



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

---

# **Application Notes for Configuring the X5 Solutions SIP Trunking Service with Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the X5 Solutions SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 7.0, Avaya Aura® Communication Manager 7.0, Avaya Session Border Controller for Enterprise 7.0 and various Avaya endpoints. X5 Solutions is a member of the Avaya 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 to configure Session Initiation Protocol (SIP) Trunking between the X5 Solutions SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 7.0, Avaya Aura® Communication Manager 7.0, Avaya Session Border Controller for Enterprise 7.0 and various Avaya endpoints. In addition, Avaya Aura® System Manager 7.0 is used to configure Avaya Aura® Session Manager.

Customers, using this Avaya SIP-enabled enterprise solution with the X5 Solutions SIP Trunking Service, are able to place and receive PSTN calls via a broadband WAN connection with SIP. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the X5 Solutions SIP Trunking Service via a broadband connection and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE).

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 for 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

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test.

- Sending and receiving SIP OPTIONS queries to the service provider
- Inbound and outbound PSTN calls (via the SIP trunk) to/from analog, digital, H.323 and SIP telephones at the enterprise
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client) using multiple protocols (H.323 and SIP) and multiple modes (Local Computer and Other Phone mode)
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows
- Various call types including: local, long distance, international, outbound toll-free, and local directory assistance
- Codecs G.711MU and G.729A
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- Voicemail Message Waiting Indicator (MWI)

- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and mobility (Extension to cellular – EC500)
- T.38 Fax with G.711 fallback
- Network Call Redirection using REFER and 302 response
- Remote Worker

Emergency calls and inbound toll-free calls were not tested as part of the compliance test.

The following items are not supported:

- Operator (0) and operator-assisted calls (0 + 10 digits)
- SIP User-to-User (UI) header when call is redirected with REFER

## 2.2. Test Results

Interoperability testing of the X5 Solutions SIP Trunking Service was completed with successful results for all test cases with the exception of the observations and/or limitations described below.

- **OPTIONS from X5 Solutions (Request-URI)** - X5 Solutions sends OPTIONS messages whose user part of the Request URI is not routable by the Session Manager which results in a 404 “User Not Found” response to X5 Solutions. This behavior had no impact on the connection. However, to clean-up the signaling, the Avaya SBCE was configured to return a 200 OK response to all OPTIONS messages instead of sending the messages to the Session Manager. (**Section 7.9.2**)
- **Call redirect with REFER** – When the SIP REFER method was used to redirect an active PSTN call to another PSTN destination (e.g., call transfer), then after the redirection was complete, unexpected messaging (in the form of message retransmissions) continued between the enterprise and X5 Solutions. The retransmissions continued until a timeout was reached. The call was successful and this behavior had no user impact.
- **T.38 Fax and outbound calls** - On outbound fax calls, Communication Manager has a 4 second timer from the time it detects fax tone to receive the reINVITE from X5 Solutions to switch to T.38 fax. Otherwise, it will fallback to G.711 fax. The T.38 reINVITE from X5 Solutions arrives after this 4 second timer has expired. The result is that all outbound faxes will use G.711 fax if Communication Manager is configured for **t.38-G711-fallback**. Alternatively, if a customer wished to force outbound fax calls to use T.38, Communication Manager can be configured for **t.38-standard**. The downside to this approach is that if the terminating media gateway does not support T.38, the call will fail. Thus, the recommendation is to use **t.38-G711-fallback** (**Section 5.4**).

## 2.3. Support

For technical support on the X5 Solutions SIP Trunking Service, please contact X5 Solutions via one of the following:

Web: <http://www.x5solutions.com/contact>  
Phone : 1-888-588-1501  
Email: [x5support@x5solutions.com](mailto:x5support@x5solutions.com)

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

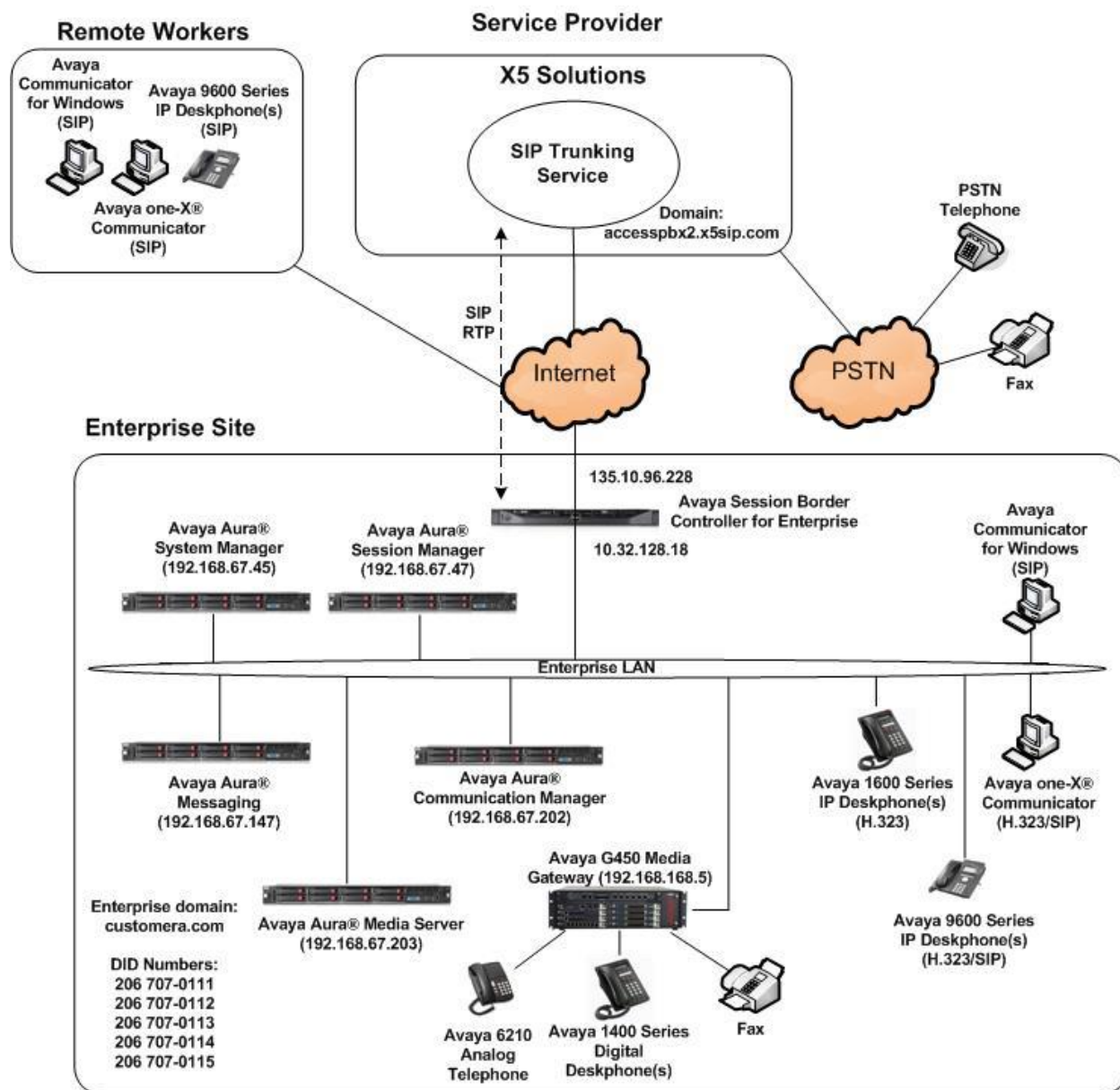
## 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to the X5 Solutions SIP Trunking Service.

The components used to create the simulated customer site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya Media Server
- Avaya Session Border Controller for Enterprise
- Avaya Aura® Messaging
- Avaya 1600 Series IP Deskphones (H.323)
- Avaya 9600 Series IP Deskphones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya Communicator for Windows

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in this document. Similarly, any references to real routable PSTN numbers have been replaced with numbers that cannot be routed over the PSTN.



**Figure 1: Test Configuration**

A separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and does not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the Avaya SBCE and then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the Avaya SBCE. From the Avaya SBCE, the call is sent to the X5 Solutions Trunking Service.

In the compliance testing, the SIP headers contained the following digit strings for calls within the North American Numbering Plan (NANP). For outbound calls, the enterprise sent (1 + 10 digits) in the Request URI and To (destination) headers. The From, PAI and Contact (source) headers contained 10 digits. For inbound calls, X5 Solutions sent 10 digits in all the headers mentioned above.

