



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.1 as an Evolution Server, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to support Vodafone UK SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Vodafone UK SIP Trunk 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. Vodafone UK is a member of the DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Vodafone UK's SIP Trunk service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Customers using this Avaya SIP-enabled enterprise solution with Vodafone UK SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. 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 use the SIP trunking service provided by Vodafone UK. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note 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.

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

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

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analogue telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analogue telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- 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 G.711 pass-through transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Inbound and outbound PSTN calls to/from Avaya One-X Communicator and Avaya Equinox for Windows softphone clients.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the test configuration was completed with successful results for Vodafone UK's SIP Trunk service with the following observations:

- T.38 fax transmission is not supported by Vodafone UK.
- Outbound G.711 pass-through fax calls failed when G.729 was selected as the priority codec as Vodafone UK failed to negotiate to G.711A once the fax call was answered. In order for G.711 pass-through fax to work correctly, please ensure G.711A is set as the priority codec as per **Section 5.4**.
- 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 (AURORA-12076).
- EC500 features such as on-net and off-net calling were not tested as the From Header CLID containing the EC500 mobility number on inbound calls to VF UK SIP Trunk service was automatically changed by VF UK to a CLID number recognizable to the VF UK network.
- All unwanted Avaya proprietary SIP headers and MIME was stripped on outbound calls using the Adaptation Module in Session Manager.
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked with the Emergency Services 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 Vodafone products described in these Application Notes, please visit the website at <http://www.vodafone.co.uk/business/business-solutions/unified-communications/index.htm> or contact an authorized Vodafone representative.

3. Reference Configuration

The following equipment in **Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Vodafone UK SIP Trunk 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 Avaya one-X® Communicator and Avaya Equinox for Windows soft phones running on a laptop PC.

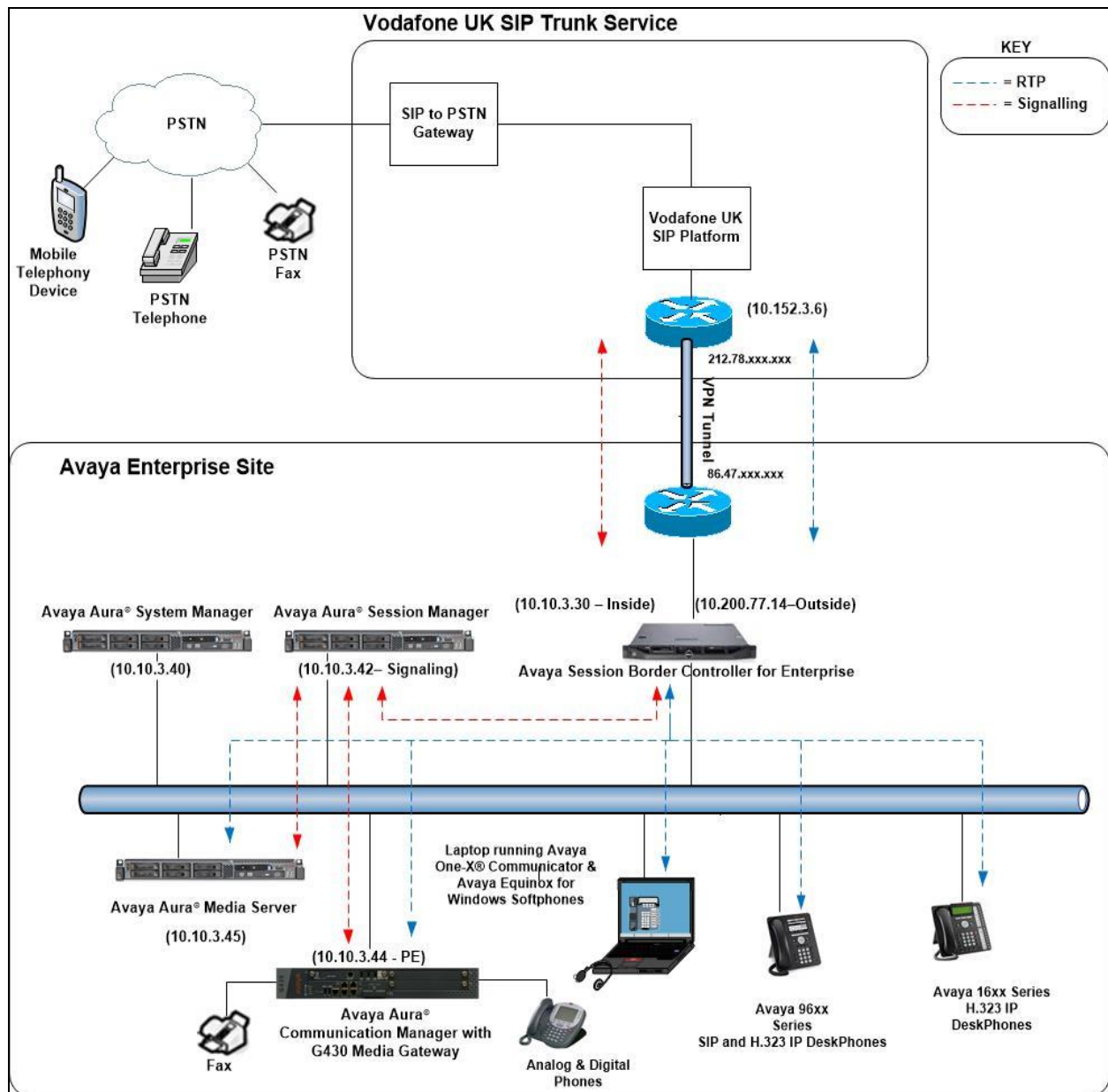


Figure 1: Test Setup Vodafone UK SIP Trunk Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running System Manager on VM Version 8	7.0.2.0. Build No. – 7.1.0.0.1125193 Software Update Revision No: 7.1.2.0.057353 FP2
Dell PowerEdge R620 running Session Manager on VM Version 8	7.0.2.0.712004
Avaya S8300D Server running Avaya Aura® Communication Manager	R017x.01.0.532.0 (24184)
Avaya G430 Media Gateway	7.1 (g430_sw_38_21.0)
Avaya Aura® Media Server	7.8.0.333
Avaya Session Border Controller for Enterprise	7.2.1-05-14222
Avaya 1600 IP Deskphone (H.323)	1.3.11
Avaya 9670 IP DeskPhone (H.323)	6.6
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 9621 IP DeskPhone (SIP)	7.1.1.0
Avaya 9608 IP DeskPhone (SIP)	7.1.1.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.04-FP12
Avaya Equinox for Windows	3.3.1.60
Analogue Handset	N/A
Analogue Fax	N/A
Vodafone UK	
SBC	ACME Packet Net-Net 9200 Version-SD7.2.0 MR-3 Patch 8 (build 209)
Softswitch	Genband C20, R19-19.0.4.0 (MCP 19.0.4.0)

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 Vodafone UK SIP trunk. 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. Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Vodafone UK 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 Vodafone UK SIP network, and any other SIP trunks used.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	0	
Maximum Concurrently Registered IP Stations:		18000	3	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		414	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		41000	0	
Maximum Video Capable IP Softphones:		18000	0	
Maximum Administered SIP Trunks:		4000	10	
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	

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

display system-parameters customer-options		Page 5 of 11
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, **SM100** and **10.10.3.42** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name 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	
SM100	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 x** command where x is the desired network-region to 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, 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 **1** 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: 1
    Location: 1          Authoritative Domain: avaya.com
        Name: default      Stub Network Region: n
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
    Codec Set: 1          Inter-region IP-IP Direct Audio: yes
        UDP Port Min: 2048                IP Audio Hairpinning? n
        UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5
H.323 IP ENDPOINTS          AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 Link Bounce Recovery? y                RSVP Enabled? n
    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**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec supported by Vodafone UK was 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 to provide a work around for the RTP to SRTP conversion issue described in **Section 2.2**.

change ip-codec-set 1		Page 1 of 2	
IP MEDIA PARAMETERS			
Codec Set: 1			
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 SRTP: best-effort	
1: none			

Vodafone UK SIP Trunk Service supports G.711 pass-through for transmission of fax. Navigate to **Page 2** and define fax properties as follows:

- Set the **FAX - Mode** to **pass-through**.

