Avaya Solution & Interoperability Test Lab

Application Notes for Telecom Liechtenstein SIP Trunking Service with Avaya Aura® Communication Manager Release 7.0, Avaya Aura® Session Manager Release 7.0 and Avaya Session Border Controller for Enterprise Release 7.1 – Issue 1.0

Abstract

These Application Notes describe the steps to configure a Session Initiation Protocol (SIP) trunk between Telecom Liechtenstein SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise 7.1, Avaya Aura® Media Server 7.7, Avaya Aura® Messaging 6.3 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for Enterprise.

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.

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

Table of Contents

1. Introduction

These Application Notes describe the steps to configure a SIP trunk between Telecom Liechtenstein (Liechtenstein) SIP Trunking Service and an Avaya SIP-enabled enterprise solution. Avaya Aura® release 7.0 is being deployed in virtualized environment that includes Avaya Aura® Communication Manager 7.0 (Communication Manager), Avaya Aura® Session Manager 7.0 (Session Manager), Avaya Aura® Media Server 7.7, Avaya Aura® Messaging and Avaya Session Border Controller for Enterprise 7.1 (Avaya SBCE). Various Avaya endpoints are also used in the test configuration.

For privacy and security, TLS for Signaling and SRTP for media encryption were used inside of the enterprise (private network side). Outside of the enterprise (public network side) to Liechtenstein was using UDP and RTP.

Customers using this Avaya SIP-enabled enterprise solution with Liechtenstein are able to place and receive PSTN calls via a broadband Internet connection. This converged network solution is an alternative to a traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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

Liechtenstein is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to Liechtenstein via the Internet and exercise the features and functionalities listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify Liechtenstein interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including H.323, SIP, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, SIP, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone.
- Dialing plans including local, long distance, international, outbound toll-free calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711A and G.729.

- Media and Early Media transmissions.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward.
- EC500 mobility (extension to cellular).
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat, Authentication and Registration.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.
- Remote Worker, which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Items, that are not supported, include the following:

- Fax T.38 is not supported by Liechtenstein.

2.2. Test Results

Interoperability testing of Liechtenstein with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations and limitations described below:

- **One Way Audio on Basic Outbound Calls** – Outbound call to service provider, the Avaya SBCE did not forward the 200OK responding to the Communication Manager re-INVITE, for direct media (shuffling), to Session Manager and Communication Manager. This resulted in one way audio path. The issue is resolved by applying a patch, sbce-7.1.0.1-07-12090-patch-trunkauth, to Avaya SBCE release 7.1 SP1.
- **Fax Support** – T.38 fax is not supported on the Liechtenstein SIP trunking service. G.711 fax pass-through was successfully tested during the compliance test. Due to the unpredictability of pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered in Communication Manager on a “best effort” basis; its success is not guaranteed, and it should be used at the customer’s discretion.

2.3. Support

For technical support on Liechtenstein SIP Trunking, contact Telecom Liechtenstein at http://www.telecom.li/de

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the Liechtenstein (Vendor Validation circuit) through a public Internet connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

The Avaya components used to create the simulated customer site included:

- Avaya Aura® Communication Manager running in Virtualized environment.
- Avaya Aura® System Manager running in Virtualized environment.
- Avaya Aura® Session Manager running in Virtualized environment.
- Avaya Aura® Messaging running in Virtualized environment.
- Avaya Aura® Media Server running in Virtualized environment.
- Avaya G450 Media Gateway.
- Avaya Session Border Controller for Enterprise.
- Avaya 9600Series IP Deskphones (H.323, SIP).
- Avaya one-X® Communicator soft phones (H.323, SIP).
- Avaya digital and analog telephones.
- Avaya Communicator for Windows.

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to Liechtenstein via Internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Liechtenstein across the public network is UDP. The transport protocol between the Avaya SBCE, Session Manager and Communication Manager is TLS.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain "avayalab.com" for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to Liechtenstein. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

Additionally, a remote worker is included in the reference configuration **Figure 1**. A remote worker is a SIP endpoint that resides in the un-trusted network, registered to Session Manager via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test, using the Avaya Communicator for Windows using TLS/SRTP The configuration tasks required to support remote workers are referenced in **Section 11**.

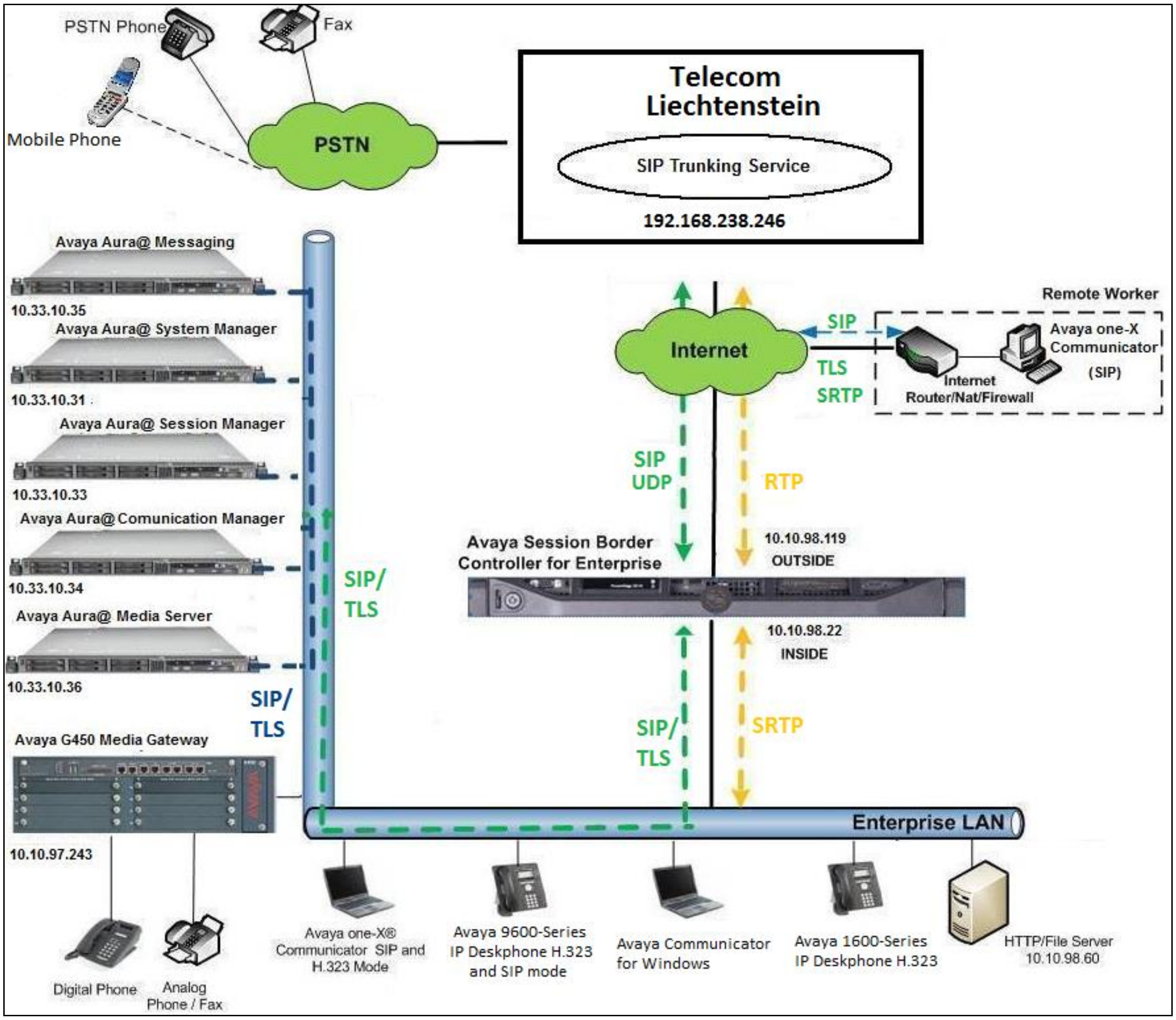


Figure 1: Avaya IP Telephony Network connecting to Liechtenstein Networks

This testing uses Convoip Trunk FL (in Europe). For outbound call from Avaya System to PSTN, user dials 9 follow 00 and 11 digits including a 1 (Canada/US country code) since the testing is performed in North America (Canada). The test was used 00 plus the 11 digits number (i.e. 9 001 613 967 5204). For inbound call to Avaya system from PSTN, user needs to dial international call beginning with 011 plus 10 digits number (011 423 237 2780).

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on Virtualized Environment	7.0.1.1 (FP1SP1, 00.0.441.0-23169)
Avaya G450 Media Gateway	37.39.0
Avaya Aura® System Manager running on Virtualized Environment	7.0.1.1 (Build No. - 7.0.0.0.16266)
Avaya Aura® Session Manager running on Virtualized Environment	7.0.1.1 (7.0.1.1.701114)
Avaya Aura® Messaging running on Virtualized Environment	6.3.124.335-1.253373
Avaya Aura® Media Server running on Virtualized Environment	7.7.0.334
Avaya Session Border Controller for Enterprise	7.1.0.1-07-12090
Avaya 9621G IP Deskphone (H.323)	6.6.302
Avaya 9641G IP Deskphone (SIP)	7.0.1.29
Avaya one-X® Communicator (H.323/SIP)	6.2.12.04-SP12
Avaya Communicator for Windows	2.1.3.8
Avaya 1608 IP Deskphone (H.323)	1.380B
Avaya 1408 Digital Telephone	1408D02A-003
Avaya Analog Telephone	n/a
Liechtenstein SIP Trunking Service Components	
Component	Release
Oracle SBC net net 3820	6.40
Teles C5 Proxy	5.0.8.48-2

Table 1: Equipment and Software Tested

Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Liechtenstein SIP Trunking service. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Media Server has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. 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 sale representative to add the additional capacity or feature.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  1
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  3
                       Maximum Administered SIP Trunks: 4000  74
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0


        (NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 4**, verify that **ARS** is set to **y**.

```
display system-parameters customer-options                      Page   4 of  12
                                OPTIONAL FEATURES

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


        (NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 5**, verify that **IP Trunks** field is set to **y** and **Media Encryption Over IP** field is set to **y**.
(Note: The Media Encryption option is only available if Media Encryption Over IP is enabled on the installed license)

```
display system-parameters customer-options                      Page   5 of  12
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                       ISDN Feature Plus? n
                  Enhanced EC500? y       ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                         ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                ISDN-PRI? y
              ESS Administration? y              Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                    Malicious Call Trace? y
     External Device Alarm Admin? y                Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y              Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

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

```
display system-parameters customer-options                      Page   6 of  12
                                OPTIONAL FEATURES

                Multinational Locations? n             Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n      Station as Virtual Extension? y
                     Multiple Locations? n
                                             System Management Data Transfer? n
          Personal Station Access (PSA)? y              Tenant Partitioning? y
                        PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                   Port Network Support? n              Time of Day Routing? y
                        Posted Messages? y      TN2501 VAL Maximum Capacity? y
                                                       Uniform Dialing Plan? y
                     Private Networking? y    Usage Allocation Enhancements? y
               Processor and System MSP? y
                     Processor Ethernet? y                Wideband Switching? y
                                                                    Wireless? n
                          Remote Office? y
          Restrict Call Forward Off Net? y
                  Secondary Data Module? y


        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow an incoming call 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. The compliance test used the value of ***Restricted*** for restricted calls and ***Unavailable*** for unavailable calls.

```
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: 001

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 Communication Manager **(procr**), Session Manager (**SM**) and Media Server (**AMS**). These node names will be needed for defining the signaling groups in **Section 5.6**.

```
change node-names ip                                           Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
SM                  10.33.10.33
AMS                 10.33.10.36
default             0.0.0.0
procr               10.33.10.34
procr6              ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 1. Liechtenstein supports G.711MU and G729. To use these codecs, enter ***G.711A***, ***G.711MU*** and ***G.729*** in the **Audio Codec.** For media encryption used within Avaya system, the ***1-srtp-aescm128-hmac80***, ***2-srtp-aescm128-hmac32 and none*** are used in **Media Encryption** and ***best-effort*** in **Encrypted SRTCP** columns of the table in the order of preference.

The following screen shows the configuration for ip-codec-set 1. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

```
change ip-codec-set 1                                          Page   1 of   2
                          IP CODEC SET
    Codec Set: 1

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

     Media Encryption                   Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
```

On **Page 2**, set the **Fax Mode** to ***pass-through*** faxing which is supported by Liechtenstein (refer to **Section 2.2**).

```
change ip-codec-set 1                                          Page   2 of   2
                          IP CODEC SET

                              Allow Direct-IP Multimedia? n
                                                                        Packet
                          Mode                   Redundancy             Size(ms)
    FAX                   pass-through            1
    Modem                 off                     0
    TDD/TTY               US                      3
    H.323 Clear-channel   n                       0
    SIP 64K Data          n                       0                     20
```

5.5. IP Network Region

For the compliance testing, ip-network-region 1 was created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is ***avayalab.com***. This domain name appears in the "From" header of SIP message 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 Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to ***yes***. Shuffling can be further restricted at the trunk level under 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 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: ToSM
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
...
```

On **Page 4**, define the IP codec set to be used for traffic between region 1 and other regions. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, IP/SIP phones and Session Manager were assigned to the same region 1.

```
change ip-network-region 1                                     Page   4 of  20

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

Non-IP telephones (e.g., analog, digital) derive network region from the IP interface of the Avaya G450 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

```
change ip-interface proc                                    Page   1 of   2
                                 IP INTERFACES


                  Type: PROCR
                                                 Target socket load: 4800

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

To define network region 1 for the Avaya G450 Media Gateway, use **change media-gateway** command as shown in the following screen.

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

                    Type: g450
                    Name: g450
               Serial No: 11N526797797
    Link Encryption Type: any-ptls/tls       Enable CF? n
          Network Region: 1                   Location: 1
                                             Site Data:
           Recovery Rule: none
...
```

If Avaya Aura® Media Server is used in parallel of Avaya Media Gateway G450, then it is needed to define network region 1 for the Avaya Aura® Media Server. Use **change media-server** command as shown in the following screen.

```
change media-server 1                                     Page   1 of   1
                                 MEDIA SERVER

                    Media Server ID: 1

                    Signaling Group: 3
          Voip Channel License Limit: 30
     Dedicated Voip Channel Licenses: 30

                          Node Name: AMS
                     Network Region: 1
                           Location: 1
           Announcement Storage Area:
...
```

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 Avaya SBCE trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group ***2*** was used and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***.
- Set the **Transport Method** to ***tls*** *(Transport Layer Security)****.*** The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to ***5061***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP interface of **procr** defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***SM***. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region ***1*** defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to ***avayalab.com***.
- Set the **DTMF over IP** to ***rtp-payload***. This setting enables Communication Manager to send or receive the DTMF transmissions using RFC2833.
- Set **Enable Layer 3 Test?** to ***y***. This setting allows Communication Manager to send OPTIONS heartbeat to Session Manager on the SIP trunk.
- 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 directly between the SIP trunk and the enterprise endpoint. If this value is set to ***n***, then the Avaya G450 Media Gateway will remain in the media path between the SIP trunk and the endpoint for the duration of the call. Depending on the number of media resources available in the Avaya G450 Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Alternate Route Timer** to ***30***. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Default values may be used for all other fields.

Signaling Group 2:

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

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: avayalab.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): 30
```

Another signaling group is created between Communication Manager and the Media Server to provide media resources for IP telephony in parallel of the media gateway G450. For the compliance test, signaling group ***3*** was used for this purpose and was configured as shown in the capture below.

Signaling Group 3:

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

 Group Number: 3              Group Type: sip
                        Transport Method: tls


  Peer Detection Enabled? n  Peer Server: AMS



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

Far-end Domain: 10.33.10.36
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 0**. For the compliance testing, trunk group ***2*** 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 **Outgoing Display** to ***y*** to enable name display on the trunk.
- Set the **Service Type** field to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group **2** shown in **Section 0**.
- Set the **Number of Members** field to customer requirement. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk group.
- Default values are used for all other fields.

```
add trunk-group 2                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip          CDR Reports: y
  Group Name: SIP-Carrier                 COR: 1        TN: 1        TAC: #02
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk           Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 32
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval a re-INVITEs must be sent to refresh the Session Timer. For the compliance testing, a default value of ***600*** seconds was used.

```
add trunk-group 2                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y

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


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

On **Page 3**, set the **Numbering Format** field to ***public***. This field specifies the format of the CPN sent to the far-end. The public numbers are automatically preceded with a + sign when passed in the "From", "Contact" and "P-Asserted Identity" headers.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on the local endpoint to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values are used for all other fields.

```
add trunk-group 2                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? Y

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

Show ANSWERED BY on Display? y
```

On **Page 4**, the settings are as follow:

- Set of **Network Call Redirection** flag to ***y*** to enable the use of SIP REFER message to transfer calls back to the PSTN as service provider does support it. It can also be set to ***n*** if the use of re-INVITE for call re-direction is preferred.
- Set the **Send Diversion Header** field to ***y*** as service provider does support it.
- Set the **Support Request History** field to ***n***.
- Set the **Telephone Event Payload Type** to ***101***.

```
add trunk-group 2                                           Page   4 of  21
                              PROTOCOL VARIATIONS

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


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

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering is selected to define the format of this number (**Section 0**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the service provider. They are used to authenticate the caller.

The screen below shows a subset of the 10 digits DID numbers assigned for testing. These 4 numbers were mapped to the 4 enterprise extensions 60396, 60397, 60379 and 60398. These same 12-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

```
change public-unknown-numbering 0                                 Page   1 of   2
                           NUMBERING - PUBLIC/UNKNOWN FORMAT

Ext Ext               Trk        CPN               Total
Len Code              Grp(s)     Prefix            Len
 5  60396             2         004232372780       12       Total Administered: 6
 5  60397             2         004232372781       12          Maximum Entries: 240
 5  60379             2         004232372782       12
 5  60398             2         004232372783       12
```

5.9. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by Liechtenstein can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 2                  Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 004232372780    12  60396
 public-ntwrk    10 004232372781    12  60397
 public-ntwrk    10 004232372782    12  60379
 public-ntwrk    10 004232372783    12  60398
```

5.10. Outbound Routing

In these Application Notes, the **Automatic Route Selection** (ARS) feature is used to route an outbound call via the SIP trunk to the service provider via the Avaya SBCE. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code **(fac**) ***9***, use the **change dialplan analysis** command as shown below.

```
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
   1           4   ext
   30          4   ext
   39          5   udp
   60          5   ext
   9           1   fac
   *           3   dac
   #           3   dac
```

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

```
change feature-access-codes                                     Page   1 of  10
                               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:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example pattern below shows a sample of the dialed strings calling on FL (or LI) SIP – Trunk: (LI: principal of Liechtenstein, FL: Furstentum Liechtenstein). All dialed strings are mapped to route pattern ***2*** for an outbound call 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: 0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    00                    2    36     2       intl         n
    11                    3    3      2       svcl         n
    14                    3    3      2       svcl         n
    15                    3    7      2       pubu         n
    18                    3    7      2       pubu         n
    02                    10   10     2       pubu         n
    09                    10   10     2       pubu         n
    2                     7    7      2       pubu         n
    3                     7    7      2       pubu         n
    4                     7    7      2       pubu         n
    69                    9    9      2       pubu         n
    7                     7    7      2       pubu         n
    8                     7    7      2       pubu         n
    9                     7    7      2       pubu         n
```

In the table above, the definition of dialed patterns following by 9 (according to Liechtenstein) is as below.

- 00 Austria, Germany, … have an open numbering plan E.164
- 02 and 09 Swiss-Fixed, Mobile, Business, Premium and Value added Service Numbers closed numbering plan
- 11 and 14 Emergency call numbers
- 15 and 18 Short numbers and Service Numbers
- 2, 3, 4 Normal Subscriber Numbers FL closed numbering plan
- 69 Voicemail- access to a FL-Voice Mail Box
- 7 Mobile Numbers
- 8 Free-phone and business numbers
- 9 Premium Numbers

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern ***2*** in the following manner.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group ***2*** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Numbering Format**: ***pub-unk***. All calls using this route pattern will use the public numbering table as shown in **Section 5.8**.

