DMZ Services 	SMVM_RW										

Figure 77: Endpoint Policy 1

From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups**

- Select Add.
- Enter Group Name: SP4
 - Application Rule: SIP-Trunk (See in Section 7.3.1)
 - Border Rule: default
 - Media Rule: SP4 (See in Section 7.3.2)
 - Security Rule: default-low
 - Signaling Rule: SIP-Trunk (See in Section 7.3.3)
- Select **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🛩 Log	s ∨ Diagr	nostics User	s				Settings	• н	lelp 🗸	Log Out
Session Bord	er Controller f	or Ent	terprise	9						AV	/AYA
EMS Dashboard Device Management Backup/Restore	Policy Groups: SP	4						Re	ename	Clone	Delete
 System Parameters Configuration Profiles Services 	Policy Groups default-low default-low-enc					: here to add a deso er a row to see its o					
Domain Policies Application Rules Border Rules	default-med default-med-enc	Policy Gr	oup							Sur	mmary
Media Rules Security Rules	default-high default-high-enc	Order	Application	Border	Media	Security	Signaling	Charging	RTCF Gen	^o Mon	
Signaling Rules Charging Rules	avaya-def-low-enc avaya-def-high-subsc	1	SIP-Trunk	default	SP4	default-low	SIP-Trunk	None	Off		Edit
End Point Policy Groups Session Policies	avaya-def-high-server										
 TLS Management Network & Flows 	SP4										
 DMZ Services Monitoring & Logging 	SMVM_RW										

Figure 78: Endpoint Policy 2

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.4.1. Manage Network Settings

From the menu on the left-hand side, select Network & Flows → Network Management.

- Select **Networks** tab and click the **Add** button to add a network for the outside interface as follows:
 - Name: Network_A1
 - Default Gateway: 10.10.98.1
 - Subnet Mask: 255.255.255.192
 - Interface: A1 (This is the Avaya SBCE outside interface)
 - Click the Add button to add the IP Address for inside interface: 10.10.98.14
 - Click the **Finish** button to save the changes

Device: SBCE 🗸 Alarms	Incidents Status 🗸 Logs	✓ Diagnostics Users		Settings 🛩	Help 🖌 Log Out
Session Borde	r Controller fo	or Enterprise			AVAYA
EMS Dashboard Device Management Backup/Restore P System Parameters	Network Managem	ent			
 Configuration Profiles Services Domain Policies TLS Management 	Name	Gateway Subnet Ma Length	ask / Prefix Interface	IP Address	Add
 Network & Flows 	Network_B1		Add Network		X Edit Delete
Network Management Media Interface Signaling Interface End Point Flows Session Flows	Network_A1	Name Default Gateway Network Prefix or Subnet Mask Interface	Network_A1 10.10.98.1 255.255.255.192 A1 ~		Edit Delete
Advanced Options DMZ Services				Add	
Monitoring & Logging			Alic IP Gateway (e IP Address Use Defau Finish		

Figure 79: Network Management – Outside Interface

From the menu on the left-hand side, select **Network & Flows** → **Network Management**.

- Select **Networks** tab and click **Add** button to add a network for the inside interface as follows:
 - Name: Network_B1
 - Default Gateway: 10.10.98.97
 - Subnet Mask: 255.255.255.224
 - Interface: B1 (This is the Avaya SBCE inside interface)
 - Click the Add button to add the IP Address for outside interface: 10.10.98.111
 - Click the **Finish** button to save the changes

Device: SBCE V Alarms	Incidents Status 🗸 Logs 🗸	Diagnostics Users		Settings 🗸	Help 🖌 Log Out
Session Borde	r Controller fo	r Enterprise			AVAYA
EMS Dashboard Device Management Backup/Restore System Parameters	Network Managemer	nt			
Configuration Profiles					Add
 Services Domain Policies 	Name	Gateway Subnet Mask / I Length	Prefix Interface	IP Address	
 TLS Management Network & Flows 	Network_B1		Add Network		X Edit Delete
Network Management Media Interface Signaling Interface End Point Flows Session Flows	Network_A1	Name Default Gateway Network Prefix or Subnet Mask Interface	Network_B1 10.10.98.97 255.255.224 B1 ~		Edit Delete
Advanced Options DMZ Services Monitoring & Logging 		IP Address Public IP 10.10.98.111 Use IP Address	Gateway Override	Add Delete	

Figure 80: Network Management – Inside Interface

From the menu on the left-hand side, select Network & Flows → Network Management

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state

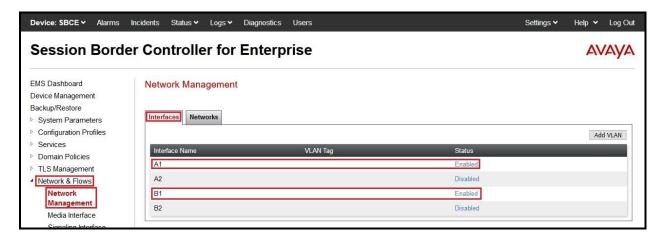


Figure 81: Network Management – Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the IP Addresses and port ranges in which the Avaya SBCE will accept media streams on each interface. The default media port range on the Avaya SBCE can be used for inside port.

From the menu on the left-hand side, **Device Specific Settings** \rightarrow **Media Interface**

- Select the **Add** button and enter the following:
- Name: OutsideMedia
- IP Address: Select Network_A1 (A1,VLAN0) and 10.10.98.14 (External IP address toward Allstream)
- Port Range: 35000 40000
- Click **Finish** (not shown)
- Select the **Add** button and enter the following:
 - Name: InsideMedia
 - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (Internal IP address toward Session Manager)
 - Port Range: 35000 40000
 - Click **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🗸	Diagnostics	Users	Settings 🗸	Help 🗸	Log Out
Session Borde	er Controller for	Enterp	rise		AN	VAYA
EMS Dashboard Device Management	Media Interface					
Backup/Restore System Parameters	Media Interface					
Configuration Profiles	h					Add
 Services Domain Policies 	Name		Media IP Network	Port Range		
TLS Management	OutsideMedia		10.10.98.14 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
 Network & Flows Network Management 	InsideMedia		10.10.98.111 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete
Media Interface Signaling Interface						

