



Application Notes for Configuring Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 to support Clearcom SIP Trunking Service using TLS – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service on an enterprise solution consisting of Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1 to interoperate with Clearcom SIP Trunking service using Transport Layer Security (TLS). These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

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.

The Clearcom SIP Trunking service provides customers with PSTN access via a SIP trunk between the enterprise and the Clearcom network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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.....	5
2.2.	Test Results	6
2.3.	Support	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	11
5.	Configure Avaya Aura® Communication Manager	12
5.1.	Licensing and Capacity	12
5.2.	System Features.....	13
5.3.	IP Node Names.....	15
5.4.	Codecs	16
5.5.	IP Network Regions	18
5.6.	Signaling Group	19
5.7.	Trunk Group.....	21
5.8.	Calling Party Information.....	25
5.9.	Inbound Routing.....	26
5.10.	Outbound Routing	27
6.	Configure Avaya Aura® Session Manager	32
6.1.	System Manager Login and Navigation.....	33
6.2.	SIP Domain	35
6.3.	Locations	36
6.4.	Adaptations.....	39
6.5.	SIP Entities.....	41
6.6.	Entity Links	44
6.7.	Routing Policies	46
6.8.	Dial Patterns	47
7.	Configure Avaya Session Border Controller for Enterprise	50
7.1.	System Access.....	50
7.2.	Device Management.....	53
7.3.	TLS Management.....	56
7.3.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	56
7.3.2.	Server Profiles.....	58
7.3.3.	Client Profiles	62
7.4.	Network Management.....	67
7.5.	Media Interfaces	68
7.6.	Signaling Interfaces.....	70
7.7.	Server Interworking.....	72
7.7.1.	Server Interworking Profile – Enterprise.....	72
7.7.2.	Server Interworking Profile – Service Provider.....	76
7.8.	Signaling Manipulation.....	79
7.9.	Server Configuration.....	80
7.9.1.	Server Configuration Profile – Enterprise	80
7.9.2.	Server Configuration Profile – Service Provider	82

7.10.	Routing	86
7.10.1.	Routing Profile – Enterprise.....	86
7.10.2.	Routing Profile – Service Provider	87
7.11.	Topology Hiding.....	88
7.11.1.	Topology Hiding Profile – Enterprise.....	88
7.11.2.	Topology Hiding Profile – Service Provider.....	90
7.12.	Domain Policies.....	91
7.12.1.	Application Rules	91
7.12.2.	Media Rules.....	93
7.12.3.	Signaling Rules	97
7.13.	End Point Policy Groups	98
7.13.1.	End Point Policy Group – Enterprise	98
7.13.2.	End Point Policy Group – Service Provider.....	99
7.14.	End Point Flows.....	100
7.14.1.	End Point Flow – SP to SM Flow	101
7.14.2.	End Point Flow – SM to SP Flow	102
8.	Clearcom SIP Trunking Service Configuration.....	103
9.	Verification and Troubleshooting	103
9.1.	General Verification Steps	103
9.2.	Communication Manager Verification.....	103
9.3.	Session Manager Verification	104
9.4.	Avaya SBCE Verification	107
10.	Conclusion	113
11.	References.....	113
12.	Appendix A – SigMa Scripts	114

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking Service between the Clearcom network and an Avaya SIP-enabled enterprise solution using Transport Layer Security (TLS). The Avaya solution consists of Avaya Aura® Communication Manager 10.1 (Communication Manager), Avaya Aura® Session Manager 10.1 (Session Manager), Avaya Session Border Controller for Enterprise 10.1 (Avaya SBCE) and various Avaya endpoints, listed in **Section 4**.

The Clearcom SIP Trunking service referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

The terms “Service Provider” or “Clearcom” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the network via a broadband connection to the public Internet.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products (private network side) and between the simulated enterprise and Clearcom (public network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

2.1. Interoperability Compliance Testing

To verify SIP trunk interoperability, the following features and functionality were covered during the interoperability compliance test:

- 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 J129 IP Deskphones (SIP), Avaya J179 IP Deskphones (H.323), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Workplace client for Windows (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya Workplace client for Windows (SIP).
- Outgoing calls to the PSTN were routed via Clearcom 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.729, G.711A and G.711MU.
- No matching codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833:
 - Outbound call to PSTN application requiring DTMF (e.g., an IVR or voice mail system).
 - Inbound call from PSTN to Avaya CPE application requiring DTMF (e.g., Aura® Messaging, Avaya vector digit collection steps).
- 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.
- Routing inbound vector call to call center agent queues.
- 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. Consult reference [9] in the **References** section for additional information on this topic.

The following items were not tested:

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

2.2. Test Results

Interoperability testing of the Clearcom SIP Trunking Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **SIP REFER method:** PSTN calls that were transferred back to the network using the SIP REFER method did not work properly. The REFER message was not accepted by Clearcom with a “202” message, with Clearcom eventually sending a BYE message. 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 trunk channels remained busy/connected for the entire duration of the call.
- **Fax support:** Fax calls using the T.38 protocol failed during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay. The issue related to T.38 fax calls failing is related to the PSTN carriers used by Clearcom in Mexico to route calls to the PSTN, not all PSTN carriers used by Clearcom in Mexico support T.38. This issue could be resolved by Clearcom selecting specific PSTN carriers that do support T.38 and routing T.38 fax traffic via these PSTN carriers.
- **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 main DID number (pilot number) assigned to the trunk was displayed, instead of “anonymous”.
- **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 calls that were 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 main DID number (pilot number) assigned to the trunk, 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 main DID number

(pilot number) assigned to the trunk, regardless of the PSTN number being used to originate the call.

- **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. (refer to **Sections 7.8** and **Appendix A**).
- **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, refer to **Section 7.8** and **Appendix A**.
- **SIP OPTION Messages:** During the compliance test Clearcom did not send SIP OPTION messages to Avaya, Session Manager did send SIP OPTION messages to Clearcom, this was sufficient to keep the SIP trunk up in-service.
- **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, refer to **Section 7.8** and **Appendix A**.

2.3. Support

For support of Clearcom SIP Trunking Service visit the corporate Web page at:

<http://www.clearcom.mx/>

For technical support on the Avaya products described in these Application Notes visit

<http://support.avaya.com>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Clearcom SIP Trunking Service through a public Internet WAN connection.

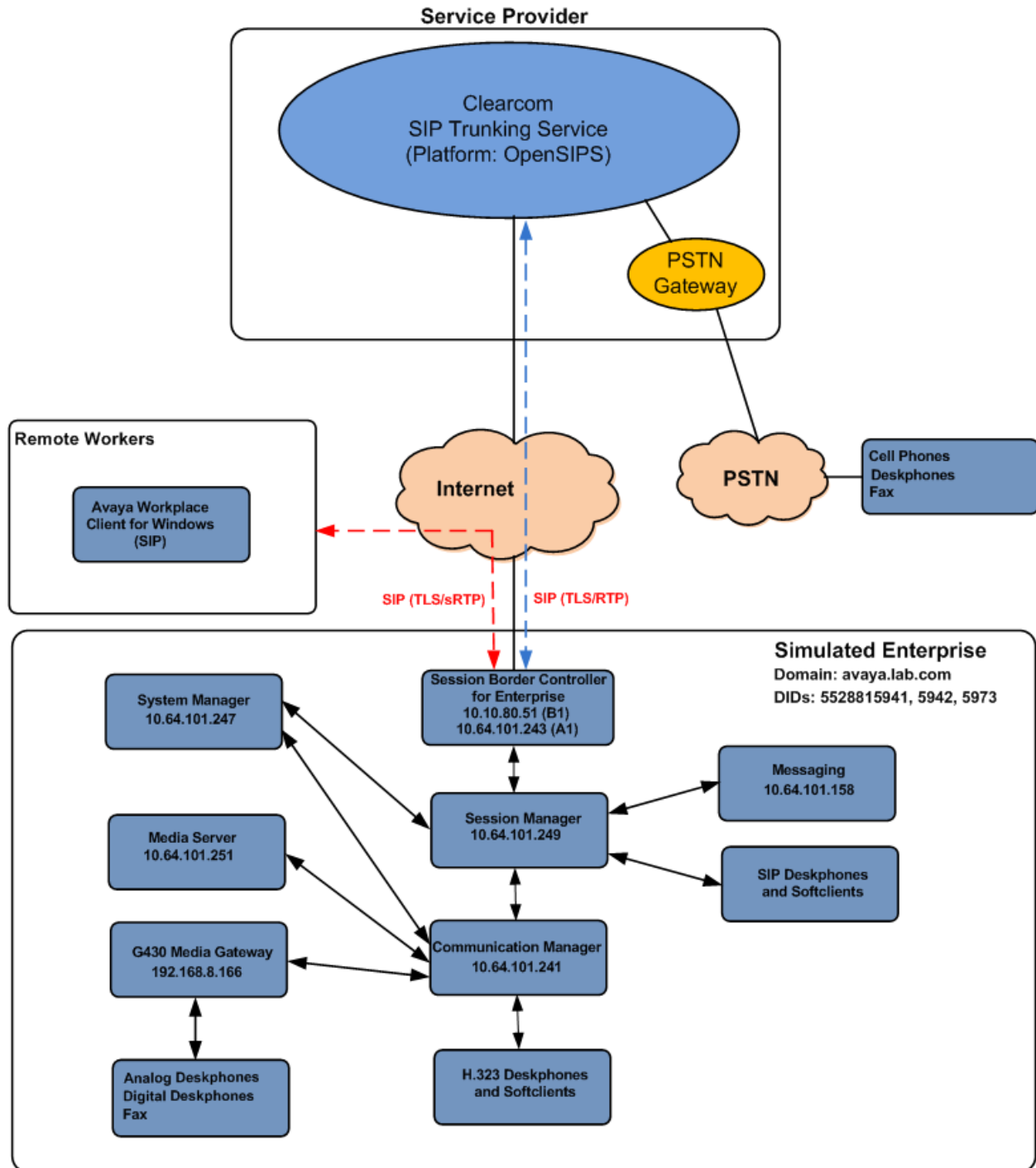


Figure 1: Avaya SIP Enterprise Solution connected to Clearcom SIP Trunking Service

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Messaging
- Avaya Aura® Media Server.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya J179 IP Deskphones (H.323).
- Avaya J129 IP Deskphones (SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Workplace Client for Windows softphone (SIP).
- Avaya Agent for Desktop (SIP).
- Avaya digital and analog telephones.
- Ventafax fax software.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya Workplace Client for Windows (SIP). Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult reference [9] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

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 (or regular expressions) and routing policies to determine the recipient (Communication Manager) and on which link to send the call.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection 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 (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Clearcom network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

Communication Manager incorporates the ability to use the Avaya Aura® Media Server (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G430 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the **References** section.

The Avaya Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Avaya Messaging are not directly related to the interoperability tests with the Clearcom network SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	10.1.0.0.0 Service Pack 0.1 (01.0.974.0-27293)
Avaya Aura® Session Manager	10.1.0.0 (10.1.0.0.1010019)
Avaya Aura® System Manager	10.1.0.0 Build No. 10.1.0.0.537353 Software Update Rev. No. 10.1.0.0.0614119
Avaya Session Border Controller for Enterprise	ASBCE 10.1 10.1.0.0-32-21432
Avaya Messaging	10.8 Service Pack 1 (IXM-10.8.20.1406)
Avaya Aura® Media Server	8.0.2.218_2022.01.05
Avaya G430 Media Gateway	g430_sw_42.4.0
Avaya 100 Series IP Deskphones (SIP)	Version 4.0.7.0.7
Avaya J179 IP Deskphones (H.323)	Version 6.8402
Avaya one-X® Communicator (H.323, SIP)	6.2.14.15-SP14-Patch7
Avaya Workplace Client for Windows (SIP)	3.25.0.73
Avaya Agent for Desktop (Windows) (SIP)	2.0.6.19.3004
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
Clearcom	
OpenSIPS Softswitch	2.6.2
OpenSIPS Session Border Controller	2.6.2

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

Note – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.7.0) platforms. Consult the installation documentation on the **References** section for more information.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the Clearcom SIP Trunking Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and the Avaya Media Server has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens capture 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-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **40000** licenses are available and **220** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	1
Maximum Administered Remote Office Trunks:	12000	0
Max Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Reg Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	0
Maximum Video Capable IP Softphones:	18000	6
Maximum Administered SIP Trunks:	40000	220
Max Administered Ad-hoc Video Conferencing Ports:	24000	0
Max Number of DS1 Boards with Echo Cancellation:	999	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. System Features

