



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R8.0, Avaya Aura® Session Manager R8.0 and Avaya Session Border Controller for Enterprise R7.2.2 to support Colt VoIP Access SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Colt VoIP Access SIP Trunking Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server.

The Colt VoIP Access SIP Trunk Platform provides PSTN access via a SIP trunk connected to the Colt VoIP Access 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.

Colt 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.....	6
4. Equipment and Software Validated	7
5. Configure Avaya Aura® Communication Manager.....	8
5.1. Confirm System Features	8
5.2. Administer IP Node Names.....	9
5.3. Administer IP Network Region.....	10
5.4. Administer IP Codec Set	11
5.5. Administer SIP Signaling Groups	12
5.6. Administer SIP Trunk Groups.....	13
5.7. Administer Calling Party Number Information	15
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.....	24
6.5.1. Avaya Aura® Session Manager SIP Entity	25
6.5.2. Avaya Aura® Communication Manager SIP Entity	26
6.5.3. Avaya Session Border Controller for Enterprise SIP Entity.....	27
6.6. Administer Entity Links	28
6.7. Administer Routing Policies	29
6.8. Administer Dial Patterns	30
7. Configure Avaya Session Border Controller for Enterprise	32
7.1. Access Avaya Session Border Controller for Enterprise	32
7.2. Define Network Management	34
7.3. Define TLS Profiles	37
7.3.1. Certificates	37
7.3.2. Client Profile	38
7.3.3. Server Profile	39
7.4. Define Interfaces	40
7.4.1. Signalling Interfaces	40
7.4.2. Media Interfaces.....	41
7.5. Define Server Interworking.....	42
7.5.1. Server Interworking Avaya.....	42

7.5.2.	Server Interworking – Colt VoIP Access.....	44
7.6.	Define Servers	46
7.6.1.	Server Configuration – Avaya	46
7.6.2.	Server Configuration – Colt VoIP Access	48
7.7.	Routing	50
7.7.1.	Routing – Avaya	50
7.7.2.	Routing – Colt VoIP Access	51
7.8.	Topology Hiding	53
7.9.	Server Flows.....	55
8.	Configure the Colt SIP Trunking Service Equipment	58
9.	Verification Steps.....	58
10.	Conclusion	60
11.	Additional References.....	61

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Colt VoIP Access (Colt) SIP Trunking 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 Session Border Controller for Enterprise R7.2.2 (Avaya SBCE).

Customers using this Avaya SIP-enabled enterprise solution with the Colt VoIP Access SIP Trunking 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 Colt SIP Trunking Service.

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 Colt SIP Trunking Service, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Colt SIP Trunking 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, G.729A and G.726-32K 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 Colt SIP Trunking Service requiring Avaya response and sent by Avaya requiring Colt response.

2.2. Test Results

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

- It was observed during testing that when a call was forwarded to Voicemail that Colt 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 when media negotiation used codec G726A-32K that the voice/sound quality was very poor. G.711A, G.729A and G726A-32K codecs are configured to be used in order of preference so this should not have any negative impact on the SIP trunk if the codecs are configured as per **Section 5.4**.
- No Inbound Toll-Free access available for test.
- No Emergency Services test call booked with Operator.

2.3. Support

For technical support on Colt VoIP Access SIP Trunking Services, contact Colt support at <http://www.vodafone.nl/midden-groot-bedrijf/oplossingen/>.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Colt SIP Trunking Service. Located at the Enterprise site is an Avaya SBCE, 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.

