Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the TELUS SIP Trunking Service IP Authentication on Release 2 Platform with Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise 7.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the TELUS SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 8.0, Avaya Aura® Communication Manager 8.0, Avaya Aura® Experience Portal, Avaya Session Border Controller for Enterprise 7.2 and various Avaya endpoints. TELUS is a member of the Avaya DevConnect Service Provider program.

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.

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.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the TELUS SIP Trunking Service (R2 Platform – IP Authentication) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 8.0, Avaya Aura® Communication Manager 8.0, Avaya Aura® Experience Portal, Avaya Session Border Controller for Enterprise 7.2 and various Avaya endpoints. In addition, Avaya Aura® System Manager 8.0 is used to configure Avaya Aura® Session Manager.

The TELUS SIP Trunking Service can be deployed using private MPLS connections from the TELUS network to the enterprise or can be deployed across the Internet. Deployment across the Internet requires registration by the enterprise while the MPLS connections do not. These Application Notes cover the MPLS deployment configuration.

Customers using this Avaya SIP-enabled enterprise solution with the TELUS SIP Trunking Service are able to place and receive PSTN calls via a broadband WAN connection with SIP. 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 the TELUS SIP Trunking Service provided via a broadband connection and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE).

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 for 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 these DevConnect Application Notes 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.

2.1. Interoperability Compliance Testing

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

- Sending and receiving SIP OPTIONS queries to the service provider
- Inbound and outbound PSTN calls (via the SIP trunk) to/from analog, digital, H.323 and SIP telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client) using multiple protocols (H.323 and SIP) and multiple modes (Local Computer and Other Phone mode)
- Inbound and outbound PSTN calls to/from Avaya Equinox® for Windows
- Various call types including: local (10 digit), long distance (1 + 10 digits), international, outbound toll-free, operator, operated-assisted calls (0 + 10 digits) and local directory assistance (411)
- Codecs G.711MU and G.729A
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- Voicemail Message Waiting Indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and mobility (Extension to cellular – EC500)
- T.38 Fax and fallback to G.711 Fax
- Network Call Redirection using REFER and a 302 response
- Initial IP-IP Direct Media

Emergency 911 calls, and inbound toll-free calls are supported but were not tested as part of the compliance test.

The following item was not supported:

- Passing of User-to User Information (UUI header) when a call is redirected with REFER.

The following features and functionalities were tested with Avaya Experience Portal.

- Basic inbound call from PSTN to Experience Portal
- Navigating IVR menu using DTMF RFC 2833
- Blind transfer using REFER
- Consultative transfer using REFER
- Consultative transfer using INVITE

2.2. Test Results

Interoperability testing of the TELUS SIP Trunking Service was completed with successful results for all test cases with the exception of the observations and/or limitations described below.

- **OPTIONS from TELUS (Request-URI)**: TELUS sends OPTIONS messages whose user part of the Request URI is not routable by the Session Manager which results in a 404 User Not Found response to TELUS. For interoperability, the Avaya SBCE was configured to return a 200 OK response to all OPTIONS messages instead of sending the messages to the Session Manager (**Section 7.10.2**).
- **Call Forwarding and EC500**: For inbound PSTN calls that are forwarded back to the PSTN or ring to an EC500 (enterprise mobility) PSTN endpoint, TELUS requires the originating calling number be present in the P-Asserted-Identity (PAI) header. Normally, Communication Manager puts this information in the Diversion header. A SIP header manipulation was created on the Avaya SBCE to modify the P-Asserted-Identity (PAI) header with information contained in the Diversion header received from Session Manager (**Section 7.6.1**). This allowed the call to complete successfully.
- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displayed the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the terminating PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/TELUS solution. It is listed here simply as an observation.
- **T.38 Fax**
    - **Network Coverage**: Not all media gateways in the TELUS network support T.38 fax. Communication Manager supports fallback to G.711 pass-through fax from T.38 fax if configured on the ip-codec-set form (**See Section 5.5**). This is the recommended setting if all gateways in the service provider network do not support T.38 fax.
    - **Transitioning to T.38 for Outbound Calls**: In general, the answering side of a fax call should send a re-INVITE to transition to T.38. For outbound fax calls to the PSTN, this means the network would typically send the re-INVITE to transition to T.38. However, TELUS never sends a T.38 re-INVITE for outbound calls even if the TELUS gateway supports T.38. The impact is that all outbound fax calls will fallback to G.711 pass-through fax regardless of the TELUS gateway support for T.38. All inbound fax calls will use T.38 if supported on the specific TELUS gateway.
- **Operator-assisted calls routed as direct dialed calls**: Operated-assisted calls (0 + 10 digits) were routed the same as direct dialed long distance calls (1 + 11 digits). This was believed to be a routing problem in the TELUS test lab and would not occur in the production environment.
- **Inbound PSTN call forward all call back to PSTN** got no audio when the secure media SRTP was used between enterprise and internal media interface of SBCE, the issue did

not happen if regular RTP was used. This issue is currently investigated by Avaya SBCE team.

- **Consultative transfer call using INVITE method by Experience Portal** to PSTN requires changing P-Asserted-Identity (PAI) header to Telus known DID number so that Telus is able to allow the call to be routed to PSTN. There is a signaling manipulation script used on the Avaya SBCE to modify this. Refer **Section 7.6** for more detail.

2.3. Support

For technical support on the TELUS system, please contact your TELUS Account Executive or visit http://telus.com.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the TELUS SIP Trunking Service. In a true customer MPLS deployment, TELUS would provide a MPLS connection from their network directly to the customer site. To simulate this type of deployment in the test environment, an IPSec VPN tunnel was established across the public Internet between the TELUS and Avaya labs. This is the configuration used for compliance testing.

The components used to create the simulated customer site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya Media Server
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Experience Portal
- Avaya Aura® Messaging
- Avaya 9600 Series IP Deskphones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya Equinox™ for Windows (SIP)

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in this document. Similarly, any references to real routable PSTN numbers have been replaced with numbers that cannot be routed over the PSTN.

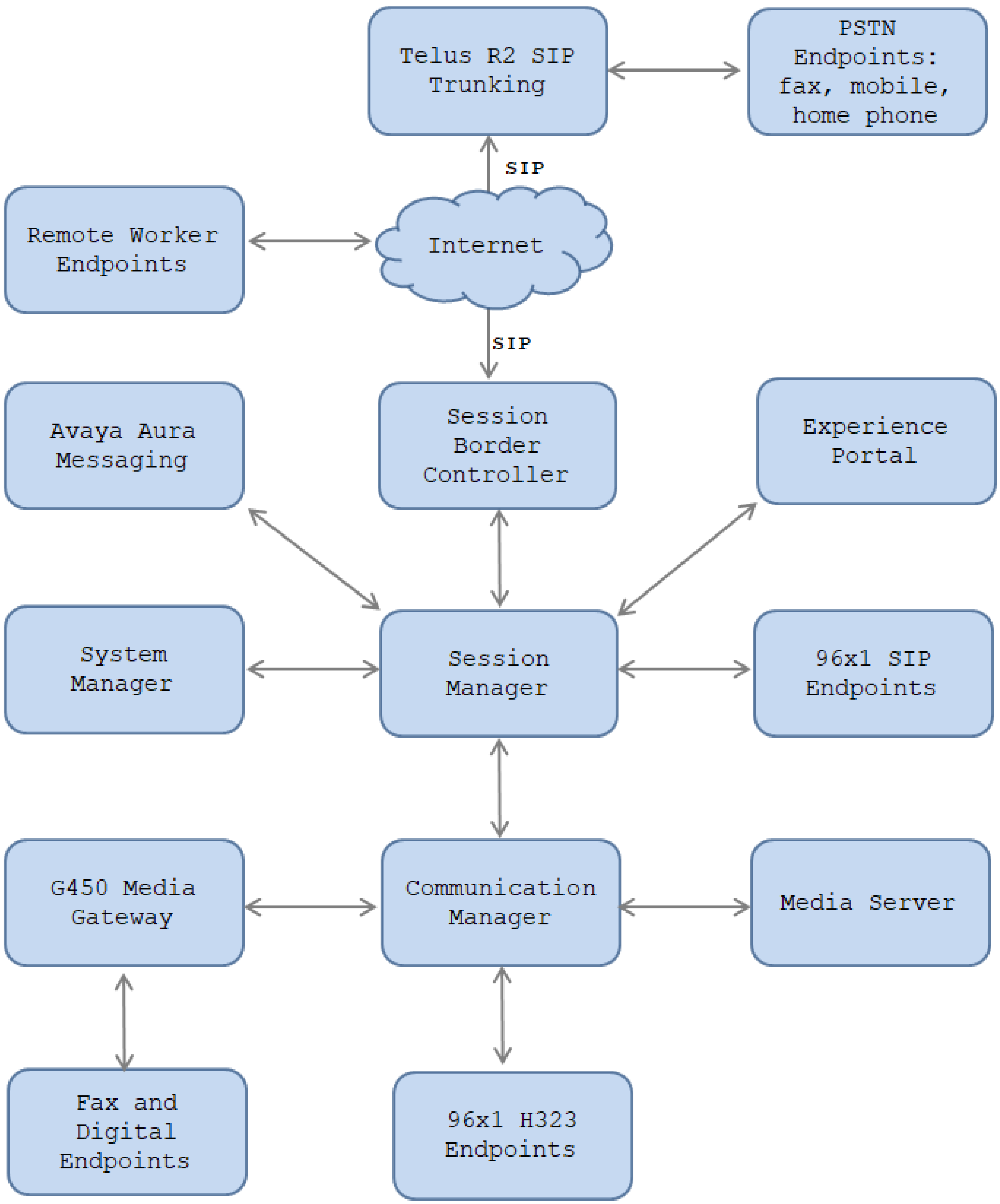


Figure 1: Test Configuration

The following table indicates the IP addresses that were assigned to the systems in the test configuration diagram:

Description	**IP Address**
System Manager	10.33.1.10
Session Manager Signaling	10.33.1.12
Aura Messaging	10.33.1.5
Session Border Controller	10.33.1.51
Experience Portal	10.33.1.25
Communication Manager	10.33.1.6
Media Server	10.33.1.30
G450 Media Gateway	10.33.1.40
96x1 Endpoints	10.33.5.40-10.33.5.46

A separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the Avaya SBCE and then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the Avaya SBCE. From the Avaya SBCE, the call is sent to the TELUS SIP Trunking Service.

TELUS requires 11 digits (1+10 digits) be sent in the Request URI header for long distance calls and 10 digits for local calls.

For inbound calls, TELUS sends 10 digits in the source headers (i.e., From, PAI, and Contact) and destination headers (i.e., Request-URI and To). For outbound long distance calls, Communication Manager was configured to send 10 digits in the source headers and 11 digits (1 + 10) in the destination headers. For outbound local calls, TELUS required 10 digits in the destination headers.

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® System Manager running on a VMware Virtual Platform	8.0.1.0 (Software Update Revision 8.0.1.0.038826)
Avaya Aura® Session Manager running on a VMware Virtual Platform	8.0.1.0 (Build 8.0.1.0.801007)
Avaya Aura® Communication Manager running on a VMware Virtual Platform	8.0.1.0 (8.0.1.0.0.822.25031)
Avaya G450 Media Gateway	40.20.0
Avaya Aura® Media Server running on a VMware Virtual Platform	8.0.137
Avaya Aura® Messaging running on a VMware Virtual Platform	7.0
Avaya Session Border Controller for Enterprise	7.2.2.1
Avaya Aura® Experience Portal	7.2
Avaya Aura Messaging	7.0
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.714
Avaya 9611G IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	7.14
Avaya one-X® Communicator (H.323 or SIP)	6.2 SP13
Avaya Equinox® for Windows	3.4
TELUS SIP Trunking Service Components	
Equipment/Software	Release/Version
Oracle Session Border Controller	7.4m2p2
Genband EXPERiUS Application Server	MCP-17.0.22.15
Genband C20 Call Session Controller	CVM17
Ribbon	C20 R19

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.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the TELUS SIP Trunking Service. A SIP trunk is established between Communication Manager and Session Manager for use by traffic to and from TELUS. It is assumed the general installation of Communication Manager, the Avaya Media Gateway, Media Server and Session Manager has been previously completed and is not discussed here.

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. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

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 **24000** SIP trunks are available and **30** 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 6
                       Maximum Administered SIP Trunks: 24000 30
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
```

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer 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? y
                                    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 **restricted** and **unavailable** respectively.

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

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

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: 1
          International Access Code: 011

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 of the server running Communication Manager **(procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AAM                 10.33.1.5
AMS                 10.33.1.31
interopSM           10.33.1.12
default             0.0.0.0
gateway             10.33.1.1
procr               10.33.1.6
procr6              ::
```

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. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference defined by the service provider. For the compliance test, codec set 3 was configured with codecs **G.711MU** and **G.729A**. Default values can be used for all other fields.

```
change ip-codec-set 3                                           Page   1 of   2

                         IP MEDIA PARAMETERS
    Codec Set: 3

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.729             n          2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: none
 2:
```

On **Page 2**, in general, the **FAX Mode** is set to **t.38-G711-fallback**. In general, TELUS supports T.38 fax but not on all media gateways in the network. Using the **t.38-G711-fallback** setting will allow all fax calls to succeed, though some may use G.711 fax instead of T.38. See **Section 2.2** for details.

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

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n
                                                                     Packet
                          Mode                   Redundancy          Size(ms)
    FAX                   t.38-G711-fallback      0          ECM: y
    Modem                 off                     0
    TDD/TTY               US                      3
    H.323 Clear-channel   n                       0
    SIP 64K Data          n                       0                  20
```

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 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 Media Gateway or Media Server. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- 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 3                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: bvwdev.com
    Name: SP Region              Stub Network Region: n
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 3               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
```

On **Page 4**, define the IP codec set to be used for traffic between region 3 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. The example below shows the settings used for the compliance test. Row 1 indicates that codec set 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 3 will automatically create a complementary table entry on the IP network region 1 form for destination region 3. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).

```
change ip-network-region 3                                      Page   4 of  20

 Source Region: 3     Inter Network Region Connection Management     I      S M
                                                                     G  A  y t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G  n c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L  c e
 1    3     y    NoLimit                                             n all y t
 2
 3    3                                                                all
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager. If TLS is used here, it must also be used on the Session Manager entity link defined in **Section 6.6**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for 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 instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a

separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.6** and **5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **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 the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic from the Avaya Media Gateway and allow it to flow directly between the SIP trunk and the enterprise endpoint.
- Set **Initial IP-IP Direct Media** to **n** or **y** depending on the customer requirements. This option attempts to directly connect the media traffic between the SIP trunk and the enterprise endpoint at initial call-setup instead of establishing a media connection to the Avaya Media Gateway or Media Server which is later redirected to the endpoints. However, if this option is set on the service provider signaling group, it must be set the same on the signaling group associated with the SIP trunk used by the enterprise SIP endpoints. In the test configuration, this was signaling group 1 (not shown). If the customer has no requirement for **Initial IP-IP Direct Media**, then the recommendation is to set the parameter to **n**.
- Set the **Alternate Route Timer** to **6**. This defines the number of seconds that 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   3
                                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: 3

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
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 3 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.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in the previous section.
- 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: OUTSIDE CALL                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**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs or UPDATE messages must be sent to keep the active session alive. For the compliance test, the value of **300** 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): 300

 Disconnect Supervision - In? y  Out? y


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

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. Public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. To remove the + sign, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.9**).

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 requests CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local 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

 DSN Term? n
 Show ANSWERED BY on Display? y
```

On **Page 4**, set **Mark Users as Phone** as **y**. This is recommended by TELUS. The **Network Call Redirection** field may be set to **y** or **n**. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer; otherwise the SIP INVITE message will be used for call transfer. Both approaches are supported with this solution.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**, the value used by TELUS.

Set **Always Use re-INVITE for Display Updates** to **y**. TELUS returned a 488 Not Acceptable Here response to some of the Communication Manager display update messages. To avoid these errors, the Communication Manager was configured to use re-INVITEs for display updates instead of UPDATE messages.

Lastly, if the **Shuffling with SDP** field appears on the form, set it to **n**. This parameter only appears if special application SA8965 is enabled. This field must also be disabled on the internal SIP trunk used by the enterprise SIP endpoints. Since calls between the enterprise SIP endpoints and TELUS traverse two SIP trunks: the internal SIP trunk for intra-enterprise traffic (trunk 1 in the test configuration) and the service provider SIP trunk to TELUS (trunk 3), the **Shuffling with SDP** parameter must be set the same on both. The **Shuffling with SDP** field may have been set to **y** if the system had been previously configured to connect to the TELUS Release 1 platform.

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

                                       Mark Users as Phone? y
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? n
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? y
                        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
```

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since **Numbering Format** was set to **private** on the trunk group form (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, the two DID numbers provided for testing were assigned to the two extensions **3301** and **3401**. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

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

Ext Ext               Trk        Private          Total
Len Code              Grp(s)     Prefix           Len
 4  3                 8          417967           10 Total Administered: 15
 4  33                1                           4     Maximum Entries: 540
 4  34                1                           4
 4  3301              3          5872330302       10
 4  3401              3          5872330303       10
```

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 private numbering entry can be applied for all extensions. In the example below, on trunk 3, all stations with a 4-digit extension beginning with 3 will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 5                                     Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
 4  3               1                           5     Total Administered: 2
 4  3               3          587233           10       Maximum Entries: 540
```

5.9. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a dial access code (**dac**).

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   0           1   attd
   1           5   ext
   2           5   ext
   3           5   ext
   4           5   ext
   411         3   udp
   5           5   ext
   6           3   dac
   7           3   dac
   8           1   dac
   9           1   dac
   *           3   fac
   #           3   fac
```

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  12
                               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 to the service provider (as defined next).

```
change ars analysis 0                                           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
    0                     1    1     3        op           n
    0                     11   11    3        op           n
    011                   12   18    3        intl         n
    1732                  11   11    3        fnpa         n
    1800                  11   11    3        fnpa         n
    1877                  11   11    3        fnpa         n
    1613                  11   11    3        fnpa         n
    587                   10   10    3        hpna         n
    411                   3    3     3        svcl         n
```

The route pattern defines which trunk group will be used for an outgoing call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider route pattern in the following manner. The example below shows the values used for route pattern 3 during 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.
- **Pfx Mrk**: Set the prefix mark (**Pfx Mrk**) to **1**. This will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance numbers within the North American Numbering Plan (NANP).
- **Numbering Format**: **unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

```
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       1                                                       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
```

Use the **save translation** command to save all Communication Manager configuration described in **Section 5**.

6. Configure Avaya Aura® Session Manager

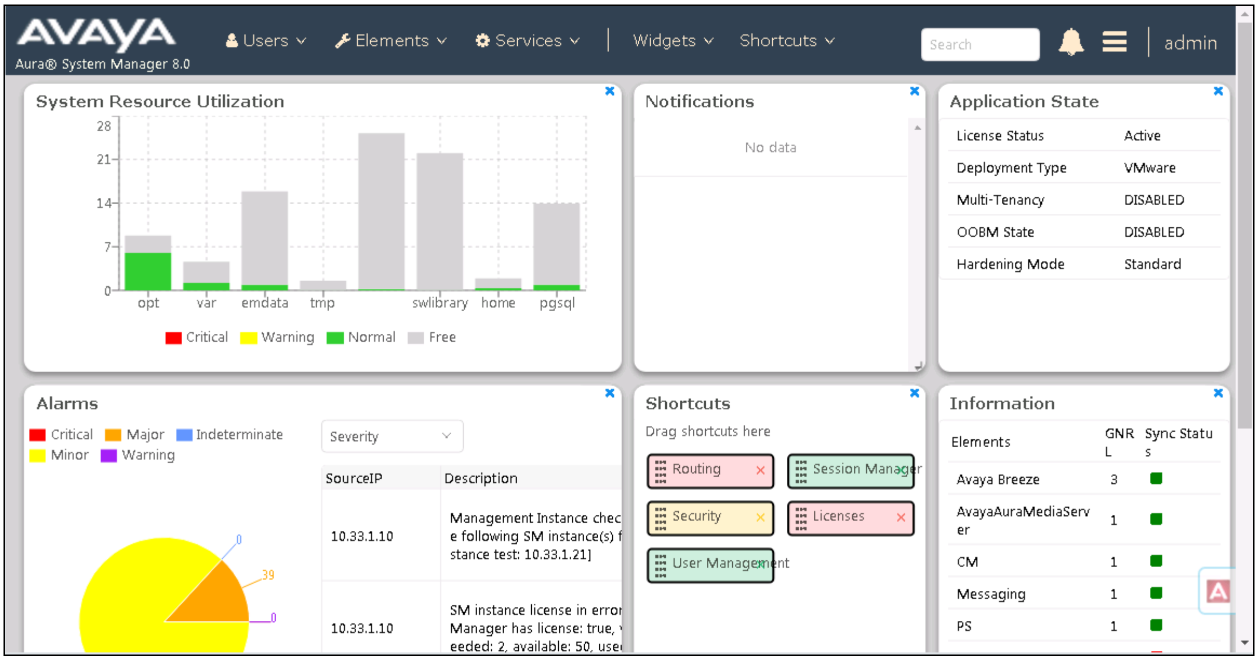
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Location
- Adaptation Modules
- SIP Entities
- Entity Links
- Routing Policies
- Dial Patterns
- Session Manager

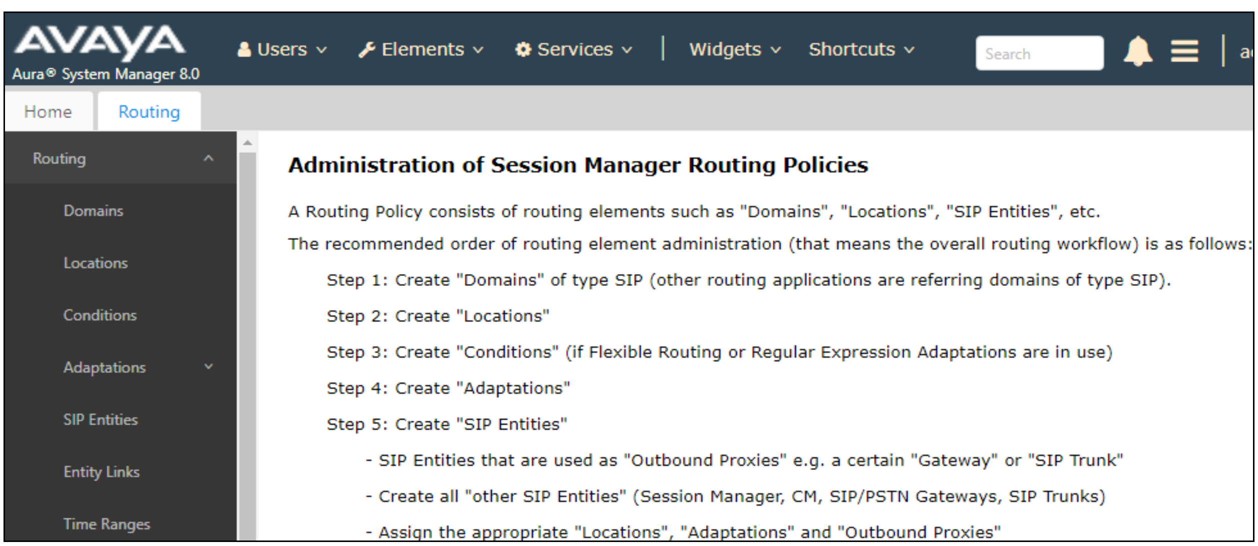
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session 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 "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The following page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements → Routing** link highlighted below.



Clicking the **Elements → Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.