## 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® System Manager running on a VMware Virtual Platform	7.0 FP1 Patch 1 (7.0.1 Patch 1) (Software Update Revision 7.0.1.0.065071)
Avaya Aura® Session Manager running on a VMware Virtual Platform	7.0 FP1 (7.0.1) (Build 7.0.1.0.701007)
Avaya Aura® Communication Manager running on a VMware Virtual Platform	7.0 FP1 (7.0.1) (R017x.00.0.441.0-23012)
Avaya G450 Media Gateway	37.38.0
Avaya Aura® Media Server running on a VMware Virtual Platform	7.7
Avaya Aura® Messaging running on a VMware Virtual Platform	6.3.3 SP5
Avaya Session Border Controller for Enterprise	7.0 SP1 (7.0.1-03-8739)
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP5 (1.3.50B)
Avaya 9641G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.6.2 (6.6229)
Avaya 9611G IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	7.0.1.1 (7.0.1.1.5)
Avaya one-X® Communicator (H.323 or SIP)	6.2 SP11 (Build 6.2.11.03-SP11)
Avaya Communicator for Windows	2.1.3.80
X5 Solutions SIP Trunking Service Components	
Equipment/Software	Release/Version
Metaswitch	v9.2
Oracle (Acme Packet) 4500 Session Border Controller	v6.3

**Table 1: Equipment and Software Tested**

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the X5 Solutions SIP Trunking Service. A SIP trunk is established between Communication Manager and Session Manager for use by traffic to and from X5 Solutions. It is assumed the general installation of Communication Manager, the Avaya Media Gateway, Media Server and Session Manager has been previously completed and is not discussed here.

The 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. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

### 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **24000** SIP trunks are available and **30** are in use. 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.

<b>display system-parameters customer-options</b>		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	2
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	6
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>30</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0



## 5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave the field set to **none**.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **restricted** and **unavailable** respectively.

```
change system-parameters features                             Page 9 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

      CPN/ANI/ICLID PARAMETERS
      CPN/ANI/ICLID Replacement for Restricted Calls: restricted
      CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

      DISPLAY TEXT
      Identity When Bridging: principal
      User Guidance Display? n
      Extension only label for Team button on 96xx H.323 terminals? n

      INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code: 1
      International Access Code: 011

      SCCAN PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

      CALLER ID ON CALL WAITING PARAMETERS
      Caller ID on Call Waiting Delay Timer (msec): 200
```

### 5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager (**procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AAM	192.168.67.147	
AMS	192.168.67.203	
<b>SM</b>	<b>192.168.67.47</b>	
default	0.0.0.0	
gateway	192.168.67.1	
<b>procr</b>	<b>192.168.67.202</b>	
procr6	::	

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference defined by the service provider. For the compliance test, codec set 2 was configured with codecs G.729A and G.711MU. Default values can be used for all other fields.

change ip-codec-set 2

Page 1 of 2

IP CODEC SET

Codec Set: 2

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

On **Page 2**, set the **FAX Mode** to **t.38-G711-fallback** or **t.38-standard**. See **Section 2.2** for the implications of each setting.

change ip-codec-set 2			Page	2 of	2
IP CODEC SET					
Allow Direct-IP Multimedia? n					
	Mode	Redundancy		Packet	
FAX	t.38-G711-fallback	0	ECM: y	Size(ms)	
Modem	off	0			
TDD/TTY	US	3			
H.323 Clear-channel	n	0			
SIP 64K Data	n	0			20

## 5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **customera.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway or Media Server. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                     Page 1 of 20

                                IP NETWORK REGION

Region: 2
Location: 1             Authoritative Domain: customera.com
                        Name: SP Region             Stub Network Region: n
MEDIA PARAMETERS        Intra-region IP-IP Direct Audio: yes
                        Codec Set: 2                Inter-region IP-IP Direct Audio: yes
                        UDP Port Min: 16384          IP Audio Hairpinning? n
                        UDP Port Max: 32767
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
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. The example below shows the settings used for the compliance test. The first entry indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 2 will automatically create a complementary table entry on the IP network region 1 form for destination region 2. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).

change ip-network-region 2										Page	4	of	20
Source Region: 2      Inter Network Region Connection Management										I		M	
										G	A	t	
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c				
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e			
1	2	y	NoLimit					n		t			
2	2								all				
3	2	y	NoLimit					n		t			

## 5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between Communication Manager and Session Manager. If TLS is used here, it must also be used on the Session Manager entity link defined in **Section 6.6**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port

value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.6** and **5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5068** for use with TLS.

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic from the Avaya Media Gateway and allow it to flow directly between the SIP trunk and the enterprise endpoint.
- Set the **Alternate Route Timer** to **10**. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

add signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5068	Far-end Listen Port: 5068	
	Far-end Network Region: 2	
Far-end Domain: customera.com		
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? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in the previous section.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 2                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 2                                     Group Type: sip          CDR Reports: y
  Group Name: Service Provider                     COR: 1                 TN: 1          TAC: 602
  Direction: two-way                               Outgoing Display? n
  Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk                         Auth Code? n
                                                    Member Assignment Method: auto
                                                    Signaling Group: 2
                                                    Number of Members: 10
```

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs or UPDATE messages must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 2                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                         Redirect On OPTIM Failure: 5000

  SCCAN? n                                         Digital Loss Group: 18
                                         Preferred Minimum Session Refresh Interval(sec): 600

  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 field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. To remove the + sign, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call requests CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

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

On **Page 4**, set the **Network Call Redirection** field may be set to **y** or **n**. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer; otherwise the SIP INVITE message will be used for call transfer. Both approaches are supported with this solution.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected.

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

## 5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since **Numbering Format** was set to **private** on the trunk group form (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, the first four DID numbers provided for testing were assigned to the four extensions 19101, 19102, 19103, and 19104. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

change private-numbering 5					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	1	1		5	Total Administered: 43
5	2	1		5	Maximum Entries: 540
5	3	1		5	
5	4	1		5	
5	19101	2	2065551234	10	
5	19102	2	2065551235	10	
5	19103	2	2065551236	10	
5	19104	2	2065551237	10	

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, on trunk 2, all stations with a 5-digit extension beginning with 1 will send the calling party number as the **Private Prefix** plus the extension number.

change private-numbering 5					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	1	1		5	Total Administered: 2
5	1	2	20655	10	Maximum Entries: 540

## 5.9. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a dial access code (dac).

<b>change dialplan analysis</b>			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	5	ext							
2	5	ext							
3	5	ext							
4	5	ext							
411	3	udp							
5	5	ext							
6	3	dac							
7	3	dac							
8	1	dac							
<b>9</b>	<b>1</b>	<b>dac</b>							
*	3	fac							
#	3	fac							

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

<b>change feature-access-codes</b>			FEATURE ACCESS CODE (FAC)						Page 1 of 10
			Abbreviated Dialing List1 Access Code: *21						
			Abbreviated Dialing List2 Access Code: *22						
			Abbreviated Dialing List3 Access Code: *23						
			Abbreviated Dial - Prgm Group List Access Code: *24						
			Announcement Access Code: *25						
			Answer Back Access Code: *26						
			Auto Alternate Routing (AAR) Access Code: 8						
			<b>Auto Route Selection (ARS) - Access Code 1: 9</b>			Access Code 2:			
			Automatic Callback Activation: *30			Deactivation: #30			
			Call Forwarding Activation Busy/DA: *31 All: *32			Deactivation: #32			
			Call Forwarding Enhanced Status: *33 Act: *34			Deactivation: #34			

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
0		1	1	2	op		n
0		11	11	2	op		n
011		12	18	2	intl		n
1206		11	11	2	fnpa		n
1732		11	11	2	fnpa		n
1800		11	11	2	fnpa		n
1877		11	11	2	fnpa		n
1908		11	11	2	fnpa		n
411		3	3	2	svcl		n

The route pattern defines which trunk group will be used for an outgoing call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider route pattern in the following manner. The example below shows the values used for route pattern 2 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **2** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk:** Set the prefix mark (**Pfx Mrk**) to **1**. This will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance numbers within the North American Numbering Plan (NANP).
- **Numbering Format:** **unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

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

Use the **save translation** command to save all Communication Manager configuration described in **Section 5**.

## 6. Configure Avaya Aura® Session Manager

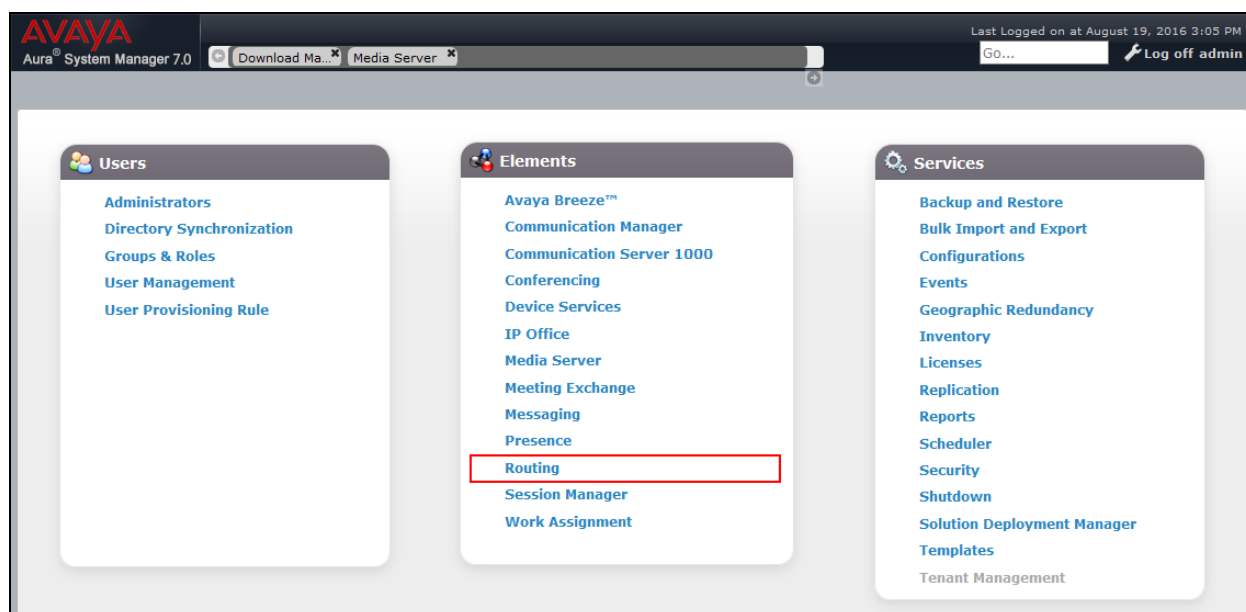
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Location
- Adaptation Modules
- SIP Entities
- Entity Links
- Routing Policies
- Dial Patterns
- Session Manager

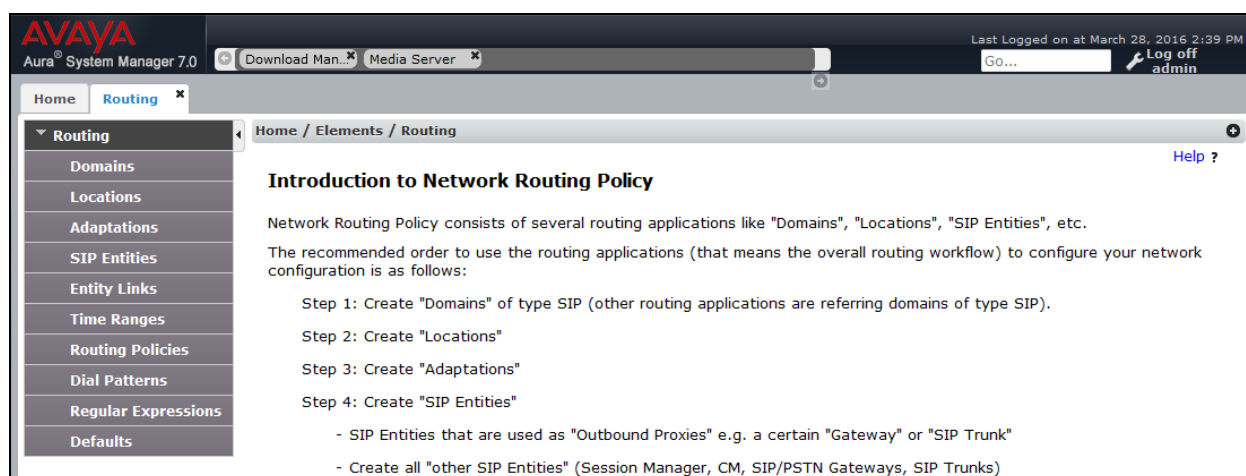
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

## 6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The following page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements** → **Routing** link highlighted below.



Clicking the **Elements** → **Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.





## 6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**customera.com**) as defined in **Section 5.5**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).


Click **Commit**. The screen below shows the entry for the enterprise domain.

[Home](#) / [Elements](#) / [Routing](#) / [Domains](#)

Domain Management

[Help ?](#)

CommitCancel

1 Item 

Filter: [Enable](#)

Name	Type	Notes
* <input type="text" value="customera.com"/>	<input type="text" value="sip"/> ▼	<input type="text"/>

### 6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single location was defined for the enterprise. The screens below show the addition of the location named **Main**, which includes all equipment at the enterprise including Communication Manager, Session Manager and the Avaya SBCE.

To add a location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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).

Home / Elements / Routing / Locations

Help ?

## Location Details

Commit Cancel

General

\* Name:

Notes:

Click **Commit** to save.

The enterprise equipment (e.g., Communication Manager, Session Manager and the Avaya SBCE ) will be associated with this location through the configuration of their respective SIP entities in **Section 6.5**.

## 6.4. Add Adaptation

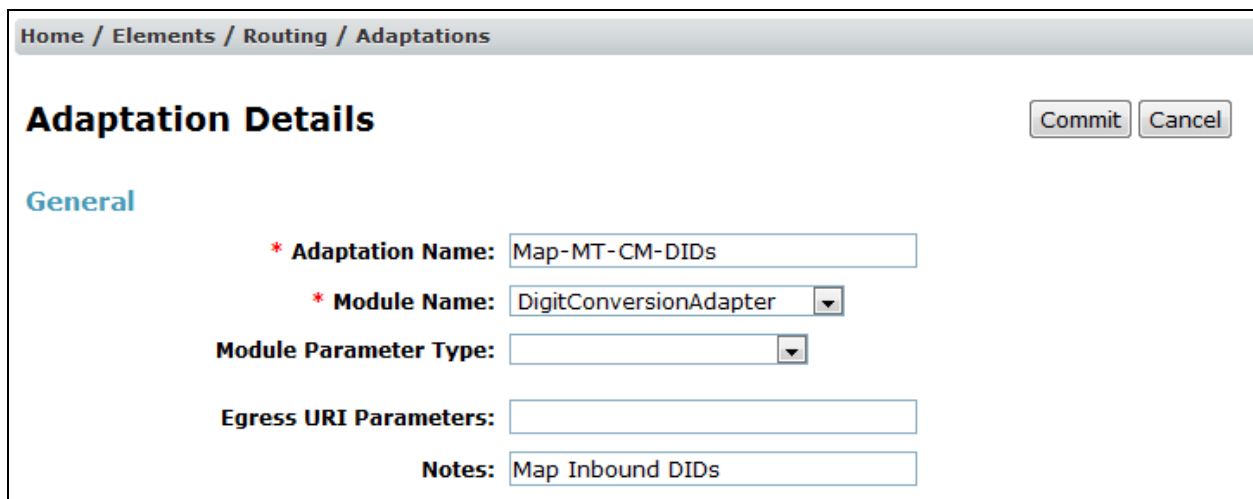
Session Manager can be configured with adaptations that can modify SIP messages before or after routing decisions have been made or perform digit manipulation. The adaptation **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages.

For the compliance test, two adaptations were used. The first adaptation was applied to the Communication Manager SIP entity and performs the mapping of inbound DID numbers from X5 Solutions to local Communication Manager extensions. The second adaptation was applied to the Avaya SBCE SIP entity and it removes SIP headers that are not used by the service provider.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the adaptation (e.g., **Map-MT-CM-DIDs**).
- **Module Name:** Select **DigitConversionAdapter** from the drop-down menu.
- **Module Parameter Type:** Leave blank.
- **Notes:** Enter a description (optional).



Home / Elements / Routing / Adaptations

### Adaptation Details

Commit Cancel

**General**

\* **Adaptation Name:** Map-MT-CM-DIDs

\* **Module Name:** DigitConversionAdapter ▼

**Module Parameter Type:** ▼


**Egress URI Parameters:**

**Notes:** Map Inbound DIDs


To map inbound DID numbers from X5 Solutions to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the digits to insert at the beginning of the received number.
- **Address to modify:** Select **destination** since this digit conversion only applies to the destination number.

Click **Commit** to save.

Digit Conversion for Outgoing Calls from SM									
<input type="button" value="Add"/> <input type="button" value="Remove"/>									
16 Items  Filter: Enable									
<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Da	
<input type="checkbox"/>	* 2065551234	* 10	* 10		* 10	19101	destination		
<input type="checkbox"/>	* 2065551235	* 10	* 10		* 10	19102	destination		
<input type="checkbox"/>	* 2065551236	* 10	* 10		* 10	19103	destination		
<input type="checkbox"/>	* 2065551237	* 10	* 10		* 10	19104	destination		

In a real customer environment, often the DID number is comprised of the local extension plus a prefix. If this is true, then a single digit conversion entry can be created for all extensions. In the example below, a 5 digit prefix is deleted from each incoming DID number leaving a 5 digit extension to be routed by Session Manager.

Digit Conversion for Outgoing Calls from SM									
<input type="button" value="Add"/> <input type="button" value="Remove"/>									
16 Items  Filter: Enable									
<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Da	
<input type="checkbox"/>	* 20655	* 10	* 10		* 5		destination		

To create the Adaptation that will be applied to the Avaya SBCE SIP entity, click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the adaptation (e.g., **Service-Provider-General**).
- **Module Name:** Select **DigitConversionAdapter** from the drop-down menu.