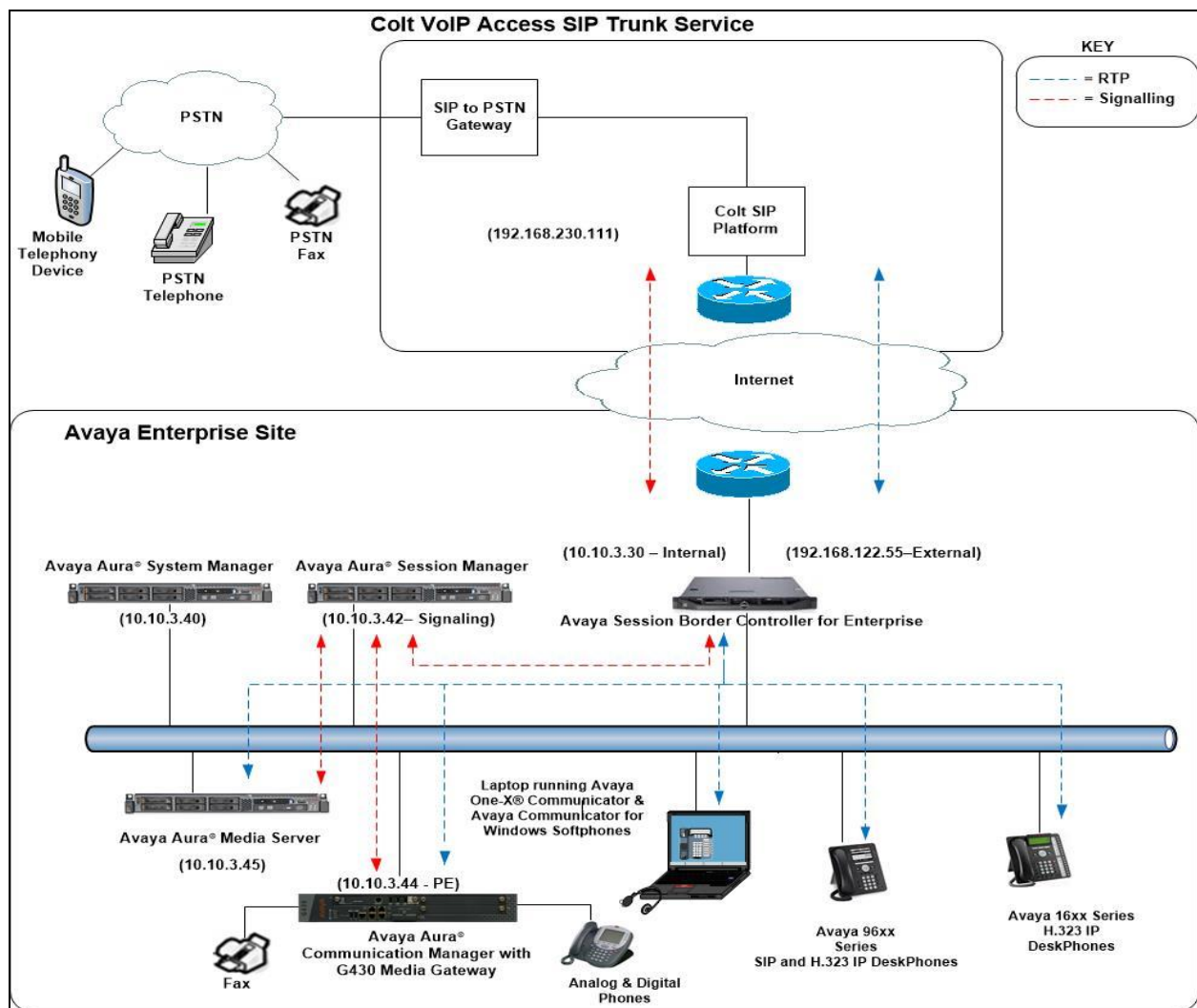


Figure 1: Test Setup Colt VoIP Access SIP Trunking Service to Avaya Enterprise

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	8.0.0.0 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.0.0.098174
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Aura® Communication Manager	00.0.822.0-24826
Avaya Session Border Controller for Enterprise	7.2.2.1-04-16104
Avaya G430 Media Gateway	40.10.0
Avaya Aura® Media Server	v.8.0.0.150
Avaya 1600 IP Deskphone (H.323)	1.3.11
Avaya 96x0 IP DeskPhone (H.323)	6.6
Avaya 9611 IP DeskPhone (SIP)	7.1.1.0
Avaya 9608 IP DeskPhone (SIP)	7.1.1.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.22 -SP12-Patch12
Avaya Equinox™ for Windows	3.4.9 (SP3)
Analogue Handset	N/A
Analogue Fax	N/A
Colt VoIP Access	
Sonus SBC7K	5.1.3R0
Sonus PSX	9.3.2 F1

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 Colt 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 Colt 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 Colt 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 Colt were configured, namely **G.711A**, **G.729A** and **G.726A-32K**.

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.729A	n	2	20
3: G.726A-32k	n	2	20
4:			
5:			
6:			
7:			

Media Encryption

1: none

2:

Encrypted SRTCP: enforce-unenc-srtp

Colt 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	ECM: y	Packet Size (ms)
FAX	t.38-standard	0		
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 Colt 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 **2**).
- 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		Alternate Route Timer(sec): 6

5.6. Administer SIP Trunk Groups

A trunk group is associated with the signaling 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-ntwrk**.
- 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		
Dial Access? n	Night Service:		
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 Colt to prevent unnecessary SIP messages during call setup. During testing, a value of **900** was used that sets Min-SE to 1800 in the SIP signalling.

add trunk-group 2		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in formats other than E.164 with leading “+”. In the test environment numbers were sent in diallable format, i.e. national numbers with a national dialling prefix of “0” and international numbers with an international dialling prefix of “00”.

add trunk-group 2	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private
	UI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no

On **Page 4** of this form:

- Set **Mark Users as Phone** to **n**.
- 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 Colt.
- Set **Always Use re-INVITE for Display Updates** to **n**.
- 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? n
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? n
	Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? y	
Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? n

5.7. Administer Calling Party Number Information

Use the **change private-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.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Trk	Private	Total		
Len Code	Grp(s)	Prefix	Len		
4 6102	1	49xxxxxx20055	13	Total Administered: 5	
4 6010	1	49xxxxxx20056	13	Maximum Entries: 540	
4 6020	1	49xxxxxx20057	13		
4 6104	1	49xxxxxx20058	13		

The public numbering table is used for numbers in E.164 format. Although this format is not used by Colt, the table was populated as entries are required for all extensions in both tables.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Ext	Trk	CPN	Total		
Len Code	Grp(s)	Prefix	CPN		
			Len		
4 6102	1	49xxxxxx20055	13	Total Administered: 4	
4 6010	1	49xxxxxx20056	13	Maximum Entries: 240	
4 6020	1	49xxxxxx20057	13	Note: If an entry applies to	
4 6104	1	49xxxxxx20058	13	a SIP connection to Avaya	
				Aura(R) Session Manager,	
				the resulting number must	
				be a complete E.164 number.	
				Communication Manager	
				automatically inserts	
				a '+' digit in this case.	

