



# **Application Notes for Configuring Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 to support Telstra Enterprise SIP Trunking Service – Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service on an enterprise solution consisting of Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 to interoperate with Telstra Enterprise SIP Trunking service. These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

The Telstra Enterprise SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the Telstra 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.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	6
2.3.	Support .....	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated .....	11
5.	Configure Avaya Aura® Communication Manager.....	12
5.1.	Licensing and Capacity .....	12
5.2.	System Features.....	13
5.3.	IP Node Names.....	15
5.4.	Codecs .....	16
5.5.	IP Network Regions .....	18
5.6.	Signaling Group .....	19
5.7.	Trunk Group.....	21
5.8.	Calling Party Information.....	25
5.9.	Inbound Routing.....	26
5.10.	Outbound Routing .....	27
6.	Configure Avaya Aura® Session Manager .....	32
6.1.	System Manager Login and Navigation.....	33
6.2.	SIP Domain .....	35
6.3.	Locations .....	36
6.4.	Adaptations.....	39
6.5.	SIP Entities.....	41
6.6.	Entity Links.....	44
6.7.	Routing Policies .....	46
6.8.	Dial Patterns .....	47
7.	Configure Avaya Session Border Controller for Enterprise .....	51
7.1.	Device Management.....	54
7.2.	TLS Management.....	57
7.2.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise .....	57
7.2.2.	Server Profiles.....	59
7.2.3.	Client Profiles .....	61
7.3.	Network Management .....	63
7.4.	Media Interfaces .....	64
7.5.	Signaling Interfaces.....	66
7.6.	Server Interworking.....	68
7.6.1.	Server Interworking Profile – Enterprise.....	68
7.6.2.	Server Interworking Profile – Service Provider.....	72
7.7.	Signaling Manipulation.....	75
7.8.	Server Configuration.....	76
7.8.1.	Server Configuration Profile – Enterprise .....	76
7.8.2.	Server Configuration Profiles – Service Provider .....	78
7.9.	Routing.....	86

7.9.1.	Routing Profile – Enterprise .....	86
7.9.2.	Routing Profile – Service Provider .....	87
7.10.	Topology Hiding.....	90
7.10.1.	Topology Hiding Profile – Enterprise.....	90
7.10.2.	Topology Hiding Profile – Service Provider.....	92
7.11.	Domain Policies.....	93
7.11.1.	Application Rules.....	93
7.11.2.	Media Rules.....	95
7.11.3.	Signaling Rules .....	98
7.12.	End Point Policy Groups .....	99
7.12.1.	End Point Policy Group – Enterprise .....	99
7.12.2.	End Point Policy Group – Service Provider.....	100
7.13.	End Point Flows.....	101
7.13.1.	End Point Flows – SP to SM.....	102
7.13.2.	End Point Flow – SM_to_SP_Flow .....	104
8.	Telstra Enterprise SIP Trunking Service Configuration.....	105
9.	Verification and Troubleshooting.....	105
9.1.	General Verification Steps .....	105
9.2.	Communication Manager Verification.....	105
9.3.	Session Manager Verification .....	106
9.4.	Avaya SBCE Verification .....	109
10.	Conclusion .....	115
11.	References.....	115
12.	Appendix A – SigMa Scripts .....	116

# 1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Telstra network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 10.1 (Communication Manager), Avaya Aura® Session Manager 10.1 (Session Manager), Avaya Session Border Controller for Enterprise 10.1 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Telstra Enterprise 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.

The terms “Service Provider”, “Telstra” or “Telstra Enterprise” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

## 2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by Telstra. Incoming PSTN calls were terminated to the following endpoints: Avaya J129 IP Deskphones (SIP), Avaya J179 IP Deskphones (H.323), Avaya 9621G IP Deskphone (SIP), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Workplace client for Windows (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya Workplace client for Windows (SIP).
- Outgoing calls to the PSTN were routed via Telstra network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.711A, G.711MU and G.729A, Telstra preferred code order.
- No matching codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833:
  - Outbound call to PSTN application requiring DTMF (e.g., an IVR or voice mail system).
  - Inbound call from PSTN to Avaya CPE application requiring DTMF (e.g., Aura® Messaging, Avaya vector digit collection steps).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Routing inbound vector call to call center agent queues.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- Malicious Call Trace (\*57).
- Emergency (000).

**Note** – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes. Consult reference [9] in the **References** section for additional information on this topic.

Items that were not tested includes the following:

- Inbound toll-free calls, “0” calls (Operator), 0+10 digits calls (Operator Assisted) and local directory assistance calls were not tested.
- G.711 pass-through fax is supported but was not tested.
- T.38 fax is not currently supported by Telstra.

## 2.2. Test Results

Interoperability testing of the Telstra Enterprise 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:

- **Direct IP-IP Audio Connection (shuffling) disabled:** Calls from the PSTN being forwarded to another PSTN party were dropping with a BYE from Telstra a few seconds after the call was “shuffled” between IP endpoints by Communication Manager. The issue appears to be related to network delay when “shuffling” takes place. This is causing a delay in Telstra receiving an ACK message sent by Communication Manager in response to a 200 OK message sent by Telstra, resulting in the re-transmission of the 200 OK by Telstra and the ACK by Communication Manager. The call is dropped by Telstra with a BYE a few seconds after the re-transmission of messages take place. The Network delay could be attributed to the Avaya DevConnect lab used for the compliance test being in the U.S., with Telstra’s network being based in Australia. For this reason, direct IP-IP Audio Connection (shuffling) was disabled in Communication Manager (Refer to **Section 5.6**). Avaya recommends enabling “shuffling” in customer deployments to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway and Media Server.
- **URI in PAI Header should be set to the Pilot Number:** Telstra requires the URI in the PAI header to be the pilot number on all outbound calls from Communication Manager to the PSTN, this is part of the Telstra’s authentication requirement. This was accomplished by using a Signaling Manipulation script (SigMa) in the Avaya SBCE (Refer to **Sections 7.7 and 12**).
- **Outbound Calling Party Number (CPN) Blocking:** To support user privacy on outbound calls (calling party number blocking), when enabled by the user, Communication Manager sends “anonymous” as the calling number in the “From” header and includes “Privacy: id” in the INVITE message. Telstra did not respond to the INVITE message sent by Communication Manager with “anonymous” in the “From” header, resulting on the call failing. Telstra requires a valid DID number, or the pilot number, in the “From” header of SIP INVITE messages, as part of Telstra’s authentication requirement. A SigMa script was added to the Avaya SBCE to change “anonymous” in the “From” header of INVITE message sent to Telstra with pilot numbers provided by Telstra (Refer to **Sections 7.7 and 12**).

- **SIP OPTION Messages:** During the compliance test Telstra did not send SIP OPTION messages to Avaya, Session Manager did send SIP OPTION messages to Telstra, this was sufficient to keep the SIP trunk up in-service.
- **Removal of unwanted xml element information from the SDP in SIP messages sent to Telstra:** A Signaling Manipulation script (SigMa) on the Avaya SBCE was added to remove unwanted xml element information from the SDP in SIP messages the Avaya SBCE sent Telstra. Unwanted element information from the SDP in SIP messages were seen during certain calls.
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider's network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location (**Section 6.4**).

## 2.3. Support

For support of Telstra SIP Trunking Service visit the corporate Web page at:

<https://www.telstra.com.au/>

For technical support on the Avaya products described in these Application Notes visit

<http://support.avaya.com>

### 3. Reference Configuration

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

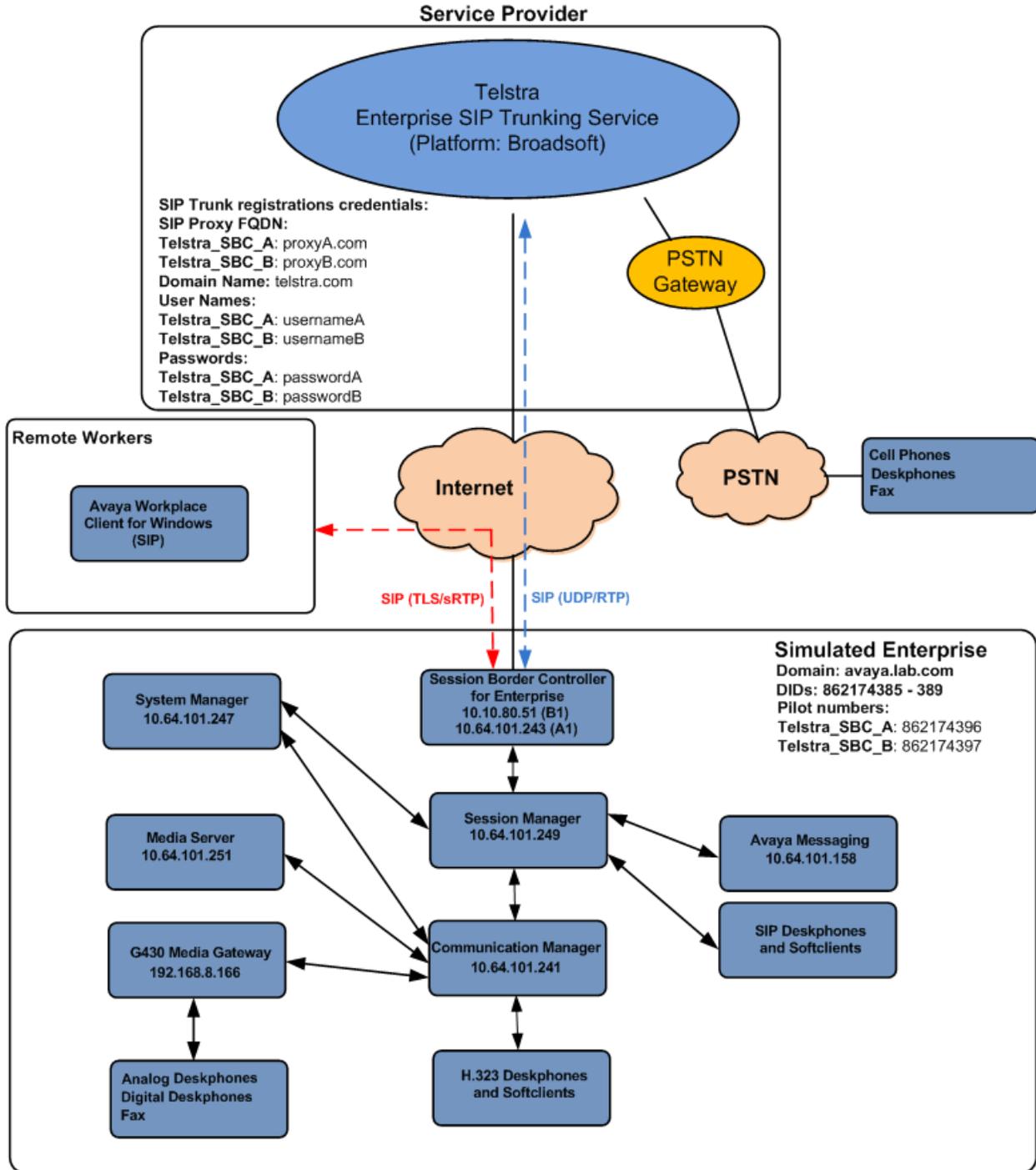


Figure 1: Avaya SIP Enterprise Solution connected to Telstra Enterprise SIP Trunking Service

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Messaging.
- Avaya Aura® Media Server.
- Avaya G430 Media Gateway.
- Avaya 9621G IP Deskphone (SIP).
- Avaya J179 IP Deskphones (H.323).
- Avaya J129 IP Deskphones (SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Workplace Client for Windows softphone (SIP).
- Avaya digital and analog telephones.
- Ventafax fax software.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya Workplace Client for Windows (SIP). Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult reference [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 public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

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

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Telstra network.

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

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

Avaya 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 Avaya Messaging is not directly related to the interoperability tests with the Telstra Enterprise SIP Trunking service, 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
<b>Avaya</b>	
Avaya Aura® Communication Manager	10.1.0.0 Service Pack 0.1 (01.0.974.0-27293)
Avaya Aura® Session Manager	10.1.0.0 (10.1.0.0.1010019)
Avaya Aura® System Manager	10.1.0.0 Build No. 10.1.0.0.537353 Software Update Rev. No. 10.1.0.0.0614119
Avaya Session Border Controller for Enterprise	ASBCE 10.1 10.1.0.0-32-21432
Avaya Messaging	10.8 Service Pack 1 (IXM-10.8.20.1406)
Avaya Aura® Media Server	8.0.2.218_2022.01.05
Avaya G430 Media Gateway	g430_sw_42.4.0
Avaya 129 IP Deskphones (SIP)	Version 4.0.7.0.7
Avaya J179 IP Deskphones (H.323)	Version 6.8.5.2.3
Avaya 9621G IP Deskphone (SIP)	Version 7.1.15.0.14
Avaya one-X® Communicator (H.323, SIP)	6.2.14.15-SP14-Patch7
Avaya Workplace Client for Windows (SIP)	3.27.0.64
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
<b>Telstra</b>	
BroadSoft	R23

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

**Note** – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.7.0) platforms. Consult the installation documentation on the **References** section for more information.

## 5. Configure Avaya Aura® Communication Manager

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

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

### 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **40000** licenses are available and **220** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

```
display system-parameters customer-options Page 2 of 12 ^
                                OPTIONAL FEATURES
IP PORT CAPACITIES                                USED
      Maximum Administered H.323 Trunks: 12000    0
      Maximum Concurrently Registered IP Stations: 18000    1
      Maximum Administered Remote Office Trunks: 12000    0
Max Concurrently Registered Remote Office Stations: 18000    0
      Maximum Concurrently Registered IP eCons: 414    0
      Max Concur Reg Unauthenticated H.323 Stations: 100    0
      Maximum Video Capable Stations: 41000    0
      Maximum Video Capable IP Softphones: 18000    6
      Maximum Administered SIP Trunks: 40000    220
Max Administered Ad-hoc Video Conferencing Ports: 24000    0
      Max Number of DS1 Boards with Echo Cancellation: 999    0

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

## 5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow 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**.

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

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

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

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

```
display system-parameters features Page 9 of 19 ^
      FEATURE-RELATED SYSTEM PARAMETERS
CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable
DISPLAY TEXT
                                     Identity When Bridging: principal
                                     User Guidance Display? n
Extension only label for Team button on 96xx H.323 terminals? n
INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code:
      International Access Code:
SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n
CALLER ID ON CALL WAITING PARAMETERS
  Caller ID on Call Waiting Delay Timer (msec): 200
```



## 5.4. Codecs

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

```
change ip-codec-set 2                                     Page 1 of 2 ^
                                                         IP MEDIA PARAMETERS
Codec Set: 2
Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size (ms)
1: G.711A      n            2           20
2: G.711MU    n            2           20
3: G.729A    n            2           20
4: _____  -            -
5: _____  -            -
6: _____  -            -
7: _____  -            -

Media Encryption                                     Encrypted SRTP: best-effort
1: l-srtp-aescml28-hmac80
2: none
3: _____
4: _____
5: _____
```

On **Page 2**, set the **Fax Mode** to **off** (Refer to **Section 2.1**).

