



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.1 and Avaya Aura® Session Border Controller to support Belgacom SIP Trunks Service for IP-PBX - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) Trunks between the Belgacom SIP Trunks service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Belgacom is a member of the Avaya DevConnect program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) Trunks between Belgacom SIP Trunks service for IP-PBX and an Avaya Aura® SIP enabled Enterprise Solution. The Avaya Aura® solution consists of Avaya Aura® Session Border Controller (AASBC), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya Aura® SIP enabled enterprise solution with Belgacom SIP Trunks service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the Enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya Aura® SIP telephony solution consisting of Communication Manager, Session Manager and AASBC. The enterprise site was configured to use the SIP Trunk Service provided by Belgacom.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DDI numbers assigned by Belgacom. Incoming PSTN calls were made to SIP, H.323 and Digital telephones at the enterprise
- Outgoing calls from the enterprise site were completed via Belgacom to PSTN destinations
- Outgoing calls from the enterprise to the PSTN were made from SIP, H.323, Digital and Analogue telephones
- Calls using G.729, G.726 and G.711A codec's
- T38 Fax is not supported by Belgacom SIP Trunks Service. DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by Belgacom requiring Avaya response and sent by Avaya requiring Belgacom response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Belgacom SIP Trunks service with the following observations:

- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested
- No Emergency services numbers were tested as test calls to these numbers should be pre-arranged with the Operator
- G.711mu is not offered by Belgacom SIP Trunks service and thus incoming calls were not tested
- Network Call Redirect (NCR) was tested but was found to cause interference with features Call Hold, Transfer and Conference. Belgacom support forwarded calls with sip 302_MOVED_TEMP response, but only for PBX's working in UNI mode (registration based). PBX's working in NNI mode (non-registration based), are not supported. For this reason NCR feature was switched off

Note: T.38 fax is not supported by Belgacom SIP Trunks service. For the purpose of these tests G711 Pass-Through was successfully tested.

Avaya only supports T38 fax. G.711 pass through is sensitive to high voice compression, network packet loss, jitter and clock synchronization, as a result some fax tonal signals may not get correctly transported across the packet network.

2.3. Support

For technical support on Belgacom products please visit the website at www.Belgacom.be or contact an authorized Belgacom representative.

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 an AASBC, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya digital telephones, Avaya analogue telephones, analogue fax machine and an PC based Avaya one-X Communicator soft phone (running H.323).



Figure 1: Test Setup Belgacom SIP Trunks to Avaya Enterprise

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 R6.0.1 (R016x.00.1.510.1) Service Pack 19009 (System Platform 6.0.3.1.3)
Avaya G450 Media Gateway	FW 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 (6.1.0.0.610023)
Avaya S8800 Server	Avaya Aura® System Manager R6.1 (System Platform 6.0.3.1.3, Template 6.1.5.0)
Avaya S8800 Server	Avaya Aura® Session Border Controller R6.1 (System Platform 6.0.3.0.3, Template E362P4)
Avaya 4621 Phone (H.323)	2.901
Avaya 9670 Phone (H.323)	2.0
Avaya 9601 Phone (SIP)	1.0.11.3
Avaya one-X® Communicator (H.323)	Avaya one-X® Communicator 6.0.1.16-SP1-25226
Analogue Phone	N/A
Belgacom Solution	
IMS Solution	IMS 7.6
ISC	Release 6.2.1
MGC Alcatel-Lucent MGC12	SP version: 105_0843D14; CLS version: 105_0843D14.8.21
MGW Alcatel-Lucent MGW-7510	SW version: A7510_R30_B19b
Application Server	Broadworks Release 16 sp1
Acme Packet Model: Net-Net 9200	SW version: SD7.0.0 MR-9 Patch 5 (Build 798)

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunks. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signaling associated with the Belgacom SIP Trunks Service. For incoming calls, the Session Manager receives SIP messages from the Session Border Controller and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the AASBC at the enterprise site; the AASBC then sends the 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		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	3
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	0
Maximum Administered SIP Trunks:		24000	10
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		128	0
Maximum Media Gateway VAL Sources:		250	1
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	0
Maximum Number of Expanded Meet-me Conference Ports:		300	0

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? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunks? y	
IP Trunks? y		
IP Attendant Consoles? y		

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.7.61** are the **Name** and **IP Address** for the Session Manager SIP routing interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signaling interface to Session Manager.

display node-names ip		IP NODE NAMES
Name	IP Address	
SM100	10.10.7.61	
default	0.0.0.0	
procr	10.10.7.52	
procr6	::	

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 enabled (**yes**) to allow audio traffic to be sent directly between end points without using gateway VoIP resources. When a PSTN call is shuffled the enterprise end point will talk directly to the public interface of the Belgacom Session Border Controller.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.

