Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise 8.0 with Masergy SIP Trunking - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise Release 8.0, to interoperate with the Masergy SIP Trunking service.

Masergy SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the service provider's network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise

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

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

Table of Contents

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise to interoperate with the Masergy SIP Trunking service.

The Masergy SIP trunking service referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya enterprise solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks.

Note that the terms “service provider” or “Masergy” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

A simulated enterprise site containing all the Avaya equipment for the SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to Masergy SIP Trunking Services via a broadband connection.

The configuration shown in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products. Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Notes, the interface between the Avaya systems and the Masergy service did not include use of any specific encryption features as requested by Masergy. Encryption (TLS/SRTP) was enabled between Avaya products internally on the enterprise.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types. Phone types included SIP, H.323, digital and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included SIP, H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (H.323 and SIP) and Avaya Equinox for Windows (SIP) softphones.
- Various call types including: local, long distance national, outbound toll free and international calls.
- Proper disconnect when the call is abandoned by the caller before it is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect for calls that are not answered.
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid numbers.
- Proper codec negotiation and two-way speech path. Testing was performed using codecs G.711MU, G711A and G.729A.
- Proper response to no matching codecs condition.
- Caller ID presentation and Caller ID restriction.
- DTMF transmission using RFC 2833. Voicemail navigation for inbound and outbound calls.
- Fax T.38.
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind and Consultative Call Transfer.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Network Call Redirection using SIP REFER messages.
- Routing PSTN calls to call center agent queues.
- Proper response/error treatment to “all trunks busy” conditions.
- Proper response/error treatment for signaling failure conditions.
- Avaya Remote Worker operation (Avaya Equinox SIP softphone) via Avaya SBCE.

Items not supported or not tested included the following:

- Local directory assistant (411) calls are not supported.
- 0, 0+10 digits calls are not supported.
- Network Call Redirection using SIP 302 message is not supported.
- Intermediate call states via NOTIFY messages is not supported.

- SIP User-to-User Information (UUI) is not supported.
- 911 Emergency calls were not tested

2.2. Test Results

All the test objectives stated in **Section 2.1**, with the limitation noted below, were verified.

- When TLS/SRTP is used within the enterprise, the SIP headers include the SIPS URI scheme for Secure SIP. The Avaya SBCE converts these headers from SIPS to SIP when it sends the SIP message toward the trunk to Masergy. However, for call forward and EC500 calls, the Avaya SBCE did not change the Diversion header scheme as expected. This caused these call types that require a Diversion header to fail since Masergy does not expect Secure SIP. This anomaly is currently under investigation by the Avaya SBCE development team. A workaround is to include a SigMa script for the Masergy Server Configuration profile on the Avaya SBCE, to convert "sips" to "sip" in the Diversion header. See **Section 7.7**.
- **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-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector, P-Location, Av-Secure-Indication (**Section 6.4**).
  The Avaya SBCE SigMa script file mentioned previously included additional provisioning to remove the "*gsid*" and "*epv*" parameters that may be present within the Contact header. The script was also used to remove unwanted xml element information on the SDP, before the message was sent to the network. See **Section 7.7**.

2.3. Support

For more information on the Masergy SIP Trunking service, visit Masergy at https://www.masergy.com/cloud-communications/intelligent-sip-trunking/

For technical support on the Avaya products described in these Application Notes, visit http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Masergy SIP Trunking Service via a WAN connection through the public Internet.

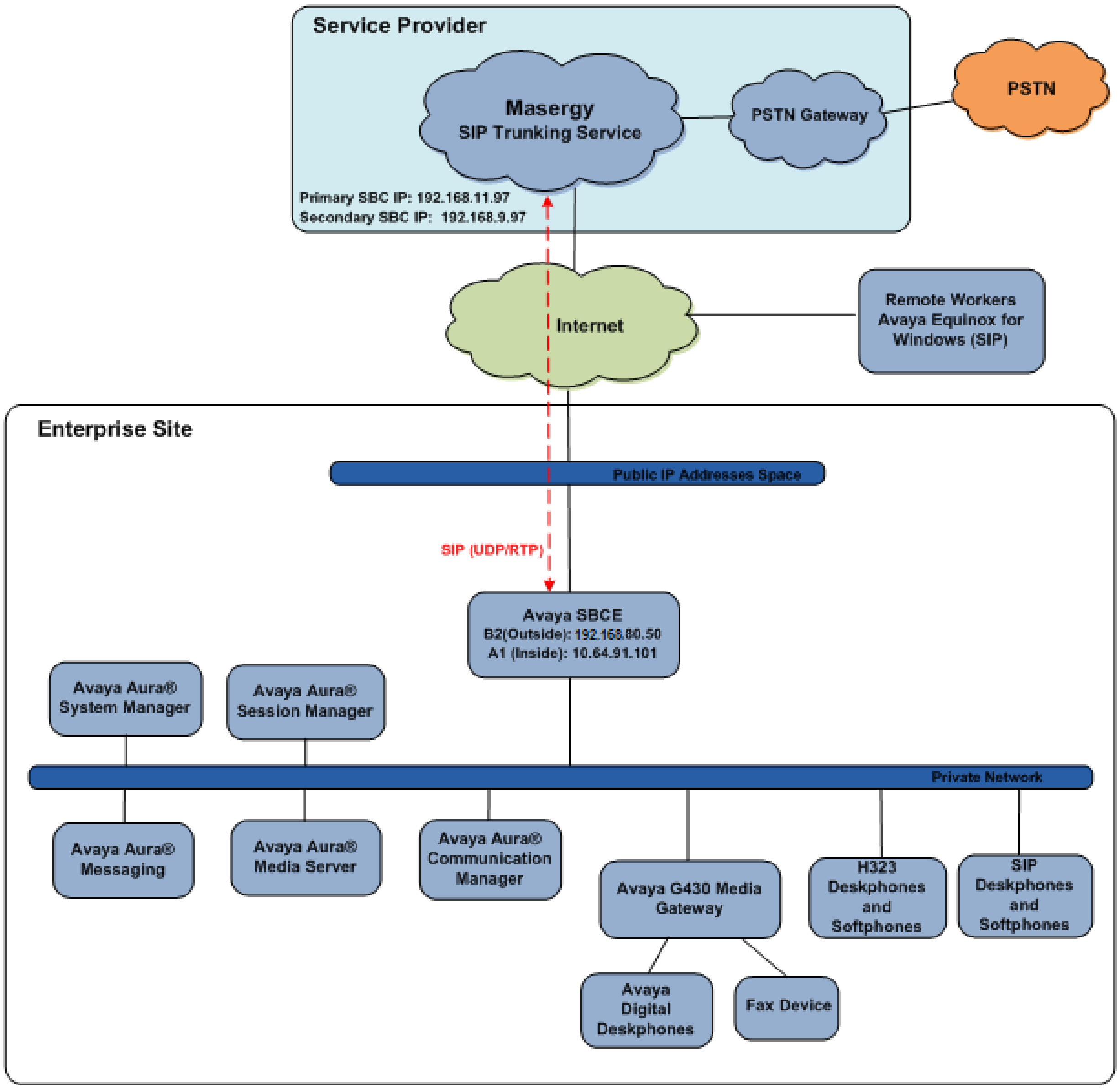


Figure 1: Test Configuration

Note – For security reasons, public IP addresses used in the reference configuration for the Avaya SBCE and the SBCs on the service provider's network are not included in this document. However, as placeholders in the following configuration sections, the IP addresses **192.168.80.50** (Avaya SBCE "Outside" interface B2), and **192.168.11.97 /192.168.9.97**(Masergy SBCs IP addresses), are specified. In addition, DID numbers shown in this document are masked as well.

In an actual customer configuration, the enterprise site may include additional network components between the service provider and the Avaya SBCE, such as a router or data firewall. A complete discussion of the configuration of these devices is beyond the scope of these Application Notes. However, it should be noted that all SIP and RTP traffic between the service provider and the Avaya SBCE must be allowed to pass through these devices.

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 G430 Media Gateway.
- Avaya endpoints

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.

UDP/5060 was the transport protocol/port used to connect the Avaya SBCE "outside" interface to the Masergy SIP trunk, across the public Internet. TLS/5061 was used to connect the "inside" interface of the Avaya SBCE to the Enterprise network.

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 in this case) 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.

Communication Manager and Session Manager were configured to send and receive calls using the E.164 numbering format, as requested by Masergy.

As part of the Avaya Aura® version 8.0 release, Communication Manager includes 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® 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 Masergy SIP Trunking service, they are not included in these Application Notes.

Avaya endpoints are represented by Avaya 9608 H.323 Deskphones, Avaya 9611 and J129 SIP Deskphones, Avaya 9408 Digital Deskphones, as well as Avaya Equinox for Windows (SIP) and Avaya one-X® Communicator for Windows (H323 and SIP) softphones. Fax endpoints are represented by PCs running Ventafax emulation software connected by modem to an analog port of the media gateway.

An Avaya Remote Worker endpoint (Avaya Equinox for Windows) was used in the reference configuration. The Remote Worker endpoint resides on the public side of an Avaya SBCE, and registers/communicates with Session Manager / Communication Manager as though it was an endpoint residing in the private CPE space. The Remote Worker uses protocols Transport Layer Security (TLS) for signaling, and Secure Real-time Transport Protocol (SRTP) for media.

Note – The configuration of the Remote Worker environment is beyond the scope of this document. Refer to [**7**] and [**8**] on the **Additional References** section for information on Remote Worker deployments.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	8.0.1.1.0-FP1SP1
Avaya Aura® System Manager	8.0.1.1.039340
Avaya Aura® Session Manager	8.0.1.1.801103
Avaya Session Border Controller for Enterprise	8.0.0.19
Avaya Aura® Messaging	7.1 SP 1
Avaya Aura® Media Server	8.0.0.183
Avaya G430 Media Gateway	40.25.0
Avaya 96x1 Series IP Deskphone (H.323)	6.8102
Avaya 96x1 Series IP Deskphone (SIP)	7.1.5.0.11
Avaya J129 IP Deskphone (SIP)	4.0.1.0.11
Avaya 9408 Digital Deskphone	2.00
Avaya one X® Communicator (H323, SIP)	6.2.12.23 -SP12-Patch1
Avaya Equinox™ for Windows	3.5.7.30.1
Fax device	Ventafax 7.10
Masergy	
Broadsoft Softswitch	R21sp1
Oracle SBC	scz7.2.0M6P2

Table 1: Equipment and Software Versions

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the Masergy 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 Aura® 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.

5.1. Licensing and Customer Options

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 **4000** licenses are available and **75** 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: 4000  0
           Maximum Concurrently Registered IP Stations: 1000  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 1000  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 1000  6
                       Maximum Administered SIP Trunks: 4000  75
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

On **Page 5** of the form, verify that the **Enhanced EC500**, **IP Trunks**, and **ISDN-PRI,** features are enabled. If the use of SIP REFER messaging will be required, verify that the **ISDN/SIP Network Call Redirection** feature is enabled. If SRTP will be required, verify that the **Media Encryption Over IP** feature is enabled.

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

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

           IP Attendant Consoles? Y
```

On **Page 6** of the form, verify that the **Processor Ethernet** field is set to **y**.

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

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

5.2. System Features

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

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

              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:
```

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Communication Manager processor ethernet interface ***(*****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
AMS                  10.64.91.80
IPOSE                10.64.19.170
SM                   10.64.91.81
default              0.0.0.0
procr                10.64.91.75
procr6               ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 7 was used for this purpose. Masergy used codecs G.711MU, G.711A and G.729A on the SIP trunk, in this order of preference. Enter the corresponding codecs in the **Audio Codec** column of the table.

```
change ip-codec-set 7                                         Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 7

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

     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
```

On **Page 2** of the ip-codec-set form, set **FAX Mode** to **t.38-standard**. Leave **ECM** at the default value of **y**.

```
change ip-codec-set 7                                          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
```

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 7 was chosen for the service provider trunk. Use the **change ip-network-region** command to configure the region with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avayalab.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. 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 7                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 7       NR Group: 7
Location: 1       Authoritative Domain: avayalab.com
    Name: Masergy                 Stub Network Region: n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 7                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 7 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 **7** will be used for calls between region 7 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 7                                      Page   4 of  20

 Source Region: 7     Inter Network Region Connection Management     I     S M
                                                                     G  A  y t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G  n c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L  c e
 1    7     y    NoLimit                                             n     y t
 2
 3
 4
 5
 6
 7    7                                                                all
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager, for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 7 was used and was configured using the parameters highlighted below:

- 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**.

```
display signaling-group 7                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 7              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: 5067                Far-end Listen Port: 5067
                                        Far-end Network Region: 7

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

- 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 the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For the compliance test both the **Near-end Listen Port** and **Far-end Listen Port** were set to **5067**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway 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, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

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 7 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 the previous section.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
display trunk-group 7                                           Page   1 of   4
                                TRUNK GROUP

Group Number: 7                   Group Type: sip           CDR Reports: y
  Group Name: Masergy                    COR: 1        TN: 1        TAC: *07
   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: 7
                                                     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 in which UPDATES must be sent to keep the active session alive. The default value of **600** seconds was used.

```
display trunk-group 7                                           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
```

On **Page 3**, the **Numbering Format** field specifies the format of the calling party number (CPN) sent to the far-end. The compliance test used numbering format E.164. Thus, **Numbering Format** was set to **public**. 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.

```
display trunk-group 7                                               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
```

On **Page 4**, set the **Network Call Redirection** to **y**. With this setting, Communication Manager will use the SIP REFER method, which is supported by Masergy, for the redirection of PSTN calls that are transferred back to the SIP trunk. Set **Send Diversion Header** and **Support Request History** fields to **y**. Set the **Telephone Event Payload Type** to **101**, the value preferred by Masergy. Default values were used for all other fields.

```
display trunk-group 7                                               Page   4 of   4
                              PROTOCOL VARIATIONS

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

                        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 Number 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. The DID numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers are assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

On the screen below, note that since these entries apply to a SIP connection to Session Manager (Trunk Group 7), the resulting number must be complete E.164 number. Communication Manager automatically will insert a "+" in front of the user number in the From, P-Asserted-Identity, Contact and Diversion headers.

```
change public-unknown-numbering 5                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                              Total
Ext Ext              Trk       CPN             CPN
Len Code             Grp(s)    Prefix          Len
                                                  Total Administered: 53
 5  50231            7         14241234567     11    Maximum Entries: 240
 5  50232            7         14241234568     11
 5  50238            7         14241234569     11 Note: If an entry applies to
                                                  a SIP connection to Avaya
                                                  Aura(R) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.

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

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 sent by the service provider 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.

On the example below, all 12 incoming digits on the DIDs are deleted, and the 5 digit internal extension numbers are inserted.

```
change inc-call-handling-trmt trunk-group 7                    Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    12 +14241234567     12  50231
 public-ntwrk    12 +14241234568     12  50232
 public-ntwrk    12 +14241234569     12  50238
 public-ntwrk
 public-ntwrk
```

5.10. Outbound Route Selection

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
 1             5  ext
 2             5  ext
 3             5  ext
 4             5  ext
 5             5  ext
 60            3  ext
 66            2  fac
 67            4  ext
 7             5  ext
 8             5  ext
 9             1  fac
 *             3  dac
 #             3  fac
```

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

```
change feature-access-codes                                    Page   1 of  11
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code: #40
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 66
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *33    Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
```

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 patterns **7** or **8**, which contain the SIP trunk group to the service provider.

```
change ars analysis 011                                        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
    011                  10   18    8        intl         n
    14                   11   11    7        fnpa         n
    15                   11   11    7        fnpa         n
    18                   11   11    7        fnpa         n
    19                   11   11    7        fnpa         n
```

5.11. Route Patterns

Route patterns defines which trunk group will be used for an outbound 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. In the reference configuration, route pattern 7 was used for national calls and route pattern 8 was used for international calls,

Enter the **change route-pattern 7** command to configure a route pattern for national calls. Enter the following parameters:

- In the **Grp No** column, enter **7** for public trunk 7, and the **FRL** column enter **0** (zero).
- 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.

```
change route-pattern 7                                          Page   1 of   4
                    Pattern Number: 7      Pattern Name: To Masergy
    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: 7    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                                          none
```

Enter the **change route-pattern 8** command to configure a route pattern for international calls.

- In the **Grp No** column, enter **7** for public trunk 7, and the **FRL** column enter **0** (zero).
- In the **Pfx mrk** column, leave blank (default).
- In the **No. Del Digits** column, enter **3** to have Communication Manager remove the international 011 prefix from the number.
- 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.

```
change route-pattern 8                                          Page   1 of   4
                    Pattern Number: 8      Pattern Name: 011 to Masergy
    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: 7    0                    3   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                                          none
```

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

6. Configure Avaya Aura® Session Manager

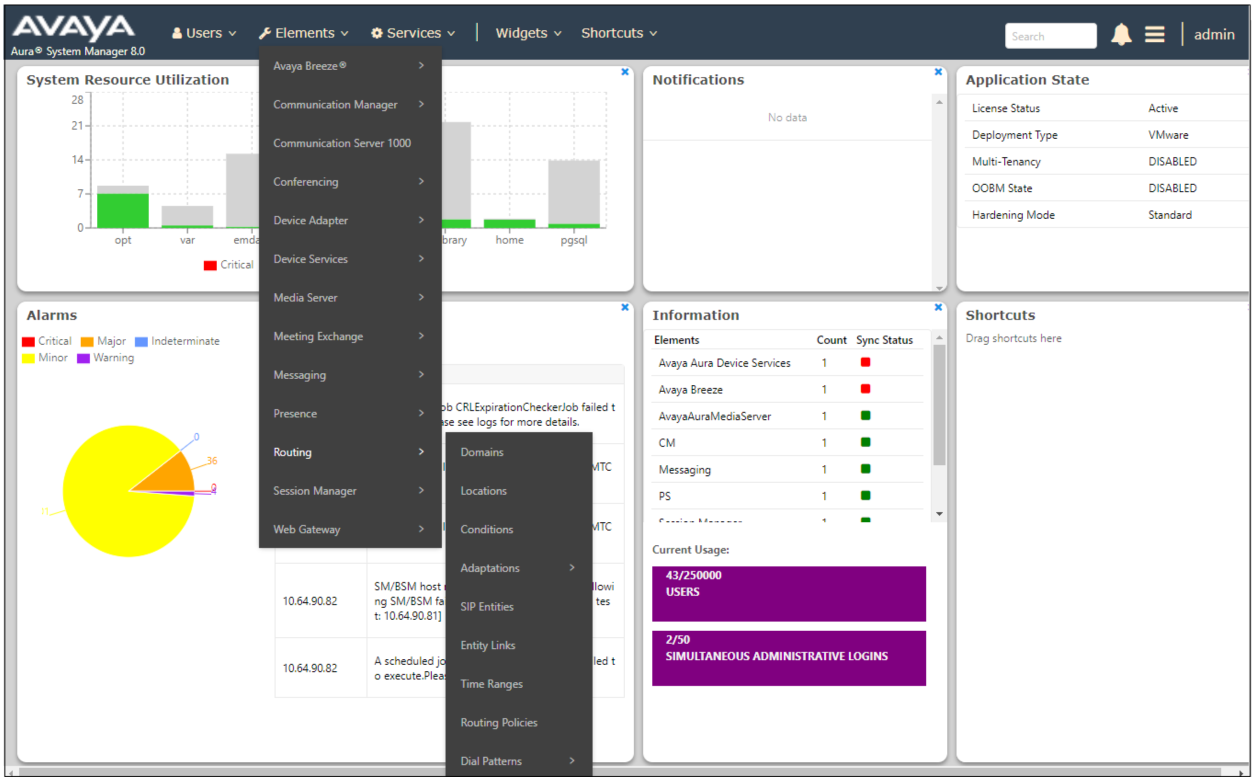
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

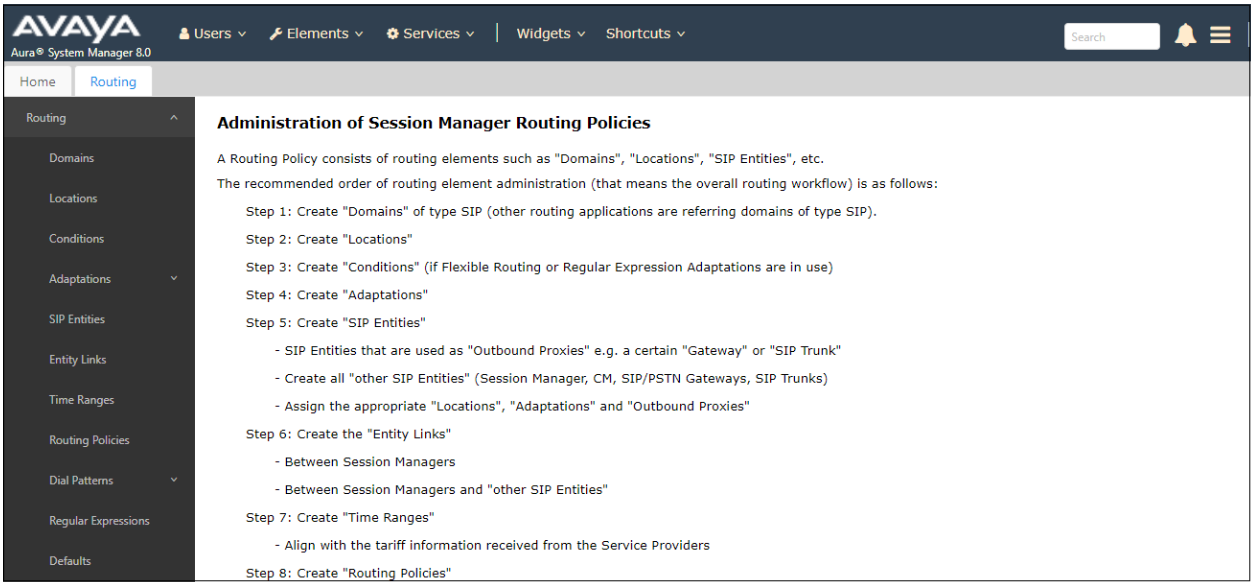
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. 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). Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading, select **Routing**.



