Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 to support Fusion Connect 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 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to interoperate with the Fusion Connect SIP Trunking service.

The Fusion Connect SIP Trunking service provides customers with 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 the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Fusion Connect SIP trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0 and various Avaya endpoints, listed in **Section 4**.

The Fusion Connect 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 and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

Note: Throughout these Application Notes, the terms "Service Provider", "Fusion Connect" and "Fusion" will be used without distinction when referring to the SIP trunking service provider.

2. General Test Approach and Test Results

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

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.

2.1. Interoperability Compliance Testing

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

- SIP trunk registration with the service provider.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using "This Computer" and "Other Phone" modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 deskphones, and the Avaya one-X® Communicator and Avaya Communicator for Windows softphones.
- Various call types, including: local, long distance, international and local directory assistant (411).
- Codecs G.711MU, G729A and proper codec negotiation.
- Inbound and outbound PSTN calls using VoIP media resources in Avaya Media Gateways and the Avaya Aura® Media Server at the enterprise network.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Network Call Redirection using Communication Manager vectors.
- Routing inbound PSTN calls to call center agent queues.
- Fax support.
- Proper response/error treatment to different failure conditions.

The following items are not supported or were not tested:

- Operator (0) and operator assisted (0+10) calls are not supported.
- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test.

2.2. Test Results

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

- **Outbound calls and Digest Authentication**: The Avaya SBCE version 7.0.0-21 used during the compliance test required patch *sbc700-p001-20151005-7.0.0-21.x86_64.rpm* to be installed, to address the issue of outbound calls failing to complete when Digest Authentication is used by the service provider, as Fusion does, in order to validate the identity of the calls made from the enterprise. Product Support Notice PSN004619u can be found on the Avaya Support website, for details and patch installation instructions. A link for the PSN is also provided on the **References** section.
- **Outbound calls to busy PSTN numbers**: Fusion did not send a "486 Busy Here" message on outbound calls to PSTN numbers that were busy, as it is expected in this condition. There was no direct impact to the user, who heard busy tone.
- **Outbound Calling Party Number (CPN) Block**: In order to process outbound calls from the enterprise, Fusion required the Main User (BTN) to be included in the From header of every outbound call. A script was needed on the Avaya SBCE (**Section 7.7**) to meet this requirement. In addition, Fusion used the calling party number included in the P-Asserted-Identity for Caller ID purposes on the PSTN. This pattern used by Fusion precludes the use of the CPN Block feature in Communication Manager, which includes "anonymous" in the From header, while it sets the Privacy: id header and sends the actual calling party number on the P-Asserted-Identity header when this feature is activated.
- **Music on Hold**: Music on Hold played by the Avaya G450 Media Gateway, and heard by PSTN callers placed on hold by enterprise users showed very bad sound quality, and occasionally it was not heard at all. The issue seems to be related to the manner in which Fusion handles the media streams after receiving the "sendonly" attribute, included in the SDP of the re-INVITE that Communication Manager sends to the service provider when calls are placed on-hold. As a workaround to this issue, a script was created on the Avaya SBCE (**Section 7.7**) that removed the "sendonly" message from the outbound Communication Manager re-INVITE. Music on Hold was heard normally after the script was applied.
- **Fax Support**: T.38 fax is the only form of fax officially supported in Communication manager over SIP trunks. While outbound T.38 was tested successfully, inbound T.38 faxes failed to complete during the compliance test. Since T.38 was not usable, G.711 pass-through fax was additionally tested. This was done by setting **Fax Mode** to ***off*** in the Communication Manager **ip-codec-set** form (**Section 5.4**). Faxes using G.711 pass-through completed successfully during the test. But it should be noted that due to the unpredictability of pass-through techniques, which only work well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered in Communication Manager on a "best effort" basis; its success is not guaranteed, and it should be used at the customer's discretion.
- **Network Call Redirection when Redirected Party is busy**: On a test scenario where an incoming call was transferred back to the PSTN via a Communication Manager vector

using the REFER method, and the referred party was busy, Fusion sent, as expected, intermediate call states status (100 Trying, 180 Ringing, etc.) of the referred call back to the referring party. This is done via NOTIFY messages in response to the REFER request, before the referring party is disconnected. But in a scenario where the redirected party was busy, instead of sending a "486 Busy Here" or similar error message in the NOTIFY message, Fusion sent a "200 OK". The caller heard a busy signal, but since no busy/unavailable condition is detected in the incoming NOTIFY message, further call processing by Communication Manager vectors, like the re-routing the call to a local agent, was not possible.

- **Network Call Redirection with User-to-User Information (UUI)**: User-to-User information can optionally be sent to the network in the REFER message of calls transferred back to the PSTN. If the referred party is reached via a SIP trunk, this means the service provider should include the User-To-User header in the new INVITE. User-to-User information was not used by Fusion, and it was not propagated to the redirected party.
- **Conference in Avaya Communicator softclients**: The Communication Manager conference feature is not supported in the Avaya Communicator current software release 2.1.2.75. An Avaya Aura® Conferencing server is required for ad-hoc conferences. This feature should be available in the upcoming release 3.0 of Avaya Communicator.
- **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 purposes 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 and P-Location (**Section 6.4**). Additionally, the parameters "gsid" and "epv" were removed from outbound Contact headers using a Signaling Script in the Avaya SBCE (**Section 7.7**).

2.3. Support

For technical support on the Fusion Connect SIP trunking offer, follow the Customer Support links at http://www.fusionconnect.com/services/cloud-communications/sip-trunking

3. Reference Configuration

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

For security purposes, references to any public IP addresses used during the compliance test have been replaced in these Application Notes with private addresses. Also, SIP trunk credentials have been replaced with fictitious values, and PSTN routable phone numbers used in the test have been changed to non-routable numbers.

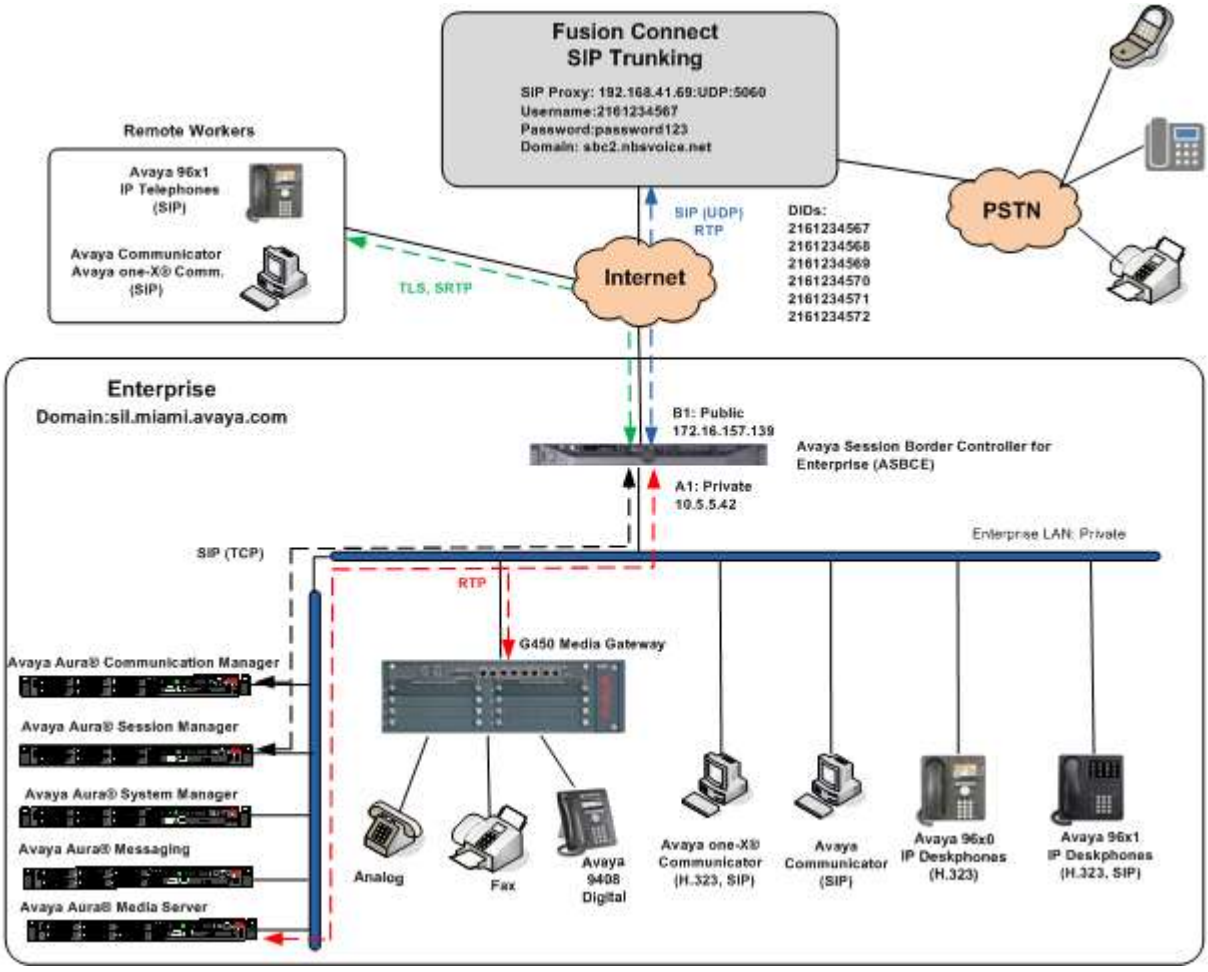


Figure 1: **Avaya SIP Enterprise Solution connected to Fusion Connect SIP Trunking**

The 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 G450 Media Gateway.
- Avaya 96x0 and 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Communicator for Windows softphones.
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test, using the following endpoints and protocols:

- Avaya 96x1 SIP Deskphones (using TLS and SRTP).
- Avaya Communicator for Windows (using TLS and SRTP).
- Avaya one-X® Communicator SIP (using TCP and RTP).

For security reasons, TLS and SRTP are the recommended protocols to be used by all remote workers endpoints. During the tests, TCP and RTP were used with Avaya one-X® Communicator for tracing and troubleshooting purposes.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [**9**] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the external network, 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.

The transport protocol between the Avaya SBCE and Fusion across the public IP network was UDP. The transport protocol between the Avaya SBCE and the enterprise Session Manager across the enterprise IP network was TCP.

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 (in this case the Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

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 Fusion network.

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

As part of the Avaya Aura® version 7.0 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Sever (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G450 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 Fusion Connect SIP Trunking, they are not included in these Application Notes.

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	7.0 Service Pack 1 (R017x.00.0.441.0 patch 22477)
Avaya Aura® Session Manager	7.0 (7.0.0.0.700007)
Avaya Aura® System Manager	7.0.0.0 (Update Revision 7.0.0.0.4036)
Avaya Session Border Controller for Enterprise	7.0.0-21-6602 Patch: sbc700-p001-20151005-7.0.0-1.x86_64.rpm
Avaya Aura® Messaging	6.3.3 SP3
Avaya Aura® Media Server	7.7.0.236
Avaya G450 Media Gateway	37.19.0
Avaya 96x0 Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.6.13
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 7.0.0.39
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 6.6
Avaya one-X® Communicator (H.323, SIP)	6.2.10.03-FP10
Avaya Communicator for Windows	2.1.2.75
Avaya 9408 Digital Telephone	Rel 12.0
Avaya 6210 Analog Telephone	N/A
Fusion Connect	
ACME Net-Net 4500	SCX6.2
NBSVoice	3.0

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

Note - The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the table above were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 5.5) platforms. Consult the installation documentation on the **References** section for more information.

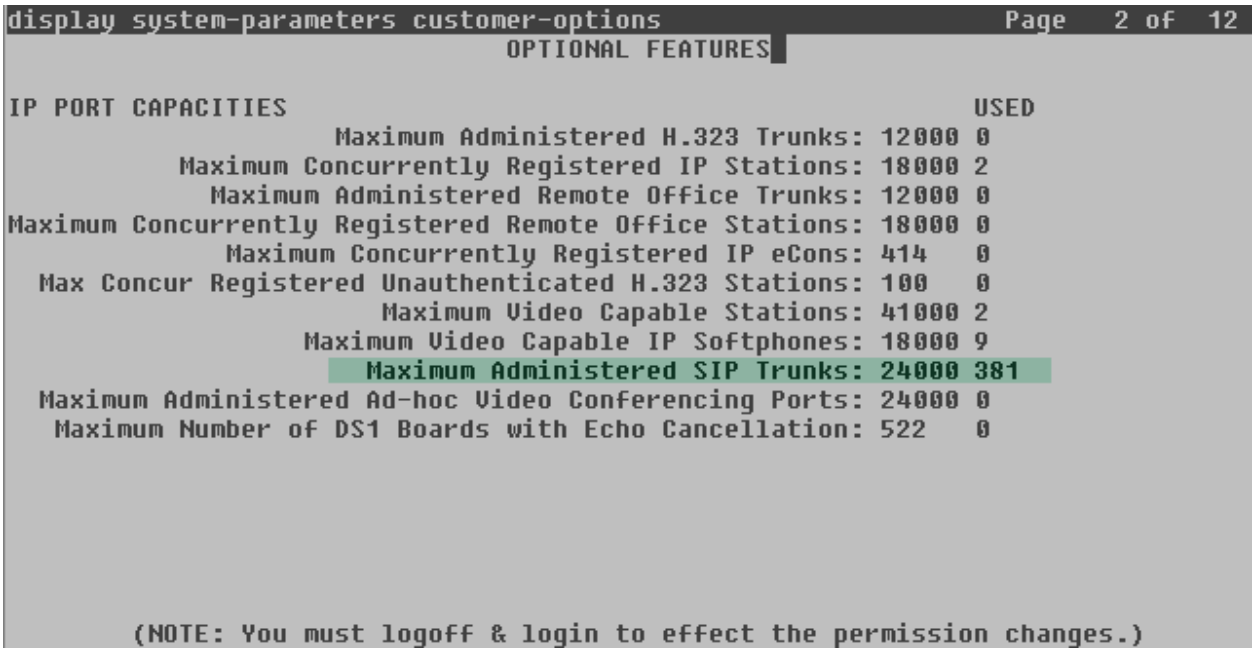
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the Fusion Connect 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 G450 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 Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **381** 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.



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  20
                            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? no
              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  20
                        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 Communication Manager *(***proc**r) and the Session Manager security module (**asm**). 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
CM_HP_server           192.168.10.12
asm                    10.10.5.32
default                0.0.0.0
media_server           192.168.10.46
procr                  10.10.5.12
procr6                 ::
tftp                   192.168.10.150
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Fusion used codecs G.711MU and G.729A, on the SIP trunk, in this order of preference. Enter the corresponding codecs in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

                       IP CODEC SET

   Codec Set: 2

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

On **Page 2**, set the **Fax Mode** to ***off***. See the note regarding fax support in **Section 2.2**.

