



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R8.1 as an Evolution Server, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.0 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.

## 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:

- Intermittent outbound calls to the Vodafone UK SIP Trunk were rejected with “408 Request Timeout”. This is a characteristic of the Vodafone UK test environment and not an interoperability issue.
- When attempting to execute a Blind Transfer to a PSTN phone for both inbound and outbound calls, Vodafone UK were responding with “415 Unsupported Media Type” as Communication Manager uses the UPDATE method to execute the Blind Transfer successfully. In order for Blind Transfers to execute successfully for inbound and outbound calls, set “Always Use re-INVITE for Display Updates” to “y” within the trunk groups settings in **Section 5.6**.
- 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 SRTP was enabled on Communication Manager and Avaya SBCE internally, it resulted in multiple re-INVITES and “491 Request Pending” responses from the Vodafone network as the codec negotiation was taking place. This resulted in extra signalling and audio delay. In order to reduce signalling and audio delay issues, SRTP was disabled on Communication Manager and Avaya SBCE internally and RTP was used for the duration of the testing.
- 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 Vodafone UK SIP Trunk service was automatically changed by Vodafone UK to a CLID number recognizable to the Vodafone 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.

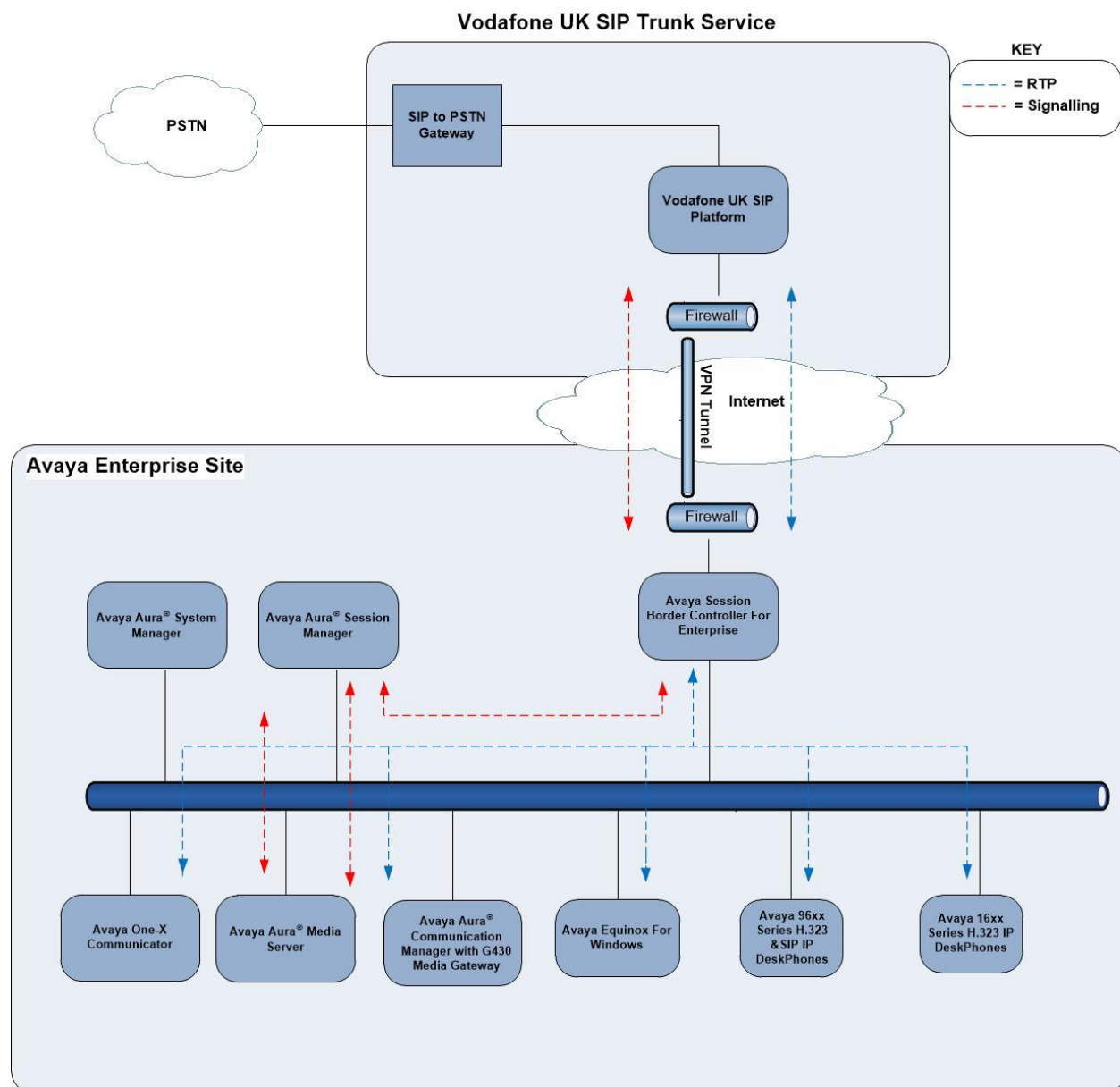
## 2.3. Support

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 Session Border Controller for Enterprise, 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 soft phone 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
<b>Avaya</b>	
Avaya Aura® System Manager	8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.0.079814
Avaya Aura® Session Manager	8.1.0.0.801007
Avaya Aura® Communication Manager	8.1.0.1.1 – SP1.1
Avaya Session Border Controller for Enterprise	8.0.1.0-10-175555
Avaya G430 Media Gateway	41.9.0
Avaya Aura® Media Server	v.8.0.0.205
Avaya 1600 IP Deskphone (H.323)	1.3.12
Avaya 96x0 IP DeskPhone (H.323)	3.2.4
Avaya 96x1 IP DeskPhone (H.323)	6.8.2
Avaya 9611 IP DeskPhone (SIP)	7.1.6.0
Avaya 9608 IP DeskPhone (SIP)	7.1.6.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.14.1 -SP14
Avaya Equinox™ for Windows	3.6.4.31.2
Analogue Handset	N/A
Analogue Fax	N/A
<b>Vodafone UK</b>	
SBC	Acme Packet 6300 SCZ8.3.0 Patch 7 (Build 123) Oracle Linux branches-7/el7-u6 {2019-06-10T07:00:00+0000} Build Date=07/24/19
Softswitch	Ribbon C20 R19 (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	
<b>Maximum Administered SIP Trunks:</b>		<b>4000</b>	<b>10</b>	
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	
<b>SM100</b>	<b>10.10.3.42</b>	
default	0.0.0.0	
<b>procr</b>	<b>10.10.3.44</b>	
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

1: none

Encrypted SRTP: best-effort

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)
<b>FAX</b>	<b>pass-through</b>	<b>0</b>	
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? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? 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**.

