



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

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise R4.0.5 to Support Vodafone NL SIP Trunk Service – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone NL 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 for Enterprise. Vodafone NL 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.

# 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 for Enterprise (Avaya SBCE). Customers using this Avaya SIP-enabled enterprise solution with the Vodafone NL SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. The Vodafone solution incorporates routing for calls placed to and from their Mobile and Fixed networks separately and offer short dialing from dedicated mobile telephones. 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 NL.

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 and Fixed short dial numbers assigned by Vodafone NL. 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 NL to PSTN and Vodafone Mobile destinations using short dial and full number. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and Analogue telephones.
- Calls using G.729, G.711A and G.711Mu codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 codec.
- 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 NL SIP Trunk Service with the following observations:

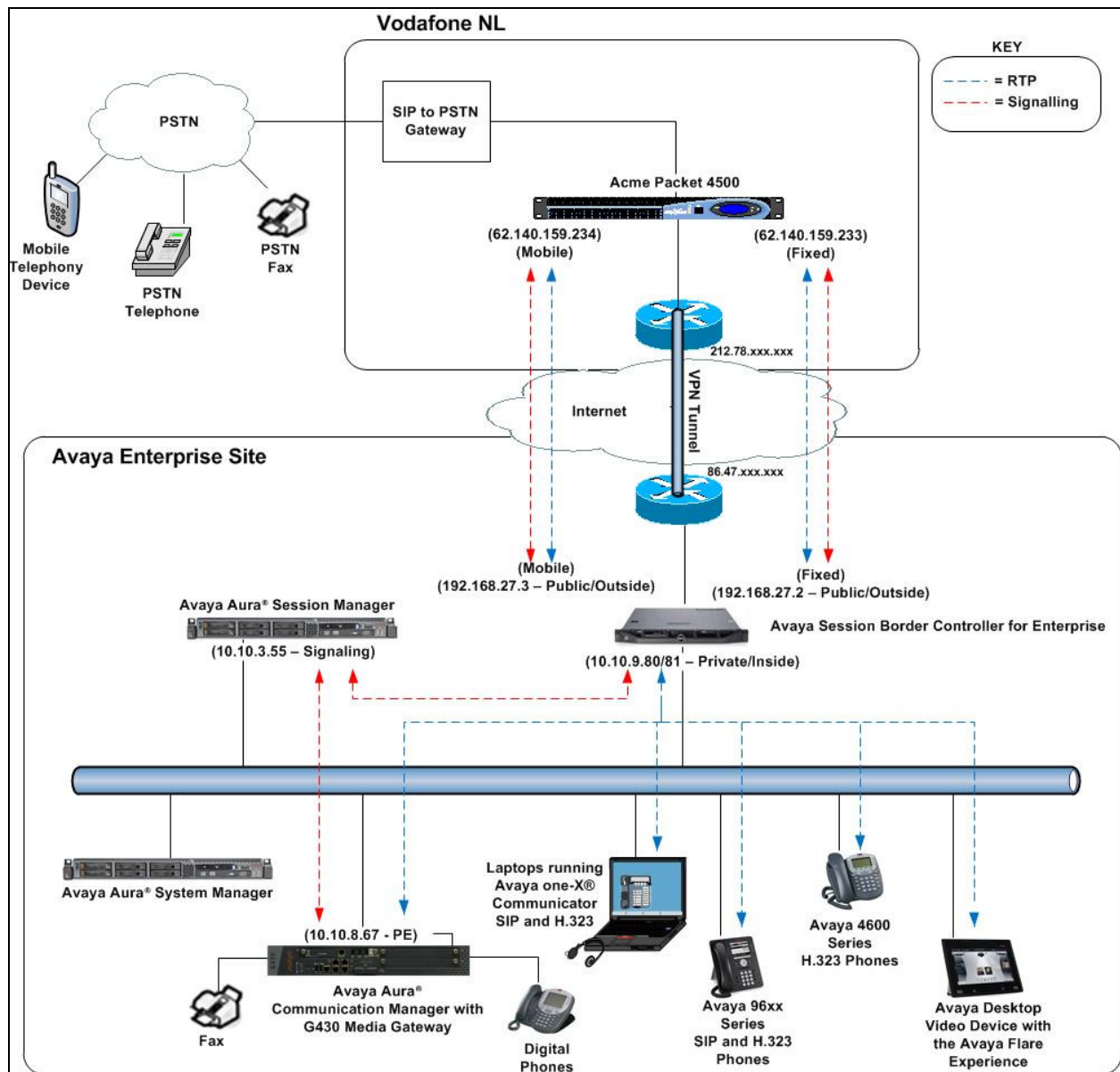
- All tests were completed using H.323, SIP, Digital and Analogue phone types. The Avaya one-X Communicator was used to test SIP soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Routing to emergency numbers (such as 112) was not tested.
- When CM responds with 488 “Not Acceptable Here” during codec rejection, the network re-attempts to establish the call during which the caller gets no indication of call failure.
- When CLI is restricted, the user part of the From and P-Asserted-ID fields is set to “anonymous” and the Privacy header is not sent. In this case, the enterprise equipment does not correctly indicate that the caller is “Private”.
- When signalling fails and a 500 “Server Link Monitor Status Down” is received from Session Manager, the network attempts to re-establish the call during which the caller gets no indication of call failure.

