



Application Notes for Configuring Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.1 to support Smart City Telecom SIP Trunk Service – Issue 1.1

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service on an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.1, to interoperate with the Smart City Telecom SIP Trunk service.

The Smart City Telecom SIP Trunk service provide customers with PSTN access via a SIP trunk between the enterprise and the Smart City Telecom 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	17
5.6.	Signaling Group	18
5.7.	Trunk Group.....	20
5.8.	Calling Party Information.....	24
5.9.	Inbound Routing.....	25
5.10.	Outbound Routing	26
6.	Configure Avaya Aura® Session Manager	30
6.1.	System Manager Login and Navigation.....	31
6.2.	SIP Domain	32
6.3.	Locations	32
6.4.	Adaptations.....	35
6.5.	SIP Entities	37
6.6.	Entity Links	40
6.7.	Routing Policies	42
6.8.	Dial Patterns	43
7.	Configure Avaya Session Border Controller for Enterprise	46
7.1.	System Access.....	46
7.2.	System Management	48
7.3.	Network Management	50
7.4.	Media Interfaces	51
7.5.	Signaling Interfaces.....	53
7.6.	Server Interworking.....	55
7.6.1.	Server Interworking Profile – Enterprise.....	55
7.6.2.	Server Interworking Profile – Service Provider.....	58
7.7.	Server Configuration	60
7.7.1.	Server Configuration Profile – Enterprise	60
7.7.2.	Server Configuration Profile – Service Provider	62
7.8.	Routing.....	66
7.8.1.	Routing Profile – Enterprise	66
7.8.2.	Routing Profile – Service Provider	67

7.9.	Topology Hiding	68
7.9.1.	Topology Hiding Profile – Enterprise.....	68
7.9.2.	Topology Hiding Profile – Service Provider.	70
7.10.	Domain Policies.....	71
7.10.1.	Application Rules.....	71
7.10.2.	Media Rules.....	72
7.10.3.	Signaling Rules	74
7.11.	End Point Policy Groups	74
7.11.1.	End Point Policy Group – Enterprise	74
7.11.2.	End Point Policy Group – Service Provider.....	76
7.12.	End Point Flows.....	77
7.12.1.	End Point Flow – Enterprise	78
7.12.2.	End Point Flow – Service Provider	79
8.	Smart City Telecom SIP Trunk Service Configuration	80
9.	Verification and Troubleshooting	80
9.1.	General Verification Steps	80
9.2.	Communication Manager Verification.....	80
9.3.	Session Manager Verification	81
9.4.	Avaya SBCE Verification	83
10.	Conclusion	89
11.	References.....	89

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service between the Smart City Telecom network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Rel. 7.1 (Communication Manager), Avaya Aura® Session Manager Rel. 7.1 (Session Manager), Avaya Session Border Controller for Enterprise Rel. 7.1(Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Smart City Telecom SIP Trunk 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”, “Smart City Telecom” and “Smart City” 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 Smart City Telecom 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.

2.1. Interoperability Compliance Testing

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

- SIP Trunk Registration (Dynamic Authentication).
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using “This Computer” and “Other Phone” modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Equinox softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 Deskphones (Only the 96x1 SIP Deskphones were used to test remote worker functionality).
- Codec G.711MU.
- Inbound and outbound PSTN calls using VoIP media resources in Avaya Media Gateways and the Avaya Aura® Media Server at the enterprise network.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Support of the SIP REFER method.
- G.711 Pass-Through fax.
- Routing inbound PSTN calls to call center agent queues.
- Proper response/error treatment to different failure conditions.

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.

The following items were not tested:

- “911” emergency calls are supported but were not tested.
- T.38 fax is not currently supported by Smart City; therefore T.38 fax was not tested (refer to the test results under **Section 2.2**).

2.2. Test Results

Interoperability testing of the Smart City Telecom SIP Trunk Service with the Avaya SIP-enabled enterprise solution was completed with the observations/limitations noted below:

- **Out-of-Band DTMF Signaling (RFC 2833)** – Out-of-band DTMF signaling (RFC 2833) initially was not supported by Smart City; this issue was later resolved by Smart City with changes made to their gateways. Out-of-band DTMF signaling (RFC 2833) was successfully tested after changes to Smart City's gateways were made.
- **Direct IP to IP audio connection (Shuffling)** – When an IP endpoint calls another IP endpoint the audio stream will initially pass through an Avaya media resource, once the call is established and the media resource is no longer required the call is “shuffled” away from the media resource and the audio path is established directly between IP endpoints, releasing the media resource at the Avaya Aura® PBX. In order to shuffle the call, Communication Manager sends a ReINVITE without SDP (slow start INVITE) to the Service Provider. During the testing, the message exchange between Communication Manager and Smart City to shuffle the call resulted in one-way audio. ReINVITE without SDP was not supported by Smart City. This issue was solved by Smart City with the application of a patch for the support of ReINVITES without SDP (slow start INVITE).
- **Calls to invalid/non-existent PSTN numbers** – When an enterprise user dials an invalid PSTN number, an announcement/treatment should be played to the user informing him/her that an invalid number was dialed and to please check the number and to dial again. Currently no announcement/treatment is played to the user, the user receives silence. This issue was reported to Smart City and is under investigation by Smart City.
- **Use of REFER** – If REFER is enabled in Communication Manager, calls redirected to the PSTN (forward, blind transfer, attended transfer) may result in some inconsequential message retransmissions when the call is disconnected from Communication Manager resources. Specifically, after the REFER is sent from Communication Manager and the SIP Trunk resources are released. Smart City sends several UPDATE messages, causing the Avaya SBCE to send BYE messages. This lead to some message responses being ignored and messages being retransmitted. However, in all cases, there was no user impact. The calls were successfully transferred, Communication Manager resources were released from the call and subsequent calls could be made.
- **Fax Support** – T.38 fax is currently not supported on the Smart City SIP trunk service offering. G.711 fax pass-through was successfully tested during the compliance test. Due to the unpredictability of pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered in Communication Manager on a “best effort” basis; its success is not guaranteed, and it should be used at the customer's discretion. Smart City is planning to implement T.38 fax support in the future.
- **SIP Network Call Redirect (NCR) via SIP REFER using Communication Manager Vector** – A Communication Manager vector was configured to answer incoming calls with an announcement and then to route the call to a PSTN telephone that was BUSY (active on a call), the vector was also configured to re-route the call to a local extension in Communication Manager if a BUSY condition was detected on the PSTN telephone, and to send a REFER message to the Smart City network. This call scenario failed, the

end result was no audio in both directions of the call, between the local extension and the PSTN telephone that originated the call. This particular call flow scenario requires the Service Provider to support sending intermediate call states (100 Trying, 180 Ringing, etc.), this is done via NOTIFY messages in response to the REFER request before the referring party is disconnected. Smart City only sends one NOTIFY message with “486 Busy Here”. This issue is only seen on calls that are routed by vectors to a PSTN telephone that is BUSY (active on a call) and that are re-routed by the same vector to a local extension when the BUSY condition is detected. This issue does not impact other call routing scenarios performed by vectors. This issue was reported to Smart City and is under investigation by Smart City.

- **SIP header optimization** – There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider’s network. These headers were removed with the purposes of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider’s network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector and P-Location (**Section 6.4**).

2.3. Support

For support on Smart City Telecom SIP Trunk Service visit the corporate Web page at:
<https://smartcitytelecom.com/about-us/contact-us/>

Email Support: nocsupport@smartcitytelecom.com

Business Support: 407-938-4357

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Smart City Telecom SIP Trunk Service through a public Internet WAN connection.

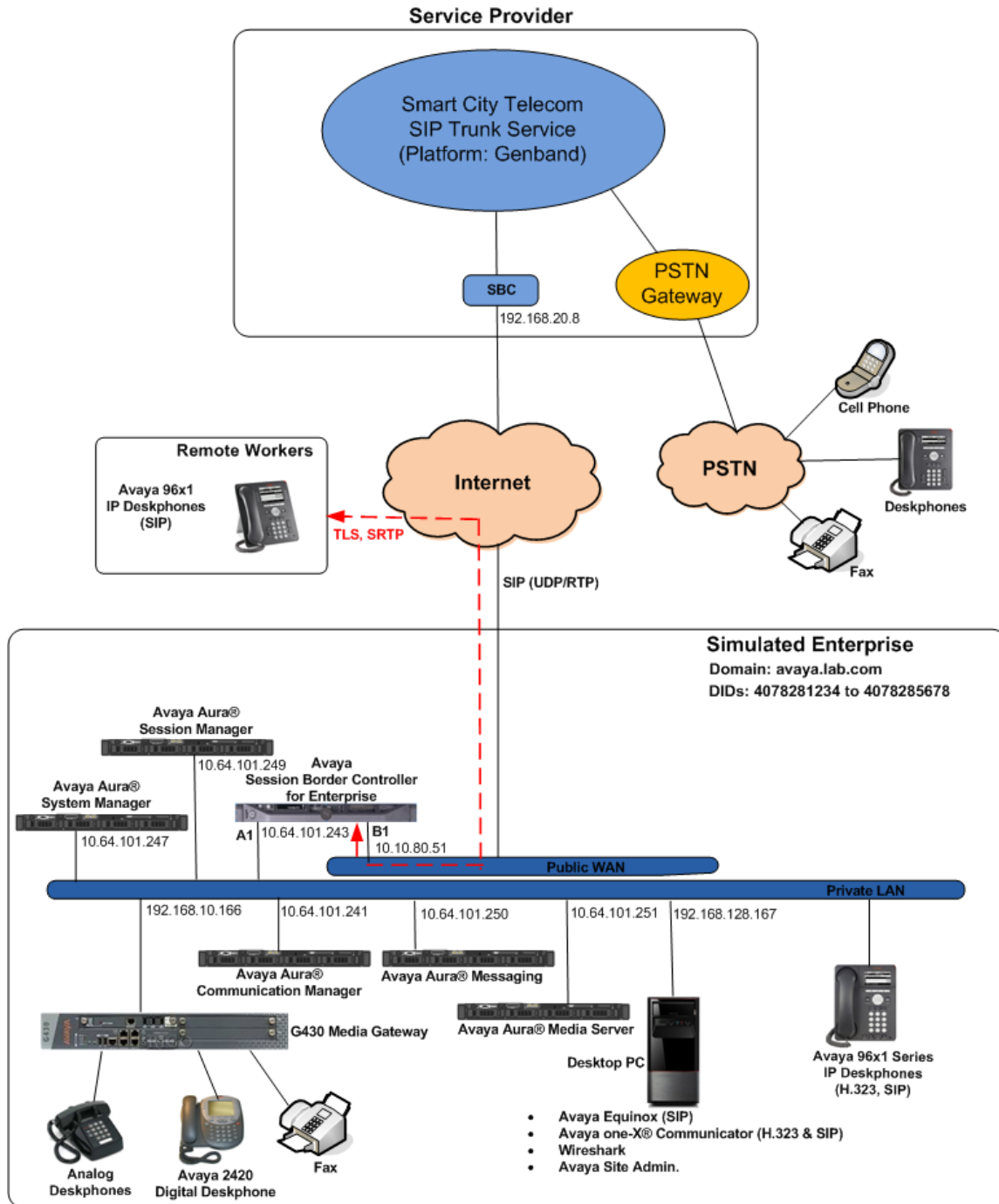


Figure 1: Avaya SIP Enterprise Solution connected to Smart City Telecom SIP Trunk Service

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 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Equinox softphone (SIP).
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya 96x1 SIP Deskphones. For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on Avaya 96x1 SIP Deskphones used to test remote worker functionality. 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 [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 (in this case Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

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

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

As part of the Avaya Aura® version 7.1 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.

