



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura ® Communication Manager 8.0, Avaya Aura ® Session Manager 8.0, Avaya Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 7.2 to support Swisscom Enterprise SIP Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Swisscom Enterprise SIP Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 7.2.

The Swisscom Enterprise SIP Platform provides PSTN access via a SIP trunk connected to the Swisscom Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks.

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.

Swisscom is a member of the DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	5
2.3.	Support	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager	9
5.1.	Confirm System Features	9
5.2.	Administer IP Node Names.....	10
5.3.	Administer IP Network Region.....	11
5.4.	Administer IP Codec Set	12
5.5.	Administer SIP Signaling Groups	13
5.6.	Administer SIP Trunk Groups.....	14
5.7.	Administer Calling Party Number Information	16
5.8.	Administer Route Selection for Outbound Calls.....	16
5.9.	Administer Incoming Digit Translation	18
5.10.	EC500 Configuration.....	19
6.	Configuring Avaya Aura® Session Manager	20
6.1.	Log in to Avaya Aura® System Manager.....	20
6.2.	Administer SIP Domain	21
6.3.	Administer Locations	22
6.4.	Administer Adaptations.....	23
6.5.	Administer SIP Entities	25
6.5.1.	Avaya Aura® Session Manager SIP Entity	26
6.5.2.	Avaya Aura® Communication Manager SIP Entity	27
6.5.3.	Avaya Aura® Experience Portal SIP Entity	28
6.5.4.	Avaya Session Border Controller for Enterprise SIP Entity	29
6.6.	Administer Entity Links	30
6.7.	Administer Routing Policies	31
6.8.	Administer Dial Patterns	32
7.	Configure Avaya Aura® Experience Portal	35
7.1.	Background	35
7.2.	Logging In and Licensing	36
7.3.	VoIP Connection	37
7.4.	Speech Servers	38
7.5.	Application References	38
7.6.	MPP Servers and VoIP Settings	40
8.	Configure Avaya Session Border Controller for Enterprise	43
8.1.	Access Avaya Session Border Controller for Enterprise	43
8.2.	Define Network Management	45
8.3.	Define TLS Profiles	48
8.3.1.	Certificates	48
8.3.2.	Client Profile.....	49

8.3.3.	Server Profile	50
8.4.	Define Interfaces	51
8.4.1.	Signalling Interfaces	51
8.4.2.	Media Interfaces.....	52
8.5.	Define Server Interworking.....	53
8.5.1.	Server Interworking Avaya.....	53
8.5.2.	Server Interworking – Swisscom Enterprise SIP.....	55
8.6.	Define Servers	57
8.6.1.	Server Configuration – Avaya	57
8.6.2.	Server Configuration – Swisscom Enterprise SIP	59
8.7.	Routing	61
8.7.1.	Routing – Avaya	61
8.7.2.	Routing – Swisscom Enterprise SIP	62
8.8.	Topology Hiding	64
8.9.	Server Flows.....	66
9.	Configure the Swisscom Enterprise SIP Equipment	69
10.	Verification Steps.....	69
11.	Conclusion	71
12.	Additional References.....	72

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Swisscom Enterprise SIP Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R8.0 (Communication Manager); Avaya Aura® Session Manager R8.0 (Session Manager); Avaya Aura® Experience Portal R7.2 (Experience Portal) and Avaya Session Border Controller for Enterprise R7.2.2 (Avaya SBCE).

Customers using this Avaya SIP-enabled enterprise solution with the Swisscom Enterprise SIP Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to connect to the Swisscom Enterprise SIP platform.

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

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the Swisscom Enterprise SIP Service, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Swisscom Enterprise SIP Service to PSTN destinations, calls made from SIP and H.323 telephones.
- Incoming and Outgoing PSTN calls to/from Avaya one-X® Communicator and Avaya Equinox™ for Windows soft phones.
- Calls using the G.711A and G.729 codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38 and G.711 pass-through fax transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by the Swisscom requiring Avaya response and sent by Avaya requiring Swisscom response.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold).
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agents and extensions.
- Call and two-way talk path establishment between callers and Communication Manager agents and extensions following redirection from Experience Portal.
- Routing inbound vector call to call center agent queues.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Swisscom SIP Trunking Service with the following observations:

- It was observed during testing that when a call was forwarded to Voicemail that Swisscom sent a PRACK after the call had been transferred which resulted in a 481 Call/Transaction Does Not Exist response from Communication Manager. This behaviour had no negative impact on the call and just resulted in extra signalling.
- It was observed during testing that Experience Portal uses REFER to complete Blind transfers to the PSTN which led to signalling issues and Blind transfer failures between Avaya and the Swisscom SIP trunk. In order to complete Blind transfers successfully within Experience Portal, REFER Handling needs to be enabled on the Swisscom Server Interworking (**Section 8.5.2**) on the Avaya SBCE. When the REFER message comes from an Avaya enterprise element such as Experience Portal, the Avaya SBCE translates that REFER into a reINVITE which will then be routed towards the trunk server (i.e. Swisscom) based on the trunk server interworking profile configuration

- When putting an outbound call on hold from the PBX, it was observed that the Avaya SBCE did not maintain the conversion between SRTP within the enterprise and RTP on the SIP Trunk. To work around this, the enterprise equipment was reconfigured to use RTP as described in **Section 5.4** and a fault report was raised on the Avaya SBCE.
- No Inbound Toll-Free access available for test.
- No Emergency Services test call booked with Operator.

2.3. Support

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

For technical support on Swisscom products please contact the Swisscom support team: Email: ent.incident-voice@swisscom.com.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Swisscom SIP platform. Located at the Enterprise site is an Avaya SBCE, Experience Portal, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Equinox™ for Windows running on laptop PCs.

