

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream SIP Trunk with Avaya Aura[®] Communication Manager 10.1, Avaya Aura[®] Session Manager 10.1, Avaya Aura[®] Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 10.1 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Windstream and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 10.1, Avaya Aura[®] Communication Manager 10.1, Avaya Aura[®] Experience Portal 8.1, Avaya Session Border Controller for Enterprise 10.1 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.

Windstream 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.	GEN	VERAL TEST APPROACH AND TEST RESULTS	4
	2.1.	INTEROPERABILITY COMPLIANCE TESTING	5
	2.2.	TEST RESULTS	
	2.3.	SUPPORT	6
3.	REF	ERENCE CONFIGURATION	7
4.	EQU	JIPMENT AND SOFTWARE VALIDATED	8
5.	CON	NFIGURE AVAYA AURA® COMMUNICATION MANAGER	
	5.1.	LICENSING AND CAPACITY	
	5.2.	System Features	
	5.3.	IP NODE NAMES	
	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 Incoming Call Handling Treatment	
	5.11. 5.12.	CONTACT CENTER CONFIGURATION	
		1. Announcements	
		2. ACD Configuration for Call Queued for Handling by Agent	
	5.13.	AVAYA AURA® COMMUNICATION MANAGER STATIONS	
	5.14.	SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES	
6.		VFIGURE AVAYA AURA® SESSION MANAGER	
υ.			
	6.1.	AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION	
	6.2.	SPECIFY SIP DOMAIN	
	6.3.	ADD LOCATION	
	6.4.	ADD SIP ENTITIES	
		Configure Session Manager SIP Entity	
		P. Configure Communication Manager SIP Entity P. Configure Avaya Session Border Controller SIP Entity	
	6.5.	ADD ENTITY LINKS	
	6.6.	CONFIGURE TIME RANGES	
	6.7.	ADD ROUTING POLICIES	
	6.8.	ADD NOUTING FOLICIES	
7.		VFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	
	7.1. 7.2.	LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	
		SERVER INTERWORKING	
		Configure Server Interworking Profile - Avaya Site	
	7.2.2	2. Configure Server Interworking Profile – Windstream SIP Trunk Site CONFIGURE SIGNALING MANIPULATION	
	7.3. 7.4.	CONFIGURE SIGNALING MANIPULATION	
		Configure SERVICES	
		2. Configure SII Server – Avaya Sie 2. Configure SIP Server – Windstream SIP Trunk	
	7.5.	ROUTING	
		. Configure Routing – Avaya Site	

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

7.5	5.2. Configure Routing – Windstream SIP Trunk Site	
7.6.	TOPOLOGY HIDING	71
7.6	5.1. Configure Topology Hiding – Avaya Site	
7.6	5.2. Configure Topology Hiding Profile – Windstream SIP Trunk site	
7.7.		
7.7	7.1. Create Application Rules	
7.7	7.2. Create Media Rules	74
7.7	7.3. Create Endpoint Policy Groups	
7.8.	NETWORK & FLOWS	77
7.8	3.1. Manage Network Settings	77
	3.2. Create Media Interfaces	
7.8	3.3. Create Signaling Interfaces	81
	3.4. Configuration Server Flows	
	7.8.4.1 Create End Point Flows – SMVM Flow	
	7.8.4.2 Create End Point Flows – Windstream SIP Trunk Flow	
8. CC	ONFIGURE AVAYA AURA® EXPERIENCE PORTAL	84
8.1.	BACKGROUND	
8.2.	LOGGING IN AND LICENSING	85
8.3.	VOIP CONNECTION	
8.4.	SPEECH SERVERS	90
8.5.	Application	
8.6.	MPP SERVERS AND VOIP SETTINGS	
8.7.	CONFIGURING RFC2833 EVENT VALUE OFFERED BY EXPERIENCE PORTAL	96
9. W	INDSTREAM SIP TRUNK CONFIGURATION	
10. VI	ERIFICATION STEPS	97
11. CO	DNCLUSION	
12. RF	EFERENCES	
13. AF	PPENDIX A - SIGMA SCRIPT	101
13. AI		

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Windstream and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 10.1, Avaya Aura[®] Communication Manager 10.1, Avaya Aura[®] Experience Portal 8.1, Avaya Session Border Controller for Enterprise (Avaya SBCE) 10.1 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Windstream 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 Windstream SIP Trunk via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager, and the Avaya SBCE with various types of Avaya phones.

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

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

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

For the testing associated with this Application Note, the interface between Avaya systems and the Windstream SIP Trunk Service did not include use of any specific encryption features as requested by Windstream.

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

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved.

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 during the test: Avaya one-X[®] 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 during the test as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using UDP, port 5070 between the Avaya enterprise and Windstream
- 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[®] Messaging and EC500 mobility (extension to cellular)
- SIP re-Invite in off-net call transfer
- Call Center scenarios
- G.711 passthrough fax
- DTMF RFC2833
- Outbound call with FROM Header included the OTG parameter
- Remote Worker (Use Avaya Agent for Desktop) Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote worker is beyond the scope of these Application Notes and are not included in these Application Notes. For these configuration details, see Reference [10]in Section 13
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold)

Items not supported include the following:

- Windstream does not support SIP Refer in off-net call redirection. The off-net call transfer still worked when using SIP Re-Invite instead of SIP REFER
- Windstream does not support TLS/SRTP
- Windstream supports inbound toll-free service in production; however it is not available in their test lab during the compliance testing.

2.2. Test Results

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

• The URI.USER in the CONTACT header of "183 Session Progress" and "200 OK" responded by Windstream contained the invalid number instead of called PSTN number. As designed intent, Session Manager uses the URI.USER in the CONTACT headers to populate in the PAI header and send it to Communication Manager. Then, Communication Manager/H323 phone used the URI.USER in the PAI header for the display purpose. Since Windstream did not fix this issue, Avaya provided a work-around to fix it by using a sigma script on Avaya SBCE to manipulate the URI.USER in the CONTACT header of "183 Session Progress" and "200 OK" coming from Windstream.

2.3. Support

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

For technical support on Windstream SIP Trunking, contact Windstream at website: https://www.windstreamenterprise.com/

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Windstream SIP Trunk. This was the configuration used during the compliance test.

For confidentiality and privacy purposes, actual public IP Addresses used during the test have been masked and replaced with fictitious IP Addresses throughout the document.

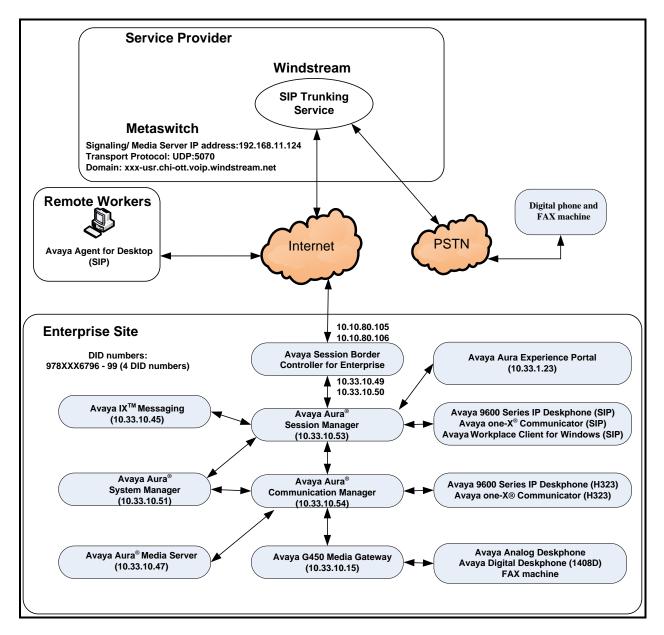


Figure 1: Avaya IP Telephony Network and Windstream SIP Trunk

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	7 of 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components				
Equipment/Software	Release/Version			
Avaya Aura [®] Communication Manager	10.1.0.1.0.974.27372			
running on VMware [®] -based Avaya appliance				
Avaya G450 Media Gateway	FW42.17			
Avaya Aura [®] Session Manager	10.1.0.0.1010019			
running on VMware [®] -based Avaya appliance				
Avaya Aura [®] System Manager	10.1.0.0			
running on VMware [®] -based Avaya appliance	Build No. 10.1.0.0.537353			
	Software Update Rev. No.			
	10.1.0.0.0614119			
Avaya IX Messaging	11.0.0.3204			
Avaya Aura [®] Media Server	8.0.2.218_2022.01.05			
running on VMware [®] -based Avaya appliance				
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872			
running on VMware [®] -based Avaya appliance				
Avaya Aura® Experience Portal running on	8.1.1.0.0121			
VMware®-based Avaya appliance				
Avaya 9621G IP Deskphone (SIP)	Avaya [®] Deskphone SIP 7.1.15.0.021022			
Avaya 9621G IP Deskphone (H.323)	Avaya [®] IP Deskphone			
	6.8.5.3.2			
Avaya 9641 IP Deskphone (H.323)	Avaya [®] IP Deskphone			
	6.8.5.3.2			
Avaya Digital Deskphone (1408D)	R48			
Avaya Workplace Client for Windows (SIP)	3.28.0.73			
Avaya one-X [®] Communicator (H.323 & SIP)	6.2.14.15-SP14P7			
Avaya Agent for Desktop (SIP)	2.0.6.5.3003			
Avaya Analog Deskphone	N/A			
VentaFax	7.10.258.664			
Windstream SIP T	runk Components			
Equipment/Software Release/Version				
Metaswitch	9.5.40			

Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance test. 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[®]- based Avaya Appliance Virtualization Platform, Avaya Aura[®] Communication Manager, Avaya Aura[®] System Manager, Avaya Aura[®] Session Manager, Avaya Aura[®] Experience Portal, Avaya Messaging, Avaya Aura[®] Media

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	8 of 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

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 Windstream 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	2 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.

