

Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support Eircom SIP Trunk Service - Issue 1.0

## Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Eircom 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. Eircom is a member of the DevConnect Service Provider program.

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.

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 Eircom's 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. Customers using this Avaya SIP-enabled enterprise solution with Eircom 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 use the SIP Trunking service provided by Eircom.

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 the SIP Trunk provided by Eircom, calls made to SIP, H.323, Digital and Analogue telephones at the enterprise
- All inbound PSTN calls were routed to the enterprise across the SIP trunk to Eircom
- Outgoing calls from the enterprise site completed via Eircom's SIP Trunk to PSTN destinations, calls made from SIP, H.323, Digital and Analogue telephones
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to Eircom
- Inbound and outbound PSTN calls to/from Avaya One-X Communicator and Avaya Flare Experience for Windows softphones
- Calls using the G.729 and G.711A codecs
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38
- Caller ID Presentation and Caller ID Restriction
- DTMF transmission using RFC 2833
- Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer and conference
- Call coverage and call forwarding for endpoints at the enterprise site
- Off-net call forwarding and twinning

## 2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Eircom's SIP Trunk Service with the following observations:

- Inbound Toll-Free calls were not tested as no Toll-Free access was available for test.
- Emergency Services access was not tested as an Emergency Services test call was not booked with the Operator.

## 2.3. Support

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

For technical support on Eircom products please contact Eircom Customer Care at:

- Telephone: 1800 255 255
- Telephone: +353 1 4688530
- Email: <u>servicedesk@eircom.ie</u>

# 3. Reference Configuration

The following equipment in **Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Eircom's SIP Trunk. 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 16xx series IP telephones (with 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 Flare for Windows running on a laptop PC.

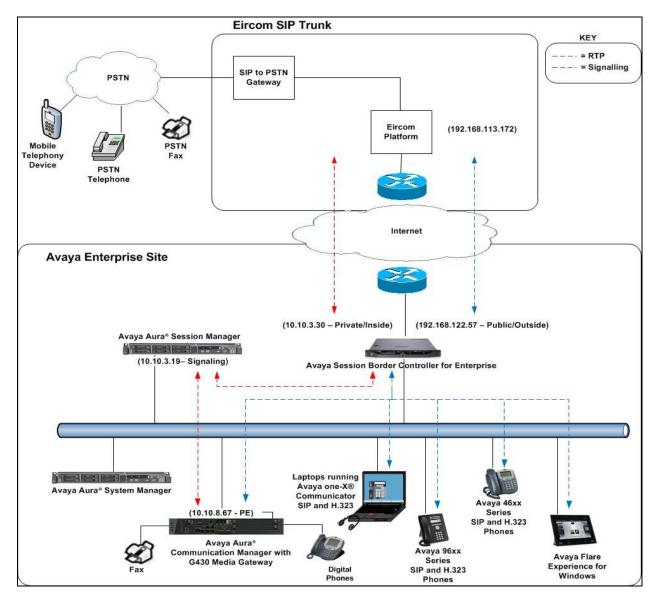


Figure 1: Test Setup Eircom SIP Trunk to Avaya Enterprise

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running Session	R6.3.9 - 6.3.9.0.639011
Manager on VM Version 8	
Dell PowerEdge R620 running System	R6.3.9 - Build No 6.3.0.8.5682-
Manager on VM Version 8	6.3.8.4417
	Software Update Revision No:
	6.3.9.1.2538
Avaya S8800 Server running	R016x.03.0.124.0 -21291
Communication Manager	
Avaya Session Border Controller for	6.2.1.Q7
Enterprise	
Avaya 16xx IP DeskPhone (H.323)	6.3
Avaya 96x0 IP DeskPhone (H.323)	6.3
Avaya 46xx IP DeskPhone (H.323)	6.2.2
Avaya 96x0 IP DeskPhone (SIP)	6.2.2
Avaya 96x1 IP DeskPhone (SIP)	6.2.2
Avaya one–X® Communicator (H.323) on	6.1.8.06-SP8-40314
Lenovo T510 Laptop PC	
Avaya Flare Experience for Windows	1.1.3.14
Avaya Digital Handset	Rel 12.0
Analogue Handset	N/A
Analogue Fax	N/A
Eircom	
Eircom SIP Trunk Service	Broadsoft Broadworks rel 19SP1
	Ericsson IMS rel 13A
	AcmePacket SD running on 4500
	platform, software release 6.4

# 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 Eircom SIP Trunk. For incoming calls, Session Manager receives SIP messages from the Avaya SBC for Enterprise (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

CMN; Reviewed: SPOC 12/8/2014 Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 5 of 55 EIR\_CMSM63SBC directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Eircom 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 Eircom SIP Trunk 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:	41000	0		
Maximum Video Capable IP Softphones:	18000	0		
Maximum Administered SIP Trunks:	24000	10		
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0		
Maximum Number of DS1 Boards with Echo Cancellation:	522	0		
Maximum TN2501 VAL Boards:	128	0		
Maximum Media Gateway VAL Sources:	250	1		
Maximum TN2602 Boards with 80 VoIP Channels:	128	0		
Maximum TN2602 Boards with 320 VoIP Channels:	128	0		
Maximum Number of Expanded Meet-me Conference Ports:	300	0		

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

```
display system-parameters customer-options
                                                                      4 of 11
                                                               Page
                               OPTIONAL FEATURES
   Emergency Access to Attendant? y
                                                                IP Stations? y
          Enable 'dadmin' Login? y
                                                          ISDN Feature Plus? n
          Enhanced Conferencing? y
                                        ISDN/SIP Network Call Redirection? y
                 Enhanced EC500? y
   Enterprise Survivable Server? n
                                                            ISDN-BRI Trunks? y
      Enterprise Wide Licensing? n
                                                                   ISDN-PRI? y
                                                 Local Survivable Processor? n
             ESS Administration? y
         Extended Cvg/Fwd Admin? y
                                                       Malicious Call Trace? y
    External Device Alarm Admin? y
                                                   Media Encryption Over IP? y
 Five Port Networks Max Per MCC? n
                                     Mode Code for Centralized Voice Mail? n
               Flexible Billing? n
   Forced Entry of Account Codes? y
                                                   Multifrequency Signaling? y
     Global Call Classification? y
                                          Multimedia Call Handling (Basic)? y
                                        Multimedia Call Handling (Enhanced)? y
           Hospitality (Basic)? 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, **SM100** and **10.10.3.19** are the **Name** and **IP Address** for Session Manager SIP interface. Also note the **procr** name, as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

display node-names	ip	
	I	IP NODE NAMES
Name	IP Address	
SM100	10.10.3.19	
default	0.0.0.0	
procr	10.10.8.67	
procr6	::	

## 5.3. Administer IP Network Region

Use the **change ip-network-region x** command where x is the desired network-region to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, 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 **1** is used.
- The rest of the fields can be left at default values.

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

## 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.** Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec supported by Eircom was configured, namely **G.729** and **G.711A**.

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

    IP Codec Set

    Codec Set: 1

    Audio
    Silence

    Codec
    Suppression

    Per Pkt
    Size(ms)

    1: G.729
    n

    2
    20

    2: G.711A
    n

    2
    20
```

