Avaya Solution & Interoperability Test Lab

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

Abstract

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

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Bell Canada is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

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

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Bell Canada 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 Bell Canada SIP Trunk Service did not include use of any specific encryption features as requested by Bell Canada.

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

2.1. Interoperability Compliance Testing

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

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

The following was not supported:

- Bell Canada does not support TLS/SRTP SIP Transport
- Bell Canada does not support Registration
- The inbound toll-free call is supported but was not available for testing during the compliance test

2.2. Test Results

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

- **OPTIONS from Bell Canada** – Bell Canada was configured to send SIP OPTIONS messages with Max-Forwards header with value equal to 0. This was by design from Bell Canada. Avaya SBCE responded correctly with 483 Too Many Hops. However, Bell Canada would accept this and keep the trunk up
- **Multiple "481 Call Leg/Transaction Does Not Exist" SIP messages are generated for transfer/ conference scenarios** - This is essentially a race condition. For example, after the REFER for a transfer is sent, both parties send a BYE for the call leg going away. When Avaya receives another BYE from Service Provider, it responds with a "481 Call Leg/Transaction Does Not Exist" (since each party has already sent its own BYE for that call leg). The transferred call was not impacted and still worked well

2.3. Support

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

For technical support on Bell Canada SIP Trunking, contact Bell Canada at https://business.bell.ca/shop/enterprise/sip-trunking-service

3. Reference Configuration

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

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

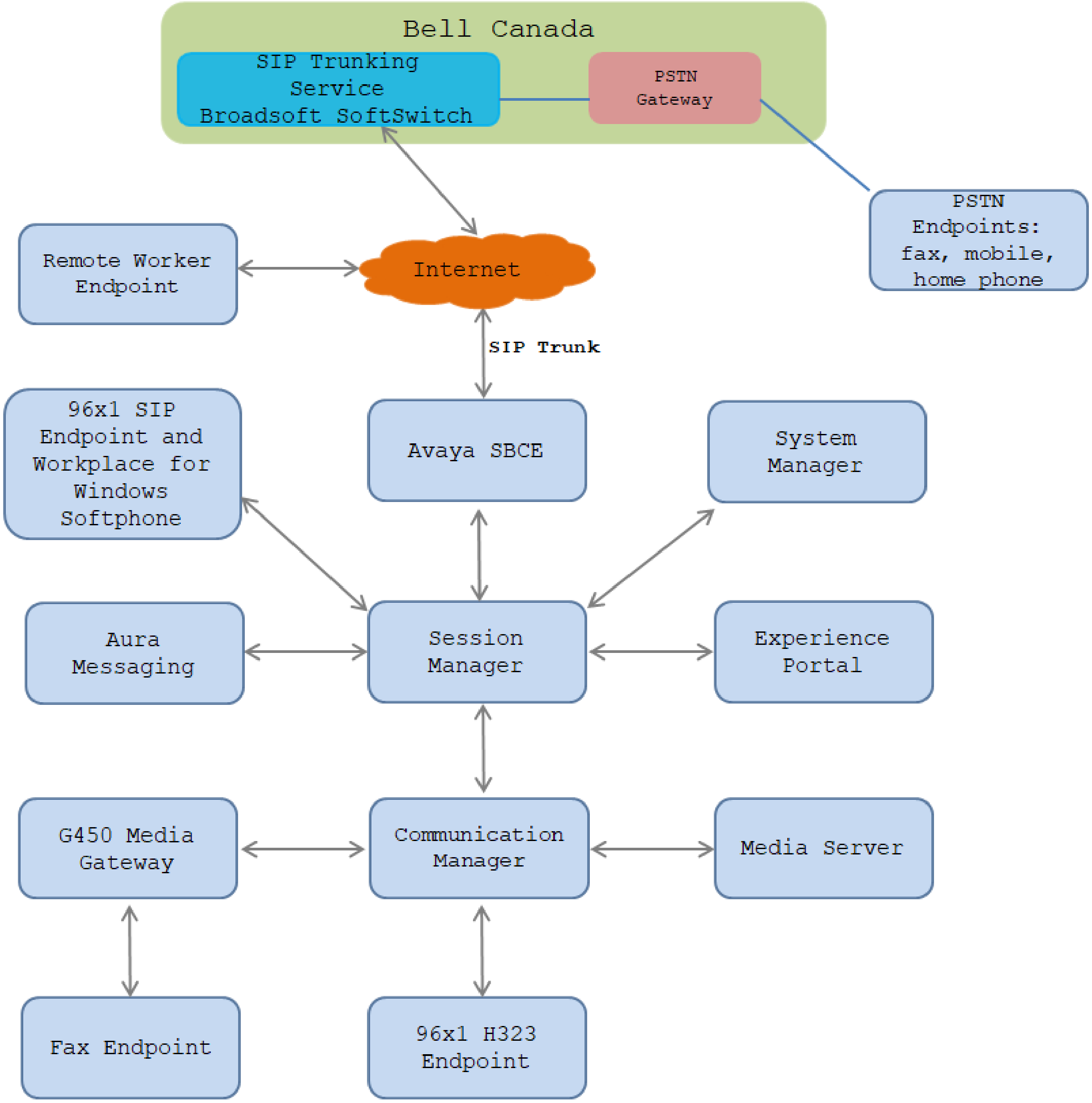


Figure 1: Avaya IP Telephony Network and Bell Canada SIP Trunk

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	**Release/Version**
Avaya Aura® Communication Manager running on Virtualized Environment	R018x.01.0.890.0 8.1.2.0.0.890.26095
Avaya Aura® Session Manager running on Virtualized Environment	8.1.2.0.812039
Avaya Aura® System Manager running on Virtualized Environment	8.1.2.0 Software Update Revision No: 8.1.2.0.0611097
Avaya Aura® Messaging running on Virtualized Environment	7.1.0.0.532.0
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.169 A6
Avaya Session Border Controller for Enterprise running on Virtualized Environment	8.1.0.0-18490
Avaya Aura® Experience Portal running on Virtualized Environment	7.2.2
Avaya G450 Media Gateway	41.16.0
Avaya 96x1 IP Deskphone (SIP)	7.1.9
Avaya 96x1 IP Deskphone (H.323)	6.8.2
Avaya Digital Deskphone (1408D)	R48
Avaya Workplace Client for Windows	3.8.5
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.23-SP12P13
Avaya Analog Deskphone	N/A
BELL CANADA SIP Trunk Components	
Equipment/Software	**Release/Version**
Acme Packet Net-Net SBC	SCZ7.4.0 MR-2 GA (Build 446)
Broadsoft SoftSwitch	R22.0

Table 1: Equipment and Software Tested

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

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

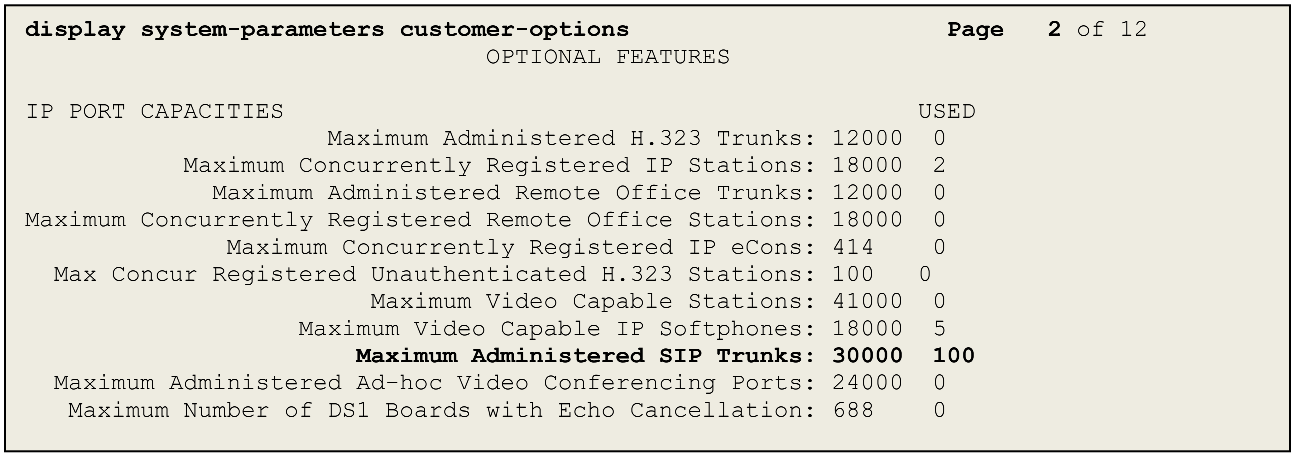
5. Configure Avaya Aura® Communication Manager

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

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

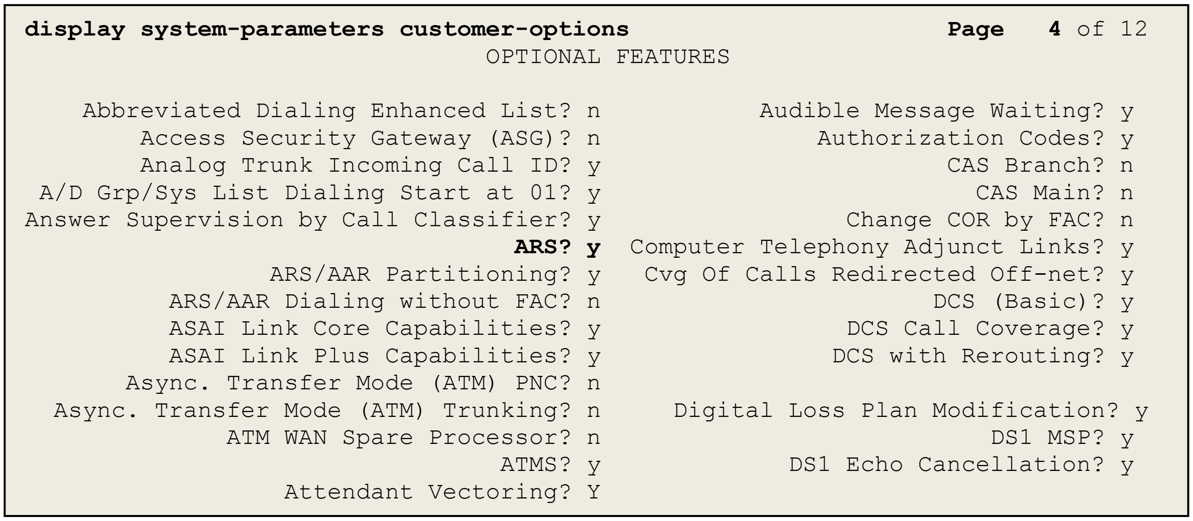
5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 30000 SIP trunks are available and 100 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.



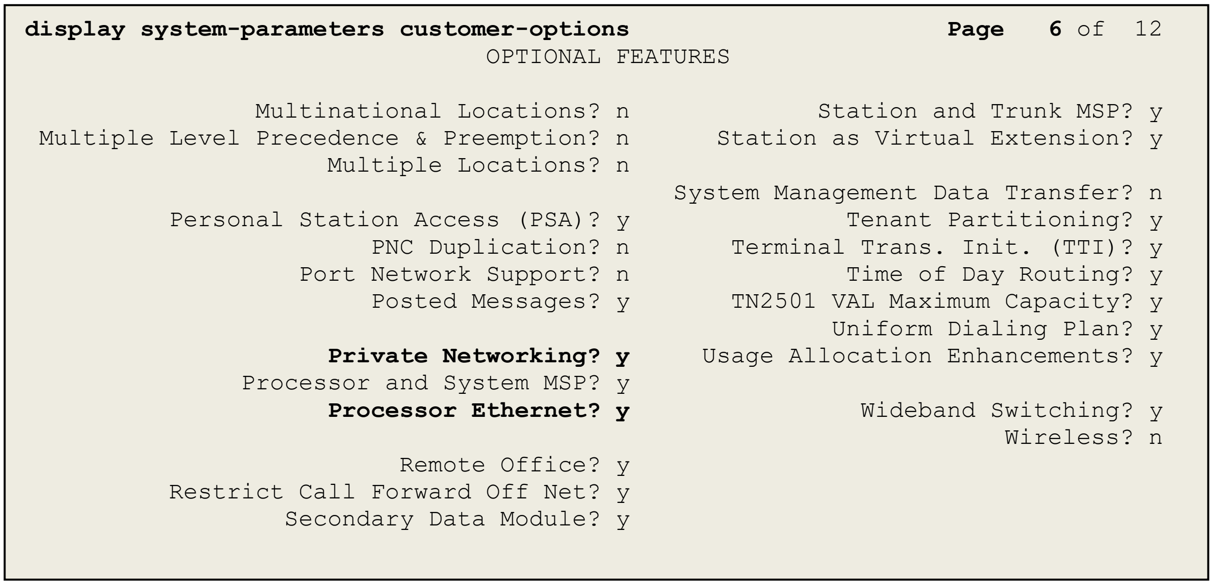
```
display system-parameters customer-options                      Page   2 of 12
                                OPTIONAL FEATURES

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

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
                                  ARS? y  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
  Async. Transfer Mode (ATM) Trunking? n     Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? Y
```

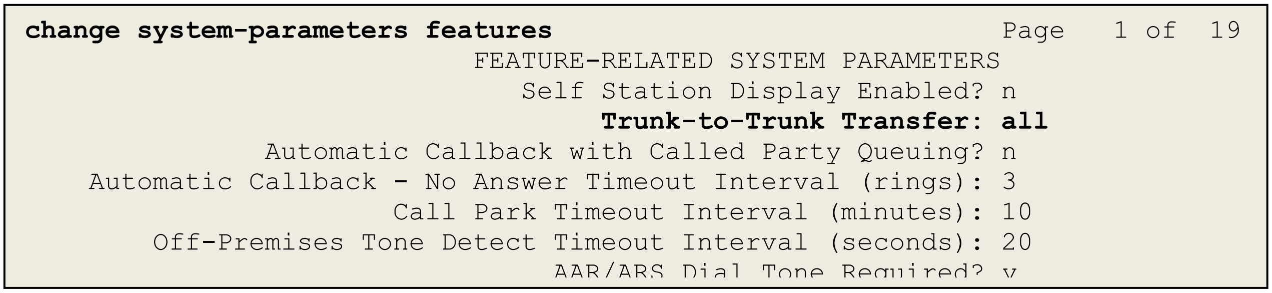
On **Page 6**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.



```
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? y
                        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
                                                        Uniform Dialing Plan? y
                     Private Networking? y     Usage Allocation Enhancements? y
               Processor and System MSP? y
                     Processor Ethernet? y                Wideband Switching? y
                                                                    Wireless? n

                          Remote Office? y
          Restrict Call Forward Off Net? y
                  Secondary Data Module? y
```

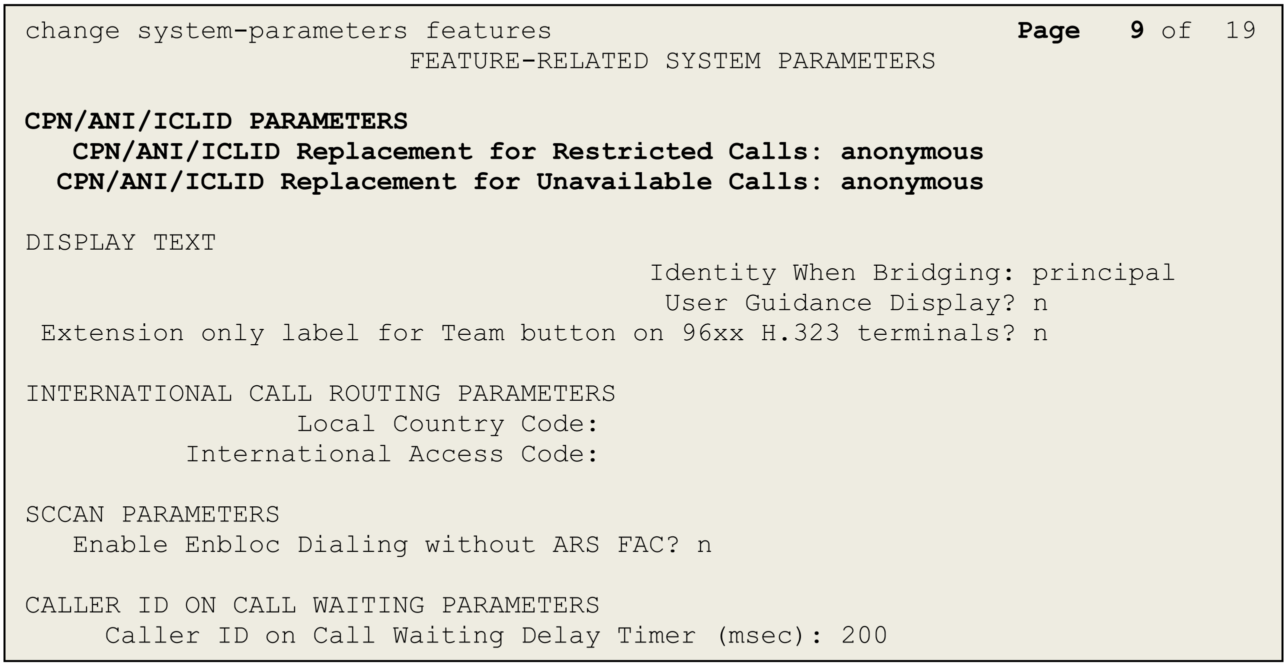
5.2. System Features

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
```

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
```

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**: **AMS1**, **IP Address**: **10.33.1.30**
- Session Manager: **Name**: **interopASM**, **IP Address**: **10.33.1.12**
- Communication Manager: **Name**: **procr**, **IP Address**: **10.33.1.6**

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
AMS1                10.33.1.30
CMS19               10.33.1.18
interopASM          10.33.1.12
loopback            10.33.1.6
lsp                 10.33.1.7
procr               10.33.1.6
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. In the compliance test, **ip-codec-set 1** was used for this purpose. Bell Canada supports the **G.711MU**, and **G.729A** codecs. Default values can be used for all other fields.

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

                          IP CODEC SET

    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU        n            2        20
 2: G.729A         n            2        20


Media Encryption                          Encryption SRCTP: enfore-unenc-
srtcp
```

On **Page 2**, set the **FAX Mode** to **t.38-standard**. Bell Canada supports Fax using T.38.

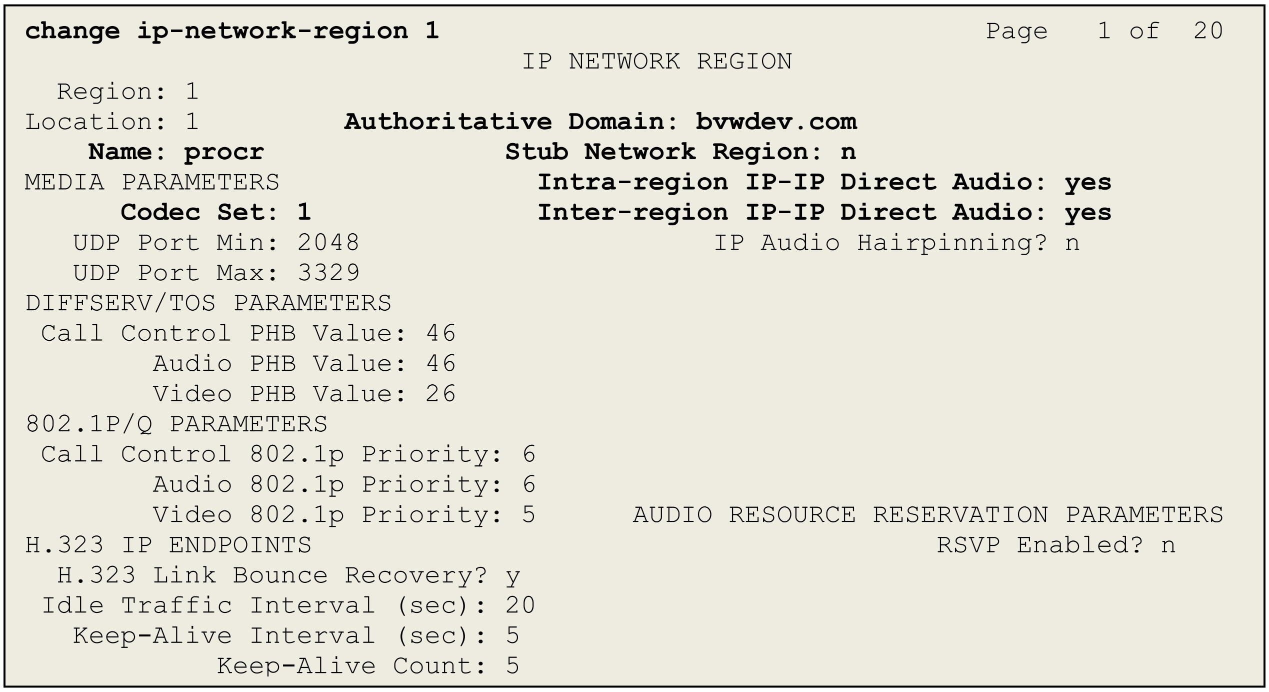
```
change ip-codec-set 1                                          Page   2 of   2

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n



                         Mode                Redundancy              Packet
Size(ms)
    FAX                  t.38-standard        0        ECM: y
    Modem                off                  0
    TDD/TTY              US                   3
```

5.5. IP Network Region for Media Gateway, Media Server

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

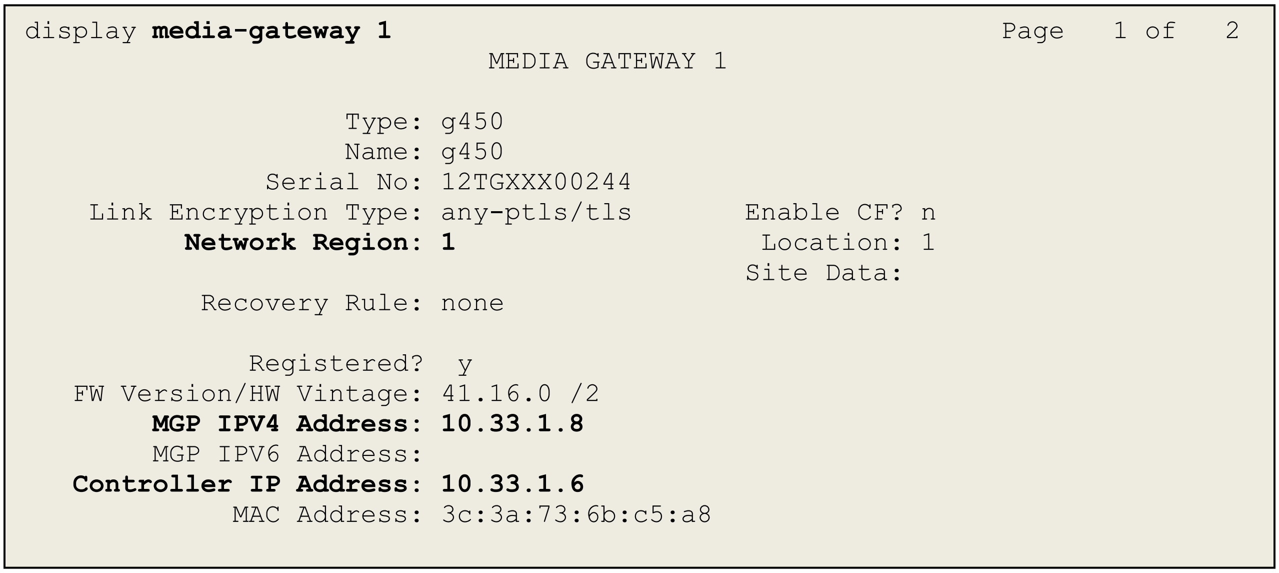
Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

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



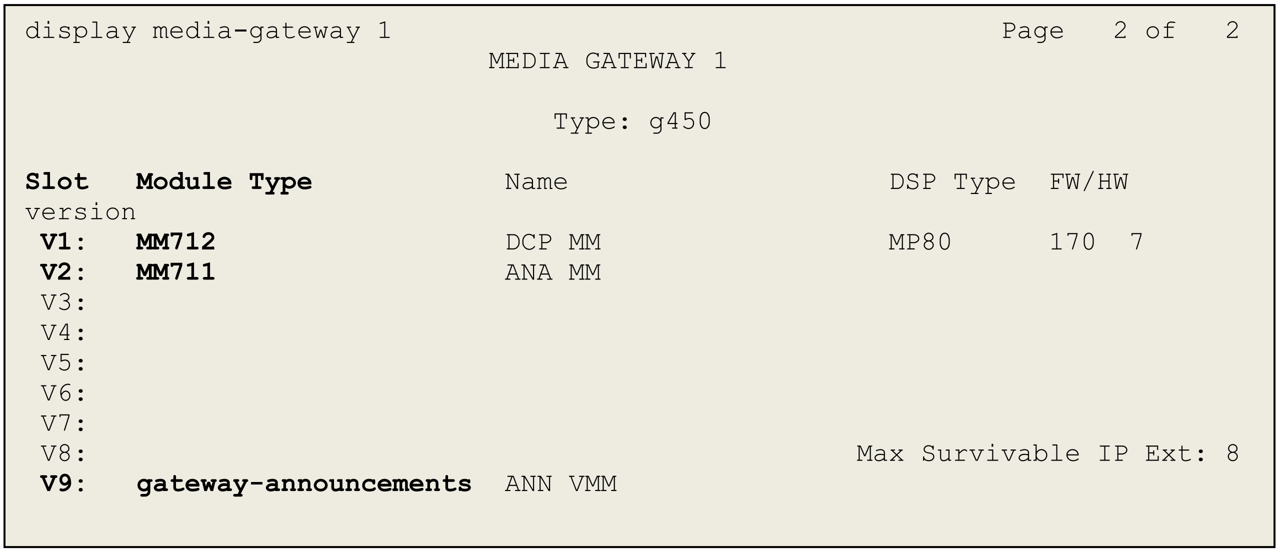
```
change ip-network-region 1                                  Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1          Authoritative Domain: bvwdev.com
    Name: procr               Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct 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
```

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 (**10.33.1.6**), and that the gateway **MGP IPv4 Address** is **10.33.1.8**. These fields are not configured in this screen, but just display the current information for the Media Gateway.



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

                    Type: g450
                    Name: g450
               Serial No: 12TGXXX00244
    Link Encryption Type: any-ptls/tls       Enable CF? n
          Network Region: 1                   Location: 1
                                             Site Data:
           Recovery Rule: none

              Registered?  y
   FW Version/HW Vintage: 41.16.0 /2
        MGP IPV4 Address: 10.33.1.8
        MGP IPV6 Address:
   Controller IP Address: 10.33.1.6
             MAC Address: 3c:3a:73:6b:c5:a8
```

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:                                                Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```

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: AMS1** (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: 2
         Voip Channel License Limit: 80
    Dedicated Voip Channel Licenses: 80

                          Node Name: AMS1
                     Network Region: 1
                           Location: 1
          Announcement Storage Area: ANNC-79def0aa-5f11-41e5-bc70--
000c29189c28
```

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**.

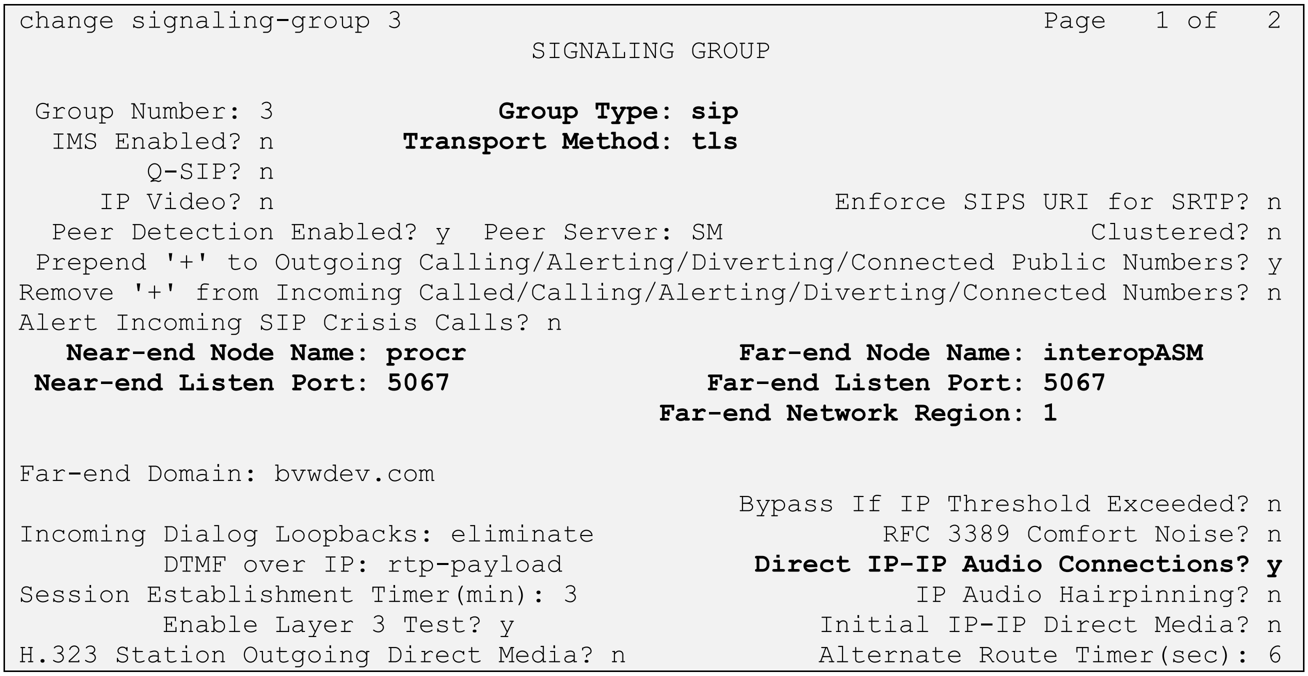
```
change ip-interface procr
                                  IP INTERFACES

                  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: 10.33.1.6
           Subnet Mask: /24
```

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. For the compliance test, signaling group **3** was used for both outbound and inbound calls between the service provider and the enterprise. It was configured using the parameters highlighted below. Note: The signaling group between Communication Manager and Session Manager used for SIP phones is not mentioned in these Application Notes.

- Set the **Group Type** field to **sip**
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**
- Set the **Far-end Node Name** to **interopASM** This node name maps to the IP address of Session Manager as defined in **Section 5.3**
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port for TLS, such as **5067**
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**

- Set the **Far-end Domain** to **bvwdev.com**, 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



```
change signaling-group 3                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                          Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: interopASM
 Near-end Listen Port: 5067                Far-end Listen Port: 5067
                                        Far-end Network Region: 1

Far-end Domain: bvwdev.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

For the compliance test, signaling group **2** 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 **AMS1**. 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 **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 **10.33.1.30**

```
change signaling-group 2                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 2              Group Type: sip
                        Transport Method: tls


  Peer Detection Enabled? n  Peer Server: AMS



   Near-end Node Name: procr                  Far-end Node Name: AMS1
 Near-end Listen Port: 9061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: 10.33.1.30
```

5.8. Trunk Group

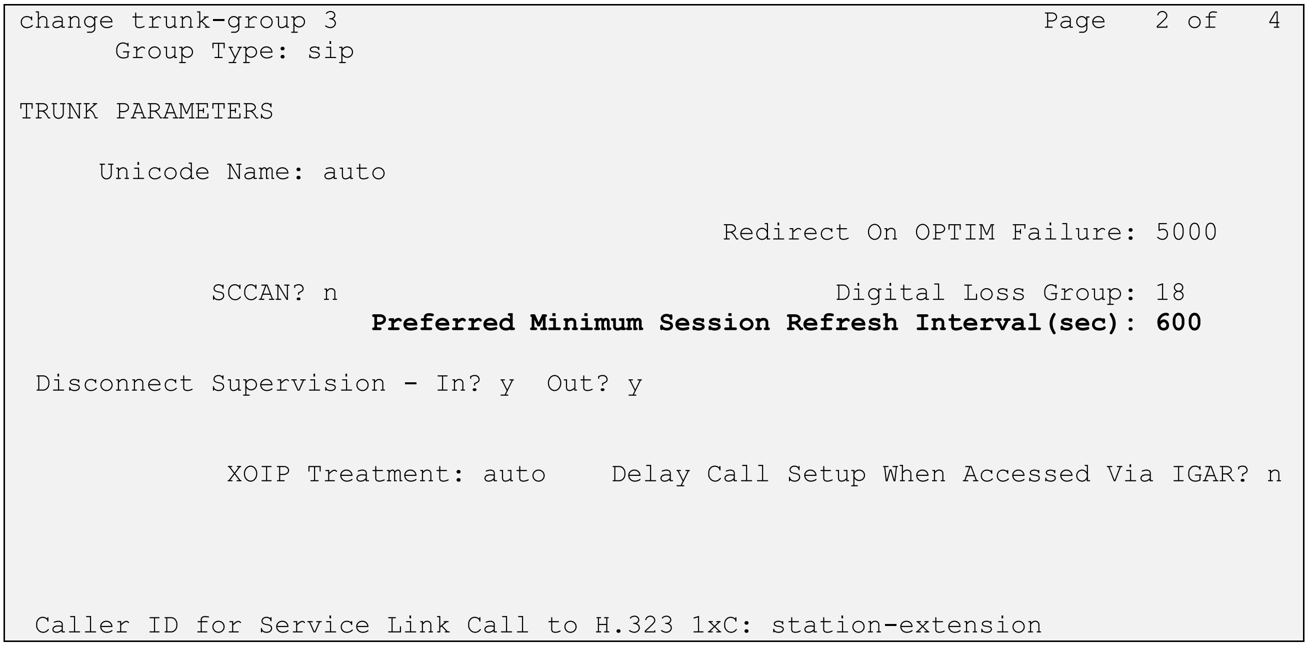
Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**.