Figure 82: Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select Network & Flows → Signaling Interface

- Select the **Add** button and enter the following:
 - Name: OutsideUDP
 - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.14** (External IP address toward Allstream)
 - UDP Port: 5060
 - Click **Finish** (not shown)

From the menu on the left-hand side, select Network & Flows → Signaling Interface

- Select the **Add** button and enter the following:
 - Name: InsideTLS
 - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (Internal IP address toward Session Manager)
 - TLS Port: 5061
 - **TLS Profile:** AvayaSBCServer. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
 - Click **Finish** (not shown)

Note: For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 the same as Allstream used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

Device: SBCE 🗸 Alarms	Incidents Status 🗸 Logs 🕻	 Diagnostics 	Users				Settir	ngs ∨ ⊦	lelp 🗸	Log Out
Session Borde	er Controller fo	r Enterp	rise						AV	AYA
EMS Dashboard Device Management Backup/Restore	Signaling Interface									
 System Parameters Configuration Profiles Services 	Signaling Interface									Add
Domain Policies	Name	Signaling IF Network		TCP Port	UDP Port	TLS Port	TLS Profile			
 TLS Management Network & Flows 	OutsideUDP	10.10.98.14 Network_A1 (A			5060		None		Edit	Delete
Network Management	InsideTLS	10.10.98.11 Network_B1 (F				5061	AvayaSBCServer		Edit	Delete
Media Interface Signaling Interface End Point Flows	L									

Figure 83: Signaling Interface

7.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize trunk-side signaling and apply a policy.

7.4.4.1 Create End Point Flows – SMVM Flow

From the menu on the left-hand side, select **Network & Flows** → **End Point Flows**

- Select the Server Flows tab
- Select Add, enter Flow Name: SMVM Flow
 - Server Configuration: SMVM (see Section 7.2.4)
 - URI Group: *
 - Transport: *
 - Remote Subnet: *
 - Received Interface: OutsideUDP (see Section 7.4.3)
 - Signaling Interface: InsideTLS (see Section 7.4.3)
 - Media Interface: InsideMedia (see Section 7.4.2)
 - Secondary Media Interface: None
 - End Point Policy Group: SMVM (see Section 7.3.4)
 - Routing Profile: SMVM_To_AS (see Section 7.2.7)
 - Topology Hiding Profile: AS_To_SMVM (see Section 7.2.8)
 - Leave other parameters as default
 - Click Finish

Device: SBCE 🛩 Alarms In							🛩 Help	> 👻 Log Ou	
Session Border	r Contro	oller for Enterpr	ise					AVAYA	1
EMS Dashboard Device Management Backup/Restore In System Parameters	End Point								
 Configuration Profiles Services 			Add Flow	×				Add	
 Domain Policies 	Modification	Flow Name	SMVM Flow						
 TLS Management Network & Flows 		SIP Server Profile	SMVM ~			_			
Network Management	- SIP Serve	URI Group	* ~	Pe	uting Profile	-	_		
Media Interface Signaling Interface		Transport	* ~						
End Point Flows		Remote Subnet	*	A	S_To_SMVM	View		Delete	
Session Flows Advanced Options	SIP Serve	Received Interface	OutsideUDP ~		_	_	_	_1	
 DMZ Services 	Priority	Signaling Interface	InsideTLS ~	Ro	uting Profile				
Monitoring & Logging	1	Media Interface	InsideMedia 🗸 🗸	As	6_To_SMVM	View	Clone Edit	Delete	
	_ SIP Serve	Secondary Media Interface	None ~						
	Update	End Point Policy Group	SMVM ~						
	Priority	Routing Profile	SMVM_To_AS ~	iuti				_	
	1	Topology Hiding Profile	AS_To_SMVM ~	ı∕ı.	VI_To_AS	View	Clone Edit	Delete	
	2	Signaling Manipulation Script	None	л∨л	M_To_SP4-1	View	Clone Edit	Delete	
	3	Remote Branch Office	Any ~	fau	It_RW	View (Clone Edit	Delete	
	SIP Serve	Link Monitoring from Peer							
	Priority		Finish	uti	ng Profile				7

Figure 84: End Point Flow 1

7.4.4.2 Create End Point Flows – Allstream SIP Trunk Flow

From the menu on the left-hand side, select Network & Flows \rightarrow End Point Flows There are 2 Server Flows associated to 2 Allstream signaling servers.

- Select the Server Flows tab
- Select Add, enter Flow Name: AS1 Flow
 - Server Configuration: AS1 (see Section 7.2.5)
 - URI Group: *
 - Transport: *
 - Remote Subnet: *
 - Received Interface: InsideTLS (see Section 7.4.3)
 - Signaling Interface: OutsideUDP (see Section 7.4.3)
 - Media Interface: OutsideMedia (see Section 7.4.2)
 - Secondary Media Interface: None
 - End Point Policy Group: SP4 (see Section 7.3.4)
 - Routing Profile: AS_To_SMVM (see Section 7.2.6)
 - Topology Hiding Profile: SMVM_To_AS (see Section 7.2.8)
 - Leave other parameters as default

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes
SPOC 7/10/2019	©2019 Avaya Inc. All Rights Reserved.

