



Application Notes for Bell Canada SIP Trunking Service with Avaya Aura® Communication Manager Release 7.1.1, Avaya Aura® Session Manager Release 7.1.1 and Avaya Session Border Controller for Enterprise Release 7.2 with T.38 Supported – Issue 1.0

Abstract

These Application Notes describe the steps to configure a Session Initiation Protocol (SIP) trunk between Bell Canada SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.1.1, Avaya Aura® Session Manager 7.1.1, Avaya Session Border Controller for Enterprise 7.2, Avaya Aura® Media Server 7.8, Avaya Aura® Messaging 7.0 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for 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.

Bell Canada is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing is 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.....	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	9
5.	Configure Avaya Aura® Communication Manager	10
5.1.	Licensing and Capacity	10
5.2.	System Features	12
5.3.	IP Node Names	13
5.4.	Codecs.....	14
5.5.	IP Network Region	15
5.6.	Signaling Group.....	17
5.7.	Trunk Group.....	19
5.8.	Calling Party Information	21
5.9.	Incoming Call Handling Treatment	21
5.10.	Outbound Routing.....	22
5.11.	Saving Communication Manager Configuration Changes	23
5.12.	TLS Management on Communication Manager.....	24
6.	Configure Avaya Aura® Session Manager	27
6.1.	System Manager Login and Navigation	27
6.2.	Specify SIP Domain.....	28
6.3.	Add Location	28
6.4.	Add Adaptations	29
6.5.	Add SIP Entities.....	30
6.6.	Add Entity Links.....	34
6.7.	Add Routing Policies	35
6.8.	Add Dial Patterns.....	37
6.9.	TLS Certificate Management on System Manager.....	39
7.	Configure Avaya Session Border Controller for Enterprise	39
7.1.	Avaya Session Border Controller for Enterprise Login.....	40
7.2.	TLS Management.....	41
7.2.1.	Certificates	42
7.2.2.	Client Profiles	43
7.2.3.	Server Profiles	44
7.3.	Global Profiles	45
7.3.1.	Uniform Resource Identifier (URI) Groups	45
7.3.2.	Server Interworking Profile	45
7.3.3.	Signaling Manipulation	51
7.3.4.	Server Configuration	51
7.3.5.	Routing Profiles	55
7.3.6.	Topology Hiding.....	57
7.4.	Domain Policies	59

7.4.1.	Media Rules	59
7.4.2.	Signaling Rules	60
7.4.3.	Endpoint Policy Groups.....	61
7.5.	Device Specific Settings	63
7.5.1.	Network Management	63
7.5.2.	Media Interface	65
7.5.3.	Signaling Interface.....	65
7.5.4.	End Point Flows - Server Flow.....	67
8.	Bell Canada Service Configuration	70
9.	Verification and Troubleshooting	70
9.1.	Verification Steps.....	70
9.2.	Protocol Traces	70
9.3.	Troubleshooting:	71
9.3.1.	The Avaya SBCE.....	71
9.3.2.	Communication Manager	71
10.	Conclusion	72
11.	References	73

1. Introduction

These Application Notes describe the steps to configure a SIP trunk between Bell Canada SIP Trunking Service and an Avaya SIP-enabled enterprise solution. Avaya Aura® Release 7.1.1 is being deployed in virtualized environment that includes Avaya Aura® Communication Manager 7.1.1 (Communication Manager), Avaya Aura® Session Manager 7.1.1 (Session Manager), Avaya Aura® Media Server 7.8, Avaya Aura® Messaging and Avaya Session Border Controller for Enterprise 7.2 (Avaya SBCE). Various Avaya endpoints are also used in the test configuration.

For privacy and security, TLS for signaling and SRTP for media encryption were used inside of the enterprise (private network side). Outside of the enterprise (public network side) to Bell Canada was using UDP and RTP.

Customers using this Avaya SIP-enabled enterprise solution with Bell Canada are able to place and receive PSTN calls via a broadband Internet connection. This converged network solution is an alternative to a traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Aura® SIP-enabled enterprise solution connecting to Bell Canada SIP Trunking service via the Avaya SBCE. This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

2.1. Interoperability Compliance Testing

To verify Bell Canada interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including H.323, SIP, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, SIP, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) and Avaya Equinox™ for Windows soft phones.
- Dialing plans including local, long distance, international, outbound toll-free, calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codec G.711MU and G.729.
- Media and Early Media transmissions.
- Incoming and outgoing fax using T.38.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with Diversion method.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.

Item that is supported but not tested includes the following:

- Inbound toll-free.

2.2. Test Results

Interoperability testing of Bell Canada with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations and limitations described below:

- **SIP Options** – Bell Canada was configured to send SIP OPTIONS messages with Max-Forwards header with value equal to 0. This was by design from Bell Canada. Avaya SBCE responded correctly with 483 Too Many Hops. However, Bell Canada would accept this and keep the trunk up.
- **Outbound Calls with “+”** – Bell Canada did not accept “+” in front of 10 digits in the From, To, Contact and P-Asserted-Identity headers. Signaling Manipulation script was used to remove the “+” sign. Also note that Bell system would accept “+” in front of 11 digits format.
- **Diversion Header** – Avaya system sent Diversion header with URI “sips:XXXX....”. Bell Canada rejected this format since it is not secure SIP. Signaling Manipulation script was used to change the URI format to “sip:XXXX....”.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on Bell Canada SIP Trunking, contact Bell Canada at http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page.

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the Bell Canada (Vendor Validation circuit) through a public Internet connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

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

- Avaya Aura® Communication Manager running in Virtualized environment.
- Avaya Aura® System Manager running in Virtualized environment.
- Avaya Aura® Session Manager running in Virtualized environment.
- Avaya Aura® Messaging running in Virtualized environment.
- Avaya Aura® Media Server running in Virtualized environment.
- Avaya G450 Media Gateway.
- Avaya Session Border Controller for Enterprise.
- Avaya 9600Series IP Deskphones (H.323, SIP).
- Avaya one-X® Communicator soft phones (H.323, SIP).
- Avaya digital and analog telephones.
- Avaya Equinox™ for Windows.

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to Bell Canada via Internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Bell Canada across the public network is UDP. The transport protocol between the Avaya SBCE, Session Manager and Communication Manager is TLS.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain “avayalab.com” for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the SIP domain based URI-Host known to Bell Canada.

Figure 1 below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

Additionally, a remote worker is included in the reference configuration **Figure 1**. A remote worker is a SIP endpoint that resides in the un-trusted network, registered to Session Manager via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test, using the Avaya Communicator for Windows using TLS/SRTP. The configuration tasks required to support remote workers are referenced in **Section 11**.

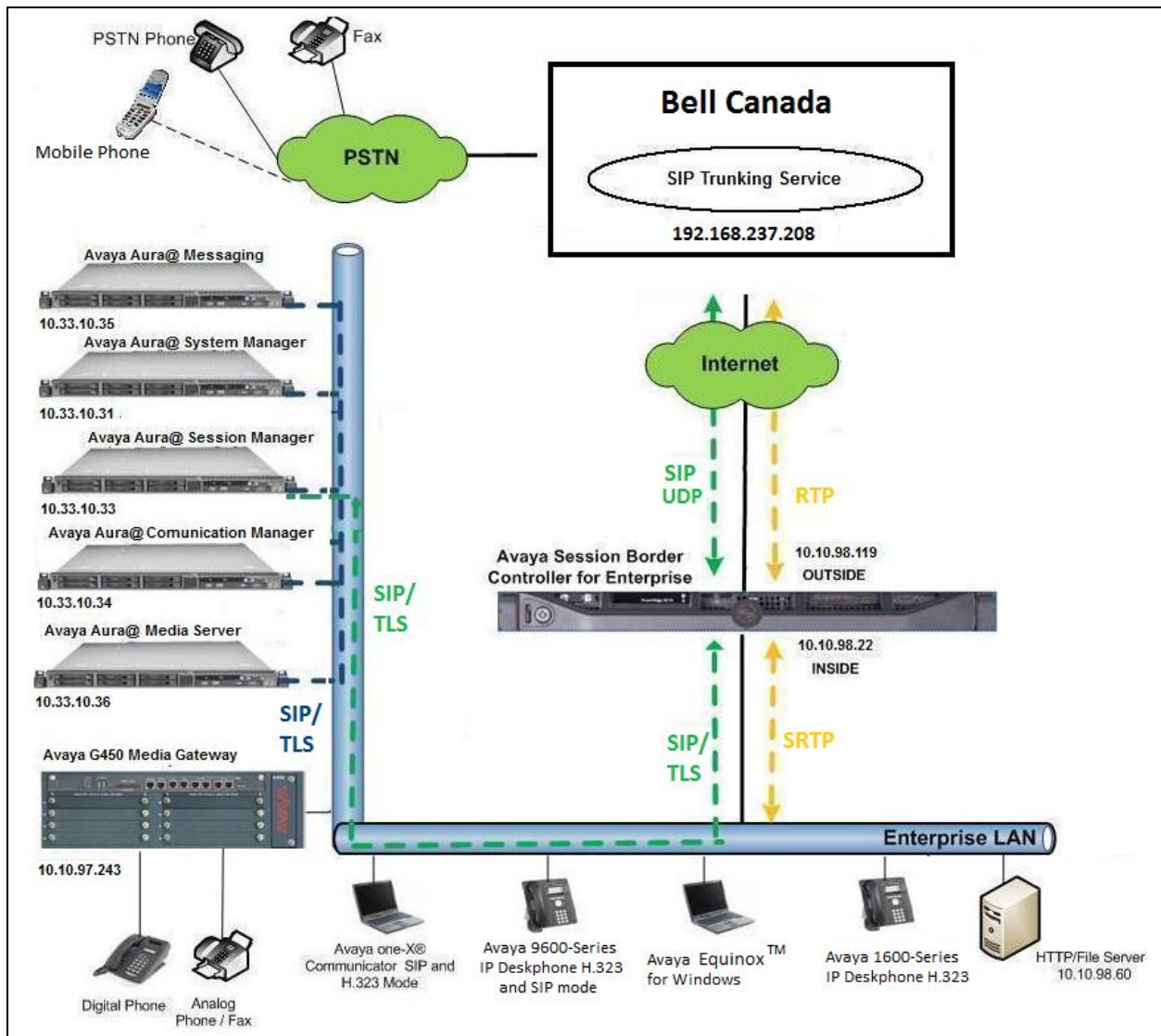


Figure 1: Avaya IP Telephony Network connecting to Bell Canada Networks

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on Virtualized Environment	7.1.1.0.0-FP1
Avaya G450 Media Gateway	38.20.1
Avaya Aura® System Manager running on Virtualized Environment	7.1.1.0
Avaya Aura® Session Manager running on Virtualized Environment	7.1.1.0.
Avaya Aura® Messaging running on Virtualized Environment	7.0.0.0.441-e55-0
Avaya Aura® Media Server running on Virtualized Environment	7.8
Avaya Session Border Controller for Enterprise	7.2.0.0-18-13712
Avaya 9621G IP Deskphone (H.323)	6.6.401
Avaya 9641G IP Deskphone (SIP)	7.0.1.2.9
Avaya one-X® Communicator (H.323/SIP)	6.2.12.04-SP12
Avaya Equinox™ for Windows	3.2.0.35
Avaya 1608 IP Deskphone (H.323)	1.380B
Avaya 1408 Digital Telephone	1408D02A-003
Avaya Analog Telephone	n/a
Bell Canada SIP Trunking Service Components	
Component	Release
ACME Packet SBC 4500	7.3.0 MR3 Patch 3
Broadworks	Release 20 SP1.1.606

Table 1: Equipment and Software Tested

Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Bell Canada SIP Trunking service. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Media Server has been previously completed and is not discussed here.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The 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 sale representative to add the additional capacity or feature.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks: 4000	0	
Maximum Concurrently Registered IP Stations: 2400	1	
Maximum Administered Remote Office Trunks: 4000	0	
Maximum Concurrently Registered Remote Office Stations: 2400	0	
Maximum Concurrently Registered IP eCons: 68	0	
Max Concur Registered Unauthenticated H.323 Stations: 100	0	
Maximum Video Capable Stations: 2400	0	
Maximum Video Capable IP Softphones: 2400	3	
Maximum Administered SIP Trunks: 4000	74	
Maximum Administered Ad-hoc Video Conferencing Ports: 4000	0	
Maximum Number of DS1 Boards with Echo Cancellation: 80	0	
(NOTE: You must logoff & login to effect the permission changes.)		

