



Application Notes for Configuring Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.2 to support Alestra Enlace IP SIP Trunk Service on Sonus Platform– Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service on an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.2, to interoperate with the Alestra Enlace IP SIP Trunk service on Sonus Platform.

The Alestra Enlace IP SIP Trunk service provide customers with PSTN access via a SIP trunk between the enterprise and the service provider's 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 | 6 |
| 3. Reference Configuration | 7 |
| 4. Equipment and Software Validated | 10 |
| 5. Configure Avaya Aura® Communication Manager | 11 |
| 5.1. Licensing and Capacity | 11 |
| 5.2. System Features..... | 12 |
| 5.3. IP Node Names..... | 14 |
| 5.4. Codecs | 15 |
| 5.5. IP Network Regions | 17 |
| 5.6. Signaling Group | 18 |
| 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 | 31 |
| 6.1. System Manager Login and Navigation..... | 32 |
| 6.2. SIP Domain | 33 |
| 6.3. Locations | 33 |
| 6.4. Adaptations..... | 36 |
| 6.5. SIP Entities | 38 |
| 6.6. Entity Links | 41 |
| 6.7. Routing Policies | 43 |
| 6.8. Dial Patterns | 44 |
| 7. Configure Avaya Session Border Controller for Enterprise | 47 |
| 7.1. System Access..... | 47 |
| 7.2. System Management | 49 |
| 7.3. Network Management | 51 |
| 7.4. Media Interfaces | 52 |
| 7.5. Signaling Interfaces..... | 54 |
| 7.6. Server Interworking..... | 56 |
| 7.6.1. Server Interworking Profile – Enterprise..... | 56 |
| 7.6.2. Server Interworking Profile – Service Provider..... | 58 |
| 7.7. Server Configuration | 59 |
| 7.7.1. Server Configuration Profile – Enterprise | 59 |
| 7.7.2. Server Configuration Profile – Service Provider | 61 |
| 7.8. Routing..... | 63 |
| 7.8.1. Routing Profile – Enterprise | 63 |
| 7.8.2. Routing Profile – Service Provider | 64 |

| | | |
|---------|--|----|
| 7.9. | Topology Hiding | 65 |
| 7.9.1. | Topology Hiding Profile – Enterprise..... | 65 |
| 7.9.2. | Topology Hiding Profile – Service Provider | 67 |
| 7.10. | Domain Policies..... | 68 |
| 7.10.1. | Application Rules..... | 68 |
| 7.10.2. | Media Rules..... | 69 |
| 7.10.3. | Signaling Rules | 72 |
| 7.11. | End Point Policy Groups | 73 |
| 7.11.1. | End Point Policy Group – Enterprise | 73 |
| 7.11.2. | End Point Policy Group – Service Provider..... | 74 |
| 7.12. | End Point Flows..... | 75 |
| 7.12.1. | End Point Flow – Enterprise | 76 |
| 7.12.2. | End Point Flow – Service Provider | 77 |
| 8. | Alestra Enlace IP SIP Trunk Service Configuration..... | 78 |
| 9. | Verification and Troubleshooting | 78 |
| 9.1. | General Verification Steps | 78 |
| 9.2. | Communication Manager Verification..... | 78 |
| 9.3. | Session Manager Verification | 79 |
| 9.4. | Avaya SBCE Verification | 81 |
| 10. | Conclusion | 86 |
| 11. | References..... | 86 |

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service between the Alestra Enlace IP network and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Rel. 7.1 (Communication Manager), Avaya Aura® Session Manager Rel. 7.1 (Session Manager), Avaya Session Border Controller for Enterprise (Avaya SBCE) Rel. 7.2 and various Avaya endpoints, listed in **Section 4**.

The Alestra Enlace IP 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” and “Alestra” 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 Alestra Enlace IP 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.

2.1. Interoperability Compliance Testing

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

- Static IP SIP Trunk authentication.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using “This Computer” and “Other Phone” modes (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Equinox softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 Deskphones (Note that only the 96x1 SIP Deskphones was used to test remote worker functionality).
- Codecs G.729, G.711A and G.711MU.
- Inbound and outbound PSTN calls using VoIP media resources in Avaya Media Gateways and the Avaya Aura® Media Server at the enterprise network.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Proper response/error treatment to different failure conditions.

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.

The following items were not tested:

- “0” operator and “0+10” digits operator assisted calls are not supported by Alestra.
- Network Call Redirection using the REFER or 302 Temporarily Unavailable methods are not supported by Alestra and they were not tested.
- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test.
- T.38 fax is not supported by the Alestra.

2.2. Test Results

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

- **Caller ID on incoming calls from the U.S.:** Calls originating from PSTN telephones in the U.S. to the DID numbers in Mexico assigned to the SIP trunk to the enterprise displayed ***Restricted/Unavailable*** on the enterprise extensions. This seems to be a PSTN restriction for all calls from the U.S. to Mexico, not limited just to Alestra. Inbound calls originating from local PSTN test numbers in Monterrey, Mexico showed the correct calling party caller ID.
- **Caller ID on outbound calls:** On calls originating from enterprise extensions to PSTN telephones, the caller ID number shown on the PSTN endpoint was always the BDN or main DID number assigned by Alestra to the SIP trunk, not the specific DID assigned to that extension. This includes incoming calls that are forwarded or transferred back on the SIP trunk to the PSTN, and also EC500 (extension to cellular) calls. This is the expected behavior on the Alestra service for outbound calls on the SIP trunk; it is listed here simply as an observation.
- **Outbound Calling Party Number (CPN) Block:** When an enterprise user activated “CPN Block” on an outbound call with the purpose of privacy, Communication Manager sent “anonymous” in the “From” header and included the “Privacy:id” header, but on the receiving end at the PSTN the display still showed the BDN number assigned by Alestra to the SIP trunk.
- **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 purposes 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**).

2.3. Support

For support on Alestra Enlace IP SIP Trunk Service visit the corporate Web page at:

<http://www.alestra.com.mx>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Alestra Enlace IP SIP Trunk Service through a public Internet WAN connection.

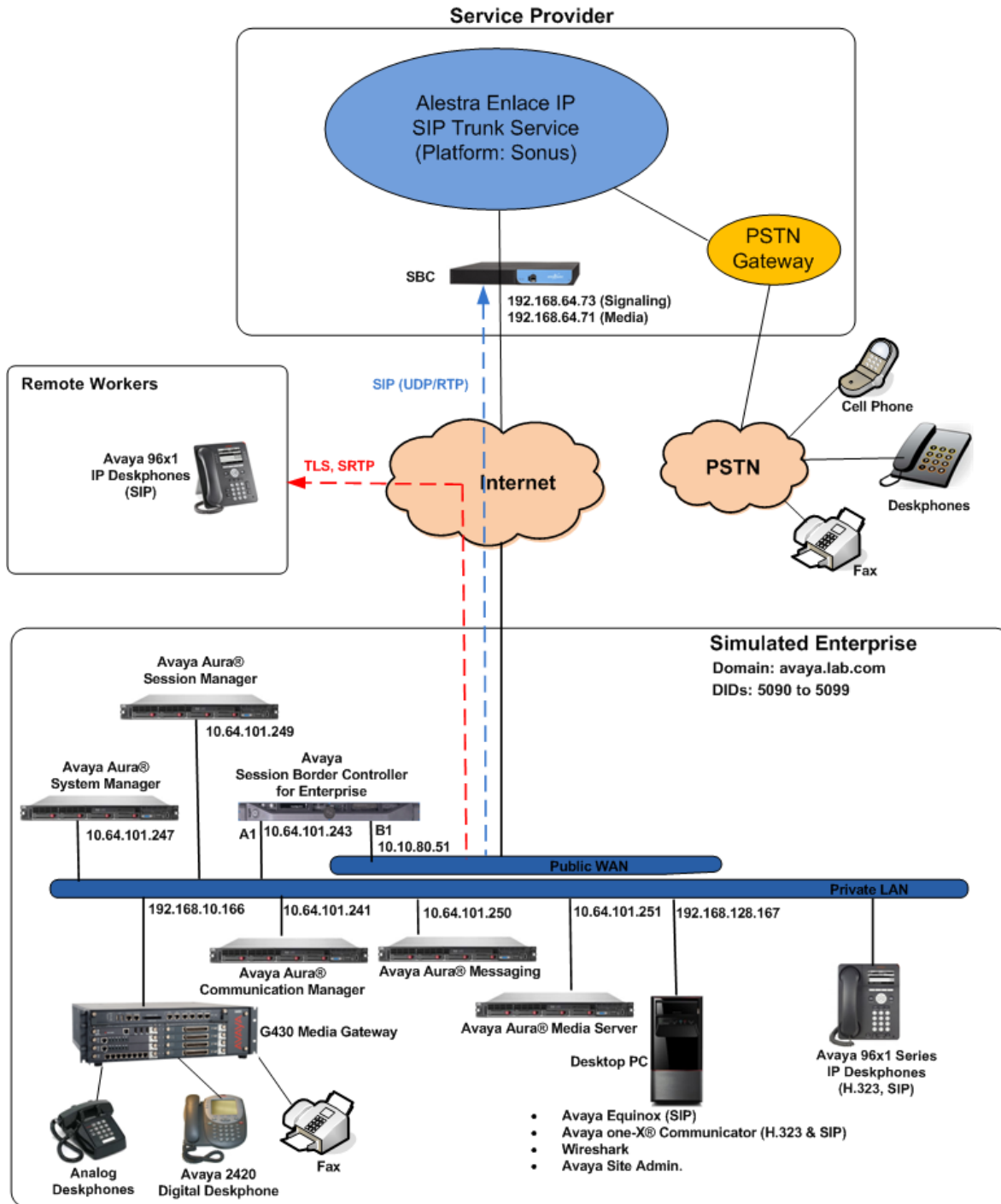


Figure 1: Avaya SIP Enterprise Solution connected to Alestra Enlace IP SIP Trunk Service

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 Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Equinox softphone (SIP).
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the 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 96x1 SIP Deskphones. For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on Avaya 96x1 SIP Deskphones used to test remote worker functionality. 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 [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 (in this case Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

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 Alestra 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.

