



# **Application Notes for Configuring Cox Communications SIP Trunk with Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller 10.1 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Cox Communications 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 Experience Portal 8.1, Avaya Session Border Controller 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.

Cox Communications 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

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>4</b>
<b>2.</b>	<b>GENERAL TEST APPROACH AND TEST RESULTS .....</b>	<b>4</b>
2.1.	INTEROPERABILITY COMPLIANCE TESTING .....	5
2.2.	TEST RESULTS .....	6
2.3.	SUPPORT.....	6
<b>3.</b>	<b>REFERENCE CONFIGURATION .....</b>	<b>7</b>
<b>4.</b>	<b>EQUIPMENT AND SOFTWARE VALIDATED.....</b>	<b>9</b>
<b>5.</b>	<b>CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....</b>	<b>11</b>
5.1.	LICENSING AND CAPACITY .....	11
5.2.	SYSTEM FEATURES.....	13
5.3.	IP NODE NAMES.....	14
5.4.	CODECS.....	14
5.5.	IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER .....	16
5.6.	CONFIGURE IP INTERFACE FOR PROCR .....	19
5.7.	SIGNALING GROUP .....	19
5.8.	TRUNK GROUP .....	21
5.9.	CALLING PARTY INFORMATION.....	25
5.10.	OUTBOUND ROUTING .....	26
5.11.	INCOMING CALL HANDLING TREATMENT .....	30
5.12.	CONTACT CENTER CONFIGURATION .....	31
5.12.1.	Announcements .....	31
5.12.2.	ACD Configuration for Call Queued for Handling by Agent.....	31
5.13.	AVAYA AURA® COMMUNICATION MANAGER STATIONS .....	35
5.14.	SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.....	35
<b>6.</b>	<b>CONFIGURE AVAYA AURA® SESSION MANAGER .....</b>	<b>36</b>
6.1.	AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION .....	37
6.2.	SPECIFY SIP DOMAIN.....	39
6.3.	ADD LOCATION.....	40
6.4.	ADD SIP ENTITIES.....	41
6.4.1.	Configure Session Manager SIP Entity.....	42
6.4.2.	Configure Communication Manager SIP Entity .....	44
6.4.3.	Configure Avaya Session Border Controller SIP Entity .....	45
6.4.4.	Configure Avaya Experience Portal SIP Entity .....	46
	Figure 46: Experience Portal SIP Entity .....	46
6.5.	ADD ENTITY LINKS .....	47
6.6.	CONFIGURE TIME RANGES .....	48
6.7.	ADD ROUTING POLICIES.....	49
6.8.	ADD DIAL PATTERNS .....	51
<b>7.</b>	<b>CONFIGURE AVAYA SESSION BORDER CONTROLLER.....</b>	<b>55</b>
7.1.	LOG IN TO AVAYA SESSION BORDER CONTROLLER .....	55
7.2.	SERVER INTERWORKING.....	58
7.2.1.	Configure Server Interworking Profile - Avaya Site .....	58
7.2.2.	Configure Server Interworking Profile – Cox Communications SIP Trunk Site .....	59
7.3.	CONFIGURE SIGNALING MANIPULATION.....	60
7.4.	CONFIGURE SERVICES .....	61
7.4.1.	Configure SIP Server – Avaya Site .....	61
7.4.2.	Configure SIP Server – Cox Communications SIP Trunk.....	63

7.5.	ROUTING .....	66
7.5.1.	Configure Routing – Avaya Site .....	66
7.5.2.	Configure Routing – Cox Communications SIP Trunk Site .....	68
7.6.	TOPOLOGY HIDING.....	69
7.6.1.	Configure Topology Hiding – Avaya Site.....	69
7.6.2.	Configure Topology Hiding Profile – Cox Communications SIP Trunk site .....	70
7.7.	DOMAIN POLICIES .....	71
7.7.1.	Create Application Rules .....	71
7.7.2.	Create Media Rules.....	72
7.7.3.	Create Endpoint Policy Groups .....	73
7.8.	NETWORK & FLOWS.....	75
7.8.1.	Manage Network Settings.....	75
7.8.2.	Create Media Interfaces.....	78
7.8.3.	Create Signaling Interfaces.....	79
7.8.4.	Configuration Server Flows.....	80
7.8.4.1	Create End Point Flows – SMVM Flow.....	80
7.8.4.2	Create End Point Flows – Cox Communications SIP Trunk Flow.....	81
<b>8.</b>	<b>CONFIGURE AVAYA EXPERIENCE PORTAL .....</b>	<b>82</b>
8.1.	BACKGROUND .....	82
8.2.	LOGGING IN AND LICENSING .....	83
8.3.	VOIP CONNECTION .....	85
8.4.	SPEECH SERVERS .....	88
8.5.	APPLICATION.....	89
8.6.	MPP SERVERS AND VOIP SETTINGS .....	91
8.7.	CONFIGURING RFC2833 EVENT VALUE OFFERED BY EXPERIENCE PORTAL.....	94
<b>9.</b>	<b>COX COMMUNICATIONS SIP TRUNK CONFIGURATION.....</b>	<b>95</b>
<b>10.</b>	<b>VERIFICATION STEPS.....</b>	<b>95</b>
<b>11.</b>	<b>CONCLUSION.....</b>	<b>96</b>
<b>12.</b>	<b>REFERENCES.....</b>	<b>97</b>
<b>13.</b>	<b>APPENDIX A - SIGMA SCRIPT.....</b>	<b>99</b>
<b>14.</b>	<b>APPENDIX B - COX MANAGED CPE CONFIGURATION.....</b>	<b>100</b>
14.1.	COX MANAGED CPE LOGIN.....	100
14.2.	NETWORK CONFIGURATION .....	102
14.3.	VLAN CONFIGURATION .....	104
14.4.	VOIP SIP SETTINGS .....	105
14.5.	VOIP SURVIVABILITY .....	106
14.6.	ALG TRUNKING CONFIGURATION .....	107
14.7.	TRUNKING GROUP CONFIGURATION .....	109

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Cox Communications 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 Experience Portal 8.1, Avaya Session Border Controller (Avaya SBCE) 10.1 and various Avaya endpoints. Cox Managed CPE (Edgewater EdgeMarc 2900E SIP Application-Layer Gateway) is included as part of the Service Provider service and not as part of the CPE solution (See **Section 14 Appendix B** for more information).

Customers using this Avaya SIP-enabled enterprise solution with Cox Communications 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 Cox Communications 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 Cox Communications SIP Trunk Service did not include use of any specific encryption features as requested by Cox Communications.

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

## 2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider
- Outgoing PSTN calls from various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used during the test: Avaya one-X<sup>®</sup> Communicator (1XC) and Avaya Workplace Client for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Workplace was used during the test as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using UDP, port 5060 between the Avaya enterprise and Cox Communications
- Codec G.711MU
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call transfer (using SIP re-Invite), conference, off-net call forwarding, forwarding to Avaya Aura<sup>®</sup> Messaging and EC500 mobility (extension to cellular)
- Call Center scenarios
- T38 fax
- DTMF - RFC2833
- Remote Worker (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 Avaya Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold)

Items not supported include the following:

- Cox Communications does not support SIP registration and authentication
- Cox Communications does not support TLS/SRTP SIP Transport
- The SIP REFER in the off-net call redirection was not tested during the compliance testing because Cox Communications did not fully support it. Cox Communications confirmed that SIP REFER is only supported without sending a NOTIFY message. Therefore, the SIP RE-INVITE was tested in the off-net call redirection instead.

## 2.2. Test Results

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

- The Cox Managed CPE did not forward Diversion header (or PAI header) to Cox Communications network in off-net call forward. Although the Cox Managed CPE did not forward Diversion header (or PAI header) to Cox Communications network in off-net call forward, the off-net call forward still worked successfully. As far as Cox Communications is aware, this issue should be fixed in new Cox Managed CPE firmware load (Potentially 15.7.0 or higher firmware).

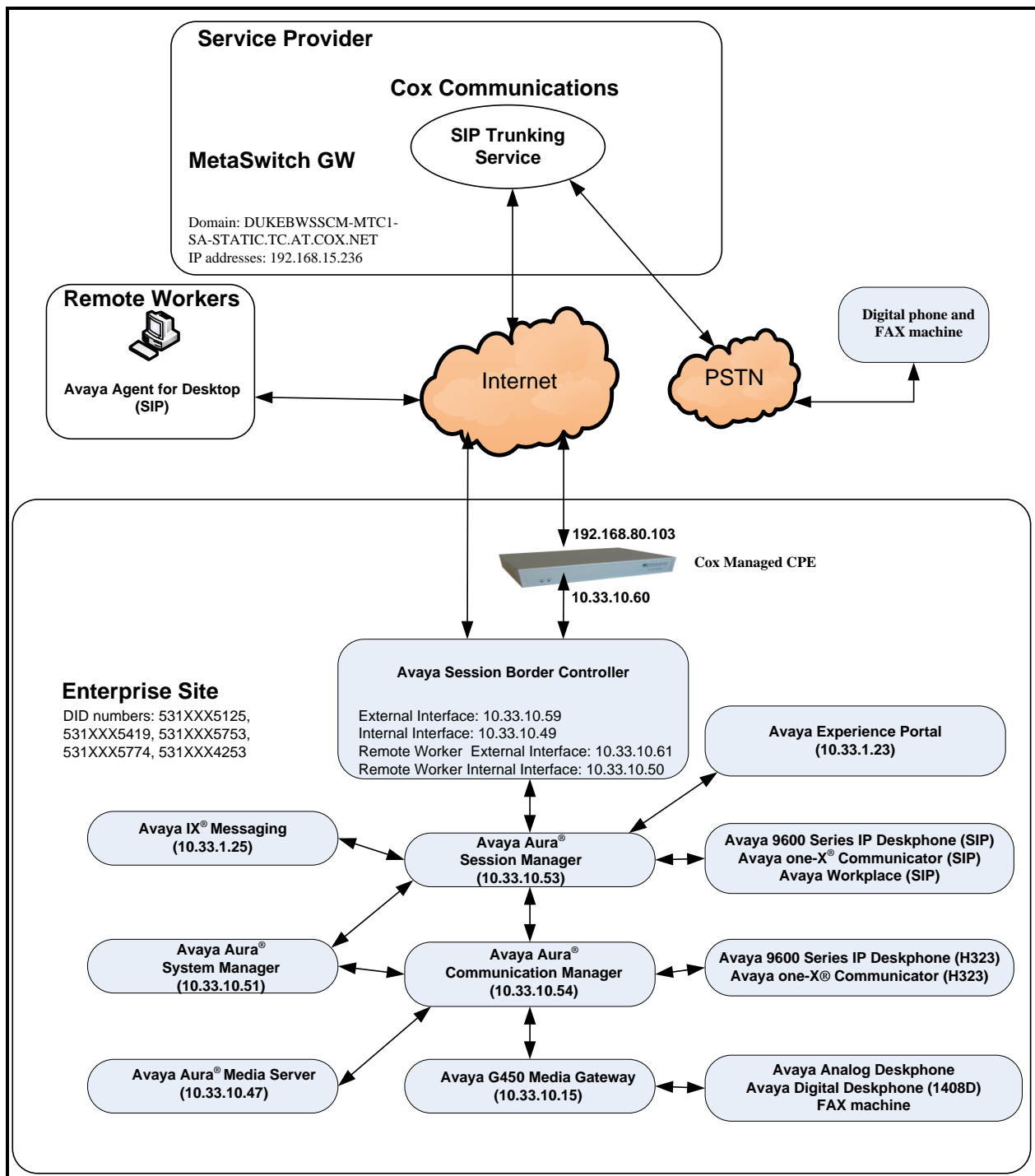
## 2.3. Support

For technical support on Cox Communications SIP Trunking, contact Cox Communications at <http://www.cox.com>

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>

### 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to Cox Communications 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 Cox Communications SIP Trunk**

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



## 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 running on VMware®-based Avaya appliance	10.1.3.0.1.974.27893
Avaya G450 Media Gateway	FW42.22
Avaya Aura® Session Manager running on VMware®-based Avaya appliance	10.1.2.0.1012016
Avaya Aura® System Manager running on VMware®-based Avaya appliance	10.1.2.0 Build No. 10.1.0.0.537353 Software Update Rev. No. 10.1.2.0.0715476 FP 2
Avaya IX Messaging	11.0.0.3204
Avaya Aura® Media Server running on VMware®-based Avaya appliance	10.1.0.147
Avaya Session Border Controller running on VMware®-based Avaya appliance	10.1.1.0-35-21872
Avaya Experience Portal running on VMware®-based Avaya appliance	8.1.1.0.0121
Avaya 9621G IP Deskphone (SIP)	Avaya® Deskphone SIP 7.1.15.2.1
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	3.28.0.73
Avaya one-X® Communicator (H.323 & SIP)	6.2.14.15-SP14P7
Avaya Agent for Desktop (SIP)	2.0.6.26.3001
Avaya Analog Deskphone	N/A
VentaFax	7.10.258.664
Cox Communications SIP Trunk Components	
Equipment/Software	Release/Version
Cox managed CPE	15.8.2
MetaSwitch GW	4.3.40

**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 Experience Portal, Avaya IX Messaging, Avaya Aura® Media Server and Avaya Media Gateway has been previously completed and is not discussed in this document.

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Cox Communications 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.

<b>display system-parameters customer-options</b>		<b>Page</b>	<b>2 of 12</b>
OPTIONAL FEATURES			
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
<b>Maximum Administered SIP Trunks:</b>		<b>4000</b>	<b>100</b>
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**.

display system-parameters customer-options		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? n	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
<b>ARS? y</b>	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? Y		

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

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

display system-parameters customer-options		Page 6 of 12
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	
Port Network Support? n	Time of Day Routing? y	
Posted Messages? y	TN2501 VAL Maximum Capacity? y	
<b>Private Networking? y</b>	Uniform Dialing Plan? y	
Processor and System MSP? y	Usage Allocation Enhancements? y	
<b>Processor Ethernet? y</b>	Wideband Switching? y	
Remote Office? y	Wireless? n	
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 features                                     Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

**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**).

```
change system-parameters features                                     Page 9 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

      CPN/ANI/ICLID PARAMETERS
      CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
      CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

      DISPLAY TEXT
      Identity When Bridging: principal
      User Guidance Display? n
      Extension only label for Team button on 96xx H.323 terminals? n

      INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code:
      International Access Code:

      SCCAN PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

      CALLER ID ON CALL WAITING PARAMETERS
      Caller ID on Call Waiting Delay Timer (msec): 200
```

**Figure 6: System-Parameters Features Form – Page 9**

### 5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP Addresses as below:

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

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

```
change node-names ip                                     Page 1 of 2
                                                         IP NODE NAMES
Name              IP Address
AMS               10.33.10.47
bvwasm2           10.33.10.53
default           0.0.0.0
procr             10.33.10.54
procr6            ::
```

Figure 7: Node-Names IP Form

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. In the compliance test, **ip-codec-set 1** was used for this purpose. Cox Communications supports the **G.711MU** codec. 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
Codec           Suppression Per Pkt   Size(ms)
1: G.711MU      n         2        20

Media Encryption                               Encrypted SRCTP: enforce-enc-srtpc
1: none
2: 1-srtp-aescm128-hmac80
```

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, set the **FAX Mode** to **t.38-standard**. Note: Cox Communications supports T.38 fax during the compliance test.

change ip-codec-set 1		Page 2 of 2	
IP MEDIA PARAMETERS			
Allow Direct-IP Multimedia? y			
Maximum Call Rate for Direct-IP Multimedia: 1024: Kbits			
Maximum Call Rate for Priority Direct-IP Multimedia: 1024: Kbits			
	Mode	Redundancy	Packet Size(ms)
<b>FAX</b>	<b>t.38-standard</b>	0 ECM: y	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

**Figure 9: IP-Codec-Set Form – Page 2**

## 5.5. IP Network Region for Media Gateway, Media Server

Network regions 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 **bvwddev.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: bvwddev.com
Name: public            Stub Network Region: n
MEDIA PARAMETERS        Intra-region IP-IP Direct Audio: yes
                        Codec Set: 1                Inter-region IP-IP Direct Audio: yes
                        UDP Port Min: 2048          IP Audio Hairpinning? n
                        UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS        RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

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



The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for **Network Region 1**. It can also be observed that the **Controller IP 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: 42 .22 .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**.

