



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise R7.0 to support Motto VoIP SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Motto VoIP SIP Trunk 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.

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.

Motto 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 Motto VoIP SIP Trunk and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R7.0 (Communication Manager); Avaya Aura® Session Manager R7.0 (Session Manager) and Avaya Session Border Controller for Enterprise R7.0 (Avaya SBCE); Endpoints as described in **Section 3**. 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 Motto VoIP SIP Trunk are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using Motto SIP Trunk, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via Motto SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones.
- Inbound and outbound PSTN calls to/from an Avaya one-X® Communicator and Avaya Communicator for Windows soft phones.
- Calls using the G.711A, G.711MU Law and G.729A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using G.711.
- 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 Motto SIP Trunk requiring Avaya response and sent by Avaya requiring Motto response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Motto VoIP SIP Trunk with the following observations:

- The recommended method of connecting to the Motto VoIP SIP Trunk is via DNS SRV. This is not yet fully supported on the Avaya SBCE so simple DNS was used.
- OPTIONS were not used by Motto VoIP to check the status of the SIP Trunk
- Occasional delays in signalling were observed during testing resulting in re-transmission of SIP messages. This was due to network issues that have since been resolved.
- When forwarding to a PSTN phone, there was no CLI presented on the PSTN phone. The original CLI was sent in the From header and the DDI of the Communication Manager extension was sent in the Diversion header.
- Although T.38 media attributes were sent in the SDP from the network when negotiating Fax, T.38 fax transmission did not function and Motto advised that it is not supported. G.711 fax transmission failed at first, but was successful after a configuration change in the Motto VoIP network.
- When making an EC500 call, there was no CLI presented on the mobile phone.
- When making an outbound call to a PSTN phone when connected via SIP and in “Other Phone” mode, no ringback is heard on the one-X Communicator soft phone. Ringback is heard when connected via H.323.
- When the SIP Trunk is busy and an incoming call is attempted, the Avaya equipment sends 503 Service Unavailable. The network repeatedly re-attempts the call set-up for a period of around 90 seconds before a tone is played.
- When the signalling link has failed and an incoming call is attempted, the Avaya equipment sends 408 Request Timeout then 503 Service Unavailable. The network repeatedly re-attempts the call set-up for a period of around 90 seconds before a tone is played.

Items not tested include the following:

- No Inbound Toll-Free access available for testing
- No test call was made to Emergency Services as a test call was not booked with the Emergency Services Operator.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on Motto VoIP products, please contact the Motto VoIP support team:

- E-mail: support@motto.nl
- Phone: +31 454040490
- Web: <http://www.motto.nl>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Motto VoIP SIP Trunk. 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 Communicator for Windows running on laptop PCs.

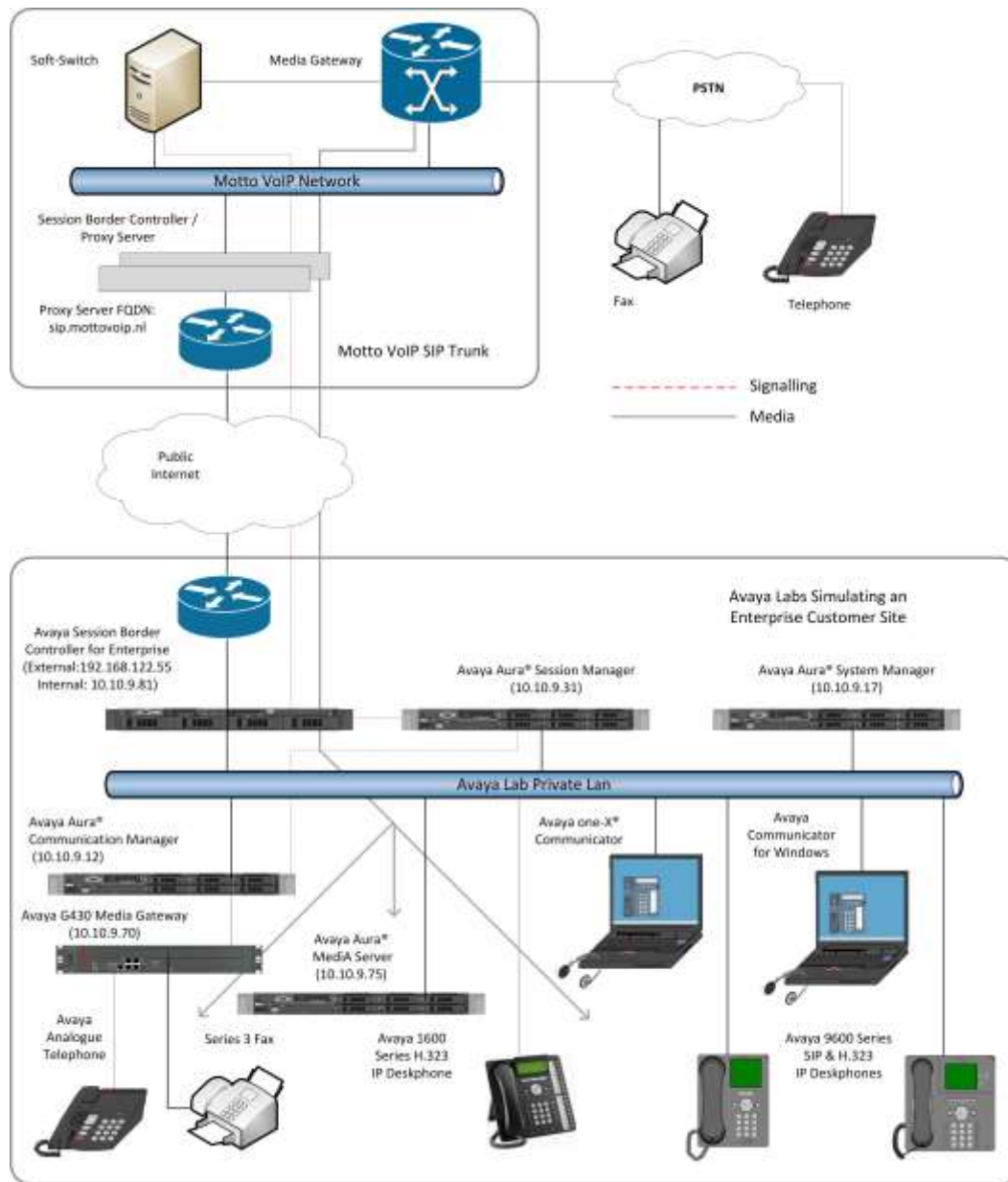


Figure 1: Test Setup Motto VoIP SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.1.0.701007
Avaya Aura® System Manager	7.0.1.0.064859 – SP1
Avaya Aura® Communication Manager	7.0.1.0.0-23012 – FP1
Avaya Session Border Controller for Enterprise	7.0.1-03-8739
Avaya Media Server	7.7.0.334
Avaya G430 Media Gateway	37.38.0
Avaya 9600 series Handsets	
SIP 96x0	2.6.16
SIP 9608	7.0.1 R46
H.323 96x0	3.2.6A
H.323 9608	6.2.29
H.323 1616	1.3.9
Avaya One-X Communicator	6.2.11.03 – SP11
Avaya Communicator for Windows	2.1.3.80
Analogue Handset	N/A
Analogue Fax	N/A
Motto	
OpenSIPS	2.1.3
Asterisk	11.14.0-motto3