- **Module Parameter Type:** Enter **Name-Value Parameter**. This section will expand with an area to enter **Name** and **Value** pairs. Click **Add**. To remove headers on the egress side of Session Manager (i.e., towards the Avaya SBCE) enter the keyword **eRHdrs** in the **Name** field and a comma-separated list of headers to remove in the **Value** field. For the compliance test, the list of removed headers included **AV-Correlation-ID, AV-Global-Session-ID, Endpoint-View, P-AV-Message-ID, P-Charging-Vector** and **P-Location**.
- **Notes:** Enter a description (optional).

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

\* Adaptation Name: Service-Provider-General

\* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

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

Select : All, None

Egress URI Parameters:

Notes:

## 6.5. Add SIP Entity

A SIP entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Notes:** Brief description (optional)
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all components were located in location **Main** created in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.

The screenshot shows the 'SIP Entity Details' form in the Avaya Session Manager interface. The breadcrumb navigation at the top reads 'Home / Elements / Routing / SIP Entities'. The form is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons in the top right corner. The 'General' section is active, showing the following fields: 'Name' (required, value: 'asm'), 'FQDN or IP Address' (required, value: '192.168.67.47'), 'Type' (dropdown menu, value: 'Session Manager'), 'Notes' (text area, value: 'Expressway'), 'Location' (dropdown menu, value: 'Main'), 'Outbound Proxy' (dropdown menu, empty), 'Time Zone' (dropdown menu, value: 'America/New\_York'), and 'Credential name' (text area, empty). Below the 'General' section is the 'SIP Link Monitoring' section, which contains a 'SIP Link Monitoring' dropdown menu with the value 'Use Session Manager Configuration'.

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Listen Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.


Defaults can be used for the remaining fields. Click **Commit** to save.









Multiple port entries are shown in the screenshot below. The first two are standard ports used for SIP traffic: port 5060 for TCP and port 5061 for TLS. These ports were provisioned as part of the Session Manager installation not covered by this document. In addition, port 5068 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list and highlighted below.

**Listen Ports**

TCP Failover port:

TLS Failover port:

5 Items  Filter: [Enable](#)

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP 	customera.com 	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	5061	TLS 	customera.com 	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	5062	TCP 	customera.com 	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	5068	TLS 	customera.com 	<input type="checkbox"/>	<input type="text"/>

The following screen shows the addition of Communication Manager. Typically, when Session Manager is first installed, a SIP entity and entity link are created for Communication Manager to carry intra-enterprise SIP traffic. In order for Session Manager to separate SIP service provider traffic on a separate entity link to Communication Manager, the creation of a second SIP entity for Communication Manager is needed. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the adaptation previously defined for dial plan digit manipulation in **Section 6.4**. The **Location** field is set to **Main** which is the location where Communication Manager resides (**Section 6.3**).

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#)

## SIP Entity Details

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

### General

\*

Name:

ACM\_public

\*

FQDN or IP Address:

192.168.67.202

Type:

CM

Notes:

Adaptation:

Map-MT-CM-DIDs

Location:

Main

Time Zone:

America/New\_York

\*

SIP Timer B/F (in seconds):

4

Credential name:

Securable:

☐

Call Detail Recording:

none

### Loop Detection

Loop Detection Mode:

Off

### SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration



The following screen shows the addition of the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). For the **Adaptation** field, select the adaptation previously defined for the Avaya SBCE in **Section 6.4**. The **Location** field is set to **Main** which is the location defined for the subnet where the Avaya SBCE resides.

Home / Elements / Routing / SIP Entities

Help ?

SIP Entity Details

Commit Cancel

General

\* Name:

VNJ-SBCE1

\* FQDN or IP Address:

10.32.128.18

Type:

SIP Trunk

Notes:

Adaptation:

Service-Provider-General

Location:

Main

Time Zone:

America/New\_York

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

4

Credential name:

Securable:

☐

Call Detail Recording:

egress

Loop Detection

Loop Detection Mode:

On

Loop Count Threshold:

5

Loop Detection Interval (in msec):

200

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

## 6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an entity link. Two entity links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an entity link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager SIP entity (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system using the SIP entity name defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **trusted** from pull-down menu.

Click **Commit** to save.

For the Communication Manager entity link (**sm\_ACM\_public\_5068\_TLS**), the protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. Specifically, the following fields must match:

- **Protocol** must match the **Transport Method** from **Section 5.6**. For the compliance test, the TCP protocol was used but the recommended configuration is to use TLS.
- SIP Entity 1 **Port** must match the **Far-end Listen Port** from **Section 5.6**.
- **SIP Entity 2** must match the SIP Entity defined for Communication Manager in **Section 6.5**.
- SIP Entity 2 **Port** must match the **Near-End Listen Port** from **Section 5.6**.

For the Avaya SBCE entity link (**VNJ-SBCE1-Link**), the protocol and ports defined here must match the values used on the Avaya SBCE in **Section 7**. Specifically, the following fields must match:

- **Protocol** must match the protocol used by the Avaya SBCE Routing profile to reach Session Manager. This value is shown in the **Next Hop Address** in **Section 7.11.1**.
- SIP Entity 1 **Port** must match the port value used by the Avaya SBCE Routing profile to reach Session Manager. This value is shown in the **Next Hop Address** in **Section 7.11.1**.
- **SIP Entity 2** must match the SIP entity defined for the Avaya SBCE in **Section 6.5**.
- SIP Entity 2 **Port** must match the port value defined in the Avaya SBCE internal signaling interface in **Section 7.3** for the selected protocol.

The screen below shows the completed entity links for both Communication Manager and the Avaya SBCE.

Home / Elements / Routing / Entity Links Help ?

### Entity Links

14 Items Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	<a href="#">BSM ACM local 5060 TCP</a>	BSM	TCP	5060	ACM_local	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	Branch local trunk
<input type="checkbox"/>	<a href="#">BSM ACM public 5062 TCP</a>	BSM	TCP	5062	ACM_public	<input type="checkbox"/>	5062	trusted	<input type="checkbox"/>	Branch public trunk
<input type="checkbox"/>	<a href="#">BSM SBCE 5060 TCP</a>	BSM	TCP	5060	SBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	Branch to ATT
<input type="checkbox"/>	<a href="#">sm AA-M 5060 TCP</a>	asm	TCP	5060	AA-M	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm ACM521 local 5060 TCP</a>	asm	TCP	5060	ACM521_local	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm ACM521 public 5062 TCP</a>	asm	TCP	5062	ACM521_public	<input type="checkbox"/>	5062	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm ACM local 5060 TCP</a>	asm	TCP	5060	ACM_local	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm ACM Meet-Me</a>	asm	TCP	5080	ACM_Meet-Me	<input type="checkbox"/>	5080	trusted	<input type="checkbox"/>	meet-me conf
<input type="checkbox"/>	<a href="#">sm ACM public 5068 TLS</a>	asm	TLS	5068	ACM_public	<input type="checkbox"/>	5068	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm ANS</a>	asm	TCP	5060	ANS	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm CS1K 5060 TCP</a>	asm	TCP	5060	CS1K	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm ExPortal 5060 TCP</a>	asm	TCP	5060	ExPortal	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">sm SBCE 5060 TCP</a>	asm	TCP	5060	SBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">VNJ-SBCE-Link</a>	asm	TCP	5060	VNJ-SBCE1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Select : All, None

## 6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

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

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the routing policy for Communication Manager.

Home / Elements / Routing / Routing Policies Help ?

### Routing Policy Details

Commit Cancel

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
ACM_public	192.168.67.202	CM	

The following screen shows the routing policy for the Avaya SBCE.

Home / Elements / Routing / Routing Policies

Help ?

Routing Policy Details

CommitCancel

General

\* Name: VNJ-SBCE1-RP

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
VNJ-SBCE1	10.32.128.18	SIP Trunk	

## 6.8. Add Dial Patterns

Dial patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to X5 Solutions and vice versa. Dial patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that outbound long distance numbers (11 digits) that begin with **1** and have a destination domain of **customerera.com** from **ALL** locations use route policy **VNJ-SBCE1-RP**.

Home / Elements / Routing / Dial Patterns

Help ?

CommitCancel

