Abstract

These Application Notes describe the configuration steps required for the Calabrio One solution to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

Calabrio One uses the Avaya Aura® Application Enablement Services Device, Media and Call Control (DMCC) and System Management Service (SMS) services to capture real-time CTI data and RTP streams from Avaya Aura® Communication Manager to produce recordings of phone activity for agents and knowledge workers.

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

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

Calabrio One (Calabrio) is a contact center and knowledge worker oriented recording solution that uses the Avaya Aura® Application Enablement Services (AES) System Management Services (SMS) and Device, Media and Call Control (DMCC) interfaces.

Before Calabrio can start recording, it establishes a client connection with AES and performs a SMS service query to obtain the list of agents and stations configured in Avaya Aura® Communication Manager (Communication Manager).

The application uses SMS to populate database information in the Calabrio system. The information collected are, list operation on Agent model, list and display operations on Station model and list operation on Hunt Group model.

The Calabrio DMCC integration works by using two supported DMCC methods, Single Step Conference and Multiple Registration, to capture the media for recording. The Single Step Conference method is used for users with Avaya SIP and Analog telephones, and the Multiple Registration method is used for users with Avaya H.323 and Digital telephones.

2. General Test Approach and Test Results

The compliance test focused on the ability for calls to be recorded. Calls were manually placed from the public switched telephone network (PSTN) directly to and from recorded devices, and to VDN or Skill group extension. For each recorded station in a call, there is one recording generated. Once a call is completed, the recordings are reviewed for their quality, completeness (number of recordings beginning to end, etc.), and accuracy of tagging information (owner, calling party, called party, etc).

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 this Application Note, the interface between Avaya systems and Calabrio One did not include use of any specific encryption features as requested by Calabrio.

2.1. Interoperability Compliance Testing
The compliance test validated the ability of Calabrio to successfully record calls routed to and from Analog, Digital, and IP endpoints as well as softphone clients. Common call scenarios including hold/resume, mute/unmute, transfer, and conference were exercised during the test. Additional tests included the ability to monitor live calls and to record screen activity associated with a recorded station.

Additionally, serviceability testing was performed to confirm the ability for Calabrio to recover from common outages such as network outages and server reboots.

2.2. Test Results
All test cases passed with the following observations.

- Calling Number column is populated with the actual Called Number data for a blind conference call recording.

2.3. Support
Technical support on Calabrio can be obtained through the following:

- Phone: +1 (763) 592-4680 or +1 (800) 303-1248
- Web: http://calabrio.com/about-calabrio/services/
- Email: calabriosupport@calabrio.com
3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services
- Avaya Endpoints
- Calabrio One server installed on a standalone machine

Calls routed to and from Communication Manager used PRI trunks to connect to the PSTN.

![Figure 1 – Calabrio One Compliance Test Configuration](image-url)
4. Equipment and Software Validated
The following equipment and version were used in the reference configuration described above:

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager running on virtualized environment</td>
<td>7.1.3.3.0-FP3SP3</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services running on virtualized environment</td>
<td>7.1.3.3.0.2-0</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager running on virtualized environment</td>
<td>7.1.3.3.713307</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>7.1.3.3.069127</td>
</tr>
<tr>
<td>Avaya Aura® Media Server</td>
<td>7.8.0.384</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>39.20.0</td>
</tr>
<tr>
<td>Avaya 96x1 Series IP Deskphone</td>
<td></td>
</tr>
<tr>
<td>• 9641G (H.323)</td>
<td>6.8102</td>
</tr>
<tr>
<td>• 9611G (SIP)</td>
<td>7.1.5</td>
</tr>
<tr>
<td>Avaya 1416 Digital Deskphone</td>
<td>FW 1</td>
</tr>
<tr>
<td>2500 analog phone</td>
<td>-</td>
</tr>
<tr>
<td>Desktop PC running Avaya One-X® Communicator (H.323)</td>
<td>6.2.14 SP14</td>
</tr>
<tr>
<td>Desktop PC running Avaya One-X® Agent (H.323)</td>
<td>2.5.13</td>
</tr>
<tr>
<td>Calabrio Recording and Quality Management running under Windows 2016 Server</td>
<td>10.4.18.810</td>
</tr>
<tr>
<td>• Avaya DMCC SDK 7.0</td>
<td>7.0</td>
</tr>
<tr>
<td>• Java Development Kit</td>
<td>1.8</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures fall into the following areas:

