



Application Notes for Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.1 with Destiny 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 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.1 to interoperate with Destiny 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 Destiny SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the Destiny 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	31
6.1.	System Manager Login and Navigation.....	32
6.2.	SIP Domain	34
6.3.	Locations	35
6.4.	Adaptations.....	38
6.5.	SIP Entities	40
6.6.	Entity Links	43
6.7.	Routing Policies	45
6.8.	Dial Patterns	47
7.	Configure Avaya Session Border Controller for Enterprise.....	50
7.1.	System Access.....	50
7.2.	Device Management.....	53
7.3.	TLS Management.....	55
7.3.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	55
7.3.2.	Server Profiles.....	57
7.3.3.	Client Profiles	59
7.4.	Network Management.....	61
7.5.	Media Interfaces.....	62
7.6.	Signaling Interfaces.....	64
7.7.	Server Interworking.....	66
7.7.1.	Server Interworking Profile – Enterprise.....	66
7.7.2.	Server Interworking Profile – Service Provider.....	68
7.8.	Signaling Manipulation.....	71
7.9.	Server Configuration	72

7.9.1.	Server Configuration Profile – Enterprise	72
7.9.2.	Server Configuration Profile – Service Provider	74
7.10.	Routing	78
7.10.1.	Routing Profile – Enterprise.....	78
7.10.2.	Routing Profile – Service Provider	79
7.11.	Topology Hiding.....	80
7.11.1.	Topology Hiding Profile – Enterprise.....	80
7.11.2.	Topology Hiding Profile – Service Provider.....	82
7.12.	Domain Policies.....	83
7.12.1.	Application Rules.....	83
7.12.2.	Media Rules.....	84
7.12.3.	Signaling Rules	87
7.13.	End Point Policy Groups	88
7.13.1.	End Point Policy Group – Enterprise	88
7.13.2.	End Point Policy Group – Service Provider.....	89
7.14.	End Point Flows.....	90
7.14.1.	End Point Flow – Enterprise	91
7.14.2.	End Point Flow – Service Provider	92
8.	Destiny SIP Trunking Service Configuration	93
9.	Verification and Troubleshooting	93
9.1.	General Verification Steps	93
9.2.	Communication Manager Verification.....	93
9.3.	Session Manager Verification	94
9.4.	Avaya SBCE Verification	96
10.	Conclusion	103
11.	References.....	103
12.	Appendix A – SigMa Scripts	104

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Destiny network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 8.1 (Communication Manager), Avaya Aura® Session Manager 8.1 (Session Manager), Avaya Session Border Controller for Enterprise 8.1 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Destiny 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” or “Destiny” 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.

For the testing associated with this Application Note, the interface between Avaya systems and the Destiny SIP Trunking service did not include the use of any specific encryption features.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible.

2.1. Interoperability Compliance Testing

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

- Public DNS “SRV” record queries to establish the SIP trunk connections across multiple servers.
- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various Avaya endpoints, including SIP, H.323, digital, and analog telephones at the enterprise. All incoming calls from the PSTN were routed to the simulated enterprise across the SIP Trunk from the service provider’s network.
- Outgoing PSTN calls from Avaya endpoints including SIP, H.323, digital and analog telephones at the enterprise. All outgoing calls to the PSTN were routed from the simulated enterprise across the SIP trunk to the service provider’s network.
- Inbound and outbound PSTN calls to/from Remote Workers using the Avaya Workplace Client for Windows SIP softphone.
- Outgoing calls to the PSTN were routed via the service provider’s network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two-way speech-path. Testing was performed with codecs: G.711A, G.711MU and G.729.
- No matching codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833:
 - Outbound call to PSTN application requiring DTMF (e.g., an IVR or voice mail system).
 - Inbound call from PSTN to Avaya CPE application requiring DTMF (e.g., Aura® Messaging, 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.

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 are supported and that were not tested includes the following:

- Inbound toll-free calls were not tested.
- 0, 0+10 digits, 411 Directory Assistance, 911 Emergency and international calls were not tested.

2.2. Test Results

Interoperability testing of the Destiny 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:

- **Caller ID on transferred calls** – On calls from the PSTN to the enterprise that were transferred back out to the PSTN, the caller ID number displayed at the PSTN endpoints was always of the transferring party instead of the originating PSTN number.
- **Caller ID on call-forward and EC500 calls** – On calls from the PSTN to the enterprise that were forwarded back out to the PSTN, the caller ID number displayed at the PSTN endpoint always showed “Restricted”. This included calls to “twinned” mobile phones (EC500).
- **OPTIONS** – Destiny does not send OPTIONS messages to the Avaya enterprise network, but it does respond to OPTIONS messages it receives from the Avaya enterprise, this was sufficient to maintain the SIP trunk link up in service.
- **Fax support** – Fax call attempts using T.38 were rejected with a “488 Not Acceptable Here” response from Destiny. G.711 fax was also tested, but it behaved unreliably. The issue related to G.711 fax being unreliable during the compliance test may be related to the unpredictability of G.711 techniques, which only works well on networks with very few hops and with limited end-to-end delay.
- **TLS/SRTP used within the enterprise** – When TLS/SRTP is used within the enterprise; the SIP headers include the SIPS URI scheme for Secure SIP. The Avaya SBCE converts these header schemes from SIPS to SIP when it sends the SIP message toward Destiny. However, for call forward and EC500 calls, the Avaya SBCE was not changing the Diversion header scheme as expected. This anomaly is currently under investigation by the Avaya SBCE team. A workaround is to include a SigMa script for the Service Provider Server Configuration profile on the Avaya SBCE to convert “sips” to “sip” in the Diversion header (**Sections 7.8 and 12**).
- **SIP REFER method** – Calls from the PSTN to the enterprise that were transferred back out to the PSTN network using the SIP REFER method did not work properly. On blind transfers, the REFER message was accepted by Destiny with a “202 Accepted message”, but the SIP trunk resources were not released after the call transfer was completed. Testing was done with REFER enabled in Communication Manager (**Network Call Redirection** set to “y” under the **trunk-group**, refer to **Section 5.7**). With REFER

enabled, blind and attended call transfers to the PSTN completed successfully, with the caveat that Communication Manager trunk channels were not released from the call path after the call was transferred; two trunks channels remained busy/connected for the entire duration of the call. There was no impact to the user, it's being mentioned here simply as an observation.

- **Removal of unwanted xml element information from the SDP in SIP messages sent to Destiny** – A Signaling Manipulation script (SigMa) was added to the Avaya SBCE to remove unwanted xml element information from the SDP in SIP messages sent to Destiny. (**Sections 7.8** and **12**).
- **SIP header optimization** – There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider's network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector, AV-Global-Session-ID and P-Location (Refer to **Section 6.4**). To help reduce the packet size further, the Avaya SBCE can remove the “*gsid*” and “*epv*” parameters that may be included within the Contact header by applying a Sigma script to the Destiny server configuration. Refer to **Section 7.8** and **12**.

2.3. Support

For support of Destiny SIP Trunking Service visit the corporate Web page at:
<http://www.destiny.nl>

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 Destiny SIP Trunking Service through a public Internet WAN connection.

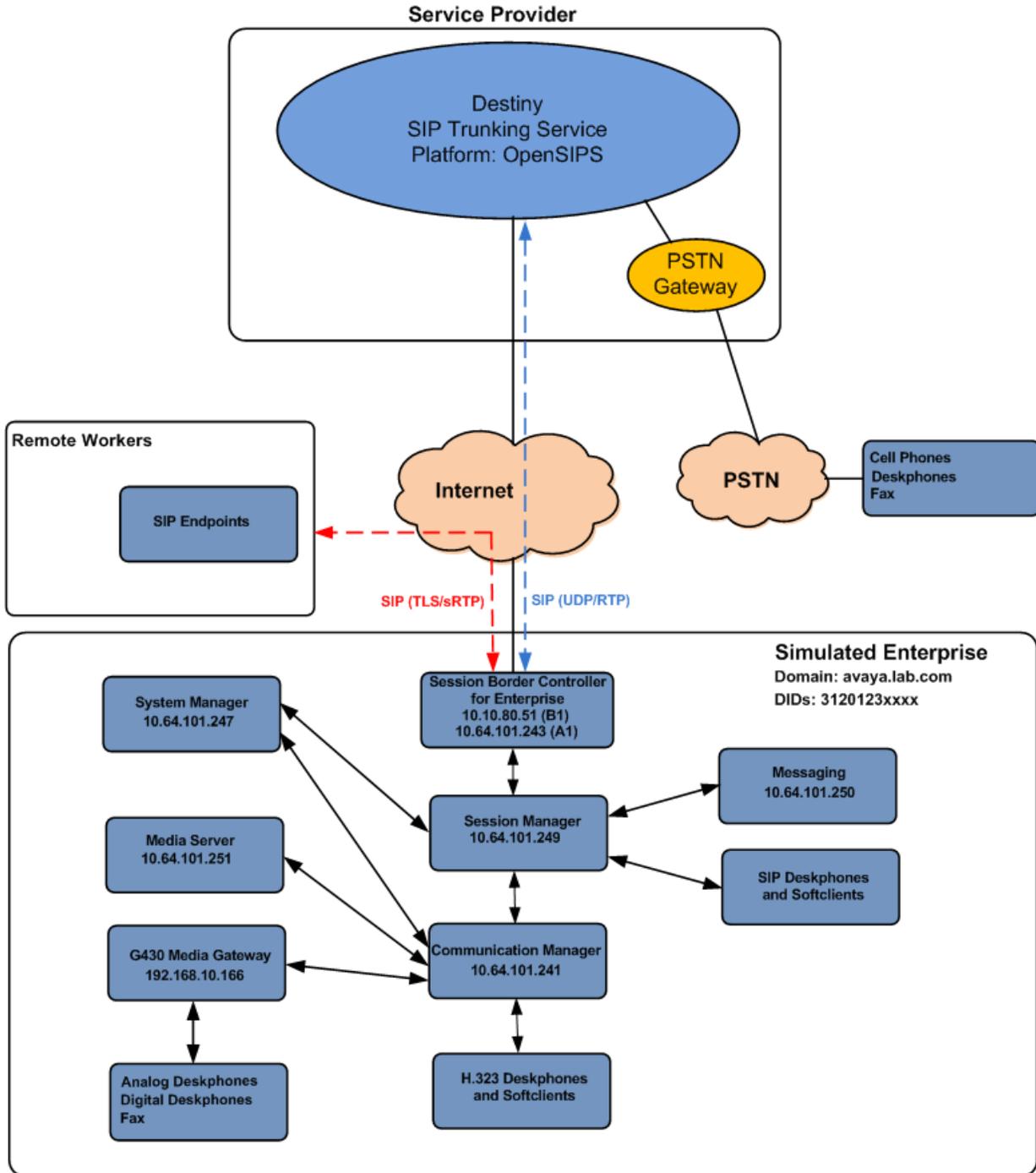


Figure 1: Avaya SIP Enterprise Solution connected to Destiny SIP Trunking Service

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

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

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using Avaya Workplace Client for Windows (SIP). For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on 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 Destiny network.

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

As part of the Avaya Aura® version 8.1 release, Communication Manager incorporates the ability to use the Avaya Aura® Media 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.