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** element shown below.



6.2. 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, **avayalab.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**. The screen below shows the entry for the enterprise domain.

6.3. 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. In the reference configuration, two locations are specified:

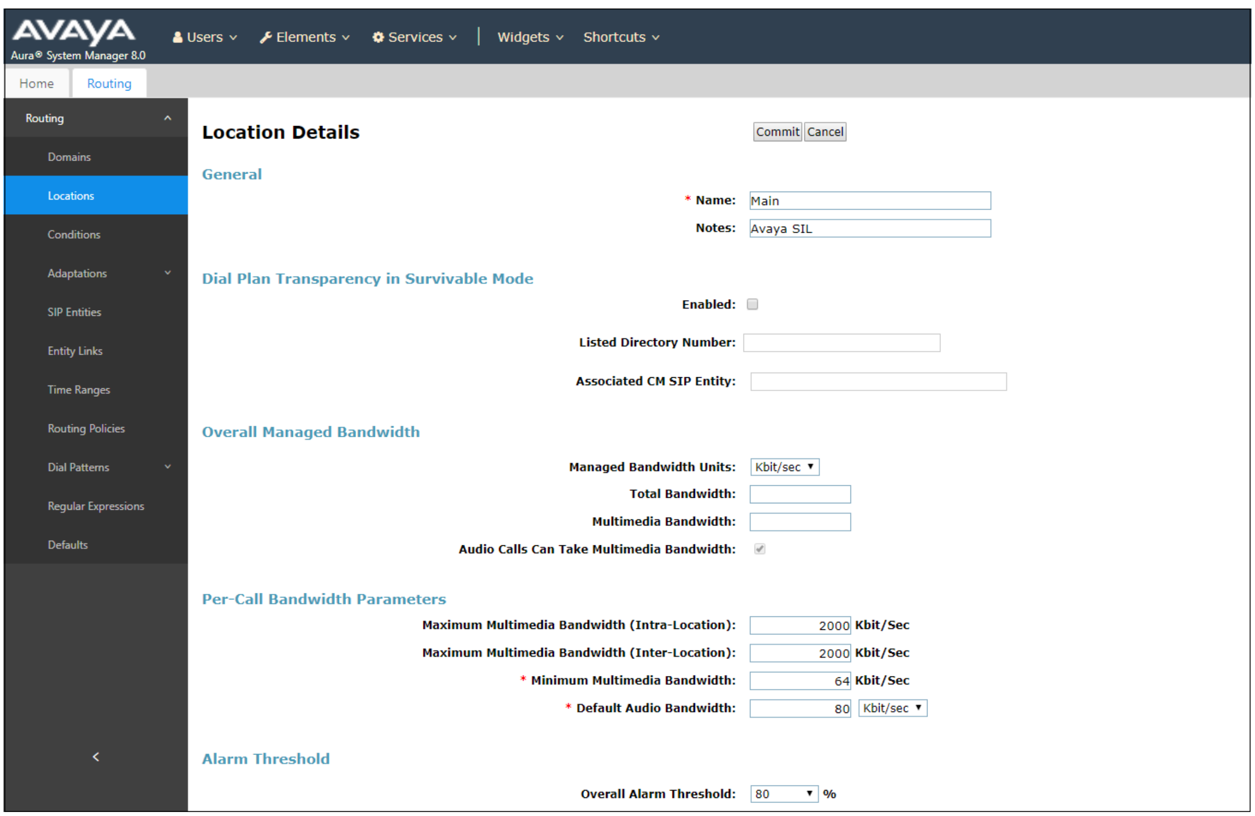
- **Main** – The customer site containing Session Manager, Communication Manager and local SIP endpoints.
- **Common SBCs** – Avaya SBCE

To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values.

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

Defaults can be used for all other parameters.

The following screen shows the location details for the location named **Main**.



A second location named **Commom-SBCs** (not shown) was similarly created following the steps described above.

6.4. Adaptations

Adaptations can be used to alter the parameters on the headers of SIP messages entering or leaving Session Manager, to meet the specific requirements of the service. Adaptations can also be used as a tool to improve interoperability with third party elements. Session Manager 8.0 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary, or deemed excessive/unnecessary for non-Avaya elements.

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

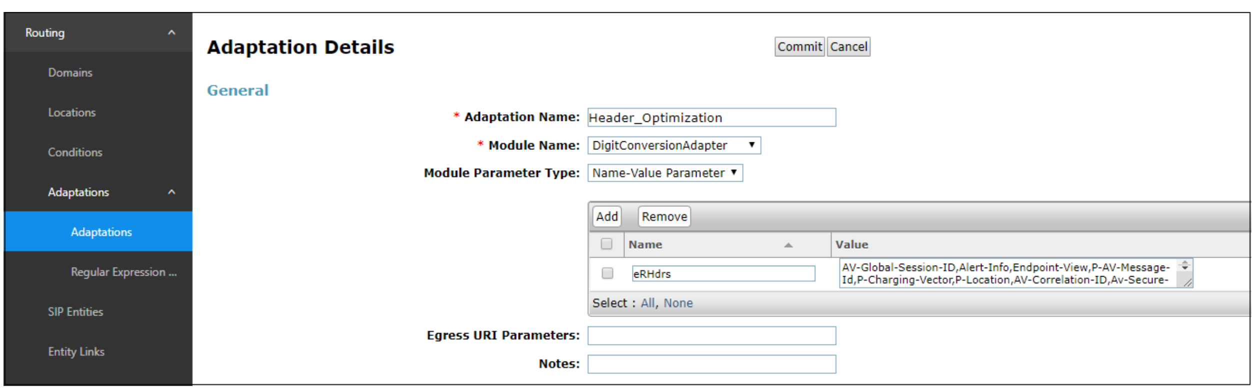
Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name**: Enter an appropriate name.
- **Module Name**: Select the **DigitConversionAdapter** option.
- **Module Parameter Type**: Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

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

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 with their default values.

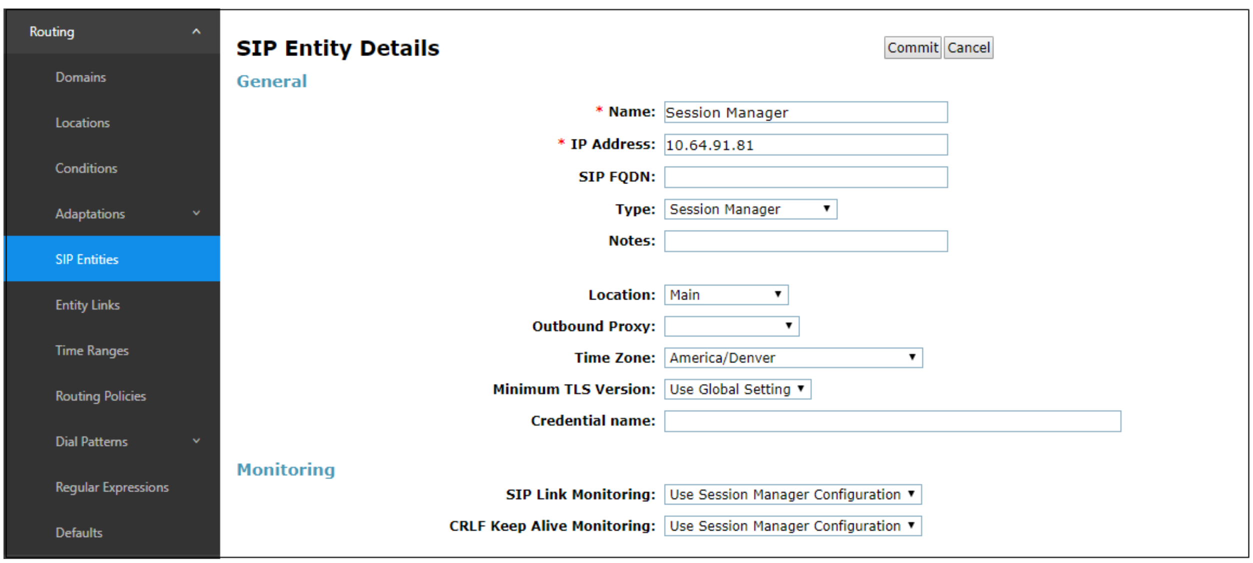


6.5. SIP Entities

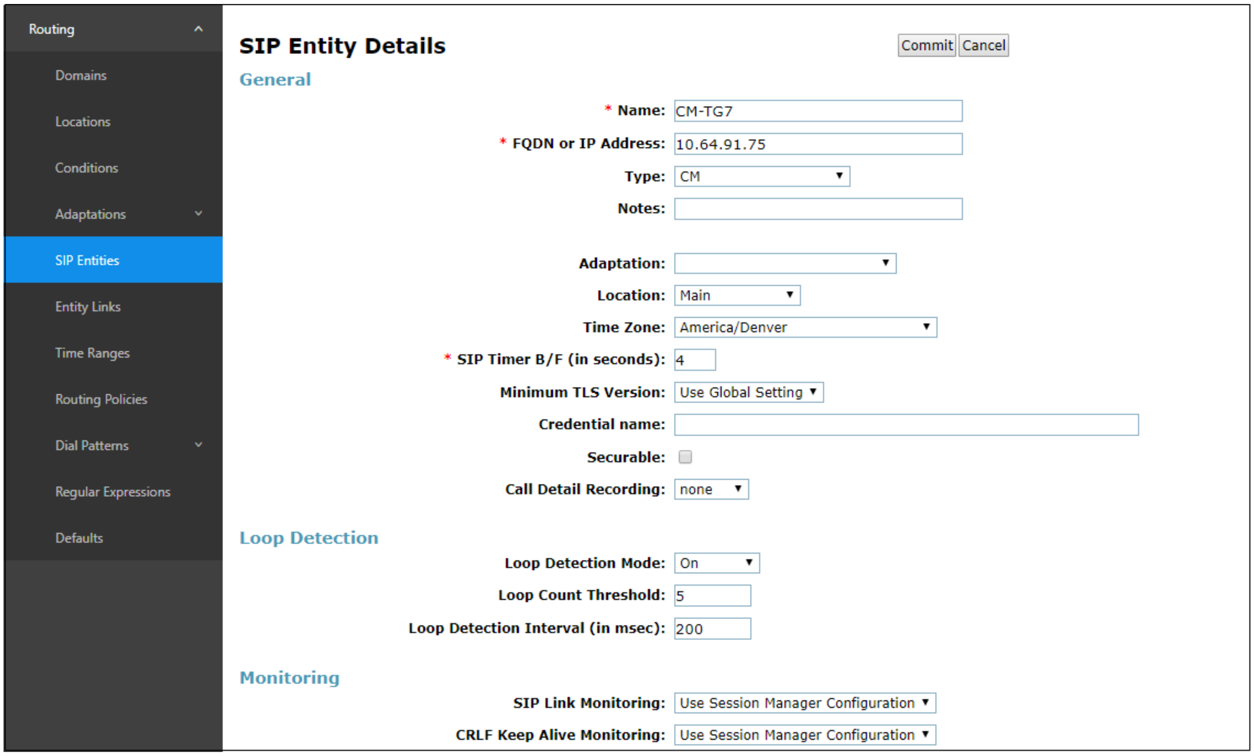
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** 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.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager** If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

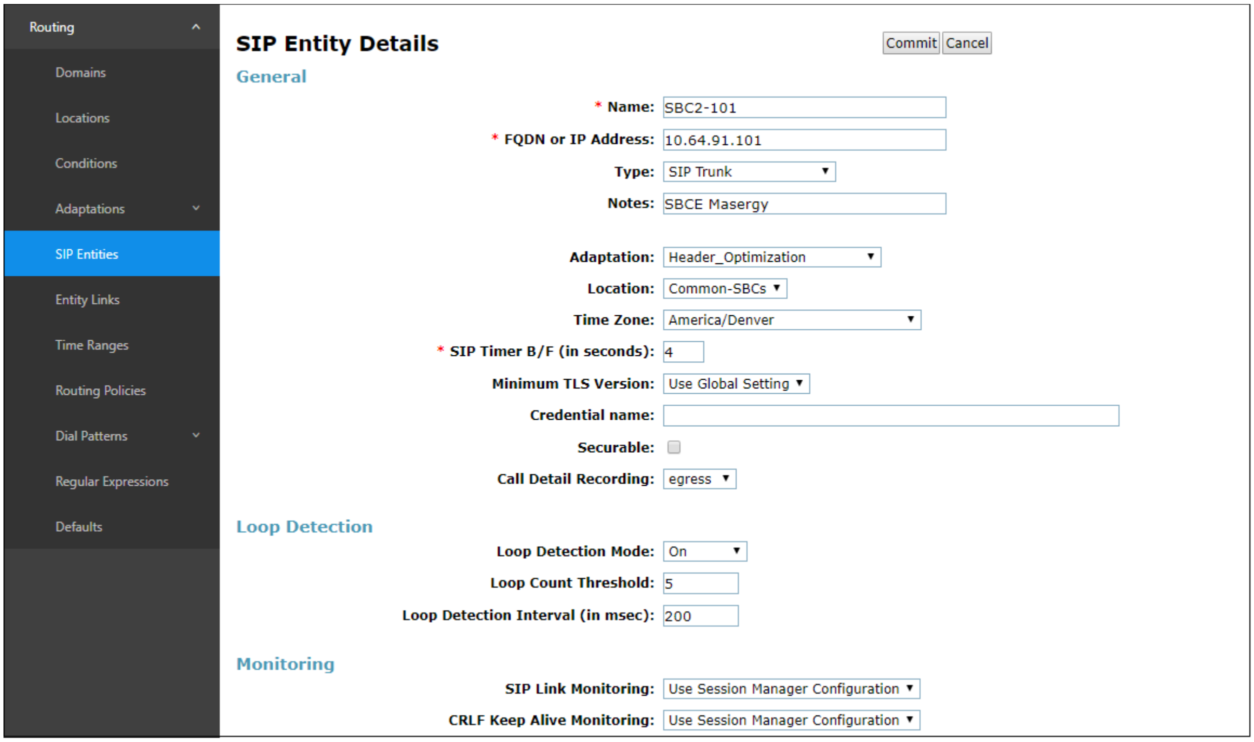
The following screen shows the addition of the **Session Manager** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field. The **Location** is set to the **Main** location defined in **Section 6.3**



The following screen shows the addition of the SIP Entity **CM-TG7** 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**. The **Location** is set to the **Main** location defined in **Section 6.3**.



The following screen shows the addition of the SIP Entity **SBC2-101**, for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface. On the **Adaptation** field, the adaptation module **Header_Optimization** previously defined in **Section 6.4** is selected. The **Location** is set to the **Common-SBCs** location defined in **Section 6.3**.



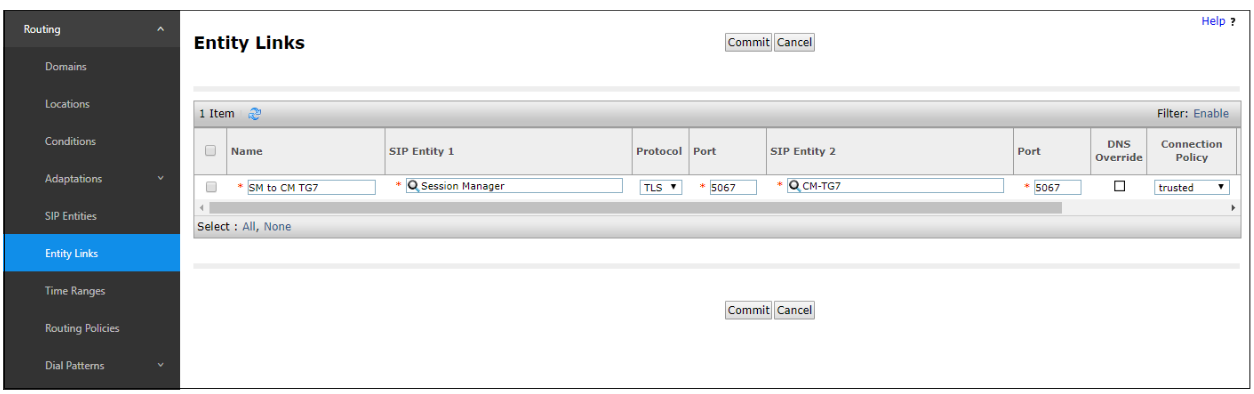
6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left 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:

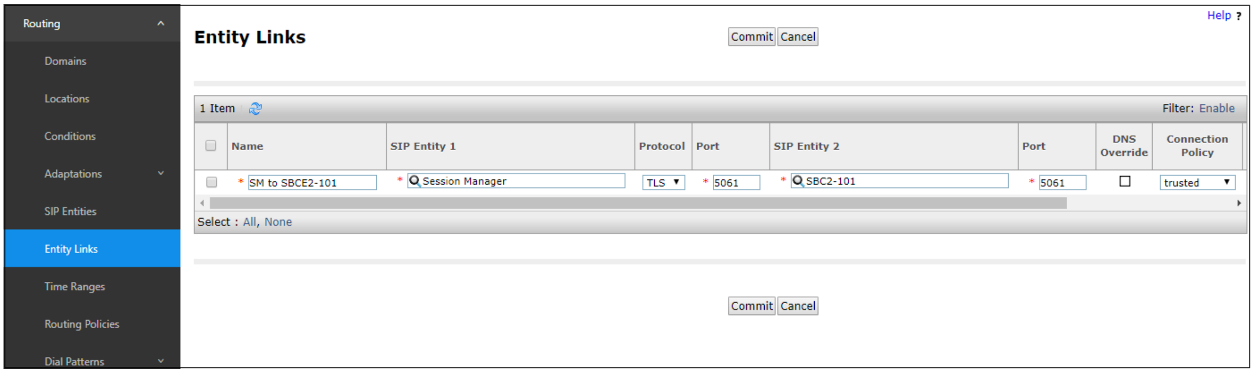
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager .
- **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 (**TLS**) and ports (**5067**) defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.



The Entity Link to the Avaya SBCE is show below. Protocol **TLS** and port **5061** were used.