As part of the Avaya Aura® version 7.1 release, 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.

Avaya Aura® 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 Messaging are not directly related to the interoperability tests with the Alestra Enlace IP network SIP Trunk service, they are not included in these Application Notes.

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 only (private 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.

For the compliance testing associated with this Application Note, the interface between the Avaya system and the Alestra network did not include the use of any specific encryption features, UDP Transport for signaling and RTP for media was used between the Avaya system and the Alestra network across the SIP Trunk. TLS transport for signaling and SRTP for media was used inside of the enterprise (private network side, in between Avaya components).

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 | 7.1.1.0.0 (01.0.532.0-23985) |
| Avaya Aura® Session Manager | 7.1.1.0 (7.1.1.0.711008) |
| Avaya Aura® System Manager | 7.1.1.0 Build No. 7.1.0.0.1125193 Software Update Rev. No. 7.1.1.0.046931 |
| Avaya Session Border Controller for Enterprise | ASBCE 7.2 7.2.0.0-18-13712 |
| Avaya Aura® Messaging | 7.0 Service Pack 0 (MSG-00.0.441.0-017_0004) |
| Avaya Aura® Media Server | 7.8.0.333 SP5 7.8.0.333_2017.07.17 |
| Avaya G430 Media Gateway | G430_sw_38_20_1 |
| Avaya 96x1 Series IP Deskphones (SIP) | Version 7.1.1.0.9 |
| Avaya 96x1 Series IP Deskphones (H.323) | Version 6.6506 |
| Avaya one-X® Communicator (H.323, SIP) | 6.2.12.04-SP12 |
| Avaya Equinox (SIP) | 3.2.2.2 |
| Avaya 2420 Series Digital Deskphones | N/A |
| Avaya 6210 Analog Deskphones | N/A |
| Alestra | |
| Sonus Soft switch | V08.04.09R000 |
| Oracle SBC | V6.2 |
| Lucent 5ESS | V16.1 |

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 6.0.0) 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 Alestra Enlace IP network SIP Trunk 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 Aura® 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 captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

5.1. Licensing and Capacity

Use the **display system-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 **24000** licenses are available and **120** 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
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 41000 0
      Maximum Video Capable IP Softphones: 18000 7
      Maximum Administered SIP Trunks: 24000 120
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0

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

5.2. System Features

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

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? 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? no
      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.

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

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

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

INTERNATIONAL CALL ROUTING PARAMETERS
  Local Country Code:       
  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. Alestra 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: | G.729 | n | 2 | 20 |
| 2: | G.711A | n | 2 | 20 |
| 3: | G.711MU | n | 2 | 20 |
| 4: | | - | - | |
| 5: | | - | - | |
| 6: | | - | - | |
| 7: | | - | - | |

Media Encryption

Encrypted SRTP: best-effort

1: 1-srtp-aescm128-hmac80

2: none

3:

4:

5:

On **Page 2**, set the **Fax Mode** to *off* (refer to **Section 2.1**).

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: <u>avaya.lab.com</u> | |
| Name: <u>SP Region</u> | Stub Network Region: <u>n</u> | |
| MEDIA PARAMETERS | | |
| Codec Set: <u>2</u> | Intra-region IP-IP Direct Audio: <u>yes</u> | |
| | Inter-region IP-IP Direct Audio: <u>yes</u> | |
| UDP Port Min: <u>2048</u> | IP Audio Hairpinning? <u>n</u> | |
| UDP Port Max: <u>3349</u> | | |
| DIFFSERV/TOS PARAMETERS | | |
| Call Control PHB Value: <u>46</u> | | |
| Audio PHB Value: <u>46</u> | | |
| Video PHB Value: <u>26</u> | | |
| 802.1P/Q PARAMETERS | | |
| Call Control 802.1p Priority: <u>6</u> | | |
| Audio 802.1p Priority: <u>6</u> | | |
| Video 802.1p Priority: <u>5</u> | | |
| H.323 IP ENDPOINTS | | AUDIO RESOURCE RESERVATION PARAMETERS |
| H.323 Link Bounce Recovery? <u>y</u> | | RSVP Enabled? <u>n</u> |
| Idle Traffic Interval (sec): <u>20</u> | | |
| Keep-Alive Interval (sec): <u>5</u> | | |
| Keep-Alive Count: <u>5</u> | | |

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 | codec | direct | WAN-BW-limits | Video | Intervening | Dyn | G | A | | G | A | t |
| rgn | set | WAN | Units | Total | Norm | Prio | Shr | Regions | CAC | R | L | e |
| 1 | <u>2</u> | 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*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- 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 | | |
| 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 21
                                     TRUNK GROUP
Group Number: 2      Group Type: sip      CDR Reports: y
Group Name: Service Provider      COR: 1      TN: 1      TAC: 602
Direction: two-way      Outgoing Display? n
Dial Access? n      Night Service: _____
Queue Length: 0
Service Type: public-ntwrk      Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 2
                                     Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** 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 21 |
| Group Type: sip | |
| TRUNK PARAMETERS | |
| Unicode Name: <u>auto</u> | |
| Redirect On OPTIM Failure: <u>5000</u> | |
| SCCAN? <u>n</u> | Digital Loss Group: <u>18</u> |
| Preferred Minimum Session Refresh Interval(sec): <u>600</u> | |
| Disconnect Supervision - In? <u>y</u> Out? <u>y</u> | |
| XOIP Treatment: <u>auto</u> Delay Call Setup When Accessed Via IGAR? <u>n</u> | |
| Caller ID for Service Link Call to H.323 1xC: <u>station-extension</u> | |

On Page 3:

- Set the **Numbering Format** field to *private*. This field specifies the format of the calling party number (CPN) sent to the far-end. When *public* format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. To keep uniformity with the format used by Alestra, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-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 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none
                                                         Maintenance Tests? y