```
display media-gateway 1                                     Page 2 of 2
                                MEDIA GATEWAY 1

                                Type: g450

Slot  Module Type      Name      DSP Type  FW/HW version
V1:   MM712            DCP MM    MP80      170  7
V2:   MM711            ANA MM
V3:
V4:
V5:
V6:
V7:
V8:
V9:   gateway-announcements  ANN VMM

Max Survivable IP Ext: 8
```

Figure 12: Media Gateway – Page 2

The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined 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

    Node 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

                                Target socket load: 4800

    Enable Interface? y          Allow H.323 Endpoints? y
                                Allow H.248 Gateways? y
    Network Region: 1           Gatekeeper Priority: 5

                                IPV4 PARAMETERS
                                Node Name: procr          IP Address: 10.33.10.54
                                Subnet Mask: /24
```

Figure 14: IP-Interface Form

## 5.7. Signaling Group

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

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

- Set the **Group Type** field to **sip**
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP Address of Communication Manager as defined in **Section 5.3**
- Set the **Far-end Node Name** to **bwasm2**. 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

add signaling-group 20		Page 1 of 2
SIGNALING GROUP		
Group Number: 20	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
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: bvwasm2	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: bvwdev.com		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP 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**

- Set the **Far-end Node Name** to **AMS**. This node name maps to the IP Address of Media Server as defined in **Section 5.3**
- Set the **Near-end Listen Port** to **9061** and **Far-end Listen Port** to a valid unused port for TLS, such as **5071**
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the **Far-end Domain** to **10.33.10.47** (This is Media Server IP Address)

change signaling-group 11

Page 1 of 2

SIGNALING GROUP

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

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

**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.

<b>add trunk-group 20</b>		Page 2 of 4
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
Redirect On OPTIM Failure: 5000		
SCCAN? n	Digital Loss Group: 18	
	<b>Preferred Minimum Session Refresh Interval (sec): 600</b>	
Disconnect Supervision - In? y Out? y		
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n	

**Figure 18: Trunk-Group – Page 2**

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

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2** if the inbound call 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.

add trunk-group 20

Page 3 of 4

TRUNK FEATURES

ACA Assignment? n

Measured: none

Maintenance Tests? y

Suppress # Outpulsing? n

Numbering Format: public

UI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Hold/Unhold Notifications? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

**Figure 19: Trunk-Group – Page 3**

On **Page 4**, the **Network Call Redirection** field should be set to **n** so that Communication Manager will not send SIP REFER. Note: In the compliance test, Cox Communications did not fully support SIP Refer (See **Section 2.1 – Items not supported** in detail). Cox Communications supported SIP re-Invite/Update in redirected call.

Set the **Send Diversion Header** field to **y**. The Diversion Header is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Note: In the compliance test, the Cox managed CPE did not forward Diversion header (or PAI header) to Cox Communications network in off-net call forward (See **Section 2.2** in detail).

Set the **Support Request History** field to **y**. For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya IX Messaging. Set **Always Use re-INVITE for Display Updates** to **y**.

add trunk-group 20

Page 4 of 4

PROTOCOL VARIATIONS

Mark Users as Phone? n

Prepend '+' to Calling/Alerting/Diverting/Connected Number? n

Send Transferring Party Information? n

**Network Call Redirection? n**

**Send Diversion Header? y**

**Support Request History? y**

Telephone Event Payload Type: 101

Convert 180 to 183 for Early Media? n

**Always Use re-INVITE for Display Updates? y**

Resend Display UPDATE Once on Receipt of 481 Response? n

Identity for Calling Party Display: P-Asserted-Identity

Block Sending Calling Party Location in INVITE? n

Accept Redirect to Blank User Destination? n

Enable Q-SIP? n

**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 **5** 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-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
					Total Administered: 1
					Maximum Entries: 240
5	0	20	531XXX	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 **5** for extension (**udp**)
- **Dialed String** beginning with **9** for feature access code (**fac**)
- **Dialed String** beginning with **\*** for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk Group 20 in **Section 5.8**

change dialplan analysis								
DIAL PLAN ANALYSIS TABLE								
Location: all								
Percent Full: 2								
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	4	ext						
181	4	ext						
189	4	ext						
3	4	ext						
5	4	udp						
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

Page1 of 11

FEATURE ACCESS CODE (FAC)

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: 9Access Code 2:

Automatic Callback Activation:Deactivation:

Call Forwarding Activation Busy/DA: All:Deactivation:

Call Forwarding Enhanced Status: Act:Deactivation:

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:Deactivation:

Contact Closure Open Code:Close Code:

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

Page1 of 2

ARS DIGIT ANALYSIS TABLE

Location: allPercent Full: 1

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req
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 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									
No		Mrk	Lmt	List	Del	Digits		DCS/	IXC							
								QSIG	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
	0	1	2	M	4	W	Request		Dgts	Format	
1:	Y	Y	Y	Y	Y	n	n		rest	pub-unk	none
2:	Y	Y	Y	Y	Y	n	n		rest		none
3:	Y	Y	Y	Y	Y	n	n		rest		none
4:	Y	Y	Y	Y	Y	n	n		rest		none
5:	Y	Y	Y	Y	Y	n	n		rest		none
6:	Y	Y	Y	Y	Y	n	n		rest		none

**Figure 25: Route–Pattern Form**

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

change cor 1		Page 1 of 23
CLASS OF RESTRICTION		
COR Number: 1		
COR Description:		
FRL: 2	APLT? y	
Can Be Service Observed? y	<b>Calling Party Restriction: none</b>	
Can Be A Service Observer? y	Called Party Restriction: none	
Time of Day Chart: 1	Forced Entry of Account Codes? n	
Priority Queuing? n	Direct Agent Calling? n	
Restriction Override: none	Facility Access Trunk Test? n	
Restricted Call List? n	Can Change Coverage? n	
Access to MCT? y	Fully Restricted Service? n	
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n	
Send ANI for MFE? n	Add/Remove Agent Skills? n	
MF ANI Prefix:	Automatic Charge Display? n	
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n	
	Can Be Picked Up By Directed Call Pickup? n	
	Can Use Directed Call Pickup? n	
	Group Controlled Restriction: inactive	

**Figure 26: Class of Restriction Form**

## 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 **531XXX5774** to **1810** or **0797** by deleting **10** of the incoming digits for Voicemail or Vector testing purpose. (1810 is voice mail number and 0797 is Vector Directory Number (VDN))
- The incoming DID number **531XXX5753** to **4800** by deleting **10** of the incoming digits for Experience Portal testing purpose
- The incoming DID number **531XXX** to 4-digit extension by deleting **6** of the incoming digits for inbound call testing purpose.

change inc-call-handling-trmt trunk-group 20				Page 1 of 3	
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del Insert		
public-ntwrk	10	531XXX5774	10	1810	
public-ntwrk	10	531XXX5753	10	4800	
public-ntwrk	10	531XXX	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
```

ANNOUNCEMENTS/AUDIO SOURCES				
Announcement Extension	Type	Name	Source	Num of Files
1898	integrated	SP2	001V9	1
1899	integrated	SP1	001V9	1

Figure 28: Announcement Configuration

### 5.12.2. ACD Configuration for Call Queued for Handling by Agent

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

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

