



Application Notes for Configuring Avaya Aura[®] Communication Manager R6.2 as an Evolution Server, Avaya Aura[®] Session Manager R6.2 and Avaya Session Border Controller for Enterprise R6.2 to Support Motto VoIP SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Motto VoIP SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura[®] Session Manager and Avaya Aura[®] Communication Manager as an Evolution Server. Motto VoIP 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 to configure Session Initiation Protocol (SIP) trunking between Motto VoIP SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with the Motto VoIP SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

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

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 from the PSTN to the enterprise site were routed to DID numbers assigned by Motto VoIP. Incoming calls were made to H.323, SIP, Digital and Analogue telephones.
- Outgoing calls from the enterprise site to the PSTN were routed to PSTN numbers. Outgoing calls were made from H.323, SIP, Digital and Analogue telephones.
- Calls using G.711A, G.711MU and G.729 codec's supported by Motto VoIP. DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones was used during this test.
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

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

- T.38 fax transmission is not supported by Motto.
- All tests were completed using H.323, SIP, Digital and Analogue phone types. The Avaya one-X® Communicator was used to test soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- No Emergency Services numbers were tested as test calls to these numbers should be pre-arranged with the Operator.

2.3. Support

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 Service. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware) Avaya A175 Desktop Video Device running Flare Experience, Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for SIP.

