



Application Notes for Configuring Avaya Aura® Communication Manager Rel. 7.0, Avaya Aura® Session Manager Rel. 7.0 and Avaya Session Border Controller for Enterprise Rel. 7.0 to support Clearcom SIP Trunking Services using TLS – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking service for an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 7.0, Avaya Aura® Session Manager Rel. 7.0, and Avaya Session Border Controller for Enterprise Rel. 7.0 to support Clearcom SIP Trunking Services using TLS.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints. For privacy, TLS for Signaling, SRTP for media encryption was used inside of the enterprise (private network side) and TLS for Signaling, RTP for media was used outside of the enterprise (public network side).

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.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	6
2.3.	Support	7
3.	Reference Configuration	8
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager.....	11
5.1.	Licensing and Capacity	12
5.2.	System Features.....	16
5.3.	IP Node Names.....	17
5.4.	Codecs and Media Encryption	18
5.5.	IP Network Region.....	19
5.6.	Signaling Group	20
5.7.	Trunk Group.....	22
5.8.	Calling Party Information.....	26
5.9.	Inbound Routing.....	27
5.10.	Outbound Routing	28
6.	Configure Avaya Aura® Session Manager	31
6.1.	System Manager Login and Navigation.....	32
6.2.	Specify SIP Domain	33
6.3.	Add Location.....	34
6.4.	Adaptations.....	37
6.5.	SIP Entities	39
6.6.	Entity Links	43
6.7.	Routing Policies	46
6.8.	Dial Patterns	47
6.9.	Add/View Avaya Aura® Session Manager	50
7.	Configure Avaya Session Border Controller for Enterprise	52
7.1.	Log in Avaya SBCE.....	52
7.2.	TLS Management.....	56
7.2.1.	TLS Certificates	56
7.2.2.	TLS Client Profile – Avaya Session Manager	56
7.2.3.	TLS Client Profile – Service Provider	57
7.2.4.	TLS Server Profile – Avaya Session Manager	59
7.2.5.	TLS Server Profile – Service Provider	60
7.3.	Global Profiles.....	61
7.3.1.	Server Interworking Avaya-SM.....	61
7.3.2.	Server Interworking SP-General.....	63
7.3.3.	Signaling Manipulation.....	64
7.3.4.	Server Configuration.....	66

7.3.5.	Routing Profiles	74
7.3.6.	Topology Hiding	78
7.4.	Domain Policies	82
7.4.1.	Application Rules.....	82
7.4.2.	Media Rules	83
7.4.3.	Signaling Rules	88
7.4.4.	End Point Policy Groups.....	89
7.5.	Device Specific Settings.....	92
7.5.1.	Network Management.....	92
7.5.2.	Media Interface	94
7.5.3.	Signaling Interface	96
7.5.4.	End Point Flows.....	99
8.	Clearcom SIP Trunking Service Configuration	103
9.	Verification and Troubleshooting	104
9.1.	Troubleshooting	104
9.1.1.	Communication Manager.....	104
9.1.2.	Session Manager	104
9.1.3.	Avaya Session Border Controller for Enterprise (Avaya SBCE)	105
9.2.	TraceSBC Tool.....	109
10.	Conclusion	110
11.	References.....	111
12.	Appendix A: SigMa Script.....	112

1. Introduction

These Application Notes describe the steps required to configure Session Initiation Protocol (SIP) trunk service between the service provider Clearcom in Mexico and an Avaya SIP-enabled enterprise solution using Transport Layer Security (TLS).

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of an Avaya Aura® Communication Manager Rel. 7.0 (hereafter referred to as Communication Manager), Avaya Aura® Session Manager Rel. 7.0 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 7.0 (hereafter referred to as Avaya SBCE), and various Avaya endpoints. This solution does not extend to configurations without the Avaya Session Border Controller for Enterprise or Avaya Aura® Session Manager.

For privacy, TLS for Signaling, SRTP for media encryption was used inside of the enterprise (private network side) and TLS for Signaling, RTP for media was used outside of the enterprise (public network side) (refer to **Section 2.2**).

During interoperability testing, feature test cases were executed to ensure interoperability between Clearcom and Communication Manager.

Customers using an Avaya SIP-enabled enterprise solution with Clearcom SIP Trunking Service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional analog trunks and/or PSTN trunks such as ISDN-PRI. This approach generally results in lower cost for the enterprise.

The terms “Service Provider” and “Clearcom” will be used interchangeable throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Avaya Solution & Interoperability Test Lab by connecting Communication Manager, Session Manager and the Avaya SBCE to Clearcom SIP Trunking Service via the public internet, as depicted in **Figure 1**.

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 trunk interoperability, the following areas were tested for compliance:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.

- Incoming calls from the PSTN were routed to DID numbers assigned by Clearcom. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator soft phone (H.323 and SIP), Avaya Communicator for Windows (SIP) soft phone, analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 deskphones (SIP), Avaya one-X® Communicator (SIP) and Avaya Communicator for Windows (SIP).
- Outgoing calls to the PSTN were routed via Clearcom's network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Testing was performed with codecs: G.729A, G.711A and G.711MU (Clearcom's preferred codec order).
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

Items not supported or not tested included the following:

- Inbound toll-free calls, outbound Toll-Free calls, 911 calls (emergency), "0" calls (Operator) and 0+10 digits calls (Operator Assisted) were not tested.
- The SIP REFER method for call redirection was not tested for reasons noted in **Section 2.2**.
- T.38 fax was not tested for reasons noted in **Section 2.2**.

2.2. Test Results

Interoperability testing of Clearcom SIP Trunk service with an Avaya SIP-enabled enterprise solution was completed successfully with the following observations/limitations.

- **Secure Real-time Transport Protocol (SRTP):** SRTP supports RTP media protection on a point to point basis providing confidentiality, message authentication, and replay protection. As SRTP is point to point, all individual links involved in the VoIP call, including key exchange/signaling, must be secure for the call to be secure from end to end. During the compliance test, it was observed that RTP, instead of SRTP, was always used outside of the enterprise (public network side). Calls would fail if the use of SRTP was enforced on the public network side. This behavior may be caused by the far-end not supporting SRTP. Thus **Best Effort** was used during the compliance test, allowing Avaya SBCE to use SRTP on the public network side if supported by the far-end, otherwise it defaults to RTP. SRTP for media encryption was used inside of the enterprise (private network side).
- **SIP REFER method:** PSTN calls that were transferred back to the network using the SIP REFER method did not work properly. Attended call transfers dropped. On blind transfers, the REFER message was accepted by Clearcom with a 202 message, but the trunks were not released after the call transfer was completed. For these reasons testing was done with REFER disabled in Communication Manager (**Network Call Redirection** set to “n” under the **trunk-group**, refer to **Section 5.7**). With REFER disabled, blind and attended call transfers to the PSTN completed successfully, with the caveat that Communication Manager trunk channels were not released from the call path after the call was transferred, two trunks channels remained busy/connected for the entire duration of the call.
- **Outbound Calling Party Number (CPN) Blocking:** To support user privacy on outbound calls (calling party number blocking), when enabled by the user, Communication Manager sends “anonymous” as the calling number in the SIP “From” header and includes “Privacy: id” in the INVITE message, while the actual number of the caller is sent in the “P-Asserted-Identity” header. On the called PSTN phone, the calling party number was not blocked, the first DID number assigned to the SIP trunk (5528810001) was displayed, instead of “anonymous”.
- **Caller ID on incoming calls from U.S. based PSTN numbers:** Calls originating from PSTN telephones based in the U.S. to Communication Manager displayed “Unavailable”. During the compliance test, Clearcom provided a local PSTN test number in Mexico, a SIP softphone was registered to this local PSTN number and was used to originate and terminate local PSTN calls to and from Communication Manager. The correct Caller ID was displayed at the Communication Manager extensions when calling from this local PSTN number. This behavior is not necessarily indicative of a limitation of the combined Avaya/Clearcom solution, this seems to be the expected behavior for international calls from the U.S., which is ultimately controlled by the PSTN providers, it is listed here simply as an observation.
- **Caller ID display on Outbound Calls, Call Forwards and Call transfers to the local PSTN in Mexico:** For outbound calls, calls from the local PSTN in Mexico to Communication Manager that were Forwarded or Transferred back out to the local PSTN in Mexico, the caller ID number displayed at the SIP softphone (local PSTN in Mexico)

was always of the first DID number assigned to the SIP Trunk (5528810001), regardless of the PSTN number being used to originate the call.

- **Caller ID display on EC500 extension to cellular:** For EC500 extension to cellular calls the Caller ID display at the Mobile/cellular station was always of the first DID number assigned to the SIP Trunk (5528810001), regardless of the PSTN number being used to originate the call.
- **Fax Support:** T.38 fax is the fax protocol officially supported by Communication Manager on SIP trunks. During the tests, Clearcom responded with “488 Not Acceptable Here” to the re-INVITE messages sent by Communication Manager to make the change from voice to T.38, causing the call to drop. Even though it was possible during the tests to complete G.711 fax pass-through calls using a local test number in Mexico, G.711 fax pass-through is available in Communication Manager on a “best effort” basis, and it’s not guaranteed that it will work in every instance, thus G.711 fax pass-through is not recommended in Communication Manager.
- **From Header Manipulation:** Clearcom uses SIP trunk registration and digest authentication in order to accept calls from the enterprise into their network. Additionally, Clearcom requires the username associated with the SIP trunk credentials to be present in the “From” header of all outbound calls from the enterprise. Otherwise, the call is rejected with a “403 Username=From not allowed” message. A Signaling Script was created in the Avaya SBCE to include the SIP trunk credential’s username in the “From” header of all outbound calls. (**Section 7.3.3**).
- **Request-URI Header Manipulation:** Clearcom sends the username associated with the SIP trunk credentials in the “Request-URI” header of all inbound calls, while the actual DID number of the party dialed is sent in the “To” header. Since the routing decision in Session Manager is based on Dial Patterns, by inspecting the number present in the “Request-URI” header of the incoming call, a Signaling Script was created in the Avaya SBCE to populate the “Request URI” header with the number present in the “To” header of inbound calls. (**Section 7.3.3**).
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider’s network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider’s network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location (**Section 6.4**). Additionally, the parameters “gsid” and “epv” were removed from outbound Contact headers using a Signaling Script in the Avaya SBCE (**Section 7.3.3**).

2.3. Support

For support on Clearcom systems visit the corporate Web page at: <http://www.clearcom.mx/>

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 below illustrates the test configuration used. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Clearcom SIP Trunk service through the public Internet.

The Avaya components used to create the simulated customer site included:

- Avaya Aura® Communication Manager running on VMware (ESXi 5.5) platform.
- Avaya Aura® Session Manager running on VMware (ESXi 5.5) platform.
- Avaya Aura® System Manager running on VMware (ESXi 5.5) platform.
- Avaya Session Border Controller for Enterprise running on a Dell R210 V2 Server.
- Avaya Aura® Messaging running on VMware (ESXi 5.5) platform.
- Avaya Aura® Media Server running on VMware (ESXi 5.5) platform.
- Avaya G450 Media Gateway.
- Avaya 96x1-Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya Communicator for Windows soft phone (SIP)
- Avaya 2420 Digital Deskphones.
- Analog Deskphones.
- Desktop PC running administration interfaces.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flow through the Avaya SBCE. 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. The transport protocol between the Avaya SBCE and Clearcom, across the public Internet, was SIP over TLS. The transport protocol between the Avaya SBCE and Session Manager, across the enterprise network, was SIP over TLS. The transport protocol between Session Manager and Communication Manager, across the enterprise network, was SIP over TLS.

A separate SIP trunk group was created between Communication Manager and Session Manager to carry the traffic to and from the service provider (two-way trunk group). To separate the codec settings required by the service provider from the codec used by the telephones, two IP network regions were used, each with dedicated signaling groups.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE, then to Session Manager. Session Manager used the configured dial patterns and routing policies to determine the recipient (in this case Communication Manager), and on which link to send the call. Once the

call arrived at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions are performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment, such as Automatic Route Selection (ARS) and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns and routing policies to determine the route to the Avaya SBCE for egress to Clearcom's network.

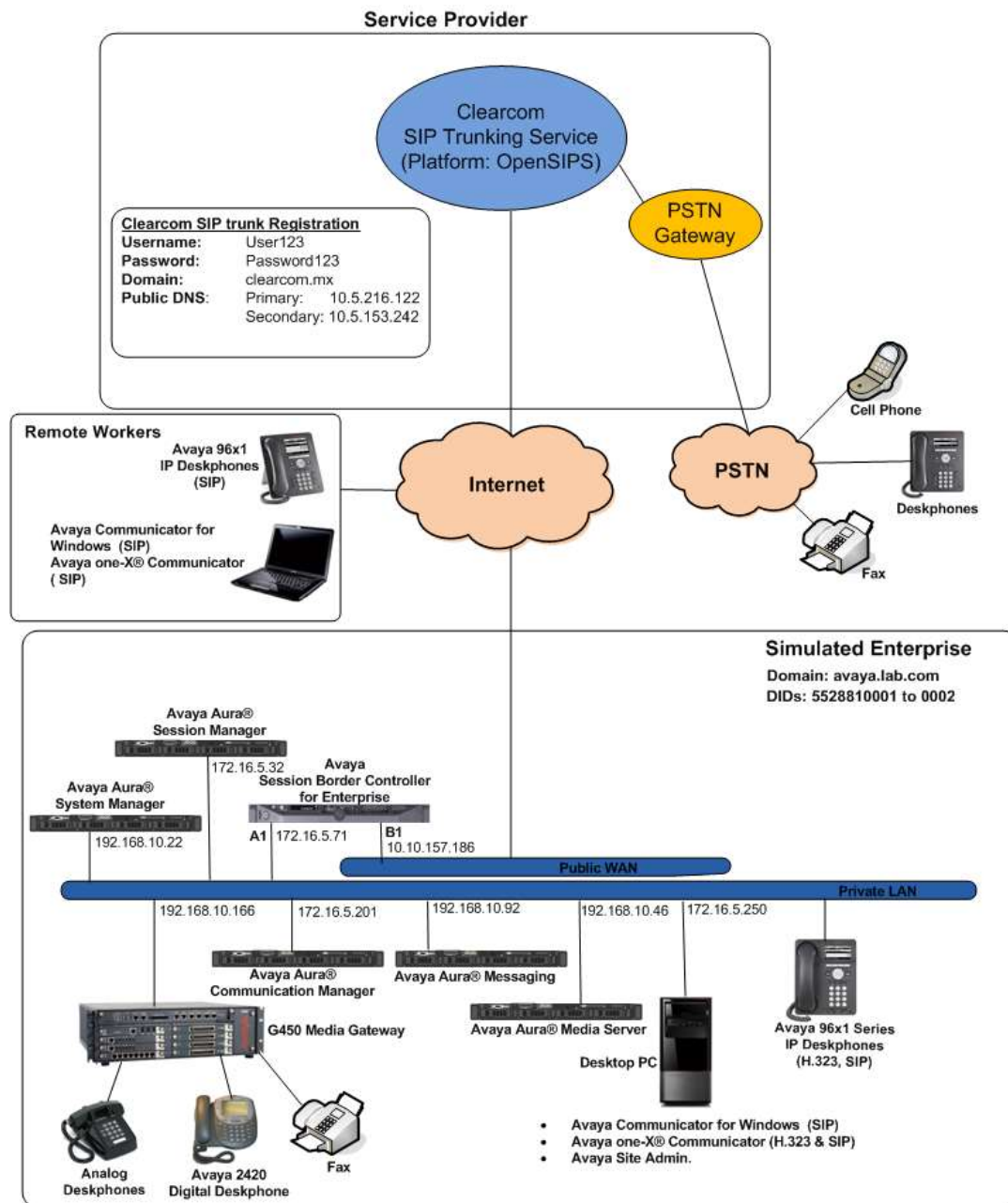


Figure 1: Avaya SIP-enabled Enterprise Solution and Clearcom SIP Trunking Service

4. Equipment and Software Validated

The following equipment and software were used for the compliance testing in the simulated enterprise:

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on VMware ESXi 5.5 platform	7.0.0.3.1 SP 3.1 (00.0.441.0-22903)
Avaya Aura® Session Manager running on VMware ESXi 5.5 platform	7.0 SP2 (7.0.0.2.700201)
Avaya Aura® System Manager running on VMware ESXi 5.5 platform	7.0.0.2 Build No. 7.0.0.0.16266-7.0.9.7002010 Software Update Rev. No. 7.0.0.2.4416
G450 Gateway	37.21.0
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	7.0.1-03-8739
Avaya Aura® Media Server running on VMware ESXi 5.5 platform	7.7.0.236
Avaya Aura® Messaging running on VMware ESXi 5.5 platform	6.3.3 Service Pack 3 (MSG-03.0.141.0-348_0304)
Avaya Aura® Integrated Management Site Administrator	6.0.07
Avaya one-X® Communicator (SIP & H.323)	6.2.11.03-SP11
Avaya Communicator for Windows (SIP)	2.1.3.80
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6029
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.0.0.39
Avaya 2420 Series Digital Deskphone	--
Lucent Analog Deskphone	--
Clearcom	
OpenSIPS Softswitch	1.9
OpenSIPS Session Border Controller	1.9

Table 2 – Hardware and Software Components Tested

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Clearcom. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and the Avaya Aura® Media Server has been previously completed.

In configuring Communication Manager, various components such as ip-network-regions, signaling groups, trunk groups, etc. need to be selected or created for use with the SIP connection to the Service Provider. Unless specifically stated otherwise, any unused ip-network-region, signaling group, trunk group, etc. can be used for this purpose.

The Communication Manager configuration was performed using the Avaya Integrated Management Site Administrator. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the public IP addresses shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements are not revealed. Some screens captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

5.1. Licensing and Capacity

Use the **display system-parameter customer-options** to verify that **Media Encryption over IP** is set to **y**.

```
display system-parameters customer-options                               Page 5 of 12
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                           ISDN Feature Plus? n
  Enhanced EC500? y                                                  ISDN/SIP Network Call Redirection? y
  Enterprise Survivable Server? n                                     ISDN-BRI Trunks? y
  Enterprise Wide Licensing? n                                       ISDN-PRI? y
  ESS Administration? y                                              Local Survivable Processor? n
  Extended Cug/Fwd Admin? y                                          Malicious Call Trace? y
  External Device Alarm Admin? y                                     Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n                                  Mode Code for Centralized Voice Mail? n
  Flexible Billing? n
  Forced Entry of Account Codes? y                                    Multifrequency Signaling? y
  Global Call Classification? y                                       Multimedia Call Handling (Basic)? y
  Hospitality (Basic)? y                                              Multimedia Call Handling (Enhanced)? y
  Hospitality (G3U3 Enhancements)? y                                Multimedia IP SIP Trunking? y
  IP Trunks? y

IP Attendant Consoles? y
(NOTE: You must logoff & login to effect the permission changes.)
```

If it's set to **n**, obtain a license file for Communication Manager with the Media Encryption feature enabled.

After installing the license, in the SMI interface of Communication Manager (web interface), go to **Administration/Licensing → Feature Administration**. Go to Current Settings (not shown); look for **Media Encryption over IP?** and enable it (select **ON**). Go to the bottom of the page and click on **Submit** (not shown).

