Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.1 with Avaya SIP Trunking Service using TLS Transport – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking service on an enterprise solution consisting of Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.1 to interoperate with the Avaya SIP Trunking service using Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) on the private (enterprise) and the public (internet) sides.

The Avaya SIP Trunking service offer referenced within these Application Notes provides customers with PSTN access via a SIP trunk between the enterprise and the service provider network. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly as an alternative to legacy analog or digital trunks. The Avaya SIP Trunking service provides you with a cost effective and flexible way to connect your business to the outside world. It helps your business use the internet bandwidth you already pay for in a more flexible way.

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.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 8.1 (Session Manager), Avaya Aura® System Manager Release 8.1 (System Manager), Avaya Aura® Communication Manager Release 8.1 (Communication Manager), Avaya Aura® Experience Portal 7.2 (Experience Portal) and Avaya Session Border Controller for Enterprise 8.1 (Avaya SBCE) with the Avaya SIP Trunking service using Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) on the private (enterprise) and public (internet) sides. The Avaya SIP Trunking service referenced in this document provides secured encrypted communications for local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

The terms "Avaya", "Avaya network" or "service provider" will be used interchangeably throughout these Application Notes to represent the far-end/service provider side of the Avaya SIP Trunking service offering, handling calls to/from the PSTN across the SIP trunk. The terms "enterprise" or "Avaya enterprise" will be used interchangeably throughout these Application Notes to represent the Customer-Premises-Equipment site containing all the equipment for the Avaya SIP-enabled enterprise solution.

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Avaya network via a broadband secured connection to the public Internet.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this Application Notes included the enablement of supported encryption capabilities (TLS/SRTP) inside of the enterprise (private network side) and outside of the enterprise (public network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

2.1. Interoperability Compliance Testing

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

- Public DNS "SRV" record queries to establish the SIP trunk connections across multiple servers.
- SIP Trunk Registration (Dynamic Authentication).
- Successful TLS negotiation (handshake) with the service provider's network for the establishment of a secured SIP trunk connection across the public internet.
- Proper negotiation of various SRTP crypto-suites with the service provider.
- Response to SIP OPTIONS queries.
- Direct IP-to-IP Media (also known as "Shuffling") when applicable.

- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, digital, and analog telephones at the enterprise. All incoming calls from the PSTN were routed to the simulated enterprise across the SIP Trunk from the service provider's network.
- Outgoing PSTN calls from Avaya endpoints including SIP, H.323, digital and analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the simulated enterprise across the SIP trunk to the service provider's network.
- Inbound and outbound PSTN calls to/from Remote Workers using the Avaya IX™ Workplace Client for Windows SIP softphone.
- Outgoing calls to the PSTN were routed via the service provider's network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two-way speech-path. Testing was performed with codecs: G.722, G.711MU G.711A and G.729.
- No matching codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833:
    - Outbound call to PSTN application requiring DTMF (e.g., an IVR or voice mail system).
    - Inbound call from PSTN to Avaya CPE application requiring DTMF (e.g., Aura® Messaging, Experience Portal, Avaya vector digit collection steps.
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold).
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agents and extensions.
- Call and two-way talk path establishment between callers and Communication Manager agents and extensions following redirection from Experience Portal.
- Routing inbound vector call to call center agent queues.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- T.38 fax.
- SIP REFER method for call re-direction from the enterprise to the PSTN.

Note – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes. Consult reference [**11**] in the **References** section for additional information on this topic.

Items that are supported that were not tested for not being available at the time of testing includes the following:

- 0, 0+10 digits and 411 calls were not tested.

2.2. Test Results

Interoperability testing of the Avaya SIP Trunking service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **SIP Trunk registrations –** After each successful SIP Trunk registration attempt the service provider would send a "484 Address Incomplete" message response to the enterprise. This behaviour did not have any service impact, registrations were successful, it's being mentioned here simply as an observation.
- **OPTIONS –** The service provider does not send OPTIONS messages to the enterprise network, but it does respond to OPTIONS messages it receives from the enterprise, this was enough to maintain the SIP trunk connection in service.
- **Music on hold** – With Communication Manager configured to play music any time calls were placed on-hold at the enterprise; music was not played to PSTN users on calls from the PSTN to the enterprise (inbound calls). The issue was resolved at the Avaya SBCE by removing the "sendonly" message Communication Manager includes in the SDP of re-INVITE messages sent to the service provider (**Sections 8.8** and **14**).
- **TLS/SRTP used within the enterprise** – When TLS/SRTP is used within the enterprise; the SIP headers include the SIPS URI scheme for Secure SIP. The Avaya SBCE converts these header schemes from SIPS to SIP when it sends the SIP message toward the service provider's network. However, for call forward and EC500 calls, the Avaya SBCE was not changing the Diversion header scheme as expected. This anomaly is currently under investigation by the Avaya SBCE team. A workaround is to include a SigMa script for the Service Provider Server Configuration Profile on the Avaya SBCE to convert "sips" to "sip" in the Diversion header (**Sections 8.8** and **14**). Sending the Diversion header scheme with the SIPS URI scheme toward the service provider's network did not have any service impact, calls were successful, the conversion from "sips" to "sip" was done for completeness.
- **Removal of unwanted xml element information from the SDP in SIP messages sent to the service provider** – A Signaling Manipulation script (SigMa) was added to the Avaya SBCE to remove unwanted xml element information from the SDP in SIP UPDATE messages sent to the service provider. (**Sections 8.8** and **14**).
- **Avaya Experience Portal** – Inbound calls from the PSTN to Experience Portal that were re-directed back out to the PSTN by Experience Portal (during blind or attended transfers) did not contained the "+" preceding the "1" in the "To" and "Request-Line-

URI" headers. This is required in order to comply with the E.164 numbering format. This issue was resolved in the Avaya SBCE by adding a SigMa script to add the "+" to the number in the "To" and "Request-Line-URI" headers of calls being re-directed back out to the PSTN by Experience Portal (**Section 8.8** and **14**). Also, Experience Portal only allows digits when entering the DID number in the "Called Number" field, as shown in **Section 6.5**, thus the "+" preceding the "1" needed to comply with the E.164 numbering format of the inbound calls could not be added. The work around is to add an Adaptation in Session Manager to remove the "+" from the Request-Line-URI header of SIP INVITE messages destined to Experience Portal (**Section 7.4**), thus matching the DID number entry defined in the "Called Number" field.

- **SIP header optimization** – There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider's network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector, AV-Global-Session-ID and P-Location (Refer to **Section 7.4**). To help reduce the packet size further, the Avaya SBCE can remove the "*gsid*" and "*epv"* parameters that may be included within the Contact header by applying a Sigma script to the service provider server configuration. Refer to **Section 8.8** and **14**.

2.3. Support

For information on Avaya SIP Trunking service go to: https://www.avaya.com/en/documents/fs-sip-uc8179en.pdf

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

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Avaya SIP Trunking service through the public Internet.

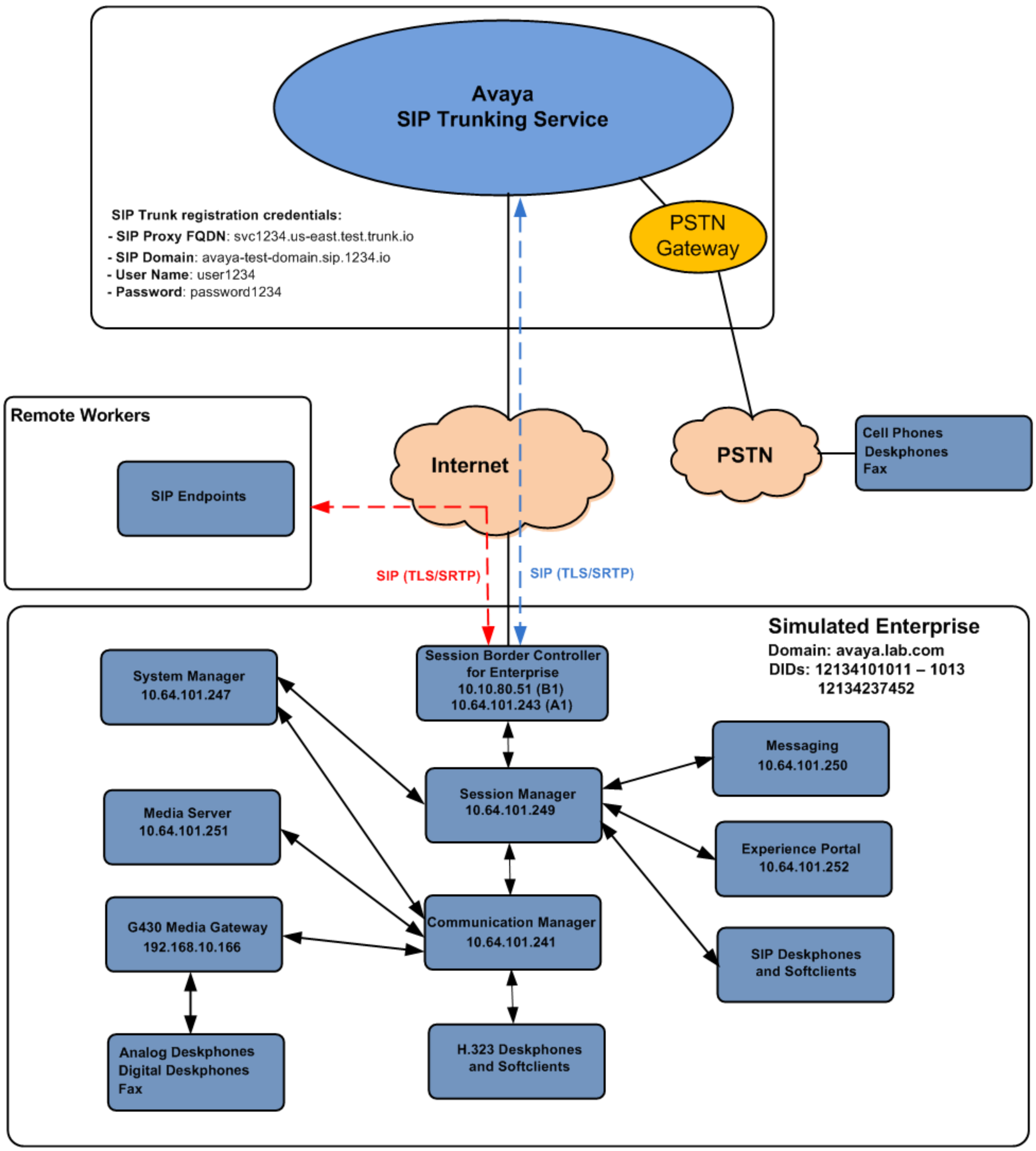


Figure 1: Avaya SIP Enterprise Solution connected to Avaya SIP Trunking service

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya Aura® Experience Portal.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya J179 IP Deskphones (H.323).
- Avaya J129 IP Deskphones (SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya IX™ Workplace Client for Windows (SIP).
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya IX™ Workplace Client for Windows (SIP). For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) were used on the Avaya IX™ Workplace Client for Windows (SIP). Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult reference [**11**] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (Communication Manager or Experience Portal) and on which link to send the call.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager.

Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Service Provider's network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

As part of the Avaya Aura® version 8.1 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Sever (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G430 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the **References** section.

Avaya Aura® System Manager provides a common administration interface for centralized management of Session Manager and Communication Manager. Avaya Aura® Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the Avaya SIP Trunking service, they are not included in these Application Notes.

Avaya Aura® Experience Portal was also used during the compliance test to verify various SIP call flow scenarios with the Avaya SIP Trunking service.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Enterprise	
Avaya Aura® Communication Manager	8.1.2.1.0 (01.0.890.0-26095)
Avaya Aura® Session Manager	8.1.2.0 (8.1.2.0.812039)
Avaya Aura® System Manager	8.1.2.0 Build No. 8.1.0.0.733078 Software Update Rev. No. 8.1.2.0.0611240
Avaya Session Border Controller for Enterprise	ASBCE 8.1.0 8.1.0.0-14-18490
Avaya Session Border Controller for Enterprise patch	sbce-8.1.0.0-14-19116-hotfix-06242020.tar.gz
Avaya Aura® Messaging	7.1 Service Pack 2 (MSG-01.0.532.0-002_0204)
Avaya Aura® Media Server	8.0.2.43 Service Pack 2
Avaya G430 Media Gateway	g430_sw_41_24_0
Avaya Aura® Experience Portal	7.2.2.0.2118
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.8304
Avaya J179 IP Deskphones (H.323)	Version 6.8304
Avaya J129 IP Deskphones (SIP)	4.0.5.0.10
Avaya one-X® Communicator (H.323, SIP)	6.2.14.6-SP14
Avaya IX™ Workplace Client for Windows (SIP)	3.8.4.10.2
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A

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

Note – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.0.0) platforms. Consult the installation documentation on the **References** section for more information.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the Avaya SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and the Avaya Media Server has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens capture will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

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 example shows that **40000** licenses are available and **120** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

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

IP PORT CAPACITIES                                        USED
                 Maximum Administered H.323 Trunks: 12000      0
       Maximum Concurrently Registered IP Stations: 18000      2
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations: 18000      0
          Maximum Concurrently Registered IP eCons:  414       0
           Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:  41000     0
               Maximum Video Capable IP Softphones:  18000     6
                   Maximum Administered SIP Trunks: 40000    120
  Max Administered Ad-hoc Video Conferencing Ports: 24000      0
   Max Number of DS1 Boards with Echo Cancellation: 999    0
```

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to ***none***.

```
change system-parameters features                               Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? all
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of ***restricted*** 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:
          International Access Code:

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**proc**r) and the Session Manager security module (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASBCE_A1            10.64.101.243
SM                  10.64.101.249
default             0.0.0.0
media_server        10.64.101.251
procr               10.64.101.241
procr6              ::

( 6  of 6    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. The service provider supports audio codecs ***G.722-64K***, ***G.711MU, G.711A*** and ***G.729***.

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

                          IP MEDIA PARAMETERS
    Codec Set: 2

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722-64K                   2        20
 2: G.711MU          n          2        20
 3: G.711A           n          2        20
 4: G.729            n          2        20
 5:
 6:
 7:

     Media Encryption                   Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
 5:
```

On **Page 2**, set the **Fax Mode** to ***t.38-standard*** and **ECM** to ***y***.

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

                          IP MEDIA PARAMETERS

                              Allow Direct-IP Multimedia? n



                                             Redun-                       Packet
                          Mode               dancy                        Size(ms)
    FAX                   t.38-standard      0     ECM: y
    Modem                 off                0
    TDD/TTY               US                 3
    H.323 Clear-channel   n                  0
    SIP 64K Data          n                  0                            20


Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

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

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2       NR Group: 2
Location: 1       Authoritative Domain: avaya.lab.com
    Name: SP Region              Stub Network Region: n
MEDIA PARAMETERS                 Intra-region IP-IP Direct Audio: yes
      Codec Set: 2               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                       IP Audio Hairpinning? n
   UDP Port Max: 3349
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set ***2*** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 2                                      Page   4 of  20

 Source Region: 2     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    2     y    NoLimit                                             n       t
 2    2                                                                all
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, ***tls*** was used.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to ***SM*** once Communication Manager detects its peer is a Session Manager.

Note: Once the **Peer-Server** field is updated to ***SM***, the system changes the default values of the following fields, setting them to display–only:

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to ***y***.
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to ***n***.

- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as 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 **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5071***.
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

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

                          IP MEDIA PARAMETERS
    Codec Set: 2
change 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                     Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5071                Far-end Listen Port: 5071
                                        Far-end Network Region: 2

Far-end Domain: avaya.lab.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? n                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 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 **Service Type** field to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
change trunk-group 2                                            Page   1 of   4
                                TRUNK GROUP

Group Number: 2                  Group Type: sip           CDR Reports: y
  Group Name: Service Provider           COR: 1        TN: 1        TAC: 602
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. The default value of ***600*** seconds was used.

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

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y


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




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

On **Page 3**:

- Set the **Numbering Format** field to ***public***. This field specifies the format of the calling party number (CPN) sent to the far-end. When ***public*** format is used, Communication Manager automatically inserts a "+" sign, preceding the numbers in the "From", "Contact" and "P-Asserted Identity" (PAI) headers. To keep uniformity with the format used by the service provider, the **Numbering Format** was set to ***public*** and the **Numbering Format** in the route pattern was set to ***pub-unk*** (see **Section 5.10**).
- Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

```
change trunk-group 2                                            Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  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**:

- Set the **Network Call Redirection** field to ***y***. With this setting, Communication Manager will use the SIP REFER method for the redirection of PSTN calls that are transferred back to the SIP trunk.
- Set the **Send Diversion Header** field to ***y*** and **Support Request History** to ***n***.
- Set the **Telephone Event Payload Type** to **101**.
- Verify that **Identity for Calling Party Display** is set to ***P-Asserted-Identity***.
- Default values were used for all other fields.

```
change trunk-group 2                                            Page   4 of   4
                              PROTOCOL VARIATIONS

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

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

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (**Section 5.7**), 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. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers assigned by the service provider are shown. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

```
change public-unknown-numbering 1                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                              Total
Ext Ext               Trk       CPN            CPN
Len Code              Grp(s)    Prefix         Len
                                                  Total Administered: 5
 4  3                                          4     Maximum Entries: 9999
 4  5                                          4
 4  3041              2         12134101011    11 Note: If an entry applies to
 4  3042              2         12134101012    11 a SIP connection to Avaya
 4  3047              2         12134101013    11 Aura(R) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.

                                                  Communication Manager
                                                  automatically inserts
                                                  a '+' digit in this case.
```

5.9. Inbound Routing

In general, the "incoming call handling treatment" form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number received from the PSTN is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID. Note the DID number is preceded by **+1** since its required in order to comply with the E.164 numbering format.

```
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    12 +12134101011     12  3041
 public-ntwrk    12 +12134101012     12  3042
 public-ntwrk    12 +12134101013     12  3047
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
 public-ntwrk
```

5.10. Outbound Routing

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

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

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
 0             13 udp
 1              4  dac
 2              4  ext
 3              4  ext
 4              4  udp
 5              4  ext
 6              3  dac
 7              4  ext
 8              1  fac
 9              1  fac
 *              3  dac
 #              2  dac
```

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

```
change feature-access-codes                                    Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: #7
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                Automatic Callback Activation:         Deactivation:
Call Forwarding Activation Busy/DA:        All:         Deactivation:
   Call Forwarding Enhanced Status:        Act:         Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
           Conditional Call Extend Activation:         Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2, which contains the SIP trunk group to the service provider.