On **Page 4**, verify that **ARS** is set to **y**.

display system-parameters customer-options		Page	4 of	12
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	Computer Telephony Adjunct Links?	y	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y	
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y	
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y	
ATMS?	y			
Attendant Vectoring?	y			
(NOTE: You must logoff & login to effect the permission changes.)				

On **Page 5**, verify that **IP Trunks** field is set to **y** and **Media Encryption Over IP** field is set to **y**.

(Note: The Media Encryption option is only available if Media Encryption Over IP is enabled on the installed license)

display system-parameters customer-options		Page	5 of	12
OPTIONAL FEATURES				
Emergency Access to Attendant? y		IP Stations? y		
Enable 'dadmin' Login? y				
Enhanced Conferencing? y		ISDN Feature Plus? n		
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y			
Enterprise Survivable Server? n		ISDN-BRI Trunks? y		
Enterprise Wide Licensing? n		ISDN-PRI? y		
ESS Administration? y	Local Survivable Processor? n			
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y			
External Device Alarm Admin? y	Media Encryption Over IP? y			
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n			
Flexible Billing? n				
Forced Entry of Account Codes? y		Multifrequency Signaling? y		
Global Call Classification? y		Multimedia Call Handling (Basic)? y		
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y			
Hospitality (G3V3 Enhancements)? y		Multimedia IP SIP Trunking? y		
IP Trunks? y				
IP Attendant Consoles? y				
(NOTE: You must logoff & login to effect the permission changes.)				

On **Page 6**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

display system-parameters customer-options		Page 6 of 12
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? n		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? n	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
Processor Ethernet? y	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		
(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 an incoming call from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to **none**.

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

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. 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: 1
    International Access Code: 001

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**), Session Manager (**SM**) and Media Server (**AMS**). These node names will be needed for defining the signaling groups in **Section 5.6**.

```

change node-names ip                                               Page 1 of 2
                                IP NODE NAMES

    Name          IP Address
SM              10.33.10.33
AMS             10.33.10.36
default          0.0.0.0
procr           10.33.10.34
procr6           ::

```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 1. Bell Canada supports G.711MU and G.729 in this order. To use these codecs, enter **G.711MU** and **G.729** in the **Audio Codec**. For media encryption used within Avaya system, the **1-srtp-aescm128-hmac80**, **2-srtp-aescm128-hmac32** and **none** are used in **Media Encryption** and **best-effort** in **Encrypted SRTCP** columns of the table in the order of preference.

The following screen shows the configuration for ip-codec-set 1. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

change ip-codec-set 1

Page1 of 2

IP CODEC SET

Codec Set: 1

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

Media Encryption

Encrypted SRTCP: best-effort

1:	1-srtp-aescm128-hmac80
2:	2-srtp-aescm128-hmac32
3:	none

On **Page 2**, set the **Fax Mode** to **t.38-standard** faxing which is supported by Bell Canada.

change ip-codec-set 1			Page	2 of	2
IP CODEC SET					
Allow Direct-IP Multimedia? n					
	Mode	Redundancy	Packet Size(ms)		
FAX	t.38-standard	1			
Modem	off	0			
TDD/TTY	US	3			
H.323 Clear-channel	n	0			
SIP 64K Data	n	0	20		

5.5. IP Network Region

For the compliance testing, ip-network-region 1 was created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is *avayalab.com*. This domain name appears in the “From” header of SIP message originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to *yes*. Shuffling can be further restricted at the trunk level under the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: avayalab.com
Name: ToSM
MEDIA PARAMETERS                                Intra-region IP-IP Direct Audio: yes
Codec Set: 1      Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
...
```

On **Page 4**, define the IP codec set to be used for traffic between region 1 and other regions. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, IP/SIP phones and Session Manager were assigned to the same region 1.

```
change ip-network-region 1                                     Page 4 of 20

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

Non-IP telephones (e.g., analog, digital) derive network region from the IP interface of the Avaya G450 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

change ip-interface procr	Page 1 of 2
IP INTERFACES	
Type: PROCR	Target socket load: 4800
Enable Interface? y	Allow H.323 Endpoints? y
Network Region: 1	Allow H.248 Gateways? y
...	Gatekeeper Priority: 5

To define network region 1 for the Avaya G450 Media Gateway, use **change media-gateway** command as shown in the following screen.

change media-gateway 1	Page 1 of 2
MEDIA GATEWAY 1	
Type: g450	
Name: g450	
Serial No: 11N526797797	
Link Encryption Type: any-ptls/tls	Enable CF? n
Network Region: 1	Location: 1
	Site Data:
Recovery Rule: none	
...	

If Avaya Aura® Media Server is used in parallel of Avaya Media Gateway G450, then it is needed to define network region 1 for the Avaya Aura® Media Server. Use **change media-server** command as shown in the following screen.

change media-server 1	Page 1 of 1
MEDIA SERVER	
Media Server ID: 1	
Signaling Group: 3	
Voip Channel License Limit: 30	
Dedicated Voip Channel Licenses: 30	
Node Name: AMS	
Network Region: 1	
Location: 1	
Announcement Storage Area:	
...	

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 Avaya SBCE 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.

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- Set the **Transport Method** to *tls* (*Transport Layer Security*). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to *5061*.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP interface of *procr* 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 **Far-end Network Region** to the IP network region *1* defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to *avayalab.com*.
- Set the **DTMF over IP** to *rtp-payload*. This setting enables Communication Manager to send or receive the DTMF transmissions using RFC2833.
- Set **Enable Layer 3 Test?** to *y*. This setting allows Communication Manager to send OPTIONS heartbeat to Session Manager on the SIP trunk.
- 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 SIP trunk and the enterprise endpoint. If this value is set to *n*, then the Avaya G450 Media Gateway will remain in the media path between the SIP trunk and the endpoint for the duration of the call. Depending on the number of media resources available in the Avaya G450 Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Alternate Route Timer** to *30*. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Default values may be used for all other fields.

Signaling Group 2:

add 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: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
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? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 30	

Another signaling group is created between Communication Manager and the Media Server to provide media resources for IP telephony in parallel of the media gateway G450. For the compliance test, signaling group 3 was used for this purpose and was configured as shown in the capture below.

Signaling Group 3:

add signaling-group 3		Page 1 of 2
SIGNALING GROUP		
Group Number: 3	Group Type: sip	
	Transport Method: tls	
Peer Detection Enabled? n Peer Server: AMS		
Near-end Node Name: procr	Far-end Node Name: AMS	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: 10.33.10.36		

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 0**. For the compliance testing, 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 **Outgoing Display** to *y* to enable name display on the trunk.
- Set the **Service Type** field to *public-ntwrk*.
- Set the **Signaling Group** to the signaling group **2** shown in **Section 0**.
- Set the **Number of Members** field to customer requirement. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk group.
- Default values are used for all other fields.

```
add trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                                     Group Type: sip          CDR Reports: y
  Group Name: SIP-Carrier                          COR: 1                TN: 1          TAC: #02
  Direction: two-way                               Outgoing Display? y
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: 32
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval re-INVITEs must be sent to refresh the Session Timer. For the compliance testing, a default value of **600** seconds was used.