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 Motto VoIP SIP Trunk. 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 Motto 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 Motto VoIP SIP Trunk 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		
Maximum Administered SIP Trunks:			4000	20		
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? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? 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 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		Page 1 of 2
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 direct media is used on a PSTN call, 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
                IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5    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. In the configuration of the G430 and Avaya Media Server (not shown) ip-network-region 1 was used in such a way that either one could be selected at call set-up.

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

change ip-codec-set 2				Page 1 of 2
IP CODEC SET				
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	

Note: Wideband codec G.722 is also supported but only for on-net calls. These were not tested during SIP compliance testing.

Motto SIP Trunk supports G.711 for transmission of fax. As this is in-band and requires no interaction from Communication Manager, there is no specific configuration required. Navigate to **Page 2** and set the **FAX - Mode** to **off**.

change ip-codec-set 2				Page 2 of 2
IP CODEC SET				
Allow Direct-IP Multimedia? n				
	Mode	Redundancy	Packet Size (ms)	
FAX	off	0		
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0	20	

Note: Transmission of fax is only supported where G.711 is the codec negotiated at call set-up.

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Motto VoIP SIP Trunk. During test, this was configured to use TCP and port 5062 though it's recommended to use TLS and port 5061 in the live environment to enhance security. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tcp**.
- 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 TCP is **5060**, though **5062** was used in test to separate the SIP Trunk from the SIP endpoints on Session Manager (See **Section 6.5**).
- 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 (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **Direct IP-IP Audio Connections** to **y** to avoid unnecessary use of MGW resources
- Set **Initial IP-IP Direct Media** to **n** to facilitate the use of Early Media.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).

The default values for the other fields may be used.

change signaling-group 2		Page 1 of 2	
SIGNALING GROUP			
Group Number: 2	Group Type: sip		
IMS Enabled? n	Transport Method: tcp		
Q-SIP? n			
IP Video? n	Enforce SIPS URI for SRTP? y		
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: 5062	Far-end Listen Port: 5062		
	Far-end Network Region: 2		
Far-end Domain:			
	Bypass If IP Threshold Exceeded? n		
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n		
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y		
Session Establishment Timer(min): 3	IP Audio Hairpinning? n		
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n		
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6		

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group 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 signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**.
- Specify the **Number of Members** supported by this SIP trunk group.

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: SIP_Trunk	COR: 1	TN: 1	TAC: 102
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
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 Motto to prevent unnecessary SIP messages during call setup. During testing, a value of **900** was used that sets Min-SE to 1800 in the SIP signalling.

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

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in E.164 format without a leading “+” as required by Motto.

add trunk-group 2		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private	
	UII Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y**.
- Set **Send Transferring Party Information** to **y** to ensure that the transferring party number is sent. This information is used by the Motto VoIP network for call transfer.
- Set **Network Call Redirection** to **y** to allow the use of REFER messages for call flows such as blind call transfer.
- Set **Support Request History** to **n** as this header is not supported by Motto.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Motto (this Payload Type is not applied to calls from SIP end-points).
- Set **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on Communication Manager extension.

add trunk-group 2		Page 4 of 21
PROTOCOL VARIATIONS		
	Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	Send Transferring Party Information? y	
	Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	Send Diversion Header? n	
	Support Request History? n	
	Telephone Event Payload Type: 101	
	Convert 180 to 183 for Early Media? n	
	Always Use re-INVITE for Display Updates? n	
	Identity for Calling Party Display: From	
Block Sending Calling Party Location in INVITE? n	Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? n	

Note: Testing was carried out with set **Network Call Redirection** to **y**, but this is only required if network call redirection is to be supported which wasn't the case during SIP compliance testing. It's shown here as it allows the use of SIP REFER messages as mentioned in the bullet points.

5.7. Administer Calling Party Number Information

Use the **change private-numbering** command to configure Communication Manager to send the calling party number in the format required. During testing, calling party numbers were sent as E.164 numbers without leading “+”. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	2	1		4	Total Administered: 8
4	2000	2	311028nnnn0	11	Maximum Entries: 540
4	2001	2	311028nnnn8	11	
4	2291	2	311028nnnn2	11	
4	2316	2	311028nnnn3	11	
4	2391	2	311028nnnn1	11	
4	2400	2	311028nnnn4	11	
4	2401	2	311028nnnn7	11	

Note: During testing the extension numbers were reformatted to E.164 numbers for Trunk Group 2 only. The numbers were analysed for Trunk Group 1 but not reformatted.

The public numbering table was similarly populated for completeness. This table can be used in cases where AAR and ARS analysis are not used. The main difference between the two tables is that the numbers in the public numbering table are prefixed with a “+”. To change the table, use the **change public-unknown-numbering** command.

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: 8
4	2000	2	311028nnnn0	11	Maximum Entries: 240
4	2001	2	311028nnnn8	11	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	2291	2	311028nnnn2	11	
4	2316	2	311028nnnn3	11	
4	2391	2	311028nnnn1	11	
4	2400	2	311028nnnn4	11	Communication Manager automatically inserts a '+' digit in this case.
4	2401	2	311028nnnn7	11	

Note: If SIP endpoints are registering as third party endpoints, i.e. not as AST devices, check the above tables for completeness.