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


Open the **IP Codec Set** form for the codec set specified in the **IP Network Region** form as per **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**, **G.726A-32K** and **G.729A**. During compliance testing, other codec set configurations were also verified.

change ip-codec-set 1 Page 1 of 2

IP Codec Set

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20
2: G.726A-32K	n	2	20
3: G.729A	n	2	20

Belgacom SIP Trunks Service does not support the T.38 fax protocol. Fax pass-through was tested using G.711. Navigate to **Page 2** to configure fax pass-through by setting the **Fax Mode** to **pass-through** as shown below.

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

Note: T.38 fax is not supported by Belgacom SIP Trunks service. For the purpose of these tests G711 Pass-Through was successfully tested.

Avaya only supports T38 fax. G.711 pass through is sensitive to high voice compression, network packet loss, jitter and clock synchronization, as a result some fax tonal signals may not get correctly transported across the packet network.

5.5. Administer SIP Signaling Groups

This signaling group (and trunk group) will be used for inbound and outbound PSTN calls to Belgacom SIP Trunks Service. During test, this was configured to use TLS and port 5061, to facilitate tracing and fault analysis TCP on port 5060 can be used. 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 x** command as follows:

- Set the **Group Type** field to **sip**
- The **Transport Method** field is set to **tls**
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- 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 **SM100**), also shown in **Section 5.2**
- Ensure that the recommended TLS port value of **5061** 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**
- Leave the **Far-end Domain** field blank, this removes the analysis of the far end domain name and subsequent handling of multiple signaling groups where it is not required
- 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		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM100	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP 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 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
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **tie**
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: to SM100	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? y		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 30	

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Belgacom to prevent unnecessary SIP messages during call setup. Also note that the value for **Redirect On OPTIM Failure** can be increased to allow additional set-up time for calls destined for an EC500 destination.

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): 600	

On **Page 3**, set the **Numbering Format** field to **public**.

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

On **Page 4**, set the **Convert 180 to 183 for Early Media** to **n**. If the 183 Session Progress message is received by Belgacom SIP Trunks, ring tone is expected by the terminating equipment. The Avaya G430 Media Gateway does not play ring tone, so none is heard by the caller. The default value for **Network Call Redirection** is **n**, but the setting is changed on the test system to facilitate testing of User-to-User Information (UUI).

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

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the sample configuration, individual stations are mapped to send numbers allocated from the Belgacom DDI range supplied. This calling party number will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. The DDI numbers below have been changed.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	1305	1	3251712371	10	Total Administered: 5
4	1306	1	3251712372	10	Total Administered: 10
4	1601	1	3251712373	10	Maximum Entries: 9999
4	1602	1	3251712374	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
4	1604	1	3251712375	10	
4	1650	1	3251712376	10	
4	1652	1	3251712377	10	
4	1670	1	3251712378	10	
4	1671	1	3251712379	10	
4	1672	1	3251712380	10	

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to Belgacom SIP Trunks 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**.

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns is 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**.

Use the **change route-pattern x** 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**.

15 of 43
BelgacomCMSBC01

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Belgacom can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DDI numbers provided by Belgacom correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DDI numbers 01712371 - 01712380 to a 4 digit extension by deleting all of the incoming digits and inserting an extension. The DDI numbers below have been changed.

change inc-call-handling-trmt trunk-group 1					Page	1 of	30
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del Insert				
tie	11	+3251712371	all	1305			
tie	11	+3251712372	all	1306			
tie	11	+3251712373	all	1601			
tie	11	+3251712374	all	1602			
tie	11	+3251712375	all	1650			
tie	11	+3251712376	all	1604			
tie	11	+3251712377	all	1652			
tie	11	+3251712378	all	1670			
tie	11	+3251712379	all	1671			
tie	11	+3251712380	all	1672			

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example **EC500** configuration for the user with **station extension 1305**. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- 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. **01712378**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**
- Other parameters can retain default value

change off-pbx-telephone station-mapping 1305							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
1305	EC500	-		01712371	1	1	
		-					