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer IP Services for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Add SMS User Account
- Verify Recorded Extensions
- Add Virtual Stations

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation in Section 10.

5.1. Verify Feature and License

Enter the `display system-parameters customer-options` command and ensure that `Computer Telephony Adjunct Links` is set to `y`. If this option is not set to `y`, contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options

OPTIONAL FEATURES

  Access Security Gateway (ASG)? n  Authorization Codes? y
  Analog Trunk Incoming Call ID? y  CAS Branch? n
  A/D Grp/Sys List Dialing Start at 01? y  CAS Main? n
  Answer Supervision by Call Classifier? y  Change COR by FAC? n
  ARS? y  Computer Telephony Adjunct Links? y
  ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
  ARS/AAR Dialing without FAC? y  DCS (Basic)? y
  ASAI Link Core Capabilities? n  DCS Call Coverage? y
  ASAI Link Plus Capabilities? n  DCS with Rerouting? y
  Async. Transfer Mode (ATM) PNC? n  Digital Loss Plan Modification? y
  Async. Transfer Mode (ATM) Trunking? n  DS1 MSP? y
  ATM WAN Spare Processor? n  DS1 Echo Cancellation? y
  ATM? n  ATMS? y
  Attendant Vectoring? y

(NOTE: You must logoff & login to effect the permission changes.)
```
5.2. Administer Communication Manager System Features

Enter the `change system-parameters features` command and ensure that on page 5 Create Universal Call ID (UCID) is enabled and a relevant UCID Network Node ID (1 was used in the test) is defined. Also ensure that on Page 13 that Send UCID to ASAI is set to y. Calabrio relies on UCID to track complex calls (Transfers and Conferences).

<table>
<thead>
<tr>
<th>SYSTEM PRINTER PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint:</td>
</tr>
<tr>
<td>Lines Per Page: 60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SYSTEM-WIDE PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Name:</td>
</tr>
<tr>
<td>Emergency Extension Forwarding (min): 10</td>
</tr>
<tr>
<td>Enable Inter-Gateway Alternate Routing? n</td>
</tr>
<tr>
<td>Enable Dial Plan Transparency in Survivable Mode? n</td>
</tr>
<tr>
<td>EC500 Routing in Survivable Mode: dpt-then-ec500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MALICIOUS CALL TRACE PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply MCT Warning Tone? n</td>
</tr>
<tr>
<td>MCT Voice Recorder Trunk Group:</td>
</tr>
<tr>
<td>Delay Sending RELease (seconds): 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SEND ALL CALLS OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send All Calls Applies to: station</td>
</tr>
<tr>
<td>Auto Inspect on Send All Calls? n</td>
</tr>
<tr>
<td>Preserve previous AUX Work button states after deactivation? n</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNIVERSAL CALL ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Universal Call ID (UCID)? y</td>
</tr>
<tr>
<td>UCID Network Node ID: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CALL CENTER MISCELLANEOUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Callr-info Display Timer (sec): 10</td>
</tr>
<tr>
<td>Clear Callr-info: next-call</td>
</tr>
<tr>
<td>Allow Ringer-off with Auto-Answer? n</td>
</tr>
<tr>
<td>Reporting for PC Non-Predictive Calls? n</td>
</tr>
<tr>
<td>Agent/Caller Disconnect Tones? n</td>
</tr>
<tr>
<td>Interruptible Aux Notification Timer (sec): 3</td>
</tr>
<tr>
<td>Zip Tone Burst for Callmaster Endpoints: double</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ASAI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy ASAI UUI During Conference/Transfer? n</td>
</tr>
<tr>
<td>Call Classification After Answer Supervision? n</td>
</tr>
<tr>
<td>Send UCID to ASAI? y</td>
</tr>
<tr>
<td>For ASAI Send DTMF Tone to Call Originator? y</td>
</tr>
<tr>
<td>Send Connect Event to ASAI For Announcement Answer? n</td>
</tr>
<tr>
<td>Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n</td>
</tr>
</tbody>
</table>
5.3. Administer IP-Services for Application Enablement Services

Add an IP Services entry for Application Enablement Services as described below:

- Enter the `change ip-services` command.
- In the Service Type field, type AESVCS.
- In the Enabled field, type y.
- In the Local Node field, type the Node name procr for the Processor Ethernet Interface.
- In the Local Port field, use the default of 8765.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration.