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for Administration / Licensing. The left sidebar contains links for 'Overview Status', 'Work/M. Configuration', and 'Feature Administration' (which is highlighted). The main content area displays a table of features with their current settings and a 'Notes' column. The feature 'Media Encryption Over IP?' is highlighted with a red border and has the 'ON' radio button selected.

Feature ID	Feature Name	Current Setting	Feature Code	Notes
33	Hospitality (Basic)?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_HM	Notes
34	Hospitality (G3v3 Enhancements)?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_V3H_ENH	Notes
35	ISDN Feature Plus?	<input type="radio"/> ON <input checked="" type="radio"/> OFF	FEAT_PP_ISDN	Notes
36	ISDN/SIP Network Call Redirection?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_NCR_ISDN	Notes
37	Malicious Call Trace?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_MCT	Notes
38	Media Encryption Over IP?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_ME	Notes
39	Mode Code for Centralized Voice Mail?	<input type="radio"/> ON <input checked="" type="radio"/> OFF	FEAT_CVM_MC	Notes
40	Multifrequency Signaling?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_MFS	Notes
41	Multimedia Call Handling (Basic)?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_MMCH	Notes
42	Multimedia Call Handling (Enhanced)?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_EMMCH	Notes
43	Multimedia IP SIP Trunking?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_MMIP_SIP	Notes
44	Multinational Locations?	<input type="radio"/> ON <input checked="" type="radio"/> OFF	FEAT_MMNL_LDC	Notes
45	Multiple Locations?	<input type="radio"/> ON <input checked="" type="radio"/> OFF	FEAT_MULTLOC	Notes
46	Personal Station Access (PSA)?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_PSA	Notes
47	Posted Messages?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_POMSG	Notes
48	PNC Duplication?	<input type="radio"/> ON <input checked="" type="radio"/> OFF	FEAT_PNC_DUPE	Notes
49	Port Network Support?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_PNS	Notes
50	Private Networking?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_ETN	Notes
51	Secondary Data Module?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_12C	Notes
52	Station as Virtual Extension?	<input checked="" type="radio"/> ON <input type="radio"/> OFF	FEAT_VDRT_EXT	Notes

© 2011-2015 Avaya Inc. All Rights Reserved.

In the Communication Manager SAT terminal, go back to display system customer options and that **Media Encryption over IP?** is set to y on page 5.

```

display system-parameters customer-options                               Page 5 of 12
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y
  Enhanced EC500? y
Enterprise Survivable Server? n
Enterprise Wide Licensing? n
  ESS Administration? y
  Extended Cug/Fwd Admin? y
  External Device Alarm Admin? y
Five Port Networks Max Per MGC? n
  Flexible Billing? n
  Forced Entry of Account Codes? y
  Global Call Classification? y
  Hospitality (Basic)? y
Hospitality (G303 Enhancements)? y
  IP Trunks? y

ISDN Feature Plus? n
ISDN/SIP Network Call Redirection? y
  ISDN-BRI Trunks? y
  ISDN-PRI? y
  Local Survivable Processor? n
  Malicious Call Trace? y
  Media Encryption Over IP? y
Mode Code for Centralized Voice Mail? n

Multifrequency Signaling? y
Multimedia Call Handling (Basic)? y
Multimedia Call Handling (Enhanced)? y
Multimedia IP SIP Trunking? y

IP Attendant Consoles? y
(NOTE: You must logoff & login to effect the permission changes.)

```

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 SIP trunks to the Service Provider. The example below shows one license with a capacity of **24000** trunks available and **122** 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.

```

display system-parameters customer-options                               Page 2 of 12
                                OPTIONAL FEATURES

IP PORT CAPACITIES
Maximum Administered H.323 Trunks: 12000 10
Maximum Concurrently Registered IP Stations: 18000 1
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 1
Maximum Video Capable IP Softphones: 18000 7
Maximum Administered SIP Trunks: 24000 122
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
Maximum Number of DS1 Boards with Echo Cancellation: 522 0

(NOTE: You must logoff & login to effect the permission changes.)

```

On Page 4, verify that ARS is set to y.

```
display system-parameters customer-options                               Page 4 of 12
                                OPTIONAL FEATURES
Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? n          Authorization Codes? y
Analog Trunk Incoming Call ID? y          CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y   CAS Main? n
Answer Supervision by Call Classifier? y   Change COR by FAC? n
ARS? y Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y                  Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? n           DCS (Basic)? y
ASAI Link Core Capabilities? n           DCS Call Coverage? y
ASAI Link Plus Capabilities? n           DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
ATM WAN Spare Processor? n               DS1 MSP? y
ATMS? y                                  DS1 Echo Cancellation? y
Attendant Vectoring? y

(NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System Features

Use the **change system-parameters feature** 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 this field set to **none**.

```
display system-parameters features                                     Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS
  Self Station Display Enabled? n
  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

  Music (or Silence) on Transferred Trunk Calls? all
  DID/Tie/ISDN/SIP Intercept Treatment: attendant
  Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
  Automatic Circuit Assurance (ACA) Enabled? n

  Abbreviated Dial Programming by Assigned Lists? n
  Auto Abbreviated/Delayed Transition Interval (rings): 2
  Protocol for Caller ID Analog Terminals: Bellcore
  Display Calling Number for Room to Room Caller ID Calls? n
```

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** for restricted calls and **unavailable** for unavailable calls.

```
display 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:
  International Access Code:
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 Avaya server running Communication Manager (**procr**), and for Session Manager (**Lab-HG-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	
ASBCE A1	172.16.5.71	
Lab-HG-SM	172.16.5.32	
MA-CM	192.168.10.12	
default	0.0.0.0	
media_server	192.168.10.46	
msgserver	172.16.5.12	
procr	172.16.5.201	
procr6	::	
(8 of 8 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

5.4. Codecs and Media Encryption

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the Service Provider. For the compliance test, **ip-codec-set 2** was used for this purpose. Clearcom supports G.729A, G.711MU and G.711A. Thus, these codecs were included in this set. Enter **G.729A**, **G.711A** and **G.711MU** in the **Audio Codec** column of the table; this is Clearcom's preferred codec order. Set **Media Encryption** to **1-srtp-aescm128-hmac80** and **2-srtp-aescm128-hmac32**, this value must match the Media Encryption value set under the Avaya SBCE Media Rules, Section 7.4.2. Set **Encrypted SRTCP** to **enforce-unenc-srtcp**.

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.711A	n	2	20
3:	G.711MU	n	2	20
4:		-	-	
5:		-	-	
6:		-	-	
7:		-	-	

	Media Encryption	Encrypted SRTCP:
1:	1-srtp-aescm128-hmac80	enforce-unenc-srtcp
2:	2-srtp-aescm128-hmac32	
3:		
4:		
5:		

On **Page 2**, set the **Fax Mode** to **off** (T.38 fax is currently not supported by Clearcom, refer Section 2.2).

change ip-codec-set 2 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	Packet Size(ms)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

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 *avaya.lab.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. 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: avaya.lab.com
Name: SP Region Stub Network Region: n
MEDIA PARAMETERS
Codec Set: 2 Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? n
UDP Port Max: 3349
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 RSUP 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. It 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).

change ip-network-region 2										Page 4 of 20		
Source Region: 2 Inter Network Region Connection Management										I	M	
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G		A	G	
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	e
1	2	y	NoLimit						n			t
2	2										all	
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												

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 SIP 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 **IMS Enabled** field to *n*. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager. The transport method used between Session Manager and the Avaya SBCE is specified as TLS in **Sections 6.6** and **7.3.4**. Lastly, the transport method between the Avaya SBCE and Clearcom is also TLS. This is defined in **Section 7.3.4**.
- 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). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5071**.
- 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 Session Manager.

- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Avaya Server running Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **Lab-HG-SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- 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 **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the inside IP of the Avaya SBCE and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```
change 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 Uiden? 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: Lab-HG-SM
Near-end Listen Port: 5071      Far-end Listen Port: 5071
Far-end Network Region: 2
Far-end Domain: avaya.lab.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? n      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 the **Signaling Group** to the signaling group shown in **Section 5.6**.
- 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.

```
change 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**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the Service Provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. Note that the value assigned to the **Preferred Minimum Session Refresh Interval (sec)** field is doubled and assigned to the “Min-SE” Header Field in SIP INVITE messages for calls originating from Communication Manager. Using the default setting of **600** seconds as in the example, the “Min-SE” Header Field would be populated for 1200 seconds in SIP INVITE messages originating from Communication Manager.

```
change 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

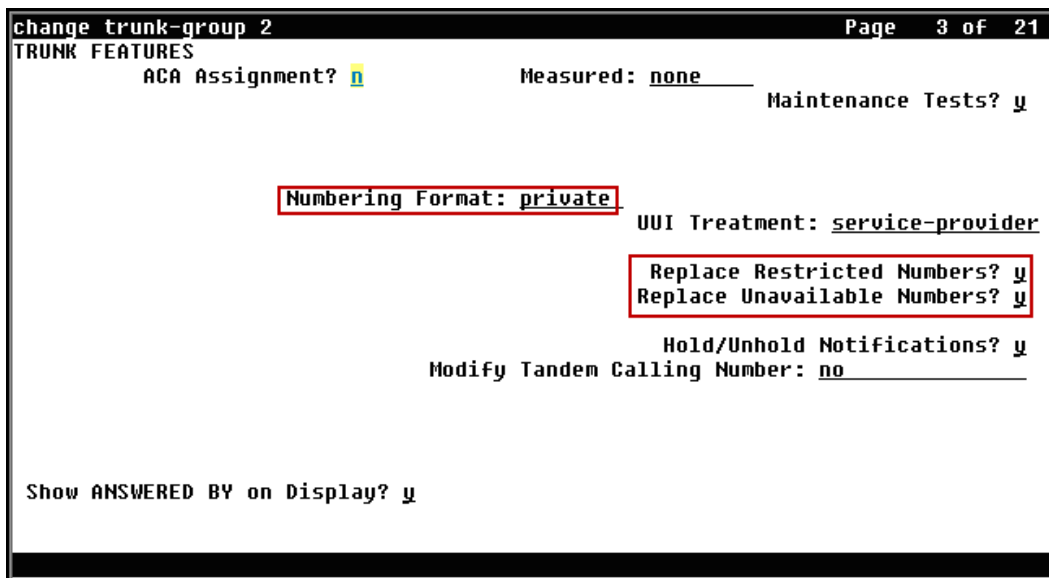
  XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n

  Caller ID for Service Link Call to H.323 1xC: station-extension
```

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 when passed in the SIP “From”, “Contact”, “P-Asserted Identity” and “Diversion” headers. The addition of the “+” sign impacted caller ID presentation on outbound calls sent to Clearcom. Thus, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-unk* (Section 5.10).

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 enabled CPN block.

Default values were used for all other fields.



```
change trunk-group 2                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none
                                                    Maintenance Tests? y

  Numbering Format: private
                                                    UUU Treatment: service-provider
  Replace Restricted Numbers? y
  Replace Unavailable Numbers? y

  Hold/Unhold Notifications? y
  Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y
```


Page 4 was configured using the parameters highlighted below.

- Set the **Network Call Redirection** field to *n*. This setting directs Communication Manager **not** to use the SIP REFER method for transferring calls off-net to the PSTN, refer to **Section 2.2**.
- Set the **Send Diversion Header** field to *n*.
- Set the **Support Request History** field to *n*.
- Set the **Telephone Event Payload Type** to *101*. The value preferred by Clearcom.
- Set the **Convert 180 to 183 for Early Media** to *y*.
- Set the **Always Use re-INVITE for Display Updates** field to *y*.
- Set the **Identity for Calling Party Display** to *P-Asserted-Identity*.

change trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? <u>n</u>	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? <u>n</u>	
Send Transferring Party Information? <u>n</u>	
Network Call Redirection? <u>n</u>	
Send Diversion Header? <u>n</u>	
Support Request History? <u>n</u>	
Telephone Event Payload Type: <u>101</u>	
Convert 180 to 183 for Early Media? <u>y</u>	
Always Use re-INVITE for Display Updates? <u>y</u>	
Identity for Calling Party Display: <u>P-Asserted-Identity</u>	
Block Sending Calling Party Location in INVITE? <u>n</u>	
Accept Redirect to Blank User Destination? <u>n</u>	
Enable Q-SIP? <u>n</u>	
Interworking of ISDN Clearing with In-Band Tones: <u>keep-channel-active</u>	
Request URI Contents: <u>may-have-extra-digits</u>	

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are assigned by the Service Provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs).

The screen below shows DID numbers assigned for testing. The DID numbers were mapped to enterprise extensions 3041, 3042, 3044 and 3045.

change private-numbering 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3			4	Total Administered: 6 Maximum Entries: 540
4	5			4	
4	3041	2	5528810001	10	
4	3042	2	5528810002	10	
4	3044	2	5528810003	10	
4	3045	2	5528810004	10	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	

Note: During the compliance test, Clearcom did not inspect the calling party number sent in the origination headers from the enterprise to authenticate outbound calls; it used SIP trunk registration and Digest Authentication instead. This is shown in **Section 7.3.4** of the Avaya SBCE configuration, later in this document. Clearcom also inserted the main DID number assigned to the SIP trunk on all outbound calls sent to the PSTN, for caller ID purposes. Since the calling party information sent from the enterprise was for all practical purposes not used by Clearcom, the configuration shown on the screen above was not strictly required, and it is shown here simply for completeness.

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Clearcom is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group, as shown below. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 2					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	5528810001	10	3041	
public-ntwrk	10	5528810002	10	3042	
public-ntwrk	10	5528810003	10	3044	
public-ntwrk	10	5528810004	10	3045	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	

5.10. 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 feature access code (**fac**).

change dialplan analysis			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	13	udp						
1	4	dac						
2	4	ext						
3	4	ext						
4	4	udp						
5	4	ext						
6	3	dac						
7	4	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	2	dac						

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

```

change feature-access-codes                                     Page 1 of 10
FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code: _____
Abbreviated Dialing List2 Access Code: _____
Abbreviated Dialing List3 Access Code: _____
Abbreviated Dial - Prgm Group List Access Code: _____
Announcement Access Code: #7
Answer Back Access Code: _____
Attendant Access Code: _____
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2: _____
Automatic Callback Activation: _____      Deactivation: _____
Call Forwarding Activation Busy/DA: _____ All: _____      Deactivation: _____
Call Forwarding Enhanced Status: _____ Act: _____      Deactivation: _____
Call Park Access Code: _____
Call Pickup Access Code: *44
CAS Remote Hold/Answer Hold-Unhold Access Code: _____
CDR Account Code Access Code: _____
Change COR Access Code: _____
Change Coverage Access Code: _____
Conditional Call Extend Activation: _____      Deactivation: _____
Contact Closure Open Code: _____      Close Code: _____

```

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. Refer to **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: 0

```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
0	1	11	2	op		n
0	13	13	1	hnpa		n
00	2	2	deny	op		n
001	13	13	2	intl		n
01	12	12	2	natl		n
011	10	18	2	intl		n
040	3	3	2	svcl		n
045	13	13	2	natl		n
101xxx0	8	8	deny	op		n
101xxx0	18	18	deny	op		n
101xxx01	16	24	deny	iop		n
101xxx011	17	25	deny	intl		n
101xxx1	18	18	deny	fnpa		n
10xxx0	6	6	deny	op		n
10xxx0	16	16	deny	op		n

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the Service Provider trunk 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 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.
- **Numbering Format:** Set to **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: Serv. Provider	
SCCAN? n															Secure SIP? n	
Used for SIP stations? n																
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts					DCS/ QSIG	IXC Intw			
1:	2											n	user			
2:												n	user			
3:												n	user			
4:												n	user			
5:												n	user			
6:												n	user			

	BCC VALUE							TSC	CA-TSC Request	ITC	BCIE	Service/Feature	PARM	Sub Dgts	Numbering Format	LAR
	0	1	2	M	4	W										
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

Note: To save all Communication Manager provisioning changes, enter the command **save translations**.

6. Configure Avaya Aura® Session Manager

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

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

It may not be necessary to create all the items above when configuring 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, Adaptations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

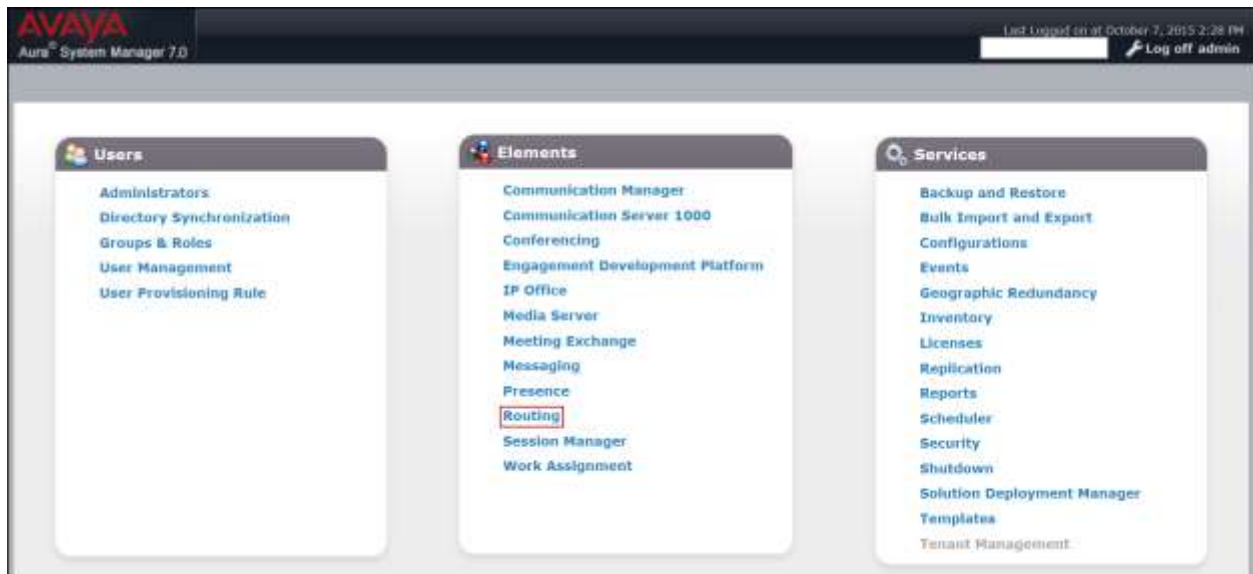
Note: Some Avaya products are shipped with a default identity TLS certificate signed by Avaya, to enable out-of-box support for TLS sessions. These are considered “demo” certificates which do not meet the current National Institute of Standards and Technology (NIST) security standards. For security reasons these default “demo” certificates should not be used in Production.

Avaya recommends using 3rd Party Certificate Authority (CA) signed identity certificates for enhanced security.

