



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

---

# **Application Notes for Computer Instruments eONE with Avaya Session Border Controller for Enterprise – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required to integrate Computer Instruments eONE MT 3.2 with Avaya Session Border Controller for Enterprise 10.1. Computer Instruments eONE is a cloud-based IVR development platform that provides self-service IVR and Web applications. In the compliance test, Computer Instruments eONE connected to Avaya Session Border Controller for Enterprise via a SIP trunk. All calls were routed through Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required to integrate Computer Instruments eONE MT 3.2 with Avaya Session Border Controller for Enterprise 10.1. Computer Instruments eONE is a cloud-based IVR development platform that provides self-service IVR and Web applications. In the compliance test, Computer Instruments eONE connected to the public/external interface of the Avaya Session Border Controller for Enterprise via a SIP trunk.

In the compliance test, incoming PSTN calls were routed from Avaya Session Border Controller for Enterprise (SBCE) through Avaya Aura® Session Manager and Avaya Aura® Communication Manager, and then to Computer Instruments eONE. Outbound calls and transferred calls from Computer Instruments eONE to local numbers in the enterprise or the PSTN were routed in a similar manner.

Calls delivered to Computer Instruments eONE were answered by an IVR application that allowed callers to hear announcements, navigate the application menu via DTMF, request a blind transfer to a local or PSTN number, and record an audio message. In addition, Computer Instruments eONE also supports outbound call campaigns.

## 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on PSTN calls being routed to eONE through SBCE, Session Manager, and Communication Manager. Calls to eONE were answered by a sample IVR application that allowed callers to hear announcements, record a message, and transfer the call. Callers interacted with eONE using DTMF via a telephone keypad. In addition, an outbound call campaign from eONE to multiple users was also verified. The serviceability test cases verified calls to eONE were successful after the SBCE was restarted and came back into service.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. 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 testing associated with these Application Notes, the interface between Avaya systems and Computer Instruments eONE utilized encryption capabilities of TLS/SRTP.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP trunk between SBCE and eONE using TLS transport.
- eONE successfully responding to SIP OPTIONS messages from SBCE.
- Calls from the PSTN and local users to eONE.
- PSTN calls routed through SBCE, Session Manager, and Communication Manager to eONE with Direct IP Media (Shuffling) enabled and disabled.
- eONE providing service via a sample IVR application and callers navigating the application using DTMF.
- eONE transferring calls to the PSTN or local users in the enterprise.
- eONE outbound call campaign to multiple users simultaneously.
- Multiple simultaneous calls to eONE.
- Telephony features, such as holding and resuming calls to eONE, transferring calls to eONE, joining eONE in a conference, and forwarding calls to eONE.
- Maintaining calls to eONE for 30 minutes.
- DTMF transmission using RFC2833.
- SIP signaling encrypted using TLS 1.2 and a secure PFS cipher.
- Audio encrypted using SRTP.
- G.711mu-law codec support.
- Restarting SBCE and verifying the SIP trunk was successfully re-established and no adverse effects on eONE.

## 2.2. Test Results

All test cases passed with the following observation.

- When eONE attempts to blind transfer a PSTN call to an invalid or busy number (i.e., transfer call not completed), eONE would send a SIP BYE to disconnect from the call. If Direct IP Media (i.e., shuffling) is enabled on Communication Manager, the SIP BYE would not be forwarded to the PSTN caller, who stays connected listening to silence. In this case, eONE sends the SIP BYE after receiving the re-INVITE from Communication Manager to initiate Direct IP Media. After approximately a minute, Communication Manager would then send a SIP BYE to the PSTN caller to drop the call. This is an uncommon scenario, because it is unlikely that eONE would attempt to transfer a call to an invalid number since eONE verifies the transfer-to number against a directory or database. It is also unlikely that phones on Communication Manager with multiple call appearances and call coverage would return busy. However, if this is an issue, Direct IP Media may be disabled on Communication Manager to avoid this issue.

## 2.3. Support

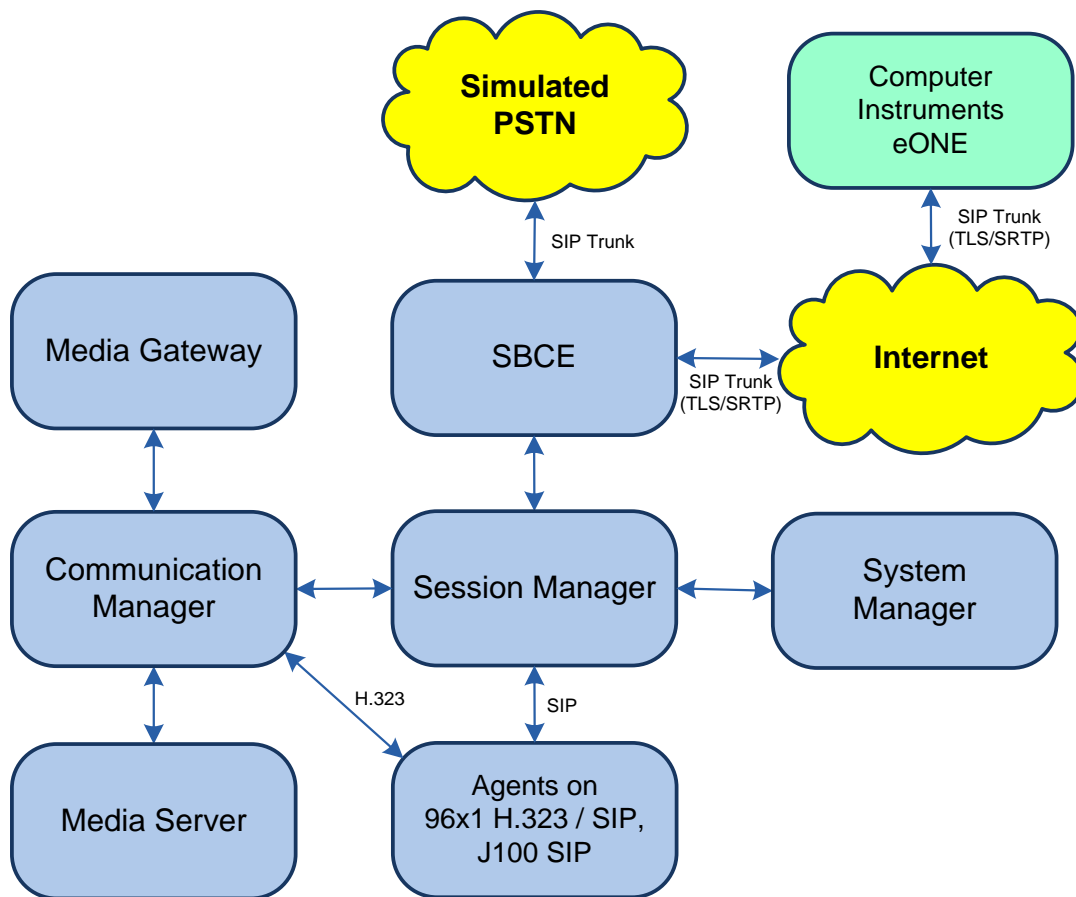
Technical support on Computer Instruments eONE can be obtained through the following:

- **Phone:** (888) 451-0851
- **Web:** <https://instruments.com/contact/>

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration consisting of eONE connected to SBCE via a SIP trunk using TLS/SRTP over the Internet. Calls are routed through an Avaya Aura® environment consisting of the following products:

- SBCE with SIP trunk connectivity to Session Manager, eONE, and the PSTN.
- Session Manager connected to SBCE and Communication Manager via SIP trunks and acting as a Registrar/Proxy for SIP telephones.
- Media resources in Avaya G430 Media Gateway and Avaya Aura® Media Server.
- System Manager used to configure Session Manager.
- Avaya 96x1 Series H.323 Deskphones and Avaya J100 Series SIP Phones registered to Communication Manager for H.323 deskphones and Session Manager for IP deskphones.



