



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1 to support Deutsche Telefon SIP Tk-Anlagenanschluss - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Deutsche Telefon SIP Tk-Anlagenanschluss and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server.

The Deutsche Telefon SIP Tk-Anlagenanschluss provides PSTN access via a SIP Trunk connected to the Deutsche Telefon Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks. Deutsche Telefon is a member of the Avaya 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.

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

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Deutsche Telefon SIP Tk-Anlagenanschluss (SIP Trunk) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R7.0.1; Avaya Aura® Session Manager R7.0.1; Avaya Session Border Controller for Enterprise R7.1; Endpoints as described in **Section 3**. Note that the shortened names Communication Manager, Session Manager and Avaya SBCE will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with the Deutsche Telefon SIP Trunk 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 connect to the Deutsche Telefon SIP Trunk.

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.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using Deutsche Telefon SIP Trunk, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via Deutsche Telefon SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator and Avaya Communicator for Windows soft phones.
- Calls using the G.711A Law codec.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media between the Avaya SBCE and the SIP and H.323 telephones.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by the Deutsche Telefon SIP Trunk requiring Avaya response and sent by Avaya requiring Deutsche Telefon response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Deutsche Telefon SIP Trunk with the following observations:

- During testing, duplicate INVITE messages were observed on some incoming calls. These were consistent with a retransmission that would occur when no response was received within half a second. This was assumed to be due to delays in the test network.
- Duplicate INVITE messages were also observed on some outgoing calls and both received a “407 Proxy Authentication Required” response from the network. These were consistent with a retransmission that would occur when no response was received within half a second. This was assumed to be due to delays in the test network.
- On the first attempt at an outgoing call from a SIP extension that was cleared from the terminating end, the SIP phone remained active after the BYE was received even though the BYE was acknowledged with 200 OK. This was not observed on subsequent calls. The internal IP codec list was changed at this point to include G.729A
- Codec test calls from a 1600 IP Deskphone did not release correctly. This was found to be related to the issue for call hold test 7.9.3 and was seen because of a re-INVITE triggered when sending DTMF.
- When attempting to put an outbound call on hold, Communication Manager sends an INVITE without SDP in the first step towards changing the media path to the G430 Media Gateway. The network responded with 200 OK with SDP. The SBCE did not send this 200 OK on to Communication Manager and the call failed. A fault report, AURORA-10162, was raised and a patch was provided that was tested successfully. The patch will be incorporated into Feature Pack 2 due for release at the end of February 2017.
- With the previous issue resolved, it was found that the media path was not fully restored when an outbound call was taken off hold. When the re-INVITE message to place the call on hold with “sendonly” in the SDP was sent, the network responded with a 200 OK with “sendrecv” in the SDP. This should have been “recvonly”. This was resolved using the “Delayed SDP” setting in the Avaya SBCE that inserts an SDP in the re-INVITE that is used to change the media path to the Media Gateway when a call is put on hold and back again when the call is taken off hold.
- When conferencing inbound and outbound calls with PSTN phones, “486 Busy Here” was received from the network when attempting to conference a second PSTN phone. This was taken to be a service limitation and not an interworking issue.
- An issue exists on the Avaya SBCE at build 7.1 SP 1 that causes T.38 fax to fail. This is resolved in build 7.1 Feature Pack 2 available at the end of February 2017. A patch was used in the test environment that allowed successful testing of T.38 fax. In the Live environment upgrade of the Avaya SBCE should be postponed until FP2 is available or G.711 should be used as a workaround. Fax transmission using G.711 was tested successfully.
- When testing Avaya one-X® Communicator in “Other phone” mode, the network declined the call when the “Other Phone” was a PSTN phone. Testing was carried out using a Communication Manager extension as the “Other Phone”.

- When testing one-X® Communicator in “Other Phone” mode and connected as a SIP endpoint, there was no ringback on outbound calls when Initial IP-IP Direct Media was set to “y”. This was set to “n” in the signalling group for the SIP endpoints.
- Network Call Redirect using REFER was not supported. The network responded to the REFER messages with 603 Declined.

Items not tested include the following:

- No Inbound Toll-Free access was available for testing
- No test call was made to Emergency Services as a test call was not 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 Deutsche Telefon products described in these Application Notes, please contact Deutsche Telefon Customer Support at:

- Mail: service@deutsche-telefon.de
- Tel: +49 800 580 2008

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Deutsche Telefon SIP Trunk. Located at the enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series IP telephones (with SIP and H.323 firmware), Avaya 1600 series IP telephone (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Communicator for Windows running on laptop PCs.

