



Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio Call Recording and Quality Management with Avaya Aura[®] Communication Manager R6.3 and Avaya Aura[®] Application Enablement Services R6.3 – 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 R6.3 and Avaya Aura[®] Application Enablement Services R6.3.

Calabrio Call Recording and Quality Management (CRQM) uses Avaya Aura[®] Application Enablement Services Device, Media and Call Control (DMCC) 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, using Avaya Aura[®] Application Enablement Services System Management Services (SMS) and Device, Media and Call Control (DMCC) interface.

Before CRQM can start recording, it registers 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 administrator then associates this data with devices to be recorded by the recording application. The recording application uses a static assignment of Call Center agents, and Knowledge Workers, to the station to which they work with.

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 Agent IDs. 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).

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. Audio codec support tested for G.711MU. Common call scenarios including hold/resume, mute/unmute, transfer, and conference at Calabrio side 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 Results

All test cases passed.

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 R6.3
- Avaya Aura® Application Enablement Services R6.3
- Various IP, Digital, and Analog endpoints
- Avaya one-X® Communicator and Avaya one-X® Agent softphones
- Calabrio CRQM server installed on a VMWare virtual machine

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

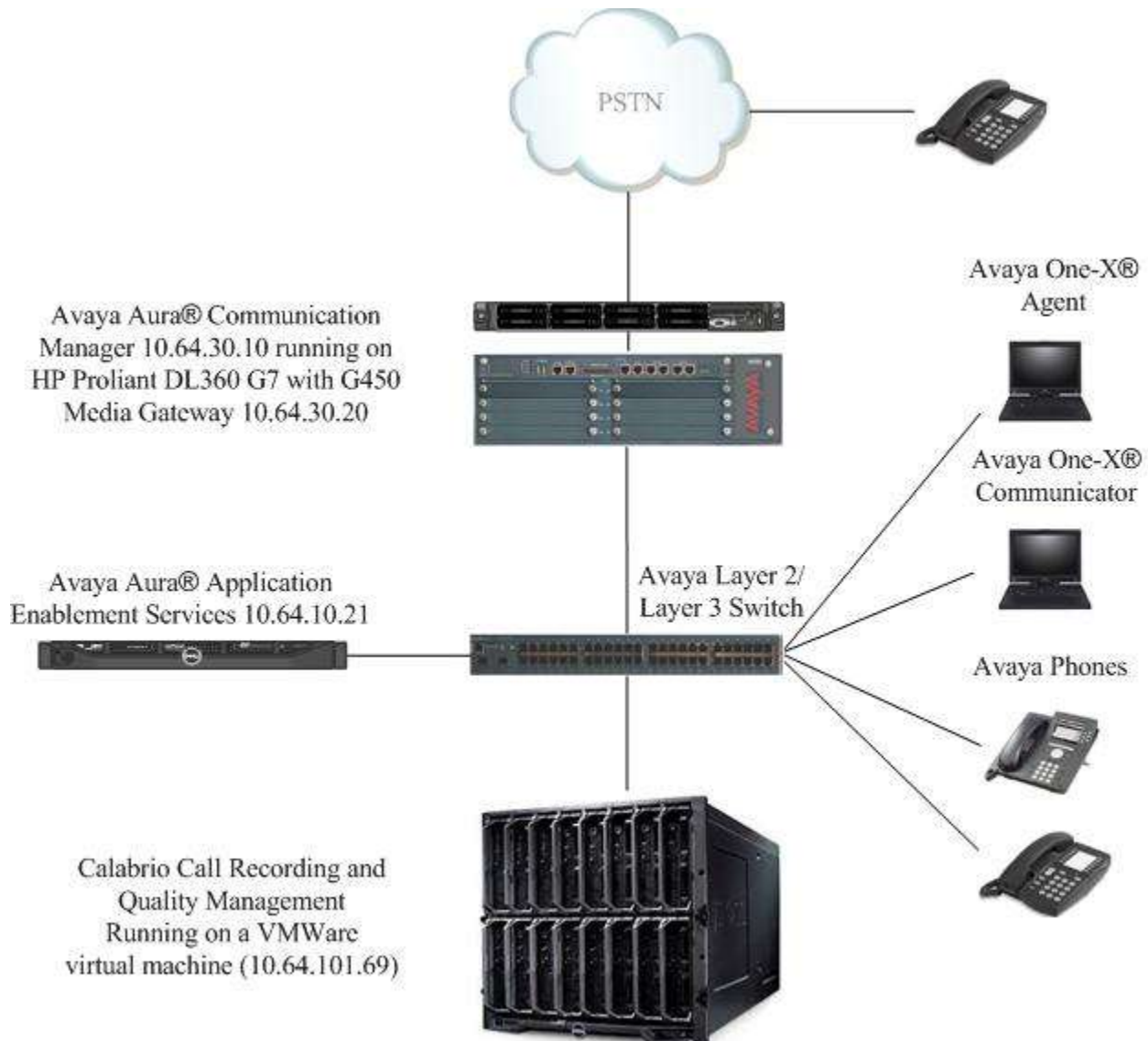


Figure 1 – Calabrio CRQM Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Version
HP Proliant DL360 G7 Server (w/ G450) running Avaya Aura® Communication Manager	6.3 SP112
Avaya G450 Media Gateway <ul style="list-style-type: none">• MGP• MM710AP (DS1)• MM712AP (DCP)• MM711AP (ANA)	HW 1 FW 31.20.0 HW 04 FW 018 HW 07, FW 011 HW 27, FW 073
Dell R610 Server running Avaya Aura® Application Enablement Services	6.3 SP3
Avaya 9600 Series IP Telephone <ul style="list-style-type: none">• 9640 (H.323)	3.2.5
Avaya 96x1 Series IP Telephone <ul style="list-style-type: none">• 9641 (H.323)	6.6.0
Desktop PC running Avaya One-X® Communicator	6.3
Calabrio Recording and Quality Management running under Windows 2012 R2 Server on a VMWare virtual machine	9.3

5. Configure Avaya Aura[®] Communication Manager

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

- 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**.

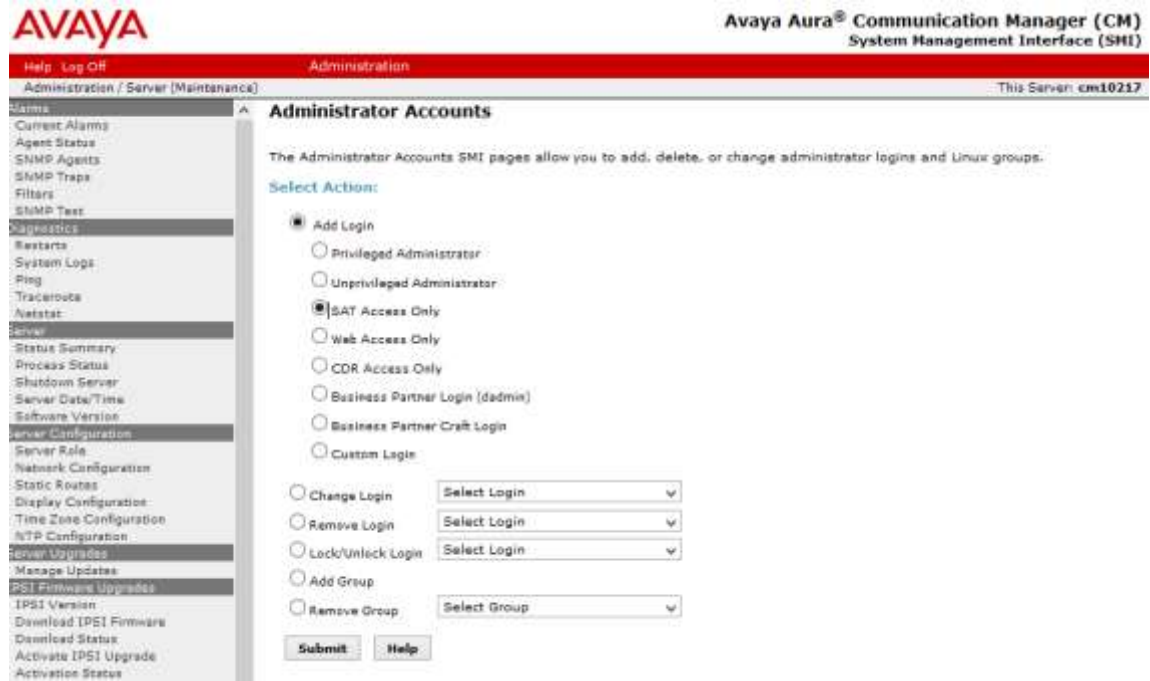
Step	Description																																				
1.	<p data-bbox="297 279 1122 310">Administer IP-Services for Application Enablement Services</p> <p data-bbox="297 312 1357 344">Add an IP-Services entry for Application Enablement Services as described below:</p> <ul data-bbox="347 352 1422 646" style="list-style-type: none"> • 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. <pre data-bbox="297 680 1433 705">change ip-services Page 1 of 4</pre> <table border="1" data-bbox="297 732 1433 846"> <thead> <tr> <th colspan="7">IP SERVICES</th> </tr> <tr> <th>Service Type</th> <th>Enabled</th> <th>Local Node</th> <th>Local Port</th> <th>Remote Node</th> <th>Remote Port</th> <th></th> </tr> </thead> <tbody> <tr> <td>AESVCS</td> <td>y</td> <td>procr</td> <td>8765</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p data-bbox="297 877 1089 909">On Page 4 of the IP Services form, enter the following values:</p> <ul data-bbox="347 917 1321 1098" style="list-style-type: none"> • 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, Step 1. • In the Enabled field, type y. <pre data-bbox="297 1129 1433 1155">change ip-services Page 4 of 4</pre> <table border="1" data-bbox="297 1157 1433 1293"> <thead> <tr> <th colspan="5">AE Services Administration</th> </tr> <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>aes10210</td> <td>xxxxxxx</td> <td>y</td> <td></td> </tr> </tbody> </table>	IP SERVICES							Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		AESVCS	y	procr	8765				AE Services Administration					Server ID	AE Services Server	Password	Enabled	Status	1:	aes10210	xxxxxxx	y	
IP SERVICES																																					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																																
AESVCS	y	procr	8765																																		
AE Services Administration																																					
Server ID	AE Services Server	Password	Enabled	Status																																	
1:	aes10210	xxxxxxx	y																																		

