



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R7.1 as an Evolution Server, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to support Eir SIP Trunk Service - Issue 1.0**

## **Abstract**

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Eir 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. Eir 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 Eir'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 Eir 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 Eir.

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

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

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

For the testing associated with this Application Note, the interface between Avaya systems and the Eir SIP Trunk Service did not include use of any specific encryption features as requested by Eir.

## 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 Eir, 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 Eir.
- Outgoing calls from the enterprise site completed via Eir'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 Eir.
- Inbound and outbound PSTN calls to/from Avaya One-X Communicator and Avaya Communicator 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 fax transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- Inbound and outbound PSTN calls to/from Avaya One-X Communicator Softphone clients
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.

## 2.2. Test Results

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

- Eir SIP Trunk service uses DNS/SRV record for SIP trunk registration and resilience. The Eir DNS/SRV record is configured with two FQDNs of two SBC servers working in active-active mode. Eir requires only one SIP trunk registration at a time. When testing with ASBCE 7.2 SP1, if the DNS/SRV record is configured both in Server Configuration and Routing profile, Avaya SBCE sends register requests simultaneously to the two Eir SBC server FQDNs configured under the Eir DNS/SRV record which is not the expected way of registering with the platform. Eir expects that only one registration should be sent from ASBCE based on the weighted response of DNS server for SRV query. A GRIP has been raised with Avaya SBCE support and this issue is expected to be resolved in Avaya SBCE R7.2 SP2 scheduled for Q3 2018. The workaround used during testing was to populate the Routing Profile and Server Configuration for Eir with the FQDN of the weighted SBC server as per **Section 7.2.5** and **Section 7.2.4**.
- When a PSTN call is directed to a host station with EC500 mobile enabled and the call is answered at host station. When attempting to extend the call from the host station to EC500 mobile, Eir send a "603 Decline" response. This is working as design due to security measures implemented on the Eir SIP trunk.
- Inbound Toll-Free calls are supported but not tested as no Toll-Free access was available for test.
- Emergency Services access is supported but not tested as an Emergency Services test call was not booked with the Operator.

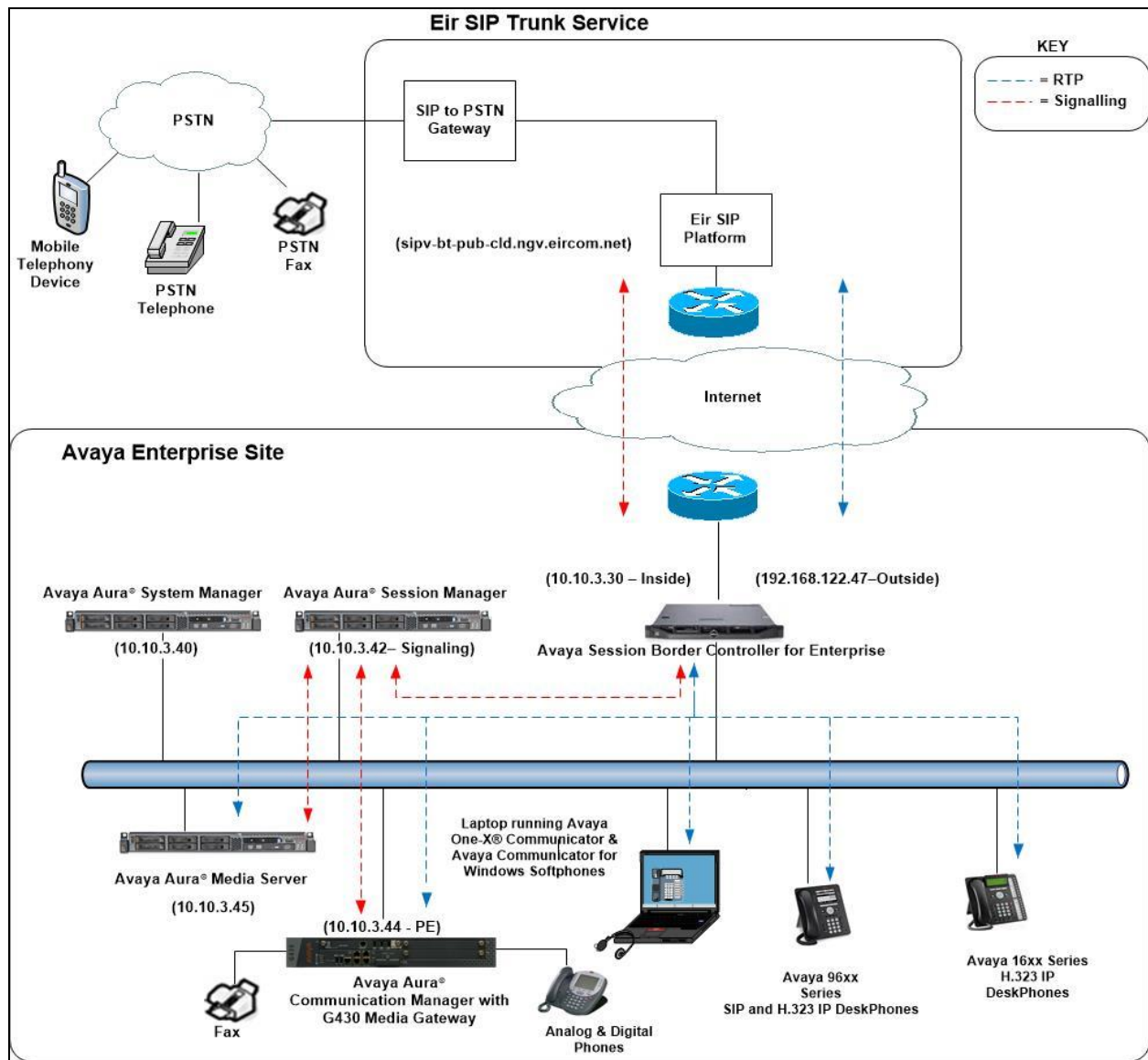
## 2.3. Support

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

For technical support on Eir products please contact the Eir authorized representative at: <https://business.eir.ie/support/> or Eir Local Support numbers.

### 3. Reference Configuration

The following equipment in **Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Eir'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 A175 Desktop Video Device running Flare Experience (audio only), 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 Eir SIP Trunk to Avaya Enterprise**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya Aura® System Manager	7.1.1.1 - Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.1.1.057109 Service Pack 1
Avaya Aura® Session Manager	7.1.1.0.711008
Avaya Aura® Communication Manager	R017x.00.0.441.0 (23985) FP1
Avaya G430 Media Gateway	7.1.1. (g430_sw_38_20_1)
Avaya Aura® Media Server	7.7.0.375
Avaya Session Border Controller for Enterprise	7.2.1.0-05-14222
Avaya 1600 IP Deskphone (H.323)	1.3.11
Avaya 9611 IP DeskPhone (H.323)	6.6
Avaya 9608 IP DeskPhone (SIP)	7.0
Avaya 9611 IP DeskPhone (SIP)	7.0
Avaya 9621 IP DeskPhone (SIP)	7.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.04-FP12
Avaya Communicator for Windows	3.3
Analogue Handset	N/A
Analogue Fax	N/A
<b>Eir</b>	
Broadsoft Broadworks	rel 21SP1
Ericsson IMS	rel 15A
AcmePacket SD running on 4500 platform	software release 6.4.0 MR4 patch 1

## 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 Eir 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 selects a SIP trunk, the SIP signalling is routed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Eir 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 Eir SIP Trunk network, and any other SIP trunks used.