<b>add trunk-group 1</b>	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	<b>Numbering Format: private</b>
	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	
	<b>Mark Users as Phone? y</b>
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	<b>Send Transferring Party Information? n</b>
	<b>Network Call Redirection? n</b>
Build Refer-To URI of REFER From Contact For NCR? n	
	<b>Send Diversion Header? y</b>
	<b>Support Request History? n</b>
	<b>Telephone Event Payload Type: 101</b>
	Convert 180 to 183 for Early Media? n
	<b>Always Use re-INVITE for Display Updates? y</b>
	<b>Identity for Calling Party Display: P-Asserted-Identity</b>
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 - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	6010	1	14xxxxxx26	11	Total Administered: 6
4	6020	1	14xxxxxx27	11	Maximum Entries: 240
4	6030	1	14xxxxxx28	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	6100	1	14xxxxxx29	11	
4	6102	1	14xxxxxx30	11	
4	6104	1	14xxxxxx31	11	
					Communication Manager automatically inserts a '+' digit in this case.

## 5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to 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		
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>		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. <b>Numbering</b>	LAR
0 1 2 M 4 W			Request									Dgts <b>Format</b>	
													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

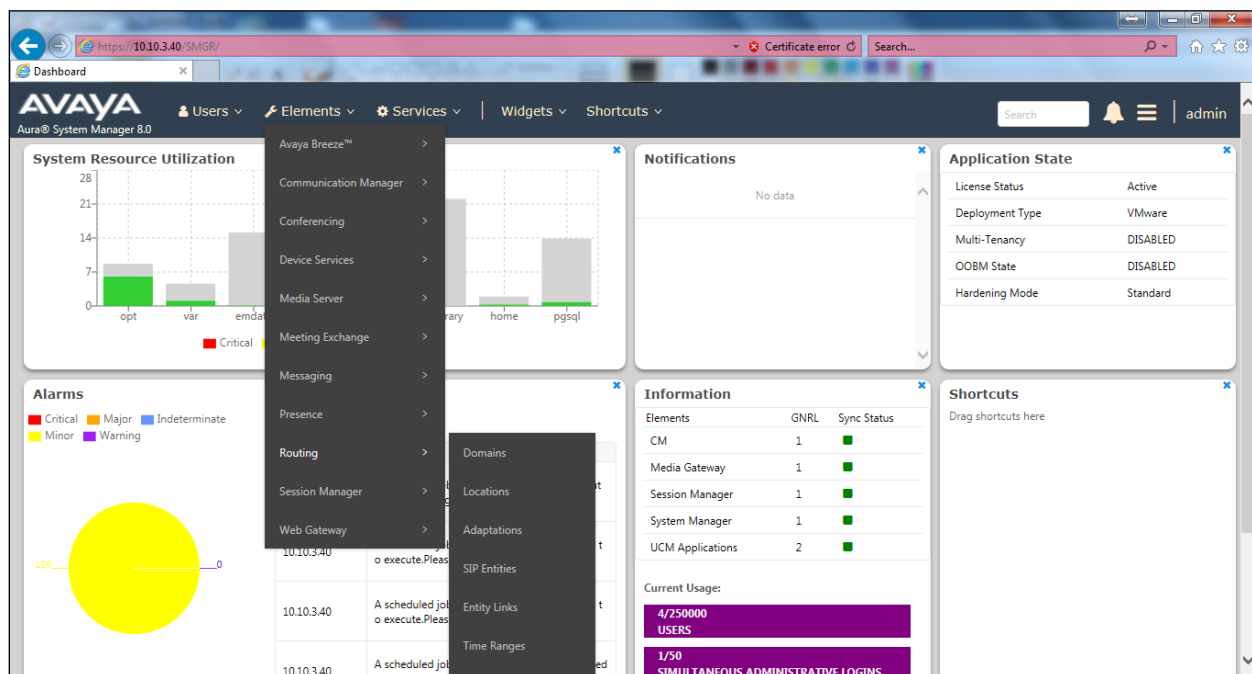
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

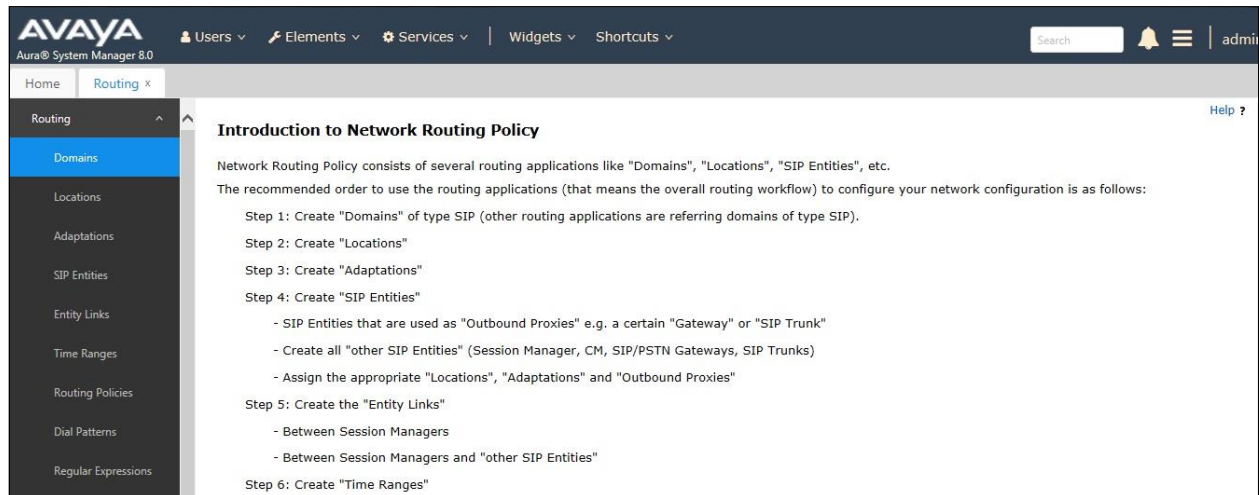
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session 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\_8** defined for the compliance testing.