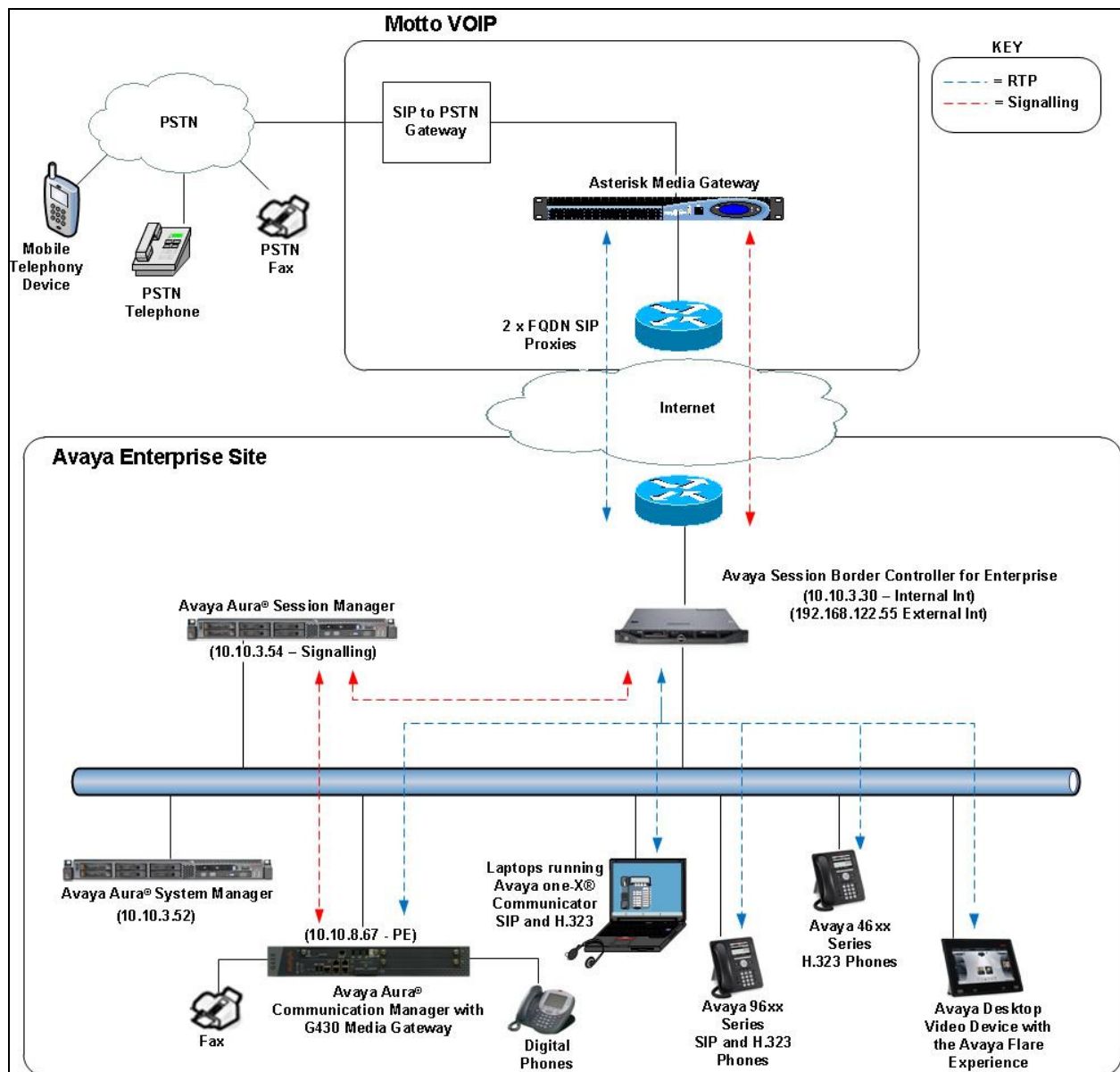


Figure 1: Test Setup Motto VoIP SIP Trunk Service to simulated Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager R6.2 (R016x.02.0.823.0-20558)
Avaya G430 Media Gateway MM711 Analogue MM712 Digital MGP Firmware	HW31 FW093 HW07 FW009 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.2 SP3 (6.2.0.0.15669 -6.2.12.307)
Avaya S8800 Server	Avaya Aura® System Manager R6.2 (6.2.0.0.15669-6.2.12.9) Update revision No: 6.2.15.1.1959
Dell R310	Avaya Session Border Controller for Enterprise. (6.2.0.Q36)
Avaya 9650 Phone (H.323)	3.171B
Avaya 9621 Phone (SIP)	6.2.0.72
Avaya 2420 Digital Phone	N/A
Analog Phone	N/A
Avaya 4620 Phone (H.323)	1.2200
Avaya 9611 Phone (SIP)	6.2.0.72
Avaya one-X® Communicator	6.1.3.06-SP3-35509
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1
Motto VoIP	
Proxy Servers	OpenSIPS 1.7 & OpenSIPS 1.8
Media Gateways	Asterisk 1.4.22-0Motto14

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 Service. For incoming calls, the 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 the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Motto VoIP network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya S8800 Server and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

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

display system-parameters customer-options		Page	2	of	11
OPTIONAL FEATURES					
IP PORT CAPACITIES		USED			
Maximum Administered H.323 Trunks:		12000	0		
Maximum Concurrently Registered IP Stations:		18000	3		
Maximum Administered Remote Office Trunks:		12000	0		
Maximum Concurrently Registered Remote Office Stations:		18000	0		
Maximum Concurrently Registered IP eCons:		414	0		
Max Concur Registered Unauthenticated H.323 Stations:		100	0		
Maximum Video Capable Stations:		18000	0		
Maximum Video Capable IP Softphones:		18000	0		
Maximum Administered SIP Trunks:		4000	10		

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

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	IP Stations? y	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? y	
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	ISDN-PRI? y	
ESS Administration? n	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? n	
IP Trunks? y		
IP Attendant Consoles? y		
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. Type **change node-names ip** to make changes to the **IP Node Names**. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.3.55** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the interface that Communication Manager will use as the SIP signaling interface to Session Manager.

change node-names ip		IP NODE NAMES
Name	IP Address	
procr	10.10.8.67	
SM100	10.10.3.55	
default	0.0.0.0	

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-region** and **Inter-region**) is set to yes to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** was used.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: avaya.com
Name: Default NR
MEDIA PARAMETERS
Codec Set: 1           Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? n
UDP Port Min: 35000
UDP Port Max: 50001
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
                                                                AUDIO RESOURCE RESERVATION PARAMETERS
                                                                RSVP Enabled? n
```

5.4. Administer IP Codec Set

Use the **change ip-codec-set** command for the codec set specified in the **IP Network Region** form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test, the codec's supported by Motto VoIP were configured, namely **G.711A**, **G.729** and **G.711MU**.

```
change ip-codec-set 1                                         Page 1 of 2
                                                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt     Size(ms)
1: G.711A   n                    2          20
2: G.729    n                    2          20
2: G.711MU  n                    2          20
```


Motto VoIP only supports pass-through for transmission of fax. Navigate to **Page 2** to configure pass-through by setting the **Fax Mode** to **pass-through** as shown below.

change ip-codec-set 1

Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

	Mode	Redundancy
FAX	pass-through	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

5.5. Administer SIP Signaling Groups

Add a signaling group and trunk group for inbound and outbound PSTN calls to Motto VoIP SIP Trunk Service and configure using TCP (Transmission Control Protocol) and tcp port of 5060.

Configure the **Signaling Group** using the **add signaling-group n** command, where **n** is an available signaling group:

- Set the **Group Type** field to **sip**.
- The **Transport Method** field is set to **tcp**.
- Set the **Near-end Node Name** to the processor interface (node name **procr**). This value is taken from the **IP Node Names** form shown in **Section 5.2**.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM100**), also shown in **Section 5.2**.
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.3**. This field logically establishes the far-end for calls using this signaling group as network region **1**.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The **Direct IP-IP Early Media** field is set to **n**.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.

The default values for the other fields may be used.

```
add signaling-group 1
                                SIGNALING GROUP

Group Number: 1                Group Type: sip
                                Transport Method: tcp
IMS Enabled? n

Near-end Node Name: procr      Far-end Node Name: SM100
Near-end Listen Port: 5060     Far-end Listen Port: 5060
                                Far-end Network Region: 1
Far-end Domain:

Incoming Dialog Loopbacks: eliminate
                                Bypass If IP Threshold Exceeded? n
                                RFC 3389 Comfort Noise? n
                                DTMF over IP: rtp-payload
                                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3
                                IP Audio Hairpinning? n
                                Enable Layer 3 Test? n
                                Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n
                                Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group

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

- Set the **Group Type** field to **sip**.
- Choose a descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan, i.e. **101**.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **public-ntwrk**.
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**.
- Specify the **Number of Members** supported by this SIP trunk group.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SIP to SM100	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Signaling Group: 1	
		Number of Members: 10	

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Motto VoIP. This value defines the interval that subsequent INVITEs must be sent to keep the active session alive. For the compliance testing, the value of **1800** seconds was used.