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

5.5. Administer SIP Signalling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Vodafone UK 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 (node name **SM** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5061** (Commonly used TLS port value).
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**.
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set **Initial IP-IP Direct Media** to **n**.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).
- Set **H.323 Station Outgoing Direct Media** to **y**.

The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? y	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? y	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

5.6. Administer SIP Trunk Group

A trunk group is associated with the signalling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. 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 Vodafone UK to prevent unnecessary SIP messages during call setup. During the compliance testing, **Preferred Minimum Session Refresh Interval (sec)** was set to **900**.

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): 900			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	
Caller ID for Service Link Call to H.323 1xC: station-extension			

On **Page 3**, set the **Numbering Format** field to **private**.

add trunk-group 1		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		
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** to match the value preferred by Vodafone UK.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- Set the **Identity for Calling Party Display** to **P-Asserted-Identity**.

PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? y	
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	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	

5.7. Administer Calling Party Number Information

Use the **change private-numbering x** command to configure Communication Manager to send the calling party number in the format required. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

change private-numbering					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
4	6010	1	149xxxxx27	10	Total Administered: 4
4	6020	1	149xxxxx28	10	Maximum Entries: 540
4	6102	1	149xxxxx26	10	
4	6104	1	149xxxxx29	10	

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 Vodafone UK's SIP trunk. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. 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		Total		Route	Call	Node	ANI
String		Min	Max	Pattern	Type	Num	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:	y	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 Vodafone UK 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 Vodafone UK correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers **14xxxxxx26**, **14xxxxxx27**, **14xxxxxx28**, **14xxxxxx29** and **14xxxxxx30** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DDI numbers have been masked for security purposes.

change inc-call-handling-trmt trunk-group 1				Page 1 of 3	
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del Insert		
public-ntwrk	10	14xxxxxx26	all	6010	
public-ntwrk	10	14xxxxxx27	all	6020	
public-ntwrk	10	14xxxxxx28	all	6030	
public-ntwrk	10	14xxxxxx29	all	6100	
public-ntwrk	10	14xxxxxx30	all	6102	

5.10. EC500 Configuration

When EC500 is enabled on the 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 the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- For the **Phone Number** enter the phone that will also be called (e.g.**0035389434xxxx**).
- Set the **Trunk Selection** to **1** so that Trunk Group 1 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	1	1		
-								

Note: The phone number shown is for a mobile phone used for testing at Avaya Labs and is in international format. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

Save Communication Manager changes by entering **save translation** to make them permanent.

6. Configuring Avaya Aura® Session Manager

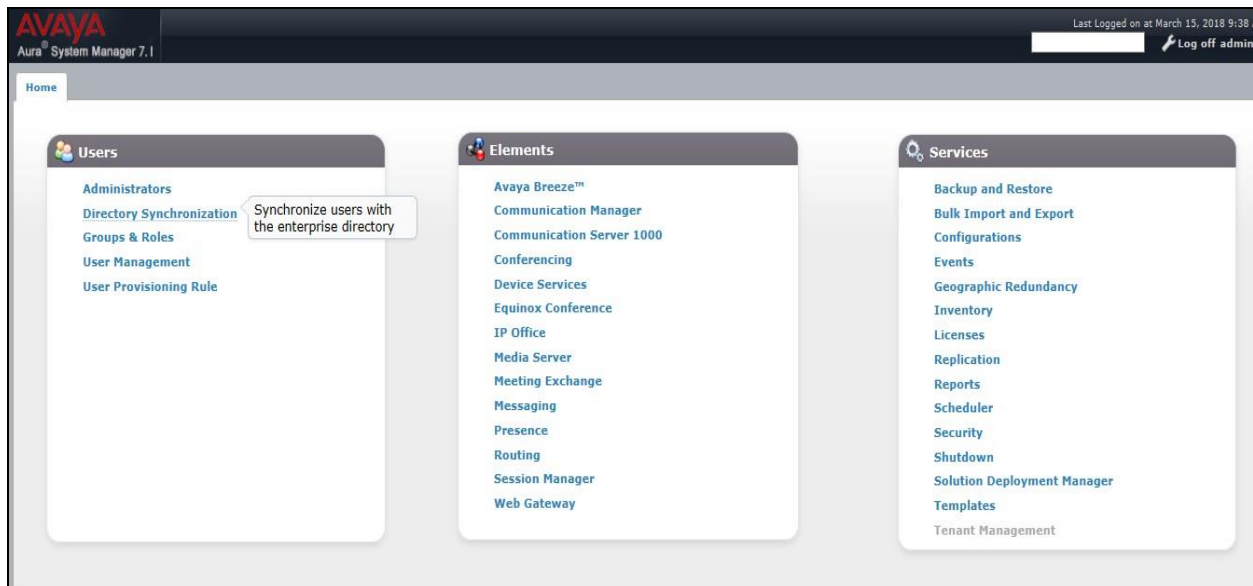
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

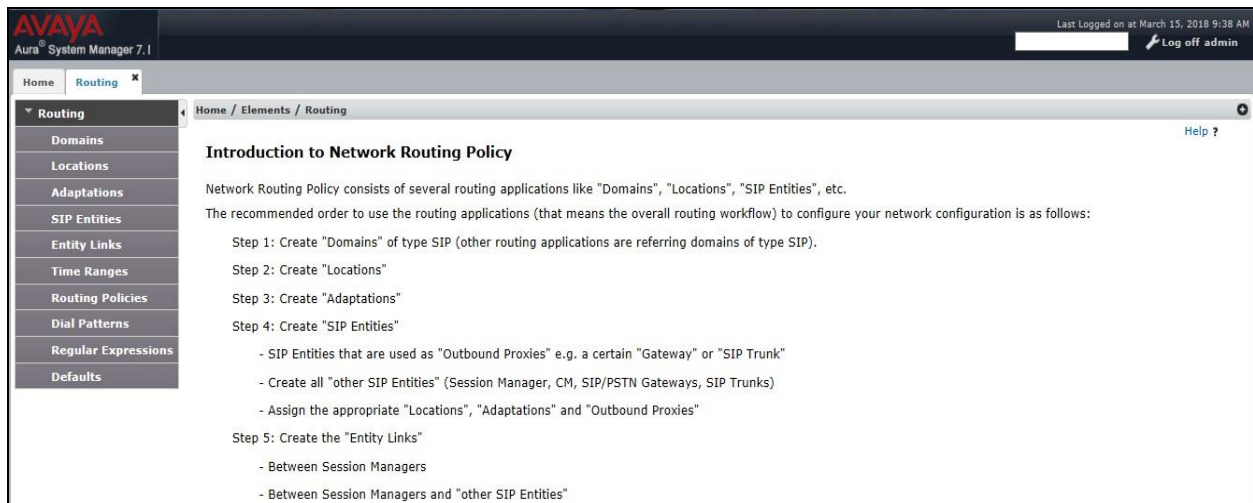
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session 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 by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** 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.