### Location Details

CommitCancel

#### General

\* Name: SMGR\_8

Notes:

#### Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

#### Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

## 6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers. An Adaptation was used during testing to remove Avaya proprietary headers from messages sent. Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. In order to improve interoperability with third party elements, Session Manager R8.1 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary unnecessary for non-Avaya elements. For the compliance test, an Adaptation named “**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 and also add unnecessary size to outbound messages, while they have no significance to the service provider.

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

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

\* **Adaptation Name:** VFUK

\* **Module Name:** DigitConversionAdapter

**Module Parameter Type:** Name-Value Parameter

Add Remove	
<input type="checkbox"/> Name	Value
<input type="checkbox"/> eRHdrs	"Require, AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID,
<input type="checkbox"/> fromto	true
<input type="checkbox"/> MIME	no

Select : All, None

**Egress URI Parameters:**

**Notes:**

## 6.5. Administer SIP Entities

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

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP Entity, **CM** for a Communication Manager SIP Entity and **SIP Trunk** for the Avaya SBCE SIP 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.

#### SIP Entity Details

CommitCancel

##### General

\* Name: Session Manager

\* IP Address: 10.10.3.42

SIP FQDN:

Type: Session Manager

Notes:

Location: SMGR\_8

Outbound Proxy:

Time Zone: Europe/Dublin

Minimum TLS Version: Use Global Setting

Credential name:

##### Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

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

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

#### Port

TCP Failover port:

TLS Failover port:

AddRemove

3 Items

Filter: Enable

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

Select : All, None

### 6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. 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.

**SIP Entity Details**

CommitCancel

**General**

\* Name: Communication Manager

\* FQDN or IP Address: 10.10.3.44

Type: CM

Notes:

Adaptation:

Location: SMGR\_8

Time Zone: Europe/Dublin

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable:

Call Detail Recording: none

**Loop Detection**

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

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

**Loop Detection**

Loop Detection Mode: Off

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

### 6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. 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.

#### SIP Entity Details

CommitCancel

##### General

\* Name: Avaya\_SBCE

\* FQDN or IP Address: 10.10.3.30

Type: SIP Trunk

Notes:

Adaptation: VFUK

Location: SMGR\_8

Time Zone: Europe/Dublin

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress

##### Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5



## 6.6. Administer Entity Links

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

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

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

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	<a href="#">Aura Messaging</a>	Session Manager	TLS	5061	Aura_Messaging	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">Avaya SBCE</a>	Session Manager	TLS	5061	Avaya_SBCE	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">Communication Manager</a>	Session Manager	TLS	5061	Communication Manager	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Select : All, None

## 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. The 'General' section includes fields for Name (to\_Communication\_Manager), Disabled (checkbox), Retries (0), and Notes. The 'SIP Entity as Destination' section shows a table with one entry: Communication\_Manager, 10.10.3.44, CM. The 'Time of Day' section shows a table with one item: 24/7, with checkboxes for all days of the week and a time range of 00:00 to 23:59.

Home / Elements / Routing / Routing Policies

**Routing Policy Details** [Commit](#) [Cancel](#) [Help ?](#)

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

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.

**Routing Policy Details** [Commit] [Cancel]

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE	10.10.3.30	SIP Trunk	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
1	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.

[Help ?](#)

### Dial Pattern Details

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

1 Item
Filter: Enable

<input checked="" type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input checked="" type="checkbox"/>	SMGR_8		to_Avaya_SBCE		<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

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

[Help ?](#)

### Dial Pattern Details

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

1 Item
Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGR_8		to_Communication_Manager	0	<input type="checkbox"/>	Communication Manager	

<  >

Select : All, None

## 7. Configure Avaya Session Border Controller for Enterprise

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

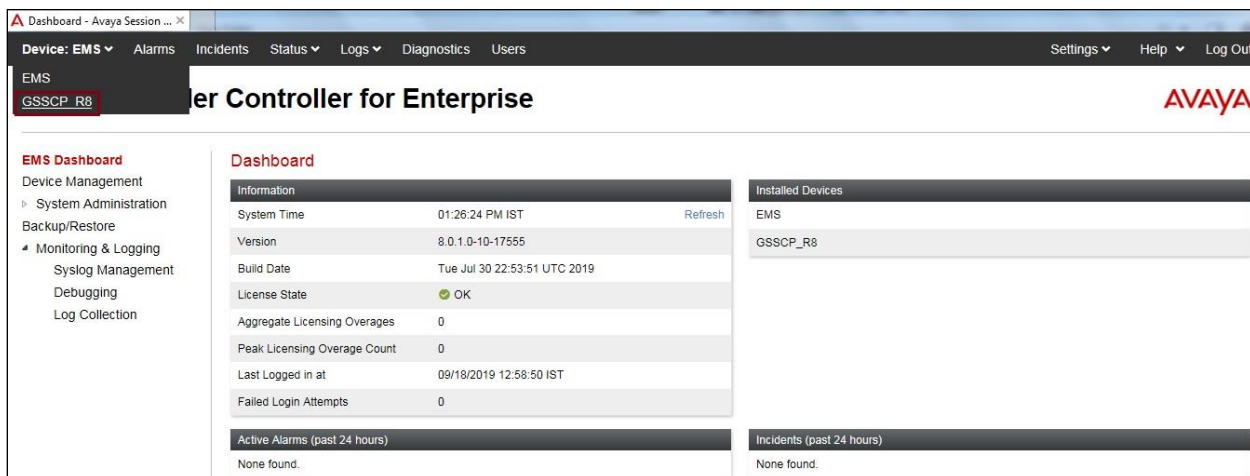
### 7.1. Access Avaya Session Border Controller for Enterprise

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



The screenshot shows the login page of the Avaya Session Border Controller for Enterprise. The page features the Avaya logo in red, the text "Session Border Controller for Enterprise", and a "Log In" section. The "Log In" section includes a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a disclaimer about unauthorized access, and a consent statement. The footer indicates the copyright years 2011-2019 for Avaya Inc.

Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu with a menu on the left-hand side. In this case, **GSSCP\_R8** is used as a starting point for all configuration of the Avaya SBCE.



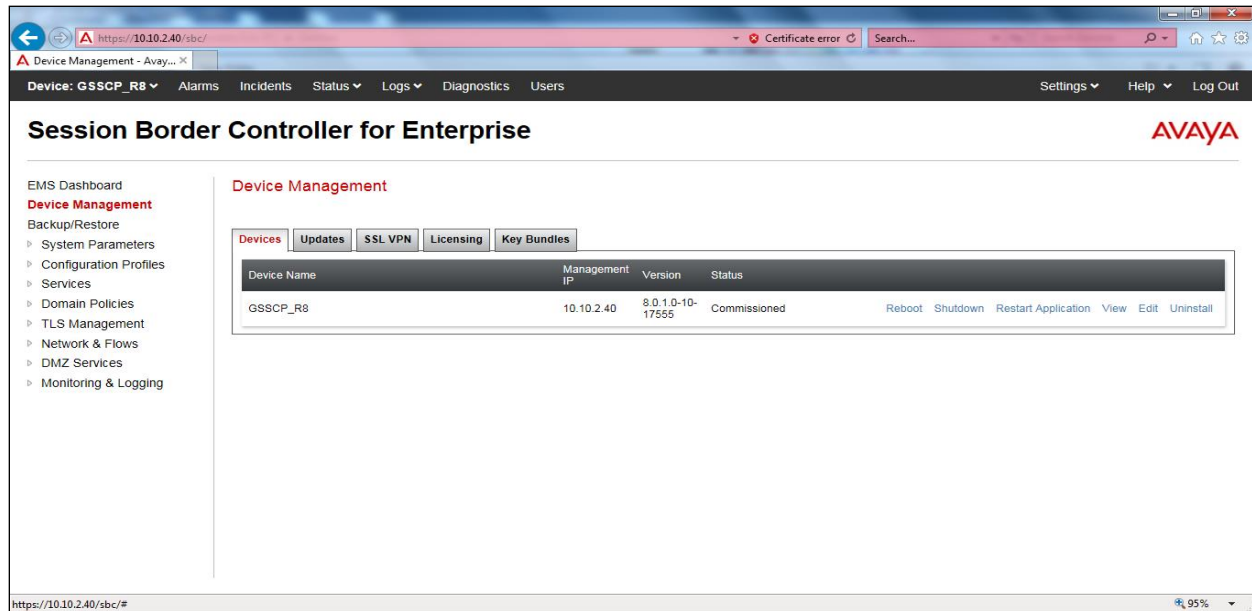
The screenshot shows the dashboard of the Avaya Session Border Controller for Enterprise. The top navigation bar includes "Device: EMS", "Alarms", "Incidents", "Status", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out". The left sidebar lists "EMS" and "GSSCP\_R8". The main content area is titled "Session Border Controller for Enterprise" and contains a "Dashboard" section. The "Dashboard" section includes a table of system information, a list of installed devices, and sections for active alarms and incidents.

Information	
System Time	01:26:24 PM IST <a href="#">Refresh</a>
Version	8.0.1.0-10-17555
Build Date	Tue Jul 30 22:53:51 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	09/18/2019 12:58:50 IST
Failed Login Attempts	0

Active Alarms (past 24 hours)  
None found.

Incidents (past 24 hours)  
None found.

To view system information that was configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP\_R8** 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.

System Information: GSSCP\_R8

**General Configuration**

Appliance Name	GSSCP_R8
Box Type	SIP
Deployment Mode	Proxy

**Device Configuration**

HA Mode	No
Two Bypass Mode	No

**License Allocation**

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
CLID	---
Encryption Available: Yes	<input checked="" type="checkbox"/>

**Network Configuration**

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
10.200.77.14	10.200.77.14	255.255.255.128	10.200.77.13	B1

**DNS Configuration**

Primary DNS	10.10.7.100
Secondary DNS	8.8.8.8
DNS Location	DMZ
DNS Client IP	10.10.3.30

**Management IP(s)**

IP #1 (IPv4)
--------------

## 7.2. Define Network Management

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

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

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

The screenshot shows a 'Network' dialog box with a warning banner at the top: 'Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.' Below the banner are four input fields: 'Name' (B1\_External), 'Default Gateway' (10.200.77.13), 'Network Prefix or Subnet Mask' (255.255.255.128), and 'Interface' (B1). An 'Add' button is to the right of the 'Interface' field. Below these fields is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The first row contains the values '10.200.77.14', 'Use IP Address', and 'Use Default'. A 'Delete' button is to the right of the first row. At the bottom of the dialog is a 'Finish' button.

IP Address	Public IP	Gateway Override
10.200.77.14	Use IP Address	Use Default



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

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

The following screenshot shows the completed Network Management configuration:

**Network Management**

Interfaces **Networks**

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1_Internal	10.10.3.1	255.255.255.0	A1	10.10.3.30	Edit Delete
B1_External	10.200.77.13	255.255.255.128	B1	10.200.77.14	Edit Delete

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



Network Management

Interfaces Networks

Add VLAN

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

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

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

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

## 7.3. Define TLS Profiles

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

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

### 7.3.1. Certificates

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

- Verify that an Avaya SBCE identity certificate (**asbce40int.pem**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**SystemManagerCA.pem**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**asbce40int.key**) is present under **Installed Keys**.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with options: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates (highlighted), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Certificates' and includes 'Install' and 'Generate CSR' buttons. It is divided into five sections: 'Installed Certificates' showing 'asbce40int.pem' with 'View' and 'Delete' links; 'Installed CA Certificates' showing 'SystemManagerCA.pem' with 'View' and 'Delete' links; 'Installed Certificate Revocation Lists' with a message 'No certificate revocation lists have been installed.'; 'Installed Certificate Signing Requests' with a message 'No certificate signing requests have been installed.'; and 'Installed Keys' showing 'asbce40int.key' with a 'Delete' link. The Avaya logo is in the top right corner.

### 7.3.2. Client Profile

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

- Set **Profile Name** to a descriptive name. **GSSCP\_Client** was used in the compliance testing.
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **SystemManagerCA.pem** identity certificate.
- Set **Verification Depth** to **1**.