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
SCCAN? n		Redirect On OPTIM Failure: 5000	
		Digital Loss Group: 18	
		Preferred Minimum Session Refresh Interval(sec): 1800	
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

On **Page 3**, set the **Numbering Format** field to **private**. This prevents the number to be sent to Motto VoIP with the + used in the E164 numbering format.

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

On **Page 4** of this form:

- Set **Send Transferring Party Information** to **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 **n**.
- Set **Send Diversion Header** to **n** to remove the Diversion Header. This information is not used and increases the size of the INVITE unnecessarily.
- Set **Support Request History** to **n** to ensure the History-Info Header is not sent. This information is not used and increases the size of the INVITE unnecessarily.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Motto VoIP.
- Set **Always Use re-INVITE for Display Updates** to **y** as the most effective method employed by Communication Manager of modifying an existing dialogue.
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension.

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

5.7. Administer Calling Party Number Information

In this section the Calling Party Number sent when making a call using the SIP trunk is specified.

5.7.1. Set Private Numbering

Use the **change private-numbering 0** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **4**-digit extension beginning with **6** will send the calling party number **31457xxxxxx** to Motto VoIP SIP Trunk Service. This calling party number will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Public DID numbers have been masked for security purposes.

change private-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
4	6	1	31457xxxxxx	11	Total Administered: 1
					Maximum Entries: 240

5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to Motto VoIP SIP Trunk Service. In the sample configuration, the single digit **9** is used as the ARS access code. Avaya telephone users will dial **9** to reach an outside line. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1** as a feature access code (**fac**).

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

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

change feature-access-codes		Page 1 of 9
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *37		
Answer Back Access Code: *12		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 7		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2: *99
Automatic Callback Activation:		Deactivation:
Call Forwarding Activation Busy/DA: *87 All: *88		Deactivation: #88
Call Forwarding Enhanced Status: Act:		Deactivation:

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning **0** or **00**. Calls are sent to **Route Pattern 1**, which contains the previously configured SIP Trunk Group.

change ars analysis 0		Page 1 of 2
ARS DIGIT ANALYSIS TABLE		
Location: all		Percent Full: 1
Dialed String	Total Min Max	Route Pattern
0	10 11	1
00	13 14	1
		Call Type
		Node Num
		ANI Req'd
		pubu
		pubu
		n
		n

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group 1.

change route-pattern 1													Page 1 of 3			
Pattern Number: 1 Pattern Name: tosm100																
SCCAN? n Secure SIP? n																
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC								
No			Mrk	Lmt	List	Del	Digits	QSIG								
								Intw								
1:	1	0													n	user
2:														n	user	
3:														n	user	
4:														n	user	
5:														n	user	
6:														n	user	
BCC VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature		PARM	No.	Numbering	LAR			
0 1 2 M 4 W			Request								Dgts	Format				
													Subaddress			
1:	y	y	y	y	y	n	n	rest				unk-unk	none			
2:	y	y	y	y	y	n	n	rest					none			
3:	y	y	y	y	y	n	n	rest					none			
4:	y	y	y	y	y	n	n	rest					none			
5:	y	y	y	y	y	n	n	rest					none			
6:	y	y	y	y	y	n	n	rest					none			

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Motto VoIP can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by Motto VoIP correlate to the internal extensions assigned within Communication Manager. The **change inc-call-handling-trmt trunk-group 1** command is used to translate numbers **+31457nnnnn0** to **+31457nnnnn5** to the 4 digit extension by deleting **all** of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

change inc-call-handling-trmt trunk-group 1				Page	1 of	3
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Number Digits	Del	Insert		
public-ntwrk	11	31457nnnnn0	all	6100		
public-ntwrk	11	31457nnnnn1	all	6102		
public-ntwrk	11	31457nnnnn2	all	6003		
public-ntwrk	11	31457nnnnn3	all	6004		
public-ntwrk	11	31457nnnnn4	all	6104		
public-ntwrk	11	31457nnnnn5	all	6006		

5.10. EC500 Configuration

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

configuration for the user with station extension 6100. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnnn**).
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing.
- Set the **Config Set** to **1**.