For the compliance test, trunk group **3** 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. (i.e. **#03**). 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 **3**
- 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 **3** was associated to signaling group **3**
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk
- Default values were used for all other fields

```
change trunk-group 3                                         Page   1 of   4
                                TRUNK GROUP

Group Number: 3                    Group Type: sip           CDR Reports: y
  Group Name: To-ServiceProvider          COR: 1        TN: 1        TAC: #03
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     Number of Members: 10
```

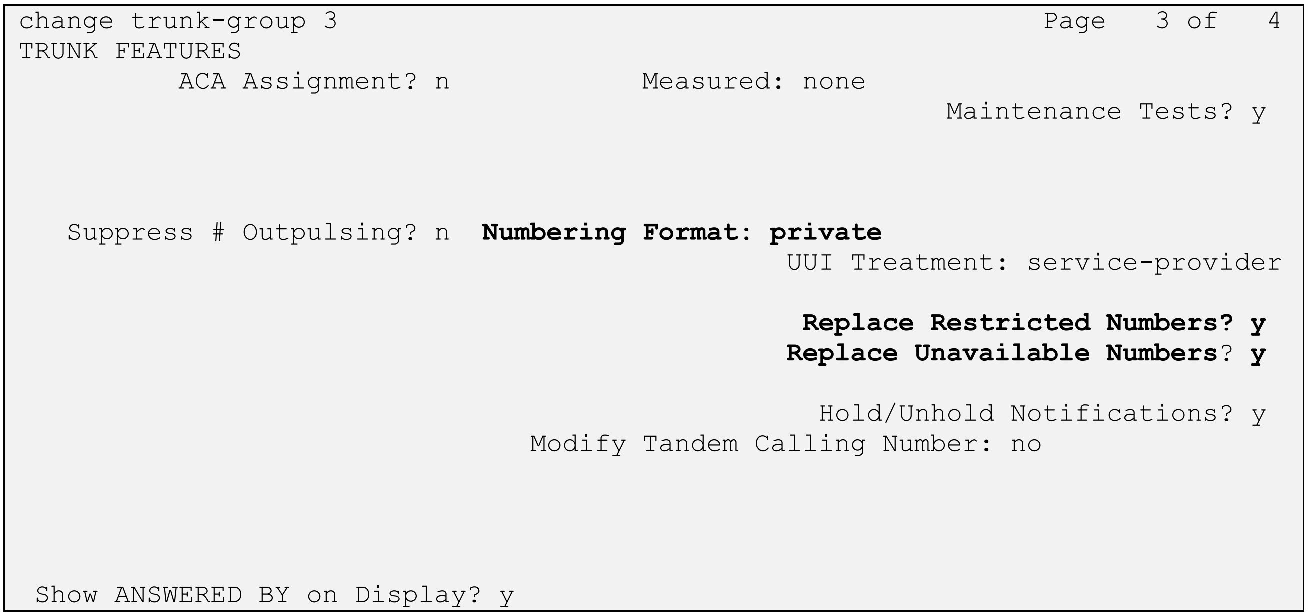
On **Page 2**, set the **Preferred Minimum Session Refresh Interval (sec)** to a value acceptable to the service provider. This value defines the interval that UPDATEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.



```
change trunk-group 3                                               Page   2 of   4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n



 Caller ID for Service Link Call to H.323 1xC: station-extension
```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end.

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



```
change trunk-group 3                                            Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

On **Page 4**, the **Network Call Redirection** field should be set to **y** so that Communication Manager will send SIP Refer in redirected calls. Note: In the compliance test, Bell Canada worked with both SIP re-Invite and SIP Refer successfully in redirected calls.

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

```
change trunk-group 3                                            Page   4 of   4
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? y
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "P-Asserted-Identity" headers. Since private numbering was selected to define the format of this number (**Section 5.8**), use the **change private-numbering 0** 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 **33** and **34** will send the calling party number as the **CPN Prefix** plus the extension number.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext               Trk        Private          Total
Len Code              Grp(s)     Prefix           Len
 4  33                1                           4  Total Administered: 15
 4  34                1                           4     Maximum Entries: 540
 4  33                3          613xxx0771       10
 4  34                3          613xxx0771       10
```

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 **6** is used as the ARS access code. Enterprise callers will dial **6** 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 **33** and **34** for extension (**ext**)
- **Dialed String** beginning with **9** for feature access code (**fac**)
- **Dialed String** beginning with **#** for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk group 3 in **Section 5.8**

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 6

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
 0             3  fac      35             4  udp      9             1  fac
 33            4  ext      4              4  aar      *             3  dac
 34            4  ext      43             4  aar      #             3  dac
```

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

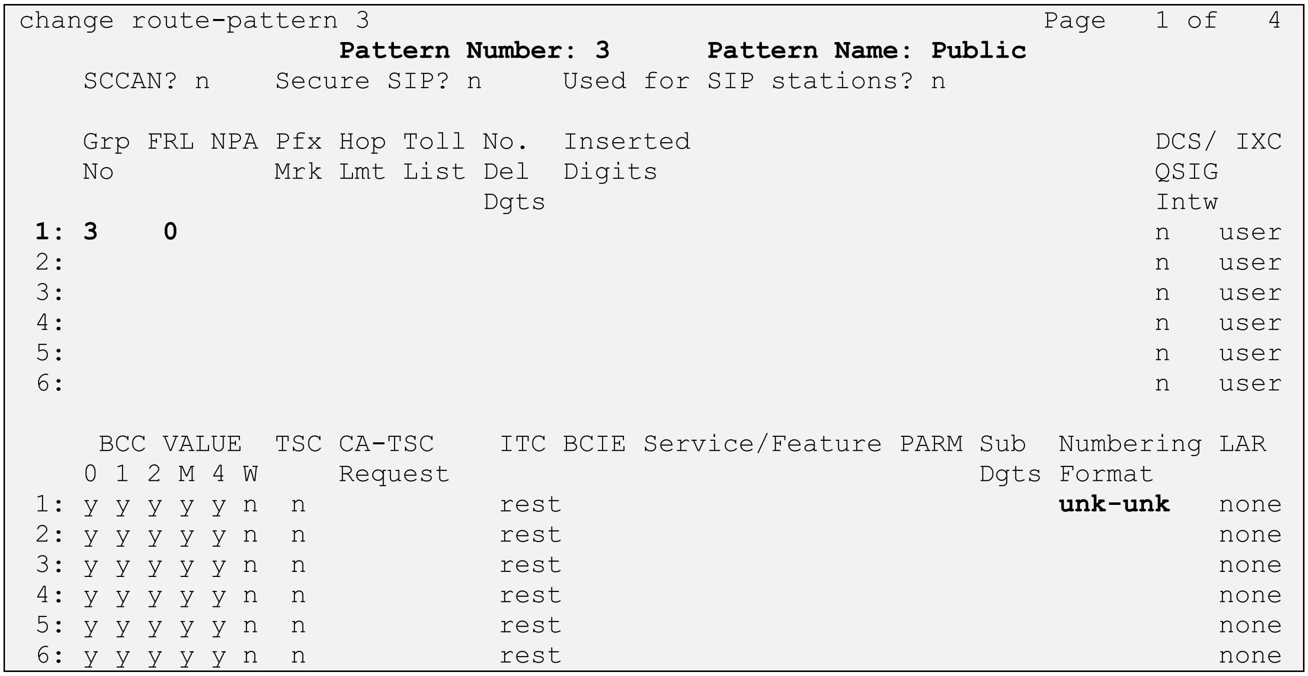
```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *05
                       Answer Back Access Code: 007
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *07    All: *06    Deactivation: *16
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: 008
                       Call Pickup Access Code: *09
CAS Remote Hold/Answer Hold-Unhold Access Code: *10
                  CDR Account Code Access Code: *11
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern 3** which contains the SIP trunk group to the service provider (as defined next).

```
change ars analysis 1                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed          Total     Route     Call    Node   ANI
          String         Min  Max  Pattern    Type    Num    Reqd
    1                    11   14    3         pubu           n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern **3** 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 **3** 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 **unk-unk** since unknown-numbering format should be used for this route (see **Section 5.8**)



```
change route-pattern 3                                          Page   1 of   4
                    Pattern Number: 3      Pattern Name: Public
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 3    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               unk-unk   none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

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 **3**. Use the **change inc-call-handling-trmt trunk-group 3** to convert incoming DID numbers as followings:

- The incoming DID number **613XXX0771** to **3000** by deleting **10** of the incoming digits for voicemail testing purpose
- The incoming DID number **613XXX0900** to 4 digit extension by deleting **10** and insert the extension number

```
change inc-call-handling-trmt trunk-group 3                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 613xxx0771       10  3000
 public-ntwrk    10 613xxx0900       10  3301
```

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

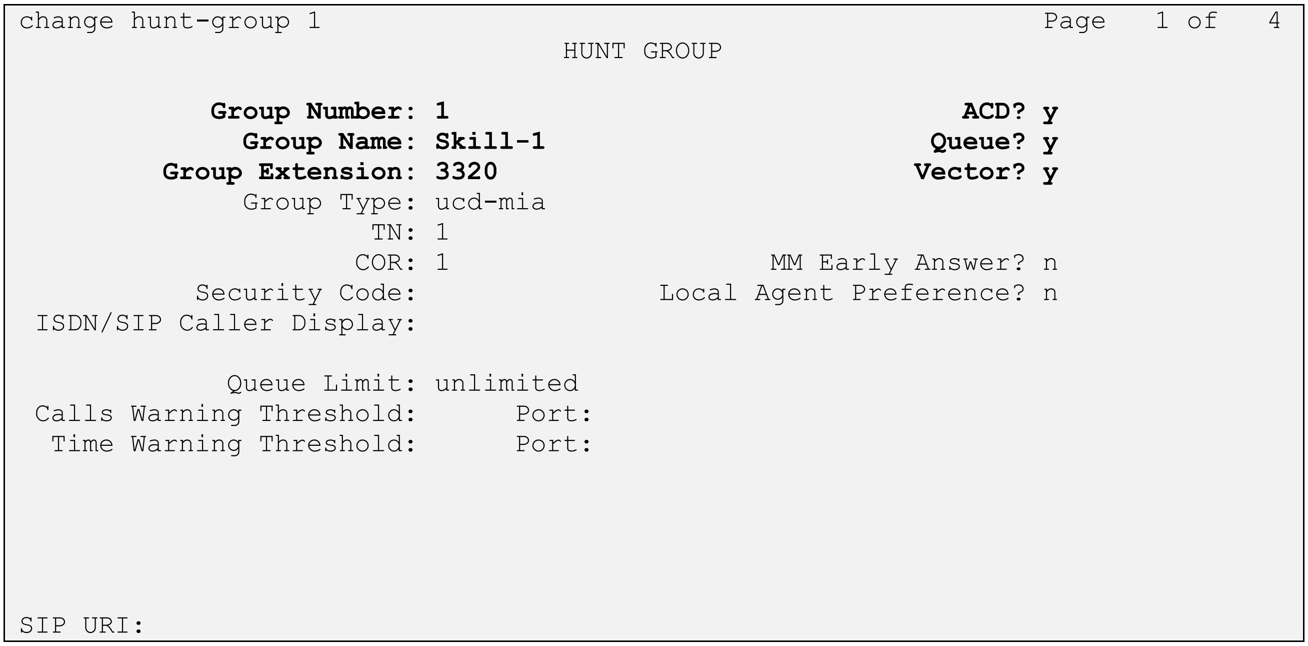
Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension,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

```
list announcement

                           ANNOUNCEMENTS/AUDIO SOURCES
Announcement                                                       Num
of
Extension             Type       Name                         Source
Sources
1101                  integ-mus  CanonD                        M1          1
1112                  integ-mus  Music1                        001V9       1
1113                  integrated H323                          001V9       1
1114                  integrated NoAgent                       001V9       1
```

5.12.2. ACD Configuration for Call Queued for Handling by Agent

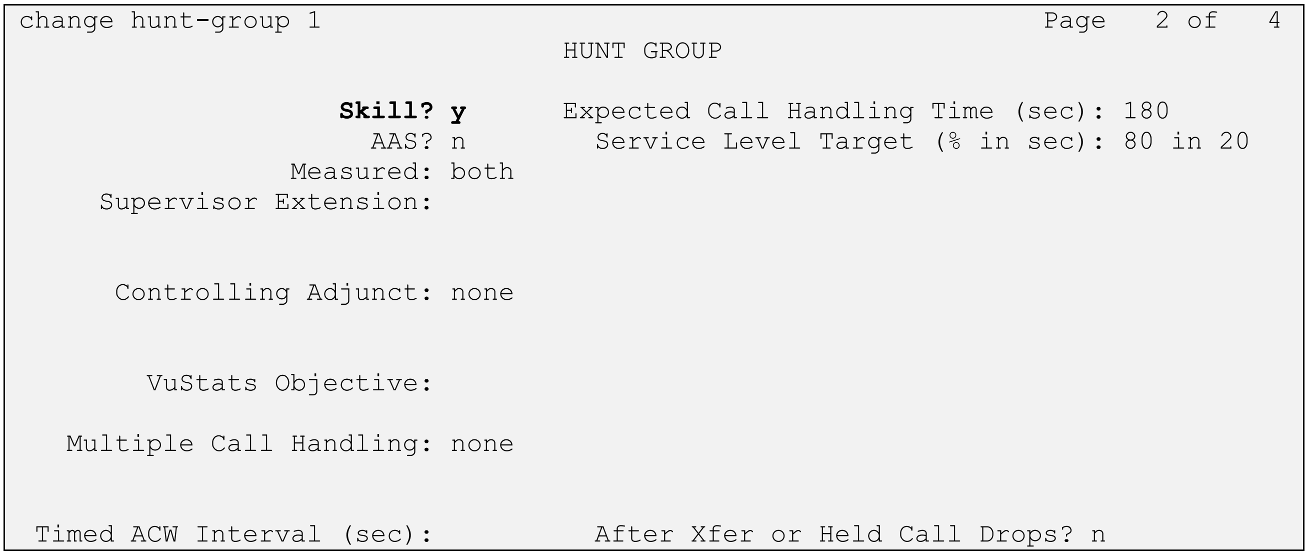
This section provides a simple example configuration for VDN, vector, hunt-group, and agent-loginID used to queue inbound calls for handling by an agent.

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



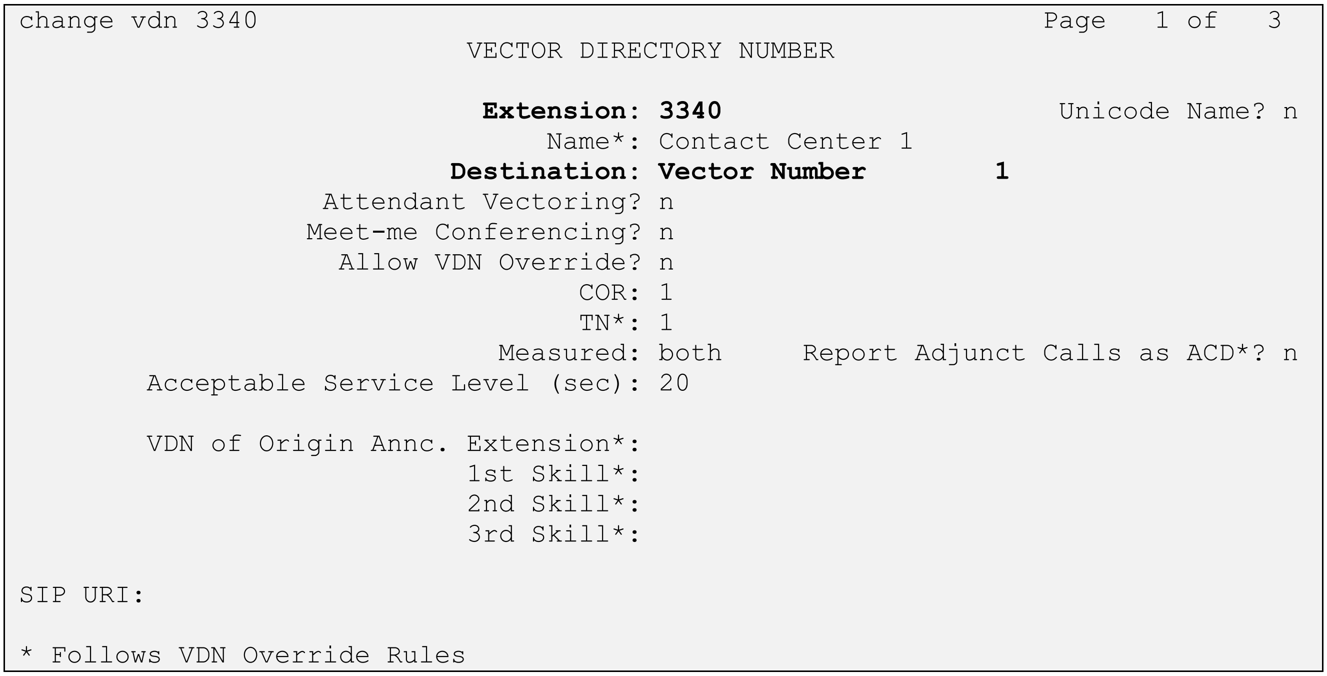
```
change hunt-group 1                                                Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                                  ACD? y
              Group Name: Skill-1                          Queue? y
         Group Extension: 3320                            Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                      MM Early Answer? n
           Security Code:                 Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:





SIP URI:
```

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



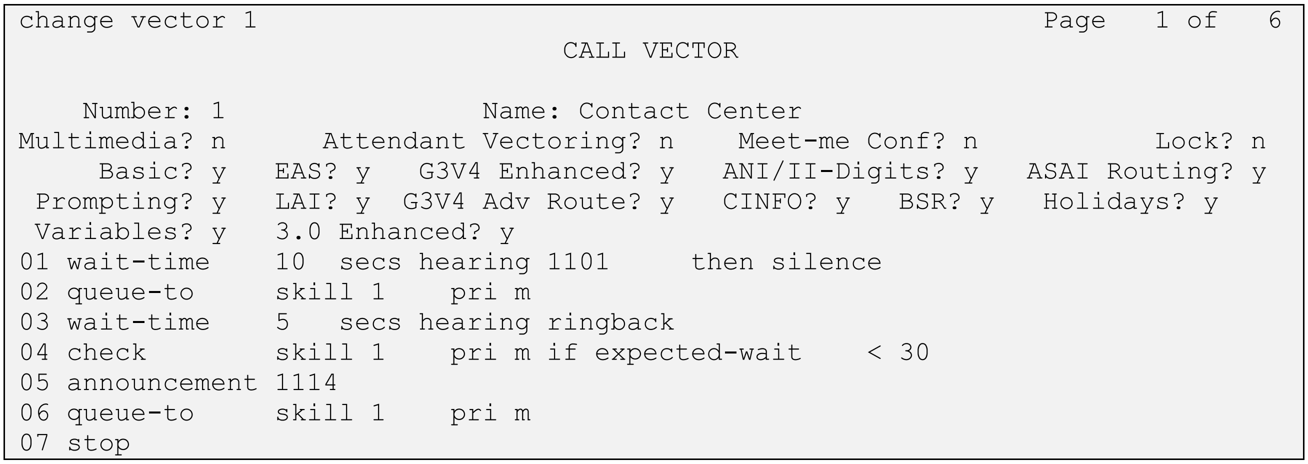
```
change hunt-group 1                                                Page   2 of   4
                                  HUNT GROUP

                     Skill? y      Expected Call Handling Time (sec): 180
                       AAS? n        Service Level Target (% in sec): 80 in 20
                  Measured: both
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:

   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

VDN 3340, shown below, is associated with vector 1.



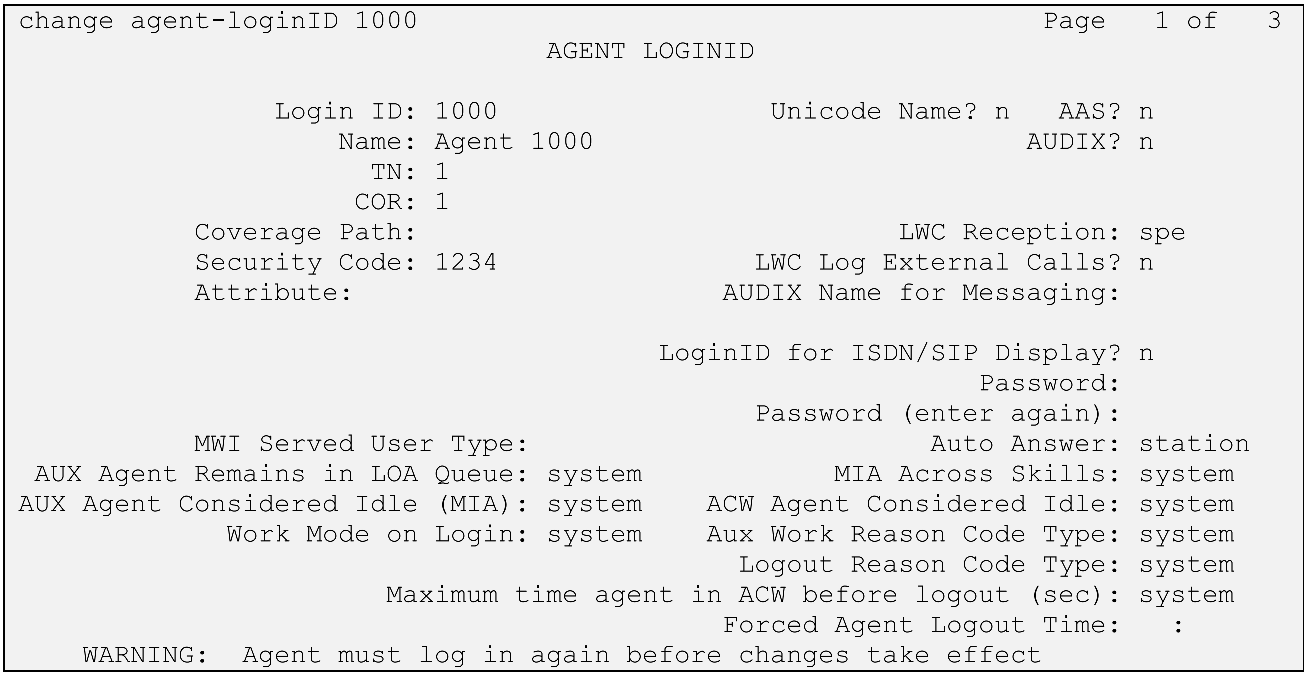
```
change vdn 3340                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 3340                     Unicode Name? n
                                 Name*: Contact Center 1
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: both     Report Adjunct Calls as ACD*? n
        Acceptable Service Level (sec): 20

        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

In this simple example, vector 1 plays music (announcement 1101) in 10 seconds, after playing the music it queues to skill 1. If there is an available agent in the queue it will route the contact center call to the available agent if there is no agent available and the expected wait time is greater than 30 seconds it will play the announcement 1114 and continue to route the call back to the ACD queue.



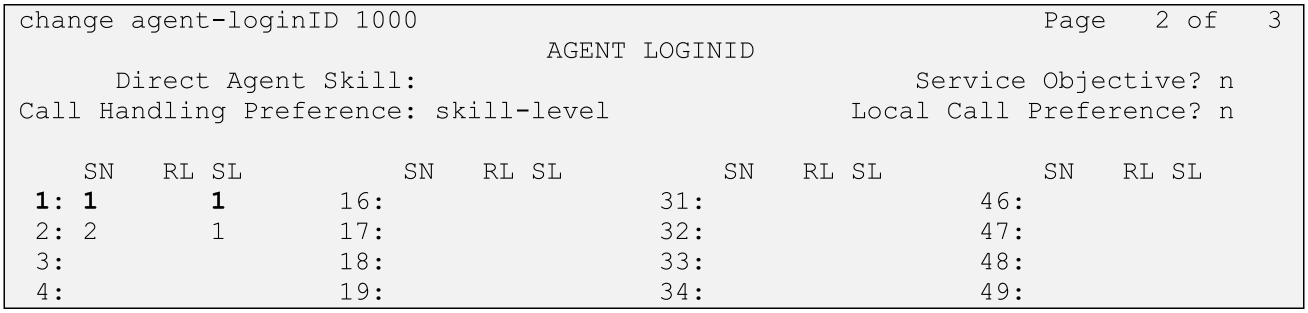
```
change vector 1                                                 Page   1 of   6
                                  CALL VECTOR

    Number: 1                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    10  secs hearing 1101     then silence
02 queue-to     skill 1    pri m
03 wait-time    5   secs hearing ringback
04 check        skill 1    pri m if expected-wait    < 30
05 announcement 1114
06 queue-to     skill 1    pri m
07 stop
```

The following screen illustrates an example agent-loginID 1000.



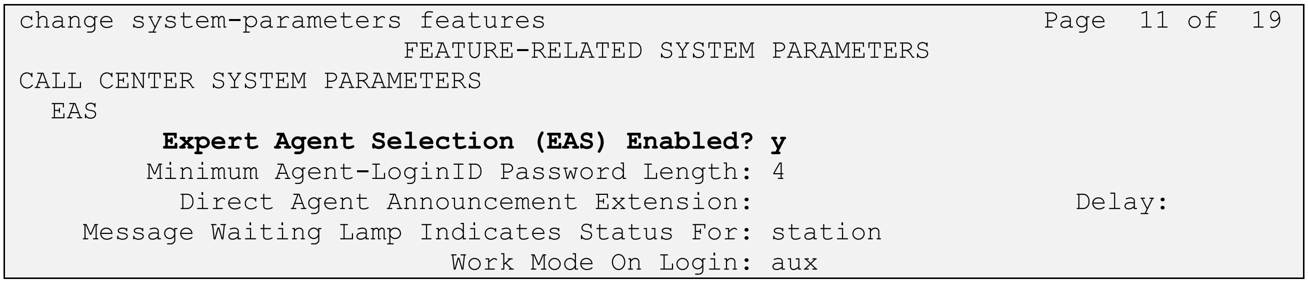
```
change agent-loginID 1000                                       Page   1 of   3
                                AGENT LOGINID

                Login ID: 1000                 Unicode Name? n    AAS? n
                    Name: Agent 1000                            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:
                                              Password (enter again):
           MWI Served User Type:                         Auto Answer: station
 AUX Agent Remains in LOA Queue: system            MIA Across Skills: system
AUX Agent Considered Idle (MIA): system    ACW Agent Considered Idle: system
             Work Mode on Login: system    Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :
    WARNING:  Agent must log in again before changes take effect
```

The following abridged screen shows Page 2 for agent-loginID 1000. Note that the Skill Number (**SN**) has been set to **1**.



```
change agent-loginID 1000                                       Page   2 of   3
                                AGENT LOGINID
      Direct Agent Skill:                                Service Objective? n
Call Handling Preference: skill-level                Local Call Preference? n

    SN   RL SL          SN   RL SL          SN   RL SL          SN   RL SL
 1: 1       1       16:             31:                 46:
 2: 2       1       17:             32:                 47:
 3:                 18:             33:                 48:
 4:                 19:             34:                 49:
```

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
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length: 4
          Direct Agent Announcement Extension:                   Delay:
    Message Waiting Lamp Indicates Status For: station
                            Work Mode On Login: aux
```

5.13. Avaya Aura® Communication Manager Stations

In the sample configuration, a four digit station extension was used with the format 33. Use the **add station 3301** command to add an Avaya H.323 IP Deskphone. Note that the table below shows the change command instead.

- Enter **Type**: **9641**, **Name**: **H323-3301**, **Security Code**: **1234**, **Coverage Path 1**: **1**, **IP SoftPhone**: **y** (if using this extension as a Softphone such as Avaya one-X® Communicator)
- Leave other values as default

```
add station 3301                                                Page   1 of   6
                                     STATION

Extension: 3301                          Lock Messages? n              BCC: 0
     Type: 9641                          Security Code: *               TN: 1
     Port: S000011                     Coverage Path 1: 1              COR: 1
     Name: H323-3301                   Coverage Path 2:                COS: 15
Unicode Name? n                     Hunt-to Station:                 Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 3301
            Speakerphone: 2-way             Mute Button Enabled? y
        Display Language: english                Button Modules: 1
 Survivable GK Node Name: lsp
          Survivable COR: internal            Media Complex Ext:
   Survivable Trunk Dest? y                        IP SoftPhone? y

                                              IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                               Customizable Labels? y
```

5.14. Save Avaya Aura® Communication Manager Configuration Changes

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

6. Configure Avaya Aura® Session Manager

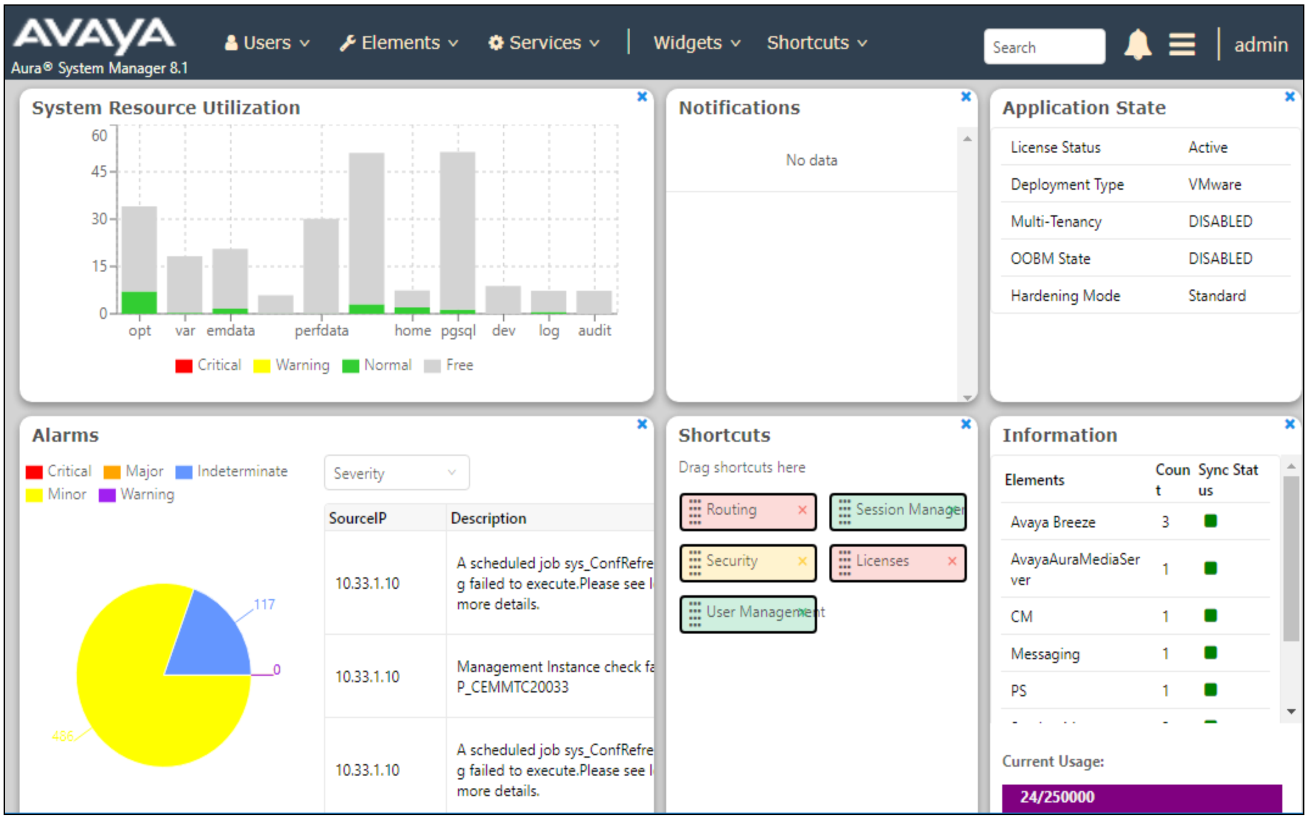
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- 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
- 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.