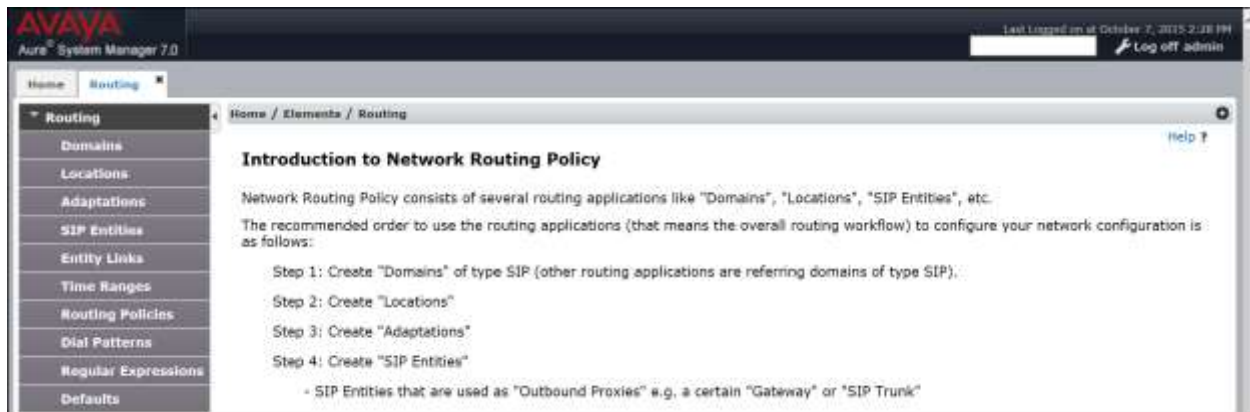
On the enterprise side (or private side), testing was done with the default “demo” TLS identity certificates. The procedure to obtain and install 3rd Party CA TLS certificates is outside the scope of these Application Notes. Refer to items [3], [5] and [8] in **Section 11**.

6.1. 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 (not shown). The screen shown below is then displayed. Click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Routing** link shown below.



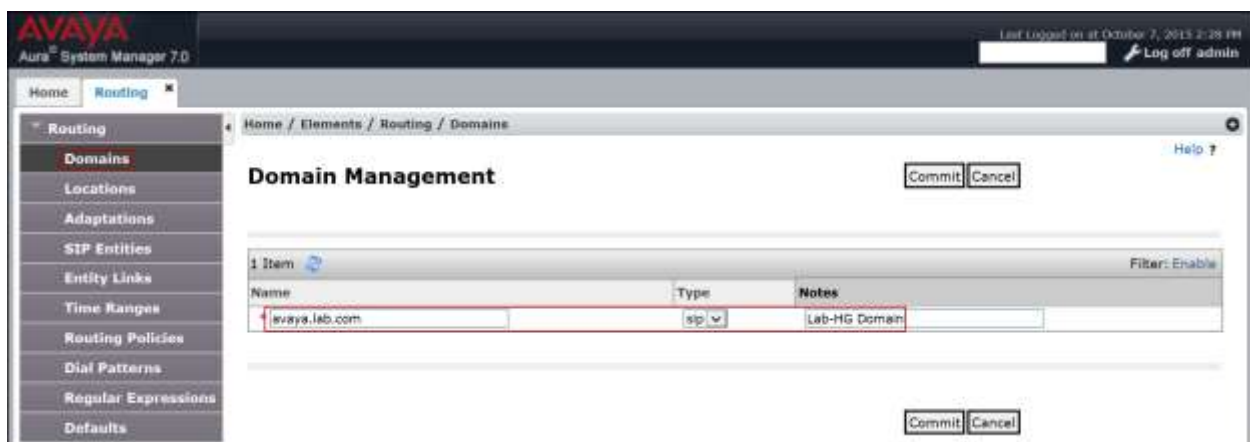
6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test the enterprise domain **avaya.lab.com** was used.

To add a domain, navigate to **Routing → Domains** in the left-hand navigation pane 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** to save (not show).

The screen below shows the entry for the enterprise domain **avaya.lab.com**.



6.3. Add Location

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

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

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

The screen below shows the **HG Session Manager** location. This location will be assigned later to the SIP Entity corresponding to Session Manager.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Location Details' and contains the following sections:

- General:** The 'Name' field is populated with 'HG Session Manager'. The 'Notes' field is empty.
- Dial Plan Transparency in Survivable Mode:** The 'Enabled' checkbox is unchecked. The 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty.
- Overall Managed Bandwidth:** The 'Managed Bandwidth Units' dropdown is set to 'Kbit/sec'. The 'Total Bandwidth' and 'Multimedia Bandwidth' fields are empty. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked.
- Per-Call Bandwidth Parameters:** The 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)' fields are both set to '1000 Kbit/Sec'. The 'Minimum Multimedia Bandwidth' field is set to '64 Kbit/Sec'. The 'Default Audio Bandwidth' dropdown is set to '80 Kbit/sec'.
- Alarm Threshold:** The 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' dropdowns are both set to '80 %'. The 'Latency before Overall Alarm Trigger' and 'Latency before Multimedia Alarm Trigger' fields are both set to '5 Minutes'.
- Location Pattern:** The 'Add' and 'Remove' buttons are visible. Below them, there is a table with 0 items. The 'Filter' is set to 'Enable'.

At the bottom right of the form, there are 'Commit' and 'Cancel' buttons.

The following screen shows the **HG Communication Manager** location. This location will be assigned later to the SIP Entity corresponding to Communication Manager.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', and a user session summary: 'Last Logged on at October 7, 2015 2:38 PM' and a 'Log off admin' link. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Locations' and 'Location Details'. It features a 'Commit' button and a 'Cancel' button in the top right. The 'General' section includes a 'Name' field with the value 'HG Communication Manager' and a 'Notes' field. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox. The 'Overall Managed Bandwidth' section includes fields for 'Managed Bandwidth Units' (set to Kbit/sec), 'Total Bandwidth', and 'Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'. The 'Alarm Threshold' section includes fields for 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', 'Latency before Overall Alarm Trigger', and 'Latency before Multimedia Alarm Trigger'. The 'Location Pattern' section includes an 'Add' button, a 'Remove' button, a table with one row 'IP Address Pattern', and a 'Notes' column. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Avaya
Aura System Manager 7.0

Last Logged on at October 7, 2015 2:38 PM
Log off admin

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

Name: HG Communication Manager

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

Latency before Overall Alarm Trigger: 5 Minutes

Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items

Filter: Enable

IP Address Pattern

Notes

Commit Cancel

The following screen shows the **HG ASBCE** location. This location will be assigned later to the SIP Entity corresponding to the Avaya SBCE.

The screenshot displays the 'Location Details' configuration page in the Avaya Aura System Manager 7.0 interface. The left sidebar shows a navigation menu with 'Locations' selected. The main content area is titled 'Location Details' and includes a 'Commit' button. The configuration is organized into several sections:

- General:** Contains a 'Name' field with the value 'HG ASBCE' and an empty 'Notes' field.
- Dial Plan Transparency in Survivable Mode:** Includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth:** Features a 'Managed Bandwidth Units' dropdown set to 'Kbit/sec', and input fields for 'Total Bandwidth' and 'Multimedia Bandwidth'.
- Audio Calls Can Take Multimedia Bandwidth:** A checkbox that is checked.
- Per-Call Bandwidth Parameters:** Includes input fields for 'Maximum Multimedia Bandwidth (Intra-Location):' (1000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location):' (1000 Kbit/Sec), '* Minimum Multimedia Bandwidth:' (64 Kbit/Sec), and '* Default Audio Bandwidth:' (80 Kbit/sec).
- Alarm Threshold:** Includes dropdowns for 'Overall Alarm Threshold:' (80 %) and 'Multimedia Alarm Threshold:' (80 %), and input fields for '* Latency before Overall Alarm Trigger:' (5 Minutes) and '* Latency before Multimedia Alarm Trigger:' (5 Minutes).
- Location Pattern:** A section at the bottom with 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' link. The table has columns for 'IP Address Pattern' and 'Notes'.

At the bottom right of the configuration area, there are 'Commit' and 'Cancel' buttons.

6.4. Adaptations

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

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

Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name:** Enter an appropriate name.
- **Module Name:** Select the *DigitConversionAdapter* option.
- **Module Parameter Type:** Select *Name-Value Parameter*.

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

- **Name:** Enter *eRHdrs*. This parameter will remove the specified headers from messages in the egress direction.
- **Value:** Enter “*Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P-Location, Endpoint-View*”

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left with their default values.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left sidebar shows a navigation menu with 'Adaptations' highlighted. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The 'Adaptation Name' is 'CM_Outbound_Header_Removal', the 'Module Name' is 'DigitConversionAdapter', and the 'Module Parameter Type' is 'Name-Value Parameter'. Below this, there is a table for 'Add' and 'Remove' parameters. The table has columns for 'Name' and 'Value'. One entry is visible: 'allhdrs' with a value that includes 'Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P-'. Below the table, there are fields for 'Egress URI Parameters' and 'Notes'. At the bottom, there are two sections for 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM', each with a table for 'Add' and 'Remove' items. The tables have columns for 'Matching Pattern', 'Min', 'Max', 'Phone Context', 'Delete Digits', 'Insert Digits', 'Address to modify', 'Adaptation Data', and 'Notes'. The 'Commit' and 'Cancel' buttons are at the bottom right.

6.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity interface that is used for SIP signaling.
- **Type:** Enter ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** (or ***Other***) for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

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:

- **Port:** Port number on which the Session Manager will listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.
- Click **Commit** to save.

The following screen shows the addition of the Session Manager SIP entity. The name ***HG Session Manager***, the IP address of the Session Manager signaling interface, the Location ***HG Session Manager*** created in **Section 6.3** and the **Time Zone** were used.

For the compliance test, only two Ports were used:

- **5061** with **TLS** for connecting to the Avaya SBCE.
- **5071** with **TLS** for connecting to Communication Manager.

AVAYA
Aura System Manager 7.0

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: HG Session Manager

* FQDN or IP Address: 172.16.5.32

Type: Session Manager

Notes: Security Module

Location: HG Session Manager

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

11 Items

Listen Ports	Protocol	Default Domain	Notes
5060	TCP	avaya.lab.com	
5060	UDP	avaya.lab.com	
5061	TLS	avaya.lab.com	
5062	TCP	avaya.lab.com	
5065	TLS	avaya.lab.com	
5070	TCP	avaya.lab.com	
5071	TLS	avaya.lab.com	
5080	TCP	avaya.lab.com	
5081	TCP	avaya.lab.com	
5085	UDP	avaya.lab.com	
5086	TCP	avaya.lab.com	

Select: All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items

Response Code & Reason Phrase	Mark Entity Up/Down	Notes
-------------------------------	---------------------	-------

Commit Cancel

The following screen shows the addition of the Communication Manager SIP Entity.

A separate SIP entity for Communication Manager is required in order to route traffic from Communication Manager to the Service Provider.

The name ***HG CM Trunk 2***, the IP of the Avaya Server running Communication Manager, the **Type** of ***CM*** for Communication Manager, the Location ***HG Communication Manager*** created in **Section 6.3** and the **Time Zone** were used.

AVAYA
Aura System Manager 7.0

Home / Routing / SIP Entities

SIP Entity Details

General

* Name: HG CM Trunk 2

* FQDN or IP Address: 172.16.5.201

Type: CM

Notes: For Service Provider Calls

Adaptation: (empty)

Location: HG Communication Manager

Time Zone: America/New_York

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

Credential name: (empty)

Securable: ☐

Call Detail Recording: none

Loop Detection Mode: Off

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association: (empty)

Backup Session Manager Bandwidth Association: (empty)

SIP Responses to an OPTIONS Request

Add Remove

0 Items

Response Code & Reason Phrase	Mark Entity Up/Down	Notes
-------------------------------	---------------------	-------

Commit Cancel

The following screen shows the addition of the SIP entity for the Avaya SBCE.

The name **HG ASBCE**, the inside IP address of the Avaya SBCE, the **Type** of **Other**, the adaptation **CM_Outbound_Header_Removal** created in **Section 6.4**, the location **HG ASBCE** created in **Section 6.3** and the **Time Zone** were used.

Note: **Type: Other** was used during the testing; **SIP Trunk** could have been used instead.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a breadcrumb trail: Home / Elements / Routing / SIP Entities. The 'General' tab is active, showing the following fields: Name (HG ASBCE), FQDN or IP Address (172.16.5.71), Type (Other), and Notes (HG ASBCE). Below these are Adaptation (CM_Outbound_Header_Removal), Location (HG ASBCE), and Time Zone (America/New_York). Further down are fields for SIP Timer B/F (4), Credential name, Securable (unchecked), Call Detail Recording (none), and CommProfile Type Preference. The 'Loop Detection' section shows Loop Detection Mode set to Off. The 'SIP Link Monitoring' section shows SIP Link Monitoring set to Use Session Manager Configuration. Below this are checkboxes for Supports Call Admission Control and Shared Bandwidth Manager, and dropdowns for Primary and Backup Session Manager Bandwidth Association. The 'SIP Responses to an OPTIONS Request' section includes an 'Add' button, a 'Remove' button, and a table with columns: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. The table currently shows 0 items. At the bottom right are 'Commit' and 'Cancel' buttons.

6.6. 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 and one to the Avaya SBCE, to be used only for Service Provider traffic. To add an entity link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link. For Communication Manager this was matched to the **Transport Method** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **Transport** defined on the **Server Configuration** for Session Manager (Call Server) in **Section 7.3.4**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this was matched to the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **Port** defined on the **Server Configuration** for Session Manager (Call Server) in **Section 7.3.4**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager or the Avaya SBCE select the respective SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system will receive SIP requests from Session Manager. For Communication Manager, this was matched to the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **TLS Port** defined for the private **Signaling Interface** on the Avaya SBCE in **Section 7.5.3**.
- **Connection Policy:** Select *Trusted*.
- Click **Commit** to save.

The following screens illustrate the entity links to Communication Manager and to the Avaya SBCE.

The following screen shows the entity link to Communication Manager:

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, and DNS Override. The row shows: *HG Session Manager, *HG Session Manager, TLS, 5071, *HG CM Trunk 2, and a checkbox for DNS Override. The table is filtered by 'Enable'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the main content area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override
*HG Session Manager	*HG Session Manager	TLS	5071	*HG CM Trunk 2	<input type="checkbox"/>

The following screen shows the entity link to the Avaya SBCE:

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, and DNS Override. The row shows: *HG Session Manager, *HG Session Manager, TLS, 5061, *HG ASBCE, and a checkbox for DNS Override. The table is filtered by 'Enable'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the main content area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override
*HG Session Manager	*HG Session Manager	TLS	5061	*HG ASBCE	<input type="checkbox"/>

The following screen shows the list of the newly added entity links. Note that only the highlighted entity links were created for the compliance test, and are the ones relevant to these Application Notes.

Entity Links

24 Items

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
HG Session Manager AAC 5060 TCP	HG Session Manager	TCP	5060	AAC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	AAC Entity Link
HG Session Manager Acme Packet sip1 5060 TCP	HG Session Manager	TCP	5060	Acme Packet sip1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
HG Session Manager CS1K7.6 5085 UDP	HG Session Manager	UDP	5085	CS1K7.6	<input type="checkbox"/>	5085	trusted	<input type="checkbox"/>	
HG Session Manager HG ASBCE 5061 TLS	HG Session Manager	TLS	5061	HG ASBCE	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
HG Session Manager HG CM Trunk 2 5071 TLS	HG Session Manager	TLS	5071	HG CM Trunk 2	<input type="checkbox"/>	5071	trusted	<input type="checkbox"/>	

Select : All, None

Page 1 of 2

6.7. Routing Policies

Routing Policies describe the conditions under which calls are 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 and click on the **New** button in the right pane (not shown). The following screen is displayed. 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:

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- Name:** To HG CM Trunk 2
- Disabled:** ☐
- Retries:** 0
- Notes:** Inbound calls to HG CM Trunk 2

The 'SIP Entity as Destination' section features a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
HG CM Trunk 2	172.16.5.201	CM	For Service Provider Calls

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

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left-hand navigation pane is expanded to 'Routing', and the 'Routing Policies' sub-item is selected. The main content area displays the 'Routing Policy Details' for a policy named 'HG ASBCE'. The 'General' tab is active, showing fields for 'Name' (To HG ASBCE), 'Disabled' (unchecked), 'Retries' (0), and 'Notes' (For outbound calls to Service Pro). Below the 'General' tab is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table listing the destination entity.

Name	FQDN or IP Address	Type	Notes
HG ASBCE	172.16.3.71	Other	HG ASBCE

6.8. 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 Clearcom 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 and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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**.

- Click **Commit** to save.

Examples of dial patterns used for the compliance testing are shown below.

The first example shows dial pattern **28**, with destination SIP Domain of **-ALL-**, Originating Location Name **HG Communication Manager** and Routing Policy name **To HG ASBCE**. This dial pattern was used for local outbound calls in Mexico.

Note: The SIP Domain was set to **-ALL-** since dial pattern 28 is shared among multiple SIP Domains in the Avaya lab, SIP Domain **Avaya.lab.com** could have been used instead.

AVAYA
Aura System Manager 7.0

Last Logged in at October 27, 2015 5:10 PM
Log off
admin

Home Routing

Home / Elements / Routing / Dial Patterns

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

General

* Pattern: 28
* Min: 8
* Max: 8

Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: -ALL-
Notes: Outbound to Clearcom Test Softphone

Originating Locations and Routing Policies

Add Remove

2 Items Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	HG Communication Manager		To HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	For outbound calls to Service Provider
<input type="checkbox"/>	MA Communication Manager	HP DL360	Outbound to MA ASBCE	0	<input type="checkbox"/>	MA_SBCE	Outbound to MA_SBCE

Select : All, None

The following dial pattern used for the compliance testing was for inbound calls to the enterprise. It uses dial pattern **55** matching the first two digits of the DID numbers assigned to Communication Manager. This dial pattern was configured with the destination SIP Domain of **-ALL-**, Originating Location Name **HG ASBCE**, and Routing Policy name **To HG CM Trunk 2**.

AVAYA
Aura System Manager 7.0

Last Logged on at October 27, 2015 5:10 PM
Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel Help

General

* Pattern: 55
* Min: 10
* Max: 10

Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: -ALL-
Notes: Clearcom Incoming

Originating Locations and Routing Policies

Add Remove

2 Items 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"/>	HG ASBCE		To HG CM Trunk 2	0	<input type="checkbox"/>	HG CM Trunk 2	Inbound calls to HG CM Trunk 2
<input type="checkbox"/>	HA SBCE	Avaya SBCE 6.3	Incoming to HA CM trunk 2	0	<input type="checkbox"/>	HA_CM Trunk 2	

Select: All, None

Note: The SIP Domain was set to **-ALL-** since dial pattern 55 is shared among multiple SIP Domains in the Avaya lab, SIP Domain **Avaya.lab.com** could have been used instead.

Note: The same procedure should be followed to add other required dial patterns.

6.9. Add/View Avaya Aura® Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If Session Manager already exists, 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 IP address of the Session Manager management interface.

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 IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of the Session Manager signaling interface.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields.

- Click **Save** (not shown).

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

AVAYA
Aura System Manager 7.0

Last logged on at October 6, 2015 3:00 PM
Log off admin

Home / Elements / Session Manager / Session Manager Administration

View Session Manager

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

SIP Entity Name: HG Session Manager
Description: Lab-HG SM
Management Access Point Host Name/IP: 172.16.5.31
Direct Routing to Endpoints: Enable
Maintenance Mode: ☐

Security Module

SIP Entity IP Address: 172.16.5.32
Network Mask: 255.255.255.0
Default Gateway: 172.16.5.254
Call Control PHB: 46
*SIP Firewall Configuration: Rule Set for HG Session Manager

7. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to Clearcom's SIP Trunking service.