## 2.3. Support

For technical support on Vodafone Netherlands SIP trunking services, contact Vodafone Netherlands support at [http://www.vodafone.nl/zakelijk/totaal\\_oplossingen/vast\\_en\\_mobiel/](http://www.vodafone.nl/zakelijk/totaal_oplossingen/vast_en_mobiel/).

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an enterprise site connected to the Vodafone NL SIP Trunk Service. Located at the enterprise site are a Session Manager and Communication Manager. Endpoints are Avaya 9600 series IP telephones, Avaya 2400 series Digital Telephone, an Avaya Desktop Video Device, a PC running Avaya one-X® Communicator and 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 NL SIP Solution Topology**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya 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 R6.2 SP3 (6.2.0.0.15669 -6.2.12.307)
Avaya S8800 Server	Avaya Aura® System Manager R6.2 (6.2.0.0.15669-6.2.12.9) Update revision No: 6.2.15.1.1959
Dell R310	Avaya Session Border Controller for Enterprise. (4.0.5.Q19)
Avaya 9650 Phone (H.323)	3.171B
Avaya 9621 Phone (SIP)	6.2.0.72
Avaya 2420 Digital Phone	N/A
Analog Phone	N/A
Avaya 4620 Phone (H.323)	1.2200
Avaya 9611 Phone (SIP)	6.2.0.72
Avaya one-X® Communicator (SIP)	6.1.3.06-SP3-35509
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1
<b>Vodafone Netherlands</b>	
Vodafone Office Voice	Vodafone 1.0
Vodafone OneVoice Corporate	Vodafone 1.0
Vodafone VF-CUBE	Cisco 2901 / 15.2(4)M3
Vodafone Core SBC	Acme Packet Net-Net 4500 / 6.2

## 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 NL SIP Trunk Service. For incoming calls, Session Manager receives SIP messages from Vodafone NL and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. Session Manager directs the outbound SIP messages to the Vodafone NL 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 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 NL 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		
<b>Maximum Administered SIP Trunks:</b>			<b>4000</b>	<b>10</b>		

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	
<b>IP Trunks? y</b>		
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 Session Manager. In this case, **SM100** and **10.10.3.55** are the **Name** and **IP Address** for 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
<b>Name</b>	<b>IP Address</b>	
<b>procr</b>	<b>10.10.8.67</b>	
<b>SM100</b>	<b>10.10.3.55</b>	
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
AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5      Keep-Alive Count: 5
```

### 5.4. Administer IP Codec Set

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 NL were configured, namely **G.711A**, **G.729** and **G.711MU**

```
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
2: G.711MU    n           2           20
```



Vodafone NL SIP Trunk Service supports T.38 for transmission of fax. Navigate to **Page 2** to configure T.38 by setting the **Fax Mode** to **t.38-standard** as shown below.

change ip-codec-set 1		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
	Mode	Redundancy
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

## 5.5. Administer SIP Signalling Groups

The signaling group (and trunk group) will be used for inbound and outbound PSTN calls to the Vodafone NL SIP Trunk service. During test, this was configured to use **TCP** and port **5060** to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of 5061 for security. Configure the **Signaling Group** using the **add signaling-group n** command; where **n** is an available signaling group:

- 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 Session Manager (node name **SM100**), 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 5.3**. 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 **Direct IP-IP Early Media** field is set to **n**.
- 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: SM100
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? n
H.323 Station Outgoing Direct Media? n  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 **public-ntwrk**.
- 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: public-ntwrk	Auth Code? n		
		Signaling Group: 1	
		Number of Members: 10	

On **Page 2** of the trunk-group form set the **Preferred Minimum Session Refresh Interval(sec)** to **900** as the optimum value for interworking with the Vodafone NL network. This value defines the interval that subsequent INVITEs must be sent to keep the active session alive. For the compliance testing, the value of **900** seconds was used.

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			

On **Page 3**, set the **Numbering Format** field to **private**. This allows the number to be sent to Vodafone NL in national format with the leading 0.

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

On **Page 4** of this form:

- Set **Send Transferring Party Information** to **n**.
- Set **Network Call Redirection** to **n**.
- Set **Send Diversion Header** to **n** to remove the Diversion Header. This information is not used and increases the size of the INVITE unnecessarily.
- Set **Support Request History** to **n** to remove the History-Info Diversion. This information is not used and increases the size of the INVITE unnecessarily.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Vodafone NL.
- Set **Always Use re-INVITE for Display Updates** to **y** as the most effective method employed by Communication Manager of modifying an existing dialogue.

add trunk-group 1		Page 4 of 21
PROTOCOL VARIATIONS		
<b>Mark Users as Phone? n</b>		
Prepend '+' to Calling Number? n		
<b>Send Transferring Party Information? n</b>		
<b>Network Call Redirection? n</b>		
Send Diversion Header? n		
<b>Support Request History? n</b>		
<b>Telephone Event Payload Type: 101</b>		
Convert 180 to 183 for Early Media? n		
<b>Always Use re-INVITE for Display Updates? y</b>		
Identity for Calling Party Display: P-Asserted-Identity		
Block Sending Calling Party Location in INVITE? n		
Enable Q-SIP? n		

## 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 Numbering

Use the **change private-numbering 0** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **4**-digit extension beginning with **6** will send the calling party number **0387xxxxx1** to Vodafone NL 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					
				Total	
Ext	Ext	Trk	CPN	CPN	
Len	Code	Grp(s)	Prefix	Len	
4	6	1	0387xxxxx1	10	Total Administered: 1
					Maximum Entries: 240

## 5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to Vodafone NL 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 dialplan analysis** command to define a dialed string beginning with **9** of length **1** as a feature access code (**fac**).