**Figure 1: Avaya Aura® Environment with Computer Instruments eONE**

## 4. Equipment and Software Validated

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

| Equipment/Software                             | Release/Version  |
|--|--|
| Avaya Aura® Communication Manager              | 10.1.0.1.0-SP1   |
| Avaya G430 Media Gateway                       | FW 42.8.0  |
| Avaya Aura® Media Server                       | v.10.1.0.77  |
| Avaya Aura® System Manager                     | 10.1.0.1<br>Build No. – 10.1.0.0.537353<br>Software Update Revision No:<br>10.1.0.1.061394<br>Service Pack 1 |
| Avaya Aura® Session Manager                    | 10.1.0.1.1010105   |
| Avaya Session Border Controller for Enterprise | 10.1.1.0-35-21872  |
| Avaya 96x1 Series IP Desk phones               | 6.8.5.3.2 (H.323)  |
| Avaya J100 Series IP Telephones                | 4.0.13.0.6 (SIP)   |
| Computer Instruments                           | MT 3.2   |

## 5. Configure Avaya Aura® Communication Manager

This section covers the configuration steps required to establish a SIP trunk between Communication Manager and Session Manager and routing calls to eONE. Communication Manager is configured through the System Access Terminal (SAT). The procedures include the following areas:

- Verify Licenses
- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer Private Numbering
- Administer AAR Call Routing
- Administer Call Center

### 5.1. Verify Licenses

Using the SAT, enter the **display system-parameters customer-options** command to verify there is sufficient capacity for SIP trunks on **Page 2**. The license file installed on the system controls these options. If there is insufficient capacity of SIP Trunks or a required feature is not enabled, 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:                      |  | 2400         |      | 2         |
| Maximum Administered Remote Office Trunks:                        |  | 12000        |      | 0         |
| Max Concurrently Registered Remote Office Stations:               |  | 2400         |      | 0         |
| Maximum Concurrently Registered IP eCons:                         |  | 128          |      | 0         |
| Max Concur Reg Unauthenticated H.323 Stations:                    |  | 100          |      | 0         |
| Maximum Video Capable Stations:                                   |  | 36000        |      | 2         |
| Maximum Video Capable IP Softphones:                              |  | 2400         |      | 2         |
| <b>Maximum Administered SIP Trunks:</b>                           |  | <b>12000</b> |      | <b>30</b> |
| Max Administered Ad-hoc Video Conferencing Ports:                 |  | 12000        |      | 0         |
| Max Number of DS1 Boards with Echo Cancellation:                  |  | 688          |      | 0         |
| (NOTE: You must logoff & login to effect the permission changes.) |  |              |      |           |

## 5.2. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

|   |                      |             |
|---|----------------------|-------------|
| change node-names ip  |                      | Page 1 of 2 |
| IP NODE NAMES   |                      |             |
| Name  | IP Address           |             |
| default   | 0.0.0.0              |             |
| devcon-aes  | 10.64.102.119        |             |
| devcon-ams  | 10.64.102.118        |             |
| <b>devcon-sm</b>  | <b>10.64.102.117</b> |             |
| <b>procr</b>  | <b>10.64.102.115</b> |             |
| 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 |                      |             |

## 5.3. Administer IP Codec Set

In the **IP Codec Set** form, specify the audio codec to be used by eONE. The form is accessed via the **change ip-codec-set** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, G.711MU was used.

**Media Encryption** was allowed and **Encrypted SRTCP** was set to *best-effort* as shown below. eONE used *1-srtp-aescm128-hmac80* for media encryption.

|                                  |             |                                     |           |
|----------------------------------|-------------|-------------------------------------|-----------|
| change ip-codec-set 2            |             | Page 1 of 2                         |           |
| IP MEDIA PARAMETERS              |             |                                     |           |
| Codec Set: 2                     |             |                                     |           |
| Audio                            | Silence     | Frames                              | Packet    |
| Codec                            | Suppression | Per Pkt                             | Size (ms) |
| 1: <b>G.711MU</b>                | <b>n</b>    | <b>2</b>                            | <b>20</b> |
| 2:                               |             |                                     |           |
| 3:                               |             |                                     |           |
| 4:                               |             |                                     |           |
| 5:                               |             |                                     |           |
| 6:                               |             |                                     |           |
| 7:                               |             |                                     |           |
| <b>Media Encryption</b>          |             | <b>Encrypted SRTCP: best-effort</b> |           |
| 1: <b>1-srtp-aescm128-hmac80</b> |             |                                     |           |
| 2: <b>2-srtp-aescm128-hmac32</b> |             |                                     |           |
| 3: <b>none</b>                   |             |                                     |           |
| 4:                               |             |                                     |           |
| 5:                               |             |                                     |           |

## 5.4. Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for eONE and enable **IP-IP Direct Audio** (Shuffling), if desired. Shuffling allows audio traffic to be sent directly between IP endpoints and SBCE without using media resources in the Avaya Media Gateway or Avaya Aura® Media Server after call establishment. For this compliance test, shuffling was enabled. The **Authoritative Domain** for this configuration is *avaya.com*.

|                                 |   |   |
|---------------------------------|---|---|
| change ip-network-region 2      |   | Page 1 of 20                                |
| IP NETWORK REGION               |   |   |
| Region: 2                       | NR Group: 2                                 |   |
| Location: 1                     | <b>Authoritative Domain: avaya.com</b>      |   |
| Name: To Avaya SBCE             | Stub Network Region: n                      |   |
| MEDIA PARAMETERS                |   | <b>Intra-region IP-IP Direct Audio: yes</b> |
| Codec Set: 2                    | <b>Inter-region IP-IP Direct Audio: yes</b> |   |
| UDP Port Min: 2048              | IP Audio Hairpinning? n                     |   |
| UDP Port Max: 3329              |   |   |
| DIFFSERV/TOS PARAMETERS         |   |   |
| Call Control PHB Value: 46      |   |   |
| Audio PHB Value: 46             |   |   |
| Video PHB Value: 26             |   |   |
| 802.1P/Q PARAMETERS             |   |   |
| Call Control 802.1p Priority: 6 |   |   |
| Audio 802.1p Priority: 6        |   |   |
| Video 802.1p Priority: 5        | AUDIO RESOURCE RESERVATION PARAMETERS       |   |
| H.323 IP ENDPOINTS              | RSVP Enabled? n                             |   |
| H.323 Link Bounce Recovery? y   |   |   |
| Idle Traffic Interval (sec): 20 |   |   |
| Keep-Alive Interval (sec): 5    |   |   |
| Keep-Alive Count: 5             |   |   |



## 5.5. Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*, but *tcp* is also supported.
- Specify Communication Manager (*procr*) and the Session Manager (*devcon-sm*) as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the appropriate TLS port value is specified (e.g., *5062*) in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- **Direct IP-IP Audio Connections** is enabled to allow shuffling for calls routed over the trunk group associated with this signaling group.
- Set **Initial IP-IP Direct Media** field to *y*.

Communication Manager supports DTMF transmission using RFC 2833 by setting **DTMF over IP** to *rtp-payload*. The default values for the other fields may be used.

| add signaling-group 11  |                                    | Page 1 of 2                  |
|---|------------------------------------|------------------------------|
| SIGNALING GROUP   |                                    |                              |
| Group Number: 11  | Group Type: sip                    |                              |
| IMS Enabled? n  | Transport Method: tls              |                              |
| Q-SIP? n  |                                    |                              |
| IP Video? y   | Priority Video? n                  | Enforce SIPS URI for SRTP? n |
| Peer Detection Enabled? y   | Peer Server: SM                    | Clustered? n                 |
| Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y  |                                    |                              |
| Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n |                                    |                              |
| Alert Incoming SIP Crisis Calls? n  |                                    |                              |
| Near-end Node Name: procr   | Far-end Node Name: devcon-sm       |                              |
| Near-end Listen Port: 5062  | Far-end Listen Port: 5062          |                              |
|   | Far-end Network Region: 2          |                              |
| Far-end Domain: avaya.com   |                                    |                              |
| Incoming Dialog Loopbacks: eliminate  | Bypass If IP Threshold Exceeded? n |                              |
| DTMF over IP: rtp-payload   | RFC 3389 Comfort Noise? n          |                              |
| Session Establishment Timer(min): 3   | Direct IP-IP Audio Connections? y  |                              |
| Enable Layer 3 Test? y  | IP Audio Hairpinning? n            |                              |
| H.323 Station Outgoing Direct Media? n  | Initial IP-IP Direct Media? y      |                              |
|   | Alternate Route Timer(sec): 6      |                              |

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to the VoIP Service Provider. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

|                                     |                                |                |           |
|-------------------------------------|--------------------------------|----------------|-----------|
| add trunk-group 11                  |                                | Page 1 of 5    |           |
| TRUNK GROUP                         |                                |                |           |
| Group Number: 11                    | <b>Group Type: sip</b>         | CDR Reports: y |           |
| Group Name: To SIP Service Provider | COR: 1                         | TN: 1          | TAC: 1011 |
| Direction: two-way                  | Outgoing Display? n            |                |           |
| Dial Access? n                      | Night Service:                 |                |           |
| Queue Length: 0                     |                                |                |           |
| <b>Service Type: tie</b>            | Auth Code? n                   |                |           |
|                                     | Member Assignment Method: auto |                |           |
|                                     | <b>Signaling Group: 11</b>     |                |           |
|                                     | <b>Number of Members: 10</b>   |                |           |

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number sent to the far-end.

