



# **Application Notes for Configuring Avaya Aura® Communication Manager R7.1, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to support NOS Comunicações SIP Trunking Service - Issue 1.0**

## **Abstract**

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

The NOS Comunicações SIP Trunk Platform provides PSTN access via a SIP trunk connected to the NOS Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

# 1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the NOS Comunicações (NOS) SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R7.1 (Communication Manager); Avaya Aura® Session Manager R7.1 (Session Manager); Avaya Session Border Controller for Enterprise R7.2 (Avaya SBCE). Note that the shortened names shown in brackets will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with the NOS SIP Trunking 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 and generally results in lower cost for the enterprise customer.

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to connect to the NOS SIP Trunking Service.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

## 2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the NOS SIP Trunking Service, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the NOS SIP Trunking Service to PSTN destinations, calls made from SIP and H.323 telephones.
- Incoming and Outgoing PSTN calls to/from Avaya one-X® Communicator and Avaya Equinox™ for Windows soft phones.
- Calls using the G.711A and G.729A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media between the Avaya SBCE and the SIP and H.323 telephones.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by the NOS SIP Trunking Service requiring Avaya response and sent by Avaya requiring NOS response.

## 2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the NOS SIP Trunking Service with the following observations:

- The network responded to OPTIONS sent from Session Manager with “502 Bad DNS Request”. Session Manager accepted this as a valid indication that the SIP Trunk was functional and there was no effect on traffic. NOS did not use OPTIONS to check the status of the SIP Trunk. Instead ICMP PING messages were sent from the network to the Avaya SBCE.
- It was observed during testing that when the Media Server is used, two ringback tones are heard on the calling phone. The NOS network sends 183 Session Progress followed by 180 Ringing when setting up calls. Communication Manager is playing ringback when it receives the 180 Ringing despite the fact that the network is playing ringback after establishing early media with the 183 Session Progress message. This issue is currently under investigation.
- Outbound calls to busy numbers received an announcement from the network “The number you have dialled cannot accept this call. Please hang up and try again later”. This is listed as an observation as it differs from the common handling of sending SIP “486 Busy Here”.
- Outbound calls to invalid numbers received an announcement from the network “The number you have dialled cannot accept this call. Please hang up and try again later”. This is listed as an observation as it differs from the common handling of sending SIP “404 Not Found”.

- DTMF payload type appeared as DynamicRTP-Type-96 as opposed to telephone-event (96). This is likely to be a Wireshark issue and did not affect successful transmission of DTMF.
- An issue was observed with transfer of outbound calls from one-X Communicator in “Other Phone” mode and connected via SIP as opposed to H.323. When transferring to an internal extension, there was no ringback heard on the one-X Communicator client.
- An issue was observed with conferencing of outbound calls from one-X Communicator in “Other Phone” mode and connected via SIP. When conferencing an internal extension, there was no ringback heard on the one-X Communicator client.
- When testing the “All Trunks Busy” condition, the call failed as expected and a failure tone was heard on the calling phone. This is listed as an issue because Communication Manager sent “422 Session Interval Too Small” as opposed to “486 Busy Here” despite the Session Refresh Interval being set to the correct value.

## 2.3. Support

For technical support on NOS SIP Trunking Services, contact NOS support at:

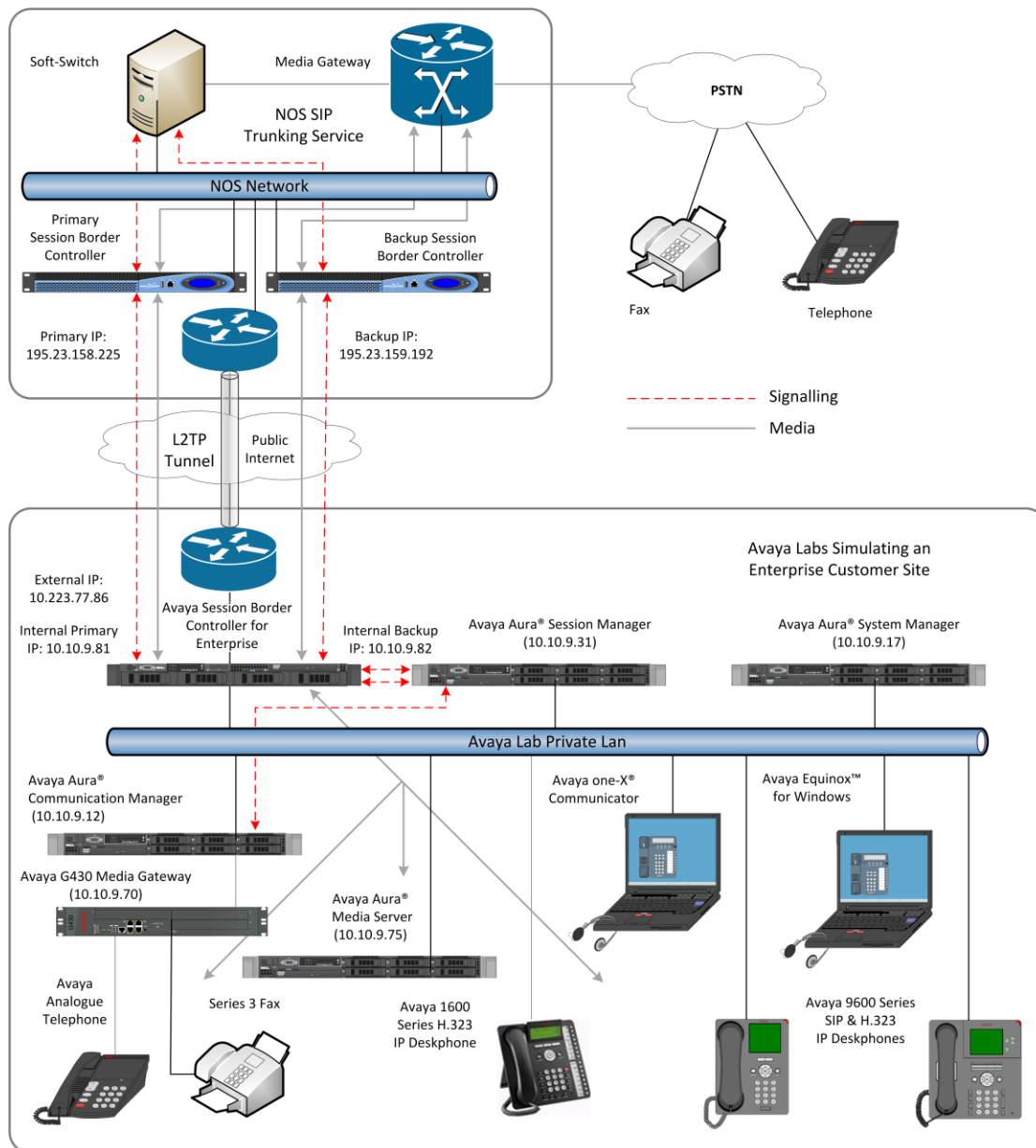
Web: <http://www.nos.pt/>

Email: [suporte.corporate@nos.pt](mailto:suporte.corporate@nos.pt)

Phone: 808101090

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to the NOS SIP Trunking Service. Located at the Enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Equinox™ for Windows running on laptop PCs.



### Figure 1: Test Setup NOS SIP Trunking Service to Avaya Enterprise

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya Aura® Session Manager	7.1.2.0.712004 – FP2
Avaya Aura® System Manager	7.1.2.0.057353 – FP2
Avaya Aura® Communication Manager	7.1.2.0.0 0-24184 – FP2
Avaya Session Border Controller for Enterprise	7.2.1.0-05-14222 – FP1
Avaya Aura® Media Server	7.8.0.355
Avaya G430 Media Gateway	38.21.0
Avaya 9600 series Handsets	
SIP 96x0	2.6.17
SIP 9608	7.1.1.0 r9
H.323 96x0	3.2.7B
H.323 9608	6.6.4.01
H.323 1616	1.3.10
Avaya one-X® Communicator	6.2.12.20 – SP12 Patch10
Avaya Equinox™ for Windows	3.3.1.60
Analogue Handset	N/A
Analogue Fax	N/A
<b>NOS</b>	
Acme Packet Net-Net 6300 SCZ7.3.0	MR-1 Patch 4 (Build 286)

## 5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the NOS SIP Trunking Service. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the NOS network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

### 5.1. Confirm System Features

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

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		4000	0
Maximum Concurrently Registered IP Stations:		2400	3
Maximum Administered Remote Office Trunks:		4000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		68	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		2400	0
Maximum Video Capable IP Softphones:		2400	0
<b>Maximum Administered SIP Trunks:</b>		<b>4000</b>	<b>22</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0

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

```
display system-parameters customer-options                                Page 5 of 12
                                OPTIONAL FEATURES

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

IP Attendant Consoles? y
```

## 5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **Session\_Manager** and **10.10.9.31** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** IP address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                IP NODE NAMES

Name          IP Address
AMS           10.10.9.75
Session_Manager  10.10.9.31
default       0.0.0.0
procr          10.10.9.12
procr6        ::
```



### 5.3. Administer IP Network Region

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

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

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

**Note:** In the test configuration, **ip-network-region 1** was used within the enterprise and **ip-network-region 2** was used for the SIP Trunk. To define a codec set for inter-region traffic, navigate to **Page 4**. In the test environment, **codec set 2** was used.

change ip-network-region 2										Page 4 of 20			
Source Region: 2		Inter Network Region Connection Management								I	M		
										G	A	t	
dst	codec	direct	WAN-BW-limits		Video	Intervening			Dyn	A	G	c	
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	e	
1	2	y	NoLimit							n	t		
2	2											all	

## 5.4. Administer IP Codec Set

Open the IP Codec Set form for the codec set specified in the IP Network Region form in **Section 5.3** by typing **change ip-codec set n** where **n** is the chosen value of the configuration for the SIP Trunk. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by NOS were configured, namely **G.711A**, **G.711MU** and **G.729A**. In addition to the codec's, the **Media Encryption** is defined here. A typical value would be **1-srtp-aescm128-hmac80**. In the test environment, a second-choice value of **none** was also used to provide an alternative in the case of issues with RTP to SRTP conversion.

```
change ip-codec-set 2 Page 1 of 2
```

IP MEDIA PARAMETERS

Codec Set: 2

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20
2: G.711MU	n	2	20
3: G.729A	n	2	20
4:			
5:			
6:			
7:			

**Media Encryption** **Encrypted SRTCP: enforce-unenc-srtcp**

1: 1-srtp-aescm128-hmac80

2: none

The NOS SIP Trunking Service supports T.38 for transmission of fax. Navigate to **Page 2** and define T.38 fax as follows:

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