No data

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

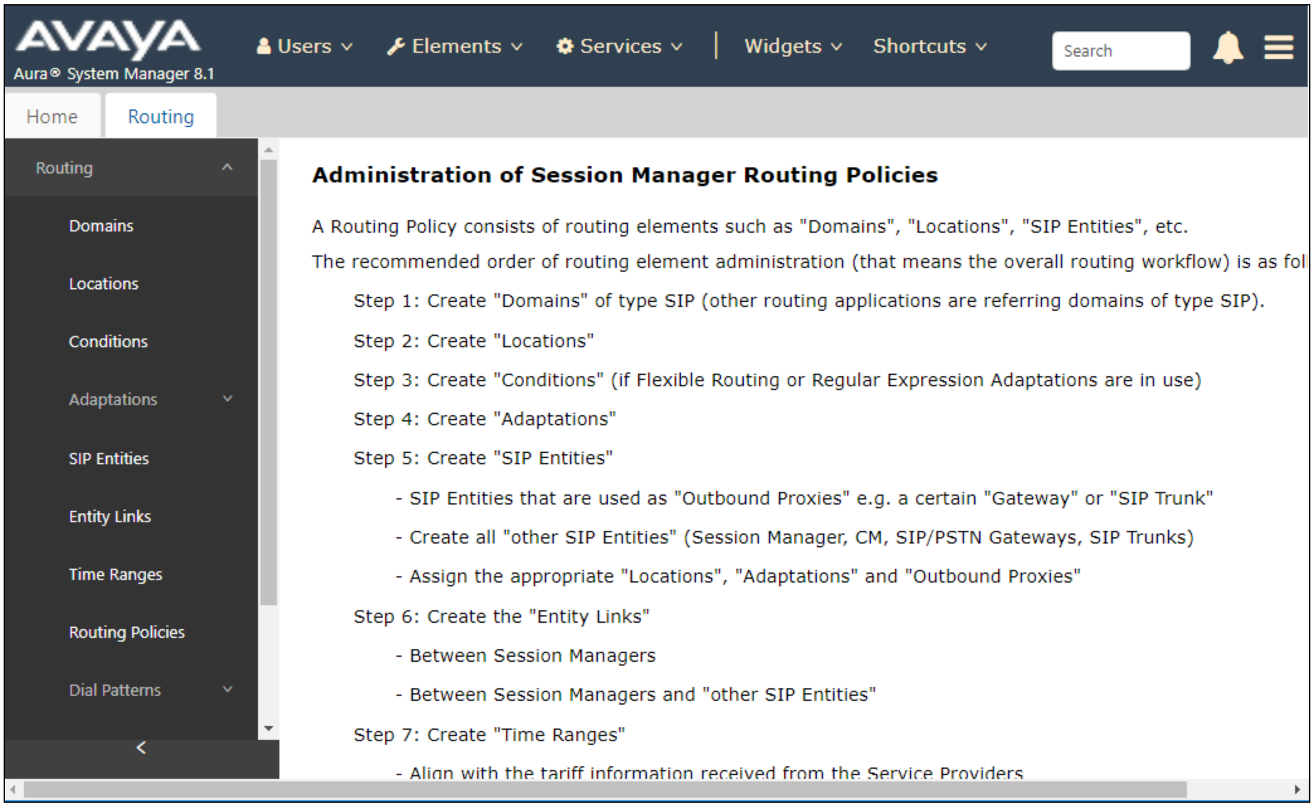
SourceIP	Description
10.33.1.10	A scheduled job sys_ConfRefre g failed to execute.Please see l more details.
10.33.1.10	Management Instance check fa P_CEMMTC20033
10.33.1.10	A scheduled job sys_ConfRefre g failed to execute.Please see l more details.

Elements	Count	Sync Status
Avaya Breeze	3	🟩
AvayaAuraMediaServer	1	🟩
CM	1	🟩
Messaging	1	🟩
PS	1	🟩

Current Usage:

24/250000

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.



Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as fol

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)

Step 4: Create "Adaptations"

Step 5: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 6: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 7: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

6.2. Specify SIP Domain

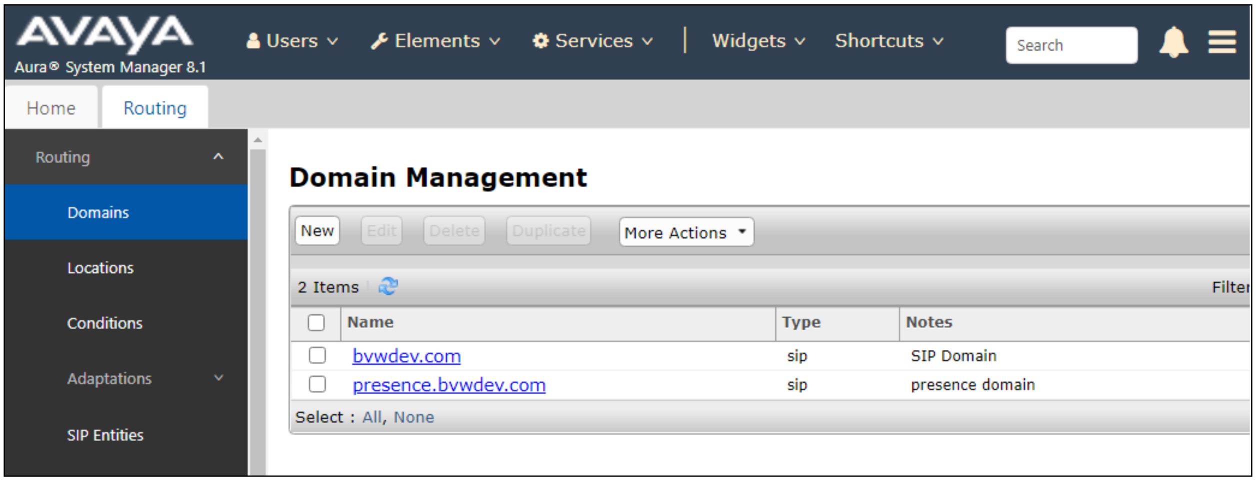
Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev.com**.

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.



Domain Management

2 Items

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

Select : All, None

6.3. Add Location

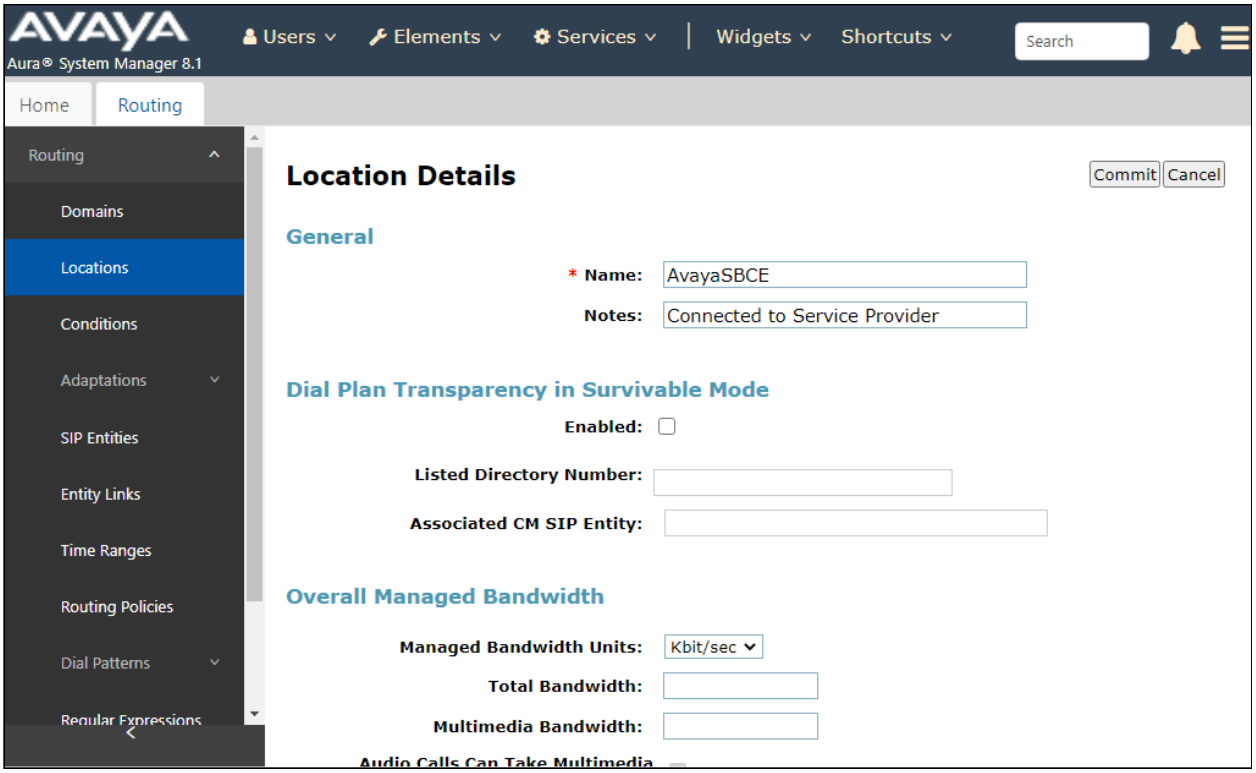
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control.

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



Location Details

General

* Name: AvayaSBCE

Notes: Connected to Service Provider

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

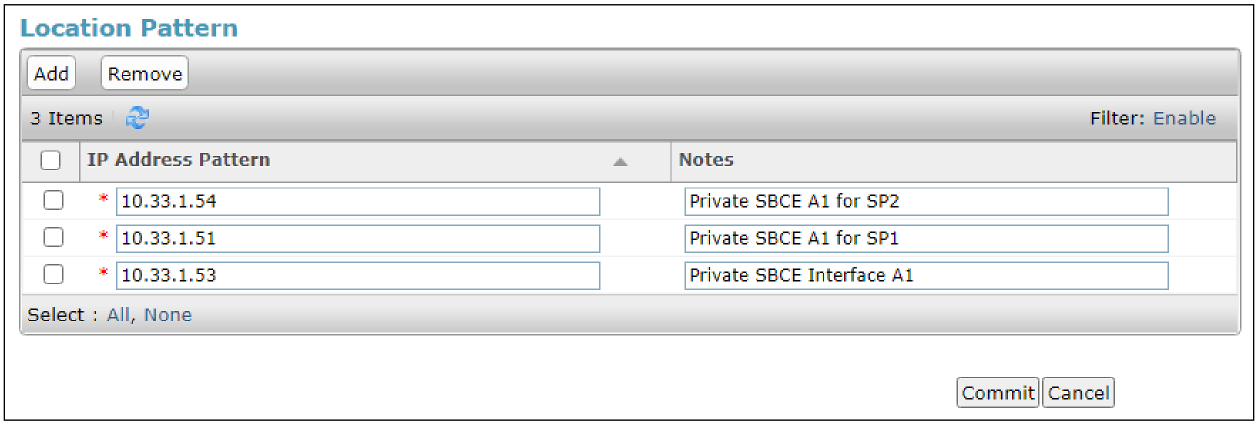
Multimedia Bandwidth:

Audio Calls Can Take Multimedia

In the **Location Pattern** section, click **Add** to enter **IP Address Pattern**. The following patterns were used in testing:

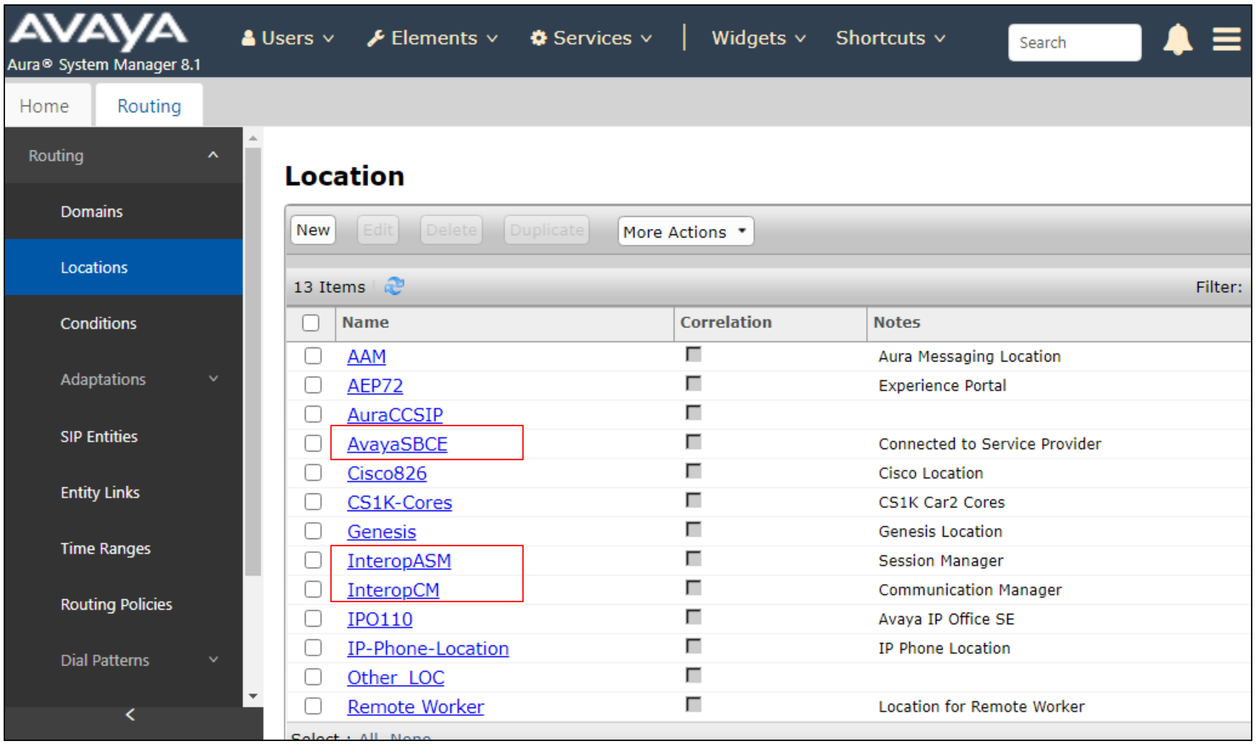
- **IP Address Pattern**: **10.33.1.51, 10.33.1.53,** and **10.33.1.54**
- Click **Commit** to save

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



☐	IP Address Pattern	Notes
☐	* 10.33.1.54	Private SBCE A1 for SP2
☐	* 10.33.1.51	Private SBCE A1 for SP1
☐	* 10.33.1.53	Private SBCE Interface A1

Repeat the procedure above to add another Location. The screenshot below shows the list of Locations created in System Manager.



☐	Name	Correlation	Notes
☐	AAM	☐	Aura Messaging Location
☐	AEP72	☐	Experience Portal
☐	AuraCCSIP	☐	
☐	AvayaSBCE	☐	Connected to Service Provider
☐	Cisco826	☐	Cisco Location
☐	CS1K-Cores	☐	CS1K Car2 Cores
☐	Genesis	☐	Genesis Location
☐	InteropASM	☐	Session Manager
☐	InteropCM	☐	Communication Manager
☐	IPO110	☐	Avaya IP Office SE
☐	IP-Phone-Location	☐	IP Phone Location
☐	Other_LOC	☐	
☐	Remote Worker	☐	Location for Remote Worker

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.

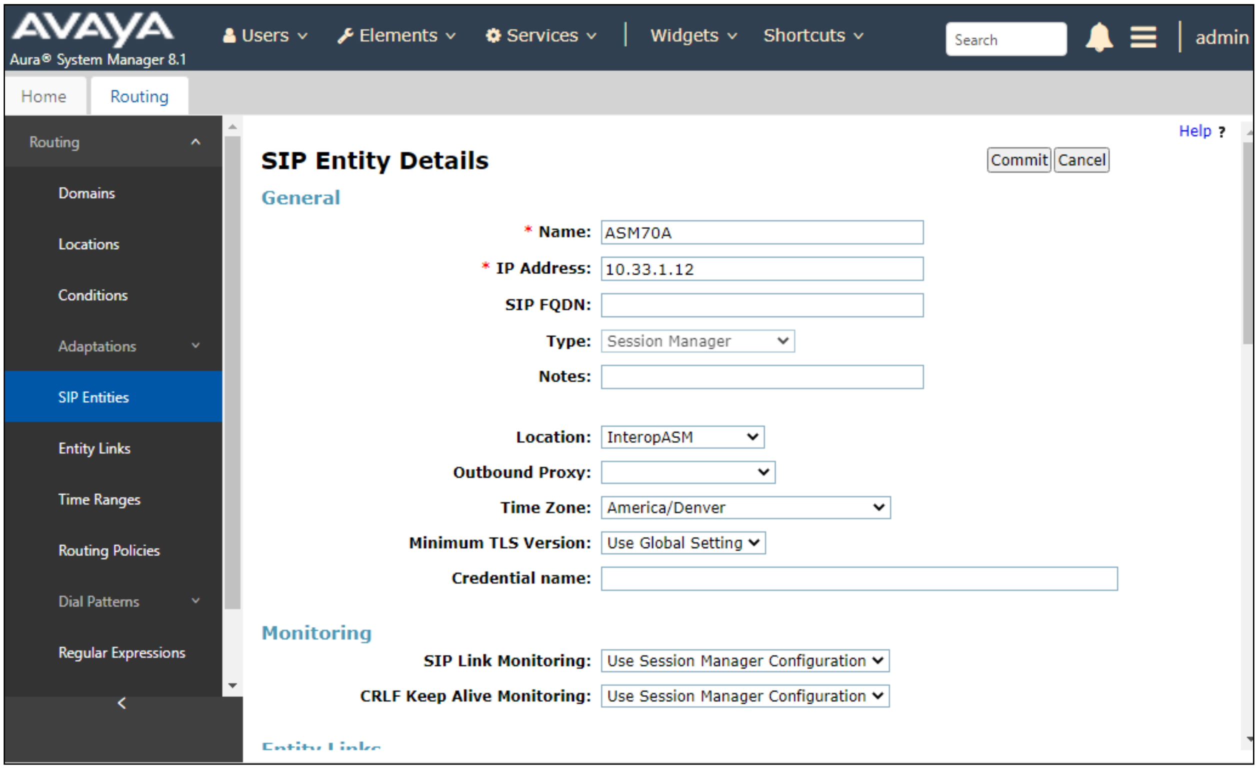
- **Name**: Enter a descriptive name
- **FQDN or IP Address**: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling
- **Type**: Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for Avaya SBCE
- **Adaptation**: This field is only 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.
- **Time Zone**: Select the time zone for the Location above

In this configuration, there are three SIP Entities:

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

6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **ASM70A**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.1.12**. The user will need to select the specific values for the **Location** and **Time Zone**.



SIP Entity Details

General

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

Monitoring

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

Entity Links

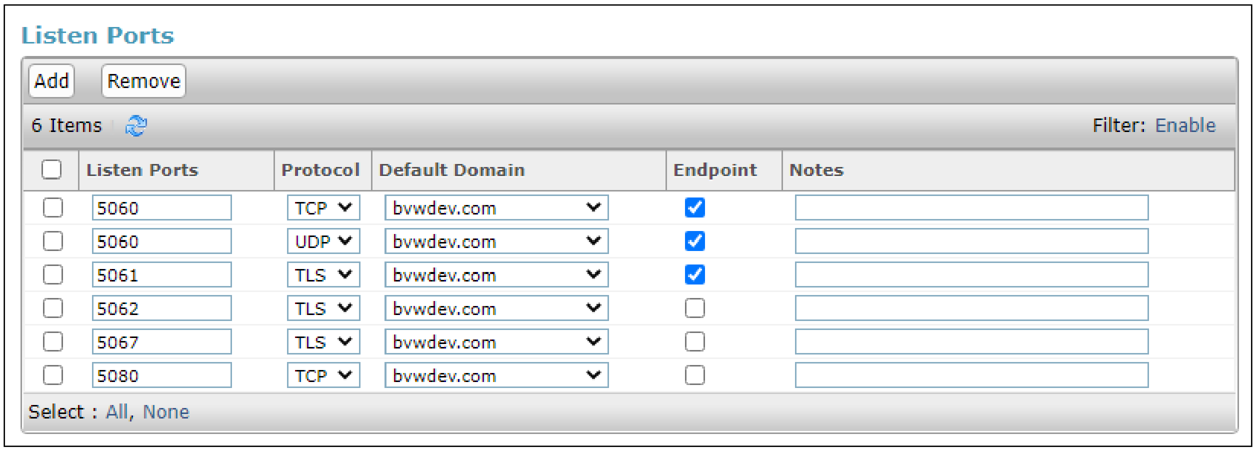
To define the ports used by Session Manager, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

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 **5067** and **5061** with **TLS** for connecting to Communication Manager and Avaya SBCE.

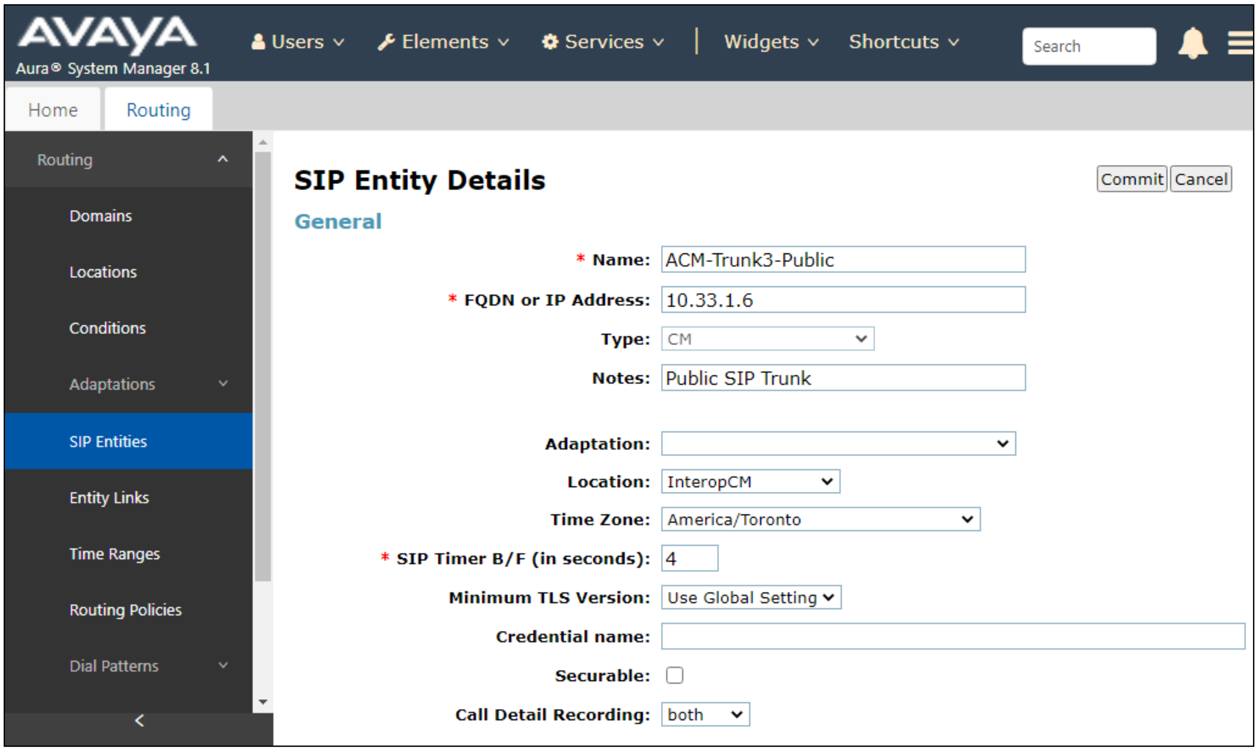


Listen Ports

□	Listen Ports	Protocol	Default Domain	Endpoint	Notes
□	5060	TCP	bvwdev.com	☑	
□	5060	UDP	bvwdev.com	☑	
□	5061	TLS	bvwdev.com	☑	
□	5062	TLS	bvwdev.com	□	
□	5067	TLS	bvwdev.com	□	
□	5080	TCP	bvwdev.com	□	

6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **ACM-Trunk3-Public**. 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 **10.33.1.6**. Note that **CM** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.



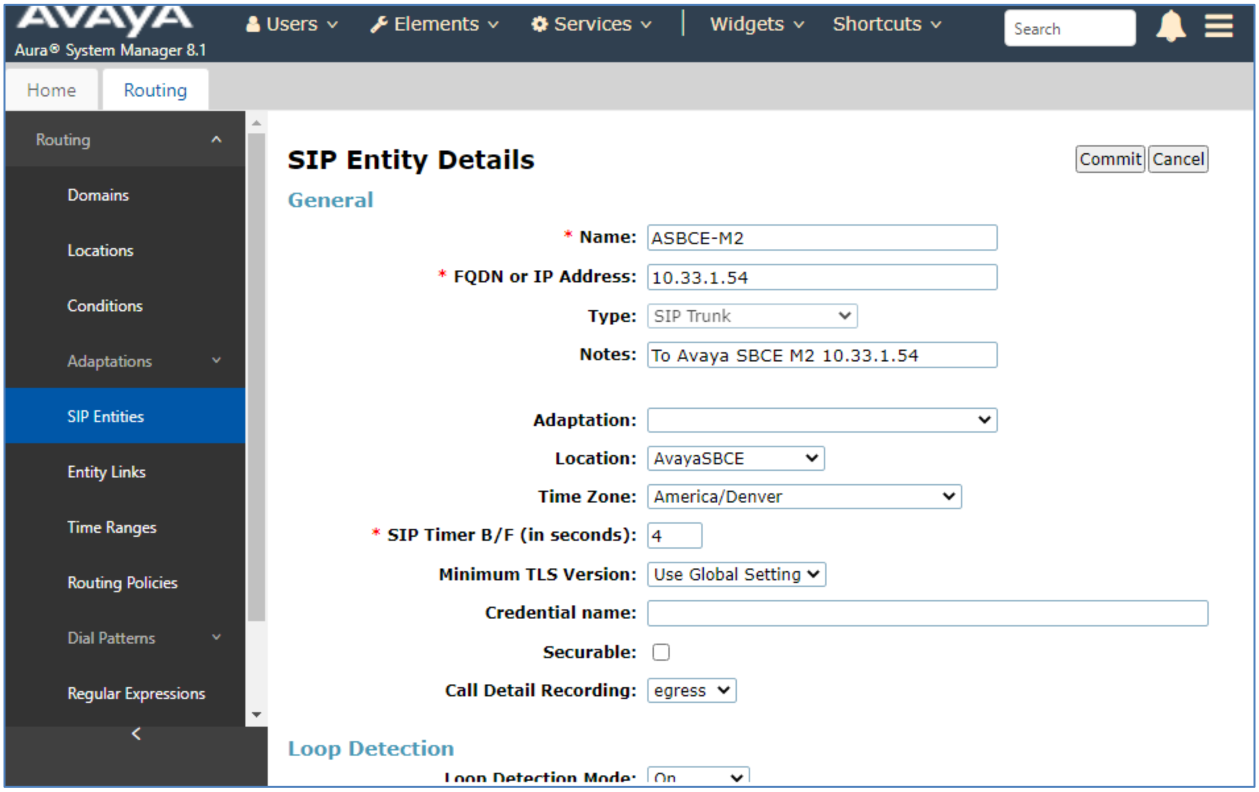
SIP Entity Details

General

* Name:	ACM-Trunk3-Public
* FQDN or IP Address:	10.33.1.6
Type:	CM
Notes:	Public SIP Trunk
Adaptation:	
Location:	InteropCM
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	both

6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **ASBCE-M2**. The **FQDN** or **IP Address** field is set to the IP address of the SBCE's private network interface **10.33.1.54**. Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.



SIP Entity Details

General

* Name:	ASBCE-M2
* FQDN or IP Address:	10.33.1.54
Type:	SIP Trunk
Notes:	To Avaya SBCE M2 10.33.1.54
Adaptation:	
Location:	AvayaSBCE
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	egress

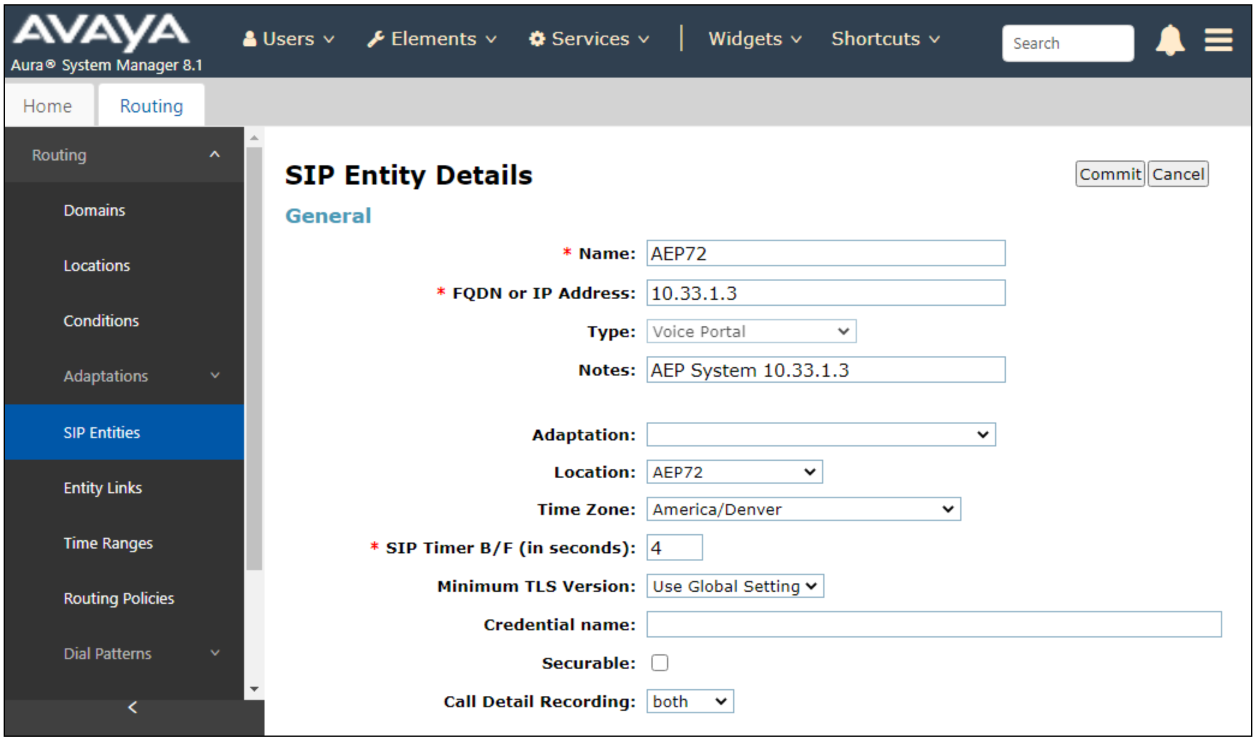
Loop Detection

Loop Detection Mode: On

6.4.4. Configure Avaya Aura® Experience Portal SIP Entity

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

- The **FQDN or IP Address** field is set to the IP address of the Experience Portal (see **Figure 1**).
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- Select the **Time Zone**.



