



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura[®] Communication Manager R6.2, Avaya Aura[®] Session Manager R6.1 and Avaya Session Border Controller Advanced for Enterprise to Support Vodafone DE SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone DE SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager, Avaya Aura[®] Communication Manager and Avaya Session Border Controller Advanced for Enterprise. Vodafone DE is a member of the DevConnect Global SIP 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.

NOTE: This Application Note is applicable with Avaya Aura[®] 6.2 which is currently in Controlled Introduction. Avaya Aura[®] 6.2 will be Generally Available in Summer 2012.

NOTE: This Application Note focused on the SIP Trunking aspect of the Avaya Session Border Controller Advanced for Enterprise. Advanced enterprise capabilities such as Remote Worker “a.k.a. Remote SIP Endpoints”, dual forking, and TLS/SRTP were not tested. As a result, the Avaya Session Border Controller for Enterprise is also considered Compliance Tested for this solution.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager, Avaya Aura[®] Communication Manager Evolution Server and Avaya Session Border Controller Advanced for Enterprise. Customers using this Avaya SIP-enabled enterprise solution with the Vodafone DE SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

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 Session Manager and Communication Manager. The enterprise site was configured to use the SIP Trunk Service provided by Vodafone DE. 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 the PSTN were routed to the DID numbers assigned by Vodafone DE. Incoming PSTN calls were made to H.323, SIP, Digital and Analogue telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Vodafone DE to PSTN. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and Analogue telephones.
- Calls using G.729 and G.711A codec's.
- DTMF transmission using RFC 2833 with successful 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 (also known as "shuffling") with SIP and H.323 telephones was used during this test.
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Vodafone DE SIP Trunk Service with the following observations:

- All tests were completed using H.323, SIP, Digital and Analogue phone types. The Avaya one-X Communicator was used to test soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Calls answered at an EC500 mobile must originate with a valid CLI. If no CLI is presented the call cannot be bridged onto the host station and the call does not clear down on the PSTN.
- Inbound and Outbound fax was tested using G.711 pass-through. This is not a method supported by Avaya

2.3. Support

For technical support on the Avaya products described in these Application Notes visit

<http://support.avaya.com>.

For technical support on Vodafone DE products please visit the website at

<http://www.vodafone.de> or contact an authorized Vodafone DE representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Vodafone DE SIP Trunk Service. Located at the enterprise site is a Session Manager and Communication Manager. Endpoints are Avaya 9600 and 4600 series IP telephones, Avaya 2400 series Digital Telephone, an Avaya Desktop Video Device, a PC running Avaya one-X Communicator an Analogue Telephone and Fax Machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