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

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

6. Configuring Avaya Aura® Session Manager

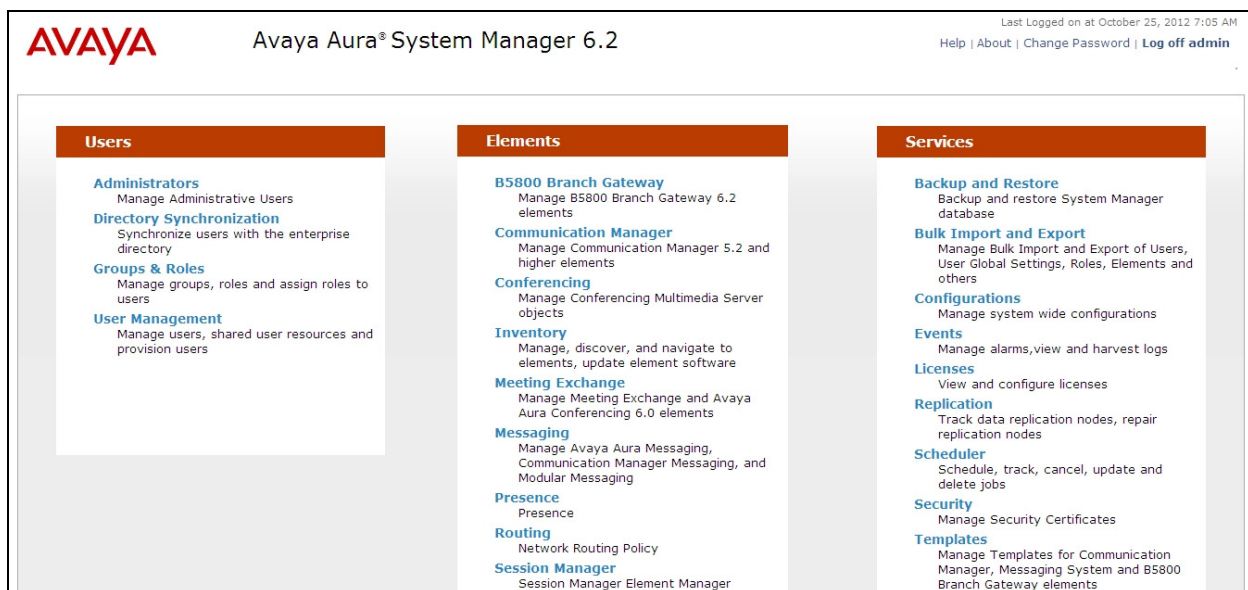
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

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

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

6.1. Log in to Avaya Aura® System Manager

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



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

6.2. Administer SIP domain

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

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

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

The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, the title 'Domain Management' is displayed. To the right of the title are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. A warning message states: 'Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.' Below the warning is a table with one item. The table has columns: Name, Type, Default, and Notes. The first row contains the domain 'avaya.com', the type 'sip', a checkbox for 'Default', and an empty 'Notes' field. The table is highlighted with a red border.

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

6.3. Administer Locations

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

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

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

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

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

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

Home / Elements / Routing / Locations - Location Details

Location Details Help ? Commit Cancel

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

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

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

Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth: Kbit/sec

Location Pattern

Add Remove

3 Items Refresh Filter: Enable

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

Select : All, None

* Input Required Commit Cancel

6.4. Administer SIP Entities

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

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the SBC SIP entity.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are three SIP Entities.

- Session Manager SIP Entity.
- Communication Manager SIP Entity.
- Avaya SBCE SIP Entity.

6.4.1. Avaya Aura® Session Manager SIP Entity

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

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

- Name:** Session Manager
- FQDN or IP Address:** 10.10.3.55
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text field)
- Location:** SMGRVL3 (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

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

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

Port
Add Remove

3 Items | Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	

Select : All, None

* Input Required Commit Cancel

6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screens show the SIP entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling. The entity **Type** is set to **CM**. Set 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 Help ? Commit Cancel

General

* Name: Communication Manager

* FQDN or IP Address: 10.10.8.67

Type: CM

Notes:

Adaptation:

Location: SMGRVL3

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.3. Avaya Session Border Controller for Enterprise SIP Entities

The following screen shows the SIP entity for the Avaya SBCE used for routing calls. The **FQDN or IP Address** field is set to the IP address of the private interfaces administered in **Section 7** of this document. Set 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 [Help ?](#)

[Commit](#) [Cancel](#)

General

* Name: Avaya SBCE

* FQDN or IP Address: 10.10.3.30

Type: Gateway

Notes:

Adaptation:

Location: SMGRVL3

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Administer Entity Links

A SIP trunk between 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 **SessionManager**.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop down menu to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.

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

Home /Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* toCommunication Ma	* Session Manager	TCP	* 5060	* Communication Manager	* 5060	Trusted	

* Input Required Commit Cancel

Home /Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* toAvaya SBCE	* Session Manager	TCP	* 5060	* Avaya SBCE	* 5060	Trusted	

* Input Required Commit Cancel

6.6. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

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

The following screen shows the routing policy for Communication Manager:

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

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.8.67	CM	

The following screens show the routing policy for Avaya SBCE:

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

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.3.30	Gateway	

6.7. Administer Dial Patterns

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

Under **General**:

- In the **Pattern** field enter a dialed number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialed number.
- In the **Max** field enter the maximum length of the dialed number.
- In the **SIP Domain** field select **-ALL-**.

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.6**. Click **Select** button to save (not shown).

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Motto VoIP SIP Trunk Service.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 00353

* Min: 5

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		toAvaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name <small>1 ▲</small>	Originating Location Notes	Routing Policy Name	Rank <small>2 ▲</small>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		toCommunication Manager	0	<input type="checkbox"/>	Communication Manager	

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE.

7.1. Accessing Avaya Session Border Controller for Enterprise

Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.

Log In to Avaya Session Border Controller for Enterprise

AVAYA

**Session Border Controller
for Enterprise**

Log In

Session expired, please sign in again.