```
display hunt-group 13
```

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

Figure 29: Hunt Group Configuration – Page 1

The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note that **Skill** is set to **y**.

display hunt-group 13	HUNT GROUP	Page 2 of 3
<b>Skill?</b> y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	

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

VDN 0797, shown below, is associated with vector 3

display vdn 0797	VECTOR DIRECTORY NUMBER	Page 1 of 3
EXTENSION: 0797	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 Adjunct Calls as ACD*? n	

**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
      Auto Answer: station
      MWI Served User Type:                          MIA Across Skills: system
      AUX Agent Remains in LOA Queue: system        ACW Agent Considered Idle: system
      AUX Agent Considered Idle (MIA): system        Aux Work Reason Code Type: system
      Work Mode on Login: 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**

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				Page 2 of 2			
				AGENT LOGINID			
Direct Agent Skill:				Service Objective? n			
Call Handling Preference: skill-level				Local Call Preference? n			
	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® Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to **y** as shown in the screen below.

change system-parameters features				Page 11 of 19			
				FEATURE-RELATED SYSTEM PARAMETERS			
CALL CENTER SYSTEM PARAMETERS							
EAS							
<b>Expert Agent Selection (EAS) Enabled? y</b>							
Minimum Agent-LoginID Password Length: 4							

Figure 35: Enable Expert Agent Selection

### 5.13. Avaya Aura® Communication Manager Stations

In the sample configuration, a 4-digit station extension was used with the format 5125. Use the **add station 5125** command to add an Avaya H.323 IP Deskphone.

- Enter **Type: 9621, Name: H323-5125, 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

<b>add station 5125</b>		Page 1 of 5
STATION		
Extension: 5125	Lock Messages? n	BCC: 0
<b>Type: 9621</b>	<b>Security Code: *</b>	TN: 1
Port: S000055	<b>Coverage Path 1: 1</b>	COR: 1
<b>Name: H323-5125</b>	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 5125	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: English	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

Figure 36: Add-Station Form

### 5.14. Save Avaya Aura® Communication Manager Configuration Changes

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

## 6. Configure Avaya Aura® Session Manager

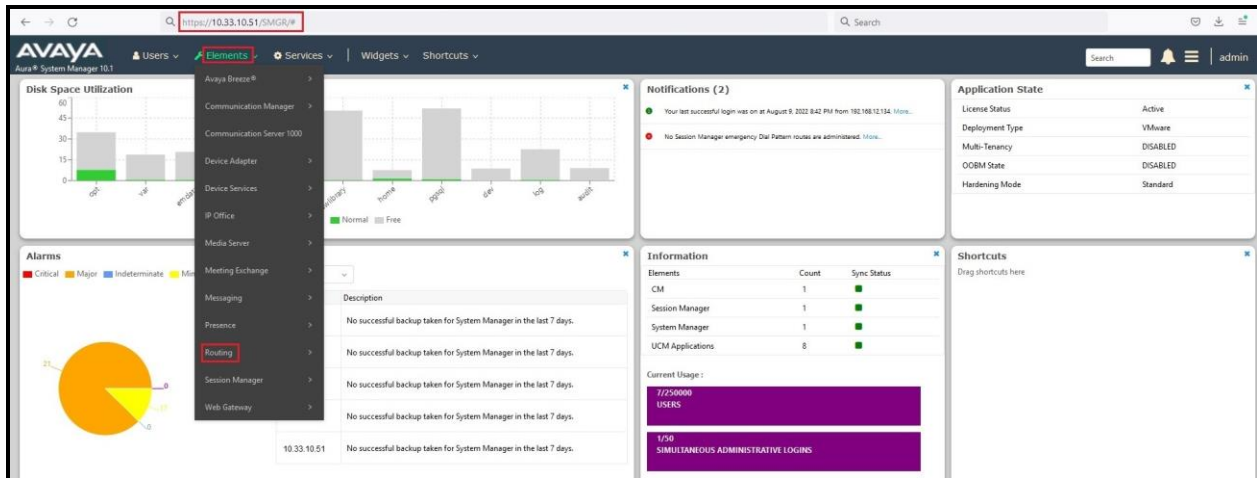
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

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

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

## 6.1. Avaya Aura® System Manager Login and Navigation

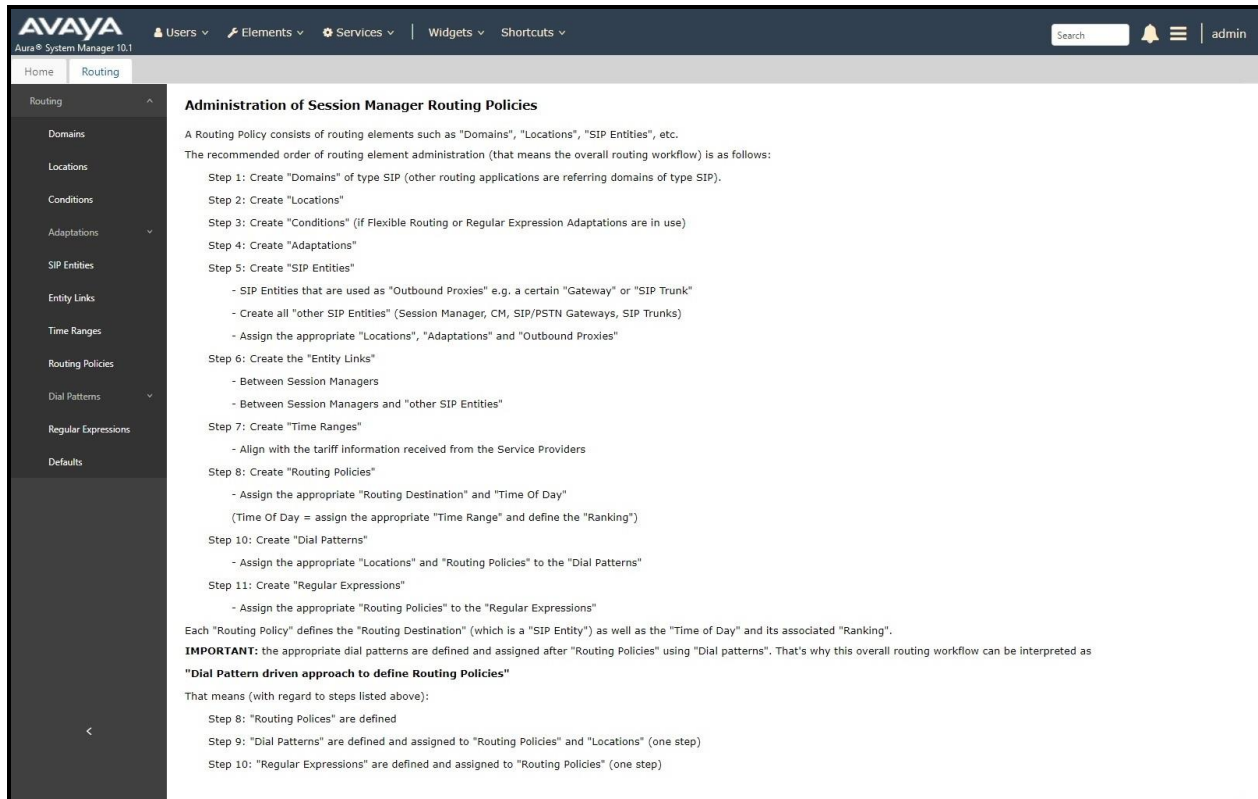
Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP Address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press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



**Figure 37: System Manager Home Screen**

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

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



**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 → 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.



**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 → 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.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left navigation pane has 'Routing' and 'Locations' highlighted. The main area is titled 'Location Details' with a 'General' tab selected. The 'Name' field is set to 'Belleville-GSSCP'. Other fields include 'Notes', 'Dial Plan Transparency in Survivable Mode' (Enabled), 'Listed Directory Number', 'Associated CM SIP Entity', 'Overall Managed Bandwidth' (Managed Bandwidth Units: Kbit/sec, Total Bandwidth, Multimedia Bandwidth, Audio Calls Can Take Multimedia Bandwidth: checked), 'Per-Call Bandwidth Parameters' (Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec, Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec, Minimum Multimedia Bandwidth: 64 Kbit/Sec, Default Audio Bandwidth: 80 Kbit/Sec), 'Alarm Threshold' (Overall Alarm Threshold: 80 %, Multimedia Alarm Threshold: 80 %, Latency before Overall Alarm Trigger: 5 Minutes, Latency before Multimedia Alarm Trigger: 5 Minutes), and 'Location Pattern'.

**Figure 40: Location Configuration**



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

The screenshot shows the 'Location Pattern' configuration window. It has a title bar 'Location Pattern' and two buttons 'Add' and 'Remove'. Below the title bar, it says '3 Items'. There is a table with the following content:

	IP Address Pattern
<input type="checkbox"/>	10.33.1.*
<input type="checkbox"/>	10.33.10.*
<input type="checkbox"/>	10.33.100.*

At the bottom left, it says 'Select : All, None'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

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

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

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

In this configuration, there are four SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller SIP Entity
- Experience Portal SIP Entity

### 6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **bvwasrm2**. 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**.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left sidebar shows the navigation menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The configuration form contains the following fields and values:

- Name:** bvwasrm2
- IP Address:** 10.33.10.53
- SIP FQDN:** (empty)
- Type:** Session Manager (dropdown)
- Notes:** (empty)
- Location:** Belleville-GSSCP (dropdown)
- Outbound Proxy:** (empty)
- Time Zone:** America/Toronto (dropdown)
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration (dropdown)

The 'Commit' and 'Cancel' buttons are located at the top right of the form.

**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.

The screenshot shows the 'Listen Ports' configuration interface. At the top, there are input fields for 'TCP Failover port:' and 'TLS Failover port:'. Below these are 'Add' and 'Remove' buttons. A table displays the current configuration with 4 items. The table has columns for 'Listen Ports', 'Protocol', 'Default Domain', and 'Notes'. The first row shows '5061' in the 'Listen Ports' column, 'TLS' in the 'Protocol' column, and 'bvwdev.com' in the 'Default Domain' column. A 'Filter: Enable' button is located on the right side of the table. At the bottom left, there is a 'Select : All, None' option.

Listen Ports	Protocol	Default Domain	Notes
5061	TLS	bvwdev.com	

**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**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left sidebar shows the navigation menu with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. The configuration fields are as follows:

- Name:** CM10
- FQDN or IP Address:** 10.33.10.54
- Type:** CM (dropdown)
- Notes:** (empty text field)
- Adaptation:** (empty dropdown)
- Location:** Belleville-GSSCP (dropdown)
- Time Zone:** America/Toronto (dropdown)
- \* SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** none (dropdown)
- Loop Detection Mode:** On (dropdown)
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration (dropdown)

There are also sections for 'Loop Detection' and 'Monitoring' which are currently empty.

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**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left sidebar shows the navigation menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. The form contains the following fields and values:

- Name:** SBCE
- FQDN or IP Address:** 10.33.10.49
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** (dropdown menu)
- Location:** Belleville-GSSCP
- Time Zone:** America/Toronto
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** (checkbox, unchecked)
- Call Detail Recording:** egress
- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200
- SIP Link Monitoring:** Link Monitoring Enabled
- Proactive Monitoring Interval (in seconds):** 900
- Reactive Monitoring Interval (in seconds):** 120
- Number of Tries:** 1
- Number of Successes:** 1
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

Figure 45: Avaya SBCE SIP Entity

#### 6.4.4. Configure Avaya 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**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left sidebar shows the navigation menu with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' with a 'General' tab. The configuration fields are as follows:

- Name:** Experience Portal
- \* FQDN or IP Address:** 10.33.1.23
- Type:** Voice Portal
- Notes:**
- Adaptation:**
- Location:** Belleville-GSSCP
- Time Zone:** America/Toronto
- \* SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:**
- Securable:**
- Call Detail Recording:** none
- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200
- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration
- Supports Call Admission Control:**
- Shared Bandwidth Manager:**
- Primary Session Manager Bandwidth Association:**
- Backup Session Manager Bandwidth Association:**
- Override Port & Transport with DNS SRV:**

Figure 46: Experience Portal SIP Entity

## 6.5. Add Entity Links

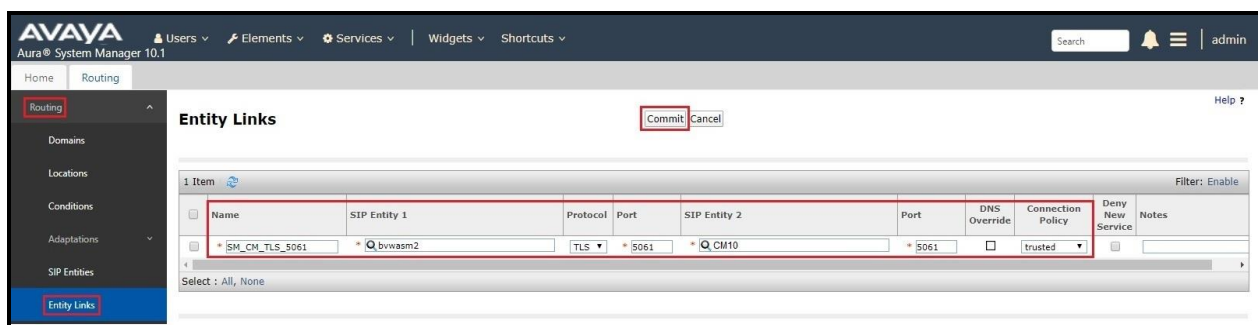
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Three Entity Links were created: one to Communication Manager for use only by the service provider traffic, one to the Avaya SBCE and one to the Experience Portal.

To add an Entity Link, navigate to **Routing → 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

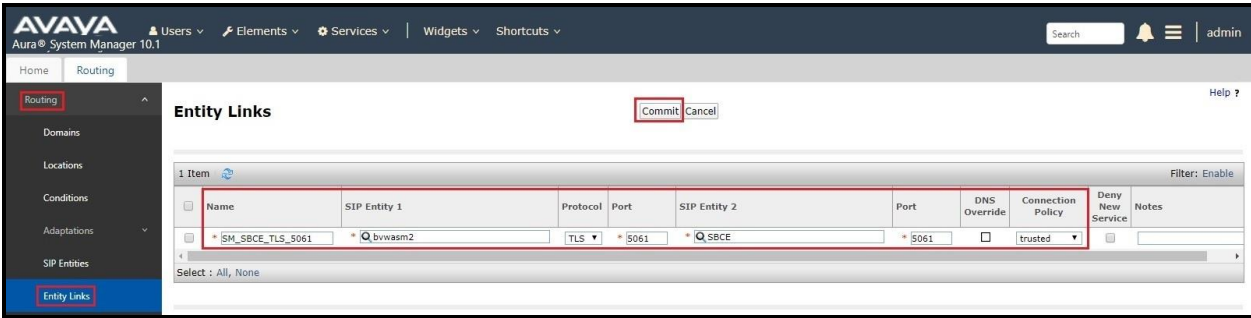
Click **Commit** to save.

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**.



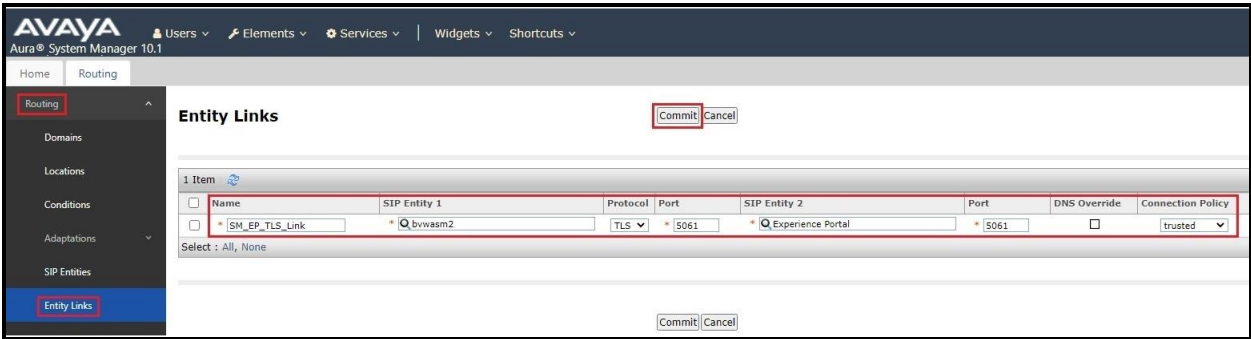
**Figure 47: Communication Manager Entity Link**

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**



**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**.



**Figure 49: Experience Portal Entity Link**

## 6.6. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a Time Range, select **Routing → 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.



**Figure 50: Time Ranges**



## 6.7. Add Routing Policies

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

To add a Routing Policy, navigate to **Routing → 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 Cox Communications to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM10**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button. The 'General' section contains fields for 'Name' (set to 'SP Inbound Calls'), 'Disabled' (unchecked), 'Retries' (set to 0), and 'Notes'. The 'SIP Entity as Destination' section features a 'Select' button and a table with the following data:

Name	FQDN or IP Address
CM10	10.33.10.54

The 'Time of Day' section is partially visible at the bottom.

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

The screenshot displays the 'Routing Policy Details' page in the Avaya Aura System Manager 10.1 interface. The left sidebar shows the 'Routing' menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'General' tab. The 'Name' field is set to 'SP Outbound Calls'. The 'Disabled' checkbox is unchecked. The 'Retries' field is set to '0'. The 'Notes' field is empty. Below the 'General' tab, the 'SIP Entity as Destination' section is visible, showing a table with one entry: 'SBCE' with the FQDN or IP Address '10.33.10.49'. The 'Commit' and 'Cancel' buttons are at the top right.

Name	FQDN or IP Address
SBCE	10.33.10.49

Figure 52: Routing to Cox Communications 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**.

The screenshot displays the 'Routing Policy Details' page in the Avaya Aura System Manager 10.1 interface. The left sidebar shows the 'Routing' menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'General' tab. The 'Name' field is set to 'To-ExperiencePortal'. The 'Disabled' checkbox is unchecked. The 'Retries' field is set to '0'. The 'Notes' field is empty. Below the 'General' tab, the 'SIP Entity as Destination' section is visible, showing a table with one entry: 'Experience Portal' with the FQDN or IP Address '10.33.1.23'. The 'Commit' and 'Cancel' buttons are at the top right.

Name	FQDN or IP Address
Experience Portal	10.33.1.23

Figure 53: Routing to Experience Portal

