



## **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 the 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 the 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. 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:

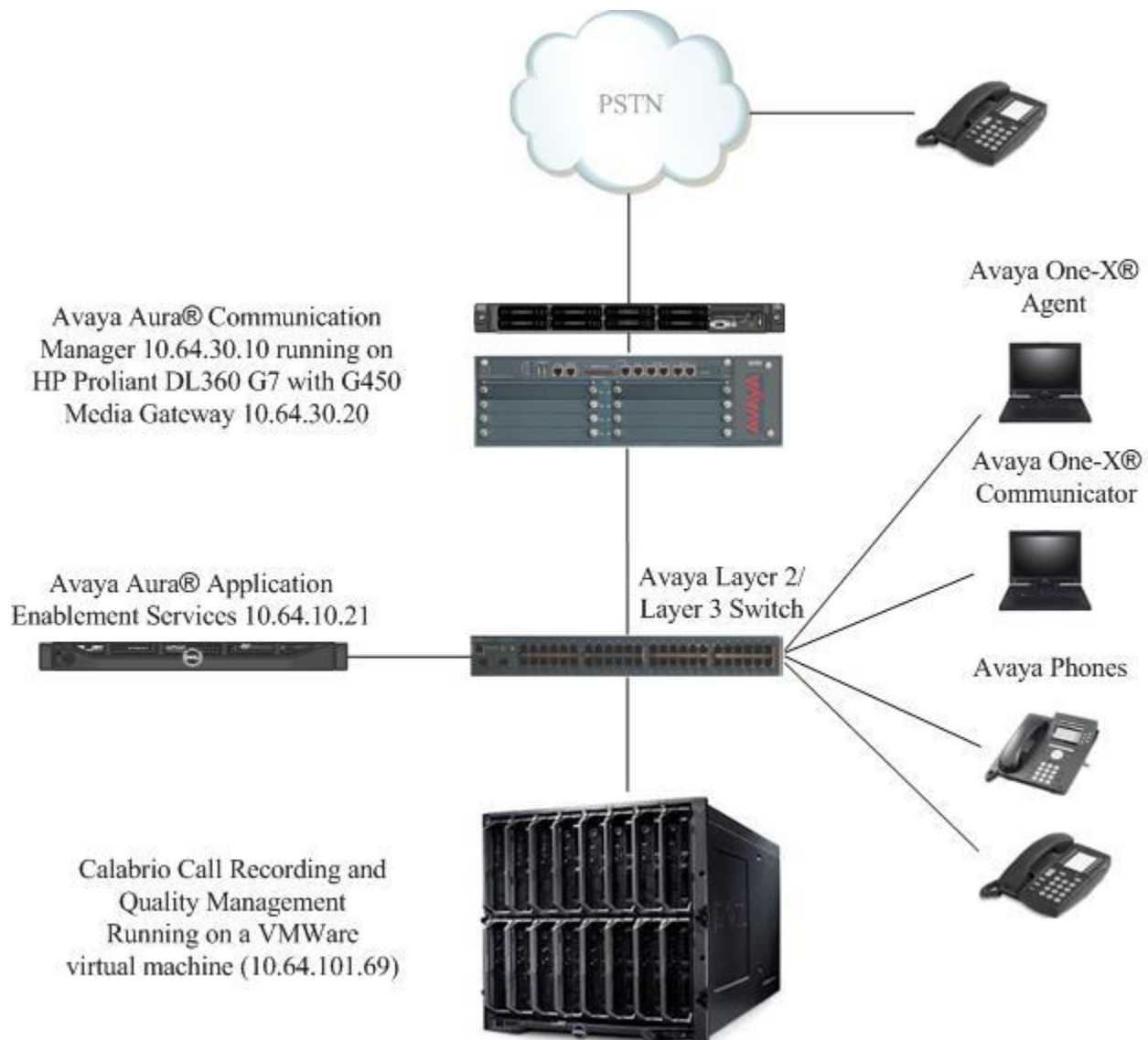
- Phone: +1 (763) 592-4680 or +1 (800) 303-1248
- Web: <http://calabrio.com/about-calabrio/services/>
- Email: [calabriosupport@calabrio.com](mailto:calabriosupport@calabrio.com)

### 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 SP5
Avaya G450 Media Gateway <ul style="list-style-type: none"><li>• MGP</li><li>• MM710AP (DS1)</li><li>• MM712AP (DCP)</li><li>• MM711AP (ANA)</li></ul>	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
Avaya 9600 Series IP Telephone <ul style="list-style-type: none"><li>• 9640 (H.323)</li></ul>	6.3
Avaya 96x1 Series IP Telephone <ul style="list-style-type: none"><li>• 9641 (H.323)</li></ul>	6.3.1
Desktop PC running Avaya One-X® Communicator	6.2
Calabrio Recording and Quality Management running under Windows 2008 R2 Server on a VMWare virtual machine	9.2

## 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**.

Step	Description
1.	<p><b>Verify Feature and License for the integration</b>  Enter the <b>display system-parameters customer-options</b> command and ensure that <b>Computer Telephony Adjunct Links</b> is set to <b>y</b>. If this option is not set to <b>y</b>, contact the Avaya sales team or business partner for a proper license file.</p> <pre> display system-parameters customer-options                               Page  3 of 11                                 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          <b>Computer Telephony Adjunct Links? y</b>     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     Async. Transfer Mode (ATM) Trunking? n        Digital Loss Plan Modification? y     ATM WAN Spare Processor? n                    DS1 MSP? y     ATMS? y          DS1 Echo Cancellation? y     Attendant Vectoring? Y </pre> <p>Each recording port or virtual station extension the recorder will use to record agent phones will require an <b>IP_API_A</b> license if not licensed on Application Enablement Services.</p> <pre> diaplay system-parameters customer-options                               Page 10 of 11                                 MAXIMUM IP REGISTRATIONS BY PRODUCT ID  Product ID  Rel. Limit      Used AgentSC    *   : 10000      0 <b>IP_API_A</b>  *   : <b>18000</b>      <b>0</b> </pre>