```
change ip-codec-set 2 Page 2 of 2
```

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

FAX	Mode	Redundancy	ECM	Packet Size (ms)
Modem	t.38-standard	0	y	
TDD/TTY	off	0		
H.323 Clear-channel	US	3		
SIP 64K Data	n	0		
				20

**Note:** **Redundancy** can be used to send multiple copies of T.38 packets which can help the successful transmission of fax over networks where packets are being dropped. This was not experienced in the test environment and **Redundancy** was left at the default value of **0**.

## 5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the NOS SIP Trunking Service. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tls**.
- Set **Peer Detection Enabled** to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to Session Manager interface (node name **Session\_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required. The standard value for TLS is **5061**.
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3** (logically establishes the far-end for calls using this signalling group as region **2**).
- Leave **Far-end Domain** blank to allow Communication Manager to accept calls from any SIP domain on the associated trunk.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set both **H.323 Station Outgoing Direct Media** and **Initial IP-IP Direct Media** to **n** so that the call is set up via the media gateway / media server, then shuffled to direct media.

The default values for the other fields may be used.

<b>add signaling-group 2</b>		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr		Far-end Node Name: Session_Manager
Near-end Listen Port: 5061		Far-end Listen Port: 5061
		Far-end Network Region: 2
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? n		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 6

**Note:** The **Initial IP-IP Direct Media** field is shown as **n**. This allows the Media Gateway or Media Server to be present in the media transmission path during call set-up. This is appropriate for NOS where early media is supported.

## 5.6. Administer SIP Trunk Groups

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

- Set the **Group Type** field to **sip**.
- Choose a descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **public-ntwrk** if the Diversion header is to be supported.
- Specify the **Signaling Group** defined in **Section 5.5** to be associated with this Trunk Group.
- Specify the **Number of Members** supported by this SIP Trunk Group.

<b>add trunk-group 2</b>		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: PSTN	COR: 1	TN: 1	TAC: 102
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 2	
		Number of Members: 10	

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with NOS to prevent unnecessary SIP messages during call setup. During testing, a value of **300** was used that sets Min-SE to 600 in the SIP signalling.

<b>add trunk-group 2</b>		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): 300			
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of Calling Line Identity (CLI) in E.164 format with leading “+”.

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

**Note:** During testing, the **Hold/Unhold Notifications** field was left at the default value of **y** so that re-INVITE messages were sent when placing a call on hold and taking it off hold.

On **Page 4** of this form:

- Set **Send Diversion Header** to **y**.
- Set the **Telephone Event Payload Type** to **96** to match the value preferred by NOS (this Payload Type is not applied to calls from SIP end-points).
- Set the **Identity for Calling Party Display** to **From** so that the number displayed on the Communication Manager extension is taken from the user part of the From header and not the P-Asserted-Identity header.

add trunk-group 2		Page 4 of 21
PROTOCOL VARIATIONS		
	Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	Send Transferring Party Information? n	
	Network Call Redirection? n	
	<b>Send Diversion Header? y</b>	
	Support Request History? n	
	<b>Telephone Event Payload Type: 96</b>	
	Convert 180 to 183 for Early Media? n	
	Always Use re-INVITE for Display Updates? n	
	<b>Identity for Calling Party Display: From</b>	
Block Sending Calling Party Location in INVITE? n	Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? n	

**Note:** During testing, a **Telephone Event Payload Type** value of **101** was used successfully to check that media attributes were negotiated correctly.

## 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 E.164 format required. These calling party numbers are sent in the SIP From, Contact and PAI headers as well as the Diversion header for forwarded calls. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2	1		4	Total Administered: 7
4	2000	2	351212nnnn12	12	Maximum Entries: 240
4	2291	2	351218nnnn98	12	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	2316	2	351212nnnn27	12	
4	2391	2	351212nnnn79	12	
4	2400	2	351212nnnn22	12	
4	2401	2	351212nnnn22	12	
					Communication Manager automatically inserts a '+' digit in this case.

**Note:** During testing the extension numbers were reformatted to national numbers for Trunk Group 2 only. The numbers were left unchanged for Trunk Group 1 which is used within the enterprise.

## 5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the NOS SIP Trunking Service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to invoke ARS directly. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *69		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>		Access Code 2:

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. In the example shown, national calls are sent to **Route Pattern 11** and international calls are sent to **Route Pattern 12** where the called party numbers are converted to E.164 format. Non-geographic numbers go to **Route Pattern 2** which does not reformat the number.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
0	7	12	11	pubu		n	
00	7	15	12	pubu		n	
001	13	13	12	pubu		n	
0035391	13	13	12	pubu		n	
11	3	3	2	pubu		n	
700	4	4	1	pubu		n	
						n	

Use the **change route-pattern n** command, where **n** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **11** is used to route **National** calls and route pattern **12** is used to route **International** calls to trunk group **2**.

The following screenshot shows an example of a route pattern for national calls:

change route-pattern 11														Page 1 of 3
Pattern Number: 11      Pattern Name: National														
SCCAN? n      Secure SIP? n      Used for SIP stations? n														
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ IXC QSIG Intw						
1:	2	0				1	p351	n	user					
2:								n	user					
3:								n	user					
4:								n	user					
5:								n	user					
6:								n	user					
	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	Sub Dgts	Numbering Format	LAR			
	0	1	2	M	4	W	Request							
1:	y	y	y	y	y	n	n	rest		intl-pub	none			
2:	y	y	y	y	y	n	n	rest			none			
3:	y	y	y	y	y	n	n	rest			none			
4:	y	y	y	y	y	n	n	rest			none			
5:	y	y	y	y	y	n	n	rest			none			
6:	y	y	y	y	y	n	n	rest			none			

**Note:** In the test environment, the **No. Del Dgts** field was used to delete the leading zero of the national number. The **Inserted Digits** field was used to prefix the dialled number with +351 (**p351**) to convert to E.164 format.

The following screenshot shows an example of a route pattern for international calls:

change route-pattern 12												Page 1 of 3		
Pattern Number: 12												Pattern Name: International		
SCCAN? n		Secure SIP? n		Used for SIP stations? n										
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted		DCS/ IXC				
No				Mrk	Lmt	List	Del	Digits		QSIG				
							Dgts			Intw				
1:	2	0					2	p		n	user			
2:										n	user			
3:										n	user			
4:										n	user			
5:										n	user			
6:										n	user			
BCC		VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature	PARM	Sub	Numbering	LAR
0		1	2	M	4	W	Request					Dgts	Format	
1:	y	y	y	y	y	n	n	rest					intl-pub	none
2:	y	y	y	y	y	n	n	rest						none
3:	y	y	y	y	y	n	n	rest						none
4:	y	y	y	y	y	n	n	rest						none
5:	y	y	y	y	y	n	n	rest						none
6:	v	v	v	v	v	n	n	rest						none

**Note:** In the test environment, the **No. Del Dgts** field was used to delete the two leading zeros of the international number. The **Inserted Digits** field was used to prefix the dialled number with + (p).

**Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP signalling as it does in TDM and during testing it was set to **intl-pub**.

## 5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to Communication Manager extensions. The incoming digits sent in the INVITE message from NOS can be manipulated as necessary to route calls to the desired extension. Use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**.

In the example shown, 12-digit numbers are received in international format for incoming calls. All digits are deleted and the extension number is inserted, this may not be required in the live environment where the extension number forms part of the DDI number. Note that some of the DDI digits have been obscured.

change inc-call-handling-trmt trunk-group 2						Page	1 of	3
INCOMING CALL HANDLING TREATMENT								
Service/ Feature	Number Len	Number Digits	Del	Insert				
public-ntwrk	12	351212nnnn12	12	2000				
public-ntwrk	12	351212nnnn27	12	2316				
public-ntwrk	12	351212nnnn79	12	2391				
public-ntwrk	12	351212nnnn22	12	2400				
public-ntwrk	12	351218nnnn98	12	2291				
public-ntwrk								



## 5.10. EC500 Configuration

When EC500 is enabled on a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone.

The following screen shows an example EC500 configuration for the user with station extension 2291. Use the command **change off-pbx-telephone station-mapping x** where **x** is Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration, in the test environment **00** was used as the international dial prefix.
- For the **Phone Number** enter the phone that will also be called (e.g. **35391nnnn25**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 2291							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2291	OPS	-	-	2291	aar	1	
2291	EC500	00	-	35391482425	ars	1	
		-	-				

**Note:** The phone number shown is for a test phone in the Avaya Lab. To use facilities for calls coming in from EC500 mobile phones, the calling party number received in Communication Manager must exactly match the number specified in the above table. Note also that the station shown is a SIP phone so is also in the off-PBX station mapping as an Off-PBX Station (OPS).

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

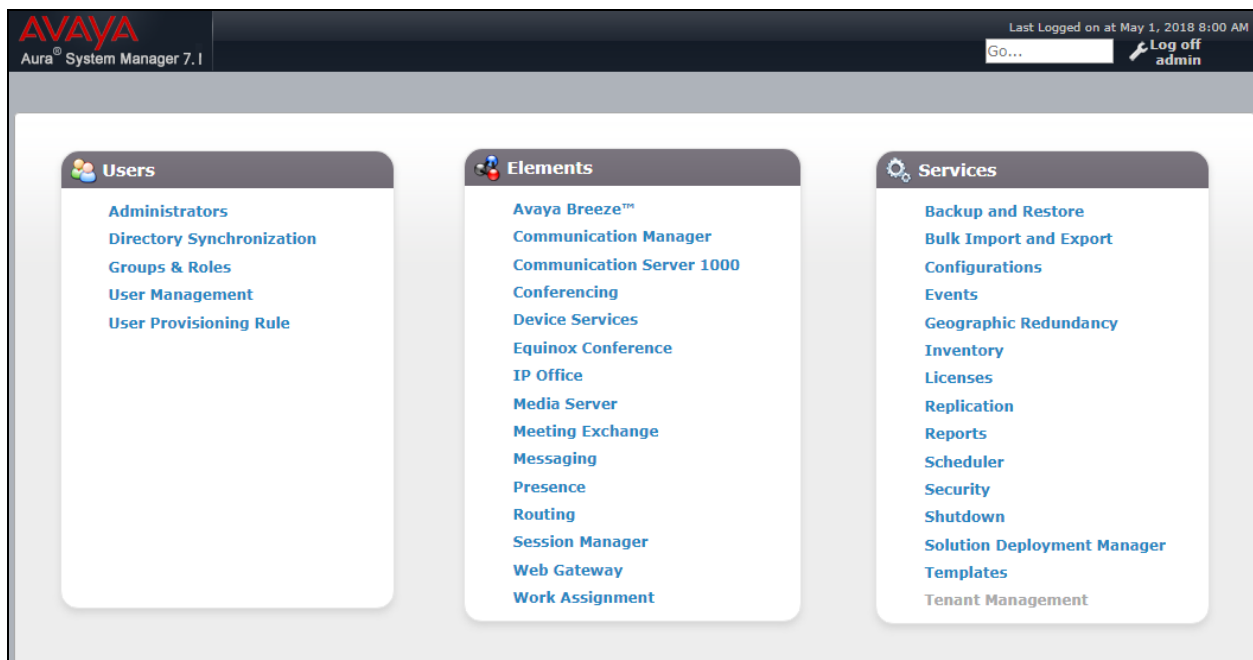
## 6. Configuring Avaya Aura® Session Manager

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

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

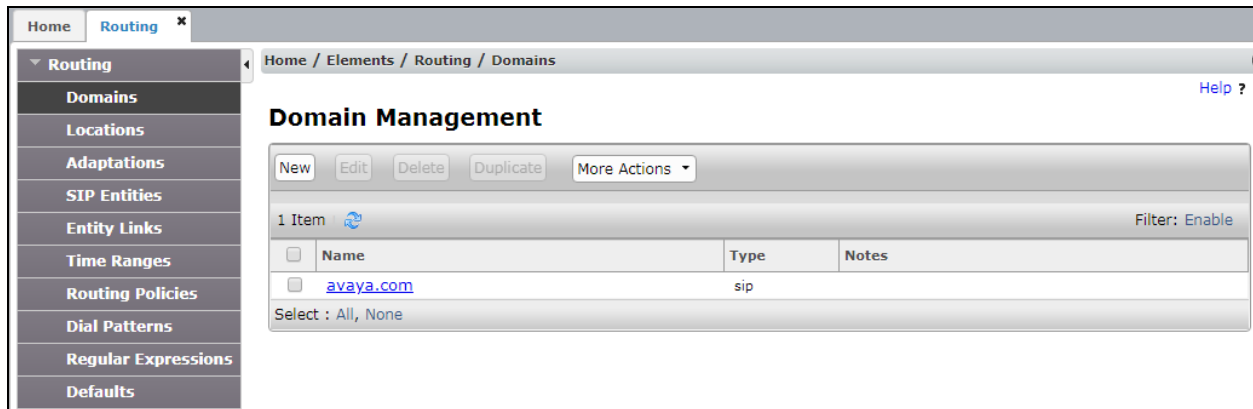
### 6.1. Log in to Avaya Aura® System Manager

Access System Manager using a web browser and entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** 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 the left-hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name of the enterprise site or a name agreed with NOS; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on Communication Manager. Refer to **Section 5.3** for details. In the test environment, **avaya.com** was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click **Commit** to save changes.



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