```
add trunk-group 2                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
                                     SCCAN? n                Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
  XOIP Treatment: auto      Delay Call Setup When Accessed Via IGAR? N
Caller ID for Service Link Call to H.323 1xC: station-extension
```

On **Page 3**, set the **Numbering Format** field to *public*. This field specifies the format of the CPN sent to the far-end. The public numbers are automatically preceded with a + sign when passed in the “From”, “Contact” and “P-Asserted Identity” headers.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to *y*. This will allow the CPN displayed on the local endpoint to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values are used for all other fields.

add trunk-group 2		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		
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**, the settings are as follow:

- Set of **Network Call Redirection** flag to *y* to enable the use of SIP REFER message to transfer calls back to the PSTN as service provider does support it. It can also be set to *n* if the use of re-INVITE for call re-direction is preferred.
- Set the **Send Diversion Header** field to *y* as service provider does support it.
- Set the **Support Request History** field to *n*.
- Set the **Telephone Event Payload Type** to *101*.

add trunk-group 2		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n		
Send Transferring Party Information? n		
Network Call Redirection? y		
Build Refer-To URI of REFER From Contact For NCR? n		
Send Diversion Header? y		
Support Request History? n		
Telephone Event Payload Type: 101		
Convert 180 to 183 for Early Media? n		
Always Use re-INVITE for Display Updates? n		
Identity for Calling Party Display: P-Asserted-Identity		
Block Sending Calling Party Location in INVITE? n		
Accept Redirect to Blank User Destination? n		
Enable Q-SIP? n		
...		

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering is selected to define the format of this number (**Section 0**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the service provider. They are used to authenticate the caller.

The screen below shows a subset of the 10-digit DID numbers assigned for testing. These 4 numbers were mapped to the 4 enterprise extensions 60396, 60397, 60379 and 60398. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

Note: When using 10-digit CPN that the + will need to be removed from the SIP message by the Avaya SBCE.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total Len	
5	60396	2	613XXX6506	10	Total Administered: 6
5	60397	2	613XXX6507	10	Maximum Entries: 240
5	60379	2	613XXX6508	10	
5	60398	2	613XXX6509	10	

5.9. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by Bell Canada can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** 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	613XXX6506	10	60396	
public-ntwrk	10	613XXX6507	10	60397	
public-ntwrk	10	613XXX6508	10	60379	
public-ntwrk	10	613XXX6509	10	60398	

5.10. Outbound Routing

In these Application Notes, the **Automatic Route Selection (ARS)** feature is used to route an outbound call via the SIP trunk to the service provider via the Avaya SBCE. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) **9**, use the **change dialplan analysis** command as shown below.

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	
1	4	ext							
30	4	ext							
39	5	udp							
60	5	ext							
9	1	fac							
*	3	dac							
#	3	dac							

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

change feature-access-codes			FEATURE ACCESS CODE (FAC)						Page 1 of 10
			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: *05						
			Answer Back Access Code:						
			Attendant Access Code:						
			Auto Alternate Routing (AAR) Access Code:						
			Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2:			

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example pattern below shows a sample of the dialed strings calling on service provider. All dialed strings are mapped to route pattern **2** for an outbound call which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0							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 Reqd	
011	3	36	2	intl		n	
1613	11	11	2	pubu		n	
613	11	11	2	pubu		n	
411	5	10	2	svcl		n	
911	3	3	2	svcl		n	

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern **2** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group **2** was used.
- **FRL:** Set the Facility Restriction Level (FRL) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** *pub-unk*. All calls using this route pattern will use the public numbering table as shown in **Section 5.8**.

change route-pattern 2													Page	1 of	3	
Pattern Number: 2													Pattern Name: SP Route			
SCCAN? n													Secure SIP? n			
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits						QSIG			
								Dgts						Intw		
1: 2	0											n	user			
2:											n	user				
....																
BCC		VALUE		TSC	CA-TSC		ITC		BCIE		Service/Feature		PARM	No.	Numbering	LAR
0	1	2	M	4	W	Request						Dgts	Format			
													Subaddress			
1:	y	y	y	y	y	n	n	rest				pub-unk		none		
...																

5.11. Saving Communication Manager Configuration Changes

The command “**save translation all**” can be used to save the configuration changes made on Communication Manager.

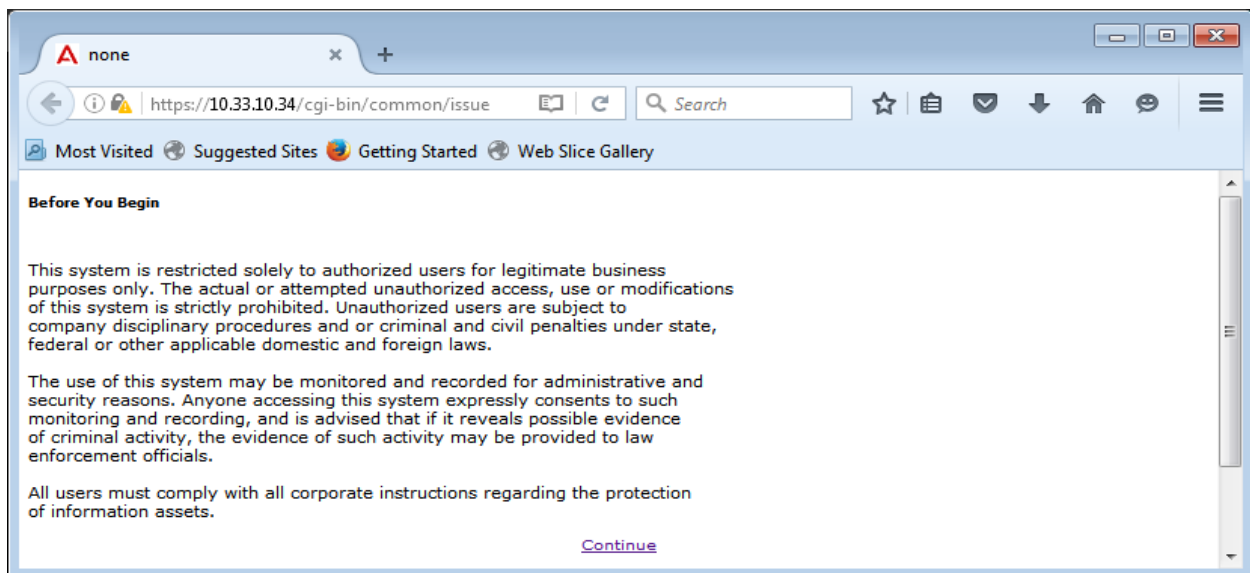
5.12. TLS Management on Communication Manager

It is (or may be) necessary to install System Manager CA certificate on Communication Manager for the TLS signaling to work between Session Manager and Avaya Communication Manager if it is not previously installed.

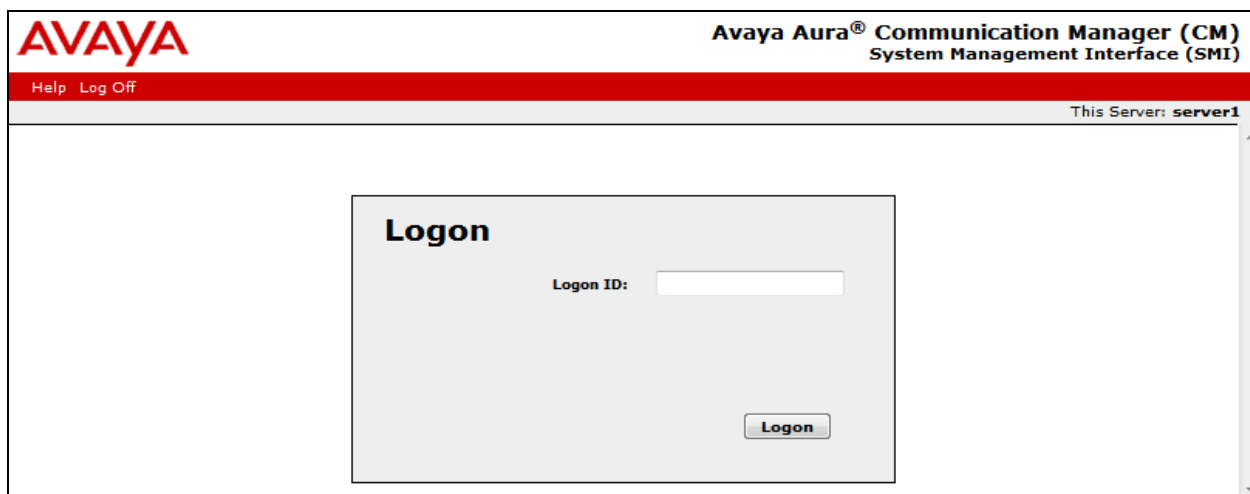
This section is to show how to install System Manager CA certificate on Communication Manager using web console.

System Manager CA certificate is obtained using procedure provided in **Section 6.10**.

From a web browser, type in “https://<ip-address>”, where “<ip-address>” is the IP address or FQDN of Communication Manager. Click on **Continue** and it will be redirect to login page.



At login page, type in the login ID and its password credential.



Click on **Continue** again (not shown), navigate to **Administration** → **Server (Maintenance)** → **Security** → **Trusted Certificates** to verify if the System Manager CA certificate is present or not. If it is not, then continue to the next step.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for 'server1'. The left sidebar contains a navigation menu with categories: Administration / Server (Maintenance), Security, and Miscellaneous. The 'Trusted Certificates' page is active, displaying a table of trusted repositories. The table has columns: Select File, Issued To, Issued By, Expiration Date, and Trusted By. Three certificates are listed: apr-ca.crt, motorola_sscca_root.crt, and sip_product_root.crt. Below the table are buttons for Display, Add, Remove, Copy, and Help.

Select File	Issued To	Issued By	Expiration Date	Trusted By
<input type="radio"/> apr-ca.crt	Avaya Product Root CA	Avaya Product Root CA	Sun Aug 14 2033	C W R
<input type="radio"/> motorola_sscca_root.crt	SCCAN Server Root CA	SCCAN Server Root CA	Sun Dec 04 2033	C
<input type="radio"/> sip_product_root.crt	SIP Product Certificate Authority	SIP Product Certificate Authority	Tue Aug 17 2027	C W R

Navigate to **Miscellaneous** → **Download Files**, click on **File** to download from the machine I'm using to connect to the server and click on **Browse** to browse to where the System Manager CA is being located. Then click on **Download** button to load the System Manager CA on Communication Manager server.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for 'server1'. The left sidebar contains a navigation menu with categories: Administration / Server (Maintenance), Security, and Miscellaneous. The 'Download Files' page is active, displaying options to download files to the server. The first option is 'File(s) to download from the machine I'm using to connect to the server', which has four 'Browse...' buttons. The second option is 'File(s) to download from the LAN using URL', which has three text input fields. Below these is a 'Proxy Server' field with a placeholder '(e.g proxy.domain:3152)'. At the bottom are 'Download' and 'Help' buttons.

Navigate to **Security** → **Trusted Certificates**, click on **Add** button and enter the certificate name which has been downloaded from above step. Then click **Open**.

AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration This Server: server1

Administration / Server (Maintenance)

Trusted Certificates - Add

This page allows for the addition of a trusted certificate to this server.

SystemManagerCA.pem PEM file containing certificate

Open Cancel Help

Enter the name of the System Manager CA certificate to store the certificate in Communication Manager. Check the Communication Manager check-box. Then click **Add**.

AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration This Server: server1

Administration / Server (Maintenance)

Trusted Certificates

This page provides management of the trusted security certificates present on this server.

Add this certificate

Issued To	Issued By	Expiration Date
System Manager CA	System Manager CA	Sat Aug 23 2025

SystemManagerCA Store the certificate in this file in each repository selected below

Add to these trusted repositories

- ☐ Authentication, Authorization and Accounting Services (e.g. LDAP)
- ☒ Communication Manager
- ☐ Web Server
- ☐ Remote Logging

Add Cancel Help

Navigate to **Security** → **Trusted Certificates** again. It now shows the System Manager CA in the **Trusted Repositories**.

AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration This Server: server1