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 Smart City Telecom network SIP Trunk service, they are not included in these Application Notes.

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 the Avaya system and the Smart City network did not include the use of any specific encryption features, UDP Transport for signaling and RTP for media was used between the Avaya system and the Smart City network across the SIP Trunk. TLS transport for signaling and SRTP for media was used inside of the enterprise (private network side, in between Avaya components inside of the enterprise).

<p>Note – The configuration tasks required to support TLS transport for signaling and SRTP for media inside of the enterprise (private network side) are beyond the scope of these Application Notes; hence they are not discussed in this document.</p>

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	7.1.0.0 (07.1.0.0.532)
Avaya Aura® Session Manager	7.1.0.0 (7.1.0.0.710028)
Avaya Aura® System Manager	7.1.0.0 Build No. 7.1.0.0.1125193 Software Update Rev. No. 7.1.0.0.116654
Avaya Session Border Controller for Enterprise	ASBCE 7.1 – SP2 7.1.0.2-01-13249
Avaya Aura® Messaging	7.0 Service Pack 0 (MSG-00.0.441.0-017_0004)
Avaya Aura® Media Server	7.8.0.312 SP3 7.8.0.312_2017.04.24
Avaya G430 Media Gateway	G430_sw_38_18_0
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.0.0.57
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6401
Avaya one-X® Communicator (H.323, SIP)	6.2.12.04-SP12
Avaya Equinox (SIP)	3.1.1.18
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
Smart City	
Genband C20 Softswitch	R19
Genband Q20 SBC	R9.2.5.0

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

Note – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the 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 Smart City Telecom network SIP Trunk service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and the Avaya Aura® Media Server has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens captures 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 **24000** 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
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 41000 0
      Maximum Video Capable IP Softphones: 18000 7
      Maximum Administered SIP Trunks: 24000 120
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0

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

5.2. System Features

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

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

  Music (or Silence) on Transferred Trunk Calls? no
  DID/Tie/ISDN/SIP Intercept Treatment: attendant
  Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
    Automatic Circuit Assurance (ACA) Enabled? n

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

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

change system-parameters features Page 9 of 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. Smart City supports audio codecs **G.711MU**.

change ip-codec-set 2 Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1:	<u>G.711MU</u>	<u>n</u>	<u>2</u>	<u>20</u>
2:	_____	-	---	
3:	_____	-	---	
4:	_____	-	---	
5:	_____	-	---	
6:	_____	-	---	
7:	_____	-	---	

Media Encryption Encrypted SRTCP: best-effort

1: 1-srtp-aescm128-hmac80

2: none

3: _____

4: _____

5: _____

On **Page 2**, set the **Fax Mode** to **t.38-G711-fallback**, **ECM = y**, **FB-Timer = 4**.

change ip-codec-set 2 Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

	Mode	Redun-dancy	Packet Size(ms)
FAX	<u>t.38-G711-fallback</u>	<u>0</u> ECM: <u>y</u> FB-Timer: <u>4</u>	
Modem	<u>off</u>	<u>0</u>	
TDD/TTY	<u>US</u>	<u>3</u>	
H.323 Clear-channel	<u>n</u>	<u>0</u>	
SIP 64K Data	<u>n</u>	<u>0</u>	<u>20</u>

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
Codec Set: 2      Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048      IP Audio Hairpinning? n
UDP Port Max: 3349
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y      RSVP Enabled? 39
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

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

change ip-network-region 2 Page 4 of 20

Source Region: 2		Inter Network Region Connection Management									
dst rgn	codec set	direct WAN	BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC	I G A R	M t c l e t			
1	2	y	NoLimit				n				
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 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 (refer to the test results under **Section 2.2** for current DTMF tone support limitation by Smart City).
- 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
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? y
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y
Enable Layer 3 Test? n	IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n
	Alternate Route Timer(sec): 6

5.7. Trunk Group

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

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

```
change trunk-group 2                                     Page 1 of 21
                                     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, **1800** seconds was used.

change trunk-group 2 Page 2 of 21

Group Type: sip

TRUNK PARAMETERS

Unicode Name: auto

Redirect On OPTIM Failure: 5000

SCCAN? n Digital Loss Group: 18

Preferred Minimum Session Refresh Interval(sec): 1800

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

The screenshot shows a terminal window titled "change trunk-group 2" with a page indicator "Page 3 of 21". The main heading is "TRUNK FEATURES". The configuration details are as follows:

- ACA Assignment? ☐ Measured: none
- Maintenance Tests? y
- Suppress # Outpulsing? n **Numbering Format: private**
- UI 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 REFER method, which is supported by Smart City, for the redirection of PSTN calls that are transferred back to the SIP trunk.
- Set the **Send Diversion Header** field to **n** and **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101**.
- Set the **Convert 180 to 183 for Early Media?** to **y**.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- 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 21

PROTOCOL VARIATIONS

Mark Users as Phone?	<u>n</u>
Prepend '+' to Calling/Alerting/Diverting/Connected Number?	<u>n</u>
Send Transferring Party Information?	<u>n</u>
Network Call Redirection?	<u>y</u>
Build Refer-To URI of REFER From Contact For NCR?	<u>n</u>
Send Diversion Header?	<u>n</u>
Support Request History?	<u>n</u>
Telephone Event Payload Type:	<u>101</u>
Convert 180 to 183 for Early Media?	<u>y</u>
Always Use re-INVITE for Display Updates?	<u>y</u>
Identity for Calling Party Display:	<u>P-Asserted-Identity</u>
Block Sending Calling Party Location in INVITE?	<u>n</u>
Accept Redirect to Blank User Destination?	<u>n</u>
Enable Q-SIP?	<u>n</u>
Interworking of ISDN Clearing with In-Band Tones:	<u>keep-channel-active</u>
Request URI Contents:	<u>may-have-extra-digits</u>

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers were assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

HG; Reviewed: Solution & Interoperability Test Lab Application Notes 24 of 90
SPOC 8/9/2017 ©2017 Avaya Inc. All Rights Reserved. SmartCMSMSBC71

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 Smart City 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/ Feature	Number Len	Number Digits	Del	Insert		
public-ntwrk	10	4078281234	10	3040		
public-ntwrk	10	4078285678	10	3047		
public-ntwrk	10	4078289123	10	5015		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		
public-ntwrk	—	—	—	—		

5.10. Outbound Routing

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

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

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