```
change ip-services

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Enabled</th>
<th>Local Node</th>
<th>Local Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AESVCS</td>
<td>y</td>
<td>procr</td>
<td>8765</td>
</tr>
</tbody>
</table>
```

On Page 3 of the IP Services form, enter the following values:

- In the AE Services Server field, type the host name of the Application Enablement Services server.
- In the Password field, type the same password to be administered on the Application Enablement Services server in Section 6.1.
- In the Enabled field, type y.

```
change ip-services

<table>
<thead>
<tr>
<th>Server ID</th>
<th>AE Services Server</th>
<th>Password</th>
<th>Enabled</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>aes15019</td>
<td>*</td>
<td>y</td>
<td>in use</td>
</tr>
<tr>
<td>2:</td>
<td>aes10210</td>
<td>*</td>
<td>y</td>
<td>in use</td>
</tr>
<tr>
<td>3:</td>
<td>aes15087</td>
<td>*</td>
<td>y</td>
<td>in use</td>
</tr>
</tbody>
</table>
```

5.4. Administer Computer Telephony Integration (CTI) Link

Enter the `add cti-link <link number>` command, where `<link number>` is an available CTI link number.

- In the Extension field, type a valid extension.
- In the Type field, type ADJ-IP.
- In the Name field, type a descriptive name.

```
add cti-link 1

CTI Link: 1
Extension: 58001
Type: ADJ-IP
Name: AES 7.1.3
```
5.5. Add SMS User Account
Calabrio uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application.

A privileged user was used in this test. Access the System Management Interface by typing the IP address of Communication Manager in the URL of a web browser. Log in using proper credentials and navigate to Administration → Server (Maintenance). The Administration/Server (Maintenance) screen is seen as shown below. Create a user account on Communication Manager by navigating to the Administrator Accounts page under Security from the left hand pane and selecting the radio button Add Login and Privileged Administrator. Click Submit to continue the process.
The Administrator Accounts -- Add Login screen is displayed. Enter a name to the Login name field and enter desired password.

Though a Privileged Administrator account was used, a new SMS user profile can be added to limit permissions. Use the add user-profile next command to add a new user profile. Set the Shell Access, Call Center B, Features C, and Stations M to y. This profile will need to be assigned to user created above.
5.6. Verify Recorded Extensions

For H.323 and Digital stations that will be recorded, enable IP Softphone as shown below, which will be used by Calabrio to correspond to the Multiple Registration recording method. Calabrio needs to know the Security Code in order to successfully register, ensure that security codes are set to the same value for these stations; however, check with Calabrio for alternatives if necessary.

For SIP and Analog stations that will be recorded, leave the IP Softphone setting disabled, which will be used by Calabrio to correspond to the Single Step Conference recording method.

Use the display station n command to verify information, or change station n to make changes if necessary.

Note that all SIP station configurations need to be completed from Session Manager via System Manager.

display station 53001

<table>
<thead>
<tr>
<th>Extension: 53001</th>
<th>Lock Messages? n</th>
<th>BCC: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: 9608</td>
<td>Security Code: *</td>
<td>TN: 1</td>
</tr>
<tr>
<td>Port: S00003</td>
<td>Coverage Path 1:</td>
<td>COR: 1</td>
</tr>
<tr>
<td>Name:</td>
<td>Coverage Path 2:</td>
<td>COS: 1</td>
</tr>
<tr>
<td></td>
<td>Hunt-to Station:</td>
<td>Tests: y</td>
</tr>
</tbody>
</table>

STATION OPTIONS

- Time of Day Lock Table: 19
- Personalized Ringing Pattern: 1
- Message Lamp Ext: 3301
- Mute Button Enabled? y
- Button Modules: 1
- Speakerphone: 2-way
- Display Language: english
- Media Complex Ext:
  - IP SoftPhone? y
- IP Video Softphone? n
- Short/Prefixed Registration Allowed: default
- Customizable Labels? y
5.7. Add Virtual Stations

Virtual stations are used by Calabrio to do Single Step Conference based call recording for SIP and Analog stations. Add a virtual station using the add station <n> command; where <n> is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields. Note that the number of virtual stations configured should be equal to the number of stations that will be recorded simultaneously.

- In the **Type** field, enter a station type such as *9640*.
- In the **Name** field, enter a name containing the **DMCC** string (e.g. **DMCC Station 1**). Calabrio uses the DMCC prefix string to identify virtual stations.
- In the **Security Code** field, enter a desired value.
- Set the **IP SoftPhone** field to **y**.