## 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 Cox Communications 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 → 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 **bwvdev.com** uses **Routing Policy Name** as **SP Outbound Calls** which is defined in **Section 6.7**.

**Avaya Aura System Manager 10.1**

Home Routing

**Dial Pattern Details**

General

Pattern: 1613

Min: 4

Max: 11

Emergency Call: ☐

SIP Domain: bwvdev.com

Notes: SP Outbound Calls

Originating Locations and Routing Policies

Add Remove

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
ALL		SP Outbound Calls	0	<input type="checkbox"/>	SBCE	

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 **531** 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 Cox Communications.

**Dial Pattern Details**

General

\* Pattern: 531  
\* Min: 6  
\* Max: 10

Emergency Call: ☐

SIP Domain: bwvdev.com

Notes: Cox Communications Inbound Calls

Originating Locations and Routing Policies

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville-GSSCP		SP Inbound Calls	0	<input type="checkbox"/>	CRM	

Figure 55: Dial Pattern 531

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**.

**Dial Pattern Details**

General

\* Pattern: 4800  
\* Min: 4  
\* Max: 4

Emergency Call: ☐

SIP Domain: bwvdev.com

Notes: Experience Portal

Originating Locations and Routing Policies

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

Figure 56: Dial Pattern\_4800

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

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Rules
0	1	36	<input type="checkbox"/>			bvdev.com	Cox Communications Outbound Calls
1012	4	11	<input type="checkbox"/>			bvdev.com	Cox Communications Outbound Calls
1002	4	11	<input type="checkbox"/>			bvdev.com	Cox Communications Outbound Calls
011	3	3	<input type="checkbox"/>			bvdev.com	Cox Communications Inbound Calls
012	6	10	<input type="checkbox"/>			bvdev.com	Cox Communications Outbound Calls
012	3	10	<input type="checkbox"/>			bvdev.com	Cox Communications Outbound Calls
011	3	3	<input type="checkbox"/>			bvdev.com	Cox Communications Outbound Calls

**Figure 57: Dial Pattern List**

## 7. Configure Avaya Session Border Controller

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

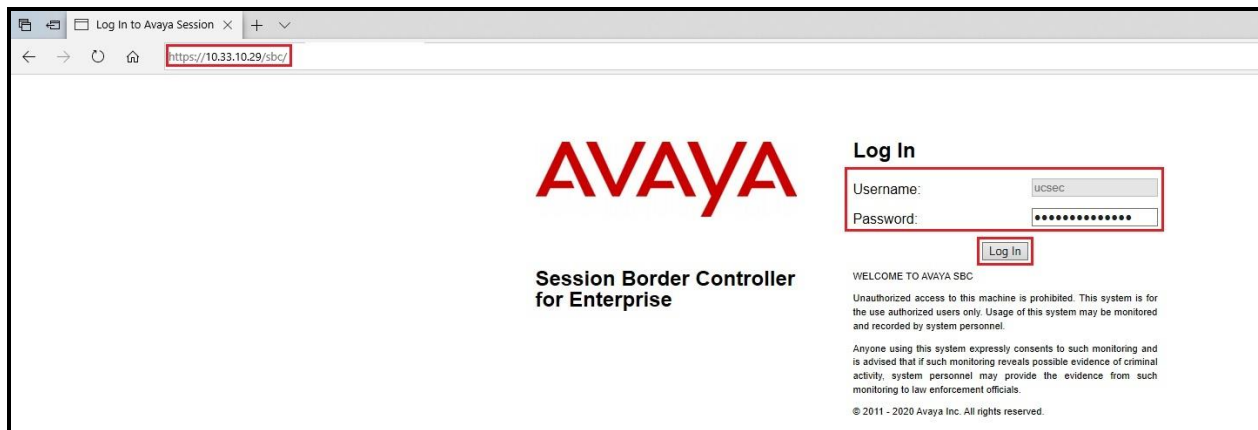
In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Cox Communications system resides on the Public side of the network.

**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

Access the web interface by typing “**https://x.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.

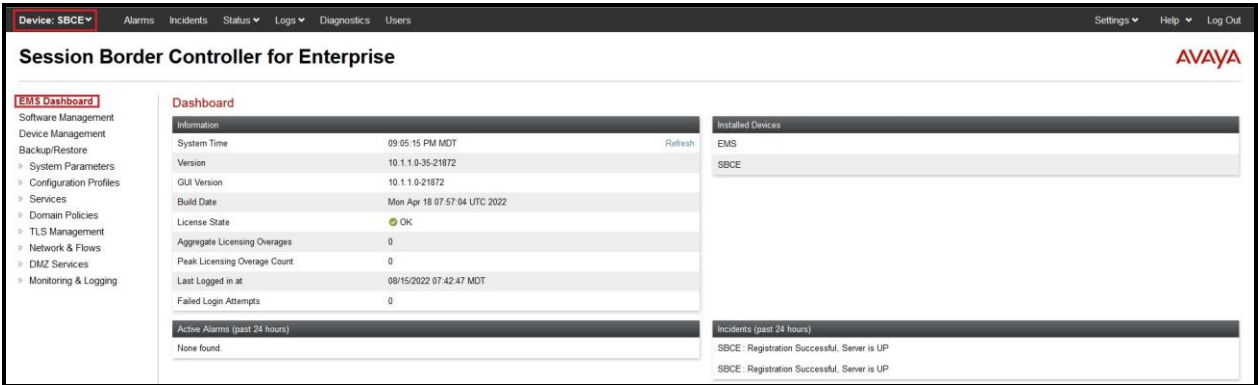


Figure 59: Avaya SBCE Dashboard

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.



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**.

System Information: SBCE

General Configuration

Appliance Name	SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 250	520
Advanced Sessions Requested: 250	520
Scopia Video Sessions Requested: 250	520
CES Sessions Requested: 250	520
Transcoding Sessions Requested: 250	520
AMR	<input type="checkbox"/>
Premium Sessions Requested: 0	0
CLID	---
Encryption Available: Yes	<input checked="" type="checkbox"/>

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.10.49	10.33.10.49	255.255.255.0	10.33.10.1	A1
10.33.10.50	10.33.10.50	255.255.255.0	10.33.10.1	A1
10.33.10.59	10.33.10.59	255.255.255.0	10.33.10.1	B2
10.33.10.61	10.33.10.61	255.255.255.0	10.33.10.1	B2

DNS Configuration

Primary DNS	10.33.100.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.33.80.106

Management IP(s)

IP #1 (IPv4)	10.33.10.29
--------------	-------------

**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** → **Server Interworking**

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

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

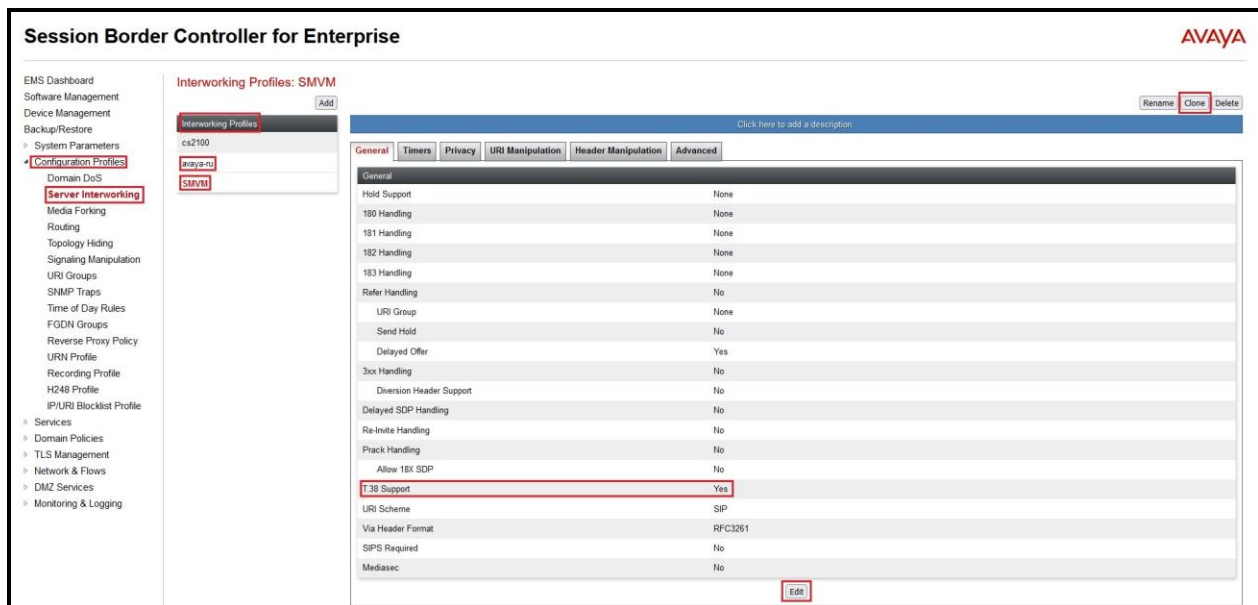


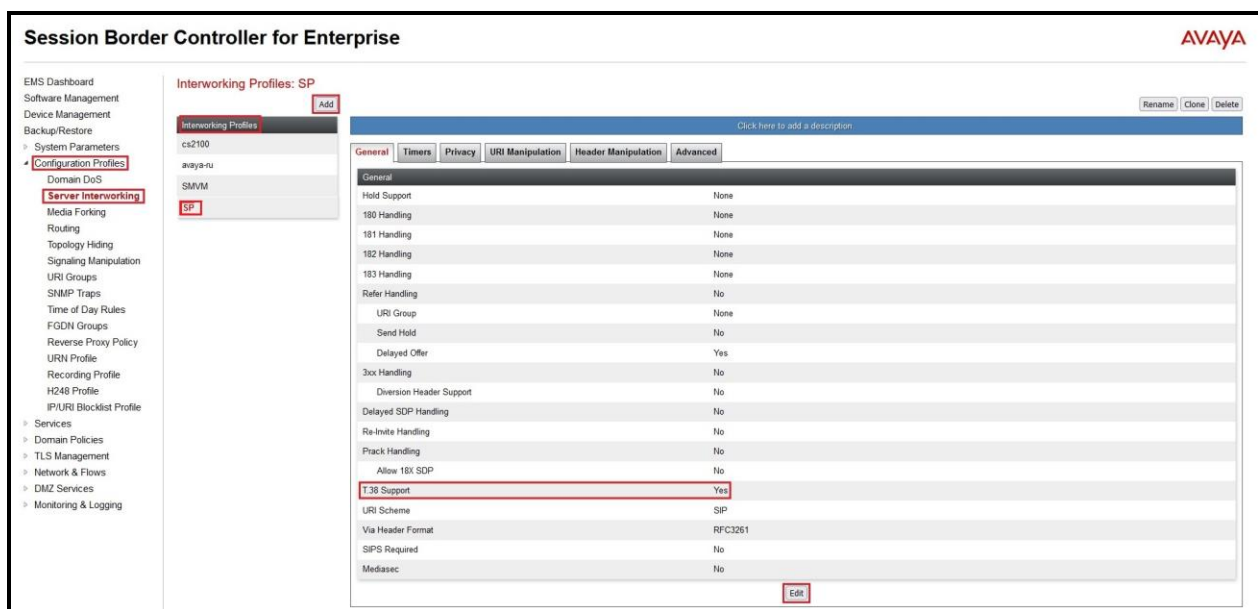
Figure 62: Server Interworking – Avaya site

## 7.2.2. Configure Server Interworking Profile – Cox Communications SIP Trunk Site

From the menu on the left-hand side, select **Configuration Profiles** → **Server Interworking** → **Add**

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

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



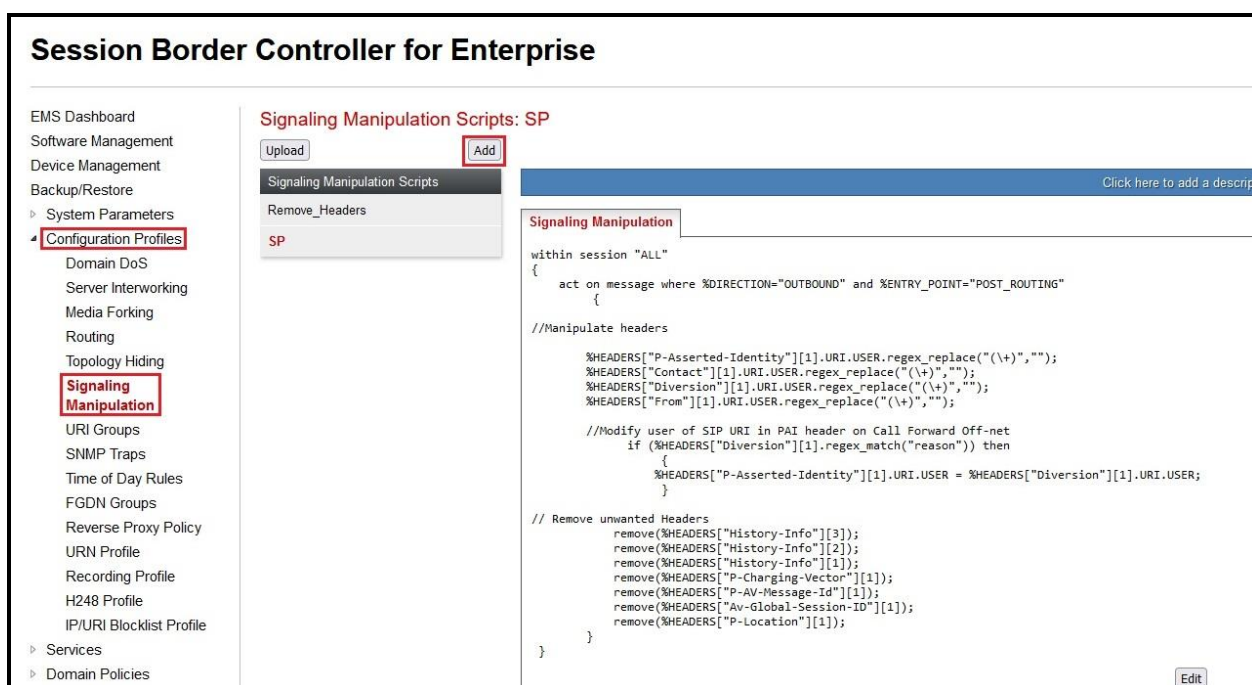
**Figure 63: Server Interworking – Cox Communications SIP Trunk site**

### 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 → Signaling Manipulation → 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 to remove the plus sign
  - Modify user of SIP URI in PAI header on call forward off-net
  - Remove un-wanted SIP headers
  - Click **Save** (not shown)



**Figure 64: Signaling Manipulation**

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

## 7.4. Configure Services

### 7.4.1. Configure SIP Server – Avaya Site

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

From the menu on the left-hand side, select **Services** → **SIP Servers** → **Add**

Enter **Profile Name**: **SMVM**

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

- **Server Type**: Select **Call Server**
- **SIP Domain**: enter **bvwdex.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)

The screenshot displays the 'Session Border Controller for Enterprise' configuration page. On the left is a navigation menu with options like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'H248 Servers', 'LDAP', 'RADIUS', 'Domain Policies', 'TLS Management', and 'Network & Flows'. The 'Services' section is expanded, showing 'SIP Servers' with an 'Add' button. The main area is titled 'SIP Servers: SMVM' and has tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'General' tab is active, showing fields for 'Server Type' (Call Server), 'SIP Domain' (bvwdex.com), 'TLS Client Profile' (AvayaSBCClient), and 'DNS Query Type' (NONE/A). Below these is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one entry: IP Address / FQDN: 10.33.10.53, Port: 5061, Transport: TLS. There are 'Rename', 'Clone', and 'Delete' buttons at the top right, and an 'Edit' button at the bottom right of the table.

IP Address / FQDN	Port	Transport
10.33.10.53	5061	TLS

Figure 65: SIP Server – General - Avaya site

On the **Advanced** tab:

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

General	Authentication	Heartbeat	Registration	Ping	Advanced
Enable DoS Protection <input type="checkbox"/>					
Enable Grooming <input checked="" type="checkbox"/>					
Interworking Profile SMVM					
Signaling Manipulation Script None					
Securable <input type="checkbox"/>					
Enable FGDN <input type="checkbox"/>					
Tolerant <input type="checkbox"/>					
URI Group None					
NG911 Support <input type="checkbox"/>					

**Figure 66: SIP Server – Advanced - Avaya site**

## 7.4.2. Configure SIP Server – Cox Communications SIP Trunk

From the menu on the left-hand side, select **Services** → **SIP Servers** → **Add**

The Cox managed CPE LAN interface IP address is 10.33.10.60

Enter **Profile Name**: **SP**

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

- **Server Type**: Select **Trunk Server**
- **IP Address/FQDN**: **10.33.10.60** (Cox Managed CPE LAN interface IP address)
- **Port**: **5060**
- **Transport**: **UDP**
- Click **Finish** (not shown)

The screenshot shows the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with 'Services' expanded and 'SIP Servers' selected. The main area is titled 'SIP Servers: SP' and has an 'Add' button. Below this is a list of server profiles with 'SP' selected. To the right, the 'General' tab is active, showing the configuration for the selected server. The 'Server Type' is 'Trunk Server', 'DNS Query Type' is 'NONE/A', 'IP Address / FQDN' is '10.33.10.60', 'Port' is '5060', and 'Transport' is 'UDP'. There is an 'Edit' button at the bottom right of the configuration area.

IP Address / FQDN	Port	Transport
10.33.10.60	5060	UDP

Figure 67: SIP Server – General – Cox Communications

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

- Check **Enable Heartbeat**
- Select **Method: OPTIONS**
- Set **Frequency: 60 seconds**
- Input **From URI: ping@10.33.10.59** (Avaya SBCE external interface IP address)
- Input **To URI: ping@10.33.10.60** (Cox Managed CPE LAN IP address)

General	Authentication	Heartbeat	Registration	Ping	Advanced
Enable Heartbeat <input checked="" type="checkbox"/>					
Method OPTIONS					
Frequency 60 seconds					
From URI ping@10.33.10.59					
To URI ping@10.33.10.60					
<a href="#">Edit</a>					

**Figure 68: SIP Server – Heartbeat – Cox Communications**



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 DoS Protection <input type="checkbox"/>					
Enable Grooming <input type="checkbox"/>					
Interworking Profile SP					
Signaling Manipulation Script SP					
Securable <input type="checkbox"/>					
Enable FGDN <input type="checkbox"/>					
Tolerant <input type="checkbox"/>					
URI Group None					
NG911 Support <input type="checkbox"/>					

Edit

**Figure 69: SIP Server – Advanced – Cox Communications**

## 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 → 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 for Enterprise

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
  - Domain DoS
  - Server Interworking
  - Media Forking
  - Routing
  - Topology Hiding
  - Signaling Manipulation
  - URI Groups
  - SNMP Traps
  - Time of Day Rules
  - FGDN Groups
  - Reverse Proxy Policy
  - URN Profile
  - Recording Profile
  - H248 Profile
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

## Routing Profiles: SP\_To\_SMVM

Add

Routing Profiles

default

To\_SMVM\_RW

default\_RW

AS\_To\_SMVM

Click here to add

Routing Profile

Update Priority

Priority	URI Group	Time of Day	Load Balancing	Next Ho
----------	-----------	-------------	----------------	---------

Routing Profile

URI Group

Time of Day

Load Balancing

Transport

LDAP Server Profile

Matched Attribute Priority

Next Hop Priority

Ignore Route Header

ENUM

Time of Day

NAPTR

LDAP Routing

LDAP Base DN (Search)

Alternate Routing

Next Hop In-Dialog

ENUM Suffix

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SMVM	10.33.10.53:5061 (TLS)	None	Delete

Back

Finish

Figure 70: Routing to Session Manager

## 7.5.2. Configure Routing – Cox Communications 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 → 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: 10.33.10.60:5060 (UDP)** (Cox Managed CPE LAN IP address)
- Click **Finish**

**Session Border Controller for Enterprise**

Routing Profiles: SMVM\_To\_SP

**Add**

Routing Profiles

**Add Routing Rule**

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

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SP	10.33.10.60:5060 (UDP)	None	Delete

**Finish**

**Figure 71: Routing to Cox Communications 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 → 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 **To**,
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bwvdev.com**
  - For the Header **From**,
    - In the **Criteria** column select **IP/Domain**
    - In the **Replace Action** column select: **Overwrite**
    - In the **Overwrite Value** column: **bwvdev.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: **bwvdev.com**
- Note: bwvdev.com is SIP domain of enterprise

Click **Finish** (not shown)

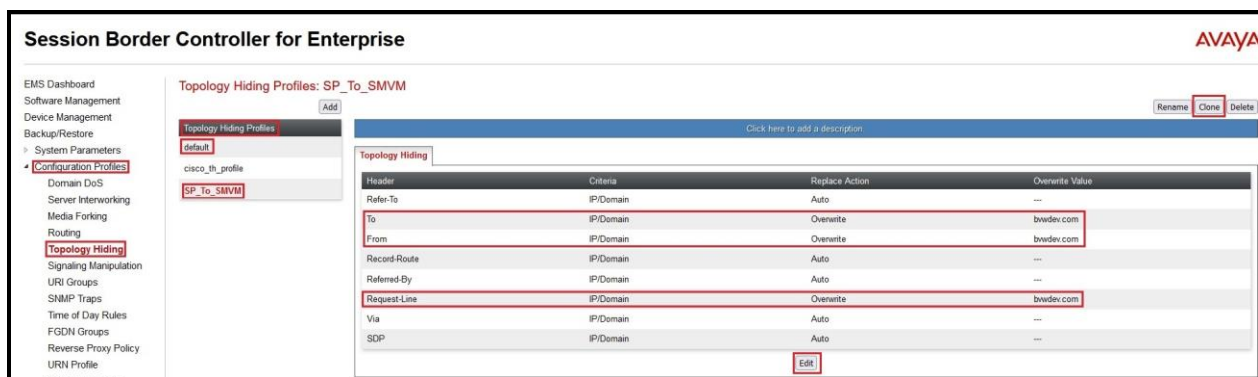


Figure 72: Topology Hiding To Session Manager

## 7.6.2. Configure Topology Hiding Profile – Cox Communications SIP Trunk site

From the menu on the left-hand side, select **Configuration Profiles → 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 **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **10.33.10.60** (Cox Managed CPE LAN IP address)
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **10.33.10.60** (Cox Managed CPE LAN IP address)
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **10.33.10.59** (Avaya SBCE external interface IP address)
- Click **Finish** (not shown)

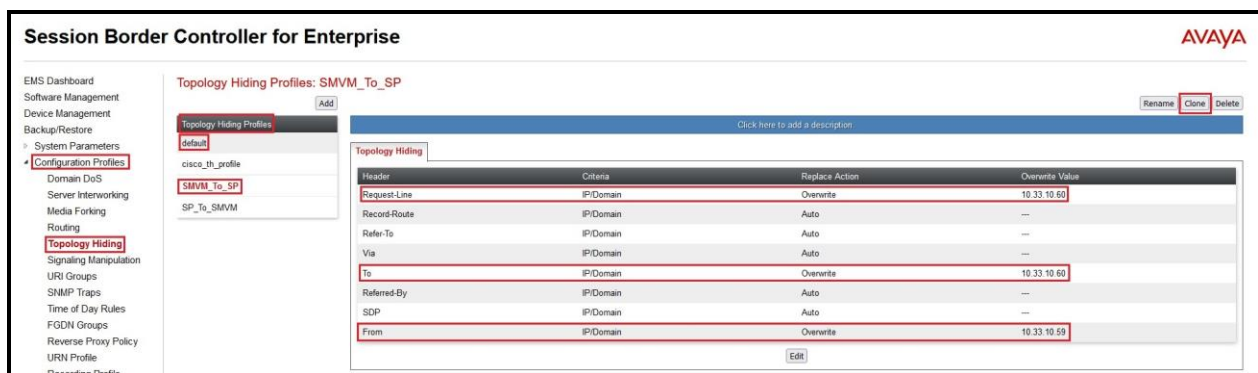


Figure 73: Topology Hiding To Cox Communications

## 7.7. Domain Policies

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

### 7.7.1. Create Application Rules

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

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

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

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

### Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▾ Domain Policies  