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
String	Length	Type	String	Length	Type	String	Length	Type
1	3	dac						
2	4	ext						
60	4	ext						
61	4	ext						
7	1	fac						
8	4	ext						
9	1	fac						
*	3	fac						
#	3	fac						

Use the **change feature-access-codes** command to configure or observe **9** as the **Auto Route Selection (ARS) - Access Code 1**.

<b>change feature-access-codes</b>	Page 1 of 10
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code:	*69
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code:	7
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>	Access Code 2:
Automatic Callback Activation:	Deactivation:
Call Forwarding Activation Busy/DA:	All: Deactivation:
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**. The entry for **06** is used to route to the Vodafone Mobile network. Calls are sent to **Route Pattern 1**, which contains the previously configured SIP Trunk Group.

change ars analysis 0						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		10	11	1	pubu		n
00		13	14	1	pubu		n
06		10	10	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. Set the **Numbering Format** to **unk-unk** to avoid conversion to E.164 format.

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	
Dgts												Intw	
1:	1	0										n	user
2:											n	user	
3:											n	user	
4:											n	user	
5:											n	user	
6:											n	user	
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR													
0	1	2	M	4	W	Request						Dgts	Format
												Subaddress	
1:	y	y	y	y	y	n	n	rest				unk-unk	none
2:	y	y	y	y	y	n	n	rest					none
3:	y	y	y	y	y	n	n	rest					none
4:	y	y	y	y	y	n	n	rest					none
5:	y	y	y	y	y	n	n	rest					none
6:	y	y	y	y	y	n	n	rest					none

## 5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Vodafone NL 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 NL correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **038xxxxxx** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. The **205x** entries are used to allow incoming calls from the Vodafone Mobile network to be directed to assigned extensions. 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	10	038xxxxxx0	all	6100			
public-ntwrk	10	038xxxxxx1	all	6102			
public-ntwrk	10	038xxxxxx2	all	6003			
public-ntwrk	10	038xxxxxx3	all	6004			
public-ntwrk	10	038xxxxxx4	all	6104			
public-ntwrk	4	2050	all	6100			
public-ntwrk	4	2051	all	6102			
public-ntwrk	4	2052	all	6003			
public-ntwrk	4	2053	all	6004			
public-ntwrk	4	2054	all	6104			

## 5.10. EC500 Configuration

When EC500 is enabled on a 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 6100. 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** (e.g., 9) if required by the routing configuration.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnnn**).
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 2396							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
6100	EC500	-	-	0035386nnnnnnnn	1	1	

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



## 6. Configuring Avaya Aura® Session Manager

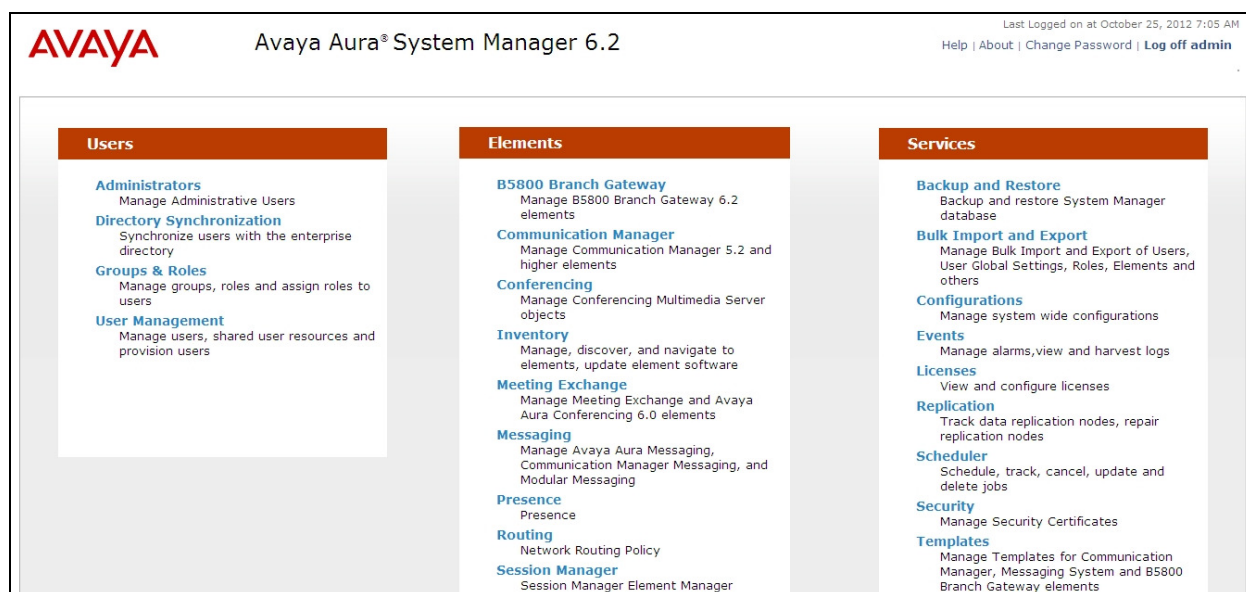
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP domain.
- Administer SIP Location.
- Administer Adaptations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Routing Policies.
- Administer Dial Patterns.

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

### 6.1. Log in to Avaya Aura® System Manager

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL <https://<ip-address>/SMGR>, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed.