5.8. 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 Colt 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	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
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:	y	y	y	y	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 Colt 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 Colt VoIP Access correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers **49xxxxxx20055**, **49xxxxxx20056**, **49xxxxxx20057** and **49xxxxxx20058** 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 Insert Digits				
public-ntwrk	13	49xxxxxx20055		all	6102	
public-ntwrk	13	49xxxxxx20056		all	6010	
public-ntwrk	13	49xxxxxx20057		all	6020	
public-ntwrk	13	49xxxxxx20058		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

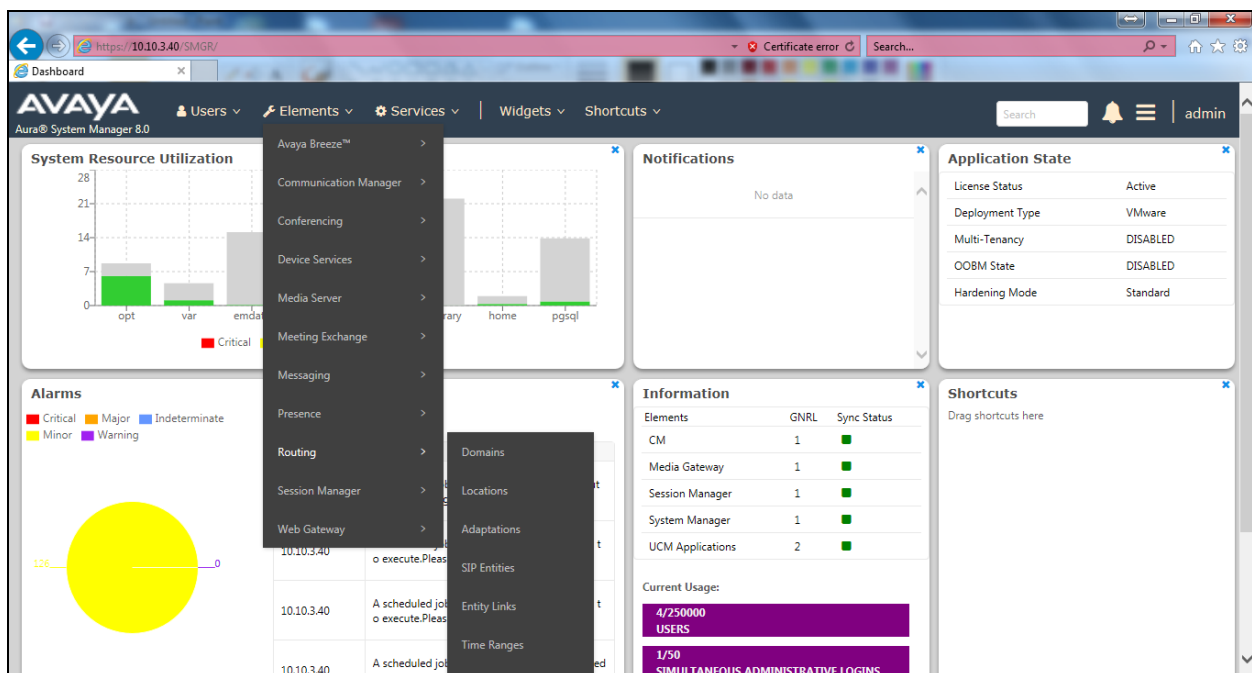
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

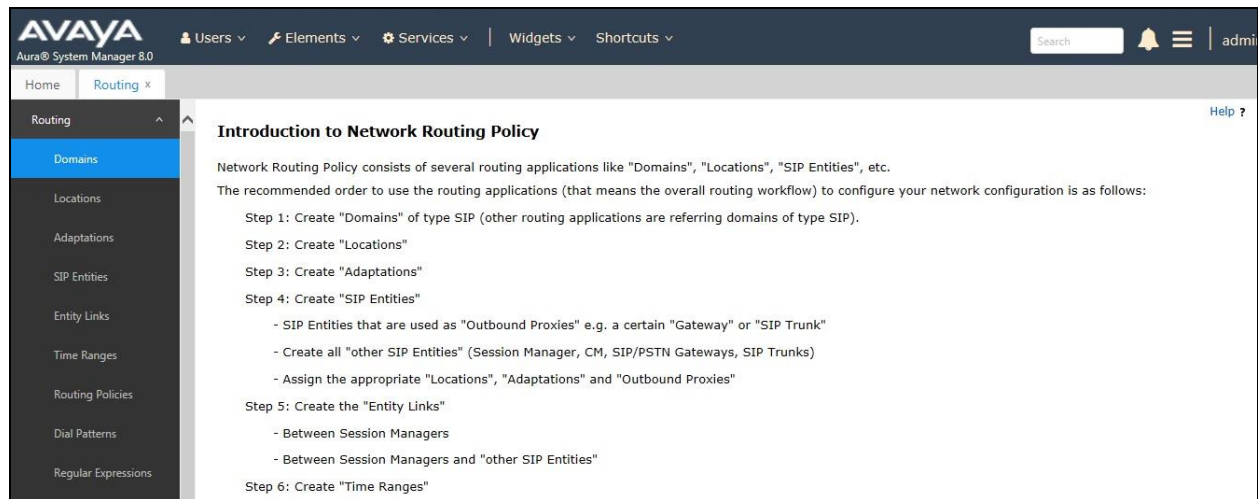
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

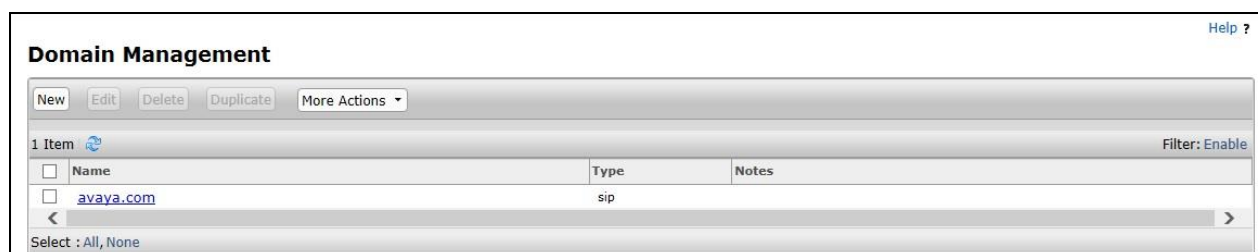


6.2. Administer SIP Domain

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

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**:

- **Adaptation Name:** Enter an appropriate name such as **Colt**.
- **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, Av-Global-Session-ID, P-Location, Endpoint-View,"
<input type="checkbox"/> fromto	true
<input type="checkbox"/> MIME	no

Select : All, None

Egress URI Parameters:

Notes:

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 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 three SIP Entities.