### Dial Pattern Details

General

\* Pattern: 1

\* Min: 11

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: customerera.com

Notes: Outbound NANP Numbers

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		VNJ-SBCE1-RP	0	<input type="checkbox"/>	VNJ-SBCE1	

Select : All, None

The second example shows that incoming DID numbers (10 digits) that start with **206555** to domain **customera.com** and originating from **ALL** locations use route policy **ACM\_Public**. These are the DID numbers assigned to the enterprise from X5 Solutions. All other Dial Patterns used as part of the compliance test were configured in a similar manner.

Home / Elements / Routing / Dial Patterns

Help ?

CommitCancel

Dial Pattern Details

General

\* Pattern: 206555

\* Min: 10

\* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: customera.com

Notes: X5 DIDs

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		ACM_Public	2	<input type="checkbox"/>	ACM_public	

Select : All, None



## 6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is most likely done as part of the initial Session Manager installation. To add a Session Manager, from the **Home** page, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the host name or IP address of the Session Manager management interface.

The screen below shows the Session Manager values used for the compliance test.

The screenshot displays the 'View Session Manager' configuration interface. At the top, there is a breadcrumb trail: 'Home / Elements / Session Manager'. A 'Help ?' link is located in the top right corner. Below the breadcrumb, the title 'View Session Manager' is shown, followed by a 'Return' button. A navigation bar contains links: 'General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |'. Below this, there are 'Expand All' and 'Collapse All' links. The 'General' section is expanded, showing the following fields:

- SIP Entity Name:
- Description:
- Management Access Point Host Name/IP:
- Direct Routing to Endpoints:
- Maintenance Mode: ☐

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the **SIP Entity Name**. Otherwise, enter the IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.

The screenshot displays the 'Security Module' configuration window. It contains the following fields and values:

Field	Value
SIP Entity IP Address	192.168.67.47
Network Mask	255.255.255.0
Default Gateway	192.168.67.1
Call Control PHB	46
*SIP Firewall Configuration	Rule Set for asm

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface must be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1).

On all screens described in this section, it is assumed that parameters are left at their default values unless specified otherwise.

### 7.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.



The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black font. On the right, under the heading 'Log In', there are input fields for 'Username:' (containing 'ucsec') and 'Password:'. Below these fields is a 'Log In' button. Further down, there is a disclaimer text: 'This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.' Below this is another paragraph: 'The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.' This is followed by a third paragraph: 'All users must comply with all corporate instructions regarding the protection of information assets.' At the bottom, it says '© 2011 - 2015 Avaya Inc. All rights reserved.'

After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

DashboardAdministrationBackup/RestoreSystem Management▸ Global Parameters▸ Global Profiles▸ PPM Services▸ Domain Policies▸ TLS Management▸ Device Specific Settings

Dashboard

Information

System Time	01:56:56 PM CDT	<a href="#">Refresh</a>
Version	7.0.1-03-8739	
Build Date	Fri Jan 15 22:53:12 EST 2016	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	03/30/2016 11:01:12 CDT	
Failed Login Attempts	0	

Alarms (past 24 hours)  
None found.

Installed Devices

EMS

sp-ucsec1

Incidents (past 24 hours)

sp-ucsec1: Max forwards Exceeded

sp-ucsec1: Max forwards Exceeded

CTM; Reviewed:  
SPOC 11/3/2016

Solution & Interoperability Test Lab Application Notes  
©2016 Avaya Inc. All Rights Reserved.

44 of 80  
X5C70S70SBCE7

## 7.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

PPM Services

Domain Policies

TLS Management

Device Specific Settings

System Management

Devices

Updates

SSL VPN

Licensing

Device Name	Management IP	Version	Status	
sp-ucsec1	10.32.101.10	7.0.1-03-8739	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. The two **Network Configuration** entries highlighted below are the only two IP addresses that are directly related to the SIP trunking solution described in these Application Notes. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE respectively. Each of these interfaces must be enabled after installation.

System Information: sp-ucsec1

General Configuration

Appliance Name sp-ucsec1

Box Type SIP

Deployment Mode Proxy

Device Configuration

HA Mode No

Two Bypass Mode No

License Allocation

Standard Sessions Requested: 0 0

Advanced Sessions Requested: 0 0

Scopia Video Sessions Requested: 0 0

Encryption ☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.32.128.18	10.32.128.18	255.255.255.0	10.32.128.254	A1
192.168.96.228	192.168.96.228	255.255.255.224	192.168.96.254	B1
192.168.96.230	192.168.96.230	255.255.255.224	192.168.96.254	B1
192.168.96.229	192.168.96.229	255.255.255.224	192.168.96.254	B1
10.32.128.19	10.32.128.19	255.255.255.0	10.32.128.254	A1

DNS Configuration

Primary DNS 192.168.132.219

Secondary DNS

DNS Location DMZ

DNS Client IP 10.32.128.18

Management IP(s)

IP 10.32.101.10

To enable the interfaces, first navigate to **Device Specific Settings** → **Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the status **Enabled/Disabled** to toggle the state of the interface.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ PPM Services

▸ Domain Policies

▸ TLS Management

▾ Device Specific Settings

**Network Management**

Media Interface

Network Management: sp-ucsec1

Devices

sp-ucsec1

Interfaces

Networks

Add VLAN

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

## 7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by one or more pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int\_Sig\_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext\_Sig\_Intf** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for TCP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since X5 Solutions will send messages using UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.

### Session Border Controller for Enterprise

Dashboard  
Administration  
Backup/Restore  
System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- ▾ Device Specific Settings
  - Network Management
  - Media Interface
  - Signaling Interface**
  - End Point Flows
  - Session Flows
    - DMZ Services
  - TURN/STUN Service
  - SNMP

Devices

- sp-ucsec1**

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_Intf	10.32.128.18 Network_A1 (A1, VLAN 0)	5060	---	---	None	Edit Delete
Ext_Sig_Intf	192.168.96.228 Network_B1-2 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
RW_Ext_Sig	192.168.96.229 Network_B1-2 (B1, VLAN 0)	5060	---	5061	AvayaSBCServer	Edit Delete
RW_Int_Sig	10.32.128.19 Network_A1 (A1, VLAN 0)	5060	---	5061	AvayaSBCServer	Edit Delete

CTM; Reviewed:  
SPOC 11/3/2016

Solution & Interoperability Test Lab Application Notes  
©2016 Avaya Inc. All Rights Reserved.

47 of 80  
X5C70S70SBCE7

## 7.4. Media Interface


A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings** → **Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by one or more pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int\_Media\_Intf** was created for the Avaya SBCE internal interface and media interface **Ext\_Media\_Intf** was created for the Avaya SBCE external interface. Each is highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Media IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.

### Session Border Controller for Enterprise



Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings
  - Network Management
    - Media Interface**
    - Signaling Interface
    - End Point Flows
    - Session Flows
    - DMZ Services

Media Interface: sp-ucsec1

Devices

sp-ucsec1

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		
Int_Media_Intf	10.32.128.18 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.228 Network_B1-2 (B1, VLAN 0)	35000 - 40000	Edit	Delete
RW_Med_Outside_229	192.168.96.229 Network_B1-2 (B1, VLAN 0)	35000 - 40000	Edit	Delete
RW_Med_Inside_19	10.32.128.19 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete



## 7.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create a server interworking profile for Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Sections 7.6.1** and **7.6.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Server Interworking (highlighted). The main content area is titled "Interworking Profiles: avaya-ru" and features an "Add" button. Below this is a list of profiles: cs2100, avaya-ru (selected), OCS-Edge-Se..., cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd..., and Avaya SM. To the right of the profile list is a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below the warning are tabs for General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The General tab is active, showing a table of settings:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No

### 7.5.1. Server Interworking – Session Manager

For the compliance test, server interworking profile **Avaya-SM-T38** was created for Session Manager by cloning the existing profile **avaya-ru**. **T.38 Support** was set to **Yes**. Highlighted values in this section indicate changes from the cloned profile or the default value. The **General** tab parameters are shown below.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
<b>General</b>					
Hold Support	NONE				
180 Handling	None				
181 Handling	None				
182 Handling	None				