```
change ars analysis 1786                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    1786                 11   11    2        fnpa         n
    179                  11   11    deny     fnpa         n
    180                  11   11    deny     fnpa         n
    1800                 11   11    2        fnpa         n
    1800555              11   11    deny     fnpa         n
    1809                 11   11    2        hnpa         n
    181                  11   11    deny     fnpa         n
    182                  11   11    deny     fnpa         n
    183                  11   11    deny     fnpa         n
    184                  11   11    deny     fnpa         n
    185                  11   11    deny     fnpa         n
    186                  11   11    deny     fnpa         n
    187                  11   11    deny     fnpa         n
    188                  11   11    deny     fnpa         n
    1880                 11   11    2        hnpa         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 in the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider.
- **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.
- In the **Pfx mrk** column, enter **1** to ensure a 1 + 10 digits are sent to the service provider for FNPA calls.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) in front of the number dialed to convert it to an E.164 formatted number.
- **Numbering Format**: Set to ***pub-unk***. All calls using this route pattern will use the public numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

```
change route-pattern 2                                          Page   1 of   4
                    Pattern Number: 2       Pattern Name: Serv. Provider
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

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

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

Note – Service numbers, e.g., x11, 1411, 5551212, etc. were not tested (**Section 2.1**). If access to service numbers needs to be added at a later date, route patterns for Non-E.164 numbers should be used, e.g., x11, 1411, 5551212. For service numbers do not add the "**P**" to insert the plus (+) sign. Also, dial patterns for Non-E.164 numbers should be added, refer to **Section 7.8**.

Note - Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.

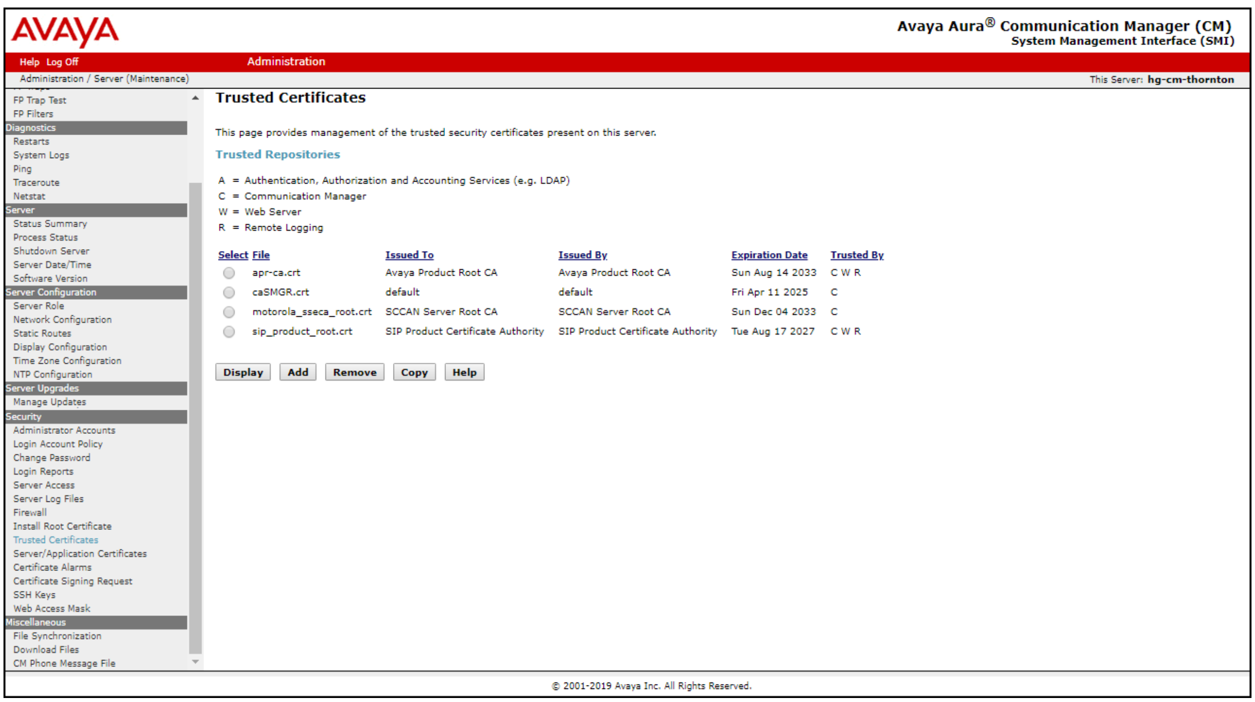
5.11. Verify TLS Certificates – Communication Manager

Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

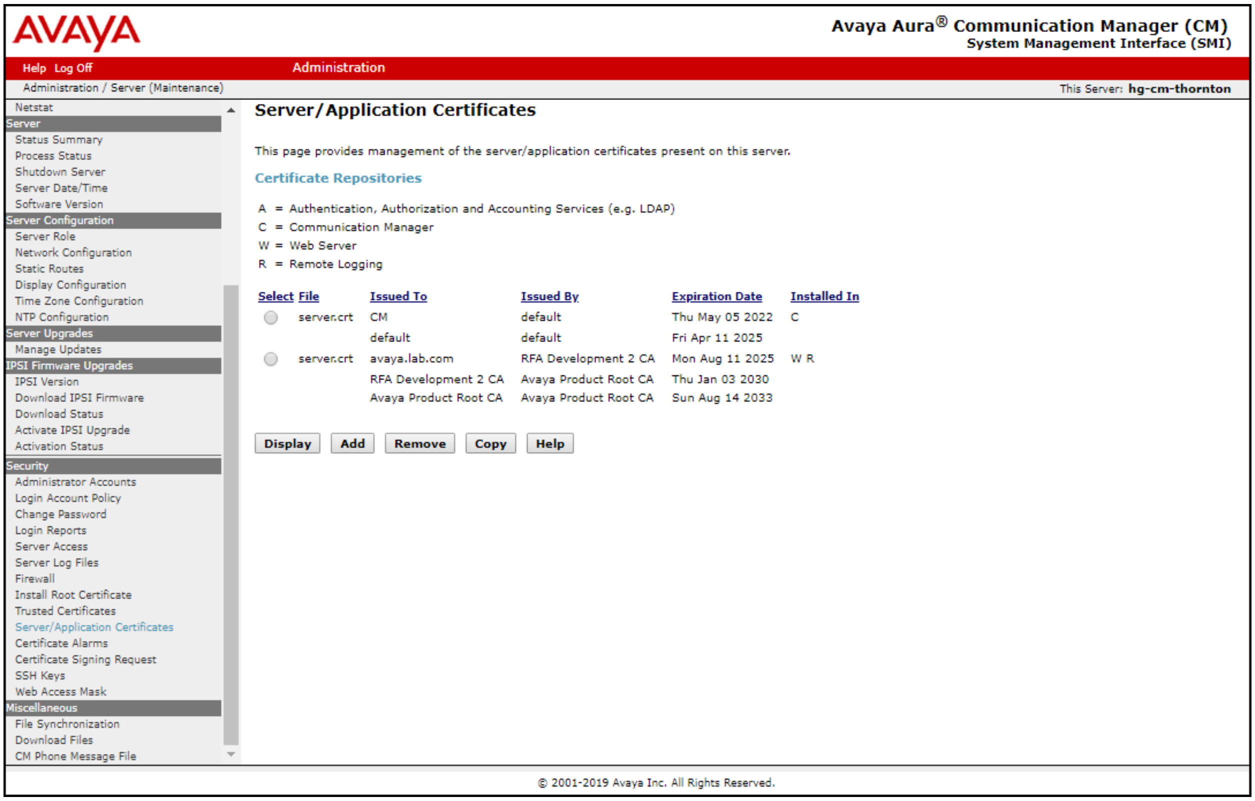
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. Follow the steps below to verify the certificates used by Communication Manager.

Step 1 - From a web browser, type in "https://<ip-address>", where "<ip-address>" is the IP address or FQDN of Communication Manager. Follow the prompted steps to enter appropriate **Logon ID** and **Password** credentials to log in (not shown).

Step 2 - Click on **Administration** at the top of the page and select **Server (Maintenance)** (not shown). Click on **Security → Trusted Certificates** and verify the System Manager Root CA certificate is present in the Communication Manager trusted repository.



Step 3 - Click on **Security → Server/Application Certificates** and verify the identity certificate signed by the System Manager CA is present in the Communication Manager certificate repository.



6. Configure Avaya Aura® Experience Portal

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

6.1. Background

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

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

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

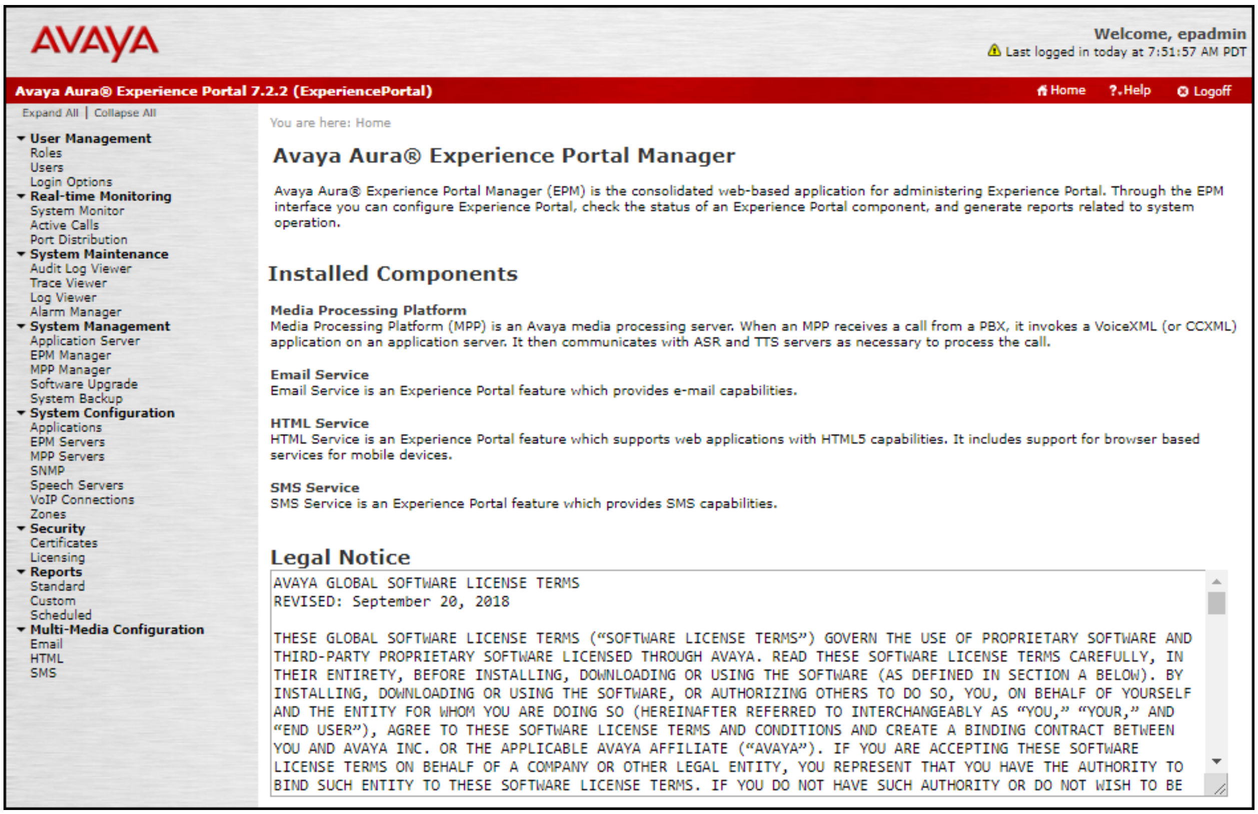
[1] An application may be configured with "inbound default" as the called number, to process all inbound calls that do not match any other application references.

6.2. Logging in and Licensing

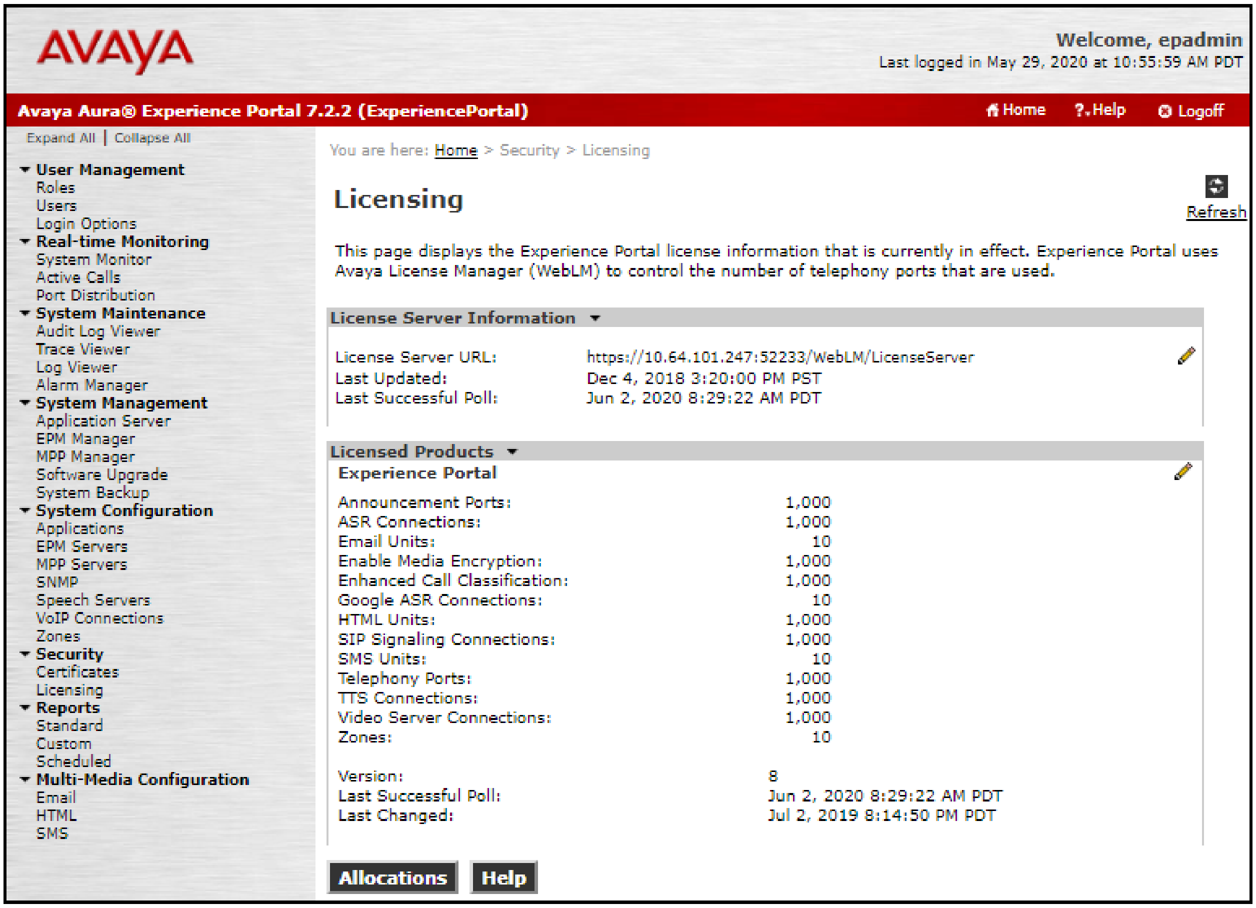
This section describes the steps on Experience Portal for administering a SIP connection to the Session Manager.

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

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



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

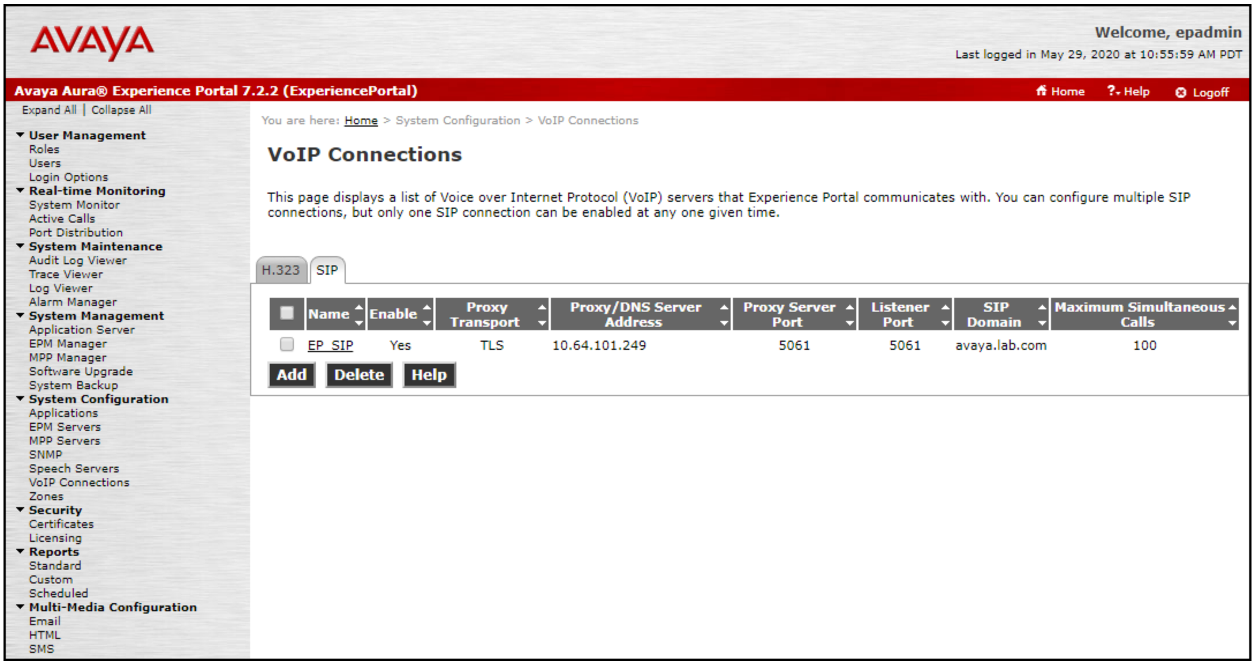


6.3. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager (**Sections 7.5 and 7.6**).

Step 1 - In the left pane, navigate to **System Configuration→VoIP Connections**. On the **VoIP Connections** page, select the **SIP** tab and click **Add** to add a SIP trunk.

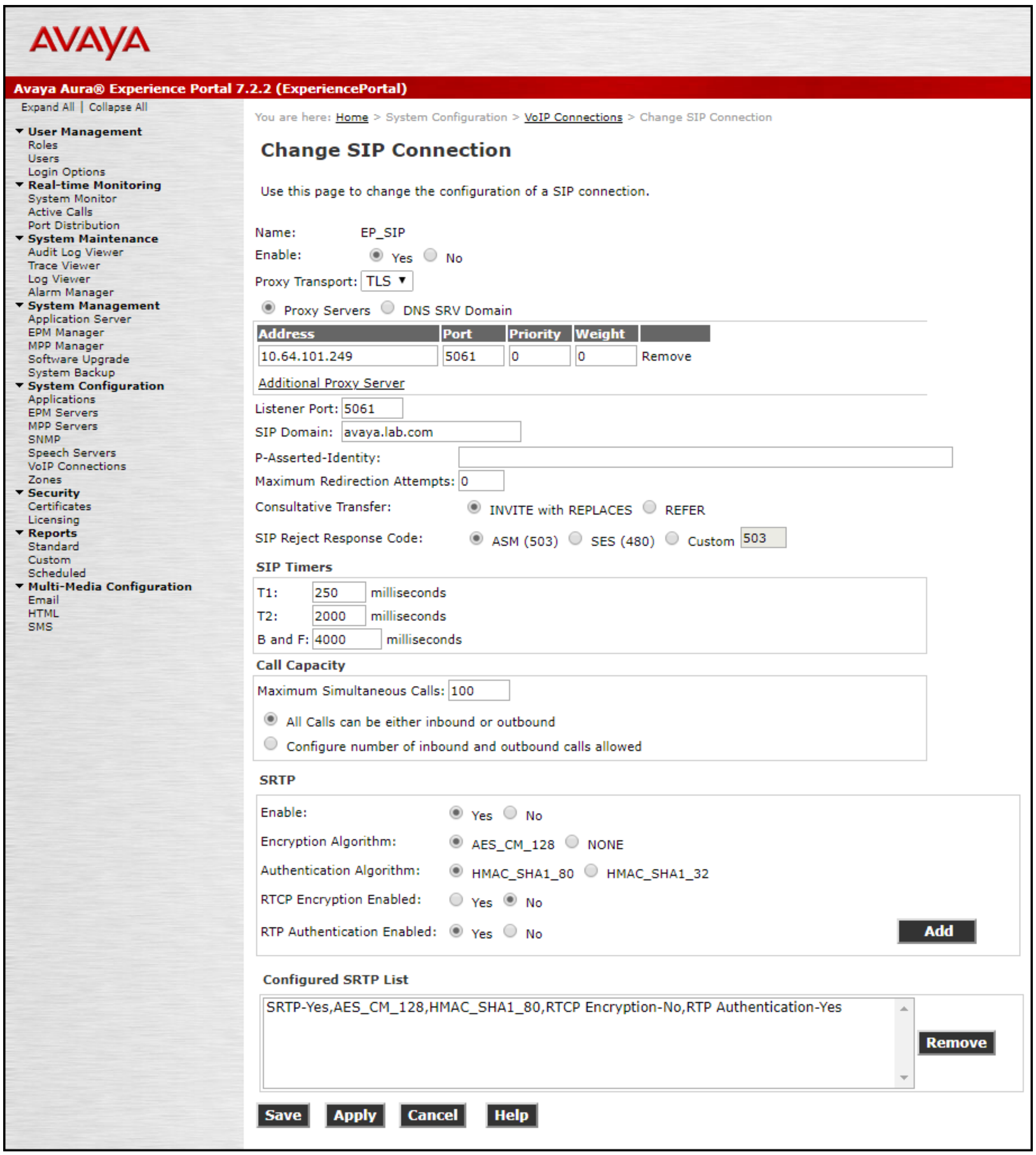
Note – Only ***one*** SIP trunk can be active at any given time on Experience Portal.



Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **EP_SIP**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address**: **10.64.101.249** (the IP address of the Session Manager signaling interface defined in **Section 7.5**).
  - **Port**: **5061**
  - **Priority**: **0** (default)
  - **Weight**: **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **avaya.lab.com** (see **Section 7.2)**.
- **Consultative Transfer** – Select **INVITE with REPLACES**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **100** was used.

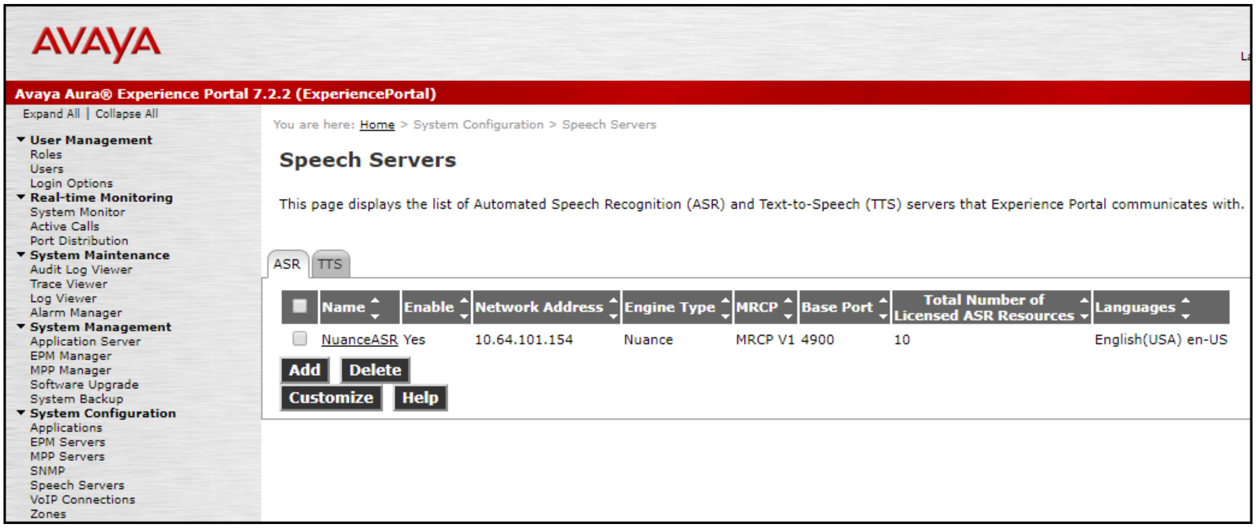
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable**: **Yes**
- **Encryption Algorithm**: **AES_CM_128**
- **Authentication Algorithm**: **HMAC_SHA1_80**
- **RTCP Encryption Enabled**: **No**
- **RTP Authentication Enabled**: **Yes**
- Click on **Add** to add SRTP settings to the **Configured SRTP List**
- Use default values for all other fields.
- Click **Save**.



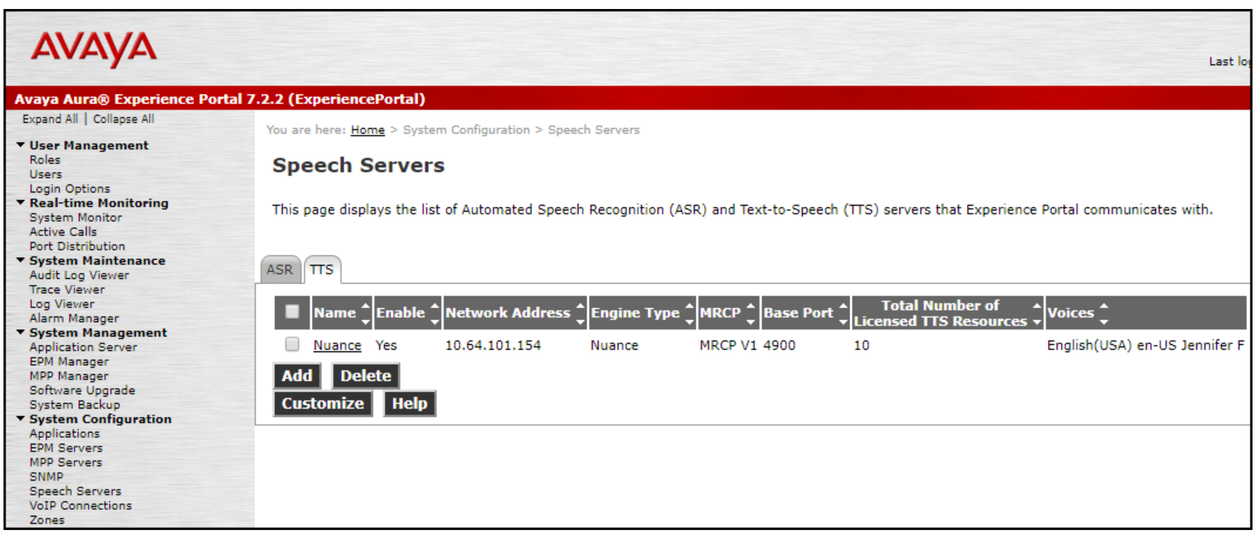
6.4. Speech Servers

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

ASR speech server:



TTS speech server:

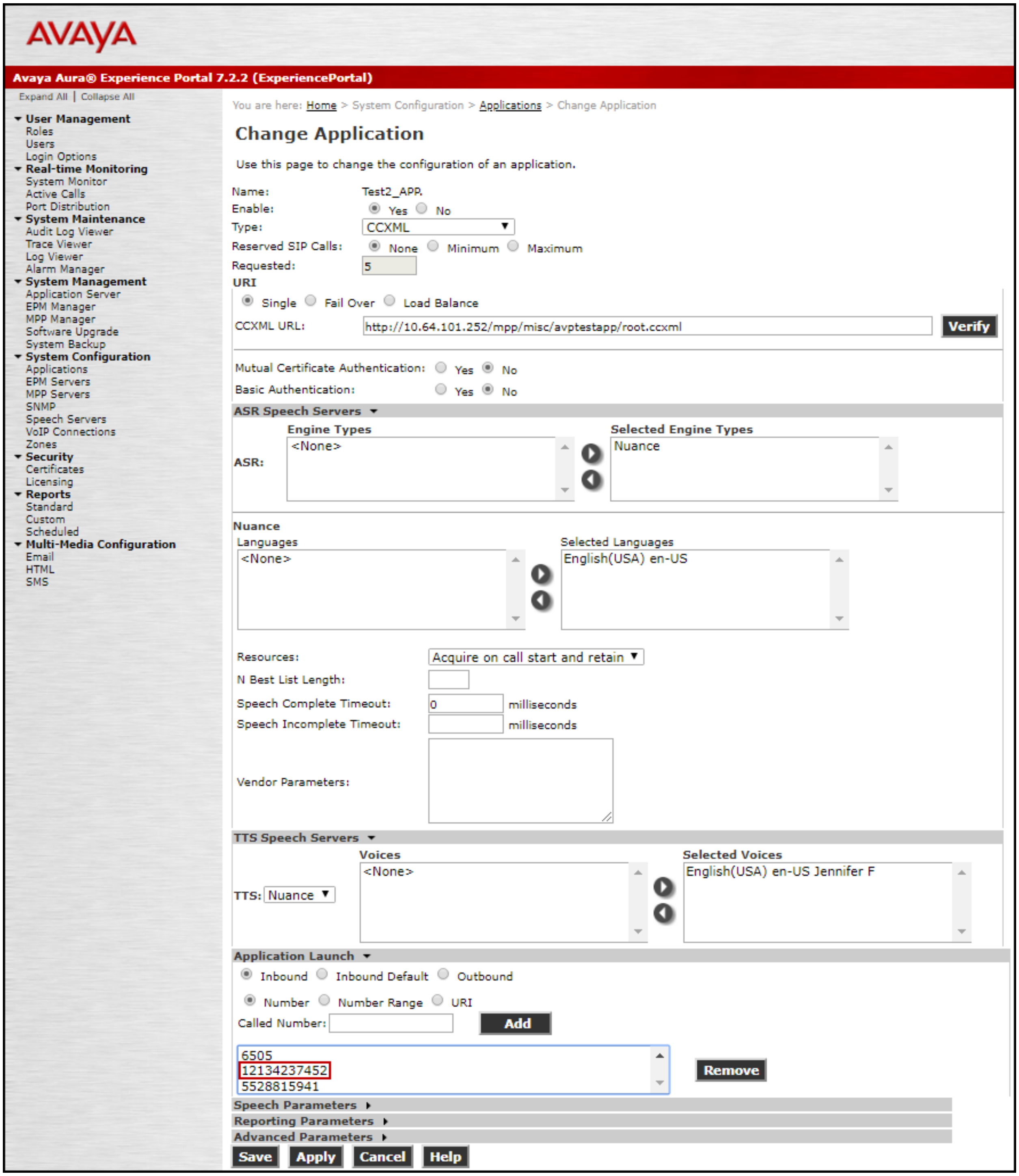


6.5. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.64.101.252.

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

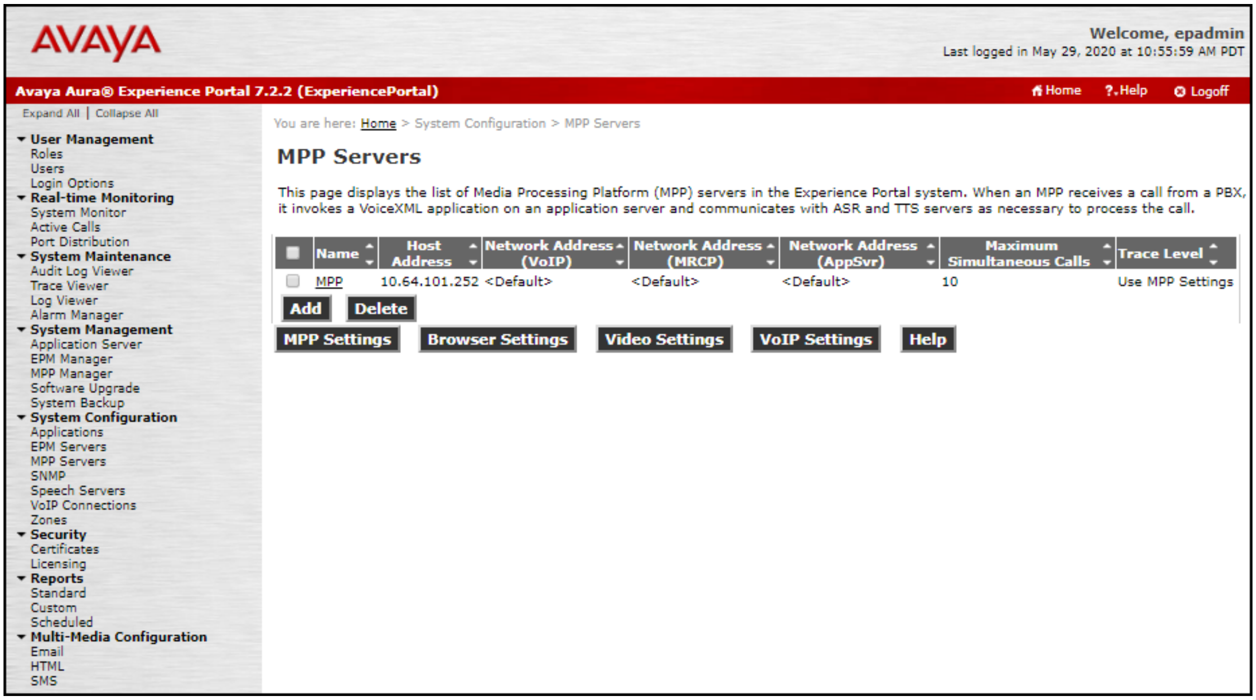
- **Name** – Set to a descriptive name (e.g., **Test2_APP**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type.
- **VoiceXML** and/or **CCXML URL** – Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Experience Portal test application on a single server is referenced.
- **Speech Servers ASR** and **TTS** – Select the appropriate ASR and/or TTS servers as necessary.
- **Application Launch** – Set to **Inbound**.
- **Called Number** – Enter the number to match against an inbound SIP INVITE message and click **Add**. In the sample configuration illustrated in these Application Notes, the dialed DID number **12134237452** provided by the service provider was used. Inbound calls with this called party number will be handled by the application defined in this section. Note that Experience Portal only allows numbers when entering the DID number in the "Called Number" field, thus the "+" preceding the "1" to comply with the E.164 numbering format could not be added. The work around is to add an Adaptation in Session Manager to remove the "+" from the Request-Line-URI header of SIP INVITE messages destined to Experience Portal (**Section 7.4**).


AVAYA
Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)
Expand All | Collapse All
User Management
Roles
Users
Login Options
Real-time Monitoring
System Monitor
Active Calls
Port Distribution
System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager
System Management
Application Server
EPM Manager
MPP Manager
Software Upgrade
System Backup
System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones
Security
Certificates
Licensing
Reports
Standard
Custom
Scheduled
Multi-Media Configuration
Email
HTML
SMS
You are here: Home > System Configuration > Applications > Change Application
Change Application
Use this page to change the configuration of an application.
Name: Test2_APP
Enable: Yes No
Type: CCXML
Reserved SIP Calls: None Minimum Maximum
Requested: 5
URI
Single Fail Over Load Balance
CCXML URL: http://10.64.101.252/mpp/misc/avptestapp/root.ccxml
Verify
Mutual Certificate Authentication: Yes No
Basic Authentication: Yes No
ASR Speech Servers
Engine Types
Selected Engine Types
ASR:
<None>
Nuance
Nuance
Languages
Selected Languages
<None>
English(USA) en-US
Resources: Acquire on call start and retain
N Best List Length:
Speech Complete Timeout: 0 milliseconds
Speech Incomplete Timeout: milliseconds
Vendor Parameters:
TTS Speech Servers
Voices
Selected Voices
TTS: Nuance
<None>
English(USA) en-US Jennifer F
Application Launch
Inbound Inbound Default Outbound
Number Number Range URI
Called Number:
Add
6505
12134237452
5528815941
Remove
Speech Parameters
Reporting Parameters