## 6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all the enterprise SIP entities and another for the NOS SIP trunk. The two Locations were named Galway\_Lab and Service\_Provider and were identical in every other way.

On the **Routing** tab select **Locations** from the left-hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Below is the location configuration used for the test enterprise.

Home / Elements / Routing / Locations
Help ?

Commit

Cancel

### Location Details

#### General

\* Name:

Notes:

#### Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

#### Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

#### Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

 Kbit/Sec

\* Minimum Multimedia Bandwidth:

 Kbit/Sec

\* Default Audio Bandwidth:

 Kbit/sec

#### Alarm Threshold

Overall Alarm Threshold:

 %

Multimedia Alarm Threshold:

 %

\* Latency before Overall Alarm Trigger:

 Minutes

\* Latency before Multimedia Alarm Trigger:

 Minutes

#### Location Pattern

Add

Remove

0 Items

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes

Commit

Cancel

**Note: Location Pattern** can be used to refine the location down to specific subnets. That refinement was not required in the test environment.

## 6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers. An Adaptation was used during testing to remove Avaya proprietary headers from messages sent from Session Manager.

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

- In the **Adaptation Name** field, enter a descriptive title for the adaptation.
- In the **Module Name** drop down menu, select **DigitConversionAdapter**.
- In the **Module Parameter Type** drop down menu, select **Name-Value Parameter**.
- In the **Name** box, type **eRHdrs**.
- In the **Value** box, type the list of headers to be deleted. During testing, the following list was used: **"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, P-Conference, Alert-Info, Correlation-ID, Accept-Language"**.

Home / Elements / Routing / Adaptations

Adaptation Details [Help ?](#)

**General**

\* **Adaptation Name:**

\* **Module Name:**

**Module Parameter Type:**

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

Select : All, None

**Egress URI Parameters:**

**Notes:**

This Adaptation is intended for traffic from Session Manager to the Avaya SBCE and was applied to the Avaya SBCE SIP Entities as described in **Section 6.5**. To apply the module, it is matched to the calling party number of calls from Session Manager, this is the DDI assigned to the Communication Manager extension.

Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear for digit manipulation.

- Enter a **Matching Pattern** to identify calls for which the Adaptation is required. In the test environment, this was the calling party number of the Communication Manager extensions.
- Enter the **Min** and **Max** values, the example is for **13**-digit numbers only.
- Enter **Delete Digits**, a value of **0** ensures that the number is analysed but not modified.
- Select **origination** from the **Address to modify** drop down menu as matching is only to be done on the calling party number.

### Digit Conversion for Incoming Calls to SM

Add
Remove

0 Items
Filter: Enable

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

### Digit Conversion for Outgoing Calls from SM

Add
Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	*+35121nnnnnnnn	*13	*13		*0		origination	

Select : All, None

Commit
Cancel

## 6.5. Administer SIP Entities

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

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP Entity, **CM** for a Communication Manager SIP Entity and **SIP Trunk** for the Avaya SBCE SIP Entity.
- In the **Adaptation** field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop-down menu.
- In the **Location** field select the appropriate location from the drop-down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are five SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity for the SIP Endpoints.
- Avaya Aura® Communication Manager SIP Entity for the SIP Trunk.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity for server flows with the primary network SBC.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity for server flows with the backup network SBC.

### 6.5.1. Avaya Aura® Session Manager SIP Entity

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

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with a 'Help ?' link and 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The form contains the following fields:

- Name:** Session\_Manager
- FQDN or IP Address:** 10.10.9.31
- Type:** Session Manager (dropdown)
- Notes:** (empty text area)
- Location:** Galway\_Lab (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text area)

The 'Monitoring' section at the bottom contains:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration (dropdown)

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 the domain added in **Section 6.2** as the default domain.

**Failover Ports**  
 TCP Failover port:   
 TLS Failover port:

**Listen Ports**  

4 Items 
Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP ▼	avaya.com ▼	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	5060	UDP ▼	avaya.com ▼	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	5061	TLS ▼	avaya.com ▼	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	5063	TLS ▼	avaya.com ▼	<input type="checkbox"/>	<input type="text"/>

Select : All, None

### 6.5.2. Avaya Aura® Communication Manager SIP Entities

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

Home / Elements / Routing / SIP Entities

**SIP Entity Details**

**General**

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

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

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:



Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

**Loop Detection**

Loop Detection Mode: On ▼

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

**Monitoring**

SIP Link Monitoring: Use Session Manager Configuration ▼

CRLF Keep Alive Monitoring: Use Session Manager Configuration ▼

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association: ▼

Backup Session Manager Bandwidth Association: ▼

**Note:** A second SIP Entity for Communication Manager is required for SIP Endpoints. In the test environment this is named “CM\_SIP\_Endpoints”.

### 6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE connection to the primary network SBC. The **FQDN or IP Address** field is the internal Avaya SBCE interface used for traffic to and from the primary network SBC. Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

**SIP Entity Details** Commit Cancel

**General**

\* Name: ASBCE\_1

\* FQDN or IP Address: 10.10.9.81

Type: SIP Trunk ▼

Notes:

Adaptation: Header\_Removal ▼

Location: Service\_Provider ▼

Time Zone: Europe/Dublin ▼

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

Minimum TLS Version: Use Global Setting ▼

Credential name:

Securable: ☐

Call Detail Recording: egress ▼

The next screen shows the SIP Entity for the Avaya SBCE connection to the backup network SBC. The **FQDN or IP Address** field is the internal Avaya SBCE interface used for traffic to and from the backup network SBC. Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

### SIP Entity Details

Commit Cancel

**General**

\* Name: ASBCE\_2

\* FQDN or IP Address: 10.10.9.82

Type: SIP Trunk ▼

Notes:

Adaptation: Header\_Removal ▼

Location: Service\_Provider ▼

Time Zone: Europe/Dublin ▼

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

Minimum TLS Version: Use Global Setting ▼

Credential name:

Securable: ☐

Call Detail Recording: egress ▼

**Note:** The SIP Entity **FQDN or IP** Addresses match the internal network IP addresses of the Avaya SBCE specified in **Section 7.2**.

## 6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left-hand 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**.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests. For the Avaya SBCE, this matches the port defined in **Section 7.4.1**.
- 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.

Home / Elements / Routing / Entity Links Help ?

### Entity Links

New Edit Delete Duplicate More Actions ▾

5 Items Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	<a href="#">ASBCE_Backup_Link</a>	Session_Manager	TLS	5061	ASBCE_2	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">ASBCE_Primary_Link</a>	Session_Manager	TLS	5061	ASBCE_1	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">CM_Endpoint_Link</a>	Session_Manager	TLS	5063	CM_SIP_Endpoints	5063	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">CM_Trunk_Link</a>	Session_Manager	TLS	5061	CM Trunk	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">Messaging_Link</a>	Session_Manager	TCP	5060	Messaging	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Select : All, None

Click **Commit** to save changes. The previous screen shows the Entity Links used in this configuration.

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

## 6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left-hand 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

In the test environment, the default **Time of Day** was used and the **Ranking** was set to enable 1<sup>st</sup> and 2<sup>nd</sup> choice routing to the network SBC's.

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

Home / Elements / Routing / Routing Policies Help ?

### Routing Policy Details

Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM Trunk	10.10.9.12	CM	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: 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

The following screen shows the Routing Policy for the SIP Trunk to the primary network SBC via the Avaya SBCE.

Home / Elements / Routing / Routing Policies Help ?

### Routing Policy Details

Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
ASBCE_1	10.10.9.81	SIP Trunk	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	10	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

**Note:** The **Ranking** parameter in the **Time of Day** policy has been assigned an arbitrary value. If this value is less than that assigned to the Routing Policy for the SIP Trunk to the backup network SBC, this Routing Policy will be selected as first choice in the Dial Pattern described in **Section 6.8**. In the test environment, the ranking was applied to the default **24/7** policy.

The next screen shows the Routing Policy for the SIP Trunk to the backup network SBC via the Avaya SBCE.

Home / Elements / Routing / Routing Policies Help ?

## Routing Policy Details

Commit Cancel

### General

\* Name:

Disabled: ☐

\* Retries:

Notes:

### SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE_2	10.10.9.82	SIP Trunk	

### Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	<input type="text" value="20"/>	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

**Note:** The **Ranking** parameter in the **Time of Day** policy has been assigned a value greater than that assigned to the Routing Policy for the SIP Trunk to the primary network SBC. This Routing Policy will be selected as second choice in the Dial Pattern described in **Section 6.8**. In the test environment, the ranking was applied to the default **24/7** policy.

## 6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern, select **Dial Patterns** on the left-hand menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Avaya SBCE which will route calls to E.164 destination numbers via the NOS primary and backup network SBC's.

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* **Pattern:** +

