



Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio Call Recording and Quality Management with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

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

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

Before CRQM can start recording, it establishes a client connection with Avaya Aura® Application Enablement Services, performs a SMS service query to obtain the list of agents and stations configured in Avaya Aura® Communication Manager.

The application uses the SMS to populate database information in the CRQM 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 CRQM 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.

2.1. Interoperability Compliance Testing

The compliance test validated the ability of CRQM 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 CRQM to recover from common outages such as network outages and server reboots.

2.2. Test ResultsRs

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.
- By design, Live Monitoring is only supported for stations using Multiple Registrations as in H.323 or Digital stations.
- A SIP user being recorded cannot use softphones since the application requires the IP Softphone setting to be disabled.

2.3. Support

Technical support on Calabrio CRQM 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
- IP, Digital, and analog endpoints
- Avaya one-X® Communicator and Avaya one-X® Agent softphones
- Calabrio CRQM server installed on a standalone machine

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

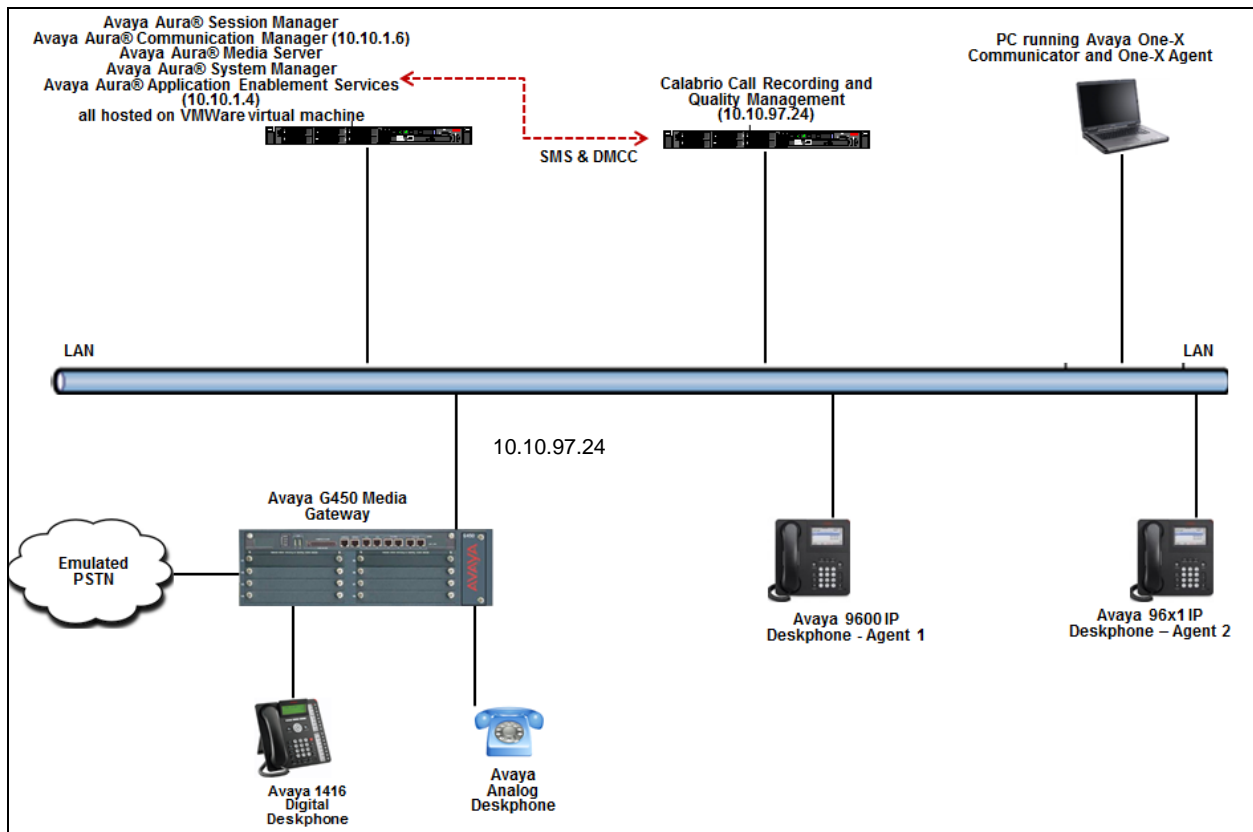


Figure 1 – Calabrio CRQM Compliance Test Configuration

4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.0.0.3.1-SP3
Avaya Aura® Application Enablement Services running on virtualized environment	7.0.0.0.13-0
Avaya Aura® Session Manager running on virtualized environment	7.0.1.1.701114
Avaya Aura® System Manager	7.0.1.1 SP1
Avaya Aura® Media Server	7.7.0.359
Avaya G450 Media Gateway	FW 37.19.0/1
Avaya 96x1 Series IP Deskphone <ul style="list-style-type: none">9641G (H.323)9611G (SIP)	6.6229 7.0.1
Avaya 1416 Digital Deskphone	FW 1
2500 analog phone	-
Desktop PC running Avaya One-X® Communicator (H.323)	6.2.11 SP11
Desktop PC running Avaya One-X® Agent (H.323)	2.5.8.6
Calabrio Recording and Quality Management running under Windows 2012 R2 Standard Server <ul style="list-style-type: none">DMCC Java SDK	9.5.1.391 6.3.1.0.175