|                                |                                   |                      |  |
|--------------------------------|-----------------------------------|----------------------|--|
| add trunk-group 11             |                                   | Page 3 of 5          |  |
| TRUNK FEATURES                 |                                   |                      |  |
| ACA Assignment? n              | Measured: none                    | Maintenance Tests? y |  |
|                                |                                   |                      |  |
| Suppress # Outpulsing? n       | <b>Numbering Format: private</b>  |                      |  |
|                                | UII Treatment: shared             |                      |  |
|                                | Maximum Size of UII Contents: 128 |                      |  |
|                                | Replace Restricted Numbers? n     |                      |  |
|                                | Replace Unavailable Numbers? n    |                      |  |
|                                |                                   |                      |  |
|                                | Modify Tandem Calling Number: no  |                      |  |
| Send UCID? n                   |                                   |                      |  |
|                                |                                   |                      |  |
| Show ANSWERED BY on Display? y |                                   |                      |  |

On **Page 5** of the trunk group form, set the **Telephone Event Payload Type** field to **101**, required by eONE in the compliance test, to avoid DTMF issues.

|   |             |
|---|-------------|
| add trunk-group 11  | Page 5 of 5 |
| <p>PROTOCOL VARIATIONS</p> <p>Mark Users as Phone? n</p> <p>Prepend '+' to Calling/Alerting/Diverting/Connected Number? n</p> <p>Send Transferring Party Information? n</p> <p>Network Call Redirection? n</p> <p>Send Diversion Header? n</p> <p>Support Request History? y</p> <p><b>Telephone Event Payload Type: 101</b></p> <p>Convert 180 to 183 for Early Media? n</p> <p>Always Use re-INVITE for Display Updates? n</p> <p>Resend Display UPDATE Once on Receipt of 481 Response? n</p> <p>Identity for Calling Party Display: P-Asserted-Identity</p> <p>Block Sending Calling Party Location in INVITE? n</p> <p>Accept Redirect to Blank User Destination? n</p> <p>Enable Q-SIP? n</p> <p>Interworking of ISDN Clearing with In-Band Tones: keep-channel-active</p> <p>Request URI Contents: may-have-extra-digits</p> |             |

## 5.6. Administer AAR Call Routing

Configure the **Uniform Dial Plan** to steer calls to eONE to AAR using extension 78880 as shown below.

| change uniform-dialplan 7  | Page 1 of 2 |                  |               |                   |               |                   |    |   |   |  |       |
|--|-------------|------------------|---------------|-------------------|---------------|-------------------|----|---|---|--|-------|
| <p>UNIFORM DIAL PLAN TABLE</p> <p>Percent Full: 0</p> <table border="1"> <thead> <tr> <th>Matching Pattern</th> <th>Len</th> <th>Del</th> <th>Insert Digits</th> <th>Node Net Conv Num</th> </tr> </thead> <tbody> <tr> <td>78</td> <td>5</td> <td>0</td> <td></td> <td>aar n</td> </tr> </tbody> </table> |             | Matching Pattern | Len           | Del               | Insert Digits | Node Net Conv Num | 78 | 5 | 0 |  | aar n |
| Matching Pattern   | Len         | Del              | Insert Digits | Node Net Conv Num |               |                   |    |   |   |  |       |
| 78   | 5           | 0                |               | aar n             |               |                   |    |   |   |  |       |

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and add entries to route calls to eONE. 78880 was used to route calls to eONE. These calls were routed to route pattern 14 as shown below.

| change aar analysis 78  | Page 1 of 2 |               |               |           |               |           |          |         |     |   |   |    |      |  |   |
|---|-------------|---------------|---------------|-----------|---------------|-----------|----------|---------|-----|---|---|----|------|--|---|
| <p>AAR DIGIT ANALYSIS TABLE</p> <p>Location: all</p> <p>Percent Full: 1</p> <table border="1"> <thead> <tr> <th>Dialed String</th> <th>Total Min</th> <th>Total Max</th> <th>Route Pattern</th> <th>Call Type</th> <th>Node Num</th> <th>ANI Req</th> </tr> </thead> <tbody> <tr> <td>788</td> <td>5</td> <td>5</td> <td>14</td> <td>lev0</td> <td></td> <td>n</td> </tr> </tbody> </table> |             | Dialed String | Total Min     | Total Max | Route Pattern | Call Type | Node Num | ANI Req | 788 | 5 | 5 | 14 | lev0 |  | n |
| Dialed String   | Total Min   | Total Max     | Route Pattern | Call Type | Node Num      | ANI Req   |          |         |     |   |   |    |      |  |   |
| 788   | 5           | 5             | 14            | lev0      |               | n         |          |         |     |   |   |    |      |  |   |

Configure a preference in **Route Pattern 14** to route calls over SIP trunk group **11** as shown below.

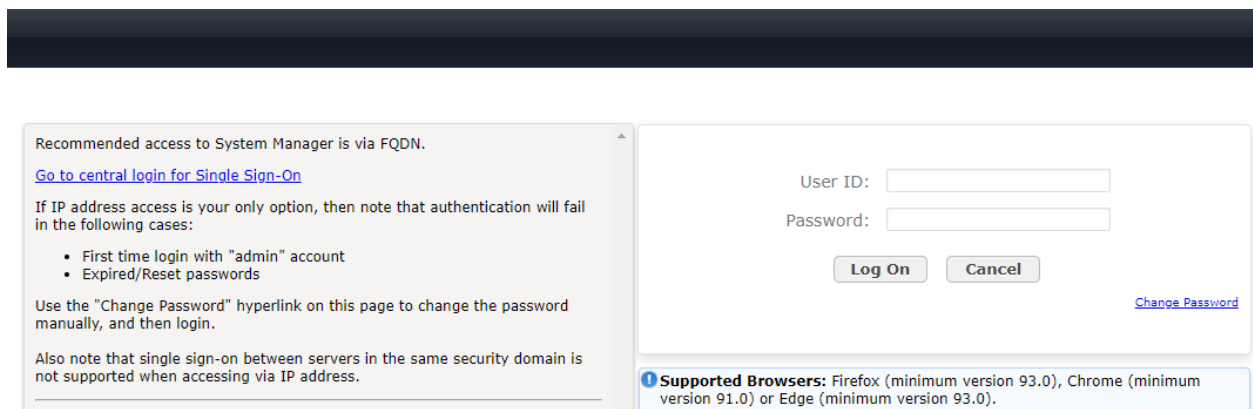
|                                       |  |               |  |                          |  |  |  |  |  |                          |  |                 |  |          |  |               |  |
|---------------------------------------|--|---------------|--|--------------------------|--|--|--|--|--|--------------------------|--|-----------------|--|----------|--|---------------|--|
| change route-pattern 14               |  |               |  |                          |  |  |  |  |  | Page                     |  | 1 of 4          |  |          |  |               |  |
| Pattern Number: 14                    |  |               |  |                          |  |  |  |  |  | Pattern Name: To CI eONE |  |                 |  |          |  |               |  |
| SCCAN? n                              |  | Secure SIP? n |  | Used for SIP stations? n |  |  |  |  |  |                          |  |                 |  |          |  |               |  |
| Grp FRL NPA Pfx Hop Toll No. Inserted |  |               |  |                          |  |  |  |  |  | DCS/ IXC                 |  |                 |  |          |  |               |  |
| No Mrk Lmt List Del Digits            |  |               |  |                          |  |  |  |  |  | QSIG                     |  |                 |  |          |  |               |  |
| Dgts                                  |  |               |  |                          |  |  |  |  |  | Intw                     |  |                 |  |          |  |               |  |
| 1: 11                                 |  | 0             |  |                          |  |  |  |  |  | n                        |  | user            |  |          |  |               |  |
| 2:                                    |  |               |  |                          |  |  |  |  |  | n                        |  | user            |  |          |  |               |  |
| 3:                                    |  |               |  |                          |  |  |  |  |  | n                        |  | user            |  |          |  |               |  |
| 4:                                    |  |               |  |                          |  |  |  |  |  | n                        |  | user            |  |          |  |               |  |
| 5:                                    |  |               |  |                          |  |  |  |  |  | n                        |  | user            |  |          |  |               |  |
| 6:                                    |  |               |  |                          |  |  |  |  |  | n                        |  | user            |  |          |  |               |  |
| BCC VALUE TSC CA-TSC                  |  |               |  |                          |  |  |  |  |  | ITC BCIE                 |  | Service/Feature |  | PARM Sub |  | Numbering LAR |  |
| 0 1 2 M 4 W Request                   |  |               |  |                          |  |  |  |  |  |                          |  |                 |  | Dgts     |  | Format        |  |
| 1: y y y y y n                        |  | n             |  |                          |  |  |  |  |  | rest                     |  |                 |  | unk-unk  |  | none          |  |
| 2: y y y y y n                        |  | n             |  |                          |  |  |  |  |  | rest                     |  |                 |  |          |  | none          |  |

## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager to route calls to/from eONE. The procedure includes adding the following items:

- SIP Entities for Communication Manager and SBCE
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and SBCE
- Routing Policies and Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager server to be managed by Avaya Aura® System 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.



Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

## 6.1. Add SIP Entities and Entity Links

In the sample configuration, two SIP Entities were added for Communication Manager and SBCE. This section also covers the configuration of the Entity Links.

### 6.1.1. SIP Entity and Entity Link for Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Although an adaptation is shown in the SIP entity, it was not required for this solution. The **Adaptation** field may be left blank.

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on Communication Manager.
- **Type:** Select *CM*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

Default values can be used for the remaining fields.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area displays the 'SIP Entity Details' form. The form has a 'General' tab and a 'Commit' button. The fields are as follows:

- Name:** devcon-cm SBC Trk
- FQDN or IP Address:** 10.64.102.115
- Type:** CM
- Notes:** From SBCE
- Adaptation:** CM SBC Adaptation
- Location:** Thornton
- Time Zone:** America/New\_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty field)
- Securable:** ☐
- Call Detail Recording:** none

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TLS*.
- **Port:** Set to appropriate TLS port (e.g., *5062*).
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** Set to appropriate TLS port (e.g., *5062*).
- **Connection Policy:** Set to *trusted*.

#### Entity Links

Override Port & Transport with DNS SRV: ☐

| <input type="button" value="Add"/> <input type="button" value="Remove"/> |                          |  |          |        |  |        |                   |
|--|--------------------------|--|----------|--------|--|--------|-------------------|
| 1 Item   |                          |  |          |        |  |        | Filter: Enable    |
| <input type="checkbox"/>   | Name                     | SIP Entity 1                           | Protocol | Port   | SIP Entity 2                                   | Port   | Connection Policy |
| <input type="checkbox"/>   | * devcon-cm SBC Trk Link | <input type="text" value="devcon-sm"/> | TLS ▼    | * 5062 | <input type="text" value="devcon-cm SBC Trk"/> | * 5062 | trusted ▼         |

Select : All, None

### 6.1.2. SIP Entity and Entity Link for SBCE

A SIP Entity must be added for SBCE. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for SBCE.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the SBCE internal interface.
- **Type:** Select *SIP Trunk*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and a menu with 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

| Field                      | Value                    |
|----------------------------|--------------------------|
| Name                       | devcon-sbce              |
| FQDN or IP Address         | 10.64.102.106            |
| Type                       | SIP Trunk                |
| Notes                      |                          |
| Adaptation                 |                          |
| Location                   | Thornton-SBC             |
| Time Zone                  | America/New_York         |
| SIP Timer B/F (in seconds) | 4                        |
| Minimum TLS Version        | Use Global Setting       |
| Credential name            |                          |
| Securable                  | <input type="checkbox"/> |
| Call Detail Recording      | egress                   |



Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TLS*. TCP may also be used between Session Manager and SBCE.
- **Port:** Set to appropriate TLS port (e.g., *5061*).
- **SIP Entity 2:** The SBCE entity name from this section.
- **Port:** Set to appropriate TLS port (e.g., *5061*).
- **Connection Policy:** Set to *trusted*.

#### Entity Links

Override Port & Transport with DNS SRV: ☐

| Add Remove               |                    | 1 Item       |          |        |              |        |                   | Filter: Enable |
|--------------------------|--------------------|--------------|----------|--------|--------------|--------|-------------------|----------------|
| <input type="checkbox"/> | Name               | SIP Entity 1 | Protocol | Port   | SIP Entity 2 | Port   | Connection Policy |                |
| <input type="checkbox"/> | * devcon-sbce Link | devcon-sm    | TLS ▼    | * 5061 | devcon-sbce  | * 5061 | trusted ▼         |                |

Select : All, None

## 6.2. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.1**. Two routing policies were added, one for SBCE to route outgoing calls to the eONE and PSTN, and for Communication Manager to route calls to local number. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

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

The following routing policy routes calls to eONE and PSTN.

**Routing Policy Details** [Commit] [Cancel] [Help ?]

**General**

\* Name: devcon-sbce Policy

Disabled: ☐

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

| Name        | FQDN or IP Address | Type      | Notes |
|-------------|--------------------|-----------|-------|
| devcon-sbce | 10.64.102.106      | SIP Trunk |       |

Time of Day

The following routing policy routes calls from eONE and PSTN to local numbers.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a navigation tree with 'Routing' selected, and 'Routing Policies' highlighted at the bottom. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Name' is 'devcon-cm SBC Trk Policy', 'Disabled' is unchecked, 'Retries' is '0', and there is a 'Notes' field. The 'SIP Entity as Destination' section features a table with one entry: 'devcon-cm SBC Trk' with FQDN or IP Address '10.64.102.115', Type 'CM', and Notes 'From SBCE'. A 'Time of Day' section is partially visible at the bottom.

**Routing Policy Details** Commit Cancel Help ?

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

| Name              | FQDN or IP Address | Type | Notes     |
|-------------------|--------------------|------|-----------|
| devcon-cm SBC Trk | 10.64.102.115      | CM   | From SBCE |

**Time of Day**

## 6.3. Add Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, 5-digit extensions beginning with '7' for local numbers were routed to Communication Manager, 10-digit numbers beginning with '91' for PSTN calls were also routed to Communication Manager and then to SBCE, and extension 78880 for eONE was routed to SBCE.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

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

The following screen shows the dial pattern definition for routing local calls to Communication Manager.

**AVAYA**  
Aura® System Manager 10.1

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

Home Routing

Routing

- Domains
- Locations
- Conditions
- Adaptations ▾
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies**
- Dial Patterns
- Origination Dial Pat...

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* **Pattern:** 7

\* **Min:** 5

\* **Max:** 5

**Emergency Call:** ☐

**SIP Domain:** -ALL-

**Notes:** CM Stations from SIP Trunks

**Originating Locations and Routing Policies**

Add Remove

2 Items

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name      | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|--------------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | Thornton-SBC              |                            | devcon-cm SBC Trk Policy | 0    | <input type="checkbox"/> | devcon-cm SBC Trk          |                      |
| <input type="checkbox"/> | Thornton                  |                            | devcon-cm Policy         | 0    | <input type="checkbox"/> | devcon-cm                  |                      |

Select : All, None

The following screen shows the dial pattern definition for routing PSTN calls to Communication Manager, which eventually will be routed to SBCE.

**AVAYA**  
Aura® System Manager 10.1

Users Elements Services Widgets Shortcuts Search admin

Home Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Origination Dial Pat...

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* Pattern: 91

\* Min: 12

\* Max: 12

Emergency Call: ☐

SIP Domain: -ALL-

Notes: CM PSTN Calls

**Originating Locations and Routing Policies**

Add Remove

2 Items

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name      | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|--------------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | Thornton-SBC              |                            | devcon-cm SBC Trk Policy | 0    | <input type="checkbox"/> | devcon-cm SBC Trk          |                      |
| <input type="checkbox"/> | Thornton                  |                            | devcon-cm Policy         | 0    | <input type="checkbox"/> | devcon-cm                  |                      |

Select : All, None

The following screen shows the dial pattern definition for routing calls to eONE.

**AVAYA**  
Aura® System Manager 10.1

Users Elements Services Widgets Shortcuts Search admin

Home Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Origination Dial Pat...

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* Pattern: 788

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes: CI eONE

**Originating Locations and Routing Policies**

Add Remove

1 Item

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled  | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | -ALL-                     |                            | devcon-sbce Policy  | 0    | <input type="checkbox"/> | devcon-sbce                |                      |

Select : All, None

## 7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya SBCE. Avaya SBCE provides SIP connectivity to Session Manager, eONE, and the PSTN.

This section covers the following SBCE configuration:

- Launch SBCE Web Interface
- Administer SIP Servers
- Administer Routing Profiles
- Administer URI Groups
- Administer Media Rules
- Administer End Point Policy Groups
- Administer TLS Management
- Administer Media Interfaces
- Administer Signaling Interfaces
- Administer End Point Flows

**Note:** This section will focus on routing and connectivity for Session Manager and eONE. The configuration for the PSTN is not covered. For security reasons, public IP addresses will be redacted in these Application Notes.

### 7.1. Launch SBCE Web Interface

Access the SBCE web interface by using the URL **https://<ip-address>/sbc** in an Internet browser window, where <ip-address> is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



The image shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with 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, a message reads "WELCOME TO AVAYA SBC". Below that, a disclaimer states: "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." This is followed by 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, the copyright notice "© 2011 - 2020 Avaya Inc. All rights reserved." is visible.

After logging in, the **Dashboard** will appear as shown below. All configuration screens of the SBCE are accessed by navigating the menu tree in the left pane. Select **Device** → **SBCE** from the top menu.

