Abstract

These Application Notes describe the steps used to configure SIP-based Media Recording (SIPREC) between MiaRec and an Avaya SIP enabled Enterprise Solution. The Avaya platform consisted of Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1.

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 steps used to configure SIP-based Media Recording (SIPREC) between MiaRec and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of the following:

- Avaya Aura® Communication Manager R7.0.1 (Communication Manager)
- Avaya Aura® Session Manager R7.0.1 (Session Manager)
- Avaya Session Border Controller for Enterprise R7.1 (Avaya SBCE)

Note that the shortened names shown in brackets will be used throughout the remainder of the document.

MiaRec is a call recording and quality management solution. Using the SIPREC interface of Avaya SBCE, MiaRec provides centralized call recording solutions for the enterprises that use SIP Trunking services and Remote Workers.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to connect to the Service Provider’s SIP Trunking service via SIP interface. MiaRec was recording calls to/from the enterprise site using the SIPREC interface on the Avaya SBCE.

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

2.1. Interoperability Compliance Testing

The interoperability test included the call recording scenarios for the following:

- Recording of incoming calls to the enterprise site from Service Provider’s SIP Trunk, calls made to SIP and H.323 telephones at the enterprise.
- Recording of outgoing calls from the enterprise site to remote destinations through the Service Provider’s SIP Trunking service, calls made from SIP and H.323 telephones.
- Recording of incoming and outgoing calls to/from SIP Remote Worker.
- Recording of calls using the G.711A and G.729A codecs.
- Recording of call scenarios involving the user features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID and DNIS presentation of recorded calls.
- Recording of call scenarios involving the call coverage and call forwarding for endpoints at the enterprise site.
• Transmission and response of SIP OPTIONS messages sent to MiaRec.
• Call recordings using combination of TCP/RTP and TLS/SRTP.

2.2. Test Results
Interoperability testing of the sample configuration was completed with successful results for the MiaRec solution with the following observations:
• Certain conference calls and transfer calls initiated from Remote Worker, result in duplicate recording on MiaRec. This is due to Avaya SBCE sending separate streams to MiaRec for each call leg. Avaya SBCE team is aware of this and is working towards resolution.

2.3. Support
For technical support on MiaRec products please contact MiaRec.
Email: support@miarec.com
Phone: 866-324-6717
Web: www.miarec.com
3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Simulated SIP Trunking service through the Avaya SBCE. Located at the Enterprise site is an Avaya SBCE, Session Manager, Communication Manager and MiaRec. Endpoints are Avaya 96x0 series and Avaya 96x1 Series IP Deskphones (with SIP and H.323 firmware and Avaya one-X® Communicator soft phone and Avaya Communicator for Windows running on laptop PCs. The Remote Workers are connecting to the Enterprise site through Avaya SBCE.
## 4. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Session Manager running on a virtual platform</td>
<td>7.0.1.2</td>
</tr>
<tr>
<td>Avaya Aura® System Manager running on a virtual platform</td>
<td>7.0.1.2</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager running on a virtual platform</td>
<td>7.0.1.2.0.441.23523</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise running on a virtual platform</td>
<td>7.1.0.1-07-12368</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>37.19.0</td>
</tr>
<tr>
<td>Avaya Aura® Media Server running on a virtual platform</td>
<td>7.7.0.236_2015.07.24</td>
</tr>
<tr>
<td>Avaya 96x0 Deskphone (H.323)</td>
<td>2_6_14_5</td>
</tr>
<tr>
<td>Avaya 96x1 Deskphone (SIP)</td>
<td>7.0.0 R39</td>
</tr>
<tr>
<td>Avaya 96x1 Deskphone (H.323)</td>
<td>3.230A</td>
</tr>
<tr>
<td>Avaya 6408D+ Digital Telephone</td>
<td>-</td>
</tr>
<tr>
<td>Avaya 6211 Analogue Telephone</td>
<td>-</td>
</tr>
<tr>
<td>Avaya one-X® Communicator running on Windows 10 PC</td>
<td>6.2.7.03-SP7</td>
</tr>
<tr>
<td>Avaya Communicator for Windows running on Windows 10 PC</td>
<td>2.1.2.75</td>
</tr>
<tr>
<td>MiaRec running on a virtual platform</td>
<td>Recorder: 5.2.1.155 Web UI: 5.2.0.2037</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager. All configuration in this section is performed via a SAT terminal. Though Communication Manager and Session Manager do not directly integrate with MiaRec in the current setup, configuration is provided for reference.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorised Avaya sales representative to add additional capacity. Use the display system-parameters customer-options command and on Page 2, verify that the Maximum Administered SIP Trunks supported by the system is sufficient for the combination of trunks to the Service Provider’s SIP Trunking service and any other SIP trunks used.