    **Application Rules**  
        Border Rules  
        Media Rules  
        Security Rules  
        Signaling Rules  
        Charging Rules  
        End Point Policy  
        Groups  
        Session Policies

**Application Rules: SIP-Trunk**

Add

Rename Clone Delete

Click here to add a description.

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

Miscellaneous

CDR Support	Off
RTCP Keep-Alive	No

Edit

Figure 74: 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** → **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: RTP**
  - **Preferred Format #2: SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**
- Click **Finish** button to apply the changes.

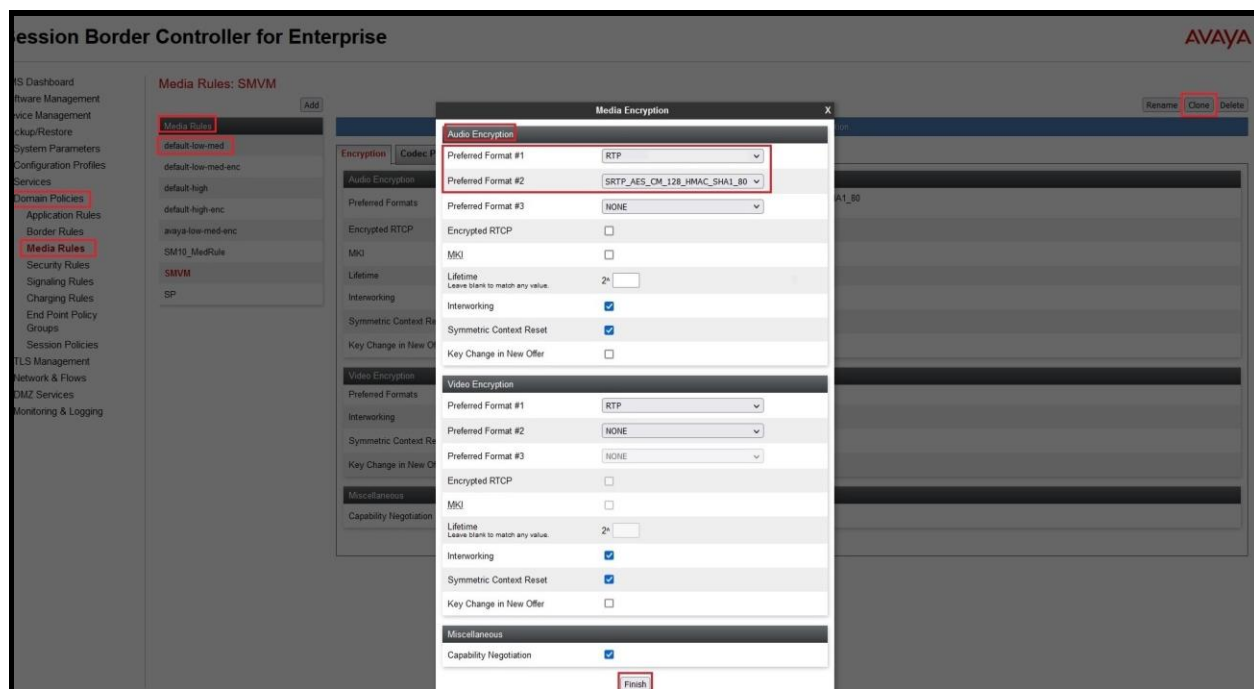
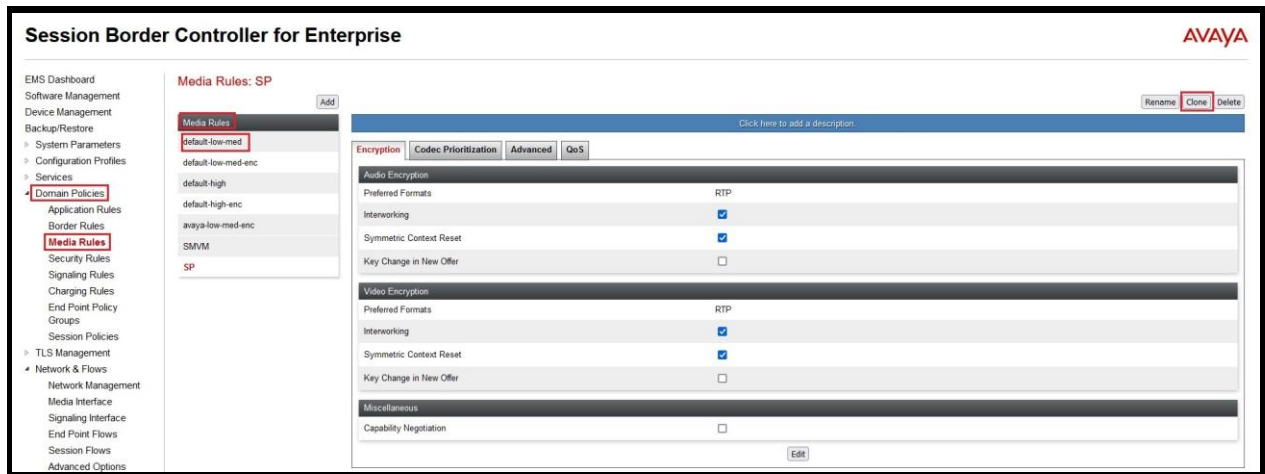


Figure 75: Media Rule 1



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

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



**Figure 76: 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 → 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)



**Figure 77: Endpoint Policy 1**

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

- Select **Add**.
- Enter **Group Name: 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)



**Figure 78: Endpoint Policy 2**

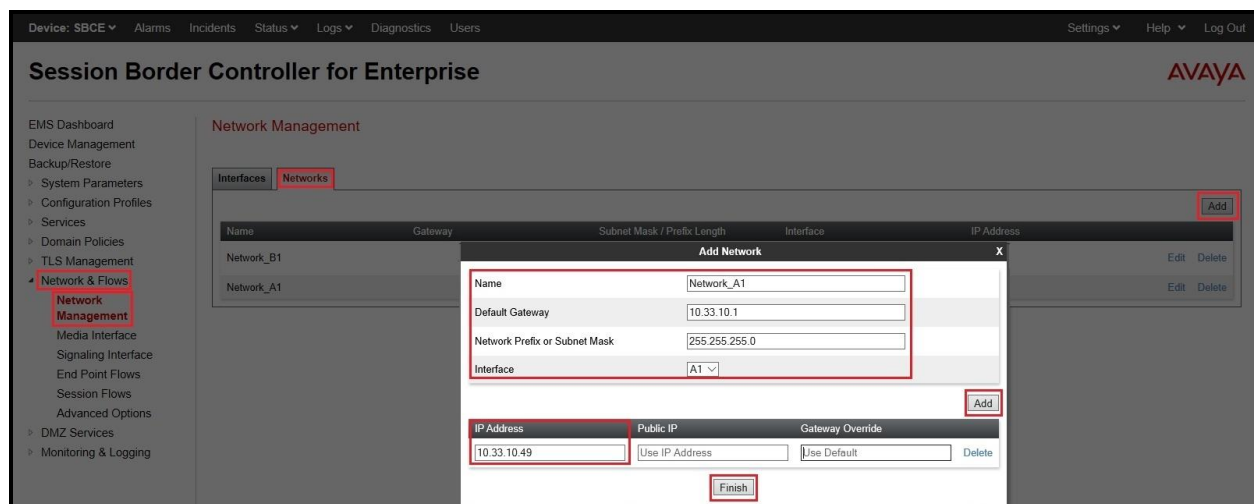
## 7.8. Network & Flows

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**.

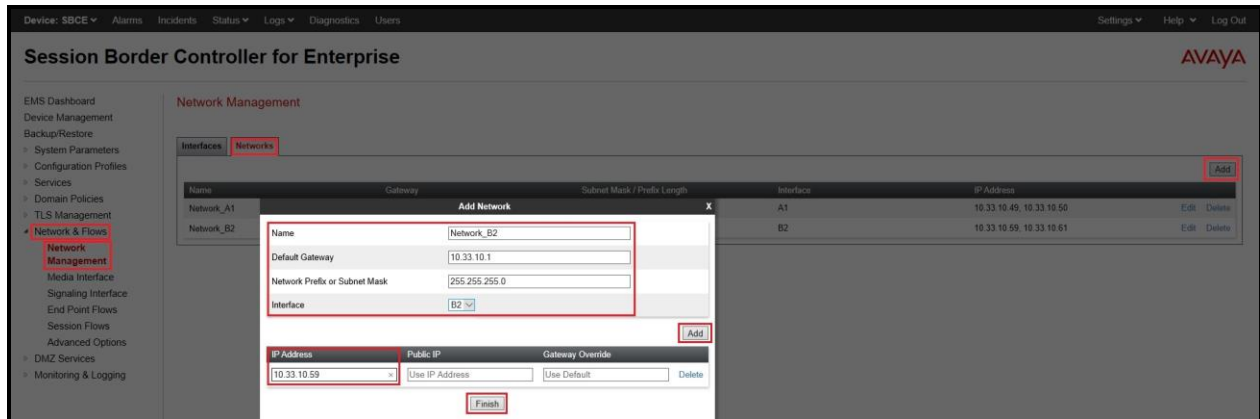
- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name: Network\_A1**
  - **Default Gateway: 10.33.10.1**
  - **Subnet Mask: 255.255.255.0**
  - **Interface: A1** (This is the Avaya SBCE inside interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.33.10.49**
  - Click the **Finish** button to save the changes



**Figure 79: Network Management – Inside Interface**

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

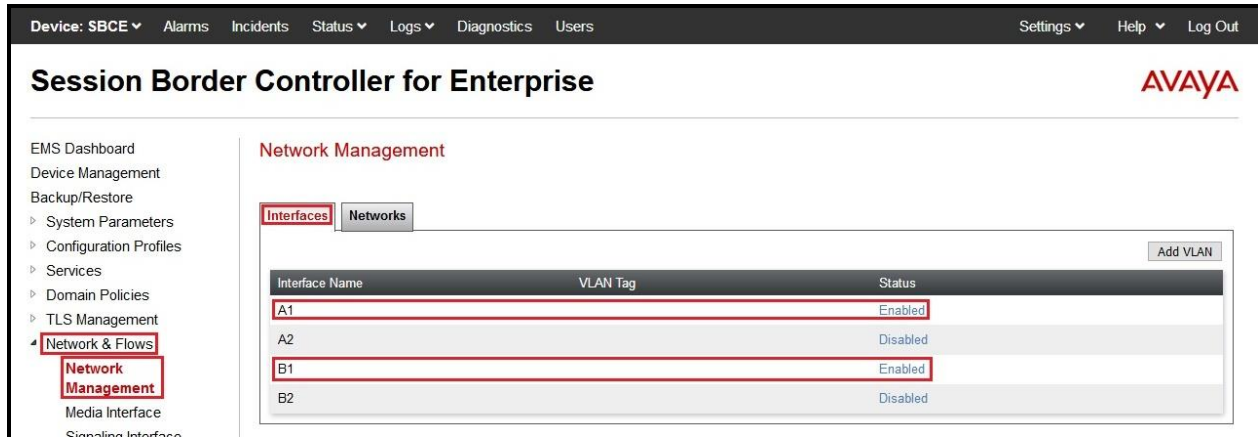
- Select **Networks** tab and click **Add** button to add a network for the outside interface as follows:
  - **Name:** Network\_B2
  - **Default Gateway:** 10.33.10.1
  - **Subnet Mask:** 255.255.255.0
  - **Interface:** B2 (This is the Avaya SBCE outside interface)
  - Click the **Add** button to add the **IP Address** for outside interface: 10.33.10.59
  - Click the **Finish** button to save the changes



**Figure 80: Network Management – Outside Interface**

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

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



**Figure 81: Network Management – Interface Status**

## 7.8.2. Create Media Interfaces

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

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

- Select the **Add** button and enter the following:
  - **Name:** **OutsideMedia**
  - **IP Address:** Select **Network\_B2 (B2, VLAN 0)** and **10.33.10.59** (External IP address toward Cox Communications)
  - **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)



**Figure 82: Media Interface**

### 7.8.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

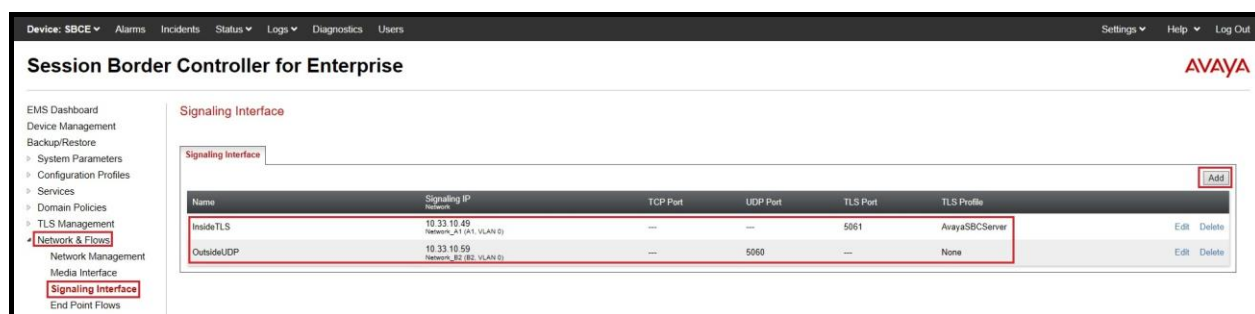
From the menu on the left-hand side, select **Network & Flows** → **Signaling Interface**

- Select the **Add** button and enter the following:
  - **Name:** **OutsideUDP**
  - **IP Address:** Select **Network\_B2 (B2, VLAN 0)** and **10.33.10.59** (External IP address toward Cox Communications)
  - **UDP Port:** **5060**
  - Click **Finish** (not shown)

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

- Select the **Add** button and enter the following:
  - **Name:** **InsideTLS**
  - **IP Address:** Select **Network\_A1 (A1, VLAN 0)** and **10.33.10.49** (Internal IP address toward Session Manager)
  - **TLS Port:** **5061**
  - **TLS Profile:** **AvayaSBCServer**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
  - Click **Finish** (not shown)

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



**Figure 83: Signaling Interface**

## 7.8.4. Configuration Server Flows

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

### 7.8.4.1 Create End Point Flows – SMVM Flow

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

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name: SMVM Flow**
  - **Server Configuration: SMVM** (see Section 7.4.1)
  - **URI Group: \***
  - **Transport: \***
  - **Remote Subnet: \***
  - **Received Interface: OutsideUDP** (see Section 7.8.3)
  - **Signaling Interface: InsideTLS** (see Section 7.8.3)
  - **Media Interface: InsideMedia** (see Section 7.8.2)
  - **Secondary Media Interface: None**
  - **End Point Policy Group: 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**

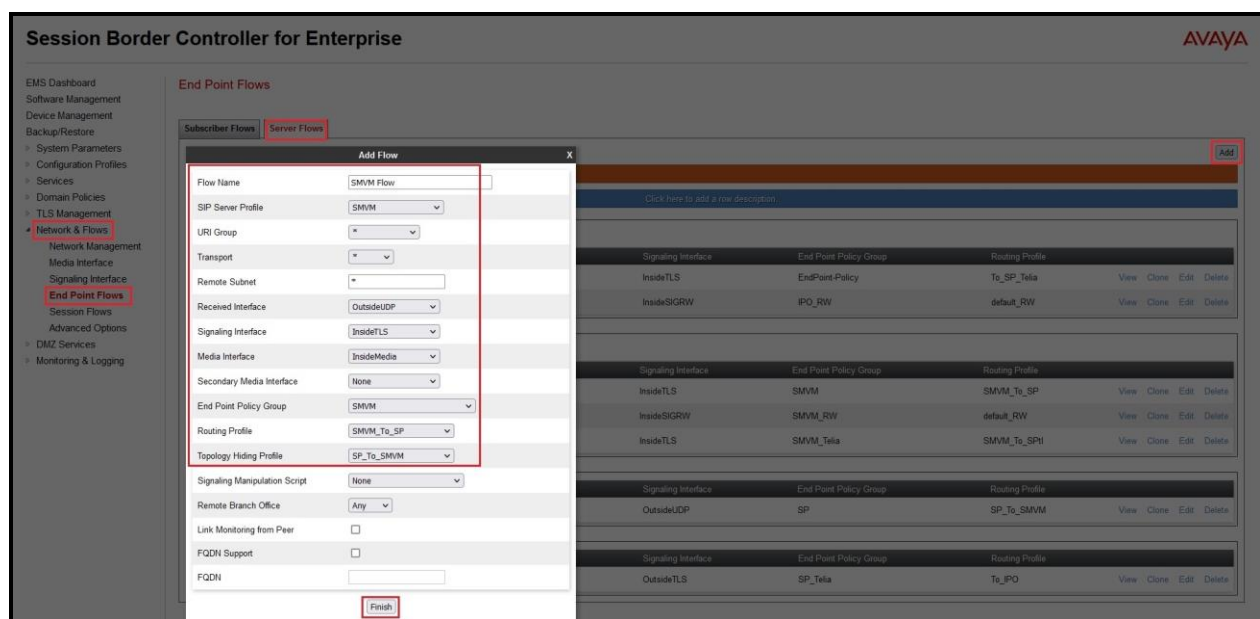


Figure 84: End Point Flow 1



### 7.8.4.2 Create End Point Flows – Cox Communications SIP Trunk Flow

From the menu on the left-hand side, select **Network & Flows** → **End Point Flows**  
There is a Server Flows associated to Cox Communications 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**

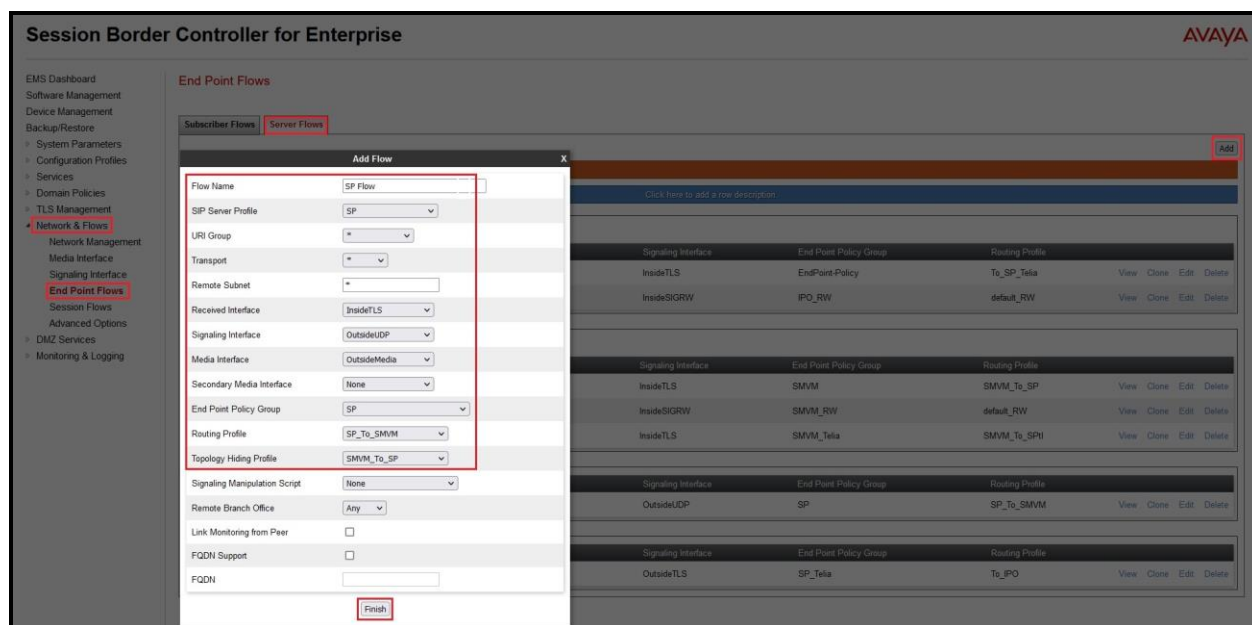


Figure 85: End Point Flow 2

## 8. Configure Avaya 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 call<sup>1</sup>.

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

---

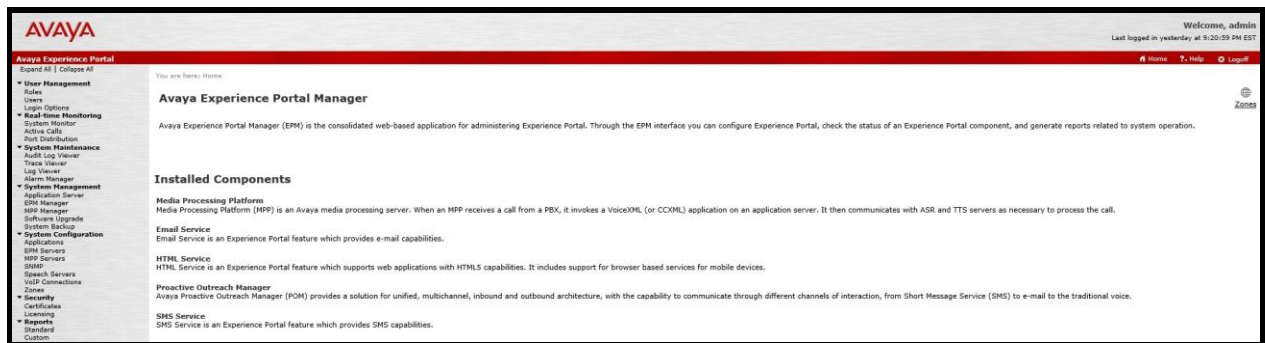
<sup>1</sup> An application may be configured with “inbound default” as the called number, to process all inbound calls that do not match any other application references.

## 8.2. Logging in and Licensing

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

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

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



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

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

**AVAYA**

**Avaya Experience Portal**  
Expand All | Collapse All

**User Management**  
Roles  
Users  
Login Options

**Real-time Monitoring**  
System Monitor  
Active Calls  
Port Distribution

**System Maintenance**  
Audit Log Viewer  
Trace Viewer  
Log Viewer  
Alarm Manager

**System Management**  
Application Server  
EPM Manager  
MPP Manager  
Software Upgrade  
System Backup

**System Configuration**  
Applications  
EPM Servers  
MPP Servers  
SNMP  
Speech Servers  
VoIP Connections  
Zones

**Security**  
Certificates  
**Licensing**

**Reports**  
Standard  
Custom  
Scheduled

**Multi-Media Configuration**  
Email  
HTML  
SMS

**POM**  
POM Home  
POM Monitor

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

## Licensing

This page displays the Experience Portal license information that is currently in effect. Experience Portal uses Avaya License Server Information

**License Server Information**

License Server URL:	https://10.33.1.10:52233/WebLM/LicenseServer
Last Updated:	Jan 28, 2021 4:33:55 AM EST
Last Successful Poll:	Jan 21, 2022 12:38:33 PM EST

**Licensed Products**

**Experience Portal**

Announcement Ports:	50
ASR Connections:	250
Call Anchoring Ports:	250
Email Units:	10
Enable Media Encryption:	250
Enhanced Call Classification:	250
Google ASR Connections:	250
Google Dialogflow Connections:	250
HTML Units:	250
SIP Signaling Connections:	50
SMS Units:	10
Telephony Ports:	50
TTS Connections:	250
Video Server Connections:	250
Zones:	10

Version: 8  
Last Successful Poll: Jan 21, 2022 12:38:33 PM EST  
Last Changed: Apr 11, 2021 11:03:26 PM EDT

**Proactive Outreach Manager**

EMAIL Channels:	0
External Selection:	0
Manual Agents:	0
Maximum Outbound Ports:	0
Predictive Agents:	0
Preview Agents:	0
SMS Channels:	0
Agent Web API Service:	0

Version: 3  
Expiration Date: Aug 3, 2021 12:00:00 AM EDT  
Last Successful Poll: Jan 21, 2022 12:38:33 PM EST  
Last Changed: Sep 2, 2021 12:02:42 AM EDT

**Allocations** **Help**

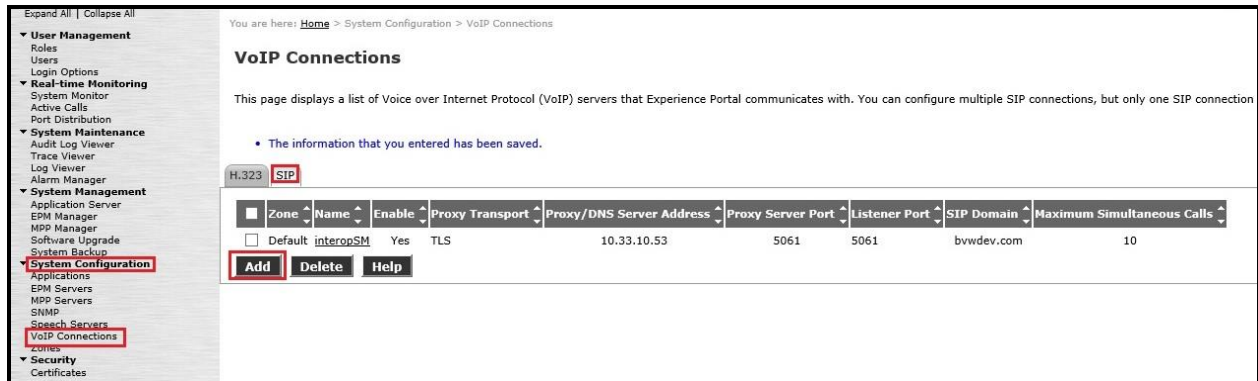
**Figure 87: Experience Portal – License**

### 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.



**Figure 88: 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 **bvwddev.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 ▼

Name: interopSM

Enable: ☒ Yes ☐ No

Proxy Transport: TLS ▼

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.33.10.53	5061	0	0	<span>Remove</span>

Additional Proxy Server

Listener Port: 5061

SIP Domain: bvwdev.com

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

☐ Configure number of inbound and outbound calls allowed

### SRTP

Enable: ☒ Yes ☐ No

Encryption Algorithm: ☒ AES\_CM\_128 ☐ NONE

Authentication Algorithm: ☒ HMAC\_SHA1\_80 ☐ HMAC\_SHA1\_32

RTCP Encryption Enabled: ☐ Yes ☒ No

RTP Authentication Enabled: ☒ Yes ☐ No

Add

### Configured SRTP List

SRTP-Yes,AES\_CM\_128,HMAC\_SHA1\_80,RTCP Encryption-No,RTP Authentication-Yes

Remove

Save Apply Cancel Help

Figure 89: Experience Portal – VoIP Connection 2

## 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

▼ User Management

Roles

Users

Login Options

▼ Real-time Monitoring

System Monitor

Active Calls

Port Distribution

▼ System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

▼ System Management

Application Server

EPM Manager

MPP Manager

Software Upgrade

System Backup

▼ System Configuration

Applications

EPM Servers

MPP Servers

SNMP

Speech Servers

VoIP Connections

Zones

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

### Speech Servers

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

ASR

TTS

<input type="checkbox"/>	Zone	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
<input type="checkbox"/>	Default	Nuance-ARS	Yes	10.33.1.61	Nuance	MRCP V2 TCP	5060	2	English(USA) en-US

Add

Delete

Customize

Help

Figure 90: Experience Portal – ASR Speech Server



TTS speech server:

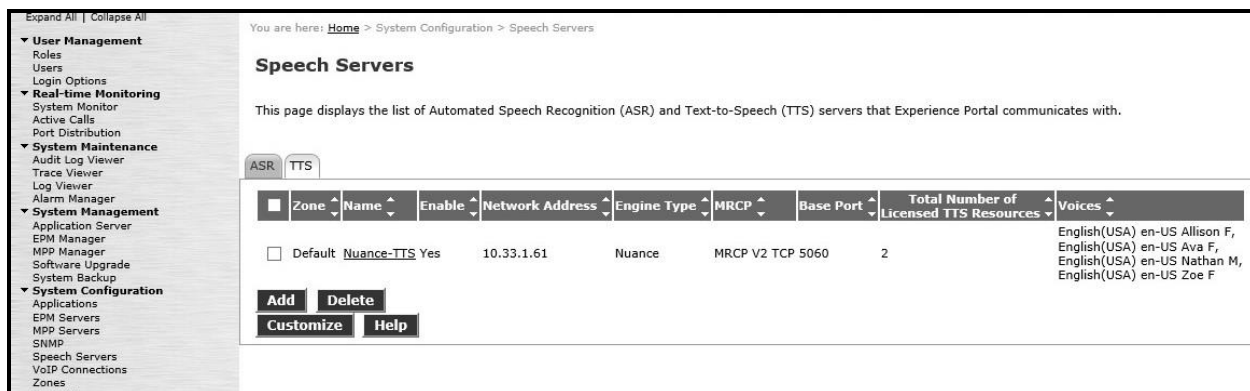


Figure 91: Experience Portal – TTS Speech Server

## 8.5. Application

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.33.1.23.

**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: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

## Change Application

Use this page to change the configuration of an application.

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

**URI**

☒ Single ☐ Fail Over ☐ Load Balance  
 VoiceXML URL:

Mutual Certificate Authentication: ☒ Yes ☐ No  
 Basic Authentication: ☐ Yes ☒ No

**ASR Speech Servers**

Engine Types:   
 Selected Engine Types:

**Nuance**

Languages:   
 Selected Languages:

Resources:   
 N Best List Length:   
 Speech Complete Timeout:  milliseconds  
 Speech Incomplete Timeout:  milliseconds  
 Vendor Parameters:

**TTS Speech Servers**

Voices:   
 Selected Voices:

**Application Launch**

☒ Inbound ☐ Inbound Default ☐ Outbound  
☒ Number ☐ Number Range ☐ URI  
 Called Number:

**Speech Parameters**

**Reporting Parameters**

**Advanced Parameters**

**Figure 92: Experience Portal – Application**

## 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

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

### MPP Servers

This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, it invokes

<input type="checkbox"/>	Zone	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/>	Default	mpp80	ep80.bvwdev.com	<Default>	<Default>	<Default>	10	Use MPP Settings

**Add** **Delete**

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

**Figure 93: 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

**▼ User Management**  
Roles  
Users  
Login Options

**▼ Real-time Monitoring**  
System Monitor  
Active Calls  
Port Distribution

**▼ System Maintenance**  
Audit Log Viewer  
Trace Viewer  
Log Viewer  
Alarm Manager

**▼ System Management**  
Application Server  
EPM Manager  
MPP Manager  
Software Upgrade  
System Backup

**▼ System Configuration**  
Applications  
EPM Servers  
MPP Servers  
SNMP  
Speech Servers  
VoIP Connections  
Zones

**▼ Security**  
Certificates  
Licensing

**▼ Reports**  
Standard  
Custom  
Scheduled

**▼ Multi-Media Configuration**  
Email  
HTML  
SMS

**▼ POM**  
POM Home  
POM Monitor

You are here: [Home](#) > [System Maintenance](#) > [System Monitor](#) > [mpp80 Details](#) > [Change MPP Server](#)

## Change MPP Server

Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels to Finest only when you are troubleshooting the system.

Zone: Default  
Name: mpp80  
Host Address: ep80.bvwdev.com  
Network Address (VoIP): <Default>  
Network Address (MRCP): <Default>  
Network Address (AppSvr): <Default>  
Maximum Simultaneous Calls: 10  
Restart Automatically: ☒ Yes ☐ No

### MPP Certificate