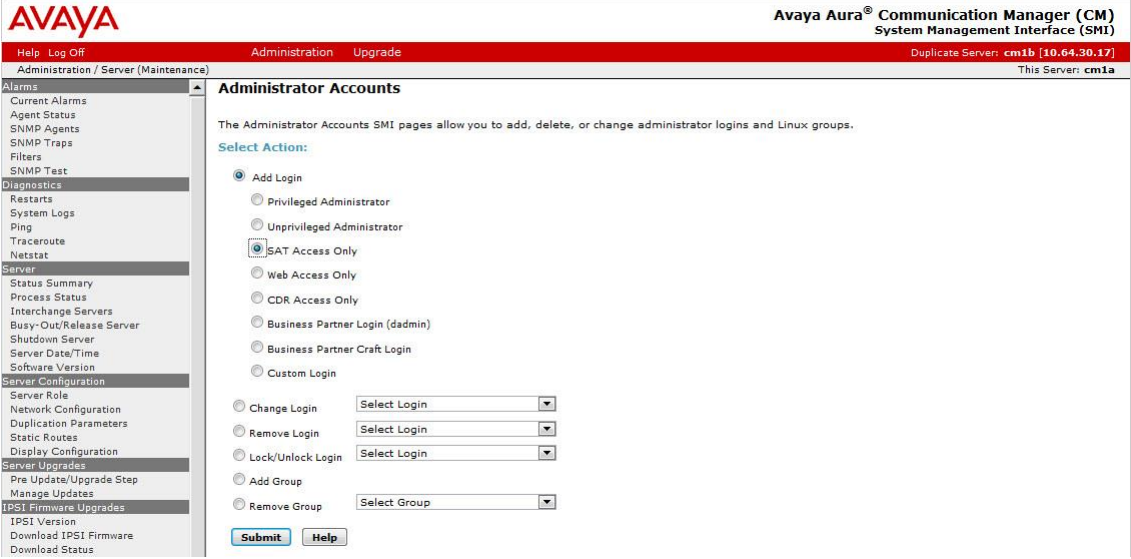
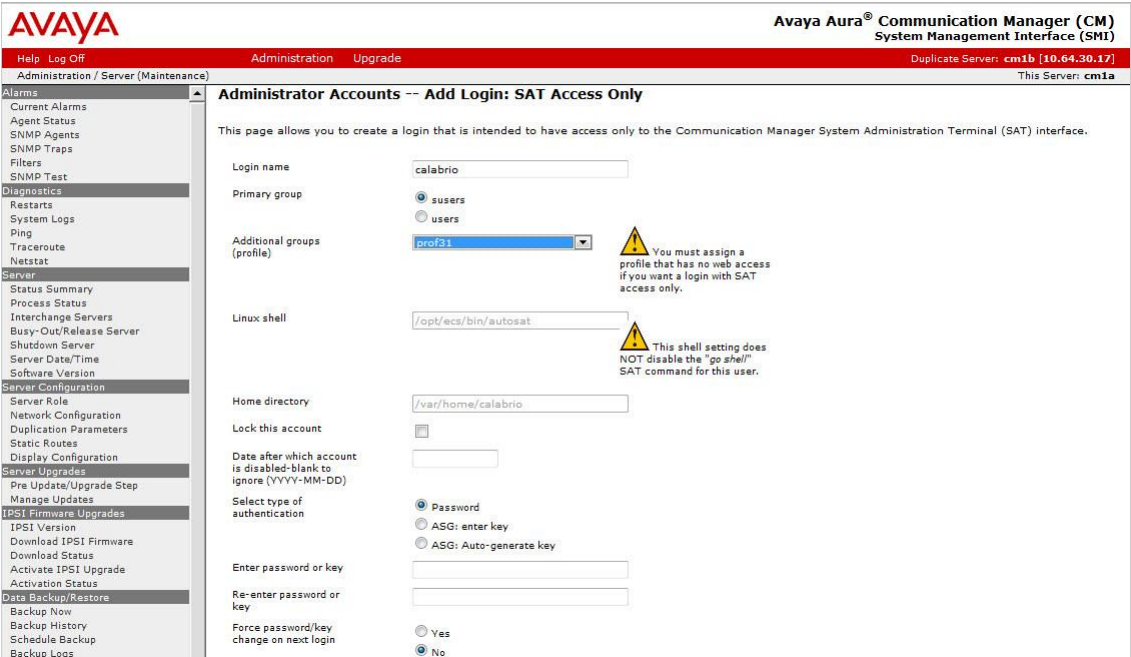
Step	Description
2.	<p><b>Administer Communication Manager System Features</b>  Enter the <b>change system-parameters features</b> command and ensure that on page 5 <b>Create Universal Call ID (UCID)</b> is enabled and a relevant <b>UCID Network Node ID</b> (1 was used in the test) is defined. Also ensure that on page 13 that <b>Send UCID to ASAI</b> is set to <b>y</b>. CRQM relies on UCID to track complex calls (Transfers and Conferences).</p> <pre> 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       <b>Create Universal Call ID (UCID)? y    UCID Network Node ID: 1</b> </pre> <pre> 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 UI During Conference/Transfer? n       Call Classification After Answer Supervision? n                                 <b>Send UCID to ASAI? y</b>       For ASAI Send DTMF Tone to Call Originator? y       Send Connect Event to ASAI For Announcement Answer? n </pre>



Step	Description																		
3.	<p><b>Administer IP-Services for Application Enablement Services</b></p> <p>Add an IP-Services entry for Application Enablement Services as described below:</p> <ul style="list-style-type: none"><li>• Enter the <b>change ip-services</b> command.</li><li>• In the <b>Service Type</b> field, type <b>AESVCS</b>.</li><li>• In the <b>Enabled</b> field, type <b>y</b>.</li><li>• In the <b>Local Node</b> field, type the Node name <b>procr</b> for the Processor Ethernet Interface.</li><li>• In the <b>Local Port</b> field, use the default of <b>8765</b>.</li><li>• Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration.</li></ul>																		
	<div>change ip-services<div>Page1 of 4</div><table><tr><th colspan="6">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></tr><tr><td>AESVCS</td><td>y</td><td>procr</td><td>8765</td><td></td><td></td></tr></table></div>	IP SERVICES						Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	AESVCS	y	procr	8765		
IP SERVICES																			
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port														
AESVCS	y	procr	8765																
	<p>On Page 4 of the IP Services form, enter the following values:</p> <ul style="list-style-type: none"><li>• In the <b>AE Services Server</b> field, type the host name of the Application Enablement Services server.</li><li>• In the <b>Password</b> field, type the same password to be administered on the Application Enablement Services server in <b>Section 6, Step 1</b>.</li><li>• In the <b>Enabled</b> field, type <b>y</b>.</li></ul>																		
	<div>change ip-services<div>Page4 of 4</div><table><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><tr><td>1:</td><td>aes6_tr1</td><td>xxxxxxx</td><td>y</td><td></td></tr></table></div>	AE Services Administration					Server ID	AE Services Server	Password	Enabled	Status	1:	aes6_tr1	xxxxxxx	y				
AE Services Administration																			
Server ID	AE Services Server	Password	Enabled	Status															
1:	aes6_tr1	xxxxxxx	y																

Step	Description																																																												
4.	<b>Administer Computer Telephony Integration (CTI) Link</b> Enter the <b>add cti-link &lt;link number&gt;</b> command, where <b>&lt;link number&gt;</b> is an available CTI link number. <ul style="list-style-type: none"><li>In the <b>Extension</b> field, type a valid station extension.</li><li>In the <b>Type</b> field, type <b>ADJ-IP</b>.</li><li>In the <b>Name</b> field, type a descriptive name.</li></ul>																																																												
	<div>add cti-link 1<div>CTI LINK</div><div>Page1 of3</div><div>CTI Link: 1</div><div>Extension: 21900</div><div>Type: ADJ-IP</div><div>Name: to AES_10_21</div><div>COR: 1</div></div>																																																												
5.	<b>Add SMS User Account</b> 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 <b>add user-profile-by-category 31</b> command was used to create the profile used in the test as shown below. The <b>Shell Access</b> , <b>Call Center B</b> and <b>Stations M</b> fields were set to <b>y</b> .																																																												
	<div>add user-profile-by-category 31<div>USER PROFILE 31</div><div>Page1 of39</div><div>User Profile Name: Calabrio SMS</div><div>This Profile is Disabled? nShell Access? y</div><div>Facility Test Call Notification? nAcknowledgement Required? n</div><div>Grant Un-owned Permissions? nExtended Profile? n</div><table><tr><td>Name</td><td>Cat</td><td>Enbl</td><td>Name</td><td>Cat</td><td>Enbl</td></tr><tr><td>Adjuncts</td><td>A</td><td>n</td><td>Routing and Dial Plan</td><td>J</td><td>n</td></tr><tr><td>Call Center B</td><td>B</td><td>y</td><td>Security</td><td>K</td><td>n</td></tr><tr><td>Features</td><td>C</td><td>n</td><td>Servers</td><td>L</td><td>n</td></tr><tr><td>Hardware</td><td>D</td><td>n</td><td>Stations M</td><td>M</td><td>y</td></tr><tr><td>Hospitality</td><td>E</td><td>n</td><td>System Parameters</td><td>N</td><td>n</td></tr><tr><td>IP</td><td>F</td><td>n</td><td>Translations</td><td>O</td><td>n</td></tr><tr><td>Maintenance</td><td>G</td><td>n</td><td>Trunking</td><td>P</td><td>n</td></tr><tr><td>Measurements and Performance</td><td>H</td><td>n</td><td>Usage</td><td>Q</td><td>n</td></tr><tr><td>Remote Access</td><td>I</td><td>n</td><td>User Access</td><td>R</td><td>n</td></tr></table></div>	Name	Cat	Enbl	Name	Cat	Enbl	Adjuncts	A	n	Routing and Dial Plan	J	n	Call Center B	B	y	Security	K	n	Features	C	n	Servers	L	n	Hardware	D	n	Stations M	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
	Name	Cat	Enbl	Name	Cat	Enbl																																																							
Adjuncts	A	n	Routing and Dial Plan	J	n																																																								
Call Center B	B	y	Security	K	n																																																								
Features	C	n	Servers	L	n																																																								
Hardware	D	n	Stations M	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																																																								

