Abstract

These Application Notes describe the steps to configure a Session Initiation Protocol (SIP) trunk between Intermedia SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise 7.0, Avaya Aura® Media Server 7.7, Avaya Aura® Messaging 6.3 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for 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.

Intermedia is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing is conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.
Table of Contents

1. Introduction .................................................................................................................. 4
2. General Test Approach and Test Results ........................................................................ 4
   2.1. Interoperability Compliance Testing ...................................................................... 4
   2.2. Test Results .......................................................................................................... 5
   2.3. Support ................................................................................................................. 6
3. Reference Configuration .................................................................................................. 6
4. Equipment and Software Validated ................................................................................ 8
5. Configure Avaya Aura® Communication Manager ...................................................... 9
   5.1. Licensing and Capacity .......................................................................................... 9
   5.2. System Features ................................................................................................... 11
   5.3. IP Node Names ..................................................................................................... 12
   5.4. Codecs .................................................................................................................. 13
   5.5. IP Network Region ............................................................................................... 14
   5.6. Signaling Group ..................................................................................................... 16
   5.7. Trunk Group .......................................................................................................... 18
   5.8. Calling Party Information ...................................................................................... 20
   5.9. Incoming Call Handling Treatment ........................................................................ 20
   5.10. Outbound Routing ............................................................................................... 21
   5.11. Saving Communication Manager Configuration Changes .................................. 22
   5.12. TLS Management on Communication Manager .................................................. 23
6. Configure Avaya Aura® Session Manager ..................................................................... 26
   6.1. System Manager Login and Navigation .................................................................. 26
   6.2. Specify SIP Domain ............................................................................................... 27
   6.3. Add Location ......................................................................................................... 28
   6.4. Add SIP Entities .................................................................................................... 29
   6.5. Add Entity Links .................................................................................................... 32
   6.6. Add Routing Policies ............................................................................................ 34
   6.7. Add Dial Patterns .................................................................................................. 35
   6.8. Add/View Session Manager .................................................................................. 37
   6.9. TLS Certificate Management on System Manager ............................................... 38
7. Configure Avaya Session Border Controller for Enterprise ......................................... 40
   7.1. Avaya Session Border Controller for Enterprise Login ........................................ 40
   7.2. TLS Management ................................................................................................. 41
       7.2.1. Certificates ..................................................................................................... 41
       7.2.2. Client Profiles ............................................................................................... 43
       7.2.3. Server Profiles .............................................................................................. 44
   7.3. Global Profiles ....................................................................................................... 45
       7.3.1. Uniform Resource Identifier (URI) Groups .................................................... 45
       7.3.2. Server Interworking Profile ......................................................................... 45
       7.3.3. Configure Signaling Manipulation ................................................................. 50
       7.3.4. Server Configuration ..................................................................................... 50
       7.3.5. Routing Profiles ............................................................................................ 54
       7.3.6. Topology Hiding ........................................................................................... 56
   7.4. Domain Policies ..................................................................................................... 58

QT; Reviewed: Solution & Interoperability Test Lab Application Notes
RRR m/d/y ©2016 Avaya Inc. All Rights Reserved. IMTTLSCMSMSBCE7 2 of 73
7.4.1. Media Rules ................................................................. 58
7.4.2. Signaling Rules ............................................................. 59
7.4.3. Endpoint Policy Groups .................................................. 60
7.5. Device Specific Settings ..................................................... 62
  7.5.1. Network Management .................................................. 62
  7.5.2. Media Interface .......................................................... 64
  7.5.3. Signaling Interface ..................................................... 65
  7.5.4. End Point Flows - Server Flow ....................................... 67
8. INTERMEDIA Service Configuration ......................................... 69
9. Verification and Troubleshooting ............................................. 69
  9.1. Verification Steps .......................................................... 69
  9.2. Protocol Traces ............................................................. 69
  9.3. Troubleshooting ........................................................... 70
    9.3.1. The Avaya SBCE ...................................................... 70
    9.3.2. Communication Manager .......................................... 70
10. Conclusion ........................................................................... 71
11. References .......................................................................... 72
1. Introduction

These Application Notes describe the steps to configure a SIP trunk between Intermedia SIP Trunking Service and an Avaya SIP-enabled enterprise solution. Avaya Aura® release 7.0 is being deployed in virtualized environment that includes Avaya Aura® Communication Manager 7.0 (Communication Manager), Avaya Aura® Session Manager 7.0 (Session Manager), Avaya Aura® Media Server, Avaya Aura® Messaging and Avaya Session Border Controller for Enterprise 7.0 (Avaya SBCE). Various Avaya endpoints are also used in test configuration.

Customers using this Avaya SIP-enabled enterprise solution with Intermedia are able to place and receive PSTN calls via a broadband Internet connection. This converged network solution is an alternative to a traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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.

Intermedia is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to INTERMEDIA via the Internet and exercise the features and functionalities listed in Section 2.1.

2.1. Interoperability Compliance Testing

To verify Intermedia interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including H.323, SIP, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, SIP, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone.
- Dialing plans including local, long distance, international, outbound toll-free calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711MU and G.729.
- Fax T.38.
- Media and Early Media transmissions.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward.
- EC500 mobility (extension to cellular).
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat, Authentication and Registration.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.
- Remote Worker, which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Items, that are not supported, include the following:
- Inbound toll-free and 911 are supported but were not tested as part of the compliance test.
- T.38 Fax is not supported.
- Operator Call (dial 0) and Operator Assisted (dial 0+10digits) are not supported.
- SIP OPTIONS sent by Intermedia is not supported.
- Intermedia does not support SIP Diversion Header.
- Call Redirection using SIP REFER and 302 are not supported by Intermedia.

2.2. Test Results
Interoperability testing of Intermedia with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations and limitations described below:

- **Fax Support**: T.38 fax is not supported on the Intermedia SIP trunking service. G.711 fax pass-through was successfully tested during the compliance test. Due to the unpredictability of pass-through techniques, which only work well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered in Communication Manager on a “best effort” basis; its success is not guaranteed, and it should be used at the customer’s discretion.

- **Call Forward Off Net**: Intermedia responded with “487 Request Terminated” error code on an inbound call from PSTN to Avaya endpoint and being forwarded to another PSTN. The issue happened due to Avaya system sent out INVITE to perform call forward with User-Agent header containing Intermedia system information. This caused an erroneous condition in Intermedia system prompting it to respond with the error code “487 Request Terminated”. Resolution is to remove the User-agent header using manipulation script in Avaya SBCE (Section 7.3.3).

- **Mobility EC500**: There was not ringing on an EC500 mobile extension when an inbound call from PSTN was made to Avaya enterprise host station. The issue happened due to Avaya system sent out INVITE to ring EC500 mobile extension with User-Agent header containing Intermedia system information. This caused an erroneous condition in the Intermedia system prompting it to respond with the error code “487 Request Terminated”. Resolution is to remove the User-agent header using manipulation script in Avaya SBCE (Section 7.3.3).

- **Call Redirection Using Consultative Transfer**: There is not voice path between two PSTN endpoints after a consultative transfer being performed by Avaya enterprise extension. With attribute Direct IP-IP Audio Connections set to “Y”, Avaya system
redirected the media by-passing Avaya media gateway. The shuffling of media caused the encryption key issue in Intermedia system. Resolution is to set attribute Direct IP-IP Audio Connections to “N”, see Section 5.6.