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

```
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 Communication Manager (**procr**) and the Session Manager security module (**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	10.64.101.243	
SM	10.64.101.249	
default	0.0.0.0	
media_server	10.64.101.251	
procr	10.64.101.241	
procr6	::	
(6 of 6 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

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. Enter the corresponding codec in the **Audio Codec** column of the table. Clearcom supports audio codecs **G.729**, **G.711A** and **G.711MU**.

change ip-codec-set 2 Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1:	<u>G.729</u>	<u>n</u>	<u>2</u>	20
2:	<u>G.711A</u>	<u>n</u>	<u>2</u>	20
3:	<u>G.711MU</u>	<u>n</u>	<u>2</u>	20
4:	<u></u>	<u>-</u>	<u>-</u>	
5:	<u></u>	<u>-</u>	<u>-</u>	
6:	<u></u>	<u>-</u>	<u>-</u>	
7:	<u></u>	<u>-</u>	<u>-</u>	

Media Encryption

1: 1-srtp-aescm128-hmac80

2: none

3:

4:

5:

Encrypted SRTP: best-effort

On **Page 2**, set the **Fax Mode** to **off** (refer to **Section 2.2**).

change ip-codec-set 2

Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

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

Media Connection IP Address Type Preferences

1: IPv4

2: _____

5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. 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** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes**, the default setting. This will 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 and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2	NR Group: 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	
UDP Port Min: 2048	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 3349	IP Audio Hairpinning? n	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
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 (the rest of the enterprise). 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 following example 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 rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Prio Shr	Intervening Regions	Dyn CAC	A R	G L						
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 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 and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, **tls** was used.
- 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 is a Session Manager.

Note: Once the **Peer-Server** field is updated to **SM**, the system changes the default values of the following fields, setting them to display-only:

- Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? is changed to y.
- Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? is changed to n.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). 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 **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to y.
- 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? <u>n</u>	Transport Method: <u>tls</u>	
Q-SIP? <u>n</u>		
IP Video? <u>n</u>	Enforce SIPS URI for SRTP? <u>y</u>	
Peer Detection Enabled? <u>y</u>	Peer Server: SM	Clustered? <u>n</u>
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? <u>y</u>		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? <u>n</u>		
Alert Incoming SIP Crisis Calls? <u>n</u>		
Near-end Node Name: <u>procr</u>	Far-end Node Name: <u>SM</u>	
Near-end Listen Port: <u>5071</u>	Far-end Listen Port: <u>5071</u>	
	Far-end Network Region: <u>2</u>	
Far-end Domain: <u>avaya.lab.com</u>		
Incoming Dialog Loopbacks: <u>eliminate</u>		Bypass If IP Threshold Exceeded? <u>n</u>
DTMF over IP: <u>rtp-payload</u>		RFC 3389 Comfort Noise? <u>n</u>
Session Establishment Timer(min): <u>3</u>	Direct IP-IP Audio Connections? <u>y</u>	
Enable Layer 3 Test? <u>n</u>	IP Audio Hairpinning? <u>n</u>	
H.323 Station Outgoing Direct Media? <u>n</u>	Initial IP-IP Direct Media? <u>n</u>	
	Alternate Route Timer(sec): <u>6</u>	

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 4 ^
                                     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** 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. The default value of **600** seconds was used.

change trunk-group 2 Page 2 of 4

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 **public**. This field specifies the format of the calling party number (CPN) sent to the far-end. When **public** format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. The **Numbering Format** was set to **public** and the **Numbering Format** in the route pattern was set to **pub-unk** (see **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 has enabled CPN block.

change trunk-group 2 Page 3 of 4

TRUNK FEATURES

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

On **Page 4**:

- Set the **Network Call Redirection** field to **n**. With this setting, Communication Manager will not use the SIP REFER method for the redirection of PSTN calls that are transferred back to the SIP trunk (refer to **Section 2.2**).
- Set the **Send Diversion Header** field to **n** and **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101**, the value preferred by Clearcom.
- Verify that **Identity for Calling Party Display** is set to **P-Asserted-Identity**.
- Default values were used for all other fields.

change trunk-group 2 Page 4 of 4

PROTOCOL VARIATIONS

Mark Users as Phone? n

Prepend '+' to Calling/Alerting/Diverting/Connected Number? n

Send Transferring Party Information? n

Network Call Redirection? n

Send Diversion Header? n

Support Request History? n

Telephone Event Payload Type: 101

Convert 180 to 183 for Early Media? n

Always Use re-INVITE for Display Updates? n

Resend Display UPDATE Once on Receipt of 481 Response? n

Identity for Calling Party Display: P-Asserted-Identity

Block Sending Calling Party Location in INVITE? n

Accept Redirect to Blank User Destination? n

Enable Q-SIP? n

Interworking of ISDN Clearing with In-Band Tones: keep-channel-active

Request URI Contents: may-have-extra-digits

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, two DID numbers assigned by the service provider are shown. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions. The country code for Mexico (52) may not be required for local calls within Mexico (only required for international dialing).