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the Introduction to Network Routing Policy screen (not shown).

## 6.2. Administer SIP domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements** → **Routing** and select **Domains** from the left navigation menu, click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter a Domain Name. In the sample configuration, **avaya.com** was used.
- **Type** Verify **SIP** is selected.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.

The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, the title 'Domain Management' is displayed. To the right of the title are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. A warning message states: 'Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.' Below the warning is a horizontal separator line. Underneath, there is a table with the following structure:

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

At the top left of the table area, it says '1 Item Refresh'. At the top right, it says 'Filter: Enable'.

## 6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity.

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **SMGRVL3** defined for the compliance testing.

The screenshot shows the 'Location Details' form for a location named 'SMGRVL3'. The form is divided into several sections: 'General', 'Overall Managed Bandwidth', 'Per-Call Bandwidth Parameters', and 'Location Pattern'. The 'General' section has fields for 'Name' (SMGRVL3) and 'Notes'. The 'Overall Managed Bandwidth' section has fields for 'Managed Bandwidth Units' (Kbit/sec), 'Total Bandwidth', 'Multimedia Bandwidth', and a checkbox for 'Audio Calls Can Take Multimedia Bandwidth' (checked). The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'. The 'Location Pattern' section has an 'Add' button and a table with 3 items. The table has columns for 'IP Address Pattern' and 'Notes'. The table contains three rows with IP address patterns: '10.10.3.\*', '10.10.9.\*', and '10.10.8.\*'. The 'Notes' column is empty for all rows. The form also has 'Commit' and 'Cancel' buttons at the bottom right.

Home / Elements / Routing / Locations - Location Details

Location Details Help ? Commit Cancel

**General**

\* Name:

Notes:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

**Per-Call Bandwidth Parameters**

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

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

Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:  Kbit/sec

**Location Pattern**

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.3.*	<input type="text"/>
<input type="checkbox"/>	* 10.10.9.*	<input type="text"/>
<input type="checkbox"/>	* 10.10.8.*	<input type="text"/>

Select : All, None

\* Input Required Commit Cancel

## 6.4. 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 signaling interface on the connecting system i.e. Communication Manager, Avaya SBCE etc.,
- 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
- Avaya SBCE 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 Session Managers SIP signaling interface.

The screenshot shows the 'SIP Entity Details' configuration page for a Session Manager SIP Entity. The page has a breadcrumb trail at the top: 'Home / Elements / Routing / SIP Entities'. On the right, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The 'General' tab is selected. The form contains the following fields:

- Name:** Session Manager (required, indicated by an asterisk)
- FQDN or IP Address:** 10.10.3.55 (required, indicated by an asterisk)
- Type:** Session Manager (dropdown menu)
- Notes:** (text input field)
- Location:** SMGRVL3 (dropdown menu)
- Outbound Proxy:** (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (text input field)

At the bottom, there is a 'SIP Link Monitoring' section with a dropdown menu set to 'Use Session Manager Configuration'.

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

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

**Port**

3 Items | [Refresh](#) 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**.

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

**General**

**\* Name:**

**\* FQDN or IP Address:**

**Type:**

**Notes:**

**Adaptation:**

**Location:**

**Time Zone:**

Override Port & Transport with DNS SRV: ☐

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

**Credential name:**

**Call Detail Recording:**

**SIP Link Monitoring**

**SIP Link Monitoring:**

### 6.4.3. Avaya Session Border Controller for Enterprise SIP Entities

The following screen shows the SIP entity for the Avaya Session Border Controller 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.

The screenshot shows the 'SIP Entity Details' configuration page for 'VFNL\_SIP\_Trunk\_Fixed'. The page has a breadcrumb trail 'Home / Elements / Routing / SIP Entities' and a 'Help ?' link. The 'General' tab is selected. The configuration fields are as follows:

- Name:** VFNL\_SIP\_Trunk\_Fixed
- FQDN or IP Address:** 10.10.9.80
- Type:** Gateway
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** SMGRVL3
- Time Zone:** Europe/Dublin
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located in the top right corner.

The screenshot shows the 'SIP Entity Details' configuration page for 'VFNL\_SIP\_Trunk\_Mobile'. The page has a breadcrumb trail 'Home / Elements / Routing / SIP Entities' and a 'Help ?' link. The 'General' tab is selected. The configuration fields are as follows:

- Name:** VFNL\_SIP\_Trunk\_Mobile
- FQDN or IP Address:** 10.10.9.81
- Type:** Gateway
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** SMGRVL3
- Time Zone:** Europe/Dublin
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none

Buttons for 'Commit' and 'Cancel' are located in the top right corner.

## 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 **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 6.4**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop-down menu to make the other system trusted.
- 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.