- **Conference Call** – There is no voice path between two PSTN endpoints after host of a conference drop out of the conference call. With attribute Direct IP-IP Audio Connections set to “Y”, Avaya system redirected the media by-passing Avaya media gateway. The shuffling of media caused the encryption key issue in Intermedia system. Resolution is to set attribute Direct IP-IP Audio Connections to “N”, see Section 5.6.

### 2.3. Support

For technical support on Intermedia SIP Trunking, contact Intermedia at [https://www.intermedia.net](https://www.intermedia.net)

### 3. Reference Configuration

**Figure 1** illustrates the sample Avaya SIP-enabled enterprise solution connected to the Intermedia (Vendor Validation circuit) through a public Internet connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

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

- Avaya Aura® Communication Manager running in VMware environment.
- Avaya Aura® System Manager running in VMware environment.
- Avaya Aura® Session Manager running in VMware environment.
- Avaya Aura® Messaging running in VMware environment.
- Avaya Aura® Media Server running in VMware environment.
- Avaya G450 Media Gateway.
- Avaya Session Border Controller for Enterprise.
- Avaya 9600Series IP Deskphones (H.323, SIP).
- Avaya one-X® Communicator soft phones (H.323, SIP).
- Avaya digital and analog telephones.

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to Intermedia via Internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Intermedia across the public network is TLS. The transport protocol between the Avaya SBCE, Session Manager and Communication Manager is TLS.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain “avayalab.com” for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to INTERMEDIA.
Figure 1 below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

Additionally, a remote worker is included in the reference configuration Figure 1. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test, using the Avaya one-X® Communicator for Windows using TCP. The configuration tasks required to support remote workers are referenced in Section 11.
4. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Avaya IP Telephony Solution Components</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager running on Virtualized Environment</td>
<td>7.0 (R017x.00.0.441.0 Patch 22477)</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>37.19.0</td>
</tr>
<tr>
<td>Avaya Aura® System Manager running on Virtualized Environment</td>
<td>7.0</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager running on Virtualized Environment</td>
<td>7.0 (7.0.0.0.3929)</td>
</tr>
<tr>
<td>Avaya Aura® Messaging running on Virtualized Environment</td>
<td>7.0 (7.0.0.700007)</td>
</tr>
<tr>
<td>Avaya Aura® Media Server running on Virtualized Environment</td>
<td>6.3.124.335-1.253373</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise</td>
<td>7.0.0-21-6602</td>
</tr>
<tr>
<td>Avaya 9621G IP Deskphone (H.323)</td>
<td>6.6.029</td>
</tr>
<tr>
<td>Avaya 9641G IP Deskphone (SIP)</td>
<td>7.0.0.39</td>
</tr>
<tr>
<td>Avaya one-X® Communicator (H.323/SIP)</td>
<td>6.2.7.03-SP7</td>
</tr>
<tr>
<td>Avaya 1408 Digital Telephone</td>
<td>1408D02A-003</td>
</tr>
<tr>
<td>Avaya Analog Telephone</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intermedia SIP Trunking Service Components</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intermedia SBC</td>
<td>16.14.2</td>
</tr>
<tr>
<td>Intermedia Softswitch</td>
<td>16.14.2</td>
</tr>
</tbody>
</table>

Table 1: Equipment and Software Tested

Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Intermedia SIP Trunking service. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Media Server has been previously completed and is not discussed here.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

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 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 sale representative to add the additional capacity or feature.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
<th>Page 2 of 12</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPTIONAL FEATURES</strong></td>
<td></td>
</tr>
<tr>
<td>IP PORT CAPACITIES</td>
<td></td>
</tr>
<tr>
<td>Maximum Administered H.323 Trunks: 4000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations: 2400</td>
<td>1</td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks: 4000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations: 2400</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP eCons: 68</td>
<td>0</td>
</tr>
<tr>
<td>Max Concur Registered Unauthenticated H.323 Stations: 100</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable Stations: 2400</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones: 2400</td>
<td>3</td>
</tr>
<tr>
<td><strong>Maximum Administered SIP Trunks: 4000</strong></td>
<td>74</td>
</tr>
<tr>
<td>Maximum Administered Ad-hoc Video Conferencing Ports: 4000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Number of DS1 Boards with Echo Cancellation: 80</td>
<td>0</td>
</tr>
</tbody>
</table>

(NOTE: You must logoff & login to effect the permission changes.)
On Page 4, verify that ARS is set to y.

```plaintext
display system-parameters customer-options

Index

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviated Dialing Enhanced List?</td>
<td>y</td>
</tr>
<tr>
<td>Access Security Gateway (ASG)?</td>
<td>n</td>
</tr>
<tr>
<td>Analog Trunk Incoming Call ID?</td>
<td>y</td>
</tr>
<tr>
<td>A/D Grp/Sys List Dialing Start at 01?</td>
<td>y</td>
</tr>
<tr>
<td>Answer Supervision by Call Classifier?</td>
<td>y</td>
</tr>
<tr>
<td>ARS?</td>
<td>y</td>
</tr>
<tr>
<td>ARS/ARR Partitioning?</td>
<td>y</td>
</tr>
<tr>
<td>ARS/BAM Dialing without FAC?</td>
<td>n</td>
</tr>
<tr>
<td>ASA1 Link Core Capabilities?</td>
<td>n</td>
</tr>
<tr>
<td>ASA1 Link Plus Capabilities?</td>
<td>n</td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) Trunking?</td>
<td>n</td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) Trunking (y)</td>
<td>y</td>
</tr>
<tr>
<td>ATM WAN Spare Processor?</td>
<td>n</td>
</tr>
<tr>
<td>ATM System - Parameters</td>
<td></td>
</tr>
<tr>
<td>Customer Options</td>
<td></td>
</tr>
<tr>
<td>Emergency Access to Attendant?</td>
<td>y</td>
</tr>
<tr>
<td>Enable 'dadmin' Login?</td>
<td>y</td>
</tr>
<tr>
<td>Enhanced Conferencing?</td>
<td>y</td>
</tr>
<tr>
<td>Enhanced EC500?</td>
<td>y</td>
</tr>
<tr>
<td>Enterprise Survivable Server?</td>
<td>n</td>
</tr>
<tr>
<td>Enterprise Wide Licensing?</td>
<td>n</td>
</tr>
<tr>
<td>ESS Administration?</td>
<td>y</td>
</tr>
<tr>
<td>Extended Cvg/Fwd Admin?</td>
<td>y</td>
</tr>
<tr>
<td>External Device Alarm Admin?</td>
<td>y</td>
</tr>
<tr>
<td>Five Port Networks Max Per MCC?</td>
<td>n</td>
</tr>
<tr>
<td>Forced Entry of Account Codes?</td>
<td>y</td>
</tr>
<tr>
<td>Global Call Classification?</td>
<td>y</td>
</tr>
<tr>
<td>Hospitality (Basic)</td>
<td>y</td>
</tr>
<tr>
<td>Hospitality (G3V3 Enhancements)</td>
<td>y</td>
</tr>
<tr>
<td>IP Attendant Consoles?</td>
<td>y</td>
</tr>
<tr>
<td>IP Stations?</td>
<td>y</td>
</tr>
<tr>
<td>IP Trunks?</td>
<td>y</td>
</tr>
</tbody>
</table>
```