```

change public-unknown-numbering 1
                                NUMBERING - PUBLIC/UNKNOWN FORMAT
                                Total
Ext  Ext      Trk      CPN      CPN
Len  Code      Grp(s)   Prefix   Len
-----
4    3          _____ 4
4    5          _____ 4
4    3041       2      525528815941 12
4    3044       2      525528815942 12
Note: If an entry applies to
a SIP connection to Avaya
Aura(R) Session Manager,
the resulting number must
be a complete E.164 number.
Communication Manager
automatically inserts
a '+' digit in this case.

```

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. Use the **change inc-call-handling-trmt** command to create an entry for each DID. The country code for Mexico (52) may not be required for local calls within Mexico (only required for international dialing).

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	12	525528815941	12	3041			
public-ntwrk	12	525528815942	12	3044			
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							
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							
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							
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							
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							
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							
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							
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							
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							
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							
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			Page 1 of 12					
DIAL PLAN ANALYSIS TABLE								
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 11
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:	_____	
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. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2, which contains the SIP trunk group to the service provider.

For international call to the U.S. (e.g., dialing: 90017863311234):

change ars analysis 001						
ARS DIGIT ANALYSIS TABLE						
Location: all						
Percent Full: 1						
Dialed String	Total		Route	Call	Node	ANI
	Min	Max	Pattern	Type	Num	Reqd
001	13	18	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
10xxx01	14	22	deny	iop	—	n
10xxx011	15	23	deny	intl	—	n
10xxx1	16	16	deny	fnpa	—	n

For local calls within Mexico (e.g., dialing: 928815943):

change ars analysis 2

Page 1 of 2

ARS DIGIT ANALYSIS TABLE

Location: all

Percent Full: 1

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
2	8	8	2	hnpa		n
3	7	7	1	hnpa		n
4	7	7	1	hnpa		n
407	10	10	2	hnpa		n
411	3	3	2	svcl		n
443	10	10	2	hnpa		n
5	7	7	2	hnpa		n
5005	4	4	2	locl		n
5006	4	4	2	locl		n
5007	4	4	2	locl		n
5008	4	4	2	locl		n
555	7	7	deny	hnpa		n
6	7	7	2	hnpa		n
611	3	3	2	svcl		n
61293	11	11	2	hnpa		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 in the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **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 **pub-unk**. All calls using this route pattern will use the public 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 4

Pattern Number: 2
Pattern Name: Serv. Provider

SCCAN? n
Secure SIP? n
Used for SIP stations? n

Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC
			Mrk	Lmt	List	Del	Digits	QSIG	
								Intw	
1:	<u>2</u>	<u>0</u>						<u>n</u>	<u>user</u>
2:								<u>n</u>	<u>user</u>
3:								<u>n</u>	<u>user</u>
4:								<u>n</u>	<u>user</u>
5:								<u>n</u>	<u>user</u>
6:								<u>n</u>	<u>user</u>

	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	Sub	Numbering	LAR	
	0	1	2	M	4	W	Request		Dgts	Format		
1:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>			<u>rest</u>		<u>pub-unk</u>	<u>none</u>
2:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>			<u>rest</u>			<u>none</u>
3:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>			<u>rest</u>			<u>none</u>
4:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>			<u>rest</u>			<u>none</u>
5:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>			<u>rest</u>			<u>none</u>
6:	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>Y</u>	<u>n</u>			<u>rest</u>			<u>none</u>

Note - Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.

6. Configure Avaya Aura® Session Manager

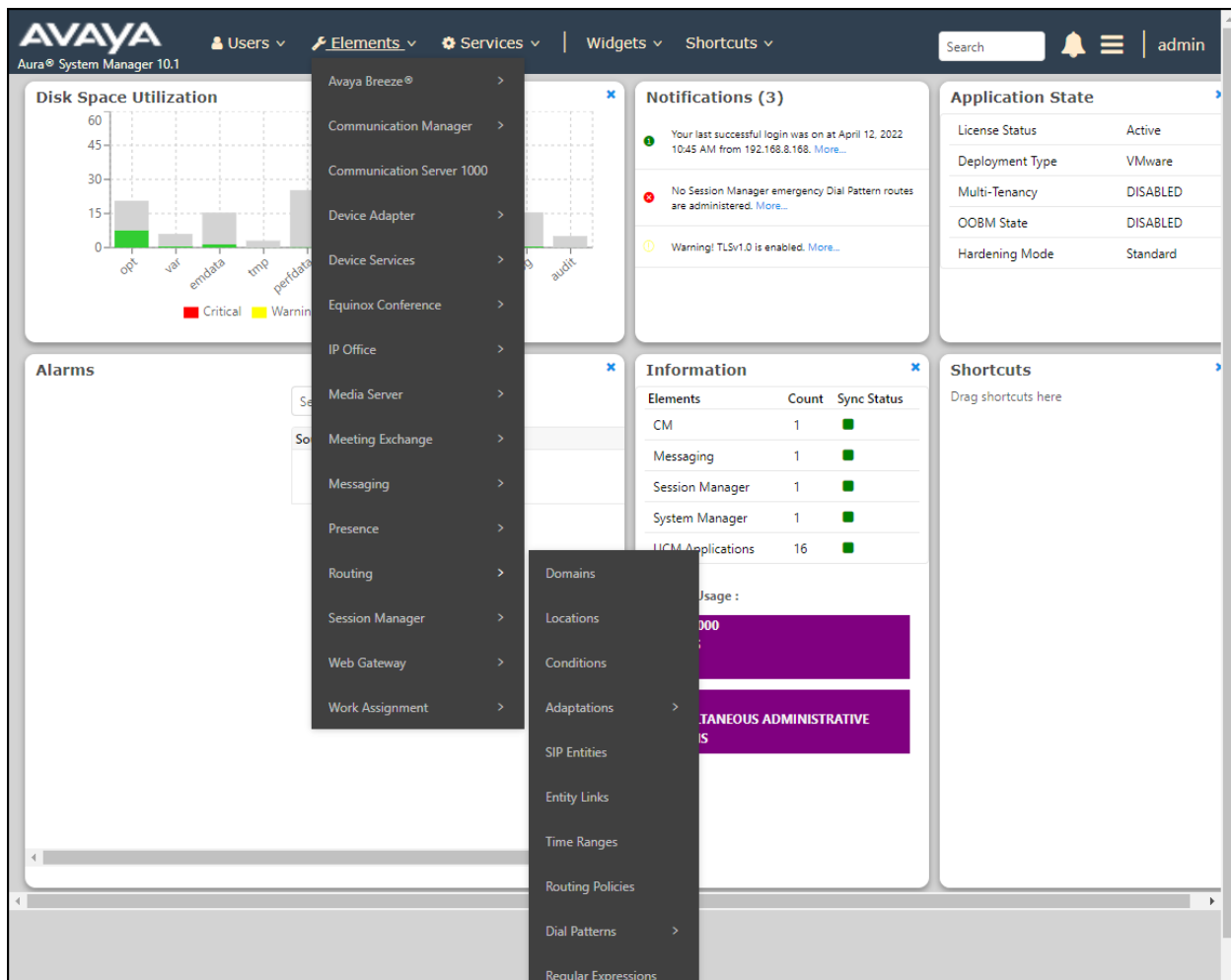
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- 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.

The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

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 and click on **Log On** (not shown). The screen shown below is then displayed; under **elements** select **Routing** → **Domains**.



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

The screenshot shows the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, version information, and links for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon are also present. The left-hand navigation pane is expanded to the 'Routing' section, with 'Domains' highlighted. The main content area is titled 'Domain Management' and features a table with one domain entry.

Name	Type	Notes
avaya.lab.com	sip	HG V-Domain

6.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, **avaya.lab.com**. 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 shown).

The screen below shows the entry for the enterprise domain.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left-hand navigation pane is expanded to 'Routing', and the 'Domains' sub-menu is selected. The main content area is titled 'Domain Management' and features a table with one entry. The table has columns for 'Name', 'Type', and 'Notes'. The entry is 'avaya.lab.com' with type 'sip' and notes 'HG V-Domain'. Above the table are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below the table is a 'Select' dropdown menu set to 'All, None'.

Name	Type	Notes
avaya.lab.com	sip	HG V-Domain

6.3. Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management, call admission control and location-based routing. 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:

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

The following screen shows the location details for the location named **Session Manager**. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'Locations' highlighted. The main content area is titled 'Location Details' and contains the following sections:

- General**: Includes fields for * Name (Session Manager) and Notes (VMware Session Manager). Buttons for 'Commit' and 'Cancel' are in the top right.
- Dial Plan Transparency in Survivable Mode**: Features an 'Enabled' checkbox (unchecked).
- Overall Managed Bandwidth**: Includes a 'Managed Bandwidth Units' dropdown (set to Kbit/sec), 'Total Bandwidth' and 'Multimedia Bandwidth' input fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.

The following screen shows the location details for the location named **Communication Manager**. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a navigation tree with 'Routing' selected, and 'Locations' highlighted. The main content area is titled 'Location Details' and contains the following sections:

- General**: Includes a required field for 'Name' (Communication Manager) and a 'Notes' field (VMware Communication Manager). 'Commit' and 'Cancel' buttons are at the top right.
- Dial Plan Transparency in Survivable Mode**: Features an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth**: Includes a 'Managed Bandwidth Units' dropdown (set to Kbit/sec), 'Total Bandwidth' and 'Multimedia Bandwidth' input fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.

The following screen shows the location details for the location named **Avaya SBCE**. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a navigation tree with 'Routing' selected, and 'Locations' highlighted. The main content area is titled 'Location Details' and contains the following sections:

- General**: Includes a required field for 'Name' (Avaya SBCE) and a 'Notes' field (VMware Avaya SBCE).
- Dial Plan Transparency in Survivable Mode**: Features an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth**: Includes a 'Managed Bandwidth Units' dropdown (set to Kbit/sec), 'Total Bandwidth' and 'Multimedia Bandwidth' input fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.

Buttons for 'Commit' and 'Cancel' are located in the top right corner of the form area.

6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 10.1 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 headers listed below before they were forwarded to the Avaya SBCE. 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, as follows:

- **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**”.
- Click **Commit** to save.

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 at their default values.

AVAYA
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing ×

Routing
Domains
Locations
Conditions
Adaptations
Adaptations
Regular Expressi...
Device Mappings
SIP Entities
Entity Links
Time Ranges

Adaptation Details

Commit Cancel Help ?

General

* Adaptation Name: CM_Outbound_Header_Removal

Notes:

* Module Name: DigitConversionAdapter ▾

Type: digit

State: enabled ▾

Module Parameter Type: Name-Value Parameter ▾

Add Remove		
<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	eRHdrs	"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View"

Select : All, None

Egress URI Parameters:

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 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 that is used for SIP signaling (see **Figure 1**).
- **Type:** Select **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 Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

The following screen shows the addition of the **Session Manager** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, user information (admin), and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a navigation tree with 'Routing' selected, and 'SIP Entities' highlighted under the 'Routing' category. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'Monitoring'. In the 'General' section, the 'Name' is 'Session Manager', 'IP Address' is '10.64.101.249', 'Type' is 'Session Manager', and 'Notes' is 'VMware Session Manager'. The 'Location' is 'Session Manager', 'Outbound Proxy' is empty, 'Time Zone' is 'America/New_York', 'Minimum TLS Version' is 'Use Global Setting', and 'Credential name' is empty. In the 'Monitoring' section, 'SIP Link Monitoring' is 'Use Session Manager Configuration' and 'CRLF Keep Alive Monitoring' is 'CRLF Monitoring Disabled'. At the top right of the form, there are 'Commit' and 'Cancel' buttons.

Field	Value
Name	Session Manager
IP Address	10.64.101.249
SIP FQDN	
Type	Session Manager
Notes	VMware Session Manager
Location	Session Manager
Outbound Proxy	
Time Zone	America/New_York
Minimum TLS Version	Use Global Setting
Credential name	
SIP Link Monitoring	Use Session Manager Configuration
CRLF Keep Alive Monitoring	CRLF Monitoring Disabled

The following screen shows the addition of the **Communication Manager Trunk 2** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**. For **Type** Select **CM** for Communication Manager. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**. Select the **Time Zone**. Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** Communication Manager Trunk 2
- * FQDN or IP Address:** 10.64.101.241
- Type:** CM (selected from a dropdown)
- Notes:** Used for SP Testing
- Adaptation:** (empty dropdown)
- Location:** Communication Manager (selected from a dropdown)
- Time Zone:** America/New_York (selected from a dropdown)
- * SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (selected from a dropdown)
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** none (selected from a dropdown)