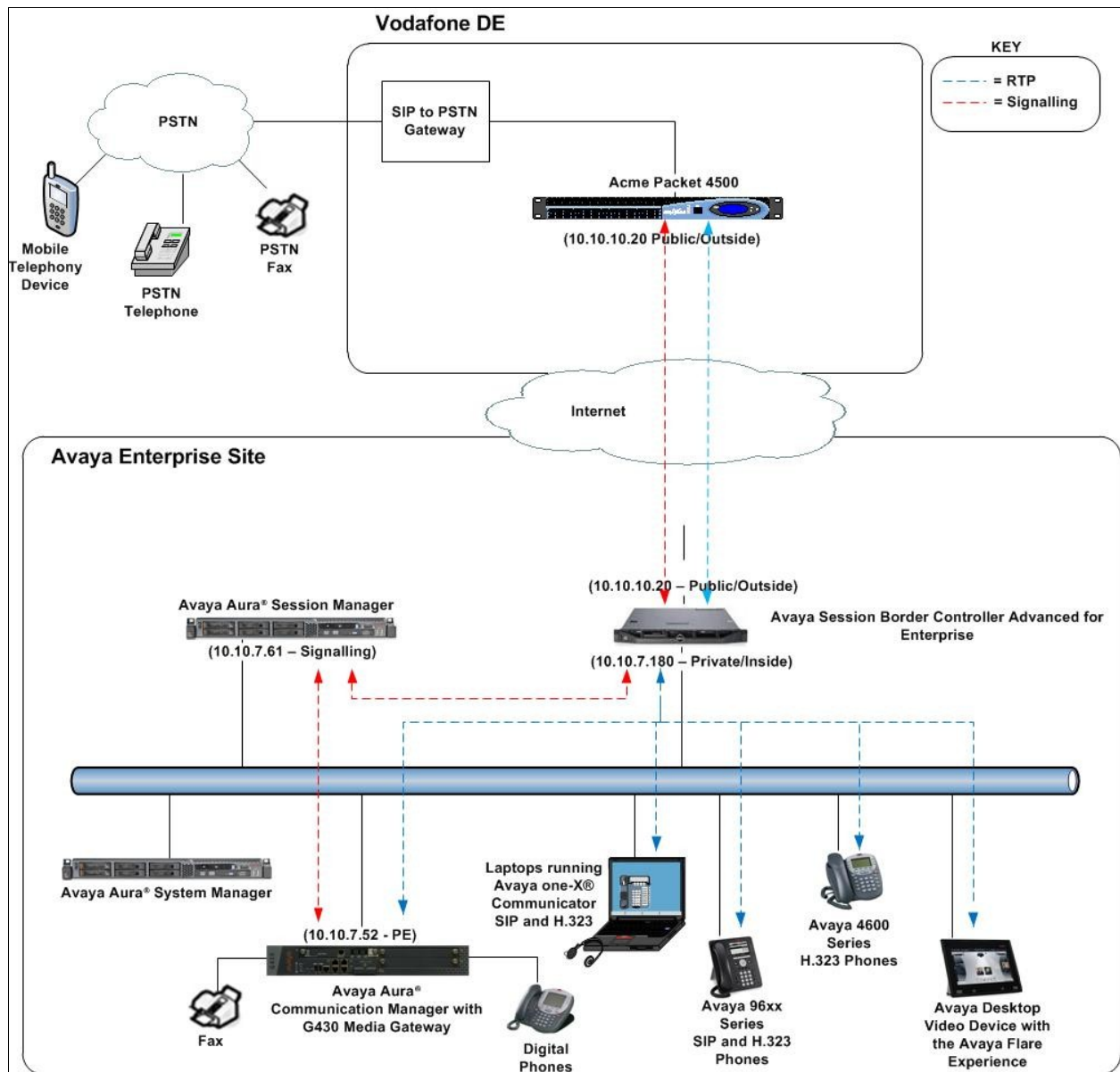


Figure 1: Vodafone DE SIP Solution Topology

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager R6.2 (R016x.02.0.823.0)
Avaya G430 Media Gateway MM711 Analogue MM712 Digital MGP Firmware	HW31 FW093 HW07 FW009 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 (6.1.6.0.616009)
Avaya S8800 Server	Avaya Aura® System Manager R6.1 (6.1.0.0.7345-6.1.5.606) Update revision No: 6.1.10.1.1806
Dell R310 running Avaya Session Border Controller Advanced for Enterprise	Avaya Session Border Controller Advanced for Enterprise (4.0.5.Q02)
Avaya 9620 Phone (H.323)	3.11
Avaya 9620 Phone (SIP)	2.6.4.0
Avaya 2420 Digital Phone	N/A
Analog Phone	N/A
Avaya 4620 Phone (H.323)	2.9
Avaya 9611G	6.0
Avaya ADVD	1.0.2
Vodafone DE	
Softswitch: iSSW	20.50.34-olxi
SBC: Acme Packet 4250	6.1.0 MR5
MG: Cisco MGX 8880	5.5(10.204)P4

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 Signaling associated with Vodafone DE SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from Vodafone DE 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 signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Vodafone DE network via the Avaya Session Border Controller Advanced for Enterprise. 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 Avaya S8800 Server and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

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

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	3
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	0
Maximum Administered SIP Trunks:		24000	30

On **Page 4**, verify that **IP Trunks** field is set to **y**.

```
display system-parameters customer-options                                Page 4 of 11
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                         IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                             ISDN Feature Plus? y
    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? n                                         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? n
    IP Trunks? y

IP Attendant Consoles? y
(NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. Type **change node-names ip** to make changes to the **IP Node Names**. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **asmV7** and **10.10.7.61** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
change node-names ip
                                IP NODE NAMES

  Name          IP Address
  procr         10.10.7.52
  asmV7         10.10.7.61
  default       0.0.0.0
```

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is set to yes to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** was used

```
change ip-network-region 1                                     Page 1 of 20
                                                              IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: avaya.com
Name: Default NR
MEDIA PARAMETERS
  Codec Set: 1           Intra-region IP-IP Direct Audio: yes
                        Inter-region IP-IP Direct Audio: yes
                        IP Audio Hairpinning? n
  UDP Port Min: 35000
  UDP Port Max: 50001
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
H.323 IP ENDPOINTS
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
                        AUDIO RESOURCE RESERVATION PARAMETERS
                        RSVP Enabled? n
```

5.4. Administer IP Codec Set

Use the **change ip-codec-set** command for the codec set specified in the **IP Network Region** form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test, the codec's supported by Vodafone DE were configured, namely **G.711A** and **G.729**.

```
change ip-codec-set 1                                         Page 1 of 2
                                                              IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711A   n                    2          20
2: G.729    n                    2          20
```

Vodafone DE SIP Trunk Service uses pass-through which is not a method supported by Avaya. Configure the pass-through fax protocol by setting the **Fax Mode** to **pass-through**

on **Page 2** of the codec set form as shown below. **Although during testing pass-through mode was shown to work, Avaya does not officially support this fax method.**

change ip-codec-set 1		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
	pass-through	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