```
Owner: C=US, ST=CO, L=Thornton, O=AVAYA, OU=SIL, CN=ep80.bvwdev.com
Issuer: O=AVAYA, OU=MGMT, CN=SystemManager CA
Serial Number: 52301cea350940e3
Signature Algorithm: SHA256withRSA
Version: 3
Valid from: March 1, 2021 11:54:52 AM EST until March 1, 2023 11:54:52 AM EST
Certificate Fingerprints
MD5: b2:56:8c:12:72:64:14:54:21:9b:2c:6b:49:54:83:7c
SHA: e9:28:ef:c9:f8:27:e2:97:8b:46:4c:7b:98:f8:5d:8e:90:45:0e:a8
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
Key Usage:
Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Extended Key Usages:
Client Auth
Server Auth
Basic Constraints:
CA: false
Path Len Constraint: undefined
Subject Alternative Names
DNS Name: ep80
DNS Name: ep80.bvwdev.com
IP Address: 10.33.1.23
```

Categories and Trace Levels ▶

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

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

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

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

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

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

## VoIP Settings

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

**Port Ranges** ▾

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

**RTCP Monitor Settings** ▾

Host Address:

Port:

**VoIP Audio Formats** ▾

MPP Native Format:

**Codecs** ▾

**Offer**

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

Packet Time:  milliseconds

G729 Discontinuous Transmission: ☐ Yes ☒ No

**Answer**

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

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☒ Yes ☐ No

**QoS Parameters** ▸

**Out of Service Threshold (% of VoIP Resources)** ▸

**Call Progress** ▸

**Miscellaneous** ▸

Figure 95: 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.  
`<parameter name="mpp.sip.rfc2833.payload">101</parameter>`
- In the verification of these Application Notes, the line was added directly above the line where the sip.session.expires parameter is configured.

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

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

Expand All | Collapse All

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

### MPP Manager (Jan 21, 2022 1:31:59 PM EST)

This page displays the current state of each MPP in the Experience Portal system. To enable the state and

Last Poll: Jan 21, 2022 1:31:39 PM EST

Zone	Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
						Today	Recurring	In	Out
<input type="checkbox"/>	Default mpp80	Online	Running	OK	Yes	No	None	0	0

State Commands

Mode Commands

Restart/Reboot Options

☒ One server at a time  
☐ All servers

Figure 96: Experience Portal – MPP Manager

## 9. Cox Communications SIP Trunk Configuration

Cox Communications is responsible for the configuration of Cox Communications SIP Trunk Service. Cox Communications will provide the Cox Managed CPE to the customer when the customer orders the Cox Communications SIP trunk service. Cox Communications will be responsible for managing the Cox Managed CPE. Customer must provide the IP Address used to reach the Avaya SBCE public interface at the enterprise. Cox Communications will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Cox Managed CPE. Cox Communications also provides the Cox Communications 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 Cox Communications SIP Trunk and the enterprise is a static IP Address configuration.

## 10. Verification Steps

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

Verification Steps:

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

## Troubleshooting:

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

## 11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura<sup>®</sup> Communication Manager 10.1, Avaya Aura<sup>®</sup> System Manager 10.1, Avaya Aura<sup>®</sup> Session Manager 10.1, Avaya Experience Portal 8.1 and Avaya Session Border Controller 10.1 to Cox Communications. 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:  
<http://support.avaya.com/>

### **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**

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

### **Avaya Experience Portal**

- [5] *Administering 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] *Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 8.1 on the Avaya Aura® Platform, 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 Cox Communications SIP Trunking may be found at:  
<http://www.cox.com>

## 13. Appendix A - 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["P-Asserted-Identity"][1].URI.USER.regex_replace("(\\+)", "");
        %HEADERS["Contact"][1].URI.USER.regex_replace("(\\+)", "");
        %HEADERS["Diversion"][1].URI.USER.regex_replace("(\\+)", "");
        %HEADERS["From"][1].URI.USER.regex_replace("(\\+)", "");

        //Modify user of SIP URI in PAI header on Call Forward Off-net
        if (%HEADERS["Diversion"][1].regex_match("reason")) then
        {
            %HEADERS["P-Asserted-Identity"][1].URI.USER =
%HEADERS["Diversion"][1].URI.USER;
        }

// 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]);
    }
}
```