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

                       IP CODEC SET

                           Allow Direct-IP Multimedia? n

                                                                Packet
                       Mode                 Redundancy          Size(ms)
   FAX                 off                  0
   Modem               off                  0
   TDD/TTY             off                  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 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***sil.miami.avaya.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 2                                    Page   1 of  20
                              IP NETWORK REGION
  Region: 2
Location: 1    Authoritative Domain: sil.miami.avaya.com
   Name: Service Provider      Stub Network Region: n
MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: yes
    Codec Set: 2               Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 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 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

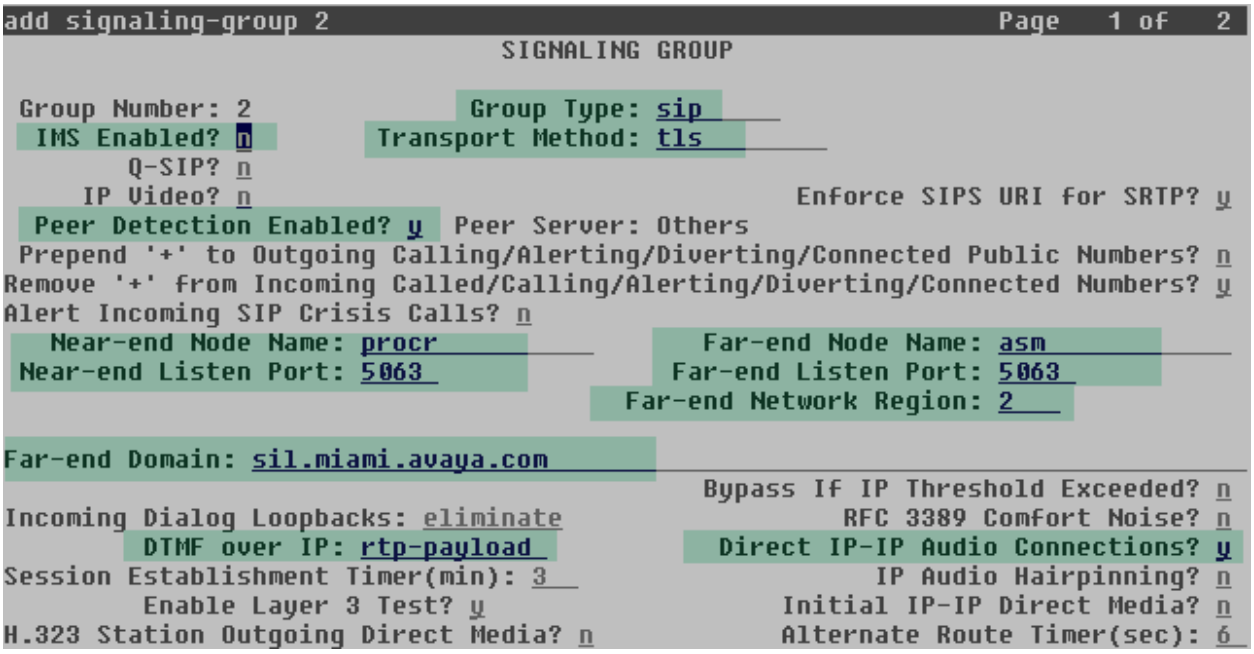
```
change ip-network-region 2                                    Page   4 of  20

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

5.6. Signaling Group

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

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

  Note: Once the **Peer-Server** field is updated to ***SM***, the system changes the default values of the following fields, setting them to display–only:
  - **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to ***y***.
  - **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to ***n***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***asm***. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.



- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so 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 ***5063***.
- 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 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group shown in 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.

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

Group Number: 2                    Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SP            COR: 1      TN: 1      TAC: 602
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk        Auth Code? n
                                          Member Assignment Method: auto
                                                    Signaling Group: 2
                                                  Number of Members: 6
```

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

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

TRUNK PARAMETERS

     Unicode Name: auto

                                        Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y
```

On **Page 3**, set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number (CPN) sent to the far-end. When ***public*** format is used, Communication Manager automatically inserts a "+" sign, preceding the numbers in the "From", "Contact" and "P-Asserted Identity" (PAI) headers. The addition of the "+" sign impacted interoperability with Fusion. Thus, the **Numbering Format** was set to ***private*** and the **Numbering Format** in the route pattern was set to ***unk-unk*** (see **Section 5.10**). Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

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


                  Numbering Format: private
                                                 UUI Treatment: service-provider

                                                  Replace Restricted Numbers? y
                                                  Replace Unavailable Numbers? y
```

On **Page 4**, set the **Network Call Redirection** field to ***y*** and the **Support Request History** field to ***n***. Set the **Telephone Event Payload Type** to **101**, the value preferred by Fusion. Set **Convert 180 to 183 for Early Media** to ***y***. Default values were used for all other fields.

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

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


                        Convert 180 to 183 for Early Media? y
                 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
```

5.8. Calling Party Information

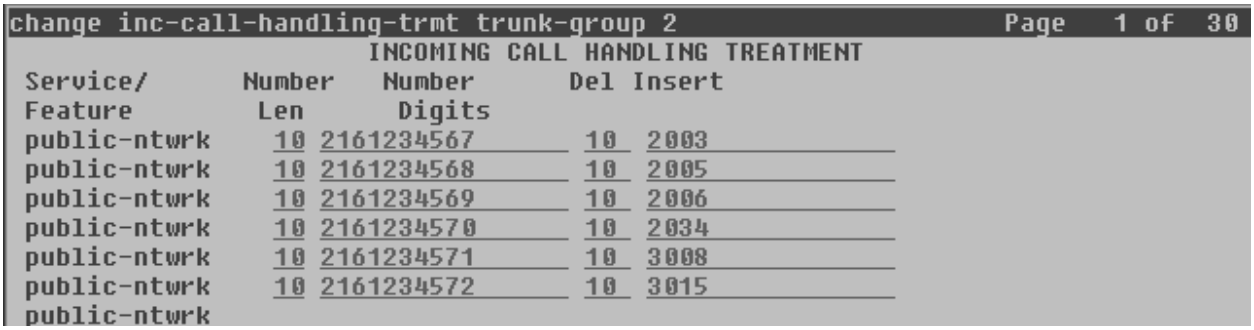
The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, six 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.

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

Ext  Ext              Trk        Private          Total
Len  Code             Grp(s)     Prefix           Len
 4   2003             2          2161234567       10    Total Administered: 10
 4   2005             2          2161234568       10       Maximum Entries: 540
 4   2006             2          2161234569       10
 4   2034             2          2161234570       10
 4   3008             2          2161234571       10
 4   3015             2          2161234572       10
                                                       
```

Note: During the compliance test, Fusion required the Main User (BTN) to be included in the From header of every outbound call. A script was created on the Avaya SBCE (**Section 7.7**) to meet this requirement. Fusion used the calling party number included in the P-Asserted-Identity for Caller ID purposes.

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 Fusion 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.



```
change inc-call-handling-trmt trunk-group 2                    Page   1 of  30
                      INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 2161234567      10  2003
 public-ntwrk    10 2161234568      10  2005
 public-ntwrk    10 2161234569      10  2006
 public-ntwrk    10 2161234570      10  2034
 public-ntwrk    10 2161234571      10  3008
 public-ntwrk    10 2161234572      10  3015
 public-ntwrk
```

5.10. Outbound Routing

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

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

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

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

```
change feature-access-codes                                   Page   1 of  10
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: ____
         Abbreviated Dialing List2 Access Code: ____
         Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
                     Announcement Access Code: 099
                      Answer Back Access Code: 015
                        Attendant Access Code: __
     Auto Alternate Routing (AAR) Access Code: 8
   Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2: ____
                Automatic Callback Activation: 016    Deactivation: 017
Call Forwarding Activation Busy/DA: 018   All: 019    Deactivation: 020
   Call Forwarding Enhanced Status: ____   Act: ____   Deactivation: ____
                       Call Park Access Code: 010
                     Call Pickup Access Code: 011
```

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

```
change ars analysis 0                                        Page   1 of   2
                          ARS DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 1

      Dialed            Total     Route    Call   Node  ANI
      String           Min  Max  Pattern  Type   Num   Reqd
  0                    1    11   2        op     ___   n
  011                  10   15   2        intl   ___   n
  1786                 11   11   2        fnpa   ___   n
  1800                 11   11   2        fnpa   ___   n
  411                  3    3    2        svcl   ___   n
  911                  3    3    2        locl   ___   n
  216                  10   10   2        hnpa   ___   n
```