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

The screenshot displays the 'Client Profiles: GSSCP\_Client' configuration window. On the left, a sidebar shows 'Client Profiles' with 'GSSCP\_Client' selected. The main area is divided into two sections. The top section, 'Client Profile', contains fields for 'Profile Name' (GSSCP\_Client), 'Certificate' (asbce40int.pem), and 'SNI' (Enabled). Below this is the 'Certificate Verification' section, which includes 'Peer Verification' (Required), 'Peer Certificate Authorities' (SystemManagerCA.pem), 'Peer Certificate Revocation Lists' (---), 'Verification Depth' (1), and 'Extended Hostname Verification' (disabled). The bottom section, 'Renegotiation Parameters', shows 'Renegotiation Time' and 'Renegotiation Byte Count' both set to 0. The 'Handshake Options' section includes 'Version' (TLS 1.2, 1.1, and 1.0 checked), 'Ciphers' (Default selected), and 'Value' (HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH). An 'Edit' button is located at the bottom right of the configuration area.

Client Profile	
Profile Name	GSSCP_Client
Certificate	asbce40int.pem
SNI	<input checked="" type="checkbox"/> Enabled

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

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

### 7.3.3. Server Profile

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

- Set **Profile Name** to a descriptive name. **GSSCP\_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **asbce40int.pem** used in the compliance testing.
- Set **Peer Verification** to **Optional**.

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

The screenshot shows the configuration page for a server profile named 'GSSCP\_Server'. The page is divided into two main sections. The top section, titled 'Server Profile', contains the following fields:

TLS Profile	
Profile Name	GSSCP_Server
Certificate	asbce40int.pem
SNI Options	None

Certificate Verification	
Peer Verification	Optional
Peer Certificate Authorities	---
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

The bottom section, titled 'Renegotiation Parameters' and 'Handshake Options', contains the following fields:

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
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:DH:ADH:MD5:1aNULL:1eNULL:@STRENGTH

Buttons for 'Add', 'Delete', and 'Edit' are visible. The 'Add' button is in the top left, 'Delete' is in the top right, and 'Edit' is at the bottom right of the configuration area.

## 7.4. Define Interfaces

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

### 7.4.1. Signalling Interfaces

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

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

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **A1\_Internal** signalling interface IP addresses defined in **Section 7.2**.
- Select **TLS** port number, **5061** is used for Session Manager.
- Select a **TLS Profile** defined in **Section 7.3.3** from the drop-down menu.
- Click **Finish**.

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

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **B1\_external** signalling interface IP address defined in **Section 7.2**.
- Select **UDP** port number, **5060** is used for the Vodafone UK SIP Trunk.
- Click **Finish**.

Signaling Interface						
Signaling Interface						
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Int	10.10.3.30 A1_Internal (A1, VLAN 0)	5060	---	5061	GSSCP_Server	Edit Delete
Sig_Ext	10.200.77.14 B1_External (B1, VLAN 0)	5060	5060	---	None	Edit Delete

## 7.4.2. Media Interfaces

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

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **A1\_Internal** media interface IP address defined in **Section 7.2**.
- For **Port Range**, enter **35000-40000**.
- Click **Finish**.

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

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **B1\_External** media interface IP address defined in **Section 7.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.

Name	Media IP Network	Port Range	
Med_Int	10.10.3.30 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Med_Ext	10.200.77.14 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete

## 7.5. Define Server Interworking

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

### 7.5.1. Server Interworking Avaya

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

→ **Server Interworking** and click on **Add**.

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

The screenshot shows the 'General' configuration tab for a server interworking profile. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - s=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None (dropdown)
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3281 <input type="radio"/> RFC2543



On the **Advanced** Tab:

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

Click **Finish**.

The screenshot displays the 'Advanced' configuration tab with the following settings:

- Record Routes:** Radio buttons for None, Single Side, **Both Sides** (selected), Dialog-Initiate Only (Single Side), and Dialog-Initiate Only (Both Sides).
- Include End Point IP for Context Lookup:** Checkmark is selected.
- Extensions:** Dropdown menu set to 'Avaya'.
- Diversion Manipulation:** Checkmark is not selected.
- Diversion Condition:** Dropdown menu set to 'None'.
- Diversion Header URI:** Empty text field.
- Has Remote SBC:** Checkmark is selected.
- Route Response on Via Port:** Checkmark is not selected.
- Relay INVITE Replace for SIPREC:** Checkmark is not selected.
- MOBX Re-INVITE Handling:** Checkmark is not selected.

A section header 'DTMF' is present, followed by:

- DTMF Support:** Radio buttons for **None** (selected), SIP Notify, RFC 2833 Relay & SIP Notify, SIP Info, RFC 2833 Relay & SIP Info, and Inband.

A 'Finish' button is located at the bottom right of the configuration area.

## 7.5.2. Server Interworking – Vodafone

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 **Configuration Profiles**

→ **Server Interworking** and click on **Add**.

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

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - s=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▾
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3281 <input type="radio"/> RFC2543

On the **Advanced** Tab:

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

Click **Finish**.