<table>
<thead>
<tr>
<th>IP PORT CAPACITIES</th>
<th>USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Administered H.323 Trunks: 12000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations: 18000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks: 12000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations: 18000 0</td>
<td></td>
</tr>
<tr>
<td>Max Concur Registered Unauthenticated H.323 Stations: 100 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Video Capable Stations: 36000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones: 18000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Administered SIP Trunks: 12000 10</td>
<td></td>
</tr>
<tr>
<td>Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0</td>
<td></td>
</tr>
<tr>
<td>Maximum Number of DS1 Boards with Echo Cancellation: 522 0</td>
<td></td>
</tr>
</tbody>
</table>
On Page 5, verify that IP Trunks field is set to y.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTIONAL FEATURES</td>
</tr>
<tr>
<td>Emergency Access to Attendant? y</td>
</tr>
<tr>
<td>Enable 'dadmin' Login? y</td>
</tr>
<tr>
<td>Enhanced Conferencing? y</td>
</tr>
<tr>
<td>Enhanced EC500? y</td>
</tr>
<tr>
<td>Enterprise Survivable Server? n</td>
</tr>
<tr>
<td>Enterprise Wide Licensing? n</td>
</tr>
<tr>
<td>ESS Administration? y</td>
</tr>
<tr>
<td>Extended Cfg/Fwd Admin? y</td>
</tr>
<tr>
<td>External Device Alerts Admin? y</td>
</tr>
<tr>
<td>Five Port Networks Max Per MCC? n</td>
</tr>
<tr>
<td>Flexible Billing? n</td>
</tr>
<tr>
<td>Forced Entry of Account Codes? y</td>
</tr>
<tr>
<td>Global Call Classification? y</td>
</tr>
<tr>
<td>Hospitality (Basic)? y</td>
</tr>
<tr>
<td>Hospitality (G3V3 Enhancements)? y</td>
</tr>
<tr>
<td><strong>IP Trunks? y</strong></td>
</tr>
<tr>
<td>IP Stations? y</td>
</tr>
<tr>
<td>ISDN Feature Plus? n</td>
</tr>
<tr>
<td>ISDN/SIP Network Call Redirection? y</td>
</tr>
<tr>
<td>ISDN-BRI Trunks? y</td>
</tr>
<tr>
<td>ISDN-PRI? y</td>
</tr>
<tr>
<td>Local Survivable Processor? n</td>
</tr>
<tr>
<td>Malicious Call Trace? y</td>
</tr>
<tr>
<td>Media Encryption Over IP? n</td>
</tr>
<tr>
<td>Mode Code for Centralized Voice Mail? n</td>
</tr>
<tr>
<td>Optional Features</td>
</tr>
</tbody>
</table>

### 5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node Name and **IP Address** for Session Manager. In this case, **asm** and **10.64.110.13** are the Name and **IP Address** for the Session Manager SIP interface. Also note the **procr** IP address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

<table>
<thead>
<tr>
<th>display node-names ip</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP NODE NAMES</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>ams</td>
</tr>
<tr>
<td>asm</td>
</tr>
<tr>
<td>default</td>
</tr>
<tr>
<td>procr</td>
</tr>
<tr>
<td>procr6</td>
</tr>
</tbody>
</table>
5.3. Administer IP Network Region

Use the `change ip-network-region n` command where `n` is the chosen value of the configuration for the SIP Trunk. Set the following values:

- **The Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is `avaya.com`.
- By default, **IP-IP Direct Audio** (both Intra- and Inter-Region) is enabled (yes) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a SIP Trunk call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set 1 is used.
- The rest of the fields can be left at default values.

```
change ip-network-region 1
Region: 1
Location: Trunk
Authoritative Domain: avaya.com
Stub Network Region: n
Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
Codec Set: 1
Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048
UDP Port Max: 3329
IP Audio Hairpinning? n
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
Audio Resource Reservation Parameters
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```
5.4. Administer IP Codec Set

Open the IP Codec Set form for the codec set specified in the IP Network Region form in Section 5.3 by typing `change ip-codec set n` where `n` is the chosen value of the configuration for the SIP Trunk. Enter the list of audio codecs eligible to be used in order of preference. For the interoperability test the codecs supported by MiaRec were configured, namely G.711A and G.729A (other supported codecs by MiaRec are G.722, G.726-32k and GSM). Also, configure the Media Encryption as shown below.