- Session Manager SIP Entity.
- Communication Manager 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

<input type="checkbox"/>	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 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 7.4.1**). 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:Colt

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

Loop Detection Interval (in msec):200

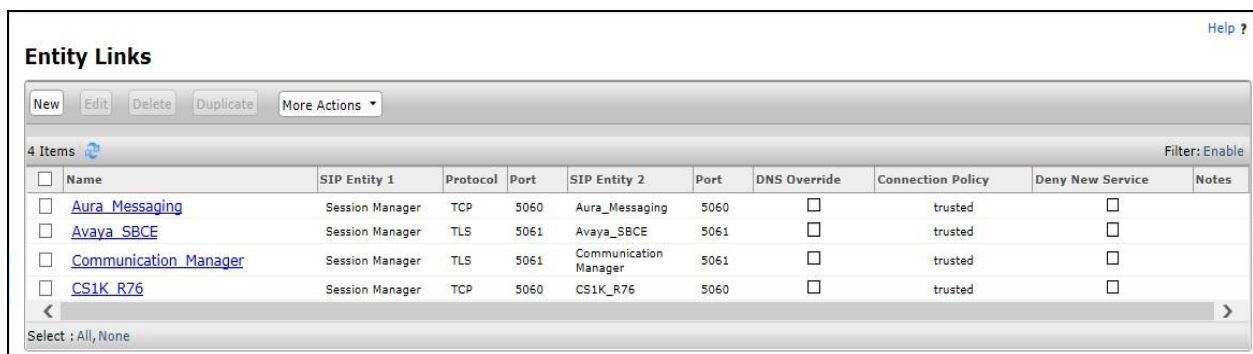
6.6. Administer Entity Links

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	TCP	5060	Aura_Messaging	5060	<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"/>	CS1K_R76	Session Manager	TCP	5060	CS1K_R76	5060	<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 Colt 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

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 Colt SIP Trunk.

Dial Pattern Details

Commit

Cancel

General

* Pattern: 00353

* Min: 5

* Max: 16

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	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

CommitCancel

General

* Pattern:4969

* Min:4

* Max:16

Emergency Call:☐

SIP Domain:avaya.com

Notes:

Originating Locations and Routing Policies

AddRemove

1 ItemFilter: 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

7. Configure Avaya Session Border Controller for Enterprise

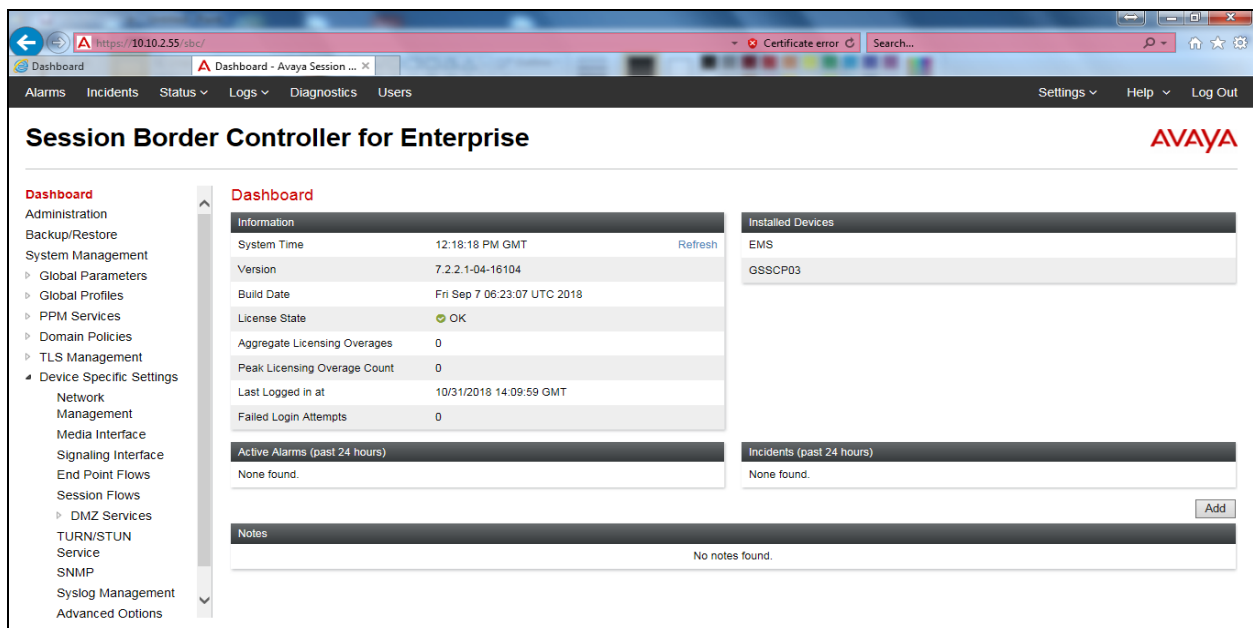
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