Step	Description
2.	<p>Administer Computer Telephony Integration (CTI) Link Enter the add cti-link <link number> command, where <link number> is an available CTI link number.</p> <ul style="list-style-type: none"> • In the Extension field, type a valid station extension. • In the Type field, type ADJ-IP. • In the Name field, type a descriptive name. <pre> add cti-link 1 CTI LINK CTI Link: 1 Extension: 58001 Type: ADJ-IP Name: aes10210 COR: 1 Page 1 of 3 </pre>
3.	<p>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 adding a new user profile, add user-profile-by-category n command can be used to create the profile.</p> <pre> add user-profile-by-category 31 USER PROFILE 31 User Profile Name: Calabrio SMS This Profile is Disabled? n Facility Test Call Notification? n Grant Un-owned Permissions? n Shell Access? y Acknowledgement Required? n Extended Profile? n Name Cat Enbl Adjuncts A n Call Center B y Features C n Hardware D n Hospitality E n IP F n Maintenance G n Measurements and Performance H n Remote Access I n Name Cat Enbl Routing and Dial Plan J n Security K n Servers L n Stations M y System Parameters N n Translations O n Trunking P n Usage Q n User Access R n </pre>

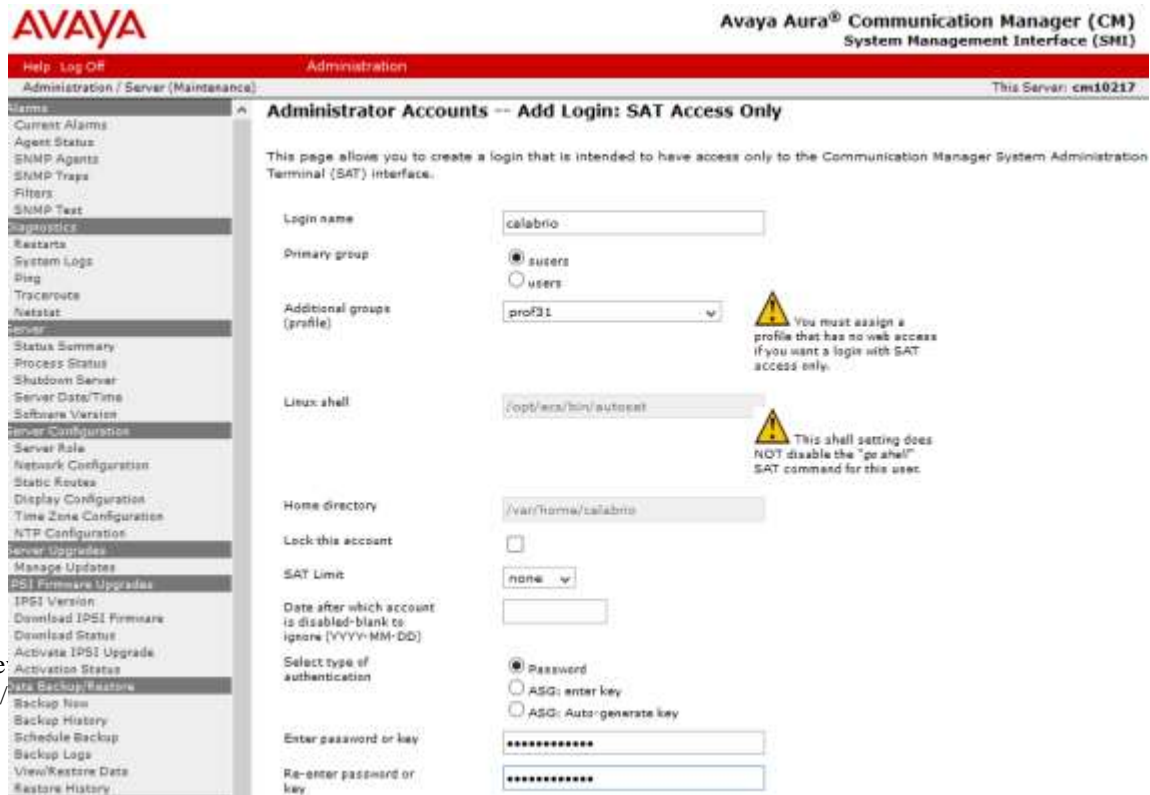
Step	Description																																																
	<p>Add SMS User Account (Continued) Read only access to Agents and Stations is required. Enter r- permissions for the B and M Categories on the Set Permissions for Category: entry on the change user-profile-by-category xx form. This requires two separate transactions, so repeat for each category.</p>																																																
	<p>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</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Cat</th> <th>Perm</th> </tr> </thead> <tbody> <tr><td>agent</td><td>B</td><td>r-</td></tr> <tr><td>agent-loginID</td><td>B</td><td>r-</td></tr> <tr><td>announcements</td><td>B</td><td>r-</td></tr> <tr><td>bcms agent</td><td>B</td><td>r-</td></tr> <tr><td>bcms skill/split</td><td>B</td><td>r-</td></tr> <tr><td>bcms summary agent</td><td>B</td><td>r-</td></tr> <tr><td>bcms summary skill/split</td><td>B</td><td>r-</td></tr> <tr><td>bcms summary trunk</td><td>B</td><td>r-</td></tr> <tr><td>bcms summary vdn</td><td>B</td><td>r-</td></tr> <tr><td>bcms system</td><td>B</td><td>r-</td></tr> <tr><td>bcms trunk</td><td>B</td><td>r-</td></tr> <tr><td>bcms vdn</td><td>B</td><td>r-</td></tr> <tr><td>best-service-routing</td><td>B</td><td>r-</td></tr> <tr><td>bcms-vustats loginIDs</td><td>B</td><td>r-</td></tr> <tr><td>crm-features</td><td>B</td><td>r-</td></tr> </tbody> </table>	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-
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-																																															
	<p>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</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Cat</th> <th>Perm</th> </tr> </thead> <tbody> <tr><td>ess</td><td>L</td><td>--</td></tr> <tr><td>ess clusters</td><td>L</td><td>--</td></tr> <tr><td>ess port-networks</td><td>L</td><td>--</td></tr> <tr><td>lsp</td><td>L</td><td>--</td></tr> <tr><td>remote-office</td><td>L</td><td>--</td></tr> <tr><td>alias station</td><td>M</td><td>r-</td></tr> <tr><td>attendant</td><td>M</td><td>r-</td></tr> <tr><td>bridged-extensions</td><td>M</td><td>r-</td></tr> <tr><td>coverage answer-group</td><td>M</td><td>r-</td></tr> <tr><td>button-location-aca</td><td>M</td><td>r-</td></tr> <tr><td>button-restriction</td><td>M</td><td>r-</td></tr> <tr><td>call-forwarding</td><td>M</td><td>r-</td></tr> <tr><td>console-parameters</td><td>M</td><td>r-</td></tr> <tr><td>coverage answer-group</td><td>M</td><td>r-</td></tr> <tr><td>coverage path</td><td>M</td><td>r-</td></tr> </tbody> </table>	Name	Cat	Perm	ess	L	--	ess clusters	L	--	ess port-networks	L	--	lsp	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-
Name	Cat	Perm																																															
ess	L	--																																															
ess clusters	L	--																																															
ess port-networks	L	--																																															
lsp	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-																																															

Step	Description
------	-------------

Add SMS User Account (Continued)
 Create a user account on the Communication Manager **System Management Interface** web page by navigating to the **Administer Accounts** page and selecting the radio button **Add Login** and **SAT Access Only**. Click **Submit** to continue the process.



The **Add Login** screen is displayed. Enter a name to the **Login name** field and select the profile defined in **Step 5 (prof31)** in the **Additional groups (profile)** field. Select **Password** for the **Select type of authentication** field and enter a **Password**.



KJA; Re
 SPOC 1/

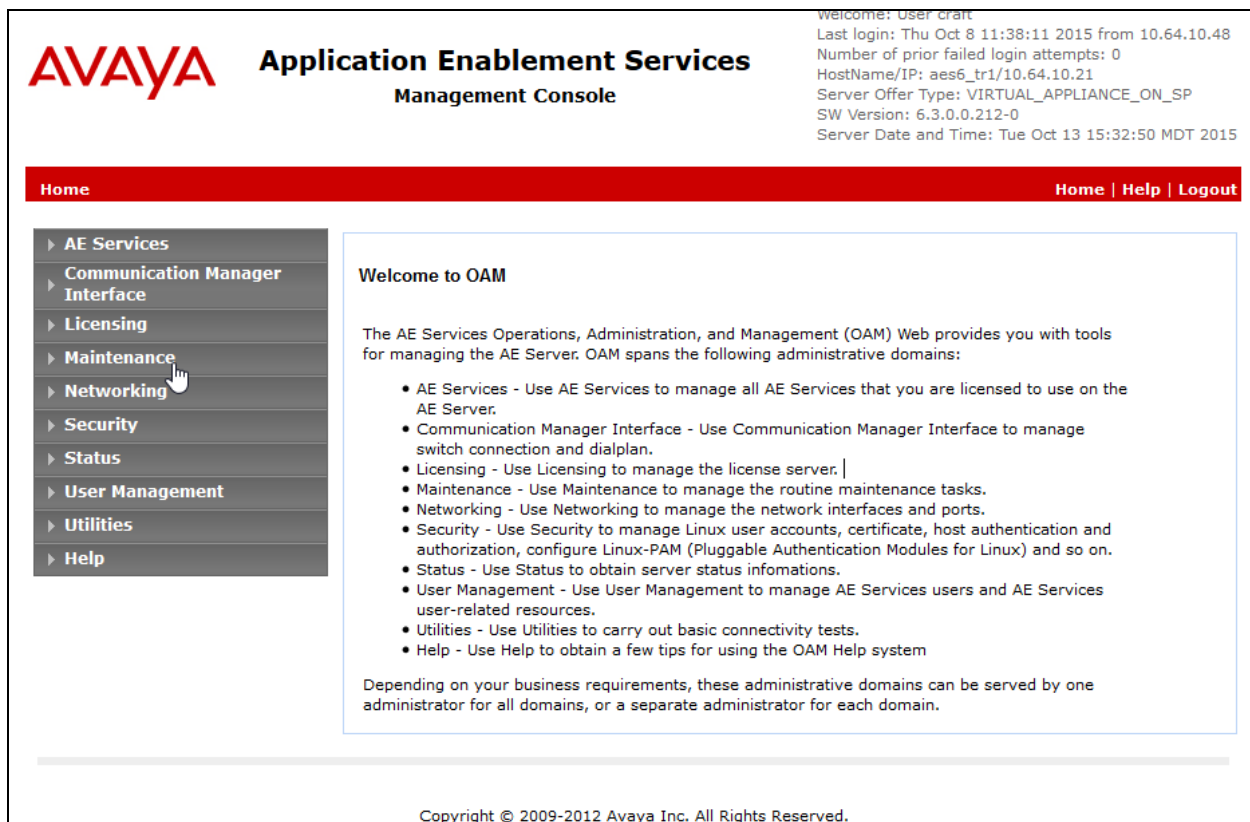
Step	Description
4.	<p data-bbox="297 237 542 268">Verify Extensions</p> <p data-bbox="297 273 1406 485">All stations that will be recorded using the Multiple Registration method must have IP Softphone enabled, and the application needs to know the Security Code in order to successfully register. For stations that are unable to support Softphone, or which the administrator prefers to record using Single Step Conference, leave the IP Softphone setting disabled. Use the display station n command to verify information, or change station n to make changes if necessary.</p> <pre data-bbox="297 527 1435 1121"> display station 53001 Page 1 of 5 STATION Extension: 53001 Lock Messages? n BCC: 0 Type: 9608 Security Code: 123456 TN: 1 Port: S00000 Coverage Path 1: 98 COR: 1 Name: 53001, Station 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: 53001 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 </pre>