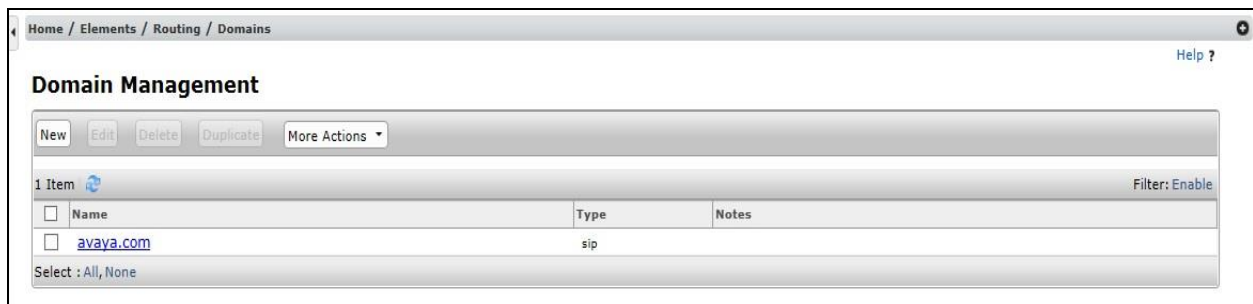


6.2. Administer SIP Domain

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_7** defined for the compliance testing.

The screenshot displays the Avaya Session Manager Administration console. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Locations'. The main title is 'Location Details', with 'Commit' and 'Cancel' buttons to its right. A 'Help ?' link is in the top right corner.

The 'General' section contains the following fields:

- Name:** SMGR_7
- Notes:** (empty text area)

The 'Dial Plan Transparency in Survivable Mode' section contains:

- Enabled:** ☐
- Listed Directory Number:** (empty text field)
- Associated CM SIP Entity:** (empty text field)

The 'Overall Managed Bandwidth' section contains:

- Managed Bandwidth Units:** Kbit/sec (dropdown menu)
- Total Bandwidth:** (empty text field)
- Multimedia Bandwidth:** (empty text field)
- Audio Calls Can Take Multimedia Bandwidth:** ☒

The 'Location Pattern' section is below, featuring an 'Add' button and a 'Remove' button. It shows a table with 3 items. The table has columns for 'IP Address Pattern' and 'Notes'. The first item is selected, and its pattern is '*10.10.3.*'. The other two items are '*10.10.4.*' and '*10.10.9.*'. A 'Filter: Enable' link is on the right. At the bottom of the table is a 'Select : All, None' link. 'Commit' and 'Cancel' buttons are at the bottom right of the section.

IP Address Pattern	Notes
10.10.3.	
10.10.4.	
10.10.9.	

6.4. Administer Adaptations

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 7.0 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements

For the compliance test, an Adaptation named “**VFUK**” 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**:

- **Adaption Name:** Enter an appropriate name such as **VFUK**.
- **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**.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

* Adaption Name: VFUK

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, P-Location
fromto	true
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 Entity.
- 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.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The page has 'Commit' and 'Cancel' buttons at the top right. The 'General' tab is active. The configuration fields are as follows:

- Name:** Session Manager
- FQDN or IP Address:** 10.10.3.42
- Type:** Session Manager (dropdown)
- Notes:** (empty text field)
- Location:** SMGR_7 (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text field)

The 'Monitoring' tab is also visible, showing:

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

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.

The screenshot shows the 'Listen Ports' configuration section. It includes fields for 'TCP Failover port' and 'TLS Failover port'. Below these is a table with 3 items. The table has columns for 'Listen Ports', 'Protocol', 'Default Domain', and 'Notes'. The data rows are as follows:

Listen Ports	Protocol	Default Domain	Notes
5060	TCP	avaya.com	
5060	UDP	avaya.com	
5061	TLS	avaya.com	

At the bottom, there is a 'Select : All, None' option.

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. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling and **Type** is **CM**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

The screenshot displays the 'SIP Entity Details' configuration page in the Avaya Aura Communication Manager interface. The page has a breadcrumb trail at the top: 'Home / Elements / Routing / SIP Entities'. On the right side, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The main title is 'SIP Entity Details'. Below the title, there is a 'General' tab. The form contains the following fields and values:

- Name:** Communication_Manager
- FQDN or IP Address:** 10.10.3.44
- Type:** CM (dropdown menu)
- Notes:** (empty text box)
- Adaptation:** (empty dropdown menu)
- Location:** SMGR_7 (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown menu)
- Credential name:** (empty text box)
- Securable:** ☐
- Call Detail Recording:** none (dropdown menu)
- Loop Detection Mode:** On (dropdown menu)
- Loop Count Threshold:** 5

At the bottom left, there is a 'Loop Detection' section with the same two fields as above.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set **Type** to **SIP Trunk**. Set **Adaptation** to the adaptation defined in **Section 6.4**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details" with "Commit" and "Cancel" buttons. A "Help ?" link is in the top right. The "General" tab is selected. The form contains the following fields:

- Name:** Avaya_SBCE
- FQDN or IP Address:** 10.10.3.35
- Type:** SIP Trunk (dropdown)
- Notes:** (empty text area)
- Adaptation:** VFUK (dropdown)
- Location:** SMGR_7 (dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress (dropdown)
- Loop Detection Mode:** On (dropdown)
- 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.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<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"/>	

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 Communication Manager.

The screenshot shows the 'Routing Policy Details' form in a web application. The breadcrumb trail is 'Home / Elements / Routing / Routing Policies'. The form has a 'Commit' button and a 'Cancel' button. The 'General' section contains fields for 'Name' (to_Communication_Manager), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with one row: 'Communication_Manager' with FQDN or IP Address '10.10.3.44' and Type 'CM'. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows '1 Item' and a table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The table has one row with Ranking '0', Name '24/7', and checkboxes for all days of the week. The Start Time is '00:00' and the End Time is '23:59'. The Notes field contains 'Time Range 24/7'. At the bottom, there is a 'Select : All, None' option.

Home / Elements / Routing / Routing Policies

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
<input type="checkbox"/> 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 the Avaya SBCE.

The screenshot shows the 'Routing Policy Details' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Routing Policies'. Below this, the title 'Routing Policy Details' is followed by 'Commit' and 'Cancel' buttons. A 'Help ?' link is in the top right corner. The 'General' section contains fields for 'Name' (set to 'to_Avaya_SBCE'), 'Disabled' (checkbox), 'Retries' (set to 0), and 'Notes'. The 'SIP Entity as Destination' section features a 'Select' dropdown and a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one entry: 'Avaya_SBCE', '10.10.3.35', 'SIP Trunk'. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows '1 Item' and a 'Filter: Enable' option. Below is a table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The table has one row: Ranking 0, Name 24/7, with checkboxes for all days of the week, Start Time 00:00, End Time 23:59, and Notes 'Time Range 24/7'. At the bottom, it says 'Select : All, None'.

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

* Name: to_Avaya_SBCE

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE	10.10.3.35	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 Avaya SBCE.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details

Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

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_7		to_Avaya_SBCE	0	<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

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

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details

Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

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_7		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.

