

Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Belgacom 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. Belgacom 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 Belgacom 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 Belgacom 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 Belgacom.

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 Belgacom. 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 Belgacom 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 Belgacom 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.
- 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 Belgacom products please contact the Belgacom authorized representative at: <u>ippbx.certification@belgacom.be</u>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Belgacom 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 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.

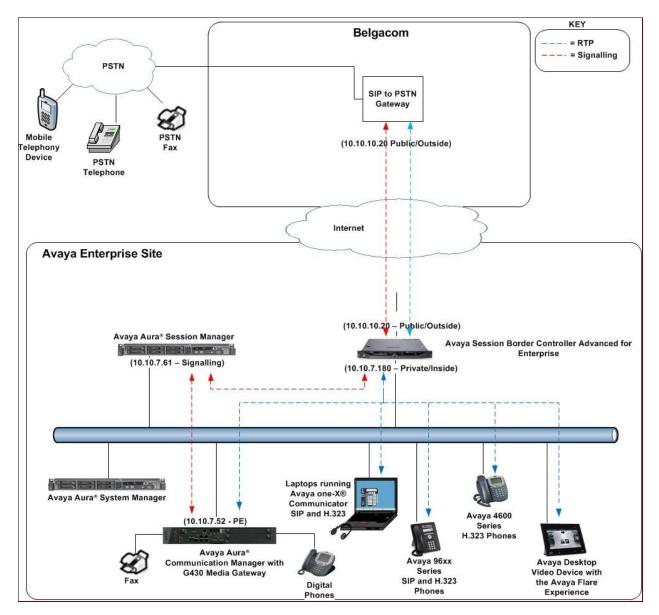


Figure 1: Belgacom SIP Solution Topology

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 4 of 40 BELGACOMASBCAE

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	HW31 FW093
MM712 Digital	HW07 FW009
MGP Firmware	30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.2
	(6.2.0.0.620110)
Avaya S8800 Server	Avaya Aura® System Manager R6.2
	(6.2.0.0.15669-6.2.12.9)
	Update revision No: 6.2.12.1.1822
Dell R310 running Avaya Session	Avaya Session Border Controller Advanced for
Border Controller Advanced for	Enterprise (4.0.5.Q02)
Enterprise	
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 one-X® Communicator	6.1
Avaya Desktop Video Device	1.0.2
Belgacom SIP Trunking	IMS Solution: Alcatel-Lucent IMS7.6
	ISC: Release 6.2.1
	Application Server: Broadworks Release 16sp1

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 Belgacom SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from Belgacom 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 directs the outbound SIP messages to the Belgacom 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 Belgacom network, and any other SIP trunks used.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES	U	SED		
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 3	0		

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

display system-parameters custome	-	11
0	PTIONAL FEATURES	
Emergency Access to Attendant? Enable 'dadmin' Login?	-	з? у
Enhanced Conferencing? Enhanced EC500?	y ISDN Feature Plus	-
Enterprise Survivable Server?	n ISDN-BRI Trunk:	з? у
Enterprise Wide Licensing?	n ISDN-PR	Г? У
ESS Administration?	n Local Survivable Processo:	:? n
Extended Cvg/Fwd Admin?	y Malicious Call Trace	≥? У
External Device Alarm Admin?	y Media Encryption Over II	?? n
Five Port Networks Max Per MCC? Flexible Billing?		.? n
Forced Entry of Account Codes?	y Multifrequency Signaling	d; A
Global Call Classification?	y Multimedia Call Handling (Basic)	? у
Hospitality (Basic)?	y Multimedia Call Handling (Enhanced)	? у
Hospitality (G3V3 Enhancements)?	y Multimedia IP SIP Trunking	j?n
IP Trunks?	У	
IP Attendant Consoles?	Y 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-region** 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

```
Page 1 of 20
change ip-network-region 1
                              IP NETWORK REGION
 Region: 1
             Authoritative Domain: avaya.com
Location: 1
   Name: Default NR
MEDIA PARAMETERS
                              Intra-region IP-IP Direct Audio: yes
     Codec Set: 1
                              Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 35000
                                        IP Audio Hairpinning? n
  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
```