## 14. Appendix B - Cox Managed CPE Configuration

The Cox Managed CPE is configured to manage all SIP signaling and provides voice quality management. All data traffic also traverses the Cox Managed CPE. It is part of the Cox Communications SIP trunk service and Cox Communications will provide it to the customer when the customer orders the Cox Communications SIP trunk service. Cox Communications manages it and the end-customer does not manage.

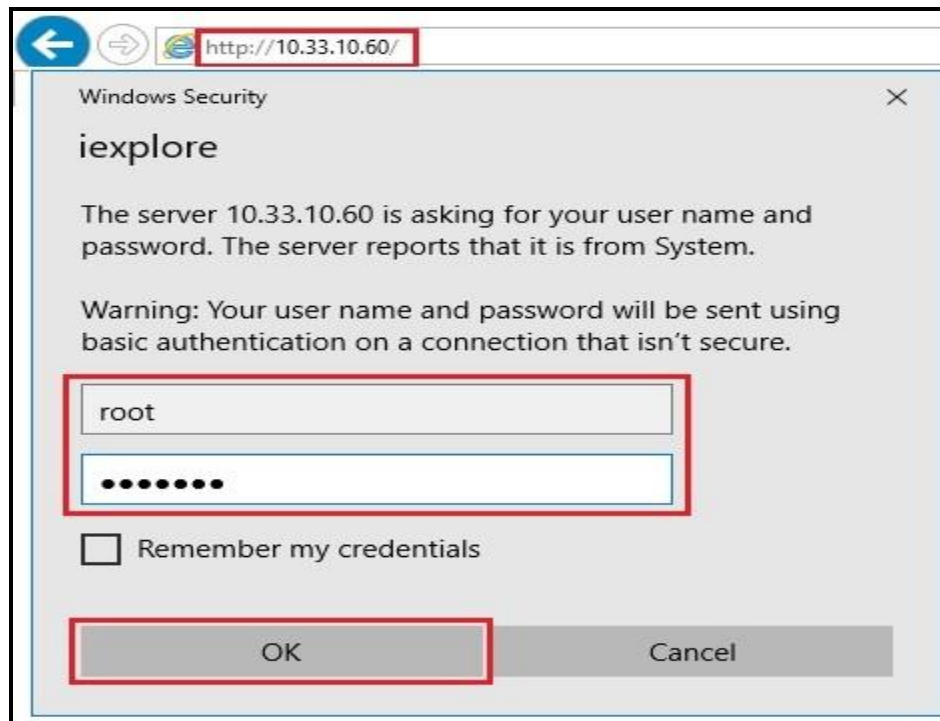
**Note: Cox Managed CPE is part of Cox Communications SIP trunk service offering and it is Cox Communications's responsibility for all the aspect of the Cox Managed CPE (i.e. support, detail configuration, maintenance, etc.). The Cox Managed CPE's sample configuration included in this document is used during this compliance testing.**

### 14.1. Cox Managed CPE Login

The Cox Managed CPE was configured with a local LAN IP Address of 10.33.10.60 and a subnet mask of 255.255.255.0. A personal computer is configured with Ethernet IP Address assigned to any IP Address other than 10.33.10.60 in the same subnet mask, for example 10.33.10.62


Launch a web browser on personal computer and enter the following URL: <http://10.33.10.60> and hit enter.