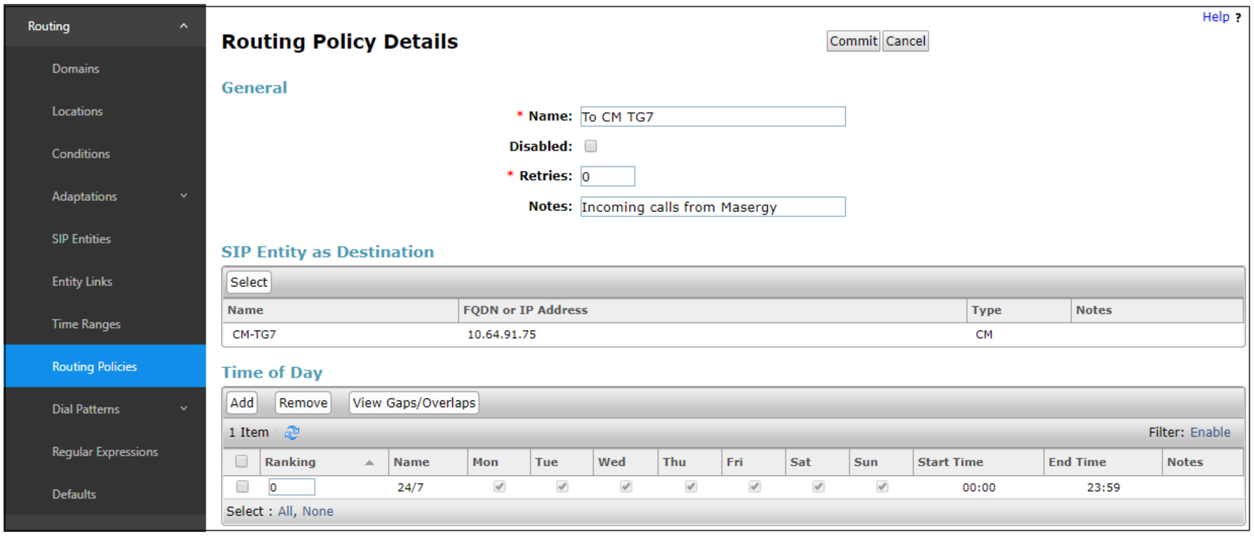


6.7. Routing Policies

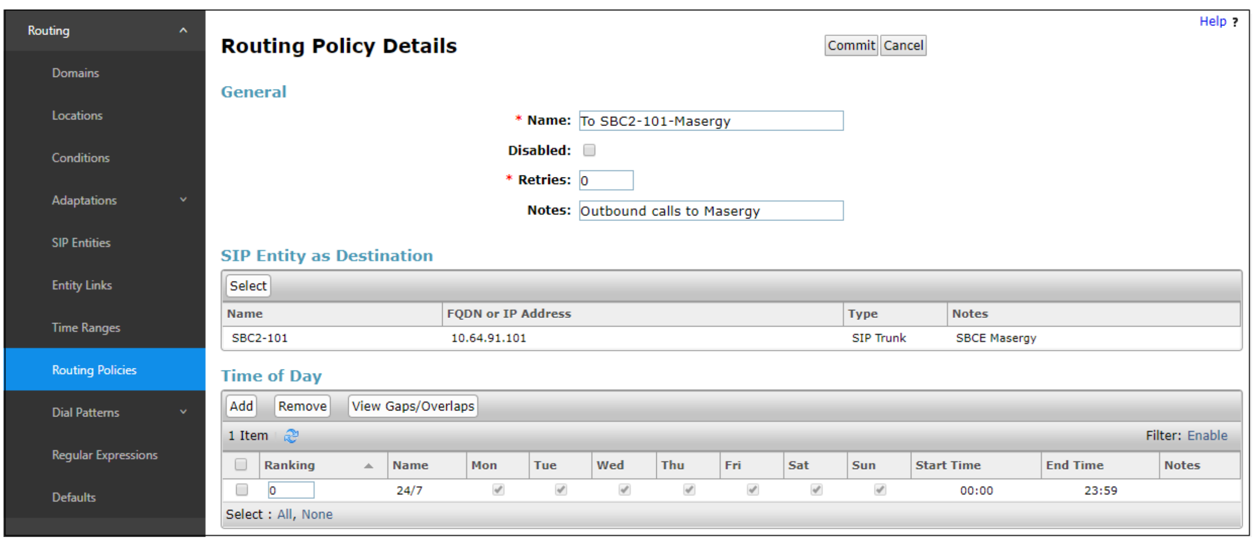
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **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 6.5**) 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 screen below shows the Routing Policy named **To CM TG7,** for inbound calls from the Masergy SIP trunk. The SIP Entity corresponding to Communication Manager is selected as the destination.



The screen below shows the Routing Policy named **To SBC2-101-Masergy**, for outbound calls to Masergy. The SIP Entity corresponding to the Avaya SBCE is selected as the destination.



6.8. 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 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:

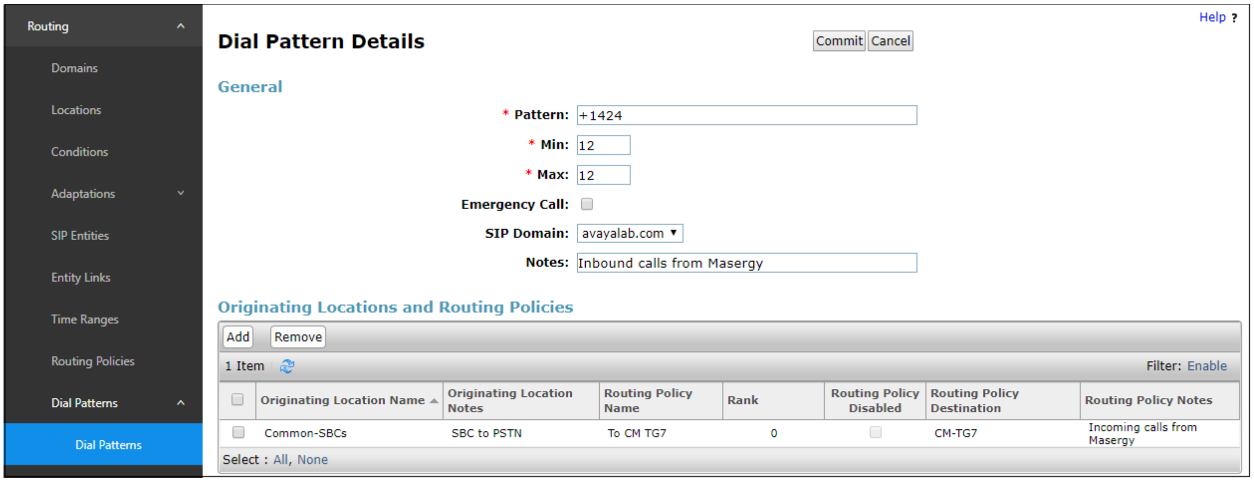
In the **General** section, enter the following values:

- **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).

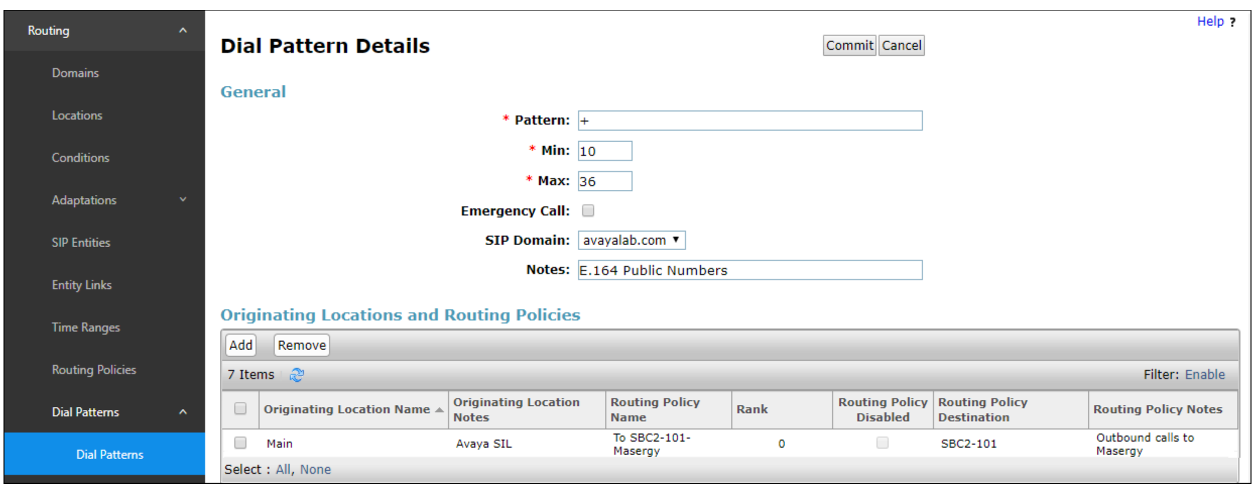
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to the E.164 formatted DID numbers assigned by the service provider to the enterprise, starting with **+1424**, string 12 digits long, arriving from the SBCE location (e.g., **Common-SBCs)**, used route policy **To CM TG7** to Communication Manager.



The screen below shows an example the dial pattern used to verify national and international outbound calls. This dial pattern will match any outbound call prefixed with a plus sign (+), such as an E.164 formatted number, arriving from the Communication Manager location (e.g., **Main**), strings 10 to 36 digits long, used route policy **To SBC2-101-Masergy**

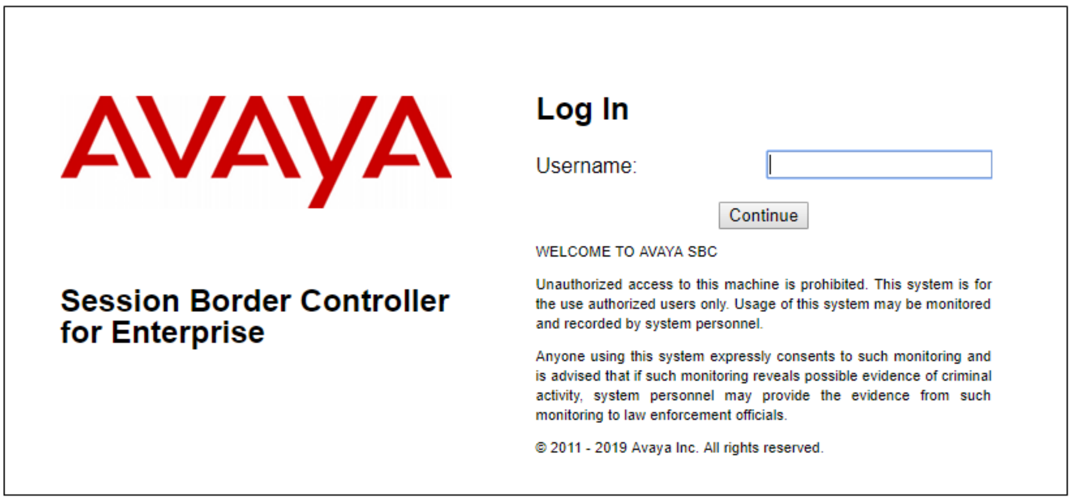


7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, including 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 provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

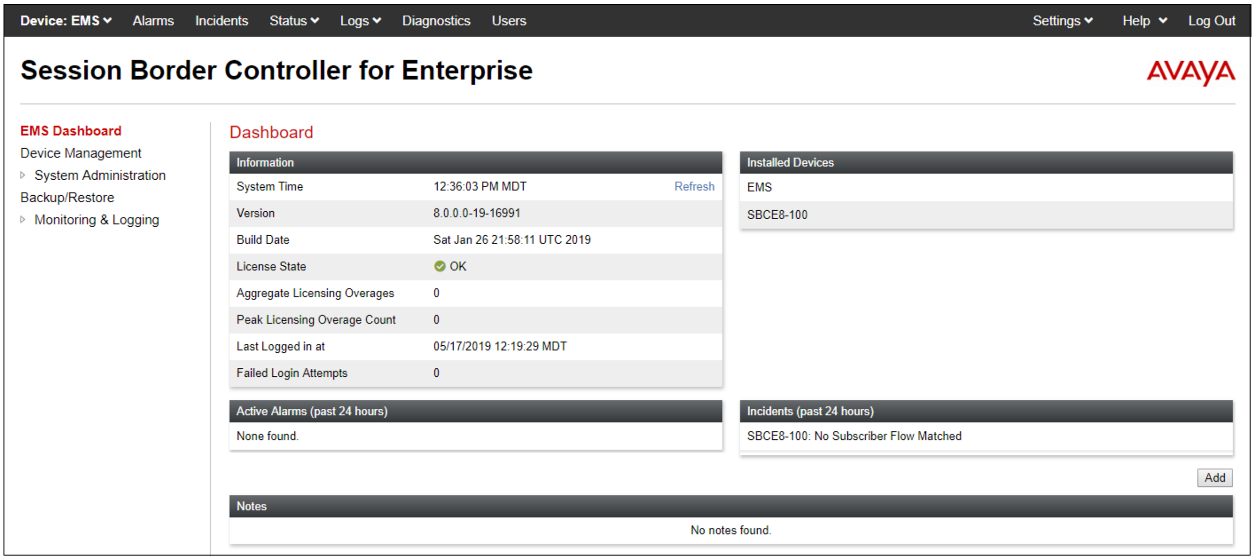
Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE.

Enter the **Username** and click on **Continue**.



Enter the password and click on **Log In**.

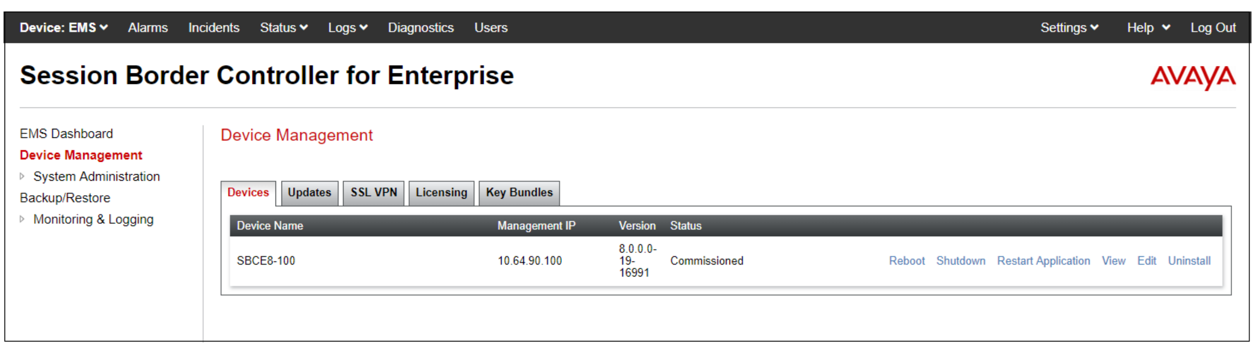
The EMS Dashboard page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.



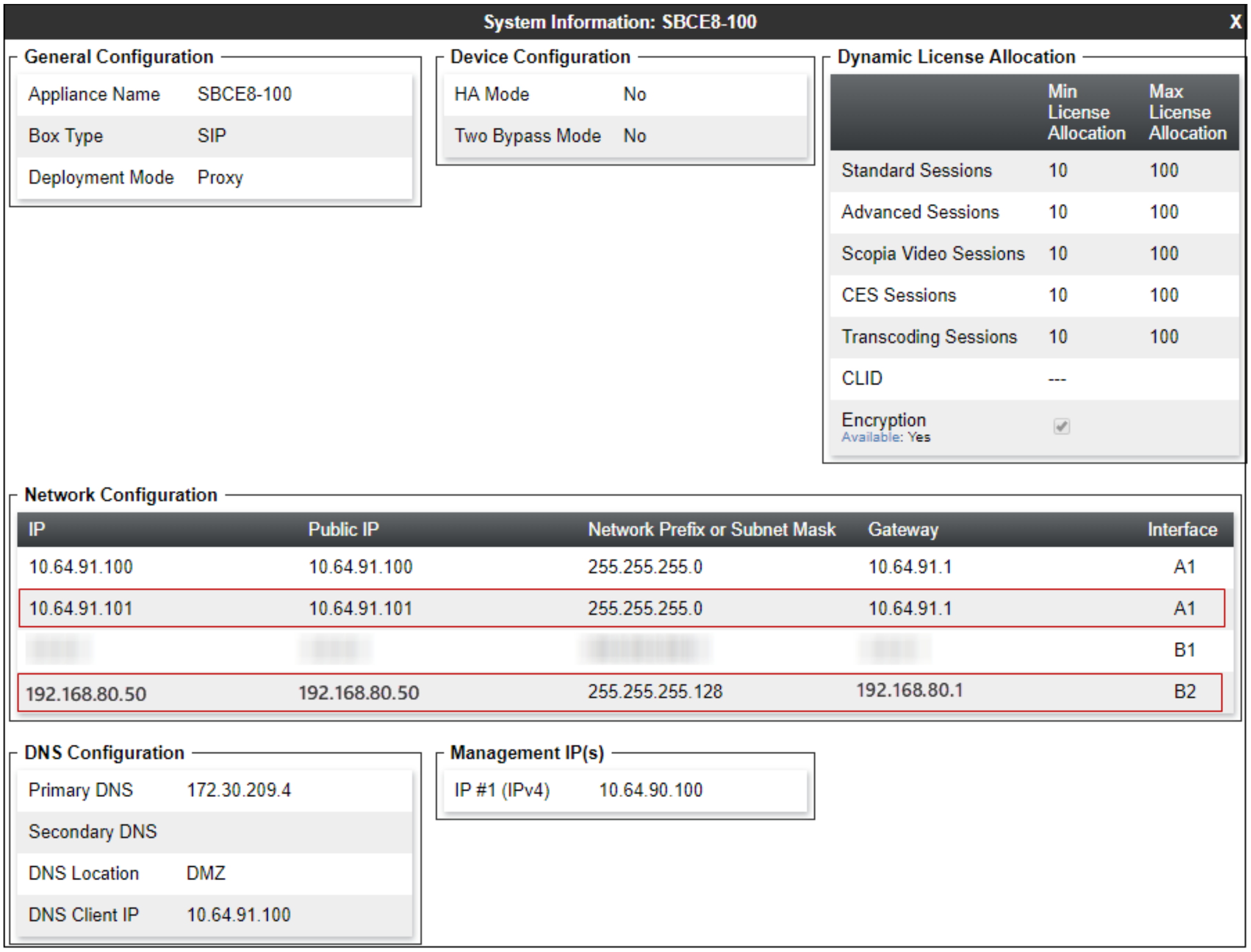
7.1. Device Management – Status

Select **Device Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative. To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **SBCE8-100** is shown. To view the configuration of this device, click **View** on the screen below.

Note – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.



The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. In the shared test environment, the highlighted **A1** and **B2** IP addresses are the ones relevant to the configuration of the SIP trunk to Masergy.



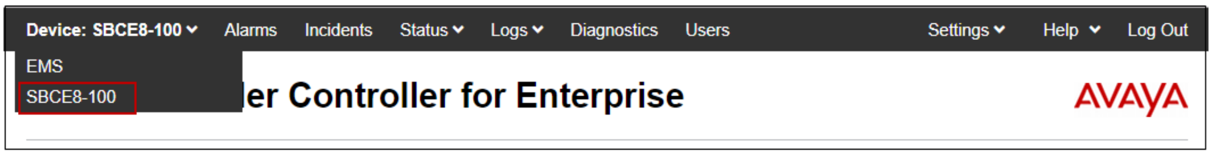
7.2. TLS Management

Note – Testing was done using identity certificates signed by a local certificate authority. 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 Avaya SBCE. The following procedures show how to view the certificates and configure the profiles to support the TLS connection.

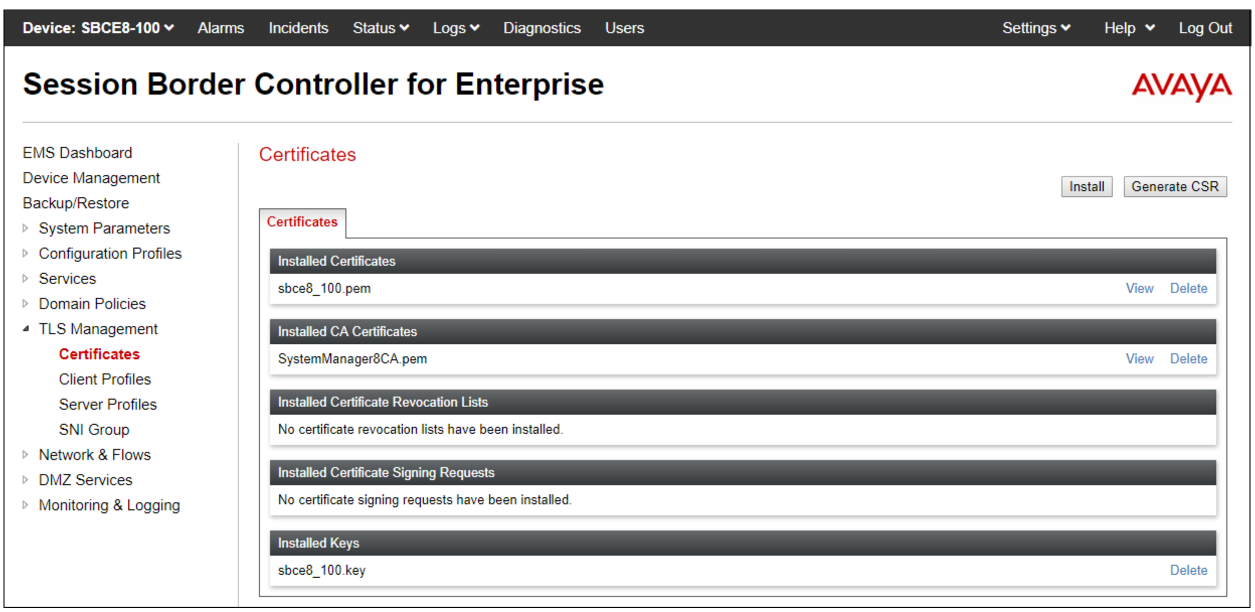
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



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

- The root CA certificate is present in the **Installed CA Certificates** area.
- The signed identity certificate is present in the **Installed Certificates** area.
- The private key associated with the identity certificate is present in the **Installed Keys** area.