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 Belgacom were configured, namely **G.711A** and **G.729**.

change ip-codec-set 1						1 of	2
					-		
	тп	Codec Set					
	IP	codec set	•				
Codec Set: 1	L						
Audio	Silence	Frames	Packet				
Codec							
	Suppression						
1: G.711A	n	2	20				
2: G.729	n	2	20				

Belgacom 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-se	t 1		Page	2 of	2
	Allow	Direct-IP Multimedia? n			
	Mode	Redundancy			
FAX	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 Belgacom 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:	-
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
Fa	ar-end Network Region: 1
Far-end Domain:	
	Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate	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 n** command, where **n** 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-grou	up 1			Page	1 of	21
	-	TRUNK GROUP		-		
Group Number:	1	Group Type: s:	ip (CDR Repor	rts: y	
Group Name:	smpub	COR: 1	TN: 1	TAC: 1	L01 -	
Direction:	two-way	Outgoing Display? n				
Dial Access?	n		Night Servio	ce:		
Queue Length:	0					
Service Type:	tie	Auth Code? n				
			Signali Number of	ing Group E Members		

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 Belgacom 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 OPTI	M Failure:	8000	
SCCAN? n Digital I	oss Group:	18	
Preferred Minimum Session Refresh Inte	erval(sec):	1800	

On **Page 3**, set the **Numbering Format** field to **public.** This allows the number to be sent to Belgacom with 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: public

UUI 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

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? n

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 public-unknown-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 **0325xxxxxxx** to Belgacom 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 public-unknown-numbering 0 Page 1 of 2							
			NUMBE	RING - PUBLIC/U	INKNOWN	FORMAT	
					Total		
	Ext	Ext	Trk	CPN	CPN		
	Len	Code	Grp(s)	Prefix	Len		
						Total Administered: 1	
	4	1	1	325xxxxxxx	10	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 Belgacom 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: Deact	ivation:		
Call Forwarding Activation Busy/DA: *87 All: *88 Deact	ivation:	#88	
Call Forwarding Enhanced Status: Act: Deact	ivation:		

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 D	IGIT ANALYS	ΞE			
		Location:	all		Percent Full:	1
Dialed	Total	Route	Call	Node	ANI	
String	Min Max	Pattern	Туре	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
                        Dqts
                                                              Tntw
1:1 0
                                                               n
                                                                  user
2:
                                                               n
                                                                  user
3:
                                                               n
                                                                   user
4:
                                                               n
                                                                   user
5:
                                                                   user
                                                               n
                                                               n
6:
                                                                  user
    BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR
   0 1 2 M 4 W Request
                                                   Dqts Format
                                                 Subaddress
1: yyyyyn n
                        rest
                                                                  none
2: yyyyyn 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 Belgacom 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 Belgacom correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **+325xxxxxxx** 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 1Page 1 of 3INCOMING CALL HANDLING TREATMENTService/NumberNumberDel InsertFeatureLenDigitspublic-ntwrk11+325xxxxxxall 1306public-ntwrk11+325xxxxxxall 1307public-ntwrk11+325xxxxxxall 1601public-ntwrk11+325xxxxxxall 1601public-ntwrk11+325xxxxxxall 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 Location
- 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.

AVAYA	Avaya Aura™ Sy	stem Manager 6.1	Help About Change Password Log off ad
Users		Elements	Services
Administrators Manage Administ Groups & Roles Manage groups, users Synchronize use directory, import User Management	roles and assign roles to Import 's with the enterprise users from file	Application Management Manage applications and application certificates Ocnomunication Manager Manage Communication Manager objects Conferencing Deferencing Manage, discover, and navigate to elements, update element software Messaging Manage Messaging System objects Presence Presence Routing Network Routing Policy SIP AS 8.1 SIP AS 8.1 Session Manager Element Manager	Backup and Restore Backup and restore System Manager database Configurations Manage system wide configurations Events Manage alarms,view and harvest logs Licenses View and configure licenses Replication Track data replication nodes, repair replication nodes Scheduler Schedule, track, cancel, update and delete jobs Security Manage Security Certificates Templates Manage Templates for Communication Manager and Messaging System objects

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).