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

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Dashboard

| Information                  |                              |                         |
|------------------------------|------------------------------|-------------------------|
| System Time                  | 11:01:28 AM EDT              | <a href="#">Refresh</a> |
| Version                      | 10.1.1.0-35-21872            |                         |
| GUI Version                  | 10.1.1.0-21872               |                         |
| Build Date                   | Mon Apr 18 07:57:04 UTC 2022 |                         |
| License State                | ✔ OK                         |                         |
| Aggregate Licensing Overages | 0                            |                         |
| Peak Licensing Overage Count | 0                            |                         |
| Last Logged in at            | 07/12/2022 08:52:18 EDT      |                         |
| Failed Login Attempts        | 0                            |                         |

| Active Alarms (past 24 hours) |  |
|-------------------------------|--|
| None found.                   |  |

| Installed Devices |  |
|-------------------|--|
| EMS               |  |
| SBCE              |  |

| Incidents (past 24 hours)                         |  |
|---|--|
| SBCE: No Server Flow Matched for Outgoing Message |  |
| SBCE: No Server Flow Matched for Outgoing Message |  |
| SBCE: No Server Flow Matched for Outgoing Message |  |
| SBCE: No Server Flow Matched for Outgoing Message |  |
| SBCE: No Server Flow Matched for Outgoing Message |  |

Add

| Notes           |  |
|-----------------|--|
| No notes found. |  |

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

23 of 53  
CI-eONE-SBCE10

## 7.2. Administer Server Interworking Profiles

A server interworking profile defines a set of parameters that aid in interworking between the SBCE and a connected server. **Server Interworking** profiles were added for Session Manager and eONE.

### 7.2.1. Server Interworking Profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile. The **General** tab below shows the default settings.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

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

Interworking Profiles: Avaya-SM

Add

Interworking Profiles

cs2100  
avaya-ru  
**Avaya-SM**  
PSTN-SIP  
PCIPal  
VoIPSP

Rename Clone Delete

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

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

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

24 of 53  
CI-eONE-SBCE10



Select the **Advanced** tab and configure as shown in the screen capture below.

Device: SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Settings ▾

Help ▾

Log Out

# Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

**Server**

**Interworking**

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

Interworking Profiles: Avaya-SM

Add

RenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader Manipulation**Advanced**

|   |            |
|---|------------|
| Record Routes                           | Both Sides |
| Include End Point IP for Context Lookup | Yes        |
| Extensions                              | Avaya      |
| Diversion Manipulation                  | No         |
| Has Remote SBC                          | Yes        |
| Route Response on Via Port              | No         |
| Relay INVITE Replace for SIPREC         | No         |
| MOBX Re-INVITE Handling                 | No         |
| NATing for 301/302 Redirection          | Yes        |

DTMF

|              |      |
|--------------|------|
| DTMF Support | None |
|--------------|------|

Edit

## 7.2.2. Server Interworking Profile for eONE

eONE profile was cloned from the same **avaya-ru** profile. The **General** tab below shows the default settings, except that **SIPS Required** was disabled.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

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

Interworking Profiles: CI-eONE

Add

Interworking Profiles

cs2100

avaya-ru

Avaya-SM

PSTN-SIP

PCIPal

VoIPSP

**CI-eONE**

Rename

Clone

Delete

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation Advanced

General

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

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

26 of 53  
CI-eONE-SBCE10

Select the **Advanced** tab and configure as shown in the screen capture below.

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

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

**Server Interworking**

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

H248 Profile

IP/URI Blocklist Profile

▸ Services

Interworking Profiles: CI-eONE

Add

RenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader Manipulation**Advanced**

|   |            |
|---|------------|
| Record Routes                           | Both Sides |
| Include End Point IP for Context Lookup | Yes        |
| Extensions                              | Avaya      |
| Diversion Manipulation                  | No         |
| Has Remote SBC                          | Yes        |
| Route Response on Via Port              | No         |
| Relay INVITE Replace for SIPREC         | No         |
| MOBX Re-INVITE Handling                 | No         |
| NATing for 301/302 Redirection          | Yes        |

DTMF

|              |      |
|--------------|------|
| DTMF Support | None |
|--------------|------|

Edit

## 7.3. Administer SIP Servers

A SIP server definition is required for each server connected to SBCE. Add **SIP Servers** for Session Manager and eONE. TLS transport was used for the SIP trunks to Session Manager and eONE.

**Note:** TLS profiles were preconfigured for Session Manager and are not shown in these Application Notes. However, TLS profile configuration for eONE is shown in **Section 7.8**.

### 7.3.1. SIP Server for Session Manager

To define a SIP server, navigate to **Services** → **SIP Servers** from the left pane to display the existing SIP server profiles. Click **Add** to create a new SIP Server or select a pre-configured SIP server to view its settings. The **General** tab of the Session Manager SIP Server was configured as follows. TLS transport was used for the Session Manager SIP trunk.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▾ Services  
    **SIP Servers**  
        H248 Servers  
        LDAP  
        RADIUS  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
▸ DMZ Services  
▸ Monitoring & Logging

SIP Servers: Session Manager

Add

Rename Clone Delete

Server Profiles

PSTN-SIP  
[REDACTED]  
[REDACTED]  
OCP-SBCE-P...  
**Session Man...**  
VoIPSP  
CI eONE

General Authentication Heartbeat Registration Ping Advanced

Server Type Call Server

TLS Client Profile sbceInternal

DNS Query Type NONE/A

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 10.64.102.117     | 5061 | TLS       |

Edit

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

28 of 53  
CI-eONE-SBCE10

The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.1**. All other tabs were left with their default values.

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

Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
    **SIP Servers**  
        H248 Servers  
        LDAP  
        RADIUS  
▸ Domain Policies  
▸ TLS Management  
▸ Network & Flows  
▸ DMZ Services  
▸ Monitoring & Logging

SIP Servers: Session Manager

Add

Server Profiles

PSTN-SIP

OCP-SBCE-P...

**Session Man...**

VoIPSP

CI eONE

RenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPing**Advanced**

Enable DoS Protection☐

Enable Grooming☒

Interworking ProfileAvaya-SM

Signaling Manipulation ScriptNone

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

NG911 Support☐

Edit

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

29 of 53  
CI-eONE-SBCE10

### 7.3.2. SIP Server for eONE

The **General** tab of the eONE SIP server was configured as shown below. The *CI eONE* SIP server. TLS transport was used for the eONE SIP trunk. The configuration of the **TLS Client Profile** is shown in **Section 7.8**.

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

Session Border Controller for Enterprise

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▾ Services

SIP ServersH248 ServersLDAPRADIUS▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

SIP Servers: CI eONE

Add

Server Profiles

PSTN-SIP

OCP-SBCE-P...

Session Mana...

VoIPSP

CI eONE

RenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Server TypeTrunk Server

TLS Client ProfileCI-eONE-ClientCert

DNS Query TypeNONE/A

IP Address / FQDNPortTransport

5061

TLS

Edit

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

30 of 53  
CI-eONE-SBCE10

The **Heartbeat** tab was configured as shown below for eONE. This allows SBCE to send SIP OPTIONS to eONE.

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

Session Border Controller for Enterprise

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services

- SIP Servers
  - H248 Servers
  - LDAP
  - RADIUS
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

SIP Servers: CI eONE

Add

Server Profiles

PSTN-SIP

OCP-SBCE-P...

Session Mana...

VoIPSP

CI eONE

RenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable Heartbeat☒

MethodOPTIONS

Frequency120 seconds

From URI**sbce@**

To URI**eone@**

Edit

The **Advanced** tab was configured as shown below for eONE. **Interworking Profile** was set to *CI-eONE*, configured in **Section 7.2.2**. All other tabs were left with their default values.

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

Session Border Controller for Enterprise

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services

- SIP Servers
  - H248 Servers
  - LDAP
  - RADIUS
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

SIP Servers: CI eONE

Add

Server Profiles

PSTN-SIP

OCP-SBCE-P...

Session Mana...

VoIPSP

CI eONE

RenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable DoS Protection☐

Enable Grooming☒

Interworking ProfileCI-eONE

Signaling Manipulation ScriptNone

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

NG911 Support☐

Edit

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

31 of 53  
CI-eONE-SBCE10

## 7.4. Administer Routing Profiles

A routing profile is used to specify the next-hop for a SIP message. A routing profile is applied only after the traffic has matched an End Point Flow defined in **Section 7.11**.

### 7.4.1. Routing Profile for eONE

A routing profile was added for routing calls to eONE based on a URI group. The routing profile was named *CI-eONE or PSTN*. This routing profile contains two routing rules. The first routing rule with **Priority** of 1 is used to route calls to eONE if the number in the To header of the SIP INVITE matches the *CI eONE* URI Group configured in **Section 7.5**. The second routing rule with **Priority** of 2 routes the call to the PSTN.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▾ Configuration Profiles  
    Domain DoS  
    Server Interworking  
    Media Forking  
    **Routing**  
    Topology Hiding  
    Signaling Manipulation  
    URI Groups  
    SNMP Traps

Routing Profiles: CI-eONE or PSTN

Add

Rename Clone Delete

Click here to add a description.