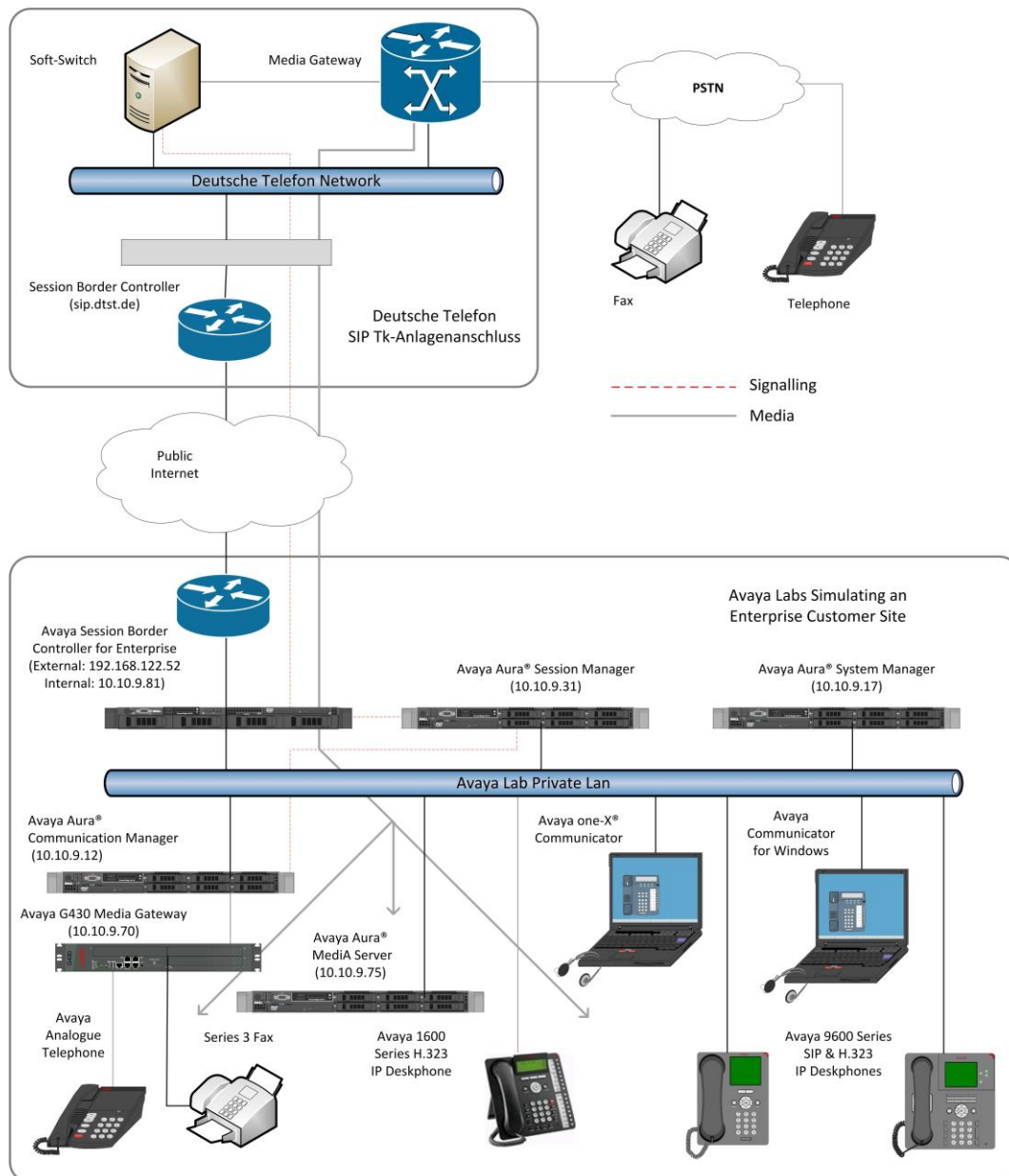


Figure 1: Test Setup Deutsche Telefon SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.1.0.701007
Avaya Aura® System Manager	7.0.1.0.65071 – SP1
Avaya Aura® Communication Manager	7.0.1.1.1 0-23384 – FP1 SP1
Avaya Session Border Controller for Enterprise	7.1.0.1-07-12090 – SP1
Media Server	7.7.0.334
Avaya G430 Media Gateway	37.39.0
Avaya IP Deskphones: SIP 96x0 SIP 9608 H.323 96x0 H.323 9608 H.323 1616	2.6.16 7.0.1.1 r5 3.2.6A 6.6.2.29 1.3.9
Avaya One-X Communicator	6.2.11.03 – SP11
Avaya Communicator for Windows	2.1.4.84
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
Deutsche Telefon	
Kamailio SIP Server	4.1.3
Mediaproxy-ng	2.3.6.3

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 Deutsche Telefon 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. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Deutsche Telefon 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 Deutsche Telefon SIP Trunk and any other SIP trunks used.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		4000	0
Maximum Concurrently Registered IP Stations:		2400	3
Maximum Administered Remote Office Trunks:		4000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		68	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		2400	0
Maximum Video Capable IP Softphones:		2400	0
Maximum Administered SIP Trunks:		4000	20
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0

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

display system-parameters customer-options		Page 5 of 12
OPTIONAL FEATURES		
Emergency Access to Attendant? y		IP Stations? y
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
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 using the **change node-names ip** command. In this case, **Session_Manager** and **10.10.9.31** are the **Name** and **IP Address** for Session Manager SIP interface. Also note the **procr** IP address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

change node-names ip		IP NODE NAMES
Name	IP Address	
AMS	10.10.9.75	
Session_Manager	10.10.9.31	
default	0.0.0.0	
procr	10.10.9.12	
procr6	::	

5.3. Administer IP Network Region

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

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

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

Note: In the test configuration, ip-network-region 1 was used within the enterprise and ip-network-region 2 was used for the SIP Trunk.

5.4. Administer IP Codec Set

Use the **change ip-codec set n** command where **n** is 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 preferred by Deutsche Telefon was configured, namely **G.711A**.

change ip-codec-set 2				Page	1 of	2
IP CODEC SET						
Codec Set: 2						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size (ms)			
1: G.711A	n	2	20			
2:						

The preferred method of transmission of fax is T.38. Navigate to **Page 2** and define T.38 fax as follows:

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

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

Note: An issue with T.38 fax on the Avaya SBCE is described in **Section 2.2**; this issue is present in Avaya SBCE Release 7.1 Service Pack 1 and is resolved in Feature Pack 2. If upgrade to Service Pack 1 is required or has already taken place, fax has been tested successfully using G.711. If required, set **FAX Mode** to **off**.

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Deutsche Telefon SIP Trunk. During test, this was configured to use TCP and port 5060.

Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to required protocol. Although TLS is recommended for security, **tcp** was used during testing.
- Set **Peer Detection Enabled** to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to Session Manager interface (node name **Session_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required, during testing, **5060** was used. These must correspond to those used on the Session Manager Entity Links (See **Section 6.5**).
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3** (logically establishes the far-end for calls using this signalling group as region **2**).
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **DTMF over IP** to **rtp--payload** which uses telephone events according to RFC 2833 for DTMF transmission.
- Set **Direct IP-IP Audio Connections** to **y** to avoid unnecessary use of resources
- Set **Initial IP-IP Direct Media** and **H.323 Station Outgoing Direct Media** to **y**. This initiates direct media when the call is set up without the need for shuffling.

add signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: Session_Manager	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 2	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? y	
H.323 Station Outgoing Direct Media? y	Alternate Route Timer(sec): 6	

5.6. Administer SIP Trunk Group

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

- Set the **Group Type** field to **sip**.
- Choose a descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **public-ntwrk** if the Diversion header is to be supported.
- 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** supported by this SIP trunk group.

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: SIP_Trunk	COR: 1	TN: 1	TAC: 102
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: 2	
		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 Deutsche Telefon to prevent unnecessary SIP messages during call setup. During testing, a value of **90** was used that sets the SIP Min-SE header to 180.

add trunk-group 2		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
		Preferred Minimum Session Refresh Interval(sec): 90	
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to **private** if national numbering is to be used as was the case during testing. If E.164 with preceding “+” is to be used, select public.

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

On **Page 4** of this form:

- Set **Network Call Redirection** to **y** to allow redirection using “302 Moved Temporarily” if required.
- Set **Send Diversion Header** to **y** so that the DDI number assigned to the extension is passed for forwarded calls.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Deutsche Telefon (this Payload Type is not applied to calls from SIP end-points).
- Set **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on Communication Manager extension.

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

Note: While Network Call Redirection using “302 Moved Temporarily” was successfully tested, redirection using REFER is not supported as described in **Section 2.2**.

5.7. Administer Calling Party Number Information

Use the **change private-numbering** command to configure Communication Manager to send the calling party number in national format. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	2	1		4	Total Administered: 10
4	600	2	0613132nnnn9	12	Maximum Entries: 540
4	2000	2	0613132nnnn0	12	
4	2001	2	0613132nnnn8	12	
4	2291	2	0613132nnnn2	12	
4	2316	2	0613132nnnn3	12	
4	2391	2	0613132nnnn1	12	
4	2400	2	0613132nnnn4	12	
4	2401	2	0613132nnnn7	12	
4	7000	2	0613132nnnn5	12	

Use the **change public-unknown-numbering** command if it has been agreed with Deutsche Telefon to use E.164 numbering. Communication Manager automatically prefixes a "+" to the numbers when this table is used. This table is also used for the Contact header in SIP responses for incoming calls even where private has been selected in the Numbering format in the Trunk settings.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2	1		4	Total Administered: 10
4	600	2	49613132nnnn9	13	Maximum Entries: 240
4	2000	2	49613132nnnn0	13	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	2001	2	49613132nnnn8	13	
4	2291	2	49613132nnnn2	13	
4	2316	2	49613132nnnn3	13	
4	2391	2	49613132nnnn1	13	Communication Manager automatically inserts a '+' digit in this case.
4	2400	2	49613132nnnn4	13	
4	2401	2	49613132nnnn7	13	
4	7000	2	49613132nnnn5	13	

Note: During testing the extension numbers were reformatted to national numbers for Trunk Group 2 only. The numbers were analysed for Trunk Group 1 but not reformatted.

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Deutsche Telefon network. 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: 8	
Auto Route Selection (ARS) - Access Code 1: 9 Access Code 2:	

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls with leading **0**. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. The example shows international numbers with country code **353** for Ireland and area code **91** for Galway. Calls are sent to **Route Pattern 2**.