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions None ▾

Diversion Manipulation ☐

Diversion Condition None ▾

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

**DTMF**

DTMF Support

☒ None

☐ SIP Notify

☐ SIP Info

☐ Inband

Finish

## 7.6. Define Servers

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

### 7.6.1. Server Configuration – Avaya

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

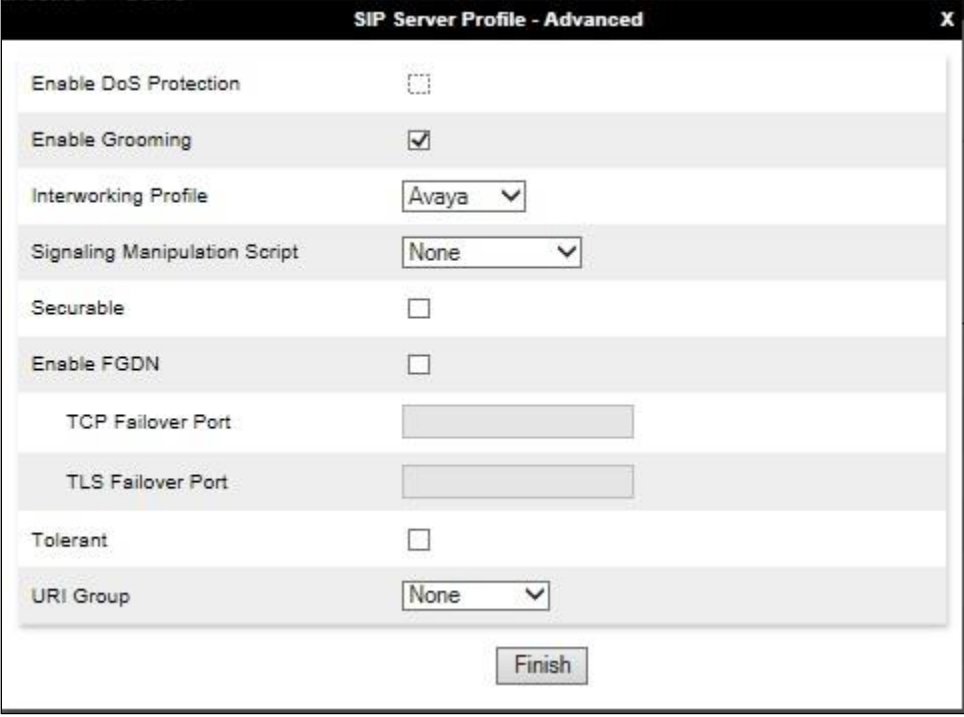
- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP\_Client** defined in **Section 7.3.2** from the drop-down menu.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5061**.
- For **Transport**, select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

The screenshot shows the 'SIP Server Profile - General' configuration window. At the top, a blue banner states: 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' Below this, the 'Server Type' is set to 'Call Server' in a dropdown menu. The 'SIP Domain' field is empty. The 'DNS Query Type' is set to 'NONE/A' in a dropdown menu. The 'TLS Client Profile' is set to 'GSSCP\_Client' in a dropdown menu. An 'Add' button is located to the right of these fields. Below a horizontal separator, there is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '10.10.3.42', '5061', and 'TLS' respectively. A 'Delete' button is located to the right of the table.

IP Address / FQDN	Port	Transport
10.10.3.42	5061	TLS

On the **Advanced** tab:

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



The screenshot shows a window titled "SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options, each with a label and a control element:

Option	Value/Control
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya (dropdown)
Signaling Manipulation Script	None (dropdown)
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	(text input field)
TLS Failover Port	(text input field)
Tolerant	<input type="checkbox"/>
URI Group	None (dropdown)

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

### 7.6.2. Server Configuration – Vodafone

To define the Vodafone UK Trunk Server, navigate to **Services → SIP Servers** 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 SIP Platform).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

The screenshot shows the 'SIP Server Profile - General' configuration window. At the top, a blue banner states: 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' Below this, there are four configuration fields: 'Server Type' is set to 'Trunk Server' (dropdown), 'SIP Domain' is an empty text box, 'DNS Query Type' is set to 'NONE/A' (dropdown), and 'TLS Client Profile' is set to 'None' (dropdown). An 'Add' button is located to the right of these fields. Below the fields is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '10.152.3.6', '5060', and 'UDP' (dropdown). A 'Delete' button is located to the right of the table.

IP Address / FQDN	Port	Transport
10.152.3.6	5060	UDP

On the Advanced tab:

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

The screenshot shows a window titled "SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options, each with a label and a control element. The options are: "Enable DoS Protection" with an unchecked checkbox; "Enable Grooming" with a checked checkbox; "Interworking Profile" with a dropdown menu showing "VFUK"; "Signaling Manipulation Script" with a dropdown menu showing "None"; "Securable" with an unchecked checkbox; "Enable FGDN" with an unchecked checkbox; "TCP Failover Port" with an empty text input field; "TLS Failover Port" with an empty text input field; "Tolerant" with an unchecked checkbox; and "URI Group" with a dropdown menu showing "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

## 7.7. Routing

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

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

### 7.7.1. Routing – Avaya

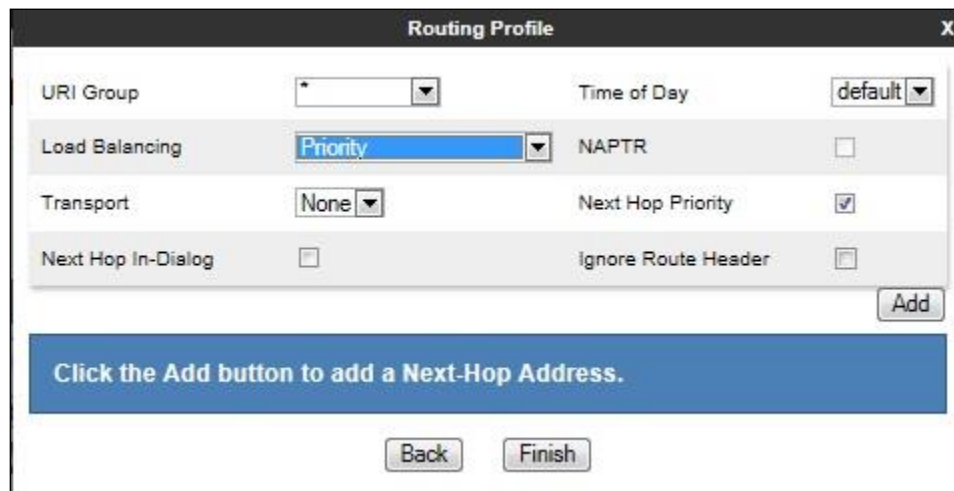
Create a Routing Profile for Session Manager.