SIP Entity Details

General

* Name:	AEP72
* FQDN or IP Address:	10.33.1.3
Type:	Voice Portal
Notes:	AEP System 10.33.1.3
Adaptation:	
Location:	AEP72
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	☐
Call Detail Recording:	both

6.5. Add Entity Links

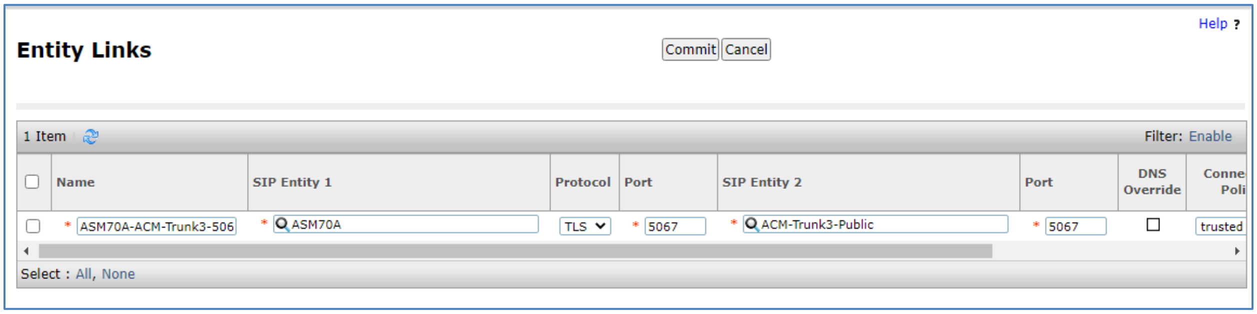
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by the service provider traffic and one to the Avaya SBCE.

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

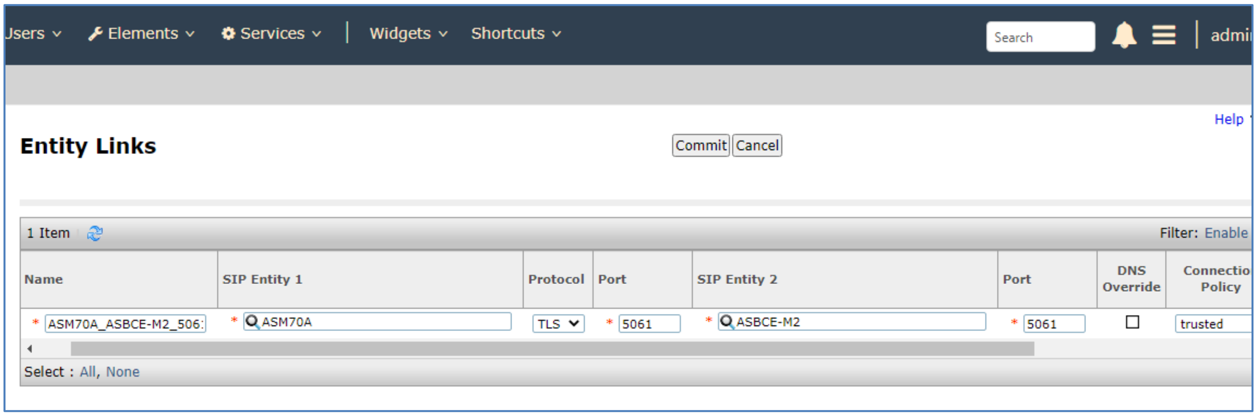
The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.



Entity Links

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Conne Poli
☐	* ASM70A-ACM-Trunk3-506	* ASM70A	TLS	* 5067	* ACM-Trunk3-Public	* 5067	☐	trusted

The following screen illustrates the Entity Links to Avaya SBCE.

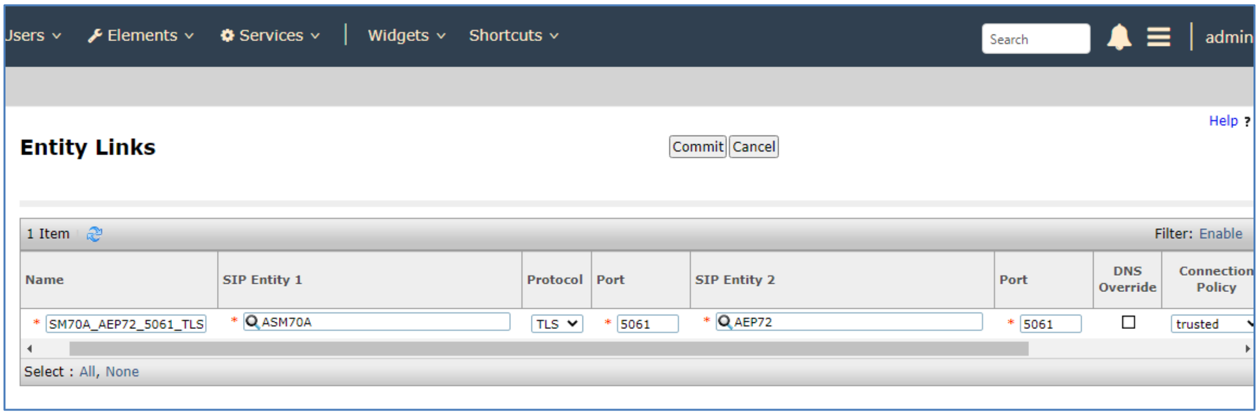


Entity Links

1 Item | Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connectio Policy
* ASM70A_ASBCE-M2_506	* ASM70A	TLS	* 5061	* ASBCE-M2	* 5061	☐	trusted

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



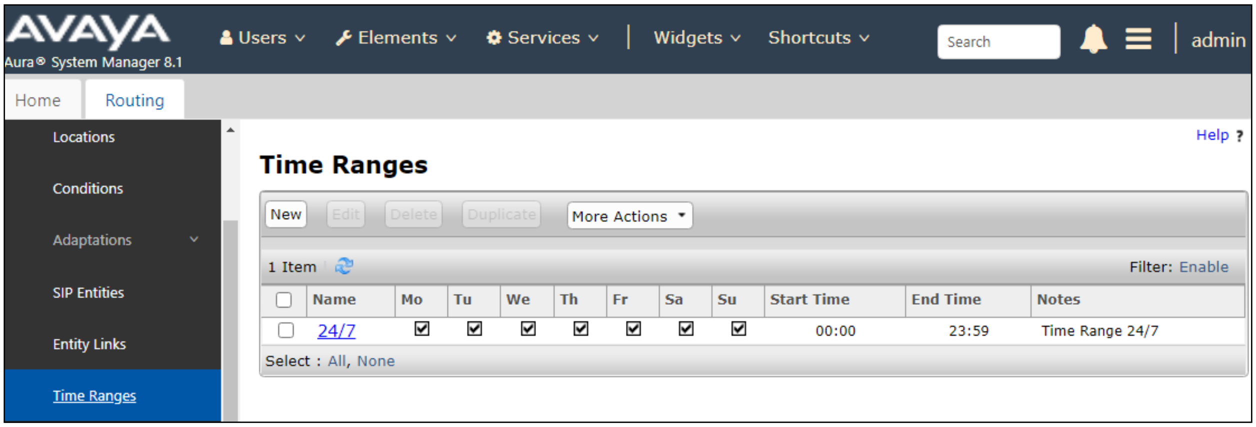
Entity Links

1 Item | Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
* SM70A_AEP72_5061_TLS	* ASM70A	TLS	* 5061	* AEP72	* 5061	☐	trusted

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.



Time Ranges

☐	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

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 Avaya SBCE and one for Experience Portal.

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:

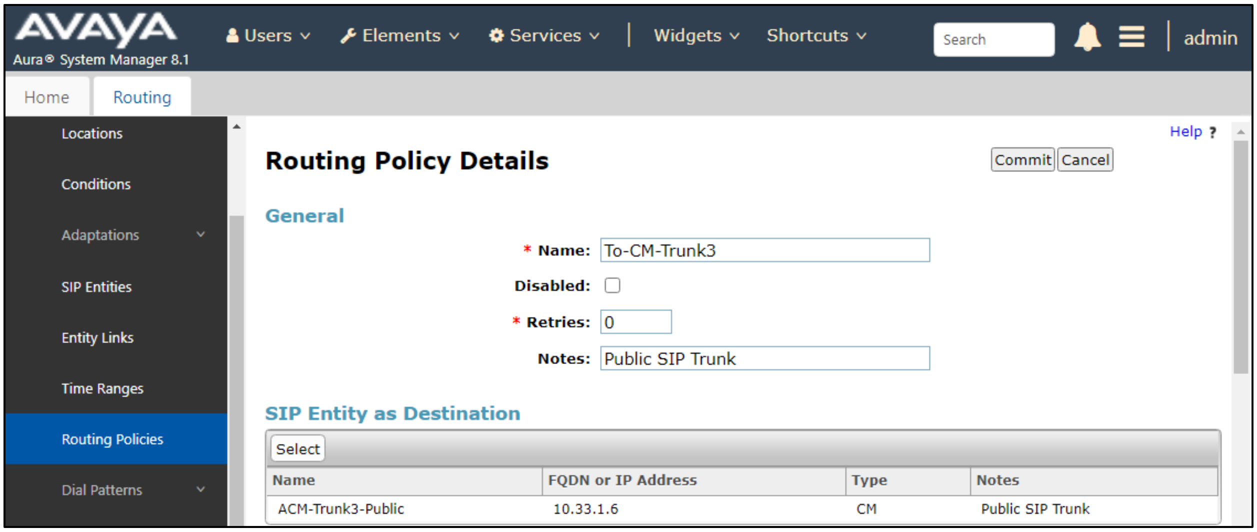
In the **General** section, enter the following values. Use default values for all remaining fields.

- **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 **To-CM-Trunk3** associated with incoming PSTN calls from Bell Canada to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **ACM-Trunk3-Public**.



Routing Policy Details

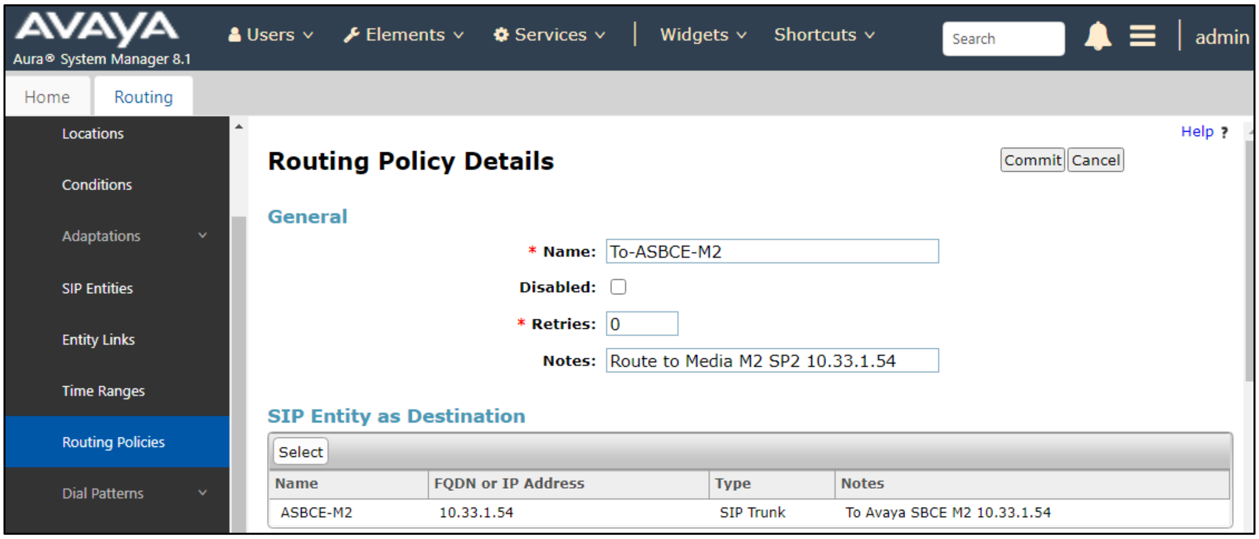
General

* Name:	To-CM-Trunk3
Disabled:	□
* Retries:	0
Notes:	Public SIP Trunk

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ACM-Trunk3-Public	10.33.1.6	CM	Public SIP Trunk

The following screen shows the **Routing Policy Details** for the policy named **To-ASBCE-M2** associated with outgoing calls from Communication Manager to the PSTN via Bell Canada SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **ASBCE-M2**.



Routing Policy Details

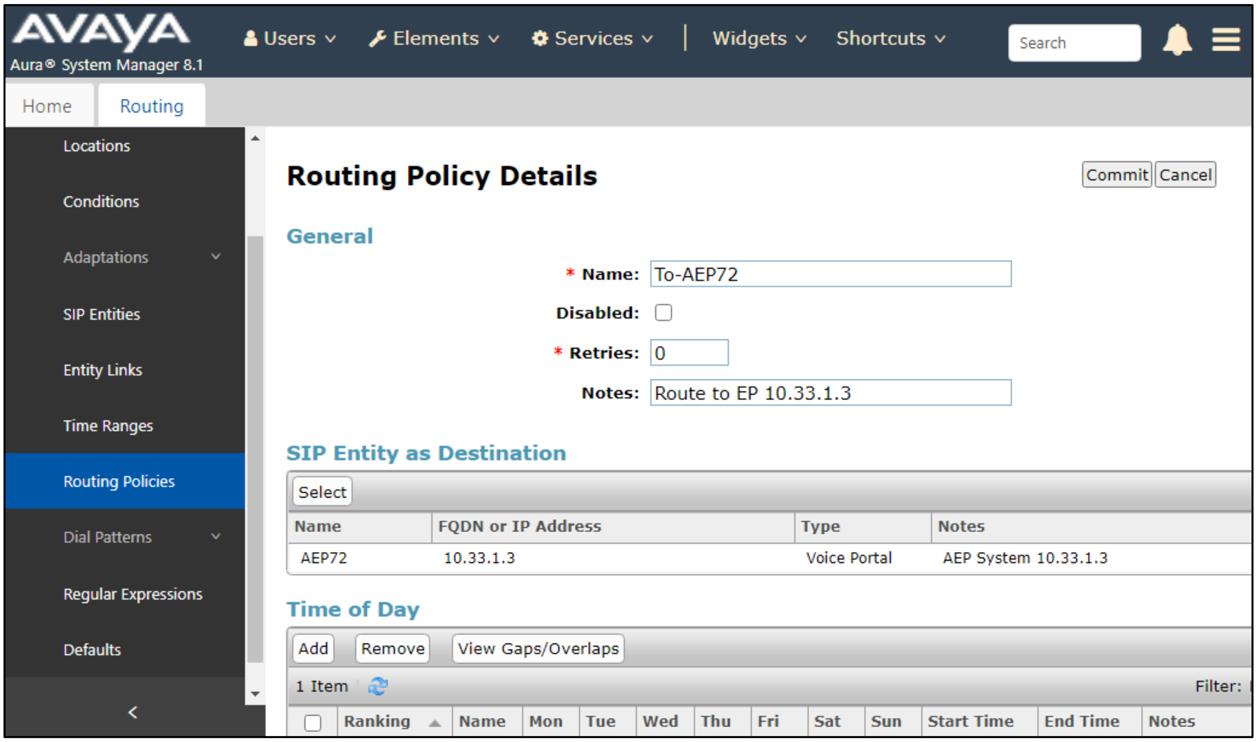
General

* Name:	To-ASBCE-M2
Disabled:	□
* Retries:	0
Notes:	Route to Media M2 SP2 10.33.1.54

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ASBCE-M2	10.33.1.54	SIP Trunk	To Avaya SBCE M2 10.33.1.54

The following screens show the Routing Policies **To-AEP72** for Experience Portal.



Routing Policy Details

General

* Name: To-AEP72

Disabled: □

* Retries: 0

Notes: Route to EP 10.33.1.3

SIP Entity as Destination

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

Time of Day

1 Item

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to Bell Canada 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.

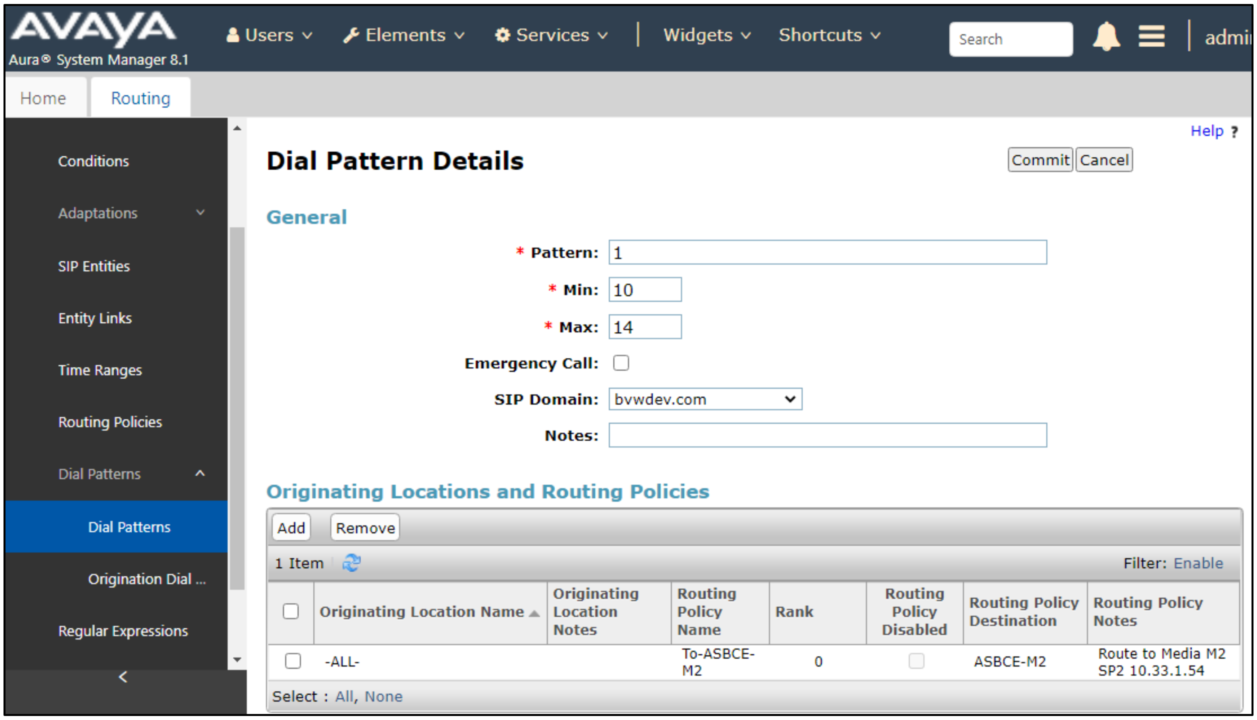
- **Pattern**: Enter a dial string that will be matched against the Request-URI of the call
- **Min**: Enter a minimum length used in the match criteria
- **Max**: Enter a maximum length used in the match criteria
- **SIP Domain**: Enter the destination domain used in the match criteria
- **Notes**: 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 below.

The first example shows that outbound 10 to 14 digit dialed numbers that begin with **1** and have a destination **SIP Domain** of **bvwdev.com** uses **Routing Policy Name** as **ASBCE-M2**.



Dial Pattern Details

General

* Pattern:	1
* Min:	10
* Max:	14
Emergency Call:	□
SIP Domain:	bvwdev.com
Notes:	

Originating Locations and Routing Policies

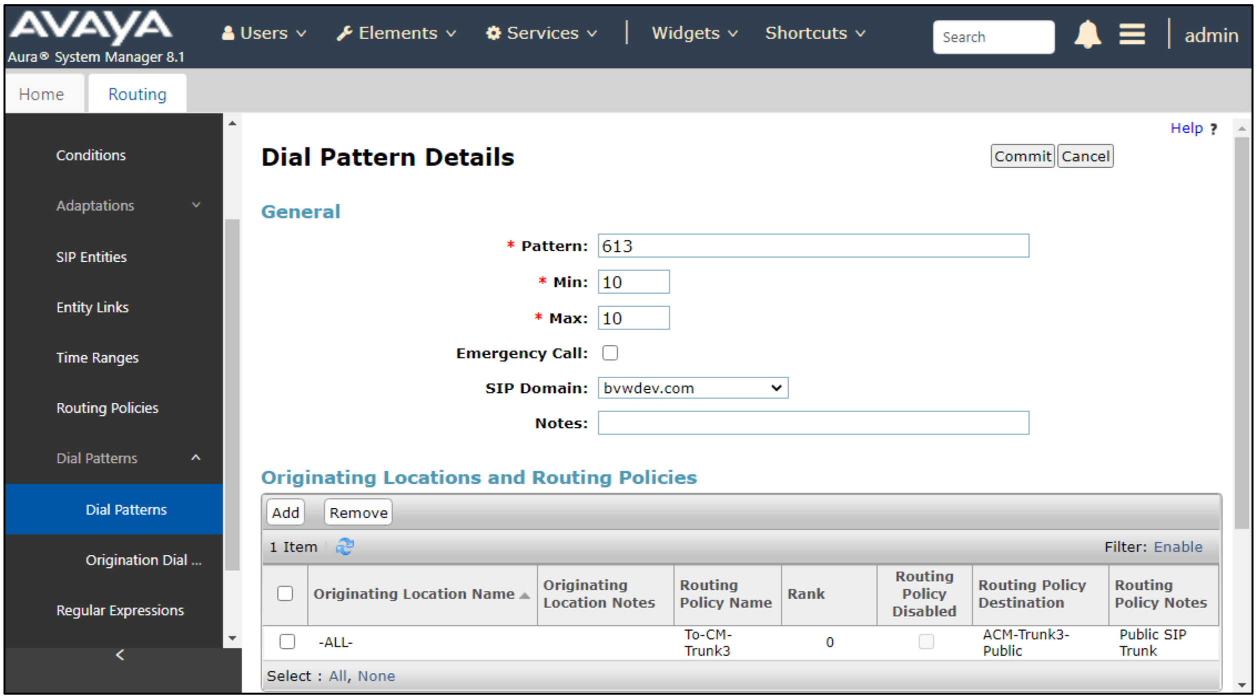
1 Item

□	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-ASBCE-M2	0	□	ASBCE-M2	Route to Media M2 SP2 10.33.1.54

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

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

The second example shows that inbound 10-digit numbers that start with **613** use **Routing Policy Name** as **ACM-Trunk3-Public**. This Dial Pattern matches the DID numbers assigned to the enterprise by Bell Canada.



Dial Pattern Details

General

* Pattern:	613
* Min:	10
* Max:	10
Emergency Call:	□
SIP Domain:	bvwdev.com
Notes:	

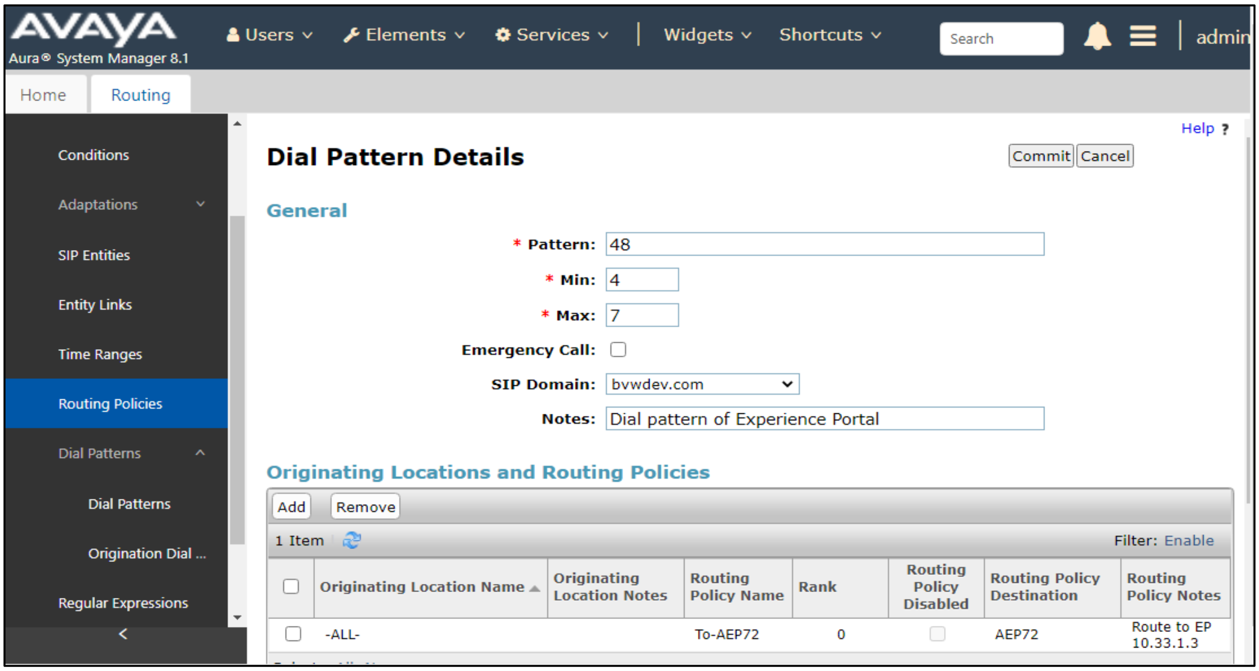
Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-CM-Trunk3	0	□	ACM-Trunk3-Public	Public SIP Trunk

Select : All, None

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to Experience Portal.



Dial Pattern Details

General

* Pattern:	48
* Min:	4
* Max:	7
Emergency Call:	□
SIP Domain:	bvwdev.com
Notes:	Dial pattern of Experience Portal

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-AEP72	0	□	AEP72	Route to EP 10.33.1.3

7. Configure Avaya Session Border Controller for Enterprise

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

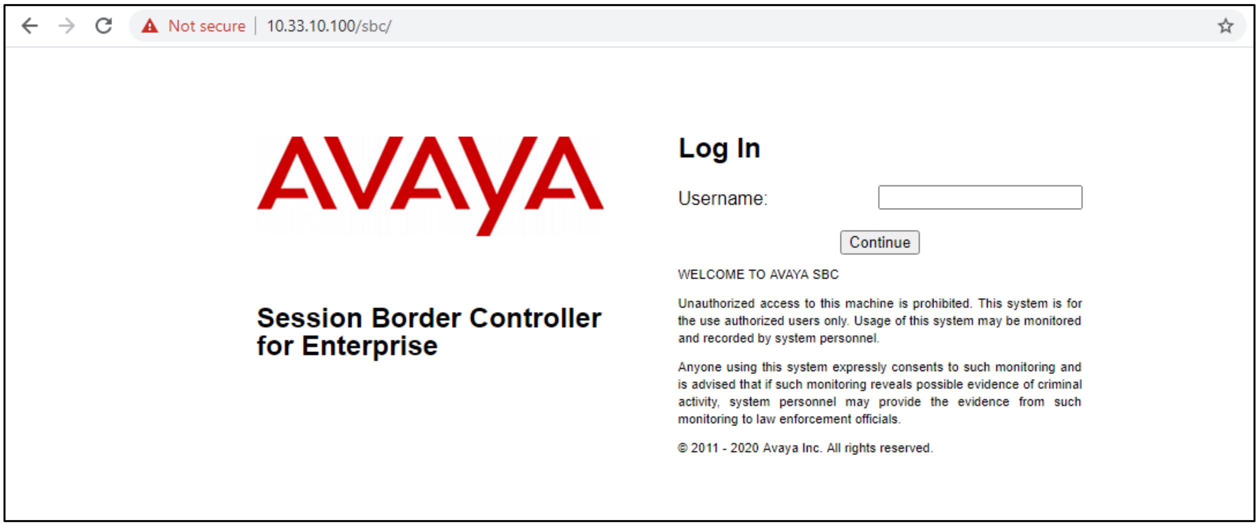
In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Bell Canada system resides on the Public side of the network.

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 122** of these Application Notes.

7.1. Log in to Avaya Session Border Controller for Enterprise

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



Not secure | 10.33.10.100/sbc/

Session Border Controller for Enterprise

Log In

Username:

Continue

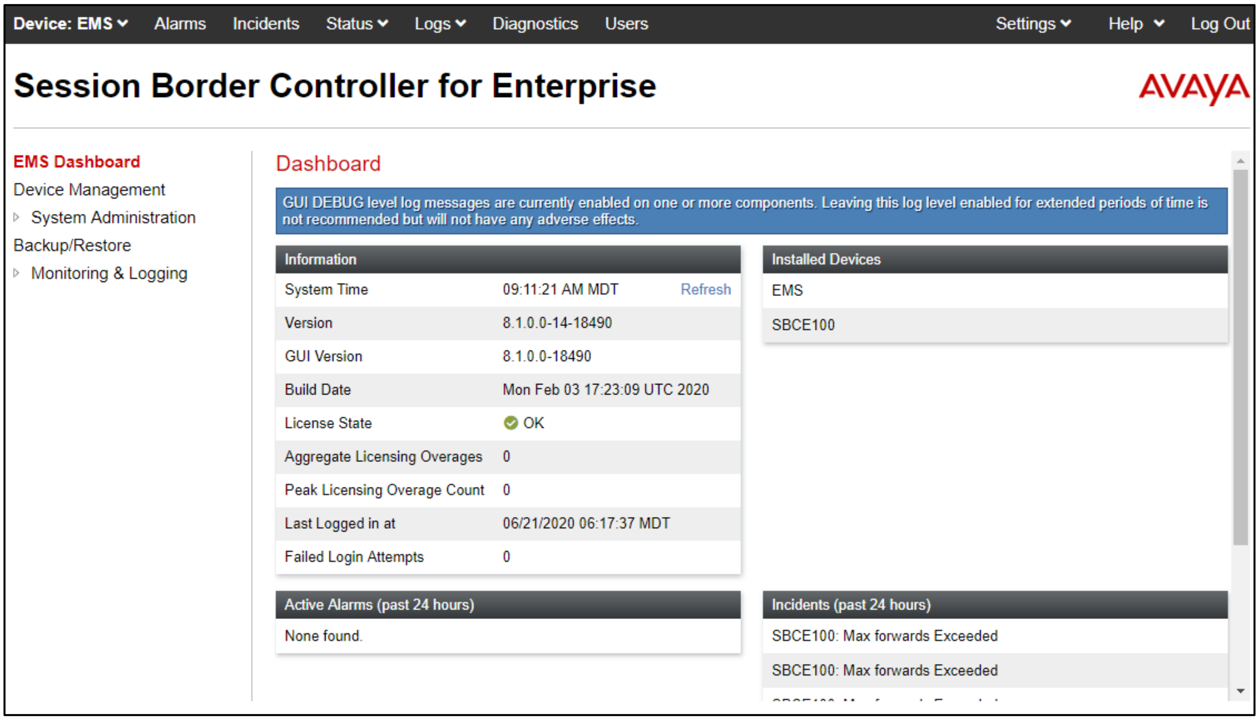
WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

The **Dashboard** main page will appear as shown below.



GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

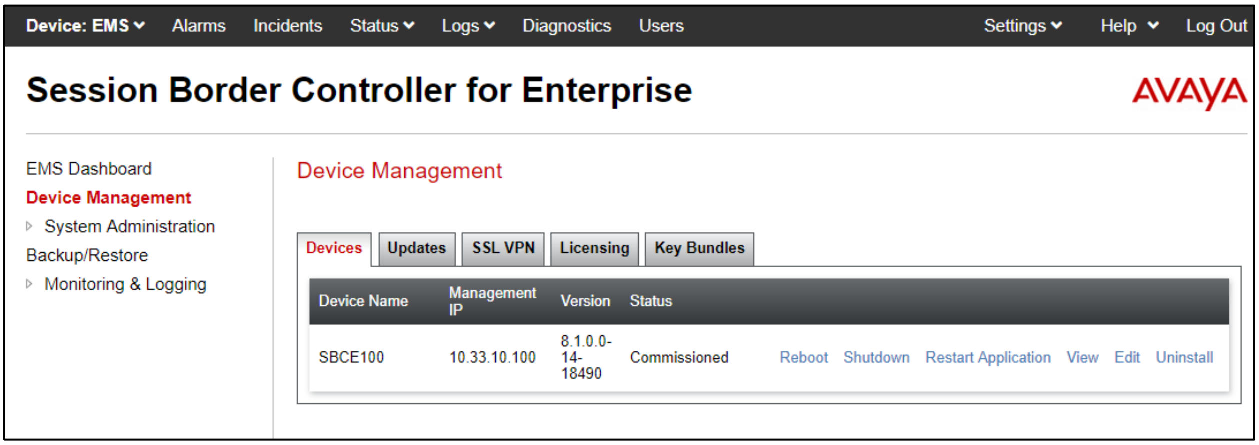
Information	
System Time	09:11:21 AM MDT
Version	8.1.0.0-14-18490
GUI Version	8.1.0.0-18490
Build Date	Mon Feb 03 17:23:09 UTC 2020
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/21/2020 06:17:37 MDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE100

Active Alarms (past 24 hours)
None found.