It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

7.1. Log in Avaya SBCE

Use a web browser to access the Avaya SBCE web interface, enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the management IP address of the Avaya SBCE.

Enter the appropriate credentials and then click **Log In**.



The screenshot displays the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is shown in red, with the text "Session Border Controller for Enterprise" below it. To the right, under the heading "Log In", there are input fields for "Username:" and "Password:". The username field contains the text "username". Below these fields is a "Log In" button. To the right of the login fields, there is a block of legal disclaimer text. At the bottom right, the copyright notice "© 2011 - 2015 Avaya Inc. All rights reserved." is visible.

AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

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

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

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

© 2011 - 2015 Avaya Inc. All rights reserved.

The **Dashboard** main page will appear as shown below.

Session Border Controller for Enterprise AVAYA

Dashboard

Information

System Time	03:47:35 AM CDT	Refresh
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	04/08/2016 06:48:12 CDT	
Failed Login Attempts	1	

Alarms (past 24 hours)

None found.

Installed Devices

EMS

Avaya SBCE

Incidents (past 24 hours)

Avaya SBCE: Heartbeat Failed, Server is Down

Avaya SBCE: Heartbeat Failed, Server is Down

Avaya SBCE: Heartbeat Failed, Server is Down

Avaya SBCE: Heartbeat Failed, Server is Down

To view the system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. For the compliance test, a single Device Name **Avaya SBCE** was already added.

Session Border Controller for Enterprise AVAYA

System Management

Devices Updates SSL VPN Licensing

Device Name	Management IP	Version	Status	
Avaya SBCE	10.10.10.10	7.0.1-03-8739	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

To view the network configuration assigned to the Avaya SBCE, click **View** as shown on the screen above. The **System Information** window is displayed as shown below.

The **System Information** screen shows **Network Configuration**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**.

System Information: Avaya SBCE

General Configuration

Appliance Name

Avaya SBCE

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 2000

2000

Advanced Sessions

Requested: 2000

2000

Scopia Video Sessions

Requested: 500

500

CES Sessions

Requested: 0

0

Encryption

☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
172.16.5.72	172.16.5.72	255.255.255.0	172.16.5.254	A1
172.16.5.73	172.16.5.73	255.255.255.0	172.16.5.254	A1
10.10.157.186	10.10.157.186	255.255.255.192	10.10.157.129	B1
10.10.157.187	10.10.157.187	255.255.255.192	10.10.157.129	B1
10.10.157.188	10.10.157.188	255.255.255.192	10.10.157.129	B1

DNS Configuration

Primary DNS

10.5.216.122

Secondary DNS

10.5.153.242

DNS Location

DMZ

DNS Client IP

10.10.157.186

Management IP(s)

IP

172.16.5.71

On the previous screen, note that the **A1** interface corresponds to the inside interface (Private Network side) and **B1** interface corresponds to the outside interface (Public Network side) of the Avaya SBCE. On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed. Refer to **Figure 1** for the IP addresses for both the A1 and B1 interfaces on the Avaya SBCE.

DNS server configuration can be entered or modified as needed, by clicking **Edit** on the **System Management/Devices** tab shown on the previous page. Under **DNS Settings**, enter the IP addresses of the **Primary** and **Secondary** DNS servers. During the compliance test, public DNS servers were used, and the IP address corresponding to the public interface of the Avaya SBCE was selected from the **DNS Client IP** scroll down menu, as shown on the screen below. Click **Finish** (not shown) when done.

Edit Device: Avaya SBCE X

Address and interface changes must be made in Network Management.

Any changes to the management network on this device will reboot the device.

General Settings

Appliance Name X

Device Settings

High Availability (HA) ☐

DNS Settings

Primary
Ex: 202.201.192.1

Secondary
Optional, Ex: 202.201.192.1

DNS Client IP ▼

Network Settings

IMPORTANT! – During the Avaya SBCE installation, the Management interface, (labeled “M1”), of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

7.2. TLS Management

7.2.1. TLS Certificates

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

This section describes the TLS profiles that were created for the Avaya SBCE, including the following:

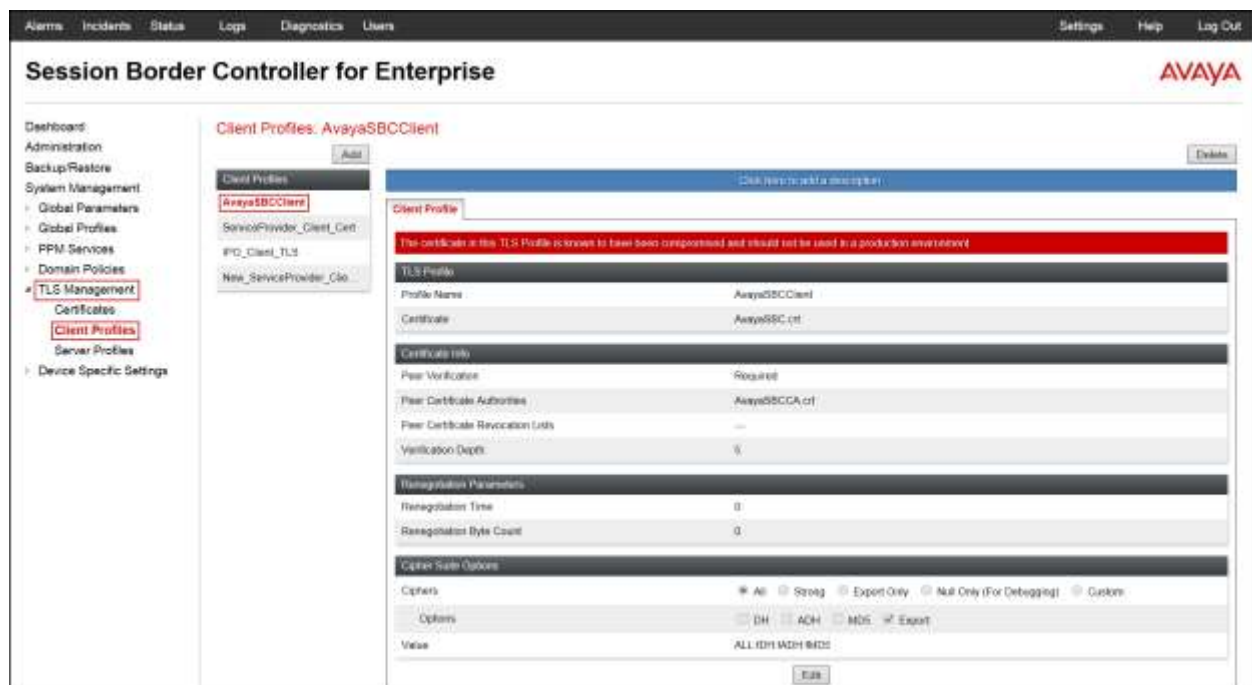
- Create TLS client and server profiles to identify which certificates will be used in various TLS connections on the Avaya SBCE.

It is assumed that generation and installation of certificates on the Avaya SBCE, and the exchange of TLS CA certificates with the Service Provider, have been previously completed, and is not discussed in this document. Refer to items [8] in **Section 11**.

7.2.2. TLS Client Profile – Avaya Session Manager

For the TLS client profile toward Session Manager, the pre-existing (pre-installed) demo TLS client profile by the name *AvayaSBCClient* was used.

The following screen capture shows the pre-existing TLS client Profile *AvayaSBCClient*.



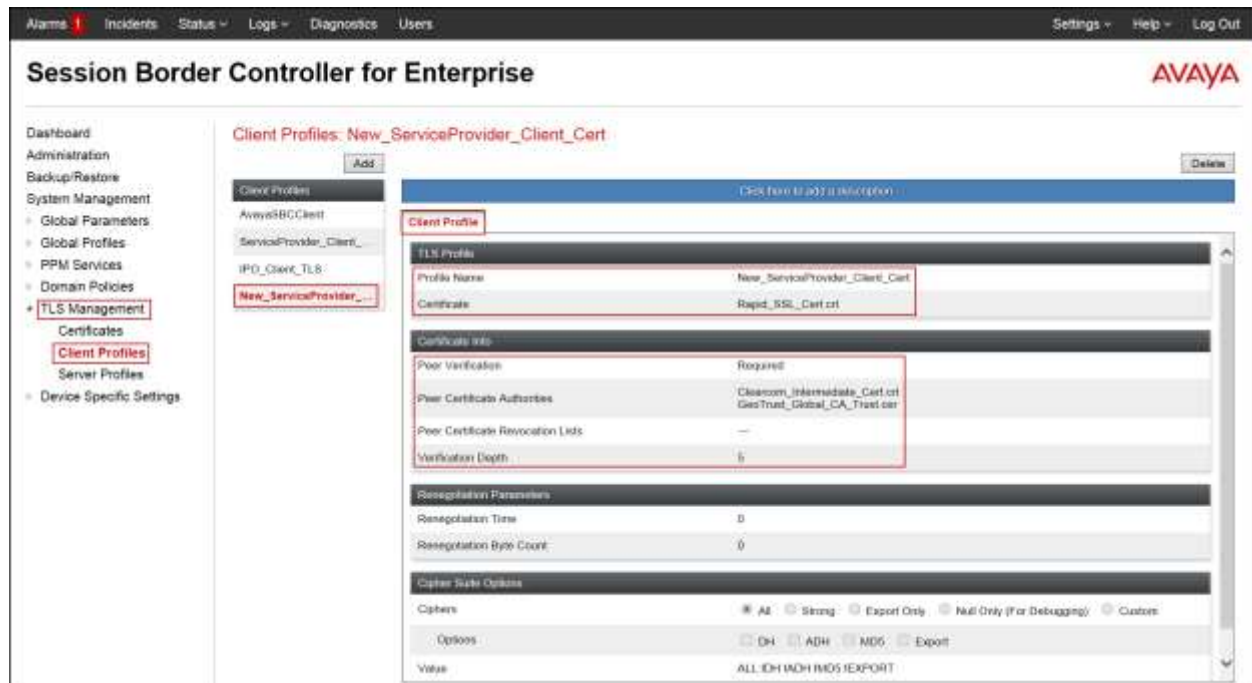
7.2.3. TLS Client Profile – Service Provider

To create a TLS client profile toward the Service Provider, navigate to **TLS Management** → **Client Profiles** and click **Add**. Configure the following parameters:

- Under TLS Profile enter the **profile name**; the name of *New_ServiceProvider_Client_Cert* was used in this example.
- Under TLS Profile select the **Certificate** to be used from the pull down menu; *Rapid_SSL_Cert.crt* was selected in the sample configuration.
- Under Certificate Info, by using Ctrl+Click, select the CA certificates to be used for the **Peer Certificate Authorities** field, *Clearcom_Intermediate_Cert.crt* and *GeoTrust_Global_CA_Trust.cer* were selected in the sample configuration.
- Set the **Verification Depth** to 5.
- Default values can be used for the remaining fields.
- Click **Finish**.

The screenshot shows the 'New Profile' configuration window. At the top, there is a warning message: 'WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.' Below the warning, the 'TLS Profile' section contains 'Profile Name' (ceProvider_Client_Cert) and 'Certificate' (Rapid_SSL_Cert.crt). The 'Certificate Info' section shows 'Peer Verification' set to 'Required'. The 'Peer Certificate Authorities' list contains 'Clearcom_Intermediate_Cert.crt' and 'GeoTrust_Global_CA_Trust.cer'. The 'Verification Depth' is set to 5. The 'Renegotiation Parameters' section shows 'Renegotiation Time' (0 seconds) and 'Renegotiation Byte Count' (0). The 'Cipher Suite Options' section shows 'Ciphers' set to 'All' and 'Options' with checkboxes for 'DH', 'ADH', 'MD5', and 'Export'. The 'Value' field shows 'ALL:!DH:!ADH:!MD5:!EXPORT'. A 'Finish' button is at the bottom.

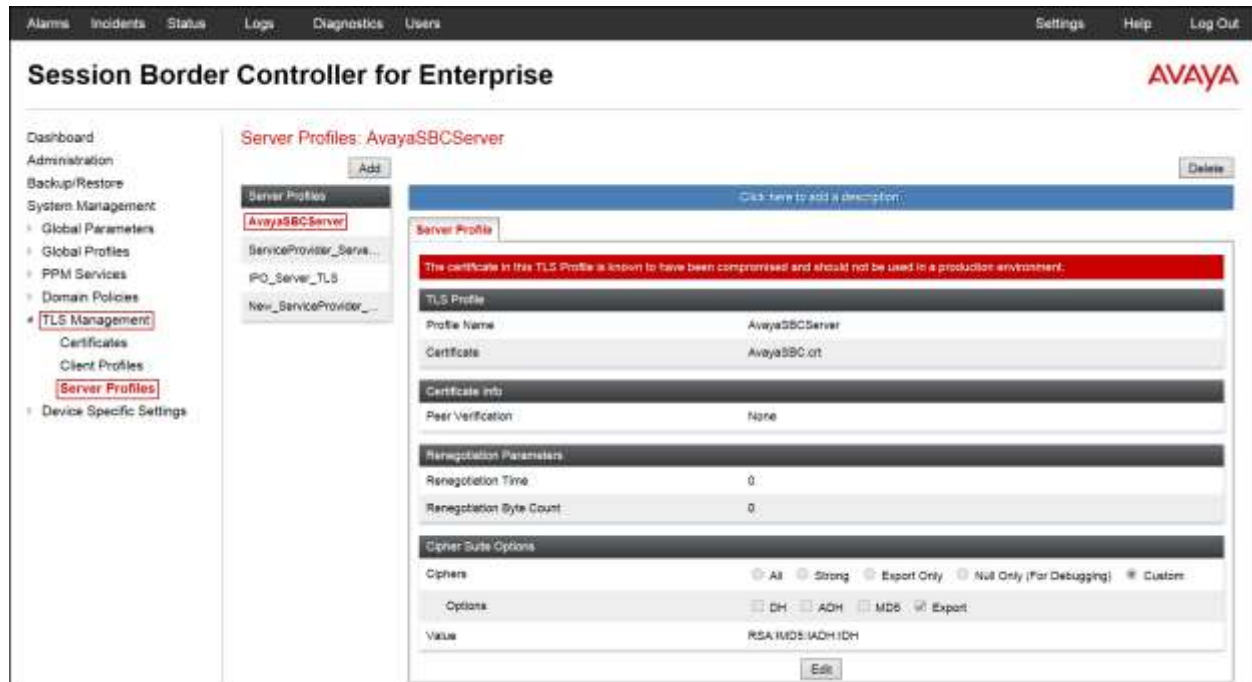
The following screen capture shows the newly created **New_ServiceProvider_Client_Cert** client Profile.



7.2.4. TLS Server Profile – Avaya Session Manager

For the TLS server profile toward Session Manager, the pre-existing (pre-installed) demo TLS server profile by the name *AvayaSBCServer* was used.

The following screen capture shows the pre-existing TLS server Profile **AvayaSBCServer**.

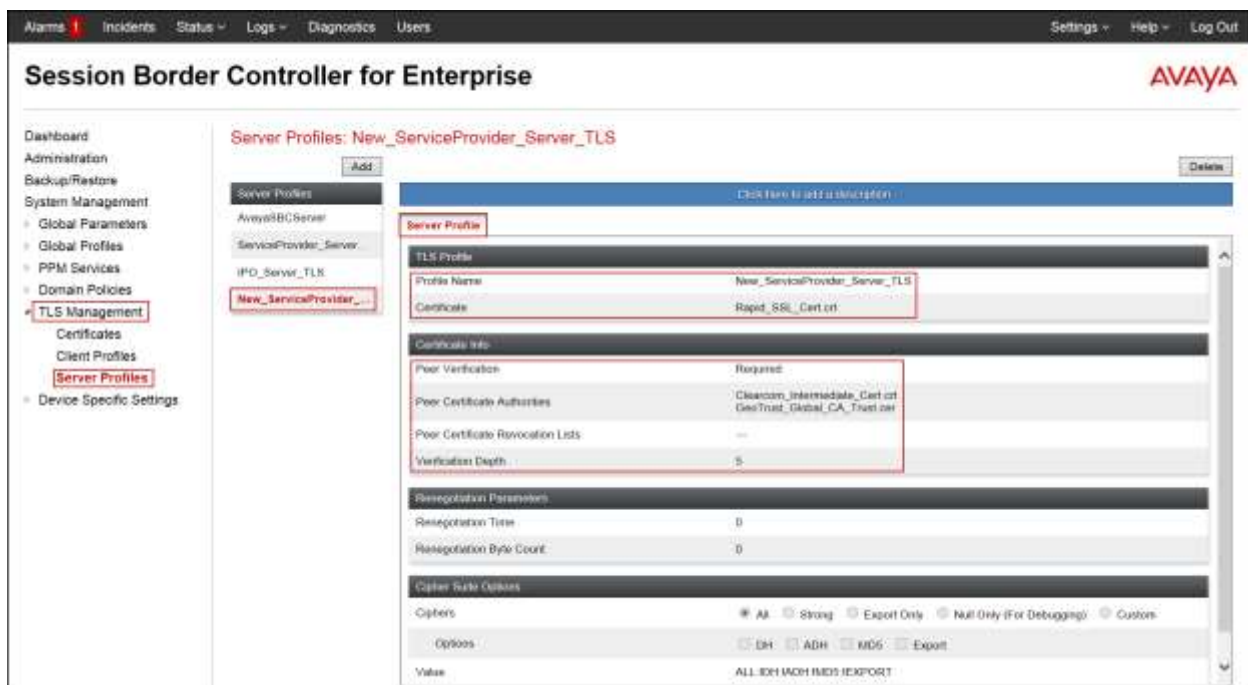


7.2.5. TLS Server Profile – Service Provider

To create a TLS server profile toward the Service Provider, navigate to **TLS Management → Server Profiles** and click **Add**. Configure the following parameters:

- Under TLS Profile enter the **profile name**; the name of *New_ServiceProvider_Server_TLS* was used in this example.
- Under TLS Profile select the **Certificate** to be used from the pull down menu; *Rapid_SSL_Cert.crt* was selected in the sample configuration.
- Under Certificate Info, **Peer Verification**, select **Required** from the pull down menu.
- Under Certificate Info, by using Ctrl+Click, select the CA certificates to be used for the **Peer Certificate Authorities** field, *Clearcom_intermediate_Cert.crt* and *GeoTrust_Global_CA_Trust.cer* were selected in the sample configuration.
- Set the **Verification Depth** to 5.
- Default values can be used for the remaining fields.
- Click **Finish**.

The following screen capture shows the newly created *New_ServiceProvider_Server_TLS* server Profile.



7.3. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

7.3.1. Server Interworking Avaya-SM

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk Service Providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or “cloned”, and then modified to meet specific requirements for the enterprise SIP-enabled solution.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone** on top right of the screen.

Enter the new profile name in the **Clone Name** field; the name of **Avaya-SM** was chosen in this example. Click **Finish** (not shown).

The following screen capture shows the **General** tab of the newly created **Avaya-SM** Server Interworking Profile.