```
display station 55551
```

<table>
<thead>
<tr>
<th>Extension: 55551</th>
<th>Lock Messages? n</th>
<th>BCC: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type: 9640</strong></td>
<td><strong>Security Code:</strong> *</td>
<td>TN: 1</td>
</tr>
<tr>
<td>Port: S00035</td>
<td>Coverage Path 1: COR: 1</td>
<td></td>
</tr>
<tr>
<td><strong>Name: DMCC Station 1</strong></td>
<td>Coverage Path 2: COS: 1</td>
<td></td>
</tr>
<tr>
<td>Hunt-to Station:</td>
<td>Tests? y</td>
<td></td>
</tr>
</tbody>
</table>

**STATION OPTIONS**

- **Time of Day Lock Table:**
- **Personalized Ringing Pattern:** 1
- **Message Lamp Ext:** 3317
- **Speakerphone:** 2-way
- **Mute Button Enabled?** y
- **Display Language:** english
- **Button Modules:** 0
- **Survivable GK Node Name:**
- **Survivable COR:** internal
- **Media Complex Ext:**
- **IP Complex**
- **Survivable Trunk Dest?** y
- **IP Video Softphone?** n
- **Short/Prefixed Registration Allowed:** default
- **Customizable Labels?** Y
6. Configure Avaya Aura® Application Enablement Services

All administration of Application Enablement Services is performed via a web browser. Enter https://<ip-addr> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the Welcome to OAM page is displayed. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

The procedures fall into the following areas:
- Configure Communication Manager Switch Connections
- Configure Calabrio User
- Confirm TSAPI and DMCC Licenses
6.1. Configure Communication Manager Switch Connections

To add links to Communication Manager, navigate to the Communication Manager Interface ➔ Switch Connections page and enter a name for the new switch connection (e.g. cm15014) and click the Add Connection button (not shown). The Connection Details screen is shown. Enter the Switch Password configured in Section 5.3 and check the Processor Ethernet box if using the procr interface. Click Apply.

The display returns to the Switch Connections screen which shows that the cm15014 switch connection has been added.
Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es). The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.

![Edit Processor Ethernet IP](image)

### 6.2. Configure Calabrio User

In the Navigation Panel, select **User Management → User Admin → Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list.

Click **Apply** (not shown) at the bottom of the pages to save the entry.
If the Security Database (SDB) is enabled on Application Enablement Services, set the Calabrio user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

Navigate to Security → Security Database → CTI Users → List All Users and select the calabrio user and click Edit.
On the Edit CTI User panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog (not shown).
6.3. Confirm TSAPI and DMCC Licenses

Calabrio uses a DMCC (VALUE_AES_DMCC_DMC) license for each recording port. Additionally, a TSAPI Basic (VALUE_AES_TSAPI_USERS) license is used for each agent station being monitored. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.

From the left pane menu on Application Enablement Services Management Console, click Licensing → WebLM Server Access (not shown). A Web License Manager login window is displayed (not shown). Enter proper credentials to log in. Click Licensed products → APPL_ENAB → Application_Enablement from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough Device Media and Call Control and TSAPI Simultaneous Users licenses available.
7. Configure Calabrio One