```
change ip-codec-set 2 Page 2 of 2 ^
IP MEDIA PARAMETERS
Allow Direct-IP Multimedia? n

Mode                               Redun-   Packet
FAX                                 dancy    Size (ms)
Modem                               0
TDD/TTY                             3
H.323 Clear-channel n           0
SIP 64K Data                    n           0                               20

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

## 5.5. IP Network Regions

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

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.lab.com** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes**, the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed (Refer to **Section 2.2**).
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

```
change ip-network-region 2                                     Page 1 of 20 ^
                                                                IP NETWORK REGION
Region: 2              NR Group: 2
Location: 1            Authoritative Domain: avaya.lab.com
Name: SP Region        Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2           Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 3349
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y      RSVP Enabled? n
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	
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr	Regions	Dyn CAC	A R	G L			
1	2	y	NoLimit				n					t
2	2											c
3												e
4												t
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												

## 5.6. Signaling Group

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

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

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

- Prepend '+' to **Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to **y**.
- Remove '+' from **Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to **n**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5071**.
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **n** (Refer to **Section 2.2**).
- Default values may be used for all other fields.

```

change signaling-group 2                                     Page 1 of 2 ^
                                     SIGNALING GROUP
Group Number: 2                Group Type: sip
IMS Enabled? n                 Transport Method: tls
  Q-SIP? n
  IP Video? n
Peer Detection Enabled? y Peer Server: SM                Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                Far-end Node Name: SM
Near-end Listen Port: 5071                Far-end Listen Port: 5071
                                     Far-end Network Region: 2

Far-end Domain: avaya.lab.com
                                     Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
  DTMF over IP: rtp-payload                Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                IP Audio Hairpinning? n
  Enable Layer 3 Test? n
                                     Alternate Route Timer(sec): c

```

## 5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
change trunk-group 2                                     Page 1 of 4 ^
                                     TRUNK GROUP
Group Number: 2                Group Type: sip          CDR Reports: y
Group Name: Service Provider   COR: 1          TN: 1          TAC: 602
Direction: two-way           Outgoing Display? n
Dial Access? n                Night Service: _____
Queue Length: 0
Service Type: public-ntwrk    Auth Code? n
                               Member Assignment Method: auto
                               Signaling Group: 2
                               Number of Members: 10
```

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

```
change trunk-group 2                                     Page 2 of 4 ^
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
  SCCAN? n                               Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
  XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n
Caller ID for Service Link Call to H.323 1xC: station-extension
```

On Page 3:

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

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

  Suppress # Outpulsing? n   Numbering Format: public
                                                         UII Treatment: service-provider

                                                         Replace Restricted Numbers? y
                                                         Replace Unavailable Numbers? y

                                                         Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y
```

On Page 4:

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

```
change trunk-group 2                                     Page 4 of 4 ^
PROTOCOL VARIATIONS
Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
Send Transferring Party Information? n
Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? n
Send Diversion Header? y
Support Request History? n
Telephone Event Payload Type: 101

Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? n
Resend Display UPDATE Once on Receipt of 481 Response? n
Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
Accept Redirect to Blank User Destination? n
Enable Q-SIP? n
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
Request URI Contents: may-have-extra-digits
```

## 5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the 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, four DID numbers assigned by the service provider are shown. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions. The country code for Australia (61) was added preceding the DID numbers, required by Telstra.

```
change public-unknown-numbering 2 Page 1 of 2 ^
NUMBERING - PUBLIC/UNKNOWN FORMAT
Ext Ext      Trk      CPN      Total
Len Code     Grp(s)   Prefix   CPN
-----
4 3          _____  _____  4
4 5          _____  _____  4
4 3037       2        61862174388  11
4 3042       2        61862174386  11
4 3044       2        61862174387  11
4 3501       2        61862174389  11
-----
Note: If an entry applies to
a SIP connection to Avaya
Aura(R) Session Manager,
the resulting number must
be a complete E.164 number.
Communication Manager
automatically inserts
a '+' digit in this case.
```



## 5.10.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			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	13	udp						
1	4	dac						
2	4	ext						
3	4	ext						
4	4	udp						
5	4	ext						
6	3	dac						
7	4	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	2	dac						

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

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

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The examples 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 61
```

Page 1 of 2

ARS DIGIT ANALYSIS TABLE  
Location: all                      Percent Full: 1

Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Reqd
	Min	Max				
61	11	11	2	hnpa		n
611	3	3	2	svcl		n
61293	11	11	2	hnpa		n
63	8	8	2	hnpa		n
631	10	10	2	hnpa		n
6501	4	4	1	svcl		n
7	10	10	2	hnpa		n
8	10	10	2	hnpa		n
808	10	10	2	hnpa		n
809	10	10	2	hnpa		n
811	3	3	1	svcl		n
828	7	7	2	hnpa		n
868	10	10	2	hnpa		n
9	10	10	2	hnpa		n
911	3	3	2	svcl		n

```
change ars analysis 0
```

Page 1 of 2

ARS DIGIT ANALYSIS TABLE  
Location: all                      Percent Full: 1

Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Reqd
	Min	Max				
0	1	11	2	op		n
0	13	13	1	hnpa		n
00	2	2	deny	op		n
001	13	18	2	intl		n
01	12	12	2	natl		n
011	10	18	2	intl		n
040	3	3	2	svcl		n
045	13	13	2	natl		n
101xxxx0	8	8	deny	op		n
101xxxx0	18	18	deny	op		n
101xxxx01	16	24	deny	iop		n
101xxxx011	17	25	deny	intl		n
101xxxx1	18	18	deny	fnpa		n
10xxx0	6	6	deny	op		n
10xxx0	16	16	deny	op		n