The Avaya Aura® Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the Destiny network 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
Avaya	
Avaya Aura® Communication Manager	8.1.2.1.0 (01.0.890.0-26095)
Avaya Aura® Session Manager	8.1.2.0 (8.1.2.0.812039)
Avaya Aura® System Manager	8.1.2.0 Build No. 8.1.0.0.733078 Software Update Rev. No. 8.1.2.0.0611240
Avaya Session Border Controller for Enterprise	ASBCE 8.1.0 8.1.0.0-14-18490
Avaya Session Border Controller for Enterprise patch	sbce-8.1.0.0-14-19116-hotfix-06242020.tar.gz
Avaya Aura® Messaging	7.1 Service Pack 2 (MSG-01.0.532.0-002_0204)
Avaya Aura® Media Server	8.0.2.43 Service Pack 2
Avaya G430 Media Gateway	g430_sw_41_24_0
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.8304
Avaya J179 IP Deskphones (H.323)	Version 6.8304
Avaya J129 IP Deskphones (SIP)	4.0.5.0.10
Avaya one-X® Communicator (H.323, SIP)	6.2.14.6-SP14
Avaya Workplace Client for Windows (SIP)	3.8.4.10.2
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
Destiny	
OpenSIPS	2.2.1 (x86_64/linux)
Asterisk	11.14.0-Destiny3

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

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

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **40000** licenses are available and **120** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

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

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

5.2. System Features

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

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

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

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

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

```
change system-parameters features Page 9 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

DISPLAY TEXT
                                Identity When Bridging: principal
                                User Guidance Display? n
Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
  Local Country Code:
  International Access Code:

SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

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

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

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

5.4. Codecs

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

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

                                IP MEDIA PARAMETERS

Codec Set: 2

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

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

On **Page 2**, set the **Fax Mode** to *off*.

Destiny SIP Trunk supports G.711 for transmission of fax. As this is in-band and requires no interaction from Communication Manager, there is no specific configuration required (refer to **Section 2.2**).

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

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

Media Connection IP Address Type Preferences

- 1: IPv4
- 2:

5.5. IP Network Regions

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

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

```
change ip-network-region 2                                     Page 1 of 20
                                                              IP NETWORK REGION
Region: 2              NR Group: 2
Location: 1           Authoritative Domain: avaya.lab.com
Name: SP Region      Stub Network Region: n
MEDIA PARAMETERS    Intra-region IP-IP Direct Audio: yes
                    Inter-region IP-IP Direct Audio: yes
                    IP Audio Hairpinning? n
Codec Set: 2
UDP Port Min: 2048
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
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
                                                              AUDIO RESOURCE RESERVATION PARAMETERS
                                                              RSVP Enabled? n
```

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

change ip-network-region 2										Page	4	of	20
Source Region: 2										Inter Network Region Connection Management			
										I			M
										G	A		t
dst	codec	direct	WAN-BW-limits		Video	Intervening			Dyn	A	G		c
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L		e
1	2	y	NoLimit						n				t
2	2										all		
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													

5.6. Signaling Group

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

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

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

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

- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *SM*. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to *5071*.
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

```

change signaling-group 2                                     Page 1 of 2
                                                           SIGNALING GROUP

Group Number: 2                                           Group Type: sip
IMS Enabled? n                                           Transport Method: tls
  Q-SIP? n
  IP Video? n                                           Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM                 Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                               Far-end Node Name: SM
Near-end Listen Port: 5071                             Far-end Listen Port: 5071
                                                           Far-end Network Region: 2

Far-end Domain: avaya.lab.com

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

  Audio      Silence      Frames      Packet
  Codec      Suppression  Per Pkt   Size(ms)
1: G.722-64K      -          2         20

```

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**). Note that in the case of Destiny the + sign was removed from SIP messages with a SigMa script added to the Avaya SBCE before sending the SIP messages to Destiny (refer to **Section 7.8** and **12**).
- 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

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

Show ANSWERED BY on Display? y
```

On Page 4:

- Set the **Network Call Redirection** field to **y**. With this setting, Communication Manager will use the SIP REFER method for the redirection of PSTN calls that are transferred back to the SIP trunk (refer to **Section 2.2**).
- Set the **Send Diversion Header** field to **y** and **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101**, the value preferred by Destiny.
- Verify that **Identity for Calling Party Display** is set to **P-Asserted-Identity**.
- Default values were used for all other fields.

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

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

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

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the 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.

change public-unknown-numbering 1				Page 1 of 2	
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	3			4	Total Administered: 5
4	5			4	Maximum Entries: 9999
4	3041	2	31201231111	11	Note: If an entry applies to
4	3042	2	31201232222	11	a SIP connection to Avaya
4	5015	2	31201233333	11	Aura(R) Session Manager,
					the resulting number must
					be a complete E.164 number.
					Communication Manager
					automatically inserts
					a '+' digit in this case.

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Destiny is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 2                               Page 1 of 30
                                INCOMING CALL HANDLING TREATMENT
Service/      Number   Number   Del Insert
Feature       Len     Digits
public-ntwrk  11 31201231111      11 3041
public-ntwrk  11 31201232222      11 3042
public-ntwrk  11 31201233333      11 5015
public-ntwrk
```

5.10.Outbound Routing

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

```

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

```

	Dialed 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 example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2, which contains the SIP trunk group to the service provider.

For international call to the U.S. (e.g., dialing: 90017863311234):

Dialled String		Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
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
10xxx01		14	22	deny	iop		n
10xxx011		15	23	deny	intl		n
10xxx1		16	16	deny	fnpa		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.
- **Numbering Format:** Set to **pub-unk**. All calls using this route pattern will use the public numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

```

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

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

      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

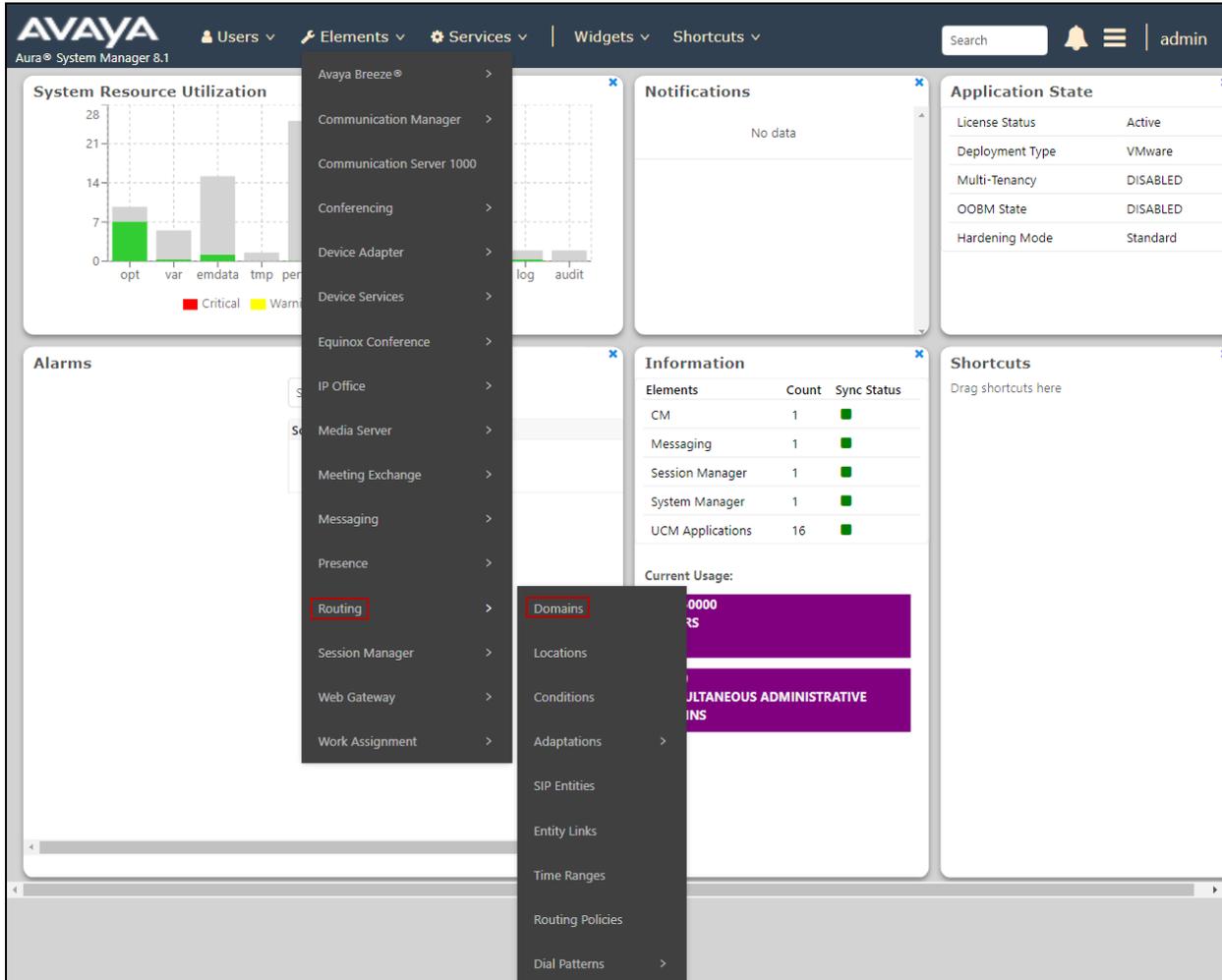
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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 shows the Avaya Aura System Manager 8.1 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 item: "avaya.lab.com" of type "sip" with the note "HG V-Domain". The left navigation pane is expanded to show the "Routing" section, with "Domains" highlighted.

AVAYA
Aura® System Manager 8.1

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

Domain Management

New Edit Delete Duplicate More Actions

1 Item Filter: Enable

<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	avaya.lab.com	sip	HG V-Domain

Select : All, None

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.

The screen below shows the entry for the enterprise domain.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The left-hand navigation pane is expanded to 'Routing' > 'Domains'. The main content area is titled 'Domain Management' and features a toolbar with 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions' buttons. Below the toolbar, there is a table with one item:

Name	Type	Notes
avaya.lab.com	sip	HG V-Domain

At the bottom of the table, there is a 'Select : All, None' option. A 'Filter: Enable' link is also present in the top right corner of the table area.

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 8.1 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 'Location Details' and is divided into several sections:

- General:** Contains fields for '* Name' (filled with 'Session Manager') and 'Notes' (filled with 'VMware Session Manager').
- Dial Plan Transparency in Survivable Mode:** Includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth:** Includes a 'Managed Bandwidth Units' dropdown menu (set to 'Kbit/sec'), 'Total Bandwidth' and 'Multimedia Bandwidth' input fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.

Buttons for 'Commit' and 'Cancel' are located at the top right of the configuration area. A 'Help ?' link is also present.

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 8.1 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 "Location Details" and is divided into several sections:

- General:** Contains fields for * Name (Communication Manager) and Notes (VMware Communication Manager).
- Dial Plan Transparency in Survivable Mode:** Includes an "Enabled" checkbox (unchecked), a "Listed Directory Number" field, and an "Associated CM SIP Entity" field.
- Overall Managed Bandwidth:** Features a "Managed Bandwidth Units" dropdown menu (set to Kbit/sec), "Total Bandwidth" and "Multimedia Bandwidth" input fields, and a checked checkbox for "Audio Calls Can Take Multimedia Bandwidth".

Buttons for "Commit" and "Cancel" are located in the top right corner of the form area. A "Help ?" link is also present.

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 8.1 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 "Location Details" and is divided into several sections:

- General:** Contains fields for "Name" (Avaya SBCE) and "Notes" (VMware Avaya SBCE).
- Dial Plan Transparency in Survivable Mode:** Includes an "Enabled" checkbox (unchecked), a "Listed Directory Number" field, and an "Associated CM SIP Entity" field.
- Overall Managed Bandwidth:** Features a "Managed Bandwidth Units" dropdown menu (set to Kbit/sec), "Total Bandwidth" and "Multimedia Bandwidth" input fields, and a checked checkbox for "Audio Calls Can Take Multimedia Bandwidth".

Buttons for "Commit" and "Cancel" are located in the top right corner of the form area. A "Help ?" link is also present.

6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 8.1 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

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

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

- **Adaptation Name:** Enter an appropriate name.
- **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 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and user information (Users, Elements, Services, Widgets, Shortcuts, Search, admin). The left sidebar shows a navigation menu with 'Adaptations' selected. The main content area is titled 'Adaptation Details' and contains the following sections:

- General:**
 - Adaptation Name:** CM_Outbound_Header_Removal
 - Notes:** (empty text field)
 - Module Name:** DigitConversionAdapter
 - Type:** digit
 - State:** enabled
 - Module Parameter Type:** Name-Value Parameter
- Module Parameters:** A table with columns 'Name' and 'Value'. One entry is visible:

Name	Value
eRHdrs	"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-
- Egress URI Parameters:** (empty text field)
- Digit Conversion for Incoming Calls to SM:** A table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, Notes. It shows 0 items.
- Digit Conversion for Outgoing Calls from SM:** (Section header, no data visible)

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 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The left sidebar shows a navigation tree with 'Routing' selected, and 'SIP Entities' highlighted in blue. The main content area is titled 'SIP Entity Details' and is divided into 'General' and 'Monitoring' sections. The 'General' section contains the following fields:

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

The 'Monitoring' section contains:

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

Buttons for 'Commit' and 'Cancel' are located 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**. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**. Select the **Time Zone**.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also visible. The main content area is titled 'SIP Entity Details' and is divided into three sections: General, Loop Detection, and Monitoring. The General section contains the following fields: Name (Communication Manager Trunk 2), FQDN or IP Address (10.64.101.241), Type (CM), Notes (Used for SP Testing), Adaptation (empty), Location (Communication Manager), Time Zone (America/New_York), SIP Timer B/F (in seconds) (4), Minimum TLS Version (Use Global Setting), Credential name (empty), Securable (unchecked), and Call Detail Recording (none). The Loop Detection section has a Loop Detection Mode (Off). The Monitoring section has SIP Link Monitoring and CRLF Keep Alive Monitoring, both set to Use Session Manager Configuration. A left sidebar shows a navigation menu with 'SIP Entities' selected. Buttons for 'Commit' and 'Cancel' are located at the top right of the configuration area.