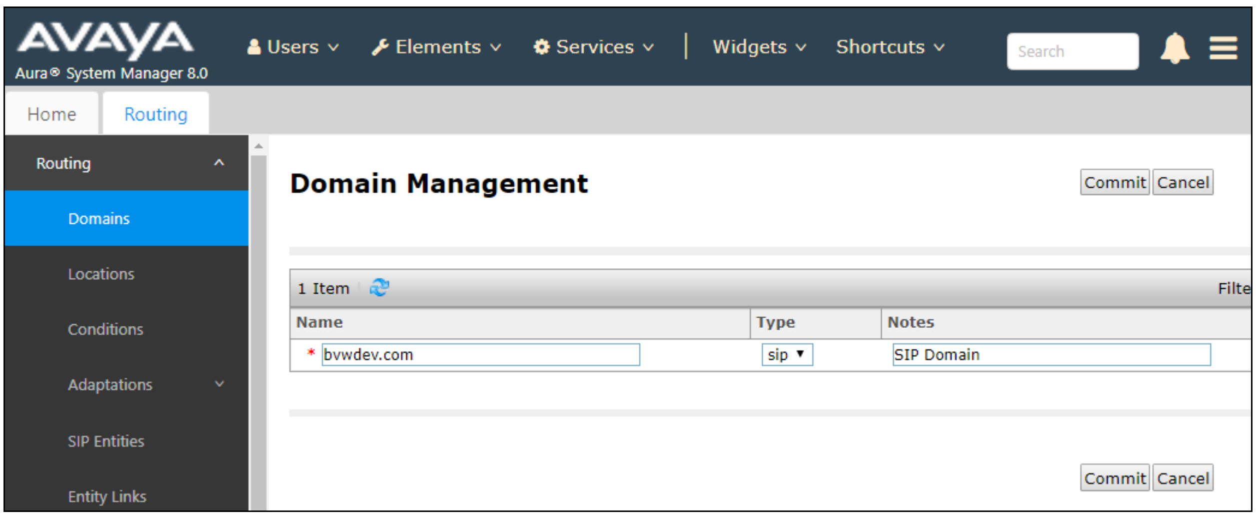


6.2. Specify SIP Domain

Create a SIP Domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**bvwdev.com**) as defined in **Section 5.5**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), 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**. The screen below shows the entry for the enterprise domain.



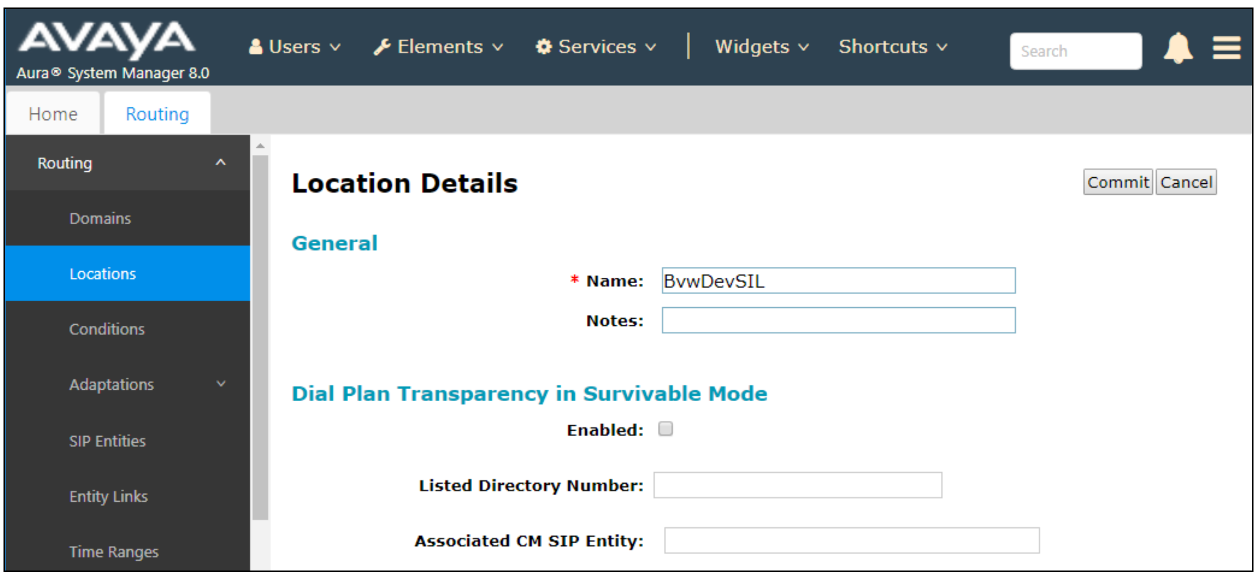
6.3. Add Location

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

To add a Location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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



Click **Commit** to save.

The enterprise equipment (e.g., Communication Manager, Session Manager and the Avaya SBCE) will be associated with this location through the configuration of their respective SIP Entities in **Section 6.5**.

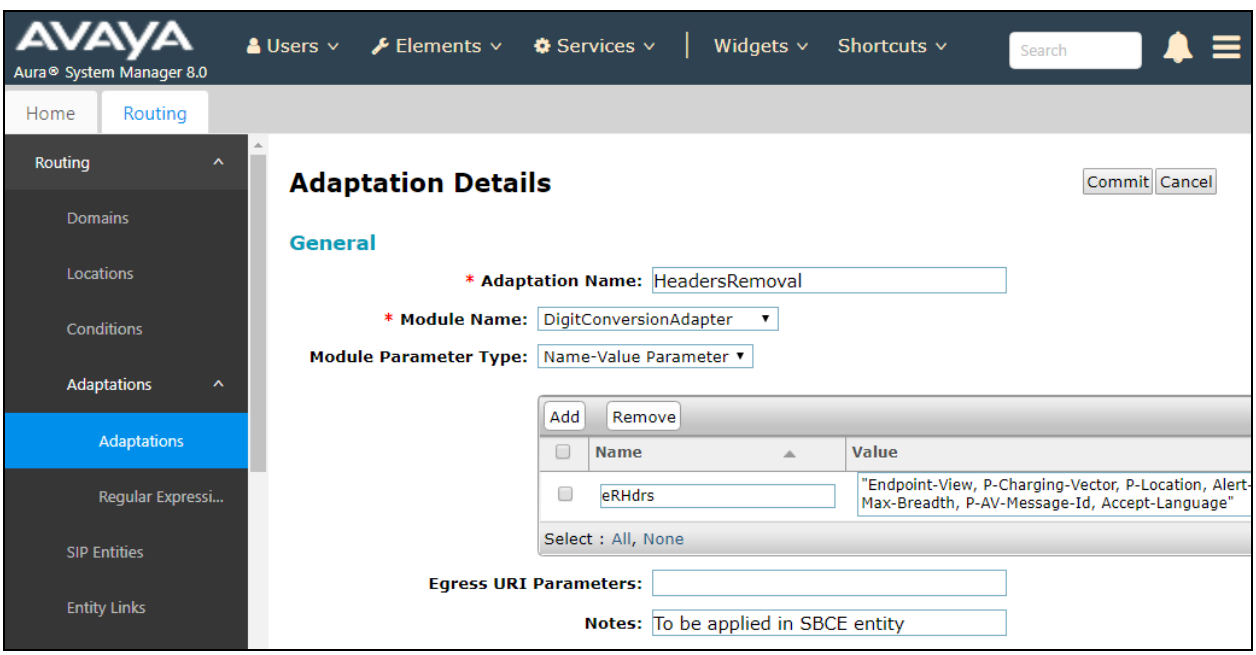
6.4. Add Adaptation

Session Manager can be configured with Adaptations that can modify SIP messages before or after routing decisions have been made or perform digit manipulation. The Adaptation **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. For the compliance test, an Adaptation was used. The adaptation was applied to the Avaya SBCE SIP Entity and it removes SIP headers that are not used by the service provider.

To create the Adaptation that will be applied to the Avaya SBCE SIP Entity, click on 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.

- **Adaptation Name:** Enter a descriptive name for the Adaptation (e.g., **HeadersRemoval**.
- **Module Name:** Select **DigitConversionAdapter** from the drop-down menu.
- **Module Parameter Type:** Enter **Name-Value Parameter**. This section will expand with an area to enter **Name** and **Value** pairs. Click **Add**. To remove headers on the egress side of Session Manager (i.e., towards the Avaya SBCE) enter the keyword **eRHdrs** in the **Name** field and a comma-separated list of headers to remove in the **Value** field. For the compliance test, the list of removed headers included **Endpoint-View**, **P-Changing-Vector**, **P-Location**, **Alert-Info**, **Max-Breadth**, **P-AV-Message-Id**, and **Accept-Language**.
- **Notes:** Enter a description (optional).



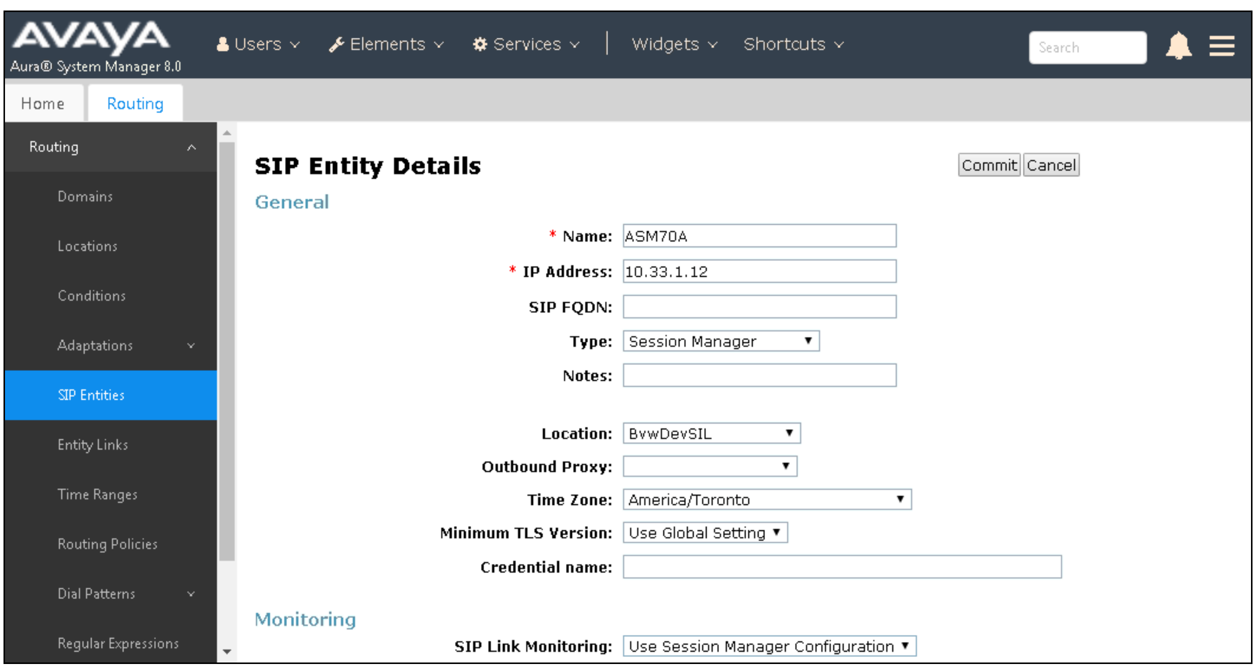
6.5. Add SIP Entity

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on 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.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Notes:** Brief description (optional)
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **BvwDevSIL**created in **Section 6.3**.
- **Time Zone:** Select the time zone for the Location above.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.



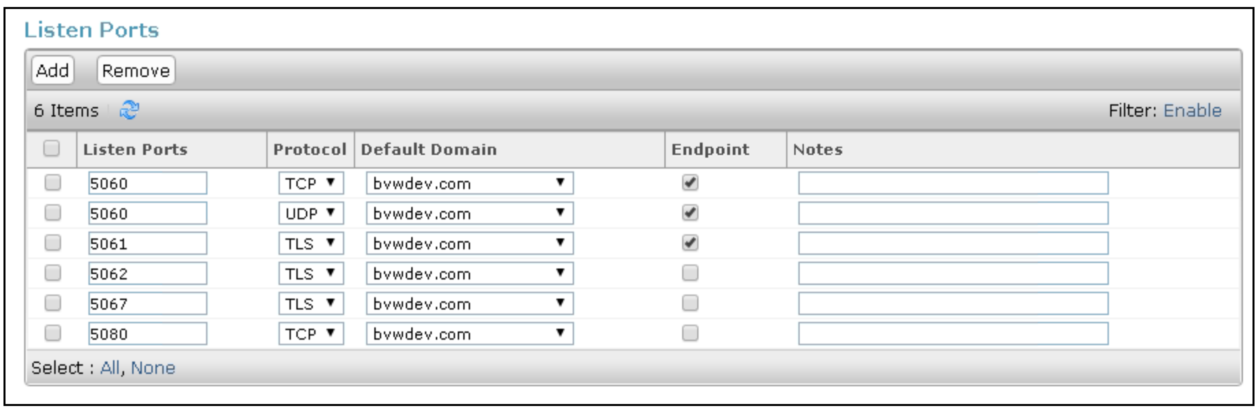
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP Entities.

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

- **Listen Port:** Port number on which Session Manager can listen 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** to save.

Three port entries are shown in the screenshot below. The first two are standard ports used for SIP traffic: port 5060 for TCP and port 5061 for TLS. These ports were provisioned as part of the Session Manager installation not covered by this document. In addition, port **5067** defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.


Listen Ports

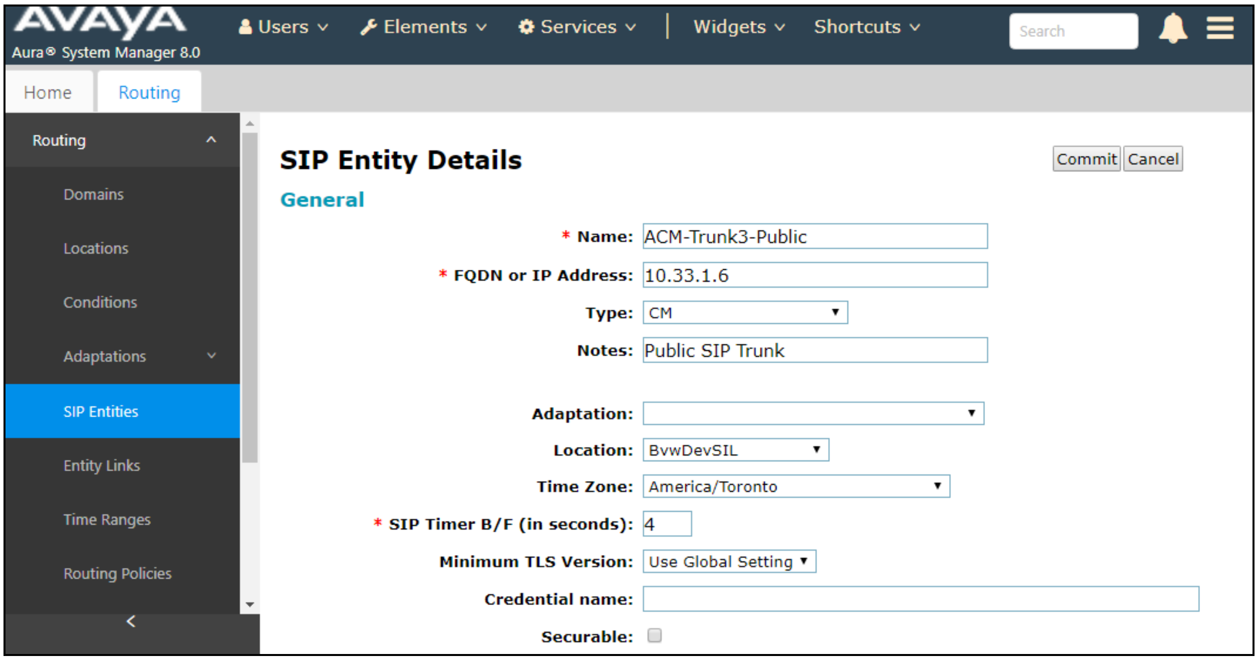
Add Remove

6 Items Filter: Enable

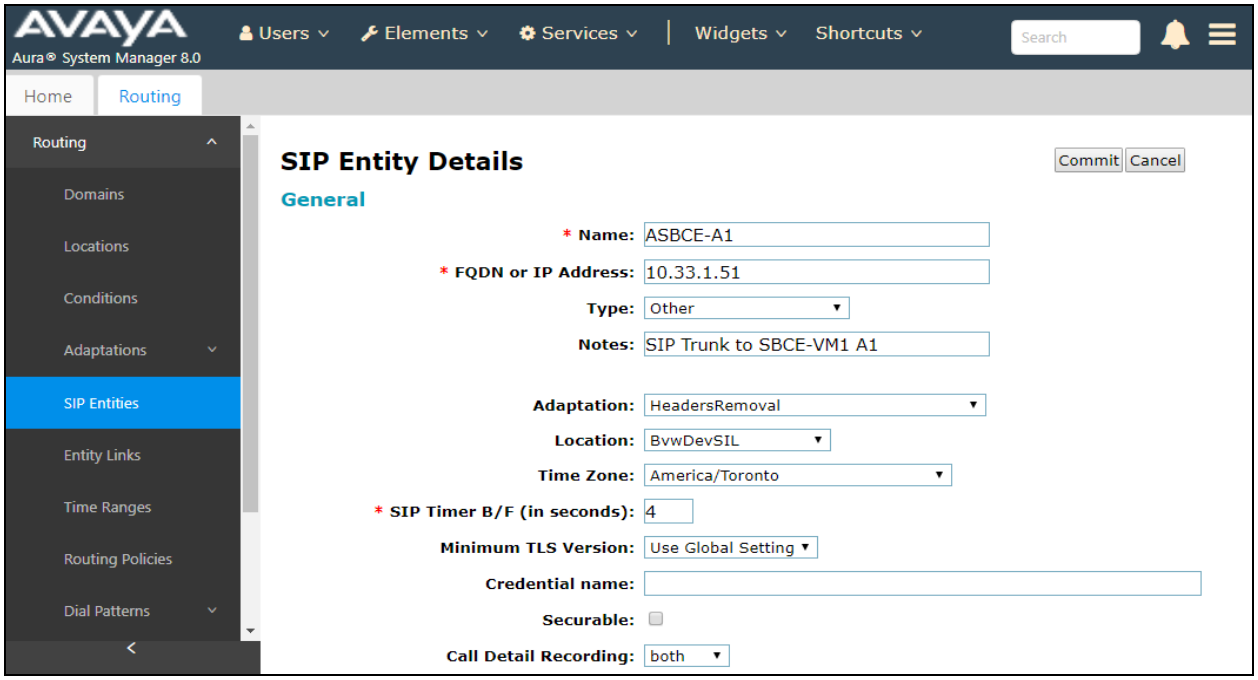
	Listen Ports	Protocol	Default Domain	Endpoint	Notes
☐	5060	TCP	bvwdev.com	☑	
☐	5060	UDP	bvwdev.com	☑	
☐	5061	TLS	bvwdev.com	☑	
☐	5062	TLS	bvwdev.com	☐	
☐	5067	TLS	bvwdev.com	☐	
☐	5080	TCP	bvwdev.com	☐	

Select : All, None

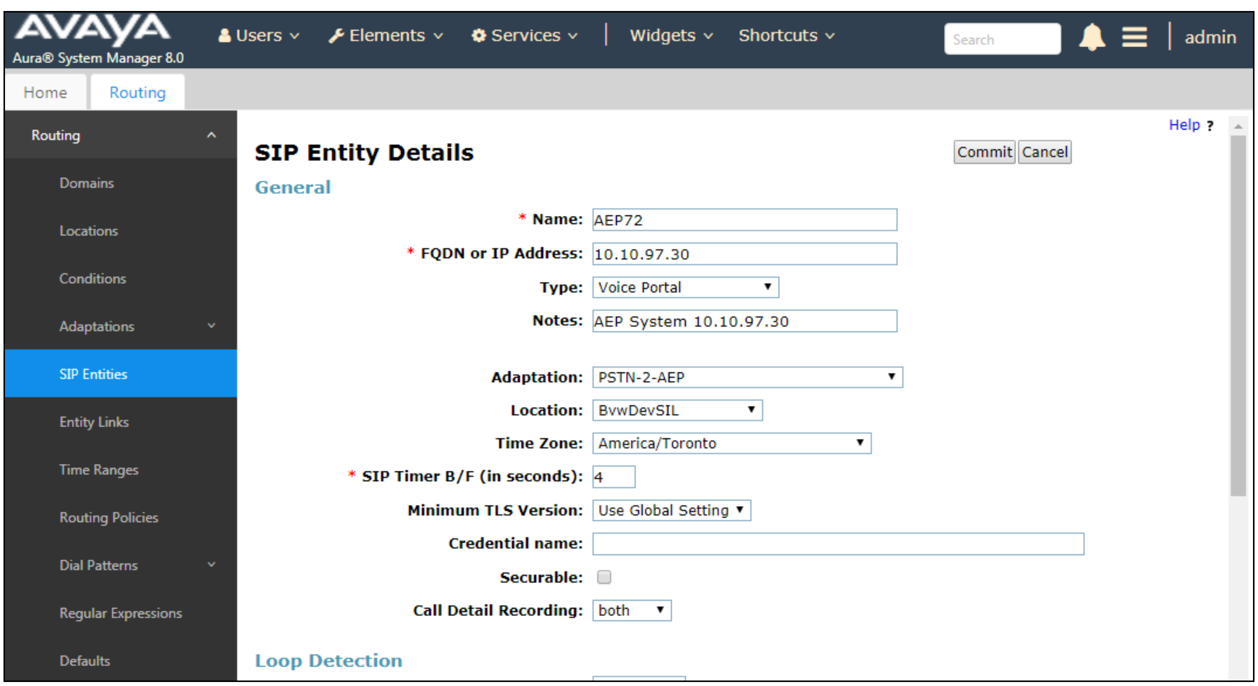
The following screen shows the addition of Communication Manager. Typically, when Session Manager is first installed, a SIP Entity and Entity Link is created for Communication Manager to carry intra-enterprise SIP traffic. In order for Session Manager to separate SIP service provider traffic on a separate Entity Link to Communication Manager, the creation of a second SIP Entity for Communication Manager is needed. The **FQDN or IP Address** field is set to the IP address of Communication Manager. The **Location** field is set to **BvwDevSIL** which is the Location where Communication Manager resides (**Section 6.3**).



The following screen shows the addition of the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). For the **Adaptation** field, select the Adaptation previously defined for the Avaya SBCE in **Section 6.4**. The **Location** field is set to **BvwDevSIL** which is the Location where the Avaya SBCE resides.



The following screen shows the addition of **Experience Portal**. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The **Location** field is set to **BvwDevSIL** which is the Location where **Experience Portal** resides.



6.6. 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 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 (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

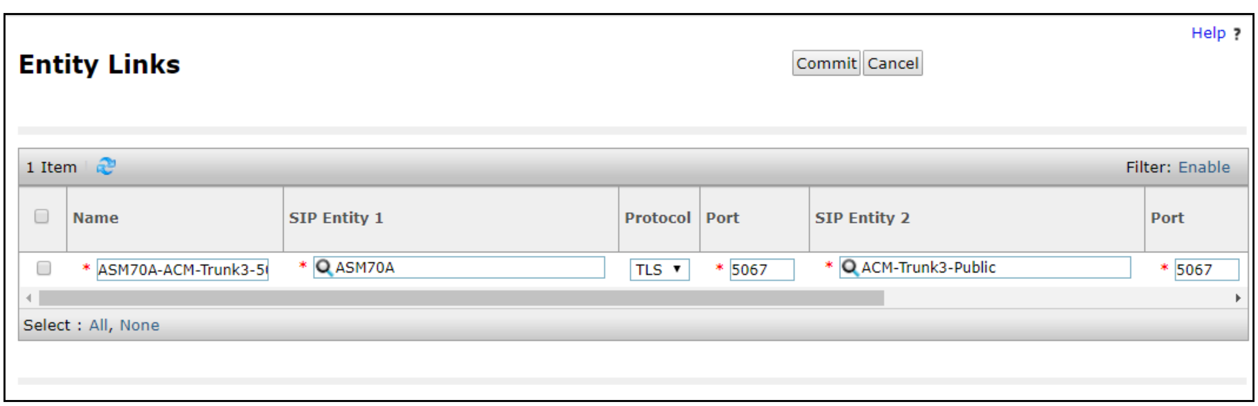
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager SIP Entity (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system using the SIP Entity name defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **trusted** from pull-down menu.