- Loop Detection Mode:** Off (selected from a dropdown)

Buttons for 'Commit' and 'Cancel' are located at the top right of the form. A 'Help ?' link is also present.

The following screen shows the addition of the **Avaya SBCE** SIP Entity for the Avaya SBCE:

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- For **Type** Select **SIP Trunk**.
- On the **Adaptation** field, the adaptation module **CM_Outbound_Header_Removal** previously defined in **Section 6.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- Select the **Time Zone**.
- Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** Avaya SBCE
- FQDN or IP Address:** 10.64.101.243
- Type:** SIP Trunk
- Notes:** VMware Avaya SBCE
- Adaptation:** CM_Outbound_Header_Removal
- Location:** Avaya SBCE
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty field)
- Securable:** ☐
- Call Detail Recording:** none
- Loop Detection Mode:** Off

At the top right of the form, there are 'Commit' and 'Cancel' buttons. The interface also shows a top navigation bar with 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, and a search bar.

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; an entity link to Communication Manager for use only by service provider traffic and an entity link to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left 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 from the drop-down menu (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link (**Section 5.6**).
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2:** Select the name of the other system from the drop-down menu (**Section 6.5**).
- **Port:** Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. TLS transport and port **5071** were used.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
Session_Manager_CM_T	Session Manager	TLS	5071	Communication Manager Trunk 2	5071	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

The Entity Link to the Avaya SBCE is shown below; **TLS** transport and port **5061** were used.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains navigation links: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), and Time Ranges. The main content area is titled 'Entity Links' and includes 'Commit' and 'Cancel' buttons. Below the title, it shows '1 Item' and a 'Filter: Enable' dropdown. The table below lists the entity link configuration:

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	Session Manager_Avaya	Session Manager	TLS	5061	Avaya SBCE	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Below the table, there is a 'Select : All, None' dropdown and another 'Commit' and 'Cancel' button at the bottom.

6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: An incoming policy with Communication Manager as the destination and an outbound policy with the Avaya SBCE as the destination. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) 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 screens show the Routing Policies for Communication Manager and the Avaya SBCE.

AVAYA Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ≡ admin

Home Routing ×

Routing

Domains

Locations

Conditions

Adaptations ▾

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns ▾

Regular Expressions

Defaults

Routing Policy Details Commit Cancel [Help ?](#)

General

* **Name:** To CM Trunk 2

Disabled: ☐

* **Retries:** 0

Notes: For inbound calls to CM via Trunk 2

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication Manager Trunk 2	10.64.101.241	CM	Used for SP Testing

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

AVAYA

Aura® System Manager 10.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Origination Dial ...

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern:

525528

* Min:

6

* Max:

36

Emergency Call:

☐

SIP Domain:

avaya.lab.com

Notes:

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

Add Remove

1 Item

	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Avaya SBCE	VMware Avaya SBCE			To CM Trunk 2	0	<input type="checkbox"/>	Communication Manager Trunk 2	For Inbound calls to CM via Trunk 2

48 of 115
ClAuraSBC101TLS

The example in this screen shows the 13-digit dialed numbers for outbound calls, beginning with **001**, arriving from the **Communication Manager** location, will use route policy **Avaya SBCE**, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP trunk. The SIP Domain was set to **avaya.lab.com**.

AVAYA

Aura® System Manager 10.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Origination Dial ...

Regular Expressions

Dial Pattern Details

Commit Cancel

General

* Pattern: 001

* Min: 13

* Max: 13

Emergency Call: ☐

SIP Domain: avaya.lab.com

Notes:

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

Add Remove

1 Item

	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Communication Manager	VMware Communication Manager			Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE

Select : All, None

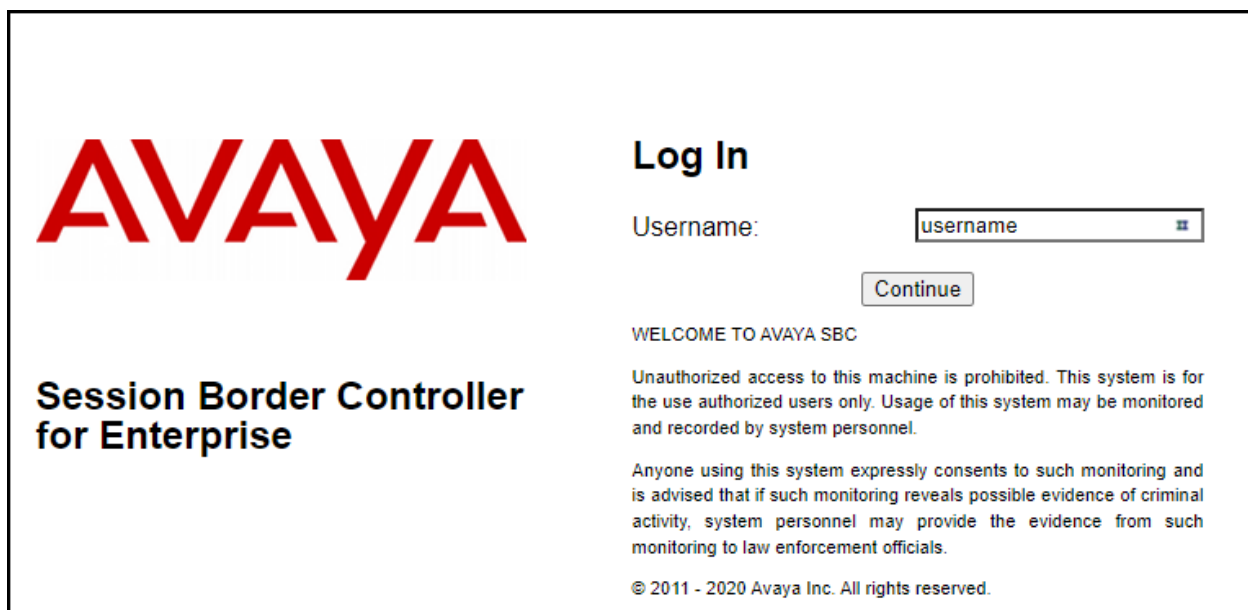
Repeat the above procedures as needed to define additional dial patterns.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **References** section.

7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The image shows the login page of the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black font. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field containing the placeholder 'username'. Below the input field is a 'Continue' button. Further down, the text 'WELCOME TO AVAYA SBC' is displayed, followed by a disclaimer: 'Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.' Below this is another paragraph: 'Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.' At the bottom, the copyright notice '© 2011 - 2020 Avaya Inc. All rights reserved.' is shown.

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **Avaya_SBCE** in the sample configuration.

The screenshot shows the Avaya SBCE web interface. At the top, there is a navigation bar with the following items: **Device: EMS** (with a dropdown arrow), **Alarms**, **Incidents**, **Status** (with a dropdown arrow), **Logs** (with a dropdown arrow), **Diagnostics**, **Users**, **Settings** (with a dropdown arrow), **Help** (with a dropdown arrow), and **Log Out**. Below the navigation bar, the main header area contains **EMS** on the left, **er Controller for Enterprise** in the center, and the **AVAYA** logo on the right. On the left side, there is a sidebar menu under the heading **EMS Dashboard**, which includes **Software Management**, **Device Management**, **System Administration** (with a right-pointing arrow), **Templates** (with a right-pointing arrow), **Backup/Restore**, and **Monitoring & Logging** (with a right-pointing arrow). The main content area is titled **Dashboard** and features a large orange and blue header bar. Below this, there are four panels: **Information** (a table with system details), **Installed Devices** (a list of devices), **Active Alarms (past 24 hours)** (showing no active alarms), and **Incidents (past 24 hours)** (showing a successful registration incident).

Information	
System Time	10:32:53 AM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-21432
Build Date	Thu Dec 02 21:33:10 UTC 2021
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	05/03/2022 10:22:18 EDT
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE: Registration Successful, Server is UP

The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

Device: Avaya_SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS Dashboard

Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Dashboard

Information

System Time	10:42:08 AM EDT	Refresh
Version	10.1.0.0-32-21432	
GUI Version	10.1.0.0-21432	
Build Date	Thu Dec 02 21:33:10 UTC 2021	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/03/2022 10:22:18 EDT	
Failed Login Attempts	0	

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS
Avaya_SBCE

Incidents (past 24 hours)

Avaya_SBCE: Registration Successful, Server is UP

HG; Reviewed:
SPOC 10/14/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

52 of 115
CI AuraSBC101TLS

7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **Avaya_SBCE** is shown. The management IP address that was configured during installation is blurred out for security reasons; the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

The screenshot displays the Avaya SBCE management console. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The left sidebar lists various management options, with 'Device Management' highlighted. The main content area shows a table of devices under the 'Devices' tab.

Device Name	Management IP	Version	Status						
Avaya_SBCE	[Blurred]	10.1.0.0-32-21432	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings. Note that **DNS configuration** is required for this solution.

System Information: Avaya_SBCE

X

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	100	200
Advanced Sessions	100	200
Scopia Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	100	200
AMR	<input type="checkbox"/>	
Premium Sessions	0	0
CLID	---	
Encryption Available: Yes	<input checked="" type="checkbox"/>	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.101.243	10.64.101.243	255.255.255.0	10.64.101.1	A1
				A1
				A1
				B1
				B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

DNS Configuration

Primary DNS	75.75.75.75
Secondary DNS	75.75.76.76
DNS Location	DMZ
DNS Client IP	10.10.80.51

Management IP(s)

IP #1 (IPv4)	
--------------	--

The highlighted IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to Clearcom and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (10.64.101.243) was used to connect to the enterprise network, while its public interface (10.10.80.51) was used to connect to the public network. See **Figure 1**.

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.

7.3. TLS Management

Note – Testing was done with System Manager signed identity certificates to enable TLS encryption inside of the enterprise (private network side). Also, testing was done with identity certificates signed by a 3rd party trusted certificate authority (CA) for enhanced security to enable TLS encryption outside of the enterprise (public network side). The procedure to create/obtain the required TLS certificates is outside the scope of these Application Notes and it's not discussed in these Application Notes.

The following procedures show how to create the client and server profiles to support TLS encryption in the Avaya SBCE.

7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **Avaya_SBCE** in the sample configuration.



Step 1 - Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- Verify the System Manager Root CA certificate is present in the **Installed CA Certificates** area, this certificate is required to enable TLS encryption inside of the enterprise (private network side). This Root CA certificate needs to be manually downloaded from System Manager and installed in the Avaya SBCE; this Root CA certificate doesn't come pre-loaded in the Avaya SBCE. Certificates from a 3rd party trusted Certificate Authority (CA) could be used for TLS encryption inside of the enterprise (private network side) instead of using Avaya System Manager as the Certificate Authority.
- Verify the Root CA certificates for the trusted certificate authority being used by the Service Provider are present in the **Installed CA Certificates** area, required to enable TLS encryption outside of the enterprise (public network side). These Root CA certificates need to be manually loaded/installed in the Avaya SBCE; these Root CA certificates don't come pre-loaded in the Avaya SBCE. The Service Provider could provide the Root CA certificates to the customer or the customer can download them directly from the 3rd party trusted Certificate Authority web/home page. The name of the 3rd party trusted Certificate Authority will be required when downloading from the 3rd party trusted Certificate Authority web/home page. The Service provider can guide the customer on how to obtain the necessary certificates.