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2   Pattern Name: SP Route
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 2    0                                                              n   user
 2:                                                                     n   user
....
     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
                                                        Subaddress
 1: y y y y y n  n            rest                              pub-unk   none
...
```

5.11. Saving Communication Manager Configuration Changes

The command "**save translation all**" can be used to save the configuration changes made on Communication Manager.

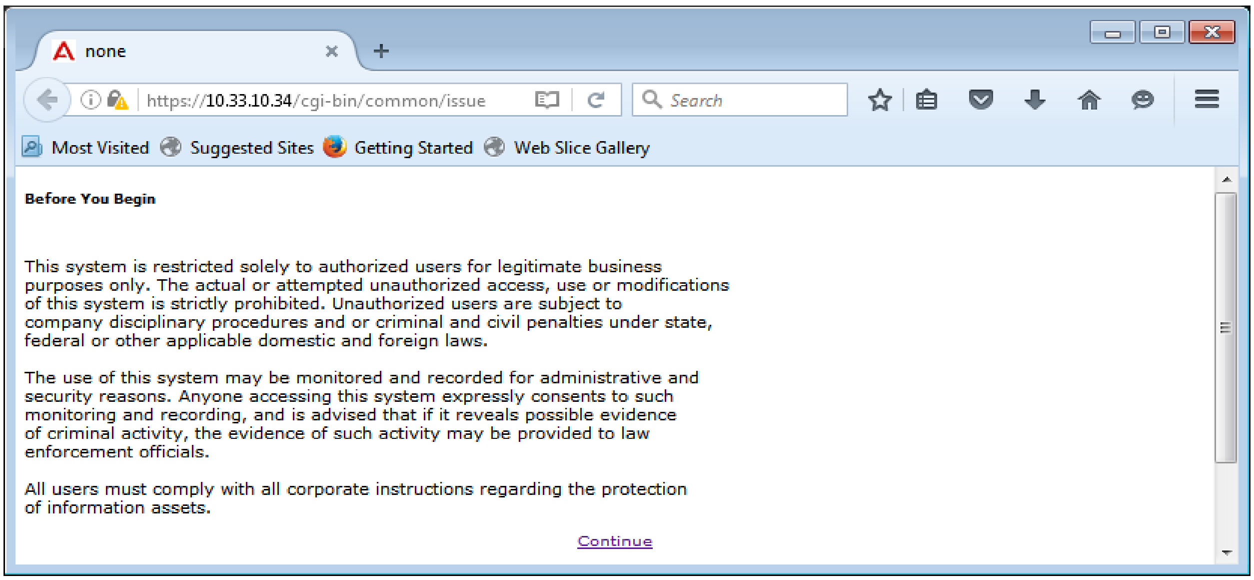
5.12. TLS Management on Communication Manager

It is (or maybe) necessary to install System Manager CA certificate on Communication Manager for the TLS signalling to work between Avaya Session Manager and Avaya Communication Manager if it is not previously installed.

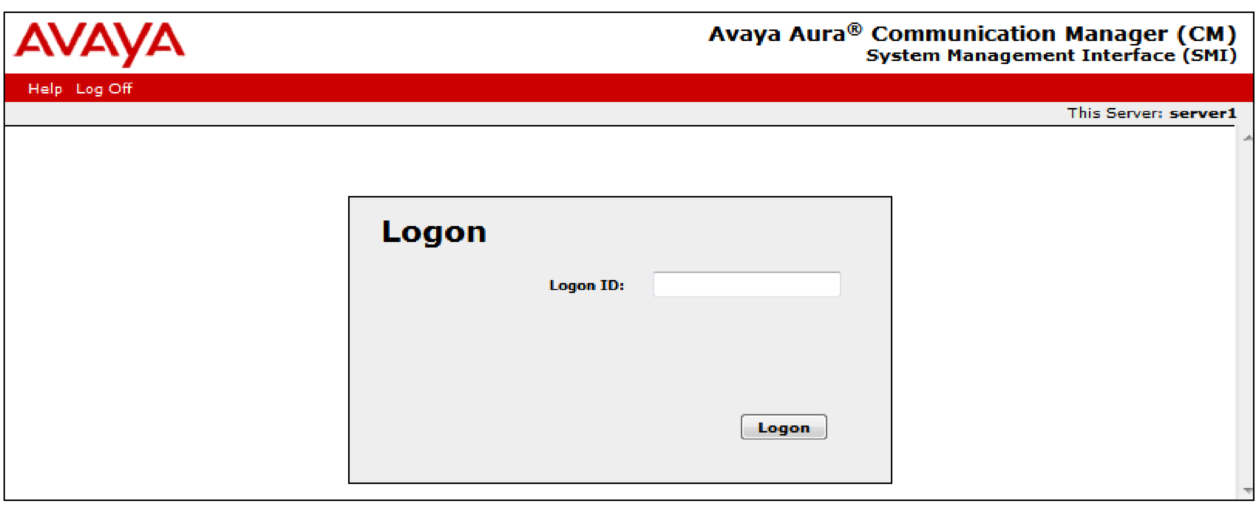
This section is to show how to install System Manager CA certificate on Communication Manager using Web console.

System Manager CA certificate is obtained using procedure provided in **Section 6.9**.

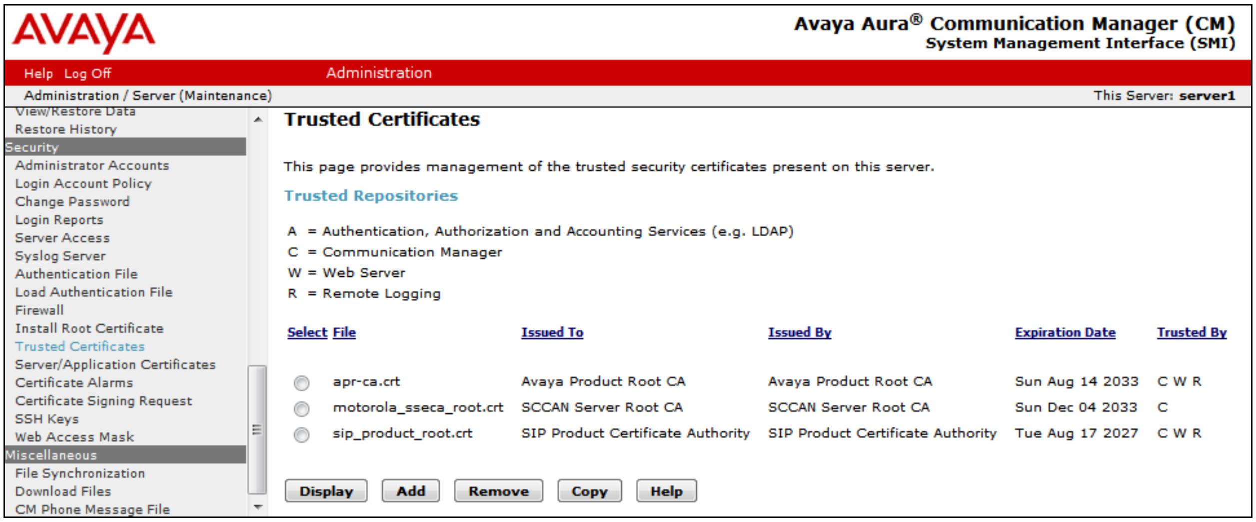
From a web browser, type in "https://<ip-address>", where "<ip-address>" is the IP address or FQDN of Communication Manager. Click on **Continue** and it will be redirect to login page.



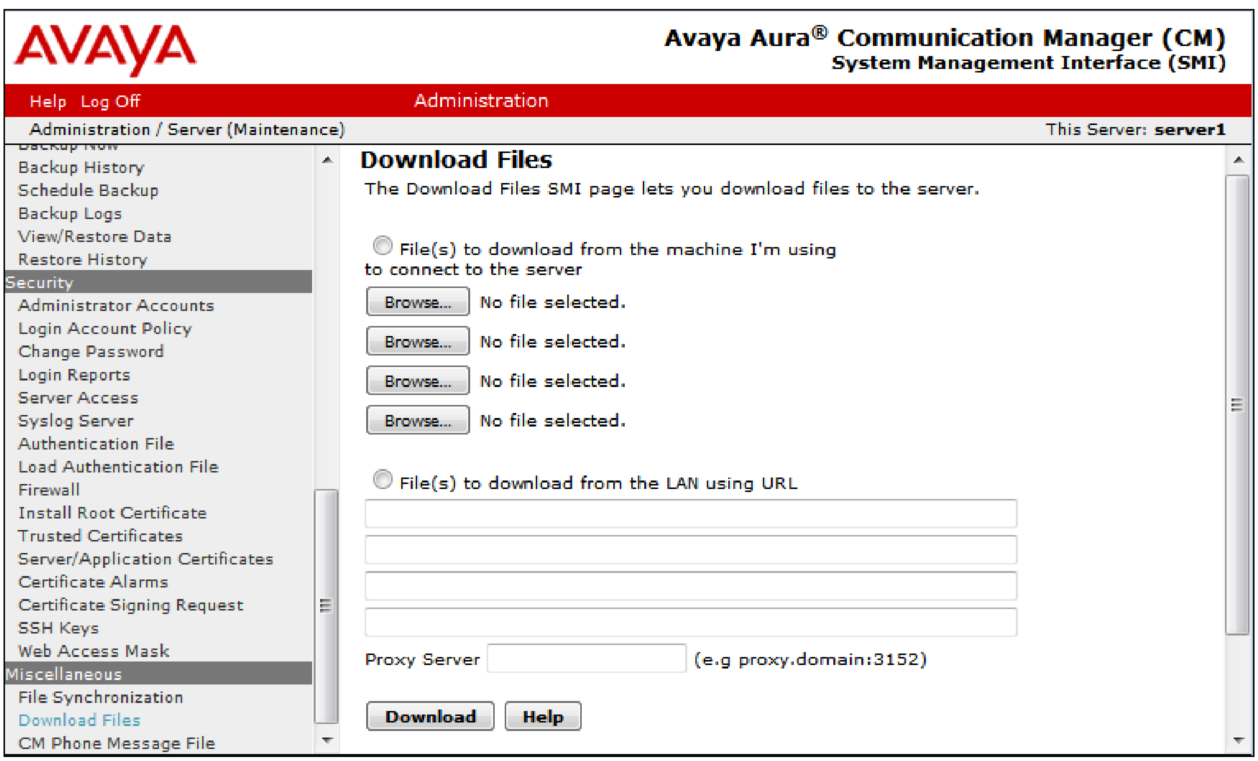
At login page, type in the login ID and its password credential.



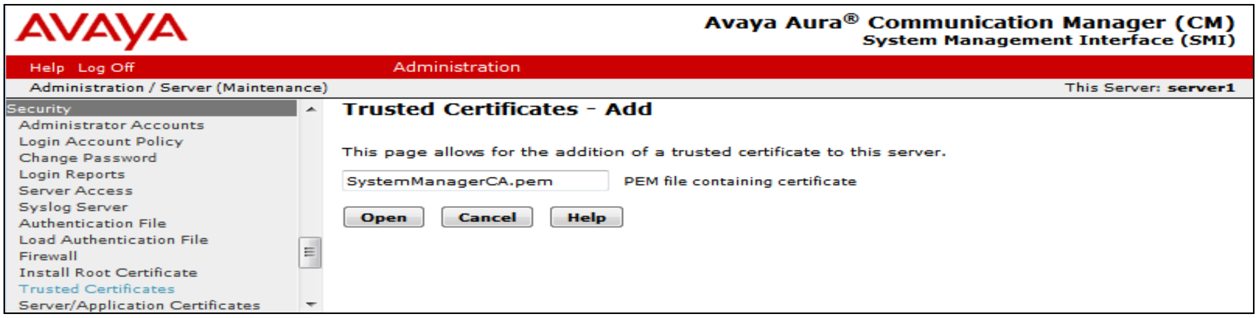
Click on **Continue** again (not shown), navigate to **Administration → Server → Trusted Certificates** to verify if the System Manager CA certificate is present or not. If it is not, then continue to the next step.



Navigate to **Miscellaneous → Download Files**, click on **File to download from the machine I'm using to connect to the server** and click on **Browse** to where the System Manager CA is being located. Then click on **Download** button to load the System Manager CA on Communication Manager Server.

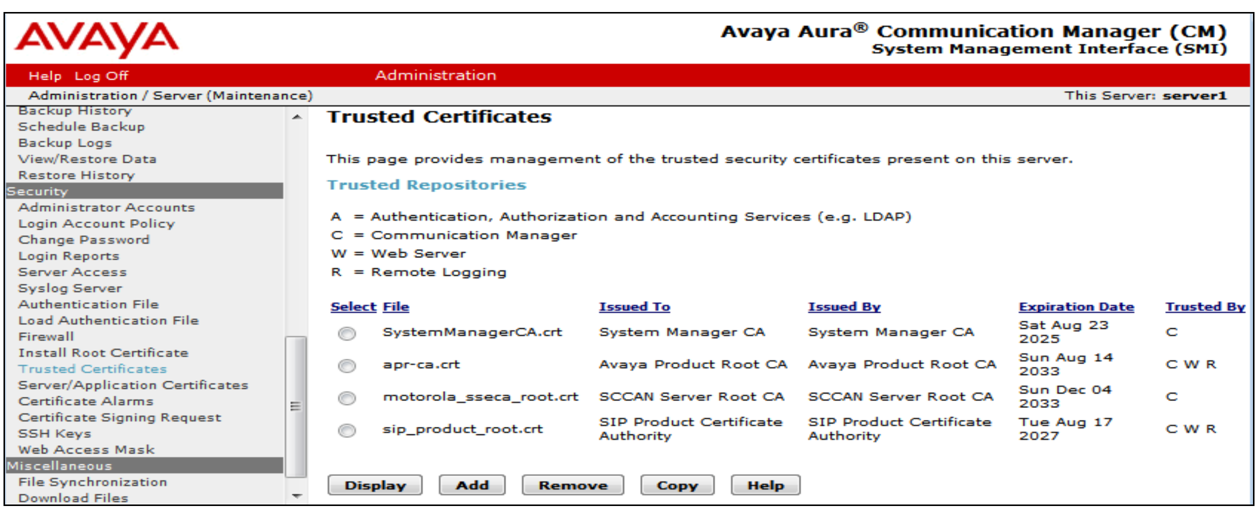


Navigate to **Security → Trusted Certificates**, click on **Add** button and enter the certificate name which has been downloaded from above step. Then click **Open**.



Enter the name of the System Manager CA certificate to store the certificate in Communication Manger. Check the Communication Manager check-box. Then click **Add**.

Navigate to **Security → Trusted Certificates** again. It now shows the System Manager CA in the **Trusted Repositories**.



6. Configure Avaya Aura® Session Manager

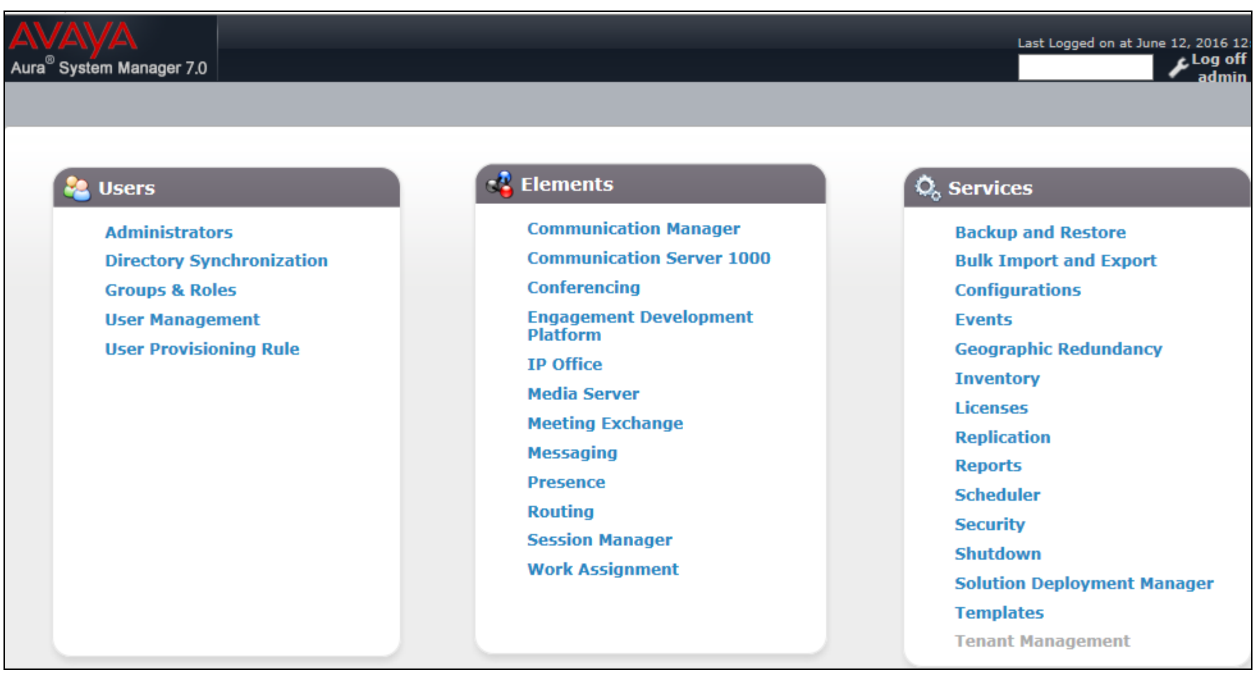
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be used by SIP Entities
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager server to be managed by System Manager

It may not be necessary to configure 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.

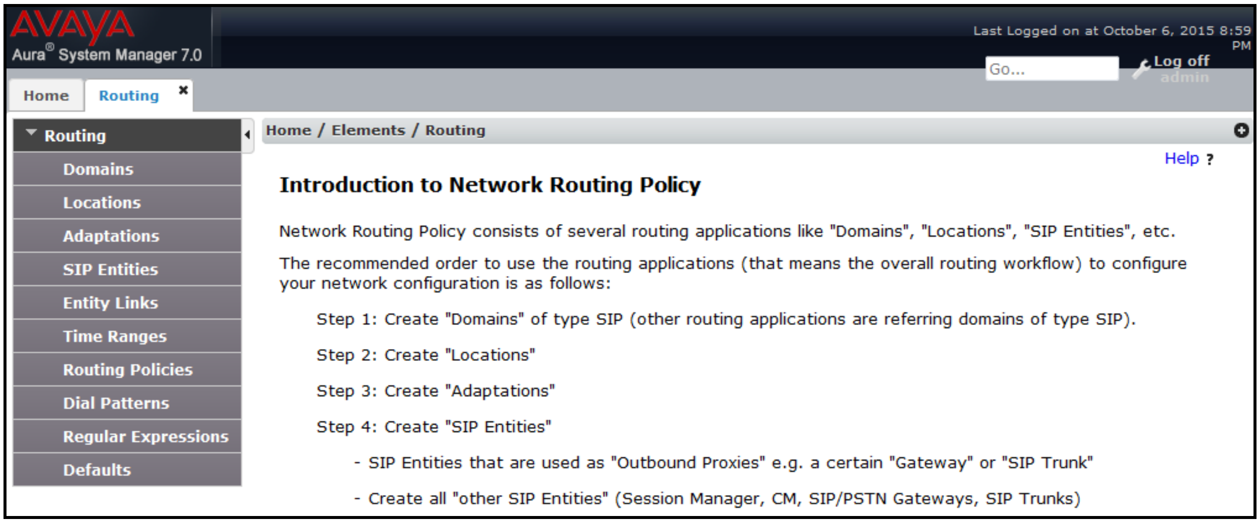
6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the Web GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address or FQDN of System Manager. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



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

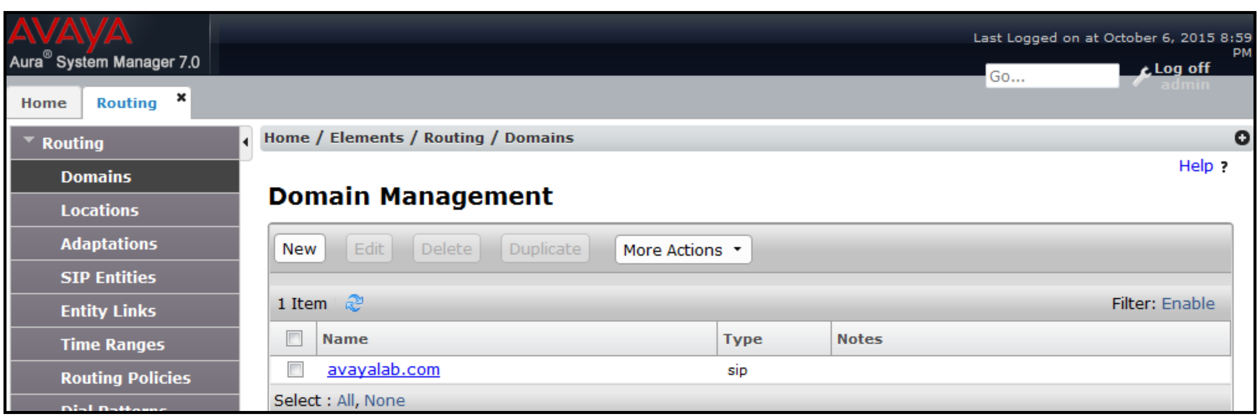
The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



6.2. Specify SIP Domain

To view or to change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain, ***avayalab.com*** was already created for communication between Session Manager and Communication Manager. The domain ***avayalab.com*** is not known to Liechtenstein. It will be adapted by the Avaya SBCE to IP address based URI-Host to meet the SIP specification of Liechtenstein system.



6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for bandwidth management and call admission control purposes. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click **New** button in the right pane (not shown).

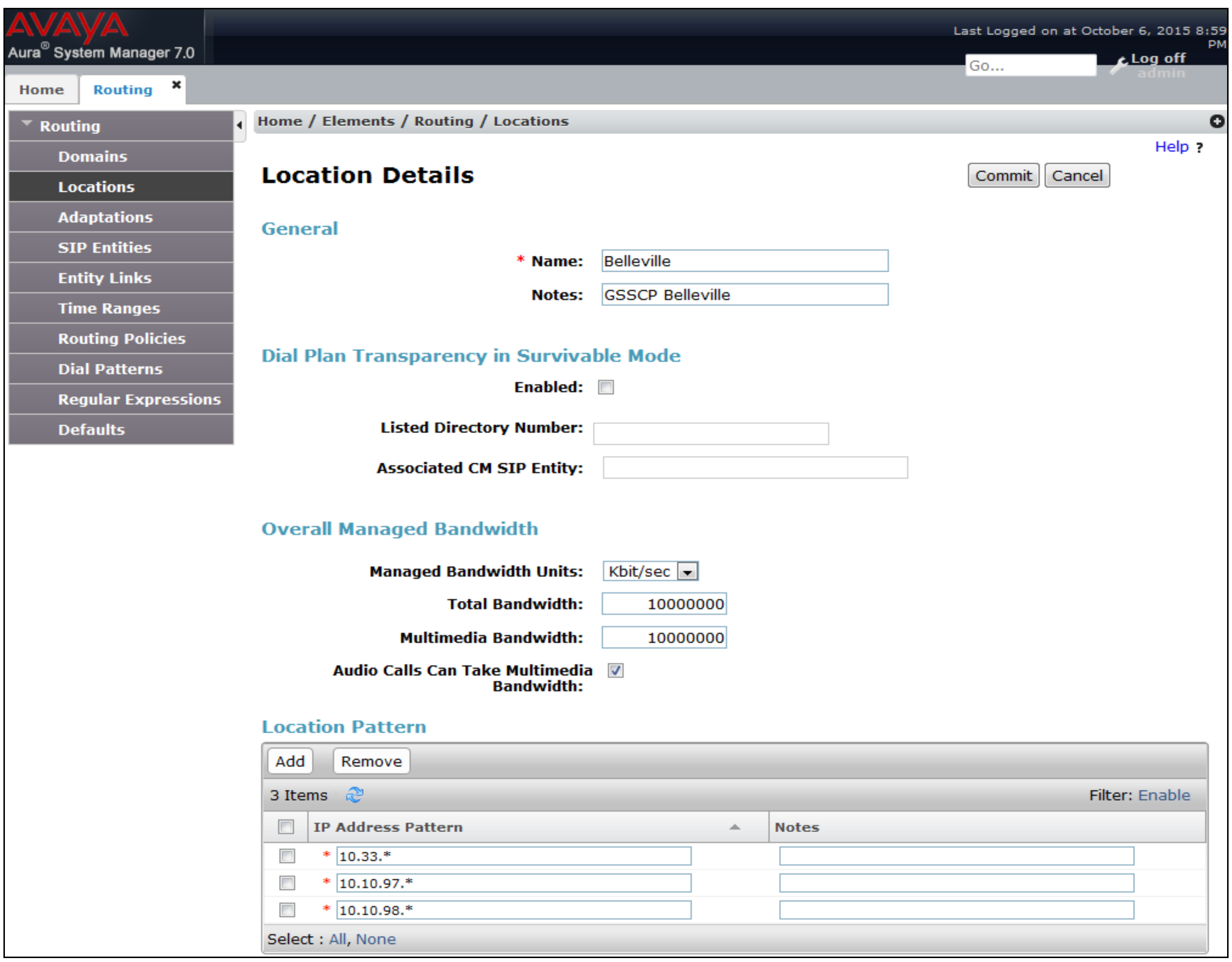
In **General** section, enter the following values:

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

In the **Location Pattern** section (see the screen below), click **Add** and configure following fields:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

Displayed below are the screenshots for location ***Belleville***, which includes all equipment on the ***10.33.*, 10.10.98.**** and ***10.10.97.**** subnet including Communication Manager, Session Manager and Avaya SBCE. Click **Commit** to save.



6.4. Add SIP Entities

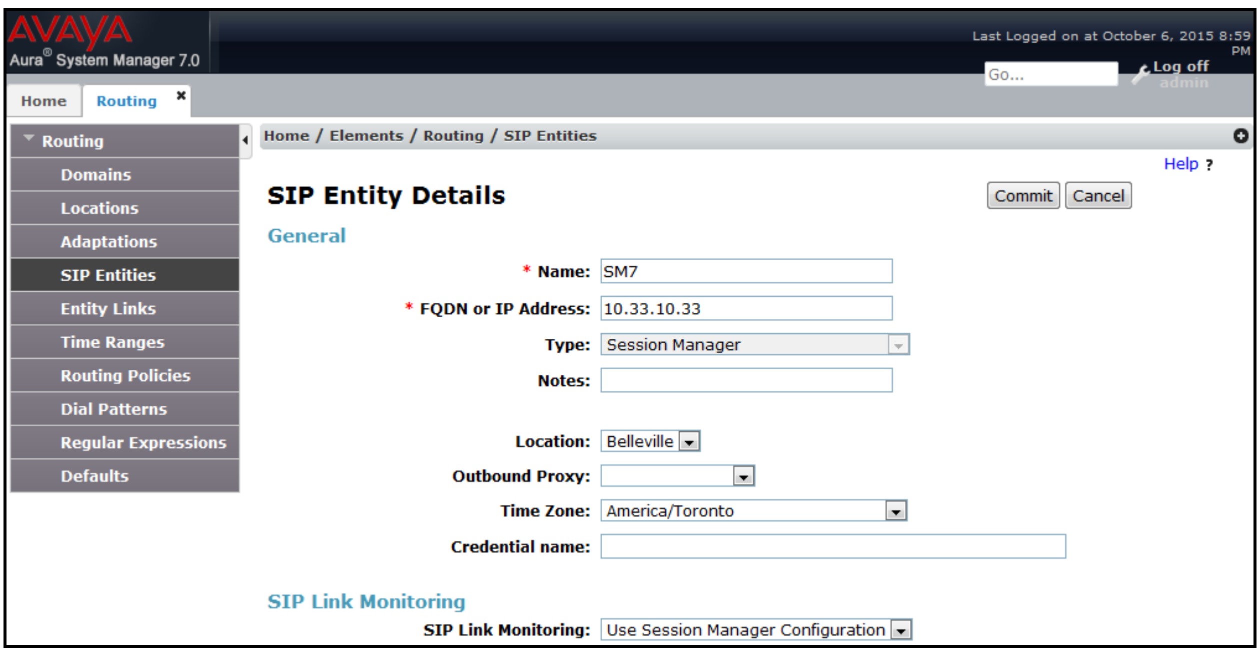
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and Avaya SBCE.

To add a new SIP Entity, navigate to **Routing → SIP Entities** in the left navigation pane and click **New** button in the right pane (not shown).

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

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** for the Avaya SBCE.
- **Location:** Select the location defined in **Section** Error! Reference source not found..
- **Time Zone**: Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface 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 the **Session Manager** SIP Entity.

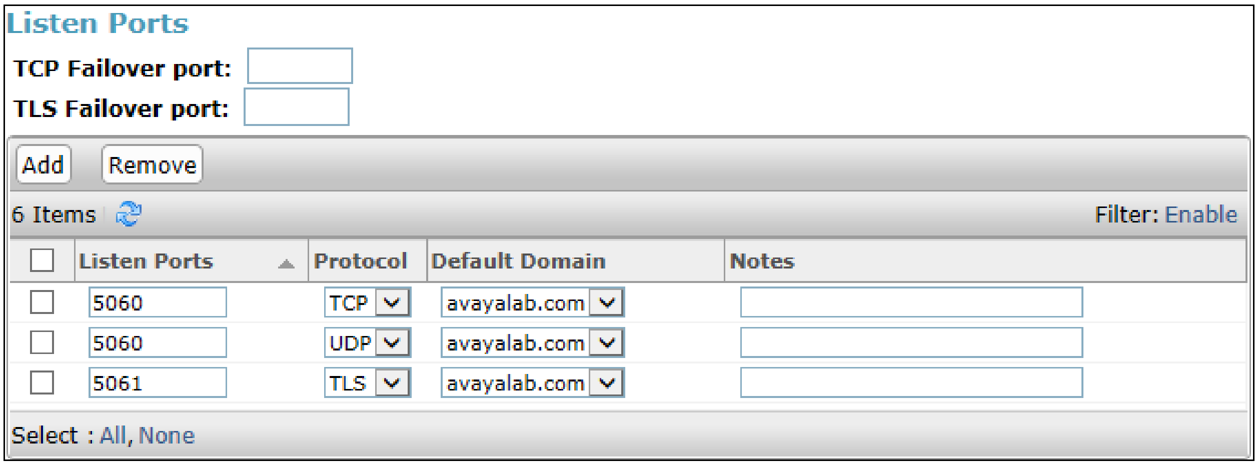