Routing Profile

Update Priority Add

| Priority | URI Group | Time of Day | Load Balancing | Next Hop Address | Transport |             |
|----------|-----------|-------------|----------------|------------------|-----------|-------------|
| 1        | CI eONE   | default     | Priority       | [REDACTED]:5061  | TLS       | Edit Delete |
| 2        | *         | default     | Priority       | [REDACTED]:5062  | UDP       | Edit Delete |



The details of the first routing rule for routing calls to eONE is shown below.

Profile : CI-eONE or PSTN - Edit Rule

|                            |                                     |                       |                          |
|----------------------------|-------------------------------------|-----------------------|--------------------------|
| URI Group                  | CI eONE                             | Time of Day           | default                  |
| Load Balancing             | Priority                            | NAPTR                 | <input type="checkbox"/> |
| Transport                  | None                                | LDAP Routing          | <input type="checkbox"/> |
| LDAP Server Profile        | None                                | LDAP Base DN (Search) | None                     |
| Matched Attribute Priority | <input type="checkbox"/>            | Alternate Routing     | <input type="checkbox"/> |
| Next Hop Priority          | <input checked="" type="checkbox"/> | Next Hop In-Dialog    | <input type="checkbox"/> |
| Ignore Route Header        | <input type="checkbox"/>            |                       |                          |
| ENUM                       | <input type="checkbox"/>            | ENUM Suffix           |                          |

Add

| Priority / Weight | LDAP Search Attribute | LDAP Search Regex Pattern | LDAP Search Regex Result | SIP Server Profile | Next Hop Address | Transport |        |
|-------------------|-----------------------|---------------------------|--------------------------|--------------------|------------------|-----------|--------|
| 1                 |                       |                           |                          | CI eONE            | :506             | None      | Delete |

Finish

The details of the second routing rule for routing PSTN calls is shown below.

Profile : Session Manager - Edit Rule

|                            |                                     |                       |                          |
|----------------------------|-------------------------------------|-----------------------|--------------------------|
| URI Group                  | *                                   | Time of Day           | default                  |
| Load Balancing             | Priority                            | NAPTR                 | <input type="checkbox"/> |
| Transport                  | None                                | LDAP Routing          | <input type="checkbox"/> |
| LDAP Server Profile        | None                                | LDAP Base DN (Search) | None                     |
| Matched Attribute Priority | <input type="checkbox"/>            | Alternate Routing     | <input type="checkbox"/> |
| Next Hop Priority          | <input checked="" type="checkbox"/> | Next Hop In-Dialog    | <input type="checkbox"/> |
| Ignore Route Header        | <input type="checkbox"/>            |                       |                          |
| ENUM                       | <input type="checkbox"/>            | ENUM Suffix           |                          |

Add

| Priority / Weight | LDAP Search Attribute | LDAP Search Regex Pattern | LDAP Search Regex Result | SIP Server Profile | Next Hop Address | Transport |        |
|-------------------|-----------------------|---------------------------|--------------------------|--------------------|------------------|-----------|--------|
| 1                 |                       |                           |                          | Session            | 10.64.102.117:   | None      | Delete |

Finish

## 7.4.2. Routing Profile for Session Manager

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

The routing profile for calls to Session Manager is shown below. The routing profile was named *Session Manager*. This routing profile contains the IP address of the signaling interface of Session Manager.

Profile : Session Manager - Edit Rule

URI Group

\*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

Session

10.64.102.117

None

Delete

Finish

## 7.5. Administer URI Groups

**URI Groups** were used to aid in routing calls to eONE. For this solution, a **URI Group** named *CI eONE* was created as shown below. *CI eONE* URI group specified a URI with 78880 followed by any domain. This URI group was specified in the routing profile configured in **Section 7.4.1**. If the To header in the SIP INVITE matches 78880, the call would be routed to eONE. If it doesn't match the URI group, the call would be routed to the PSTN.

The *CI eONE* URI group is shown below.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. At the top, a navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand navigation menu lists various management options, with "URI Groups" highlighted in red. The main content area is titled "URI Groups: CI eONE" and features an "Add" button. Below this is a list of URI Groups, including "Emergency", "Session Man...", "PSTN-SIP", "CI eONE" (highlighted in red), "Internal-Exten...", and "OCP-PSTN". The "CI eONE" group is expanded, showing a "URI Listing" table with one entry: "78880@.\*". The table has "Edit" and "Delete" buttons for each entry. A blue bar at the top of the expanded group says "Click here to add a description."

## 7.6. Administer Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.7**.

To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. For the compliance test, the following media rule was used, *RTP-SRTP*. The **Encryption** tab was configured as shown below.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

Application Rules

Border Rules

**Media Rules**

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Media Rules: RTP-SRTP

Add

Rename Clone Delete

Media Rules

default-low-med

default-low-m...

default-high

default-high-enc

avaya-low-me...

**RTP-SRTP**

RTP-SRTP-P...

Click here to add a description.

Encryption

Codec Prioritization

Advanced

QoS

Audio Encryption

Preferred FormatsSRTP\_AES\_CM\_128\_HMAC\_SHA1\_80  
RTP

Encrypted RTCP☒

MKI☐

LifetimeAny

Interworking☒

Symmetric Context Reset☒

Key Change in New Offer☐

Video Encryption

Preferred FormatsRTP

Interworking☒

Symmetric Context Reset☒

Key Change in New Offer☐

Miscellaneous

Capability Negotiation☐

Edit

## 7.7. Administer End Point Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the SBCE and an endpoint (connected server). The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.11**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by the **Policy Group** window (not shown) to configure the group parameters. Once complete, the settings will be displayed. To view the settings of an existing group, select the group from the list. The settings will appear in the right pane.

The new endpoint policy group, named *RTP-SRTP*, is shown below and is assigned the *RTP-SRTP* media rule configured above. This endpoint policy group is used for Session Manager, PSTN, and eONE.

The screenshot displays the Avaya Session Border Controller (SBCE) configuration interface. The top navigation bar includes tabs for Device, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The left sidebar shows a tree view of configuration options, with 'Domain Policies' expanded and 'End Point Policy Groups' selected. The main area shows the 'Edit Policy Set' dialog box, which is a pop-up window for configuring policy rules. The dialog box contains the following fields:

- Application Rule: default
- Border Rule: default
- Media Rule: RTP-SRTP
- Security Rule: default-low
- Signaling Rule: default
- Charging Rule: None
- RTCP Monitoring Report Generation: Off

Below the dialog box, a table lists the configured policy groups. The table has columns for Order, Application, Border, Media, Security, Signaling, Charging, and RTCP Mon Gen. The first row shows the 'RTP-SRTP' group with the following values:

| Order | Application | Border  | Media    | Security    | Signaling | Charging | RTCP Mon Gen |
|-------|-------------|---------|----------|-------------|-----------|----------|--------------|
| 1     | default     | default | RTP-SRTP | default-low | default   | None     | Off          |

## 7.8. Administer TLS Management

This section covers installing the eONE certificate, configuring the eONE client profile, and configuring the server profile for the B2 public interface, which connects to the eONE, to set up secure communications using TLS. The TLS configuration for Session Manager is assumed to already be in place and is not shown in these Application Notes.