Field	Value
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	<input type="checkbox"/>
Call Detail Recording	none
Loop Detection Mode	Off
SIP Link Monitoring	Use Session Manager Configuration
CRLF Keep Alive Monitoring	Use Session Manager Configuration

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

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- On the **Adaptation** field, the adaptation module *CM_Outbound_Header_Removal* previously defined in **Section 6.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- Select the **Time Zone**.

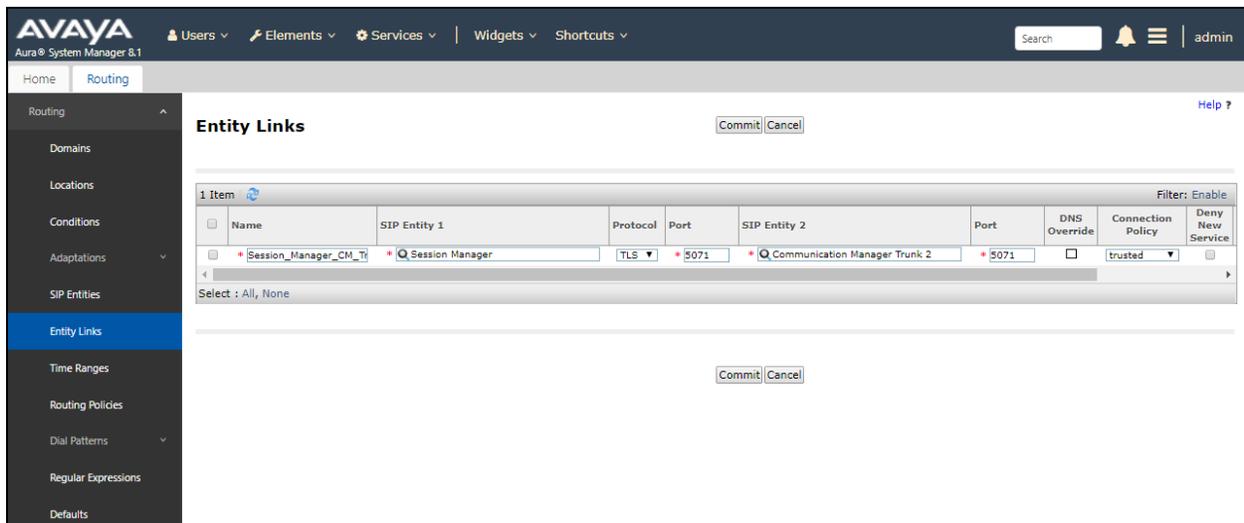
The screenshot displays the 'SIP Entity Details' configuration page in the Avaya Aura System Manager 8.1 interface. The page is organized into three main sections: General, Loop Detection, and Monitoring. The General section contains the following fields: Name (Avaya SBCE), FQDN or IP Address (10.64.101.243), Type (SIP Trunk), Notes (VMware Avaya SBCE), Adaptation (CM_Outbound_Header_Removal), Location (Avaya SBCE), Time Zone (America/New_York), SIP Timer B/F (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (unchecked), and Call Detail Recording (none). The Loop Detection section includes Loop Detection Mode (Off). The Monitoring section includes SIP Link Monitoring (Use Session Manager Configuration) and CRLF Keep Alive Monitoring (Use Session Manager Configuration). The interface also features a navigation menu on the left, a search bar, and a user profile (admin) in the top right corner.

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 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager &1", and various menu items like "Users", "Elements", "Services", "Widgets", and "Shortcuts". A search bar and a user profile "admin" are also visible. The left navigation pane is expanded to "Routing", and "Entity Links" is selected. The main content area is titled "Entity Links" and contains a table with one row of configuration data. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, and Deny New Service. The row shows a name "Session_Manager_CM_Trunk 2", SIP Entity 1 "Session Manager", Protocol "TLS", Port "5071", SIP Entity 2 "Communication Manager Trunk 2", Port "5071", DNS Override "No", Connection Policy "trusted", and Deny New Service "No". There are "Commit" and "Cancel" buttons above and below the table.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
Session_Manager_CM_Trunk 2	Session Manager	TLS	5071	Communication Manager Trunk 2	5071	No	trusted	No

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "Entity Links" and includes "Commit" and "Cancel" buttons. Below the title, there is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, and Deny New Service. The table contains one row with the following data: Name: *Session_Manager_ASBCI, SIP Entity 1: *Session Manager, Protocol: TLS, Port: *5061, SIP Entity 2: *Avaya SBCE, Port: *5061, DNS Override: , Connection Policy: trusted, Deny New Service: . The table also includes a "Filter: Enable" button and a "Select : All, None" dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
*Session_Manager_ASBCI	*Session Manager	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.

Routing Policy Details [Commit] [Cancel] [Help ?]

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication Manager Trunk 2	10.64.101.241	CM	Used for SP Testing

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search admin

Home Routing

Routing Policy Details Commit Cancel Help ?

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.64.101.243	SIP Trunk	VMware Avaya SBCE

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

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 PSTN calls to Communication Manager. In the example, calls to 11-digit numbers starting with **31**, 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 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'Dial Pattern Details' and contains the following fields:

- Pattern:** 31
- Min:** 2
- Max:** 11
- Emergency Call:**
- SIP Domain:** avaya.lab.com
- Notes:** (empty)

Below the form is a section titled 'Originating Locations, Origination Dial Pattern Sets, and Routing Policies' containing 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"/> 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

The interface also includes a sidebar with navigation options like 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Origination Dial...', and 'Regular Expressions'.

The example in this screen shows the 13-digit dialed numbers for outbound calls, beginning with **001**, 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**.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'Dial Pattern Details' and includes a 'Commit' and 'Cancel' button. The 'General' section contains the following fields:

- * Pattern: 001
- * Min: 13
- * Max: 13
- Emergency Call:
- SIP Domain: avaya.lab.com
- Notes: (empty text box)

Below the general section is a table titled 'Originating Locations, Origination Dial Pattern Sets, and Routing Policies'. The table has columns for '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', and 'Routing Policy Notes'. There is one item listed:

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
Communication Manager	VMware Communication Manager			Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE

The interface also includes a sidebar with navigation options like 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'Routing Policies' option is currently selected.

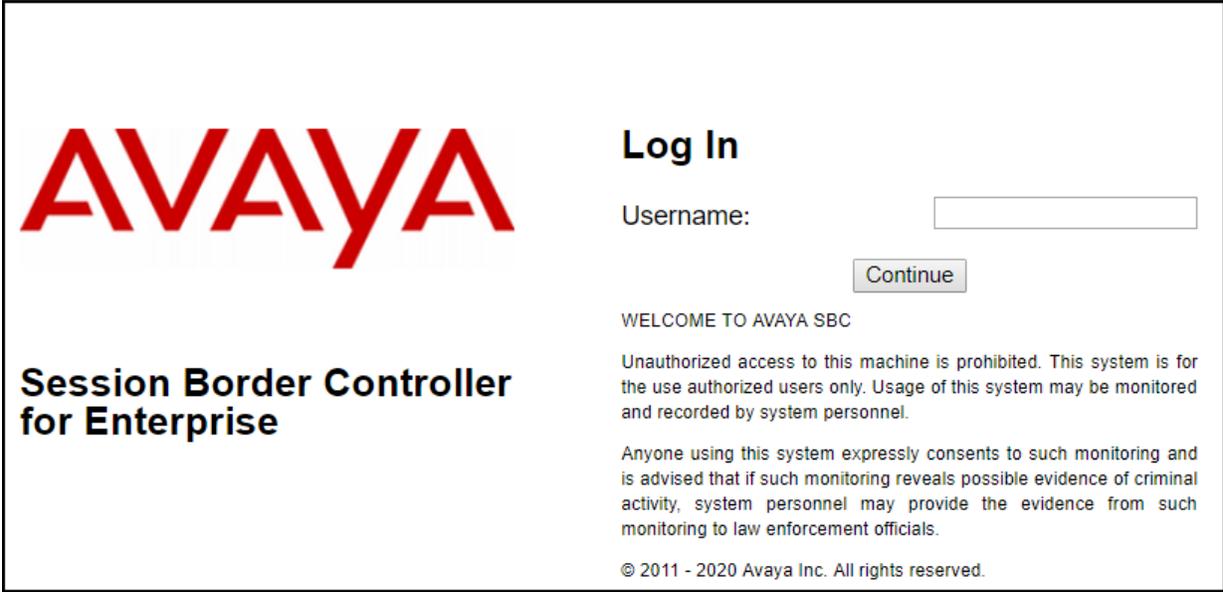
Repeat the above procedures as needed to define additional dial patterns.

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.

7.1. System Access

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



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, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a warning about unauthorized access, a consent statement, and a copyright notice: "© 2011 - 2020 Avaya Inc. All rights reserved."

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 Enterprise. The top navigation bar includes 'Device: EMS', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar shows 'EMS' with 'Avaya_SBCE' selected, and a menu for 'EMS Dashboard' including 'Device Management', 'System Administration', 'Backup/Restore', and 'Monitoring & Logging'. The main content area is titled 'Dashboard' and contains several sections: '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 EMS and Avaya_SBCE), 'Active Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (None found), and 'Notes' (No notes found). An 'Add' button is located at the bottom right of the dashboard area.

Information	
System Time	10:03:00 AM EDT Refresh
Version	8.1.0.0-14-18490
GUI Version	8.1.0.0-18490
Build Date	Mon Feb 03 17:23:09 UTC 2020
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/24/2020 09:03:43 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours): None found.

Incidents (past 24 hours): None found.

Notes: No notes found.

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 displays the Avaya SBCE 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 reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right.

The left sidebar, titled 'EMS Dashboard', lists the following menu items: Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.

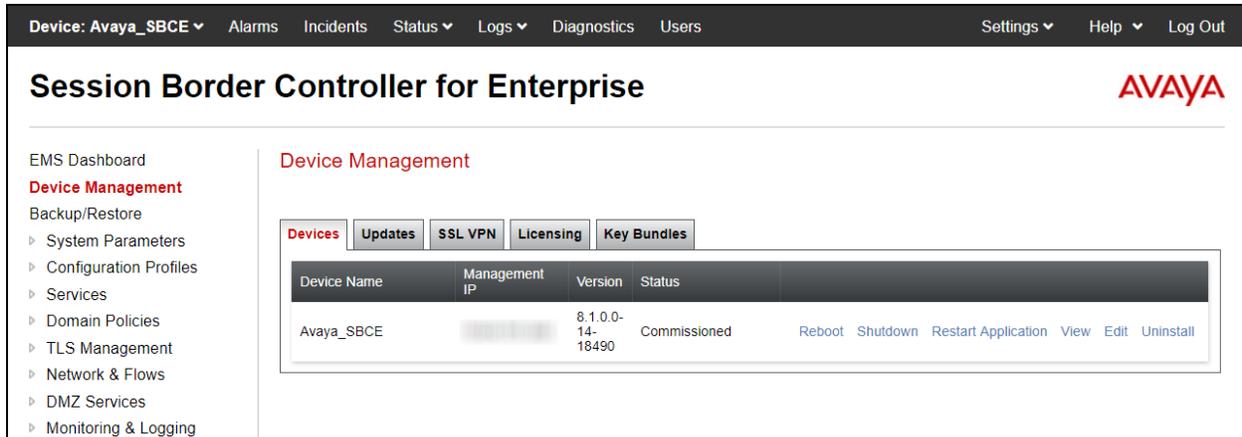
The main content area is titled 'Dashboard' and contains several panels:

- Information:** A table with the following data:

System Time	10:05:18 AM EDT	Refresh
Version	8.1.0.0-14-18490	
GUI Version	8.1.0.0-18490	
Build Date	Mon Feb 03 17:23:09 UTC 2020	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/24/2020 09:03:43 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):** None found. An 'Add' button is located to the right of this panel.
- Notes:** No notes found.