5.5. Administer SIP Signaling Groups

Add a signaling group and trunk group for inbound and outbound PSTN calls to Vodafone DE SIP Trunk Service and configure using TCP (Transmission Control Protocol) and TCP port of 5060. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set the **Group Type** field to **sip**
- The **Transport Method** field is set to **tcp**
- Set the **Near-end Node Name** to the processor interface (node name **procr**). This value is taken from the **IP Node Names** form shown in **Section 5.2**
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **asmV7**), also shown in **Section 5.2**
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 6.2**. This field logically establishes the **far-end** for calls using this signaling group as network region **1**
- The **Direct IP-IP Audio Connections** field is set to **y**
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833

The default values for the other fields may be used.

```
add signaling-group 1
                                SIGNALING GROUP

Group Number: 1                Group Type: sip
                                Transport Method: tcp
IMS Enabled? n

Near-end Node Name: procr      Far-end Node Name: asmV7
Near-end Listen Port: 5060     Far-end Listen Port: 5060
                                Far-end Network Region: 1
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? n
                                Direct IP-IP Early 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 x** command, where x is an available trunk group.

On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (TAC) consistent with the dial plan, i.e. **101**
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **tie**
- Specify the signaling 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 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: smpub	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 1			
Number of Members: 30			

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Vodafone DE to prevent unnecessary SIP messages during call setup.

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 8000			
SCCAN? n		Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 1800			

On **Page 3**, set the **Numbering Format** field to **private**. This allows the number to be sent to Vodafone DE without the + used in the E164 numbering format.

add trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UI Treatment: service-provider		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		
Modify Tandem Calling Number:		

On **Page 4**, set the **Mark Users as Phone** to **y**, this field inserts a parameter to SIP requests indicating to any receiving SIP entity that the user part of the request URI should be treated as a telephone number. Set **Send Transferring Party Information** to **y**, to allow trunk to trunk transfers. Set **Telephone Event Payload Type** to **120**.

add trunk-group 1		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? y		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? y		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type: 120		

5.7. Administer Calling Party Number Information

In this section the Calling Party Number sent when making a call using the SIP trunk is specified

5.7.1. Set Private Unknown Numbering

Use the **change private-numbering** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a 4-digit extension beginning with 1 will send the calling party number **069xxxxxxxxx** to Vodafone DE SIP Trunk Service. This calling party number will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Public DID numbers have been masked for security purposes.

change private-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
4	1	1	069xxxxxxxxx	13	Total Administered: 1
					Maximum Entries: 240

5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to Vodafone DE SIP Trunk Service. In the sample configuration, the single digit **9** is used as the ARS access code. Avaya telephone users will dial **9** to reach an outside line. Use the **change feature-access-codes** command to configure or observe **9** as the **Auto Route Selection (ARS) - Access Code 1**.

change feature-access-codes		Page 1 of 9
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: *37		
Answer Back Access Code: *12		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 7		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2: *99
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA: *87	All: *88	Deactivation: #88
Call Forwarding Enhanced Status:	Act:	Deactivation:

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning **0** or **00**. Calls are sent to **Route Pattern 1**, which contains the previously configured SIP Trunk Group.

change ars analysis 02						Page	1 of	2
ARS DIGIT ANALYSIS TABLE								
Location: all						Percent Full:	1	
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