  Suppress # Outpulsing? n   Numbering Format: private
                                                         UI Treatment: service-provider
                                                         Replace Restricted Numbers? y
                                                         Replace Unavailable Numbers? y
                                                         Hold/Unhold Notifications? y
  Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y
```

On Page 4:

- Set the **Network Call Redirection** field to *n*. With this setting, Communication Manager will not use the REFER method, which is not supported by Alestra, for the redirection of PSTN calls that are transferred back to the SIP trunk (refer to **Section 2.1**)
- 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 Alestra.
- Set the **Convert 180 to 183 for Early Media?** to *y*.
- 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 21 |
|---|------------------------------|
| PROTOCOL VARIATIONS | |
| Mark Users as Phone? | <u>n</u> |
| Prepend '+' to Calling/Alerting/Diverting/Connected Number? | <u>n</u> |
| Send Transferring Party Information? | <u>n</u> |
| Network Call Redirection? | <u>n</u> |
| Send Diversion Header? | <u>n</u> |
| Support Request History? | <u>n</u> |
| Telephone Event Payload Type: | <u>101</u> |
| Convert 180 to 183 for Early Media? | <u>y</u> |
| Always Use re-INVITE for Display Updates? | <u>n</u> |
| Identity for Calling Party Display: | <u>P-Asserted-Identity</u> |
| Block Sending Calling Party Location in INVITE? | <u>n</u> |
| Accept Redirect to Blank User Destination? | <u>n</u> |
| Enable Q-SIP? | <u>n</u> |
| Interworking of ISDN Clearing with In-Band Tones: | <u>keep-channel-active</u> |
| Request URI Contents: | <u>may-have-extra-digits</u> |

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-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, three DID numbers were assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

| change private-numbering 1 | | | | | Page 1 of 2 |
|----------------------------|----------|------------|----------------|-----------|---|
| NUMBERING - PRIVATE FORMAT | | | | | |
| Ext Len | Ext Code | Trk Grp(s) | Private Prefix | Total Len | |
| 4 | 3 | | | 4 | Total Administered: 5 Maximum Entries: 540 |
| 4 | 5 | | | 4 | |
| 4 | 3037 | 2 | 5512535093 | 10 | |
| 4 | 3040 | 2 | 5512535091 | 10 | |
| 4 | 3042 | 2 | 5512535092 | 10 | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |
| — | — | — | — | — | |

Note - During the compliance test, Alestra inserted the BDN or main DID number assigned to the SIP trunk on all outbound calls sent to the PSTN, for caller ID purposes. Since the calling party information sent from the enterprise was not used for caller ID or authentication purposes by Alestra, the configuration shown on the screen above was not strictly required, and it is shown here simply for completeness.

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Alestra 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.

| change inc-call-handling-trmt trunk-group 2 | | | | | Page | 1 of | 30 |
|---|---------------|------------------|-----|--------|------|------|----|
| INCOMING CALL HANDLING TREATMENT | | | | | | | |
| Service/ Feature | Number Len | Number Digits | Del | Insert | | | |
| public-ntwrk | 10 | 5512535091 | 10 | 3040 | | | |
| public-ntwrk | 10 | 5512535092 | 10 | 3042 | | | |
| public-ntwrk | 10 | 5512535093 | 10 | 3037 | | | |
| public-ntwrk | 10 | 5512535094 | 10 | 3046 | | | |
| public-ntwrk | 10 | 5512535095 | 10 | 3045 | | | |
| public-ntwrk | 10 | 5512535096 | 10 | 3777 | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |
| public-ntwrk | — | — | — | — | | | |

5.10. Outbound Routing

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

| change dialplan analysis | | | DIAL PLAN ANALYSIS TABLE | | | | | | Page 1 of 12 |
|--------------------------|--------------|-----------|--------------------------|--------------|-----------|-----------------|--------------|-----------|--------------|
| | | | Location: all | | | Percent Full: 2 | | | |
| Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | |
| 0 | 13 | udp | | | | | | | |
| 1 | 4 | dac | | | | | | | |
| 2 | 4 | ext | | | | | | | |
| 3 | 4 | ext | | | | | | | |
| 4 | 4 | udp | | | | | | | |
| 5 | 4 | ext | | | | | | | |
| 6 | 3 | dac | | | | | | | |
| 7 | 4 | ext | | | | | | | |
| 8 | 1 | fac | | | | | | | |
| 9 | 1 | fac | | | | | | | |
| * | 3 | dac | | | | | | | |
| # | 2 | dac | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

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

| change feature-access-codes | | Page 1 of 10 |
|---|------------------|----------------------|
| FEATURE ACCESS CODE (FAC) | | |
| Abbreviated Dialing List1 Access Code: | _____ | |
| Abbreviated Dialing List2 Access Code: | _____ | |
| Abbreviated Dialing List3 Access Code: | _____ | |
| Abbreviated Dial - Prgm Group List Access Code: | _____ | |
| Announcement Access Code: | #7 | |
| Answer Back Access Code: | _____ | |
| Attendant Access Code: | _____ | |
| Auto Alternate Routing (AAR) Access Code: | 8 | |
| Auto Route Selection (ARS) - Access Code 1: | 9 | Access Code 2: _____ |
| Automatic Callback Activation: | _____ | Deactivation: _____ |
| Call Forwarding Activation Busy/DA: | _____ All: _____ | Deactivation: _____ |
| Call Forwarding Enhanced Status: | _____ Act: _____ | Deactivation: _____ |
| Call Park Access Code: | _____ | |
| Call Pickup Access Code: | _____ | |
| 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.

| change ars analysis 001 | | | | | | | Page 1 of 2 |
|--------------------------|-----------|-----------|---------------|-----------|----------|-----------|-----------------|
| ARS DIGIT ANALYSIS TABLE | | | | | | | |
| Location: all | | | | | | | Percent Full: 0 |
| Dialed String | Total Min | Total Max | Route Pattern | Call Type | Node Num | ANI Req'd | |
| 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 | |
| 101xxxx0 | 8 | 8 | deny | op | | n | |
| 101xxxx0 | 18 | 18 | deny | op | | n | |
| 101xxxx01 | 16 | 24 | deny | iop | | n | |
| 101xxxx011 | 17 | 25 | deny | intl | | n | |
| 101xxxx1 | 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 | |

- **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 *unk-unk*. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

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

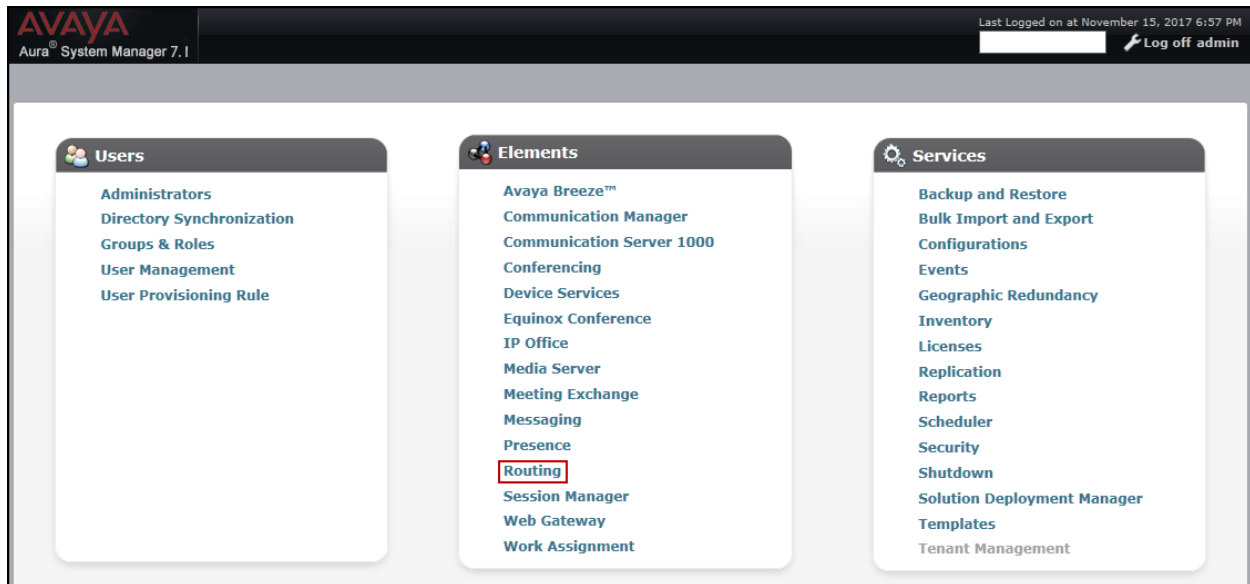
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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.

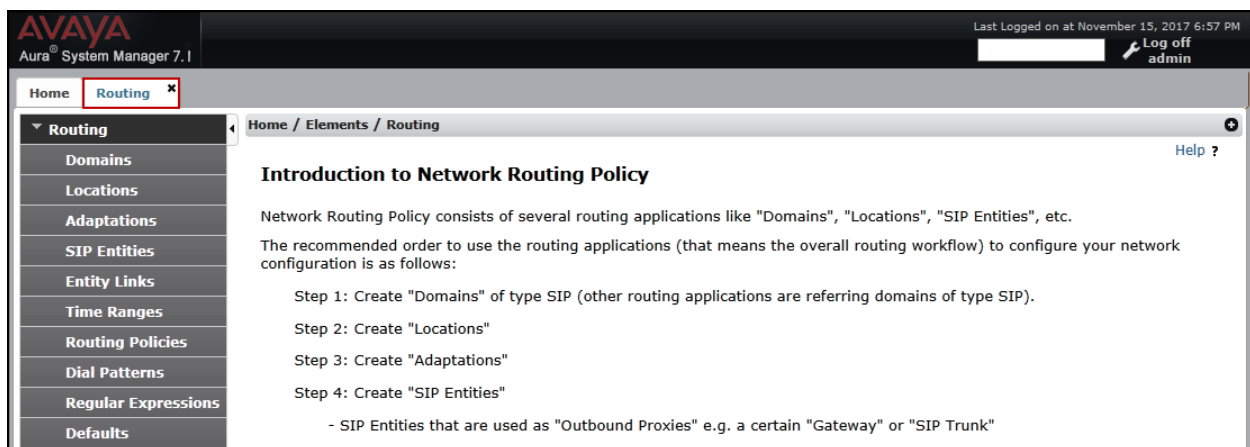
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

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; click on **Routing**.



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



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.

The screen below shows the entry for the enterprise domain.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top header includes the Avaya logo and 'Aura® System Manager 7.1'. The right header shows 'Last Logged on at November 15, 2017 6:57 PM' and a 'Log off admin' button. The left navigation pane has 'Home' and 'Routing' tabs, with 'Routing' selected. Under 'Routing', 'Domains' is highlighted. The main content area is titled 'Domain Management' and shows 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'. The table is filtered by 'Enable'.

| 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 7.1 web interface. The top navigation bar includes the Avaya logo, the text "Aura® System Manager 7.1", and a "Last Logged on at November 15, 2017 6:57 PM" timestamp. A "Log off admin" button is visible. The left sidebar contains a menu with "Routing" selected and highlighted. The main content area shows the "Location Details" page for "Session Manager". The "General" section includes a red-bordered input field for "* Name:" containing "Session Manager" and a "Notes:" field containing "VMware Session Manager". Below this is the "Dial Plan Transparency in Survivable Mode" section, which has an "Enabled:" checkbox (unchecked), a "Listed Directory Number:" field, and an "Associated CM SIP Entity:" field. "Commit" and "Cancel" buttons are located in the top right corner of the form area.

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.

This screenshot shows the same Avaya Aura System Manager 7.1 interface as the previous one, but for the "Communication Manager" location. The "Routing" menu item is still selected in the sidebar. In the "Location Details" page, the "* Name:" field now contains "Communication Manager" and the "Notes:" field contains "VMware Communication Manager". The "Dial Plan Transparency in Survivable Mode" section remains unchanged with the "Enabled:" checkbox unchecked. The "Commit" and "Cancel" buttons are still present in the top right.