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 (selected), and Server Interworking (selected). The main content area is titled "Interworking Profiles: Avaya-SM" and shows a list of profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-cdm, csp, Spers-Halo, OCS-FrontEnd-Server, Avaya-SM (highlighted), SP-General, Avaya-CS1000, Avaya-IPD, and Avaya-CM. The "Avaya-SM" profile is selected, and the "General" tab is active. The "General" tab shows various settings for the profile, including Hold Support, 180 Handling, 181 Handling, 182 Handling, 183 Handling, Refer Handling, URI Group, Send Hold, Delayed Offer, 3xx Handling, Diversion Header Support, Delayed SDP Handling, Re-Invite Handling, Prack Handling, Allow 18X SDP, T.38 Support, URI Scheme, and Via Header Format.

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

The following screen capture shows the **Advanced** tab of the newly created **Avaya-SM** Server Interworking Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' expanded to show 'Server' and 'Interworking' sub-menus. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left, including 'cs2100', 'avaya-cu', 'OCS-Edge-Server', 'cisco-com', 'cups', 'Spera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM' (highlighted), 'SP-General', 'Avaya-CS1000', 'Avaya-IPO', and 'Avaya-CM'. The 'Avaya-SM' profile is selected, and its configuration is shown in the 'Advanced' tab. The configuration includes a table for 'Record Routes' with columns for 'Record Routes' and 'Both Sides'. The table contains the following data:

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

Below the table is a section for 'DTMF' with a single row: 'DTMF Support' set to 'None'. An 'Edit' button is located at the bottom right of the configuration area.

7.3.2. Server Interworking SP-General

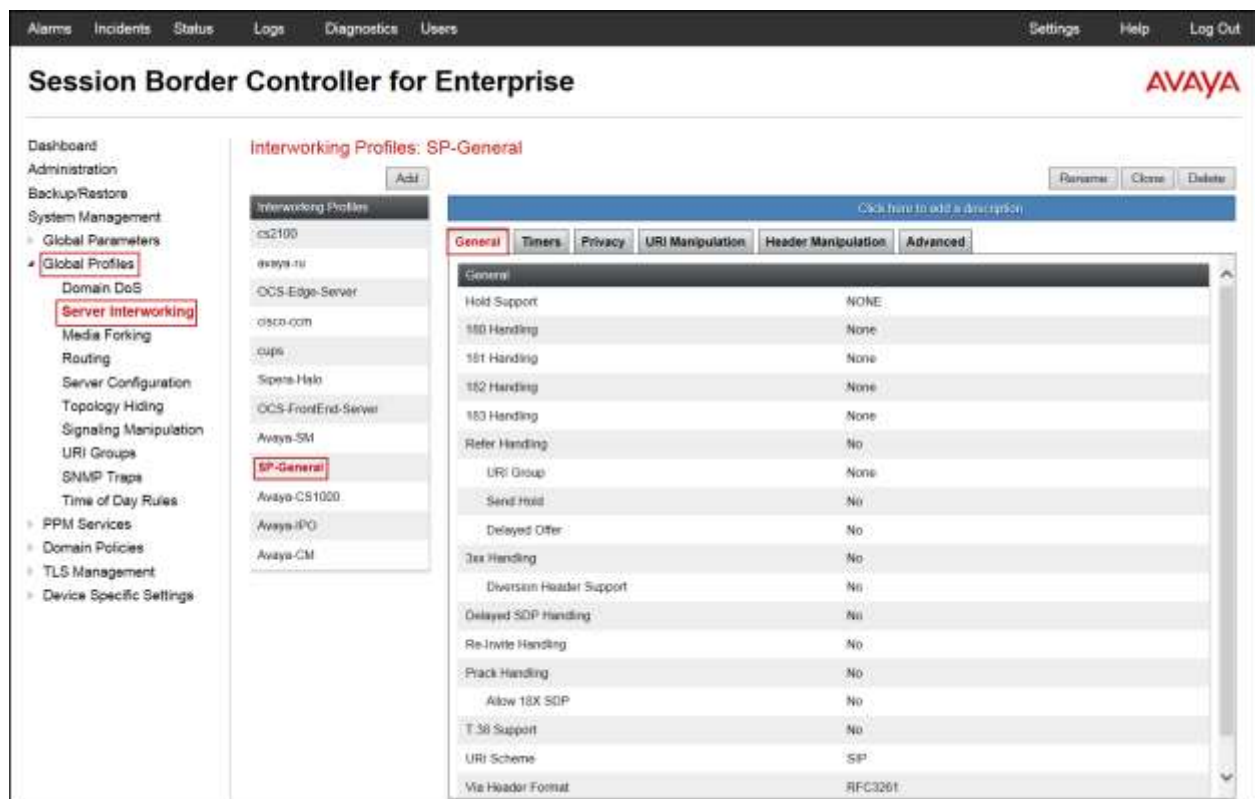
A second Server Interworking profile named **SP-General** was created for the Service Provider.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add**.

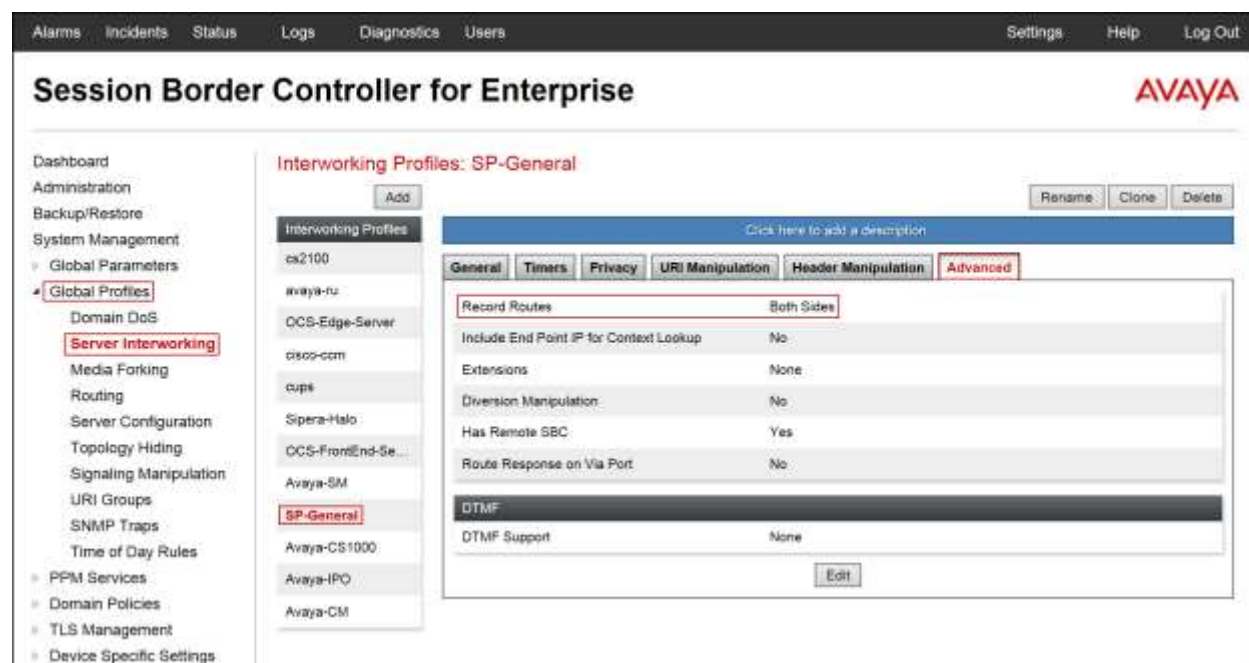
Enter the new profile name (not shown); the name of **SP-General** was chosen in this example. Click **Next**:

- Leaving other fields with their default values, click **Next** until the Advanced tab is reached, check **Both Sides** then click **Finish** on the Advanced tab.

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.



The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.



7.3.3. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [8] in the **References** section for more information on this topic.

Sigma scripts were created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

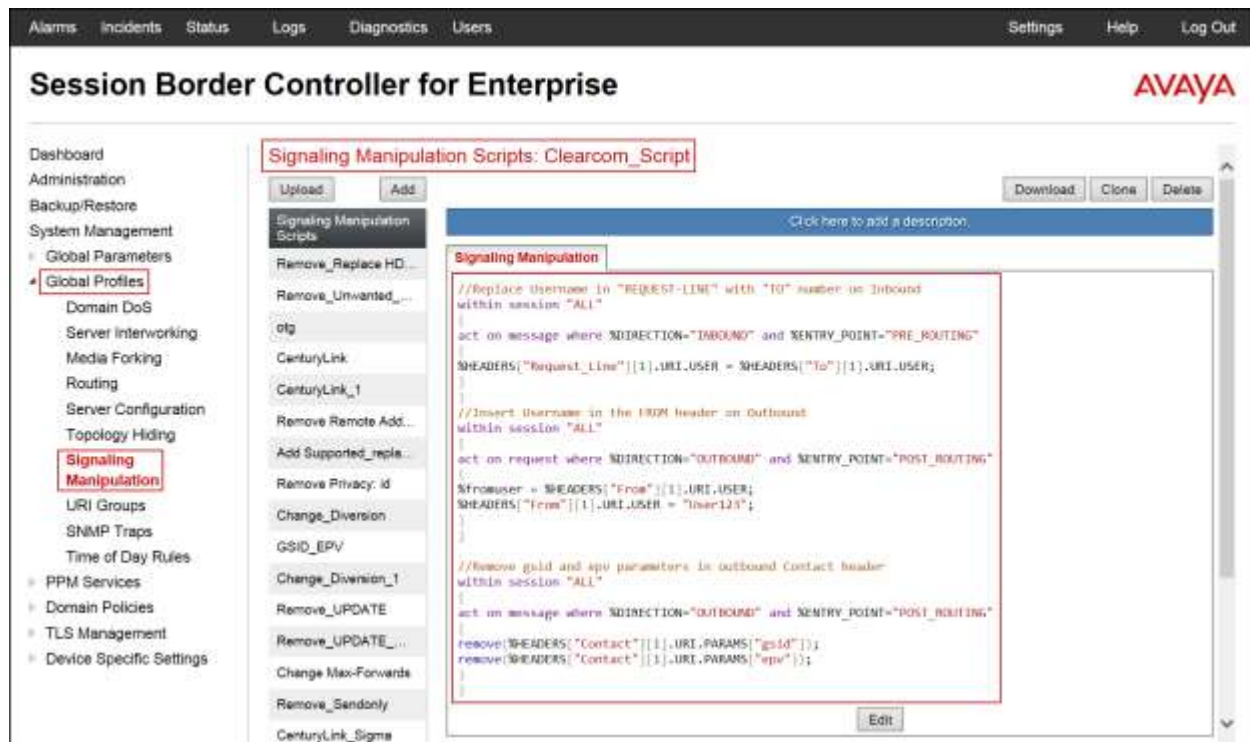
- Include the SIP trunk credential's username in the "From" header of all outbound calls.
- Copy the destination DID number present in the "To" header of incoming calls to the "Request-URI" header.
- Remove the "gsid" and "epv" parameters from outbound "Contact" headers.

The script will later be applied to the Server Configuration profile corresponding to the service provider in **Section 7.3.4**.

On the left navigation pane, select **Global Profiles** → **Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name; the name *Clearcom_Script* was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.

The following screen capture shows the **Clearcom_Script** script after it was added.



7.3.4. Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server which is the SIP Proxy at the Service Provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add** in the **Server Profiles** section and enter the profile name: *Session Manager*.

On the **Edit Server Configuration Profile – General** window:

- **Server Type:** select *Call Server*.
- **IP Address / FQDN:** *172.16.5.32* (IP Address of the Session Manager SIP entity).
- **Port:** *5061* (This port must match the port number defined in **Section 6.6**).
- **Transports:** Select *TLS*.
- Click **Next**.

The screenshot shows the 'Edit Server Configuration Profile - General' window. At the top, a blue banner states: 'Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.' Below this, the 'Server Type' is set to 'Call Server'. An 'Add' button is to the right. A table lists the configuration details:

IP Address / FQDN	Port	Transport	
172.16.5.32	5061	TLS	Delete
			Delete

A 'Finish' button is located at the bottom center.

- Click **Next** in the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** in the **Add Server Configuration Profile - Heartbeat** window (not shown).

On the **Add Server Configuration Profile - Advanced** window:

- Check **Enable Grooming**.
- Select **Avaya-SM** from the **Interworking Profile** drop down menu.
- Select **AvayaSBCClient** from the **TLS Client Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Avaya-SM

TLS Client Profile AvayaSBCClient

Signaling Manipulation Script None

Connection Type SUBID

Securable ☐

Back Finish

The following screen capture shows the **General** tab of the newly created **Session Manager** Server Profile.

Session Border Controller for Enterprise

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Server Configuration: Session Manager

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles Server Configuration Topology Hiding Signaling Manipulation URI Groups SNMP Traps Time of Day Rules PPM Services Domain Policies TLS Management Device Specific Settings

Server Profiles Add

Session Manager

Service Provider

Com Manager

CS1000

IP Office

Service Provider TLS

General Authentication Heartbeat Advanced

Server Type Call Server

IP Address / FQDN	Port	Transport
172.16.5.32	5061	TLS

Edit

Rename Clone Delete

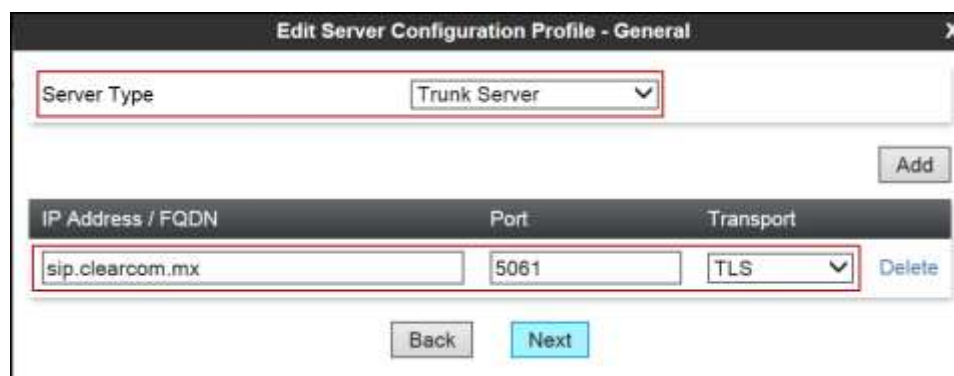
The following screen capture shows the **Advanced** tab of the newly created **Session Manager** Server Profile.



To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** section and enter the profile name: *Service Provider TLS*.

On the **Edit Server Configuration Profile – General** window

- **Server Type:** select *Trunk Server*.
- **IP Address/FQDN:** *sip.clearcom.mx* (the Fully Qualified Domain Name of the service provider SIP proxy server. This information was provided by Clearcom.).
- **Port:** *5061*.
- **Transports:** Select *TLS*.
- Click **Next**.



On the **Add Server Configuration Profile - Authentication** window:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Enter the **Realm** credential provided by the service provider for SIP trunk registration. Note that the Service Provider's Domain Name was used (Must be entered, currently cannot be detected automatically from the challenge).
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

The screenshot shows a window titled "Add Server Configuration Profile - Authentication". Inside the window, a red box highlights the following fields:

- Enable Authentication**: A checkbox that is checked.
- User Name**: A text field containing "User123".
- Realm**: A text field containing "clearcom.mx". Below this field is the text "(Leave blank to detect from server challenge)".
- Password**: A text field with masked characters ".....".
- Confirm Password**: A text field with masked characters "....." and a small circular icon to its right.

Below the highlighted fields are two buttons: "Back" and "Next".

On the **Add Server Configuration Profile - Heartbeat** window:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider, **120** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI**: Use the **User Name** entered above in the **Authentication** screen (**User123**) and the Service Provider's domain name (**clearcom.mx**), as shown on the screen below.
 - **To URI**: Use the **User Name** entered above in the **Authentication** screen (**User123**) and the Service Provider's domain name (**clearcom.mx**), as shown on the screen below.
- Click **Next**.

The screenshot shows a window titled "Add Server Configuration Profile - Heartbeat". The window contains a form with the following fields and values:

Field	Value
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER
Frequency	120 seconds
From URI	User123@clearcom.mx
To URI	User123@clearcom.mx

At the bottom of the form are two buttons: "Back" and "Next".

On the **Add Server Configuration Profile - Advanced** window:

- Select **SP-General** from the **Interworking Profile** drop down menu.
- Select **New_ServiceProvider_Client_Cert** from the **TLS Client Profile** drop down menu
- Select the **Clearcom_Script** from the **Signaling Manipulation Script** drop down menu (Section 7.4.3.).
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

TLS Client Profile New_ServiceProvider_Client_Cert

Signaling Manipulation Script Clearcom_Script

Connection Type SUBID

Securable ☐

Back Finish

The following screen capture shows the **General** tab of the newly created **Service Provider TLS** Server Configuration Profile.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
PPM Services
Domain Policies
TLS Management
Device Specific Settings

Server Configuration: Service Provider TLS

Add Rename Clone Delete

General Authentication Heartbeat Advanced

Server Type Trunk Server

IP Address / FQDN	Port	Transport
sip.clearcom.mx	5061	TLS

Edit

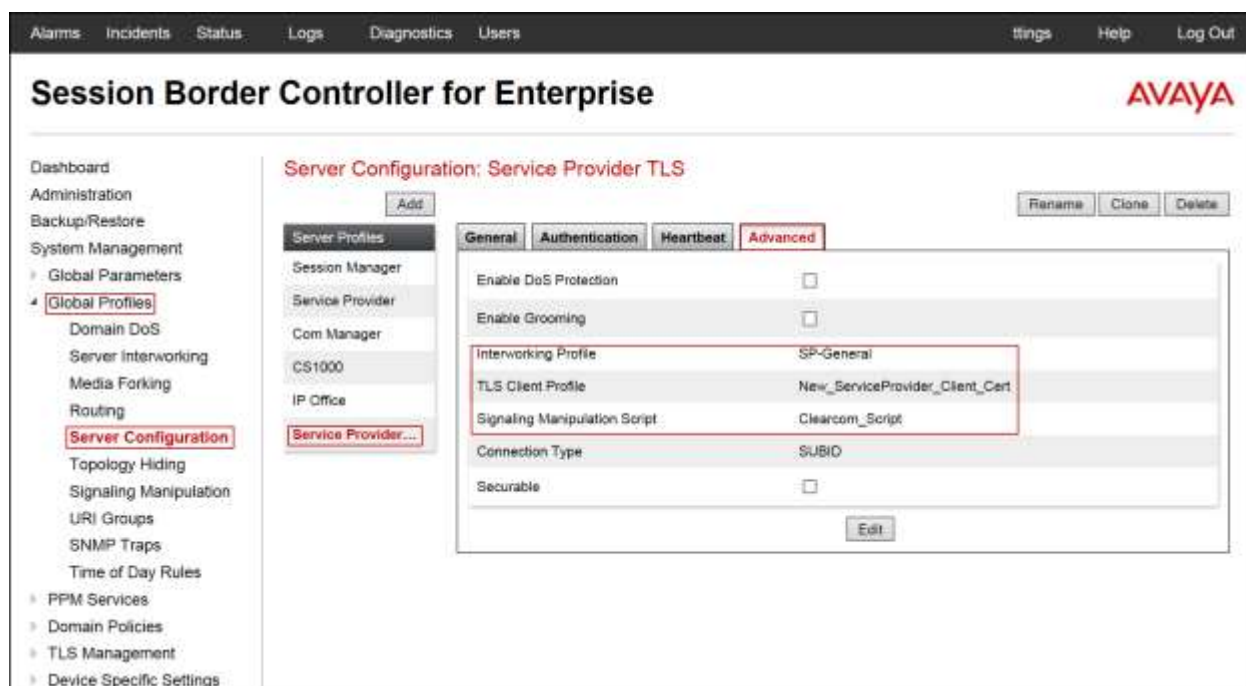
The following screen capture shows the **Authentication** tab of the newly created **Service Provider TLS** Server Configuration Profile.