0		11	11	1	pubu		n	
00		13	13	1	pubu		n	

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group 1.

change route-pattern 1															Page 1 of 3		
Pattern Number: 1 Pattern Name: tosm100																	
SCCAN? n Secure SIP? n																	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted								DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits								QSIG		
															Intw		
1:	1	0													n	user	
2:															n	user	
3:															n	user	
4:															n	user	
5:															n	user	
6:															n	user	
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR																	
0 1 2 M 4 W Request																	
															Dgts Format		
															Subaddress		
1:	y	y	y	y	y	n	n	rest							none		
2:	y	y	y	y	y	n	n	rest							none		

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Vodafone DE can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by Vodafone DE correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **0691xxxxxxxx** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DID numbers have been masked for security purposes.

change inc-call-handling-trmt trunk-group 1					Page	1 of	3
INCOMING CALL HANDLING TREATMENT							
Service/	Number	Number	Del Insert				
Feature	Len	Digits					
public-ntwrk	13	0691xxxxxxxx	all	1306			
public-ntwrk	13	0691xxxxxxxx	all	1307			
public-ntwrk	13	0691xxxxxxxx	all	1601			
public-ntwrk	13	0691xxxxxxxx	all	1602			

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

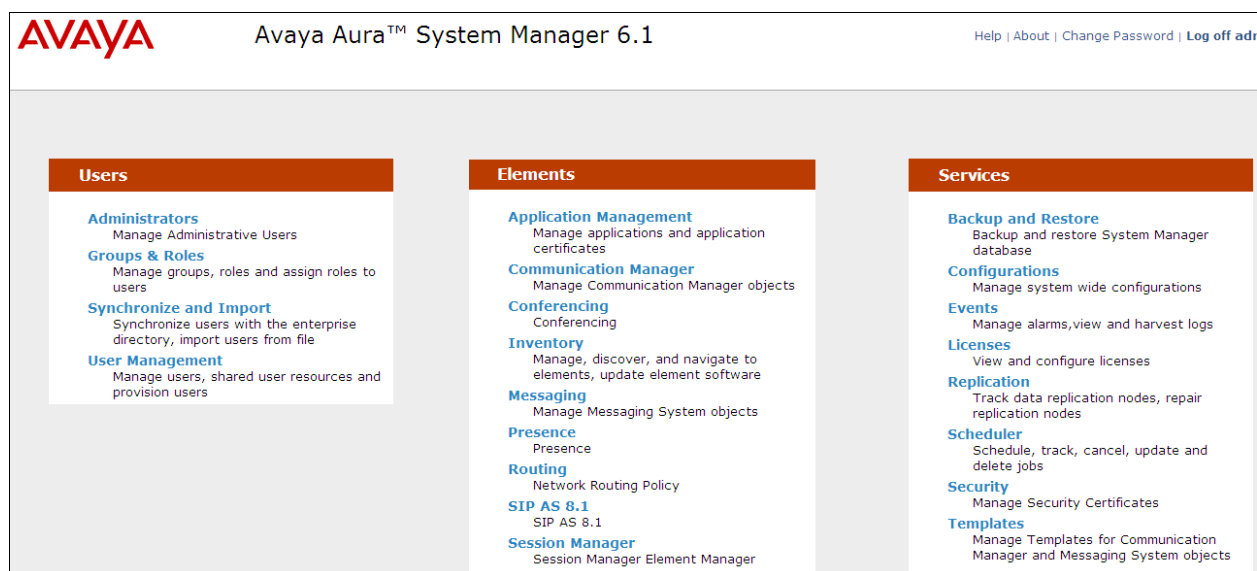
6. Configuring Avaya Aura® Session Manager

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

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Communication Manager as Managed Element
- 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 by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.



6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu (not shown) and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **Avaya.com**). Click **Commit** to save changes (not shown).

Home / Elements / Routing / Domains - Domain Management			
Domain Management			
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/>			
2 Items Refresh			
<input type="checkbox"/>	Name	Type	Default
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>

6.3. Administer Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field enter an informative name for the location. 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. Below is the location configuration used for the simulated enterprise.

Home / Elements / Routing / Locations - Location Details			
Location Details <input type="button" value="Commit"/>			
Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting			
General			
* Name: <input type="text" value="SPLab7"/>			
Notes: <input type="text"/>			
Overall Managed Bandwidth			
Managed Bandwidth Units: <input type="text" value="Kbit/sec"/>			
Total Bandwidth: <input type="text"/>			
Per-Call Bandwidth Parameters			
* Default Audio Bandwidth: <input type="text" value="80"/> <input type="text" value="Kbit/sec"/>			
Location Pattern			
<input type="button" value="Add"/> <input type="button" value="Remove"/>			
3 Items Refresh Filter: E			
<input type="checkbox"/>	IP Address Pattern	Notes	
<input type="checkbox"/>	* 10.10.9.*	<input type="text"/>	
<input type="checkbox"/>	* 10.10.8.*	<input type="text"/>	
<input type="checkbox"/>	* 10.10.7.*	<input type="text"/>	

6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the 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 signaling 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 **Gateway** for the SBC SIP entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Session Border Controller SIP Entity

6.4.1. 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 signaling interface.

The screenshot displays the 'SIP Entity Details' configuration page for a Session Manager SIP Entity. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'Commit' button in the top right. The 'General' tab is active, showing the following fields:

- Name:** ASMDot7
- FQDN or IP Address:** 10.10.7.61
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text field)
- Location:** Siplab7 (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Etc/GMT (dropdown menu)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

The 'Name', 'FQDN or IP Address', and 'Location' fields are highlighted with red boxes in the original image.

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 **Port**, click **Add**, then edit the fields in the resulting new row.

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

Port

3 Items Filter: Enable

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

Select : All, None

* Input Required

6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screens show the SIP entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling. The entity **Type** is set to **CM**.