Eircom SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define fax properties as follows:

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

change ip-codec-set	t 1			Page	2 of	2
	IP Codec Set	Ę				
	Allow D	irect-IP Multimedi	a? n			
	Mode	Redundancy				
FAX	t.38-standard	0	ЕСМ У			
Modem	off	0				
TDD/TTY	US	3				
Clear-channel	n	0				

## 5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Eircom SIP Trunk network. During test, this was configured to use TCP and port 5060 to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of 5061 for security. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set Group Type to sip
- Set Transport Method to tcp
- Set **Peer Detection Enabled** to **y** allowing the 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 (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set Near-end Listen Port and Far-end Listen Port to 5060 (Commonly used TCP port value)
- 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 network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk )
- Set Direct IP-IP Audio Connections to y
- Set Initial IP-IP Direct Media to n
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

```
Page 1 of 2
add signaling-group 1
                              STGNALING GROUP
Group Number: 1
                            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
  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:
                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate
                                           RFC 3389 Comfort Noise? n
                                         Direct IP-IP Audio Connections? y
        DTMF over IP: rtp-payload
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 x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the Group Type field to sip
- Choose a descriptive Group Name
- Specify a trunk access code (TAC) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the Service Type field to public-netwrk
- 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 1
      Page 1 of 21

      TRUNK GROUP
      TRUNK GROUP

      Group Number: 1
      Group Type: sip
      CDR Reports: y

      Group Name: OUTSIDE CALL
      COR: 1
      TN: 1
      TAC: 101

      Direction: two-way
      Outgoing Display? n
      Outgoing Display? n

      Dial Access? n
      Night Service:
      Queue Length: 0

      Service Type: public-ntwrk
      Auth Code? n
      Member Assignment Method: auto

      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 Eircom to prevent unnecessary SIP messages during call setup.

```
add trunk-group 1

Group Type: sip

TRUNK PARAMETERS

Unicode Name: auto

Redirect On OPTIM Failure: 10000

SCCAN? n

Digital Loss Group: 18

Preferred Minimum Session Refresh Interval(sec): 900

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 allows delivery of CLI in national formats.

add trunk-group 1 TRUNK FEATURES		Page 3	of 21
ACA Assignment? n	Measured:	none Maintenance Te	ests? y
Numbering Format:	-	UUI Treatment: service-p	provider
		Replace Restricted Numb Replace Unavailable Numb	

On Page 4 of this form:

- Set Mark Users as Phone to y
- Set Send Transferring Party Information to n
- Set Network Call Direction to n
- Set Send Diversion Header to y
- Set Support Request History to n
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Eircom
- Set Always Use re-INVITE for Display Updates to y
- Set the Identity for Calling Party Display to P-Asserted-Identity

add trunk-group 1	Page	<b>4</b> of 21	
PROTOCOL VARIATIONS			
Mark Users as Phone?	У		
Prepend '+' to Calling/Alerting/Diverting/Connected Number?	n		
Send Transferring Party Information?	n		
Network Call Redirection?	n		
Send Diversion Header?	У		
Support Request History?	n		
Telephone Event Payload Type:	101		
Convert 180 to 183 for Early Media?	n		
Always Use re-INVITE for Display Updates?	У		
Identity for Calling Party Display:	P-Assert	ted-Identity	
Block Sending Calling Party Location in INVITE?	n		
Accept Redirect to Blank User Destination?			
Enable O-SIP?			

## 5.7. Administer Calling Party Number Information

Use the **change private-numbering x** command to configure Communication Manager to send the calling party number in the format required. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

cha	nge private-num	bering O			Page 1 of 2
		NU	MBERING - PRIVATE	FORMA	Т
E.+	Ext	Trk	Private	Total	
LXC	EXC	TIK	Private	TOLAL	
Len	Code	Grp(s)	Prefix	Len	
4	60	1	0768nnnn10	10	Total Administered: 2
4	61	1	0768nnnn11	10	Maximum Entries: 540

Note: The above configuration accepts all **4** digit numbers starting with **6**, which includes all SIP and H.323 extension numbers, and passes them on with no prefix.

## 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 Eircom's SIP Trunk. 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: 7			
Auto Route Selection (ARS) - Access Code 1: 9 Access Co	de 2:		

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0	P		GIT ANALY Location:		LE	Page 1 of 2 Percent Full: 0
Dialed	Tot	al	Route	Call	Node	ANI
String	Min	Max	Pattern	Туре	Num	Reqd
0	11	14	1	pubu		n
00	13	15	1	pubu		n
0035391	13	13	1	pubu		n
030	10	10	1	pubu		n
0800	8	10	1	pubu		n
0900	8	8	1	pubu		n
118	3	6	1	pubu		n

Use the **change ars digit-conversion x** command to change a dialled number for more efficient routing. As Eircom require a prefix 0 to be inserted before all dialled numbers for calls to route correctly, the **change ars digit-conversion 0** replaces the need of a Session Manager Adaptation or Avaya SBCE Sigma Script resulting in less header manipulation and SBC processing. The example entry shown will match outgoing calls to national and international numbers beginning with 0.

change ars digit-conve	1 of	2						
	ARS D			ION TABLE				
			Locatio	n: all	Perce	ent	Full:	0
Matching Pattern	Min	Max	Del	Replacement String	Net	Con	V ANI	Req
0	1	16	0	0	ars	У		n
								n