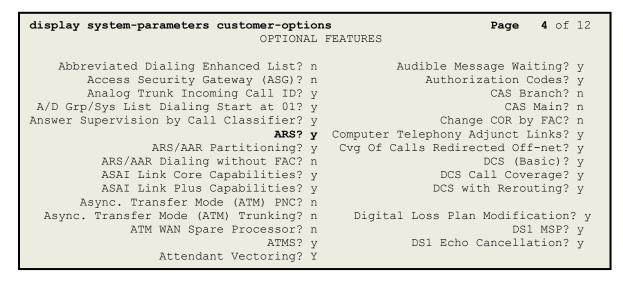


Figure 3: System-Parameters Customer-Options Form – Page 4

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? n
                        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**.

```
2
                                                            Page 1 of
change node-names ip
                               IP NODE NAMES
                  IP Address
Name
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. Windstream supports the **G.711MU**, **G.729A** codecs. The **Media Encryption** was set as **none**, **1-srtp-aescm128-hmac80** in order priority. Default values can be used for all other fields.

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

        IP CODEC SET

        Codec Set: 1
        Audio
        Silence
        Frames
        Packet
        Yes
        Yes
```

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, set the **FAX Mode** to **pass-through**. Note: Windstream supports only fax G.711 pass-through.

change ip-codec-set 1			Page	2 of	2
	IP MEIDA PARA	METERS			
Maximum Call Ra Maximum Call Rate for Pr	te for Direct-I	ect-IP Multimedia? y P Multimedia: 384: Kbits P Multimedia: 384: Kbits			
	Mode	Redundancy	P	acket	Size(ms)
FAX	pass-through	0			
Modem	off	0			
TDD/TTY	US	3			
H.323 Clear-channel	n	0			
SIP 64K Data	n	0			20

Figure 9: IP-Codec-Set Form – Page 2

5.5. IP Network Region for Media Gateway, Media Server

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

Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

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

```
change ip-network-region 1
                                                               Page 1 of 20
                         IP NETWORK REGION
Region: 1 NR Group: 1
Location: 1 Authoritative Domain: bvwdev.com
Name: public
MEDIA PARAMETERS
                              Stub Network Region: n
     PARAMETERS
Codec Set: 1
                              Intra-region IP-IP Direct Audio: yes
                              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048
                                   IP Audio Hairpinning? n
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p 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

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for **Network Region 1**. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (10.33.10.54), 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
                                                               Page
                                                                      1 of
                                                                             2
                               MEDIA GATEWAY 1
                   Type: g450
                   Name: g450
              Serial No: 12TG18000244
   Link Encryption Type: any-ptls/tls
  Mutual Authentication: optional
         Network Region: 1
                                            Location: 1
        Use for IP Sync? y
                                            Site Data:
         Recovery Rule: none
             Registered: y
           Gateway Mode: Enterprise
  FW Version/HW Vintage: 41 .17 .0 /2
       MGP IPV4 Address: 10.33.10.15
       MGP IPV6 Address:
  Controller IP Address: 10.33.10.54
            MAC Address: 3c:3a:73:17:c5:a8
```

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**.

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

Figure 12: Media Gateway – Page 2

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined in **Section 5.3**) and the **Signaling Group: 11** (Defined in **Section 5.7**) have been used. These fields are not configured in this screen, but just display the current information for the Media Server.

```
display media-server 1

MEDIA SERVER

Media Server ID: 1

Signaling Group: 11

Voip Channel License Limit: 80

Dedicated Voip Channel Licenses: 80

Mode Name: AMS

Network Region: 1

Location: 1

Announcement Storage Area: ANNC-44de7b8-ade78-0000c29acfea
```

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

Node Name: procr

Subnet Mask: /24

IPV4 PARAMETERS

IP Address: 10.33.10.54
```

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 Alert Incoming SIP Crisis Calls? 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 Domain: bvwdev.com Bypass If IP Threshold Exceeded? n Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Session Establishment Timer(min): 3 RFC 3389 Comfort Noise? n Direct IP-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 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

- 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
                                                                     1 of
                                                                            2
                                                              Page
                               SIGNALING GROUP
 Group Number: 11
                     Group Type: sip
                       Transport Method: tls
  Peer Detection Enabled? n Peer Server: AMS
  Near-end Node Name: procr
                                           Far-end Node Name: AMS
Near-end Listen Port: 9061
                                         Far-end Listen Port: 5071
                                      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 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

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.

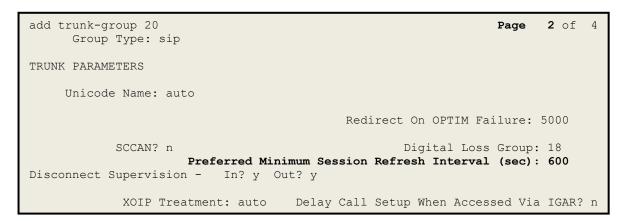


Figure 18: Trunk-Group – Page 2

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.

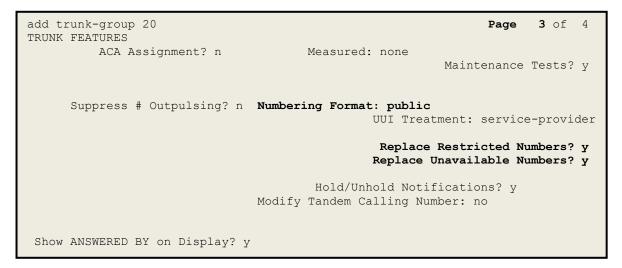


Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **n** so that Communication Manager will not send SIP REFER, Windstream does not support SIP REFER in off-net call redirection (See **Section 2.2** in detail).

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **y**. Note: For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya IX Messaging.

add trunk-group 20 PROTOCOL VARIATIONS	Page 4 of 4
Mark Users as Phone? Prepend '+' to Calling/Alerting/Diverting/Connected Number? Send Transferring Party Information? Network Call Redirection?	n n
Send Diversion Header? Support Request History? Telephone Event Payload Type:	y Y
Convert 180 to 183 for Early Media? Always Use re-INVITE for Display Updates? Resend Display UPDATE Once on Receipt of 481 Response? Identity for Calling Party Display: Block Sending Calling Party Location in INVITE? Accept Redirect to Blank User Destination? Enable Q-SIP?	N n P-Asserted-Identity n n

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 **6** 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.

change public-un		Page 1 of 2 UNKNOWN FORMAT	
			Total
Ext Ext	Trk	CPN	CPN
Len Code	Grp(s)	Prefix	Len
			Total Administered: 1
			Maximum Entries: 240
4 6	20	978XXX	10
			Note: If an entry applies to a SIP
			connection to Avaya Aura(R) Session
			Manager, the resulting number must be
			a complete E.164 number.
			Communication Manager automatically
			inserts a '+' digit in this case.

Figure 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 **48** for extension (**udp**)
- **Dialed String** beginning with **6** for extension (**ext**)**Dialed String** beginning with **9** for feature access code (**fac**)
- **Dialed String** beginning with * for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk Group 20 in **Section 5.8**

change dialplan analysis							Page	1 of	12
			DIAL PLAN ANALYSIS TABLE Location: all			Pe			
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call	
String	Length	Туре	String	Length	Туре	String	Length	Туре	
181	4	ext							
189	4	ext							
3	4	ext							
48	4	udp							
6	4	ext							
800	4	ext							
9	1	fac							
*	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 Co	ode 2:		
Automatic Callback Activation: Deactivatio	on:		
Call Forwarding Activation Busy/DA: All: Deactivation	on:		
Call Forwarding Enhanced Status: Act: Deactivation	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: Deactive	ation:		
Contact Closure Open Code: Close Co	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		ADO DICIM	ANATVOTO			Page	1 of	2
		ARS DIGIT ANALYSIS TABLE Location: all					Percent Fi	ıll: 1	
Dialed	Tot		Route	Call	Node	ANI			
String	Min	Max	Pattern	Type	Num	Reqd			
0	1	11	20	op		n			
1613	11	11	20	pubu		n			
1800	11	11	20	pubu		n			
613	10	10	20	pubu		n			
411	3	3	20	pubu		n			
911	3	3	20	pubu		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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	26 of 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

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: 20 Pattern Name: SP
   SCCAN? n Secure SIP? n Used for SIP stations? n
  Grp FRL NPA Pfx Hop Toll No. Inserted
                                                          DCS/ IXC
      Mrk Lmt List Del Digits
                                                          OSIG
  No
                      Dgts
                                                          Intw
1: 20
       0
                                                           n user
2:
                                                           n user
3:
                                                           n user
4:
                                                          n user
5:
                                                          n user
6:
                                                           n user
  BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub Numbering LAR
                                                Dgts Format
1: yyyyyn n
                                                     pub-unk
                                                             none
2: y y y y y n n
                                                             none
3: ууууул п
                       rest
                                                             none
4: yyyyyn n
                       rest
                                                             none
5: yyyyyn n
                        rest
                                                             none
6: ууууул п
                                                             none
                        rest
```

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	Pa CLASS OF RESTRICTION	age 1 of 23
COR Number: COR Description:		
FRL: Can Be Service Observed? Can Be A Service Observer? Time of Day Chart: Priority Queuing? Restriction Override: Restricted Call List?	Called Party Restriction: Forced Entry of Account Codes? Direct Agent Calling? one Facility Access Trunk Test?	none none n n n
Access to MCT? Group II Category For MFC: Send ANI for MFE? MF ANI Prefix: Hear System Music on Hold?	Fully Restricted Service? Hear VDN of Origin Annc.? Add/Remove Agent Skills?	n n n n n n

Figure 26: Class of Restriction Form

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 **978XXX6799** to **1810** by deleting **10** of the incoming digits for voicemail testing purpose. (1810 is voice mail number)
- The incoming DID number **978XXX6798** to **4800** by deleting **10** of the incoming digits for Experience Portal testing purpose
- The incoming DID number **978XXX** to 4-digit extension by deleting **6** of the incoming digits for inbound call testing purpose.

change inc-call-h	Page	1 of	3			
	INCOM	ING CALL HANDLIN	IG TREATMENT			
Service/	Number	Number	Del Insert			
Feature	Len	Digits				
public-ntwrk	10	978XXX6799	10 1810			
public-ntwrk	10	978XXX6798	10 4800			
public-ntwrk	10	978xxx	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.

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

Figure 29: Hunt Group Configuration – Page 1

HV; Reviewed: SPOC 9/28/2022 Solution & Interoperability Test Lab Application Notes ©2022 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			
Skill? y AAS? n	Expected Call Handling Time (sec) Service Level Target (% in sec):		0	

Figure 30: Hunt Group Configuration – Page 2

VDN 6797, shown below, is associated with vector 3

display vdn 6797		Page 1 of 3
	VECTOR DIRECTORY NUMBER	
	VECTOR DIRECTORI NOMBER	
	EXTENSION: 6797	Unicode Name? n
	Name*: Contact Center	
	DESTINATION: VECTOR NUMBER	3
	Attendant Vectoring? n	
	Meet-me Conferencing? n	
	Allow VDN Override? n	
	COR: 1	
	TN*: 1	
	Measured: none Report	t Adjunct Calls as ACD*? n
	Measured, none Report	t Aujunet Calls as ACD"! I

Figure 31: VDN Configuration

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

display vector 3 Page 1 of 6 CALL VECTOR Number: 3 Name: Contact Center Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y Variables? y 3.0 Enhanced? y 01 wait-time 2 secs hearing ringback 02 announcement 1899 03 queue-to skill 13 pri m 04 wait-time 2 secs hearing silence 05 announcement 1898 06 goto step 3 if unconditionally

Figure 32: Vector 3 Configuration

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

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

Figure 33: Agent-loginID Configuration – Page 1

HV; Reviewed: SPOC 9/28/2022

Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. The following abridged screen shows Page 2 for agent-loginID 3311. Note that the Skill Number (SN) has been set to 13.

```
Display agent-loginID 3311

AGENT LOGINID

Direct Agent Skill:

Call Handling Preference: skill-level

SN RL SL SN RL SL

1: 13 1 16:

2: 17:
```

Figure 34: Agent LoginID Configuration – Page 2

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

2 of

Page 11 of 19

Page

Service Objective? n

Local Call Preference? n

2

5.13. Avaya Aura[®] Communication Manager Stations

In the sample configuration, a 4-digit station extension was used with the format 6796. Use the **add station 6796** command to add an Avaya H.323 IP Deskphone.