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

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: Set to **1** to ensure 1 + 10 digits are sent to the service provider for long distance numbers in the North American Numbering Plan (NANP).
- **Numbering Format**: Set to ***unk-unk***. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

```
change route-pattern 2                                       Page   1 of   3
                    Pattern Number: 2      Pattern Name: Route to SP
                                  SCCAN? n     Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
   No          Mrk Lmt List Del  Digits                          QSIG
                                 Dgts                            Intw
1: 2   0       1                                                  n    user
2:                                                                n    user
3:                                                                n    user
4:                                                                n    user
5:                                                                n    user
6:                                                                n    user

    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W    Request                                 Dgts Format
                                                        Subaddress
1: y y y y y n  n           rest                        _     _  unk-unk   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

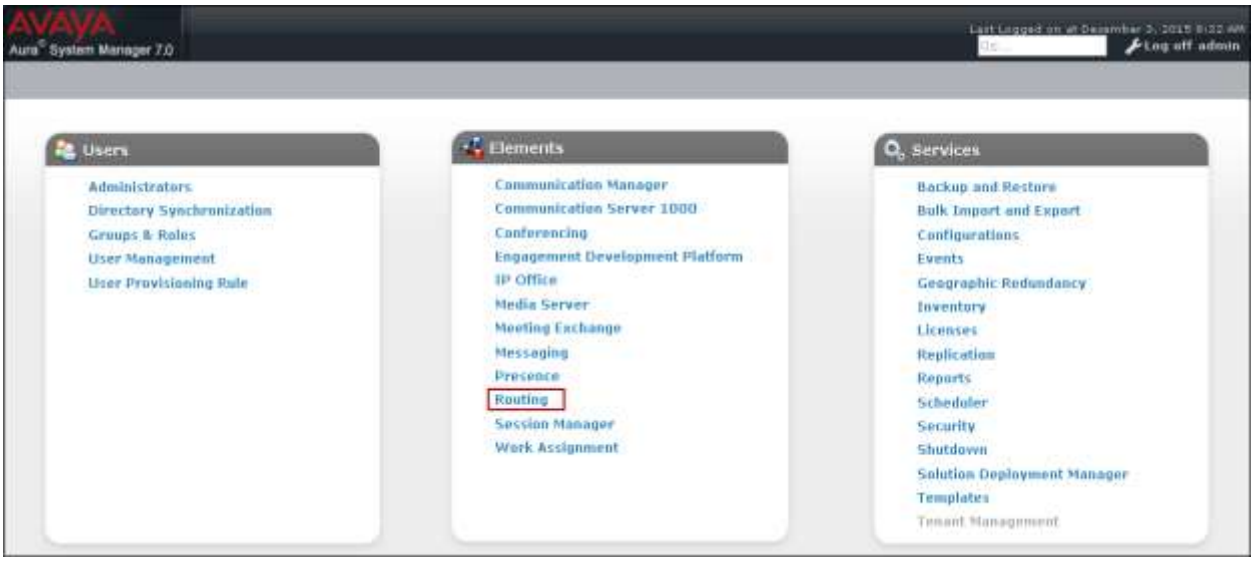
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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.

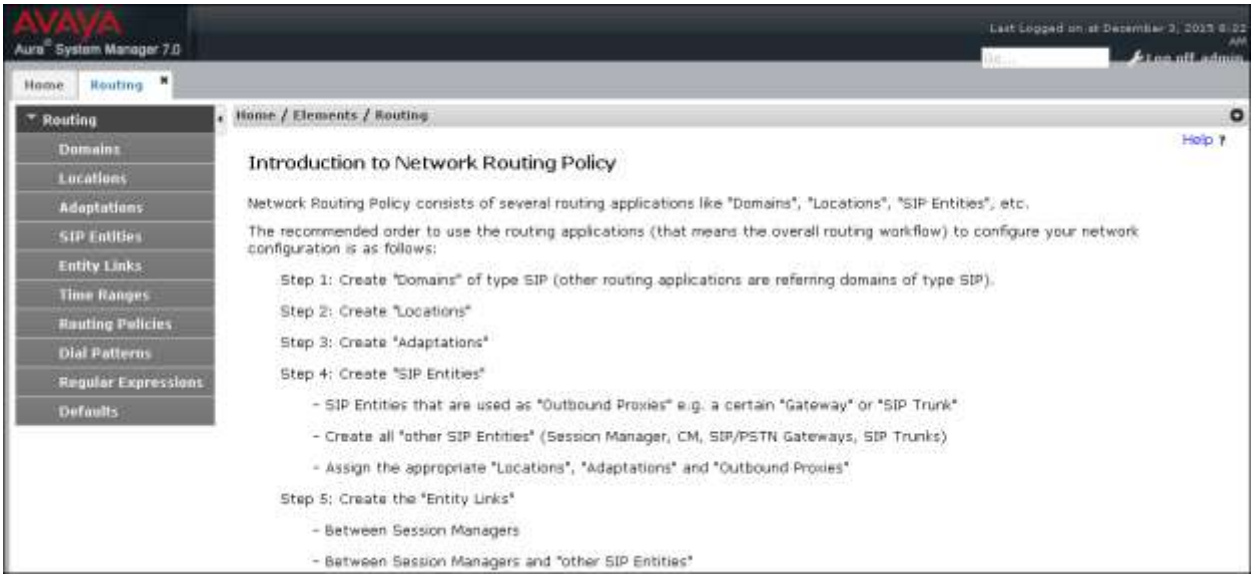
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

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). The screen shown below is then displayed; click on **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** link 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, ***sil.miami.avaya.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.

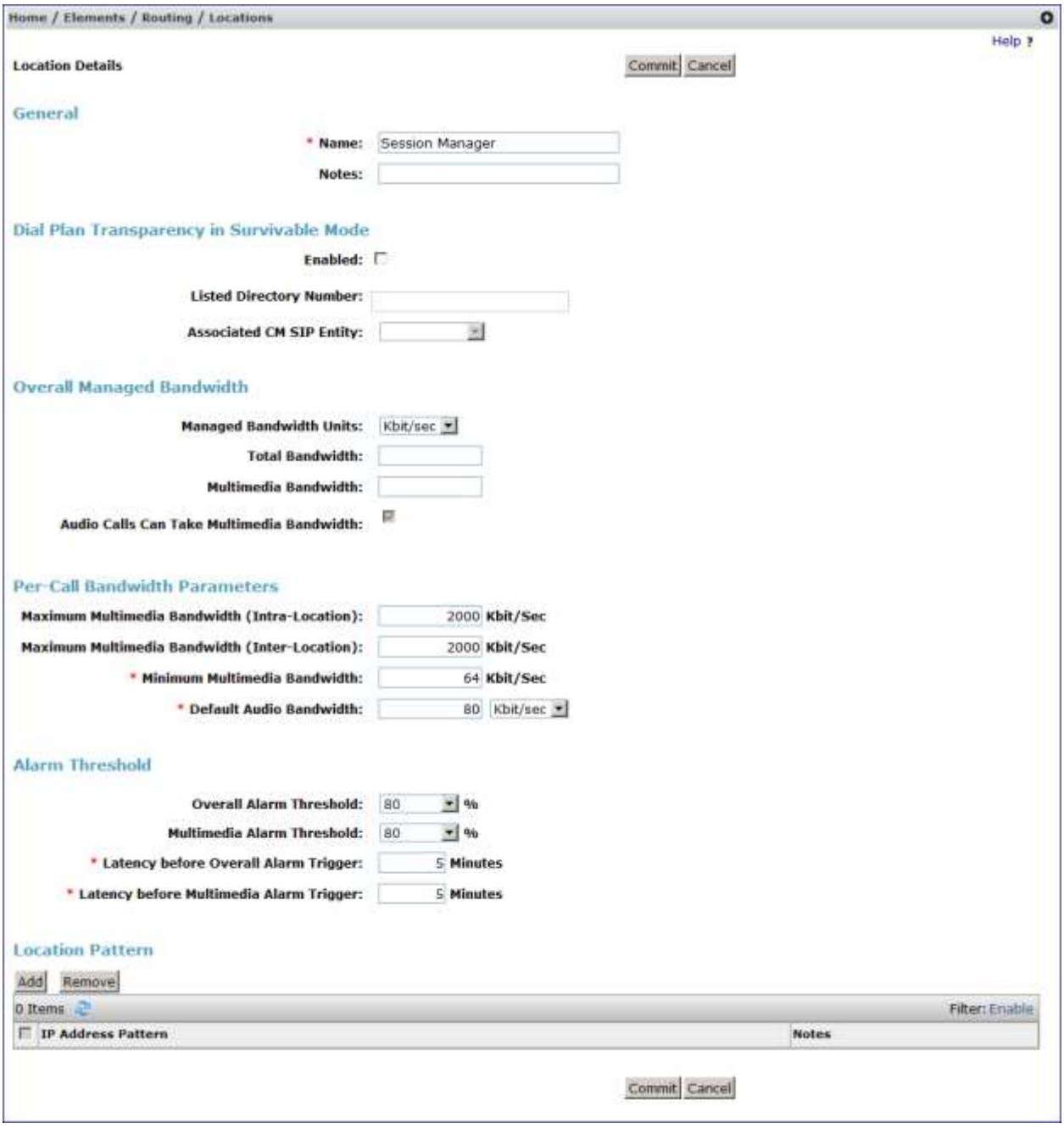
6.3. Locations

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. 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.

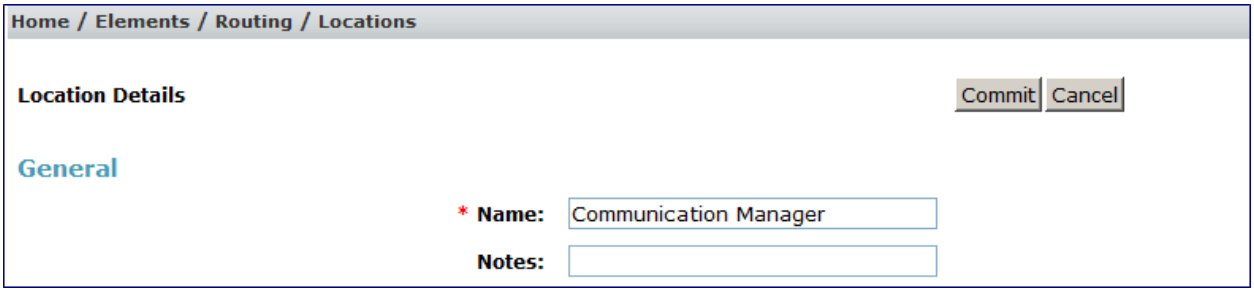
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

Defaults can be used for all other parameters.

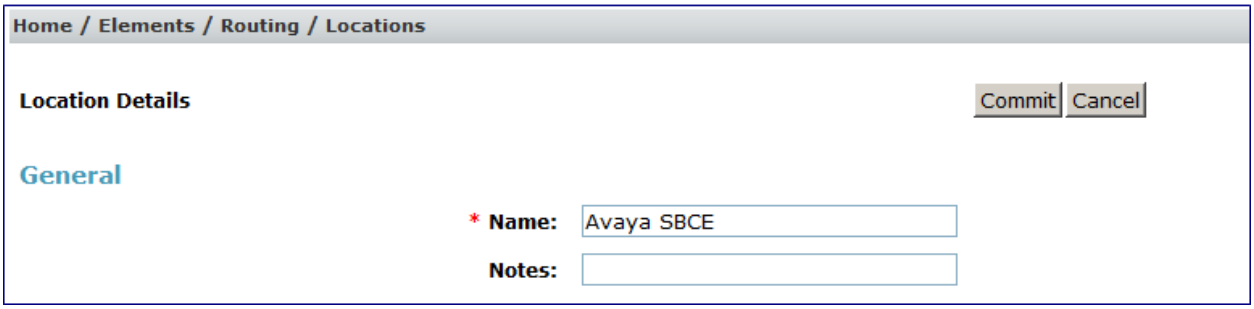
The following screen shows the location details for the location named ***Session Manager***. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Default values were used for all parameters.



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



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



6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.0 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 "Outbound_Header_Removal" 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 and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

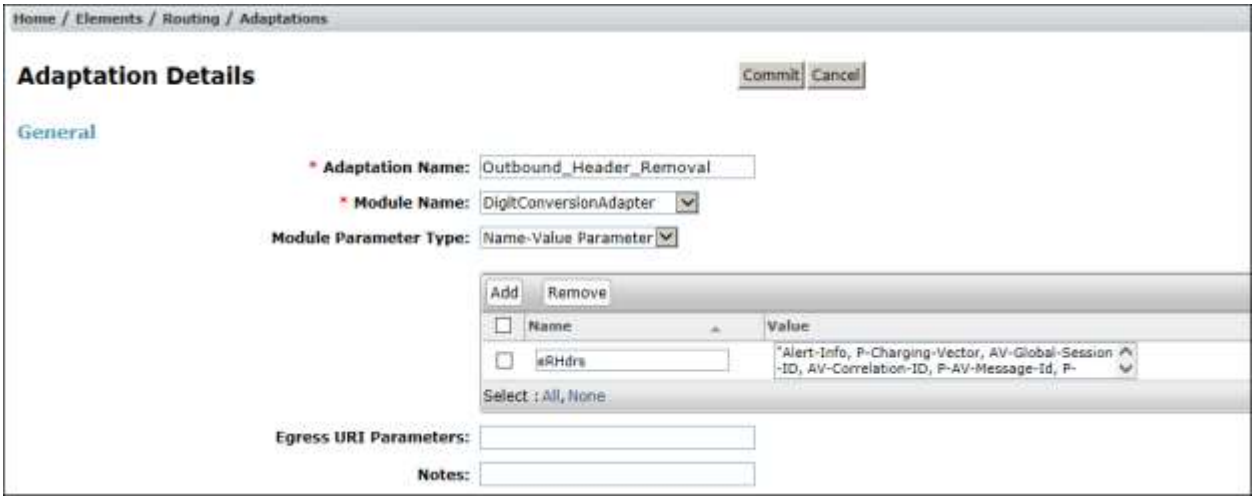
Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name**: Enter an appropriate name.
- **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 ***"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View"***

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.

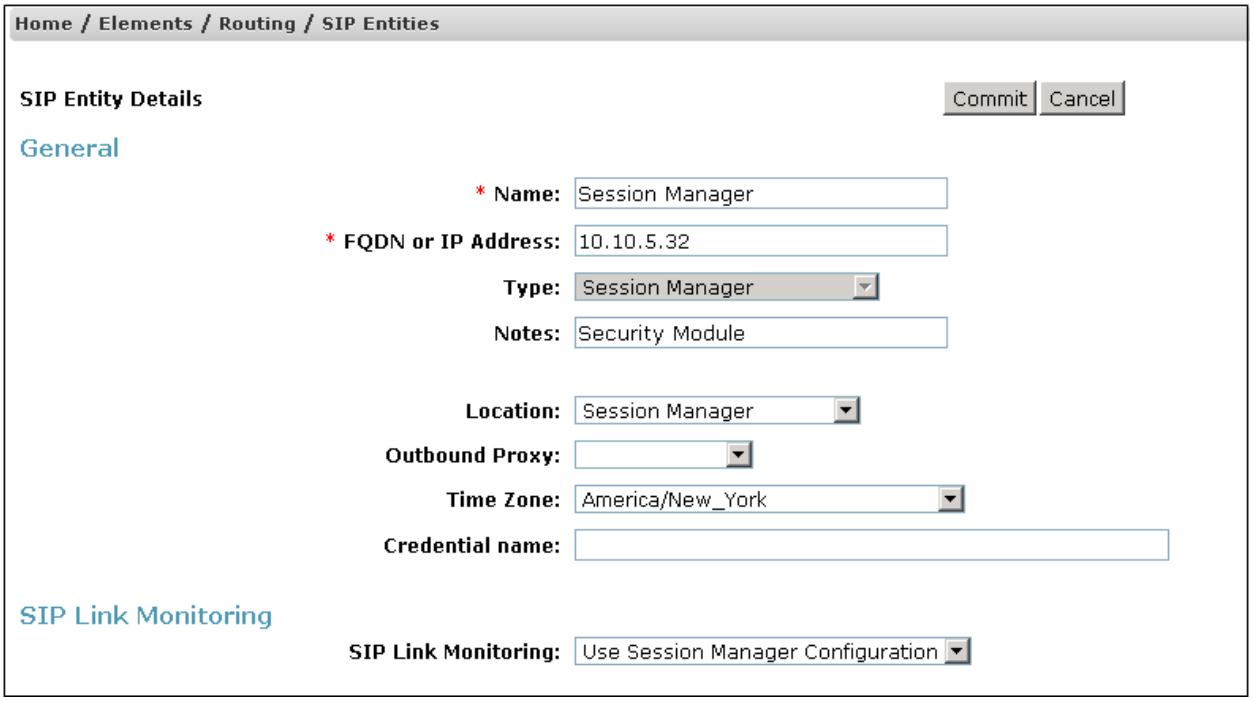


6.5. SIP Entities

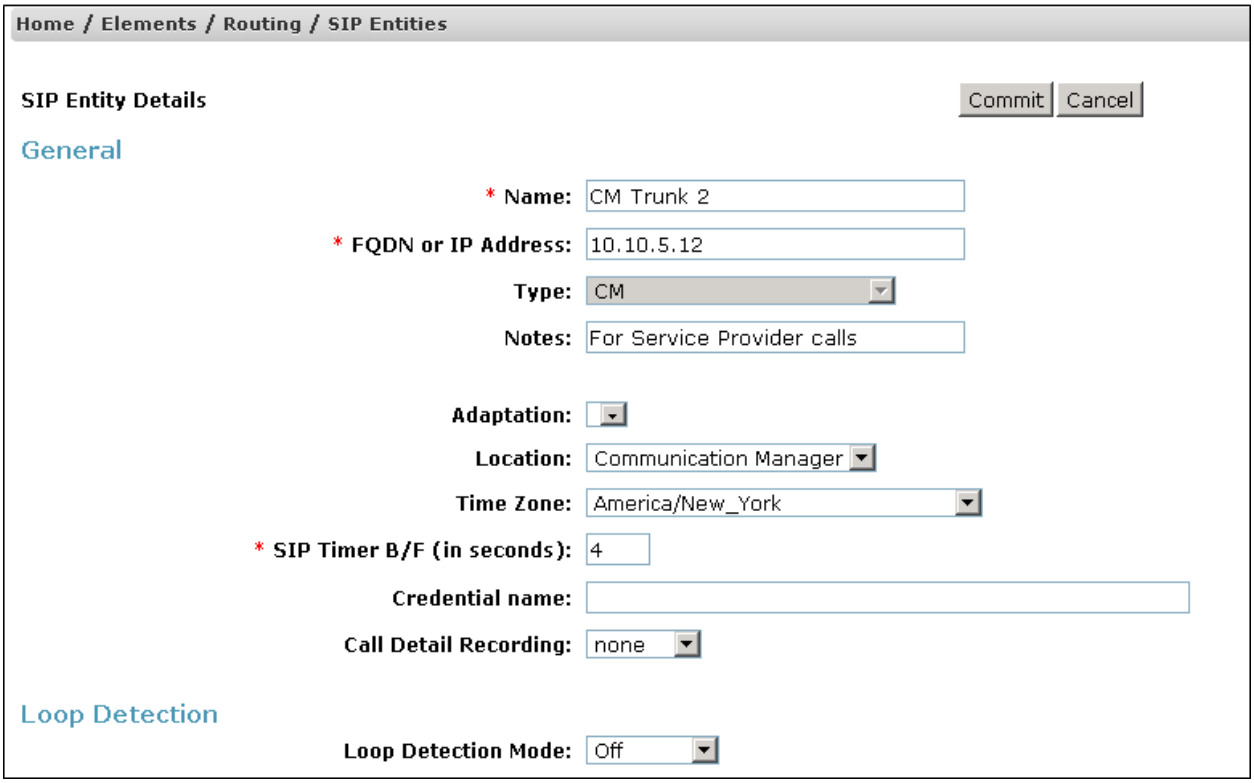
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** 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.

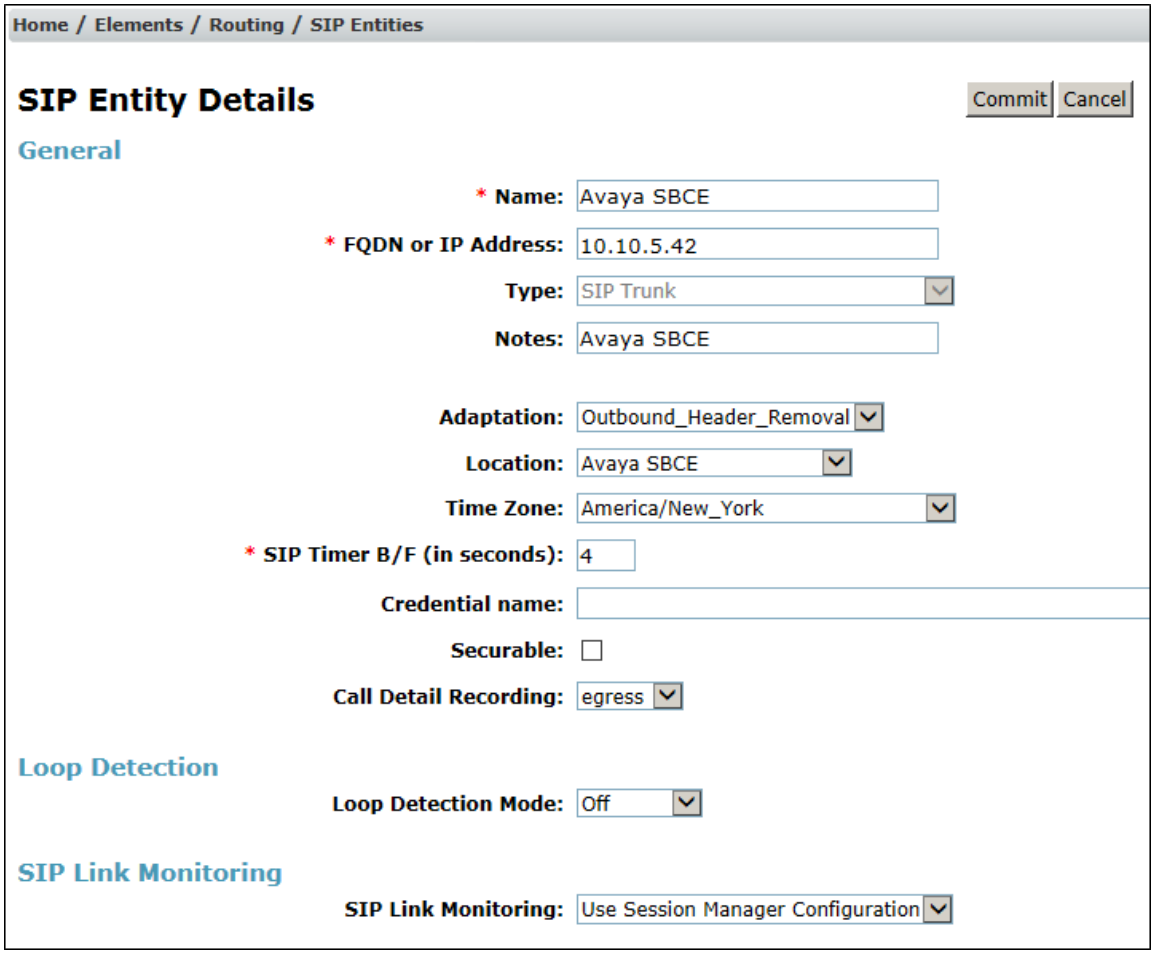
The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.



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



The following screen shows the addition of the Avaya SBCE Entity. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). On the **Adaptation** field, the adaptation module ***Outbound_Header_Removal*** previously defined in **Section 6.4** was selected.



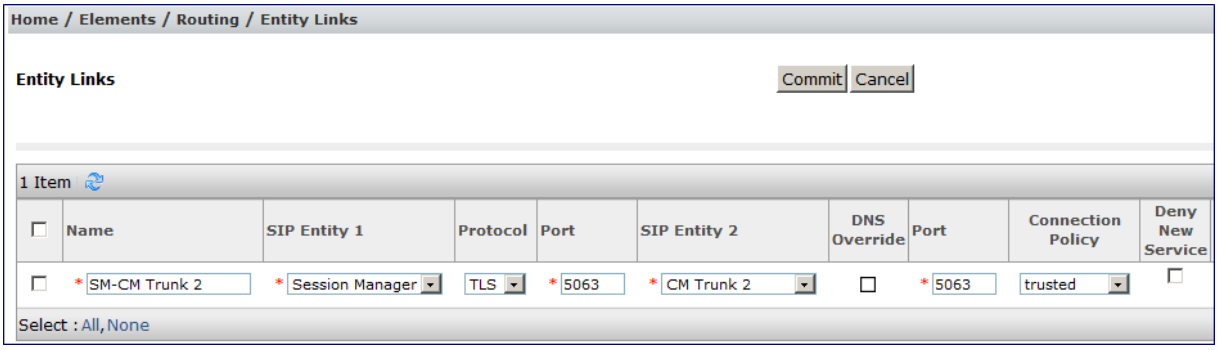
6.6. Entity Links