- Click Finish

ession Border (Contr	oller for Enterp	rise				1	AVAY
S Dashboard vice Management skup/Restore System Parameters	End Poir							
Configuration Profiles			Add Flow	×				Add
Services Jomain Policies	Modificatio	Flow Name	AS1 Flow					
LS Management		SIP Server Profile	AS1 v					
letwork & Flows Network Management	SIP Serv	URI Group	* ~			_	-	
Media Interface	Priority	Transport	* ~	F	Routing Profile			
Signaling Interface End Point Flows	1	Remote Subnet	*	P	NS_To_SMVM	View Clone	Edit	Delete
Session Flows	SIP Serv	Received Interface	InsideTLS 🗸 🗸					
Advanced Options DMZ Services	Priority	Signaling Interface	OutsideUDP ~	R				
Ionitoring & Logging	1	Media Interface	OutsideMedia 🗸	F	S_To_SMVM	View Clone	Edit	Delete
		Secondary Media Interface	None ~					
	Update	End Point Policy Group	SP4 v					
	Priority	Routing Profile	AS_To_SMVM ~	ou				
	1	Topology Hiding Profile	SMVM_To_AS ~	M	/M_To_AS	View Clone	Edit	Delete
	2	Signaling Manipulation Script	None	M	/M_To_SP4-1	View Clone		Delete
	3	Remote Branch Office	Any ~	efa	ult RW	View Clone	Edit	Delete
		Link Monitoring from Peer						

Figure 85: End Point Flow 2

From the menu on the left-hand side, select Network & Flows → End Point Flows

- Select the Server Flows tab
- Select Add, enter Flow Name: AS2 Flow
 - Server Configuration: AS2 (see Section 7.2.5)
 - URI Group: *
 - Transport: *
 - Remote Subnet: *
 - Received Interface: InsideTLS (see Section 7.4.3)
 - Signaling Interface: OutsideUDP (see Section 7.4.3)
 - Media Interface: OutsideMedia (see Section 7.4.2)
 - Secondary Media Interface: None
 - End Point Policy Group: SP4 (see Section 7.3.4)
 - Routing Profile: AS_To_SMVM (see Section 7.2.6)
 - Topology Hiding Profile: SMVM_To_AS (see Section 7.2.8)
 - Leave other parameters as default
 - Click Finish

Device: SBCE 🗸 Alarms In	cidents Stat	us 🗸 Logs 🖌 Diagnostics	Users		i i i i i i i i i i i i i i i i i i i	Settings 🛩	Help	✓ Log Out	
Session Border	Contro	oller for Enterp	rise					AVAYA	
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	End Point		Add Flow	×					
 Services 	Modificatio			^		_	_	Add	
 Domain Policies TLS Management 	Modificate	Flow Name SIP Server Profile	AS2 Flow				_		
Network & Flows	_ SIP Serv	URI Group	* v						
Network Management Media Interface	Priority	Transport	* v		Routing Profile				
Signaling Interface	1	Remote Subnet	*		AS_To_SMVM	View Clo	e Edit	Delete	
End Point Flows Session Flows	⊢ SIP Serv	Received Interface	InsideTLS ~						
Advanced Options DMZ Services	Priority	Signaling Interface	OutsideUDP ~		Routing Profile		_		
 Monitoring & Logging 	1	Media Interface	OutsideMedia V		AS_To_SMVM	View Clo	e Edit	Delete	
		Secondary Media Interface	None ~						
	SIP Serv	End Point Policy Group	SP4 ~						
	Priority	Routing Profile	AS_To_SMVM ~		outing Profile				
		Topology Hiding Profile	SMVM_To_AS ~		MVM_To_AS	View Clo	e Edit	Delete	
	2	Signaling Manipulation Script	None ~		MVM_To_SP4-1	View Cla	e Edit	Delete	
	3	Remote Branch Office	Any ~		efault_RW	View Clo	e Edit	Delete	
		Link Monitoring from Peer							
	- SIP Serv		Finish		outina Profile				

Figure 86: End Point Flow 3

8. Allstream SIP Trunk Configuration

Allstream is responsible for the configuration of Allstream SIP Trunk Service. Customer must provide the IP Address used to reach the Avaya SBCE public interface at the enterprise. Allstream will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Allstream. Allstream also provides the Allstream SIP Specification document for reference. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between Allstream SIP Trunk and the enterprise is a static IP Address configuration.

9. Verification Steps

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 useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

- 1. 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.
- 2. 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.
- 3. Verify that the user on the PSTN can end an active call by hanging up.
- 4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

- 1. Communication Manager: Enter the following commands using the Communication Manager System Access Terminal (SAT) interface.
 - **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 station** <extension number> Displays signaling and media information for an active call on a specific station.
 - **status trunk-group** <trunk-group number> Displays trunk-group state information.
 - **status signaling-group** <signaling-group number> Displays signaling-group state information.
- 2. Session Manager:
 - Call Routing Test The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to Elements → Session Manager → System Tools → Call Routing Test. Enter the requested data to run the test.
 - **traceSM** Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
- 3. Avaya SBCE: Debug logging can be started in two different ways:
 - GUI of the SBC: Monitoring & Logging → Debugging. Check on Debug option
 - SIP only: enable LOG_SUB_SIPCC subsystem under SSYNDI process.
 - CALL PROCESSING: enable all subsystems under SSYNDI process.
 - The log files are stored at: /usr/local/ipcs/log/ss/logfiles/elog/SSYNDI.
 - **Command Line Interface**: Login with root user and enter the command: **#traceSBC**. The tool updates the database directly based on which trace mode is selected.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura[®] Communication Manager, Avaya Aura[®] Session Manager and Avaya Session Border Controller for Enterprise to Allstream. This solution successfully passed compliance testing via the Avaya DevConnect Program.

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at: <u>http://support.avaya.com/</u>

Avaya Aura® Session Manager/System Manager

- [1] Administering Avaya Aura[®] Session Manager, Release 8.0.1, Issue 3, December 2018
- [2] Administering Avaya Aura® System Manager, Release 8.0.1, Issue 6, January 2019

Avaya Aura[®] Communication Manager

[3] Administering Avaya Aura ®Communication Manager, Release 8.0.1, Issue 3, December 2018

Avaya Phones

- [4] Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones H.323, Issue 2, March 2018
- [5] Installing and Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones SIP, Issue 3, March 2018
- [6] Avaya one-X® Communicator Release 6.2 SP13 Release Notes, Issue 1.0, February 2019
- [7] Avaya Equinox® Client (Windows) Release 3.5.5 (Feature Pack) Release Notes, Issue 1.1, April 2019

Avaya Session Border Controller for Enterprise

[8] Avaya Session Border Controller for Enterprise 8.0 Release Notes, Release 8.0.0.0, Issue 1 November 2018

IETF (Internet Engineering Task Force) SIP Standard Specifications

[9] RFC 3261 SIP: Session Initiation Protocol, <u>http://www.ietf.org/</u>

Product documentation for Allstream SIP Trunking may be found at: <u>https://allstream.com/solutions/sip-trunking/</u>

12. Appendix A – Remote Worker Configuration

This section describes the process for connecting remote Avaya SIP endpoints on the public Internet, access through the Avaya SBCE to Session Manager on the private enterprise. It builds on the Avaya SBCE configuration described in previous sections of this document.