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 Motto network. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. 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	
Auto Route Selection (ARS) - Access Code 1: 9 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 international numbers beginning 00 and national numbers beginning with 0. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 2**.

change ars analysis 0						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 0		
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
0	8	12	2	pubu		n	
00	13	15	2	pubu		n	
0035391	13	13	2	pubu		n	
1	3	4	2	pubu		n	
118	5	6	2	pubu		n	
3	4	4	2	pubu		n	
7000	4	4	1	pubu		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 **2** is used to route calls to trunk group **2**. **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 calls and during testing it was set to **unk-unk**.

change route-pattern 2										Page 1 of 3
Pattern Number: 2 Pattern Name: SIP_Endpoints										
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							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	unk-unk	none
2:	y	y	y	y	y	n	n	rest		none
3:	y	y	y	y	y	n	n	rest		none
4:	y	y	y	y	y	n	n	rest		none
5:	y	y	y	y	y	n	n	rest		none
6:	y	y	y	y	y	n	n	rest		none

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to Communication Manager extensions. The incoming digits sent in the INVITE message from Motto 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, 11 digits are received in E.164 format with no prefix. All digits are deleted and the extension number is inserted. 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/	Number	Number	Del		Insert					
Feature	Len	Digits								
public-ntwrk	11	311028nnnn0	11	2000						
public-ntwrk	11	311028nnnn1	11	2391						
public-ntwrk	11	311028nnnn2	11	2291						
public-ntwrk	11	311028nnnn3	11	2316						
public-ntwrk	11	311028nnnn4	11	2400						
public-ntwrk	11	311028nnnn5	11	7000						
public-ntwrk	11	311028nnnn6	11	6002						
public-ntwrk	11	311028nnnn7	11	2401						
public-ntwrk	11	311028nnnn8	11	2001						
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, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **003538941nnnn7**).
- 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	-		003538941nnnn7	ars	1	

Note: The phone number shown is for a mobile phone in the Avaya Lab. To use facilities such as Feature Name Extension (FNE) 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.

The additional line in the previous screenshot with **Application** of **OPS** is standard on SIP endpoints where the phone is registered to the Session Manager and is essentially “Off PBX”.

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

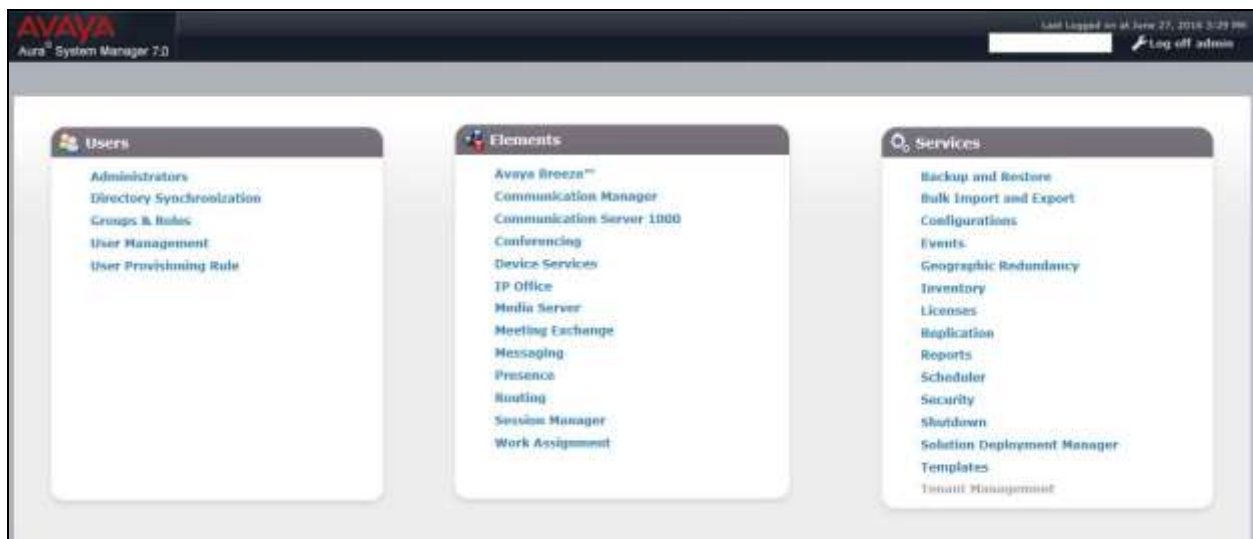
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured by opening a web browser to the 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 the System Manager using a web browser and enter **http://<FQDN>/SMGR**, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name of the enterprise site or a name agreed with Motto; 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 test, **avaya.com** was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click **Commit** to save changes.



Home / Elements / Routing / Domains

Domain Management

New Edit Delete Duplicate More Actions ▾

1 Item 

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

Select : All, None

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 of the enterprise SIP entities. 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. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.

The screenshot shows the 'Location Details' configuration page. At the top, there is a breadcrumb trail 'Home / Elements / Routing / Locations' and a 'Help ?' link. The page title is 'Location Details' with 'Commit' and 'Cancel' buttons. The 'General' section contains a 'Name' field with 'Galway' and a 'Notes' field. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox, a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field. The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth', 'Multimedia Bandwidth', and an 'Audio Calls Can Take Multimedia Bandwidth' checkbox. The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', '* Minimum Multimedia Bandwidth', and '* Default Audio Bandwidth'. The 'Alarm Threshold' section includes 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', '* Latency before Overall Alarm Trigger', and '* Latency before Multimedia Alarm Trigger'. The 'Location Pattern' section at the bottom has 'Add' and 'Remove' buttons, a table with one row containing '*10.10.9.x' under the 'IP Address Pattern' column, and a 'Select : All, None' option.

Home / Elements / Routing / Locations

Help ?

Location Details

Commit Cancel

General

* Name: Galway

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☐

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

1 Item

Filter: Enable

IP Address Pattern	Notes
*10.10.9.x	

Select : All, None

6.4. Administer Adaptations

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 are not recognized by the Motto network. In addition, the called and calling party number formats passed between the Enterprise and the Motto VoIP network are in E.164 format without any prefix. A Session Manager Adaptation is used both to remove proprietary headers and to convert numbers to and from diallable format.

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**. This is used for simple digit conversion adaptations.
- 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"**.
- Click on Add.
- In the **Name** box, type **fromto**.
- In the **Value** box, type **true**. This will apply the number conversion rules to the From and To headers in the SIP messages.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel Help ?

General

* Adaptation Name: Header_Removal

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, P-Conference"
fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Number analysis is used to apply the above Module Parameter rule and to convert the called and calling party numbers between E.164 and diallable format. Scroll down and in the section **Digit Conversion for Incoming Calls to SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of numbers coming from the network.

The screenshot below shows analysis of called and calling party numbers for incoming calls. The called party number is the DDI number associated with the Communication manager extensions.

- Under **Matching Pattern** enter the DDI number as received from the network.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number, in this case the DDI number length is fixed at **11**.
- Under **Delete Digits** enter 0 as the number is not to be modified.
- Leave the **Insert Digits** field blank as the number is not to be modified.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the called party number.

Digit Conversion for Incoming Calls to SM

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*311028nnnn	*11	*11		*0		destination		

Select : All, None

Note: In the above screenshot the DDI number is partially obscured. If the calling party number is to be modified for display on Communication Manager extensions in diallable format, it should be done here. For international numbers, prefix with 00. For national numbers, analyse country code 31 and replace with 0. **Address to modify** would be **origination**.

Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of numbers going out to the network

The screenshot below shows analysis of called party numbers for outgoing calls. The called party number is the dialled public number.