Username:

Password:

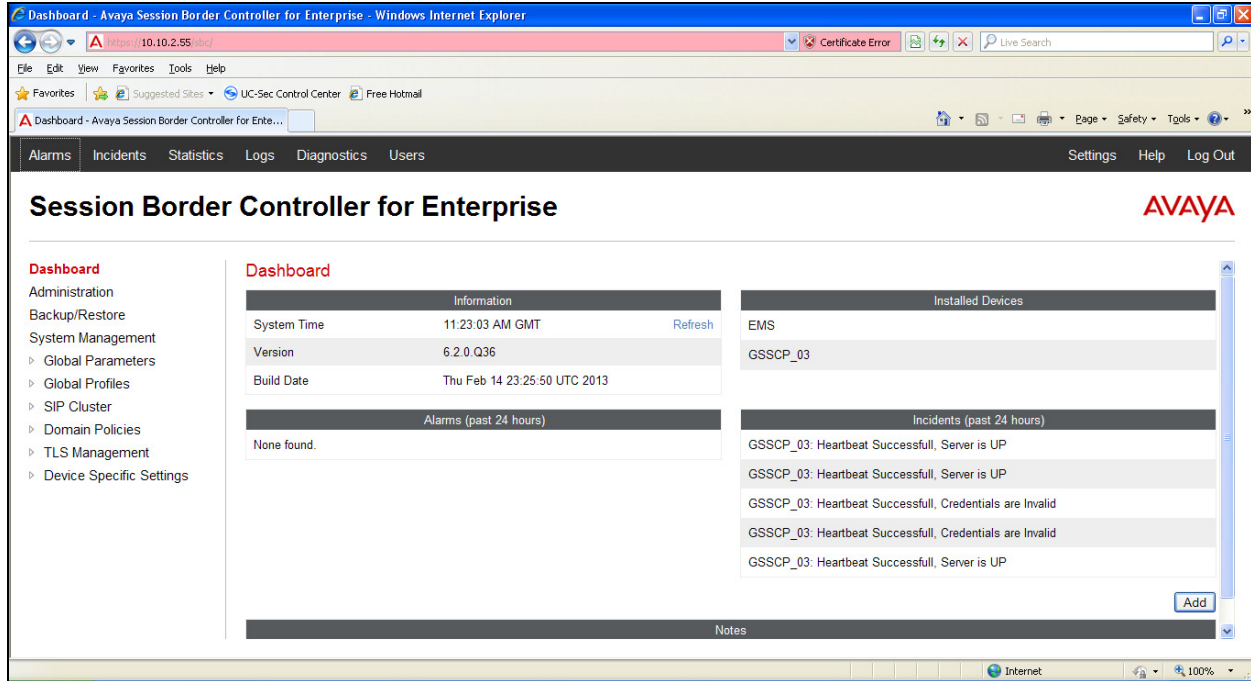
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

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.

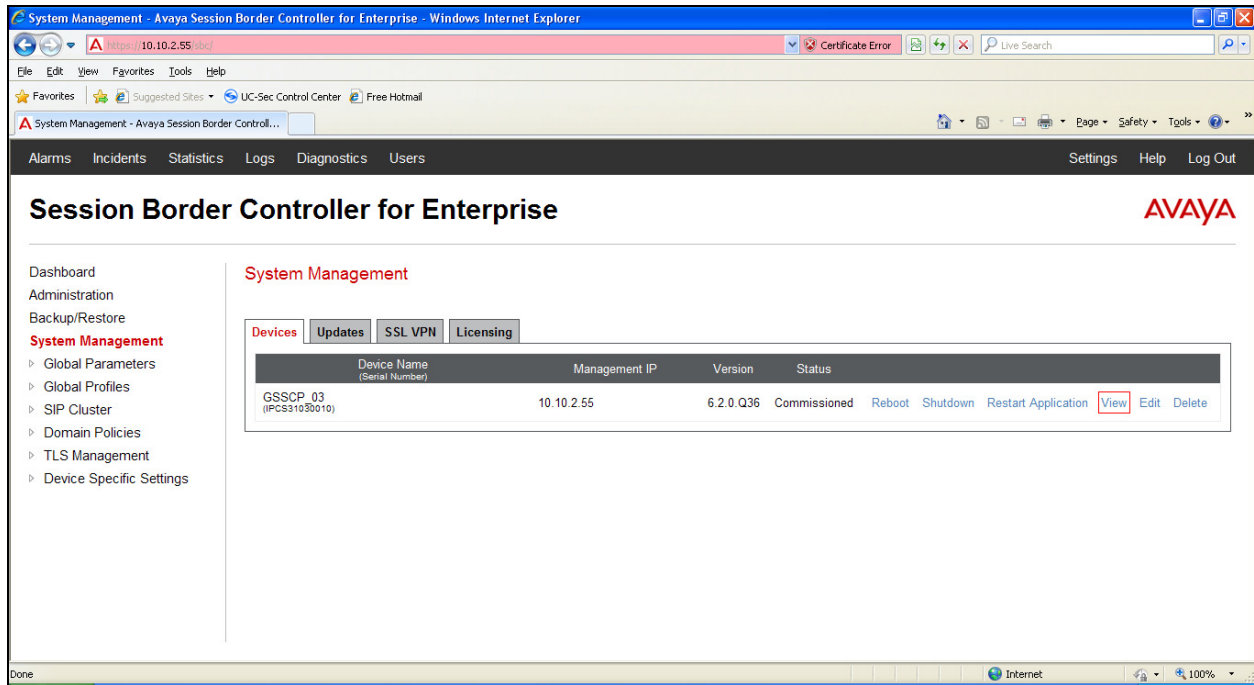
All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

The main page of the Avaya SBCE will appear.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_03** is shown. To view the configuration of this device, click **View** (the third option from the right).