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	8	12	2	pubu		n	
00	13	15	2	pubu		n	
0035391	13	13	2	pubu		n	
1	3	4	2	pubu		n	
118	5	6	2	pubu		n	

Use the **change route-pattern n** command, where **n** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **2** is used to route calls to trunk group **2**. **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 2										Page 1 of 3
Pattern Number: 2 Pattern Name: SIP_Endpoints										
SCCAN? n Secure SIP? n Used for SIP stations? n										
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC		
No			Mrk	Lmt	List	Del	Digits	QSIG		
							Dgts	Intw		
1:	2	0						n	user	
2:								n	user	
3:								n	user	
4:								n	user	
5:								n	user	
6:								n	user	
	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM Sub	Numbering	LAR
	0	1	2	M	4	W	Request	Dgts	Format	
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 Communication Manager extensions. The incoming digits sent in the INVITE message from Deutsche Telefon can be manipulated as necessary to route calls to the desired extension. Use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**. In the example shown, 12 digits numbers are received in national format. All digits are deleted and the extension number is inserted. Note that some of the DDI digits have been obscured.

change inc-call-handling-trmt trunk-group 2										Page 1 of 3
INCOMING CALL HANDLING TREATMENT										
Service/	Number	Number	Del		Insert					
Feature	Len	Digits								
public-ntwrk	12	0613132nnnn0	12		2000					
public-ntwrk	12	0613132nnnn1	12		2391					
public-ntwrk	12	0613132nnnn2	12		2291					
public-ntwrk	12	0613132nnnn3	12		2316					
public-ntwrk	12	0613132nnnn4	12		2400					
public-ntwrk	12	0613132nnnn5	12		7000					
public-ntwrk	12	0613132nnnn6	12		3					
public-ntwrk	12	0613132nnnn7	12		2401					
public-ntwrk	12	0613132nnnn8	12		2001					
public-ntwrk	12	0613132nnnn9	12		6002					
public-ntwrk										

5.10. EC500 Configuration

When EC500 is enabled on a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2291. Use the command **change off-pbx-telephone station-mapping x** where **x** is a Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **00353914nnnn3**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 2291							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2291	OPS	-		2291	aar	1	
2291	EC500	-		00353914nnnn3	ars	1	

Note: The phone number shown is for a test phone in the Avaya Lab. To use facilities such as Feature Name Extension (FNE) for calls coming in from EC500 mobile phones, the calling party number received in Communication Manager must exactly match the number specified in the above table.

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

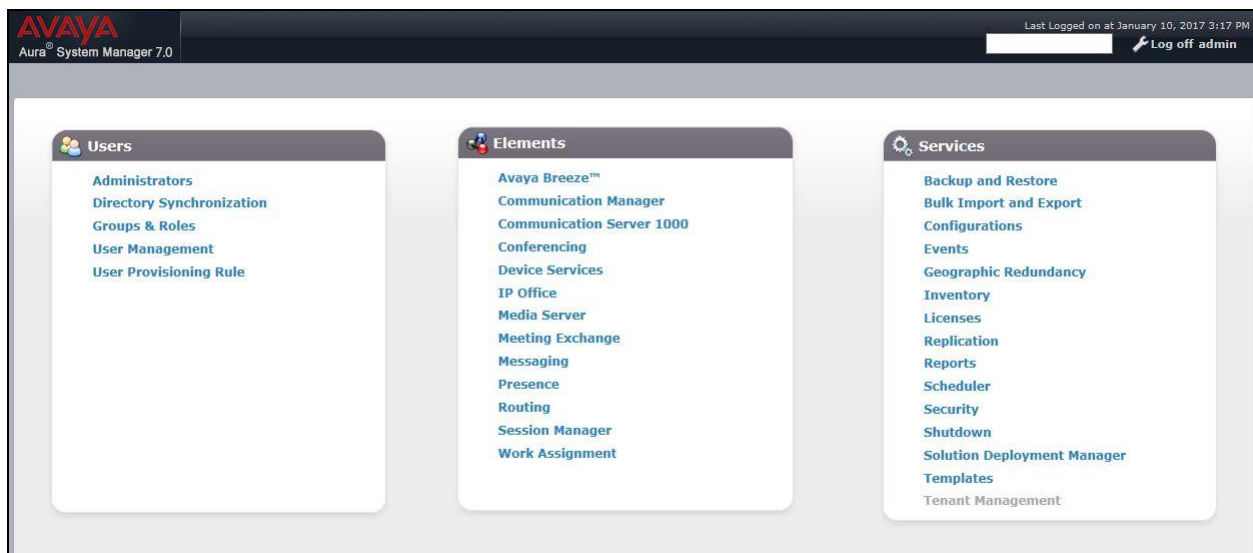
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured by opening a web browser to the System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

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



6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Elements, Home** screen menu and in the resulting tab select **Domains** from the left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name of the enterprise site or a name agreed with Deutsche Telefon; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on Communication Manager. Refer to **Section 5.3** for details. In test, **avaya.com** was used. Optionally, a description for the domain can be entered in the **Notes** field. Click **Commit** to save changes.

The screenshot shows the 'Domain Management' interface. On the left is a navigation menu with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table lists 1 item with columns for Name, Type, and Notes. The item 'avaya.com' is listed with Type 'sip'. A 'Filter: Enable' link is on the right. At the bottom, it says 'Select : All, None'.

Name	Type	Notes
avaya.com	sip	

Note: If the existing domain name used in the enterprise equipment does not match that used in the network, a Session Manager Adaptation can be used to change it (see **Section 6.4**).

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management and Session Manager routing. One location is added to the sample configuration for all of the enterprise SIP entities and another for the Deutsche Telefon SIP Trunk. On the **Routing** tab select **Locations** from the left hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Define bandwidth requirements, during testing these were left at default values.

Home / Elements / Routing / Locations

Location Details

CommitCancel

General

* Name:Galway_Lab

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:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):2000Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):2000Kbit/Sec

* Minimum Multimedia Bandwidth:64Kbit/Sec

* Default Audio Bandwidth:80Kbit/sec

Alarm Threshold

Overall Alarm Threshold:80%

Multimedia Alarm Threshold:80%

* Latency before Overall Alarm Trigger:5Minutes

* Latency before Multimedia Alarm Trigger:5Minutes

The location pattern is a way of using subnets to further refine the location information, this may be useful for endpoints that could be logged in from different subnets. This was not used during testing. If required, scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string.

Although routing based on location was not used on Session Manager during testing, a separate location was defined for the Deutsche Telefon SIP Trunk called Service_Provider. The bandwidth parameters were left at default values and are not shown here.

6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers, during compliance testing, two were used. One Adaptation was used on the Communication Manager SIP Entity to convert the Calling Party Numbers sent from Session Manager to diallable formats for display on Communication Manager extensions. The other was used on the Avaya SBCE SIP Entity to remove Avaya proprietary headers from messages sent from Session Manager.

6.4.1. Communication Manager

Calling Party Numbers were received from the network in E.164 format with leading “+”, so the Adaption was used to convert to national numbers with a single zero and international numbers with two zeros.

On the **Routing** tab select **Adaptations** from the left-hand menu. Click on **New** (not shown).

- In the **Adaptation Name** field, enter a descriptive title for the adaptation. During testing **Diallable** was used.
- In the **Module Name** drop down menu, select **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module Parameter Type** drop down menu, select **Name-Value Parameter**.
- In the **Name** field, type **fromto**.
- In the **Value** field, type **true**.
- Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of originating numbers going to Communication Manager.

Home / Elements / Routing / Adaptations Help ?

Adaptation Details

Commit Cancel

General

* **Adaptation Name:**

* **Module Name:**

Module Parameter Type:

Add Remove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+	*12	*15		*1	00	origination		
<input type="checkbox"/>	*+49	*12	*15		*3	0	origination		

Select : All, None

Commit Cancel

The screenshot shows how the calling party numbers in messages going to Communication Manager were analysed for testing. Numbers beginning with “+49” were prefixed with 0 for national numbers and numbers beginning with “+” and any other country code were prefixed with 00 for international numbers.