The following screen capture shows the **Heartbeat** tab of the newly created **Service Provider TLS** Server Configuration Profile.



The following screen capture shows the **Advanced** tab of the newly created **Service Provider TLS** Server Configuration Profile.



7.3.5. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created; one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are sent to the service provider.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SM**.
- Click **Next**.

On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **Session Manager**.
- The **Next Hop Address** is populated automatically with **172.16.5.32:5061 (TLS)** (Session Manager IP address, Port and Transport).
- Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window. At the top, there are dropdowns for 'URI Group' (set to '*') and 'Time of Day' (set to 'default'). Below these are checkboxes for 'Load Balancing' (set to 'Priority'), 'NAPTR' (unchecked), 'Transport' (set to 'None'), 'Next Hop Priority' (checked), 'Next Hop In-Dialog' (unchecked), and 'Ignore Route Header' (unchecked). An 'Add' button is located to the right of these settings. Below the settings is a table with the following columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The table contains one row with the following values: '1', 'Session Manager', '172.16.5.32:5061 (TLS)', and 'None'. A 'Delete' button is located to the right of the table. At the bottom of the window are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manager	172.16.5.32:5061 (TLS)	None

The following screen capture shows the newly created **Route_to_SM** Routing Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Routing' highlighted under 'Global Profiles'. The main content area is titled 'Routing Profiles: Route_to_SM' and features an 'Add' button. Below this, a list of routing profiles is shown, with 'Route_to_SM' selected. The 'Route_to_SM' profile is detailed in a table with columns for Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The table shows a single entry with Priority 1, URI Group *, Time of Day default, Load Balancing Priority, Next Hop Address 172.16.5.32, and Transport TLS. The table also includes 'Edit' and 'Delete' buttons for each entry.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	172.16.5.32	TLS

Similarly, for the outbound route:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SP_TLS**.
- Click **Next**.

On the **Routing Profile** screen complete the following:

- **Load Balancing:** Select **DNS/SRV**
- **Priority / Weight:** **1**
- Click on the **Add** button to add a **Next-Hop Address**.
- **Server Configuration:** Select **Service Provider**.
- The **Next Hop Address** is populated automatically with **sip.clearcom.mx:5061 (TLS)** (Service Provider FQDN, Port and Transport).
- Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window. At the top, there are dropdowns for 'URI Group' (set to '*') and 'Time of Day' (set to 'default'). Below these are several configuration options: 'Load Balancing' is set to 'DNS/SRV', 'Transport' is set to 'None', 'Next Hop In-Dialog' is unchecked, and 'Ignore Route Header' is unchecked. An 'Add' button is located to the right of these options. Below the 'Add' button is a table with four columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The table contains one row with the following values: '1' in the first column, 'Service Provider' in the second, 'sip.clearcom.mx:5061 (TLS)' in the third, and 'None' in the fourth. A 'Delete' button is located to the right of the table. At the bottom of the window are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	sip.clearcom.mx:5061 (TLS)	None

The following screen capture shows the newly created **Route_to_SP_TLS** Routing Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Routing' highlighted under 'Global Profiles'. The main content area is titled 'Routing Profiles: Route_to_SP_TLS' and features an 'Add' button. Below this, a list of routing profiles is shown, with 'Route_to_SP_TLS' selected. The details for this profile are displayed in a table with columns for Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The table contains one entry with Priority 1, URI Group *, Time of Day default, Load Balancing DNS/SRV, Next Hop Address sip.clearcom.mx, and Transport TLS. Edit and Delete buttons are available for this entry.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	DNS/SRV	sip.clearcom.mx	TLS

7.3.6. Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk Service Provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

To add the Topology Hiding profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name: *Session_Manager***.
- Click **Finish**.
- Click **Edit** on the newly added **Session_Manager** Topology Hiding profile.
- For **To** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Enterprise (***avaya.lab.com***) under **Overwrite Value**.
- For **From** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the enterprise (***avaya.lab.com***) under **Overwrite Value**.
- For **Request-Line** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Enterprise (***avaya.lab.com***) under **Overwrite Value**.

The screenshot shows a window titled "Edit Topology Hiding Profile" with a table of configuration options. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The rows are for Record-Route, Referred-By, Refer-To, SDP, Via, To, From, and Request-Line. The 'To', 'From', and 'Request-Line' rows are highlighted with a red border. In these rows, the 'Replace Action' is set to 'Overwrite' and the 'Overwrite Value' is 'avaya.lab.com'. A 'Finish' button is at the bottom.

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

Finish

The following screen capture shows the newly created **Session_Manager** Topology Hiding Profile.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Topology Hiding Profiles: Session_Manager

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles Domain DoS Server Interworking Media Forking Routing Server Configuration **Topology Hiding** Signaling Manipulation URI Groups SNMP Traps Time of Day Rules PPM Services Domain Policies TLS Management

Topology Hiding Profile

default cisco_th_profile **Session_Manager** Service_Provider Com Manager C51000 IP Office

Click here to add a description

Topology Hiding

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

Edit

To add the Topology Hiding profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name: *Service_Provider***.
- Click **Finish**.
- Click **Edit** on the newly added **Service_Provider** Topology Hiding profile.
- For **To** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***Clearcom.mx***) under **Overwrite Value**.
- For **From** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***Clearcom.mx***) under **Overwrite Value**.
- For **Request-Line** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***Clearcom.mx***) under **Overwrite Value**.

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

Finish

The following screen capture shows the newly created **Service_Provider** Topology Hiding Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' and 'Topology Hiding' highlighted. The main content area is titled 'Topology Hiding Profiles: Service_Provider'. It features a list of profiles on the left, including 'default', 'clsco_th_profile', 'Session_Manager', 'Service_Provider' (which is selected and highlighted in red), 'Com Manager', 'CS1000', and 'IP Office'. An 'Add' button is located above this list. To the right, the configuration for the 'Service_Provider' profile is shown. It includes a 'Click here to add a description' link and a table of headers and their corresponding actions and values. The table is titled 'Topology Hiding' and has columns for Header, Criteria, Replace Action, and Overwrite Value. The headers listed are Record-Route, Referred-By, Refer-To, SDP, Via, To, From, and Request-Line. The 'To', 'From', and 'Request-Line' headers are highlighted with a red border, and their 'Overwrite Value' is set to 'clearcom.mx'. An 'Edit' button is located below the table.

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

7.4. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

Note: The **default-trunk** Application Rule could have been used instead of creating a new one, but a new Application Rule was created to allow changes in the future.

7.4.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Click on the **Add** button to add a new rule.
- **Rule Name:** enter the name of the profile, e.g., *2000 Sessions*.
- Under **Audio** check *In* and *Out* and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values; the value of *2000* was used in the sample configuration.
- Click **Finish**.

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
☐ CDR w/ RTP
☐ CDR w/o RTP

RTCP Keep-Alive
☐

Back Finish

The following screen capture shows the newly created **2000 Sessions** Application Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Domain Policies' expanded and 'Application Rules' highlighted. The main content area is titled 'Application Rules: 2000 Sessions'. It features a list of application rules on the left, including 'default', 'default-trunk', 'default-subscriber...', 'default-server-low', 'default-server-high', '2000 Sessions' (which is selected and highlighted in red), '500 Sessions', 'Remote-Workers', and 'test'. The '2000 Sessions' rule is shown in detail on the right. It has a table with columns for 'Application Type', 'In', 'Out', 'Maximum Concurrent Sessions', and 'Maximum Sessions Per Endpoint'. The 'Audio' application type is configured with 'In' and 'Out' checked, and both 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint' set to 2000. The 'Video' application type is not configured. Below the table, there is a 'Miscellaneous' section with 'CDR Support' set to 'None' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is located at the bottom right of the rule configuration area.

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

7.4.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward Session Manager and one toward the Service Provider.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

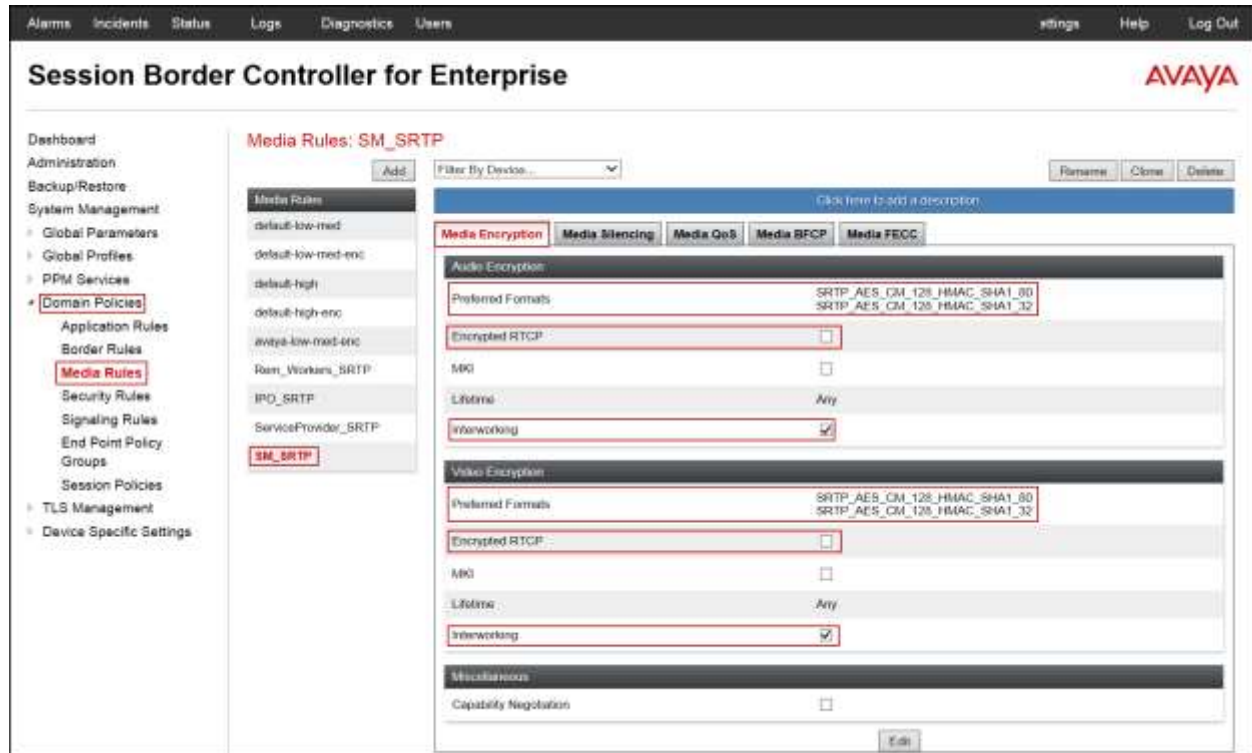
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter **SM_SRTP**.
- Click Next (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **SRTP_AES_CM_128_HMAC_SHA1_32**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that **Capability Negotiation** is unchecked.
- Click **Next**.

The screenshot shows the 'Media Rule' configuration window. It is divided into three main sections: Audio Encryption, Video Encryption, and Miscellaneous. In the Audio Encryption section, Preferred Format #1 is set to SRTP_AES_CM_128_HMAC_SHA1_80, Preferred Format #2 is set to SRTP_AES_CM_128_HMAC_SHA1_32, Preferred Format #3 is set to NONE, Encrypted RTCP is unchecked, MKI is unchecked, Lifetime is set to 2^, and Interworking is checked. The Video Encryption section has identical settings. In the Miscellaneous section, Capability Negotiation is unchecked. At the bottom, there are 'Back' and 'Next' buttons.

Section	Setting	Value
Audio Encryption	Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
	Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_32
	Preferred Format #3	NONE
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	2^
	Interworking	<input checked="" type="checkbox"/>
Video Encryption	Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
	Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_32
	Preferred Format #3	NONE
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	2^
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Capability Negotiation	<input type="checkbox"/>

Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

The following screen capture shows the newly created **SM_SRTP** Media Rule



To add a media rule in the Service Provider direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

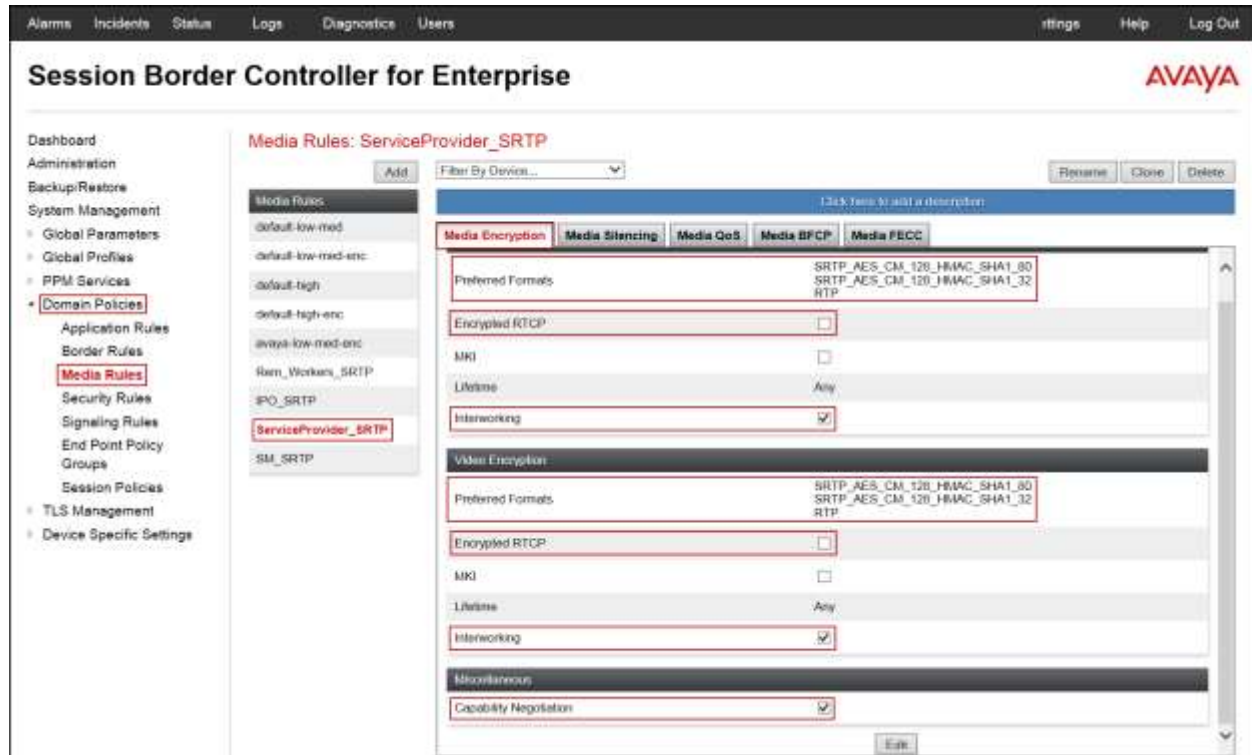
- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter *ServiceProvider_SRTP*.
- Click Next.
- Under Audio Encryption, **Preferred Format #1**, select *SRTP_AES_CM_128_HMAC_SHA1_80*.
- Under Audio Encryption, **Preferred Format #2**, select *SRTP_AES_CM_128_HMAC_SHA1_32*.
- Under Audio Encryption, **Preferred Format #3**, select *RTP*.
- Under Audio Encryption, uncheck *Encrypted RTCP*.
- Under Audio Encryption, check *Interworking*.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous check *Capability Negotiation*.
- Click **Finish**.

The screenshot shows a 'Media Encryption' configuration window with three main sections: Audio Encryption, Video Encryption, and Miscellaneous. Each section has a red box highlighting the 'Preferred Format' dropdowns and the 'Interworking' checkbox. The 'Encrypted RTCP' checkbox is unchecked in both Audio and Video sections. The 'Capability Negotiation' checkbox is checked in the Miscellaneous section. A 'Finish' button is at the bottom.

Section	Option	Value
Audio Encryption	Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
	Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_32
	Preferred Format #3	RTP
	Encrypted RTCP	<input type="checkbox"/>
	Interworking	<input checked="" type="checkbox"/>
Video Encryption	Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
	Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_32
	Preferred Format #3	RTP
	Encrypted RTCP	<input type="checkbox"/>
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Capability Negotiation	<input checked="" type="checkbox"/>

Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

The following screen capture shows the newly created **ServiceProvider_SRTP** Media Rule.



7.4.3. Signaling Rules

For the compliance test, the **default** Signaling Rule was used.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBC) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo.

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 (highlighted), Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (highlighted), End Point Policy Groups, Session Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Signaling Rules: default". It features an "Add" button, a "Filter By Device..." dropdown, and a "Clone" button. A warning message states: "It is not recommended to add the defaults. Try cloning or adding a new rule instead!".

The "Signaling Rules" section includes a list of rules with "default" selected. Below this, the "General" tab is active, showing the following settings:

Category	Item	Action
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
Content-Type Policy	Enable Content-Type Checks	<input checked="" type="checkbox"/>
	Action	Allow

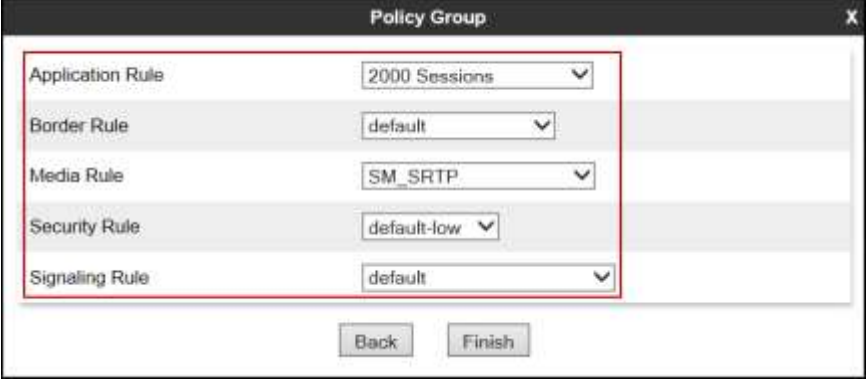
At the bottom of the Content-Type Policy section, there are additional settings for "Multipart Action" and "Allow".

