

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Bell MTS SIP Trunk with Avaya Aura<sup>®</sup> Communication Manager 8.1, Avaya Aura<sup>®</sup> Session Manager 8.1, Avaya Aura<sup>®</sup> Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.1 – Issue 1.0

### Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell MTS and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager 8.1, Avaya Aura<sup>®</sup> Communication Manager 8.1, Avaya Aura<sup>®</sup> Experience Portal 7.2, Avaya Session Border Controller for Enterprise 8.1 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.

Bell MTS 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.	GE	NERAL TEST APPROACH AND TEST RESULTS	4
	2.1.	INTEROPERABILITY COMPLIANCE TESTING	5
	2.2.	TEST RESULTS	
	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	12
-	5.3.	IP NODE NAMES	
4	5.4.	CODECS	
	5.5.	IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER	
	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	
		1. Announcements	
	5.12 5.13.	2.2. ACD Configuration for Call Queued for Handling by Agent AVAYA AURA® COMMUNICATION MANAGER STATIONS	
	5.15. 5.14.	AVAYA AURA <sup>®</sup> COMMUNICATION MANAGER STATIONS	
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	
(	6.4.	ADD SIP ENTITIES	
		1. Configure Session Manager SIP Entity	
		2. Configure Communication Manager SIP Entity	
		3. Configure Avaya Session Border Controller SIP Entity	
		4. Configure Avaya Aura <sup>®</sup> Experience Portal SIP Entity	
	6.5.	ADD ENTITY LINKS	
		CONFIGURE TIME RANGES	
	6.7.	ADD ROUTING POLICIES.	
(	6.8.	ADD DIAL PATTERNS	
7.	CO	NFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	56
,	7.1.	LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	
,	7.2.	Server Interworking	
		1. Configure Server Interworking Profile - Avaya Site	
		2. Configure Server Interworking Profile – Bell MTS SIP Trunk Site	
	7.3.	CONFIGURE SIGNALING MANIPULATION	
,	7.4.	CONFIGURE SERVICES	
		1. Configure SIP Server – Avaya Site	
,		2. Configure SIP Server – Bell MTS SIP Trunk	
	7.5.	ROUTING	

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

7	7.5.1. Configure Routing – Avaya Site	
7	7.5.2. Configure Routing – Bell MTS SIP Trunk Site	69
7.6.		
7	.6.1. Configure Topology Hiding – Avaya Site	
7	.6.2. Configure Topology Hiding Profile – Bell MTS SIP Trunk site	71
7.7.	DOMAIN POLICIES	72
7	7.1. Create Application Rules	72
7	7.2. Create Signaling Rules	73
	7.3. Create Endpoint Policy Groups	74
7.8.		
	7.8.1. Manage Network Settings	
	2.8.2. Create Media Interfaces	
	7.8.3. Create Signaling Interfaces	
7	2.8.4. Configuration Server Flows	
	7.8.4.1 Create End Point Flows – SMVM Flow	
	7.8.4.2 Create End Point Flows – Bell MTS SIP Trunk Flow	
<b>8.</b> C	CONFIGURE AVAYA AURA® EXPERIENCE PORTAL	84
8.1.	BACKGROUND	
8.2.	LOGGING IN AND LICENSING	
8.3.	VoIP Connection	
8.4.	Speech Servers	90
8.5.	Application	
8.6.		
8.7.	CONFIGURING RFC2833 EVENT VALUE OFFERED BY EXPERIENCE PORTAL	97
9. B	BELL MTS SIP TRUNK CONFIGURATION	
10. V	/ERIFICATION STEPS	
11. C	CONCLUSION	
12. R	REFERENCES	
13. A	APPENDIX A – REMOTE WORKER CONFIGURATION	
13.1		
13.2		
13.3		
13.4		
13.5		
13.6		
13.7		
13.8		
	3.8.1. Subscriber Flow	
1	3.8.2. Server Flow on Avaya SBCE	
	13.8.2.1 Remote Worker Server Flow	
13.9	-	
	IP Global Settings Screen	
14. A	APPENDIX B - SIGMA SCRIPT	120

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Bell MTS and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager 8.1, Avaya Aura<sup>®</sup> Communication Manager 8.1, Avaya Aura<sup>®</sup> Experience Portal 7.2, Avaya Session Border Controller for Enterprise (Avaya SBCE) 8.1 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Bell MTS 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 Bell MTS 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, Experience Portal 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 Bell MTS SIP Trunk Service did not include use of any specific encryption features as requested by Bell MTS.

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<sup>®</sup> Communicator (1XC) and Avaya Workplace Client 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 Workplace Client 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 Bell MTS
- 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
- Codec G.711MU, G.729A
- 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<sup>®</sup> Messaging and EC500 mobility (extension to cellular)
- SIP re-Invite in off-net call transfer
- SIP Diversion header in off-net call forward
- Call Center scenarios
- DTMF RFC2833
- Remote Worker
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold)

Items not tested or supported include the following:

- TLS/SRTP SIP Transport on the public side (between the Avaya SBCE and Bell MTS)
- Bell MTS supports inbound toll-free service in their production environment, however Bell MTS did not have inbound toll-free service configured in their test lab environment during the compliance testing

HV; Reviewed:	
SPOC 11/3/2020	

• Bell MTS supports SIP REFER method for call redirection to the PSTN, but there were issues with this feature during the compliance test. Therefore, SIP REFER was disabled in Communication Manager (refer to **Section 5.8**)

## 2.2. Test Results

Interoperability testing of Bell MTS was completed with successful results for all test cases with the exception of the observation described below:

• There was no audio in both directions of the call after completion of call redirections to the PSTN, this included inbound calls from the PSTN being forwarded back out to the PSTN and inbound calls from the PSTN being transferred back out to the PSTN (blind and attended transfers) - The work-around for this issue is to use RTP between Communication Manager and the Avaya SBCE, instead of using SRTP (refer to Sections 5.4 and 7.7.3)

### 2.3. Support

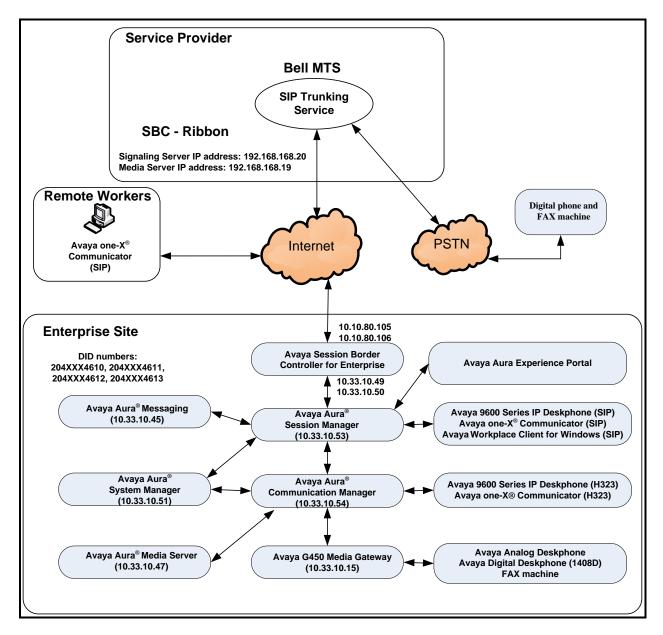
For technical support on the Avaya products described in these Application Notes visit: http://support.avaya.com

For technical support on Bell MTS SIP Trunking, contact Bell MTS at website: https://www3.bellmts.ca/mts/enterprise/business+solutions/voice/sip+trunking

# 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to Bell MTS 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 Bell MTS SIP Trunk

Note: The compliance testing was done over the internet, but Bell MTS only provide SIP trunking service over private Bell MTS access network services.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	7 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

# 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 <sup>®</sup> Communication Manager	8.1.2.0.0.890.26095				
running on VMware <sup>®</sup> -based Avaya appliance					
Avaya G450 Media Gateway	HW2 FW41.16				
– MM711AP Analog	HW46 FW096				
<ul> <li>MM712AP Digital</li> </ul>	HW10 FW014				
– MM710AP	HW5 FW020				
Avaya Aura <sup>®</sup> Session Manager	8.1.2.0.812033				
running on VMware <sup>®</sup> -based Avaya appliance					
Avaya Aura <sup>®</sup> System Manager	8.1.2.0				
running on VMware <sup>®</sup> -based Avaya appliance	Build 8.1.0.0.733078				
	Revision 8.1.2.0.0611097 FP 2				
Avaya Aura <sup>®</sup> Messaging	7.1.0.1.532.002.0 (SP2)				
running on VMware <sup>®</sup> -based Avaya appliance					
Avaya Aura <sup>®</sup> Media Server	8.0.2.43				
running on VMware <sup>®</sup> -based Avaya appliance					
Avaya Session Border Controller for Enterprise	8.1.1.0-26-19214				
running on VMware <sup>®</sup> -based Avaya appliance					
Avaya Aura <sup>®</sup> Experience Portal running on	7.2.2.0.2118				
VMware <sup>®</sup> -based Avaya appliance					
Avaya 9621G IP Deskphone (SIP)	Avaya <sup>®</sup> Deskphone SIP 7.1.7.0.11				
Avaya 9621G IP Deskphone (H.323)	Avaya <sup>®</sup> IP Deskphone				
	6.8.304				
Avaya 9641 IP Deskphone (H.323)	Avaya <sup>®</sup> IP Deskphone				
	6.8.304				
Avaya Digital Deskphone (1408D)	R48				
Avaya Workplace Client for Windows (SIP)	3.9.1.46.29				
Avaya one-X <sup>®</sup> Communicator (H.323 & SIP)	6.2.14.2-SP14P1				
Avaya Analog Deskphone	N/A				
HP Officejet 4500 Fax	N/A				
BELL MTS SIP Trunk Components					
Equipment/Software	Equipment/Software Release/Version				
SBC - Ribbon	Q20 version 9.3				

#### **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.

**Note**: It is assumed the general installation of VMware<sup>®</sup>- based Avaya Appliance Virtualization Platform, Avaya Aura<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> System Manager, Avaya Aura<sup>®</sup> Session Manager, Avaya Aura<sup>®</sup> Experience Portal, Avaya Aura<sup>®</sup> Messaging, Avaya Aura<sup>®</sup> 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 Bell MTS 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.

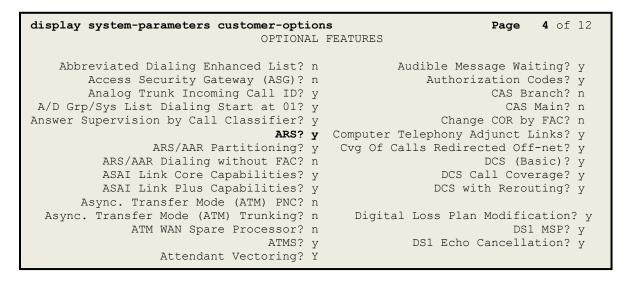
## 5.1. Licensing and Capacity

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 4000 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	<b>2</b> of 12
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	4000	0	
Maximum Concurrently Registered IP Stations:	1000	1	
Maximum Administered Remote Office Trunks:	4000	0	
Maximum Concurrently Registered Remote Office Stations:	1000	0	
Maximum Concurrently Registered IP eCons:	68	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	2400	0	
Maximum Video Capable IP Softphones:	1000	5	
Maximum Administered SIP Trunks:	4000	100	
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	80	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
                        PNC Duplication? n
                                                Terminal Trans. Init. (TTI)? y
                                                        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? nTrunk-to-Trunk Transfer: allAutomatic Callback with Called Party Queuing? nAutomatic Callback with Called Party Queuing? nCall Park Timeout Interval (rings): 3<br/>Call Park Timeout Interval (minutes): 10Off-Premises Tone Detect Timeout Interval (seconds): 20<br/>AAR/ARS Dial Tone Required? y
```

#### 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:

- Media Server: Name: AMS, IP Address: 10.33.10.47
- Session Manager: Name: bvwasm2, IP Address: 10.33.10.53
- Communication Manager: Name: procr, IP Address: 10.33.10.54

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

change node-na	Page	1 of	2		
		IP NODE NAMES			
Name	IP Address				
AMS	10.33.10.47				
bvwasm2	10.33.10.53				
default	0.0.0.0				
procr	10.33.10.54				
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. Bell MTS supports the **G.711MU** and **G.729A** codecs. Default values can be used for all other fields. Note: With the setting of none in Media Encryption, RTP was used between Communication Manager and Avaya SBCE. See **Section 2.2** for the media issue in details.

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

      IP CODEC SET
      III Codec Set: 1
      III Codec
      III Codec
```

Figure 8: IP-Codec-Set Form – Page 1

Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved. On Page 2, set the FAX Mode to t.38-standard. Note: Bell MTS supports T38 fax.

change ip-codec-set 1				Page	<b>2</b> of 2
	IP CODEC SET				
	Allow Direc	t-IP Multimedia	? n		
	Mode	Redundancy		P	acket 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
                              TP NETWORK REGION
 Region: 1
Location: 1
                 Authoritative Domain: bvwdev.com
   Name: procr
                               Stub Network Region: n
MEDIA PARAMETERS
                              Intra-region IP-IP Direct Audio: yes
     Codec Set: 1
                             Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048
                                        IP Audio Hairpinning? n
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
       Audio 802.1p Priority: 6
       Video 802.1p Priority: 5
                                 AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
                                                      RSVP Enabled? n
 H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

#### Figure 10: IP-Network-Region Form

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** 

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	15 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

Address is the Avaya Processor Ethernet (10.33.10.54), 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
                                                                      1 of
                                                                             2
                                                               Page
                            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: 41 .16 .0 /2
       MGP IPV4 Address: 10.33.10.15
       MGP IPV6 Address:
  Controller IP Address: 10.33.10.54
            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 "gateway-announcements" in logical slot **V9**.

```
display media-gateway 1
                                                                 2 of
                                                          Page
                                                                       2
                          MEDIA GATEWAY 1
                              Type: g450
Slot
     Module Type
                                                 DSP Type FW/HW version
                          Name
V1:
     MM712
                          DCP MM
                                                 MP80 170 7
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

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	16 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

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 MEDIA SERVER Media Server ID: 1 Signaling Group: 11 Voip Channel License Limit: 10 Dedicated Voip Channel Licenses: 10 Node Name: AMS Network Region: 1 Location: 1 Announcement Storage Area:

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

Enable Interface? y

Network Region: 1

IPV4 PARAMETERS

Node Name: procr

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, Messaging are 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

- 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 IP Audio Connections? y IP Audio Hairpinning? n Enable Layer 3 Test? y Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6

#### 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 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

- 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: n Peer Server: 5071<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 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

add trunk-group 20	Page 1 of 4 TRUNK GROUP
Group Number: 20 Group Name: SIP Trunks Direction: two-way Dial Access? n Queue Length: 0	Group Type: sip CDR Reports: y COR: 1 TN: 1 TAC: *020 Outgoing Display? n Night Service:
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**, 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 **600** seconds was used.