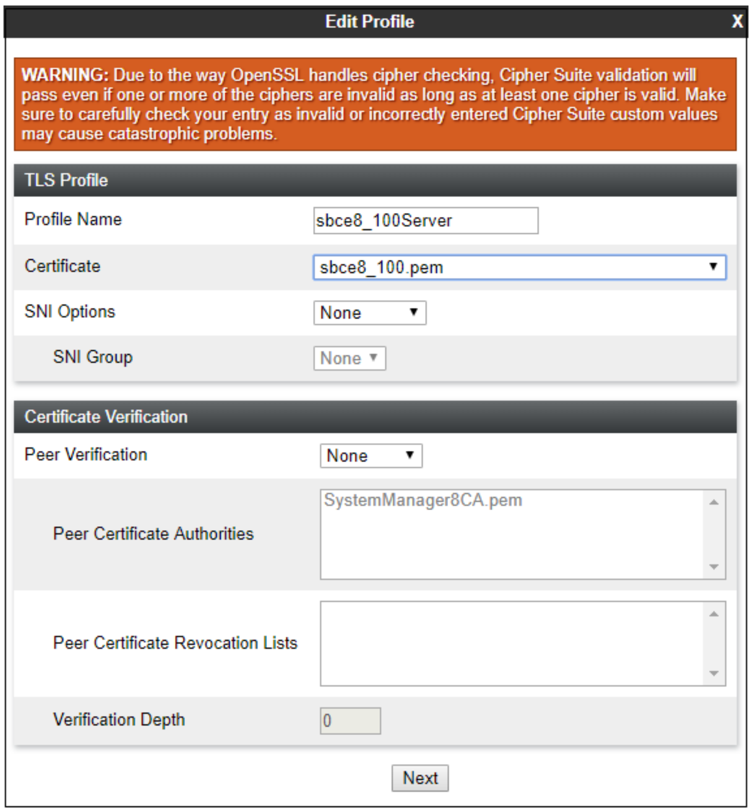


7.2.2. Server Profiles

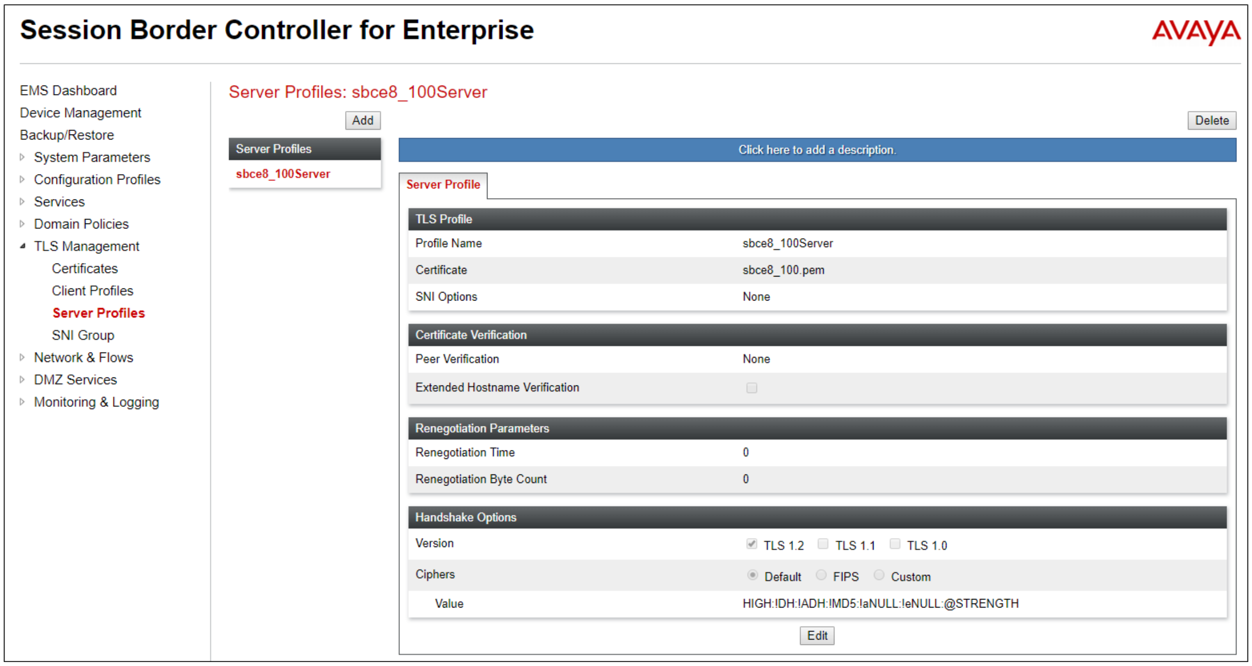
Select **TLS Management → Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_100.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

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



The following screen shows the completed TLS **Server Profile** form:

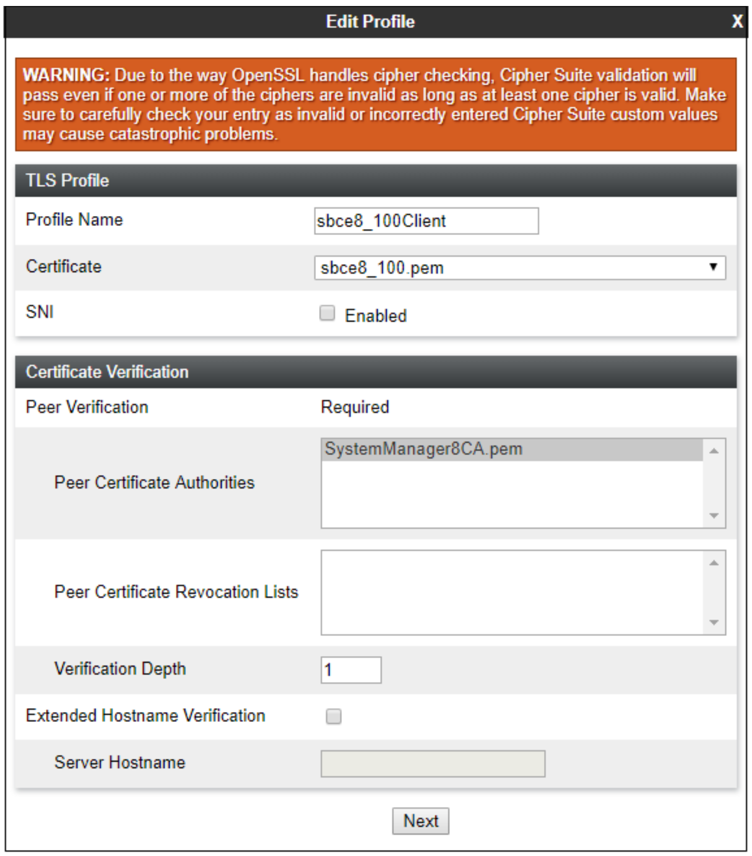


7.2.3. Client Profiles

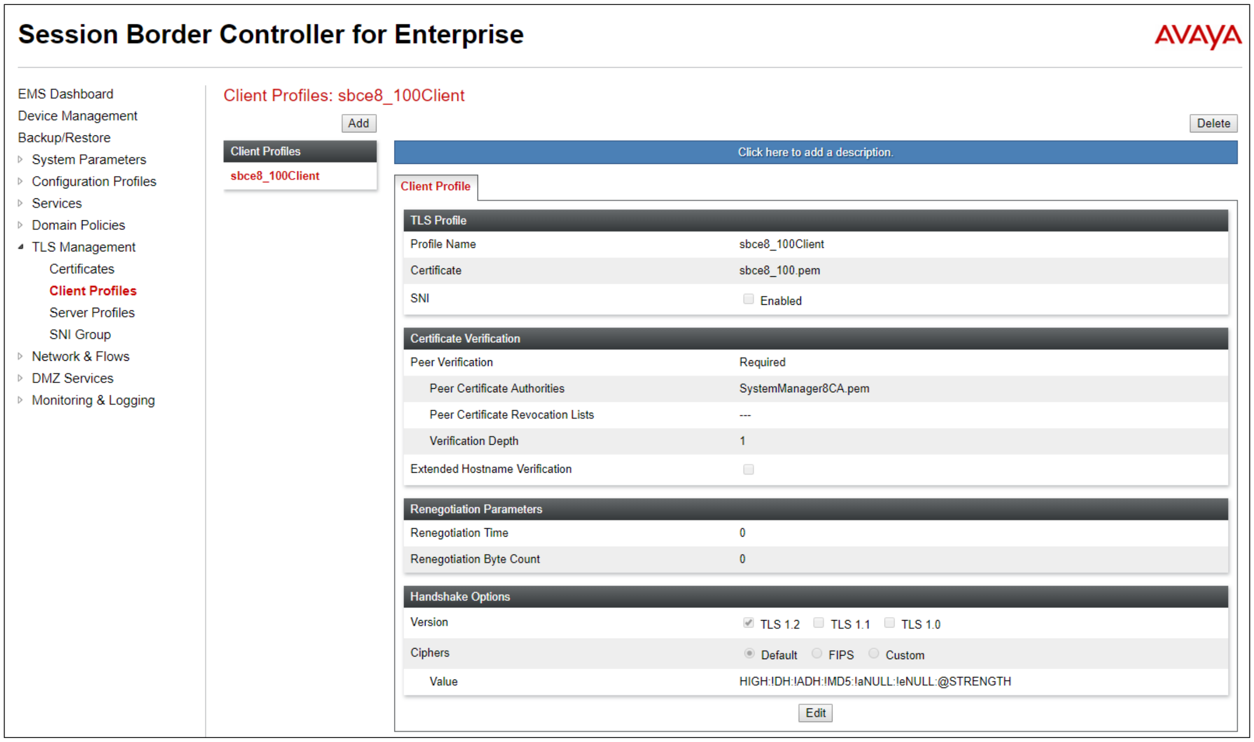
Select **TLS Management → Client Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_100.pem**, from pull down menu.
- **Peer Verification** = **Required**.
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManager8CA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

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



The following screen shows the completed TLS **Client Profile** form:

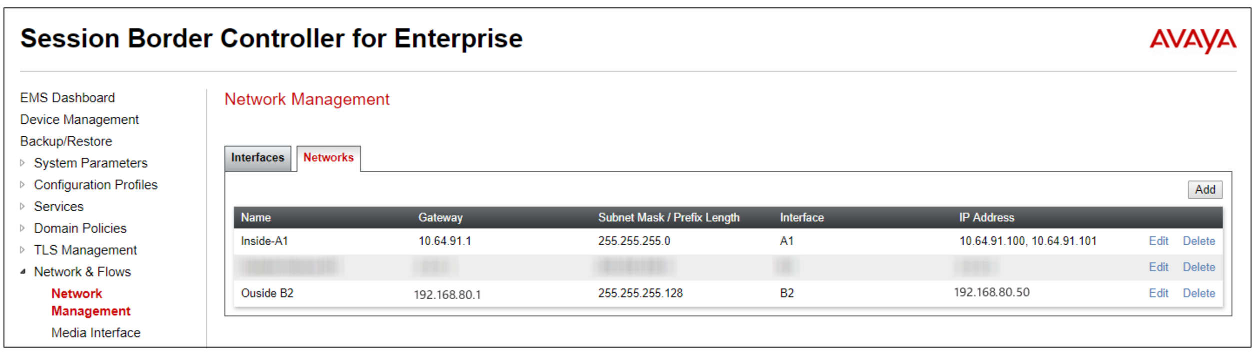


7.3. Network Management

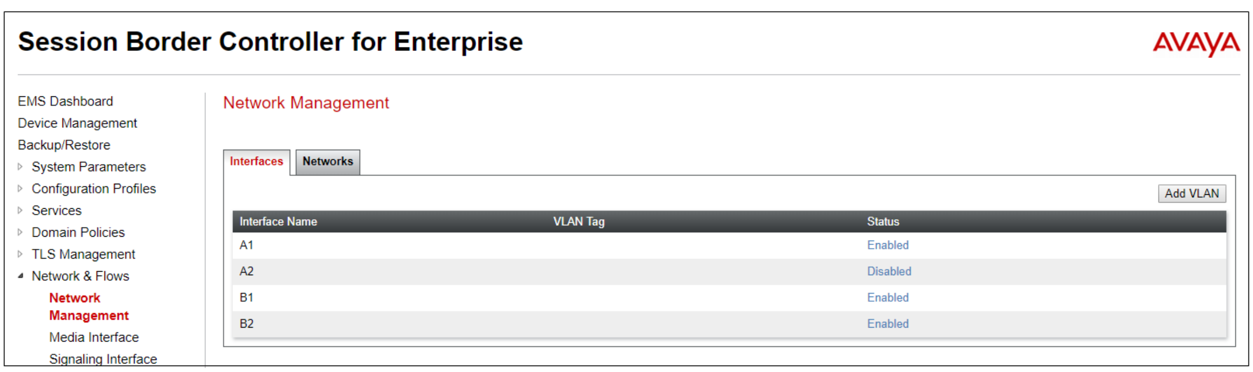
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Networks & Flows → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the enterprise interface is assigned to **A1** and the interface toward Masergy is assigned to **B2**.

The following Avaya SBCE IP addresses and associated interfaces were used in the sample configuration for the Masergy SIP Trunking service:

- **A1**: **10.64.91.101** – "Inside" IP address, toward Session Manager.
- **B2: 192.168.80.50** – "Outside" IP address toward the Masergy SIP trunk. This address is known to Masergy.



The following screen shows interface **A1**, and **B2** are **Enabled**. To enable an interface, click the corresponding **Disabled** Status link to change it to **Enabled**.

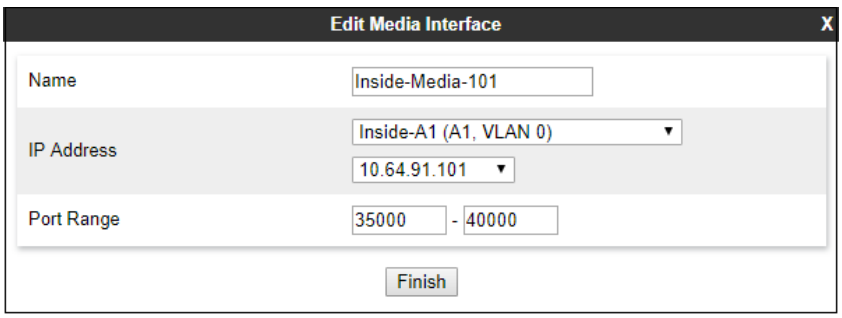


7.4. Media Interface

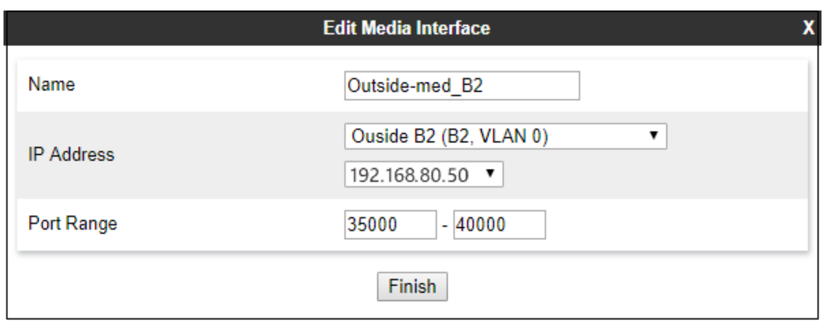
The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP Media Interface for the inside and outside IP interfaces.

To add the Media Interface in the enterprise direction, select **Network & Flows → Media Interface** from the menu on the left-hand side, and click the **Add** button (not shown). On the -**Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the Avaya SBCE private IP Address from the **IP Address** drop-down menu. The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.

The screen below shows the **Inside-Media-101** media interface created in the reference configuration.



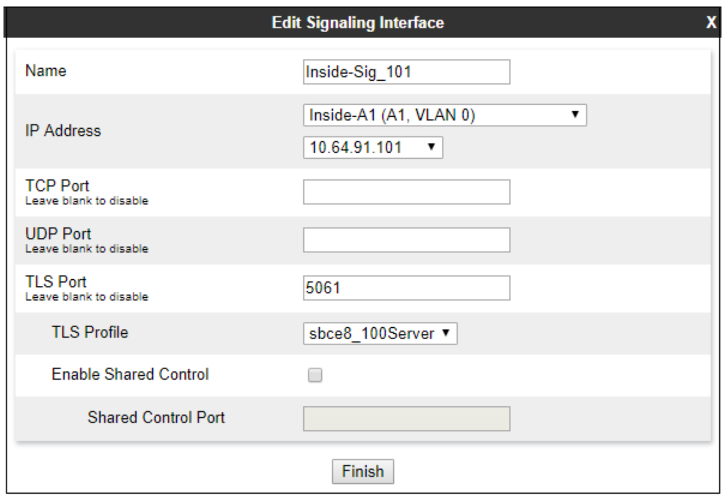
A second Media Interface facing the public network side was similarly created with the name **Outside-med_B2**, as shown below. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was left at the default values. Click **Finish**.



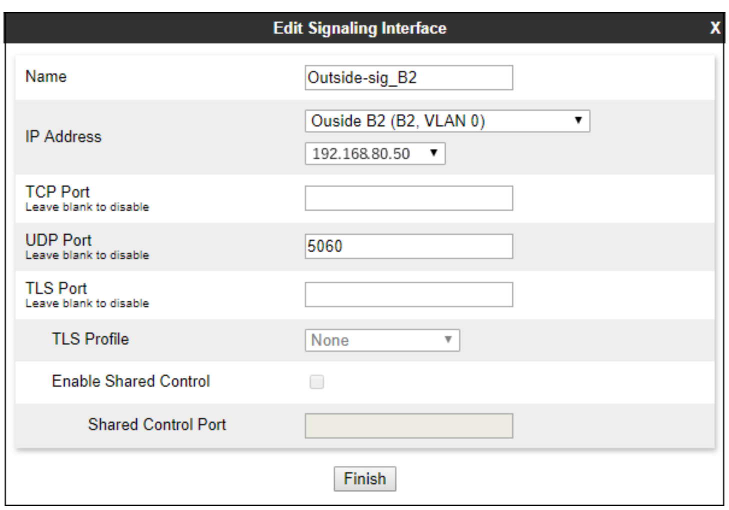
7.5. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for the inside and outside IP interfaces.

To create a new Signaling Interface on the enterprise direction, navigate to **Network and Flows → Signaling Interface** and click Add. On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Since TLS is used in the sample configuration to listen for signaling traffic from the Session Manager, **5061** is entered under **TLS Port**. The TLS Profile is set to the TLS server profile **sbce8_100Server** shown on **Section 7.2.2**. Click **Finish**.



A second Signaling Interface with the name **Outside-sig_B2** was similarly created in the network direction. The B2 interface IP Address of the Avaya SBCE was selected from the drop-down menu. Under **UDP Port,** enter **5060** as specified by Masergy. Click **Finish**.



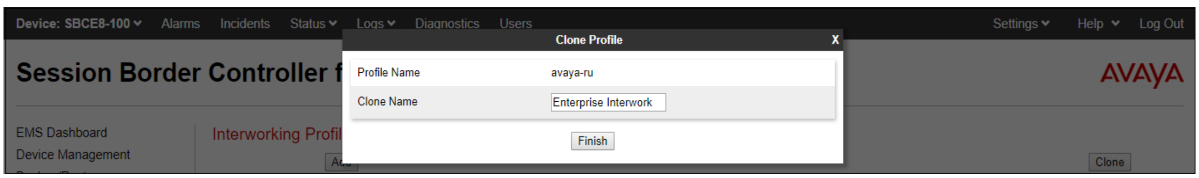
7.6. Server Interworking Profile

The Server Interworking Profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

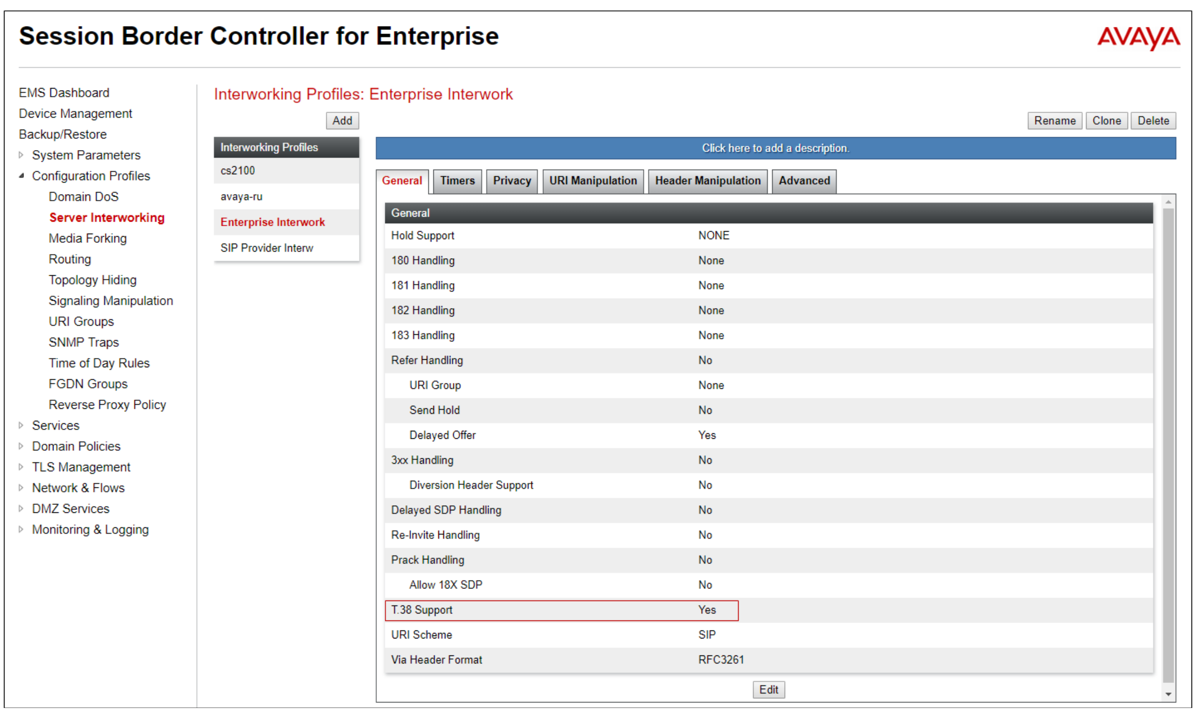
In the sample configuration, separate Server Interworking Profiles were created for the enterprise and the service provider.