In the reference configuration, an existing Avaya SBCE is provisioned to access the Allstream SIP Trunk Services (see **Section 2.1** of this document). The Avaya SBCE also supports Remote Worker configurations, allowing remote SIP endpoints (connected via the public Internet) to access the private enterprise.

Supported endpoints are Avaya 96x1 SIP Deskphones, Avaya one- $X^{\text{®}}$ Communicator SIP softphone and Avaya EquinoxTM for Windows SIP softphone.

Note: In the compliance testing, only Avaya one- $X^{\mathbb{R}}$ Communicator SIP softphone was used to test as the remote worker.

Standard and Advanced Session Licenses are required for the Avaya SBCE to support Remote Workers. Contact an authorized Avaya representative for assistance if additional licensing is required. The settings presented here illustrate a sample configuration and are not intended to be prescriptive.

12.1. Network Management on Avaya SBCE

The following screen shows the **Network Management** of the Avaya SBCE. The Avaya SBCE is configured with two "outside" IP Addresses assigned to physical interface A1, and two "inside" IP Addresses assigned to physical interface B1.

Note: A SIP Entity in Session Manager was not configured for the Avaya SBCE's internal IP Address used for Remote Worker. This keeps the Remote Worker interface untrusted in Session Manager, thereby allowing Session Manager to properly challenge user registration requests.

These are the IP Addresses used in the reference configuration:

- **10.10.98.14** is the Avaya SBCE "outside" IP address previously provisioned for SIP Trunking with Allstream (see Section 7.4.1)
- **10.10.98.34** is the new Avaya SBCE "outside" IP address for Remote Worker access to Session Border Controller
- **10.10.98.111** is the Avaya SBCE "inside" IP address previously provisioned for SIP Trunking with Session Manager (see Section 7.4.1)
- **10.10.98.123** is the new Avaya SBCE "inside" IP address for Remote Worker access to Session Manager

From the menu on the left-hand side, select Network & Flows → Network Management

- Enter the above **IP** Addresses and Gateway Addresses for both the Inside and the Outside interfaces
- Select the physical interface used in the **Interface** column accordingly

Session Bord	er Controller	for Enterpris	se			AVAY
EMS Dashboard	Network Manage	ement				
Device Management	J					
ackup/Restore		-				
System Parameters	Interfaces Network	(S				
Configuration Profiles						Add
Services			Subnet Mask / Prefix			
Domain Policies	Name	Gateway	Length	Interface	IP Address	
			055 055 055 004	B1	10.10.98.111,	Edit Delete
TLS Management Network & Flows	Network_B1	10.10.98.97	255.255.255.224	51	10.10.98.123	Edit Doroto

Figure 87: Network Management

On the **Interfaces** tab, verify that Interfaces **A1** and **B1** are both set to **Enabled** as previously configured for the Allstream SIP Trunk access in **Section 7.4.1**.

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🖌 Diagno	ostics Users	Se	ttings ❤ Help ❤ Log Out
Session Bord	er Controller for Ent	erprise		Αναγα
EMS Dashboard Device Management Backup/Restore	Network Management			
 Configuration Profiles 				Add VLAN
 Services Domain Policies TLS Management 	Interface Name	VLAN Tag	Status Enabled	
 Network & Flows Network Management 	A2 B1		Disabled Enabled	
Media Interface Signaling Interface	B2		Disabled	

Figure 88: Network Interface Status

12.2. Media Interface on Avaya SBCE

From the menu on the left-hand side, select **Device Specific Settings** \rightarrow **Media Interface**

- Select the **Add** button and enter the following:
 - Name: OutsideMedRW
 - **IP Address**: Select **Network_A1 (A1, VLAN0)** and **10.10.98.34** (External IP address toward Remote Worker phones)
 - Port Range: 35000 40000
 - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
 - Name: InsideMedRW
 - **IP Address**: Select **Network_B1 (B1, VLAN0)** and **10.10.98.123** (Internal IP address toward Session Manager)
 - Port Range: 35000 40000
 - Click **Finish** (not shown)

Session Borde	er Controller for Ent	erprise		AVA
EMS Dashboard Device Management Backup/Restore	Media Interface			
System Parameters Configuration Profiles	Media Interface			Add
 Services Domain Policies 	Name	Media IP Network	Port Range	
TLS Management	OutsideMedia	10.10.98.14 Network_A1 (A1. VLAN 0)	35000 - 40000	Edit Delet
Network & Flows Network Management	InsideMedia	10.10.98.111 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit Delet
Media Interface Signaling Interface	OutsideMedRW	10.10.98.34 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit Delet
End Point Flows	InsideMedRW	10.10.98.123 Network B1 (B1, VLAN 0)	35000 - 40000	Edit Delet

Figure 89: Media Interface

Note: Media Interface **OutsideMedRW** is used in the Remote Worker Subscriber Flow (Section 12.8.1), and Media Interface **InsideMedRW** is used in the Remote Worker Server Flow (Section 12.8.2.1).