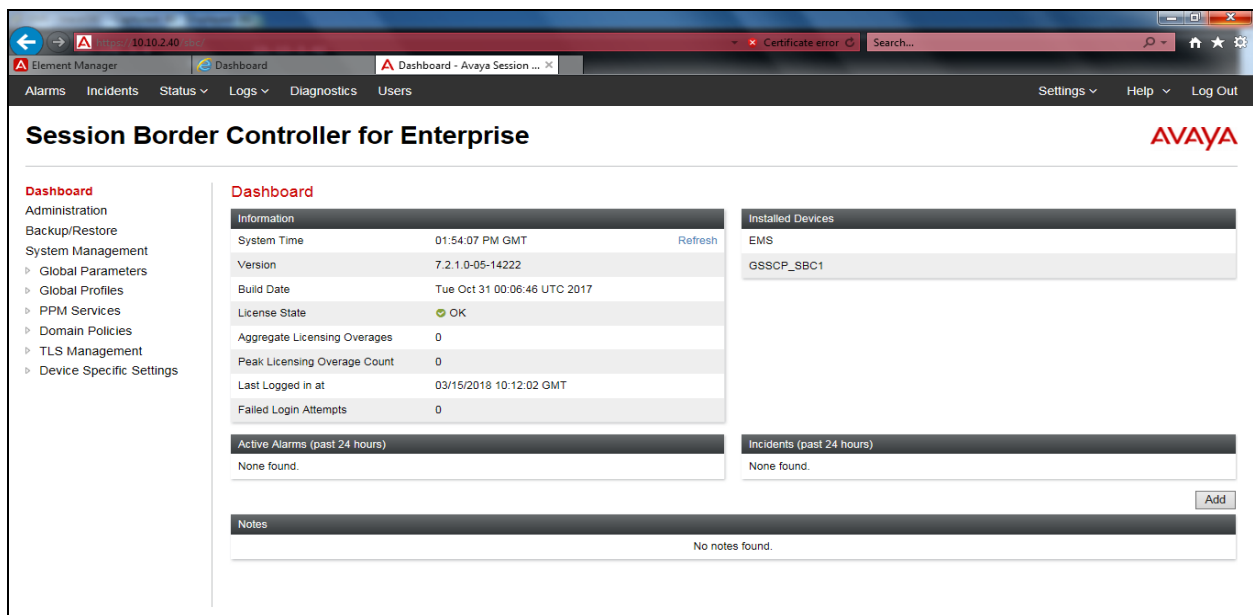
7.1. Accessing Avaya Session Border Controller for Enterprise

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**.



The login page features the Avaya logo and the text "Session Border Controller for Enterprise". On the right, there is a "Log In" section with a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a warning about unauthorized access, a consent statement, and a copyright notice: "© 2011 - 2017 Avaya Inc. All rights reserved."

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.

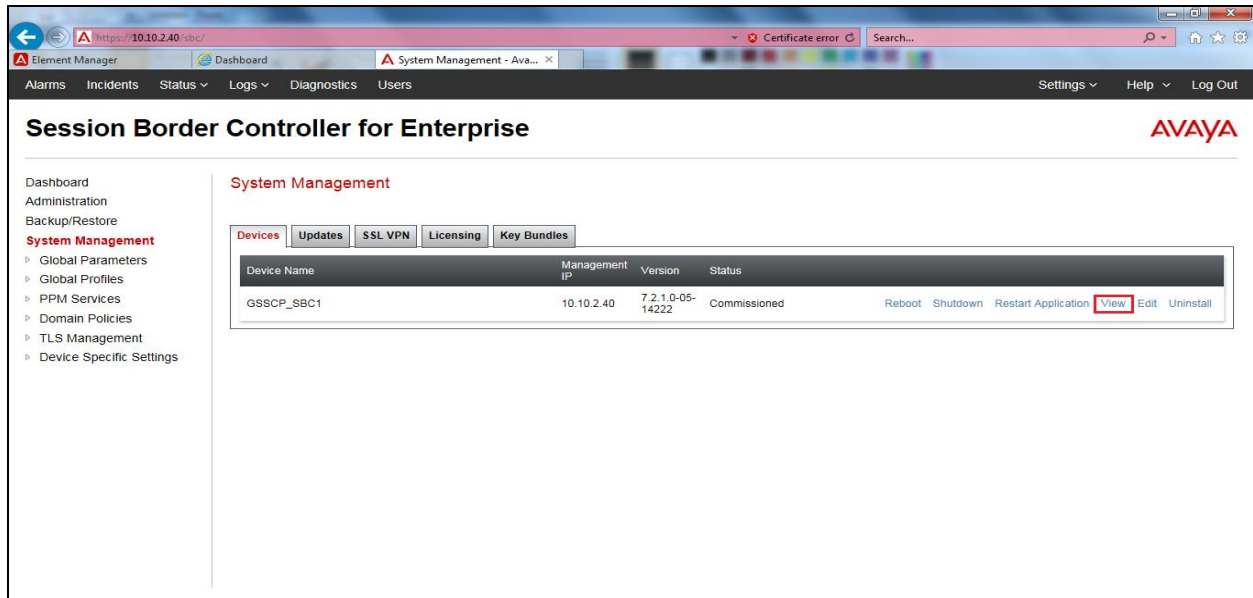


The dashboard is titled "Session Border Controller for Enterprise" and features the Avaya logo. A left-hand menu lists various sections: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into several sections:

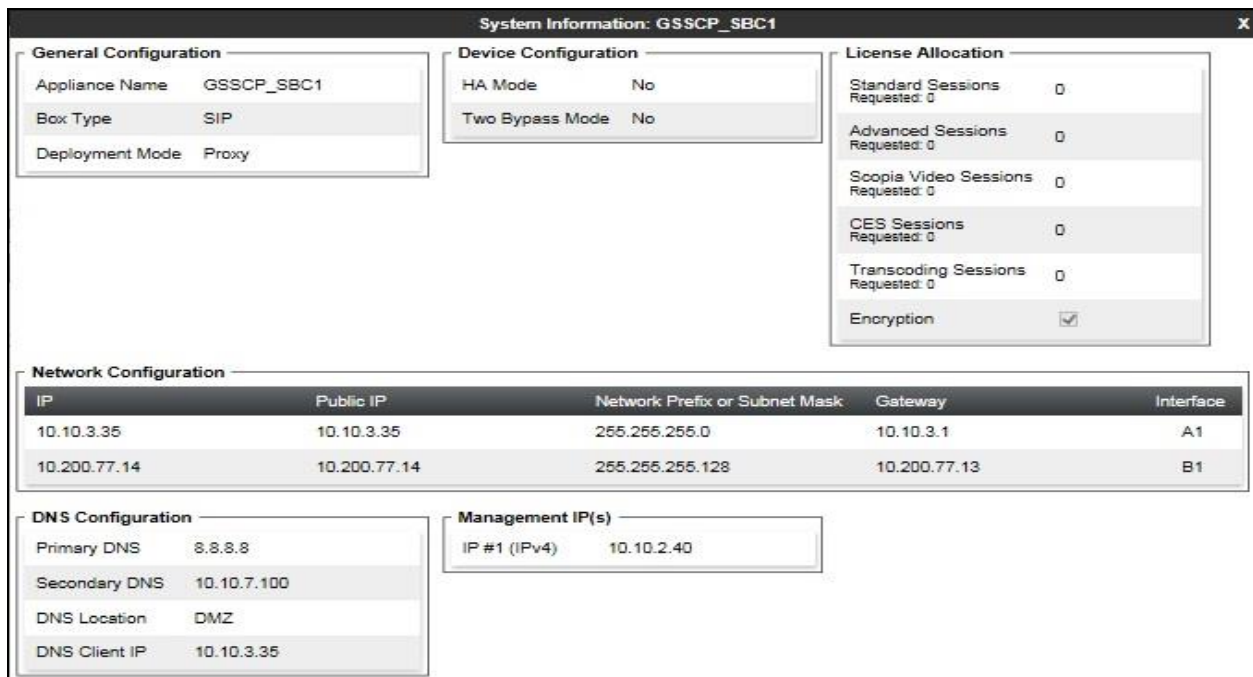
- Information:** A table with system details.