6.4.2. Avaya SBCE

Communication Manager and Session Manager make use of Avaya proprietary SIP headers to facilitate the full suite of Avaya functionality within the enterprise. These are not required on the SIP trunk however, and make the SIP messages unnecessarily large. A Session Manager Adaptation is used to remove proprietary headers. On the **Routing** tab select **Adaptations** from the left-hand menu. Click on **New** (not shown).

- In the **Adaptation Name** field, enter a descriptive title for the adaptation.
- In the **Module Name** drop down menu, select **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module Parameter Type** drop down menu, select **Name-Value Parameter**.
- In the **Name** box, type **eRHdrs**
- In the **Value** box, type the list of headers to be deleted. During testing, the following list was used: **"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, P-Conference, Alert-Info"**.
- In **Digit Conversion for Outgoing Calls from SM**, specify the common digits in the Calling Party Number from Communication Manager in the **Matching Pattern** such that a match is found for all outgoing calls.

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel Help ?

General

* Adaptation Name:

* Module Name:

Module Parameter Type:

Name	Value
<input type="checkbox"/> eRHdrs	"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, P-Conference, Alert-Info"
<input type="checkbox"/> fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/> +496131nnnn6	<input type="text" value="14"/>	<input type="text" value="14"/>	<input type="text" value="14"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="origination"/>	<input type="text"/>	<input type="text"/>

Select : All, None

Commit Cancel

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 **Adaptation** field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are four SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity for the SIP Endpoints.
- Avaya Aura® Communication Manager SIP Entity for the SIP Trunk.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity for PSTN destinations.

There is also a SIP Entity for Avaya Aura® Messaging but that is not described in this document.

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.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Session_Manager

* FQDN or IP Address: 10.10.9.31

Type: Session Manager

Notes:

Location: Galway_Lab

Outbound Proxy:

Time Zone: Europe/Dublin

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The 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 **Listen Ports**, click **Add**, then edit the fields in the resulting new row.

- In the **Listen Ports** 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.
- Click on **Commit** (not shown).

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

3 Items Filter: Enable

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

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entities

The following screen shows one of the SIP entities for Communication Manager which is configured as an Evolution Server. This SIP Entity is used for the SIP Trunk. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the Adaptation to that defined in **Section 6.4** and set the **Location** to that defined in **Section 6.3**.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: CM Trunk

*** FQDN or IP Address:** 10.10.9.12

Type: CM

Notes:

Adaptation: Diallable

Location: Galway_Lab

Time Zone: Europe/Dublin

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

Credential name:

Securable: ☐

Call Detail Recording: none

Commit **Cancel**

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: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Note: The Adaptation assigned is that defined in **Section 6.4.1**. Note also that a second SIP Entity for Communication Manager is required for SIP Endpoints. In the test environment this is named “CM_SIP_Endpoints”. The parameters are the same apart from the Adaptation, and the two are assigned to different Entity Links, as described in **Section 6.6**, so that different ports can be used. It is these different ports that distinguish between traffic for SIP Endpoints and traffic for the SIP Trunk.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The screenshot shows the SIP Entity for the Avaya SBCE used for PSTN destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface used for PSTN fixed calls (see **Figure 1**). Set the **Adaptation** to that defined in **Section 6.4.2**, the **Location** to that defined in **Section 6.3** for the SIP Trunk, and the **Time Zone** to the appropriate time zone.

The screenshot displays the 'SIP Entity Details' configuration page. At the top right are 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

- Name:** ASBCE
- FQDN or IP Address:** 10.10.9.81
- Type:** SIP Trunk (dropdown menu)
- Notes:** (empty text field)
- Adaptation:** Header_Removal (dropdown menu)
- Location:** Service_Provider (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress (dropdown menu)

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. Fill in the following fields in the new row that is displayed (not shown).

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- 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.
- Leave the **Connection Policy** drop down menu at the default value of **trusted** to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- Click **Commit** (not shown) to save changes. The screenshot shows the Entity Links used in this configuration.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	ASBCE Link	Session_Manager	TCP	5060	ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM Endpoint link	Session_Manager	TLS	5061	CM_SIP_Endpoints	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM Trunk Link	Session_Manager	TCP	5060	CM Trunk	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging Link	Session_Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Note: There are two Entity Links for Communication Manager, one for the SIP Endpoints and the other for the SIP Trunk. These are differentiated by port number. The **Messaging Link** Entity Link is used for the Avaya Aura® Messaging system and is not described in this document.

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, defined in **Section 6.5**, to which this routing policy applies (not shown).
- Under **Time of Day**, click **Add**, and then select the time range. **24/7** is provided as a default.

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

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM Trunk	10.10.9.12	CM	

Time of Day

1 Item Filter: Enable

<input type="checkbox"/>	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 interface that will be routed to PSTN destinations via Deutsche Telefon SIP Trunk.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.10.9.81	SIP Trunk	

Time of Day

1 Item Filter: Enable

<input type="checkbox"/>	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

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 one of the locations 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 which will route all calls starting with zero to the PSTN via Deutsche Telefon SIP Trunk.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		PSTN_Outbound	0	<input type="checkbox"/>	ASBCE	

Select : All, None

Note: Additional dial patterns (not shown) will be required for PSTN numbers that do not start with zero, for example directory enquiries. This was tested with a dial pattern for 4 digit numbers starting with 1.

The next screenshot shows the test dial pattern configured for Communication Manager. This is used to analyze the DDI numbers assigned to the extensions on Communication Manager. Some of the digits of the pattern to be matched have been obscured.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 06131nnnn6

* Min: 12

* Max: 12

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- v

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Service_Provider		CM_Inbound	0	<input type="checkbox"/>	CM Trunk	

Select : All, None

Note: A specific location for the SIP Trunk was used for routing to Communication Manager. If required, an additional policy could be added to route calls differently if they originated within the enterprise. This may be useful if there is a requirement to route calls from one Communication Manager DDI number to another via the network.

6.9. Administer Application for Avaya Aura® Communication Manager

From the **Home** screen select **Session Manager** from the Elements menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New** (not shown).

- In the **Name** field enter a name for the application.
- In the **SIP Entity** field select the SIP Entity for Communication Manager Endpoints described in **Section 6.5**.
- In the **CM System for SIP Entity** field select the appropriate Communication Manager from the System Manager inventory and select **Commit** to save the configuration.

The screenshot shows the Avaya Aura Session Manager web interface. The top navigation bar includes 'Home' and 'Session Manager'. The left sidebar menu is expanded to 'Session Manager', showing options like 'Dashboard', 'Session Manager Administration', 'Communication Profile Editor', 'Network Configuration', 'Device and Location Configuration', 'Application Configuration', and 'Applications'. The main content area is titled 'Application Editor' and contains a form for creating or editing an application. The form fields are: 'Name' (text input with 'CM_App'), 'SIP Entity' (dropdown menu with 'CM_SIP_Endpoints'), 'CM System for SIP Entity' (dropdown menu with 'CM1_Element' and a 'Refresh' button), and 'Description' (text input). There are 'Commit' and 'Cancel' buttons at the top right of the form. A breadcrumb trail at the top of the main area reads 'Home / Elements / Session Manager / Application Configuration / Applications'. A 'View/Add CM Systems' link is also visible next to the 'CM System for SIP Entity' dropdown.

Note: The Application described here and the Application Sequence described in the next section are likely to have been defined during installation. The configuration is shown here for reference. Note also that the Communication Manager SIP Entity selected is that set up specifically for SIP endpoints. In the test environment there is also a Communication Manager SIP Entity that is used specifically for the SIP Trunk and is not to be used in this case.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New** (not shown).

- In the **Name** field enter a descriptive name.
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading. Select **Commit**.