- Verify the identity certificate signed by the System Manager CA is present in the **Installed Certificates** area.
- Verify the Private key associated with the identity certificate signed by the System Manager CA is present in the **Installed Keys** area (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: Avaya_SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar contains a menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The 'Certificates' section is active, showing a list of installed certificates and CA certificates. The 'Installed Certificates' table lists 'sbceExternal.pem' and 'sbceInternal.pem'. The 'Installed CA Certificates' table lists 'RootCA.crt' and 'default.pem'. Buttons for 'Install' and 'Generate CSR' are visible in the top right of the Certificates section.

Installed Certificates	
sbceExternal.pem	View Delete
sbceInternal.pem	View Delete

Installed CA Certificates	
RootCA.crt	View Delete
default.pem	View Delete

7.3.2. Server Profiles

7.3.2.1 Inside Server Profile

Step 1 - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name, **Inside_Server** was used.
- **Certificate:** select the identity certificate, e.g., **sbceInternal.pem**, from pull down menu.
- **Peer Verification = None.**
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

The screenshot shows the 'Edit Profile' dialog box with the following fields and values:

- Profile Name:** Inside_Server
- Certificate:** sbceInternal.pem
- SNI Options:** None
- SNI Group:** None
- Peer Verification:** None
- Peer Certificate Authorities:** (empty list)
- Peer Certificate Revocation Lists:** (empty list)
- Verification Depth:** 0

A **Next** button is located at the bottom right of the dialog box.

7.3.2.2 Outside Server Profile

Step 1 - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **Profile Name**: enter a descriptive name, **Outside_Server** was used.
- **Certificate**: select the identity certificate, e.g., **sbceExternal.pem**, from the pull-down menu.
- **Peer Verification**: Select **None** from the pull-down menu.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**

The screenshot shows the 'Edit Profile' dialog box with the following fields and values:

- Profile Name**: Outside_Server
- Certificate**: sbceExternal.pem
- SNI Options**: None
- SNI Group**: None
- Peer Verification**: None
- Peer Certificate Authorities**: (empty list)
- Peer Certificate Revocation Lists**: (empty list)
- Verification Depth**: 0

A warning message is displayed at the top: "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. Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid."

A "Next" button is located at the bottom right of the dialog.

The following screen shows the completed **Inside_Server** profile form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: Avaya_SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo.

On the left, a sidebar menu lists various management options, with 'Server Profiles' highlighted under the 'TLS Management' section. The main content area is titled 'Server Profiles: Inside_Server' and features an 'Add' button and a 'Delete' button. A blue bar with the text 'Click here to add a description.' is visible.

The 'Server Profile' configuration form is shown, containing the following sections:

- TLS Profile**
 - Profile Name: Inside_Server
 - Certificate: sbcInternal.pem
 - SNI Options: None
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom

The following screen shows the completed **Outside_Server** profile form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: Avaya_SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo.

On the left, a sidebar menu lists various management options, with 'Server Profiles' highlighted under the 'TLS Management' section. The main content area is titled 'Server Profiles: Outside_Server' and features an 'Add' button and a 'Delete' button. A blue bar with the text 'Click here to add a description.' is visible.

The 'Server Profile' configuration form is shown, containing the following sections:

- TLS Profile**
 - Profile Name: Outside_Server
 - Certificate: sbceExternal.pem
 - SNI Options: None
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom

7.3.3. Client Profiles

7.3.3.1 Inside Client Profile

Step 1 - Select **TLS Management** → **Client Profiles** and click on **Add**. Enter the following:

- **Profile Name**: enter a descriptive name, **Inside_Client** was used.
- **Certificate**: select the identity certificate, e.g., **sbceInternal.pem**, from the pull-down menu.
- **Peer Verification**: Select **Required** from the pull-down menu.
- **Peer Certificate Authorities**: select the Root CA certificate used to verify the identity certificate received from Session Manager, e.g., **default.pem**.
- **Verification Depth**: enter **1**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

Edit Profile

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.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name:

Certificate:

SNI: ☐ Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

Extended Hostname Verification: ☐

Server Hostname:

Next

7.3.3.2 Outside Client Profile

Step 1 - Select **TLS Management** → **Client Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter a descriptive name, **Outside_Client** was used.
- **Certificate:** select **None** from the pull-down menu.
- **Peer Verification:** **Required** from the pull-down menu.
- **Peer Certificate Authorities:** select the Root CA certificates used to verify the identity certificate received from the Service Provider, e.g., **xxxxxxxRootCA.crt**. (Note: for security reasons part of the Root CA certificate name was blurred out).
- **Verification Depth:** enter **2**.
- Click **Next**.

Edit Profile [X]

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.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name:

Certificate:

SNI: ☐ Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

Extended Hostname Verification: ☐

Server Hostname:

Step 2 – Under **Handshake Options**, select **TLS 1.1** and **TLS 1.0** and click **Finish**.

Note – Currently Clearcom only supports TLS Version 1.0

The screenshot shows a 'New Profile' dialog box with two main sections: 'Renegotiation Parameters' and 'Handshake Options'. In the 'Renegotiation Parameters' section, 'Renegotiation Time' is set to 0 seconds and 'Renegotiation Byte Count' is set to 0. In the 'Handshake Options' section, 'Version' has checkboxes for TLS 1.2, TLS 1.1, and TLS 1.0, all of which are checked. 'Ciphers' has radio buttons for Default, FIPS, and Custom, with 'Default' selected. Below 'Ciphers' is a 'Value' field with a link '(What's this?)' and the text 'HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGT'. At the bottom are 'Back' and 'Finish' buttons.

Renegotiation Parameters	
Renegotiation Time	0 seconds
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value (What's this?)	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGT

Back Finish

The following screen shows the completed **Inside_Client** profile form:

Device: Avaya_SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services▸ Domain Policies▸ TLS Management

- Certificates
- Client Profiles**
- Server Profiles
- SNI Group

▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Client Profiles: Inside_Client

AddDelete

Client Profiles

CenturyLink_...Remote_Wor...MiguelsOutsi...IPO_Inside_...sbcInternalClearcom_O...Inside_ClientOutside_Client

Click here to add a description.

Client Profile

TLS Profile

Profile Name	Inside_Client
Certificate	sbcInternal.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	default.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

HG; Reviewed:
SPOC 10/14/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

65 of 115
CIAuraSBC101TLS

The following screen shows the completed **Outside_Client** profile form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: Avaya_SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo.

On the left, a sidebar menu lists various management options, with 'Client Profiles' highlighted under the 'TLS Management' section. The 'Outside_Client' profile is selected in the list.

The main content area is titled 'Client Profiles: Outside_Client' and features an 'Add' button and a 'Delete' button. A blue bar prompts the user to 'Click here to add a description.' Below this, the 'Client Profile' configuration form is shown, containing several sections:

- TLS Profile**: Profile Name (Outside_Client), Certificate (None), and SNI (Enabled).
- Certificate Verification**: Peer Verification (Required), Peer Certificate Authorities (RootCA.crt), Peer Certificate Revocation Lists (---), Verification Depth (2), and Extended Hostname Verification (disabled).
- Renegotiation Parameters**: Renegotiation Time (0) and Renegotiation Byte Count (0).
- Handshake Options**: Version (TLS 1.2, TLS 1.1, TLS 1.0), Ciphers (Default, FIPS, Custom), and Value (HIGH:DH:ADH:IMD5:1aNULL:1eNULL:@STRENGTH).

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

7.4. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from the **Network & Flows** on the left-side menu. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (**10.64.101.243**) and public (**10.10.80.51**) sides of the Avaya SBCE are the ones relevant to these Application Notes.

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B1** interfaces. Click the buttons under the **Status** column, if necessary, to enable the interfaces.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: Avaya_SBCE', '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 lists various management options, with 'Network Management' highlighted under the 'Network & Flows' section. The main content area is titled 'Network Management' and features two tabs: 'Interfaces' (selected) and 'Networks'. An 'Add VLAN' button is located in the top right of the interface table. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled). Each interface has a corresponding status button in the 'Status' column.

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

7.5. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

The screenshot shows a dialog box titled "Edit Media Interface" with a close button "X" in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing the value "Private_med".
- IP Address:** Two dropdown menus. The first dropdown shows "Network_A1 (A1, VLAN 0)" and the second dropdown shows "10.64.101.243".
- Port Range:** Two text input fields containing "35000" and "40000", separated by a hyphen.
- Finish:** A button at the bottom center of the dialog.

A Media Interface facing the public side was similarly created with the name **Public_med**, as shown below.

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

Edit Media Interface X

Name

IP Address

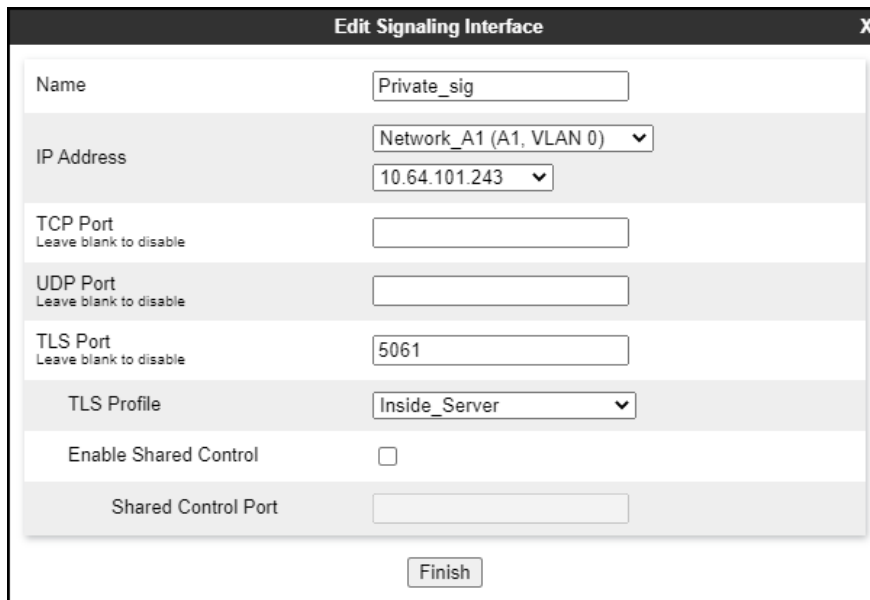
Port Range -

7.6. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**.
- Select a **TLS Profile** (**Section 7.3.2.1**).
- Click **Finish**.



The screenshot shows a web-based configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The form contains the following fields and options:

- Name:** A text input field containing "Private_sig".
- IP Address:** A section with two dropdown menus. The first dropdown is set to "Network_A1 (A1, VLAN 0)". The second dropdown is set to "10.64.101.243".
- TCP Port:** A text input field with the label "Leave blank to disable" below it.
- UDP Port:** A text input field with the label "Leave blank to disable" below it.