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                               Page 4 of 12
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
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
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**. CRQM relies on UCID to track complex calls (Transfers and Conferences).

```
change system-parameters features                               Page 5 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station      Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y      UCID Network Node ID: 1
```

```
change system-parameters features                               Page 13 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
  Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? n
  Call Classification After Answer Supervision? n
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

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					Page	1 of	3
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				

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				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes70	*	y	in use		
2:	aesvm63	*	y	idle		
3:	aesvm70	*	y	idle		
4:	aes7	*	y	idle		

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		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 3332		
Type: ADJ-IP		
		COR: 1
Name: AES70		

5.5. Add SMS User Account

CRQM 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; however, a local administrator would want to restrict the user account. This involves creating a user profile at the SAT, and then creating and assigning that user to the profile in the web admin pages. To illustrate, the **add user-profile-by-category 31** command was used to create the profile used in the test as shown below, where **31** is the user profile number used during compliance testing. Enter a descriptive name for the **User Profile Name** field. The **Shell Access**, **Call Center B** and **Stations M** fields were set to **y**.

```
add user-profile-by-category 31                                     Page 1 of 39
                        USER PROFILE 31

User Profile Name: Calabrio SMS

    This Profile is Disabled? n                                Shell Access? y
Facility Test Call Notification? n    Acknowledgement Required? n
    Grant Un-owned Permissions? n        Extended Profile? n

Name          Cat Enbl          Name          Cat Enbl
Adjuncts A    n                Routing and Dial Plan J    n
Call Center B y                Security K    n
Features C    y                Servers L    n
Hardware D    n                Stations M    y
Hospitality E    n            System Parameters N    n
IP F          n                Translations O    n
Maintenance G    n            Trunking P    n
Measurements and Performance H    n    Usage Q    n
Remote Access I    n            User Access R    n
```

Read only access to Agents and Stations is required. Enter **r-** permissions for the **B** and **M** Categories on the **Set Permissions for Category** entry on the **change user-profile-by-category** form. This requires two separate transactions, so repeat for each category. Please note that this profile will be used later in this section.

```
change user-profile-by-category 31                                     Page 3 of 39
      USER PROFILE BY CATEGORY 31
Set Permissions For Category: B To: r-      Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
      Name          Cat  Perm
              agent B    r-
      agent-loginID B    r-
      announcements B    r-
      bcms agent B      r-
      bcms skill/split B    r-
      bcms summary agent B    r-
      bcms summary skill/split B    r-
      bcms summary trunk B    r-
      bcms summary vdn B    r-
      bcms system B      r-
      bcms trunk B       r-
      bcms vdn B         r-
      best-service-routing B    r-
      bcms-vustats loginIDs B    r-
      crm-features B      r-
```