System Time	01:54:07 PM GMT	Refresh
Version	7.2.1.0-05-14222	
Build Date	Tue Oct 31 00:06:46 UTC 2017	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	03/15/2018 10:12:02 GMT	
Failed Login Attempts	0	
- Installed Devices:** A list showing "EMS" and "GSSCP_SBC1".
- Active Alarms (past 24 hours):** "None found."
- Incidents (past 24 hours):** "None found."
- Notes:** "No notes found."

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 **GSSCP-SBC1** 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. TLS Management

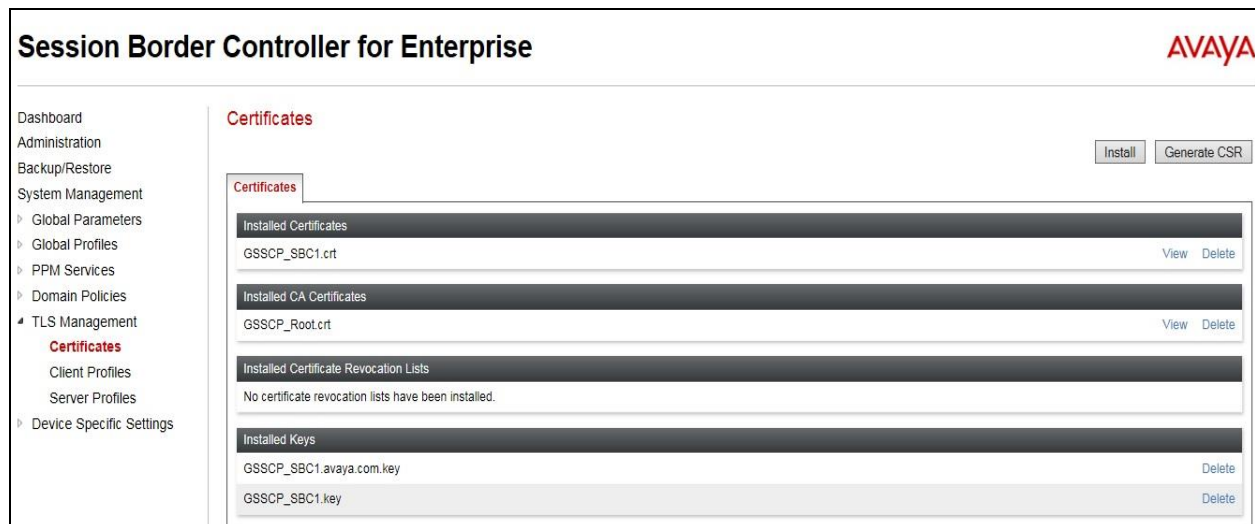
For the compliance test, TLS transport is used for signalling on the SIP trunk between Session Manager and the Avaya SBCE. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these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

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

7.2.1. Certificates

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

- Verify that an Avaya SBCE identity certificate (**GSSCP_SBC1.crt**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**GSSCP_Root.crt**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**GSSCP_SBC1.key**) is present under **Installed Keys**.



7.2.2. 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_SBC1_Client** was used in the compliance testing.
- Set **Certificate** to the identity certificate **GSSCP_SBC1.crt** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **GSSCP_Root.crt** identity certificate.
- Set **Verification Depth** to **2**. A SUBCA was used in the test configuration resulting in the use of intermediate certs, hence why Verification Depth is required to be set to 2. If a SUBCA is not been used in the test configuration, then Verification Depth would be required to be set to 1.

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

The screenshot shows the 'Client Profiles: GSSCP_SBC1_Client' configuration window. On the left, a sidebar lists 'Client Profiles' with 'GSSCP_SBC1_Client' selected. The main area is titled 'Client Profile' and contains several sections: 'TLS Profile' with 'Profile Name' as 'GSSCP_SBC1_Client' and 'Certificate' as 'GSSCP_SBC1.crt'; 'Certificate Verification' with 'Peer Verification' set to 'Required', 'Peer Certificate Authorities' as 'GSSCP_Root.crt', 'Peer Certificate Revocation Lists' as '---', 'Verification Depth' as '2', and 'Extended Hostname Verification' as an unchecked checkbox; 'Renegotiation Parameters' with 'Renegotiation Time' and 'Renegotiation Byte Count' both set to '0'; and 'Handshake Options' with 'Version' showing checkboxes for 'TLS 1.2', 'TLS 1.1', and 'TLS 1.0', all of which are checked. A blue bar at the top of the main area says 'Click here to add a description.'.

7.2.3. 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_SBC1_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **GSSCP_SBC1.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 list containing 'GSSCP_SBC1_Server'. The main area is titled 'Server Profiles: GSSCP_SBC1_Server' and includes an 'Add' button and a 'Delete' button. Below the title bar, there is a description field with the placeholder text 'Click here to add a description.' The 'Server Profile' section is expanded, showing the following configuration details:

TLS Profile	
Profile Name	GSSCP_SBC1_Server
Certificate	GSSCP_SBC1.crt

Certificate Verification	
Peer Verification	Optional
Peer Certificate Authorities	GSSCP_Root.crt
Peer Certificate Revocation Lists	---
Verification Depth	2
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. Global Profiles

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

7.3.1. 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**.
- 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"/> 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 ▼
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	<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"/>	

7.3.2. Server Interworking – Vodafone UK

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 VFUK and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	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 = None**.
- Ensure **Extensions = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

Record Routes	<input checked="" type="radio"/> None <input type="radio"/> Single Side <input 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 type="checkbox"/>
Extensions	None ▾
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"/>	

7.3.3. Server Configuration– Avaya

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

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signalling parameters and some advanced options.

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_SBC1_Client** defined in **Section 7.2.2**.
- 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:

TLS Client Profile: GSSCP_SBC1_Client

Add

IP Address / FQDN	Port	Transport
10.10.3.42	5061	TLS

Delete

Finish

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

7.3.4. Server Configuration – Vodafone UK

To define the Vodafone UK SBC as a 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 **10.152.3.6** (Vodafone UK SBC IP Address).
- 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

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

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
10.152.3.6	5060	UDP

Delete

Finish

On the Advanced tab:

- Check **Enable Grooming**.
- Select **VFUK** 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 a list of configuration options, each with a label and a control element (checkbox or dropdown menu). The options are: "Enable DoS Protection" (checkbox, unchecked), "Enable Grooming" (checkbox, checked), "Interworking Profile" (dropdown menu, set to "VFUK"), "Signaling Manipulation Script" (dropdown menu, set to "None"), "Securable" (checkbox, unchecked), "Enable FGDN" (checkbox, unchecked), "TCP Failover Port" (text input field, empty), "TLS Failover Port" (text input field, empty), "Tolerant" (checkbox, unchecked), and "URI Group" (dropdown menu, set to "None"). At the bottom right of the window is a "Finish" button.

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

Finish

7.3.5. 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 Vodafone UK addresses 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.