Routing / Domains / Locations / Adaptations / **SIP Entities** / Entity Links / Time Ranges / Routing Policies / Dial Patterns / Regular Expressions / Defaults

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: CMEVO

* FQDN or IP Address: 10.10.7.52

Type: CM

Notes:

Adaptation:

Location: SPLab7

Time Zone: Etc/GMT

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.3. Avaya Session Border Controller Advanced for Enterprise SIP Entity

The following screen shows the SIP entity for the Avaya Session Border Controller Advanced for Enterprise used for routing Fixed and Mobile calls. The **FQDN or IP Address** field is set to the IP address of the private interfaces administered in **Section 7** of this document.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off](#)

[Routing](#) x

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details [Commit](#)

General

* Name: ASBCAE

* FQDN or IP Address: 10.10.7.180

Type: Gateway

Notes:

Adaptation:

Location: SPLab7

Time Zone: Etc/GMT

Override Port & Transport with DNS SRV: ☐

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

6.5. 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.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **SessionManager**
- 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 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box 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 following screen shows the Entity Links used in this configuration.

SIP Entities	1 Item Refresh	Filter: t
Entity Links		
Time Ranges		
Routing Policies		
Dial Patterns		
Regular Expressions		
Defaults		

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* toCM	* ASM61	TCP	* 5060	* CMEVO	* 5060	Trusted	

* Input Required

Commit

SIP Entities	1 Item Refresh	Filter: E
Entity Links		
Time Ranges		
Routing Policies		
Dial Patterns		
Regular Expressions		
Defaults		

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* toASBCAE	* ASM61	TCP	* 5060	* ASBCAE	* 5060	Trusted	

* Input Required

Commit

6.6. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager:

Adaptations	<div>General</div> <div><div>* Name: TO CMEVO</div><div>Disabled: <input type="checkbox"/></div><div>Notes: </div></div> <div>SIP Entity as Destination</div> <div>Select</div> <table><thead><tr><th>Name</th><th>FQDN or IP Address</th><th>Type</th><th>Notes</th></tr></thead><tbody><tr><td>CMEVO</td><td>10.10.7.52</td><td>CM</td><td></td></tr></tbody></table>	Name	FQDN or IP Address	Type	Notes	CMEVO	10.10.7.52	CM	
Name		FQDN or IP Address	Type	Notes					
CMEVO		10.10.7.52	CM						
SIP Entities									
Entity Links									
Time Ranges									
Routing Policies									
Dial Patterns									
Regular Expressions									
Defaults									

The following screens show the routing policy for Avaya Session Border Controller Advanced for Enterprise

Adaptations	<div>General</div> <div><div>* Name: to_ASBCAE</div><div>Disabled: <input type="checkbox"/></div><div>Notes: </div></div> <div>SIP Entity as Destination</div> <div>Select</div> <table><thead><tr><th>Name</th><th>FQDN or IP Address</th><th>Type</th><th>No</th></tr></thead><tbody><tr><td>ASBCAE</td><td>10.10.7.180</td><td>Gateway</td><td></td></tr></tbody></table>	Name	FQDN or IP Address	Type	No	ASBCAE	10.10.7.180	Gateway	
Name		FQDN or IP Address	Type	No					
ASBCAE		10.10.7.180	Gateway						
SIP Entities									
Entity Links									
Time Ranges									
Routing Policies									
Dial Patterns									
Regular Expressions									
Defaults									

6.7. 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 dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select the domain configured in **Section 6.2**

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save (not shown). The following screens show an example dial pattern configured for Vodafone DE SIP Trunk Service.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Commit

General

* Pattern: 0

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: E

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Notes
<input type="checkbox"/>	SPLab7		to_ASBCAE	0	<input type="checkbox"/>	ASBCAE	

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

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Commit

General

* Pattern: 069

* Min: 13

* Max: 13

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: 0

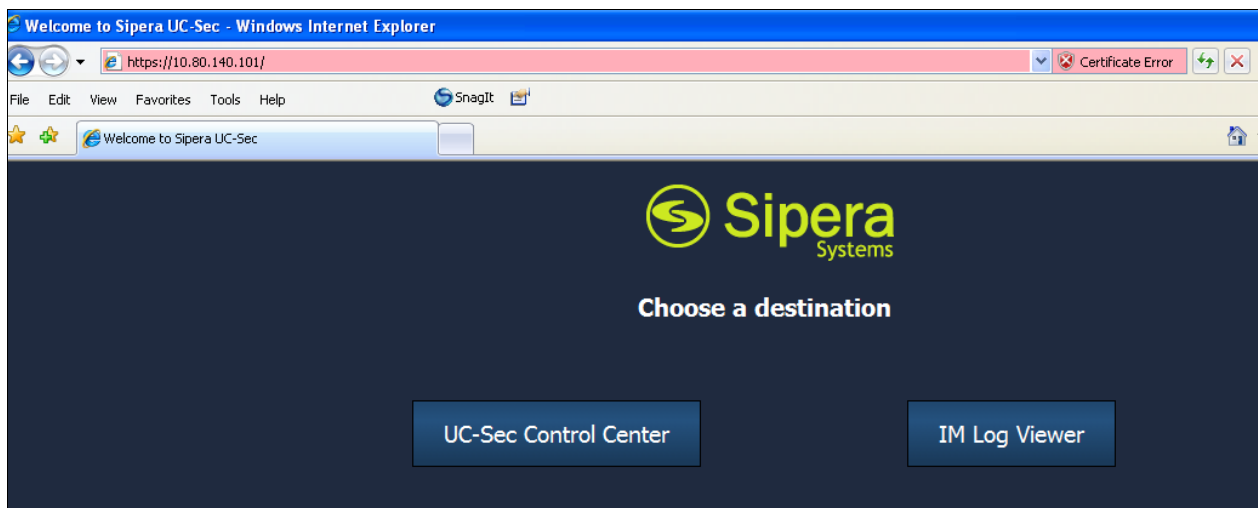
<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Notes
<input type="checkbox"/>	-ALL-	Any Locations	ToCMEVO	0	<input type="checkbox"/>	CMEVO	

7. Avaya Session Border Controller Advanced for Enterprise Configuration

This section provides the procedures for configuring Session Border Controller Advanced for Enterprise.

7.1. Accessing UC-Sec Control Centre