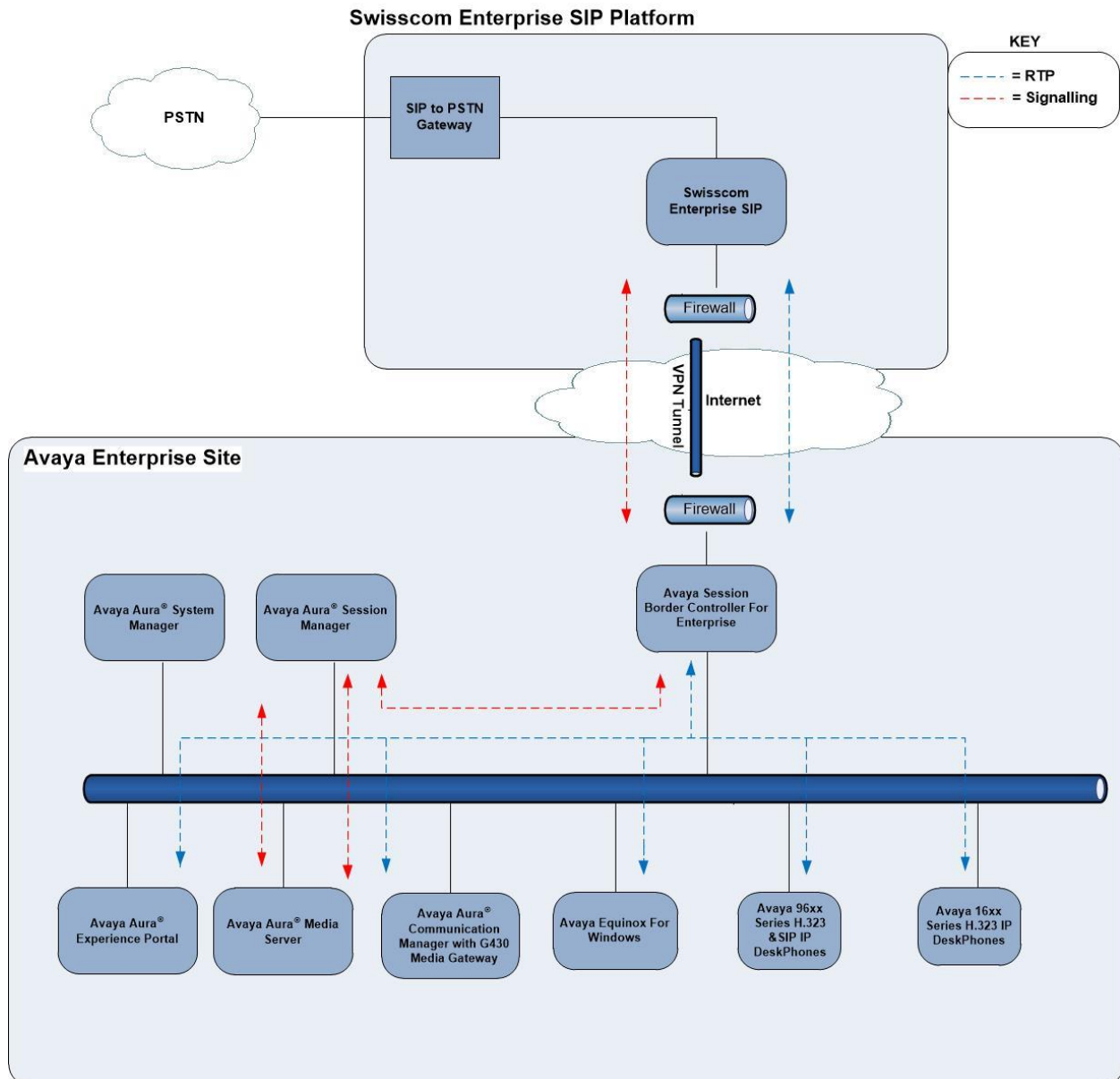


Figure 1: Test Setup Swisscom Enterprise SIP Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® System Manager	8.0.1.0 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.1.0.038836 Feature Pack 1
Avaya Aura® Session Manager	8.0.1.0.801007
Avaya Aura® Communication Manager	00.0.822.0-25031
Avaya Aura® Experience Portal	7.2.2
Avaya Session Border Controller for Enterprise	7.2.2.1-04-16104
Avaya G430 Media Gateway	40.20.0
Avaya Aura® Media Server	v.8.0.0.173
Avaya 1600 IP Deskphone (H.323)	1.3.11
Avaya 96x0 IP DeskPhone (H.323)	6.7
Avaya 9611 IP DeskPhone (SIP)	7.1.4.0
Avaya 9608 IP DeskPhone (SIP)	7.1.4.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.23 -SP12-Patch13
Avaya Equinox™ for Windows	3.4.10
Analogue Handset	N/A
Analogue Fax	N/A
Swisscom Enterprise SIP	
eSBC	Cisco 897VA 15.5 (3) M6a
C-SBC	ACME Net-Net 6300 Firmware 8.1.0 MR 1 P 3
SESM	Genband MCP_19.0.21.2_2019-02-27-0907

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the Swisscom SIP Trunking Service. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Swisscom network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Swisscom SIP Trunking Service and any other SIP trunks used.

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	3
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	0
Maximum Administered SIP Trunks:	4000	20
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0

On **Page 5**, verify that **IP Trunks** field is set to **y**.

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		

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **Session Manager** and **10.10.3.42** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** IP address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

display node-names ip		IP NODE NAMES
Name	IP Address	
AMS	10.10.3.45	
Session_Manager	10.10.3.42	
default	0.0.0.0	
procr	10.10.3.44	
procr6	::	

5.3. Administer IP Network Region

Use the **change ip-network-region n** command where **n** is the chosen value of the configuration for the SIP Trunk. Set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled or the call is set up with initial IP-IP direct media, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **2** is used.
- The rest of the fields can be left at default values.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2
Location:                Authoritative Domain: avaya.com
Name: Trunk              Stub Network Region: n
MEDIA PARAMETERS        Intra-region IP-IP Direct Audio: yes
Codec Set: 2            Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048      IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS        RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

5.4. Administer IP Codec Set

Open the IP Codec Set form for the codec set specified in the IP Network Region form in **Section 5.3** by typing **change ip-codec set n** where **n** is the chosen value of the configuration for the SIP Trunk. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by Swisscom were configured, namely **G.711A** and **G.729**.

In addition to the codec's, the **Media Encryption** is defined here. A typical value would be 1-srtp-aescm128-hmac80, but during testing a value of **none** was used as RTP was used for the compliance testing.

change ip-codec-set 2				Page 1 of 2
IP MEDIA PARAMETERS				
Codec Set: 2				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711A	n	2	20	
2: G.729	n	2	20	
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp
1: none				
2:				

Swisscom SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define fax properties as follows:

- Set the **FAX - Mode** to **t.38-standard**.
- Leave **ECM** at default value of **y**.

change ip-codec-set 2				Page 2 of 2
IP MEDIA PARAMETERS				
Allow Direct-IP Multimedia? n				
	Mode	Redun- dancy	Packet Size (ms)	
FAX	t.38-standard	0	ECM: y	
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0	20	

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Swisscom SIP Trunking Service. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tls**.
- Set **Peer Detection Enabled** to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to Session Manager interface (node name **Session_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required. The standard value for TLS is **5061**.
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3** (logically establishes the far-end for calls using this signalling group as region **1**).
- Leave **Far-end Domain** blank to allow Communication Manager to accept calls from any SIP domain on the associated trunk.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set both **H.323 Station Outgoing Direct Media** and **Initial IP-IP Direct Media** to **y** so that the call is set up to use direct media.

The default values for the other fields may be used.

add signaling-group 1		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? n		
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: Session_Manager		
Near-end Listen Port: 5061	Far-end Listen Port: 5061		
	Far-end Network Region: 1		
Far-end Domain:			
		Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y		
Session Establishment Timer(min): 3	IP Audio Hairpinning? n		
Enable Layer 3 Test? n	Initial IP-IP Direct Media? y		
H.323 Station Outgoing Direct Media? y	AlternateRoute Timer(sec): 6		

5.6. Administer SIP Trunk Groups

A trunk group is associated with the signalling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group n** command, where **n** is an available trunk group for the SIP Trunk. On **Page 1** of this form:

- Set the **Group Type** field to **sip**.
- Choose a descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **public-network**.
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**.
- Specify the **Number of Members** administered for this SIP trunk group.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 10	

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Swisscom to prevent unnecessary SIP messages during call setup. During testing, a value of **450** was used that sets Min-SE to 900 in the SIP signalling.

add trunk-group 1		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): 450			
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 allows delivery of CLI in E.164 format with leading “+”.

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: public
	UII Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y**.
- Set **Send Transferring Party Information** to **n**.
- Set **Network Call Direction** to **n**.
- Set **Send Diversion Header** to **y**.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101** as requested by Swisscom.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- Set the **Identity for Calling Party Display** to **P-Asserted-Identity**.

add trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? 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? y
	Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? N
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
	Request URI Contents: may-have-extra-digits

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. These calling party numbers are sent in the SIP From, Contact and PAI headers as well as the Diversion header for forwarded calls. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network. The public numbering table is used for numbers in E.164 format.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	6102	1	41438xxxxx80	13	Total Administered: 4
4	6010	1	41438xxxxx81	13	Maximum Entries: 240
4	6020	1	41438xxxxx82	13	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	6104	1	41438xxxxx83	13	
					Communication Manager automatically inserts a '+' digit in this case.

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Swisscom SIP Trunking Service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to invoke ARS directly. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *69		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 7		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning **0**. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Max	Route Pattern	Call Type	Node Num	ANI Reqd	
0	11	14	1	pubu		n	
00	13	15	1	pubu		n	
0035391	13	13	1	pubu		n	
030	10	10	1	pubu		n	
0800	8	10	1	pubu		n	
0900	8	8	1	pubu		n	

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **unk-unk**.

change route-pattern 1													Page	1 of	3	
Pattern Number: 1													Pattern Name:			
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: 1	0											n	user			
2:											n	user				
3:											n	user				
4:											n	user				
5:											n	user				
6:											n	user				
BCC		VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature		PARM	No.	Numbering	LAR	
0	1	2	M	4	W	Request						Dgts	Format			
													Subaddress			
1:	y	y	y	y	y	n	n	rest				unk-unk	none			
2:	y	y	y	y	y	n	n	rest					none			
3:	y	y	y	y	y	n	n	rest					none			
4:	y	y	y	y	y	n	n	rest					none			
5:	y	y	y	y	y	n	n	rest					none			
6:	v	v	v	v	n	n		rest					none			

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Swisscom can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DDI numbers provided by Swisscom Enterprise SIP platform correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers **+41438xxxxx80**, **+41438xxxxx81**, **+41438xxxxx82** and **+41438xxxxx83** to a 4-digit extension by deleting all of the incoming digits and inserting an extension.

change inc-call-handling-trmt trunk-group 1					Page 1 of 3	
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Del Digits	Insert			
public-ntwrk	13	+41438xxxxx80	all	6102		
public-ntwrk	13	+41438xxxxx81	all	6010		
public-ntwrk	13	+41438xxxxx82	all	6020		
public-ntwrk	13	+41438xxxxx83	all	6104		

5.10. EC500 Configuration

When EC500 is enabled on a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone.

The following screen shows an example EC500 configuration for the user with station extension 6102. Use the command **change off-pbx-telephone station-mapping x** where **x** is Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035389434xxxx**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 6102							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
6102	EC500	-		0035389434xxxx	ars	1	

Note: The phone number shown is for a mobile phone in the Avaya Lab. To use facilities for calls coming in from EC500 mobile phones, the calling party number received in Communication Manager must exactly match the number specified in the above table.

Save Communication Manager configuration by entering **save translation**.