The initial configuration of the Calabrio server is typically performed by Calabrio technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the Calabrio solution to interoperate with Communication Manager and Application Enablement Services. Configuration in this section was performed with the assistance from a Calabrio engineer.

The steps include:

- Configuration of the Application Enablement Interfaces – SMS
- Installation of the Data Server
- Configuration of the Data Server
- Configuration of the Application Enablement Interfaces – DMCC
- Configuration of Device Associations

The configuration of the Calabrio server is performed using Calabrio One web interface. Access the web interface via a browser to the IP Address of Calabrio One server. Log on using appropriate credentials.
7.1. Configuration of the Application Enablement Interfaces – SMS

From the Dashboard, navigate to Application Management → ACD Configuration.

On the ACD Configuration page, select Add to add a new ACD. Select Avaya CM with Contact Center Elite from the Select ACD drop down menu and type in a Name for the ACD.
Configure the ACD as shown below:

- **SMS SERVER URL**: Type in the SMS Server URL for the AES.
- **COMMUNICATION MANAGER IP ADDRESS**: Communication Manager IP Address
- **COMMUNICATION MANAGER LOGIN & PASSWORD**: As configured in Section 5.5
- **VIRTUAL EXTENSION PREFIX**: Type in DMCC

Add the other configuration as instructed by a Calabrio. Select **Save** once done.
In the **Application Enablement Services Information** section:

- Type in the hostname of Communication Manager in **SWITCH CONNECTION NAME**
- FOR **HOSTNAME / IP ADDRESS**, type in the IP Address of AES
- Configure the default DMCC Port in the **PORT** field, 4721
7.2. Installation of the Data Server

From the Application Management page, select Downloads.

From the Downloads page, select Calabrio One Data Server to download the Data Server. Install the Data Server on the Calabrio One server.

Downloads

Use this page to access the Calabrio ONE installers available to you. Click the desired installer to download it and follow the instructions in the installation wizard.

Available Installers

Calabrio One Data Server

Calabrio One Smart Desktop
7.3. Configuration of the Data Server

Navigate to Application Management → Data Server Configuration.
On the **Data Server Configuration** page, select the name of the Data Server to be configured. Check box for **Enable Sync** and **Enable Capture** (not shown) and choose the ACD configured in previous step to retrieve the data from.
Continuing from above, check box for **Enable CTI Signaling** and type in the IP Address of Data Server being configured. Check box for **Enable Audio Recording**. Enter the IP Address of the Recording server and the path to where recordings should be sent to for processing.

**Note:** The Data Server can be installed on multiple machines and the functions split between them to increase performance. For this testing, the Data Server was installed on the same server running Calabrio One.

Select **Test Connection** to test this configuration, followed by **Save**.
7.4. Configuration of the Application Enablement Interfaces – DMCC

From the Application Management page, select Telephony Groups.

On the Telephone Groups page, Type in a TELEPHONY GROUP NAME and select Avaya Communication Manager from the TELEPHONY GROUP PLATFORM TYPE drop down menu. Select Add.
In the **Avaya Telephony Platform Configuration** section:

- Select **Use Static Password** radio button and type in the password from **Section 5.6**.