7.1. Access Avaya Session Border Controller for Enterprise

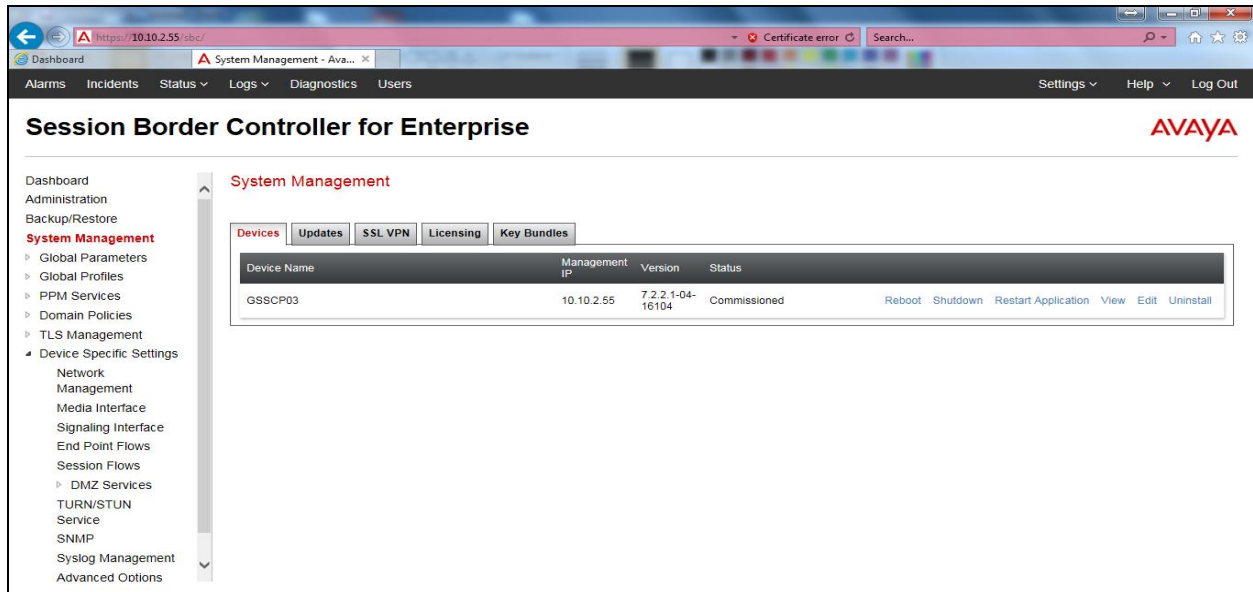
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



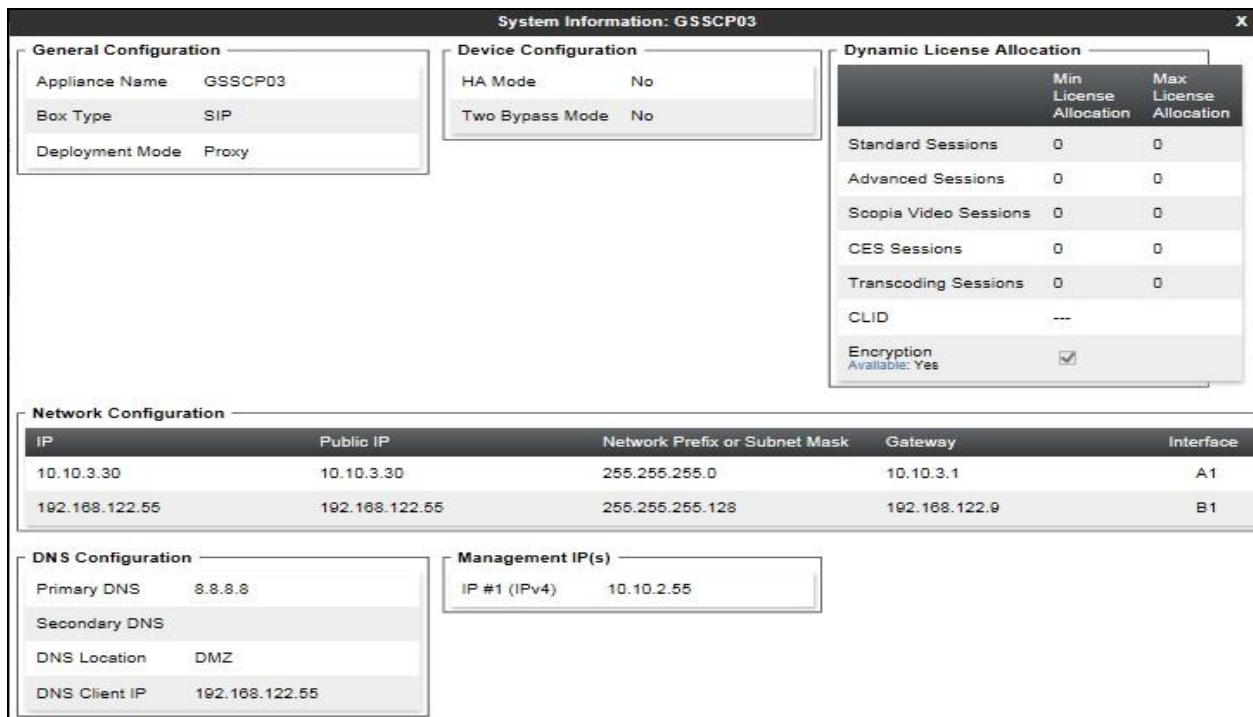
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



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.