- Enter Type: 9621, Name: H323-6796, Security Code: 1234, Coverage Path 1: 1, IP SoftPhone: y (if using this extension as a Softphone such as Avaya one-X[®] Communicator)
- Leave other values as default

add station 6796 Page 1 of 5 STATION Extension: 6796 Lock Messages? n BCC: 0 Security Code: * Coverage Path 1: 1 Coverage Path 2: Type: 9621 TN: 1 COR: 1 COS: 1 Port: S000055 Name: H323-6796 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 Modules. 0 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[®] Communication Manager Configuration Changes

Use the save translation command to save the configuration.

6. Configure Avaya Aura® Session Manager

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

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

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

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

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

← → C Q	https://10.33.10.51/SM	GR/#				Q, Search	h		0	± ≡
AVAYA Users		• Services v	Widgets v Shortcuts v					Search	■ 🔺 ≡	admin
Disk Space Utilization	Avaya Breze * Communication Ma Communication Ser Device Adapter Device Services IP Office	ver 1000 3	Normal Tree		*	Notifications (2) • Too late second sign was on a August 8, 2022 842 MM from 192168.5 • Too laten Merager emergines; Die Peter mode als administered. Voor		Application State Licens Status Deployment Type Multi-Tenany OGBM State Hardening Mode	Active VMware DISABLED DISABLED Standard	×
Alarms Critical Major Major Andeterminate	Media Server Mir Meeting Exchange Messaging	• • •	Information X Shortcuts Exercise Count Sync Status Description Description 1 Image: Status Description				×			
21	Presence Routing Session Manager	> > >	No successful backup taken for System No successful backup taken for System No successful backup taken for System	n Manager in the last 7 days.		System Manager 1 UCM Applications 8 Current Usage : 7/25000				
and a second sec	Web Gateway	10.33.10.51	No successful backup taken for System			USERS 1/50 SIMULTANEOUS ADMINISTRATIVE LOGINS				

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.

System Manager 10.1	Lusers ∨ Felements ∨ Services ∨ Widgets ∨ Shortcuts ∨ Search Ad
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	Step 4: Create "Adaptations"
SIP Entities	Step 5: Create "SIP Entities"
	- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
Entity Links	- 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"
Notiling Policies	- Between Session Managers
Dial Patterns	- 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 "Require Expressions"
	- Assign the appropriate "Routing Policies" to the "Regular Expressions"
	Each "Routing Policy" defines the "Routing Destination" (which is a "STP 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 10.1	Users ∨ ≯Elements ∨ ♦ Services ∨ Widgets ∨ Shortcuts ∨ Search	\blacksquare \blacksquare \parallel admin
Home Routing		
Routing	Domain Management	Help ?
Domains	New Edit Delete Duplicate More Actions -	
Locations	1 Item 🧔	Filter: Enable
Conditions	Name Type Notes	
Adaptations Y	bywdev.com sip	

Figure 39: Domain Management

6.3. Add Location

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

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

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

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

Click Commit to save.

	stem Manager 10.1	Users 🗸 🎤 Elements 🗸 🌣 Services 🗸 Widgets 🗸 Shortcut	5 v	Search 👃 🗮 🛛 admin
Home	Routing			
Routing		Location Details	Commit Cancel	Help ? 🔺
Dom	ains	General		
Locat	tions		Belleville-GSSCP	
Cond	litions	Notes:		
Adap	otations v	Dial Plan Transparency in Survivable Mode		
SIP E	ntities	Enabled:		
Entity	y Links	Listed Directory Number:		
Time	Ranges	Associated CM SIP Entity:		
	ing Policies	Overall Managed Bandwidth		
Dial F	Patterns v	Managed Bandwidth Units:	Kbit/sec •	
		Total Bandwidth:		
Regu	lar Expressions	Multimedia Bandwidth:		
Defau	ults	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 V	
		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 9/28/2022 Solution & Interoperability Test Lab Application Notes ©2022 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 Ite	ms 🧶		
	IP Address Pattern		*
	* 10.33.1.*		
	* 10.33.10.*		
	* 10.33.100.*		
Selec	t: All, None		
		Commit Cancel	

Figure 41: IP Ranges Configuration

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

6.4. Add SIP Entities

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

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

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

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	40 of 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

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 10.1	Users ∨ 🖌 Elements ∨ 🌣 Services ∨ Widgets ∨ Shortcut	s 🗸 🔰 Search 🔰 🌲 🚍 🗍 admin
Home Routing		
Routing	SIP Entity Details	Commit Cancel
Domains	General	
Locations	* Name: * IP Address:	bvwasm2
Conditions	SIP FQDN:	
Adaptations v		Session Manager
SIP Entities	Notes:	
Entity Links	Location:	Belleville-GSSCP V
	Outbound Proxy:	T
Time Ranges		America/Toronto T
Routing Policies	Minimum TLS Version:	Use Global Setting T
Dial Patterns 🗸 🗸	Credential name:	
Regular Expressions	Monitoring SIP Link Monitoring:	Use Session Manager Configuration V
Defaults		Use Session Manager Configuration •

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 bvwdev.com		
Select : All, None			

Figure 43: Session Manager SIP Entity Port

6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **CM10**. 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 10.1	Users 🗸 🎤 Elements 🗸 🏟 Services 🗸 Widgets 🗸 Shortcuts 🗸	
Home Routing ×		
Routing	SIP Entity Details	Commit
Domains	General	
Locations	* Name:	СМ10
Conditions	* FQDN or IP Address:	10.33.10.54
Conditions	Туре:	CM v
Adaptations 🗸 🗸 🗸	Notes:	
SIP Entities	Adaptation:	~
Entity Links	and the second se	Belleville-GSSCP v
Time Ranges	Time Zone: * SIP Timer B/F (in seconds):	America/Toronto
Routing Policies	Minimum TLS Version:	Use Global Setting 🗸
	Credential name:	
Dial Patterns 🛛 🗸 🗸	Securable:	
Regular Expressions	Call Detail Recording:	none v
Defaults	Loop Detection	
	Loop Detection Mode:	On v
	Loop Count Threshold:	5
	Loop Detection Interval (in msec):	200
	Monitoring	
		Use Session Manager Configuration \vee
	CRLF Keep Alive Monitoring:	Use Session Manager Configuration 🗸

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**.

Aura® System Manager 10.1	Users ∨ 🖌 Elements ∨ 🗢 Services ∨ │ Widgets ∨ Shortcut	ts ∽ Search 🔍 🌲 📃 admin
Home Routing		
Routing ^	SIP Entity Details	Commit Cancel
Locations	* Name: * FQDN or IP Address:	
Conditions	Type:	SIP Trunk •
Adaptations 🗸	Notes:	
SIP Entities	Adaptation:	
Entity Links		Belleville-GSSCP *
Time Ranges	* SIP Timer B/F (in seconds):	America/Toronto
	Minimum TLS Version:	
Routing Policies	Credential name:	
Dial Patterns 🗸 🗸	Securable:	
Regular Expressions	Call Detail Recording:	egress •
Defaults	Loop Detection	
10000000	Loop Detection Mode:	On •
	Loop Count Threshold:	5
	Loop Detection Interval (in msec):	200
	Monitoring	
	200	Link Monitoring Enabled
	* Proactive Monitoring Interval (in seconds):	
	* Reactive Monitoring Interval (in seconds):	
	* Number of Tries: * Number of Successes:	
		1 Use Session Manager Configuration *
	CREF Reep Ailve Molitoring.	Die Jession Hanager Comportation -

Figure 45: Avaya SBCE SIP Entity

6.4.4. Configure Avaya Aura® 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 **10.33.1.23**. Note that **Voice Portal** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

Aura® System Manager 10.1	Users 🗸 🎤 Elements 🗸 🏟 Services 🗸 ╞ Widgets 🗸	Shortcuts ~	
Home Routing			
Routing ^	SIP Entity Details		Commit
Domains	General	and the second se	
Locations			Experience Portal
Conditions		* FQDN or IP Address:	
		Type: Notes:	Voice Portal
Adaptations 🗸 🗸		Notes.	
SIP Entities		Adaptation:	•
Entity Links		Location:	Belleville-GSSCP 🗸
-			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		Call Detail Recording:	
Defaults	Loop Detection		
		Loop Detection Mode:	
	Loop Date	Loop Count Threshold: ction Interval (in msec):	
		ction interval (in insec).	200
	Monitoring		
			Use Session Manager Configuration V
			Use Session Manager Configuration V
		5 Call Admission Control: red Bandwidth Manager:	
	Primary Session Manager		· ·
		Bandwidth Association:	
<	Entity Links	Fransport with DNS SRV:	
	Svende Port &	nunsport with Didd SKV.	

Figure 46: Experience Portal SIP Entity

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**.

AVAYA Aura® System Manager 10.1	users v 🎤 Elements v 1	🌣 Services 🗸 Widgets 🗸	Shortcuts v					Search		▲ ≡	admin
Home Routing											
Routing	Entity Links			Con	nmit Cancel						Help ?
Domains	2				_						
Locations	1 Item									Filte	er: 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 bywasm2	TLS V	* 5061	* Q CM10	* 5061		trusted 🔻			
SIP Entities	Select : 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 10.1	Users v 🌾 Elements v 🌣	Services ~ Widgets ~	Shortcuts 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 V	* 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**.

Avra®_System	YA m Manager	≜ U 10.1	sers 🗸 🦻	Elements ~	Services	~ Widgets ~	Shortcuts v						
Home	Routing												
Routing		^	Entity L	inks					Commit Cano	cel			
Domains													
Location	ns		1 Item 🏾 🥭										
Conditio	ons		Name		s	IP Entity 1		Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
Adaptat		~	Select : All,	_EP_TLS_Link None		* Q bywasm2		TLS ¥	* 5061	* Q Experience Portal	* 5061		trusted 💙
SIP Entit	ties												
Entity Li	inks								Commit Cano	el			

Figure 49: Experience Portal Entity Link

6.6. Configure Time Ranges

HV; Reviewed:

SPOC 9/28/2022

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 10.1											
Home Routing											
Routing	Time Ranges										Help 7
Domains	New Edit Delet	te Duplicate	More Actions	•]							
Locations								Filter: Enable			
Conditions	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
Adaptations ×	24/7 Select : All, None	Y	V	Ð	¥	¥	×	Ð	00:00	23:59	
SIP Entities											
Entity Links											
Time Ranges											

Figure 50: Time Ranges

Solution & Interoperability Test Lab Application Notes	
©2022 Avaya Inc. All Rights Reserved.	WS

47 of 103 WS_CMSM10SBC10

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 Windstream to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM10**.

Aura® System Manager 10.	Aura® System Manager 10.1								
Home Routing									
Routing	Routing Policy Details	Commit Cancel							
Domains	General								
Locations		* Name: SP Inbound Calls							
Conditions		Disabled:							
Adaptations 🗸 🗸		Notes:							
SIP Entities	SIP Entity as Destination								
Entity Links	Select								
Time Ranges		N or IP Address							
Routing Policies	CM10 10.	3.10.54							

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 Windstream SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

AV/ Aura® Sys	stem Manage		Jsers ∨ 🖌 Elements ∨ 🌣 Services ∨ │ Widgets ∨	Shortcuts ~
Home	Routing			
Routing		^	Routing Policy Details	Commit
Dom	ains		General	
Locat	tions			* Name: SP Outbound Calls
Cond	litions			Disabled:
Adap	itations	~		* Retries: 0 Notes:
SIP E	ntities		SIP Entity as Destination	
Entity	/ Links		Select	
Time	Ranges		Name FQDN or IF	Address
			SBCE 10.33.10.4	
Routi	ing Policies		Time of Day	

Figure 52: Routing to Windstream SIP Trunk

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

AVAYA Aura®_System Mana	Lusers ∨ → Elements v 💠 Services v Widg ger 10.1	ets v Shortcuts v
Home Routing		
Routing	Routing Policy Details	Commit
Domains	General	
Locations		* Name: To-ExperiencePortal
Conditions		Disabled:
Adaptations	v	Retries: 0 Notes:
SIP Entities	SIP Entity as Destination	
Entity Links	Select	
Time Ranges	Name	FQDN or IP Address
Routing Policies	Experience Portal	10.33.1.23

Figure 53: Routing to Experience Portal

Solution & Interoperability Test Lab Application Notes ©2022 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 Windstream 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.