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



The image shows a 'Routing Profile' window. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text field labeled 'Profile Name' containing the text 'Avaya'. Below the text field 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. The title bar has 'Routing Profile' and a close button 'X'. The settings are as follows:

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

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



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

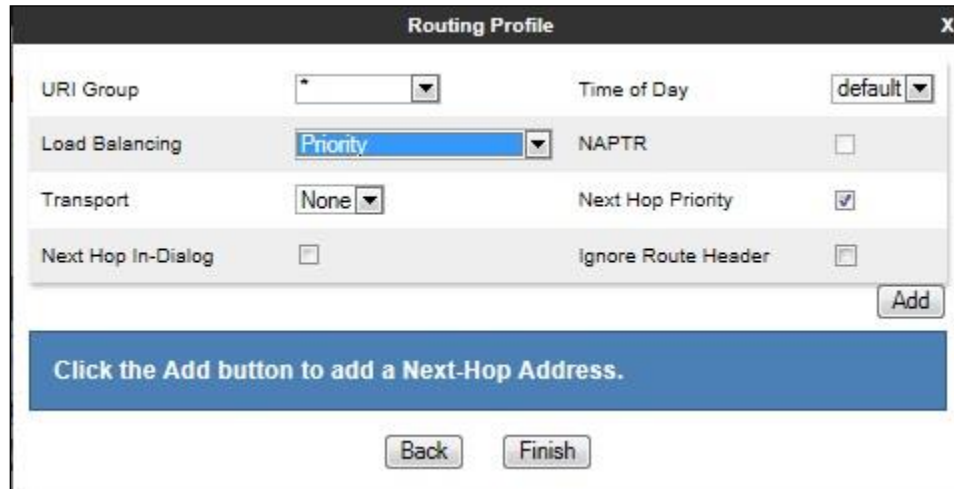
- **Priority/Weight = 1.**
- **SIP Server Profile = Avaya (Section 7.6.1)** from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5061(TLS)** from drop down menu.
- Click **Finish**.

## 7.7.2. Routing – Vodafone

Create a Routing Profile for Vodafone SIP network.

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

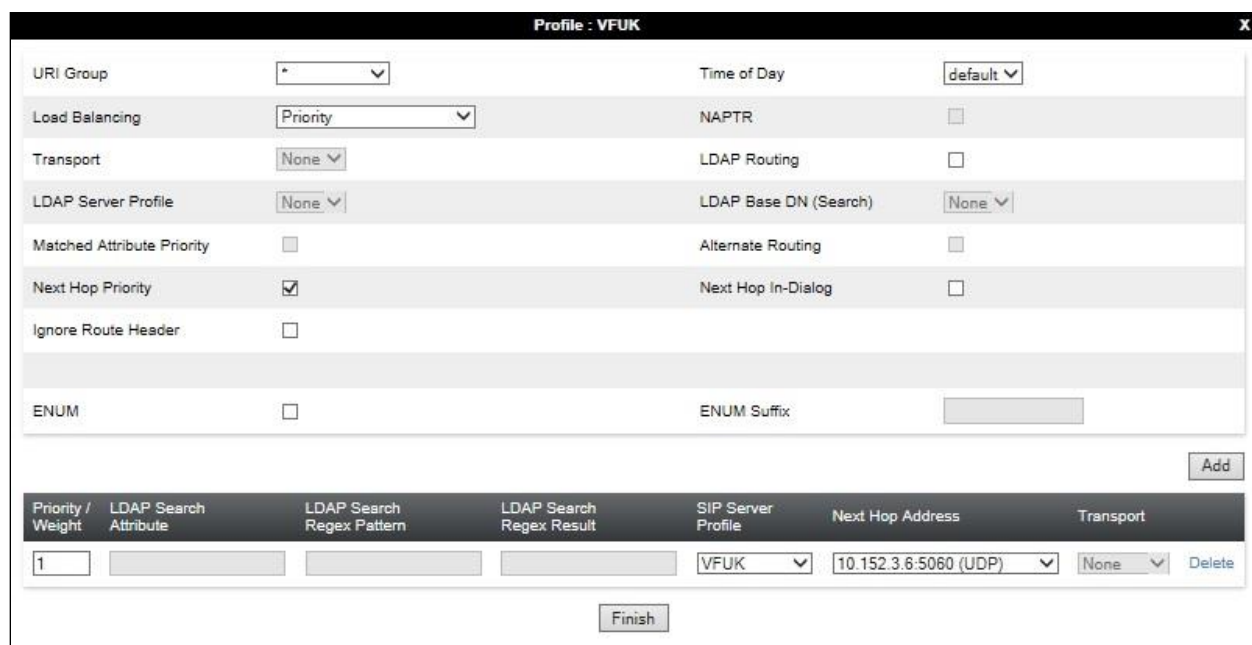
The Routing Profile window will open. Use the default values displayed and click **Add**.



The screenshot shows the 'Routing Profile' window. It contains several configuration fields: 'URI Group' (dropdown with '\*'), 'Time of Day' (dropdown with 'default'), 'Load Balancing' (dropdown with 'Priority'), 'NAPTR' (checkbox, unchecked), 'Transport' (dropdown with 'None'), 'Next Hop Priority' (checkbox, checked), 'Next Hop In-Dialog' (checkbox, unchecked), and 'Ignore Route Header' (checkbox, unchecked). An 'Add' button is located at the bottom right. Below the form 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.**
- **SIP Server Profile = VFUK (Section 7.6.2)** from drop down menu.
- **Next Hop Address = Select 10.152.3.6:5060 (UDP)** from drop down menu.
- Click **Finish**.



The screenshot shows the 'Profile : VFUK' window. It contains configuration fields for 'URI Group', 'Time of Day', 'Load Balancing', 'NAPTR', 'Transport', 'LDAP Server Profile', 'LDAP Base DN (Search)', 'Matched Attribute Priority', 'Alternate Routing', 'Next Hop Priority', 'Next Hop In-Dialog', 'Ignore Route Header', 'ENUM', and 'ENUM Suffix'. An 'Add' button is at the bottom right. Below the form is a table with the following columns: 'Priority / Weight', 'LDAP Search Attribute', 'LDAP Search Regex Pattern', 'LDAP Search Regex Result', 'SIP Server Profile', 'Next Hop Address', 'Transport', and 'Delete'. The table contains one row with the following values: '1', an empty field, an empty field, an empty field, 'VFUK', '10.152.3.6:5060 (UDP)', 'None', and a 'Delete' link. A 'Finish' button is located at the bottom center.