In the **Port** section, click **Add** and enter following values. Use default values for all remaining fields:

- **Listen Ports:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to receive SIP requests.

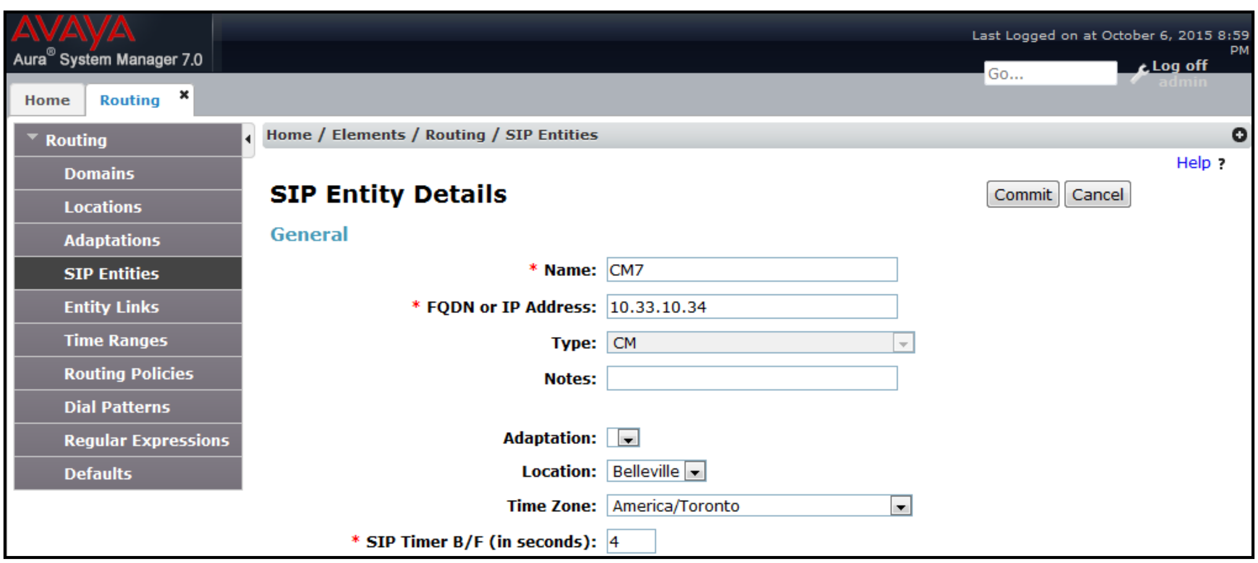
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save (not shown).

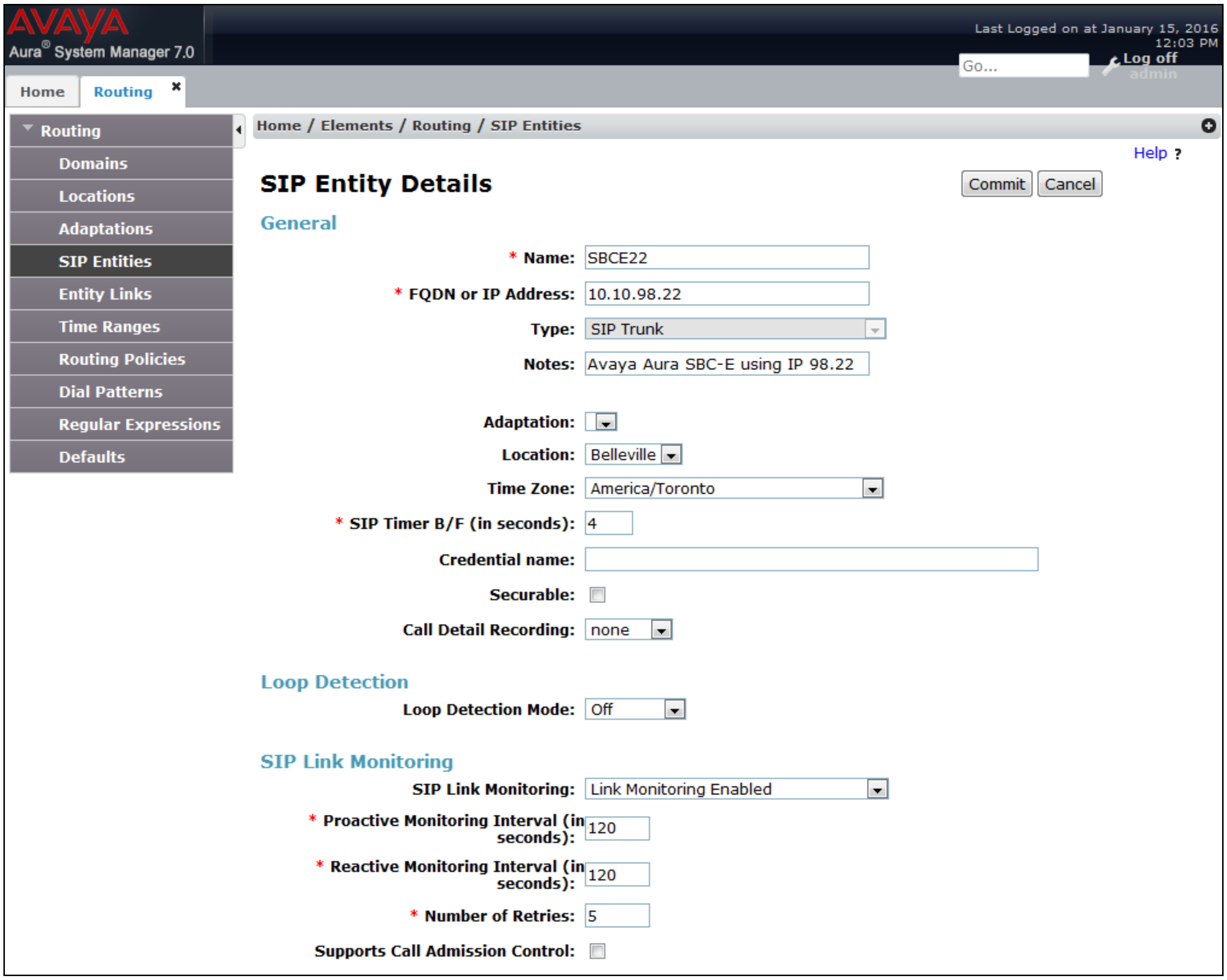
The compliance test used **Listen Ports** entry ***5061*** with ***TLS*** for connecting to Communication Manager and for connecting to the Avaya SBCE.



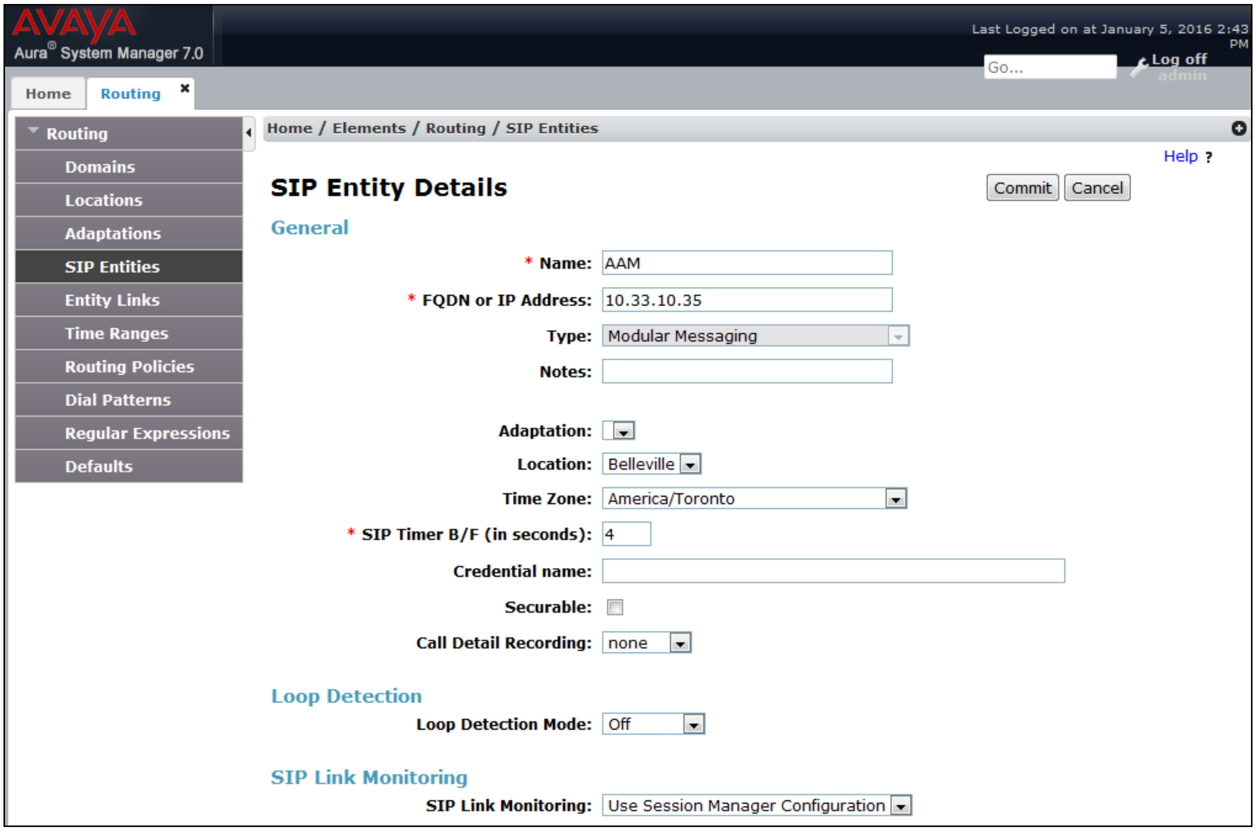
The following screen shows the addition of the Communication Manager SIP Entity. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to IP address of Communication Manager and **Type** to ***CM***. The **Location** and **Time Zone** parameters are set as shown in screen below.



The following screen shows the addition of the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as ***SIP Trunk***. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of ***120*** seconds. This setting allows Session Manager to send outbound OPTIONS heartbeat every ***120*** seconds to service provider (which is forwarded by the Avaya SBCE) to query the status of the SIP trunk connecting to service provider.



Similarly, a SIP Entity is added for Avaya Aura® Messaging server as shown in the capture below.



6.5. Add Entity Links

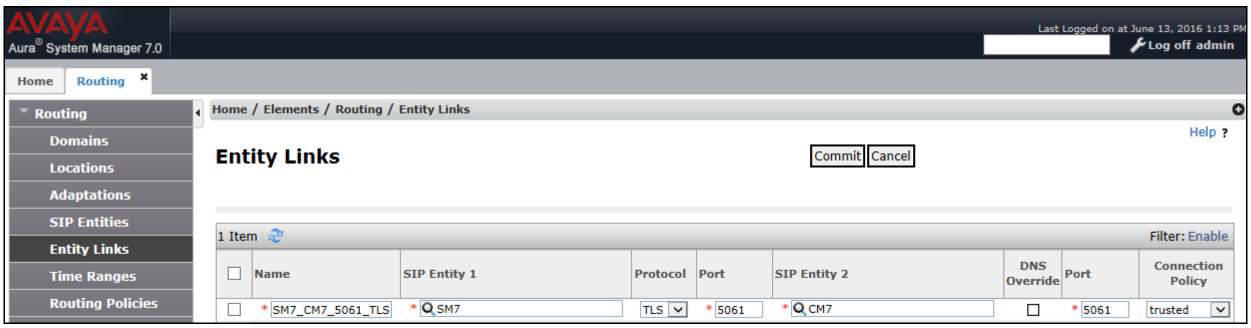
A SIP trunk between Session Manager and a telephony entity is described by an Entity Link. During compliance testing, three Entity Links were created, one for Communication Manager, Avaya Aura® Messaging and other for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager entity defined in **Section 6.4**.
- **Protocol:** Select the transport protocol used for this link, ***TLS*** for the Entity Link to Communication Manager and Avaya Aura® Messaging and ***TLS*** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section** Error! Reference source not found.. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section** Error! Reference source not found..

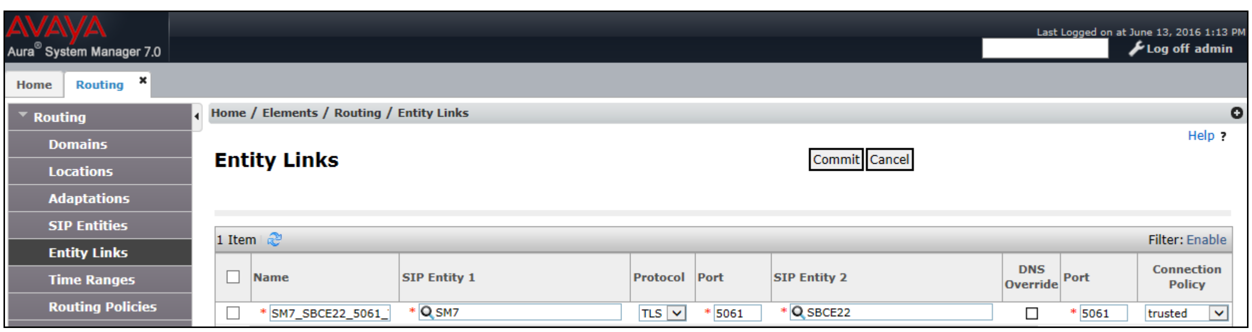
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. **Note**: If this is not selected, calls from the associated SIP Entity specified in **Section** Error! Reference source not found. will be denied.
- Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and to the Avaya SBCE.

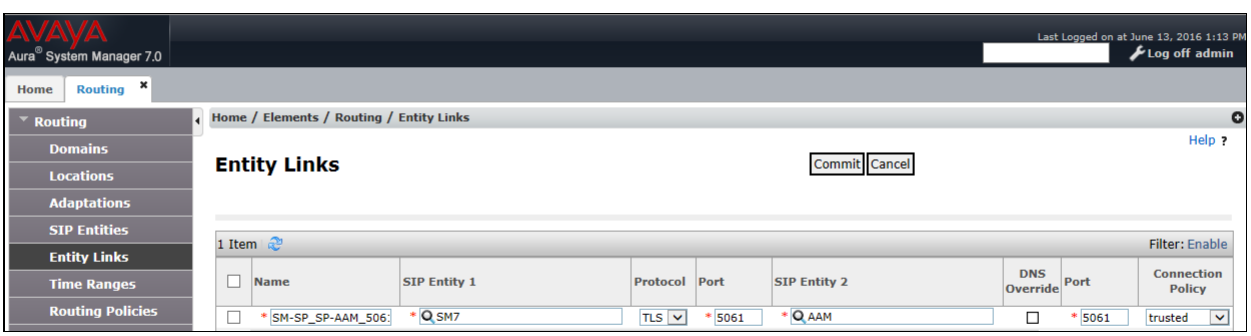
Entity Link to Communication Manager



Entity Link to Avaya SBCE



Entity Link to Avaya Aura® Messaging



6.6. Add Routing Policies

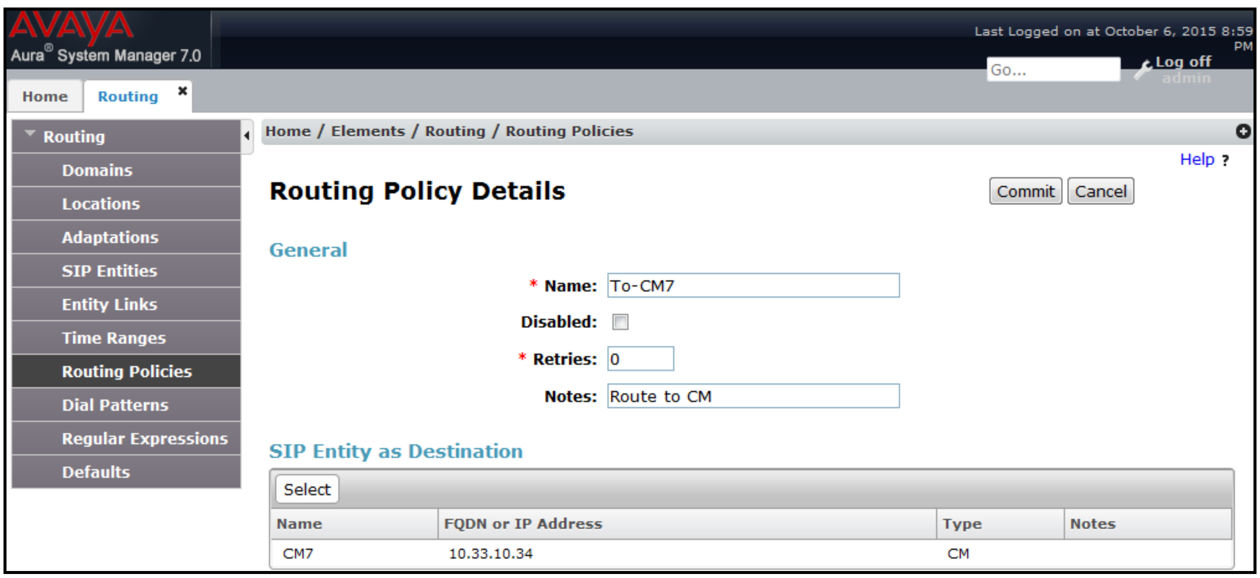
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section** Error! Reference source not found.. Three routing policies were added, one for Communication Manager, Avaya Aura® Messaging and other for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click **New** button in the right pane (not shown). The following screen is displayed.

In the **General** section, configure the following fields:

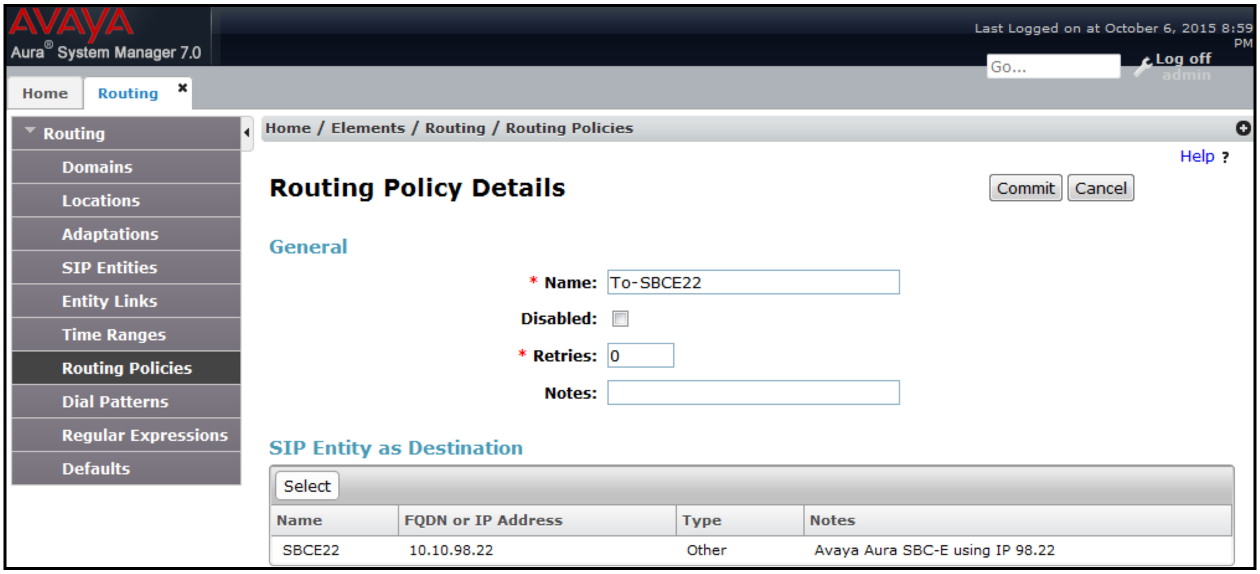
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In **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 is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

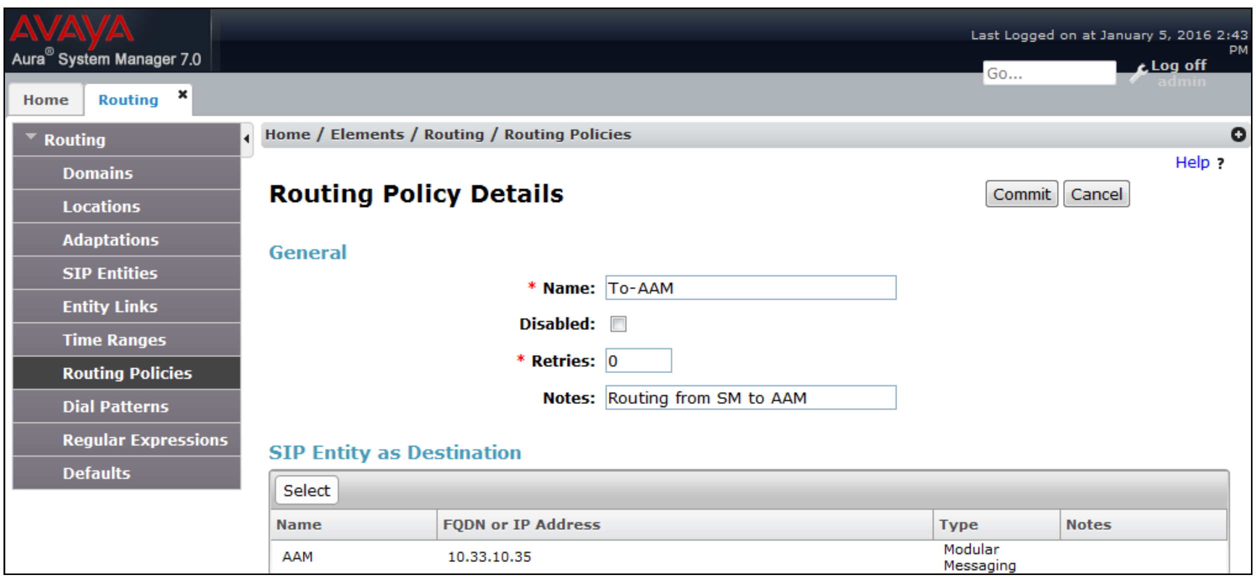
The following screens show the Routing Policy for Communication Manager.



The following screens show the Routing Policy for the Avaya SBCE.



The following screens show the Routing Policy for the Avaya Aura® Messaging.



6.7. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Avaya Aura® Messaging and from Communication Manager to Liechtenstein and vice versa. Dial Patterns define which routing 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 navigation pane and click **New** button in the right pane (not shown).

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

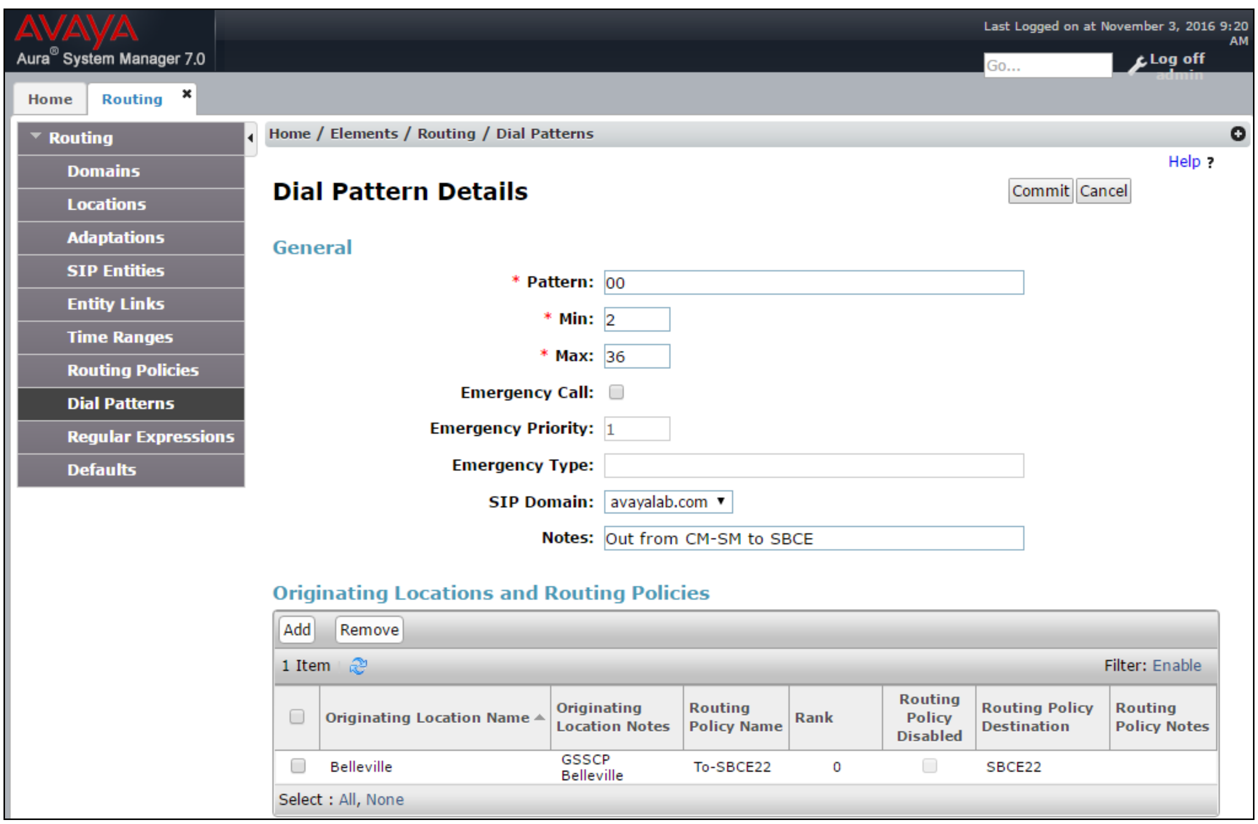
- **Pattern:** Enter a dial string that will be matched against the "Request-URI" of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:**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

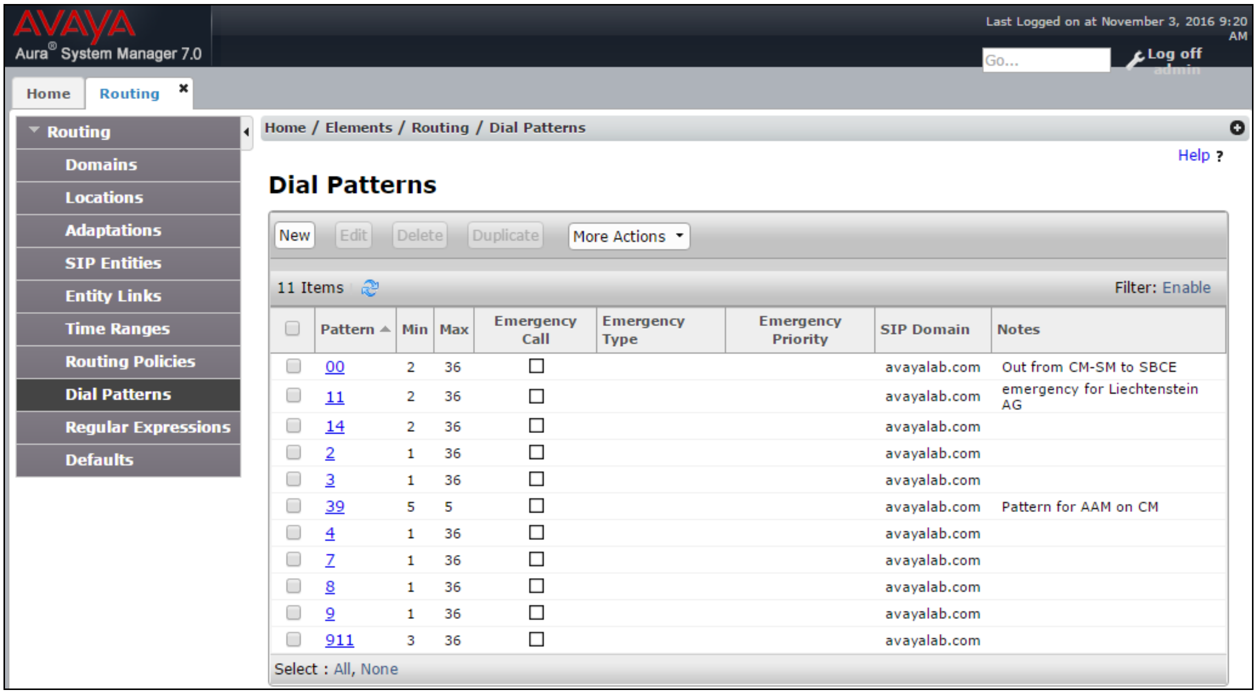
Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance testing are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

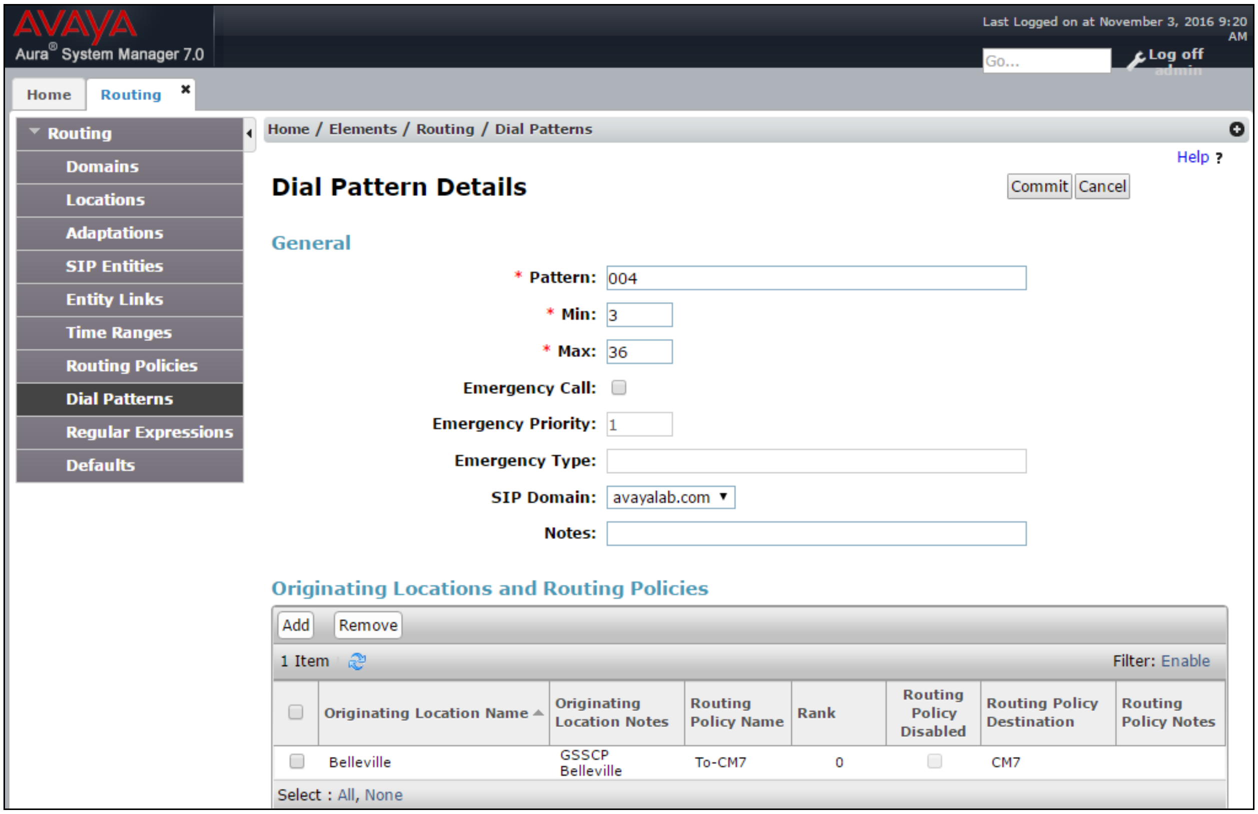
The first example shows that 12-digit dialed numbers that have a destination domain of "avayalab.com" uses route policy to Avaya SBCE as defined in **Section** Error! Reference source not found..



Similarly, the some other dial patterns can be defined for numbering plan mentioning in **Section 5.10.**



The second example shows that inbound 10-digit numbers with domain “avayalab.com” to use route policy to Communication Manager as defined in **Section** Error! Reference source not found.. These are the DID numbers assigned to the enterprise by Liechtenstein. In the testing, 004232372780 - 004232372789 was used.



6.8. 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, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click **New** button in the right pane (not shown). If the Session Manager Instance already exists, 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, configure the following fields:

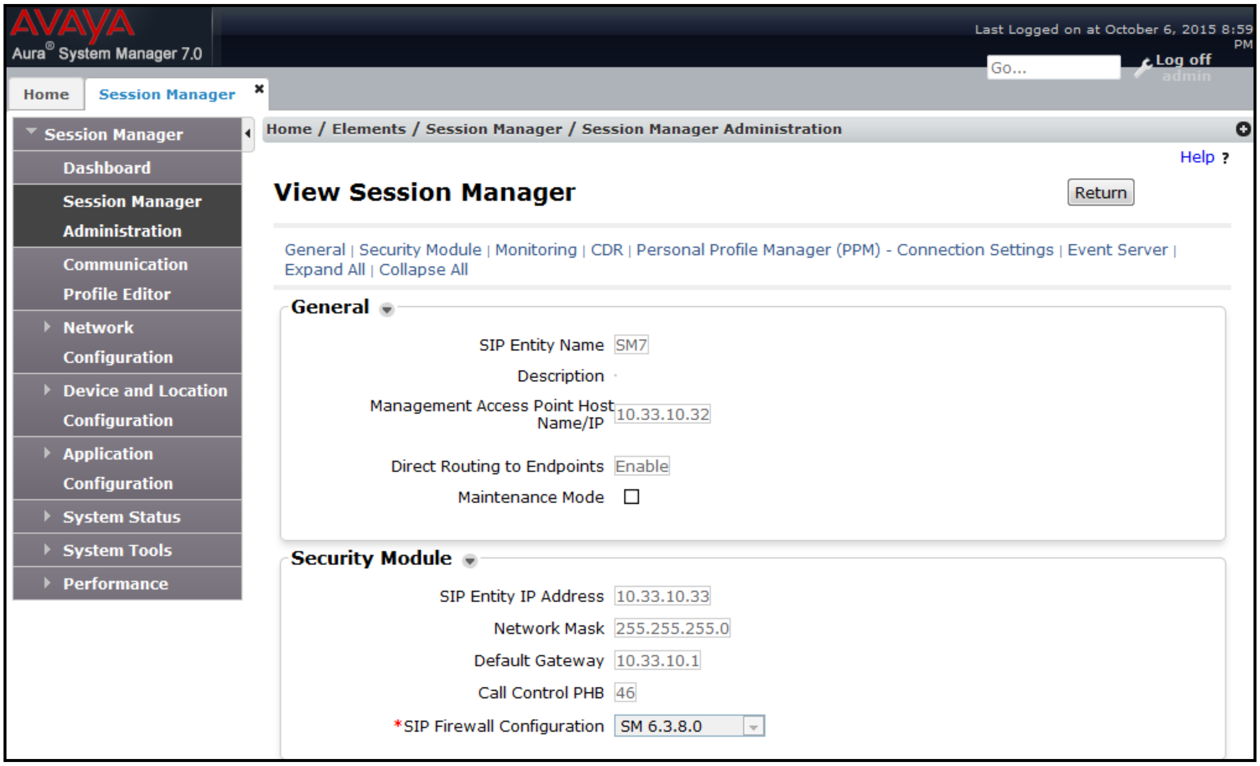
- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.
- **Directs Routing to Endpoints**: Enabled, to enable call routing on the Session Manager.

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.

- **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 **Commit** to save (not shown).

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

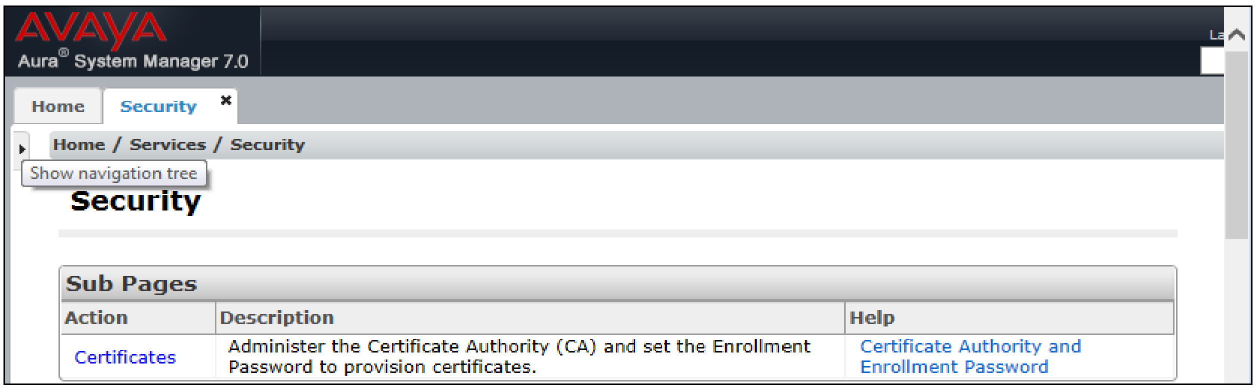


6.9. TLS Certificate Management on System Manager

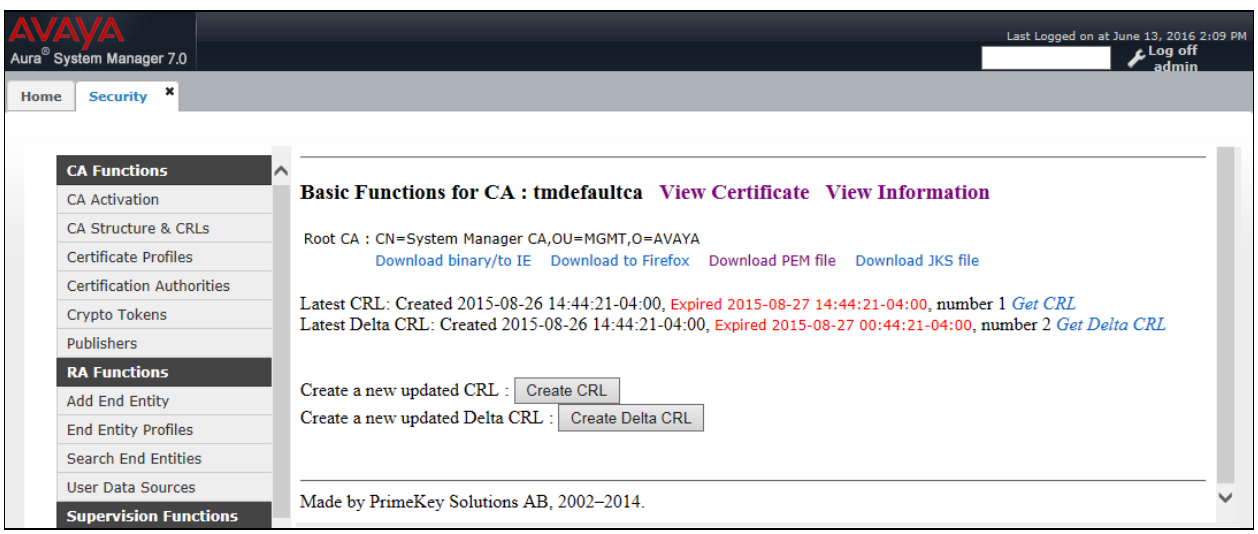
This section is to provide a procedure how to download System Manger CA certificate which is being installed on Avaya Communication Manager and Avaya SBCE for the communication between Avaya system components using TLS connectivity.

How to download System Manager CA certificate from Avaya System Manger

From System Manager Menu in **Section 6.1**, navigate to **Services → Security**. Click on arrow tab to show navigation tree as shown.



Navigate to **Certificates → Authority → CA Functions → CA Structure & CRLs**. Then click on **Download PEM file** to download the System Manager CA and save it as ***SystemManagerCA.pem*** to a directory on local management PC.



7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya SBCE is used as the edge device between the Avaya CPE and Liechtenstein SIP Trunking Service.

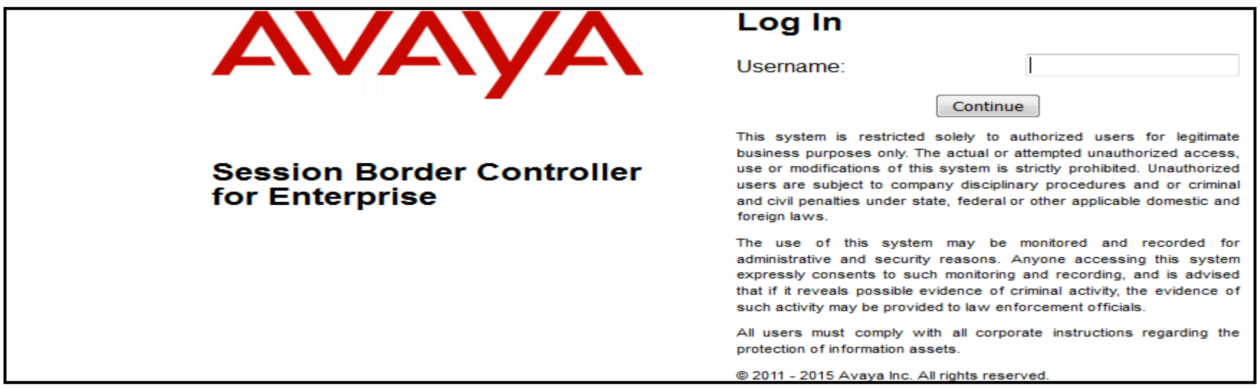
These Application Notes assume that the installation of the Avaya SBCE and the assignment of a management IP Address have already been completed.

In this session, the naming convention used for Liechtenstein is Service Provider (**SP**), which is connected to the external interface of the Avaya SBCE. And for the Avaya side is Enterprise (**EN**), which is connected to the internal interface of the Avaya SBCE.

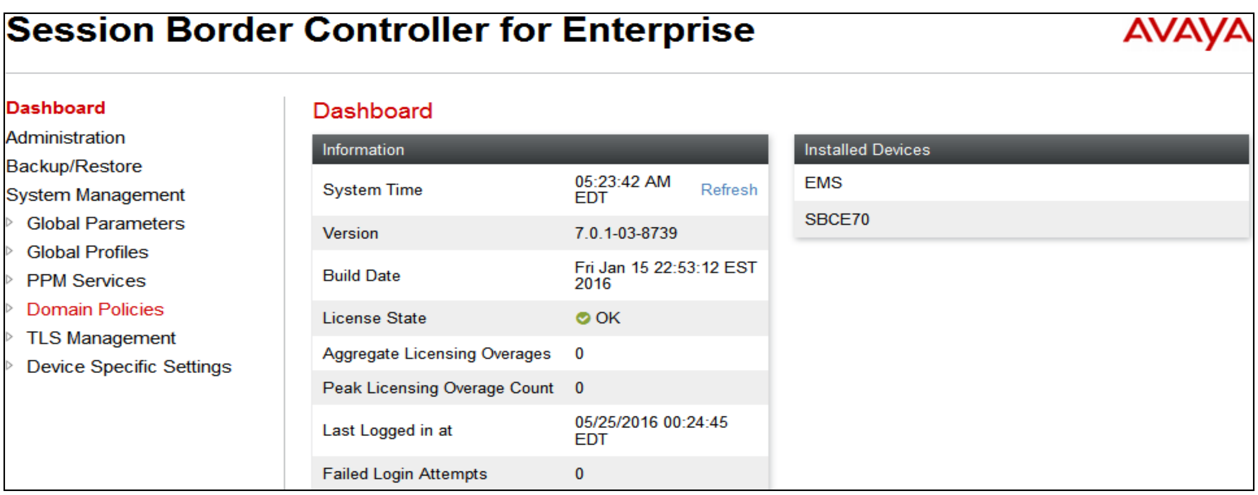
7.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Avaya SBCE web interface, enter "https://<ip-addr>/ucsec" in the address field of the web browser (not shown), where "<ip-addr>" is the management LAN IP address of Avaya SBCE.

Enter appropriate credentials and click ***Log In***.



The main page of the Avaya SBCE will appear as shown below.



7.2. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. The Avaya SBCE utilizes TLS primarily to facilitate secure communications with remote users.

Avaya SBCE is preinstalled with several certificates and profiles that can be used to quickly set up secure communication using TLS, which are listed in the Pre-installed Avaya Profiles and Certificates section. Session Manager, Avaya SBCE and the 96x1 IP Deskphones are shipped with default identify certificate to enable out-of-box support for TLS sessions. Do not use this default certificate in a production/customer environment since this certificate is common across all instances of Session Manager, Avaya SBCE and 96x1 IP Deskphones. Avaya SBCE supports the configuration of third-party certificates and TLS settings. For optimum security, Avaya recommends using third-party CA certificates for enhanced security

Testing was done with default identity certificates, the procedure to obtain and install 3rd party CA certificates is outside the scope of these application notes.

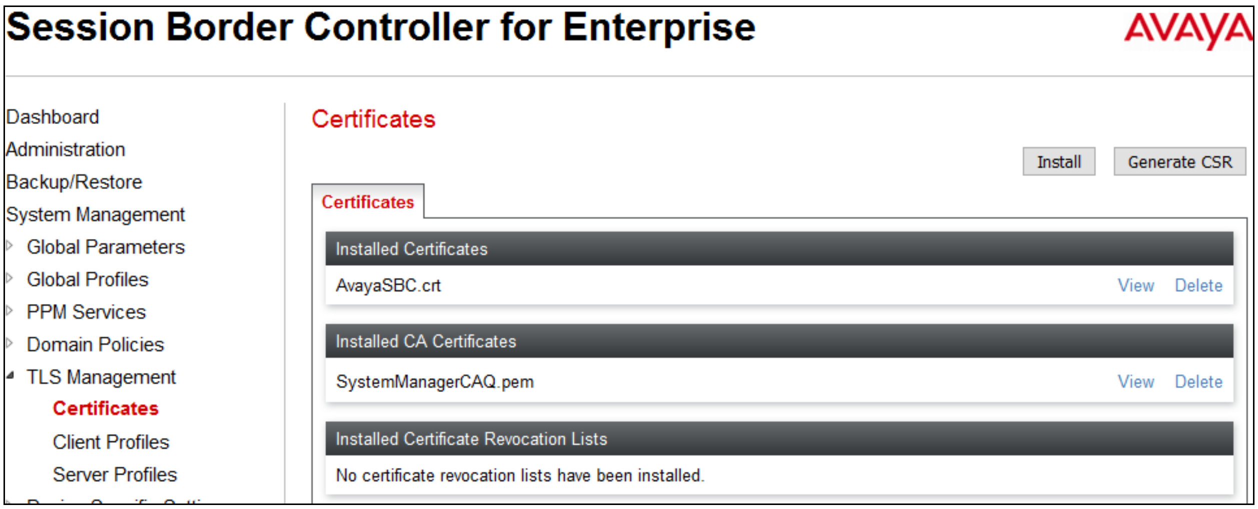
In this compliance testing, TLS transport is used for the communication between Avaya Session Manager and Avaya SBCE. The following procedures show how to create the client and server profiles.

7.2.1. Certificates

You can use the certificate management functionality that is built into the Avaya SBCE to control all certificates used in TLS handshakes. You can access the Certificates screen from **TLS Management → Certificates**.

Ensure the preinstalled certificates are presented in the system as shown below.

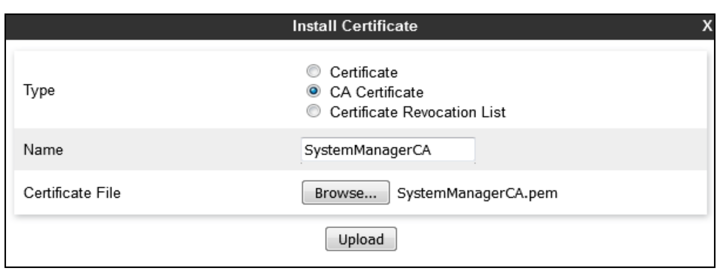
- ***AvayaSBCcrt*** is Avaya SBCE Certificate Authority root certificate.
- ***SystemManagerCAQ.pem*** is System Manager Certificate Authority root certificate.



If System Manager Certificate Authority certificate (SystemManagerCAQ.pem) is not present, the following procedure shows how to install it on the Avaya SBCE.

System Manager CA certificate is obtained using procedure provided in **Section 6.9**. Then on the Avaya SBCE, navigate to **TLS Management → Certificates**. Click on **Install** button.

- Select **CA Certificate**.
- Provide a descriptive **Name**.
- **Browse** to the directory where the System Manager CA previously saved and select it.
- Click **Upload**.

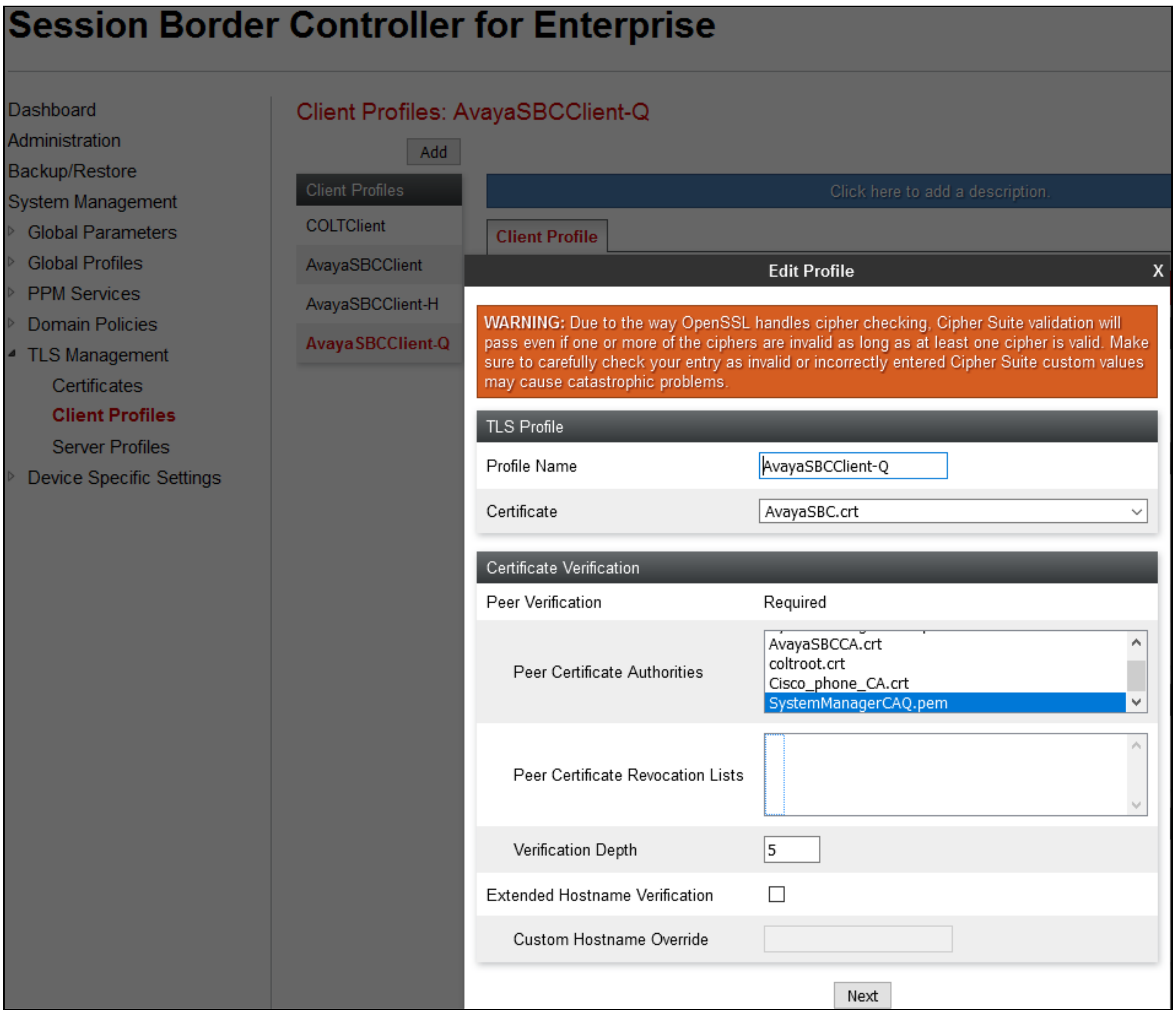


7.2.2. Client Profiles

This section describes the procedure to create client profile for Avaya SBCE to communicate with Avaya Session Manager via TLS signalling.

To create Client profile, navigate to **TLS Management → Client Profiles**, click on **Add**.

- Enter descriptive name in **Profile Name**.
- Select ***AvayaSBC.crt*** from pull down menu of **Certificate**.
- Select ***SystemManagerCAQ.pem*** from pull down of **Peer Certificate Authorities**.
- Enter ***5*** as **Verification Depth**.
- Click **Finish**.

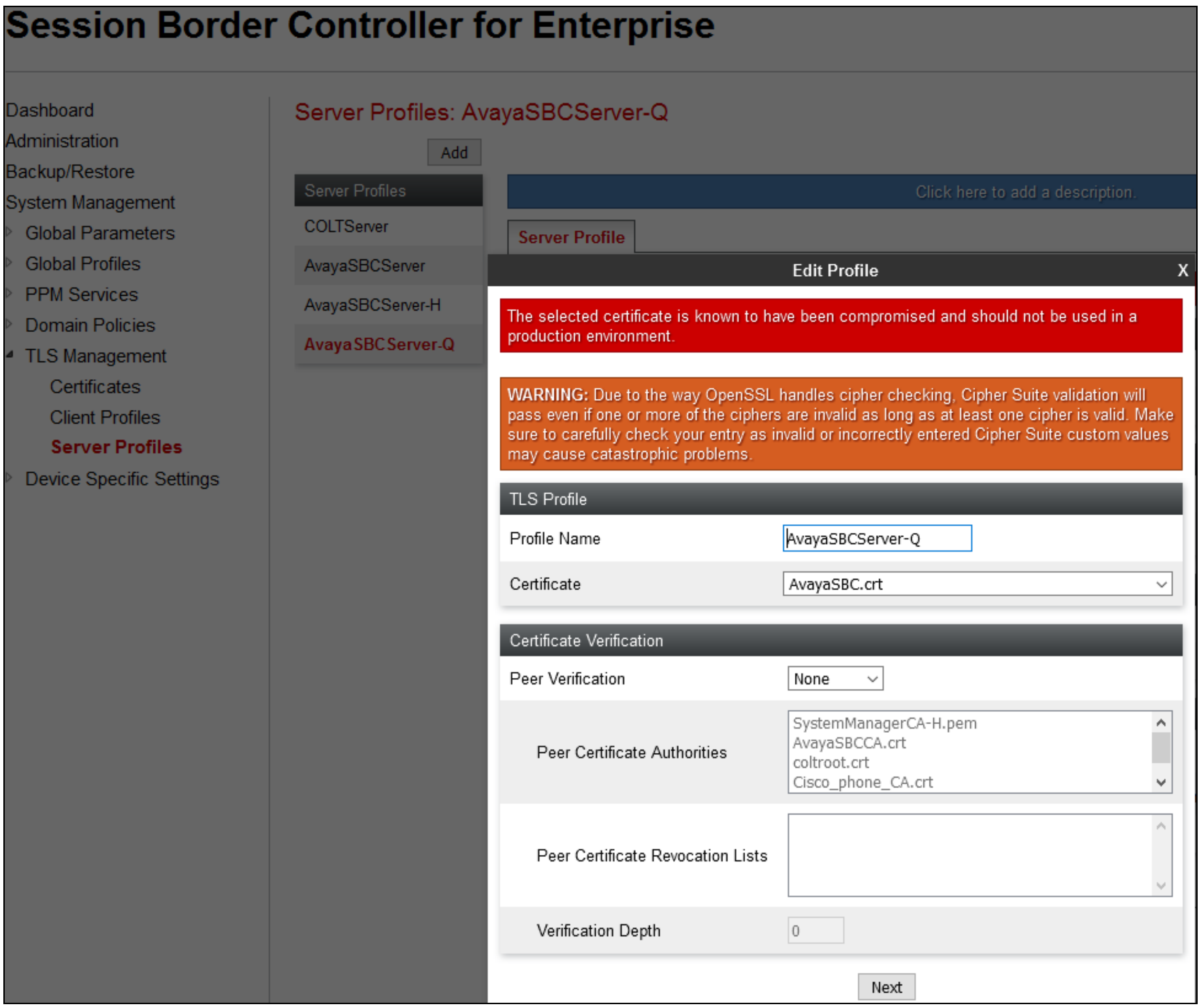


7.2.3. Server Profiles

This section describes the procedure to create server profile for Avaya SBCE to communicate with Avaya Session Manager via TLS signalling.