1 Item Refresh		Filter: Enable					
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* CM Link	* Session Manager	TCP	* 5060	* Communication Manager	* 5060	Trusted	

1 Item Refresh		Filter: Enable					
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* VFNL Fixed Link	* Session Manager	TCP	* 5060	* VFNL_SIP_Trunk_Fixed	* 5060	Trusted	

1 Item Refresh		Filter: Enable					
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* VFNL Mobile Link	* Session Manager	TCP	* 5060	* VFNL_SIP_Trunk_Mobile	* 5060	Trusted	

## 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:

The screenshot shows the 'Routing Policy Details' form for a policy named 'toCommunication Manager'. The 'General' tab is active. The 'Name' field is populated with 'toCommunication Manager'. The 'Disabled' checkbox is unchecked. The 'Retries' field is set to 0. The 'Notes' field is empty. Below the 'General' tab is the 'SIP Entity as Destination' section, which includes a 'Select' button. At the bottom, a table lists the selected SIP entity:

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.8.67	CM	

The following screen shows the routing policy for Avaya Session Border Controller for Enterprise Fixed:

The screenshot shows the 'Routing Policy Details' form for a policy named 'VFNL External Fixed'. The 'General' tab is active. The 'Name' field is populated with 'VFNL External Fixed'. The 'Disabled' checkbox is unchecked. The 'Retries' field is set to 0. The 'Notes' field is empty. Below the 'General' tab is the 'SIP Entity as Destination' section, which includes a 'Select' button. At the bottom, a table lists the selected SIP entity:

Name	FQDN or IP Address	Type	Notes
VFNL_SIP_Trunk_Fixed	10.10.9.80	Gateway	



The following screen shows the routing policy for Avaya Session Border Controller for Enterprise Mobile:

Home / Elements / Routing / Routing Policies

Routing Policy Details [Help ?](#)

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
VFNL_SIP_Trunk_Mobile	10.10.9.81	Gateway	

## 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 6.6**. Click **Select** button to save (not shown). The following screen shows an example dial pattern configured for Vodafone NL SIP Trunk Service Fixed.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel Help ?

General

\* Pattern: 00353

\* Min: 5

\* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		VFNL External Fixed	0	<input type="checkbox"/>	VFNL_SIP_Trunk_Fixed	

The following screen shows an example dial pattern configured for Vodafone NL SIP Trunk Service Mobile.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Help ?

Commit Cancel

General

\* Pattern: 06

\* Min: 2

\* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh 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"/>	SMGRVL3		VFNL External Mobile	0	<input type="checkbox"/>	VFNL_SIP_Trunk_Mobile	

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Help ?

Commit Cancel

General

\* Pattern: 038700

\* Min: 6

\* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

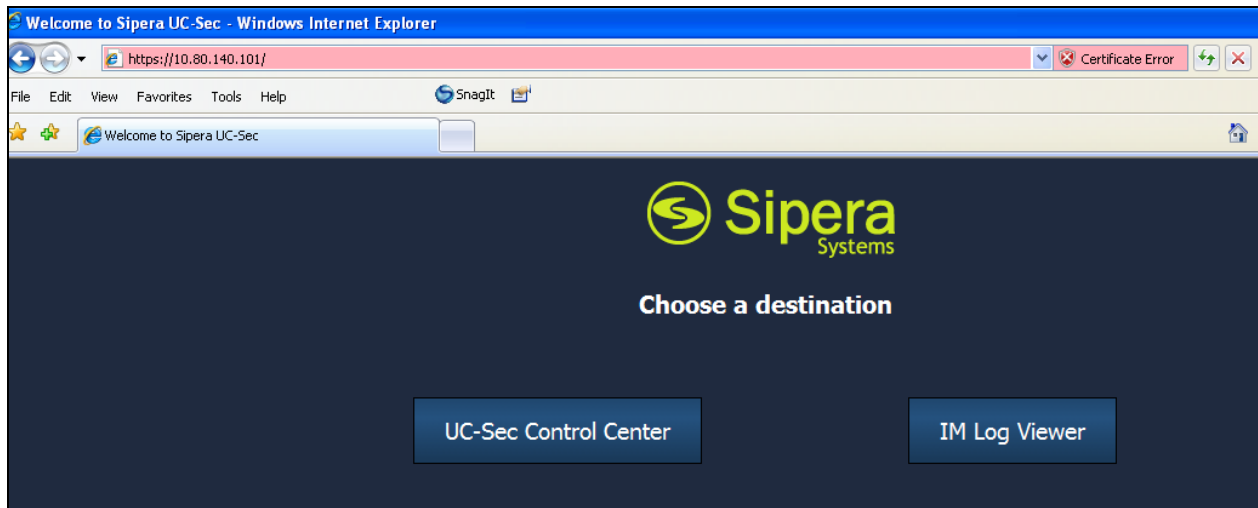
<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		toCommunication Manager	0	<input type="checkbox"/>	Communication Manager	

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. The Avaya SBCE is administered using the UC-Sec Control Center.

### 7.1. Accessing UC-Sec Control Centre

Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Select the **UC-Sec Control Center**.



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

A screenshot of the UC-Sec Control Center login page. The page has a dark blue header with the "Sipera Systems" logo and the tagline "LEARN - VERIFY - PROTECT". On the right side, there is a white "Sign in" box. Inside this box, there are two input fields: "Login ID" and "Password". Below these fields is a yellow "Sign in" button. Below the header, there is a paragraph of text: "The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks." Below this paragraph is a link: "Visit the Sipera Systems website to learn more." At the bottom, there is a "NOTICE TO USERS" section: "NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address."

The main page of the UC-Sec Control Center will appear.

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 10:17:32 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

Welcome

**Securing your real-time unified communications**

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail [support@sipera.com](mailto:support@sipera.com).