12.3. Signaling Interface on Avaya SBCE

The following screen shows the Signaling Interface settings. Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

Select the Add button to create Signaling Interface OutsideSIGRW using the parameters:

- IP Address: Select Network_A1 (A1, VLAN0) and 10.10.98.34 (External IP address toward Remote Worker phones)
- TLS Port: 5061
- **TLS Profile:** AvayaSBCServer. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use
- Click on **Finish** (not shown)

Select the Add button to create Signaling Interface InsideSIGRW using the parameters:

- IP Address: Select Network_B1 (B1, VLAN0) and 10.10.98.123 (Internal IP address toward Session Manager)
- TLS Port: 5061
- **TLS Profile:** AvayaSBCServer. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use

Session Borde	er Controller for	r Enterprise					AN	/AY
EMS Dashboard	Signaling Interface							
Device Management	0 0							
Backup/Restore								
System Parameters	Signaling Interface							
Configuration Profiles								Add
Services	Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Domain Policies	Name	Network	ΙΟΡ Ροπ	UDP Port	ILS Port	ILS Profile		
TLS Management	OutsideUDP	10.10.98.14 Network A1 (A1, VLAN 0)	532	5060		None	Edit	Delete
 Network & Flows 		10.10.98.111			5061		Edit	
Network Management	InsideTLS	Network_B1 (B1, VLAN 0)			5061	AvayaSBCServer	Edit	Delete
Media Interface Signaling Interface	OutsideSIGRW	10.10.98.34 Network_A1 (A1, VLAN 0)			5061	AvayaSBCServer	Edit	Delete
End Point Flows	InsideSIGRW	10.10.98.123			5061	AvayaSBCServer	Edit	Delete

• Click on **Finish** (not shown)

Figure 90: Signaling Interface

Note: Signaling Interface **OutsideSIGRW** is used in the Subscriber Flows (**Section 12.8.1**), and in the Remote Worker Server Flow (**Section 12.8.2.1**). Signaling Interface **InsideSIGRW** is used in the Remote Worker Server Flow (**Section 12.8.2.1**).

12.4. Routing Profile on Avaya SBCE

The Routing Profile **To_SMVM_RW** is created for routing the SIP traffic from Remote Worker to Session Manager via Avaya SBCE.

From the menu on the left-hand side, select **Configuration Profiles** \rightarrow **Routing** \rightarrow **Add**

Enter Profile Name: To_SMVM_RW (not shown)

- Load Balancing: Priority
- Check Next Hop Priority
- Click Add button to add a Next-Hop Address
- Priority/Weight: 1
- SIP Server Profile: SMVM
- Next Hop Address: 10.33.10.43:5061 (TLS) (IP address of Session Manager)
- Click **Finish**

The Routing Profile **To_SMVM_RW** is used in the Subscriber Flows (**Section 12.8.1**).

Device: SBCE - Alarms In					Help 🖌 Log Out
Session Border	Controller fo	r Enterprise			AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters Configuration Profiles Domain DoS Server Interworking Media Forking	Routing Profiles: To Add Routing Profiles default SP4_To_SMVM SMVM_To_SP4	SMVM_RW Routing Profile Update Priority	Click here to add a description.	Renam	e Clone Delete
Routing			Routing Profile		x
Topology Hiding Signaling Manipulation	URI Group	* ~	Time of Day	default 🗸	Delete
URI Groups	Load Balancing	Priority ~	NAPTR		
SNMP Traps	Transport	None 🗸	LDAP Routing		
Time of Day Rules FGDN Groups	LDAP Server Profile	None 🗸	LDAP Base DN (Search)	None 🗸	_
Reverse Proxy Policy	Matched Attribute Priority		Alternate Routing		
 Services Domain Policies 	Next Hop Priority		Next Hop In-Dialog		_
 TLS Management 	Ignore Route Header				
Network & Flows					_
 DMZ Services Monitoring & Logging 	ENUM		ENUM Suffix		
5 55 5					Add
	Priority / Weight 1	LDAP Search LDAP Search Regex Pattern Regex Result	SIP Server Profile Next Hop Address SMVM International In	S) V	✓ Delete

Figure 91: Remote Worker Routing to Session Manager

The Routing Profile **default_RW** is created for routing SIP traffic from Session Manager to Remote Worker via Avaya SBCE.

From the menu on the left-hand side, select Configuration Profiles \rightarrow Routing \rightarrow Add Enter Profile Name: default_RW

- Check Load Balancing: DNS/SRV
- **NAPTR** box is checked
- Click **Finish**

The Routing Profile default_RW is used in the Remote Worker Server Flow in Section 12.8.2.1.

Device: SBCE - Alarms In	cidents Status ❤ Logs *	 Diagnostics 	Users				Settings 🗸	Help 🗸	Log Out
Session Border	Controller fo	r Enterp	rise					AVA	ΔΥΑ
		•							_
EMS Dashboard	Routing Profiles: det	fault_RW							
Device Management Backup/Restore	Add						Rename	Clone	Delete
System Parameters	Routing Profiles			Cl	ick here to add a description.				
Configuration Profiles Domain DoS	default	Routing Profile							
Server Interworking	SP4_To_SMVM	Update Priority							Add
Media Forking	SMVM_To_SP4	Priority URI C	Group Time of Day	Load Balan	icing Next Hop Addre	ss	Transport		
Routing Topology Hiding		1 *	default	Routing Profil	Auto-Detect.		Auto-Detect	Fair x	elete
Signaling Manipulation		*	1	reading i rem					
URI Groups	URI Group				Time of Day	default ~			
SNMP Traps Time of Day Rules	Load Balancing	DNS/SRV	~		NAPTR				
FGDN Groups	Transport	None 🗸			LDAP Routing				
Reverse Proxy Policy	LDAP Server Profile	None 🗸			LDAP Base DN (Search)	None \vee			
 Services Domain Policies 	Matched Attribute Priority				Alternate Routing				
 TLS Management 	Next Hop Priority				Next Hop In-Dialog				
Network & Flows	Ignore Route Header								
 DMZ Services Monitoring & Logging 									
workoring a Logging	ENUM				ENUM Suffix				
								Add	
		10 10.00 Mag	-						
	Click the Add buttor	to add a Next-H	Hop Address.						
				Back Fin	hish				

Figure 92: Remote Worker Default Routing

12.5. User Agent on Avaya SBCE

User Agents are created for each type of endpoints tested. In this compliance testing, Avaya one-X Communicator is used as the User Agent.

From the menu on the left-hand side, select **System Parameters** \rightarrow **User Agents** Click **Add** button to add the user agent:

- Enter Name: Avaya one-X Communicator
- Enter Regular Expression: Avaya one-X Communicator.*
- Click on **Finish** (not shown)



Figure 93: User Agents for Remote Worker

The following abridged output of Session Manager trace shows the details of an INVITE from an Avaya one-X Communicator. The User-Agent shown in this trace will match User Agent **one-X Communicator** shown above with a **Regular Expression** of "**Avaya one-X Communicator**.". In this expression, ".*" will match anything listed after the user agent name.