```
change feature-access-codes                                     Page 1 of 10
FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code: ____
Abbreviated Dialing List2 Access Code: ____
Abbreviated Dialing List3 Access Code: ____
Abbreviated Dial - Prgm Group List Access Code: ____
Announcement Access Code: #7
Answer Back Access Code: ____
Attendant Access Code: ____
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9 Access Code 2: ____
Automatic Callback Activation: ____ Deactivation: ____
Call Forwarding Activation Busy/DA: ____ All: ____ Deactivation: ____
Call Forwarding Enhanced Status: ____ Act: ____ Deactivation: ____
Call Park Access Code: ____
Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
CDR Account Code Access Code: ____
Change COR Access Code: ____
Change Coverage Access Code: ____
Conditional Call Extend Activation: ____ Deactivation: ____
Contact Closure Open Code: ____ Close Code: ____
```

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

change ars analysis 17 Page 1 of 2

ARS DIGIT ANALYSIS TABLE
Location: all Percent Full: 0

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
170	11	11	deny	fnpa	3~	n
1700	11	11	deny	fnpa	---	n
171	11	11	deny	fnpa	---	n
172	11	11	2	fnpa	---	n
173	11	11	deny	fnpa	---	n
174	11	11	deny	fnpa	---	n
175	11	11	deny	fnpa	---	n
176	11	11	deny	fnpa	---	n
177	11	11	deny	fnpa	---	n
178	11	11	deny	fnpa	---	n
1786	11	11	2	fnpa	---	n
179	11	11	deny	fnpa	---	n
180	11	11	deny	fnpa	---	n
1800	11	11	2	fnpa	---	n
1800555	11	11	deny	fnpa	---	n

change ars analysis 407 Page 1 of 2

ARS DIGIT ANALYSIS TABLE
Location: all Percent Full: 0

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
407	10	10	2	hnpa	---	n
411	3	3	2	svcl	---	n
443	10	10	2	hnpa	---	n
5	7	7	2	hnpa	---	n
555	7	7	deny	hnpa	---	n
6	7	7	2	hnpa	---	n
611	3	3	2	svcl	---	n
63	8	8	2	hnpa	---	n
7	10	10	2	hnpa	---	n
808	10	10	2	hnpa	---	n
809	10	10	2	hnpa	---	n
811	3	3	1	svcl	---	n
828	7	7	2	hnpa	---	n
868	10	10	2	hnpa	---	n
9	10	10	2	hnpa	---	n

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

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

change route-pattern 2 Page 1 of 3

Pattern Number: 2 Pattern Name: Serv. Provider

SCCAN? n Secure SIP? n Used for SIP stations? n

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

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

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

6. Configure Avaya Aura® Session Manager

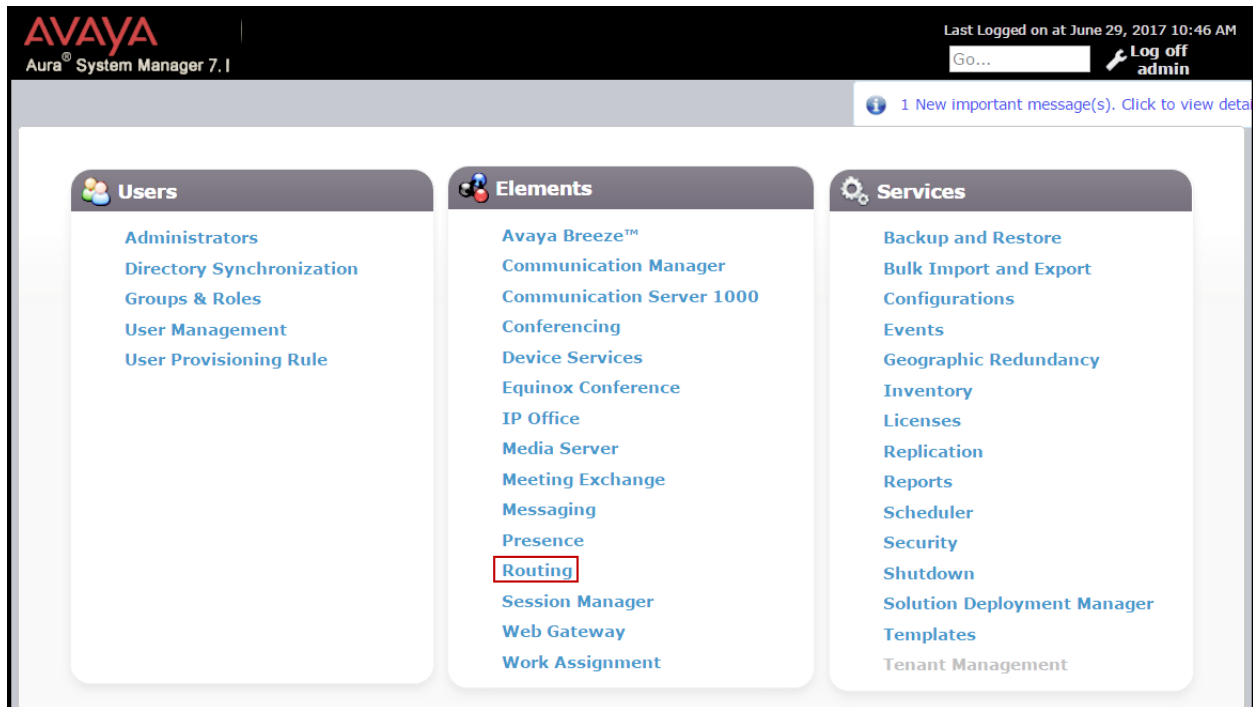
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

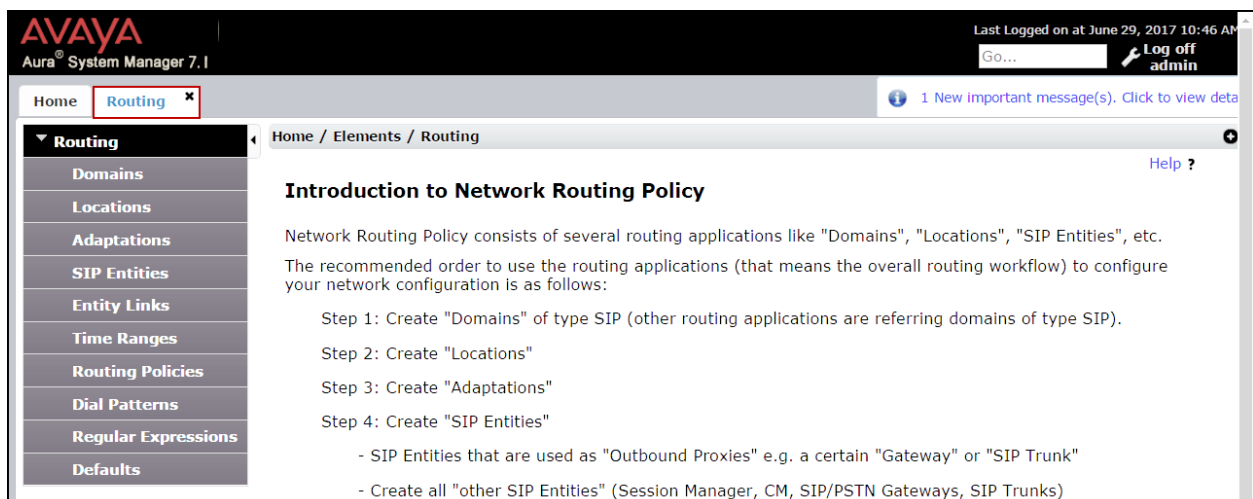
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. System Manager Login and Navigation

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



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



6.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, **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 shows the Avaya Aura System Manager 7.1 interface. The top header includes the Avaya logo, 'Aura System Manager 7.1', and a 'Last Logged on at June 29, 2017 10:46 AM' status. The left navigation pane has 'Routing' and 'Domains' highlighted. The main content area is titled 'Domain Management' and shows a table with one item: 'avaya.lab.com' of type 'sip' with notes 'HG V-Domain'. The table has columns for Name, Type, and Notes. The 'Name' column contains 'avaya.lab.com', the 'Type' column contains 'sip', and the 'Notes' column contains 'HG V-Domain'. The table is filtered by 'Enable'.

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

6.3. Locations

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

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

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

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a 'Last Logged on at June 29, 2017 10:46 AM' status. A search bar with 'Go...' and a 'Log off admin' button are also present. The main navigation menu on the left lists 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'Routing' menu is expanded, and 'Locations' is selected. The breadcrumb trail shows 'Home / Elements / Routing / Locations'. The 'Location Details' page for 'Session Manager' is displayed. The 'General' tab is active, showing the 'Name' field set to 'Session Manager' and the 'Notes' field set to 'VMware Session Manager'. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox that is unchecked. A 'Listed Directory Number' field is at the bottom. 'Commit' and 'Cancel' buttons are in the top right corner.

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.

This screenshot shows the same Avaya Aura System Manager 7.1 interface as the previous one, but for the 'Communication Manager' location. The navigation and breadcrumb trail are identical. In the 'Location Details' page, the 'Name' field is now 'Communication Manager' and the 'Notes' field is 'VMware Communication Manager'. The 'Dial Plan Transparency in Survivable Mode' section and the 'Listed Directory Number' field remain the same. The 'Commit' and 'Cancel' buttons are still in the top right corner.

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 7.1 web interface. The top header shows the Avaya logo and 'Aura System Manager 7.1'. On the right, it indicates 'Last Logged on at June 29, 2017 10:46 AM' and provides a 'Log off admin' button. Below the header, there are tabs for 'Home' and 'Routing'. The 'Routing' tab is active, and a sub-tab 'Locations' is selected in the left-hand navigation menu. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. Under the 'General' section, the 'Name' field is set to 'Avaya SBCE' and the 'Notes' field is set to 'VMware Avaya SBCE'. Below this, the 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox that is currently unchecked. At the bottom, there is a 'Listed Directory Number' field.

AVAYA
Aura System Manager 7.1

Last Logged on at June 29, 2017 10:46 AM
Go... Log off admin

Home Routing x

Home / Elements / Routing / Locations

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

Location Details

Commit Cancel

Help ?

General

* Name: Avaya SBCE
Notes: VMware Avaya SBCE

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.1 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-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

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

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

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

AVAYA
Aura System Manager 7.1

Last Logged on at June 29, 2017 10:46 AM
Go... Log off admin

Home Routing x 1 New important message(s). Click to view details

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel Help ?

General

* Adaptation Name: CM_Outbound_Header_Removal

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	*Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P-Location,

Select : All, None

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* 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 7.1 web interface. The top header shows the Avaya logo and 'Aura® System Manager 7.1'. The left navigation pane has 'Routing' expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and has a 'General' tab. The form fields are as follows:

- Name:** Session Manager
- FQDN or IP Address:** 10.64.101.249
- Type:** Session Manager
- Notes:** VMware Session Manager
- Location:** Session Manager
- Outbound Proxy:** (empty)
- Time Zone:** America/New_York

The 'Commit' and 'Cancel' buttons are located at the top right of the form. The breadcrumb trail at the top reads 'Home / Elements / Routing / SIP Entities'.