Click **Commit** to save.

For the Communication Manager Entity Link (**ASM70A-ACM-Trunk3-5067**), the protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. Specifically, the following fields must match:

- **Protocol** must match the **Transport Method** from **Section 5.6**.
- SIP Entity 1 **Port** must match the **Far-end Listen Port** from **Section 5.6**.
- **SIP Entity 2** must match the SIP Entity defined for Communication Manager in **Section 6.5**.
- SIP Entity 2 **Port** must match the **Near-End Listen Port** from **Section 5.6**.

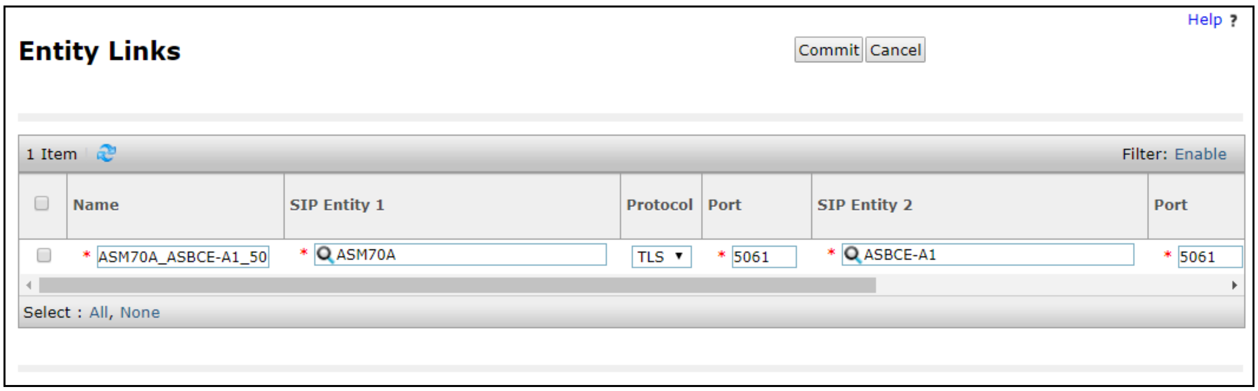
The screen below shows the completed Entity Links for Communication Manager.



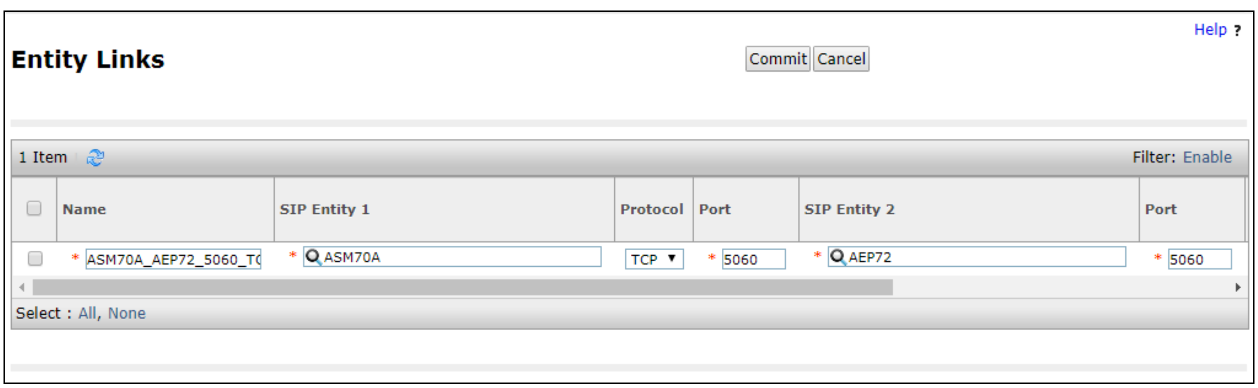
For the Avaya SBCE Entity Link (**ASM70A_ASBCE-A1_5061_TLS**), the protocol and ports defined here must match the values used on the Avaya SBCE in **Section 7**. Specifically, the following fields must match:

- **Protocol** must match the protocol used by the Avaya SBCE Routing profile to reach Session Manager. This value is shown in the **Next Hop Address** in **Section 7.12.1**.
- SIP Entity 1 **Port** must match the port value used by the Avaya SBCE Routing profile to reach Session Manager. This value is shown in the **Next Hop Address** in **Section 7.12.1**.
- **SIP Entity 2** must match the SIP Entity defined for the Avaya SBCE in **Section 6.5**.
- SIP Entity 2 **Port** must match the port value defined in the Avaya SBCE internal signaling interface in **Section 7.3** for the selected protocol.

The screen below shows the completed Entity Links for the Avaya SBCE.



Similarly, the screenshot below show the Entity Link for Experience Portal (**ASM70_AEP72_5060_TCP**).



6.7. Add Routing Policies

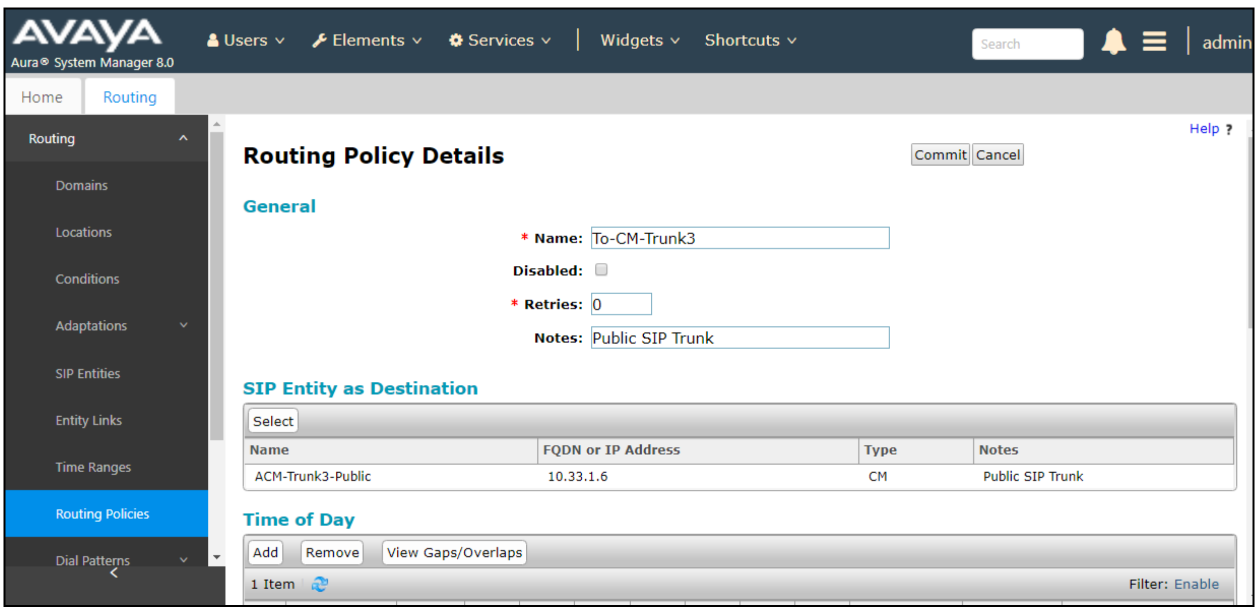
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on 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.

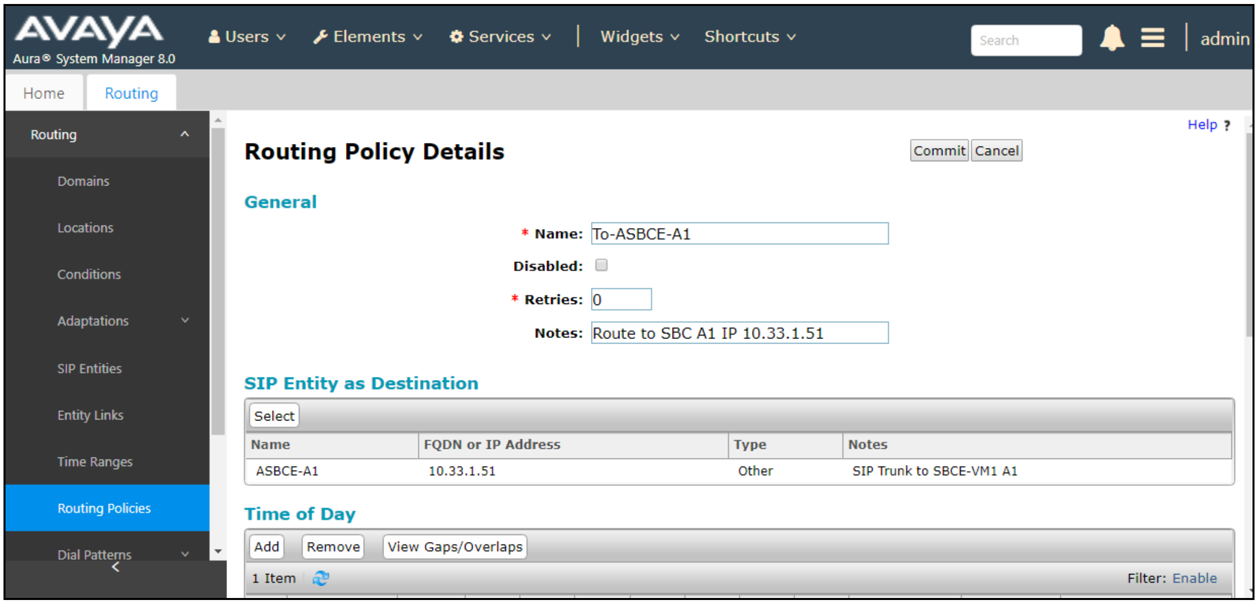
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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 for Communication Manager.



The following screen shows the Routing Policy for the Avaya SBCE.



6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were needed to route calls from Communication Manager to TELUS and vice versa. Dial Patterns define which Route Policy will be selected 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 (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

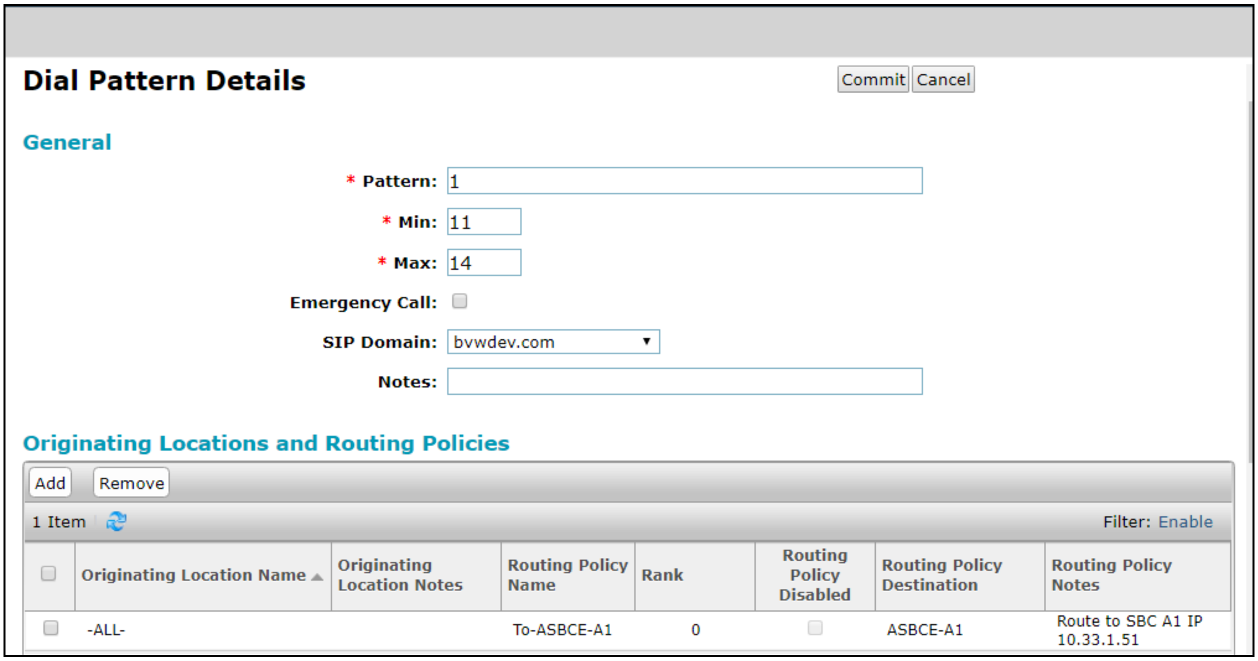
In the **General** section, enter the following values. Use default values for all remaining fields.

- **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).

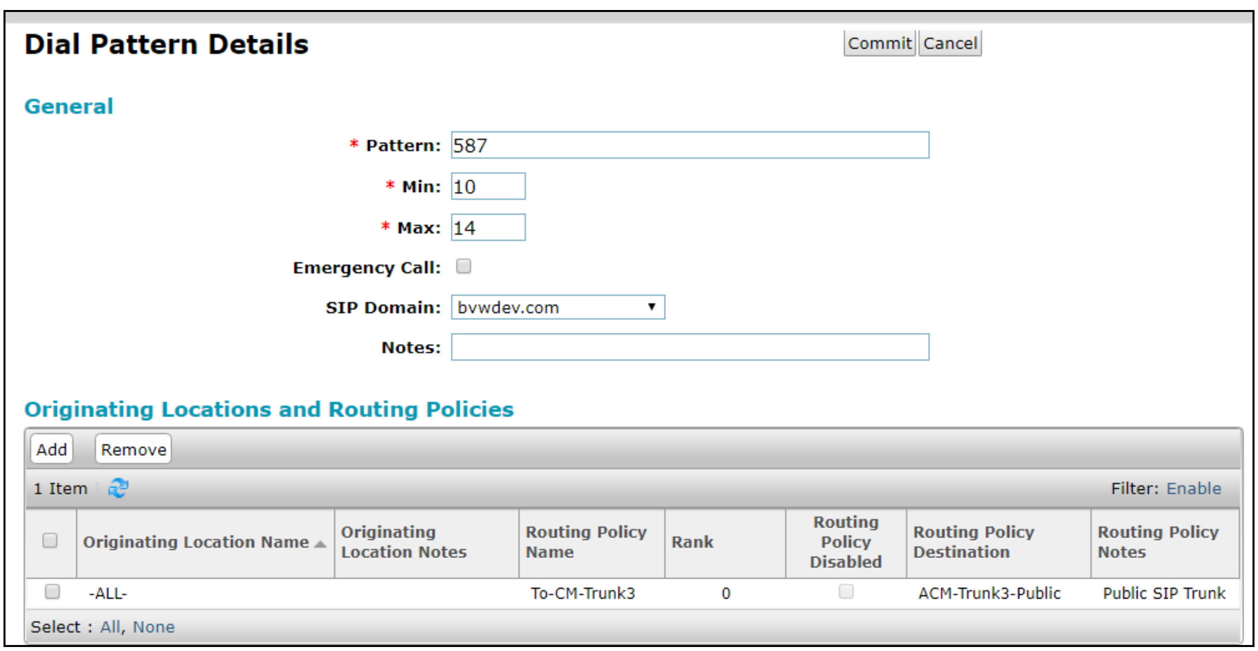
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

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

Two examples of the Dial Patterns used for the compliance test are shown below. The first example shows that outbound long distance numbers (11 digits) that begin with **1** to destination domain of **bvwdev.com** from **ALL** locations use route policy **To-ASBCE-A1**.



The second example shows that incoming DID numbers (10 digits) that start with **587** to domain **bvwdev.com** and originating from **ALL** locations use route policy **To-CM-Trunk3**. These are the DID numbers assigned to the enterprise from TELUS. All other Dial Patterns used as part of the compliance test were configured in a similar manner.



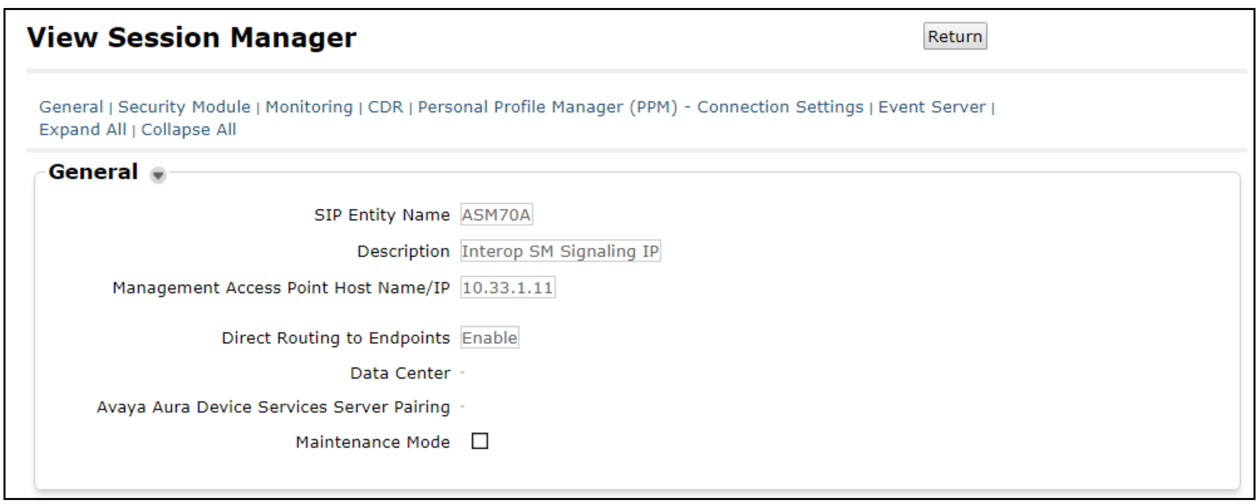
6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is most likely done as part of the initial Session Manager installation. To add a Session Manager, from the **Home** page, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the host name or IP address of the Session Manager management interface.

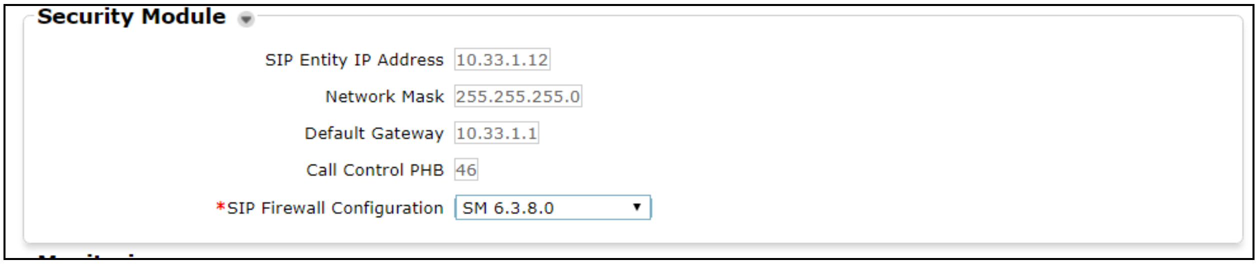
The screen below shows the Session Manager values used for the compliance test.



In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter the IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.



7. Configure Avaya Session Border Controller for Enterprise

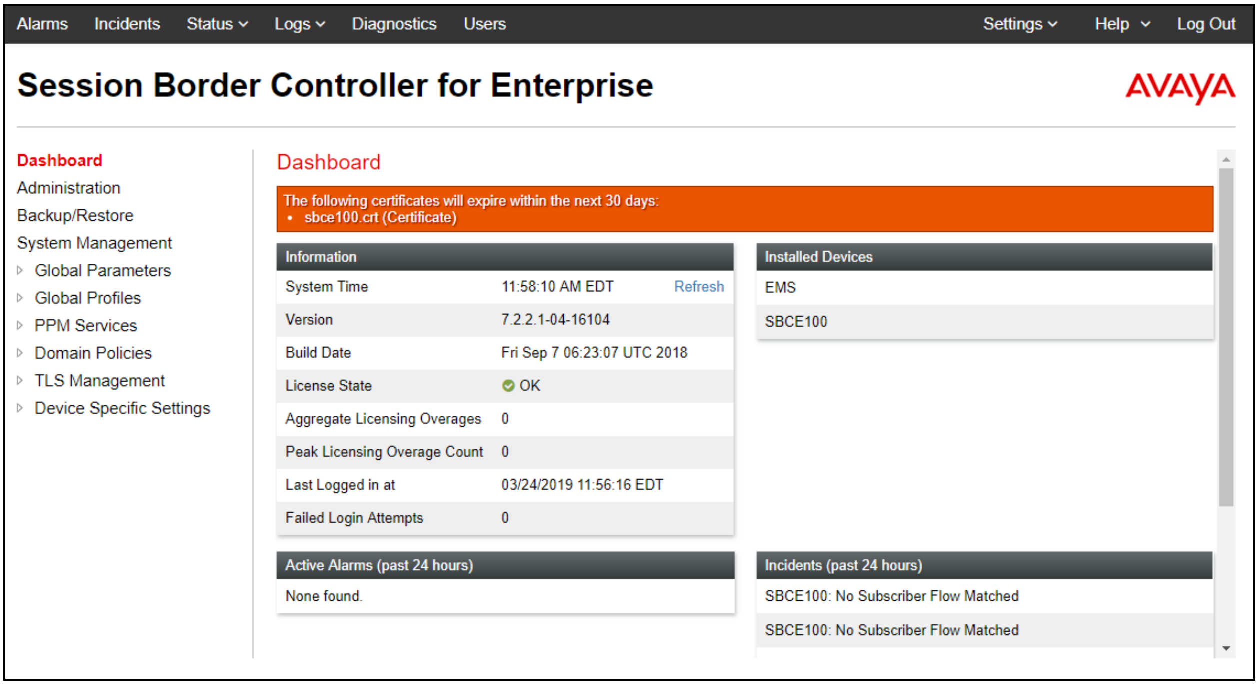
This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1).

On all screens described in this section, it is assumed that parameters are left at their default values unless specified otherwise.

7.1. Access the Management Interface

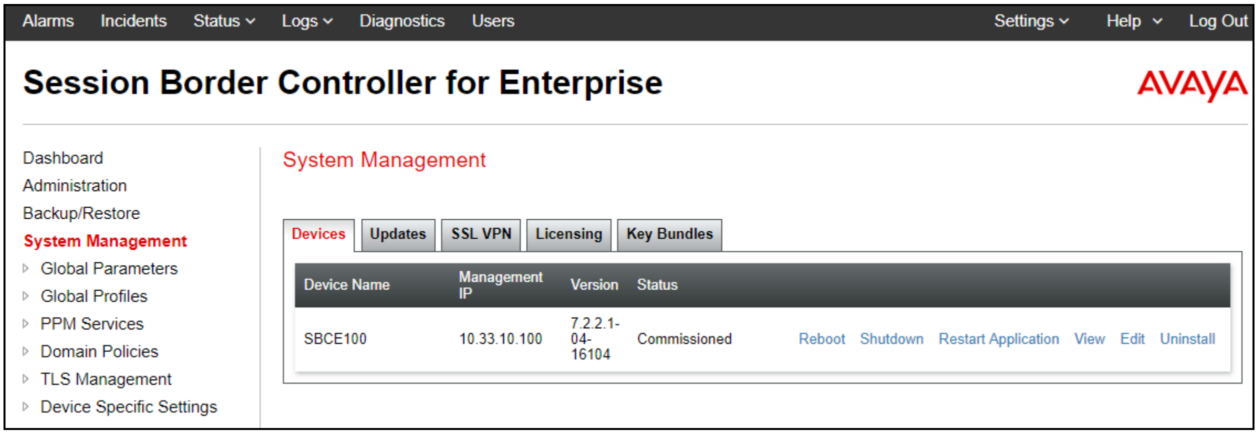
Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.