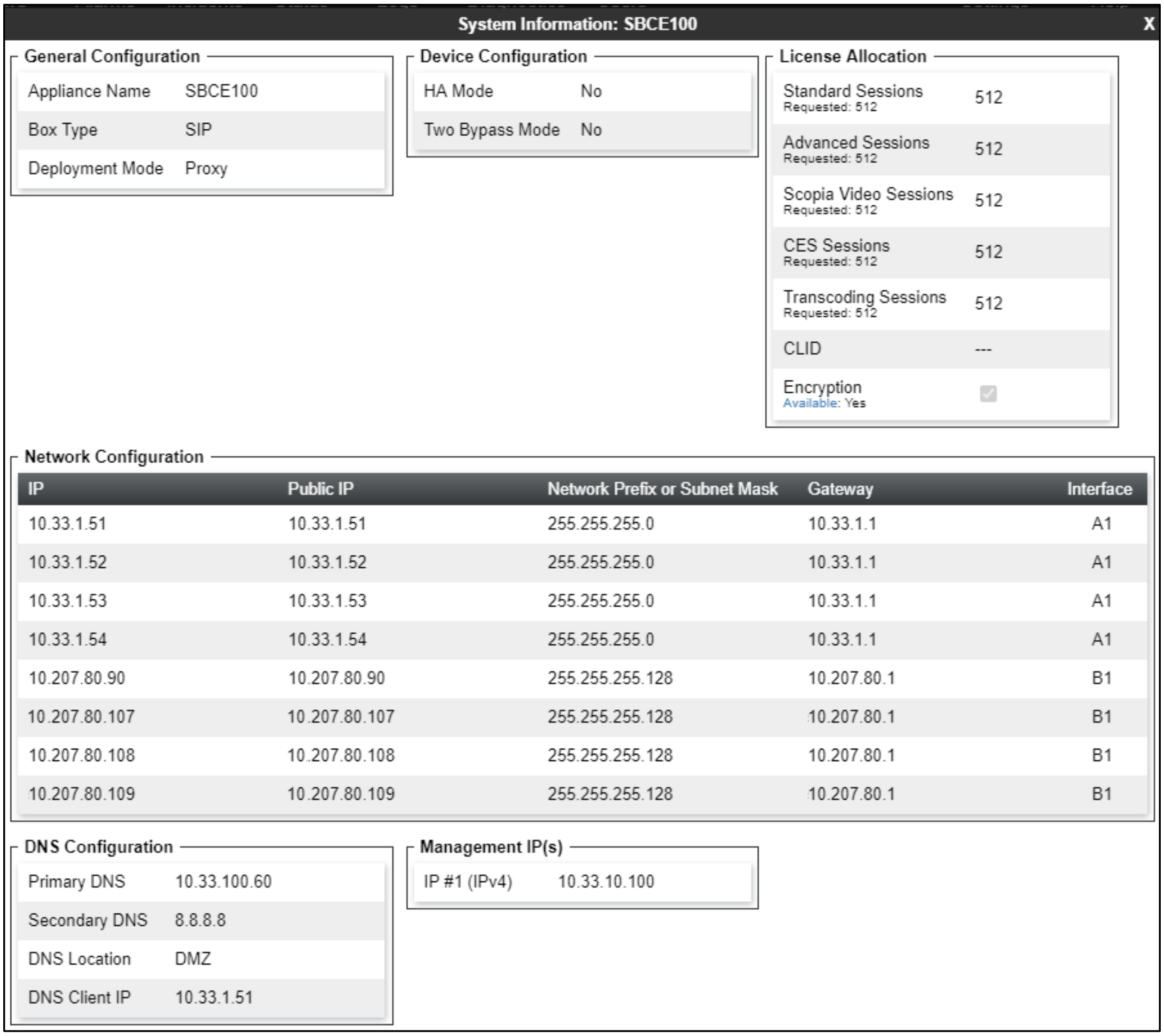
Incidents (past 24 hours)
SBCE100: Max forwards Exceeded
SBCE100: Max forwards Exceeded

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 **SBCE100** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.



Device Name	Management IP	Version	Status	
SBCE100	10.33.10.100	8.1.0.0-14-18490	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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: SBCE100

X

General Configuration

Appliance Name	SBCE100
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 512	512
Advanced Sessions Requested: 512	512
Scopia Video Sessions Requested: 512	512
CES Sessions Requested: 512	512
Transcoding Sessions Requested: 512	512
CLID	---
Encryption Available: Yes	☑

Network Configuration

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

DNS Configuration

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

Management IP(s)

IP #1 (IPv4)	10.33.10.100

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).

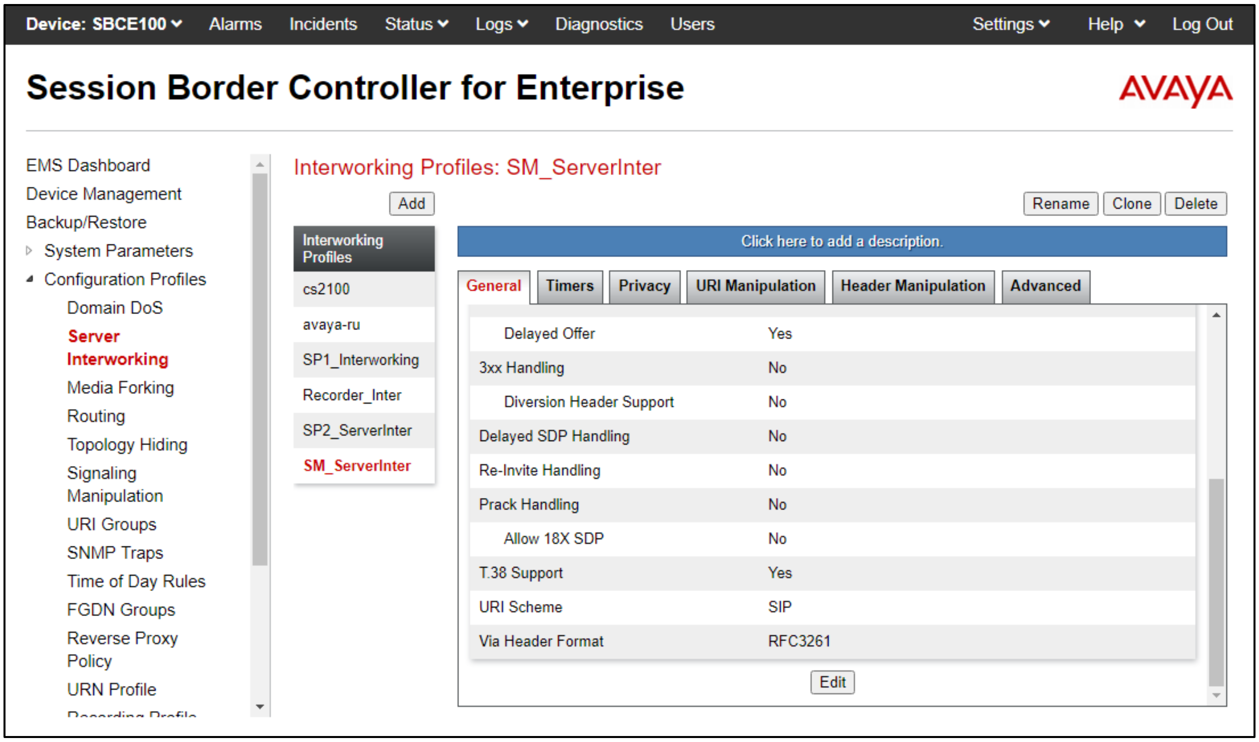
7.2.1. Configure Server Interworking Profile - Avaya Site

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**: **SM_ServerInter** and click **Finish** (not shown)
- Select **SM_ServerInter** 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 **SM_ServerInter** was added.



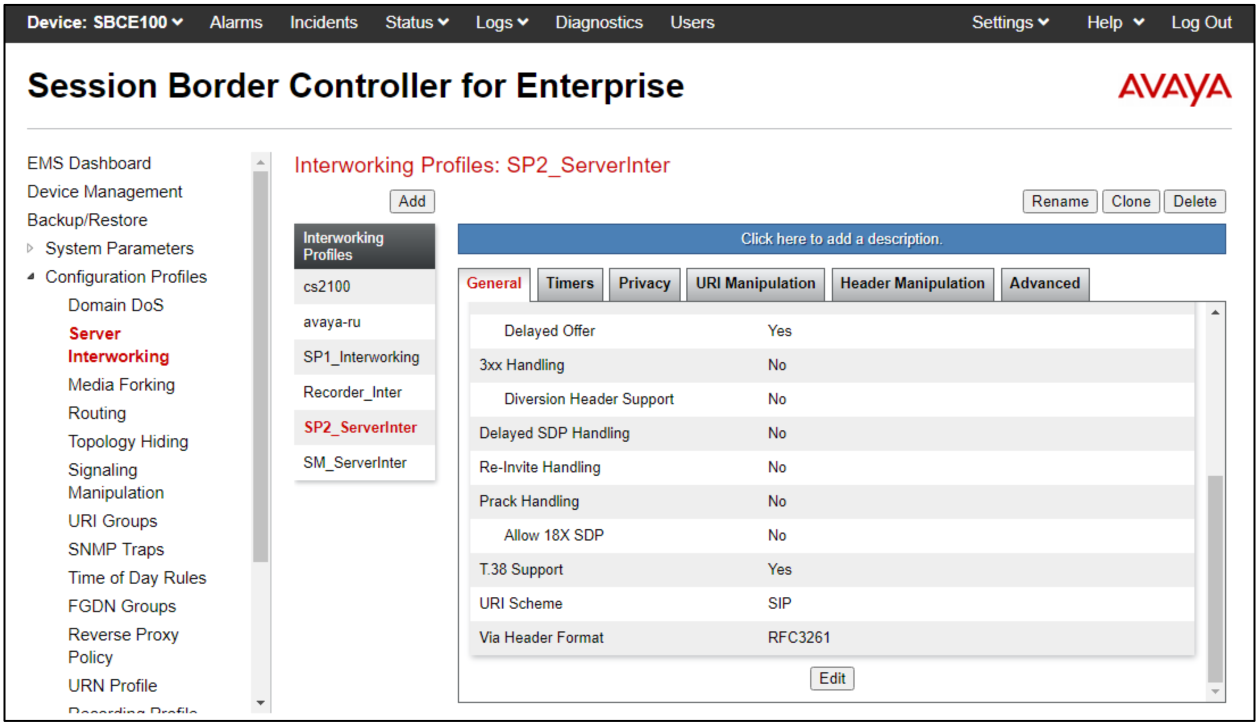
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

7.2.2. Configure Server Interworking Profile – Bell Canada SIP Trunk Site

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

- Enter **Profile Name**: **SP2_ServerInter** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)
- Select **SP2_ServerInter** in **Interworking Profiles**
- Click **Edit** button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that Bell Canada server interworking profile **SP2_ServerInter** was added.



Interworking Profiles: SP2_ServerInter

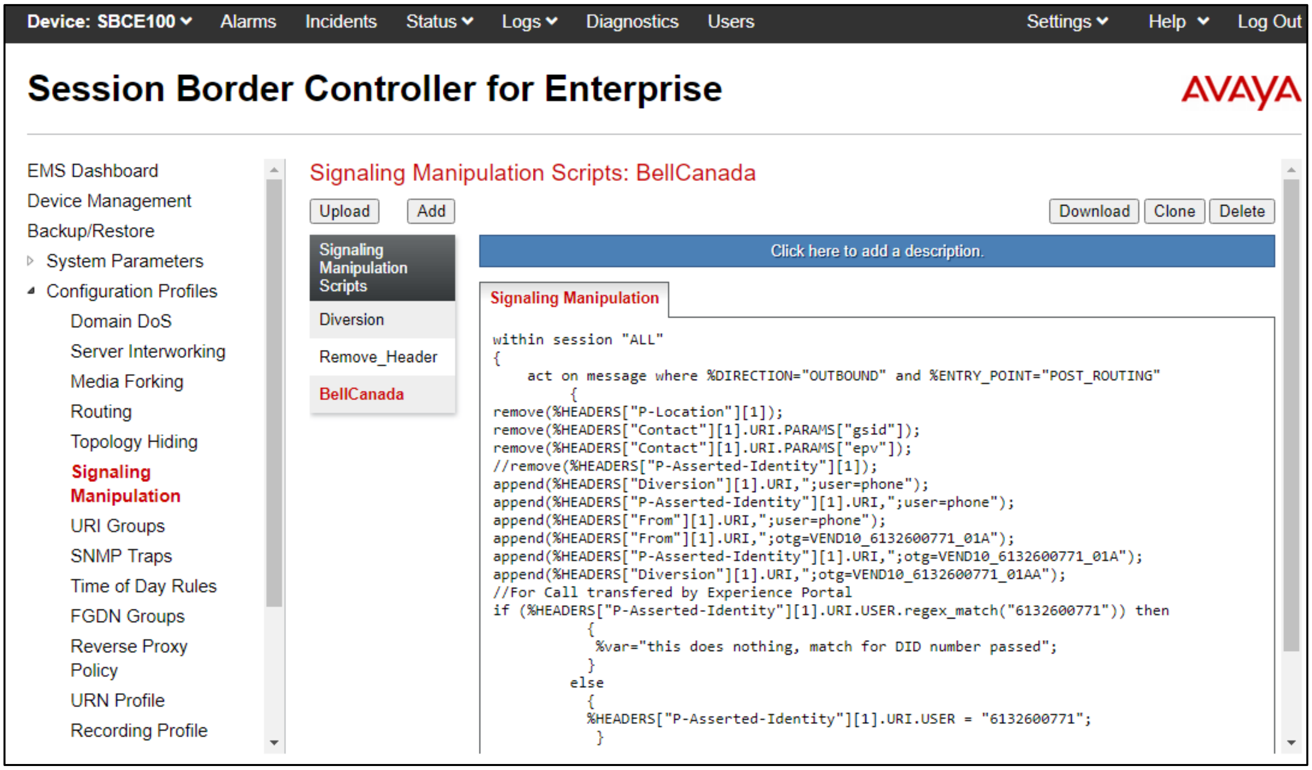
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

7.3. 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**: **BellCanada**. In the script editing window, enter the text exactly as shown in the below screenshot to perform the following:
  - Manipulate the SIP headers for outbound calls
  - Remove unwanted headers
  - Manipulate the SIP headers for ONND (Outbound Calling Name and Number Display) testing. This is optional configuration
  - Modify user of SIP URI in PAI header on off-net call forward
- Click **Save** (not shown)



```
within session "ALL"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
         {
remove(%HEADERS["P-Location"][1]);
remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
//remove(%HEADERS["P-Asserted-Identity"][1]);
append(%HEADERS["Diversion"][1].URI,";user=phone");
append(%HEADERS["P-Asserted-Identity"][1].URI,";user=phone");
append(%HEADERS["From"][1].URI,";user=phone");
append(%HEADERS["From"][1].URI,";otg=VEND10_6132600771_01A");
append(%HEADERS["P-Asserted-Identity"][1].URI,";otg=VEND10_6132600771_01A");
append(%HEADERS["Diversion"][1].URI,";otg=VEND10_6132600771_01AA");
//For Call transfered by Experience Portal
if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("6132600771")) then
           {
            %var="this does nothing, match for DID number passed";
           }
         else
           {
           %HEADERS["P-Asserted-Identity"][1].URI.USER = "6132600771";
            }
```

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

Bell Canada's Static/Dynamic ONND and Trunk Group Selection features require header manipulation in Avaya SBCE. However, this Header Manipulation is NOT required under a normal configuration. This is provided as reference configuration for this specific testing. For more details, refer to Bell Canada SIP Trunking Service Interface Specification, version 2.0.7.

For Static ONND in this compliance testing, the From, PAI and Diversion headers should always be including parameter user=phone. And for Trunk Group Selection, it is optional that the From, PAI and Diversion headers include parameter otg=trunk-group-id**.** With the presence of a Trunk Group Selection the display will be as in the From header. The display will be as in the PAI with an implicit Trunk Group Selection (i.e. without a Trunk Group Selection). Even though, these **user** and **otg** parameters are not required in the From header, it is being included in here for completeness. When using a Trunk Group Selection, the otg tag must be present in the From, PAI and Diversion headers when applicable.

Note: For multi-trunk group and geographic redundant configuration refer to document: Application Notes for Bell Canada SIP Trunking Service using Least Cost Routing with Avaya Aura® Communication Manager R6.0.1, Geographic Redundant Avaya Aura® Session Managers R6.1 and Avaya Session Border Controllers for Enterprise R4.0.5 –Issue 1.0 https://www.devconnectprogram.com/fileMedia/download/f1603e7f-a6c4-4555-bea5-3b0a8deb61e0

7.4. SIP Server Profiles

The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains

7.4.1. Configure SIP Server – Avaya Site

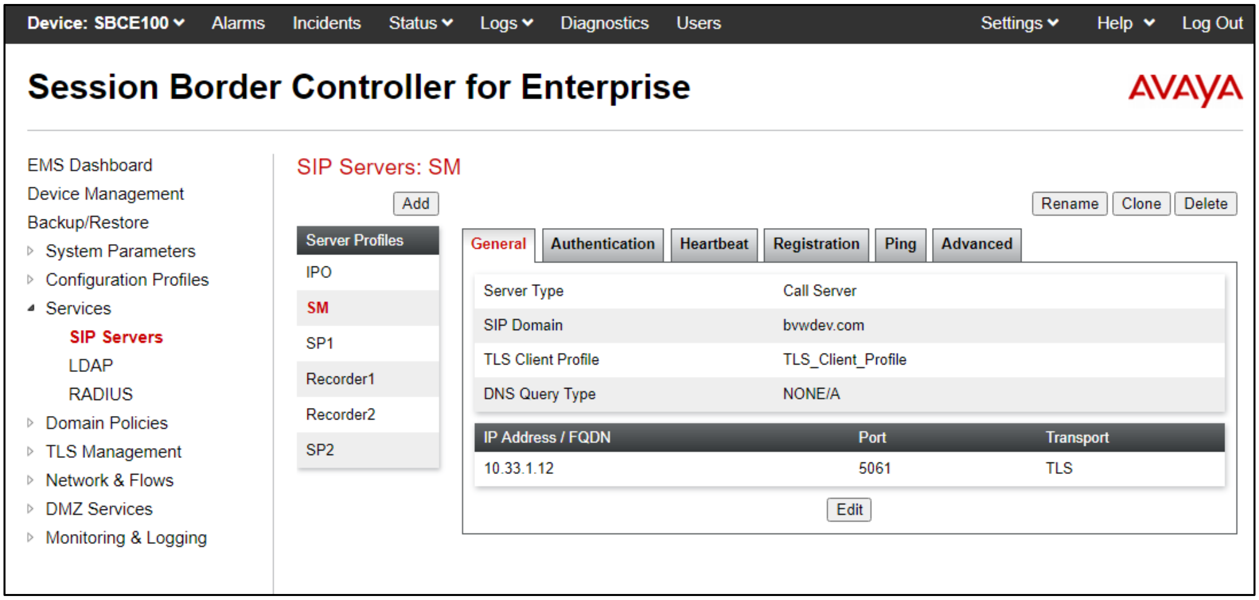
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server specific parameters such as port assignment, IP Server type, heartbeat signaling parameters and some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

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

Enter **Profile Name**: **SM**

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

- **Server Type**: Select **Call Server**
- **TLS Client Profile**: Select **TLS_Client_Profile**. Note that the TLS client profile is previously configured and not covered in this document.
- **IP Address/FQDN**: **10.33.1.12** (Session Manager IP Address)
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)



Session Border Controller for Enterprise

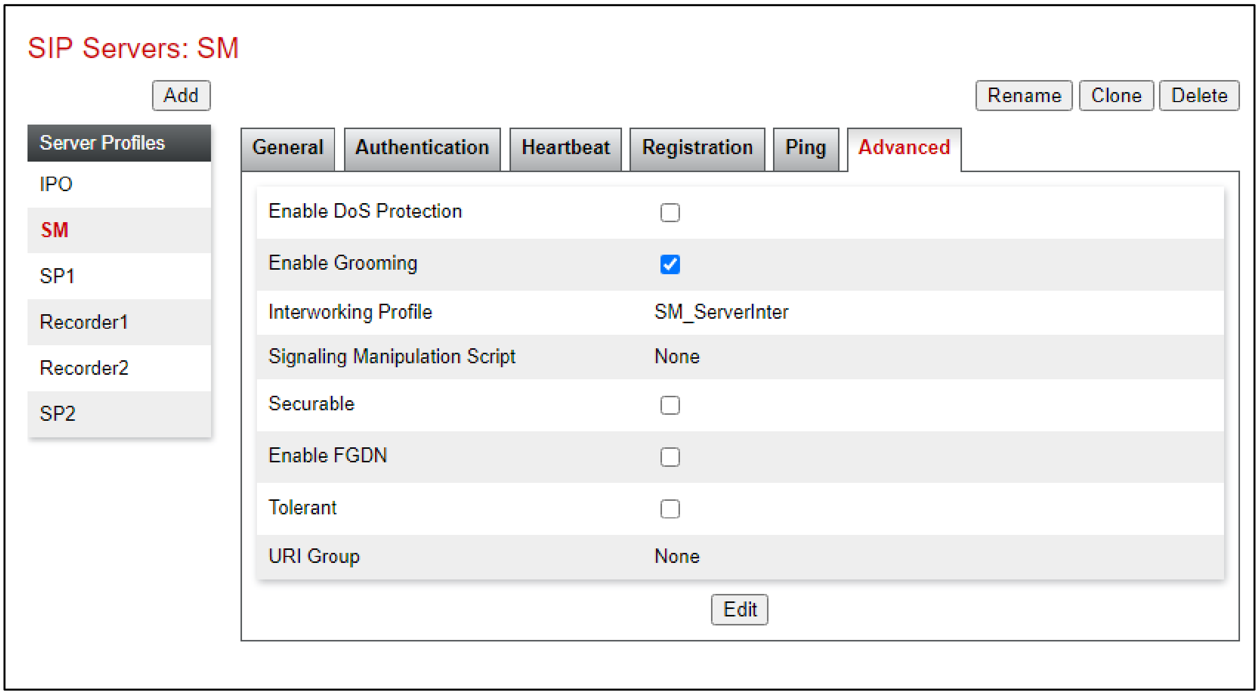
SIP Servers: SM

Server Type	Call Server
SIP Domain	bvwdev.com
TLS Client Profile	TLS_Client_Profile
DNS Query Type	NONE/A

IP Address / FQDN	Port	Transport
10.33.1.12	5061	TLS

On the **Advanced** tab:

- **Enable Grooming** box is checked
- Select **SM_ServerInter** for **Interworking Profile**
- Click **Finish** (not shown)



SIP Servers: SM

Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	SM_ServerInter
Signaling Manipulation Script	None
Securable	☐
Enable FGDN	☐
Tolerant	☐
URI Group	None

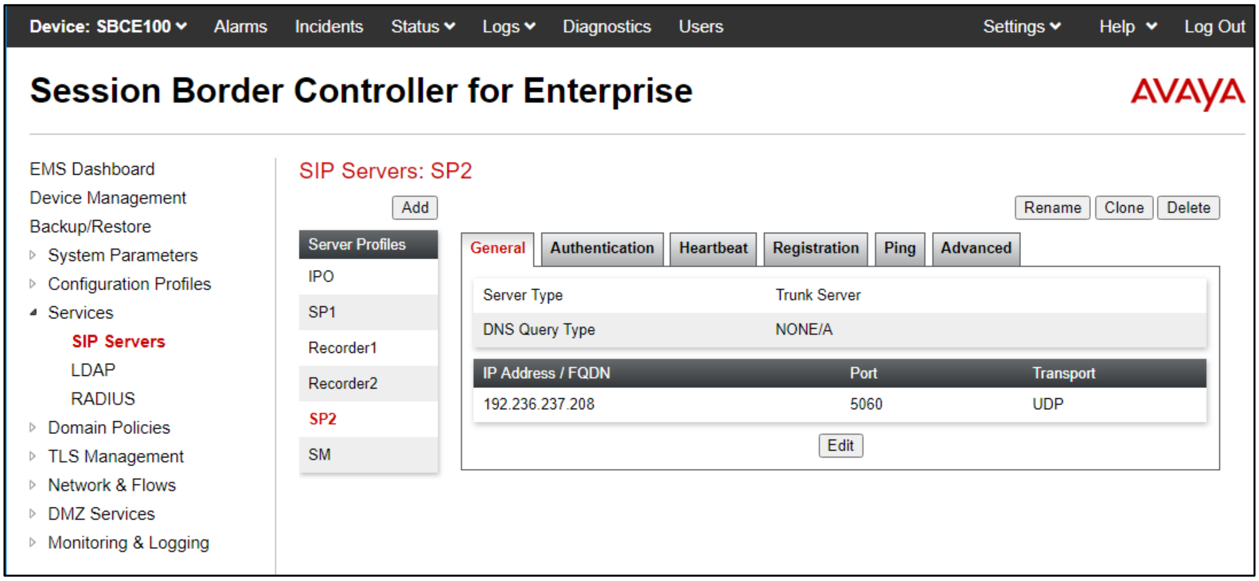
7.4.2. Configure SIP Server – Bell Canada SIP Trunk

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

Enter **Profile Name**: **SP2**

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

- **Server Type**: Select **Trunk Server**
- **IP Address/FQDN**: **192.236.237.208** (Bell Canada SBC IP Address)
- **Port**: **5060**
- **Transport**: **UDP**
- Click **Finish** (not shown)



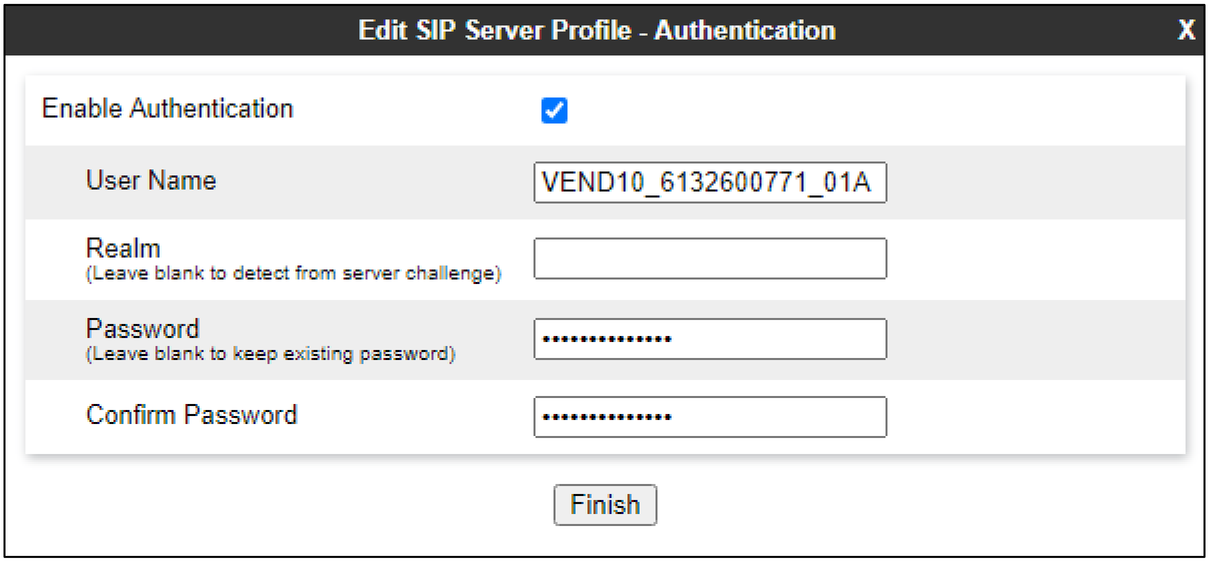
SIP Servers: SP2

Server Type	Trunk Server
DNS Query Type	NONE/A

IP Address / FQDN	Port	Transport
192.236.237.208	5060	UDP

On **Authentication** tab, click **Edit** button (not shown) to enter the following:

- Check **Enable Authentication**
- Input **User Name**: Bell Canada provided this information
- Input **Password:** Bell Canada provided this information
- Input **Confirm Password:** Bell Canada provided this information
- Click **Finish** button



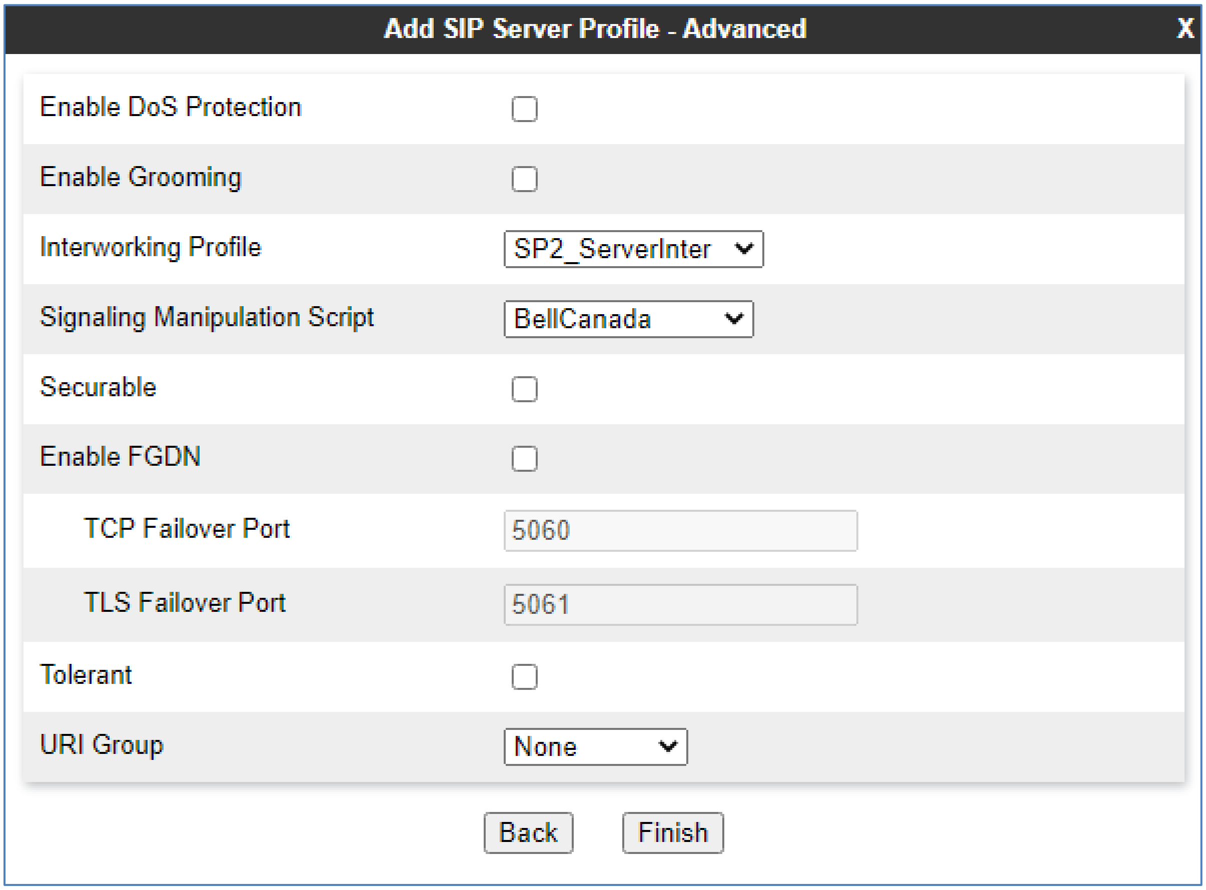
Edit SIP Server Profile - Authentication

Enable Authentication	☑
User Name	VEND10_6132600771_01A
Realm (Leave blank to detect from server challenge)	
Password (Leave blank to keep existing password)	••••••••••••••
Confirm Password	••••••••••••••

On **Heartbeat** tab, leave it as default as not enabling the heartbeat so that Avaya SBCE will forward the OPTIONS message from Session Manager to Bell Canada.