Routing	Home / Elements / Routing / Domains - Domain Management					
Domains	Domain Management					
Locations	_					
Adaptations	Edit New Duplicate Delete More Actions -					
SIP Entities						
Entity Links	2 Items Refresh					
Time Ranges	□ Name	Туре	Default			
Routing Policies	<u>avaya.com</u>	sip				

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. Click **Commit** to save changes. Below is the location configuration used for the simulated enterprise.

* Routing	Home / Elements / Routing / Locations - Location Details	
Domains	Location Details	Commit
Locations	Location Details	comme
Adaptations	Call Admission Control has been set to ignore SDP. All calls will be counted using the De	fault Audio Bandwidth.
SIP Entities	See Session Manager -> Session Manager Administration -> Global Setting	
Entity Links	General	
Time Ranges		
Routing Policies	* Name: SPLab7	
Dial Patterns	Notes:	
Regular Expressions		
Defaults	Overall Managed Bandwidth	
	Total Bandwidth: Per-Call Bandwidth Parameters * Default Audio Bandwidth: 80 Kbit/s Location Pattern Add Remove	sec 💌
	3 Items Refresh	Filter: E
	IP Address Pattern	Notes
	* 10.10.9.*	
	* 10.10.8.*	
	* 10.10.7.*	

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

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.

Routing	Home / Elements / Routing /	/ SIP Entities - SIP Entit	y Details		
Domains	SIP Entity Details				Commit
Locations					Comme
Adaptations	General			1	
SIP Entities		* Name:	ASMdot7		
Entity Links		* FQDN or IP Address:	10.10.7.61		
Time Ranges		Type:	Session Manager		
Routing Policies		Notes:		1	
Dial Patterns		Notes.			
Regular Expressions		Location:	SIPLab7 💌		
Defaults		Outbound Proxy:	×		
		Time Zone:	Etc/GMT		
		Credential name:			
	SIP Link Monitoring			=	
		SIP Link Monitoring:	Use Session Manager Configuration	*	

The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **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 Add	Remove					
3 Iten	ns Refresh					Filter: Enable
	Port	A	Protocol	Default Domain	Notes	
	5060		UDP 💌	avaya.com 🔹		
	5060		TCP -	avaya.com		
	5061		TLS 💌	avaya.com		
Select	t : All, None					
* Input	Required					Commit Cancel

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	Home / Elements / Routing / SIP Entities - SIP Entity Details
Domains	SIP Entity Details Commit
Locations	
Adaptations	General
SIP Entities	* Name: CMEVO
Entity Links	* FQDN or IP Address: 10.10.7.52
Time Ranges	Type: CM 💌
Routing Policies	Notes:
Dial Patterns	
Regular Expressions	Adaptation:
Defaults	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: Use Session Manager Configuration 💌

6.4.3. Avaya Session Border Controller Advanced for Enterprise SIP Entities

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.

Αναγα	Avaya Aura® System Manager 6.1	Help About Change Password Log off
-		Routing *
Routing	Home / Elements / Routing / SIP Entities - SIP Entity Details	
Domains	SIP Entity Details	Commit
Locations		Comme
Adaptations	General	
SIP Entities	* Name: ASBCAE	
Entity Links	* FQDN or IP Address: 10.10.7.180	
Time Ranges	Type: Gateway	
Routing Policies	Notes:	
Dial Patterns		
Regular Expressions	Adaptation:	
Defaults	Location: SPLab7	
	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								
Entity Links	1 Item Refresh							Filter:
Time Ranges	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
Routing Policies	* toCM	* ASM61 💌	TCP -	* 5060	* CMEVO	* 5060	Trusted	
Dial Patterns								
Regular Expressions								
Defaults	* Input Required							Commit