After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

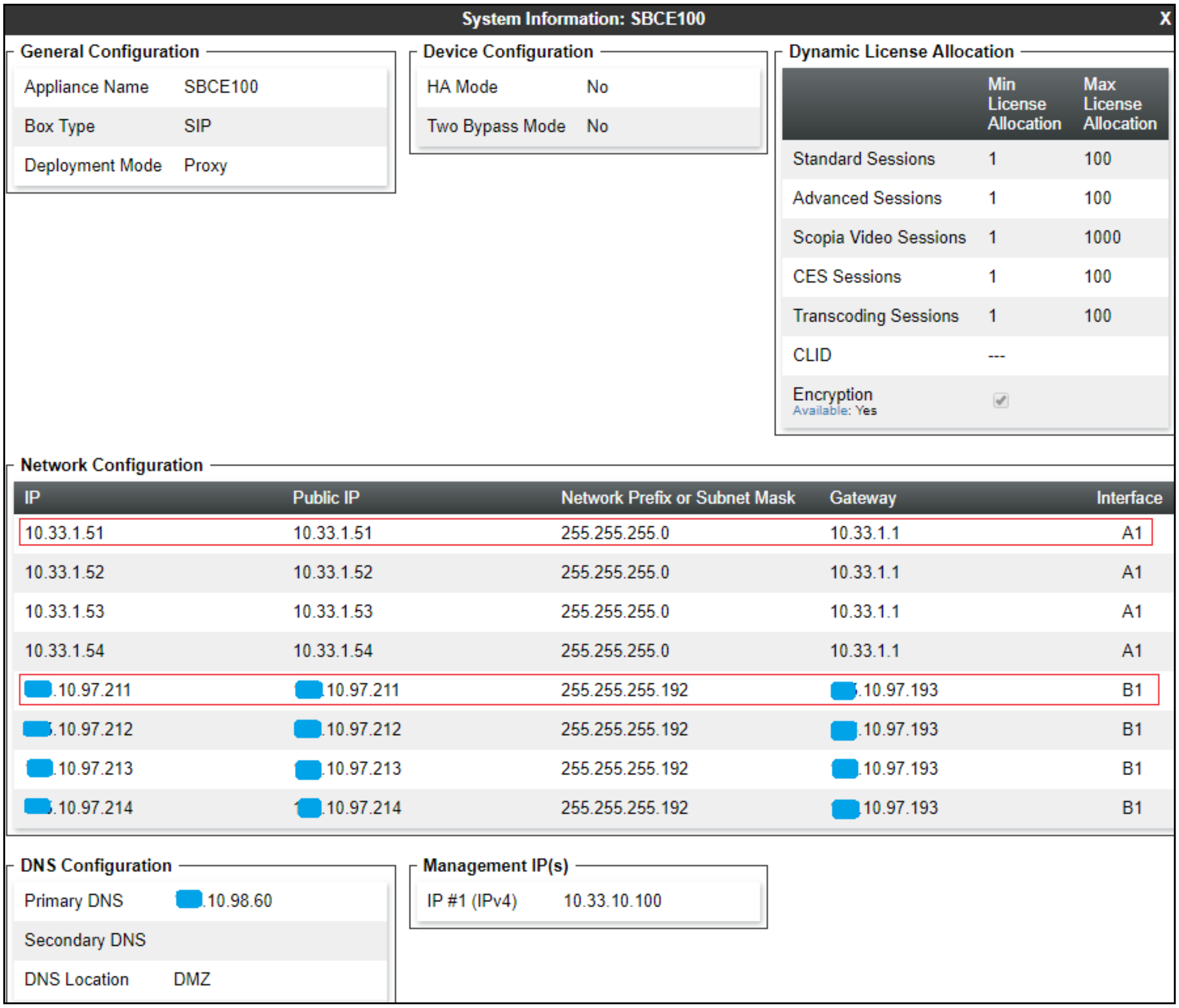


7.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.



A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**SBCE100**). This name will be referenced in other configuration screens. The two **Network Configuration** entries highlighted below are the only two IP addresses that are directly related to the SIP trunking solution described in these Application Notes. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE respectively. Each of these interfaces must be enabled after installation.



System Information: SBCE100

General Configuration

Appliance Name	SBCE100
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	1	100
Advanced Sessions	1	100
Scopia Video Sessions	1	1000
CES Sessions	1	100
Transcoding Sessions	1	100
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
[redacted].10.97.211	[redacted].10.97.211	255.255.255.192	[redacted].10.97.193	B1
[redacted].10.97.212	[redacted].10.97.212	255.255.255.192	[redacted].10.97.193	B1
[redacted].10.97.213	[redacted].10.97.213	255.255.255.192	[redacted].10.97.193	B1
[redacted].10.97.214	[redacted].10.97.214	255.255.255.192	[redacted].10.97.193	B1

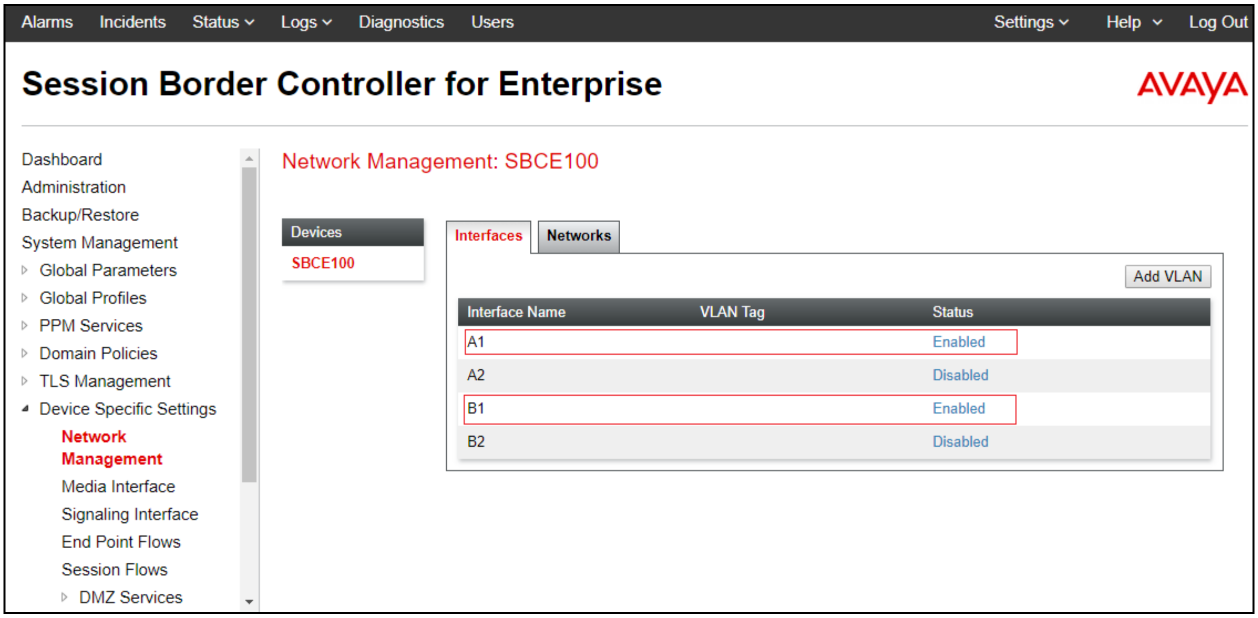
DNS Configuration

Primary DNS	[redacted].10.98.60
Secondary DNS	
DNS Location	DMZ

Management IP(s)

IP #1 (IPv4)	10.33.10.100

To enable the interfaces, first navigate to **Device Specific Settings → Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the status **Enabled/Disabled** to toggle the state of the interface.



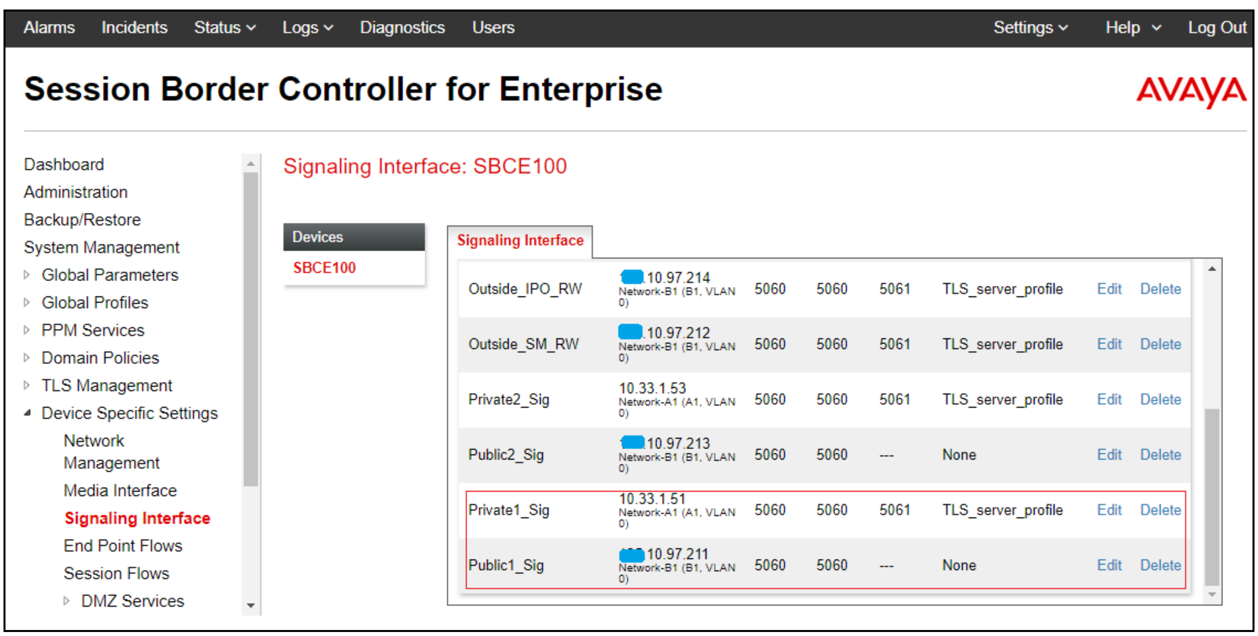
7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**SBCE100**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by one or more pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Private1_Sig** was created for the Avaya SBCE internal interface and signaling interface **Public1_Sig** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since TELUS will send messages using UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.



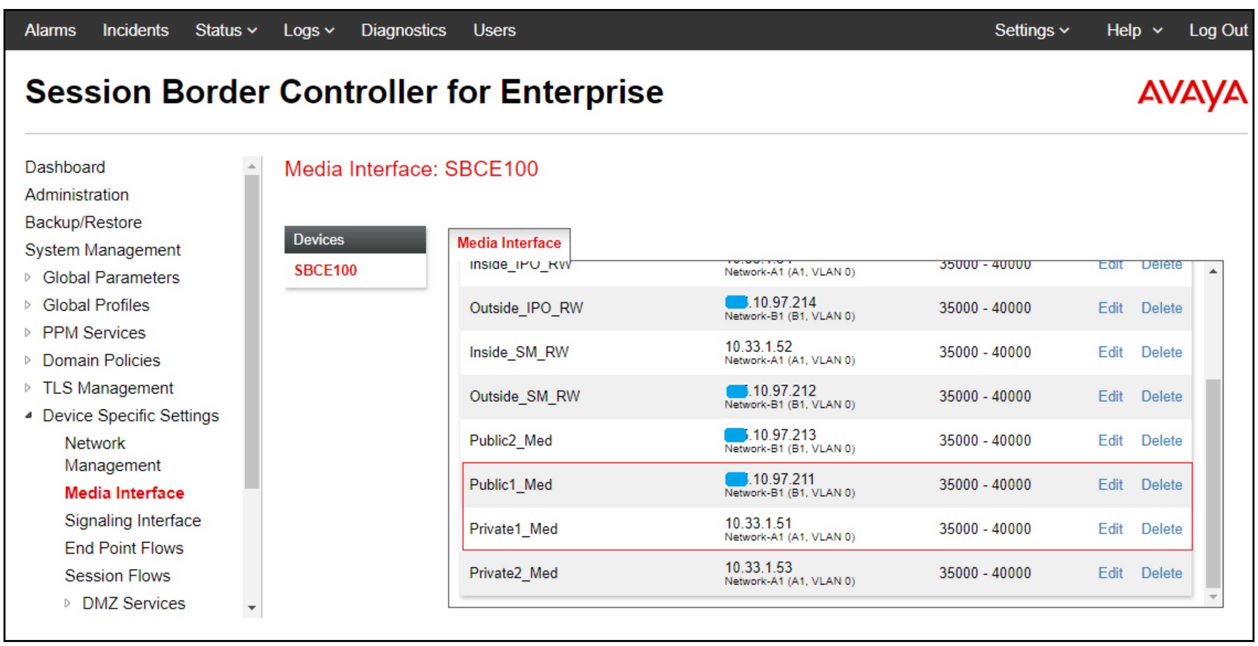
7.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**SBCE100**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by one or more pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Private1_Med** was created for the Avaya SBCE internal interface and media interface **Public1_Med** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

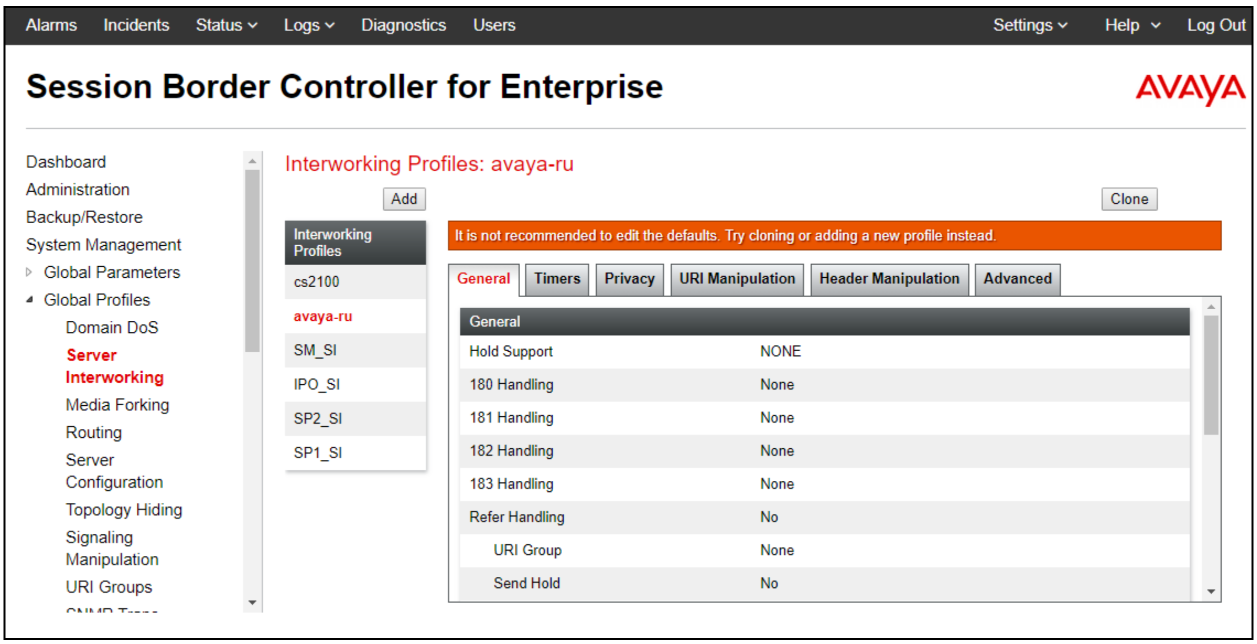
- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.



7.5. Server Interworking

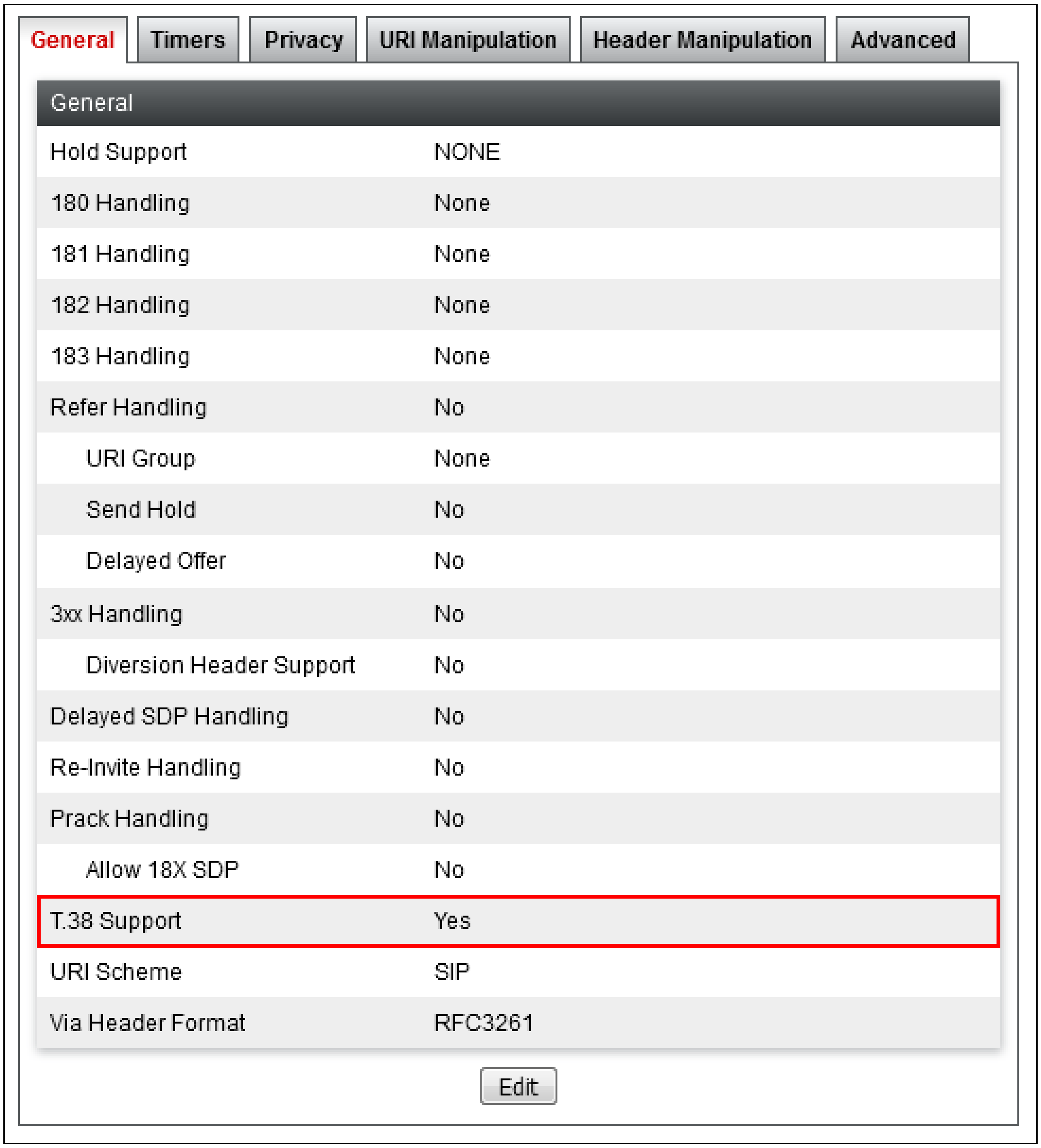
A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create a server interworking profile for Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Sections 7.7.1** and **7.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.



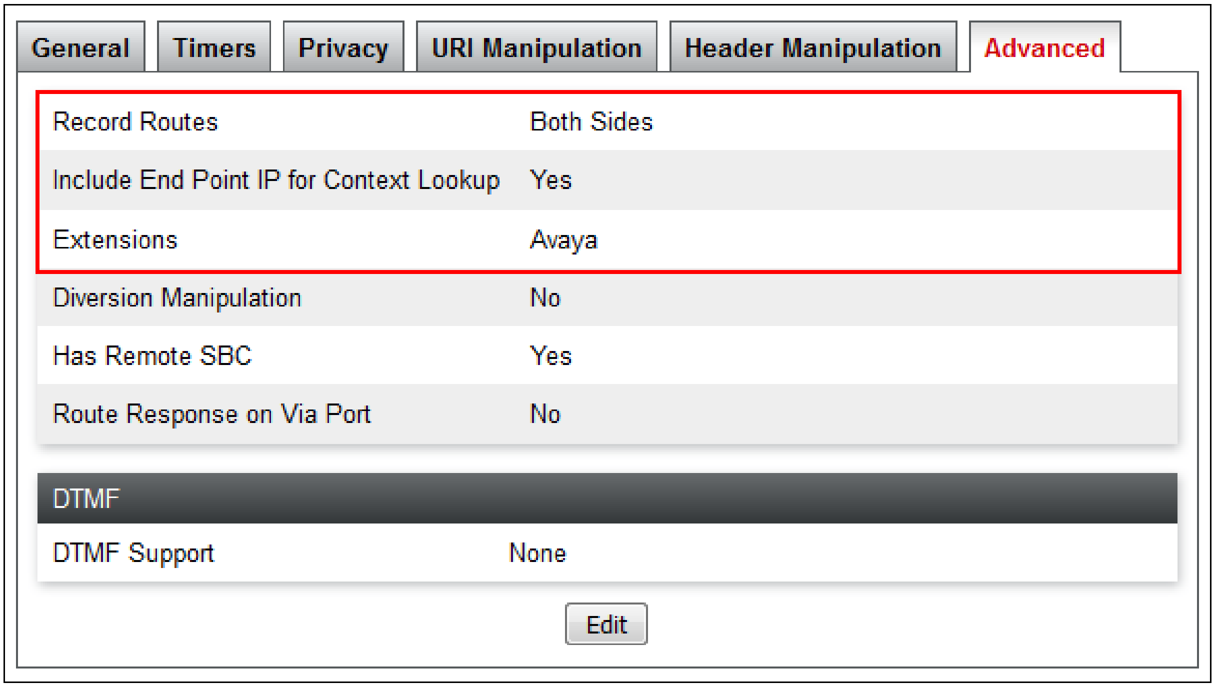
7.5.1. Server Interworking – Session Manager

For the compliance test, server interworking profile **Avaya-SM-T38** was created for Session Manager by cloning the existing profile **avaya-ru**. **T.38 Support** was set to **Yes**. Highlighted values in this section indicate changes from the cloned profile or the default value. The **General** tab parameters are shown below.