Advanced Parameters
Save
Apply
Cancel
Help

6.6. MPP Servers and VoIP Settings

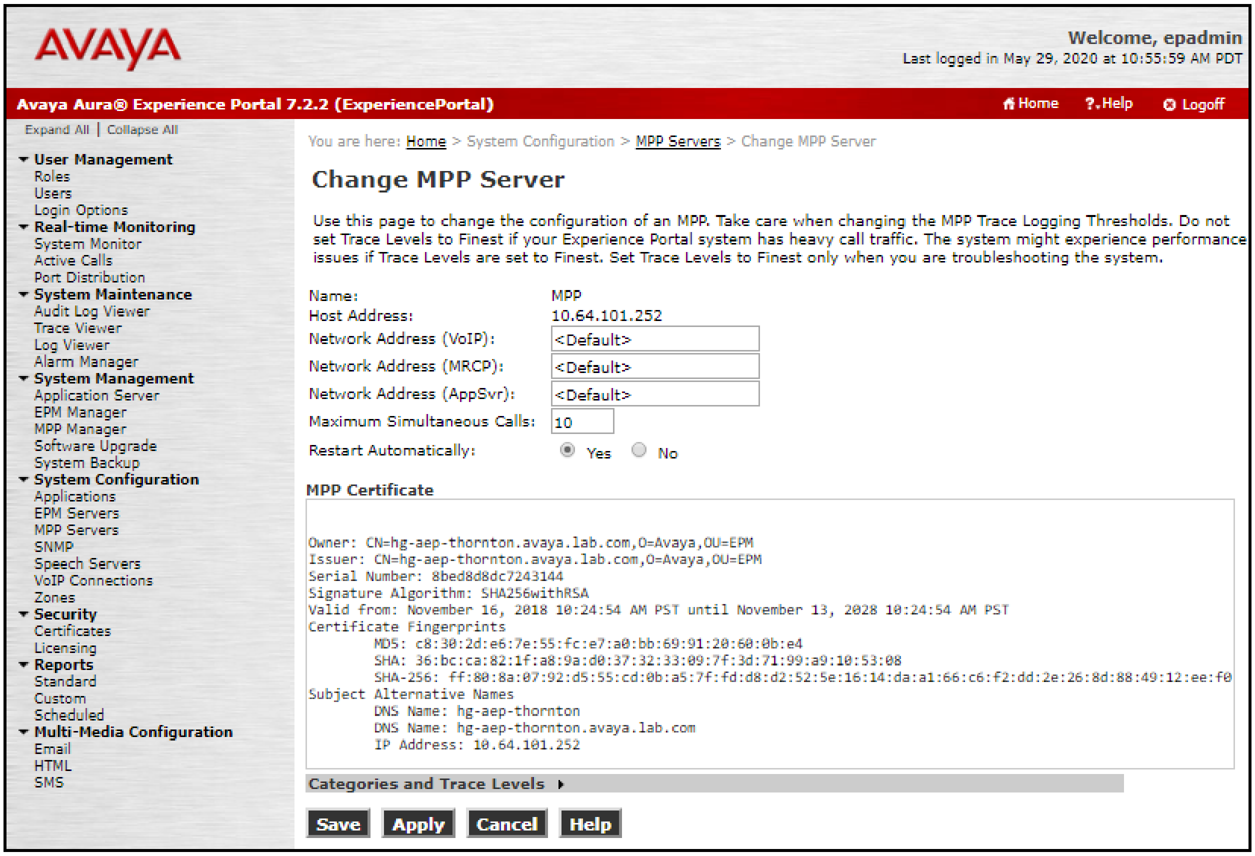
This section illustrates the procedure for viewing or changing the MPP Settings. In the sample configuration, the MPP Server is co-resident on a single server with the Experience Portal Management server (EPM).

Step 1 - In the left pane, navigate to **System Configuration→MPP Servers** and the following screen is displayed. Click **Add**.



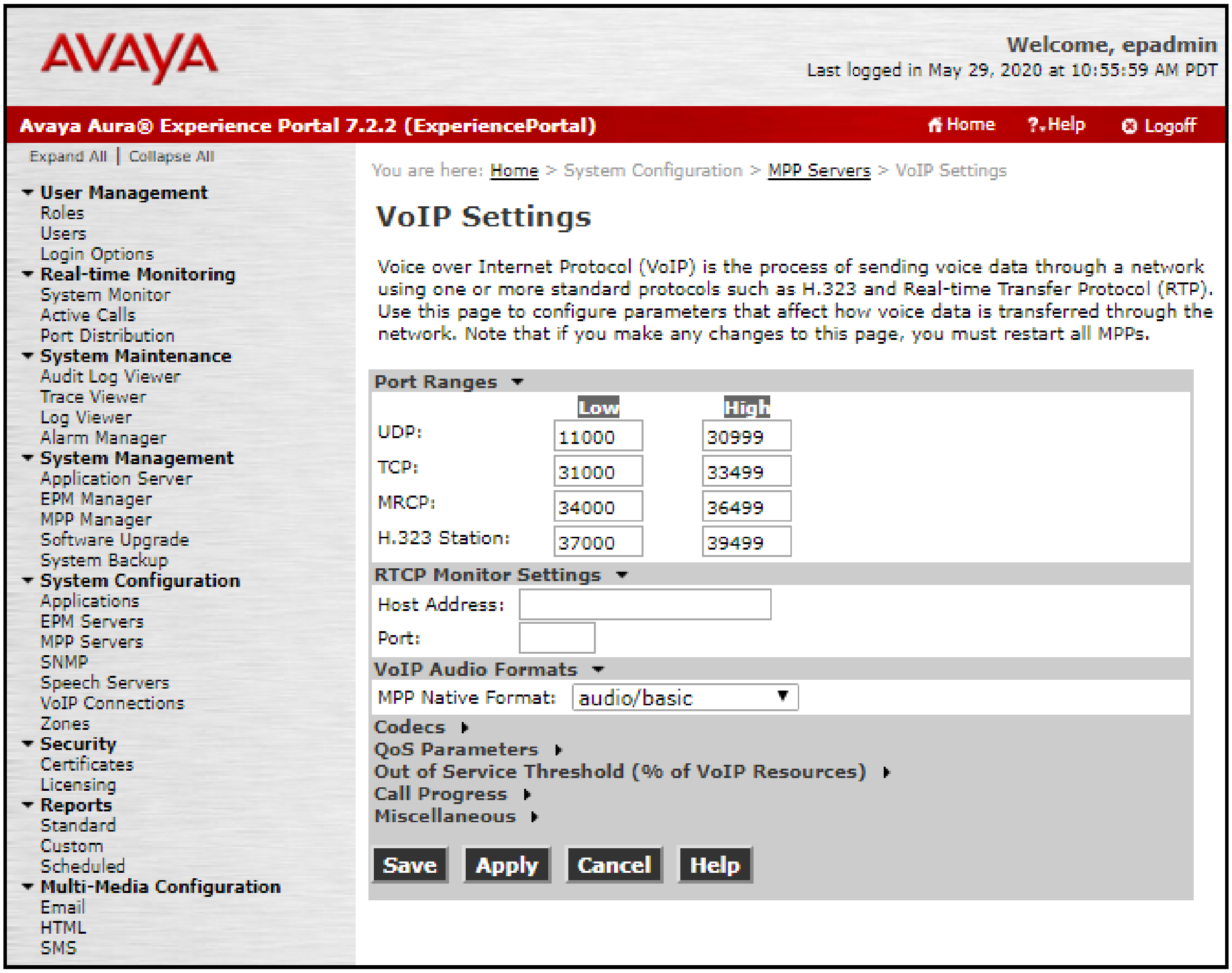
Step 2 - Enter any descriptive name in the **Name** field (e.g., **MPP**) and the IP address of the MPP server in the **Host Address** field and click **Continue** (not shown). Note that the Host Address used is the same IP address assigned to Experience Portal.

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



Step 4 - Click **VoIP Settings** tab on the screen displayed in **Step 1**, and the following screen is displayed.

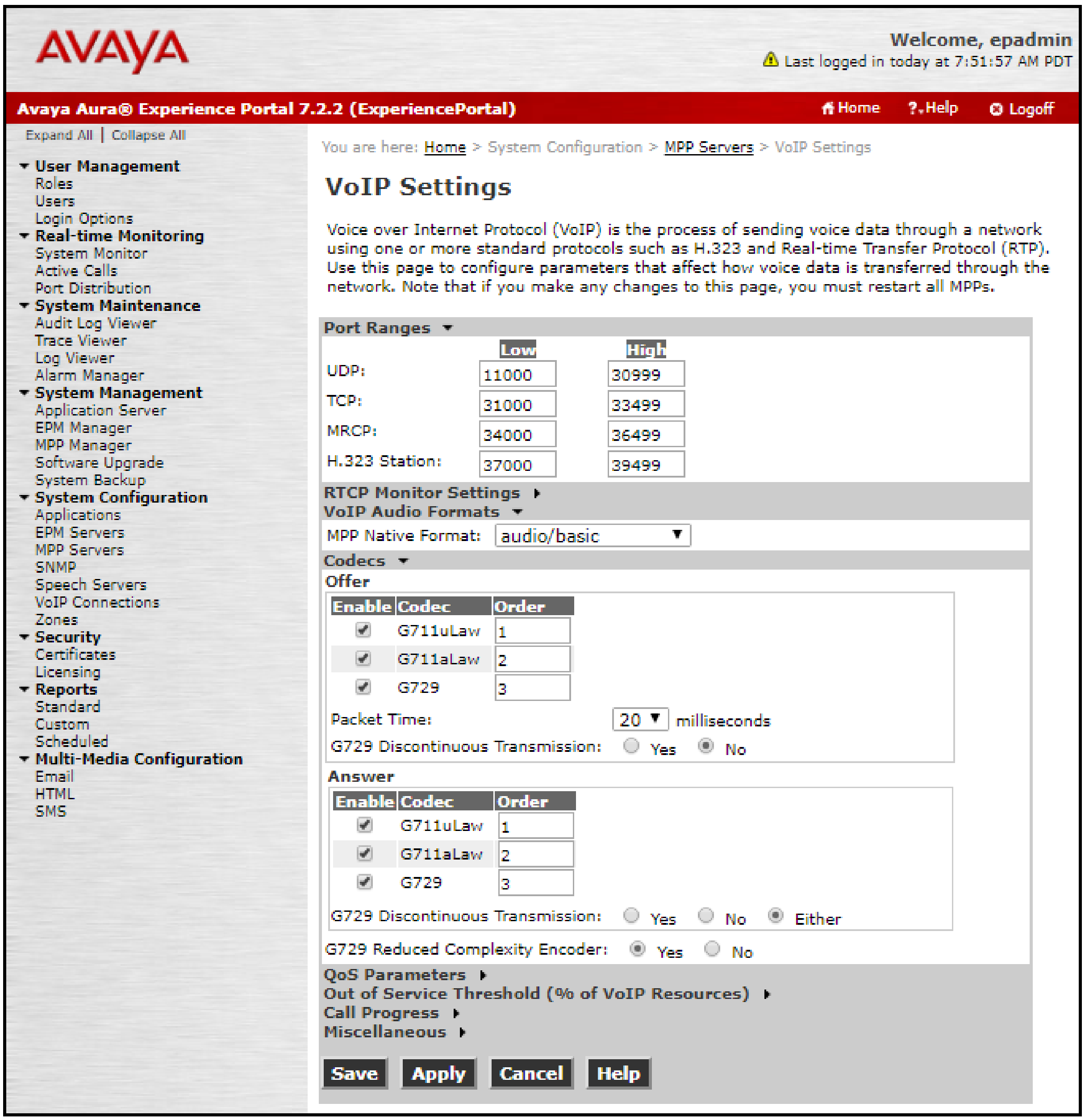
- In the Port Ranges section, default ports were used.



- In the Codecs section set:
  - Set **Packet Time** to **20**.
  - Verify Codecs **G711uLaw**, **G711aLaw** and **G.729** are enabled (check marks). Set the **Offer** and Answer **Order** as shown. In the sample configuration **G711uLaw** is the preferred codec, with **Order 1**, followed by **G711aLaw** with **Order 2** and **G729** with **Order 3**.
  - On the codec Answer set **G729 Discontinuous Transmission** to **Either**.

- Use default values for all other fields.

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



6.7. Configuring RFC2833 Event Value Offered by Experience Portal

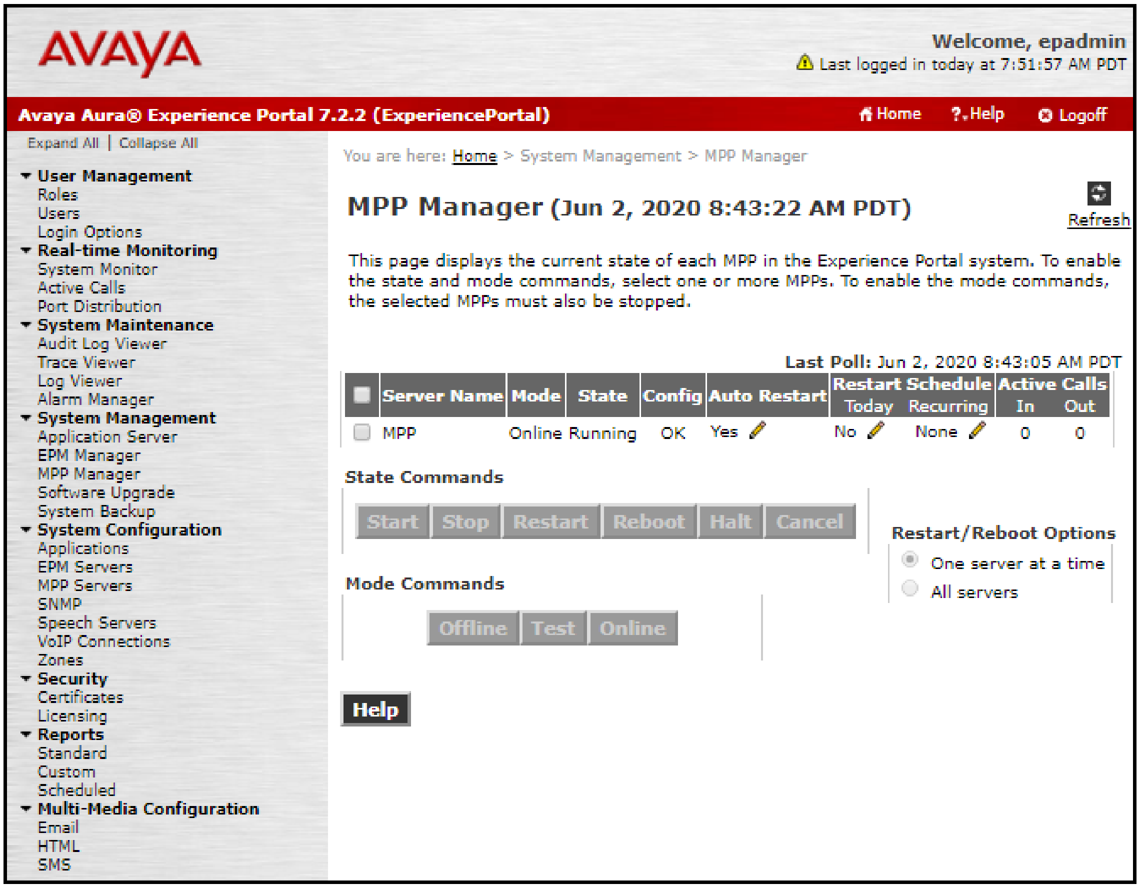
The configuration change example noted in this section was not required for any of the call flows illustrated in these Application Notes. For incoming calls from the service provider to Experience Portal, the service provider specifies the value 101 for the RFC2833 telephone-events that signal DTMF digits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

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

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

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

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



7. Configure Avaya Aura® Session Manager

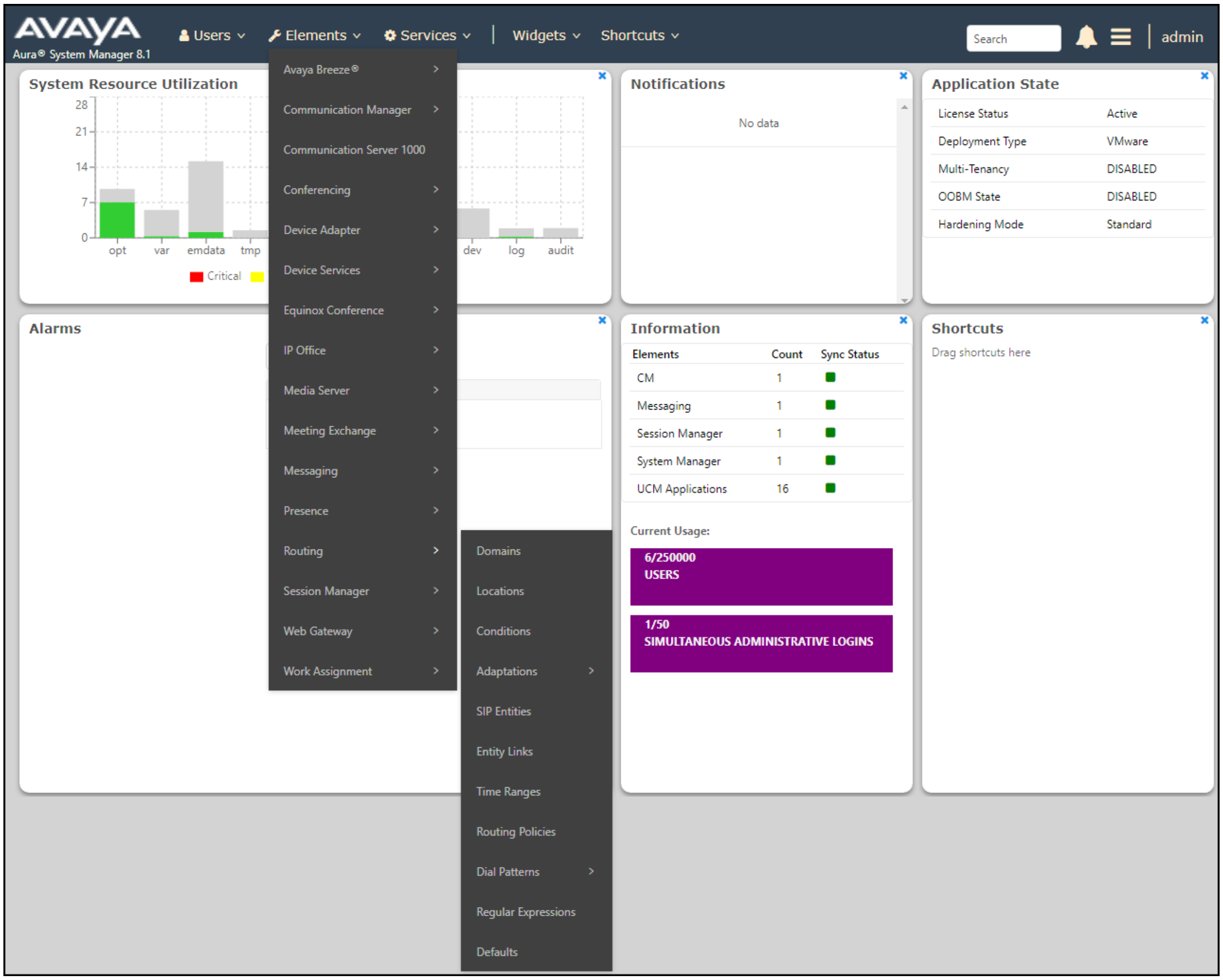
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager, Experience Portal 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.

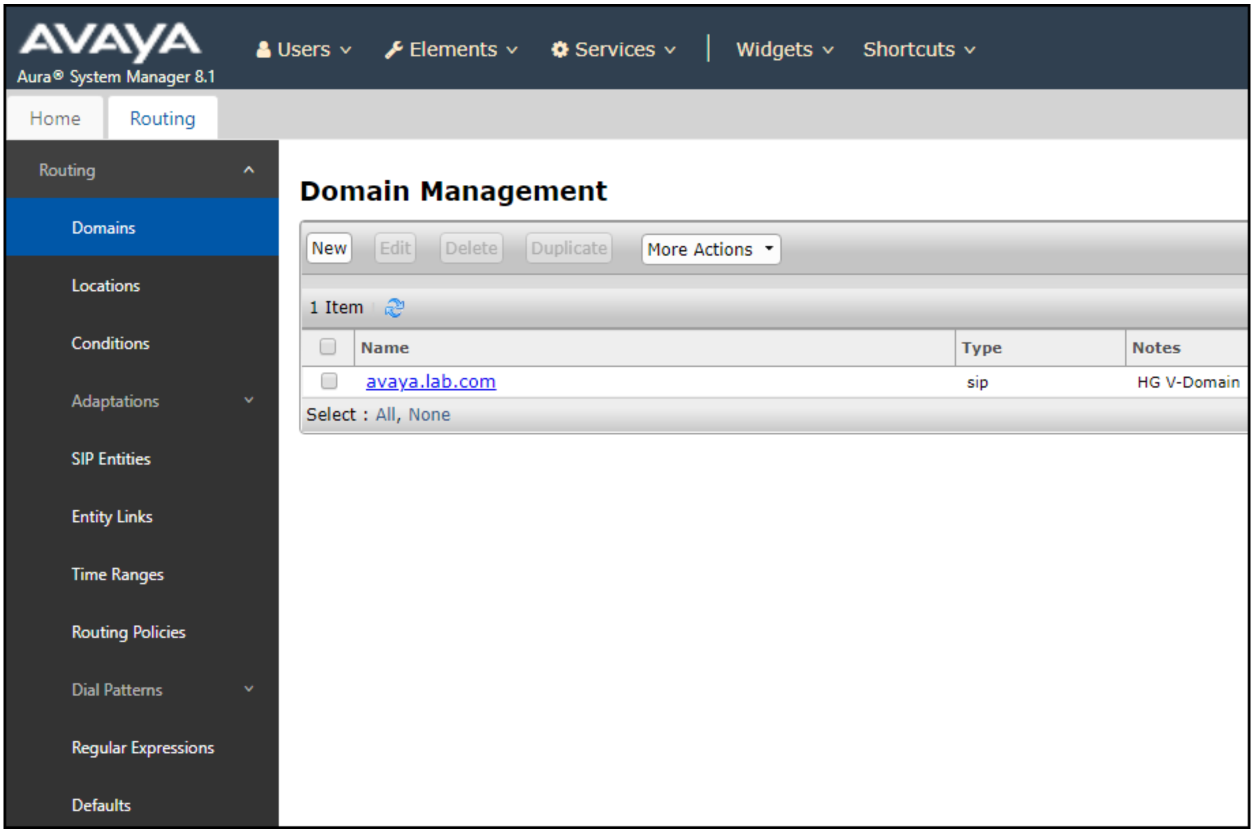
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

7.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed; under **Elements** select **Routing → Domains**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.

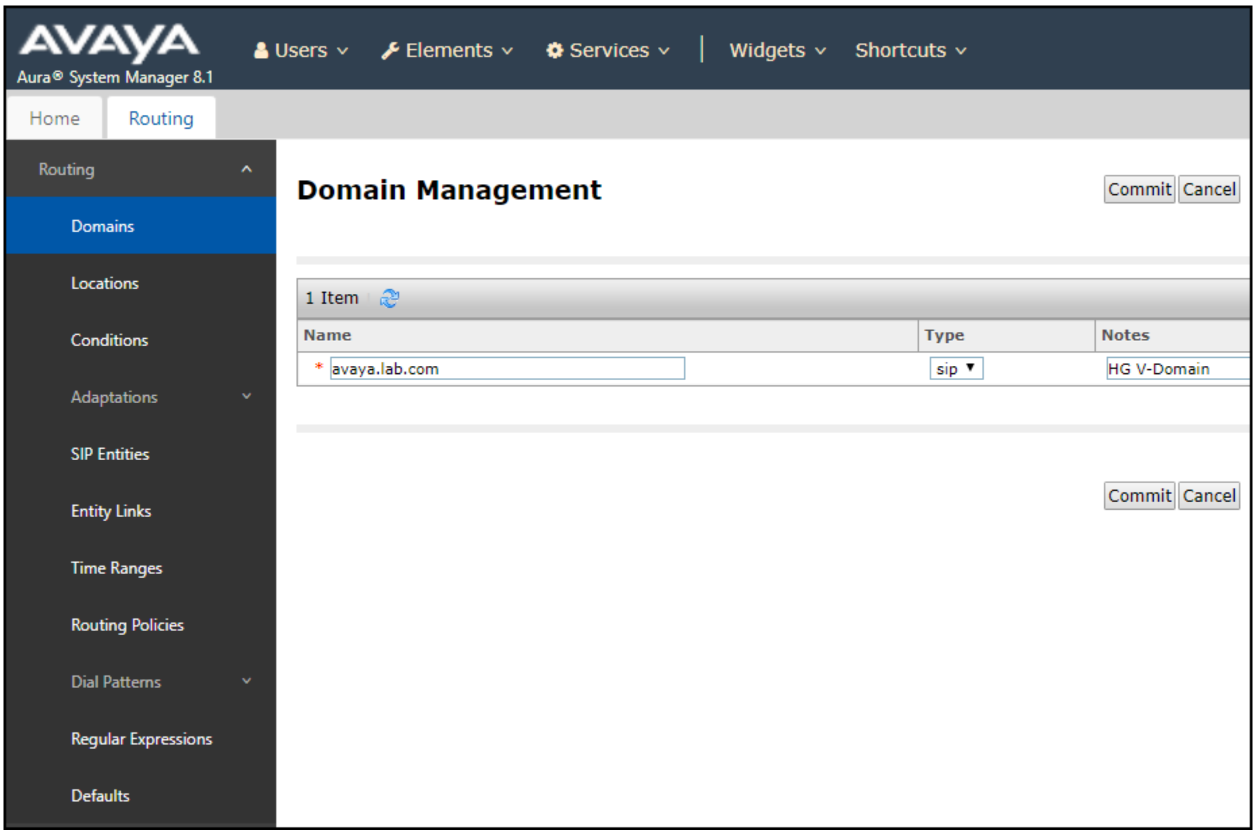


7.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, ***avaya.lab.com***. Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name**: Enter the domain name.
- **Type**: Select **sip** from the pull-down menu.
- **Notes**: Add a brief description (optional).
- Click **Commit** to save.

The screen below shows the entry for the enterprise domain.

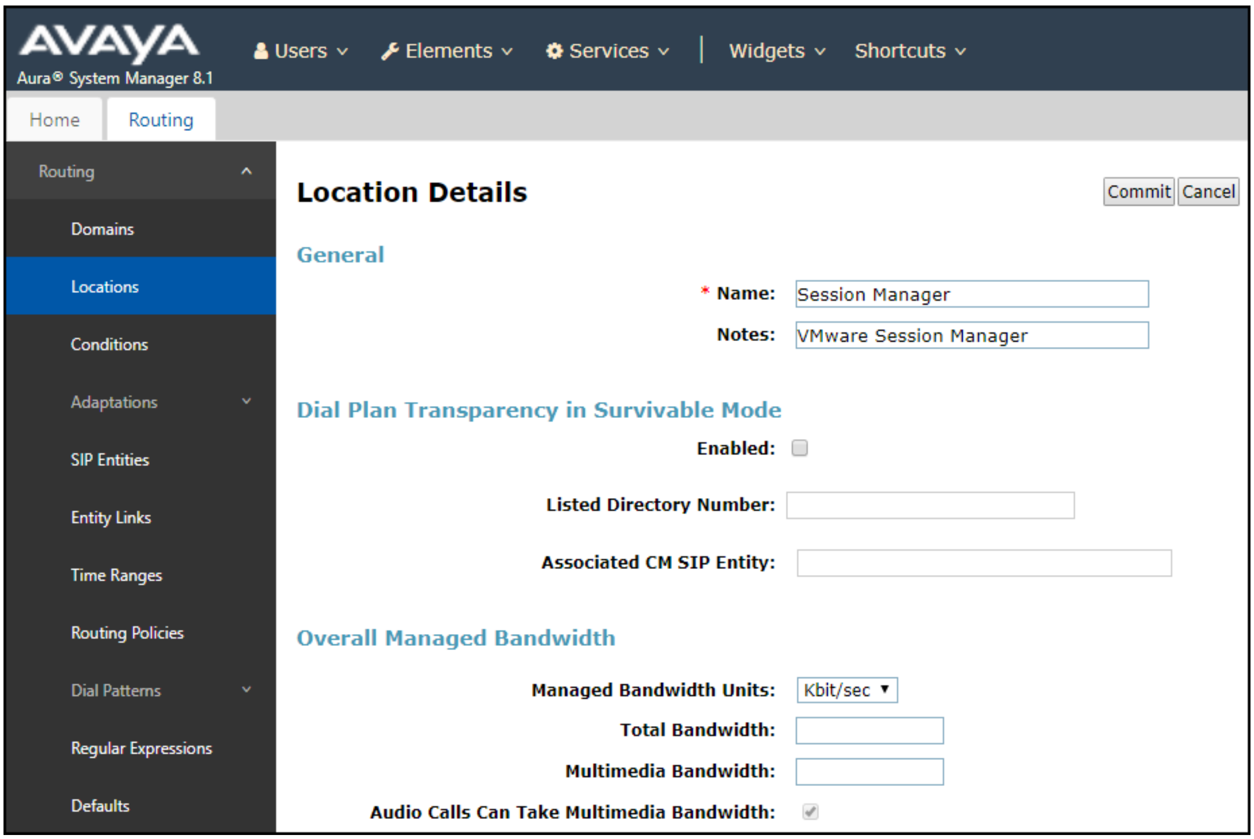


7.3. Locations

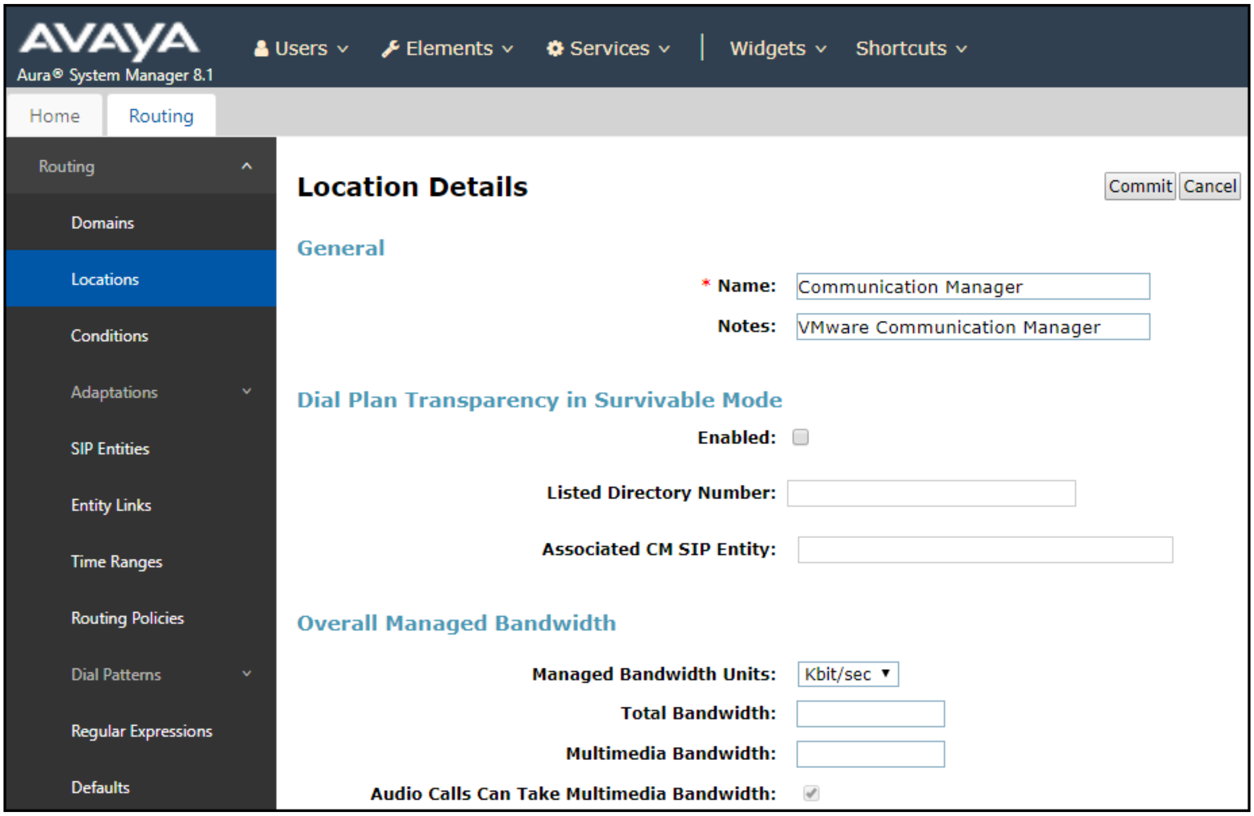
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management, call admission control and location-based routing. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in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

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

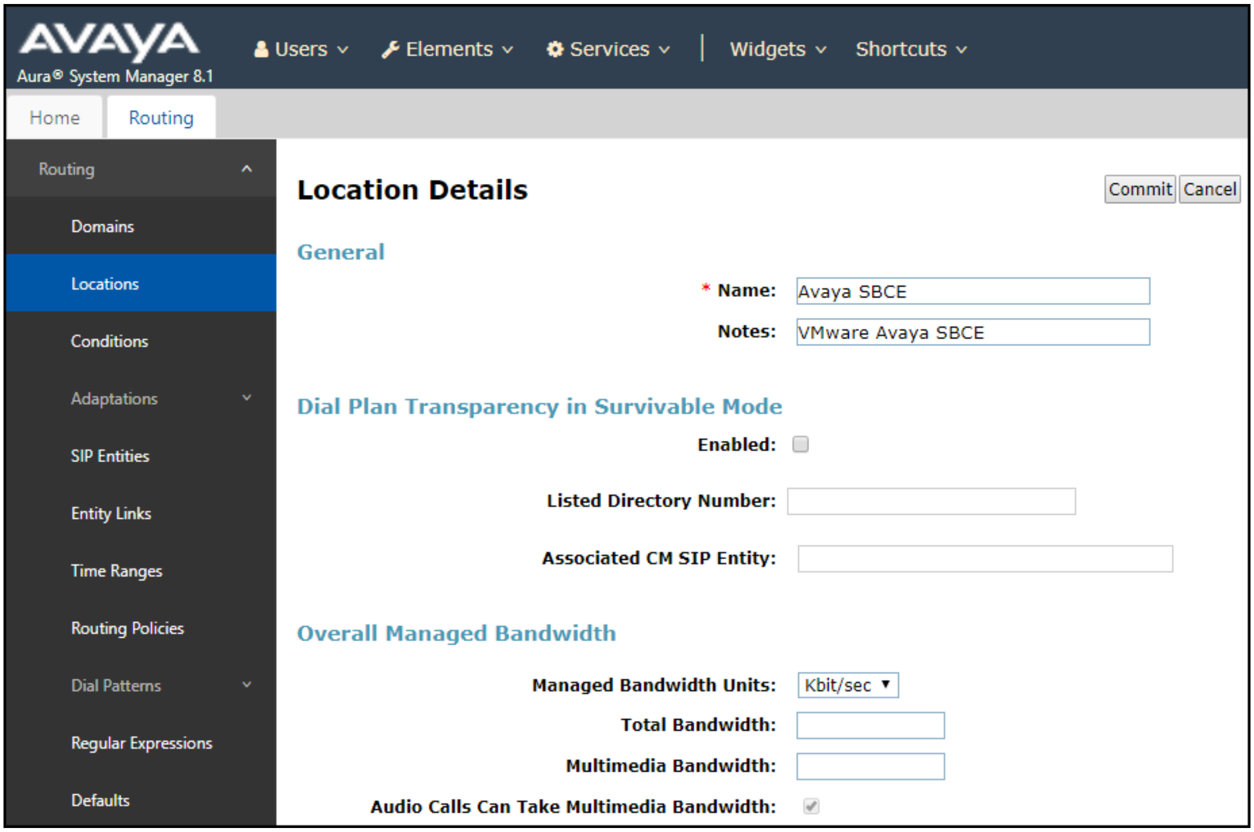
The following screen shows the location details for the location named ***Session Manager***. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Other location parameters (not shown) retained the default values.



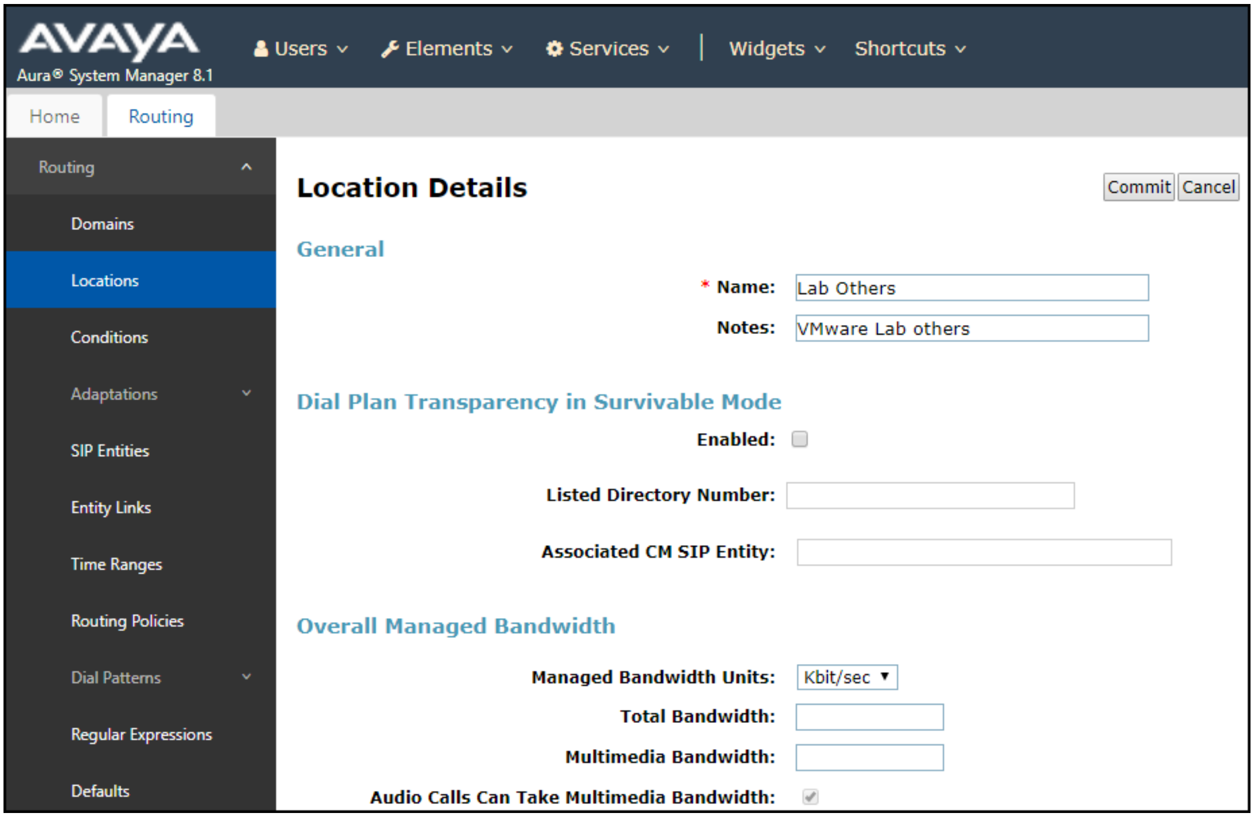
The following screen shows the location details for the location named ***Communication Manager***. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.



The following screen shows the location details for the location named ***Avaya SBCE***. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.



The following screen shows the location details for the location named ***Lab Others***. Later, this location will be assigned to the SIP Entity corresponding to the Experience Portal. Other location parameters (not shown) retained the default values.



7.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 8.1 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements. Adaptations can also be used to modify the numbers in SIP INVITE message headers before sending to its destinations (e.g., Communication Manager, Experience Portal or the Avaya SBCE).

For the compliance test, an Adaptation was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

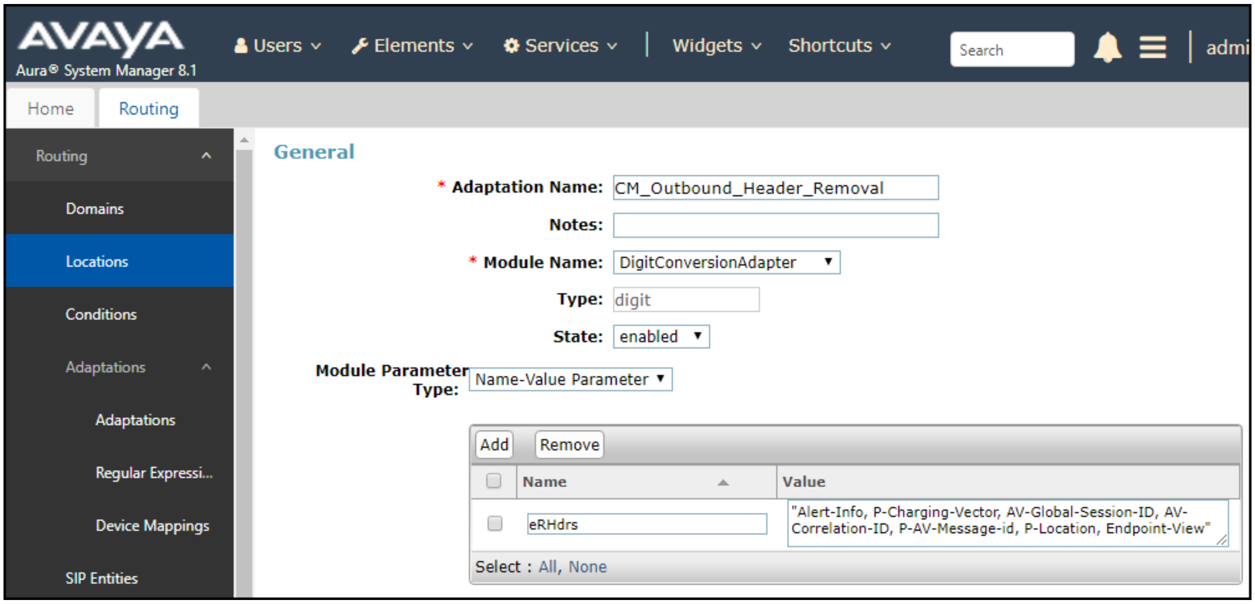
Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name**: Enter an appropriate name, ***CM_Outbound_Header_Removal*** was used in the sample configuration.
- **Module Name**: Select the ***DigitConversionAdapter*** option.
- **Module Parameter Type**: Select ***Name-Value Parameter***.

Click **Add** to add the name and value parameters, as follows:

- **Name**: Enter ***eRHdrs***. This parameter will remove the specified headers from messages in the egress direction.
- **Value**: Enter ***"Alert-Info***, ***P-Charging-Vector***, ***AV-Global-Session-ID***, ***AV-Correlation-ID***, ***P-AV-Message-Id***, ***P-Location***, ***Endpoint-View"***
- Click **Commit** to save.

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left at their default values.



A second Adaptation was created to remove the "+" from the number in the "Request-Line-URI" of SIP INVITE messages received from the Avaya SBCE destined to Experience Portal. This was necessary in order to match the DID number entry defined in Experience Portal, **Section 6.5**. Experience Portal only accepts digit entries (e.g., 12134237452).

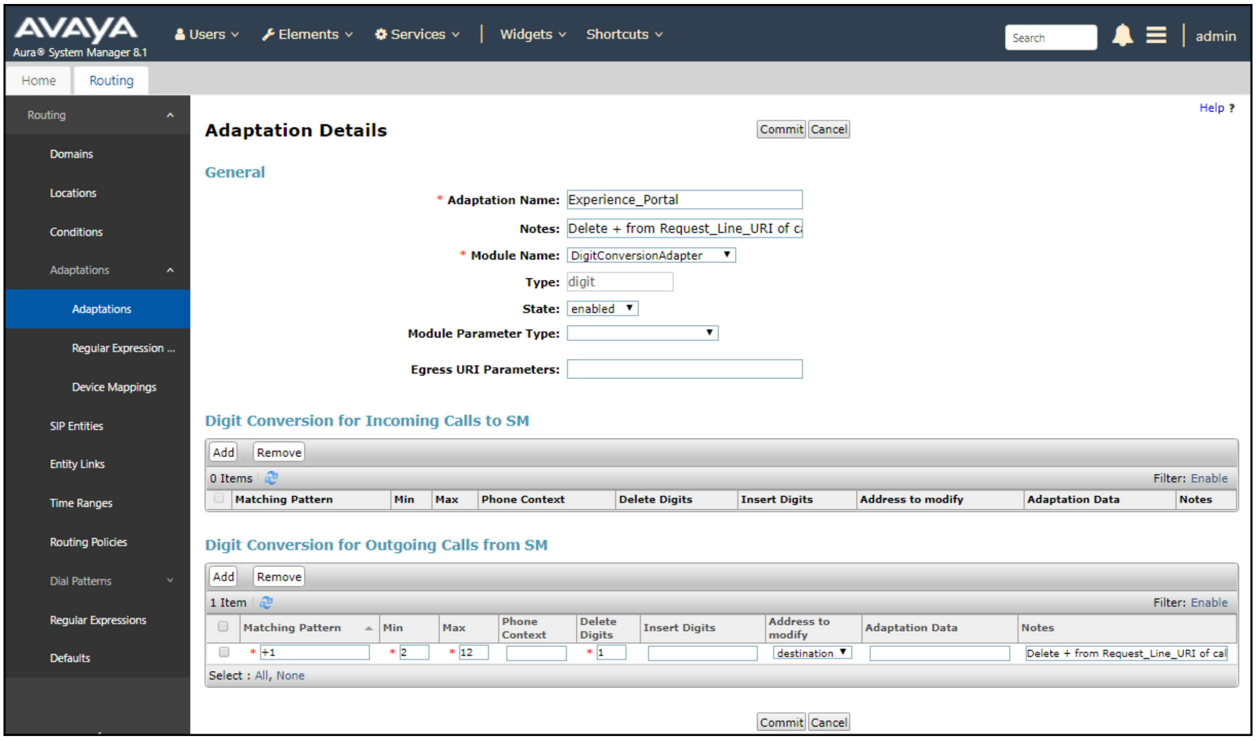
Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name**: Enter an appropriate name, ***Experience_Portal*** was used in the sample configuration.
- **Module Name**: Select the ***DigitConversionAdapter*** option.
- **Module Parameter Type**: Leave blank.

On the **Digit Conversion for outgoing calls from SM** section at the bottom of the screen add the following entries:

- **Matching Pattern**: Enter ***+1***.
- **Min**: Enter ***2***.
- **Max**: Enter ***12***.
- **Delete Digits**: Enter ***1***.
- **Address to Modify***:* Select ***Destination.***
- Click **Commit** to save.

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to Experience Portal. All other fields were left at their default values.

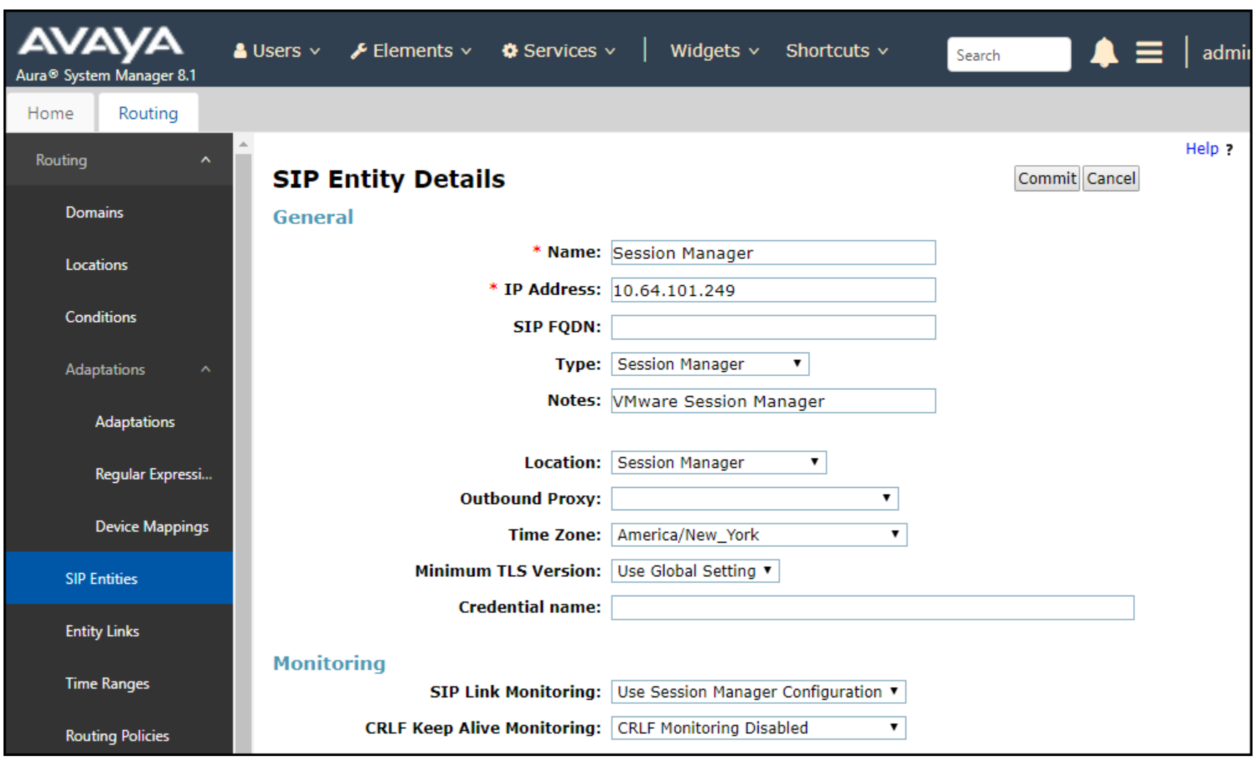


7.5. SIP Entities

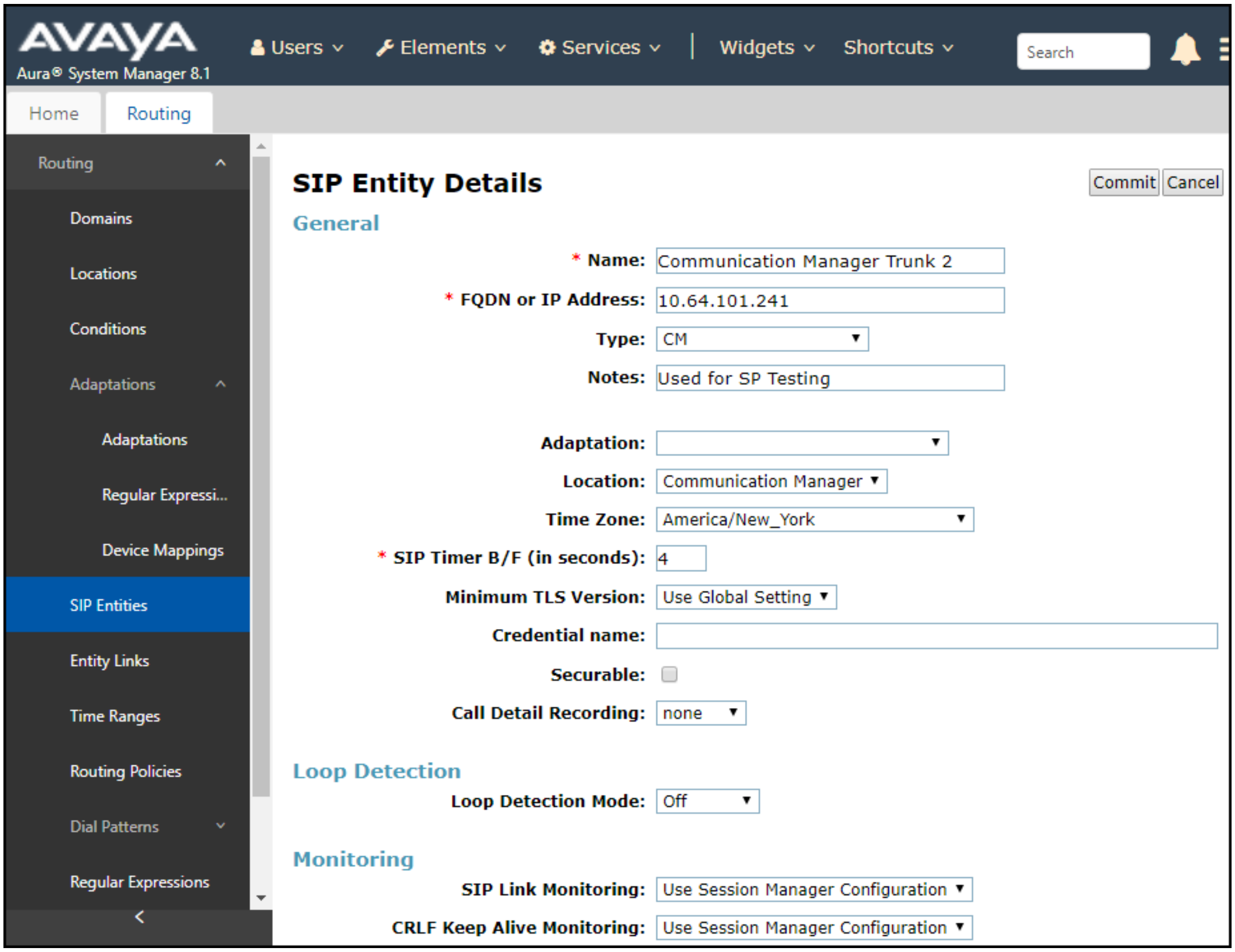
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager, Avaya SBCE and Experience Portal. Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In 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 (see **Figure 1**).
- **Type**: Select ***Session Manager*** for Session Manager, ***CM*** for Communication Manager, ***SIP Trunk*** (or ***Other***) for the Avaya SBCE and ***Voice Portal*** for the Experience Portal.
- **Adaptation**: This field is only present if **Type** is not set to **Session Manager**. If Adaptations were created, here is where they would be applied to the SIP entity.
- **Location**: Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- **Time Zone**: Select the time zone for the location above.
- Click **Commit** to save.

The following screen shows the addition of the ***Session Manager*** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.



The following screen shows the addition of the ***Communication Manager Trunk 2*** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the "**procr**" interface in Communication Manager, as seen in **Section 5.3**. Select the location that applies to the SIP Entity being created, defined in **Section 7.3**. Select the **Time Zone**.

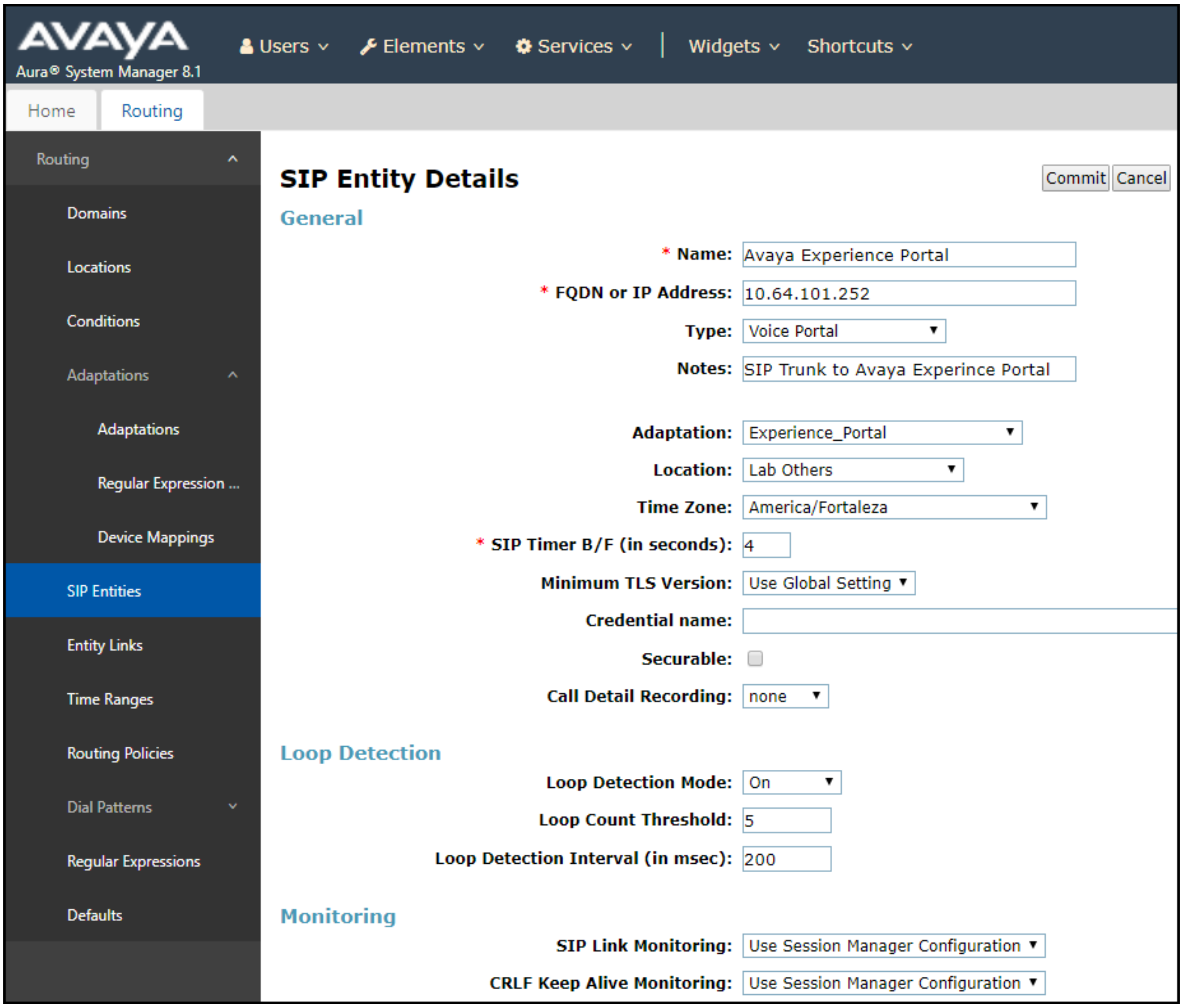


The following screen shows the addition of the ***Avaya SBCE*** SIP Entity for the Avaya SBCE:

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- On the **Adaptation** field, the adaptation module ***CM_Outbound_Header_Removal*** previously defined in **Section 7.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- Select the **Time Zone**.

The following screen shows the addition of the ***Avaya Experience Portal*** SIP Entity:

- The **FQDN or IP Address** field is set to the IP address of the Experience Portal (see **Figure 1**).