\* **Min:** 8

\* **Max:** 16

**Emergency Call:** ☐

**Emergency Priority:** 1

**Emergency Type:**

**SIP Domain:** -ALL-

**Notes:**

**Originating Locations and Routing Policies**

Add Remove

2 Items 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"/>	Galway_Lab		Outbound_Primary	10	<input type="checkbox"/>	ASBCE_1	
<input type="checkbox"/>	Galway_Lab		Outbound_Backup	20	<input type="checkbox"/>	ASBCE_2	

Select : All, None

**Note:** The **Rank** value ensures that the **Outbound\_Primary** Routing Policy is the 1<sup>st</sup> choice and the **Outbound\_Backup** is the second choice Routing Policy. The Rank values are defined in the Time of Day policy as described in **Section 6.7**.

The next screen shows an example dial pattern configured for the Avaya SBCE which will route calls to non-geographic numbers, in this case Directory Enquiries, via the NOS primary and backup network SBC's.

Home / Elements / Routing / Dial Patterns
[Help ?](#)

**Dial Pattern Details**

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

2 Items 
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"/>	Galway_Lab		Outbound_Primary	10	<input type="checkbox"/>	ASBCE_1	
<input type="checkbox"/>	Galway_Lab		Outbound_Backup	20	<input type="checkbox"/>	ASBCE_2	

Select : [All](#), [None](#)

**Note:** The above Dial Pattern uses the same first and second choice Routing Policies as used for E.164 destinations.

The following screen shows the test dial pattern configured for assigned DDI numbers.

Home / Elements / Routing / Dial Patterns

Help ?

## Dial Pattern Details

CommitCancel

### General

\* Pattern:

35121

\* Min:

12

\* Max:

12

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

### Originating Locations and Routing Policies

AddRemove

2 Items

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"/>	Galway_Lab		Outbound_Primary	10	<input type="checkbox"/>	ASBCE_1	
<input type="checkbox"/>	Service_Provider		CM_Inbound	0	<input type="checkbox"/>	CM Trunk	

Select : All, None

### Denied Originating Locations

AddRemove

0 Items

Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

CommitCancel

**Note:** The above configuration was used to analyse the DDI numbers assigned to the extensions on Communication Manager. It was required for testing that a DDI number could be dialled from a Communication Manager extension and the call would route via the network and back to the enterprise. To allow this, locations were used so that if the call originated in the network, it would route to the enterprise. If the call originated in the enterprise, it would route to the network.



The following screen shows the test dial pattern configured for Communication Manager extension numbers.

Home / Elements / Routing / Dial Patterns
[Help ?](#)

Dial Pattern Details
Commit Cancel

General

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items 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"/>	Galway_Lab		CM_Endpoints	0	<input type="checkbox"/>	CM_SIP_Endpoints	
<input type="checkbox"/>	Service_Provider		CM_Inbound	0	<input type="checkbox"/>	CM Trunk	

Select : All, None

**Note:** The configuration above was used to analyse the extension numbers and route to Communication Manager via the Entity Link for **CM\_SIP\_Endpoints** which uses a different port number than that used for calls coming in from the SIP Trunk. This is required for off-PBX extensions such as SIP Endpoints.

## 6.9. Administer Application for Avaya Aura® Communication Manager

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

- In the **Name** field enter a name for the application.
- In the **SIP Entity** field select the SIP entity for Communication Manager.
- In the **CM System for SIP Entity** field select the SIP entity for Communication Manager and select **Commit** to save the configuration.

The screenshot shows the 'Application Editor' window in the Avaya Aura Communication Manager interface. The left-hand menu is expanded to 'Session Manager', and the 'Applications' option is selected. The main content area displays the 'Application Editor' form. The form includes fields for 'Name' (CM\_App), 'SIP Entity' (CM\_SIP\_Endpoints), 'CM System for SIP Entity' (CM1\_Element), and 'Description'. Below these fields is a section for 'Application Attributes (optional)' with a table for 'Name' and 'Value'. The table has two rows: 'Application Handle' and 'URI Parameters'. Below this is a section for 'Application Media Attributes' with a checkbox for 'Enable Media Filtering' and a table for 'Audio', 'Video', 'Text', 'Match Type', and 'If SDP Missing'. The table has five columns and one row of values: YES, YES, YES, NOT\_EXACT, and ALLOW.

Home / Elements / Session Manager / Application Configuration / Applications

**Application Editor** Commit Cancel Help ?

**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"/>

**Application Media Attributes**

Enable Media Filtering ☐

Audio	Video	Text	Match Type	If SDP Missing
<input type="text" value="YES"/>	<input type="text" value="YES"/>	<input type="text" value="YES"/>	<input type="text" value="NOT_EXACT"/>	<input type="text" value="ALLOW"/>

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

## 6.10. Administer Application Sequence for Avaya Aura® Communication Manager

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

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

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

### Application Sequence Editor

---

#### Application Sequence

\*Name

Description

---

#### Applications in this Sequence

1 Item

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

Select : All, None

---

#### Available Applications

1 Item Filter: [Enable](#)

	Name	SIP Entity	Description
	<a href="#">CM_App</a>	CM_SIP_Endpoints	

## 6.11. Administer SIP Extensions

The SIP extensions are likely to have been defined during installation. The configuration shown in this section is for reference. SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** 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. [2292@avaya.com](mailto:2292@avaya.com) which is used to create the user's primary handle.
- The **Authentication Type** should be **Basic**.
- In the **Password/Confirm Password** fields enter an alphanumeric password.
- Set the **Language Preference** and **Time Zone** as required.

Home | User Management x

Home / Users / User Management / Manage Users

Help ?

**New User Profile**

Commit & Continue | Commit | Cancel

Identity \* | Communication Profile | Membership | Contacts

User Provisioning Rule

User Provisioning Rule: [v]

Identity

\* Last Name: [SIP]  
Last Name (Latin Translation): [SIP]

\* First Name: [9608]  
First Name (Latin Translation): [9608]  
Middle Name: [ ]  
Description: [ ]

\* Login Name: [2292@avaya.com]  
Email Address: [ ]  
User Type: [Basic v]  
Password: [ ]  
Confirm Password: [ ]  
Localized Display Name: [ ]  
Endpoint Display Name: [ ]  
Title: [ ]  
Language Preference: [English (United Kingdom) v]  
Time Zone: [(+1:0)GMT : Dublin, Edinburgh, v]  
Employee ID: [ ]  
Department: [ ]  
Company: [ ]

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

**Communication Profile**

Communication Profile Password: .....  
 Confirm Password: ..... [Generate](#)

**Communication Address**

Type	Handle	Domain
No Records found		

☐ **Session Manager Profile** ▶  
☐ **CM Endpoint Profile** ▶

**\*Required** Commit & Continue Commit Cancel

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

**Communication Address**

Type	Handle	Domain
No Records found		


Type: Avaya SIP

**\* Fully Qualified Address:** 2292 @ avaya.com

Add Cancel

Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked.
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field.
- Select the appropriate **Application Sequences** from the drop-down menus in the **Origination Sequence** and **Termination Sequence** fields configured in **Section 6.10**.
- Repeat the previous step for **Emergency Calling Application Sequences**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.

☒ **Session Manager Profile** 

### SIP Registration

\* Primary Session Manager

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices

Block New Registration When  
Maximum Registrations Active?

☐

Primary	Secondary	Maximum
4	0	4

### Application Sequences

Origination Sequence

Termination Sequence

### Emergency Calling Application Sequences

Emergency Calling Origination Sequence

Emergency Calling Termination Sequence

### Call Routing Settings

\* Home Location

Conference Factory Set

### Call History Settings

Enable Centralized Call History?

☐

Expand the **Endpoint Profile** section.

- Select Communication Manager Element from the **System** drop-down menu.
- Select **Endpoint** from the drop-down menu for **Profile Type**.
- Enter the extension in the **Extension** field.
- Select the desired template from the **Template** drop-down menu.
- In the **Port** field **IP** is automatically inserted.
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.
- Select **Commit** (Not Shown) to save changes and the System Manager will add Communication Manager user configuration automatically.

☒ **CM Endpoint Profile** ▼

\* System

CM1\_Element ▼

\* Profile Type

Endpoint ▼

Use Existing Endpoints ☐

\* Extension

Display Extension Ranges

2292

Endpoint Editor

\* Template

9608SIP\_DEFAULT\_CM\_7\_1 ▼

Set Type 9608SIP

Security Code

Port IP

Voice Mail Number 7000

Preferred Handle (None) ▼

Calculate Route Pattern ☐

Sip Trunk aar

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☒

Override Endpoint Name and Localized Name ☒

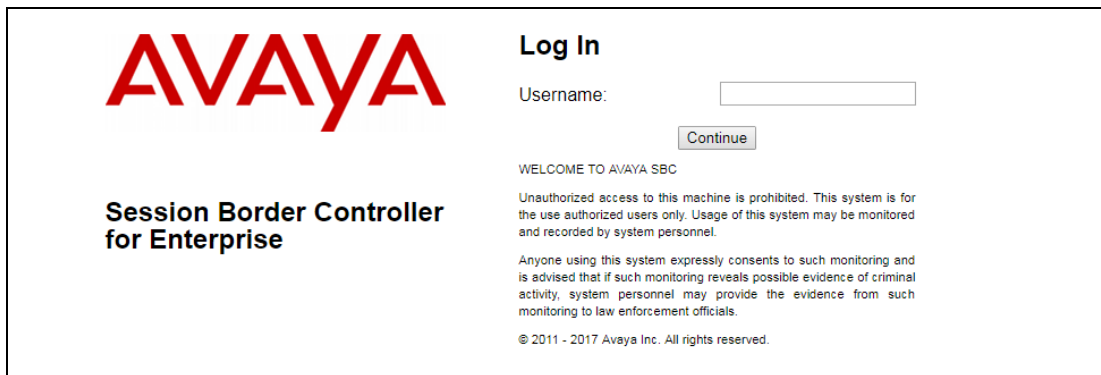
Allow H.323 and SIP Endpoint Dual Registration ☐

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

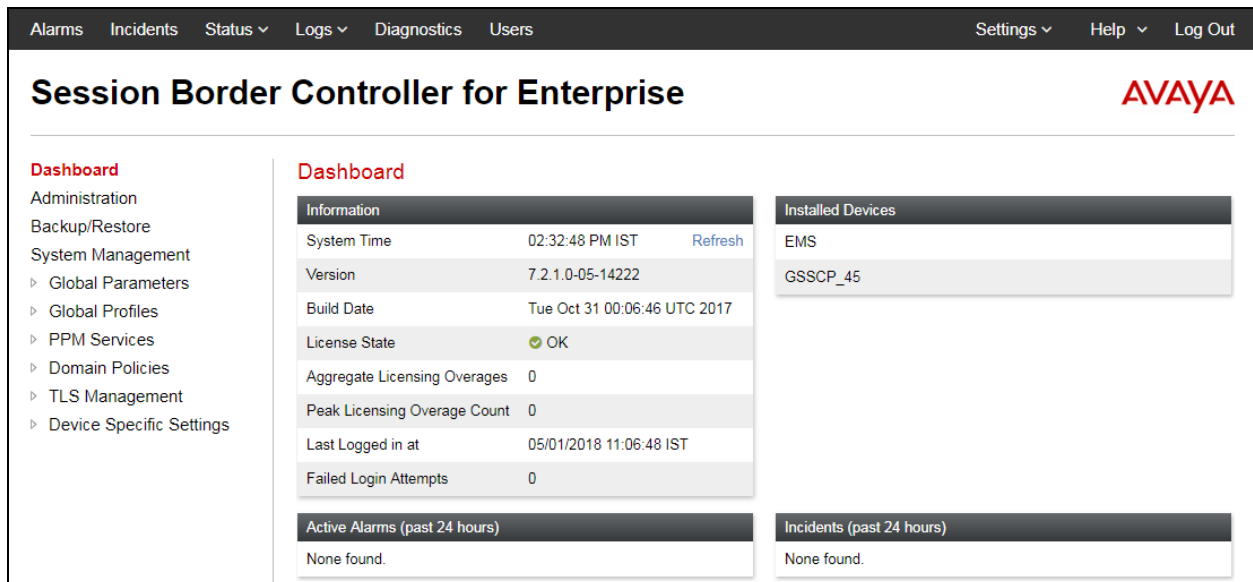
### 7.1. Access Avaya Session Border Controller for Enterprise

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



The login screen for the Avaya Session Border Controller for Enterprise. It features the Avaya logo in red on the left. To the right, under the heading "Log In", there is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, a message reads: "WELCOME TO AVAYA SBC. Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, it states "© 2011 - 2017 Avaya Inc. All rights reserved."

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



The dashboard for the Avaya Session Border Controller for Enterprise. It has a top navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left is a sidebar menu with "Dashboard" selected, and sub-items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Dashboard" and contains several sections: "Information" (System Time: 02:32:48 PM IST, Version: 7.2.1.0-05-14222, Build Date: Tue Oct 31 00:06:46 UTC 2017, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 05/01/2018 11:06:48 IST, Failed Login Attempts: 0), "Installed Devices" (EMS, GSSCP\_45), "Active Alarms (past 24 hours)" (None found), and "Incidents (past 24 hours)" (None found).



## 7.2. Define Network Management

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

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

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.81	Edit Delete