- Under **Matching Pattern** enter the first dialled digits. For international calls, these will be **00**. For national calls, these will be **0**.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the dialled number.
- Under **Delete Digits** enter **2** for international numbers and **1** for national.
- Under **Insert Digits**, enter the Netherlands country code for national numbers.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the called party number.

Digit Conversion for Outgoing Calls from SM

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*0	*8	*15		*1	31	destination		
<input type="checkbox"/>	*00	*10	*17		*2		destination		

Select : All, None

Commit Cancel

Click **Commit** to save changes.

Note: For international calls, the maximum number length would be that specified by E.164, i.e. 15 without the international dialling prefix, **17** in total. The maximum number length for national calls was set to **15** during testing. This value is not critical as long as it is the same or higher than the maximum according to the national numbering plan.

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 panel menu, and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the 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 four 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 PSTN destinations.

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. There are 'Commit' and 'Cancel' buttons in the top right. 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 menu)
- Notes:** (empty text area)
- Location:** Galway (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text area)

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

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop down menu select the domain added in **Section 6.2** as the default domain.

Listen Ports	Protocol	Default Domain	Notes
5060	TCP	avaya.com	
5060	UDP	avaya.com	
5061	TLS	avaya.com	
5062	TCP	avaya.com	

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**.

SIP Entity Details

General

* Name: CM Trunk

* FQDN or IP Address: 10.10.9.12

Type: CM

Notes:

Adaptation:

Location: Galway

Time Zone: Europe/Dublin

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

Credential name:

Securable: ☐

Call Detail Recording: none

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

SIP Link Monitoring

SIP Link 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 used for PSTN destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface used for PSTN fixed calls (see **Figure 1**). 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

* FQDN or IP Address: 10.10.9.81

Type: SIP Trunk

Notes:

Adaptation: Header_Removal

Location: Galway

Time Zone: Europe/Dublin

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

Credential name:

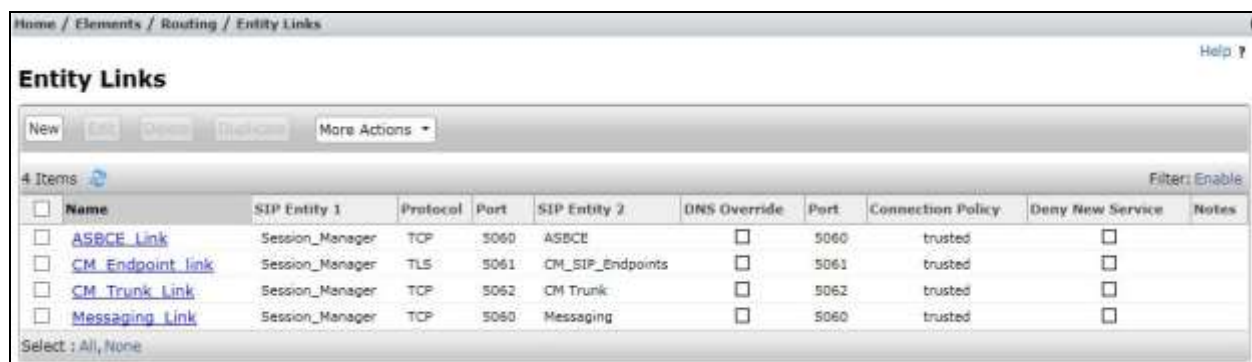
Securable: ☐

Call Detail Recording: egress

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 panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- 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.
- 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.



<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	ASBCE_Link	Session_Manager	TCP	5060	ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Endpoint_Link	Session_Manager	TLS	5061	CM_SIP_Endpoints	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Trunk_Link	Session_Manager	TCP	5062	CM_Trunk	<input type="checkbox"/>	5062	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging_Link	Session_Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

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. 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 panel menu and then click on the **New** button (not shown).

Under **General**:

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

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

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

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

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 Avaya SBCE interface that will be routed to PSTN destinations via the Motto VoIP SIP Trunk.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.10.9.81	SIP Trunk	

Time of Day

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

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 panel 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 the calls to PSTN destinations via the Motto VoIP SIP Trunk.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* Pattern: 0

* Min: 8

* Max: 17

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item [Filter: Enable]

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		PSTN_Outbound	0	<input type="checkbox"/>	ASBCE	

Select : All, None

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

Dial Pattern Details [Commit] [Cancel] Help ?

General

* Pattern: 311026nnnn

* Min: 11

* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		CM_Inbound	0	<input type="checkbox"/>	CM Trunk	

Select : All, None

Note: The above configuration is used to analyze the DDI numbers assigned to the extensions on Communication Manager. Some of the digits of the pattern to be matched have been obscured.

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 panel 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.

Application Editor [Commit] [Cancel]

Application

*Name: CM_App

*SIP Entity: CM_SIP_Endpoints

*CM System for SIP Entity: CM1_Element [Refresh] [View/Add CM Systems](#)

Description:

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

Commit Cancel

Application Sequence

*Name x

Description

Applications in this Sequence

Move First Move Last Remove

1 Item

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

Select : All, None

Available Applications

1 Item Filter: Enable

	Name	SIP Entity	Description
+	CM_App	CM_SIP_Endpoints	

*Required Commit Cancel

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. 2291@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.

The screenshot shows the 'New User Profile' form in the Avaya Session Manager interface. The form is divided into tabs: Identity, Communication Profile, Membership, and Contacts. The Identity tab is active, showing fields for User Provisioning Rule, Last Name, First Name, Login Name, Authentication Type, Password, Confirm Password, Localized Display Name, Endpoint Display Name, Title, Language Preference, Time Zone, Employee ID, Department, and Company. The form is pre-filled with example data: Last Name: SIP, First Name: 9608, Login Name: 2291@avaya.com, Authentication Type: Basic, Password: ****, Confirm Password: ****, Language Preference: English (United Kingdom), Time Zone: (0:0)GMT : Dublin, Edinburgh, L.

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


The screenshot shows the 'Communication Profile' tab in a configuration window. At the top, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' section has two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these is a 'Name' section with a 'New' button, a 'Delete' button, a 'Done' button, and a 'Cancel' button. The 'Name' list shows 'Primary' selected. Below the list, there is a 'Name' field with 'Primary' entered and a 'Default' checkbox checked. The 'Communication Address' section is expanded, showing a 'New' button, an 'Edit' button, and a 'Delete' button. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, with 'No Records found' displayed. Below the table, there is a 'Type' dropdown menu set to 'Avaya SIP', a 'Fully Qualified Address' field with '2291' entered, and a 'Domain' dropdown menu set to 'avaya.com'. At the bottom right, there are 'Add' and 'Cancel' buttons.

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.