Step	Description																																																
	<div><div>Add SMS User Account (Continued)</div><div>Read only access to Agents and Stations is required. Enter <b>r-</b> permissions for the <b>B</b> and <b>M</b> Categories on the <b>Set Permissions for Category:</b> entry on the <b>change user-profile-by-category xx</b> form. This requires two separate transactions, so repeat for each category. Please note that this profile will be used later in this section.</div></div>																																																
	<div><div>change user-profile-by-category 31<div>Page3 of 39</div></div><div><div>USER PROFILE BY CATEGORY 31</div><div><div>Set Permissions For Category: B To: r-</div><div>Set All Permissions To:</div></div><div>'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance</div><table><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></div></div>	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-																																															
	<div><div>change user-profile-by-category 31<div>Page29 of 39</div></div><div><div>USER PROFILE BY CATEGORY 31</div><div><div>Set Permissions For Category: M To: r-</div><div>Set All Permissions To:</div></div><div>'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance</div><table><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></div></div>	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
	<p><b>Add SMS User Account (Continued)</b></p> <p>Create a user account on the Communication Manager <b>System Management Interface</b> web page by navigating to the <b>Administer Accounts</b> page and selecting the radio button <b>Add Login</b> and <b>SAT Access Only</b>. Click <b>Submit</b> to continue the process.</p>  <p>The <b>Add Login</b> screen is displayed. Enter a name to the <b>Login name</b> field and select the profile defined in earlier in this section (<b>prof31</b>) in the <b>Additional groups (profile)</b> field. Select <b>Password</b> for the <b>Select type of authentication</b> field and enter a <b>Password</b>.</p> 

Step	Description
6.	<p><b>Verify Recorded Extensions</b></p> <p>All stations that will be recorded using the Multiple Registration method must have <b>IP Softphone</b> enabled, and the application needs to know the <b>Security Code</b> 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 <b>IP Softphone</b> setting disabled. Use the <b>display station n</b> command to verify information, or <b>change station n</b> to make changes if necessary.</p>
	<pre> display station 21949                                     Page 1 of 5 STATION Extension: 21949           Lock Messages? n           BCC: 0 Type: 9640                Security Code: 123456         TN: 1 Port: S00009              Coverage Path 1:         COR: 1 Name: King, John          Coverage Path 2:         COS: 1                           Hunt-to Station: STATION OPTIONS                           Time of Day Lock Table:                           Loss Group: 19               Personalized Ringing Pattern: 1                           Speakerphone: 2-way          Message Lamp Ext: 21949                           Display Language: english    Mute Button Enabled? y                           Survivable GK Node Name:      Button Modules: 0                           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>

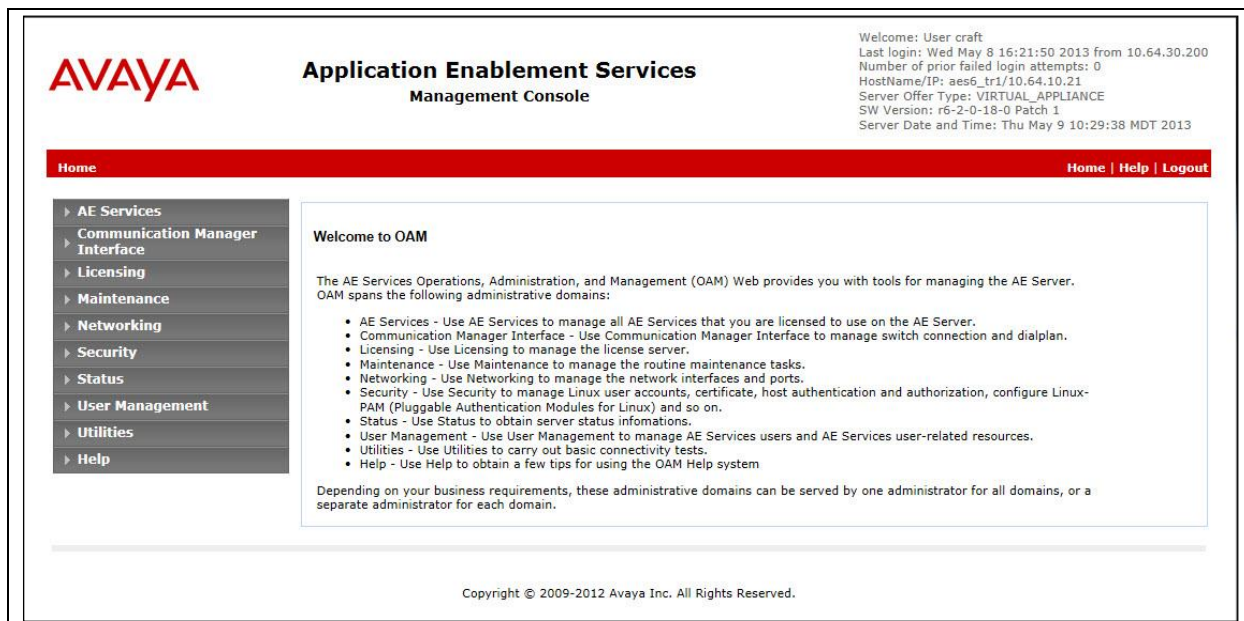
Step	Description
7.	<p><b>Add Virtual Stations</b></p> <p>Virtual stations are used by CRQM to do Single Step Conference based call recording for stations that are not capable of supporting IP Softphone or have the IP Softphone setting disabled. Add a virtual station using <b>the add station &lt;n&gt;</b> command; where &lt;n&gt; is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.</p> <ul style="list-style-type: none"> <li>• In the <b>Type</b> field, enter a station type such as <b>9640</b></li> <li>• In the <b>Name</b> field, enter a name containing the <b>DMCC</b> string (e.g. <b>DMCC station 2</b>). CRQM uses the DMCC string to identify virtual stations.</li> <li>• In the <b>Security Code</b> field, enter a desired value.</li> <li>• Set the <b>IP SoftPhone</b> field to <b>y</b></li> </ul> <pre> add station 24001                                     Page 1 of 5                                  STATION  Extension: 24001                                Lock Messages? n                BCC: 0   Type: 9640                                Security Code: 123456            TN: 1   Port: S00021                                Coverage Path 1:                COR: 1   Name: DMCC station 2                        Coverage Path 2:                COS: 1  Hunt-to Station:  STATION OPTIONS                                  Time of Day Lock Table:       Loss Group: 19                    Personalized Ringing Pattern: 1  Message Lamp Ext: 24001       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