7.6.1. Server Interworking Profile – Enterprise

In the sample configuration, the enterprise Server Interworking profile was cloned from the default **avaya-ru** profile. Navigate to **Configuration Profiles → Server Interworking**, select the **avayu-ru** profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.

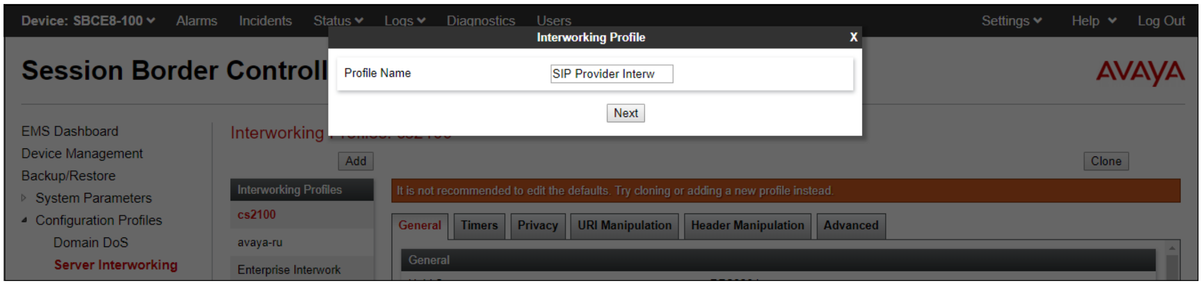


The following screen shows the **Enterprise Interwork** profile used in the sample configuration, with **T.38 Support** set to **Yes**. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown). Default values can be used for all other fields.

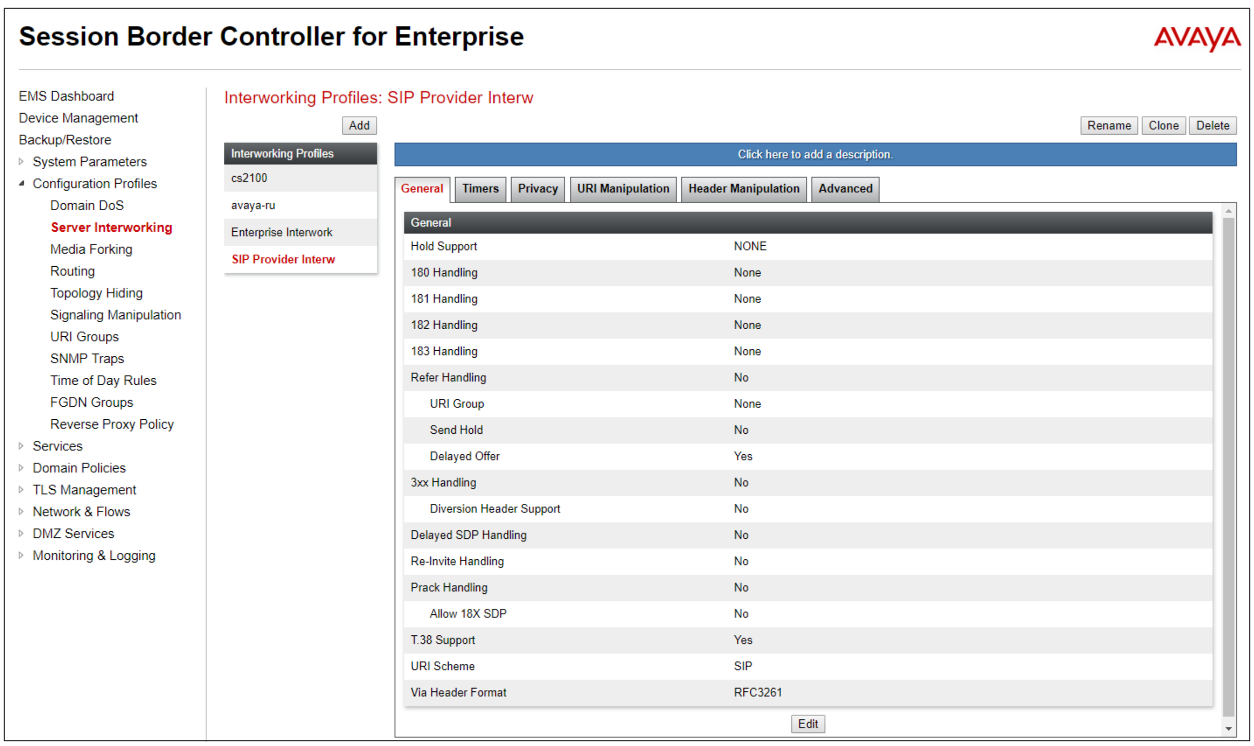


7.6.2. Server Interworking Profile – Service Provider

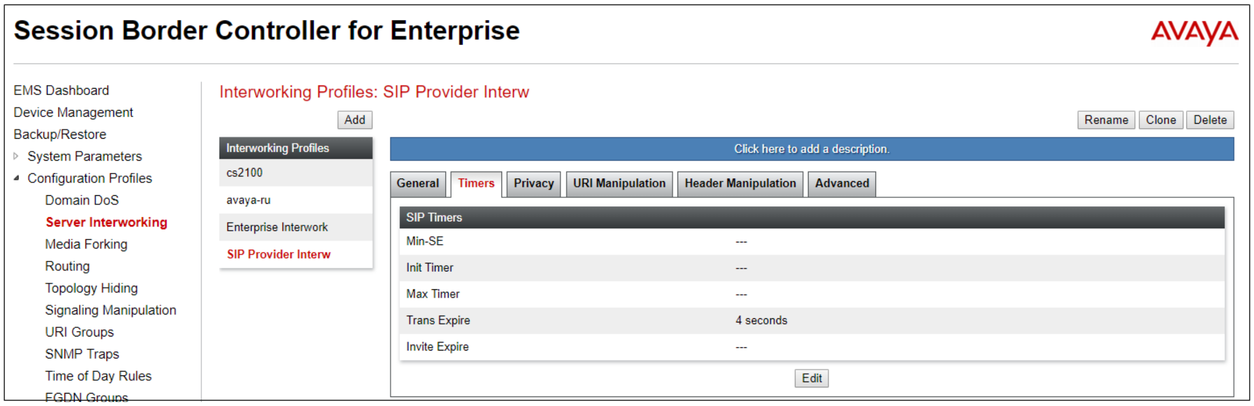
To create a new Server Interworking Profile for Masergy, navigate to **Configuration Profiles → Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**.



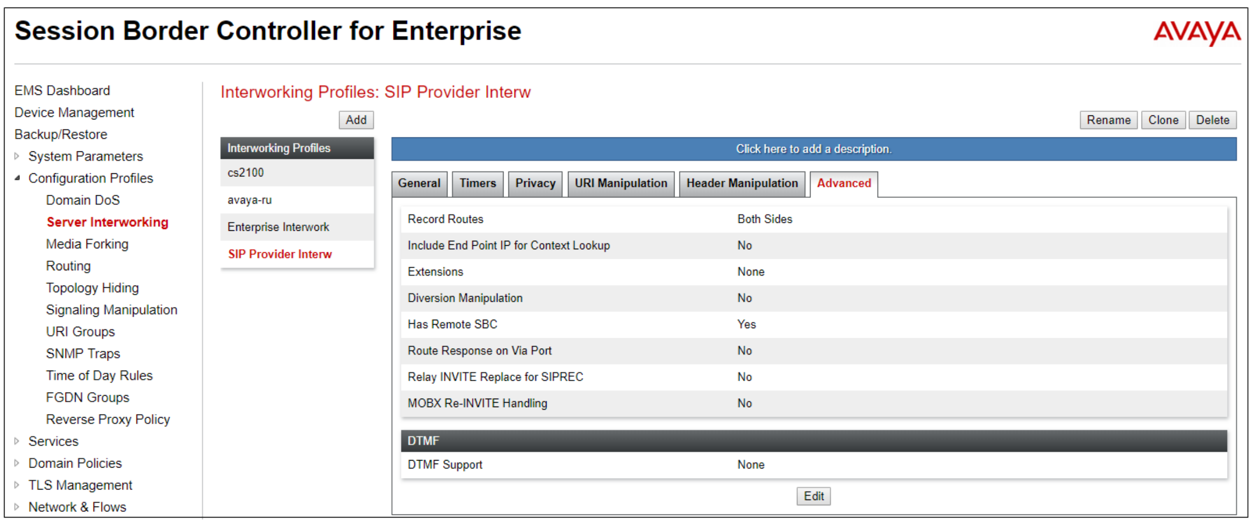
The following screens show the **SIP Provider Interw** profile used in the sample configuration. On the **General** tab, default values are used with the exception of **T.38 Support** set to **Yes**.



The **Timers** tab shows the values used for compliance testing for the **Trans Expire** field. The **Trans Expire** timer sets the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if it exists. See **Sections 7.8.2** and **7.9.2** for the configuration for redundant SBCs on the Masergy's network.



Default parameters are used for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown). On the **Advanced** tab, verify **Record Routes** is set to **Both Sides**. Default values can be used for all other fields.



7.7. Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, one signaling manipulation script is used on the outbound direction to the Masergy SIP trunk.

Note – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Server Interworking Profiles (**Section 7.6**) or Signaling Rules (**Section 7.13**) does not meet the desired result. Refer to [**8**] on the **Additional References** section for information on the Avaya SBCE scripting language.

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. A script was created during the compliance test to correct the following interoperability issues, as stated on **Section 2.2**:

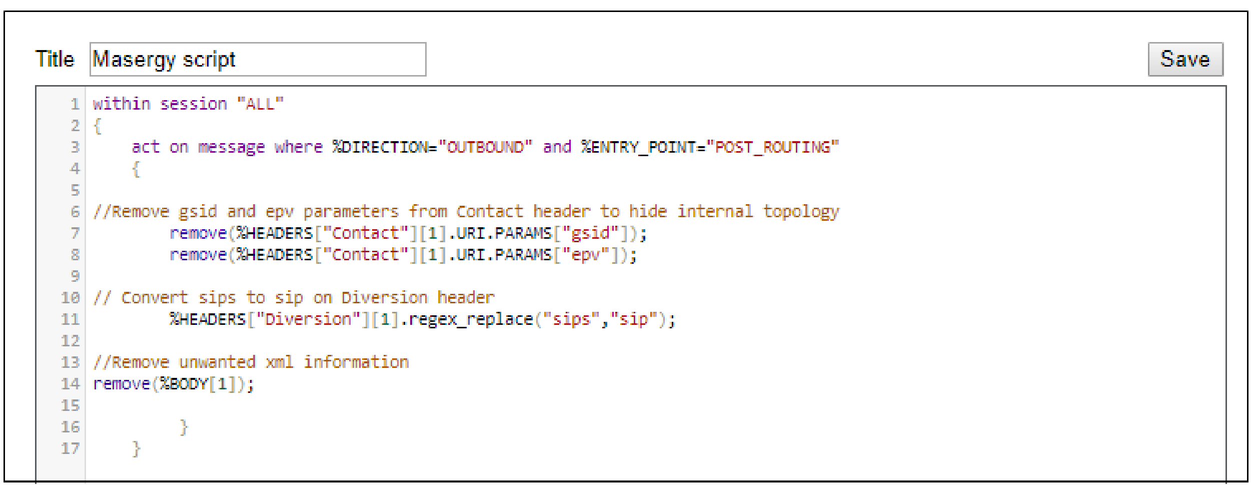
- Remove the gsid and epv parameters from the Contact header.
- Change the Diversion header scheme from SIPS to SIP.
- Remove unwanted xml element information from being sent as part of the SDP.

The details of the script appear on **Appendix A**.

To create the SigMa script, on the left navigation pane select **Configuration Profiles → Signaling Manipulation**. Select **Add**.

- Enter a name for the script in the **Title** box . The example shows the script named as **Masergy script**.
- Copy and paste the script from **Appendix A**.
- Click **Save**.

The script editor will test for any errors, and the window will close. This script will later be applied to the Masergy Server Configuration profile, in **Section 7.8.2**.



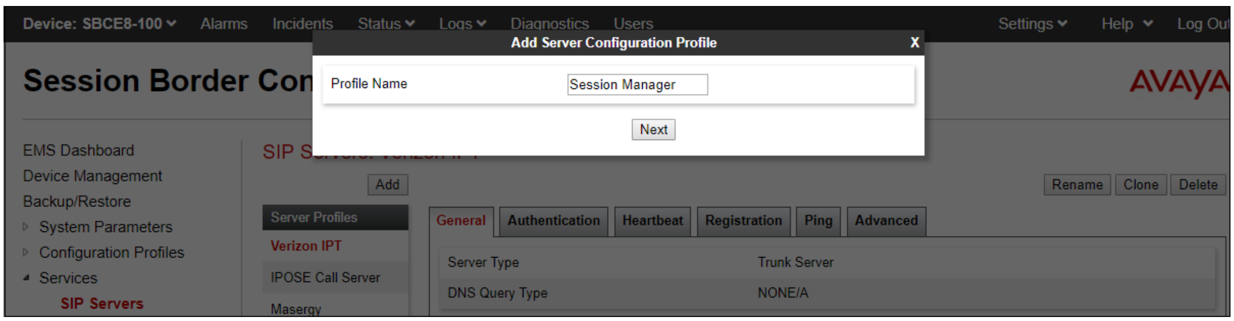
7.8. SIP Server Profiles

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

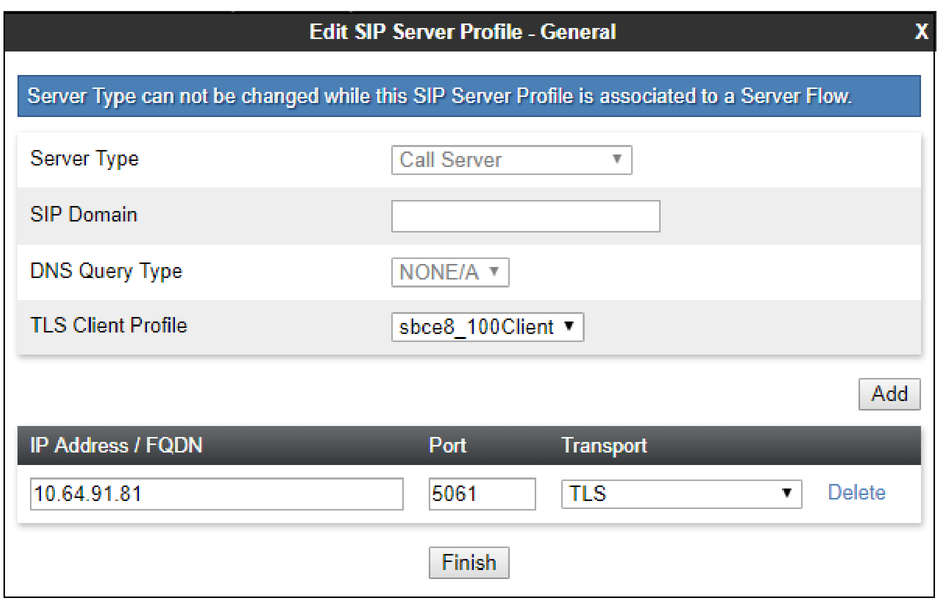
In the sample configuration, separate SIP Server Profiles were created for the enterprise (Session Manager) and the service provider.

7.8.1. SIP Server Profile – Enterprise

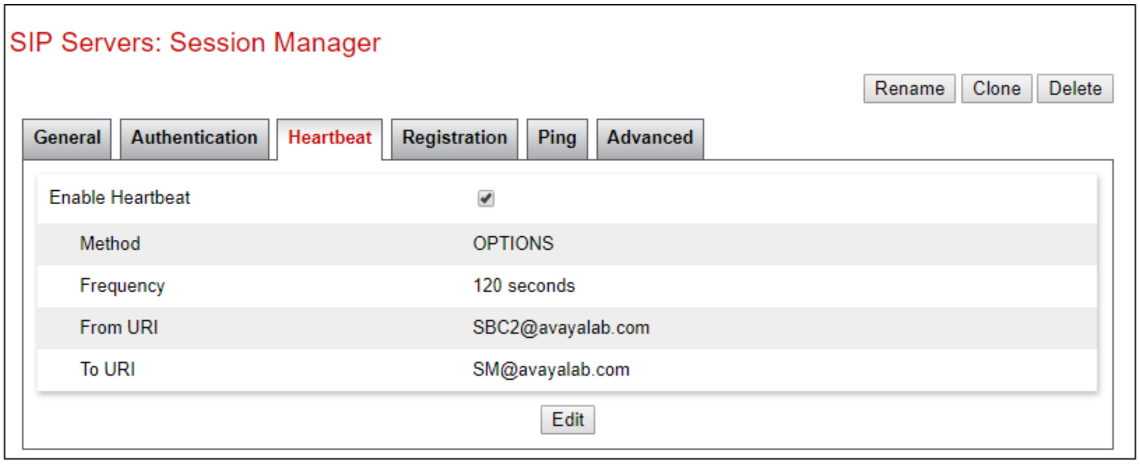
To add a SIP Server Profile for the enterprise, navigate to **Services → SIP Servers** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



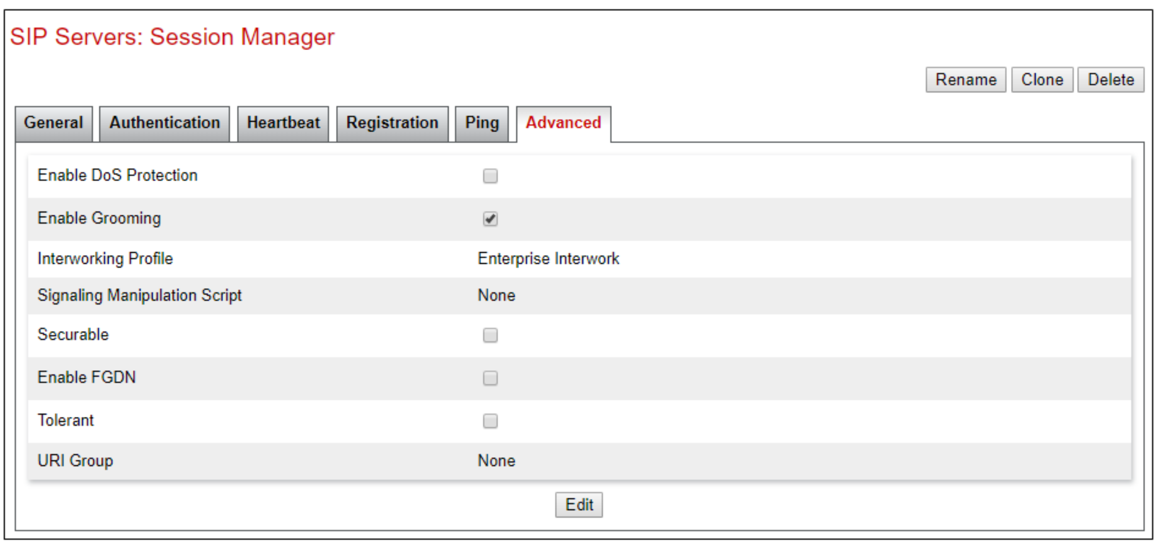
The following screens illustrate the SIP Server Profile named **Session Manager**. In the **General** tab, the **Server Type** is set to **Call Server**. In the **IP Address / FQDN** field, the IP address of the Session Manager Security Module**.** This IP address is **10.64.91.81** (**Section 6.5)**. Under **Port**, **5061** is entered, and the **Transport** parameter is set to **TLS**. The TLS profile **sbce8_100Client** created in **Section 7.2.3** is selected for **TLS Client Profile**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeat** tab. The Avaya SBCE can be optionally configured to source "heartbeats" toward Session Manager. Check the **Enable Heartbeat** box and select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS toward Session Manager.

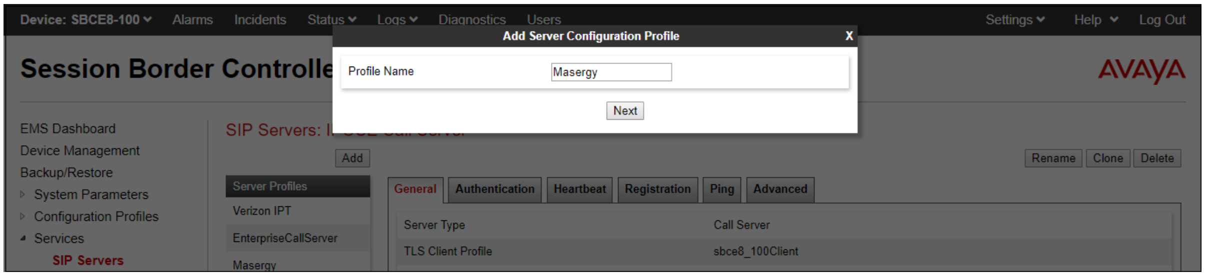


On the **Advanced** tab, **Enable Grooming** is checked and the **Interworking Profile** is set to **Enterprise Interwork** created in **Section 7.6.1** for the enterprise.