7.2. 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 '192.168.122.9'), '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 fields is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The first row contains the values '192.168.122.55', 'Use IP Address', and 'Use Default'. A 'Delete' button is located to the right of the first row. At the bottom of the window is a 'Finish' button.

IP Address	Public IP	Gateway Override
192.168.122.55	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	Edit	Delete
A1_Internal	10.10.3.1	255.255.255.0	A1	10.10.3.30	Edit	Delete
B1_External	192.168.122.9	255.255.255.128	B1	192.168.122.55	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.

Network Management: GSSCP03

Devices
GSSCP03

Interfaces Networks

Add VLAN

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.

7.3. Define TLS Profiles

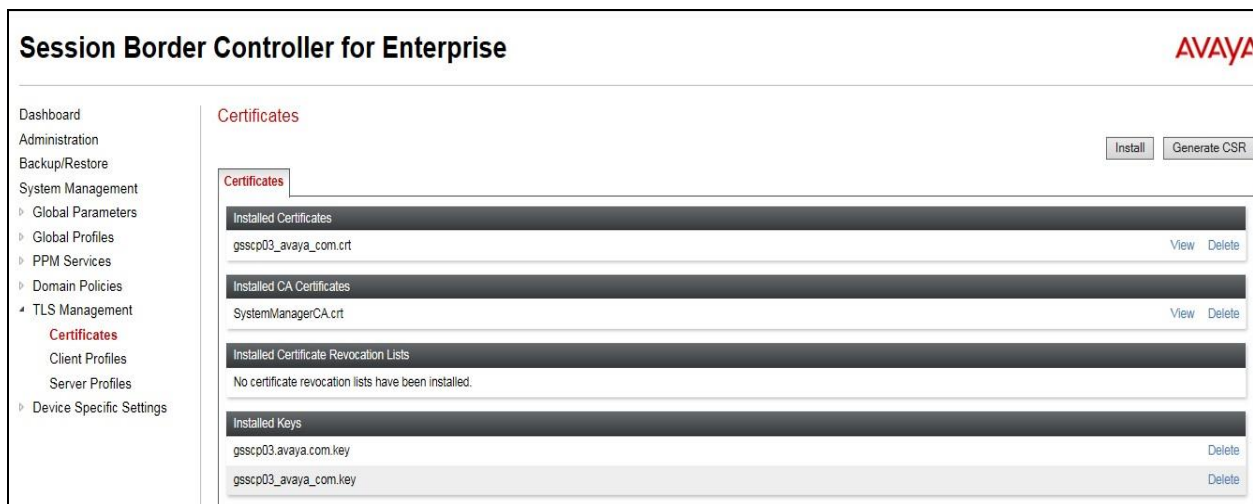
For the compliance test, TLS transport is used for signalling on the SIP trunk between Session Manager and the Avaya SBCE. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these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

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

7.3.1. 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**.



7.3.2. 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 a web-based configuration interface for Client Profiles. The title bar reads "Client Profiles: GSSCP_Client". On the left, a sidebar lists "Client Profiles" with "GSSCP_Client" selected. The main area contains a "Client Profile" form. The form is divided into several sections: "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: ☐), "Renegotiation Parameters" (Renegotiation Time: 0, Renegotiation Byte Count: 0), and "Handshake Options" (Version: ☒ TLS 1.2 ☒ TLS 1.1 ☒ TLS 1.0). Buttons for "Add" and "Delete" are visible at the top of the sidebar.

Client Profile	
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

7.3.3. 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 shows the 'Server Profiles: Gsscp_Server' configuration window. On the left is a sidebar with 'Server Profiles' and 'Gsscp_Server' (selected). The main area has a blue header with 'Click here to add a description.' and a 'Delete' button. Below is the 'Server Profile' configuration table:

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

7.4. Define Interfaces

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

7.4.1. 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 7.2**.
- Select **TLS** port number, **5061** is used for Session Manager.
- Select a **TLS Profile** defined in **Section 7.3.3** 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 7.2**.
- Select **UDP** port number, **5060** is used for the Colt 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	
Ext_Sig	192.168.122.55 B1_External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Int_Sig	10.10.3.30 A1_Internal (A1, VLAN 0)	5060	---	5061	Gsscp_Server	Edit Delete

7.4.2. 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 7.2**.
- 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 7.2**.
- 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	192.168.122.55 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete
Int_Media	10.10.3.30 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete

7.5. Define Server Interworking

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

7.5.1. 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' tab of a configuration window. It contains various settings for SIP server interworking. The 'Hold Support' section has three radio buttons: 'None' (selected), 'RFC2543 - c=0.0.0.0', and 'RFC3284 - s=sendonly'. Below this are four rows for '180 Handling', '181 Handling', '182 Handling', and '183 Handling', each with three radio buttons: 'None' (selected), 'SDP', and 'No SDP'. There are checkboxes for 'Refer Handling', 'Send Hold', 'Delayed Offer', '3xx Handling', 'Diversion Header Support', 'Delayed SDP Handling', 'Re-Invite Handling', 'Prack Handling', and 'Allow 18X SDP'. A 'URI Group' dropdown menu is set to 'None'. The 'T.38 Support' checkbox is checked. The 'URI Scheme' section has three radio buttons: 'SIP' (selected), 'TEL', and 'ANY'. The 'Via Header Format' section has two radio buttons: 'RFC3281' (selected) and 'RFC2543'.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - s=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 ▼
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"/> RFC3281 <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	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
Extensions	Avaya ▼
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None ▼
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP Notify <input type="radio"/> RFC 2833 Relay & SIP Notify <input type="radio"/> SIP Info <input type="radio"/> RFC 2833 Relay & SIP Info <input type="radio"/> Inband
<input type="button" value="Finish"/>	

7.5.2. Server Interworking – Colt VoIP Access

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 Colt 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.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - 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 ▾
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"/> RFC3281 <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

7.6. Define Servers

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

7.6.1. 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 [X]

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	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

Finish

7.6.2. Server Configuration – Colt VoIP Access

To define the Colt 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 **192.168.230.111** (Colt SIP Network).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- 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
192.168.230.111	5060	UDP ▼

[Delete]

On the Advanced tab:

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

The screenshot shows a dialog box titled "Server Configuration Profile - Advanced". It contains the following settings:

Option	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Colt
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

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

7.7. 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 Colt 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.