Alarms (Past 24 Hours)	Incidents (Past 24 Hours)
None found.	Sipera: Server Heartbeat is UP
	Sipera: Server Heartbeat is failed
	Sipera: Server Heartbeat is UP
	Sipera: Server Heartbeat is UP
	Sipera: Server Heartbeat is UP

Administrator Notes [ Add ]

No notes posted.

**Quick Links**

- Sipera Website
- Sipera VIPER Labs
- Contact Support

UC-Sec Devices	Network Type
Sipera	DMZ_ONLY

To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP\_SBC1** is shown. To view the configuration of this device, click the monitor icon highlighted in screenshot below.

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 3:40:58 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Log

UC-Sec Control Center

System Management

Installed Updates

Device Name	Serial Number	Version	Status			
GSSCP-SBC1	IPCS31020128	4.0.5.Q19	Commissioned			

The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

System Information: GSSCP-SBC1

Network Configuration

General Settings

Appliance Name	GSSCP-SBC1
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.10.9.81	10.10.9.81	255.255.255.0	10.10.9.1	A1
192.168.27.2	192.168.27.2	255.255.255.240	192.168.27.1	B1
10.10.9.80	10.10.9.80	255.255.255.0	10.10.9.1	A1
192.168.27.3	192.168.27.3	255.255.255.240	192.168.27.1	B1

DNS Configuration

Primary DNS	10.10.7.100
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.9.81

Management IP(s)

IP	10.10.2.40
----	------------

## 7.2. Global Profiles

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

### 7.2.1. Server Internetworking - Avaya

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

- Enter profile name such as **Call\_Server** and click **Next** (Not Shown)
- **Check Hold Support= RFC2543**
- **Check T.38 Support**
- All other options on the **General** Tab can be left at default

Profile: Call_Server	
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 checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<b>Next</b>	



Default values can be used for the next window that appears. Click **Finish**.

The screenshot shows a window titled "Profile: Call\_Server" with a close button in the top right corner. The window is divided into two main sections: "Privacy" and "DTMF".

Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

At the bottom of the window, there are two buttons: "Back" and "Finish".

Default values can be used for the **Advanced Settings** window. Click **Finish**

The screenshot shows a window titled "Profile: Call\_Server" with a close button in the top right corner. The window is divided into two main sections: "Advanced Settings" and "Finish".

Advanced Settings	
Record Routes	<input checked="" type="radio"/> None <input type="radio"/> Single Side <input type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input checked="" type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

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



### 7.2.2. Server Internetworking – Vodafone NL

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 such as **VFNL\_Trunk** and click **Next** (Not Shown)
- **Check Hold Support= RFC2543**
- **Check T.38 Support**
- 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 checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

Default values can be used for the next window that appears. Click **Finish**.

The screenshot shows a window titled "Profile: VFNL\_Trunk" with a close button in the top right corner. The window is divided into two main sections: "Privacy" and "DTMF".

Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

At the bottom of the window, there are two buttons: "Back" and "Finish".

Default values can be used for the **Advanced Settings** window. Click **Finish**.

The screenshot shows a window titled "Profile: VFNL\_Trunk" with a close button in the top right corner. The window is divided into two main sections: "Advanced Settings" and "Finish".

Advanced Settings	
Record Routes	<input type="checkbox"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

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

### 7.2.3. Routing

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

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

Create a Routing Profile for Session Manager and Routing Profiles for Vodafone NL Fixed and Mobile networks. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue. In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select “\*” from the drop down box
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server, e.g. Session Manager
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
- **Routing Priority Based on Next Hop Server:** Checked
- **Use Next Hop for In-Dialog Messages:** Select only if there is no secondary Next Hopserver
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

Click **Finish**.

The following screen shows the Routing Profile to Session Manager.

Global Profiles > Routing: Call\_Server

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	*	10.10.3.55	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The following screen shows the Routing Profile to Vodafone NL Fixed network.

Global Profiles > Routing: VFNL\_Fixed

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	*	62.140.159.233	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

The following screen shows the Routing Profile to Vodafone NL Mobile network.

Global Profiles > Routing: VFNL\_Mobile

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	*	62.140.159.234	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

#### 7.2.4. Server Configuration– Avaya Aura® Session Manager

Servers are defined for each server connected to the Avaya SBCE. In this case, the Vodafone NL SBC is connected as the Trunk Server and Session Manager is connected as the Call Server. The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow 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** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**
- Enter **IP Addresses / Supported FQDNs** to **10.10.3.55** (Session Manager IP Address)
- For **Supported Transports**, check **TCP**
- **TCP Port:5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs

Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.10.3.55
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
Finish	

On the **Advanced** tab:

- Select **Call\_Server** for **Interworking Profile**
- Click **Finish**

The screenshot shows a window titled "Server Configuration Profile - Advanced". It contains a table with configuration options:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Call_Server
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

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

### 7.2.5. Server Configuration– Vodafone NL

To define the Vodafone NL SBC as two separate Trunk Servers for the Fixed and Mobile networks, navigate to select **Global Profiles** → **Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**
- Set **IP Address** to **64.140.159.233** (Vodafone NL Fixed Trunk)
- **Supported Transports**: Check **UDP**
- **UDP Port**: **5060**
- Hit **Next**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs

**Server Configuration Profile - General**

Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	62.140.159.233
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	

Finish

On the **Advanced** tab:

- Select **VFNL\_Trunk** for **Interworking Profile**
- Click **Finish**

**Server Configuration Profile - Advanced**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	VFNL_Trunk
Signaling Manipulation Script	None
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish



Repeat the process for Vodafone NL Mobile Trunk Server and in the **IP Addresses / Supported FQDNs** box, type the IP address of the Vodafone NL SBC that's to be used for the mobile network.