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

On Page 5, verify that IP Trunks field is set to y and Media Encryption Over IP field is set to y.
(Note: The Media Encryption option is only available if Media Encryption Over IP is enabled on the installed license)

```plaintext
display system-parameters customer-options

Index

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviated Dialing Enhanced List?</td>
<td>y</td>
</tr>
<tr>
<td>Access Security Gateway (ASG)?</td>
<td>n</td>
</tr>
<tr>
<td>Analog Trunk Incoming Call ID?</td>
<td>y</td>
</tr>
<tr>
<td>A/D Grp/Sys List Dialing Start at 01?</td>
<td>y</td>
</tr>
<tr>
<td>Answer Supervision by Call Classifier?</td>
<td>y</td>
</tr>
<tr>
<td>ARS?</td>
<td>y</td>
</tr>
<tr>
<td>ARS/ARR Partitioning?</td>
<td>y</td>
</tr>
<tr>
<td>ARS/BAM Dialing without FAC?</td>
<td>n</td>
</tr>
<tr>
<td>ASA1 Link Core Capabilities?</td>
<td>n</td>
</tr>
<tr>
<td>ASA1 Link Plus Capabilities?</td>
<td>n</td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) Trunking?</td>
<td>n</td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) Trunking (y)</td>
<td>y</td>
</tr>
<tr>
<td>ATM WAN Spare Processor?</td>
<td>n</td>
</tr>
<tr>
<td>ATM System - Parameters</td>
<td></td>
</tr>
<tr>
<td>Customer Options</td>
<td></td>
</tr>
<tr>
<td>Emergency Access to Attendant?</td>
<td>y</td>
</tr>
<tr>
<td>Enable 'dadmin' Login?</td>
<td>y</td>
</tr>
<tr>
<td>Enhanced Conferencing?</td>
<td>y</td>
</tr>
<tr>
<td>Enhanced EC500?</td>
<td>y</td>
</tr>
<tr>
<td>Enterprise Survivable Server?</td>
<td>n</td>
</tr>
<tr>
<td>Enterprise Wide Licensing?</td>
<td>n</td>
</tr>
<tr>
<td>ESS Administration?</td>
<td>y</td>
</tr>
<tr>
<td>Extended Cvg/Fwd Admin?</td>
<td>y</td>
</tr>
<tr>
<td>External Device Alarm Admin?</td>
<td>y</td>
</tr>
<tr>
<td>Five Port Networks Max Per MCC?</td>
<td>n</td>
</tr>
<tr>
<td>Forced Entry of Account Codes?</td>
<td>y</td>
</tr>
<tr>
<td>Global Call Classification?</td>
<td>y</td>
</tr>
<tr>
<td>Hospitality (Basic)</td>
<td>y</td>
</tr>
<tr>
<td>Hospitality (G3V3 Enhancements)</td>
<td>y</td>
</tr>
<tr>
<td>IP Attendant Consoles?</td>
<td>y</td>
</tr>
<tr>
<td>IP Stations?</td>
<td>y</td>
</tr>
<tr>
<td>IP Trunks?</td>
<td>y</td>
</tr>
</tbody>
</table>
```

(Note: You must logoff & login to effect the permission changes.)
On Page 6, verify that Private Networking and Processor Ethernet are set to y.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
<th>OPTIONAL FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multinational Locations? n</td>
<td>Station and Trunk MSP? y</td>
</tr>
<tr>
<td>Multiple Level Precedence &amp; Preemption? n</td>
<td>Station as Virtual Extension? y</td>
</tr>
<tr>
<td>Multiple Locations? n</td>
<td>System Management Data Transfer? n</td>
</tr>
<tr>
<td>Personal Station Access (PSA)? y</td>
<td>Tenant Partitioning? y</td>
</tr>
<tr>
<td>PNC Duplication? n</td>
<td>Terminal Trans. Init. (TTI)? y</td>
</tr>
<tr>
<td>Posted Messages? y</td>
<td>TN2501 VAL Maximum Capacity? y</td>
</tr>
<tr>
<td>Private Networking? y</td>
<td>Uniform Dialing Plan? y</td>
</tr>
<tr>
<td>Processor and System MSP? y</td>
<td>Usage Allocation Enhancements? y</td>
</tr>
<tr>
<td>Processor Ethernet? y</td>
<td>Wireless? n</td>
</tr>
<tr>
<td>Remote Office? y</td>
<td></td>
</tr>
<tr>
<td>Restrict Call Forward Off Net? y</td>
<td></td>
</tr>
<tr>
<td>Secondary Data Module? y</td>
<td>(NOTE: You must logoff &amp; login to effect the permission changes.)</td>
</tr>
</tbody>
</table>

5.2. System Features

Use the change system-parameters features command to set the Trunk-to-Trunk Transfer field to all to allow an incoming call 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.

<table>
<thead>
<tr>
<th>change system-parameters features</th>
<th>FEATURE-RELATED SYSTEM PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Station Display Enabled? y</td>
<td></td>
</tr>
<tr>
<td>Trunk-to-Trunk Transfer: all</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback with Called Party Queuing? n</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback – No Answer Timeout Interval (rings): 3</td>
<td></td>
</tr>
<tr>
<td>Off-Premises Tone Detect Timeout Interval (seconds): 20</td>
<td></td>
</tr>
<tr>
<td>AAR/ANS Dial Tone Required? y</td>
<td></td>
</tr>
</tbody>
</table>
On Page 9 verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test used the value of *Restricted* for restricted calls and *Unavailable* for unavailable calls.

### Feature-Related System Parameters

#### CPN/ANI/ICLID Parameters

- **CPN/ANI/ICLID Replacement for Restricted Calls:** Restricted
- **CPN/ANI/ICLID Replacement for Unavailable Calls:** Unavailable

#### Display Text

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

#### International Call Routing Parameters

- Local Country Code: 1
- International Access Code: 001

#### 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**), Session Manager (**SM**) and Media Server (**AMS**). These node names will be needed for defining the signaling groups in Section 5.6.

#### IP Node Names

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM</td>
<td>10.33.10.33</td>
</tr>
<tr>
<td>AMS</td>
<td>10.33.10.36</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>procr</td>
<td>10.33.10.34</td>
</tr>
<tr>
<td>procr6</td>
<td>::</td>
</tr>
</tbody>
</table>
5.4. Codecs

Use the `change ip-codec-set` command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 1. INTERMEDIA supports G.711MU and G729. To use these codecs, enter `G.711MU` and `G.729` in the Audio Codec. For media encryption used within Avaya Aura system, the `1-srtp-aescm128-hmac32` is used in Media Encryption and `best-effort` in Encrypted SRTCP columns of the table in the order of preference.

The following screen shows the configuration for ip-codec-set 1. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

```
change ip-codec-set 1

IP CODEC SET
Codec Set: 1
Audio  Silence  Frames  Packet
Codec    Suppression  Per Pkt  Size(ms)
1: G.711MU  n   2    20
2: G.729  n   2    20
3: 4: 5: 6: 7:

Media Encryption: Encrypted SRTCP: best-effort
1: 2-srtp-aescm128-hmac32
2: none
```

On Page 2, set the Fax Mode to `pass-through` faxing which is supported by Intermedia.

```
change ip-codec-set 1

IP CODEC SET
Fax Mode  Redundancy
Allow Direct-IP Multimedia? n
Packet
FAX                  Size(ms)
Mode                Size
pass-through        1
Modem               0
TDD/TTY             3
H.323 Clear-channel n  0
SIP 64K Data        n  20
```

QT; Reviewed: Solution & Interoperability Test Lab Application Notes
RRR m/d/y ©2016 Avaya Inc. All Rights Reserved. IMTTLSCMSMSBCE7
5.5. IP Network Region

A separate IP network region for the service provider trunk group is created. This allows separate codec or quality of service setting to be used (if necessary) for a call between the enterprise and the service provider versus a call within the enterprise or elsewhere. For the compliance testing, ip-network-region 1 was created by the change ip-network-region 1 command with the following parameters:

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

On Page 4, define the IP codec set to be used for traffic between region 1 and other regions. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, IP/SIP phones and Session Manager were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the codec set column of the table with appropriate destination region (dst rgn). Default values may be used for all other fields. The example below shows codec set 1 will be used for a call between region 1 and other regions.