Enter details for the external interfaces in the dialogue box:

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

IP Address	Public IP	Gateway Override	
10.223.77.85	Use IP Address	Use Default	Delete

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBCE. Enter details in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** twice and additional rows will appear allowing IP addresses to be entered.
- Enter the internal IP addresses for the fixed and mobile trunks in the **IP Address** fields and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

**Edit Network**

This Network contains one or more IP Address entries which are in use. If the Interface, an IP Address, or Public IP which is in use is modified, the application **must** be restarted or the device may stop functioning.

Name:

Default Gateway:

Network Prefix or Subnet Mask:

Interface:

IP Address	Public IP	Gateway Override	
<input type="text" value="10.10.9.81"/>	<input type="text" value="Use IP Address"/>	<input type="text" value="Use Default"/>	<input type="button" value="Delete"/>
<input type="text" value="10.10.9.82"/>	<input type="text" value="Use IP Address"/>	<input type="text" value="Use Default"/>	<input type="button" value="Delete"/>

The following screenshot shows the completed Network Management configuration:

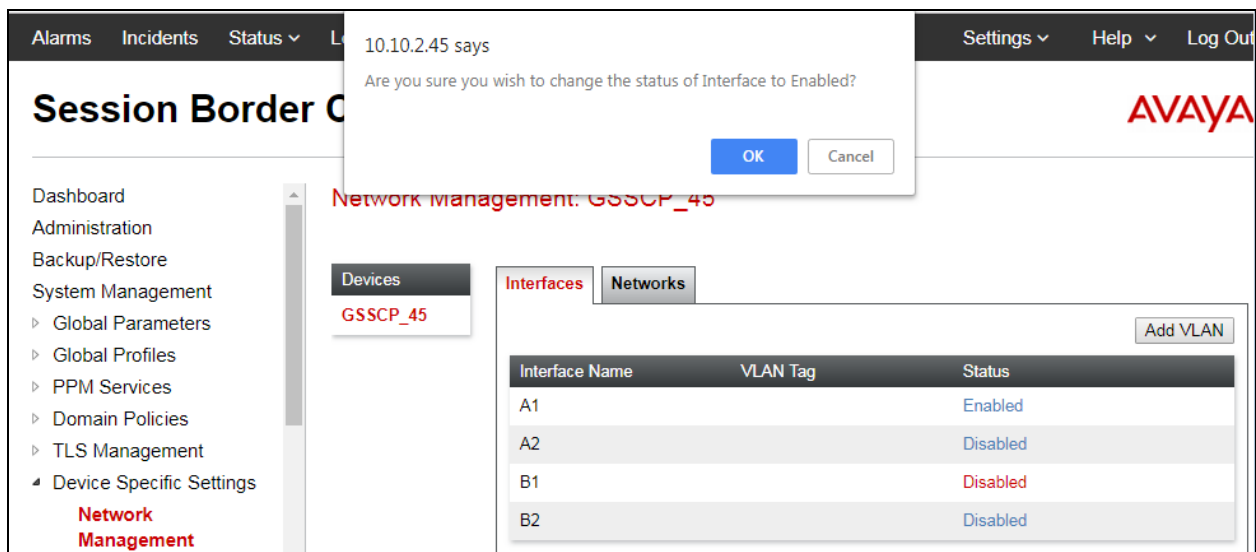
**Network Management: GSSCP\_45**

Devices: **GSSCP\_45**

Interfaces: **Networks**

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.81, 10.10.9.82	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
External	10.223.77.85	255.255.255.252	B1	10.223.77.86	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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



**Note:** to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

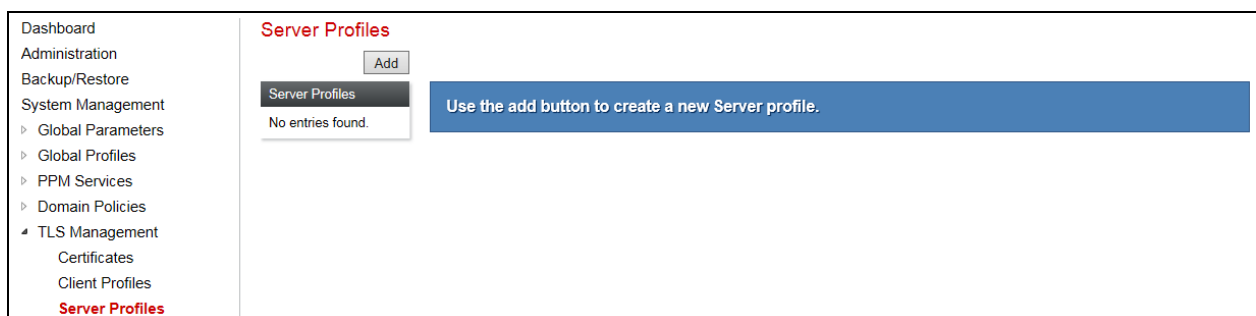
A status box will appear that will indicate when the restart is complete.

## 7.3. Define TLS Profiles

TLS profiles are required to support TLS on the interfaces. The implementation of certificates is beyond the scope of this document and is assumed to be already in place. The signalling interfaces require a TLS server profile and the server configuration requires a TLS client profile.

### 7.3.1. Server Profile

To define a TLS server profile on the Avaya SBCE, navigate to **TLS Management → Server Profiles** in the main menu on the left-hand side. Click on **Add**.



Details of the TLS server profile for the signalling interfaces are entered here.

- In the **Name** field enter a descriptive name for the server profile.
- In the **Certificate** drop down menu, select the Avaya SBCE identity certificate to be used for this profile.
- Select **Peer Verification** as required. In the test environment peer verification was made optional by selecting **Optional** in the drop-down menu.
- Highlight the trusted root certificate in the **Peer Certificate Authorities** field.
- Set the **Verification Depth** as required. The example shown is for the link with Session Manager which has an identity certificate provided by a System Manager implemented as a sub-CA. This means that the Session Manager identity certificate is signed by an intermediate certificate which is in turn signed by a root certificate. This gives it a verification depth of **2**.

**New Profile** X

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

**TLS Profile**

Profile NameASBCE45\_Server

Certificateasbce45.pem

**Certificate Verification**

Peer VerificationOptional

Peer Certificate AuthoritiesGSSCP\_Root.crt

Peer Certificate Revocation Lists

Verification Depth2

Next

Click on **Next** to complete the server profile configuration. In the test environment, these parameters were left at default values.

The screenshot shows a 'New Profile' configuration window with two main sections: 'Renegotiation Parameters' and 'Handshake Options'. In the 'Renegotiation Parameters' section, 'Renegotiation Time' is set to 0 seconds and 'Renegotiation Byte Count' is set to 0. The 'Handshake Options' section shows 'Version' with 'TLS 1.2' selected, and 'Ciphers' with 'Default' selected. A 'Value' field contains the string 'HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH'. At the bottom are 'Back' and 'Finish' buttons.

Click on **Finish**.

### 7.3.2. Client Profile

To define a TLS client profile on the Avaya SBCE, navigate to **TLS Management → Client Profiles** in the main menu on the left-hand side. Click on **Add**.

The screenshot shows the Avaya SBCE interface. On the left is a navigation menu with 'Client Profiles' highlighted. The main area shows a 'Client Profiles' section with an 'Add' button and a message: 'Use the add button to create a new Client profile.' Below this, a box indicates 'No entries found.'

Details of the TLS client profile for the signalling interfaces are entered here.

- In the **Name** field enter a descriptive name for the server profile.
- In the **Certificate** drop down menu, select the Avaya SBCE identity certificate to be used for this profile.
- Note that **Peer Verification** is always **Required** for the client profile.
- Highlight the trusted root certificate in the **Peer Certificate Authorities** field.
- Set the **Verification Depth** as required. The example shown is for the link with Session Manager which has an identity certificate provided by a System Manager implemented as a sub-CA. This means that the Session Manager identity certificate is signed by an intermediate certificate which is in turn signed by a root certificate. This gives it a verification depth of **2**.

New ProfileX

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

Profile NameASBCE45\_Client

Certificateasbce45.pem

Certificate Verification

Peer VerificationRequired

Peer Certificate AuthoritiesGSSCP\_Root.crt

Peer Certificate Revocation Lists

Verification Depth2

Extended Hostname Verification☐

Custom Hostname Override

Next

BG; Reviewed:  
SPOC 7/9/2018

Solution & Interoperability Test Lab Application Notes  
©2018 Avaya Inc. All Rights Reserved.

46 of 81  
NOS\_CM71\_SBC72

Click on **Next** to complete the client profile configuration. In the test environment, these parameters were left at default values.

The screenshot shows a 'New Profile' configuration window with two main sections: 'Renegotiation Parameters' and 'Handshake Options'. In the 'Renegotiation Parameters' section, 'Renegotiation Time' is set to 0 seconds and 'Renegotiation Byte Count' is set to 0. The 'Handshake Options' section shows 'Version' with 'TLS 1.2' selected, and 'Ciphers' with 'Default' selected. A 'Value' field contains the text 'HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH'. At the bottom are 'Back' and 'Finish' buttons.

Click on **Finish**.

## 7.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TLS used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the NOS SIP Trunking Service. Two signalling interfaces were required on the internal side of the Avaya SBCE to allow selection of the primary or backup network SBC's from the Session Manager as described in **Section 6.7** and **Section 6.8**.

### 7.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** (not shown) in the main menu on the left-hand side. Click on **Add**.

The screenshot shows the 'Signaling Interface: GSSCP\_45' configuration page. On the left is a navigation menu with 'Signaling Interface' selected. The main area has a 'Signaling Interface' tab and a message: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a blue button labeled 'Add'. At the bottom, a blue box contains the text 'Use the add button to create a new Signaling Interface.'

Details of transport protocol and ports for the external and internal SIP signalling are entered here.

- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop-down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **10.223.77.86**.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the NOS SIP Trunking Service.

The screenshot shows the 'Add Signaling Interface' dialog box with the following fields and values:

- Name:** External
- IP Address:** External (B1, VLAN 0) (selected), 10.223.77.86 (selected)
- TCP Port:** (empty, with text 'Leave blank to disable')
- UDP Port:** 5060 (with text 'Leave blank to disable')
- TLS Port:** (empty, with text 'Leave blank to disable')
- TLS Profile:** None (selected)
- Enable Shared Control:** ☐
- Shared Control Port:** (empty)
- Finish** button at the bottom.

The internal signalling interfaces are defined in the same way. The two interfaces allow routing via the primary and backup network SBC's from Session Manager.

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TLS** port number, **5061** is used for Session Manager.
- Select the **TLS Profile** defined in **Section 7.3** from the drop-down menu.

The two screenshots show the 'Add Signaling Interface' dialog box for internal interfaces with the following fields and values:

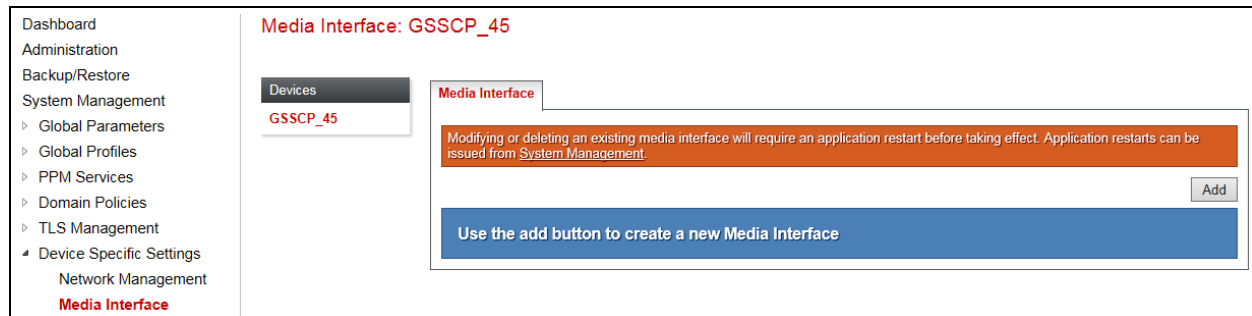
- Left Screenshot (Internal\_Primary):**
  - Name:** Internal\_Primary
  - IP Address:** Internal (A1, VLAN 0) (selected), 10.10.9.81 (selected)
  - TCP Port:** 5060 (with text 'Leave blank to disable')
  - UDP Port:** (empty, with text 'Leave blank to disable')
  - TLS Port:** 5061 (with text 'Leave blank to disable')
  - TLS Profile:** ASBCE45\_Server (selected)
  - Enable Shared Control:** ☐
  - Shared Control Port:** (empty)
  - Finish** button at the bottom.
- Right Screenshot (Internal\_Backup):**
  - Name:** Internal\_Backup
  - IP Address:** Internal (A1, VLAN 0) (selected), 10.10.9.81 (selected)
  - TCP Port:** 5060 (with text 'Leave blank to disable')
  - UDP Port:** (empty, with text 'Leave blank to disable')
  - TLS Port:** 5061 (with text 'Leave blank to disable')
  - TLS Profile:** ASBCE45\_Server (selected)
  - Enable Shared Control:** ☐
  - Shared Control Port:** (empty)
  - Finish** button at the bottom.



**Note:** In the test environment, the internal IP addresses were **10.10.9.81** for routing via the primary and **10.10.9.82** for routing via the backup network SBC's.

## 7.4.2. Media Interfaces

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

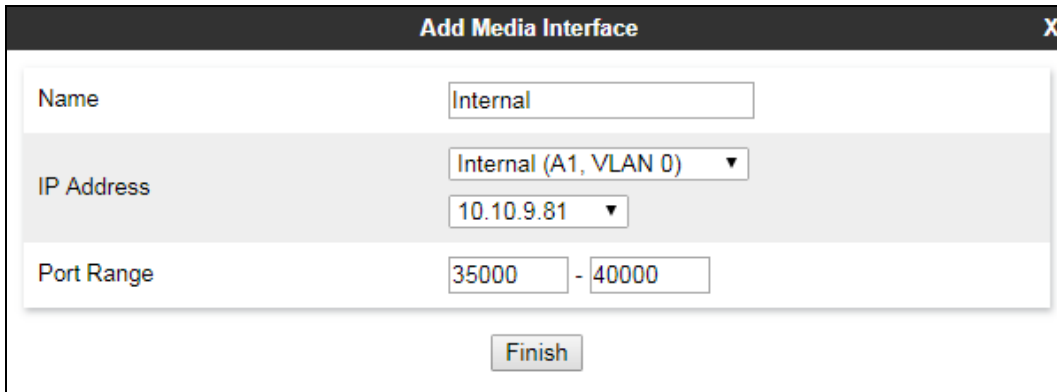


Details of the RTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop-down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **10.223.77.86**.
- Define the RTP **Port Range** for the media path with the NOS SIP Trunking Service, during testing this was left at the default values.

The internal media interface is defined in the same way:

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Define the RTP **Port Range** for the media path with the enterprise endpoints, during testing this was left at the default values.
- Select the TLS server profile defined in **Section 7.3**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three rows of input fields:

- Name:** A text input field containing the value "Internal".
- IP Address:** A dropdown menu showing "Internal (A1, VLAN 0)" with a downward arrow. Below it, a sub-dropdown menu shows the IP address "10.10.9.81" with a downward arrow.
- Port Range:** Two text input boxes separated by a hyphen. The first box contains "35000" and the second box contains "40000".

At the bottom center of the dialog is a button labeled "Finish".