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

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) preceding the number dialed (+61 plus dialed number) to conform with Telstra's E.164 number format requirement.
- **Numbering Format:** Set to **pub-unk**. All calls using this route pattern will use the public numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

```

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

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

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

**Note** - 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

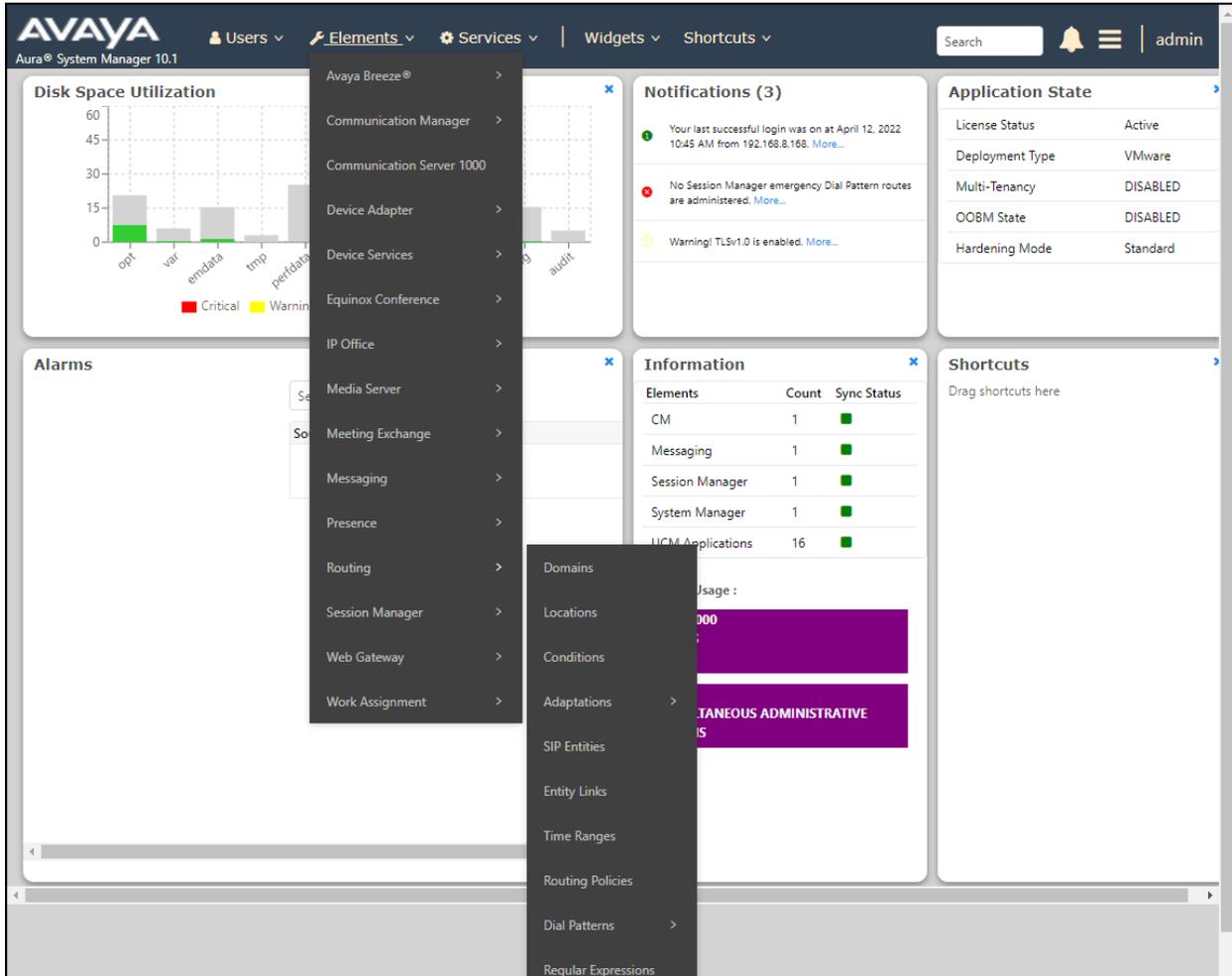
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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; under **elements** select **Routing → Domains**.



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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu options (Elements, Services, Widgets, Shortcuts). A search bar and a user profile (admin) are also visible. The main content area is titled "Domain Management" and features a table with one entry: "avaya.lab.com" of type "sip" with the note "HG V-Domain". The left sidebar shows a navigation tree with "Routing" selected, and "Domains" highlighted. The table has columns for Name, Type, and Notes, and includes action buttons like New, Edit, Delete, Duplicate, and More Actions.

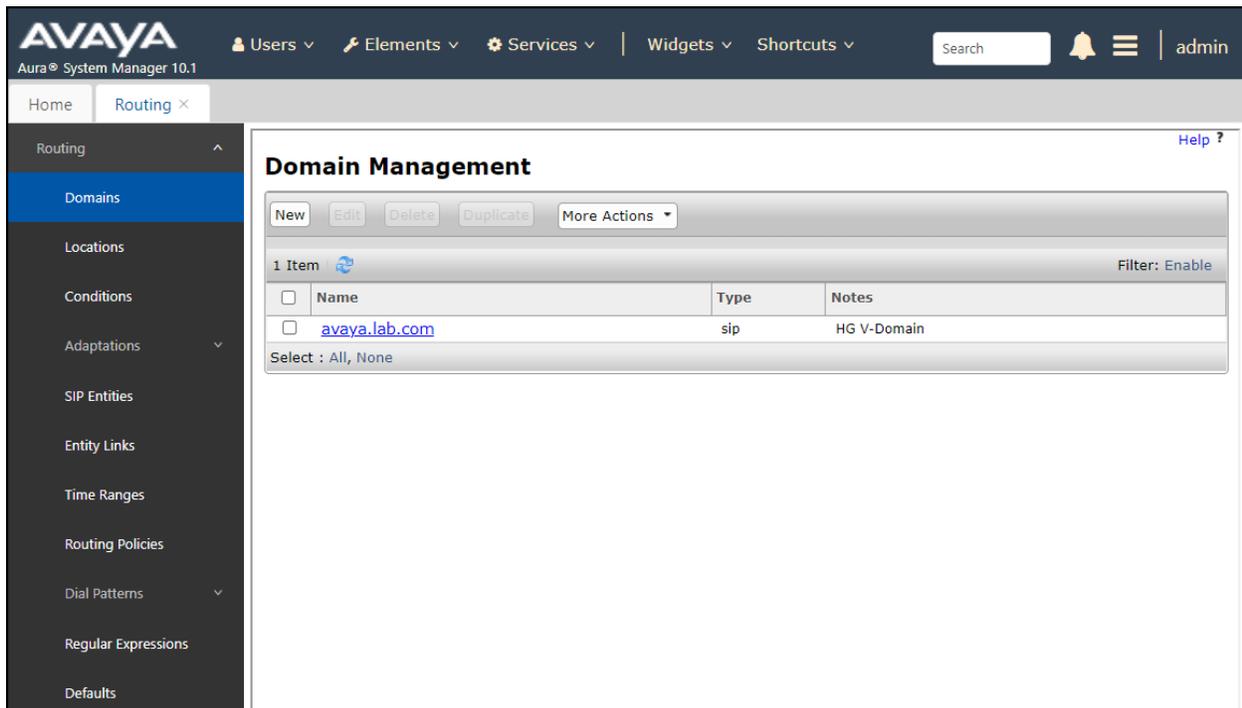
Name	Type	Notes
<a href="#">avaya.lab.com</a>	sip	HG V-Domain

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

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).
- Click **Commit** to save (not shown).

The screen below shows the entry for the enterprise domain.



The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). A search bar and a user profile (admin) are also visible. The left-hand navigation pane is expanded to show the 'Routing' section, with 'Domains' selected. The main content area is titled 'Domain Management' and features a table with one entry. The table has columns for Name, Type, and Notes. The entry is 'avaya.lab.com' with Type 'sip' and Notes 'HG V-Domain'. There are also buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions' at the top of the table.

Name	Type	Notes
<a href="#">avaya.lab.com</a>	sip	HG V-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).
- Click **Commit** to save.

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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 10.1', and menu items for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'Locations' highlighted. The main content area is titled 'Location Details' and contains the following sections:

- General**:
  - Name:** Session Manager
  - Notes:** VMware Session Manager
- Dial Plan Transparency in Survivable Mode**:
  - Enabled:**
  - Listed Directory Number:** [Empty text box]
  - Associated CM SIP Entity:** [Empty text box]
- Overall Managed Bandwidth**:
  - Managed Bandwidth Units:** Kbit/sec
  - Total Bandwidth:** [Empty text box]
  - Multimedia Bandwidth:** [Empty text box]
  - Audio Calls Can Take Multimedia Bandwidth:**

Buttons for 'Commit' and 'Cancel' are located in the top right corner of the form area.

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 screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). A search bar and a user profile (admin) are also visible. The left sidebar shows a navigation tree with 'Locations' selected. The main content area is titled 'Location Details' and contains the following sections:

- General**:
  - Name**: Communication Manager
  - Notes**: VMware Communication Manager
- Dial Plan Transparency in Survivable Mode**:
  - Enabled**:
  - Listed Directory Number**:
  - Associated CM SIP Entity**:
- Overall Managed Bandwidth**:
  - Managed Bandwidth Units**: Kbit/sec
  - Total Bandwidth**:
  - Multimedia Bandwidth**:
  - Audio Calls Can Take Multimedia Bandwidth**:

Buttons for 'Commit' and 'Cancel' are located in the top right corner of the form area.

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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, a search box, a notification bell, and the user 'admin'. The left sidebar shows a navigation tree with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Location Details' and contains the following sections:

- General**:
  - Name**: Avaya SBCE
  - Notes**: VMware Avaya SBCE
- Dial Plan Transparency in Survivable Mode**:
  - Enabled**:
  - Listed Directory Number**: [Empty text box]
  - Associated CM SIP Entity**: [Empty text box]
- Overall Managed Bandwidth**:
  - Managed Bandwidth Units**: Kbit/sec
  - Total Bandwidth**: [Empty text box]
  - Multimedia Bandwidth**: [Empty text box]
  - Audio Calls Can Take Multimedia Bandwidth**:

Buttons for 'Commit' and 'Cancel' are located in the top right corner of the configuration area.

## 6.4. Adaptations

To improve interoperability with third party elements, Session Manager 10.1 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named **CM\_Outbound\_Header\_Removal** was created to block the headers listed below before they were forwarded to the Avaya SBCE. 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, as follows:

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

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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu options (Elements, Services, Widgets, Shortcuts). A search bar and a user profile icon (admin) are also present. The left sidebar shows a navigation tree with 'Routing' selected, and sub-items like Domains, Locations, Conditions, Adaptations, Regular Expressions, Device Mappings, SIP Entities, Entity Links, and Time Ranges. The main content area is titled 'Adaptation Details' and contains the following configuration fields:

- Adaptation Name:** CM\_Outbound\_Header\_Removal
- Notes:** (empty text field)
- Module Name:** DigitConversionAdapter (dropdown menu)
- Type:** digit (text field)
- State:** enabled (dropdown menu)
- Module Parameter Type:** Name-Value Parameter (dropdown menu)

Below these fields is a table for defining module parameters:

Add		Remove	
<input type="checkbox"/>	Name		Value
<input type="checkbox"/>	eRHdrs		"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View"

At the bottom of the table, there is a 'Select' dropdown menu with options for 'All' and 'None'. Below the table is an 'Egress URI Parameters' text field.

## 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 (see **Figure 1**).
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** (or **Other**) for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

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

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information, and various menu options like Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled "SIP Entity Details" and is divided into two sections: "General" and "Monitoring".

**General Section:**

- Name:** Session Manager
- IP Address:** 10.64.101.249
- SIP FQDN:** (empty field)
- Type:** Session Manager (dropdown menu)
- Notes:** VMware Session Manager
- Location:** Session Manager (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/New\_York (dropdown menu)
- Minimum TLS Version:** Use Global Setting (dropdown menu)
- Credential name:** (empty text field)

**Monitoring Section:**

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)
- CRLF Keep Alive Monitoring:** CRLF Monitoring Disabled (dropdown menu)

Buttons for "Commit" and "Cancel" are visible at the top right of the form area.

The following screen shows the addition of the **Communication Manager Trunk 2** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**. For **Type** Select **CM** for Communication Manager. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**. Select the **Time Zone**. Click **Commit** to save.

**AVAYA** Aura System Manager 10.1

Users Elements Services Widgets Shortcuts Search admin

Home Routing

Routing Domains Locations Conditions Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults

### SIP Entity Details

Commit Cancel Help ?

#### General

\* Name: Communication Manager Trunk 2

\* FQDN or IP Address: 10.64.101.241

Type: CM

Notes: Used for SP Testing

Adaptation:

Location: Communication Manager

Time Zone: America/New\_York

\* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

Securable:

Call Detail Recording: none

#### Loop Detection

Loop Detection Mode: Off

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

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- For **Type** Select **SIP Trunk**.
- On the **Adaptation** field, the adaptation module **CM\_Outbound\_Header\_Removal** previously defined in **Section 6.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- Select the **Time Zone**.
- Click **Commit** to save.

**AVAYA** Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing ×

Routing Domains Locations Conditions Adaptations **SIP Entities** Entity Links Time Ranges Routing Policies Dial Patterns ▾ Regular Expressions Defaults

### SIP Entity Details

Commit Cancel Help ?

**General**

\* Name: Avaya SBCE

\* FQDN or IP Address: 10.64.101.243

Type: SIP Trunk ▾

Notes: VMware Avaya SBCE

Adaptation: CM\_Outbound\_Header\_Removal ▾

Location: Avaya SBCE ▾

Time Zone: America/New\_York ▾

\* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable:

Call Detail Recording: none ▾

**Loop Detection**

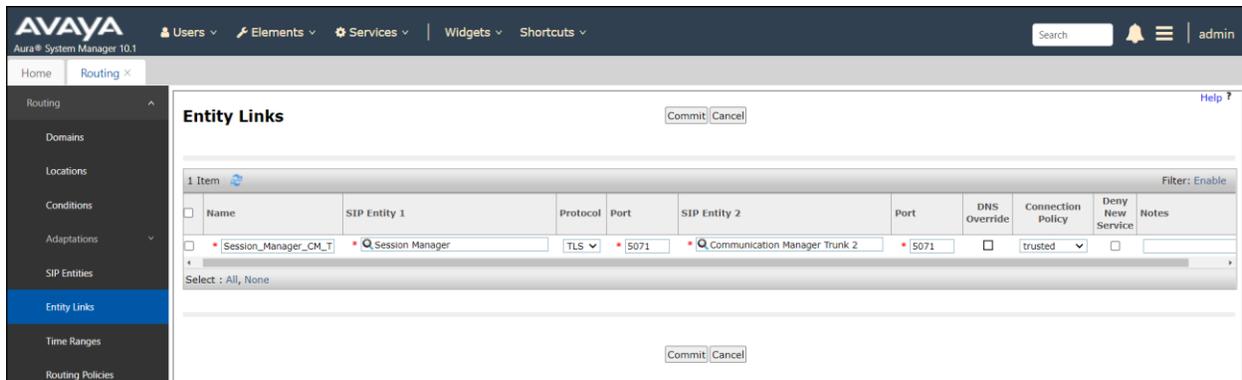
Loop Detection Mode: Off ▾

## 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; an entity link to Communication Manager for use only by service provider traffic and an entity link 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 (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link (**Section 5.6**).
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2:** Select the name of the other system from the drop-down menu (**Section 6.5**).
- **Port:** Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

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



The screenshot shows the Avaya Aura System Manager 10.1 interface. The left navigation pane is open to 'Entity Links'. The main content area shows a table with one row of configuration data. The table has the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row contains the following values: Name: Session\_Manager\_CM\_T, SIP Entity 1: Session Manager, Protocol: TLS, Port: 5071, SIP Entity 2: Communication Manager Trunk 2, Port: 5071, DNS Override: (unchecked), Connection Policy: trusted, Deny New Service: (unchecked), and Notes: (empty). There are 'Commit' and 'Cancel' buttons at the top and bottom of the table.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
Session_Manager_CM_T	Session Manager	TLS	5071	Communication Manager Trunk 2	5071	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

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

The screenshot shows the Avaya System Manager 10.1 interface. The left sidebar contains navigation options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), and Time Ranges. The main content area is titled "Entity Links" and contains a table with one item. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The row shows a link between "Session Manager\_Avaya" and "Avaya SBCE" using "TLS" protocol on port "5061".

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	Session Manager_Avaya	TLS	5061	Avaya SBCE	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

## 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 with the Avaya SBCE as the destination. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

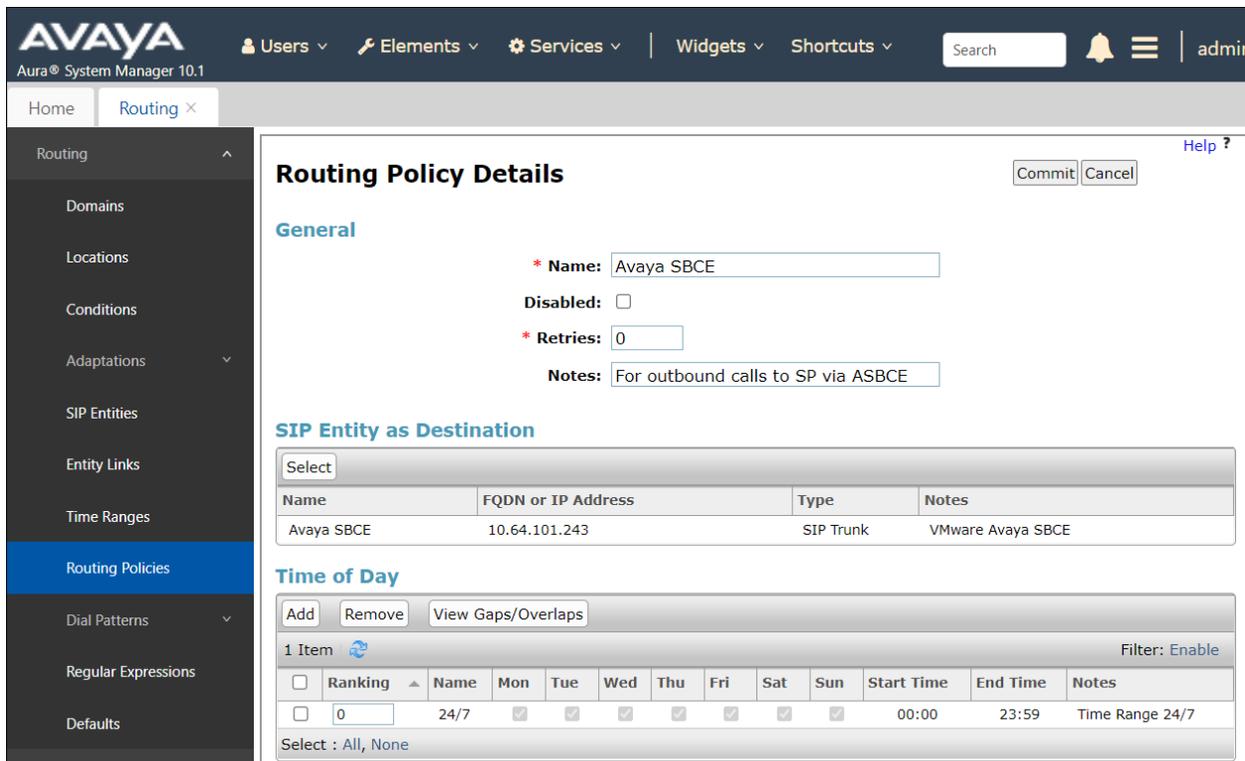
The following screens show the Routing Policies for Communication Manager and the Avaya SBCE.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', 'Shortcuts', a search bar, and a user profile 'admin'. The left sidebar shows a navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains the following sections:

- General:**
  - Name:** To CM Trunk 2
  - Disabled:**
  - Retries:** 0
  - Notes:** For inbound calls to CM via Trunk 2
- SIP Entity as Destination:**

Name	FQDN or IP Address	Type	Notes
Communication Manager Trunk 2	10.64.101.241	CM	Used for SP Testing