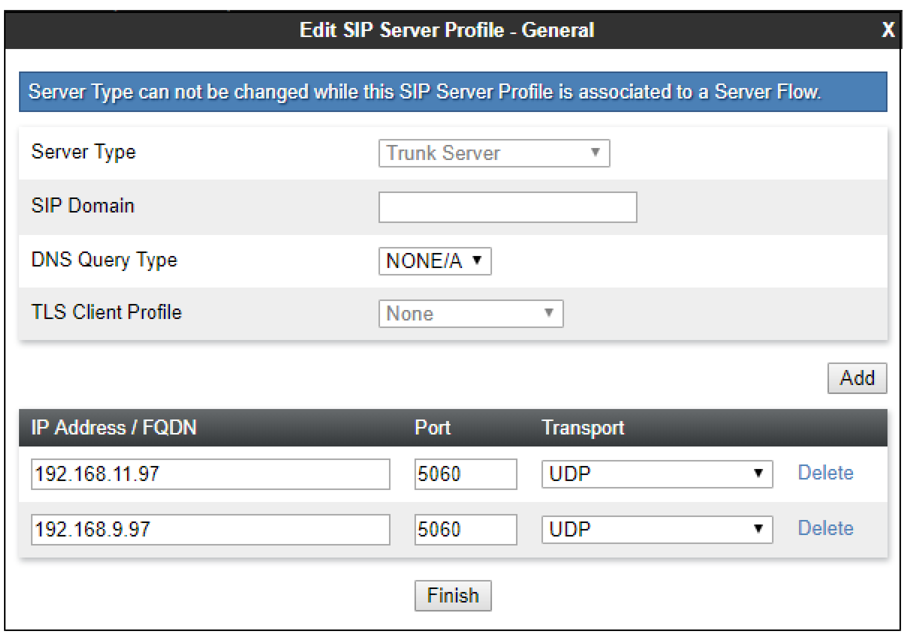
7.8.2. SIP Server Profile – Service Provider

To add a SIP server profile for the service provider, navigate to **Services → SIP Servers** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



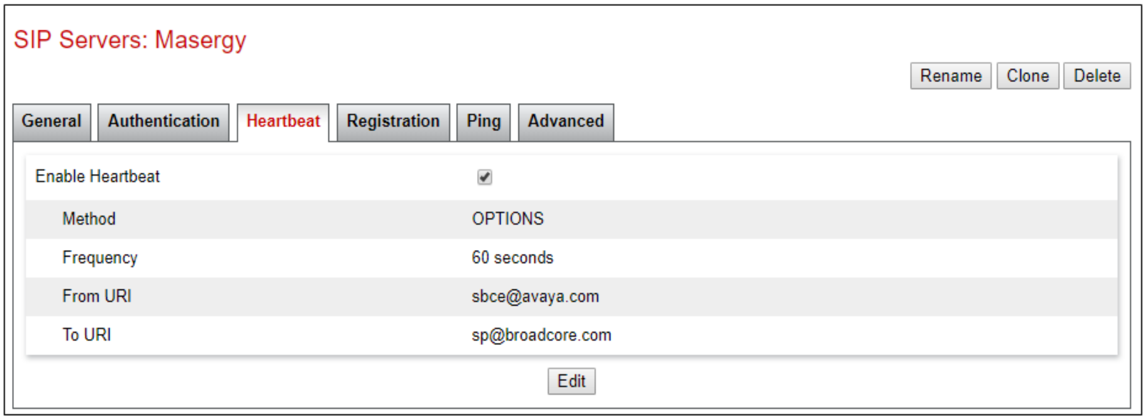
In the reference configuration, Masergy provided two SBCs, **192.168.11.97** (Primary) and **192.168.9.97** (Secondary), for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration.

The following screens illustrate the SIP Server Profile **Masergy**. In the **General** parameters, the **Server Type** is set to **Trunk Server**. In the **IP Address / FQDN** fields, the Masergy-provided SBCs IP addresses are entered. This is **192.168.11.97** (Primary) and **192.168.9.97** (Secondary). Under **Port**, **5060** is entered, and the **Transport** parameter is set to **UDP**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



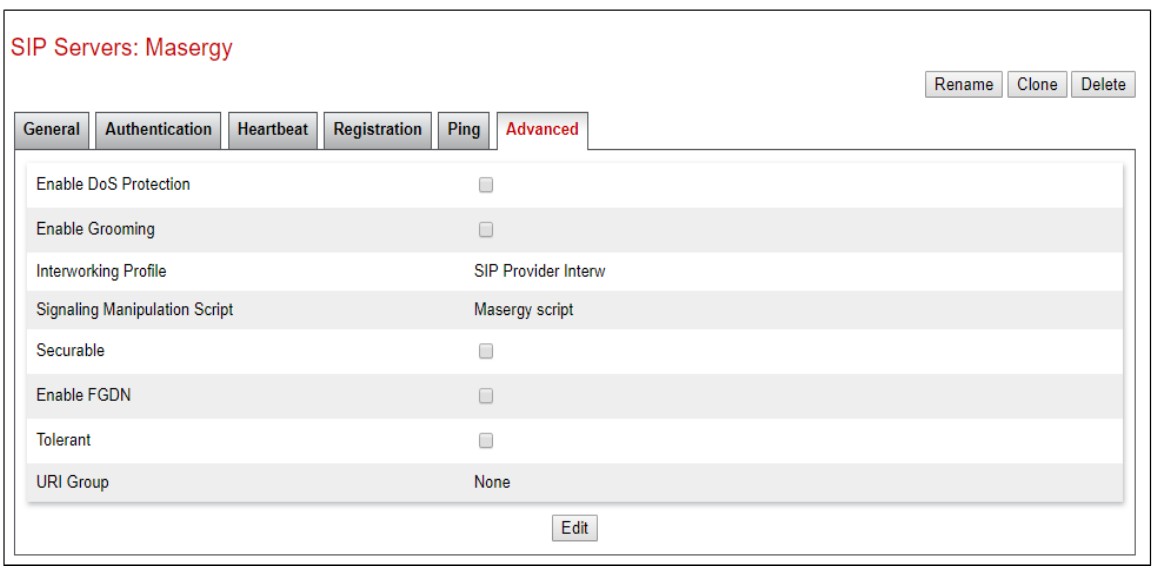
Default values can be used on the **Authentication** tab, click **Next** (not shown) to proceed to the **Heartbeats** tab.

On the Heartbeat tab, check the **Enable Heartbeat** box. Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the **Advanced** settings.



Note – The Avaya SBCE will issue OPTIONS messages to both Masergy SBC, primary (192.168.11.97) and secondary (192.168.9.97). If the SBCE fails to get a response to the OPTIONS sent to 192.168.11.97, the SBCE will redirect outbound calls to 192.168.9.97.

On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and is left unchecked. The **Interworking Profile** is set to the **SIP Provider Interw** created in **Section 7.6.2** for Masergy. The **Signaling Manipulation Script** is set to the script created in **Section 7.7**.

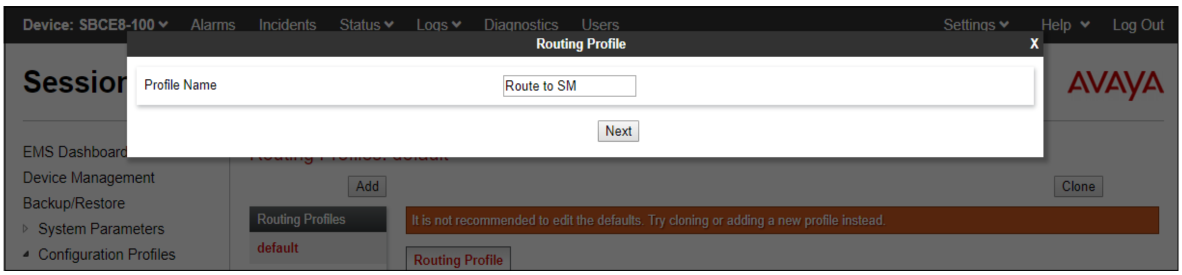


7.9. Routing Profile

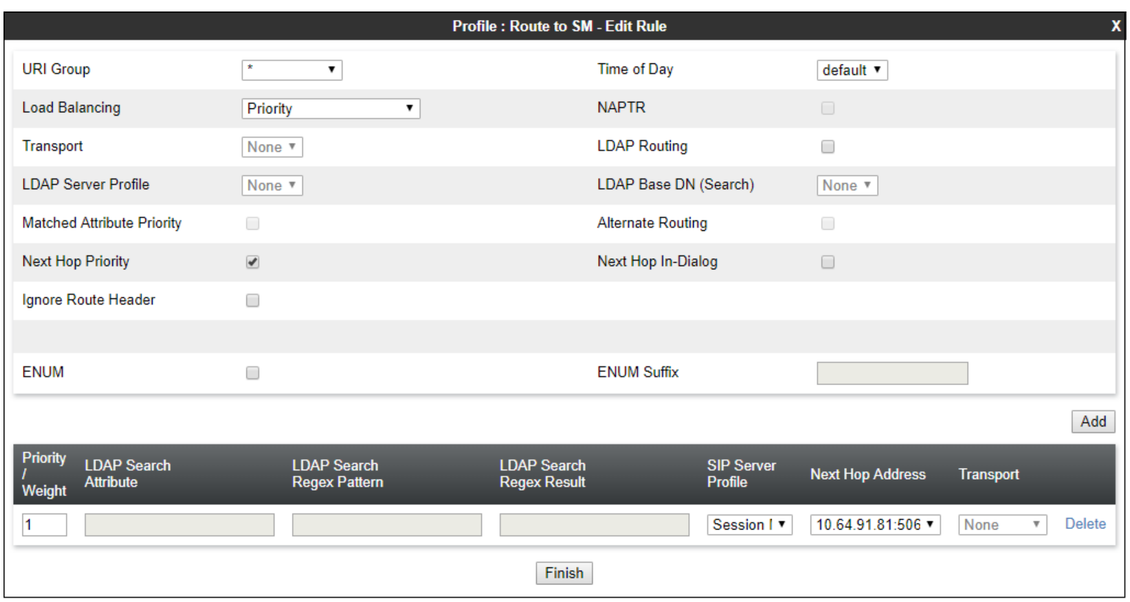
Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

7.9.1. Routing Profile – Enterprise

To add the Routing Profile toward the enterprise, navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



The following screen shows the Routing Profile **Route to SM** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. Clicking the **Add** button on this screen allows to enter the routing rule at the bottom of the profile. The **Priority / Weight** parameter is set to **1**, and the enterprise **SIP Server Profile Session Manager**, created in **Section 7.8.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically populated with the values from the Session Manager SIP Server Profile, and **Transport** becomes grayed out. Click **Finish**.



7.9.2. Routing Profile – Service Provider

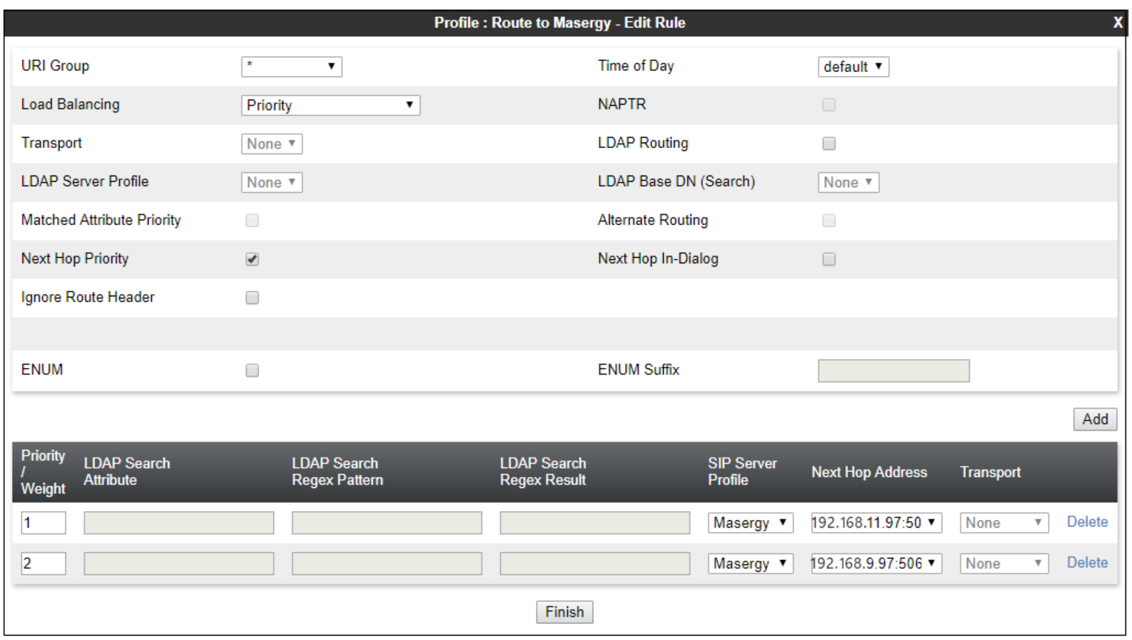
Similarly, add a Routing Profile to the Masergy SIP trunk. The following screen shows the Routing Profile **Route to Masergy** created in the sample configuration. The parameters in the top portion of the profile are left at their default settings.

For the first routing rule (Masergy Primary SBC), set the following:

- Set **Priority / Weight** to **1**
- **SIP Server Profile**: select the **Masergy** profile created in **Section 7.8.2** from the drop-down menu.
- On the **Next Hop Address** select **192.168.11.97:5060 (UDP)** from the drop-down menu.

For the second routing rule (Masergy Secondary SBC):

- Set **Priority / Weight** to **2**
- **Server Configuration**: select the **Masergy** profile created in **Section 7.8.2** from the drop-down menu.
- On the **Next Hop Address** select **192.168.9.97:5060 (UDP)** from the drop-down menu.
- Click **Finish**.



Note – If desired, the **Load Balancing** parameter may be used to modify how the traffic is handed to the service provider's SBCs. **Priority** was used in the Reference Configuration.

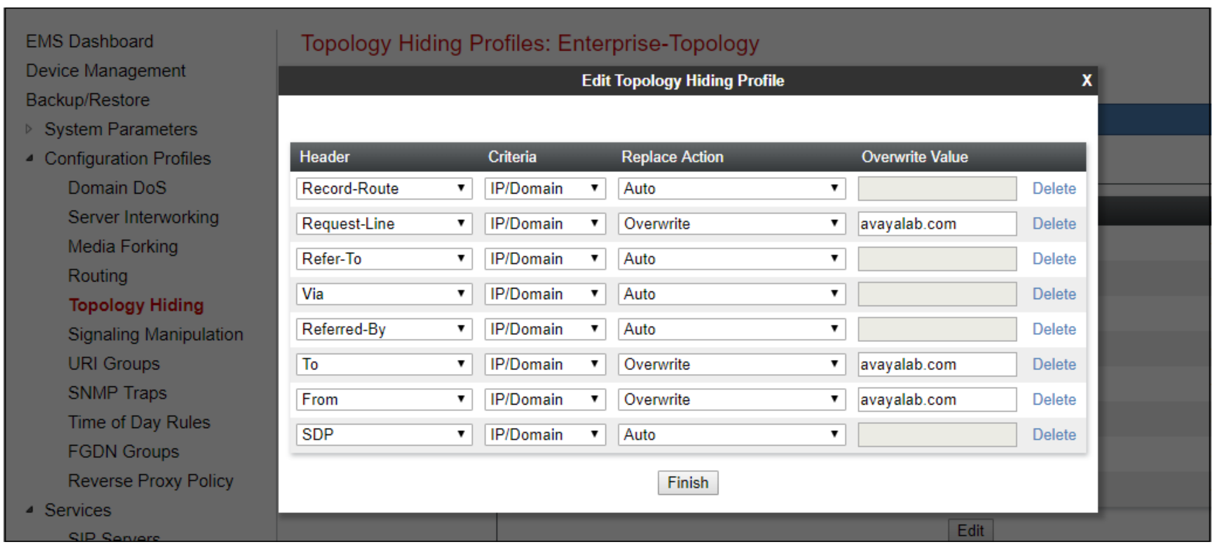
7.10. Topology Hiding Profile

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. These profiles will later be applied to the Server Flows in **Section 7.155**.

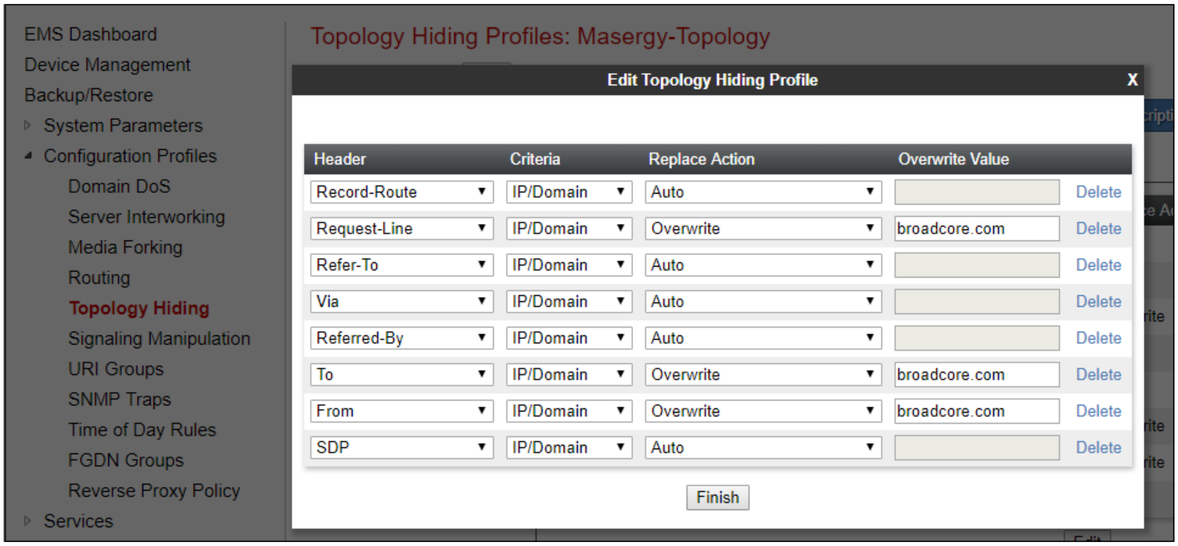
To create the Topology Hiding profiles for the enterprise and the service provider, navigate to **Configuration Profiles → Topology Hiding**. Click the **Add** button to add a new profile, or select an existing topology hiding profile to clone or edit. In the sample configuration, the **default** profile was cloned to create the profiles.

In the **Replace Action** column an action of **Auto** will replace the header field with the IP address of the Avaya SBCE interface and the **Overwrite** will use the value in the **Overwrite Value**.

The example below shows the **Enterprise-Topology** profile created in the reference configuration. The profile was cloned from the default. The Request-Line, To and From headers were overwritten with the domain of the enterprise.



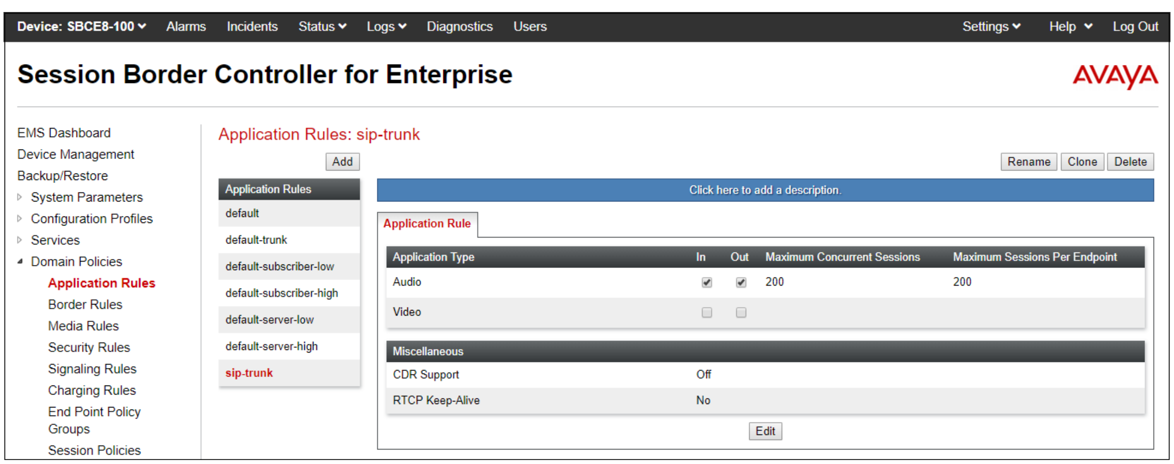
A second profile, **Masergy-Topology** was similarly cloned from the default. The Request-Line, To and From headers were overwritten with the domain used by Masergy.



7.11. Application Rule

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing application rule to edit. In the sample configuration, one **sip-trunk** rule was created for both the enterprise and Masergy. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** and **Video** applications to a value slightly larger than the licensed sessions. For example, if licensed for 150 session set the values to **200**. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.