6. Configuring Avaya Aura® Session Manager

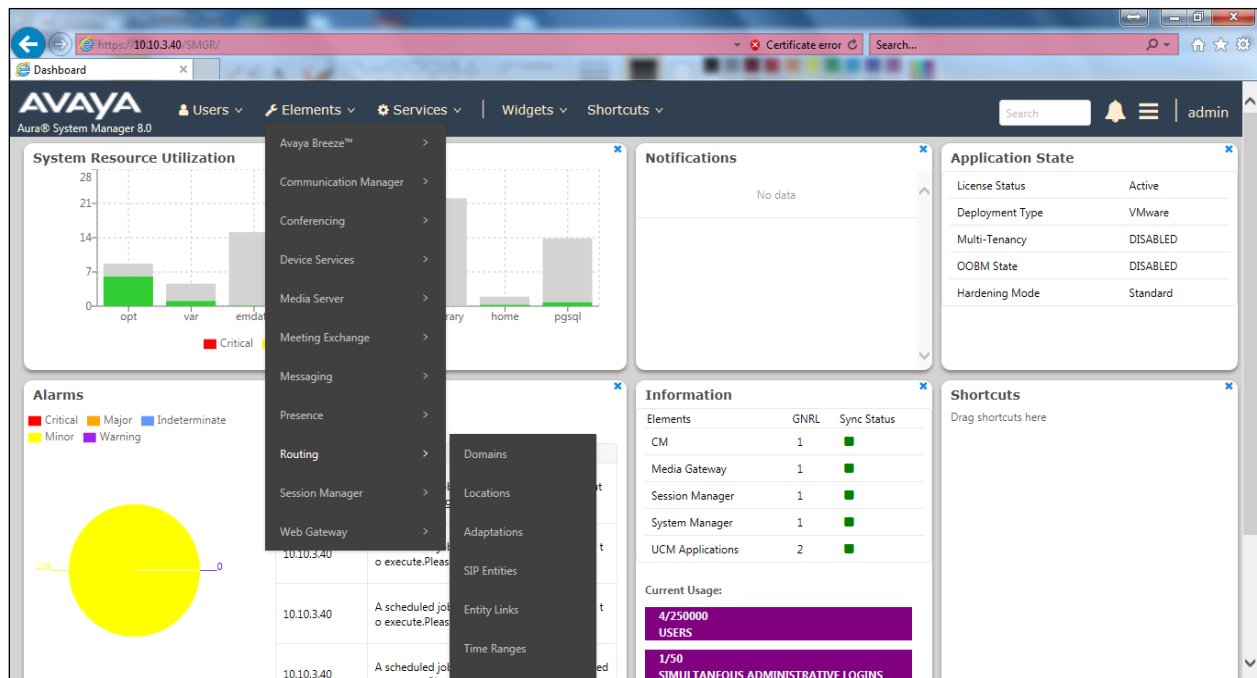
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP Domain.
- Administer SIP Location.
- Administer Adaptations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Routing Policies.
- Administer Dial Patterns.

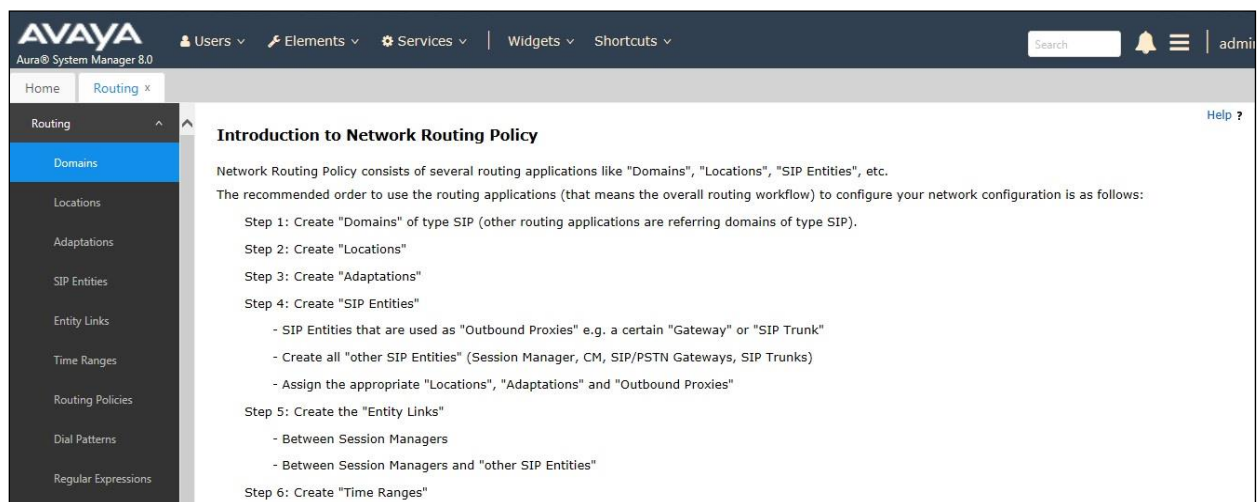
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser and entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Dashboard tab will be presented with menu options shown below.



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

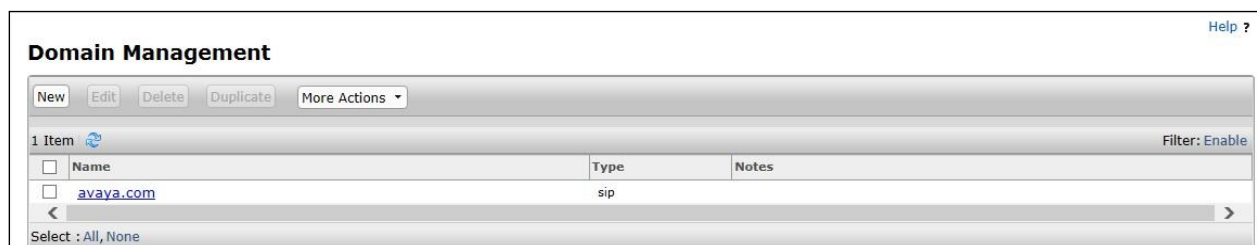


6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements** → **Routing** and select **Domains** from the left navigation menu, click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter a Domain Name. In the sample configuration, **avaya.com** was used.
- **Type** Verify **SIP** is selected.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



6.3. Administer Locations

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

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

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern, then Session Manager uses the location administered for the SIP Entity.

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **SMGR_8** defined for the compliance testing.

The screenshot shows a web form titled "Location Details" with "Commit" and "Cancel" buttons in the top right. The form is divided into three sections: "General", "Dial Plan Transparency in Survivable Mode", and "Overall Managed Bandwidth".

- General**: Contains a required field "Name:" with the value "SMGR_8" and an optional "Notes:" field.
- Dial Plan Transparency in Survivable Mode**: Contains an "Enabled:" checkbox (unchecked), a "Listed Directory Number:" field, and an "Associated CM SIP Entity:" field.
- Overall Managed Bandwidth**: Contains a "Managed Bandwidth Units:" dropdown menu set to "Kbit/sec", a "Total Bandwidth:" field, a "Multimedia Bandwidth:" field, and a checked checkbox for "Audio Calls Can Take Multimedia Bandwidth:".

6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers. An Adaptation was used during testing to remove Avaya proprietary headers from messages sent. Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. In order to improve interoperability with third party elements, Session Manager R8.0 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary unnecessary for non-Avaya elements. For the compliance test, an Adaptation named “**Swiss**” was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. These headers contain private information from the enterprise and also add unnecessary size to outbound messages, while they have no significance to the service provider.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left-hand menu and then click on the **New** button (not shown). Under **Adaptation Details** → **General**:

- **Adaption Name:** Enter an appropriate name such as **Swisscom**.
- **Module Name:** Select **DigitConversionAdapter**.
- **Modular Parameter Type:** Select **Name-Value Parameter**.

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

- **Name:** Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value:** Enter **AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, P-Location**.
- **Name:** Enter **fromto**. Modifies From and To header of a message.
- **Value:** Enter **true**.
- **Name:** Enter **MIME**. Remove MIME message bodies from Session Manager.
- **Value:** Enter **no**.

Adaptation Details Commit Cancel Help ?

General

Adaptation Name:

Module Name:

Module Parameter Type:

Name	Value
<input type="checkbox"/> eRHdrs	"P-AV-Message-Id, P-Charging-Vector, P-Location, Endpoint-View, P-Conference, Alert-
<input type="checkbox"/> fromto	true
<input type="checkbox"/> MIME	no

Select : All, None

Egress URI Parameters:

Notes:

Scroll down the page and under **Digit Conversion for Outgoing Calls from SM**, click the **Add**

button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so **both** have been selected.

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*00	2	15		2	+	both		

Select : All, None

Commit Cancel

This will ensure any outgoing numbers matching 00 will be deleted and have + inserted being converted to E.164 format before being forwarded to the Avaya SBCE.

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP Entity, **CM** for a Communication Manager SIP Entity, **Voice Portal** for an Experience Portal SIP Entity and **SIP Trunk** for the Avaya SBCE SIP Entities.
- In the **Location** field select the appropriate location from the drop-down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are four SIP Entities.

- Session Manager SIP Entity.
- Communication Manager SIP Entity.
- Experience Portal SIP Entity.
- Avaya SBCE SIP Entity.

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

SIP Entity Details

CommitCancel

General

* Name: Session Manager

* IP Address: 10.10.3.42

SIP FQDN:

Type: Session Manager

Notes:

Location: SMGR_8

Outbound Proxy:

Time Zone: Europe/Dublin

Minimum TLS Version: Use Global Setting

Credential name:

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop-down menu select the domain added in **Section 6.2** as the default domain.

Port

TCP Failover port:

TLS Failover port:

AddRemove

3 Items

Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	
<input type="checkbox"/>	5061	UDP	avaya.com	

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. This SIP Entity is used for the SIP Trunk. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the **Location** to that defined in **Section 6.3**.

SIP Entity Details

CommitCancel

General

* Name: Communication Manager

* FQDN or IP Address: 10.10.3.44

Type: CM

Notes:

Adaptation:

Location: SMGR_8

Time Zone: Europe/Dublin

* 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: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5.3. Avaya Aura® Experience Portal SIP Entity

The following screen shows the SIP entity for Experience Portal. The **FQDN or IP Address** field is set to the IP address of the Experience Portal. Set the **Location** to that defined in **Section 6.3**.