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 7.1 web interface. The top header shows the Avaya logo and 'Aura System Manager 7.1'. The user is logged in as 'admin' on November 15, 2017, at 6:57 PM. The breadcrumb trail is 'Home / Elements / Routing / Locations'. The left sidebar menu has 'Routing' expanded, with 'Locations' selected. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, the '* Name' field is set to 'Avaya SBCE' and the 'Notes' field is 'VMware Avaya SBCE'. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox that is unchecked. Below this, there are input fields for 'Listed Directory Number' and 'Associated CM SIP Entity'.

AVAYA
Aura System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM
Log off admin

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

Help ?

General

* Name: Avaya SBCE

Notes: VMware Avaya SBCE

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

6.4. Adaptations

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

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

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.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user session summary showing 'Last Logged on at November 15, 2017 6:57 PM' and a 'Log off admin' button. The left sidebar contains a menu with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Adaptations' (highlighted with a red box), 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Adaptation Details' with a breadcrumb trail 'Home / Elements / Routing / Adaptations'. It features 'Commit' and 'Cancel' buttons and a 'Help ?' link. Under the 'General' tab, the 'Adaptation Name' is 'CM_Outbound_Header_Removal', the 'Module Name' is 'DigitConversionAdapter' (selected from a dropdown), and the 'Module Parameter Type' is 'Name-Value Parameter' (selected from a dropdown). Below these fields is a table with 'Add' and 'Remove' buttons. The table has two columns: 'Name' and 'Value'. One row is visible with 'Name' 'eRHdrs' and 'Value' '"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P-'. A 'Select : All, None' option is at the bottom of the table.

| Name | Value |
|--------|--|
| eRHdrs | "Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P- |

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 shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home', 'Routing', and 'SIP Entities'. The left sidebar lists various configuration areas, with 'SIP Entities' selected. The main content area displays the 'SIP Entity Details' form. The form has a 'General' section with the following fields: 'Name' (Session Manager), 'FQDN or IP Address' (10.64.101.249), 'Type' (Session Manager), 'Notes' (VMware Session Manager), 'Location' (Session Manager), 'Outbound Proxy' (empty), 'Time Zone' (America/New_York), and 'Minimum TLS Version' (Use Global Setting). The 'Commit' and 'Cancel' buttons are located at the top right of the form.

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**. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user status area showing 'Last Logged on at November 15, 2017 6:57 PM' and a 'Log off admin' button. A breadcrumb trail reads 'Home / Elements / Routing / SIP Entities'. The left sidebar contains a menu with 'Routing' selected, and sub-items including 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible:

- * Name: Communication Manager Trunk 2
- * FQDN or IP Address: 10.64.101.241
- Type: CM (dropdown menu)
- Notes: Used for SP Testing
- Adaptation: (dropdown menu)
- Location: Communication Manager (dropdown menu)
- Time Zone: America/New_York (dropdown menu)

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**).
- 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**.

AVAYA
Aura® System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM
Log off
admin

Home Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* 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

6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left 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.

AVAYA
Aura® System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM
Log off admin

Home Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

| <input type="checkbox"/> | Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | DNS Override | Connection Policy |
|--------------------------|----------------------|-------------------|----------|--------|---------------------------------|--------|--------------------------|-------------------|
| <input type="checkbox"/> | * Session_Manager_Ch | * Session Manager | TLS | * 5071 | * Communication Manager Trunk 2 | * 5071 | <input type="checkbox"/> | trusted |

Select : All, None

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

AVAYA
Aura® System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM
Log off admin

Home Routing

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

| <input type="checkbox"/> | Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | DNS Override | Connection Policy |
|--------------------------|------------------------|-----------------|----------|----------|--------------|----------|--------------------------|-------------------|
| <input type="checkbox"/> | * Session_Manager_AS * | Session Manager | TLS | * 5061 * | Avaya SBCE | * 5061 * | <input type="checkbox"/> | trusted |

Select : All, None

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 to the Avaya SBCE. 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 7.1

Last Logged on at November 15, 2017 6:57 PM

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

* Name: To CM Trunk 2

Disabled: ☐

* Retries: 0

Notes: For inbound calls to CM via Trunk

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 |

AVAYA
Aura® System Manager 7.1

Last Logged on at November 21, 2017 8:32 AM

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

* Name: Avaya SBCE

Disabled: ☐

* Retries: 0

Notes: For outbound calls to SP via ASB

SIP Entity as Destination

Select

| Name | FQDN or IP Address | Type | Notes |
|------------|--------------------|-----------|-------------------|
| Avaya SBCE | 10.64.101.243 | SIP Trunk | VMware Avaya SBCE |

6.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select “**ALL**” to route incoming calls to all SIP domains.
- **Notes:** Add a brief description (optional).
- In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria (**Section 6.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 6.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with **5512**, arriving from location **Avaya SBCE**, used route policy **Communication Manager trunk 2** to Communication Manager.

AVAYA
Aura® System Manager 7.1

Last Logged on at November 21, 2017 8:32 AM

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel Help ?

General

* Pattern: 5512

* Min: 4

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.lab.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

| | Originating Location Name | Originating Location 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 |

Select : All, None

Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The example in this screen shows the 13 digit dialed numbers for outbound international 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 7.1

Last Logged on at November 21, 2017 8:32 AM

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel Help ?

General

* Pattern: 001

* Min: 13

* Max: 13

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.lab.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

| | Originating Location Name | Originating Location 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 this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

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 **Additional 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 for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' below it. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field. Below the input field is a 'Continue' button. Further down, there is a 'WELCOME TO AVAYA SBC' message, 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 a consent statement: '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, it says '© 2011 - 2017 Avaya Inc. All rights reserved.'

Once logged in, the Dashboard screen is presented. 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.

AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

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