7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named *Avaya_SBCE* is shown. The management IP address that was configured during installation is blurred out for security 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 displays the Avaya Session Border Controller for Enterprise interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main heading is 'Session Border Controller for Enterprise' with the AVAYA logo. The left sidebar lists navigation options: EMS Dashboard, Device Management (highlighted), Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Device Management' and contains tabs for 'Devices', 'Updates', 'SSL VPN', 'Licensing', and 'Key Bundles'. The 'Devices' tab is active, showing a table with the following data:

Device Name	Management IP	Version	Status						
Avaya_SBCE	[Blurred]	8.1.0.0-14-18490	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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

The highlighted IP addresses in the **System Information** screen shown below are the ones used for the SIP trunk to Destiny 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.

System Information: Avaya_SBCE

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 1000	1000
Advanced Sessions Requested: 1000	1000
Scopio Video Sessions Requested: 500	500
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 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)	
--------------	--

7.3. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

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.

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.

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

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



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

- 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.

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', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left, a sidebar menu lists various management options, with 'TLS Management' and 'Certificates' highlighted. The main content area is titled 'Certificates' and features 'Install' and 'Generate CSR' buttons. It contains several sections: 'Installed Certificates' with entries like 'sbce_inside.pem'; 'Installed CA Certificates' with entries like 'default.pem'; 'Installed Certificate Revocation Lists' with a message 'No certificate revocation lists have been installed.'; 'Installed Certificate Signing Requests' with entry 'sbceExternal.req'; and 'Installed Keys' with entry 'sbce_inside.key'. Each entry includes 'View' and 'Delete' links.

7.3.2. 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., **sbce_inside.pem**, from pull down menu.
- **Peer Verification = None.**
- 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 warning message in an orange box: "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." Below this, a smaller orange box states: "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." The main configuration area is divided into two sections: "TLS Profile" and "Certificate Verification". Under "TLS Profile", there are four fields: "Profile Name" (text input with "Inside_Server"), "Certificate" (dropdown menu with "sbce_inside.pem"), "SNI Options" (dropdown menu with "None"), and "SNI Group" (dropdown menu with "None"). Under "Certificate Verification", there are four fields: "Peer Verification" (dropdown menu with "None"), "Peer Certificate Authorities" (list box containing "Avaya_EP_CA_cert.pem", "DigiCertGlobalRootCA.cer", "GeoTrust_Global_CA_Trust.cer", and "default.pem"), "Peer Certificate Revocation Lists" (empty list box), and "Verification Depth" (text input with "0"). A "Next" button is located at the bottom center of the window.

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 the following items: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates, Client Profiles, **Server Profiles** (highlighted), SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled 'Server Profiles: Inside_Server'. It features an 'Add' button and a 'Delete' button. Below these is a blue bar with the text 'Click here to add a description.' A 'Server Profile' tab is active, showing the configuration for the 'Inside_Server' profile.

TLS Profile	
Profile Name	Inside_Server
Certificate	sbce_inside.pem
SNI Options	None

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
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:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

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

7.3.3. 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., **sbce_inside.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 the 'Edit Profile' window with the following configuration:

- 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:
 - Certificate:
 - SNI: Enabled
- Certificate Verification:**
 - Peer Verification: Required
 - Peer Certificate Authorities:
 - Peer Certificate Revocation Lists:
 - Verification Depth:
 - Extended Hostname Verification:
 - Server Hostname:
- Next** button

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.

The left sidebar contains a navigation menu with the following items: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (expanded), Certificates, **Client Profiles** (highlighted), Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled 'Client Profiles: Inside_Client' and features an 'Add' button and a 'Delete' button. A blue bar contains the text 'Click here to add a description.' Below this, the 'Client Profile' configuration form is shown, which is divided into several sections:

- TLS Profile**: Profile Name (Inside_Client), Certificate (sbce_inside.pem), SNI (Enabled).
- Certificate Verification**: Peer Verification (Required), Peer Certificate Authorities (default.pem), Peer Certificate Revocation Lists (---), Verification Depth (1), Extended Hostname Verification (disabled).
- Renegotiation Parameters**: Renegotiation Time (0), Renegotiation Byte Count (0).
- Handshake Options**: Version (TLS 1.2 selected), Ciphers (Default selected), Value (HIGH:IDH:IADH:IMD5:1aNULL:1eNULL:@STRENGTH).

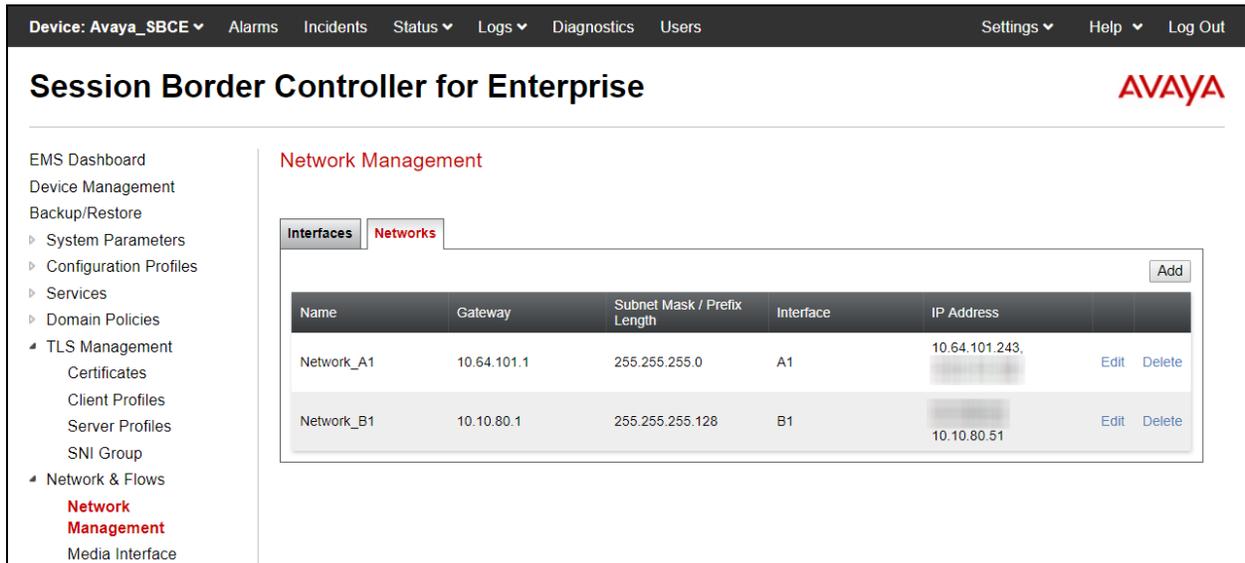
An 'Edit' button is located at the bottom of the configuration form.

7.4. Network Management

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

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

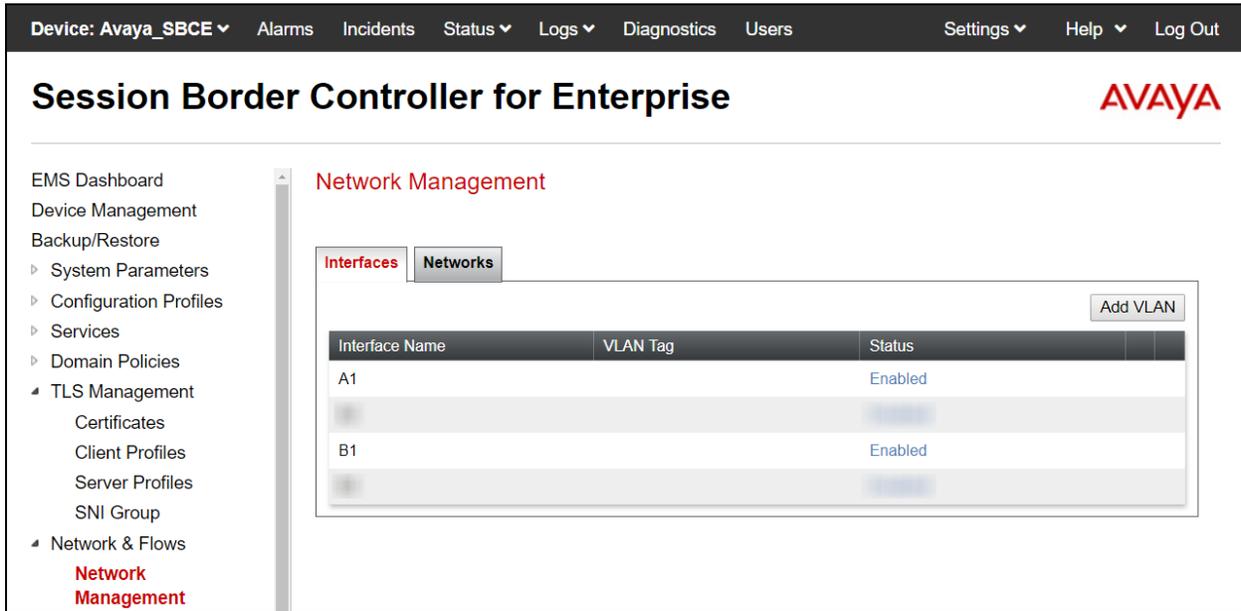
Note that in the configuration used during the compliance test, the IP addresses assigned to the private (**10.64.101.243**) and public (**10.10.80.51**) sides of the Avaya SBCE are the ones relevant to these Application Notes.



The screenshot displays 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 features two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, showing a table with the following data:

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Network_A1	10.64.101.1	255.255.255.0	A1	10.64.101.243	Edit	Delete
Network_B1	10.10.80.1	255.255.255.128	B1	10.10.80.51	Edit	Delete

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.



7.5. Media Interfaces

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

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

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

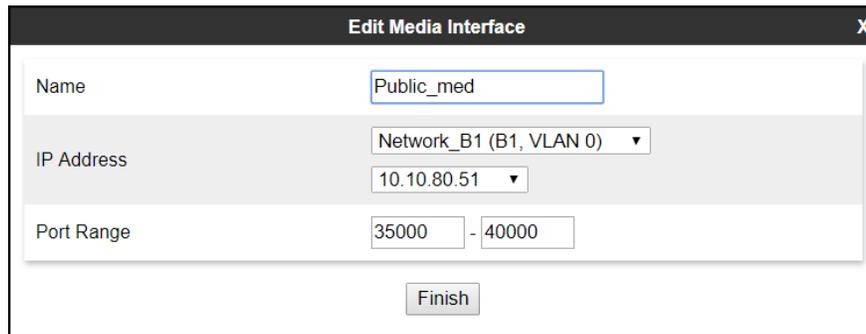
The screenshot shows the 'Edit Media Interface' dialog box. It contains the following fields and values:

- Name:** Private_med
- IP Address:** Network_A1 (A1, VLAN 0) (selected in a dropdown menu), 10.64.101.243 (selected in a dropdown menu)
- Port Range:** 35000 - 40000

A 'Finish' button is located at the bottom of the dialog box.

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

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



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 "Public_med".
- IP Address:** A dropdown menu showing "Network_B1 (B1, VLAN 0)" with a downward arrow. Below it, a sub-dropdown menu shows "10.10.80.51" with a downward arrow.
- Port Range:** Two text input fields, the first containing "35000" and the second containing "40000", separated by a hyphen.
- Finish:** A button located at the bottom center of the dialog.

7.6. Signaling Interfaces

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

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

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface, in the example *Private_sig* was used.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**.
- Select a **TLS Profile** defined in **Section 7.3.2**.
- Click **Finish**.