Use the **change route-pattern x** command, where **x** is an available route pattern, 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**. **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 1
                                                           Page
                                                                 1 of
                                                                       3
                Pattern Number: 1 Pattern Name:
SCCAN? n Secure SIP? n
                                      Pattern Name:
   Grp FRL NPA Pfx Hop Toll No. Inserted
                                                                 DCS/ IXC
   No Mrk Lmt List Del Digits
                                                                 OSIG
                          Dqts
                                                                 Intw
 1:1 0
                                                                 n
                                                                     user
 2:
                                                                     user
                                                                 n
 3:
                                                                 n
                                                                     user
    BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR
   012M4W Request
                                                     Dgts Format
                                                   Subaddress
1: yyyyyn n
                                                           unk-unk none
                           rest
 2: yyyyyn n
                           rest
                                                                    none
 3: yyyyyn n
                           rest
                                                                    none
```

## 5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Eircom 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 Eircom correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **0768xxxxxxx** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DID numbers have been masked for security purposes.

change inc-cal	change inc-call-handling-trmt trunk-group 1				3
Service/	Number Numbe	er Del Insert			
Feature	Len Dig:	ts			
public-ntwrk	10 0768nnnn:	l0 all 6010			
public-ntwrk	10 0768nnnn:	1 all 6012			
public-ntwrk	10 0768nnnn:	l2 all 6102			

## 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 6102. 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. **089434nnnn**)
- Set the **Trunk Selection** to **ARS**
- Set the **Config Set** to **1**

change off-pb	x-telephone st	ation-mapp	ing 2396		Page 1	of 3
	STATIONS	WITH OFF-P	BX TELEPHONE INT	EGRATION		
Station	Application	Dial CC	Phone Number	Trunk	Config	Dual
Extension		Prefix		Selection	Set.	Mode
6102	EC500	-	089434nnnn	ARS	1	110 40
0101	20000		00010111111	1110	-	
-						

**Note:** The phone number shown is for a mobile phone used for testing at Avaya Labs and is in national format with national dialling prefix 0. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

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

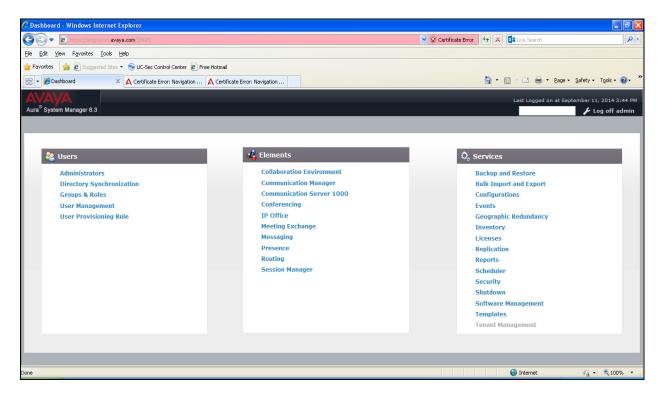
# 6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via 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

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

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



### 6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements**  $\rightarrow$  **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.

Home / Elements / Routing / Domains			11 Notes of
Domain Management			Help ?
New Edit Delete Duplicate More Actions •			
1 Item			Filter: Enable
Name	Туре	Notes	
avava.com	sip		
Select : All, None			

### 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**  $\rightarrow$ **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 **VM\_SMGR** defined for the compliance testing.

Name:: VM_SMGR Notes:	Home / Elemen	its / Routing / Locations			
Name:: VM_SMGR Notes:	Location Details	5			Commit Cancel
Notes: Dial Plan Transparency in Survivable Mode  Listed Directory Number: Associated CM SIP Entity:  Overall Managed Bandwidth Managed Bandwidth Units: Kbit/sec  Associated CM SIP Entity:  Overall Managed Bandwidth Managed Bandwidth Units: Kbit/sec  Total Bandwidth:  Total Bandwidth:  Audio Calls Can Take Multimedia Bandwidth:  Per-Call Bandwidth Parameters  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec	General				
Notes: Dial Plan Transparency in Survivable Mode  Listed Directory Number: Associated CM SIP Entity:  Overall Managed Bandwidth Managed Bandwidth Units: Kbit/sec  Associated CM SIP Entity:  Overall Managed Bandwidth Managed Bandwidth Units: Kbit/sec  Total Bandwidth:  Total Bandwidth:  Audio Calls Can Take Multimedia Bandwidth:  Per-Call Bandwidth Parameters  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec		* Name:	VM SMGR		
Dial Plan Transparency in Survivable Mode  Enabled: Listed Directory Number: Associated CM SIP Entity: Overall Managed Bandwidth Managed Bandwidth Units: Kbit/sec Total Bandwidth: Dultimedia Bandwidth: Current 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			14 BOOK		
Enabled:   Listed Directory Number:   Associated CM SIP Entity:   Overall Managed Bandwidth   Managed Bandwidth Units:   Kbit/sec   Total Bandwidth:   Multimedia Bandwidth:   Multimedia Bandwidth:   Per-Call Bandwidth Parameters   Maximum Multimedia Bandwidth (Intra-Location):   2000 Kbit/Sec   Maximum Multimedia Bandwidth (Intra-Location):   2000 Kbit/Sec   Maximum Multimedia Bandwidth (Intra-Location):   2000 Kbit/Sec		Notes:			
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	Dial Plan Tra	nsparency in Survivable Mode			
Associated CM SIP Entity:		Enabled:			
Overall Managed Bandwidth          Managed Bandwidth Units:       Kbit/sec         Total Bandwidth:		Listed Directory Number:	[		1
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 (Intra-Location): 2000 Kbit/Sec Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec Inter Inter In		Associated CM SIP Entity:			
Total Bandwidth: Multimedia Bandwidth: Multimedia Bandwidth: Audio Calls Can Take Multimedia Bandwidth: Per-Call Bandwidth Parameters Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec	Overall Man	aged Bandwidth			