**Note:** In the test environment, only one internal media interface was defined as separate interfaces for the primary and backup network SBC's were not required for media.

## 7.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, NOS SIP Trunking is connected as the Trunk Server and Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions. Note that only one interworking profile is required for NOS even though there are separate signalling links for the primary and backup network SBC's.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left-hand side. To define Server Interworking for NOS SIP Trunking, highlight the **avaya-ru** profile and click on **Clone**.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

A pop-up menu is generated. In the **Name** field enter a descriptive name for the NOS SIP Trunking network and click **Finish**.

Select the General tab of the resulting Interworking Profile and click on Edit (not shown).

Select the General tab of the resulting Interworking Profile and click on Edit (not shown). The screenshot shows the cloned profile. Check the **T.38 Support** box and leave the rest of the parameters at their original settings. Click on **Finish**.

**Editing Profile: SIP\_Trunk** X

**General**

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

**Finish**

Select the **Advanced** tab (not shown) and click on **Edit**.

Set **Record Routes** to **None** as this header is not used by the network and select **None** in the **Extensions** drop down menu. Ensure that the **Has Remote SBC** box is checked. Click on **Finish**.

Editing Profile: SIP\_Trunk

X

Record Routes

☒ None

☐ Single Side

☐ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

☒

Extensions

None

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

Relay INVITE Replace for SIPREC

☐

MOBX Re-INVITE Handling

☐

DTMF

DTMF Support

☒ None

☐ SIP Notify

☐ RFC 2833 Relay & SIP Notify

☐ SIP Info

☐ RFC 2833 Relay & SIP Info

☐ Inband

Finish

Repeat the process to define Server Interworking for Session Manager. In the **Advanced** tab, leave the settings at the original values cloned from the avaya-ru profile. **Record Routes** is set to **Both Sides** as Session Manager uses the Record-Route header and **Avaya** is selected in the **Extensions** drop down menu:

**Interworking Profiles: Session\_Manager**

Buttons: Add, Rename, Clone, Delete

Interworking Profiles: cs2100, avaya-ru, SIP\_Trunk, **Session\_Mana...**

Click here to add a description.

Tabs: General, Timers, Privacy, URI Manipulation, Header Manipulation, **Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No

**DTMF**

DTMF Support	None
--------------	------

Edit

## 7.6. Define Servers

A server definition is required for each server connected to the Avaya SBCE. The NOS SIP Trunking Service has two separate interfaces for routing via the primary and backup network SBC's. Each of these is connected as a separate Trunk Server. Session Manager has a single signalling interface and is connected as a Call Server.

To define the NOS SIP Trunk Server for the primary network SBC, navigate to **Global Profiles** → **Server Configuration** in the main menu on the left-hand side. Click on **Add**.

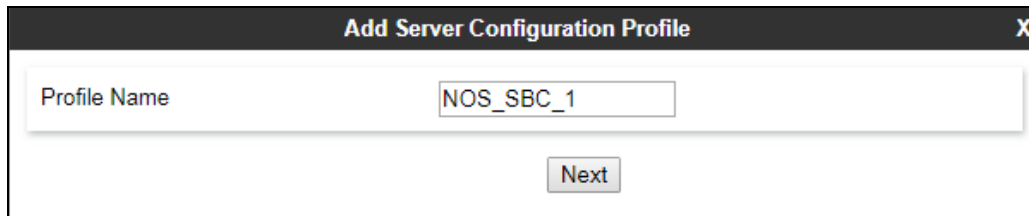
**Server Configuration**

Buttons: Add

Server Profiles: No entries found.

Use the add button to create a new Server Configuration profile.

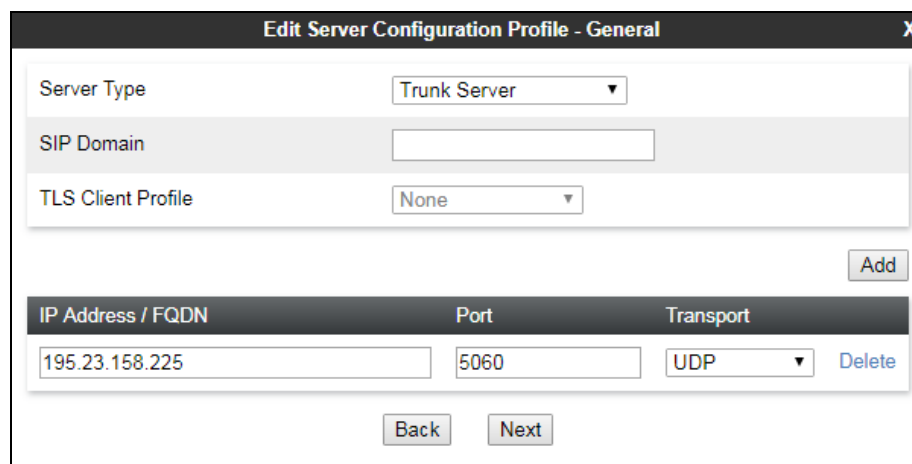
Enter an appropriate name in the pop-up menu.



The dialog box titled "Add Server Configuration Profile" has a close button (X) in the top right corner. It contains a text input field labeled "Profile Name" with the value "NOS\_SBC\_1" entered. Below the input field is a "Next" button.

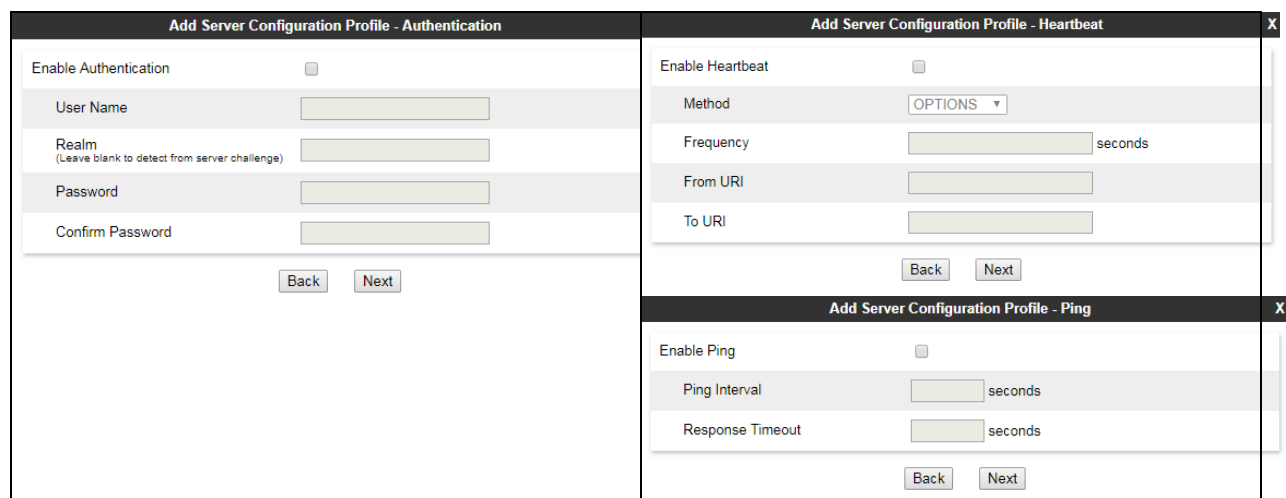
Click on **Next** and enter details in the dialogue box.

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



The dialog box titled "Edit Server Configuration Profile - General" has a close button (X) in the top right corner. It contains several fields: "Server Type" (Trunk Server), "SIP Domain" (empty), and "TLS Client Profile" (None). There is an "Add" button to the right of these fields. Below these is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "195.23.158.225", "5060", and "UDP". There is a "Delete" button to the right of the table. At the bottom are "Back" and "Next" buttons.

Click on **Next** three times for the Authentication, Heartbeat and Ping dialogue boxes:



The image shows three stacked dialog boxes. The first is "Add Server Configuration Profile - Authentication" with fields for "Enable Authentication", "User Name", "Realm", "Password", and "Confirm Password", and "Back" and "Next" buttons. The second is "Add Server Configuration Profile - Heartbeat" with fields for "Enable Heartbeat", "Method", "Frequency", "From URI", and "To URI", and "Back" and "Next" buttons. The third is "Add Server Configuration Profile - Ping" with fields for "Enable Ping", "Ping Interval", and "Response Timeout", and "Back" and "Next" buttons.

In the test environment, the Authentication, Heartbeat and Ping dialogue boxes were left at default values. Click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for the NOS SIP Trunking Service defined in **Section 7.5**.
- Leave the other fields at default settings.
- Click **Finish**.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The dialog contains several configuration options, each with a label and a control element:

- Enable DoS Protection**: A checkbox that is currently unchecked.
- Enable Grooming**: A checkbox that is currently unchecked.
- Interworking Profile**: A dropdown menu with "SIP\_Trunk" selected.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- Securable**: A checkbox that is currently unchecked.
- Enable FGDN**: A checkbox that is currently unchecked.
- TCP Failover Port**: A text input field containing the value "5060".
- TLS Failover Port**: A text input field containing the value "5061".
- Tolerant**: A checkbox that is currently unchecked.
- URI Group**: A dropdown menu with "None" selected.

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

To define the NOS SIP Trunk Server for the backup network SBC, return to **Global Profiles** → **Server Configuration** in the main menu on the left-hand side (not shown). Click on **Add**. Enter an appropriate name in the pop-up menu.

The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. The dialog contains a single text input field labeled "Profile Name" with the value "NOS\_SBC\_2" entered. Below the input field is a "Next" button.



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

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

The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. It has a title bar with 'Edit Server Configuration Profile - General' and a close button 'X'. The main area contains several fields: 'Server Type' with a dropdown menu set to 'Trunk Server', 'SIP Domain' with an empty text box, and 'TLS Client Profile' with a dropdown menu set to 'None'. Below these fields is an 'Add' button. At the bottom, there is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '192.23.159.192', '5060', and 'UDP' respectively, with a 'Delete' button to the right of the 'Transport' dropdown. Below the table are 'Back' and 'Next' buttons.

IP Address / FQDN	Port	Transport
192.23.159.192	5060	UDP

Click on **Next** three times for the Authentication, Heartbeat and Ping dialogue boxes (not shown) and click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings which are the same as those for the primary network SBC:

The screenshot shows the 'Add Server Configuration Profile - Advanced' dialog box. It has a title bar with 'Add Server Configuration Profile - Advanced' and a close button 'X'. The main area contains several settings: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown menu set to 'SIP\_Trunk'), 'Signaling Manipulation Script' (dropdown menu set to 'None'), 'Securable' (checkbox), 'Enable FGDN' (checkbox), 'TCP Failover Port' (text box with '5060'), 'TLS Failover Port' (text box with '5061'), 'Tolerant' (checkbox), and 'URI Group' (dropdown menu set to 'None'). At the bottom are 'Back' and 'Finish' buttons.

Use the process above to define the Call Server configuration for Session Manager if not already defined.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box.
- If TLS is used between the Avaya SBCE and Session manager, ensure that the TLS client profile created in **Section 7.3** is selected in the **TLS Client Profile** drop down menu in the **General** dialogue box.
- Ensure that the Interworking Profile defined for Session Manager in **Section 7.5** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box.

The following screenshot shows the **General** tab of the completed Server Configuration:

**Server Configuration: Avaya\_SM**

Add Rename Clone Delete

**Server Profiles**

- NOS\_SBC\_1
- NOS\_SBC\_2
- Avaya\_SM**

**General** **Authentication** **Heartbeat** **Ping** **Advanced**

Server Type: Call Server

TLS Client Profile: ASBCE45\_Client

IP Address / FQDN	Port	Transport
10.10.9.31	5061	TLS

Edit

**Note:** The IP Address matches the SIP Entity for Session Manager described in **Section 6.5** and the Port and Transport matches the Entity Link described in **Section 6.6**. The next screenshot shows the **Advanced** tab.

**Server Configuration: Avaya\_SM**

Add Rename Clone Delete

**Server Profiles**

- NOS\_SBC\_1
- NOS\_SBC\_2
- Avaya\_SM**

**General** **Authentication** **Heartbeat** **Ping** **Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile: Session\_Manager

Signaling Manipulation Script: None

Securable ☐

Enable FGDN ☐

Tolerant ☐

URI Group: None

Edit

## 7.7. Define Routing

Routing information is required for routing to the NOS off-net PSTN and on-net mobile services on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling. To define routing to the NOS off-net PSTN service, navigate to **Global Profiles** → **Routing** in the main menu on the left-hand side. Click on **Add**.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	DNS/SRV	Auto-Detect	Auto-Detect

Enter an appropriate name in the dialogue box.

Profile Name: Primary\_SBC

Next

Click on **Next** and enter details for the Routing Profile for the off-net PSTN trunk:

- During testing, **Load Balancing** was left at the default value of **Priority**.
- Click on **Add** to specify an IP address for the primary network SBC.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration defined in **Section 7.6** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	NOS_SBC_1	195.23.158.225:5060 (UDP)	None

Click **Finish** and repeat the above process for the Routing Profile for the backup network SBC. return to **Global Profiles → Routing** in the main menu on the left-hand side. Click on **Add** (not shown). Enter an appropriate name in the dialogue box (not shown), in the test environment, **Alternative\_SBC** was used. Click on **Next** and enter details:

The screenshot shows the 'Routing Profile' dialog box. The 'URI Group' is set to '\*' and 'Time of Day' is 'default'. 'Load Balancing' is 'Priority', 'NAPTR' is unchecked, 'Transport' is 'None', 'Next Hop Priority' is checked, 'Next Hop In-Dialog' is unchecked, 'Ignore Route Header' is unchecked, 'ENUM' is unchecked, and 'ENUM Suffix' is empty. An 'Add' button is visible. Below, a table shows the configuration for a single entry:

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	NOS_SBC_2	195.23.159.192:5060 (UDP)	None

'Delete' and 'Finish' buttons are at the bottom.

Repeat the process for the Routing Profile for Session Manager: return to **Global Profiles → Routing** in the main menu on the left-hand side. Click on **Add** (not shown). Enter an appropriate name in the dialogue box:

The screenshot shows the 'Routing Profile' dialog box with 'Profile Name' set to 'Avaya\_SM'. A 'Next' button is at the bottom.

Click on **Next** and enter details for the Routing Profile for the Session Manager:

The screenshot shows the 'Routing Profile' dialog box with the same settings as the first SBC profile. The table below shows the configuration for a single entry:

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Avaya_SM	10.10.9.31:5061 (TLS)	None

'Delete' and 'Finish' buttons are at the bottom.

## 7.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop for termination information and the external interfaces for origination information.

To define Topology Hiding for NOS SIP Trunking, navigate to **Global Profiles → Topology Hiding** in the main menu on the left-hand side. Select the default profile and click on **Clone**.

Dashboard  
Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
  Domain DoS  
  Server Interworking  
  Media Forking  
  Routing  
  Server Configuration  
  **Topology Hiding**  
  Signaling Manipulation  
  URI Groups  
  SNMP Traps  
  Time of Day Rules  
  FGDN Groups  
  Reverse Proxy Policy

Topology Hiding Profiles: default

Add Clone

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Topology Hiding

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

Edit

Assign an appropriate name in the dialogue box and click on **Finish**:

Clone Profile X

Profile Name default

Clone Name NOS

Finish

Highlight the new Topology Hiding profile (not shown) and click on **Edit**. Make changes if required.

During testing, fields were left at default values. If changes are required:

- Select **Header** to modify. If header is not already specified, click on **Add Header** and select from the drop-down menu.

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	

- Select **IP** or **IP/Domain** from the **Criteria** drop down menu. The default setting **IP/Domain** hides both domain names and IP addresses.
- Default action **Auto** in the **Replace Action** drop down menu replaces internal IP addresses or domain names with external IP addresses.
- If **Overwrite** is selected as the action, define the required domain name in the **Overwrite Value** field. This was not used during testing.
- Click on **Finish**.

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

To define Topology Hiding for Session Manager, follow the same process. During testing, the default profile was used so an additional profile was not required.

## 7.9. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.10**. NOS SIP Trunking was tested with a signalling rule to remove the Route header present in the SIP INVITE for incoming calls. This did not contain a valid IP address and caused a routing issue on the Avaya SBCE. In addition, a media rule was used to convert the encrypted media used within the enterprise to unencrypted media on the SIP Trunk.

### 7.9.1. Signalling Rules

Signalling rules are used to handle any non-standard signalling that may be encountered on a SIP Trunk, in this case the inclusion of the Route header in incoming SIP INVITE messages.

To define the signalling rule, navigate to **Domain Policies → Signaling Rules** in the main menu on the left-hand side. Highlight the default signalling rule and click on **Clone**.

The screenshot shows the 'Signaling Rules: default' configuration page. On the left is a navigation menu with 'Domain Policies' expanded, showing 'Signaling Rules' as the selected option. The main area has a 'default' rule selected in a list. A 'Clone' button is visible in the top right. Below the rule list, there's a warning banner: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The configuration tabs include 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'General' tab is active, showing 'UCID' as the rule type. The configuration is divided into 'Inbound' and 'Outbound' sections, each with a table of actions and their status (all set to 'Allow'). The 'Content-Type Policy' section has a checkbox for 'Enable Content-Type Checks' which is checked, and an 'Exception List' field. An 'Edit' button is at the bottom right.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks <input checked="" type="checkbox"/>			
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Enter a **Rule Name** in the **Clone Rule** dialogue box and click on **Finish**.

The 'Clone Rule' dialog box is shown. It has a title bar with 'Clone Rule' and a close button 'X'. Inside, there are two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'SIP\_Trunk'. At the bottom is a 'Finish' button.

To remove the Route header, highlight the recently created Signalling Rule click on the **Request Headers** tab and click on **Add In Header Control** (not shown).

- Select **Route** in the **Header Name** field drop-down menu.
- Leave **Method Name** at the default value of **ALL**.
- Check the **Forbidden** radio button in the **Header Criteria** field.
- Leave the **Presence Action** at the default value of **Remove Header**.
- Click on **Finish**.

The following screenshot shows the applied Request Header removal:

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	Route	ALL	Forbidden	Remove Header	No	IN

## 7.9.2. Media Rules

Media rules are used to handle media attributes where differences may exist between the enterprise and SIP Trunk. In the test environment, a media rule was used to handle the conversion between encrypted media on the enterprise side and unencrypted media on the SIP Trunk.



To define the media rule, navigate to **Domain Policies** → **Media Rules** in the main menu on the left-hand side. Highlight an appropriate default signalling rule and click on **Clone**. In the test environment, a media rule with encryption was cloned.

**Media Rules: avaya-low-med-enc**

Add Filter By Device... Clone

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

**Encryption** Codec Prioritization Advanced QoS

**Audio Encryption**

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

**Video Encryption**

Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>

**Miscellaneous**

Capability Negotiation	<input type="checkbox"/>
------------------------	--------------------------

Edit

Enter a **Rule Name** in the **Clone Rule** dialogue box and click on **Finish**.

**Clone Rule** X

Rule Name avaya-low-med-enc

Clone Name ASM-low-med-enc

Finish

To define media encryption, highlight the recently created Media Rule click on the **Encryption** tab and click on **Edit**. Configure as required, in the test environment the following settings were used:

- Select **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80** in the **Preferred Format #1** field drop-down menu.
- Select **RTP** in the **Preferred Format #2** field drop-down menu to allow fallback to unencrypted media.
- Leave **Capability Negotiation** unchecked.
- Click on **Finish**.

The screenshot shows a 'Media Encryption' configuration window with three main sections: Audio Encryption, Video Encryption, and Miscellaneous. Each section contains several settings with checkboxes and dropdown menus.

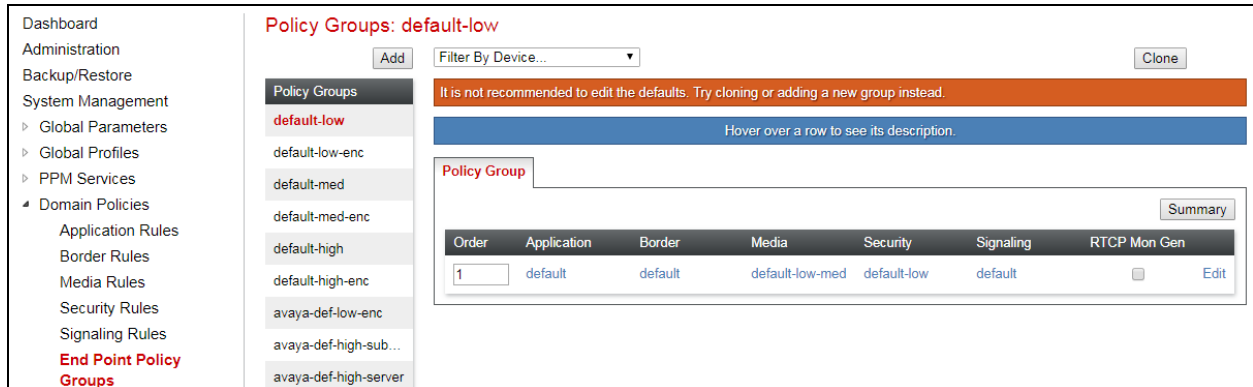
Section	Setting	Value
Audio Encryption	Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
	Preferred Format #2	RTP
	Preferred Format #3	NONE
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	2^ <input type="text"/>
	Interworking	<input checked="" type="checkbox"/>
Video Encryption	Preferred Format #1	RTP
	Preferred Format #2	NONE
	Preferred Format #3	NONE
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	2^ <input type="text"/>
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Capability Negotiation	<input type="checkbox"/>

At the bottom of the window is a 'Finish' button.

### 7.9.3. External End Point Policy Group

An End Point Policy Group is required for use on the external side of the Avaya SBCE to implement the previously defined signalling rule.

To define an End Point Policy Group for use in the NOS network SBC server flows, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Select an appropriate pre-defined Policy Group, in the test environment this was **default-low**, and click on **Clone**.



Enter an appropriate name in the pop-up box.

**Clone Group** X

Group Name: default-low

Clone Name:

Highlight the resulting Policy Group and click on **Edit**. Enter details as follows:

- Leave the **Application Rule**, **Border Rule**, **Media Rule** and **Security Rule** at their default values.
- Select the **Signaling Rule** created **Section 7.9.1** in the drop-down menu.
- Click on **Finish**.

**Edit Policy Set** X

Application Rule:

Border Rule:

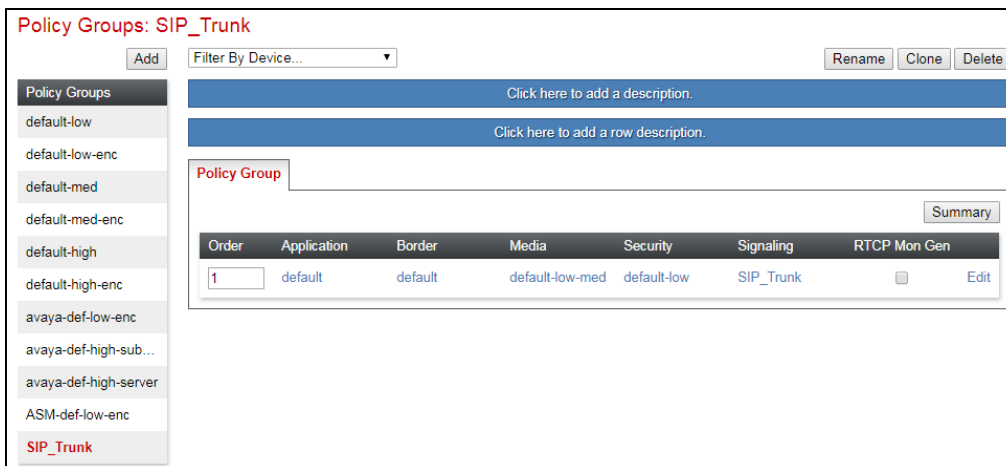
Media Rule:

Security Rule:

Signaling Rule:

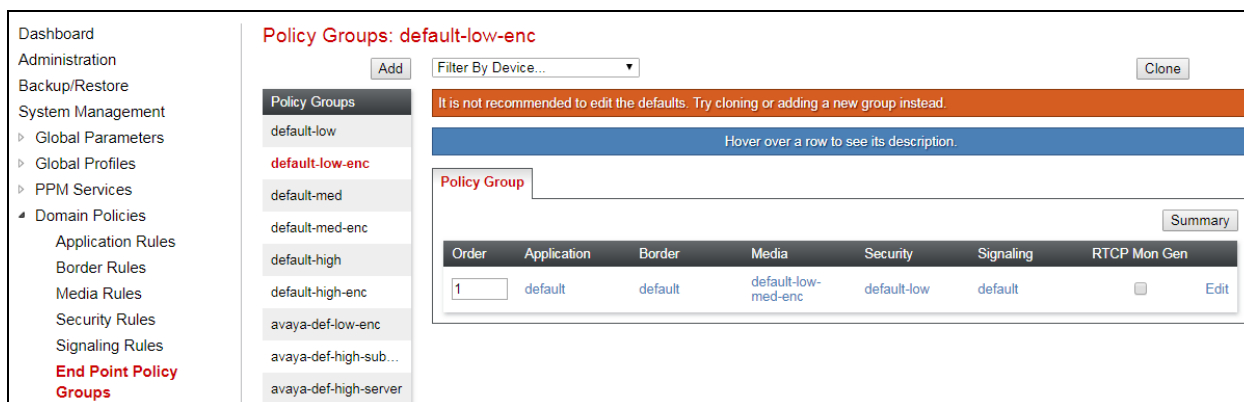
RTCP Monitoring Report Generation: ☐ Enabled

The following screenshot shows the completed configuration:

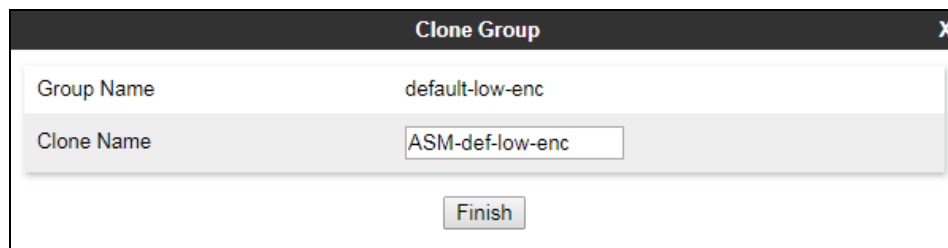


#### 7.9.4. Internal End Point Policy Group

An End Point Policy Group is required for use on the internal side of the Avaya SBCE to implement the previously defined media rule. To define an End Point Policy Group for use in the enterprise server flows, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Select an appropriate pre-defined Policy Group, in the test environment this was **default-low-enc**, and click on **Clone**.



Enter an appropriate name in the pop-up box.



Highlight the resulting Policy Group and click on **Edit**. Enter details as follows:

- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signaling Rule** at their default values.
- Select the **Media Rule** created in **Section 7.9.2** in the drop-down menu.
- Click on **Finish**.

Edit Policy Set	
Application Rule	default
Border Rule	default
Media Rule	ASM-low-med-enc
Security Rule	default-low
Signaling Rule	default
RTCP Monitoring Report Generation	<input checked="" type="checkbox"/> Enabled
Finish	

The following screenshot shows the completed configuration:

**Policy Groups: ASM-def-low-enc**

Add Filter By Device... Rename Clone Delete

Click here to add a description.

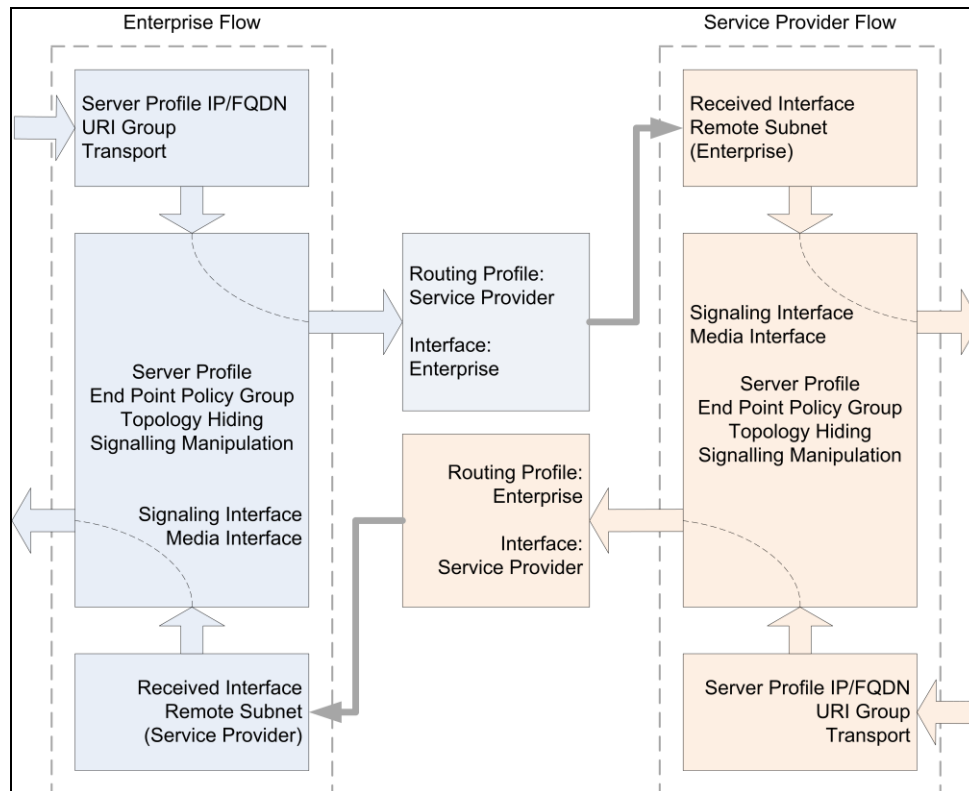
Hover over a row to see its description.

**Policy Group** Summary

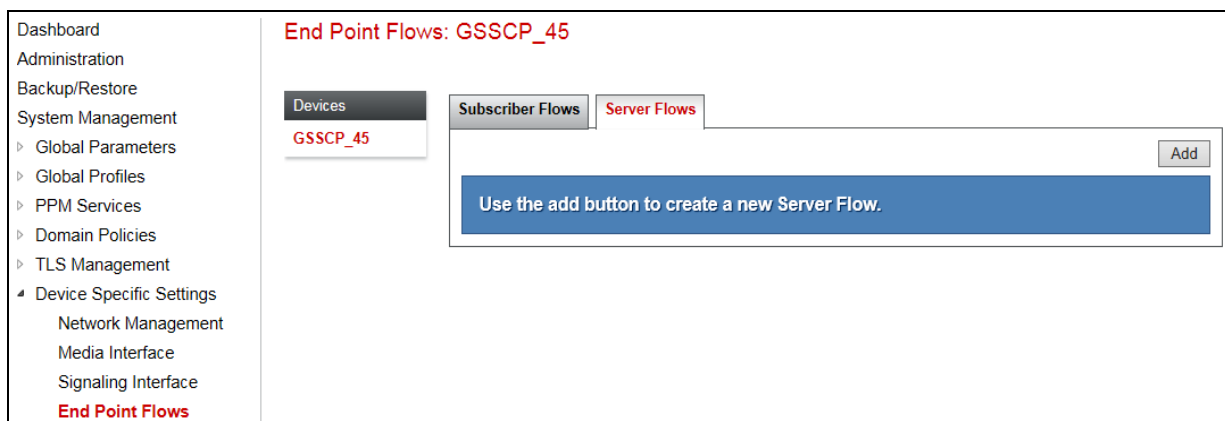
Order	Application	Border	Media	Security	Signaling	RTCP Mon Gen	
1	default	default	ASM-low-med-enc	default-low	default	<input type="checkbox"/>	Edit

## 7.10. Server Flows

Server Flows combine the previously defined profiles into End Point Server Flows. The following diagram shows the inputs and outputs of the server flows:



Four End Point Server Flows are defined for the NOS SIP Trunking Service, one for primary network SBC, one for the backup network SBC and two for Session Manager. These End Point Server Flows allow calls to be routed from Session Manager to the NOS SIP Trunks and vice versa. To define a Server Flow for the NOS primary network SBC, navigate to **Device Specific Settings → End Point Flows**. Click on the **Server Flows** tab and click on **Add**.



Enter details in the pop-up menu.

- In the **Flow Name** field enter a descriptive name for the server flow for the NOS primary network SBC, in the test environment **Primary\_SBC** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the primary network SBC defined in **Section 7.6**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4**. This is the interface that signalling bound for the primary network SBC is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4**. This is the interface that signalling bound for the primary network SBC is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4**. This is the interface that outbound media is sent on.