Name	Private_sig
IP Address	Network_A1 (A1, VLAN 0) 10.64.101.243
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	Inside_Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

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

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

7.7. Server Interworking

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

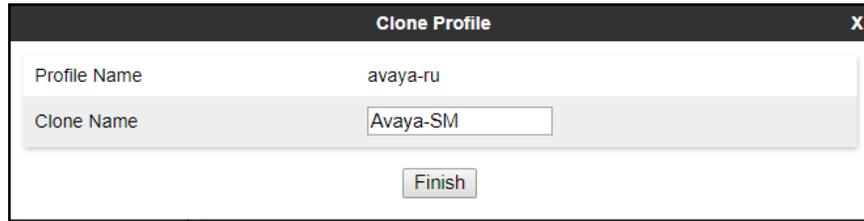
7.7.1. Server Interworking Profile – Enterprise

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

The screenshot shows the configuration page for the Session Border Controller for Enterprise, specifically for the Interworking Profiles: avaya-ru. The interface includes a top navigation bar with options like Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main content area is divided into a left navigation pane and a main configuration area. The left pane shows a tree view with 'Configuration Profiles' expanded to 'Server Interworking'. The main area displays a list of interworking profiles, with 'avaya-ru' selected. Below the list is a configuration table for the 'General' tab, which includes settings for various SIP-related parameters.

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	

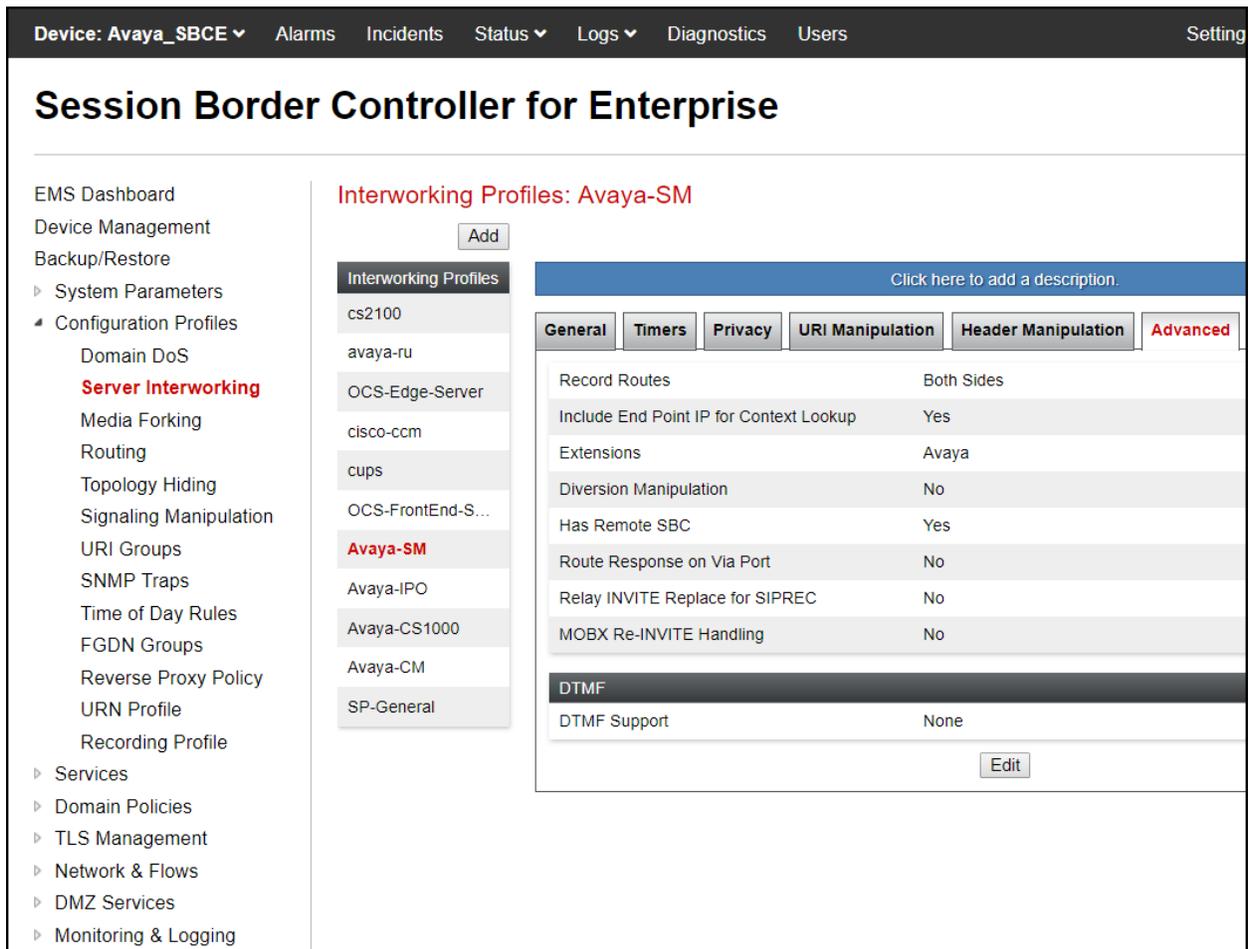
- Enter a descriptive name for the cloned profile.
- Click **Finish**.



The image shows a 'Clone Profile' dialog box with the following fields and buttons:

- Profile Name: avaya-ru
- Clone Name: Avaya-SM
- Finish button

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



The screenshot shows the configuration page for the Session Border Controller for Enterprise. The page title is 'Session Border Controller for Enterprise'. The left sidebar contains a navigation menu with the following items:

- EMS Dashboard
- 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
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

The main content area is titled 'Interworking Profiles: Avaya-SM'. It features an 'Add' button and a list of interworking profiles:

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

The 'Avaya-SM' profile is selected, and its configuration is shown in a table with the following tabs: General, Timers, Privacy, URI Manipulation, Header Manipulation, and **Advanced**.

Setting	Value
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
DTMF	
DTMF Support	None

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

7.7.2. Server Interworking Profile – Service Provider

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

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



The screenshot shows a configuration window titled "Interworking Profile". It has a close button "X" in the top right corner. The main area contains a text input field labeled "Profile Name" with the text "SP-General" entered. Below the input field 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).

Interworking Profile
X

General

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	<input type="text" value="None"/>
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

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

Device: Avaya_SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Setting

Session Border Controller for Enterprise

- EMS Dashboard
- 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
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Interworking Profiles: SP-General

Interworking Profiles

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

Click here to add a description.

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

DTMF

DTMF Support	None
--------------	------

7.8. Signaling Manipulation

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

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

A single Sigma script was created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- Remove + sign from SIP messages before sending to Destiny.
- Remove unwanted “gsid” and “epv” parameter from being sent to the Service Provider in the Contact header.
- Remove the P-Location parameter from being sent to the Service Provider.
- Change the Diversion header scheme from SIPS to SIP.
- Remove unwanted xml element information from the SDP in SIP messages sent to the Service Provider.

The scripts will later be applied to the Server Configuration profile corresponding to the Service Provider (toward Destiny) in **Section 7.9.2**.

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

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

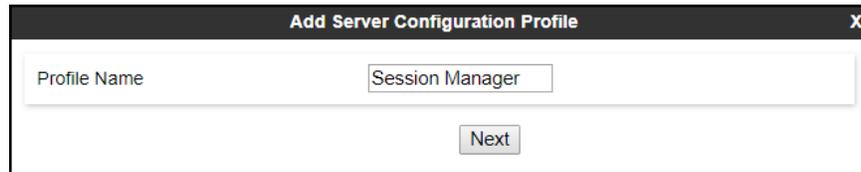
7.9. Server Configuration

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

7.9.1. Server Configuration Profile – Enterprise

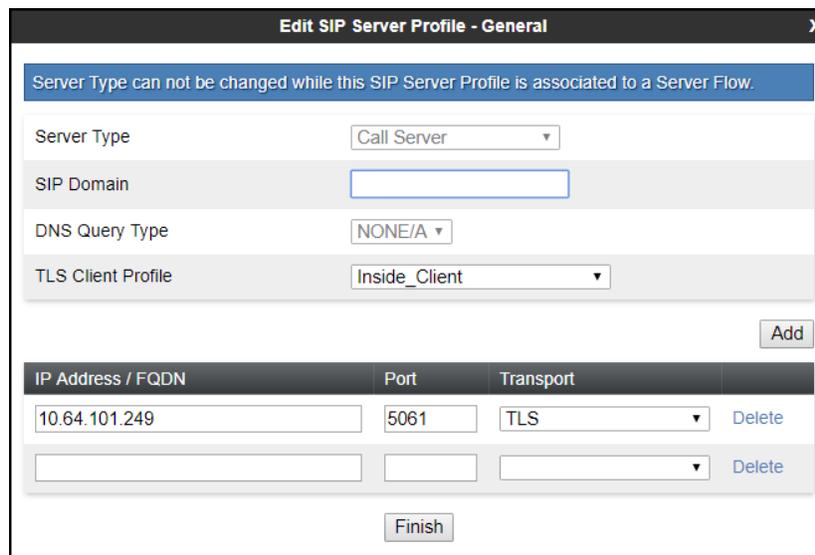
From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

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



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

- 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** defined in **Section 7.3.3**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit SIP Server Profile - General". It has a close button (X) in the top right corner. Below the title bar, there is a blue warning banner that reads "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below the banner, there are several fields: "Server Type" (Call Server), "SIP Domain" (empty), "DNS Query Type" (NONE/A), and "TLS Client Profile" (Inside_Client). There is an "Add" button to the right of these fields. Below these fields is a table with columns "IP Address / FQDN", "Port", and "Transport". The first row contains "10.64.101.249", "5061", and "TLS". There is a "Delete" button to the right of each row. At the bottom of the dialog is a "Finish" button.

IP Address / FQDN	Port	Transport	
10.64.101.249	5061	TLS	Delete
			Delete

- 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**.
 - Select **Avaya-SM** from the **Interworking Profile** drop-down menu (**Section 7.7.1**).
- Click **Finish**.

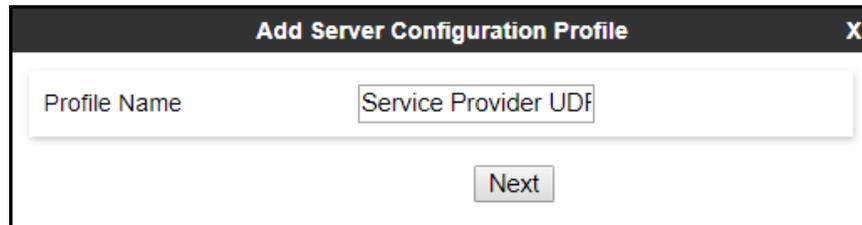
Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None

Finish

7.9.2. Server Configuration Profile – Service Provider

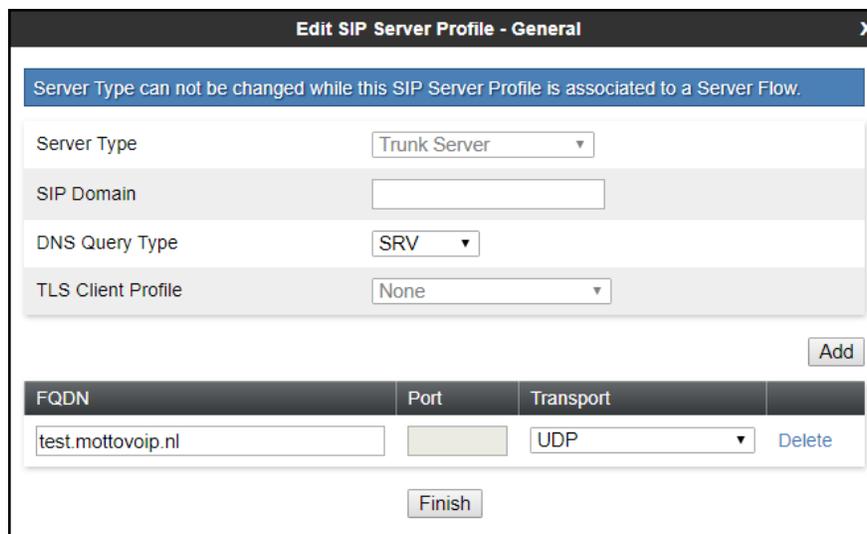
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below (*Service Provider UDP* 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 "Service Provider UDP". 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**.
- Select *SRV* from the drop-down menu for **DNS Query Type**.
- On the **IP Addresses / FQDN** field, enter *test.mottovoip.nl* (Destiny SIP proxy server FQDN). This information was provided by Destiny.
- Select *UDP* for **Transport** (note the port cannot be enter since SRV was selected for **DNS Query Type**, the port being used will be collected from the DNS response).
- Click **Next**.