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

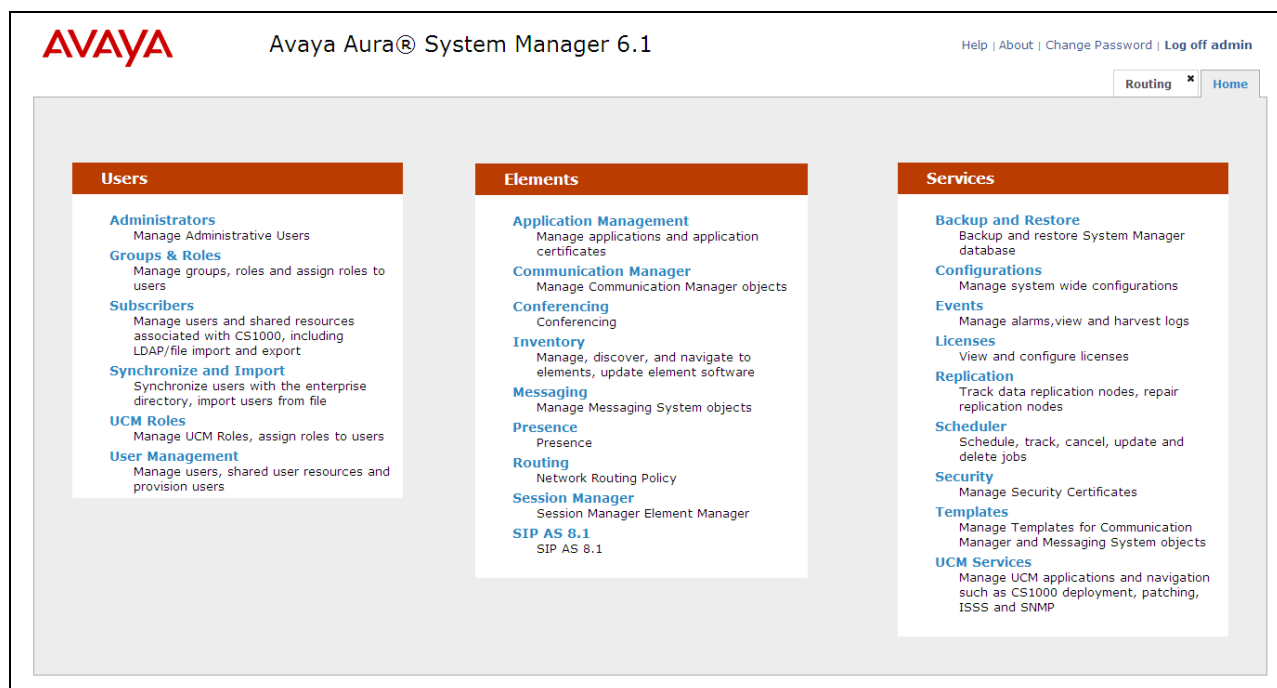
6. Configuring Avaya Aura® Session Manager

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

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

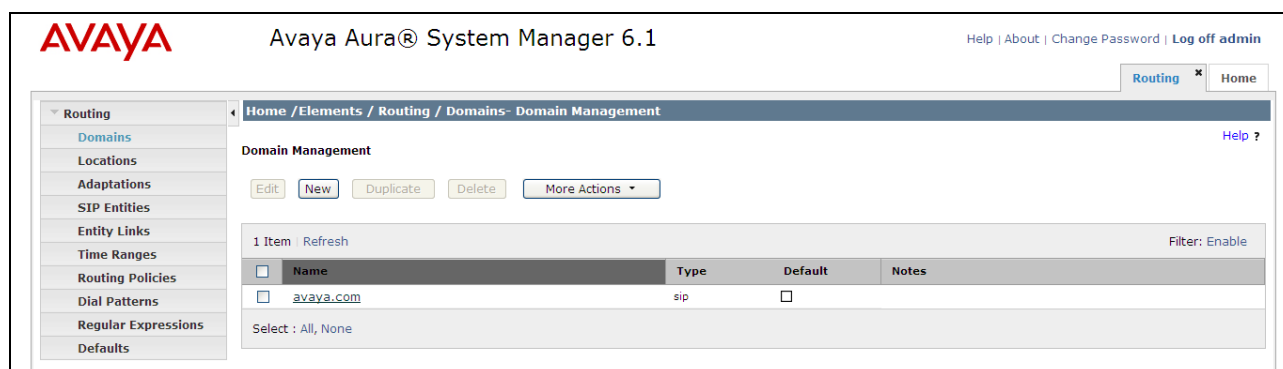
6.1. Log in to Avaya Aura® System Manager

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



6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu 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**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.



6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the simulated enterprise.

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

[Routing](#) * [Home](#)

Home / Elements / Routing / Locations- Location Details

Location Details [Help ?](#) [Commit](#) [Cancel](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

Location Pattern

[Add](#) [Remove](#)

2 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*10.10.8.*	<input type="text"/>
<input type="checkbox"/>	*10.10.7.*	<input type="text"/>

6.4. Administer SIP Entities

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

Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the AASBC 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:

- Avaya Aura® Session Manager SIP Entity
- Avaya Aura® Communication Manager SIP Entity
- Avaya Aura® Session Border Controller SIP Entity

6.4.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signaling interface.