- On the **Adaptation** field, the adaptation module ***Experience_Portal*** previously defined in **Section 7.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 7.3**.
- Select the **Time Zone**.

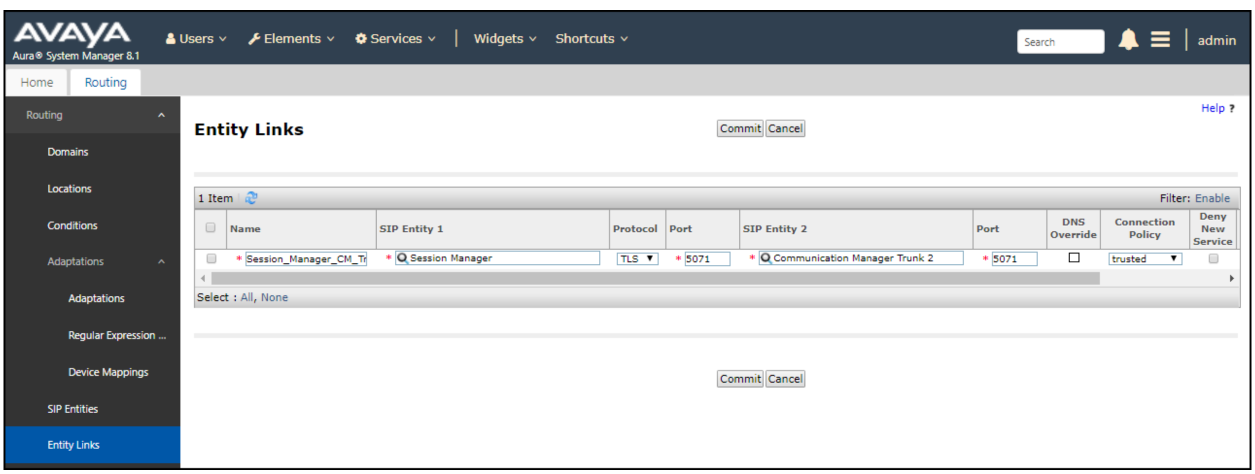


7.6. Entity Links

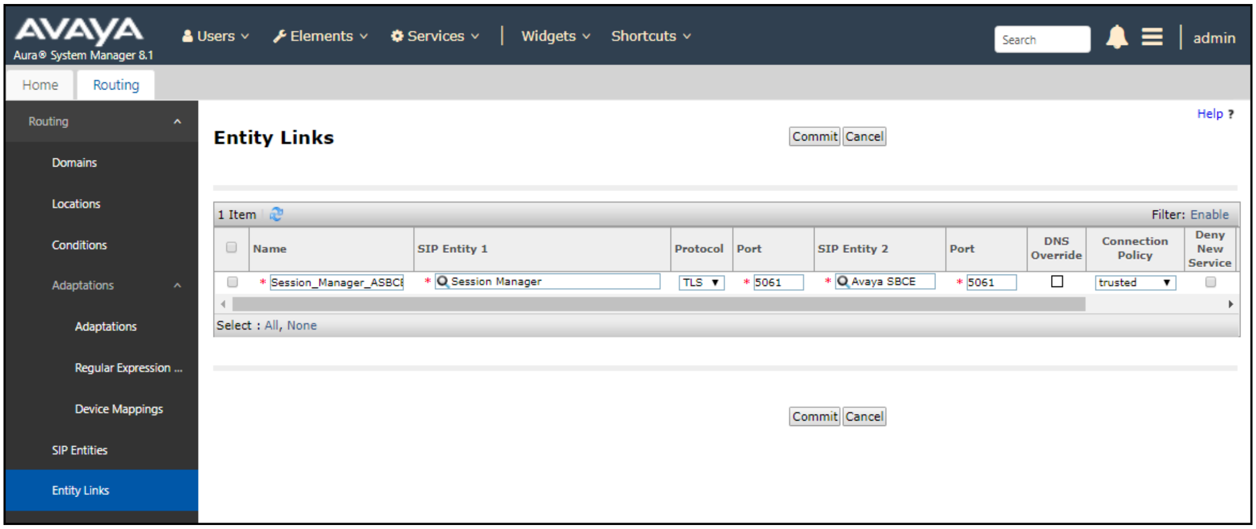
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Three Entity Links were created; an entity link to Communication Manager for use only by service provider traffic, an entity link to the Avaya SBCE and an entity link to Experience Portal. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **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 from the drop-down menu (**Section 7.5**).
- **Protocol**: Select the transport protocol used for this link (**Section 5.6**).
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2**: Select the name of the other system from the drop-down menu (**Section 7.5**).
- **Port**: Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy**: Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

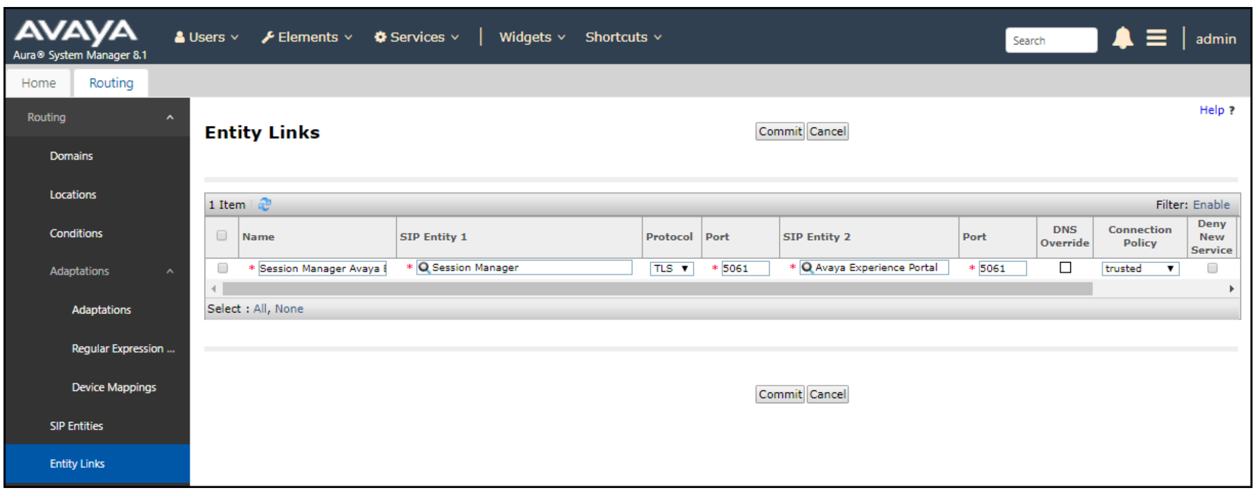
The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. ***TLS*** transport and port ***5071*** were used.



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



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

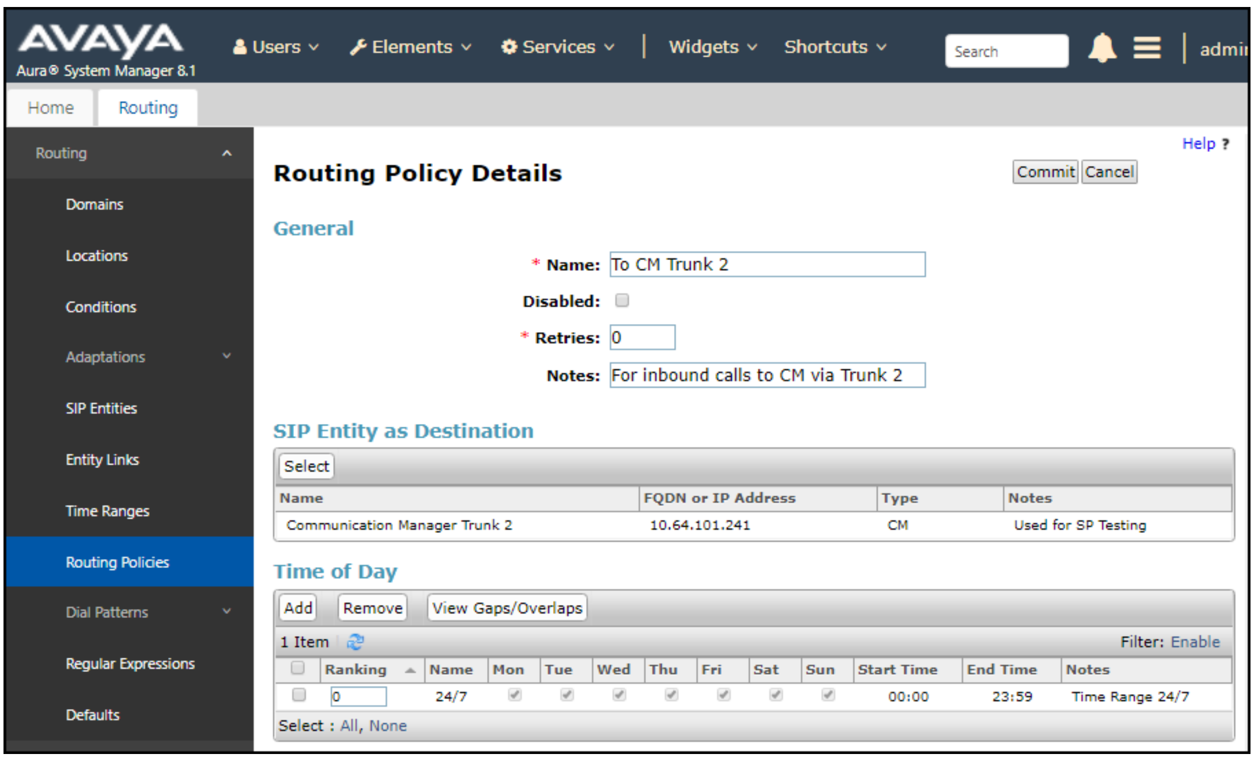


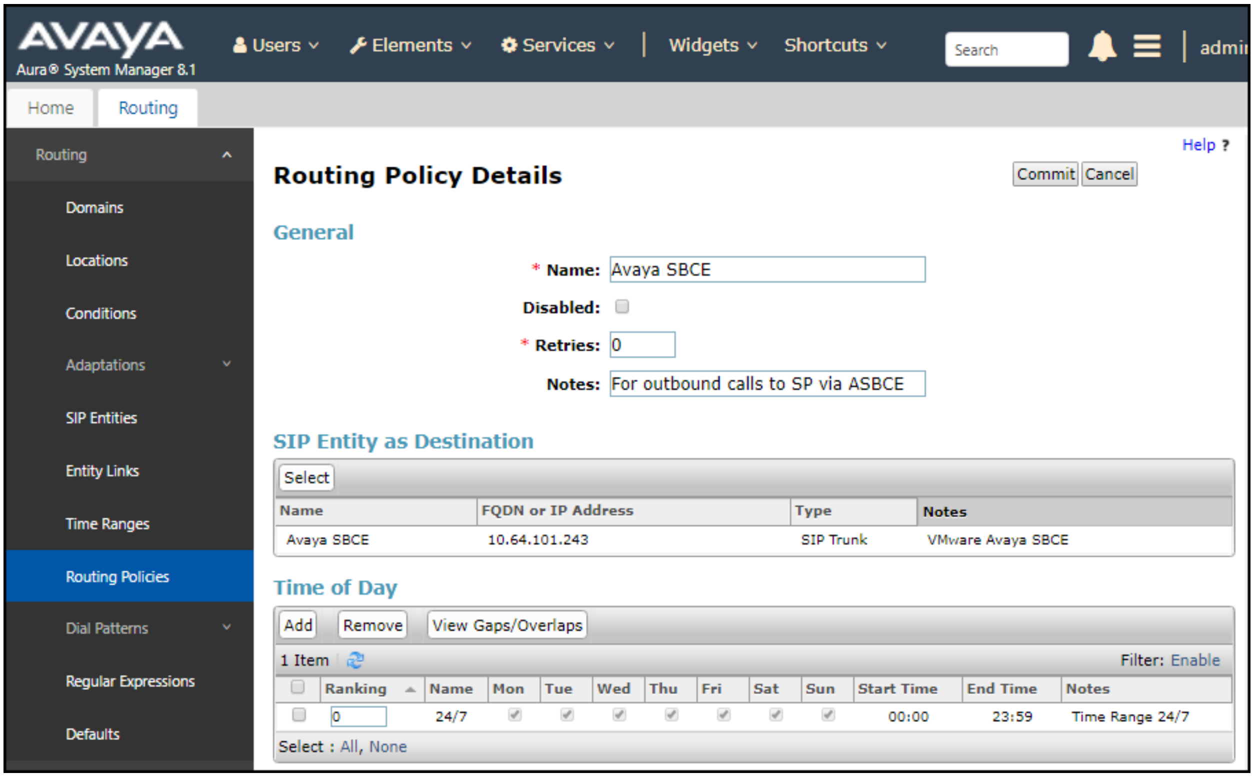
7.7. Routing Policies

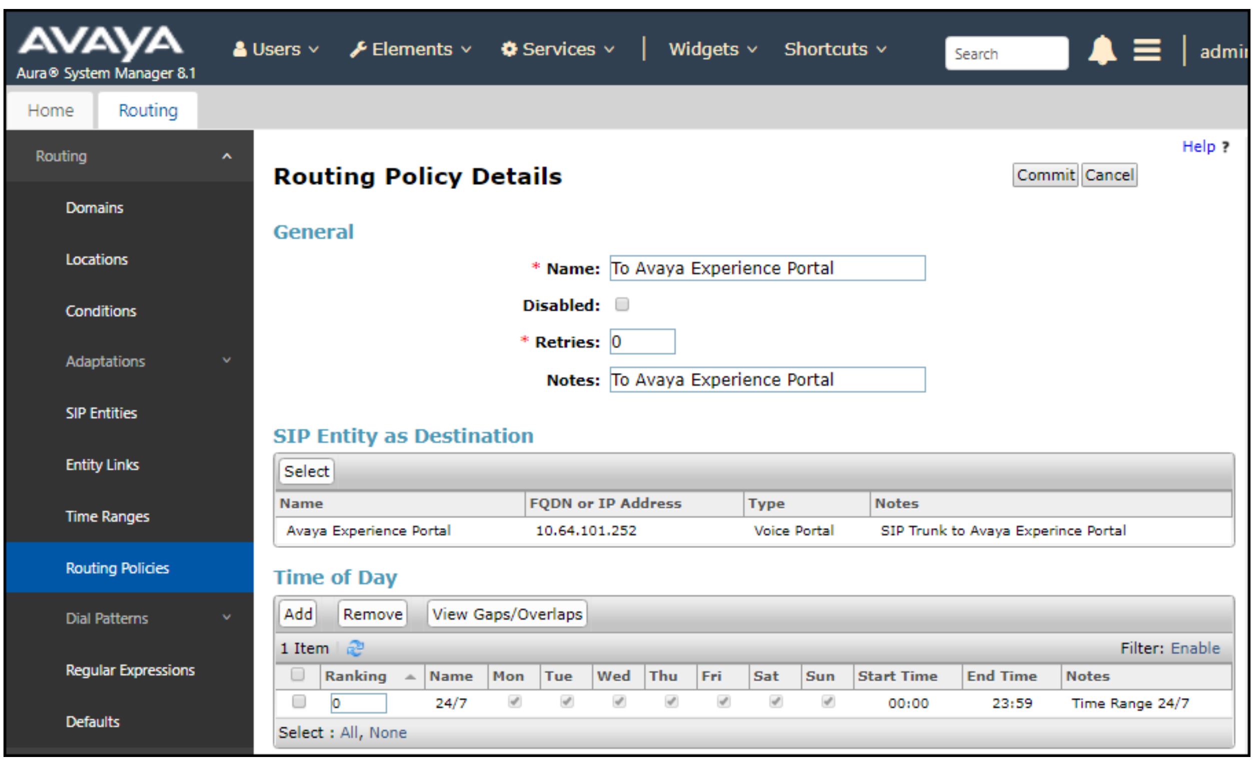
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 7.5**. Three routing policies were added; an incoming policy with Communication Manager as the destination, an outbound policy with the Avaya SBCE as the destination and an incoming policy with Experience Portal as the destination. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 7.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager, the Avaya SBCE and the Experience Portal.




AVAYA
Aura® System Manager 8.1
Users
Elements
Services
Widgets
Shortcuts
Search
admi
Home
Routing
Routing
Domains
Locations
Conditions
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Help ?
Routing Policy Details
Commit
Cancel
General
* Name: Avaya SBCE
Disabled:
* Retries: 0
Notes: For outbound calls to SP via ASBCE
SIP Entity as Destination
Select
Name | FQDN or IP Address | Type | Notes
Avaya SBCE | 10.64.101.243 | SIP Trunk | VMware Avaya SBCE
Time of Day
Add
Remove
View Gaps/Overlaps
1 Item
Filter: Enable
Ranking | Name | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start Time | End Time | Notes
0 | 24/7 | 00:00 | 23:59 | Time Range 24/7
Select : All, None


AVAYA
Aura® System Manager 8.1
Users
Elements
Services
Widgets
Shortcuts
Search
admi
Home
Routing
Routing
Domains
Locations
Conditions
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Help ?
Routing Policy Details
Commit
Cancel
General
* Name: To Avaya Experience Portal
Disabled:
* Retries: 0
Notes: To Avaya Experience Portal
SIP Entity as Destination
Select
Name | FQDN or IP Address | Type | Notes
Avaya Experience Portal | 10.64.101.252 | Voice Portal | SIP Trunk to Avaya Experince Portal
Time of Day
Add
Remove
View Gaps/Overlaps
1 Item
Filter: Enable
Ranking | Name | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start Time | End Time | Notes
0 | 24/7 | 00:00 | 23:59 | Time Range 24/7
Select : All, None

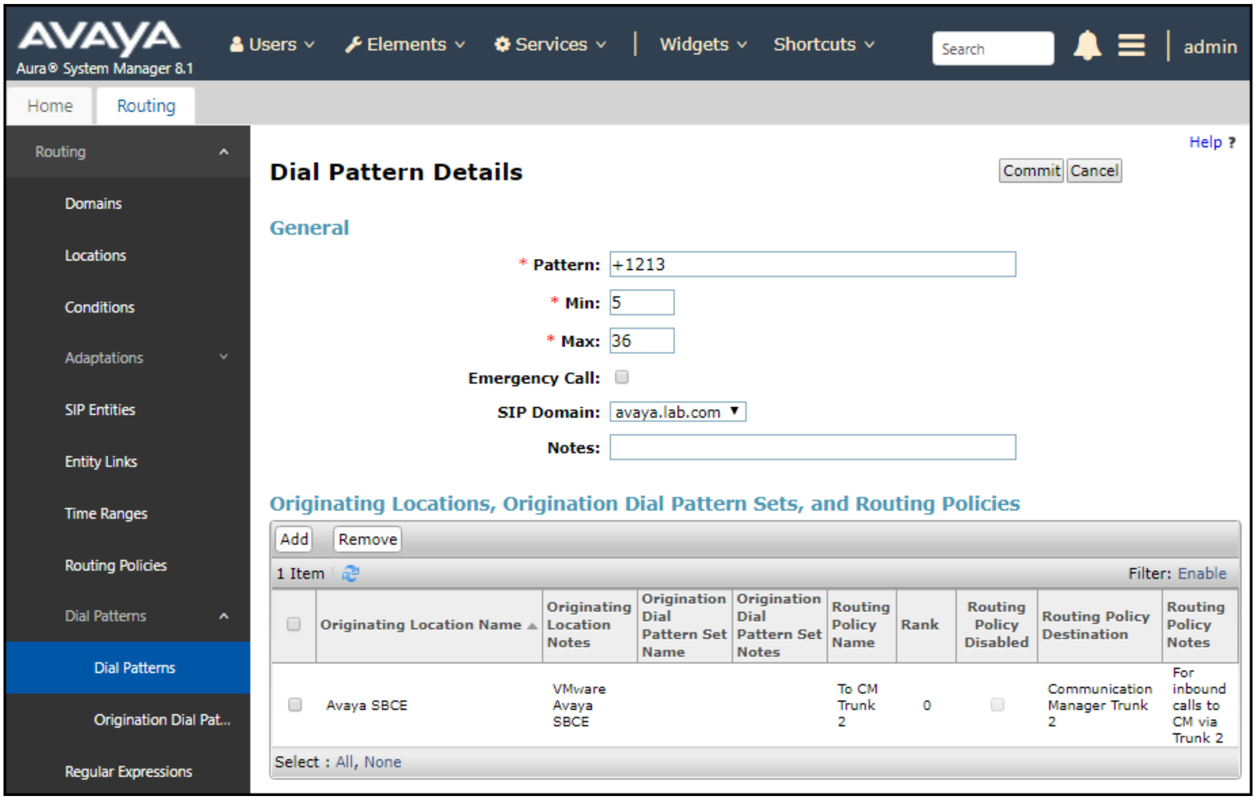
7.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager and from Experience Portal to the service provider and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

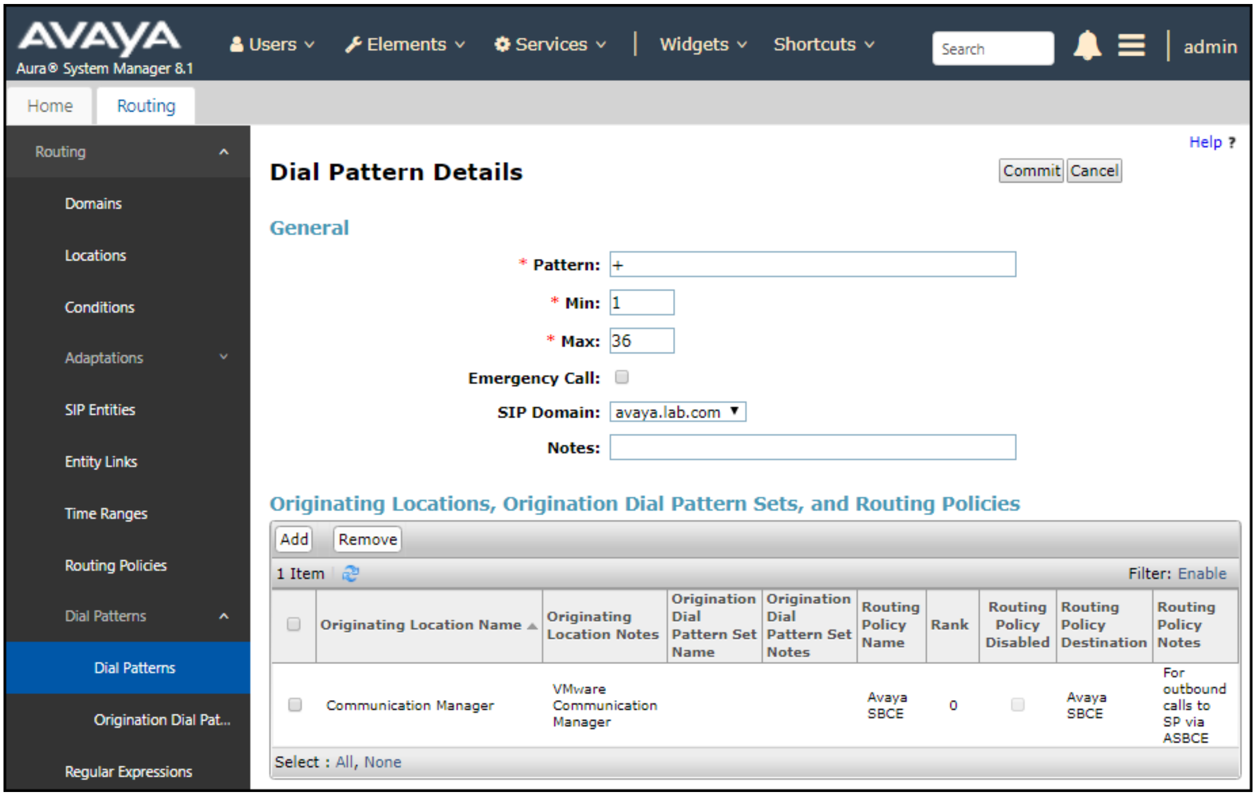
In the **General** section, enter the following values:

- **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, or select "**ALL**" to route incoming calls to all SIP domains.
- **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 (**Section 7.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 7.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound calls from the PSTN to Communication Manager. In the example, calls to 11-digit numbers, preceded by a "+", starting with ***+1213***, arriving from location ***Avaya SBCE***, used route policy ***To CM Trunk 2*** to Communication Manager. The SIP Domain was set to ***avaya.lab.com***.



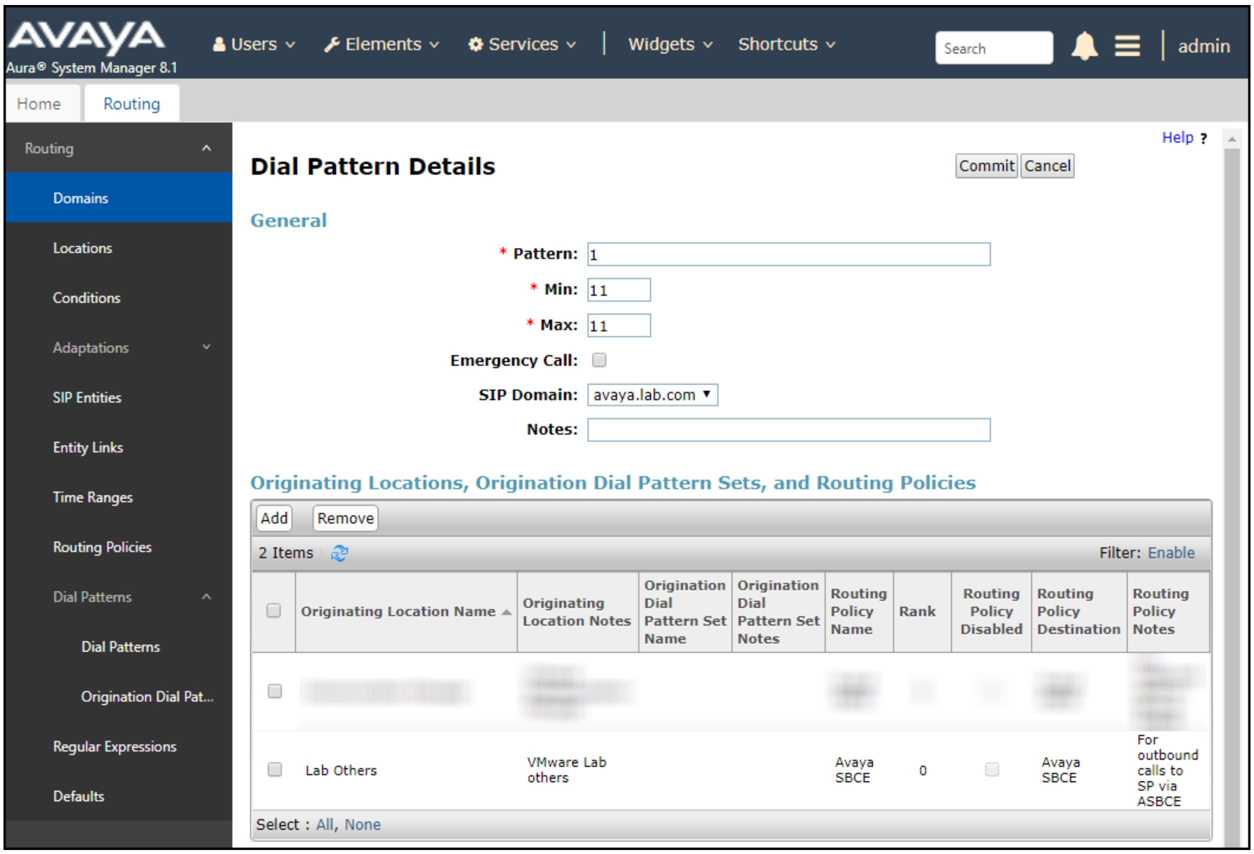
The following screen illustrates an example dial pattern used to verify outbound calls from Communication Manager to the PSTN. In the example, calls to 11-digit numbers, preceded by a "+", arriving from location ***Communication Manager***, used route policy to ***Avaya SBCE*** to the Avaya SBCE. The SIP Domain was set to ***avaya.lab.com***. In the reference configuration shown below E.164 numbering format were used for national and international calls. Note that this dial pattern does not include calls originating from Experience Portal to the PSTN.



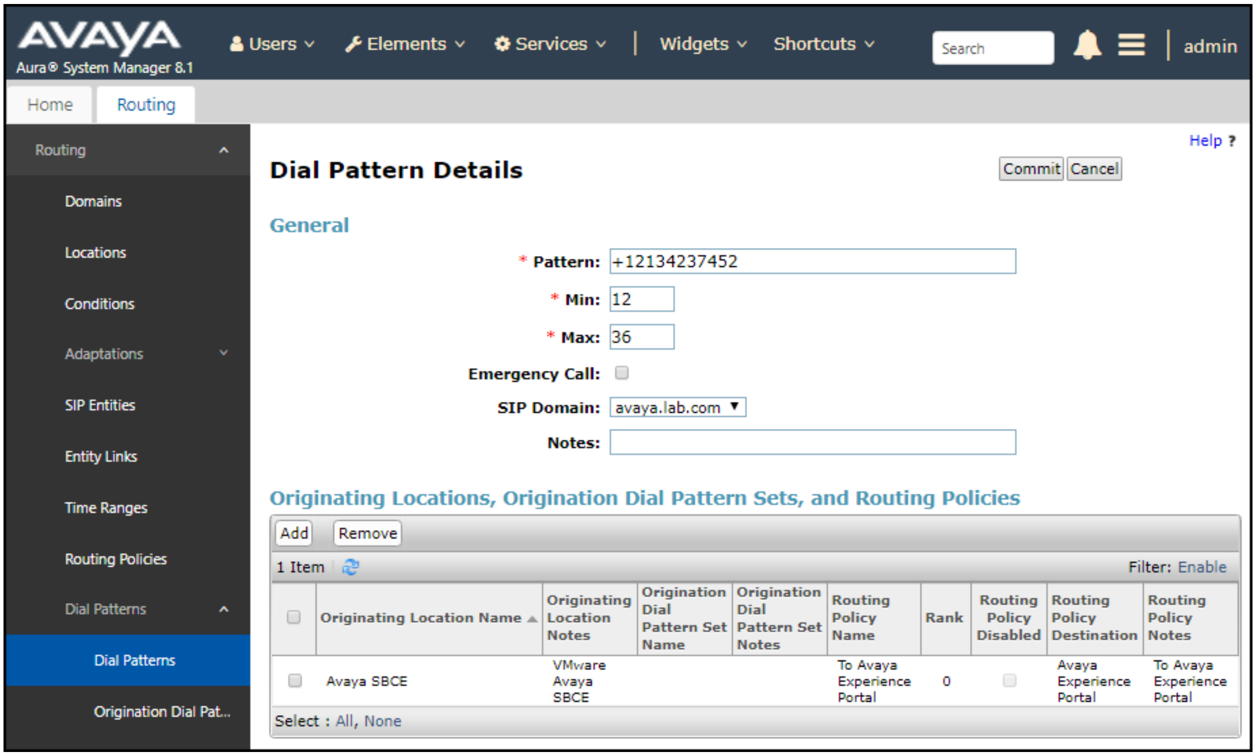
Note – Service numbers, e.g., x11, 1411, 5551212, etc. were not tested (**Section 2.1**), if access to service numbers needs to be added at a later date, dial patterns for Non-E.164 numbers should be used, e.g., x11, 1411, 5551212, using Originating Location: ***Communication Manager*** and Route policy: ***Avaya SBCE***, same as shown in the above screenshot. Also, route patterns for Non-E.164 numbers should be added, refer to **Section 5.10**.

The following screen illustrates an example dial pattern used to verify outbound calls from Experience Portal to the PSTN. Note that this dial pattern does not include the "+" preceding the "1" since Experience Portal does not include the "+". In the example below, calls to 11-digit numbers, arriving from location ***Lab Others*** (Experience Portal) used route policy to ***Avaya SBCE*** to route calls to the Avaya SBCE, this entry handles all other outbound calls from Experience Portal to the PSTN. The domain was set to ***avaya.lab.com***.

Note – If Experience Portal is not included as part of the Avaya Enterprise equipment the dial pattern shown below can be omitted/excluded.



The following screen illustrates an example dial pattern used to verify inbound calls from the PSTN to Experience Portal. In the sample configuration one of the DID numbers provided by the service provider was used as a test number to route calls from the PSTN to Experience Portal, arriving from location ***Avaya SBCE***, used routing policy ***To Avaya Experience Portal***. The SIP Domain was set to ***avaya.lab.com***.



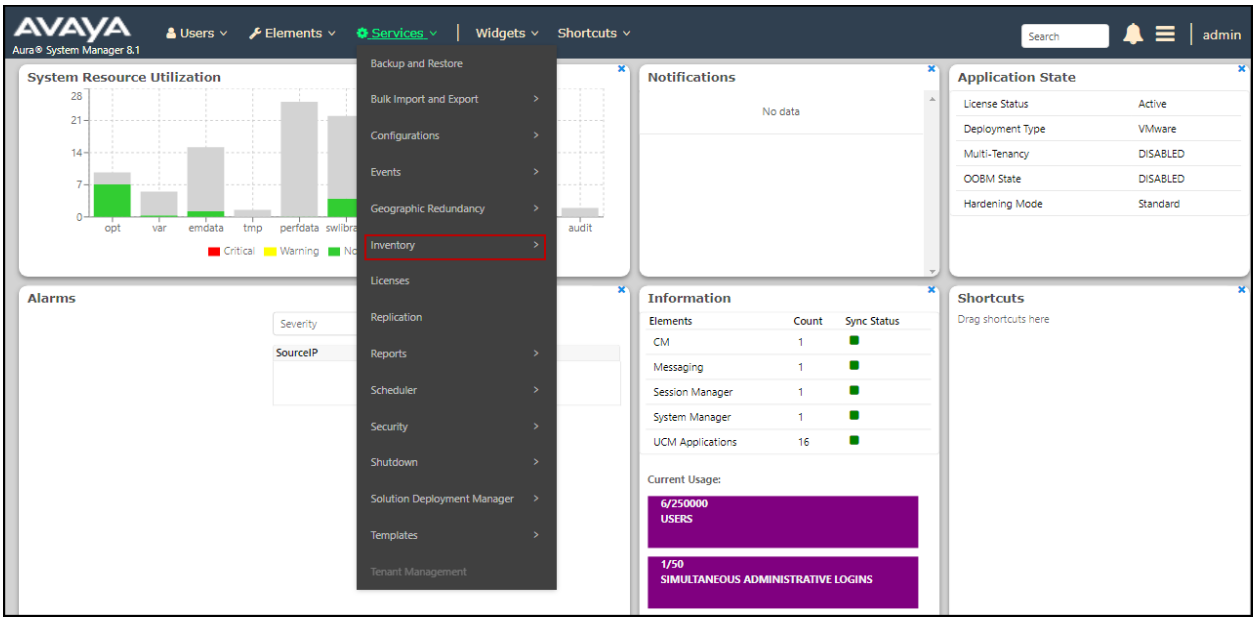
Repeat the above procedures as needed to define additional dial patterns.

7.9. Verify TLS Certificates – Session Manager

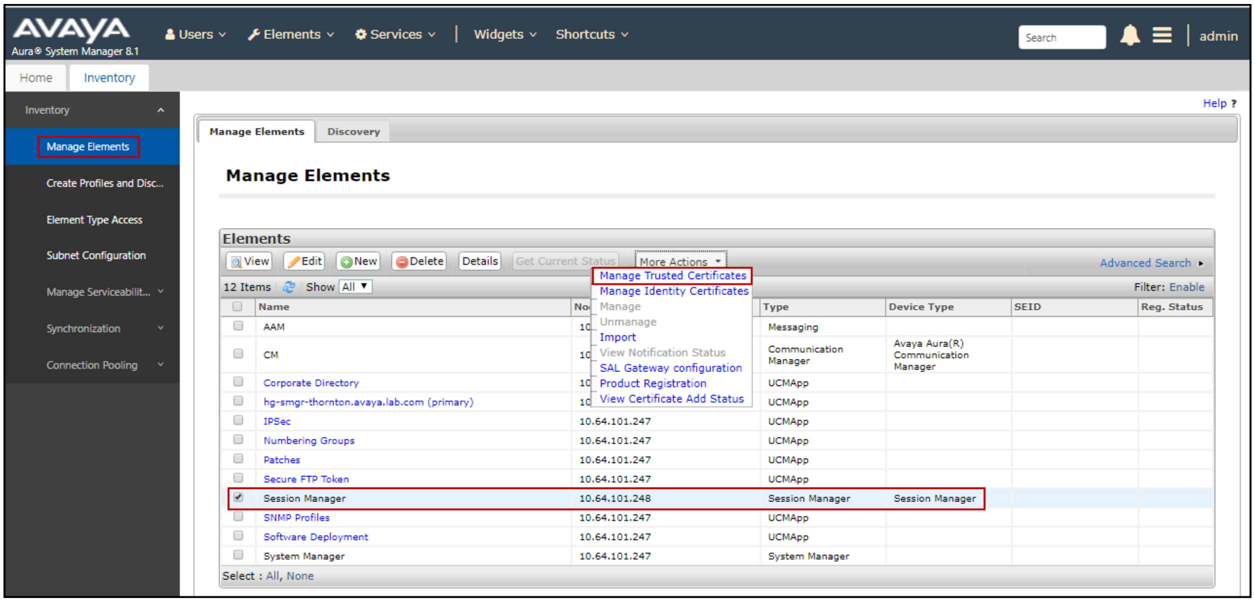
Note – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

The following procedures show how to verify the certificates used by Session Manager.

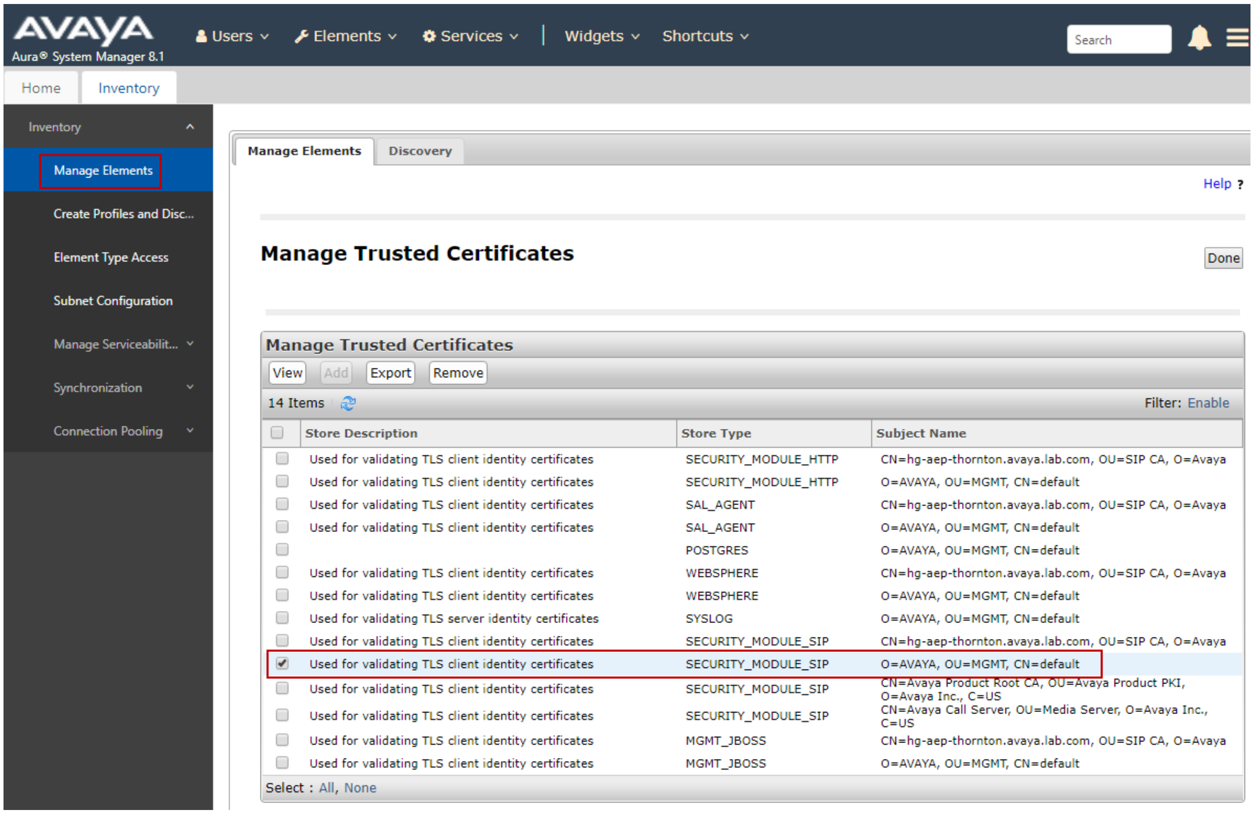
Step 1 - From the **Home** screen, under the **Services** heading, select **Inventory**.



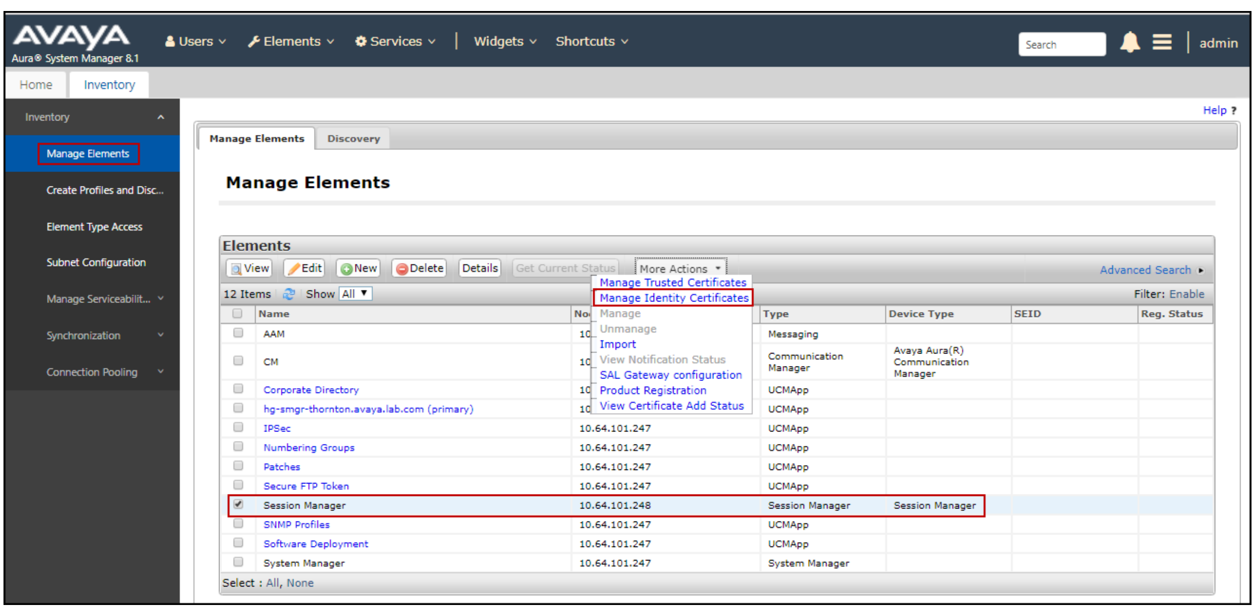
Step 2 - In the left pane under **Inventory**, click on **Manage Elements** and select the Session Manager element, e.g., **Session Manager**. Click on **More Actions → Manage Trusted Certificates**.



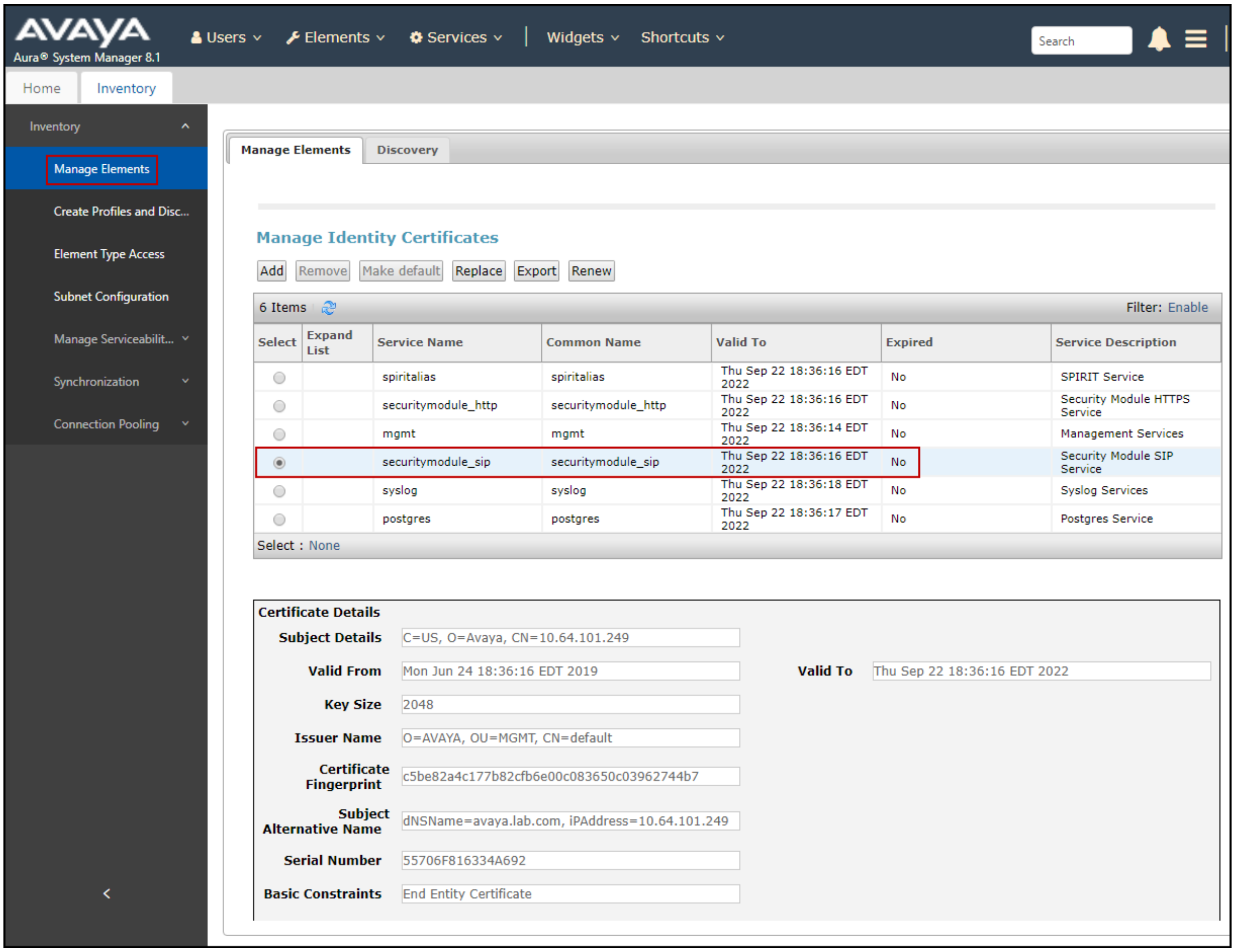
Step 3 - Verify the **System** Manager Certificate Authority certificate is listed in the trusted store, **SECURITY_MODULE_SIP**. Click **Done** to return to the previous screen.



Step 4 - With Session **Manager** selected, click on **More Actions → Manage Identity Certificates**.



Step 5 - Verify the **Security Module SIP** service has a valid identity certificate signed by System Manager. If the **Subject Details** and **Subject Alternative Name** fields of the System Manager signed certificate need to be updated, click **Replace**, otherwise click **Done** (not shown).



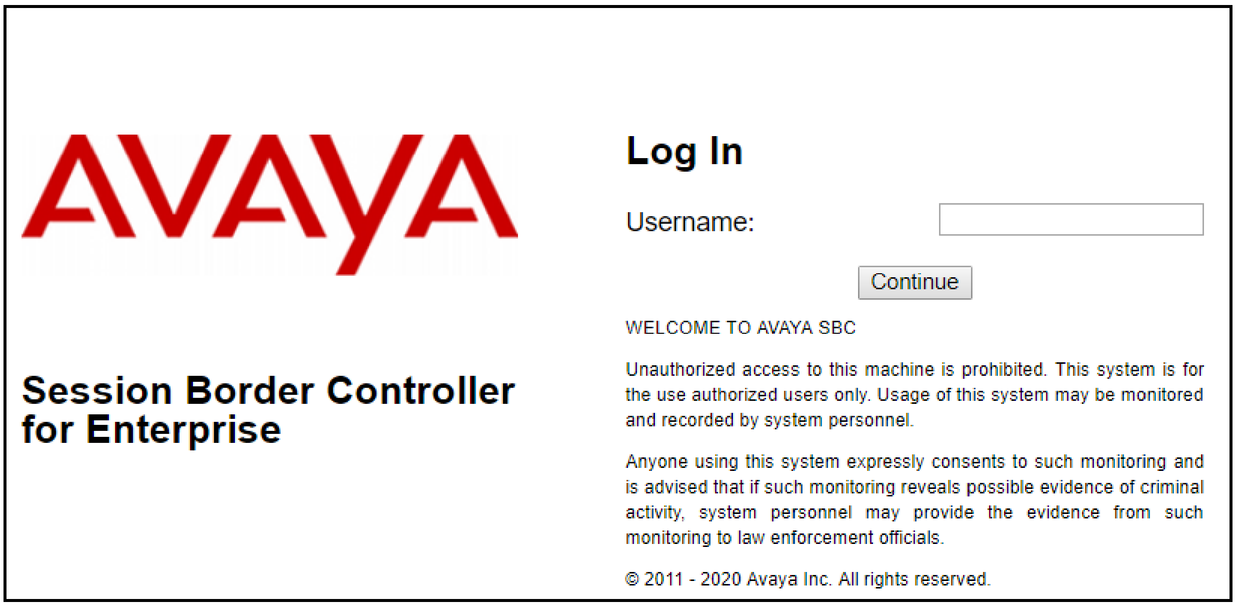
8. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **References** section.

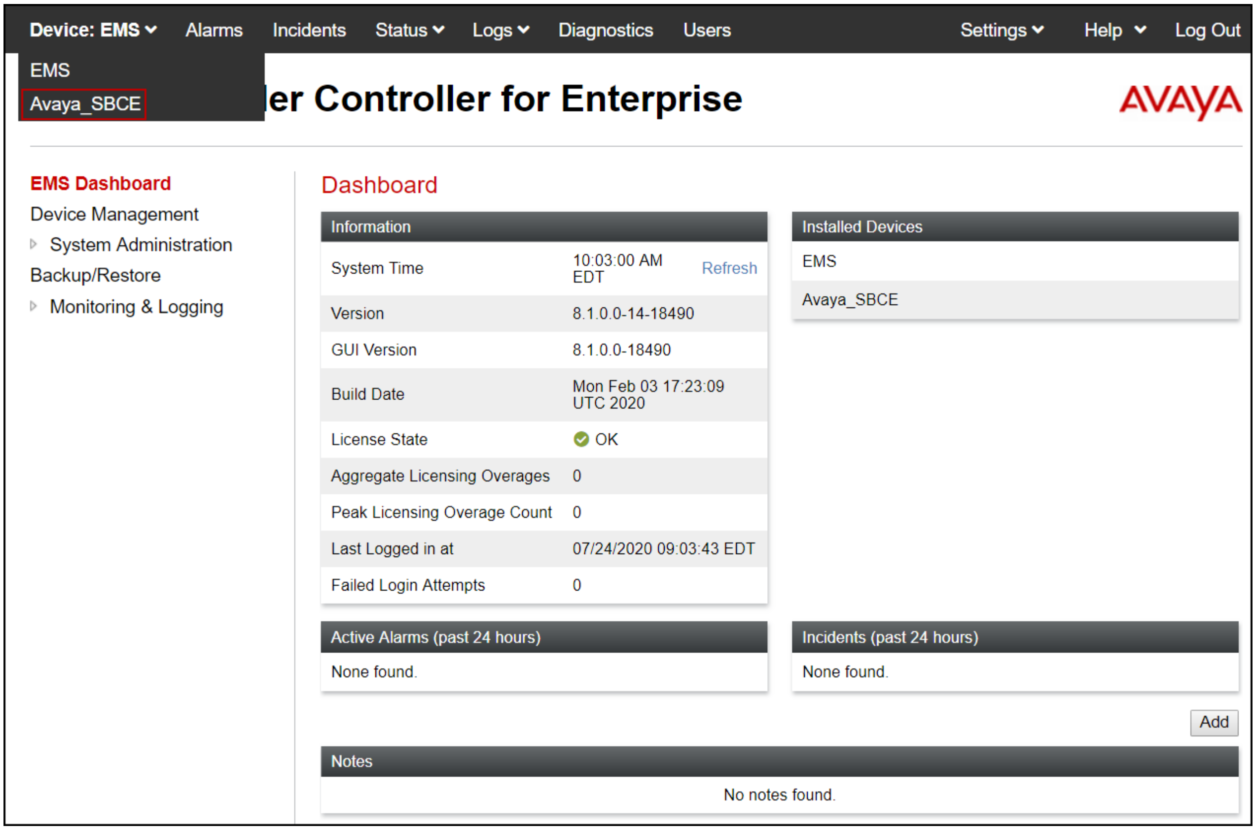
Some screens capture will show the use of the **Edit** command instead of the **add** command, since the configuration used for the testing was previously added.

8.1. System Access

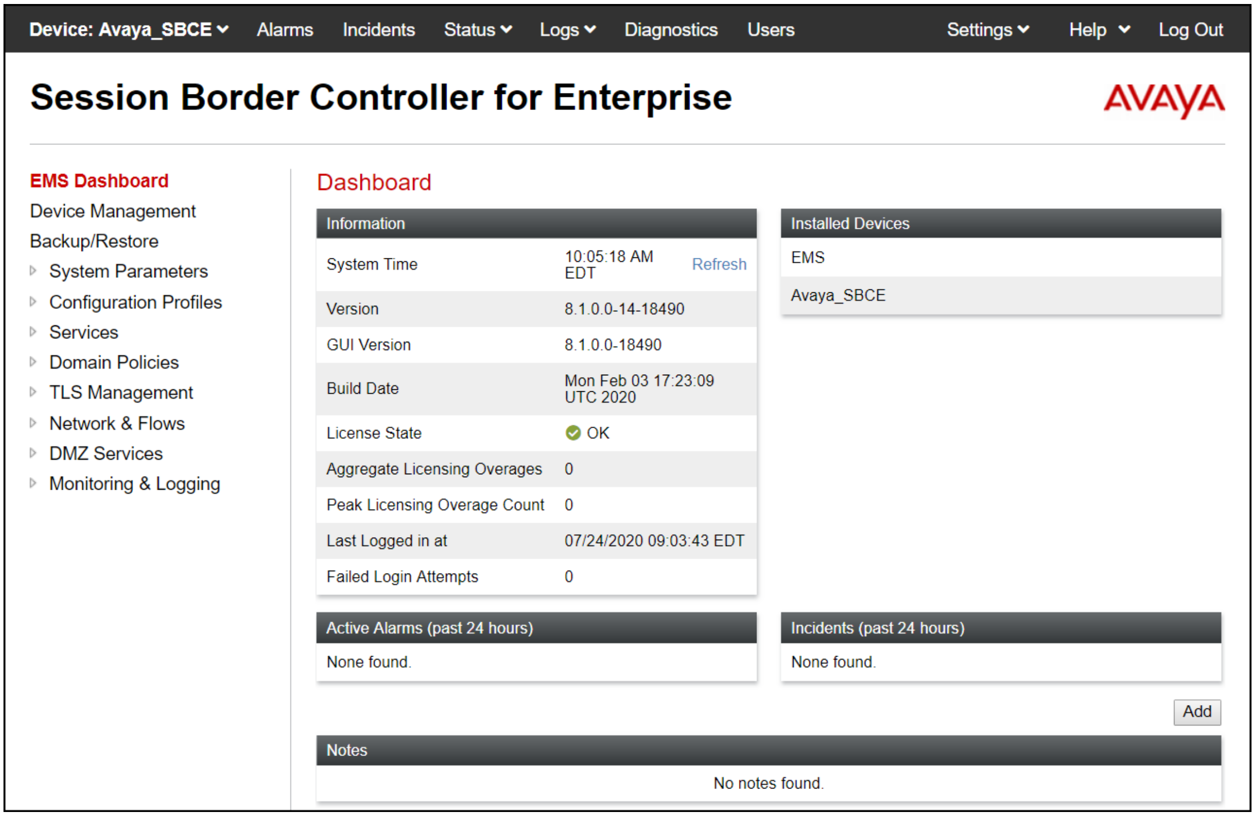
Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



Once logged in, on the top left of the screen, under **Device**: select the device being managed, ***Avaya_SBCE*** in the sample configuration.

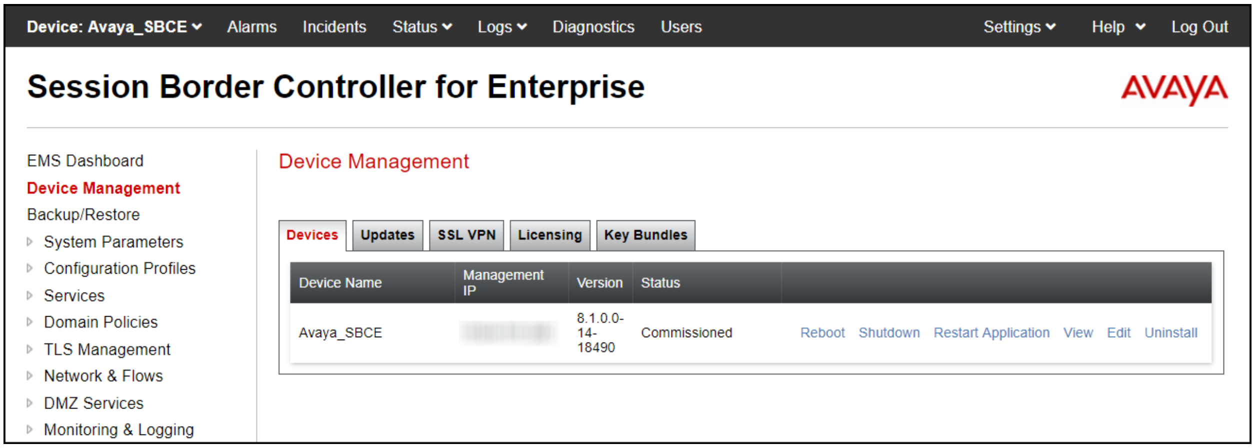


The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

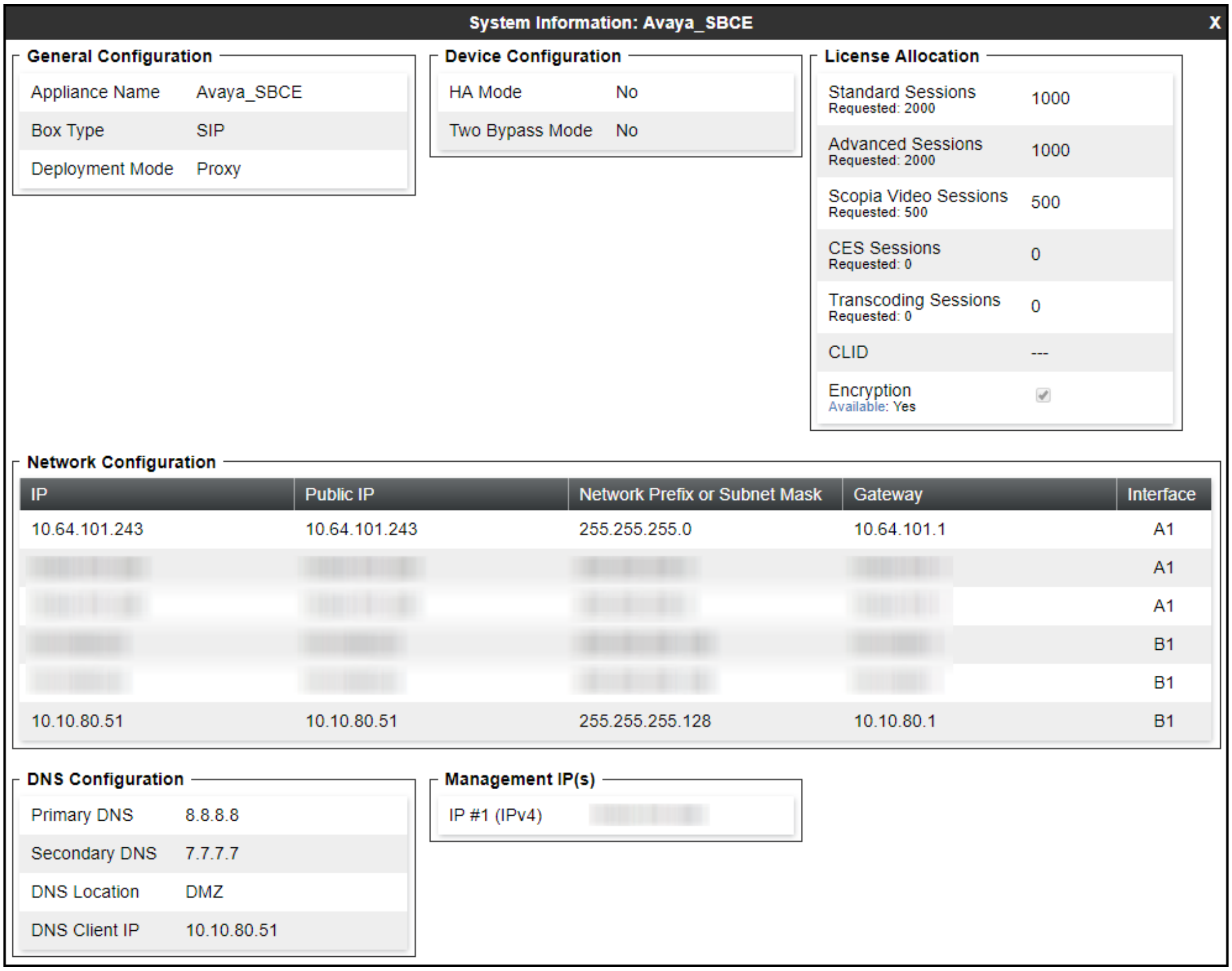


8.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named ***Avaya_SBCE*** is shown. The management IP address that was configured during installation is blurred out for security reason; the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is ***Commissioned***, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