- TLS Port:** A text input field containing "5061" with the label "Leave blank to disable" below it.
- TLS Profile:** A dropdown menu set to "Inside_Server".
- Enable Shared Control:** A checkbox that is currently unchecked.
- Shared Control Port:** A text input field.
- Finish:** A button at the bottom center of the form.

A second Signaling Interface with the name **Public_sig** was similarly created in the service provider's direction.

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Clearcom in the sample configuration.
- Select a **TLS Profile (Section 7.3.2.2)**.
- Click **Finish**.

Edit Signaling Interface X

Name	Public_sig
IP Address	Network_B1 (B1, VLAN 0) 10.10.80.51
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	Outside_Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

7.7. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

7.7.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Configuration Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select **avaya-ru** from the list of pre-defined profiles. Click **Clone** (not shown).

Device: Avaya_SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users

Session Border Controller for Enterprise

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▾ Configuration Profiles
 Domain DoS
 Server Interworking
 Media Forking
 Routing
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps
 Time of Day Rules
 FGDN Groups
 Reverse Proxy Policy
 URN Profile
 Recording Profile
 H248 Profile
 IP/URI Blocklist Profile
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Interworking Profiles: avaya-ru

Add

Interworking Profiles
avaya-ru
OCS-Edge-Server
cisco-ccm
cups
OCS-FrontEnd-Server
Avaya-SM
Avaya-IPO
Avaya-CS1000
Avaya-CM
cs2100
SP-General

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

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

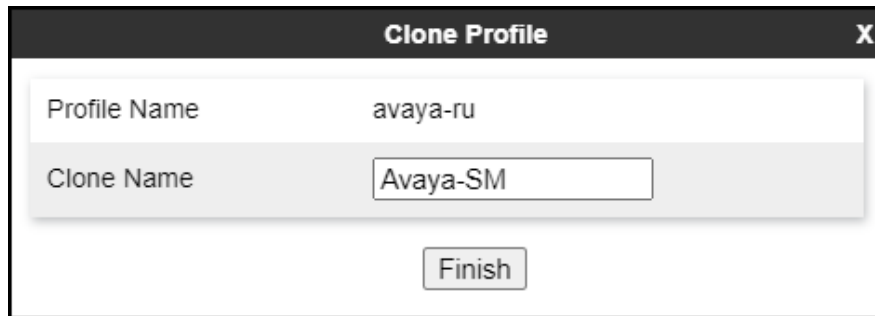
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme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

HG; Reviewed:
SPOC 10/14/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

72 of 115
CIAuraSBC101/TLS

- Enter a descriptive name for the cloned profile.
- Click **Finish**.



The image shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The main area is white and contains two input fields. The first field is labeled 'Profile Name' and has the text 'avaya-ru' entered. The second field is labeled 'Clone Name' and has the text 'Avaya-SM' entered. Below these fields is a 'Finish' button.

Clone Profile	
Profile Name	avaya-ru
Clone Name	Avaya-SM
<button>Finish</button>	

Click **Edit** on the newly cloned **Avaya-SM** interworking profile:

- On the **General** tab, set **SIPS Required** to **No**.
- Leave remaining fields with default values.
- Click **Finish** (not shown).

The **General** tab settings are shown on the screen below:

Device: Avaya_SBCE ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users

Session Border Controller for Enterprise

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy Policy
URN Profile
Recording Profile
H248 Profile
IP/URI Blocklist Profile
Services
Domain Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging

Interworking Profiles: Avaya-SM

Add

Interworking Profiles

avaya-ru
OCS-Edge-Server
cisco-ccm
cups
OCS-FrontEnd-Server
Avaya-SM
Avaya-IPO
Avaya-CS1000
Avaya-CM
cs2100
SP-General

General
Timers
Privacy
URI Manipulation
Header Manipulation
Advanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
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
SIPS Required	No
Mediasec	No

HG; Reviewed:
SPOC 10/14/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

74 of 115
CIAuraSBC101TLS

The **Advanced** tab settings are shown on the screen below:

Device: Avaya_SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Session Border Controller for Enterprise

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

Routing

Topology Hiding

Signaling

Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy

Policy

URN Profile

Recording Profile

Interworking Profiles: Avaya-SM

Add

Interworking Profiles

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

Click here to add a device

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

Record Routes

Both Sides

Include End Point IP for Context Lookup

Yes

Extensions

Avaya

Diversion Manipulation

No

Has Remote SBC

Yes

Route Response on Via Port

No

Relay INVITE Replace for SIPREC

No

MOBX Re-INVITE Handling

No

NATing for 301/302 Redirection

Yes

DTMF

DTMF Support

None

Edit

7.7.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown).

- Enter a descriptive name for the new profile.
- Click **Next**.
- On the **General** tab, set **SIPS Required** to **No** (not shown).



The screenshot shows a dialog box titled "Interworking Profile" with a close button "X" in the top right corner. The dialog contains a label "Profile Name" and a text input field with the value "SP-General". Below the input field is a "Next" button.

- Click **Next** until the last tab is reached then click **Finish** on the last tab leaving remaining fields with default values (not shown).

The **General** tab settings are shown on the screen below:

Device: Avaya_SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsers

Session Border Controller for Enterprise

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▴ Configuration ProfilesDomain DoS**Server Interworking**Media ForkingRoutingTopology HidingSignaling ManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse Proxy PolicyURN ProfileRecording ProfileH248 ProfileIP/URI Blocklist Profile▸ Services▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Interworking Profiles: SP-General

Add

Interworking Profiles

avaya-ruOCS-Edge-Servercisco-ccmcupsOCS-FrontEnd-ServerAvaya-SMAvaya-IPOAvaya-CS1000Avaya-CMcs2100**SP-General**

Click here

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
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
SIPS Required	No
Mediasec	No

HG; Reviewed:
SPOC 10/14/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

77 of 115
CIAuraSBC101TLS

The **Advanced** tab settings are shown on the screen below:

Device: Avaya_SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Session Border Controller for Enterprise

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

H248 Profile

IP/URI Blocklist Profile

Interworking Profiles: SP-General

Add

Interworking Profiles

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

OCS-FrontEnd-Server

Avaya-SM

Avaya-IPO

Avaya-CS1000

Avaya-CM

cs2100

SP-General

Click here

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

Record Routes

Both Sides

Include End Point IP for Context Lookup

No

Extensions

None

Diversion Manipulation

No

Has Remote SBC

Yes

Route Response on Via Port

No

Relay INVITE Replace for SIPREC

No

MOBX Re-INVITE Handling

No

NATing for 301/302 Redirection

Yes

DTMF

DTMF Support

None

7.8. 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 reference [8] in the **References** section for more information on this topic.

A single Sigma script was created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

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

The scripts will later be applied to the Server Configuration profile corresponding to the Service Provider (toward Clearcom) in **Section 7.9.2**.

To create the SigMa script to be applied to the Server Configuration Profile corresponding to the Service Provider, on the left navigation pane, select **Configuration 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**.

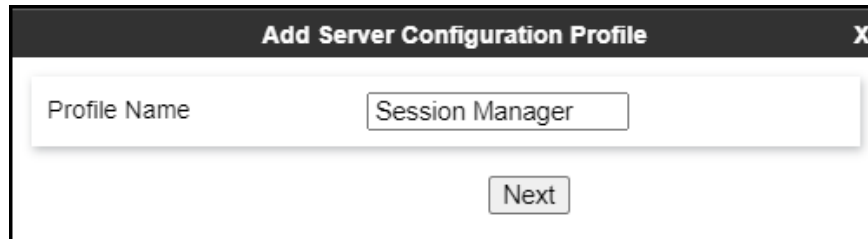
7.9. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and Clearcom SIP Proxy (Trunk Server).

7.9.1. Server Configuration Profile – Enterprise

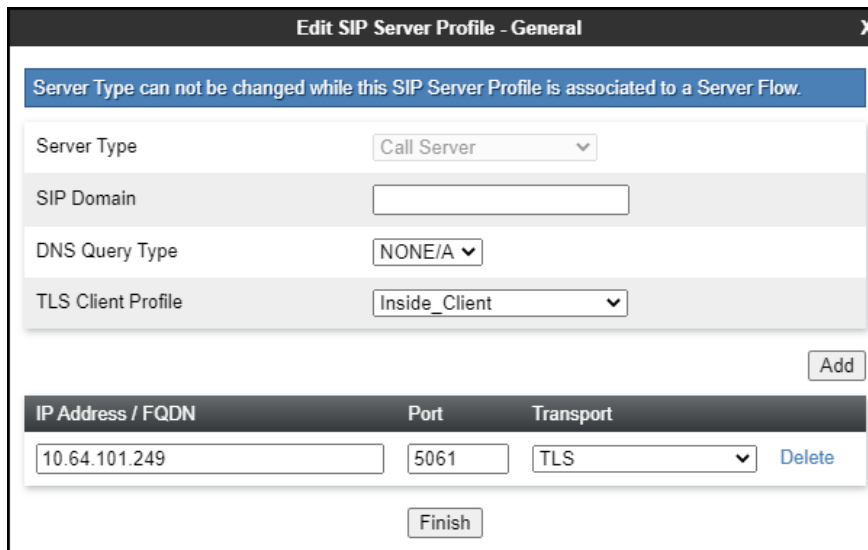
From the **Services** menu on the left-hand navigation pane, select **SIP Servers** and click the **Add** button (not shown) to add a new profile for the Call Server.

- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Session Manager". Below this field, there is a button labeled "Next".

- On the **Edit SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.6**.
- Select a **TLS Profile** (**Section 7.3.3.1**).
- Click **Next** (not shown).



The screenshot shows a dialog box titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. At the top, there is a blue warning message: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several fields: "Server Type" (a dropdown menu showing "Call Server"), "SIP Domain" (an empty text field), "DNS Query Type" (a dropdown menu showing "NONE/A"), and "TLS Client Profile" (a dropdown menu showing "Inside_Client"). To the right of these fields is an "Add" button. Below these fields is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "10.64.101.249", "5061", and "TLS" (a dropdown menu). To the right of the table is a "Delete" button. At the bottom of the dialog is a "Finish" button.

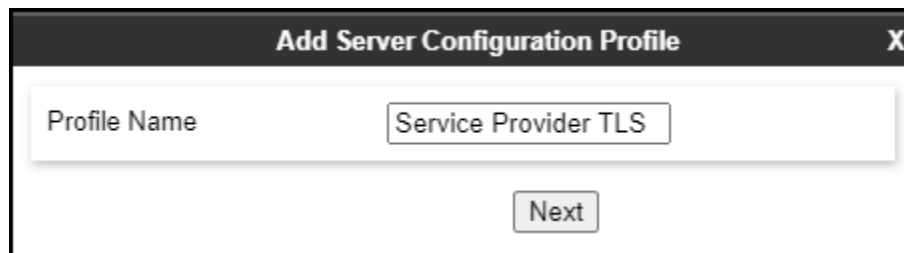
- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
 - Check **Enable Grooming** (required for TLS transport).
 - Select **Avaya-SM** from the **Interworking Profile** drop-down menu (**Section 7.7.1**).
- Click **Finish**.

Add SIP Server Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>
<div>Back Finish</div>	

7.9.2. Server Configuration Profile – Service Provider

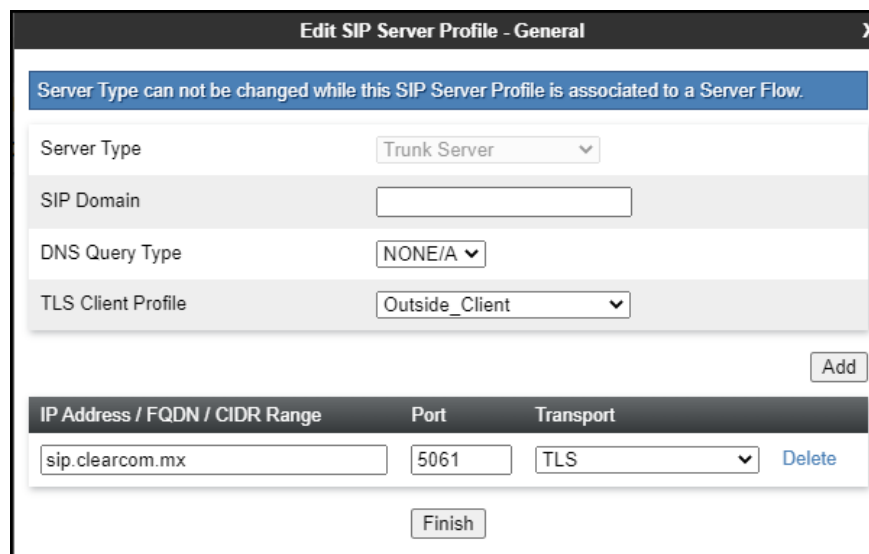
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below (**Service Provider TLS** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Service Provider TLS". Below this field is a button labeled "Next".

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop-down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter **sip.clearcom.mx** (Clearcom SIP proxy server FQDN). This information was provided by Clearcom.
- Enter **5061** under **Port** and select **TLS** for **Transport**.
- Select a **TLS Profile** (**Section 7.3.3.2**).
- Click **Next**.

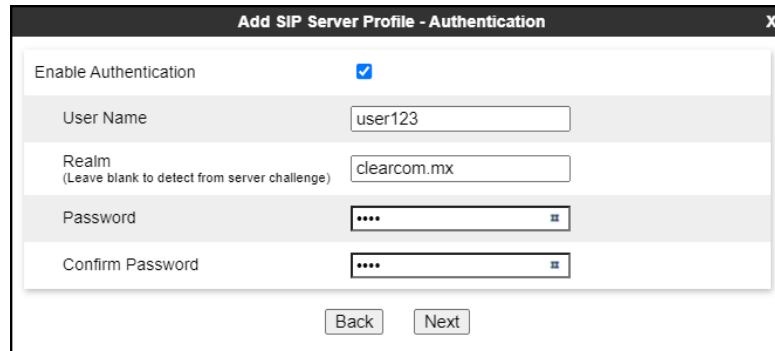


The screenshot shows the "Edit SIP Server Profile - General" tab. At the top, a blue banner states: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are several fields: "Server Type" (Trunk Server), "SIP Domain" (empty), "DNS Query Type" (NONE/A), and "TLS Client Profile" (Outside_Client). An "Add" button is to the right of these fields. Below these is a table with three columns: "IP Address / FQDN / CIDR Range", "Port", and "Transport". The first row contains "sip.clearcom.mx", "5061", and "TLS". A "Delete" link is next to the "Transport" field. At the bottom is a "Finish" button.

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

On the **Add SIP Server Profile - Authentication** tab:

- 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.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

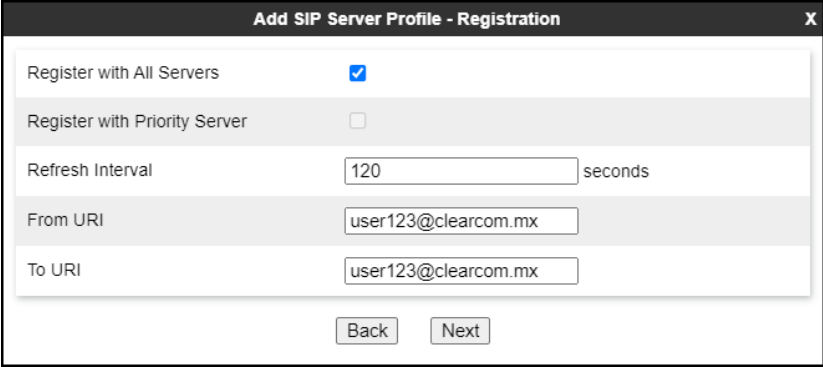


The screenshot shows a window titled "Add SIP Server Profile - Authentication". It contains a checkbox labeled "Enable Authentication" which is checked. Below this are four input fields: "User Name" (containing "user123"), "Realm (Leave blank to detect from server challenge)" (containing "clearcom.mx"), "Password" (masked with "...."), and "Confirm Password" (masked with "...."). At the bottom of the window are "Back" and "Next" buttons.

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

On the **Add SIP Server Profile - Registration** tab:

- Check the **Register with All Servers** box.
- **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**.

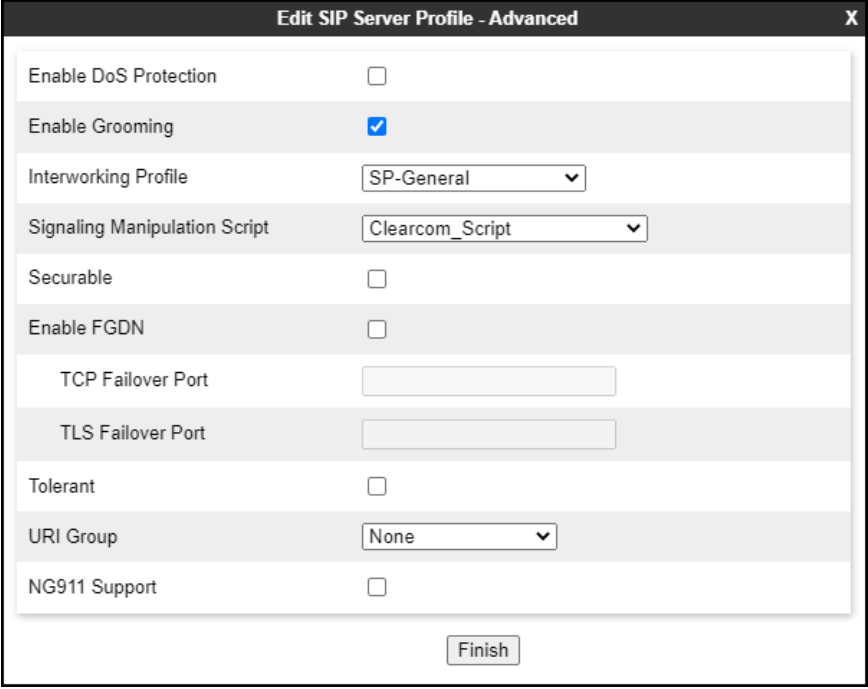


Add SIP Server Profile - Registration	
Register with All Servers	<input checked="" type="checkbox"/>
Register with Priority Server	<input type="checkbox"/>
Refresh Interval	<input type="text" value="120"/> seconds