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

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

Below the settings is an "Add" button. At the bottom of the window, there is a blue banner with the text "Click the Add button to add a Next-Hop Address." and two buttons: "Back" and "Finish".

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

- **Priority/Weight = 1.**
- **Server Configuration = Avaya** (Section 7.6.1) 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

7.7.2. Routing – Colt VoIP Access

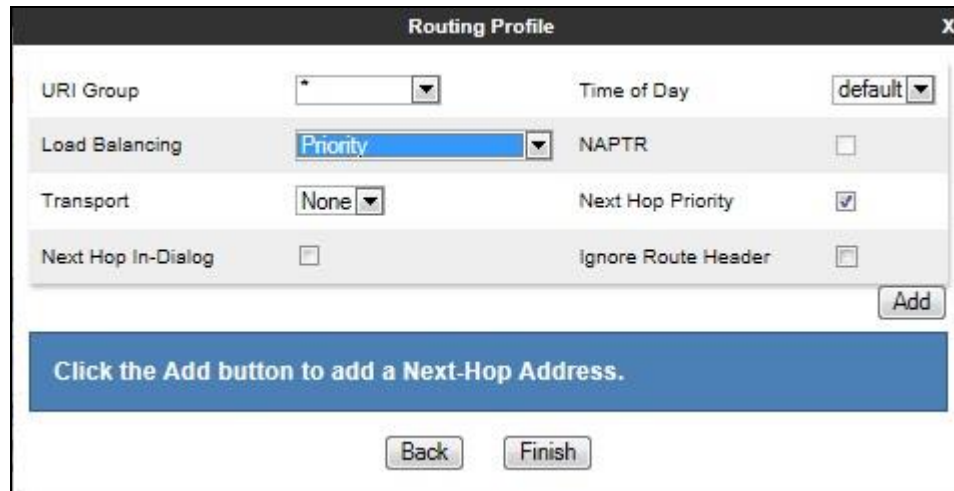
Create a Routing Profile for Colt SIP network.

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

Profile Name: Colt

Next

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

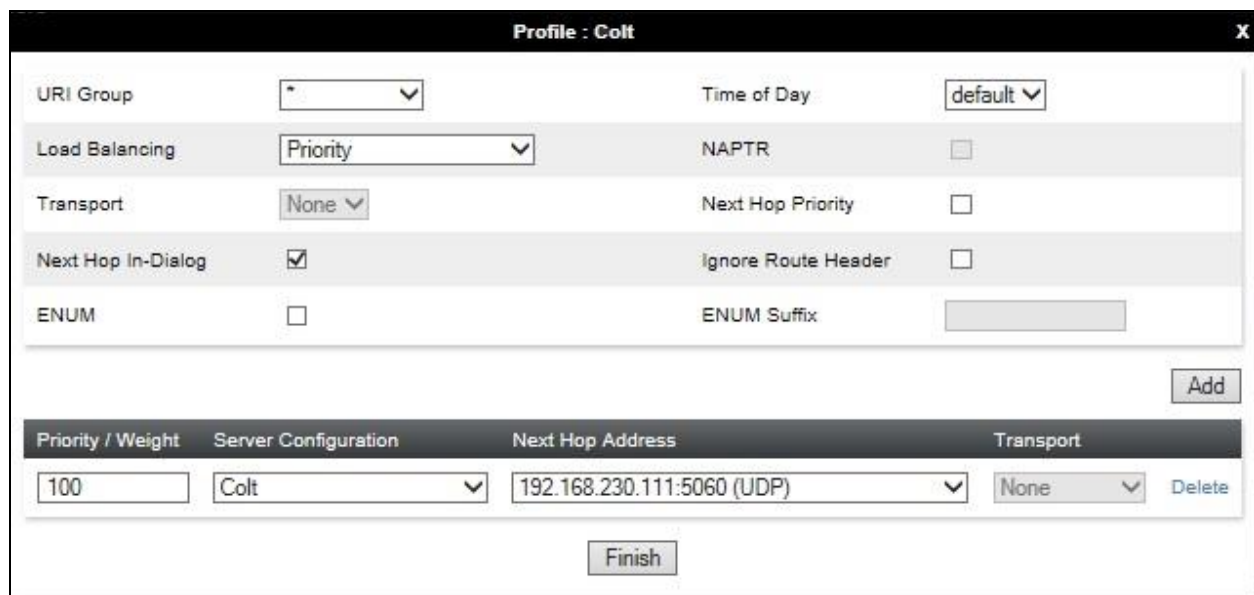


The screenshot shows the 'Routing Profile' window. It contains the following fields and controls:

- 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.
- Instructional Bar:** A blue bar with the text 'Click the Add button to add a Next-Hop Address.'
- Back:** A button at the bottom left.
- Finish:** A button at the bottom right.