Access the web interface by typing **https://x.x.x.x** (where x.x.x.x is the management IP of the E-SBC).



Select **UC-Sec Control Center** and enter the **Login ID** and **Password**.



7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.2.1. Server Internetworking Avaya Side

Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the lefthand menu select **Global Profiles → Server Internetworking** and click on **Add Profile**.

- Enter profile name: **ToASM** and click **Next**
- **Check Hold Support= RFC2543**
- All other options on the General Tab can be left at default.

Click on **Next** on the following screens and then **Finish**.

Editing Profile: ToASM	
General	
Hold Support	<input type="radio"/> None <input checked="" type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<input type="button" value="Next"/>	

7.2.2. Server Internetworking – Vodafone DE side

Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the lefthand menu select **Global Profiles → Server Internetworking** and click on **Add Profile**.

- Enter profile name: **ToVDE** and click on **Next**
- **Check Hold Support= RFC2543**
- All other options on the General Tab can be left at default.

Click on **Next** on the following screens and then **Finish**.

General	
Hold Support	<input type="radio"/> None <input checked="" type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

7.2.3. Routing – Avaya side

The Routing Profile allows you to manage parameters related to routing SIP signaling messages. From the lefthand menu select **Global Profiles → Routing** and click on **Add Profile**.

- Enter Profile Name: **ASM_7**
- Hit **Next** (not shown)
- **Next Hop Server 1: 10.10.7.61** (Session Manager IP address)
- Select **Routing Priority Based on Next Hop Server**
- Select **Use Next Hop for In-Dialog Messages**
- **Outgoing Transport: TCP**

Click **Finish** (not shown).

Global Profiles > Routing: ASM_7

Buttons: Add Profile, Rename Profile, Clone Profile, Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.10.7.61	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	TCP

7.2.4. Routing – Vodafone DE side

The Routing Profile allows you to manage parameters related to routing SIP signaling messages. A routing profile must be set for Fixed and Mobile calls. From the lefthand menu select **Global Profiles → Routing** and click on **Add Profile**.

- Enter Profile Name: **VDE**
- Hit **Next**
- **Next Hop Server 1: 10.10.10.10** (IP Address provided by Vodafone)
- Select **Routing Priority Based on Next Hop Server**
- Select **Use Next Hop for In-Dialog Messages**
- **Outgoing Transport: UDP**
- Click **Finish** (not shown)

Global Profiles > Routing: VDE

Buttons: Add Profile, Rename Profile, Clone Profile, Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.10.10.10	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	UDP

7.2.5. Server Configuration– Avaya SM

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the lefthand menu select **Global Profiles** → **Server Configuration** and click on **Add Profile**.

- **Enter profile name: ASM_CallServer**
- On the **Add Server Configuration Profile** Tab:
- Select Server Type: **Call Server**
- **IP Address: 10.10.7.61 (Session Manager IP Address)**
- **Supported Transports: Check UDP and TCP**
- **TCP Port:5060**
- **UDP Port: 5060**
- Click on **Next** for the **Authentication** and **Heartbeat** tabs.
- On the **Advanced** Tab
- Select **ToASM** for Interworking Profile
- Hit **Next**
- Click **Finish**

The screenshot shows a window titled "Edit Server Configuration Profile - General". It contains several input fields and checkboxes. The "Server Type" dropdown is set to "Call Server". The "IP Addresses / Supported FQDNs" text box contains "10.10.7.61". Under "Supported Transports", the checkboxes for "TCP" and "UDP" are checked, while "TLS" is unchecked. The "TCP Port" and "UDP Port" text boxes both contain "5060". The "TLS Port" field is disabled (grayed out). A "Finish" button is located at the bottom center of the window.

Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.10.7.61
Supported Transports	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	5060
TLS Port	
Finish	

Edit Server Configuration Profile - Advanced

Enable DoS Protection

☐

Enable Grooming

☐

Interworking Profile

ToASM

Signaling Manipulation Script

None

TCP Connection Type

☒ SUBID ☐ PORTID ☐ MAPPING

UDP Connection Type

☒ SUBID ☐ PORTID ☐ MAPPING

Finish

7.2.6. Server Configuration– Vodafone DE side

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles** → **Server Configuration** and click on **Add Profile**.

- **Name: VDE_Trunk**
- On the **Add Server Configuration Profile** Tab:
- Click on **Edit**
- Select Server Type: **Trunk Server**
- **IP Address: 10.10.10.10 (Vodafone DE Trunk Server)**
- **Supported Transports: Check UDP**
- **UDP Port: 5060**
- Hit **Next**