- Time of Day:**

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7						



## 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 (**Section 6.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 6.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound calls from the PSTN to Communication Manager. In the examples, calls to 9-digit numbers starting with **8621** arriving from location **Avaya SBCE**, used route policy **To CM Trunk 2** to Communication Manager. The SIP Domain was set to **avaya.lab.com**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). A search bar and a user profile (admin) are also visible. The main content area is titled "Dial Pattern Details" and contains the following information:

- General**
  - \* Pattern: 8621
  - \* Min: 4
  - \* Max: 36
  - Emergency Call:
  - SIP Domain: avaya.lab.com
  - Notes:
- Originating Locations, Origination Dial Pattern Sets, and Routing Policies**
  - Buttons: Add, Remove
  - 1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Avaya SBCE	VMware Avaya SBCE			To CM Trunk 2	0	<input type="checkbox"/>	Communication Manager Trunk 2	For inbound calls to CM via Trunk 2

  - Select : All, None

The example in the screen below shows the 11-digits dialed numbers for outbound calls from Communication Manager to the PSTN, beginning with +, arriving from the **Communication Manager** location, will use route policy **Avaya SBCE**, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP trunk. The SIP Domain was set to **avaya.lab.com**.

**Note** - Telstra requires the numbers in E.164 format (+61 plus dialed number). Communication Manager was configured to insert a plus (+) preceding the number dialed to convert it to E.164 format before sending the INVITE message to Session Manager (Refer to **Section 5.10**).

The screenshot shows the 'Dial Pattern Details' configuration page in Avaya Aura System Manager 10.1. The 'General' section contains the following fields:

- Pattern:** +
- Min:** 1
- Max:** 36
- Emergency Call:**
- SIP Domain:** avaya.lab.com
- Notes:** (empty)

The 'Originating Locations, Origination Dial Pattern Sets, and Routing Policies' section shows a table with 1 item:

Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> Communication Manager	VMware Communication Manager			Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE

The example in the screen below shows the \*57 dialed number to initiate malicious call trace.

The screenshot shows the 'Dial Pattern Details' configuration page in Avaya Aura System Manager 10.1. The 'General' section contains the following fields:

- Pattern:** \*57
- Min:** 3
- Max:** 36
- Emergency Call:**
- SIP Domain:** avaya.lab.com
- Notes:** (empty)

The 'Originating Locations, Origination Dial Pattern Sets, and Routing Policies' section shows a table with 1 item:

Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> Communication Manager	VMware Communication Manager			Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE

The example in the screen below shows the dialed number starting with “0”, this dial pattern is used when dialing “000” for emergency.

The screenshot displays the 'Dial Pattern Details' configuration page in Avaya Aura System Manager 10.1. The interface includes a top navigation bar with 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, along with a search bar and a user profile 'admin'. A left sidebar shows a navigation tree with 'Routing' selected, containing sub-items like Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions.

The main content area is titled 'Dial Pattern Details' and features a 'Commit' and 'Cancel' button. It is divided into several sections:

- General:** Contains fields for 'Pattern' (set to '0'), 'Min' (set to '1'), and 'Max' (set to '12'). There is an 'Emergency Call' checkbox (unchecked) and a 'SIP Domain' dropdown menu (set to 'avaya.lab.com'). A 'Notes' field is also present.
- Originating Locations, Origination Dial Pattern Sets, and Routing Policies:** This section includes 'Add' and 'Remove' buttons and shows '1 Item'. Below is a table with the following data:
 

Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> Communication Manager	VMware Communication Manager			Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE
- Denied Originating Locations and Origination Dial Pattern Sets:** This section includes 'Add' and 'Remove' buttons and shows '0 Items'.

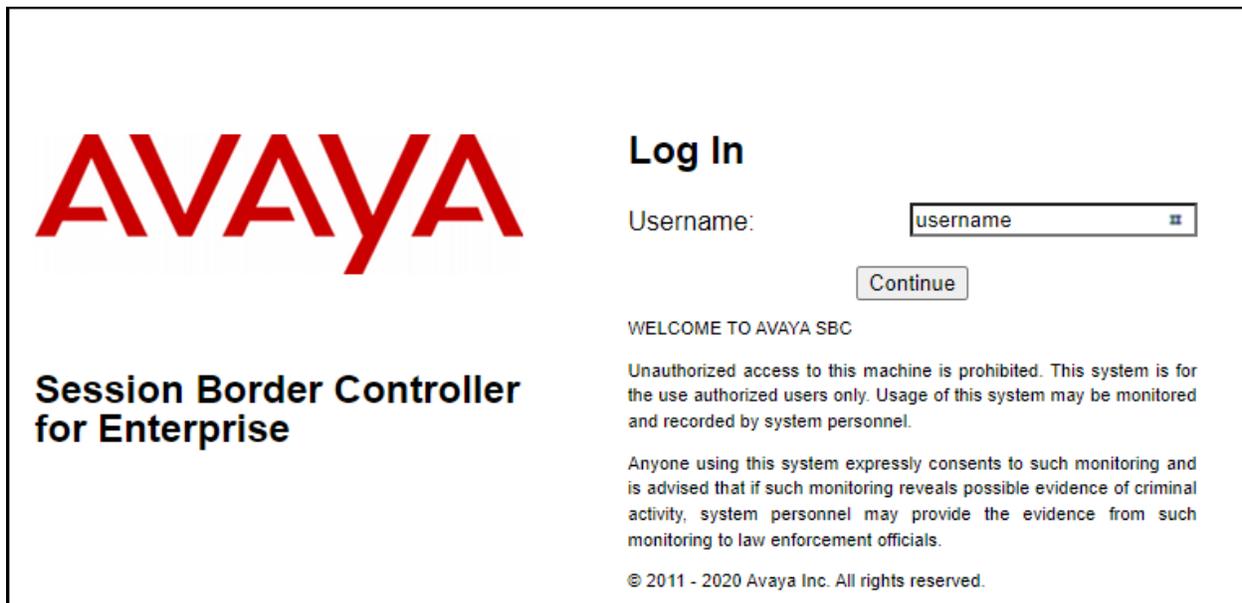
Repeat the above procedures as needed to define additional dial patterns. Similar Dial Patterns are required for special numbers arriving at Session Manager from Communication Manager that are not in E.164 format (numbers from Communication Manager that **do not** begin with +).

## 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 **References** section.

**Note** – Information, such as FQDNs, domain name, trunk registration credentials, public IP addresses, etc. haven been masked for security reasons. Telstra will provide valid information to the customer during the signup process.

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.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field containing the placeholder text "username". Below the input field is a "Continue" button. Underneath the button, the text "WELCOME TO AVAYA SBC" is displayed. Below that, a warning message states: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." A second paragraph follows: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2020 Avaya Inc. All rights reserved." is visible.

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

The screenshot displays the Avaya EMS dashboard for the device 'Avaya\_SBCE'. The top navigation bar includes 'Device: EMS', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'EMS' and 'Avaya\_SBCE' in a dropdown menu, followed by 'er Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar contains the 'EMS Dashboard' menu with options: Software Management, Device Management, System Administration, Templates, Backup/Restore, and Monitoring & Logging.

The main dashboard area is titled 'Dashboard' and features several sections:

- Information:** A table with system details.
 

System Time	10:32:53 AM EDT	<a href="#">Refresh</a>
Version	10.1.0.0-32-21432	
GUI Version	10.1.0.0-21432	
Build Date	Thu Dec 02 21:33:10 UTC 2021	
License State	<span style="color: green;">OK</span>	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/03/2022 10:22:18 EDT	
Failed Login Attempts	0	
- Installed Devices:** A list showing 'EMS' and 'Avaya\_SBCE'.
- Active Alarms (past 24 hours):** A section indicating 'None found.'
- Incidents (past 24 hours):** A section showing 'Avaya\_SBCE: Registration Successful, Server is UP'.

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.

The screenshot shows the Avaya SBCE web interface. At the top, there is a navigation bar with the following items: Device: Avaya\_SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo.

The left navigation pane is titled "EMS Dashboard" and includes the following menu items: Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled "Dashboard" and contains several sections:

- Information**: A table showing system details.
 

System Time	10:42:08 AM EDT	<a href="#">Refresh</a>
Version	10.1.0.0-32-21432	
GUI Version	10.1.0.0-21432	
Build Date	Thu Dec 02 21:33:10 UTC 2021	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/03/2022 10:22:18 EDT	
Failed Login Attempts	0	
- Installed Devices**: A list showing "EMS" and "Avaya\_SBCE".
- Active Alarms (past 24 hours)**: None found.
- Incidents (past 24 hours)**: Avaya\_SBCE: Registration Successful, Server is UP.

## 7.1. Device Management

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left navigation pane lists various management options, with 'Device Management' highlighted. The main content area is titled 'Device Management' and contains several tabs: 'Devices', 'Updates', 'Licensing', 'Key Bundles', and 'License Compliance'. The 'Devices' tab is active, showing a table with the following data:

Device Name	Management IP	Version	Status						
Avaya_SBCE	[Blurred]	10.1.0.0-32-21432	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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. Note that **DNS configuration** is required for this solution.

System Information: Avaya\_SBCE X

**General Configuration**

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

**Device Configuration**

HA Mode	No
Two Bypass Mode	No

**Dynamic License Allocation**

	Min License Allocation	Max License Allocation
Standard Sessions	100	200
Advanced Sessions	100	200
Scopia Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	100	200
AMR	<input type="checkbox"/>	
Premium Sessions	0	0
CLID	---	
Encryption Available: Yes	<input checked="" type="checkbox"/>	

**Network Configuration**

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.101.243	10.64.101.243	255.255.255.0	10.64.101.1	A1
				A1
				A1
				B1
				B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

**DNS Configuration**

Primary DNS	75.75.75.75
Secondary DNS	75.75.76.76
DNS Location	DMZ
DNS Client IP	10.10.80.51

**Management IP(s)**

IP #1 (IPv4)	
--------------	--

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

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

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

## 7.2. TLS Management

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

In the reference configuration, TLS transport is used for the communication between Session Manager and Avaya SBCE. The following procedures show how to create the client and server profiles to support the TLS connection.

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

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



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

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. At the top, a navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header features the 'Session Border Controller for Enterprise' title and the 'AVAYA' logo. A left-hand navigation menu lists various management options, with 'TLS Management' and 'Certificates' highlighted. The main content area, titled 'Certificates', contains two sections: 'Installed Certificates' and 'Installed CA Certificates'. Each section lists certificates with 'View' and 'Delete' links. The 'Installed Certificates' section includes 'sbclInternal.pem'. The 'Installed CA Certificates' section includes 'default.pem'. 'Install' and 'Generate CSR' buttons are visible in the top right of the main content area.

Section	Certificate Name	View	Delete
Installed Certificates	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	sbclInternal.pem	<a href="#">View</a>	<a href="#">Delete</a>
Installed CA Certificates	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	[blurred]	<a href="#">View</a>	<a href="#">Delete</a>
	default.pem	<a href="#">View</a>	<a href="#">Delete</a>

## 7.2.2. Server Profiles

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

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

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

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

**TLS Profile**

Profile Name: sbclInternal

Certificate: sbclInternal.pem

SNI Options: None

SNI Group: None

**Certificate Verification**

Peer Verification: None

Peer Certificate Authorities: AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust\_g2\_ca.cer, DigiCertGlobalRootCA.cer

Peer Certificate Revocation Lists:

Verification Depth: 0

Next

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Certificates', 'Client Profiles', 'Server Profiles', 'SNI Group', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Server Profiles' section is highlighted.

The main content area is titled 'Server Profiles: sbcInternal' and includes an 'Add' button. Below this is a list of server profiles: 'Outside\_Server', 'Inside\_Server', 'Clearcom\_Outside\_Server', 'IPO\_Inside\_Server', 'Remote\_Worker\_Dec17', and 'sbcInternal' (which is selected and highlighted in red). A 'Delete' button is located at the top right of the profile list.

The configuration details for the selected 'sbcInternal' profile are shown in a form with the following sections:

- Server Profile**: A blue bar with the text 'Click here to add a description'.
- TLS Profile**:
  - Profile Name: sbcInternal
  - Certificate: sbcInternal.pem
  - SNI Options: None
- Certificate Verification**:
  - Peer Verification: None
  - Extended Hostname Verification:
- Renegotiation Parameters**:
  - Renegotiation Time: 0
  - Renegotiation Byte Count: 0
- Handshake Options**:
  - Version:  TLS 1.2  TLS 1.1  TLS 1.0
  - Ciphers:  Default  FIPS  Custom
  - Value: HIGH:IDH:1ADH:1MD5:1aNULL:1eNULL:@STRENGTH

An 'Edit' button is located at the bottom of the configuration form.

### 7.2.3. Client Profiles

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

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

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

The screenshot shows a web-based configuration window titled "Edit Profile" with a close button (X) in the top right corner. At the top, there is a red warning box with the following text: "WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems. Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid." Below the warning, the configuration is organized into two main sections: "TLS Profile" and "Certificate Verification". The "TLS Profile" section includes a "Profile Name" text box containing "sbclInternal", a "Certificate" dropdown menu set to "sbclInternal.pem", and an "SNI" checkbox which is currently unchecked. The "Certificate Verification" section includes a "Peer Verification" label with the value "Required", a "Peer Certificate Authorities" dropdown menu set to "default.pem", an empty "Peer Certificate Revocation Lists" dropdown menu, a "Verification Depth" text box containing "1", an "Extended Hostname Verification" checkbox which is unchecked, and a "Server Hostname" text box which is empty. A "Next" button is located at the bottom center of the window.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

On the left, a navigation menu lists various management options, with 'Client Profiles' highlighted under 'TLS Management'. The main content area is titled 'Client Profiles: sbclnternal' and features an 'Add' button and a 'Delete' button.

The configuration details for the 'sbclnternal' profile are as follows:

Client Profile	
Click here to add a description.	
<b>TLS Profile</b>	
Profile Name	sbclnternal
Certificate	sbclnternal.pem
SNI	<input type="checkbox"/> Enabled
<b>Certificate Verification</b>	
Peer Verification	Required
Peer Certificate Authorities	default.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>
<b>Renegotiation Parameters</b>	
Renegotiation Time	0
Renegotiation Byte Count	0
<b>Handshake Options</b>	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:IDH:ADH:IMD5:1aNULL:1eNULL:@STRENG

An 'Edit' button is located at the bottom of the configuration form.

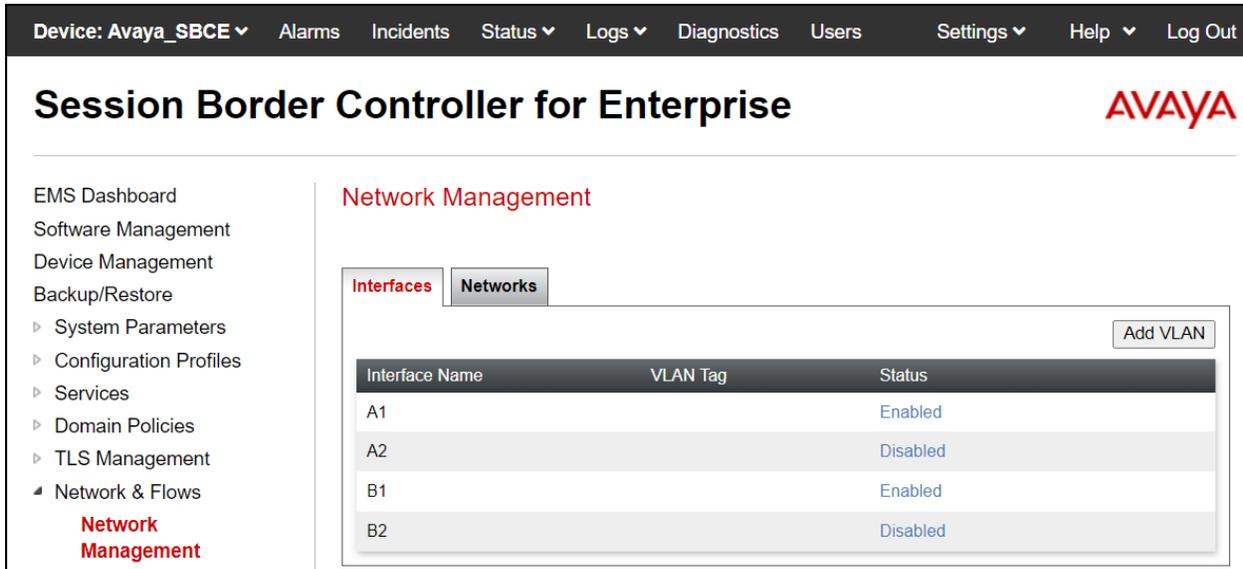
### 7.3. Network Management

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

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

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



The screenshot shows the Avaya SBCE management console. The top navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo. The left sidebar lists various management options, with 'Network Management' highlighted under 'Network & Flows'. The main content area is titled 'Network Management' and has two tabs: 'Interfaces' (selected) and 'Networks'. An 'Add VLAN' button is located in the top right of the interface table. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled).

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

## 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 Server or the trunk server.

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

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

The screenshot shows a dialog box titled "Edit Media Interface" with a close button "X" in the top right corner. The dialog contains the following fields:

- Name:** A text input field containing "Private\_med".
- IP Address:** A dropdown menu showing "Network\_A1 (A1, VLAN 0)" with a downward arrow. Below it, a sub-dropdown menu shows "10.64.101.243" with a downward arrow.
- Port Range:** Two text input boxes containing "35000" and "40000" separated by a hyphen.

At the bottom center of the dialog is a button labeled "Finish".

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

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

**Edit Media Interface** X

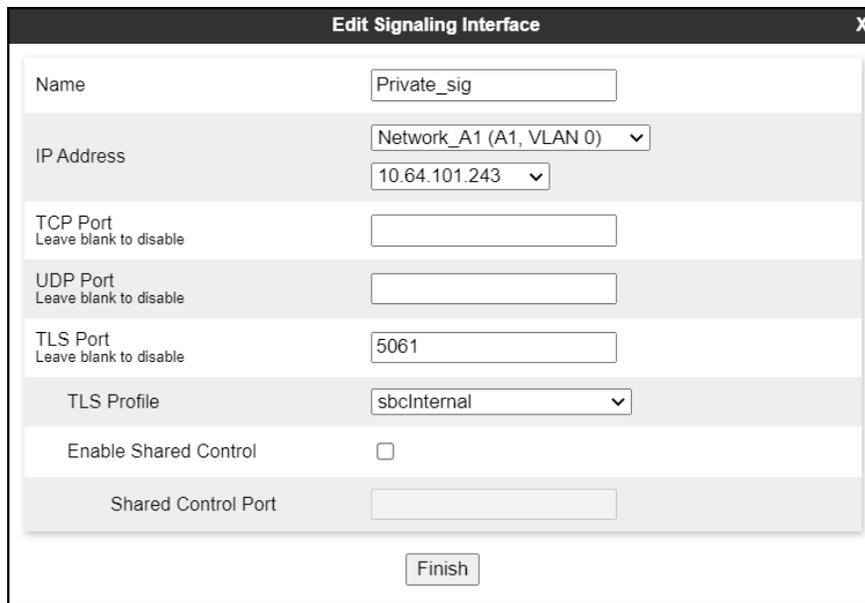
Name	<input type="text" value="Public_med"/>
IP Address	<input type="text" value="Network_B1 (B1, VLAN 0)"/> <input type="text" value="10.10.80.51"/>
Port Range	<input type="text" value="35000"/> - <input type="text" value="40000"/>

## 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 **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**.
- Select a **TLS Profile** (**Section 7.2.2**).
- Click **Finish**.



The screenshot shows a web-based configuration window titled "Edit Signaling Interface". The window contains several fields for configuring a signaling interface:

- Name:** A text input field containing "Private\_sig".
- IP Address:** A dropdown menu showing "Network\_A1 (A1, VLAN 0)" and a sub-dropdown showing "10.64.101.243".
- TCP Port:** A text input field with the label "Leave blank to disable".
- UDP Port:** A text input field with the label "Leave blank to disable".
- TLS Port:** A text input field containing "5061" with the label "Leave blank to disable".
- TLS Profile:** A dropdown menu showing "sbcInternal".
- Enable Shared Control:** A checkbox that is currently unchecked.
- Shared Control Port:** A text input field.

At the bottom of the window is a "Finish" button.

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

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5060** for **UDP Port**, since UDP port 5060 is used to listen for signaling traffic from Telstra in the sample configuration.
- Click **Finish**.

Name	Public_sig
IP Address	Network_B1 (B1, VLAN 0) 10.10.80.51
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

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).

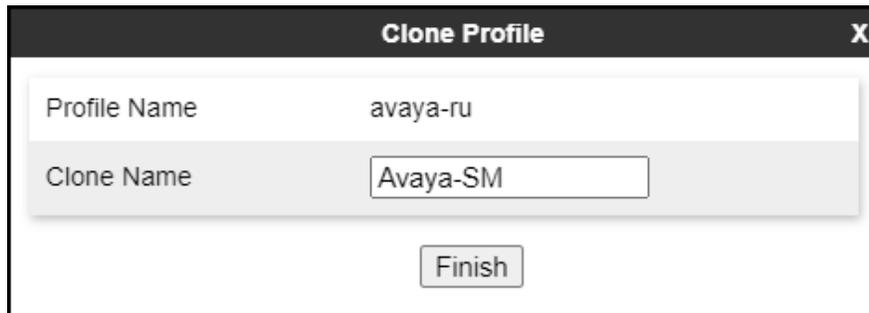
### 7.6.1. Server Interworking Profile – Enterprise

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 **Configuration Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select **avaya-ru** from the list of pre-defined profiles. Click **Clone** (not shown).

The screenshot shows the configuration page for the 'avaya-ru' interworking profile. The left navigation pane is expanded to 'Server Interworking'. The main content area has a title 'Interworking Profiles: avaya-ru' and an 'Add' button. Below this is a list of interworking profiles, with 'avaya-ru' selected. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' The configuration is divided into tabs: General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The 'General' tab is active, showing a table of configuration parameters.

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

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



The image shows a dialog box titled "Clone Profile" with a close button (X) in the top right corner. The dialog contains two input fields: "Profile Name" with the value "avaya-ru" and "Clone Name" with the value "Avaya-SM". A "Finish" button is located at the bottom center of the dialog.

Profile Name	avaya-ru
Clone Name	Avaya-SM

Finish

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

- On the **General** tab, set **SIPS Required** to **No**.
- Leave remaining fields with default values.
- Click **Finish** (not shown).

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

The screenshot displays the configuration page for the Session Border Controller for Enterprise. The top navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The main title is 'Session Border Controller for Enterprise'. On the left is a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Server Interworking' option is highlighted. The main content area is titled 'Interworking Profiles: Avaya-SM' and features an 'Add' button. A list of interworking profiles is shown, with 'Avaya-SM' selected. The configuration details for 'Avaya-SM' are displayed in a table with tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing various settings and their values.

Setting	Value
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No

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

Device: Avaya\_SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users

## Session Border Controller for Enterprise

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

- Domain DoS
- Server
- Interworking**
- Media Forking
- Routing
- Topology Hiding
- Signaling Manipulation
- URI Groups
- SNMP Traps
- Time of Day Rules
- FGDN Groups
- Reverse Proxy Policy
- URN Profile
- Recording Profile

### Interworking Profiles: Avaya-SM

[Add](#)

**Interworking Profiles**

- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- OCS-FrontEnd-Server
- Avaya-SM**
- Avaya-IPO
- Avaya-CS1000
- Avaya-CM
- cs2100
- SP-General

Click here to add a device

General
Timers
Privacy
URI Manipulation
Header Manipulation
Advanced

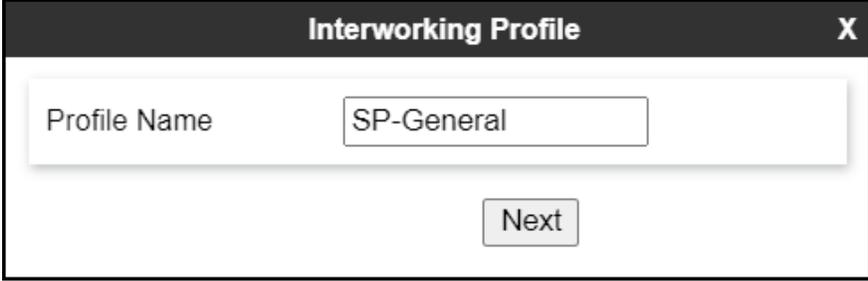
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
<b>DTMF</b>	
DTMF Support	None

[Edit](#)

## 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** tab, set **SIPS Required** to **No** (not shown).



The screenshot shows a dialog box titled "Interworking Profile" with a close button "X" in the top right corner. Inside the dialog, there is a label "Profile Name" followed by a text input field containing the text "SP-General". Below the input field, there is a "Next" button.

- Click **Next** until the last tab is reached then click **Finish** on the last tab leaving remaining fields with default values (not shown).

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

Device: Avaya\_SBCE ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users

## Session Border Controller for Enterprise

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- ▾ Configuration Profiles
  - Domain DoS
  - Server Interworking**
  - Media Forking
  - Routing
  - Topology Hiding
  - Signaling Manipulation
  - URI Groups
  - SNMP Traps
  - Time of Day Rules
  - FGDN Groups
  - Reverse Proxy Policy
  - URN Profile
  - Recording Profile
  - H248 Profile
  - IP/URI Blocklist Profile
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

### Interworking Profiles: SP-General

Add

Interworking Profiles

- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- OCS-FrontEnd-Server
- Avaya-SM
- Avaya-IPO
- Avaya-CS1000
- Avaya-CM
- cs2100
- SP-General**

Click here

**General**

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No

HG; Reviewed:  
SPOC 7/28/2022

Solution & Interoperability Test Lab Application Notes  
©2022 Avaya Inc. All Rights Reserved.

73 of 118  
Telstra-Aura101

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

Device: Avaya\_SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users

## Session Border Controller for Enterprise

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- ▾ Configuration Profiles
  - Domain DoS
  - Server Interworking**
  - Media Forking
  - Routing
  - Topology Hiding
  - Signaling Manipulation
  - URI Groups
  - SNMP Traps
  - Time of Day Rules
  - FGDN Groups
  - Reverse Proxy Policy
  - URN Profile
  - Recording Profile
  - H248 Profile
  - IP/URI Blocklist Profile

### Interworking Profiles: SP-General Click h

Interworking Profiles	
avaya-ru	
OCS-Edge-Server	
cisco-ccm	
cups	
OCS-FrontEnd-Server	
Avaya-SM	
Avaya-IPO	
Avaya-CS1000	
Avaya-CM	
cs2100	
<b>SP-General</b>	

Interworking Profiles: SP-General					
General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes					Both Sides
Include End Point IP for Context Lookup					No
Extensions					None
Diversion Manipulation					No
Has Remote SBC					Yes
Route Response on Via Port					No
Relay INVITE Replace for SIPREC					No
MOBX Re-INVITE Handling					No
NATing for 301/302 Redirection					Yes
DTMF					
DTMF Support					None

## 7.7. Signaling Manipulation

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

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

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