Multimedia Bandwidth: Audio Calls Can Take Multimedia Bandwidth: Per-Call Bandwidth Parameters Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec		Managed Bandwidth Units:	Kbit/sec 💌		
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  ation Pattern  Remove  ID Address Pattern  ID A		Total Bandwidth:			
Per-Call Bandwidth Parameters  Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec  Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec  ation Pattern  Remove  IP Address Pattern  ID 10.0.2*  ID 10.0.3*		Multimedia Bandwidth:			
Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec ation Pattern Remove IP Address Pattern 10:10:2.* 10:10:3.* 10:10:10:3.* 10:10:10:3.* 10:10:10:10:3.* 10:10:10:10:10:10:10:10:10:10:		Audio Calls Can Take Multimedia Bandwidth:			
Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec	Per-Call Bar	dwidth Parameters			
IP Adress Pattern     Notes       10:10:2.*		Maximum Multimedia Bandwidth (Intra-Location):	2000	Kbit/Sec	
Remove         Filter           IP Adress Patran         Nets           10.10.2.*            10.10.3.*            10.10.3.*            10.10.3.*            10.10.3.*            10.10.3.*            10.10.3.*            10.10.3.*            10.10.3.*            10.10.3.*            10.10.9.*		Maximum Multimedia Bandwidth (Inter-Location):	2000	Kbit/Sec	
Imm         Imp         Imp <td>cation Pattern</td> <td></td> <td></td> <td></td> <td></td>	cation Pattern				
IP Adress Pattern     Notes       10.10.2.*        10.10.3.*        10.10.5.*        10.10.7.*        10.10.6.*        10.10.9.*        10.10.9.*	d Remove				
* 10.10.2.* * 10.10.3.* 10.10.5.* * 10.10.7.* * 10.10.7.* * 10.10.9.* * 10.10.9.* * 10.10.9.* * 10.10.9.*	tems 🤃				Filter: Ena
* 10.10.3.* * 10.10.5.* * 10.10.7.3.* * 10.10.9.* * 10.10.9.* * 10.10.9.*		Notes			
* 10.10.5.* * 10.10.73.* * 10.10.8.* * 10.10.9.* *					
* 10.10.73.* * 10.10.8.* * 10.10.9.* *					
* 10.10.8.* * 10.10.9.* *					
*					
	ect : All, None				

## 6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. The example below was applied to the Avaya SBCE SIP Entity and was used in test to convert numbers being passed between the Avaya SBCE and Session Manager.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown). Under **Adaption Details**  $\rightarrow$  **General**:

- In the Adaptation name field enter an informative name.
- In the **Module name** field click on the down arrow and then select the <**click to add module**> entry from the drop down list and type **DigitConversionAdapter** in the resulting New Module Name field.
- Module Parameter Type MIME =no Strips MIME message bodies on egress from Session Manager

Seneral  * Adaptation Name: Eircom Module Name: DigitConversionAdapter Module Parameter Type: Name-Value Parameter  Add Remove Add Remove Fromto true Fromto true Select : All, None Egress URI Parameters:	daptation Details			Commit	Cancel	Help
Module Name: DigitConversionAdapter  Module Parameter Type: Name-Value Parameter  Add Remove Name Value fromto fromto Kute Select : All, None	eneral					1
Module Parameter Type: Name-Value Parameter  Add Remove Add Remove fromto fromto MIME no Select : All, None		* Adaptation Name:	Eircom			
Add Remove   Name Value   fromto true   MIME no   Select : All, None		Module Name:	DigitConversionAdapter			
Name     Value       fromto     true       MIME     no       Select : All, None		Module Parameter Type:	Name-Value Parameter	~		
Name     Value       fromto     true       MIME     no       Select : All, None			Add Remove			
ifromto     true       MIME     no       Select : All, None					Value	
Select : All, None					true	
			MIME		no	
Egress URI Parameters:			Select : All, None			

fromto=true Modifies from and to headers of a message

Scroll down the page and under **Digit Conversion for Incoming Calls to SM**, click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so **both** have been selected.

Digi Add	t Conversion for D Remove	Incomi	ing Call	s to SM						
1 Ite	m 🍣									Filter: Enable
	Matching Pattern 🔺	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes	
	* +353	* 4	* 16		* 4	0	both 💌			
Sele	t : All, None							-		

This will ensure any incoming numbers will have the +353 digits removed and 0 digit inserted before being presented to Communication Manager.

## 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 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 **SIP Trunk** for the Avaya SBCE 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 four SIP Entities.

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

#### 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 Session Manager SIP signalling interface and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

SIP Entity Details		Commit] Cancel	Help ?
		Commit Cancer	
General			
	* Name:	Session_Manager	
	* FQDN or IP Address:	10.10.3.19	
	Type:	Session Manager	
	Notes:		
	Location:	VM_SMGR V	
	Outbound Proxy:		
	Time Zone:	Europe/Dublin	
	Credential name:		
SIP Link Monitoring	L		
	SIP Link Monitoring:	Use Session Manager Configuration 💌	

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

and the second	Failover port: Failover port: Remove				
3 Iter	ns				Filter: Enable
	Port 🔺	Protocol	Default Domain	Notes	
	5060	TCP 💌	avaya.com 💌		
	5060	UDP 💌	avaya.com 💌		
	5061	TLS 💌	avaya.com 🔽		
Selec	t : All, None				

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

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signaling and **Type** is **CM**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

Home / Elements / Routing / SIP Entities		0
SIP Entity Details	Commit) Cancel	Help ?
General		
* Na	me: Communication_Manager	
* FQDN or IP Add	ess: 10.10.8.67	
т	/pe: CM	
No	tes:	
Adapta	ion:	
Loca	ion: VM_SMGR 💌	
Time Z	Dine: Europe/Dublin	
* SIP Timer B/F (in secon	ds): 4	
Credential na	me:	
Call Detail Record	ing: none 💌	
Loop Detection		
Loop Detection M	ode: Off 💌	
SIP Link Monitoring		
	ing: Use Session Manager Configuration 💌	

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:	Off •
SIP Link Monitoring		
	SIP Link Monitoring:	Use Session Manager Configuration 💌

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

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set **Type** to **SIP Trunk** and **Adaptation** to that defined in **Section 6.4**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Rout	ing / SIP Entities		
SIP Entity Details		(Commit) (Cancel)	Help ?