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:

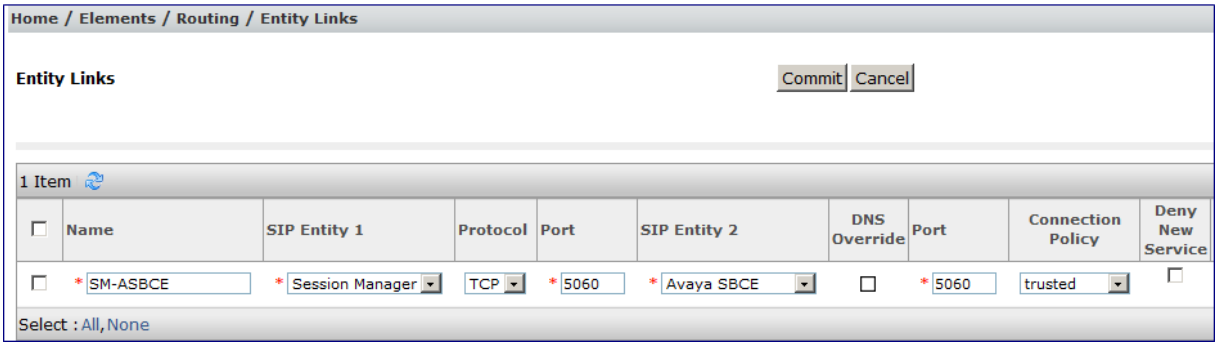
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name 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 and ports 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. ***TCP*** and port ***5060*** were used.

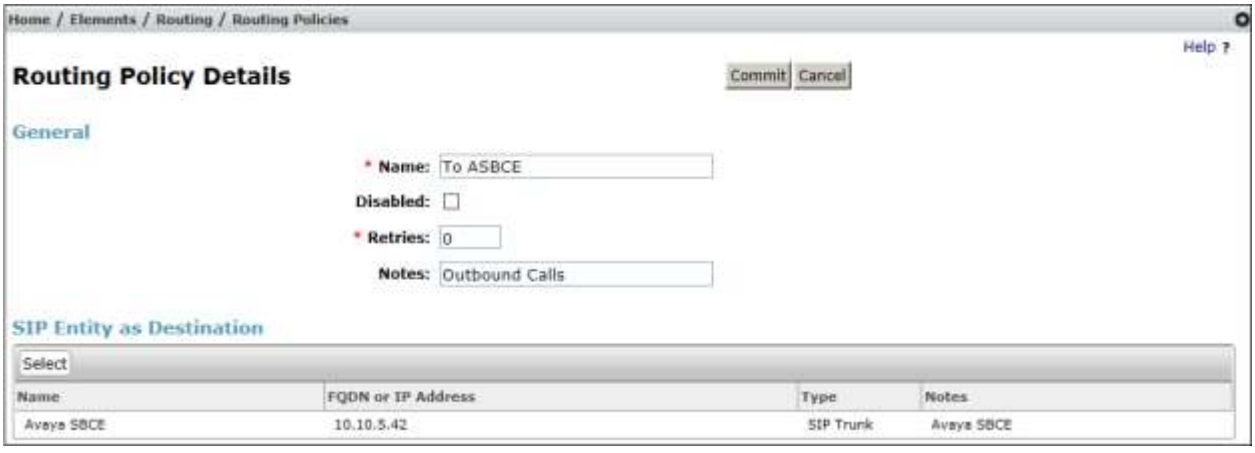


6.7. Routing Policies

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 and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

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



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:

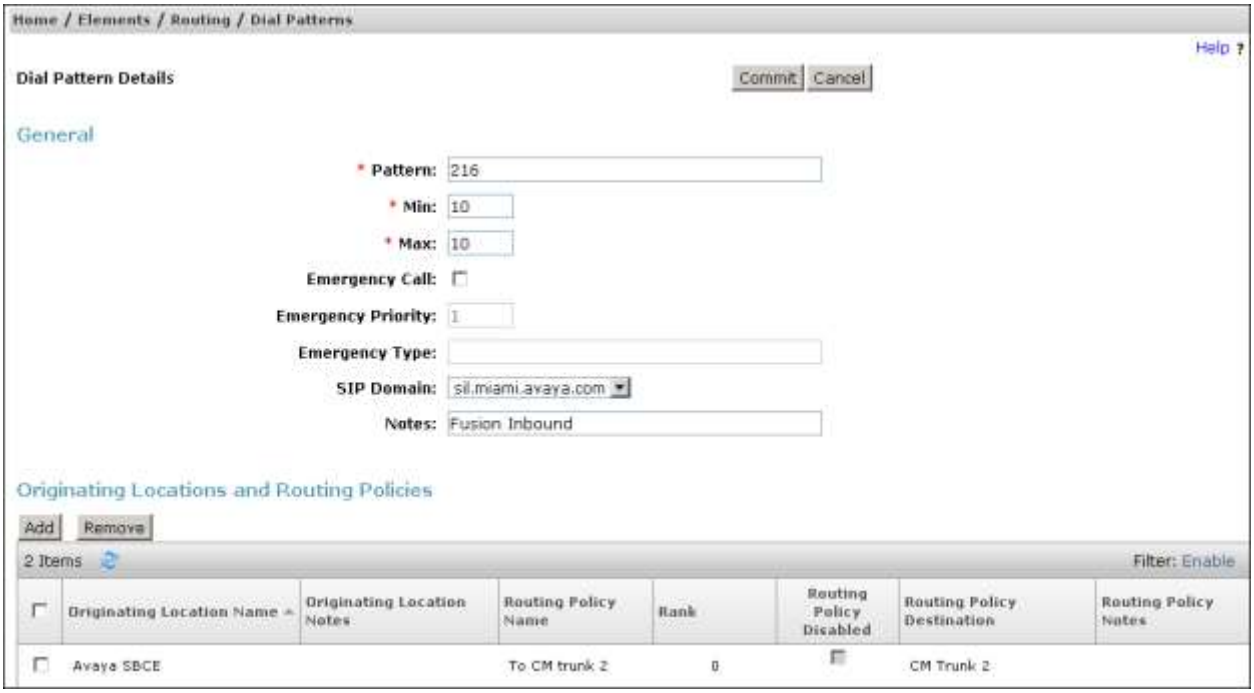
In the **General** section, enter the following values:

- **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**.

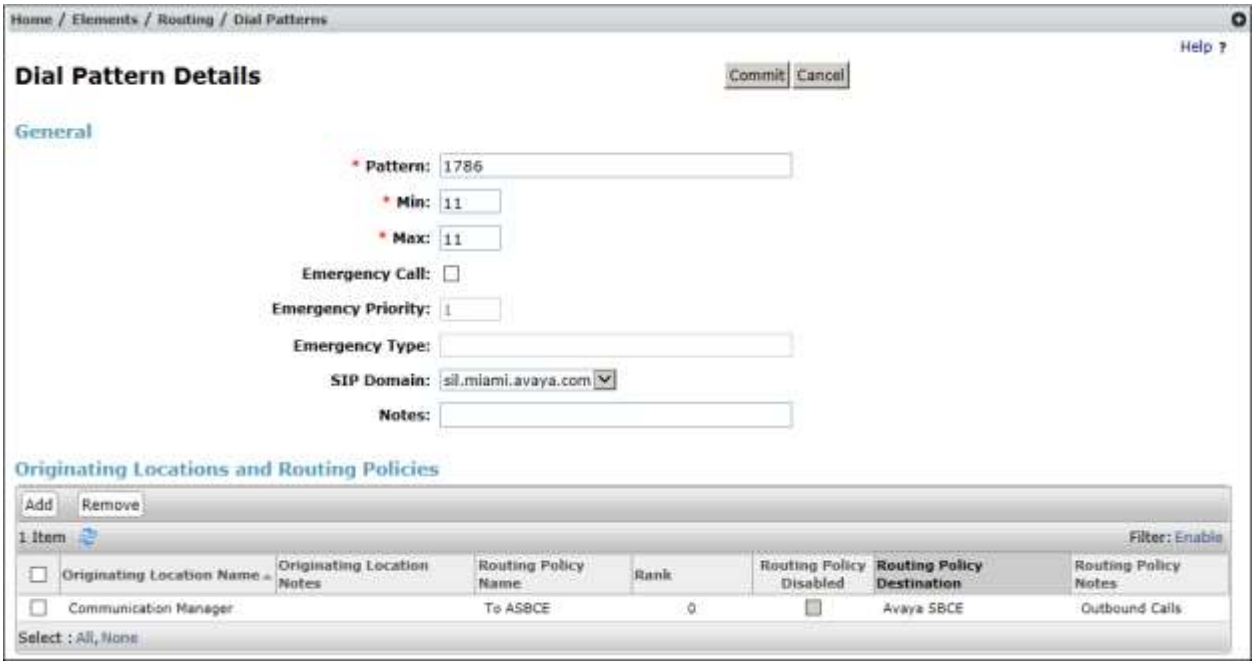
Default values can be used for the remaining fields. Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with ***216***, which was in the range of the DID numbers assigned by the service provider to the SIP trunk, arriving from location ***Avaya SBCE***, used route policy ***To CM trunk 2*** to Communication Manager.



Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The example in this screen shows that 11 digit dialed numbers for outbound calls, beginning with a number such as ***1786*** used for test purposes during the compliance test, arriving from the ***Communication Manager*** location**,** will use route policy ***To ASBCE***, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP Trunk.



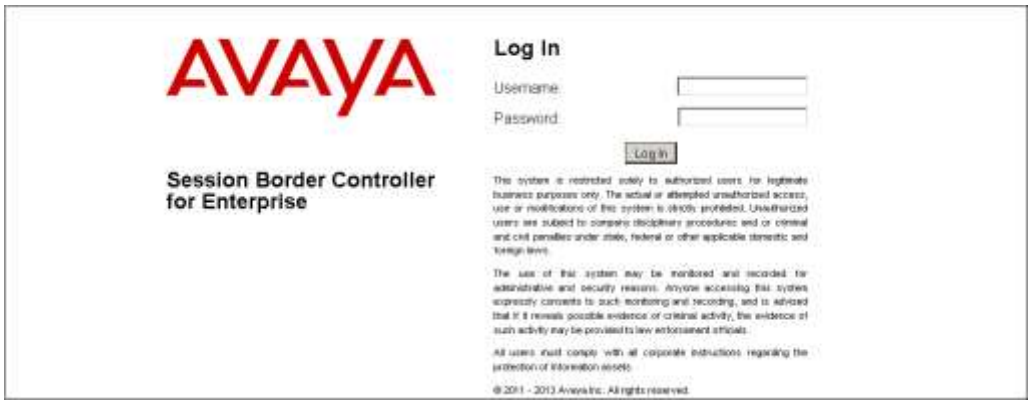
Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

7. Configure Avaya Session Border Controller for Enterprise

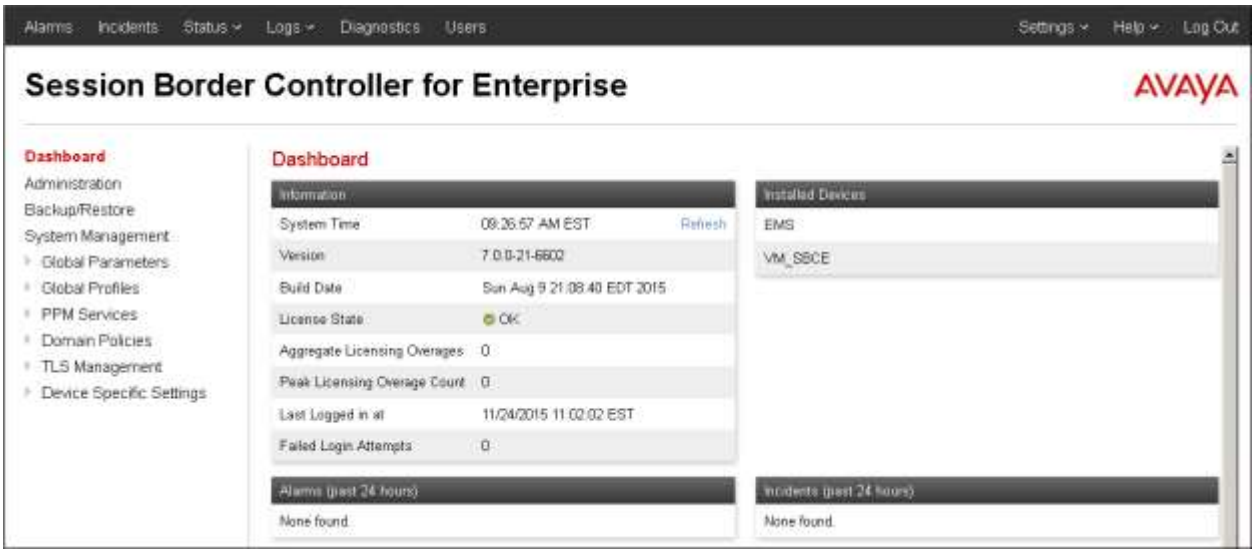
This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more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

7.1. System Access

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



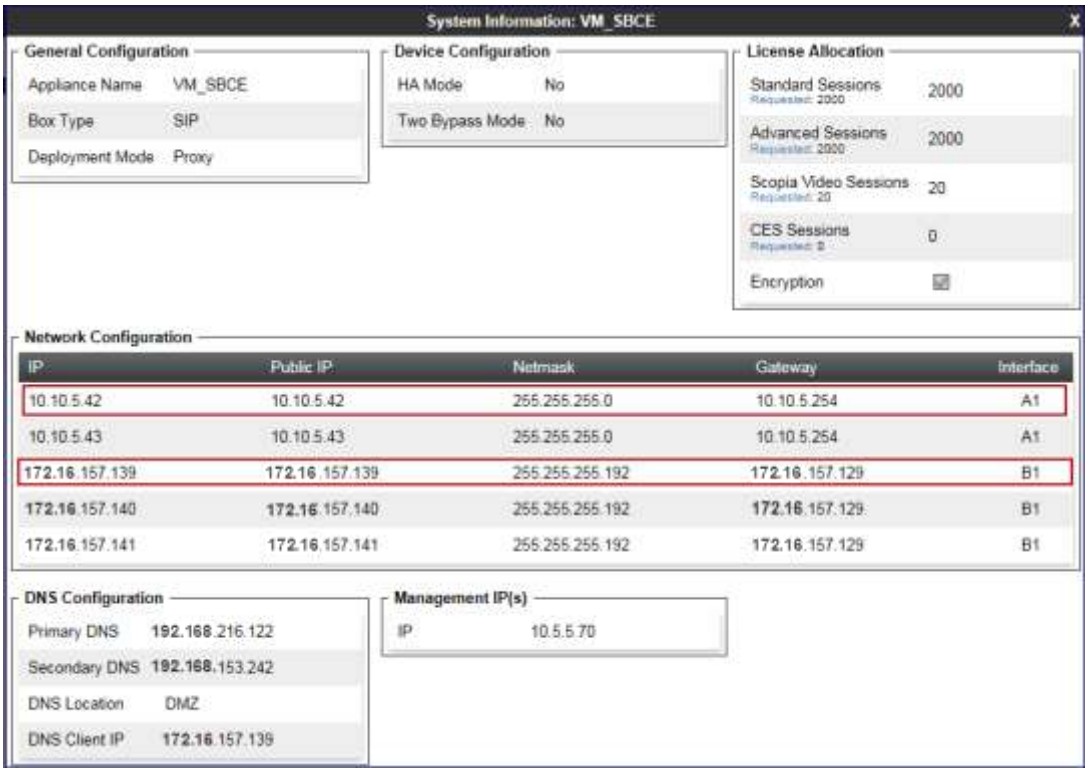
Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya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



7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named ***VM_SBCE*** is shown. The management IP address that was configured during installation and the current software version are shown here. Note that the management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is ***Commissioned***, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings.



The **A1** and **B1** interfaces correspond to the private and public interfaces of the Avaya SBCE. Note that the highlighted **A1** and **B1** IP addresses are the ones used for the SIP trunk to the service provider, and the ones relevant to these Application Notes. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

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

7.3. Network Management

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

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, ***VM_SBCE*** in the sample configuration. On the **Networks** tab, verify or enter the network information as needed. Note that the **A1** and **B1** interfaces correspond to the private and public interfaces for the Avaya SBCE.

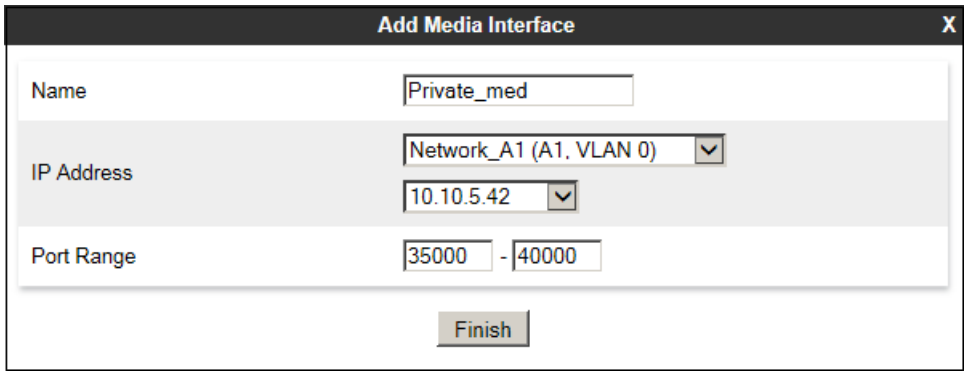
In the configuration used during the compliance test, IP address ***10.10.5.42*** was assigned to interface **A1**, and IP address ***172.16.157.139*** was assigned to interface **B1**.

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

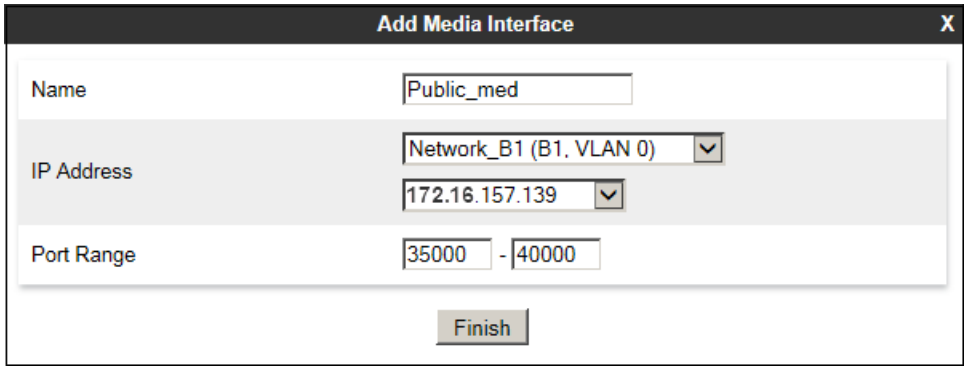
7.4. Media Interfaces

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

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Under **IP Address**, select from the drop-down menus the network and IP address associated with the private interface of the SBCE (A1). The **Port Range** was left at the default values of ***35000-40000***. Click **Finish**.



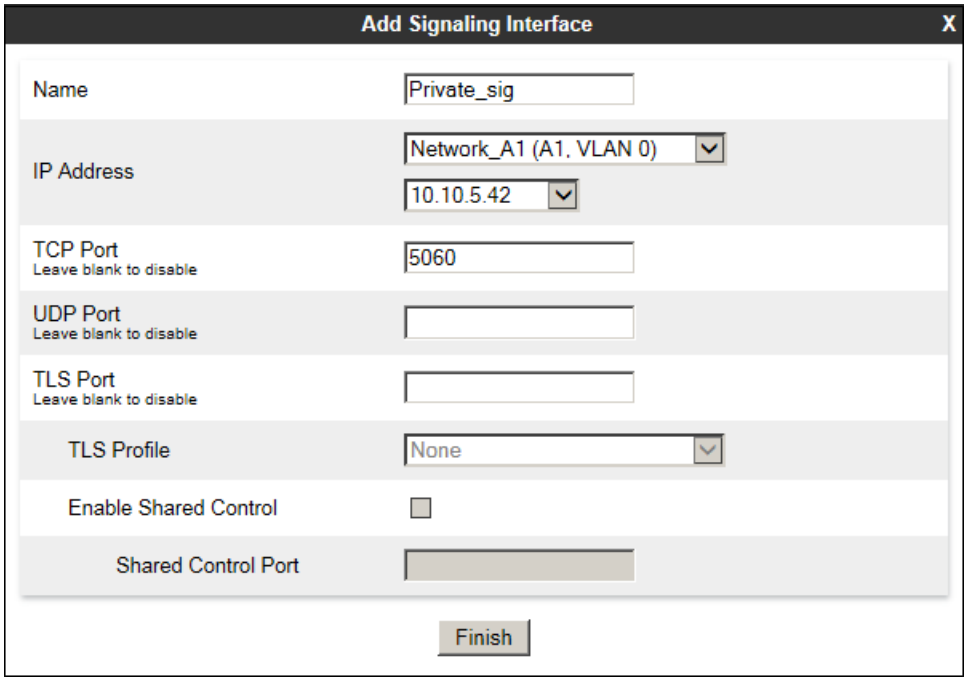