- In the **End Point Policy Group** drop-down menu, select the external End Point Policy Group defined in **Section 7.9.3**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the NOS SIP Trunking Service defined in **Section 7.8** and click **Finish**.

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

Field Label	Value
Flow Name	Primary_SBC
Server Configuration	NOS_SBC_1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal_Primary
Signaling Interface	External
Media Interface	External
Secondary Media Interface	None
End Point Policy Group	SIP_Trunk
Routing Profile	Avaya_SM
Topology Hiding Profile	NOS
Signaling Manipulation Script	None
Remote Branch Office	Any

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

To define a Server Flow for the NOS backup network SBC, return to **Device Specific Settings** → **End Point Flows** and click on the **Server Flows** tab.

- Select **Add** and enter details in the pop-up menu
- In the **Flow Name** field enter a descriptive name for the server flow for the NOS backup network SBC, in the test environment **Alternative\_SBC** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the backup network SBC defined in **Section 7.6**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4**. This is the interface that signalling bound for the backup network SBC is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4**. This is the interface that signalling bound for the backup network SBC is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4**. This is the interface that outbound media is sent on.
- In the **End Point Policy Group** drop-down menu, select the external End Point Policy Group defined in **Section 7.9.3**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the NOS SIP Trunking Service defined in **Section 7.8** and click **Finish**.

The screenshot shows a 'Add Flow' dialog box with the following configuration:

Field	Value
Flow Name	Alternative_SBC
Server Configuration	NOS_SBC_2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal_Backup
Signaling Interface	External
Media Interface	External
Secondary Media Interface	None
End Point Policy Group	SIP_Trunk
Routing Profile	Avaya_SM
Topology Hiding Profile	NOS
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish



To define a Server Flow for Session Manager for traffic to and from the primary network SBC, return to **Device Specific Settings → End Point Flows** and click on the **Server Flows** tab.

- Select **Add** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Avaya\_SM\_(Primary)** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.6**.
- In the **Remote Subnet** field, enter the IP address of the primary network SBC as /.32
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4**. This is the primary interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.4**. This is the interface that inbound media is sent on.
- In the **End Point Policy Group** drop-down menu, select the internal End Point Policy Group defined in **Section 7.9.4**.
- In the **Routing Profile** drop-down menu, select the routing profile of the primary network SBC defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish**.

The screenshot shows a dialog box titled "Add Flow" with a close button (X) in the top right corner. The dialog contains the following fields and values:

Field	Value
Flow Name	Avaya_SM_(Primary)
Server Configuration	Avaya_SM
URI Group	*
Transport	*
Remote Subnet	195.23.158.225/32
Received Interface	External
Signaling Interface	Internal_Primary
Media Interface	Internal
Secondary Media Interface	None
End Point Policy Group	ASM-def-low-enc
Routing Profile	Primary_SBC
Topology Hiding Profile	Session_Manager
Signaling Manipulation Script	None
Remote Branch Office	Any

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

To define a Server Flow for Session Manager for traffic to and from the backup network SBC, return to **Device Specific Settings → End Point Flows** and click on the **Server Flows** tab.

- Select **Add** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Avaya\_SM\_(Alternative)** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.6**.
- In the **Remote Subnet** field, enter the IP address of the backup network SBC as **/32**
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4**. This is the backup interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.4**. This is the interface that inbound media is sent on.
- In the **End Point Policy Group** drop-down menu, select the internal End Point Policy Group defined in **Section 7.9.4**.
- In the **Routing Profile** drop-down menu, select the routing profile of the backup network SBC defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish**.

The screenshot shows a dialog box titled "Add Flow" with a close button (X) in the top right corner. The dialog contains several fields and dropdown menus for configuring a server flow. The fields are as follows:

Field	Value
Flow Name	Avaya_SM_(Alternative)
Server Configuration	Avaya_SM
URI Group	*
Transport	*
Remote Subnet	195.23.159.192/32
Received Interface	External
Signaling Interface	Internal_Backup
Media Interface	Internal
Secondary Media Interface	None
End Point Policy Group	ASM-def-low-enc
Routing Profile	Alternative_SBC
Topology Hiding Profile	Session_Manager
Signaling Manipulation Script	None
Remote Branch Office	Any

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

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

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: Avaya\_SM

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya_SM_(Primary)	*	External	Internal_Primary	ASM-def-low-enc	Primary_SBC	View Clone Edit Delete
2	Avaya_SM_(Alternative)	*	External	Internal_Backup	ASM-def-low-enc	Alternative_SBC	View Clone Edit Delete

Server Configuration: NOS\_SBC\_1

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Primary_SBC	*	Internal_Primary	External	SIP_Trunk	Avaya_SM	View Clone Edit Delete

Server Configuration: NOS\_SBC\_2

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Alternative_SBC	*	Internal_Backup	External	SIP_Trunk	Avaya_SM	View Clone Edit Delete

## 8. Configure the NOS SIP Trunking Service Equipment

The configuration of the NOS Comunicações equipment used to support the SIP Trunk is outside the scope of these Application Notes and will not be covered. To obtain further information on NOS equipment and system configuration please contact an authorised NOS 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 Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

The screenshot shows the 'Session Manager Entity Link Connection Status' page. The left sidebar contains a navigation menu with options like Dashboard, Session Manager, Administration, Global Settings, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. The main content area shows a table titled 'All Entity Links for Session Manager: Session\_Manager'. The table has columns for SIP Entity Name, IP Address Family, SIP Entity Resolved IP, Port, Proto, Deny, Conn. Status, Reason Code, and Link Status. There are 5 items listed, all with a Link Status of 'UP'.

SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM SIP Endpoints	IPv4	10.10.9.12	5063	TLS	FALSE	UP	200 OK	UP
ASBCE_2	IPv4	10.10.9.82	5061	TLS	FALSE	UP	502 Bad DNS Request 02035190E	UP
CM Trunk	IPv4	10.10.9.12	5061	TLS	FALSE	UP	200 OK	UP
Messaging	IPv4	10.10.2.90	5060	TCP	FALSE	UP	200 OK	UP
ASBCE_1	IPv4	10.10.9.81	5061	TLS	FALSE	UP	502 Bad DNS Request 02035190E	UP

2. 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 2
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00011	in-service/idle	no
0002/002	T00012	in-service/idle	no
0002/003	T00013	in-service/idle	no
0002/004	T00014	in-service/idle	no
0002/005	T00015	in-service/idle	no
0002/006	T00016	in-service/idle	no

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left-hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address from the **Local Address** drop down menu or select **ALL**.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a \* to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, **1000** is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

**Trace: GSSCP\_45**

**Devices**  
GSSCP\_45

**Packet Capture** **Captures**

**Packet Capture Configuration**

Status	Ready
Interface	B1
Local Address IP[:Port]	All
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename Using the name of an existing capture will overwrite it.	SIP_Trunk_Test.pcap

**Start Capture** **Clear**

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

Trace: GSSCP\_45

Devices

GSSCP\_45

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20180508134341.pcap	0	May 8, 2018 1:49:07 PM IST	Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response to OPTIONS in the form of a 200 OK will be seen from the NOS network.

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.1, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to the NOS SIP Trunking Service. The NOS SIP Trunking Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

## 11. Additional References

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

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.1, May 2017.
- [2] *Upgrading and Migrating Avaya Aura® applications to Release 7.1.1 from System Manager*, Aug 2017.
- [3] *Deploying Avaya Aura® applications from System Manager*, Release 7.1.1, Aug 2017
- [4] *Deploying Avaya Aura® Communication Manager*, Release 7.1.1, Aug 2017
- [5] *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Aug 2017.
- [6] *Upgrading Avaya Aura® Communication Manager*, Release 7.1.1, Aug 2017
- [7] *Deploying Avaya Aura® System Manager Release 7.1.1*, Aug 2017
- [8] *Upgrading Avaya Aura® System Manager to Release 7.1.1*, Aug 2017.
- [9] *Administering Avaya Aura® System Manager for Release 7.1.1*, Aug 2017
- [10] *Deploying Avaya Aura® Session Manager*, Release 7.1 May 2017
- [11] *Upgrading Avaya Aura® Session Manager Release 7.1.1*, Aug 2017
- [12] *Administering Avaya Aura® Session Manager Release 7.1.1*, Aug 2017,
- [13] *Deploying Avaya Session Border Controller for Enterprise Release 7.2*, Sep 2017
- [14] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2*, Aug 2017
- [15] *Administering Avaya Session Border Controller for Enterprise Release 7.2*, Sep 2017
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

## 12. Appendix A – Linux L2TP Settings

A Linux server was used to establish the L2TP tunnel with the following configuration:

Add the following to the /etc/xl2tpd/xl2tpd.conf file:

```
[global]
listen-addr = <local public IP address>
auth file = /etc/xl2tpd/l2tp-secrets

[lac nosvpn]
lns = <remote public IP address>
hostname = <L2TP host name assigned by NOS>
pppoptfile = /etc/ppp/options.xl2tpd.client
```

Add L2TP password to /etc/xl2tpd/l2tp-secrets file

Add the following to the /etc/ppp/options.xl2tpd.client file:

```
noccp
idle 1800
mtu 1410
mru 1410
nodefaultroute
debug
connect-delay 5000
name <PPP username assigned by NOS>
```

Add PPP password to /etc/ppp/chap-secrets file



---

**©2018 Avaya Inc. All Rights Reserved.**

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

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