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
- Add TSAPI Links
- Note the TLink Information
- Configure Calabrio User
- Enable Unrestricted Access for Calabrio User



AVAYA Application Enablement Services Management Console

welcome: User craft
Last login: Thu Oct 8 11:38:11 2015 from 10.64.10.48
Number of prior failed login attempts: 0
HostName/IP: aes6_tr1/10.64.10.21
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Oct 13 15:32:50 MDT 2015

Home Home | Help | Logout

Navigation Panel:

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

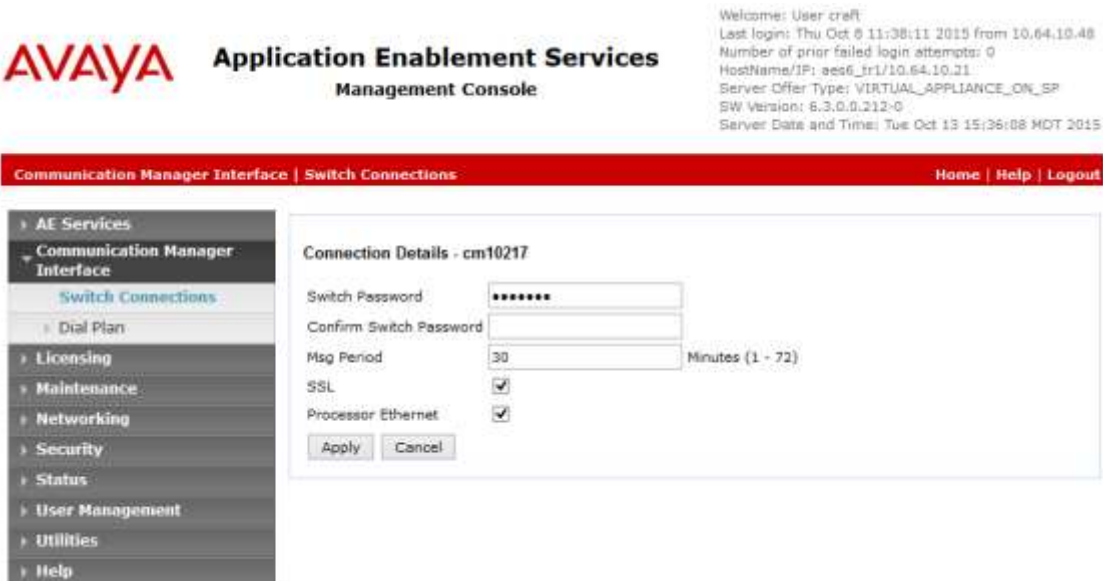
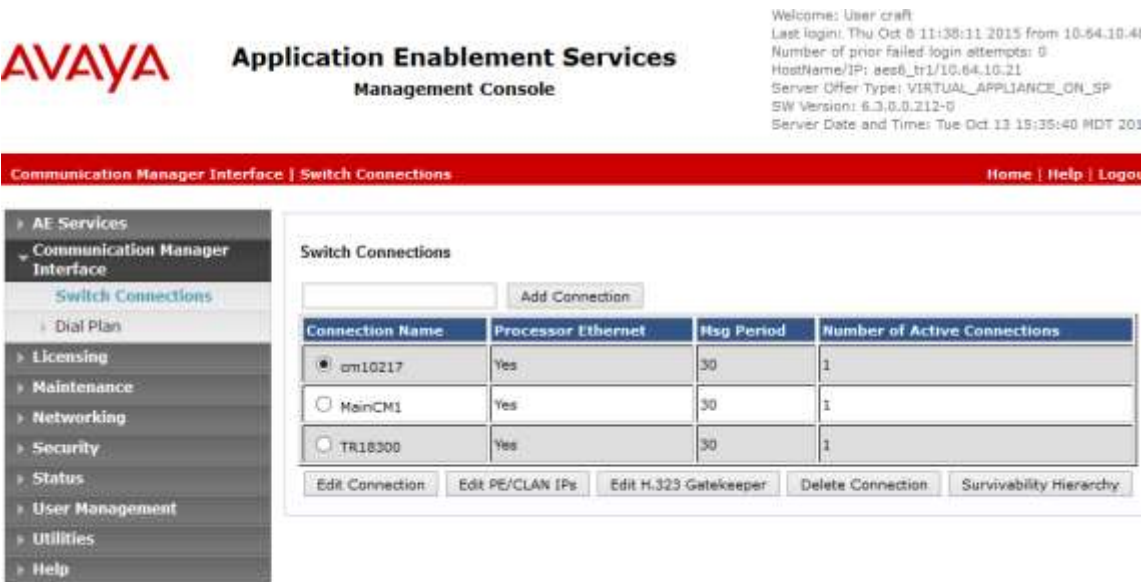
Welcome to OAM


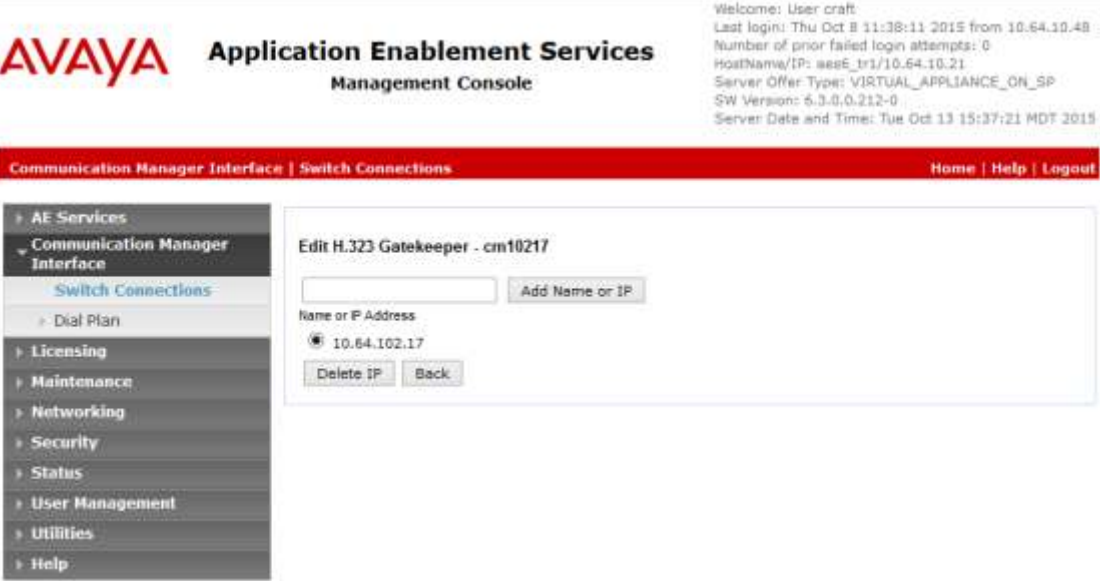
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

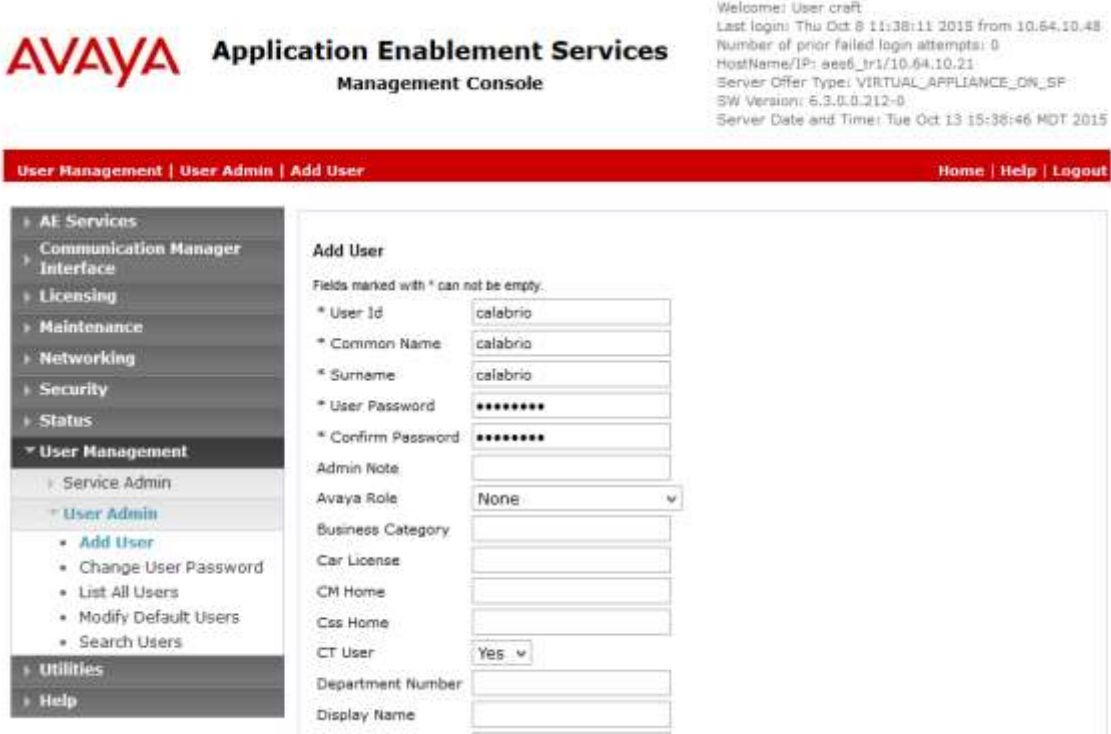
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server. |
- Maintenance - Use Maintenance 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.