- Telstra requires the PAI Header on outbound calls from Communication Manager to the PSTN to be set to the Pilot Numbers provided by Telstra.
- Telstra requires a valid DID number, or a pilot number, in the “From” header of SIP INVITE messages. To support user privacy (calling party number blocking), on outbound calls from Communication Manager to the PSTN, a SigMa script was added to change “anonymous” in the FROM header of SIP INVITE messages to pilot numbers provided by Telstra.
- Remove unwanted xml element information from being sent to Telstra as part of the SDP. It was observed that on certain outbound calls from Communication Manager to Telstra xml elements were present in the SDP. A SigMa script was added to remove them.

The scripts will later be applied to the Server Configuration profile corresponding to the Service Provider (toward Telstra) in **Section 7.8.2**.

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

- For **Title** enter a name, the names **Telstra\_Script\_A** and **Telstra\_Script\_B** were chosen in the examples.
- Copy the complete scripts from **Appendix A**.

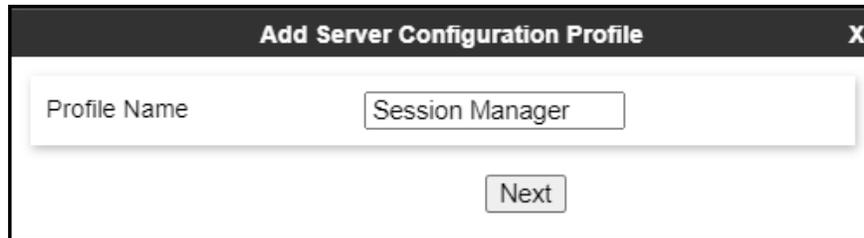
## 7.8. Server Configuration

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

### 7.8.1. Server Configuration Profile – Enterprise

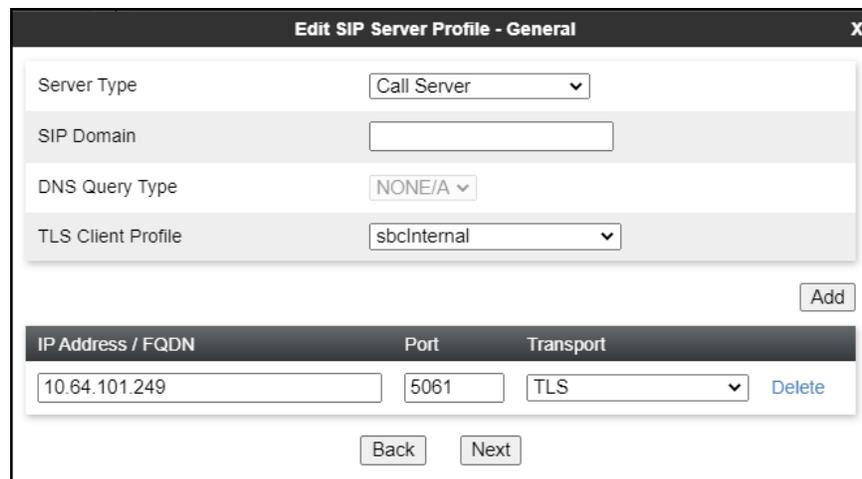
From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

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



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Session Manager". Below this field is a button labeled "Next".

- On the **Edit SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.6**.
- Select a **TLS Profile** (**Section 7.2.3**).
- Click **Next**.



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and a table:

- Server Type:** Call Server (dropdown menu)
- SIP Domain:** (empty text field)
- DNS Query Type:** NONE/A (dropdown menu)
- TLS Client Profile:** sbcInternal (dropdown menu)
- Add:** (button)
- Table:** A table with three columns: IP Address / FQDN, Port, and Transport. The first row contains: 10.64.101.249, 5061, and TLS. A "Delete" button is located to the right of the first row.
- Back:** (button)
- Next:** (button)

- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
  - Check **Enable Grooming** (required for TLS transport).
  - Select **Avaya-SM** from the **Interworking Profile** drop-down menu (**Section 7.6.1**).
- Click **Finish**.

Add SIP Server Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

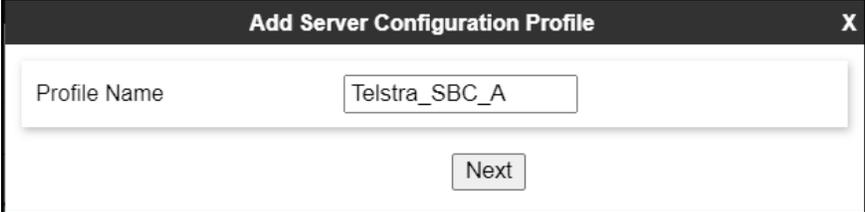
Back Finish

## 7.8.2. Server Configuration Profiles – Service Provider

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

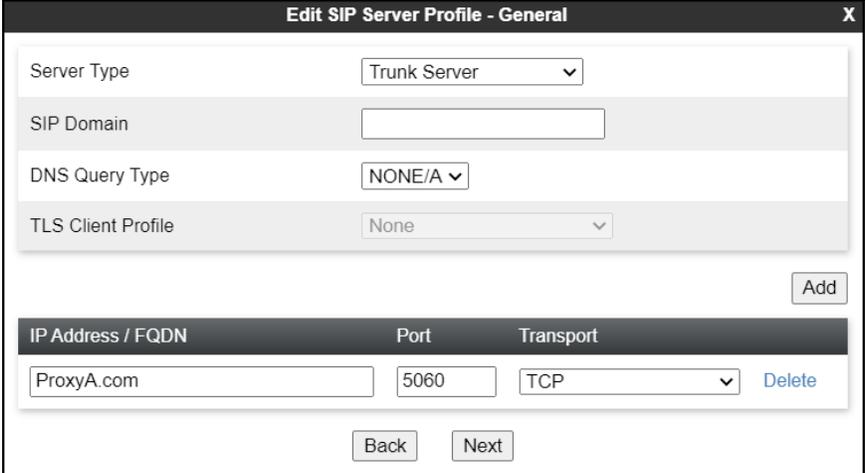
**Note** – Telstra requires two separate SIP server profiles. SIP traffic was distributed between the two SIP server profiles using Round-Robin load balancing (Refer to **Section 7.9.2**).

- Enter an appropriate **Profile Name** similar to the screen below (**Telstra\_SBC\_A** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Telstra\_SBC\_A". Below the input field is a button labeled "Next".

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop-down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter **ProxyA.com** (Telstra SIP proxy server FQDN). This information was provided by Telstra.
- Enter **5060** under **Port** and select **TCP** for **Transport** (TCP Transport was used per Telstra's request).
- Click **Next**.



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and a table:

- Server Type:** Trunk Server (dropdown menu)
- SIP Domain:** (empty text input field)
- DNS Query Type:** NONE/A (dropdown menu)
- TLS Client Profile:** None (dropdown menu)
- Add:** (button)
- IP Address / FQDN:** ProxyA.com (text input field)
- Port:** 5060 (text input field)
- Transport:** TCP (dropdown menu)
- Delete:** (button)
- Back:** (button)
- Next:** (button)

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

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave the **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

The screenshot shows a window titled "Add SIP Server Profile - Authentication". The window contains a form with the following fields and values:

Field	Value
Enable Authentication	<input checked="" type="checkbox"/>
User Name	usernameA
Realm (Leave blank to detect from server challenge)	
Password	*****
Confirm Password	*****

At the bottom of the form, there are two buttons: "Back" and "Next".

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

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

- Check the **Register with All Servers** box.
- **Frequency:** Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **30** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI:** Enter the pilot number for SIP Proxy Server **Telstra\_SBC\_A** and Telstra's domain name, as shown on the screen below. This information should be provided by Telstra.
  - **To URI:** Enter the pilot number for SIP Proxy Server **Telstra\_SBC\_A** and Telstra's domain name, as shown on the screen below. This information should be provided by Telstra.
  - Click **Next**.

Add SIP Server Profile - Registration	
Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	<input type="text" value="30"/> seconds
From URI	<input type="text" value="862174396@telstra.com"/>
To URI	<input type="text" value="862174396@telstra.com"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

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

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

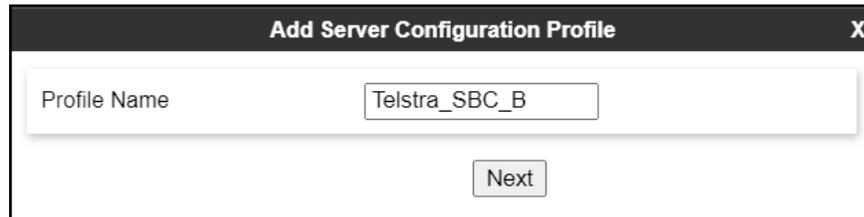
- Check **Enable Grooming** (required for TCP transport).
- Select **SP-General** from the **Interworking Profile** drop-down menu (**Section 7.6.2**).
- Select the **Telstra\_Script\_A** from the **Signaling Manipulation Script** drop down menu (**Sections 7.7 and 12**).
- Click **Finish**.

Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	Telstra_Script_A
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

Back Finish

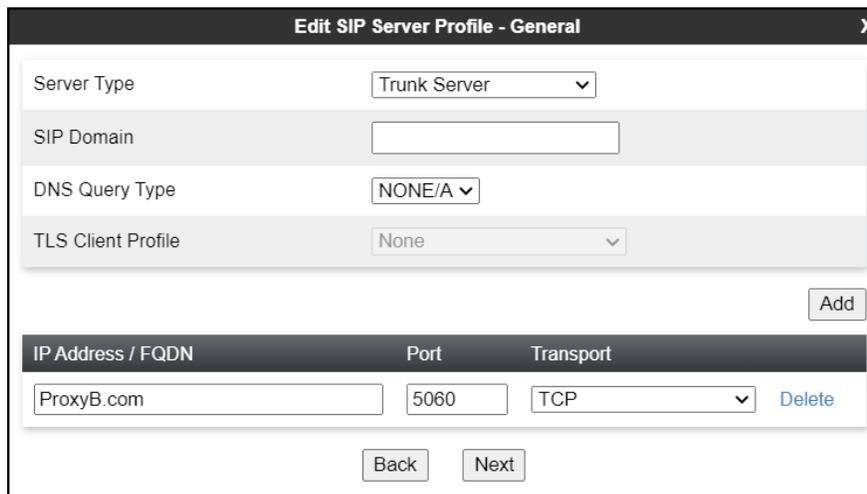
Similarly, to add the profiles for the second Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below (**Telstra\_SBC\_B** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Telstra\_SBC\_B". Below the input field is a button labeled "Next".

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop-down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter **ProxyB.com** (Telstra SIP proxy server FQDN). This information was provided by Telstra.
- Enter **5060** under **Port** and select **TCP** for **Transport** (TCP Transport was used per Telstra's request).
- Click **Next**.



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. The dialog contains several configuration fields:

- Server Type:** Trunk Server (dropdown menu)
- SIP Domain:** (empty text input field)
- DNS Query Type:** NONE/A (dropdown menu)
- TLS Client Profile:** None (dropdown menu)

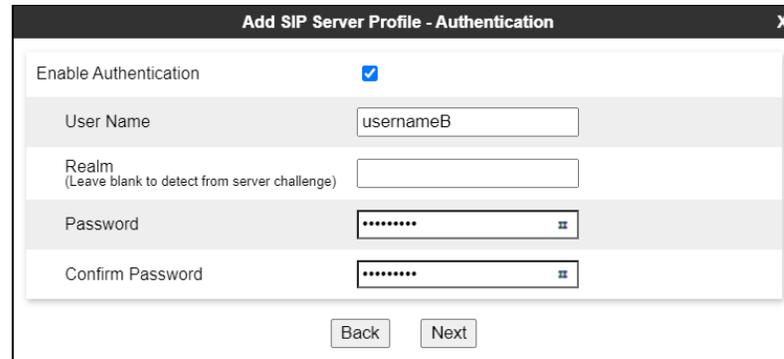
Below these fields is an **Add** button. Underneath is a table with three columns: **IP Address / FQDN**, **Port**, and **Transport**.

IP Address / FQDN	Port	Transport
ProxyB.com	5060	TCP

At the bottom of the table is a **Delete** link. Below the table are **Back** and **Next** buttons.

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

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration for the second Trunk Server.
- Leave the **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration for the second Trunk Server.
- Click **Next**.



The screenshot shows a window titled "Add SIP Server Profile - Authentication". The window contains a form with the following fields and controls:

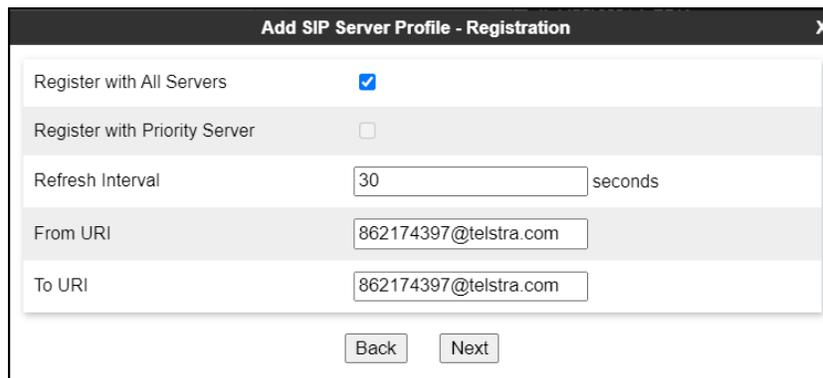
- Enable Authentication:** A checkbox that is checked.
- User Name:** A text input field containing "usernameB".
- Realm:** A text input field that is empty. Below the field is the text "(Leave blank to detect from server challenge)".
- Password:** A password input field with masked characters (dots) and a small icon on the right.
- Confirm Password:** A password input field with masked characters (dots) and a small icon on the right.

At the bottom of the form, there are two buttons: "Back" and "Next".

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

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

- Check the **Register with All Servers** box.
- **Frequency:** Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **30** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI:** Enter the pilot number for SIP Proxy Server **Telstra\_SBC\_B** and Telstra's domain name, as shown on the screen below. This information should be provided by Telstra.
  - **To URI:** Enter the pilot number for SIP Proxy Server **Telstra\_SBC\_B** and Telstra's domain name, as shown on the screen below. This information should be provided by Telstra.
  - Click **Next**.



The screenshot shows a configuration window titled "Add SIP Server Profile - Registration". It contains the following fields and controls:

Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	<input type="text" value="30"/> seconds
From URI	<input type="text" value="862174397@telstra.com"/>
To URI	<input type="text" value="862174397@telstra.com"/>

At the bottom of the window are two buttons: "Back" and "Next".

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

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

- Check **Enable Grooming** (required for TCP transport).
- Select **SP-General** from the **Interworking Profile** drop-down menu (**Section 7.6.2**).
- Select the **Telstra\_Script\_B** from the **Signaling Manipulation Script** drop down menu (**Sections 7.7 and 12**).
- Click **Finish**.

Add SIP Server Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	Telstra_Script_B
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>
Back 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

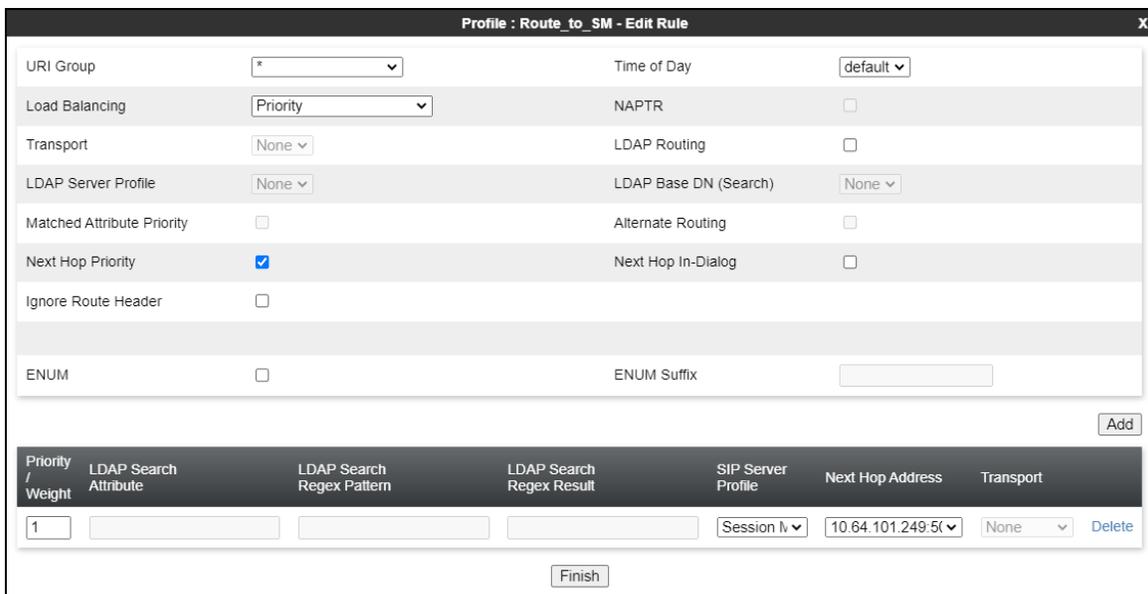
To create the inbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

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



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route\_to\_SM". Below the input field is a button labeled "Next".

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



The screenshot shows the "Profile : Route\_to\_SM - Edit Rule" configuration screen. The screen is divided into two main sections. The top section contains various configuration options with checkboxes and dropdown menus. The bottom section contains a table with columns for "Priority / Weight", "LDAP Search Attribute", "LDAP Search Regex Pattern", "LDAP Search Regex Result", "SIP Server Profile", "Next Hop Address", and "Transport".

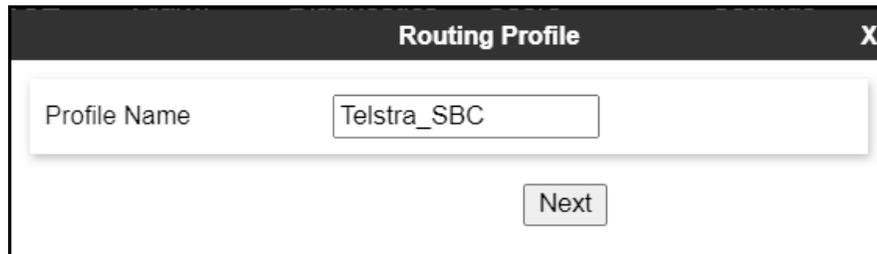
Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				Session M	10.64.101.249:5060	None

Buttons for "Add" and "Finish" are visible at the bottom of the screen.

## 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 (**Telstra\_SBC** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Routing Profile" with a close button "X" in the top right corner. Inside the dialog, there is a label "Profile Name" followed by a text input field containing the text "Telstra\_SBC". Below the input field, there is a button labeled "Next".

- Under **Load Balancing** select **Round-Robin**.
- Uncheck **Next Hop Priority**.
- Click the **Add** button to enter the first SIP Server Profile.
- Under **SIP Server Profile**, select **Telstra\_SBC\_A**. The **Next Hop Address** is populated automatically with **ProxyA.com:5060 (TCP)**. Telstra SIP Proxy FQDN, Port and Transport, Server Configuration Profile defined in **Section 7.8.2**.
- Click the **Add** button again to enter the second SIP Server Profile.
- Under **SIP Server Profile**, select **Telstra\_SBC\_B**. The **Next Hop Address** is populated automatically with **ProxyB.com:5060 (TCP)**. Telstra SIP Proxy FQDN, Port and Transport, Server Configuration Profile defined in **Section 7.8.2**
- Click **Finish**.

**Profile : Telstra\_SBC - Edit Rule** X

URI Group	*	Time of Day	default
Load Balancing	Round-Robin	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
0				Telstra_SI	ProxyA.com:5060	None	Delete
0				Telstra_SI	ProxyB.com:5060	None	Delete