<table>
<thead>
<tr>
<th>Source Region: 1</th>
<th>Inter Network Region Connection Management</th>
<th>I M</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>G A t</td>
<td></td>
</tr>
<tr>
<td>dst codec direct</td>
<td>WAN-BW-limits Video Intervening Dyn A G c</td>
<td></td>
</tr>
<tr>
<td>rgn set MAN Units Total Norm Prio Shr Regions</td>
<td>CAC R L e</td>
<td></td>
</tr>
<tr>
<td>1 1 1 y NoLimit</td>
<td></td>
<td>t</td>
</tr>
</tbody>
</table>

QT; Reviewed: Solution & Interoperability Test Lab Application Notes 14 of 73
RRR m/d/y ©2016 Avaya Inc. All Rights Reserved. IMTTLSCMSMSBCE7
Non-IP telephones (e.g., analog, digital) derive network region from the IP interface of the Avaya G450 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

```
change ip-interface procr
```

```
Type: PROCR
Enable Interface? y
Allow H.323 Endpoints? y
Allow H.248 Gateways? y
Network Region: 1
Gatekeeper Priority: 5
```

To define network region 1 for the Avaya G450 Media Gateway, use **change media-gateway** command as shown in the following screen.

```
change media-gateway 1
```

```
Type: g450
Name: g450
Serial No: 11N526797797
Link Encryption Type: any-pts/tls
Network Region: 1
Location: 1
Recovery Rule: none
```

If Avaya Aura® Media Server is used in parallel of Avaya Media Gateway G450, then it is needed to define network region 1 for the Avaya Aura® Media Server. Use **change media-server** command as shown in the following screen.

```
change media-server 1
```

```
Media Server ID: 1
Signaling Group: 3
Voip Channel License Limit: 30
Dedicated Voip Channel Licenses: 30
Node Name: AMS
Network Region: 1
Location: 1
Announcement Storage Area:
```
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 Avaya SBCE 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.

- Set the **Group Type** field to `sip`.
- Set the **IMS Enabled** field to `n`.
- Set the **Transport Method** to `tls` (*Transport Layer Security*). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5061**.
- Set the **Near-end Node Name** to `procr`. This node name maps to the IP interface of `procr` 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 **Far-end Network Region** to the IP network region 1 defined for the service provider in Section 5.5.
- Set the **Far-end Domain** to `avayalab.com`.
- Set the **DTMF over IP** to `rtp-payload`. This setting enables Communication Manager to send or receive the DTMF transmissions using RFC2833.
- Set **Enable Layer 3 Test?** to `y`. This setting allows Communication Manager to send OPTIONS heartbeat to Session Manager on the SIP trunk.
- Set **Direct IP-IP Audio Connections** to `n`. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to `n`, then the Avaya G450 Media Gateway will remain in the media path between the SIP trunk and the endpoint for the duration of the call. Depending on the number of media resources available in the Avaya G450 Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Alternate Route Timer** to **30**. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Default values may be used for all other fields.
Another signaling group is created between Communication Manager and the Media Server to provide media resources for IP telephony in parallel of the media gateway G450. For the compliance test, signaling group 3 was used for this purpose and was configured as shown in the capture below.

### Signaling Group 3:

<table>
<thead>
<tr>
<th><strong>add signaling-group 3</strong></th>
<th><strong>Page 1 of 2</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIGNALING GROUP</strong></td>
<td></td>
</tr>
<tr>
<td>Group Number: 3</td>
<td></td>
</tr>
<tr>
<td>Group Type: sip</td>
<td></td>
</tr>
<tr>
<td>Transport Method: tls</td>
<td></td>
</tr>
<tr>
<td>Peer Detection Enabled? n</td>
<td>Peer Server: AMS</td>
</tr>
<tr>
<td>Near-end Node Name: procr</td>
<td></td>
</tr>
<tr>
<td>Far-end Node Name: AMS</td>
<td></td>
</tr>
<tr>
<td>Near-end Listen Port: 5061</td>
<td></td>
</tr>
<tr>
<td>Far-end Listen Port: 5061</td>
<td></td>
</tr>
<tr>
<td>Far-end Network Region: 1</td>
<td></td>
</tr>
<tr>
<td>Far-end Domain: 10.33.10.36</td>
<td></td>
</tr>
</tbody>
</table>
### 5.7. Trunk Group

Use the `add trunk-group` command to create a trunk group for the signaling group created in Section 0. For the compliance testing, 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 **Outgoing Display** to `y` to enable name display on the trunk.
- Set the **Service Type** field to `public-ntwrk`.
- Set the **Signaling Group** to the signaling group 2 shown in Section 0.
- Set the **Number of Members** field to customer requirement. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk group.
- Default values are used for all other fields.

<table>
<thead>
<tr>
<th>add trunk-group 2</th>
<th>Page 1 of 21</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Number</strong>: 2</td>
<td><strong>Group Type</strong>: sip</td>
</tr>
<tr>
<td><strong>Group Name</strong>: SIP-Carrier</td>
<td><strong>CDR Reports</strong>: y</td>
</tr>
<tr>
<td><strong>Dial Access</strong></td>
<td><strong>Outgoing Display</strong>: y</td>
</tr>
<tr>
<td><strong>Queue Length</strong>: 0</td>
<td><strong>Service Type</strong>: public-ntwrk</td>
</tr>
<tr>
<td><strong>Service Type</strong>: call-center</td>
<td><strong>Auth Code</strong>: n</td>
</tr>
<tr>
<td><strong>Direction</strong>: two-way</td>
<td><strong>Member Assignment Method</strong>: auto</td>
</tr>
<tr>
<td><strong>Auth Code</strong>: n</td>
<td><strong>Signaling Group</strong>: 2</td>
</tr>
<tr>
<td><strong>Direction</strong>: two-way</td>
<td><strong>Number of Members</strong>: 32</td>
</tr>
</tbody>
</table>

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval a re-INVITEs must be sent to refresh the Session Timer. For the compliance testing, a default value of **600** seconds was used.

<table>
<thead>
<tr>
<th>add trunk-group 2</th>
<th>Page 2 of 21</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Type</strong>: sip</td>
<td><strong>Redirect On OPTIM Failure</strong>: 5000</td>
</tr>
<tr>
<td><strong>Unicode Name</strong>: auto</td>
<td><strong>Digital Loss Group</strong>: 18</td>
</tr>
<tr>
<td><strong>Preferred Minimum Session Refresh Interval (sec)</strong>: 600</td>
<td><strong>Disconnect Supervision - In</strong>: y <strong>Out</strong>: y</td>
</tr>
<tr>
<td>** XOIP Treatment**: auto</td>
<td><strong>Delay Call Setup When Accessed Via IGAR</strong>: N</td>
</tr>
<tr>
<td><strong>Caller ID for Service Link Call to H.323 1xC</strong>: station-extension</td>
<td></td>
</tr>
</tbody>
</table>
On Page 3, set the **Numbering Format** field to **public**. This field specifies the format of the CPN sent to the far-end. The public numbers are automatically preceded with a + sign when passed in the “From”, “Contact” and “P-Asserted Identity” headers.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on the local endpoint to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values are used for all other fields.