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

- **Interworking Profile**: select **SP2_ServerInter**
- **Signaling Manipulation Script**: select **BellCanada** sigma script
- Click **Finish**



Add SIP Server Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP2_ServerInter
Signaling Manipulation Script	BellCanada
Securable	□
Enable FGDN	□
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	□
URI Group	None

7.5. Routing Profiles

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

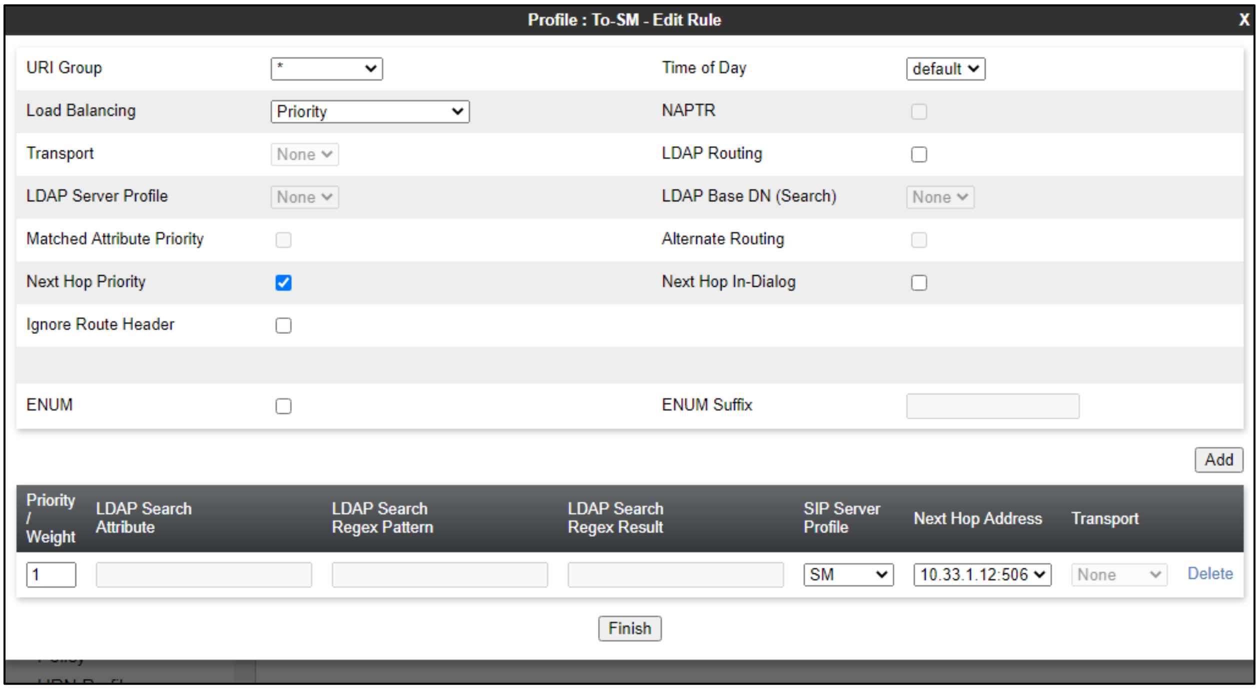
7.5.1. Configure Routing – Avaya Site

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

Enter **Profile Name**: **To-SM** and click **Next** button (Not Shown)

- Select **Load Balancing**: select **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a SIP Server Profile
- **Priority/Weight**: **1**
- **SIP Server Profile**: select **SM** from the dropdown menu, the Session Manager IP address is auto filled in the Next Hop Address
- Click **Finish**

Note that the screenshot below shows the **Edit Rule** of the Session Manager routing.



Profile : To-SM - Edit 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	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SM	10.33.1.12:506	None	Delete

7.5.2. Configure Routing – Bell Canada SIP Trunk Site

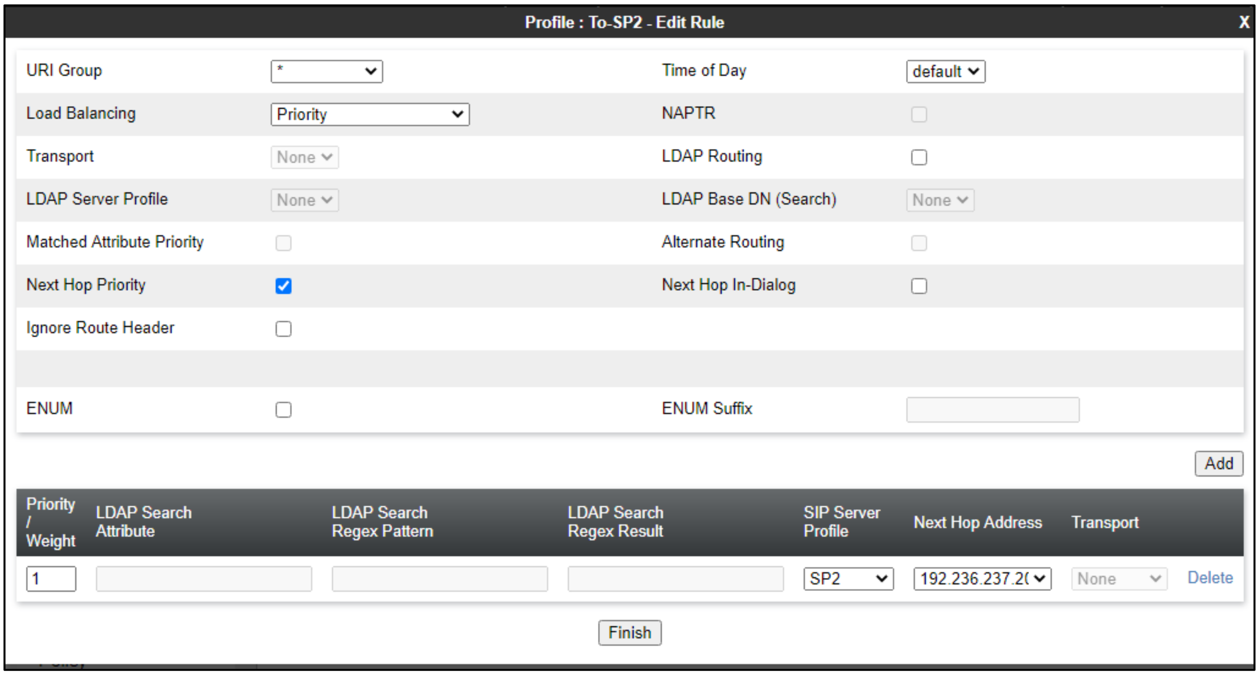
The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

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

Enter **Profile Name**: **To-SP2** and click **Next** button (Not Shown)

- Select **Load Balancing**: select **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a SIP Server Profile
- **Priority/Weight**: **1**
- **SIP Server Profile**: select **SP2** from the dropdown menu, the Bell Canada IP address is auto filled in the **Next Hop Address** field
- Click **Finish**

Note that the screenshot below shows the **Edit Rule** of the Bell Canada routing.



Profile : To-SP2 - Edit 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	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SP2	192.236.237.2(	None	Delete

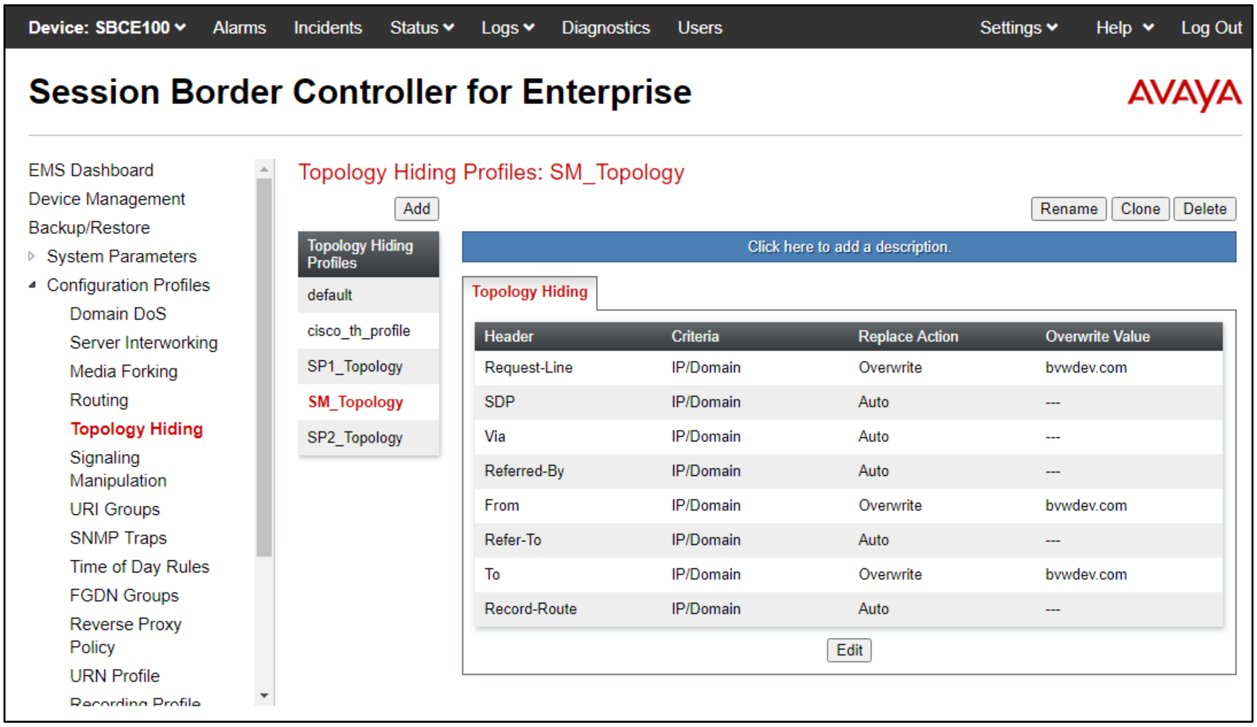
7.6. Configure Topology Hiding

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

From the menu on the left-hand side, select **Configuration Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **SM_Topology** and click **Finish** (not shown)
- Select **SM_Topology** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- In the Headers **Request-Line**, **From** and **To**: enter the following values. Note that the SIP domain bvwdev.com is the enterprise SIP domain configured in Session Manager
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**

Click **Finish** (not shown)



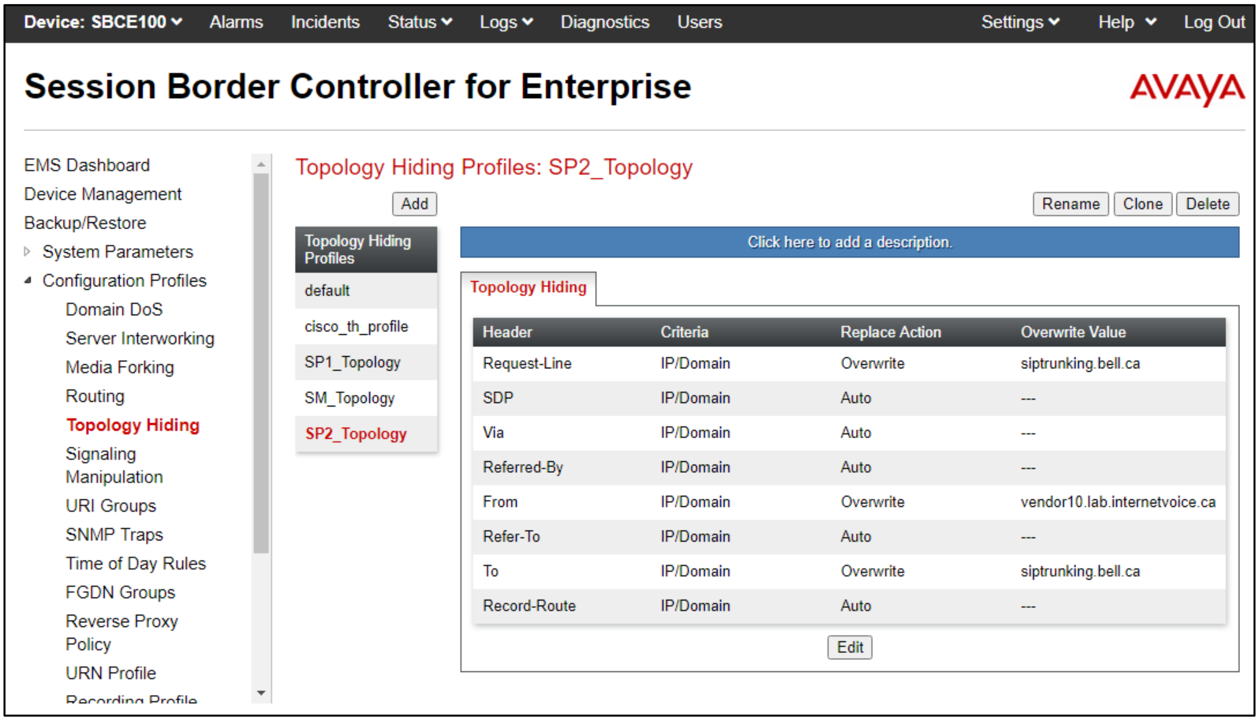
Topology Hiding Profiles: SM_Topology

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

Repeat the same procedure above to add a topology profile for Bell Canada.

- In the Headers **Request-Line** and **To**: enter the following values
  - In the **Criteria** column select: **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **siptrunking.bell.ca** (This is Bell Canada peer FQDN)
- In the Header **From**: enter the following values
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **vendor10.lab.internetvoice.ca** (This is customer domain)
- Click **Finish** (not shown)

Note that the customer domain **vendor10.lab.internetvoice.ca** will have the trunk ID "vendor10" removed in the **Overwrite Value** column of the **From** header for the dynamic ONND works. This is a requirement from Bell Canada.



Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	siptrunking.bell.ca
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Overwrite	vendor10.lab.internetvoice.ca
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	siptrunking.bell.ca
Record-Route	IP/Domain	Auto	---

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.

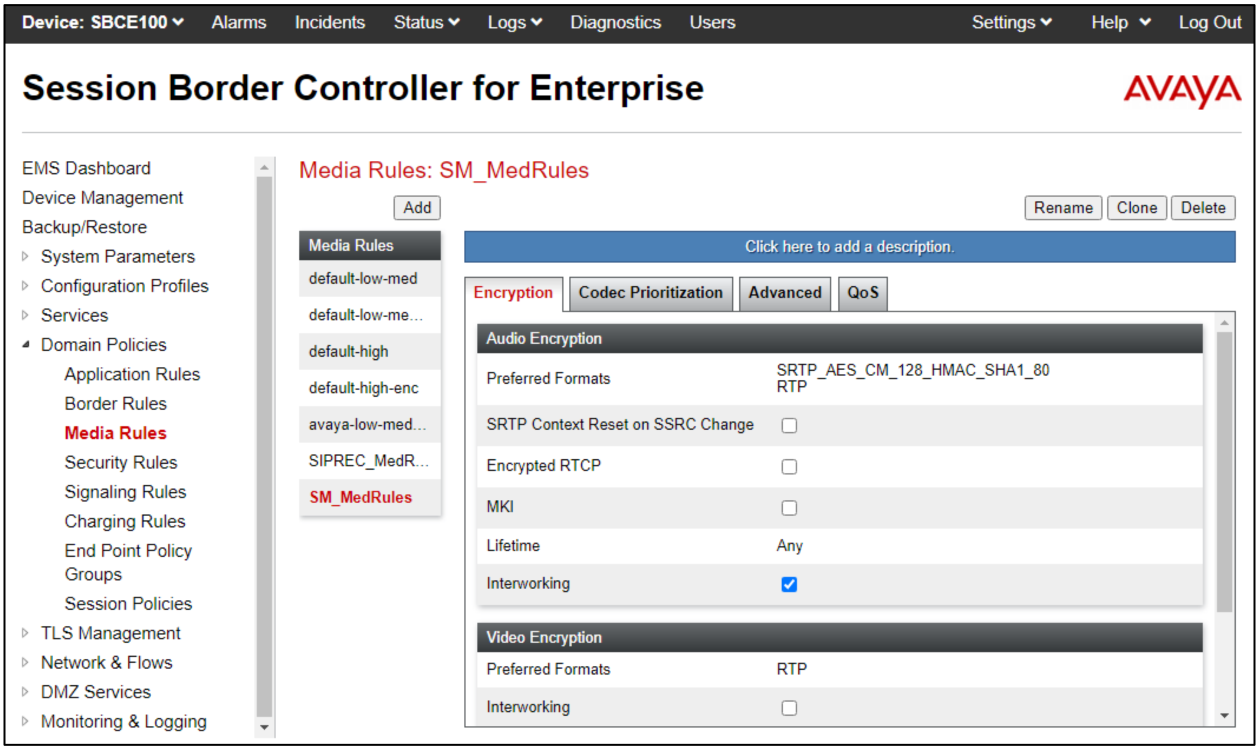
7.7.1. Create Media Rules

Media Rules allow one to define media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, the predefined **default-low-med-enc** media rule (shown below) was used to clone and edit.

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

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

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



Media Rules: SM_MedRules

Media Rules
default-low-med
default-low-me...
default-high
default-high-enc
avaya-low-med...
SIPREC_MedR...
SM_MedRules

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
SRTP Context Reset on SSRC Change	□
Encrypted RTCP	□
MKI	□
Lifetime	Any
Interworking	☑

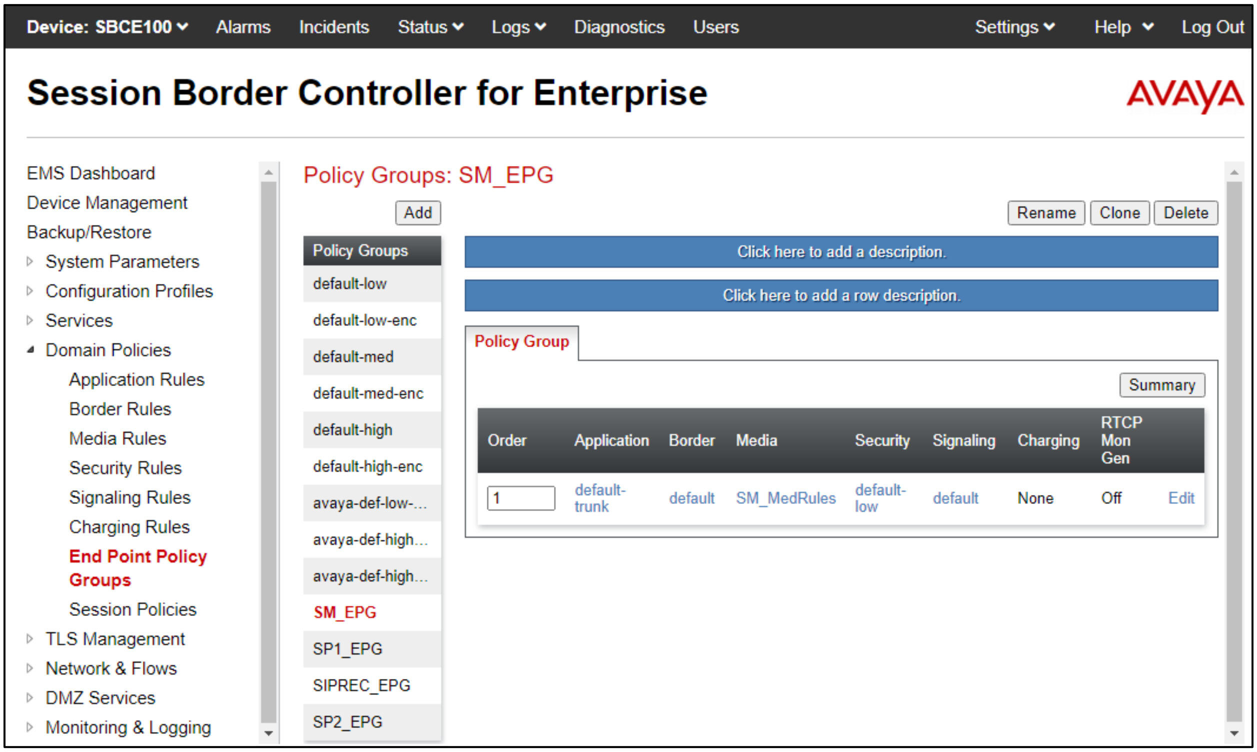
Video Encryption	
Preferred Formats	RTP
Interworking	□

7.7.2. 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, security, signaling, 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.

To add an endpoint policy group for Session Manager. From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups,** select **Add** and enter the following parameters.

- **Group Name**: **SM_EPG**
- **Application Rule**: **default-trunk**
- **Border Rule**: **default**
- **Media Rule**: **SM_MedRules**
- **Security Rule**: **default-low**
- **Signaling Rule**: **default**
- Select **Finish** (not shown)

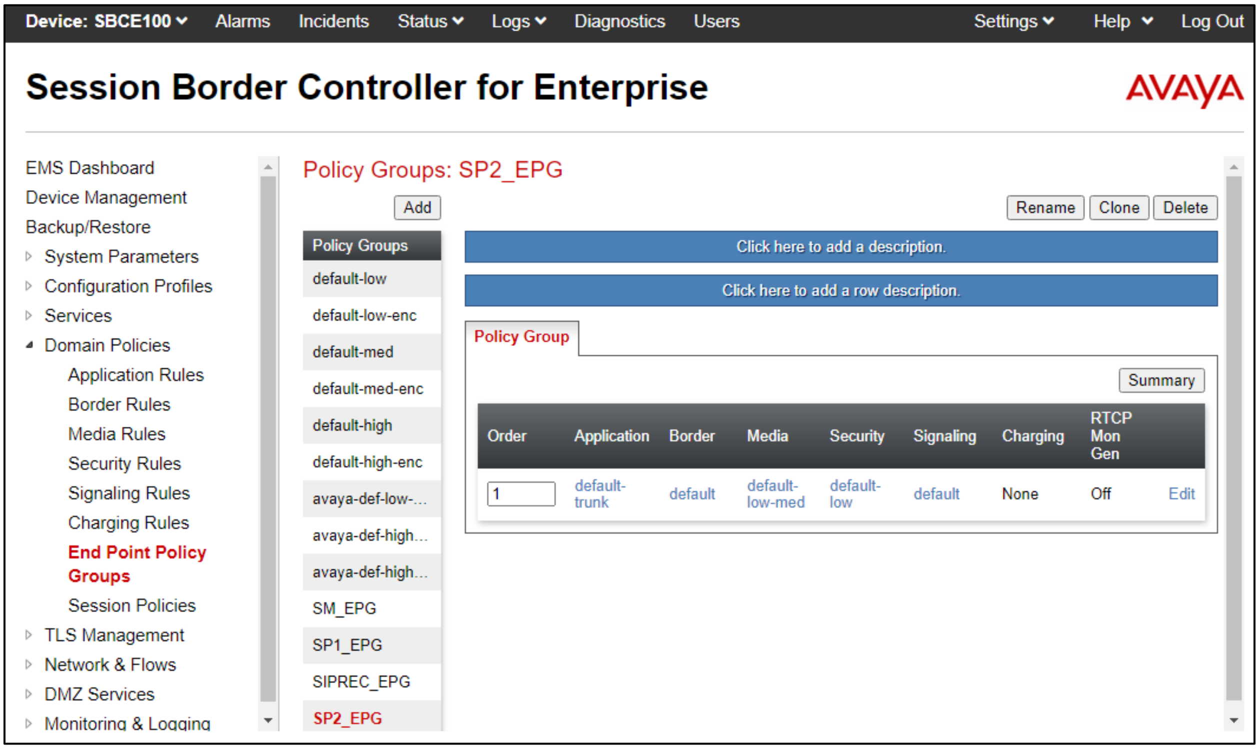


Policy Groups: SM_EPG

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default-trunk	default	SM_MedRules	default-low	default	None	Off	Edit

Repeat the same procedure above to add an end point policy for Bell Canada.

- **Group Name**: **SP2_EPG**
- **Application Rule**: **default-trunk**
- **Border Rule**: **default**
- **Media Rule**: **default**
- **Security Rule**: **default-low**
- **Signaling Rule**: **default**
- Select **Finish** (not shown)



Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default-trunk	default	default-low-med	default-low	default	None	Off	Edit

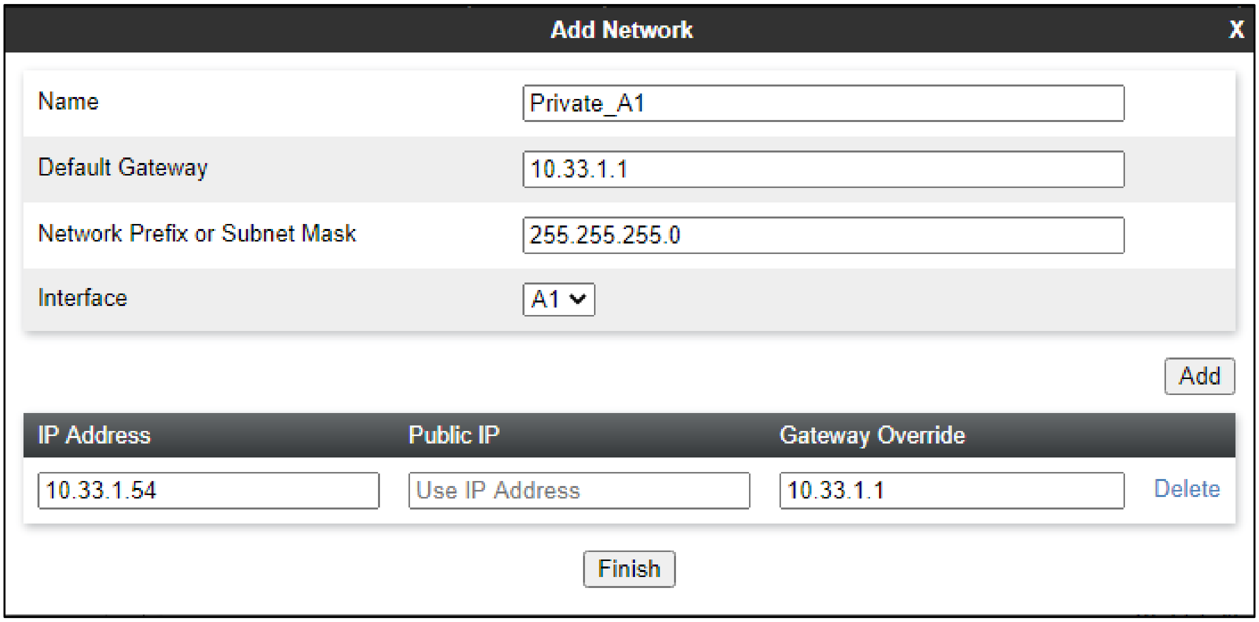
7.8. Network & Flows

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**: **Private_A1**
- **Default Gateway**: **10.33.1.1**
- **Network Prefix or 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 private interface: **10.33.1.54**
- Click the **Finish** button to save the changes

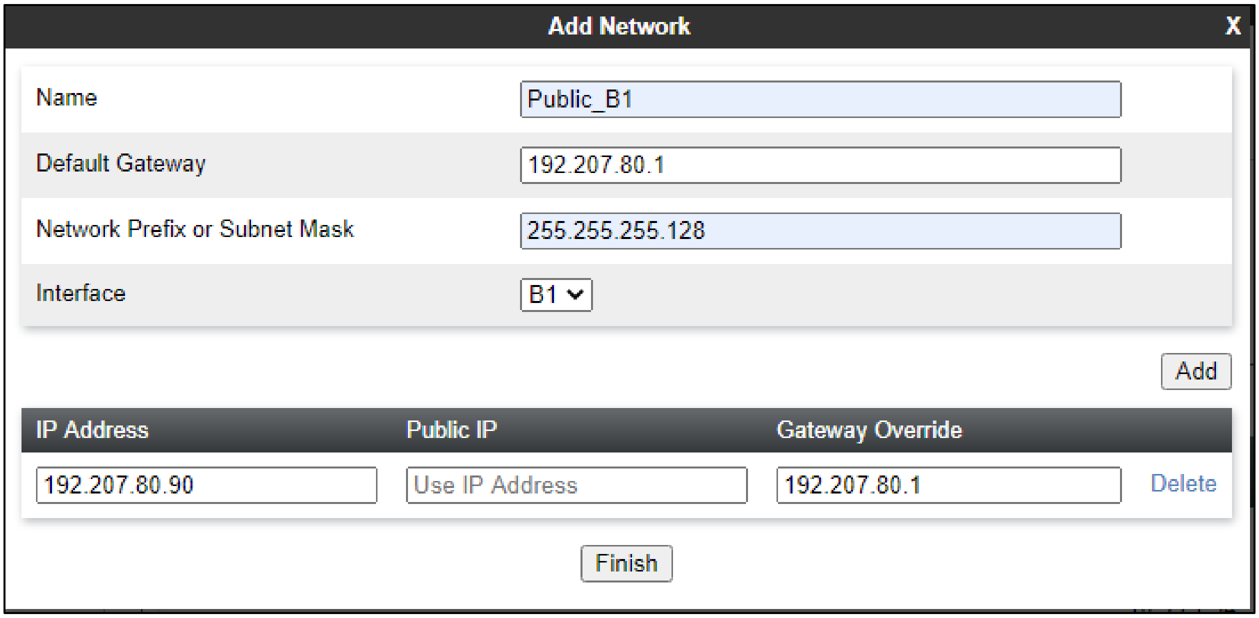


Name	Private_A1
Default Gateway	10.33.1.1
Network Prefix or Subnet Mask	255.255.255.0
Interface	A1

IP Address	Public IP	Gateway Override
10.33.1.54	Use IP Address	10.33.1.1

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**: **Public_B1**
- **Default Gateway**: **192.207.80.1**
- **Network Prefix or Subnet Mask**: **255.255.255.128**
- **Interface**: **B1** (This is the Avaya SBCE public interface)
- Click the **Add** button to add the **IP Address** for public interface: **192.207.80.90**
- Click the **Finish** button to save the changes



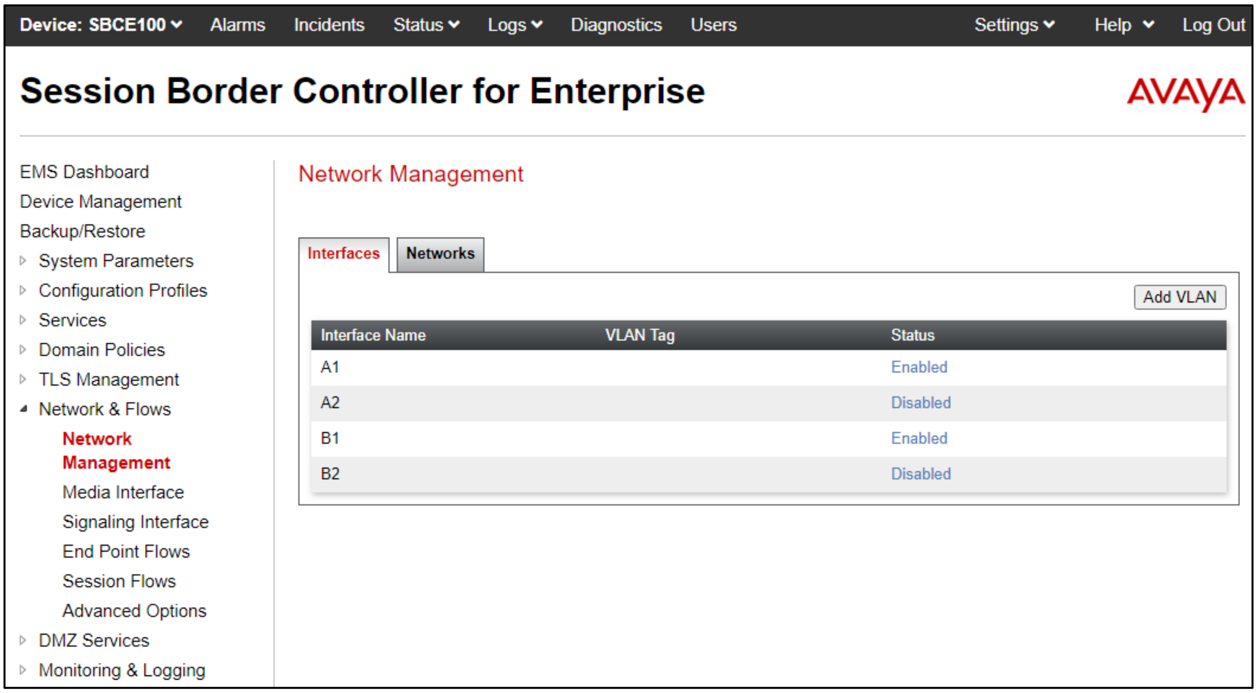
Add Network

Name	Public_B1
Default Gateway	192.207.80.1
Network Prefix or Subnet Mask	255.255.255.128
Interface	B1

IP Address	Public IP	Gateway Override	
192.207.80.90	Use IP Address	192.207.80.1	Delete

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 it to **Enabled** state



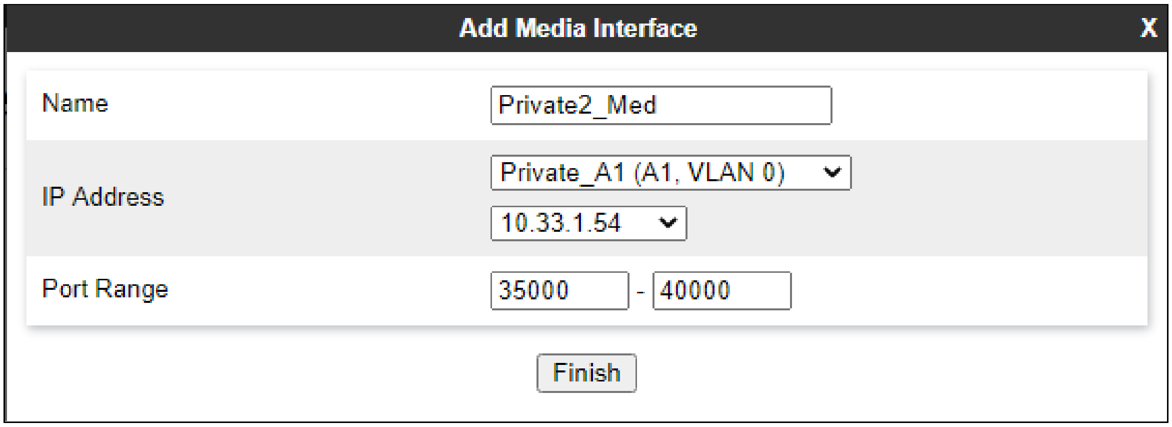
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

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 interfaces. The default media port range on the Avaya SBCE can be used.