General			
	* Name:	Avaya_SBCE	
	* FQDN or IP Address:	10.10.3.30	
	Туре:	SIP Trunk	
	Notes:		
	Time Zone:	VM_SMGR	
	* SIP Timer B/F (in seconds):	4	
	Credential name: Call Detail Recording:	egress 💌	
Loop Detection	Loop Detection Mode:	Off 💌	
SIP Link Monitoring		Use Session Manager Configuration 💌	

## 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 **Protocol** field enter the transport protocol to be used to send SIP requests
- 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 **Trusted** from the drop-down menu to make the other system trusted

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

Hon	me	/ Elements / Routing / Entity Links									C
Ent	100.05	/ Links									Help ?
5 I	Ite	ms 🥏								Filter:	Enable
		Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS	Port	Connection Policy	Deny New Service	Notes
		Avaya SBCE	Session_Manager	TCP	5060	Avaya_SBCE		5060	trusted		
		Communication Manager	Session_Manager	TCP	5060	Communication_Manager		5060	trusted		
E		CS1K R7.6	Session_Manager	TCP	5060	CS1K_R7.6		5060	trusted		
E		Mesaging	Session_Manager	TCP	5060	Messaging		5060	trusted		

## 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 Communication Manager.

lome / Elements / Routing / Rout	ng Foncies							_				Help ?
touting Policy Details						Com	mit Cance					Second Second
Seneral		Disa * Re	Name: to_ abled: etries: 0 Notes:	_Communi	cation_Ma	nager		]				
Select					FQDI	N or IP Addr	ess			Туре	Notes	
Select						N or IP Addr 10.8.67	ess			Туре СМ	Notes	
Select	aps						ress					r: Enable
Select) Iame Communication_Manager Ime of Day Add (Remove) (View Gaps/Over	laps Mon	Tue	Wed	Thu			Sun	Start Time	End Time			r: Enable
ame Communication_Manager ime of Day add (Remove) (View Gaps/Over Item 2		Tue	Wed	Thu	10.1	10.8.67		Start Time 00:00	End Time 23:59	СМ	Filter	r: Enable

The following scree	n shows the Rout	ing Policy fo	or the Avaya SBCE.
$\mathcal{O}$		0	2

												Help ?
outing Policy Details						Con	nmit Cano	cel				
Seneral		Disa * Re	Name: to_/ abled:	Avaya_SE	3CE							
IP Entity as Destination			1							-		
ame		2	1.00.000	N or IP Add	dress					Туре	Notes	
elect		2	1.00.000	N or IP Ad 0.9.71	dress					Type SIP Trunk	Notes	
ame Avaya_SBCE ime of Day dd Remove View Gaps/Ove	laps		1.00.000		dress				_		Notes	Filter: Enable
elect) ame waya_SBCE me of Day dd Remove View Gaps/Ove	laps	Tue	1.00.000		dress Fri	Sat	Sun	Start Time	End Time			Filter: Enable
ieled ame Avaya_SBCE ime of Day dd Remove View Gaps/Ove Item 2		Tue	10.1	0.9.71		Sat	Sun	Start Time 00:00	End Time 23:5	SIP Trunk		Filter: Enable

## 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.

ome / Elements / Routing / Dial P	atterns					
al Pattern Details			Commit Can	cel		Help
General				1		
	* Pattern: 00	353				
	* Min: 5					
	* Max: 20	1				
	Emergency Call:					
	Emergency Type:					
	SIP Domain: -A	LL- 💌				
	Notes:					
				No.		
riginating Locations and I	Routing Policies					
Item 🥲						Filter: Enabl
Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
VM_SMGR		to_Avaya_SBCE	0		Avaya_SBCE	
elect : All, None						

The following screen shows an example dial pattern configured for the Avaya SBCE.

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

me / Elements / Routing / Dial Patterns					
al Pattern Details		Commit Cancel			Help ?
eneral					
* Pattern:	07689				
* Min:	5				
* Max:	16				
Emergency Call:					
Emergency Priority:	1				
Emergency Type:					
SIP Domain:	-ALL-				
Notes:					
riginating Locations and Routing Policies					
dd Remove					
Item 🧶					Filter: Enable
Originating Location Name 🔺 Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
VM_SMGR	to_Communication_Manager	o		Communication_Manager	
elect : All, None					-

# 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of 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 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.



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.

🖉 Dashboard - Avaya Session Borde	er Controller for Enterprise -	Windows Internet Explorer			- 7 🛛	
A https://10.10.2.55/sbc/	1			🕑 😵 Certificate Error 🛛 🗟 🖅 🗶 🧕 Eive Search	P -	
Ele Edit View Favorites Tools Help						
👷 Favorites 🛛 🎭 🖻 Supposted Sites 🔹 🕤 UC-Sec Control Center 🔊 Free Hotmal						
🔠 👻 🗛 Dashboard - Avaya Sessi 🗙	//smgr1cmn.avaya.co	Cashboard		🏠 • 🔂 - 🖻 🖶 • Bage •	Safety • Tools • 🕢 • 👋	
Alarms Incidents Statistic	cs Logs Diagnostics	Users		Setting	is Help Log Out	
Session Borde	er Controller	for Enterprise			AVAYA	
Dashboard	Dashboard				~	
Administration		Information		Installed Devices		
Backup/Restore	System Time	12:16:19 PM GMT	Refresh	EMS		
System Management Global Parameters	Version	6.2.1.Q07		GSSCP 03		
<ul> <li>Global Profiles</li> </ul>	Build Date	Mon Dec 9 17:33:02 CST 2013				
Domain DoS						
Fingerprint		Alarms (past 24 hours)		Incidents (past 24 hours)		
Server Interworking	None found.			GSSCP_03: No Subscriber Flow Matched		
Phone Interworking				GSSCP_03: Method Prohibited Out-of-Dialog		
Media Forking				GSSCP_03: No Subscriber Flow Matched		
Routing Server Configuration				GSSCP_03: Method Prohibited Out-of-Dialog		
Topology Hiding				GSSCP_03: No Subscriber Flow Matched		
Signaling Manipulation					Add	
URI Groups	✓		No	tes		
				S Internet	🐴 • 🔍 100% • 💡	

CMN; Reviewed: SPOC 12/8/2014

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 30 of 55 EIR\_CMSM63SBC 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).

🖉 System Management - Avaya Sess	sion B	order Controller for Enterprise - W	indows Interne	t Explorer							
A https://10.10.2.55/sbc/	1					🖌 😵 Certificat	e Error	3 fg 🗙	o∎ Live Search		ρ.
Ele Edit View Favorites Tools H	<u>t</u> elp										
🖕 Favorites 🛛 👍 🙋 Suggested Sites 🔹	- 🕤 I	JC-Sec Control Center 🙋 Free Hotmail									
🔠 👻 🗛 System Management - Av 🗙	🏉 ht	tps://smgr1cmn.avaya.co 🏀 Dashboa	d					🟠 • 🛙	S - 🖃 🖶 - Ba	sge + <u>S</u> afety +	T <u>o</u> ols • 🔞 •
Alarms Incidents Statistic	cs	Logs Diagnostics Users							Se	ttings Hel	p Log Out
Session Borde	er (	Controller for E	nterpri	ise						4	VAYA
Dashboard Administration Backup/Restore	^	System Management									
System Management		Devices Updates SSL VPN	Licensing								
Global Parameters		Device Name		Management IP	Version	Status					
<ul> <li>Global Profiles</li> </ul>		(Serial Number) GSSCP 03									