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**.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 7.1', and a user status area showing 'Last Logged on at June 29, 2017 10:46 AM' with 'Go...' and 'Log off admin' links. Below this is a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. The left sidebar contains a menu with 'Routing' selected, and sub-items: 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' with a 'Help ?' link. It features a 'General' tab and a 'Commit' button. The form fields are as follows: 'Name' is 'Communication Manager Trunk 2'; 'FQDN or IP Address' is '10.64.101.241'; 'Type' is 'CM'; 'Notes' is 'Used for SP Testing'; 'Adaptation' is an empty dropdown; 'Location' is 'Communication Manager'; and 'Time Zone' is 'America/New_York'. Red boxes highlight the 'Name', 'FQDN or IP Address', 'Type', 'Location', and 'Time Zone' fields.

AVAYA
Aura® System Manager 7.1

Last Logged on at June 29, 2017 10:46 AM
Go... Log off admin

Home Routing x 1 New Important message(s). Click to view details

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: Communication Manager Trunk 2

* FQDN or IP Address: 10.64.101.241

Type: CM

Notes: Used for SP Testing

Adaptation:

Location: Communication Manager

Time Zone: America/New_York

Commit Cancel

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.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user status area showing 'Last Logged on at June 29, 2017 10:46 AM' and a 'Log off admin' button. Below the navigation bar, a breadcrumb trail reads 'Home / Elements / Routing / SIP Entities'. The left sidebar contains a menu with 'Routing' selected, and sub-items including 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' with a 'General' tab. The form 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), and 'Time Zone' (America/New_York). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

* 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

6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu (**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.

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

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

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a menu with options: Routing, Domains, Locations, 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 a 'Commit' button and a 'Cancel' button. Below the title 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 item, 'Session_Manager_ASBCI', which is linked to 'Session Manager' (SIP Entity 1) and 'Avaya SBCE' (SIP Entity 2) using the 'TLS' protocol on port '5061'. The 'Connection Policy' is set to 'trusted'. The 'Deny New Service' checkbox is unchecked. The table is filtered by 'Enable'.

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

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

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

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a 'Log off admin' button. The left sidebar shows a navigation menu with 'Routing Policies' highlighted. The main content area is titled 'Routing Policy Details' and contains two sections: 'General' and 'SIP Entity as Destination'. The 'General' section has fields for 'Name' (To CM Trunk 2), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (For inbound calls to CM via Trunk 2). The 'SIP Entity as Destination' section shows a table with one entry: 'Communication Manager Trunk 2' with FQDN or IP Address '10.64.101.241', Type 'CM', and Notes 'Used for SP Testing'.

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

AVAYA
Aura® System Manager 7.1

Last Logged on at June 29, 2017 10:46 AM
Go... Log off admin

Home Routing x 1 New important message(s). Click to view details

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name: Avaya SBCE

Disabled: ☐

* Retries: 0

Notes: For outbound calls to SP via ASBCE

SIP Entity as Destination

Select

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

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 (**Section 6.2**).
- **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 the enterprise and outbound local calls within the 407 area code. In the example, calls to 10 digit numbers starting with **407**, the area code assigned to the DID numbers provided by Smart City, arriving from location **Avaya SBCE**, used route policy **Communication Manager trunk 2** to Communication Manager. Also, for outbound local calls to 10 digit local numbers starting with **407**, the area code assigned to the DID numbers provided by Smart City, arriving from location **Communication Manager**, used route policy **Avaya SBCE** to the Avaya SBCE.

AVAYA
Aura® System Manager 7.1

Last Logged on at June 29, 2017 10:46 AM
Go... [Log off admin](#)

Home Routing x 1 New important message(s). Click to view details

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel Help ?

General

* Pattern: 407
* Min: 3
* Max: 10

Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: avaya.lab.com
Notes:

Originating Locations and Routing Policies

Add Remove

2 Items Filter: Enable

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

Select : All, None

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

The example in this screen shows the 11 digit dialed numbers for outbound calls, beginning with *1*, for long distance numbers in the North American Numbering Plan (NANP), 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*.

AVAYA
Aura® System Manager 7.1

Last Logged on at July 5, 2017 8:36 AM
Go... Log off admin

Home Routing x 1 New important message(s). Click to view details

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 1
* Min: 11
* Max: 11

Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: avaya.lab.com
Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

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

Select : All, None

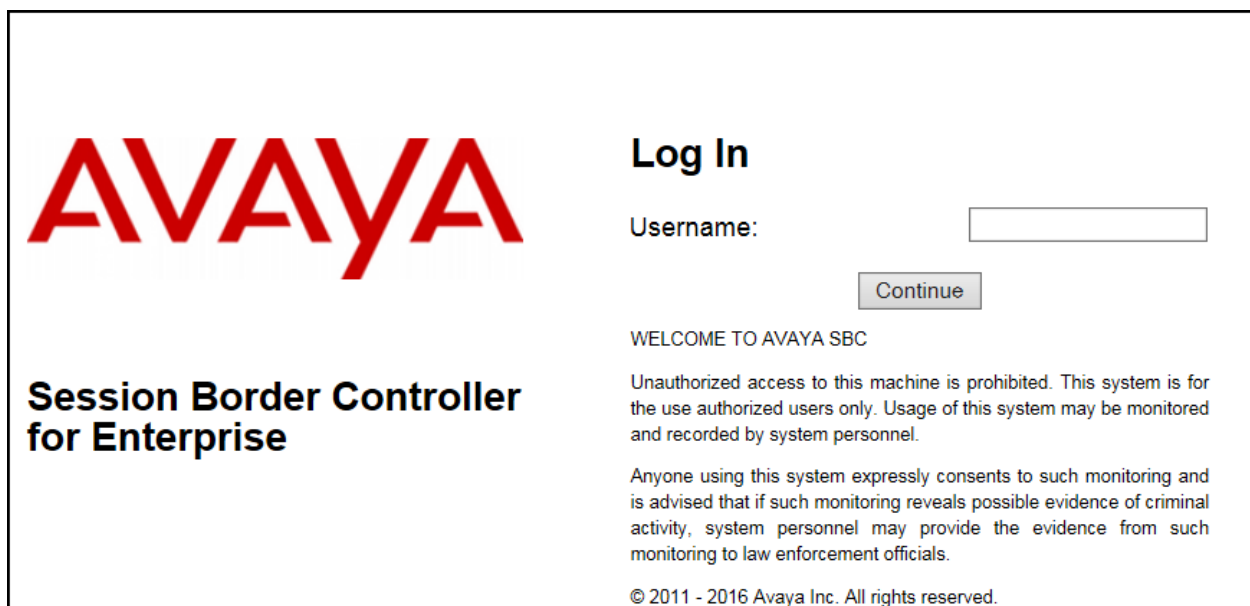
Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **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 image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black font. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field. Below the input field is a 'Continue' button. Further down, the text 'WELCOME TO AVAYA SBC' is displayed, followed by a disclaimer: 'Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.' Below this is a consent statement: 'Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.' At the bottom, the copyright notice '© 2011 - 2016 Avaya Inc. All rights reserved.' is shown.

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

[Alarms](#) [Incidents](#) [Status ▾](#) [Logs ▾](#) [Diagnostics](#) [Users](#) [Settings ▾](#) [Help ▾](#) [Log Out](#)

Session Border Controller for Enterprise



Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

Information	
System Time	11:35:47 AM EDT Refresh
Version	7.1.0.2-01-13249
Build Date	Fri Mar 3 17:33:08 EST 2017
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/29/2017 15:59:19 EDT
Failed Login Attempts	0

Alarms (past 24 hours)

None found.

Installed Devices

EMS

Avaya_SBCE

Incidents (past 24 hours)

None found.

7.2. System Management

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left navigation pane lists 'Dashboard', 'Administration', 'Backup/Restore', and 'System Management' (which is highlighted with a red box). Under 'System Management', there are sub-items: 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The main content area is titled 'System Management' and contains several tabs: 'Devices' (highlighted with a red box), 'Updates', 'SSL VPN', 'Licensing', and 'Key Bundles'. The 'Devices' tab displays a table with the following data:

Device Name	Management IP	Version	Status				