7.3.5.1 Routing – Avaya

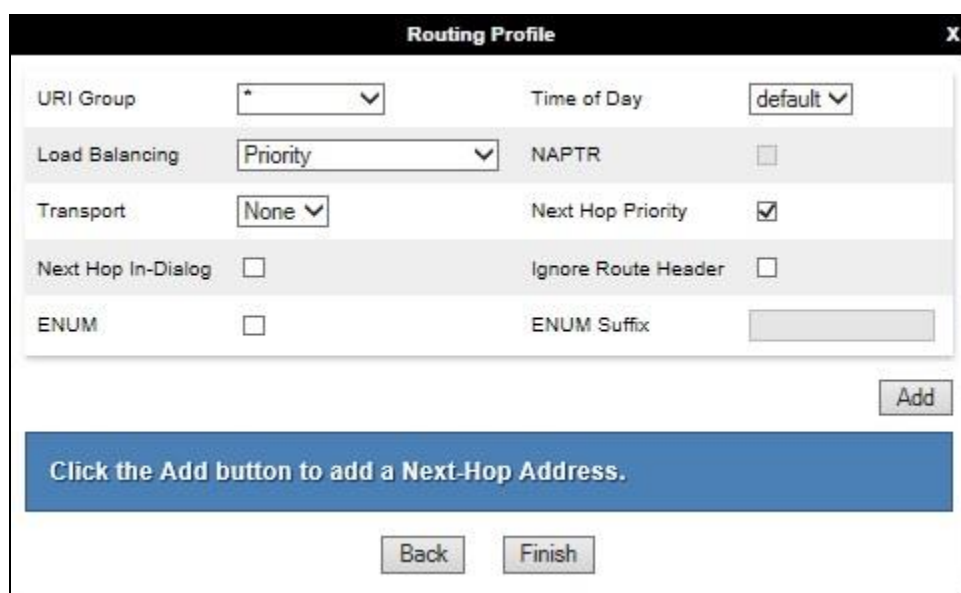
Create a Routing Profile for Session Manager.

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



The image shows a 'Routing Profile' window. At the top, it says 'Routing Profile' with a close button 'X'. Below this is a text input field for 'Profile Name' containing the text 'Avaya' and a small 'x' icon to clear the field. At the bottom center of the window is a 'Next' button.

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



The image shows a 'Routing Profile' window with various settings. At the top, it says 'Routing Profile' with a close button 'X'. The settings are organized into two columns. The left column includes: 'URI Group' with a dropdown menu showing '*'; 'Load Balancing' with a dropdown menu showing 'Priority'; 'Transport' with a dropdown menu showing 'None'; 'Next Hop In-Dialog' with an unchecked checkbox; and 'ENUM' with an unchecked checkbox. The right column includes: 'Time of Day' with a dropdown menu showing 'default'; 'NAPTR' with an unchecked checkbox; 'Next Hop Priority' with a checked checkbox; 'Ignore Route Header' with an unchecked checkbox; and 'ENUM Suffix' with an empty text input field. At the bottom right is an 'Add' button. Below the 'Add' button 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 7.3.3)** from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5061 (TLS)** from drop down menu.
- Click **Finish**.

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

7.3.5.2 Routing – Vodafone UK

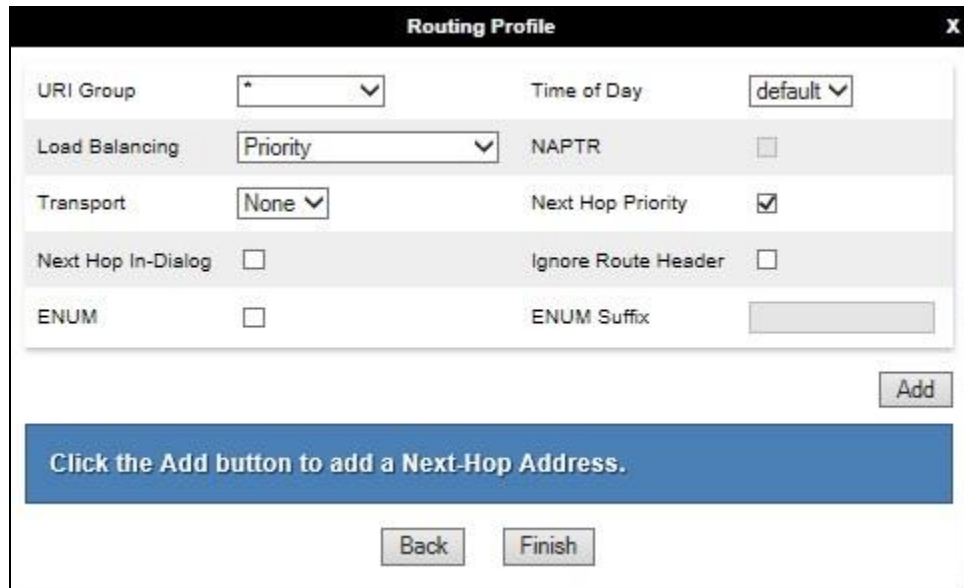
Create a Routing Profile for Vodafone UK.

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

Profile Name: VFUK

Next

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



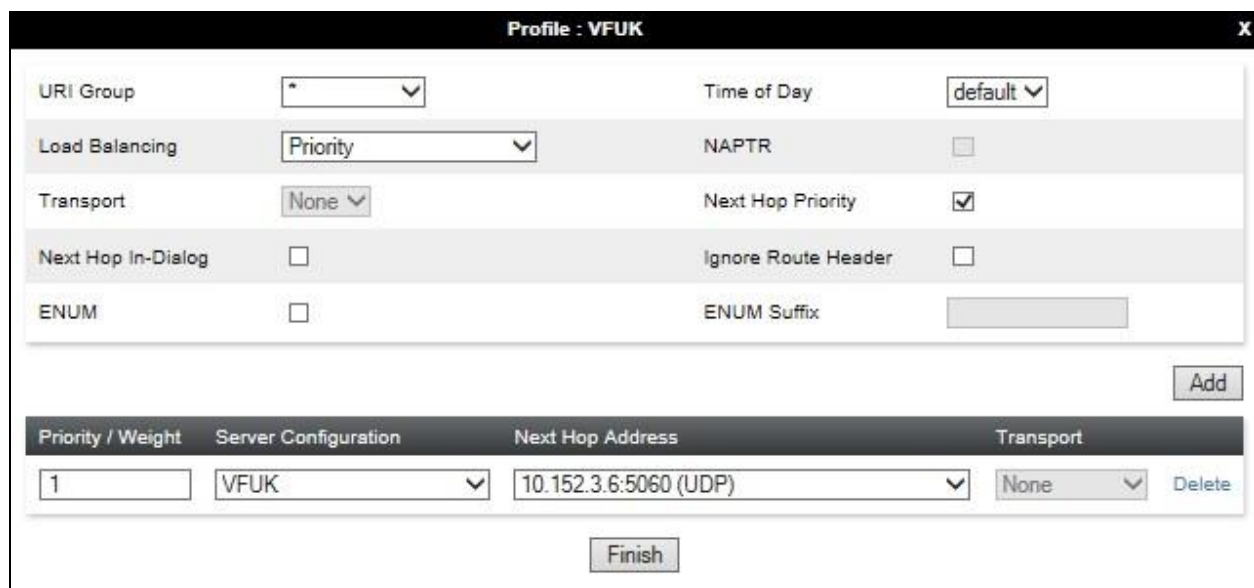
The Routing Profile window is a configuration dialog with a title bar "Routing Profile" and a close button "X". It contains several settings:

- 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: ☐
- ENUM: ☐
- ENUM Suffix: (text field)

At the bottom right is an "Add" button. Below the settings is a blue instruction bar: "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 = VFUK** (Section 7.3.4) from drop down menu.
- **Next Hop Address = Select 10.15.2.3.6:5060 (UDP)** from drop down menu.
- Click **Finish**.



The Profile : VFUK window is a configuration dialog with a title bar "Profile : VFUK" and a close button "X". It contains the same settings as the Routing Profile window:

- 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: ☐
- ENUM: ☐
- ENUM Suffix: (text field)

At the bottom right is an "Add" button. Below the settings is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, Transport, and a Delete button.

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	VFUK	10.15.2.3.6:5060 (UDP)	None	Delete

At the bottom center is a "Finish" button.