Domain DoS		(IPCS31030010)		10.10.2.55	6.2.1.Q07	Commissioned	Reboot	Shutdown	Restart Application	n View Edit	t Delete
Fingerprint											
Server Interworking											
Phone Interworking											
Media Forking											
Routing											
Server Configuration											
Topology Hiding											
Signaling Manipulation											
URI Groups	~										
Done									😝 Internet		• 🔍 100% 🔹

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

General Configura	ition —	Device Conf	iguration —				
Appliance Name GSSCP_03		HA Mode	No				
Box Type	Type SIP		Two Bypass Mode No				
Deployment Mode	Proxy						
Network Configura	Public IP	Netmask	Gateway	Interfac			
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1			
192.168.122.57	192.168.122.57	255.255.255. <mark>1</mark> 28	192.168.122.7	B1			
	r	Managemen	nt IP(s)				
DNS Configuration			10.10.2.55				
DNS Configuration Primary DNS	8.8.8.8	IP	10.10.2.55				
	8.8.8.8 10.10.7.100	IP	10.10.2.55				
Sector Sector Contractors		IP	10.10.2.55				

## 7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

#### 7.2.1. Server Interworking - Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles**  $\rightarrow$  **Server Interworking** and click on **Add Profile.** 

- Enter profile name such as Avaya\_SM and click Next (Not Shown)
- Check Hold Support=None
- Check T.38 Support
- All other options on the General Tab can be left at default

	Profile: Avaya_SM	х
	General	
Hold Support	<ul> <li>None</li> <li>RFC2543 - c=0.0.0.0</li> <li>RFC3284 - a=sendonly</li> </ul>	2
180 Handling	None O SDP O No SDP	
181 Handling	None O SDP O No SDP	
182 Handling	None O SDP O No SDP	
183 Handling	None O SDP O No SDP	
Refer Handling		
URI Group	None 😒	
3xx Handling		
Diversion Header Support		13
Delayed SDP Handling		
Re-Invite Handling		
T.38 Support		
URI Scheme	SIP ○ TEL ○ ANY	
Via Header Format	<ul> <li>RFC3281</li> <li>RFC2543</li> </ul>	
	Next	

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

	Profile: Avaya_SM	Х
Record Routes	O None O Single Side O Both Sides	
Topology Hiding: Change Call-ID		
Call-Info NAT		
Change Max Forwards		
Include End Point IP for Context Lookup		
OCS Extensions		
AVAYA Extensions		
NORTEL Extensions		
Diversion Manipulation		
Diversion Header URI		
Metaswitch Extensions		
Reset on Talk Spurt		
Reset SRTP Context on Session Refresh		
Has Remote SBC		
Route Response on Via Port		
Cisco Extensions		
	Finish	

#### 7.2.2. Server Interworking – Eircom

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles**  $\rightarrow$  **Server Interworking** and click on **Add Profile**.

- Enter profile name such as **Eircom** and click **Next** (Not Shown)
- Check Hold Support = None
- Check T.38 Support
- All other options on the **General** Tab can be left at default

Click on Next on the following screens and then Finish

	Profile: Eircom
	General
Hold Support	<ul> <li>None</li> <li>RFC2543 - c=0.0.0.0</li> <li>RFC3264 - a=sendonly</li> </ul>
180 Handling	None     SDP     No SDP
181 Handling	None     SDP     No SDP
182 Handling	None     SDP     No SDP
183 Handling	None O SDP O No SDP
Refer Handling	
URI Group	None 😒
3xx Handling	
Diversion Header Support	
Delayed SDP Handling	
Re-Invite Handling	
T.38 Support	
URI Scheme	● SIP O TEL O ANY
Via Header Format	
	Next

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

	Profile: Eircom X
Record Routes	O None O Single Side O Both Sides
Topology Hiding: Change Call-ID	
Call-Info NAT	
Change Max Forwards	
Include End Point IP for Context Lookup	
OCS Extensions	
AVAYA Extensions	
NORTEL Extensions	
Diversion Manipulation	
Diversion Header URI	
Metaswitch Extensions	
Reset on Talk Spurt	
Reset SRTP Context on Session Refresh	
Has Remote SBC	
Route Response on Via Port	
Cisco Extensions	
	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.

Routing information is required for routing to Session Manager on the internal side and Eircom addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

Create a Routing Profile for both Session Manager and Eircom SIP trunk. To add a routing profile, navigate to **Global Profiles**  $\rightarrow$  **Routing** and select **Add Profile**. 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
• Next Hop Server 2:	Primary Next Hop server, e.g. Session Manager (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
Routing Priority Based on	
Next Hop Server:	Checked (not shown)
• Use Next Hop for	
In-Dialog Messages:	Select only if there is no secondary Next Hopserver (not shown)
Outgoing Transport:	Choose the protocol used for transporting outgoing signaling packets (not shown)

Click Finish.

The following screen shows the Routing Profile to Session Manager

Add	1			Rename Clone D
Routing Profiles				
efault	Routing Profile			
vaya_SM	J			7
F_UK		Next Hop Server 1		

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

Add	]					Rename Clone D
Routing Profiles			Click he	re to add a description.		
default	Routing Profile					
Avaya_SM		7				A
Eircom	Priority	URI Group	Next Hop Server 1	Next Hop Server 2	2	
	1 *		192.168.113.172		View Edit	

The following screen shows the Routing Profile to Eircom SIP Trunk.

#### 7.2.4. Server Configuration– Avaya Aura® Session Manager

Servers are defined for each server connected to the Avaya SBCE. In this case, Eircom is connected as the Trunk Server and Session Manager is connected as the Call Server. 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 left-hand menu select Global Profiles → Server Configuration and click on Add Profile and enter a descriptive name. On the Add Server Configuration Profile tab, set the following:

- Select Server Type to be Call Server
- Enter IP Addresses / Supported FQDNs to 10.10.3.19 (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

Server	r Configuration Profile - General	х
Server Type	Call Server 😽	
IP Addresses / Supported FQDNs Separate entries with commas	10,10.3.19	
Supported Transports	☑ TCP □ UDP □ TLS	
TCP Port	5060	
JDP Port		
TLS Port		

On the **Advanced** tab:

- Select Avaya\_SM for Interworking Profile defined in Section 7.2.1.
- Click **Finish**

Serve	r Configuration Profile - Advanced	Х
Enable DoS Protection		
Enable Grooming		
Interworking Profile	Avaya_SM 💌	
Signaling Manipulation Script	None 💌	
TCP Connection Type	SUBID ○ PORTID ○ MAPPING	