```
change ip-codec-set 1

IP CODEC SET

Codec Set: 1

Audio Codec      Silence Suppression Frames Per Pkt Packet Size(ms)

1: G.711MU       n         2        20
2: G.729         n         2        20
3:
4:
5:
6:
7:

Media Encryption

1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: none
4:
5:

Encrypted SRTCP: enforce-unenc-srtp
```
5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound calls to the Service Provider’s SIP Trunking service. Configure the Signaling Group using the add signaling-group n command as follows:

- Set Group Type to sip.
- Set Transport Method to tls.
- Set Peer Detection Enabled to y allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set Near-end Node Name to the processor interface (node name procr as defined in the IP Node Names form shown in Section 5.2).
- Set Far-end Node Name to the Session Manager (node name Session_Manager as defined in the IP Node Names form shown in Section 5.2).
- Set Near-end Listen Port and Far-end Listen Port as required. The standard value for TCP is 5060, though 5061 was used in test to separate the SIP Trunk from the SIP endpoints on the Session Manager (See Section 6.5).
- Set Far-end Network Region to the IP Network Region configured in Section 5.3 (logically establishes the far-end for calls using this signalling group as network region 2).
- Set Far-end Domain to avaya.com.
- Set Direct IP-IP Audio Connections to y.
- Leave DTMF over IP at default value of rtp-payload (Enables RFC2833 for DTMF transmission from Communication Manager).

**Note:** The default values for the other fields may be used.
5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in Section 5.5. Configure the trunk group using the add trunk-group n command, where n is an available trunk group for the SIP Trunk. On Page 1 of this form:

- Set the Group Type field to sip.
- Choose a descriptive Group Name.
- Specify a trunk access code (TAC) consistent with the dial plan.
- The Direction is set to two-way to allow incoming and outgoing calls.
- Set the Service Type field to tie.
- Specify the signalling group associated with this trunk group in the Signaling Group field as previously configured in Section 5.5.
- Specify the Number of Members supported by this SIP trunk group.

```
add trunk-group 1

TRUNK GROUP

Group Number: 1
Group Type: sip
Group Name: asm
Direction: two-way
Dial Access? n
Queue Length: 0
Service Type: tie
CDR Reports: y
COR: 1        TN: 1        TAC: 101
Outgoing Display? y
Night Service:
Member Assignment Method: auto
Signaling Group: 1
Number of Members: 10

Page 1 of 22
```

On Page 2 of the trunk-group form, the Preferred Minimum Session Refresh Interval (sec) field should be set to a value mutually agreed with MiaRec to prevent unnecessary SIP messages during call setup. During testing, a value of 900 was used that sets Min-SE to 1800 in the SIP signalling.

```
add trunk-group 1

TRUNK PARAMETERS

Unicode Name: auto

Redirect On OPTIM Failure: 5000
SCCAN? n
Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 900

Disconnect Supervision - In? y  Out? y

Page 2 of 22
```
On Page 3, set the Numbering Format field to **private**. This allows delivery of CLI in formats other than E.164 with leading “+”.

```
add trunk-group 1
TRUNK FEATURES
   ACA Assignment? n          Measured: none
   Maintenance Tests? y

   Numbering Format: private
   UUI Treatment: service-provider
   Replace Restricted Numbers? n
   Replace Unavailable Numbers? n
```

### 5.7. Administer Calling Party Number Information

Use the `change private-unknown-numbering` command to configure Communication Manager to send the calling party number in the format required. In test, calling party numbers were sent as Communication Manager extension numbers to be modified in Session Manager. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

```
change private-numbering 0
NUMBERING - PRIVATE FORMAT
Ext Ext Trk Trk
Len Code Grp(s) Private Total
  5  1     1      1      1
Total Administered: 2
Maximum Entries: 540
```

### 5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the Avaya SBCE to the Service Provider’s SIP Trunking service. The single digit 9 was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the `change feature-access-codes` command to configure a digit as the Auto Route Selection (ARS) - Access Code 1.