```
add trunk-group 20
Group Type: sip
TRUNK PARAMETERS
Unicode Name: auto
Redirect On OPTIM Failure: 5000
SCCAN? n
Digital Loss Group: 18
Preferred Minimum Session Refresh Interval (sec): 600
Disconnect Supervision - In? y Out? y
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n
```

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 **publue 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.

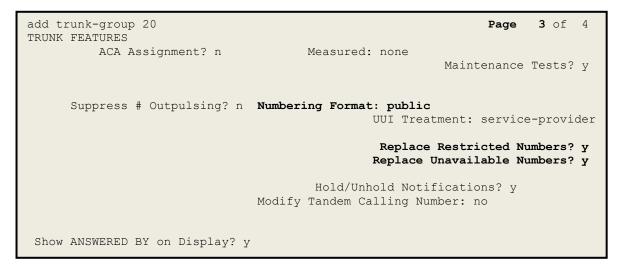


Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **n** so that Communication Manager will not send SIP Refer. Note: In the compliance testing, Bell MTS supports SIP REFER, but there has been issues with this feature in the past. Therefore, re-INVITE is the best option for testing the call transfers.

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. Set **Always Use re-INVITE for Display Updates** to **y**.

add trunk-group 20	<b>Page 4</b> of 4
PROTOCOL VARIATIONS	
Mark Users as Phone? Prepend '+' to Calling/Alerting/Diverting/Connected Number? Send Transferring Party Information?	n
Network Call Redirection?	n
Send Diversion Header? Support Request History?	-
Telephone Event Payload Type:	-
Convert 180 to 183 for Early Media? <b>Always Use re-INVITE for Display Updates?</b> Identity for Calling Party Display: Place Calling Calling Party Logation in UNUTED	<b>y</b> P-Asserted-Identity
Block Sending Calling Party Location in INVITE? Accept Redirect to Blank User Destination?	
Enable Q-SIP? Interworking of ISDN Clearing with In-Band Tones:	

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 **46** 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.

char	<b>change public-unknown-numbering 0</b> NUMBERING - PUBLIC/UNKNOWN FORMAT					1 of	2
	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len			
4	46	20	204xxx	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 **46** for extension (**ext**)
- **Dialed String** beginning with **48** for extension (**udp**)
- **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 dial	olan analysis	Page 1 of 1	12
		DIAL PLAN ANALYSIS TABLE Location: all Percent Full: 2	
Dialed String 181 189 3 46 48 800 9	TotalCallLengthType4ext4ext4ext4ext4udp4ext1fac	Dialed Total Call Dialed Total Call String Length Type String Length Type	
*	4 dac		

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).

change ars analysis	0		ARS DIGIT .				Page	1 of	2
				tion: all			Percent Fu	ıll: 1	
Dialed String <b>0</b>	Tot Min <b>1</b>	al Max <b>11</b>	Route Pattern 20	Call Type <b>op</b>	Node Num	ANI Reqd <b>n</b>			
011 1613 1800	10 11 11	18 11 11	20 20 20	intl pubu pubu		n n n			
204784 411 911	10 3 3	10 3 3	20 20 20	pubu pubu pubu		n n 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 Secure SIP? n SCCAN? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Intw Dgts 1: 20 0 n user 2: n user user 3: n 4: n user 5: n user 6: user n 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: ууууул п rest none 3: yyyyyn n rest none 4: y y y y y n n rest none 5: y y y y y n n rest none rest none 6: ууууул п

#### 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.

change cor 1 Page 1 of 23 CLASS OF RESTRICTION COR Number: 1 COR Description: FRL: 0 APLT? y Can Be Service Observed? n Calling Party Restriction: none Can Be A Service Observer? n Called Party Restriction: none 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 11/3/2020

Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved. 29 of 122 BM\_CMSM81SBC81

## 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 **204XXX4613** to **1810** by deleting **10** of the incoming digits for voicemail testing purpose. (1810 is voice mail pilot number)
- The incoming DID number **204XXX4612** to **4800** by deleting **10** of the incoming digits for Experience Portal testing purpose
- The incoming DID number **204XXX** to 4-digit extension by deleting **6** of the incoming digits for inbound call testing purpose

change inc-call-h	Page	1 of	3			
Service/	Number	Number	Del Insert			
Feature	Len	Digits				
public-ntwrk	10	204XXX4613	10 1810			
public-ntwrk	10	204 <b>xxx4612</b>	10 4800			
public-ntwrk	10	204XXX	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	ANNC	DUNCEMENTS/AUDIO	SOURCES	Num of
Extension 1898	Type integrate	Name	Source 001V	e Files
1899	integrate		001V	

### 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.

Page 1 of 3
UP
ACD? y
Queue? y
Vector? y
MM Early Answer? n
l Agent Preference? n
,
l
Port:
Port:

Figure 29: Hunt Group Configuration – Page 1

HV; Reviewed: SPOC 11/3/2020

Solution & Interoperability Test Lab Application Notes ©2020 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		Page	2 of	3	
	HUNT GROUP				
<b>Skill? y</b> AAS? n	Expected Call Handling Time (sec) Service Level Target (% in sec):		0		

#### **Figure 30: Hunt Group Configuration – Page 2**

VDN 4610, shown below, is associated with vector 3

display vdn 4610				Page	1 of	3
	VECTOR DIREC	TORY NUMBER				
	EXTENSION:	4610				
	Name*: C	ontact Center				
	DESTINATION:	VECTOR NUMBER	3			
	Attendant Vectoring?	n				
	Meet-me Conferencing?	n				
	Allow VDN Override?	n				
	COR:	1				
	TN*:	1				
	Measured:	none				



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: 3Name: Contact CenterMultimedia? nAttendant Vectoring? nMeet-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 Variables? y 3.0 Enhanced? y Holidays? 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	AGENT	Page 1 (	of 2
Login ID:	3311	AAS?	n
Name:	SP	AUDIX?	n
TN:	1	LWC Reception:	spe
COR:	1	LWC Log External Calls?	n
Coverage Path:		AUDIX Name for Messaging:	
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
Ma:	ximum time age	ent in ACW before logout (sec):	system
		Forced Agent Logout Time:	:

Figure 33: Agent-loginID Configuration – Page 1

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	33 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

```
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:

Page 2 of 2

Service Objective? n

Local Call Preference? n
```

#### Figure 34: Agent LoginID Configuration – Page 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.

Figure 35: Enable Expert Agent Selection

Page 11 of 19

## 5.13. Avaya Aura<sup>®</sup> Communication Manager Stations

In the sample configuration, a 4-digit station extension was used with the format 4611. Use the **add station 4611** command to add an Avaya H.323 IP Deskphone.

- Enter Type: 9621, Name: H323-4611, Security Code: 1234, Coverage Path 1: 1, IP SoftPhone: y (if using this extension as a Softphone such as Avaya one-X<sup>®</sup> Communicator)
- Leave other values as default

add station 4611 Page 1 of 5 STATION Extension: 4611 Lock Messages? n Security Code: \* Coverage Path 1: 1 Coverage Path 2: BCC: 0 Type: 9621 TN: 1 COR: 1 COS: 1 Port: S000055 Name: H323-4611 Tests? y Hunt-to Station: STATION OPTIONS Time of Day Lock Table: Loss Group: 19 Personalized Ringing Pattern: 1 Speakerphone: 2-wayMute Button Enabled? yDisplay Language: EnglishButton Modulesable GK Node Name:Button Modules 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?  ${f y}$ 

### Figure 36: Add-Station Form

### 5.14. Save Avaya Aura<sup>®</sup> 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<sup>®</sup> 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.

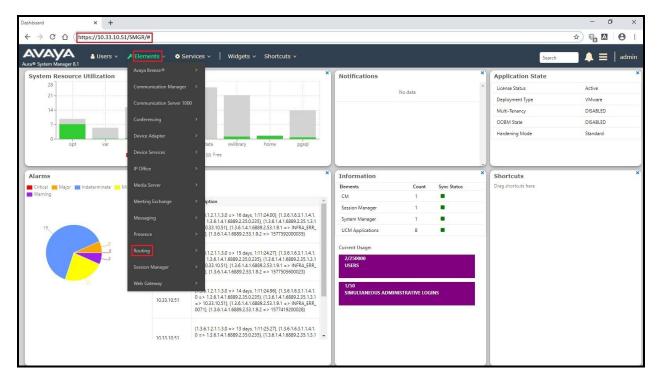


Figure 37: System Manager Home Screen

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.

<ul> <li>System Manager 8.1</li> </ul>	Lusers ∨ Felements ∨ O Services ∨   Widgets ∨ Shortcuts ∨ Search ↓ ≡   a
me Routing	
	Administration of Session Manager Routing Policies
Domains	A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.
	The recommended order of routing element administration (that means the overall routing workflow) is as follows:
Locations	Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
Conditions	Step 2: Create "Locations"
	Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)
Adaptations Y	Step 4: Create "Adaptations"
SIP Entities	Step 5: Create "SIP Entities"
Entity Links	- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
chury canks	- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
Time Ranges	- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
Routing Policies	Step 6: Create the "Entity Links"
	- Between Session Managers
Dial Patterns Y	- Between Session Managers and "other SIP Entities"
Regular Expressions	Step 7: Create "Time Ranges"
	- Align with the tariff information received from the Service Providers
Defaults	Step 8: 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 10: Create "Dial Patterns"
	- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"
	Step 11: 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 after "Routing Policies" using "Dial patterns". That's why this overall routing workflow can be interpreted as
	"Dial Pattern driven approach to define Routing Policies"
	That means (with regard to steps listed above):
	Step 8: "Routing Polices" are defined
	Step 9: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)
	Step 10: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

#### 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.

Aura® System Manager 8.1	Users ∨ <i>F</i> Elements ∨ Services ∨   Widgets ∨ Shortcuts ∨ Search	📄 🜲 🗮 🛛 admin
Home Routing		
Routing	Domain Management	Help ?
Domains	New Edit Delete Duplicate More Actions •	
Locations	1 Rem 🧶	Filter: Enable
Conditions	Name Type Notes	
Adaptations Y	bywdey.com Select : All, None	

**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

Avra® System Manager 8.1	Users 🗸 🖌 Elements 🗸 🌣 Services 🗸   Widgets 🗸 Shortcut	S Ý	Search 👃 🚍 🛛 admin
Home Routing			
Routing ^	Location Details	Commit Cancel	Help ?
Domains	General		
Locations		Belleville-GSSCP	
Conditions	Notes:		
Adaptations 🗸 🗸	Dial Plan Transparency in Survivable Mode		
SIP Entities	Enabled:		
Entity Links	Listed Directory Number:		
Time Ranges	Associated CM SIP Entity:		
Routing Policies	Overall Managed Bandwidth		
Dial Patterns 🗸 🗸	Managed Bandwidth Units:	Kbit/sec •	
	Total Bandwidth:		
Regular Expressions	Multimedia Bandwidth:		
Defaults	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:	64 Kbit/Sec	
	* Default Audio Bandwidth:	80 Kbit/sec •	
	Alarm Threshold		
	Overall Alarm Threshold:	80 • %	
	Multimedia Alarm Threshold:	80 • %	
	* Latency before Overall Alarm Trigger:	5 Minutes	
<	* Latency before Multimedia Alarm Trigger:	5 Minutes	
	Location Pattern		

#### **Figure 40: Location Configuration**

HV; Reviewed: SPOC 11/3/2020

Solution & Interoperability Test Lab Application Notes ©2020 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: 10.33.1.\*, 10.33.10.\*, 10.33.100.\*
- Click **Commit** to save

Loca	tion Pattern		
Add	Remove		
3 Iter	ms		
	IP Address Pattern		*
	* 10.33.1.*		
	* 10.33.10.*		
	* 10.33.100.*		
Selec	t: All, None		
		Commit	

#### **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, Experience Portal 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
• FQDN or IP Address	: Enter the FQDN or IP Address of the SIP Entity that is
	used for SIP signaling
• Type:	Select Session Manager for Session Manager, CM for
	Communication Manager, Voice Portal for Experience Portal and
	SIP Trunk for Avaya SBCE configuration
Adaptation:	This field is only present if <b>Type</b> is not set to <b>Session Manager</b> . Adaptation modules were not used in this configuration
Location:	Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location <b>Belleville-GSSCP</b>

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	41 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

• **Time Zone**: Select the time zone for the Location above

In this configuration, there are four SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller SIP Entity
- Experience Portal 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 10.33.10.53**. The user will need to select the specific values for the **Location** and **Time Zone**.

Aura® System Manager 8.1	Users ∨ 🖌 Elements ∨ 💠 Services ∨   Widgets ∨ Shortcu	rts v Search 💄 📃   admin
Home Routing		
Routing	SIP Entity Details	Commit Cancel
Domains	General	
Locations		bvwasm2
Conditions	* IP Address: SIP FQDN:	10.33.10.53
Adaptations 🗸 🗸	Туре:	Session Manager
SIP Entities	Notes:	
Entity Links	Location:	Belleville-GSSCP V
Time Berner	Outbound Proxy:	
Time Ranges		America/Toronto 🔹
Routing Policies	Minimum TLS Version:	
Dial Patterns 🗸 🗸	Credential name:	
	Monitoring	
Regular Expressions	SIP Link Monitoring:	Use Session Manager Configuration 🔻
Defaults	CRLF Keep Alive Monitoring:	Use Session Manager Configuration V

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, to Avaya SBCE and to Experience Portal.

Listen Ports TCP Failover port: TLS Failover port:			
Add Remove			
4 Items 🍣			Filter: Enable
Listen Ports	Protocol Default Domain	Notes	
5061	TLS V bvwdev.com V		
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 **10.33.10.54**. Note that **CM** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA Aura® System Manager 8.1	Users × <b>∕</b> Elements × <b>◊</b> Services ×           Widgets ×    Shortcul	ts v Search 🌲 🚍   admin
Home Routing		
Routing ^	SIP Entity Details	Commit Cancel
Locations	* Name: * FQDN or IP Address:	
Conditions	Туре:	CM •
Adaptations ~	Notes:	
SIP Entities	Adaptation:	
Entity Links		Belleville-GSSCP T
Time Ranges	Fime Zone: * SIP Timer B/F (in seconds):	America/Toronto T
Routing Policies	Minimum TLS Version:	
Dial Patterns 🗸 🗸	Credential name:	
	Securable: Call Detail Recording:	
Regular Expressions	Can betan Recording:	none •
Defaults	Loop Detection Loop Detection Mode:	On Y
	Loop Detection mode.	
	Loop Detection Interval (in msec):	
	Monitoring SIP Link Monitoring:	Link Monitoring Enabled
	* Proactive Monitoring Interval (in seconds):	900
	* Reactive Monitoring Interval (in seconds):	120
	* Number of Tries:	1
	* Number of Successes:	1
	CRLF Keep Alive Monitoring:	Use Session Manager Configuration V

Figure 44: Communication Manager SIP Entity

### 6.4.3. Configure Avaya Session Border Controller 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 **10.33.10.49**. 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 8.1	Users ∨ 🖌 Elements ∨ 🏟 Services ∨   Widgets ∨ Shortcu	ts v Search 🗼 🚍   admin
Home Routing		
Routing ^	SIP Entity Details	Commit Cancel
Domains	General	
Locations	* Name:	
Conditions	* FQDN or IP Address:	
CONDITIONS		SIP Trunk •
Adaptations 🗸 🗸	Notes:	
SIP Entities	Adaptation:	T
Entity Links	Location:	Belleville-GSSCP •
	Time Zone:	America/Toronto
Time Ranges	* SIP Timer B/F (in seconds):	
Routing Policies	Minimum TLS Version:	
Dial Patterns 🗸 🗸	Credential name:	
	Securable: Call Detail Recording:	
Regular Expressions	Can betan Recording:	egress v
Defaults	Loop Detection	
	Loop Detection Mode:	
	Loop Count Threshold: Loop Detection Interval (in msec):	
	Loop Detection Interval (in insec).	200
	Monitoring	
	SIP Link Monitoring: * Proactive Monitoring Interval (in seconds):	Link Monitoring Enabled
	* Reactive Monitoring Interval (in seconds):	
	* Number of Tries:	
	* Number of Successes:	
		Use Session Manager Configuration •

Figure 45: Avaya SBCE SIP Entity

### 6.4.4. Configure Avaya Aura<sup>®</sup> Experience Portal SIP Entity

The following screen shows the addition of the Avaya Experience Portal SIP entity named **Experience Portal**. The **FQDN** or **IP Address** field is set to the IP Address of the Experience Portal interface **10.33.1.3**. Note that **Voice Portal** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA Aura® System Manager 8.1	Users ∨ → Elements ∨ ♥ Services ∨   Widgets ∨ 3	Shortcuts v	
Home Routing			
Routing	SIP Entity Details		Commit
Domains	General		
Locations		* FQDN or IP Address:	Experience Portal
Conditions			Voice Portal
Adaptations 🗸 🗸		Notes:	
SIP Entities		Adaptation:	▼
Entity Links		Location:	Belleville-GSSCP V
		Time Zone:	America/Toronto 🗸
Time Ranges	* SIP	Timer B/F (in seconds):	
Routing Policies		Minimum TLS Version:	Use Global Setting 🗸
Dial Patterns 🗸 🗸		Credential name:	
		Securable: Call Detail Recording:	
Regular Expressions		can betan kecorang.	none •
Defaults	Loop Detection	to a bar the state	2
		Loop Detection Mode: Loop Count Threshold:	
	Loop Dete	ction Interval (in msec):	
		under van (in misses).	
	Monitoring	CTD Link Maniharian	Use Session Manager Configuration V
	CRI		Use Session Manager Configuration V
		Call Admission Control:	
		ed Bandwidth Manager:	
	Primary Session Manager	Bandwidth Association:	~
	Backup Session Manager	Bandwidth Association:	
<	Entity Links		
		ransport with DNS SRV:	

**Figure 46: Experience Portal SIP Entity** 

Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved.

# 6.5. Add Entity Links

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

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
- 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**.

Aura® System Manager 8.1	Users	🗸 🍾 Elements 🗸 🕻	Services v   Widgets v	Shortcuts v					Search		▲ ≡	admin
Home Routing												
Routing	Ent	tity Links			Com	mit Cancel						Help ?
Domains						_						
Locations	1 Ite	em 🥲									Filter	: Enable
Conditions		Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes	
Adaptations ~		* SM_CM_TLS_5061	* Q bvwasm2	TLS V	* 5061	* Q СМ8	* 5061		trusted 🔻			
SIP Entities	∢ Sele	ct : All, None										•
Entity Links	_											

#### Figure 47: 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 7.4.1**, **7.5.1** and **7.8.3**.

Aura® System Manager 8.1	Users 🗸 🎤 Elements 🗸 🕏	Services ~   Widgets ~ S	hortcuts v					Search		▲ ≡	admin
Home Routing											
Routing ^	Entity Links			Com	nmit Cancel						Help ?
Domains					_						
Locations	1 Item 🔊									Filt	er: Enable
Conditions	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes	
Adaptations 🗸 🗸	SM_SBCE_TLS_5061	* Q bvwasm2	TLS ¥	* 5061	* Q SBCE	* 5061		trusted 🔻			
SIP Entities	Select : All, None										•
Entity Links											

Figure 48: Avaya SBCE Entity Link

The following screen illustrates the Entity Links to Experience Portal. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 8.3**.

Aura® System Manager 8.1	.Users ∨ 🖌 Elements ∨ 🌣 Services ∨   Widgets ∨ S	Shortcuts v	
Home Routing			
Routing	Entity Links	Commit Cancel	
Domains			
Locations	1 Item 🧶		
Conditions	Name SIP Entity 1	Protocol Port SIP Entity 2	Port DNS Override Connection Policy
Adaptations 🗸 🗸	* SM_EP_TLS_Link         * Q bvwasm2           Select : All, None	TLS V * 5061 * Q Experience Portal	* 5061 trusted V
SIP Entities			
Entity Links		[Commit][Cancel]	

**Figure 49: Experience Portal 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.

Aura® System Manager 8.1	Users 🗸 🎤 Elements	s 🗸 🏟 Service	s~   Wid	lgets v Sh	ortcuts ~					Search	📄 🜲 🚍   admin
Home Routing											
Routing	Time Ranges										Help 7
Domains	New Edit Delete	e Duplicate (	More Actions	•]							
Locations	1 Item 🤕										Filter: Enable
Conditions	Name	Mo	ти	We	тh	Fr	Sa	Su	Start Time	End Time	Notes
Adaptations 😪	24/7 Select : All, None	V	V	V	Ø	V	X	V	00:00	23:59	
SIP Entities											
Entity Links											
Time Ranges											

Figure 50: 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**. Three Routing Policies must be added; one for Communication Manager, one for Experience Portal 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.

- 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 **SP Inbound Calls** associated with incoming PSTN calls from Bell MTS to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM8**.

AVAYA Aura® System Manager 8.1	🛔 Users 🗸 🎤 Elements 🗸 🏟 Services 🗸 🍐	Widgets v Shortcuts v
Home Routing		
Routing	Routing Policy Details	Commit Cancel
Domains	General	
Locations		* Name: SP Inbound Calls
Conditions		Disabled:
Adaptations 🗸 🗸		* Retries: 0
SIP Entities	SIP Entity as Destination	
Entity Links	Select	
Time Ranges	Name	FQDN or IP Address
Routing Policies	CM8 Time of Day	10.33.10.54

Figure 51: Routing to Communication Manager

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

AVAYA Aura® System Manager 8.1	🛔 Users 🗸 🎤 Elements 🗸 🔅 Services 🗸 1	<ul> <li>Widgets          Shortcuts          </li> </ul>
Home Routing		
Routing	A Routing Policy Details	Commit) Cancel
Domains	General	
Locations		* Name: SP Outbound Calls
Conditions		Disabled:
Adaptations		* Retries: 0 Notes:
SIP Entities	SIP Entity as Destination	
Entity Links	Select	
Time Ranges	Name	FQDN or IP Address