On Page 4, the settings are as follow:

- Set the **Network Call Redirection** flag to **n** to disable the use of SIP REFER message to transfer calls back to the PSTN as service provider does not support it.
- Set the **Send Diversion Header** field to **n** as service provider does not support it.
- Set the **Support Request History** field to **n**.
- Set the **Telephone Event Payload Type** to **101**.

---

**TRUNK FEATURES**

- ACA Assignment? **n**
- Measured: **none**
- Maintenance Tests? **y**
- Numbering Format: **public**
- UUI 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**

**PROTOCOL VARIATIONS**

- Mark Users as Phone? **n**
- Prepend ‘+’ to Calling/Alerting/Diverting/Connected Number? **n**
- Send Transferring Party Information? **n**
- Network Call Redirection? **n**
- Send Diversion Header? **n**
- Support Request History? **n**
- Telephone Event Payload Type: **101**
- Convert 180 to 183 for Early Media? **n**
- Always Use re-INVITE for Display Updates? **n**
- Identity for Calling Party Display: **P-Asserted-Identity**
- Block Sending Calling Party Location in INVITE? **n**
- Accept Redirect to Blank User Destination? **n**
- Enable Q-SIF? **n**
5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering is selected to define the format of this number (Section 0), use the `change public-unknown-numbering` command to create an entry for each extension which has a DID assigned. DID numbers are provided by the service provider. They are used to authenticate the caller.

The screen below shows a subset of the 10 digits DID numbers assigned for testing. These 4 numbers were mapped to the 4 enterprise extensions 60396, 60397, 60379 and 60398. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

```
<table>
<thead>
<tr>
<th>Ext Ext Len Code</th>
<th>Trk Grp(s)</th>
<th>CPN Prefix Len</th>
<th>Total Len</th>
<th>Total Administered: 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 60396</td>
<td>2</td>
<td>2066864936</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>5 60397</td>
<td>2</td>
<td>2066864943</td>
<td>10</td>
<td>Maximum Entries: 240</td>
</tr>
<tr>
<td>5 60379</td>
<td>2</td>
<td>2066860216</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>5 60398</td>
<td>2</td>
<td>2066860218</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>
```

5.9. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by INTERMEDIA can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the `change inc-call-handling-trmt trunk-group` command to create an entry for each DID.

```
<table>
<thead>
<tr>
<th>Service/Feature Len Length Digits</th>
<th>Number Number Del Insert</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-ntwrk 10 2066864936</td>
<td>10 60396</td>
</tr>
<tr>
<td>public-ntwrk 10 2066864943</td>
<td>10 60397</td>
</tr>
<tr>
<td>public-ntwrk 10 2066860216</td>
<td>10 60379</td>
</tr>
<tr>
<td>public-ntwrk 10 2066860218</td>
<td>10 60398</td>
</tr>
</tbody>
</table>
```

5.10. Outbound Routing

In these Application Notes, the **Automatic Route Selection** (ARS) feature is used to route an outbound call via the SIP trunk to the service provider via the Avaya SBCE. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code (fac) 9, use the `change dialplan analysis` command as shown below.

<table>
<thead>
<tr>
<th>change dialplan analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIAL PLAN ANALYSIS TABLE</td>
</tr>
<tr>
<td>Location: all</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dialed</th>
<th>Total Call</th>
<th>Dialed</th>
<th>Total Call</th>
<th>Dialed</th>
<th>Total Call</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Length Type</td>
<td></td>
<td>Length Type</td>
<td></td>
<td>Length Type</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>ext</td>
<td>9</td>
<td>1</td>
<td>fac</td>
</tr>
<tr>
<td>30</td>
<td>4</td>
<td>ext</td>
<td>*</td>
<td>3</td>
<td>dac</td>
</tr>
<tr>
<td>39</td>
<td>5</td>
<td>udp</td>
<td>#</td>
<td>4</td>
<td>dac</td>
</tr>
<tr>
<td>60</td>
<td>5</td>
<td>ext</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>change feature-access-codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEATURE ACCESS CODE (FAC)</td>
</tr>
<tr>
<td>Abbreviated Dialing List1 Access Code:</td>
</tr>
<tr>
<td>Abbreviated Dialing List2 Access Code:</td>
</tr>
<tr>
<td>Abbreviated Dialing List3 Access Code:</td>
</tr>
<tr>
<td>Abbreviated Dial – Prm Group List Access Code:</td>
</tr>
<tr>
<td>Announcement Access Code: *05</td>
</tr>
<tr>
<td>Answer Back Access Code:</td>
</tr>
<tr>
<td>Attendant Access Code:</td>
</tr>
<tr>
<td>Auto Alternate Routing (AAR) Access Code:</td>
</tr>
<tr>
<td><strong>Auto Route Selection</strong> (ARS) – Access Code 1: 9 Access Code 2:</td>
</tr>
</tbody>
</table>
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 testing. See Section 2.1 for the complete list of call types tested. All dialed strings are mapped to route pattern 2 for an outbound call which contains the SIP trunk to the service provider (as defined next).

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node Num</th>
<th>Reqd</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>11</td>
<td>2</td>
<td>op</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>011</td>
<td>10</td>
<td>18</td>
<td>2</td>
<td>intl</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>206</td>
<td>11</td>
<td>11</td>
<td>2</td>
<td>publi</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>411</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>pubcl</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>613</td>
<td>11</td>
<td>11</td>
<td>2</td>
<td>publi</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>1866</td>
<td>11</td>
<td>11</td>
<td>2</td>
<td>publi</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>911</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>svcl</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the `change route-pattern` command to configure the parameters for route pattern 2 in the following manner.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group 2 was used.
- **FRL**: Set the Facility Restriction Level (FRL) field to a level that allows access to this trunk for all users that require it. The value of 0 is the least restrictive level.
- **Numbering Format**: `pub-unk`. All calls using this route pattern will use the public numbering table as shown in Section 5.8.

### 5.11. Saving Communication Manager Configuration Changes

The command “save translation all” can be used to save the configuration changes made on Communication Manager.
5.12. TLS Management on Communication Manager

It is (or maybe) necessary to install System Manager CA certificate on Communication Manager for the TLS signalling to work between Avaya Session Manager and Avaya Communication Manager if it is not previously installed.

This section is to show how to install System Manager CA certificate on Communication Manager using Web console.

System Manager CA certificate is obtained using procedure provided in Section 6.9.

From a web browser, type in “https://<ip-address>”, where “<ip-address>” is the IP address or FQDN of Communication Manager. Click on Continue and it will be redirect to login page.

At login page, type in the login ID and its password credential.
Click on Continue again (not shown), navigate to Administration → Server → Trusted Certificates to verify if the System Manager CA certificate is present or not. If it is not, then continue to the next step.

Navigate to Miscellaneous → Download Files, click on File to download from the machine I'm using to connect to the server and click on Browse to where the System Manager CA is being located. Then click on Download button to load the System Manager CA on Communication Manager Server.
Navigate to **Security → Trusted Certificates**, click on **Add** button and enter the certificate name which has been downloaded from above step. Then click **Open**.

Enter the name of the System Manager CA certificate to store the certificate in Communication Manager. Check the Communication Manager check-box. Then click **Add**.