The following screen shows the completed **Telstra\_SBC** Routing Profile form

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'ings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left-hand navigation menu lists various management options, with 'Routing' highlighted in red. The main content area is titled 'Routing Profiles: Telstra\_SBC' and features an 'Add' button. Below this is a list of routing profiles, with 'Telstra\_SBC' selected. A 'Routing Profile' configuration window is open, showing a table with columns for Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The table contains one entry with Priority 1, URI Group \*, Time of Day default, Load Balancing Round-Robin, and two Next Hop Addresses: ProxyA.com:5060 (TCP) and ProxyB.com:5060 (TCP). The interface also includes buttons for 'Rename', 'Clone', 'Delete', and 'Update Priority'.

Device: Avaya\_SBCE Alarms Incidents Status Logs Diagnostics Users ings Help Log Out

### Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Domain DoS  
Server Interworking  
Media Forking  
**Routing**  
Topology Hiding  
Signaling  
Manipulation  
URI Groups  
SNMP Traps  
Time of Day Rules  
FGDN Groups

#### Routing Profiles: Telstra\_SBC

Add

Rename Clone Delete

Click here to add a description.

#### Routing Profile

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Round-Robin	ProxyA.com:5060	TCP	Edit Delete
				ProxyB.com:5060	TCP	

## 7.10. Topology Hiding

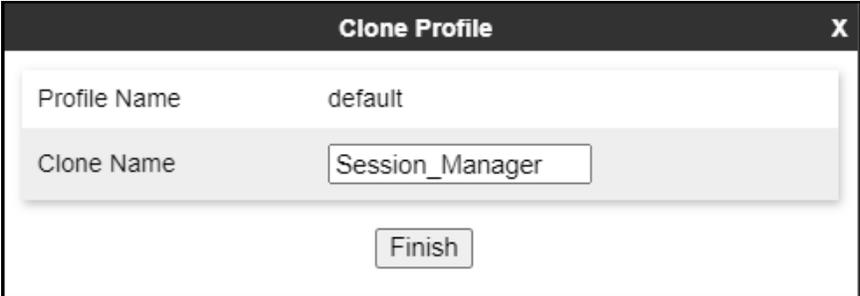
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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 **Configuration Profiles** menu on the left-hand side, select **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

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



Clone Profile	
Profile Name	default
Clone Name	<input type="text" value="Session_Manager"/>
<input type="button" value="Finish"/>	

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

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

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

### 7.10.2. Topology Hiding Profile – Service Provider

To add the Topology Hiding Profile in the service provider 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**.

The screenshot shows a dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains two input fields: "Profile Name" with the value "default" and "Clone Name" with the value "Service\_Provider". A "Finish" button is located at the bottom center of the dialog.

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

- For the, **From, To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the Service Provider SIP domain **telstra.com**, in the **Overwrite Value** column of these headers, as shown below. This is the service provider’s domain name, this information is provided by the Service Provider.
- Default values were used for all other fields.
- Click **Finish**.

The screenshot shows a dialog box titled "Edit Topology Hiding Profile" with a close button (X) in the top right corner. It contains a table with the following data:

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

A "Finish" button is located at the bottom center of the dialog.

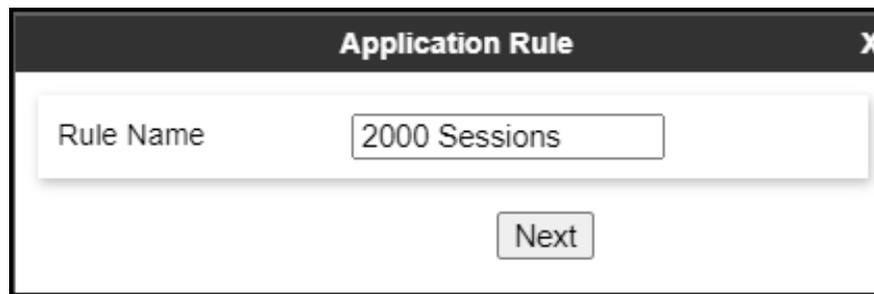
## 7.11.Domain Policies

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

### 7.11.1.Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**, click on the **Add** button to add a new rule.

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



The screenshot shows a dialog box titled "Application Rule" with a close button (X) in the top right corner. The dialog contains a label "Rule Name" and a text input field with the value "2000 Sessions". Below the input field is a "Next" button.

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

Editing Rule: 2000 Sessions X

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="2000"/>	<input type="text" value="2000"/>
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="100"/>

**Miscellaneous**

CDR Support  Off  
 RADIUS  
 CDR Adjunct

RADIUS Profile

Media Statistics Support

Call Duration  Setup  
 Connect

RTCP Keep-Alive

## 7.11.2. Media Rules

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

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **SM\_SRTP**.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Repeat the above steps under Video Encryption, if needed.
- Click **Next**.

**Media Encryption**
X

**Audio Encryption**

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▾
Preferred Format #2	RTP ▾
Preferred Format #3	NONE ▾
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input style="width: 40px;" type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

**Video Encryption**

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▾
Preferred Format #2	RTP ▾
Preferred Format #3	NONE ▾
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input style="width: 40px;" type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

**Miscellaneous**

Capability Negotiation	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

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

Audio Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

Finish

### 7.11.3. Signaling Rules

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

Device: Avaya\_SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users

## Session Border Controller for Enterprise

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- ▾ Domain Policies
  - Application Rules
  - Border Rules
  - Media Rules
  - Security Rules
  - Signaling Rules**
  - Charging Rules
  - End Point Policy
  - Groups
  - Session Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Signaling Rules: default

Add

Signaling Rules
Add

- default**
- No-Content-Type-Checks
- SessMgr\_CM\_SigRule
- OPTIONS
- Remote Workers
- Remove\_Update
- Contact
- Remove PAI
- Remove PAI\_1
- Remove\_headers
- Remove Record Route

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

**General**

Requests

Responses

Request Headers

Response Headers

Signaling QoS

UCID

Inbound

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

Outbound

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

Content-Type Policy

Enable Content-Type Checks	<input checked="" type="checkbox"/>
Action	Allow
Exception List	Multipart Action Allow
	Exception List

Edit

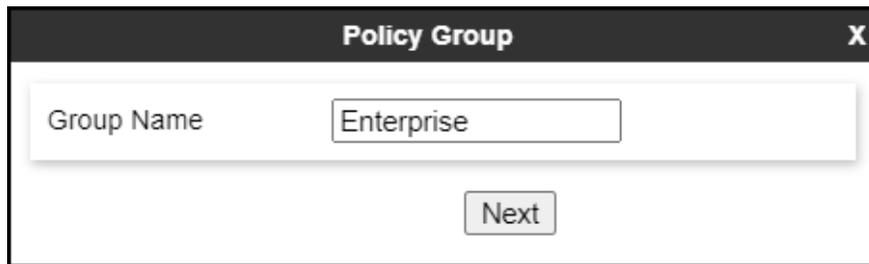
## 7.12. End Point Policy Groups

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

### 7.12.1. 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).

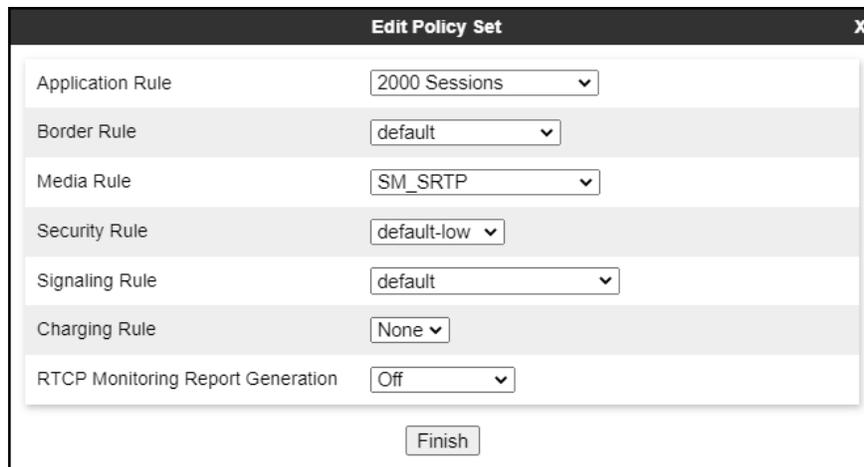
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" containing the text "Enterprise". Below the input field is a button labeled "Next".

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

- **Application Rule: 2000 Sessions** (Section 7.11.1).
- **Border Rule: default**.
- **Media Rule: SM\_SRTP** (Section 7.11.2).
- **Security Rule: default-low**.
- **Signaling Rule: default** (Section 7.11.3).
- Click **Finish**.



The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows of settings, each with a label and a dropdown menu:

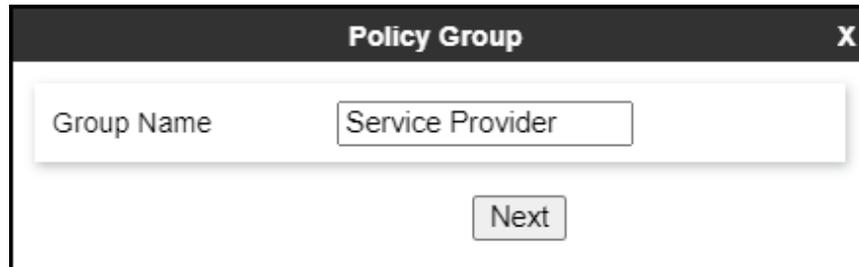
Application Rule	2000 Sessions
Border Rule	default
Media Rule	SM_SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

At the bottom of the dialog is a button labeled "Finish".

## 7.12.2. End Point Policy Group – Service Provider

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

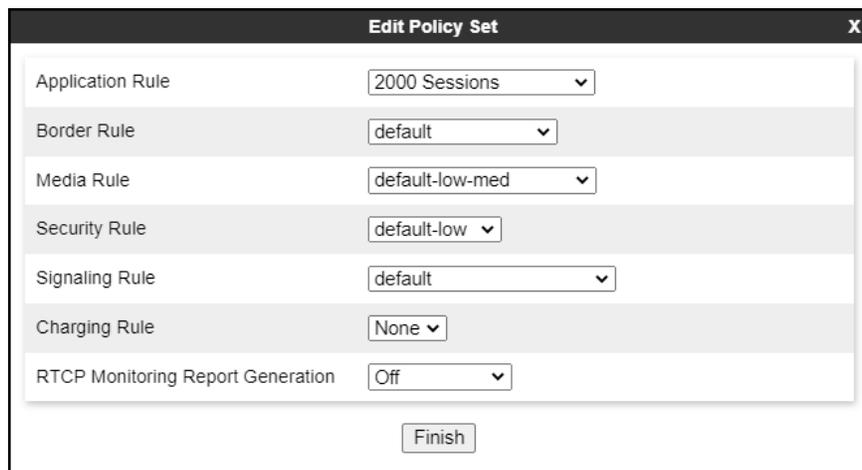
- Enter an appropriate name in the **Group Name** field (**Service Provider** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" containing the text "Service Provider". Below the input field is a button labeled "Next".

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

- **Application Rule: 2000 Sessions** (Section 7.11.1).
- **Border Rule: default**.
- **Media Rule: default-low-med** (Section 7.11.2).
- **Security Rule: default-low**.
- **Signaling Rule: default** (Section 7.11.3).
- Click **Finish**.



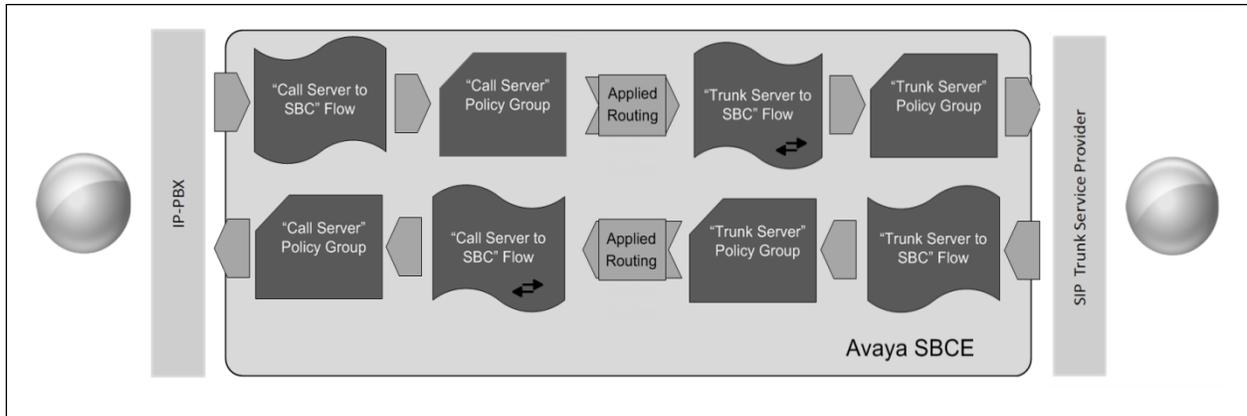
The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a label and a dropdown menu:

Application Rule	2000 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

At the bottom of the dialog is a button labeled "Finish".

## 7.13. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.



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

### 7.13.1. End Point Flows – SP to SM

Two server flows were created to route inbound calls from Telstra to the Enterprise across the two SIP Proxy Servers provided by Telstra.

To create the first server flow from Telstra to the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The screen below shows the server flow named **SP\_Trunk\_Server\_A\_to\_SM\_Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: SP Trunk Server A to SM Flow	
Flow Name	SP_Trunk_Server_A_to_SM_Flow
SIP Server Profile	Telstra_SBC_A
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
<input type="button" value="Finish"/>	

Repeat to add the second server flow from Telstra to the Enterprise.

The screen below shows the server flow named **SP\_Trunk\_Server\_B\_to\_SM\_Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: SP_Trunk_Server_B_to_SM_Flow	
Flow Name	SP_Trunk_Server_B_to_SM_Flow
SIP Server Profile	Telstra_SBC_B
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
<input type="button" value="Finish"/>	

### 7.13.2. End Point Flow – SM\_to\_SP\_Flow

A Server Flow with the name **SM\_to\_SP\_Flow** was similarly created to route calls from the Enterprise to Telstra. To create the server flow, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: SM_to_SP_Flow	
Flow Name	SM_to_SP_Flow
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
Secondary Media Interface	None
End Point Policy Group	Enterprise
Routing Profile	Telstra_SBC
Topology Hiding Profile	Session_Manager
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
<input type="button" value="Finish"/>	

## 8. Telstra Enterprise SIP Trunking Service Configuration

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

During the signup process, Telstra and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Telstra network.

Telstra will provide the following information:

- SIP Trunk registration credentials (user name, password, SIP domain, pilot numbers).
- Fully Qualified Domain Names of the Telstra's SIP proxy servers.
- DID numbers.
- Public DNS IP addresses.
- 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 (firewall).
- E.164 numbering format requirements.

## 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:

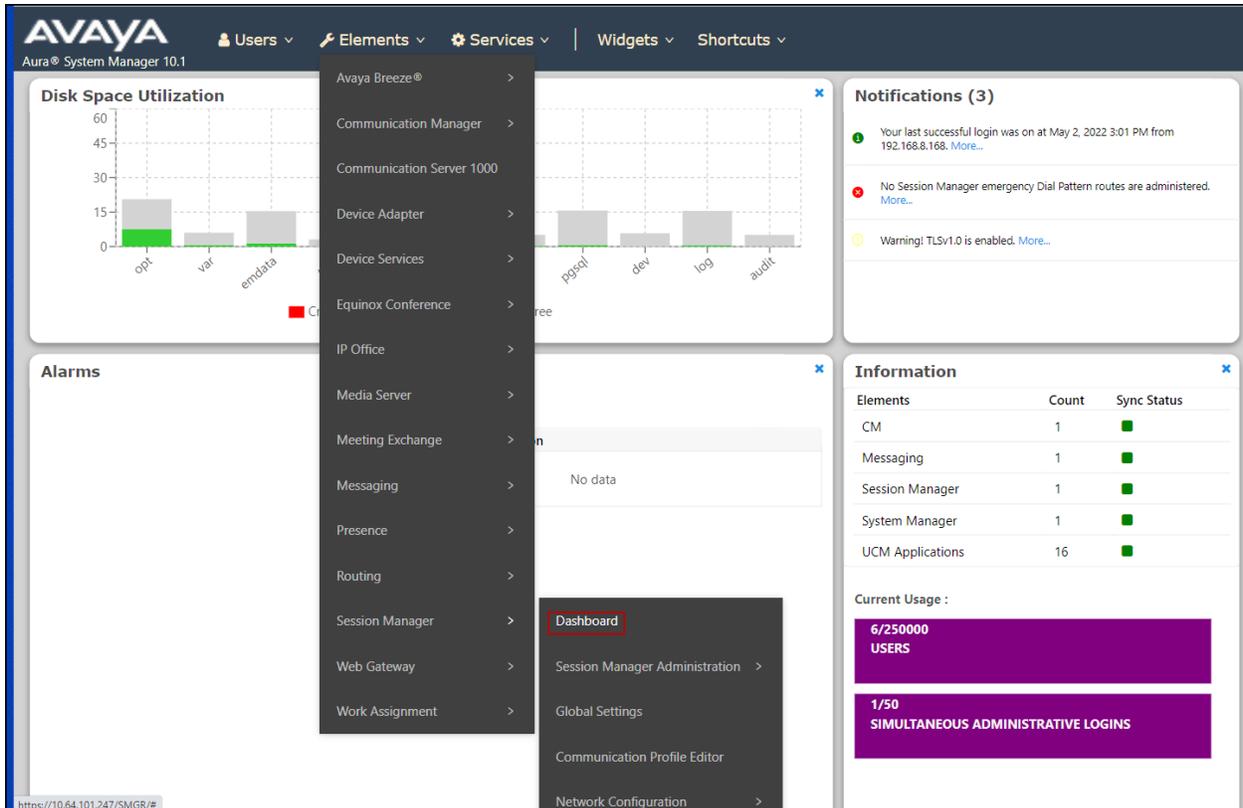
- **list trace station** <extension number>  
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>  
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>  
Displays signaling group service state.
- **status trunk** <trunk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

The Session Manager configuration may be verified via System Manager.

**Step 1** - Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**, then select **Dashboard**.



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

In the **Entity Monitoring** column, Session Manager shows that there are **3** alarms out of the **9** Entities defined.

**Session Manager Dashboard**  
This page provides the overall status and health summary of each administered Session Manager.

**Session Manager Instances**

Service State: [Dropdown] Shutdown System: [Dropdown] EASG: [Dropdown] Clear Logs: [Button] As of: 9:09 AM

1 Item [Refresh] Show: All [Dropdown] Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Load Factor	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Profile	Version
<input type="checkbox"/>	Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/0/0	3/9	0	1/1	✓	✓	Normal	Enabled	3	10.1.0.0.1010019

Select: All, None

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

**Session Manager Entity Link Connection Status**  
This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

**All Entity Links for Session Manager: Session Manager**

Summary View

9 Items [Refresh] Filter: Enable

<input type="checkbox"/>	SIP Entity Name	Session Manager IP Address	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="checkbox"/>	CS1K7.6	IPv4	172.16.5.60	5085	UDP	FALSE	DOWN	408 Request Timeout	DOWN