Routing Policies	SBCE	10.33.10.49
Routing Policies	Time of Day	

#### Figure 52: Routing to Bell MTS SIP Trunk

The following screen shows the **Routing Policy Details** for the policy named **To-Experience-Portal** associated with outgoing calls to Experience Portal. Observe the **SIP Entity as Destination** is the entity named **Experience Portal**.

AVAYA Aura® System Manager 8.1	🛓 Users 🗸 🎤 Elements 🗸 💠 Services 🗸 📔 Widgets 🗸	Shortcuts v
Home Routing		
Routing	A Routing Policy Details	Commit
Domains	General	
Locations		* Name: To-Experience-Portal
Conditions		Disabled:
Adaptations	·•	* Retries: 0 Notes:
SIP Entities	SIP Entity as Destination	
Entity Links	Select	
Time Ranges	Name	FQDN or IP Address
,	Experience Portal	10.33.1.3
Routing Policies	Time of Day	

**Figure 53: Routing to Experience Portal** 

Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved.

### 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 Bell MTS 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 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.

Three examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN, one for inbound calls from the PSTN to the enterprise and one for calls to Experience Portal. 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 **SP Outbound Calls** which is defined in **Section 6.7**.

AVAYA A	Users 🗸 🌾 Elements 🗸 💠 Services 🗸	Widgets v Shortcuts v					Search 💄 🗮 🕴	admin
Home Routing								
Routing	Dial Pattern Details	Co	mmit Cancel					Help ?
Domains	General							
Locations		* Pattern: 161	3					
Conditions		* Min: 4						
		* Max: 11 Emergency Call:						
SIP Entities		SIP Domain: bvv	vdev.com 🗸					
Entity Links		Notes: SP	Outbound Calls					
Time Ranges	Originating Locations and Routing	Policies						
Routing Policies	Add Remove						Filter: Er	able
	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes	aure
Unai Petterns A	-ALL-		SP Outbound Calls	0	C	SBCE		
Dial Patterns	Select : All, None							

Figure 54: Dial Pattern\_1613

Note that 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 **204** use **Routing Policy Name** as **SP Inbound Calls** which is defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Bell MTS.

AVAYA Aura® System Manager 8.1	å Users ×   ≠ Elements ×   ✿ Services ×     Widgets × Shortcuts ×			
Home Routing				
Routing	Dial Pattern Details			
Domains	General			
Locations	* Pattern: 204			
Conditions	* Min: 3			
Adaptations 🗸 🗸	* Max: 10			
SIP Entities	SIP Domain: bvwdev.com 🗸			
Entity Links	Notes: Bell MTS Inbound Call			
Time Ranges	Originating Locations and Routing Policies			
Routing Policies	Add Remove 1 Item 🐡			
Dial Patterns	A Originating Location Name A Originating Location Notes Routing Policy Name Ram	ak	Routing Policy Disabled	Routing Policy Destination
Dial Patterns	Select : All, None	0		CM8

Figure 55: Dial Pattern\_204

The third example shows that the inbound PSTN calls to Experience Portal use **Routing Policy** Name as **To-Experience-Portal** which is defined in **Section 6.7**.

Routing Policy Destination
Experience Portal

Figure 56: Dial Pattern\_4800

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

New		Duplicate	More Actions	•				
38 It	ems ಿ							
	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
	0	1	11				bvwdev.com	Bell MTS Outbound Cal
	011852	13	13				bvwdev.com	Bell MTS Outbound Cal
	1800	11	11				bvwdev.com	Bell MTS Outbound Cal
	204	3	10				bvwdev.com	Bell MTS Inbound Call
	204784	6	10				bvwdev.com	Bell MTS Outbound Ca
	411	3	3				bywdev.com	Bell MTS Outbound Ca
	46	2	4				bvwdev.com	Bell MTS SIP Phones
	4800	4	4				bvwdev.com	Experience Portal
	1613	4	11				bvwdev.com	SP Outbound Calls
$\square$	911	3	3				bywdev.com	Bell MTS Outbound C

Figure 57: 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 Bell MTS.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Bell MTS 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 12** 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.k/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 58: Avaya SBCE Login

Dashboard	Dashboard				
ice Management	Information			Installed Devices	
ystem Administration kup/Restore	System Time	04:03:35 PM EDT	Refresh	EMS	
onitoring & Logging	Version	8.1.1.0-26-19214		SBCE	1
	GUI Version	8.1.1.0-19189			
	Build Date	Wed Jul 22 23:36:51 UTC 2020			
	License State	© OK			
	Aggregate Licensing Overages	0			
	Peak Licensing Overage Count	0			
	Last Logged in at	09/02/2020 18:28:05 EDT			
	Failed Login Attempts	0			
	Active Alarms (past 24 hours)			Incidents (past 24 hours)	
	None found.			SBCE: Registration Successful, Server is UP	
				SBCE: Registration Failed, Server is Down	
				SBCE: Registration Successful, Server is UP	
				SBCE: Registration Failed, Server is Down	
				SBCE: Registration Successful, Server is UP	
					5

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

Figure 59: 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: EMS ~ Alarms	Incidents Status V Logs V Diagnostics Users				Settings 🗸 Help 🖌 Log Out
Session Borde	r Controller for Enterprise				Ανάγα
EMS Dashboard  Device Management  System Administration	Device Management				
Backup/Restore	Devices Updates SSL VPN Licensing Key Bundles				
Monitoring & Logging	Device Name	Management IP	Version	Status	
	SBCE	10.33.10.29	8.1.1.0- 26-19214	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Figure 60: 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.

Ceneral Configuration Appliance Name       SBCE         Box Type       SIP         Deployment Mode       Proxy         Viron Bypass Mode       No         Two Bypass Mode       No         Advanced Sessions Requested: 0       512         Scopia Video Sessions Requested: 0       512         CES Sessions Requested: 0       512         CLID          Encryption Available: Yes       512         Network Configuration IP       Network Prefix or Subnet Mask       Gateway         I0.33.10.49       10.33.10.49       255.255.255.0       10.33.10.1         10.33.10.50       10.33.10.50       255.255.255.128       10.0.33.10.1         10.10.80.105       10.10.80.105       255.255.255.128       10.10.80.1         DNS Location DNS Location DNS Location DNS       Management IP(s) IP #1 (IPv4)       I0.33.10.29				System Information: SBCE		9
N       Requested: 0       512         Box Type       SIP       SIP       Advanced Sessions       512         Deployment Mode       Proxy       Scopia Video Sessions       512         Scopia Video Sessions       512       CES Sessions       512         Transcoding Sessions       512       CLID          Encryption       Requested: 0       Still       CLID          Image: Ves       Image: Ves       Image: Ves       Image: Ves       Image: Ves         Network Configuration       Image: Ves       Image: Ves       Image: Ves       Image: Ves         Network Configuration       Image: Ves       Image: Ves       Image: Ves       Image: Ves       Image: Ves         Network Configuration       Image: Ves       Image: Ves       Image: Ves       Image: Ves       Image: Ves         No       10.33.10.49       10.33.10.49       255.255.255.0       10.33.10.1       A1         10.10.80.105       10.10.80.105       255.255.255.128       10.10.80.1       B1         10.10.80.106       10.10.80.106       255.255.255.128       10.10.80.1       B1         10.10.80.106       10.10.80.106       255.255.255.128       10.10.80.1       B1         NS Config	General Configura	tion		Device Configuration	License Allocation —	
Deployment Mode       Proxy         Deployment Mode       Proxy         Advanced Sessions       512         Requested: 0       512         CES Sessions       512         Transcoding Sessions       512         CLID          Encryption       Z         Available: Yes       Z         ID-2000       10.33.10.49         10.33.10.49       10.33.10.49         255.255.255.0       10.33.10.1         A1       10.33.10.50         10.33.10.50       10.33.10.1         A1       10.33.10.50         10.33.10.50       10.33.10.1         A1       10.10.80.105         10.10.80.106       10.10.80.106         255.255.255.128       10.10.80.1         B1       10.10.80.106         10.10.80.106       10.10.80.1         B1       10.10.80.10         B1       10.10.80.1         B1       10.10.80.10	C			1998		512
Scopia Video Sessions       512         Requested: 0       512         CES Sessions       512         Transcoting Sessions       512         CLID          Encryption       Image: Comparison of the second s				Two Bypass Mode No		512
Network Configuration         Prequested: 0         512           IP         Public IP         Network Prefix or Subnet Mask         Gateway         Interface           10.33.10.49         10.33.10.49         255.255.255.0         10.33.10.1         A1           10.33.10.50         10.33.10.50         255.255.255.0         10.33.10.1         A1           10.10.80.105         10.10.80.105         255.255.255.128         10.10.80.1         B1           10.10.80.106         10.10.80.106         255.255.128         10.10.80.1         B1           DNS Configuration         Primary DNS         10.33.10.60         Primary DNS         10.33.10.29	Deployment mode	Полу				512
Requested: 0       0 <th0< th=""> <th< td=""><td></td><td></td><td></td><td></td><td>CES Sessions Requested: 0</td><td>512</td></th<></th0<>					CES Sessions Requested: 0	512
IP         Public IP         Network Prefix or Subnet Mask         Gateway         Interface           10.33.10.49         10.33.10.49         255.255.255.0         10.33.10.1         A1           10.33.10.50         10.33.10.50         255.255.255.0         10.33.10.1         A1           10.10.80.105         10.10.80.105         255.255.255.128         10.10.80.1         B1           10.10.80.106         10.10.80.106         255.255.255.128         10.10.80.1         B1           Primary DNS         10.33.100.60         IP #1 (IPv4)         10.33.10.29         IP #1 (IPv4)         10.33.10.29					Transcoding Sessions Requested: 0	512
Network Configuration         Public IP         Network Prefix or Subnet Mask         Gateway         Interface           10.33.10.49         10.33.10.49         255.255.255.0         10.33.10.1         A1           10.33.10.50         10.33.10.50         255.255.255.0         10.33.10.1         A1           10.10.80.105         10.10.80.105         255.255.255.128         10.10.80.1         B1           10.10.80.106         10.10.80.106         255.255.255.128         10.10.80.1         B1 <b>DNS Configuration</b> Primary DNS         10.33.100.60         IP #1 (IPv4)         10.33.10.29           Secondary DNS         10.33.100.60         IP #1 (IPv4)         10.33.10.29         IP #1 (IPv4)         10.33.10.29					CLID	
IP         Public IP         Network Prefix or Subnet Mask         Gateway         Interface           10.33.10.49         10.33.10.49         255.255.255.0         10.33.10.1         A1           10.33.10.50         10.33.10.50         255.255.255.0         10.33.10.1         A1           10.30.105         10.10.80.105         255.255.255.128         10.10.80.1         B1           10.10.80.106         10.10.80.106         255.255.255.128         10.10.80.1         B1           Primary DNS         10.33.100.60         IP #1 (IPv4)         10.33.10.29         IP #1 (IPv4)         10.33.10.29					Encryption Available: Yes	
10.33.10.49       10.33.10.49       255.255.255.0       10.33.10.1       A1         10.33.10.50       10.33.10.50       255.255.255.0       10.33.10.1       A1         10.10.80.105       10.10.80.105       255.255.255.128       10.10.80.1       B1         10.10.80.106       10.10.80.106       255.255.255.128       10.10.80.1       B1         DNS Configuration       Management IP(s)       IP #1 (IPv4)       10.33.10.29         Secondary DNS       10.33.100.60       IP #1 (IPv4)       10.33.10.29	Network Configura	ation				
10.33.10.50       10.33.10.50       255.255.255.0       10.33.10.1       A1         10.10.80.105       10.10.80.105       255.255.255.128       10.10.80.1       B1         10.10.80.106       10.10.80.106       255.255.255.128       10.10.80.1       B1 <b>DNS Configuration</b> Primary DNS       10.33.100.60       IP #1 (IPv4)       10.33.10.29         Secondary DNS	IP		Public IP	Network Prefix or Subnet Mas	k Gateway	Interface
10.10.80.105       10.10.80.105       255.255.255.128       10.10.80.1       B1         10.10.80.106       10.10.80.106       255.255.255.128       10.10.80.1       B1         DNS Configuration       Image: Configuration	10.33.10.49		10.33.10.49	255.255.255.0	10.33.10.1	A1
10.10.80.106       10.10.80.106       255.255.128       10.10.80.1       B1         DNS Configuration	10.33.10.50		10.33.10.50	255.255.255.0	10.33.10.1	A1
DNS Configuration     Management IP(s)       Primary DNS     10.33.100.60       Secondary DNS     IP #1 (IPv4)	10.10.80.105		10.10.80.105	255.255.255.128	10.10.80.1	B1
Primary DNS         10.33.100.60         IP #1 (IPv4)         10.33.10.29           Secondary DNS         IIII = 100000000000000000000000000000000	10.10.80.106		10.10.80.106	255.255.255.128	10.10.80.1	B1
Secondary DNS	DNS Configuration	ī		Management IP(s)		
	Primary DNS	10.33.100.60		IP #1 (IPv4) 10.33.10.29		
DNS Location DMZ	Secondary DNS					
	DNS Location	DMZ				
DNS Client IP 10.10.80.106	DNS Client IP	10.10.80.106				

Figure 61: Avaya SBCE System Information

### 7.2. Server Interworking

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

### 7.2.1. 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.

ession Borde	r Controller for Ente	rprise		AVAy
IS Dashboard vice Management ckup/Restore	Interworking Profiles: SMVM Add			Rename Clone Dela
System Parameters Configuration Profiles Domain DoS Server Interworking	Interworking Profiles cs2100 avaya-ru SMVM	General Timers Privacy URI Manipulation Header Manip	Click here to add a description	
Media Forking Routing	SMVM	Hold Support 180 Handling	None None	
Topology Hiding Signaling Manipulation		181 Handling	None	
URI Groups SNMP Traps		182 Handling 183 Handling	None	
Time of Day Rules		Refer Handling	No	
FGDN Groups Reverse Proxy Policy		URI Group Send Hold	None No	
URN Profile Recording Profile		Delayed Offer 3xx Handling	Yes No	
ervices omain Policies		Diversion Header Support	No	
LS Management letwork & Flows		Delayed SDP Handling Re-Invite Handling	No	
MZ Services Ionitoring & Logging		Prack Handling	No	
ionitoring & Logging		Allow 18X SDP T.38 Support	No Yes	