<b>display system-parameters customer-options</b>		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
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>10</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0

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

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

## 5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **SM** and **10.10.3.42** 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		IP NODE NAMES
Name	IP Address	
<b>SM</b>	<b>10.10.3.42</b>	
default	0.0.0.0	
procr	10.10.3.44	
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 NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: 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 Eir was configured, namely **G.729** and **G.711A**.

change ip-codec-set 1				Page 1 of 2
IP Codec Set				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.729	n	2	30	
2: G.711A	n	2	20	

Eir 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 1				Page 2 of 2
IP CODEC SET				
Allow Direct-IP Multimedia? n				
	Mode	Redundancy	ECM:	Packet Size (ms)
<b>FAX</b>	<b>t.38-standard</b>	0	<b>y</b>	
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0		20

## 5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Eir 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 **SM** 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**.
- 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 Communication Manager 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**.
- Set **H.323 Station Outgoing Direct Media** to **y**.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).

The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2
SIGNALING 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: SM
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	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? y	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group 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-ntwrk**.
- 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			
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	Night Service:	
Dial Access? n			
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 Eir to prevent unnecessary SIP messages during call setup.

add trunk-group 1		Page 2 of 21	
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 **public**. This allows delivery of CLI in format of E.164 with leading “+” as requested by Eir.

TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Suppress # Outpulsing? n	<b>Numbering Format: public</b>	UI Treatment: service-provider
	Replace Restricted Numbers? n	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y	
	Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y		

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 Eir.
- 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 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? y	
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: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

## 5.7. Administer Calling Party Number Information

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

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	6010	1	35376xxxxx50	12	Total Administered: 4
4	6020	1	35376xxxxx51	12	Maximum Entries: 240
4	6102	1	35376xxxxx52	12	
4	6030	1	35376xxxxx53	12	Note: If an entry applies to
4	6104	1	35376xxxxx54	12	a SIP connection to Avaya
					Aura(R) Session Manager,
					the resulting number must
					be a complete E.164 number.
					Communication Manager
					automatically inserts
					a '+' digit in this case.

**Note:** The above configuration accepts all 4 digit numbers starting with 6, which includes all SIP and H.323 extension numbers.

## 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 Eir'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 Code 2:

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

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req	
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 Eir 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-conversion 0							Page 1 of 2
ARS DIGIT CONVERSION TABLE							
Location: all							Percent Full: 0
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI Req
0	1	16	0	0	ars	y	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						
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted							DCS/	IXC				
No			Mrk	Lmt	List	Del	Digits							QSIG					
													Dgts					Intw	
1: 1	0												n	user					
2:													n	user					
3:													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						

## 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 Eir 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 Eir correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **076xxxxxx** 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-call-handling-trmt trunk-group 1					Page	1	of	3
INCOMING CALL HANDLING TREATMENT								
Service/ Feature	Number Len	Number Digits	Del Insert					
public-ntwrk	10	076xxxxx50	all 6010					
public-ntwrk	10	076xxxxx51	all 6020					
public-ntwrk	10	076xxxxx52	all 6102					
public-ntwrk	10	076xxxxx53	all 6030					
public-ntwrk	10	076xxxxx54	all 6104					

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

change off-pbx-telephone station-mapping 6102							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode		
6102	EC500	-		089434xxxx	ARS	1			
-									

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

## 6. Configuring Avaya Aura® Session Manager

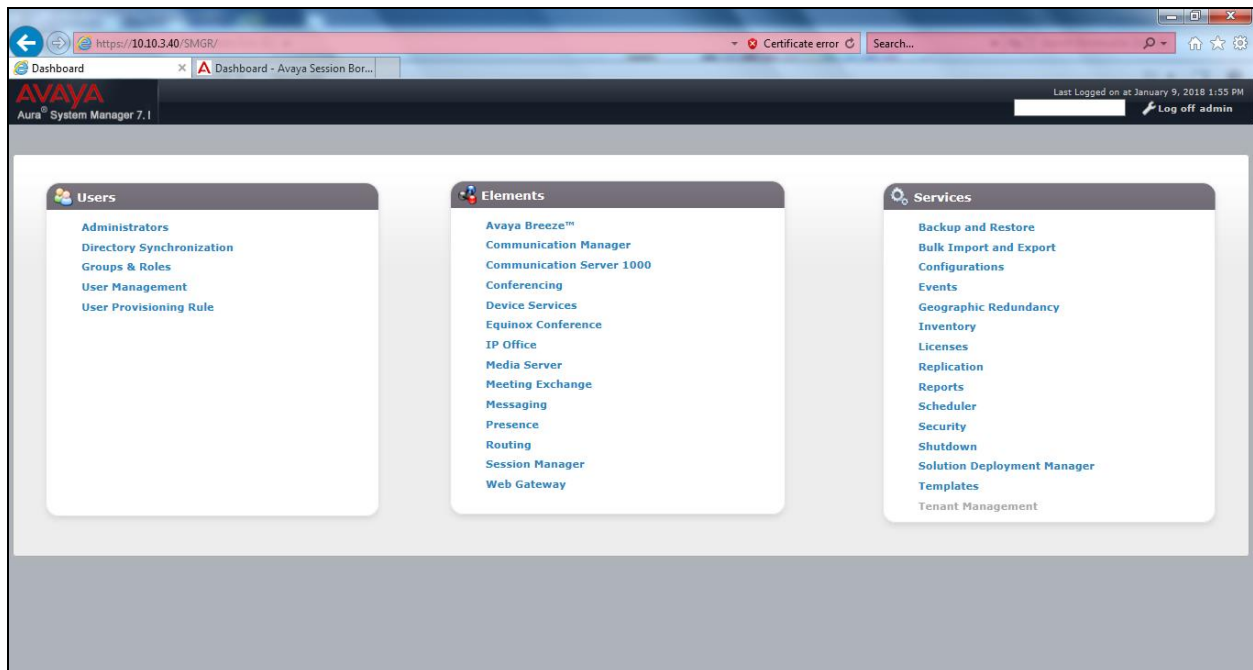
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

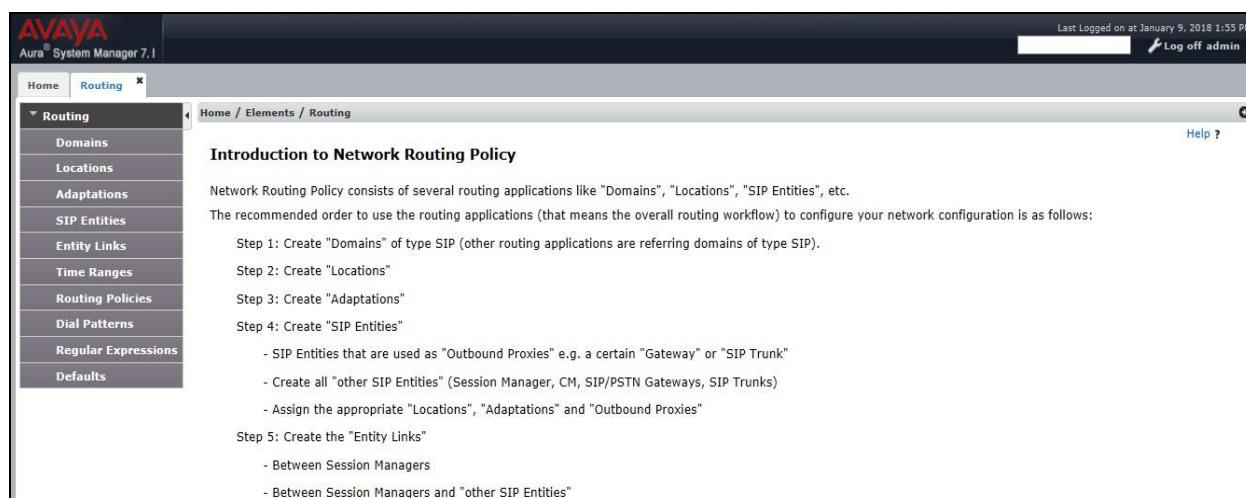
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

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

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



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.