183 Handling	None				
Refer Handling	No				
URI Group	None				
Send Hold	No				
Delayed Offer	No				
3xx Handling	No				
Diversion Header Support	No				
Delayed SDP Handling	No				
Re-Invite Handling	No				
Prack Handling	No				
Allow 18X SDP	No				
<b>T.38 Support</b>	<b>Yes</b>				
URI Scheme	SIP				
Via Header Format	RFC3261				
<input type="button" value="Edit"/>					

The **Timers**, **Privacy**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes		Both Sides			
Include End Point IP for Context Lookup		Yes			
Extensions		Avaya			
Diversion Manipulation		No			
Has Remote SBC		Yes			
Route Response on Via Port		No			
DTMF					
DTMF Support		None			
<div>Edit</div>					

### 7.5.2. Server Interworking – X5 Solutions

For the compliance test, server interworking profile **SP-General-T38** was created for the X5 Solutions SIP server. When creating the profile, the default values were used for all parameters with the exception that **T.38 Support** was set to **Yes**. The **General** tab parameters are shown below.

The screenshot shows a configuration window for the 'SP-General-T38' profile. At the top, there are six tabs: 'General' (highlighted in red), 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. Below the tabs is a table of parameters. The 'T.38 Support' row is highlighted with a red border. At the bottom of the table is an 'Edit' button.

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

Edit

The **Timers**, **Privacy**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

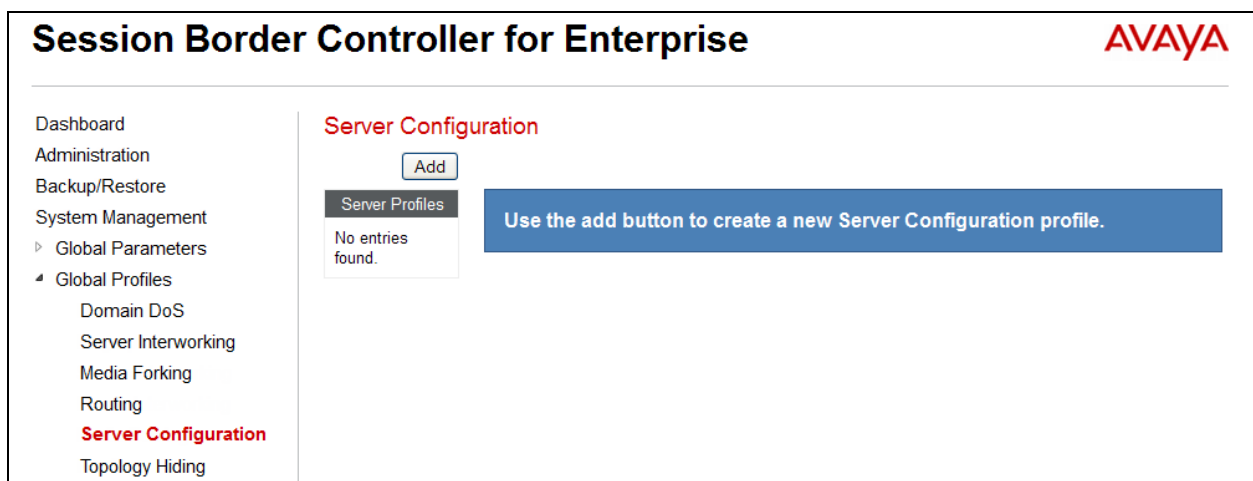
The **Advanced** tab parameters are shown below.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes ---					
Include End Point IP for Context Lookup No					
Extensions None					
Diversion Manipulation No					
Has Remote SBC Yes					
Route Response on Via Port No					
DTMF					
DTMF Support None					
<a href="#">Edit</a>					

## 7.6. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a server configuration profile for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured. Once complete, the profile name will appear under **Server Profiles** in the center pane and the settings will be shown in the far right pane. If a profile already exists, then the settings of the existing profile may be viewed by selecting the profile from the center pane. The settings will appear in the right pane.



### 7.6.1. Server Configuration – Session Manager

For the compliance test, server configuration profile **Expway-SM** was created for Session Manager. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Call Server**.
- Enter a valid combination of **IP Address / FQDN**, **Port** and **Transport** that Session Manager will use to listen for SIP requests. The standard SIP UDP/TCP port is 5060. The standard SIP TLS port is 5061. Additional combinations can be entered by clicking the **Add** button (not shown).

The screenshot displays the configuration interface for a Session Manager profile. At the top right are buttons for 'Rename', 'Clone', and 'Delete'. Below these are four tabs: 'General' (highlighted in red), 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab contains a 'Server Type' dropdown set to 'Call Server'. Below this is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The table contains two entries: one for TCP on port 5060 and another for TLS on port 5061, both using the IP address 192.168.67.47. An 'Edit' button is located at the bottom of the table.

IP Address / FQDN	Port	Transport
192.168.67.47	5060	TCP
192.168.67.47	5061	TLS

The **Authentication** and **Heartbeat** tabs have no entries.

On the **Advanced** tab, check **Enable Grooming** and set the **Interworking Profile** field to the interworking profile for Session Manager defined in **Section 7.5.1**. Set the **TLS Client Profile** to the profile containing the proper TLS certificates for the customer environment. A complete description of the use of TLS certificates are beyond the scope of these Application Notes. For more information on TLS certificates and the Avaya SBCE see reference [8].

Rename Clone Delete

General
Authentication
Heartbeat
Advanced

Enable DoS Protection

Enable Grooming

Interworking Profile

TLS Client Profile

Signaling Manipulation Script

Connection Type

Securable

☐

☒

Avaya-SM-T38

TimSBCCClient

None

SUBID

☐

Edit

### 7.6.2. Server Configuration – X5 Solutions

For the compliance test, server configuration profile **SP-X5** was created for X5 Solutions. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Trunk Server**.
- Enter a valid combination of **IP Address / FQDN**, **Port** and **Transport** that the X5 Solutions SIP proxy will use to listen for SIP requests. This information is provided by X5 Solutions. Additional combinations can be entered by clicking the **Add** button (not shown). The Avaya SBCE will perform a DNS lookup on the FQDN provided by X5 Solutions to determine the IP address of the server.

General
Authentication
Heartbeat
Advanced

Server Type

IP Address / FQDN

accesspbx2.x5sip.com

Trunk Server

Port

5060

Transport

UDP

Edit

X5 Solutions requires use of Digest Authentication to authenticate each SIP request from the enterprise. On the **Authentication** tab, check the **Enable Authentication** box. Enter the **User Name** and **Password** (not shown) provided by X5 Solutions.



General	<b>Authentication</b>	Heartbeat	Advanced
Enable Authentication		<input checked="" type="checkbox"/>	
User Name		2065551234	
Realm		---	
		<input type="button" value="Edit"/>	

On the **Heartbeat** tab, keep the default values.

On the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for X5 Solutions defined in **Section 7.5.2**.

		<input type="button" value="Rename"/>	<input type="button" value="Clone"/>	<input type="button" value="Delete"/>
General	Authentication	Heartbeat	<b>Advanced</b>	
Enable DoS Protection		<input type="checkbox"/>		
Enable Grooming		<input type="checkbox"/>		
Interworking Profile		SP-General-T38		
Signaling Manipulation Script		None		
Connection Type		SUBID		
Securable		<input type="checkbox"/>		
		<input type="button" value="Edit"/>		

## 7.7. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 7.10**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Session Manager and the X5 Solutions SIP server.

To view an existing rule, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select the rule (e.g., **default-trunk**) to be viewed.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies (expanded), Application Rules (selected), Border Rules, Media Rules, Security Rules, Signaling Rules, End Point Policy Groups, Session Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Application Rules: default-trunk' and includes an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, the 'Application Rule' configuration is shown in a table format.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

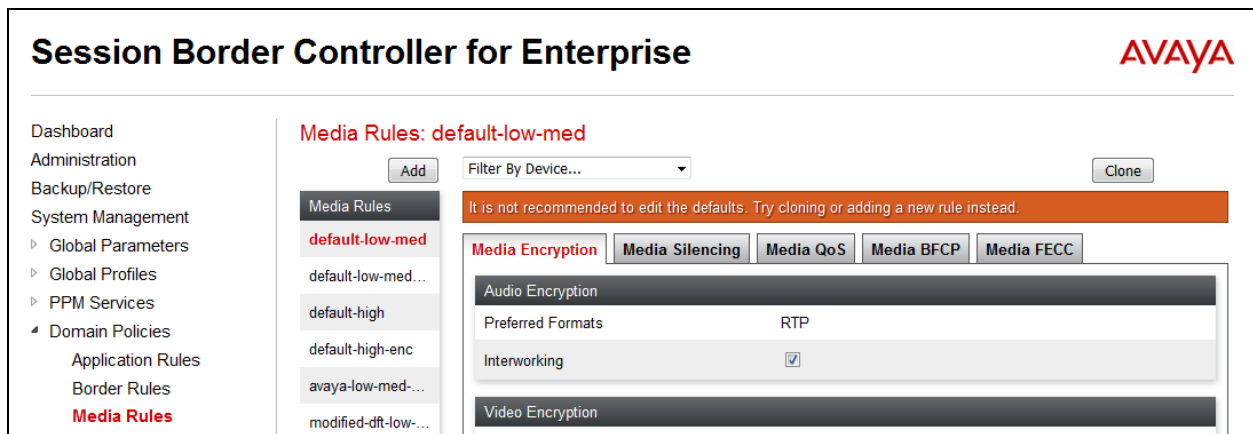
An 'Edit' button is located at the bottom of the configuration area.

## 7.8. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.10**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Session Manager and the X5 Solutions SIP server.

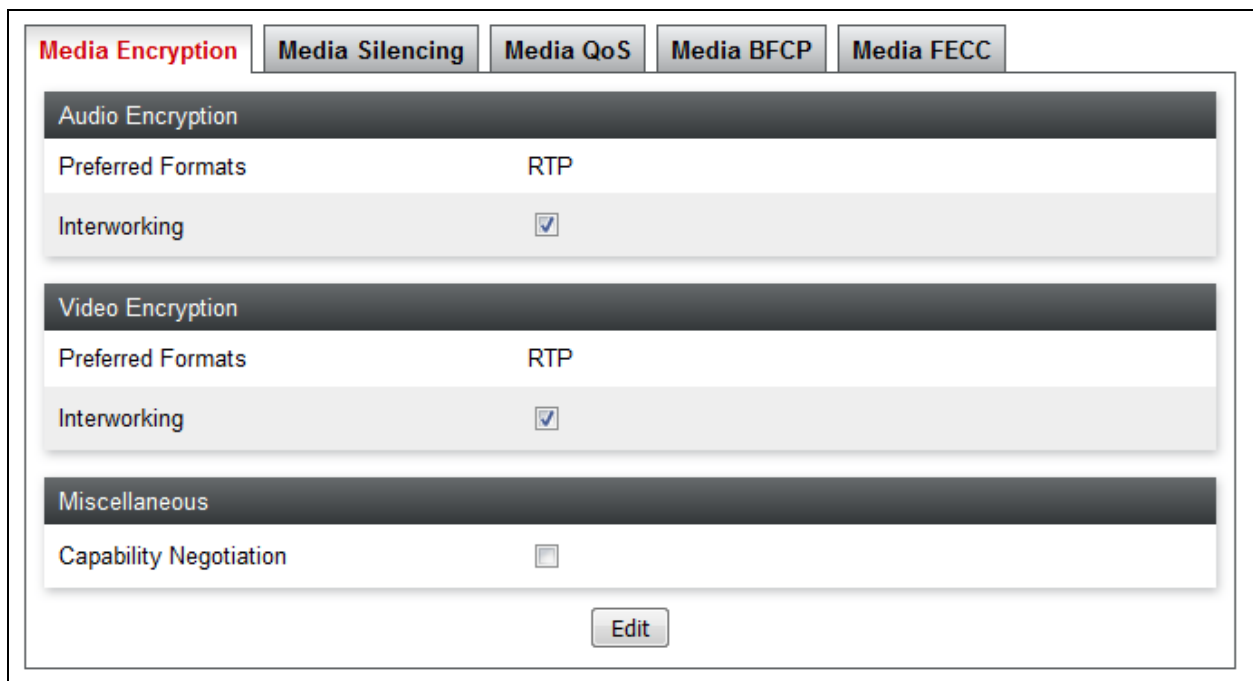
To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.

The contents of the **default-low-med** media rule are described below.



The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left navigation pane includes 'Domain Policies' with 'Media Rules' selected. The main content area displays the 'Media Rules: default-low-med' configuration. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, the 'Media Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. Other tabs like 'Media Silencing', 'Media QoS', 'Media BFCP', and 'Media FECC' are visible but not active.

The **Media Encryption** tab shows the **Preferred Formats** field for both Audio Encryption and Video Encryption is set to **RTP** (as opposed to **SRTP**) indicating that no encryption was used.



This detailed view of the 'Media Encryption' tab shows the configuration for 'Audio Encryption' and 'Video Encryption'. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. There is also a 'Miscellaneous' section with 'Capability Negotiation' unchecked. An 'Edit' button is located at the bottom of the configuration area.

On the **Media Silencing** tab, **Media Silencing** is disabled.

The screenshot shows a configuration interface with five tabs: Media Encryption, Media Silencing (highlighted in red), Media QoS, Media BFCP, and Media FECC. Below the tabs is a section titled "Media Silencing" with a single checkbox that is unchecked. An "Edit" button is located at the bottom right of the section.

The **Media QoS** settings are shown below. These QoS settings are not a requirement for interoperability and QoS was not tested as part of the compliance test. If the QoS settings shown here do not meet the needs of the customer then the media rule should be cloned and modified as per customer requirements.

The screenshot shows a configuration interface with five tabs: Media Encryption, Media Silencing, Media QoS (highlighted in red), Media BFCP, and Media FECC. Below the tabs are two sections. The first section, "Media QoS Reporting", contains a checkbox for "RTCP Enabled" which is unchecked. The second section, "Media QoS Marking", contains a checkbox for "Enabled" which is also unchecked. An "Edit" button is located at the bottom right of the section.

On the **Media BFCP** tab, BFCP is disabled.

The screenshot shows a configuration interface with five tabs: Media Encryption, Media Silencing, Media QoS, Media BFCP (highlighted in red), and Media FECC. Below the tabs is a section titled "Binary Floor Control Protocol" with a checkbox for "BFCP Enabled" which is unchecked. An "Edit" button is located at the bottom right of the section.

On the **Media FECC** tab, FECC is disabled.