```
change feature-access-codes
FEATURE ACCESS CODE (FAC)
   Abbreviated Dialing List1 Access Code:
   Abbreviated Dialing List2 Access Code:
   Abbreviated Dialing List3 Access Code:
   Abbreviated Dial - Prgm Group List Access Code:
   Announcement Access Code:
   Answer Back Access Code: #25
   Attendant Access Code:
   Auto Alternate Routing (AAR) Access Code: 8
   Auto Route Selection (ARS) - Access Code 1: 9
```

---

KJA: Reviewed:                          Solution & Interoperability Test Lab Application Notes
SPOC 5/12/2017:                          ©2017 Avaya Inc. All Rights Reserved.
MiaRec_SBCE70:                          12 of 50
Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 1. A sample of dial pattern is shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 1. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node ANI</th>
<th>Reqd</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>11</td>
<td>1</td>
<td>natl</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

Use the **change route-pattern** command, where **n** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern 1 is used to route calls to trunk group 1. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn’t have the same significance in SIP calls and during testing it was set to **lev0-pvt** to ensure that calling party number was not prefixed with a leading “+”.

<table>
<thead>
<tr>
<th>Pattern Number: 1</th>
<th>Pattern Name: SIP_Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCAN? n</td>
<td>Secure SIP? n</td>
</tr>
<tr>
<td>Grp</td>
<td>FRL</td>
</tr>
<tr>
<td>No</td>
<td>Mrk</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCC VALUE</th>
<th>TSC</th>
<th>CA-TSC</th>
<th>ITC</th>
<th>BCIE Service/Feature</th>
<th>PARM</th>
<th>Sub</th>
<th>Numbering</th>
<th>LAR</th>
<th>Dgts Format</th>
<th>Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>rest</td>
<td>lev0-pvt</td>
</tr>
<tr>
<td>2</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>rest</td>
<td>none</td>
</tr>
<tr>
<td>3</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>rest</td>
<td>none</td>
</tr>
<tr>
<td>4</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>rest</td>
<td>none</td>
</tr>
<tr>
<td>5</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>rest</td>
<td>none</td>
</tr>
<tr>
<td>6</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>rest</td>
<td>none</td>
</tr>
</tbody>
</table>

Save the Communication Manager configuration by entering **save translation**.
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured by opening a web browser to System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP Domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser and entering http://<FQDN>/SMGR, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.
6.2. Administer SIP Domain
To add the SIP domain that will be used with Session Manager, select Routing from the Home tab menu and in the resulting tab select Domains from left hand menu. Click the New button to create a new SIP domain entry. In the Name field enter the domain; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on Communication Manager. Refer to Section 5.3 for details. In test, avaya.com was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click Commit to save changes.

Note: If the existing domain name used in the enterprise equipment does not match that used in the network, Topology Hiding in the Avaya SBCE can be used to change it (see Section 7.8).
6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the Routing tab select Locations from the left hand menu (not shown). Under General, in the Name field, enter an informative name for the location. Scroll to the bottom of the page and under Location Pattern, click Add, then enter an IP Address Pattern in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.

![Location Details](image)
6.4. Administer Adaptation

An Adaptation needs to be added to ensure that the From header contains proper hostname. To add an Adaptation, select Adaptations on the left pane and select New (not shown). Configure the Adaptation as follows:

- In the Adaptation Name field enter an informative name.
- In the Module Name select DigitConversionAdapter.
- Select the Add button to add adaptation parameters. Following two values were configured during Compliance Testing.
  - fromto=true
  - osrcd=Avaya.com
6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to Session Manager. To add a SIP Entity, select SIP Entities on the left panel menu, and then click on the New button (not shown). The following will need to be entered for each SIP Entity.

Under General:

- In the Name field enter an informative name.
- In the FQDN or IP Address field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the Type field use Session Manager for a Session Manager SIP entity, CM for a Communication Manager SIP entity and SIP Trunk for the Avaya SBCE SIP entity.
- In the Adaptation field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu.
- In the Location field select the appropriate location from the drop down menu.
- In the Time Zone field enter the time zone for the SIP Entity.

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity.

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The FQDN or IP Address field is set to the IP address of the Session Manager SIP signalling interface.
Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop down menu select the domain added in **Section 6.2** as the default domain.
- Note that the **Endpoints** boxes were checked to allow SIP Endpoints to register on the specified ports.

![Listen Ports Table]

In the **Port** field enter the port number on which the system listens for SIP requests. In the **Protocol** field enter the transport protocol to be used for SIP requests. In the **Default Domain** field, from the drop down menu select the domain added in **Section 6.2** as the default domain. Note that the **Endpoints** boxes were checked to allow SIP Endpoints to register on the specified ports.
6.5.2. Avaya Aura® Communication Manager SIP Entities

The following screen shows one of the SIP entities for Communication Manager which is configured as an Evolution Server. This SIP Entity is used for the SIP Trunk. The FQDN or IP Address field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the Location to that defined in Section 6.3.

Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.
6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see Figure 1). Set **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.
6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select Entity Links on the left panel menu and click on the New button (not shown). Fill in the following fields in the new row that is displayed.

- In the Name field enter an informative name.
- In the SIP Entity 1 field select Session Manager.
- In the Port field enter the port number to which the other system sends its SIP requests.
- In the SIP Entity 2 field enter the other SIP Entity for this link, created in Section 6.5.
- In the Port field enter the port number to which the other system expects to receive SIP requests.
- Select the Trusted tick box to make the other system trusted.
- In the Protocol field enter the transport protocol to be used to send SIP requests.

Click Commit to save changes. The following screen shows the Entity Links used in this configuration.
6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select Routing Policies on the left panel menu and then click on the New button (not shown).

Under General:
- Enter an informative name in the Name field.
- Under SIP Entity as Destination, click Select, and then select the appropriate SIP entity to which this routing policy applies.
- Under Time of Day, click Add, and then select the time range.

The following screen shows the routing policy for calls inbound from the SIP Trunk to Communication Manager and ASBCE.
6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:
- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**:
- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to Service Provider’s SIP Trunking service.
The following screen shows the test dial pattern configured for Communication Manager.
6.9. Administer Application for Avaya Aura® Communication Manager

The Application for Communication Manager would normally be defined at system installation, but is shown here for reference. From the Home tab select Session Manager from the menu. In the resulting tab from the left panel menu select Application Configuration → Applications and click New (not shown).

- In the Name field enter a name for the application.
- In the SIP Entity field select the SIP entity for Communication Manager.
- In the CM System for SIP Entity field select the SIP entity for Communication Manager SIP Endpoints and select Commit to save the configuration.

![Application Editor](image-url)
6.10. Administer Application Sequence for Avaya Aura® Communication Manager

The Application Sequence for Communication Manager would normally be defined at system installation, but is shown here for reference. From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New** (not shown).

- In the **Name** field enter a descriptive name.
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading. Select **Commit**.

![Application Sequence Editor](image-url)
6.11. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab select User Management from the menu. Then select Manage Users and click New (not shown).

On the Identity tab:
- Enter the user's name in the Last Name and First Name fields.
- In the Login Name field enter a unique system login name in the form of user@domain e.g. 11101@avaya.com which is used to create the user's primary handle.
- The Authentication Type should be Basic.
- Set the Language Preference and Time Zone as required.

On the Communication Profile tab, enter a numeric Communication Profile Password and confirm it.
Expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.

Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked.
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field.
- Select the appropriate application sequence from the drop-down menu in the **Origination Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.10**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.
Expand the **Endpoint Profile** section.
- Select Communication Manager Element from the **System** drop-down menu.
- Select **Endpoint** from the drop-down menu for **Profile Type**.
- Enter the extension in the **Extension** field.