```
change user-profile-by-category 31                                     Page 29 of 39
      USER PROFILE BY CATEGORY 31
Set Permissions For Category: M To: r-      Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
      Name          Cat  Perm
              ess L      --
      ess clusters L    --
      ess port-networks L    --
              lsp L      --
      media-server L     --
      remote-office L    --
      alias station M     r-
      attendant M        r-
      bridged-extensions M    r-
      coverage answer-group M    r-
      button-location-aca M     r-
      button-restriction M      r-
      call-forwarding M         r-
      console-parameters M      r-
      coverage answer-group M    r-
      coverage path M           r-
```

Access the System Management Interface by typing the IP address of Communication Manager in the URL of a web browser. Login 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 **Administer Accounts** page under **Security** from the left hand pane and selecting the radio button **Add Login** and **SAT Access Only**. Click **Submit** to continue the process.

AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration This Server: interopCM

Administration / Server (Maintenance)

Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

☒ Add Login

☐ Privileged Administrator

☐ Unprivileged Administrator

☒ SAT Access Only

☐ Web Access Only

☐ CDR Access Only

☐ Business Partner Login (dadmin)

☐ Business Partner Craft Login

☐ Custom Login

☐ Change Login

☐ Remove Login

☐ Lock/Unlock Login

☐ Add Group

☐ Remove Group

Submit **Help**

The **Administrator Accounts -- Add Login** screen is displayed. Enter a name to the **Login name** field and select the profile defined earlier in this section (**prof31**) in the **Additional groups (profile)** field. Select **Password** for the **Select type of authentication** field and enter desired password.

Administrator Accounts -- Add Login: SAT Access Only

This page allows you to create a login that is intended to have access only to the Communication Manager System Administration Terminal (SAT) interface.

Login name:

Primary group: ☐ users ☒ **susers**

Additional groups (profile):

Linux shell:

Home directory:

Lock this account: ☐

SAT Limit:

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Select type of authentication: ☐ ASG: Auto-generate key ☐ ASG: enter key ☒ **Password**

Enter password or key:

Re-enter password or key:

Force password/key change on next login: ☒ No ☐ Yes

You must assign a profile that has no web access if you want a login with SAT access only.

This shell setting does NOT disable the "go shell" SAT command for this user.

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. CRQM 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 3301	Page 1 of 6	
STATION		
Extension: 3301	Lock Messages? n	BCC: 0
Type: 9641	Security Code: *	TN: 1
Port: S00011	Coverage Path 1:	COR: 1
Name:	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 3301	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 1	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	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 CRQM 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**).
CRQM uses the DMCC string to identify virtual stations.
- In the **Security Code** field, enter a desired value.
- Set the **IP SoftPhone** field to **y**.


display station 3317		Page 1 of 5
STATION		
Extension: 3317	Lock Messages? n	BCC: 0
Type: 9640	Security Code: *	TN: 1
Port: S00019	Coverage Path 1:	COR: 1
Name: DMCC Station 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	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:	
Survivable Trunk Dest? y	IP SoftPhone? 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

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Mon Sep 12 20:23:09 2016 from 10.10.97.236
Number of prior failed login attempts: 0
HostName/IP: aes70/10.10.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.13-0
Server Date and Time: Wed Sep 21 15:23:33 UTC 2016
HA Status: Not Configured

Home

Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
▶ High Availability
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▶ Status
▶ User Management
▶ Utilities
▶ Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

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. **interopCM**) 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**.

Communication Manager Interface | Switch Connections Home | Help | Logout

▶ AE Services
 ▼ Communication Manager Interface
 Switch Connections
 ▶ Dial Plan
 High Availability
 ▶ Licensing
 ▶ Maintenance
 ▶ Networking
 ▶ Security
 ▶ Status
 ▶ User Management
 ▶ Utilities
 ▶ Help

Connection Details - interopCM

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

Provide AE Services certificate to switch ☒