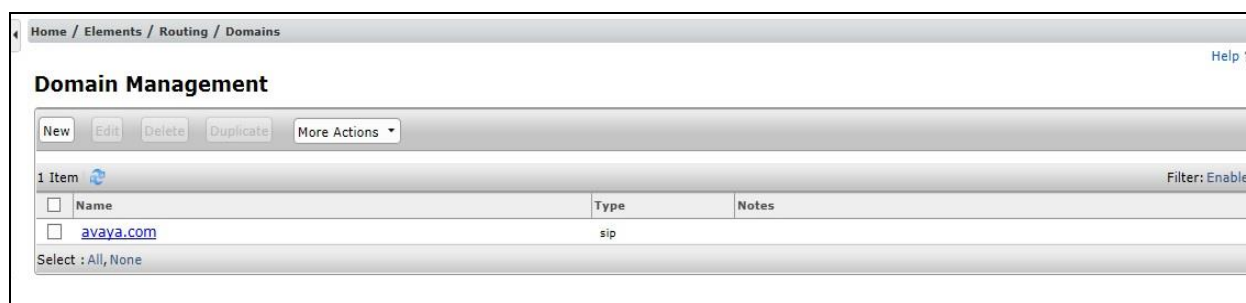


## 6.2. Administer SIP Domain

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.



## 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 **SMGR\_7** defined for the compliance testing.

The screenshot displays the Avaya Session Manager Administration console interface. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Locations'. The main section is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. It is divided into three sub-sections: 'General', 'Dial Plan Transparency in Survivable Mode', and 'Overall Managed Bandwidth'.

**General Section:**

- Name:** SMGR\_7
- Notes:** (empty text area)

**Dial Plan Transparency in Survivable Mode Section:**

- Enabled:** ☐
- Listed Directory Number:** (empty text area)
- Associated CM SIP Entity:** (empty text area)

**Overall Managed Bandwidth Section:**

- Managed Bandwidth Units:** Kbit/sec (dropdown menu)
- Total Bandwidth:** (empty text area)
- Multimedia Bandwidth:** (empty text area)
- Audio Calls Can Take Multimedia Bandwidth:** ☒

**Location Pattern Section:**

This section includes 'Add' and 'Remove' buttons. It shows a table with 3 items. The table has columns for 'IP Address Pattern' and 'Notes'. The 'Filter' is set to 'Enable'.

IP Address Pattern	Notes
* 10.10.3.*	
* 10.10.4.*	
* 10.10.9.*	

At the bottom of the 'Location Pattern' section, there is a 'Select' dropdown menu with options 'All' and 'None', and 'Commit' and 'Cancel' buttons.

## 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. In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements

For the compliance test, an Adaptation named “**Eir**” was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

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 **Adaptation Details** → **General**:

- **Adaption Name:** Enter an appropriate name such as **Eir**.
- **Module Name:** Select **DigitConversionAdapter**.
- **Modular Parameter Type:** Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

- **Name:** Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value:** Enter **AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, P-Location**.
- **Name:** Enter **fromto**. Modifies From and To header of a message.
- **Value:** Enter **true**.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

\* Adaption Name: Eir

\* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, P-Location
fromto	true

Select : All, None

Egress URI Parameters:

Notes:

## 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.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb navigation is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is active. Fields include: Name (Session Manager), FQDN or IP Address (10.10.3.42), Type (Session Manager), Notes, Location (SMGR\_7), Outbound Proxy, Time Zone (Europe/Dublin), Minimum TLS Version (Use Global Setting), and Credential name. The 'Monitoring' tab is also visible, showing SIP Link Monitoring and CRLF Keep Alive Monitoring, both set to 'Use Session Manager Configuration'.

Field	Value
Name	Session Manager
FQDN or IP Address	10.10.3.42
Type	Session Manager
Notes	
Location	SMGR_7
Outbound Proxy	
Time Zone	Europe/Dublin
Minimum TLS Version	Use Global Setting
Credential name	
SIP Link Monitoring	Use Session Manager Configuration
CRLF Keep Alive 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.

The screenshot shows the 'Entity Links' configuration page. It has 'Add' and 'Remove' buttons. Below is a table with 3 items. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. The table shows three rows of links between Session Manager and other entities (Avaya\_SBCE, Communication\_Man, Messaging). Below the table is a 'Failover Ports' section with fields for TCP and TLS failover ports.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* Avaya_SBCE	Session Manager	TCP	* 5060	Avaya_SBCE	* 5060	trusted	<input type="checkbox"/>
* Communication_Man	Session Manager	TCP	* 5060	Communication_Man	* 5060	trusted	<input type="checkbox"/>
* Messaging	Session Manager	TCP	* 5060	Messaging	* 5060	trusted	<input type="checkbox"/>

Failover Ports

TCP Failover port:

TLS Failover port:

### 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.

The screenshot shows the 'SIP Entity Details' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. Below this, the title 'SIP Entity Details' is followed by 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The form contains the following fields: 'Name' (Communication\_Manager), 'FQDN or IP Address' (10.10.3.44), 'Type' (CM), 'Notes' (empty), 'Adaptation' (dropdown), 'Location' (SMGR\_7), 'Time Zone' (Europe/Dublin), '\* SIP Timer B/F (in seconds):' (4), 'Minimum TLS Version' (Use Global Setting), 'Credential name' (empty), 'Securable' (checkbox), 'Call Detail Recording' (none), 'Loop Detection Mode' (On), and 'Loop Count Threshold' (5). The 'Loop Detection' and 'SIP Link Monitoring' sections are partially visible at the bottom.

Home / Elements / Routing / SIP Entities

### SIP Entity Details

Commit Cancel

**General**

\* Name: Communication\_Manager

\* FQDN or IP Address: 10.10.3.44

Type: CM

Notes:

Adaptation:

Location: SMGR\_7

Time Zone: Europe/Dublin

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

**Loop Detection**

Loop Detection Mode: On

Loop Count Threshold: 5

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

The screenshot shows the 'Loop Detection' and 'SIP Link Monitoring' sections. The 'Loop Detection Mode' is set to 'Off' and the 'SIP Link Monitoring' is set to 'Use Session Manager Configuration'.

**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.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb navigation at the top reads "Home / Elements / Routing / SIP Entities". The main heading is "SIP Entity Details", with "General" selected as the tab. In the top right corner are "Commit" and "Cancel" buttons. The form contains the following fields and values:

- Name:** Avaya\_SBCE
- \* FQDN or IP Address:** 10.10.3.30
- Type:** SIP Trunk (dropdown menu)
- Notes:** (empty text area)
- Adaptation:** Eir (dropdown menu)
- Location:** SMGR\_7 (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- \* SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown menu)
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress (dropdown menu)

Below these fields is the "Loop Detection" section, which includes:

- Loop Detection Mode:** On (dropdown menu)
- Loop Count Threshold:** 5

## 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** to make the other system trusted.

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

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	<a href="#">Avaya_SBCE</a>	Session Manager	TCP	5060	Avaya_SBCE	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">Communication_Manager</a>	Session Manager	TCP	5060	Communication_Manager	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">Messaging</a>	Session Manager	TCP	5060	Messaging	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Select : All, None

## 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.

The screenshot shows the 'Routing Policy Details' form. The 'General' section includes fields for 'Name' (to\_Communication\_Manager), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with one entry: 'Communication\_Manager' with FQDN or IP Address '10.10.3.44' and Type 'CM'. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows '1 Item' with a table of time ranges. The table has columns for Ranking, Name, days of the week (Mon-Sun), Start Time, End Time, and Notes. One item is listed with Ranking 0, Name 24/7, and Start/End times 00:00 to 23:59. The filter is set to 'Enable'.