7.4.4. End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add Group**, under **Group Name** enter *SM_SRTP*.

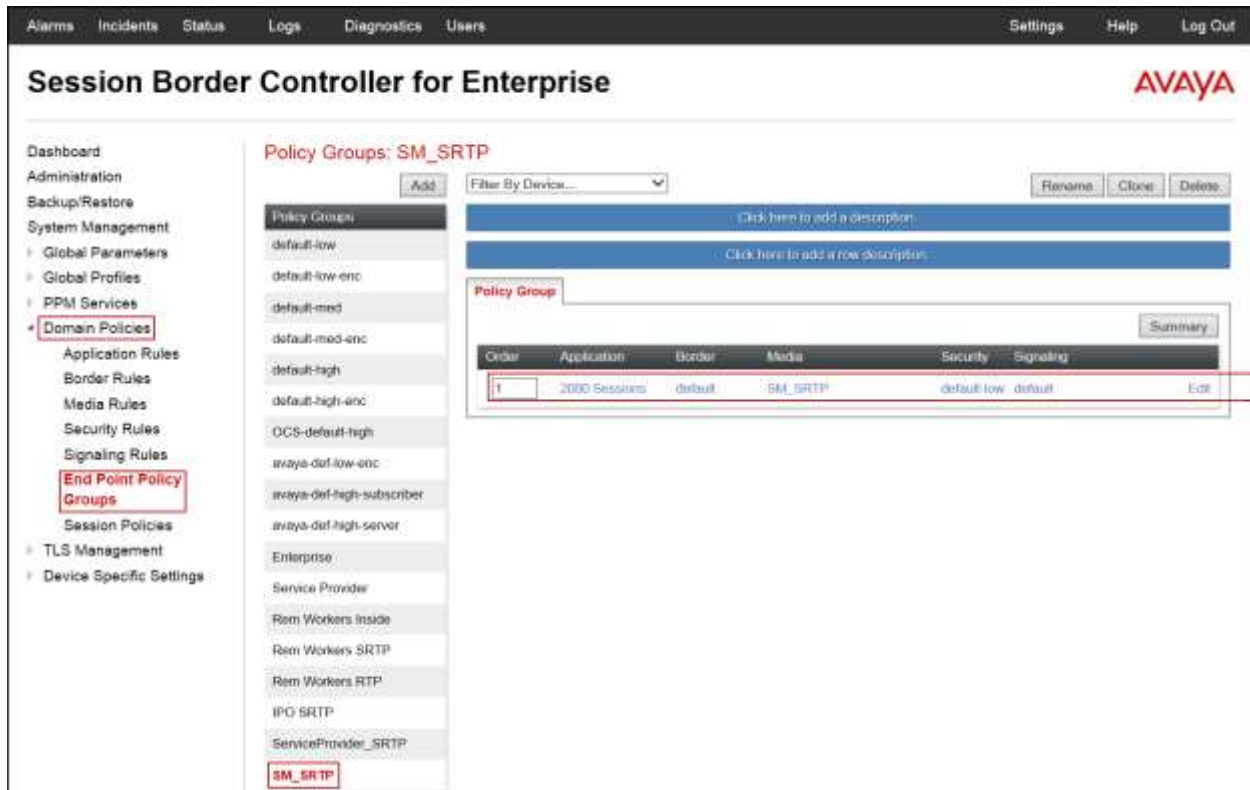
- **Application Rule:** *2000 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *SM_SRTP*.
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default*
- Click **Finish**.



The screenshot shows a 'Policy Group' configuration window with a red border. It contains five rows of configuration options, each with a label and a dropdown menu. The values selected in the dropdowns are: '2000 Sessions' for Application Rule, 'default' for Border Rule, 'SM_SRTP' for Media Rule, 'default-low' for Security Rule, and 'default' for Signaling Rule. At the bottom of the window are two buttons: 'Back' and 'Finish'.

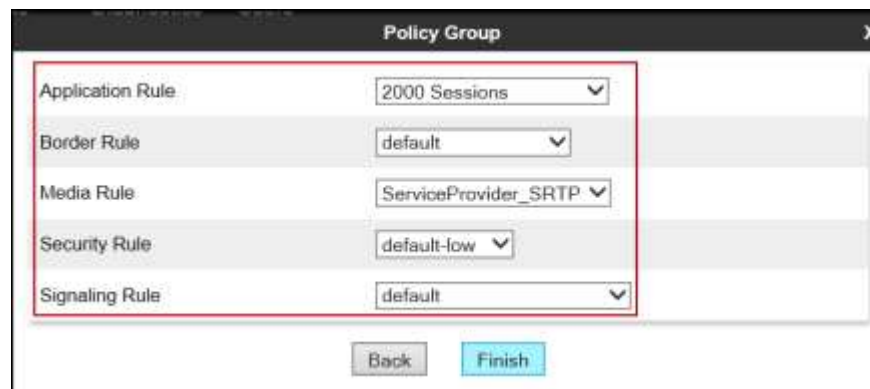
Rule Type	Selected Value
Application Rule	2000 Sessions
Border Rule	default
Media Rule	SM_SRTP
Security Rule	default-low
Signaling Rule	default

The following screen capture shows the newly created **SM_SRTP** End Point Policy Group.



Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add Group**, under **Group Name** enter *ServiceProvider_SRTP*.

- **Application Rule:** *2000 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *ServiceProvider_SRTP*.
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default*.
- Click **Finish**.



The following screen capture shows the newly created **ServiceProvider_SRTP** End Point Policy Group.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Policy Groups: ServiceProvider_SRTP

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
End Point Policy Groups
Session Policies
TLS Management
Device Specific Settings

Policy Groups: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, OCS-default-high, avaya-def-low-enc, avaya-def-high-subscriber, avaya-def-high-server, Enterprise, Service Provider, Rem Workers Inside, Rem Workers SRTP, Rem Workers RTP, IPO SRTP, **ServiceProvider_SRTP**, SM SRTP

Click here to add a description
Hover over a row to see its description

Policy Group

Order	Application	Border	Media	Security	Signing	Summary
1	2000 Sessions	default	ServiceProvider_SRTP	default-low	default	Edit

7.5. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

7.5.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted entity items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in these Application Notes.

Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

Network Management: Avaya SBCE

Devices: Avaya SBCE

Interfaces: Networks

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	172.16.5.254	255.255.255.0	A1	172.16.5.71	Edit Delete
Network_B1	192.168.157.129	255.255.255.192	B1	192.168.157.186	Edit Delete

PPM Services

- Domain Policies
 - Application Rules
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules
 - End Point Policy Groups
 - Session Policies
- TLS Management
- Device Specific Settings
 - Network Management**
 - Media Interface
 - Signaling Interface
 - End Point Flows
 - Session Flows
 - DMZ Services
 - TURN/STUN Service
 - SNMP
 - Syslog Management
 - Advanced Options
 - Troubleshooting

On the Interface Configuration tab, click the **Status** for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

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 Signaling Interface End Point Flows Session Flows DMZ Services TURN/STUN Service SNMP Syslog Management

Network Management: Avaya SBCE

Devices Avaya SBCE

Interfaces Networks

Add VLAN

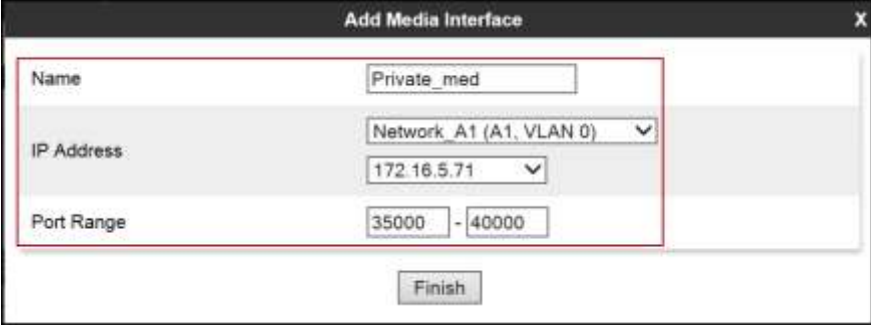
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

7.5.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, port range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. Below is the configuration of the inside, private Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name:** *Private_med*.
- Under **IP Address** select: *Network_A1 (A1, VLAN 0)*
Select **IP Address:** *172.16.5.71* (Private or A1 IP Address of the Avaya SBCE, toward Session Manager).
- Enter **Port Range:** *35000-40000*.
- Click **Finish**.

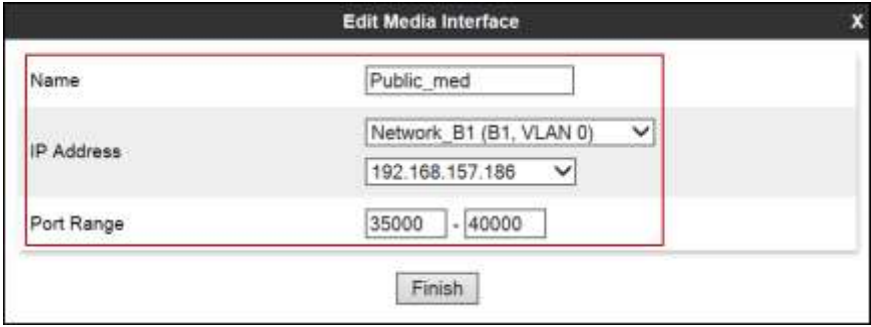


The screenshot shows a window titled "Add Media Interface" with a close button (X) in the top right corner. The window contains the following fields:

- Name:** A text box containing "Private_med".
- IP Address:** A dropdown menu showing "Network_A1 (A1, VLAN 0)". Below it, a text box contains "172.16.5.71".
- Port Range:** Two text boxes containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom center.

Below is the configuration of the outside, public Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name:** *Public_med*.
- Under **IP Address** select: *Network_B1 (B1, VLAN 0)*
Select **IP Address:** *10.10.157.186* (Public or B1 IP Address of the Avaya SBCE toward the Service Provider).
- **Port Range:** *35000-40000*.
- Click **Finish**.



The screenshot shows a window titled "Edit Media Interface" with a close button (X) in the top right corner. The window contains the following fields:

- Name:** A text box containing "Public_med".
- IP Address:** A dropdown menu showing "Network_B1 (B1, VLAN 0)". Below it, a text box contains "192.168.157.186".
- Port Range:** Two text boxes containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom center.

The following screen capture shows the newly created Media Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand navigation menu lists various system management options, with "Device Specific Settings" expanded and "Media Interface" selected. The main content area is titled "Media Interface: Avaya SBCE" and features a "Media Interface" tab. A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this is a table of configured media interfaces. The table has columns for Name, Media IP (Network), and Port Range, with Edit and Delete links for each entry. The visible entries are Private_med (172.16.5.71, 35000-40000) and Public_med (192.168.157.186, 35000-40000). There are also two partially visible entries for Private_med and Public_med with IP addresses 172.16.5.71 and 192.168.157.186 respectively.

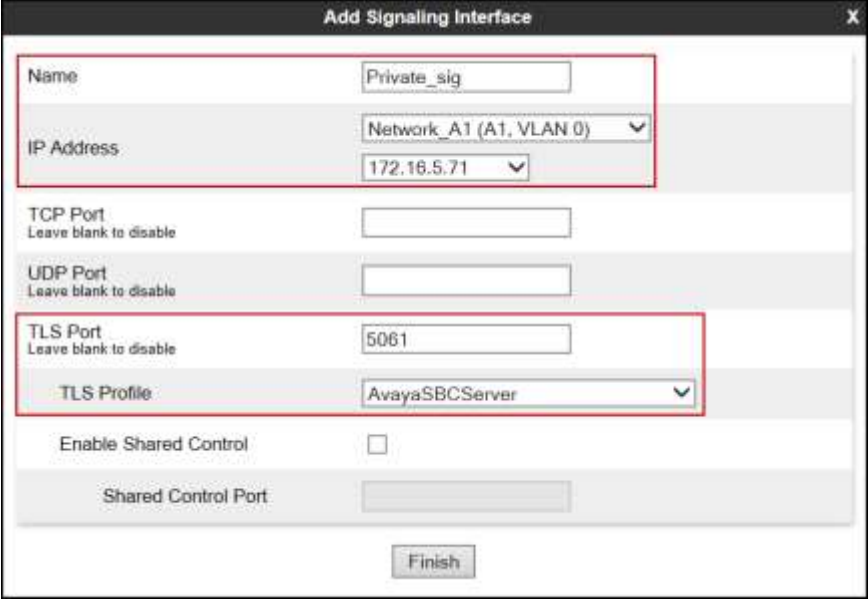
Name	Media IP Network	Port Range	Edit	Delete
Private_med	172.16.5.71 Network_A1 (A1, VLAN 2)	35000 - 40000	Edit	Delete
Private_med	172.16.5.71 Network_A1 (A1, VLAN 2)	35000 - 40000	Edit	Delete
Public_med	192.168.157.186 Network_B1 (B1, VLAN 2)	35000 - 40000	Edit	Delete

7.5.3. Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**.

Below is the configuration of the inside private Signaling Interface of the Avaya SBCE.

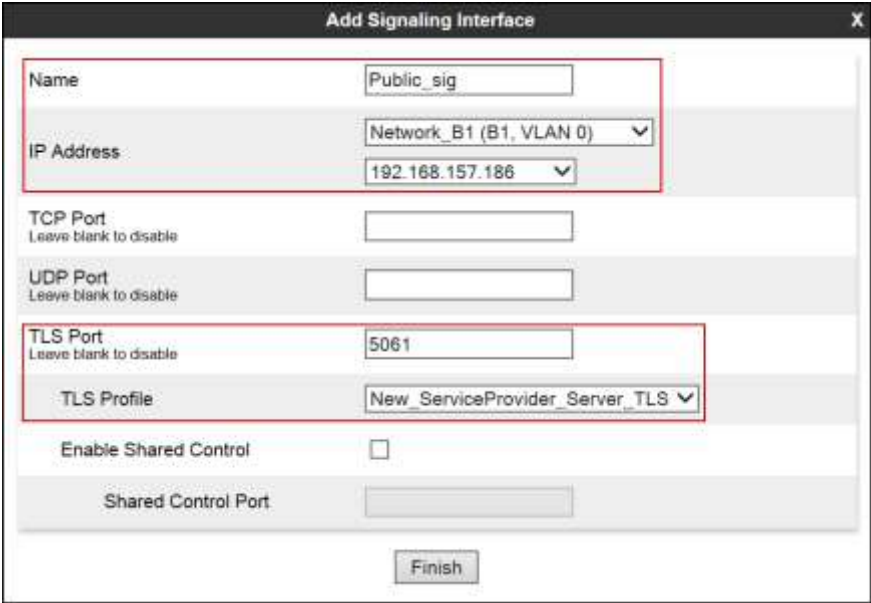
- Select **Add** in the **Signaling Interface** area.
- **Name:** *Private_sig*.
- Under **IP Address** select: *Network_A1 (A1, VLAN 0)*
Select **IP Address:** *172.16.5.71* (Inside or A1 IP Address of the Avaya SBCE, toward Session Manager).
- **TLS Port:** *5061*
- Under **TLS Profile** select: **AvayaSBCServer**
- Click **Finish**.



The screenshot shows a configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. The fields are organized into sections with alternating light and dark gray backgrounds. The first section (light gray) contains "Name" (text input: "Private_sig") and "IP Address" (dropdown menu: "Network_A1 (A1, VLAN 0)" with a sub-dropdown showing "172.16.5.71"). The second section (dark gray) contains "TCP Port" (text input, with "Leave blank to disable" below it) and "UDP Port" (text input, with "Leave blank to disable" below it). The third section (light gray) contains "TLS Port" (text input: "5061", with "Leave blank to disable" below it) and "TLS Profile" (dropdown menu: "AvayaSBCServer"). The fourth section (dark gray) contains "Enable Shared Control" (checkbox, unchecked) and "Shared Control Port" (text input). A "Finish" button is located at the bottom center.

Below is the configuration of the outside, public Signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area.
- **Name:** *Public_sig*.
- Under **IP Address** select: *Network_B1 (B1, VLAN 0)*
- Select **IP Address:** *10.10.157.186* (Public or B1 IP Address of the Avaya SBCE toward the Service Provider).
- **UDP Port:** *5061*.
- Under **TLS Profile** select: *New_ServiceProvider_Server_TLS*.
- Click **Finish**.



The screenshot shows a configuration window titled "Add Signaling Interface". The window contains several fields and a "Finish" button. The fields are organized into sections. The first section, highlighted with a red box, contains the "Name" field with the value "Public_sig", the "IP Address" dropdown menu with "Network_B1 (B1, VLAN 0)" selected, and the "IP Address" text field with the value "192.168.157.186". The second section contains the "TCP Port" field with the text "Leave blank to disable" below it. The third section contains the "UDP Port" field with the text "Leave blank to disable" below it. The fourth section, also highlighted with a red box, contains the "TLS Port" field with the value "5061" and the text "Leave blank to disable" below it. The fifth section contains the "TLS Profile" dropdown menu with "New_ServiceProvider_Server_TLS" selected. The sixth section contains the "Enable Shared Control" checkbox, which is unchecked. The seventh section contains the "Shared Control Port" field. The "Finish" button is located at the bottom right of the window.

Name	Public_sig
IP Address	Network_B1 (B1, VLAN 0) ▼
	192.168.157.186 ▼
TCP Port	
Leave blank to disable	
UDP Port	
Leave blank to disable	
TLS Port	5061
Leave blank to disable	
TLS Profile	New_ServiceProvider_Server_TLS ▼
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	
Finish	

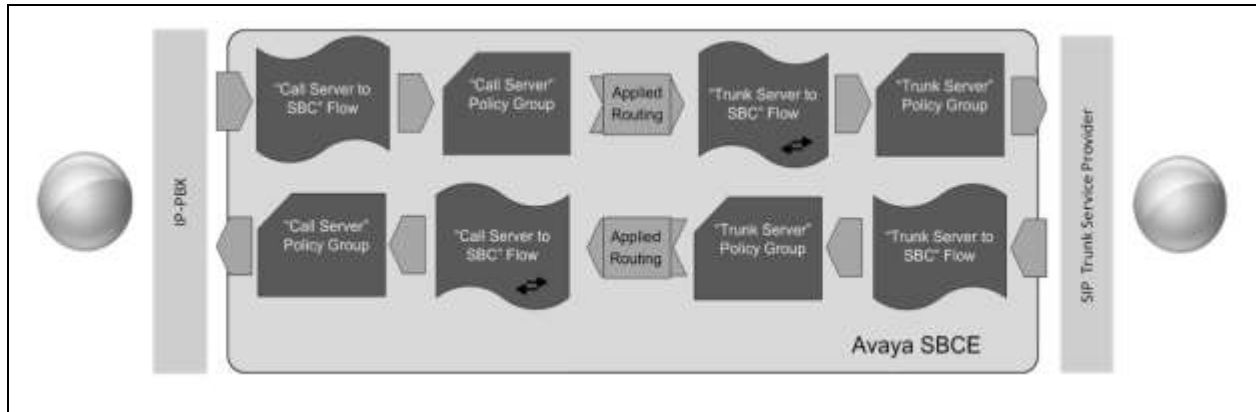
The following screen capture shows the newly created Signaling Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Device Specific Settings' and its sub-item 'Signaling Interface' highlighted. The main content area is titled 'Signaling Interface: Avaya SBCE' and features a sub-tab 'Signaling Interface'. A warning message states: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table of signaling interfaces. The table has columns for Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, and TLS Profile. Two interfaces are listed: 'Private_sig' and 'Public_sig'. The 'Public_sig' row is highlighted with a red box. Each row includes 'Edit' and 'Delete' links. An 'Add' button is located at the top right of the table area.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.5.1 Network_A1 (A1, VLAN 0)	---	---	5061	AvayaSBCServer	Edit Delete
Public_sig	10.10.157.188 Network_B1 (B1, VLAN 0)	---	---	5061	New_ServiceProvider_Server_TLS	Edit Delete
...	Edit Delete
...	Edit Delete

7.5.4. End Point Flows

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



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, and then the **Server Flows** tab. Click **Add** (not shown).