		URI Scheme	ves SIP	
		Via Header Format	RFC3261	

Figure 62: Server Interworking – Avaya site

### 7.2.2. Configure Server Interworking Profile – Bell MTS 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 Bell MTS server interworking profile (named: SP4) was added.

Seccion Bordo	r Controller for Ente	rariaa		AVAV
bession border	Controller for Ente	iprise		AVAY
MS Dashboard	Interworking Profiles: SP4			
evice Management				Rename Clone Delet
ackup/Restore	Add			Rename Clone Delet
System Parameters	Interworking Profiles		Click here to add a description.	
Configuration Profiles	cs2100	General Timers Privacy URI Manipulat	on Header Manipulation Advanced	
Domain DoS	avaya-ru	General		
Server Interworking	SMVM			
Media Forking	SP4	Hold Support	None	
Routing		180 Handling	None	
Topology Hiding Signaling Manipulation		181 Handling	None	
URI Groups		182 Handling	None	
SNMP Traps		183 Handling	None	
Time of Day Rules		Refer Handling	No	
FGDN Groups		URI Group	None	
Reverse Proxy Policy		Send Hold	No	
URN Profile		Delayed Offer	Yes	
Recording Profile		3xx Handling	No	
Services Domain Policies		Diversion Header Support	No	
TLS Management		Delayed SDP Handling	No	
Network & Flows				
DMZ Services		Re-Invite Handling	No	
Monitoring & Logging		Prack Handling	No	
		Allow 18X SDP	No	
		T.38 Support	Yes	
		URI Scheme	SIP	
		Via Header Format	RFC3261	

#### Figure 63: Server Interworking – Bell MTS SIP Trunk site

### 7.3. Configure Signaling Manipulation

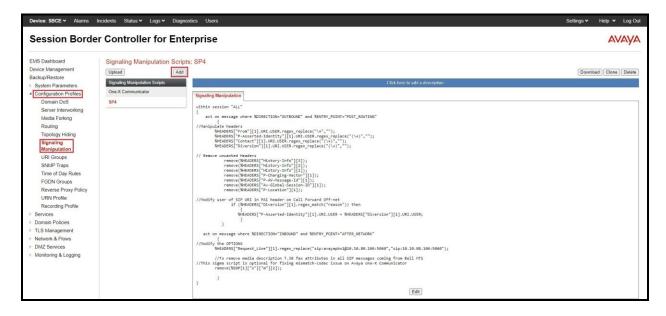
The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

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 user of SIP URI in SIP OPTION coming from Bell MTS

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	60 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

- Remove media description T38 fax attributes in all SIP messages coming from Bell MTS
- Remove the unwanted codec on SDP coming from Bell MTS (This is optional for fixing the mismatch-codec issue on Avaya one-X Communicator
- Click **Save** (not shown)



**Figure 64: Signaling Manipulation** 

Note: See Appendix B in Section 14 for the reference of this signaling manipulation (SigMa) script.

### 7.4. Configure Services

#### 7.4.1. Configure SIP 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: 10.33.10.53 (Session Manager IP Address)
- Port: 5061
- Transport: TLS
- Click **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🖌 Di	agnostics Users				Set	tings 🗸 🛛 He	lp 🗸 Log Out
Session Borde	r Controller for E	nterprise						AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles Services LDAP	SIP Servers: SMVM Add Server Profiles SMVM	General Authentication H Server Type TLS Client Profile DNS Query Type	eartbeat Registration	Ping Advanced Call Server AvayaSBCClient NONE/A			Rename	Cione Delete
RADIUS Domain Policies		IP Address / FQDN 10.33.10.53	_	_	Port 5061	Transport TLS		
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> <li>DMZ Services</li> </ul>				E	Edit			

Figure 65: 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	eartbeat Registration Ping Advanced
Enable DoS Protection	
Enable Grooming	
Interworking Profile	SMVM
Signaling Manipulation Script	None
Securable	
Enable FGDN	
Tolerant	
URI Group	None
	Edit

Figure 66: SIP Server – Advanced - Avaya site

### 7.4.2. Configure SIP Server – Bell MTS SIP Trunk

From the menu on the left-hand side, select Services  $\rightarrow$  SIP Servers  $\rightarrow$  Add The signaling server IP addresses is 192.168.168.20 (Bell MTS signaling server)

#### Enter Profile Name: SP4

On General tab, enter the following:

- Server Type: Select Trunk Server
- IP Address/FQDN: 192.168.168.20 (Bell MTS signaling server IP address)
- Port: 5060
- Transport: UDP
- Click **Finish** (not shown)

Device: SBCE Y Alarms	Incidents Status V Logs V Diagno	stics Users		
Session Borde	er Controller for Ente	rprise		
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles Services SIP Servers	SIP Servers: SP4 Add Server Profiles SMM SP4	General         Authentication         Heartbeat         Registration         Ping         Advanced           Server Type         DNS Query Type	Trunk Server NONE/A	
LDAP		IP Address / FQDN	Port	Transport
RADIUS		192.168.168.20	5060	UDP
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>			Edit	

Figure 67: SIP Server – General – Bell MTS

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

- Check Enable Heartbeat
- Select Method: OPTIONS
- Set Frequency: 60 seconds
- Input From URI: avaya.mts.ca (Bell MTS domain for production service)
- Input **To URI**: **avaya.mts.ca** (Bell MTS domain for production service)

nable Heartbeat	
Method	OPTIONS
Frequency	60 seconds
From URI	avayapbx1@avaya.mts.
To URI	avayapbx1@avaya.mts.c

#### Figure 68: SIP Server – Heartbeat – Bell MTS

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

- Interworking Profile: SP4 (see Section 7.2.2)
- Signaling Manipulation Script: SP4 (see Section 7.3)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping	Advanced		
Enable [	DoS Protection						
Enable (	Grooming						
Interwor	king Profile					SP4	
Signalin	g Manipulation Scrip	ot				SP4	
Securab	le						
Enable F	FGDN						
Tolerant							
URI Gro	up					None	
							Edit

#### Figure 69: SIP Server – Advanced – Bell MTS

HV; Reviewed: SPOC 11/3/2020 Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved. On the **Authentication** tab, enter the following:

- Check **Enable Authentication** option
- Input User Name (Bell MTS provides the user name)
- Leave **Realm** as blank
- Enter **Password** (Bell MTS provides the password)
- Enter **Confirm Password** (Bell MTS provides the password)
- Click **Finish**

e Auth	Edit SIP Serv	er Profile - Authentication
er Na	Enable Authentication	
alm	User Name	avayapbx1
	Realm (Leave blank to detect from server challenge)	
	Password (Leave blank to keep existing password)	
	Confirm Password	©

**Figure 70: SIP Server – Authentication – Bell MTS** 

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

- Check **Register with All Servers** option
- Set Refresh Interval: 30 seconds
- Set From URI and To URI: avaya.mts.ca (Bell MTS provides this information)
- Click **Finish**

eneral	Authentication	Heartbeat	Registration	Ping	Advanced	
Register	with All Servers					
Register	with Priority Server	r				
Refresh I	nterval					30 seconds
From UR	1					avayapbx1@avaya.mts.ca
To URI						avayapbx1@avaya.mts.ca

Figure 71: SIP Server – Registration – Bell MTS

### 7.5. Routing

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

### 7.5.1. Configure Routing – Avaya Site

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

Enter Profile Name: SP4\_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 7.4.1)
- Next Hop Address: 10.33.10.53:5061 (TLS) (Session Manager IP address)
- Click Finish

MS Dashboard levice Management	Routing Profiles: SP4_					Rename Clone De
ackup/Restore	Add Routing Profiles			Click here to add a description.		Rename Clone De
System Parameters Configuration Profiles	default	Routing Profile				
Domain DoS Server Interworking	SP4_To_SMVM			Routing Profile		X Ac
Media Forking		URI Group	* ~	Time of Day	default ~	nsport
Routing Topology Hiding		Load Balancing	Priority ~	NAPTR		Edit Dele
Signaling Manipulation		Transport	None $\vee$	LDAP Routing		
URI Groups		LDAP Server Profile	None $\vee$	LDAP Base DN (Sear	ch) None 🗸	
SNMP Traps Time of Day Rules		Matched Attribute Priority		Alternate Routing		
FGDN Groups		Next Hop Priority		Next Hop In-Dialog		
Reverse Proxy Policy Services		Ignore Route Header				
Domain Policies						
TLS Management		ENUM		ENUM Suffix		
Network & Flows DMZ Services						Add
Monitoring & Logging		Priority LDAP Search	LDAP Search LDAP Search	SIP Server Profile Next Hop Address	Transport	
		Weight Attribute	Regex Pattern Regex Result	SIP Server Profile Next Hop Address	Transport	

Figure 72: Routing to Session Manager

### 7.5.2. Configure Routing – Bell MTS 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\_SP4** 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: SP4 (see Section 7.4.2); Next Hop Address: 192.168.168.20:5060 (UDP) (Bell MTS signaling server IP address)
- Click **Finish**

Device: SBCE ❤ Alarms Inc	idents Status 🗸 Logs 🕯	<ul> <li>Diagnostics</li> </ul>	Users					
		Diagnoonoo		_		_		
Session Border	<b>Controller fo</b>	r Enterpi	ise					
-								
EMS Dashboard Device Management	Routing Profiles: SM	The second se						
Backup/Restore		Add						
<ul> <li>System Parameters</li> </ul>	Routing Profiles							add a descrip
<ul> <li>Configuration Profiles</li> </ul>	default	Rot	ting Profile					
Domain DoS	To_SMVM_RW							
Server Interworking			odate Priority	Add Routing	Dulo			x
Media Forking	· · · · · · · · · · · · · · · · · · ·			Add Rodding	Kule			~
Routing	URI Group	* •	]		Time of Day	default 🗸		
Topology Hiding	Load Balancing	Priority	~		NAPTR			
Signaling Manipulation URI Groups	Transport	None 🛩			LDAP Routing	0		
SNMP Traps								
Time of Day Rules	LDAP Server Profile	None 🛩			LDAP Base DN (Search)	None 🛩		
FGDN Groups	Matched Attribute Priority	12			Alternate Routing			
Reverse Proxy Policy	Next Hop Priority				Next Hop In-Dialog			
URN Profile	Ignore Route Header	0						
Recording Profile	ignoro riculo riculor	U.						
<ul> <li>Services</li> </ul>								
SIP Servers	ENUM				ENUM Suffix			
LDAP RADIUS								Add
<ul> <li>Domain Policies</li> </ul>								7100
<ul> <li>TLS Management</li> </ul>	Priority / LDAP Search / Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Pro	file Next Hop Address		Transport	
Network & Flows	Weight	Reger Futtern	Reger Result					
DMZ Services	1			SP4	▶ 192.168.168.20:50	60 (UDP) 🗸	None 🗸	Delete
Monitoring & Logging				Finish				

Figure 73: Routing to Bell MTS SIP Trunk

# 7.6. **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.

### 7.6.1. Configure Topology Hiding – Avaya Site

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: SP4\_To\_SMVM and click Finish (not shown)
- Select **SP4\_To\_SMVM** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- 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**
- 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

#### Click Finish (not shown)

Device: SBCE ~ Alarms I Session Borde	ncidents Status V Logs				Settings v Help v Log C
EMS Dashboard Device Management Backup/Restore	Topology Hiding Pro	ofiles: SP4_To_SMVM		Click here to add a description	Rename Clone Delete
System Parameters Configuration Profiles	default	Topology Hiding			
Domain DoS Server Interworking	cisco_th_profile SP4_To_SMVM	Header	Criteria	Replace Action	Overwrite Value
Media Forking	314_10_3MVM	Record-Route	IP/Domain	Auto	(mm)
Routing		SDP	IP/Domain	Auto	
Topology Hiding		Refer-To	IP/Domain	Auto	
Signaling Manipulation		From	IP/Domain	Overwrite	bvwdev.com
URI Groups SNMP Traps		То	IP/Domain	Overwrite	bvwdev.com
Time of Day Rules		Referred-By	IP/Domain	Auto	
FGDN Groups		Request-Line	IP/Domain	Overwrite	bvwdev.com
Reverse Proxy Policy		Via	IP/Domain	Auto	
Services Domain Policies				Edit	
TLS Management					

#### Figure 74: Topology Hiding To Session Manager

HV; Reviewed: SPOC 11/3/2020 Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved. 70 of 122 BM\_CMSM81SBC81

### 7.6.2. Configure Topology Hiding Profile – Bell MTS SIP Trunk site

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\_SP4 and click Finish (not shown)
- Select **SMVM\_To\_SP4** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite** In the **Overwrite Value** column: **avaya.mts.ca**
- For the Header **To**,
  - In the Criteria column select IP/Domain
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **avaya.mts.ca**
- For the Header **Request-Line**,
  - In the Criteria column select IP/Domain
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **avaya.mts.ca** Note: avaya.mts.ca is Bell MTS SIP domain
- Click **Finish** (not shown)

	ncidents Status 🛩 Logs 🛩				Settings 🛩 Help 🛩 Lu
Session Borde	r Controller for	Enterprise			AVA
EMS Dashboard	Topology Hiding Profile	es: SMVM_To_SP4			
evice Management		Add			Rename Clone D
ackup/Restore System Parameters	Topology Hiding Profiles			Click here to add a description	
Configuration Profiles	default	Topology Hiding			
Domain DoS Server Interworking	cisco_th_profile SP4 To SMVM	Header	Criteria	Replace Action	Overwrite Value
Media Forking		Referred-By	IP/Domain	Auto	
Routing	SMVM_To_SP4	Via	IP/Domain	Auto	-
Topology Hiding		From	IP/Domain	Overwrite	avaya.mts.ca
Signaling Manipulation		To	IP/Domain	Overwrite	avaya.mts.ca
URI Groups SNMP Traps		Refer-To	IP/Domain	Auto	-
Time of Day Rules		Request-Line	IP/Domain	Overwrite	avaya.mts.ca
FGDN Groups		Record-Route	IP/Domain	Auto	6775 Gold
Reverse Proxy Policy		SDP	IP/Domain	Auto	
URN Profile Recording Profile				Edit	

Figure 75: Topology Hiding To Bell MTS

# 7.7. **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.

### 7.7.1. 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** → **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 fo	or Enterprise				AV	AYA
EMS Dashboard Device Management	Application Rules:	SIP-Trunk			Rename	Clone	Delete
Backup/Restore ▹ System Parameters	Application Rules		Click here to add a o	lescription.			
<ul> <li>Configuration Profiles</li> <li>Services</li> </ul>	default default-trunk	Application Rule					
Domain Policies	default-subscriber-low	Application Type	In Out Max	imum Concurrent Sessions	Maximum Sess	ions Per Ei	ndpoint
Application Rules	default-subscriber-high	Audio	2000	l.	2000		
Media Rules	default-server-low	Video					
Security Rules	default-server-high	Miscellaneous					
Signaling Rules	SIP-Trunk	CDR Support	Off				
Charging Rules End Point Policy	RW_AR	RTCP Keep-Alive	No				
Groups			Edit				
Session Policies							

Click on **Finish** (not shown)

**Figure 76: Application Rule** 

Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved.

### 7.7.2. 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	ıs	Users			Se	ettings 🗸	Help 🗸	Log Out
Session Bord	er Controller f	or Enterp	orise					AV	AYA
EMS Dashboard Device Management Backup/Restore	Signaling Rules: S	IP-Trunk					Rename	Clone	Delete
System Parameters	Signaling Rules			Click h	ere to add a description				·
<ul> <li>Configuration Profiles</li> <li>Services</li> </ul>	No-Content-Type-Ch	General Requ	lests Responses	Request Headers	Response Headers	Signaling QoS	UCID		
Domain Policies	SIP-Trunk	Signaling QoS		$\checkmark$					