- **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 in next page, 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**.

Aura® System Manager 10.1									
Home Routing									
Routing ^	Dial Pattern Details	Con	Cancel					Help ?	
	General								
Locations	* Pattern: 1613								
Conditions	* Min: 4								
Adeptations ~		* Max: 11							
Paaptauena		Emergency Call:							
SIP Entities		SIP Domain: byw							
Entity Links		Notes: SP C	outbound Calls						
Time Ranges	Originating Locations and Routing Policie	s							
Time hanges	Add Remove								
Routing Policies	1 Item 🥏							Filter: Enable	
Dial Patterns		Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy N	otes	
,	-ALL-		SP Outbound Calls	0		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 978 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 Windstream.

Aura® System Manager 10.1	Jsers v	Widgets v Shortcuts v				Search	🜲 🗮 admin
Home Routing ×							
Routing ^	Dial Pattern Details	[Commit Cancel				Help ?
Locations	General						
Conditions		* Pattern: 9 * Min: 1 * Max: 1	10				
Adaptations ~		Emergency Call:					
SIP Entities		SIP Domain:					
Entity Links		Notes: V	Windstream Inbound Calls				
Time Ranges	Originating Locations and Routing Polic	ies			 		
Routing Policies	1 Item 🤤						
Dial Patterns	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Destination	Routing Policy I	Notes
Dial Patterns	Belleville-GSSCP Select : All, None		SP Inbound Calls	0	CM10		

Figure 55: Dial Pattern 978

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

Aura® System Manager 10.1	Users × ∮ Elements × • Ø Services × Widgets × Shortcuts ×
Home Routing	
Routing ^	Dial Pattern Details Commit Cancel
Domains	General
Locations	* Pattern: 4800
Conditions	* Min: 4
Adaptations 🗸 🗸	* Max: 4
SIP Entities	SIP Domain: bywdev.com 🗸
Entity Links	Notes: Experience Portal
Time Ranges	Originating Locations and Routing Policies Add Remove
Routing Policies	l Item 🤄
Dial Patterns	Criginating Location Name A Originating Location Notes Routing Policy Name Rank Routing Policy Disabled Routing Policy Destination
Dial Patterns	Image: Constraint of the second se

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.

Vial Patterns	e Duplicate	More Acti	ions 🔹					
19 Items 🛛 🥲								Filter: Enabl
Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes	
0	1	13				bvwdev.com	Windstream Outbound Calls	
1613	4	11				bvwdev.com	Windstream Outbound Calls	
1800	11	11				bvwdev.com	Windstream Outbound Calls	
613	3	10				bvwdev.com	Windstream Outbound Calls	
G 67	4	4				bywdey.com	Windstream SIP Phones	
911	з	3				bywdey.com	Windstream Outbound Calls	
978	10	10				bywdey.com	Windstream Inbound Calls	

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 Windstream.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Windstream 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/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

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

Concentration of the second	ns Incidents Status ✔ Logs ✔ Diag				Settings ♥ Help ♥ Log Out
Session Bora	er Controller for Ente	erprise			ΑνΑγΑ
EMS Dashboard	Dashboard				
Software Management Device Management	Information		Installod Devices		
Backup/Restore	System Time	09:05:15 PM MDT	Refresh	EMS	
System Parameters	Version	10.1.1.0-35-21872		SBCE	
Configuration Profiles	GUI Version	10.1.1.0-21872			
Services	Build Date	Mon Apr 18 07:57:04 UTC 2022			
 Domain Policies TLS Management 	License State	O OK			
 Network & Flows 	Aggregate Licensing Overages	0			
DMZ Services	Peak Licensing Overage Count	0			
Monitoring & Logging	Last Logged in at	08/15/2022 07:42:47 MDT			
	Failed Login Attempts	0			
	Active Alarms (past 24 hours)		Incidents (past 24 hours)		
	None found.			SBCE : Registration Successful, Server is UP	
				SBCE : Registration Successful, Server is UP	

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.

Session Borde	er Controller for Enterprise				AVAYA
EMS Dashboard Software Management Device Management Backup/Restore	Device Management Devices Updates Licensing Key Bundles License C	ompliance			
 System Parameters Configuration Profiles 	Device Name SBCE	Management IP 10.33.10.29	Version 10.1.1.0-35-21872	Status Commissioned Rebost Shutdown R	estart Application View Edit Uninstall
Services					

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.

	Sys	tem Information: SBCE		х
General Configuration	Device	Configuration	License Allocation —	
Appliance Name SBCE	HA Mod	55 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Standard Sessions Requested: 250	520
Box Type SIP Deployment Mode Proxy	Тwo Вур	pass Mode No	Advanced Sessions Requested: 250	520
			Scopia Video Sessions Requested: 250	520
			CES Sessions Requested: 250	520
			Transcoding Sessions Requested: 250	520
			AMR	
			Premium Sessions Requested: 0	0
			CLID	
			Encryption Available: Yes	
Network Configuration				
IP	Public IP	Network Prefix or Subnet Mas	sk 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
10.10.80.106	10.10.80.106	255.255.255.128	10.10.80.1	B1
10.10.80.105	10.10.80.105	255.255.255.128	10.10.80.1	B1
DNS Configuration	Manage	ment IP(s)		
Primary DNS 10.33.100.60	IP #1 (IF	Pv4) 10.33.10.29		
Secondary DNS 8.8.8.8				
DNS Location DMZ				
DNS Client IP 10.33.10.35				

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)

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

Session Borde	er Controller for Ente	rprise		AVAY
MS Dashboard Software Management Device Management Backup/Restore	Interworking Profiles: SMVM Add		Click here to add a description	Rename Clone Delet
System Parameters Configuration Profiles Domain DoS Server Interworking Media Forking Routing Topology Hiding Signaling Manipulation	cs2100 Tarayaru SMVM	General Timers Privacy URI Manipulation Central Hold Support 189 Handling 182 Handling 182 Handling 182 Handling	Header Manipulation Advanced None None None None None	
URI Groups SMMP Traps Time of Day Rules FGDN Groups Reverse Proxy Policy URI Profile Recording Profile H248 Profile Services Domain Policies TLS Management Network & Flows DMZ Services Monitoring & Logging		Ito - Induning Refer Handling URI Group Send Hold Delayed Offer Deversion Header Support Delayed SDP Handling Re-Inste Handling Patck Handling Allow 18/L SDP T.38 Support URI Scheme	Non No No No No No No No No No SP	
		Via Header Format SIPS Required Mediasec	RFC3261 Yes No	

Figure 62: Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – Windstream SIP Trunk Site

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

- Enter **Profile Name**: **SP** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)

The following screen shows that Windstream server interworking profile (named: **SP**) was added.

ession Borde	er Controller for Ente	rprise		AVAy
IS Dashboard ftware Management wice Management	Interworking Profiles: SP			Rename Clone Del
ckup/Restore System Parameters Configuration Profiles	Interworking Profiles	General Timers Privacy URI Manipu	Click here to add a description.	
Domain DoS Server Interworking	avaya-ru SMVM	General Held Support	None	
Media Forking Routing		180 Handling 181 Handling	None	
Topology Hiding Signaling Manipulation URI Groups		182 Handling 183 Handling	None	
SNMP Traps Time of Day Rules		Refer Handling URI Group	No None	
FGDN Groups Reverse Proxy Policy		Send Hold	No	
URN Profile Recording Profile		Delayed Offer 3xx Handling	Yes No	
H248 Profile rvices omain Policies		Diversion Header Support Delayed SDP Handling	No No	
S Management twork & Flows		Re-Invite Handling Prack Handling	No	
MZ Services onitoring & Logging		Allow 18X SDP T.38 Support	No	
		URI Scheme Via Header Format	SIP RFC3261	
		SIPS Required Mediasec	Yes No	
			Edit	

Figure 63: Server Interworking – Windstream SIP Trunk site

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

- Select SP in Interworking Profiles
- On Header Manipulation tab, click Add button to create a new header manipulation
- Select **Header** as **From**
- Select Action as Add Parameter w/ [Value]
- Enter **Parameter** as **otg**
- Enter Value as 200XXX9054-1 (Windstream provided this information)
- Click **Finish** to save the changes

Session Borde	r Controller for Enter	prise	AVAYA
EMS Dashboard Software Management Device Management Backup/Restore	Interworking Profiles: SP Add Interworking Profiles	- Cick have to add a descriptor-	Rename Clone Delete
 System Parameters Configuration Profiles Domain DoS Server Interworking 	cs2100 axaya-tu SMVM SP	General Timers Privacy URI Manipulation Header Manipulation Advanced	Add
Media Forking Routing Topology Hiding Signaling Manyalation URI Groups SMMP Traps Time of Day Rules FGDN Groups Revense Proxy Policy URN Profile Recording Profile		Add Raile X Header Manupulation Header Hadar From Action Add Parameter w/ (Value) Parameter otg Value 200000695-1 Even steen for withand 200000695-1	ESP Delive

Figure 64: Server Interworking – Header Manipulation – Windstream 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**: **SP**. In the script editing window, enter the text exactly as shown in the below screenshot to perform the following:
 - Manipulate SIP headers
 - Remove un-wanted SIP headers
 - Modify URI.USER on Re-INVITE/ UPDATE/ 180 Ringing/183 Session Progress/200 OK coming from Windstream
 - Click **Save** (not shown)

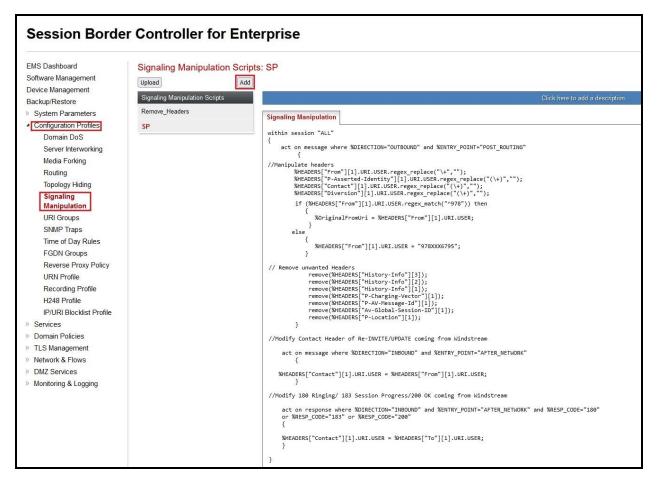


Figure 65: Signaling Manipulation

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	60 of 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

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
- SIP Domain: enter bvwdev.com
- **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)