A Media Interface facing the public network side was similarly created with the name **Public_med**, as shown below. Under **IP Address**, the network and IP address associated with the public interface of the SBCE (B1) were selected from the drop-down menus. The **Port Range** was left at the default values. Click **Finish**.



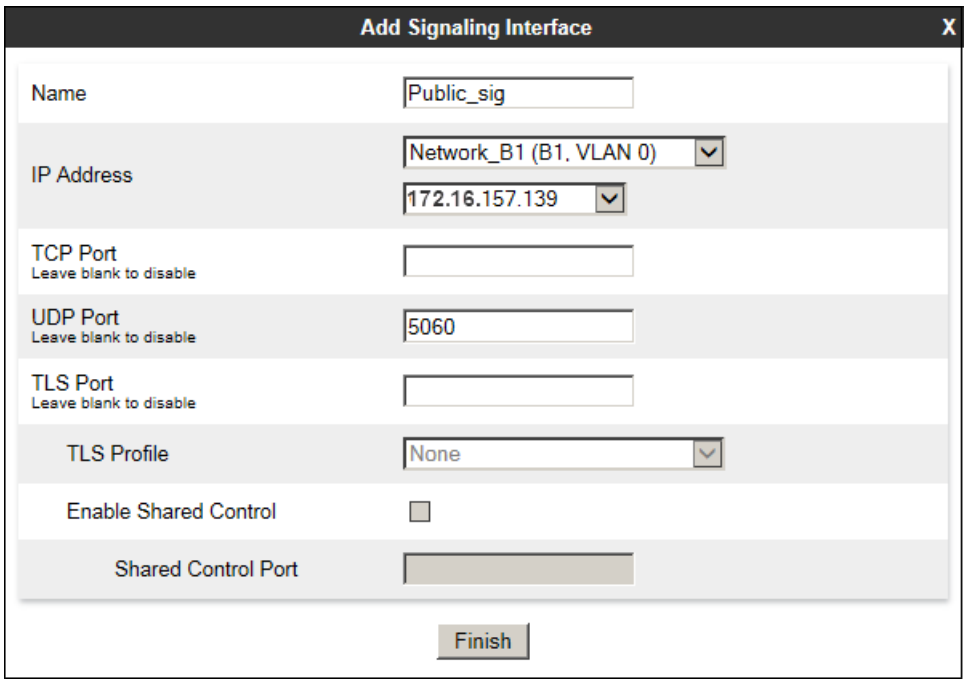
7.5. Signaling Interfaces

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

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Under **IP Address**, select from the drop-down menus the network and IP address associated with the private interface of the SBCE (A1). Enter ***5060*** for **TCP Port**, since TCP port 5060 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**. Click **Finish**.



A second Signaling Interface with the name **Public_sig** was similarly created in the service provider's direction. Under **IP Address**, the network and IP address associated with the public interface of the SBCE (B1) were selected from the drop-down menus. Enter ***5060*** for **UDP Port**, since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic. Click **Finish**.

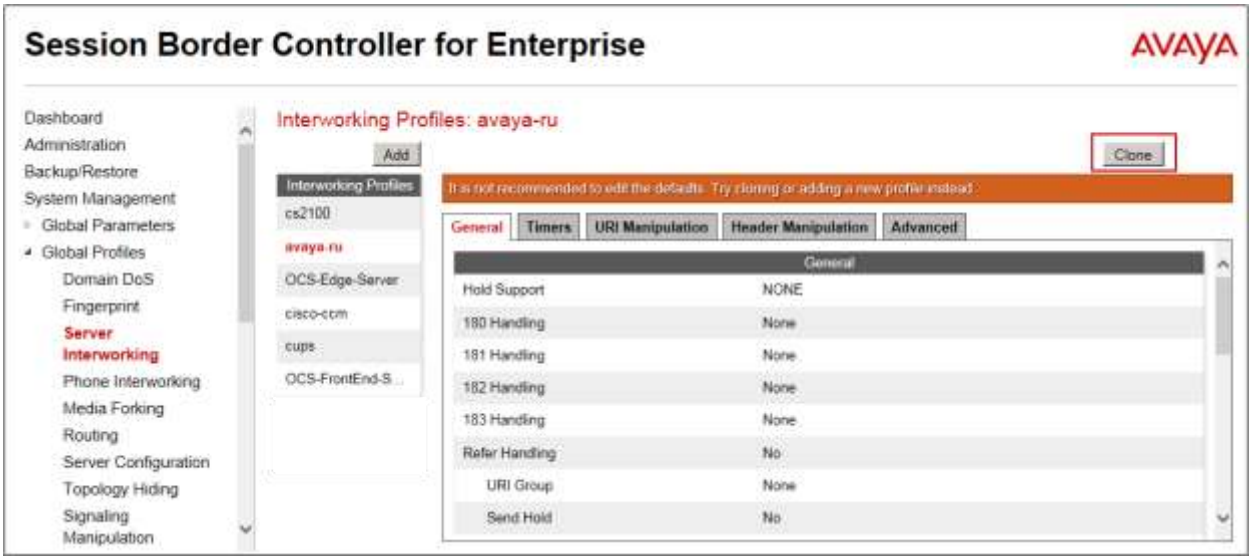


7.6. Server Interworking

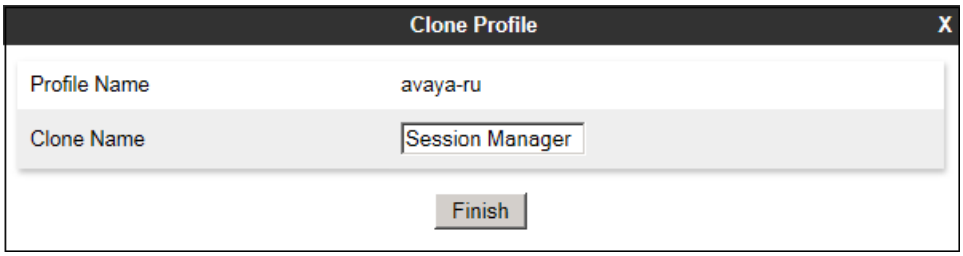
Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server). In the reference configuration, Session Manager functions as the Call Server and the Fusion SIP Proxy as the Trunk Server.

7.6.1. Server Interworking Profile – Enterprise

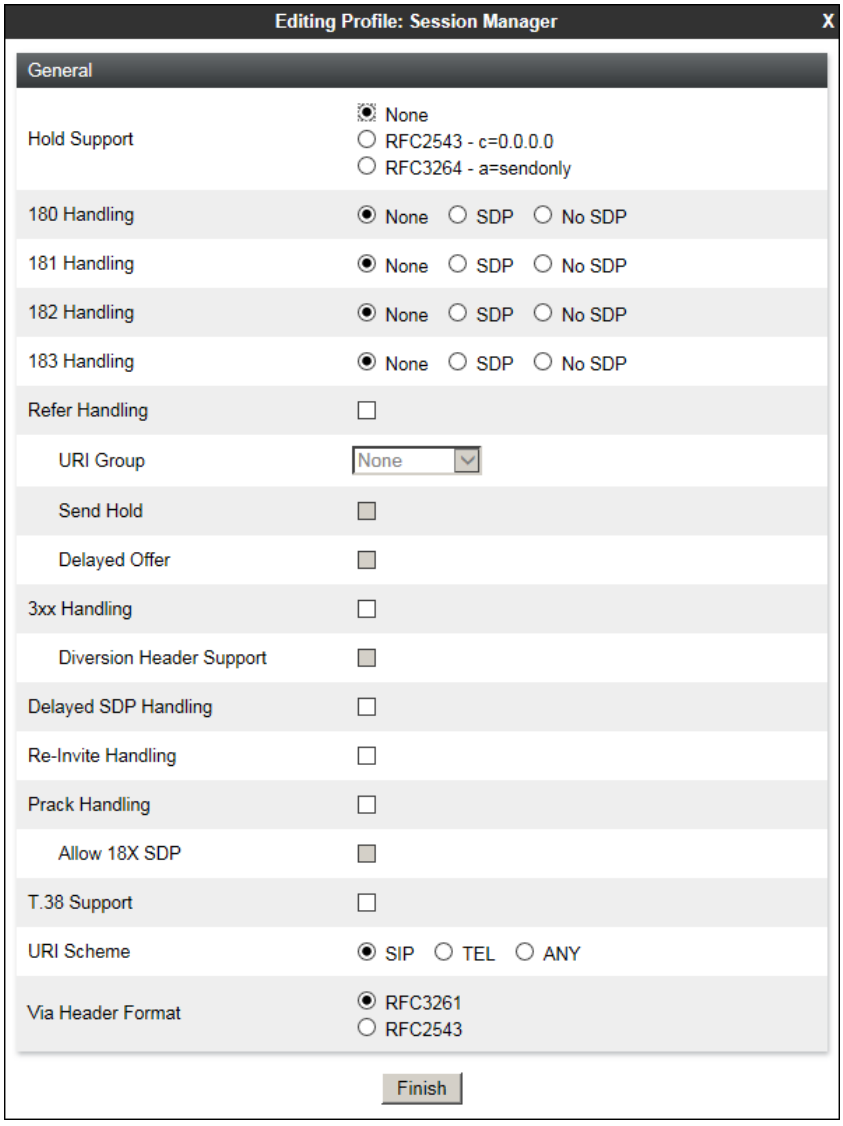
Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select ***avaya-ru*** from the list of pre-defined profiles. Click **Clone**.



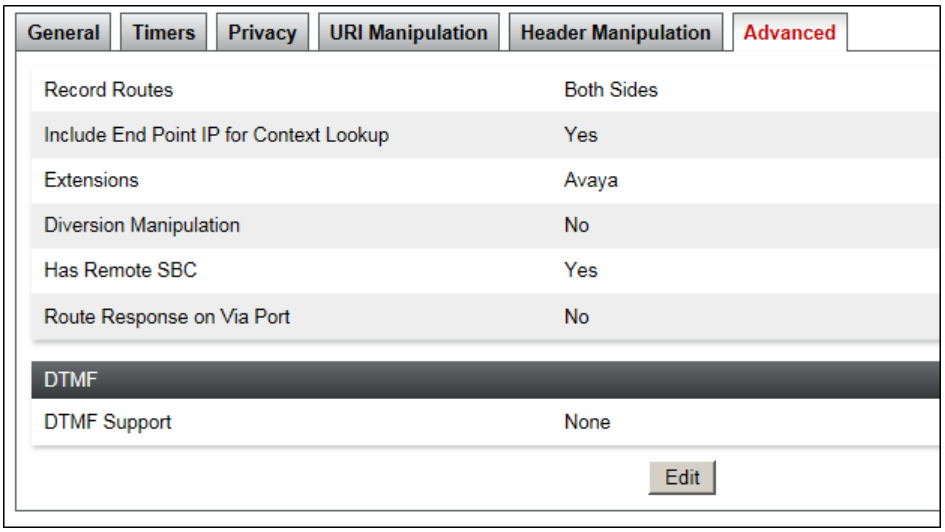
Enter a descriptive name for the cloned profile. Click **Finish**.



On the newly cloned ***Session Manager*** interworking profile, on the **General** tab, scroll down to the bottom of the page and click **Edit** (not shown). All parameters retain their default values, as shown on the screen below. Click **Finish**.



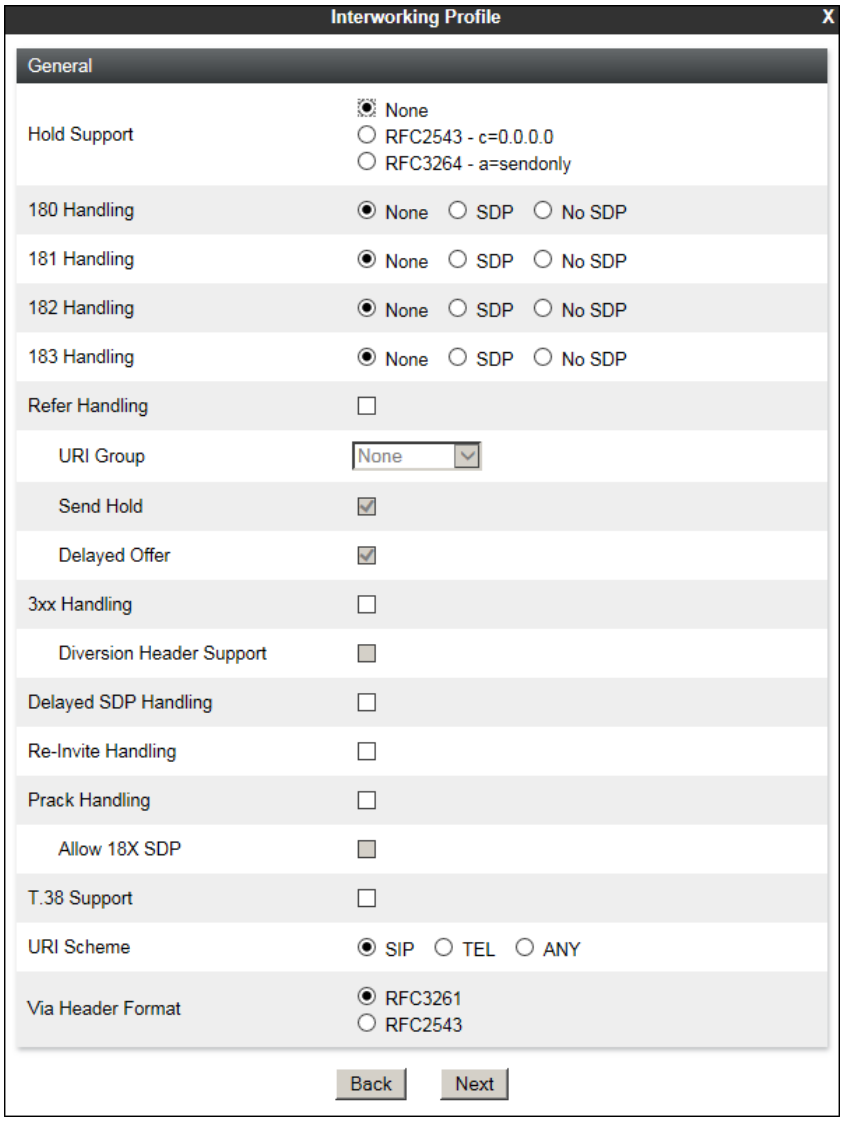
The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries. The **Advaced** tab settings are shown on the screen below:



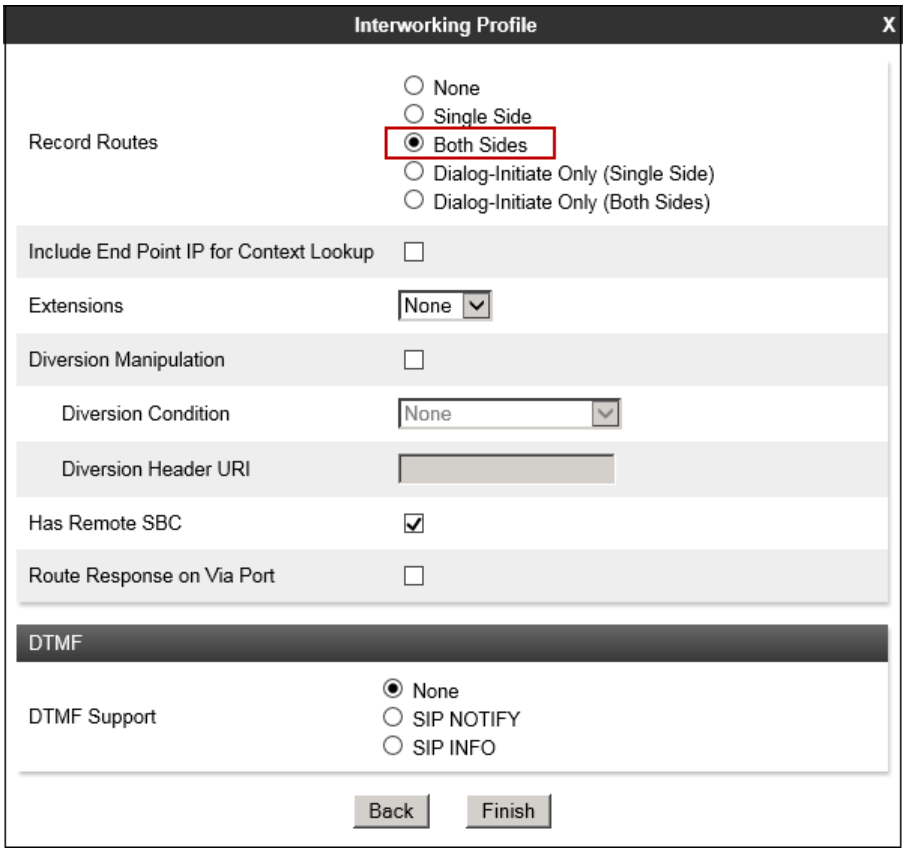
7.6.2. Server Interworking Profile – Service Provider

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

On the **General** screen, all parameters retain their default values. Click **Next**.



Click **Next** on the **SIP Timers** and **Privacy** tabs (not shown). On the **Advanced/DTMF** tab, select ***Both Sides*** under **Record Routes**. Accept the defaults settings for all other fields. Click **Finish**.



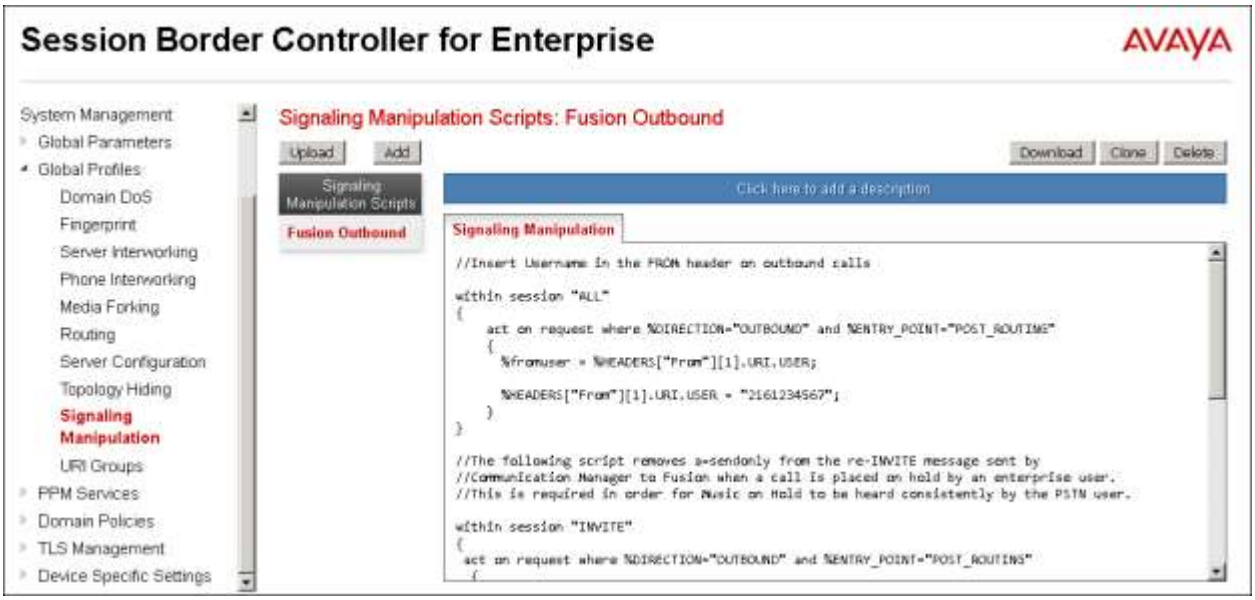
7.7. Signaling Manipulation

The screen below shows the finished Signaling Manipulation script named ***Fusion Outbound*** created during the compliance test. This script was needed to:

- Include the Main User (BTN) in the "From" header of all outbound calls. This was a requirement specified by Fusion, in order for outbound calls from the enterprise to be accepted and processed.
- Remove the "sendonly" attribute, included in the SDP of the re-INVITEs Communication Manager sends to the service provider when calls are placed on-hold. This was necessary as a workaround to the Music on Hold issue described in **Section 2.2**.
- Remove the "gsid" and "epv" parameters from outbound "Contact" headers. These parameters had no significance to the service provider and add unnecessary size to the packets entering the service provider's network.

The script will later be applied to the Server Configuration profile corresponding to the service provider, later in **Section 7.8.2**.

To add a Signaling Manipulation script, from the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click **Add** to open the SigMa Editor screen, where the text of the script can be entered or copied.



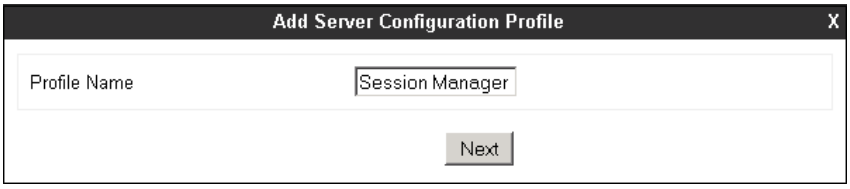
The details of the script can be found in **Appendix A** in this document.

7.8. Server Configuration