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

| | | |
|------------------------------|-----------------------------|---------|
| | | |
| System Time | 12:45:10 PM EST | Refresh |
| Version | 7.2.0.0-18-13712 | |
| Build Date | Thu Jun 1 00:12:50 UTC 2017 | |
| License State | ✔ OK | |
| Aggregate Licensing Overages | 0 | |
| Peak Licensing Overage Count | 0 | |
| Last Logged in at | 11/21/2017 12:42:59 EST | |
| Failed Login Attempts | 0 | |

| |
|------------|
| |
| EMS |
| Avaya_SBCE |

| |
|-------------|
| |
| None found. |

| |
|---|
| |
| Avaya_SBCE : No Subscriber Flow Matched |

HG; Reviewed:
SPOC 12/21/2017

Solution & Interoperability Test Lab Application Notes
©2017 Avaya Inc. All Rights Reserved.

48 of 87
AISO_CMSM71SBC72

7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single 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 Session Border Controller for Enterprise (SBCE) management interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management (highlighted), Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The 'System Management' section contains tabs for Devices, Updates, SSL VPN, Licensing, and Key Bundles. The 'Devices' tab is active, showing a table with the following data:

| Device Name | Management IP | Version | Status | |
|-------------|---------------|------------------|--------------|---|
| Avaya_SBCE | [Blurred] | 7.2.0.0-18-13712 | 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.

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 |

License Allocation

| | |
|-----------------------|-------------------------------------|
| Standard Sessions | 2000 |
| Requested: 2000 | |
| Advanced Sessions | 2000 |
| Requested: 2000 | |
| Scopia Video Sessions | 500 |
| Requested: 500 | |
| CES Sessions | 0 |
| Requested: 0 | |
| Transcoding Sessions | 0 |
| Requested: 0 | |
| Encryption | <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 | 8.8.8.8 |
| Secondary DNS | 7.7.7.7 |
| DNS Location | DMZ |
| DNS Client IP | 10.10.80.23 |

Management IP(s)

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

The highlighted IP addresses in the **System Information** screen are the ones used for the SIP trunk to Alestra, 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. 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 **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, **Avaya_SBCE** in the sample configuration. 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.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar contains a menu with 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', 'Device Specific Settings' (expanded), 'Network Management' (selected), and 'Media Interface'. The main content area is titled 'Network Management: Avaya_SBCE' and has two tabs: 'Interfaces' and 'Networks' (selected). Under the 'Networks' tab, there is an 'Add' button and a table with the following data:

| Name | Gateway | Subnet Mask / Prefix Length | Interface | IP Address | Edit | Delete |
|------------|-------------|-----------------------------|-----------|---------------|------|--------|
| Network_A1 | 10.64.101.1 | 255.255.255.0 | A1 | 10.64.101.243 | Edit | Delete |
| Network_B1 | 10.10.80.1 | 255.255.255.128 | B1 | 10.10.80.51 | Edit | Delete |

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.

7.4. 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 **Device Specific Settings** menu on the left-hand side, select the device being managed and 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**.

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.
- Click **Finish**.

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

- Name:** A text input field containing "Public_med".
- IP Address:** A dropdown menu showing "Network_B1 (B1, VLAN 0)" with a downward arrow. Below it, a sub-dropdown menu shows "10.10.80.51" with a downward arrow.
- Port Range:** Two text input boxes. The first contains "35000" and the second contains "40000", separated by a hyphen.
- TLS Profile:** A dropdown menu showing "None" with a downward arrow.
- Finish:** A button located at the bottom center of the window.

A red rectangular box highlights the "Name", "IP Address", and "Port Range" fields.

7.5. 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 **Device Specific Settings** menu on the left-hand side, select the device being managed and 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** (See Note below).
- Click **Finish**.

The screenshot shows the 'Add Signaling Interface' configuration window. The window has a title bar 'Add Signaling Interface' with a close button 'X'. It contains several input fields and a 'Finish' button. Two red boxes highlight specific sections: the first box encloses the 'Name' field (containing 'Private_sig'), the 'IP Address' dropdown (showing 'Network_A1 (A1, VLAN 0)' and '10.64.101.243'), and the 'TCP Port' field (empty). The second box encloses the 'TLS Port' field (containing '5061') and the 'TLS Profile' dropdown (showing 'New_ServiceProvider_Server_TLS'). Other fields include 'UDP Port' (empty), 'Enable Shared Control' (checkbox), and 'Shared Control Port' (empty).

Note - As previously mentioned, the configuration tasks required to support TLS transport for signaling and SRTP for media inside of the enterprise (private network side) are beyond the scope of these Application Notes; hence they are not discussed in this document

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 **5060** for **UDP Port**, since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.
- Click **Finish**.

Add Signaling Interface X

| | |
|------------------------------------|-------------------------------------|
| Name | Public_sig |
| IP Address | Network_B1 (B1, VLAN 0) 10.10.80.51 |
| TCP Port Leave blank to disable | |
| UDP Port Leave blank to disable | 5060 |
| TLS Port Leave blank to disable | |
| TLS Profile | None |
| Enable Shared Control | <input type="checkbox"/> |
| Shared Control Port | |

Finish

7.6. 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).

7.6.1. 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 **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select *avaya-ru* from the list of pre-defined profiles. Click **Clone**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the Avaya logo. The left navigation pane lists various configuration areas, with 'Global Profiles' expanded and 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: avaya-ru' and features a list of profiles on the left, including 'cs2100', 'avaya-ru' (highlighted), 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd...', 'Avaya-SM', 'SP-General', 'Avaya-IPO', 'Avaya-CS1000', and 'Avaya-CM'. A 'Clone' button is visible. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, the 'General' tab is active, displaying a table of settings:

| Setting | Value |
|--------------------------|-------|
| Hold Support | NONE |
| 180 Handling | None |
| 181 Handling | None |
| 182 Handling | None |
| 183 Handling | None |
| Refer Handling | No |
| URI Group | None |
| Send Hold | No |
| Delayed Offer | No |
| 3xx Handling | No |
| Diversion Header Support | No |
| Delayed SDP Handling | No |
| Re-Invite Handling | No |

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

The 'Clone Profile' dialog box is shown with the following fields:

- Profile Name: avaya-ru
- Clone Name: Avaya-SM (with a red box around the input field and a clear 'x' button)

A 'Finish' button is located at the bottom of the dialog.

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries. The **Advanced** tab settings are shown on the screen below:

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various configuration categories, with 'Global Profiles' and 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left, including 'Avaya-SM' which is selected. The right-hand pane shows the configuration for the selected profile, with tabs for General, Timers, Privacy, URI Manipulation, Header Manipulation, and Advanced. The Advanced tab is active, displaying settings for Record Routes, Include End Point IP for Context Lookup, Extensions, Diversion Manipulation, Has Remote SBC, Route Response on Via Port, Relay INVITE Replace for SIPREC, and DTMF Support.

| Interworking Profiles: Avaya-SM | |
|---|------------|
| 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 |
| DTMF | |
| DTMF Support | None |

7.6.2. 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**, then click **Finish** on the last tab leaving remaining fields with default values (not shown).