Session Bord	der Controller for Ente	erprise		Αναγα
EMS Dashboard Software Management Device Management Backup/Restore	SIP Servers: SMVM	General Authentication Heartbest Registration Ping Advanced		[Rename] [Glone] [Delete]
System Parameters	SMVM	Server Type	Call Server	
 Configuration Profiles Services 		SIP Domain	bwwdev.com	
SIP Servers		TLS Client Profile	AvayaSBCClient	
H248 Servers		DNS Query Type	NONE/A	
LDAP		IP Address / FQDN	Port	Transport
RADIUS Domain Policies		10.33.10.53	5061	TLS
 TLS Management Network & Flows 			Edit	

Figure 66: 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)

Enable D	OoS Protection			
Enable G	Grooming			
Interwork	king Profile			SMVM
Signaling	g Manipulation Scrip	t		None
Securabl	le			
Enable F	GDN			
Tolerant				
URI Grou	qu			None
NG911 S	Support			

Figure 67: SIP Server – Advanced - Avaya site

7.4.2. Configure SIP Server – Windstream SIP Trunk

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

The Windstream signaling server IP addresses is 192.168.11.124

Enter **Profile Name: SP**

On General tab, enter the following:

- Server Type: Select Trunk Server
- IP Address/FQDN: 192.168.11.124 (Windstream signaling server IP address)
- Port: 5070
- Transport: UDP
- Click **Finish** (not shown)

Session Bord	er Controller for En	terprise		
EMS Dashboard Software Management Device Management Backup/Restore > System Parameters > Configuration Profiles < Services	SIP Servers: SP Server Profiles SP SMVM	d General Authentication Heartbeat Registration I Server Type DNS Query Type	Ping Advanced Trunk Server NORE/A	
SIP Servers H248 Servers LDAP RADIUS		IP Address / FQDN 192.168.11.124	Port 5070 Edit	Transport UDP

Figure 68: SIP Server – General – Windstream

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

- Check Enable Heartbeat
- Select Method: OPTIONS
- Set Frequency: 60 seconds
- Input **From URI**: **978XXX6795@xxx-usr.chi-ott.voip.windstream.net** (Windstream provides this information)
- Input **To URI**: **978XXX6795**@**xxx-usr.chi-ott.voip.windstream.net** (Windstream provides this information)

neral Authenticatio	n Heartbeat	Registration	Ping	Advanced	
nable Heartbeat					
Method					OPTIONS
Frequency					60 seconds
From URI					978XXX6795@xxx-usr.chi-ott.voip.windstream.ne
To URI					978XXX6795@xxx-usr.chi-ott.voip.windstream.ne
					Edit

Figure 69: SIP Server – Heartbeat – Windstream

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

- Uncheck Enable Grooming option
- Interworking Profile: SP (see Section 7.2.2)
- Signaling Manipulation Script: SP (see Section 7.3)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping	Advanced		
Enable [oS Protection						
Enable C	Grooming						
Interwork	king Profile					SP	
Signaling	g Manipulation Scrip	t				SP	
Securab	le						
Enable F	GDN						
Tolerant							
URI Grou	qu					None	
NG911 5	Support						
							Edit

Figure 70: SIP Server – Advanced – Windstream

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

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

	neral		egistration Ping Advanced
E	nable	Authentication	
		Edit SIP Serve	er Profile - Authentication
	En	able Authentication	
L.		User Name	978XXX6795
		Realm (Leave blank to detect from server challenge)	
		Password (Leave blank to keep existing password)	•••••
		Confirm Password	•••••
			Finish

Figure 71: SIP Server – Authentication – Windstream

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

- Check **Register with All Servers** option
- Input **Refresh Interval**: 60 seconds
- Input **From URI**: **978XXX6795@xxx-usr.chi-ott.voip.windstream.net** (Windstream provides this information)
- Input **To URI**: **978XXX6795**@**xxx-usr.chi-ott.voip.windstream.net** (Windstream provides this information)
- Click **Finish** (not shown)

Register with All Servers	
Register with Priority Server	
Refresh Interval	60 seconds
From URI	978XXX6795@xxx-usr.chi-ott.voip.windstream.ne
To URI	978XXX6795@xxx-usr.chi-ott.voip.windstream.ne

Figure 72: SIP Server – Registration – Windstream

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: SP_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

Session Border	Controller fo	r Ente	rprise				
EMS Dashboard Software Management Device Management	Routing Profiles: SP	_To_SMVI	М				
Backup/Restore	Routing Profiles						Click here to add
System Parameters	default		Routing Profile	Î			
 Configuration Profiles 	To_SMVM_RW						
Domain DoS	default_RW		Update Priority				
Server Interworking	AS TO SMVM		Priority	URI Group	Time of Day	Load Balancing	Next Ho
Media Forking Routing				Routing Pr	ofile		X 3.1
Topology Hiding	URI Group	æ	~		Time of Day	default 🗸	
Signaling Manipulation URI Groups	Load Balancing	Priority	v]		NAPTR		
SNMP Traps	Transport	None v			LDAP Routing		
Time of Day Rules FGDN Groups	LDAP Server Profile	None 🗸			LDAP Base DN (Search)	None 🗸	
Reverse Proxy Policy	Matched Attribute Priority				Alternate Routing		
URN Profile Recording Profile	Next Hop Priority				Next Hop In-Dialog		
H248 Profile	Ignore Route Header						
Services							
Domain Policies	ENUM				ENUM Suffix		_
TLS Management	ENOM	U					
Network & Flows							Add
DMZ Services Monitoring & Logging	Priority LDAP Search	LDAP Search	LDAP Search				
Monitoring & Logging	/ Attribute	Regex Patterr			Profile Next Hop Address	Transport	
	1			SMVM	 10.33.10.53:5061 ((TLS) V None	✓ Delete
		1					
				Back	Finish		

Figure 73: Routing to Session Manager

7.5.2. Configure Routing – Windstream 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_SP 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; SIP Server Profile: SP (see Section 7.4.2); Next Hop Address: 192.168.11.124:5070 (UDP) (Windstream signaling server IP address)
- Click **Finish**

Session Border (Controller for	Enterprise			
Software Management Device Management	Routing Profiles: SMV	M_To_SP			Click here to
System Parameters			Routing Profile	÷	
Configuration Profiles Domain DoS	URI Group	* •	Routing Frome	Time of Day	default v
Server Interworking	Load Balancing	Priority 🗸		NAPTR	
Media Forking Routing	Transport	None V		LDAP Routing	
Topology Hiding Signaling Manipulation	LDAP Server Profile	None 🗸		LDAP Base DN (Search)	None 🗸
URI Groups	Matched Attribute Priority			Alternate Routing	
SNMP Traps	Next Hop Priority			Next Hop In-Dialog	
Time of Day Rules FGDN Groups	Ignore Route Header				
Reverse Proxy Policy					
URN Profile Recording Profile	ENUM			ENUM Suffix	
H248 Profile	-				Add
 Services Domain Policies 	Priority / Weight LDAP Search Attribute	LDAP Search LDAP Search Regex Pattern Regex Result	SIP Server Profile	e Next Hop Address	Transport
 TLS Management Network & Flows 			SP	✓ 192.168.11.124:5070 (U	DP) V None V Delete
 DMZ Services Monitoring & Logging 			Back Finis	h	

Figure 74: Routing to Windstream 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: SP_To_SMVM and click Finish (not shown)
- Select **SP_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)

Stability Stabi	Session Borde	er Controller for E	Enterprise			A	VAY
Topology Hiding Configuration Fridies Topology Hiding Configuration Fridies Configuration Fridies Configuration Fridies Configuration Fridies Configuration Fridies Configuration Fridies Configuration Fridies Provint Value Hadria Contest Registry Configuration Fridies Media Fridies Provint Value Hadria Contest Registry Contest Media Fridies Media Fridies<	oftware Management	Topology Hiding Profiles				Rename Clor	one De
Configuration Profiles cisco ft, profile reproduct vision Domain DoS Server Intervorking Hader Ortenia Replace Action overweite Value Media Forking RefeTio IP/Domain Auto					Click here to add a description		
Dornain DoS Server Harworking Header Criteria Reptace Action Owwardte Value Media Fording Routing Rafe-Ta PDomain Add Topology Hiding Signaling Manipulation URI Groups Topology Hiding Signaling Manipulation PDomain Overnite Value bwder.com Struct Flood PDomain Overnite Overnite bwder.com bwder.com Struct Flood PDomain Overnite Overnite bwder.com Struct Flood PDomain Auto Struct Flood PDomain Auto Vial PDomain Overnite bwder.com Struct Flood PDomain Auto Time of Day Rules PDomain Auto FGDN Groups SDP IPDomain Auto		the second s	Topology Hiding				
Server Intervorking Natio			Header	Criteria	Replace Action	Overwrite Value	
Routing Routing <t< td=""><td>Server Interworking</td><td>SP_To_SMVM</td><td>Refer-To</td><td>IP/Domain</td><td>Auto</td><td></td><td></td></t<>	Server Interworking	SP_To_SMVM	Refer-To	IP/Domain	Auto		
Topology Hiding Prom Profession Overring	Media Forking		To	IP/Domain	Overwrite	bwwdev.com	
Signaling Manipulation Records (rotation Probination Auto			From	IP/Domain	Overwrite	bwwdev.com	
URI Groups Refered By IP/Domain Auto			Record-Route	IP/Domain	Auto		
SMMP Traps Request-Line IP/Demain Overwrite bwder.com Time of Day Rules Via IP/Demain Auto FGDM Groups SOP IP/Demain Auto			Referred-By	IP/Domain	Auto		
FGDN Groups SDP IP/Domain Auto			Request-Line	IP/Domain	Overwrite	bwwdev.com	
Reverse Proxy Policy SUP IP/Demain Auto	Time of Day Rules		Via	IP/Domain	Auto		
Reverse Proxy Policy			SDP	IP/Domain	Auto		
			(Edit		

Figure 75: Topology Hiding To Session Manager

7.6.2. Configure Topology Hiding Profile – Windstream 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_SP and click Finish (not shown)
- Select **SMVM_To_SP** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **xxx-usr.chi-ott.voip.windstream.net** (Windstream provided this information)
- For the Header **From**,
 - In the Criteria column select IP/Domain
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **xxx-usr.chi-ott.voip.windstream.net** (Windstream provided this information)
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the Replace Action column select: Overwrite
 - In the **Overwrite Value** column: **xxx-usr.chi-ott.voip.windstream.net** (Windstream provided this information)
- Click **Finish** (not shown)

Session Borde	er Controller for I	Enterprise			AVAY
MS Dashboard Software Management Device Management	Topology Hiding Profile	s: SMVM_To_SP			Rename Clone Dele
ickup/Restore	Topology Hiding Profiles			Click here to add a description.	
System Parameters	default	Topology Hiding			
Configuration Profiles Domain DoS	cisco_th_profile SP_To_SMVM	Header	Criteria	Replace Action	Overwrite Value
Server Interworking		To	IP/Domain	Overwrite	xxx-usr.chi-ott.voip.windstream.net
Media Forking	SMVM To SP	SDP	IP/Domain	Auto	<u>~</u>
Routing		Via	IP/Domain	Auto	-
Topology Hiding Signaling Manipulation		Refer-To	IP/Domain	Auto	=
URI Groups		Record-Route	IP/Domain	Auto	-
SNMP Traps		From	IP/Domain	Overwrite	xxx-usr chi-ott voip windstream net
Time of Day Rules		Request-Line	IP/Domain	Overwrite	xxx-usr.chi-ott.voip.windstream.net
FGDN Groups		Referred-By	IP/Domain	Auto	_
Reverse Proxy Policy URN Profile				Edit	
Recording Profile					