Avaya_SBCE	[Blurred]	7.1.0.2-01-13249	Commissioned	Reboot	Shutdown	Restart Application	View

The 'View' link in the table is highlighted with a red box. Below the table are links for 'Edit' and 'Uninstall'.

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

System Information: Avaya_SBCE
X

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 2000	2000
Advanced Sessions Requested: 2000	2000
Scopia Video Sessions Requested: 500	500
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
Encryption	<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	8.8.8.8
Secondary DNS	7.7.7.7
DNS Location	DMZ
DNS Client IP	10.10.80.51

Management IP(s)

IP #1 (IPv4)

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

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

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

7.3. Network Management

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

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, **Avaya_SBCE** in the sample configuration. 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 shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar contains a menu with 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', 'Device Specific Settings' (which is expanded to show 'Network Management' and 'Media Interface'), and 'Media Interface'. The 'Network Management: Avaya_SBCE' section is active, showing a 'Devices' tab with 'Avaya_SBCE' selected and a 'Networks' tab. The 'Networks' tab displays 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.

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

7.4. Media Interfaces

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

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

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

Add Media Interface

Name: Private_med

IP Address: Network_A1 (A1, VLAN 0) 10.64.101.243

Port Range: 35000 - 40000

Finish

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

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

The screenshot shows a dialog box titled "Add Media Interface". It contains the following fields and values:

- Name:** Public_med
- IP Address:** Network_B1 (B1, VLAN 0) (selected), 10.10.80.51 (selected)
- Port Range:** 35000 - 40000

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

7.5. Signaling Interfaces

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

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address 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**.
- Click **Finish**.

Add Signaling Interface X

Name: Private_sig

IP Address: Network_A1 (A1, VLAN 0) 10.64.101.243

TCP Port: Leave blank to disable

UDP Port: Leave blank to disable

TLS Port: 5061 Leave blank to disable

TLS Profile: NewRemoteWorkerServerProfile

Enable Shared Control: ☐

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 this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.
- Click **Finish**.

Add Signaling Interface X

Name

IP Address

TCP Port
Leave blank to disable

UDP Port
Leave blank to disable

TLS Port
Leave blank to disable

TLS Profile

Enable Shared Control ☐

Shared Control Port

7.6. Server Interworking

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

7.6.1. Server Interworking Profile – Enterprise

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the Avaya logo. The left navigation pane lists various configuration areas, with 'Global Profiles' expanded and 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: avaya-ru' and features a list of profiles on the left, including 'cs2100', 'avaya-ru' (highlighted), 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd...', 'Avaya-SM', 'SP-General', 'Avaya-IPO', 'Avaya-CS1000', and 'Avaya-CM'. A 'Clone' button is visible. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, the 'General' tab is active, displaying a table of settings:

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	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No

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

The 'Clone Profile' dialog box is shown with the following fields:

- Profile Name:** avaya-ru
- Clone Name:** Avaya-SM (with a red box around the input field and a clear 'x' button)
- Finish** button

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

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

The screenshot shows a window titled "Editing Profile: Avaya-SM" with a close button (X) in the top right corner. The window contains a "General" tab with various configuration options. The "T.38 Support" checkbox is checked and highlighted with a red rectangular box. Other options include "Hold Support" (radio buttons for None, RFC2543, RFC3264), "180 Handling" through "183 Handling" (radio buttons for None, SDP, No SDP), "Refer Handling" (checkbox), "URI Group" (dropdown menu set to None), "Send Hold" (checkbox), "Delayed Offer" (checkbox), "3xx Handling" (checkbox), "Diversion Header Support" (checkbox), "Delayed SDP Handling" (checkbox), "Re-Invite Handling" (checkbox), "Prack Handling" (checkbox), "Allow 18X SDP" (checkbox), "URI Scheme" (radio buttons for SIP, TEL, ANY), and "Via Header Format" (radio buttons for RFC3261, RFC2543). A "Finish" button is located at the bottom right of the dialog.

Note – Currently Smart City does not support T.38 fax in their SIP Trunk service offering, T.38 fax support was enabled for future use by Smart City.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo.

On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' and 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left and a configuration table on the right. The 'Advanced' tab is selected in the configuration table.

Interworking Profiles: Avaya-SM	
cs2100	
avaya-ru	
OCS-Edge-Server	
cisco-ccm	
cups	
OCS-FrontEnd-...	
Avaya-SM	
SP-General	
Avaya-IPO	
Avaya-CS1000	
Avaya-CM	

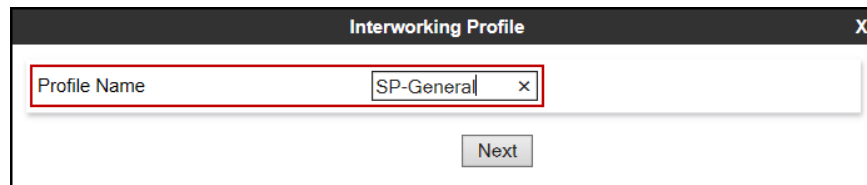
Click here to add a description.	
General	Timers
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No

DTMF	
DTMF Support	None

7.6.2. Server Interworking Profile – Service Provider

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

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



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "SP-General". A red rectangular box highlights the "Profile Name" field and its contents. Below the input field, there is a button labeled "Next".

- On the **General** tab, check **T.38 Support** (See note below). Click **Next**, then click **Finish** on the last tab leaving remaining fields with default values (not shown).

Interworking Profile X

General

Hold Support ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

URI Group None ▾

Send Hold ☒

Delayed Offer ☒

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

Re-Invite Handling ☐

Prack Handling ☐

Allow 18X SDP ☐

T.38 Support ☒

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261 ☐ RFC2543

Back Next

Note – Currently Smart City does not support T.38 fax in their SIP Trunk service offering, T.38 fax support was enabled for future use by Smart City.

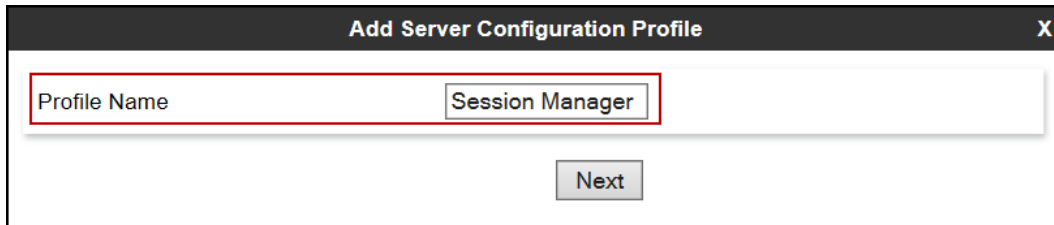
7.7. Server Configuration

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

7.7.1. Server Configuration Profile – Enterprise

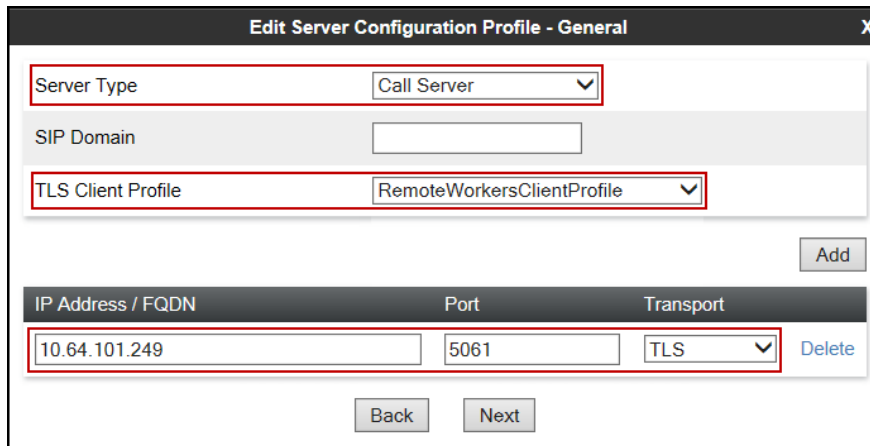
From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server.

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



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" which contains the text "Session Manager". Below this field is a button labeled "Next".

- On the **Edit Server Configuration Profile – General** tab select **Call Server** from the drop down menu under the **Server Type**.