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel Help ?

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
Communication_Manager	10.10.3.44	CM	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

The following screen shows the Routing Policy for the Avaya SBCE.

Home / Elements / Routing / Routing Policies Help ?

### Routing Policy Details

Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE	10.10.3.30	SIP Trunk	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

## 6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**:

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

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

Home / Elements / Routing / Dial Patterns Help ?

### Dial Pattern Details

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGR_7		to_Avaya_SBCE	0	<input type="checkbox"/>	Avaya_SBCE	

Select : All, None

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

Home / Elements / Routing / Dial Patterns Help ?

### Dial Pattern Details

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGR_7		to_Communication_Manager	0	<input type="checkbox"/>	Communication_Manager	

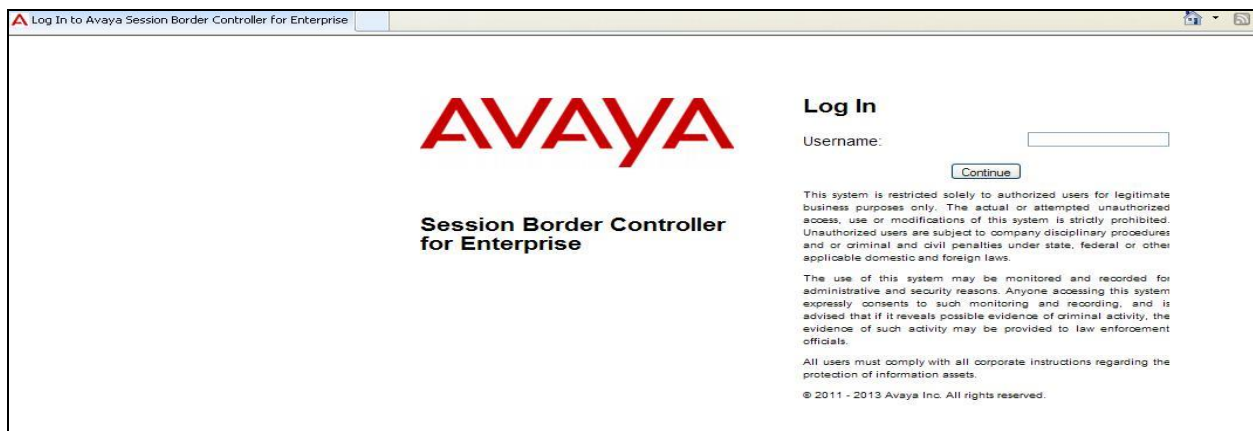
Select : All, None

## 7. Configure Avaya Session Border Controller for Enterprise

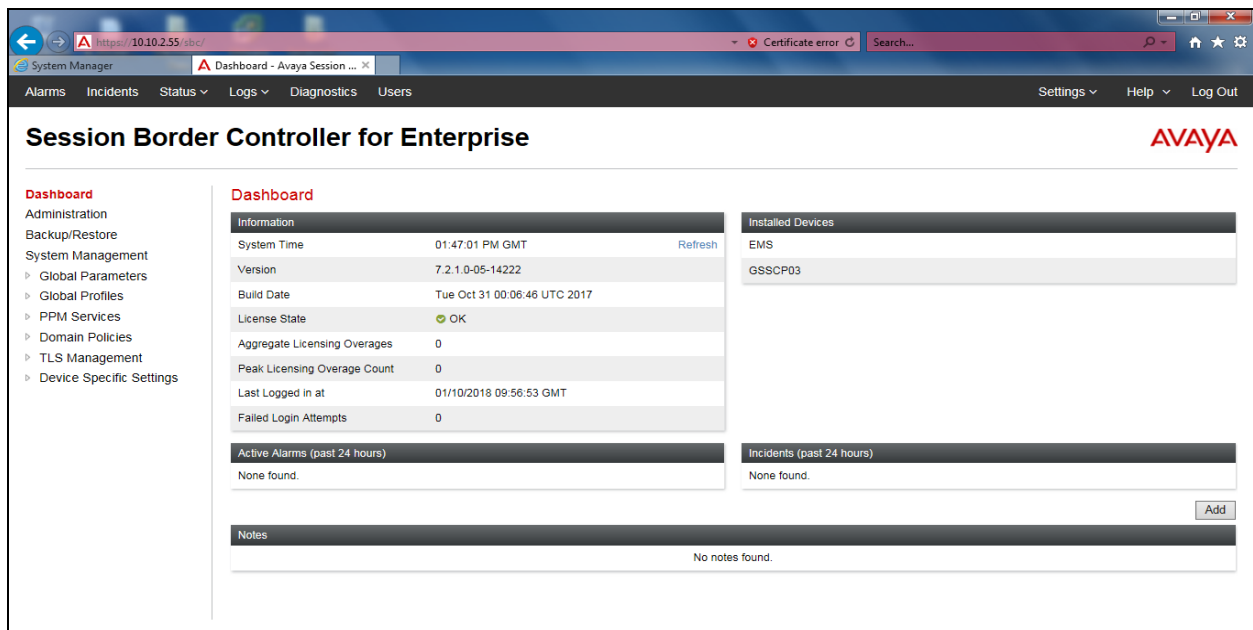
This section describes the configuration of Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation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

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

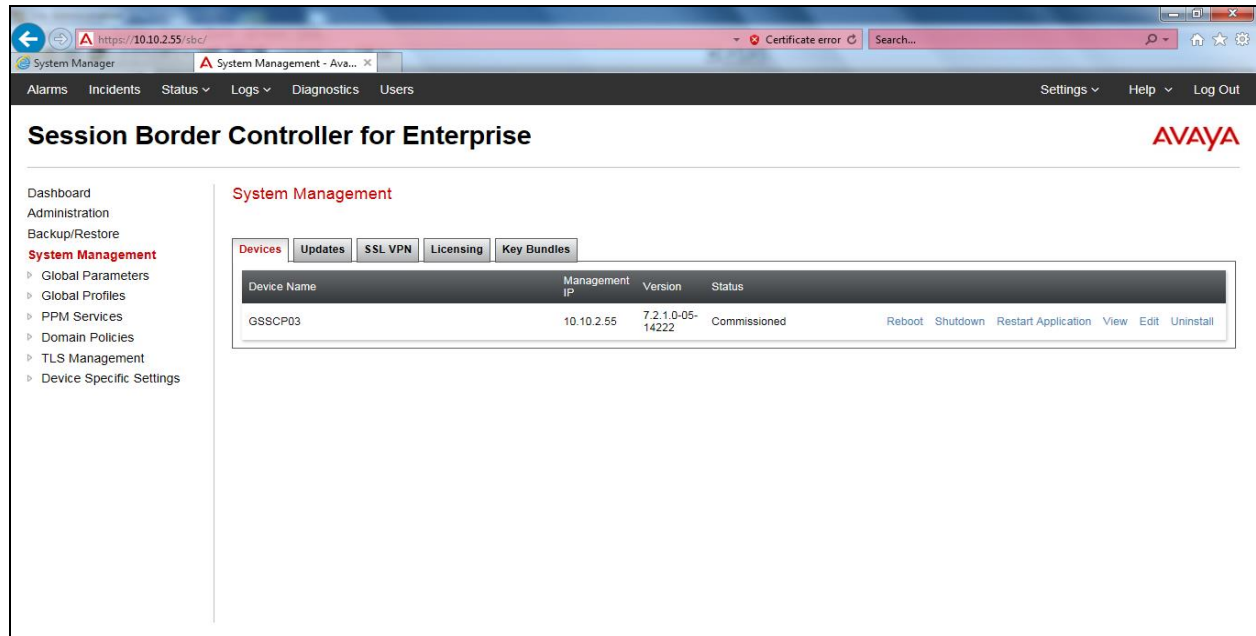
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