The screenshot shows a dialog box titled "Interworking 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 "SP-General". A red rectangle highlights the "Profile Name" field and its label. Below the input field, there is a "Next" button.

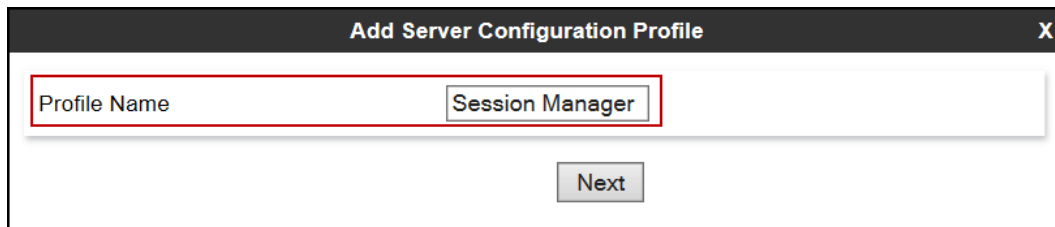
7.7. Server Configuration

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

7.7.1. Server Configuration Profile – Enterprise

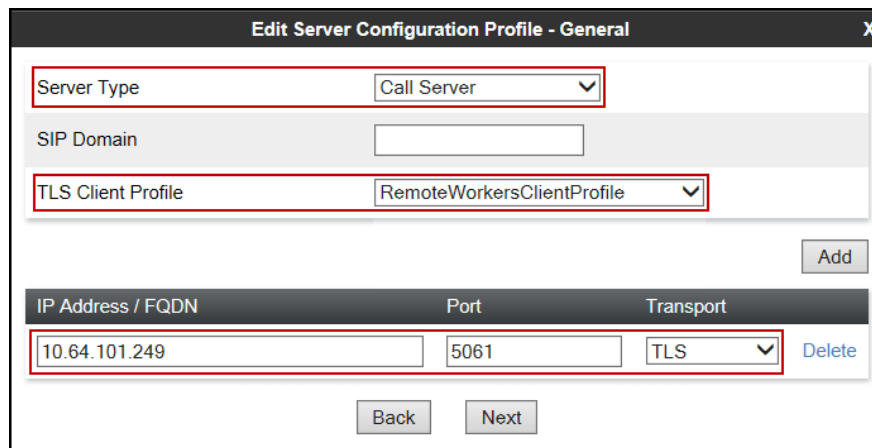
From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server.

- 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 is a button labeled "Next".

- On the **Edit Server Configuration Profile – General** tab select *Call Server* from the drop down menu under the **Server Type**.
- Select a **TLS Profile**.
- 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**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and a table. The "Server Type" dropdown is set to "Call Server". The "SIP Domain" field is empty. The "TLS Client Profile" dropdown is set to "RemoteWorkersClientProfile". Below these fields is an "Add" button. A table with three columns: "IP Address / FQDN", "Port", and "Transport" is shown. The first row of the table has the values "10.64.101.249", "5061", and "TLS". A "Delete" button is next to the first row. At the bottom of the dialog are "Back" and "Next" buttons.

- Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown).
- Select **Avaya-SM** from the **Interworking Profile** drop down menu.
- Click **Finish**.

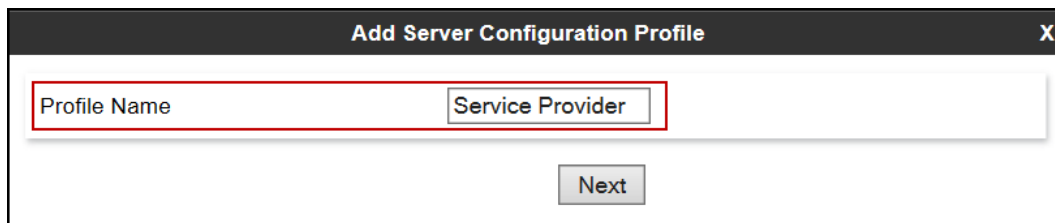
Add Server Configuration Profile - Advanced X

| | |
|-------------------------------|--------------------------|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input 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 ▼ |

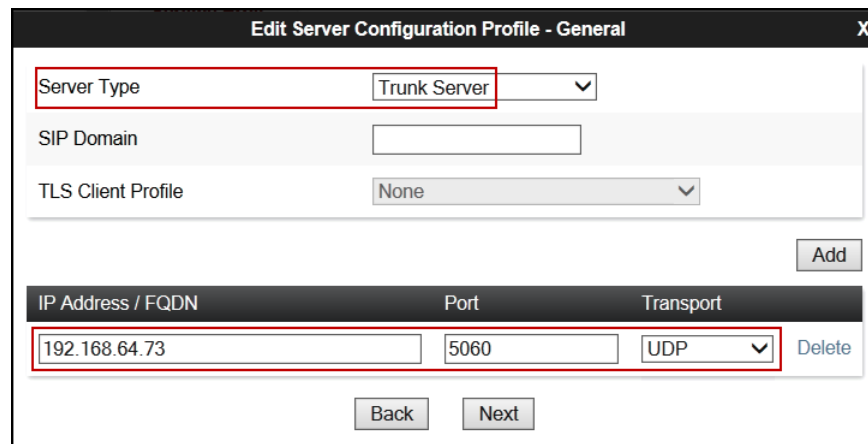
7.7.2. Server Configuration Profile – Service Provider

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.
- Click **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 Alestra's proxy IP address (See figure 1).
- Enter **5060** under **Port**, and select **UDP** for **Transport** for both entries.
- Click **Next**.



- Click **Next** on the **Authentication** and **Heartbeat** tab (not shown).

- On the **Advanced** tab, select **SP-General** from the **Interworking Profile** drop down menu.
- Click **Finish**.

Add Server Configuration Profile - Advanced X

| | |
|-------------------------------|--------------------------|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input type="checkbox"/> |
| Interworking Profile | SP-General ▼ |
| 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 ▼ |

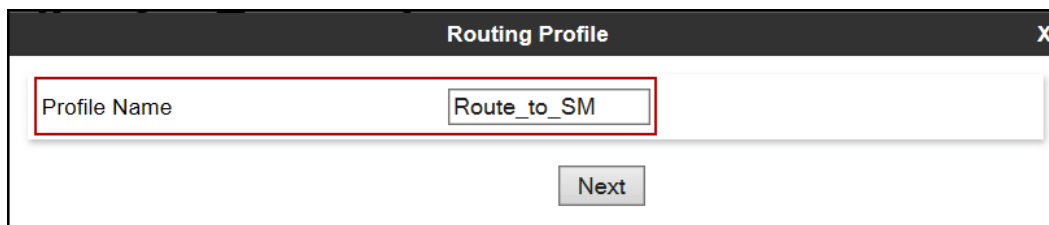
7.8. Routing

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.

7.8.1. Routing Profile – Enterprise

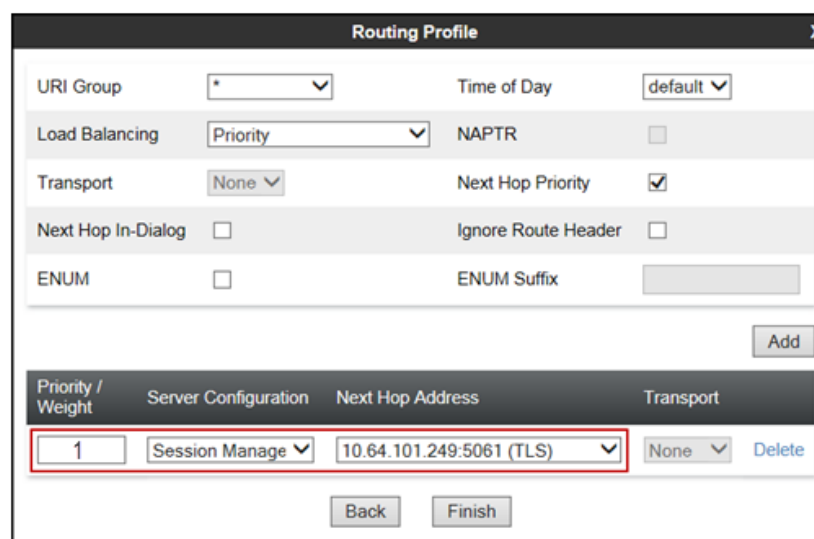
To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown).

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



The screenshot 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_SM". Below the input field is a button labeled "Next".

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **Server Configuration**, 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 7.7.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



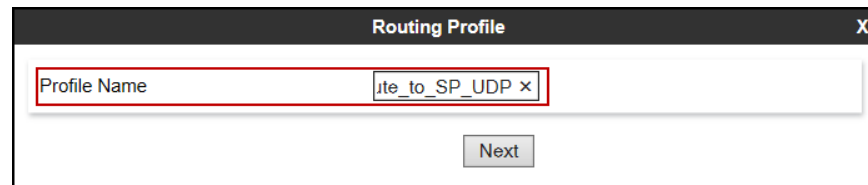
The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. The dialog contains several configuration fields and a table. The fields are: URI Group (dropdown with asterisk), Time of Day (dropdown with default), Load Balancing (dropdown with Priority), NAPTR (checkbox), Transport (dropdown with None), Next Hop Priority (checkbox checked), Next Hop In-Dialog (checkbox), Ignore Route Header (checkbox), ENUM (checkbox), and ENUM Suffix (text field). Below these fields is an "Add" button. At the bottom, there is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, Transport, and a Delete button. The table contains one row with the following values: 1, Session Manager, 10.64.101.249:5061 (TLS), None. Below the table are "Back" and "Finish" buttons.

| Priority / Weight | Server Configuration | Next Hop Address | Transport |
|-------------------|----------------------|--------------------------|-----------|
| 1 | Session Manager | 10.64.101.249:5061 (TLS) | None |

7.8.2. Routing Profile – Service Provider

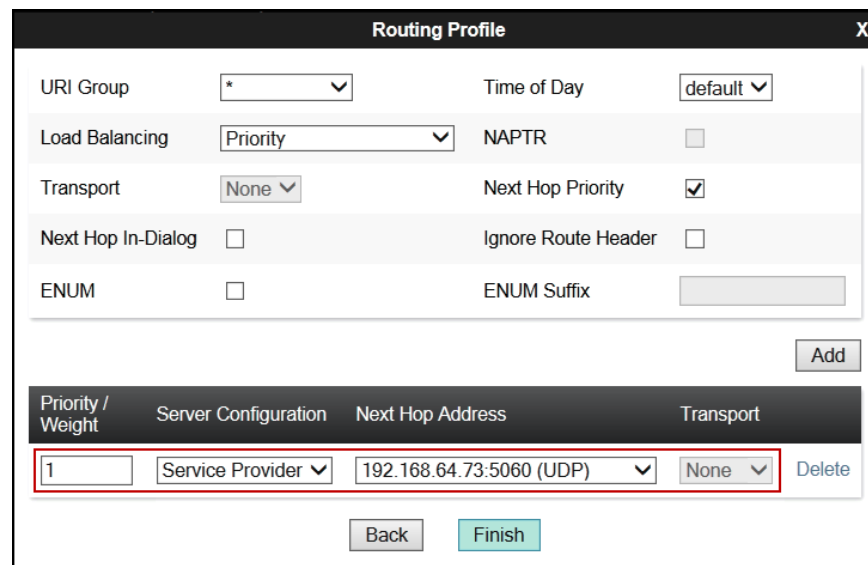
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

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



The image shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text input field for 'Profile Name' containing 'lte_to_SP_UDP' with a small 'X' icon to its right. Below the input field is a 'Next' button.

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **Server Configuration**, select **Service Provider** created in **Section 7.7.2**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in **Section 7.7.2**.
- Defaults were used for all other parameters.
- Click **Finish**.



The image shows a 'Routing Profile' dialog box with various configuration options and a table of entries. The title bar has 'Routing Profile' and a close button 'X'. The configuration options are as follows:

| URI Group | Time of Day |
|-----------|-------------|
| * | default |

| Load Balancing | NAPTR |
|----------------|--------------------------|
| Priority | <input type="checkbox"/> |

| Transport | Next Hop Priority |
|-----------|-------------------------------------|
| None | <input checked="" type="checkbox"/> |

| Next Hop In-Dialog | Ignore Route Header |
|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> |

| ENUM | ENUM Suffix |
|--------------------------|-------------|
| <input type="checkbox"/> | |

Below the configuration options is an 'Add' button. Below that is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, Transport, and a Delete button.

| Priority / Weight | Server Configuration | Next Hop Address | Transport | |
|-------------------|----------------------|--------------------------|-----------|--------|
| 1 | Service Provider | 192.168.64.73:5060 (UDP) | None | Delete |

At the bottom are 'Back' and 'Finish' buttons.

7.9. Topology Hiding

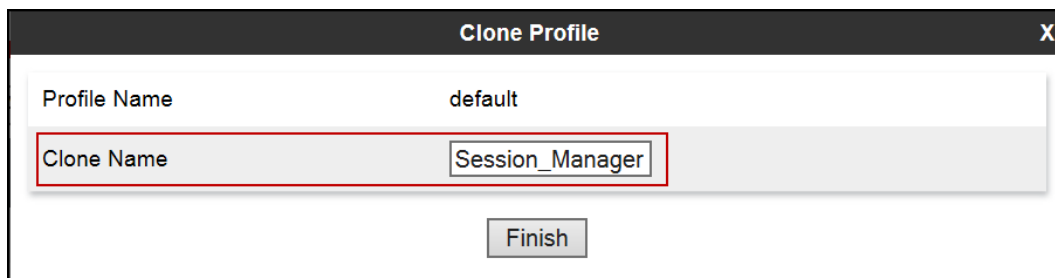
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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.

7.9.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise 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 screenshot shows a 'Clone Profile' dialog box. It has a title bar with 'Clone Profile' and a close button 'X'. Inside, there are two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Session_Manager'. The 'Clone Name' field is highlighted with a red border. At the bottom right, there is a '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**.

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

Finish

7.9.2. Topology Hiding Profile – Service Provider

A Topology Hiding profile named *Service_Provider* was similarly created in the direction of the SIP trunk to the service provider. During the compliance test, IP addresses and not domains names were used in all SIP messages between the service provider and the Avaya SBCE. Note that since the default action of *Auto* implies the insertion of IP addresses in the host portion of these headers, it was not necessary to modify any of the headers sent to the service provider. The screen below shows the *Service_Provider* profile once the configuration was completed.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' expanded and 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: Service_Provider' and features an 'Add' button. Below this, a list of profiles includes 'default', 'cisco_th_profile', 'Session_Manager', 'Service_Provider' (highlighted), 'Com Manager', 'CS1000', and 'IP Office'. The 'Service_Provider' profile is detailed in a table with columns for Header, Criteria, Replace Action, and Overwrite Value. The table lists headers such as SDP, To, From, Refer-To, Via, Record-Route, Request-Line, and Referred-By, all with 'IP/Domain' as criteria and 'Auto' as the replace action. An 'Edit' button is located at the bottom right of the table.

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

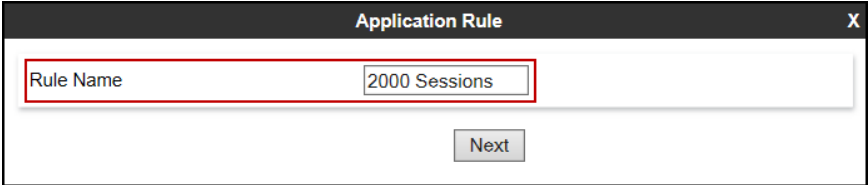
7.10. Domain Policies

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.

7.10.1. Application Rules

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

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

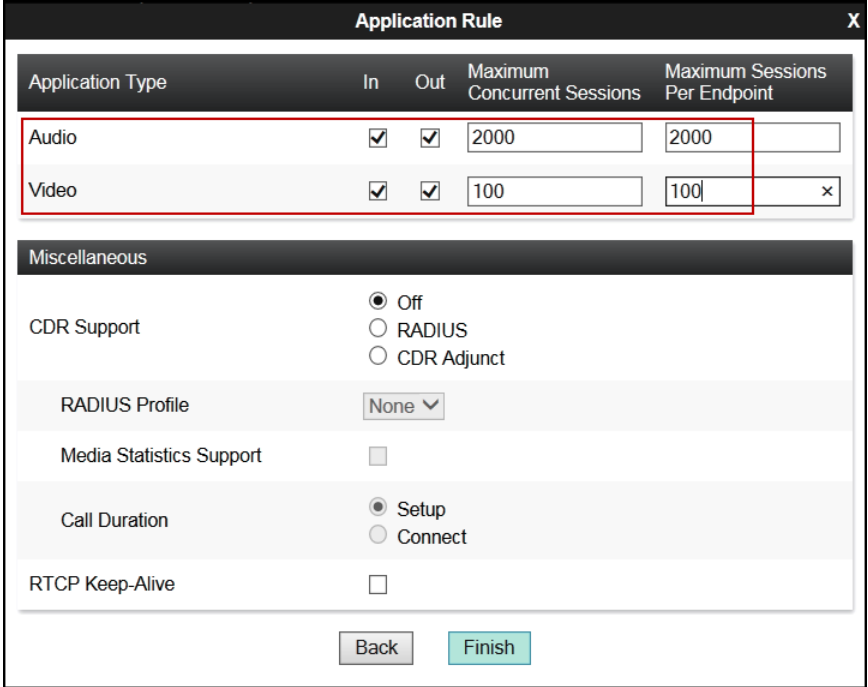


Application Rule

Rule Name: 2000 Sessions

Next

- Under **Audio** check *In* and *Out* and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the values of *2000* for Audio and *100* for Video were used in the sample configuration.