The screenshot shows the 'Application Sequence Editor' window. At the top, the breadcrumb navigation is 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The window title is 'Application Sequence Editor' with 'Commit' and 'Cancel' buttons. Below the title bar, there's a section for 'Application Sequence' with fields for '*Name' (containing 'CM_App_Seq') and 'Description'. Below this is a section titled 'Applications in this Sequence' with 'Move First', 'Move Last', and 'Remove' buttons. It shows '1 Item' in a table with columns: Sequence Order (first to last), Name, SIP Entity, Mandatory, and Description. The table contains one row with a checkbox, a plus icon, 'CM_App', 'CM_SIP_Endpoints', a checked 'Mandatory' box, and an empty 'Description' field. Below the table is a 'Select : All, None' dropdown. At the bottom is an 'Available Applications' section with '1 Item' and a 'Filter: Enable' link. It contains a table with columns 'Name', 'SIP Entity', and 'Description', showing one row with a plus icon, 'CM_App', 'CM_SIP_Endpoints', and an empty 'Description' field. At the very bottom, there's a '*Required' label and 'Commit' and 'Cancel' buttons.

Home / Elements / Session Manager / Application Configuration / Application Sequences [Help ?](#)

Application Sequence Editor

Application Sequence

*Name

Description

Applications in this Sequence

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		CM_App	CM_SIP_Endpoints	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item [Filter: Enable](#)

	Name	SIP Entity	Description
	CM_App	CM_SIP_Endpoints	

*Required

6.11. Administer SIP Extensions

The SIP extensions are likely to have been defined during installation. The configuration shown in this section is for reference. SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** screen select **User Management** from the **Users** menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields.
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. **2291@avaya.com** which is used to create the user's primary handle.
- The **Authentication Type** should be **Basic**.
- In the **Password/Confirm Password** fields enter an alphanumeric password.
- Set the **Language Preference** and **Time Zone** as required.

The screenshot shows the 'New User Profile' form in the Avaya User Management interface. The form is divided into tabs: Identity (selected), Communication Profile, Membership, and Contacts. The Identity tab contains the following fields:

- User Provisioning Rule:** A dropdown menu.
- Identity:**
 - Last Name:** SIP
 - Last Name (Latin Translation):** SIP
 - First Name:** 9608
 - First Name (Latin Translation):** 9608
 - Middle Name:**
 - Description:**
 - Login Name:** 2291@avaya.com
 - User Type:** Basic
 - Password:** [masked]
 - Confirm Password:** [masked]
 - Localized Display Name:**
 - Endpoint Display Name:**
 - Title:**
 - Language Preference:** English (United Kingdom)
 - Time Zone:** (+1:0)GMT : Dublin, Edinburgh
 - Employee ID:**
 - Department:**
 - Company:**

In the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it.


The screenshot shows the 'Communication Profile' tab in a web interface. At the top, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. Below the tabs, there is a section for 'Communication Profile' with two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below the passwords, there is a table with one row: 'Primary'. The 'Name' field is set to 'Primary' and the 'Default' checkbox is checked. Below the table, there is a section for 'Communication Address' with a table that has three columns: 'Type', 'Handle', and 'Domain'. The table is empty, showing 'No Records found'. Below the table, there are two checkboxes: 'Session Manager Profile' and 'CM Endpoint Profile'. At the bottom right, there are buttons for 'Commit & Continue', 'Commit', and 'Cancel'. A legend at the bottom left indicates that an asterisk (*) denotes a required field.

Expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.


The screenshot shows the 'Communication Address' section in a web interface. It has a table with three columns: 'Type', 'Handle', and 'Domain'. The table is empty, showing 'No Records found'. Below the table, there is a 'Type' field with a dropdown menu set to 'Avaya SIP'. Below that, there is a 'Fully Qualified Address' field with two input boxes: the first contains '2291' and the second contains 'avaya.com'. At the bottom right, there are buttons for 'Add' and 'Cancel'.

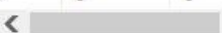
Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked.
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field.
- Select the appropriate application sequence from the drop-down menu in the **Origination Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.10**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.



☒ **Session Manager Profile** 

SIP Registration



- * Primary Session Manager
- Secondary Session Manager
- Survivability Server
- Max. Simultaneous Devices 
- Block New Registration When Maximum Registrations Active? ☐

Primary	Secondary	Maximum
6	0	6
		

Application Sequences

- Origination Sequence 
- Termination Sequence 

Call Routing Settings

- * Home Location 
- Conference Factory Set 

Call History Settings

- Enable Centralized Call History? ☐

Expand the **Endpoint Profile** section.

- Select Communication Manager Element from the **System** drop-down menu.
- Select **Endpoint** from the drop-down menu for **Profile Type**.
- Enter the extension in the **Extension** field.
- Select the desired template from the **Template** drop-down menu.
- In the **Port** field **IP** is automatically inserted.
- Enter a **Voice Mail Number** if required. In the test environment, this was **7000**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.

The screenshot shows the 'CM Endpoint Profile' configuration form. It includes fields for System (CM1_Element), Profile Type (Endpoint), Extension (2291), Template (9608SIP_DEFAULT_CM_7_0), Set Type (9608SIP), Security Code, Port (IP), Voice Mail Number (7000), Preferred Handle (None), and Sip Trunk (aar). There are also checkboxes for 'Use Existing Endpoints', 'Calculate Route Pattern', 'Enhanced Callr-Info display for 1-line phones', 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' (checked), 'Override Endpoint Name and Localized Name' (checked), and 'Allow H.323 and SIP Endpoint Dual Registration'. An 'Endpoint Editor' button is next to the Extension field.

Select **Commit** (Not Shown) to save changes and the System Manager will add Communication Manager user configuration automatically.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya 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.

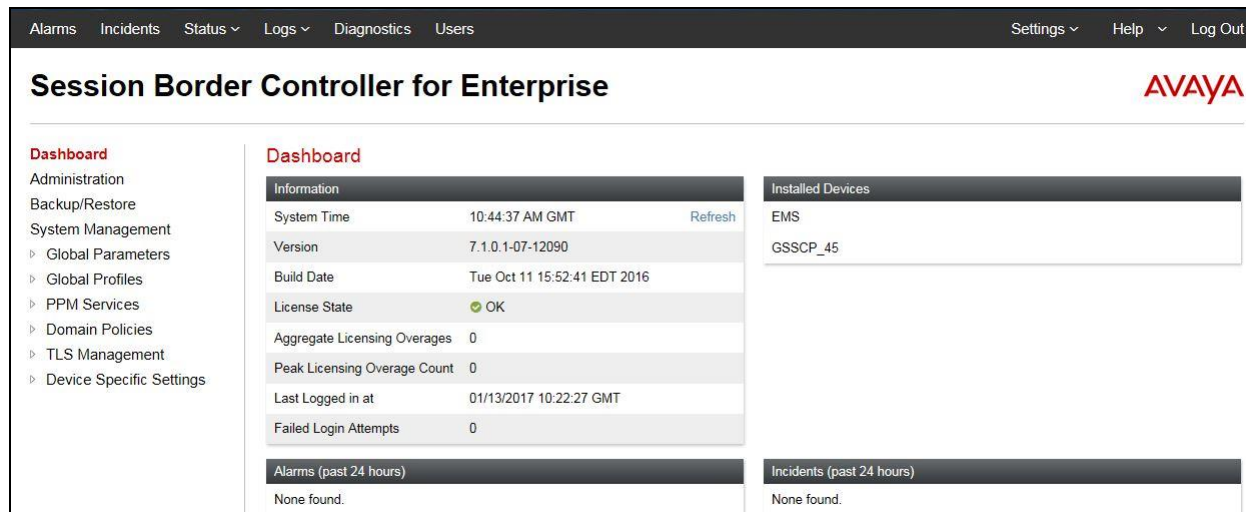
7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left is the Avaya logo and the product name. On the right, under the 'Log In' heading, there is a 'Username:' label followed by a text input field and a 'Continue' button. Below the login fields, there are three paragraphs of legal disclaimer text and a copyright notice at the bottom: '© 2011 - 2016 Avaya Inc. All rights reserved.'