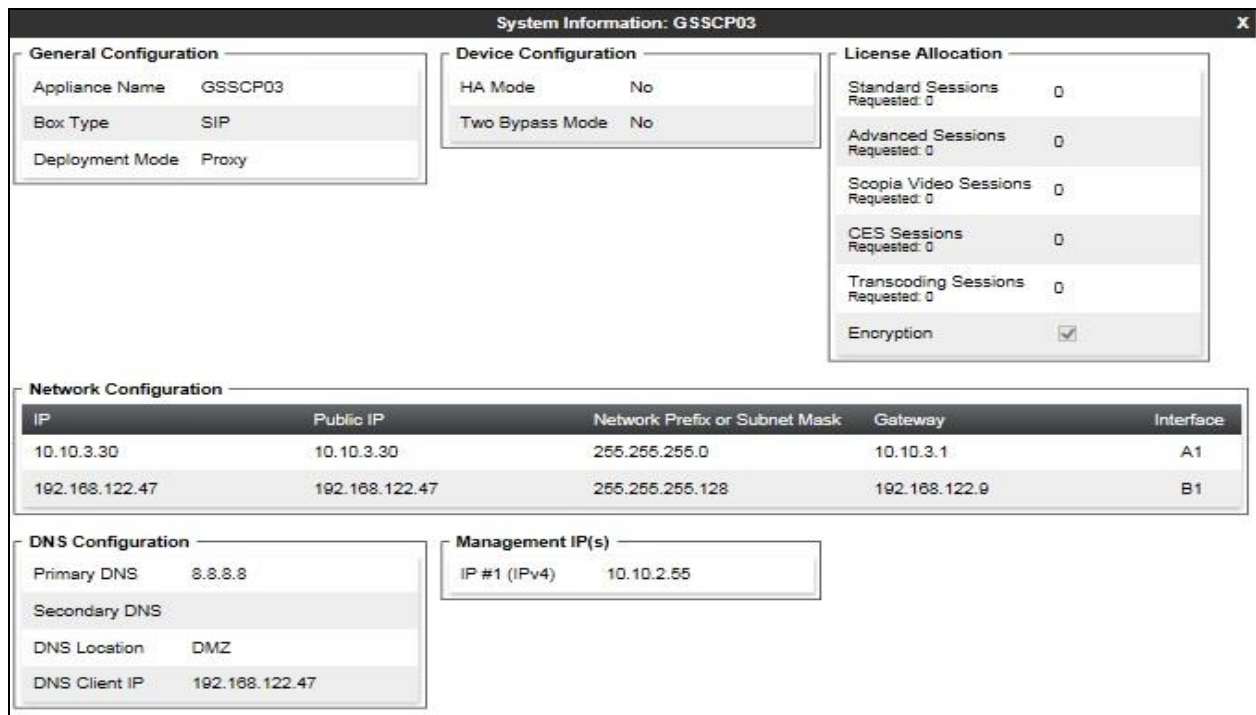
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



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.



## 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** → **Server Interworking** and click on **Add Profile**.

- Enter profile name such as **Avaya** 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.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3281 <input type="radio"/> RFC2543

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

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
Extensions	Avaya ▾
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None ▾
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
<b>DTMF</b>	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP Notify <input type="radio"/> RFC 2833 Relay & SIP Notify <input type="radio"/> SIP Info <input type="radio"/> RFC 2833 Relay & SIP Info <input type="radio"/> Inband
<input type="button" value="Finish"/>	

### 7.2.2. Server Interworking – Eir

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** → **Server Interworking** and click on **Add Profile**.

- Enter profile name such as **Eir** 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**.

The screenshot shows the 'General' configuration tab for a SIP server profile. The settings are as follows:

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

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

Record Routes	<input checked="" type="radio"/> None <input type="radio"/> Single Side <input type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
Extensions	None ▾
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None ▾
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
<b>DTMF</b>	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP Notify <input type="radio"/> RFC 2833 Relay & SIP Notify <input type="radio"/> SIP Info <input type="radio"/> RFC 2833 Relay & SIP Info <input type="radio"/> Inband
<input type="button" value="Finish"/>	

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

Servers are defined for each server connected to the Avaya SBCE. In this case, Eir 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 /FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Call Server

SIP Domain:

TLS Client Profile: None

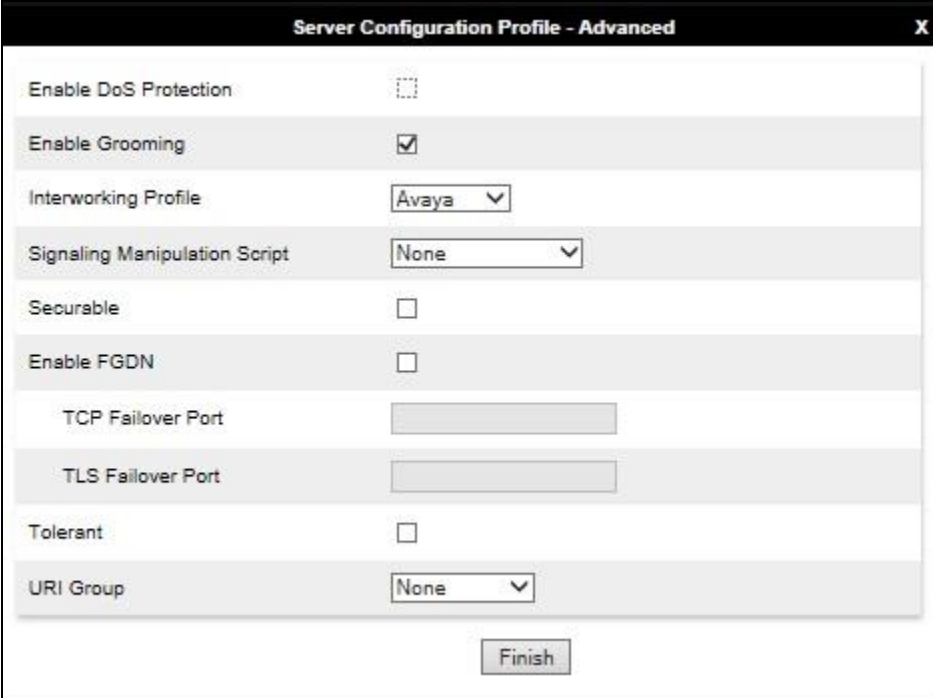
Add

IP Address / FQDN	Port	Transport
10.10.3.42	5060	TCP

Delete

On the **Advanced** tab:

- Enable **Grooming**.
- Select **Avaya** for **Interworking Profile** defined in **Section 7.2.1**.
- Click **Finish**.



Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None ▼
<div>Finish</div>	

## 7.2.4. Server Configuration – Eir

To define the Eir SBC as a Trunk Servers, navigate to select **Global Profiles → 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/FQDN** to **sipv-bt-pub-cld.ngv.eircom.net** (Eir SIP Trunk).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Hit **Next**.