To view the network configuration assigned to the Avaya SBCE, click **View** on the screen shown above. The **System Information** window is displayed, containing the current device configuration and network settings. Note that **DNS configuration** is required for this solution. The DNS information can be added by clicking on **Edit** shown on the previous screen.



The IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to the service provider and are the ones relevant to these Application Notes. The other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces that are blurred out are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (***10.64.101.243***) was used to connect to the enterprise network, while its public interface (***10.10.80.51***) was used to connect to the public network. See **Figure 1**.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

8.3. TLS Management

Note – Testing was done with System Manager signed identity certificates to enable TLS encryption inside of the enterprise (private network side). Also, testing was done with identity certificates signed by a 3rd party trusted certificate authority (CA) for enhanced security to enable TLS encryption outside of the enterprise (public network side). The procedure to create/obtain the required TLS certificates is outside the scope of these Application Notes and it's not discussed in these Application Notes.

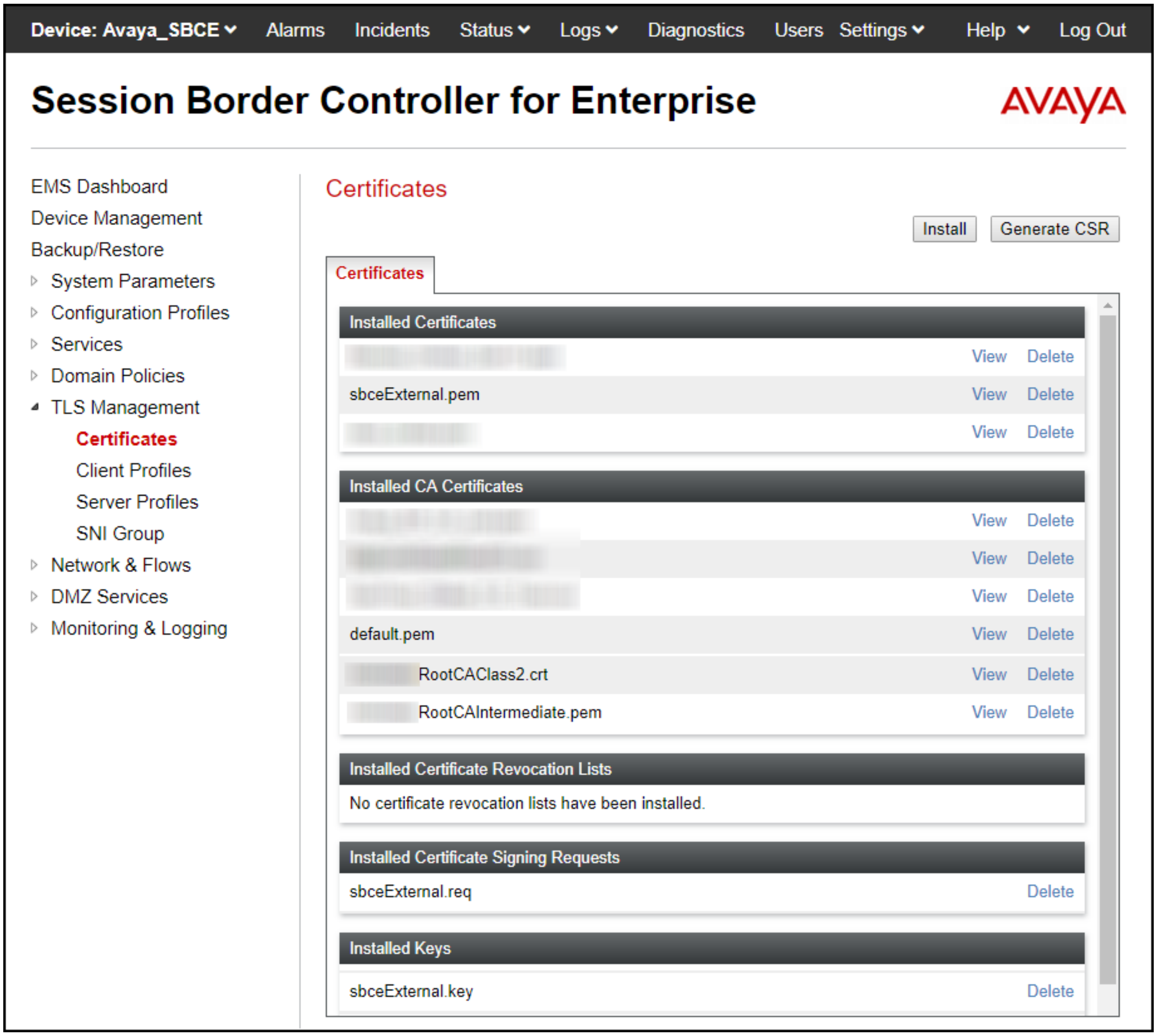
The following procedures show how to create the client and server profiles to support TLS encryption in the Avaya SBCE.

8.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

Once logged in, on the top left of the screen, under **Device**: select the device being managed, ***Avaya_SBCE*** in the sample configuration.

Step 1 - Select **TLS Management → Certificates** from the left-hand menu. Verify the following:

- Verify the System Manager Root CA certificate is present in the **Installed CA Certificates** area, this certificate is required to enable TLS encryption inside of the enterprise (private network side). This Root CA certificate needs to be manually downloaded from System Manager and installed in the Avaya SBCE; this Root CA certificate doesn't come pre-loaded in the Avaya SBCE. Certificates from a 3rd party trusted Certificate Authority (CA) could be used for TLS encryption inside of the enterprise (private network side) instead of using Avaya System Manager as the Certificate Authority.
- Verify the Root CA certificates for the trusted certificate authority being used by the Service Provider are present in the **Installed CA Certificates** area, required to enable TLS encryption outside of the enterprise (public network side). These Root CA certificates need to be manually loaded/installed in the Avaya SBCE; these Root CA certificates don't come pre-loaded in the Avaya SBCE. The Service Provider (Avaya) could provide the Root CA certificates to the customer or the customer can download them directly from the 3rd party trusted Certificate Authority web/home page. The name of the 3rd party trusted Certificate Authority will be required when downloading from the 3rd party trusted Certificate Authority web/home page. The Service provider (Avaya) can guide the customer on how to obtain the necessary certificates.
- Verify the identity certificate signed by the System Manager CA is present in the **Installed Certificates** area.
- Verify the Private key associated with the identity certificate signed by the System Manager CA is present in the **Installed Keys** area.


Device: Avaya_SBCE
Alarms
Incidents
Status
Logs
Diagnostics
Users
Settings
Help
Log Out
Session Border Controller for Enterprise
AVAYA
EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Certificates
Client Profiles
Server Profiles
SNI Group
Network & Flows
DMZ Services
Monitoring & Logging
Certificates
Install
Generate CSR
Certificates
Installed Certificates
View Delete
sbceExternal.pem
View Delete
View Delete
Installed CA Certificates
View Delete
View Delete
View Delete
default.pem
View Delete
RootCAClass2.crt
View Delete
RootCAIntermediate.pem
View Delete
Installed Certificate Revocation Lists
No certificate revocation lists have been installed.
Installed Certificate Signing Requests
sbceExternal.req
Delete
Installed Keys
sbceExternal.key
Delete

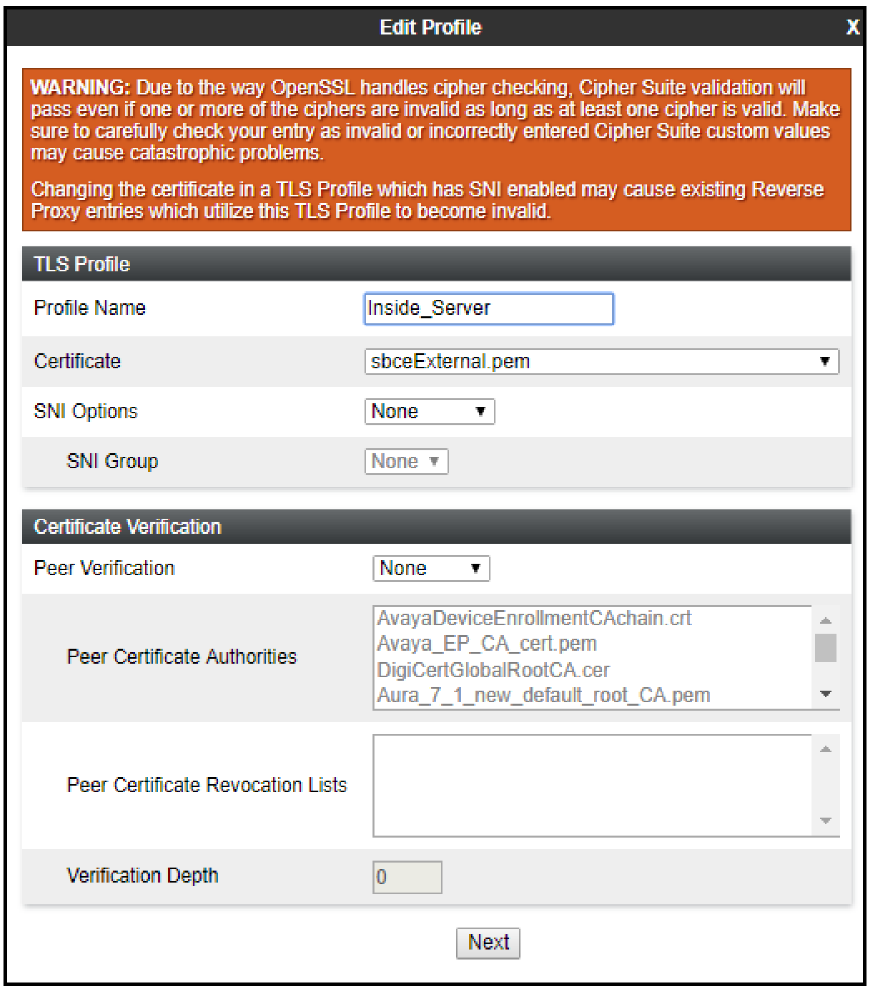
8.3.2. Server Profiles

8.3.2.1 Inside Server Profile

Step 1 - Select **TLS Management → Server Profiles** and click on **Add**. Enter the following:

- **Profile Name**: enter a descriptive name, ***Inside_Server*** was used.
- **Certificate**: select the identity certificate, e.g., ***sbceExternal.pem***, from the pull-down menu.
- **Peer Verification**: Select ***None***.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

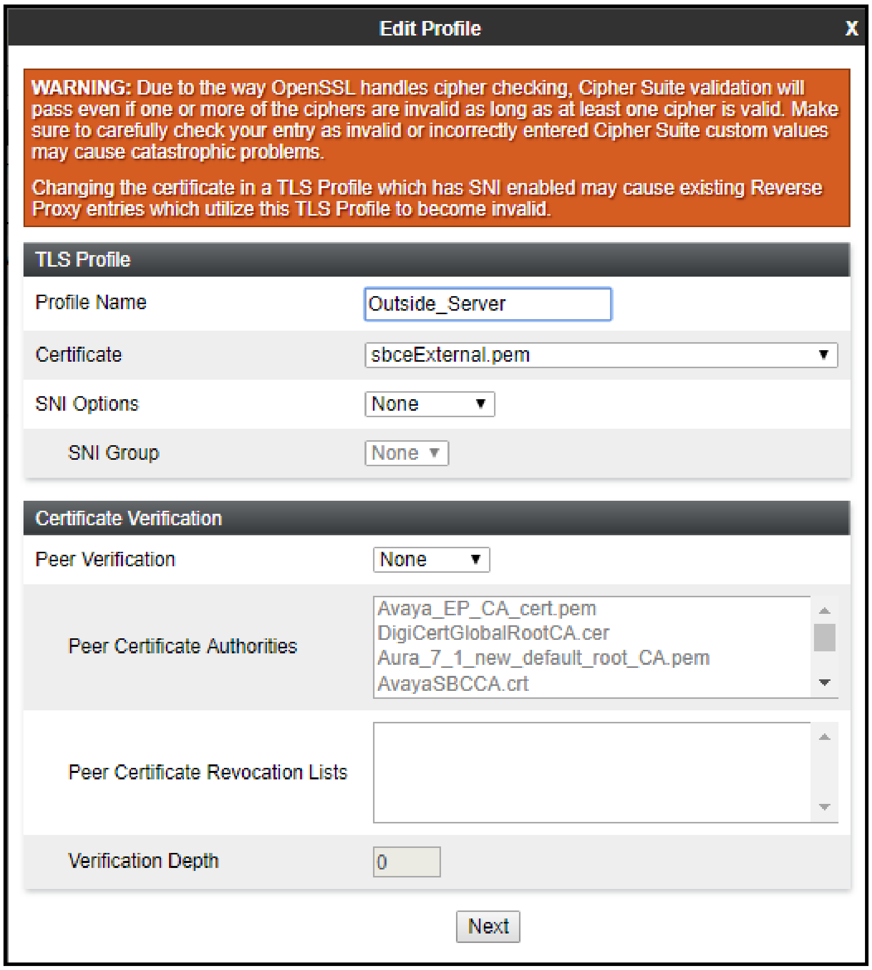


8.3.2.2 Outside Server Profile

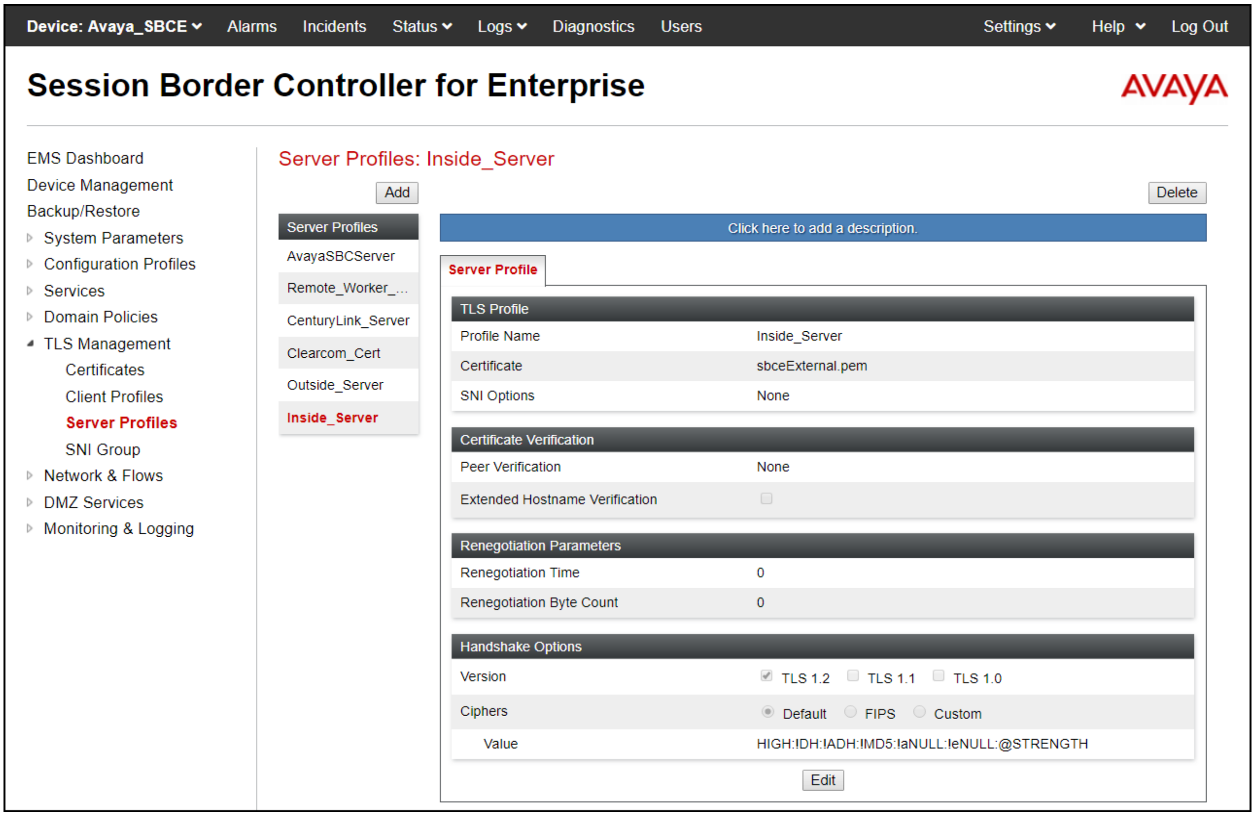
Step 1 - Select **TLS Management → Server Profiles** and click on **Add**. Enter the following:

- **Profile Name**: enter a descriptive name, ***Outside_Server*** was used.
- **Certificate**: select the identity certificate, e.g., ***sbceExternal.pem***, from the pull-down menu.
- **Peer Verification**: Select ***None*** from the pull-down menu.
- Click **Next**.

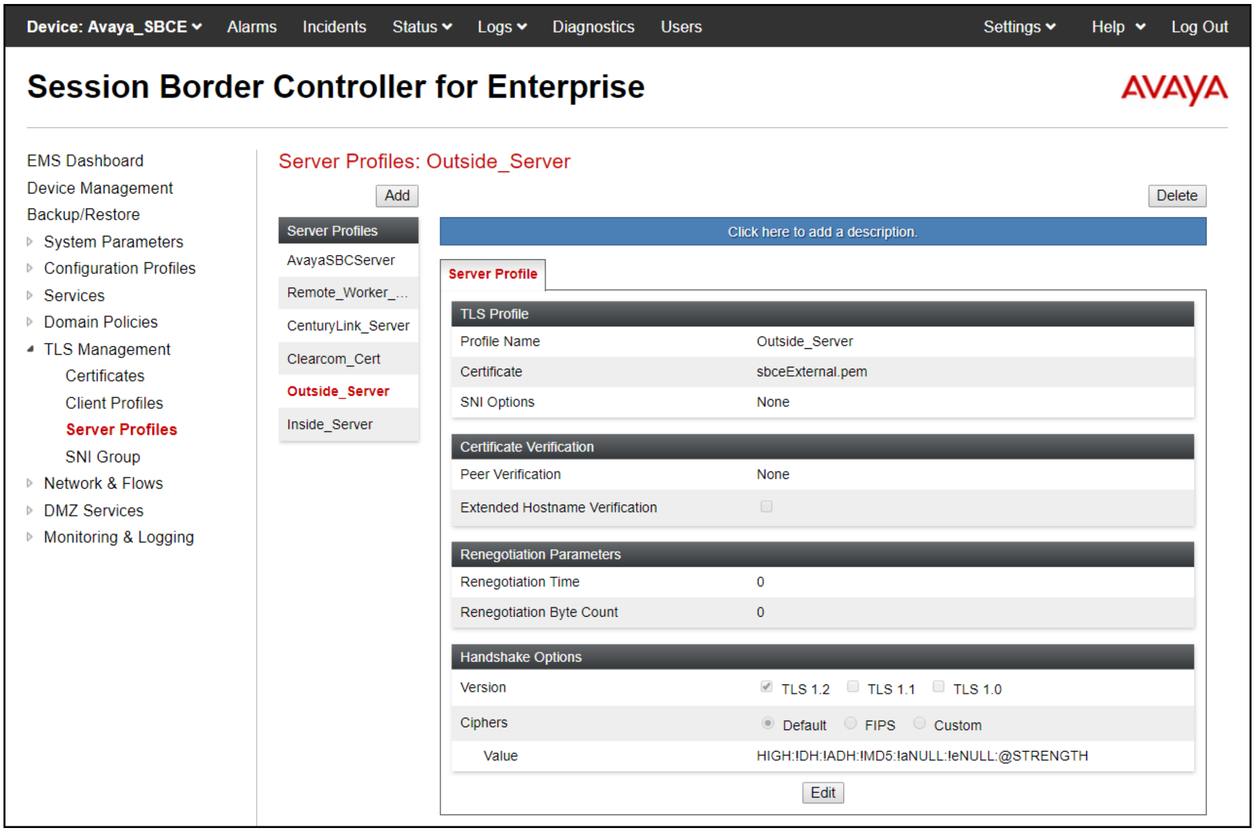
Step 2 - Accept default values for the next screen (not shown) and click **Finish**.



The following screen shows the completed ***Inside_Server*** profile form:



The following screen shows the completed ***Outside_Server*** profile form:



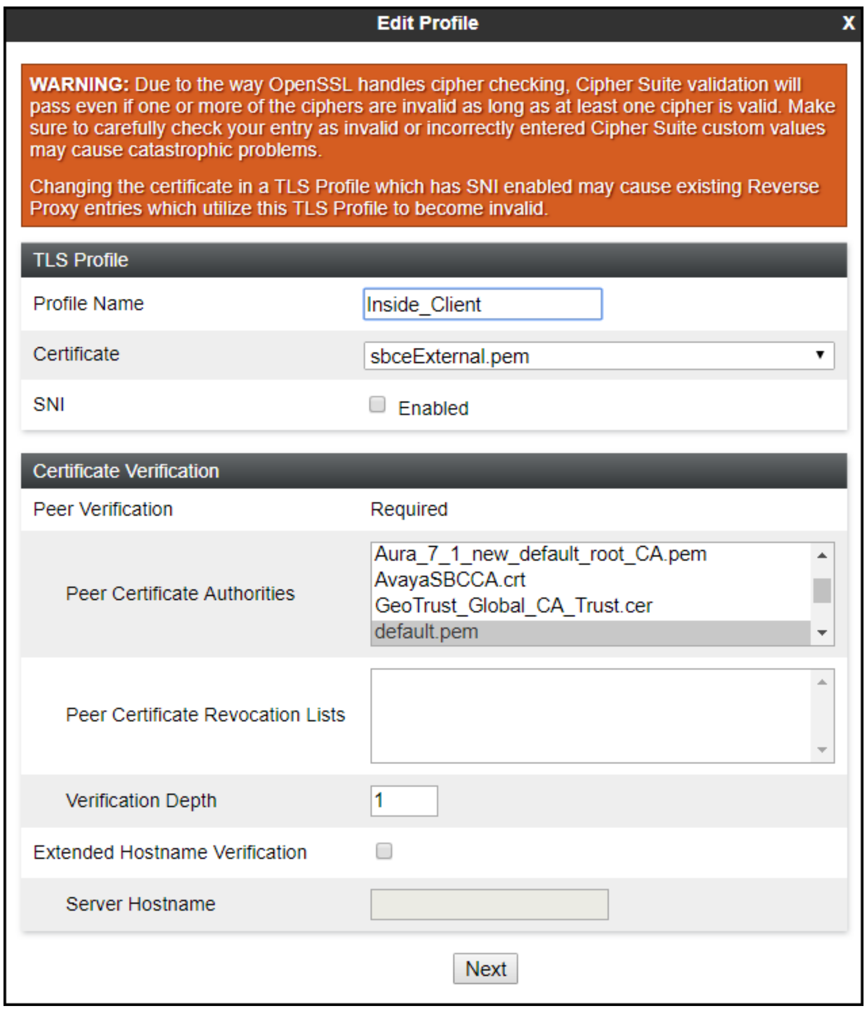
8.3.3. Client Profiles

8.3.3.1 Inside Client Profile

Step 1 - Select **TLS Management → Client Profiles** and click on **Add**. Enter the following:

- **Profile Name**: enter a descriptive name, ***Inside_Client*** was used.
- **Certificate**: select the identity certificate, e.g., ***sbceExternal.pem***, from the pull-down menu.
- **Peer Verification**: Select ***Required*** from the pull-down menu.
- **Peer Certificate Authorities**: select the Root CA certificate used to verify the identity certificate received from Session Manager, e.g., ***default.pem***.
- **Verification Depth**: enter ***1***.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

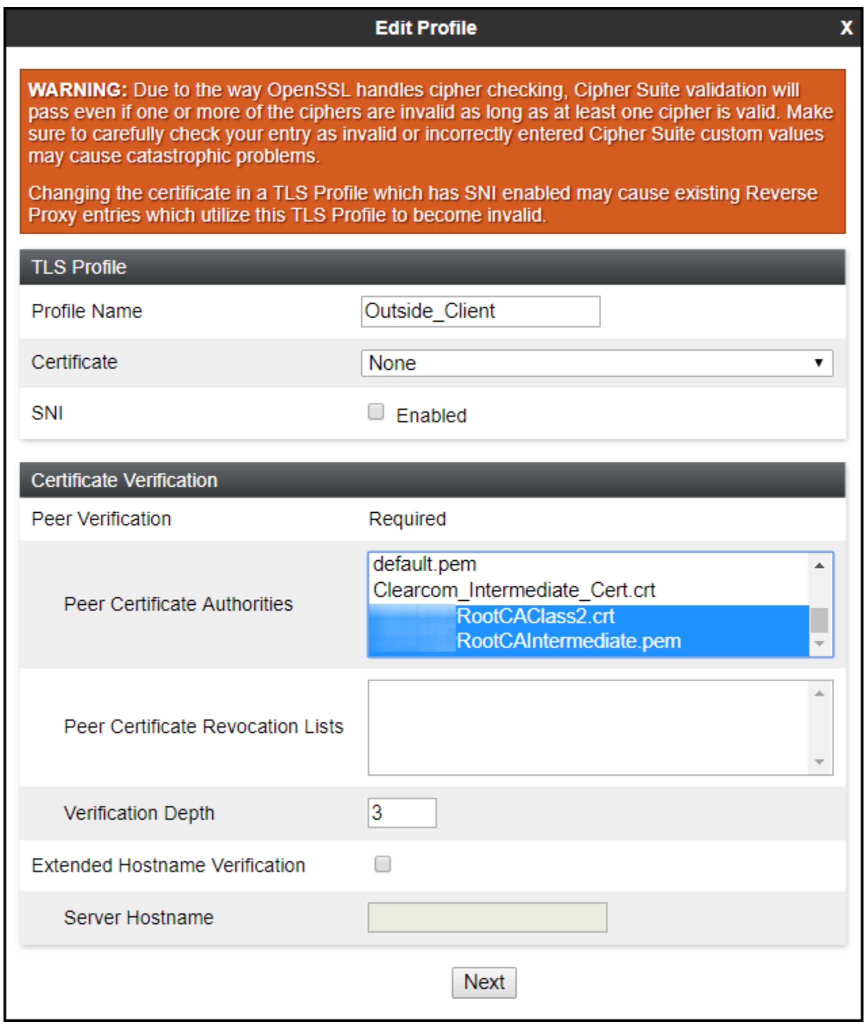


8.3.3.2 Outside Client Profile

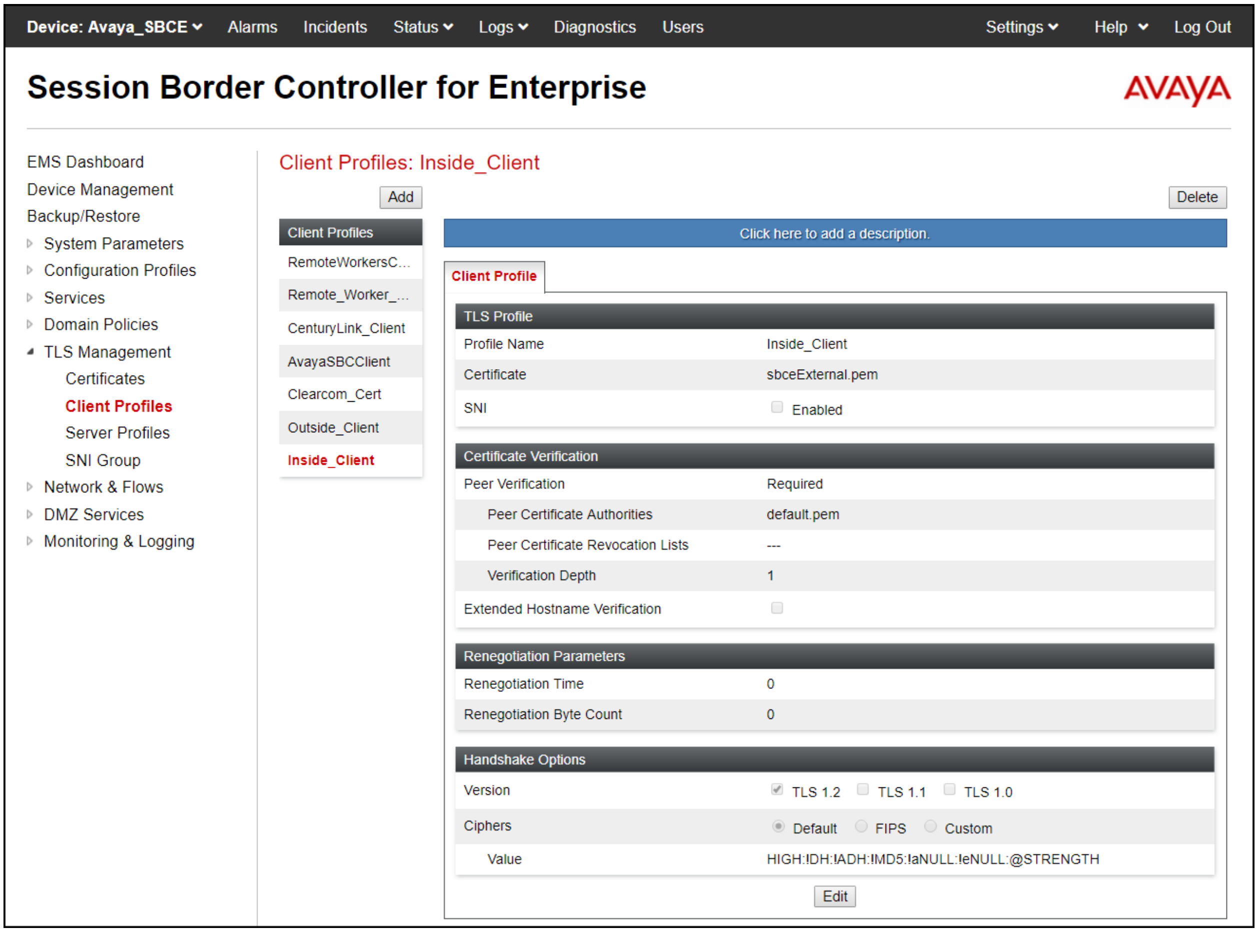
Step 1 - Select **TLS Management → Client Profiles** and click on **Add**. Enter the following:

- **Profile Name**: enter a descriptive name, ***Outside_Client*** was used.
- **Certificate**: select **None** from the pull-down menu.
- **Peer Verification**: ***Required*** from the pull-down menu.
- **Peer Certificate Authorities**: select the Root CA certificates used to verify the identity certificate received from the Service Provider, e.g., ***mycacertRootCAClass2.crt*** and ***mycacertRootCAIntermediate.pem***. (Note: for security reasons fictitious certificate names were given).
- **Verification Depth**: enter ***3***.
- Click **Next**.

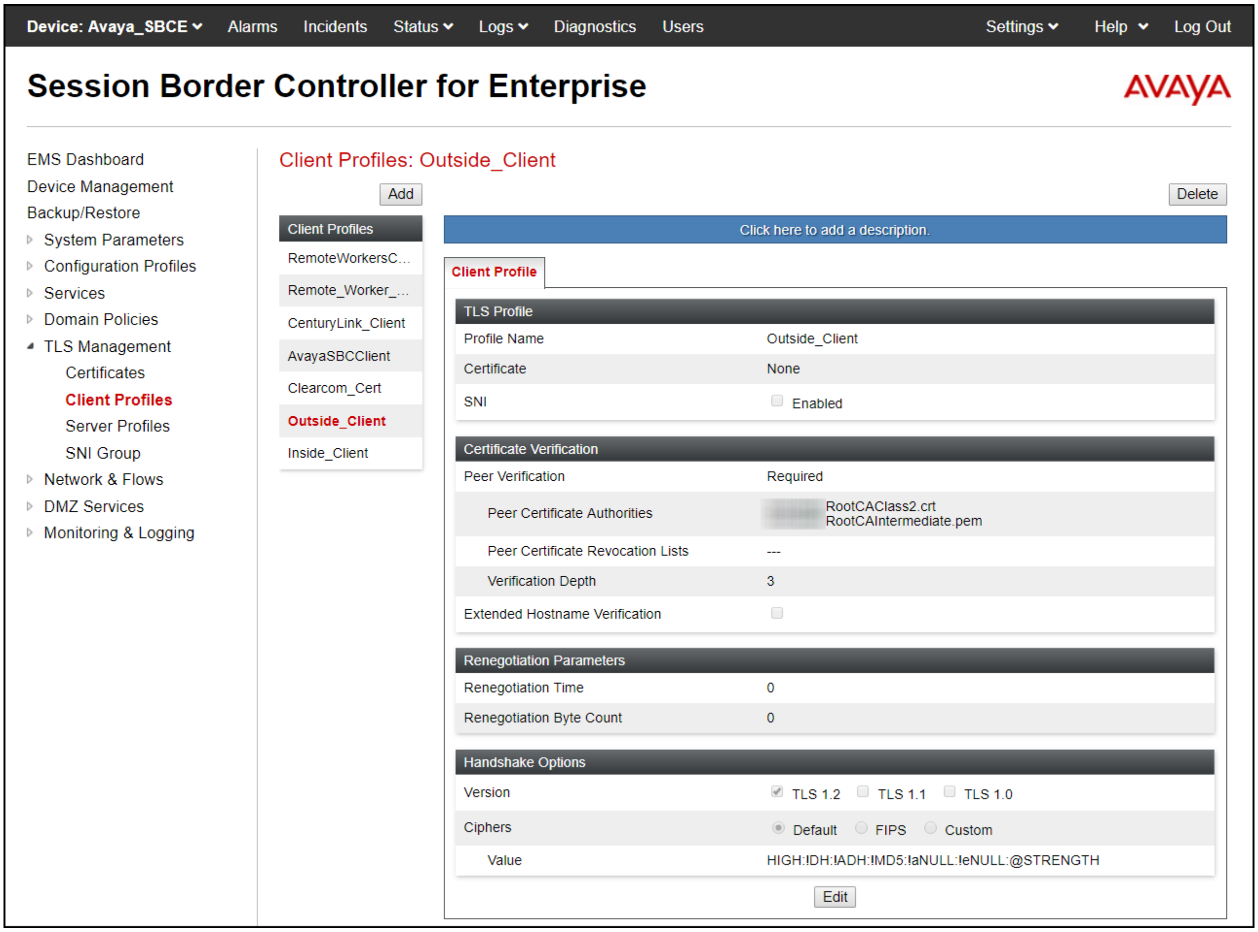
Step 2 - Accept default values for the next screen (not shown) and click **Finish**.



The following screen shows the completed ***Inside_Client*** profile form:



The following screen shows the completed ***Outside_Client*** profile form:

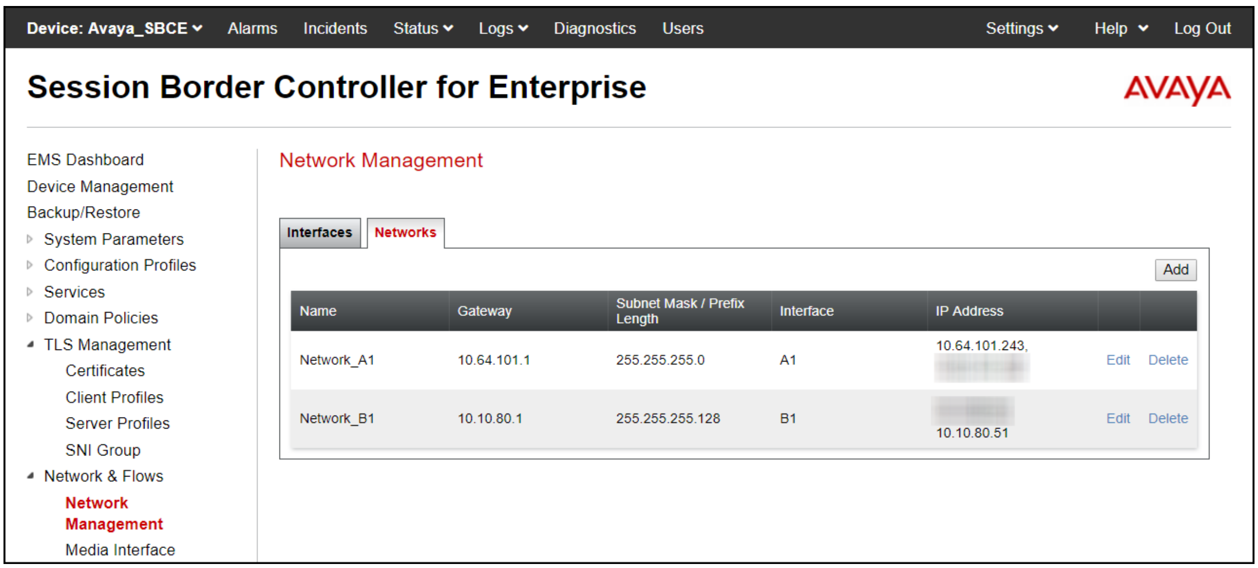


8.4. Network Management

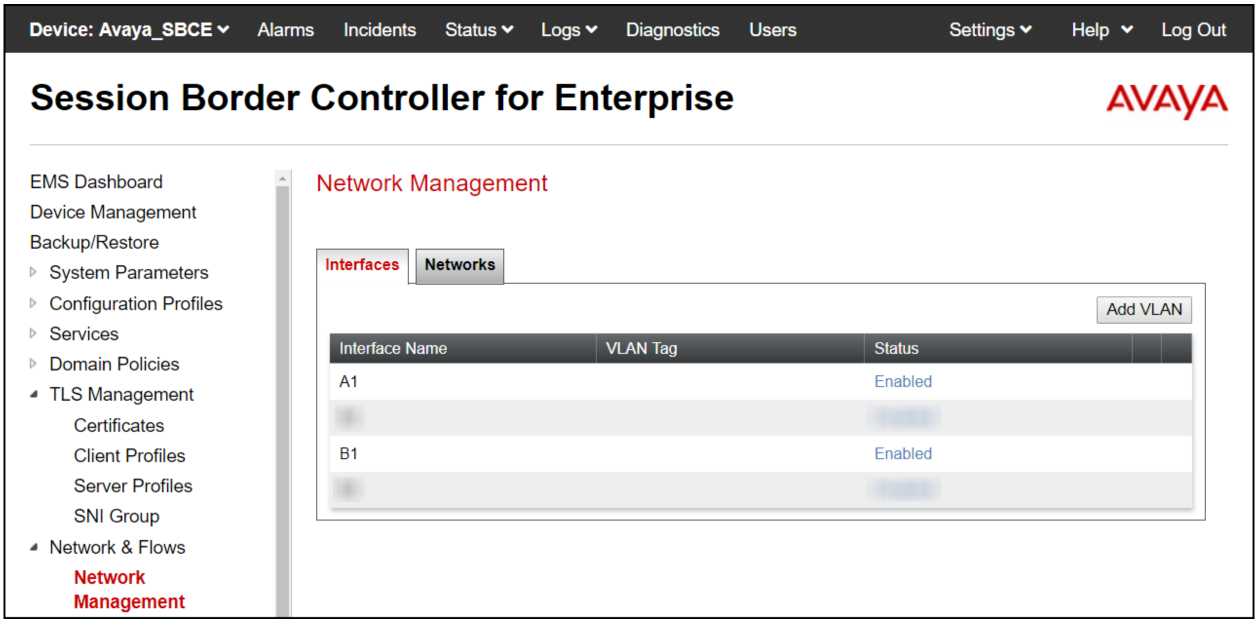
The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from the **Network & Flows** on the left-side menu. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (***10.64.101.243***) and public (***10.10.80.51***) sides of the Avaya SBCE are the ones relevant to these Application Notes.



On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B1** interfaces. Click the buttons under the **Status** column if necessary, to enable the interfaces.

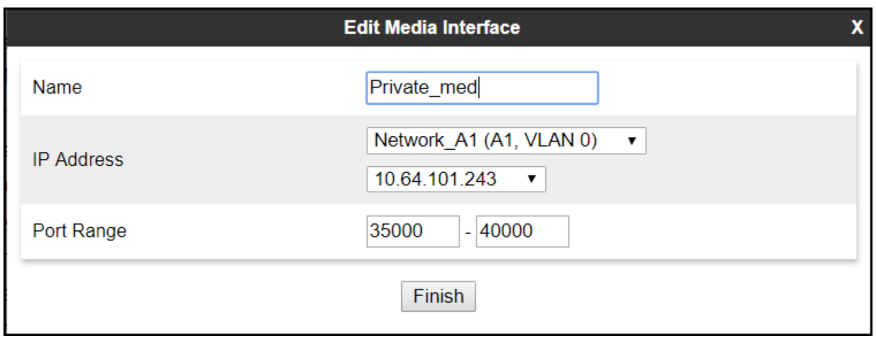


8.5. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

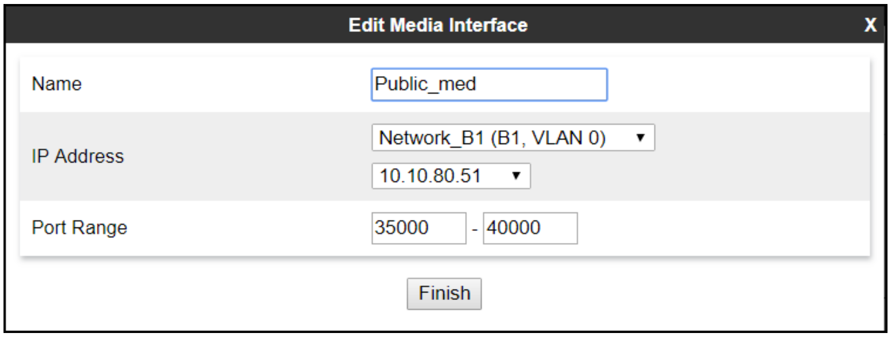
To add the Media Interface in the enterprise direction, select **Media Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface, in the example ***Private_med*** was used.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of ***35000-40000***.
- Click **Finish**.



A Media Interface facing the public side was similarly created with the name ***Public_med***, as shown below.

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values.
- Click **Finish**.

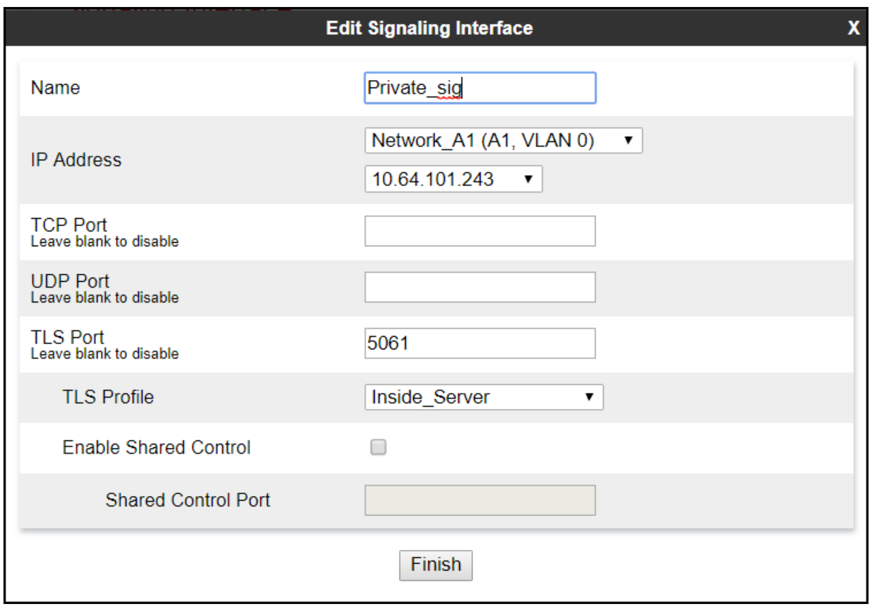


8.6. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