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. A blue banner at the top reads "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several fields: "Server Type" (Trunk Server), "SIP Domain" (empty), "DNS Query Type" (SRV), and "TLS Client Profile" (None). An "Add" button is located to the right of the "TLS Client Profile" field. Below these fields is a table with columns for "FQDN", "Port", "Transport", and "Delete". The table contains one row with "test.mottovoip.nl" in the FQDN column, an empty Port column, "UDP" in the Transport column, and a "Delete" button. A "Finish" button is located at the bottom of the dialog.

FQDN	Port	Transport	Delete
test.mottovoip.nl		UDP	Delete

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**.

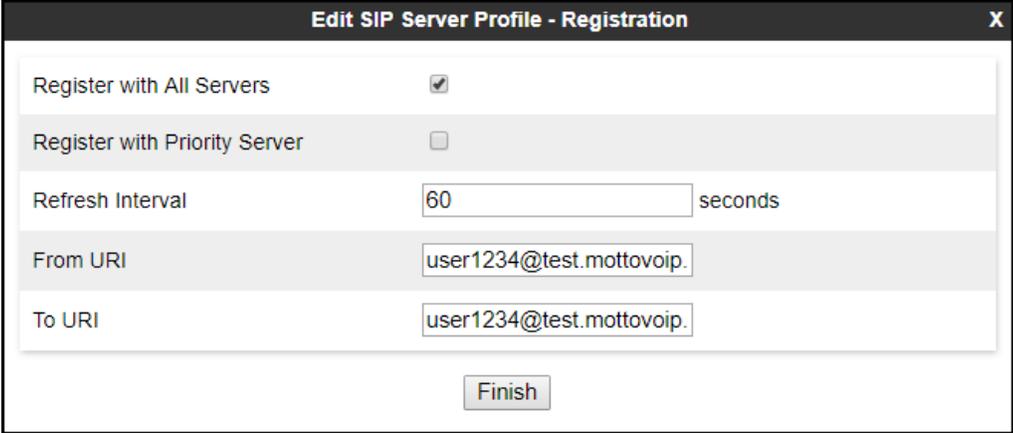
The screenshot shows a window titled "Edit SIP Server Profile - Authentication". Inside the window, there is a form with the following elements:

- Enable Authentication**: A checkbox that is checked.
- User Name**: A text input field containing the value "user1234".
- Realm**: A text input field with the placeholder text "(Leave blank to detect from server challenge)".
- Password**: A text input field with the placeholder text "(Leave blank to keep existing password)".
- Confirm Password**: A text input field.
- Finish**: A button located at the bottom right of the form area.

- 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. **60** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI:** Use the **User Name** entered above in the **Authentication** screen (user1234) and the Service Provider's SIP proxy server FQDN (**test.mottovoip.nl**), as shown on the screen below.
 - **To URI:** Use the **User Name** entered above in the **Authentication** screen (user1234) and the Service Provider's SIP proxy server FQDN (**test.mottovoip.nl**), as shown on the screen below.
 - Click **Next**.

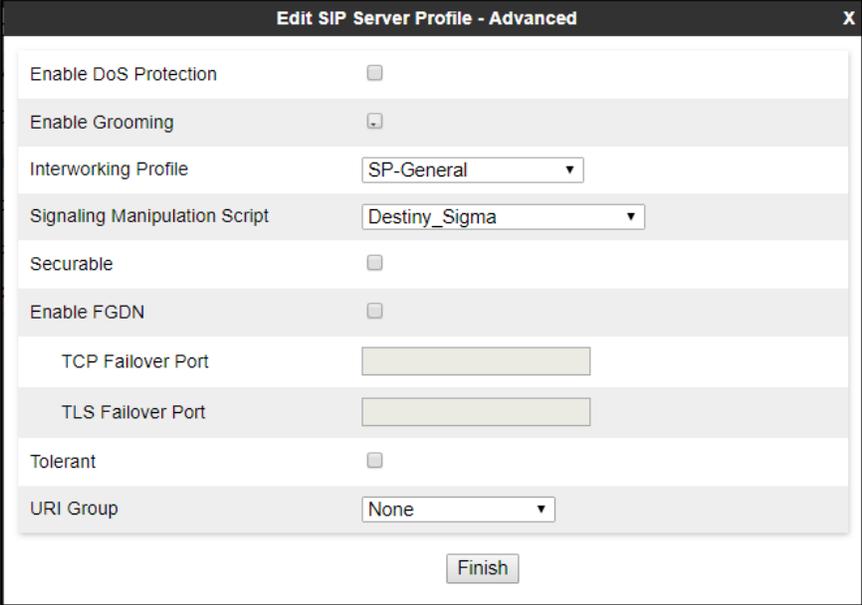


Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	<input type="text" value="60"/> seconds
From URI	<input type="text" value="user1234@test.mottovoip."/>
To URI	<input type="text" value="user1234@test.mottovoip."/>

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

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

- Uncheck **Enable Grooming**.
- Select **SP-General** from the **Interworking Profile** drop-down menu (**Section 7.7.2**).
- Select the **Destiny_Sigma** from the **Signaling Manipulation Script** drop down menu (**Sections 7.8 and 12**).
- Click **Finish**.



The screenshot shows a window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General ▼
Signaling Manipulation Script	Destiny_Sigma ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

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

7.10.Routing

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

7.10.1. Routing Profile – Enterprise

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

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

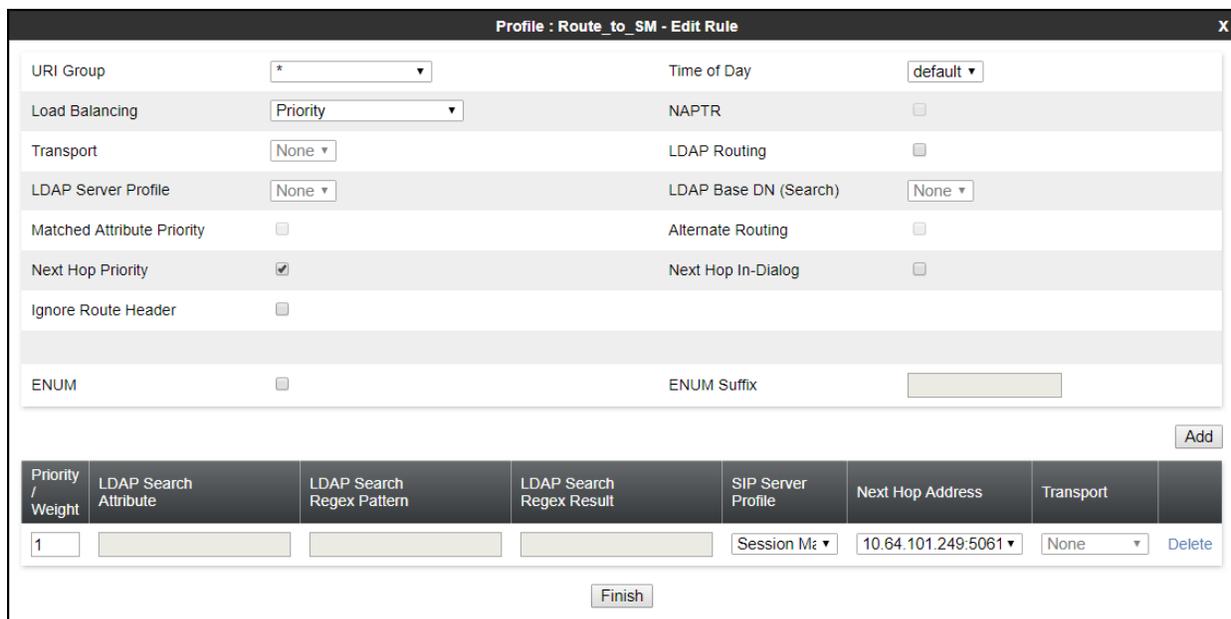


Routing Profile

Profile Name: Route_to_SM

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 7.9.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



Profile : Route_to_SM - Edit Rule

URI Group: * Time of Day: default

Load Balancing: Priority NAPTR:

Transport: None LDAP Routing:

LDAP Server Profile: None LDAP Base DN (Search): None

Matched Attribute Priority: Alternate Routing:

Next Hop Priority: Next Hop In-Dialog:

Ignore Route Header:

ENUM: ENUM Suffix:

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session Mz	10.64.101.249:5061	None	Delete

Finish

7.10.2. Routing Profile – Service Provider

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

- Enter an appropriate **Profile Name** similar to the example below (*Route_to_SP_UDP* was used).
- Click **Next**.

- Under **Load Balancing** select *DNS/SRV*.
- Click the **Add** button to enter the next-hop address.
- Under **SIP Server Profile**, select *Service Provider UDP*. The **Next Hop Address** is populated automatically with *test.mottovoip.nl:5060 (UDP)*. Destiny SIP Proxy FQDN, Port and Transport, Server Configuration Profile defined in **Section 7.9.2**.
- Defaults were used for all other parameters.
- Click **Finish**

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
0				Service Prc	test.mottovoip.nl (U)	None	Delete

7.11. Topology Hiding

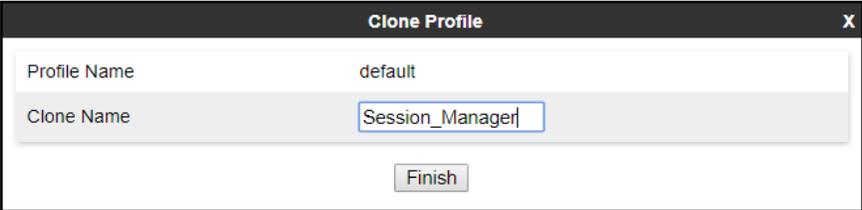
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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

7.11.1. Topology Hiding Profile – Enterprise

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

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



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

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

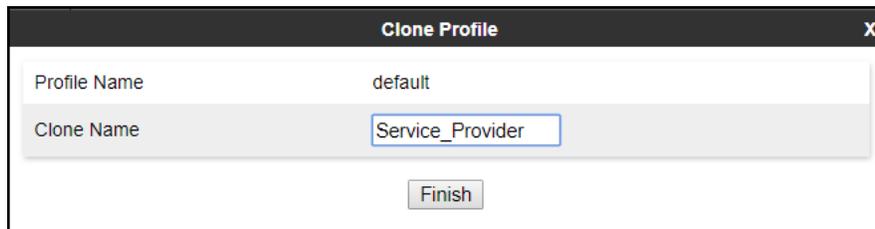
- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain *avaya.lab.com*, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**.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

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

7.11.2. 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.

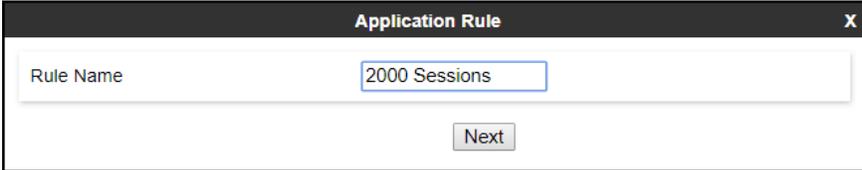
7.12.Domain Policies

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

7.12.1.Application Rules

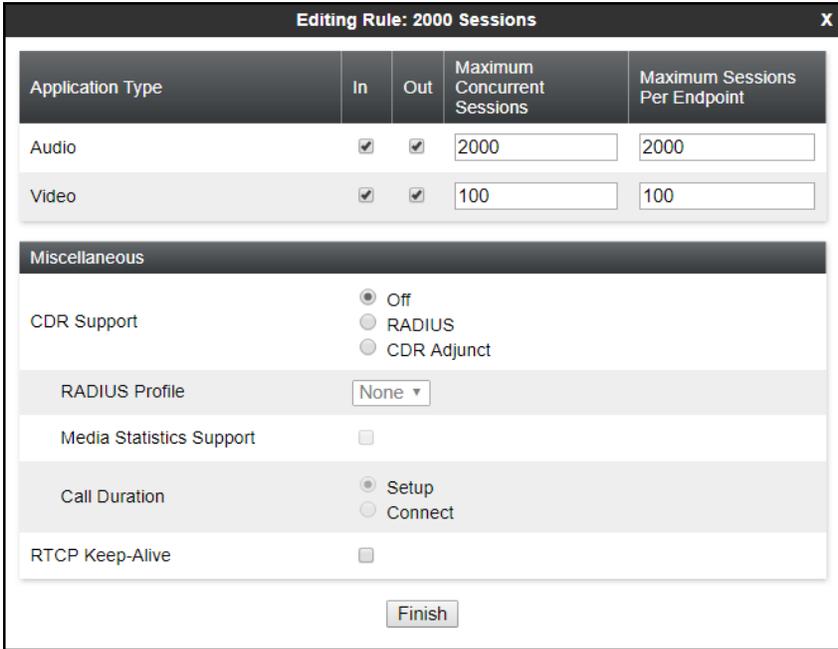
Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice sessions the network will process in order to prevent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

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



The screenshot shows a window titled "Application Rule" with a close button (X) in the top right corner. Below the title bar, there is a text input field labeled "Rule Name" containing the text "2000 Sessions". Below the input field, there 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, the value of **100** for Video was used for the test.
- Click **Finish**.