From the menu on the left-hand side, **Network & Flows → Media Interface**. Select the **Add** button and enter the following:

- **Name: Private2_Med**
- **IP Address**: Select **Private_A1 (A1,VLAN0)** and **10.33.1.54** (Internal IP Address toward Session Manager)
- **Port Range**: **35000 – 40000**
- Click **Finish**

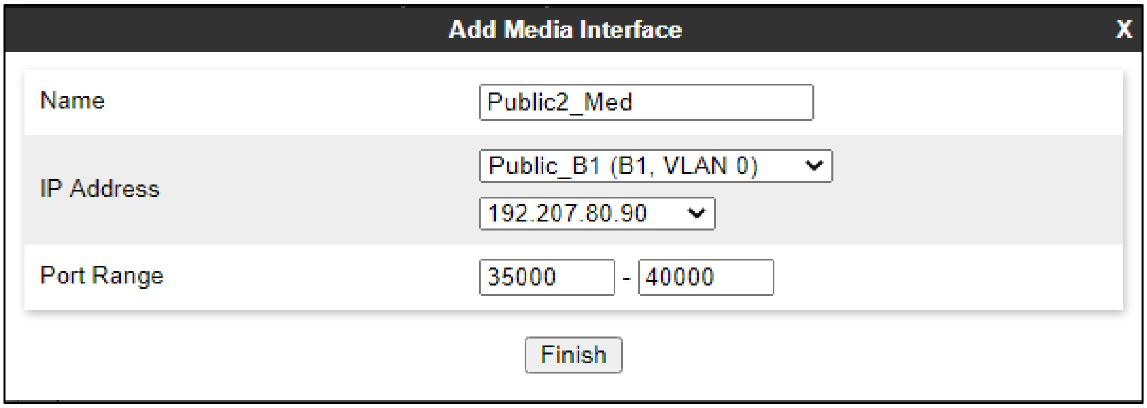


Add Media Interface

Name	Private2_Med
IP Address	Private_A1 (A1, VLAN 0) 10.33.1.54
Port Range	35000 - 40000

Do the same procedure to add the public media interface:

- **Name: Public2_Med**
- **IP Address**: Select **Public_B1 (B1,VLAN0)** and **192.207.80.90** (Public IP Address toward Bell Canada)
- **Port Range**: **35000 – 40000**
- Click **Finish**



Add Media Interface

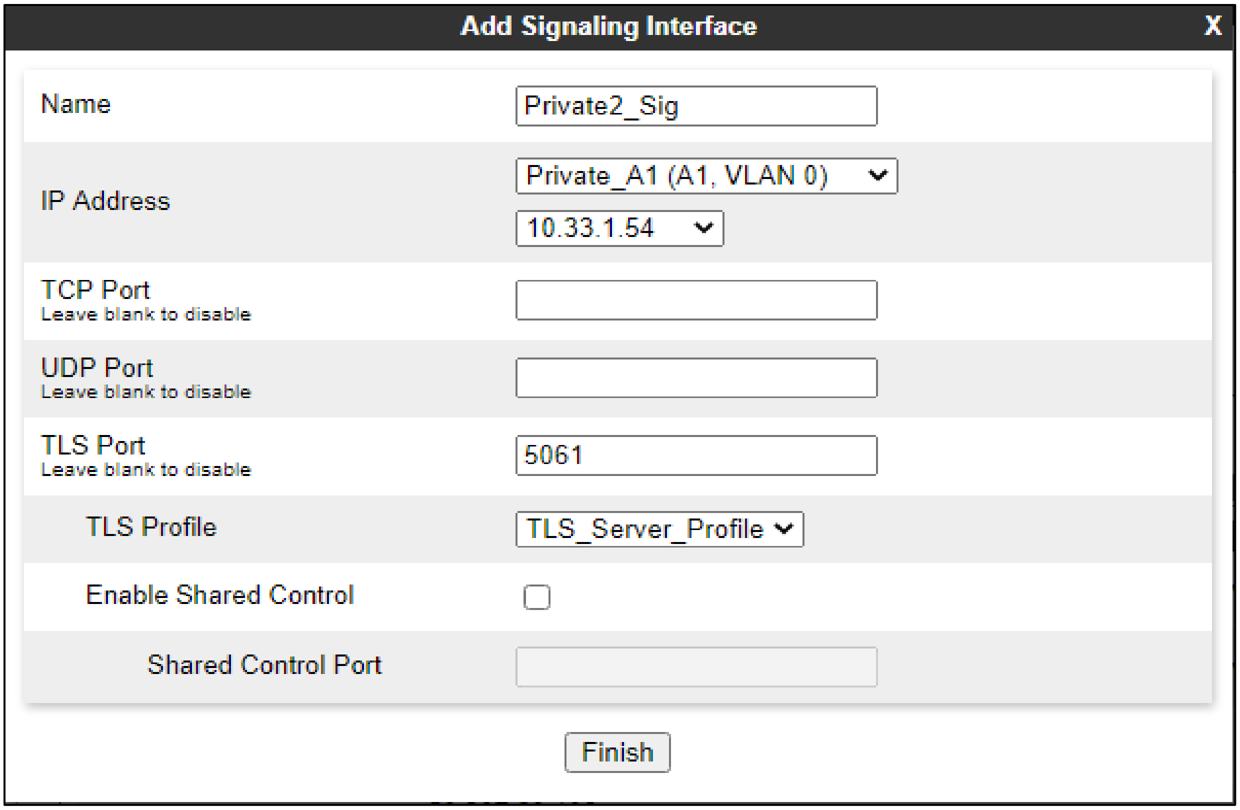
Name	Public2_Med
IP Address	Public_B1 (B1, VLAN 0) 192.207.80.90
Port Range	35000 - 40000

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: Private2_Sig**
- **IP Address**: Select **Private_A1 (A1,VLAN0)** and **10.33.1.54** (Internal IP Address toward Session Manager)
- **TLS Port**: **5061**
- **TLS Profile**: **TLS_Server_Profile**. Note that the TLS server profile is previously configured and not covered in this application note.
- Click **Finish**

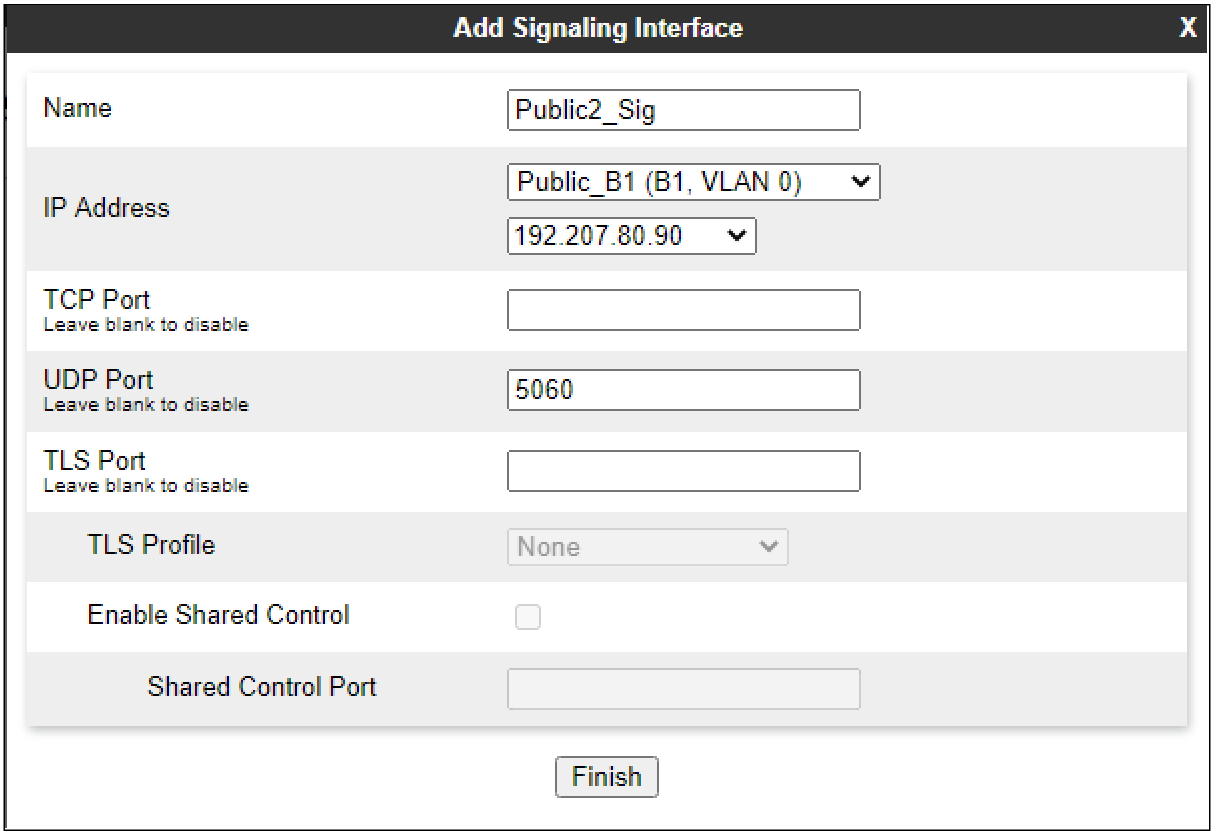


Add Signaling Interface

Name	Private2_Sig
IP Address	Private_A1 (A1, VLAN 0) 10.33.1.54
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	TLS_Server_Profile
Enable Shared Control	□
Shared Control Port	

Do the same procedure above to add the public signaling interface.

- **Name: Public2_Sig**
- **IP Address**: Select **Public_B1 (B1,VLAN0)** and **192.207.80.90** (External IP Address toward Bell Canada)
- **UDP Port**: **5060**
- Click **Finish**



Name	Public2_Sig
IP Address	Public_B1 (B1, VLAN 0) 192.207.80.90
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
TLS Profile	None
Enable Shared Control	□
Shared Control Port	

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

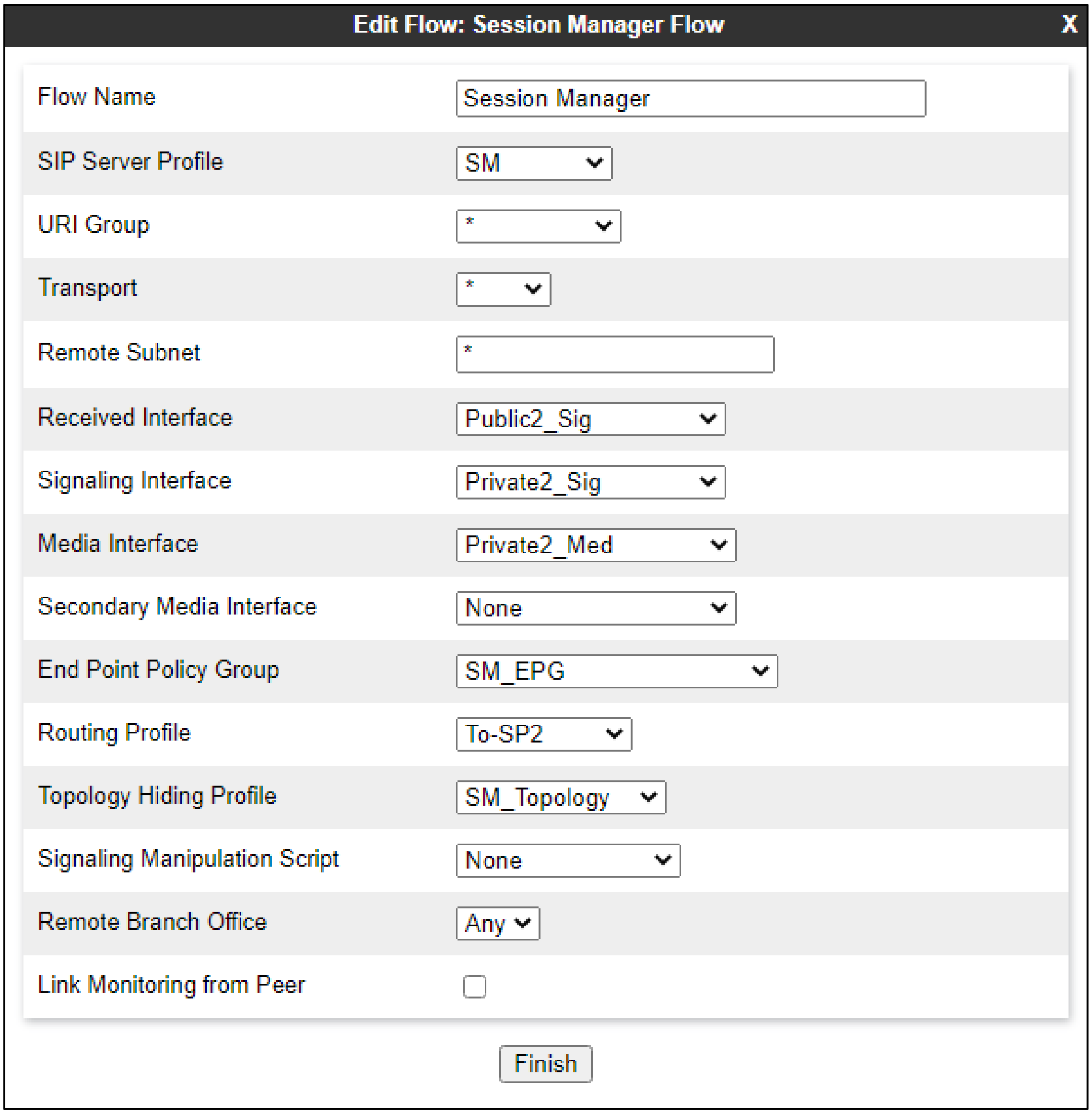
7.8.4. Configuration Server Flows

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

7.8.4.1 Create End Point Flows – Session Manager Flow

From the menu on the left-hand side, select **Network & Flows → End Point Flows.** Select the **Server Flows** tab and Select **Add** button (not shown):

- **Flow Name**: **Session Manager**
- **SIP Server Profile**: **SM** (see **Section 7.4.1**)
- **URI Group**, **Transport**, and **Remote Subnet** fields leave it as default
- **Received Interface**: **Public2_Sig** (see **Section7.8.3**)
- **Signaling Interface**: **Private2_Sig** (see **Section7.8.3**)
- **Media Interface**: **Private2_Med** (see **Section 7.8.2**)
- **Secondary Media Interface**: **None**
- **End Point Policy Group**: **SM_EPG** (see **Section 7.7.2**)
- **Routing Profile**: **To-SP2** (see **Section 7.5.2**)
- **Topology Hiding Profile**: **SM_Topology** (see **Section 7.6**)
- Leave other fields as default
- Click **Finish**



Edit Flow: Session Manager Flow

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

7.8.4.2 Create End Point Flows – Bell Canada SIP Trunk Flow

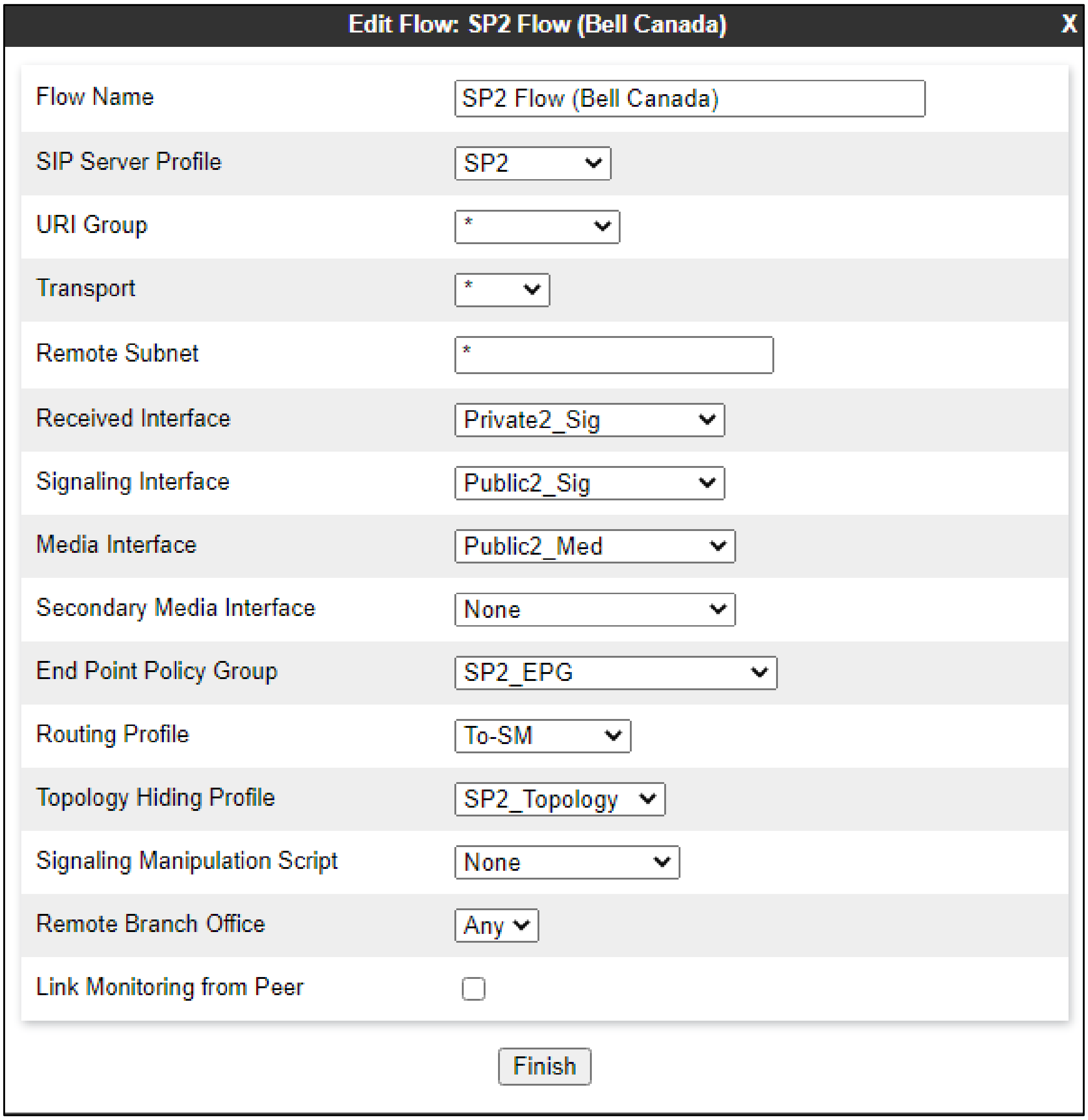
From the menu on the left-hand side, select **Network & Flows → End Point Flows.** Select the **Server Flows** tab and Select **Add** button (not shown):

Flow Name: Session Manager Flow

- **SIP Server Profile: SP2 Flow (Bell Canada)**
- **URI Group**, **Transport**, and **Remote Subnet** fields leave it as default
- **Received Interface**: **Private2_Sig** (see **Section 7.8.3**)
- **Signaling Interface**: **Public2_Sig** (see **Section 7.8.3**)
- **Media Interface**: **Public2_Med** (see **Section 7.8.2**)
- **Secondary Media Interface**: **None**
- **End Point Policy Group**: **SP2_EPG** (see **Section 7.7.2**)
- **Routing Profile**: **To-SP2** (see **Section 7.5.1**)

- **Topology Hiding Profile**: **SP2_Topology** (see **Section 7.6**)
- Leave other fields as default

Click **Finish**



Edit Flow: SP2 Flow (Bell Canada)

Flow Name	SP2 Flow (Bell Canada)
SIP Server Profile	SP2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private2_Sig
Signaling Interface	Public2_Sig
Media Interface	Public2_Med
Secondary Media Interface	None
End Point Policy Group	SP2_EPG
Routing Profile	To-SM
Topology Hiding Profile	SP2_Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□

8. Configure Avaya Aura® Experience Portal

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

8.1. Background

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

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

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

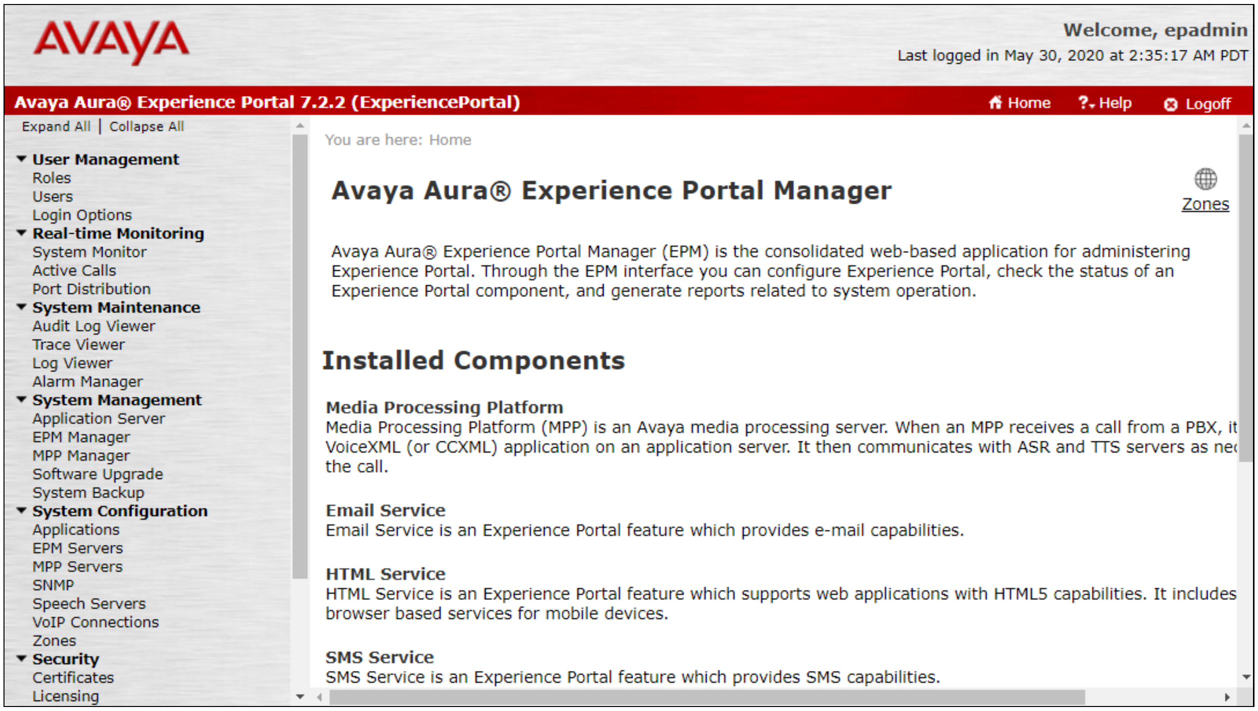
[1] An application may be configured with "inbound default" as the called number, to process all inbound calls that do not match any other application references.

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.



Welcome, epadmin

Last logged in May 30, 2020 at 2:35:17 AM PDT

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)

Avaya Aura® Experience Portal Manager

Avaya Aura® Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

Installed Components

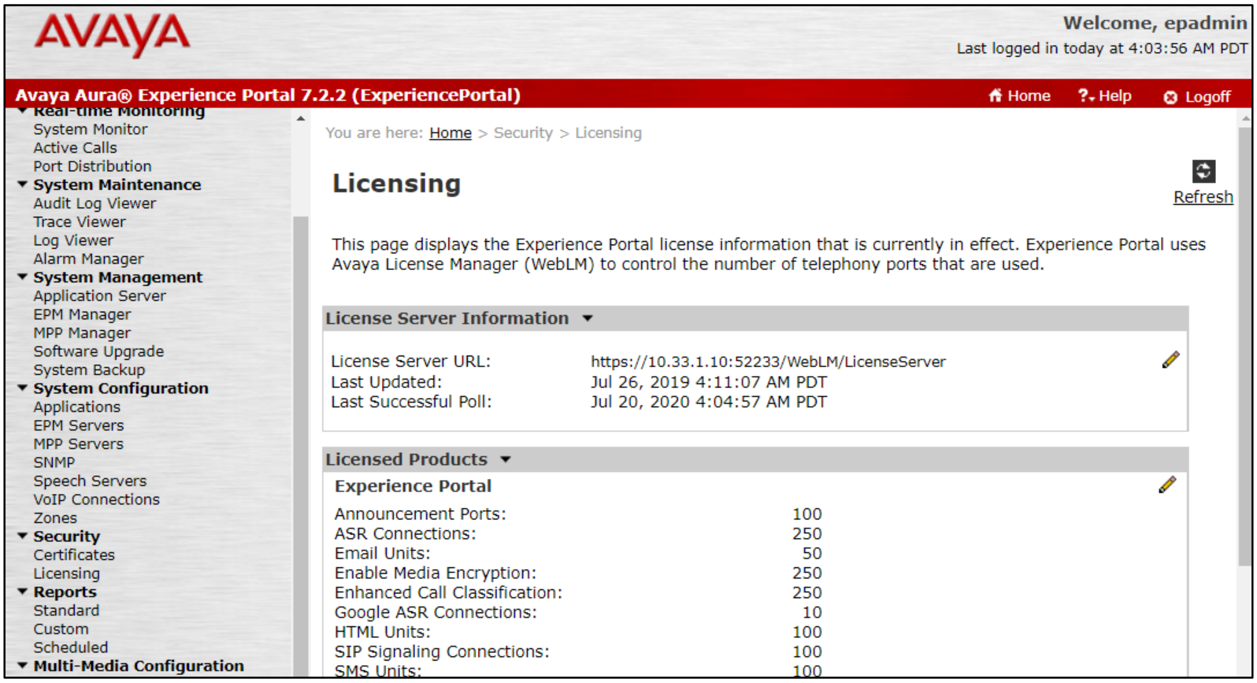
Media Processing Platform
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as nec the call.

Email Service
Email Service is an Experience Portal feature which provides e-mail capabilities.

HTML Service
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes browser based services for mobile devices.

SMS Service
SMS Service is an Experience Portal feature which provides SMS capabilities.

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.



Licensing

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

License Server Information

License Server URL:	https://10.33.1.10:52233/WebLM/LicenseServer
Last Updated:	Jul 26, 2019 4:11:07 AM PDT
Last Successful Poll:	Jul 20, 2020 4:04:57 AM PDT

Licensed Products

Experience Portal

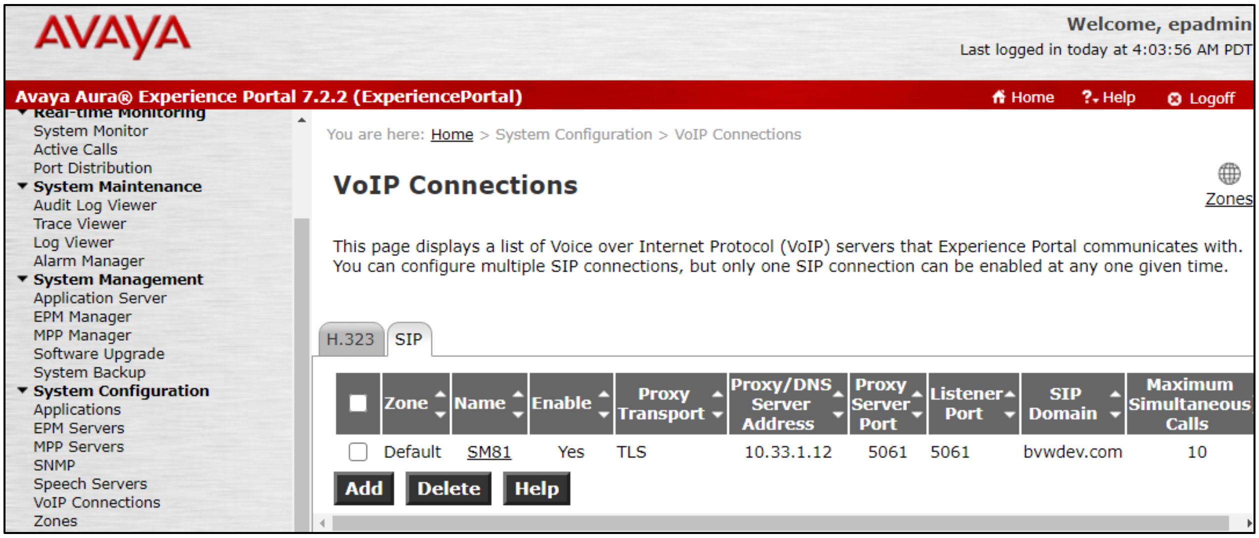
Announcement Ports:	100
ASR Connections:	250
Email Units:	50
Enable Media Encryption:	250
Enhanced Call Classification:	250
Google ASR Connections:	10
HTML Units:	100
SIP Signaling Connections:	100
SMS Units:	100

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.