Application Rules Border Rules		QoS Type		DSI	CP				
Media Rules		DSCP		EF					
Security Rules					Edit				
Signaling Rules		L							

**Figure 77: Signaling Rule** 

## 7.7.3. 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: SIP-Trunk
  - Application Rule: SIP-Trunk (See in Section 7.7.1)
  - Border Rule: default
  - Media Rule: default-low-med (With this setting, RTP was used between Communication Manager and Avaya SBCE. See Section 2.2 for media issue in details)
  - Security Rule: default-low
  - Signaling Rule: SIP-Trunk (See in Section 7.7.2)
- Select **Finish** (not shown)

Session Bord	er Controller for Ent	erprise								AVAY
MS Dashboard Device Management Backup/Restore	Policy Groups: SIP-Trunk	]							Rename	Clone Delet
System Parameters	Policy Groups				10	Click here to add a descript	ion.			
Configuration Profiles	default-low				CI	ick here to add a row descri	iption.			
Services	default-low-enc		1				Participant and a second se			
Domain Policies	default-med	Policy Group								
Application Rules	default-med-enc	1								Summary
Border Rules Media Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Security Rules	default-high-enc	1	SIP-Trunk	default	default-low-med	default-low	SIP-Trunk	None	Off	Edit
Signaling Rules	avaya-def-low-enc									
Charging Rules	avava-def-high-subscriber									
End Point Policy Groups	avaya-def-high-server									
Session Policies	SMVM RW									
TLS Management	SIP.Trunk									

Figure 78: Endpoint Policy

### 7.8. Network & Flows

The Network & Flows 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.

#### 7.8.1. 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 inside interface as follows:
  - Name: Network\_A1
  - Default Gateway: 10.33.10.1
  - Subnet Mask: 255.255.255.0
  - Interface: A1 (This is the Avaya SBCE inside interface)
  - Click the Add button to add the IP Address for inside interface: 10.33.10.49
  - Click the **Finish** button to save the changes

Device: SBCE 🛩 Alarms I	ncidents Status 🕶 Logs 🛩 Diagnostics l	Isers				Settings 🛩	Help 🗸	Log Out
Session Borde	r Controller for Enterpri	se					A۷	AYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Network Management							Add
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Name Gateway	Subne	et Mask / Prefix Length	Interface	IP Address			
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>	Network_B1		Add Network		x		Edit	Delete
Network & Flows Network	Network_A1	Name	Network_A1				Edit	Delete
Management		Default Gateway	10.33.10.1					
Media Interface Signaling Interface		Network Prefix or Subnet Mask	255.255.255.0					
End Point Flows		Interface	A1 🗸					
Session Flows Advanced Options					Add			
<ul> <li>DMZ Services</li> </ul>		IP Address	Public IP	Gateway Override				
Monitoring & Logging		10.33.10.49	Use IP Address	Use Default	Delete			
			Finish					

Figure 79: Network Management – Inside 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 outside interface as follows:
  - Name: Network\_B1
  - Default Gateway: 10.10.80.1
  - Subnet Mask: 255.255.255.128
  - Interface: B1 (This is the Avaya SBCE outside interface)
  - Click the Add button to add the IP Address for outside interface: 10.10.80.106
  - Click the **Finish** button to save the changes

Device: SBCE - Alarms	ncidents Status 🗸 Logs 🗸 Diagnostics Users		Settings 👻 Help 👻 Log Out
Session Borde	r Controller for Enterprise		AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Network Management		
<ul> <li>Services</li> </ul>	Name Gateway	Subnet Mask / Prefix Length Interface	Add IP Address
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>	Network_B1	Add Network	X Edit Delete
Network & Flows     Network     Management     Media Interface     Signaling Interface	Network_A1	Name         Network_B1           Default Gateway         10.10.80.1           Network Prefix or Subnet Mask         255 255 255 128	Edit Delete
End Point Flows Session Flows Advanced Options		Interface B1 V	Add
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>		IP Address     Ptolic IP     Cateway Overnoe       10.10.80.106     X     Use IP Address     Use Default	Delete

Figure 80: Network Management – Outside 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

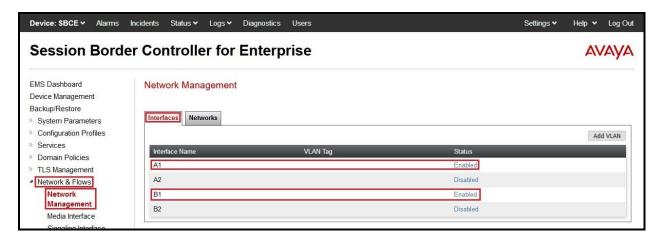


Figure 81: Network Management – Interface Status

### 7.8.2. 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 both inside and outside ports.

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\_B1 (B1, VLAN 0)** and **10.10.80.106** (External IP address toward Bell MTS)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - Name: InsideMedia
  - IP Address: Select Network\_A1 (A1, VLAN 0) and 10.33.10.49 (Internal IP address toward Session Manager)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)

Device: SBCE ~ Alarms	Incidents Status  ✓ Logs  ✓ Diagnostics	Users	s	ettings 🛩 🛛 Help	✓ Log Ou
Session Bord	er Controller for Enterp	orise		4	VAYA
EMS Dashboard Device Management Backup/Restore System Parameters Configuration Profiles	Media Interface				Add
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Name	Media IP Network	Port Range		
TLS Management	OutsideMedia	10.10.80.106 Network_B1 (B1, VLAN 0)	35000 - 40000	Ed	lit Delete
Network & Flows     Network Management     Media Interface	InsideMedia	10.33 10.49 Network A1 (A1, VLAN 0)	35000 - 40000	Ed	lit Delete

Figure 82: Media Interface

#### 7.8.3. 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\_B1 (B1, VLAN 0)** and **10.10.80.106** (External IP address toward Bell MTS)
  - 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\_A1 (A1, VLAN 0) and 10.33.10.49 (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 Bell MTS used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🖌 Diagn	gnostics Users					Settings 🗸	Help 🗸	Log Out
Session Borde	er Controller for Ent	terprise						AV	VAYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Signaling Interface								Add
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile			
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	OutsideUDP	10.10.80.106 Network_B1 (B1, VLAN 0)		5060		None		Edit	Delete
Network Management Media Interface Signaling Interface	InsideTLS	10.33.10.49 Network_A1 (A1, VLAN 0)			5061	AvayaSBCServer		Edit	Delete

**Figure 83: Signaling Interface** 

### 7.8.4. Configuration Server Flows

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

#### 7.8.4.1 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 7.4.1)
  - URI Group: \*
  - Transport: \*
  - Remote Subnet: \*
  - Received Interface: OutsideUDP (see Section 7.8.3)
  - Signaling Interface: InsideTLS (see Section 7.8.3)
  - Media Interface: InsideMedia (see Section 7.8.2)
  - Secondary Media Interface: None
  - End Point Policy Group: SIP-Trunk (see Section 7.7.3)
  - Routing Profile: SMVM\_To\_SP4 (see Section 7.5.2)
  - Topology Hiding Profile: SP4\_To\_SMVM (see Section 7.6.1)
  - Leave other parameters as default
  - Click Finish

Session Border Cont	troller for Ente	rprise		
Device Management Backup/Restore System Parameters Configuration Profiles Services	bint Flows	nly take effect on new sessions.		Add
TLS Management				Click here to add a row description.
Network & Flows		Add Flow	x	
Media Interface	v Name	SMVM Flow		
Signaling Interface SIP	Server Profile	SMVM V	_	
Session Flows	Group	* •		
Advanced Options Tran	nsport	* •	_	
	note Subnet	*		
Monitoring & Logging Rec	eived Interface	OutsideUDP		
Sign	naling Interface	InsideTLS V		
Med	dia Interface	InsideMedia 🗸		
Sec	ondary Media Interface	None 🗸		
End	Point Policy Group	SIP-Trunk 🗸		
Rou	iting Profile	SMVM_To_SP4 V		
Торо	ology Hiding Profile	SP4_To_SMVM V	_	
Sigr	naling Manipulation Script	None 🗸		
Ren	note Branch Office	Any 🗸		
Link	Monitoring from Peer	0		
		Finish		

Figure 84: End Point Flow 1

#### 7.8.4.2 Create End Point Flows – Bell MTS SIP Trunk Flow

From the menu on the left-hand side, select Network & Flows  $\rightarrow$  End Point Flows There is a Server Flows associated to Bell MTS signaling server.

- Select the Server Flows tab
- Select Add, enter Flow Name: SP4 Flow
  - Server Configuration: SP4 (see Section 7.4.2)
  - URI Group: \*
  - Transport: \*
  - Remote Subnet: \*
  - Received Interface: InsideTLS (see Section 7.8.3)
  - Signaling Interface: OutsideUDP (see Section 7.8.3)
  - Media Interface: OutsideMedia (see Section 7.8.2)
  - Secondary Media Interface: None
  - End Point Policy Group: SIP-Trunk (see Section 7.7.3)
  - Routing Profile: SP4\_To\_SMVM (see Section 7.5.1)
  - Topology Hiding Profile: SMVM\_To\_SP4 (see Section 7.6.2)
  - Leave other parameters as default
  - Click **Finish**

# **Session Border Controller for Enterprise**

/IS Dashboard evice Management	End Point Flows		
ackup/Restore System Parameters	Subscriber Flows Server Flows		
Configuration Profiles			1
Services			
Domain Policies	Modifications made to a Server How	will only take effect on new sessions.	500
TLS Management		Add Flow	X
Network & Flows Network Management	Flow Name	SP4 Flow	
Media Interface	SIP Server Profile	SP4 V	
Signaling Interface	URI Group	*	
End Point Flows Session Flows	Transport	*	
Advanced Options	Remote Subnet	*	
DMZ Services Monitoring & Logging	Received Interface	InsideTLS 🗸	
Monitoring & Logging	Signaling Interface	OutsideUDP 🗸	
	Media Interface	OutsideMedia 🗸	
	Secondary Media Interface	None 🗸	
	End Point Policy Group	SIP-Trunk	
	Routing Profile	SP4_To_SMVM 🗸	
	Topology Hiding Profile	SMVM_To_SP4	
	Signaling Manipulation Script	None 🗸	
	Remote Branch Office	Any 🗸	
	Link Monitoring from Peer		

Figure 85: End Point Flow 2

# 8. Configure Avaya Aura<sup>®</sup> Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [12] in the **References** section for further details if necessary.

## 8.1. Background

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

References to the Voice XML and/or Call Control XML applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party DID number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match is found, Experience Portal informs the caller that the call cannot be handled and disconnects the call<sup>1</sup>.

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

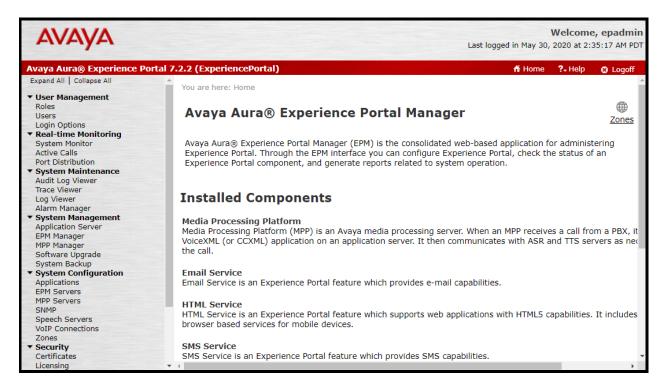
<sup>&</sup>lt;sup>1</sup> An application may be configured with "inbound default" as the called number, to process all inbound calls that do not match any other application references.

## 8.2. Logging in and Licensing

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

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

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



**Figure 86: Experience Portal – Home page** 

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

Avaya Aura® Experience Porta	al 7.2.2 (ExperiencePortal)		
Expand All   Collapse All			
	You are here: <u>Home</u> > Security >	Licensing	
<ul> <li>User Management</li> </ul>			
Roles	Licensing		
Users	Licensing		
Login Options • Real-time Monitoring			
System Monitor	This was a disalawy the Francis	n an Dautal Bannas Information that is summable in offert. Function	D+-1
Active Calls		nce Portal license information that is currently in effect. Experience	ce Portal us
Port Distribution	are used.		
System Maintenance			
Audit Log Viewer	License Server Information	_	
Trace Viewer	License Server Information		
Log Viewer			
Alarm Manager	License Server URL:	https://10.33.1.10:52233/WebLM/LicenseServer	6
System Management	Last Updated:	Jul 26, 2019 4:11:07 AM PDT	
Application Server	Last Successful Poll:	Sep 15, 2020 9:19:14 PM PDT	
EPM Manager			
MPP Manager			
Software Upgrade	Licensed Products 🔻		
System Backup	Experience Portal		4
<ul> <li>System Configuration</li> </ul>			0
Applications EPM Servers	Announcement Ports:	100	
MPP Servers	ASR Connections:	250	
SNMP	Email Units:	50	
Speech Servers	Enable Media Encryption:	250	
VoIP Connections	Enhanced Call Classification:	250	
Zones	Google ASR Connections:	10	
Security	HTML Units:	100	
Certificates	SIP Signaling Connections:	100	
Licensing	SMS Units:	100	
Reports	Telephony Ports:	100	
Standard	TTS Connections:	250	
Custom	Video Server Connections:	250	
Scheduled	Zones:	10	
<ul> <li>Multi-Media Configuration</li> </ul>	Zones.	10	
Email	Version:	8	
HTML	Last Successful Poll:	o Sep 15, 2020 9:19:14 PM PDT	
SMS			
	Last Changed:	Aug 14, 2019 4:25:43 AM PDT	

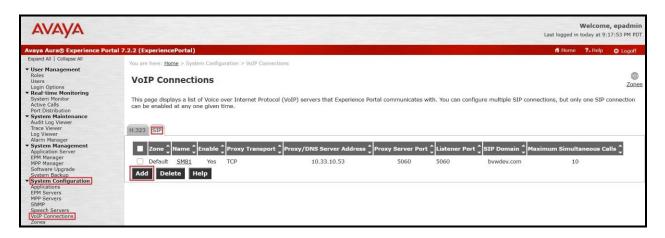
**Figure 87: Experience Portal – License** 

## 8.3. VolP Connection

This section defines a SIP trunk between Experience Portal and Session Manager.

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

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



**Figure 88: Experience Portal – VoIP Connection 1** 

**Step 2** - Configure a SIP connection as follows:

- Name Set to a descriptive name (e.g., SM81)
- Enable Set to Yes
- **Proxy Transport** Set to **TLS**
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address** = **10.33.10.53** (The IP address of the Session Manager)
  - **Port** = **5061**
  - **Priority** = 0 (default)
  - Weight = 0 (default)
- Listener Port Set to 5061
- SIP Domain Set to bvwdev.com
- Consultative Transfer Select INVITE with REPLACES
- SIP Reject Response Code Select ASM (503)
- Maximum Simultaneous Calls Set to a number in accordance with licensed capacity. In the reference configuration a value of **100** was used.
- Select All Calls can be either inbound or outbound
- SRTP Enable = Yes
- Encryption Algorithm = AES\_CM\_128
- Authentication Algorithm = HMAC\_SHA1\_80

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	87 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

- **RTCP Encryption Enabled = No**
- **RTP** Authentication Enabled = Yes
- Click on Add to add SRTP settings to the Configured SRTP List
- Use default values for all other fields
- Click **Save** (Not shown)

You are here: Home > System Configuration > VoIP Connections > Change SIP Connection	
Change SIP Connection	
Use this page to change the configuration of a SIP connection.	
Zone: Default  Name: SM81 Enable:  Yes No Proxy Transport: TLS DNS SRV Domain Address Port Priority Weight	
10.33.10.53 5061 0 0 Remove	
Additional Proxy Server	
SIP Domain: bvwdev.com	
P-Asserted-Identity:	
Maximum Redirection Attempts: 0	
Consultative Transfer: <ul> <li>INVITE with REPLACES</li> <li>REFER</li> </ul>	
SIP Reject Response Code: <ul> <li>ASM (503)</li> <li>SES (480)</li> <li>Custom</li> </ul>	