Administration / Server (Maintenance)

Trusted Certificates

This page provides management of the trusted security certificates present on this server.

Trusted Repositories

A = Authentication, Authorization and Accounting Services (e.g. LDAP)
C = Communication Manager
W = Web Server
R = Remote Logging

Select File	Issued To	Issued By	Expiration Date	Trusted By
<input type="radio"/> SystemManagerCA.crt	System Manager CA	System Manager CA	Sat Aug 23 2025	C
<input type="radio"/> apr-ca.crt	Avaya Product Root CA	Avaya Product Root CA	Sun Aug 14 2033	C W R
<input type="radio"/> motorola_sseca_root.crt	SCCAN Server Root CA	SCCAN Server Root CA	Sun Dec 04 2033	C
<input type="radio"/> sip_product_root.crt	SIP Product Certificate Authority	SIP Product Certificate Authority	Tue Aug 17 2027	C W R

Display Add Remove Copy Help

6. Configure Avaya Aura® Session Manager

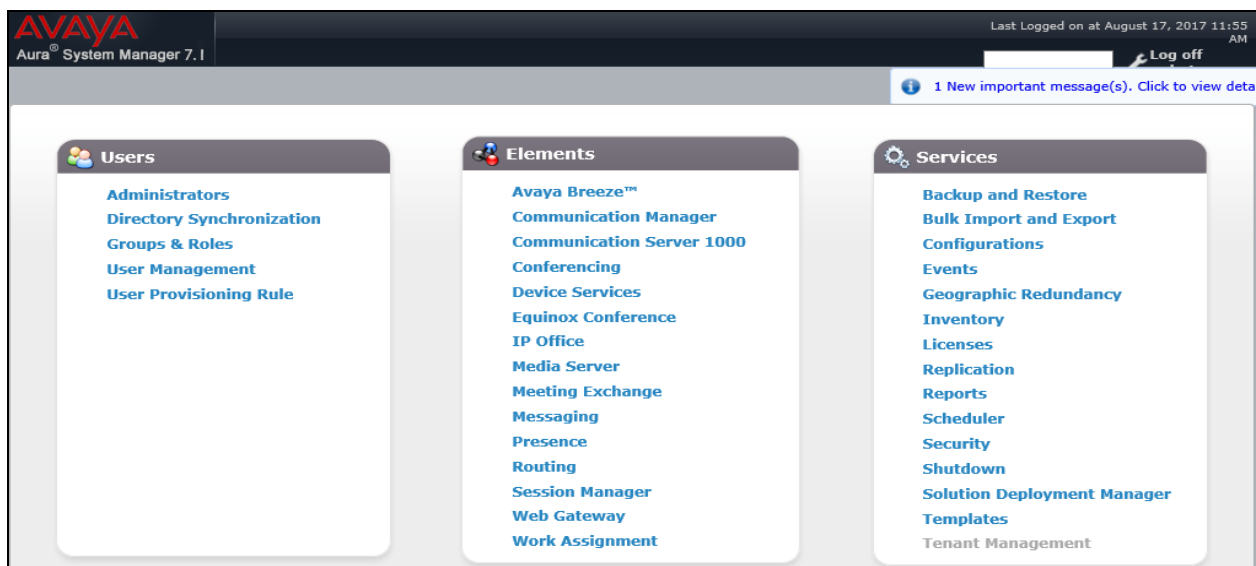
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be used by SIP Entities
- Adaptations
- 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
- TLS Certificate Management

It may not be necessary to configure all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

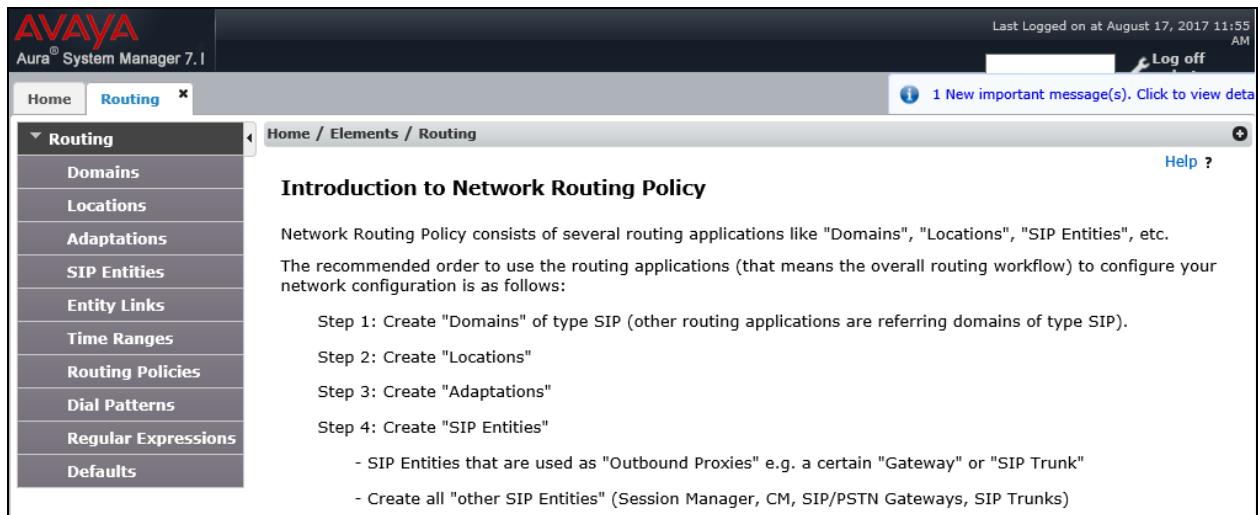
6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the Web GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address or FQDN of System Manager. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



Most of the configuration items are performed in the Routing element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

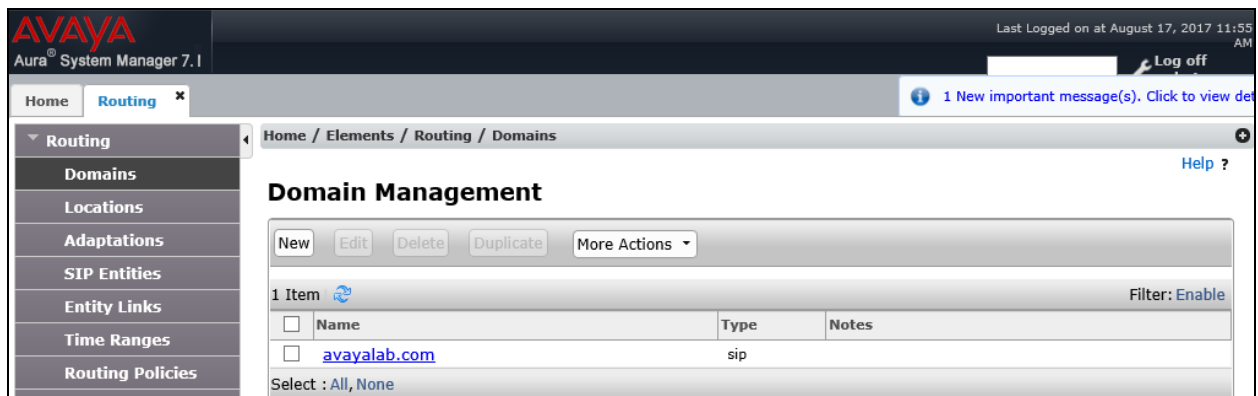
The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



6.2. Specify SIP Domain

To view or to change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain, *avayalab.com* was already created for communication between Session Manager and Communication Manager. The domain *avayalab.com* is not known to Bell Canada. It will be adapted by the Avaya SBCE to SIP domain based URI-Host to meet the SIP specification of Bell Canada system.



6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for bandwidth management and call admission control purposes. To add a location, navigate to

Routing → Locations in the left-hand navigation pane and click **New** button in the right pane (not shown).

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

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

In the **Location Pattern** section (see the screen below), click **Add** and configure following fields:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

Displayed below are the screenshots for location **Belleville**, which includes all equipment on the **10.33.***, **10.10.98.*** and **10.10.97.*** subnets including Communication Manager, Session Manager and Avaya SBCE. Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The left-hand navigation pane shows the 'Routing' section expanded, with 'Locations' selected. The main content area is titled 'Location Details' and includes a 'Commit' button. The 'General' section contains fields for 'Name' (set to 'Belleville') and 'Notes' (set to 'GSSCP Belleville'). Below this is the 'Dial Plan Transparency in Survivable Mode' section, which includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field with a search icon. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'Kbit/sec', 'Total Bandwidth' set to '10000000', and 'Multimedia Bandwidth' set to '10000000'. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked. The 'Location Pattern' section at the bottom features an 'Add' button and a table with 3 items. The table has columns for 'IP Address Pattern' and 'Notes'. The items listed are: '10.33.*', '10.10.97.*', and '10.10.98.*'. The 'Filter' is set to 'Enable' and the 'Select' options are 'All' and 'None'.

IP Address Pattern	Notes
10.33.*	
10.10.97.*	
10.10.98.*	

6.4. Add Adaptations

An adaptation is required by the service provider in order to remove un-wanted or proprietary headers that are not used or understood by the service provider.

To add a new adaptation, navigating to **Routing** → **Adaptations** in the left navigation pane and click **New** button in the right pane (not shown).

- **Adaptation Name:** Enter a descriptive name.
- **Module Name:** Select *DigitConversionAdapter* from pull down list.
- **Module Parameter Type:** Select *Name-Value Parameter* from pull down list.
- Click the **Add** button to enter a **Name** as shown in capture.
- **Value:** Enter the following information as shown in capture and click **Commit** button.

The newly created Adaptation is shown below.

Name	Module Name	Module Parameters	Egress URI Parameters	Notes
Remove-Unused-Headers	DigitConversionAdapter	eRHdrs=AV-Correlation-ID,AV-Global-Session-ID,Endpoint-View,P-AV-Message-ID,P-Charging-Vector,P-Location,P-Preferred-Identity,Alert-Info		

6.5. Add 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 Avaya SBCE.

To add a new SIP Entity, navigate to **Routing** → **SIP Entities** in the left navigation pane and click **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select *Session Manager* for Session Manager, *CM* for Communication Manager and *SIP Trunk* for the Avaya SBCE.
- **Location:** Select the location defined in **Section Error! Reference source not found.**
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot shows the Avaya Aura System Manager 7.1 web interface. The left sidebar contains a navigation menu with options like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. The form fields are as follows:

- Name:** SM7
- FQDN or IP Address:** 10.33.10.33
- Type:** Session Manager (dropdown)
- Location:** Belleville (dropdown)
- Time Zone:** America/Toronto (dropdown)
- SIP Link Monitoring:** Link Monitoring Enabled (dropdown)

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Port** section, click **Add** and enter following values. Use default values for all remaining fields:

- **Listen Ports:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to receive SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save (not shown).

The compliance test used **Listen Ports** entry **5061** with **TLS** for connecting to Communication Manager and for connecting to the Avaya SBCE.

Listen Ports

Add Remove

6 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avayalab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avayalab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avayalab.com	<input checked="" type="checkbox"/>	

Select : All, None

The following screen shows the addition of the Communication Manager SIP Entity. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to IP address of Communication Manager and **Type** to **CM**. The **Location** and **Time Zone** parameters are set as shown in screen below.

AVAYA
Aura® System Manager 7.1

Last Logged on at August 17, 2017 12:32 PM
Go... Log off admin

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

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel Help ?

General

* Name: CM7

* FQDN or IP Address: 10.33.10.34

Type: CM

Notes:

Adaptation:

Location: Belleville

Time Zone: America/Toronto

The following screen shows the addition of the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as *SIP Trunk*. Select created **Adaptation** from pull down menu list. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of **120** seconds. This setting allows Session Manager to send outbound OPTIONS heartbeat every **120** seconds to the service provider (which is forwarded by the Avaya SBCE) to query the status of the SIP trunk connecting to the service provider.

AVAYA
Aura® System Manager 7.1

Last Logged on at August 17, 2017 12:32 PM
Go... Log off admin

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

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: SBCE22

* FQDN or IP Address: 10.10.98.22

Type: SIP Trunk

Notes: SBC-E 10.33.10.29 using IP 98.22

Adaptation: Remove-Unused-Headers

Location: Belleville

Time Zone: America/Toronto

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 120

* Reactive Monitoring Interval (in seconds): 30

* Number of Tries: 5

* Number of Successes: 1

CRLF Keep Alive Monitoring: CRLF Monitoring Disabled

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Similarly, a SIP Entity is added for Avaya Aura® Messaging server as shown in the capture below.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home', 'Routing', and a search bar. The left sidebar lists various configuration options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and contains the following fields:

- Name:** AAM
- FQDN or IP Address:** 10.33.10.35
- Type:** Messaging
- Notes:** (empty text area)
- Adaptation:** (empty dropdown)
- Location:** Belleville
- Time Zone:** America/Toronto
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text area)
- Securable:** ☐
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony entity is described by an Entity Link. During compliance testing, three Entity Links were created, one for Communication Manager, Avaya Aura® Messaging and other for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click **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 entity defined in **Section 6.5**.
- **Protocol:** Select the transport protocol used for this link, **TLS** for the Entity Link to Communication Manager and Avaya Aura® Messaging and **TLS** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section Error! Reference source not found.5**. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section Error! Reference source not found.5**.

- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. **Note:** If this is not selected, calls from the associated SIP Entity specified in **Section Error! Reference source not found.** will be denied.
- Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and to the Avaya SBCE.

Entity Link to Communication Manager

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
* SM7_CM7_5061_TLS	* SM7	TLS	* 5061	* CM7	* 5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>

Entity Link to Avaya SBCE

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
* SM7_SBCE22_5061_TLS	* SM7	TLS	* 5061	* SBCE22	* 5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>

Entity Link to Avaya Aura® Messaging

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
* SM-SP-SP-AAM_5061_TI	* SM7	TLS	* 5061	* AAM	* 5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section Error! Reference source not found.** Three routing policies were added,

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

In the **General** section, configure the following fields:

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

In **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the Routing Policy for Communication Manager.

AVAYA Aura® System Manager 7.1

Last Logged on at August 17, 2017 12:32 PM

GO... Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel

General

* Name: To-CM7

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM7	10.33.10.34	CM	

The following screen shows the Routing Policy for the Avaya SBCE.

AVAYA Aura® System Manager 7.1

Last Logged on at August 17, 2017 12:32 PM

GO... Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel

General

* Name: To-SBCE22

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SBCE22	10.10.98.22	SIP Trunk	SBC-E 10.33.10.29 using IP 98.22

The following screen shows the Routing Policy for the Avaya Aura® Messaging.

The screenshot shows the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 7.1', and a user status bar indicating 'Last Logged on at August 17, 2017 12:32 PM' with a 'Log off admin' button. A breadcrumb trail shows 'Home / Elements / Routing / Routing Policies'. The left sidebar contains a tree view with 'Routing' expanded, showing sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: 'Name' (To-AAM), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (Routing from SM to AAM). Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
AAM	10.33.10.35	Messaging	

6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Avaya Aura® Messaging and from Communication Manager to Bell Canada and vice versa. Dial Patterns define which routing 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 **New** button in the right pane (not shown).

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.
- **Notes:** Add a brief description (optional).

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

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

Two examples of the dial patterns used for the compliance testing are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows that 10-digit dialed numbers that have a destination domain of “avayalab.com” uses route policy to Avaya SBCE as defined in **Section Error! Reference source not found.7**.

Avaya
Aura® System Manager 7.1

Last Logged on at August 17, 2017 12:32 PM
GO... Log off admin

Home Routing x

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 613

* Min: 3

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab.com

Notes: Outgoing to PSTN 613

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	GSSCP Belleville	To-SBCE22	0	<input type="checkbox"/>	SBCE22	

The second example shows that inbound 10-digit numbers assigned by Bell Canada with domain “avayalab.com” to use route policy to Communication Manager as defined in **Section Error! Reference source not found.7**.

AVAYA
Aura® System Manager 7.1

Last Logged on at August 17, 2017 12:32 PM
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: 613XXX

* Min: 6

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	GSSCP Belleville	To-CM7	0	<input type="checkbox"/>	CM7	

6.9. TLS Certificate Management on System Manager

This section is to provide a procedure how to download System Manager CA certificate which is being installed on Avaya Communication Manager and Avaya SBCE for the communication between Avaya system components using TLS connectivity.

From System Manager Menu in **Section 6.1**, navigate to **Services → Security**. Click on arrow tab to show navigation tree as shown.

AVAYA
Aura® System Manager 7.1

Last Logged on at August 17, 2017 12:32 PM
Go... Log off admin

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

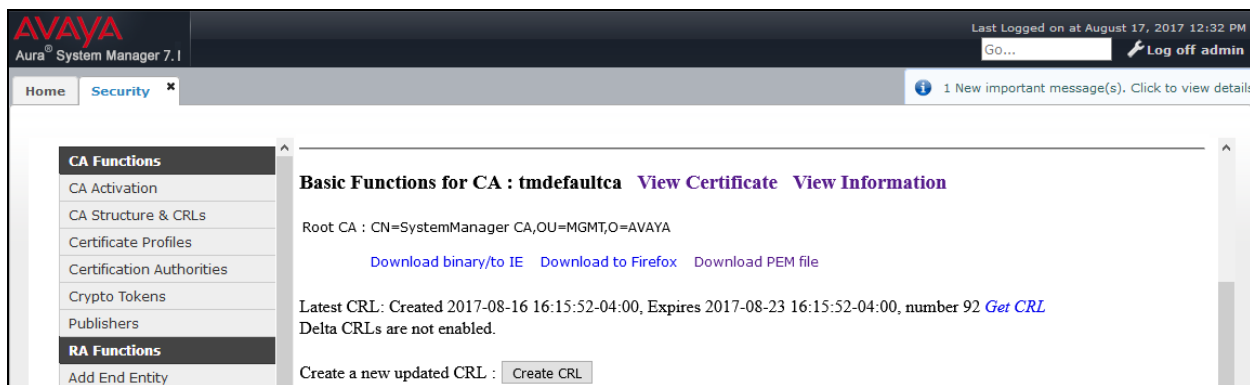
Home / Services / Security

Security

Sub Pages

Action	Description	Help
Certificates	Administer the Certificate Authority (CA) and set the Enrollment Password to provision certificates.	Certificate Authority and Enrollment Password
Configuration	Manage security and CRL configuration.	TM Security Configuration

Navigate to **Certificates → Authority → CA Functions → CA Structure & CRLs**. Then click on **Download PEM file** to download the System Manager CA and save it as **SystemManagerCA.pem** to a directory on local management PC.



7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya SBCE is used as the edge device between the Avaya CPE and Bell Canada SIP Trunking Service.

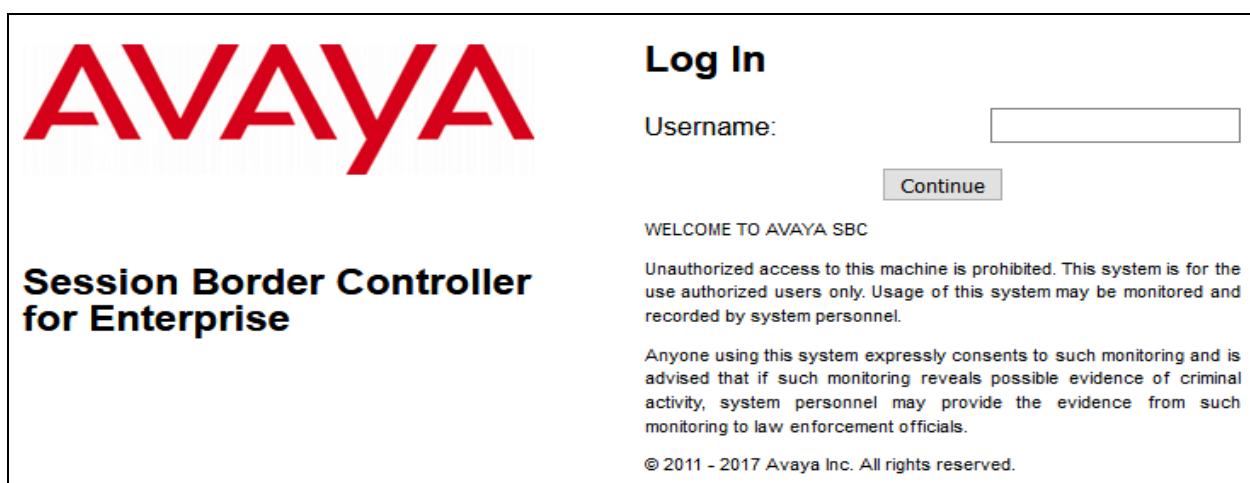
These Application Notes assume that the installation of the Avaya SBCE and the assignment of a management IP Address have already been completed.

In this session, the naming convention used for Bell Canada is Service Provider (**SP**), which is connected to the external interface of the Avaya SBCE. And for the Avaya side is Enterprise (**EN**), which is connected to the internal interface of the Avaya SBCE.

7.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Avaya SBCE web interface, enter “https://<ip-addr>/sbc” in the address field of the web browser (not shown), where “<ip-addr>” is the management LAN IP address of Avaya SBCE.

Enter appropriate credentials and click *Continue*. Then enter password to login.



The main page of the Avaya SBCE will appear as shown below.

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.

Information

System Time	05:32:22 AM EDT	Refresh
Version	7.2.0.0-18-13712	
Build Date	Thu Jun 1 00:12:50 UTC 2017	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	08/17/2017 02:22:50 EDT	
Failed Login Attempts	0	

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS
SBCE72

Incidents (past 24 hours)

SBCE72 : Max forwards Exceeded

7.2. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. The Avaya SBCE utilizes TLS primarily to facilitate secure communications with remote users.

Avaya SBCE supports the configuration of third-party certificates and TLS settings. For optimum security, Avaya recommends using third-party CA certificates for enhanced security

Testing was done with System Manager signed identity certificates. The procedure to obtain and install 3rd party CA certificates is outside the scope of these application notes.

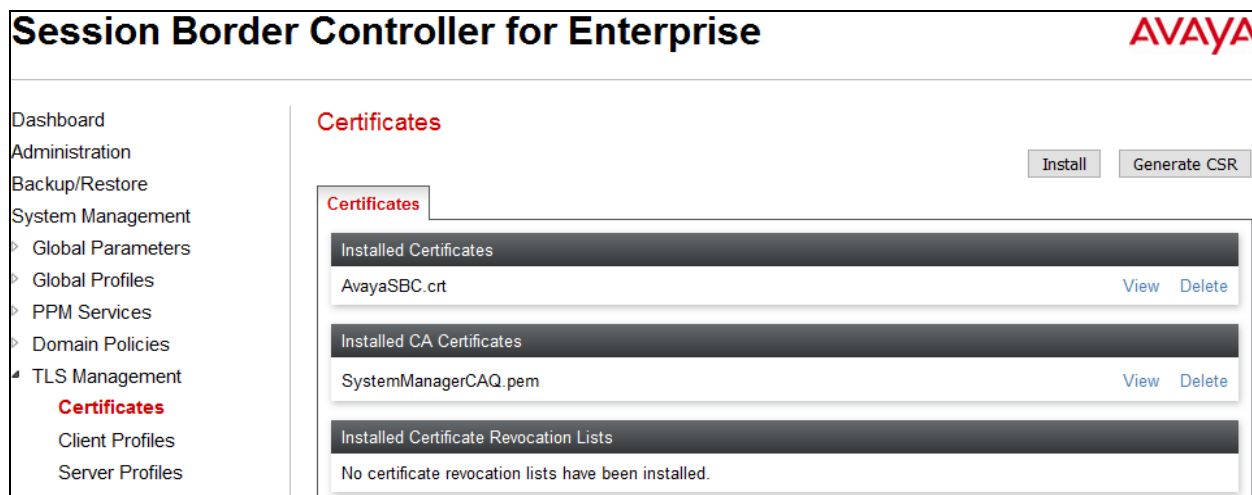
In this compliance testing, TLS transport is used for the communication between Session Manager and Avaya SBCE. The following procedures show how to create the client and server profiles.

7.2.1. Certificates

You can use the certificate management functionality that is built into the Avaya SBCE to control all certificates used in TLS handshakes. You can access the Certificates screen from **TLS Management → Certificates**.

Ensure the preinstalled certificates are presented in the system as shown below.

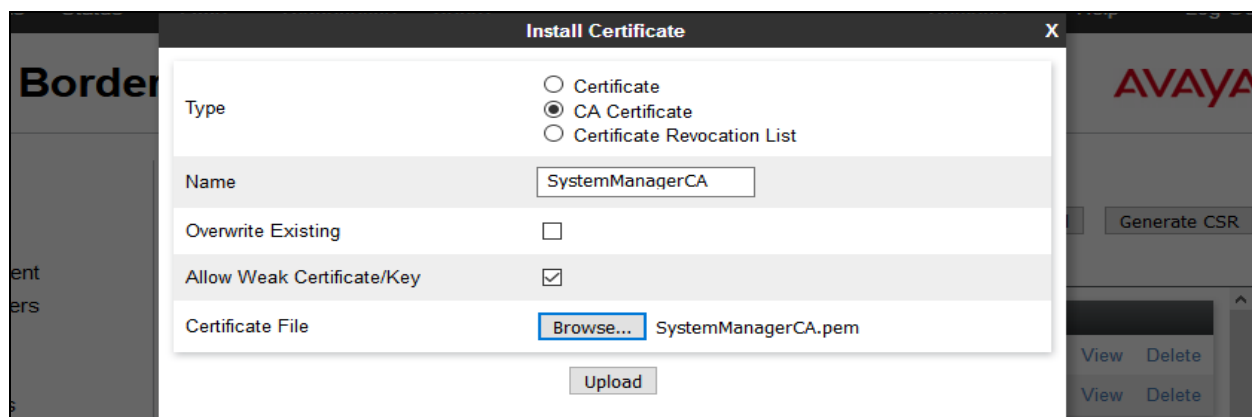
- *AvayaSBC.crt* is Avaya SBCE identify certificate.
- *SystemManagerCAQ.pem* is System Manager Certificate Authority root certificate.



If System Manager Certificate Authority certificate (SystemManagerCAQ.pem) is not present, the following procedure shows how to install it on the Avaya SBCE.

System Manager CA certificate is obtained using procedure provided in **Section 6.9**. Then on the Avaya SBCE, navigate to **TLS Management → Certificates**. Click on **Install** button.

- Select **CA Certificate**.
- Provide a descriptive **Name**.
- **Browse** to the directory where the System Manager CA previously saved and select it.
- Click **Upload**.



7.2.2. Client Profiles

This section describes the procedure to create client profile for Avaya SBCE to communicate with Session Manager via TLS signaling. This profile will be used in **Section 7.3.4**.

To create Client profile, navigate to **TLS Management → Client Profiles**, click on **Add**.

- Enter descriptive name in **Profile Name**.
- Select *AvayaSBC.crt* from pull down menu of **Certificate**.
- Select *SystemManagerCAQ.pem* from pull down of **Peer Certificate Authorities**.
- Enter **5** as **Verification Depth**.
- Click **Next** and **Finish** (not shown).

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management (selected), Certificates, Client Profiles (highlighted), Server Profiles, and Device Specific Settings. The main content area is titled 'Client Profiles: AvayaSBCCClient-Q' and includes an 'Add' button. Below this is a list of client profiles: COLTClient, AvayaSBCCClient, AvayaSBCCClient-H, and AvayaSBCCClient-Q (selected). The 'Edit Profile' form for 'AvayaSBCCClient-Q' is shown, featuring a warning message about OpenSSL cipher checking. The form fields are: Profile Name (AvayaSBCCClient-Q), Certificate (AvayaSBC.crt), Peer Certificate Authorities (SystemManagerCAQ.pem selected), Peer Certificate Revocation Lists (empty), Verification Depth (5), Extended Hostname Verification (unchecked), and Custom Hostname Override (empty). A 'Next' button is at the bottom right.

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ Domain Policies
‣ **TLS Management**
‣ Certificates
‣ **Client Profiles**
‣ Server Profiles
‣ Device Specific Settings

Client Profiles: AvayaSBCCClient-Q

Add

Client Profiles
COLTClient