To create Server profile, navigate to **TLS Management** → **Server Profiles**, click on **Add**.

- Enter descriptive name in **Profile Name**.
- Select ***AvayaSBC.crt*** from pull down menu of **Certificate**.
- Select ***None*** from pull down menu of **Peer Verification**.
- Others are left at default.
- Click Next and **Finish** (not shown).



7.3. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.3.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*” is used for all incoming and outgoing traffic.

7.3.2. Server Interworking Profile

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles → Server Interworking**. Click on the **Add** button.

In the compliance testing, two Server Interworking profiles were created for SP and EN respectively.

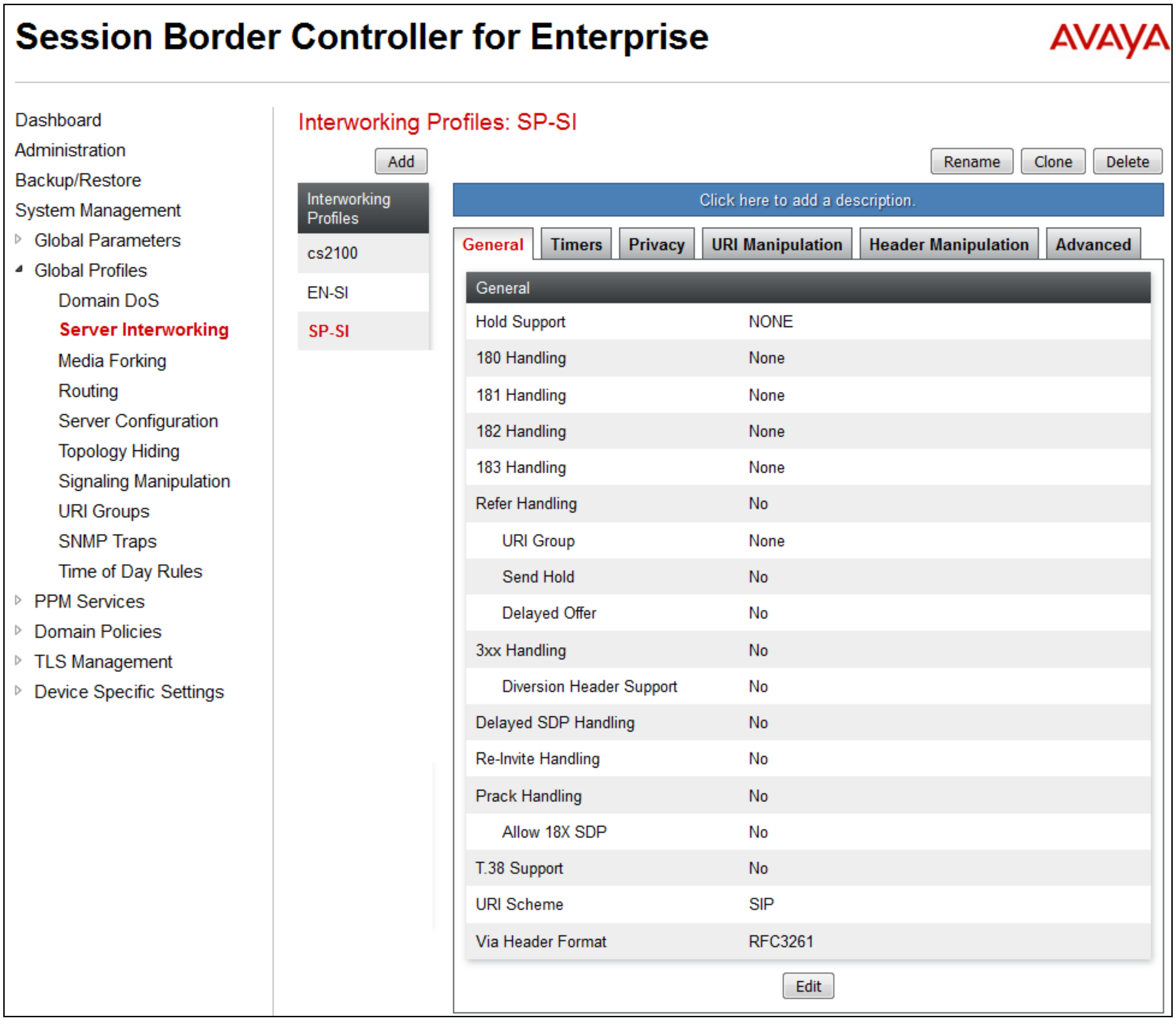
Server Interworking profile for SP

Profile **SP-SI** was defined to match the specification of SP. The **General, URI Manipulation** and **Advanced** tabs are configured with the following parameters while the other tabs for **Timers, Privacy** and **Header Manipulations** are kept as default.

General tab:

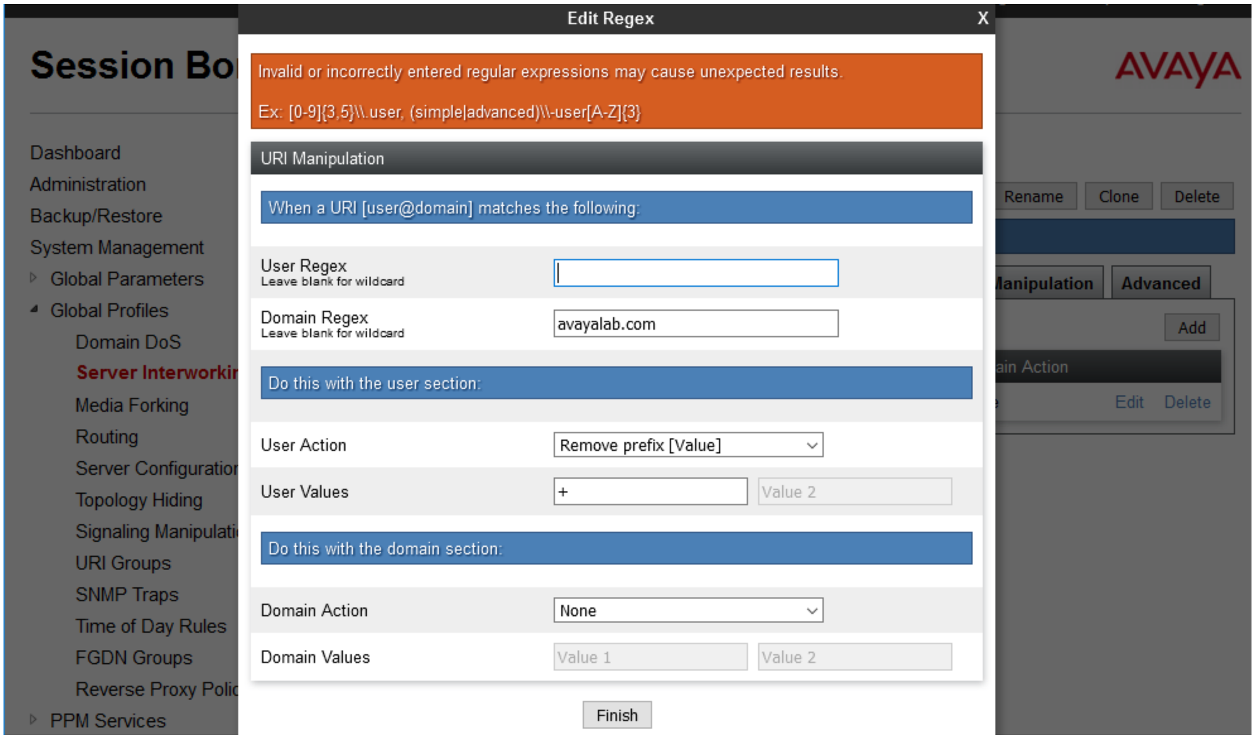
- **Hold Support** = ***NONE***. The Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- **18X Handling** = ***None***. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = ***No.*** The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = ***No***. SP does not support T.38 fax in the compliance testing.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI, General**.

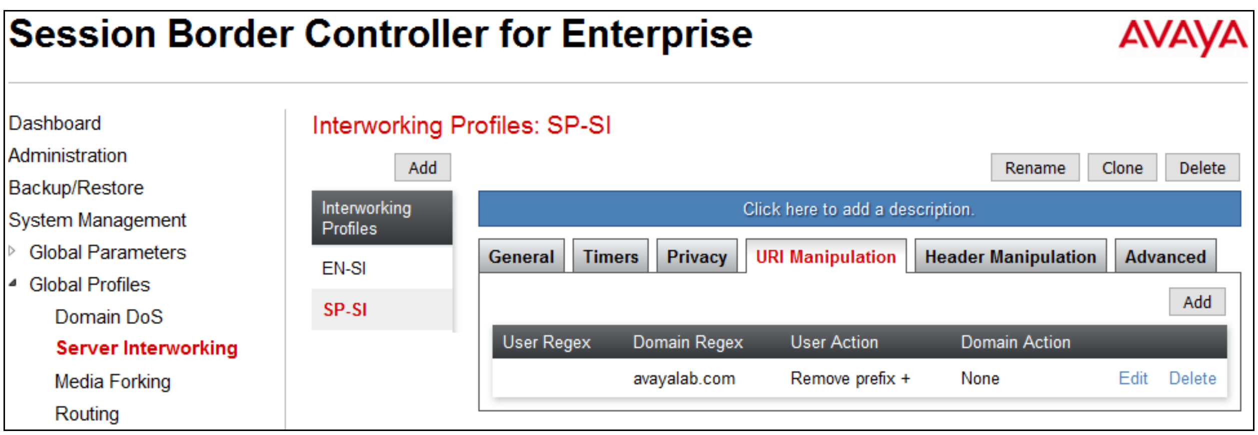


URI Manipulation tab:

- **Domain Regex** is set to ***avayalab.com***.
- **User Action** is set to ***Remove prefix [Value]***.
- **User Values** is **+.**
- Other fields are left at default.



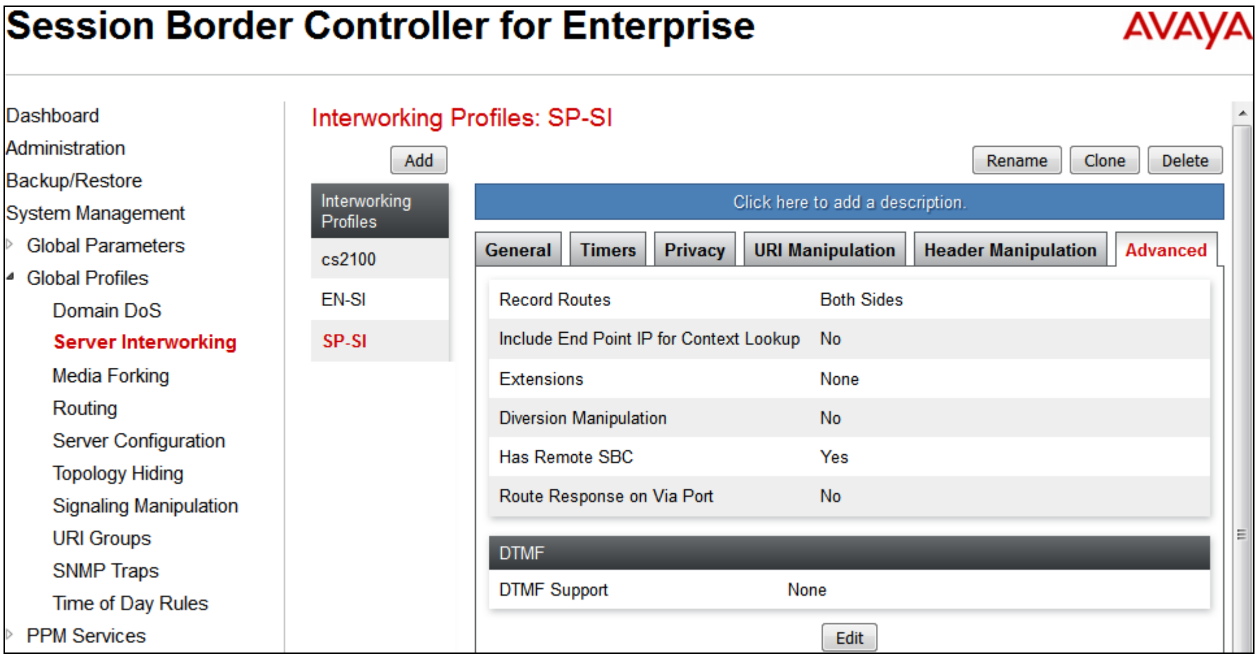
URI Manipulation as shown.



Advanced tab:

- **Record Routes**: ***Both Sides***.
- **Include End Point IP for Context Lookup**: ***No***.
- **Extensions**: ***None***.
- **Has Remote SBC**: ***Yes***. SP has a SBC which interfaces its Central Office (CO) to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from SP for the media.
- **DTMF Support**: ***None***. The Avaya SBCE will send original DTMF method from EN to SP.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI**, **Advanced**.



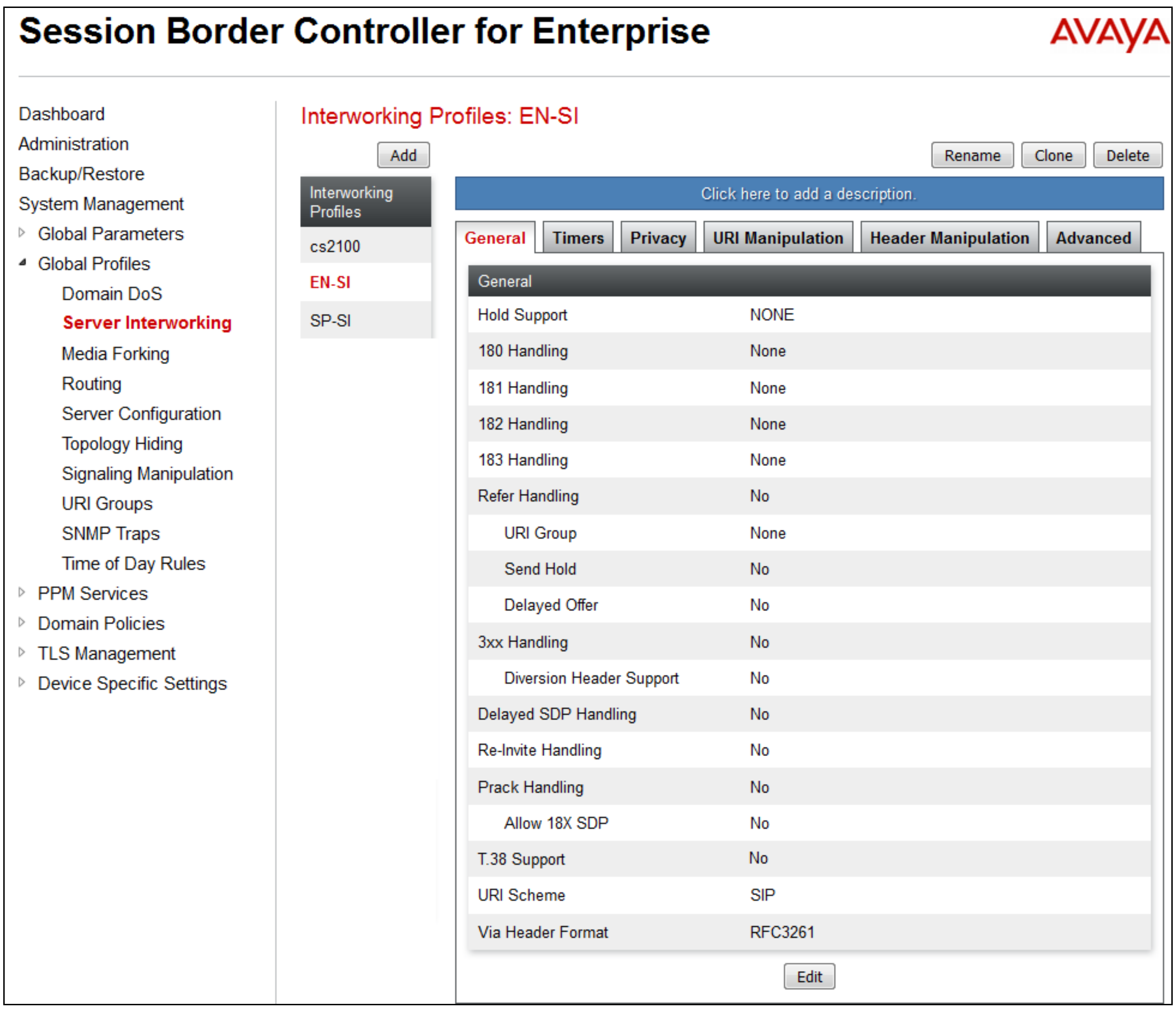
Server Interworking profile for EN

Profile **EN-SI** was defined to match the specification of EN. The **General** and **Advanced** tabs are configured with the following parameters while the other settings for **Timers**, **Privacy, URI Manipulation** and **Header Manipulation** are kept as default.

General tab:

- **Hold Support**: *None*.
- **18X Handling**: *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling**: *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support**: *No*.
- Others are left as default values.

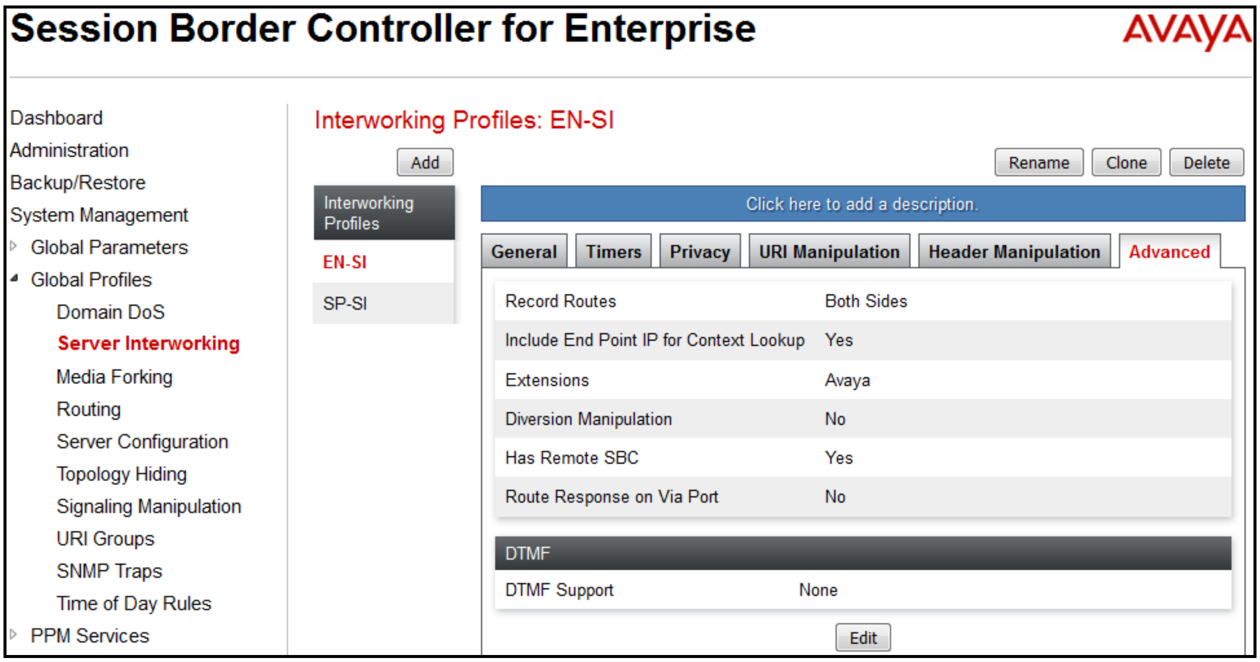
The screenshots below illustrate the Server Interworking profile **EN-SI**, **General**.



Advanced tab:

- **Record Routes**: ***Both Sides***. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup** = ***Yes***.
- **Extensions**: ***Avaya***.
- **Has Remote SBC**: ***Yes***. This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support**: ***None***. The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **EN-SI**, **Advanced.**

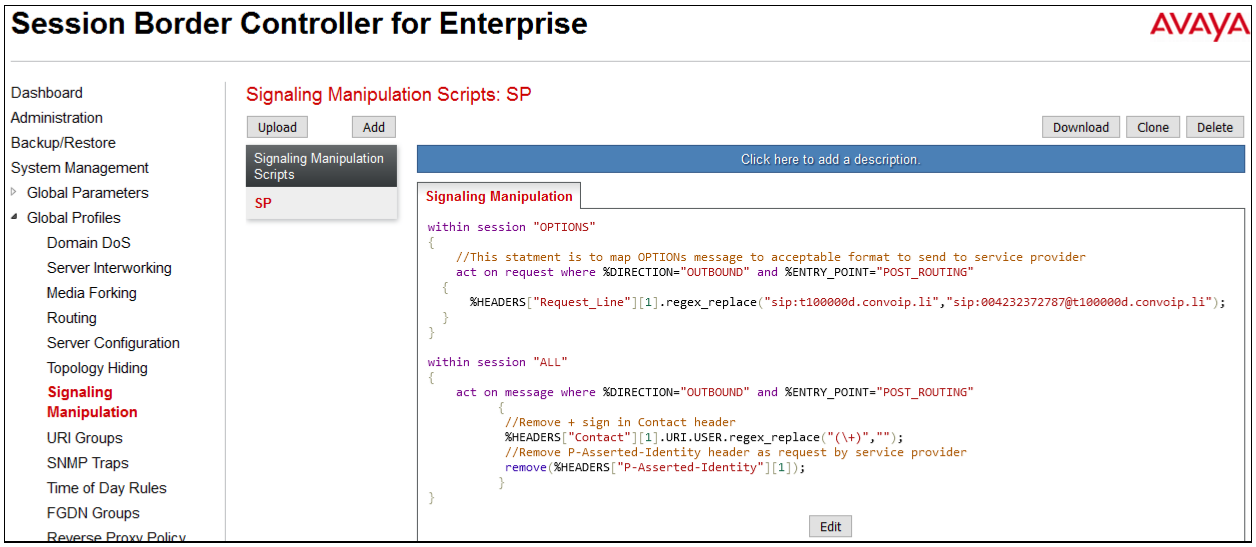


7.3.3. Configure Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature adds the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called **SigMa**.

To create a Signaling Manipulation script, select **Global Profiles → Signaling Manipulation**. Click **Add Script** (not shown).

In the compliance testing, a SigMa script by the name **SP** was created for the Server Configuration for SP and its details are captured below.



7.3.4. Server Configuration

The Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains. No configuration of **Heartbeat** is required.

To create a Server Configuration entry, select **Global Profiles →Server Configuration**. Click on the **Add** button.
In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for SP and server entry **EN-SC** for EN.

Server Configuration for SP

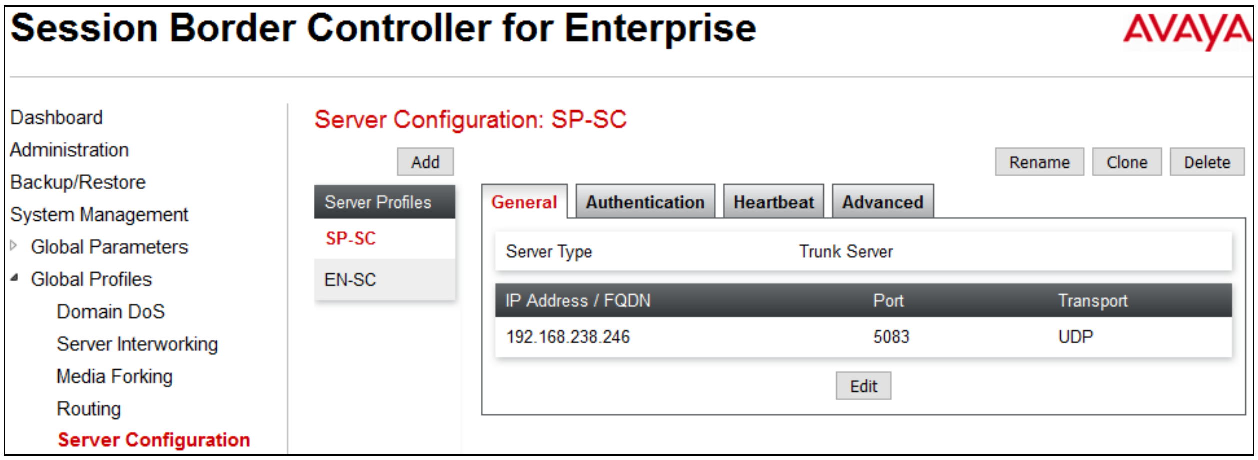
Server Configuration named **SP-SC** was created for SP. All tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN.

General tab:

Click on the **Add** button and enter the following information.

- Enter **Profile Name** ***SP-SC*** and click **Next**.
- Set **Server Type** for SP as ***Trunk Server***.
- Enter **IP Addresss/FQDN** provided by SP.
- In the compliance testing, SP supported ***UDP*** and listened on port ***5083***.
- Click **Next**, then **Next** and **Finish**.

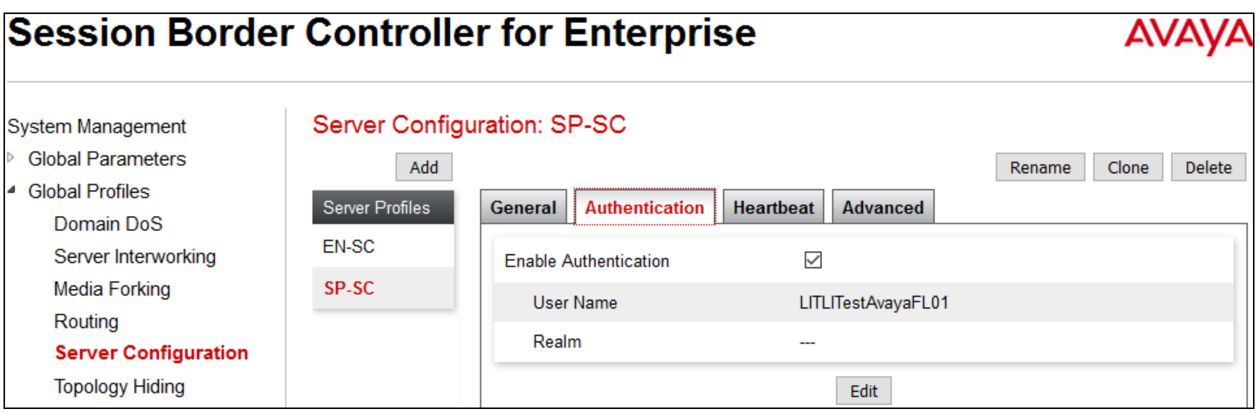
The completed server profile is shown below.



Authentication tab:

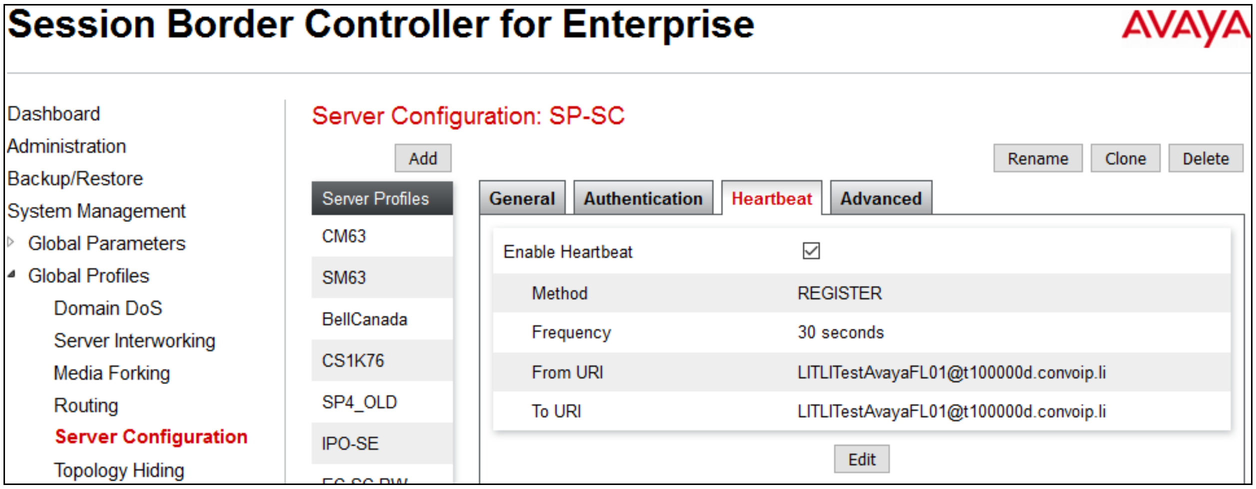
Click on the **Edit** button and enter following information.

- Check **Enable Authentication** check box.
- Enter **User Name** (provided by SP).
- Leave **Realm** blank.
- Enter **Password** and **Confirm Password** (provided by SP) (not shown).
- Click **Finish**.



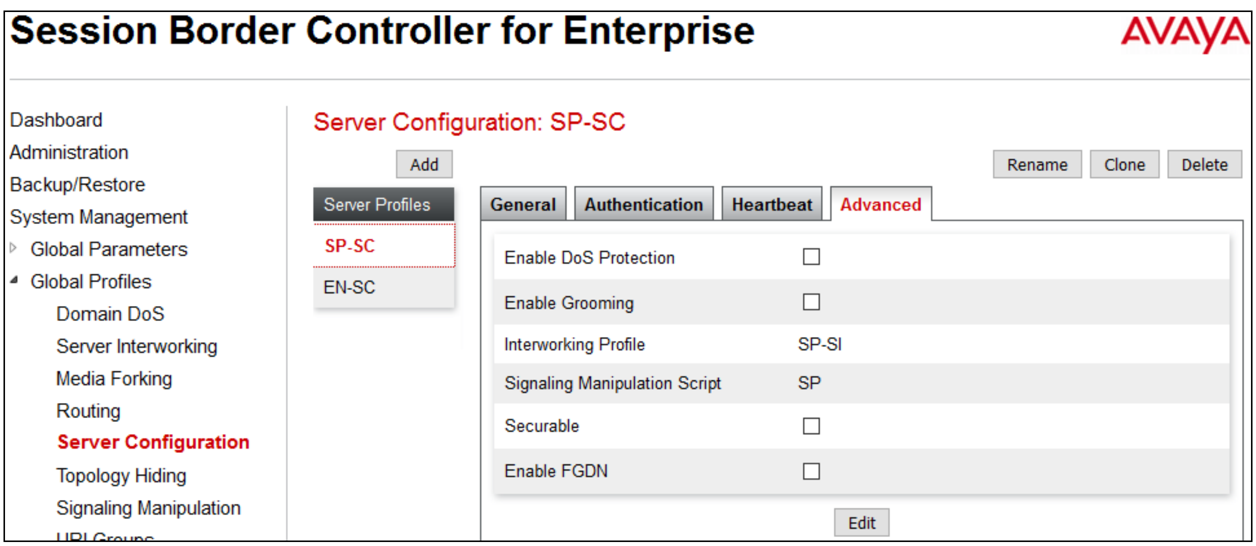
Heartbeat tab:
Click on the **Edit** button and enter following information.