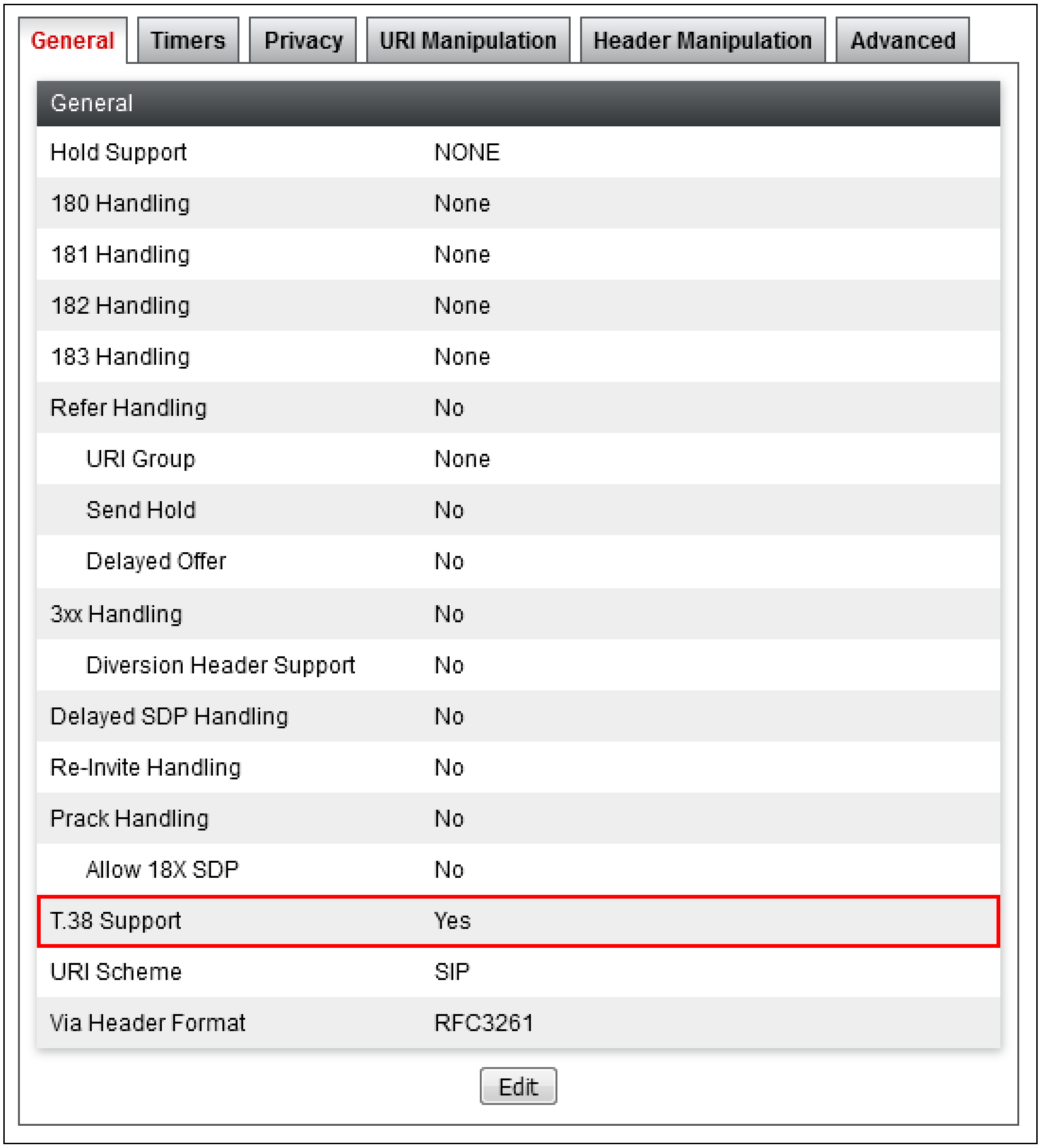
The **Timers**, **Privacy**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below.



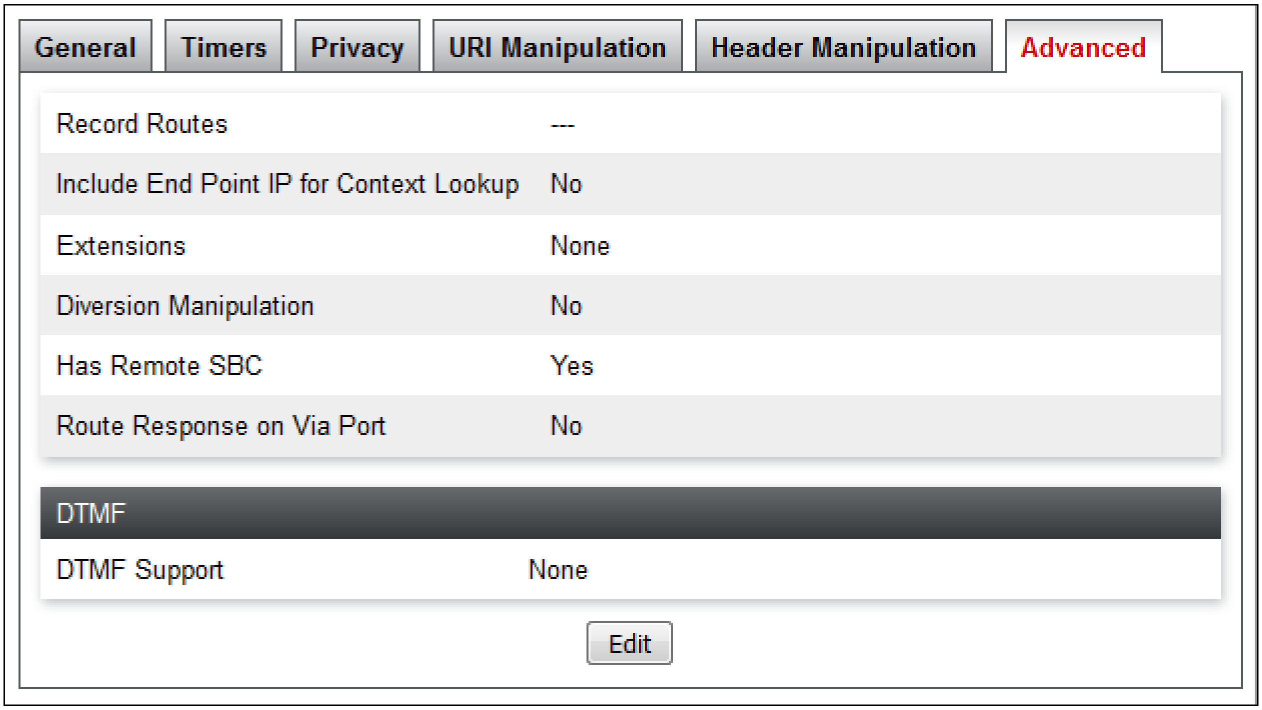
7.5.2. Server Interworking – TELUS

For the compliance test, server interworking profile **SP1_SI** was created for the TELUS SIP server. When creating the profile, the default values were used for all parameters with the exception that **T.38 Support** was set to **Yes**. The **General** tab parameters are shown below.



The **Timers**, **Privacy**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

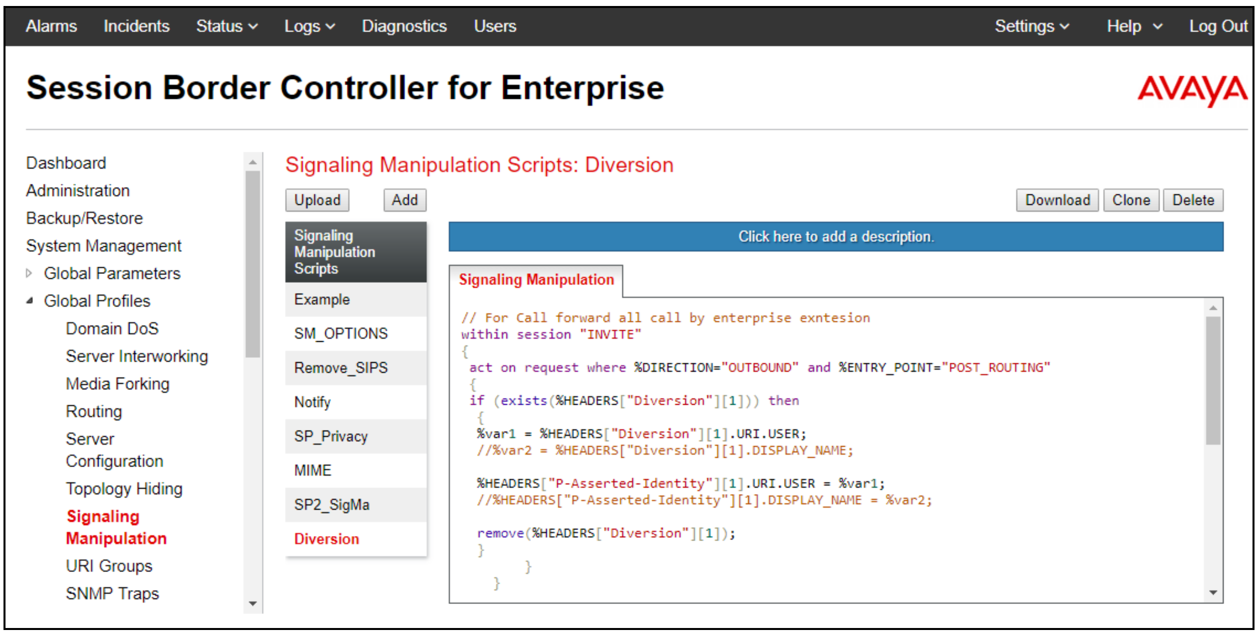
The **Advanced** tab parameters are shown below.



7.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be done by other configuration within the Avaya SBCE. TELUS required the signaling manipulation script defined in **Section 7.6.1**. It is applied to the TELUS SIP server in **Section 7.7.2**.

To create a script, navigate to **Global Profiles → Signaling Manipulation** in the left pane. In the center pane, select **Add**. A script editor window (not shown) will appear in which the script can be entered line by line. The **Title** box at the top of the editor window (not shown) is where the name of the script is entered. Once complete, the script is shown in the far right pane. To view an existing script, select the script from the center pane. The settings will appear in the right pane as shown in the example below.



7.6.1. Signaling Manipulation Script – TELUS

For the compliance test, signaling manipulation script **Diversion** was created for the TELUS SIP server. The script contains two manipulations. The first checks to see if a Diversion header is present in the outbound INVITE, and if so it will overwrite the user and display name in the PAI header with the contents of the Diversion Header. This is necessary for call forwarding and EC500. In these scenarios, TELUS expects the information provided by Communication Manager in the Diversion header to be present in the PAI. The script instructions to perform this manipulation are shown below.

```
// For Call forward all call and EC500
within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
 {
 if (exists(%HEADERS["Diversion"][1])) then
  {
  %var1 = %HEADERS["Diversion"][1].URI.USER;
  //%var2 = %HEADERS["Diversion"][1].DISPLAY_NAME;

  %HEADERS["P-Asserted-Identity"][1].URI.USER = %var1;
  //%HEADERS["P-Asserted-Identity"][1].DISPLAY_NAME = %var2;

  remove(%HEADERS["Diversion"][1]);
  }
        }
    }
```

Below is the signaling script that replaces a number in the P-Asserted-Identity (PAI) header to a known DID number provided by Telus for the consultative transfer call in Experience Portal.

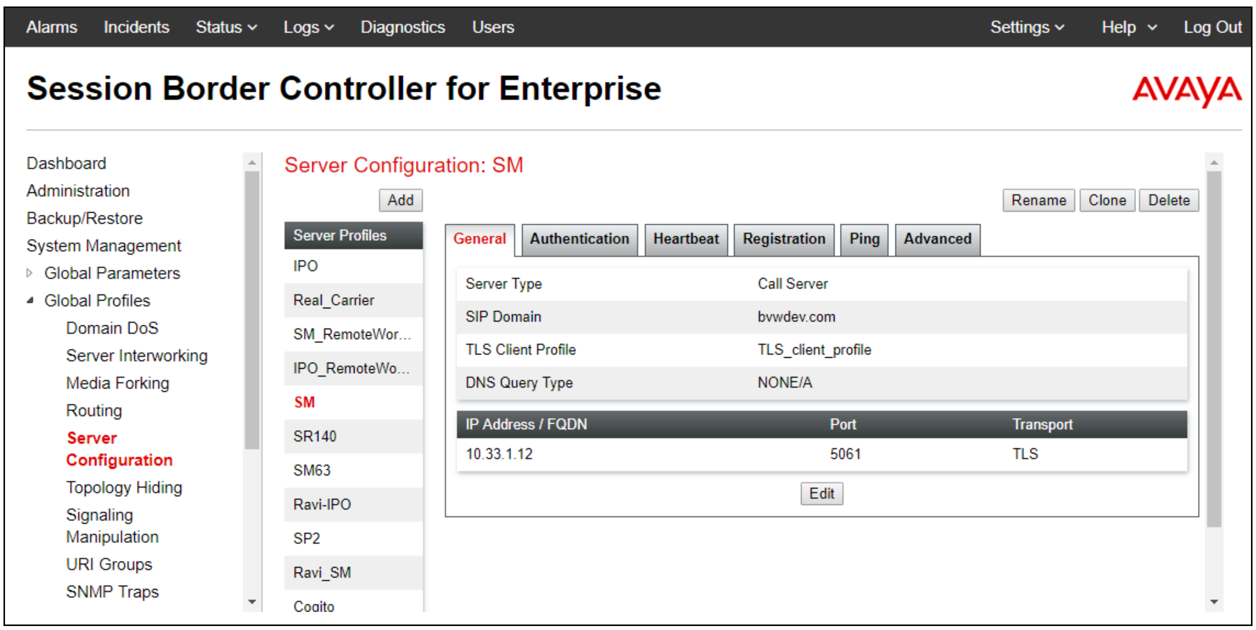
```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
if (%HEADERS["P-Asserted-
Identity"][1].URI.USER.regex_match("587233030[2-3]")) then
           {
            %var="this does nothing, match for DID number passed";
           }
         else
           {
           %HEADERS["P-Asserted-Identity"][1].URI.USER = "5872330303";
}

}
}
```

7.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a server configuration profile for Session Manager and the service provider SIP server.

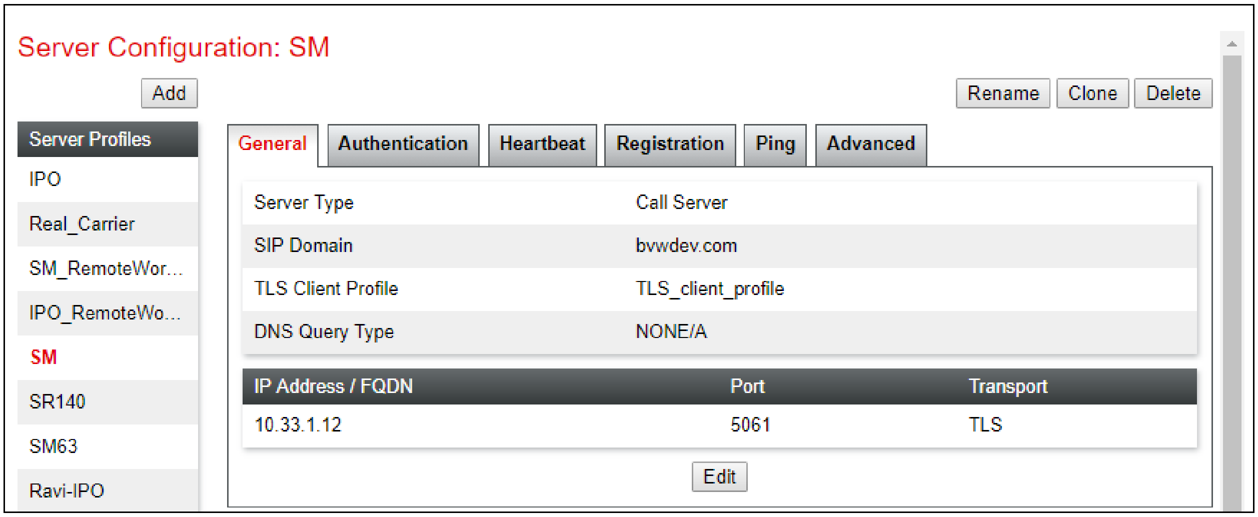
To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured. Once complete, the profile name will appear under **Server Profiles** in the center pane and the settings will be shown in the far right pane. If a profile already exists, then the settings of the existing profile may be viewed by selecting the profile from the center pane. The settings will appear in the right pane.



7.7.1. Server Configuration – Session Manager

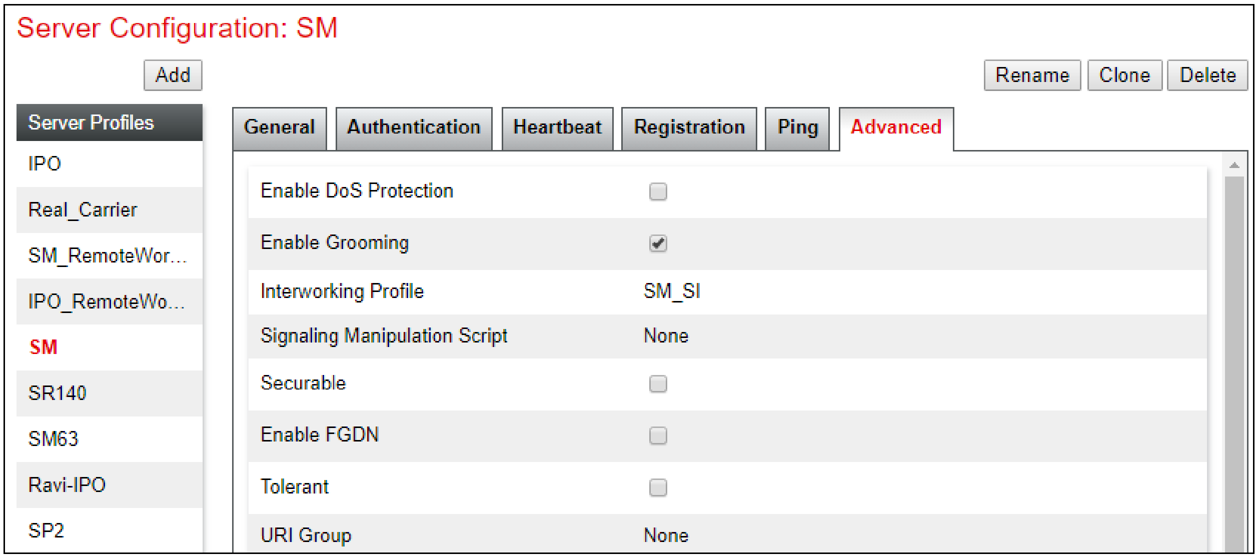
For the compliance test, server configuration profile **SM** was created for Session Manager. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Call Server**.
- Enter a sip domain in **SIP Domain**.
- Select a TLS profile in the **TLS Client Profile** dropdown menu.
- Enter a valid combination of **IP Address / FQDN**, **Port** and **Transport** that Session Manager will use to listen for SIP requests. The standard SIP UDP/TCP port is 5060. The standard SIP TLS port is 5061. Additional combinations can be entered by clicking the **Add** button (not shown).



The **Authentication** and **Heartbeat** tabs have no entries.

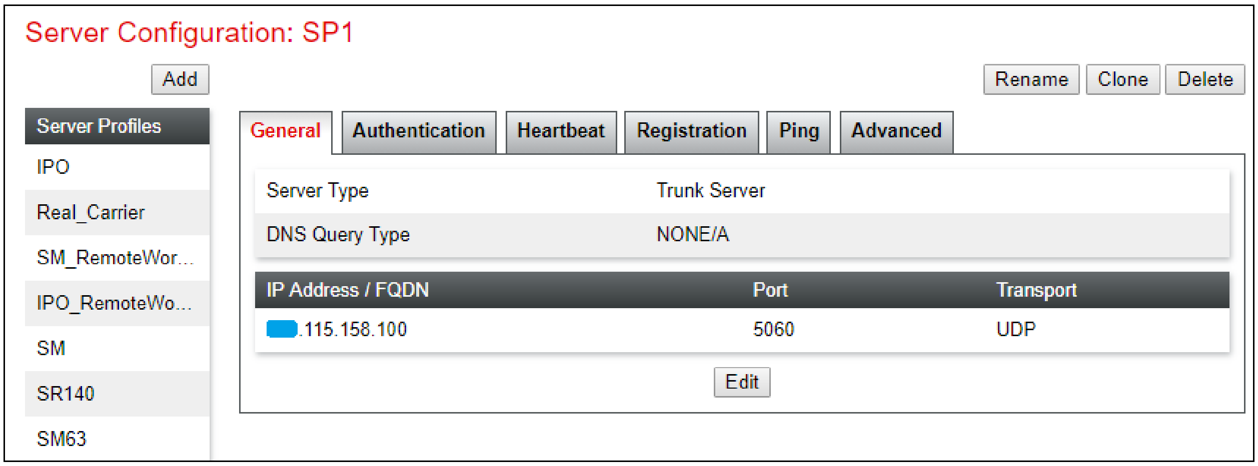
On the **Advanced** tab, check **Enable Grooming** and set the **Interworking Profile** field to the interworking profile for Session Manager defined in **Section 7.5.1**. A complete description of the use of TLS certificates are beyond the scope of these Application Notes.



7.7.2. Server Configuration – TELUS

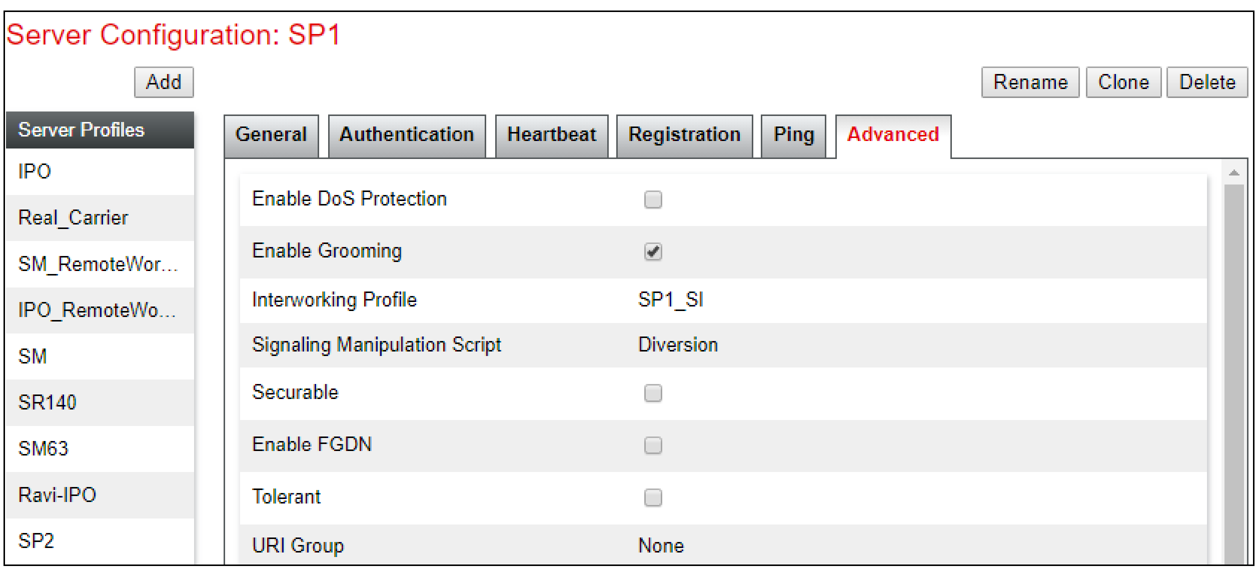
For the compliance test, server configuration profile **SP1** was created for TELUS. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Trunk Server**.
- Enter a valid combination of **IP Address / FQDN**, **Port** and **Transport** that the TELUS SIP proxy will use to listen for SIP requests. This information is provided by TELUS. Additional combinations can be entered by clicking the **Add** button (not shown).



The **Authentication** and **Heartbeat** tabs have no entries.