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

Step	Description
<p>1.</p>	<p>Configure Communication Manager Switch Connections</p> <p>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. cm10217) and click the Add Connection button (not shown). The Connection Details screen is shown. Enter the Switch Password configured in Section 5, Step 3 and check the Processor Ethernet box if using the procr interface. Click Apply.</p>  <p>The display returns to the Switch Connections screen which shows that the cm10217 switch connection has been added.</p> 

Step	Description				
	<p data-bbox="297 233 1433 411">Configure Communication Manager Switch Connections (Continued) Click the Edit PE/CLAN IPs button on the Switch Connections screen to configure the procr or CLAN IP Address(es) for TSAPI message traffic. 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.</p> <div data-bbox="321 453 1414 1031">  <p data-bbox="1031 453 1414 579">Welcome: User craft Last login: Thu Oct 8 11:38:11 2015 from 10.64.10.48 Number of prior failed login attempts: 0 HostName/IP: aes6_tr1/10.64.10.21 Server Offer Type: VIRTUAL_APPLIANCE_ON_SP SW Version: 6.3.0.0.212-0 Server Date and Time: Tue Oct 13 15:36:53 MDT 2015</p> <p data-bbox="329 611 1409 632">Communication Manager Interface Switch Connections Home Help Logout</p> <p data-bbox="329 657 591 1024"> <ul style="list-style-type: none"> > AE Services > Communication Manager Interface <li style="background-color: #f0f0f0;">Switch Connections > Dial Plan > Licensing > Maintenance > Networking > Security > Status > User Management > Utilities > Help </p> <p data-bbox="618 684 898 705">Edit Processor Ethernet IP - cm10217</p> <p data-bbox="618 730 987 751"><input type="text"/> Add/Edit Name or IP</p> <table border="1" data-bbox="618 758 1393 821"> <thead> <tr> <th>Name or IP Address</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>10.64.102.17</td> <td>In Use</td> </tr> </tbody> </table> <p data-bbox="618 827 678 848">Back</p> </div> <p data-bbox="297 1073 1433 1213">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.</p> <div data-bbox="321 1262 1414 1839">  <p data-bbox="1031 1262 1414 1388">Welcome: User craft Last login: Thu Oct 8 11:38:11 2015 from 10.64.10.48 Number of prior failed login attempts: 0 HostName/IP: aes6_tr1/10.64.10.21 Server Offer Type: VIRTUAL_APPLIANCE_ON_SP SW Version: 6.3.0.0.212-0 Server Date and Time: Tue Oct 13 15:37:21 MDT 2015</p> <p data-bbox="329 1419 1409 1440">Communication Manager Interface Switch Connections Home Help Logout</p> <p data-bbox="329 1465 591 1833"> <ul style="list-style-type: none"> > AE Services > Communication Manager Interface <li style="background-color: #f0f0f0;">Switch Connections > Dial Plan > Licensing > Maintenance > Networking > Security > Status > User Management > Utilities > Help </p> <p data-bbox="618 1497 865 1518">Edit H.323 Gatekeeper - cm10217</p> <p data-bbox="618 1543 959 1564"><input type="text"/> Add Name or IP</p> <p data-bbox="618 1570 735 1591">Name or IP Address</p> <p data-bbox="618 1598 743 1619"> <input checked="" type="radio"/> 10.64.102.17 </p> <p data-bbox="618 1625 776 1646">Delete IP Back</p> </div>	Name or IP Address	Status	10.64.102.17	In Use
Name or IP Address	Status				
10.64.102.17	In Use				

Step	Description
<p data-bbox="201 237 233 268">2.</p>	<p data-bbox="298 237 634 268">Configure Calabrio user</p> <p data-bbox="298 275 1406 380">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.</p> <p data-bbox="298 422 1040 453">Click Apply at the bottom of the pages to save the entries.</p>  <p>The screenshot shows the Avaya Application Enablement Services Management Console. At the top right, there is a welcome message for 'User craft' with system information including the last login time (Thu Oct 8 11:38:11 2015), number of failed login attempts (0), host name/IP (aee6_tr1/10.64.10.21), server offer type (VIRTUAL_APPLIANCE_ON_SF), SW version (6.3.0.0.212-0), and server date and time (Tue Oct 13 15:36:46 MDT 2015). Below this is a red navigation bar with 'User Management User Admin Add User' and links for 'Home Help Logout'. On the left is a navigation tree with 'User Management' expanded to 'User Admin' and 'Add User' selected. The main content area is the 'Add User' form, which has a note that fields marked with an asterisk are required. The form contains the following fields: <ul style="list-style-type: none"> * User Id: calabrio * Common Name: calabrio * Surname: calabrio * User Password: masked with asterisks * Confirm Password: masked with asterisks Admin Note: empty text area Avaya Role: dropdown menu set to 'None' Business Category: empty text area Car License: empty text area CM Home: empty text area Cms Home: empty text area CT User: dropdown menu set to 'Yes' Department Number: empty text area Display Name: empty text area </p>

Step	Description
------	-------------

3. Enable Unrestricted Access for Calabrio User

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 **cala** user and click **Edit** (not shown).



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.



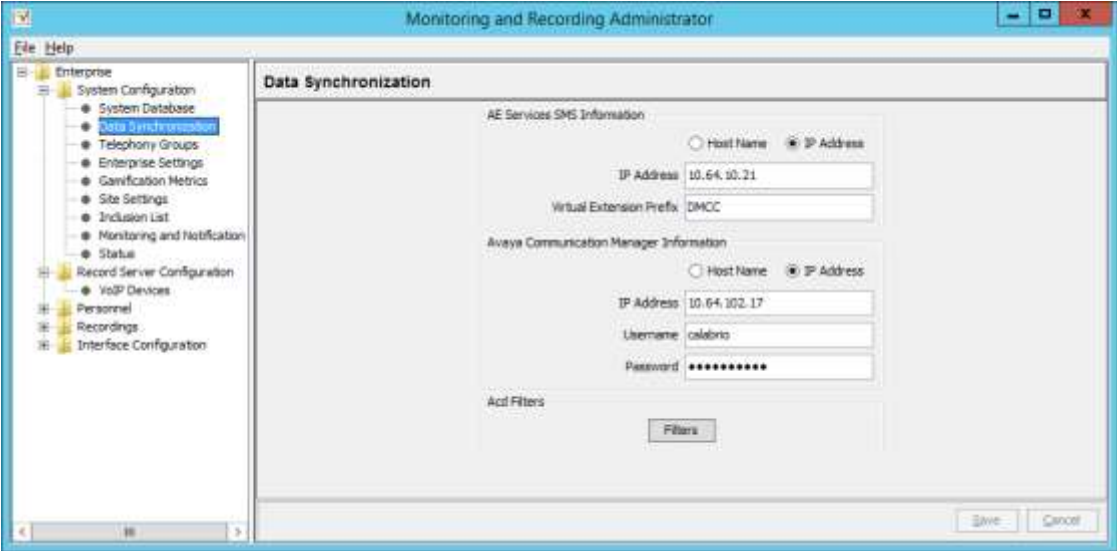
7. Configure Calabrio Call Recording and Quality Management

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.

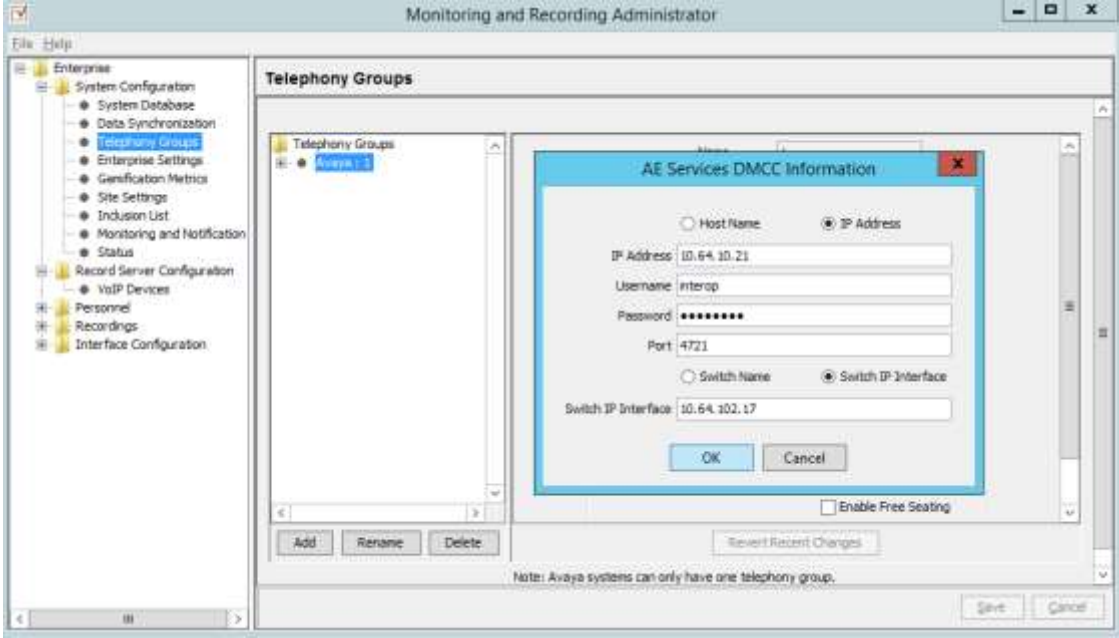
The steps include:

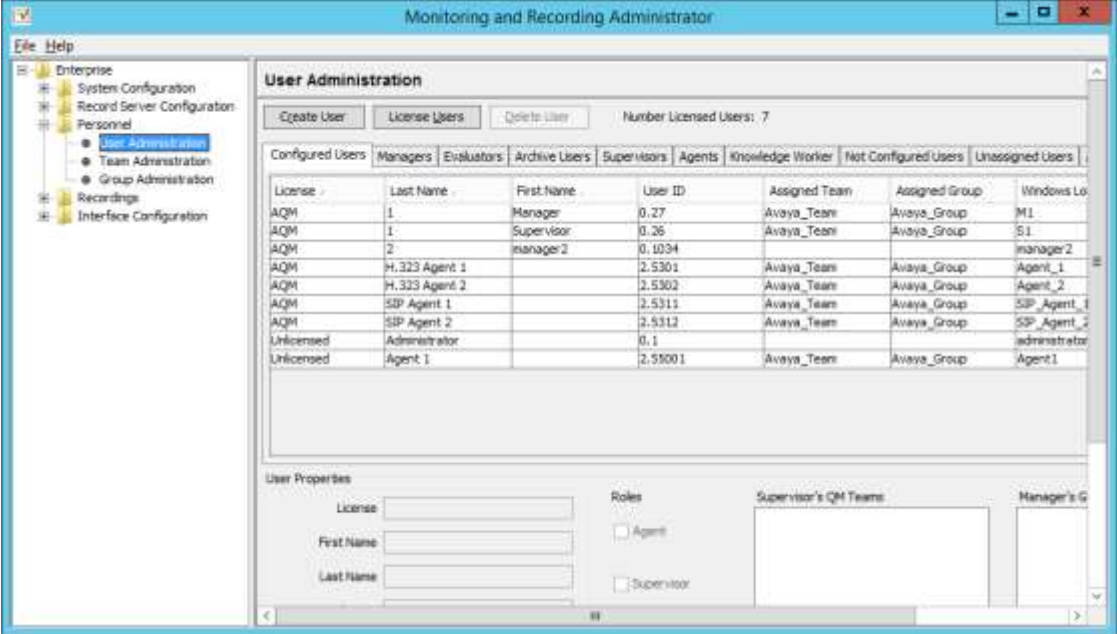
- Configuration of the Application Enablement Interfaces – SMS
- Configuration of the Application Enablement Interfaces – DMCC
- Configuration of Users
- Configuration of Devices
- Configuration of Recording Schedules (Workflows)