INVITE sip: 1613XXX7497@bvwdev.com SIP/2.0 From: sip:0139@bvwdev.com;tag=-59f03c7f529fb7c152aa3fd4_F0950710.10.98.79 To: sip:161613XXX7497@bvwdev.com CSeq: 24 INVITE Call-ID: 18_a7e80-49279ea452aa365c_I@10.10.98.79 Contact: <<u>sip:0139@10.10.98.79:5061;transport=tls;subid_ipcs=3784557512</u>>;+avaya-cm-line=1 Allow:INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,PRA CK Supported: eventlist, 100rel, replaces, vnd.avaya.ipo **User-Agent: Avaya one-X Communicator**/6.2.13.2 (Engine GA-2.2.0.178; Windows NT 6.2, 32-bit) Max-Forwards: 70 Via: SIP/2.0/TLS 10.10.98.79:62151;branch=z9hG4bK18_a7e80-312c149e52aa3fe8_I09507 Accept-Language: en Content-Type: application/sdp Content-Length: 440

Figure 94: Output of trace for User Agent

Note: The User Agent is defined in its associated Subscriber Flows in Section 12.8.1.

12.6. Application Rules on Avaya SBCE

The following section describes Application Rule **RW_AR**, used in this Remote Worker setting. In a typical customer installation, set the **Maximum Concurrent Sessions** for the **Voice** application to a value slightly larger than the licensed sessions.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Application Rules**

- Select default from Application Rules and click Clone button:
- Enter Clone Name (e.g., RW_AR) and click Finish (not shown)
- Click on **RW_AR** from **Application Rules**, then click **Edit** button:
- In the **Audio** field:
 - Check In and Out
 - Enter an appropriate value in the **Maximum Concurrent Sessions** field (e.g., **2000**), and the same value in the **Maximum Session Per Endpoint** field
 - Leave the **CDR Support** field at **None** and the **RTCP Keep-Alive** field unchecked (**No**)
 - Click on **Finish** (not shown)

Device: SBCE 🛩 Alarms	Incidents Status 🗸 Logs	s∨ Diagnostics Users				Settings 🗸	• Help •	 Log Out
Session Borde	er Controller fo	or Enterprise					A	VAYA
EMS Dashboard	Application Rules: F	RW AR						
Device Management	Add	Man da - O Martin				Rena	ame Clone	e Delete
Backup/Restore ▶ System Parameters	Application Rules		Click h	ere to a	add a description.			
Configuration Profiles	default	Application Rule						
Services	default-trunk			201				
Domain Policies	default-subscriber-low	Application Type	In	Out	Maximum Concurrent Sessions	Maximum	Sessions Per	Endpoint
Application Rules	default-subscriber-high	Audio			2000	2000		
Border Rules Media Rules	default-server-low	Video			100	10		
Security Rules	default-server-high	Miscellaneous						
Signaling Rules	SIP-Trunk	CDR Support	Off					
Charging Rules		RTCP Keep-Alive	No					
End Point Policy Groups	RW_AR				Edit			
Session Policies		L		_				

Figure 95: Remote Worker Application Rule

Note: The rule RW_AR is assigned to the End Point Policy Groups in Section 12.7.

12.7. End Point Policy Groups on Avaya SBCE

A new End Point Policy Groups is defined for Remote Worker: SMVM_RW.

To create the new **SMVM_RW** group, click on **Add**. Enter the following:

- Enter a name (e.g., **SMVM_RW**), and click on **Next** (not shown)
- The **Policy Group** window will open. Enter the following:
 - Application Rule = RW_AR (see Section 12.6)
 - Border Rule = default
 - Media Rule = SMVM (see Section 7.3.2)
 - Security Rule = default-low
 - Signaling Rule = SIP-Trunk (see Section 7.3.3)
- Click on **Finish** (not shown)

The End Point Policy Group **SMVM_RW** is used in the Subscriber Flow **Avaya one-X Communicator** in **Section 12.8.1** and Remote Worker Server Flow in **Section 12.8.2.1**.

Device: SBCE 🗸 Alarms	Incidents Status 🛩 Log	gs 🗸 🛛 Diagn	ostics User	s				Settings	י Help	 Log Out
Session Borde	er Controller f	or Ent	erprise	2					A	VAYA
EMS Dashboard Device Management Backup/Restore	Policy Groups: SM	IVM_RW						R	ename Clone	e Delete
System Parameters	Policy Groups				Click	here to add a desc	ription.			
Configuration Profiles	default-low				Hover ov	er a row to see its c	escription			
ServicesDomain Policies	default-low-enc default-med	Policy Gro	oup							
Application Rules Border Rules	default-med-enc						_			Summary
Media Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Security Rules	default-high-enc	1	RW_AR	default	SMVM	default-low	SIP-Trunk	None	Off	Edit
Signaling Rules	avaya-def-low-enc		-					laces of stren	1686703	
Charging Rules	avaya-def-high-subsc									
Groups	avaya-def-high-server									
Session Policies	SMVM									
 TLS Management Network & Flows 	SP4									
 DMZ Services 	SMVM RW									
Monitoring & Logging										

Figure 96: Remote Worker End Point Policy

12.8. End Point Flows on Avaya SBCE

12.8.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent one-X Communicator** that was created in **Section 12.5**. The below subscriber flow is configured for Remote Worker to access Session Manager via Avaya SBCE.

From the menu on the left-hand side, select Network & Flows \rightarrow End Point Flows On the Subscriber Flows tab, click on the Add button and enter the following:

- Enter a Flow Name (e.g., Avaya one-X Communicator)
- **URI Group** = * (default)
- User Agent = Avaya one-X Communicator (see Section 12.5)
- **Source Subnet** = * (default)
- Via Host = * (default)
- **Contact Host** = * (default)
- Signaling Interface = OutsideSIGRW (see Section 12.3)

Click on Next (not shown) and the Profile window will open (not shown). Enter the following:

- Source = Subscriber
- Methods Allowed Before REGISTER = Leave as default
- Media Interface = OutsideMedRW (see Section 12.2)
- **Received Interface = None.**
- End Point Policy Group = SMVM_RW (see Section 12.7)
- Routing Profile = To_SMVM_RW (see Section 12.4)
- TLS Client Profile = None
- Signaling Manipulation Script = None
- **Presence Server Address** = Leave as blank

Click on **Finish** (not shown).