Secure H323 Connection ☐

Processor Ethernet ☒

The display returns to the **Switch Connections** screen which shows that the **interopCM** switch connection has been added.

Communication Manager Interface | Switch Connections Home | Help | Logout

▶ AE Services
 ▼ Communication Manager Interface
 Switch Connections
 ▶ Dial Plan
 High Availability
 ▶ Licensing
 ▶ Maintenance
 ▶ Networking

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> interopCM	Yes	30	1
<input type="radio"/> server1	Yes	30	1

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.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance

Edit Processor Ethernet IP - interopCM

10.10.1.6

Name or IP Address	Status
10.10.1.6	In Use

Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing

Edit H.323 Gatekeeper - interopCM

Name or IP Address

☒ 10.10.1.6

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.

The screenshot shows the 'Add User' form within the 'User Management' application. The breadcrumb trail at the top reads 'User Management | User Admin | Add User'. The left navigation pane shows a tree structure with 'User Management' expanded, containing 'Service Admin' and 'User Admin'. 'User Admin' is further expanded to show 'Add User' (highlighted in blue), 'Change User Password', 'List All Users', 'Modify Default Users', and 'Search Users'. The main content area is titled 'Add User' and includes a note: 'Fields marked with * can not be empty.' The form fields are as follows:

Field	Value
* User Id	calabrio
* Common Name	calabrio
* Surname	calabrio
* User Password	
* Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	

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**.

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> calabrio	calabrio	NONE	NONE
<input type="radio"/> dmcc	dmcc	NONE	NONE

EditList All

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).

Security | Security Database | CTI Users | List All Users
Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users
Search Users

Edit CTI User

User Profile:	User ID	calabrio
	Common Name	calabrio
	Worktop Name	NONE
	Unrestricted Access	<input checked="" type="checkbox"/>

Call and Device Control:	Call Origination/Termination and Device Status	None
--------------------------	--	------

Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	<input type="checkbox"/>

Routing Control:	Allow Routing on Listed Devices	None
------------------	---------------------------------	------

Apply Changes
Cancel Changes

6.3. Confirm TSAPI and DMCC Licenses

CRQM 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.

▼ Application_Enablement	License File Host IDs:		
View license capacity			
View peak usage			
CCTR	Licensed Features		
►ContactCenter			
CE	13 Items Show All ▼		
►COLLABORATION_ENVIRONMENT	Feature (License Keyword)	Expiration date	Licensed capacity
MESSAGING	Device Media and Call Control VALUE_AES_DMCC_DMC	January 2, 2017	250
►Messaging	AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	January 2, 2017	250
POM	AES HA LARGE VALUE_AES_HA_LARGE	January 2, 2017	250
►POM	AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	January 2, 2017	250
PRESENCE_SERVICES	Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	January 2, 2017	250
►Presence_Services	CVLAN ASAI VALUE_AES_CVLAN_ASAI	January 2, 2017	250
SessionManager	AES HA MEDIUM VALUE_AES_HA_MEDIUM	January 2, 2017	250
►SessionManager	AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	January 2, 2017	250
Uninstall license	DLG VALUE_AES_DLG	January 2, 2017	250
Server properties	TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	January 2, 2017	250
Shortcuts			
Help for Installed Product			

7. Configure Calabrio Call Recording and Quality Management

The initial configuration of the CRQM server is typically performed by Calabrio technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the CRQM solution to interoperate with Communication Manager and Application Enablement Services.

The steps include:

- Configuration of the Application Enablement Interfaces – SMS
- Configuration of the Application Enablement Interfaces – DMCC
- Configuration of Users
- Configuration of Devices
- Configuration of Recording Schedules (Workflows)

The configuration of the CRQM server is performed using the **Calabrio Monitoring and Recording Administrator** application, which can be launched by clicking **Start → All Programs → Calabrio → Monitoring and Recording Administrator** from the CRQM server. Log in to the application with the proper credentials.

7.1. Configuration of the Application Enablement Interfaces – SMS

From the left pane, navigate to **Enterprise → System Configuration → Data Synchronization**.