Navigate to **Security → Trusted Certificates** again. It now shows the System Manager CA in the **Trusted Repositories**.
6. Configure Avaya Aura® Session Manager

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

- SIP domain
- Logical/physical Location that can be used by SIP Entities
- 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
- Session Manager, corresponding to the Session Manager server to be managed by System Manager

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

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the Web GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address or FQDN of System Manager. At the System Manager Log On screen, provide the appropriate credentials and click on Login (not shown). The initial screen shown below is then displayed.
Most of the configuration items are performed in the Routing element. Click on Routing in the Elements column to bring up the Introduction to Network Routing Policy screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

6.2. Specify SIP Domain

To view or to change SIP domains, select Routing → Domains. Click on the checkbox next to the name of the SIP domain and Edit to edit an existing domain, or the New button to add a domain. Click the Commit button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain, avayalab.com was already created for communication between Session Manager and Communication Manager. The domain avayalab.com is not known to INTERMEDIA. It will be adapted by the Avaya SBC E to IP address based URI-Host to meet the SIP specification of INTERMEDIA system.
6.3. Add Location

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

In General section, enter the following values:
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

In the Location Pattern section (see the screen below), click **Add** and configure following fields:
- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

Displayed below are the screenshots for location **Belleville**, which includes all equipment on the 10.33.x, 10.10.98.x and 10.10.97.x subnet including Communication Manager, Session Manager and Avaya SBC E. Click **Commit** to save.
6.4. Add 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 Avaya SBCE.

To add a new SIP Entity, navigate to **Routing → SIP Entities** in the left navigation pane and click **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.
- **Type**: Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Location**: Select the location defined in Section Error! Reference source not found. Reference source not found..
- **Time Zone**: Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

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

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

- **Listen Ports**: Port number on which the Session Manager can listen for SIP requests.
- **Protocol**: Transport protocol to be used to send SIP requests.
• **Default Domain**: The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save (not shown).

The compliance test used **Listen Ports** entry 5061 with **TLS** for connecting to Communication Manager and for connecting to the Avaya SBCE.

The following screen shows the addition of the Communication Manager SIP Entity. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to IP address of Communication Manager and **Type** to **CM**. The **Location** and **Time Zone** parameters are set as shown in screen below.
The following screen shows the addition of the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as **SIP Trunk**. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of **120 seconds**. This setting allows Session Manager to send outbound OPTIONS heartbeat every **120 seconds** to service provider (which is forwarded by the Avaya SBCE) to query the status of the SIP trunk connecting to service provider.
Similarly, a SIP Entity is added for Avaya Aura® Messaging server as shown in the capture below.

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony entity is described by an Entity Link. During compliance testing, three Entity Links were created, one for Communication Manager and other for the Avaya SBCE. To add an Entity Link, navigate to Routing → Entity Links in the left navigation pane and click 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 entity defined in Section 6.4.
- **Protocol:** Select the transport protocol used for this link, TLS for the Entity Link to Communication Manager and Avaya Aura® Messaging and TLS for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the Far-end Listen Port defined on the Communication Manager in Section 5.6.
- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in Section Error! Reference source not found. Error! Reference source not found.. For Avaya SBCE, select Avaya SBCE SIP Entity defined in Section Error! Reference source not found..
- **Port**: Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager in **Section 5.6**.

- **Connection Policy**: Select **Trusted**. **Note**: If this is not selected, calls from the associated SIP Entity specified in **Section** will be denied.

- Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and to the Avaya SBCE.

**Entity Link to Communication Manager**

![Entity Link to Communication Manager](image1)

**Entity Link to Avaya SBCE**

![Entity Link to Avaya SBCE](image2)

**Entity Link to Avaya Aura® Messaging**

![Entity Link to Avaya Aura® Messaging](image3)
6.6. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in Section Error! Reference source not found.. Three routing policies were added, one for Communication Manager and other for Avaya SBC. To add a routing policy, navigate to Routing → Routing Policies in the left navigation pane and click New button in the right pane (not shown). The following screen is displayed.

In the General section, configure the following fields:
- Name: Enter a descriptive name.
- Notes: Add a brief description (optional).

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

The following screens show the Routing Policy for Communication Manager.
The following screens show the Routing Policy for the Avaya SBCE.

![Routing Policy for Avaya SBCE](image1)

The following screens show the Routing Policy for the Avaya Aura® Messaging.

![Routing Policy for Avaya Aura](image2)

### 6.7. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Avaya Aura® Messaging and from Communication Manager to INTERMEDIA and vice versa. Dial Patterns define which routing 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 **New** button in the right pane (not shown).
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.
- **Notes**: Add a brief description (optional).

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

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

Two examples of the dial patterns used for the compliance testing are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows that 11-digit dialed numbers that have a destination domain of "avayalab.com" uses route policy to Avaya SBCE as defined in **Section** Error! Reference source not found.
The second example shows that inbound 10-digit numbers with domain “avayalab.com” to use route policy to Communication Manager as defined in Section Error! Reference source not found. These are the DID numbers assigned to the enterprise by INTERMEDIA.

6.8. Add/View Session Manager

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

In the General section, configure the following fields:
- **SIP Entity Name**: Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP**: Enter the IP address of the Session Manager management interface.
- **Directs Routing to Endpoints**: Enabled, to enable call routing on the Session Manager.

In the Security Module section, enter the following values:
- **SIP Entity IP Address**: Should be filled in automatically based on the SIP Entity Name.
- **Network Mask**: Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.
- **Use default values for the remaining fields. Click Commit to save (not shown).
The screen below shows the Session Manager values used for the compliance testing.

### 6.9. TLS Certificate Management on System Manager

This section is to provide a procedure how to download System Manager CA certificate which is being installed on Avaya Communication Manager and Avaya SBCE for the communication between Avaya Aura system component using TLS connectivity.

**How to download System Manager CA certificate from Avaya System Manger**

From System Manager Menu in **Section 6.1**, navigate to **Services → Security**. Click on arrow tab ![](image) to show navigation tree as shown.
Navigate to **Certificates → Authority → CA Functions → CA Structure & CRLs**. Then click on **Download PEM file** to download the System Manager CA and save it as **SystemManagerCA.pem** to a directory on local management PC.
7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya SBCE is used as the edge device between the Avaya CPE and INTERMEDIA SIP Trunking Service.

These Application Notes assume that the installation of the Avaya SBCE and the assignment of a management IP Address have already been completed.

In this session, the naming convention used for INTERMEDIA is Service Provider (SP), which is connected to the external interface of the Avaya SBCE. And for the Avaya side is Enterprise (EN), which is connected to the internal interface of the Avaya SBCE.

7.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Avaya SBCE web interface, enter “https://<ip-addr>/ucsec” in the address field of the web browser (not shown), where “<ip-addr>” is the management LAN IP address of Avaya SBCE.

Enter appropriate credentials and click Log In.

The main page of the Avaya SBCE will appear as shown below.
**7.2. TLS Management**

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

Avaya SBCE is preinstalled with several certificates and profiles that can be used to quickly set up secure communication using TLS, which are listed in the Pre-installed Avaya Profiles and Certificates section. Alternatively, Avaya SBCE supports the configuration of third-party certificates and TLS settings. For optimum security, Avaya recommends using System Manager or third-party certificates.

In this compliance testing, TLS signaling is used for the communication between Avaya Session Manager and Avaya SBCE. The following procedures show how to create the client and server profiles.

**7.2.1. Certificates**

You can use the certificate management functionality that is built into the Avaya SBCE to control all certificates used in TLS handshakes. You can access the Certificates screen from **TLS Management → Certificates**.

Ensure the preinstalled certificates are presented in the system as shown below.

- AvayaSBCCA.crt is Avaya SBCE Certificate Authority root certificate.
- SystemManagerCA.pem is System Manager Certificate Authority root certificate.
If System Manager Certificate Authority certificate (SystemManagerCA.pem) is not present, the following procedure will show how to install it here on Avaya SBCE.