The screenshot shows the 'Communication Address' section of the configuration window. It has a 'New' button, an 'Edit' button, and a 'Delete' button. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, with 'No Records found' displayed. Below the table, there is a 'Type' dropdown menu set to 'Avaya SIP', a 'Fully Qualified Address' field with '2291' entered, and a 'Domain' dropdown menu set to 'avaya.com'. At the bottom right, there are 'Add' and 'Cancel' buttons.

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 sequence from the drop-down menu in the **Origination Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.10**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.

☒ **Session Manager Profile** 


SIP Registration

* Primary Session Manager

Primary	Secondary	Maximum
4	0	4
<div>< <div></div> ></div>		


Secondary Session Manager


Survivability Server

Max. Simultaneous Devices 


Block New Registration When Maximum Registrations Active? ☐


Application Sequences

Origination Sequence 

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

Q 2291

Endpoint Editor

* Template

9608SIP_DEFAULT_CM_7_0 ▼

Set Type

9608SIP

Security Code

Port

IP

Voice Mail Number

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.

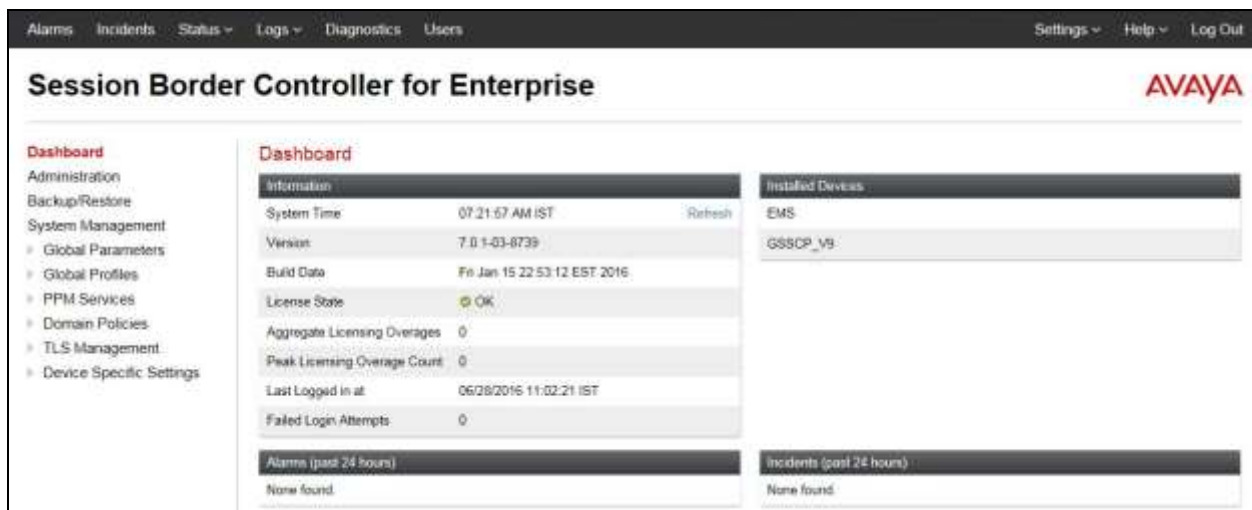
7.1. Access Avaya Session Border Controller for Enterprise

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 image shows the login page for the Avaya Session Border Controller for Enterprise. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." Below this is another disclaimer: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." Below that is a statement: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, it says "© 2011 - 2015 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 image shows the dashboard of the Avaya Session Border Controller for Enterprise. At the top, there is a navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below the navigation bar, the title "Session Border Controller for Enterprise" is displayed. On the left is a sidebar menu with the following items: Dashboard, 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" with fields for System Time (07:21:57 AM IST), Version (7.0 1-03-0739), Build Date (Fri Jan 15 22:53:12 EST 2016), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (06/26/2016 11:02:21 IST), and Failed Login Attempts (0); "Installed Devices" with a table showing EMS and GSSCP_V9; "Alarms (past 24 hours)" with "None found"; and "Incidents (past 24 hours)" with "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. Each side of the Avaya SBCE can have only one physical interface assigned.

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**.



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.



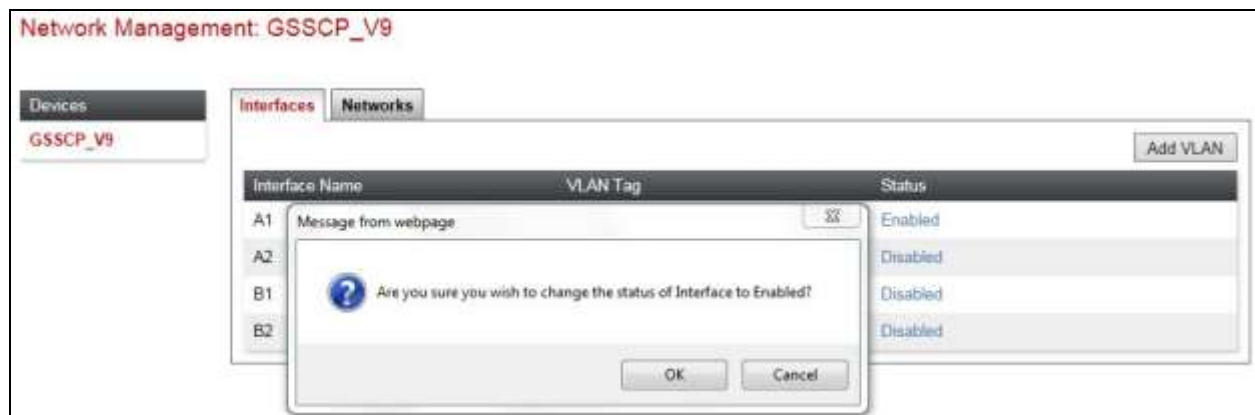
Click on **Add** to define the internal interface. Enter details in the dialogue box (not shown):

- 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** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address for the Avaya SBCE in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:



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 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 TCP used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the Motto VoIP SIP Trunk. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

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

- Select **Add** and enter details of the external signalling interface in the pop-up menu.
- 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 **192.168.122.55**.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the Motto SIP Trunk.

The screenshot shows the 'Add Signaling Interface' dialog box. On the left is a sidebar menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, Signaling Interface (highlighted in red), End Point Flows, Session Flows, and DMZ Services. The main dialog box has a title bar 'Add Signaling Interface' with a close button 'X'. The form contains the following fields: 'Name' (text input with 'External'), 'IP Address' (dropdown menu showing 'External (B1, VLAN 0)' and '192.168.122.55'), 'TCP Port' (text input with 'Leave blank to disable'), 'UDP Port' (text input with '5060'), 'TLS Port' (text input with 'Leave blank to disable'), 'TLS Profile' (dropdown menu with 'None'), 'Enable Shared Control' (checkbox, unchecked), and 'Shared Control Port' (text input). A 'Finish' button is at the bottom right.