#### 7.2.5. Server Configuration – Eircom

To define the Eircom SBC as a Trunk Servers, navigate to select **Global Profiles**  $\rightarrow$  Server **Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select Server Type as Trunk Server
- Set IP Address to 192.168.113.172 (Eircom SIP Trunk)
- Supported Transports: Check UDP
- UDP Port: 5060
- Click **Next** (not shown)

Serve	er Configuration Profile - General	X
Server Type	Trunk Server	
IP Addresses / Supported FQDNs Separate entries with commas	192.168.113.172	
Supported Transports		
TCP Port		
UDP Port	5060	
TLS Port		
	Finish	

In the new window that appears, enter the following values as Eircom 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 **Next** to continue (not shown).

Server 0	Configuration Profile - Authentication	x
Enable Authentication		
User Name	pxxxxxxx_TG1@ngv.ein	
Realm (Leave blank to detect from server challenge)		
Password (Leave blank to keep existing password)		
Confirm Password	•••••	
	Finish	

In the new window that appears, enter the following values.

- 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
  - REGIST
- TO URI: Enter an URI to be sent in the TO header for SIP REGISTERS

Click **Next** to continue (not shown).

Enable Heartbeat		
Method	REGISTER 💌	
Frequency	300 seconds	
From URI	pxxxxxxx_TG1@ngv.eirc	
	pxxxxxxxx_TG1@ngv.eim	

On the **Advanced** tab:

- Select **Eircom** for **Interworking Profile** as defined in **Section 7.2.2**.
- Click **Finish**

Serve	er Configuration Profile - Advanced	х
Enable DoS Protection		
Enable Grooming		
Interworking Profile	Eircom M	
Signaling Manipulation Script	None	
UDP Connection Type	SUBID O PORTID O MAPPING	
UDP Connection Type	SUBID O PORTID O MAPPING     Finish	

### 7.2.6. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for Session Manager, navigate to **Global Profiles**  $\rightarrow$  **Topology Hiding** from menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as Avaya\_SM
- If the required Header is not shown, click on Add Header (not shown)
- Under the Header field for To, From and Request Line, select IP/Domain under Criteria and Overwrite under Replace Action. For Overwrite Value, insert avaya.com.
- Click **Finish** (not shown)

	Add				Rename Clone De
Topology Hiding Profiles	5	Cli	ick here to add a description.		
lefault	Topology Hiding				
isco_th_profile	Header	Criteria	Replace Action		Overwrite Value
Avaya_SM	Request-Line	IP/Domain	Overwrite	avaya.com	
lircom	Record-Route	IP/Domain	Auto	-	
	SDP	IP/Domain	Auto	-	
	Refer-To	IP/Domain	Auto	-	_
	From	IP/Domain	Overwrite	avaya.com	
	Referred-By	IP/Domain	Auto	-	
	То	IP/Domain	Overwrite	avaya.com	
	Via	IP/Domain	Auto	-	

To define Topology Hiding for Eircom, navigate to **Global Profiles**  $\rightarrow$  **Topology Hiding** from the menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive **Profile Name** such as **Eircom** and click **Next**
- If the required Header is not shown, click on Add Header
- Under the Header field for To, From and Request Line, select IP/Domain under Criteria and Overwrite under Replace Action. For Overwrite Value, insert ngv.eircom.net
- Click **Finish** (not shown)

Add				Rename Clone D
Topology Hiding Profiles		Clid	k here to add a description.	
efault	Topology Hiding			
sco_th_profile	Header	Criteria	Replace Action	Overwrite Value
vaya_SM	Request-Line	IP/Domain	Overwrite	ngv.eircom.net
rcom	Record-Route	IP/Domain	Auto	
	SDP	IP/Domain	Auto	-
	Refer-To	IP/Domain	Auto	-
	From	IP/Domain	Overwrite	ngv.eircom.net
	Referred-By	IP/Domain	Auto	
	То	IP/Domain	Overwrite	ngv.eircom.net
	Via	IP/Domain	Auto	

### 7.3. Define Network Information

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 interface assigned.

To define the network information, navigate to **Device Specific Settings**  $\rightarrow$  **Network Management** from the menu on the left-hand side and click on Add. Enter details in the blank box that appears at the end of the list

- Define the internal IP address and assign to interface A1
- Select Save Changes to save the information
- Click on Add
- Define the external IP address and assign to interface **B1**
- Select Save Changes to save the information
- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar (not shown)

Network Management	GSSCP_03				
Devices GSSCP_03		Configuration	re an application restart before taking effect	Application restarts can be issued	l from <u>System Management</u> .
	Changes will not take effect until the inte	erface is updated.			
	A1 Netmask 255.255.255.0	A2 Netmask	B1 Netmask 255.255.255	128 B2 Netmask	
	Add		100000 (121)		Save Clear
	IP Address		Public IP	Gateway	Interface
	10.10.3.30		10.10.3.1		A1 Delete
	192.168.122.57		192.168.122	.7	B1 Delete

Select the Interface Configuration tab and click on Toggle State to enable the interfaces.

Network Managemen	t: GSSCP_03		
Devices	Network Configuration Interface Configuration	ion	
GSSCP_03	Name	Administrative Stat	tus
	A1	Enabled	Toggle
	A2	Disabled	Toggle
	B1	Enabled	Toggle
	B2	Disabled	Toggle

### 7.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

#### 7.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings**  $\rightarrow$  **Signaling Interface** from the menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

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 Session Manager)
- TCP Port: 5060
- UDP Port: 5060
- Click **Finish**
- Select Add
- Name: Ext\_Sig
- Signaling IP: 192.168.122.57 (External address for calls toward Eircom)
- 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: GS	SCP_03								
Devices GSSCP_03	Signaling Interface								Add
	Name	Signaling IP	TCP Port	UDP Port	TLS Port		TLS Profile		
	Int_Sig	10.10.3.30	5060	5060		None		Edit	Delete
	Ext_Sig	192.168.122.57	5060	5060		None		Edit	Delete

#### 7.4.2. Media Interfaces

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**.

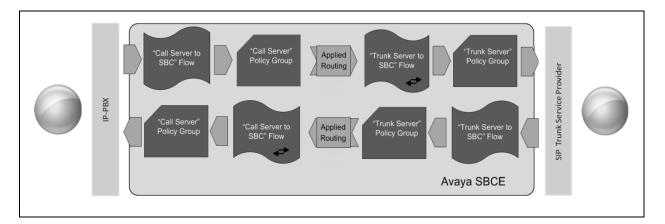
- Select Add
- Name: Int\_Media
- Media IP: 10.103.30 (Internal address for calls toward Session Manager)
- Port Range: 35000-51000
- Click Finish
- Select Add
- Name: Ext\_Media
- Media IP: 192.168.122.57 (External address for calls toward Eircom)
- Port Range: 35000-51000
- Click Finish

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

Media Interface: GSS	CP_03					
Devices GSSCP_03	Media Interface Modifying or deleting a	an existing media interface v	vill require an application restart before taking effect. Appli	cation restarts can be issued from <u>System Management</u>		