- Select the desired template from the **Template** drop-down menu.
- In the **Port** field IP is automatically inserted.
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.
- Select **Commit** (not shown) to save changes and System Manager will add the Communication Manager user configuration automatically.

![CM Endpoint Profile](image-url)
7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider’s SIP Trunk that is standard where possible and adapted to the Service Provider’s SIP implementation where necessary. Avaya SBCE also provides the SIPREC interface that is used by MiaRec to record calls. Configuration related to Session Manager and Service Provider’s SIP Trunk is not shown in this document.

![Login Screen](image)

7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL https://<ip-address>, where <ip-address> is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.
7.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and subnet masks to the interfaces. Note that only the A1 and B1 interfaces are used, typically the A1 interface is used for the internal side and B1 is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to Device Specific Settings → Network Management in the main menu on the left hand side and click on Add. The following interfaces were added for Session Manager and Service Provider’s SIP Trunk.

Select the Interface Configuration tab and click on the Status of the physical interface to toggle it. A status of Disabled will be changed to Enabled.

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on System Management in the main menu (not shown).
- Select Restart Application indicated by an icon in the status bar (not shown).

A status box will appear (not shown) that will indicate when the application has restarted.
7.3. Define Servers
A server definition is required for each server connected to the Avaya SBCE. In this case, the MiaRec is configured as a Recording Server.

To define the MiaRec Recording Server, navigate to Global Profiles → Server Configuration in the main menu on the left hand side. Click on Add and enter an appropriate name in the pop-up menu.

Click on Next and enter details in the dialogue box.

- In the Server Type drop down menu, select Recording Server.
- In the SIP Domain type in the domain configured in Section 6.2.
- Select a configured TLS profile for TLS Client Profile.
- Click on Add to enter an IP address.
- In the IP Addresses / FQDN box, type the MiaRec recording server interface address.
- In the Port box, enter the port to be used for the TLS listening port configured on the MiaRec (shown in the step 8).
- In the Transport drop down menu, select TLS.
- Click on Next.
Click on **Next** and configure as follows.

![Add Server Configuration Profile - Heartbeat](image)

Select **Next** and then **Finish** (not shown).

### 7.4. Define Routing
Routing information is required for routing recordings to MiaRec. The IP addresses and ports defined here will be used as the destination addresses for signalling.

To define routing to the MiaRec SIP Trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.

![Routing Profiles: MiaRec Server](image)
Click on **Next** and enter details for the Routing Profile:

- Click on **Add** to specify the IP address for the MiaRec SIP trunk.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used.
- Select the Server Configuration defined in **Section 7.3** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field.
- Click **Finish**.

### 7.5. Define Application Rules

An application rules needs to be defined for MiaRec. To create a new Application Rules, navigate to **Domain Policies → Application Rules**. Click on **Add** and enter an appropriate name in the pop-up menu and select **Next**.
On the **Application Rule** pop-up windows check **In** and **Out** boxes for **Audio**, and select **Finish**.

![Application Rule](image)

### 7.6. Define Media Rules

Audio formats need to be specified for MiaRec. To create a Media Rule for MiaRec, navigate to **Domain Policies → Media Rules**. Click on **Add** and enter an appropriate name in the pop-up menu and select **Next**.

![Media Rules: MiaRec](image)
On the Media Rule pop-up, under Audio Encryption, select a Preferred Format #1 and select continue. If using, SRTP select SRTP_AES_CM_128_128_HMAC_SHA1_80 or for RTP select RTP, select Next.
On the Media Rule pop-up, under the Audio Codec section, select box for Codec Prioritization. For Preferred Codecs select PCMU, PCMA and telephone-event, and click >. Select Next and Finish to save the configuration (not shown).
7.7. Configure UCID

UCID needs to be enabled for Signaling Rules that are defined for Session Manager and MiaRec. Navigate to Domain Policies → Signaling Rules. Select the policy for Session Manager and select the UCID tab. Click Edit, check box for Enabled and type in a unique value in Node ID field. Select Finish to save configuration.

Perform similar steps for MiaRec signaling rule.

7.8. Define End Point Policy Group

To define an End Point Policy Group for MiaRec, navigate to Domain Policies → End Point Policy Group and select Add. Click on Add and enter an appropriate name in the pop-up menu and select Next.
On the Policy Group pop-up, select the Application Rule defined in Section 7.5 and select the Media Rule defined in Section 7.6. Select Finish to save configuration.