System Manager CA certificate is obtained using procedure provided in Section 6.9. Then on Avaya SBCE, navigate to TLS Management → Certificates. Click on Install button.

- Select CA Certificate.
- Provide a descriptive Name.
- Browse to the directory where the System Manager CA previously saved and select it.
- Click Upload.
### 7.2.2. Client Profiles

This section describes the procedure to create client profile for Avaya SBCE to communicate with Avaya Session Manager via TLS signalling.

To create Client profile, navigate to **TLS Management ➔ Client Profiles**, click on **Add**.
- Enter descriptive name in **Profile Name**.
- Select **AvayaSBC.crt** from pull down menu of **Certificate**.
- Enter **1** as **Verification Depth**.
- Click **Finish**.

![New Profile](image)

> **WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.
7.2.3. Server Profiles
This section describes the procedure to create server profile for Avaya SBCE to communicate with Avaya Session Manager via TLS signalling.

To create Server profile, navigate to TLS Management → Server Profiles, click on Add.

- Enter descriptive name in Profile Name.
- Select AvayaSBC.crt from pull down menu of Certificate.
- Select Required from pull down menu of Peer Verification.
- Enter 1 as Verification Depth.
- Select Custom for Ciphers in Cipher Suit Options section. And Value is specified in the capture shown below.
- Click Finish.
7.3. Global Profiles
Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.3.1. Uniform Resource Identifier (URI) Groups
URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*” is used for all incoming and outgoing traffic.

7.3.2. Server Interworking Profile
Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select Global Profiles → Server Interworking. Click on the Add button.

In the compliance testing, two Server Interworking profiles were created for SP and EN respectively.

Server Interworking profile for SP
Profile SP-SI was defined to match the specification of SP. The General and Advanced tabs are configured with the following parameters while the other tabs for Timers, Header Manipulations and URI Manipulation are kept as default.

General tab:
- Hold Support = NONE. The Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- 18X Handling = None. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- Refer Handling = No. The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- T.38 Support = No. SP does not support T.38 fax in the compliance testing.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile SP-SI, General.
Advanced tab:

- **Record Routes**: Both Sides.
- **Include End Point IP for Context Lookup**: No.
- **Extensions**: None.
- **Has Remote SBC**: Yes. SP has a SBC which interfaces its Central Office (CO) to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from SP for the media.
- **DTMF Support**: None. The Avaya SBCE will send original DTMF method from EN to SP.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile **SP-SI, Advanced**.
Server Interworking profile for EN
Profile EN-SI was defined to match the specification of EN. The General and Advanced tabs are configured with the following parameters while the other settings for Timers, URI Manipulation and Header Manipulation are kept as default.

General tab:
- **Hold Support:** None.
- **18X Handling:** None. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling:** No. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support:** No.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile EN-SI, General.
Advanced tab:

- **Record Routes: Both Sides.** The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Include End Point IP for Context Lookup = Yes.**
- **Extensions: Avaya.**
- **Has Remote SBC: Yes.** This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- **DTMF Support: None.** The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default values.

The screenshots below illustrate the Server Interworking profile EN-SI, Advanced.
### 7.3.3. Configure Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature adds the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

To create a Signaling Manipulation script, select **Global Profiles ➔ Signaling Manipulation**. Click **Add Script** (not shown).

In the compliance testing, a SigMa SP script is created for the Server Configuration for SP and its details are captured below.

![Session Border Controller for Enterprise](image)

### 7.3.4. Server Configuration

The Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains. No configuration of **Heartbeat** is required.

To create a Server Configuration entry, select **Global Profiles ➔ Server Configuration**. Click on the **Add** button.

In the compliance testing, two separate Server Configurations were created, server entry SP-SC for SP and server entry EN-SC for EN.
Server Configuration for SP
Server Configuration named SP-SC was created for SP. All tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN.

**General** tab:
Click on the Edit button and enter the following information.
- Set **Server Type** for SP as **Trunk Server**.
- In the compliance testing, SP supported **TLS** and listened on port **5061**.

**Authentication** tab:
Click on the Edit button and enter following information.
- Check **Enable Authentication** check box.
- Enter **User Name** (provided by SP).
- Leave **Realm** blank.
- Enter **Password** and **Confirm Password** (provided by SP) (not shown).
- Click **Finish**.
**Heartbeat** tab:
Click on the **Edit** button and enter following information.

- Enable **Enable Heartbeat** checkbox.
- Set the **Method** to **REGISTER**.
- Set the **Frequency** to **30 seconds**.
- Set From URI and To URI to `dgwsid169411@192.168.122.44`.

**Advanced** tab:
Click on the **Edit** button and enter following information.

- **Interworking Profile** drop down list, select **SP-SI** as defined in **Section 7.3.2**.
- **Signaling Manipulation Script** drop down list, select **SP** as defined in **Section 7.3.3**.
- The other settings are kept as default.
Server Configuration for EN

Server Configuration named EN-SC created for EN is discussed in detail below. General and Advanced tabs are provisioned but no configuration is done for Authentication tab. The Heartbeat tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

General tab:
Click on the Edit button then specify the following.

- **Server Type** for EN as Call Server.
- **IP Address/FQDN** is Session Manager IP address.
- **Transport**, the link between the Avaya SBCE and EN was **TLS**.
- **Listened on Port 5061**.

![Session Border Controller for Enterprise](image-url)
Advanced tab:
Click on the Edit button to enter the following information.

- **Interworking Profile** drop down list select **EN-SI** as defined in **Section** Error! Reference source not found.
  - The reference source is not found.
- **TLS Client Profile** drop down list select **AvayaSBCClient** as defined in **Section** 7.2.2.
  - The other settings are kept as default.

### 7.3.5. Routing Profiles
Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a Routing Profile, select **Global Profiles → Routing**. Click on the **Add** button.

In the compliance testing, a Routing Profile **EN-to-SP** was created to use in conjunction with the server flow defined for EN. This entry is to route the outbound call from the enterprise to the service provider.

In the opposite direction, a Routing Profile named **SP-to-EN** was created to be used in conjunction with the server flow defined for SP. This entry is to route the inbound call from the service provider to the enterprise.
Routing Profile for SP
The screenshot below illustrate the routing profile from Avaya SBCE to the SP network. Global Profiles → Routing: EN-to-SP. As shown in Figure 1, the SP SIP trunk is connected with transport protocol TLS (not shown). If there is a match in the “To” or “Request URI” headers with the URI Group “*” as described in Section 7.3.1, the call will be routed to the Next Hop Address which is the IP address of SP SIP trunk.

Routing Profile for EN
The Routing Profile for SP to EN, SP-to-EN, was defined to route call where the “To” header matches the URI Group SP defined in Section 7.3.1 to Next Hop Address which is the IP address of Session Manager as a destination. As shown in Figure 1, the SIP trunk between EN and the Avaya SBCE is connected with transport protocol TLS.
7.3.6. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select Global Profiles → Topology Hiding. Click on the Add button.

In the compliance testing, two Topology Hiding profiles EN-to-SP and SP-to-EN were created.

Topology Hiding Profile for SP

Profile EN-to-SP was defined to mask the enterprise SIP domain avayalab.com in the “Request-URI”, “From” and “To” headers to SP provided IP Address. This is done to secure the enterprise network topology and to meet the SIP requirement of the service provider.

Notes:
- The Criteria should be selected as IP/Domain to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header also applies to “Referred-By” and “P-Asserted-Identity” headers.
- The masking applied on “To” header also applies to “Refer-To” header.