**Server Configuration Profile - General**

Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma separated list	62.140.159.234
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	

Finish

**Server Configuration Profile - Advanced**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	VFNL_Trunk
Signaling Manipulation Script	None
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish



## 7.2.6. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten or next hop IP addresses can be used. As IP addressing was used in test instead of domain names, there was little requirement for topology hiding. IP addresses are translated to the Avaya SBCE external addresses using NAT. To define Topology Hiding for Session Manager, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for Session Manager and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line, To** as the required headers from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Next Hop** was used for test

**Note:** The use of **Next Hop** results in the IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used for the **Request-Line** header with the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the Vodafone NL network.

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

To define Topology Hiding for the Vodafone NL SBC, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Vodafone NL SBC and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line**, **To** as the required headers from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Next Hop** was used for test

Global Profiles > Topology Hiding: VFNL

[Add Profile](#) [Rename Profile](#) [Clone Profile](#) [Delete Profile](#)

Topology Hiding Profiles

default

cisco\_th\_profile

Call\_Server

**VFNL**

Click here to add a description.

Topology Hiding

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

[Edit](#)

## 7.3. Device Specific Settings

The Device Specific Settings feature allows aggregation of system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network.

### 7.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.

The screenshot shows the 'Network Configuration' tab for device 'GSSCP-SBC1'. It includes a warning banner about IP address changes requiring a restart. Below are input fields for A1, A2, B1, and B2 netmasks. A table lists IP addresses, public IPs, gateways, and interfaces (A1, B1) with 'Add IP' and 'Toggle State' buttons.

IP Address	Public IP	Gateway	Interface
10.10.9.81		10.10.9.1	A1
192.168.27.2		192.168.27.1	B1
10.10.9.80		10.10.9.1	A1
192.168.27.3		192.168.27.1	B1

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

The screenshot shows the 'Interface Configuration' tab for device 'GSSCP\_V9'. It displays a table with interface names (A1, A2, B1, B2), their administrative status (Enabled/Disabled), and a 'Toggle State' button for each.

Name	Administrative Status	Toggle State
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

### 7.3.2. Media Interface

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signalling Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface for the Vodafone NL fixed network
- Select an **internal** interface IP address defined in **Section 7.3.1**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface for the Vodafone NL fixed network
- Select an **external** interface IP address (not shown) defined in **Section 7.3.1**
- Select **RTP port** ranges for the media path with the Vodafone NL SBC
- Repeat this process for the internal and external signalling interfaces for the Vodafone NL mobile network.

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces. After the Media Interfaces are created, an application restart is necessary before the changes will take effect.

Device Specific Settings > Media Interface: GSSCP-SBC1









UC-Sec Devices

GSSCP-SBC1

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		
Int_Media_Mobile	10.10.9.81	35000 - 40000		
Ext_Media_Fixed	192.168.27.2	35000 - 40000		
Int_Media_Fixed	10.10.9.80	35000 - 40000		
Ext_Media_Mobile	192.168.27.3	35000 - 40000		

### 7.3.3. Signalling Interface

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

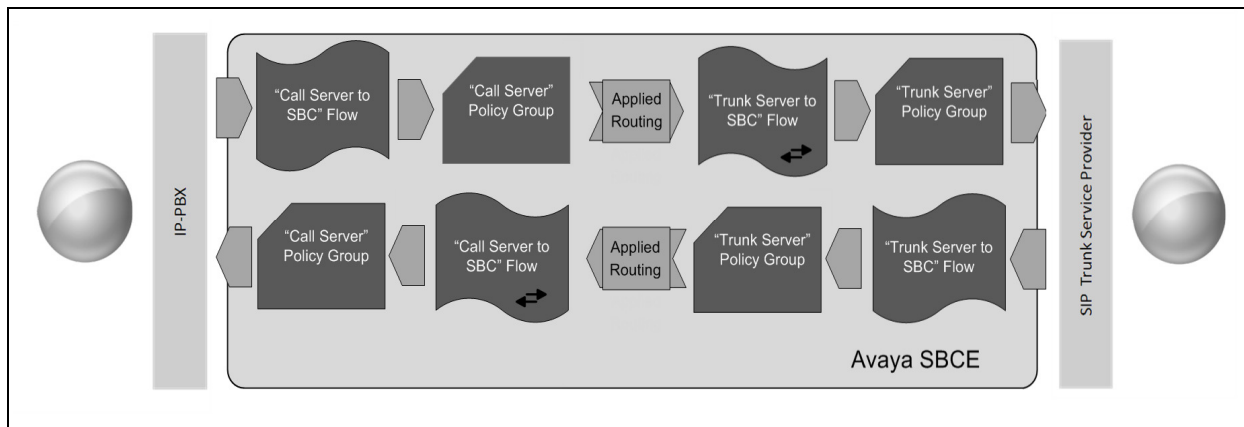
- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface for the Vodafone NL fixed network
- Select an **internal** interface IP address defined in **Section 7.3.1**
- Select **UDP** and **TCP** port numbers, **5060** is used for Vodafone NL
- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external signalling interface for the Vodafone NL fixed network
- Select an **external** interface IP address (not shown) defined in **Section 7.3.1**
- Select **UDP** and **TCP** port numbers, **5060** is used for Vodafone NL
- Repeat this process for the internal and external signalling interfaces for the Vodafone NL mobile network.