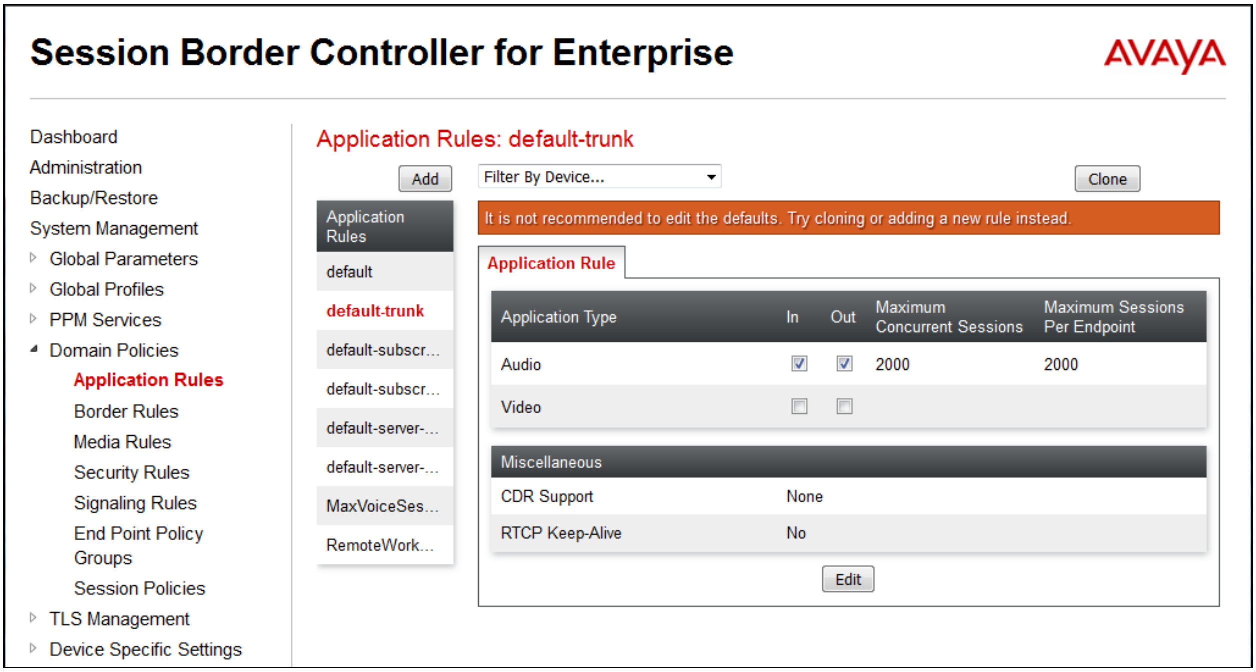
On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for TELUS defined in **Section 7.5.2**. Set the **Signaling Manipulation Script** to **Diversion** defined in **Section 7.6.1.**



7.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 7.11**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Session Manager and the TELUS SIP server.

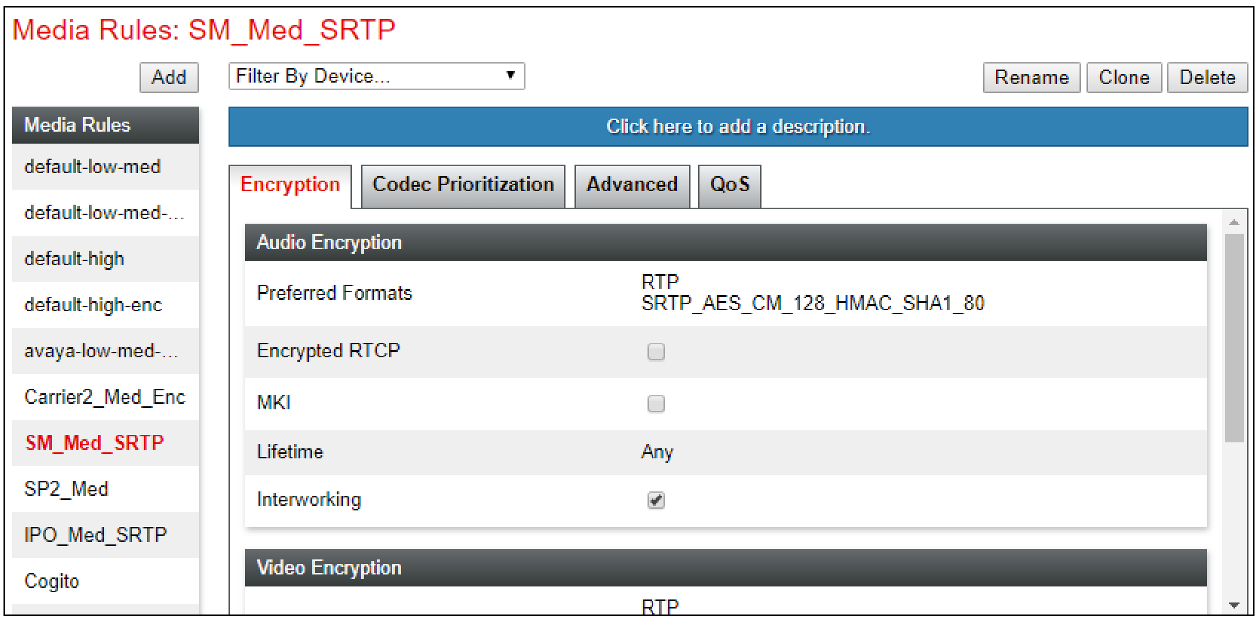
To view an existing rule, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select the rule (e.g., **default-trunk**) to be viewed.



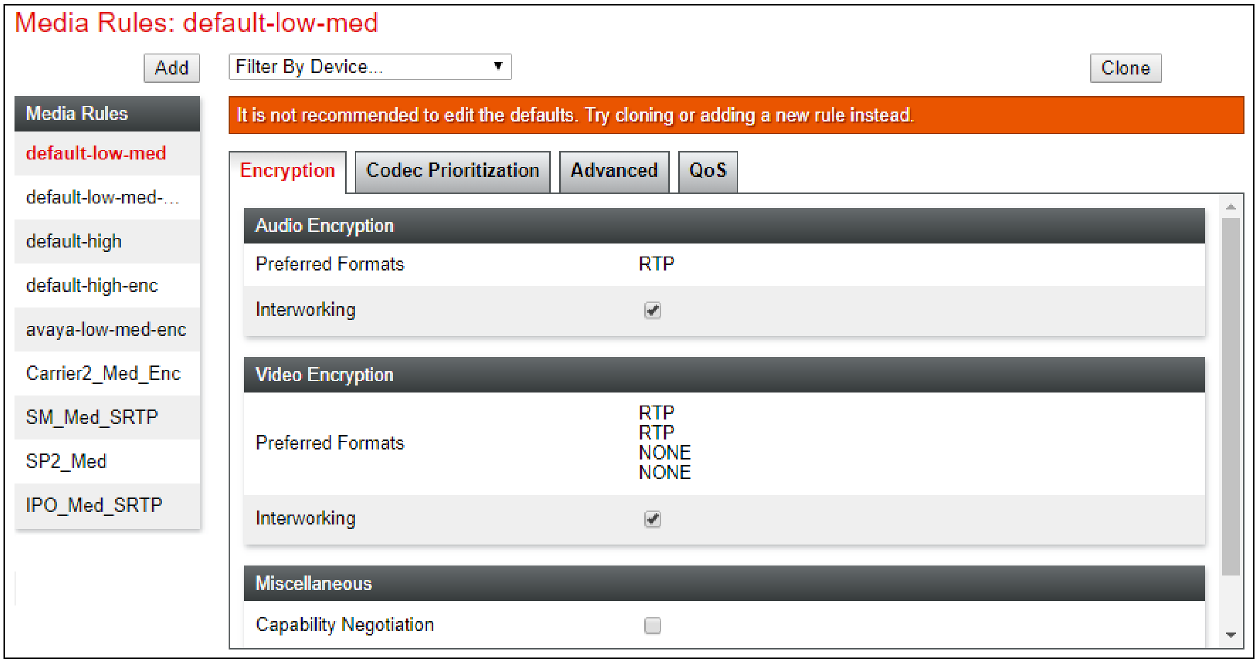
7.9. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward Session Manager and one toward the Service Provider.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**. The media rule **SM_Med_SRTP** below was used for the testing. Default values are kept in the other tabs.



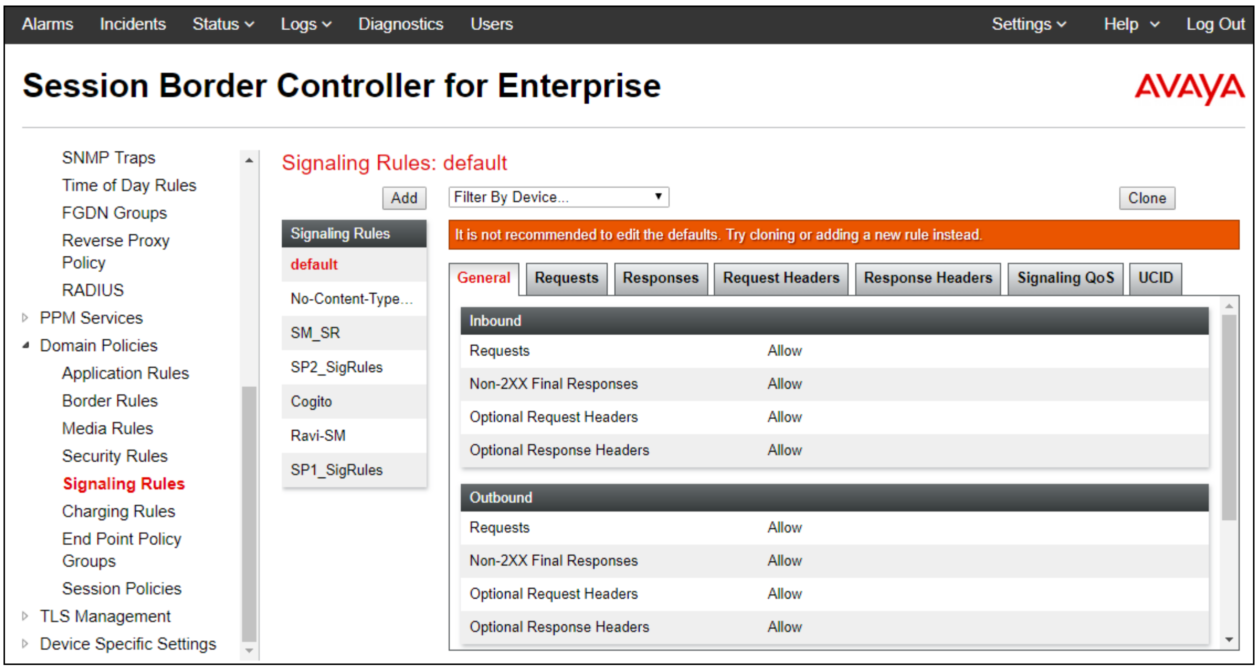
For the compliance test, the **default-low-med** Media Rule was used in the Service Provider direction.



7.10. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.11**. A specific signaling rule was created for Session Manager and the TELUS SIP server.

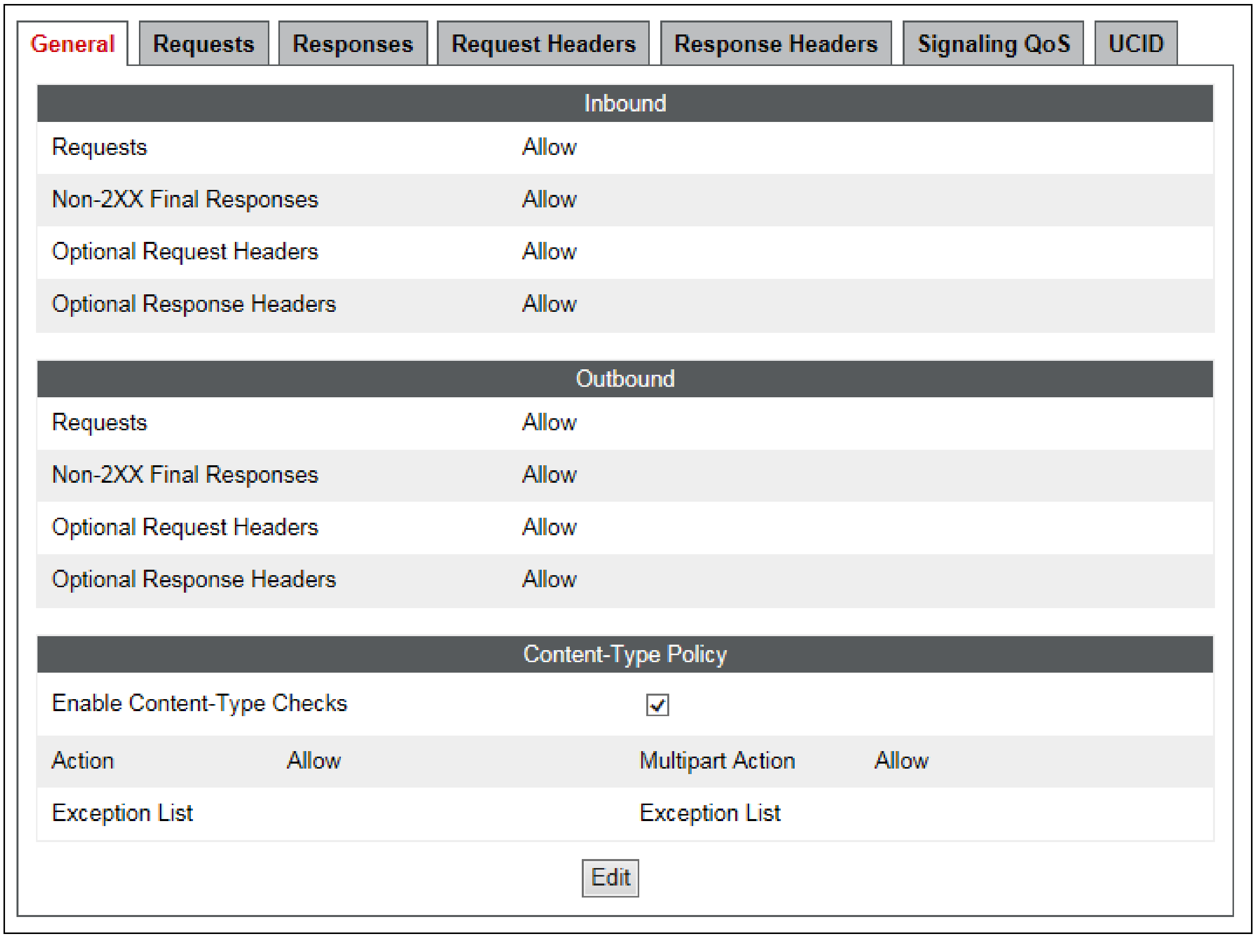
To create a new rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by one or more pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.



7.10.1. Signaling Rules – Session Manager

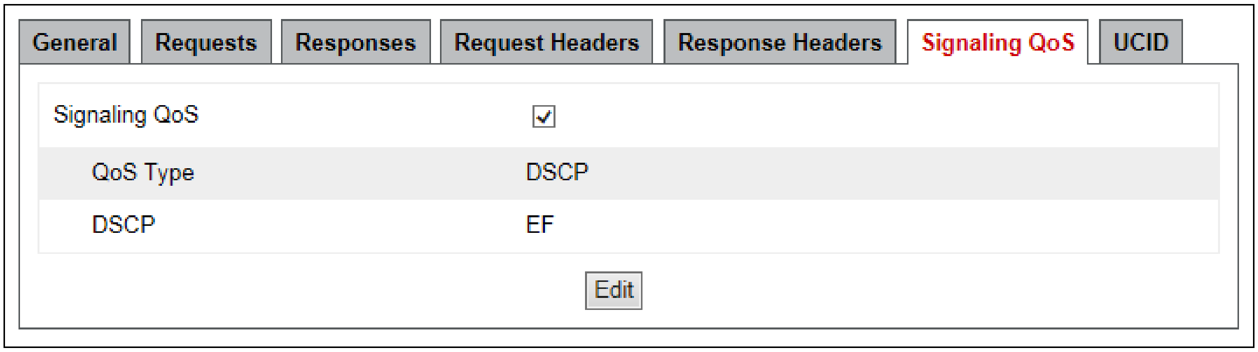
For the compliance test, signaling rule **SM_SigRules** was created for Session Manager. **SM_SigRules** was created using all default values except the **Signaling QoS** tab.

The **General** tab settings are shown below.



The **Requests**, **Responses**, **Request Headers**, and **Response Headers** tabs have no entries.

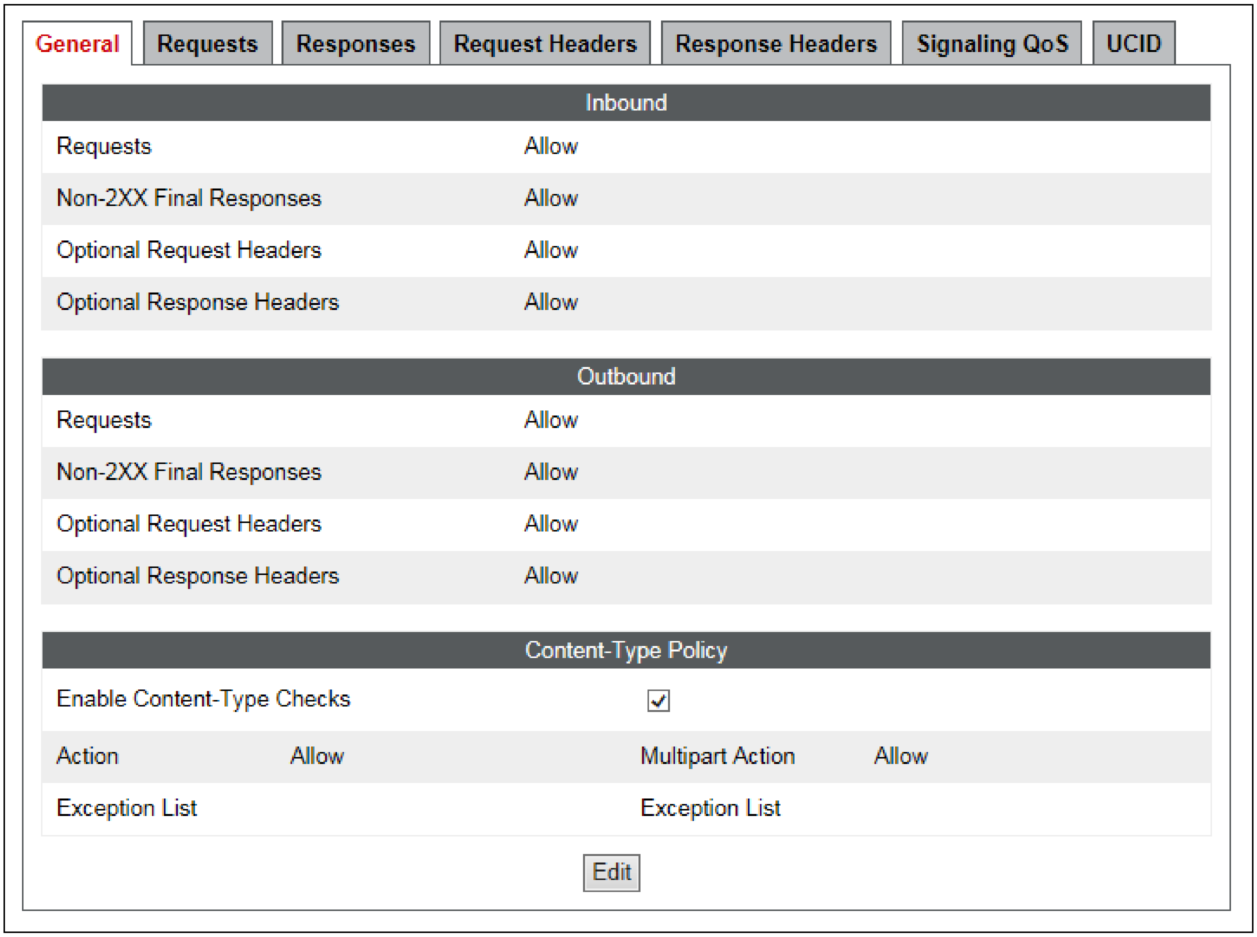
The **Signaling QoS** settings used for the compliance test are shown below. These QoS settings are not a requirement for interoperability and QoS is not tested as part of the compliance test. If the QoS settings shown here do not meet the needs of the customer then they should be set as per customer requirements.



The **UCID** setting is shown below.

7.10.2. Signaling Rules – TELUS

The **SP1_SigRules** signaling rule (shown below) was used for the TELUS SIP server. The **General** tab settings use the default values and are shown below.



General | Requests | Responses | Request Headers | Response Headers | Signaling QoS | UCID

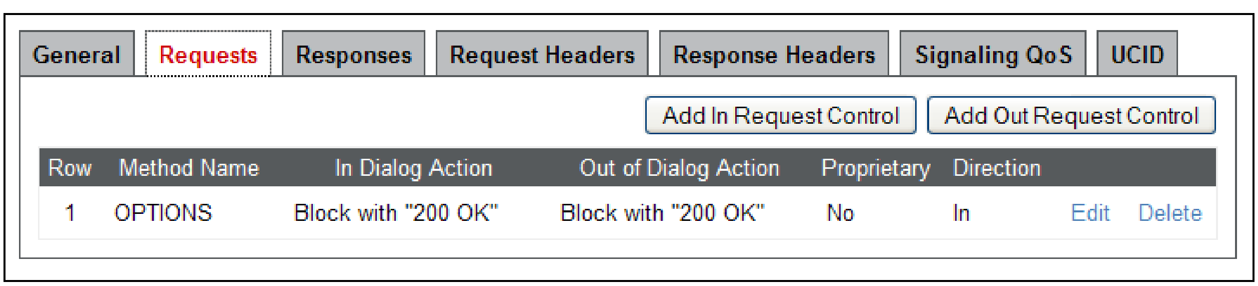
Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Edit

The **Requests** tab shows the actions performed on request messages. An entry is created by clicking the **Add In Header Control** or **Add Out Header Control** button depending on the direction (relative to the Avaya SBCE) of the message to be modified. The entry shown below blocks incoming OPTIONS messages and returns a 200 OK response. See **Section 2.2** for full details.



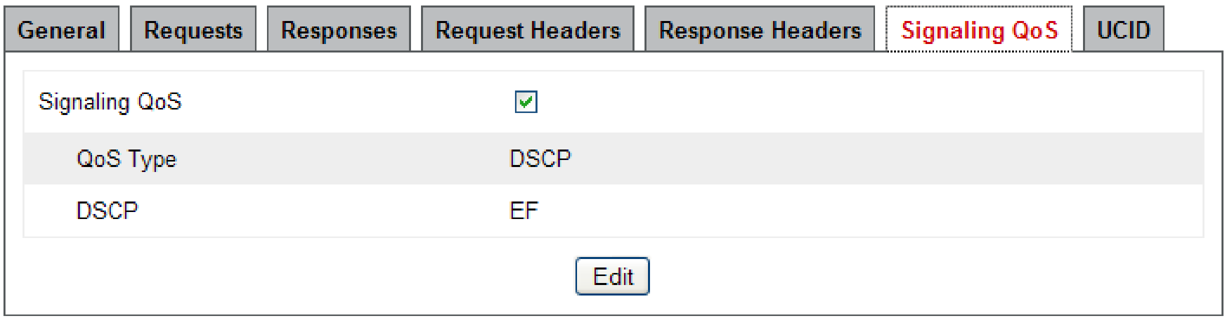
General | Requests | Responses | Request Headers | Response Headers | Signaling QoS | UCID

Add In Request Control | Add Out Request Control

Row	Method Name	In Dialog Action	Out of Dialog Action	Proprietary	Direction		
1	OPTIONS	Block with "200 OK"	Block with "200 OK"	No	In	Edit	Delete

The **Responses**, **Request Headers** and **Response Headers** tabs have no entries.