- Click **Finish**.



Application Rule

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

Miscellaneous

CDR Support: ☒ Off, ☐ RADIUS, ☐ CDR Adjunct

RADIUS Profile: None

Media Statistics Support: ☐

Call Duration: ☒ Setup, ☐ Connect

RTCP Keep-Alive: ☐

Back Finish

7.10.2. 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.
- 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

Leave blank to match any value.

2^

Interworking

☒

Video Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

Leave blank to match any value.

2^

Interworking

☒

Miscellaneous

Capability Negotiation

☒

Finish

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

For the compliance test, the **default-low-med** Media Rule was used in the Service Provider direction.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Domain Policies' and 'Media Rules' highlighted. The main content area is titled 'Media Rules: default-low-med' and features an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing settings for Audio Encryption, Video Encryption, and Miscellaneous. The Audio Encryption section shows 'Preferred Formats' set to RTP and 'Interworking' checked. The Video Encryption section also shows 'Preferred Formats' set to RTP and 'Interworking' checked. The Miscellaneous section shows 'Capability Negotiation' unchecked. An 'Edit' button is located at the bottom right of the configuration area.

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

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

Media Rules: default-low-med

Add Filter By Device... Clone

Media Rules
default-low-med
default-low-me...
default-high
default-high-enc
avaya-low-med...
Rem_Workers_...
IPO_SRTP
ServiceProvide...
SM_SRTP

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

Encryption Codec Prioritization Advanced QoS

Audio Encryption

| | |
|-------------------|-------------------------------------|
| Preferred Formats | RTP |
| Interworking | <input checked="" type="checkbox"/> |

Video Encryption

| | |
|-------------------|-------------------------------------|
| Preferred Formats | RTP |
| Interworking | <input checked="" type="checkbox"/> |

Miscellaneous

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

Edit

7.10.3. Signaling Rules

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various configuration areas, with 'Signaling Rules' highlighted under 'Domain Policies'. The main content area is titled 'Signaling Rules: default' and features a 'Filter By Device...' dropdown and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'General' tab is active, showing a table of signaling rules. The table is divided into 'Inbound' and 'Outbound' sections. The 'Inbound' section has five rows: 'Requests' (Allow), 'Non-2XX Final Responses' (Allow), 'Optional Request Headers' (Allow), 'Optional Response Headers' (Allow), and 'Content-Type Policy'. The 'Outbound' section has five rows: 'Requests' (Allow), 'Non-2XX Final Responses' (Allow), 'Optional Request Headers' (Allow), 'Optional Response Headers' (Allow), and 'Content-Type Policy'. The 'Content-Type Policy' section includes a checkbox for 'Enable Content-Type Checks' (checked), a table with 'Action' (Allow) and 'Multipart Action' (Allow), and an 'Exception List' field. An 'Edit' button is located at the bottom right of the table.

| Content-Type Policy | | | |
|----------------------------|-------|-------------------------------------|-------|
| Enable Content-Type Checks | | <input checked="" type="checkbox"/> | |
| Action | Allow | Multipart Action | Allow |
| Exception List | | Exception List | |

7.11. 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.

7.11.1. 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).

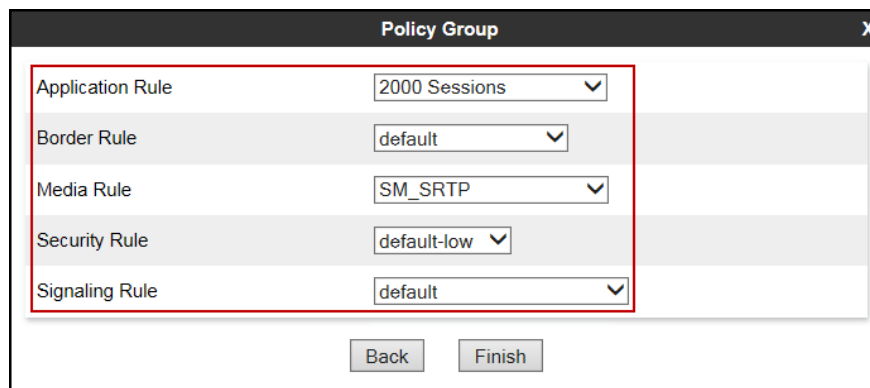
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



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 text input field labeled "Group Name" which contains the word "Enterprise". This field is highlighted with a red rectangular border. Below the input field is a button labeled "Next".

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

- **Application Rule:** *2000 Sessions* (Section 7.10.1).
- **Border Rule:** *default*.
- **Media Rule:** *SM_SRTP* (Section 7.10.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.10.3).
- Click **Finish**.



The screenshot shows the "Policy Group" dialog box with several dropdown menus. The "Application Rule" is set to "2000 Sessions", "Border Rule" is set to "default", "Media Rule" is set to "SM_SRTP", "Security Rule" is set to "default-low", and "Signaling Rule" is set to "default". These dropdowns are highlighted with a red rectangular border. At the bottom of the dialog, there are two buttons: "Back" and "Finish".

7.11.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described. In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, except for the Application Rule, which was set to **2000 Sessions** (Section 7.10.1).

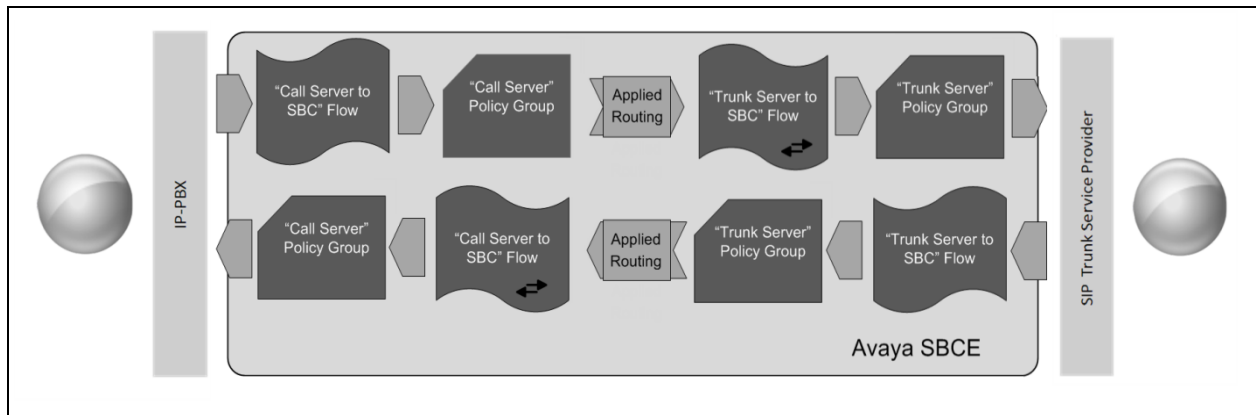
The screen below shows the End Point Policy Group named **Service Provider** after the configuration was completed.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various configuration areas, with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: Service Provider' and features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default...', 'avaya-def-low...', 'avaya-def-hig...', 'avaya-def-hig...', 'Enterprise', and 'Service Prov...'. The 'Service Prov...' group is selected. The right-hand pane shows the configuration details for the 'Service Provider' group, including a table with columns for Order, Application, Border, Media, Security, and Signaling. The table contains one row with the following values: Order 1, Application 2000 Sessions, Border default, Media default-low-med, Security default-low, and Signaling default. The '2000 Sessions' value is highlighted with a red box.

| Order | Application | Border | Media | Security | Signaling |
|-------|---------------|---------|-----------------|-------------|-----------|
| 1 | 2000 Sessions | default | default-low-med | default-low | default |

7.12. 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.

7.12.1. End Point Flow – Enterprise

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). The screen below shows the flow named *Session_Manager_Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.8.2**, which is the reverse route of the flow. Click **Finish**.

| Edit Flow: Session_Manager_Flow | |
|---------------------------------|----------------------|
| Flow Name | Session_Manager_Flow |
| Server Configuration | Session Manager |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | Public_siq |
| Signaling Interface | Private_siq |
| Media Interface | Private_med |
| Secondary Media Interface | None |
| End Point Policy Group | Enterprise |
| Routing Profile | Route_to_SP_UDP |
| Topology Hiding Profile | Session_Manager |
| Signaling Manipulation Script | None |
| Remote Branch Office | Any |

Finish

7.12.2. End Point Flow – Service Provider

A second Server Flow with the name *SIP_Trunk_Flow_UDP* was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.8.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.

| Edit Flow: SIP_Trunk_Flow_UDP | |
|-------------------------------|----------------------|
| Flow Name | SIP_Trunk_Flow_UDP |
| Server Configuration | Service Provider UDP |
| 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 |
| Finish | |

8. Alestra Enlace IP SIP Trunk Service Configuration

To use Alestra Enlace IP SIP Trunk Service, a customer must request the service from Alestra using the established sales processes. The process can be started by contacting Alestra via the corporate web site at: <http://www.alestra.com.mx>

During the signup process, Alestra and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Alestra's network. Alestra will provide their SIP Proxy public IP address, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

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

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Click the Session Manager instance (*Session Manager* in the example below).