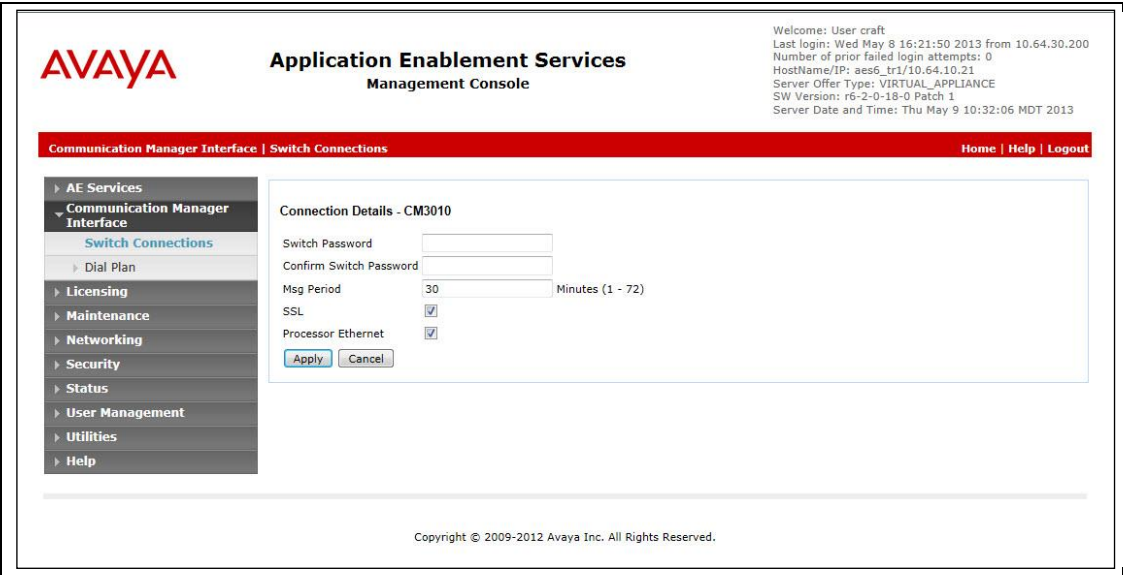
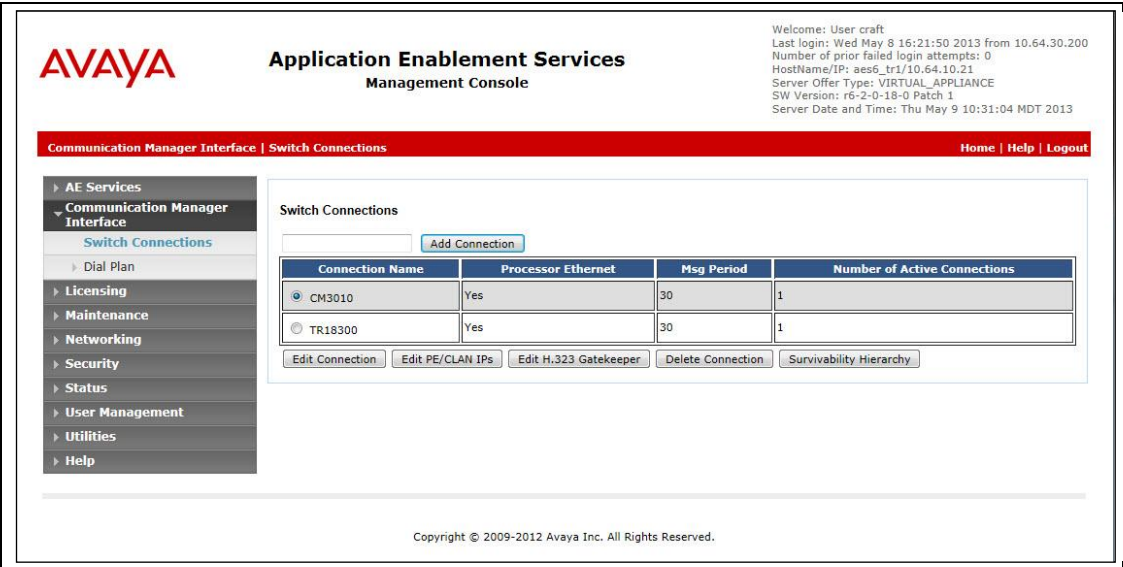
All administration of Application Enablement Services is performed via a web browser. Enter <https://<ip-addr>> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. Note that all 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:

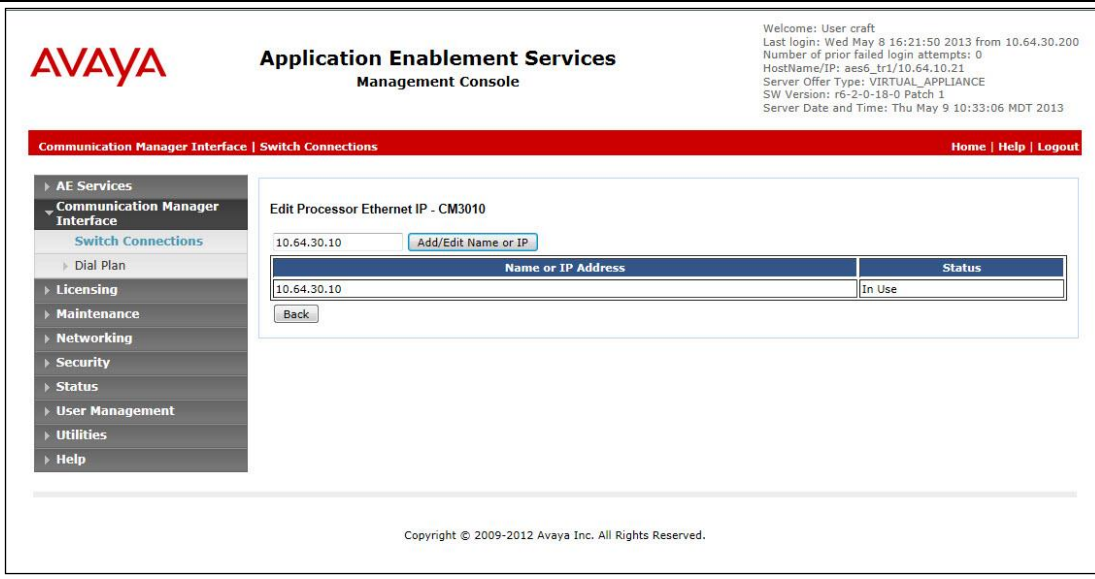
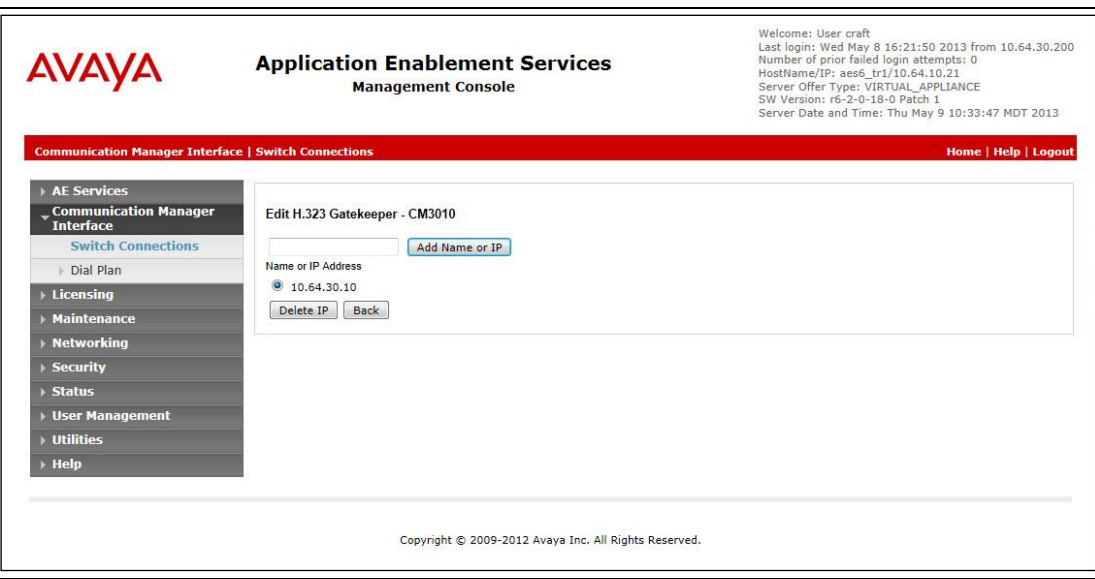
- Configure Communication Manager Switch Connections
- Add TSAPI Links
- Note the TLink Information
- Configure Calabrio User
- Enable Unrestricted Access for Calabrio User
- Confirm TSAPI and DMCC Licenses