The internal signalling interface is defined in the same way; the dialogue box is not shown:

- 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 **TCP** port number, **5060** is used for Session Manager.

The following screenshot shows details of the signalling interfaces:

Signaling Interface: GSSCP_V9

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Internal	10.10.9.81 Internal (A1, VLAN 0)	5060	5060	---	None	Edit Delete
External	192.168.122.55 External (B1, VLAN 0)	5060	5060	---	None	Edit Delete

Note: In the test environment, the internal IP address was **10.10.9.81**.

7.3.2. 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. 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.

- Select **Add** and enter details of the external media interface in the pop-up menu.
- 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 **192.168.122.55**.
- Define the RTP **Port Range** for the media path with the Motto SIP Trunk, during testing this was left at default values of **35000** to **40000**.

Add Media Interface X

Name: External

IP Address: External (B1, VLAN 0) 192.168.122.55

Port Range: 35000 - 40000

Finish

The internal media interfaces are defined in the same way; the dialogue box is not shown:

- 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.

The following screenshot shows details of the media interfaces:

Media Interface: GSSCP_V9

Devices
GSSCP_V9

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Media IP Network	Port Range	
Internal	10.10.9.81 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
External	192.168.122.55 External (B1, VLAN 0)	35000 - 40000	Edit Delete

Note: In the test environment, the internal IP address was **10.10.9.81** and the port range was left at default values.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the Motto SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

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 the Motto VoIP SIP Trunk, click on **Add** (not shown). A pop-up menu is generated. In the **Name** field enter a descriptive name for the Motto VoIP network and click **Next**.

System Management

- Global Parameters
- Global Profiles
 - Domain DoS
 - Server Interworking**

Interworking Profile

Profile Name: Motto

Next

Check the **T.38 Support** box and click on **Next**.

The screenshot shows the 'Interworking Profile' dialog box with the 'General' tab selected. The 'T.38 Support' checkbox is checked. Other settings include 'Hold Support' set to 'None', '180 Handling' through '183 Handling' set to 'None', 'Refer Handling' unchecked, 'URI Group' set to 'None', 'Send Hold' and 'Delayed Offer' checked, '3xx Handling' unchecked, 'Diversion Header Support' unchecked, 'Delayed SDP Handling' unchecked, 'Re-Invite Handling' unchecked, 'Prack Handling' unchecked, 'Allow 18X SDP' unchecked, 'URI Scheme' set to 'SIP', and 'Via Header Format' set to 'RFC3261'. 'Back' and 'Next' buttons are at the bottom.

Interworking Profile	
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 checked="" type="checkbox"/>
Delayed Offer	<input checked="" 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
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

The image shows two side-by-side screenshots of the 'Interworking Profile' dialog box. The left screenshot shows the 'SIP Timers' tab with input fields for Min-SE, Init Timer, Max Timer, Trans Expire, and Invite Expire, each with a unit and range. The right screenshot shows the 'Privacy' tab with checkboxes for Privacy Enabled, P-Asserted-Identity, and P-Preferred-Identity, and a text field for Privacy Header. Both screenshots have 'Back' and 'Next' buttons at the bottom.

Interworking Profile	
SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Interworking Profile	
Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

In the final dialogue box, leave the **Record Routes** at the default setting of **None** and ensure that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk. Click on **Finish**

The screenshot shows the 'Interworking Profile' dialog box. The 'Record Routes' section has radio buttons for 'None' (selected), 'Single Side', 'Both Sides', 'Dialog-Initiate Only (Single Side)', and 'Dialog-Initiate Only (Both Sides)'. Below this is a checkbox for 'Include End Point IP for Context Lookup'. The 'Extensions' field is a dropdown menu set to 'None'. The 'Diversion Manipulation' section has a checkbox and a 'Diversion Condition' dropdown set to 'None'. The 'Diversion Header URI' field is empty. The 'Has Remote SBC' checkbox is checked. The 'Route Response on Via Port' checkbox is unchecked. The 'DTMF' section has a 'DTMF Support' dropdown with radio buttons for 'None' (selected), 'SIP NOTIFY', and 'SIP INFO'. At the bottom are 'Back' and 'Finish' buttons.

Repeat the process to define Server Interworking for Session Manager using the same parameter settings apart from **Record Routes**. The following screenshot shows the **General** tab.

The screenshot shows the 'Interworking Profiles: ASM' configuration page. On the left is a list of profiles: 'ts2100', 'avaya-nu', 'OCS-Edge-Server', 'cisco-cm', 'cupi', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'ASM' (highlighted in red), and 'Motto'. The main area shows the 'General' tab for the 'ASM' profile. It includes a description field and several configuration options:

Option	Value
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	No
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	Yes
URI Scheme	SIP
Via Header Format	RFC3261

At the bottom right is an 'Edit' button.

The next screenshot shows the **Advanced** tab:

The screenshot displays the 'Interworking Profiles: ASM' configuration interface. On the left, a sidebar lists various profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-cm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'ASM' (highlighted in red), and 'Motto'. The main area shows the 'Advanced' tab selected, with a description field at the top. Below the tabs, the configuration is organized into sections: '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), and a 'DTMF' section with 'DTMF Support' set to 'None'. An 'Edit' button is located at the bottom right of the configuration area.

7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. The Motto SIP Trunk is connected as a Trunk Server. Session Manager is connected as a Call Server.

To define the Motto SIP Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu.

The screenshot shows the 'Add Server Configuration Profile' dialog box. The left sidebar contains a menu with options: 'Domain DoS', 'Server Interworking', 'Media Forking', 'Routing', and 'Server Configuration' (highlighted in red). The main area of the dialog has a 'Profile Name' input field containing the text 'NTWK' and a 'Next' button below it.

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 Motto SIP Trunk FQDN.
- In the **Port** box, enter the port to be used for the SIP Trunk. This was left blank during testing which defaults to 5060 when UDP is used for transport.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.

Edit Server Configuration Profile - General		
Server Type	Trunk Server	
		Add
IP Address / FQDN	Port	Transport
sip.mottovoip.nl	5060	UDP
		Delete
Back		Next

Click on **Next** and **Next** again. Leave the fields in the dialogue boxes at default values.

Add Server Configuration Profile - Authentication	Add Server Configuration Profile - Heartbeat
Enable Authentication <input type="checkbox"/>	Enable Heartbeat <input type="checkbox"/>
User Name	Method
Realm <small>(Leave blank to detect from server challenge)</small>	Frequency
Password	From URI
Confirm Password	To URI
Back Next	Back Next

Click on **Next** again to get to the final dialogue box.