- Enable **Enable Hearbeat** checkbox.
- Set the **Method** to ***REGISTER.***
- Set the **Frequency** to ***30 seconds***.
- Set **From URI** and **To URI** to provided URI by service provider.



Advanced tab:
Click on the **Edit** button and enter following information.

- **Interworking Profile** drop down list, select ***SP-SI*** as defined in **Section 7.3.2**.
- **Signaling Manipulation Script** drop down list, select ***SP*** as defined in **Section 7.3.3**.
- The other settings are kept as default.



Server Configuration for EN

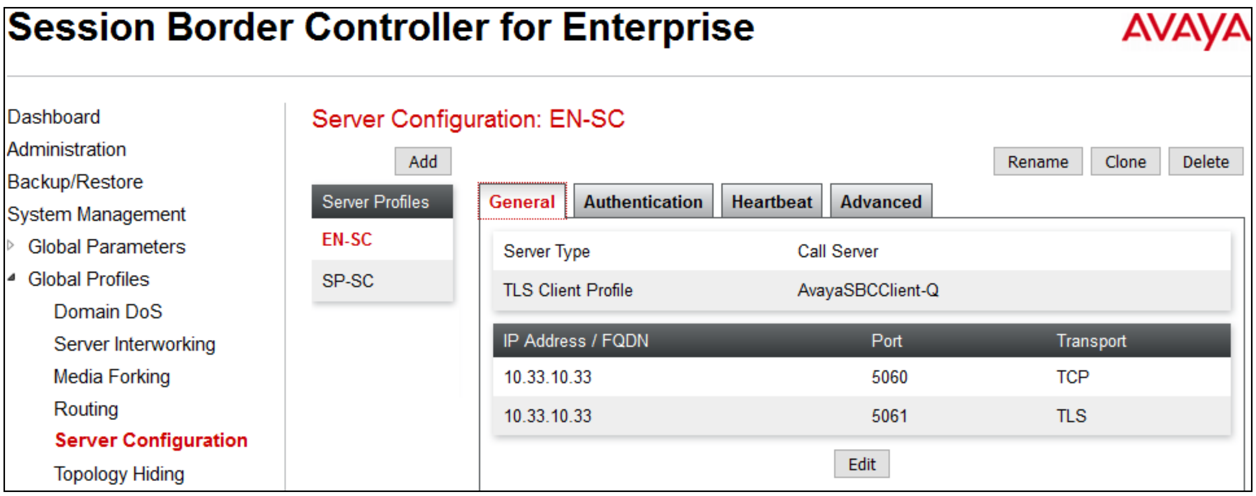
Server Configuration named **EN-SC** created for EN is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as ***disabled*** as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

General tab:

Click on the **Add** button and enter the following information.

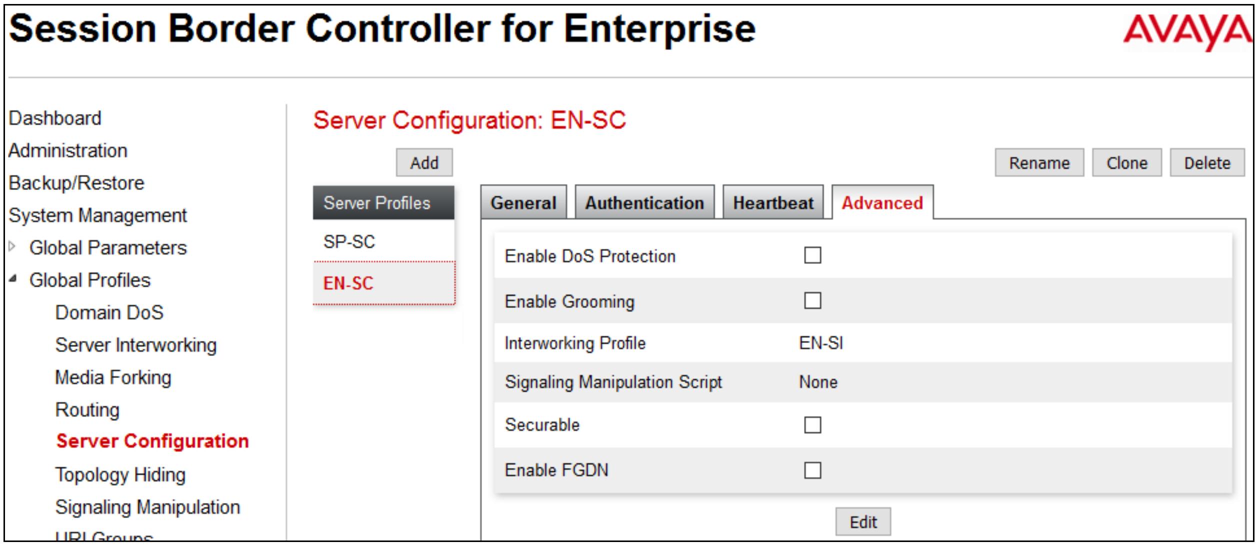
- Enter **Profile Name** as ***EN-SC*** and click **Next**.
- **Server Type** for EN as ***Call Server***.
- Select ***AvayaSBCClien-Q*** for **TLS Client Profile.**
- **IP Address/FQND** is Session Manager IP address.
- **Transport**, the link between the Avaya SBCE and EN was ***TLS***.
- Listened on **Port *5061***.
- Click **Next**, **Next** and then **Finish**.

The completed server profile is shown below.



Advanced tab:
Click on the **Edit** button to enter the following information.

- **Interworking Profile** drop down list select ***EN-SI*** as defined in **Section** Error! Reference source not found..
- The other settings are kept as default.



7.3.5. Routing Profiles

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

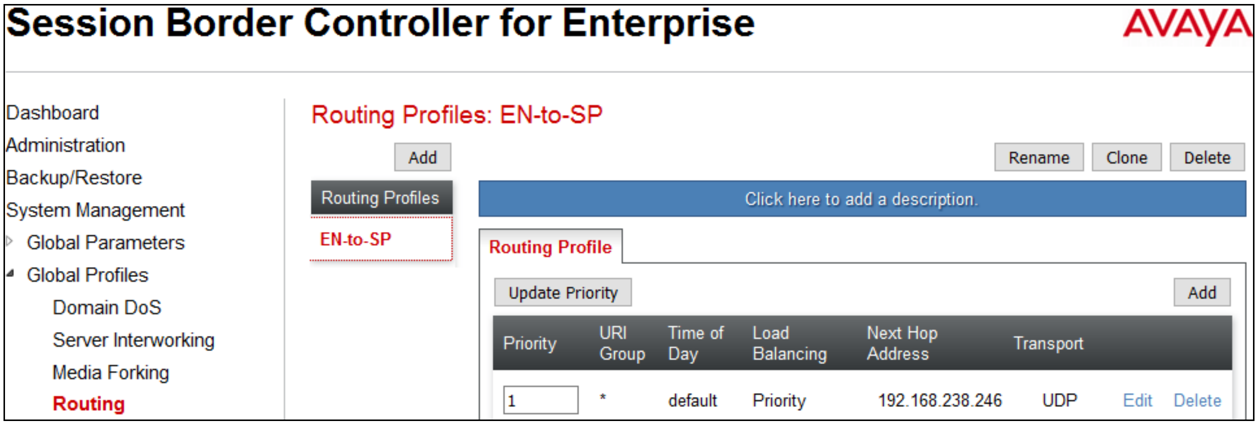
To create a Routing Profile, select **Global Profiles → Routing**. Click on the **Add** button.

In the compliance testing, a Routing Profile **EN-to-SP** was created to use in conjunction with the server flow defined for EN. This entry is to route the outbound call from the enterprise to the service provider.

In the opposite direction, a Routing Profile named **SP-to-EN** was created to be used in conjunction with the server flow defined for SP. This entry is to route the inbound call from the service provider to the enterprise.

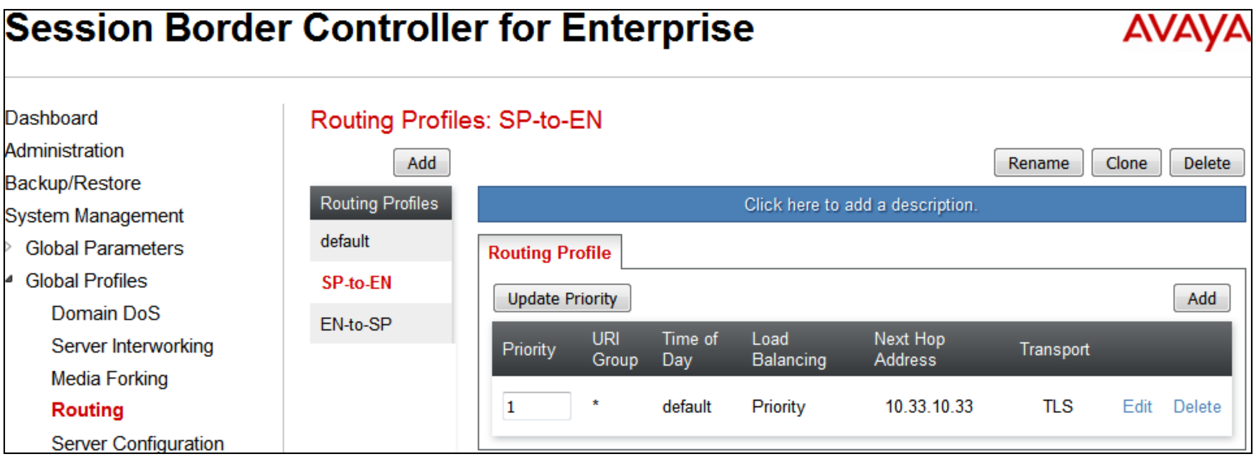
Routing Profile for SP

The screenshot below illustrate the routing profile from Avaya SBCE to the SP network, **Global Profiles → Routing**: **EN-to-SP**. As shown in **Figure 1**, the SP SIP trunk is connected with transport protocol ***UDP*** (not shown). If there is a match in the "To" or "Request URI" headers with the URI Group "*" as described in **Section 7.3.1**, the call will be routed to the **Next Hop Address** which is the IP address of SP SIP trunk.



Routing Profile for EN

The Routing Profile for SP to EN, **SP-to-EN**, was defined to route call where the "To" header matches the URI Group **SP** defined in **Section 7.3.1** to **Next Hop Address** which is the IP address of Session Manager as a destination. As shown in **Figure 1**, the SIP trunk between EN and the Avaya SBCE is connected with transport protocol ***TLS***.



7.3.6. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding**. Click on the **Add** button.

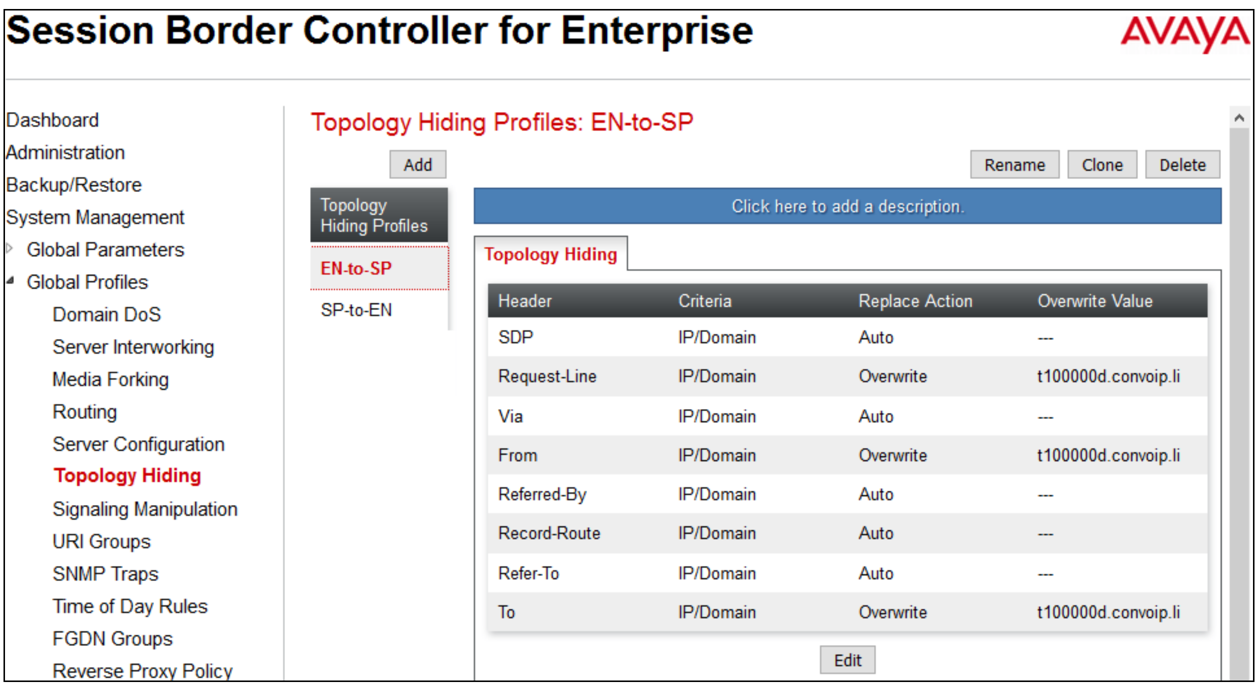
In the compliance testing, two Topology Hiding profiles **EN-to-SP** and **SP-to-EN** were created.

Topology Hiding Profile for SP

Profile **EN-to-SP** was defined to mask the enterprise SIP domain avayalab.com in the “Request-Line”, “From” and “To” headers to SP provided full qualified domain name. This is done to secure the enterprise network topology and to meet the SIP requirement of the service provider.
Notes:

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header.
- The masking applied on “To” header.

The screenshots below illustrate the Topology Hiding profile **EN-to-SP**.



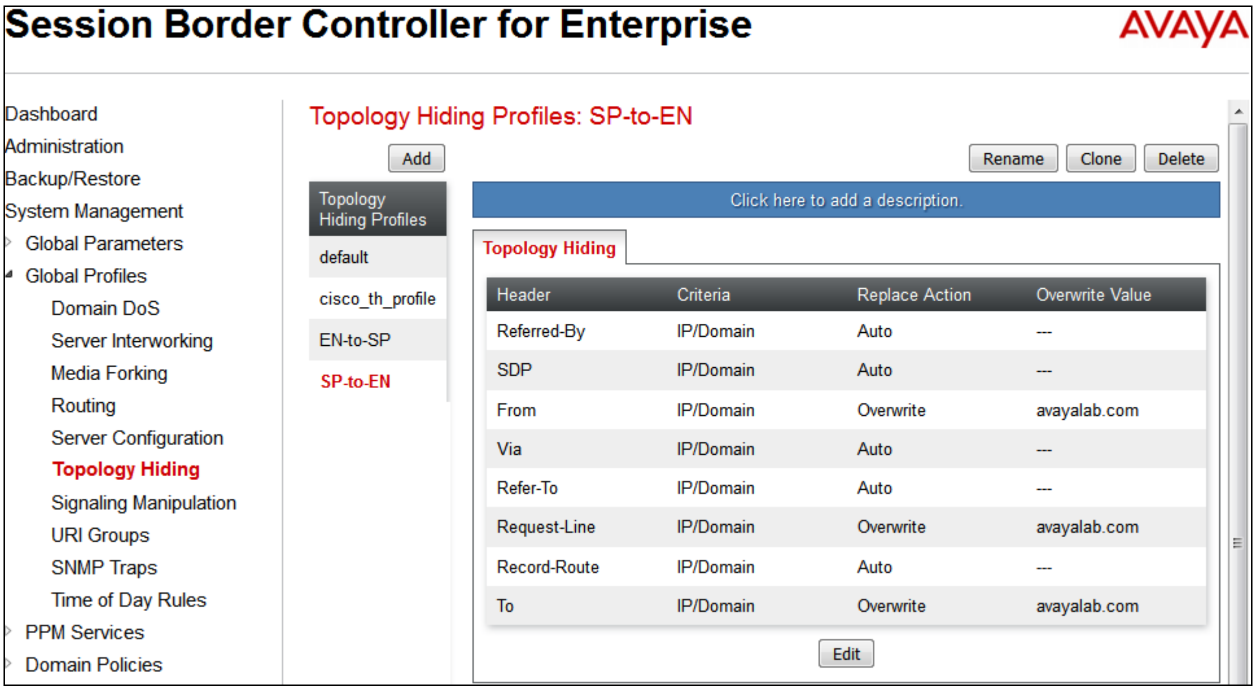
Topology Hiding Profile for EN

Profile **SP-to-EN** was also created to mask SP URI-Host in “Request-Line”, “From” and “To”, headers to the enterprise domain ***avayalab.com***, replace Record-Route, Via headers and SDP added by SP to internal IP address known to EN.

Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header.
- The masking applied on “To” header.

The screenshots below illustrate the Topology Hiding profile **SP-to-EN**.



7.4. Domain Policies

Domain Policies configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

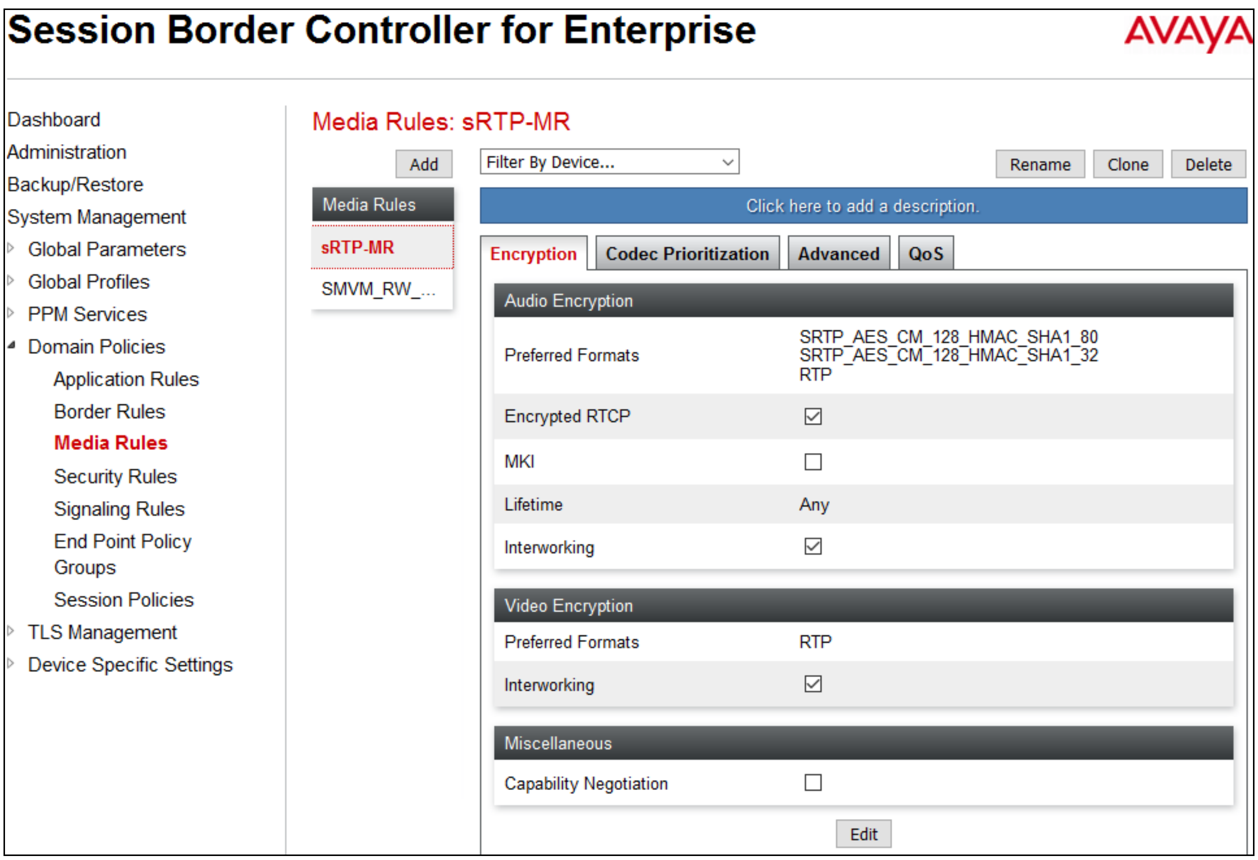
7.4.1. Media Rules

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

To clone a Media Rule, navigate to **Domain Policies → Media Rules**. With ***default-low-med*** rule chosen, click on the **Clone** button.

Media Rules for EN

In this compliance testing, Secure Real-Time Transport Protocol (SRTP, media encryption) is used within enterprise network only. Therefore, it is necessary to create a media rule to apply to the internal interface of Avaya SBCE and EN. Created **sRTP-MR** rule is shown below.



7.4.2. Signaling Rules

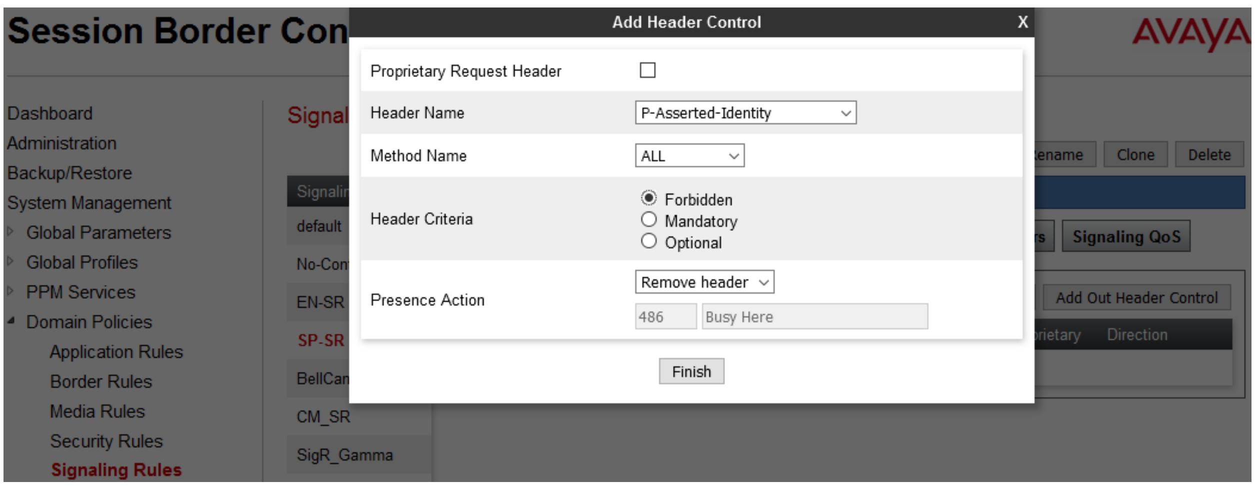
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To clone a Signaling Rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click on the **Clone** button.

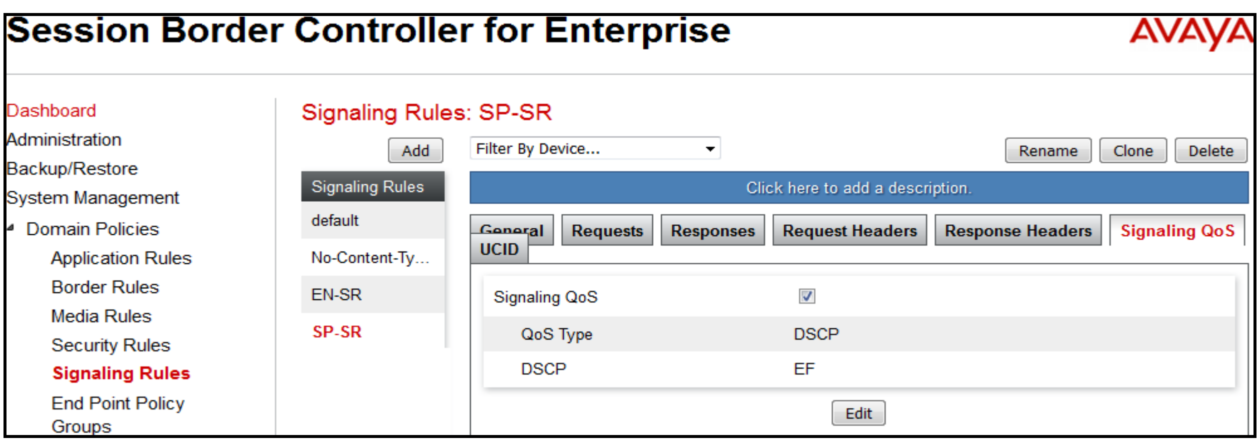
Signaling Rules for SP