Figure 76: Topology Hiding To Windstream

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** \rightarrow **Application Rules**

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

Device: SBCE 🗸 Alarms	Incidents Status 🛩 Logs	 ➤ Diagnostics Users 			Settings 🗸	Help 🗸	Log Out
Session Borde	er Controller fo	or Enterprise				AV	aya
EMS Dashboard Device Management	Application Rules:	SIP-Trunk			Renam	ie Clone	Delete
Backup/Restore System Parameters Configuration Profiles 	Application Rules		Click he	ere to add a description.			
 Services Domain Policies 	default-trunk default-subscriber-low	Application Rule	In.	Out Maximum Concurrent Sessior	ns Maximum Se	essions Per En	idpoint
Application Rules Border Rules	default-subscriber-high	Audio Video		2000	2000		
Media Rules Security Rules Signaling Rules	default-server-high	Miscellaneous			_		
Charging Rules End Point Policy	SIP-Trunk RW_AR	CDR Support RTCP Keep-Alive	Off No				
Groups Session Policies				Edit			

Click on **Finish** (not shown)

Figure 77: Application Rule

7.7.2. Create Media Rules

Media rule feature allows one to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. Together, these media-related parameters define a strict profile that is associated with other SIP specific policies. You can also define how Avaya SBCE must handle media packets that adhere to the set parameters.

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

- Select **default-low-med** from **Media Rules** and click **Clone** button:
- Enter Clone Name (e.g., SMVM) and click Finish (not shown)
- Click on **SMVM** from **Media Rules**, then click **Edit** button (not shown):
- For Audio Encryption, select the followings:
 - Preferred Format #1: SRTP_AES_CM_128_HMAC_SHA1_80
 - Preferred Format #2: RTP
- Click **Finish** button to apply the changes.

Session Bord	er Controller for E	interprise					AVAY
MS Dashboard Software Management	Media Rules: SMVM						
Jevice Management		Add		Media Encryption		x	Renome Clone Delet
lackup/Restore	Media Roles		Audio Encryption			Ken.	
System Parameters Configuration Profiles	default-low-med	Encryption Codec	Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA	1_80 ~		
Services	default-high	Audio Encryption	Preferred Format #2	RTP	~		
Iomain Policies	default-high-enc	Preferred Formats	Preferred Format #3	NONE	~	A1_80	
Application Rules Border Rules	avaya-low-med-enc	Encrypted RTCP	Encrypted RTCP				
Media Rules	SM10_MedRule	MK	MKI				
Security Rules Signaling Rules	SMVM	Lifetime	Lifetime	2*			
Charging Rules	SP	Interworking	Leave blank to match any value.				
End Point Policy		Symmetric Context F	Interworking				
Groups Session Policies		Key Change in New O	Symmetric Context Reset				
S Management			Key Change in New Offer				
twork & Flows IZ Services		Video Encryption Preferred Formats	Video Encryption				
initoring & Logging		Interworking	Preferred Format #1	RTP	~		
		Symmetric Context F	Preferred Format #2	NONE	v		
		Key Change in New 0	Preferred Format #3	NONE	~		
		Key Change in New C	Encrypted RTCP				
		Macellaneous	мка				
		Capability Negotiation	Lifetime Leave blank to match any value.	2ª			
			Leave blank to match any value.				
			Symmetric Context Reset				
			Key Change in New Offer				
			Miscellaneous				
			Capability Negotiation				
				Finish			

Figure 78: Media Rule 1

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

- Select **default-low-med** from **Media Rules** and click **Clone** button:
- Enter Clone Name (e.g., SP) and click Finish (not shown)

EMS Dashboard	Media Rules: SP			
Software Management		Add		Rename Clone Dele
Device Management	Media Rules		Click here to add a description.	Committee Commit
ackup/Restore	default-low-med		circk mere to add a description.	
System Parameters		Encryption Codec Prioritization Advanced QoS		
Configuration Profiles Services	default-low-med-enc	Audio Encryption		
Domain Policies	default-high	Preferred Formats	RTP	
Application Rules	default-high-enc	1000 1000		
Border Rules	avaya-low-med-enc	Interworking		
Media Rules	SMVM	Symmetric Context Reset		
Security Rules		Key Change in New Offer	0	
Signaling Rules	SP			
Charging Rules		Video Encryption		
End Point Policy		Preferred Formats	RTP	
Groups Session Policies		Interworking		
TLS Management		Symmetric Context Reset		
Network & Flows				
Network Management		Key Change in New Offer		
Media Interface		Miscellaneous		
Signaling Interface		Capability Negotiation		
End Point Flows		Capability regonation		
Session Flows			Edit	
Advanced Options				

Figure 79: Media Rule 2

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: SMVM
 - Application Rule: SIP-Trunk (See in Section 7.7.1)
 - Border Rule: default
 - Media Rule: SMVM (See in Section 7.7.2)
 - Security Rule: default-low
 - Signaling Rule: default
- Select **Finish** (not shown)

Session Bord	er Controller for Ent	terprise								avaya
EMS Dashboard Software Management Device Management	Policy Groups: SMVM	0							Rename	Clone Delete
Backup/Restore	Policy Groups					Glick here to add a descript	ion.			
System Parameters	default-low					Hover over a row to see its desi	inption.			
Configuration Profiles	default-low-enc		1							
Services	default-med	Policy Group								
Domain Policies Application Rules	default-med-enc									Summary
Border Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Media Rules	default-high-enc	1	SIP-Trunk	default	SMVM	default-low	default	None	Off	Edit
Security Rules	avaya-def-low-enc									
Signaling Rules Charging Rules	avaya-def-high-subscriber									
End Point Policy	avaya-def-high-server									
Groups Session Policies	SMVM									

Figure 80: Endpoint Policy 1

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

- Select Add.
- Enter Group Name: SP
 - Application Rule: SIP-Trunk (See in Section 7.7.1)
 - Border Rule: default
 - Media Rule: SP (See in Section 7.7.2)
 - Security Rule: default-low
 - Signaling Rule: default
- Select **Finish** (not shown)

EMS Dashboard	Policy Groups: SP									
Software Management		Add							Rename	Clone Delete
Device Management Backup/Restore	Policy Groups					Click here to add a descripti	оп			
System Parameters	default-low					Hover over a row to see its desc	rotion			
Configuration Profiles	default-low-enc	N.	1							
Services	default-med	Policy Group								
Domain Policies Application Rules	default-med-enc									Summary
Border Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Media Rules	default-high-enc	1	SIP-Trunk	default	SP	default-low	default	None	Off	Edit
Security Rules	avaya-def-low-enc									
Signaling Rules Charging Rules	avaya-def-high-subscriber									
End Point Policy	avaya-def-high-server									
Groups Session Policies	SMVM									
TLS Management	SP									

Figure 81: Endpoint Policy 2

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 V Alarms I							
Session Borde	r Controller for Enterpri	se				AVA	AYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Network Management						Add
Services Domain Policies	Name Gateway	Subn	et Mask / Prefix Length	Interface	IP Address		
 Domain Policies TLS Management 	Network_B1		Add Network		x	Edit D	elete
Network & Flows	Network_A1	Name	Network_A1			Edit D	elete
Network Management		Default Gateway	10.33.10.1				
Media Interface		Network Prefix or Subnet Mask	255.255.255.0				
Signaling Interface End Point Flows		Interface	A1 🗸				
Session Flows Advanced Options					Add		
 DMZ Services 		IP Address	Public IP	Gateway Override			
Monitoring & Logging		10.33.10.49	Use IP Address	Use Default	Delete		
			Finish				

Figure 82: 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	incidents Status 🕶 Logs 🕶 Diagnostics User					Settings 🗸	Help 🖌 🛛 Log Out
Session Borde	r Controller for Enterprise	•					AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Network Management						Add
Services Domain Policies	Name Gateway	Subnet Ma	sk / Prefix Length Interface	e	IP Address		
 TLS Management 	Network_B1		Add Network		X		Edit Delete
Network & Flows Network	Network_A1	Name	Network_B1				Edit Delete
Management		Default Gateway	10.10.80.1				
Media Interface		Network Prefix or Subnet Mask	255.255.255.128				
Signaling Interface End Point Flows		Interface	B1 ~				
Session Flows Advanced Options					Add		
 DMZ Services 		IP Address	Public IP	Gateway Override			
Monitoring & Logging		10.10.80.106 ×	Use IP Address	Use Default	Delete		
			Finish				

Figure 83: 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

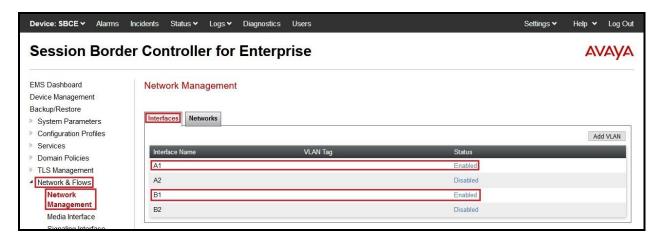


Figure 84: Network Management – Interface Status

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 Windstream)
 - 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	s Users	Sett	tings 🗸 Help 🖌 Lo	Log Out
Session Bord	ler Controller for Enterp	prise		AVA	ŊА
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Media Interface Media Interface				Add
 Services Domain Policies 	Name	Media IP Network	Port Range		
 TLS Management Network & Flows 	OutsideMedia	10.10.80.105 Network_B1 (51.VLAN 0) 10.33.10.49	35000 - 40000	Edit Dek	
Network Management Media Interface	InsideMedia	10.33.10.49 Network A1 (A1, VLAN 0)	35000 - 40000	Edit Dele	lete

Figure 85: 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 Windstream)
 - UDP Port: 5070
 - 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 5070 the same as Windstream used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

d gement	Signaling Interface						
ment e meters	Signaling Interface						
Profiles	Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
ies ment	InsideTLS	10.33.10.49 Network_A1 (A1, VLAN 0)	_	-	5061	AvayaSBCServer	Ed
ws	OutsideUDP	10.10.80.106 Network B1 (B1, VLAN 0)	-	5070	-	None	Edi

Figure 86: 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: SMVM (see Section 7.7.3)
 - Routing Profile: SMVM_To_SP (see Section 7.5.2)
 - Topology Hiding Profile: SP_To_SMVM (see Section 7.6.1)
 - Leave other parameters as default
 - Click Finish

End Point Flows					
Subscriber Flows Server Flow	3				
	Add Flow	X			_
Flow Name	SMVM Flow				
SIP Server Profile	SMVM 🗸	Cick here to add a row dea	onstan).		
URI Group	× •				
Transport	* *	Signaling Interface	End Point Policy Group	Routing Profile	
Remote Subnet	•	InsideTLS	EndPoint-Policy	To_SP_Telia	View Clone Edi
Received Interface	OutsideUDP V	InsideSIGRW	IPO_RW	default_RW	
Signaling Interface	InsideTLS v				
Media Interface	InsideMedia v				
Secondary Media Interface	None 🗸	Signaling Interface	End Point Policy Group	Routing Profile	
End Point Policy Group	SMVM	InsideTLS	SMVM	SMVM_To_SP	View Clone Ed
Routing Profile	SMVM_To_SP V	InsideSIGRW	SMVM_RW	default_RW	
Topology Hiding Profile	SP_To_SMVM ¥	InsideTLS	SMVM_Telia	SMVM_To_SPti	View Clone Edi
Signaling Manipulation Script	None v			ALC: VI AND ALL -	
Remote Branch Office	Any v	Signaling Interface OutsideUDP	End Point Policy Group	Routing Profile SP_To_SMVM	View Clone Ed
Link Monitoring from Peer					
FQDN Support		Signaling Interface	End Point Policy Group	Routing Profile	
FQDN		OutsideTLS	SP Tela	To_IPO	View Clone Edi

Figure 87: End Point Flow 1

7.8.4.2 Create End Point Flows – Windstream 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 Windstream signaling server.