The System Information screen shows the **Appliance Name**, **Device Settings** and **DNS Configuration** information.

System Information: GSSCP_03

X

General Configuration

Appliance NameGSSCP_03

Box TypeSIP

Deployment ModeProxy

Device Configuration

HA ModeNo

Two Bypass ModeNo

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
86.47.122.55	86.47.122.55	255.255.255.128	86.47.122.7	B1

DNS Configuration

Primary DNS10.10.7.100

Secondary DNS10.10.101.115

DNS LocationDMZ

DNS Client IP10.10.3.30

Management IP(s)

IP10.10.2.55

7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Server Internetworking Avaya

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

- Enter profile name such as **Avaya_SM** and click **Next** (Not Shown)
- Check **Hold Support= RFC2543**
- Check **T.38 Support** (not required but checked to avoid restriction on Avaya SBCE)
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens and then **Finish**.

Profile: Avaya_SM

General

Hold Support	<input type="radio"/> None <input checked="" type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - s=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

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

Profile: Avaya_SM X

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

Finish

7.2.2. Server Internetworking – Motto VoIP

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

- Enter profile name such as **Motto** and click **Next** (Not Shown)
- Check **Hold Support= RFC2543**
- Check **T.38 Support** (not required but checked to avoid restriction on Avaya SBCE)
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens and then **Finish**.

Profile: Motto

General

Hold Support

☐ None

☒ RFC2543 - c=0.0.0.0

☐ RFC3264 - a=sendonly

180 Handling

☒ None ☐ SDP ☐ No SDP

181 Handling

☒ None ☐ SDP ☐ No SDP

182 Handling

☒ None ☐ SDP ☐ No SDP

183 Handling

☒ None ☐ SDP ☐ No SDP

Refer Handling

☐

3xx Handling

☐

Diversion Header Support

☐

Delayed SDP Handling

☐

T.38 Support

☒

URI Scheme

☒ SIP ☐ TEL ☐ ANY

Via Header Format

☒ RFC3261 ☐ RFC2543

Next

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

Profile: Motto X

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

Finish

7.2.3.Routing

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

Create a Routing Profile for Session Manager and a Routing Profile for Motto VoIP. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.

In the new window that appears, enter the following values. Use default values for all remaining fields:

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

Click **Finish**.

The following screen shows the Routing Profile to Session Manager.

Routing Profiles: Avaya_SM

Add

Rename Clone Delete

Click here to add a description.

Routing Profile

Add

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.10.3.55	---	View Edit

The following screen shows the Routing Profile to Motto VoIP.

Routing Profiles: Motto

Add

Routing Profiles

default

Avaya_SM

Motto

Rename

Clone

Delete

Click here to add a description.

Routing Profile

Add

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	srv-ams3-hproxy-228.mottovoip.nl	srv-ams1-hproxy-231.mottovoip.nl	View Edit

7.2.4. Server Configuration– Avaya Aura® Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the lefthand menu select **Global Profiles** → **Server Configuration** and click on **Add**. Enter **Profile Name: Avaya_SM**. On the **Add Server Configuration Profile** tab, set the following:

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

The screenshot shows the 'Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Call Server'. The 'IP Addresses / Supported FQDNs' text area contains '10.10.3.55'. Under 'Supported Transports', the 'TCP' checkbox is checked, while 'UDP' and 'TLS' are unchecked. The 'TCP Port' text box contains '5060'. The 'UDP Port' and 'TLS Port' text boxes are empty. A 'Finish' button is at the bottom.

Field	Value
Server Type	Call Server
IP Addresses / Supported FQDNs	10.10.3.55
Supported Transports	<input checked="" type="checkbox"/> TCP, <input type="checkbox"/> UDP, <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	

On the **Advanced** tab:

- Select **Avaya_SM** for **Interworking Profile**
- Click **Finish**

The screenshot shows a window titled "Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options:

- Enable DoS Protection**: A checkbox that is currently unchecked.
- Enable Grooming**: A checkbox that is currently unchecked.
- Interworking Profile**: A dropdown menu with "Avaya_SM" selected. This dropdown is highlighted with a red rectangular box.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- TCP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". The "SUBID" radio button is selected.

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

7.2.5. Server Configuration – Motto VoIP

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles** → **Server Configuration** and click on **Add**. Enter Name as **Motto**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** as **Trunk Server**
- Enter the **FQDNs** of the SIP proxies to Motto VoIP
- **Supported Transports**: Check **UDP**
- **UDP Port**: **5060**
- Click on **Next** (not shown)

The screenshot shows the 'Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Trunk Server'. The 'IP Addresses / Supported FQDNs' text area contains 'srv-ams3-hproxy-228.mottovoip.nl,srv-ams1-hproxy-231.mottovoip.nl'. Under 'Supported Transports', the 'UDP' checkbox is checked. The 'UDP Port' field is set to '5060'. A 'Finish' button is at the bottom.