Navigate to **TLS Management** → **Certificates** and install the eONE certificate. For the compliance test, the certificate was named *CI\_eONE\_Cert.crt* as shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar contains a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates (selected), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Certificates' and features 'Install' and 'Generate CSR' buttons. It displays two sections: 'Installed Certificates' and 'Installed CA Certificates'. The 'Installed Certificates' section lists 'sbceExternalB2.pem', 'sbceInternal.pem', and 'sbceExternalB1.pem'. The 'Installed CA Certificates' section lists 'AvayaDeviceEnrollmentCAchain.crt', 'avayaItrootca2.pem', 'entrust\_g2\_ca.cer', 'SystemManagerCA.pem', 'ocpSystemManagerCA.pem', a redacted entry, 'OCP\_Lab7CACert.cer', another redacted entry, and 'DigitCertGlobalRootCA.pem'. The certificate 'CI\_eONE\_Cert.crt' is listed at the bottom of the 'Installed CA Certificates' section and is highlighted with a red box.

| Installed Certificates |   |
|------------------------|---|
| sbceExternalB2.pem     | <a href="#">View</a> <a href="#">Delete</a> |
| sbceInternal.pem       | <a href="#">View</a> <a href="#">Delete</a> |
| sbceExternalB1.pem     | <a href="#">View</a> <a href="#">Delete</a> |

| Installed CA Certificates        |   |
|----------------------------------|---|
| AvayaDeviceEnrollmentCAchain.crt | <a href="#">View</a> <a href="#">Delete</a> |
| avayaItrootca2.pem               | <a href="#">View</a> <a href="#">Delete</a> |
| entrust_g2_ca.cer                | <a href="#">View</a> <a href="#">Delete</a> |
| SystemManagerCA.pem              | <a href="#">View</a> <a href="#">Delete</a> |
| ocpSystemManagerCA.pem           | <a href="#">View</a> <a href="#">Delete</a> |
| [Redacted]                       | <a href="#">View</a> <a href="#">Delete</a> |
| OCP_Lab7CACert.cer               | <a href="#">View</a> <a href="#">Delete</a> |
| [Redacted]                       | <a href="#">View</a> <a href="#">Delete</a> |
| [Redacted]                       | <a href="#">View</a> <a href="#">Delete</a> |
| DigitCertGlobalRootCA.pem        | <a href="#">View</a> <a href="#">Delete</a> |
| CI_eONE_Cert.crt                 | <a href="#">View</a> <a href="#">Delete</a> |

Next, create a **Client Profile** for eONE as shown below. The **Profile Name** was *CI-eONE-ClientCert* and the certificate for B2 public interface was selected. **Peer Verification** was set to *Required* and the *CI\_eON\_Cert.crt* certificate was selected for **Peer Certificate Authorities**. The **Verification Depth** was set to 2 and the **Version** was set to *TLS 1.2*. This client profile was assigned to the eONE SIP server in **Section 7.3.2**.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
▸ TLS Management  
    Certificates  
    **Client Profiles**  
    Server Profiles  
    SNI Group  
▸ Network & Flows  
▸ DMZ Services  
▸ Monitoring & Logging

Client Profiles: CI-eONE-ClientCert

Add

Delete

Client Profiles

sbceInternal

sbceExternalB2

sbceExternalB1

CI-eONE-Clie...

Click here to add a description.

Client Profile

TLS Profile

|              |                                  |
|--------------|----------------------------------|
| Profile Name | CI-eONE-ClientCert               |
| Certificate  | sbceExternalB2.pem               |
| SNI          | <input type="checkbox"/> Enabled |

Certificate Verification

|                                   |                          |
|-----------------------------------|--------------------------|
| Peer Verification                 | Required                 |
| Peer Certificate Authorities      | CI_eONE_Cert.crt         |
| Peer Certificate Revocation Lists | ---                      |
| Verification Depth                | 2                        |
| Extended Hostname Verification    | <input type="checkbox"/> |

Renegotiation Parameters

|                          |   |
|--------------------------|---|
| Renegotiation Time       | 0 |
| Renegotiation Byte Count | 0 |

Handshake Options

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

Edit

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

39 of 53  
CI-eONE-SBCE10

The following server profile is assigned to the B2 public interface covered in **Section 7.10**.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

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

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Server Profiles: sbceExternalB2

AddDelete

Server Profiles

sbceExternalB1

**sbceExternal...**

sbceInternal

Click here to add a description.

Server Profile

TLS Profile

|              |                    |
|--------------|--------------------|
| Profile Name | sbceExternalB2     |
| Certificate  | sbceExternalB2.pem |
| SNI Options  | None               |

Certificate Verification

|                                |                          |
|--------------------------------|--------------------------|
| Peer Verification              | None                     |
| Extended Hostname Verification | <input type="checkbox"/> |

Renegotiation Parameters

|                          |   |
|--------------------------|---|
| Renegotiation Time       | 0 |
| Renegotiation Byte Count | 0 |

Handshake Options

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

Edit



## 7.9. Administer Media Interfaces


A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the SBCE. Media Interfaces need to be defined for each SIP server to send and receive media (RTP or SRTP).

Navigate to **Networks & Flows → Media Interface** to define a new Media Interface. During the compliance test, the following interfaces were defined. For security reasons, public IP addresses have been masked. The media interfaces used for this solution are listed below.

- **PrivateMedia:** Interface used by Session Manager to send and receive media.
- **PublicMediaB2:** Interface used by eONE to send and receive media.

**Device: SBCE** ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

# Session Border Controller for Enterprise



EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

- Network Management
- Media Interface**
- Signaling Interface
- End Point Flows
- Session Flows
- Advanced Options

▸ DMZ Services

▸ Monitoring & Logging

## Media Interface

**Media Interface** Add

| Name           | Media IP Network                         | Port Range    |             |
|----------------|--|---------------|-------------|
| PrivateMedia   | 10.64.102.106<br>Private-A1 (A1, VLAN 0) | 35000 - 40000 | Edit Delete |
| PublicMedia    | 10.64.101.101<br>Public-B1 (B1, VLAN 0)  | 35000 - 40000 | Edit Delete |
| PublicMediaB2  | ██████████<br>Public-B2 (B2, VLAN 0)     | 35000 - 40000 | Edit Delete |
| PrivateMediaRW | 10.64.102.108<br>Private-A1 (A1, VLAN 0) | 35000 - 40000 | Edit Delete |
| PublicMediaRW  | 10.64.101.102<br>Public-B1 (B1, VLAN 0)  | 35000 - 40000 | Edit Delete |

## 7.10. Administer Signaling Interfaces

A signaling interface defines an IP address, protocols and listen ports that the SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the SBCE. Signaling Interface needs to be defined for each SIP server to send and receive SIP signaling messages.

Navigate to **Networks & Flows → Signaling Interface** to define a new **Signaling Interface**. During the Compliance Testing the following interfaces were defined. For security reasons, public IP addresses have been masked. The signaling interfaces used for this solution are listed below.

- **PrivateSignaling:** Interface used by Session Manager to send and receive calls.
- **PublicSignalingB2:** Interface used by eONE to send and receive calls.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

Network Management

Media Interface

**Signaling Interface**

End Point Flows

Session Flows

Advanced Options

▸ DMZ Services

▸ Monitoring & Logging

Signaling Interface

Signaling Interface

Add

| Name               | Signaling IP Network                     | TCP Port | UDP Port | TLS Port | TLS Profile    |             |
|--------------------|--|----------|----------|----------|----------------|-------------|
| PublicSignaling    | 10.64.101.101<br>Public-B1 (B1, VLAN 0)  | 5060     | 5060     | ---      | None           | Edit Delete |
| PrivateSignaling   | 10.64.102.106<br>Private-A1 (A1, VLAN 0) | 5060     | 5060     | 5061     | sbceInternal   | Edit Delete |
| PrivateSignalingRW | 10.64.102.108<br>Private-A1 (A1, VLAN 0) | 5060     | 5060     | 5061     | sbceInternal   | Edit Delete |
| PublicSignalingRW  | 10.64.101.102<br>Public-B1 (B1, VLAN 0)  | ---      | ---      | 5061     | sbceExternalB1 | Edit Delete |
| ServiceProvider    | Public-B2 (B2, VLAN 0)                   | 5060     | 5060     | ---      | None           | Edit Delete |
| PublicSignalingB2  | Public-B2 (B2, VLAN 0)                   | ---      | 5062     | 5061     | sbceExternalB2 | Edit Delete |

## 7.11. Administer End Point Flows

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

Navigate to **Network & Flows → End Point Flows → Server Flows** and select the **Server Flows** tab. The configured **Server Flows** used in the compliance test are shown below. The following subsections will review the settings for each server flow.

The **Server Flows** for eONE and the PSTN are shown below. The details of the PSTN server flow will not be shown in these Application Notes.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

Network Management

Media Interface

Signaling Interface

**End Point Flows**

Session Flows

Advanced Options

▸ DMZ Services

▸ Monitoring & Logging

End Point Flows

Subscriber Flows

Server Flows

Add

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: CI eONE

| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |  |
|----------|-----------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| 1        | CI eONE   | *         | PrivateSignaling   | PublicSignalingB2   | RTP-SRTP               | Session Manager | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |

SIP Server: OCP-SBCE-PUBLIC

| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |  |
|----------|-----------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| 1        | OCP-PSTN  | *         | PrivateSignaling   | PublicSignalingB2   | RTP-SRTP               | Session Manager | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |

JAO; Reviewed:  
SPOC 3/23/2023

Solution & Interoperability Test Lab Application Notes  
©2023 Avaya Inc. All Rights Reserved.

43 of 53  
CI-eONE-SBCE10

The **Server Flows** for Session Manager are shown below.