- Select a **TLS Client Profile**.
- 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**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and a table. The "Server Type" dropdown is set to "Call Server". The "SIP Domain" field is empty. The "TLS Client Profile" dropdown is set to "RemoteWorkersClientProfile". Below these fields is an "Add" button. A table with three columns: "IP Address / FQDN", "Port", and "Transport" is shown. The first row of the table has the values "10.64.101.249", "5061", and "TLS". A "Delete" button is next to the first row. At the bottom of the dialog are "Back" and "Next" buttons.

- Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown).
- Select **Avaya-SM** from the **Interworking Profile** drop down menu.
- Click **Finish**.

Add Server Configuration Profile - Advanced X

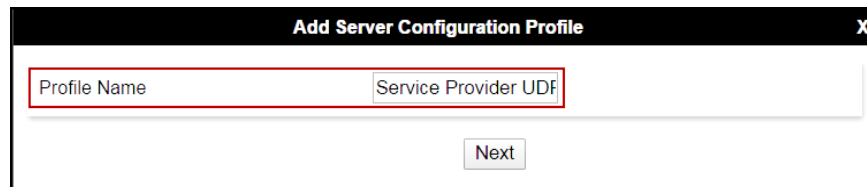
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya-SM ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061

Back Finish

7.7.2. Server Configuration Profile – Service Provider

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

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

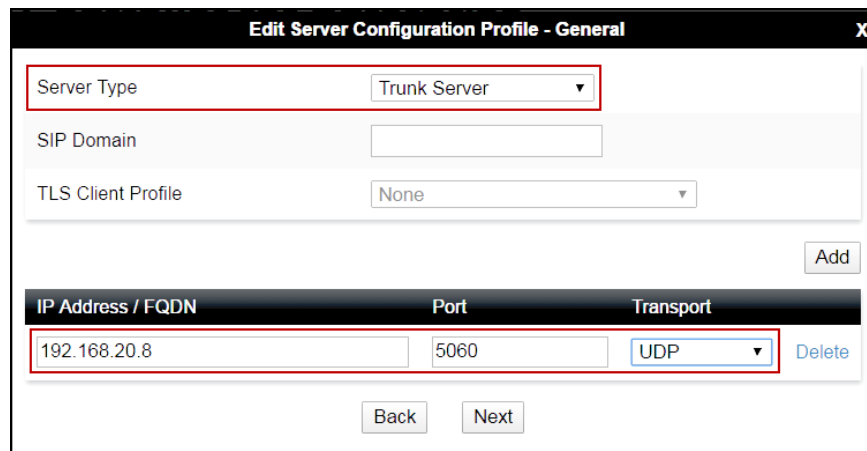


Add Server Configuration Profile X

Profile Name: Service Provider UDF

Next

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter Smart City's proxy IP address (See figure 1).
- Enter **5060** under **Port**, and select **UDP** for **Transport** for both entries.
- Click **Next**.



Edit Server Configuration Profile - General X

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport	
192.168.20.8	5060	UDP	Delete

Back Next

On the **Add Server Configuration Profile - Authentication** window:

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

Add Server Configuration Profile - Authentication X

Enable Authentication ☒

User Name

Realm
(Leave blank to detect from server challenge)

Password

Confirm Password

Back Next

On the **Add Server Configuration Profile - Heartbeat** window:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the 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 (*user123*) and the Service Provider's domain name (*avayatest.sippbx.smartcity.net*), as shown on the screen below. **Note**: The user name and domain name should be provided by the Service Provider.
 - **To URI**: Use the **User Name** entered above in the **Authentication** screen (*user123*) and the Service Provider's domain name (*avayatest.sippbx.smartcity.net*), as shown on the screen below. **Note**: The user name and domain name should be provided by the Service Provider.
- Click **Next**.

Add Server Configuration Profile - Heartbeat X

Enable Heartbeat ☒

Method REGISTER ▾

Frequency 60 seconds

From URI user123@avayatest.sippbx:

To URI user123@avayatest.sippbx:

Back Next

- On the **Add Server Configuration Profile - Advanced** tab, select *SP-General* from the **Interworking Profile** drop down menu.
- Click **Finish**.

Add Server Configuration Profile - Advanced X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061

Back Finish

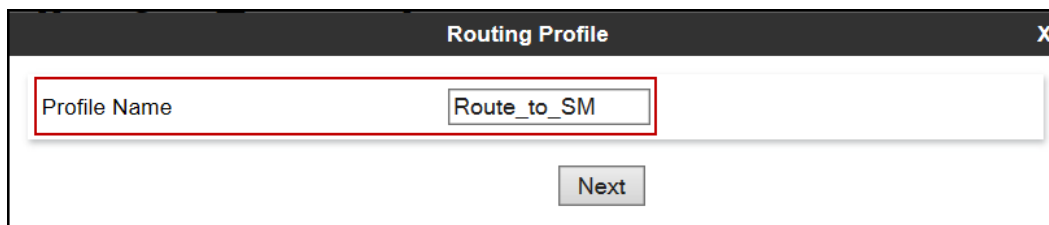
7.8. Routing

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.

7.8.1. Routing Profile – Enterprise

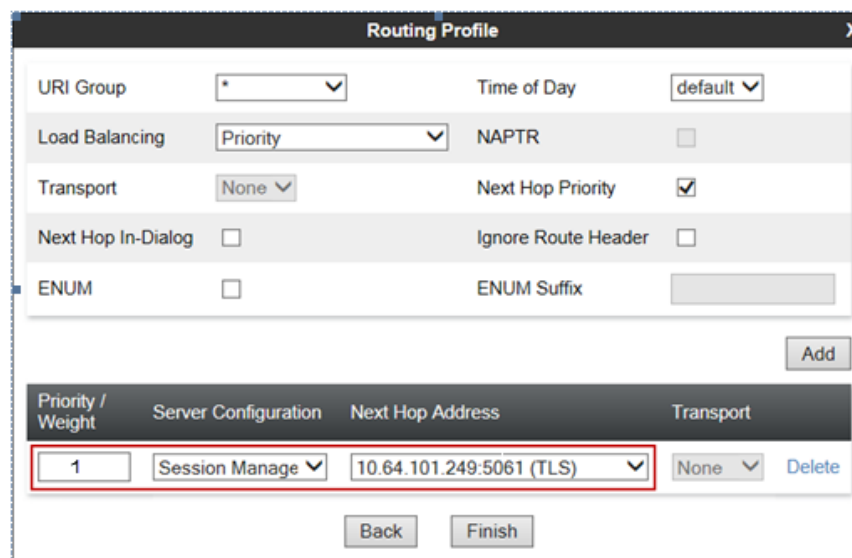
To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown).

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



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

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Server Configuration**, select *Session Manager*. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.7.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



The screenshot shows the "Routing Profile" dialog box with various configuration options. The "URI Group" is set to "*", "Time of Day" is "default", "Load Balancing" is "Priority", "NAPTR" is unchecked, "Transport" is "None", "Next Hop Priority" is checked, "Next Hop In-Dialog" is unchecked, "Ignore Route Header" is unchecked, "ENUM" is unchecked, and "ENUM Suffix" is empty. An "Add" button is visible. Below these options is a table with the following data:

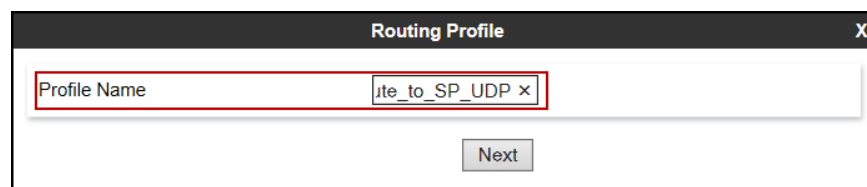
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manage	10.64.101.249:5061 (TLS)	None

At the bottom of the dialog are "Back" and "Finish" buttons. A red box highlights the "1" in the Priority / Weight column and the "10.64.101.249:5061 (TLS)" in the Next Hop Address column.

7.8.2. Routing Profile – Service Provider

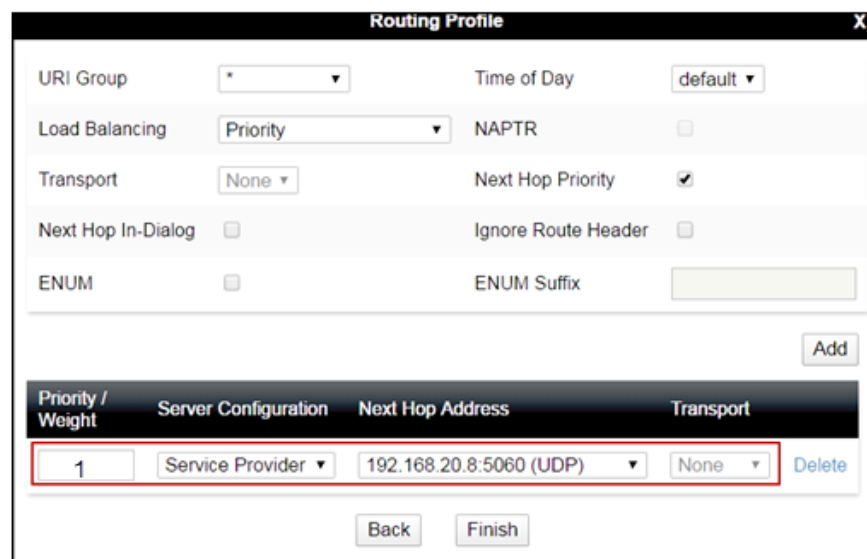
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

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



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "lte_to_SP_UDP". To the right of the input field is a small "X" icon. Below the input field is a "Next" button.

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Under **Server Configuration**, select the Server Configuration for the Service Provider created in **Section 7.7.2**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in **Section 7.7.2**.
- Defaults were used for all other parameters.
- Click **Finish**.



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

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐
- ENUM: ☐
- ENUM Suffix: (empty field)

Below these fields is an "Add" button. Underneath the "Add" button is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	192.168.20.8:5060 (UDP)	None

Below the table is a "Delete" button. At the bottom of the dialog are "Back" and "Finish" buttons.

7.9. Topology Hiding

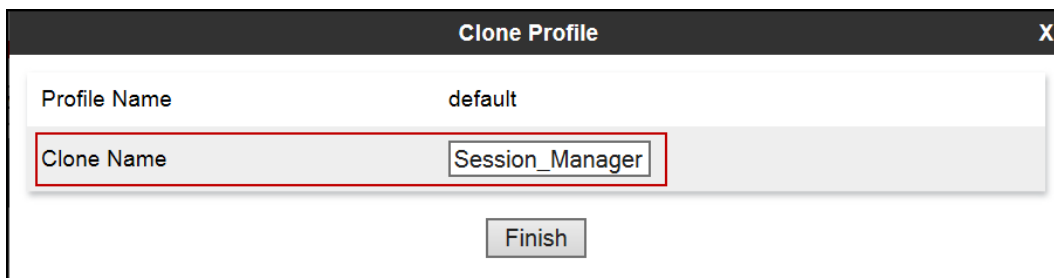
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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.

7.9.1. Topology Hiding Profile – Enterprise

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

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



The screenshot shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The main area is white and contains two input fields. The first field is labeled 'Profile Name' and contains the text 'default'. The second field is labeled 'Clone Name' and contains the text 'Session_Manager'; this field is highlighted with a red rectangular border. Below these fields is a 'Finish' button.

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**.

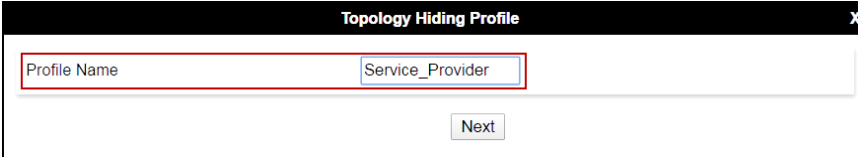
Header	Criteria	Replace Action	Overwrite Value	
SDP	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	avaya.lab.com	Delete
From	IP/Domain	Overwrite	avaya.lab.com	Delete
Refer-To	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	avaya.lab.com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

Finish

7.9.2. 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**.



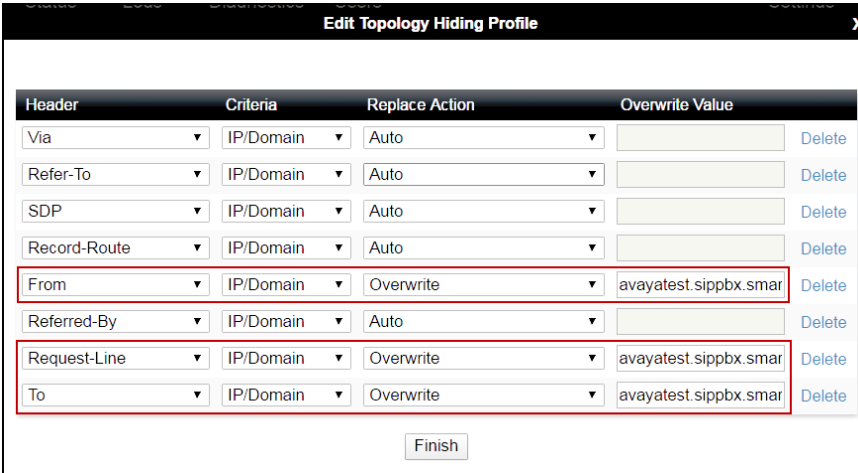
Topology Hiding Profile

Profile Name: Service_Provider

Next

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

- For the, **From**, **To** and **Request-Line** headers, select *Overwrite* in the **Replace Action** column and enter the Service Provider's SIP domain *avayatest.sippbx.smartcity.net*, in the **Overwrite Value** column of these headers, as shown below.
- Default values were used for all other fields.
- Click **Finish**.



Edit Topology Hiding Profile

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

Finish

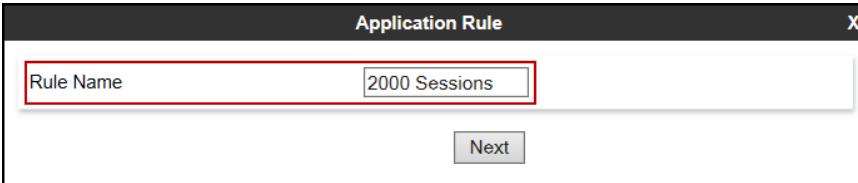
7.10. Domain Policies

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.

7.10.1. 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 and video 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**.

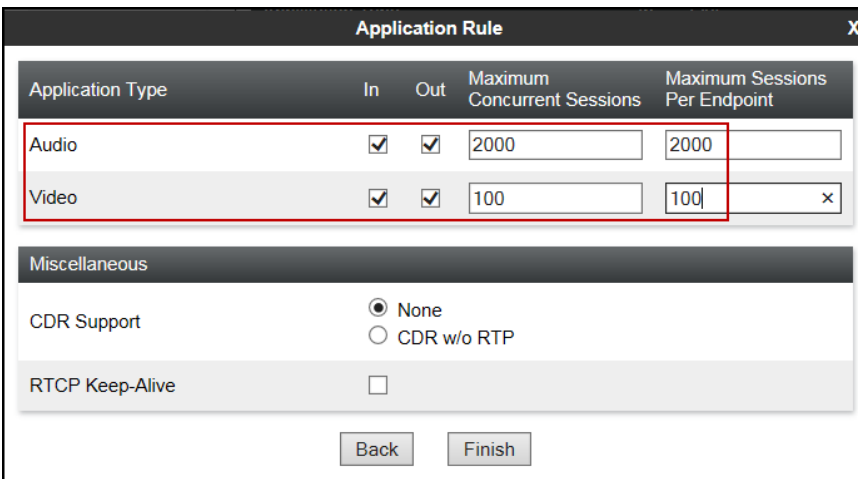


Application Rule

Rule Name: 2000 Sessions