Field	Value
Server Type	Trunk Server
IP Addresses / Supported FQDNs	srv-ams3-hproxy-228.mottovoip.nl,srv-ams1-hproxy-231.mottovoip.nl
Supported Transports	<input checked="" type="checkbox"/> UDP, <input type="checkbox"/> TCP, <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	

In the new window that appears, enter the following values as Motto VoIP require authentication to connect to their network:

- **Enabled Authentication:** Checked
- **User Name:** Enter username provided by the Service Provider
- **Realm:** Enter realm details provided by the Service Provider
- **Password** Enter password provided by the Service Provider
- **Confirm Password** Re-enter password provided by the Service Provider

Click **Finish** to continue.



In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked
- **Method:** Select **REGISTER** from the drop-down box
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP REGISTERS
- **From URI:** Enter an URI to be sent in the FROM header for SIP REGISTERS
- **TO URI:** Enter an URI to be sent in the TO header for SIP REGISTERS

Click **Next** to continue.



On the **Advanced** tab:

- Select **Motto** for **Interworking Profile**
- Click **Finish**

The screenshot shows a window titled "Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options:

- Enable DoS Protection**: A checkbox that is currently unchecked.
- Enable Grooming**: A checkbox that is currently unchecked.
- Interworking Profile**: A dropdown menu with "Motto" selected. This dropdown is highlighted with a red rectangular border.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- UDP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". The "SUBID" radio button is selected.

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

7.2.6. Topology Hiding – Avaya

The **Topology Hiding** screen manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. Navigate to **Global Profiles → Topology Hiding** (not shown).

- Click **default** profile and select **Clone** (not shown)
- Enter Profile Name : **Avaya_SM**
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Destination IP** under **Replace Action**
- Click **Finish** (not shown)

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

Topology Hiding Profiles: Avaya_SM

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya_SM

Motto

Rename

Clone

Delete

Click here to add a description.

Topology Hiding

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

Edit

7.2.7. Topology Hiding – Motto VoIP

The **Topology Hiding** screen manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. Navigate to **Global Profiles → Topology Hiding** (not shown).

- Click **default** profile and select **Clone** (not shown)
- Enter Profile Name : **Motto**
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Override Value** type **mottovoip.nl**
- Click **Finish** (not shown)

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

Topology Hiding Profiles: Motto

Add

Topology Hiding Profiles

- default
- cisco_th_profile
- Avaya_SM
- Motto**

Rename Clone Delete

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Override Value
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	mottovoip.nl
SDP	IP/Domain	Auto	---
From	IP/Domain	Overwrite	mottovoip.nl
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	mottovoip.nl

Edit

7.3. Device Specific Settings

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

7.3.1. Network Management

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

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

The screenshot shows the 'Network Management: GSSCP_03' interface. On the left, a sidebar lists 'Devices' with 'GSSCP_03' selected. The main area has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning banner states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.128), and 'B2 Netmask'. An 'Add' button is next to the A1 field, and 'Save' and 'Clear' buttons are on the right. Below these is a table with columns: IP Address, Public IP, Gateway, and Interface. The table contains two rows: one for A1 with IP 10.10.3.30 and Gateway 10.10.3.1, and one for B1 with IP 192.168.122.55 and Gateway 192.168.122.1. Each row has a 'Delete' button next to the interface name.

IP Address	Public IP	Gateway	Interface	
10.10.3.30		10.10.3.1	A1	Delete
192.168.122.55		192.168.122.1	B1	Delete

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

The screenshot shows the 'Network Management: GSSCP_03' interface with the 'Interface Configuration' tab selected. It displays a table with columns 'Name' and 'Administrative Status'. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled). Each row has a 'Toggle' button next to the status.

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

7.3.2. Media Interface

The Media Interface screen allows the IP address and ports to be set for transporting Media over the SIP trunk. The Avaya SBCE listens for SIP media on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface**.

- Select **Add**
- **Name: Int_Media**
- **Media IP: 10.10.3.30** (Internal address for calls toward Communication Manager)
- **Port Range: 35000-40000**
- Click **Finish**
- Select **Add**
- **Name: Ext_Media**
- **Media IP: 192.168.122.55** (External address for calls toward Motto VoIP)
- **Port Range: 35000-40000**
- Click **Finish**

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

Media Interface: GSSCP_03

Devices

GSSCP_03

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	Port Range	
Int_Media	10.10.3.30	35000 - 40000	Edit Delete
Ext_Media	192.168.122.55	35000 - 40000	Edit Delete

7.3.3. Signalling Interface

The Signalling Interface screen allows the IP Address and ports to be set for transporting signaling messages over the SIP trunk. The Avaya SBCE listens for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**.