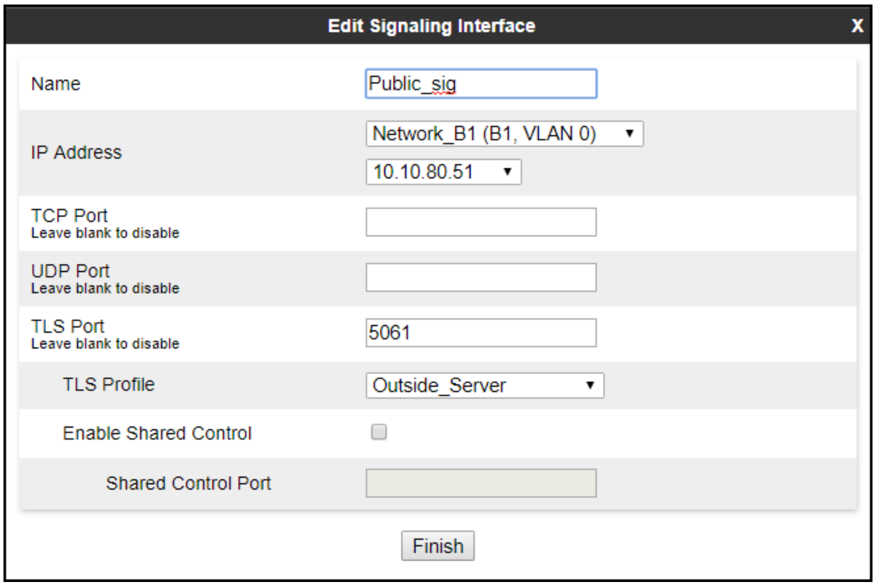
To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface, in the example ***Private_sig*** was used.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter ***5061*** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 7.6**.
- Select the **TLS Server Profile** defined in **Section 8.3.2.1**.
- Click **Finish**.



A second Signaling Interface with the name ***Public_sig*** was similarly created in the service provider's direction.

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter ***5061*** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from the service provider in the sample configuration.
- Select the **TLS Server Profile** defined in **Section 8.3.2.2**.
- Click **Finish**.

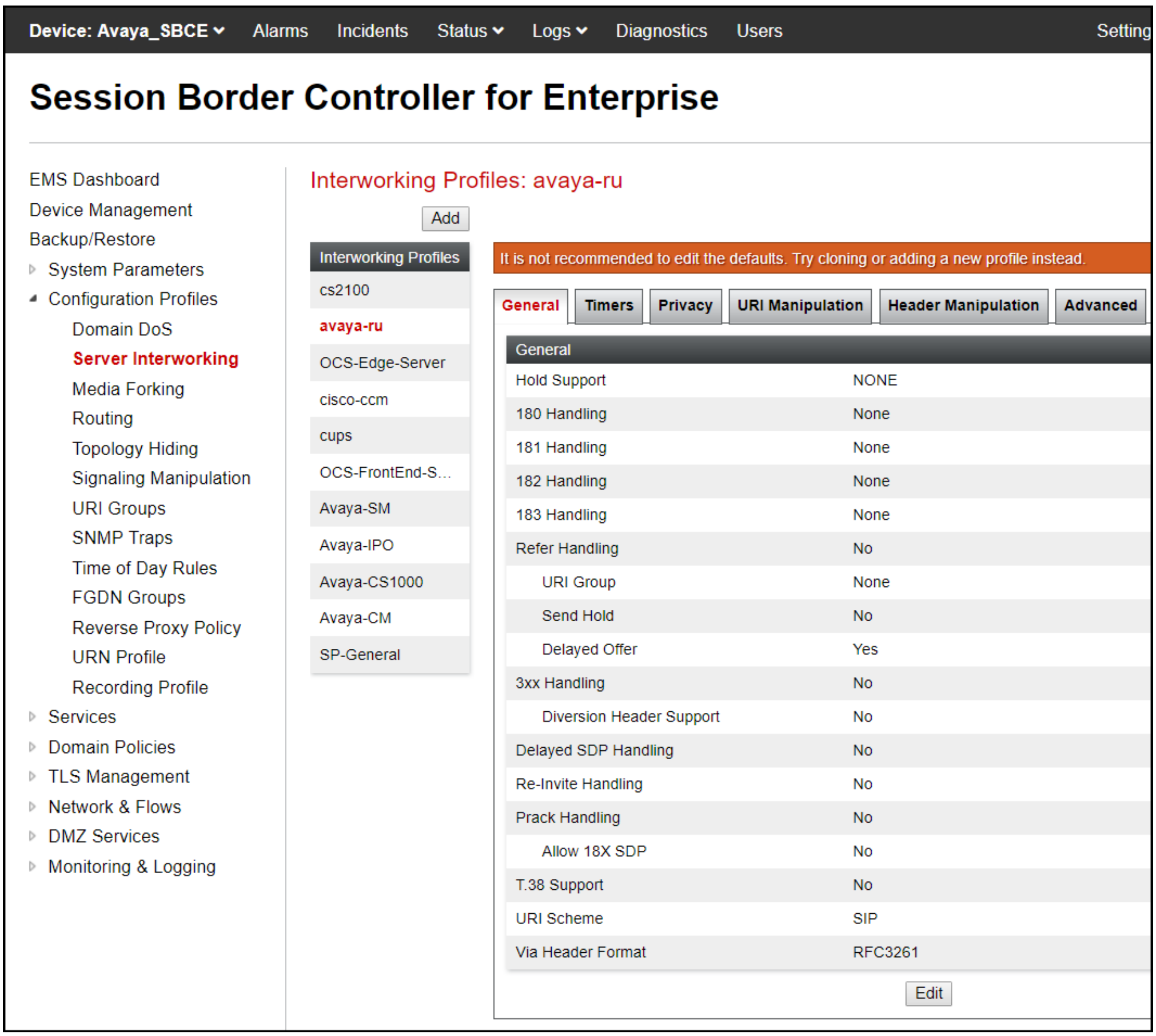


8.7. Server Interworking

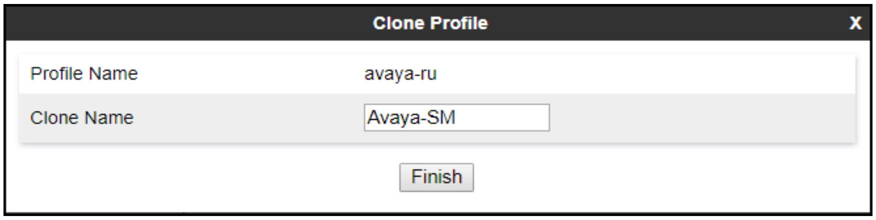
Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

8.7.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Configuration Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select ***avaya-ru*** from the list of pre-defined profiles. Click **Clone** (not shown).



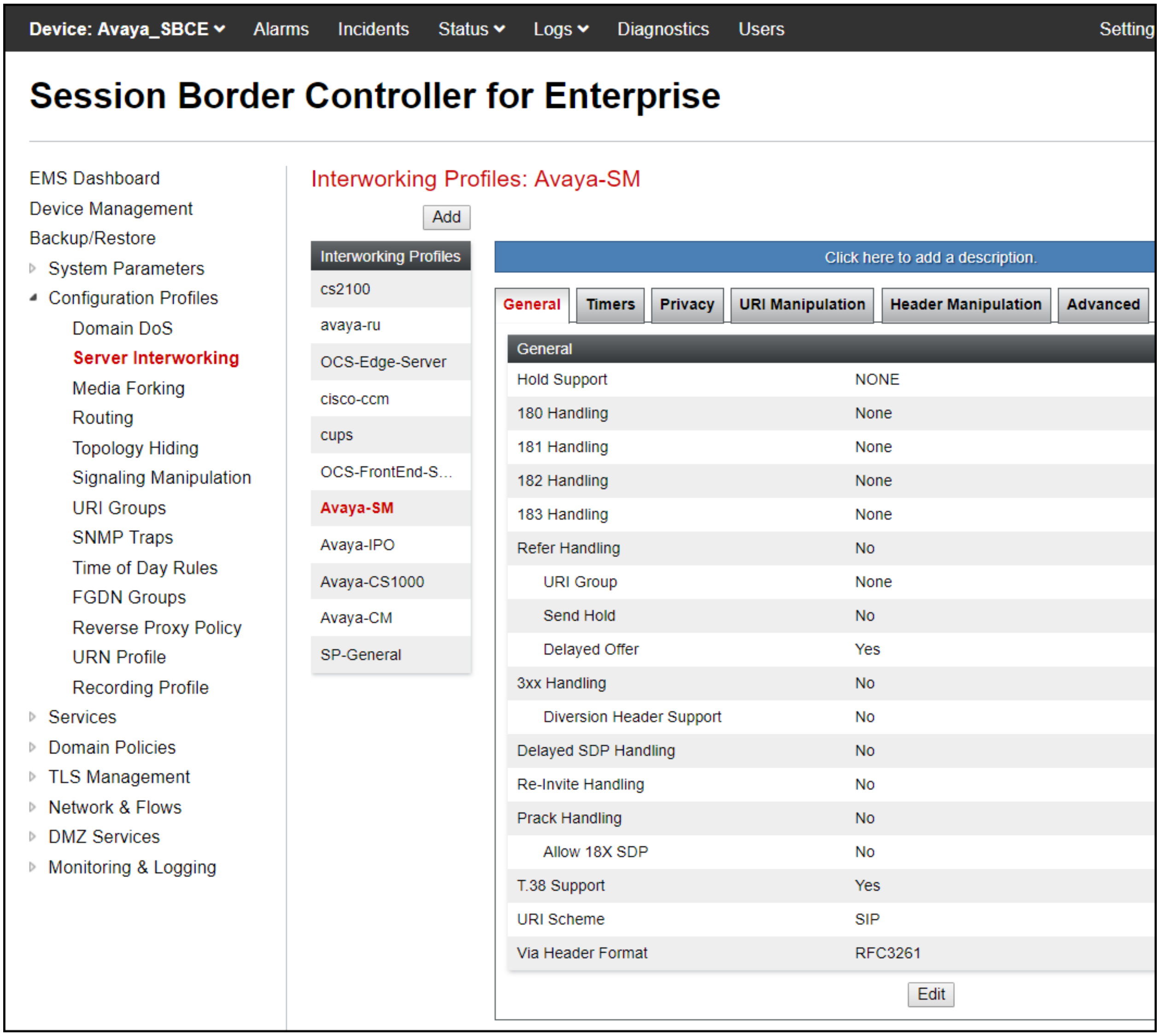
- Enter a descriptive name for the cloned profile.
- Click **Finish**.



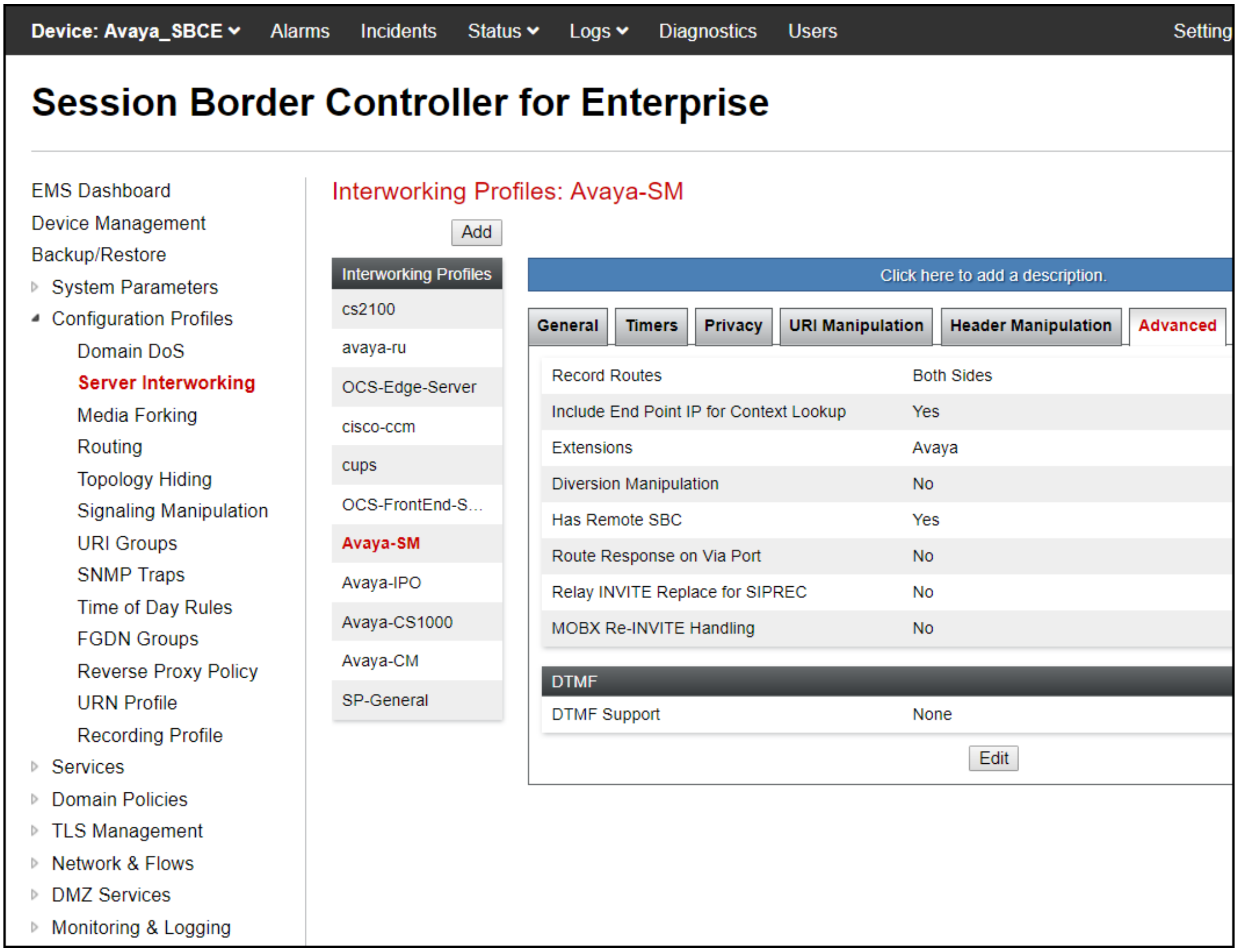
Click **Edit** on the newly cloned ***Avaya-SM*** interworking profile:

- On the **General** tab, check ***T.38 Support***.
- Leave remaining fields with default values.
- Click **Finish**.

The **General** tab settings are shown on the screen below:



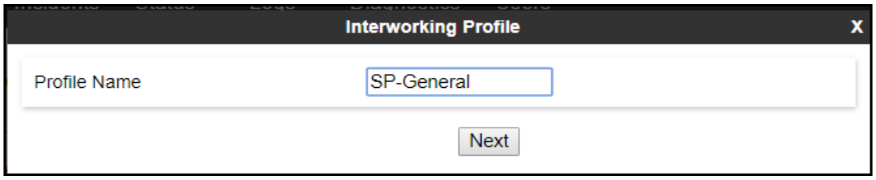
The **Advanced** tab settings are shown on the screen below:



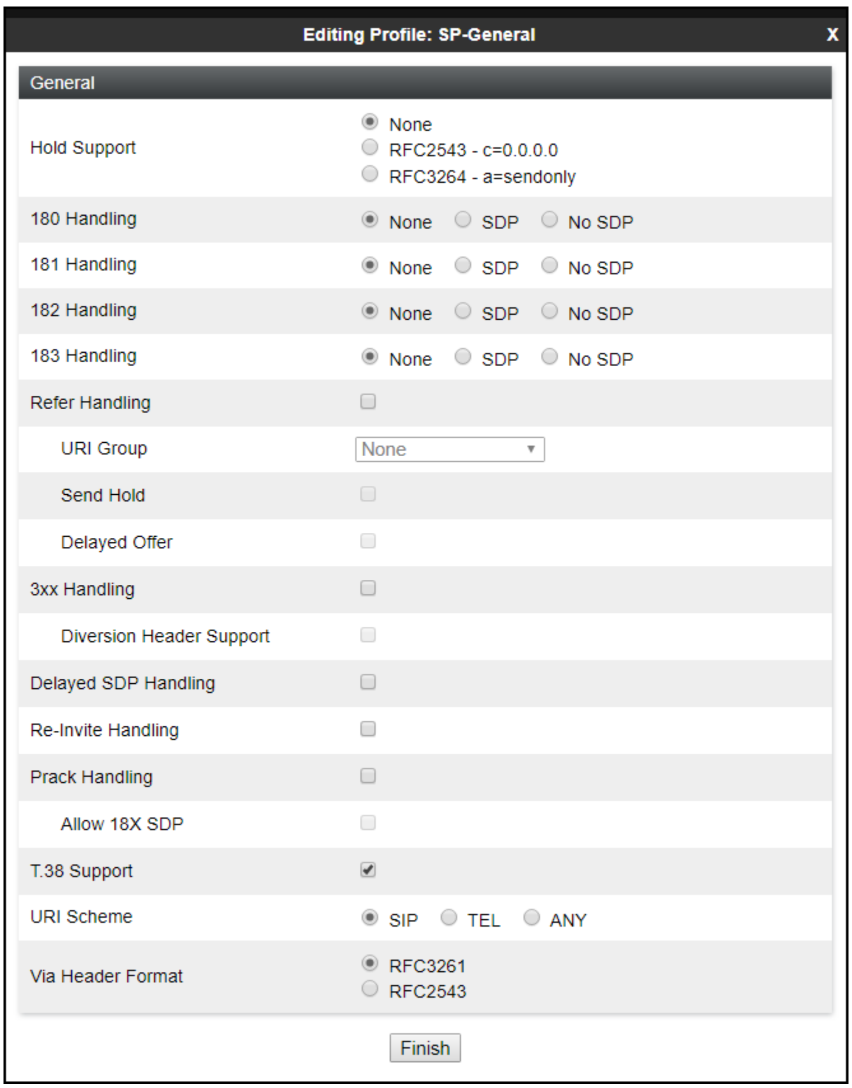
8.7.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Configuration Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown).

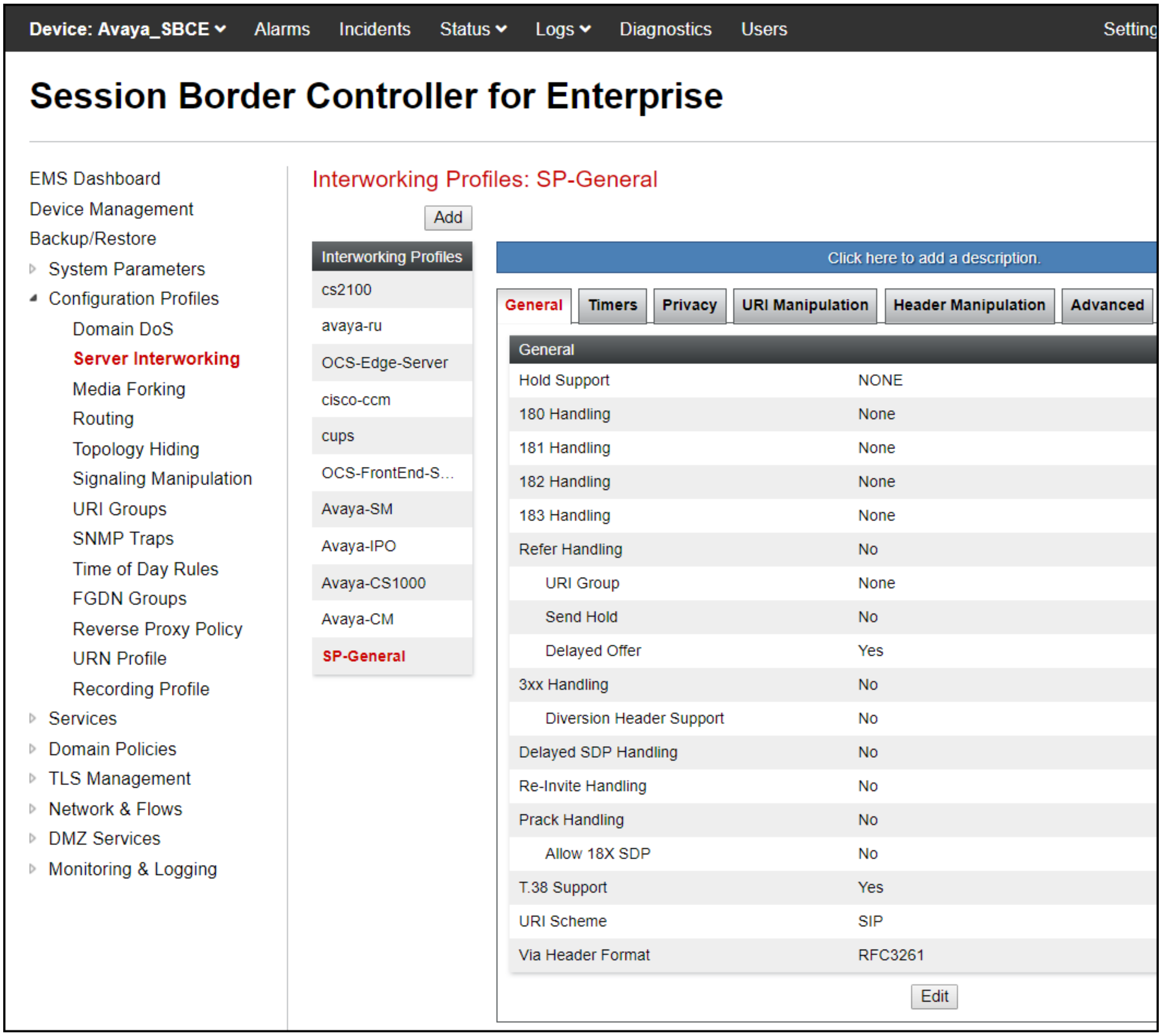
- Enter a descriptive name for the new profile.
- Click **Next**.



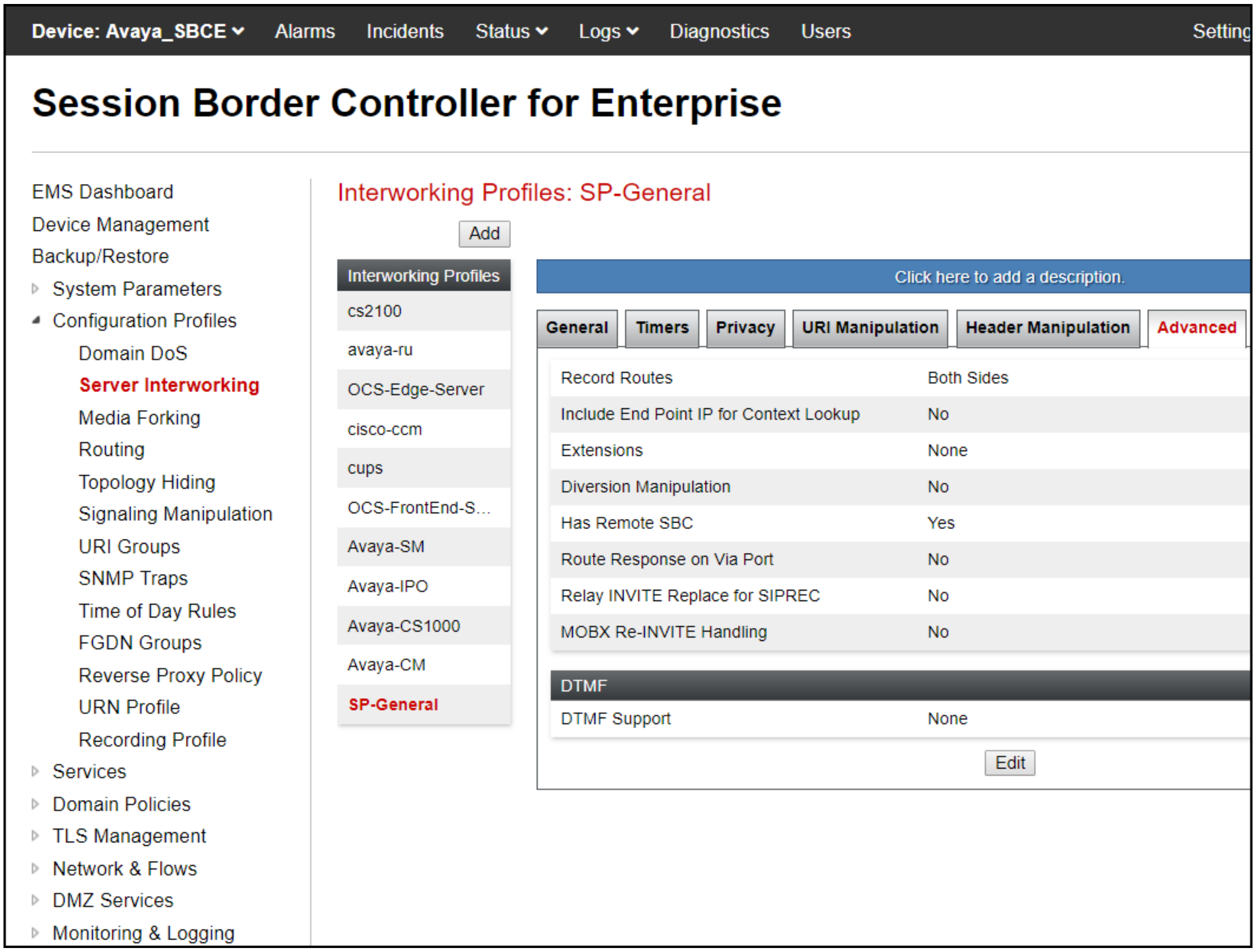
On the **General** tab, check ***T.38 Support***, click **Next** until the last tab is reached then click **Finish** on the last tab leaving remaining fields with default values (not shown).



The **General** tab settings are shown on the screen below:



The **Advanced** tab settings are shown on the screen below:



8.8. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult reference **[8]** in the **References** section for more information on this topic.

Sigma scripts were created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- Removes a=sendonly from re-INVITE message to correct an issue with Music On-Hold not playing when inbound calls are placed On-Hold.

- Remove unwanted “gsid” and “epv” parameter from being sent to the service provider in the Contact header.
- Remove the P-Location parameter from being sent to the service provider.
- Change the Diversion header scheme from SIPS to SIP in SIP messages sent to the service provider.
- Remove unwanted xml element information from the SDP in SIP messages sent to the service provider.
- Inserts "+" in the "To" and "Request-Line-URI" headers of SIP INVITE messages destined to the service provider to comply with E.164 numbering format. This change is required for calls from Experience Portal to the PSTN.

The scripts will later be applied to the Server Configuration Profiles corresponding to the Service Provider in **Section 8.9.2**.

To create the SigMa script to be applied to the Server Configuration Profile corresponding to the Service Provider, on the left navigation pane, select **Configuration Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name ***CPaaS_SigMa*** was chosen in this example.
- Copy the complete script from **Appendix B**.
- Click **Save**.

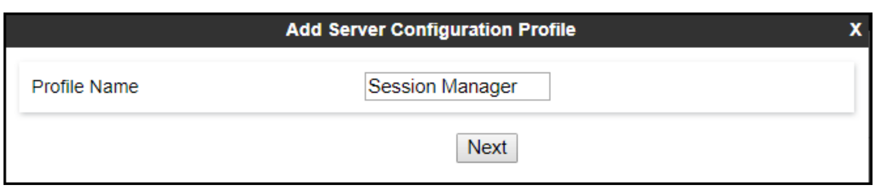
8.9. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and the service provider SIP Proxy (Trunk Server).

8.9.1. Server Configuration Profile – Enterprise

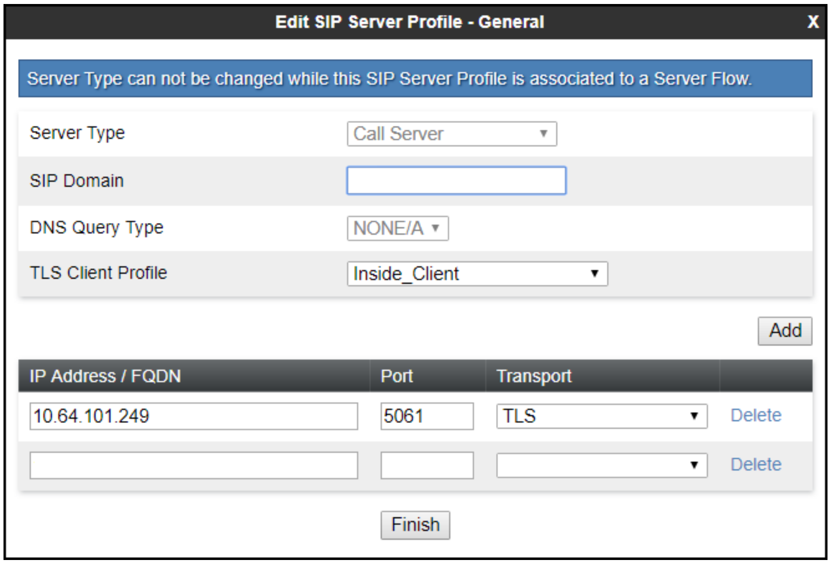
From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.

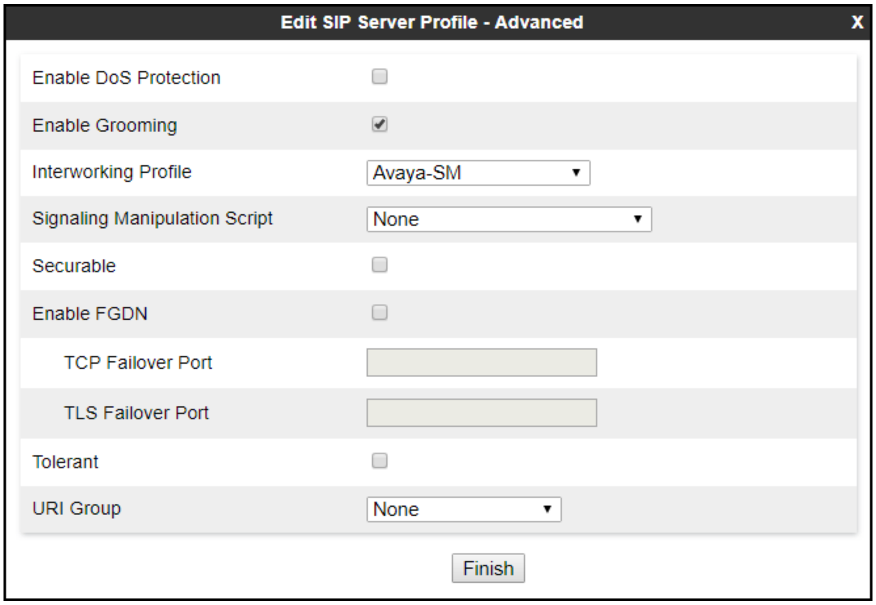


- On the **Edit SIP Server Profile – General** tab select ***Call Server*** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field**,** enter the IP address of the Session Manager Security Module (**Section 7.5)**.
- Enter ***5061*** under **Port** and select ***TLS*** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 7.6**.

- Select the **TLS Client Profile** defined in **Section 8.3.3.1.**
- Click **Next** (not shown).



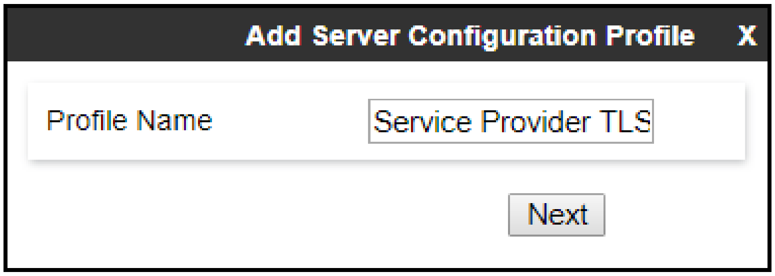
- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
  - Check ***Enable Grooming*** (required when TLS or TCP transports are used).
  - Select ***Avaya-SM*** from the **Interworking Profile** drop-down menu (**Section 8.7.1**).
- Click **Finish**.



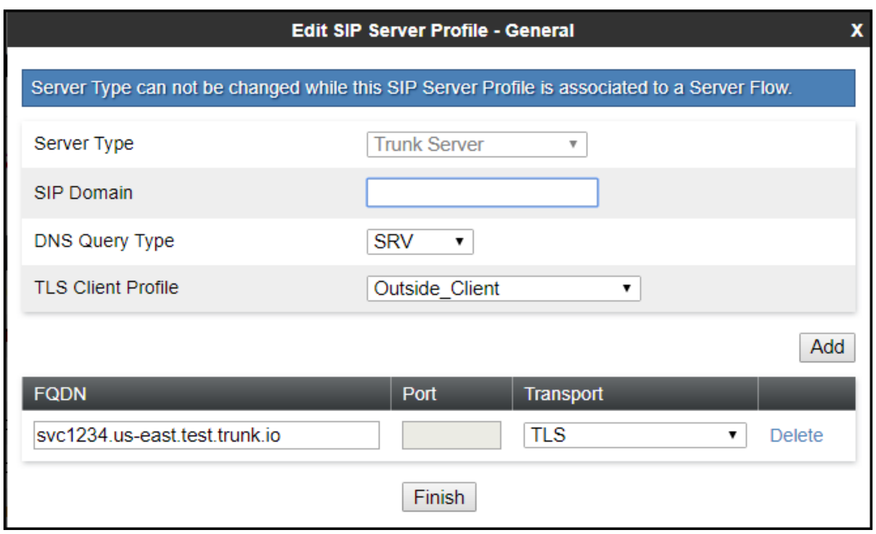
8.9.2. Server Configuration Profile – Service Provider

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below, ***Service Provider TLS*** was used.
- Click **Next**.

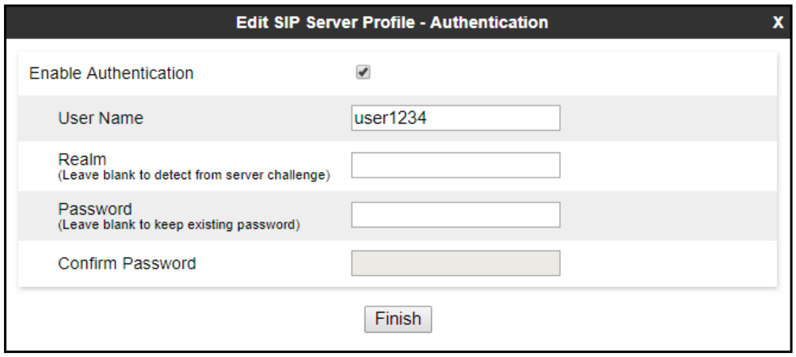


- On the **Edit Server Configuration Profile - General** Tab select ***Trunk Server*** from the drop-down menu for the **Server Type**.
- Select ***SRV*** from the drop-down menu for **DNS Query Type**.
- On the **IP Addresses / FQDN** field, enter ***svc1234.us-east.test.trunk.io*** (service provider's SIP proxy server FQDN used for DNS SRV record queries). This information should be provided by the service provider.
- Select ***TLS*** for **Transport** (note the port cannot be enter since SRV was selected for **DNS Query Type**, the port being used will be collected from the DNS response).
- Select the **TLS Client Profile** defined in **Section 8.3.3.2**.
- Click **Next** (not shown).



On the **Add SIP Server Profile - Authentication** tab:

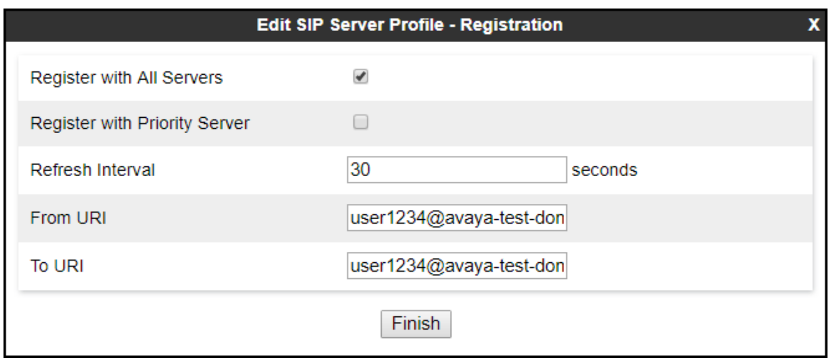
- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave the **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next** (not shown).



Click **Next** on the **Add Server Configuration Profile - Heartbeat** window (not shown).

On the **Add SIP Server Profile - Registration** tab:

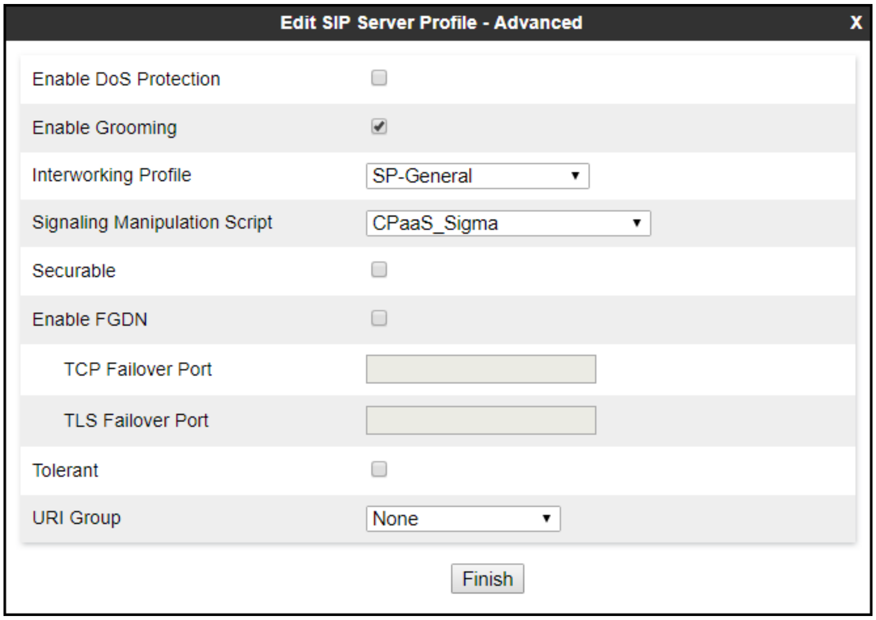
- Check the ***Register with All Servers*** box (***Register with Priority Server*** could also be used).
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the service provider Proxy Servers to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. ***30*** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI**: Use the **User Name** entered above in the **Authentication** screen (***user1234***) and the service provider's SIP Domain (***avaya-test-domain.sip.1234.io***), as shown in the screen below. This information should be provided by the service provider.
  - **To URI**: Use the **User Name** entered above in the **Authentication** screen (***user1234***) and the service provider's SIP Domain (***avaya-test-domain.sip.1234.io***), as shown in the screen below. This information should be provided by the service provider.
  - Click **Next** (not shown).



Click **Next** on the **Add SIP Server Profile - Ping** window (not shown).

On the **Add SIP Server Profile - Advanced** window:

- Check ***Enable Grooming*** (required when TLS or TCP transports are used).
- Select ***SP-General*** from the **Interworking Profile** drop-down menu (**Section 8.7.2)**.
- Select the ***CPaaS_SigMa*** from the **Signaling Manipulation Script** drop down menu (**Sections 8.8** and **14**).
- Click **Finish**.



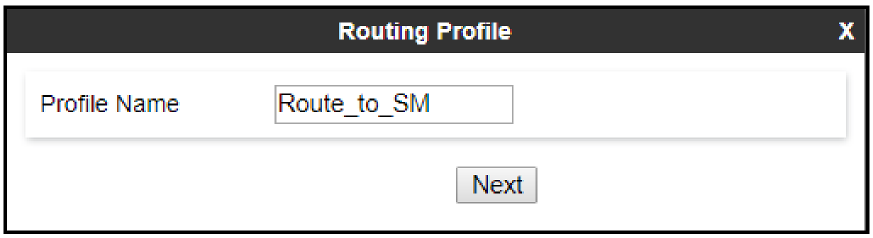
8.10. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the service provider SIP trunk.

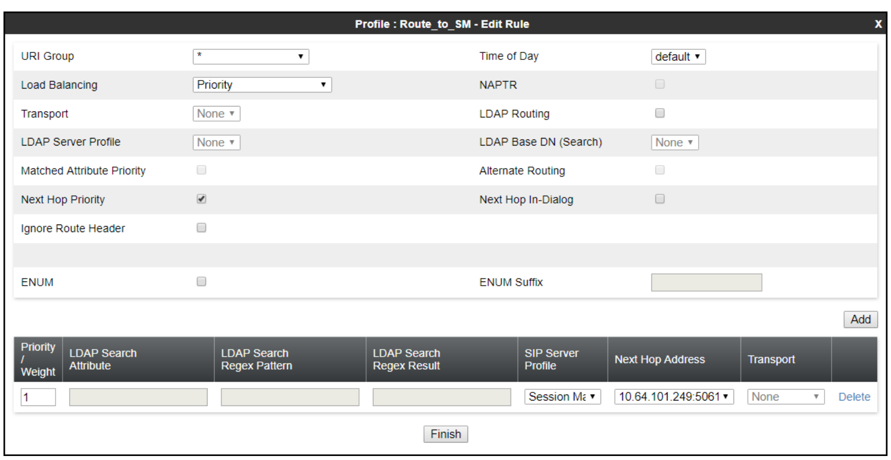
8.10.1. Routing Profile – Enterprise

To create the inbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



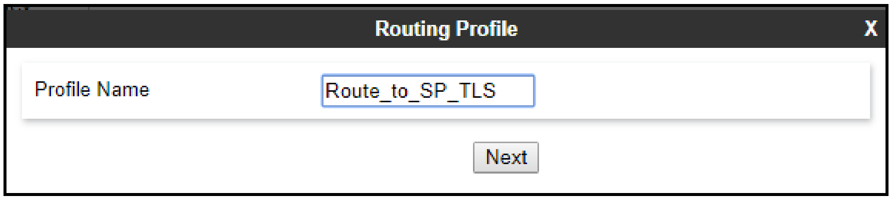
- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter ***1***.
- Under **SIP Server Profile**, select ***Session Manager***. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 8.9.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



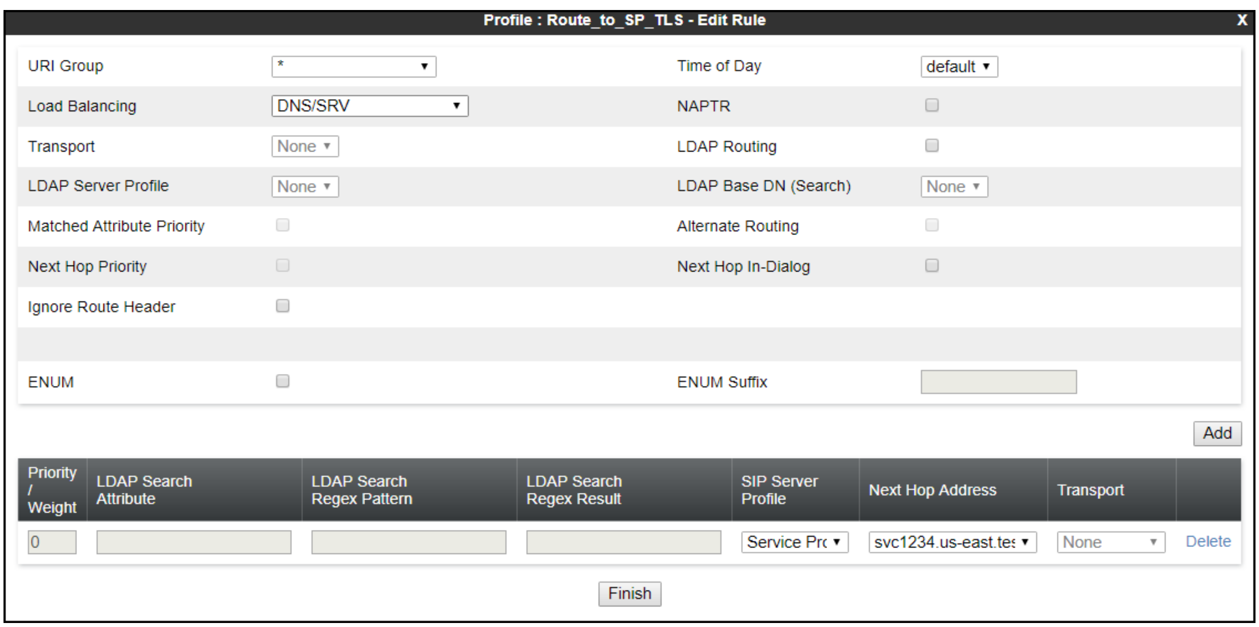
8.10.2. Routing Profile – Service Provider

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below, ***Route_to_SP_TLS*** was used.
- Click **Next**.



- Under **Load Balancing** select ***DNS/SRV***.
- Click the **Add** button to enter the next-hop address.
- Under **SIP Server Profile**, select ***Service Provider TLS***.
- The **Next Hop Address** is populated automatically with ***svc1234.us-east.test.trunk.io*** (service provider's SIP proxy server FQDN and Transport), Server Configuration Profile defined in **Section 8.9.2**.
- Click **Finish**.