SIP Entity Details

CommitCancel

General

* Name: Experience_Portal

* FQDN or IP Address: 10.10.3.50

Type: Voice Portal

Notes:

Adaptation:

Location: SMGR_8

Time Zone: Europe/Dublin

* 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: On

Loop Count Threshold: 5

6.5.4. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE used for PSTN destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (See **Section 8.4.1**). Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

SIP Entity Details

CommitCancel

General

* Name: Avaya_SBCE

* FQDN or IP Address: 10.10.3.30

Type: SIP Trunk

Notes:

Adaptation: Swiss

Location: SMGR_8

Time Zone: Europe/Dublin

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop-down menu to make the other system trusted.

Click **Commit** to save changes. The following screenshot shows the Entity Links used in this configuration.

Note: The Entity Links configurations used in the compliance testing are Avaya_SBCE and Communication_Manager as per the screenshot below.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	Aura_Messaging	Session Manager	TLS	5061	Aura_Messaging	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Avaya_SBCE	Session Manager	TLS	5061	Avaya_SBCE	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Communication_Manager	Session Manager	TLS	5061	Communication_Manager	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Experience_Portal	Session Manager	TLS	5061	Experience_Portal	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown). Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for calls inbound from the SIP Trunk to Communication Manager.

Routing Policy Details [Commit] [Cancel]

General

* Name: to_Communication_Manager

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.3.44	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

The following screen shows the routing policy for Avaya SBCE for the Swisscom SIP trunk.

Routing Policy Details [Commit] [Cancel]

General

* Name: to_Avaya_SBCE

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE	10.10.3.30	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

The following screen shows the routing policy for calls inbound from the SIP Trunk to Experience Portal.

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Experience_Portal	10.10.3.50	Voice Portal	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern, select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Swisscom SIP Trunk.

Dial Pattern Details
Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

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"/>	SMGR_8		to_Avaya_SBCE	0	<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

The following screen shows the dial pattern configured for Communication Manager.

Dial Pattern Details
Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

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"/>	SMGR_8		to_Communication_Manager	0	<input type="checkbox"/>	Communication Manager	

Select : All, None

The following screen shows the dial pattern configured for Experience Portal.

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern: +41438xxxx85

* Min: 13

* Max: 13

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

AddRemove

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"/>	SMGR_8		to_Experience_Portal	0	<input type="checkbox"/>	Experience_Portal	

Select : All, None

7. Configure Avaya Aura® Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [13] in the **References** section for further details if necessary.

7.1. Background

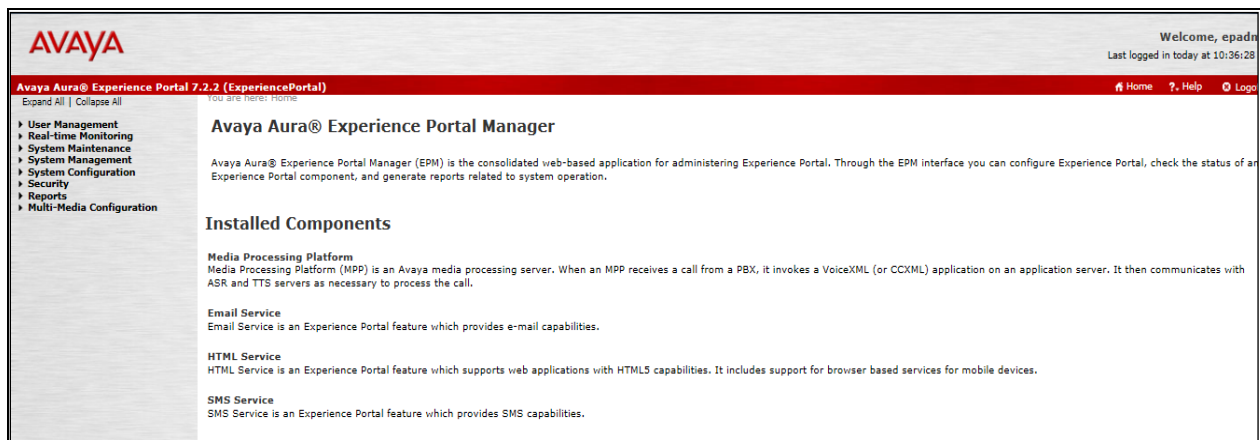
Experience Portal consists of one or more Media Processing Platform (MPP) servers and an Experience Portal Manager (EPM) server. A single “server configuration” was used in the reference configuration. This consisted of a single MPP and EPM, running on a VMware environment, including an Apache Tomcat Application Server (hosting the Voice XML (VXML) and/or Call Control XML (CCXML) application scripts), that provide the directives to Experience Portal for handling the inbound calls.

References to the Voice XML and/or Call Control XML applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party DDI number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match is found, Experience Portal informs the caller that the call cannot be handled, and disconnects the call sample configuration described in these Application Notes. A simple VXML test application was used to exercise various SIP call flow scenarios with the Swisscom SIP Trunk service. In production, enterprises can develop their own VXML and/or CCXML applications to meet specific customer self-service needs, or consult Avaya Professional Services and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes.

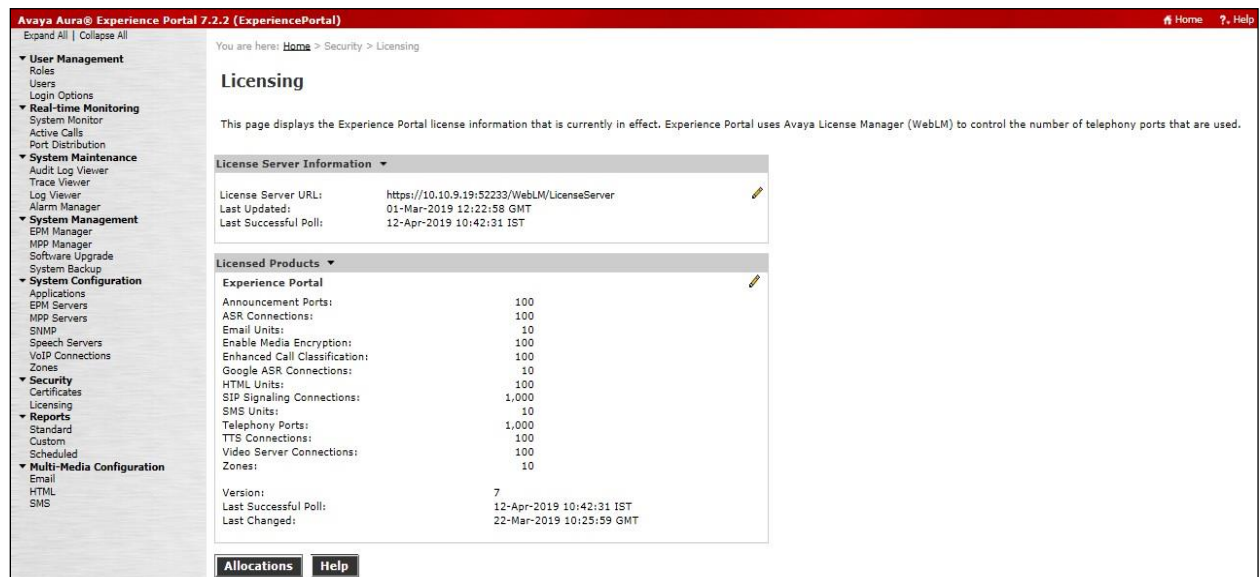
7.2. Logging In and Licensing

This section describes the steps on Experience Portal for administering a SIP connection to the Session Manager.

Step 1 - Launch a web browser, enter `http://<IP address of the Avaya EPM server>/` in the URL, log in with the appropriate credentials and the following screen is displayed.



Step 2 - In the left pane, navigate to **Security**→**Licensing**. On the **Licensing** page, verify that Experience Portal is properly licensed. If required licenses are not enabled, contact an authorized Avaya representative to obtain the licenses.



7.3. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager.

Step 1 - In the left pane, navigate to **System Configuration**→**VoIP Connections**. On the **VoIP Connections** page, select the **SIP** tab and click **Add** to add a SIP trunk. **Note** – Only one SIP trunk can be active at any given time on Experience Portal.

Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls
SM8	Yes	TLS	10.10.3.42	5061	5061	avaya.com	10

Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g. SM8).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
 - **Proxy Server Address** = **10.10.3.42** (the IP address of the Session Manager signaling interface defined in **Section 6.5.1**).
 - **Port** = **5061**
 - **Priority** = **0** (default)
 - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **avaya.com** (see **Section 6.2**).
- **Consultative Transfer** – Select **INVITE with REPLACES**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **10** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES_CM_128**
- **Authentication Algorithm** = **HMAC_SHA1_80**
- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- Use default values for all other fields.
- Click **Save**.

7.4. Speech Servers

The installation and administration of the ASR and TSR Speech Servers are beyond the scope of this document. Some of the values shown below were defined during the Speech Server installations. Note that in the reference configuration the ASR and TTS servers used the same IP address.

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)

You are here: [Home](#) > System Configuration > Speech Servers

Speech Servers

This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.