- Select the **ASSOCIATED AVAYA ACD** as configured in previous section.
- Select a **DEVICE SYNCHRONIZATION DATA SERVER**. This Data Server was pre-configured.

Select the **Signaling** tab, type in a name for a **Signaling Group** and select **Add**.
Telephony Groups

1. Telephony  2. Signaling  3. Recording

Signaling Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephony Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES7</td>
<td>AES7</td>
</tr>
</tbody>
</table>

Add  | Update  | Delete  | Reset Signaling Group
- **PRIMARY QM SIGNALING DATA SERVER**: Type in the IP Address of Calabrio One server
- **AES SERVER**: Type in the IP Address of AES

Select the **Recording** tab, type in a name for a **Recording Group** and select **Add**.
Select the **Recording Group** from that is being configured and set **Priority** to **Primary**. Select **Save** once done.
7.5. Configuration of Device Associations
Navigate to Application Management → Device Associations.
Configure the device association as needed. During the compliance test, the following extensions were configured to be recorded.

### Device Associations

<table>
<thead>
<tr>
<th>Configured</th>
<th>Device Name</th>
<th>Device Type</th>
<th>Extension</th>
<th>Virtual Ext...</th>
<th>Agent</th>
<th>Telephony G...</th>
<th>Signaling G...</th>
<th>Recording G...</th>
<th>Recording Ty...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>53000</td>
<td>Avaya Phone</td>
<td>53000</td>
<td>55555</td>
<td>Analog Agent</td>
<td>AES/CXM?</td>
<td>AES7</td>
<td>AES7</td>
<td>Single Step</td>
</tr>
<tr>
<td>Yes</td>
<td>53001</td>
<td>Avaya Phone</td>
<td>53001</td>
<td>55551</td>
<td>IP Agent1</td>
<td>AES/CXM?</td>
<td>AES7</td>
<td>AES7</td>
<td>Multiple Regi</td>
</tr>
<tr>
<td>Yes</td>
<td>53002</td>
<td>Avaya Phone</td>
<td>53002</td>
<td>55552</td>
<td>IP Agent2</td>
<td>AES/CXM?</td>
<td>AES7</td>
<td>AES7</td>
<td>Multiple Regi</td>
</tr>
<tr>
<td>Yes</td>
<td>53101</td>
<td>Avaya Phone</td>
<td>53101</td>
<td>55551</td>
<td>SIP Agent1</td>
<td>AES/CXM?</td>
<td>AES7</td>
<td>AES7</td>
<td>Single Step</td>
</tr>
<tr>
<td>Yes</td>
<td>53003</td>
<td>Avaya Phone</td>
<td>53003</td>
<td>55553</td>
<td>IP Agent3</td>
<td>AES/CXM?</td>
<td>AES7</td>
<td>AES7</td>
<td>Multiple Regi</td>
</tr>
<tr>
<td>Yes</td>
<td>53102</td>
<td>Avaya Phone</td>
<td>53102</td>
<td>55552</td>
<td>SIP Agent2</td>
<td>AES/CXM?</td>
<td>AES7</td>
<td>AES7</td>
<td>Single Step</td>
</tr>
</tbody>
</table>
8. Verification Steps

8.1. Verify AES
From the AES OAM page, navigate to Status  Status and Control  DMCC Service Summary. Verify the user configured in Section 6.2 is successfully connected to AES.

8.2. Verify Calabrio One
Place a few calls between recorded extensions. Verify the recordings are available on the Calabrio One web interface.
Select a call of interest and double click to launch a playback window as shown below.
9. Conclusion

These Application Notes describe the procedures for configuring Calabrio One to monitor and record calls placed to and from agents and phones on Avaya Aura® Communication Manager. In the configuration described in these Application Notes, Calabrio uses the Device and Media Control Services and System Management Service of Avaya Aura® Application Enablement Services to perform recording. All feature and serviceability test cases were completed and passed with the observations noted in Section 2.2.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

Product documentation related to Calabrio One can be obtained directly from Calabrio.