The screenshot shows a configuration interface with five tabs: Media Encryption, Media Silencing, Media QoS, Media BFCP, and Media FECC. The Media FECC tab is selected and highlighted in red. Below the tabs is a section titled "Far End Camera Control" with a dark header. Under this header, there is a label "FECC Enabled" followed by an unchecked checkbox. At the bottom of this section is an "Edit" button.

## 7.9. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.10**. A specific signaling rule was created for Session Manager and the X5 Solutions SIP server.

To create a new rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by one or more pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. Under 'Domain Policies', 'Signaling Rules' is highlighted. The main content area is titled 'Signaling Rules: default' and includes an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'General' tab is active, showing 'Inbound' and 'Outbound' sections. Each section contains a table with four rows: 'Requests', 'Non-2XX Final Responses', 'Optional Request Headers', and 'Optional Response Headers', all set to 'Allow'.

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

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

### 7.9.1. Signaling Rules – Session Manager

For the compliance test, signaling rule **SM-SRules-Aura7** was created for Session Manager. **SM-SRules-Aura7** was created using all default values except the **Signaling QoS** tab.

The **General** tab settings are shown below.

<b>General</b>	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
<b>Inbound</b>						
Requests		Allow				
Non-2XX Final Responses		Allow				
Optional Request Headers		Allow				
Optional Response Headers		Allow				
<b>Outbound</b>						
Requests		Allow				
Non-2XX Final Responses		Allow				
Optional Request Headers		Allow				
Optional Response Headers		Allow				
<b>Content-Type Policy</b>						
Enable Content-Type Checks		<input checked="" type="checkbox"/>				
Action	Allow	Multipart Action	Allow			
Exception List		Exception List				
<div>Edit</div>						

The **Requests**, **Responses**, **Request Headers**, and **Response Headers** tabs have no entries.

The **Signaling QoS** settings used for the compliance test are shown below. These QoS settings are not a requirement for interoperability and QoS was not tested as part of the compliance test. If the QoS settings shown here do not meet the needs of the customer then the signaling rule should be set as per customer requirements.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
<div>Signaling QoS <input checked="" type="checkbox"/></div> <div>QoS Type DSCP</div> <div>DSCP EF</div> <div>Edit</div>						

The **UCID** setting is shown below.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
<div>UCID <input type="checkbox"/></div> <div>Edit</div>						



## 7.9.2. Signaling Rules – X5 Solutions

The **SrvPrvder-SR2** signaling rule (shown below) was used for the X5 Solutions SIP server. The **General** tab settings use the default values and are shown below.

<b>General</b>	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
<b>Inbound</b>						
Requests		Allow				
Non-2XX Final Responses		Allow				
Optional Request Headers		Allow				
Optional Response Headers		Allow				
<b>Outbound</b>						
Requests		Allow				
Non-2XX Final Responses		Allow				
Optional Request Headers		Allow				
Optional Response Headers		Allow				
<b>Content-Type Policy</b>						
Enable Content-Type Checks		<input checked="" type="checkbox"/>				
Action	Allow	Multipart Action	Allow			
Exception List		Exception List				
<a href="#">Edit</a>						

The **Requests** tab shows the actions performed on request messages. An entry is created by clicking the **Add In Header Control** or **Add Out Header Control** button depending on the direction (relative to the Avaya SBCE) of the message to be modified. The entry shown below blocks incoming OPTIONS messages and returns a 200 OK response. See **Section 2.2** for full details.

<b>General</b>	<b>Requests</b>	Responses	Request Headers	Response Headers	Signaling QoS	UCID
<a href="#">Add In Request Control</a> <a href="#">Add Out Request Control</a>						
Row	Method Name	In Dialog Action	Out of Dialog Action	Proprietary	Direction	
1	OPTIONS	Block with "200 OK"	Block with "200 OK"	No	In	<a href="#">Edit</a> <a href="#">Delete</a>

The **Responses**, **Requests Headers** and **Response Headers** tabs have no entries.

The **Signaling QoS** settings are shown below. These QoS settings are not a requirement for interoperability and QoS was not tested as part of the compliance test. If the QoS settings shown here do not meet the needs of the customer then the signaling rule should be set as per customer requirements.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
Signaling QoS <input checked="" type="checkbox"/>						
QoS Type DSCP						
DSCP EF						
<div>Edit</div>						

The **UCID** settings are shown below.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
UCID <input type="checkbox"/>						
<div>Edit</div>						

## 7.10. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and an endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.13**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed one or more of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left navigation pane includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, and Domain Policies (selected). Under Domain Policies, there are links for Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, and End Point Policy Groups (highlighted in red). The main content area is titled 'Policy Groups: default-low' and includes an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new group instead.' Below this is a table of policy groups. The 'Policy Group' tab is selected, showing a table with columns: Order, Application, Border, Media, Security, and Signaling. The first row shows '1', 'default', 'default', 'default-low-med', 'default-low', and 'default'. An 'Edit' link is next to the last cell. A 'Summary' button is also present.

Order	Application	Border	Media	Security	Signaling
1	default	default	default-low-med	default-low	default

### 7.10.1. Endpoint Policy Group – Session Manager

For the compliance test, endpoint policy group **SM** was created for Session Manager. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Signaling**. For **Application**, enter the application rule created in **Section 7.7**. For **Signaling**, enter the signaling rule created in **Section 7.9.1**. The details of the default settings for **Media** are showed in **Section 7.8**.

The screenshot shows the 'Policy Group' configuration page. The 'Policy Group' tab is selected, showing a table with columns: Order, Application, Border, Media, Security, and Signaling. The first row shows '1', 'default-trunk', 'default', 'default-low-med', 'default-low', and 'SM-SRules-Aura7'. An 'Edit' link is next to the last cell. A 'Summary' button is also present.

Order	Application	Border	Media	Security	Signaling
1	default-trunk	default	default-low-med	default-low	SM-SRules-Aura7

## 7.10.2. Endpoint Policy Group – X5 Solutions

For the compliance test, endpoint policy group **X5-EP-Policy** was created for the X5 Solutions SIP server. Default values were used for each of the rules which comprise the group with the exception of **Application** and **Signaling**. For **Application**, enter the application rule created in **Section 7.7**. For **Signaling**, enter the signaling rule created in **Section 7.9.2**. The details of the default settings for **Media** are showed in **Section 7.8**.

Policy Group						
						Summary
Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	SrvPrvder-SR2	Edit

## 7.11. Routing

A routing profile defines where traffic will be directed based on the contents of the Request-URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 7.13**. Create a routing profile for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

### Session Border Controller for Enterprise

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Server Interworking

Media Forking

**Routing**

Server Configuration

Routing Profiles: default

Add

Routing Profiles

default

To\_SM

To\_Trunks

To\_NwkCM

To\_PrtCM

To\_PrtSM

Clone

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

Routing Profile

Update Priority

Add

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

### 7.11.1. Routing – Session Manager

For the compliance test, routing profile **To\_ExpwaySM** was created for Session Manager. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card \* to match on any URI.
- Set **Load Balancing** to **Priority** from the pull-down menu.
- Enable **Next Hop Priority**.
- Click **Add** to enter the following for the Next Hop Address:
  - Set **Priority/Weight** to **1**.
  - For **Server Configuration**, select **Expway-SM (Section 7.6.1)** from the pull-down menu. The **Next Hop Address** pull-down menu will show each entry of Address/Port/Transport defined in the **Server Configuration** selected. For the **Next Hop Address**, select the entry that represents the connection between Session Manager and the Avaya SBCE. In this case, the connection used TCP on port 5060. This must match the Session Manager SIP entity link settings for the Avaya SBCE in **Section 6.6**.

Click **Finish**.

Profile : To_ExpwaySM - Edit Rule			
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"/>
<b>Add</b>			
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Expway-SM	192.168.67.47:5060 (TCP)	None
			<a href="#">Delete</a>
<b>Finish</b>			

### 7.11.2. Routing – X5 Solutions

For the compliance test, routing profile **To\_X5** was created for X5 Solutions. When creating the profile, configure the parameters as follows:

- Set the **URI Group** to the wild card \* to match on any URI.
- Set **Load Balancing** to **DNS/SRV** from the pull-down menu.
- Click **Add** to enter the following for the Next Hop Address:
  - Set **Priority/Weight** to **1**.