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



The screenshot displays the main dashboard of the Avaya Session Border Controller for Enterprise. At the top, there is a navigation bar with links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various sections: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into several panels. The 'Dashboard' panel shows system information: System Time (10:44:37 AM GMT), Version (7.1.0.1-07-12090), Build Date (Tue Oct 11 15:52:41 EDT 2016), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (01/13/2017 10:22:27 GMT), and Failed Login Attempts (0). There are also sections for 'Alarms (past 24 hours)' and 'Incidents (past 24 hours)', both showing 'None found'. On the right, the 'Installed Devices' panel lists 'EMS' and 'GSSCP_45'.

7.2. Define Network Management

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

To define the network information, navigate to **Device Specific Settings** → **Network Management** in the main menu on the left hand side and click on **Add**.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address
------	---------	-----------------------------	-----------	------------

Enter details for the external interfaces in the dialogue box:

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

Name	Default Gateway	Network Prefix or Subnet Mask	Interface
External	192.168.122.9	255.255.255.128	B1

IP Address	Public IP	Gateway Override
192.168.122.46	Use IP Address	Use Default

Click on **Add** to define the internal interface. Enter details in the dialogue box (not shown):

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address for the Avaya SBCE 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: GSSCP_45

Devices: GSSCP_45

Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.81	Edit	Delete
External	192.168.122.9	255.255.255.128	B1	192.168.122.46	Edit	Delete

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

Network Management: GSSCP_45

Devices: GSSCP_45

Interfaces Networks

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Disabled

Message from webpage

Are you sure you wish to change the status of Interface to Enabled?

OK Cancel

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted. Click on **System Management** in the main menu (not shown) and select **Restart Application** indicated by an icon in the status bar (not shown).

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TCP used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the Deutsche Telefon SIP Trunk. A signalling and media interface was required on both the internal and external sides of the Avaya SBCE. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

7.3.1. Signalling Interfaces

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

- Select **Add** (not shown) and enter details of the external signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **192.168.122.46** for the Avaya SBCE interface on the SIP Trunk.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the Deutsche Telefon SIP Trunk.
- Click on **Finish**

The screenshot shows the 'Add Signaling Interface' configuration window. On the left is a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (selected), Network Management, Media Interface, **Signaling Interface** (highlighted in red), End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, and SNMP. The main configuration area has a title bar 'Add Signaling Interface' with a close button 'X'. Below the title bar is a blue warning message: 'TLS Port has been disabled because no TLS Server Profiles exist. Create a new [TLS Server Profile](#) to allow creation of a TLS enabled Signaling Interface.' The configuration fields are: Name (text box with 'External'), IP Address (dropdown menu with 'External (B1. VLAN 0)' selected, and a sub-dropdown with '192.168.122.46' selected), TCP Port (text box with 'Leave blank to disable' below it), UDP Port (text box with '5060' and 'Leave blank to disable' below it), TLS Port (text box with 'Leave blank to disable' below it), TLS Profile (dropdown menu with 'None' selected), Enable Shared Control (checkbox, unchecked), and Shared Control Port (text box). At the bottom right is a 'Finish' button.

The internal signalling interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TCP** port number, **5060** is used for Session Manager.

The following screenshot shows details of the signalling interfaces:

Signaling Interface: GSSCP_45

Devices

GSSCP_45

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
External	192.168.122.46 External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Internal	10.10.9.81 Internal (A1, VLAN 0)	5060	5060	---	None	Edit Delete

Note: In the test environment, the internal IP address was **10.10.9.81**.

7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** in the main menu on the left hand side. Details of the RTP 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.

- Select **Add** and enter details of the external media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **192.168.122.46**.
- Define the **RTP Port Range** for the media path with the Deutsche Telefon SIP Trunk, during testing this was left at default values of **35000 - 40000**.

System Management

Global Parameters

Global Profiles

PPM Services

Domain Policies

TLS Management

Device Specific Settings

Network Management

Media Interface

Add Media Interface

Name: External

IP Address: External (B1, VLAN 0) 192.168.122.46

Port Range: 35000 - 40000

Finish

The internal media interfaces are defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

Media Interface: GSSCP_45

Devices: **GSSCP_45**

Media Interface

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

[Add](#)

Name	Media IP Network	Port Range	
Internal	10.10.9.81 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
External	192.168.122.46 External (B1, VLAN 0)	35000 - 40000	Edit Delete

Note: In the test environment, the internal IP address was **10.10.9.81** and the port range was left at default values.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the Deutsche Telefon SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the Deutsche Telefon SIP Trunk, click on **Add** (not shown). A pop-up menu is generated. In the **Name** field enter a descriptive name for the Deutsche Telefon network and click **Next**.

System Management

- Global Parameters
- Global Profiles
 - Domain DoS
 - Server Interworking**

Interworking Profile X

Profile Name:

[Next](#)

Note: Delayed SDP handling is required to work around a hold issue described in **Section 2.2**. This inserts an SDP into the empty INVITE messages sent from Communication Manager when it is redirecting media to and from the Media Gateway. When the call is coming off hold, the SDP ensures that the media path is re-established.

Check the **Delayed SDP Handling** and **T.38 Support** boxes and click on **Next**.

Interworking Profile

General

Hold Support: ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling: ☒ None ☐ SDP ☐ No SDP

181 Handling: ☒ None ☐ SDP ☐ No SDP

182 Handling: ☒ None ☐ SDP ☐ No SDP

183 Handling: ☒ None ☐ SDP ☐ No SDP

Refer Handling: ☐

URI Group:

Send Hold: ☒

Delayed Offer: ☒

3xx Handling: ☐

Diversion Header Support: ☐

Delayed SDP Handling: ☒

Re-Invite Handling: ☐

Prack Handling: ☐

Allow 18X SDP: ☐

T.38 Support: ☒

URI Scheme: ☒ SIP ☐ TEL ☐ ANY

Via Header Format: ☒ RFC3261 ☐ RFC2543

Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

Interworking Profile

All fields are optional.

SIP Timers

Min-SE: seconds, [90 - 86400]

Init Timer: milliseconds, [50 - 1000]

Max Timer: milliseconds, [200 - 8000]

Trans Expire: seconds, [1 - 64]

Invite Expire: seconds, [180 - 300]

Interworking Profile

Privacy

Privacy Enabled: ☐

User Name:

P-Asserted-Identity:

P-Preferred-Identity:

Privacy Header:

In the final dialogue box, leave the **Record Routes** at the default setting of **None** and ensure that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk. Click on **Finish**

Repeat the process to define Server Interworking for Session Manager using the same parameter settings apart from **Record Routes** which is set to **Both Sides** as the Session Manager uses the Record-Route header.

7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. The Deutsche Telefon SIP Trunk is connected as a Trunk Server. Session Manager is connected as a Call Server.

To define the Deutsche Telefon SIP Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** (not shown) and enter an appropriate name in the pop-up menu.

Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the Deutsche Telefon SIP Trunk FQDN.
- In the **Port** box, enter the port to be used for the SIP Trunk.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.