7.9. Define Session Policies
To define Session Policy for MiaRec, navigate to Domain Policies → Session Policies and select Add. Click on Add and enter an appropriate name in the pop-up menu and select Next.

On the Session Policy pop-up, select box for Media Anchoring and Recording Server. For Routing Profile select the Routing profile configured in Section 7.4.
7.10. Define Session Flows

To define Session Policy for MiaRec, navigate to **Device Specific Settings → Session Flows** and select **Add**. Click on **Add** and enter an appropriate **Flow Name** in the pop-up menu and select the **Session Policy** defined in **Section 7.9**. Select **Finish** to save the configuration.

![Add Flow Window](image-url)
7.11. Server Flows

Server Flows combine the previously defined profiles for Session Manager and Service Provider’s SIP Trunk. These End Point Server Flows allow calls to be recorded by MiaRec when they are passing through Avaya SBCE to the Service Provider’s SIP Trunk. Navigate to **Device Specific Setting** → **End Point Flows** → **Server Flows**. There were two Server Flows added for MiaRec, one to record calls coming in from Service Provider’s SIP Trunking service and another for calls coming in from Session Manager. The screen capture below displays the configured Session Flows. Configure the fields as shown in the screen capture.

Screen captures for configuration of each Server Flow are as shown below:
Additionally, for a **Subscriber Flow** was added for Remote Workers, as shown below. The Subscriber Flow allows Remote Workers to register to Session Manager via Avaya SBCE and also SIPREC recordings for MiaRec.
8. Configure the MiaRec

MiaRec was deployed as a virtual machine on a virtualization platform. Configuration for MiaRec is performed via MiaRec web user interface which can be accessed through a browser. Point the browser to http://<ip-address>, where ip-address is the IP Address of MiaRec. Log on using appropriate credentials.

Navigate to Administration → System → Recording Interfaces and select Configure for SIPREC.
On the **Configure Recording Interface** page:

- Check box for **Enable SIPREC recording**.
- Type in port values for the signaling port depending on whether TCP or TLS is being used.

Select **Save** once done (not shown).

![Configure Recording Interface](image)
To access the call recordings, select **Recordings** on the MiaRec web interface:

Select a recording to view the details and playback.
9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **UP**.

2. From Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 1

TRUNK GROUP STATUS

Member    Port    Service State    Mtce Connected Ports

0001/001 T00011    in-service/idle    no
0001/002 T00012    in-service/idle    no
0001/003 T00013    in-service/idle    no
0001/004 T00014    in-service/idle    no
0001/005 T00015    in-service/idle    no
0001/006 T00016    in-service/idle    no
0001/007 T00017    in-service/idle    no
0001/008 T00018    in-service/idle    no
0001/009 T00019    in-service/idle    no
0001/010 T00020    in-service/idle    no
```
3. Verify that endpoints at the enterprise site can place calls to the Service Provider’s SIP Trunk and that the calls are being recorded by MiaRec.
4. Verify that endpoints at the enterprise site can receive calls from the Service Provider’s SIP Trunk and that the calls are being recorded by MiaRec.
5. Verify that the Remote Worker endpoints can place calls to the endpoints at the enterprise site and that the calls are being recorded by MiaRec.
6. Verify that the endpoints at the enterprise can place calls to the Remote Worker endpoints and that the calls are being recorded by MiaRec.
7. Verify that the Remote Worker endpoints can place calls to other Remote Workers and that the calls are being recorded by MiaRec.
8. Verify that the Remote Worker endpoints can place calls to the Service Provider’s SIP Trunk and that the calls are being recorded by MiaRec.
9. Verify that the Remote Worker endpoints can receive calls from the Service Provider’s SIP Trunk and that the calls are being recorded by MiaRec.
10. Should issues arise with the call recording, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from the Avaya SBCE to the MiaRec server are receiving a response.

10. Conclusion
These Application Notes describe the configuration necessary to record calls using MiaRec in the Avaya Aura Platform consisting of Avaya Aura ® Communication Manager R7.0.1, Avaya Aura ® Session Manager 7.0.1 and Avaya Session Border Controller for Enterprise R7.1. The MiaRec call recording and quality management solutions help businesses to easily record, analyze and access important interactions to meet regulatory compliance requirements, enhance customer service and increase agent productivity. The software was successfully tested with a number of observations listed in Section 2.2.
11. Additional References

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


[2] *Upgrading and Migrating Avaya Aura® applications to 7.0.1 from System Manager*, Release 7.0.1, Aug 2016


[12] *Administering Avaya Aura® Session Manager Release 7.0.1*, May 2016


[14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015