The screenshot shows a window titled "Editing Rule: 2000 Sessions" with a close button (X) in the top right corner. Below the title bar, there is a table with the following columns: Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The table has two rows: Audio and Video. Below the table, there is a "Miscellaneous" section with several options: CDR Support (radio buttons for Off, RADIUS, CDR Adjunct), RADIUS Profile (dropdown menu set to None), Media Statistics Support (checkbox), Call Duration (radio buttons for Setup, Connect), and RTCP Keep-Alive (checkbox). At the bottom of the window, there is a "Finish" button.

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

Miscellaneous

CDR Support: Off, RADIUS, CDR Adjunct

RADIUS Profile: None

Media Statistics Support:

Call Duration: Setup, Connect

RTCP Keep-Alive:

7.12.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, 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*.
- Repeat the above steps under Video Encryption, if needed.
- Under Miscellaneous verify that *Capability Negotiation* is checked.
- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish**

Media Encryption X

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▾
Preferred Format #2	RTP ▾
Preferred Format #3	NONE ▾
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
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"/>

Video Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▾
Preferred Format #2	RTP ▾
Preferred Format #3	NONE ▾
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
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"/>

Miscellaneous

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

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

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

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

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

7.12.3. Signaling Rules

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

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 sidebar contains a navigation menu with categories like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'Charging Rules', 'End Point Policy Groups', 'Session Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Signaling Rules' option is highlighted in red.

The main content area is titled 'Signaling Rules: default' and includes an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'General' tab is active, showing configuration for 'Inbound' and 'Outbound' traffic. The 'Content-Type Policy' section is also visible, with 'Enable Content-Type Checks' checked and 'Action' set to 'Allow'.

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	Multipart Action	Allow
Exception List		Exception List	

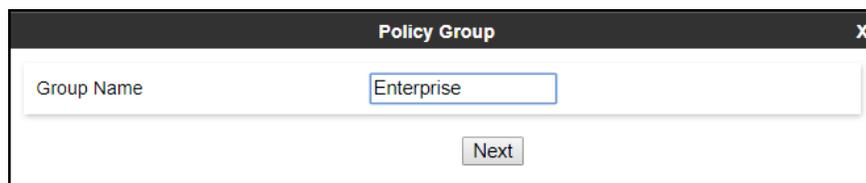
7.13. End Point Policy Groups

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

7.13.1. End Point Policy Group – Enterprise

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

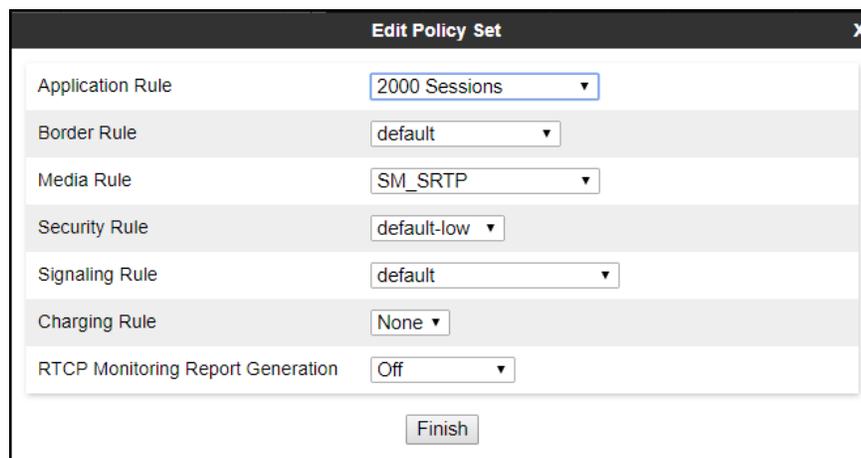
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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 7.12.1).
- **Border Rule:** *default*.
- **Media Rule:** *SM_SRTP* (Section 7.12.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.12.3).
- 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:

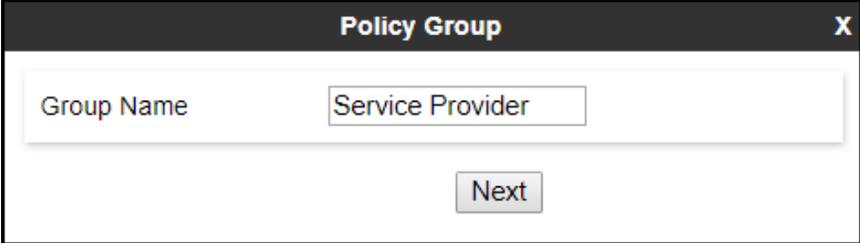
Application Rule	2000 Sessions
Border Rule	default
Media Rule	SM_SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

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

7.13.2. End Point Policy Group – Service Provider

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

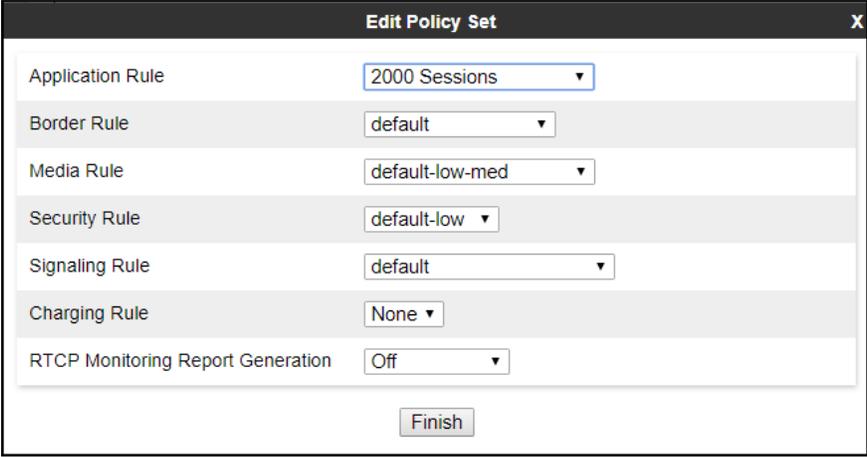
- Enter an appropriate name in the **Group Name** field (*Service Provider* was used).
- Click **Next**.



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 7.12.1).
- **Border Rule:** *default*.
- **Media Rule:** *default-low-med* (Section 7.12.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.12.3).
- Click **Finish**.



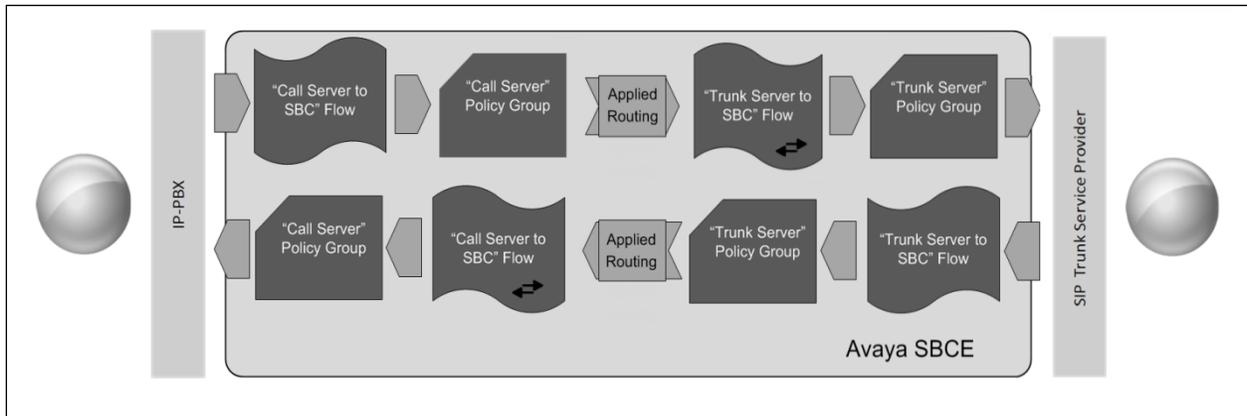
The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains several rows, each with a label and a dropdown menu:

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".

7.14. End Point Flows

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



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

7.14.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named *Session_Manager_Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.10.2**, which is the reverse route of the flow. Click **Finish**.

Field	Value
Flow Name	Session_Manager_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	Route_to_SP_UDP
Topology Hiding Profile	Session_Manager
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

Finish

7.14.2. End Point Flow – Service Provider

A second Server Flow with the name *SIP_Trunk_Flow_UDP* was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.10.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.

Edit Flow: SIP_Trunk_Flow_UDP	
Flow Name	SIP_Trunk_Flow_UDP
SIP Server Profile	Service Provider UDP
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"/>
<input type="button" value="Finish"/>	

8. Destiny SIP Trunking Service Configuration

To use Destiny SIP Trunking Service, a customer must request the service from Destiny using the established sales processes. The process can be started by contacting Destiny via the corporate web site at: <http://www.destiny.nl>

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

Destiny will provide the following information:

- Destiny's SIP Proxy FQDN to be used for public DNS SRV record queries.
- SIP Trunk registration credentials (User Name, Password, etc.).
- DID numbers.
- Public DNS IP addresses.
- Etc.

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

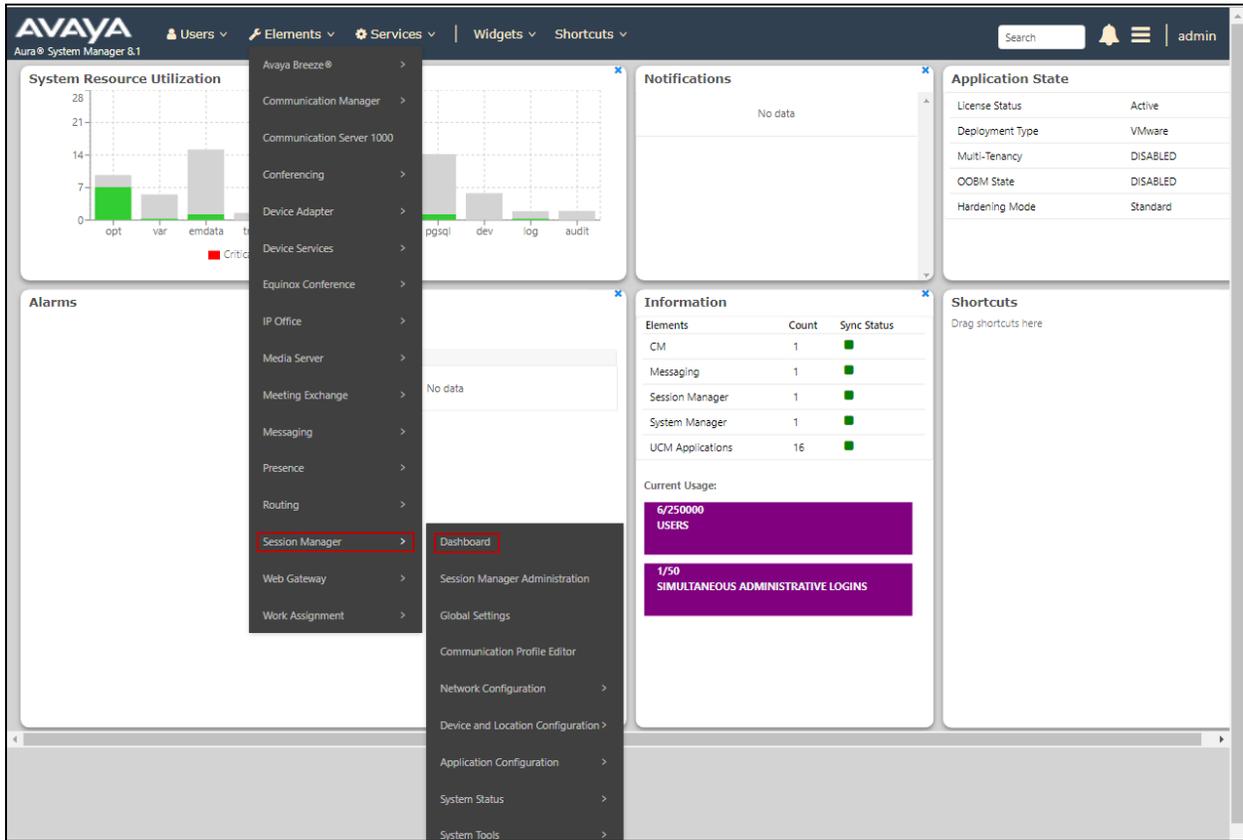
The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **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 **1** alarm out of the **7** Entities defined.