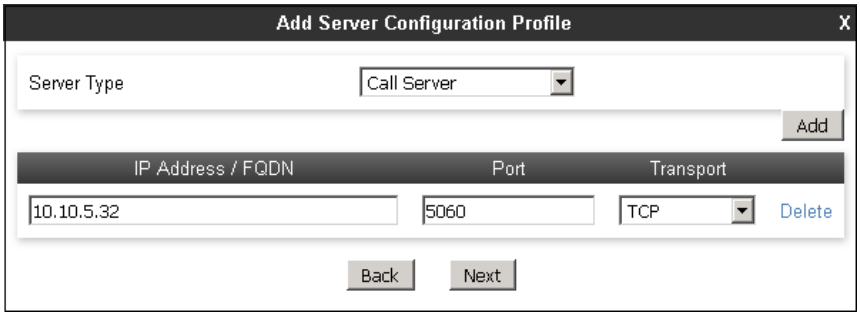
Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and the SIP Proxy at the service provider network (Trunk Server).

7.8.1. Server Configuration Profile – Enterprise

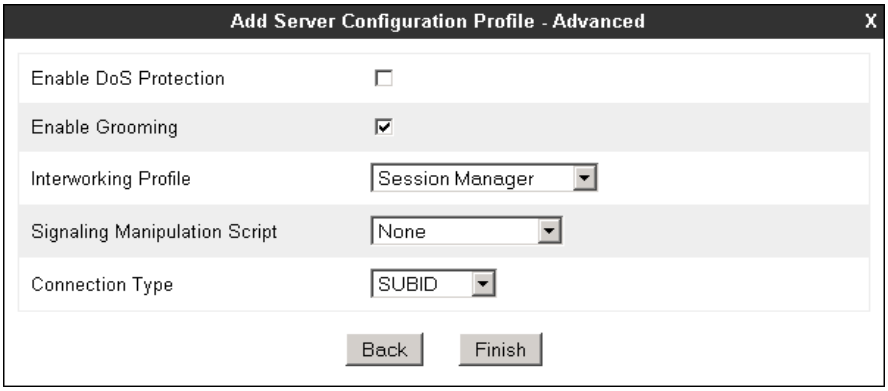
From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server. Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



On the **Add Server Configuration Profile** Tab select ***Call Server*** from the drop down menu under the **Server Type**. On the **IP Addresses / FQDN** field**,** enter the IP address of the Session Manager Security Module (**Section 6.5)**. Enter ***5060*** under **Port** and select ***TCP*** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously in **Section 6.6**. Click **Next**.

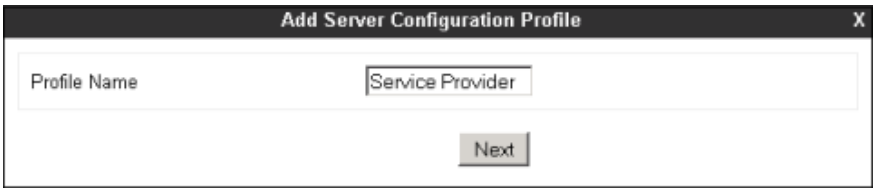


Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, since TCP is used, check the **Enable Grooming** box. Select ***Session Manager*** from the **Interworking Profile** drop down menu. Click **Finish**.

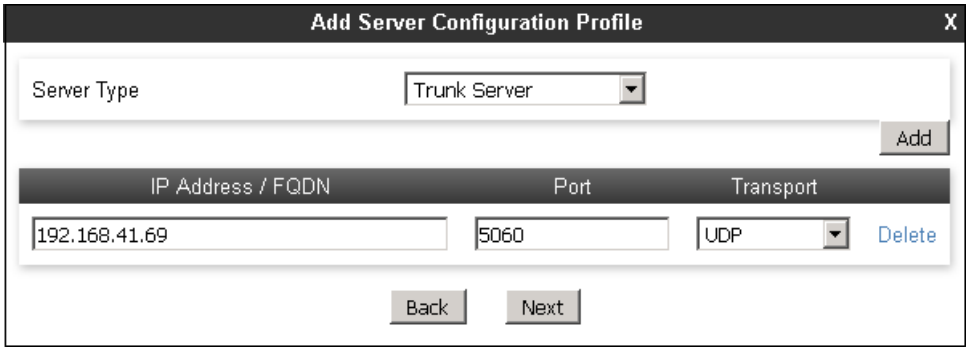


7.8.2. Server Configuration Profile – Service Provider

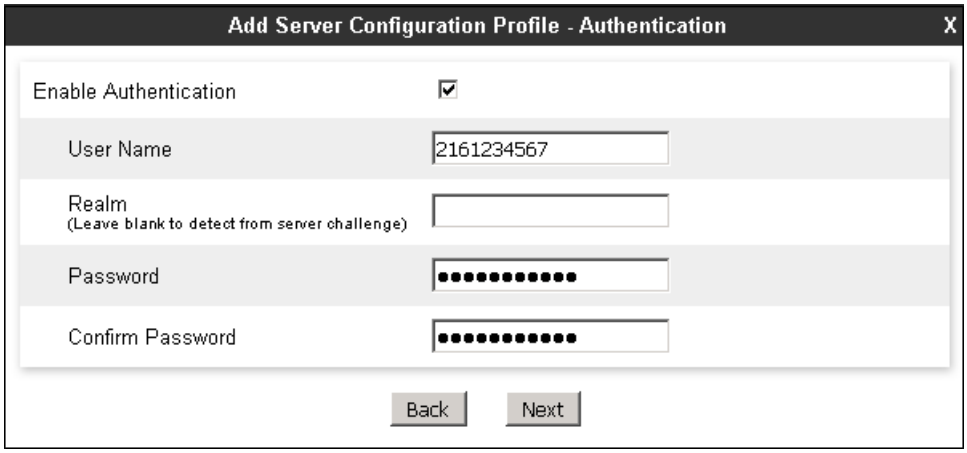
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



On the **Add Server Configuration Profile** Tab select ***Trunk Server*** from the drop down menu for the **Server Type**. On the **IP Addresses / FQDN** field, enter the IP address of the service provider SIP proxy server. Enter ***5060*** under **Port**, and select **UDP** for **Transport**. Click **Next**.

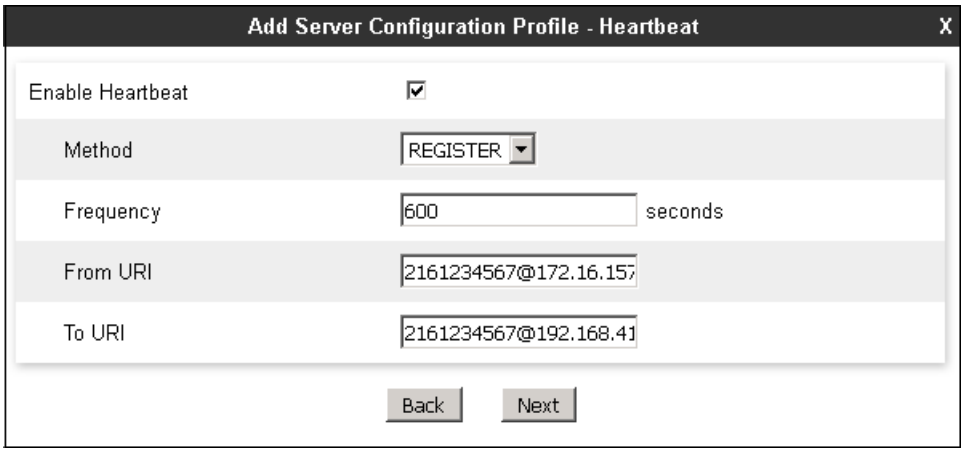


On the **Authentication** tab, check the **Enable Authentication** box. Enter the **User Name**, and **Password** information supplied by the service provider for the authentication of the SIP trunk. Leave the **Realm** field blank. The Realm will be automatically detected from the service provider authentication challenge. Click **Next**.

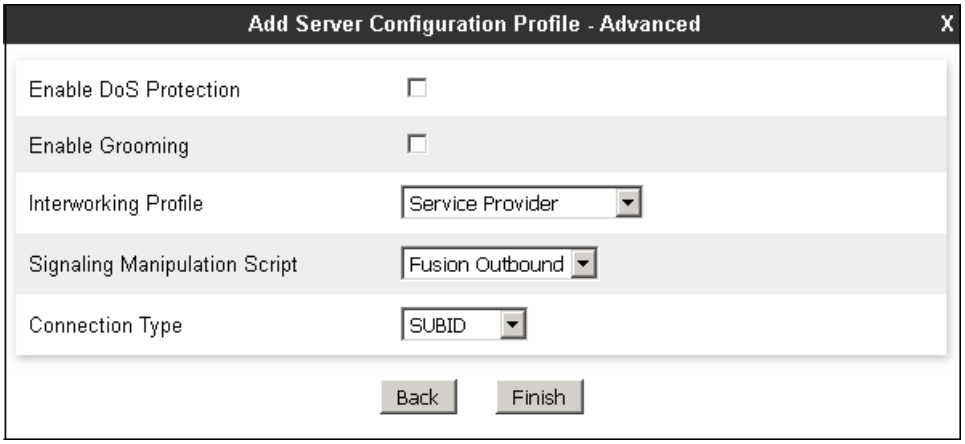


On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency:** Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Fusion proxy server in order to refresh the registration binding of the SIP trunk. ***600*** seconds was the value used. The actual amount of time between REGISTER messages is negotiated during the trunk registration process, and it is ultimately set by the service provider.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the **User Name** entered in the **Authentication** screen, and the IP addresses of the public interface of the Avaya SBCE (***172.16.157.139***) and the service provider proxy server (***192.168.41.69***) respectively, like shown on the example below.
- Click **Next**.



On the **Advanced** tab, select ***Service Provider*** from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the ***Fusion Outbound*** script created in **Section 7.7**. Click **Finish**.

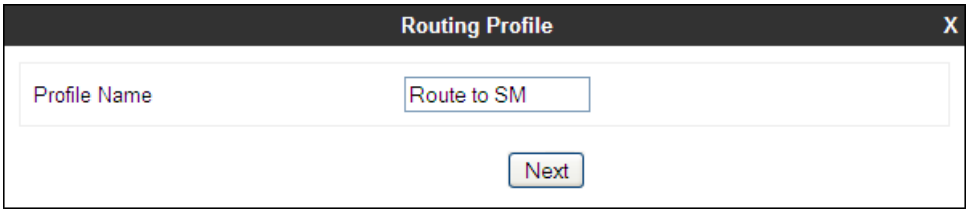


7.9. Routing

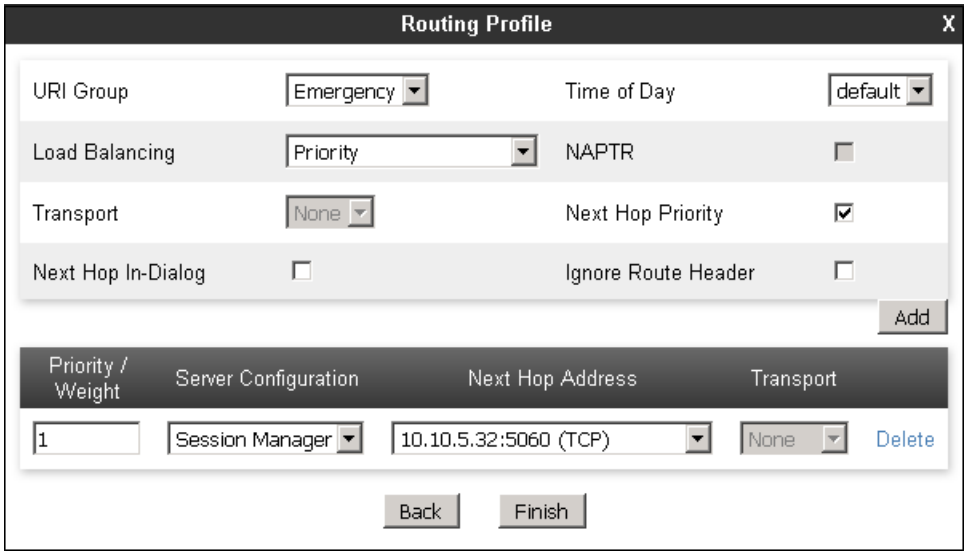
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls,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

7.9.1. Routing Profile – Enterprise

To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown). Enter an appropriate **Profile Name** similar to the example below. Click **Next**.

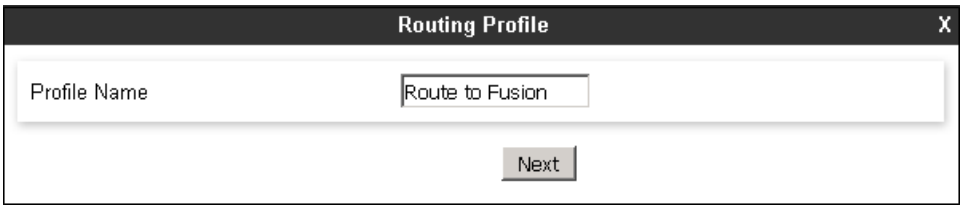


On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Enter ***1*** under **Priority/Weight**. Under **Server Configuration**, select ***Session Manager***. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.8.1**. Defaults were used for all other parameters. Click **Finish**.

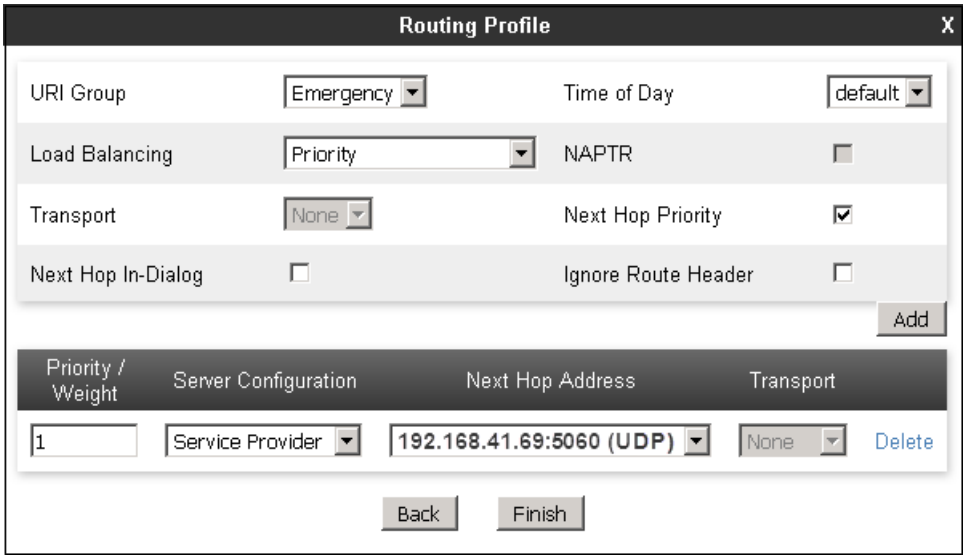


7.9.2. Routing Profile – Service Provider

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route. Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Enter ***1*** under **Priority/Weight**. Under **Server Configuration**, select ***Service Provider***. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in **Section 7.8.2**. Defaults were used for all other parameters. Click **Finish**.