ASR TTS

Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
<input type="checkbox"/> ASR	Yes	10.10.3.50	Nuance	MRCP V1	5060	10	English(UK) en-GB

[Add](#) [Delete](#) [Customize](#) [Help](#)

7.5. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.10.3.50.

Step 1 - In the left pane, navigate to **System Configuration** → **Applications**. On the **Applications** page (not shown), click **Add** to add an application and configure as follows:

- **Name** – Set to a descriptive name (e.g., **Test_App**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type. CCXML was used in the test configuration.
- **VoiceXML** and/or **CCXML URL** – Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Experience Portal test application on a single server is referenced. CCXML was used in the test configuration.
- **Speech Servers ASR** and **TTS** – Select the appropriate ASR and/or TTS servers as necessary.
- **Application Launch** – Set to **Inbound**.
- **Called Number** – Enter the number to match against an inbound SIP INVITE message, and click **Add**.

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of an application.

Name: Test_App
Enable: ☒ Yes ☐ No
Type: CCXML
Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum
Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

CCXML URL:

Verify

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

ASR Speech Servers ▾

ASR:	Engine Types	Selected Engine Types
	<None>	<None>

TTS Speech Servers ▾

TTS:

Application Launch ▾

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number:

Add

418380000085
8000

Remove

Speech Parameters ▸

Reporting Parameters ▸

Advanced Parameters ▸

Save

Apply

Cancel

Help

7.6. MPP Servers and VoIP Settings

This section illustrates the procedure for viewing or changing the MPP Settings. In the sample configuration, the MPP Server is co-resident on a single server with the Experience Portal Management server (EPM).

Step 1 - In the left pane, navigate to **System Configuration**→**MPP Servers** and the following screen is displayed. Click **Add**.

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)

Expand All | Collapse All

► User Management
► Real-time Monitoring
► System Maintenance
► System Management
▼ System Configuration
 Applications
 EPM Servers
 MPP Servers
 SNMP
 Speech Servers
 VoIP Connections
 Zones
► Security
► Reports
► Multi-Media Configuration

You are here: [Home](#) > System Configuration > MPP Servers

MPP Servers

This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, communicates with ASR and TTS servers as necessary to process the call.

<input type="checkbox"/>	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/>	mpp1	10.10.3.50	<Default>	<Default>	<Default>	10	Use MPP Settings

[Add](#) [Delete](#)

[MPP Settings](#) [Browser Settings](#) [Video Settings](#) [VoIP Settings](#) [Help](#)

Step 2 - Enter any descriptive name in the **Name** field (e.g. **mpp1**) and the IP address of the MPP server in the **Host Address** field and click **Continue** (not shown).

Step 3 - The certificate page will open. Check the **Trust this certificate** box (not shown). Once complete, click **Save**.

You are here: [Home](#) > System Configuration > [MPP Servers](#) > Change MPP Server

Change MPP Server

Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels to Finest if your Experience Portal system has heavy call traffic. The system might experience performance issues if Trace Levels are set to Finest. Set Trace Levels to Finest only when you are troubleshooting the system.

Name: mmp1
Host Address: 10.10.3.50
Network Address (VoIP): <Default>
Network Address (MRCP): <Default>
Network Address (AppSvr): <Default>
Maximum Simultaneous Calls: 10
Restart Automatically: ☐ Yes ☒ No

MPP Certificate

Owner: CN=ep7cmn.avaya.com, O=Avaya, OU=EPM
Issuer: CN=ep7cmn.avaya.com, O=Avaya, OU=EPM
Serial Number: 952c116c181b7515
Signature Algorithm: SHA256withRSA
Valid from: 28 February 2019 12:17:17 GMT until 28 February 2029 12:17:17 GMT
Certificate Fingerprints
MD5: 8b:17:0c:92:48:ef:64:3d:86:b2:60:6a:bb:f5:09:69
SHA: 9a:50:a4:2c:48:21:46:a2:e6:18:a0:35:b0:e6:c1:48:3a:9b:d1:be
SHA-256: 09:cb:da:79:0d:e6:ae:02:95:80:eb:92:56:0c:15:17:b2:f6:9e:f6:f9:2e:90:68:8e:06:be:98:96:cc:fa:26
Subject Alternative Names
DNS Name: ep7cmn
DNS Name: ep7cmn.avaya.com
IP Address: 10.10.3.50

[Categories and Trace Levels](#)

Step 4 - Click **VoIP Settings** tab on the screen displayed in **Step 1**, and the following screen is displayed.

- In the Port Ranges section, default ports were used.

You are here: [Home](#) > [System Configuration](#) > [MPP Servers](#) > VoIP Settings

VoIP Settings

Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.

Port Ranges

	Low	High
UDP:	11000	30999
TCP:	31000	33499
MRCP:	34000	36499
H.323 Station:	37000	39499

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format: audio/basic

- In the Codecs section set:
 - Set **Packet Time** to **20**.
 - Verify the **G711alaw**, **G729** and **G711ulaw** codecs are enabled.
 - Set **G729 Discontinuous Transmission** to **No** (G.729A).
 - Set the **Offer Order** to the preferred codec.
- Use default values for all other fields.

Step 5 - Click on **Save**.

Codecs

Offer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G711aLaw	1
<input checked="" type="checkbox"/>	G729	2
<input checked="" type="checkbox"/>	G711uLaw	3

Packet Time: 20 milliseconds

G729 Discontinuous Transmission: ☐ Yes ☒ No

Answer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G711uLaw	1
<input checked="" type="checkbox"/>	G711aLaw	1
<input checked="" type="checkbox"/>	G729	1

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☒ Yes ☐ No

QoS Parameters

Out of Service Threshold (% of VoIP Resources)

Call Progress

Miscellaneous

Save

Apply

Cancel

Help

After saving the configuration changes, restart the MPP server for the change to take effect. As shown below, the MPP may be restarted using the **Restart** button available via the Experience Portal GUI at **System Management → MPP Manager**. Note that the **State** column shows when the MPP is running after the restart.

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal)
Expand All | Collapse All

- ▶ User Management
- ▶ Real-time Monitoring
- ▶ System Maintenance
- ▶ System Management
 - EPM Manager
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▶ System Configuration
- ▶ Security
- ▶ Reports
- ▶ Multi-Media Configuration

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (12-Apr-2019 13:48:10 IST)

This page displays the current state of each MPP in the Experience Portal system. To enable the state and mode commands, stopped.

Last Poll: 12-Apr-2019 13:48:03 IST

	Server Name	Mode	State	Config	Auto Restart	Restart Schedule		Active Calls	
						Today	Recurring	In	Out
<input type="checkbox"/>	mpp1	Online	Running	OK	Yes	No	None	0	0

State Commands

Start Stop Restart Reboot Halt Cancel

Mode Commands

Offline Test Online

Restart/Reboot Options
☒ One server at a time
☐ All servers

Help

8. Configure Avaya Session Border Controller for Enterprise

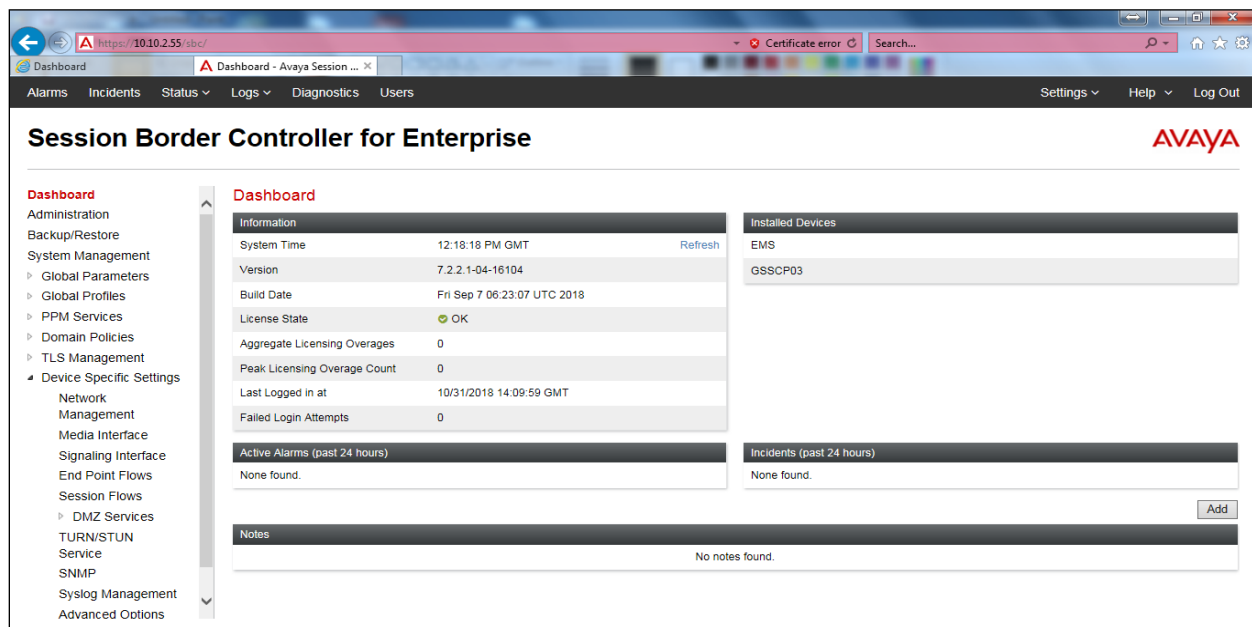
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