Next

- Under **Audio** check *In* and *Out* and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the values of *2000* for Audio and *100* for Video were used in the sample configuration.
- Click **Finish**.



Application Rule

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: ☒ None ☐ CDR w/o RTP

RTCP Keep-Alive: ☐

Back Finish

7.10.2. Media Rules

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

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

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **SM_SRTP** (not shown).
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Click **Next**.

The screenshot displays the 'Media Rule' configuration window, which is divided into three main sections: Audio Encryption, Video Encryption, and Miscellaneous. Each section contains several configuration options, many of which are highlighted with red boxes to indicate the required settings for the compliance test.

- Audio Encryption:**
 - Preferred Format #1: SRTP_AES_CM_128_HMAC_SHA1_80 (dropdown)
 - Preferred Format #2: RTP (dropdown)
 - Preferred Format #3: NONE (dropdown)
 - Encrypted RTCP: ☐ (unchecked)
 - MKI: ☐ (unchecked)
 - Lifetime: 2^ (text input)
 - Interworking: ☒ (checked)
- Video Encryption:**
 - Preferred Format #1: SRTP_AES_CM_128_HMAC_SHA1_80 (dropdown)
 - Preferred Format #2: RTP (dropdown)
 - Preferred Format #3: NONE (dropdown)
 - Encrypted RTCP: ☐ (unchecked)
 - MKI: ☐ (unchecked)
 - Lifetime: 2^ (text input)
 - Interworking: ☒ (checked)
- Miscellaneous:**
 - Capability Negotiation: ☒ (checked)

At the bottom of the window, there are 'Back' and 'Next' buttons.

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Domain Policies' and 'Media Rules' highlighted. The main content area is titled 'Media Rules: default-low-med' and features an 'Add' button, a 'Filter By Device...' dropdown, 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 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing settings for Audio Encryption and Video Encryption. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. A 'Miscellaneous' section at the bottom has 'Capability Negotiation' unchecked. An 'Edit' button is located at the bottom right of the configuration area.

7.10.3. Signaling Rules

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

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ **Domain Policies**
  Application Rules
  Border Rules
  Media Rules
  Security Rules
  Signaling Rules
  End Point Policy Groups
  Session Policies
‣ TLS Management
‣ Device Specific Settings

Signaling Rules: default

Add Filter By Device... Clone

Signaling Rules
default
No-Content-Typ...
SessMgr_CM_S...
OPTIONS
Remote Workers
Remove_Update
Contact
Remove PAI
Remove PAI_1
Remove_headers

General Requests Responses Request Headers Response Headers Signaling QoS UCID

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

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 ☒

Action	Allow	Multipart Action	Allow
--------	-------	------------------	-------

Exception List Exception List

Edit

7.11. End Point Policy Groups

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

7.11.1. End Point Policy Group – Enterprise

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

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

Policy Group X

Group Name Enterprise

Next

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

- **Application Rule: 2000 Sessions** (Section 7.10.1).
- **Border Rule: default**.

- **Media Rule:** *SM_SRTP* (Section 7.10.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.10.3).
- Click **Finish**.

Policy Group	
Application Rule	2000 Sessions
Border Rule	default
Media Rule	SM_SRTP
Security Rule	default-low
Signaling Rule	default

Back Finish

7.11.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described. In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, except for the Application Rule, which was set to **2000 Sessions** (Section 7.10.1).

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

Session Border Controller for Enterprise AVAYA

Alarms **1** Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Policy Groups: Service Provider

Filter By Device... ▾

Policy Groups

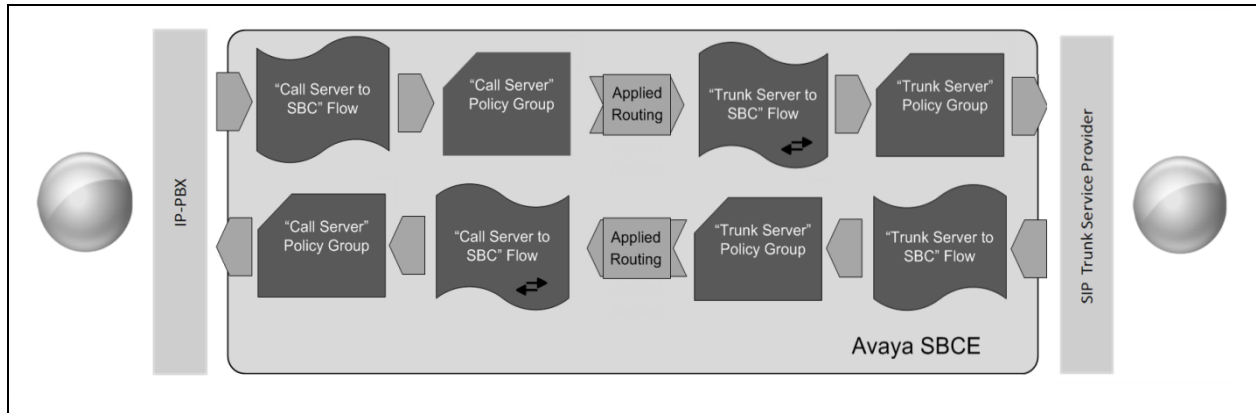
- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-s...
- avaya-def-high-s...
- Enterprise
- Service Provider**

Policy Group

Order	Application	Border	Media	Security	Signaling	
1	2000 Sessions	default	default-low-med	default-low	default	<input type="button" value="Edit"/>

7.12. 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.

7.12.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named *Session_Manager_Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.8.2**, which is the reverse route of the flow. Click **Finish**.

Edit Flow: Session_Manager_Flow	
Flow Name	Session_Manager_Flow
Server Configuration	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

Finish

7.12.2. 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 7.8.1**, 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
Server Configuration	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 ▼

Finish

8. Smart City Telecom SIP Trunk Service Configuration

To use Smart City Telecom SIP Trunk Service, a customer must request the service from Smart City using the established sales processes. The process can be started by contacting Smart City via the corporate web site at: <https://www.smartcitytelecom.com/> or call 407-828-6700.

During the signup process, Smart City and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Smart City's network. Smart City will provide their SIP Proxy public IP address, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, SIP Trunk registration credentials, etc. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

9. Verification and Troubleshooting

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

9.1. General Verification Steps

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

9.2. Communication Manager Verification

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

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

9.3. Session Manager Verification

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

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text "Aura® System Manager 7.1", a "Last Logged on at July 5, 2017 11:33 AM" timestamp, a "Go..." search field, and a "Log off admin" button. Below this is a breadcrumb trail: "Home / Elements / Session Manager / System Status / SIP Entity Monitoring". The left sidebar contains a tree view with categories like "Session Manager", "Network", "Device and Location", "Application", "System Status", "Managed", "Bandwidth Usage", "Security Module", and "SIP Firewall". The "System Status" category is expanded, and "SIP Entity Monitoring" is selected. The main content area is titled "SIP Entity Link Monitoring Status Summary" and includes a description: "This page provides a summary of Session Manager SIP entity link monitoring status." Below this is a section titled "SIP Entities Status for All Monitoring Session Manager Instances" with a "Run Monitor" button. A table shows the status of monitored entities. The table has columns for "Session Manager", "Type", and "Monitored Entities" (which includes "Down", "Partially Up", "Up", "Not Monitored", "Deny", and "Total"). There is one row for "Session Manager" of type "Core" with 1 Down, 0 Partially Up, 5 Up, 0 Not Monitored, 0 Deny, and a Total of 6. At the bottom, there is a "Select: All, None" option.

Session Manager	Type	Monitored Entities					
		Down	Partially Up	Up	Not Monitored	Deny	Total