The screenshot displays the Avaya Aura® System Manager 6.1 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and shows the 'General' tab. The 'Name' field is set to 'ASM61', 'FQDN or IP Address' is '10.10.7.61', and 'Type' is 'Session Manager'. The 'Location' is set to 'SPLab7' and 'Time Zone' is 'Etc/GMT'. The 'SIP Link Monitoring' section shows 'Use Session Manager Configuration' selected. At the bottom, the 'Entity Links' table shows a link between 'ASM61' and 'AASBC' on port 5060.

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
ASM61	TCP	* 5060	AASBC	* 5060	<input checked="" type="checkbox"/>

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	Protocol	Default Domain	Notes
5060	UDP	avaya.com	
5060	TCP	avaya.com	
5061	TLS	avaya.com	

6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screens show the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signaling.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

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

SIP Entity Details

General

* Name: CMEVO

* FQDN or IP Address: 10.10.7.52

Type: CM

Notes:

Adaptation:

Location: SPLab7

Time Zone: Etc/GMT

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

6.4.3. Avaya Aura® Session Border Controller SIP Entity

The following screen shows the SIP Entity for the AASBC. The **FQDN or IP Address** field is set to the IP address of the AASBC private network interface (see **Figure 1**).

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". A breadcrumb trail shows "Home / Elements / Routing / SIP Entities- SIP Entity Details". The left sidebar contains a menu with "Routing" selected, and sub-items: "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The main content area is titled "SIP Entity Details" and has a "General" tab selected. It includes a "Help ?" link, "Commit", and "Cancel" buttons. The form fields are as follows:

- Name:** AASBC
- FQDN or IP Address:** 10.10.7.67
- Type:** Gateway
- Notes:** (empty text field)
- Adaptation:** (empty dropdown menu)
- Location:** SPLab7
- Time Zone:** Etc/GMT
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

At the bottom, there is an "Entity Links" section with "Add" and "Remove" buttons.

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

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **Session Manager 1**
- 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** to save changes. The following screen shows the Entity Links used in this configuration.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with two items. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. Both links are marked as trusted.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	CM Link	Session Manager 1	TCP	5060	Communication Manager	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SBC Link	Session Manager 1	TCP	5060	SBC	5060	<input checked="" type="checkbox"/>	

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
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains the following sections:

- General:** The 'Name' field is set to 'TO CMEVO'. The 'Disabled' checkbox is unchecked. The 'Notes' field is empty.
- SIP Entity as Destination:** A 'Select' button is present. Below it, a table lists the selected SIP entity:

Name	FQDN or IP Address	Type	Notes
CMEVO	10.10.7.52	CM	

- Time of Day:** Includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below is a table with one item:

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Below the table, it says 'Select : All, None'.

- Dial Patterns:** Includes 'Add' and 'Remove' buttons.

The following screen shows the routing policy for the AASBC.

AVAYA

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing

Home

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

CommitCancelHelp ?

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

General

* Name: toAASBC

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AASBC	10.10.7.67	Gateway	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

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 **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.6**. Click **Select** button to save. The following screen shows an example dial pattern configured for AASBC which will route the calls out to the Belgacom SIP Trunks Service.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

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

Dial Pattern Details

General

* Pattern: 00353

* Min: 10

* Max: 16

Emergency Call: ☐

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"/>	SPLab7	toAASBC	0	<input type="checkbox"/>	AASBC		

Select : All, None

Denied Originating Locations

Add Remove

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

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing Home

Routing

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

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

Dial Pattern Details Help ? Commit Cancel

General

* Pattern: 44203551

* Min: 10

* Max: 12

Emergency Call: ☐

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"/>	-ALL-	Any Locations	TO CMEVO	0	<input type="checkbox"/>	CMEVO	

Select : All, None

Denied Originating Locations

Add Remove

6.8. Administer Application for Avaya Aura® Communication Manager

From the home tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New**.

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager

Select **Commit** to save the configuration.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

Home / Elements / Session Manager / Application Configuration / Applications- Applications

Help ?

Application Editor

Commit Cancel

Application

*Name

*SIP Entity

*CM System for SIP Entity Refresh [View/Add CM Systems](#)

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

*Required

Commit Cancel

6.9. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration → Applications Sequences** and click on **New**.

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

Select **Commit**.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager, Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, Applications, Application Sequences, Implicit Users, NRS Proxy Users, System Status, and System Tools. The main content area is titled 'Application Sequence Editor' and includes a breadcrumb trail: 'Home / Elements / Session Manager / Application Configuration / Application Sequences- Application Sequences'. Below the breadcrumb, there are 'Commit' and 'Cancel' buttons. The 'Application Sequence' section contains a form with 'Name' (set to 'app_seq') and 'Description' fields. The 'Applications in this Sequence' section shows a table with one item: 'application' (SIP Entity: CMEVO, Mandatory: checked). The 'Available Applications' section shows a table with one item: 'application' (SIP Entity: CMEVO). Red boxes highlight the 'Name' and 'Description' fields, the 'application' row in the 'Applications in this Sequence' table, and the 'application' row in the 'Available Applications' table.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Session Manager Home

Home / Elements / Session Manager / Application Configuration / Application Sequences- Application Sequences

Help ?