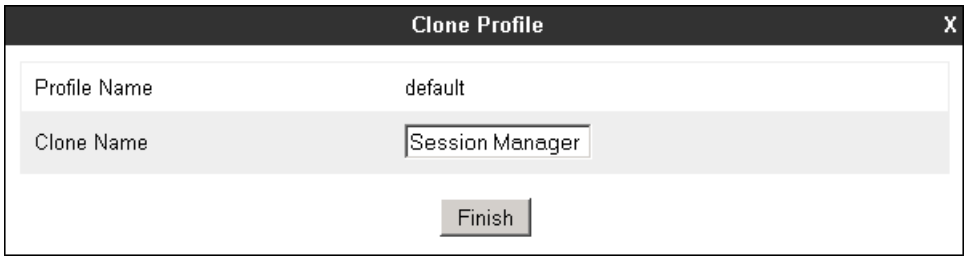
7.10. Topology Hiding

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

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

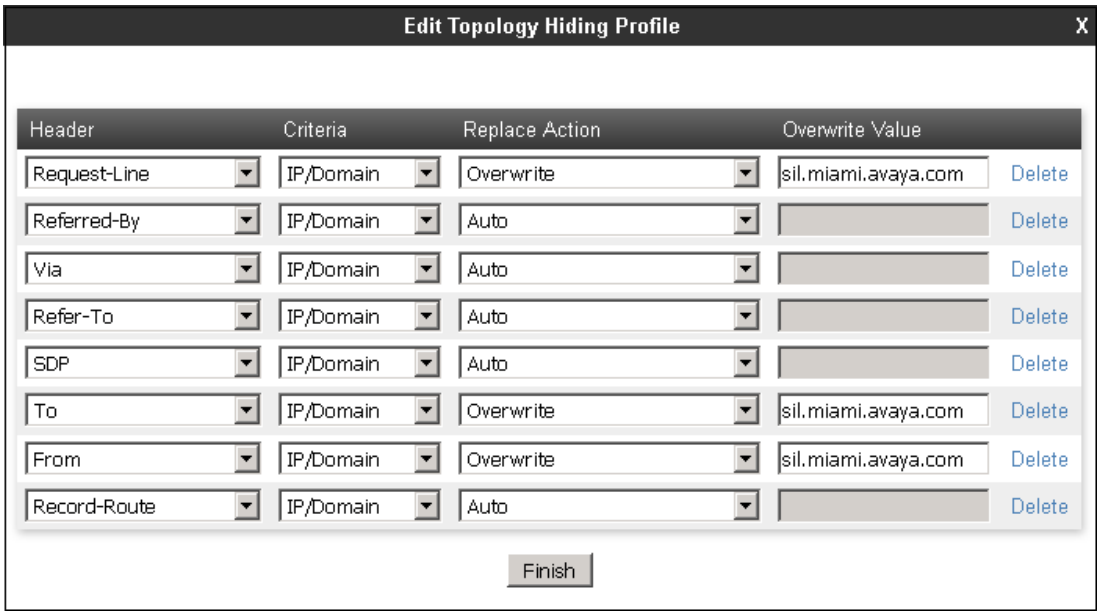
7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select ***default*** from the list of pre-defined profiles and click the **Clone** button (not shown). Enter a **Clone Name** such as the one shown below. Click **Finish**.



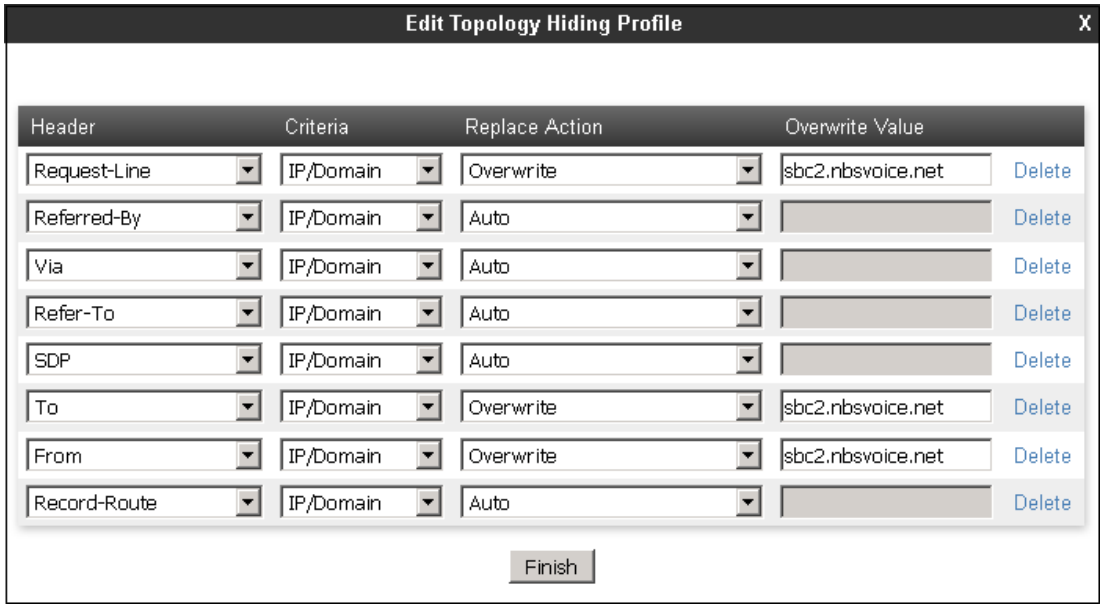
On the newly cloned **Session Manager** profile screen, click the **Edit** button (not shown).

For the **Request-Line**, **To** and **From** headers, select ***Overwrite*** in the **Replace Action** column and enter the enterprise SIP domain ***sil.miami.avaya.com***, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**. Default values were used for all other fields. Click **Finish**.



7.10.2. Topology Hiding Profile – Service Provider

A Topology Hiding profile named ***Service Provider*** was similarly configured in the direction of the SIP trunk to the service provider. For the **Request-Line**, **To** and **From** headers, select **Overwrite** in the **Replace Action** column. In the **Overwrite Value** column, enter the SIP domain expected by the service provider on these headers. During the compliance test, this domain was ***sbc2.nbsvoice.net***. Click **Finish**.



7.11. End Point Policy Groups

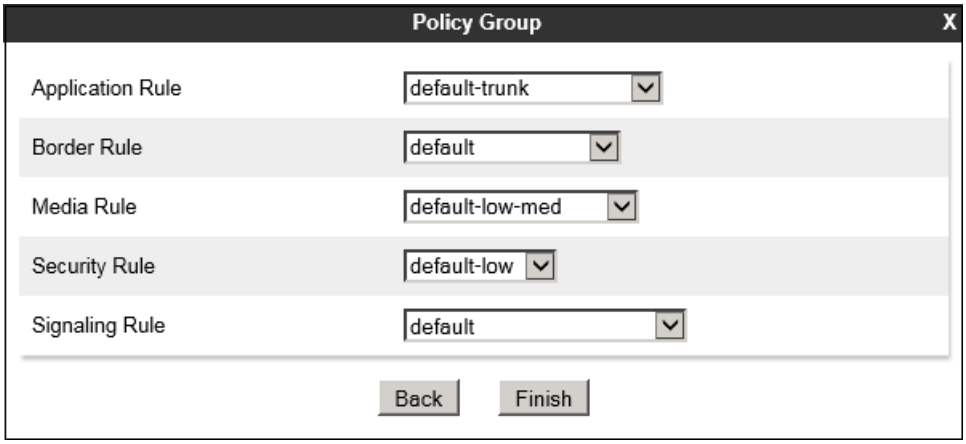
End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. In the reference configuration, the End Point Policy Groups used default sets of rules already pre-defined in the configuration. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule. Also note that even though the End Point Policy Groups for both the Enterprise and the Service Provider used the same set of rules, they were still separately defined, to allow for future changes to be made in one direction if needed, without affecting the other direction.

7.11.1. End Point Policy Group – Enterprise

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

Enter an appropriate name in the **Group Name** field. Click **Next**.

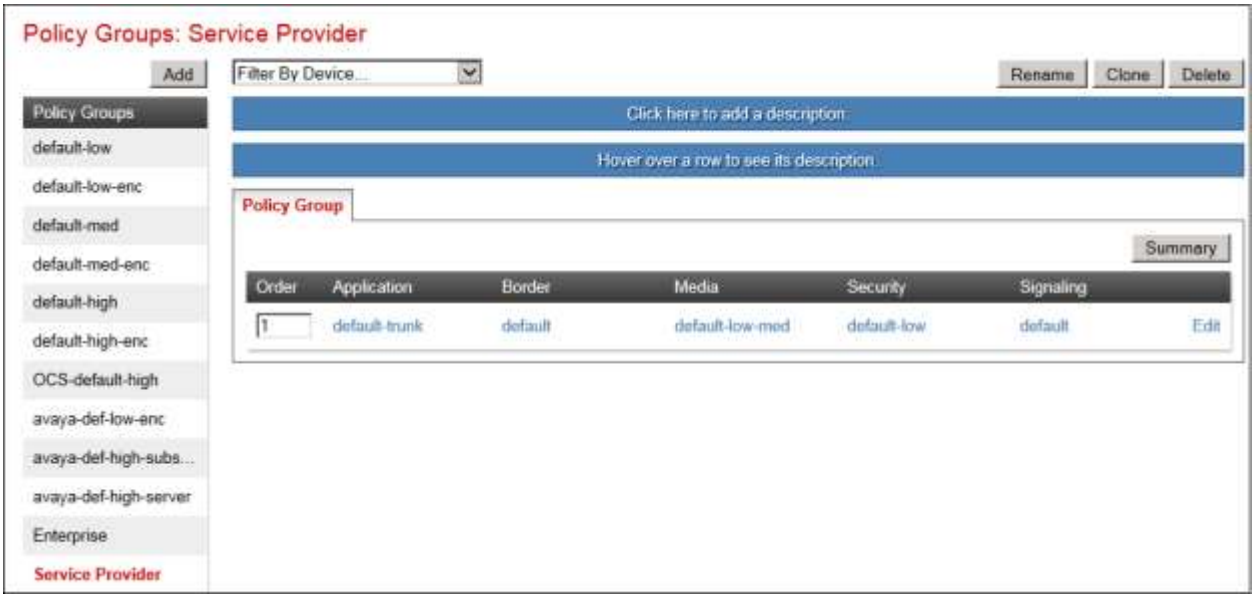
In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration. Click **Finish**.



7.11.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described. In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration.

The screen below shows the End Point Policy Group named ***Service Provider*** after the configuration was completed.

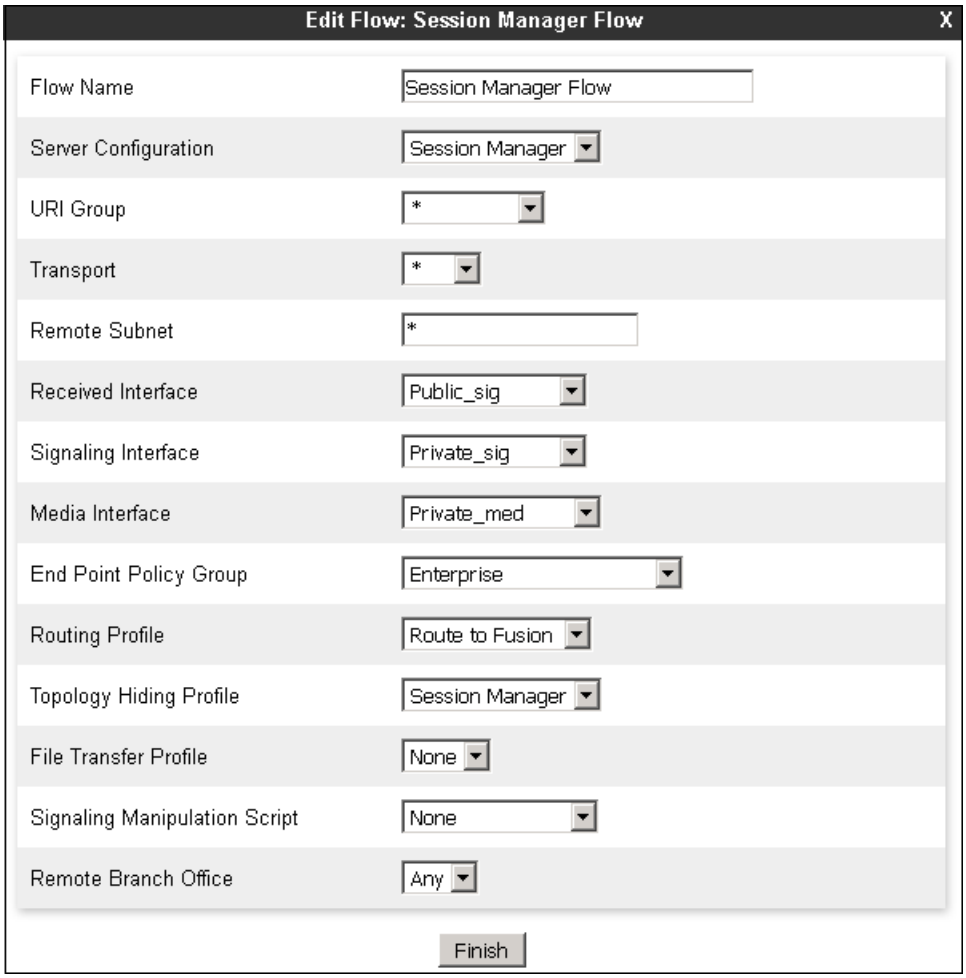


7.12. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

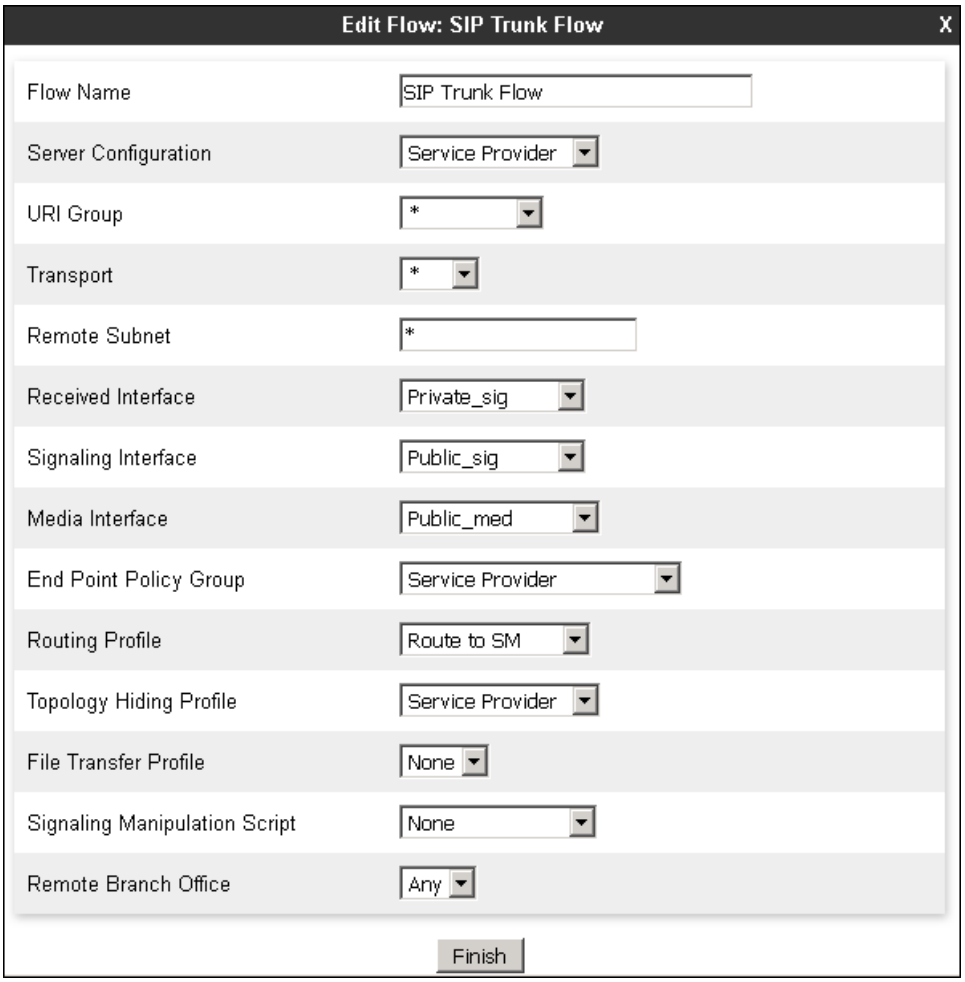
7.12.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named ***Session Manager Flow*** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.9.2**, which is the reverse route of the flow. Click **Finish**.



7.12.2. End Point Flow – Service Provider

A second Server Flow with the name ***SIP Trunk Flow*** was similarly created in the network direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Since the script created in **Section 7.7** was previously applied to the service provider's Server Configuration Profile in **Section 7.8.2**, it is not necessary to make a selection here. Click **Finish**.



8. Fusion Connect SIP Trunking Service Configuration

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

- SIP Trunk registration/Digest Authentication credentials (user name, password)
- Service Provider SIP domain.
- DID numbers.
- Supported codecs and order of preference.
- 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. General Verification Steps

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

9.2. Communication Manager Verification

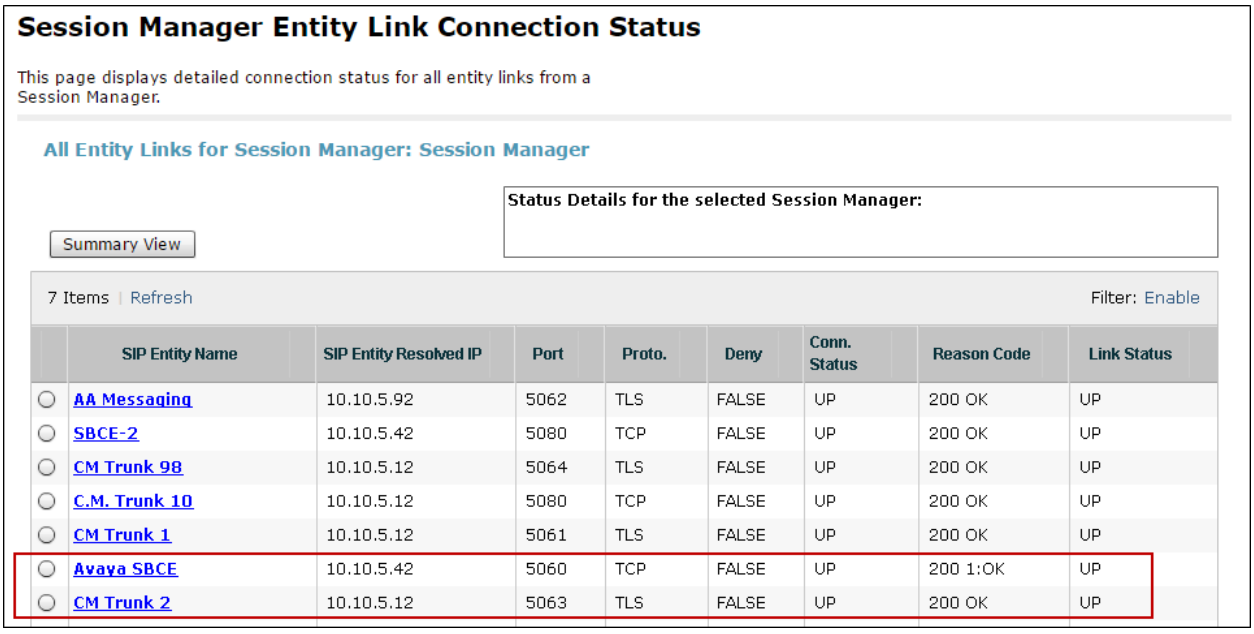
The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

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