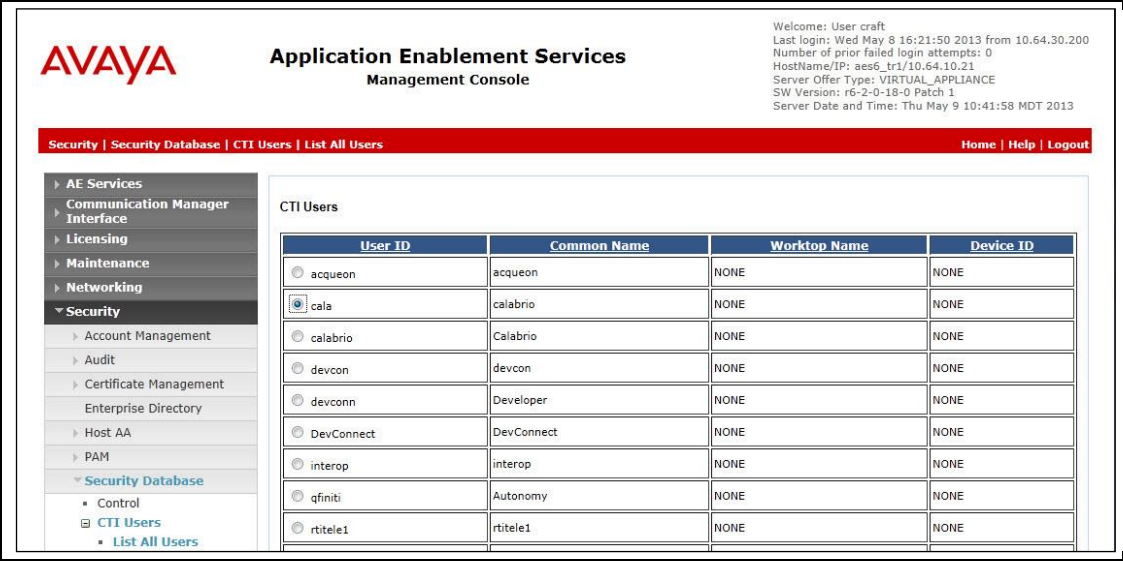
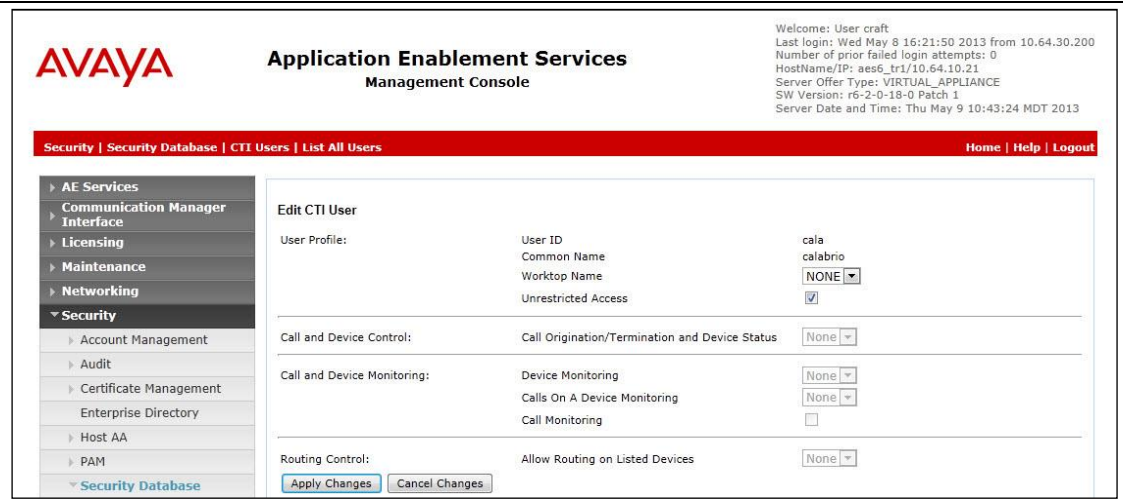
Step	Description
------	-------------

Step	Description
1.	<p><b>Configure Communication Manager Switch Connections</b></p> <p>To add links to Communication Manager, navigate to the <b>Communication Manager Interface</b> → <b>Switch Connections</b> page and enter a name for the new switch connection (e.g. <b>CM3010</b>) and click the <b>Add Connection</b> button (not shown). The <b>Connection Details</b> screen is shown. Enter the <b>Switch Password</b> configured in <b>Section 5, Step 3</b> and check the <b>Processor Ethernet</b> box if using the <b>procr</b> interface. Click <b>Apply</b>.</p>  <p>The display returns to the <b>Switch Connections</b> screen which shows that the <b>CM3010</b> switch connection has been added.</p> 



Step	Description				
	<p data-bbox="300 233 1421 411"><b>Configure Communication Manager Switch Connections (Continued)</b> Click the <b>Edit PE/CLAN IPs</b> button on the <b>Switch Connections</b> screen to configure the <b>procr</b> or <b>CLAN</b> IP Address(es) for TSAPI message traffic. The <b>Edit Processor Ethernet IP</b> screen is displayed. Enter the IP address of the <b>procr</b> interface and click the <b>Add/Edit Name or IP</b> button.</p> <div data-bbox="300 449 1421 1024">  <p data-bbox="347 491 477 533"><b>AVAYA</b></p> <p data-bbox="574 491 932 533"><b>Application Enablement Services</b> Management Console</p> <p data-bbox="1071 470 1386 562">Welcome: User craft Last login: Wed May 8 16:21:50 2013 from 10.64.30.200 Number of prior failed login attempts: 0 HostName/IP: aes6_tr1/10.64.10.21 Server Offer Type: VIRTUAL_APPLIANCE SW Version: r6-2-0-18-0 Patch 1 Server Date and Time: Thu May 9 10:33:06 MDT 2013</p> <p data-bbox="347 583 688 604">Communication Manager Interface   Switch Connections</p> <p data-bbox="1256 583 1386 604"><a href="#">Home</a>   <a href="#">Help</a>   <a href="#">Logout</a></p> <ul data-bbox="347 625 558 919" style="list-style-type: none"> <li>AE Services</li> <li>Communication Manager Interface <ul style="list-style-type: none"> <li>Switch Connections</li> <li>Dial Plan</li> </ul> </li> <li>Licensing</li> <li>Maintenance</li> <li>Networking</li> <li>Security</li> <li>Status</li> <li>User Management</li> <li>Utilities</li> <li>Help</li> </ul> <p data-bbox="574 646 802 667">Edit Processor Ethernet IP - CM3010</p> <p data-bbox="574 680 850 701">10.64.30.10 <a href="#">Add/Edit Name or IP</a></p> <table data-bbox="574 701 1370 743"> <thead> <tr> <th>Name or IP Address</th><th>Status</th></tr> </thead> <tbody> <tr> <td>10.64.30.10</td><td>In Use</td></tr> </tbody> </table> <p data-bbox="574 743 623 764"><a href="#">Back</a></p> <p data-bbox="721 974 1013 995">Copyright © 2009-2012 Avaya Inc. All Rights Reserved.</p> </div> <p data-bbox="300 1066 1421 1203">Click the <b>Edit H.323 Gatekeeper</b> button on the <b>Switch Connections</b> screen to configure the <b>procr</b> or <b>CLAN</b> IP Address(es) for DMCC registrations. The <b>Edit H.323 Gatekeeper</b> screen is displayed. Enter the IP address of the <b>procr</b> interface and click the <b>Add Name or IP</b> button.</p> <div data-bbox="300 1241 1421 1816">  <p data-bbox="347 1283 477 1325"><b>AVAYA</b></p> <p data-bbox="574 1283 932 1325"><b>Application Enablement Services</b> Management Console</p> <p data-bbox="1071 1262 1386 1354">Welcome: User craft Last login: Wed May 8 16:21:50 2013 from 10.64.30.200 Number of prior failed login attempts: 0 HostName/IP: aes6_tr1/10.64.10.21 Server Offer Type: VIRTUAL_APPLIANCE SW Version: r6-2-0-18-0 Patch 1 Server Date and Time: Thu May 9 10:33:47 MDT 2013</p> <p data-bbox="347 1375 688 1396">Communication Manager Interface   Switch Connections</p> <p data-bbox="1256 1375 1386 1396"><a href="#">Home</a>   <a href="#">Help</a>   <a href="#">Logout</a></p> <ul data-bbox="347 1417 558 1711" style="list-style-type: none"> <li>AE Services</li> <li>Communication Manager Interface <ul style="list-style-type: none"> <li>Switch Connections</li> <li>Dial Plan</li> </ul> </li> <li>Licensing</li> <li>Maintenance</li> <li>Networking</li> <li>Security</li> <li>Status</li> <li>User Management</li> <li>Utilities</li> <li>Help</li> </ul> <p data-bbox="574 1438 769 1459">Edit H.323 Gatekeeper - CM3010</p> <p data-bbox="574 1472 818 1493"><input type="text"/> <a href="#">Add Name or IP</a></p> <p data-bbox="574 1493 672 1514">Name or IP Address</p> <p data-bbox="574 1514 672 1535"><input checked="" type="radio"/> 10.64.30.10</p> <p data-bbox="574 1535 704 1556"><a href="#">Delete IP</a> <a href="#">Back</a></p> <p data-bbox="721 1766 1013 1787">Copyright © 2009-2012 Avaya Inc. All Rights Reserved.</p> </div>	Name or IP Address	Status	10.64.30.10	In Use
Name or IP Address	Status				
10.64.30.10	In Use				