EMS Dashboard End Point Flows	
Jevice Management	
Surface Surface Subscriber Flows Server Flows	
System Falameters	
Configuration Profiles	Add
Services Modifications made to an End-Point Flow will only take effect on new registrations or re-registrations	
Domain Policies TLS Management Hover over a row to see its description.	
TLS Management Hover over a row to see its description. Network & Flows	
Network Management Priority Flow Name URI Group Source Subnet User Agent End Point Policy Group	
	dit Delete

Figure 97: Remote Worker Subscriber Flows – 1

HV; Reviewed: SPOC 7/10/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

	View Flow: Avaya	one-X Communicator		Х
Criteria ———		Optional Settings		
Flow Name	Avaya one-X Communicator	TLS Client Profile	None	
URI Group	*	Signaling Manipulation Script	None	
User Agent	Avaya one-X Communicator			
Source Subnet	*			
Via Host	*			
Contact Host	*			
Signaling Interface	OutsideSIGRW			
Profile Source	Subscr	iber		
Methods Allowed B				
User Agent	Avaya	one-X Communicator		
Media Interface	Outside	eMedRW		
Secondary Media In	nterface None			
	CMV/M	_RW		
End Point Policy G	Sivivivi			
End Point Policy G Routing Profile		VM_RW		

Figure 98: Remote Worker Subscriber Flows – 2

12.8.2. Server Flow on Avaya SBCE

The new Remote Worker Server Flow (**SMVM_RemoteWorker**) is configured for the SIP traffic flow from Session Manager to Remote Worker via Avaya SBCE. Three existing Trunking Server Flows (SMVM Flow in **Section 7.4.4.1** and AS1 Flow & AS2 Flow in **Section 7.4.4.2**) are also used for Remote Worker.

12.8.2.1 Remote Worker Server Flow

From the menu on the left-hand side, select **Device Specific Settings** \rightarrow **Endpoint Flows** Select the **Server Flows** tab and click the **Add** button (not shown) to enter the following:

- Name = SMVM_RemoteWorker
- Server Configuration = SMVM (see Section 7.2.4)
- **URI Group** = * (default)
- **Transport** = * (default)
- **Remote Subnet** = * (default)
- Received Interface = OutsideSIGRW (see Section 12.3)
- Signaling Interface = InsideSIGRW (see Section 12.3)
- Media Interface = InsideMedRW (see Section 12.2)
- Secondary Media Interface = None
- End Point Policy Group = SMVM_RW (see Section 12.7)
- Routing Profile = default_RW (see Section 12.4)
- **Topology Hiding Profile** = **None** (default)
- **Signaling Manipulation Script = None** (default)
- **Remote Branch Office** = **Any** (default)
- Link Monitoring from Peer = uncheck (default)

Click **Finish** (not shown).

Criteria ———		¬ ⊢ Profile —	
	0.0.04.0	I have been seen to	
Flow Name	SMVM_RemoteWorker	Signaling Interface	InsideSIGRW
Server Configuration	SMVM	Media Interface	InsideMedRW
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	SMVM_RW
Remote Subnet	*	Routing Profile	default_RW
Received Interface	OutsideSIGRW	Topology Hiding Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 99: Remote Worker Server Flow

12.8.2.2 Trunking Server Flow

Three existing Trunking Server Flows (SMVM Flow in Section 7.4.4.1; AS1 Flow & AS2 Flow in Section 7.4.4.2) are also used for Remote Worker.

	View	Flow: SMVM Flow	x
Criteria ———		Profile	<u>.</u>
Flow Name	SMVM Flow	Signaling Interface	InsideTLS
Server Configuration	SMVM	Media Interface	InsideMedia
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	SMVM
Remote Subnet	*	Routing Profile	SMVM_To_AS
Received Interface	OutsideUDP	Topology Hiding Profile	AS_To_SMVM
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 100: Trunking Server Flow – SMVM Flow

	Vie	w Flow: AS1 Flow	
Criteria —		Profile	
Flow Name	AS1 Flow	Signaling Interface	OutsideUDP
Server Configuration	AS1	Media Interface	OutsideMedia
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	SP4
Remote Subnet	*	Routing Profile	AS_To_SMVM
Received Interface	InsideTLS	Topology Hiding Profile	SMVM_To_AS
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 101: Trunking Server Flow – AS1 Flow

	Profile	
S2 Flow	Signaling Interface	OutsideUDP
S2	Media Interface	OutsideMedia
	Secondary Media Interface	None
	End Point Policy Group	SP4
	Routing Profile	AS_To_SMVM
sideTLS	Topology Hiding Profile	SMVM_To_AS
	Signaling Manipulation Script	None
	Remote Branch Office	Any
	Link Monitoring from Peer	
	52	S2 Media Interface Secondary Media Interface End Point Policy Group Routing Profile Signaling Manipulation Script Remote Branch Office

Figure 102: Trunking Server Flow – AS2 Flow

12.9. System Manager

12.9.1. Modify Session Manager Firewall: Elements \rightarrow Session Manager \rightarrow Network Configuration \rightarrow SIP Firewall

Select Rule Sets as Rule Set for SMVM, click Edit button

iession Manager 🔷 🔨					
SS SUM VEN	SIP Firewall Configue Create, configure and assign SIP Fire		ession Managers		He
Session Manager Admi	Rule Sets				
Global Settings		View A	ssign • OPlete	Import • Status	
Communication Profile	7 Items 🍣				
Network Configuration ^	Rule Sets	Туре	Assigned Count	Avaya Provided	Description
	BSM 6.3.2.0	BSM	<u>0</u>	Yes	Avaya provided Rule Set for BSM
Failover Groups	BSM 6.3.8.0	BSM	<u>0</u>	Default	Avaya provided Rule Set for BSM
	BSM 6.3.4.0	BSM	<u>0</u>	Yes	Avaya provided Rule Set for BSM
Local Host Name R	SM 6.3.2.0	SM	0	Yes	Avaya provided Rule Set for SM
Local Host Name R Remote Access	SM 6.3.2.0 SM 6.3.8.0	SM	<u>0</u>	Default	Avaya provided Rule Set for SM Avaya provided Rule Set for SM