- Select the Server Flows tab
- Select Add, enter Flow Name: SP Flow
 - Server Configuration: SP (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: SP (see Section 7.7.3)
 - Routing Profile: SP_To_SMVM (see Section 7.5.1)
 - Topology Hiding Profile: SMVM_To_SP (see Section 7.6.2)
 - Leave other parameters as default
 - Click Finish

ashboard	End Point Flows					
re Management						
Management /Restore	Subscriber Flows Server Flow					
em Parameters			-			
iguration Profiles		Add Flow	x			
ices ain Policies	Flow Name	SP Flow	Click here to add a row des	uriction		
Management	SIP Server Profile	SP v				
ork & Flows etwork Management	URI Group	* v				
edia Interface	Transport	• v	Signaling Interface	End Point Policy Group	Routing Profile	
ignaling Interface	Remote Subnet	•	InsideTLS	EndPoint-Policy	To_SP_Telia	View Clone Edit D
nd Point Flows	Received Interface	InsideTLS	InsideSIGRW	IPO_RW	default_RW	
dvanced Options	Signaling Interface	OutsideUDP V				
Services toring & Logging						
toriniti or coddiniti	Media Interface	OutsideMedia V	Signaling Interface	End Point Policy Group	Routing Profile	
	Secondary Media Interface	None	InsideTLS	SMVM	SMVM_To_SP	View Clone Edit D
	End Point Policy Group	SP 👻	InsideSIGRW	SMVM_RW	default_RW	
	Routing Profile	SP_To_SMVM V	InsideTLS	SMVM_Telia	SMVM_To_SPtI	View Clone Edit D
	Topology Hiding Profile	SMVM_To_SP V				
	Signaling Manipulation Script	None 🗸	Signaling Interface	End Point Policy Group	Routing Profile	
	Remote Branch Office	Any 🗸	OutsideUDP	SP	SP_To_SMVM	View Clone Edit D
	Link Monitoring from Peer					
	FQDN Support	0	Signaling Interface	End Point Policy Group	Routing Profile	
	FQDN		OutsideTLS	SP_Telia	To_IPO	View Clone Edit D

Figure 88: End Point Flow 2

8. Configure Avaya Aura[®] Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult in the **References [5]- Section 12** 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 call¹.

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

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

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.

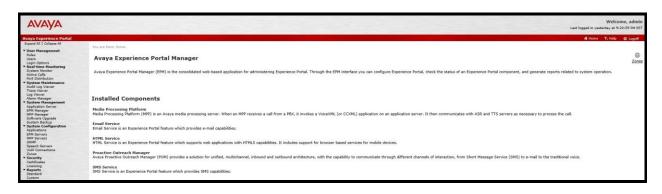


Figure 89: Experience Portal – Home page

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.

waya Experience Portal Expand All Collapse All			
Expand All Collapse All 'User Management Roles Users Login Options Real-time Monitoring	You are here: <u>Home</u> > Security > Li	censing	
System Monitor Active Calls	This page displays the Experien	ce Portal license information that is currently in effect. Experier	nce Portal use
Port Distribution	License Server Information	▼	
System Maintenance Audit Log Viewer Trace Viewer Log Viewer Alarm Manager System Management Application Server	License Server URL: Last Updated: Last Successful Poll:	https://10.33.1.10:52233/WebLM/LicenseServer Jan 28, 2021 4:33:55 AM EST Jan 21, 2022 12:38:33 PM EST	I
EPM Manager	Licensed Products 👻		
MPP Manager Software Upgrade System Backup	Experience Portal Announcement Ports:	50	Ø
System Configuration Applications EPM Servers SNMP Speech Servers VoIP Connections Zones Security Certificates	ASR Connections: Call Anchoring Ports: Email Units: Enable Media Encryption: Enhanced Call Classification: Google ASR Connections: Google Dialogflow Connections HTML Units:	250 250 10 250 250 250 250 250 250 250	
Licensing Reports Standard Custom Scheduled Multi-Media Configuration Email HTML	SIP Signaling Connections: SMS Units: Telephony Ports: TTS Connections: Video Server Connections: Zones: Version:	50 10 50 250 250 10 8	
SMS POM POM Home POM Monitor	Last Successful Poll: Last Changed:	Jan 21, 2022 12:38:33 PM EST Apr 11, 2021 11:03:26 PM EDT	
	Proactive Outreach Manage EMAIL Channels: External Selection: Manual Agents: Maximum Outbound Ports: Predictive Agents: Preview Agents: SMS Channels: Agent Web API Service:	r 0 0 0 0 0 0 0 0 0 0 0	I
	Version: Expiration Date: Last Successful Poll: Last Changed:	3 Aug 3, 2021 12:00:00 AM EDT Jan 21, 2022 12:38:33 PM EST Sep 2, 2021 12:02:42 AM EDT	

Figure 90: Experience Portal – License

8.3. VoIP 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.

Expand All Collapse All	You are here: Home > System Configuration > VoIP Connections
▼ User Management	
Roles	
Users	VoIP Connections
Login Options	
 Real-time Monitoring 	
System Monitor Active Calls	This page displays a list of Voice over Internet Protocol (VoIP) servers that Experience Portal communicates with. You can configure multiple SIP connections, but only one SIP connection
Port Distribution	
System Maintenance	
Audit Log Viewer	The information that you entered has been saved.
Trace Viewer	
Log Viewer	
Alarm Manager	H.323 SIP
 System Management 	
Application Server	🔳 Zone 📩 Name 📩 Enable 🍐 Proxy Transport 🍐 Proxy/DNS Server Address 🖒 Proxy Server Port 🕹 Listener Port 🖕 SIP Domain 🖕 Maximum Simultaneous Calls 🖕
EPM Manager	■ Zone _ Iname _ Iname _ Proxy transport _ Proxy Jukes Server Address _ Proxy Server Port _ Estener Port _ Str Domain _ Maximum Simultaneous Cans _
MPP Manager Software Upgrade	Default interopSM Yes TLS 10.33.10.53 5061 5061 bvwdev.com 10
System Backup	
System Configuration	Add Delete Help
Applications	Aug Delete help
EPM Servers	
MPP Servers	
SNMP	
Speech Servers	
VoIP Connections	
* Security	
Certificates	

Figure 91: Experience Portal – VoIP Connection 1

Step 2 - Configure a SIP connection as follows:

- Name Set to a descriptive name (e.g., interopSM)
- 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 10 was used.
- Select All Calls can be either inbound or outbound
- SRTP Enable = Yes
- Encryption Algorithm = AES_CM_128
- Authentication Algorithm = HMAC_SHA1_80
- **RTCP Encryption Enabled = No**
- **RTP** Authentication Enabled = Yes

- Click on Add to add SRTP settings to the Configured SRTP List
- Use default values for all other fields
- Click **Save** (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 V Name: interopSM
Enable: O Yes No
Proxy Transport: TLS V
Proxy Servers O DNS SRV Domain
Address Port Priority Weight
10.33.10.53 5061 0 0 Remove
Additional Proxy Server
Listener Port: 5061 SIP Domain: bvwdev.com
P-Asserted-Identity:
P-Asserted-Identity: Maximum Redirection Attempts: 0
Consultative Transfer: INVITE with REPLACES REFER
SIP Reject Response Code: ASM (503) SES (480) Custom 503
SIP Timers
T1: 250 milliseconds
T2: 2000 milliseconds B and F: 4000 milliseconds
Call Capacity
Maximum Simultaneous Calls: 10
All Calls can be either inbound or outbound
O Configure number of inbound and outbound calls allowed
SRTP
Enable: Yes O No
Encryption Algorithm: AES_CM_128 NONE
Authentication Algorithm: HMAC_SHA1_80 HMAC_SHA1_32
RTCP Encryption Enabled: O Yes O No
RTP Authentication Enabled: Yes No
Configured SRTP List
SRTP-Yes,AES_CM_128,HMAC_SHA1_80,RTCP Encryption-No,RTP Authentication-Yes
Remove
Save Apply Cancel Help

Figure 92: Experience Portal – VoIP Connection 2

HV; Reviewed: SPOC 9/28/2022

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:

Expand All Collapse All	You are here: Home > System Configuration > Speech Servers
▼ User Management	
Roles Users	Speech Servers
Login Options	Speech Servers
▼ Real-time Monitoring	
System Monitor	This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.
Active Calls Port Distribution	
▼ System Maintenance	
Audit Log Viewer	ASR ITS
Trace Viewer	AJR 113
Log Viewer Alarm Manager	🔳 📴 👝 🗛 🚛 🖕 👘 🚛 🖕 🚛 🗛 🗛 🖕 🕹 🗛 🗛 🖕 🖕
▼ System Management	■ Zone ĴName Ĵ Enable Ĵ Network Address ĴEngine Type Ĵ MRCP Ĵ Base Port Ĵ Total Number of ĴLanguages Ĵ
Application Server	Default Nuance-ARS Yes 10.33.1.61 Nuance MRCP V2 TCP 5060 2 English(USA) en-US
EPM Manager MPP Manager	Detail Mance Aks Tes 10.51.101 Mance Microz Ter 5000 2 English (554) en-05
Software Upgrade	Add Delete
System Backup	
 System Configuration Applications 	Customize Help
EPM Servers	
MPP Servers	
SNMP	
Speech Servers VoIP Connections	
Zones	

Figure 93: Experience Portal – ASR Speech Server

TTS speech server:

Expand All Collapse All You are here: Home > System Configuration > Speech Servers V User Management Roles Speech Servers Users Speech Servers Space Monitor Active Calls This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with. Port Distribution System Maintenance
V User Management Roles Users Users Users Users Speech Servers This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with. Port Distribution System Maintenance
Users Speech Servers Login Options Seal-time Monitoring System Monitor Active Calls Port Distribution System Maintenance System Maintenance System Maintenance
Login Options ▼ Real-time Monitoring System Monitor Active Calls ▼ System Maintenance ▼ System Maintenance
Keal-time Monitoring System Monitor Active Calls Port Distribution System Maintenance
System Monitor This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with. Port Distribution System Maintenance
Active Calls Inits page displays the list of Automated Speech Recognition (KSR) and Text-to-Speech (TTS) servers due Experience Fortal communicates with. System Maintenance
Active Calls Port Distribution
▼ System Maintenance
A distance of the second s
Audit Log Viewer ASR TTS
Trace Viewer
Log Viewer
Alarm Manager Zone Name Enable Network Address Engine Type MRCP Base Port Total Number of Voices Voices Voices Voices Name _
v system Management
Application Server English(USA) en-US Alli
EPM Manager
Derault Nuance-TTS Tes 10.33.1.61 Nuance MRCP V2 TCP 5060 2
Solitinate opgrade
System Configuration Add Delete
Apprications Voor Dece
MPD Servers Customize Help
mmy servers
Speech Servers
VoIP Connections
Zones
- Security

Figure 94: 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 10.33.1.23.