IP Address / FQDN	Port	Transport
sip.dtst.de	5060	UDP

Click on **Next** and enter the authentication details required for the Deutsche Telefon SIP trunk:

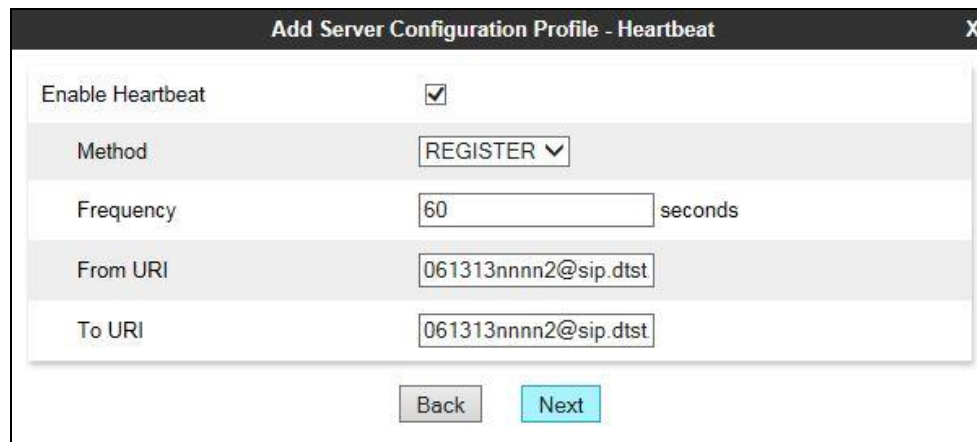
- Check the Enable Authentication box
- Enter the **User Name** provided by Deutsche Telefon
- Leave the **Realm** blank to use server settings
- Enter and confirm the **Password** provided by Deutsche Telefon

Enable Authentication	<input checked="" type="checkbox"/>
User Name	061313nnnn2
Realm (Leave blank to detect from server challenge)	
Password
Confirm Password

Click on **Next** again and enter the details for registration of the Avaya SBCE with the Deutsche Telefon SIP Trunk.

Registration is set up using the Heartbeat function of the Avaya SBCE as follows:

- Check the **Enable Heartbeat** box.
- Select **REGISTER** from the **Method** drop down menu.
- Enter a **Frequency** value. This is not important as the frequency of the REGISTER messages is determined by the “expires” parameter in the Contact header returned by the network in the 200 OK response to the REGISTER message. A value of **60** was used for testing.
- Enter a **From URI** and **To URI**. The Authentication User Name and Deutsche Telefon domain were used during testing.

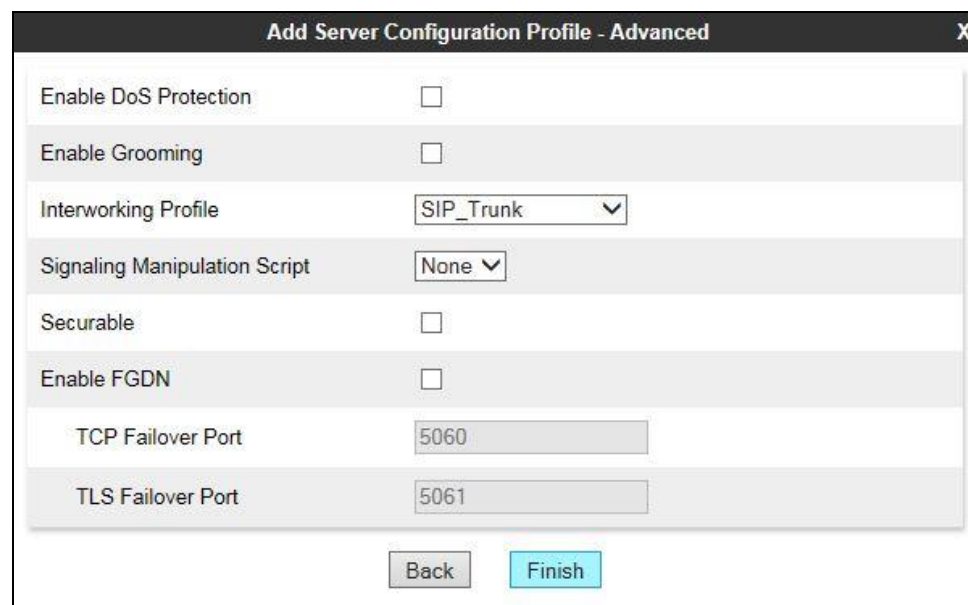


The screenshot shows a dialog box titled "Add Server Configuration Profile - Heartbeat". It contains the following fields and controls:

- Enable Heartbeat**: A checkbox that is checked.
- Method**: A dropdown menu with "REGISTER" selected.
- Frequency**: A text input field containing "60", followed by the label "seconds".
- From URI**: A text input field containing "061313nnnn2@sip.dtst".
- To URI**: A text input field containing "061313nnnn2@sip.dtst".
- At the bottom, there are two buttons: "Back" and "Next".

Click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for Deutsche Telefon SIP Trunk defined in **Section 7.4**.
- Leave the other fields at default settings.
- Click **Finish**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains the following fields and controls:

- Enable DoS Protection**: A checkbox that is unchecked.
- Enable Grooming**: A checkbox that is unchecked.
- Interworking Profile**: A dropdown menu with "SIP_Trunk" selected.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- Securable**: A checkbox that is unchecked.
- Enable FGDN**: A checkbox that is unchecked.
- TCP Failover Port**: A text input field containing "5060".
- TLS Failover Port**: A text input field containing "5061".
- At the bottom, there are two buttons: "Back" and "Finish".

Use the process described to define the Call Server configuration for Session Manager if not already defined. Leave the Authentication and Heartbeat settings at default values.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box (not shown).
- Ensure that the Interworking Profile defined for Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box (not shown).

The following screenshots show the **General** and **Advanced** tabs of the completed Server Configuration:

Server Configuration: SM_31

Buttons: Add, Rename, Clone, Delete

Server Profiles: DT, **SM_31**

General | Authentication | Heartbeat | Advanced

Server Type: Call Server

IP Address / FQDN	Port	Transport
10.10.9.31	5060	UDP

Edit

Server Configuration: SM_31

Buttons: Add, Rename, Clone, Delete

Server Profiles: DT, **SM_31**

General | **Advanced** | Authentication | Heartbeat

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile: Session_Manager

Signaling Manipulation Script: None

Securable ☐

Enable FGDN ☐

Edit

7.6. Define Routing

Routing information is required for routing to the Deutsche Telefon SIP Trunk on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling. To define routing to Deutsche Telefon SIP Trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** (not shown) and enter an appropriate name in the dialogue box.

Global Profiles

- Domain DoS
- Server Interworking
- Media Forking
- Routing**

Routing Profile [X]

Profile Name: DT

Next

Click on **Next** and enter details for the Routing Profile for the SIP Trunk:

- During testing, **Load Balancing** was not required and was left at the default value of **Priority**.
- Click on **Add** to specify an address for the SIP Trunk.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration defined in **Section 7.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

Repeat the process for the Routing Profile for Session Manager. The following screenshot shows the completed configuration:

7.7. 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 for termination information and the external interfaces for origination information.

To define Topology Hiding for Deutsche Telefon SIP Trunk, navigate to **Global Profiles** → **Topology Hiding** in the main menu on the left hand side. Click on **Add** (not shown) to bring up a dialogue box, assign an appropriate name and click on **Next** to configure Topology Hiding for each header as required:

The screenshot shows a dialog box titled "Topology Hiding Profile". On the left is a sidebar with navigation options: Server Interworking, Media Forking, Routing, Server Configuration, and **Topology Hiding**. The main area has a "Profile Name" input field containing the text "DT" and a "Next" button.

Enter details in the **Topology Hiding Profile** pop-up menu.

- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing the default **IP/Domain** was used for all headers that hides both domain names and IP addresses.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.

This screenshot shows the configuration step within the "Topology Hiding Profile" dialog. It features a table with columns: Header, Criteria, Replace Action, and Overwrite Value. The first row shows "Request-Line" selected for Header, "IP/Domain" for Criteria, and "Auto" for Replace Action. The Overwrite Value field is empty. There is an "Add Header" button at the top right and "Back" and "Finish" buttons at the bottom.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

The following screenshot shows the completed **Topology Hiding** configuration for the Deutsche Telefon SIP Trunk.