SIP Entities								
Entity Links	1 Item Refresh							Filte
Time Ranges	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
Routing Policies	* toASBCAE	* ASM61 💽	TCP 💽	* 5060	* ASBCAE	* 5060	Trusted	
Dial Patterns								
Regular Expressions								
Defaults	* Input Required							Comm

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	General				
SIP Entities		* Name:	TO CMEVO		
Entity Links					
Time Ranges		Disabled:			
Routing Policies		Notes:			
Dial Patterns					
	SIP Entity as Do	estination			
Regular Expressions	SIF LIULY as D	and the second			
Regular Expressions Defaults	Select				
		FQDN or IP Address		Туре	Notes

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

Adaptations	General		
SIP Entities	oonordi	* Name: to_ASBCAE	
Entity Links			
Time Ranges		Disabled: 🗌	
Routing Policies		Notes:	
Dial Patterns			
Regular Expressions	SIP Entity as Destination		
Defaults	Select		
	Name	FQDN or IP Address	Type N
	ASBCAE	10.10.7.180	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 -ALL-

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 Belgacom SIP Trunk Service.

Domains							
Locations	Dial Pattern Details						Commit
Adaptations	Company						
SIP Entities	General		-		1		
Entity Links		* Pattern: (
Time Ranges		* Min: 9	9				
Routing Policies		* Max:	13				
Dial Patterns	E	mergency Call:					
Regular Expressions	Eme	rgency Priority:	1				
Defaults	Er	mergency Type:					
		SIP Domain:	-ALL-				
		Notes:					
	Originating Locations and Routing	g Policies					
	Add Remove						
	1 Item Refresh						Filter: 6
	Originating Location Name 1 🔺	Originating Locat Notes	tion Routing Polic Name	Rank 2 🛋	Routing Policy Disabled	Routing Policy Destination	Routing Po Notes
	-ALL-	Any Locations	ToASBCAE	0		ASBCAE	

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

Domains							
Locations	Dial Pattern Details						Commit
Adaptations							
SIP Entities	General				1		
Entity Links		* Pattern: +325					
Time Ranges		* Min: 10					
Routing Policies		* Max: 11]				
Dial Patterns	Em	nergency Call: 🔲			1		
Regular Expressions	Emerg	ency Priority: 1					
Defaults	Eme	ergency Type:					
		SIP Domain: -ALL-	~				
	L	Notes:					
	Originating Locations and Routing	Policies					
	Add Remove						
	1 Item Refresh						Filter: B
)riginating Location lotes	Routing Policy Name	Rank 2 🛋	Routing Policy Disabled	Routing Policy Destination	Routing Po Notes
	-ALL- A	ny Locations	ToCMEVO	0		CMEVO	

7. Avaya Session Border Controller Advanced for Enterprise Configuration

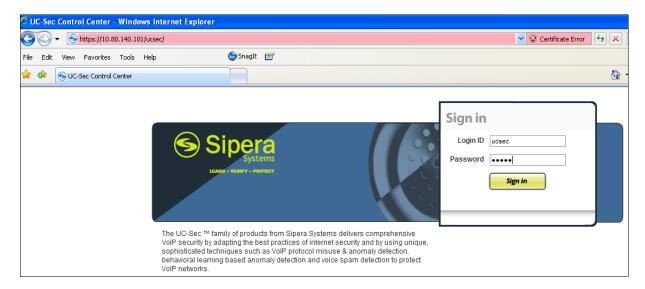
This section provides the procedures for configuring Session Border Controller Advanced or Enterprise.

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).

🗧 Welcome to Sipera UC-Sec - Windows Internet Explo	prer	
🕒 🕞 👻 🙋 https://10.80.140.101/		💌 😵 Certificate Error 😽 🗙
File Edit View Favorites Tools Help	SnagIt 📷	
🖌 🚸 🌈 Welcome to Sipera UC-Sec		🟠 -
	Sipera Systems Choose a destination	
	UC-Sec Control Center	IM Log Viewer

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



Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

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 left-hand menu select Global Profiles \rightarrow Server Interworking and click on Add Profile. Enter Profile Name: ToASM and click Next. Check Hold Support to RFC2543 – c 0.0.0.0. All other options on the General tab can be left at default. Click on Next on the following screens and then Finish.