7.3.6. 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

RenameCloneDelete

Topology Hiding Profiles

default

cisco_th_profile

Avaya

VFUK

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Vodafone UK, 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 Vodafone UK 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: VFUK

Add

Rename Clone Delete

Topology Hiding Profiles

default

cisco_th_profile

Avaya

VFUK

Click here to add a description.

Topology Hiding

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

Edit

7.4. Domain Policies

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

In the reference configuration, only new Media Rules were defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

7.4.1. Media Rules

A media rule defines the processing to be applied to the selected media. For the compliance test, a media rule was created for Session Manager to use SRTP, while the predefined **default-low-med** media rule was used for the Vodafone UK SIP server.

To define the Media Rule for Session Manager, navigate to **Domain Policies** → **Media Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **Avaya_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Set **Preferred Format #2** to **SRTP_AES_CM_128_HMAC_SHA1_30**.
- Set **Preferred Format #3** to **RTP**.
- Check **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous**.

Default values were used for all other fields. Click **Finish** (not shown).

The screenshot shows the 'Media Rules: Avaya_SRTP' configuration window. On the left is a sidebar with a list of media rules: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_SRTP' (which is highlighted in red). The main area has tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing settings for 'Audio Encryption'. Under 'Audio Encryption', 'Preferred Formats' are listed as 'SRTP_AES_CM_128_HMAC_SHA1_80', 'SRTP_AES_CM_128_HMAC_SHA1_32', and 'RTP'. 'Encrypted RTCP' is checked, 'MKI' is unchecked, 'Lifetime' is set to 'Any', and 'Interworking' is checked. Below this is the 'Video Encryption' section, where 'Preferred Formats' is 'RTP' and 'Interworking' is unchecked. At the bottom is the 'Miscellaneous' section, where 'Capability Negotiation' is checked. At the top right of the main area are buttons for 'Rename', 'Clone', and 'Delete'. A 'Filter By Device...' dropdown is also present at the top left of the main area.

For the compliance test, the default media rule **default-low-med** was used for Vodafone UK.

The screenshot shows the 'Media Rules: default-low-med' configuration page. On the left is a sidebar with a list of media rules: 'default-low-med' (highlighted), 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Avaya_SRTP'. The main area has tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. A 'Miscellaneous' section at the bottom has 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right. A warning banner at the top states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.'

7.5. End Point Policy Groups

An end point policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, one end point policy group must be created for Session Manager and another for the Vodafone UK SIP server. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 7.8**.

7.5.1. End Point Policy Group – Session Manager

To define an End Point policy for Session Manager, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name, in this case **Avaya**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signalling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **Avaya_SRTP**.

Click **Finish**.

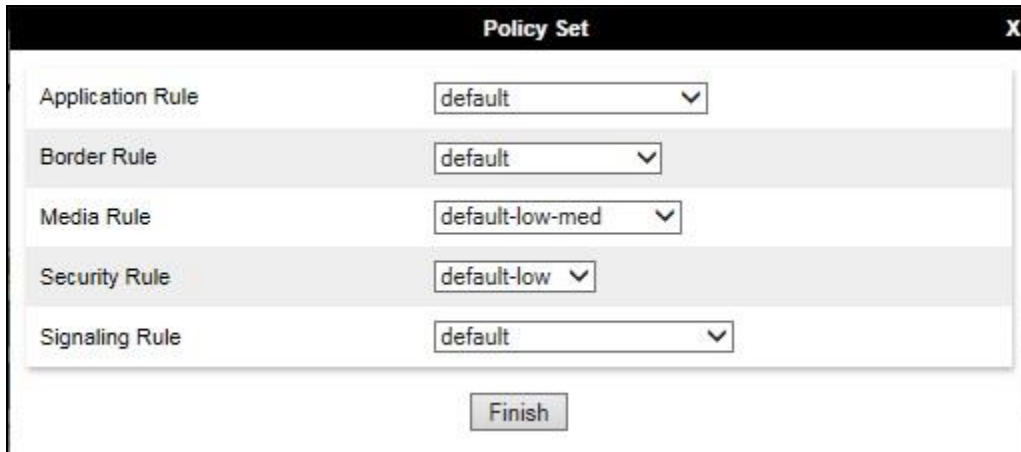
The screenshot shows the 'Policy Set' dialog box with a title bar and a close button. It contains five rows of configuration options, each with a label and a dropdown menu: 'Application Rule' (default), 'Border Rule' (default), 'Media Rule' (Avaya_SRTP), 'Security Rule' (default-low), and 'Signaling Rule' (default). A 'Finish' button is located at the bottom center.

7.5.2. End Point Policy Group – Vodafone UK

For the compliance test, the end point policy group **VFUK** was created for the Vodafone UK SIP server. Default values were used for each of the rules which comprise the group.

- In the **Group Name** field enter a descriptive name, in this case **VFUK** and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Media Rule**, **Security Rule** and **Signaling Rule** fields at their default values.

Click **Finish**.



The screenshot shows a window titled "Policy Set" with a close button (X) in the top right corner. Inside the window, there are five rows, each representing a different rule type with a corresponding dropdown menu:

Rule Type	Selected Value
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

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

7.6. Define Network Information

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 interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add**. Enter details in the blank box that appears at the end of the list.

- Define the internal IP address with screening mask and assign to interface **A1**.
- Select **Save** to save the information.
- Click on **Add**.
- Define the external IP address with screening mask and assign to interface **B1**.
- Select **Save** to save the information.
- Click on **System Management** in the main menu.
- Select **Restart Application** indicated by an icon in the status bar (not shown).

Network Management: GSSCP_SBC1

Devices
GSSCP_SBC1

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	10.10.3.35	Edit	Delete
B1_External	10.200.77.13	255.255.255.128	B1	10.200.77.14	Edit	Delete

Select the **Interface Configuration** Tab and click on **Status** to toggle the interfaces.

Network Management: GSSCP_SBC1

Devices
GSSCP_SBC1

Interfaces Networks

Add VLAN

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

7.7. Define Interfaces

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

7.7.1. 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.
- In the **IP Address** drop down menus, select the internal network interface and IP address. When the internal network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.6**.
- Insert **TLS** port number, **5061** is used for Session Manager.
- For **TLS Profile**, select **GSSCP_SBC1_Server** defined in **Section 7.2.3**.

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.
- In the **IP Address** drop down menus, select the external network interface and IP address. When the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.6**.
- Insert **UDP** port number, **5060** is used for Vodafone UK SIP Trunk service.

The following screen shows the Signalling Interfaces created in the sample configuration for the inside and outside IP interfaces.

Signaling Interface: GSSCP_SBC1

Devices

GSSCP_SBC1

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	10.200.77.14 B1_External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Int_Sig	10.10.3.35 A1_Internal (A1, VLAN 0)	---	---	5061	GSSCP_SBC1_Server	Edit Delete

7.7.2. 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 on 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.
- In the **IP Address** drop down menus, select the internal network interface and IP address. When the internal network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.6**.
- Select **RTP port** ranges for the media path with the enterprise end-points.