Application Sequence Editor

Commit Cancel

Application Sequence

*Name

Description

Applications in this Sequence

Move First Move Last Remove

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	1	application	CMEVO	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item Refresh Filter: Enable

Name	SIP Entity	Description
application	CMEVO	

6.10. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain (e.g. **2296@avaya.com**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

User Management Manage Users Public Contacts Shared Addresses System Presence ACLs

Home / Users / User Management / Manage Users - New User Profile

Help ?

Commit Cancel

Identity * Communication Profile * Membership Contacts

Identity

* Last Name: Sip

* First Name: 9630

Middle Name:

Description:

* Login Name: 1305@avaya.com

* Authentication Type: Basic

* Password:

* Confirm Password:

Localized Display Name:

On the **Communication Profile** tab enter a numeric **Communication Profile Password** and confirm it, then click on the show/hide button for **Communication Address** and click **New**. For the **Type** field select **sip** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

User Management * Home

User Management Manage Users Public Contacts Shared Addresses System Presence ACLs

Home /Users / User Management / Manage Users- User Profile Edit

User Profile Edit: 1305@avaya.com

Commit Cancel

Identity * Communication Profile * Membership Contacts

Communication Profile *

Communication Profile Password: *****

Confirm Password: ***** Cancel

New Delete Done Cancel

Name

Primary

Select: None

* Name: Primary

Default: ☒

Communication Address *

New Edit Delete

Type	Handle	Domain
<input checked="" type="checkbox"/> Avaya SIP	1305	avaya.com

Select: All, None

Type: Avaya SIP

* Fully Qualified Address: 1305 @ avaya.com

Add Cancel

Click the Session Manager Profile to expand the **Session Manager Profile** menu:

- Make sure the **Session Manager** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.9**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.9**
- Select the appropriate location from the drop-down menu in the **Home Location** field

☒ Session Manager Profile

* Primary Session Manager

ASM61

Secondary Session Manager

(None)

Origination Application Sequence

app_seq

Termination Application Sequence

app_seq

Survivability Server

(None)

* Home Location

SPLab7

Primary	Secondary	Maximum
6	0	6

Primary	Secondary	Maximum

Click the Endpoint Profile to expand the **Endpoint Profile** menu:

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** to save changes and the System Manager will add the Communication Manager user configuration automatically

The screenshot shows the 'Endpoint Profile' configuration form. Red boxes highlight the following fields:

- System**: CMEVO
- Profile Type**: Endpoint
- Extension**: 1305
- Template**: Select/Reset
- Port**: S00011
- Delete Endpoint on Unassign of Endpoint from User or on Delete User**: ☒

Other visible fields include:

- Use Existing Endpoints**: ☐
- Set Type**: 9630SIP
- Security Code**: •••••
- Voice Mail Number**: (empty field)
- Endpoint Editor**: (button)

7. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the AASBC. The configuration is done using the AASBC web interface.

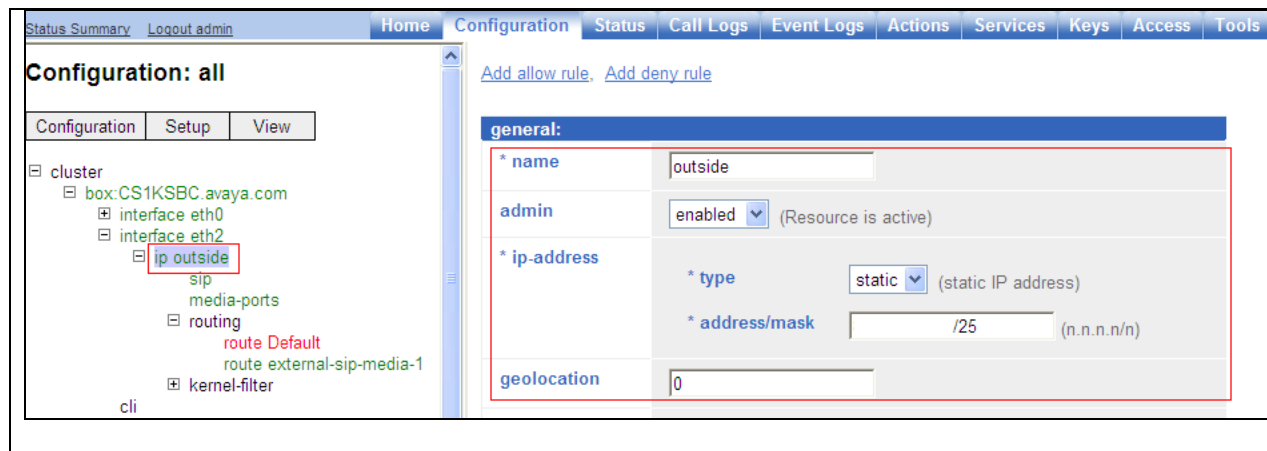
7.1. Access Avaya Aura® Session Border Controller

Access the AASBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. Log in with the appropriate credentials.