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

You are here: <u>Home</u> > 9	System Confi	iguration > <u>Applications</u> :	> Change Ap	oplication	
Change Application					
Use this page to change the configuration of an application.					
Zone:					
Name:	Test-VXML				
inable: • Yes No					
Reserved SIP Calls:	Type: VoiceXML Reserved SIP Calls: None Minimum Maximum				
Requested:	 None 		kimum		
URI					
🖲 Single 🔵 Fail C	over 🔍 Lo	ad Balance			
VoiceXML URL:	https://	/10.33.1.23/mpp/misc/	'avptestapp	/intro.vxml	
Mutual Certificate Aut	thentication	1: 🖲 Yes 🔘 No			
Basic Authentication:		🔘 Yes 🖲 No			
ASR Speech Server	s 🔻				
Engine Typ	pes			Selected Er	ngine Types
<none></none>				Nuance	
Nuance					~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Languages			Selected	l Languages	
<none></none>				(USA) en-U	- -
Resources:		Acquire on call sta	rt and reta	ain 🔻	
N Best List Length:					
Speech Complete Tir	meout:	0 millisec	onds		
Speech Incomplete 1	fimeout:	millisec	onds		
Vendor Parameters:			11		
TTS Speech Servers	s 🔻				
	Voices				Selected Voices
TTS: Nuance V	English(USA) en-US Ava F USA) en-US Nathan M USA) en-US Zoe F	4		English(USA) en-US Allison F
Application Launch	-				
 Inbound Int 					
 Number Nu 					
Called Number:		Add	ĺ.		
4800				*	Remove
Speech Parameters	5 🕨				
Reporting Paramet	ers 🕨				
Advanced Paramete	ers 🕨				
Save Apply	Cancel	Help			

Figure 95: Experience Portal – Application

HV; Reviewed: SPOC 9/28/2022 Solution & Interoperability Test Lab Application Notes ©2022 Avaya Inc. All Rights Reserved. 92 of 103 WS_CMSM10SBC10

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.

Expand All Collapse All	Vau are been Users > Sucker Configuration > URD Server
▼ User Management Roles	You are here: <u>Home</u> > System Configuration > MPP Servers.
Users	MPP Servers
Login Options ▼ Real-time Monitoring	
System Monitor Active Calls Port Distribution	This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, it invokes
✓ System Maintenance Audit Log Viewer Trace Viewer Log Viewer	■ Zone ↓ Name ↓ Host Address ↓ Network Address ↓ Address ↓ Address ↓ Address ↓ Address ↓ Address ↓ Simultaneous Calls ↓ Trace Level ↓
Alarm Manager System Management	Default mpp80 ep80.bvwdev.com <default> <default> <default> 10 Use MPP Settings</default></default></default>
Application Server EPM Manager MPP Manager	Add Delete
Software Upgrade System Backup	MPP Settings Browser Settings Video Settings VoIP Settings Help
 System Configuration Applications 	
EPM Servers MPP Servers SNMP	
Speech Servers	

Figure 96: Experience Portal – MPP Server 1

- Step 2 Enter any descriptive name in the Name field (e.g., mpp80) 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**.

Expand All Collapse All	You are here: Home > Surtem Ma	intenance > System Monitor > mpp80 Details > Change MPP Server		
▼ User Management	iou are nere: nome - system Ma	Artenance < avstein monitor < Inppor Details < Change MPP Server		
Roles	Change MDD Carry			
Users	Change MPP Server			
Login Options				
▼ Real-time Monitoring	11 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
System Monitor	Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels			
Active Calls	to Finest only when you are the	oubleshooting the system.		
Port Distribution				
▼ System Maintenance	7	Default		
Audit Log Viewer	Zone:			
Trace Viewer	Name:	mpp80		
Log Viewer	Host Address:	ep80.bvwdev.com		
Alarm Manager	Host Address.	cpoolstwacticom		
▼ System Management	Network Address (VoIP):	<default></default>		
Application Server				
EPM Manager	Network Address (MRCP):	<default></default>		
MPP Manager	and the second sec			
Software Upgrade	Network Address (AppSvr):	<default></default>		
System Backup				
 System Configuration 	Maximum Simultaneous Calls:	10		
Applications	12 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
EPM Servers	Restart Automatically:	● Yes ○ No		
MPP Servers				
SNMP	MPP Certificate			
Speech Servers	MPP Certificate			
VoIP Connections				
Zones				
▼ Security		on, O=AVAYA, OU=SIL, CN=ep80.bvwdev.com		
Certificates	Issuer: O=AVAYA,OU=MGMT,CN=SystemManager CA			
Licensing	Serial Number: 52301cea350940e3			
▼ Reports Standard	Signature Algorithm: SHA256withRSA			
Custom	Version: 3			
Scheduled	Valid from: March 1, 2021 11:54:52 AM EST until March 1, 2023 11:54:52 AM EST			
 Multi-Media Configuration 	Certificate Fingerprints			
Email	MD5: b2:56:8c:12:72:64:14:56:21:9b:2c:6b:49:54:83:7c			
HTML	SHA: e9:28:ef:c9:f8:27:e2:97:8b:46:4c:7b:98:f8:5d:8e:90:45:0e:a8			
SMS	SHA-256: 4c:a5:bf:62:90:4d:db:03:1b:27:31:7f:ce:b8:f9:b3:6b:34:af:81:91:3f:a7:2f:53:eb:83:e8:3e:e9:65:26			
▼ POM	Key Usage: Digital Signature			
POM Home	Non Repudiation			
POM Monitor	Key Encipherment			
	Data Encipherment			
	Key Agreement			
	Extended Key Usages:			
	Client Auth			
	Server Auth			
	Basic Constraints:			
	CA: false			
	Path Len Constrain	t: undefined		
	Subject Alternative Names			
	DNS Name: ep80			
	DNS Name: ep80.bvw	dev.com		
	IP Address: 10.33.			
	Categories and Trace Levels			
	Save Apply Canc	el Help		

Figure 97: 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

Step 5 - Click on Save (not shown)

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	94 of 103
SPOC 9/28/2022	©2022 Avaya Inc. All Rights Reserved.	WS_CMSM10SBC10

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		
Station:		
RTCP Monitor Settings Host Address:		
Port:		
VoIP Audio Formats 🔻		
MPP Native Format: audio/basic 🔻		
Codecs 🔻		
Offer		
EnableCodecOrderImage: Second seco		
Packet Time: 20 V milliseconds		
G729 Discontinuous Transmission: O Yes No		
Answer		
EnableCodecOrderImage: CodecOrderImage: CodecImage: Codec		
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 98: Experience Portal – MPP Server - VoIP

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. cparameter name="mpp.sip.rfc2833.payload">101</parameter>
- In the verification of these Application Notes, the line was added directly above the line where the sip.session.expires parameter is configured.

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

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

Expand All Collapse All	You are here; Home > System Management > MPP Manager			
 User Management 				
Roles				
Users	MPP Manager (Jan 21, 2022 1:31:59 PM EST)			
Login Options Real-time Monitoring				
System Monitor				
Active Calls	This page displays the current state of each MPP in the Experience Portal system. To enable the state and			
Port Distribution				
▼ System Maintenance				
Audit Log Viewer	Last Poll: Jan 21, 2022 1:31:39 PM EST			
Trace Viewer	Restart Schedule Active Calls			
Log Viewer Alarm Manager	Zone Server Name Mode State Config Auto Restart Today Recurring In Out			
▼ System Management				
Application Server	Default mpp80 Online Running OK Yes No None 0 0			
EPM Manager				
MPP Manager	State Commands			
Software Upgrade				
System Backup				
 System Configuration Applications 	Start Stop Restart Reboot Halt Cancel Restart/Reboot Options			
EPM Servers				
MPP Servers	One server at a time			
SNMP	Mode Commands			
Speech Servers	All servers			
VoIP Connections	Offline Test Online			
Zones • Security	onine resc onine			
* Security				

Figure 99: Experience Portal – MPP Manager

HV; Reviewed: SPOC 9/28/2022

9. Windstream SIP Trunk Configuration

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

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[®] Communication Manager 10.1, Avaya Aura[®] System Manager 10.1, Avaya Aura[®] Session Manager 10.1, Avaya Aura[®] Experience Portal 8.1 and Avaya Session Border Controller for Enterprise 10.1 to Windstream. 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[®] Communication Manager

[1] Administering Avaya Aura® Communication Manager, Release 10.1, Issue 1, December 2021

Avaya Aura[®] Session Manager/System Manager

- [2] Administering Avaya Aura® Session Manager, Release 10.1.x, Issue 3, April 2022
- [3] Administering Avaya Aura® System Manager for Release 10.1.x, Issue 5, April 2022

Avaya Session Border Controller for Enterprise

[4] Administering Avaya Session Border Controller for Enterprise, Release 10.1, Issue 1, December 2021

Avaya Aura Experience Portal

[5] Administering Avaya Aura® Experience Portal, Release 8.1, Issue 1, July 2021

Avaya Phones

- [6] Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones H.323, Release 6.8.2, Issue 1, June 2019
- [7] Installing and Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP Release 7.1.7, Issue 1, October 2019
- [8] Avaya one-X® Communicator Release 6.2 SP14 Release Notes, Issue 1.0, June 2019
- [9] Avaya Workplace Client (Windows) Release 3.23.1 Release Notes, Issue 1.0, December 2021

Remote Worker

 [10] Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel.
 7.0, Avaya Aura® Communication Manager Rel.
 7.0 and Avaya Aura® Session Managers Rel.
 7.0 - Issue 1.0

Avaya Media Server

[11] Deploying and Updating Avaya Aura® Media Server Appliance, Release 10.1.x, Issue 1, April 2022

IETF (Internet Engineering Task Force) SIP Standard Specifications

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

Product documentation for Windstream SIP Trunking may be found at: https://www.windstreamenterprise.com/

13. Appendix - 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("(\+)","");
//Manipulate From headers for Experience Portal
    if (%HEADERS["From"][1].URI.USER.regex match("^978")) then
       %OriginalFromUri = %HEADERS["From"][1].URI.USER;
      }
   else
       %HEADERS["From"][1].URI.USER = "978XXX6795";
      }
// 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 Contact Header of Re-INVITE/UPDATE coming from Windstream

```
act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" {
```

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

```
//Modify 180 Ringing/ 183 Session Progress/200 OK coming from Windstream
```

```
act on response where %DIRECTION="INBOUND" and
%ENTRY_POINT="AFTER_NETWORK" and %RESP_CODE="180"
or %RESP_CODE="183" or %RESP_CODE="200"
{
%HEADERS["Contact"][1].URI.USER = %HEADERS["To"][1].URI.USER;
}
```

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM 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