Provide the **IP Address** or **Host Name** of the Application Enablement Services server in the **AE Services SMS Information** section. In the **Avaya Communication Manager Information** section, provide the **IP Address** of Communication Manager procr interface as well as the **Username** and **Password** configured in **Section 5.5**.

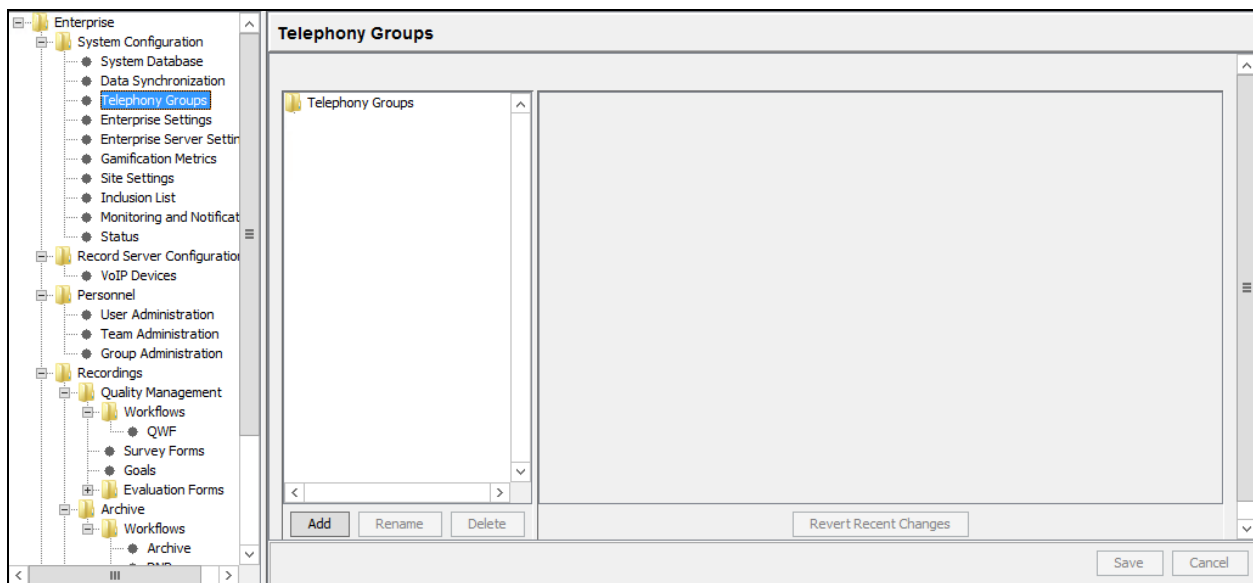
The screenshot shows the 'Data Synchronization' configuration window. On the left is a tree view of the system configuration, with 'Data Synchronization' selected under 'Enterprise > System Configuration'. The main area is titled 'Data Synchronization' and contains three sections:

- AE Services SMS Information:** Includes radio buttons for 'Host Name' and 'IP Address' (selected). The 'IP Address' field contains '10.10.1.4'. The 'Virtual Extension Prefix' field contains 'DMCC'. There is an unchecked checkbox for 'Synchronize Agents'.
- Avaya Communication Manager Information:** Includes radio buttons for 'Host Name' and 'IP Address' (selected). The 'IP Address' field contains '10.10.1.6'. The 'Username' field contains 'calabrio'. The 'Password' field is masked with dots. There is an unchecked checkbox for 'Enable CMS'.
- Avaya Call Management System (CMS) Information:** Includes radio buttons for 'Host Name' and 'IP Address' (selected). The 'IP Address' field is empty. The 'Username' field is empty. The 'Password' field is empty. The 'Time Zone' dropdown menu is set to 'Africa/Abidjan'.

At the bottom of the main area are 'Add', 'Rename', and 'Delete' buttons. At the bottom right of the window are 'Save' and 'Cancel' buttons.

7.2. Configuration of the Application Enablement Interfaces – DMCC

From the left pane, navigate to **Enterprise → System Configuration → Telephony Groups**. The **Telephony Groups** screen is displayed. Click the **Add** button. In the **Telephony Group Configuration** window that pops up (not shown), enter a **Name** and select **Avaya** as the **Telephony Group Type**. Click **OK**.



The **Avaya Configuration** screen is displayed. In the **AE Services DMCC Information** section, provide:

- **Host Name** or **IP Address** of the **Application Enablement Services** server.
- **Username** and **Password** (from **Section 6.2**).
- **4721** as the **Port** (the default DMCC listening port).
- **Device Password** for the recorded stations (from **Section 5.6**). Note that all station passwords must be the same for this solution; however, check with Calabrio for alternatives if necessary.
- **Switch Name** or **Switch IP Interface**. Enter the switch name or IP address of Communication Manager.

Click **OK** to complete this step.

The screenshot shows the Avaya Configuration interface. On the left is a tree view with categories like Enterprise, System Configuration, Record Server Configuration, and Interface Configuration. The main area is titled 'Telephony Groups' and shows a configuration for a group named 'TG1'. A modal window titled 'AE Services DMCC Information' is open in the foreground. This modal has two tabs: 'Host Name' and 'IP Address', with 'IP Address' selected. It contains the following fields: IP Address (10.10.1.4), Username (calabrio), Password (masked with dots), Port (4721), and Switch IP Interface (10.10.1.6). There are 'OK' and 'Cancel' buttons at the bottom of the modal. In the background, the 'Telephony Groups' window shows fields for Name (TG1), Telephony Group Type (Avaya), and several buttons like CDR Configuration, Filters, ACD, and Set Associated ACD. Below these are sections for AE Services DMCC Information and AE Services, with a list containing '10.10.1.4' and buttons for Add, Edit, and Remove. Other settings like Use Device Extension, Device Password, Enable Free Seating, and Recording Skill Hunt Group Extension are also visible.

7.3. Configuration of Users

Navigate to **Enterprise → Personnel → User Administration** page to configure users. Once created, users can be statically assigned to a VoIP Device as demonstrated in **Section 7.4**.

The screenshot shows the 'User Administration' window. On the left is a tree view with 'Enterprise' expanded, showing 'System Configuration', 'Record Server Configuration', 'Personnel' (with 'User Administration' selected), 'Recordings', and 'Interface Configuration'. The main area has tabs for 'Create User', 'License Users', and 'Delete User'. Below these are input fields for 'Last Name', 'First Name', 'ACD', 'Group', 'Team', 'Windows Username', and 'Extension'. A 'Number Licensed Users: 6' indicator is present. A table titled 'Configured Users' lists users with columns: License, Last Name, First Name, User ID, ACD Source, Assigned Team, Assigned Group, Windows Username, and Top A. The table contains 7 rows of data, including 'agent1' through 'agent6' and a 'manager' user. Below the table are 'User Properties' fields for 'License', 'First Name', and 'Last Name', and 'Roles' checkboxes for 'Agent', 'Supervisor', 'Evaluator', and 'Manager'. There are also sections for 'Supervisor's ACD Teams', 'Supervisor's QM Teams', and 'Evaluator's Teams'.