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

Device Specific Settings > Signaling Interface: GSSCP-SBC1						
UC-Sec Devices						
GSSCP-SBC1						
Signaling Interface						
Add Signaling Interface						
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig_Mobile	10.10.9.81	5060	5060	---	None	 
Ext_Sig_Fixed	192.168.27.2	---	5060	---	None	 
Int_Sig_Fixed	10.10.9.80	5060	5060	---	None	 
Ext_Sig_Mobile	192.168.27.3	---	5060	---	None	 

### 7.3.4. End Point Flows

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.






This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the Vodafone NL SBC for both fixed and mobile calls and vice versa. The following screenshot shows all flows:




Device Specific Settings > End Point Flows: GSSCP-SBC1													
UC-Sec Devices GSSCP-SBC1	Subscriber Flows		Server Flows										
	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	ASM_Call_Server_Fixed	*	*	*	Ext_Sig_Fixed	Int_Sig_Fixed	Int_Media_Fixed	default-low	VFNL Fixed	SM9_CS	None	
	2	ASM_Call_Server_Mobile	*	*	*	Ext_Sig_Mobile	Int_Sig_Mobile	Int_Media_Mobile	default-low	VFNL Mobile	SM9_CS	None	
	Server Configuration: VFNL Trunk Fixed												
	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	VFNL_Trunk_Server_Fixed	*	*	*	Int_Sig_Fixed	Ext_Sig_Fixed	Ext_Media_Fixed	default-low	SM9_Call_Server	SP_Trunk	None	
	Server Configuration: VFNL Trunk Mobile												
	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	VFNL_Trunk_Server_Mobile	*	*	*	Int_Sig_Mobile	Ext_Sig_Mobile	Ext_Media_Mobile	default-low	SM9_Call_Server	SP_Trunk	None	

To define an outgoing Server Flow for the fixed network, navigate to **Device Specific Settings** → **End Point Flows**.

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the outgoing server flow to the Vodafone NL SBC for the fixed network
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3.3**
- In the **Signalling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3.3**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3.2**
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.2.3**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone NL SBC defined in **Section 7.2.6** and click **Finish**

Server Configuration: VFNL_Fixed												
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	SP_Trunk_Server_Fixed	*	*	*	Int_Sig_Fixed	Ext_Sig_Fixed	Ext_Media_Fixed	default-low	Call_Server	Call_Server	None	  

Repeat the process for an outgoing Server Flow for the mobile network. In the **Name** field enter a descriptive name for the outgoing server flow to the Vodafone NL SBC for the mobile network.

Server Configuration: VFNL_Mobile												
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	SP_Trunk_Server_Mobile	*	*	*	Int_Sig_Mobile	Ext_Sig_Mobile	Ext_Media_Mobile	default-low	Call_Server	Call_Server	None	  



The incoming Server Flows are defined as a reversal of the outgoing Server Flows

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the incoming server flow to Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3.3**
- In the **Signalling Interface** drop-down menu, select the internal SIP signalling defined in **Section 7.3.3**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3.2**
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone NL SBC defined in **Section 7.2.3**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.2.6** and click **Finish**

Server Configuration: Call_Server												Update Order	
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signalling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
1	SM9_Call_Server_Fixed	*	*	*	Ext_Sig_Fixed	Int_Sig_Fixed	Int_Media_Fixed	default-low	VFNL_Fixed	VFNL	None		
2	SM9_Call_Server_Mobile	*	*	*	Ext_Sig_Mobile	Int_Sig_Mobile	Int_Media_Mobile	default-low	VFNL_Mobile	VFNL	None		



## 8. Vodafone NL Configuration

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

## 9. Verification Steps

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

1. From System Manager Home Tab click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP 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 Vodafone NL SBC for the fixed network:

Home / Elements / Session Manager / System Status / SIP Entity Monitoring							
SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: VFNL SIP Trunk Fixed							
Summary View							
1 Item   Refresh							
Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.9.80	5060	TCP	Up	200 OK	Up

This is the SIP Entity link to the Vodafone NL SBC for the mobile network:

Home / Elements / Session Manager / System Status / SIP Entity Monitoring							
SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: VFNL SIP Trunk Mobile							
Summary View							
1 Item   Refresh							
Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.9.81	5060	TCP	Up	200 OK	Up

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

status trunk 1			
TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no
0001/004	T00004	in-service/idle	no
0001/005	T00005	in-service/idle	no
0001/006	T00006	in-service/idle	no
0001/007	T00007	in-service/idle	no
0001/008	T00008	in-service/idle	no
0001/009	T00009	in-service/idle	no
0001/010	T00010	in-service/idle	no

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

## 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 for Enterprise to Vodafone NL SIP Trunk Service. The testing was successfully performed with Vodafone NL, 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 6.2*, March 2012.
- [2] *Administering Avaya Aura® System Platform Release 6.2*, February 2012.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.0.1, April 2011.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, February 2012, Document Number 555-245-205.
- [5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.
- [6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473
- [7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.
- [8] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2
- [10] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

---

**©2013 Avaya Inc. All Rights Reserved.**

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

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