- **Flow Name:** *SIP_Trunk_Flow_TLS*.
- **Server Configuration:** *Service Provider TLS*.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** *Private_sig*.
- **Signaling Interface:** *Public_sig*.
- **Media Interface:** *Public_med*.
- **End Point Policy Group:** *ServiceProvider_SRTP*.
- **Routing Profile:** *Route_to_SM* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Service_Provider*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.

The screenshot shows a configuration window titled "Edit Flow: SIP_Trunk_Flow_TLS". It contains the following fields and values:

Field	Value
Flow Name	SIP_Trunk_Flow_TLS
Server Configuration	Service Provider TLS
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
End Point Policy Group	ServiceProvider_SRTP
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

A "Finish" button is located at the bottom right of the configuration area.

To create the call flow toward the Session Manager, click **Add**.

- **Flow Name:** *Session_Manager_Flow*.
- **Server Configuration:** *Session Manager*.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** *Public_sig*.
- **Signaling Interface:** *Private_sig*.
- **Media Interface:** *Private_med*.
- **End Point Policy Group:** *SM_SRTP*
- **Routing Profile:** *Route_to_SP_TLS* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Session_Manager*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.

Flow Name: Session_Manager_Flow

Server Configuration: Session Manager

URI Group: *

Transport: *

Remote Subnet: *

Received Interface: Public_sig

Signaling Interface: Private_sig

Media Interface: Private_med

End Point Policy Group: SM_SRTP

Routing Profile: Route_to_SP_TLS

Topology Hiding Profile: Session_Manager

Signaling Manipulation Script: None

Remote Branch Office: Any

Finish

The following screen capture shows the newly created **End Point Flows**.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

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
Syslog Management
Advanced Options
Troubleshooting

End Point Flows: Avaya SBCE

Devices: Avaya SBCE

Subscriber Flows Server Flows

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	SIP_Trunk_Flow	*	Private_sig	Public_sig	Service Provider	Route_to_SM

Server Configuration: Service Provider TLS

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	SIP_Trunk_Flow_TLS	*	Private_sig	Public_sig	ServiceProvider_SRTP	Route_to_SM

Server Configuration: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	Session_Manager_Flow	*	Public_sig	Private_sig	SM_SRTP	Route_to_SP_TLS
2	SM from Ram Workers	*	RW_Public_sig	RW_Private_sig	Rem Workers SRTP	To SM from Rem W

8. Clearcom SIP Trunking Service Configuration

To use Clearcom's SIP Trunking Service, a customer must request the service from Clearcom using the established sales processes. The process can be started by contacting Clearcom via the corporate web site at: <http://www.clearcom.mx/> and requesting information.

During the signup process, Clearcom and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Clearcom's network.

Clearcom is responsible for the configuration of Clearcom SIP Services. The customer will need to provide a public IP address to be used to reach the Avaya SBCE at the enterprise. In the case of the compliance test, this is the outside or public IP address of the Avaya SBCE (B1 interface). The customer will also need the IP addresses for the primary and the secondary public DNS servers, these addresses can be obtained from the local ISP in Mexico.

Clearcom will provide the following information:

- SIP Trunk registration credentials (user name, password, SIP domain).
- Fully Qualified Domain Name of the Clearcom SIP proxy server.
- DID numbers.
- Supported codecs and order of preference.
- Any IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

9. Verification and Troubleshooting

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 with two-way audio for more than 35 seconds.
3. Verify that the 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.

9.1. Troubleshooting

9.1.1. Communication Manager

- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Traces calls over a specific trunk group.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group number>
Displays trunk group service state.
- **status station** <extension number>
Displays signaling and media information for an active call on a specific station.

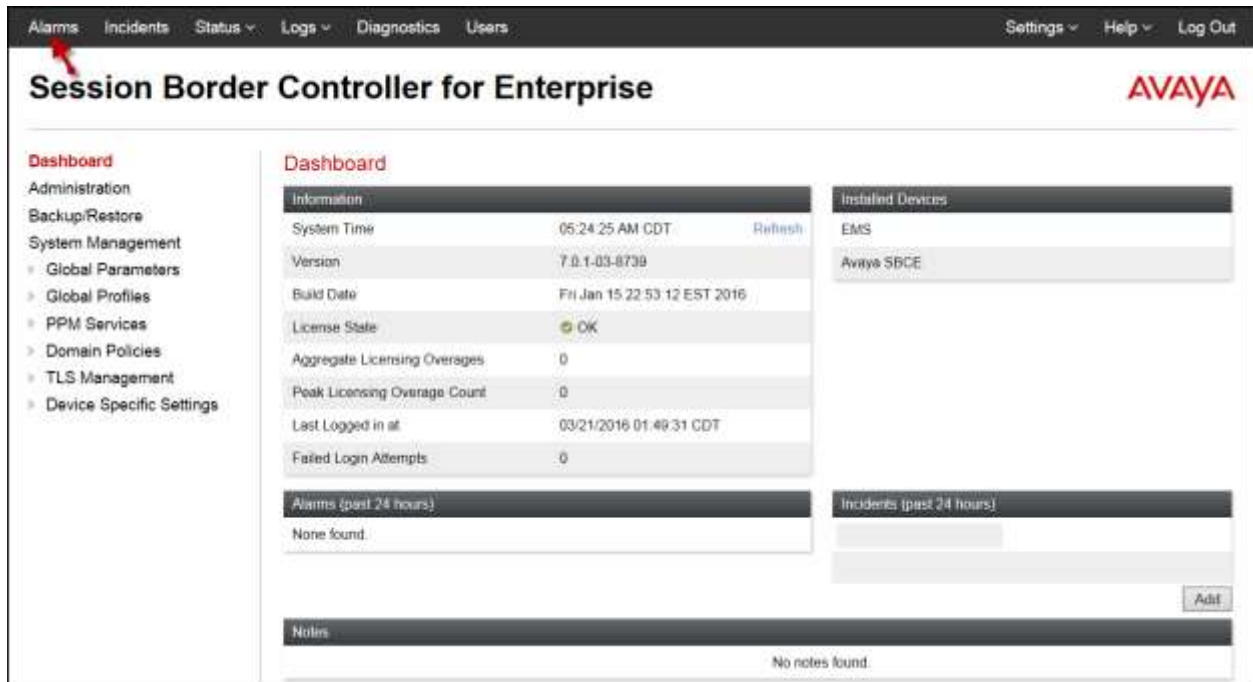
9.1.2. Session Manager

- **traceSM -x** – Session Manager command line tool for traffic analysis. Login to the Session Manager management CLI interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Home → Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

9.1.3. Avaya Session Border Controller for Enterprise (Avaya SBCE)

There are several links and menus located on the taskbar at the top of the screen of the web interface that can be used for diagnostic and troubleshooting.

Alarms: Provides information about the health of the Avaya SBCE.



The following screen shows the **Alarm Viewer** page.



Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.

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

Information

System Time	05:24:25 AM CDT	Refresh
Version	7.0.1-03-0739	
Build Date	Fri Jan 15 22:53:12 EST 2016	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	03/21/2016 01:48:31 CDT	
Failed Login Attempts	0	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Add

Notes
No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

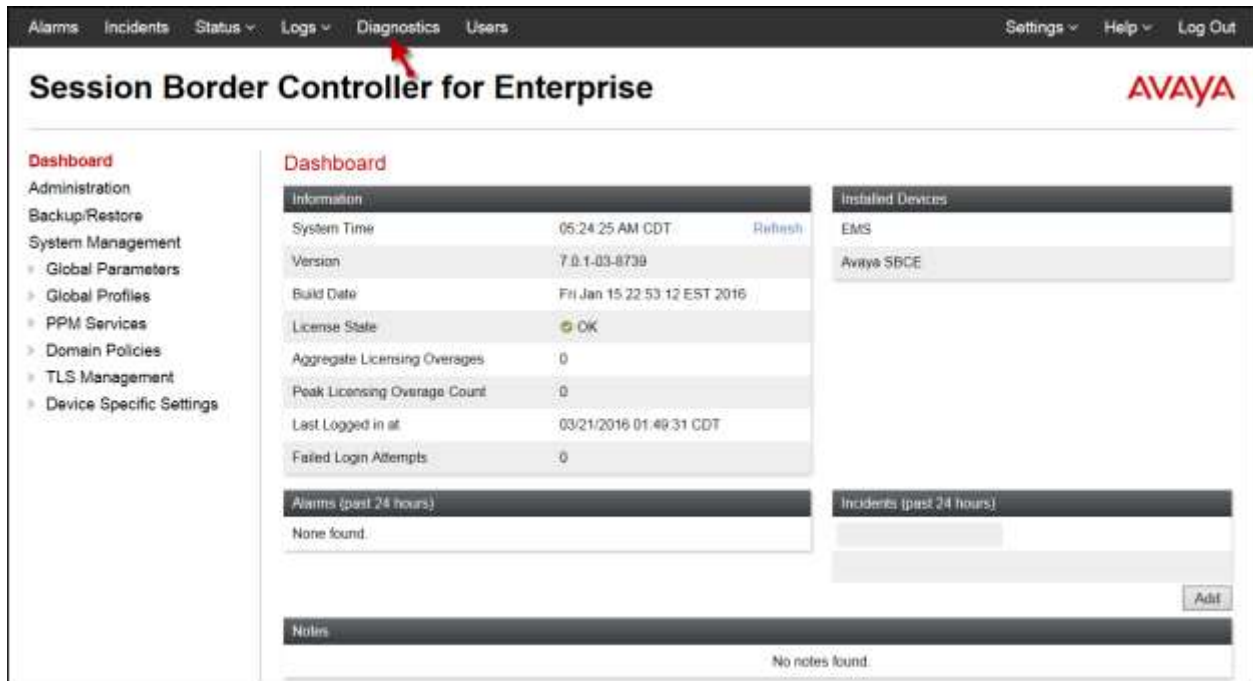
Device: All Category: All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 2002.

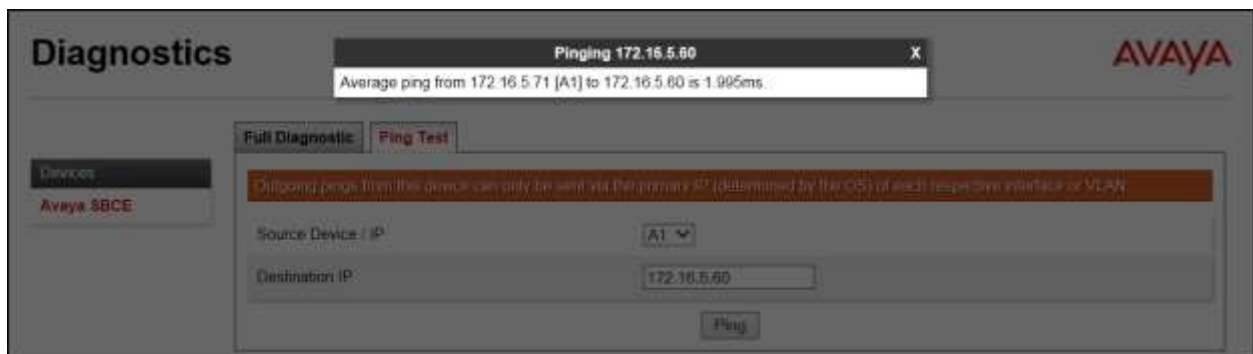
Type	ID	Date	Time	Category	Device	Cause
Routing Failure	729364126400041	3/23/16	5:17 AM	Policy	Avaya SBCE	Max forwards Exceeded
Routing Failure	729364096481672	3/23/16	5:16 AM	Policy	Avaya SBCE	Max forwards Exceeded

<< < 1 2 3 4 5 > >>

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



The following screen shows the Diagnostics page with the results of a ping test.

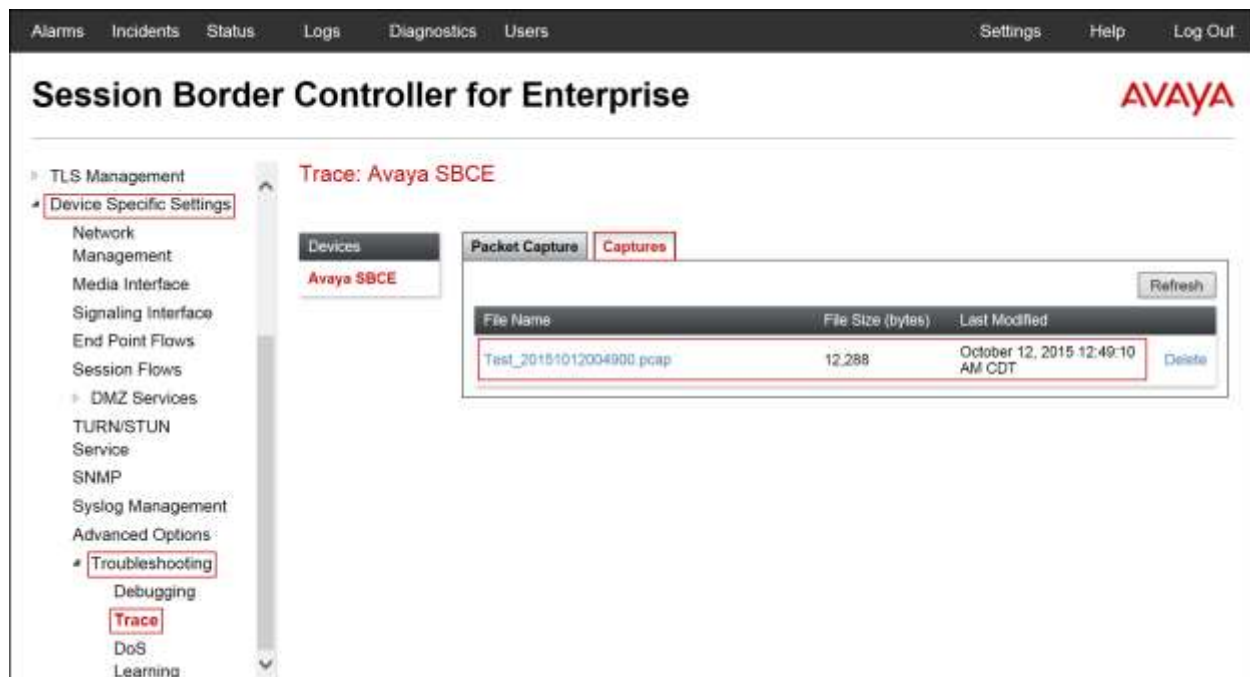


Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web management interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. On the left sidebar, the "Device Specific Settings" menu is expanded, showing options like Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, and Advanced Options. Under "Advanced Options", the "Troubleshooting" section is selected, and the "Trace" option is highlighted. The main content area is titled "Trace: Avaya SBCE" and contains two tabs: "Packet Capture" (active) and "Captures". The "Packet Capture Configuration" form is visible, with fields for Status (Ready), Interface (A1), Local Address (IP:Port) (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Test.pcap). A red box highlights the configuration fields. At the bottom of the form are "Start Capture" and "Clear" buttons.

Packet Capture Configuration	
Status	Ready
Interface	A1
Local Address (IP:Port)	All
Remote Address (*, *Port, IP, IP-Port)	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename (Using the name of an existing capture will overwrite it)	Test.pcap

Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



9.2. TraceSBC Tool

traceSBC is a perl script that parses Avaya SBCE log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, the tool can easily be used in case of TLS and HTTPS. traceSBC can parse the log files downloaded from Avaya SBCE. traceSBC can also process log files in real time on Avaya SBCE, so that IP and PPM traffic can be checked during live calls. Refer to items [8] in **Section 11**

Operation modes:

- **Non real-time mode:**

The tool starts with at least one file in the command line parameters. The tool automatically detects the type of files, processes the files, and finally displays messages from the different files in one diagram ordered by the timestamp. If filters are set, only the messages that match the filters are displayed in the diagram. In this mode, enabling live capture is not an option.

Example: # traceSBC tracesbc_sip_1408635251

- **Real-time mode**

In this mode, traceSBC must be on active Avaya SBCE. traceSBC is started without specifying a file in the command line parameters. The tool automatically starts processing the log files. The live capture can be started and stopped anytime without affecting service.

Example: # traceSBC

Log Files:

Avaya SBCE can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files real-time by opening the latest log files in the given directories. TraceSBC also checks regularly if a new file is generated, in which case the old one is closed and processing continues with the new one. A new log file is generated every time the relevant processes restart, or when the size reaches the limit of ~10 Megabytes.

Log Locations:

SIP messages are found at /archive/log/tracesbc/tracesbc_sip/ and PPM messages can be found at /archive/log/tracesbc/tracesbc_ppm/.

Active files are of the following format:

```
-rw-rw---- 1 root root 112445 Aug 21 10:12 tracesbc_sip_1408631651
```

Inactive or closed files are of the following format:

```
-rw-rw---- 1 root root 175236 Aug 21 06:33 tracesbc_sip_1408617250_1408620820_1
```

or

```
-rw-rw---- 1 root root 31706 Jul 10 13:34 tracesbc_sip_1436549674_1436553270_1.gz
```

10. Conclusion

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Aura® Communication Manager Release 7.0, Avaya Aura® Session Manager Release 7.0, and Avaya Session Border Controller for Enterprise Release 7.0 to support Clearcom SIP Trunking Service using TLS, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

11.References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya Aura® Communication Manager, including the following, is available at: <http://support.avaya.com/>

- [1] *Administering Avaya Aura® Communication Manager*, Release 7.0, August 2015, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, August 2015, Document Number 555-245-205.
- [3] *Avaya Aura® Communication Manager Security Design, Release 6.3*, Issue 6, June 2015, Document Number 03-601973.

Product documentation for Avaya Aura® System Manager, including the following, is available at: <http://support.avaya.com/>

- [4] *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0, Issue 1, August 2015.
- [5] *Avaya Aura® System Manager Release 7.0 Security Guide*, Release 7.0, Issue 1, August 2015

Product documentation for Avaya Aura® Session Manager, including the following, is available at: <http://support.avaya.com/>

- [6] *Administering Avaya Aura® Session Manager*, Release 7.0, August 2015.

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: <http://support.avaya.com/>

- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.

Product documentation for Avaya Aura® Media Server, is available at: <http://support.avaya.com/>

- [9] *Implementing and Administering Avaya Aura® Media Server*. Release 7.7. August 2015.
- [10] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager. White Paper*. August 2015.

Other resources:

- [11] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [12] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

12. Appendix A: SigMa Script

Following is the Signaling Manipulation script that was used in the configuration of the Avaya SBCE, **Section 7.3.3**. When adding this script as instructed in **Section 7.3.4** enter a name for the script in the Title (e.g., **Clearcom_Script**) and copy/paste the entire script. Note that the user name, shown below as “User123”, will need to be changed with the correct user name provided by Clearcom for registration purpose.

Title: Clearcom_Script

```
//Replace Username in "REQUEST-LINE" with "TO" number on Inbound
within session "ALL"
{
act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
{
%HEADERS["Request_Line"][1].URI.USER = %HEADERS["To"][1].URI.USER;
}
}

//Insert Username in the FROM header on Outbound
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%fromuser = %HEADERS["From"][1].URI.USER;
%HEADERS["From"][1].URI.USER = "User123";
}
}

//Remove gsid and epv parameters in outbound Contact header
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
}
}
```


©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.