8.1. Access Avaya Session Border Controller for Enterprise

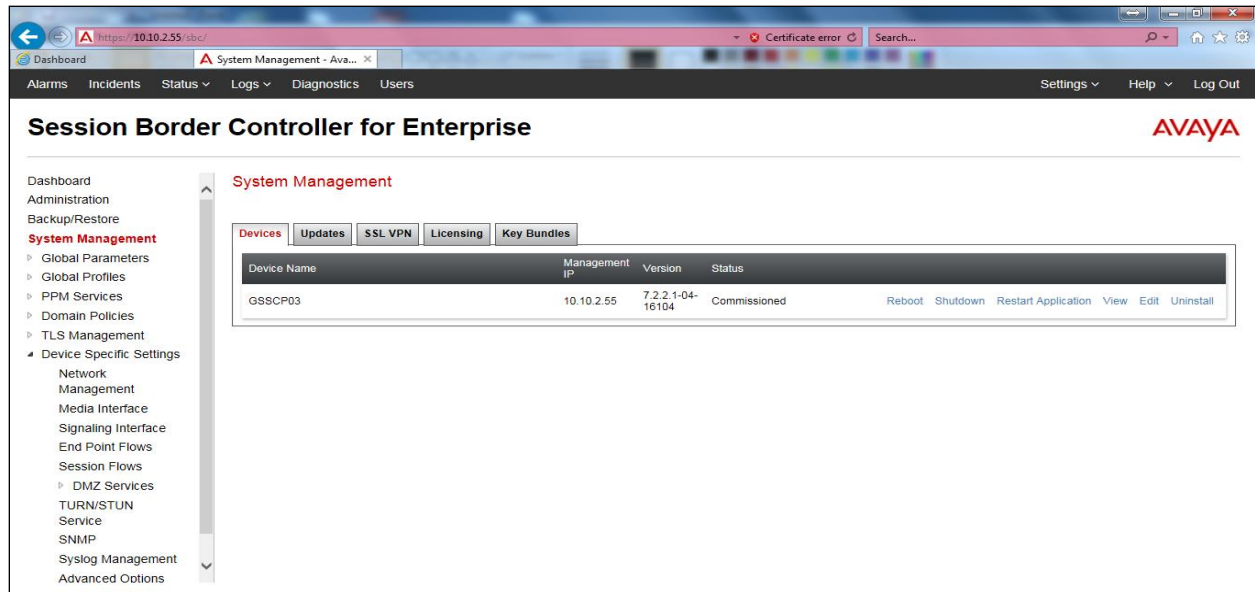
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



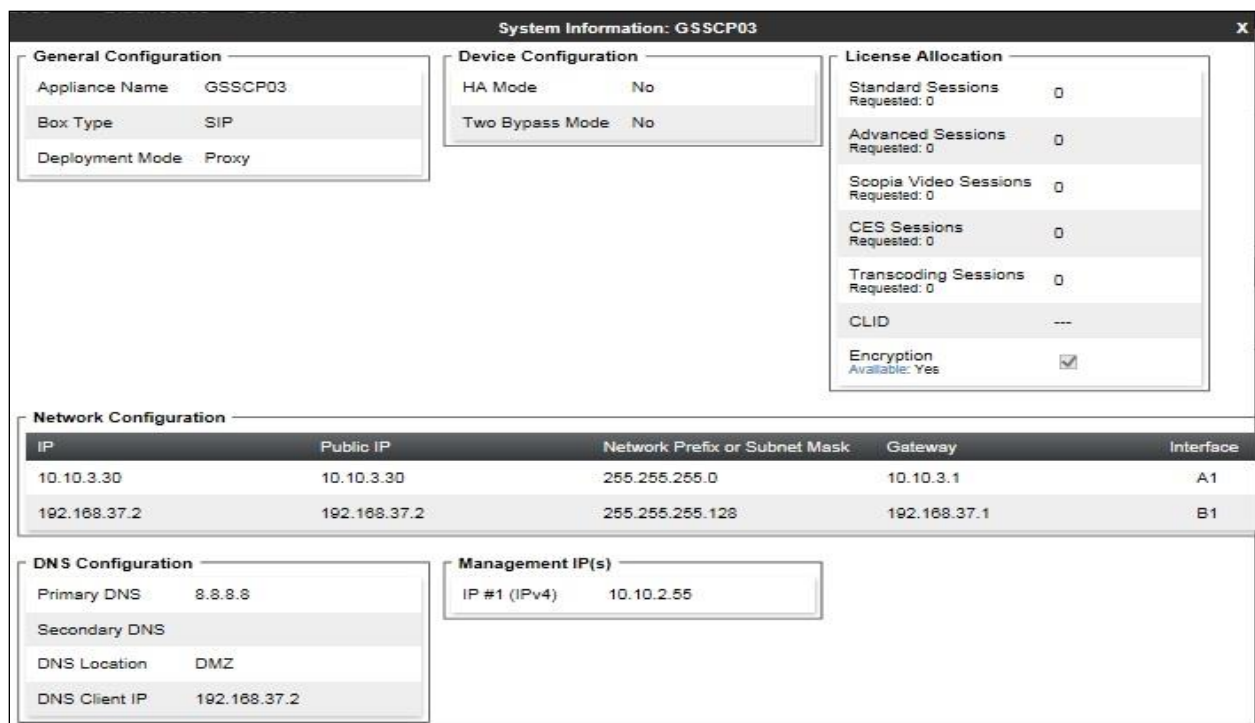
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP03** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



8.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left-hand side and click on **Add**. Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The screenshot shows a 'Network' configuration window. At the top, a warning message states: '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.' Below this, there are four input fields: 'Name' (containing 'B1_External'), 'Default Gateway' (containing '192.168.37.1'), 'Network Prefix or Subnet Mask' (containing '255.255.255.128'), and 'Interface' (a dropdown menu showing 'B1'). To the right of these fields is an 'Add' button. Below the 'Add' button is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The first row of the table contains the values '192.168.37.2', 'Use IP Address', and 'Use Default'. To the right of the table is a 'Delete' button. At the bottom of the window is a 'Finish' button.

IP Address	Public IP	Gateway Override
192.168.37.2	Use IP Address	Use Default

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBCE. Enter details in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

Network

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: A1_Internal

Default Gateway: 10.10.3.1

Network Prefix or Subnet Mask: 255.255.255.0

Interface: A1

Add

IP Address	Public IP	Gateway Override
10.10.3.30	Use IP Address	Use Default

Delete

Finish

The following screenshot shows the completed Network Management configuration:

Network Management: GSSCP03

Devices: GSSCP03

Interfaces: Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address
A1_Internal	10.10.3.1	255.255.255.0	A1	10.10.3.30
B1_External	192.168.37.1	255.255.255.128	B1	192.168.37.2

Edit Delete

Edit Delete

Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.



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

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

8.3. Define TLS Profiles

For the compliance test, TLS transport is used for signalling on the SIP trunk between Session Manager and the Avaya SBCE. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these Application Notes.

The following procedures show how to view the certificates and configure the Client and Server profiles to support the TLS connection.

8.3.1. Certificates

To view the certificates currently installed on the Avaya SBCE, navigate to **TLS Management** → **Certificates**:

- Verify that an Avaya SBCE identity certificate (**gsscp03_avaya_com.crt**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**SystemManagerCA.crt**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**gsscp_avaya_com.key**) is present under **Installed Keys**.

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. A left sidebar contains navigation links: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management (selected), Certificates (highlighted), Client Profiles, Server Profiles, and Device Specific Settings. The main content area is titled "Certificates" and includes "Install" and "Generate CSR" buttons. It is divided into four sections: "Installed Certificates" showing "gsscp03_avaya_com.crt" with "View" and "Delete" links; "Installed CA Certificates" showing "SystemManagerCA.crt" with "View" and "Delete" links; "Installed Certificate Revocation Lists" showing a message that no lists have been installed; and "Installed Keys" showing two entries, "gsscp03_avaya_com.key" and "gsscp03_avaya_com.key", each with a "Delete" link.

8.3.2. Client Profile

To create a new client profile, navigate to **TLS Management** → **Client Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Client** was used in the compliance testing.
- Set **Certificate** to the identity certificate **gsscp_avaya_com.crt** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **SystemManagerCA.crt** identity certificate.
- Set **Verification Depth** to **1**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

The screenshot shows the 'Client Profiles' configuration page for a profile named 'GSSCP_Client'. The page has a left sidebar with 'Client Profiles' and 'GSSCP_Client' listed. The main area contains a 'Client Profile' tab with the following settings:

TLS Profile	
Profile Name	GSSCP_Client
Certificate	gsscp03_avaya_com.crt

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.crt
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0

8.3.3. Server Profile

To create a new server profile, navigate to **TLS Management** → **Server Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **Gsscp_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **gsscp_avaya_com.crt** used in the compliance testing.
- Set **Peer Verification** to **Optional**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).