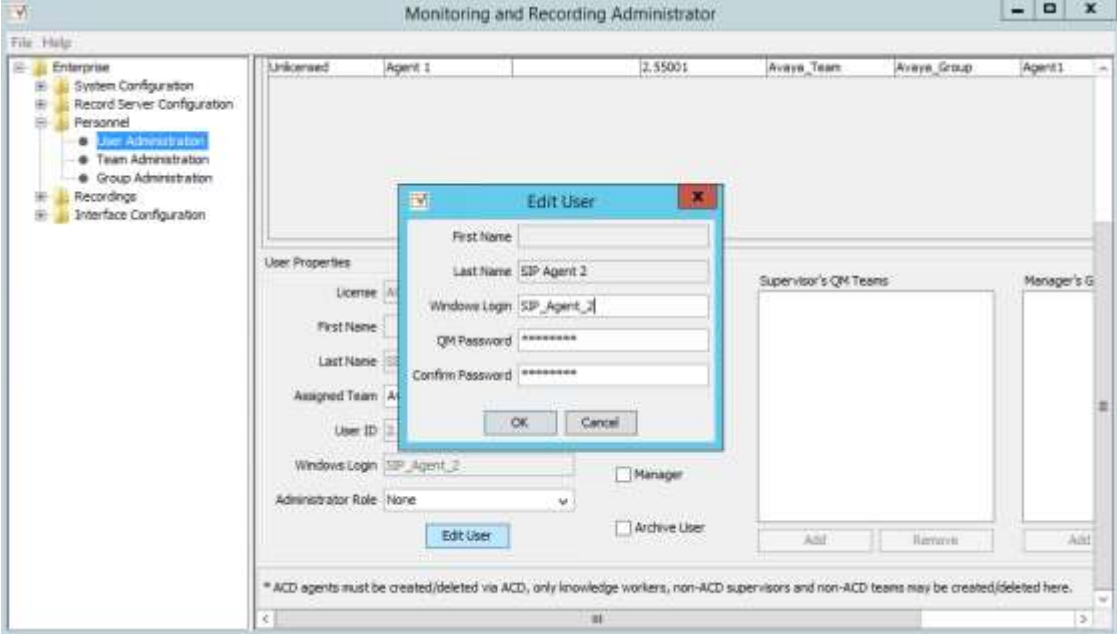
The configuration of the CRQM server is performed using the **Calabrio Monitoring and Recording Administrator** application, which can be launched by clicking **Start → All Programs → Calabrio → Monitoring and Recording Administrator**. Log in with proper credentials.

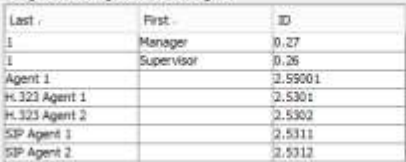
Step	Description
<p data-bbox="201 268 230 298">1.</p>	<p data-bbox="282 268 1143 298">Configuration of the Application Enablement Interfaces – SMS</p> <p data-bbox="282 340 1286 411">From the left pane, navigate to Enterprise → System Configuration → Data Synchronization.</p> <p data-bbox="282 453 1386 625">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, Step 5.</p> 

Step	Description
2.	<p>Configuration of the Application Enablement Interfaces – DMCC and JTAPI</p> <p>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, enter a Name and select Avaya as the Telephony Group Type. Click OK.</p>

Step	Description
	<p>Configuration of the Application Enablement Interfaces – DMCC (Continued) The Avaya Configuration screen is displayed. In the AE Services select Add:</p> <ul style="list-style-type: none"> • Host Name or IP Address of the Application Enablement Services server • Username and Password (from Section 6, Step 4) • 4721 as the port (the default DMCC listening port) • Device Password for the recorded stations (from Section 5, Step 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. <p>Click OK to complete this step.</p> 

Step	Description																																																																						
<p>3.</p>	<p>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 Step 4.</p>  <p>The screenshot displays the 'Monitoring and Recording Administrator' application window. The 'User Administration' section is active, showing a table of configured users. The table has the following data:</p> <table border="1"> <thead> <tr> <th>License</th> <th>Last Name</th> <th>First Name</th> <th>User ID</th> <th>Assigned Team</th> <th>Assigned Group</th> <th>Windows Log</th> </tr> </thead> <tbody> <tr> <td>AQM</td> <td>1</td> <td>Manager</td> <td>0.27</td> <td>Avaya_Team</td> <td>Avaya_Group</td> <td>M1</td> </tr> <tr> <td>AQM</td> <td>1</td> <td>Supervisor</td> <td>0.26</td> <td>Avaya_Team</td> <td>Avaya_Group</td> <td>S1</td> </tr> <tr> <td>AQM</td> <td>2</td> <td>manager2</td> <td>0.1034</td> <td></td> <td></td> <td>manager2</td> </tr> <tr> <td>AQM</td> <td>H.323 Agent 1</td> <td></td> <td>2.5301</td> <td>Avaya_Team</td> <td>Avaya_Group</td> <td>Agent_1</td> </tr> <tr> <td>AQM</td> <td>H.323 Agent 2</td> <td></td> <td>2.5302</td> <td>Avaya_Team</td> <td>Avaya_Group</td> <td>Agent_2</td> </tr> <tr> <td>AQM</td> <td>SIP Agent 1</td> <td></td> <td>2.5311</td> <td>Avaya_Team</td> <td>Avaya_Group</td> <td>SIP_Agent_1</td> </tr> <tr> <td>AQM</td> <td>SIP Agent 2</td> <td></td> <td>2.5312</td> <td>Avaya_Team</td> <td>Avaya_Group</td> <td>SIP_Agent_2</td> </tr> <tr> <td>Unlicensed</td> <td>Administrator</td> <td></td> <td>0.1</td> <td></td> <td></td> <td>administrator</td> </tr> <tr> <td>Unlicensed</td> <td>Agent 1</td> <td></td> <td>2.55001</td> <td>Avaya_Team</td> <td>Avaya_Group</td> <td>Agent1</td> </tr> </tbody> </table> <p>Below the table, the 'User Properties' section includes input fields for License, First Name, and Last Name. There are checkboxes for 'Agent' and 'Supervisor' roles. There are also empty fields for 'Supervisor's QM Teams' and 'Manager's Group'.</p>	License	Last Name	First Name	User ID	Assigned Team	Assigned Group	Windows Log	AQM	1	Manager	0.27	Avaya_Team	Avaya_Group	M1	AQM	1	Supervisor	0.26	Avaya_Team	Avaya_Group	S1	AQM	2	manager2	0.1034			manager2	AQM	H.323 Agent 1		2.5301	Avaya_Team	Avaya_Group	Agent_1	AQM	H.323 Agent 2		2.5302	Avaya_Team	Avaya_Group	Agent_2	AQM	SIP Agent 1		2.5311	Avaya_Team	Avaya_Group	SIP_Agent_1	AQM	SIP Agent 2		2.5312	Avaya_Team	Avaya_Group	SIP_Agent_2	Unlicensed	Administrator		0.1			administrator	Unlicensed	Agent 1		2.55001	Avaya_Team	Avaya_Group	Agent1
License	Last Name	First Name	User ID	Assigned Team	Assigned Group	Windows Log																																																																	
AQM	1	Manager	0.27	Avaya_Team	Avaya_Group	M1																																																																	
AQM	1	Supervisor	0.26	Avaya_Team	Avaya_Group	S1																																																																	
AQM	2	manager2	0.1034			manager2																																																																	
AQM	H.323 Agent 1		2.5301	Avaya_Team	Avaya_Group	Agent_1																																																																	
AQM	H.323 Agent 2		2.5302	Avaya_Team	Avaya_Group	Agent_2																																																																	
AQM	SIP Agent 1		2.5311	Avaya_Team	Avaya_Group	SIP_Agent_1																																																																	
AQM	SIP Agent 2		2.5312	Avaya_Team	Avaya_Group	SIP_Agent_2																																																																	
Unlicensed	Administrator		0.1			administrator																																																																	
Unlicensed	Agent 1		2.55001	Avaya_Team	Avaya_Group	Agent1																																																																	