Step	Description
2.	<p><b>Configure Calabrio user</b></p> <p>In the Navigation Panel, select <b>User Management</b> → <b>User Admin</b> → <b>Add User</b>. The <b>Add User</b> panel will display as shown below. Enter an appropriate <b>User Id</b>, <b>Common Name</b>, <b>Surname</b>, and <b>User Password</b>. Select <b>Yes</b> from the <b>CT User</b> dropdown list.</p> <p>Click <b>Apply</b> at the bottom of the pages to save the entries.</p> <div data-bbox="300 485 1425 1467"> </div>

Step	Description
3.	<p><b>Enable Unrestricted Access for Calabrio User</b></p> <p>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.</p> <p>Navigate to <b>Security</b> → <b>Security Database</b> → <b>CTI Users</b> → <b>List All Users</b> and select the <b>cala</b> user and click <b>Edit</b> (not shown).</p>  <p>On the <b>Edit CTI User</b> panel, check the <b>Unrestricted Access</b> box and click the <b>Apply Changes</b> button. Click <b>Apply</b> when asked to confirm the change on the <b>Apply Changes to CTI User Properties</b> dialog.</p> 

Step	Description
4.	<p><b>Confirm TSAPI and DMCC Licenses</b></p> <p>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 VALUE_AES_DMCC_DMC is licensed on Application Enablement Services, then an IP_API_A is generally not required on Communication Manager. Please consult product offer documentation for more details. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.</p> <p>From the left pane menu on Application Enablement Services Management Console, click <b>Licensing → WebLM Server Access</b>. A <b>Web License Manager</b> login window is displayed. Enter proper credentials to log in. Click <b>Licensed products → APPL_ENAB → Application Enablement</b> from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough VALUE_AES_DMCC_DMC and VALUE_AES_TSAPI_USERS licenses available.</p>

AVAYA

Web License Manager (WebLM v6.2)

Help | About | Change Password | Log off admin

WebLM Home

Install license

Licensed products

APPL\_ENAB

Application Enablement

View license capacity

View peak usage

Uninstall license

Server properties

Manage users

Shortcuts

Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)

You are here: Licensed Products > Application\_Enablement > View License Capacity

License installed on: November 16, 2012 2:53:55 PM -06:00

License File Host IDs: 00-16-3E-C5-B5-A3

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASA1 (VALUE_AES_CVLAN_ASA1)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent		Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	9
DLG (VALUE_AES_DLG)	permanent	16	1
DMCC (VALUE_AES_DMCC_DMC)	permanent	10000	9
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	16	0

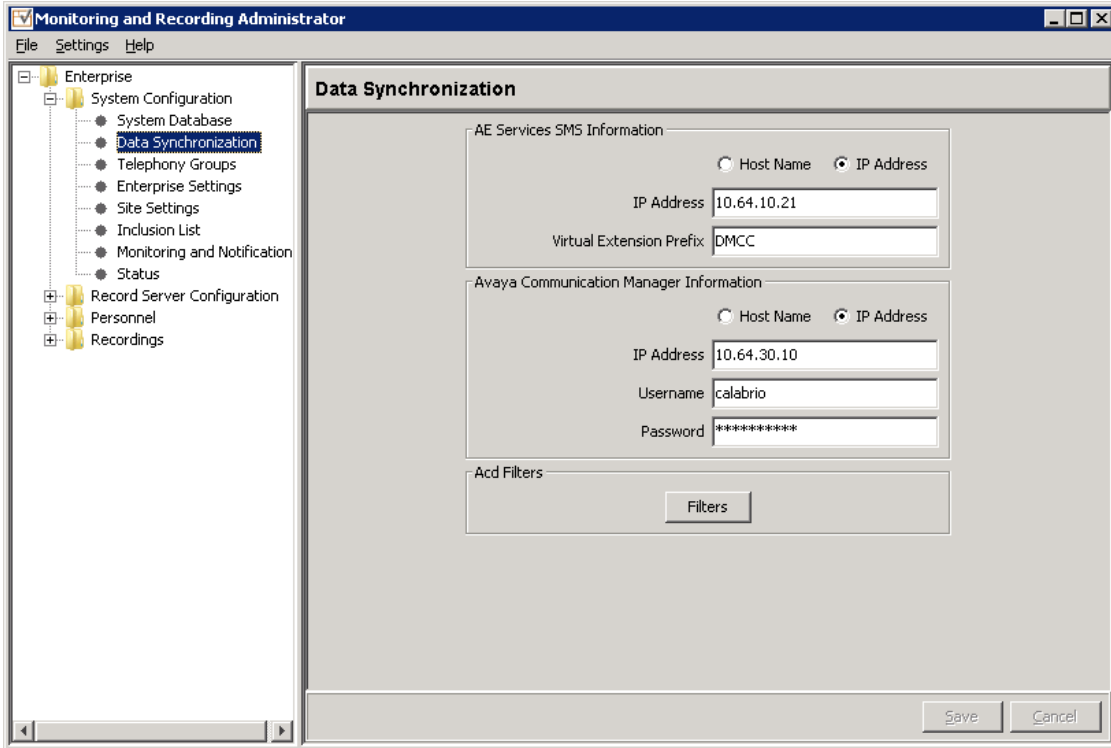
## 7. Configure Calabrio Call Recording and Quality Management

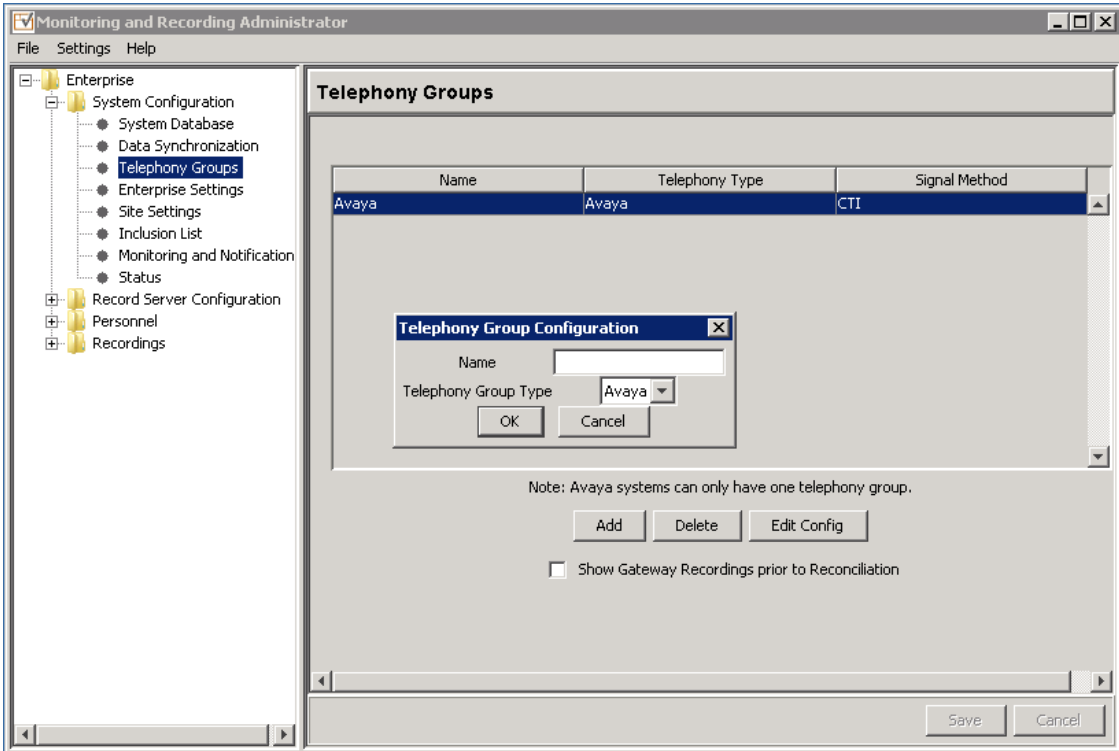
The initial configuration of the CRQM server is typically performed by Calabrio technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the CRQM solution to interoperate with Communication Manager and Application Enablement Services.