From URI	<input type="text" value="user123@clearcom.mx"/>
To URI	<input type="text" value="user123@clearcom.mx"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Click **Next** on the **Add SIP Server Profile - Ping** window (not shown).

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

- Check **Enable Grooming** (required for TLS transport).
- Select **SP-General** from the **Interworking Profile** drop-down menu (**Section 7.7.2**).
- Select the **Clearcom_Script** from the **Signaling Manipulation Script** drop down menu (**Sections 7.8 and Appendix A**).
- Click **Finish**.



The screenshot shows the 'Edit SIP Server Profile - Advanced' window with the following settings:

Option	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	Clearcom_Script
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

Finish

7.10.Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the service provider SIP trunk.

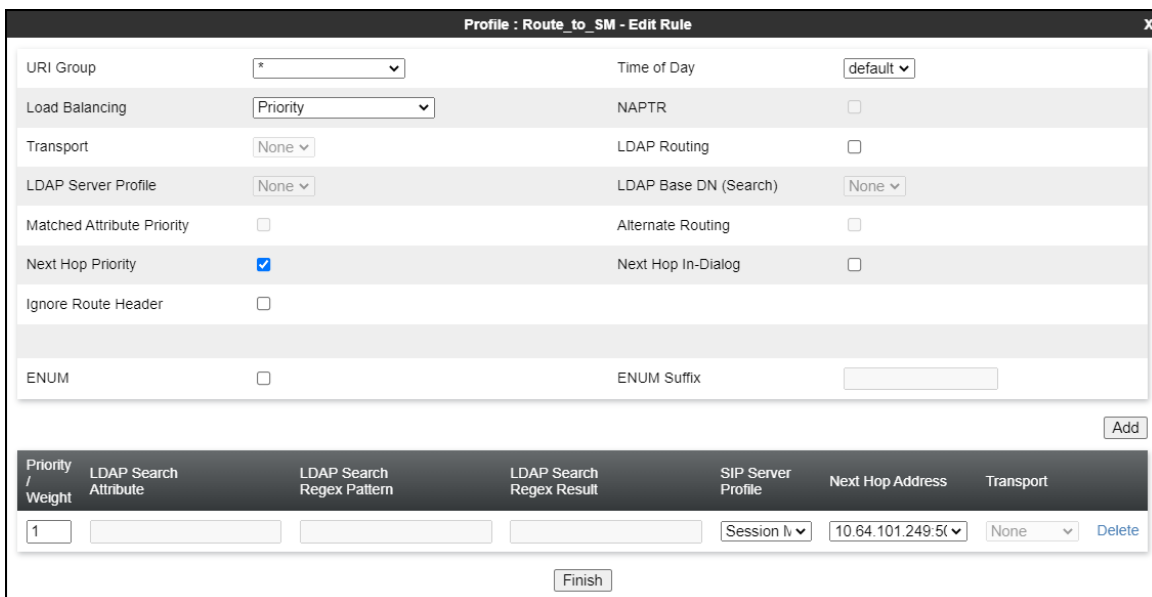
7.10.1. Routing Profile – Enterprise

To create the inbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add** (not shown).

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



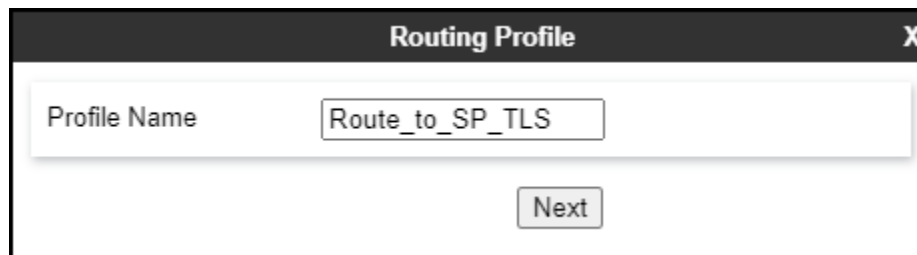
- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select **Session Manager**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.9.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



7.10.2. Routing Profile – Service Provider

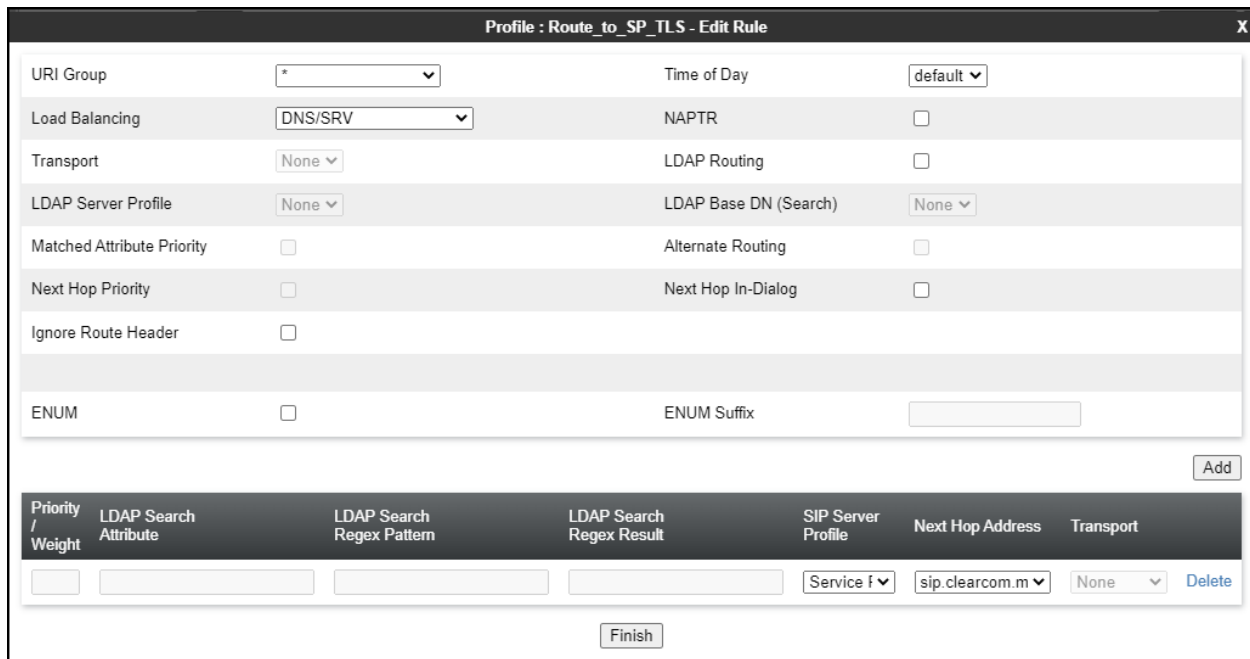
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below (**Route_to_SP_TLS** was used).
- Click **Next**.



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

- Under **Load Balancing** select **DNS/SRV**.
- Click the **Add** button to enter the next-hop address.
- Under **SIP Server Profile**, select **Service Provider TLS**.
- The **Next Hop Address** is populated automatically with **sip.clearcom.mx:5061 (TLS)**. Clearcom SIP Proxy FQDN, Port and Transport, Server Configuration Profile defined in **Section 7.9.2**.
- Click **Finish**



The image shows a dialog box titled "Profile : Route_to_SP_TLS - Edit Rule" with a close button (X) in the top right corner. The dialog contains a form with various settings for a routing profile. The settings are as follows:

URI Group	Time of Day
*	default
Load Balancing	DNS/SRV
Transport	None
LDAP Server Profile	None
Matched Attribute Priority	Alternate Routing
Next Hop Priority	Next Hop In-Dialog
Ignore Route Header	
ENUM	ENUM Suffix

Below the form is an "Add" button. At the bottom of the dialog is a "Finish" button.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
				Service t	sip.clearcom.m	None	Delete

7.11.Topology Hiding

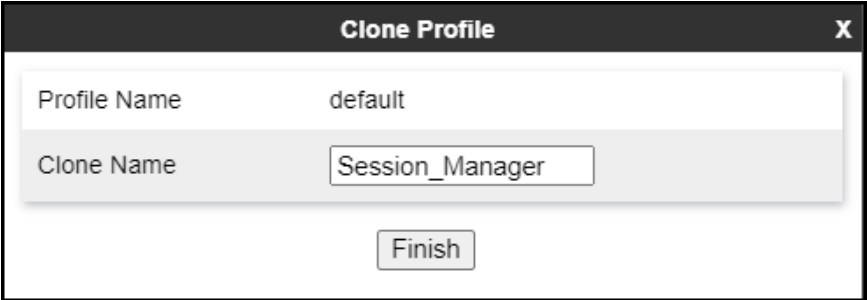
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. 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.

7.11.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side, select **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



Clone Profile	
Profile Name	default
Clone Name	Session_Manager
<button>Finish</button>	

On the newly cloned **Session_Manager** profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **avaya.lab.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**.
- Default values were used for all other fields.
- Click **Finish**.

Edit Topology Hiding Profile

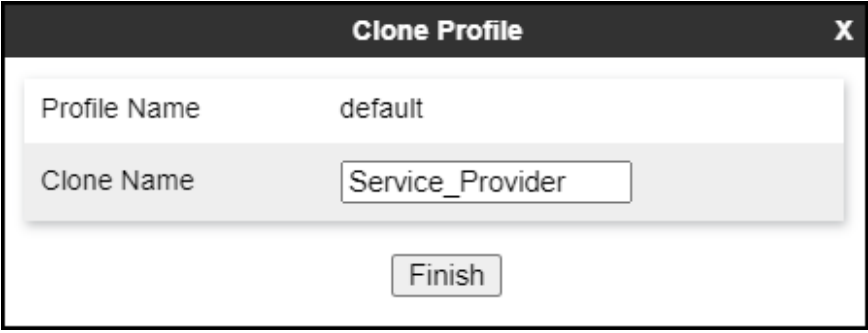
Header	Criteria	Replace Action	Overwrite Value	
Via	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	avaya.lab.com	Delete
Referred-By	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	avaya.lab.com	Delete
SDP	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Request-Line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

Finish

7.11.2. Topology Hiding Profile – Service Provider

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 **default** from the list of pre-defined profiles and click the **Clone** button (not shown).

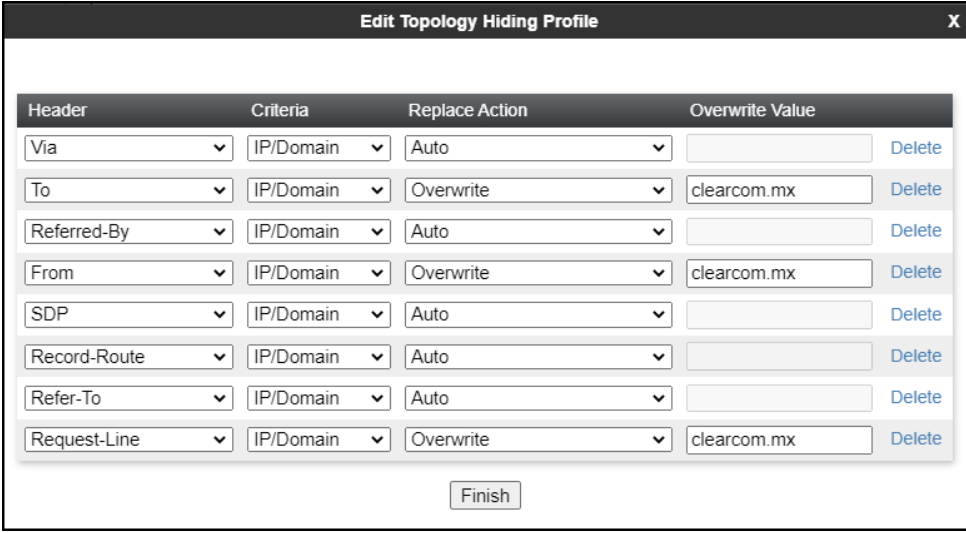
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The 'Clone Profile' dialog box has a title bar with 'Clone Profile' and a close button 'X'. It contains two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Service_Provider'. Below these fields is a 'Finish' button.

On the newly cloned **Service_Provider** profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **clearcom.mx**, in the **Overwrite Value** column of these headers, as shown below. This is the service provider's domain name.
- Default values were used for all other fields.
- Click **Finish**.



The 'Edit Topology Hiding Profile' dialog box has a title bar with 'Edit Topology Hiding Profile' and a close button 'X'. It contains a table with the following data:

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

Below the table is a 'Finish' button.

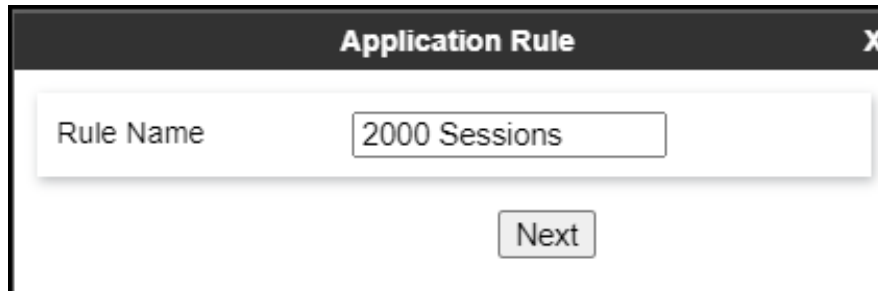
7.12.Domain Policies

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.

7.12.1.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 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.

- Under **Rule Name** enter the name of the profile, e.g., **2000 Sessions**.
- Click **Next**.



The screenshot shows a web-based configuration window titled "Application Rule". It features a close button (X) in the top right corner. The main content area contains a label "Rule Name" and a text input field with the value "2000 Sessions". Below the input field is a "Next" button.

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** for Audio. Repeat for video if needed, 100 sessions each was used for video in the sample configuration.
- Click **Finish**.

Editing Rule: 2000 Sessions

X

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="2000"/>	<input type="text" value="2000"/>
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="100"/>

Miscellaneous

CDR Support

☒ Off
☐ RADIUS
☐ CDR Adjunct

RADIUS Profile

None ▾

Media Statistics Support

☐

Call Duration

☒ Setup
☐ Connect

RTCP Keep-Alive

☐

Finish

7.12.2. 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 **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption, if needed.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Click **Next**.

Media Encryption
X

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

Capability Negotiation	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

Finish

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

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** (not shown).
- 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 **RTP**.
- 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 checked.
- Click **Next**.

Media Encryption

X

Audio Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Video Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Miscellaneous

Capability Negotiation

☒

Finish

7.12.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.

Device: Avaya_SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Session Border Controller for Enterprise

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▾ Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Charging Rules

End Point Policy

Groups

Session Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Signaling Rules: default

Add

Signaling Rules

default

No-Content-Type-Checks

SessMgr_CM_SigRule

OPTIONS

Remote Workers

Remove_Update

Contact

Remove PAI

Remove PAI_1

Remove_headers

Remove Record Route

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

GeneralRequestsResponsesRequest HeadersResponse HeadersSignaling QoSUCID

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☒

Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Edit

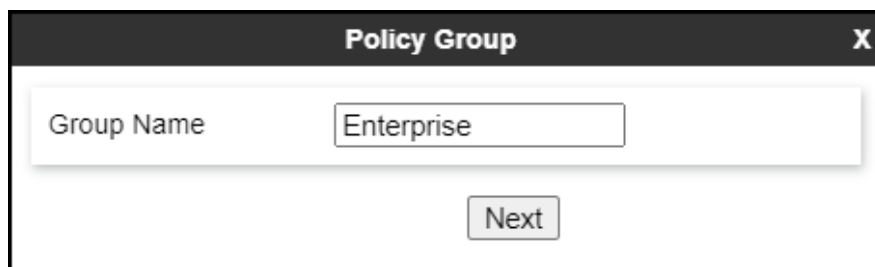
7.13.End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

7.13.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

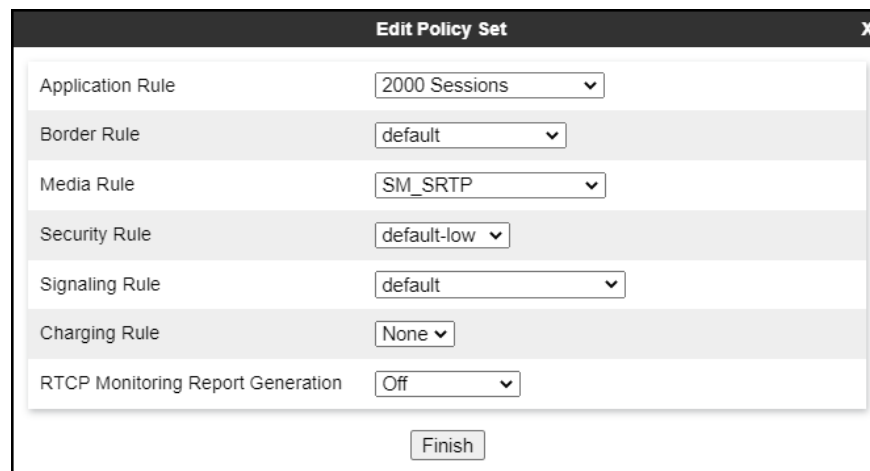
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a label "Group Name" followed by a text input field containing the word "Enterprise". Below the input field, there is a button labeled "Next".

Under the **Policy Group** tab enter the following:

- **Application Rule: 2000 Sessions** (Section 7.12.1).
- **Border Rule: default**.
- **Media Rule: SM_SRTP** (Section 7.12.2).
- **Security Rule: default-low**.
- **Signaling Rule: default** (Section 7.12.3).
- Click **Finish**.

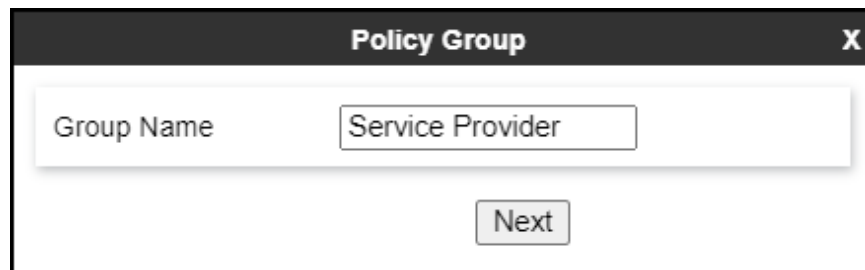


The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. The dialog contains a list of rules with corresponding dropdown menus. The rules and their selected values are: Application Rule (2000 Sessions), Border Rule (default), Media Rule (SM_SRTP), Security Rule (default-low), Signaling Rule (default), Charging Rule (None), and RTCP Monitoring Report Generation (Off). At the bottom of the dialog, there is a button labeled "Finish".

7.13.2. End Point Policy Group – Service Provider

To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

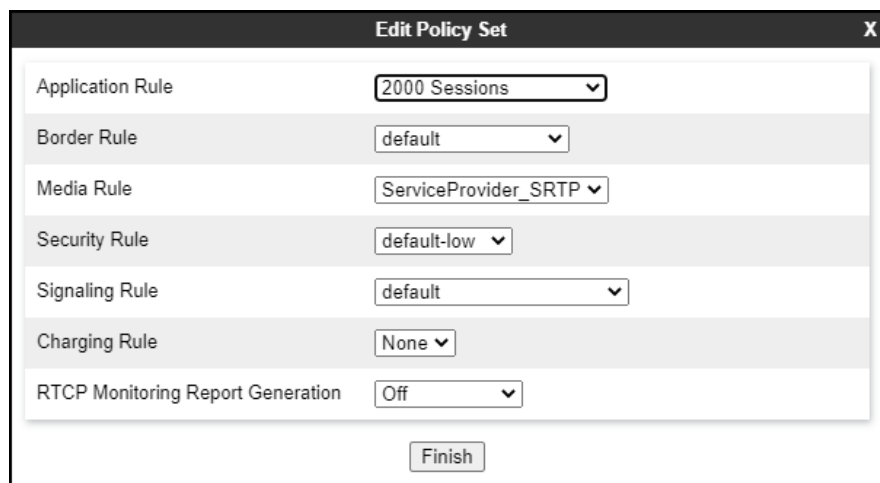
- Enter an appropriate name in the **Group Name** field (**Service Provider** was used).
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Service Provider". Below this field, there is a button labeled "Next".

Under the **Policy Group** tab enter the following:

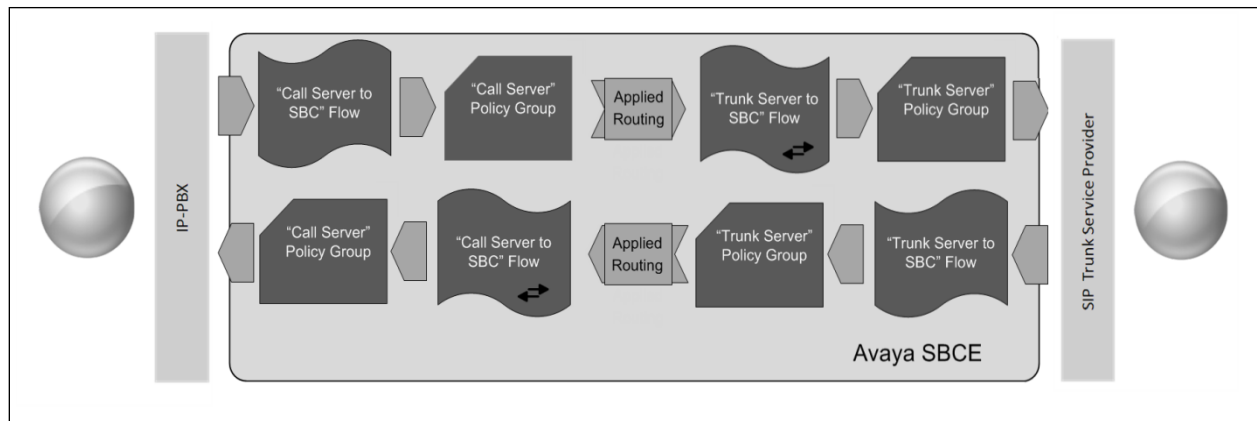
- **Application Rule: 2000 Sessions** (Section 7.12.1).
- **Border Rule: default**.
- **Media Rule: ServiceProvider_SRTP** (Section 7.12.2).
- **Security Rule: default-low**.
- **Signaling Rule: default** (Section 7.12.3).
- Click **Finish**.



The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. Inside the dialog, there are several rows, each with a label and a dropdown menu. The labels and their corresponding dropdown values are: "Application Rule" (2000 Sessions), "Border Rule" (default), "Media Rule" (ServiceProvider_SRTP), "Security Rule" (default-low), "Signaling Rule" (default), "Charging Rule" (None), and "RTCP Monitoring Report Generation" (Off). At the bottom of the dialog, there is a button labeled "Finish".

7.14.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.

7.14.1. End Point Flow – SP to SM Flow

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The screen below shows the flow named **SP to SM Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: SP to SM FlowX

Flow Name	SP to SM Flow
SIP Server Profile	Service Provider TLS
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	Service Provider
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
Finish	

7.14.2. End Point Flow – SM to SP Flow

A second Server Flow with the name **SM to SP Flow** was similarly created in the Service Provider direction. To create the call flow toward the Service Provider, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown), set parameters as shown below, click **Finish**. The flow uses the interfaces, policies, and profiles defined in previous sections.

Edit Flow: SM to SP Flow	
Flow Name	SM to SP Flow
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
Secondary Media Interface	None
End Point Policy Group	Enterprise
Routing Profile	Route_to_SP_TLS
Topology Hiding Profile	Session_Manager
Signalling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
Finish	

8. Clearcom SIP Trunking Service Configuration

To use Clearcom 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/>

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 network.

Clearcom will provide the following information:

- The **Root CA** certificates for the trusted certificate authority being used by the Clearcom, required to enable TLS encryption outside of the enterprise (public network side). The customer can download the **Root CA** certificates directly from the 3rd party trusted Certificate Authority web/home page, the name of the 3rd party trusted Certificate Authority will be needed when downloading from their web/home page, Clearcom can guide the customer on how to obtain the necessary certificate.