Figure 103: Session Manager – SIP Firewall Configuration - Rules

On Whitelist tab, select New

- In the Key field, select Remote IP Address
- In the Value field, enter internal Avaya SBCE IP address used for Remote Worker (10.10.98.123 as defined in Section 12.1)
- In the Mask field, enter the appropriate mask (e.g., 255.255.255.255)
- **Enabled** box is checked
- Select Commit

Aura® System Manager 8.0	Users v 🖌 Elements v 🗢 Services v 📔 Widgets v Shortcuts v	Search	▲ ≡	admin
Home Session Manager	Session Manager			
Session Manager ^	Rule Set Edit or view SIP Firewall Rule Set whitelist, blacklist, and rules. Commit			Help ?
Session Manager Admi	*Name Rule Set for SMVM Description			
Global Settings	*SM Type SM 🐷			
Communication Profile	Rules Blacklist Whitelist			
Network Configuration ^	New Delete			
Failover Groups			-	
Local Host Name R	Key Value Remote IP Address 10.10.98.123	Mask 255.255.255.25	5	
Remote Access	Select : All, None			
SIP Firewall				

Figure 104: Session Manager – SIP Firewall Configuration - Whitelist

12.9.2. Disable PPM Limiting: Elements \rightarrow Session Manager \rightarrow Session Manager Administration

Select the Session Manager Instance named bvwasm2, and select Edit

Aura © System Manager 8.0	Isers v 📕 Elements v 🔹 S	Services v Widgets v Sh	ortcuts v	Search 🔰 🛔	∎ admin
Home Session Manager	Session Manager				
Session Manager ^	Session Manager A	dministration			Help ?
Dashboard	This page allows you to administer S their global settings.	Session Manager instances and configure	•		
Session Manager Admi	Session Manager Instances	Branch Session Manager Instan	ces		
Global Settings	Session Manager Instan	ces			
Communication Profile	New View Edit Delete				
Network Configuration ^	1 Item 🥭			F	ilter: Enable
Network Configuration	Name License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
Failover Groups	bvwasm2 Normal	1	0	1	
Local Host Name R	Select : None				

Figure 105: Session Manager – Edit Instance

The Session Manager View screen is displayed. Scroll down to the Personal Profile Manager (PPM) – Connection Settings section.

- Uncheck the Limited PPM Client Connection and PPM Packet Rate Limiting options
- Select **Commit** (not shown)

Personal Profile Manager (PPM) - Connection Settings 💩	
Limited PPM Client Connection	
*Maximum Connection per PPM Client 3	
PPM Packet Rate Limiting	
*PPM Packet Rate Limiting Threshold 200	

Figure 106: Session Manager – Disable PPM limit

12.10. Remote Worker Client Configuration

The following screen illustrates Avaya one- X^{\otimes} Communicator administration settings for the Remote Worker, used in the reference configuration (note that some screen formats may differ from endpoint to endpoint).

SIP Global Settings Screen

Launch to Avaya one-X[®] Communicator settings and click on Telephony under Accounts. Select Using as SIP Enter Extension and Password Click Add button to add a server into Server List Enter Proxy Server as 10.10.98.34 (see Section 12.1). Set Transport Type: TLS and Port: 5061. Click OK to submit the changes. Set the Demain to buwdey com

Set the **Domain** to **bvwdev.com**.

The other fields are default. Click **OK** to submit the settings.

Avaya one-X® Communicator Login	General Settings			
	Accounts	Telephony Using: O H.323 O SIP		
Please log In:	Telephony Login			
Extension: 0139	Messaging	Extension:	0139	
Password:	IM and Presence Security	Password:	•••••	
Place and receive calls using This Computer Computer	Devices and Services Outgoing Calls Phone Numbers	Server List:	Add	Remove
	Dialing Rules Audio	Domain:	bvwdev.com	
	Video Public Directory	Mode:	Proxied	\$
	Preferences	Avaya Environment:	Auto	¢
	Desktop Integration	Failback Policy:	Auto	0
	Hot Keys Network	Registration Policy: Add Server	Simultaneous	¢
	Advanced	Proxy Server Transport Type Port is optional. If will be used (TLS	TLS ÷ 5061 not specified, the det	fault
	Auto-configure			OK Cancel

Figure 107: Avaya one-X Communicator - Settings

13. Appendix B - SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.2.3**.

```
within session "ALL"
  act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
//Manipulate headers
    %HEADERS["From"][1].URI.USER.regex_replace("\+","");
    %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("(\+)","");
    %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
    %HEADERS["Diversion"][1].URI.USER.regex_replace("(\+)","");
// Remove unwanted Headers
      remove(%HEADERS["History-Info"][3]);
      remove(%HEADERS["History-Info"][2]);
      remove(%HEADERS["History-Info"][1]);
//Modify user of SIP URI in PAI header on Call Forward Off-net
        if (%HEADERS["Diversion"][1].regex_match("reason")) then
         %HEADERS["P-Asserted-Identity"][1].URI.USER =
%HEADERS["Diversion"][1].URI.USER;
          }
     }
  act on message where %DIRECTION="INBOUND" and
%ENTRY_POINT="AFTER_NETWORK"
  {
//Modify the OPTIONS
%HEADERS["Request_Line"][1].regex_replace("sip:metaswitch@10.10.98.14:5060","sip:10.10
.98.14:5060");
    }
//Modify Contact header for Called party information on 180 Ringing/183 Session Progress/200
OK coming from Allstream
  act on response where %DIRECTION="INBOUND" and
%ENTRY POINT="AFTER NETWORK" and %RESP CODE="180" or
%RESP_CODE="183" or %RESP_CODE="200"
  {
```

```
%HEADERS["Contact"][1].URI.USER = %HEADERS["To"][1].URI.USER;
}
```

}

©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 <u>devconnect@avaya.com</u>.