AvayaSBCCClient
AvayaSBCCClient-H
AvayaSBCCClient-Q

Click here to add a description.

Client Profile

Edit Profile X

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

TLS Profile

Profile Name

Certificate

Certificate Verification

Peer Verification Required

Peer Certificate Authorities
AvayaSBCCA.crt
coltroot.crt
Cisco_phone_CA.crt
SystemManagerCAQ.pem

Peer Certificate Revocation Lists

Verification Depth

Extended Hostname Verification ☐

Custom Hostname Override

Next

7.2.3. Server Profiles

This section describes the procedure to create server profile for Avaya SBCE to communicate with Session Manager via TLS signaling. This will be used in **Section 7.5.3**.

To create Server profile, navigate to **TLS Management → Server Profiles**, click on **Add**.

- Enter descriptive name in **Profile Name**.
- Select **AvayaSBC.crt** from pull down menu of **Certificate**.
- Select **None** from pull down menu of **Peer Verification**.
- Others are left at default.
- Click **Next** and **Finish** (not shown).

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, and TLS Management. The 'Server Profiles' section under TLS Management is highlighted. The main content area is titled 'Server Profiles: AvayaSBCServer-Q' and includes an 'Add' button. Below this is a list of server profiles: COLTServer, AvayaSBCServer, AvayaSBCServer-H, and AvayaSBCServer-Q (which is selected). To the right of the list is a 'Server Profile' tab and an 'Edit Profile' button. A red warning banner states: 'The selected certificate is known to have been compromised and should not be used in a production environment.' Below this is an orange warning box: 'WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.' The configuration form includes fields for 'Profile Name' (AvayaSBCServer-Q), 'Certificate' (AvayaSBC.crt), 'Peer Verification' (None), 'Peer Certificate Authorities' (a list containing SystemManagerCA-H.pem, AvayaSBCCA.crt, coltroot.crt, and Cisco_phone_CA.crt), 'Peer Certificate Revocation Lists' (empty), and 'Verification Depth' (0). A 'Next' button is at the bottom right.

7.3. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.3.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*” is used for all incoming and outgoing traffic.

7.3.2. Server Interworking Profile

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles → Server Interworking**. Click on the **Add** button.

In the compliance testing, two Server Interworking profiles were created for SP and EN respectively.

Server Interworking profile for SP


Profile **SP-SI** was defined to match the specification of SP. The **General** and **Advanced** tabs are configured with the following parameters while the other tabs for **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** are kept as default.

General tab:

- **Hold Support** = *NONE*. The Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = *Yes*. SP does support T.38 fax in the compliance testing.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI, General**.

Session Border Controller for Enterprise



- Dashboard
- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - Domain DoS
 - Server Interworking**
 - Media Forking
 - Routing
 - Server Configuration
 - Topology Hiding
 - Signaling Manipulation
 - URI Groups
 - SNMP Traps
 - Time of Day Rules
 - FGDN Groups
 - Reverse Proxy Policy
 - RADIUS
 - PPM Services
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Interworking Profiles: SP-SI

Add
Rename
Clone
Delete

Interworking Profiles

- EN-SI
- SP-SI**

Click here to add a description.

General
Timers
Privacy
URI Manipulation
Header Manipulation
Advanced

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

Edit

Advanced tab:

- **Record Routes:** *Both Sides*.
- **Include End Point IP for Context Lookup:** *No*.
- **Extensions:** *None*.
- **Has Remote SBC:** *Yes*. SP has an SBC which interfaces its Central Office (CO) to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from SP for the media.
- **DTMF Support:** *None*. The Avaya SBCE will send original DTMF method from EN to SP.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI**, **Advanced**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Server Interworking' highlighted in red. The main content area is titled 'Interworking Profiles: SP-SI' and includes an 'Add' button and action buttons (Rename, Clone, Delete). A list of profiles is shown, with 'SP-SI' selected and highlighted in red. The 'Advanced' tab is active, displaying a table of configuration settings for the selected profile. The settings include Record Routes (Both Sides), Include End Point IP for Context Lookup (No), Extensions (None), Diversion Manipulation (No), Has Remote SBC (Yes), Route Response on Via Port (No), Relay INVITE Replace for SIPREC (No), MOBX Re-INVITE Handling (No), and DTMF Support (None). An 'Edit' button is located at the bottom right of the settings table.

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

Header Manipulation tab:

This is optional and added here for reference when setting up Dynamic ONND (Outbound Calling Name and Number Display) feature. It won't be shown in details.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

Interworking Profiles: SP-SI

Add

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-S...

cisco-ccm

cups

OCS-FrontEn...

CM63

EN-SI

SP-SI

RenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Add

Header	Action		
Diversion	Add parameter otg with value [redacted]01A;user=phone	Edit	Delete
P-Asserted-Identity	Remover parameter user with value phone	Edit	Delete
From	Remover parameter user with value phone	Edit	Delete
From	Add parameter otg with value [redacted]01A	Edit	Delete
P-Asserted-Identity	Add parameter otg with value [redacted]01A	Edit	Delete

Server Interworking profile for EN

Profile **EN-SI** was defined to match the specification of EN. The **General** and **Advanced** tabs are configured with the following parameters while the other settings for **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** are kept as default.

General tab:

- **Hold Support:** *None*.
- **18X Handling:** *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling:** *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support:** *Yes*.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **EN-SI**, **General**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) configuration interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: EN-SI' and includes an 'Add' button. Below this, there are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is selected, showing a table of configuration parameters. The table has two columns: the parameter name and its value. The parameters and their values are: 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), Prack Handling (No), Allow 18X SDP (No), T.38 Support (Yes), URI Scheme (SIP), and Via Header Format (RFC3261). There are 'Rename', 'Clone', and 'Delete' buttons at the top right, and an 'Edit' button at the bottom right of the table.

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
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Advanced tab:

- **Record Routes: *Both Sides***. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup = *Yes***.
- **Extensions: *Avaya***.
- **Has Remote SBC: *Yes***. This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support: *None***. The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **EN-SI**, **Advanced**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) configuration interface. The left sidebar shows the navigation menu with 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: EN-SI' and includes a list of profiles on the left and a configuration table on the right. The 'Advanced' tab is active, showing settings for Record Routes, Include End Point IP for Context Lookup, Extensions, Diversion Manipulation, Has Remote SBC, Route Response on Via Port, Relay INVITE Replace for SIPREC, and MOBX Re-INVITE Handling. The DTMF Support is set to None.

Profile	Record Routes	Include End Point IP for Context Lookup	Extensions	Diversion Manipulation	Has Remote SBC	Route Response on Via Port	Relay INVITE Replace for SIPREC	MOBX Re-INVITE Handling	DTMF Support
cs2100	Both Sides	Yes	Avaya	No	Yes	No	No	No	None
avaya-ru									
OCS-Edge-S...									
cisco-ccm									
cups									
OCS-FrontEn...									
CM63									
EN-SI									
SP-SI									
SM									
BellCanada									
CS1K76									

7.3.3. Signaling Manipulation

Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature adds the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called **SigMa**.

To create a Signaling Manipulation script, select **Global Profiles → Signaling Manipulation**. Click **Add Script** (not shown).

In the compliance testing, a SigMa SP-BELL script is created for Server Configuration for SP and its details are captured below.

The screenshot displays the 'Session Border Controller for Enterprise' (AVAYA) web interface. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and PPM Services. Under 'Global Profiles', 'Signaling Manipulation' is highlighted. The main content area is titled 'Signaling Manipulation Scripts: SP-BELL'. It features buttons for 'Upload', 'Add', 'Download', 'Clone', and 'Delete'. A blue bar prompts the user to 'Click here to add a description.' Below this, a tab labeled 'Signaling Manipulation' is active, showing a code editor with a SigMa script. The script is designed to manipulate SIP headers for outbound requests, specifically replacing the 'From', 'Contact', 'P-Asserted-Identity', and 'Diversions' headers with values derived from the 'user=phone' parameter. Comments within the script provide instructions for dynamic and static ONND configurations. An 'Edit' button is located at the bottom right of the script editor.