License	Last Name	First Name	User ID	ACD Source	Assigned Team	Assigned Group	Windows Username	Top A
AQM	user	agent1	0.2		DNR		agent1	
AQM	user	agent2	0.3		Team1	Group1	agent2	
AQM	user	agent4	0.4		Team1	Group1	agent4	
AQM	user	agent5	0.5		Team1	Group1	agent5	
AQM	user	agent6	0.6		Team1	Group1	agent6	
AQM	user	manager	0.7				manager	
Unlicensed	Administrator		0.1				administrator	System

Click **Create User** to create a new user. A **Create User** window pops up. Enter the **First Name**, **Last Name**, **Windows Username**, and **QM Password**. Click **OK**.

Note: CRQM also automatically populates the Agent list under the **Agent** tab based upon the agents configured in Communication Manager. The administrator can edit an agent using the **Edit User** button as an alternative way to create a user.

If Screen Recording is required for a user, the **Windows Login** and **QM Password** configured for the user have to match the login and password of the PC that the user uses.

This screenshot shows the 'User Administration' window with the 'Create User' dialog box open in the foreground. The dialog box has fields for 'First Name', 'Last Name', 'Windows Username', 'QM Password', and 'Confirm Password', along with 'OK' and 'Cancel' buttons. The background window shows the same 'Configured Users' table as the previous screenshot, with the 'Create User' button highlighted.

The user appears in the list. Check one of the checkboxes (e.g. Knowledge Worker) under the **Roles** section and select a pre-configured team from the dropdown list of the **Assigned Team** field.

The screenshot shows the 'User Administration' window. On the left is a tree view with 'Enterprise' as the root, containing 'System Configuration', 'Record Server Configuration', 'Personnel', 'Recordings', 'Interface Configuration', 'Role Permissions', 'Interface Settings', and 'Recording Columns'. 'Personnel' is expanded, showing 'User Administration' (selected), 'Team Administration', and 'Group Administration'. The main area has a search bar with fields for 'Last Name', 'First Name', 'ACD', 'Group', 'Team', 'Windows Username', and 'Extension'. Below the search bar are tabs: 'Configured Users', 'Managers', 'Evaluators', 'Archive Users', 'Supervisors', 'Agents', 'Knowledge Worker', 'Not Configured Users', 'Unassigned Users', 'Administrators', and 'Search'. The 'Configured Users' tab is active, displaying a table of users. Below the table is the 'User Properties' section, which includes fields for 'License', 'First Name', 'Last Name', 'Assigned Team' (a dropdown menu), and 'User ID'. To the right of these fields is a 'Roles' section with checkboxes for 'Knowledge Worker', 'Supervisor', 'Evaluator', 'Manager', 'Archive User', and 'Administrator'. Further right are sections for 'Supervisor's ACD Teams', 'Supervisor's QM Teams', and 'Evaluator's Teams'.

License	Last Name	First Name	User ID	ACD Source	Assigned Team	Assigned Group	Windows Username	To
AQM	user	agent1	0.2		DNR		agent1	
AQM	user	agent2	0.3		Team1	Group1	agent2	
AQM	user	agent4	0.4		Team1	Group1	agent4	
AQM	user	agent5	0.5		Team1	Group1	agent5	
AQM	user	agent6	0.6		Team1	Group1	agent6	
AQM	user	manager	0.7				manager	
Unlicensed	Administrator		0.1				administrator	Sys

Click the **License Users** button at the top to display the **Licensed/Unlicense Users** window. Use the **AQM** and **Unlicensed** buttons to set the license mode.

The screenshot shows the 'License/Unlicense Users' window. It has a title bar with a maximize button, a close button, and the text 'License/Unlicense Users'. The window contains a table with columns: 'AQM', 'Unlicensed', 'Last Name', 'First Name', 'Team', and 'Windows Username'. Below the table are two buttons: 'AQM' and 'Unlicensed'. At the bottom are 'OK' and 'Cancel' buttons.

AQM	Unlicensed	Last Name	First Name	Team	Windows Username
<input checked="" type="radio"/>	<input type="radio"/>	user	agent1	DNR	agent1
<input checked="" type="radio"/>	<input type="radio"/>	user	agent2	Team1	agent2
<input checked="" type="radio"/>	<input type="radio"/>	user	agent4	Team1	agent4
<input checked="" type="radio"/>	<input type="radio"/>	user	agent5	Team1	agent5
<input checked="" type="radio"/>	<input type="radio"/>	user	agent6	Team1	agent6
<input checked="" type="radio"/>	<input type="radio"/>	user	manager		manager
<input type="radio"/>	<input checked="" type="radio"/>	Administrator			administrator

7.4. Configuration of Devices

Navigate to **Enterprise → Record Server Configuration → VoIP Devices** to configure devices.