In the compliance testing, created signaling rule **SP-SR** is discussed below. All the tabs are kept as default values except the **Signaling QoS** tab.

In **Request Headers** tab, click **Add Out Header Control** button then enter information as shown in capture below.



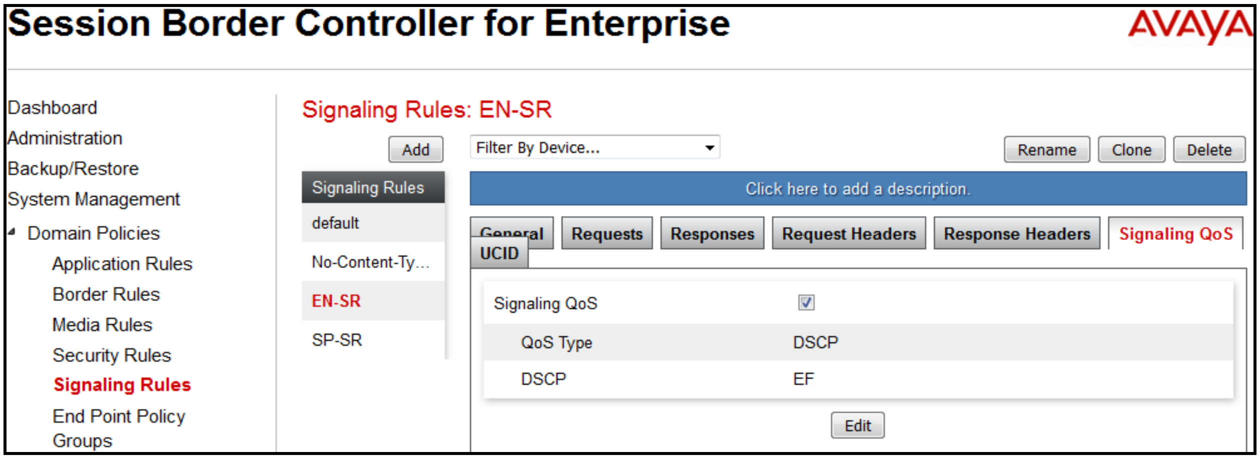
In the **Signaling QoS** tab, click on **Edit** button then check on checkbox. Then select ***EF*** value for **DSCP** option.



Signaling Rules for EN

In the compliance testing, created signaling rule **EN-SR** is discussed below. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button then check on checkbox. Then select ***EF*** value for **DSCP** option.



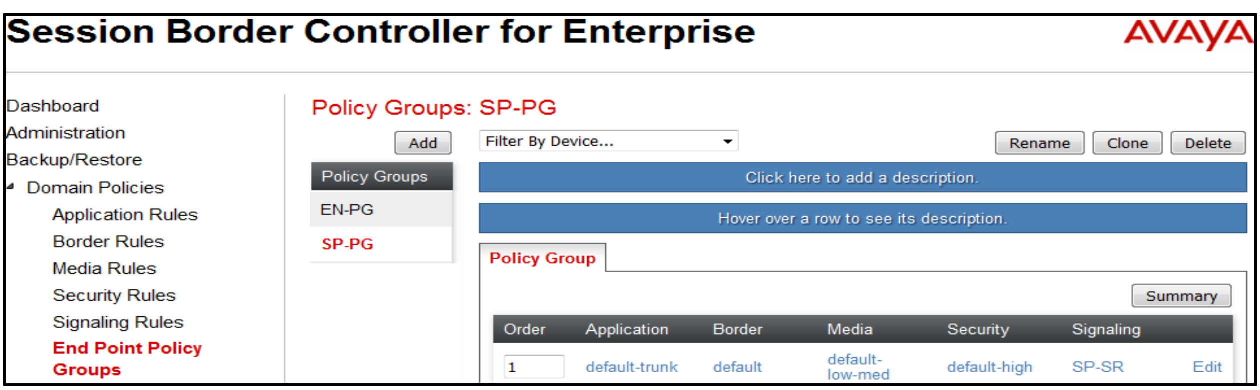
7.4.3. Endpoint Policy Groups

The rules created within the **Domain Policies** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section. Endpoint Policy Groups were created for SP and EN. To create a new policy group, navigate to **Domain Policies** → **Endpoint Policy Groups** and click on **Add**.

Endpoint Policy Group for SP

The following screen shows **SP-PG** created for SP:

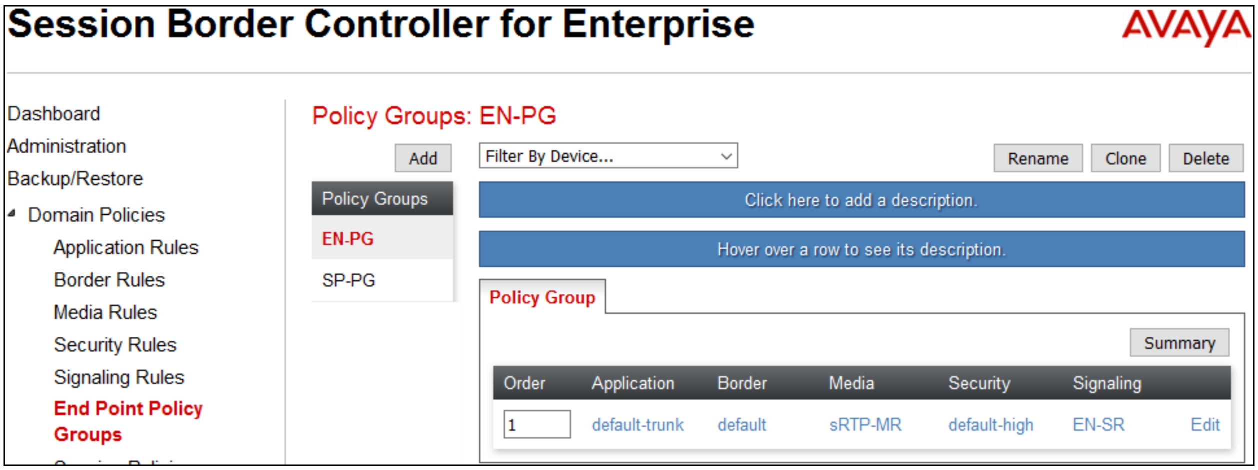
- Set Application Rule to ***default-trunk***.
- Set Border Rule to ***default***.
- Set Media Rule to ***default-low-med*** as created in **Section 7.4.1**.
- Set Security Rule to ***default-high***
- Set Signaling Rule to ***SP-SR*** as created in **Section 7.4.2**.



Endpoint Policy Group for EN

The following screen shows **EN-PG** created for EN:

- Set Application Rule to ***default-trunk***.
- Set Border Rule to ***default***.
- Set Media Rule to ***sRTP-MR*** as created in **Section 7.4.1**.
- Set Security Rule to ***default-high*.**
- Set Signaling Rule to ***EN-SR*** as created in **Section 7.4.2**.



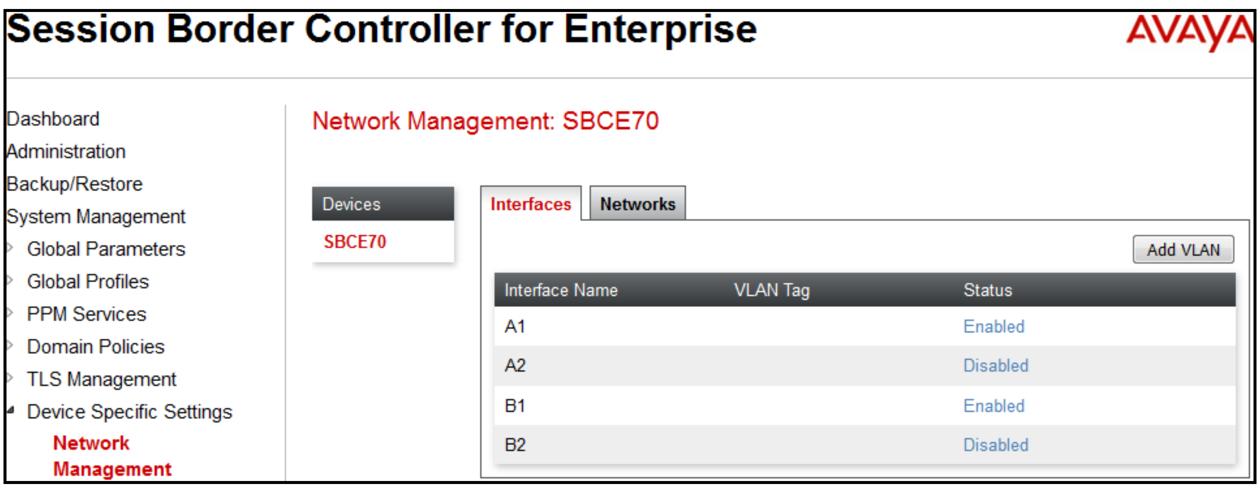
7.5. Device Specific Settings

Device Specific Settings allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

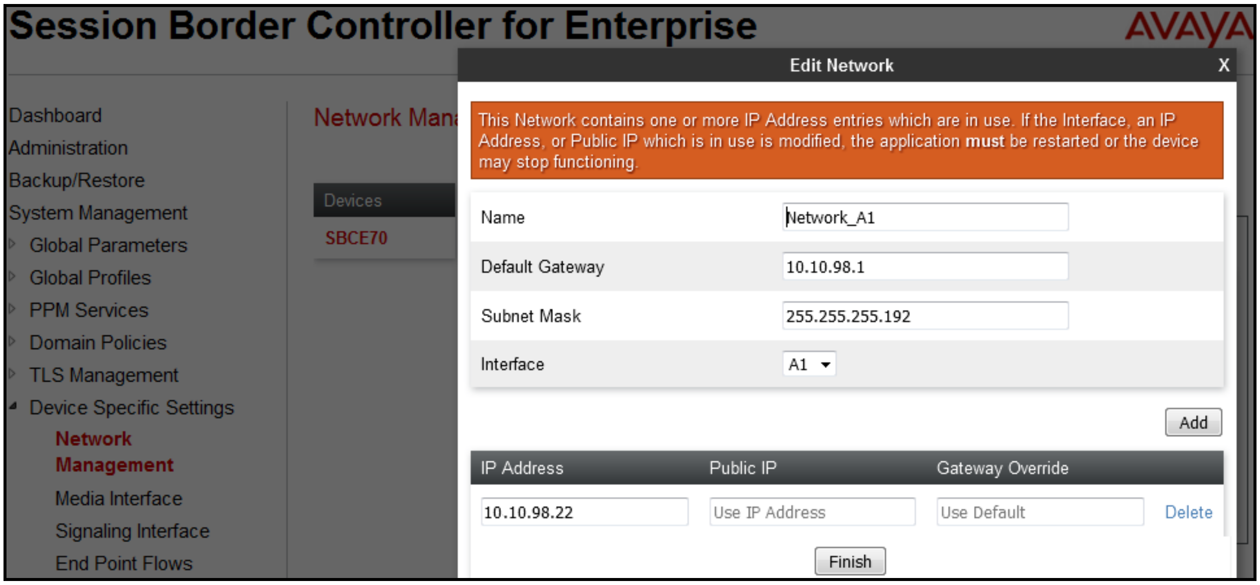
7.5.1. Network Management

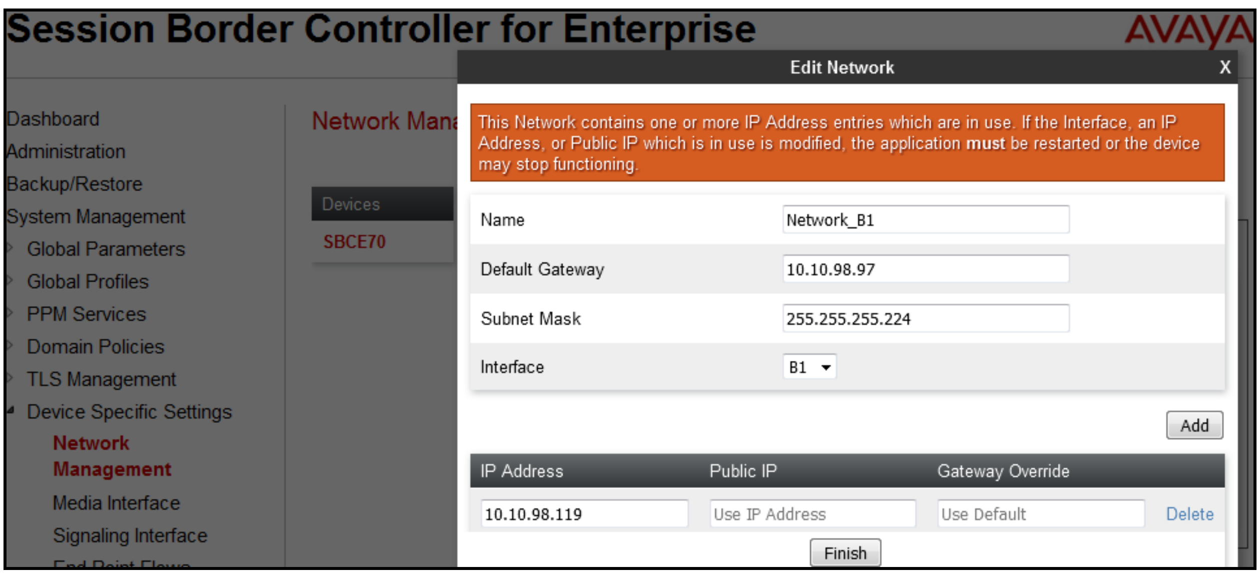
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was defined such as; device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the **Network Management** tab, which can be edited as needed to optimize device performance and network efficiency.

Enable the interfaces used to connect to the inside and outside networks on the **Interface** tab. The following screen shows Interface Names, **A1** and **B1** are **Enabled**. To enable an interface, click on its **Status** corresponding to the interface names.



Navigate to **Device Specific Settings → Network** and under the **Network Configuration** tab verify the IP addresses assigned to the interfaces. The following screens show the private interface is assigned to **A1** and the public interface is assigned to **B1** respectively.





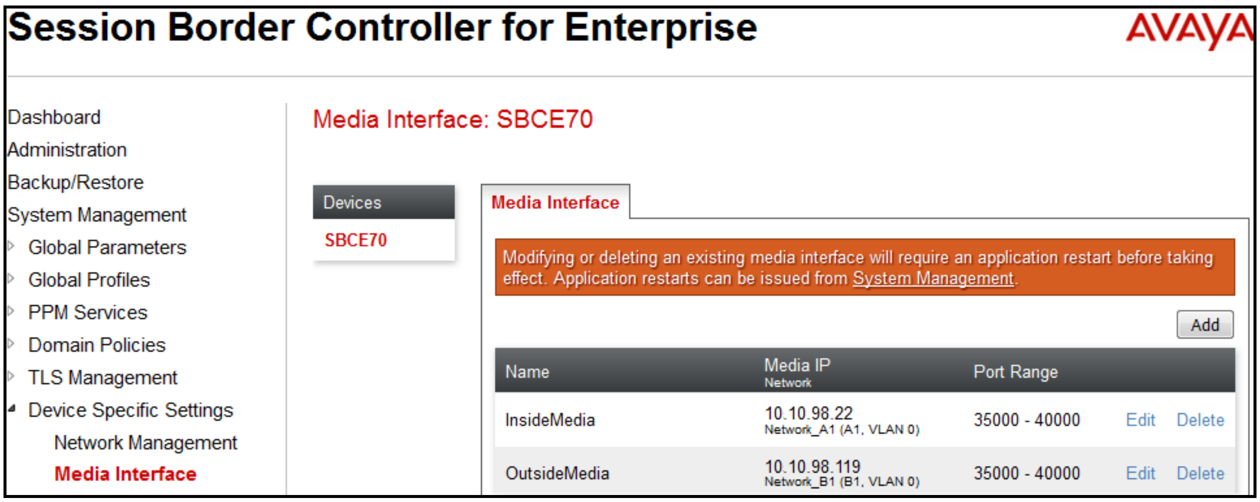
7.5.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open a connection for RTP on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**.

Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.



7.5.3. Signaling Interface

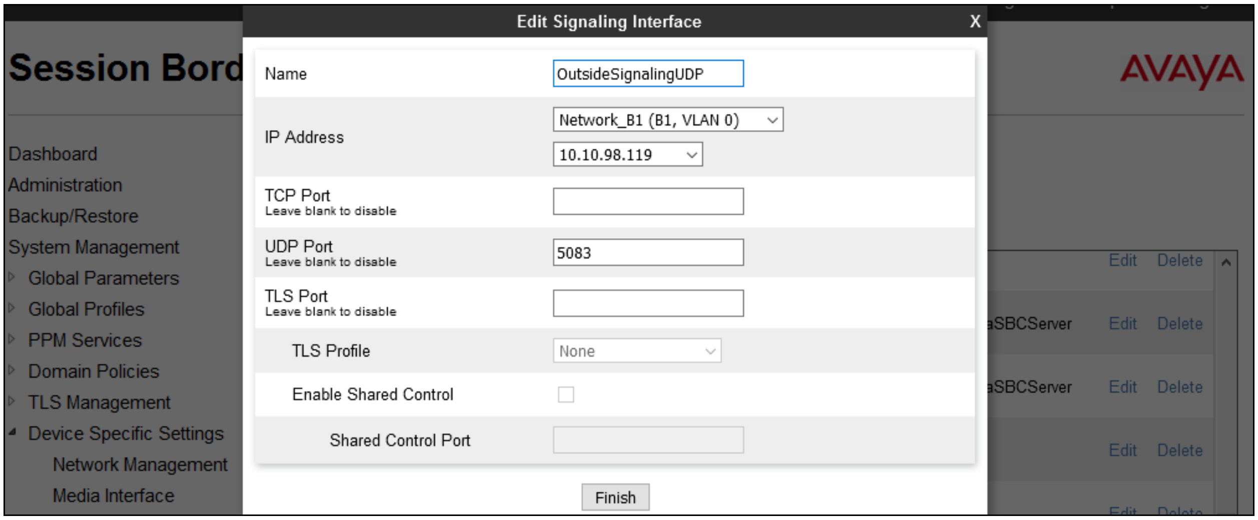
The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

To create a new Signaling Interface, navigate to **Device Specific → Settings → Signaling Interface** and click **Add**.

Separate Signaling Interfaces were created for both inside and outside interfaces.

Signaling Interface for SP

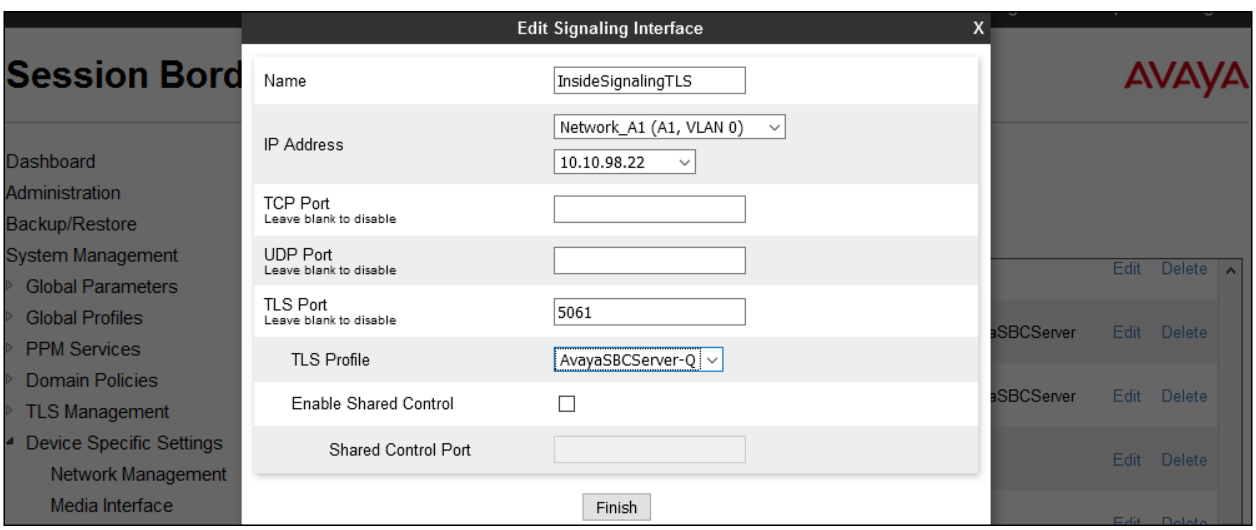
The outside interface to service provider is created with UDP/5083 as shown below.



Signaling Interface for EN

The inside to service provider interface is created with TLS/5061 as shown below.

- Enter descriptive name for **Name** field.
- Select **IP Address** from pull down menu defined as internal network interface **Section 7.5.1**.
- Specified ***5061*** for **TLS Port**. Then select **TLS profile** from pull down menu as defined in **Section 7.2.3**.
- Click **Finish**.



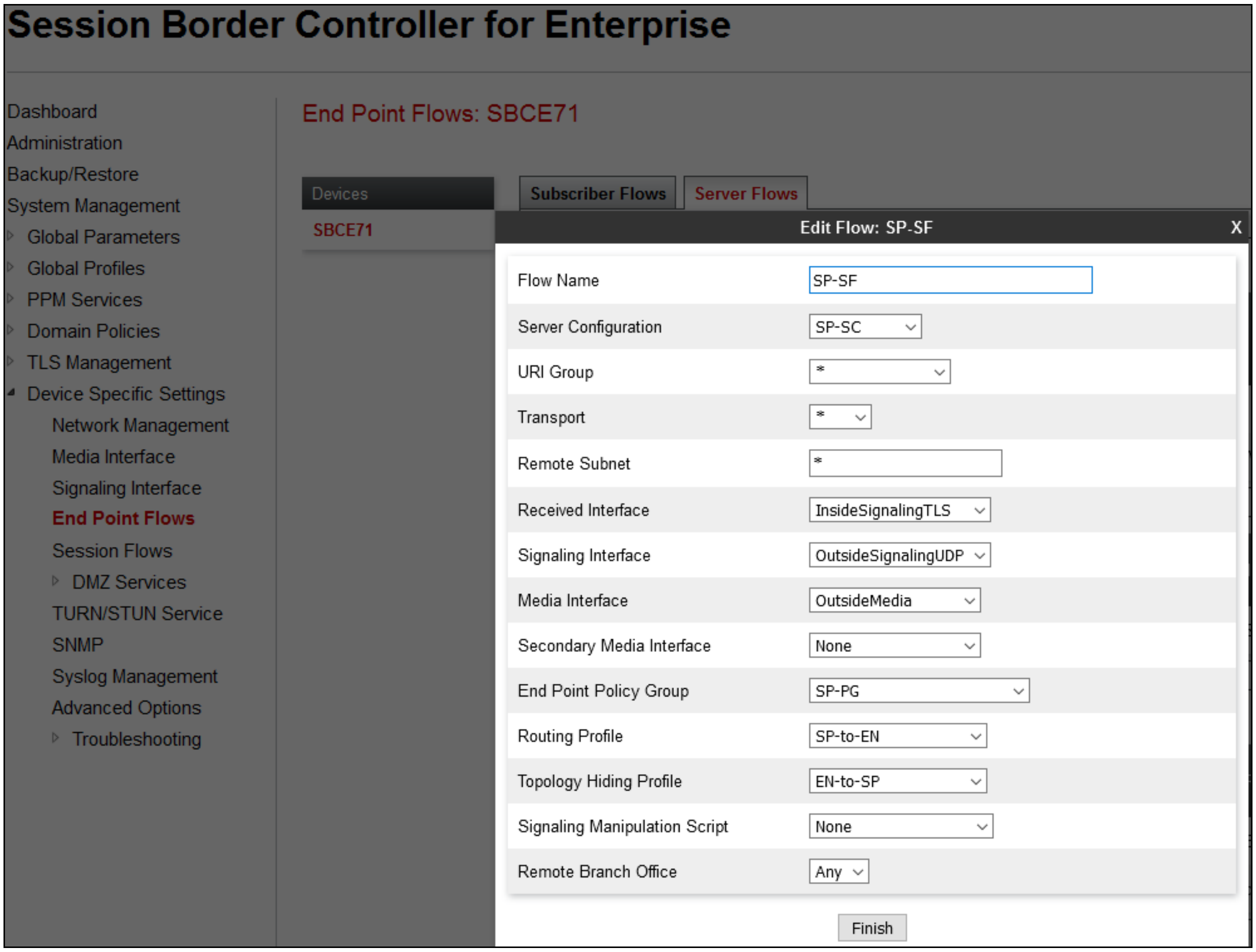
7.5.4. End Point Flows - Server Flow

When a packet is received by 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 a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screens illustrate the flow through the Avaya SBCE to secure a SIP Trunk call.

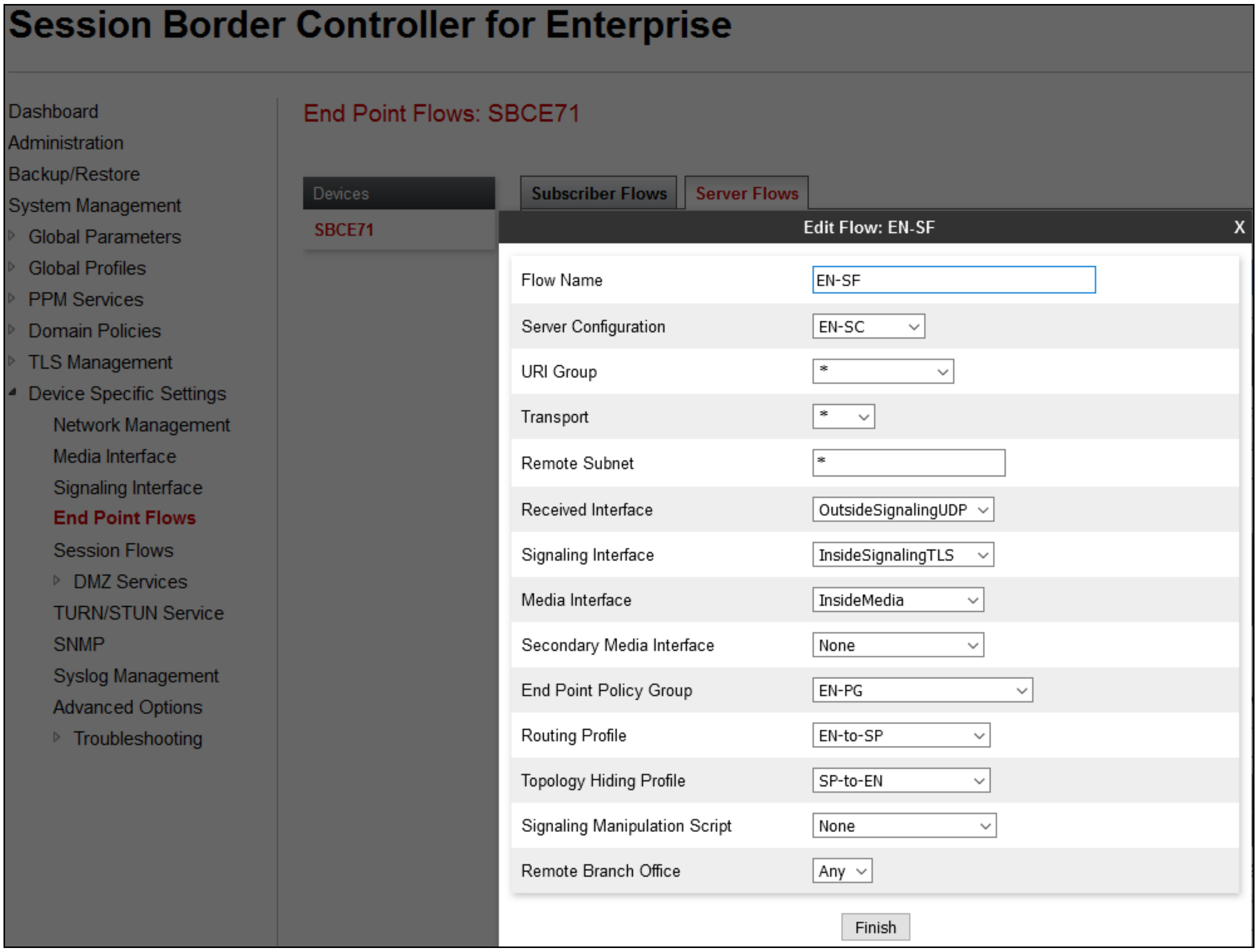
In the compliance testing, separate Server Flows were created for SP and EN. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select a Server Configuration created in **Section 7.3.4** to assign to the Flow.
- **URI Group**: Select the URI Group created in **Section 7.3.1** to assign to the Flow.
  Note: URI Group can be set to "*" to match all calls.
- **Received Interface**: Select the Signaling Interface created in **Section 7.5.3** that the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface**: Select the Signaling Interface created in **Section 7.5.3** used to communicate with the Server Configuration.
- **Media Interface**: Select the Media Interface created in **Section 7.5.2** used to communicate with the Server Configuration.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 7.4.3** to assign to the Server Configuration.
- **Routing Profile**: Select the Routing Profile created in **Section 7.3.2** that the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile**: Select the Topology-Hiding profile created in **Section 7.3.6** to apply to the Server Configuration.