The screenshot displays the 'Server Profiles' management interface. On the left, a sidebar shows 'Server Profiles' with a sub-item 'Gsscp_Server'. The main area is titled 'Server Profiles: Gsscp_Server' and contains a table of server profiles. The 'Gsscp_Server' profile is selected and its details are shown in a form. The form is organized into sections: 'TLS Profile', 'Certificate Verification', 'Renegotiation Parameters', and 'Handshake Options'. The 'TLS Profile' section includes 'Profile Name' (Gsscp_Server) and 'Certificate' (gsscp03_avaya_com.crt). The 'Certificate Verification' section includes 'Peer Verification' (Optional), 'Peer Certificate Authorities' (SystemManagerCA.crt), 'Peer Certificate Revocation Lists' (---), 'Verification Depth' (1), and 'Extended Hostname Verification' (unchecked). The 'Renegotiation Parameters' section includes 'Renegotiation Time' (0) and 'Renegotiation Byte Count' (0). The 'Handshake Options' section includes 'Version' with checkboxes for TLS 1.2, TLS 1.1, and TLS 1.0, all of which are checked.

Server Profiles: Gsscp_Server	
Click here to add a description.	
Server Profile	
TLS Profile	
Profile Name	Gsscp_Server
Certificate	gsscp03_avaya_com.crt
Certificate Verification	
Peer Verification	Optional
Peer Certificate Authorities	SystemManagerCA.crt
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0

8.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

8.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **IP Address**, select the **A1_Internal** signalling interface IP addresses defined in **Section 8.2**.
- Select **TLS** port number, **5061** is used for Session Manager.
- Select a **TLS Profile** defined in **Section 8.3.3** from the drop-down menu.
- Click **Finish**.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **IP Address**, select the **B1_external** signalling interface IP address defined in **Section 8.2**.
- Select **TCP** port number, **5060** is used for the Swisscom SIP Trunk.
- Click **Finish**.

Signaling Interface: GSSCP03

Devices

GSSCP03

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30 A1_Internal (A1, VLAN 0)	5060	---	5061	Gsscp_Server	Edit Delete
Ext_Sig	192.168.37.2 B1_External (B1, VLAN 0)	5060	---	---	None	Edit Delete

8.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** from the menu on the left-hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To enter details of the media IP and RTP port range for the internal interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **IP Address**, select the **A1_Internal** media interface IP address defined in **Section 8.2**.
- For **Port Range**, enter **35000-40000**.
- Click **Finish**.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **IP Address**, select the **B1_External** media interface IP address defined in **Section 8.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.

Media Interface: GSSCP03

Devices
GSSCP03

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP Network	Port Range	
Ext_Media	192.168.37.2 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete
Int_Media	10.10.3.30 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete

8.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Swisscom SIP Trunking is connected as the Trunk Server and the Session Manager is connected as the Call Server.

8.5.1. Server Interworking Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

The screenshot shows the 'General' configuration tab for Server Interworking. The settings are as follows:

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

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

Record Routes

☐ None
☐ Single Side
☒ Both Sides
☐ Dialog-Initiate Only (Single Side)
☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions Avaya

Diversion Manipulation ☐

Diversion Condition None

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

MOBX Re-INVITE Handling ☐

DTMF

DTMF Support

☒ None
☐ SIP Notify
☐ RFC 2833 Relay & SIP Notify
☐ SIP Info
☐ RFC 2833 Relay & SIP Info
☐ Inband

Finish

8.5.2. Server Interworking – Swisscom Enterprise SIP

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles** →

Server Interworking and click on **Add**.

- Enter profile name such as Swisscom and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **Refer Handling** as per **Section 2.2**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

The screenshot shows the 'General' configuration tab for Server Interworking. The settings are as follows:

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

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

Record Routes

☐ None
☐ Single Side
☒ Both Sides
☐ Dialog-Initiate Only (Single Side)
☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions None ▾

Diversion Manipulation ☐

Diversion Condition None ▾

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

DTMF

DTMF Support

☒ None
☐ SIP Notify
☐ SIP Info
☐ Inband

Finish

8.6. Define Servers

Servers are defined for each server connected to the Avaya SBCE. In this case, Swisscom is connected as the Trunk Server and Session Manager is connected as the Call Server.

8.6.1. Server Configuration – Avaya

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Call Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: GSSCP_Client

Add

IP Address / FQDN	Port	Transport
10.10.3.42	5061	TLS

Delete

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.

Server Configuration Profile - Advanced

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

Finish

8.6.2. Server Configuration – Swisscom Enterprise SIP

To define the Swisscom Trunk Server, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **10.254.150.52** (Swisscom SIP Enterprise).
- For **Port**, enter **5060**.
- For **Transport**, select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

Server Configuration Profile - General [X]

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server ▼

SIP Domain:

DNS Query Type: NONE/A ▼

TLS Client Profile: None ▼

[Add]

IP Address / FQDN	Port	Transport	
<input type="text" value="10.254.150.52"/>	<input type="text" value="5060"/>	TCP ▼	[Delete]

On the Advanced tab:

- Check **Enable Grooming**.
- Select **Swisscom** for Interworking Profile.
- Click **Finish**.

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

- Enable DoS Protection: ☐
- Enable Grooming: ☒
- Interworking Profile:
- Signaling Manipulation Script:
- Securable: ☐
- Enable FGDN: ☐
- TCP Failover Port:
- TLS Failover Port:
- Tolerant: ☐
- URI Group:

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

8.7. Routing

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.

Routing information is required for routing to Session Manager on the internal side and Swisscom address on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

8.7.1. Routing – Avaya

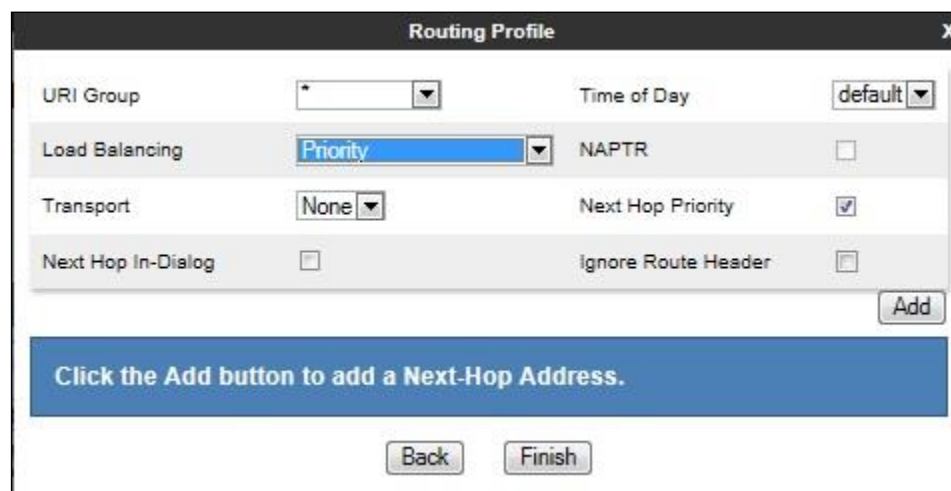
Create a Routing Profile for Session Manager.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



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

The Routing Profile window will open. Use the default values displayed and click **Add**.



The image shows a window titled "Routing Profile" with a close button (X) in the top right corner. The window contains several settings:

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

At the bottom right is an "Add" button. Below the settings is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the very bottom are "Back" and "Finish" buttons.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Avaya (Section 8.6.1)** from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5061(TLS)** from drop down menu.
- Click **Finish**.

URI Group	Time of Day	Load Balancing	NAPTR	Transport	Next Hop Priority	Next Hop In-Dialog	Ignore Route Header	ENUM	ENUM Suffix
*	default	Priority	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Avaya	10.10.3.42:5061 (TLS)	None


8.7.2. Routing – Swisscom Enterprise SIP

Create a Routing Profile for Swisscom SIP network.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

Profile Name:

The Routing Profile window will open. Use the default values displayed and click **Add**.

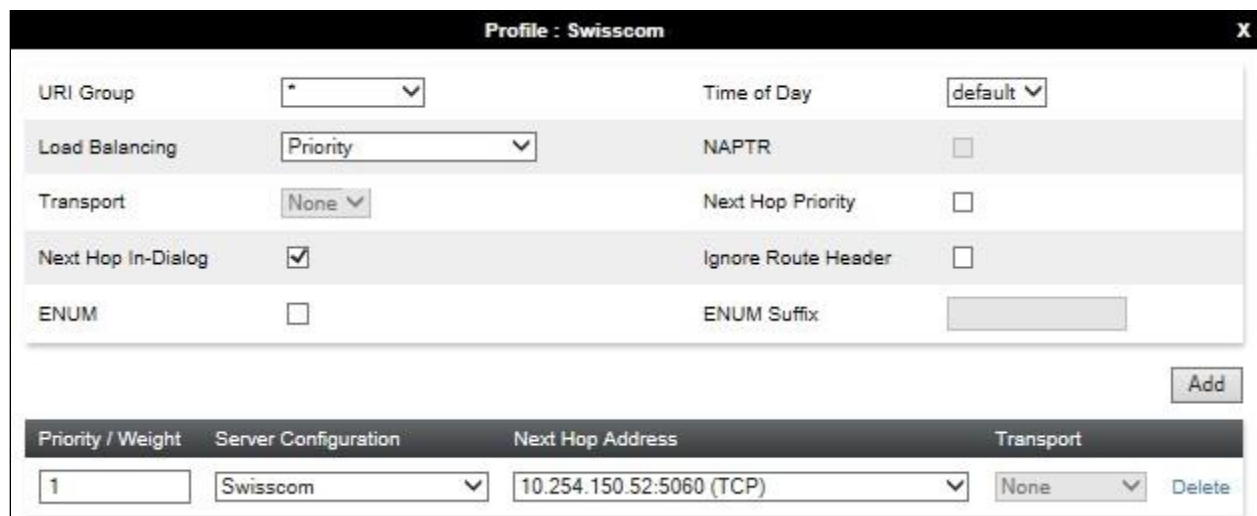


The screenshot shows the 'Routing Profile' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (*) as the selected value.
- Time of Day:** A dropdown menu with 'default' as the selected value.
- Load Balancing:** A dropdown menu with 'Priority' as the selected value.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' as the selected value.
- Next Hop Priority:** A checked checkbox.
- Next Hop In-Dialog:** An unchecked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- Add:** A button located at the bottom right of the configuration area.
- Message:** A blue banner with the text 'Click the Add button to add a Next-Hop Address.'
- Back:** A button at the bottom center.
- Finish:** A button at the bottom right.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Swisscom** (Section 8.6.2) from drop down menu.
- **Next Hop Address = Select 10.254.150.52:5060 (TCP)** from drop down menu.
- Click **Finish**.