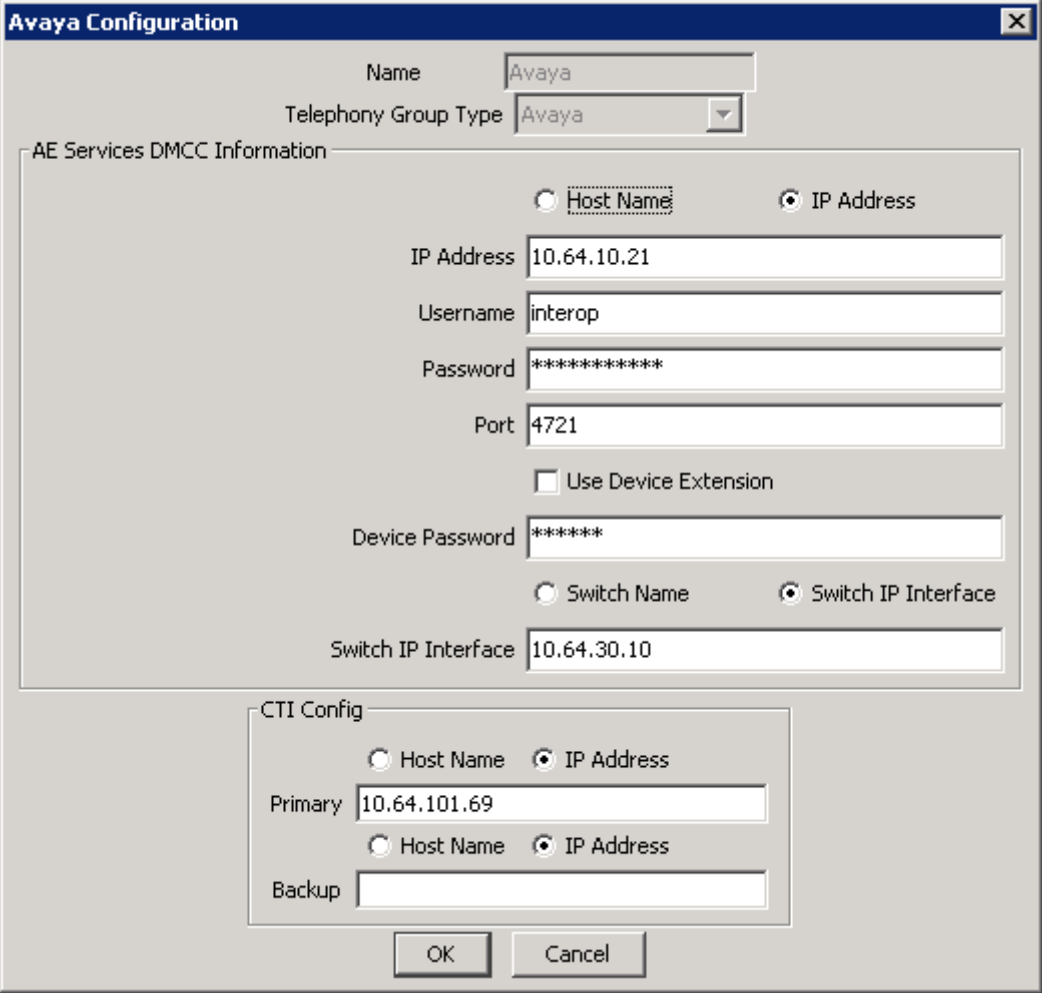
The steps include:

- 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)

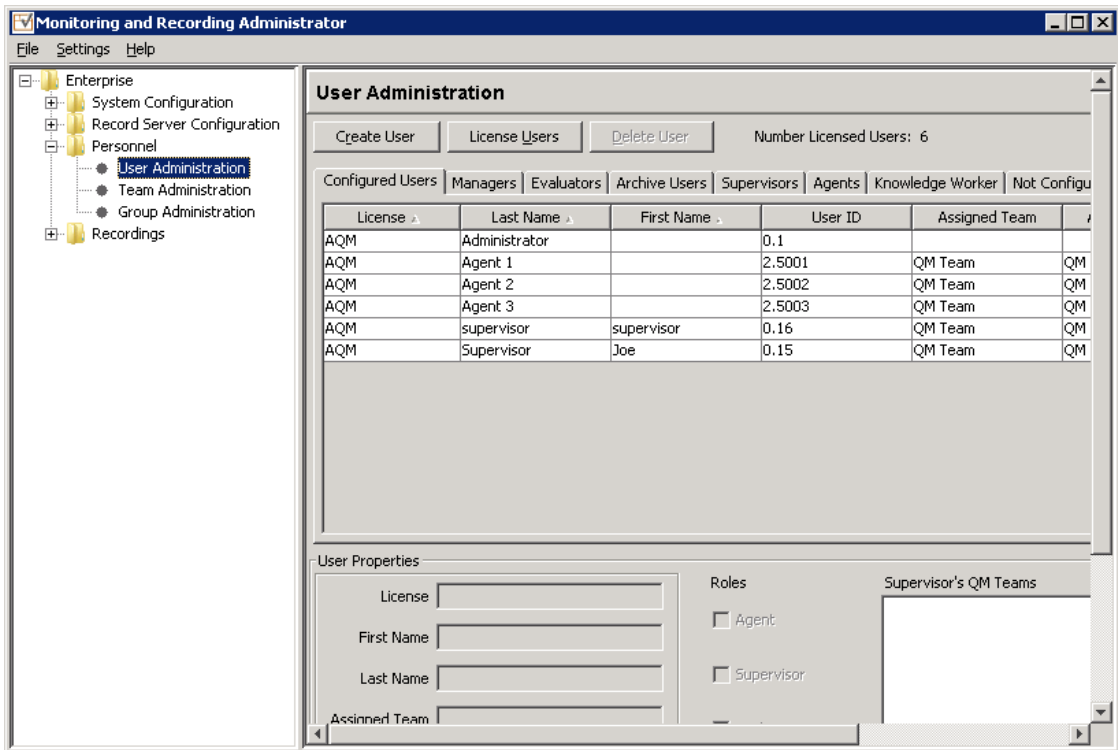
The configuration of the CRQM server is performed using the **Calabrio Monitoring and Recording Administrator** application, which can be launched by clicking **Start → All Programs → Calabrio → Monitoring and Recording Administrator**. Log in with proper credentials.