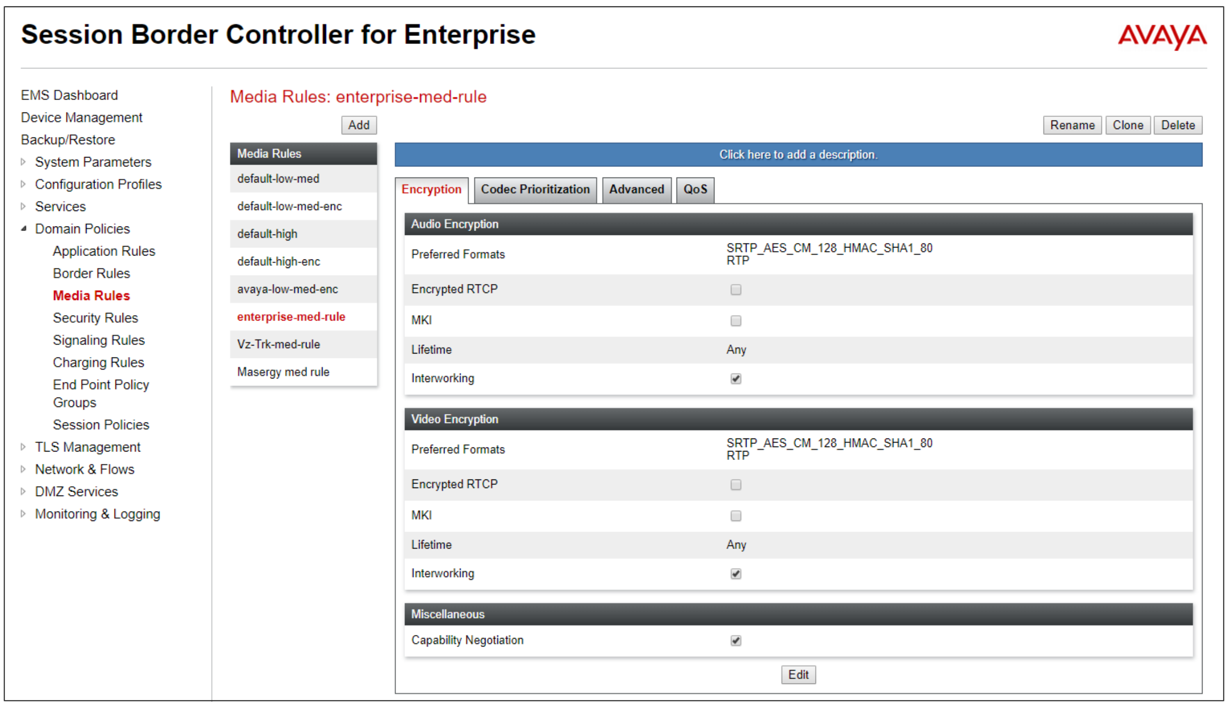


7.12. Media Rule

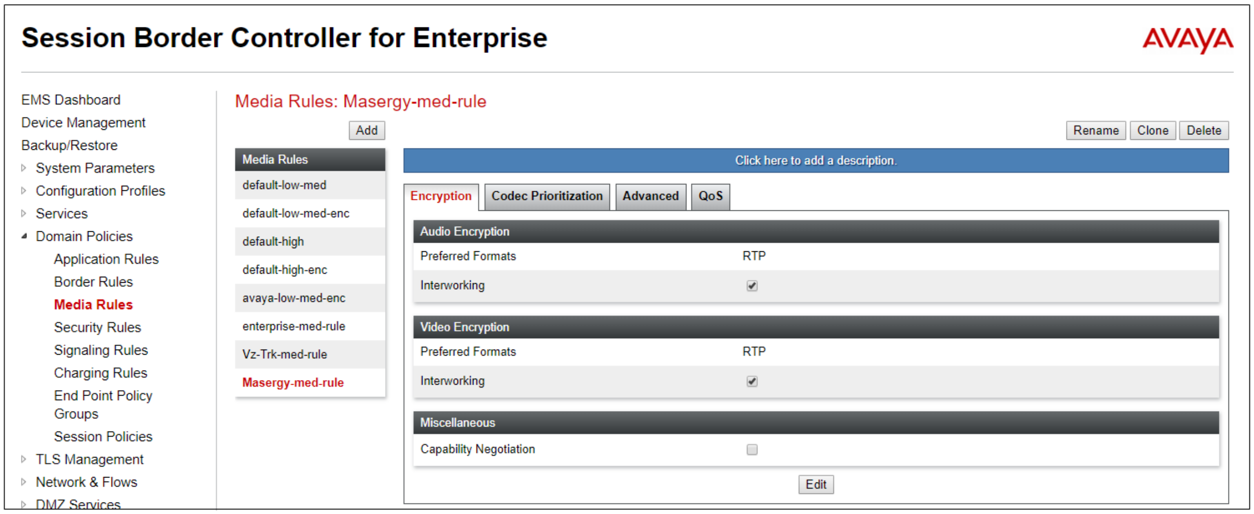
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

Select **Domain Policies → Media Rules** from the left-side menu as shown below. In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the **enterprise med rule**, and modified as shown below. With the **avaya-low-med-enc** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

The media rule **enterprise med rule** was used for the enterprise as shown below.



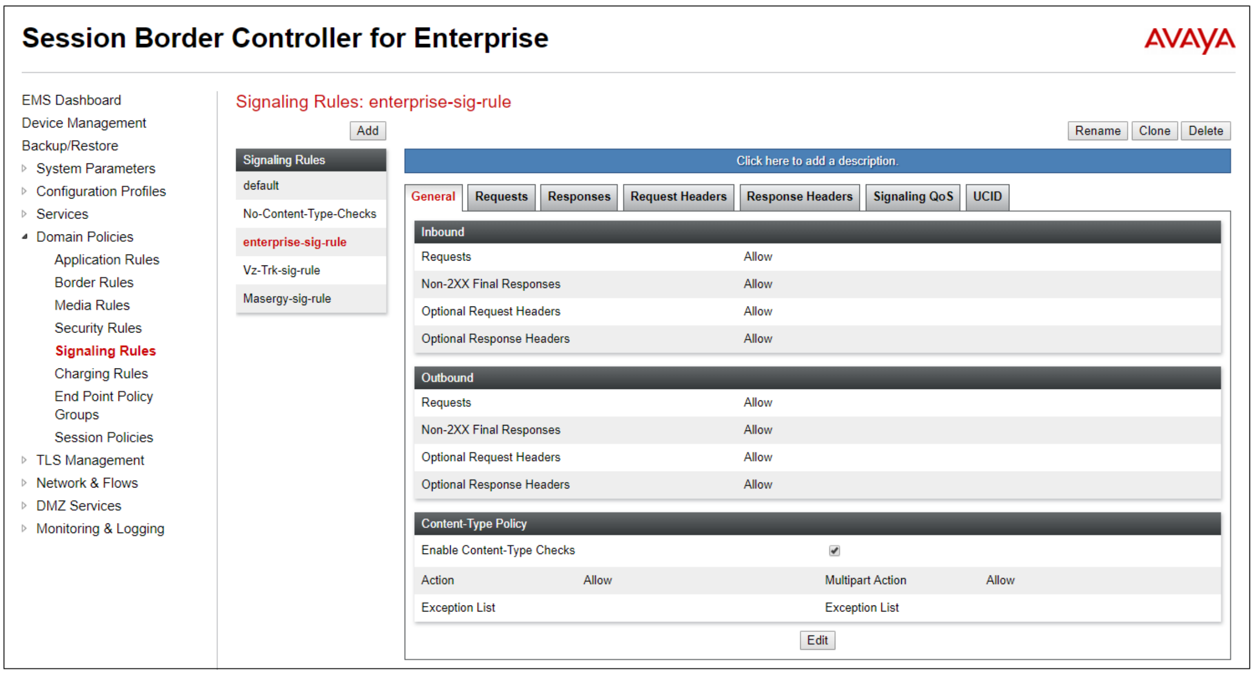
To create the Media Rule to be used for the service provider, the default media rule **default-low-med** was cloned in this case to create the **Masergy-med-rule**, shown below.



7.13. Signaling Rule

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

Clone and modify the **default** Signaling Rule to add the proper quality of service to the SIP signaling. To clone a Signaling Rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown). In the sample configuration, Signaling Rule **enterprise-sig-rule** created for the enterprise was unchanged from the default rule.

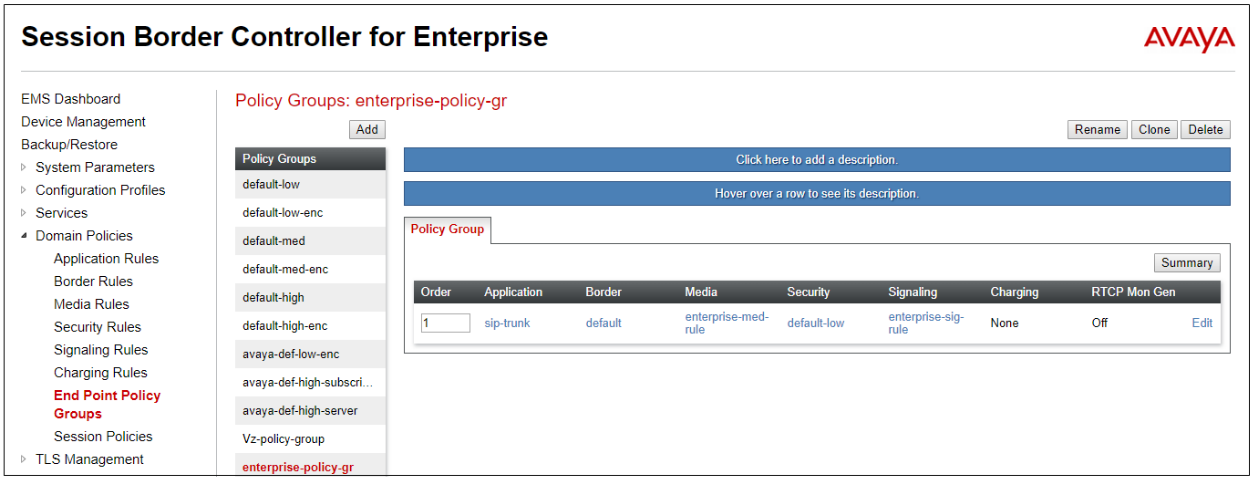


Similarly, the **Masergy-sig-rule** (not shown) for Masergy was also cloned from the default rule and left unchanged from the default values.

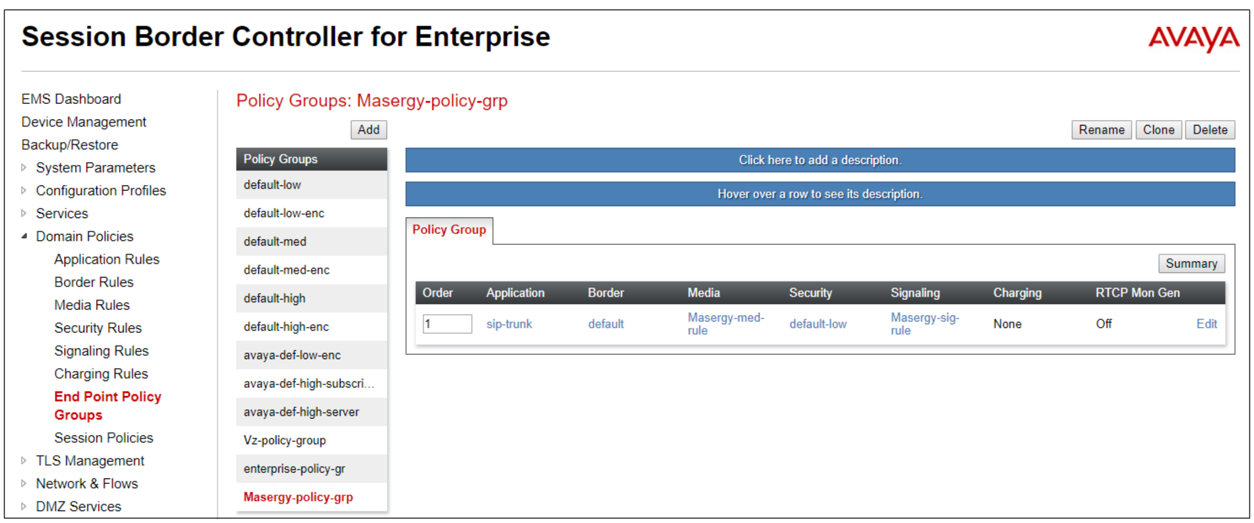
7.14. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.15**.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the **enterprise-policy-gr** created for the enterprise. The details of the non-default rules chosen are shown in previous sections.



The following screen shows the **Masergy-policy-grp** created for Masergy. The details of the non-default rules chosen are shown in previous sections.

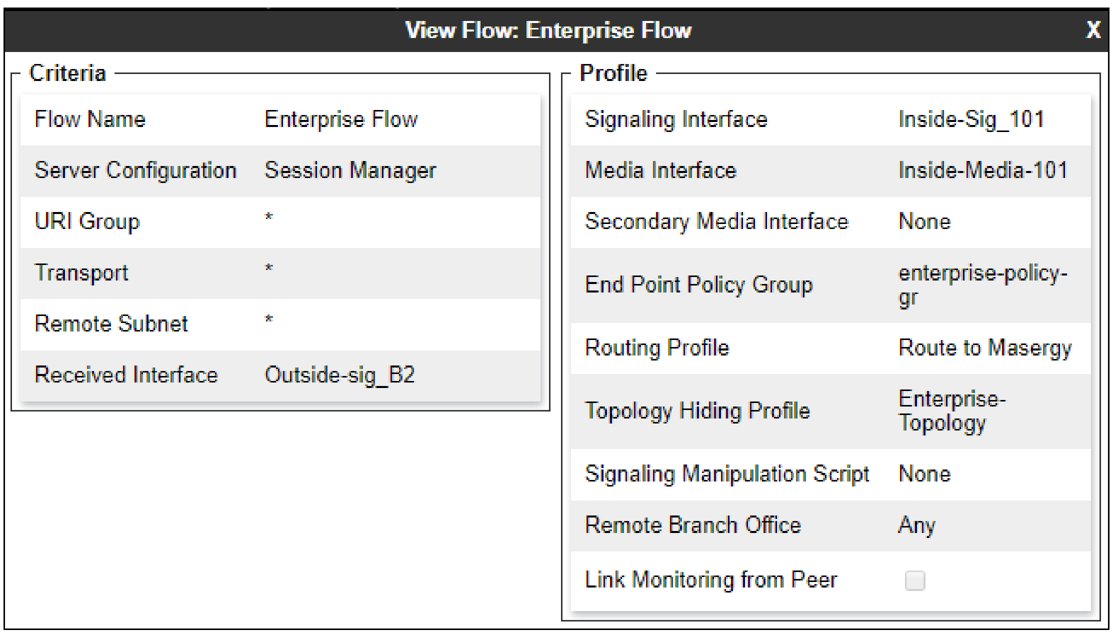


7.15. End Point Flows - Server Flow

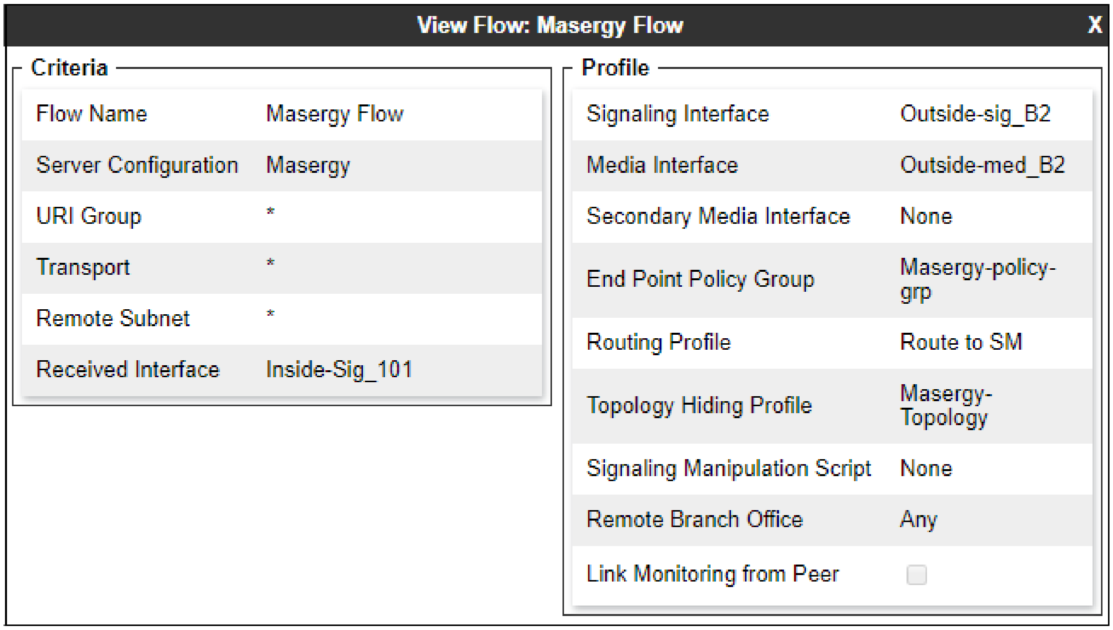
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing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

Create Server Flows for the enterprise and the service provider. To create a Server Flow, navigate to **Network and Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown).

The following screen shows the flow named **Enterprise Flow** viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.



Once again, select the **Server Flows** tab and click **Add**. The following screen shows the flow named **Masergy Flow** viewed from the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections.


View Flow: Masergy Flow

Criteria

Flow Name	Masergy Flow
Server Configuration	Masergy
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig_101

Profile

Signaling Interface	Outside-sig_B2
Media Interface	Outside-med_B2
Secondary Media Interface	None
End Point Policy Group	Masergy-policy-grp
Routing Profile	Route to SM
Topology Hiding Profile	Masergy-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	

8. Masergy SIP Trunking Service Configuration

To use the Masergy SIP Trunking Service, a customer must request the service from Masergy using the established sales processes. The process can be started by contacting Masergy via the corporate web site at https://www.masergy.com/

Masergy is responsible for the configuration of the Masergy SIP Trunking service. The customer will need to provide the IP address and port used to reach the Avaya SBCE at the enterprise. Masergy will provide the customer the necessary information to configure the SIP trunk connection from the enterprise site to the network, including:

- IP address of the Masergy SIP proxy or proxies.
- Supported codecs.
- DID numbers.
- Any IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

This information is used to complete the configuration of Communication Manager, Session Manager and the Avaya SBCE discussed in the previous sections.