<input type="checkbox"/>	Avaya Experience Portal	IPv4	10.64.101.252	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="checkbox"/>	AA-Messaging	IPv4	10.64.101.250	5060	TCP	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="checkbox"/>	Avaya SBCE	IPv4	10.64.101.243	5061	TLS	FALSE	UP	200 OK	UP
<input type="checkbox"/>	Communication Manager Trunk 1	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
<input type="checkbox"/>	Communication Manager Trunk 108	IPv4	10.64.101.241	5068	TLS	FALSE	UP	200 OK	UP
<input type="checkbox"/>	IX Messaging	IPv4	10.64.101.158	5061	TLS	FALSE	UP	200 OK	UP
<input type="checkbox"/>	Communication Manager Trunk 2	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
<input type="checkbox"/>	Communication Manager Trunk 98	IPv4	10.64.101.241	5065	TLS	FALSE	UP	200 OK	UP

Select: None

Other Session Manager useful verification and troubleshooting tools include:

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

## 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.

The screenshot shows the Avaya SBCE Dashboard for device Avaya\_SBCE. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main content area is divided into a left sidebar with navigation options and a central dashboard. The dashboard displays system information, installed devices, active alarms, and incidents.

Information	
System Time	09:13:01 AM EDT <a href="#">Refresh</a>
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-21432
Build Date	Thu Dec 02 21:33:10 UTC 2021
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	05/03/2022 15:46:29 EDT
Failed Login Attempts	1

Installed Devices	
EMS	
Avaya_SBCE	

Active Alarms (past 24 hours)	
None found.	

Incidents (past 24 hours)	
Avaya_SBCE: Registration Successful, Server is UP	
Avaya_SBCE: Registration Successful, Server is UP	

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

The screenshot shows the Avaya SBCE Alarm Viewer page. The top navigation bar includes links for EMS, Avaya\_SBCE, and Help. The main content area displays a table with columns for ID, Details, State, Time, and Device. A message indicates that no alarms were found for this device.

ID	Details	State	Time	Device
No alarms found for this device.				

Buttons: Clear Selected, Clear All

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

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. At the top, a navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents' (highlighted with a red arrow), 'Status', 'Logs', 'Diagnostics', and 'Users'. The main content area is divided into a left sidebar with a navigation menu and a central dashboard. The sidebar menu includes 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services' (with sub-items like SIP Servers, H248 Servers, LDAP, RADIUS), 'Domain Policies', 'TLS Management', 'Network & Flows' (with sub-items like Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, Advanced Options), 'DMZ Services', and 'Monitoring & Logging'. The central dashboard has a title 'Dashboard' and contains several panels: 'Information' (System Time, Version, GUI Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), 'Installed Devices' (listing Avaya\_SBCE), 'Active Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (listing Avaya\_SBCE: Registration Successful, Server is UP).

The following screen shows the Incident Viewer page.

The screenshot shows the 'Incident Viewer' page. At the top, it displays 'Device: Avaya\_SBCE' and a 'Help' link. The page title is 'Incident Viewer' with the AVAYA logo. Below the title, there is a 'Category' dropdown menu set to 'All', a 'Clear Filters' button, and 'Refresh' and 'Generate Report' buttons. The main content area is titled 'Summary' and shows 'Displaying entries 1 to 15 of 2002.' Below this is a table with the following data:

ID	Date & Time	Category	Type	Cause
825835107193461	May 4, 2022 9:16:54 AM	Policy	Server Registration	Registration Successful, Server is UP
825835047173505	May 4, 2022 9:14:54 AM	Policy	Server Registration	Registration Successful, Server is UP

**Status:** This screen provides the registration status of the servers.

The screenshot shows the Avaya EMS Dashboard for a Session Border Controller for Enterprise. The top navigation bar includes 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status' (highlighted with a red arrow), 'Logs', 'Diagnostics', and 'Users'. The main content area is titled 'Session Border Controller for Enterprise' and contains a 'Dashboard' section with several panels:

- Information:** A table showing system details:
 

System Time	09:13:01 AM EDT	<a href="#">Refresh</a>
Version	10.1.0.0-32-21432	
GUI Version	10.1.0.0-21432	
Build Date	Thu Dec 02 21:33:10 UTC 2021	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/03/2022 15:46:29 EDT	
Failed Login Attempts	1	
- Installed Devices:** A list showing 'Avaya\_SBCE' under the 'EMS' category.
- Active Alarms (past 24 hours):** A section indicating 'None found'.
- Incidents (past 24 hours):** A list of incidents:
  - Avaya\_SBCE: Registration Successful, Server is UP
  - Avaya\_SBCE: Registration Successful, Server is UP

The following screen shows the Telstra servers registration status.

The screenshot shows the 'Status' page for a device 'Avaya\_SBCE'. The page title is 'Status' and the Avaya logo is visible in the top right. A 'Server Status' section contains a table with the following data:

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Telstra_SBC_B	[redacted] telstra.com	[redacted].164.24	5060	TCP	UNKNOWN	REGISTERED	06/17/2022 08:55:18 EDT
Telstra_SBC_A	[redacted] telstra.com	[redacted].164.8	5060	TCP	UNKNOWN	REGISTERED	06/17/2022 08:55:18 EDT

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

The screenshot shows the Avaya SBCE management interface. At the top, there is a navigation bar with the following items: Device: Avaya\_SBCE, Alarms, Incidents, Status, Logs, Diagnostics (highlighted with a red arrow), and Users. Below the navigation bar is the main header "Session Border Controller for Enterprise". On the left side, there is a sidebar menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services (expanded), SIP Servers, H248 Servers, LDAP, RADIUS, Domain Policies, TLS Management, Network & Flows (expanded), Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, Advanced Options, DMZ Services, and Monitoring & Logging. The main content area is titled "Dashboard" and contains several panels: Information (System Time: 09:13:01 AM EDT, Version: 10.1.0.0-32-21432, GUI Version: 10.1.0.0-21432, Build Date: Thu Dec 02 21:33:10 UTC 2021, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged In at: 05/03/2022 15:46:29 EDT, Failed Login Attempts: 1), Installed Devices (EMS, Avaya\_SBCE), Active Alarms (past 24 hours) (None found), and Incidents (past 24 hours) (Avaya\_SBCE: Registration Successful, Server is UP, Avaya\_SBCE: Registration Successful, Server is UP).

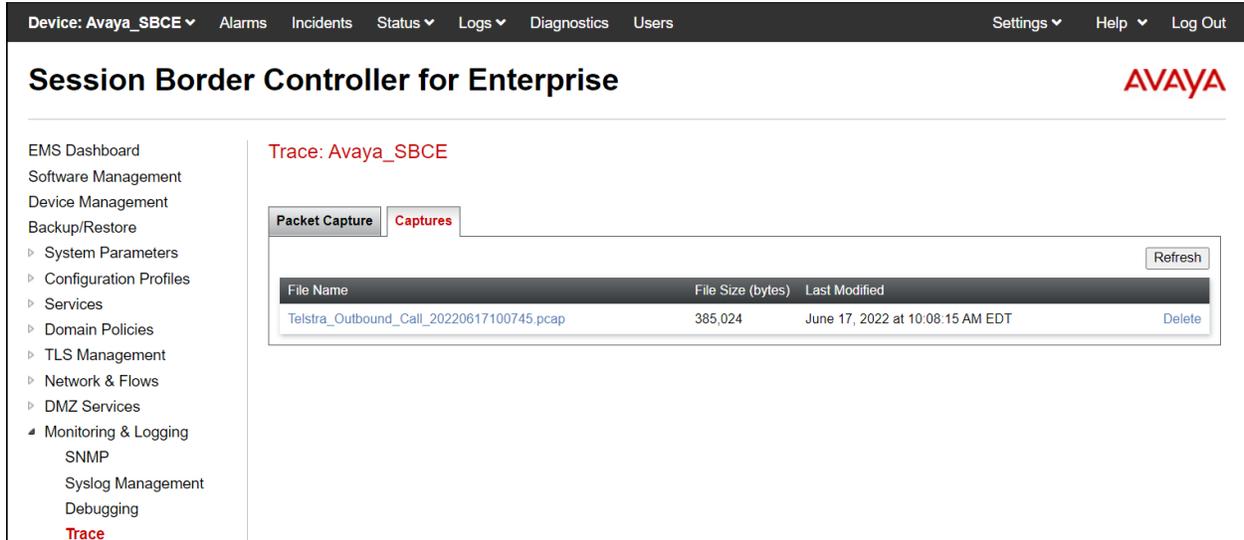
The following screen shows the Diagnostics page with the results of a ping test.

The screenshot shows the Avaya SBCE Diagnostics page. At the top, there is a navigation bar with the following items: Device: Avaya\_SBCE, Help, and a "Pinging 10.64.101.247" notification box. The main header is "Diagnostics". Below the header, there are two tabs: "Full Diagnostic" and "Ping Test" (selected). A message box states: "Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN." Below the message box, there is a form with the following fields: Source Device / IP (A1), Destination IP (10.64.101.247), and a "Ping" button. The AVAYA logo is visible in the top right corner.

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

The screenshot shows the Avaya SBCE web interface. At the top, there is a navigation bar with 'Device: Avaya\_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this is the main header 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left is a sidebar menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', 'Monitoring & Logging' (expanded), 'SNMP', 'Syslog Management', 'Debugging', 'Trace' (highlighted), 'Log Collection', and 'DoS Learning'. The main content area is titled 'Trace: Avaya\_SBCE' and contains two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' form includes: 'Status: Ready', 'Interface: Any', 'Local Address: All', 'Remote Address: \*', 'Protocol: All', 'Maximum Number of Packets to Capture: 10000', and 'Capture Filename: Telstra\_Outbound\_Call.pcap'. There are 'Start Capture' and 'Clear' buttons at the bottom of the form.

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.



The screenshot shows the Avaya SBCE web interface. At the top, there is a navigation bar with the following items: Device: Avaya\_SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below this is the main header "Session Border Controller for Enterprise" with the AVAYA logo on the right. On the left side, there is a sidebar menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, Monitoring & Logging (expanded), SNMP, Syslog Management, Debugging, and Trace (highlighted in red). The main content area is titled "Trace: Avaya\_SBCE" and contains two tabs: "Packet Capture" and "Captures" (highlighted in red). Below the tabs is a table with the following columns: File Name, File Size (bytes), Last Modified, and a "Delete" button. The table contains one row with the following data: File Name: Telstra\_Outbound\_Call\_20220617100745.pcap, File Size (bytes): 385,024, Last Modified: June 17, 2022 at 10:08:15 AM EDT, and a "Delete" button. There is also a "Refresh" button in the top right corner of the table area.

Also, the **traceSBC** tool can be used to monitor the SIP signaling messages between the Service provider and the Avaya SBCE.

## 10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1, to connect to the Telstra Enterprise 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 **Sections 2.1** and **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 a Virtualized Environment*, Release 10.1, Issue 3, April 2022.
- [2] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021.
- [3] *Administering Avaya Aura® System Manager* for Release 10.1.x, Issue 5, April 2022.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 10.1.x, Issue 2, March 2022.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 10.1., Issue 2, March 2022.
- [6] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022.
- [7] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*, Release 10.1, Issue 1, December 2021.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, Issue 1, December 2021.
- [9] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 10.1, Avaya Aura® Communication Manager Rel. 10.1 and Avaya Aura® Session Managers Rel. 10.1 - Issue 1.0*.
- [10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 10.1.x, Issue 1, April 2022.
- [11] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [12] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

## 12. Appendix A – SigMa Scripts

Following are the Signaling Manipulation scripts that were used in the configuration of the Avaya SBCE. Add the scripts as instructed in **Sections 7.7** and **7.8.2**, enter the names for the scripts in the Title and copy/paste the entire scripts shown below.

---

### **Title: Telstra\_Script\_A**

```
within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["P-Asserted-Identity"][1].URI.USER = "862174396";
  }
}

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

if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
  {
%HEADERS["FROM"][1].URI.USER = "862174396";
  }

//Remove xml element information from being sent to SP
remove(%BODY[1]);

}
}
```

## Title: Telstra\_Script\_B

within session "INVITE"

```
{
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["P-Asserted-Identity"][1].URI.USER = "862174397";
  }
}
```

within session "ALL"

```
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
    {
      %HEADERS["FROM"][1].URI.USER = "862174397";
    }
  }
}
```

```
//Remove xml element information from being sent to SP
remove(%BODY[1]);
```

```
}
}
```

---

**©2022 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).