When the SMS query completes, all stations from Communication Manager are listed on the **VoIP Devices** page. A device is designated to be recorded by assigning a pre-configured **Recording Cluster** (e.g. RC1) on the **VoIP Devices** page, and then assigning an **Agent** to that device using dropdown lists in each column. The agent dropdown list includes the users configured on the **User Administration** page in **Section 7.3** that have the AQM license assigned.

Click Save to complete this step.

VoIP Devices

Agent List Filter: Users assigned to site: All Sites

Device Search: Find devices of type: All Types in telephony group: TG1 where: Device Name matches *

Device Name	Device Type	Telephony Group	Agent	Recording Tones	Signaling Group	Recording Cluster	Recording Type
3302	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3304	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3405	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3313	Avaya SSC Phone	TG1	User Login Required	<input type="checkbox"/>			Single Step Confi
3300	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3305	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3404	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3403	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3301	Avaya Phone	TG1	user, agent1 (agent1)	<input type="checkbox"/>	SG1	RC1	Multiple Registrat
3402	Avaya SSC Phone	TG1	user, agent4 (agent4)	<input type="checkbox"/>	SG1	RC1	Single Step Confi
3406	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3309	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3303	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3312	Avaya Phone	TG1	user, agent5 (agent5)	<input type="checkbox"/>	SG1	RC1	Multiple Registrat
3316	Avaya SSC Phone	TG1	user, agent2 (agent2)	<input type="checkbox"/>	SG1	RC1	Single Step Confi
3401	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3400	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat
3306	Avaya Phone	TG1	User Login Required	<input type="checkbox"/>			Multiple Registrat

Create/Edit Default Hoteling Agents

7.5. Configuration of Recording Schedules (Workflows)

Navigate to the **Recordings → Quality Management → Workflows** page. Click the **New** button to create a Workflow. Enter a name for the new workflow and click **OK**. To assign the workflow to a team, select a team from the **Teams Assigned to Groups** list on the bottom left of the page, and click the **>** button to move that group into the **Assigned Teams** for the workflow.

Click on **Save** (not shown) to complete this step.

The screenshot displays the 'Workflow Administration' interface. On the left is a navigation tree with categories like Enterprise, System Configuration, Record Server Configuration, Personnel, Recordings, Quality Management (selected), and Archive. Under Quality Management, 'Workflows' is highlighted. The main panel is titled 'Workflow Administration' and contains several sections:

- Workflows:** A table with columns 'Name' and 'State'. It lists 'QWF' as 'Active' and 'Default Quality' as 'Inactive'. To the right are buttons for 'New', 'Rename', and 'Delete'.
- Settings:** A section with various options: 'End of Day: Hour: 0 Minutes: 00', 'Enable Screen Recording' (checkbox), 'Immediate Voice Upload' (checkbox), 'Immediate Screen Upload' (checkbox), 'Allow Evaluators to Change Form' (checkbox), and 'Extend Screen Recording (in seconds)' (0).
- Recording Retentions:** A section with five columns: 'Scored', 'Unscored', 'Tagged', 'HR', and 'Training'. Each column has an 'Unlimited' checkbox and a 'Days' dropdown set to '0'.
- Teams Assigned to Groups:** A table with columns 'Id', 'Team', and 'Workflow'.
- Assigned Teams:** A table with columns 'Id' and 'Team'.

Between the 'Teams Assigned to Groups' and 'Assigned Teams' tables are four buttons: '>', '>>', '<', and '<<'. The '>' button is used to move a team from the left list to the right list.

Click the newly created Workflow in the left pane to edit the details of the schedule. For the Compliance Test, the **Inbound** and **Outbound** checkboxes are checked to enable recording for inbound and outbound calls. In addition, the **100% QM Logging** checkbox is checked to enable screen recording. If an **Evaluation Form** is to be used by users reviewing the recordings for this workflow, then select a previously configured Evaluation Form. Configuration of Evaluation Forms is beyond the scope of these Application Notes.

Workflow Administration: QWF

Enterprise

- System Configuration
- Record Server Configuration
- Personnel
- Recordings
 - Quality Management
 - Workflows
 - QWF**
 - Survey Forms
 - Goals
 - Evaluation Forms
 - Archive
 - Metadata
 - Call Events
 - Retention Policies
 - Interface Configuration

Classifier Configuration: QWF

Classifiers

New Rename Delete

Classifier Settings

☒ Record

Evaluation Form %NoApprovalReq ▾

☒ 100% QM Logging

☒ Inbound

☒ Outbound