7.2. Verify Outside Interface was configured at installation

An IP address was given to the outside interface that is on the public internet. The ip address is blanked out in the screenshot below for security purposes. Click on the **Configuration** tab and browse to **cluster** → **interface eth2** → **ip outside**.



7.2.1. Configure SIP Port

For the outside interface a transport protocol needs to be configured. In the compliance testing we used UDP for the SIP messaging. Click on the **Configuration** tab and browse to **cluster** → **interface eth2** → **ip outside** → **sip**.

- **Port** Port number to be used for SIP messaging, default is **5060**

Configuration: all

Configuration Setup View

cluster

- box:cs1ksbc.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip

media-ports

Create cluster\box 1\interface eth2\ip outside\sip\udp-port 5060 - Step 1 of 1: Edit

Please provide some basic information for udp-port 5060. Then press "Create".

* port 5060 (at minimum 1,default=5060)

Create Reset Cancel

The newly created UDP port is shown below.

Configuration: all

Configuration Setup View

cluster

- box:CS1KSBC.avaya.com
 - interface eth0
 - interface eth2
 - ip outside
 - sip

media-ports

routing

- route Default
- route external-sip-media-1

kernel-filter

cli

vsp

- default-session-config
- tls
- session-config-pool

Configure cluster\box:CS1KSBC.avaya.com\interface eth2\ip outside\sip [Help](#) [Index](#)

Set Reset Back Delete

admin enabled (Resource is active)

nat-translation disabled (Resource is inactive)

nat-add-received-from disabled (Resource is inactive)

nat-add-X-Remote-Info enabled (Resource is active)

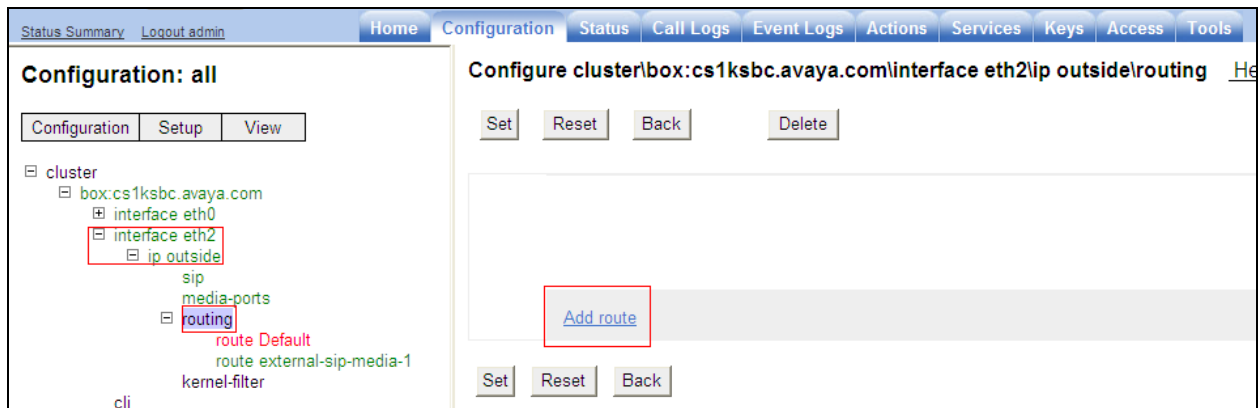
load-balance-head-end false

udp-port

	udp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	udp-port 5060	Edit	Edit	any	0	Edit