  - For **Server Configuration**, select **SP-X5 (Section 7.6.2)** from the pull-down menu. The **Next Hop Address** pull-down menu will show each entry of Address/Port/Transport defined in the **Server Configuration** selected. For the **Next Hop Address**, select the entry that represents the connection between X5 Solutions and the Avaya SBCE. This connection used UDP on port 5060.

Click **Finish**.

Profile : To_X5 - Edit Rule			
URI Group	*	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
<a href="#">Add</a>			
Priority / Weight	Server Configuration	Next Hop Address	Transport
0	SP-X5	accesspbx2.x5sip.com:5060 (UDP)	None
<a href="#">Delete</a>			
<a href="#">Finish</a>			

## 7.12. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.13**.

To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a pop-up window in which a header can be selected and configured. Additional headers can be added in this window. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile (e.g., **default**), select the profile from the center pane. The settings will appear in the right pane.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, and Global Profiles (expanded). Under Global Profiles, the following options are listed: Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration, **Topology Hiding** (highlighted in red), and Signaling Manipulation.

The main content area is titled "Topology Hiding Profiles: default". It includes an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, a tab labeled "Topology Hiding" is active, showing a table of configured headers.

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

### 7.12.1. Topology Hiding – Session Manager

For the compliance test, topology hiding profile **MT-Domain** was created for Session Manager. This profile will be applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**customera.com**).

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	customera.com
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	customera.com
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	customera.com
SDP	IP/Domain	Auto	---
<input type="button" value="Edit"/>			



### 7.12.2. Topology Hiding – X5 Solutions

For the compliance test, topology hiding profile **SP-X5-TH** was created for X5 Solutions. This profile will be applied to traffic from the Avaya SBCE to X5 Solutions. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **From** which should be set to **Overwrite**. It was necessary to overwrite the From header for OPTIONS to work properly. The **Replace Action** of **Auto** puts the public IP of the SBCE in the From header which causes the OPTIONS message to return an error.
- For those headers to be overwritten, the **Overwrite Value** is set to the X5 Solutions domain (**accesspbx2.x5sip.com**).

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	accesspbx2.x5sip.com
Referred-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
<div>Edit</div>			

## 7.13. End Point Flows

Endpoint flows are used to determine the endpoints (connected servers) involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the endpoints are Session Manager and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the far right pane.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, Signaling Interface, and End Point Flows (highlighted in red). The main content area is titled "End Point Flows: sp-ucsec1". It features a "Devices" tab with "sp-ucsec1" selected. Below this, there are two tabs: "Subscriber Flows" and "Server Flows" (selected). An "Add" button is located in the top right corner of the "Server Flows" tab. The "Server Configuration: Avaya-SM" section includes an "Update" button and a table of configured flows.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya-SM	*	Ext_Sig_Intf	Int_Sig_Intf	SM	To_Trunks	View Clone Edit Delete
2	RW-Avaya-SM	*	RW_Ext_Sig	RW_Int_Sig	Remote-User-SM	default	View Clone Edit Delete

### 7.13.1. End Point Flow – Session Manager

For the compliance test, endpoint flow **Expway-SM** was created for Session Manager. All traffic from Session Manager will match this flow as the source flow and use the specified **Routing Profile To\_X5** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.6.1**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to \*.
- Set the **Received Interface** to the external signaling interface (**Section 7.3**).
- Set the **Signaling Interface** to the internal signaling interface (**Section 7.3**).
- Set the **Media Interface** to the internal media interface (**Section 7.4**).
- Set the **End Point Policy Group** to the endpoint policy group defined for Session Manager in **Section 7.10.1**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.11.2** used to direct traffic to the X5 Solutions SIP server.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.12.1**.

View Flow: Expway-SM

X

Criteria	
Flow Name	Expway-SM
Server Configuration	Expway-SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf

Profile	
Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	SM
Routing Profile	To_X5
Topology Hiding Profile	MT-Domain
Signaling Manipulation Script	None
Remote Branch Office	Any

### 7.13.2. End Point Flow – X5 Solutions

For the compliance test, endpoint flow **X5-Flow** was created for the X5 Solutions SIP server. All traffic from X5 Solutions will match this flow as the source flow and use the specified **Routing Profile To\_ExpwaySM** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the X5 Solutions SIP server created in **Section 7.6.2**.
- To match all traffic, set the **URI Group**, **Transport**, and **Remote Subnet** to \*.
- Set the **Received Interface** to the internal signaling interface (**Section 7.3**).
- Set the **Signaling Interface** to the external signaling interface (**Section 7.3**).
- Set the **Media Interface** to the external media interface (**Section 7.4**).
- Set the **End Point Policy Group** to the endpoint policy group defined for X5 Solutions in **Section 7.10.2**.
- Set the **Routing Profile** to the routing profile defined in **Section 7.11.1** used to direct traffic to Session Manager.
- Set the **Topology Hiding Profile** to the topology hiding profile defined for X5 Solutions in **Section 7.12.2**.

View Flow: X5-Flow

X

Criteria	
Flow Name	X5-Flow
Server Configuration	SP-X5
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf

Profile	
Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
End Point Policy Group	X5-EP-Policy
Routing Profile	To_ExpwaySM
Topology Hiding Profile	SP-X5-TH
Signaling Manipulation Script	None
Remote Branch Office	Any

## 8. X5 Solutions SIP Trunking Service Configuration

X5 Solutions is responsible for the network configuration and deployment of the X5 Solutions SIP Trunking Service.

X5 Solutions will require that the customer provide the IP address and port number used to reach the Avaya SBCE at the edge of the enterprise. X5 Solutions will provide the FQDN and port number of the X5 Solutions SIP proxy/SBC, IP addresses/ports of media sources, SIP credentials and DID numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager and Avaya SBCE configuration discussed in the previous sections.

## 9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that a user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

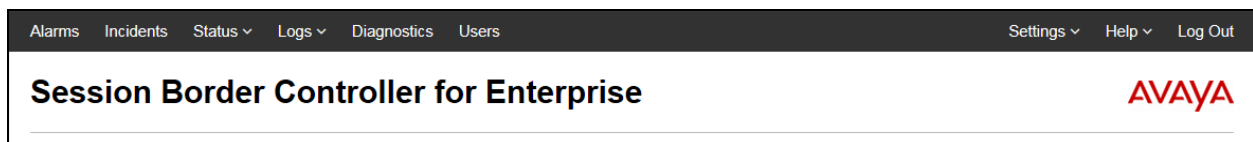
1. Communication Manager:
  - **list trace station** <extension number> - Traces calls to and from a specific station.
  - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
  - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
  - **status trunk** <trunk access code number> - Displays real-time trunk group information.
  - **status trunk** <trunk access code number/channel number> - Displays real-time signaling and media information for an active trunk channel.
2. Session Manager:
  - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session**

**Manager → System Tools → Call Routing Test.** Enter the requested data to run the test.

3. Avaya Session Border Controller for Enterprise:

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

- **Alarms:** This option provides information about active alarms.
- **Incidents:** This option provides detailed reports of anomalies, errors, policies violations, etc.
- **Status:** This option provides statistical and current status information.
- **Diagnostics:** This option provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Session Border Controller for Enterprise to the X5 Solutions SIP Trunking Service. The X5 Solutions SIP Trunking Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Please refer to **Section 2.2** for exceptions or workarounds.

## 11. References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 7.0, Document Number 03-300509, Issue 1, August 2015.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, Document Number 555-245-205, Issue 1, August 2015.
- [3] *Upgrading Avaya Aura® System Manager to Release 7.0*, Release 7.0, Issue 1, March 2016.
- [4] *Administering Avaya Aura® System Manager*, Release 7.0, Issue 1, January 2016.
- [5] *Upgrading Avaya Aura® Session Manager*, Release 7.0, Issue 1, August 2015.
- [6] *Administering Avaya Aura® Session Manager*, Release 7.0, Issue 1, August 2015.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 3, January 2016
- [9] *Avaya 1600 Series IP Deskphones Administrator Guide Release*, Document Number 16-601438, Issue 7, May 2015.
- [10] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones Edition H.323*, Issue 1, April 2015.
- [11] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones Edition SIP*, Issue 2, August 2015.
- [12] *Administering Avaya one-X® Communicator*, November 2015.
- [13] *Administering Avaya Communicator for Android, iPad, iPhone, and Windows*, Release 2.1, Issue 5, September 2015.
- [14] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [15] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

**©2016 Avaya Inc. All Rights Reserved.**

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

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