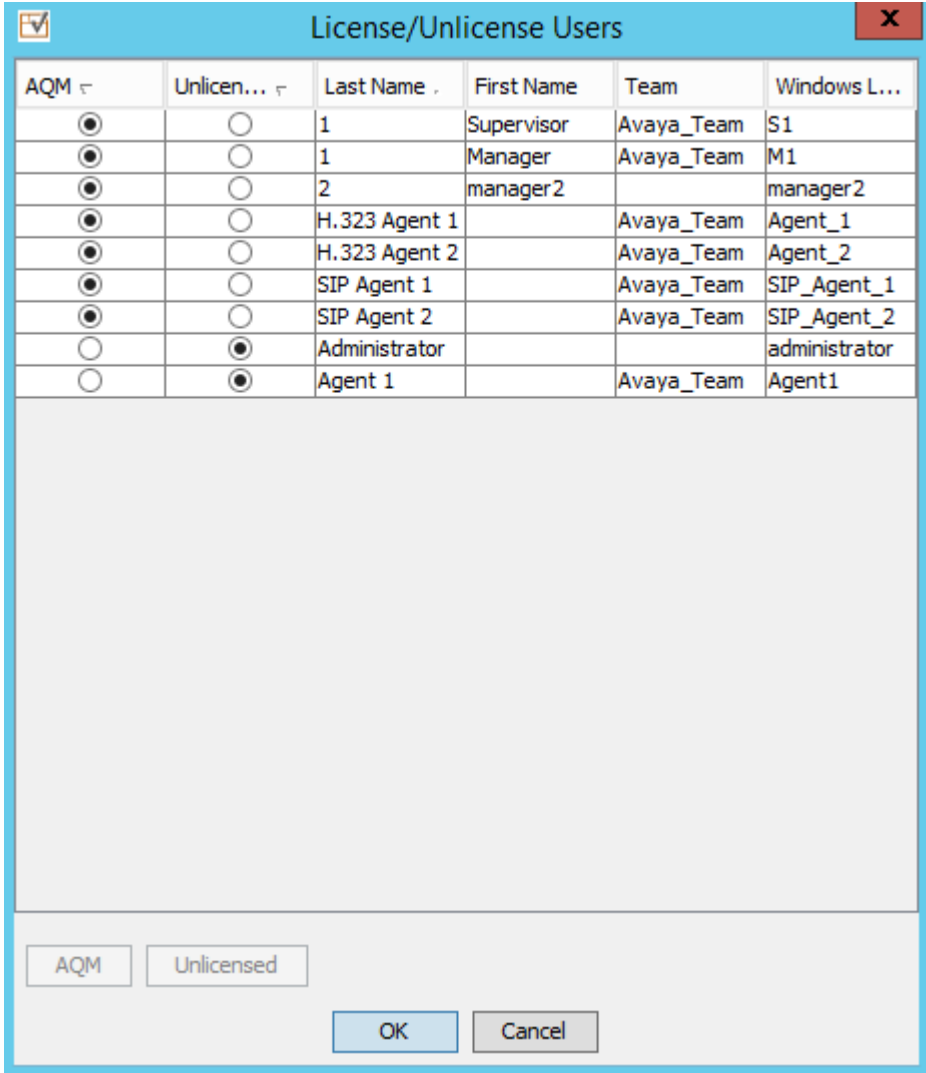
Step	Description
	<p>Configuration of Users (Continued) Clicking Create User to create a new user. A Create User window pops up. Enter the First Name, Last Name, Windows Login, and QM Password. Click OK.</p> <p>Note: CRQM also automatically populates the Agent list under the Agent tab based upon the agents configured in Communication Manager. The administrator can edit an agent using the Edit User button to create a user.</p> 

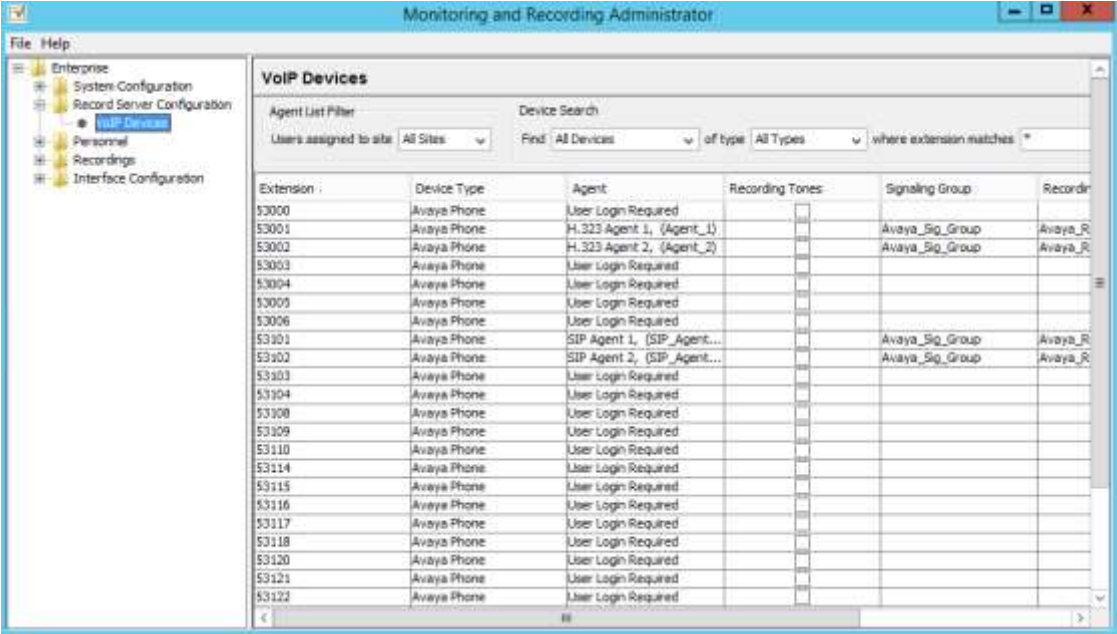
Step	Description																								
	<p data-bbox="280 233 760 264">Configuration of Users (Continued)</p> <p data-bbox="280 268 1349 369">The user appears in the list. Check one of the checkboxes (e.g. Agent) under the Roles section and select a pre-configured team from the dropdown list of the Assigned Team field.</p>  <thead> <tr> <th>Last</th> <th>First</th> <th>ID</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Manager</td> <td>0.27</td> </tr> <tr> <td>1</td> <td>Supervisor</td> <td>0.26</td> </tr> <tr> <td>Agent 1</td> <td></td> <td>2.59001</td> </tr> <tr> <td>H.323 Agent 1</td> <td></td> <td>2.5301</td> </tr> <tr> <td>H.323 Agent 2</td> <td></td> <td>2.5302</td> </tr> <tr> <td>SP Agent 1</td> <td></td> <td>2.5311</td> </tr> <tr> <td>SP Agent 2</td> <td></td> <td>2.5312</td> </tr> </tbody>	Last	First	ID	1	Manager	0.27	1	Supervisor	0.26	Agent 1		2.59001	H.323 Agent 1		2.5301	H.323 Agent 2		2.5302	SP Agent 1		2.5311	SP Agent 2		2.5312
Last	First	ID																							
1	Manager	0.27																							
1	Supervisor	0.26																							
Agent 1		2.59001																							
H.323 Agent 1		2.5301																							
H.323 Agent 2		2.5302																							
SP Agent 1		2.5311																							
SP Agent 2		2.5312																							

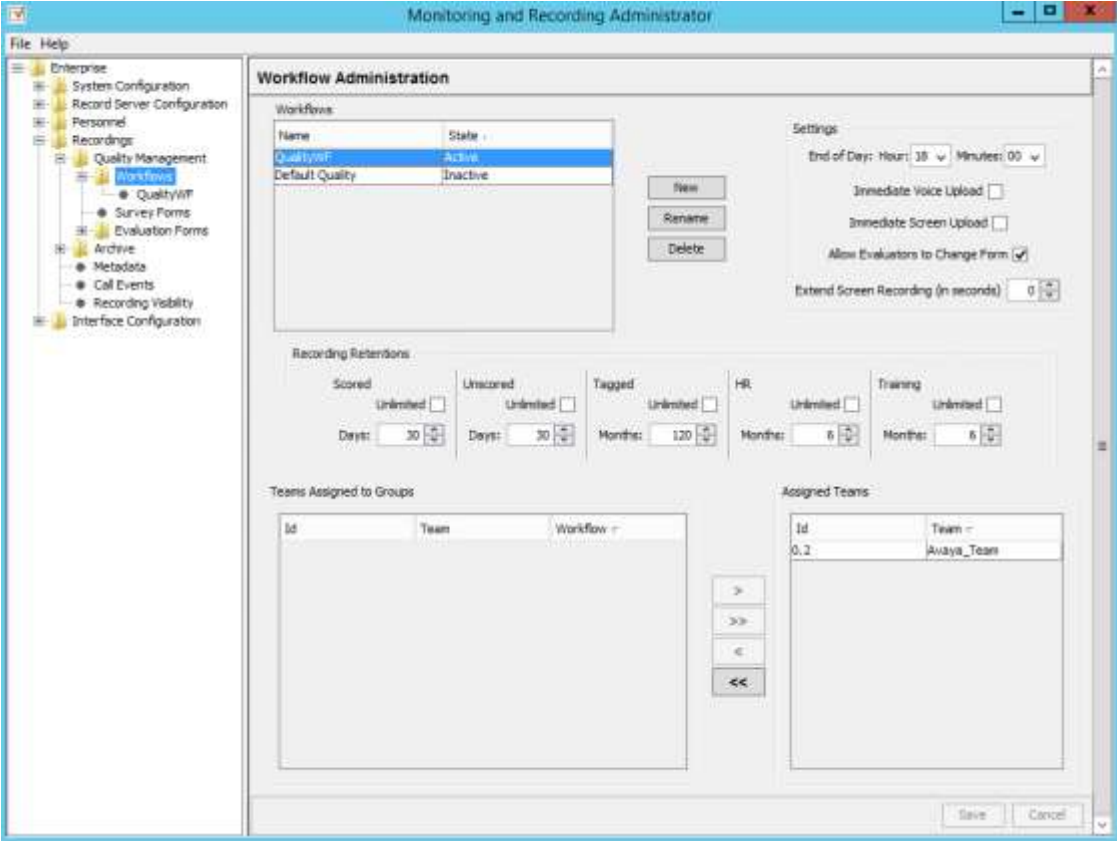
 The 'Assigned ACD Agents with the Supervisor Role' table is empty. The 'Assigned QM Supervisors' table contains the following data:

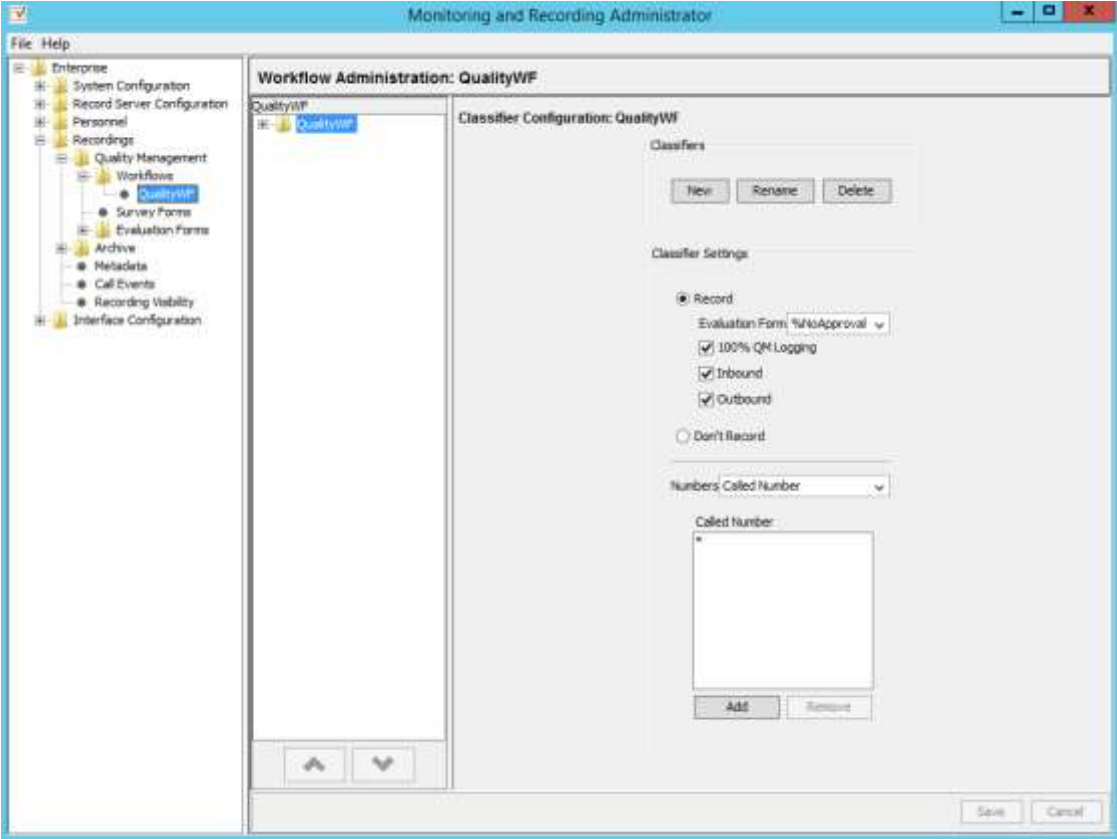
Last	First	ID
1	Manager	0.27

 The interface also includes a left-hand navigation tree with 'Team Administration' selected, and a bottom status bar with 'Add' and 'Remove' buttons for each table." data-bbox="173 194 856 494"/>