- SIP Trunk registration credentials (user name, password, SIP domain).
- Fully Qualified Domain Name of the Clearcom SIP proxy server.
- DID numbers.
- Public DNS IP addresses.
- 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 (firewall).

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 commands that can be used to troubleshoot the solution.

9.1. General Verification Steps

- 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.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

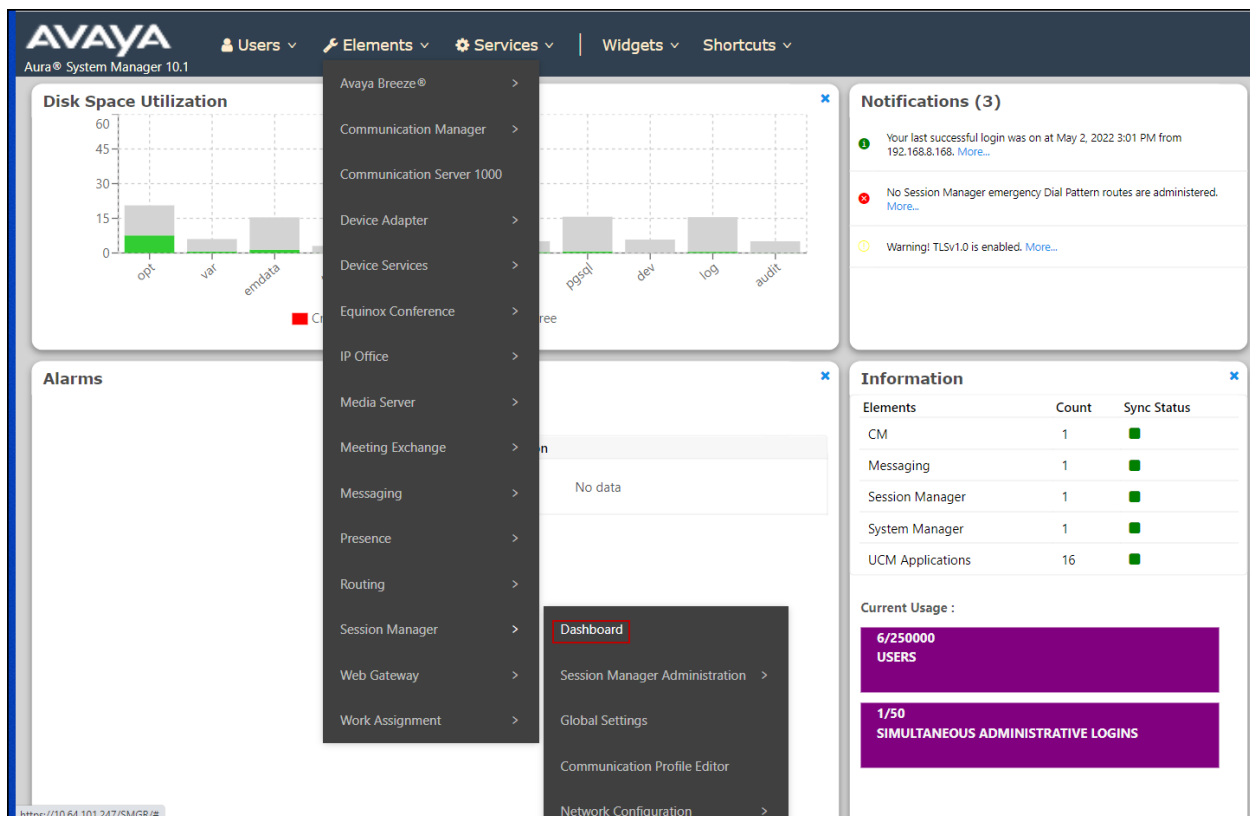
- **list trace station** <extension number>
Traces calls to and from a specific station.

- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **status 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.

9.3. Session Manager Verification

The Session Manager configuration may be verified via System Manager.

Step 1 - Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**, then select **Dashboard**.



Step 2 - The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns all show good status.

In the **Entity Monitoring** column, Session Manager shows that there are **1** alarm out of the **7** Entities defined.

Session Manager Dashboard
This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: Shutdown System EASG Clear Logs As of 9:09 AM

1 Item Show All Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Load Factor	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Profile	Version
<input type="checkbox"/>	Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/0/0	3/9	0	1/1	✓	✓	Normal	Enabled	3	10.1.0.0.1010019

Select : All, None

Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns are **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status
This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

All Entity Links for Session Manager: Session Manager

Summary View

9 Items Filter: Enable

	SIP Entity Name	Session Manager IP Address	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	CS1K7.6	IPv4	172.16.5.60	5085	UDP	FALSE	DOWN	408 Request Timeout	DOWN
<input type="radio"/>	Avaya Experience Portal	IPv4	10.64.101.252	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	AA-Messaging	IPv4	10.64.101.250	5060	TCP	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	Avaya SBCE	IPv4	10.64.101.243	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager Trunk 1	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager Trunk 108	IPv4	10.64.101.241	5068	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	IX Messaging	IPv4	10.64.101.158	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager Trunk 2	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager Trunk 98	IPv4	10.64.101.241	5065	TLS	FALSE	UP	200 OK	UP

Select : None

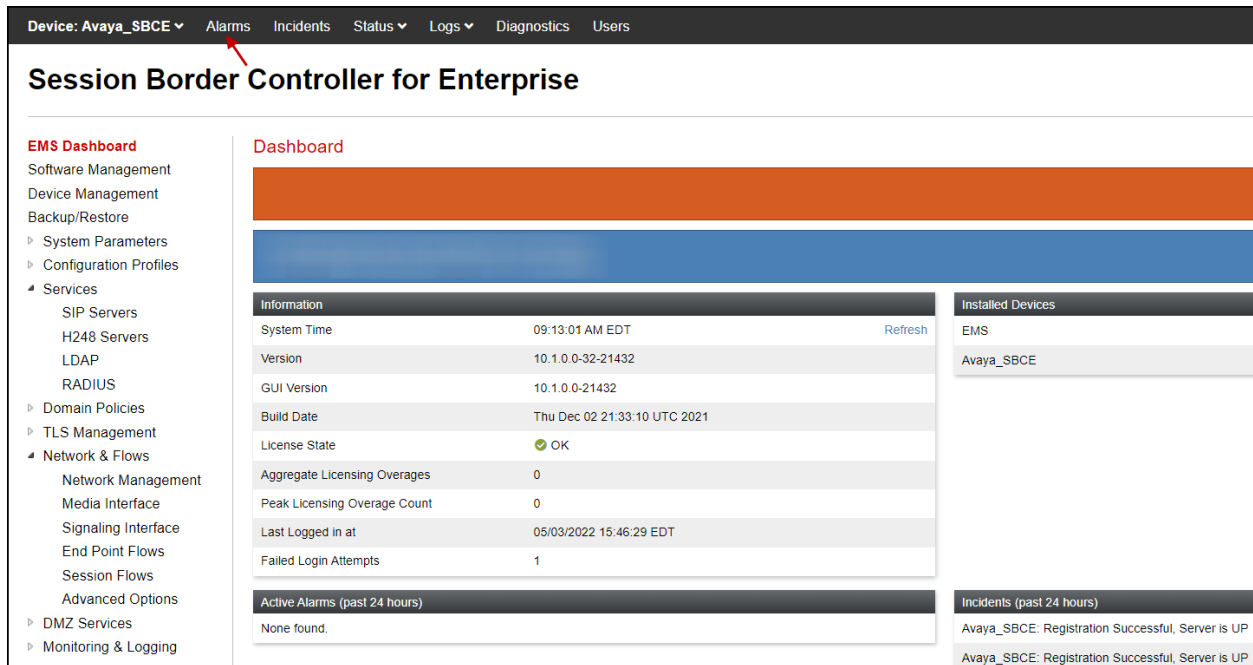
Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management 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, from the System Manager Home screen navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

9.4. Avaya SBCE Verification

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

Alarms: This screen provides information about the health of the SBC.



The screenshot shows the Avaya SBCE Dashboard. At the top, a dark navigation bar contains the text "Device: Avaya_SBCE" followed by a dropdown arrow, and then links for "Alarms", "Incidents", "Status", "Logs", "Diagnostics", and "Users". A red arrow points to the "Alarms" link. Below the navigation bar, the main heading is "Session Border Controller for Enterprise". On the left is a sidebar menu under "EMS Dashboard" with categories like Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services (SIP Servers, H248 Servers, LDAP, RADIUS), Domain Policies, TLS Management, Network & Flows (Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, Advanced Options), DMZ Services, and Monitoring & Logging. The main content area is titled "Dashboard" and features a large orange header bar. Below this, there are several sections: "Information" with a table of system details, "Installed Devices" with a list, "Active Alarms (past 24 hours)" showing "None found.", and "Incidents (past 24 hours)" showing two successful registration events.

Information		Refresh
System Time	09:13:01 AM EDT	
Version	10.1.0.0-32-21432	
GUI Version	10.1.0.0-21432	
Build Date	Thu Dec 02 21:33:10 UTC 2021	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/03/2022 15:46:29 EDT	
Failed Login Attempts	1	

Installed Devices
EMS
Avaya_SBCE

Active Alarms (past 24 hours)	
None found.	

Incidents (past 24 hours)	
Avaya_SBCE: Registration Successful, Server is UP	
Avaya_SBCE: Registration Successful, Server is UP	

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



The screenshot shows the Avaya SBCE Alarm Viewer page. At the top, a dark navigation bar contains "Device: Avaya_SBCE" with a dropdown arrow and a "Help" link. Below the navigation bar, there is a sidebar with "EMS" and "Avaya_SBCE" (the latter is highlighted with a red box). The main content area has a red "Alarms" tab. Below the tab is a table with columns: ID, Details, State, Time, and Device. The table is currently empty, displaying the message "No alarms found for this device." At the bottom of the table, there are two buttons: "Clear Selected" and "Clear All". The Avaya logo is visible in the top right corner of the main content area.

ID	Details	State	Time	Device
No alarms found for this device.				

Clear Selected Clear All

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

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents' (highlighted with a red arrow), 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar lists various management options under 'EMS Dashboard', including 'Services' and 'Network & Flows'. The main content area is titled 'Dashboard' and contains several sections: 'Information' (System Time, Version, GUI Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), 'Installed Devices' (listing 'Avaya_SBCE'), 'Active Alarms (past 24 hours)' (None found), and 'Incidents (past 24 hours)' (listing 'Avaya_SBCE: Registration Successful, Server is UP').

The following screen shows the Incident Viewer page.

The screenshot shows the 'Incident Viewer' page. The top navigation bar includes 'Device: Avaya_SBCE' and 'Help'. The page title is 'Incident Viewer' with the 'AVAYA' logo. Below the title, there is a 'Category' dropdown menu set to 'All', a 'Clear Filters' button, and 'Refresh' and 'Generate Report' buttons. The main content area is titled 'Summary' and displays a table of incidents. The table has columns for ID, Date & Time, Category, Type, and Cause. The table shows two entries: '825835107193461' and '825835047173505', both categorized as 'Policy' and 'Server Registration', with the cause being 'Registration Successful, Server is UP'. A scrollbar on the right indicates that there are more entries (1 to 15 of 2002).

Status: This screen provides the registration status of the servers.

Device: Avaya_SBCE ▾ Alarms Incidents **Status ▾** Logs ▾ Diagnostics Users

Session Border Controller for Enterprise

EMS Dashboard

- Software Management
- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
- ▾ Services
 - SIP Servers
 - H248 Servers
 - LDAP
 - RADIUS
- Domain Policies
- TLS Management
- ▾ Network & Flows
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows
 - Session Flows
 - Advanced Options
- DMZ Services
- Monitoring & Logging

Dashboard

Information	
System Time	09:13:01 AM EDT Refresh
Version	10.1.0.0-32-21432
GUI Version	10.1.0.0-21432
Build Date	Thu Dec 02 21:33:10 UTC 2021
License State	🟢 OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	05/03/2022 15:46:29 EDT
Failed Login Attempts	1

Active Alarms (past 24 hours)	
None found.	

Installed Devices	
EMS	
Avaya_SBCE	

Incidents (past 24 hours)	
Avaya_SBCE: Registration Successful, Server is UP	
Avaya_SBCE: Registration Successful, Server is UP	

The following screen shows the Clearcom server registration status.

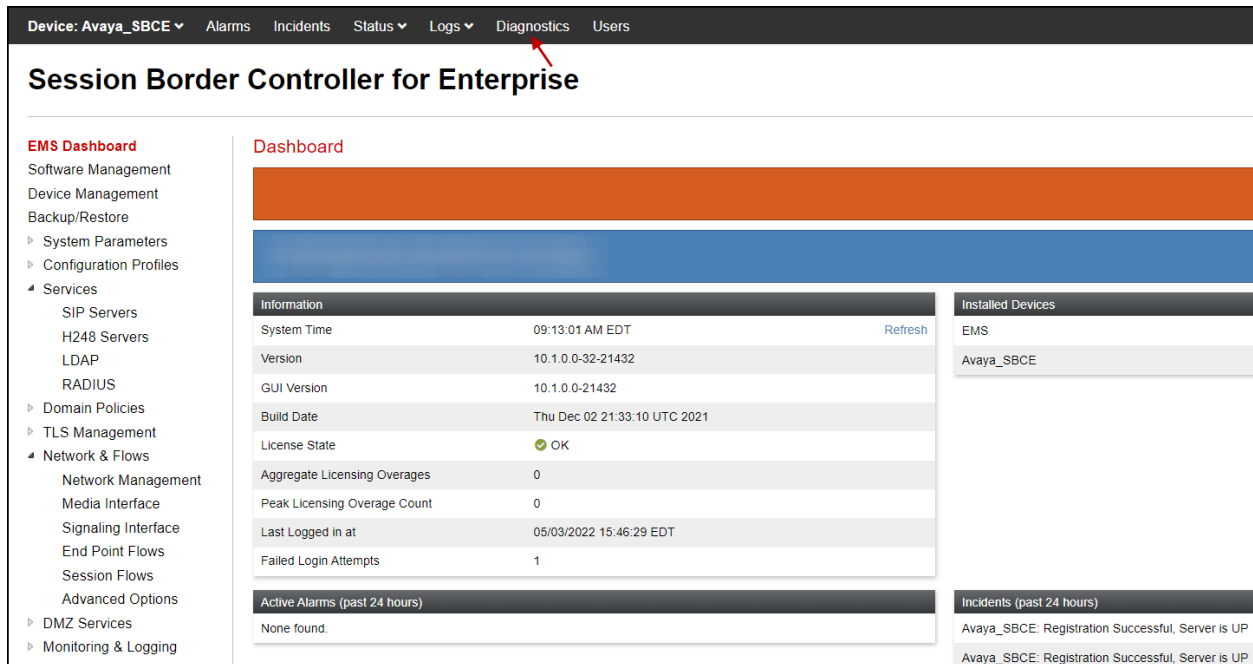
Device: Avaya_SBCE ▾ Help

Status

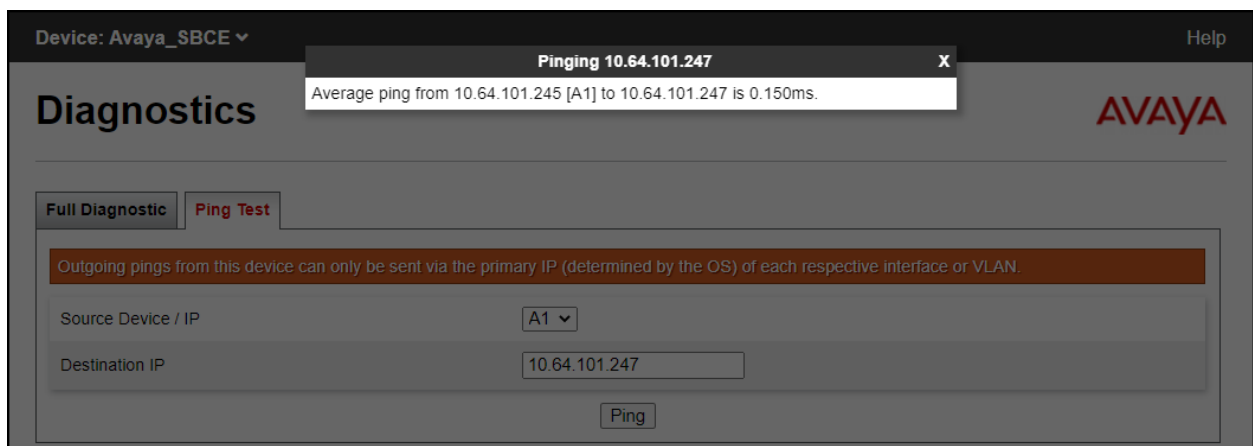
Server Status

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Service Provider TLS	sip.clearcom.mx	150.38.168	5061	TLS	UNKNOWN	REGISTERED	09/14/2022 10:18:46 EDT
Service Provider TLS	sip.clearcom.mx	175.6.202	5061	TLS	UNKNOWN	REGISTERED	09/14/2022 10:18:46 EDT

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 **Monitor & Logging → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

Note – Since TLS is being used inside of the enterprise (private network side) and outside of the enterprise (public network side) the Avaya SBCE internal packet capture tool shown below cannot be used since it cannot decrypt TLS encrypted data, instead the Avaya SBCE packet trace tool “**traceSBC**” should be used.

The screenshot shows the Avaya SBCE web interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo. A left sidebar lists various management options, with 'Monitoring & Logging' expanded to show 'Trace' in red. The main content area is titled 'Trace: Avaya_SBCE' and contains a 'Packet Capture' tab. Below this is a 'Packet Capture Configuration' form with the following fields: Status (Ready), Interface (Any), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Clearcom.pcap). 'Start Capture' and 'Clear' buttons are at the bottom right.

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address IP:Port	All
Remote Address *, *Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	Clearcom.pcap

Start Capture Clear

Once the capture is stopped, click 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.

Device: Avaya_SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Settings ▾

Help ▾

Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▾ Monitoring & Logging

SNMP

Syslog Management

Debugging

Trace

Log Collection

Trace: Avaya_SBCE

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified
Clearcom_20220504101452.pcap	286,720	May 4, 2022 at 10:15:06 AM EDT

Delete

10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller for Enterprise 10.1, to connect to the Clearcom SIP Trunking service, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Sections 2.1** and **2.2**.

11. References

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

- [1] *Deploying Avaya Aura® Communication Manager in a Virtualized Environment*, Release 10.1, Issue 3, April 2022.
- [2] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021.
- [3] *Administering Avaya Aura® System Manager* for Release 10.1.x, Issue 5, April 2022.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 10.1.x, Issue 2, March 2022.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 10.1., Issue 2, March 2022.
- [6] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022.
- [7] *Deploying Avaya Session Border Controller for Enterprise on a Virtualized Environment Platform*, Release 10.1, Issue 1, December 2021.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, Issue 1, December 2021.
- [9] Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 10.1 on the Avaya Aura® Platform - *Issue 1.0*.
- [10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 10.1.x, Issue 1, April 2022.
- [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 Scripts

Following are the Signaling Manipulation script that was used in the configuration of the Avaya SBCE. Add the scripts as instructed in **Sections 7.8**, enter a name for the script in the Title and copy/paste the entire scripts shown below.

```
//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
//Remove P-Location parameter
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"]);
remove(%HEADERS["P-Location"][1]);
}
}
```

©2022 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.