The final dialogue box contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for Motto SIP Trunk defined in **Section 7.4**.
- Leave the other fields at default settings.
- Click **Finish**.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains several settings:

- Enable DoS Protection: ☐
- Enable Grooming: ☐
- Interworking Profile: Motto (selected in a dropdown menu)
- Signaling Manipulation Script: None (selected in a dropdown menu)
- Connection Type: SUBID (selected in a dropdown menu)
- Securable: ☐

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

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.
- Ensure that the Interworking Profile defined for Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box

The following screenshot shows the completed Server Configuration:

The screenshot shows the "Server Configuration: CPE" window. It has a sidebar with "Server Profiles" and "CPE" selected. The main area has tabs for "General", "Authentication", "Heartbeat", and "Advanced".

General Tab:

- Server Type: Call Server
- IP Address / FQDN: 10.10.9.31
- Port: 5060
- Transport: TCP

Advanced Tab:

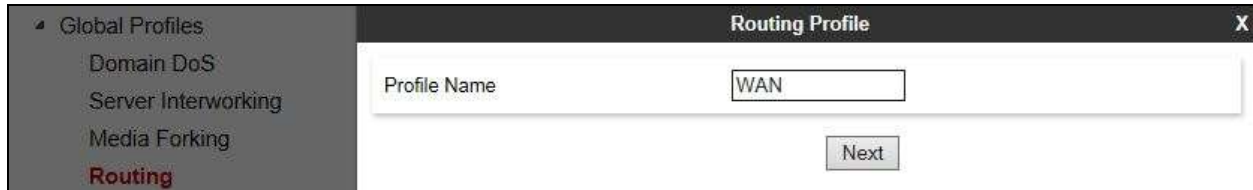
- Enable DoS Protection: ☐
- Enable Grooming: ☐
- Interworking Profile: ASM
- Signaling Manipulation Script: None
- Connection Type: SUBID
- Securable: ☐

Buttons at the top right include "Add", "Rename", "Clone", and "Delete". Buttons at the bottom include "Edit".

7.6. Define Routing

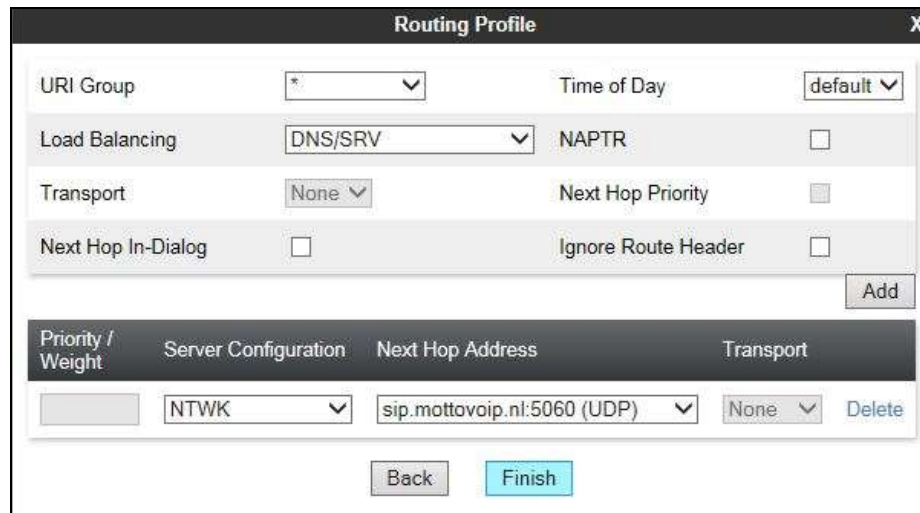
Routing information is required for routing to the Motto VoIP SIP Trunk on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling.

To define routing to the Motto SIP Trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.



Click on **Next** and enter details for the Routing Profile for the SIP Trunk:

- During testing, DNS was used to connect to Motto VoIP. To use DNS, select **DNS/SRV** from the **Load Balancing** drop down menu.
- Click on **Add** to specify an FQDN for the SIP Trunk.
- Select the Server Configuration defined in **Section 7.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.



Note: While DNS SRV can be selected here, the Avaya SBCE does not resolve SRV records. It will only handle simple DNS where an IP address is returned for the DNS query.

Repeat the process for the Routing Profile for Session Manager: The screenshot over the page shows the completed configuration. The **Next Hop Address** in this case is the private IP address of the Session Manager:

Routing Profiles: LAN

Buttons: Add, Rename, Clone, Delete

Routing Profiles: default, LAN, WAN

Click here to add a description

Routing Profile

Update Priority

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.10.9.31	TCP

Buttons: Add, Edit, Delete

7.7. 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 address. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop or external interfaces.

To define Topology Hiding for the Motto VoIP SIP Trunk, navigate to **Global Profiles** → **Topology Hiding** in the main menu on the left hand side. Click on **Add** to bring up a dialogue box, assign an appropriate name and click on **Next** to configure Topology Hiding for each header as required:

Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding

Topology Hiding Profile

Profile Name: Motto

Next

Enter details in the **Topology Hiding Profile** pop-up menu.

- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing the default **IP/Domain** was used for all headers that hides both domain names and IP addresses.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.

Topology Hiding Profile

Add Header

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

Buttons: Back, Finish, Delete

The following screenshot shows the completed **Topology** Hiding configuration for the Motto SIP Trunk.

Topology Hiding Profiles: Motto

Click here to add a description

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

Edit

To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for Motto SIP Trunk. Do this by highlighting the profile defined for Motto and clicking on **Clone**. Enter an appropriate name for Session Manager and click on **Next** (not shown). Make any changes where required, none were made in the test environment.

Topology Hiding Profiles

Click here to add a description

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

Edit

7.8. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the Motto VoIP SIP Trunk. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the Motto SIP Trunk and vice versa.

To define a Server Flow for the Motto VoIP SIP Trunk, navigate to **Device Specific Settings** → **End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for the Motto SIP Trunk, in the test environment **Network** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the Motto VoIP SIP Trunk defined in **Section 7.5**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Motto VoIP SIP Trunk defined in **Section 7.7** 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	Network
Server Configuration	NTWK
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal
Signaling Interface	External
Media Interface	External
End Point Policy Group	default-low
Routing Profile	LAN
Topology Hiding Profile	Motto
Signaling Manipulation Script	None
Remote Branch Office	Any

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

To define a Server Flow for Session Manager, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **CPE** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5**.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. 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 7.3**. This is the 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 7.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Motto VoIP SIP Trunk defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** 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	CPE
Server Configuration	CPE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External
Signaling Interface	Internal
Media Interface	Internal
End Point Policy Group	default-low
Routing Profile	WAN
Topology Hiding Profile	ASM
Signaling Manipulation Script	None
Remote Branch Office	Any

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

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

End Point Flows: GSSCP_V9

Devices
GSSCP_V9

Subscriber Flows Server Flows

Add

Hover over a row to see its description.