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

Session Border Controller for EnterpriseAVAYA

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

Network ManagementMedia InterfaceSignaling InterfaceEnd Point Flows

End Point Flows

Subscriber FlowsServer Flows

SIP Server: Session ManagerUpdate

| Priority | Flow Name            | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |  |
|----------|----------------------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| 1        | eONE or PSTN         | *         | PublicSignalingB2  | PrivateSignaling    | RTP-SRTP               | CI-eONE or PSTN | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |
| 2        | Session Manager Flow | *         | PublicSignaling    | PrivateSignaling    | RTP-SRTP               | PSTN-SIP        | <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a> |

### 7.11.1. Server Flows for eONE

The eONE server flow is shown below. This is the source flow for incoming calls from eONE and the destination flow for outgoing calls to eONE.

**Edit Flow: CI eONE** X

|                               |  |
|-------------------------------|--|
| Flow Name                     | <input type="text" value="CI eONE"/>             |
| SIP Server Profile            | <input type="text" value="CI eONE"/> ▼           |
| URI Group                     | <input type="text" value="*"/> ▼                 |
| Transport                     | <input type="text" value="*"/> ▼                 |
| Remote Subnet                 | <input type="text" value="*"/>                   |
| Received Interface            | <input type="text" value="PrivateSignaling"/> ▼  |
| Signaling Interface           | <input type="text" value="PublicSignalingB2"/> ▼ |
| Media Interface               | <input type="text" value="PublicMediaB2"/> ▼     |
| Secondary Media Interface     | <input type="text" value="None"/> ▼              |
| End Point Policy Group        | <input type="text" value="RTP-SRTP"/> ▼          |
| Routing Profile               | <input type="text" value="Session Manager"/> ▼   |
| Topology Hiding Profile       | <input type="text" value="default"/> ▼           |
| Signaling Manipulation Script | <input type="text" value="None"/> ▼              |
| Remote Branch Office          | <input type="text" value="Any"/> ▼               |
| Link Monitoring from Peer     | <input type="checkbox"/>                         |
| FQDN Support                  | <input type="checkbox"/>                         |
| FQDN                          | <input type="text"/>                             |

**Finish**

### 7.11.2. Server Flow for Session Manager

This section covers the server flows for Session Manager. The following is the source flow for calls from Session Manager to eONE or the PSTN. This server flow is not used as the destination flow. The Routing Profile, *eONE or PSTN*, is used to route calls to eONE or the PSTN according to URI groups.

**Edit Flow: eONE or PSTN** X

|                               |  |
|-------------------------------|--|
| Flow Name                     | <input type="text" value="eONE or PSTN"/>      |
| SIP Server Profile            | <input type="text" value="Session Manager"/>   |
| URI Group                     | <input type="text" value="*/"/>                |
| Transport                     | <input type="text" value="*/"/>                |
| Remote Subnet                 | <input type="text" value="*/"/>                |
| Received Interface            | <input type="text" value="PublicSignalingB2"/> |
| Signaling Interface           | <input type="text" value="PrivateSignaling"/>  |
| Media Interface               | <input type="text" value="PrivateMedia"/>      |
| Secondary Media Interface     | <input type="text" value="None"/>              |
| End Point Policy Group        | <input type="text" value="RTP-SRTP"/>          |
| Routing Profile               | <input type="text" value="CI-eONE or PSTN"/>   |
| Topology Hiding Profile       | <input type="text" value="Session Manager"/>   |
| Signaling Manipulation Script | <input type="text" value="None"/>              |
| Remote Branch Office          | <input type="text" value="Any"/>               |
| Link Monitoring from Peer     | <input type="checkbox"/>                       |
| FQDN Support                  | <input type="checkbox"/>                       |
| FQDN                          | <input type="text"/>                           |

Finish

The following is the destination flow for calls from eONE or PSTN to Session Manager. This server flow is not used as the source flow.

**Edit Flow: Session Manager Flow** **X**

|                               |   |
|-------------------------------|---|
| Flow Name                     | <input type="text" value="Session Manager Flow"/> |
| SIP Server Profile            | <input type="text" value="Session Manager"/> ▼    |
| URI Group                     | <input type="text" value="*"/> ▼                  |
| Transport                     | <input type="text" value="*"/> ▼                  |
| Remote Subnet                 | <input type="text" value="*"/>                    |
| Received Interface            | <input type="text" value="PublicSignaling"/> ▼    |
| Signaling Interface           | <input type="text" value="PrivateSignaling"/> ▼   |
| Media Interface               | <input type="text" value="PrivateMedia"/> ▼       |
| Secondary Media Interface     | <input type="text" value="None"/> ▼               |
| End Point Policy Group        | <input type="text" value="RTP-SRTP"/> ▼           |
| Routing Profile               | <input type="text" value="PSTN-SIP"/> ▼           |
| Topology Hiding Profile       | <input type="text" value="Session Manager"/> ▼    |
| Signaling Manipulation Script | <input type="text" value="None"/> ▼               |
| Remote Branch Office          | <input type="text" value="Any"/> ▼                |
| Link Monitoring from Peer     | <input type="checkbox"/>                          |
| FQDN Support                  | <input type="checkbox"/>                          |
| FQDN                          | <input type="text"/>                              |

**Finish**

## 8. Configure Computer Instruments eONE

The configuration of eONE is performed by Computer Instruments technical personnel. For provisioning, Computer Instruments would require the SBCE public IP address and the TLS certificate.



## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, SBCE, and eONE.

1. From the System Manager home page (not shown), select **Elements → Session Manager** from the top menu to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager → System Status → SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the Communication Manager entity name from **Section 6.1.1**.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are “UP”, as shown below.

The screenshot shows the Avaya System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Session Manager' section with 'SIP Entity Monit...' selected. The main content area displays the 'SIP Entity, Entity Link Connection Status' screen. This screen includes a 'Summary View' button and a table showing the connection status for the 'devcon-sm' entity. The table has columns for Session Manager Name, Session Manager IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The 'devcon-sm' entry shows 'UP' for both 'Conn. Status' and 'Link Status'.

| Session Manager Name | Session Manager IP Address Family | SIP Entity Resolved IP | Port | Proto. | Deny  | Conn. Status | Reason Code | Link Status |
|----------------------|-----------------------------------|------------------------|------|--------|-------|--------------|-------------|-------------|
| devcon-sm            | IPv4                              | 10.64.102.115          | 5062 | TLS    | FALSE | UP           | 200 OK      | UP          |

2. Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the SBCE entity name from **Section 6.1.2**.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are “UP”, as shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, version information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon are also present. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Application Confi..., System Status, Load Factor, and SIP Entity Monit... The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a description: "This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity." Below this, there is a section for "Status Details for the selected Session Manager:" and a table titled "All Entity Links to SIP Entity: devcon-sbce". The table has a "Summary View" button and a "Filter: Enable" link. The table contains one item, "devcon-sm", with columns for Session Manager Name, Session Manager IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The Conn. Status and Link Status are both "UP".

|                       | Session Manager Name      | Session Manager IP Address Family | SIP Entity Resolved IP | Port | Proto. | Deny  | Conn. Status | Reason Code | Link Status |
|-----------------------|---------------------------|-----------------------------------|------------------------|------|--------|-------|--------------|-------------|-------------|
| <input type="radio"/> | <a href="#">devcon-sm</a> | IPv4                              | 10.64.102.106          | 5061 | TLS    | FALSE | UP           | 200 OK      | UP          |

Select : None

3. To verify the SIP trunk between SBCE and eONE is in service, navigate to **Status → Server Status**. The **Hearbeat Status** for the eONE SIP trunk should be *UP* as shown below.

Device: SBCE ▾ Help

Status

AVAYA

Server Status

|                 |  |  |      |     |    |         |                         |
|-----------------|--|--|------|-----|----|---------|-------------------------|
| OCP-SBCE-PUBLIC |  |  | 5062 | UDP | UP | UNKNOWN | 02/06/2023 13:08:35 EST |
| CI eONE         |  |  | 5061 | TLS | UP | UNKNOWN | 02/21/2023 11:24:13 EST |

4. Place a call to eONE and verify the application answers and the appropriate greeting is heard.
5. Caller navigates through the application using DTMF. Verify eONE provides the appropriate response.
6. Request eONE to transfer the call to a local number or PSTN. Verify the transferred call is established with two-way audio.
7. Caller terminates the call successfully.
8. An eONE outbound call campaign may also be verified.

## 10. Conclusion

These Application Notes have described the configuration steps required to integrate Computer Instruments eONE with Avaya Session Border Controller for Enterprise. Callers were able to navigate the Computer Instruments eONE sample IVR application using DTMF, establish two-way audio, and transfer calls. In addition, Computer Instruments eONE was able to initiate an outbound call campaign. All test cases passed with observations noted in **Section 2.2**.

## 11. Additional References

This section references the product documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, December 2021, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022, available at <http://support.avaya.com>.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1.x, Issue 1, December 2021, available at <http://support.avaya.com>.

---

**©2023 Avaya Inc. All Rights Reserved.**

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

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