The following login window should appear:



**Figure 99 – Cox Managed CPE Login**

- Enter **User Name** and **Password** field
- Click **OK** and the Configuration Menu page should be appeared next


Admin
Help

### Configuration Menu

- Admin
  - [Encryption Key](#)
  - [Backup / Restore](#)
  - [Upgrade Firmware](#)
  - [RADIUS Settings](#)
  - [TACACS+ Settings](#)
  - [Services Configuration](#)
  - [System Information](#)
  - [System Analysis](#)
  - [Time Settings](#)
  - [User Commands](#)
  - [File Download](#)
  - [File Server](#)
  - [SD Card](#)
  - [Reboot System](#)
- + Network
- + Users
- + Security
  - [SD-WAN](#)
- + VoIP
- + VPN
- [GRE](#)

**Software Version:**  
Version 15.8.2 -- Mon Nov 30 10:27:36 PST 2020

---

**Hostname:**  
2900E

---

**Model:**  
EdgeMarc 2900E with IPv6 support

---

**Vendor:**  
Ribbon

---

**LAN Interface MAC Address:**  
54:39:68:12:7D:00

---

**Registration Status:**  
The ALG feature is registered. View [license key](#).

---

**System:**  
Date : 07/14/2023 03:18:17 UTC  
Erase Button : Enabled

---

**Change Administrative Password:**  
The password of the read-write administrative user can be [changed](#).

---

**Change Read-Only Password:**  
The password of the read-only user can be [changed](#).

**Figure 100 – Cox Managed CPE – Configuration Menu**


## 14.2. Network Configuration

From the **Configuration Menu**, select **Network** option.

Under Network, input the public and private networks as followings:

- LAN Interface Settings:
  - **IP Address: 10.33.10.60** (Cox Managed CPE LAN interface IP address)
  - **Subnet Mask: 255.255.255.0**
  - Check **Enable VLAN Support**
  - **Default VLAN ID: 1**
- WAN Interface IPv4 Settings:
  - Check **Static IP**
  - **IP Address: 192.168.80.103** (Cox Managed CPE WAN interface IP address)
  - **Subnet Mask: 255.255.255.128**
- Network Settings:
  - **Default Gateway: 192.168.80.1**

Submit the changes.


Help

## Network

Networking configuration information for the public and private networks.

### Configuration Menu

- + Admin
- **Network**
  - + NAT
  - + VLAN
  - + WAN VLAN
  - + 802.1X Supplicant
  - + High Availability
  - + DHCP Relay
  - + DHCP Server
  - + Traffic Shaper
  - + Pass-Through Rules
  - + Subinterfaces
  - + Proxy ARP
  - + Switch Ports
  - + Static Routes
  - + Dynamic DNS
  - + Network Information
  - + Network Restart
  - + Network Test Tools
  - + WAN Failover
  - + Router Advertisement
  - + IP Multicast
- + Users
- + Security
- + SD-WAN
- + VoIP
- + VPN
- + GRE

### LAN Interface Settings:

IP Address:

Subnet Mask:

IPv6 Address/Prefix:

Enable VLAN support ☒

Default VLAN ID:

[VLAN Configuration](#)

---

### WAN Interface IPv6 Settings:

Select the type of IPv6 WAN Interface to use:

☒ Disabled  
☐ DHCP  
☐ Static IP (ethernet)  
☐ IPv6 in IPv4 Tunnel  
☐ VLAN

---

### WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:

☐ Disabled  
☐ PPPoE  
☐ DHCP  
☒ Static IP  
☐ VLAN

IP Address:

Subnet Mask:

---

### Network Settings:

Default Gateway:

---

### DNS servers:

Note: In case of dynamic links, if the manual override checkbox is not checked the address provided will be used.

Manually set DNS: ☒

Primary DNS Server:

Secondary DNS Server:

**Figure 101 – Cox Managed CPE - Network Configuration**

## 14.3. VLAN Configuration

There is a VLAN which has been created and configured as shown in capture below. Details how to create the VLAN is not shown.

**Configuration Menu**

- + Admin
- Network
- + NAT
- VLAN
- + WAN VLAN
- + 802.1X Supplicant
- + High Availability
- + DHCP Relay
- + DHCP Server
- + Traffic Shaper
- + Pass-Through Rules
- + Subinterfaces
- + Proxy ARP
- + Switch Ports
- + Static Routes
- + Dynamic DNS
- + Network Information
- + Network Restart
- + Network Test Tools
- + WAN Failover
- + Router Advertisement
- + IP Multicast
- + Users
- + Security
- + SD-WAN
- + VoIP
- + VPN
- + GRE

**VLAN Configuration**

VLAN Configuration allows the user to configure VLAN support.  
Note - Changes to this page may require additional changes to the 'VLAN Membership' and 'VLAN Port' pages.

| [Create/Edit VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN Configuration								
Select: <a href="#">All</a> <a href="#">None</a> <a href="#">Delete</a>								
	VLAN ID	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Prefix	Virtual IPv4 Address	Virtual IPv6 Address	Isolate VLAN
<input type="checkbox"/>	1	10.33.10.60	255.255.255.0					N

**Create a new VLAN**

Action: [Add new VLAN](#)

VLAN ID:

IPv4 Address:

Subnet Mask:

IPv6 Address:

IPv6 Prefix:

Addresses for [High Availability](#)

Virtual IPv4 Address:

Virtual IPv6 Address:

Isolate VLAN from other VLANs ☐

[Add](#) [Reset](#)

Figure 102 – Cox Managed CPE - VLAN Configuration



## 14.4. VoIP SIP Settings

From the **Configuration Menu**, select **VoIP** menu option → **SIP** option.

Under **SIP Settings**, input the parameters as followings:

- **SIP Server Address:** Cox Communications provided this information
- **SIP Server Port:** 5060
- **SIP Server Transport:** Select **Pass Through**
- Check **Use Custom Domain**
- **SIP Server Domain:** Cox Communications provided this information

Submit the changes.

**ribbon** **SIP Settings** [Help](#)

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Address:	DUKEBWSSCM-MTC1-SA-XXXX.TC.AT.COX.NET
SIP Server Port:	5060
SIP Server Transport	Pass Through ▼
Exclude sips headers for TLS Transport	<input type="checkbox"/>
Use Custom Domain:	<input checked="" type="checkbox"/>
SIP Server Domain:	rd.xxx.cox.net

List of SIP Servers: [Create](#)

Enable Multi-homed Outbound Proxy Mode:	<input type="checkbox"/>
Enable Transparent Proxy Mode:	<input type="checkbox"/>
Limit Outbound to listed SIP Servers:	<input checked="" type="checkbox"/>
Limit Inbound to listed SIP Servers:	<input checked="" type="checkbox"/>
Include UPDATE In Allow:	<input checked="" type="checkbox"/>
PRACK Support:	<input checked="" type="checkbox"/>

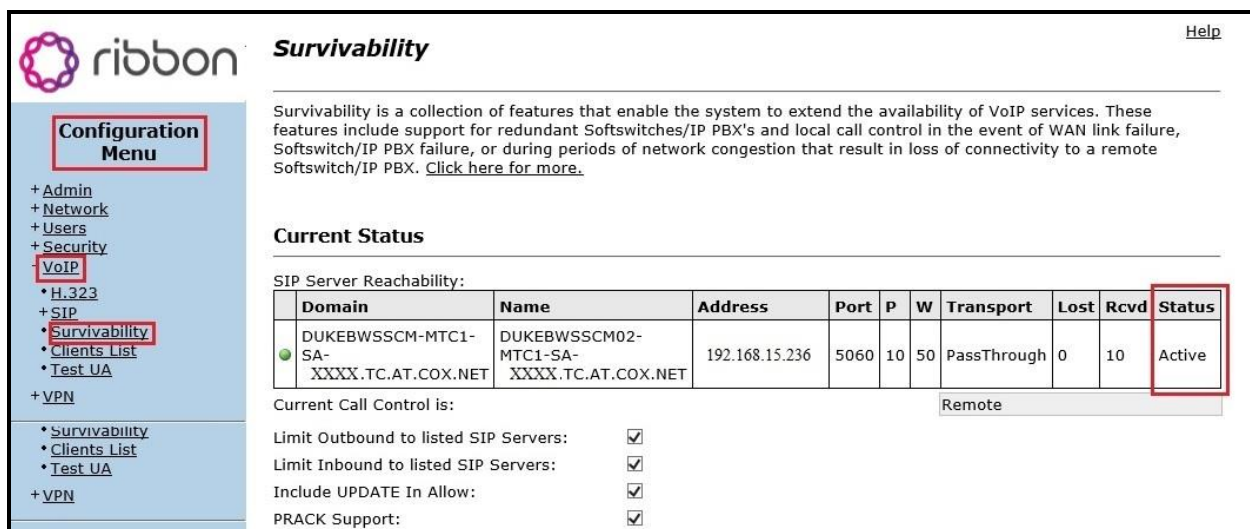
**Configuration Menu**

- + Admin
- + Network
- + Users
- + Security
- + **VoIP**
  - H.323
  - **SIP**
    - ALG
    - B2BUA
    - SIP Routing
    - Media Server
  - Survivability
  - Clients List
  - Test UA
- + VPN

Figure 103 – Cox Managed CPE - VoIP SIP Settings

## 14.5. VoIP Survivability

From the **Configuration Menu**, select **VoIP → Survivability** to check SIP Server Reachability status. When the SIP Server connectivity is up, the status is **Active**.



The screenshot shows the Ribbon Survivability configuration page. On the left is a Configuration Menu with options like Admin, Network, Users, Security, VoIP, SIP, Survivability, Clients List, Test UA, and VPN. The main content area is titled 'Survivability' and includes a description of the feature set. Below this is a 'Current Status' section with a table for SIP Server Reachability. The table has columns for Domain, Name, Address, Port, P, W, Transport, Lost, Rcvd, and Status. A single entry is shown with a green status icon and the status 'Active'. Below the table, there are checkboxes for various call control settings, all of which are checked.

**Configuration Menu**

- + Admin
- + Network
- + Users
- + Security
- + **VoIP**
  - H.323
  - + SIP
  - **Survivability**
  - Clients List
  - Test UA
- + VPN
  - Survivability
  - Clients List
  - Test UA

**Survivability**

Survivability is a collection of features that enable the system to extend the availability of VoIP services. These features include support for redundant Softswitches/IP PBX's and local call control in the event of WAN link failure, Softswitch/IP PBX failure, or during periods of network congestion that result in loss of connectivity to a remote Softswitch/IP PBX. [Click here for more.](#)

**Current Status**

SIP Server Reachability:

Domain	Name	Address	Port	P	W	Transport	Lost	Rcvd	Status
DUKEBWSSCM-MTC1-SA-XXXX.TC.AT.COX.NET	DUKEBWSSCM02-MTC1-SA-XXXX.TC.AT.COX.NET	192.168.15.236	5060	10	50	PassThrough	0	10	Active

Current Call Control is:

Limit Outbound to listed SIP Servers: ☒

Limit Inbound to listed SIP Servers: ☒

Include UPDATE In Allow: ☒

PRACK Support: ☒

Remote

**Figure 104 – Cox Managed CPE - SIP Server Survivability**

## 14.6. ALG Trunking Configuration

From the **Configuration Menu**, select **VoIP → SIP → ALG** option.

Under **SIP Trunking Devices**, add a trunking device as followings:

- **Action:** choose **Add new trunking device**
- **Name:** **Avaya Aura**
- **Address:** **10.33.10.59** (Avaya SBCE public interface IP address)
- **Port:** **5060**

Select **Commit** button

**Configuration Menu**

- + Admin
- + Network
- + Users
- + Security
- + SD-WAN
- + **VoIP**
  - + H.323
  - + **SIP**
    - + **ALG**
    - + B2BUA
    - + Trunking Group
    - + Availability
    - + Media Server
  - + Survivability
  - + Clients List
  - + Test UA
- + VPN
- + GRE

### ALG Trunking Configuration

Configuration of SIP trunking devices.

#### SIP Trunking devices

A SIP trunking device can be a PSTN gateway, or similar device, that does not issue REGISTER messages. Calls will be forwarded to the device based on the dial-plan rules below.

If VLANS are enabled, the SIP trunking device needs to be in the same VLAN as defined in the VoIP ALG page.

SIP Trunking Devices				
Select: <a href="#">All</a> <a href="#">None</a> <a href="#">Delete</a>				
	Address	Port	Name	Group
<input type="checkbox"/>	10.33.10.59	5060	Avaya Aura	

#### Add a trunking device

Action: [Add new trunking device](#)

Name:

Address:

Port:

[Commit](#) [Reset](#)

Figure 105 – Cox Managed CPE - SIP ALG Trunk Configuration

The following captured screens show the rest of the ALG Trunking Configuration page, continue from above screen. Detail configuration is not discussed here.

## Header Transformation

These header transformation rules are applied to all SIP trunking devices. They define how specified SIP headers should be transformed when forwarding to the SIP Server.

### From Header

Select the domain to use in From header when sending requests to the SIP Server:

☒ SIP Server Address (default)
   
☐ System WAN IP

## Rules

Rules are used to forward and/or modify incoming and outgoing calls. There are 3 types of rules:

- Inbound: from server to trunking device
- Outbound: from trunking device to server
- Redirect: from local phone to trunking device (w/o routing to server)

Outbound rules can match against and/or modify either the calling or called number. Inbound and redirect rules operate on the called number only. Stripped and added digits always apply to the left-most digits of the DID.

Dial Rules								
Select: <a href="#">All</a> <a href="#">None</a>								<input type="button" value="Delete"/>
	Type	Mode	Party	PRIO	Pattern-match	Strip	Add	Trunking device
<input type="checkbox"/>	Inbound	BothModes			Default Rule			Avaya Aura (10.33.10.59:5060)

### Add a rule

Action:

Type:

Mode:

Call Party:

Default rule: ☐

Priority: ☐

Pattern-match (if not default):

Strip digits:

Add string:

Trunking device:

Note: "Use SIP proxy as secondary target" rule can be configured on the B2BUA page

**Figure 106 – Cox Managed CPE - Header Transformation and Rules**

## 14.7. Trunking Group Configuration

From the **Configuration Menu**, select **VoIP → SIP → Trunking Group** option. A new SIP Routing was created as below screenshot.

The screenshot displays the 'Trunking Group Availability' configuration page in the Ribbon interface. On the left, the 'Configuration Menu' is visible, with 'VoIP', 'SIP', and 'Trunking Group' highlighted. The main content area is titled 'Create New Routing Group'. It includes a 'Name' input field and a 'Select group members:' section. Below this is a table with two columns: 'Name' and 'Address'. A single member, 'Avaya Aura', is listed with the address '10.33.10.59'. A 'Create' button is located below the table. At the bottom, there is a section for 'Existing Routing Groups'.

Name	Address
Avaya Aura	10.33.10.59

Figure 107 – Cox Managed CPE – SIP Routing Configuration

---

**©2023 Avaya Inc. All Rights Reserved.**

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

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