## 7.8. Topology Hiding

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

To define Topology Hiding for Session Manager, navigate to **Configuration 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

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

Edit

To define Topology Hiding for Vodafone, navigate to **Configuration 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

**Topology Hiding Profiles**  
 default  
 cisco\_th\_profile  
 Avaya  
**VFUK**

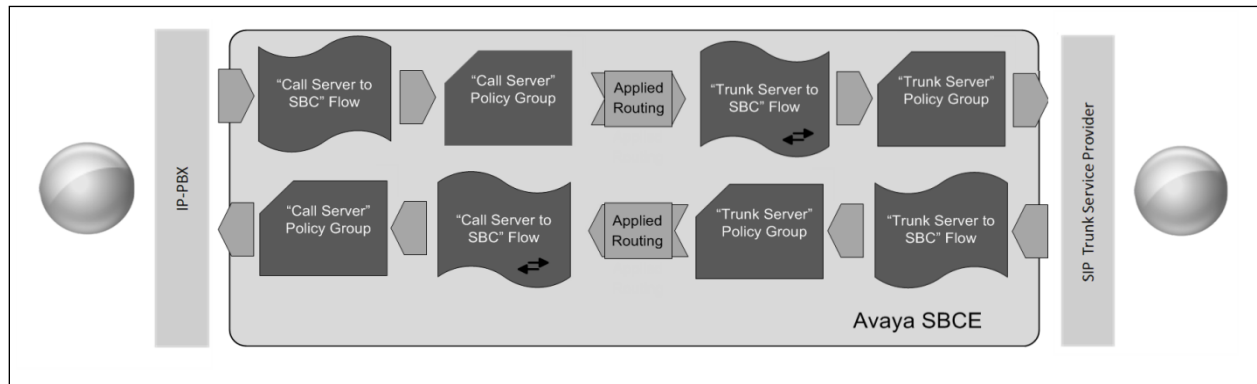
Click here to add a description.

**Topology Hiding**

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

## 7.9. Server Flows

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



This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Vodafone's SIP platform and vice versa. The following screenshot shows all configured flows.

**End Point Flows**

Subscriber Flows **Server Flows** Add

Modifications made to a Server Flow will only take effect on new sessions.

[Click here to add a row description.](#)

**SIP Server: Avaya**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Sig_Ext	Sig_Int	default-low	VFUK	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

**SIP Server: VFUK**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server	*	Sig_Int	Sig_Ext	default-low	Avaya	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

To define a Server Flow for the Vodafone SIP Trunk, navigate to **Network & Flows → 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 Vodafone SIP Trunk, in the test environment **Trunk\_Server** was used.
- In the **Server Configuration** drop-down menu, select the Vodafone server configuration defined in **Section 7.6.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone SIP Trunk defined in **Section 7.8** and click **Finish** (not shown).

Criteria	
Flow Name	Trunk_Server
Server Configuration	VFUK
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Int

Profile	
Signaling Interface	Sig_Ext
Media Interface	Med_Ext
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	VFUK
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

To define an incoming server flow for Session Manager from the Vodafone network, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call\_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.6.1**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone SIP Trunk defined in **Section 7.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish** (not shown).

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

Criteria		Profile	
Flow Name	Call_Server	Signaling Interface	Sig_Int
Server Configuration	Avaya	Media Interface	Med_Int
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	default-low
Remote Subnet	*	Routing Profile	VFUK
Received Interface	Sig_Ext	Topology Hiding Profile	Avaya
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	<input type="checkbox"/>

## 8. Configure the Vodafone SIP Trunk Equipment

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

## 9. Verification Steps

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

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

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

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

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



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

To define the trace, navigate to **Monitoring & Logging → Trace** in the main menu on the left-hand side and select the **Packet Capture** tab.

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

**Trace: GSSCP\_R8**

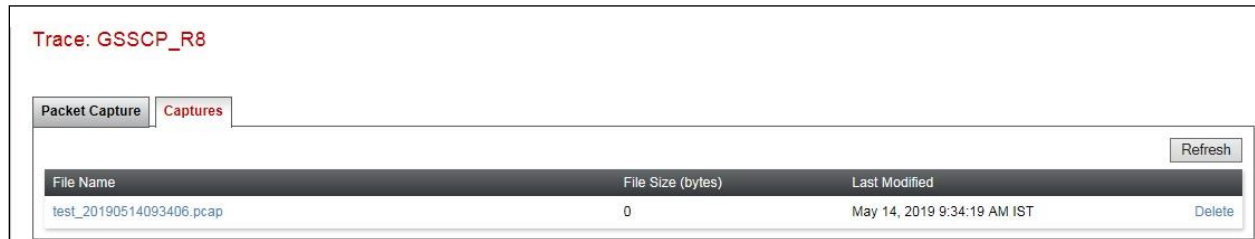
Packet Capture
Captures

**Packet Capture Configuration**

Status	Ready
Interface	B1 ▼
Local Address <small>IP[:Port]</small>	All ▼ : <input style="width: 50px;" type="text"/>
Remote Address <small>*, *:Port, IP, IP:Port</small>	<input style="width: 150px;" type="text" value="*"/>
Protocol	UDP ▼
Maximum Number of Packets to Capture	<input style="width: 50px;" type="text" value="10000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input style="width: 150px;" type="text" value="test.pcap"/>

Start Capture
Clear

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



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

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R8.1 as an Evolution Server, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.0 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] *Deploying Avaya Appliance Virtualization Platform*, Release 8.1, Jun 2019.
- [2] *Upgrading Avaya Aura® applications*, Release 8.1, Jun 2019.
- [3] *Deploying Avaya Aura® applications from System Manager*, Release 8.1, Jun 2019
- [4] *Deploying Avaya Aura® Communication Manager*, Release 8.1, Jul 2019
- [5] *Administering Avaya Aura® Communication Manager*, Release 8.1, Jul 2019
- [6] *Upgrading Avaya Aura® Communication Manager*, Release 8.1, Jun 2019
- [7] *Deploying Avaya Aura® System Manager Release 8.1*, Jul 2019
- [8] *Upgrading Avaya Aura® System Manager to Release 8.1*, Jul 2019.
- [9] *Administering Avaya Aura® System Manager for Release 8.1*, Jul 2019
- [10] *Deploying Avaya Aura® Session Manager*, Release 8.1 Jun 2019
- [11] *Upgrading Avaya Aura® Session Manager Release 8.1*, Jun 2019
- [12] *Administering Avaya Aura® Session Manager Release 8.1*, Jun 2019
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 8.0*, Jul 2019
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 8.0*, Jul 2019
- [15] *Administering Avaya Session Border Controller for Enterprise Release 8.0*, Jul 2019
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

---

**©2019 Avaya Inc. All Rights Reserved.**

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

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