The screenshot shows the 'Profile : Swisscom' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (*) as the selected value.
- Time of Day:** A dropdown menu with 'default' as the selected value.
- Load Balancing:** A dropdown menu with 'Priority' as the selected value.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' as the selected value.
- Next Hop In-Dialog:** A checked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- ENUM:** An unchecked checkbox.
- ENUM Suffix:** An empty text field.
- Add:** A button located at the bottom right of the configuration area.
- Table:** A table with the following columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', 'Transport', and 'Delete'.

Priority / Weight	Server Configuration	Next Hop Address	Transport	Delete
1	Swisscom	10.254.150.52:5060 (TCP)	None	Delete

8.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for Session Manager, navigate to **Global Profiles** → **Topology Hiding** from menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Avaya

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Swisscom

Rename Clone Delete

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Swisscom, navigate to **Global Profiles → Topology Hiding** from the menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Swisscom and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Swisscom

Add

RenameCloneDelete

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Swisscom

Click here to add a description.

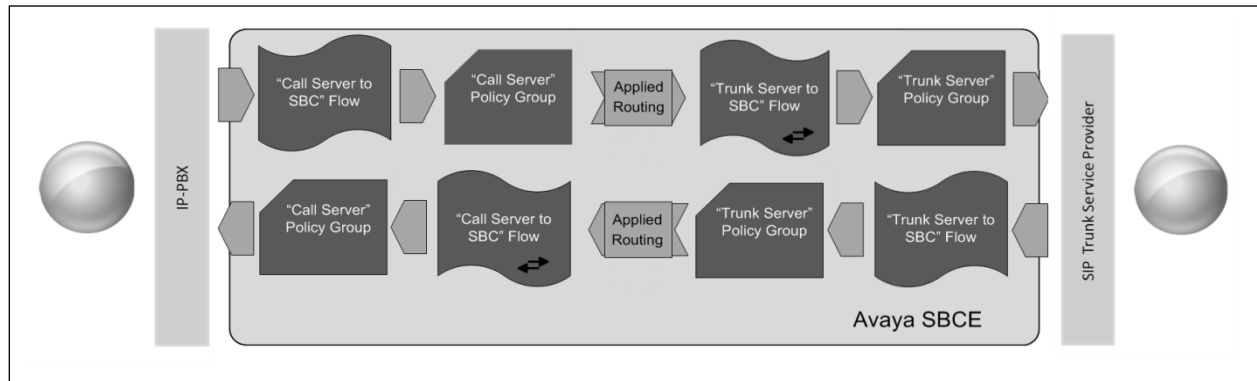
Topology Hiding

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

Edit

8.9. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Swisscom's SIP Trunk and incoming flows from Swisscom's SIP Trunk to Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from Session Manager to the PSTN via the Swisscom network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



The following screenshot shows all configured flows.

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	Swisscom	View	Clone	Edit	Delete

Server Configuration: Swisscom

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server	*	Int_Sig	Ext_Sig	default-low	Avaya	View	Clone	Edit	Delete

To define a Server Flow for the Swisscom SIP Trunk, navigate to **Device Specific Settings** → **End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Swisscom SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Swisscom server configuration defined in **Section 8.6.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 8.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 8.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 8.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 8.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Swisscom SIP Trunk defined in **Section 8.8** and click **Finish** (not shown).

The screenshot shows a configuration window titled "View Flow: Trunk_Server". It is divided into two main sections: "Criteria" and "Profile".

Criteria	
Flow Name	Trunk_Server
Server Configuration	Swisscom
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig

Profile	
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Swisscom
Signaling Manipulation Script	None
Remote Branch Office	Any

To define an incoming server flow for Session Manager from the Swisscom network, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 8.6.1**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 8.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 8.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 8.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Swisscom SIP Trunk defined in **Section 8.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 8.8** and click **Finish** (not shown).

The screenshot shows a dialog box titled "View Flow: Call_Server" with a close button (X) in the top right corner. The dialog is divided into two main sections: "Criteria" and "Profile".

Criteria Section:

Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig

Profile Section:

Signaling Interface	Int_Sig
Media Interface	Int_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Swisscom
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

9. Configure the Swisscom Enterprise SIP Equipment

The configuration of the Swisscom Enterprise SIP equipment used to support the SIP Trunk is outside the scope of these Application Notes and will not be covered. To obtain further information on Swisscom equipment and system configuration please contact an authorised Swisscom representative.

10. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

Session Manager Entity Link Connection Status									
This page displays detailed connection status for all entity links from a Session Manager.									
Status Details for the selected Session Manager:									
All Entity Links for Session Manager: Session Manager									
Summary View									
4 Items Filter: Enable									
SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status	
<input type="radio"/> Avaya SBCE	IPv4	10.10.3.30	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/> Experience Portal	IPv4	10.10.3.50	5060	TCP	FALSE	UP	200 OK	UP	
<input type="radio"/> Communication Manager	IPv4	10.10.3.44	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/> Aura Messaging	IPv4	10.10.2.90	5060	TCP	FALSE	UP	200 OK	UP	
Select : None									

2. From Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

status trunk 2			
TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00011	in-service/idle	no
0002/002	T00012	in-service/idle	no
0002/003	T00013	in-service/idle	no
0002/004	T00014	in-service/idle	no
0002/005	T00015	in-service/idle	no
0002/006	T00016	in-service/idle	no

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left-hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, **1000** is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP03

Devices

GSSCP03

Packet Capture | Captures

Packet Capture Configuration

Status	Ready
Interface	B1 ▾
Local Address <small>IP[:Port]</small>	192.168.37.2 ▾ : <input style="width: 50px;" type="text"/>
Remote Address <small>*, *-Port, IP, IP:Port</small>	<input style="width: 150px;" type="text" value="*"/>
Protocol	UDP ▾
Maximum Number of Packets to Capture	<input style="width: 50px;" type="text" value="1000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input style="width: 150px;" type="text" value="TEST.pcap"/>

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

Trace: GSSCP03

Devices

GSSCP03

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
TEST_20170413141915.pcap	0	April 13, 2017 2:19:52 PM IST	Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response to OPTIONS in the form of a 200 OK will be seen from the Swisscom network.

11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura[®] Communication Manager R8.0, Avaya Aura[®] Session Manager R8.0, Avaya Aura[®] Experience Portal R7.2 and Avaya Session Border Controller for Enterprise R7.2.2 to the Swisscom Enterprise SIP platform. The Swisscom Enterprise SIP Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

12. Additional References

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

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 8.0, Feb 2019.
- [2] *Upgrading and Migrating Avaya Aura® applications to Release 8.0 from System Manager*, Dec 2018.
- [3] *Deploying Avaya Aura® applications from System Manager*, Release 8.0, Dec 2018
- [4] *Deploying Avaya Aura® Communication Manager*, Release 8.0, Feb 2019
- [5] *Administering Avaya Aura® Communication Manager*, Release 8.0, Dec 2018
- [6] *Upgrading Avaya Aura® Communication Manager*, Release 8.0, Dec 2018
- [7] *Deploying Avaya Aura® System Manager Release 8.0*, Feb 2019
- [8] *Upgrading Avaya Aura® System Manager to Release 8.0*, Jan 2019.
- [9] *Administering Avaya Aura® System Manager for Release 8.0*, Jan 2019
- [10] *Deploying Avaya Aura® Session Manager*, Release 8.0 Mar 2019
- [11] *Upgrading Avaya Aura® Session Manager Release 8.0*, Mar 2019
- [12] *Administering Avaya Aura® Session Manager Release 8.0*, Mar 2019
- [13] *Administering Avaya Aura® Experience Portal*, Release 7.2.2, Issue 1, Mar 2019
- [14] *Implementing Avaya Aura® Experience Portal on a single server*, Release 7.2, Mar 2019
- [15] *Deploying Avaya Session Border Controller for Enterprise Release 7.2.2*, Feb 2019
- [16] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018
- [17] *Administering Avaya Session Border Controller for Enterprise Release 7.2.2*, Nov 2018
- [18] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2019 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.