The **Signaling QoS** settings are shown below. These QoS settings are not a requirement for interoperability and QoS is not tested as part of the compliance test. If the QoS settings shown here do not meet the needs of the customer then they should be set as per customer requirements.

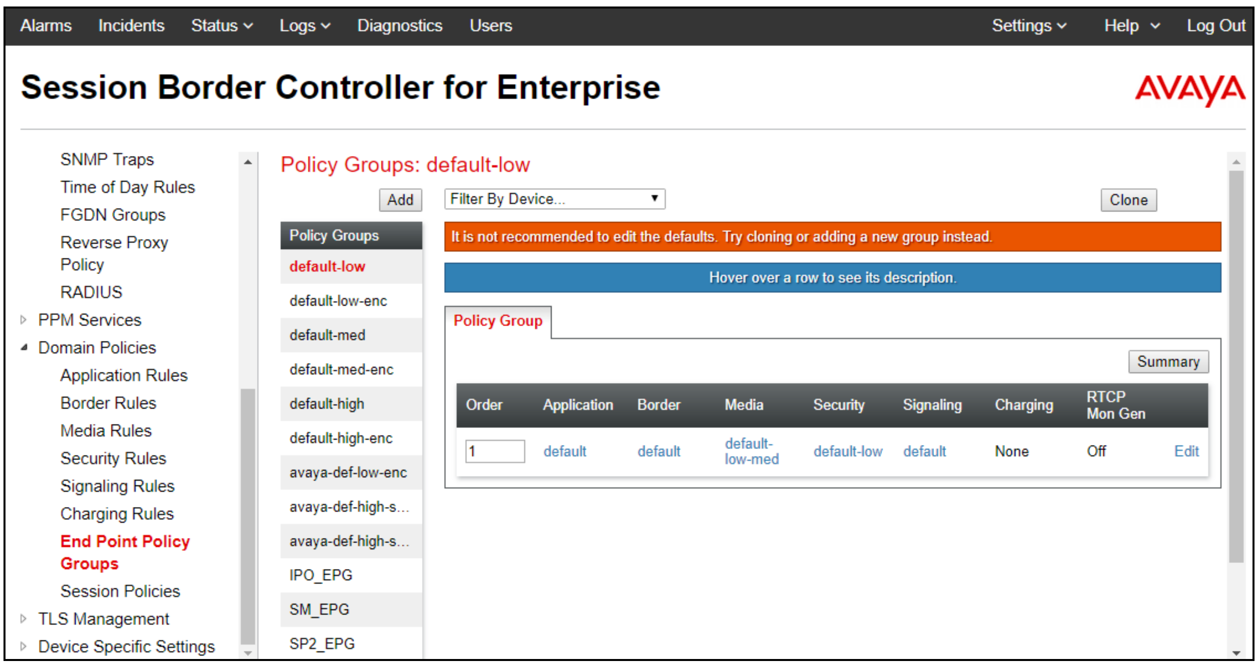


The **UCID** settings are shown below.

7.11. Endpoint Policy Groups

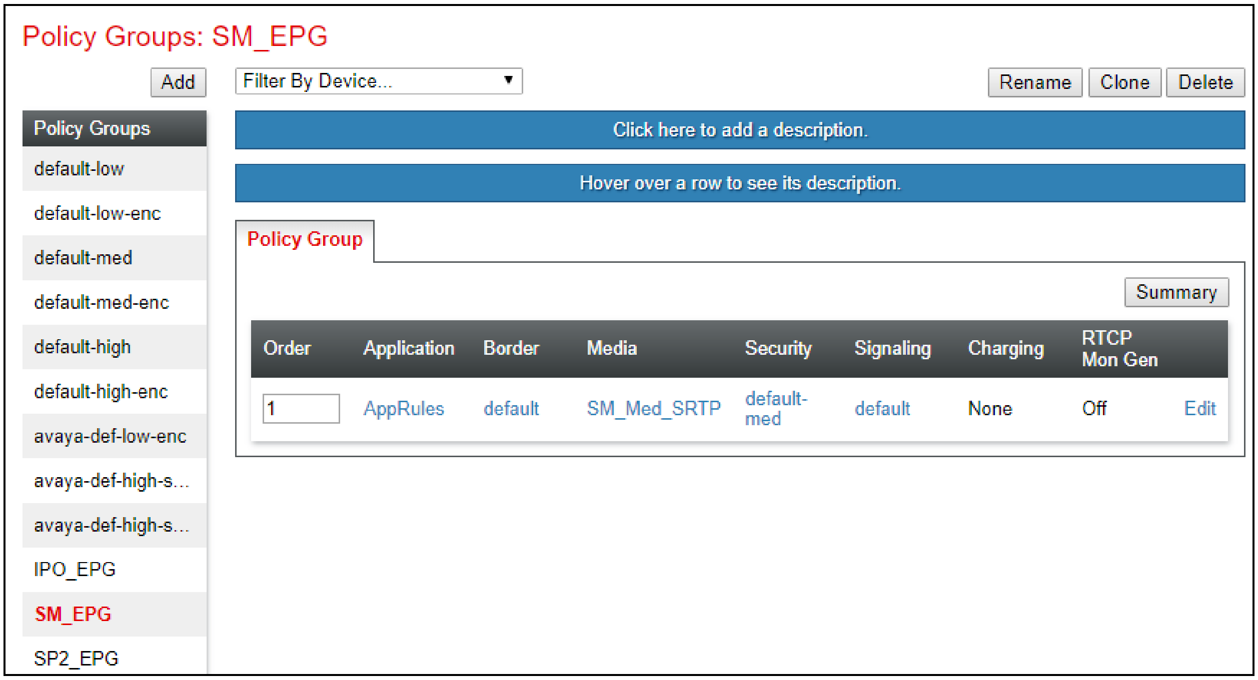
An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and an endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.14**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed one or more of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.



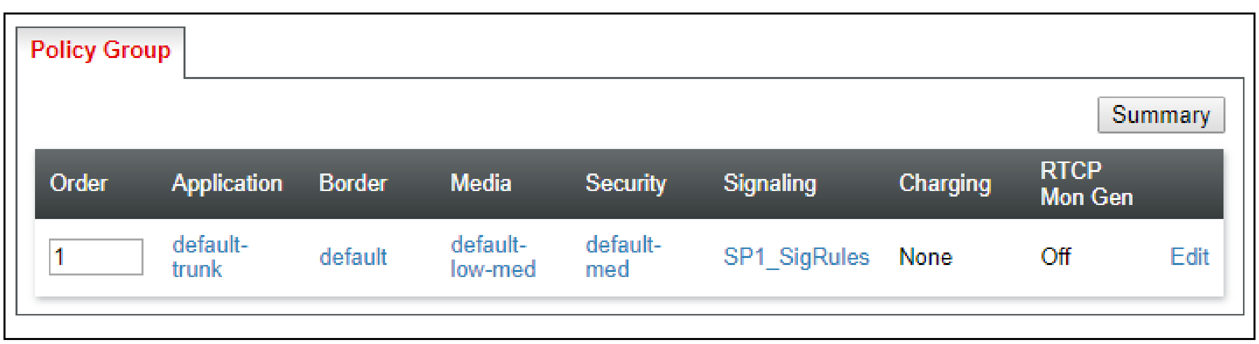
7.11.1. Endpoint Policy Group – Session Manager

For the compliance test, endpoint policy group **SM_EPG** was created for Session Manager. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Signaling**. For **Application**, enter the application rule created in **Section 7.8**. For **Signaling**, enter the signaling rule created in **Section 7.10.1**. The details of the default settings for **Media** are showed in **Section 7.9**.



7.11.2. Endpoint Policy Group – TELUS

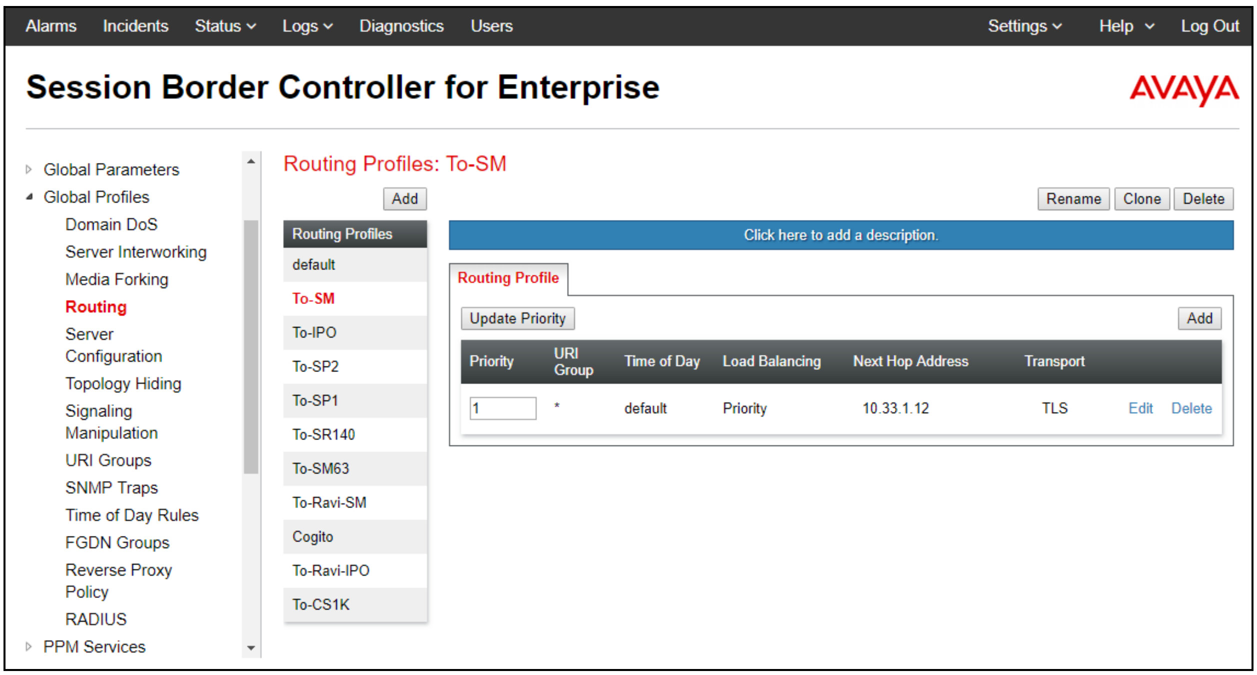
For the compliance test, endpoint policy group **SP1_EPG** was created for the TELUS SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Signaling**. For **Application**, enter the application rule created in **Section 7.8**. For **Signaling**, enter the signaling rule created in **Section 7.10.2**. The details of the default settings for **Media** are showed in **Section 7.9**.



7.12. Routing

A routing profile defines where traffic will be directed based on the contents of the Request-URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 7.14**. Create a routing profile for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

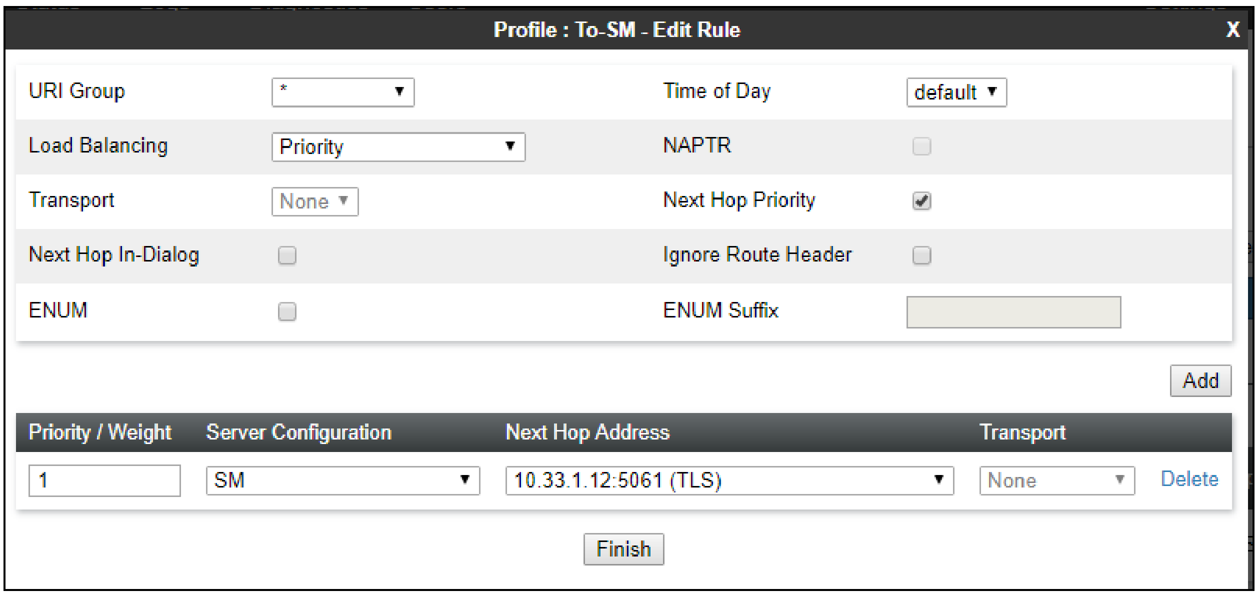


7.12.1. Routing – Session Manager

For the compliance test, routing profile **To-SM** was created for Session Manager. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set **Load Balancing** to **Priority** from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
    - Set **Priority/Weight** to **1**.
    - For **Server Configuration**, select **SM** (**Section 7.7.1**) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.

Click **Finish**.

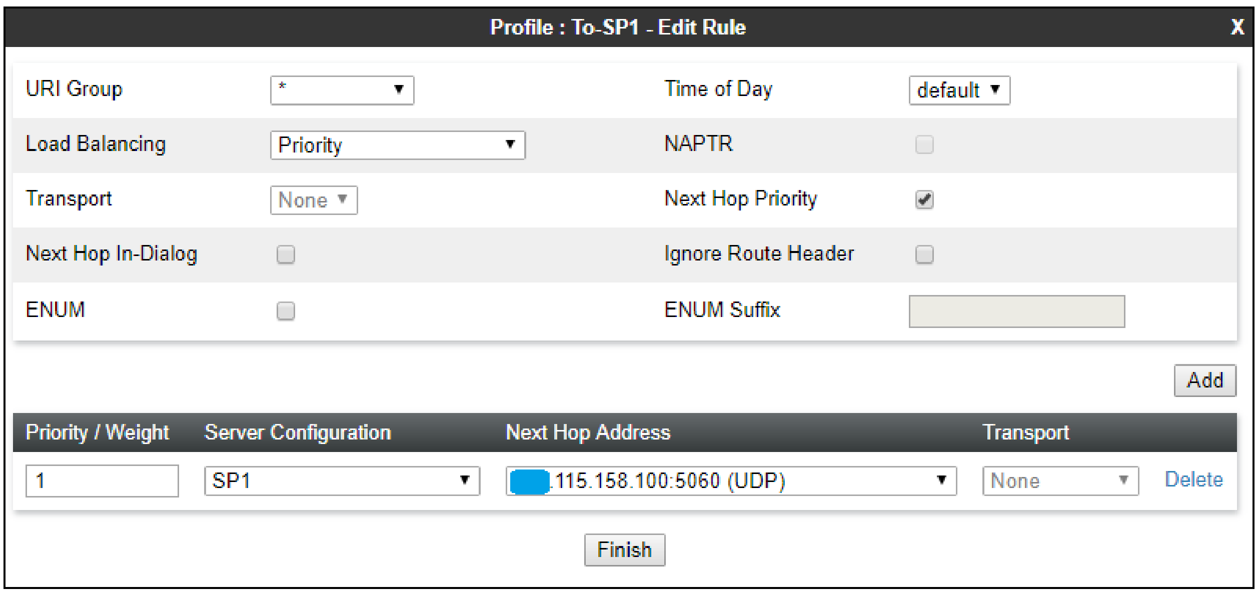


7.12.2. Routing – TELUS

For the compliance test, routing profile **To-SP1** was created for TELUS. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card ***** to match on any URI.
- Set **Load Balancing** to **Priority** from the pull-down menu.
- Click **Add** to enter the following for the Next Hop Address:
    - Set **Priority/Weight** to **1**.
    - For **Server Configuration**, select **SP1** (**Section 7.7.2**) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.

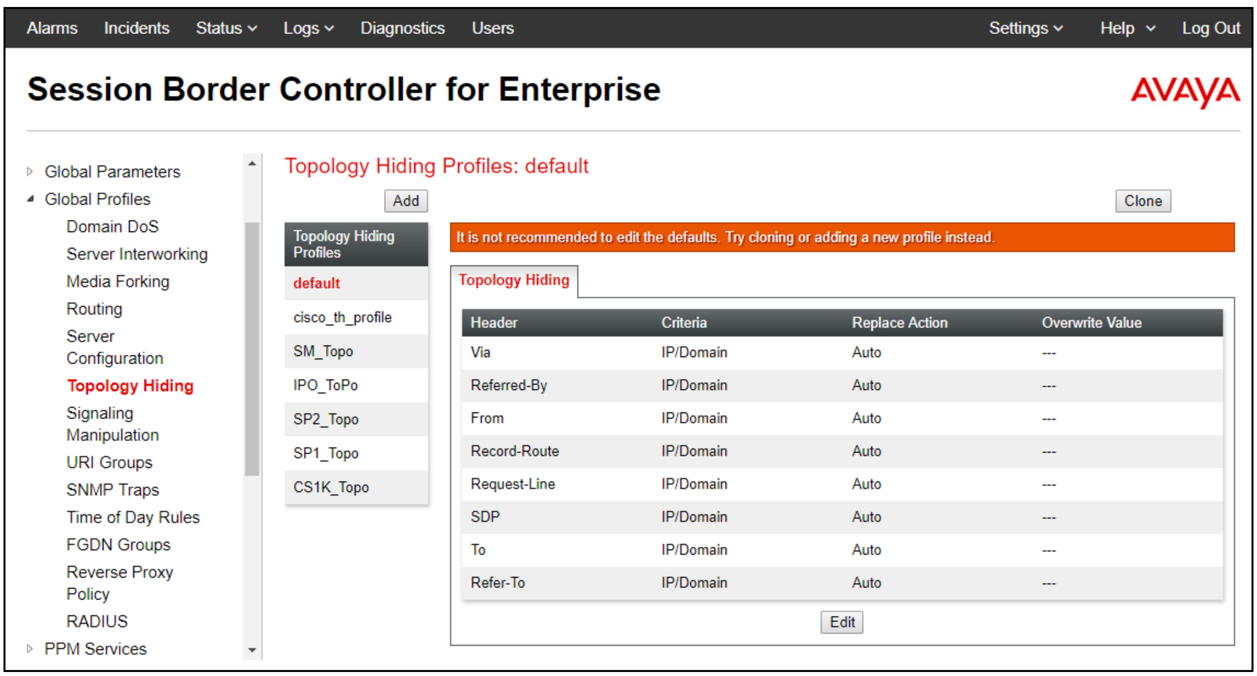
Click **Finish**.



7.13. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.14**.

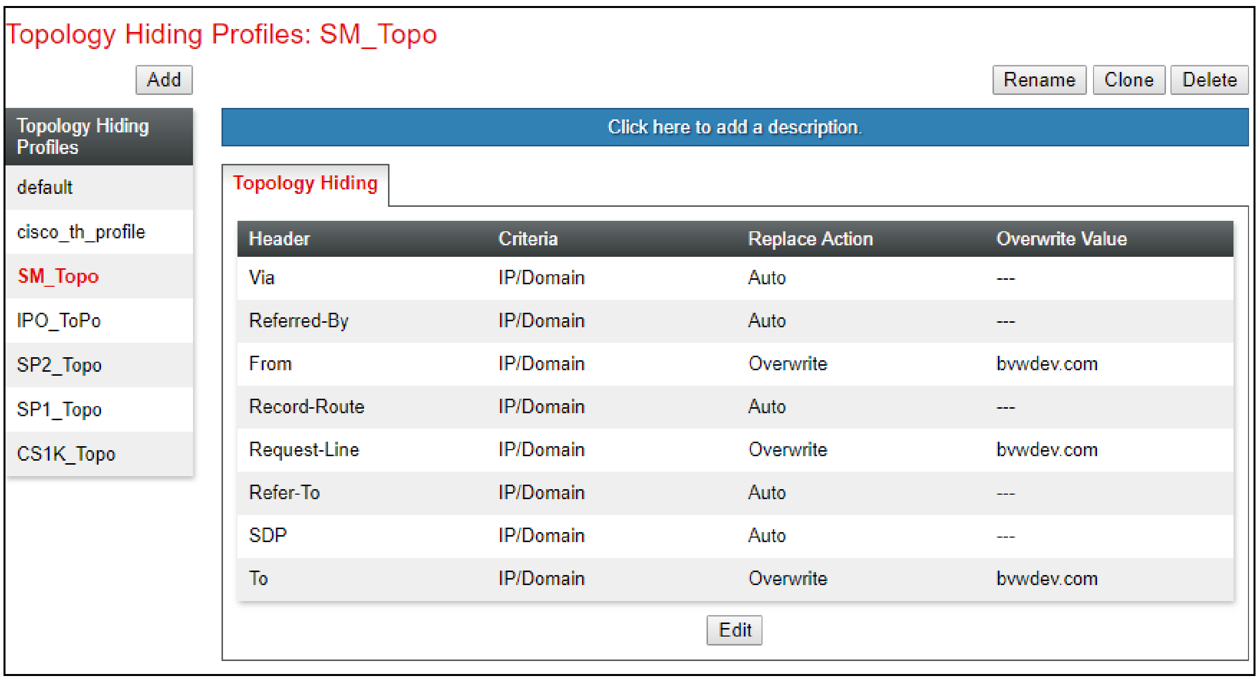
To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a pop-up window in which a header can be selected and configured. Additional headers can be added in this window. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile (e.g., **default**), select the profile from the center pane. The settings will appear in the right pane.



7.13.1. Topology Hiding – Session Manager

For the compliance test, topology hiding profile **SM_Topo** was created for Session Manager. This profile will be applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**bvwdev.com**).