SIP Timers         T1:       250         milliseconds         T2:       2000         milliseconds         B and F:       4000         milliseconds	
Call Capacity Maximum Simultaneous Calls: 100	
All Calls can be either inbound or outbound	
Configure number of inbound and outbound calls allowed	
SRTP	
Enable: • Yes No	
Encryption Algorithm:	
Authentication Algorithm: <ul> <li>HMAC_SHA1_80</li> <li>HMAC_SHA1_32</li> </ul>	
RTCP Encryption Enabled: O Yes No	_
RTP Authentication Enabled:   Yes No	bb
Configured SRTP List	
SRTP-Yes,AES_CM_128,HMAC_SHA1_80,RTCP Encryption-No,RTP Authentication-Yes	en

**Figure 89: Experience Portal – VoIP Connection 2** 

HV; Reviewed: SPOC 11/3/2020 Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved.

## 8.4. Speech Servers

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

ASR speech server:

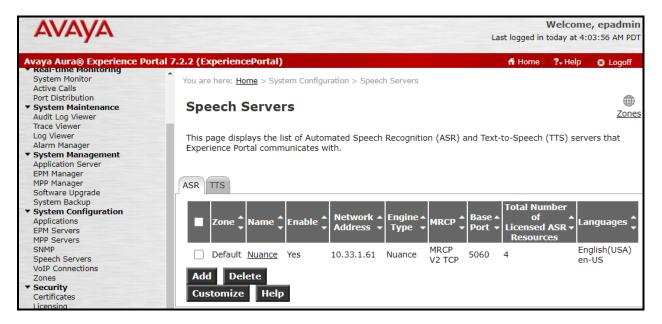


Figure 90: Experience Portal – ASR Speech Server

#### TTS speech server:

		Last logged in to		epadmin :56 AM PDT
al 7.2.2 (ExperiencePortal)		👫 Home	<b>?</b> ₊ Help	😫 Logoff
Speech Servers				① Zones
This page displays the list of Automated Speech Experience Portal communicates with.	Recognition (ASR) and	Text-to-Speech (1	ITS) server	s that
ASR TTS				
■ Zone ↓ Name ↓ Enable ↓ Network ↓ Address ↓			Voices	
Default <u>Nuance</u> Yes 10.33.1.61	Nuance MRCP V2 TCP 506		en-US Àl English(U en-US Av English(U	lison F, JSA) /a F, JSA)
	This page displays the list of Automated Speech Experience Portal communicates with.	Speech Servers         This page displays the list of Automated Speech Recognition (ASR) and Experience Portal communicates with.         ASR_TTS         Image: Some the list of Automated Speech Recognition (ASR) and Experience Portal communicates with.         ASR_TTS         Image: Some the list of Automated Speech Recognition (ASR) and Experience Portal communicates with.         ASR_TTS         Image: Some the list of Automated Speech Recognition (ASR) and Experience Portal communicates with.         ASR_TTS         Image: Some the list of Automated the list of Automated Speech Recognition (ASR) and Experience Portal communicates with.         ASR_TTS         Image: Some the list of Automated Speech Recognition (ASR) and Experience Portal communicates with.         ASR_TTS         Image: Some the list of Automated Speech Recognition (ASR) and Experience Portal communicates with.         Image: Some the list of Automated Speech Recognition (ASR) and Experience Portal communicates with the list of Automated Speech Recognition (ASR) and Experience Portal communicates with the list of Automated Speech Recognition (ASR) and the list of Automated Speech Recognited Speech Recognited Speech Recognition (ASR) and the list of Aut	Speech Servers         This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (Texperience Portal communicates with.         ASR TTS         Image: Some im	Speech Servers         This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) server Experience Portal communicates with.         ASR_TTS         Image: Some image: Name image: Some ima

Figure 91: Experience Portal – TTS Speech Server

## 8.5. Application

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

Step 1 - In the left pane, navigate to System Configuration→Applications. On the

**Applications** page (not shown), click **Add** to add an application and configure as follows:

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	91 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

needed. Inbound calls with these called party numbers will be handled by the application defined in this section.

You are he	re: <u>Home</u> > S	ystem Config	juration > <u>Appli</u>	cations > (	Change Ap	oplication			
Chan	ge Appl	ication							
Use this p	page to chan	ge the conf	iguration of an	applicatio	on.				
Zone: Name: Enable: Type: Reserved : Requested <b>URI</b>	SIP Calls:	Default Test_Voice> • Yes VoiceXML • None	No		num				
Sing	le 🔍 Fail O	ver 🔍 Loa	ad Balance						
VoiceXML	URL:	https://1	10.33.1.3/mpp	/misc/avp	testapp/	intro.vxml			
	ertificate Autl hentication:	hentication:	<ul><li>Yes</li><li>Yes</li><li>Yes</li></ul>						
ASR Spe	ech Servers	•							
	Engine Typ	es				Selected	Engine Ty	pes	
ASR:	<none></none>					Nuance			
Nuance									
Language	es				Selected	l Language	5		
<none></none>	>			Û	English	(USA) en-	US		•
Resource	es:		Acquire on o	call start	and reta	ain 🔻			
N Best Li	ist Length:								
Speech C	Complete Tim	eout:	0	millisecon	ds				
Speech I	ncomplete Ti	meout:		millisecon	ds				
Vendor P	arameters:				11				
TTS Spee	ech Servers	•							
TTS: Nu	ance ▼	English(U	SA) en-US Av SA) en-US Na SA) en-US Zo	athan M				d Voices I(USA) en-US	Allison F
Applicati	ion Launch	•							
Inbo	und 🔍 Inb	ound Defau	lt 🔍 Outbour	nd					
Nun	nber 🔍 Nur	nber Range							
Called N				Add					
4800						•	Rem	ove	
Speech F	Parameters	•							
-	ig Paramete								
Advance Save	d Paramete	rs ↓ Cancel	Help						
Save	мрру	Cancer	meip.						

#### **Figure 92: Experience Portal – Application**

HV; Reviewed: SPOC 11/3/2020 Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved. 93 of 122 BM\_CMSM81SBC81

## 8.6. MPP Servers and VoIP Settings

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

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

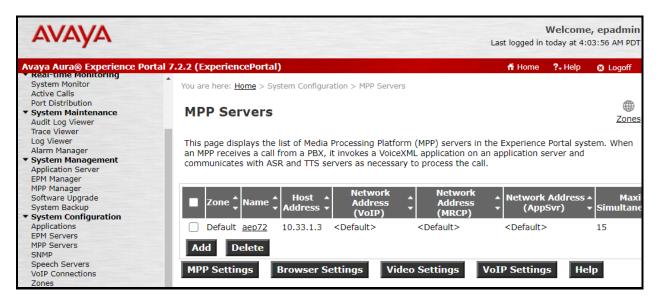


Figure 93: Experience Portal – MPP Server 1

- Step 2 Enter any descriptive name in the Name field (e.g., aep72) and the IP address of the MPP server in the Host Address field and click Continue (not shown). Note that the Host Address used is the same IP address assigned to Experience Portal.
- Step 3 The certificate page will open. Check the **Trust this certificate** box (not shown). Once complete, click **Save**.

You are here: <u>Home</u> > System Con	nfiguration > MPP Servers > Change MPP Server					
Change MPP Serve	er					
Trace Levels to Finest if your E	onfiguration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set xperience Portal system has heavy call traffic. The system might experience performance o Finest. Set Trace Levels to Finest only when you are troubleshooting the system.					
Zone:	Default					
Name:	aep72					
Host Address:	10.33.1.3					
Network Address (VoIP):	<default></default>					
Network Address (MRCP):	<default></default>					
Network Address (AppSvr):	<default></default>					
Maximum Simultaneous Calls:	15					
Restart Automatically:	🔍 Yes 🔍 No					
MPP Certificate						
<pre>MPP Certificate Owner: C=US,O=AVAYA,OU=SDP,CN=aep72 Issuer: O=AVAYA,OU=MGMT,CN=SystemManager CA Serial Number: 352dbbbde22c8aa8 Signature Algorithm: SHA256withRSA Valid from: June 28, 2019 4:38:19 AM PDT until September 26, 2022 4:38:19 AM PDT Certificate Fingerprints</pre>						
Categories and Trace Levels	• •					
Save Apply Cancel	Нер					

#### Figure 94: Experience Portal – MPP Server 2

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

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	95 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

#### Step 5 - Click on Save (not shown)

You are here: <u>Home</u> > System Configuration > <u>MPP Servers</u> > VoIP Settings
VoIP Settings
Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.
Port Ranges 🔻
Low         High           UDP:         11000         30999           TCP:         31000         33499           MRCP:         34000         36499
H.323 37000 39499 39499
RTCP Monitor Settings 🔻
Host Address:
VoIP Audio Formats 🔻
MPP Native Format: audio/basic 🔻
Codecs 🔻
Offer
Enable Codec Order
G711uLaw         1
<ul> <li>✓ G711aLaw 2</li> <li>✓ G729 3</li> </ul>
Packet Time: 20 V milliseconds
G729 Discontinuous Transmission: O Yes No
Answer
Enable Codec Order
G711uLaw 1
Image: G711aLaw         2           Image: G729         3
G729 3 G729 Discontinuous Transmission: Yes No Either
G729 Reduced Complexity Encoder:       Yes       No
QoS Parameters → Out of Service Threshold (% of VoIP Resources) → Call Progress →
Miscellaneous >
Save Apply Cancel Help

#### Figure 95: Experience Portal – MPP Server - VoIP

HV; Reviewed: SPOC 11/3/2020 Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved. 96 of 122 BM\_CMSM81SBC81

## 8.7. Configuring RFC2833 Event Value Offered by Experience Portal

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

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

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

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

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

Avaya Aura® Experience Por Real-time Monitoring	tal 7.2.2 (ExperiencePortal)	📅 Home 🛛 😯 Help 🛛 😆 Logoff
System Monitor Active Calls	You are here: <u>Home</u> > System Management > MPP Manager	
Port Distribution • System Maintenance Audit Log Viewer Trace Viewer	MPP Manager (Jul 20, 2020 4:17:42 AM I	PDT) Refresh Zones
Log Viewer Alarm Manager System Management Application Server EPM Manager	This page displays the current state of each MPP in the Experi mode commands, select one or more MPPs. To enable the mo stopped.	
MPP Manager Software Upgrade System Backup	La	st Poll: Jul 20, 2020 4:17:27 AM PDT Restart Schedule Active Calls
<ul> <li>System Configuration Applications</li> </ul>	Zone Server Name Mode State Config Auto Rest	Today Recurring In Out
EPM Servers MPP Servers SNMP	✓ Default aep72 Online Running OK Yes 🖋	No 🖉 None 🖉 0 0
Speech Servers VoIP Connections	State Commands	
Zones • Security	Start Stop Restart Reboot Halt Cancel	Restart/Reboot Options
Certificates Licensing <b>Reports</b>	Mode Commands	One server at a time
Standard Custom	Offline Test Online	All servers
Scheduled	onnic rese onnic	

Figure 96: Experience Portal – MPP Manager

# 9. Bell MTS SIP Trunk Configuration

Bell MTS is responsible for the configuration of Bell MTS SIP Trunk Service. Customer must provide the IP Address used to reach the Avaya SBCE public interface at the enterprise. Bell MTS will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Bell MTS. Bell MTS also provides the Bell MTS 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 Bell MTS SIP Trunk and the enterprise is a static IP Address configuration.

## 10. 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.

## 11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura<sup>®</sup> Communication Manager 8.1, Avaya Aura<sup>®</sup> Session Manager 8.1, Avaya Aura<sup>®</sup> Experience Portal 7.2.2 and Avaya Session Border Controller for Enterprise 8.1 to Bell MTS. This solution successfully passed compliance testing via the Avaya DevConnect Program.

## 12. 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<sup>®</sup> Session Manager/System Manager

- [1] Administering Avaya Aura® Session Manager, Release 8.1.x, Issue 5, July 2020
- [2] Administering Avaya Aura® System Manager, Release 8.1.x, Issue 6, April 2020

#### Avaya Aura<sup>®</sup> Communication Manager

[3] Administering Avaya Aura ®Communication Manager, Release 8.1.x, Issue 6, March 2020

#### Avaya Phones

- [4] Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones H.323, Release 6.8.2, Issue 1, June 2019
- [5] Installing and Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP Release 7.1.7, Issue 1, October 2019
- [6] Avaya one-X® Communicator Release 6.2 SP14 Release Notes, Issue 1.0, June 2019
- [7] Avaya IX<sup>TM</sup> Workplace Client (Windows) Release 3.9 Release Notes, Issue 1.0, June 2020

#### Avaya Session Border Controller for Enterprise

[8] Avaya Session Border Controller for Enterprise 8.1 Release Notes, Release 8.1.0.0, Issue 1, February 2020

#### Avaya Aura Experience Portal

[9] Administering Avaya Aura® Experience Portal, Release 7.2.2, Issue 1, March 2019

#### IETF (Internet Engineering Task Force) SIP Standard Specifications

[10] RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org

Product documentation for Bell MTS SIP Trunking may be found at: https://www3.bellmts.ca/mts/enterprise/business+solutions/voice/sip+trunking

# 13. 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 Bell MTS 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<sup>®</sup> Communicator SIP softphone and Avaya Workplace Client.

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.

## 13.1. 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 B1, and two "inside" IP Addresses assigned to physical interface A1.

**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:

- **10.10.80.106** is the Avaya SBCE "outside" IP address previously provisioned for SIP Trunking with Bell MTS (see Section 7.8.1)
- **10.10.80.105** is the new Avaya SBCE "outside" IP address for Remote Worker access to Session Border Controller
- **10.33.10.49** is the Avaya SBCE "inside" IP address previously provisioned for SIP Trunking with Session Manager (see **Section 7.8.1**)
- **10.33.10.50** 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 Borg	der Controller for E	nternrise				AVA
Dession Dore		nerprise				FIVE
EMS Dashboard	Network Management					
evice Management	Network Management					
ackup/Restore						
System Parameters	Interfaces Networks					
Configuration Profiles						Ad
				Interface	IP Address	Lincol
Services	Nama	Cateway				
Services Domain Policies	Name	Gateway	Subnet Mask / Prefix Length		A CONTRACTOR OF A CONTRACTOR O	
	Name Network_B1	Gateway 10.10.80.1	Subnet Mask / Prenx Length 255.255.255.128	B1	10.10.80.105 10.10.80.106	Edit Delet

Figure 97: Network Management

On the **Interfaces** tab, verify that Interfaces **A1** and **B1** are both set to **Enabled** as previously configured for the Bell MTS SIP Trunk access in **Section 7.8.1**.

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🗸 Diag	gnostics Users	S	ettings 🛩 He	elp 🖌 Log Out
Session Bord	er Controller for Er	terprise			AVAYA
EMS Dashboard	Network Management				
Device Management					
Backup/Restore					
System Parameters	Interfaces Networks				
Configuration Profiles					Add VLAN
Services	Interface Name	VLAN Tag	Status		
Domain Policies	A1	,	Enabled		
TLS Management	A2		Disabled		
<ul> <li>Network &amp; Flows</li> </ul>	Manage				
Network Management	B1		Enabled		
Media Interface	B2		Disabled		
Signaling Interface					

**Figure 98: Network Interface Status** 

## 13.2. Media Interface on Avaya SBCE

From the menu on the left-hand side, select Network & Flows  $\rightarrow$  Media Interface

- Select the **Add** button and enter the following:
  - Name: OutsideMedRW