Session Manager	Core	1	0	5	0	0	6

Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

AVAYA
Aura® System Manager 7.1

Last Logged on at July 5, 2017 11:33 AM
Go... Log off admin

Home / Session Manager x

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Session Manager Entity Link Connection Status

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

All Entity Links for Session Manager: Session Manager

Status Details for the selected Session Manager:

Summary View

6 Items Refresh Filter: Enable

SIP Entity Name	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 SBCE	IPv4	10.64.101.2	5061	TLS	FALSE	UP	200 OK	UP
Communication Manager Trunk 1	IPv4	10.64.101.2	5061	TLS	FALSE	UP	200 OK	UP
AA-Messaging	IPv4	10.64.101.2	5060	TCP	FALSE	UP	200 OK	UP
Communication Manager Trunk 2	IPv4	10.64.101.2	5071	TLS	FALSE	UP	200 OK	UP
Communication Manager Trunk 98	IPv4	10.64.101.2	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.

Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

Information	
System Time	04:34:02 PM EDT Refresh
Version	7.1.0.2-01-13249
Build Date	Fri Mar 3 17:33:08 EST 2017
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/05/2017 15:52:57 EDT
Failed Login Attempts	0

Installed Devices

EMS

Avaya_SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya_SBCE : Heartbeat Successful, Server is UP

Avaya_SBCE : Heartbeat Failed, Server is Down

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

The screenshot shows the 'Alarm Viewer' page. On the left, there is a sidebar with a 'Devices' section containing 'EMS' and 'Avaya_SBCE' (with a red '1' next to it). The main area is titled 'Alarms' and contains a table with columns: ID, Details, State, Time, and Device. Below the table, it states 'No alarms found for this device.' and has two buttons: 'Clear Selected' and 'Clear All'.

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

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The top navigation bar includes 'Alarms', 'Incidents' (highlighted with a red arrow), 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists various management options under 'Dashboard', 'Administration', 'Backup/Restore', and 'System Management'. The main content area displays a warning about Avaya demo certificates, a list of expired certificates, and sections for 'Information', 'Installed Devices', 'Alarms (past 24 hours)', and 'Incidents (past 24 hours)'.

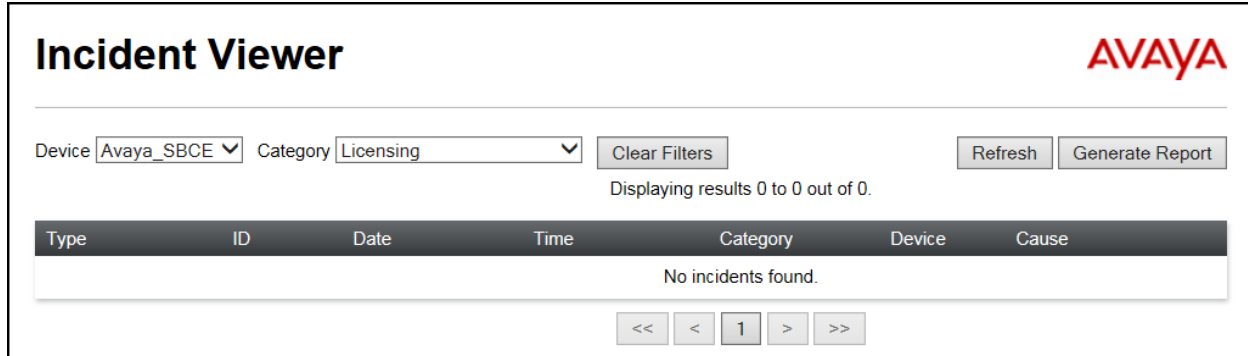
Information	
System Time	04:34:02 PM EDT Refresh
Version	7.1.0.2-01-13249
Build Date	Fri Mar 3 17:33:08 EST 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/05/2017 15:52:57 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE : Heartbeat Successful, Server is UP
Avaya_SBCE : Heartbeat Failed, Server is Down

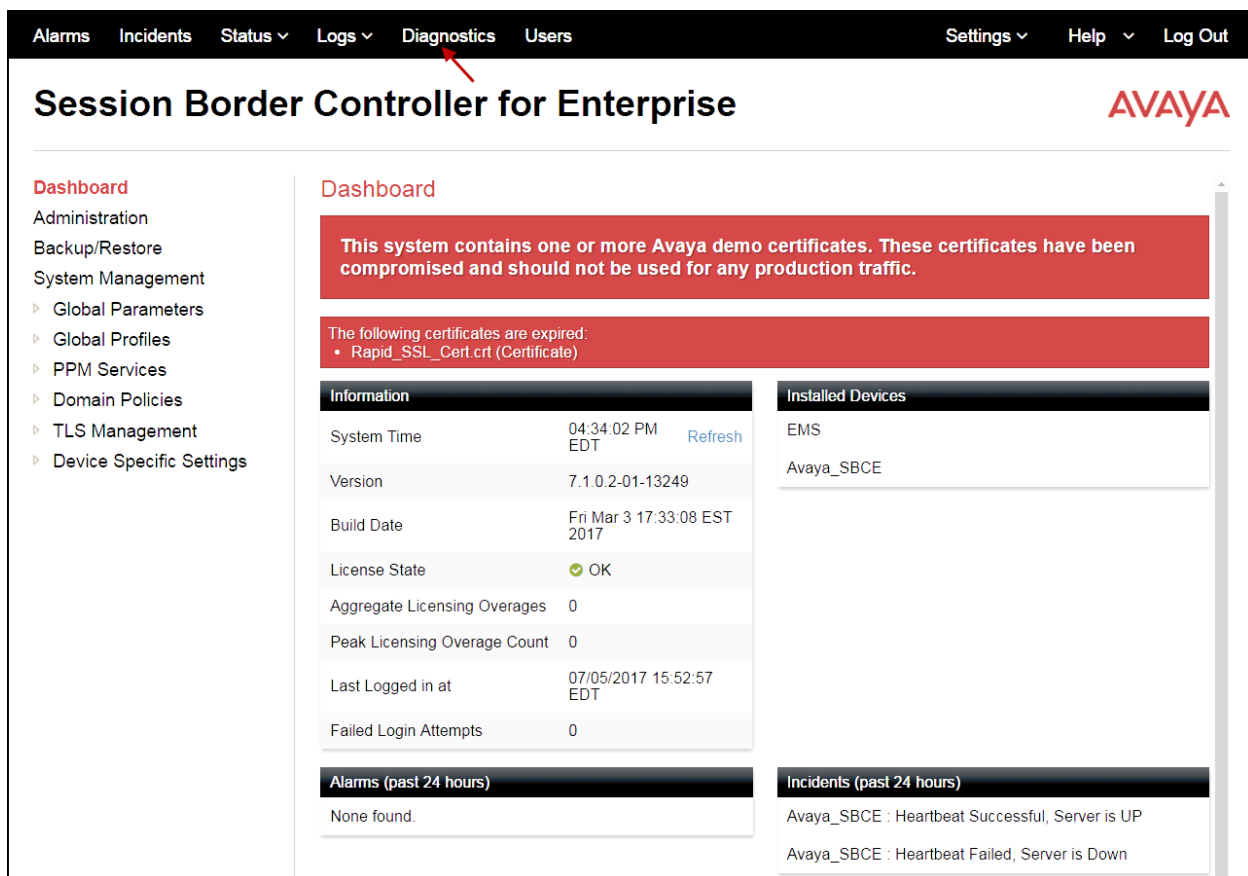
The following screen shows the Incident Viewer page.



The Incident Viewer page features a header with the Avaya logo. Below the header, there are filters for 'Device' (set to 'Avaya_SBCE') and 'Category' (set to 'Licensing'), along with 'Clear Filters', 'Refresh', and 'Generate Report' buttons. A status message indicates 'Displaying results 0 to 0 out of 0.' Below this is a table with columns: Type, ID, Date, Time, Category, Device, and Cause. The table is currently empty, displaying 'No incidents found.' At the bottom, there are pagination controls showing page 1 of 1.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

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



The 'Session Border Controller for Enterprise' Diagnostics page has a top navigation bar with links for Alarms, Incidents, Status, Logs, Diagnostics (highlighted with a red arrow), and Users. On the right, there are links for Settings, Help, and Log Out. The left sidebar lists navigation options under 'Dashboard', including Administration, Backup/Restore, System Management, and various configuration settings. The main content area displays a warning about compromised demo certificates, a list of expired certificates, and several informational panels.

Warning: This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

Expired Certificates:

- Rapid_SSL_Cert.crt (Certificate)

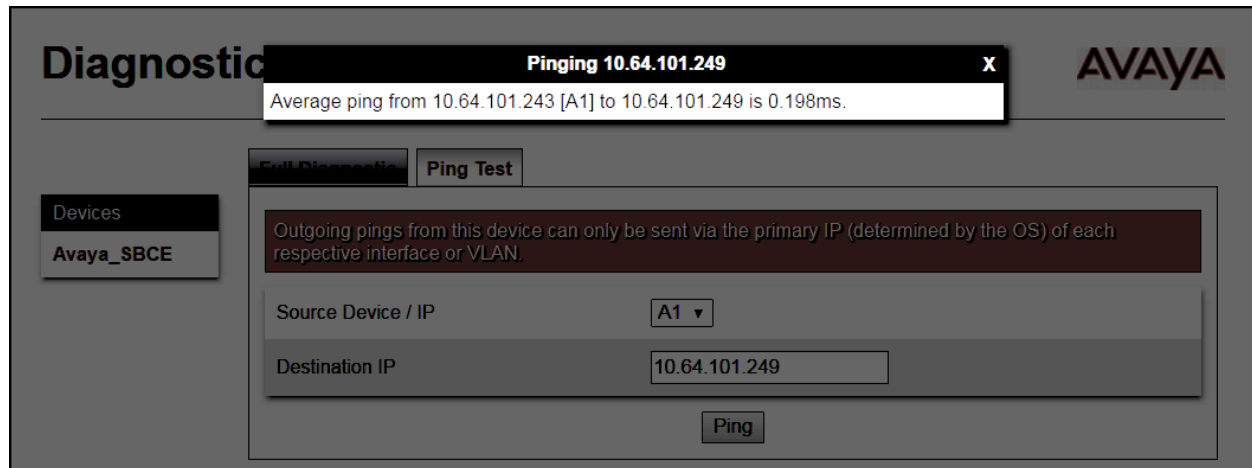
Information	
System Time	04:34:02 PM EDT Refresh
Version	7.1.0.2-01-13249
Build Date	Fri Mar 3 17:33:08 EST 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/05/2017 15:52:57 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE : Heartbeat Successful, Server is UP
Avaya_SBCE : Heartbeat Failed, Server is Down

The following screen shows the Diagnostics page with the results of a successful 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 **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot displays the Avaya SBCE web interface. The top navigation bar includes links for 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. A left-hand navigation menu lists various system management options, with "Device Specific Settings" expanded to show "Troubleshooting" and "Trace". The "Trace" option is selected, leading to the "Trace: : Avaya_SBCE" page. This page has two tabs: "Packet Capture" (active) and "Captures". A blue notification banner states: "A packet capture is currently in progress. This page will automatically refresh until the capture completes." Below this is the "Packet Capture Configuration" section, which includes a table with the following details:

Packet Capture Configuration	
Status	In Progress
Interface	Any
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	Test_Capture.pcap

A "Stop Capture" button is located at the bottom right of the configuration table.

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 displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various system management options, with 'Device Specific Settings' and 'Troubleshooting' expanded. The 'Trace' option under Troubleshooting is highlighted. The main content area shows a 'Trace: : Avaya_SBCE' header. Below this, there are tabs for 'Devices' and 'Avaya_SBCE'. The 'Captures' tab is active, displaying a table of captured files. The table has columns for File Name, File Size (bytes), and Last Modified. A single entry is shown: 'Test_Capture_20170705164248.pcap' with a size of 172,032 bytes and a timestamp of July 5, 2017 4:43:08 PM EDT. A 'Delete' button is next to the entry. A 'Refresh' button is located at the top right of the table.

File Name	File Size (bytes)	Last Modified
Test_Capture_20170705164248.pcap	172,032	July 5, 2017 4:43:08 PM EDT

10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1 and Avaya Session Border Controller for Enterprise 7.1, to connect to the Smart City Telecom SIP Trunk 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*, Release 7.1, Issue 1, May 2017.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.1, Issue 1, May 2017.
- [3] *Administering Avaya Aura® System Manager for Release 7.1*, Issue 3, July 2017.
- [4] *Deploying Avaya Aura® System Manager*, Release 7.1, Issue 2, July 2017.
- [5] *Deploying Avaya Aura® Session Manager*, Release 7.1, Issue 1, May 2017.
- [6] *Administering Avaya Aura® Session Manager*, Release 7.1, Issue 1, May 2017.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 2, January 2017.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Issue 3, May 2017.
- [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 7.7 FP1, Issue 4, April 2017.
- [11] *Implementing and Administering Avaya Aura® Media Server*. Release 7.7, Issue 5, September 2016.
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [13] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2017 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.