- Click on **Next** for the **Authentication** and **Heartbeat** tabs.
- On the **Advanced** Tab
- Select **ToVDE** for Interworking Profile
- Hit **Next**
- Click **Finish**

The screenshot shows the 'Edit Server Configuration Profile - General' window. The fields are as follows:

Field	Value
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma separated list	10.10.10.10
Supported Transports	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	5060
TLS Port	

Finish

Edit Server Configuration Profile - Advanced

Enable DoS Protection

☐

Enable Grooming

☐

Interworking Profile

ToVDE

Signaling Manipulation Script

None

TCP Connection Type

☒ SUBID ☐ PORTID ☐ MAPPING

UDP Connection Type

☒ SUBID ☐ PORTID ☐ MAPPING

Finish

7.2.7. Topology Hiding – Avaya side

The **Topology Hiding** screen allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. From the left-hand menu select **Global Profiles → Topology Hiding**.

- Click **default** profile and select **Clone Profile**
- Enter Profile Name: **ASM**
- For the **Header To** and **Request Line** select **IP/Domain** under **Criteria** and **Next Hop** under **Replace Action**.
- Click **Finish**

The screen below is a result of the details configured above

The screenshot shows the 'Global Profiles > Topology Hiding: ASM' interface. On the left, a sidebar lists 'Topology Hiding Profiles' with 'default', 'cisco_th_profile', 'ASM' (selected), and 'VDE'. The main area has buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. A yellow banner says 'Click here to add a description.' Below this is a table titled 'Topology Hiding' with columns: Header, Criteria, Replace Action, and Overwrite Value. The table contains the following rows:

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Next Hop	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Next Hop	---
From	IP/Domain	Auto	---

An 'Edit' button is located at the bottom right of the table.

7.2.8. Topology Hiding – Vodafone DE side

The **Topology Hiding** screen allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. From the left-hand menu select **Global Profiles → Topology Hiding**.

- Click **default** profile and select **Clone Profile**
- **Enter Profile Name: VDE**
- For the Header **To** and **Request Line** select **IP/Domain** under **Criteria** and **Next Hop** under **Replace Action**
- Click **Finish**

The screen below is a result of the details configured above

The screenshot shows the 'Global Profiles > Topology Hiding: VDE' interface. On the left, a sidebar lists 'Topology Hiding Profiles' with 'default', 'cisco_th_profile', 'ASM', and 'VDE' (selected). The main area has buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. A yellow banner says 'Click here to add a description.' Below this is a table titled 'Topology Hiding' with columns: Header, Criteria, Replace Action, and Overwrite Value. The table contains the following rows:

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Next Hop	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Next Hop	---
From	IP/Domain	Auto	---

An 'Edit' button is located at the bottom right of the table.

7.3. Device Specific Settings

7.3.1. The **Network Management** feature allows the public and private interface addresses and state to be set. From the left-hand menu select **Device Specific Settings → Network Management**.

- Enter in the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces
- Select the **physical interface used in the Interface** column

Device Specific Settings > Network Management: GSSCP_07

UC-Sec Devices
GSSCP_07

Network Configuration | Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.128 B2 Netmask:

Add IP Changes will not take effect until the interface is updated. Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface	
10.10.7.180		10.10.7.1	A1	✕
10.10.10.20		10.10.10.1	B1	✕

Select the **Interface Configuration** Tab and use the **Toggle State** button to enable the interfaces.

Network Configuration		Interface Configuration	
Name		Administrative Status	
A1		Enabled	Toggle State
A2		Disabled	Toggle State
B1		Enabled	Toggle State
B2		Disabled	Toggle State

7.3.2. The **Media Interfaces** feature allows the IP Address and ports to be set for transporting Media over the SIP trunk. From the left-hand menu select **Device Specific Settings** → **Media Interface**.

- Select **Add Media Interface**
- **Name:** ASM7
- **Media IP:** 10.10.7.180 (Internal Address for calls toward Communication Manager)
- **Port Range:** 35000-50000
- Click **Finish**
- Select **Add Media Interface**
- **Name:** VDEMed
- **Media IP:** 10.10.10.20 (External Address for calls toward Vodafone trunk)
- **Port Range:** 35000-50000
- Click **Finish**
- Select **Add Media Interface**

The screen below is a result of the details configured above.

Device Specific Settings > Media Interface: GSSCP_07

UC-Sec Devices