9. Verification and Troubleshooting

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

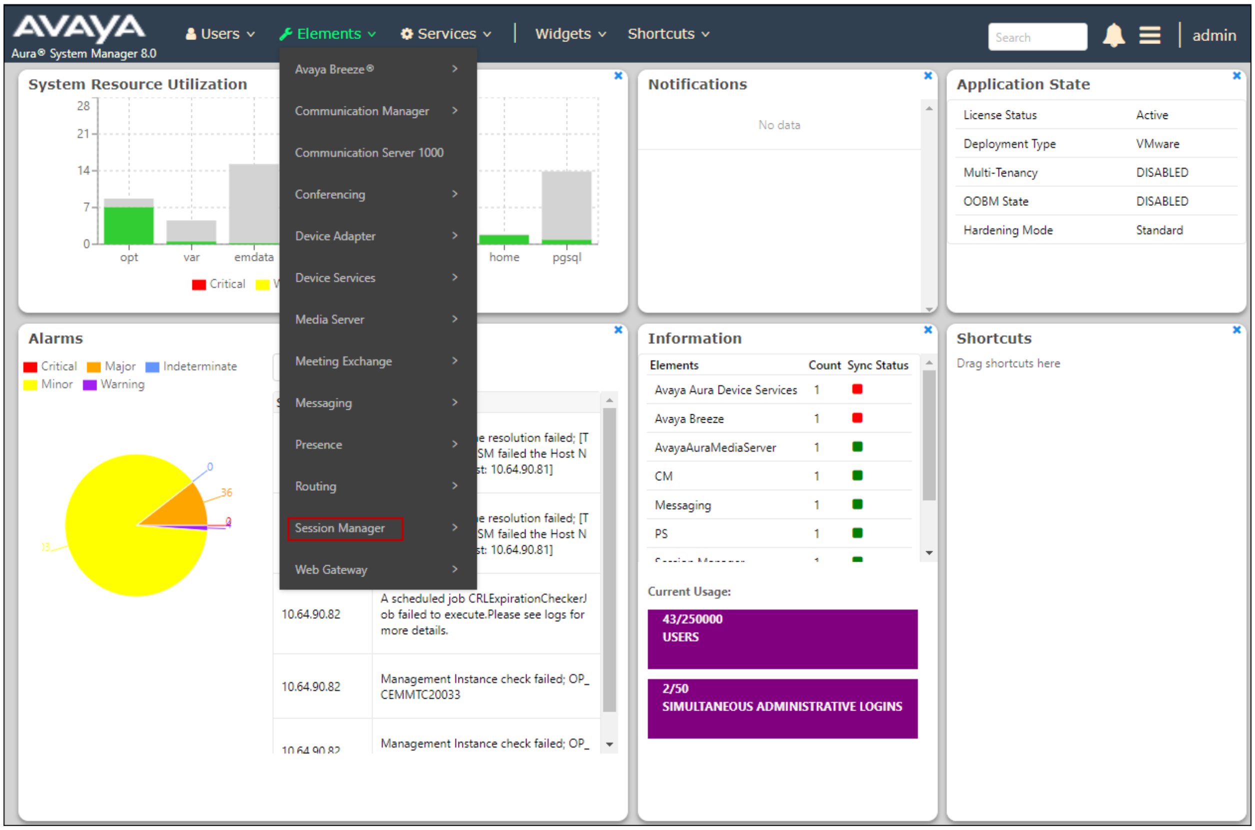
9.1. Communication Manager Verification

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

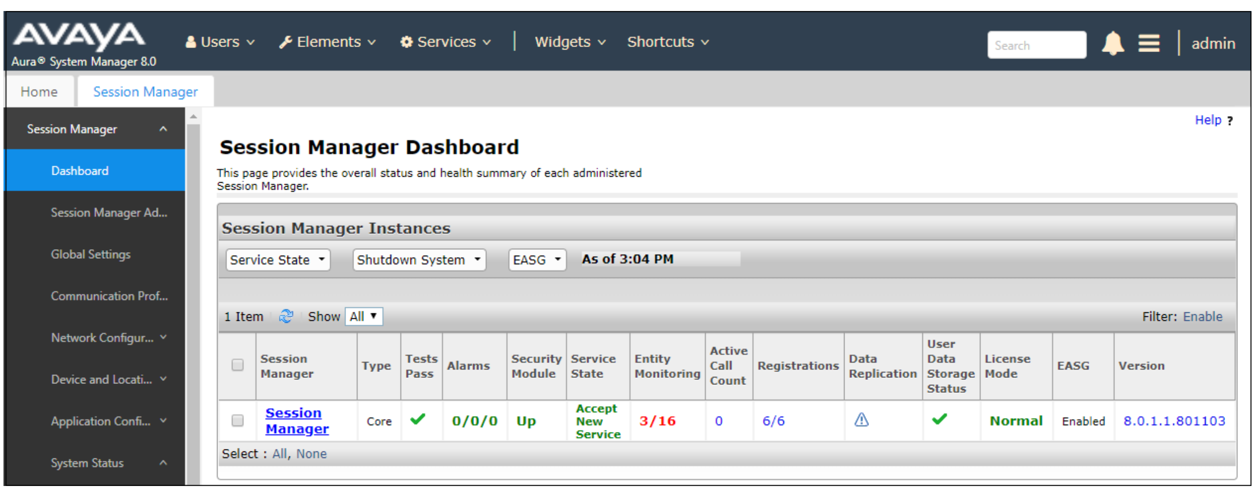
- **list trace station** <extension number>
  Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
  Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
  Displays signaling group service state.
- **status trunk** <trunk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

9.2. Session Manager Verification

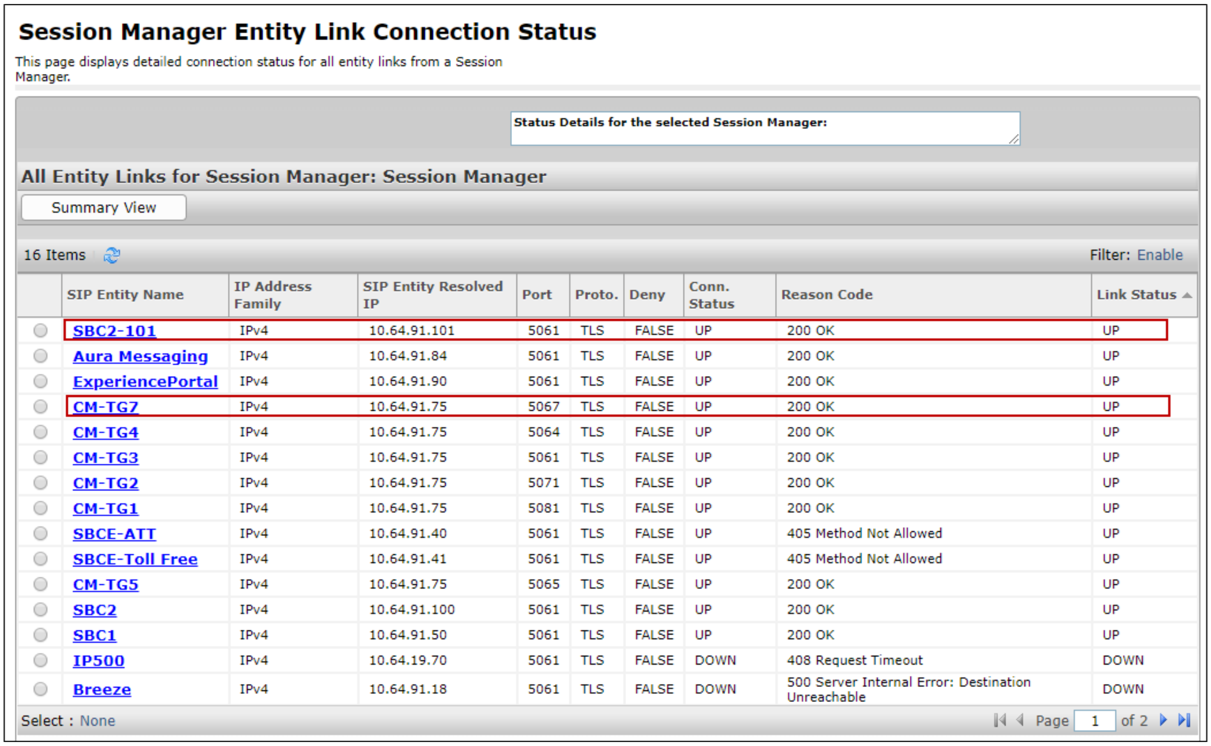
Log in to System Manager. Under the **Elements** heading, select **Session Manager**



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



On the example, the entry **3/16** under the **Entity Monitoring** column shows that there are alarms on 3 out of the 16 Entities being monitored by Session Manager. Clicking the entry under the **Entity Monitoring** column brings up the **Session Manager Entity Link Connection Status** page. Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **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

16 Items | Filter: Enable

SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SBC2-101	IPv4	10.64.91.101	5061	TLS	FALSE	UP	200 OK	UP
Aura Messaging	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP
ExperiencePortal	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP
CM-TG7	IPv4	10.64.91.75	5067	TLS	FALSE	UP	200 OK	UP
CM-TG4	IPv4	10.64.91.75	5064	TLS	FALSE	UP	200 OK	UP
CM-TG3	IPv4	10.64.91.75	5061	TLS	FALSE	UP	200 OK	UP
CM-TG2	IPv4	10.64.91.75	5071	TLS	FALSE	UP	200 OK	UP
CM-TG1	IPv4	10.64.91.75	5081	TLS	FALSE	UP	200 OK	UP
SBCE-ATT	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
SBCE-Toll Free	IPv4	10.64.91.41	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
CM-TG5	IPv4	10.64.91.75	5065	TLS	FALSE	UP	200 OK	UP
SBC2	IPv4	10.64.91.100	5061	TLS	FALSE	UP	200 OK	UP
SBC1	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
IP500	IPv4	10.64.19.70	5061	TLS	FALSE	DOWN	408 Request Timeout	DOWN
Breeze	IPv4	10.64.91.18	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN

Select : None | Page 1 of 2

Other Session Manager useful verification and troubleshooting tools include:

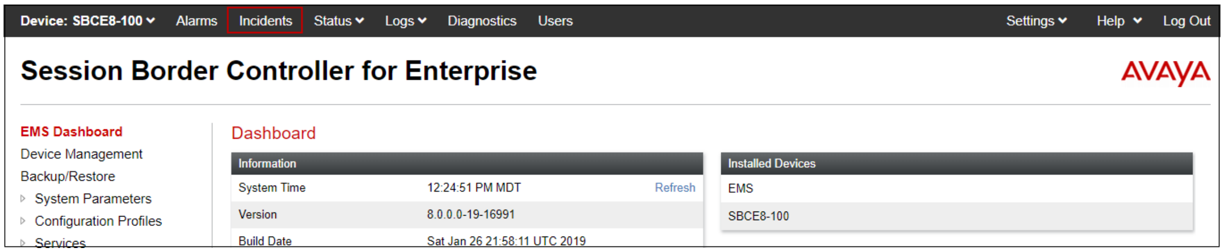
- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System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

9.3. Avaya SBCE Verification

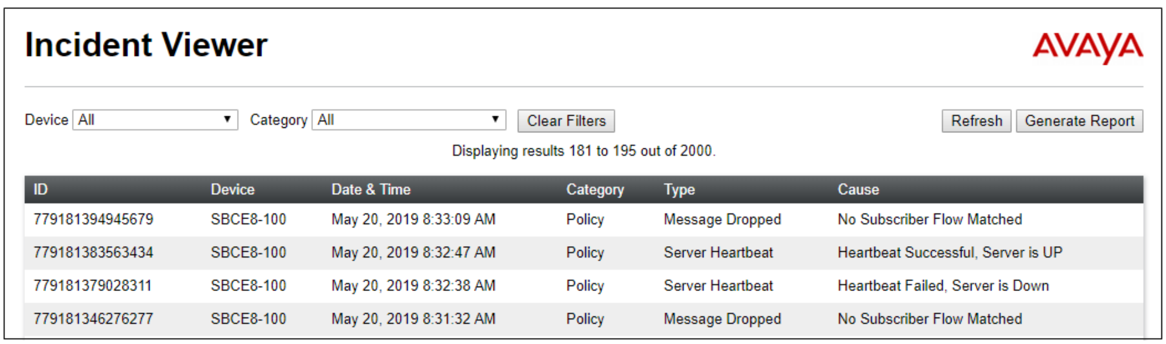
This section provides verification steps that may be performed with the Avaya SBCE.

9.3.1. Incidents

The Incident Viewer can be accessed from the Avaya top navigation menu as highlighted in the screenshot below.

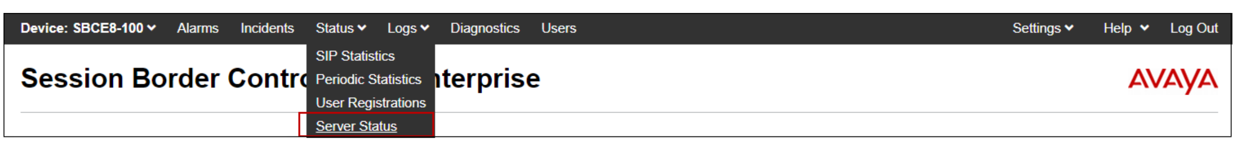


Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.



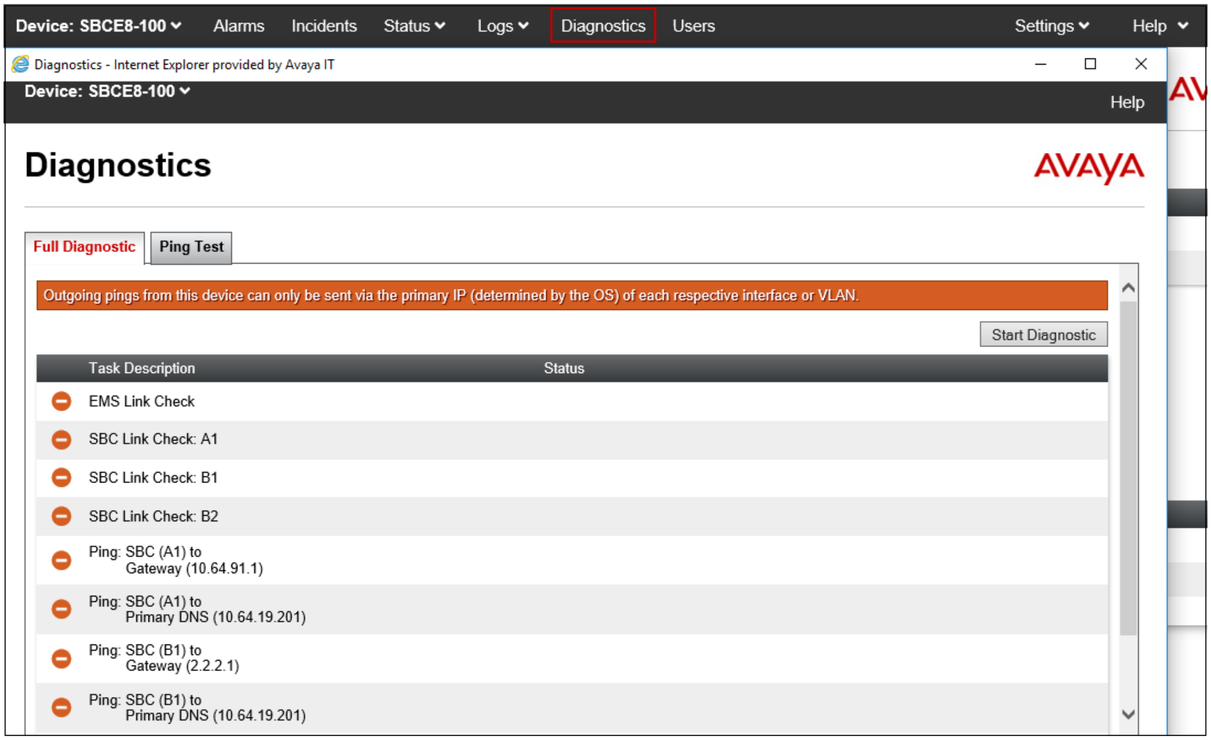
9.3.2. Server Status

The **Server Status** can be access from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **Server Status**. The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the Server Configuration profiles, as configured in **Section 7.8**.



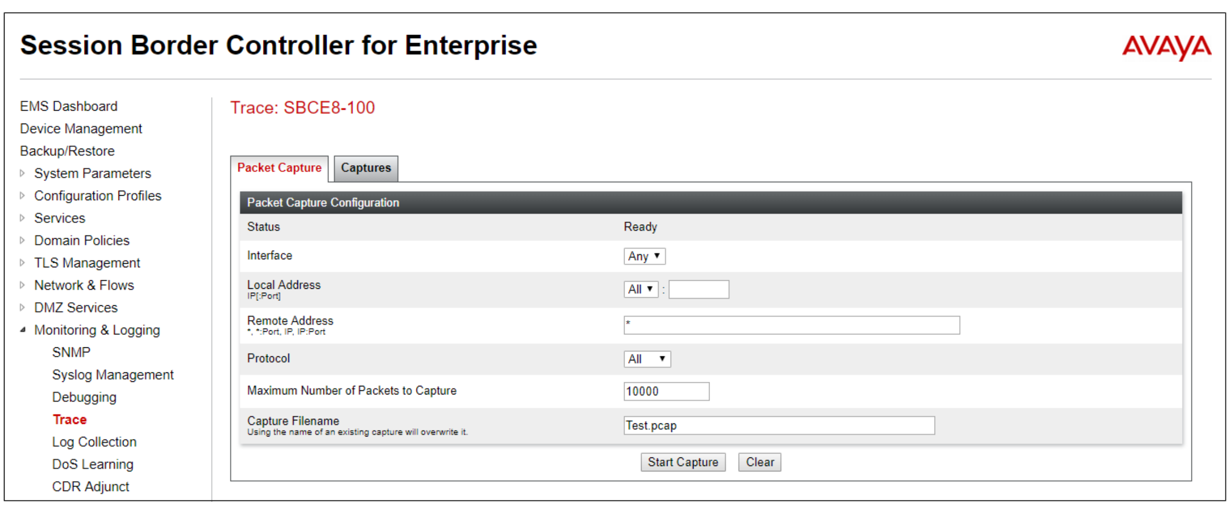
9.3.3. Diagnostics

This screen provides a **Full Diagnostics** tool to verify the link of each interface and ping the configured next-hop gateways and DNS servers. The **Ping Test** tool can be used to ping specific devices from any Avaya SBCE interface.

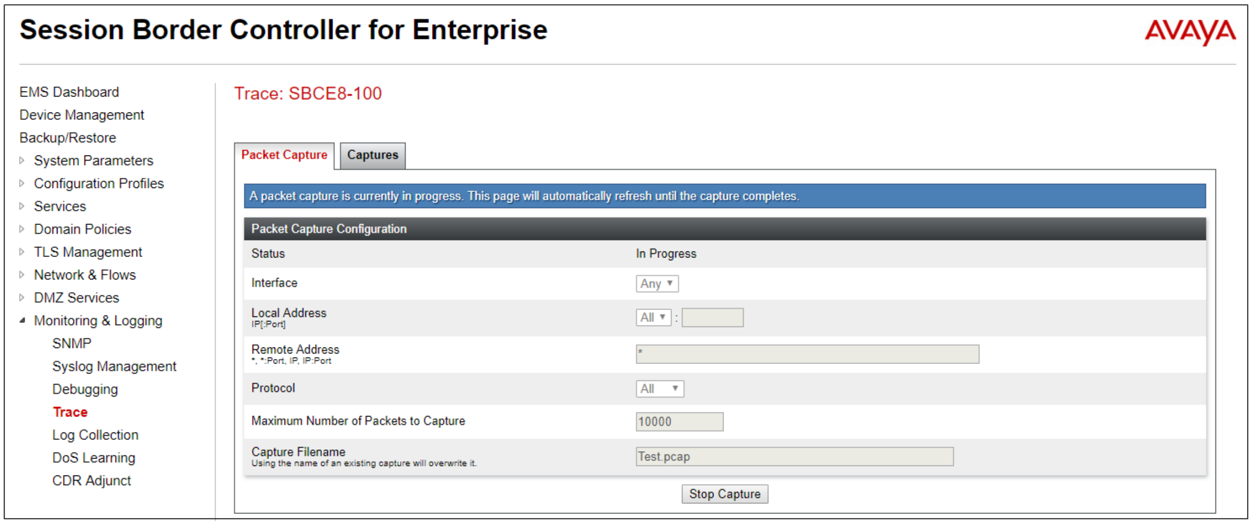


9.3.4. Tracing

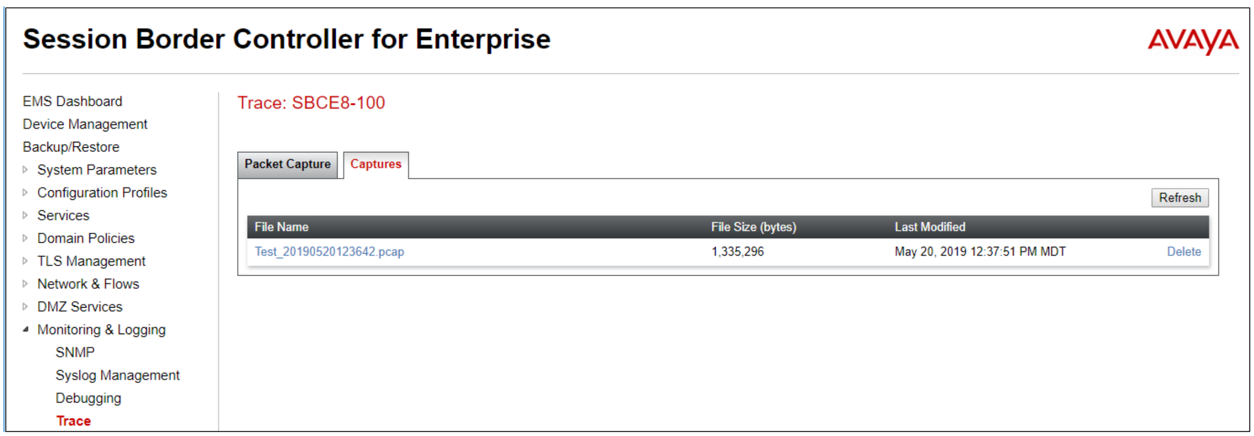
To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.



When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.



Select the **Captures** tab to view the files created during the packet capture.



The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like WireShark.

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and the Avaya Session Border Controller for Enterprise 8.0 can be configured to interoperate successfully with the Masergy SIP Trunking Service.

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**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

11. Additional 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 8.0.1, Issue 7, April 2019.
[2] *Administering Avaya Aura® Communication Manager*, Release 8.0.x, Issue 4, May 2019.
[3] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 8.0.x, Issue 5, May 2019.
[4] *Administering Avaya Aura® System Manager* for Release 8.0.1, Issue 9, May 2019
[5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 8.0.1, Issue 4, February 2019.
[6] *Administering Avaya Aura® Session Manager*, Release 8.0.1, Issue 3, December 2018.
[7] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 8.0, Issue 2, March 2019.
[8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 1, February 2019.
[9] *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*
[10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0, Issue 6, March 2019.
[11] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0, Issue 4, April 2019.
[12] *Planning for and Administering Avaya Equinox for Android, iOS, Mac and Windows*, Release 3.5.5, March 2019
[13] *Administering Avaya one-X® Communicator*. Release 6.2, Feature Pack 10, November 2015.
[14] *RFC 3261 SIP: Session Initiation Protocol*. https://www.ietf.org/rfc/rfc3261.txt

12. Appendix A

Details of the Signaling Manipulation script named **Masergy script,** used in the configuration of the Avaya SBCE, **Section 7.7**.

```
within session "ALL"
{
    act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
    {

//Remove gsid and epv parameters from Contact header to hide internal
topology
        remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
        remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

// Convert sips to sip on Diversion header
        %HEADERS["Diversion"][1].regex_replace("sips","sip");

//Remove unwanted xml information
remove(%BODY[1]);

         }
    }
```

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