VoIP Connections

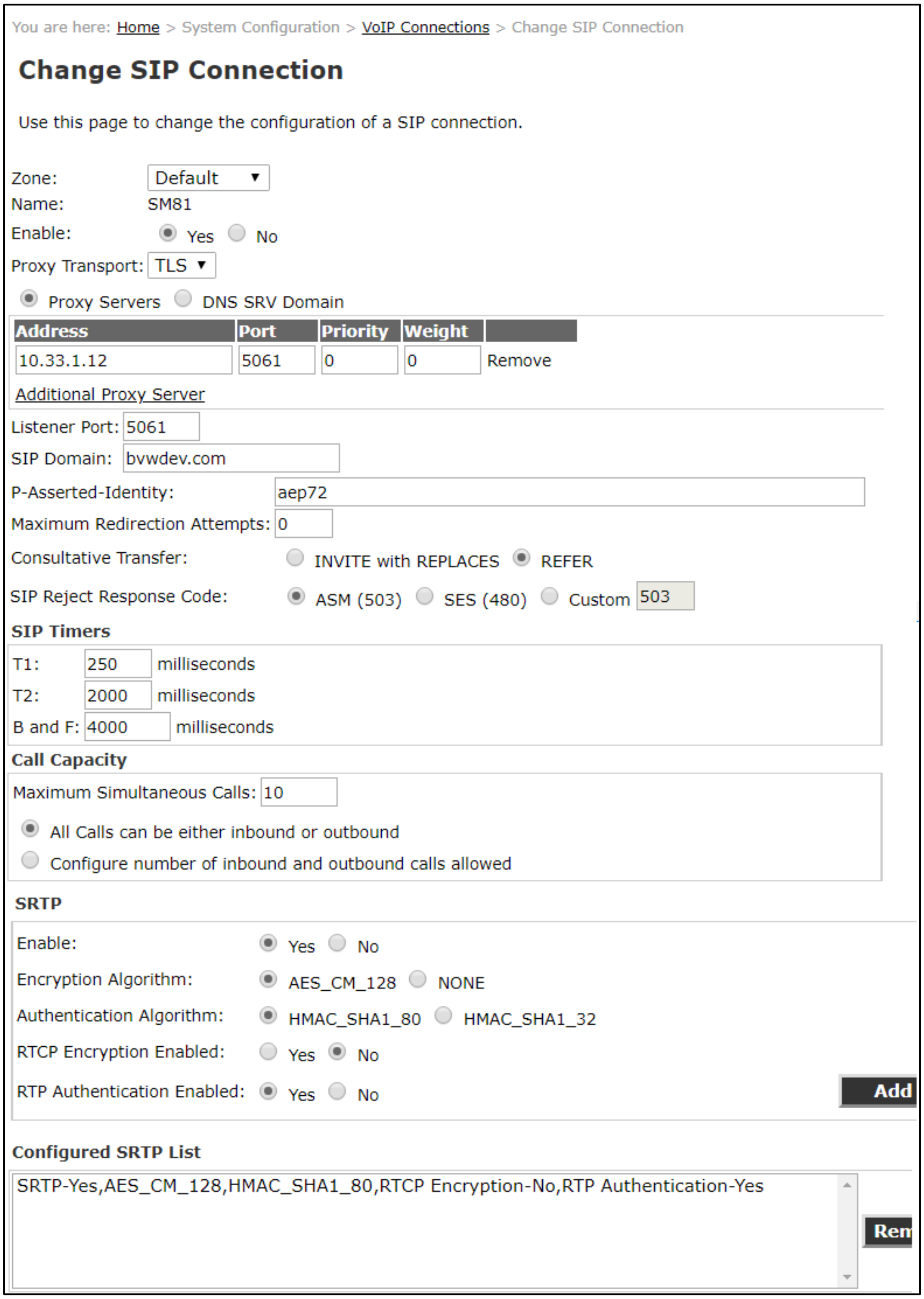
This page displays a list of Voice over Internet Protocol (VoIP) servers that Experience Portal communicates with. You can configure multiple SIP connections, but only one SIP connection can be enabled at any one given time.

□	Zone	Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls
□	Default	SM81	Yes	TLS	10.33.1.12	5061	5061	bvwdev.com	10

Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **EP_SIP**).
- **Enable** – Set to **Yes**. mnvv
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
    - **Proxy Server Address** = **10.33.1.12** (the IP address of the Session Manager signaling interface defined in **Section 7.5**).
    - **Port** = **5061**
    - **Priority** = **0** (default)
    - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **bvwdev.com** (see **Section 7.2)**.
- **Consultative Transfer** – Select **REFER**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **100** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES_CM_128**
- **Authentication Algorithm** = **HMAC_SHA1_80**

- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- Click on **Add** to add SRTP settings to the **Configured SRTP List**
- Use default values for all other fields.
- Click **Save**.



You are here: Home > System Configuration > VoIP Connections > Change SIP Connection

Change SIP Connection

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

Zone: Default ▾
Name: SM81
Enable: ● Yes ○ No
Proxy Transport: TLS ▾
● Proxy Servers ○ DNS SRV Domain

Address	Port	Priority	Weight	
10.33.1.12	5061	0	0	Remove

Additional Proxy Server

Listener Port: 5061
SIP Domain: bvwdev.com
P-Asserted-Identity: aep72
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

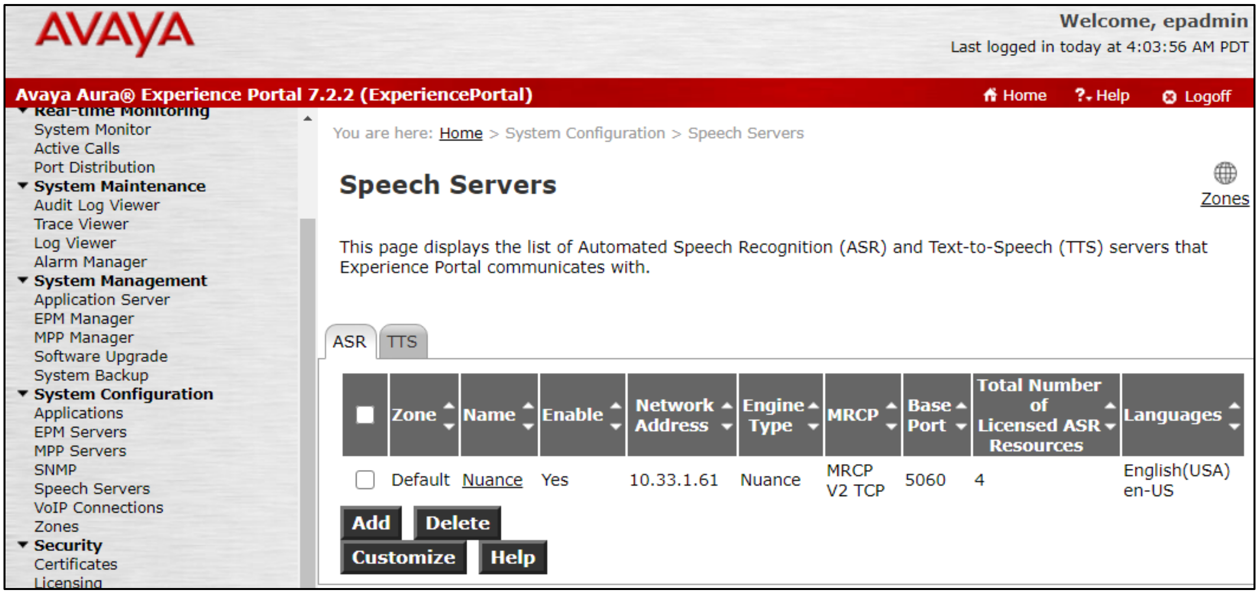
SRTP
Enable: ● Yes ○ No
Encryption Algorithm: ● AES_CM_128 ○ NONE
Authentication Algorithm: ● HMAC_SHA1_80 ○ HMAC_SHA1_32
RTCP Encryption Enabled: ○ Yes ● No
RTP Authentication Enabled: ● Yes ○ No

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

8.4. Speech Servers

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

ASR speech server:



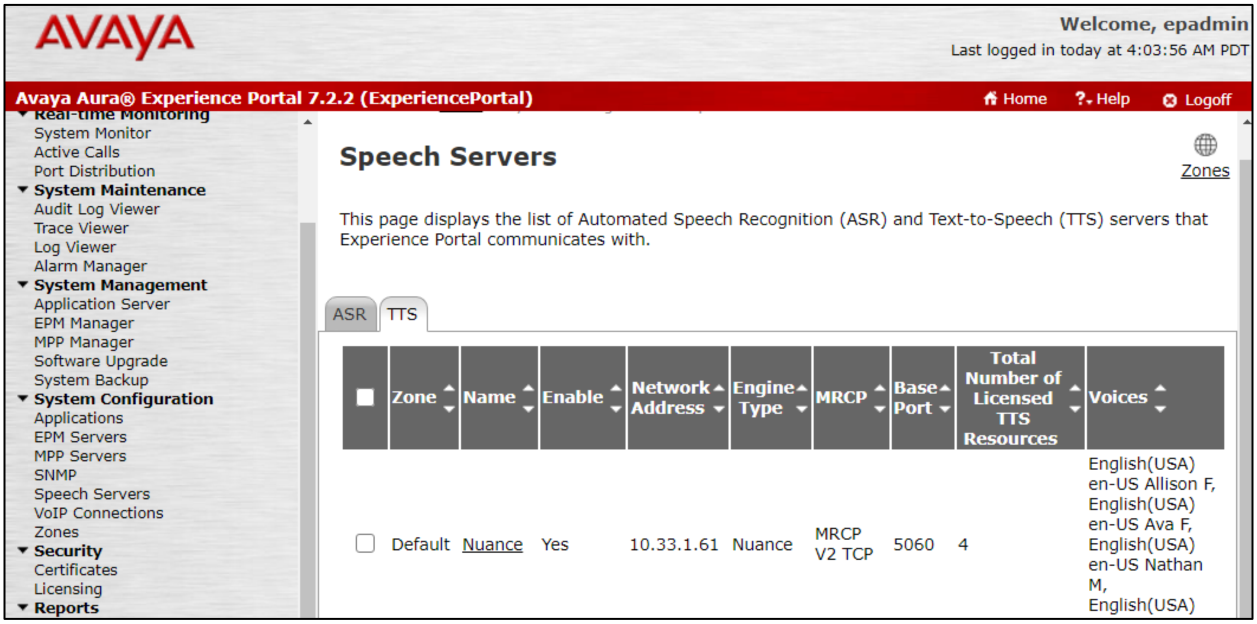
You are here: Home > System Configuration > Speech Servers

Speech Servers

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

□	Zone	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
□	Default	Nuance	Yes	10.33.1.61	Nuance	MRCP V2 TCP	5060	4	English(USA) en-US

TTS speech server:



Speech Servers

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

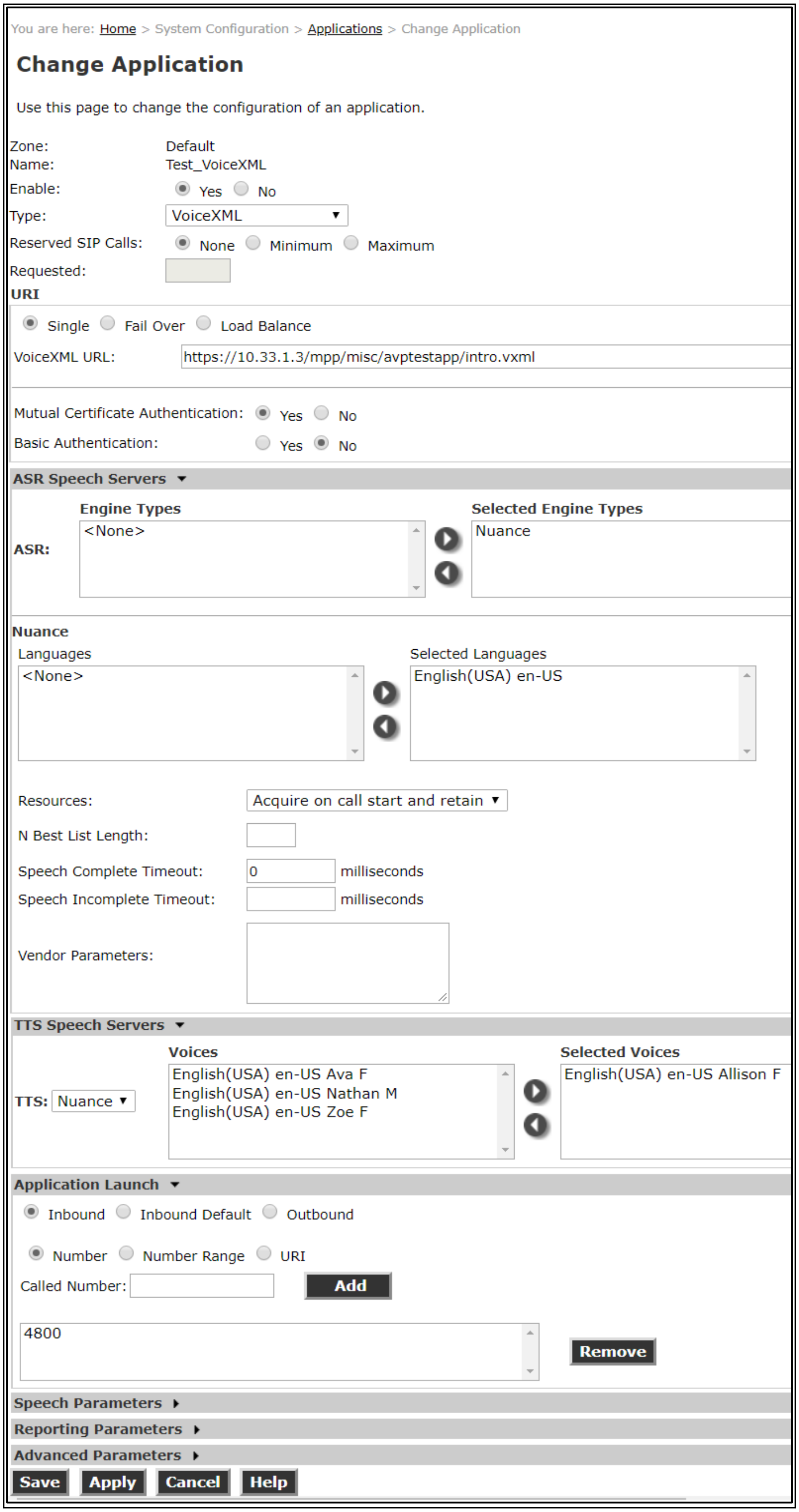
□	Zone	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed TTS Resources	Voices
□	Default	Nuance	Yes	10.33.1.61	Nuance	MRCP V2 TCP	5060	4	English(USA) en-US Allison F, English(USA) en-US Ava F, English(USA) en-US Nathan M, English(USA)

8.5. Application References

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

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

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



You are here: Home > System Configuration > Applications > Change Application

Change Application

Use this page to change the configuration of an application.

Zone:	Default
Name:	Test_VoiceXML
Enable:	● Yes ○ No
Type:	VoiceXML ▾
Reserved SIP Calls:	● None ○ Minimum ○ Maximum
Requested:	

URI

● Single ○ Fail Over ○ Load Balance

VoiceXML URL: https://10.33.1.3/mpp/misc/avptestapp/intro.vxml

Mutual Certificate Authentication: ● Yes ○ No

Basic Authentication: ○ Yes ● No

ASR Speech Servers ▾

	Engine Types	Selected Engine Types
ASR:	<None>	Nuance

Nuance

Languages	Selected Languages
<None>	English(USA) en-US

Resources: Acquire on call start and retain ▾

N Best List Length:

Speech Complete Timeout: 0 milliseconds

Speech Incomplete Timeout: milliseconds

Vendor Parameters:

TTS Speech Servers ▾

	Voices	Selected Voices
TTS: Nuance ▾	English(USA) en-US Ava F English(USA) en-US Nathan M English(USA) en-US Zoe F	English(USA) en-US Allison F

Application Launch ▾

● Inbound ○ Inbound Default ○ Outbound

● Number ○ Number Range ○ URI

Called Number: Add

4800

Remove

Speech Parameters ▸

Reporting Parameters ▸

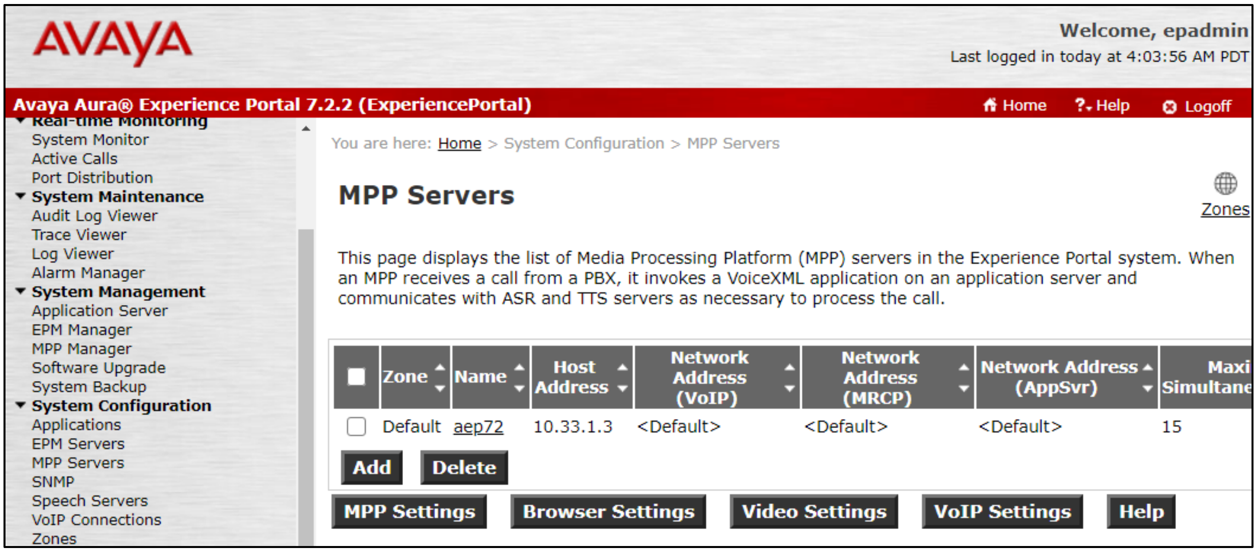
Advanced Parameters ▸

Save Apply Cancel Help

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**.



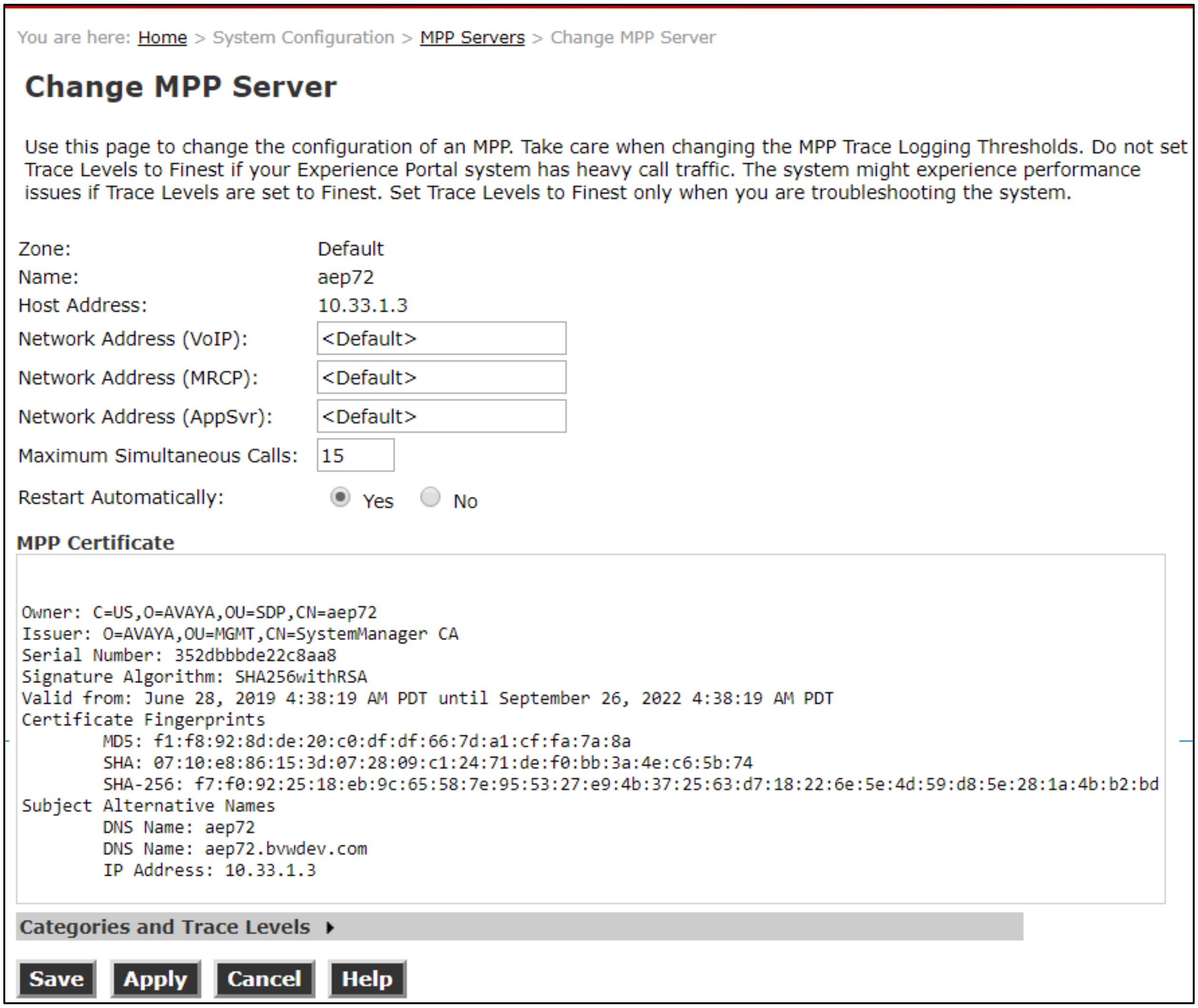
MPP Servers

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

□	Zone	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maxi Simultane
□	Default	aep72	10.33.1.3	<Default>	<Default>	<Default>	15

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

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



You are here: Home > System Configuration > MPP Servers > Change MPP Server

Change MPP Server

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

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

MPP Certificate

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

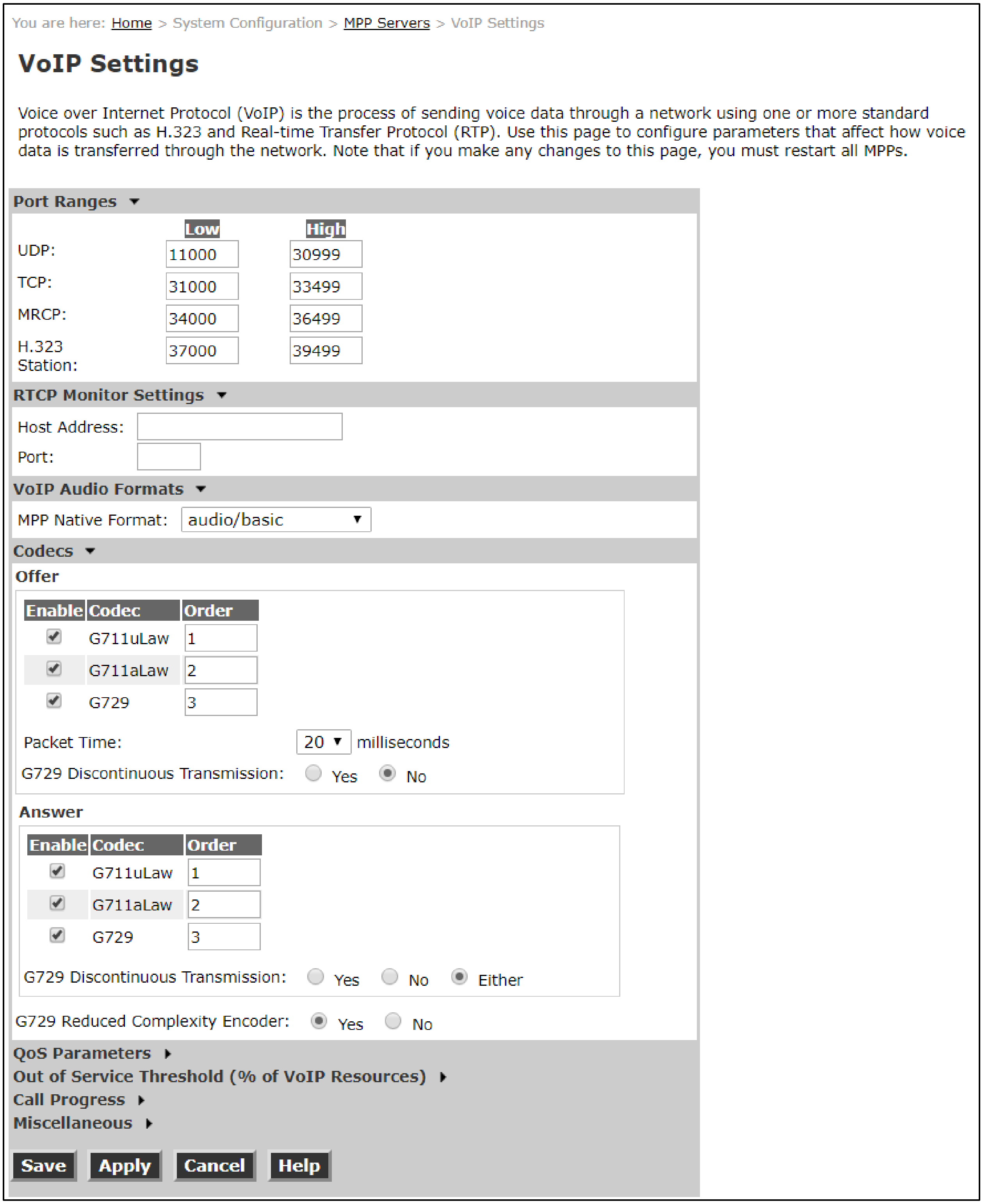
Step 4 - Click **VoIP Settings** tab on the screen displayed in **Step 1**.

- In the Port Ranges section, default ports were used.

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

- Use default values for all other fields.

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



You are here: Home > System Configuration > MPP Servers > VoIP Settings

VoIP Settings

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

Port Ranges ▼

	Low	High
UDP:	11000	30999
TCP:	31000	33499
MRCP:	34000	36499
H.323 Station:	37000	39499

RTCP Monitor Settings ▼

Host Address:

Port:

VoIP Audio Formats ▼

MPP Native Format: audio/basic ▼

Codecs ▼

Offer

Enable	Codec	Order
☑	G711uLaw	1
☑	G711aLaw	2
☑	G729	3

Packet Time: 20 ▼ milliseconds

G729 Discontinuous Transmission: ○ Yes ● No

Answer

Enable	Codec	Order
☑	G711uLaw	1
☑	G711aLaw	2
☑	G729	3

G729 Discontinuous Transmission: ○ Yes ○ No ● Either

G729 Reduced Complexity Encoder: ● Yes ○ No

QoS Parameters ▶

Out of Service Threshold (% of VoIP Resources) ▶

Call Progress ▶

Miscellaneous ▶

8.7. Configuring RFC2833 Event Value Offered by Experience Portal

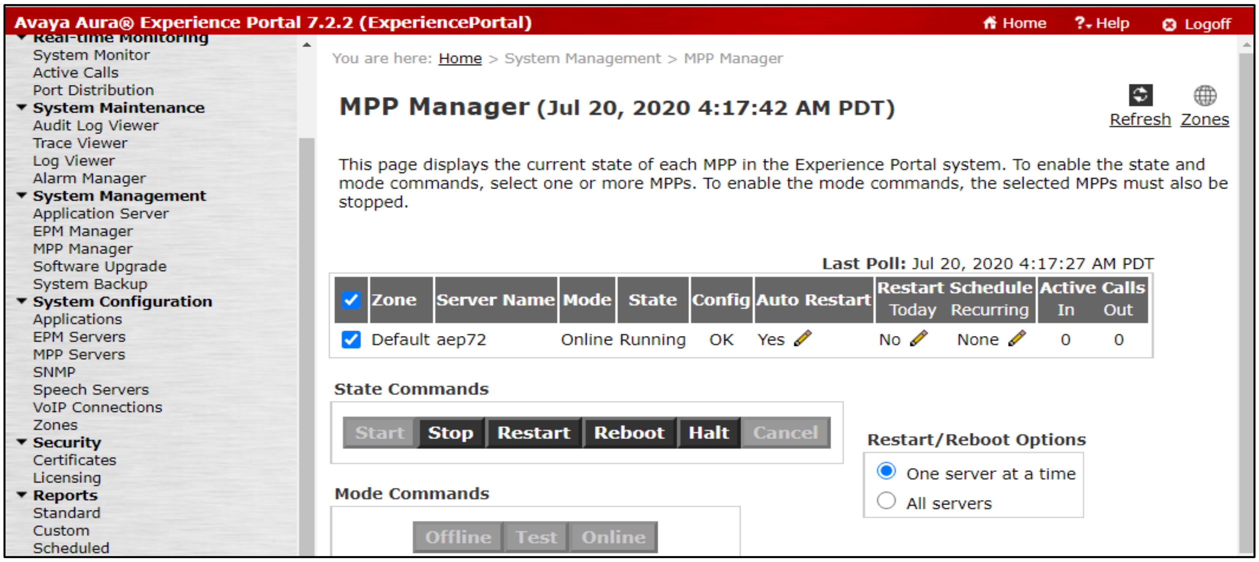
The configuration change example noted in this section was not required for any of the call flows illustrated in these Application Notes. For incoming calls from G12 to Experience Portal, G12 specifies the value 101 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Experience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

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

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

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

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



MPP Manager (Jul 20, 2020 4:17:42 AM PDT)

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

Last Poll: Jul 20, 2020 4:17:27 AM PDT

☑	Zone	Server Name	Mode	State	Config	Auto Restart	Restart Schedule		Active Calls	
							Today	Recurring	In	Out
☑	Default	aep72	Online	Running	OK	Yes	No	None	0	0

State Commands

Mode Commands

Restart/Reboot Options

● One server at a time
○ All servers

9. Bell Canada SIP Trunk Configuration

Bell Canada is responsible for the network configuration of the Bell Canada SIP Trunk service. Bell Canada will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. Bell Canada will provide the IP address of the Bell Canada SIP Trunk SIP signaling/SBC IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. Bell Canada also provides the Bell Canada SIP Specification document for reference. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between Bell Canada 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: **Device Specific Settings → Troubleshooting → Debugging**.
        - SIP only: enable LOG_SUB_SIPCC subsystem under SSYNDI process.
        - CALL PROCESSING: enable all subsystems under SSYNDI process.
        - PPM: enable all subsystems under CONFIG_PROXY process.

      The log files are stored at: /usr/local/ipcs/log/ss/logfiles/elog/SSYNDI.
    - **Command Line Interface**: Login with root user and enter the command: **#traceSBC**. The tool updates the database directly based on which trace mode is selected.

11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Bell Canada. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workaround.

12. References

This section references the documentation relevant to these Application Notes.

Avaya product documentation, including the following, is available at http://support.avaya.com

Avaya Aura® **Session Manager/System Manager**

[1] *Deploying Avaya Aura® Session Manager and Branch Session Manager in Virtualized Environment*, Release 8.1, Issue 3, March 2020
[2] *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 3, March 2020
[3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 4, March 2020
[4] *Administering Avaya Aura® System Manager for Release 8.1*, Release 8.1.x, Issue 5, March 2020

Avaya Aura® **Communication Manager**

[5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 4, March 2020
[6] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020
[7] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1.x, Issue 6, March 2020
[8] *Administering Avaya G430 Branch Gateway*, Release 8.1.x, Issue 3, March 2020
[9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.2, Issue 9, December 2019
[10] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*, Issue 1.1, June 2018

Avaya Session Border Controller for Enterprise

[11] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 1, February 2020
[12] *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment* Release 8.1, Issue 1, February 2020
[13] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 8.1, Issue 1, February 2020

Avaya Aura® Messaging

[14] *Administering Avaya Aura® Messaging*, Release 7.1.0, Issue 9, April 2020

IETF (Internet Engineering Task Force) SIP Standard Specifications

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

Product documentation for Bell Canada SIP Trunking may be found at:
https://business.bell.ca/shop/enterprise/sip-trunking-service

Appendix A: SigMa Script

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

Note:

- The following of the “otg=” is the trunk group ID
- siptrunking.bell.ca is the Bell Canada peer FQDN

```
within session "ALL"
{
    act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
         {
//Remove unwanted headers
remove(%HEADERS["P-Location"][1]);
remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
//For the static ONND, the From and PAI headers need to have user=phone and no “otg” trunk
ID
append(%HEADERS["From"][1].URI,";user=phone");
append(%HEADERS["P-Asserted-Identity"][1].URI,";user=phone");
//For the dynamic ONND, the From and PAI headers need to have the “otg” trunk ID and no
“user=phone”
append(%HEADERS["From"][1].URI,";otg=VEND10_6132600771_01A");
append(%HEADERS["P-Asserted-Identity"][1].URI,";otg=VEND10_6132600771_01A");
// For the call forward off-net with Diversion header
append(%HEADERS["Diversion"][1].URI,";user=phone");
append(%HEADERS["Diversion"][1].URI,";otg=VEND10_6132600771_01AA");
//For Call transferred by Experience Portal
if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("6132600771"))
then
           {
            %var="this does nothing, match for DID number passed";
           }
         else
           {
           %HEADERS["P-Asserted-Identity"][1].URI.USER = "6132600771";
            }

           }
}
```

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.