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with the following items: Home, Session Manager, Dashboard, Session Manager Administration, Global Settings, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, Managed, and Bandwidth Usage. The 'Session Manager' and 'System Status' items are highlighted with red boxes. The main content area displays the 'SIP Entity Link Monitoring Status Summary' page. The page title is 'SIP Entity Link Monitoring Status Summary'. Below the title, there is a description: 'This page provides a summary of Session Manager SIP entity link monitoring status.' A 'Run Monitor' button is present. The table shows the status of monitored entities for the 'Session Manager' instance. The table has columns for Session Manager, Type, Down, Partially Up, Up, Not Monitored, Deny, and Total. The data row shows 'Session Manager' as the instance, 'Core' as the type, 1 Down, 0 Partially Up, 5 Up, 0 Not Monitored, 0 Deny, and a Total of 6. The 'Session Manager' and 'Core' cells are highlighted with red boxes. The 'Total' cell is also highlighted with a red box. The table is titled 'SIP Entities Status for All Monitoring Session Manager Instances'.

| Session Manager | Type | Monitored Entities | | | | | Total |
|---------------------------------|------|--------------------|--------------|----|---------------|------|-------|
| | | Down | Partially Up | Up | Not Monitored | Deny | |
| Session Manager | Core | 1 | 0 | 5 | 0 | 0 | 6 |

Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **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.

All Entity Links for Session Manager: Session Manager

Summary View

Status Details for the selected Session Manager:

| SIP Entity Name | IP Address Family | SIP Entity Resolved IP | Port | Proto. | Deny | Conn. Status | Reason Code | Link Status |
|--------------------------------|-------------------|------------------------|------|--------|-------|--------------|---------------------|-------------|
| CS1K7.6 | IPv4 | 172.16.5.60 | 5085 | UDP | FALSE | DOWN | 408 Request Timeout | DOWN |
| Avaya SBCE | IPv4 | 10.64.101.243 | 5061 | TLS | FALSE | UP | 200 OK | UP |
| Communication Manager Trunk 1 | IPv4 | 10.64.101.241 | 5061 | TLS | FALSE | UP | 200 OK | UP |
| AA-Messaging | IPv4 | 10.64.101.250 | 5060 | TCP | FALSE | UP | 200 OK | UP |
| Communication Manager Trunk 2 | IPv4 | 10.64.101.241 | 5071 | TLS | FALSE | UP | 200 OK | UP |
| Communication Manager Trunk 98 | IPv4 | 10.64.101.241 | 5065 | TLS | FALSE | UP | 200 OK | UP |

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.

Alarms 1 Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

| Information | |
|------------------------------|---|
| System Time | 12:27:04 PM EST Refresh |
| Version | 7.2.0.0-18-13712 |
| Build Date | Thu Jun 1 00:12:50 UTC 2017 |
| License State | OK |
| Aggregate Licensing Overages | 0 |
| Peak Licensing Overage Count | 0 |
| Last Logged in at | 11/22/2017 10:47:24 EST |
| Failed Login Attempts | 0 |

| Installed Devices | |
|-------------------|---|
| EMS | |
| Avaya_SBCE | 1 |

Active Alarms (past 24 hours)

Avaya_SBCE : Disk utilization is more than 75% for /archive/log/pcs

Incidents (past 24 hours)

Avaya_SBCE : No Subscriber Flow Matched

Avaya_SBCE : No Subscriber Flow Matched

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

Alarm Viewer

Devices

EMS

Avaya_SBCE 1

Alarms

| <input checked="" type="checkbox"/> | 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.

Session Border Controller for Enterprise

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

| Information | |
|------------------------------|---|
| System Time | 12:27:04 PM EST Refresh |
| Version | 7.2.0.0-18-13712 |
| Build Date | Thu Jun 1 00:12:50 UTC 2017 |
| License State | OK |
| Aggregate Licensing Overages | 0 |
| Peak Licensing Overage Count | 0 |
| Last Logged in at | 11/22/2017 10:47:24 EST |
| Failed Login Attempts | 0 |

| Installed Devices | |
|-------------------|---|
| EMS | |
| Avaya_SBCE | 1 |

| Active Alarms (past 24 hours) | |
|-------------------------------|---|
| Avaya_SBCE | Disk utilization is more than 75% for /archive/log/ipcs |

| Incidents (past 24 hours) | |
|---------------------------|----------------------------|
| Avaya_SBCE | No Subscriber Flow Matched |
| Avaya_SBCE | No Subscriber Flow Matched |

The following screen shows the Incident Viewer page.

Incident Viewer

Device: Category: [Clear Filters](#) [Refresh](#) [Generate Report](#)

Displaying results 0 to 0 out of 0.

| Type | ID | Date | Time | Category | Device | Cause |
|---------------------|----|------|------|----------|--------|-------|
| No incidents found. | | | | | | |

<< < 1 > >>

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

Session Border Controller for Enterprise

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

| Information | |
|------------------------------|---|
| System Time | 12:27:04 PM EST Refresh |
| Version | 7.2.0.0-18-13712 |
| Build Date | Thu Jun 1 00:12:50 UTC 2017 |
| License State | OK |
| Aggregate Licensing Overages | 0 |
| Peak Licensing Overage Count | 0 |
| Last Logged in at | 11/22/2017 10:47:24 EST |
| Failed Login Attempts | 0 |

Installed Devices

| Device | Count |
|------------|-------|
| Avaya_SBCE | 1 |

Active Alarms (past 24 hours)

Avaya_SBCE : Disk utilization is more than 75% for /archive/log/ipcs

Incidents (past 24 hours)

Avaya_SBCE : No Subscriber Flow Matched

Avaya_SBCE : No Subscriber Flow Matched

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

Diagnostics

Pinging 10.64.101.249

Average ping from 10.64.101.244 [A1] to 10.64.101.249 is 0.369ms.

Full Diagnostic **Ping Test**

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Source Device / IP: A1

Destination IP: 10.64.101.249

Ping

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. The left sidebar contains a menu with categories like Dashboard, Administration, System Management, and Troubleshooting. The "Troubleshooting" category is expanded, showing "Device Specific Settings" and "Trace". The "Trace" option is selected. The main content area is titled "Trace: Avaya_SBCE" and features two tabs: "Packet Capture" (selected) and "Captures". The "Packet Capture Configuration" form includes fields for Status (Ready), Interface (Any), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Test.pcap). The "Start Capture" button is highlighted.

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ Domain Policies
‣ TLS Management
‣ **Device Specific Settings**
  Network Management
  Media Interface
  Signaling Interface
  End Point Flows
  Session Flows
  ‣ DMZ Services
  TURN/STUN Service
  SNMP
  Syslog Management
  Advanced Options
‣ **Troubleshooting**
  Debugging
  Trace
  DoS Learning

Trace: Avaya_SBCE

Devices
Avaya_SBCE

Packet Capture Captures

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 Using the name of an existing capture will overwrite it. | Test.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.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Device Specific Settings' and its sub-item 'Trace' highlighted. The main content area is titled 'Trace: Avaya_SBCE' and contains two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active, showing a table of captured files. The table has columns for File Name, File Size (bytes), Last Modified, and a Delete button. One file is listed: 'Test_20171122123225.pcap' with a size of 176,128 bytes and a timestamp of November 22, 2017, 12:32:47 PM EST.

| File Name | File Size (bytes) | Last Modified | |
|--------------------------|-------------------|-----------------------------------|--------|
| Test_20171122123225.pcap | 176,128 | November 22, 2017 12:32:47 PM EST | Delete |

10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1 and Avaya Session Border Controller for Enterprise 7.2, to connect to the Alestra Enlace IP SIP Trunk 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*, Release 7.1.1, Issue 2, August 2017.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017.
- [3] *Administering Avaya Aura® System Manager* for Release 7.1.1, Issue 7, October 2017.
- [4] *Deploying Avaya Aura® System Manager*, Release 7.1.1, Issue 3, August 2017.
- [5] *Deploying Avaya Aura® Session Manager*, Release 7.1, Issue 1, May 2017.
- [6] *Administering Avaya Aura® Session Manager*, Release 7.1.1, Issue 2, August 2017.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2.1, Issue 4, November 2017.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2.1, Issue 4, November 2017.
- [9] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0 - Issue 1.0*.
- [10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.8, Issue 3, August 2017.
- [11] *Implementing and Administering Avaya Aura® Media Server*. Release 7.8, Issue 5, October 2017.
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [13] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2017 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.