Step	Description																																																												
	<p data-bbox="280 233 760 268">Configuration of Users (Continued)</p> <p data-bbox="280 268 1341 338">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.</p> <div data-bbox="375 373 1295 1440" style="border: 1px solid black; padding: 10px;">  <table border="1" data-bbox="386 432 1284 768"> <thead> <tr> <th>AQM</th> <th>Unlicen...</th> <th>Last Name</th> <th>First Name</th> <th>Team</th> <th>Windows L...</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td>1</td> <td>Supervisor</td> <td>Avaya_Team</td> <td>S1</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td>1</td> <td>Manager</td> <td>Avaya_Team</td> <td>M1</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td>2</td> <td>manager2</td> <td></td> <td>manager2</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td>H.323 Agent 1</td> <td></td> <td>Avaya_Team</td> <td>Agent_1</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td>H.323 Agent 2</td> <td></td> <td>Avaya_Team</td> <td>Agent_2</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td>SIP Agent 1</td> <td></td> <td>Avaya_Team</td> <td>SIP_Agent_1</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> <td>SIP Agent 2</td> <td></td> <td>Avaya_Team</td> <td>SIP_Agent_2</td> </tr> <tr> <td><input type="radio"/></td> <td><input checked="" type="radio"/></td> <td>Administrator</td> <td></td> <td></td> <td>administrator</td> </tr> <tr> <td><input type="radio"/></td> <td><input checked="" type="radio"/></td> <td>Agent 1</td> <td></td> <td>Avaya_Team</td> <td>Agent1</td> </tr> </tbody> </table> </div>	AQM	Unlicen...	Last Name	First Name	Team	Windows L...	<input checked="" type="radio"/>	<input type="radio"/>	1	Supervisor	Avaya_Team	S1	<input checked="" type="radio"/>	<input type="radio"/>	1	Manager	Avaya_Team	M1	<input checked="" type="radio"/>	<input type="radio"/>	2	manager2		manager2	<input checked="" type="radio"/>	<input type="radio"/>	H.323 Agent 1		Avaya_Team	Agent_1	<input checked="" type="radio"/>	<input type="radio"/>	H.323 Agent 2		Avaya_Team	Agent_2	<input checked="" type="radio"/>	<input type="radio"/>	SIP Agent 1		Avaya_Team	SIP_Agent_1	<input checked="" type="radio"/>	<input type="radio"/>	SIP Agent 2		Avaya_Team	SIP_Agent_2	<input type="radio"/>	<input checked="" type="radio"/>	Administrator			administrator	<input type="radio"/>	<input checked="" type="radio"/>	Agent 1		Avaya_Team	Agent1
AQM	Unlicen...	Last Name	First Name	Team	Windows L...																																																								
<input checked="" type="radio"/>	<input type="radio"/>	1	Supervisor	Avaya_Team	S1																																																								
<input checked="" type="radio"/>	<input type="radio"/>	1	Manager	Avaya_Team	M1																																																								
<input checked="" type="radio"/>	<input type="radio"/>	2	manager2		manager2																																																								
<input checked="" type="radio"/>	<input type="radio"/>	H.323 Agent 1		Avaya_Team	Agent_1																																																								
<input checked="" type="radio"/>	<input type="radio"/>	H.323 Agent 2		Avaya_Team	Agent_2																																																								
<input checked="" type="radio"/>	<input type="radio"/>	SIP Agent 1		Avaya_Team	SIP_Agent_1																																																								
<input checked="" type="radio"/>	<input type="radio"/>	SIP Agent 2		Avaya_Team	SIP_Agent_2																																																								
<input type="radio"/>	<input checked="" type="radio"/>	Administrator			administrator																																																								
<input type="radio"/>	<input checked="" type="radio"/>	Agent 1		Avaya_Team	Agent1																																																								

Step	Description																																																																																																																																										
<p>4.</p>	<p>Configuration of Devices Navigate to Enterprise → Record Server Configuration → VoIP Devices to configure devices.</p> <p>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 Step 3 that have the AQM license assigned.</p> <p>Click Save to complete this step.</p>  <table border="1" data-bbox="532 877 1393 1312"> <thead> <tr> <th>Extension</th> <th>Device Type</th> <th>Agent</th> <th>Recording Tones</th> <th>Signaling Group</th> <th>Recording</th> </tr> </thead> <tbody> <tr><td>53000</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53001</td><td>Avaya Phone</td><td>H.323 Agent 1, (Agent_1)</td><td></td><td>Avaya_Sig_Group</td><td>Avaya_R</td></tr> <tr><td>53002</td><td>Avaya Phone</td><td>H.323 Agent 2, (Agent_2)</td><td></td><td>Avaya_Sig_Group</td><td>Avaya_R</td></tr> <tr><td>53003</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53004</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53005</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53006</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53301</td><td>Avaya Phone</td><td>SIP Agent 1, (SIP_Agent...</td><td></td><td>Avaya_Sig_Group</td><td>Avaya_R</td></tr> <tr><td>53302</td><td>Avaya Phone</td><td>SIP Agent 2, (SIP_Agent...</td><td></td><td>Avaya_Sig_Group</td><td>Avaya_R</td></tr> <tr><td>53303</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53304</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53308</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53309</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53110</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53114</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53115</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53116</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53117</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53118</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53120</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53121</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> <tr><td>53122</td><td>Avaya Phone</td><td>User Login Required</td><td></td><td></td><td></td></tr> </tbody> </table>	Extension	Device Type	Agent	Recording Tones	Signaling Group	Recording	53000	Avaya Phone	User Login Required				53001	Avaya Phone	H.323 Agent 1, (Agent_1)		Avaya_Sig_Group	Avaya_R	53002	Avaya Phone	H.323 Agent 2, (Agent_2)		Avaya_Sig_Group	Avaya_R	53003	Avaya Phone	User Login Required				53004	Avaya Phone	User Login Required				53005	Avaya Phone	User Login Required				53006	Avaya Phone	User Login Required				53301	Avaya Phone	SIP Agent 1, (SIP_Agent...		Avaya_Sig_Group	Avaya_R	53302	Avaya Phone	SIP Agent 2, (SIP_Agent...		Avaya_Sig_Group	Avaya_R	53303	Avaya Phone	User Login Required				53304	Avaya Phone	User Login Required				53308	Avaya Phone	User Login Required				53309	Avaya Phone	User Login Required				53110	Avaya Phone	User Login Required				53114	Avaya Phone	User Login Required				53115	Avaya Phone	User Login Required				53116	Avaya Phone	User Login Required				53117	Avaya Phone	User Login Required				53118	Avaya Phone	User Login Required				53120	Avaya Phone	User Login Required				53121	Avaya Phone	User Login Required				53122	Avaya Phone	User Login Required			
Extension	Device Type	Agent	Recording Tones	Signaling Group	Recording																																																																																																																																						
53000	Avaya Phone	User Login Required																																																																																																																																									
53001	Avaya Phone	H.323 Agent 1, (Agent_1)		Avaya_Sig_Group	Avaya_R																																																																																																																																						
53002	Avaya Phone	H.323 Agent 2, (Agent_2)		Avaya_Sig_Group	Avaya_R																																																																																																																																						
53003	Avaya Phone	User Login Required																																																																																																																																									
53004	Avaya Phone	User Login Required																																																																																																																																									
53005	Avaya Phone	User Login Required																																																																																																																																									
53006	Avaya Phone	User Login Required																																																																																																																																									
53301	Avaya Phone	SIP Agent 1, (SIP_Agent...		Avaya_Sig_Group	Avaya_R																																																																																																																																						
53302	Avaya Phone	SIP Agent 2, (SIP_Agent...		Avaya_Sig_Group	Avaya_R																																																																																																																																						
53303	Avaya Phone	User Login Required																																																																																																																																									
53304	Avaya Phone	User Login Required																																																																																																																																									
53308	Avaya Phone	User Login Required																																																																																																																																									
53309	Avaya Phone	User Login Required																																																																																																																																									
53110	Avaya Phone	User Login Required																																																																																																																																									
53114	Avaya Phone	User Login Required																																																																																																																																									
53115	Avaya Phone	User Login Required																																																																																																																																									
53116	Avaya Phone	User Login Required																																																																																																																																									
53117	Avaya Phone	User Login Required																																																																																																																																									
53118	Avaya Phone	User Login Required																																																																																																																																									
53120	Avaya Phone	User Login Required																																																																																																																																									
53121	Avaya Phone	User Login Required																																																																																																																																									
53122	Avaya Phone	User Login Required																																																																																																																																									

Step	Description						
5.	<p>Configuration of Recording Schedules (Workflows)</p> <p>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.</p> <p>Click on Save (not shown) to complete this step.</p>  <p>The screenshot shows the 'Monitoring and Recording Administrator' application window. The 'Workflow Administration' section is active, displaying a table of workflows:</p> <table border="1" data-bbox="548 674 889 884"> <thead> <tr> <th>Name</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>QualityWF</td> <td>Active</td> </tr> <tr> <td>Default Quality</td> <td>Inactive</td> </tr> </tbody> </table> <p>Below the table are buttons for 'New', 'Rename', and 'Delete'. To the right, the 'Settings' section includes options for 'End of Day' (Hour: 18, Minutes: 00), 'Immediate Voice Upload', 'Immediate Screen Upload', 'Allow Evaluators to Change Form' (checked), and 'Extend Screen Recording (in seconds)' (0).</p> <p>The 'Recording Retentions' section has checkboxes for 'Scored', 'Unscored', 'Tagged', 'HR', and 'Training', each with a 'Days' or 'Months' field. For example, 'Scored' is set to 30 days.</p> <p>The 'Teams Assigned to Groups' and 'Assigned Teams' sections each have a table with 'Id', 'Team', and 'Workflow' columns. The 'Assigned Teams' table shows one entry: Id: 0.2, Team: Avaya_Team. Navigation buttons (>, >>, <, <<) are located between these two tables.</p>	Name	State	QualityWF	Active	Default Quality	Inactive
Name	State						
QualityWF	Active						
Default Quality	Inactive						

Step	Description
	<p>Configuration of Recording Schedules (Workflows) - Continued</p> <p>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.</p> 

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 **con 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 in its VoIP Device table.
- Verify that the Calabrio recording ports are registered as **IP_API_A** stations 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.