```
//testing
within session "ALL"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["From"][1].URI.USER.regex_replace("\+", "");
    %HEADERS["Contact"][1].URI.USER.regex_replace("\+", "");
    %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("\+", "");
    %HEADERS["Diversions"][1].URI.USER.regex_replace("\+", "");
    //For Dynamic ONND, remember to change xxxxxxxx.lab.xxxxxxxxvoice.ca
    //to lab.xxxxxxxxvoice.ca using Topology Hiding setting
    %HEADERS["From"][1].URI.regex_replace("user=phone", "");
    %HEADERS["To"][1].URI.regex_replace("user=phone", "");
    //For Static ONND, remember to change back
    //to xxxxxxxx.lab.xxxxxxxxvoice.ca using Topology Hiding
    remove(%HEADERS["P-Asserted-Identity"][1]);
    append(%HEADERS["Diversions"][1].URI, "user=phone");
    append(%HEADERS["From"][1].URI, "user=phone");
    append(%HEADERS["P-Asserted-Identity"][1].URI, "user=phone");
    // To change Diversions header from <sips:xxxxxxx...> to <sip:xxxxxxx...>
    %HEADERS["Diversions"][1].regex_replace("sips", "sip");
  }
}
```

7.3.4. Server Configuration

The Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains. No configuration of **Heartbeat** is required.

To create a Server Configuration entry, select **Global Profiles → Server Configuration**. Click on the **Add** button.

In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for SP and server entry **EN-SC** for EN.

Server Configuration for SP

Server Configuration named **SP-SC** was created for SP. All tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN.

General tab:

Click on the **Add** button and enter the following information.

- Enter **Profile Name** *SP-SC* and click **Next**.
- Set **Server Type** for SP as *Trunk Server*.
- Enter **IP Address/FQDN** provided by SP.
- In the compliance testing, SP supported **UDP** and listened on port **5060**.
- Click **Next**, then **Next** and **Finish**.

The completed server profile is shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar lists various configuration categories, with 'Server Configuration' highlighted. The main area displays the 'Server Configuration: SP-SC' page. The 'General' tab is active, showing the 'Server Type' as 'Trunk Server'. Below this, a table lists the IP Address / FQDN as '192.168.237.208', the Port as '5060', and the Transport as 'UDP'. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

IP Address / FQDN	Port	Transport
192.168.237.208	5060	UDP

Authentication tab:

Click on the **Edit** button and enter following information.

- Check **Enable Authentication** check box.
- Enter **User Name** (provided by SP).
- Enter **Realm** (provided by SP).
- Enter **Password** and **Confirm Password** (provided by SP) (not shown).
- Click **Finish**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, specifically the 'Authentication' tab for the 'SP-SC' server profile. The 'Enable Authentication' checkbox is checked. The 'User Name' field contains '01A' and the 'Realm' field contains 'ca'. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.


User Name	Realm
01A	ca

Advanced tab:

Click on the **Edit** button and enter following information.

- **Interworking Profile** drop down list, select **SP-SI** as defined in **Section 7.3.2**.
- **Signaling Manipulation Script** drop down list, select **SP-BELL** as defined in **Section 7.3.3**.
- The other settings are kept as default.

Session Border Controller for Enterprise



Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

Server Configuration: SP-SC

Add

Server Profiles

CM63

SM63

CS1K76

SP4_OLD

IPO-SE

EC-SC-RW

SP-SC-1

SMVM

SP4

EN-SC

SP-SC

RenameCloneDelete

GeneralAuthenticationHeartbeatPingAdvanced

Enable DoS Protection☐

Enable Grooming☐

Interworking ProfileSP-SI

Signaling Manipulation ScriptSP-BELL

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

Edit

Server Configuration for EN

Server Configuration named **EN-SC** created for EN is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as *disabled* as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

General tab:

Click on the **Add** button and enter the following information.

- Enter **Profile Name** as *EN-SC* and click **Next**.
- **Server Type** for EN as *Call Server*.
- Select *AvayaSBCEClient-Q* for **TLS Client Profile**.
- **IP Address/FQDN** is Session Manager IP address.
- **Transport**, the link between the Avaya SBCE and EN was *TLS*.
- Listened on **Port 5061**.
- Click **Next**, **Next** and then **Finish**.

The completed server profile is shown below.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The title bar at the top reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand navigation menu includes links for Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (with sub-links for Domain DoS, Server Interworking, Media Forking, Routing, and **Server Configuration**), and Topology Hiding. The main content area is titled "Server Configuration: EN-SC" and features an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a tabbed interface with "General", "Authentication", "Heartbeat", "Ping", and "Advanced" tabs. The "General" tab is active, showing the following configuration details:

Server Type	Call Server	
SIP Domain	avayalab.com	
TLS Client Profile	AvayaSBCEClient-Q	
IP Address / FQDN	Port	Transport
10.33.10.33	5061	TLS

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

Advanced tab:

Click on the **Edit** button to enter the following information.

- **Interworking Profile** drop down list select **EN-SI** as defined in **Section Error!** Reference source not found..
- The other settings are kept as default.

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
  Domain DoS
  Server Interworking
  Media Forking
  Routing
  Server Configuration
  Topology Hiding
  Signaling Manipulation
  URI Groups
  SNMP Traps
  Time of Day Rules
  FGDN Groups
  Reverse Proxy Policy

Server Configuration: EN-SC

Add Rename Clone Delete

Server Profiles

- CM63
- SM63
- CS1K76
- SP4_OLD
- IPO-SE
- EC-SC-RW
- SP-SC-1
- SMVM
- SP4
- EN-SC**
- SP-SC

General Authentication Heartbeat Ping **Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile EN-SI

Signaling Manipulation Script None

Securable ☐

Enable FGDN ☐

Tolerant ☐

URI Group None

Edit

7.3.5. Routing Profiles

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

To create a Routing Profile, select **Global Profiles → Routing**. Click on the **Add** button.

In the compliance testing, a Routing Profile **EN-RP** was created to use in conjunction with the server flow defined for EN. This entry is to route the outbound call from the enterprise to the service provider.

In the opposite direction, a Routing Profile named **SP-RP** was created to be used in conjunction with the server flow defined for SP. This entry is to route the inbound call from the service provider to the enterprise.

Routing Profile for SP

The screenshot below illustrates the routing profile from Avaya SBCE to the SP network, **Global Profiles → Routing: SP-RP**. As shown in **Figure 1**, the SP SIP trunk is connected with transport protocol **UDP**. If there is a match in the “To” or “Request URI” headers with the URI Group “*” as described in **Section 7.3.1**, the call will be routed to the **Next Hop Address** which is the IP address of SP SIP trunk.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Server Interworking, Media Forking, **Routing** (highlighted), and Server Configuration. The main content area is titled "Routing Profiles: SP-RP" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." The "Routing Profile" section contains an "Update Priority" button and an "Add" button. A table lists the routing profile configuration:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	192.168.237.208	UDP	Edit Delete

Routing Profile for EN

The Routing Profile for SP to EN, **EN-RP**, was defined to route call where the “To” header matches the URI Group **SP** defined in **Section 7.3.1** to **Next Hop Address** which is the IP address of Session Manager as a destination. As shown in **Figure 1**, the SIP trunk between EN and the Avaya SBCE is connected with transport protocol **TLS**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Server Interworking, Media Forking, **Routing** (highlighted), and Server Configuration. The main content area is titled "Routing Profiles: EN-RP" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a blue bar with the text "Click here to add a description." The "Routing Profile" section contains an "Update Priority" button and an "Add" button. A table lists the routing profile configuration:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.33.10.33	TLS	Edit Delete

7.3.6. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding**. Click on the **Add** button.

In the compliance testing, two Topology Hiding profiles **EN-TH** and **SP-TH** were created.

Topology Hiding Profile for SP

Profile **SP-TH** was defined to mask the enterprise SIP domain *avayalab.com* in the “Request-Line”, “From” and “To” headers to SP provided full qualified domain name. This is done to secure the enterprise network topology and to meet the SIP requirement of the service provider.

Notes:

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header.
- The masking applied on “To” header.

The screenshots below illustrate the Topology Hiding profile **SP-TH**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted in red), Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, and Reverse Proxy Policy. The main content area is titled 'Topology Hiding Profiles: SP-TH' and includes an 'Add' button, a 'Rename' button, a 'Clone' button, and a 'Delete' button. Below these buttons is a blue bar with the text 'Click here to add a description.' The 'Topology Hiding' tab is active, showing a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	[Redacted] ca
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Overwrite	[Redacted] ca
Request-Line	IP/Domain	Overwrite	[Redacted] ca

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

Topology Hiding Profile for EN

Profile **EN-TH** was also created to mask SP URI-Host in “Request-Line”, “From” and “To”, headers to the enterprise domain **avayalab.com**, replace Record-Route, Via headers and SDP added by SP to internal IP address known to EN.

Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header.
- The masking applied on “To” header.

The screenshots below illustrate the Topology Hiding profile **EN-TH**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration, **Topology Hiding**, Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, and Reverse Proxy Policy. The main content area is titled "Topology Hiding Profiles: EN-TH" and includes an "Add" button, a "Rename" button, a "Clone" button, and a "Delete" button. Below these buttons is a table with the following data:

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

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

7.4. Domain Policies

Domain Policies configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

7.4.1. Media Rules

Media rules can be used 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. You can also define how Avaya SBCE must handle media packets that adhere to the set parameters.

To clone a Media Rule, navigate to **Domain Policies → Media Rules**. With *default-low-med* rule chosen, click on the **Clone** button.

Media Rules for EN

In this compliance testing, Secure Real-Time Transport Protocol (SRTP, media encryption) is used within enterprise network only. Therefore, it is necessary to create a media rule to apply to the internal interface of Avaya SBCE and EN. Created **SRTP-MR** rule is shown below.

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

Media Rules: SRTP-MR

AddFilter By Device...RenameCloneDelete

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Encryption

Preferred FormatsSRTP_AES_CM_128_HMAC_SHA1_80
SRTP_AES_CM_128_HMAC_SHA1_32
RTP

Encrypted RTCP☒

MKI☐

LifetimeAny

Interworking☒

Video Encryption

Preferred FormatsRTP

Interworking☒

Miscellaneous

Capability Negotiation☐

Edit

Media Rules for SP

In this compliance testing, media rule using for service provider is *default-low-med* as default (not show).

7.4.2. Signaling Rules

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

To clone a Signaling Rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click on the **Clone** button.

Signaling Rules for SP

In the compliance testing, created signaling rule **SP-SR** is discussed below. All the tabs are kept as default values except the **Signaling QoS** tab.

In the **Signaling QoS** tab, click on **Edit** button then check on checkbox. Then select **EF** value for **DSCP** option.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top header shows "Session Border Controller for Enterprise" and the "AVAYA" logo. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (highlighted), End Point Policy, and Groups. The main content area is titled "Signaling Rules: SP-SR". It includes an "Add" button, a "Filter By Device..." dropdown, and "Rename", "Clone", and "Delete" buttons. Below these is a list of signaling rules: "default", "No-Content-Ty...", "EN-SR", and "SP-SR" (highlighted). The "SP-SR" rule is selected, and its configuration is shown in a tabbed interface. The tabs are "General", "Requests", "Responses", "Request Headers", "Response Headers", and "Signaling QoS" (selected). The "Signaling QoS" tab contains a checkbox for "Signaling QoS" which is checked. Below this, there are two rows of configuration: "QoS Type" set to "DSCP" and "DSCP" set to "EF". An "Edit" button is located at the bottom right of the configuration area.

Signaling Rules for EN

In the compliance testing, created signaling rule **EN-SR** is discussed below. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button then check on checkbox. Then select **EF** value for **DSCP** option.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with 'Domain Policies' expanded, showing 'Signaling Rules' as the selected option. The main content area is titled 'Signaling Rules: EN-SR'. It features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below these is a 'Click here to add a description.' link. The 'General' tab is active, showing a table with columns 'UCID' and 'QoS Type'. The 'QoS Type' is set to 'DSCP'. The 'DSCP' value is set to 'EF'. There is an 'Edit' button at the bottom right of the table.

7.4.3. Endpoint Policy Groups

The rules created within the **Domain Policies** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section. Endpoint Policy Groups were created for SP and EN. To create a new policy group, navigate to **Domain Policies** → **Endpoint Policy Groups** and click on **Add**.

Endpoint Policy Group for SP

The following screen shows **SP-PG** created for SP:

- Set Application Rule to *default-trunk*.
- Set Border Rule to *default*.
- Set Media Rule to *default-low-med* as created in **Section 7.4.1**.
- Set Security Rule to *default-med*