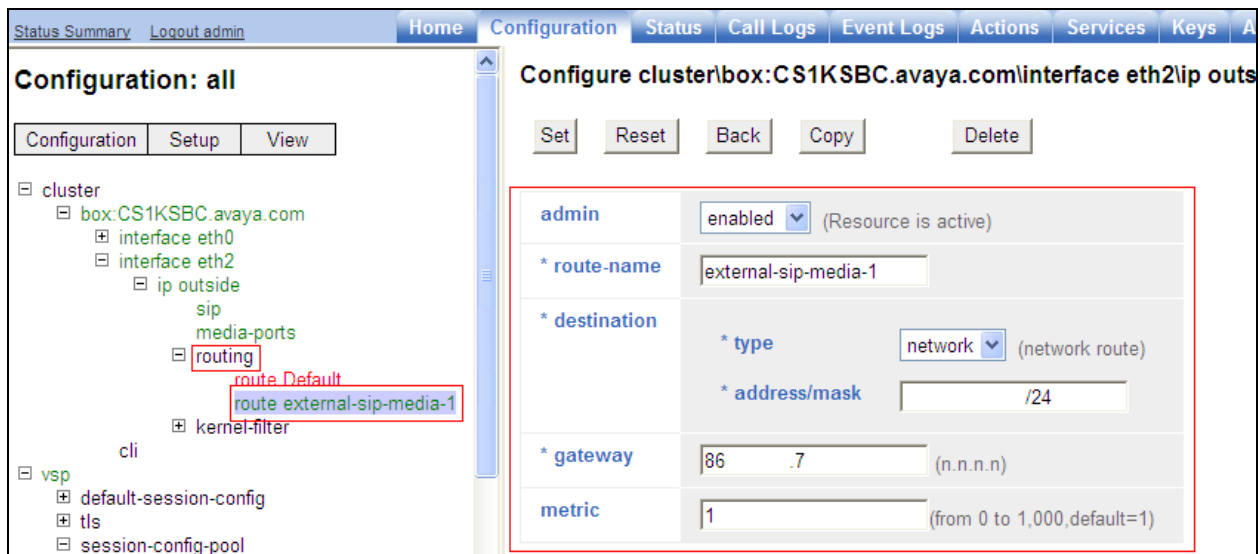
7.2.2. Configure Routing

For the outside interface routing needs to be configured to advise the SIP traffic how to route out to Belgacom network from the outside interface of the AASBC. The ip address is blanked out in the screenshot below for security purposes. Click on the **Configuration** tab and browse to **cluster** → **interface eth2** → **ip outside** → **routing** → **add route**.



The following values need to be added for the new route that is being created:

- **admin** Enables or disables this route configuration
- **route name** Enter a name for the route
- **destination type** Use network as the network route
- **destination address/mask** The destination address is the subnet used by the service provider and mask
- **gateway** Sets the gateway or next hop IP address for the packet
- **metric** Associates a cost for the route, default is 1



7.3. Configuring VSP

7.3.1. Configure Session-Config-Pool Entry ToTelco

In the **to-uri-specification** a valid host was added for Belgacom. Expand **vsp** → **session-config pool** → **entry ToTelco** → **to-uri-specification**. For our testing we used **imsu.belgacom.be** as shown below.

Notes: Please note the domain name used by Belgacom may change depending on access method, please consult Belgacom to confirm what this will be.

Configuration: all

Configuration Setup View

cluster

box: SBC7GSSCP.avaya.com

vsp

default-session-config

tls

session-config-pool

entry ToTelco

to-uri-specification

from-uri-specification

request-uri-specification

p-asserted-identity-uri-specification

entry ToPBX

Configure vspsession-config-poolentry ToTelco to-uri-specification Help Index

Set Reset Back Delete

user enter to-uri or select from to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

host enter imsu.belgacom.be or select from imsu.belgacom.be

port enter to-uri or select from to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

display enter to-uri or select from to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

transport to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

In the **from-uri-specification** a valid host was added for Belgacom. Expand **vsp** → **session-config pool** → **entry ToTelco** → **to-from-specification**. For our testing we used **imsu.belgacom.be** as seen below.

Configuration: all

Configuration Setup View

cluster

box: SBC7GSSCP.avaya.com

vsp

default-session-config

tls

session-config-pool

entry ToTelco

to-uri-specification

from-uri-specification

request-uri-specification

p-asserted-identity-uri-specification

entry ToPBX

entry Discard

dial-plan

Configure vspsession-config-poolentry ToTelco from-uri-specification Help Index

Set Reset Back Delete

user enter from-uri or select from from-uri (Net-Net OS-E uses the value from the incoming FROM URI.)

host enter imsu.belgacom.be or select from imsu.belgacom.be

port enter from-uri or select from from-uri (Net-Net OS-E uses the value from the incoming FROM URI.)

display enter from-uri or select from from-uri (Net-Net OS-E uses the value from the incoming FROM URI.)

Repeat the same process to the change the host value in the request **imsu.belgacom.be**, this is not shown.

7.3.2. Configure Session-Config-Pool Entry ToPBX

In the **to-uri-specification** a new host was added **avaya.com**, this is the SIP domain used in the enterprise and is configured in **Section 6.1**. Expand **vsp** → **session-config pool** → **entry ToPBX** → **to-uri-specification**.