Editin	g Profile: ToA SM 🛛 🔀
	General
Hold Support	 None RFC2543 - c=0.0.0.0 RFC3264 - a=sendonly
180 Handling	⊙ None ○ SDP ○ No SDP
181 Handling	⊙ None ○ SDP ○ No SDP
182 Handling	⊙ None ○ SDP ○ No SDP
183 Handling	⊙ None ○ SDP ○ No SDP
Refer Handling	
3xx Handling	
Diversion Header Support	
Delayed SDP Handling	
T.38 Support	
URI Scheme	
Via Header Format	 RFC3261 RFC2543
	Next

7.2.2. Server Internetworking – Belgacom 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** \rightarrow Server **Interworking** and click on **Add Profile**. Enter profile name: **ToBelgacom** and click on **Next**. Check **Hold Support** to **RFC2543** – **c=0.0.0.** All other options on the **General** tab can be left at default. Click on **Next** on the following screens and then **Finish**.

Editing	Editing Profile: ToBelgacom				
	General				
Hold Support	 None RFC2543 - c=0.0.0.0 RFC3264 - a=sendonly 				
180 Handling	💿 None 🔘 SDP 🔘 No SDP				
181 Handling	💿 None 🔿 SDP 🔿 No SDP				
182 Handling	💿 None 🔿 SDP 🔿 No SDP				
183 Handling	⊙ None ○ SDP ○ No SDP				
Refer Handling					
3xx Handling					
Diversion Header Support					
Delayed SDP Handling					
T.38 Support					
URI Scheme	💿 SIP 🔘 TEL 🔘 ANY				
Via Header Format	 RFC3261 RFC2543 				
	Hext				

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** \rightarrow **Routing** and click on **Add Profile**.

- Enter **Profile Name: ASM_7**
- Hit Next (not shown)
- Set Next Hop Server 1 to 10.10.7.61 (Session Manager IP address)
- Select Routing Priority Based on Next Hop Server
- Select use Next Hop in Dialog Messages
- Set **Outgoing Transport** to **TCP**
- Click **Finish** (not shown)

The screen below is a result of the details configured above

Global Profiles > Routing: ASM_7					_			_	_		
Add Profile						Rei	name P	rofile Cl	lone Profi	le Delete	Profile
Routing Profiles			C	lick here to add a descri	ption.						
default	Routing Pro	file									
ASM_7	litterating										
VDE									Ad	ld Routing R	lule
	Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	lgnore Route Header	Outgoing Transport	
	1	*	10.10.7.61		◄			•		TCP	ø

7.2.4. Routing – Belgacom 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** \rightarrow **Routing** and click on **Add Profile**.

- Enter **Profile Name** as **Belgacom**
- Hit Next
- Set Next Hop Server 1 to 10.10.10.10 (IP Address provided by Belgacom)
- Select Routing Priority Based on Next Hop Server
- Select use Next Hop in Dialog Messages
- Set Outgoing Transport to UDP
- Click **Finish** (not shown)

The screen below is a result of the details configured above

Add Profile						F	lename	Profile (Clone Profi	le Delete	Prof
Routing Profiles			С	lick here to add a descriptio)n.						
default	Routing Profile										
ASM_7											
Belgacom									Ad	ld Routing R	tule
	Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	lgnore Route Header	Outgoing Transport	
	1 *		10.10.10.10		~			V		UDP	ø

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 27 of 40 BELGACOMASBCAE

7.2.5. Server Configuration– Avaya Aura® Session Manager

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 \rightarrow Server Configuration and click on Add Profile. Enter Profile Name to ASM_CallServer. On the Add Server Configuration Profile tab, set the following:

- Select Server Type to be Call Server
- Enter IP Addresses / Supported FQDNs to 10.10.7.61 (Session Manager IP Address)
- For Supported Transports, check UDP and TCP
- TCP Port:5060
- UDP Port: 5060
- Click on **Next** (not shown) to use deault entries on the **Authentication** and **Heartbeat** tabs.