A screenshot of the Calabrio 1 login interface. It features a light gray background with a central white form. The form has three input fields: "Username" with a cursor in the first field, "Password", and "Language" with "English" selected and a red dropdown arrow. Below the form are two buttons: "Validate my PC configuration" with a red play icon and "Log In".

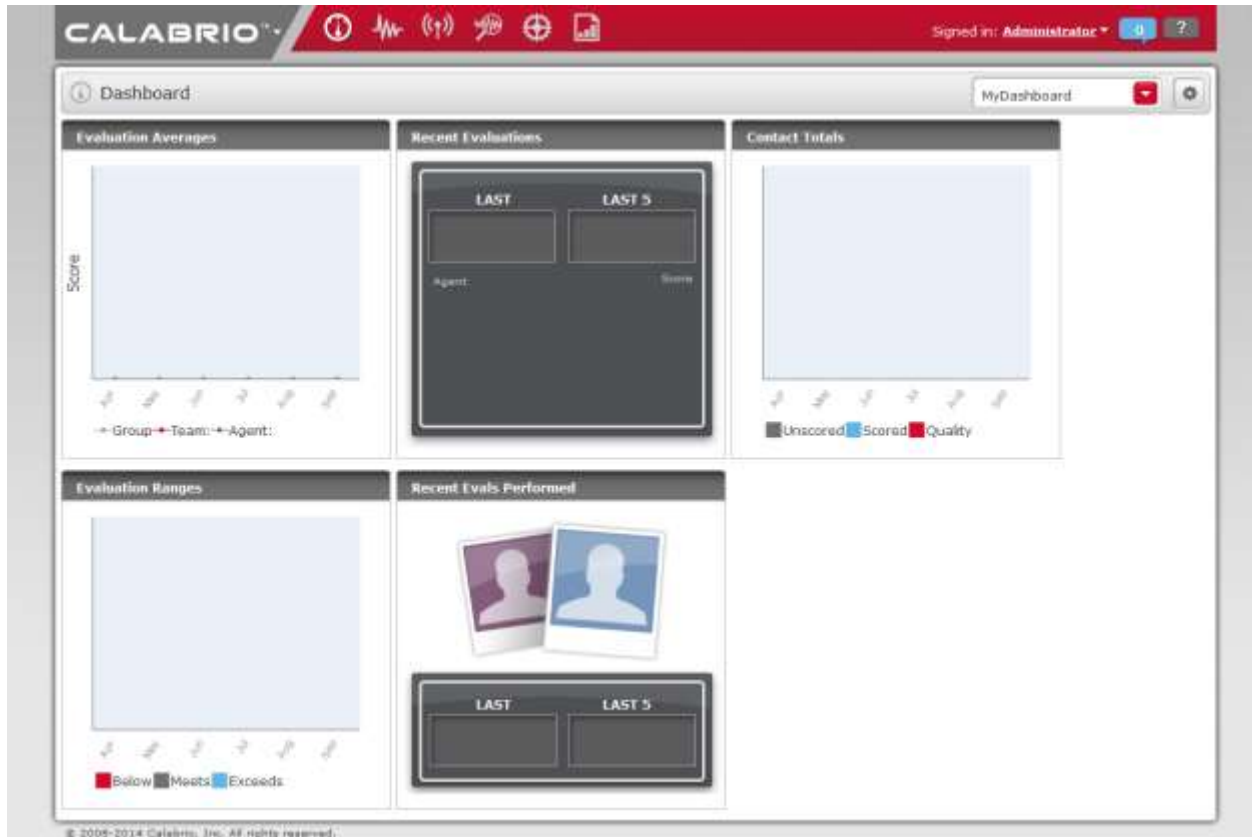
Username

Password

Language

[Validate my PC configuration](#) 

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



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

The screenshot shows the CALABRIO Recordings interface. At the top, there is a navigation bar with the CALABRIO logo and several icons. Below the navigation bar, there is a search bar labeled "New or Refined Search" and a toolbar with various icons. The main area displays a table of recordings with the following columns: Last Name, First Name, Group Name, Team Name, Calling Number, Called Number, Date, Time, Time Zone, Score, and Agent ID. The table contains 20 rows of data, all from the "Avaya_Group" and "Avaya_Team". The scores range from 2.5301 to 2.5312. The interface also shows "AQP:0%", "ATT:43 secs", and "Total:58" at the top right. At the bottom left, there is a copyright notice: "© 2008-2014 Calabrio, Inc. All rights reserved."

Last Name	First Name	Group Name	Team Name	Calling Number	Called Number	Date	Time	Time Zone	Score	Agent ID
H.323 Agent 1		Avaya_Group	Avaya_Team	53120	53001	8/30/15	03:10 PM	America/Los_Angeles	2.5301	
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	8/30/15	03:02 PM	America/Los_Angeles	2.5312	
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	8/30/15	03:00 PM	America/Los_Angeles	2.5312	
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	8/30/15	02:30 PM	America/Los_Angeles	2.5312	
H.323 Agent 1		Avaya_Group	Avaya_Team	53120	53001	8/30/15	02:23 PM	America/Los_Angeles	2.5301	
H.323 Agent 1		Avaya_Group	Avaya_Team	53104	57801	8/30/15	02:10 PM	America/Los_Angeles	2.5301	
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	8/30/15	02:09 PM	America/Los_Angeles	2.5312	
SIP Agent 1		Avaya_Group	Avaya_Team	53101	59990	8/30/15	02:09 PM	America/Los_Angeles	2.5311	
H.323 Agent 1		Avaya_Group	Avaya_Team	53001	59990	8/30/15	02:03 PM	America/Los_Angeles	2.5301	
SIP Agent 1		Avaya_Group	Avaya_Team	53101	59990	8/30/15	01:59 PM	America/Los_Angeles	2.5311	
SIP Agent 1		Avaya_Group	Avaya_Team	53101	59990	8/30/15	01:58 PM	America/Los_Angeles	2.5311	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:57 AM	America/Los_Angeles	2.5301	
H.323 Agent 2		Avaya_Group	Avaya_Team	53002	59990	8/11/15	10:56 AM	America/Los_Angeles	2.5302	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:50 AM	America/Los_Angeles	2.5301	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:50 AM	America/Los_Angeles	2.5301	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:41 AM	America/Los_Angeles	2.5301	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:35 AM	America/Los_Angeles	2.5301	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:19 AM	America/Los_Angeles	2.5301	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:12 AM	America/Los_Angeles	2.5301	
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	11:12 AM	America/Los_Angeles	2.5301	

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

The screenshot displays the CALABRIO interface. At the top, the logo 'CALABRIO' is visible on the left, and 'Signed in: Administrator' is on the right. Below the header, there's a 'Recordings' section with a search bar and several icons. A table lists various recordings with columns for Last Name, First Name, Group Name, Team Name, Calling Number, Called Number, Date, Time, Time Zone, Score, and Agent ID. The 14th row is highlighted in blue. Below the table, there are two tabs: 'Contact Information' and 'Associated Contacts'. At the bottom, a playback window is open, showing a waveform and a progress bar with standard media control buttons.

Last Name	First Name	Group Name	Team Name	Calling Number	Called Number	Date	Time	Time Zone	Score	Agent ID
H.323 Agent 1		Avaya_Group	Avaya_Team	53120	53001	9/30/15	03:10 PM	America/Los_Angeles		2.5301
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	9/30/15	03:32 PM	America/Los_Angeles		2.5312
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	9/30/15	03:00 PM	America/Los_Angeles		2.5312
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	9/30/15	02:30 PM	America/Los_Angeles		2.5312
H.323 Agent 1		Avaya_Group	Avaya_Team	53120	53001	9/30/15	02:23 PM	America/Los_Angeles		2.5301
H.323 Agent 1		Avaya_Group	Avaya_Team	53104	57801	9/30/15	02:10 PM	America/Los_Angeles		2.5301
SIP Agent 2		Avaya_Group	Avaya_Team	53102	59990	9/30/15	02:09 PM	America/Los_Angeles		2.5312
SIP Agent 1		Avaya_Group	Avaya_Team	53101	59990	9/30/15	02:09 PM	America/Los_Angeles		2.5311
H.323 Agent 1		Avaya_Group	Avaya_Team	53001	59990	9/30/15	02:03 PM	America/Los_Angeles		2.5301
SIP Agent 1		Avaya_Group	Avaya_Team	53101	59990	9/30/15	01:58 PM	America/Los_Angeles		2.5311
SIP Agent 1		Avaya_Group	Avaya_Team	53101	59990	9/30/15	01:58 PM	America/Los_Angeles		2.5311
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:57 AM	America/Los_Angeles		2.5301
H.323 Agent 2		Avaya_Group	Avaya_Team	53002	59990	8/11/15	10:56 AM	America/Los_Angeles		2.5302
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:50 AM	America/Los_Angeles		2.5301
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:50 AM	America/Los_Angeles		2.5301
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:41 AM	America/Los_Angeles		2.5301
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:35 AM	America/Los_Angeles		2.5301
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:19 AM	America/Los_Angeles		2.5301
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/11/15	10:12 AM	America/Los_Angeles		2.5301
H.323 Agent 1		Avaya_Group	Avaya_Team	3035380121	17209772874	8/5/15	11:12 AM	America/Los_Angeles		2.5301

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 of Avaya Aura[®] Application Enablement Services to perform recording. During compliance testing, Calabrio successfully recorded calls placed to and from agents and station.

10. Additional References

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

1. *Administering Avaya Aura[®] Communication Manager*, Release 6.3, Issue 10, July 2015, Document Number 03-300509.
2. *Avaya Aura[®] Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2015

©2016 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.