- **Name: Int_Sig**
- **Signaling IP: 10.10.3.30** (Internal address for calls toward Communication Manager)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**
- Select **Add**
- **Name: Ext_Sig**
- **Signaling IP: 192.168.122.55** (External address for calls toward Motto VoIP)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**

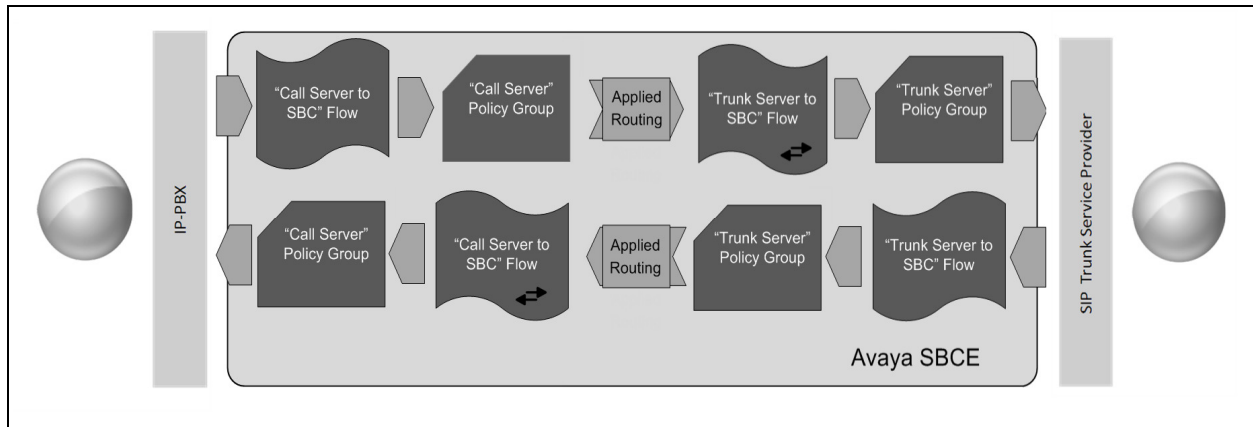
The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

Signaling Interface: GSSCP_03

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30	5060	5060	---	None	Edit Delete
Ext_Sig	192.168.122.55	5060	5060	---	None	Edit Delete

7.3.4. End Point Flows

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



To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow**.

- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.4** and **7.2.5** and assign to the Flow
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration
- **End Point Policy Group:** Select the policy assigned to the Server Configuration
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration

Click **Finish** to save and exit.

The following screen shows the Sever Flow for Session Manager.

Flow: Call_Server	
Flow Name	Call_Server
Server Configuration	Avaya_SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	Motto
Topology Hiding Profile	Avaya_SM
File Transfer Profile	None
<button>Finish</button>	

The following screen shows the Sever Flow for Motto VoIP.

Flow: Trunk_Server	
Flow Name	Trunk_Server
Server Configuration	Motto
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya_SM
Topology Hiding Profile	Motto
File Transfer Profile	None
<button>Finish</button>	

8. Motto VoIP SIP Trunk Configuration

The configuration of the Motto VoIP equipment used to support the Motto VoIP SIP Trunk Service is outside of 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 VoIP representative.

9. Verification Steps

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

1. From System Manager Home Tab click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**. The screenshot shows the status of the Entity Link for the Avaya SBCE

Home / Elements / Session Manager / System Status / SIP Entity Monitoring							
SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: Avaya SBCE							
Summary View							
1 Item Refresh							
Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.9.71	5060	TCP	Up	200 OK	Up

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

```
status trunk 1
```

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

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 for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
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, check from the Avaya SBCE using OPTIONS. This is done by defining the heartbeat in the Server configuration then running a trace. To define the heartbeat, navigate to **Global Profiles → Server Configuration** in the menu on the left hand side and click on the Trunk Server profile. Select the **Heartbeat** tab and click on **Edit**
 - Check the **Enable Heartbeat** box
 - Select **OPTIONS** from the **Method** drop down menu
 - Enter the **Frequency** in seconds, for convenience this can be set to the minimum value of **60** seconds
 - Enter the **From URI** in Fully Qualified Domain Name format
 - Enter the **To URI** in FQDN format
 - Click on **Finish**

Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	300 seconds
From URI	PING@192.168.10.99
To URI	PING@192.168.10.130
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
Finish	

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

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the Service Provider's 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 shows a web-based configuration interface for packet capture. On the left, a sidebar contains a 'Devices' section with a list of devices, including 'GSSCP_03'. The main area has three tabs: 'Call Trace', 'Packet Capture' (which is selected), and 'Captures'. The 'Packet Capture' tab displays a 'Packet Capture Configuration' form. The form includes a 'Status' field set to 'Ready'. Below this, a red rectangular box highlights the configuration fields: 'Interface' (set to 'B1'), 'Local Address' (set to '192.168.1.1'), 'Remote Address' (set to '*'), 'Protocol' (set to 'All'), 'Maximum Number of Packets to Capture' (set to '10000'), and 'Capture Filename' (set to 'options.pcap'). At the bottom of the form are 'Start Capture' and 'Clear' buttons.

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 200 OK response will be seen from the Service Provider.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Motto VoIP SIP Trunk Service. The service was successfully tested with observations listed in **Section 2.2**.

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform Release 6.2*, March 2012.
- [2] *Administering Avaya Aura® System Platform Release 6.2*, February 2012.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.2, February 2012.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, February 2012, Document Number 555-245-205.
- [5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.
- [6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473.
- [7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.
- [8] *Avaya One-X® Communicator Getting Started*, November 2009, Document Number 03-600758.
- [9] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2
- [10] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2]
- [11] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2013 Avaya Inc. All Rights Reserved.

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

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