Edit Server Co	onfiguration Profile - General	
Server Type	Call Server	
IP Addresses / Supported FQDNs Comma seperated list	10.10.7.61	
Supported Transports	UDP	
TCP Port	5060	
UDP Port	5060	
TLS Port		

On the Advanced tab

- Select ToASM for Interworking Profile
- Click Finish

Edit Server C	configuration Profile - Advanced 🛛 🔀
Enable DoS Protection	
Enable Grooming	
Interworking Profile	ToASM
Signaling Manipulation Script	None
TCP Connection Type	€ SUBID C PORTID C MAPPING
UDP Connection Type	• SUBID O PORTID O MAPPING
	Finish

7.2.6. Server Configuration- Belgacom side

The Server Configuration screen contains fourtabs: 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. Enter Name as Belgacom_TS. On the Add Server Configuration Profile tab, click on Edit and set the following:

- Select Server Type as Trunk Server
- Set IP Address to 10.10.10.10 (Belgacom Trunk Server)
- Supported Transports: Check UDP
- UDP Port: 5060
- Hit Next
- Click on Next (not shown) to use deault entries on the Authentication and Heartbeat tabs.

Edit Server Cont	figuration Profile - General 🛛 🔀
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	10.10.10
Supported Transports	TCP UDP TLS
TCP Port	5060
UDP Port	5060
TLS Port	
	Finish

On the Advanced tab

- Select ToBelgacom for Interworking Profile
- Click Finish

Edit Server Configuration Profile - Advanced					
Enable DoS Protection					
Enable Grooming					
Interworking Profile	ToBelgacom 💌				
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** \rightarrow **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.

Add Profile			Ren	ame Profile Clone Profile Delete Profile
Topology Hiding Profiles		Click here t	o add a description.	
default	Topology Hiding			
cisco_th_profile				
ASM	Header	Criteria	Replace Action	Overwrite Value
Belgacom	То	IP/Domain	Next Hop	
	From	IP/Domain	Auto	
	SDP	IP/Domain	Auto	
	Record-Route	IP/Domain	Auto	
	Via	IP/Domain	Auto	
	Request-Line	IP/Domain	Next Hop	
			Edit	

7.2.8. Topology Hiding – Belgacom 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** \rightarrow **Topology Hiding**.

- Click default profile and select Clone Profile
- Enter Profile Name: Belgacom
- For the Header From, To and Request-Line select IP/Domain under Criteria, Overwrite under Replace Action and imsu.belgacom.be under Overwrite Value
- Click Finish

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

Add Profile			Ren	ame Profile Clone Profile Delete Prof
Topology Hiding Profiles		Click here to	add a description.	
default	Topology Hiding			
cisco_th_profile				
ASM	Header	Criteria	Replace Action	Overwrite Value
Belgacom	То	IP/Domain	Overwrite	imsu.belgacom.be
	From	IP/Domain	Overwrite	imsu.belgacom.be
	SDP	IP/Domain	Auto	
	Record-Route	IP/Domain	Auto	
	Via	IP/Domain	Auto	
	Request-Line	IP/Domain	Overwrite	imsu.belgacom.be
		I	Edit	

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 32 of 40 BELGACOMASBCAE

7.3. Device Specific Settings

7.3.1. Network Management

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 \rightarrow 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 Manage	ement: GSSCP_07					
UC-Sec Devices	Network Configuration Interface Configu	Iration				
GSSCP_07						
	Modifications or deletions of an IP ad restarts can be issued from <u>System</u>	dress or its associated data require an ap <u>Management</u> .	pplication restart before t	taking effect. Appli	cation	
	A1 Netmask 255.255.255.0		B1 Netmask 55.255.128	B2 Netr	nask	
	Add IP	Changes will not take effect until t	he interface is updated.	Save Changes	Clear Chang	ges
	IP Address	Public IP Gate		ay	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
В1	Enabled	Toggle State
82	Disabled	Toggle State

7.3.2. Media Interfaces

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** \rightarrow Media Interface.