8.11. Topology Hiding

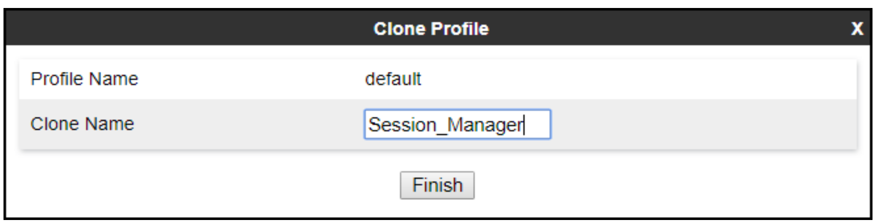
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

8.11.1. Topology Hiding Profile – Enterprise

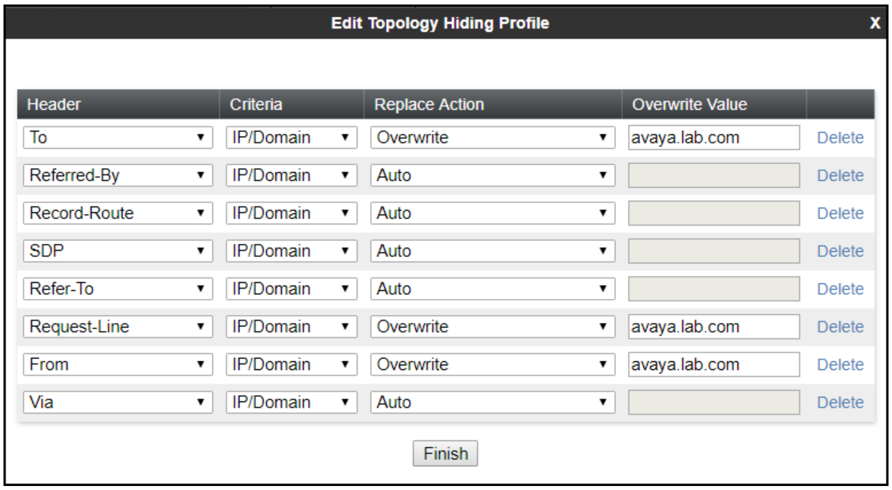
To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



On the newly cloned ***Session_Manager*** profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***avaya.lab.com***, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 7.2**.
- Default values were used for all other fields.
- Click **Finish**.



Edit Topology Hiding Profile

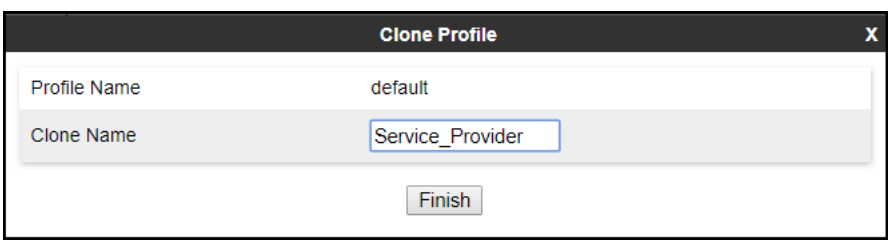
Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Overwrite	avaya.lab.com	Delete
Referred-By	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	avaya.lab.com	Delete
From	IP/Domain	Overwrite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

Finish

8.11.2. Topology Hiding Profile – Service Provider

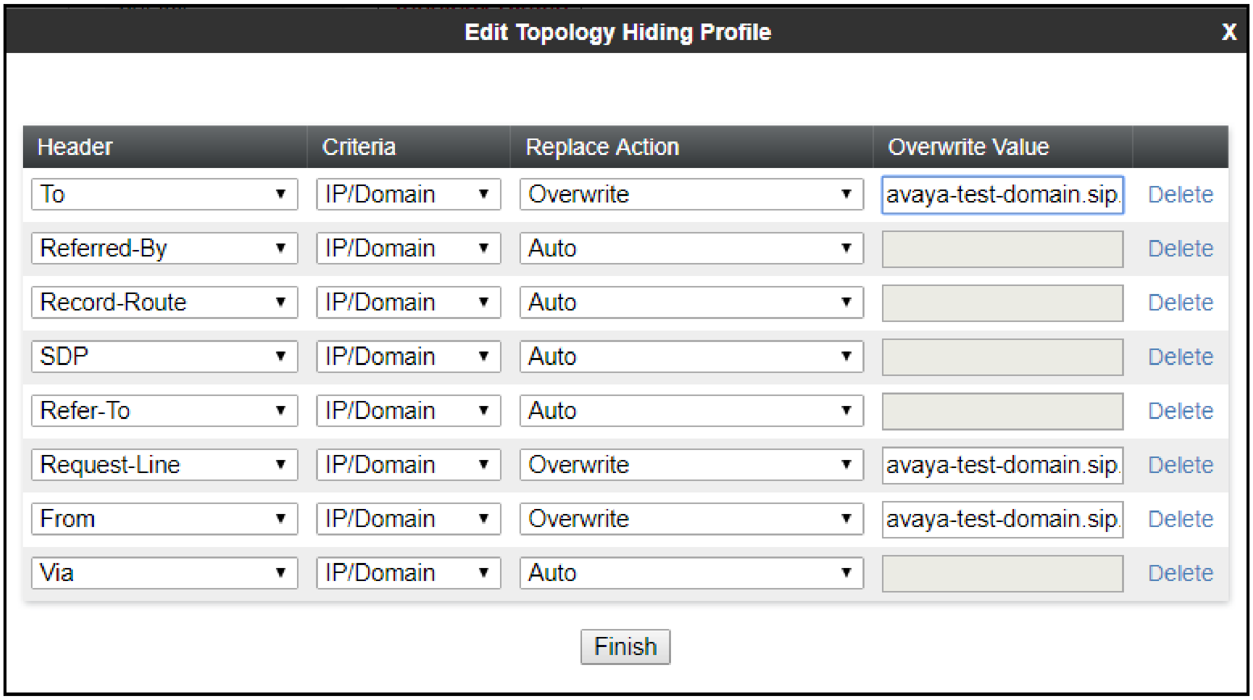
To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



On the newly cloned ***Service_Provider*** profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select ***Overwrite*** in the **Replace Action** column and enter the service provider SIP domain ***avaya-test-domain.sip.1234.io***, in the **Overwrite Value** column of these headers, as shown below. This information should be provided by the service provider.
- Default values were used for all other fields.
- Click **Finish**.



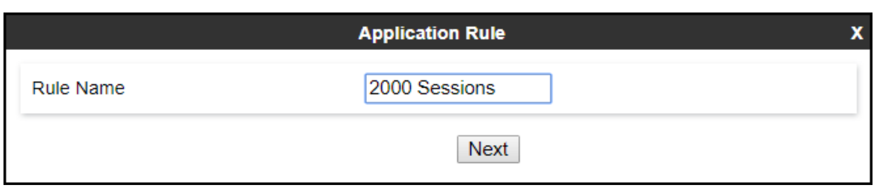
8.12. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

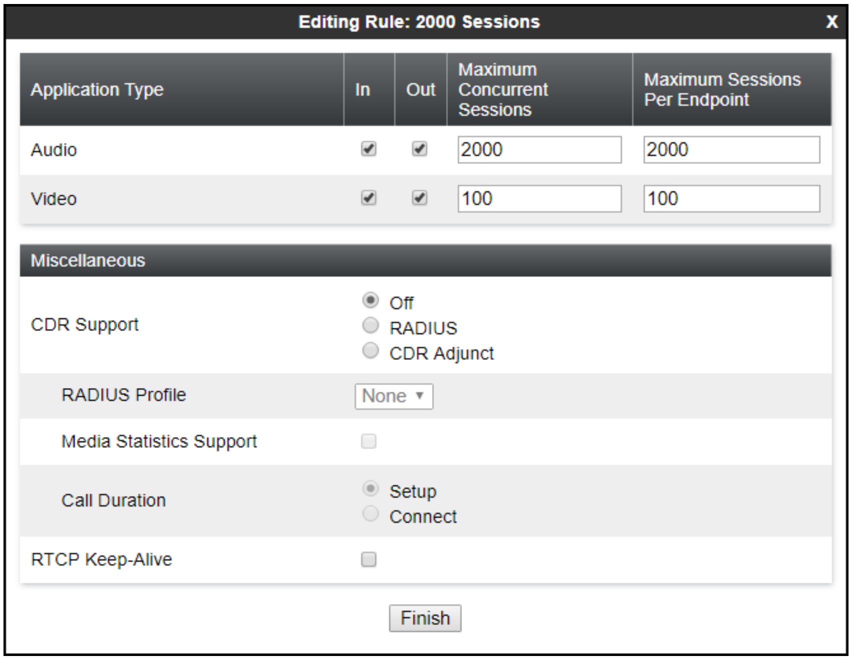
8.12.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies → Application Rules**, click on the **Add** button to add a new rule (not shown).

- Under **Rule Name** enter the name of the profile, e.g., ***2000 Sessions***.
- Click **Next**.



- Under **Audio** check ***In*** and ***Out*** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of ***2000*** for Audio was used for the test. Repeat for video if needed, the value of ***100*** for Video was used for the test.
- Click **Finish**.



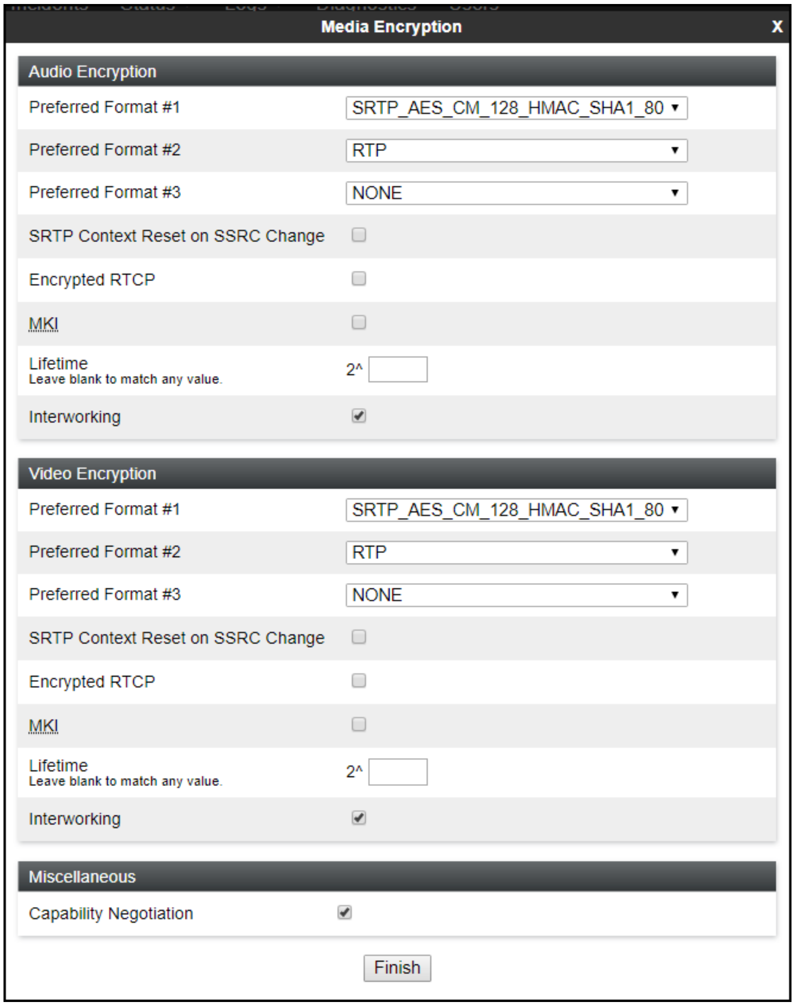
8.12.2. Media Rules

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

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules** (not shown).

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter a name, ***SM_SRTP*** was used (not shown).
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck ***Encrypted RTCP***.
- Under Audio Encryption, check ***Interworking***.
- Repeat the above steps under Video Encryption, if needed.

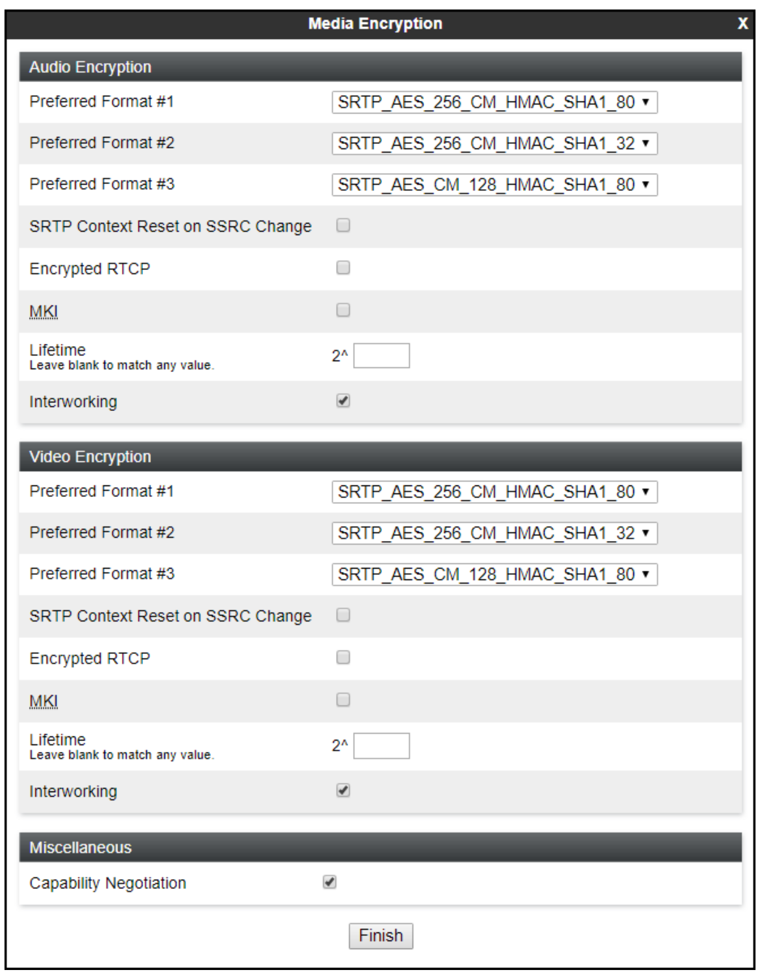
- Under Miscellaneous verify that ***Capability Negotiation*** is checked.
- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish**.



.

To add a media rule in the Service Provider direction, from the menu on the left-hand side, select **Domain Policies → Media Rules** (not shown).

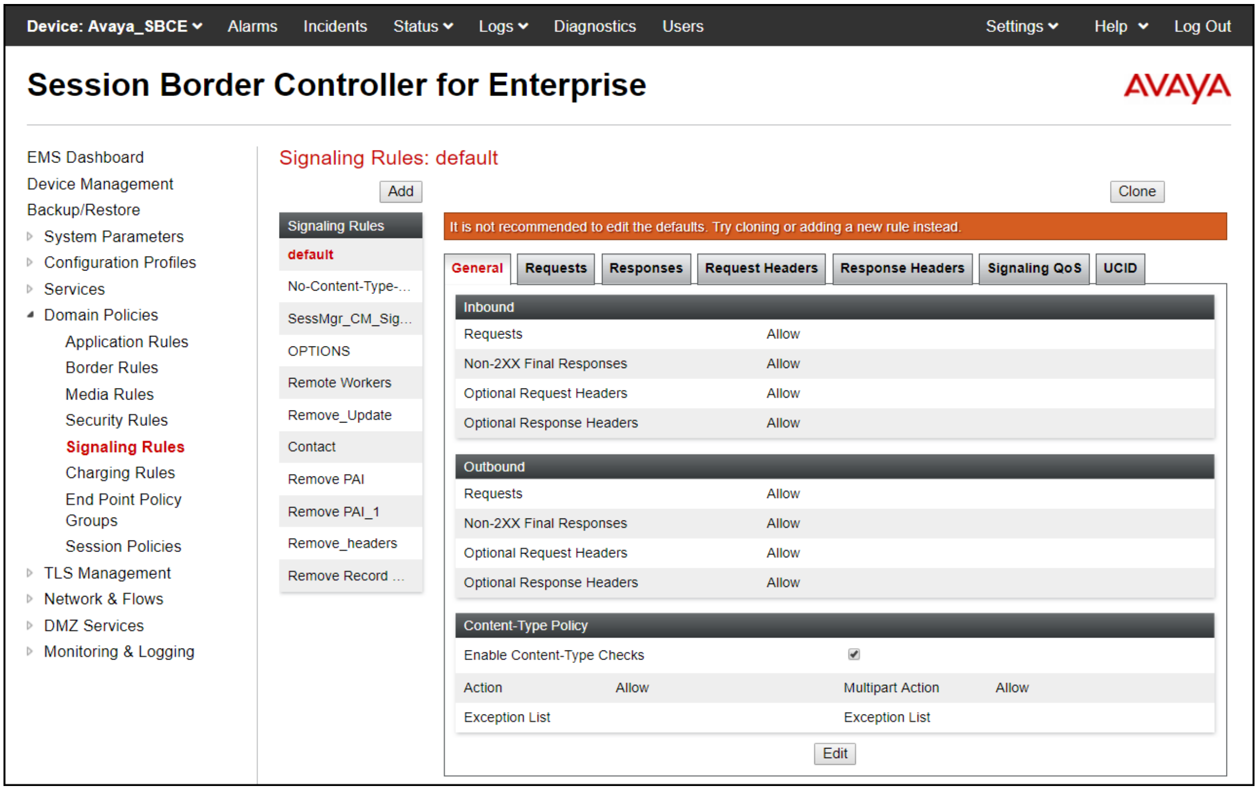
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter a name, ***ServiceProvider_SRTP*** was used (not shown).
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select ***SRTP_AES_256_CM_HMAC_SHA1_80***.
- Under Audio Encryption, **Preferred Format #2**, select ***SRTP_AES_256_CM_HMAC_SHA1_32***.
- Under Audio Encryption, **Preferred Format #3**, select ***SRTP_AES_128_CM_HMAC_SHA1_80***.
- Under Audio Encryption, uncheck ***Encrypted RTCP***.
- Under Audio Encryption, check ***Interworking***.
- Repeat the above steps under Video Encryption, if needed.
- Under Miscellaneous verify that ***Capability Negotiation*** is checked.
- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish**.



Note – SRTP media encryption is being enforced, fallback to RTP, or to unencrypted media, is not supported in the Service Provider's direction.

8.12.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.



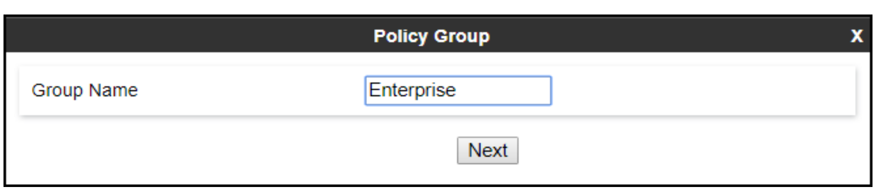
8.13. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

8.13.1. End Point Policy Group – Enterprise

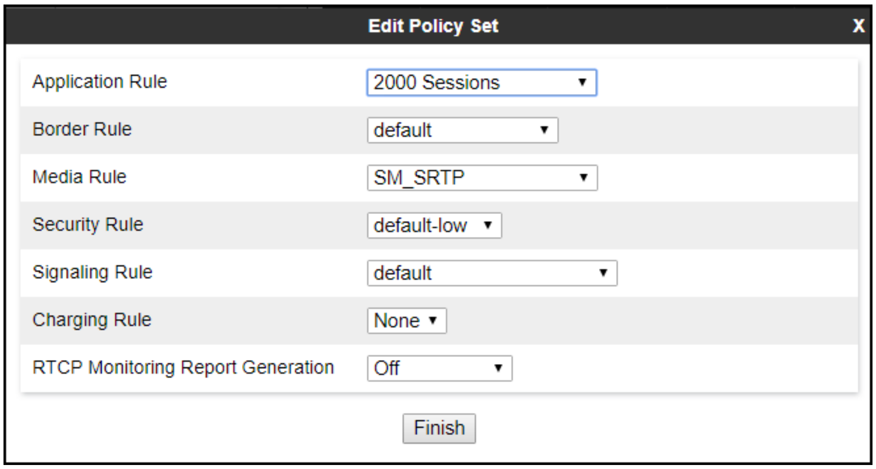
To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

- Enter an appropriate name in the **Group Name** field, ***Enterprise*** was used.
- Click **Next**.



Under the **Policy Group** tab enter the following:

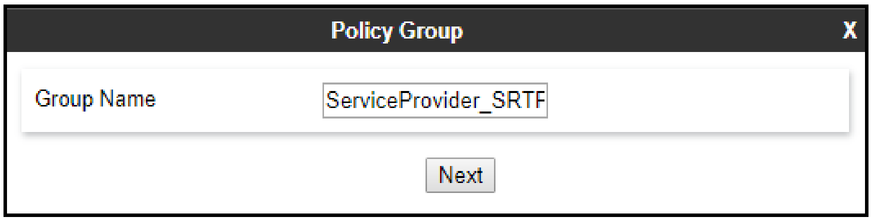
- **Application Rule**: ***2000 Sessions*** (**Section 8.12.1**).
- **Border Rule**: ***default****.*
- **Media Rule**: ***SM_SRTP*** (**Section 8.12.2**).
- **Security Rule**: ***default-low***.
- **Signaling Rule**: ***default*** (**Section 8.12.3**).
- Click **Finish**.



8.13.2. End Point Policy Group – Service Provider

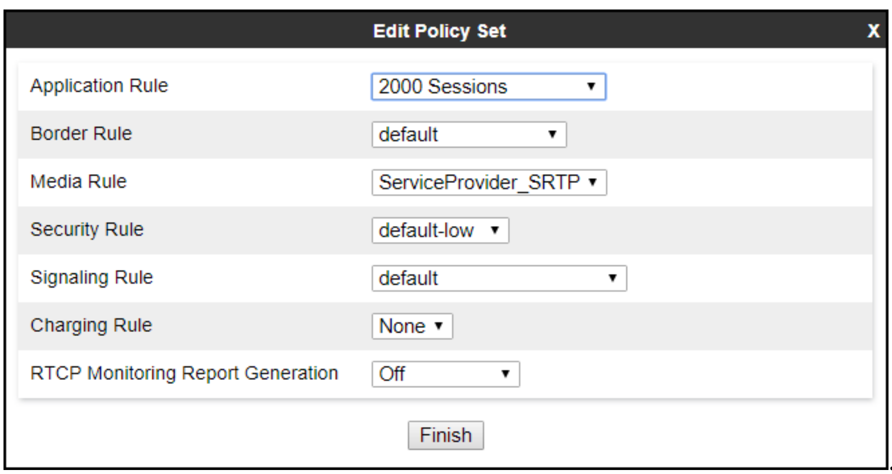
To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

- Enter an appropriate name in the **Group Name** field, ***ServiceProvider_SRTP*** was used.
- Click **Next**.



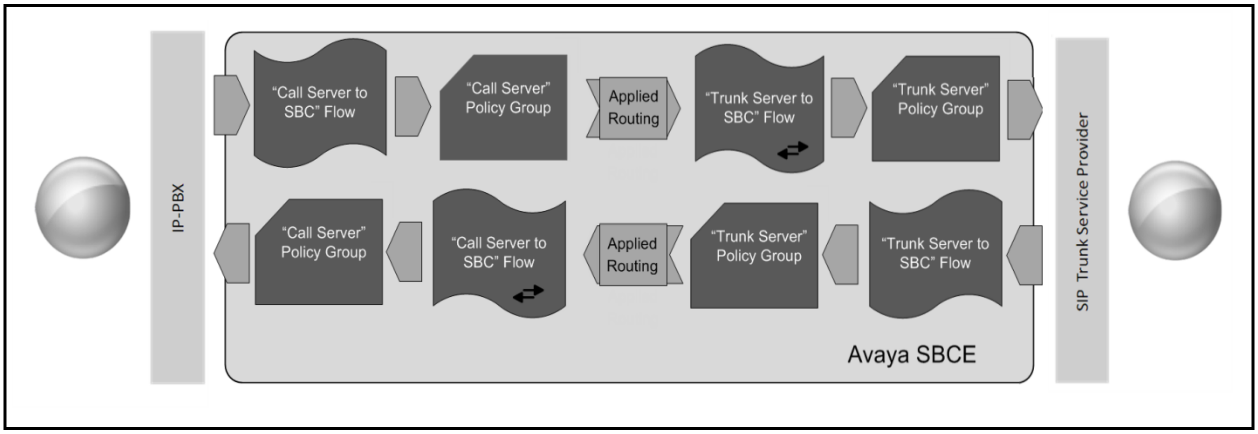
Under the **Policy Group** tab enter the following:

- **Application Rule**: ***2000 Sessions*** (**Section 8.12.1**).
- **Border Rule**: ***default***.
- **Media Rule**: ***ServiceProvider_SRTP*** (**Section 8.12.2**).
- **Security Rule**: ***default-low***.
- **Signaling Rule**: ***default*** (**Section 8.12.3**).
- Click **Finish**.



8.14. End Point Flows

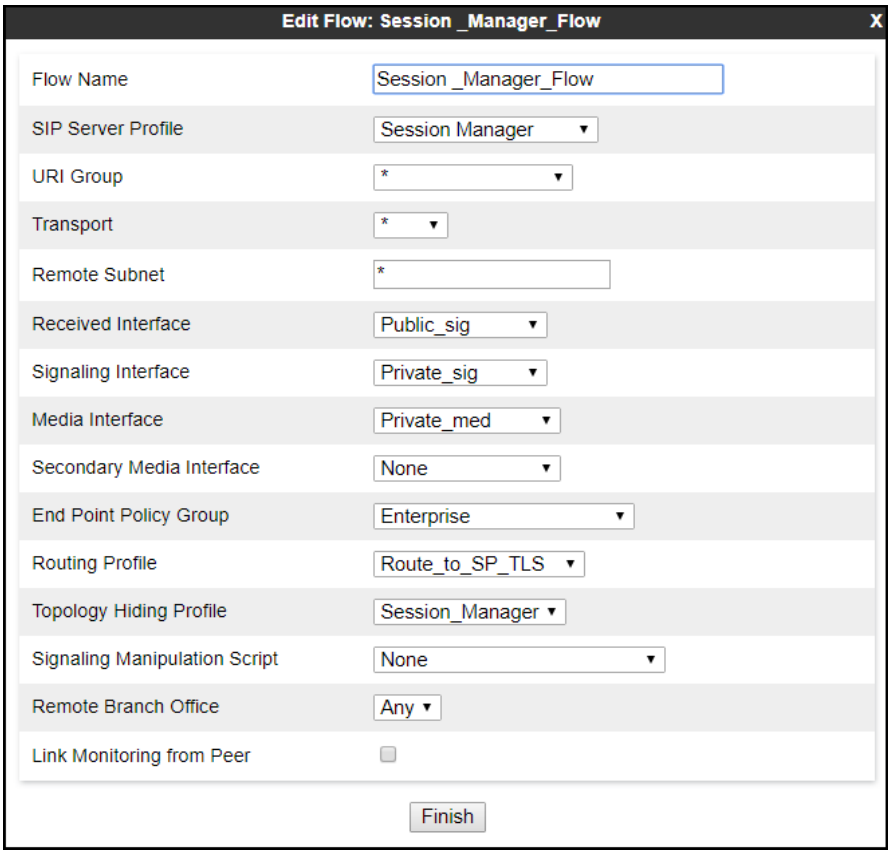
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing 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 screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

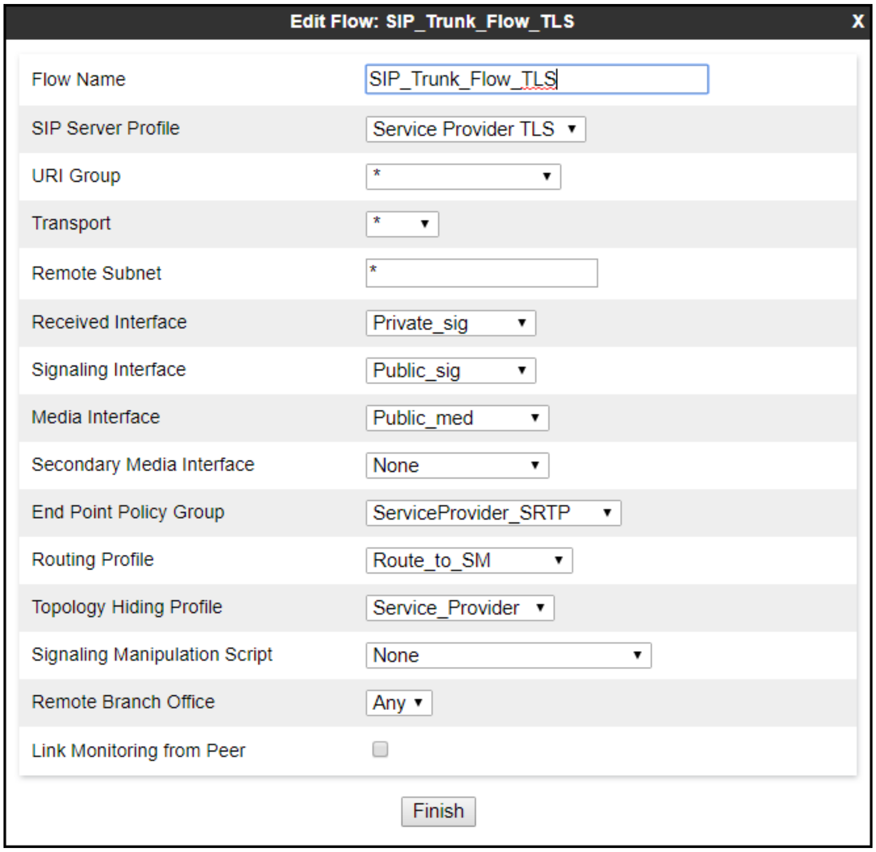
8.14.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named ***Session_Manager_Flow*** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 8.10.2**, which is the reverse route of the flow. Click **Finish**.



8.14.2. End Point Flow – Service Provider

A second Server Flow with the name ***SIP_Trunk_Flow_TLS*** was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 8.10.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.



9. Avaya SIP Trunking Service Configuration

To use the Avaya SIP Trunking service, a customer must request the service from Avaya using the established sales processes. To learn more about the Avaya SIP Trunking service call your Avaya Account Manager Authorized Partner or go to https://www.avaya.com/en/documents/fs-sip-uc8179en.pdf

During the signup process, the Service Provider (Avaya) and the customer will discuss details about the preferred method to be used to connect the customer's Avaya enterprise network to the Avaya SIP Trunking service network.

The Service Provider (Avaya) will provide the following information:

- The **Root CA** certificates for the trusted certificate authority being used by the Service Provider (Avaya), required to enable TLS encryption outside of the enterprise (public network side). The customer can download the **Root CA** certificates directly from the 3rd party trusted Certificate Authority web/home page, the name of the 3rd party trusted Certificate Authority will be needed when downloading from their web/home page, the Service provider (Avaya) can guide the customer on how to obtain the necessary certificates.
- Service Provider's SIP Proxy FQDN to be used for public DNS SRV record queries.
- Service Provider's SIP domain name to be used.
- SIP Trunk registration credentials (User Name, Password, etc.).
- DID numbers.
- Public DNS IP addresses.
- Etc.

10. 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 commands that can be used to troubleshoot the solution.

10.1. General Verification Steps

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the 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.

10.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **list trace station** <extension number>

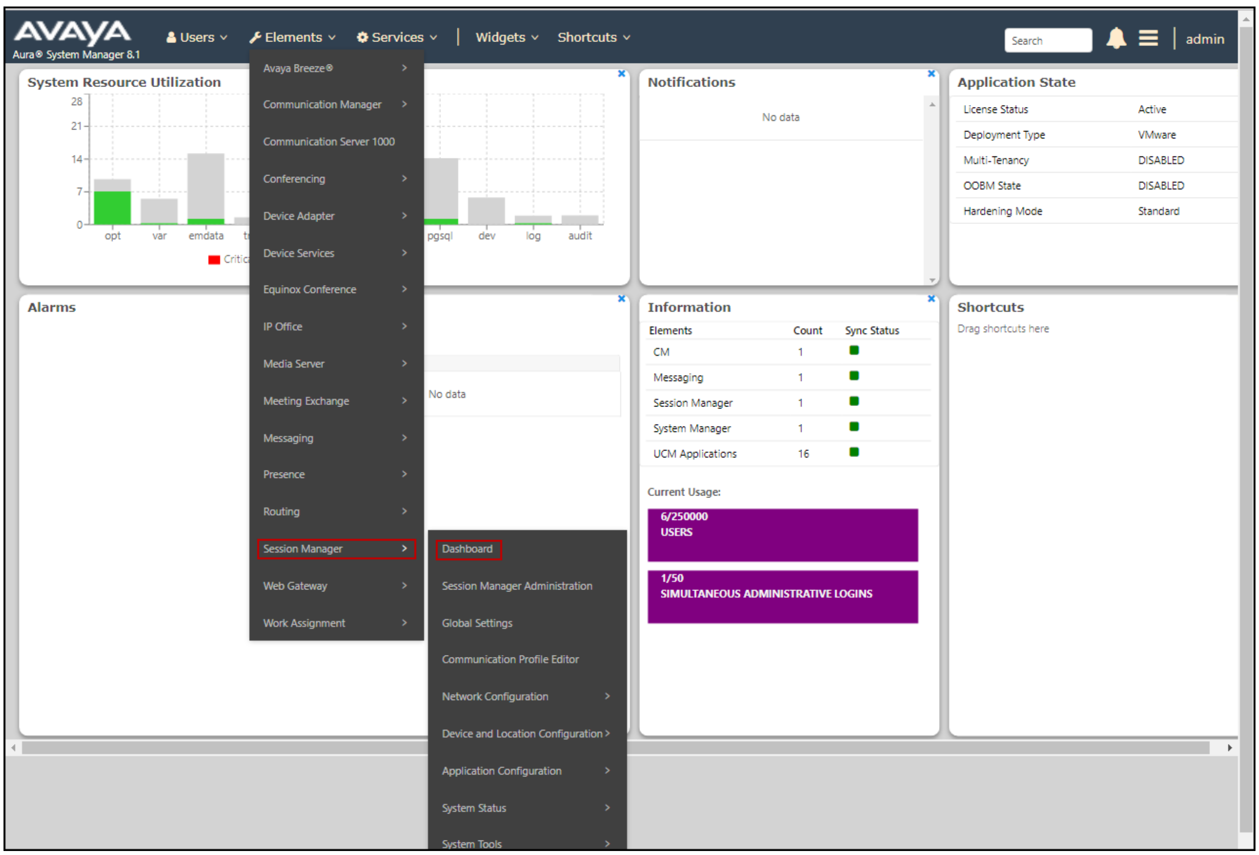
Traces calls to and from a specific station.

- **list trace tac** <trunk access code number>
  Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
  Displays signaling group service state.
- **status trunk** <trunk group number>
  Displays trunk group service state.
- **status station** <extension number>
  Displays signaling and media information for an active call on a specific station.

10.3. Session Manager Verification

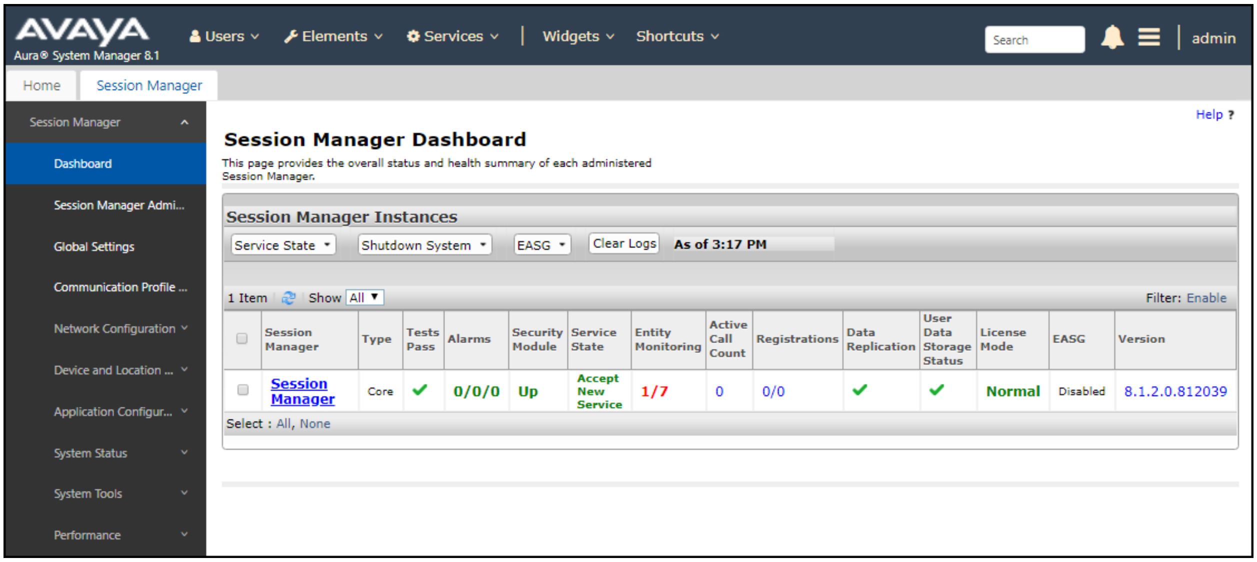
The Session Manager configuration may be verified via System Manager.

Step 1 - Using the procedures described in **Section 7**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager,** then select **Dashboard**.

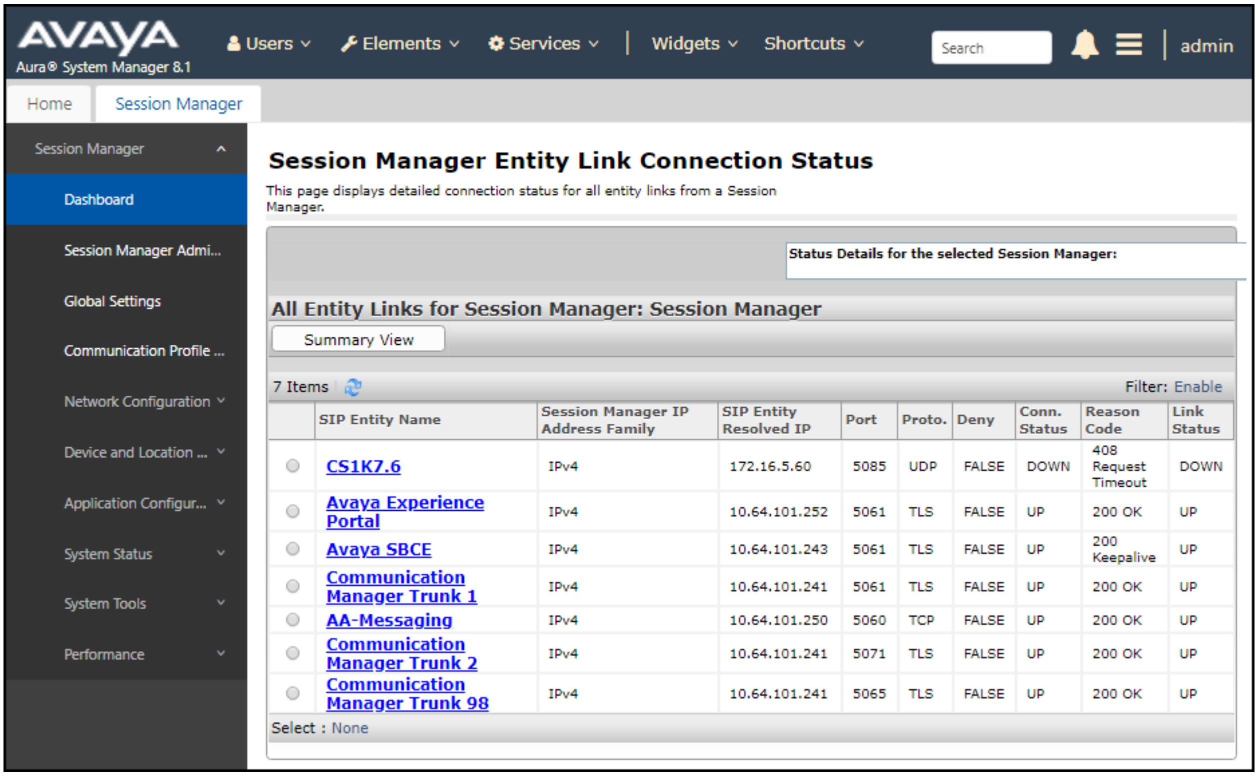


Step 2 - The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns all show good status.

In the **Entity Monitoring** column, Session Manager shows that there is **1** alarm out of the **7** Entities defined.



Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns are ***UP***, like shown on the screen below



Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

All Entity Links for Session Manager: Session Manager

Summary View

7 Items Filter: Enable

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
	CS1K7.6	IPv4	172.16.5.60	5085	UDP	FALSE	DOWN	408 Request Timeout	DOWN
	Avaya Experience Portal	IPv4	10.64.101.252	5061	TLS	FALSE	UP	200 OK	UP
	Avaya SBCE	IPv4	10.64.101.243	5061	TLS	FALSE	UP	200 Keepalive	UP
	Communication Manager Trunk 1	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
	AA-Messaging	IPv4	10.64.101.250	5060	TCP	FALSE	UP	200 OK	UP
	Communication Manager Trunk 2	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
	Communication Manager Trunk 98	IPv4	10.64.101.241	5065	TLS	FALSE	UP	200 OK	UP

Select : None

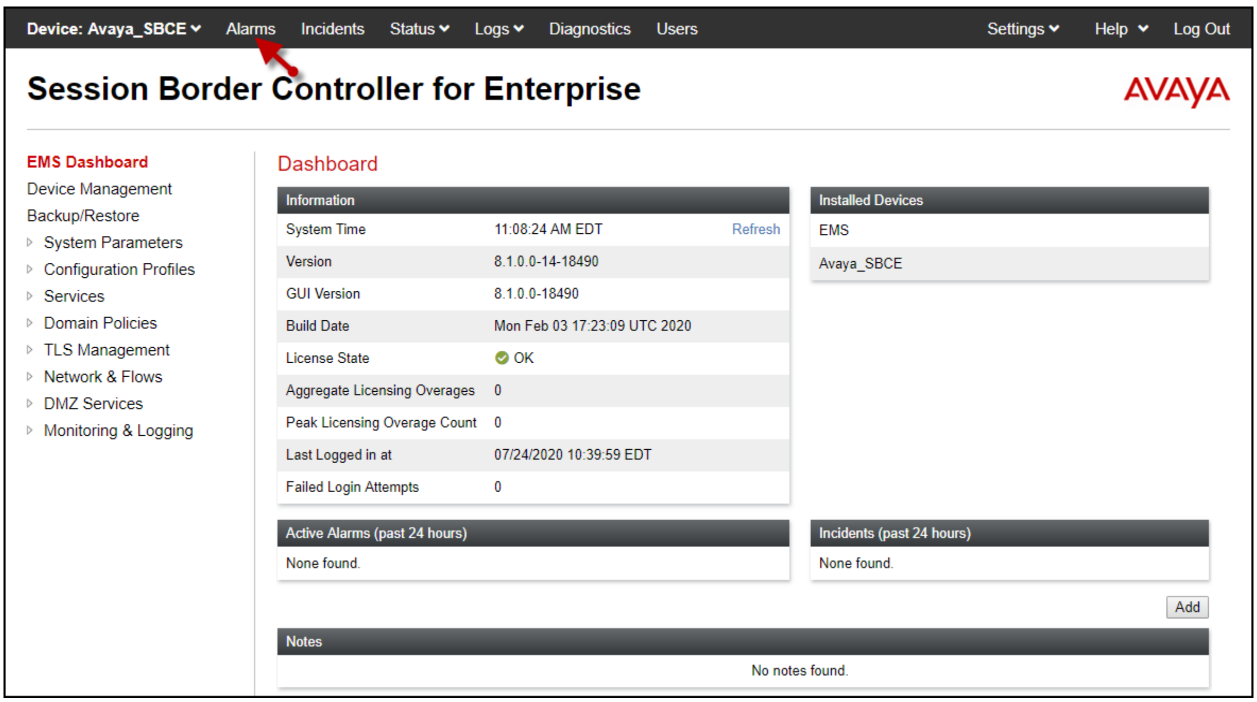
Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** – The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements → Session Manager →System Tools → Call Routing Test**. Enter the requested data to run the test.

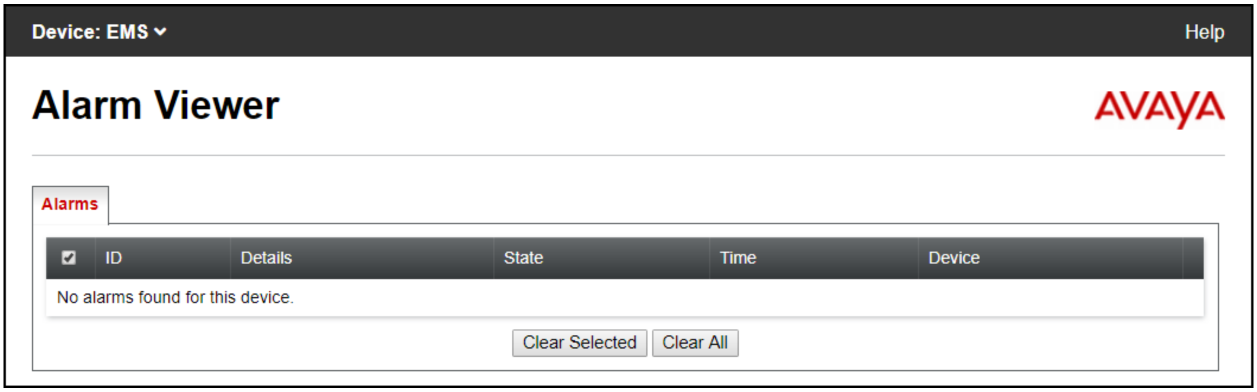
10.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

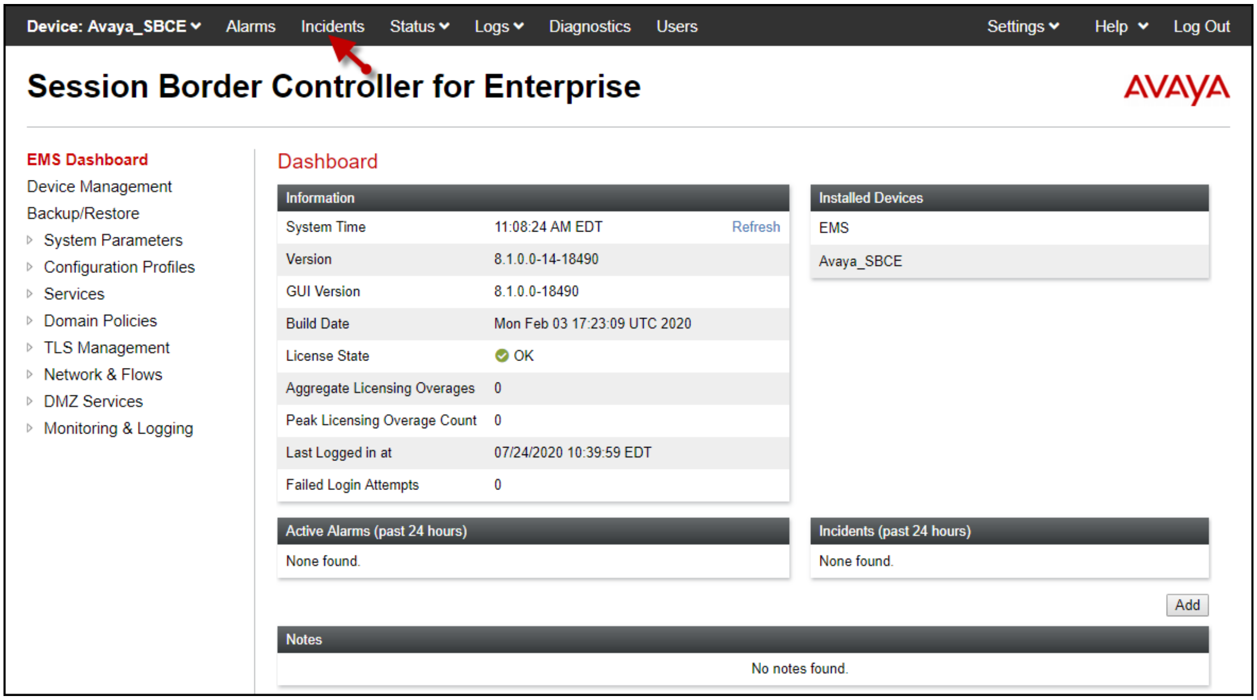
Alarms: This screen provides information about the health of the SBC.



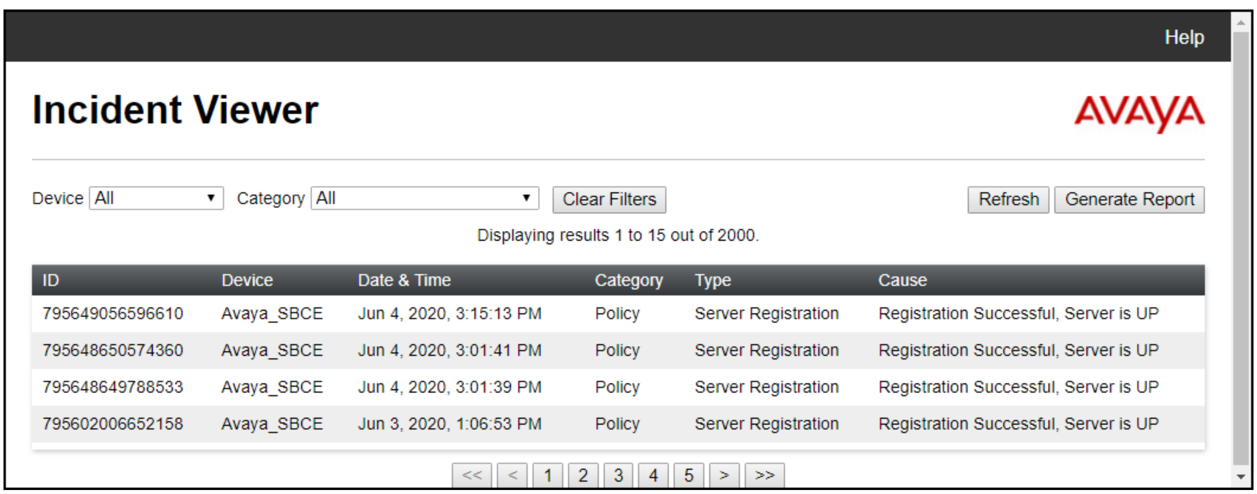
The following screen shows the **Alarm Viewer** page.



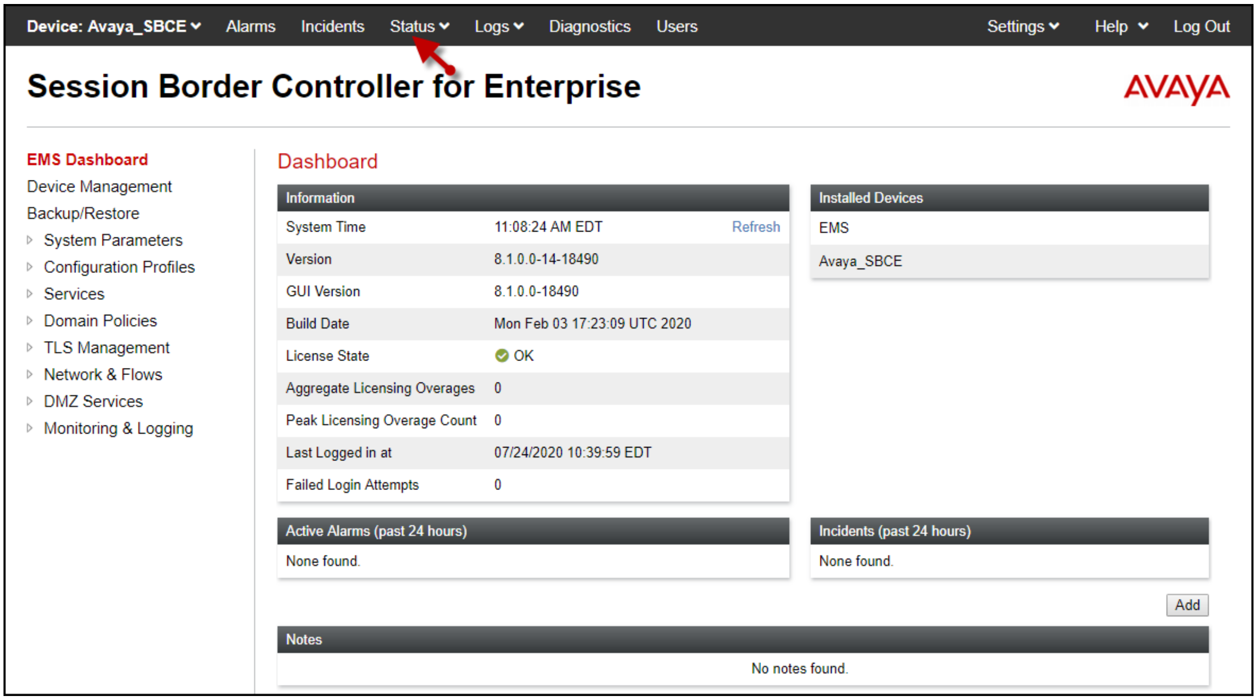
Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.

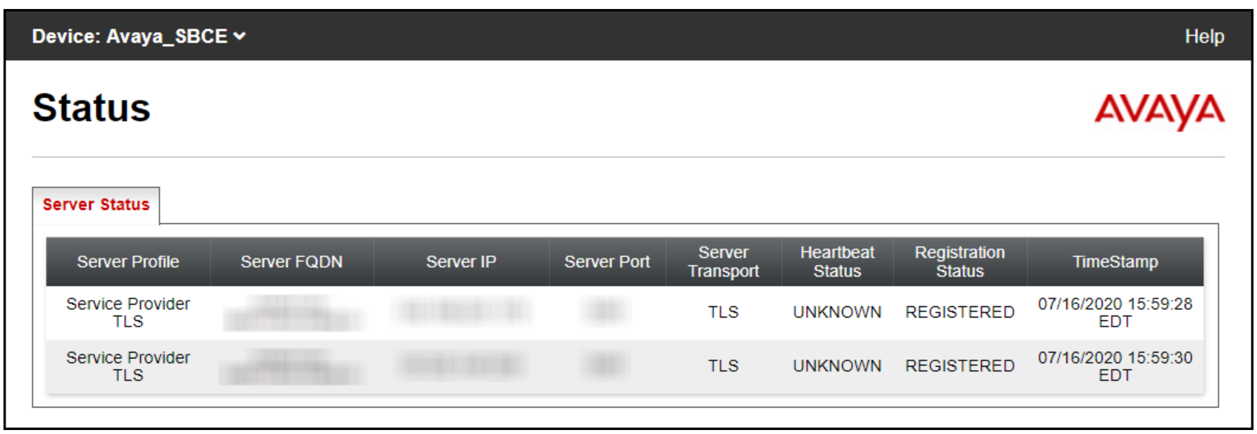


The following screen shows the **Incident Viewer** page.

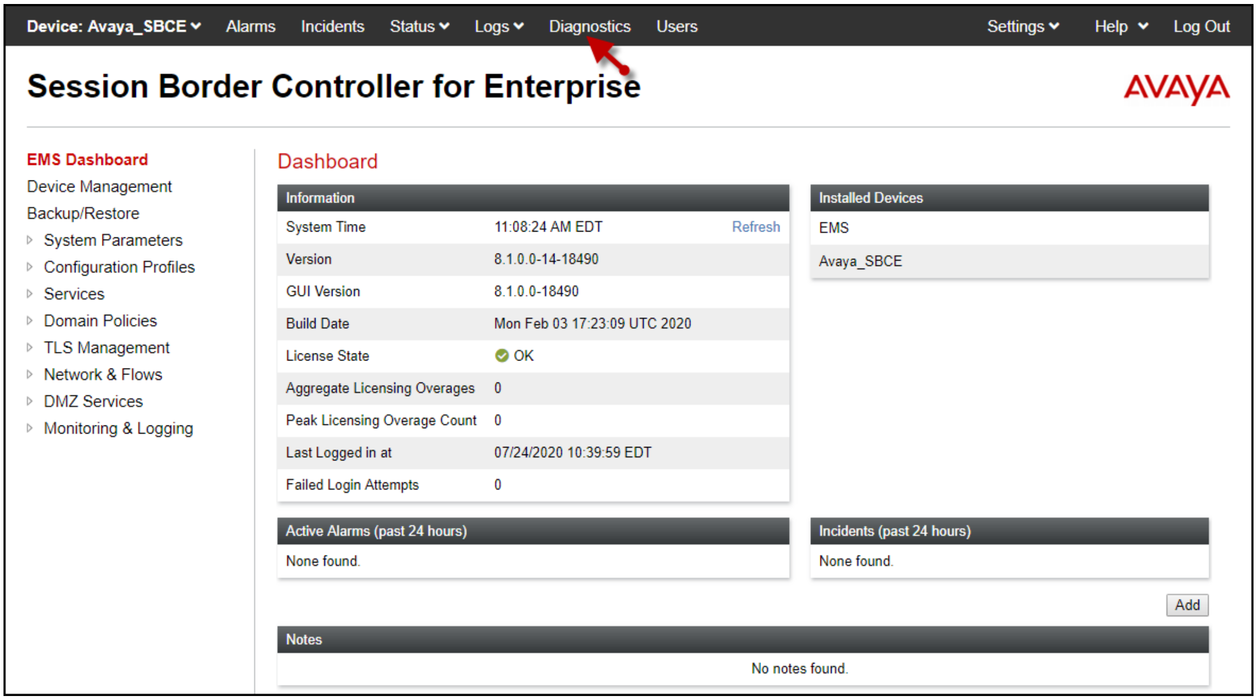


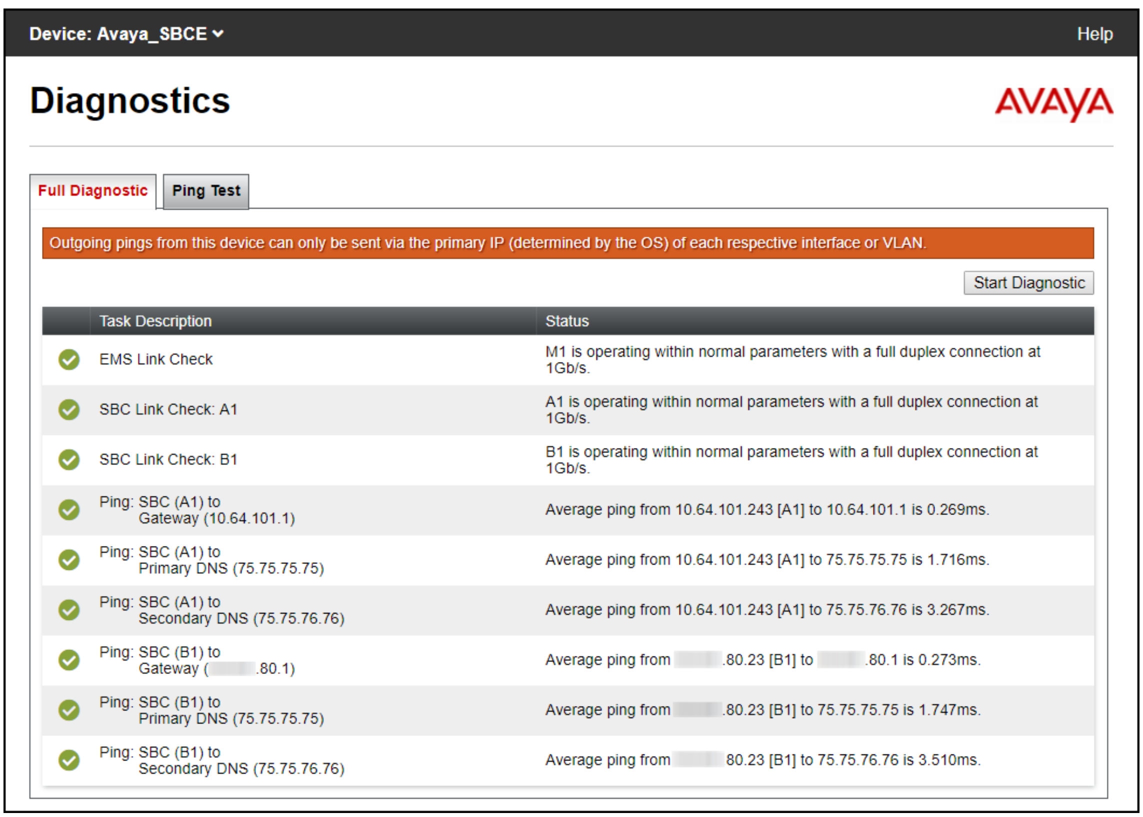
Status : Provides the status for each server resolved during DNS SRV queries handling calls to/from the PSTN. Note that Server FQDN and Server IP/Port were blurred out for security reasons.



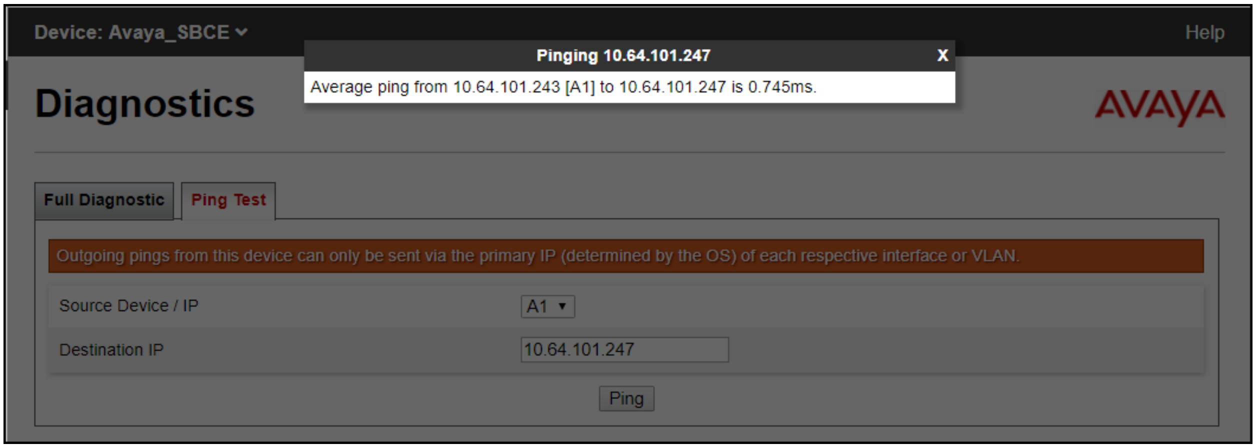


Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



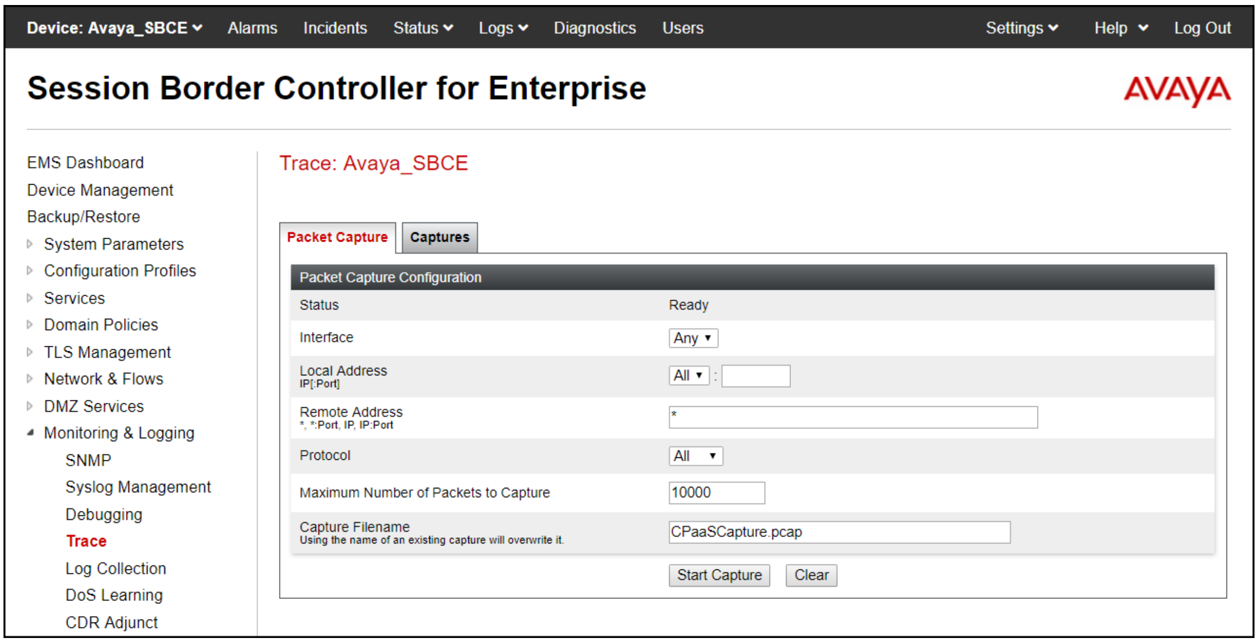


The following screen shows the Diagnostics page with the results of a ping test.

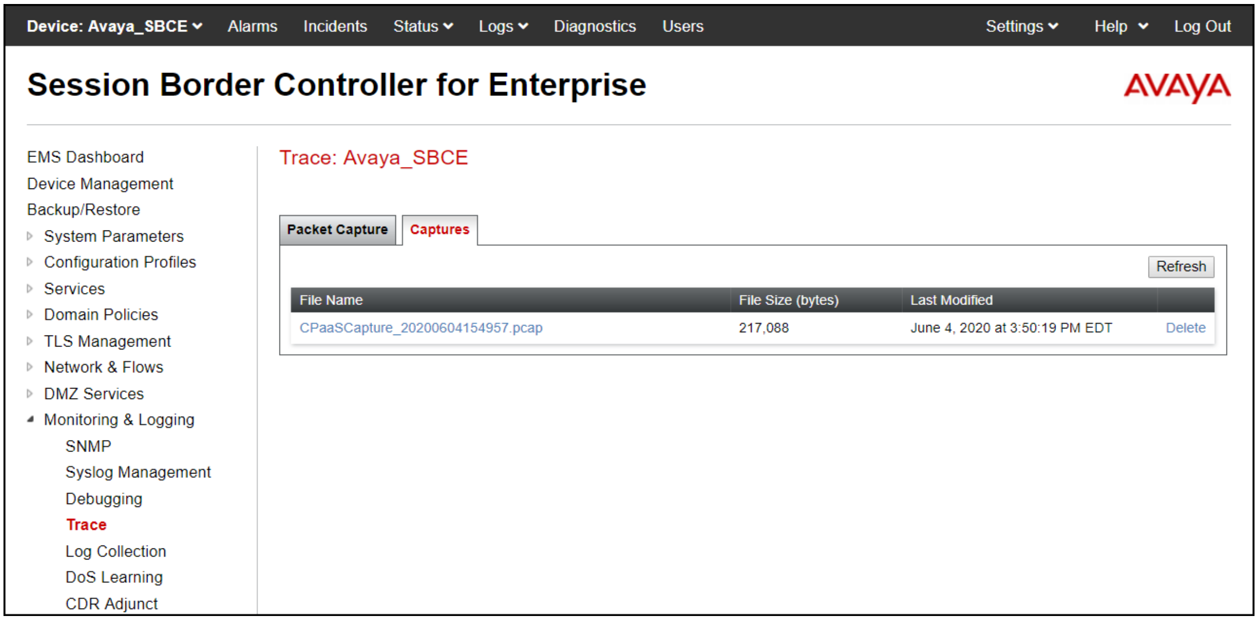


Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Monitor & Logging → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

Note – Since TLS is being used inside of the enterprise (private network side) and outside of the enterprise (public network side) the Avaya SBCE internal packet capture tool shown below cannot be used since it cannot decrypt TLS encrypted data, instead the Avaya SBCE packet trace tool "**traceSBC**" should be used.



Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



11. Conclusion

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 8.1, Avaya Aura® System Manager Release 8.1, Avaya Aura® Communication Manager Release 8.1, Avaya Aura® Experience Portal 7.2 and the Avaya Session Border Controller for Enterprise 8.1 to interoperate with the Avaya SIP Trunking service using Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) on the private (enterprise) and the public (internet) sides, as shown in **Figure 1**. The Avaya SIP Trunking service referenced in this document provides secured encrypted communications for local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Sections 2.1** and **2.2**.

12. References

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

[1] *Deploying Avaya Aura® Communication Manager* in a Virtualized Environment, Release 8.1.x, Issue 4, March 2020.
[2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020.
[3] *Administering Avaya Aura® System Manager* for Release 8.1.x, Issue 6, April 2020.
[4] *Deploying Avaya Aura® System Manager* in a Virtualized Environment, Release 8.1.x, Issue 5, May 2020.
[5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager* in a Virtualized Environment, Release 8.1., Issue 3, March 2020.
[6] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 4, May 2020.
[7] *Deploying Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 3, June 2020.
[8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 2, April 2020.
[9] *Administering Avaya Aura® Experience Portal*, Release 7.2.3, Issue 1, September 2019
[10] *Implementing Avaya Aura® Experience Portal on a single server*, Release 7.2.3, Issue 1, September 2019.
[11] *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.*
[12] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 9, April 2020.
[13] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0.x, Issue 9, April 2020.
[14] *Planning for and Administering Avaya IX ™ Workplace Client for Android, iOS, Mac, and Windows*. Release 3.8, Issue 1, March 2020.
[15] *Administering Avaya one-X® Communicator*. Release 6.2, Feature Pack 10, November 2015.
[16] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[17] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

13. Appendix A – Avaya Session Border Controller for Enterprise – Refer Handling

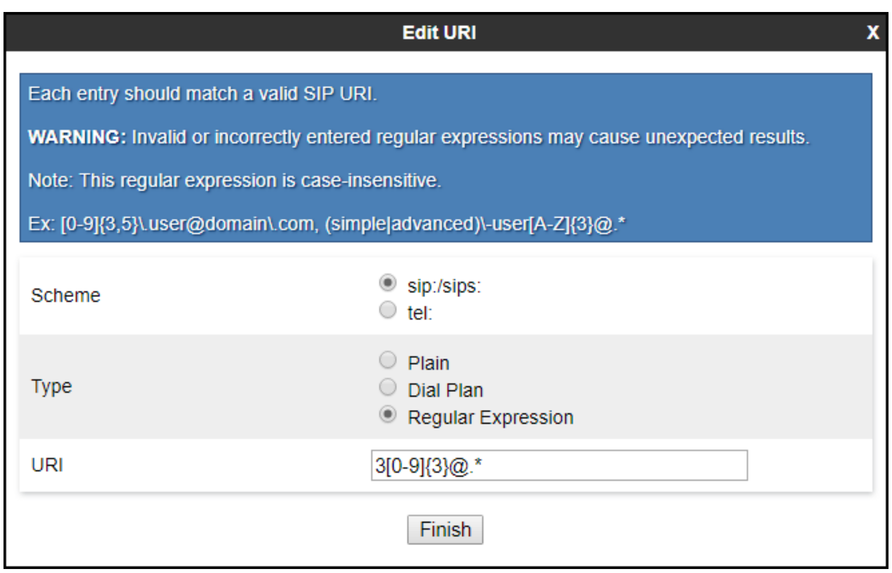
One of the capabilities important to the Experience Portal environment is the Avaya SBCE Refer Handling option. Experience Portal inbound call processing may include call redirection to Communication Manager agents, or other CPE destinations. This redirection is accomplished by having Experience Portal send SIP REFER messaging to the Avaya SBCE. Enabling the Refer Handling option causes the Avaya SBCE to intercept and process the REFER and generate a new SIP INVITE messages back to the CPE (e.g., Communication Manager).

As an additional option, the Refer Handling feature can also specify *URI Group* criteria as a discriminator, whereby SIP REFER messages matching the URI Group criteria are processed by the Avaya SBCE, while SIP REFER messages that do not match the URI Group criteria, are passed through to the Service Provider.

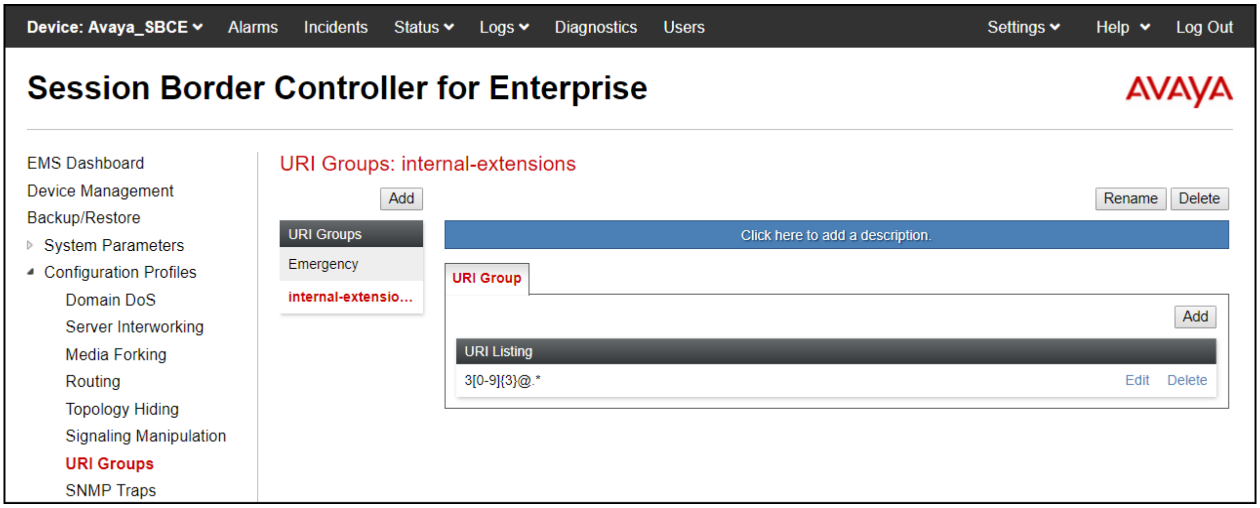
Note – If Experience Portal is not included as part of the Avaya Enterprise equipment Refer Handling should not be used, it should be left unchecked/disabled.

Create a URI Group for numbers intended for Communication Manager.
Step 1 - Select **Global Profiles → URI Groups** from the left-hand menu.
Step 2 - Select **Add** and enter a descriptive **Group Name**, e.g., **internal-extension**, and select **Next** (not shown).
Step 3 - Enter the following:

- **Scheme**: **sip:/sips**:
- **Type**: **Regular Expression**
- **URI**: **3[0-9]{3}@.*** This will match 4-digit local extensions starting with 3, e.g., 3041 or 3042.
- Select **Finish**.



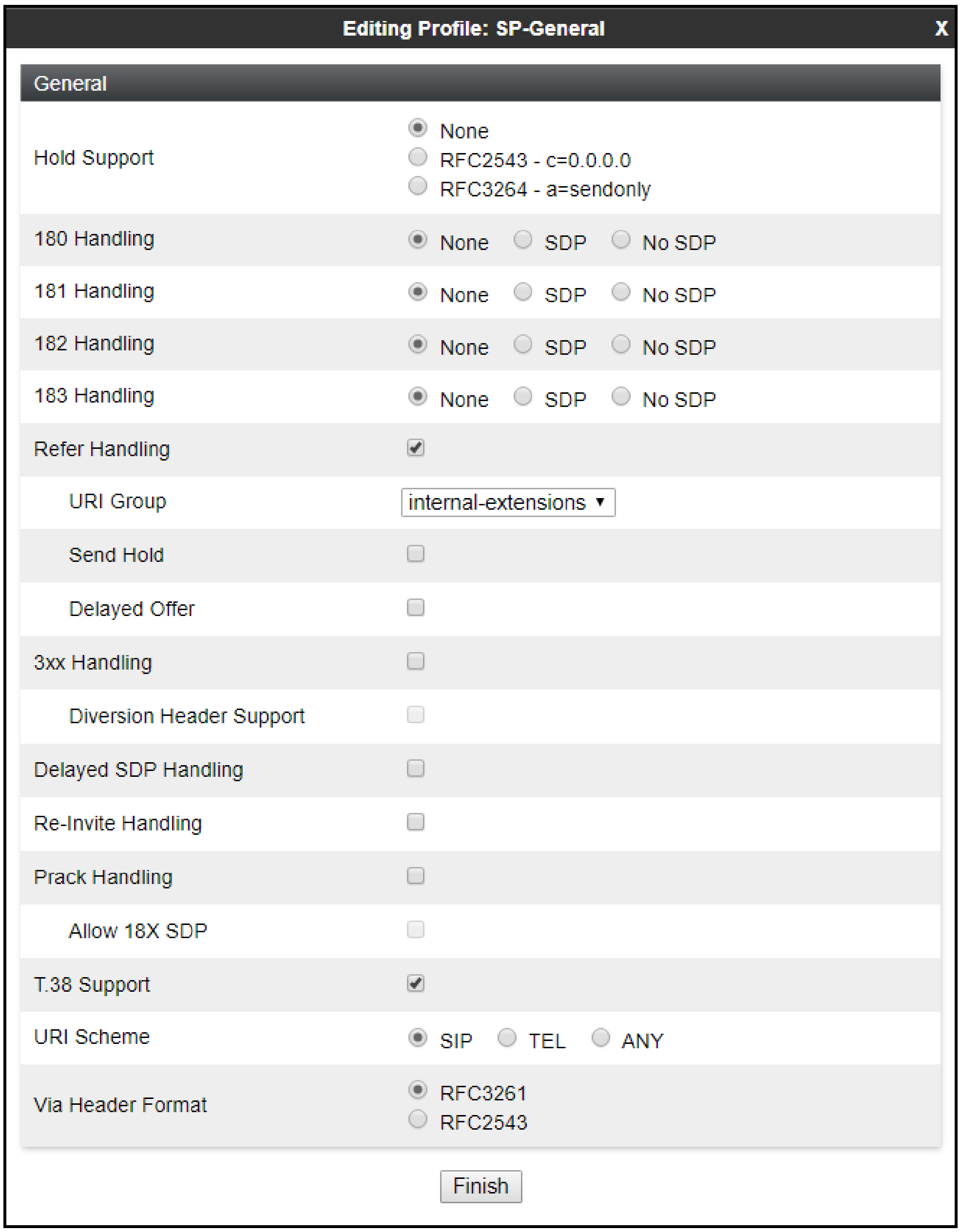
Step 4 - For additional entries, select **Add** on the right-hand side of the URI Group tab and repeat **Step 3**.



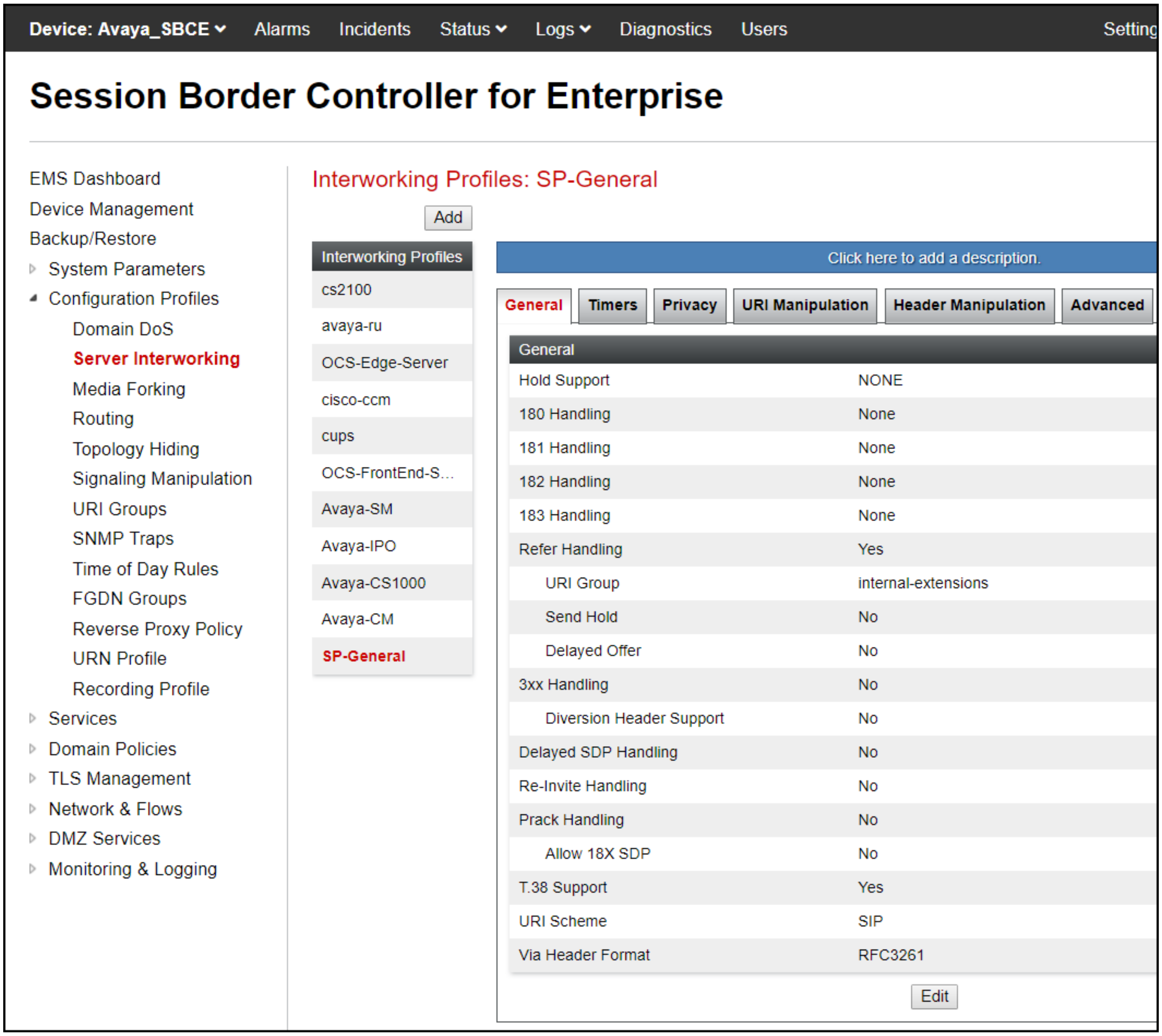
Edit the existing **SP-General** Server Interworking Profile to enable Refer Handling.

Step 1 - Select **Configuration Profiles → Server Interworking** from the left-hand menu (not shown).
Step 2 - Select the **SP-General** Server Interworking Profile created in **Section 8.7.2** and click **Edit**

- Check **Refer Handling**.
- **URI Group**: **internal-extensions**.
- Select **Finish**.



Following is the SP-General Server Interworking profile after editing.



14. Appendix B – SigMa Scripts

Following are the Signaling Manipulation scripts that were used in the configuration of the Avaya SBCE. Add the scripts as instructed in **Sections 8.8**, enter a name for the script in the Title and copy/paste the entire scripts shown below.

```
//Removes a=sendonly from re-INVITE message to correct an issue with Music On-Hold not
playing when inbound calls are placed On-Hold.

within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{

   %BODY[1].regex_replace("a=sendonly\r\n","");

}

}

//Removes gsid and epv parameters from Contact header.
//Changes the Diversion header scheme from SIPS to SIP.
//Removes P-Location parameter. This is required since the adaptation in Session Manager is not
removing the P-Location header.
//Removes unwanted xml element information from the SDP in SIP messages sent to Service
Provider. SP replies with invalid media type if not removed.

within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
    remove(%HEADERS["P-Location"][1]);
    %HEADERS["Diversion"][1].regex_replace("sips","sip");
    remove(%BODY[1]);

}

}
```

```
//Inserts "+" in the "To" and "Request-Line-URI" headers to comply with E.164 numbering
format. This change is required for calls from Experience Portal to the PSTN.

within session "INVITE"
{
 act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{

   %HEADERS["To"][1].URI.USER.regex_replace("^1","+1");
   %HEADERS["Request_Line"][1].URI.USER.regex_replace("^1","+1");

}

}
```