The screenshot displays the "Topology Hiding Profiles: DT" window. On the left is a list of profiles: default, cisco_th_profile, SM_31, and **DT**. The main area shows a table of configured headers. Above the table is a blue bar with the text "Click here to add a description." and buttons for "Rename", "Clone", and "Delete". Below the table is an "Edit" button.

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

To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for Deutsche Telefon SIP Trunk. Do this by highlighting the profile defined for Deutsche Telefon and clicking on **Clone**. Enter an appropriate name for Session Manager and click on **Next** (not shown). Make any changes where required, in the test environment the settings were left at the same values.

Topology Hiding Profiles: SM_31

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco_th_profile

SM_31

DT

Click here to add a description.

Topology Hiding

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

Edit

7.8. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the Deutsche Telefon SIP Trunk. This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the Deutsche Telefon SIP Trunk and vice versa.

To define a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click on **Add**.

Session Border Controller for Enterprise AVAYA

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ PPM Services

▸ Domain Policies

▸ TLS Management

▸ Device Specific Settings

 Network Management

 Media Interface

 Signaling Interface

End Point Flows

End Point Flows: GSSCP_45

Devices Subscriber Flows **Server Flows**

GSSCP_45

Add

Use the add button to create a new Server Flow.

Define the Server flow for the Deutsche Telefon SIP Trunk as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for the Deutsche Telefon SIP Trunk, in the test environment **DT_Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the Deutsche Telefon SIP Trunk defined in **Section 7.5**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Deutsche Telefon SIP Trunk defined in **Section 7.7** and click **Finish**.

The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a corresponding input field or dropdown menu. The fields are as follows:

Field Label	Value
Flow Name	DT_Trunk_Server
Server Configuration	DT
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal
Signaling Interface	External
Media Interface	External
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	SM_31
Topology Hiding Profile	DT
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom of the window, there is a "Finish" button.

Define a Server Flow for Session Manager as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **SM_Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5**.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Deutsche Telefon SIP Trunk defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** and click **Finish**.

Add Flow	
Flow Name	SM_Call_Server
Server Configuration	SM_31
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External
Signaling Interface	Internal
Media Interface	Internal
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	DT
Topology Hiding Profile	SM_31
Signaling Manipulation Script	None
Remote Branch Office	Any
Finish	

The information for all Server Flows is shown on a single screen on the Avaya SBCE.

End Point Flows: GSSCP_45

Devices
GSSCP_45

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: DT

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	DT_Trunk_Server	*	Internal	External	default-low	SM_31	View Clone Edit Delete

Server Configuration: SM_31

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM_Call_Server	*	External	Internal	default-low	DT	View Clone Edit Delete

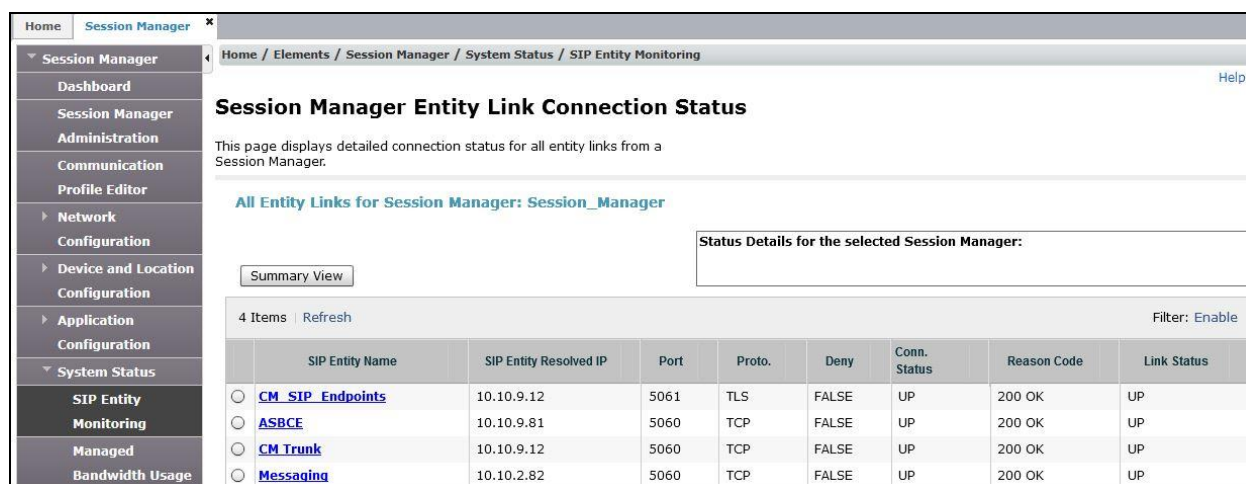
8. Configure the Deutsche Telefon SIP Trunk Equipment

The configuration of the Deutsche Telefon 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 Deutsche Telefon equipment and system configuration please contact an authorized Deutsche Telefon 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** screen 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**.



The screenshot shows the 'Session Manager Entity Link Connection Status' page. The left sidebar contains a navigation menu with 'Session Manager' expanded, showing 'Dashboard', 'Session Manager', 'Administration', 'Communication', 'Profile Editor', 'Network', 'Configuration', 'Device and Location', 'Configuration', 'Application', 'Configuration', 'System Status', 'SIP Entity Monitoring', 'Managed', and 'Bandwidth Usage'. The main content area has a breadcrumb trail: 'Home / Elements / Session Manager / System Status / SIP Entity Monitoring'. Below the title, a message states: 'This page displays detailed connection status for all entity links from a Session Manager.' A section titled 'All Entity Links for Session Manager: Session_Manager' contains a 'Summary View' button and a table with 4 items. The table has columns: SIP Entity Name, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. All four items show 'UP' for both 'Conn. Status' and 'Link Status'.

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> CM SIP Endpoints	10.10.9.12	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/> ASBCE	10.10.9.81	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> CM Trunk	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

2. From Communication Manager SAT interface run the command **status trunk n** where **n** is the 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
0002/007	T00017	in-service/idle	no
0002/008	T00018	in-service/idle	no
0002/009	T00019	in-service/idle	no
0002/010	T00020	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 a trace on the Avaya SBCE, navigate to **Device Specific Settings** → **Advanced Options** → **Troubleshooting** → **Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or **All** from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP_45

Devices
GSSCP_45

Packet Capture **Captures**

Packet Capture Configuration

Status	Ready
Interface	B1
Local Address <small>IP[:Port]</small>	All
Remote Address <small>*, *Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	SIP_Trunk_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 Deutsche Telefon network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1 to Deutsche Telefon SIP Tk-Anlagenanschluss. Deutsche Telefon SIP Tk-Anlagenanschluss 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. Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0.1, Aug 2016.
- [2] *Upgrading and Migrating Avaya Aura® applications to 7.0.1 from System Manager*, Release 7.0.1, Aug 2016.
- [3] *Deploying Avaya Aura® applications*, Release 7.0, Dec 2015
- [4] *Deploying Avaya Aura® Communication Manager*, Oct 2016
- [5] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, May 2016.
- [6] *Deploying Avaya Aura® System Manager*, Release 7.0.1 Aug 2016
- [7] *Upgrading Avaya Aura® Communication Manager*, Release 7.0.1, Oct 2016
- [8] *Upgrading Avaya Aura® System Manager to Release 7.0.1*, Aug 2016.
- [9] *Administering Avaya Aura® System Manager for Release 7.0.1*, Nov 2016
- [10] *Deploying Avaya Aura® Session Manager*, Release 7.0.1 Nov 2016
- [11] *Upgrading Avaya Aura® Session Manager Release 7.0.1*, Nov 2016
- [12] *Administering Avaya Aura® Session Manager Release 7.0.1*, May 2016,
- [13] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1, Nov 2016
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.1, Aug 2016
- [15] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Jun 2016
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2017 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.