**Server Configuration Profile - General**

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

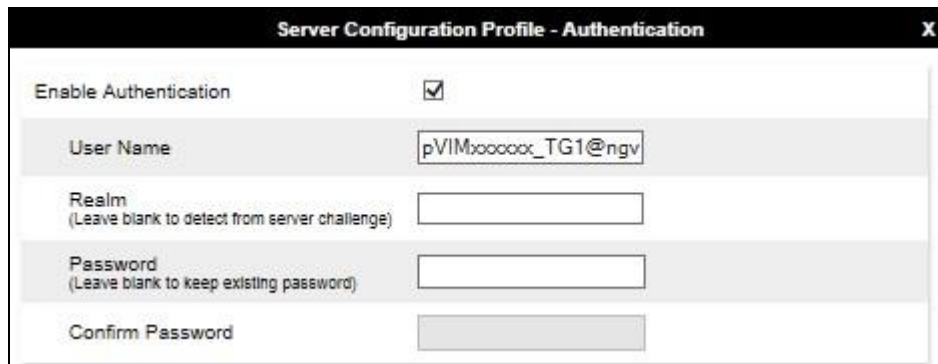
IP Address / FQDN	Port	Transport
sipv-bt-pub-cld.ngv.eircom.net	5060	UDP

Delete

In the new window that appears, enter the following values as Eir 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 or leave blank to be detected by the server challenge.
- **Password** Enter password provided by the Service Provider.
- **Confirm Password** Re-enter password provided by the Service Provider.

Click **Next** to continue.



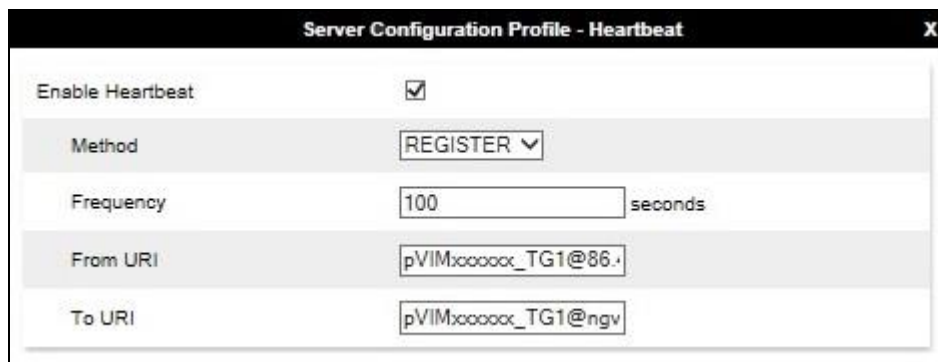
The screenshot shows a dialog box titled "Server Configuration Profile - Authentication". It contains the following fields and controls:

- Enable Authentication:** A checkbox that is checked.
- User Name:** A text input field containing "pVIM:xxxxxx\_TG1@ngv".
- Realm:** A text input field with the placeholder text "(Leave blank to detect from server challenge)".
- Password:** A text input field with the placeholder text "(Leave blank to keep existing password)".
- Confirm Password:** A text input field.

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

Click **Next** to continue.

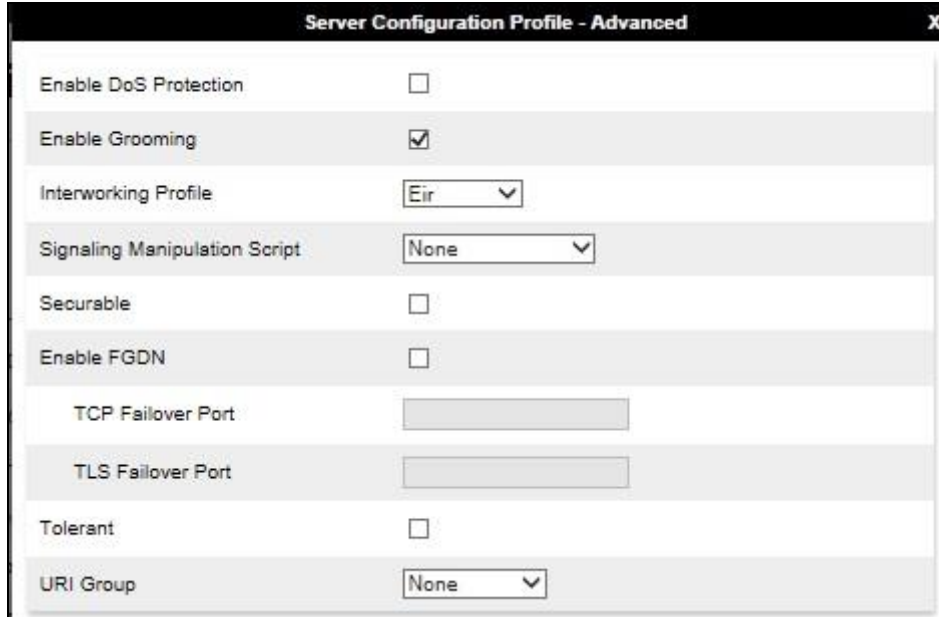


The screenshot shows a dialog box titled "Server Configuration Profile - Heartbeat". It contains the following fields and controls:

- Enable Heartbeat:** A checkbox that is checked.
- Method:** A drop-down menu showing "REGISTER".
- Frequency:** A text input field containing "100" with the unit "seconds" to its right.
- From URI:** A text input field containing "pVIM:xxxxxx\_TG1@86.".
- To URI:** A text input field containing "pVIM:xxxxxx\_TG1@ngv".

On the **Advanced** tab:

- Enable **Grooming**.
- Select **Eir** for **Interworking Profile** as defined in **Section 7.2.2**.
- Click **Finish**.



Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Eir
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None

### 7.2.5. 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 Eir 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.

### 7.2.5.1 Routing – Avaya

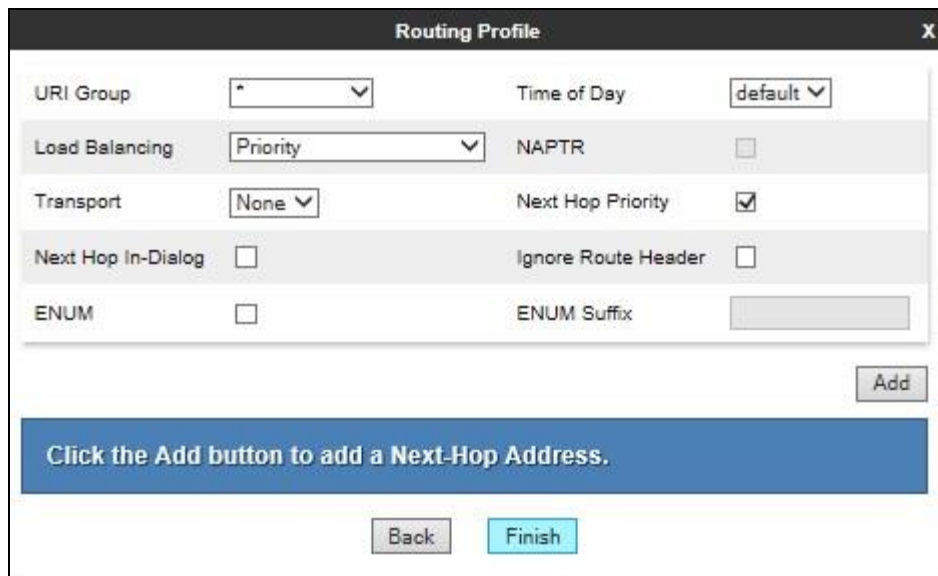
Create a Routing Profile for Session Manager.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Avaya". Below the input field is a button labeled "Next".