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

- **Priority/Weight = 1.**
- **Server Configuration = Colt** (Section 7.6.2) from drop down menu.
- **Next Hop Address = Select 192.168.230.111:5060(UDP)** from drop down menu.
- Click **Finish**.



The screenshot shows the 'Profile : Colt' 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 input 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', and 'Transport'.

Priority / Weight	Server Configuration	Next Hop Address	Transport
100	Colt	192.168.230.111:5060 (UDP)	None
- Delete:** A button next to the table row.
- Finish:** A button at the bottom center.

7.8. 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

Colt

RenameCloneDelete

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Colt, 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 Colt 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: Colt

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Colt

Rename
Clone
Delete

Click here to add a description.

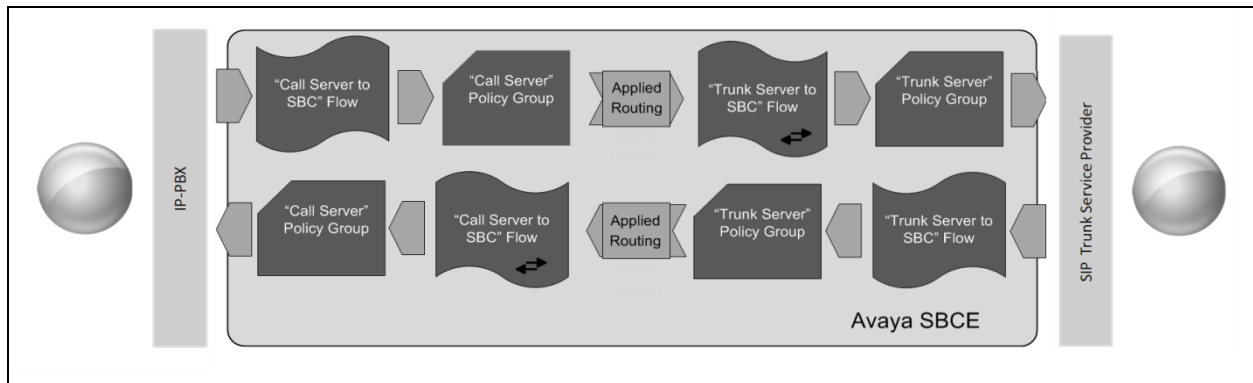
Topology Hiding

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

Edit

7.9. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Colt's SIP Trunk and incoming flows from Colt'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 Colt network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Colt SIP Trunk service and vice versa. 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	Colt	View Clone Edit Delete

Server Configuration: Colt

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 Colt 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 Colt SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Colt server configuration defined in **Section 7.6.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- 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 7.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Colt SIP Trunk defined in **Section 7.8** and click **Finish** (not shown).

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

Criteria Section:

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

Profile Section:

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

To define an incoming server flow for Session Manager from the Colt 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 7.6.1**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- 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 Colt SIP Trunk defined in **Section 7.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish** (not shown).

Flow: Call_Server

Criteria

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

Profile

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

8. Configure the Colt VoIP Access SIP Trunking Service Equipment

The configuration of the Colt VoIP Access 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 Colt equipment and system configuration please contact an authorised Colt representative.

9. 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									
5 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 Fixed	IPv4	10.10.3.30	5061	TLS	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
<input type="radio"/>	CS1K R76	IPv4	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya SBCE Mobile	IPv4	10.10.3.35	5061	TLS	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

IP:Port

192.168.37.2

Remote Address

*:Port, IP, IP:Port

*

Protocol

UDP

Maximum Number of Packets to Capture

1000

Capture Filename

Using the name of an existing capture will overwrite it.

TEST.pcap

Start Capture

Clear

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

The screenshot shows a web-based configuration interface for packet capture. On the left, a sidebar lists 'Devices' with 'GSSCP03' selected. The main area has two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' section includes the following fields:

Packet Capture Configuration	
Status	Ready
Interface	B1
Local Address <small>IP[:Port]</small>	192.168.37.2
Remote Address <small>*.*.Port, IP, IP:Port</small>	*
Protocol	UDP
Maximum Number of Packets to Capture	1000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	TEST.pcap
<div>Start Capture Clear</div>	

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 Colt network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura[®] Communication Manager R8.0, Avaya Aura[®] Session Manager 8.0 and Avaya Session Border Controller for Enterprise R7.2.2 to the Colt One Access SIP Trunking Service. The Colt One Access SIP Trunking 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**.

11. 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, Aug 2018.
- [2] *Upgrading and Migrating Avaya Aura® applications to Release 8.0 from System Manager*, Aug 2018.
- [3] *Deploying Avaya Aura® applications from System Manager*, Release 8.0, Jul 2018
- [4] *Deploying Avaya Aura® Communication Manager*, Release 8.0, Aug 2018
- [5] *Administering Avaya Aura® Communication Manager*, Release 8.0, Aug 2018.
- [6] *Upgrading Avaya Aura® Communication Manager*, Release 8.0, Jul 2018
- [7] *Deploying Avaya Aura® System Manager Release 8.0*, Jul 2018
- [8] *Upgrading Avaya Aura® System Manager to Release 8.0*, Jul 2018.
- [9] *Administering Avaya Aura® System Manager for Release 8.0*, Jul 2018
- [10] *Deploying Avaya Aura® Session Manager*, Release 8.0 Jul 2018
- [11] *Upgrading Avaya Aura® Session Manager Release 8.0*, Jul 2018
- [12] *Administering Avaya Aura® Session Manager Release 8.0*, Jul 2018,
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018
- [15] *Administering Avaya Session Border Controller for Enterprise Release 7.2.2*, Jun 2018
- [16] *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.