Server Configuration: CPE

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	CPE	*	External	Internal	default-low	WAN	View	Clone	Edit	Delete

Server Configuration: NTWK

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Network	*	Internal	External	default-low	LAN	View	Clone	Edit	Delete

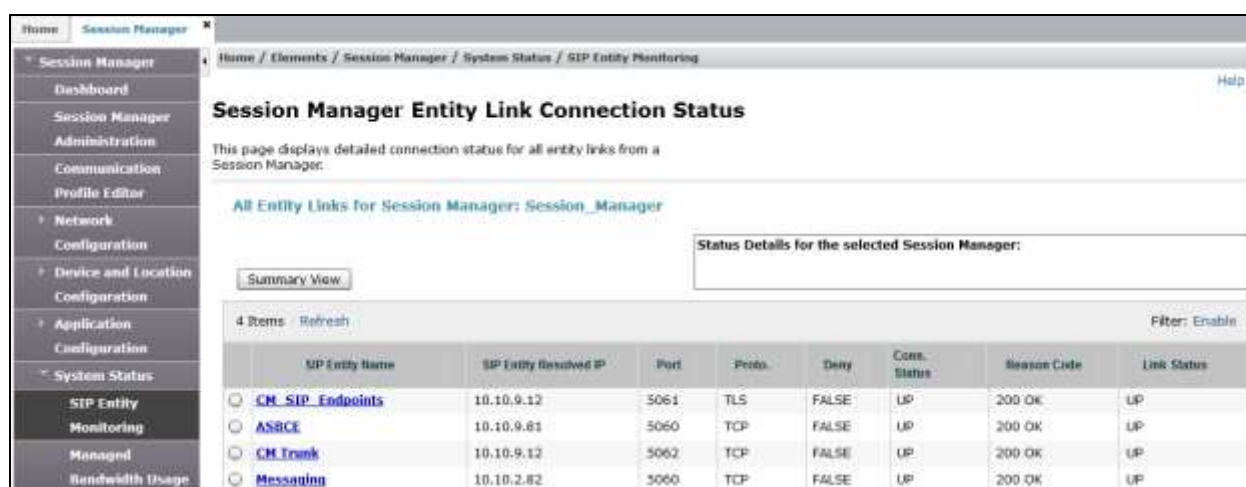
8. Configure the Motto SIP Trunk Equipment

The configuration of the Motto 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 Motto VoIP equipment and system configuration please contact an authorized Motto 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**.



SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM SIP Endpoints	10.10.9.12	5061	TLS	FALSE	UP	200 OK	UP
ASBCE	10.10.9.81	5060	TCP	FALSE	UP	200 OK	UP
CM Trunk	10.10.9.12	5062	TCP	FALSE	UP	200 OK	UP
Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

2. From Communication Manager SAT interface run the command **status trunk n** where **n** is the 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
0002/007	T00017	in-service/idle	no
0002/008	T00018	in-service/idle	no
0002/009	T00019	in-service/idle	no
0002/010	T00020	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.

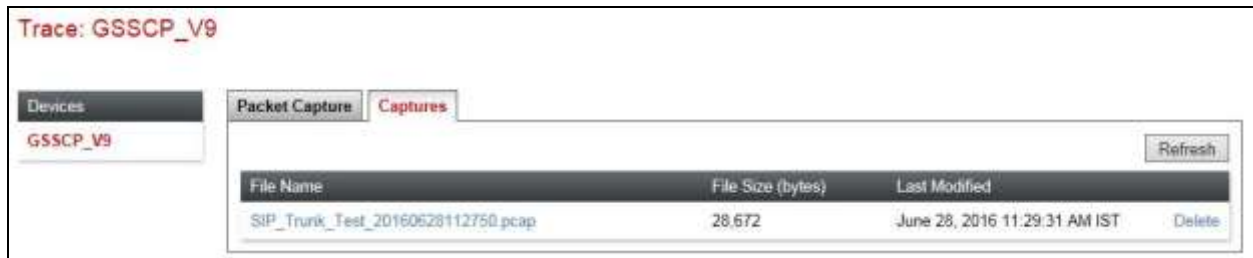
- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or **All** from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

The screenshot displays the 'Packet Capture Configuration' window in the Avaya SBCE interface. The left-hand navigation pane shows the path: Dashboard > Administration > System Management > Device Specific Settings > Troubleshooting > Trace. The main content area is titled 'Trace: GSSCP_V9'. Within this area, the 'Packet Capture' tab is active. The configuration form contains the following fields and values:

- Status:** Ready
- Interface:** B1 (selected from a dropdown)
- Local Address (IP Port):** All (selected from a dropdown)
- Remote Address:** * (entered in the text field)
- Protocol:** All (selected from a dropdown)
- Maximum Number of Packets to Capture:** 10000 (entered in the text field)
- Capture Filename:** SIP_Trunk_Test.pcap (entered in the text field, with a note: 'Using the name of an existing capture will overwrite it')

At the bottom of the configuration form, there are two buttons: 'Start Capture' and 'Clear'.

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



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 Motto VoIP network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura ® Communication Manager R7.0, Avaya Aura ® Session Manager 7.0 and Avaya Session Border Controller for Enterprise R7.0 to Motto VoIP SIP Trunk. The Motto VoIP SIP Trunk 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. The Motto SIP Trunk is described by the *Motto SIP Specification – MBN* document provided by Motto.

Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0.1, 06 May 2016.
- [2] *Upgrading and Migrating Avaya Aura® applications to 7.0*, Release 7.0.1, 06 May 2016.
- [3] *Deploying Avaya Aura® 7.0.1 applications*, Release 7.0.1, 09 May 2016
- [4] *Deploying Avaya Aura® Communication Manager*, Release 7.0.1, 08 May 2016
- [5] *Administering Avaya Aura® Communication Manager* Release 7.0.1, 09 May 2016.
- [6] *Upgrading Avaya Aura® Communication Manager*, Release 7.0.1, 08 May 2016
- [7] *Deploying Avaya Aura® System Manager*, Release 7.0.1, 09 May 2016
- [8] *Upgrading Avaya Aura® System Manager to 7.0.1*, 06 May 2016.
- [9] *Administering Avaya Aura® System Manager for 7.0.1*, 25 Jun 2016
- [10] *Deploying Avaya Aura® Session Manager*, Release 7.0.1, 09 May 2016
- [11] *Upgrading Avaya Aura® Session Manager* Release 7.0.1, 09 May 2016
- [12] *Administering Avaya Aura® Session Manager* Release 7.0.1, 09 May 2016,
- [13] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [15] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Jan 2016
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2016 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.