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
Session Manager	Core	✓	0/0/0	Up	Accept New Service	1/7	0	0/0	✓	✓	Normal	Disabled	8.1.2.0.812039

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

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

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 displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main dashboard area is titled 'Session Border Controller for Enterprise' and features the AVAYA logo. The left sidebar shows the 'EMS Dashboard' with various management options. The main content area is divided into several sections: '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' (EMS, Avaya_SBCE), 'Active Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (None found), and 'Notes' (No notes found). A red arrow points to the 'Alarms' menu item in the top navigation bar.

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

Device: EMS ▾ Help

Alarm Viewer AVAYA

Alarms

<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

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

The following screen shows the Incident Viewer page.

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

Session Border Controller for Enterprise AVAYA

Device: Avaya_SBCE | Alarms | Incidents | **Status** | Logs | Diagnostics | Users | Settings | Help | Log Out

EMS Dashboard

- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging

Dashboard

Information

System Time	11:08:24 AM EDT	Refresh
Version	8.1.0.0-14-18490	
GUI Version	8.1.0.0-18490	
Build Date	Mon Feb 03 17:23:09 UTC 2020	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/24/2020 10:39:59 EDT	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya_SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found. [Add](#)

Notes
No notes found.

Device: Avaya_SBCE | Help

Status AVAYA

Server Status

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Service Provider UDP	...mottovoip.nl	...215.228	5060	UDP	UNKNOWN	REGISTERED	08/28/2020 09:09:06 EDT
Service Provider UDP	...mottovoip.nl	...192.231	5060	UDP	UNKNOWN	REGISTERED	08/28/2020 09:09:06 EDT

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity. Note that public Server IPs were blurred out for security reasons.

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. At the top, there is a navigation bar with 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics' (highlighted with a red arrow), 'Users', 'Settings', 'Help', and 'Log Out'. The main header includes the title 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The dashboard is divided into several sections:

- EMS Dashboard:** A sidebar menu with options like Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.
- Dashboard Information:** A table showing system details:

System Time	11:08:24 AM EDT	Refresh
Version	8.1.0.0-14-18490	
GUI Version	8.1.0.0-18490	
Build Date	Mon Feb 03 17:23:09 UTC 2020	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/24/2020 10:39:59 EDT	
Failed Login Attempts	0	
- Installed Devices:** A list showing 'Avaya_SBCE' under the 'EMS' category.
- Active Alarms (past 24 hours):** A section stating 'None found.'
- Incidents (past 24 hours):** A section stating 'None found.'
- Notes:** A section at the bottom stating 'No notes found.'

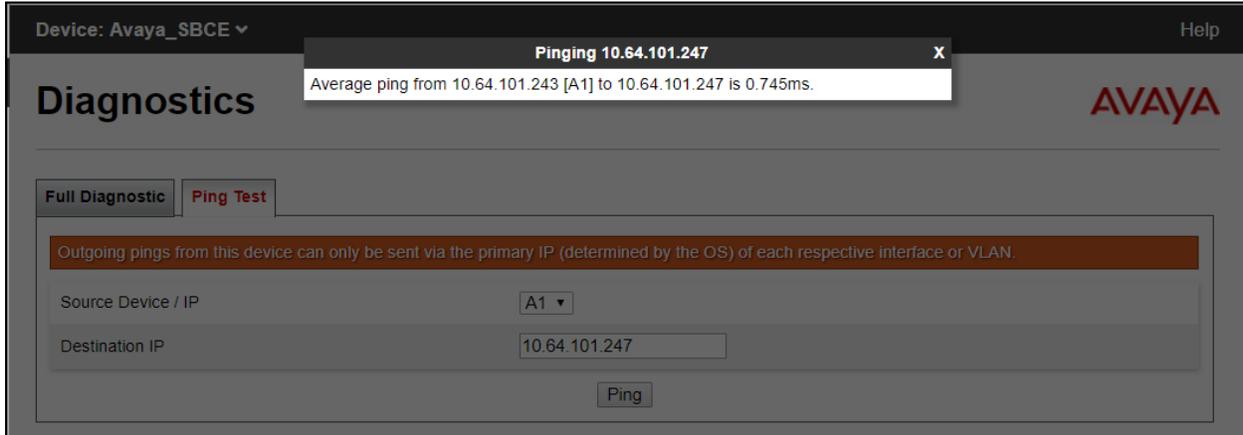
The screenshot shows the 'Diagnostics' screen. At the top, there is a navigation bar with 'Device: Avaya_SBCE' and 'Help'. The main header includes the title 'Diagnostics' and the 'AVAYA' logo.

The diagnostics section has two tabs: 'Full Diagnostic' and 'Ping Test'. Below the tabs, there is a warning message: 'Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.' A 'Start Diagnostic' button is located to the right of this message.

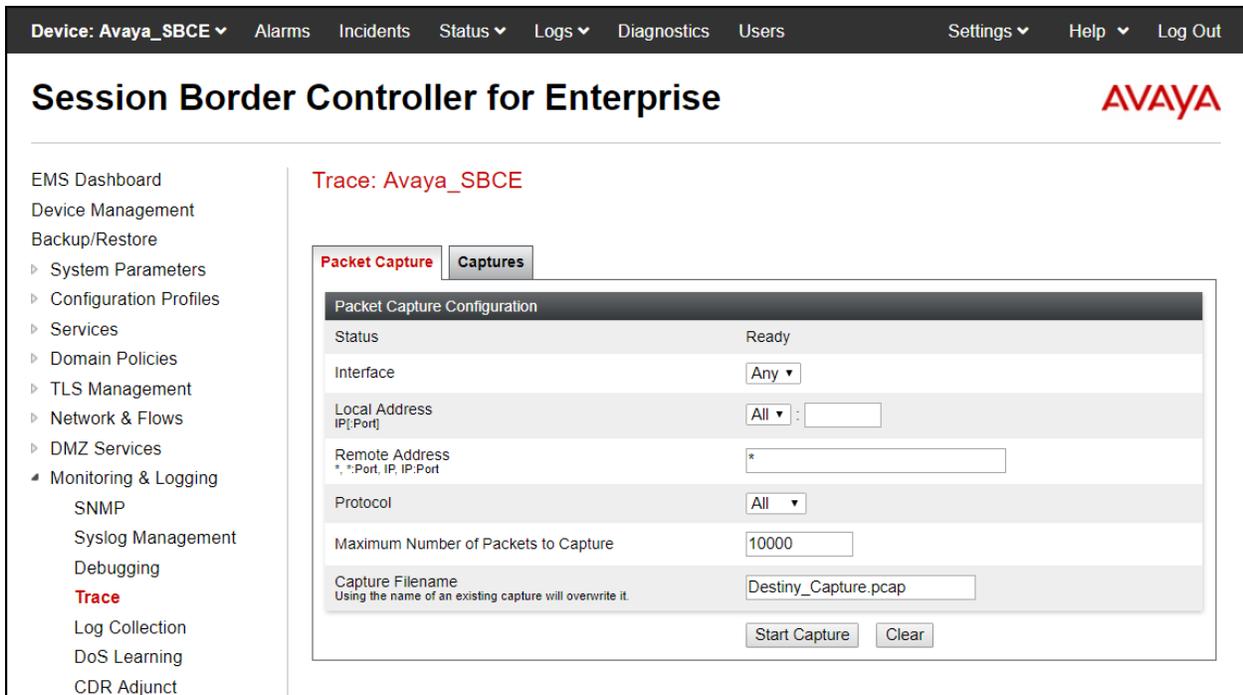
The diagnostic results are presented in a table:

Task Description	Status
EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
Ping: SBC (A1) to Gateway (10.64.101.1)	Average ping from 10.64.101.243 [A1] to 10.64.101.1 is 0.221ms.
Ping: SBC (A1) to Primary DNS (75.75.75.75)	Average ping from 10.64.101.243 [A1] to 75.75.75.75 is 1.817ms.
Ping: SBC (A1) to Secondary DNS (75.75.76.76)	Average ping from 10.64.101.243 [A1] to 75.75.76.76 is 3.687ms.
Ping: SBC (B1) to Gateway (.....80.1)	Average ping from80.23 [B1] to80.1 is 0.310ms.
Ping: SBC (B1) to Primary DNS (75.75.75.75)	Average ping from80.23 [B1] to 75.75.75.75 is 2.009ms.
Ping: SBC (B1) to Secondary DNS (75.75.76.76)	Average ping from80.23 [B1] to 75.75.76.76 is 3.365ms.

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



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



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 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. A left sidebar menu lists various management options, with 'Trace' highlighted in red. The main content area is titled 'Trace: Avaya_SBCE' and features two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active, showing a table with one entry: 'Destiny_Capture_20200828091956.pcap', which is 512,000 bytes and was last modified on August 28, 2020 at 9:20:11 AM EDT. A 'Delete' link is visible next to the entry. A 'Refresh' button is located in the top right corner of the table area.

File Name	File Size (bytes)	Last Modified	
Destiny_Capture_20200828091956.pcap	512,000	August 28, 2020 at 9:20:11 AM EDT	Delete

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 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.1, to interoperate with the Destiny 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 8.1.x, Issue 4, March 2020.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020.
- [3] *Administering Avaya Aura® System Manager for Release 8.1.x*, Issue 6, April 2020.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 8.1.x, Issue 5, May 2020.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 8.1., Issue 3, March 2020.
- [6] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 4, May 2020.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 3, June 2020.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 2, April 2020.
- [9] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0 - Issue 1.0*.
- [10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 9, April 2020.
- [11] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0.x, Issue 9, April 2020.
- [12] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*. Release 3.8, Issue 1, March 2020.
- [13] *Administering Avaya one-X® Communicator*. Release 6.2, Feature Pack 10, November 2015.
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [15] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

12. Appendix A – SigMa Scripts

Following are the Signaling Manipulation scripts that were used in the configuration of the Avaya SBCE. Add the scripts as instructed in **Sections 7.8**, enter a name for the script in the Title and copy/paste the entire scripts shown below.

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

- For **Title** enter a name, the name *Destiny_Sigma* was chosen in this example.
- Copy and paste the entire script shown below.
- Click **Save**.

within session "ALL"

```
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{

//Removes + signs from headers
%HEADERS["To"][1].URI.USER.regex_replace("\+", "");
%HEADERS["From"][1].URI.USER.regex_replace("\+", "");
%HEADERS["Contact"][1].URI.USER.regex_replace("\+", "");
%HEADERS["Diversion"][1].URI.USER.regex_replace("\+", "");
%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("\+", "");

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

//Remove P-Location parameter.
remove(%HEADERS["P-Location"][1]);

//Changes the Diversion header scheme from SIPS to SIP.
%HEADERS["Diversion"][1].regex_replace("sips", "sip");

//Remove unwanted xml element information from the SDP in SIP messages sent to the Service
Provider.
remove(%BODY[1]);

}
}
```

©2020 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.