The Routing Profile window will open. Use the default values displayed and click **Add**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. The window contains several configuration options arranged in two columns:

Routing Profile	
URI Group	* ▼
Time of Day	default ▼
Load Balancing	Priority ▼
NAPTR	<input type="checkbox"/>
Transport	None ▼
Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>
ENUM	<input type="checkbox"/>
ENUM Suffix	

Below the configuration options is an "Add" button. At the bottom of the window, there is a blue banner with the text "Click the Add button to add a Next-Hop Address." and two buttons: "Back" and "Finish".

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Avaya** (Section 7.2.3) from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5060 TCP** from drop down menu.
- Click **Finish**.

URI Group	Time of Day
*	default
Load Balancing	NAPTR
Priority	<input type="checkbox"/>
Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>
Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>
ENUM	ENUM Suffix
<input type="checkbox"/>	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	Delete
1	Avaya	10.10.3.42:5060 (TCP)	None	

Finish

## 7.2.5.2 Routing – Eir

Create a Routing Profile for Eir.

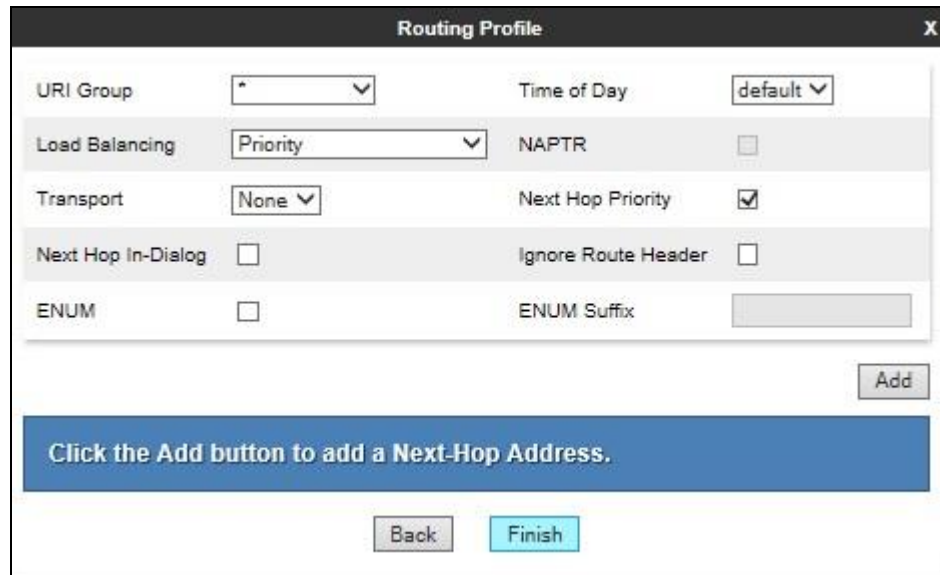
- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

Routing Profile

Profile Name: Eir

Next

The Routing Profile window will open. Use the default values displayed and click **Add**.



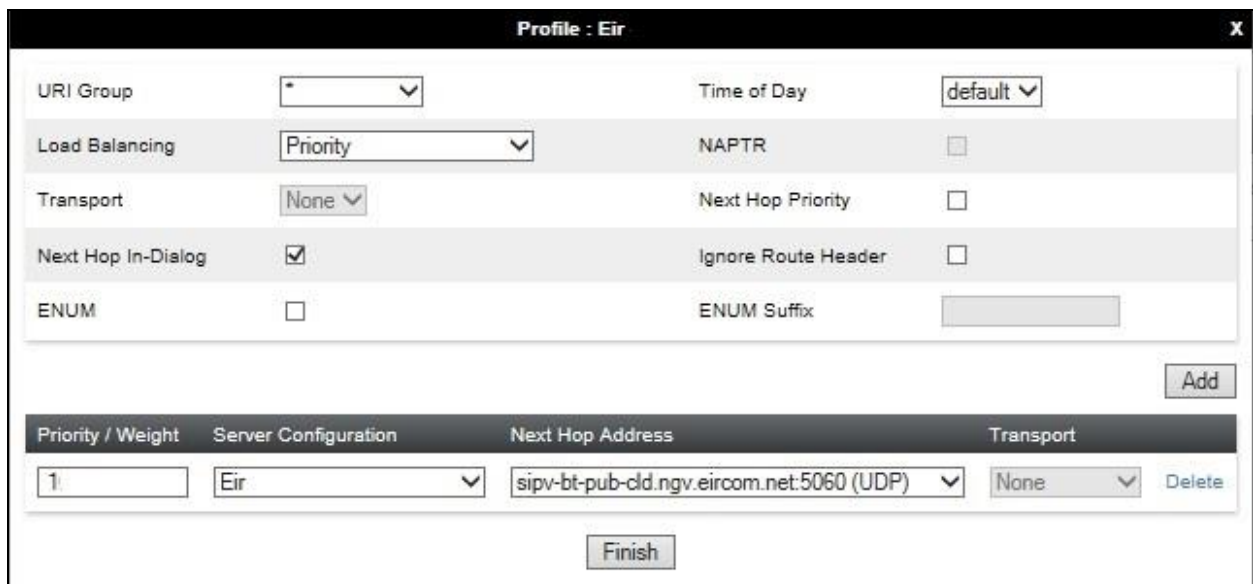
The Routing Profile window is a dialog box with a title bar "Routing Profile" and a close button "X". It contains several configuration fields:

- URI Group: dropdown menu with "\*" selected.
- Time of Day: dropdown menu with "default" selected.
- Load Balancing: dropdown menu with "Priority" selected.
- NAPTR: checkbox, unchecked.
- Transport: dropdown menu with "None" selected.
- Next Hop Priority: checkbox, checked.
- Next Hop In-Dialog: checkbox, unchecked.
- Ignore Route Header: checkbox, unchecked.
- ENUM: checkbox, unchecked.
- ENUM Suffix: text input field.

At the bottom right is an "Add" button. Below the form is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the very bottom are "Back" and "Finish" buttons.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Eir (Section 7.2.4)** from drop down menu.
- **Next Hop Address = Select sipv-bt-pub-cld.ngv.eircom.net:5060 UDP** from drop down menu.
- Click **Finish**.



The Profile : Eir window is a dialog box with a title bar "Profile : Eir" and a close button "X". It contains the same configuration fields as the Routing Profile window, but with some differences:

- URI Group: dropdown menu with "\*" selected.
- Time of Day: dropdown menu with "default" selected.
- Load Balancing: dropdown menu with "Priority" selected.
- NAPTR: checkbox, unchecked.
- Transport: dropdown menu with "None" selected.
- Next Hop Priority: checkbox, unchecked.
- Next Hop In-Dialog: checkbox, checked.
- Ignore Route Header: checkbox, unchecked.
- ENUM: checkbox, unchecked.
- ENUM Suffix: text input field.

At the bottom right is an "Add" button. Below the form is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Eir	sipv-bt-pub-cld.ngv.eircom.net:5060 (UDP)	None

At the bottom right of the table is a "Delete" button. At the very bottom is a "Finish" button.

## 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 → 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**.
- 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 **avaya.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Avaya

Add

Topology Hiding Profiles

default

cisco\_th\_profile

Avaya

Eir

RenameCloneDelete

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Eir, navigate to **Global Profiles → 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 **Eir** 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).

### Topology Hiding Profiles: Eir

Add

Topology Hiding Profiles

default

cisco\_th\_profile

Avaya

**Eir**

Rename

Clone

Delete

Click here to add a description.