9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Click the Session Manager instance (***Session Manager*** in the example below).

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.



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

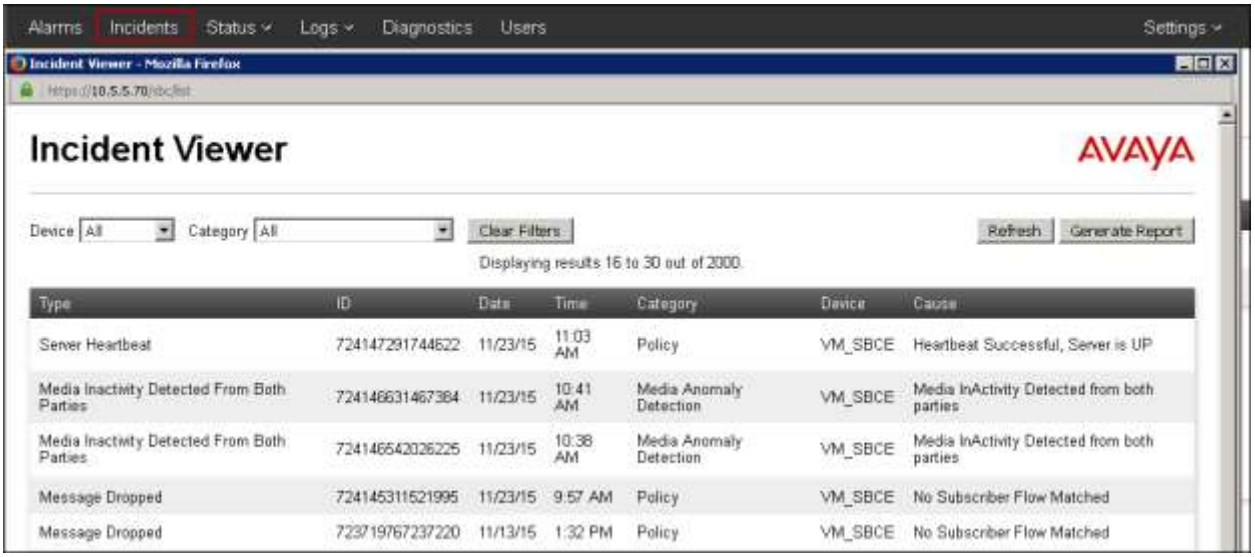
Elements → Session Manager →System Tools → Call Routing Test. Enter the requested data to run the test.

9.4. Avaya SBCE Verification

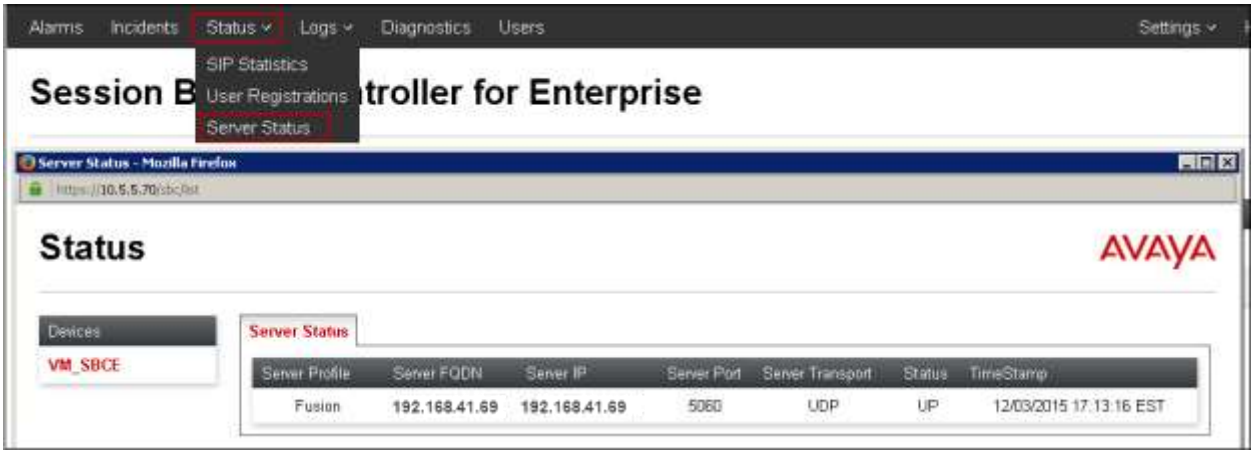
There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

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

Incidents : This screen provides detailed reports of anomalies, errors, policies violations, etc.



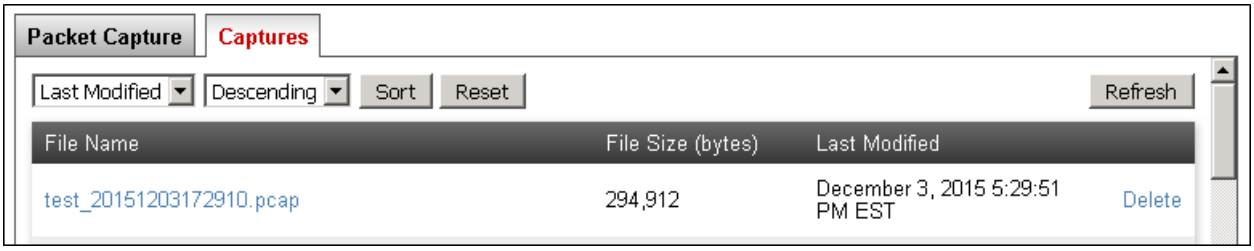
Status: Statistical and current status information. The **Server Status** screen below provides information about the condition of the connection to the Service Provider. This functionality requires Heartbeat to be enabled on the Server Configuration profile, as configured in **Section 7.8.2**.



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

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

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



10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to connect to the Fusion Connect SIP Trunking service, as shown in **Figure 1**.

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

11. 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 Virtualized Environment*, Release 7.0 August 2015.
[2] *Administering Avaya Aura® Communication Manager*, Release 7.0, August 2015, Document Number 03-300509.
[3] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, August 2015, Document Number 555-245-205.
[4] *Deploying Avaya Aura® System Manager*, Release 7.0, October 2015.
[5] *Deploying Avaya Aura® Session Manager on VMware®*, Release 7.0, August 2015.
[6] *Administering Avaya Aura® Session Manager*, Release 7.0, August 2015.
[7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
[8] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.0, August 2015.
[9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
[10] *Product Support Notice PSN004619u*, November 2015. https://downloads.avaya.com/css/P8/documents/101015817
[11] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7. August 2015.
[12] *Implementing and Administering Avaya Aura® Media Server*. Release 7.7. August 2015.
[13] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*. *White Paper*. August 2015.
[14] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[15] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

12. Appendix A: SigMa Script

The following is the Signaling Manipulation script used during the compliance test. The script can be copied here and pasted in the SigMa Editor screen shown in **Section 7.7** of the Avaya SBCE configuration. Note that the digit string to be inserted in the From header shown below will need to be replaced with the actual Main User (BTN) provided by Fusion for the specific customer SIP trunk implementation.

```
//Insert Username in the FROM header on outbound calls.

within session "ALL"
{
    act on request where %DIRECTION="OUTBOUND" and ENTRY_POINT="POST_ROUTING"
    {
      %fromuser = %HEADERS["From"][1].URI.USER;

      %HEADERS["From"][1].URI.USER = "2161234567";
    }
}

//The following script removes a=sendonly from the re-INVITE message sent by
//Communication Manager to Fusion when a call is placed on hold by an
//enterprise user. This is required in order for Music on Hold to be heard
//consistently by the PSTN user.

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

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

  }
}

//Remove gsid and epv parameters in outbound Contact header

within session "ALL"
{
   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
   {
      remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);

      remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
   }
}
```

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.