- Set Signaling Rule to *SP-SR* as created in **Section 7.4.2**.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with 'Domain Policies' expanded, showing 'End Point Policy Groups' as the selected option. The main content area is titled 'Policy Groups: SP-PG'. It features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below these is a 'Click here to add a description.' link. The 'Policy Group' tab is active, showing a table with columns 'Order', 'Application', 'Border', 'Media', 'Security', and 'Signaling'. The 'Order' is 1, 'Application' is 'default-trunk', 'Border' is 'default', 'Media' is 'default-low-med', 'Security' is 'default-med', and 'Signaling' is 'SP-SR'. There is an 'Edit' button at the bottom right of the table.

Endpoint Policy Group for EN

The following screen shows **EN-PG** created for EN:

- Set Application Rule to *default-trunk*.
- Set Border Rule to *default*.
- Set Media Rule to *SRTP-MR* as created in **Section 7.4.1**.
- Set Security Rule to *default-med*.
- Set Signaling Rule to *EN-SR* as created in **Section 7.4.2**.

Session Border Controller for Enterprise

AVAYA

Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

End Point Policy Groups

Session Policies

TLS Management

Device Specific Settings

Policy Groups: EN-PG

Add

Filter By Device...

Rename

Clone

Delete

Policy Groups

EN-PG

SP-PG

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	SRTP-MR	default-med	EN-SR	Edit

7.5. Device Specific Settings

Device Specific Settings allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

7.5.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was defined such as; device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. This information populates the **Network Management** tab, which can be edited as needed to optimize device performance and network efficiency.

Enable the interfaces used to connect to the inside and outside networks on the **Interface** tab. The following screen shows **Interface Names**, **A1** and **B1** are **Enabled**. To enable an interface, click on its **Status** corresponding to the interface names.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The title bar at the top 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 "Network Management" as the selected option. The main content area is titled "Network Management: SBCE72" and contains two tabs: "Interfaces" (active) and "Networks". Under the "Interfaces" tab, there is a table with three columns: "Interface Name", "VLAN Tag", and "Status". The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled). An "Add VLAN" button is located in the top right corner of the table area.

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

Navigate to **Device Specific Settings** → **Network** and under the **Network Configuration** tab verify the IP addresses assigned to the interfaces. The following screens show the private interface is assigned to **A1** and the public interface is assigned to **B1** respectively.

Session Border Controller for Enterprise AVAYA

Edit Network X

This Network contains one or more IP Address entries which are in use. If the Interface, an IP Address, or Public IP which is in use is modified, the application **must** be restarted or the device may stop functioning.

Name: Network_A1

Default Gateway: 10.10.98.1

Network Prefix or Subnet Mask: 255.255.255.192

Interface: A1

Add

IP Address	Public IP	Gateway Override	
10.10.98.22	Use IP Address	Use Default	Delete

Finish

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings
‣ **Network Management**
Media Interface
Signaling Interface
End Point Flows
Session Flows

Edit Delete

Edit Delete

Session Border Controller for Enterprise AVAYA

Edit Network X

This Network contains one or more IP Address entries which are in use. If the Interface, an IP Address, or Public IP which is in use is modified, the application **must** be restarted or the device may stop functioning.

Name: Network_B1

Default Gateway: 10.10.98.97

Network Prefix or Subnet Mask: 255.255.255.224

Interface: B1

Add

IP Address	Public IP	Gateway Override	
10.10.98.119	Use IP Address	Use Default	Delete

Finish

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings
‣ **Network Management**
Media Interface
Signaling Interface
End Point Flows
Session Flows

Edit Delete

Edit Delete

7.5.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open a connection for RTP on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**.

Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The 'Media Interface' option under 'Device Specific Settings' is highlighted. The main content area is titled 'Media Interface: SBCE72'. It features a warning message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table listing the configured media interfaces.

Name	Media IP Network	Port Range	TLS Profile	Edit	Delete
InsideMedia	10.10.98.22 Network_A1 (A1, VLAN 0)	35000 - 40000	None	Edit	Delete
OutsideMedia	10.10.98.119 Network_B1 (B1, VLAN 0)	35000 - 40000	None	Edit	Delete

7.5.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

To create a new Signaling Interface, navigate to **Device Specific → Settings → Signaling Interface** and click **Add**.

Separate Signaling Interfaces were created for both inside and outside interfaces.

Signaling Interface for SP

The outside interface to service provider is created with UDP/5060 as shown below.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The 'Signaling Interface' option under 'Device Specific Settings' is highlighted. A modal window titled 'Edit Signaling Interface' is open. It contains the following fields: 'Name' (text box with 'OutsideSignalingUDP'), 'IP Address' (dropdown menu with 'Network_B1 (B1, VLAN 0)' selected), 'TCP Port' (text box with 'Leave blank to disable' below it), 'UDP Port' (text box with '5060'), 'TLS Port' (text box with 'Leave blank to disable' below it), 'TLS Profile' (dropdown menu with 'None' selected), 'Enable Shared Control' (checkbox, unchecked), and 'Shared Control Port' (text box). A 'Finish' button is at the bottom right of the modal.

Signaling Interface for EN

The inside to service provider interface is created with TLS/5061 as shown below.

- Enter descriptive name for **Name** field.
- Select **IP Address** from pull down menu defined as internal network interface **Section 7.5.1**.
- Specified **5061** for **TLS Port**. Then select **TLS profile** from pull down menu as defined in **Section 7.2.3**.
- Click **Finish**.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The 'Signaling Interface' option under 'Device Specific Settings' is highlighted. A modal window titled 'Edit Signaling Interface' is open. It contains the following fields: 'Name' (text box with 'InsideSignalingTLS'), 'IP Address' (dropdown menu with 'Network_A1 (A1, VLAN 0)' selected), 'TCP Port' (text box with 'Leave blank to disable' below it), 'UDP Port' (text box with 'Leave blank to disable' below it), 'TLS Port' (text box with '5061'), 'TLS Profile' (dropdown menu with 'AvayaSBCServer-Q' selected), 'Enable Shared Control' (checkbox, unchecked), and 'Shared Control Port' (text box). A 'Finish' button is at the bottom right of the modal.

7.5.4. End Point Flows - Server Flow

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

In the compliance testing, separate Server Flows were created for SP and EN. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.3.4** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 7.3.1** to assign to the Flow.
Note: URI Group can be set to “*” to match all calls.
- **Received Interface:** Select the Signaling Interface created in **Section 7.5.3** that the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.5.3** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.5.2** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.4.3** to assign to the Server Configuration.
- **Routing Profile:** Select the Routing Profile created in **Section 7.3.2** that the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 7.3.6** to apply to the Server Configuration.
- Click **Finish**.

The following screen shows the Server Flow **SP-SF** configured for SP.

The screenshot displays the 'Edit Flow: SP-SF' configuration window within the Avaya Session Border Controller for Enterprise interface. The window is titled 'Edit Flow: SP-SF' and features a close button (X) in the top right corner. The configuration is organized into a table-like structure with the following fields and values:

Field	Value
Flow Name	SP-SF
Server Configuration	SP-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideSignalingTLS
Signaling Interface	OutsideSignalingUDP
Media Interface	OutsideMedia
Secondary Media Interface	None
End Point Policy Group	SP-PG
Routing Profile	EN-RP
Topology Hiding Profile	SP-TH
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom of the configuration window is a 'Finish' button. The background of the interface shows a sidebar with navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (highlighted), Network Management, Media Interface, Signaling Interface, End Point Flows (highlighted in red), Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, and Troubleshooting. The main content area on the right shows a list of flows with buttons for 'Edit' and 'Delete'.

Similarly, the following screen shows the Server Flow **EN-SF** configured for EN.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBC) web interface. The main title is "Session Border Controller for Enterprise" with the Avaya logo in the top right corner. A sidebar on the left contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, Signaling Interface, End Point Flows (highlighted in red), Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, and Troubleshooting. The main content area shows a modal window titled "Edit Flow: EN-SF" with a close button (X) in the top right corner. The modal contains the following configuration fields:

Field	Value
Flow Name	EN-SF
Server Configuration	EN-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideSignalingUDP
Signaling Interface	InsideSignalingTLS
Media Interface	InsideMedia
Secondary Media Interface	None
End Point Policy Group	EN-PG
Routing Profile	SP-RP
Topology Hiding Profile	EN-TH
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom of the modal is a "Finish" button. On the right side of the modal, there are "Clone", "Edit", and "Delete" buttons for each configuration item.

8. Bell Canada Service Configuration

Bell Canada is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Bell Canada will provide the customer with the necessary information to configure the SIP connection from the enterprise to Bell Canada. The information provided by Bell Canada includes:

- SIP domain and port number used for signaling through security devices (if any).
- SIP domain and port number used for media through security devices (if any).
- Bell Canada SIP domain. In the compliance testing, Bell Canada preferred to use SIP domain as an URI-Host.
- CPE SIP domain. In the compliance testing, Bell Canada preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers, User Name, Domain and Password.

The sample configuration between Bell Canada and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP trunk implemented on either Bell Canada or enterprise side.

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 useful troubleshooting commands.

9.1. Verification Steps

- Verify that endpoints at the enterprise site can place calls to PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from PSTN and that the call can remain active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
- Verify that the user on 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. Protocol Traces

The following SIP headers are inspected using Wireshark trace analysis:

- Request-URI: verify the called party number and SIP domain.
- From: verify the calling party name and number.
- To: verify the called party name and number.
- P-Asserted-Identity: verify the calling party name and number.
- Privacy: verify the value “user” and/or “id” presents the private call scenario.

The following attributes in SIP message body are inspected using Wireshark trace analysis:

- Connection Information (c line): verify IP address of near end and far end endpoints.
- Time Description (t line): verify session timeout value of near end and far end endpoints.
- Media Description (m line): verify audio port, codec, DTMF event description.
- Media Attribute (a line): verify specific audio port, codec,ptime, send/ receive ability, DTMF event and fax attributes.

9.3. Troubleshooting:

9.3.1. The Avaya SBCE

Use Avaya SBCE trace tool, traceSBC to monitor the SIP signaling messages between Bell Canada and the Avaya SBCE.

9.3.2. Communication Manager

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 7.1.1, Avaya Aura® Session Manager 7.1.1 and Avaya Session Border Controller for Enterprise 7.2 to Bell Canada SIP Trunking Service. Bell Canada SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Bell Canada provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases were executed. Despite the observation seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The Bell Canada SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 7.1.1, Avaya Aura® Session Manager 7.1.1 and Avaya Session Border Controller for Enterprise 7.2.

11.References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *What's New in Avaya Aura Release 7.1.1*, Release 7.1.1, Issue 2, August 2017.
- [2] *Upgrading Avaya Aura® System Manager to Release 7.1.1*, Issue 2, August 2017.
- [3] *Administering Avaya Aura® System Manager for Release 7.1.1*, Issue 5, August 2017.
- [4] *Administering Avaya Aura® Session Manager for Release 7.1.1*, Issue 2, August 2017.
- [5] *Deploying Avaya Aura Communication Manager in Virtualized Environment*, Release 7.1.1, Issue 2, August 2017.
- [6] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.2, Issue 2, June 2017.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2, Issue 3, September 2017.
- [8] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.2, Issue 1, June 2017.
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2, January 2017.
- [10] *Deploying and Updating Avaya Aura Media Server Appliance*, Release 7.8, Issue 3, August 2017.
- [11] *9600 Series IP Deskphones Overview and Specification*, Release 7.1, June 2017.
- [12] *Installing and Maintaining Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.1, June 2017.
- [13] *Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.1, June 2017.
- [14] *Avaya Equinox™ Overview and Specification for Android, iOS, Mac, and Window*, Release 3.0, January 2017.
- [15] *Administering Avaya one-X® Communicator*, Release 6.2, April 2015.
- [16] *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*
- [17] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [18] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [19] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for Bell Canada Networks' SIP Trunking Solution is available from Bell Canada.

©2018 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.