- Select Add Media Interface
- Name: ASM7
- Media IP: 10.10.7.180 (Internal Address for calls toward Session Manager)
- Port Range: 10000-10019
- Click Finish
- Select Add Media Interface
- Name: Belgacom
- Media IP: 10.10.10.20 (External Address for calls toward Belgacom trunk)
- Port Range: 10000-10019
- Click Finish
- Select Add Media Interface

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

UC-Sec Devices	Media Interface			
GSSCP_07				
	Modifying or deleting an existing media interface System Management.	e will require an application restart before tak	ing effect. Application restarts can be issued fr	om
			Add Media	Interface
	Name	Media IP	Port Range	
	ASM7	10.10.7.180	10000 - 10019	0 X
	Belgacom	10.10.10.20	10000 - 10019	🥒 🖉 🗙

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** \rightarrow **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 Signaling Interface
- Name: Belgacom
- Media IP: 10.10.10.20 (External Address for calls toward Belgacom)
- TCP Port: 5060
- UDP Port: 5060
- Click Finish

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

UC-Sec Devices	s	ignaling Interface								
GSSCP_07										
	Add Signali								ace	4
	Name		Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile			
		ASM7	10.10.7.180	5060	5060		None	ø	×	
		Belgacom	10.10.7.20	5060	5060		None	ø	×	
									-	-

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 \rightarrow Endpoint Flows.

• Select the Server Flows tab

To add the settings for Fixed call flow to Session Manager click on Add Flow.

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

To add the settings for Fixed call flow to Belgacom select Add Flow.

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

UC-Sec Devices	Subscribe	F Flows Server Flow	s												
GSSCP_07													Ado	i Flov	
		Click here to add a row description.													
	Server C	onfiguration: ASM_CallS	erver												
	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	Callserver	*	*	*	Belgacom	ASM7	ASM7	default-low	Belgacom	ASM	None	ø	×	Þ
	Server C	onfiguration: Belgacom_	TS												
	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	Trunkserver	*	*	*	ASM7	Belgacom	Belgacom	default-low	ASM_7	Belgacom	None	ø	×	Þ

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

8. Belgacom Configuration

The configuration required by Belgacom 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 Belgacom 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.

Summ	nary View						
1 Item F	Refresh						Filter: Er
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Statu:
►Show	ASMdot7	10.10.7.52	5060	TCP	Up	200 OK	Up

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

	Summ	nary View						
1	. Item F	Refresh						Filter: Enable
D	etails	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
	Show	ASMdot7	10.10.7.180	5060	ТСР	Up	420 Bad Extension	Up

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

```
status trunk 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 Belgacom SIP Trunk Service. The testing was successfully performed with Belgacom, 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.

- Installing and Configuring Avaya Aura® System Platform, Release 6.03, February [1]2011.
- Administering Avaya Aura® System Platform, Release 6.03, February 2011. [2]
- Administering Avaya Aura® Communication Manager, August 2010, Document [3] Number 03-300509.
- Avaya Aura® Communication Manager Feature Description and Implementation, May [4] 2009, Document Number 555-245-205.
- Upgrading Avaya Aura® System Manager to Release 6.2, March 2012. [5]
- Implementing Avaya Aura® Session Manager, February 2012, Document Number 03-[6] 603473
- Administering Avaya Aura® Session Manager, February 2012, Document Number 03-[7] 603324.

[8] RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/.

SJW; Reviewed:	Solution & Interoperability Test Lab Application Notes	39 of 40
SPOC 4/25/2012	©2012 Avaya Inc. All Rights Reserved.	BELGACOMASBCAE

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM 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 <u>devconnect@avaya.com</u>.