☐ Don't Record

Numbers Called Number ▾

Called Number

*

Add Remove

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that the interface on Communication Manager to Application Enablement Services is enabled and in **listening** status (use the **status aesvcs interface** command on the Communication Manager SAT).
- Verify that the link between Communication Manager and Application Enablement Services is transmitting and receiving messages (use the **status aesvcs link** command on the SAT).
- Verify that the **Conn State** of the Switch Connection is **talking** (on Application Enablement Services web page, navigate to **Status → Status and Control → Switch Conn Summary**).
- Verify that the **service state** of the CTI link is **established** (use the **status aesvcs cti-link** command on the SAT).
- Verify that CRQM lists all the stations configured in Communication Manager in its VoIP Device table.
- Verify that the Calabrio recording ports are registered in Communication Manager (use the **list registered-ip-stations** command on the SAT).
- Verify the Calabrio server has successfully monitored the agent stations using TSAPI (use the **list monitored-stations** command on the SAT).
- Verify that calls may be successfully completed to and from stations and agents. Verify that the call recordings are accurate and complete.

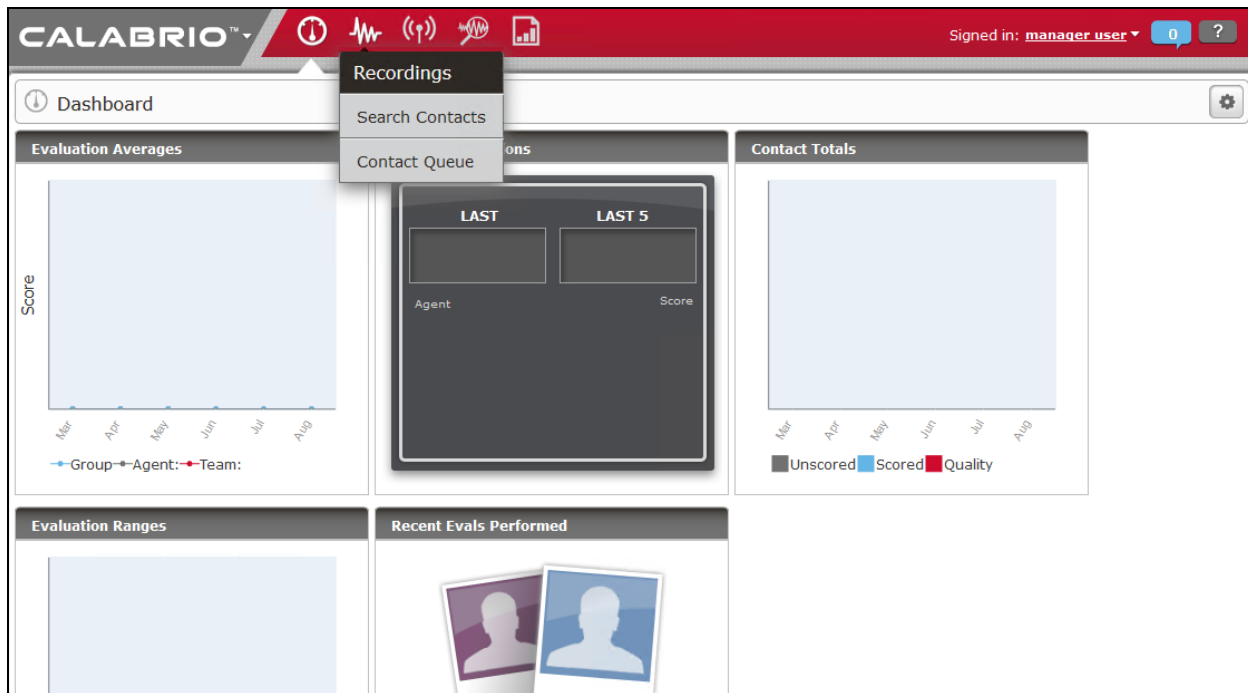
8.1. Verify Recording and Playback

Access the Calabrio web-based user interface using the URL **http://<ip-address>** in a browser window, where **<ip-address>** is the address of the CRQM server. The Log In screen is displayed as shown below. Use appropriate credentials to log in.

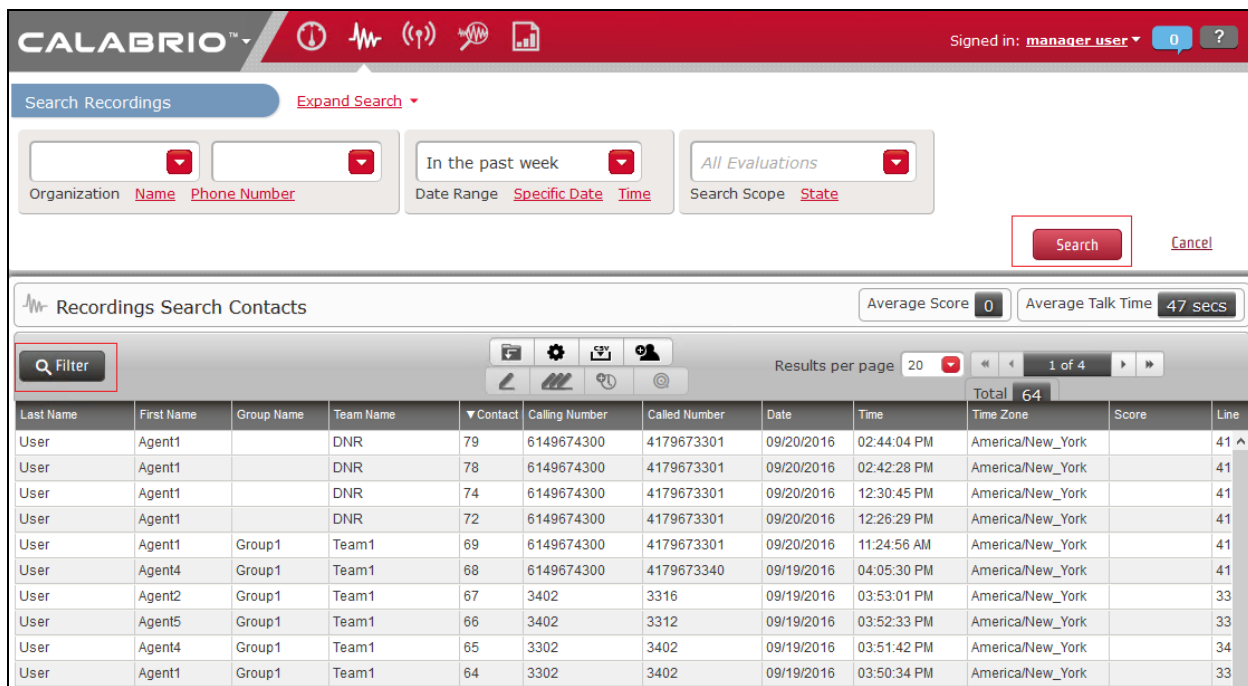


The image shows the Calabrio 1 Log In screen. At the top, the word "CALABRIO" is displayed in a large, bold, sans-serif font, followed by a large, dark, circular button with the number "1" inside. Below this, there is a light gray rectangular box containing the login fields. Inside this box, there are two input fields: "Username" and "Password". Below these fields is a "Language" dropdown menu currently set to "English". At the bottom of the login box, there is a blue link that says "Validate my PC configuration" with a red play button icon next to it, and a red "Log In" button.

Once logged in, launch the **Recording** interface from the Dashboard by clicking the **Recording** icon in the red tool bar to reach the **Recordings** page.



On the **Recording** page, click **Filter**, create search criteria and click **Search** to find recordings.



Select a call of interest and double click to launch a playback window as shown below.

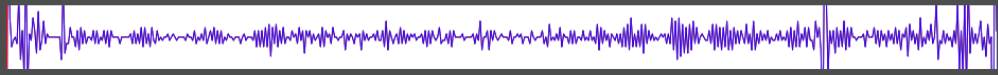
CALABRIO Signed in: manager.user

Recordings Search Contacts Average Score 0 Average Talk Time 47 secs

Filter Results per page 20 1 of 4 Total 64

Last Name	First Name	Group Name	Team Name	Contact ID	Calling Number	Called Number	Date	Time	Time Zone	Score	Line
User	Agent1		DNR	79	6149674300	4179673301	09/20/2016	02:44:04 PM	America/New_York		41
User	Agent1		DNR	78	6149674300	4179673301	09/20/2016	02:42:28 PM	America/New_York		41
User	Agent1		DNR	74	6149674300	4179673301	09/20/2016	12:30:45 PM	America/New_York		41
User	Agent1		DNR	72	6149674300	4179673301	09/20/2016	12:26:29 PM	America/New_York		41
User	Agent1	Group1	Team1	69	6149674300	4179673301	09/20/2016	11:24:56 AM	America/New_York		41
User	Agent4	Group1	Team1	68	6149674300	4179673340	09/19/2016	04:05:30 PM	America/New_York		41
User	Agent2	Group1	Team1	67	3402	3316	09/19/2016	03:53:01 PM	America/New_York		33
User	Agent5	Group1	Team1	66	3402	3312	09/19/2016	03:52:33 PM	America/New_York		33
User	Agent4	Group1	Team1	65	3302	3402	09/19/2016	03:51:42 PM	America/New_York		34
User	Agent1	Group1	Team1	64	3302	3402	09/19/2016	03:50:34 PM	America/New_York		33
User	Agent5	Group1	Team1	63	6149674300	3312	09/19/2016	03:42:21 PM	America/New_York		33
User	Agent4	Group1	Team1	62	3302	3402	09/19/2016	03:41:52 PM	America/New_York		34
User	Agent1	Group1	Team1	61	6149674300	4179673301	09/19/2016	03:40:39 PM	America/New_York		33
User	Agent1	Group1	Team1	60	6149674300	4179673301	09/19/2016	03:34:17 PM	America/New_York		41
User	Agent1	Group1	Team1	59	6149674300	4179673301	09/19/2016	03:33:08 PM	America/New_York		33

Contact Information Associated Contacts

00:00:00  00:00:28

Keep Windows in Focus

9. Conclusion

These Application Notes describe the procedures for configuring Calabrio CRQM 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>.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
2. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.

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

©2017 Avaya Inc. All Rights Reserved.

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

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