						Add
		Name	Media IP	Port Range		
	Int_Media		10.10.3.30	35000 - 51000	Edit	Delete
	Ext_Media		192.168.122.57	35000 - 51000	Edit	Delete

### 7.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Eircom's SIP Trunk and incoming flows from Eircom's SIP Trunk to Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from Session Manager to the PSTN via the Eircom network and vice versa. 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**  $\rightarrow$  End Point Flows. Select the **Server Flows** tab and click Add Flow.

•	Flow Name:	Enter a descriptive name
•		±
٠	Server Configuration:	Select a Server Configuration created in Section 7.2.4 and
	_	7.2.5 and assign to the Flow
•	<b>Received Interface:</b>	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
٠	Media Interface:	Select the Media Interface used to communicate with the
		Server Configuration
٠	<b>End Point Policy Group:</b>	Select the policy assigned to the Server Configuration
٠	<b>Routing Profile:</b>	Select the profile the Server Configuration will use to route
		SIP messages
-	Topology Hiding Drofiles	Select the modile to comby toward the Server Configuration

• Topology Hiding Profile: Select the profile to apply toward the Server Configuration

Click **Finish** to save and exit.

The following screen shows the Server 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	Eircom
Topology Hiding Profile	Avaya_SM
File Transfer Profile	None 😪
	Finish

The following screen shows the Server Flow for Eircom.

	Flow: Trunk_Server	>
Flow Name	Trunk_Server	
Server Configuration	Eircom 😪	
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	Eircom 💌	
File Transfer Profile	None 💌	
	Finish	

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Eircom SIP Trunk service and vice versa. The following screenshot shows all configured flows.



# 8. Configure Eircom SIP Trunk Equipment

The configuration of the Eircom equipment used to support Eircom's SIP Trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Eircom equipment and system configuration please contact an authorized Eircom 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.

								Help
es	sion Manager Enti	ty Link Connectic	on Statu	s				
	age displays detailed connectior	, status for all optitu links from						
	age displays detailed connection in Manager.	i status for all entity links from	Id					
All	Entity Links for Session M	lanager: Session_Manag	er					
				Status D	tails for the s	elected Session	Manager:	
				orates b		cieccea acosten	lanagen	
_								
S	Summary View			-				
_				<u></u>				Filter: Enable
_	Summary View tems Refresh							Filter: Enable
_		SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Filter: Enable
5 I	tems   Refresh	SIP Entity Resolved IP 10.10.8.67	Port 5060	Proto. TCP	Deny FALSE	Conn. Status UP	Reason Code 200 OK	
5 I )	tems Refresh SIP Entity Name	-	1010700			and the second s		Link Status
5 I 0	tems   Refresh SIP Entity Name <u>Communication Manager</u>	10.10.8.67	5060	ТСР	FALSE	UP	200 OK	Link Status
5 I 0 0 0	tems   Refresh SIP Entity Name <u>Communication Manager</u> <u>Avaya SBCE</u>	10.10.8.67 10.10.3.30	5060 5060	TCP TCP	FALSE	UP	200 OK 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 ti	runk 1			
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	in-service/idle	no	
0001/002	т00002	in-service/idle	no	
0001/003	т00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	
0001/005	т00005	in-service/idle	no	
0001/006	T00006	in-service/idle	no	
0001/007	т00007	in-service/idle	no	
0001/008	T00008	in-service/idle	no	
0001/009	Т00009	in-service/idle	no	
0001/010	T00010	in-service/idle	no	

CMN; Reviewed: SPOC 12/8/2014

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 51 of 55 EIR\_CMSM63SBC

- 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**  $\rightarrow$  **Advanced Options**  $\rightarrow$  **Troubleshooting**  $\rightarrow$  **Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the Local Address drop down menu
- 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**

Trace: GSSCP_0	3			
Devices	Call Trace Packet Capture Captures			
GSSCP_03	Status	Packet Capture Configuration Ready		
	Interface	B1 💌		
	Local Address IP[:Port]	192.168.122.57 💌 :		
	Remote Address *, *:Port, IP, IP:Port	•		
	Protocol	All		
	Maximum Number of Packets to Capture	10000		
	Capture Filename Using the name of an existing capture will overwrite it.	SIP_Trunk_Testpcap		
		Start Capture Clear		

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

Trace: GSSCP_03					
Devices GSSCP_03	Call Trace Pa	cket Capture Capture	es		Refresh
		File Name		File Size (bytes)	Last Modified
	SIP_Trunk_Tes	_20140916121852.pcap	0		September 16, 2014 12:18:52 PM GMT Delete

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

# 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to Eircom's SIP Trunk Service. Eircom's SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

## 11. Additional References

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

- [1] Installing and Configuring Avaya Aura® System Platform, Release 6.3, May 2014
- [2] Administering Avaya Aura® System Platform, Release 6.3, May 2014
- [3] Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide, April 2014
- [4] Avaya Aura® Communication Manager 6.3 Documentation library, August 2014
- [5] Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide Release 6.3 April 2014
- [6] Implementing Avaya Aura® System Manager Release 6.3, May 2014
- [7] Upgrading Avaya Aura® System Manager to 6.3 May 2014
- [8] Administering Avaya Aura® System Manager Release 6.3, May 2014
- [9] Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide Release 6.3 August 2014
- [10] Implementing Avaya Aura® Session Manager Release 6.3, May 2014
- [11] Upgrading Avaya Aura® Session Manager Release 6.3, May 2014
- [12] Administering Avaya Aura® Session Manager Release 6.3, June 2014
- [13] Installing Avaya Session Border Controller for Enterprise, Release 6.2 June 2014
- [14] Upgrading Avaya Session Border Controller for Enterprise Release 6.2 July 2014
- [15] Administering Avaya Session Border Controller for Enterprise Release 6.2 March 2014
- [16] RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/

#### ©2014 Avaya Inc. All Rights Reserved.

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

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