Topology Hiding

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

Edit

### 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 → 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 with screening mask and assign to interface **A1**.
- Select **Save** to save the information.
- Click on **Add**.
- Define the external IP address with screening mask and assign to interface **B1**.
- Select **Save** 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: GSSCP03

Devices: GSSCP03

Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Internal_A1	10.10.3.1	255.255.255.0	A1	10.10.3.30	Edit	Delete
External_B1	192.168.122.9	255.255.255.128	B1	192.168.122.47	Edit	Delete

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

Network Management: GSSCP03

Devices: GSSCP03

Interfaces Networks

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

## 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** → **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.

To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **internal** signalling interface IP addresses defined in **Section 7.3**.
- For **TCP Port**, **5060** is used for Session Manager.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select the **external** signalling interface IP address defined in **Section 7.3**.
- For **UDP Port**, **5060** is used for Eir SIP Trunk service.

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

Signaling Interface: GSSCP03

Devices  
GSSCP03

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30 Internal_A1 (A1, VLAN 0)	5060	---	---	None	Edit Delete
Ext_Sig	192.168.122.47 External_B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete

## 7.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** from the menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **internal** media interface IP address defined in **Section 7.3**.
- Select **Port Range** for the media path with the enterprise end-points.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **external** media interface IP address defined in **Section 7.3**.
- Select **Port Range** for the external media path.

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

Media Interface: GSSCP03

Devices  
GSSCP03

Media Interface

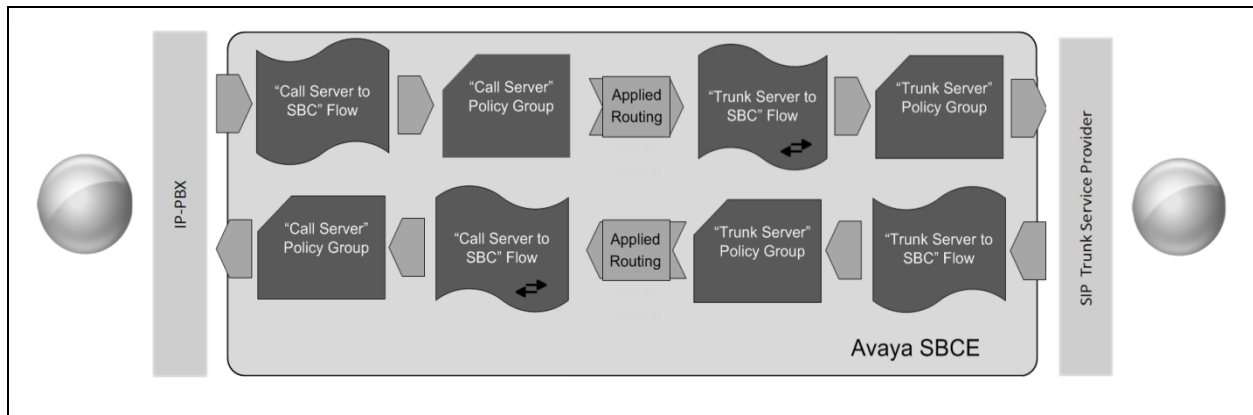
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#)

Add

Name	Media IP Network	Port Range	
Ext_Media	192.168.122.47 External_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
Int_Media	10.10.3.30 Internal_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete

## 7.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Eir's SIP Trunk and incoming flows from Eir'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 Eir network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Eir SIP Trunk and vice versa. The following screenshot shows all configured flows

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Server Configuration: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	Eir	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

Server Configuration: Eir

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server	*	Int_Sig	Ext_Sig	default-low	Avaya	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

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

- Click on the **Server Flows** tab (shown above).
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Eir SIP Trunk, in the test environment **Trunk\_Server** was used.
- In the **Server Configuration** drop-down menu, select the Eir server configuration defined in **Section 7.2.5**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Eir SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Eir SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Eir SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Eir SIP Trunk defined in **Section 7.2.6** and click **Finish**.

The screenshot shows a configuration window titled "Trunk\_Server" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a value field (either a text box or a dropdown menu). The fields are as follows:

Field Label	Value
Flow Name	Trunk_Server
Server Configuration	Eir
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Eir
Signaling Manipulation Script	None
Remote Branch Office	Any

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

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

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call\_Server** was used.
- In the **Server Configuration** drop-down menu, select the Session Manager server configuration defined in **Section 7.2.4**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Eir SIP Trunk defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.2.6** and click **Finish**.

The screenshot shows a configuration window titled "Call\_Server" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a value field (either a text box or a dropdown menu). At the bottom of the window is a "Finish" button.

Field Label	Value
Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Eir
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

## 8. Configure Eir SIP Trunk Equipment

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

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

### Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: Session Manager

Summary View

Status Details for the selected Session Manager:

SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> Communication Manager	IPv4	10.10.3.44	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> Avaya SBCE	IPv4	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> Messaging	IPv4	10.10.2.90	5060	TCP	FALSE	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.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

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

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address from the **Local Address** drop down menu.
- 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: GSSCP03

Devices

GSSCP03

Packet Capture

Captures

Packet Capture Configuration

Status

Ready

Interface

B1

Local Address

IP[:Port]

All

Remote Address

\*, \*Port, IP, IP:Port

\*

Protocol

UDP

Maximum Number of Packets to Capture

1000

Capture Filename

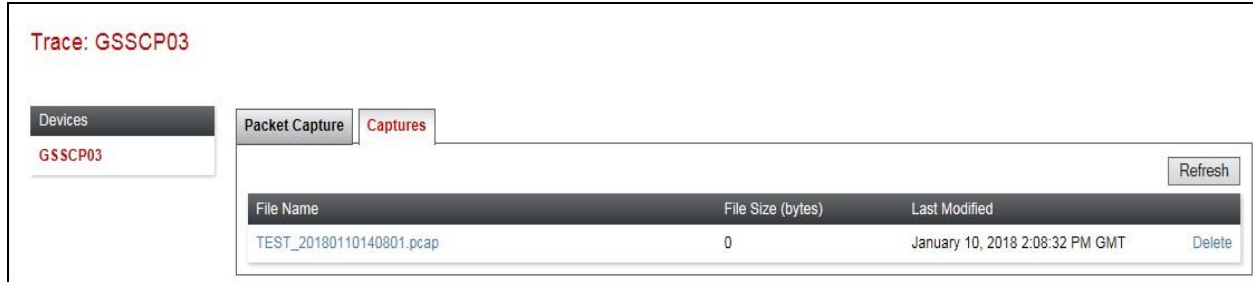
Using the name of an existing capture will overwrite it.

TEST.pcap

Start Capture

Clear

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



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

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.1 as an Evolution Server, Avaya Aura® Session Manager R7.1 and Avaya Session Border Controller for Enterprise R7.2 to Eir's SIP Trunk Service. Eir'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 <http://support.avaya.com>.

- [1] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, Dec 2017
- [2] *Avaya Aura® Communication Manager 7.1 Documentation library*, Dec 2017
- [3] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide Release 7.1* Dec 2017
- [4] *Implementing Avaya Aura® System Manager Release 7.1*, Dec 2017
- [5] *Upgrading Avaya Aura® System Manager to Release 7.1*, Dec 2017
- [6] *Administering Avaya Aura® System Manager Release 7.1*, Dec 2017
- [7] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide Release 7.1*, Dec 2017
- [8] *Implementing Avaya Aura® Session Manager Release 7.1*, Dec 2017
- [9] *Upgrading Avaya Aura® Session Manager Release 7.1*, Dec 2017
- [10] *Administering Avaya Aura® Session Manager Release 7.1*, Dec 2017
- [11] *Deploying Avaya Session Border Controller for Enterprise Release 7.2*, Jan 2018
- [12] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2*, Jan 2018
- [13] *Administering Avaya Session Border Controller for Enterprise Release 7.2*, Jan 2017
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

---

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

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

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