GSSCP_07

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 Media Interface

Name	Media IP	Port Range		
ASM7	10.10.7.180	35000 - 40000		
VDEMed	10.10.10.20	35000 - 40000		

7.3.3. The **Signalling Interfaces** feature allows the IP Address and ports to be set for transporting Media over the SIP trunk. From the left-hand menu select **Device Specific Settings → Signalling Interface**.

- Select **Add Signaling Interface**
- **Name:** ASM7
- **Media IP:** 10.10.7.180 (Internal Address for calls toward Session Manager)
- **TCP Port:** 5060
- **UDP Port:** 5060
- Click **Finish**
- Select **Add Media Interface**
- **Name:** VDE
- **Media IP:** 10.10.10.20(External Address for calls toward Vodafone DE)
- **TCP Port:** 5060
- **UDP Port:** 5060
- Click **Finish**

The screen below is a result of the details configured above.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
ASM7	10.10.7.180	5060	5060	---	None		
VDE	10.10.10.20	5060	5060	---	None		

7.3.4. The **End Point Flows** allow the Interfaces, Policies and Profiles administered to be used to transport the SIP traffic. From the left-hand menu select **Device Specific Settings → Endpoint Flows**.

- Select the **Server Flows** Tab

To add the settings for Fixed call flow to Session Manager Click on select **Add Flow**.

- **Name:** Callserver
- **Server Configuration:** ASM7_CallServer
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** VDE_Fixed
- **Signaling Interface:** ASM7
- **Media Interface:** ASM7
- **End Point Policy Group:** default-low
- **Routing Profile:** VDE
- **Topology Hiding Profile:** ASM
- **File Transfer Profile:** None
- Click **Finish**

To add the settings for Fixed call flow to Vodafone DE select **Add Flow**.

- **Name:** TrunkServer
- **Server Configuration:** VDE_Trunkfixed
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** ASM7
- **Signaling Interface:** VDEFixed
- **Media Interface:** VDEFixed
- **End Point Policy Group:** default-low
- **Routing Profile:** ASM_7
- **Topology Hiding Profile:** VDE
- **File Transfer Profile:** None
- Click **Finish**

The screen below is a result of the details configured above.

Device Specific Settings > End Point Flows: GSSCP_07

UC-Sec Devices

GSSCP_07

Subscriber Flows

Server Flows

Add Flow

Hover over a row to see its description.

Server Configuration: ASM_CallServer

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	ToASM7	*	TCP	*	VDE	ASM7	ASM7	default-low	VDE	ASM	None			

Server Configuration: VDE_Trunk

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	ToVDE	*	UDP	*	ASM7	VDE	VDEMed	default-low	ASM_7	VDE	None			

8. Vodafone DE Configuration

The configuration required by Vodafone DE to allow the tests to be carried out is not covered in this document and any further information required shown be obtained through the local Vodafone DE representative.

9. Verification Steps

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

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

This is the SIP Entity link to the Communication Manager:

Communication Profile Editor	All Entity Links to SIP Entity: CMEVO						
Network Configuration	Summary View						
Device and Location Configuration	1 Item Refresh Filter: Enable						
Application Configuration	Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code
System Status	► Show	ASM61	10.10.7.52	5060	TCP	Up	200 OK
SIP Entity Monitoring							Link Status
							Up

This is the SIP Entity link to the Avaya Session Border Controller Advanced for Enterprise:

1 Item Refresh Filter: Enable						
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code
► Show	ASMDot7	10.10.7.180	5060	TCP	Up	200 OK
						Link Status
						Up

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

```
status trunk 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00007	in-service/idle	no
0001/003	T00008	in-service/idle	no
0001/004	T00009	in-service/idle	no
0001/005	T00010	in-service/idle	no

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Session Border Controller Advanced for Enterprise to Vodafone DE SIP Trunk Service. The testing was successfully performed with Vodafone DE, refer to **Section 2.2** for more details.

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.03, February 2011.
- [2] *Administering Avaya Aura® System Platform*, Release 6.03, February 2011.
- [3] *Administering Avaya Aura® Communication Manager*, August 2010, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, May 2009, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager Release 6.1*, November 2010.
- [6] *Installing and Configuring Avaya Aura® Session Manager*, January 2011, Document Number 03-603473
- [7] *Administering Avaya Aura® Session Manager*, March 2011, Document Number 03-603324.
- [8] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>.

©2012 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.