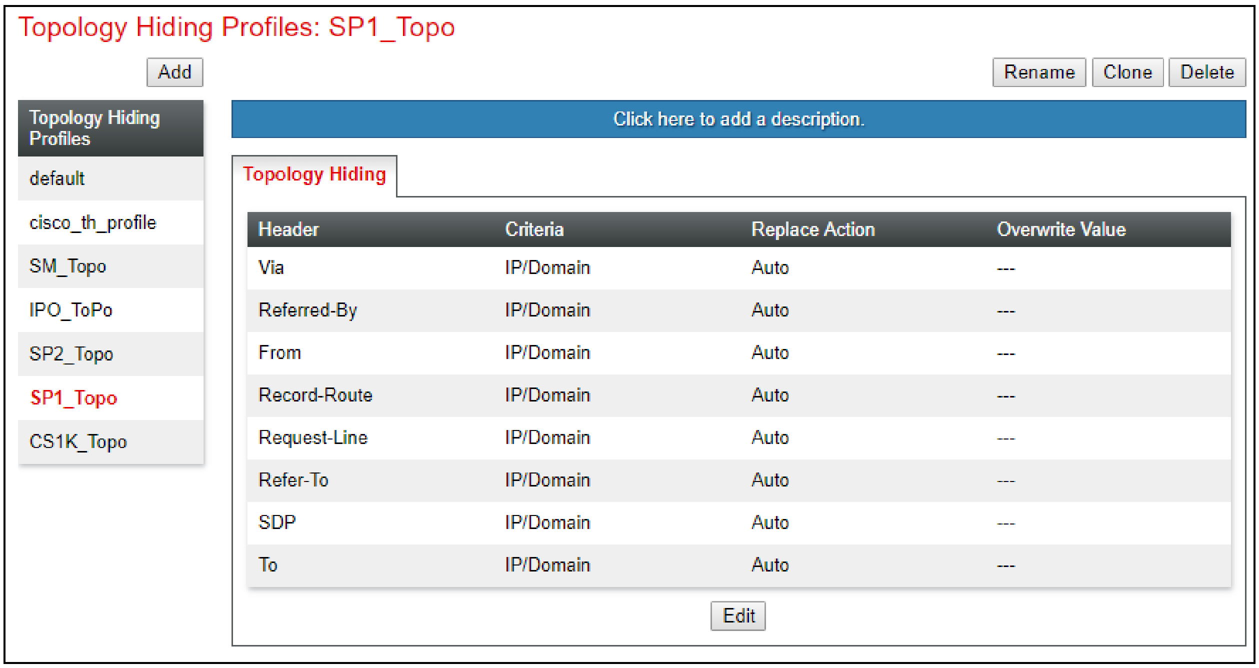


Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Overwrite	bvwdev.com
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	bvwdev.com
Refer-To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	bvwdev.com

7.13.2. Topology Hiding – TELUS

For the compliance test, topology hiding profile **SP1_Topo** was created for TELUS. This profile will be applied to traffic from the Avaya SBCE to TELUS. When creating the profile, configure the parameters as follows:

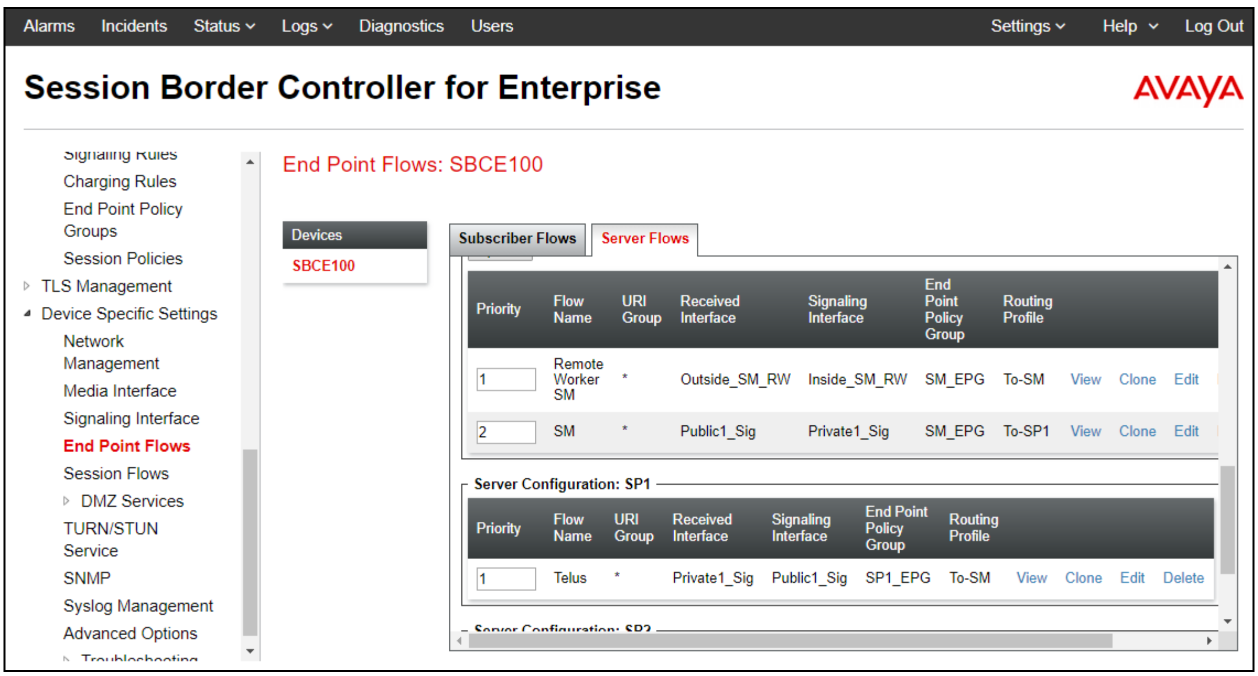
- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers.



7.14. End Point Flows

Endpoint flows are used to determine the endpoints (connected servers) involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the endpoints are Session Manager and the service provider SIP server.

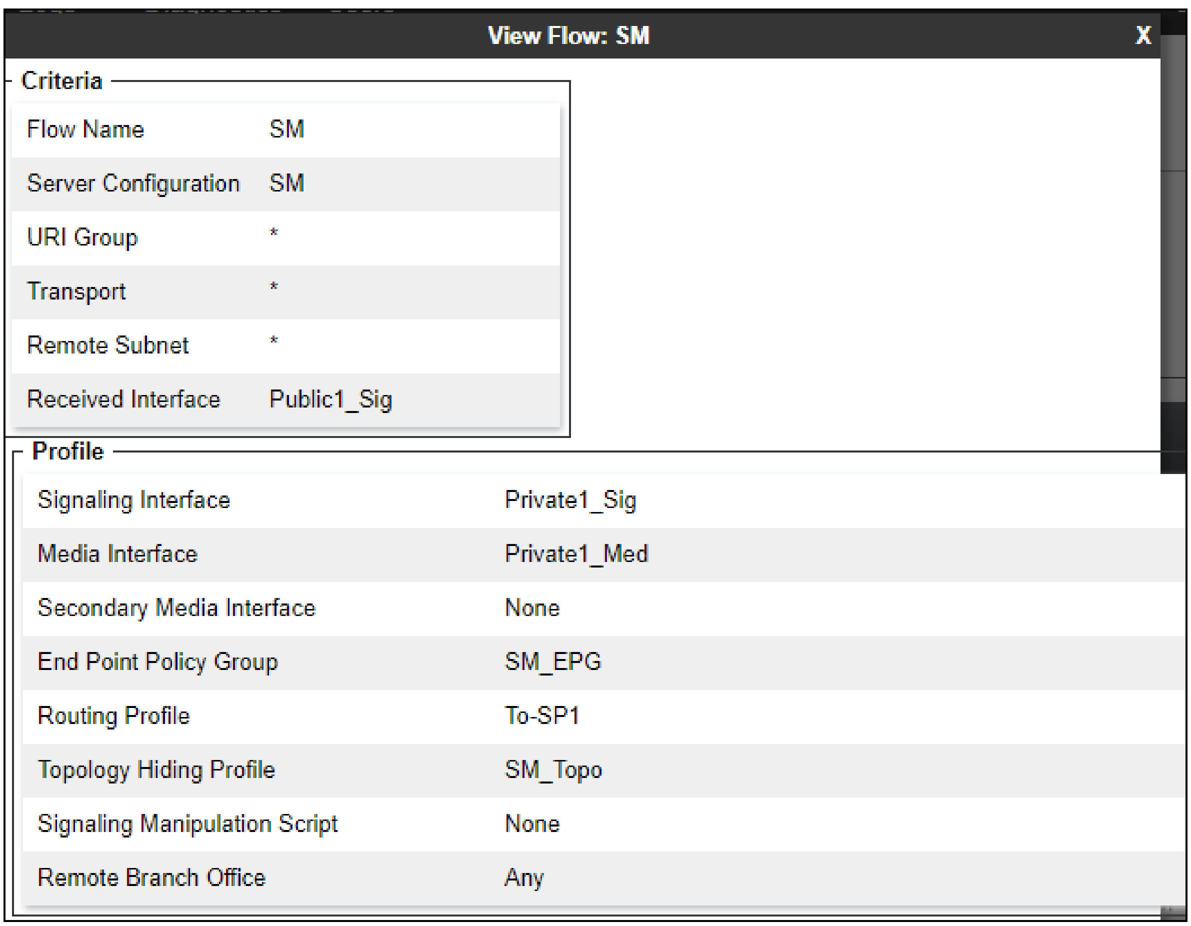
To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.



7.14.1. End Point Flow – Session Manager

For the compliance test, endpoint flow **SM** was created for Session Manager. All traffic from Session Manager will match this flow as the source flow and use the specified **Routing Profile To-SP1** to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.7.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *.
- Set the **Received Interface** to the external signaling interface (**Section 7.3**).
- Set the **Signaling Interface** to the internal signaling interface (**Section 7.3**).
- Set the **Media Interface** to the internal media interface (**Section 7.4**).
- Set the **End Point Policy Group** to the endpoint policy group defined for Session Manager in **Section 7.11.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.12.2** used to direct traffic to the TELUS SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.13.1**.



7.14.2. End Point Flow – TELUS

For the compliance test, endpoint flow **Telus** was created for the TELUS SIP server. All traffic from TELUS will match this flow as the source flow and use the specified **Routing Profile To-SM** to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the TELUS SIP server created in **Section 7.7.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set the **Received Interface** to the internal signaling interface (**Section 7.3**).
- Set the **Signaling Interface** to the external signaling interface (**Section 7.3**).
- Set the **Media Interface** to the external media interface (**Section 7.4**).
- Set the **End Point Policy Group** to the endpoint policy group defined for TELUS in **Section 7.11.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.12.1** used to direct traffic to Session Manager.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for TELUS in **Section 7.13.2**.

View Flow: Telus

Criteria

Flow Name	Telus
Server Configuration	SP1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private1_Sig

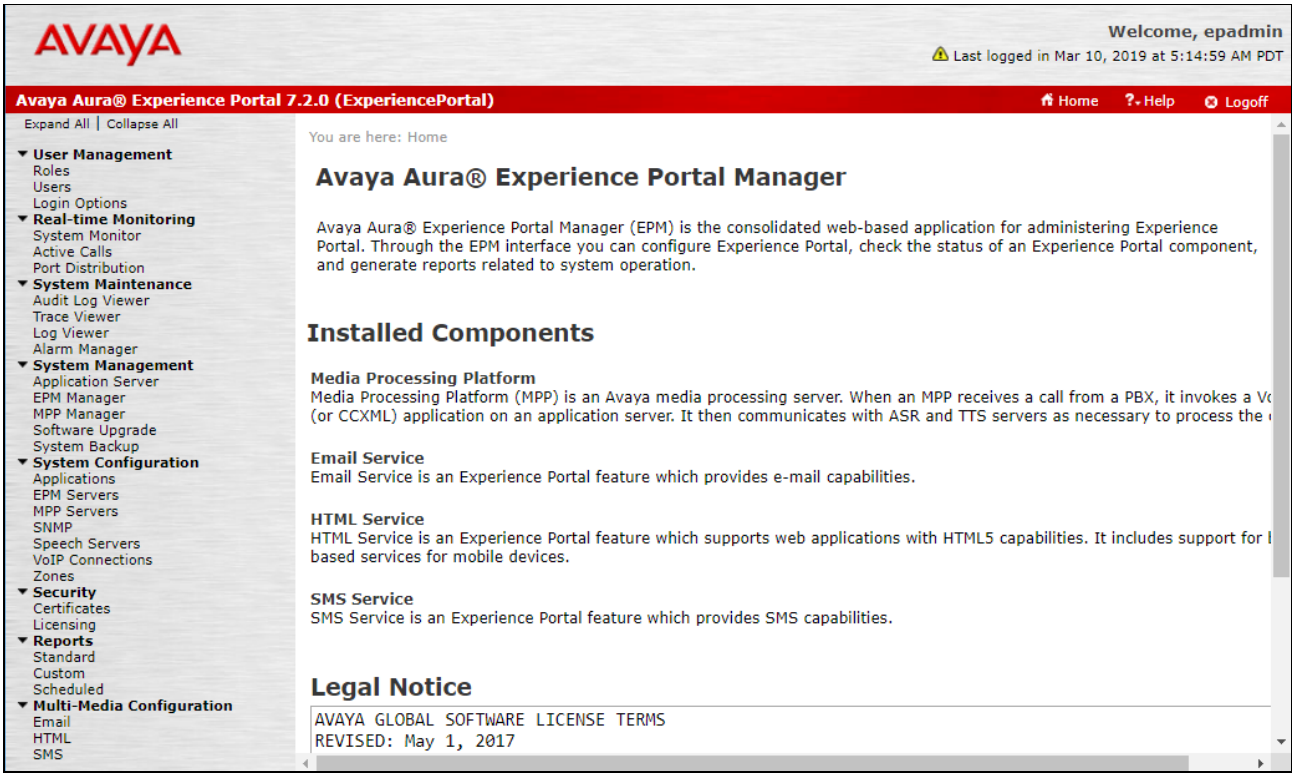
Profile

Signaling Interface	Public1_Sig
Media Interface	Public1_Med
Secondary Media Interface	None
End Point Policy Group	SP1_EPG
Routing Profile	To-SM
Topology Hiding Profile	SP1_Topo
Signaling Manipulation Script	None
Remote Branch Office	Any

8. Configure Avaya Aura® Experience Portal

Avaya Aura® Experience Portal is configured via the Experience Portal Manager (EPM) web interface, to access the web interface, enter **http://<*ip-addr*>/** as the URL in a web browser, where <*ip-addr*> is the IP address of the EPM. Log in using the appropriate credentials.

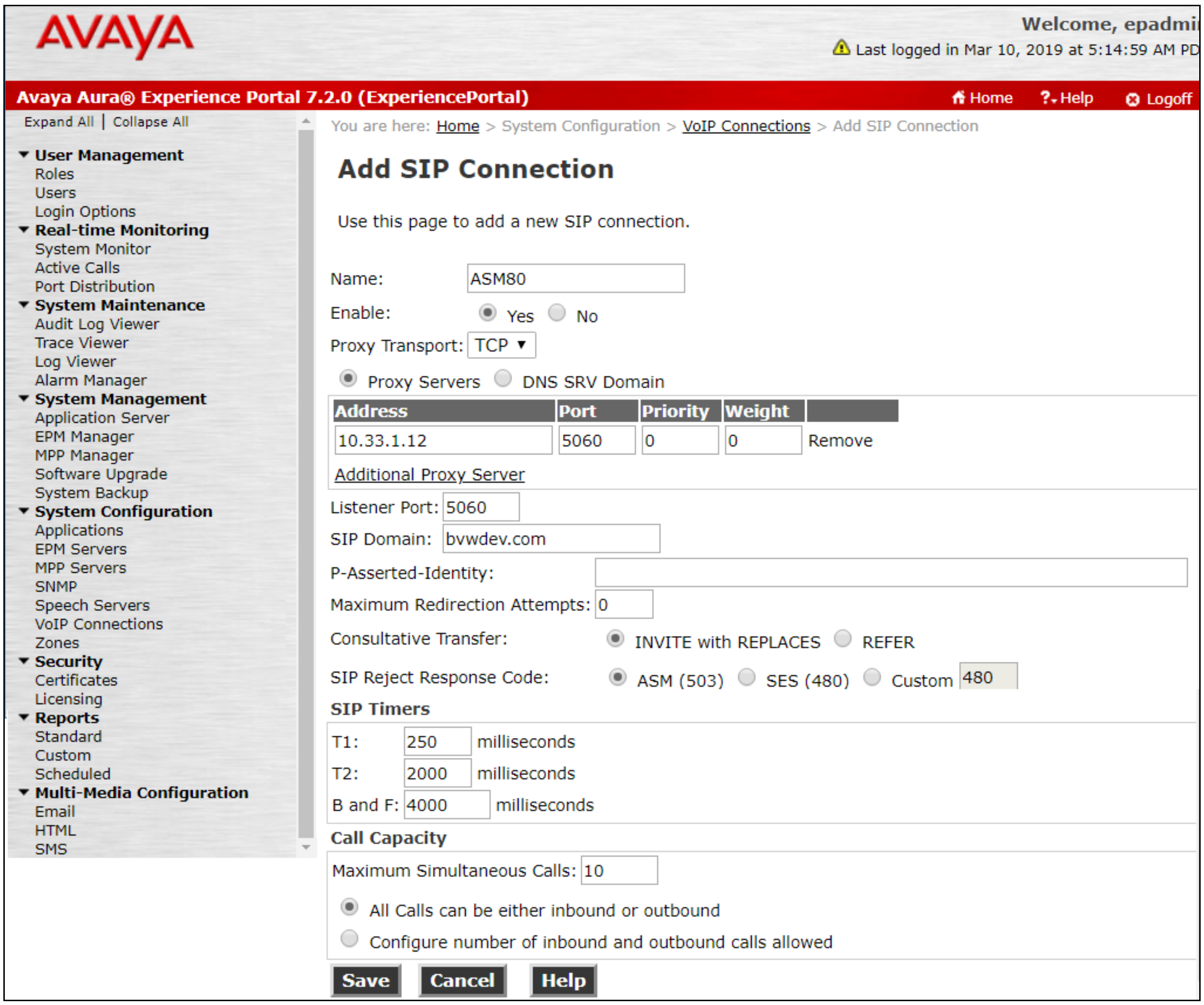
Note: Some of the screens in this section are shown after the Experience Portal had been configured. Don't forget to save the screen parameters as you configure Avaya Aura® Experience Portal.



8.1. Administer VoIP Connection

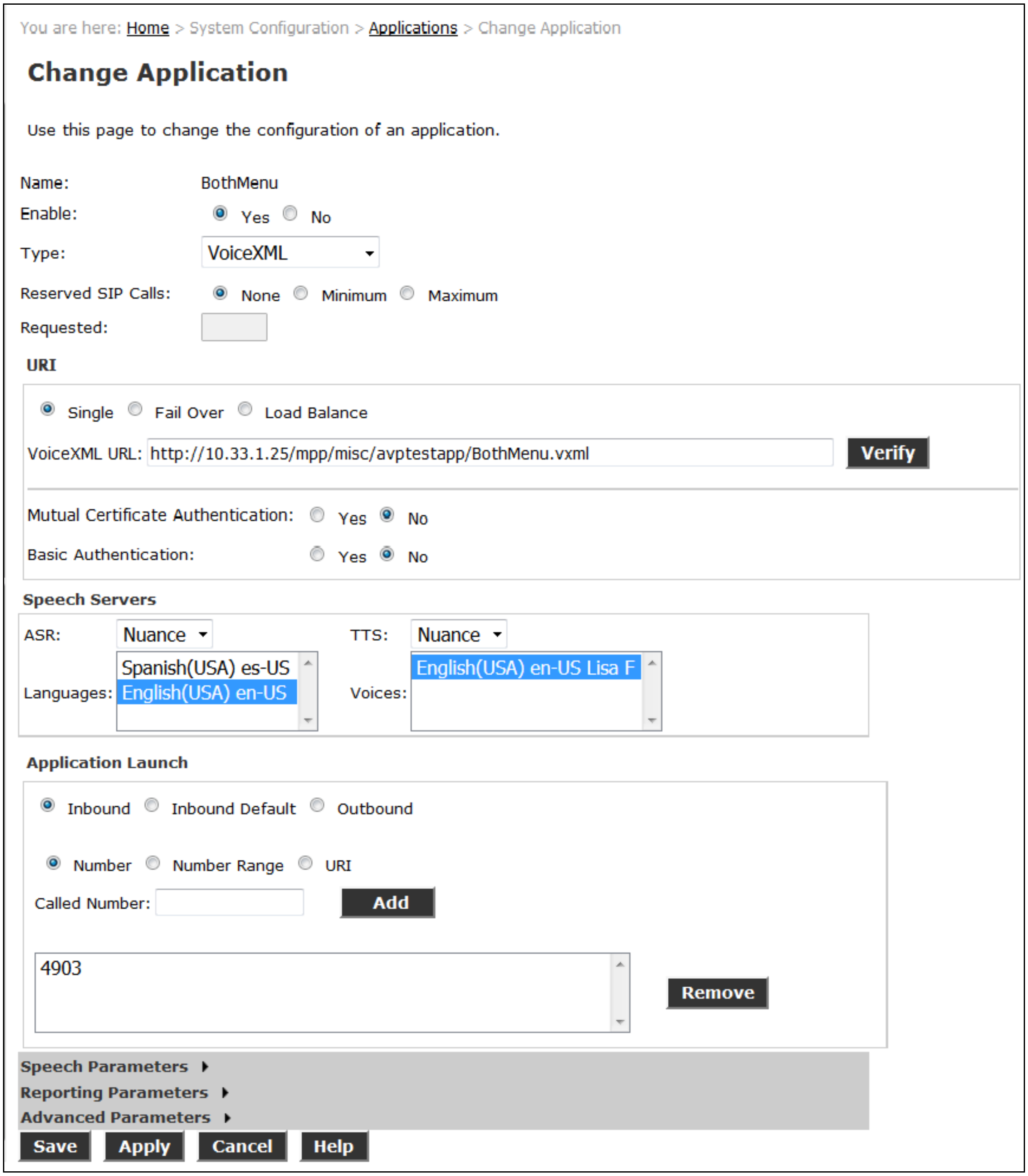
On the left pane, click on the VoIP Connections under System Configuration (not shown). To add a **SIP Connection**, click on **SIP** tab on **VoIP Connections** page (not shown).

- Fill in **Name**, in the **Address** and **Port** boxes.
- Select "**TCP**" in the **Proxy Transport** dropdown menu.
- Fill the SM signaling IP address and Port of the SIP Proxy used for call transport, in this case Session Manager was used.
- **SIP Domain,** fill in the domain and.
- Set the **Maximum Simultaneous Calls**. All other values can be left as **Default**. Click **Save** to save changes.



8.2. Administer Applications

Applications are needed to drive calls in Experience Portal. To add a new application, from the left pane, navigate to **System Configurations → Applications** and in the Application page click Add button (not shown). Below are sample of application used during the compliance test.



9. TELUS SIP Trunking Service Configuration

TELUS is responsible for the network configuration and deployment of the TELUS SIP Trunking Service.

TELUS will require that the customer provide the IP address and port number used to reach the Avaya SBCE at the edge of the enterprise. TELUS will provide the IP address and port number of the TELUS SIP proxy/SBC, IP addresses/ports of media sources, and DID numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager and Avaya SBCE configuration discussed in the previous sections.

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 a 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:
    - **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** <trunk access code number> - Displays real-time trunk group information.
    - **status trunk** <trunk access code number/channel number> - Displays real-time signaling and media information for an active trunk channel.

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.

3. Avaya Session Border Controller for Enterprise:
   There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

   - **Alarms**: This option provides information about active alarms.
   - **Incidents**: This option provides detailed reports of anomalies, errors, policies violations, etc.
   - **Status**: This option provides statistical and current status information.
   - **Diagnostics**: This option provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Experience Portal and the Avaya Session Border Controller for Enterprise to the TELUS SIP Trunking Service. The TELUS SIP Trunking Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Please refer to **Section 2.2** for exceptions or workarounds.

12. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 8.0, Feb 2019.

[2] *Upgrading and Migrating Avaya Aura® applications to Release 8.0 from System Manager*, Dec 2018.

[3] *Deploying Avaya Aura® applications from System Manager*, Release 8.0, Dec 2018

[4] *Deploying Avaya Aura® Communication Manager*, Release 8.0, Feb 2019

[5] *Administering Avaya Aura® Communication Manager*, Release 8.0, Dec 2018

[6] *Upgrading Avaya Aura® Communication Manager*, Release 8.0, Dec 2018

[7] *Deploying Avaya Aura® System Manager Release 8.0*, Feb 2019

[8] *Upgrading Avaya Aura® System Manager to Release 8.0*, Jan 2019.

[9] *Administering Avaya Aura® System Manager for Release 8.0*, Dec 2018

[10] *Deploying Avaya Aura® Session Manager*, Release 8.0 Dec 2018

[11] *Upgrading Avaya Aura® Session Manager* Release 8.0, Dec 2018

[12] *Administering Avaya Aura® Session Manager* Release 8.0, Dec 2018

[13] *Deploying Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018

[14] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018

[15] *Administering Avaya Session Border Controller for Enterprise Release 7.2.2*, Jun 2018

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

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.