- Click **Finish**.

The following screen shows the Server Flow **SP-SF** configured for SP.



Similarly, the following screen shows the Server Flow **EN-SF** configured for EN.



8. Liechtenstein Service Configuration

Liechtenstein is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Liechtenstein will provide the customer with the necessary information to configure the SIP connection from the enterprise to Liechtenstein. The information provided by Liechtenstein includes:

- IP address and port number used for signaling through security devices (if any).
- IP address and port number used for media through security devices (if any).
- Liechtenstein SIP domain. In the compliance testing, Liechtenstein preferred to use IP address as an URI-Host.
- CPE SIP domain. In the compliance testing, Liechtenstein preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers.

The sample configuration between Liechtenstein and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP trunk implemented on either Liechtenstein or enterprise side.

9. Verification and Troubleshooting

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.

9.1. Verification Steps

- Verify that endpoints at the enterprise site can place call to PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
- Verify that endpoints at the enterprise site can receive call from PSTN and that the call can remain active for more than 35 seconds. This time period is included satisfy SIP protocol timers.
- Verify that the user on PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. Protocol Traces

The following SIP headers are inspected using Wireshark trace analysis:

- Request-URI: verify the called party number and SIP domain.
- From: verify the calling party name and number.
- To: verify the called party name and number.
- P-Asserted-Identity: verify the calling party name and number.
- Privacy: verify the value “user” and/or “id” presents the private call scenario.

The following attributes in SIP message body are inspected using Wireshark trace analysis:

- Connection Information (c line): verify IP address of near end and far end endpoints.
- Time Description (t line): verify session timeout value of near end and far end endpoints.
- Media Description (m line): verify audio port, codec, DTMF event description.
- Media Attribute (a line): verify specific audio port, codec, ptime, send/ receive ability, DTMF event and fax attributes.

9.3. Troubleshooting:

9.3.1. The Avaya SBCE

Use Avaya SBCE trace tool, traceSBC to monitor the SIP signaling messages between Liechtenstein and the Avaya SBCE.

9.3.2. Communication Manager

- **list trace station** <extension number>. Traces call to and from a specific station.
- **list trace tac** <trunk access code number>. Trace call 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 group number>. Displays trunk group information.
- **status trunk** <trunk group number/channel number>. Displays signaling and media information for an active trunk channel.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.1 to Liechtenstein SIP Trunking Service. Liechtenstein SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Liechtenstein provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases were executed. Despite the observation seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The Liechtenstein SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.1.

11. References

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

[1] *What's New in Avaya Aura Release 7.0,* Release 7.0, 03-601818, Issue 1, August 2015.
[2] *Deploying Avaya Aura® System Manager*, Release 7.0, Issue 1, October 2015.
[3] *Administering Avaya Aura® System Manager for Release 7.0*, Issue 1, August 2015.
[4] *Administering Avaya Aura® Session Manager,* Release 7.0, Issue 1, August 2015.
[5] *Deploying Avaya Aura Communication Manager in Virtualized Environment*, Release7, Issue 1, August 2015.
[6] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.0, Issue 1, August 2015.
[7] *Deploying Avaya Session Border Controller for Enterprise,* Release 7.0, Issue 1, August 2015.
[8] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.0, Issue 1, August 2015.
[9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.
[10] *Deploying and Updating Avaya Aura Media Server Appliance, Release 7.7,* Issue 1, August 2015.
[11] *9600 Series IP Deskphones Overview and Specification*, Release 7.0, Issue 1, August 2015.
[12] *Installing and Maintaining Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.0, Issue 1, August 2015.
[13] *Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.0, Issue 2, August 2015.
[14] *Administering Avaya one-X® Communicator*, Release 6.2, April 2015.
[15] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0 Issue 1.0*
[16] *RFC 3261 SIP: Session Initiation Protocol,* http://www.ietf.org/
[17] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, http://www.ietf.org/
[18] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,* http://www.ietf.org/

Product documentation for Liechtenstein Networks' SIP Trunking Solution is available from Liechtenstein.

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.