The screenshot shows the Avaya configuration interface. On the left, a tree view shows the configuration hierarchy: **cluster** → **box:CS1KSBC.avaya.com** → **vsp** → **default-session-config** → **tls** → **session-config-pool** → **entry ToPBX** → **to-uri-specification**. The main panel is titled "Configure vsp|session-config-pool|entry ToPBX|to-uri-specification". It contains a table with the following fields:

Field	Value	Notes
user	enter to-uri or select from to-uri (Net-Net OS-)	
host	enter avaya.com or select from avaya.com	
port	enter to-uri or select from to-uri (Net-Net OS-E uses t)	
display	enter to-uri or select from to-uri (Net-Net OS-E uses t)	
transport	to-uri (Net-Net OS-E uses the value from the incoming TO URI.)	
user-param	omit	
user-truncate-non-digits	disabled (Resource is inactive)	

In the **request-uri-specification** a new host was added **avaya.com**, this is the SIP domain used in the enterprise and is configured in **Section 6.1**. Expand **vsp** → **session-config pool** → **entry ToPBX** → **request-uri-specification**.

The screenshot shows the Avaya configuration interface. On the left, a tree view shows the configuration hierarchy: **cluster** → **box:CS1KSBC.avaya.com** → **vsp** → **default-session-config** → **tls** → **session-config-pool** → **entry ToPBX** → **request-uri-specification**. The main panel is titled "Configure vsp|session-config-pool|entry ToPBX|request-uri-specification". It contains a table with the following fields:

Field	Value	Notes
user	enter request-uri or select from request-uri (Net-Net OS-E t REQUEST URI.)	
host	enter avaya.com or select from avaya.com	
port	enter request-uri or select from request-uri (Net-Net OS-E uses the URI.)	
transport	request-uri (Net-Net OS-E uses the value from the incoming REQUEST URI.)	
user-param	omit	
user-truncate-non-digits	disabled (Resource is inactive)	

7.3.3. Configuring Enterprise

In the **sip-gateway-Telco** the domain name used is **avaya.com**. A newly added server was created for **Belgacom's SBC**; information needed here is the ip address, port and transport protocol. Click on the **Configuration** tab and browse to **vsp → enterprise → servers → sip-gateway Telco → server-pool**. Click the **Add server** link. The IP address of the SBC has been changed.

The screenshot shows the Avaya Aura Configuration interface. The left pane displays the navigation tree with 'vsp' and 'enterprise' highlighted. The main pane shows the configuration for 'server Telco1' in the 'server-pool'. The configuration includes fields for 'name' (Telco), 'admin' (enabled), 'domain' (avaya.com), and 'failover-detection' (ping). A table lists the servers in the pool, with 'server Telco1' highlighted.

server	admin	host	transport	port	outbound-normalization	inbound-normalization	admission-control	emission-control	max-bandwidth
server Telco1	enabled	192.168.1.1	UDP	5060	Configure	Configure	disabled	disabled	unlimited

7.4. Save the Configuration

To save the configuration, click on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.

The screenshot shows the Configuration menu in the Avaya Aura Configuration interface. The menu is open, displaying various options. The 'Update and save configuration' option is highlighted, and a tooltip indicates that this action will 'Update and save the current configuration.'.

8. Service Provider Configuration

The configuration of the Belgacom equipment used to support the Belgacom SIP Trunks service is outside of the scope for these Application Notes and will not be covered. To obtain further information on Belgacom equipment and system configuration please contact an authorised Belgacom 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**.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. The main content area is titled 'SIP Entity, Entity Link Connection Status' and shows a table of entity links for 'AASBC'. The table has columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The 'Conn. Status' and 'Link Status' for the entry 'ASM61' are highlighted in red and show 'Up'.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	ASM61	10.10.7.67	5060	TCP	Up	200 OK	Up

From the 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	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

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

Note: It is possible to gain further information From the Communication Manager SAT interface by entering in the following commands **list trace station n** where **n** is a previously configured station number. **list trace tac n** where **n** is a previously configured tac (Trunk Access Code).

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to Belgacom SIP Trunks Service. Belgacom Explore Business Trunking solutions are oriented towards professional customers who want to integrate their voice and data traffics on a single data network. And, at the same time, be able through this network, to communicate with the traditional switched-voice network (PSTN/ISDN). The service was successfully tested with a number of observations listed in **Section 2.2**.

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 6.0.3, February 2011.
- [2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.0.1, April 2011.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, August 2010, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager Release 6.1*, November 2010.
- [6] *Installing and Configuring Avaya Aura® Session Manager*, April 2011, Document Number 03-603473
- [7] *Administering Avaya Aura® Session Manager*, May 2011, Document Number 03-603324.
- [8] *Avaya Aura® Session Border Controller System Administration*, September 2010
- [9] *Installing and Configuring Avaya Aura® Session Border Controller*, May 2011
- [8] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2011 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.