  - **IP Address**: Select **Network\_B1 (B1, VLAN 0)** and **10.10.80.105** (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\_A1 (A1, VLAN 0) and 10.33.10.50 (Internal IP address toward Session Manager)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)

Session Borde	er Controller for Enterpr	ise		AVAY
MS Dashboard	Media Interface			
vice Management				
ickup/Restore				
System Parameters	Media Interface			
Configuration Profiles				Add
Services Domain Policies	Name	Media IP Network	Port Range	
TLS Management	OutsideMedia	10.10.80.106 Network_B1 (01. VLAN 0)	35000 - 40000	Edit Delete
Network & Flows Network Management	OutsideMedRW	10.10.80.105 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
Media Interface Signaling Interface	InsideMedia	10.33.10.49 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
End Point Flows	InsideMedRW	10.33.10.50	35000 - 40000	Edit Delete

#### **Figure 99: Media Interface**

Note: Media Interface **OutsideMedRW** is used in the Remote Worker Subscriber Flow (Section 13.8.1), and Media Interface **InsideMedRW** is used in the Remote Worker Server Flow (Section 13.8.2.1).

## 13.3. 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\_B1 (B1, VLAN 0) and 10.10.80.105 (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\_A1 (A1, VLAN 0) and 10.33.10.50 (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 on **Finish** (not shown)

Session Borde	er Controller for En	terprise					AVA
MS Dashboard Device Management Backup/Restore	Signaling Interface						
System Parameters Configuration Profiles	Signaling Interface						
Services Domain Policies	Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
TLS Management	InsideSIGRW	10.33.10.50 Network_A1 (A1, VLAN 0)			5061	AvayaSBCServer	Edit De
Network & Flows	OutsideUDP	50.207.80.106 Network_B1 (B1, VLAN 0)		5060		None	Edit De
Network Management		10.33.10.49			5061	AvayaSBCServer	Edit De
Network Management Media Interface Signaling Interface	InsideTLS	Network_A1 (A1, VLAN 0)					

#### **Figure 100: Signaling Interface**

Note: Signaling Interface **OutsideSIGRW** is used in the Subscriber Flows (**Section 13.8.1**), and in the Remote Worker Server Flow (**Section 13.8.2.1**). Signaling Interface **InsideSIGRW** is used in the Remote Worker Server Flow (**Section 13.8.2.1**).

## 13.4. 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: 10.33.10.53:5061 (TLS) (IP address of Session Manager)
- Click **Finish**

The Routing Profile To\_SMVM\_RW is used in the Subscriber Flows (Section 13.8.1).

Device: SBCE 🗸 Alarms In	cidents Status 🗸 Logs 🗸	Diagnostics Users			Settings 🕶 Help 👻 Log Out
Session Border	Controller for	r Enterprise			AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles Domin DoS	Routing Profiles: To Routing Profiles default To SMVM RW			Click here to add a description.	Rename Clone Delete
Server Interworking			Routing Profile	x	Add
Media Forking Routing	URI Group	* ~	Time of Day	default ∨	Transport TLS Edit Delete
Topology Hiding	Load Balancing	Priority ~	NAPTR		
Signaling Manipulation URI Groups	Transport	None $\sim$	LDAP Routing		
SNMP Traps	LDAP Server Profile	None $\vee$	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				
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>					
<ul> <li>Network &amp; Flows</li> </ul>	ENUM		ENUM Suffix		
DMZ Services				Add	
Monitoring & Logging	Priority // Weight 1	LDAP Search Regex Pattern Regex Result	SIP Server Profile Next Hop Address SMVM V 10.33.10.53.5061 (T Bock Finish	Transport LS) V None V Delete	

Figure 101: 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 13.8.2.1.

Device: SBCE - Alarms Ind	cidents Status 🛩 Logs	✓ Diagnostics Users				
Session Border	Controller fo	or Enterprise				
EMS Dashboard Device Management Backup/Restore	Routing Profiles: de	fault_RW				Click here to ad
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> <li>Domain DoS</li> <li>Server Interworking</li> <li>Mode Endors</li> </ul>	default To_SMVM_RW	Routing Profile	Routing Profile			X
Media Forking Routing	URI Group	* ~	1	Time of Day	default $\vee$	
Topology Hiding Signaling Manipulation	Load Balancing	DNS/SRV		NAPTR		
URI Groups	Transport	None $\vee$	l	LDAP Routing		
SNMP Traps Time of Day Rules	LDAP Server Profile	None $\vee$	L	LDAP Base DN (Search)	None $\vee$	
FGDN Groups	Matched Attribute Priority		4	Alternate Routing		
Reverse Proxy Policy	Next Hop Priority		1	Next Hop In-Dialog		
Services     Domain Policies	Ignore Route Header					
TLS Management						
<ul> <li>Network &amp; Flows</li> <li>DMZ Services</li> </ul>	ENUM		E	ENUM Suffix		
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>						Add
	Click the Add button	to add a Next-Hop Address.				
			Back			

Figure 102: Remote Worker Default Routing

# 13.5. 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)

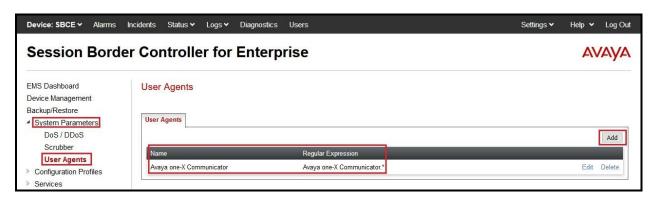


Figure 103: User Agents for Remote Worker

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 Avaya 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: 1613XXX5095@bvwdev.com SIP/2.0 From: sip:4612@bvwdev.com;tag=-59f03c7f529fb7c152aa3fd4\_F0950710.10.98.79 To: sip:1613XXX5095@bvwdev.com CSeq: 24 INVITE Call-ID: 18\_a7e80-49279ea452aa365c\_I@10.10.98.79 Contact: < sip:4612@10.10.98.79:5061;transport=tls;subid\_ipcs=378455751>;+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**/6.2.14.2 (Engine GA-2.2.0.183; 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 104: Output of trace for User Agent

Note: The User Agent is defined in its associated Subscriber Flows in Section 13.8.1.

# 13.6. 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)

Incidents Status V Logs	s∨ Diagnostics Users				Settings 🗸	<ul> <li>Help </li> </ul>	<ul> <li>Log Out</li> </ul>
r Controller fo	or Enterprise					A	VAYA
Application Rules:	RW_AR						
Add					Ren	ame Clone	Delete
Application Rules		Click h	ere to a	add a description.			
default	Application Rule						
default-trunk							
default-subscriber-low	Balance and a second	In	Section of the	Maximum Concurrent Sessions	Maximum <sup>•</sup>	Sessions Per F	Endpoint
default-subscriber-high	Audio			2000	2000		
default-server-low	Video			100	10		
default-server-high	Miscellaneous						
SIP-Trunk	CDR Support	Off					
RW_AK			E	Edit			
	er Controller for Application Rules: f Add Application Rules default-trunk default-subscriber-low default-subscriber-low default-server-low default-server-low default-server-high	Application Rules: RW_AR Add Application Rules  Add Application Rules  Add Application Rules  Add Application Rule  CDR Support	er Controller for Enterprise	Application Rules: RW_AR Add Application Rules  Add Application Rules  Click here to a  Application Rule  Click here to a  Application Rule  Application Rul	Application Rules: RW_AR         Add         Application Rules:         Add         Application Rules         Image: Click here to add a description.         Image: Click here to add a description. <td< td=""><td>Application Rules: RW_AR         Add         Application Rules: RW_AR         Add         Application Rules         Gefault         default-subscriber-low         default-server-low         default-server-low</td><td>er Controller for Enterprise</td></td<>	Application Rules: RW_AR         Add         Application Rules: RW_AR         Add         Application Rules         Gefault         default-subscriber-low         default-server-low         default-server-low	er Controller for Enterprise

#### Figure 105: Remote Worker Application Rule

Note: The rule **RW\_AR** is assigned to the End Point Policy Groups in Section 13.7.

### 13.7. 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 13.6)
  - Border Rule = default
  - Media Rule = default-low-med
  - Security Rule = default-low
  - Signaling Rule = SIP-Trunk (see Section 7.8.3)
- Click on **Finish** (not shown)

The End Point Policy Group **SMVM\_RW** is used in the Subscriber Flow **Avaya one-X Communicator** in **Section 13.8.1** and Remote Worker Server Flow in **Section 13.8.2.1**.



Figure 106: Remote Worker End Point Policy

# 13.8. End Point Flows on Avaya SBCE

#### 13.8.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent Avaya one-X Communicator** that was created in **Section 13.5**. 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 13.5)
- **Source Subnet** = \* (default)
- Via Host = \* (default)
- **Contact Host** = \* (default)
- Signaling Interface = OutsideSIGRW (see Section 13.3)

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 13.2)
- Received Interface = None.
- End Point Policy Group = SMVM\_RW (see Section 13.7)
- Routing Profile = To\_SMVM\_RW (see Section 13.4)
- TLS Client Profile = None
- Signaling Manipulation Script = None
- **Presence Server Address** = Leave as blank

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

Session Borde	er Contro	oller for Enter	rprise						AVAY
MS Dashboard	End Point	t Flows							
evice Management									
ackup/Restore	-								
System Parameters	Subscriber	Flows Server Flows							
Configuration Profiles									Add
Services	Medification	ns made to an End-Point Flow w	ill only take of	laat on now reministre	tiono er re registratione				
Domain Policies	Woullication	ns made to an End-Foint Flow w	nii oniy take en	ect on new registra	atons or re-registrations.				
TLS Management				Hover over a	row to see its description.				
Network & Flows	Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group			
Network Management Media Interface	1	Avaya one-X Communicator	* -	*	Avaya one-X Communicator	SMVM RW	View	Clone	Edit Delete

#### **Figure 107: Remote Worker Subscriber Flows – 1**

HV; Reviewed: SPOC 11/3/2020 Solution & Interoperability Test Lab Application Notes ©2020 Avaya Inc. All Rights Reserved.

	View Flow: Avaya	one-X Communicator		)		
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	<b>*</b>					
Contact Host	*					
Signaling Interface	OutsideSIGRW					
Source	Subscri	ber				
Methods Allowed B	efore REGISTER					
User Agent	Avaya c	Avaya one-X Communicator				
Media Interface	Outside	OutsideMedRW				
	storfago Nono	None				
Secondary Media In	nenace None					
Secondary Media Ir End Point Policy G		_RW				
78	roup SMVM_	_RW /M_RW				

#### Figure 108: Remote Worker Subscriber Flows – 2

### 13.8.2. 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. Two existing Trunking Server Flows (SMVM Flow in **Section 7.8.4.1** and SP4 Flow in **Section 7.8.4.2**) are also used for Remote Worker.

### 13.8.2.1 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 7.4.1)
- **URI Group** = \* (default)
- **Transport** = \* (default)
- **Remote Subnet** = \* (default)
- Received Interface = OutsideSIGRW (see Section 13.3)
- Signaling Interface = InsideSIGRW (see Section 13.3)
- Media Interface = InsideMedRW (see Section 13.2)
- Secondary Media Interface = None
- End Point Policy Group = SMVM\_RW (see Section 13.7)
- Routing Profile = default\_RW (see Section 13.4)
- **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 —	
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	s <b>*</b> )	Routing Profile	default_RW
Received Interface	OutsideSIGRW	Topology Hiding Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 109: Remote Worker Server Flow

### 13.8.2.2 Trunking Server Flow

Two existing Trunking Server Flows (SMVM Flow in Section 7.8.4.1; SP4 Flow in Section 7.8.4.2) are also used for Remote Worker.

	View	Flow: SMVM Flow	)
- Criteria —		Profile	
Flow Name	SMVM Flow	Signaling Interface	InsideTLS
Server Configuration	SMVM	Media Interface	InsideMedia
URI Group	×	Secondary Media Interface	None
Transport	*	End Point Policy Group	SIP-Trunk
Remote Subnet	*	Routing Profile	SMVM_To_SP4
Received Interface	OutsideUDP	Topology Hiding Profile	SP4_To_SMVM
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 110: Trunking Server Flow – SMVM Flow

Criteria ———		Profile	
Flow Name	SP4 Flow	Signaling Interface	OutsideUDP
Server Configuration	SP4	Media Interface	OutsideMedia
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	SIP-Trunk
Remote Subnet	*	Routing Profile	SP4_To_SMVM
Received Interface	InsideTLS	Topology Hiding Profile	SMVM_To_SP4
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 111: Trunking Server Flow – SP4 Flow

# 13.9. Remote Worker Client Configuration

The following screen illustrates Avaya one-X 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<sup>®</sup> Communicator settings and click on Telephony under Accounts. Select Using as SIP Enter Extension and Password Set the Domain to bvwdev.com Click Add button to add a server into Server List Enter Proxy Server as 10.10.80.105 (see Section 13.1). Set Transport Type: TLS and Port: 5061. Click OK to submit the changes The other fields are default. Click OK to submit the settings.

Avaya one-X® Communicator Login	General Settings			? ×
	Accounts	Telephony		
Please log In:	Telephony Login	Using: O		
Extension: 4611 Password:	Messaging Security	Password:	4612	
	security		•••••	
Place and receive calls using This Computer + Log In	Devices and Services Outgoing Calls Phone Numbers Dialing Rules	Server List:	Add Rem	love
	Audio Video	Domain:	bvwdev.com	
	Public Directory Preferences	Mode:	Proxied	0
	Desktop Integration	Avaya Environment: Failback Policy:		\$
	Hot Keys		Auto	\$
	Network Advanced	Registration Policy:	Simultaneous	\$
	Advanced	Add Server		
		Proxy Server 10. Transport Type TLS Port 500	÷	
		will be used (TLS=50	ot specified, the default (61). DK Cancel	
	Auto-configure		ОК	Cancel

Figure 112: Avaya one-X Communicator - Settings

# 14. Appendix B - SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.3**.

```
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]);
      remove(%HEADERS["P-Charging-Vector"][1]);
      remove(%HEADERS["P-AV-Message-Id"][1]);
      remove(%HEADERS["Av-Global-Session-ID"][1]);
      remove(%HEADERS["P-Location"][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:avayapbx1@10.10.80.106:5060","sip:10.1 0.80.106:5060");

//To remove media description T.38 fax attributes in all SIP messages coming from Bell  $\ensuremath{\mathsf{MTS}}$ 

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	120 of 122
SPOC 11/3/2020	©2020 Avaya Inc. All Rights Reserved.	BM_CMSM81SBC81

//This sigma script is optional for fixing mismatch-codec issue on Avaya one-X Communicator remove(%SDP[1]["s"]["m"][2]);

}

}

#### ©2020 Avaya Inc. All Rights Reserved.

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

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