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

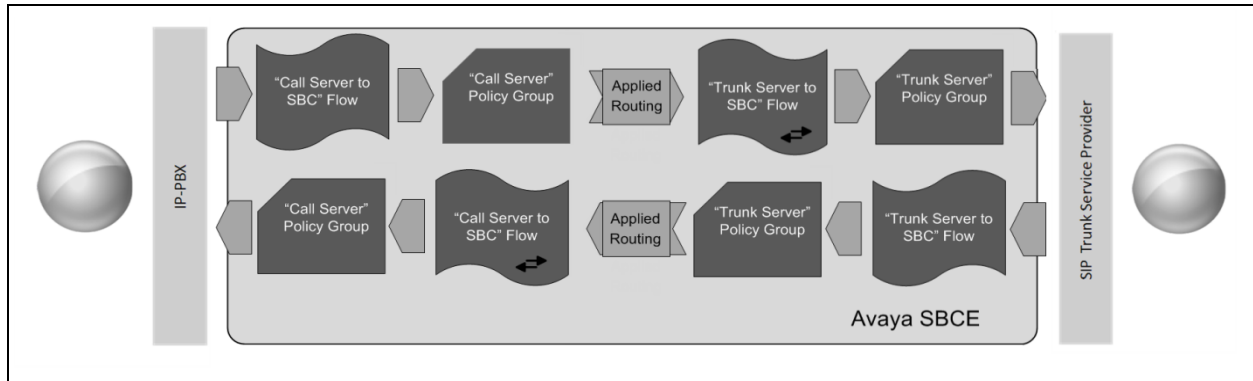
- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. When the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.6**.
- Select **RTP port** ranges for the external media path.

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces.

Name	Media IP Network	Port Range	
Int_Media	10.10.3.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Ext_Media	10.200.77.14 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete

7.8. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Vodafone UK's SIP Trunk and incoming flows from Vodafone UK'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 Vodafone UK 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.

End Point Flows: GSSCP_SBC1

Devices: GSSCP_SBC1

Subscriber Flows | **Server Flows** | Add

Hover over a row to see its 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	Avaya_SRTP	VFUK	View Clone Edit Delete

Server Configuration: VFUK

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

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

- Click on the **Server Flows** tab (shown above).
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Vodafone UK SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Vodafone UK server configuration defined in **Section 7.3.4**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.7.1**. This is the interface that signalling bound for Vodafone UK SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.7.1**. This is the interface that signalling bound for Vodafone UK SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.7.2**. This is the interface that media bound for Vodafone UK SIP Trunk is sent on.
- Set the **End Point Policy Group** to the endpoint policy group defined for Vodafone UK in **Section 7.5.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.3.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Vodafone UK SIP Trunk defined in **Section 7.3.6** and click **Finish**.

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

Criteria		Profile	
Flow Name	Trunk_Server	Signaling Interface	Ext_Sig
Server Configuration	VFUK	Media Interface	Ext_Media
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	VFUK
Remote Subnet	*	Routing Profile	Avaya
Received Interface	Int_Sig	Topology Hiding Profile	VFUK
		Signaling Manipulation Script	None
		Remote Branch Office	Any

To define a Server Flow for Session Manager, 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 Session Manager server configuration defined in **Section 7.3.3**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.7.1**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.7.1**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.7.2**. This is the interface that media bound for Session Manager is sent on.
- Set the **End Point Policy Group** to the endpoint policy group defined for Session Manager in **Section 7.5.1**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone UK SIP Trunk defined in **Section 7.3.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.3.6** and click **Finish**.

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	Avaya_S RTP
Routing Profile	VFUK
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

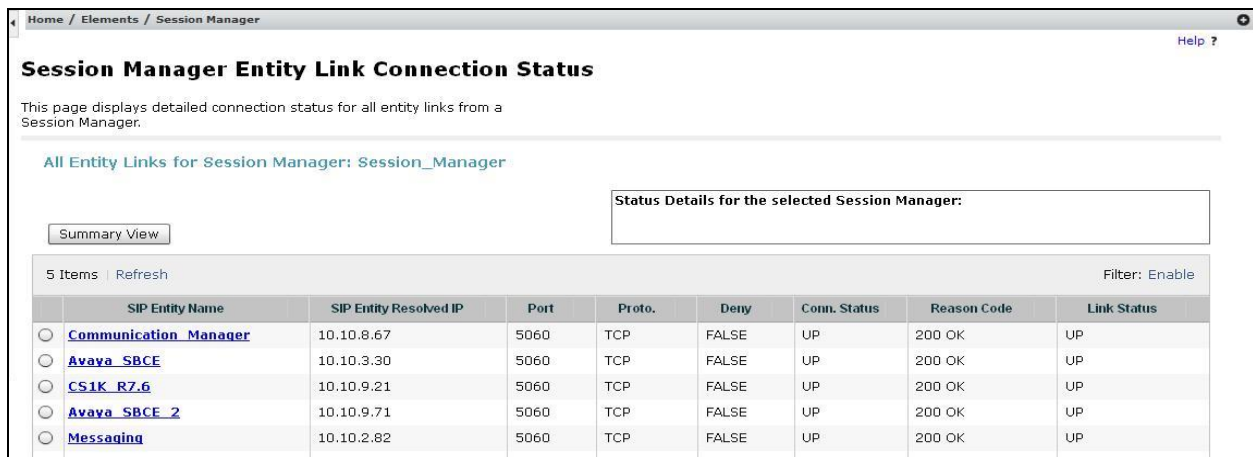
8. Vodafone UK SIP Trunk Service Configuration

The configuration of the Vodafone UK equipment used to support Vodafone UK's SIP trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Vodafone UK equipment and system configuration please contact an authorized Vodafone UK 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**.



SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
Communication Manager	10.10.8.67	5060	TCP	FALSE	UP	200 OK	UP
Avaya SBCE	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
CS1K R7.6	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP
Avaya SBCE 2	10.10.9.71	5060	TCP	FALSE	UP	200 OK	UP
Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

2. From the 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 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no
0001/004	T00004	in-service/idle	no
0001/005	T00005	in-service/idle	no
0001/006	T00006	in-service/idle	no
0001/007	T00007	in-service/idle	no
0001/008	T00008	in-service/idle	no
0001/009	T00009	in-service/idle	no
0001/010	T00010	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 **All** 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**, 10000 is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP_SBC1

Devices

GSSCP_SBC1

Packet Capture

Captures

Packet Capture Configuration

Status	Ready
Interface	B1 ▾
Local Address IP[:Port]	All ▾ : <input type="text"/>
Remote Address *:Port, IP, IP:Port	<input type="text" value="*"/>
Protocol	All ▾
Maximum Number of Packets to Capture	<input type="text" value="10000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input type="text" value="TestCall.pcap"/>
<input type="button" value="Start Capture"/> <input type="button" value="Clear"/>	

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

Trace: GSSCP_SBC1

Devices

GSSCP_SBC1

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
TestCall.pcap	735,874	March 14, 2018 4:24:42 PM GMT	Delete

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.1 as an Evolution Server, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to Vodafone UK SIP Trunk Service. Vodafone UK SIP Trunk 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] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, Dec 2017
- [2] *Avaya Aura® Communication Manager 7.1 Documentation library*, Dec 2017
- [3] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide Release 7.1* Dec 2017
- [4] *Implementing Avaya Aura® System Manager Release 7.1*, Dec 2017
- [5] *Upgrading Avaya Aura® System Manager to Release 7.1*, Dec 2017
- [6] *Administering Avaya Aura® System Manager Release 7.1*, Dec 2017
- [7] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide Release 7.1*, Dec 2017
- [8] *Implementing Avaya Aura® Session Manager Release 7.1*, Dec 2017
- [9] *Upgrading Avaya Aura® Session Manager Release 7.1*, Dec 2017
- [10] *Administering Avaya Aura® Session Manager Release 7.1*, Dec 2017
- [11] *Deploying Avaya Session Border Controller for Enterprise Release 7.2*, Jan 2018
- [12] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2*, Jan 2018
- [13] *Administering Avaya Session Border Controller for Enterprise Release 7.2*, Jan 2017
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.