The screenshots below illustrate the Topology Hiding profile EN-to-SP.
Topology Hiding Profile for EN

Profile SP-to-EN was also created to mask SP URI-Host in “Request-URI”, “From”, “To”, “Refer-To”, “Referred-By” headers to the enterprise domain avayalab.com. replace Record-Route, Via headers and SDP added by SP to internal IP address known to EN.

Notes:
- The Criteria should be IP/Domain to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header also applies to “Referred-By” and “P-Asserted-Identity” headers.
- The masking applied on “To”, header also applies to “Refer-To” header.

The screenshots below illustrate the Topology Hiding profile SP-to-EN.
7.4. Domain Policies

Domain Policies configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

7.4.1. Media Rules

Media rules can be used 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. You can also define how Avaya SBCE must handle media packets that adhere to the set parameters.

To clone a Media Rule, navigate to Domain Policies → Media Rules. With default-low-med rule chosen, click on the Clone button.

Media Rules for EN and SP

In this compliance testing, Secure Real-Time Transport Protocol (SRTP, media encryption) is used. Therefore, it is necessary to create a media rule to apply to the internal interface of Avaya SBCE, EN and to SP. Created sRTP-MR rule is shown below.
7.4.2. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To clone a Signaling Rule, navigate to Domain Policies → Signaling Rules. With the default rule chosen, click on the Clone button.

Signaling Rules for SP

In the compliance testing, created signaling rule SP-SR is discussed below. All the tabs are kept as default values except the Signaling QoS tab.

In the Signaling QoS tab, click on Edit button then check on checkbox. Then select EF value for DSCP option.
Signaling Rules for EN
In the compliance testing, created signaling rule EN-SR is discussed below. All the tabs are kept as default values except Signaling QoS tab.

In Signaling QoS tab, click on Edit button then check on checkbox. Then select EF value for DSCP option.

### 7.4.3. Endpoint Policy Groups
The rules created within the Domain Policies section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow defined in the next section. Endpoint Policy Groups were created for SP and EN. To create a new policy group, navigate to Domain Policies → Endpoint Policy Groups and click on Add.

**Endpoint Policy Group for SP**
The following screen shows SP-PG created for SP:
- Set Application Rule to default-trunk.
- Set Border Rule to default.
- Set Media Rule to sRTP-MR as created in Section 7.4.1.
- Set Security Rule to default-high
- Set Signaling Rule to SP-SR as created in Section 7.4.2.
Endpoint Policy Group for EN

The following screen shows EN-PG created for EN:

- Set Application Rule to `default-trunk`.
- Set Border Rule to `default`.
- Set Media Rule to `sRTP-MR` as created in Section 7.4.1.
- Set Security Rule to `default-high`.
- Set Signaling Rule to `EN-SR` as created in Section 7.4.2.
7.5. Device Specific Settings

Device Specific Settings allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

7.5.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was defined such as; device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the Network Management tab, which can be edited as needed to optimize device performance and network efficiency.

Enable the interfaces used to connect to the inside and outside networks on the Interface tab. The following screen shows Interface Names, A1 and B1 are Enabled. To enable an interface, click on its Status corresponding to the interface names.
Navigate to **Device Specific Settings → Network** and under the **Network Configuration** tab verify the IP addresses assigned to the interfaces. The following screens show the private interface is assigned to A1 and the public interface is assigned to B1 respectively.
7.5.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open a connection for RTP on the defined ports.

To create a new Media Interface, navigate to Device Specific Settings ➔ Media Interface and click Add.

Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.
7.5.3. Signaling Interface
The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

To create a new Signaling Interface, navigate to Device Specific → Settings → Signaling Interface and click Add.

Separate Signaling Interfaces were created for both inside and outside interfaces.

Signaling Interface for SP
The outside interface to service provider is created with TLS/5061 and TLS profile (Section 7.2.3) as shown below.
**Signaling Interface for EN**

The outside to service provider interface is created with UDP/5060 as shown below.

- Enter descriptive name for **Name** field.
- Select **IP Address** from pull down menu defined as internal network interface Section 7.5.1.
- Specified **5061** for **TLS Port**. Then select **TLS profile** from pull down menu as defined in Section 7.2.3.
- Click **Finish**.
7.5.4. End Point Flows - Server Flow

When a packet is received by the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy 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 screens illustrate the flow through the Avaya SBCE to secure a SIP Trunk call.

In the compliance testing, separate Server Flows were created for SP and EN. To create a Server Flow, navigate to Device Specific Settings → End Point Flows. Select the Server Flows tab and click Add (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select a Server Configuration created in Section 7.3.4 to assign to the Flow.
- **URI Group**: Select the URI Group created in Section 7.3.1 to assign to the Flow.  
  *Note*: URI Group can be set to “*” to match all calls.
- **Received Interface**: Select the Signaling Interface created in Section 7.5.3 that the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface**: Select the Signaling Interface created in Section 7.5.3 used to communicate with the Server Configuration.
- **Media Interface**: Select the Media Interface created in Section 7.5.2 used to communicate with the Server Configuration.
- **End Point Policy Group**: Select the End Point Policy Group created in Section 7.4.3 to assign to the Server Configuration.
- **Routing Profile**: Select the Routing Profile created in Section 7.3.2 that the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile**: Select the Topology-Hiding profile created in Section 7.3.6 to apply to the Server Configuration.
- **Click Finish**.
The following screen shows the Server Flow **SP-SF** configured for SP.

![Session Border Controller for Enterprise](image)

Similarly, the following screen shows the Server Flow **EN-SF** configured for EN.

![Session Border Controller for Enterprise](image)
8. INTERMEDIA Service Configuration

INTERMEDIA is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. INTERMEDIA will provide the customer with the necessary information to configure the SIP connection from the enterprise to INTERMEDIA. The information provided by INTERMEDIA includes:

- IP address and port number used for signaling through security devices (if any).
- IP address and port number used for media through security devices (if any).
- INTERMEDIA SIP domain. In the compliance testing, INTERMEDIA preferred to use IP address as an URI-Host.
- CPE SIP domain. In the compliance testing, INTERMEDIA preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers.

The sample configuration between INTERMEDIA and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP trunk implemented on either INTERMEDIA or enterprise side.

9. Verification and Troubleshooting

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

9.1. Verification Steps

- Verify that endpoints at the enterprise site can place call to PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
- Verify that endpoints at the enterprise site can receive call from PSTN and that the call can remain active for more than 35 seconds. This time period is included satisfy SIP protocol timers.
- Verify that the user on 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. Protocol Traces

The following SIP headers are inspected using Wireshark trace analysis:

- Request-URI: verify the called party number and SIP domain.
- From: verify the calling party name and number.
- To: verify the called party name and number.
- P-Asserted-Identity: verify the calling party name and number.
- Privacy: verify the value “user” and/or “id” presents the private call scenario.

The following attributes in SIP message body are inspected using Wireshark trace analysis:
9.3. Troubleshooting:

9.3.1. The Avaya SBCE

Use a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling messages between INTERMEDIA and the Avaya SBCE.

9.3.2. Communication Manager

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

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 to INTERMEDIA SIP Trunking Service. INTERMEDIA SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. INTERMEDIA provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases were executed. Despite the observation seen during testing as noted in Section 2.2, the test results met the objectives outlined in Section 2.1. The INTERMEDIA SIP Trunking Service is considered compliant with Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0.
11. References

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


Product documentation for Intermedia Networks’ SIP Trunking Solution is available from Intermedia.