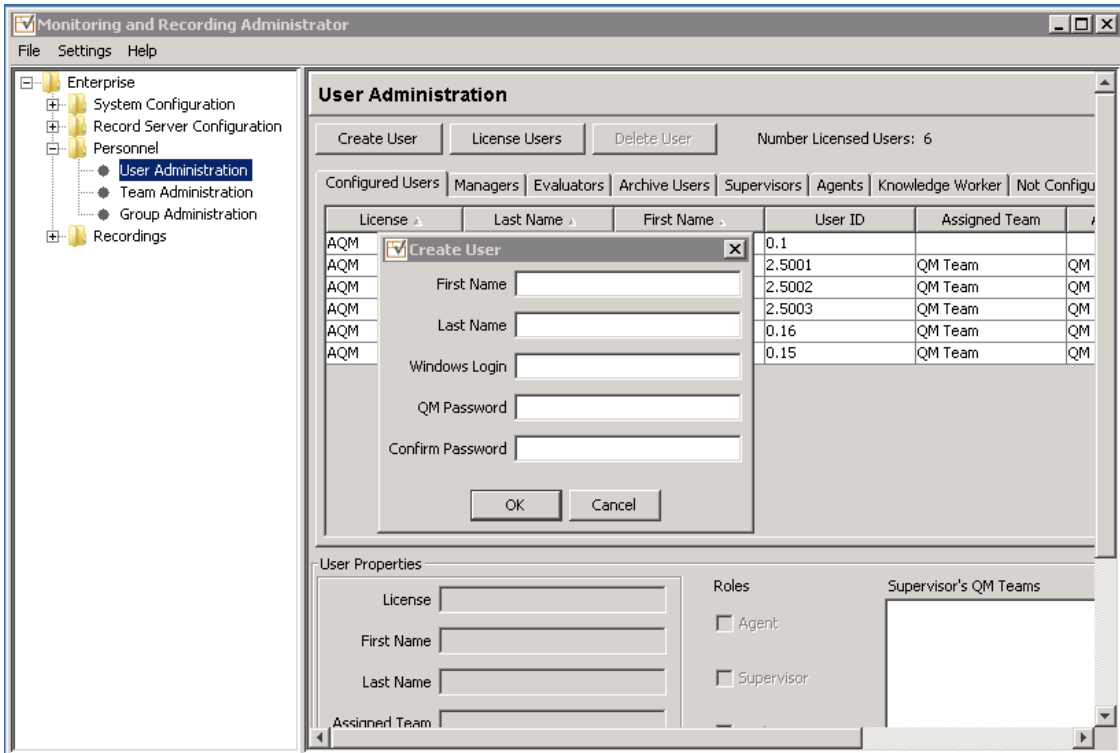
Step	Description
1.	<p><b>Configuration of the Application Enablement Interfaces – SMS</b></p> <p>From the left pane, navigate to <b>Enterprise → System Configuration → Data Synchronization</b>.</p> <p>Provide the <b>IP Address</b> or <b>Host Name</b> of the Application Enablement Services server in the <b>AE Services SMS Information</b> section. In the <b>Avaya Communication Manager Information</b> section, provide the <b>IP Address</b> of Communication Manager procr interface as well as the <b>Username</b> and <b>Password</b> configured in <b>Section 5, Step 5</b>.</p> 

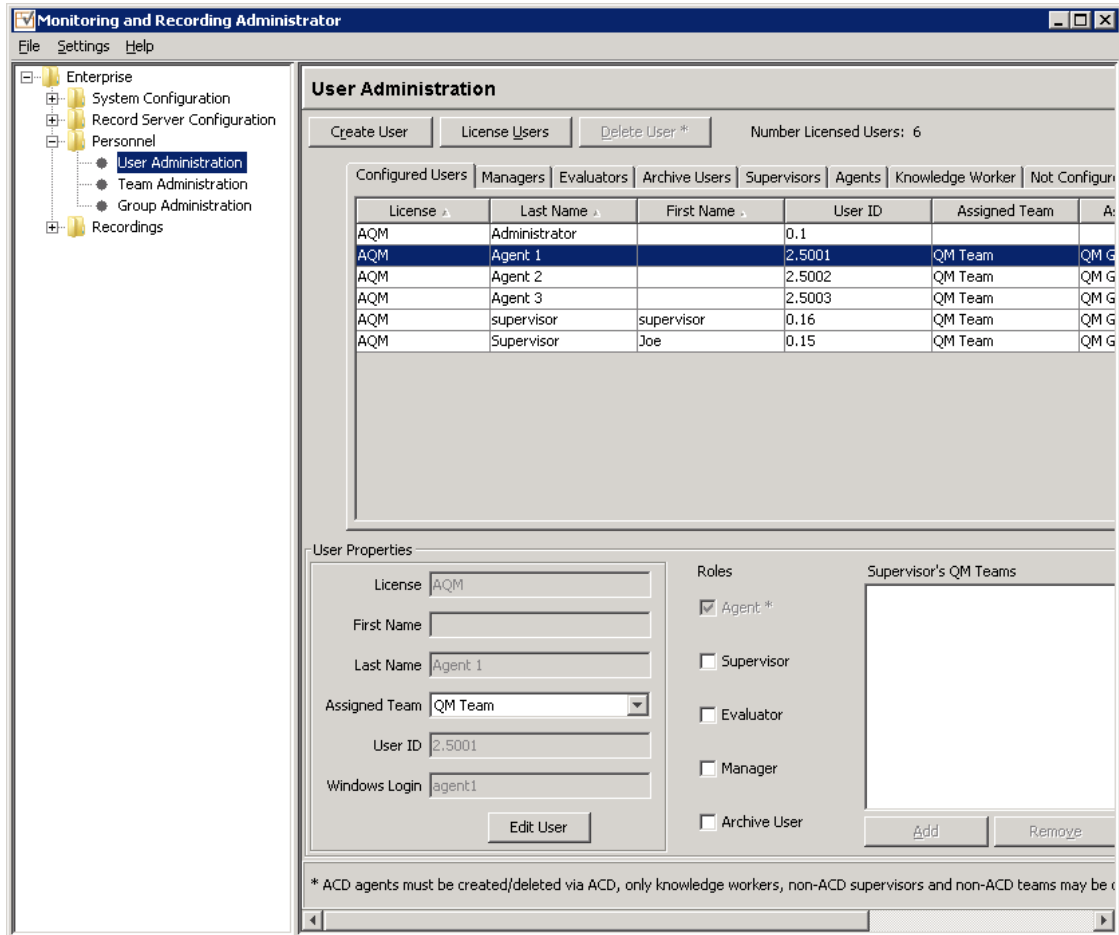
Step	Description
2.	<p data-bbox="280 233 1336 268"><b>Configuration of the Application Enablement Interfaces – DMCC and JTAPI</b></p> <p data-bbox="280 300 1364 443">From the left pane, navigate to <b>Enterprise → System Configuration → Telephony Groups</b>. The <b>Telephony Groups</b> screen is displayed. Click the <b>Add</b> button. In the <b>Telephony Group Configuration</b> window that pops up, enter a <b>Name</b> and select <b>Avaya</b> as the <b>Telephony Group Type</b>. Click <b>OK</b>.</p>  <p>The screenshot shows the 'Monitoring and Recording Administrator' application window. On the left is a tree view with 'Enterprise' expanded, showing 'System Configuration' and 'Telephony Groups' selected. The main pane displays the 'Telephony Groups' configuration screen. It features a table with columns 'Name', 'Telephony Type', and 'Signal Method'. A row with 'Avaya' is highlighted. Below the table is a 'Telephony Group Configuration' dialog box with a 'Name' text field and a 'Telephony Group Type' dropdown menu set to 'Avaya'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. Below the dialog, a note states: 'Note: Avaya systems can only have one telephony group.' There are 'Add', 'Delete', and 'Edit Config' buttons. A checkbox labeled 'Show Gateway Recordings prior to Reconciliation' is also present. At the bottom right of the main window are 'Save' and 'Cancel' buttons.</p>

Step	Description
	<p><b>Configuration of the Application Enablement Interfaces – DMCC (Continued)</b>  The <b>Avaya Configuration</b> screen is displayed. In the <b>AE Services DMCC Information</b> section, provide:</p> <ul style="list-style-type: none"> <li>• <b>Host Name</b> or <b>IP Address</b> of the <b>Application Enablement Services</b> server</li> <li>• <b>Username</b> and <b>Password</b> (from <b>Section 6, Step 4</b>)</li> <li>• <b>4721</b> as the <b>port</b> (the default DMCC listening port)</li> <li>• <b>Device Password</b> for the recorded stations (from <b>Section 5, Step 6</b>). Note that all station passwords must be the same for this solution; however, check with Calabrio for alternatives if necessary.</li> <li>• <b>Switch Name</b> or <b>Switch IP Interface</b>. Enter the switch name or IP address of Communication Manager.</li> </ul> <p>Click <b>OK</b> to complete this step.</p> 

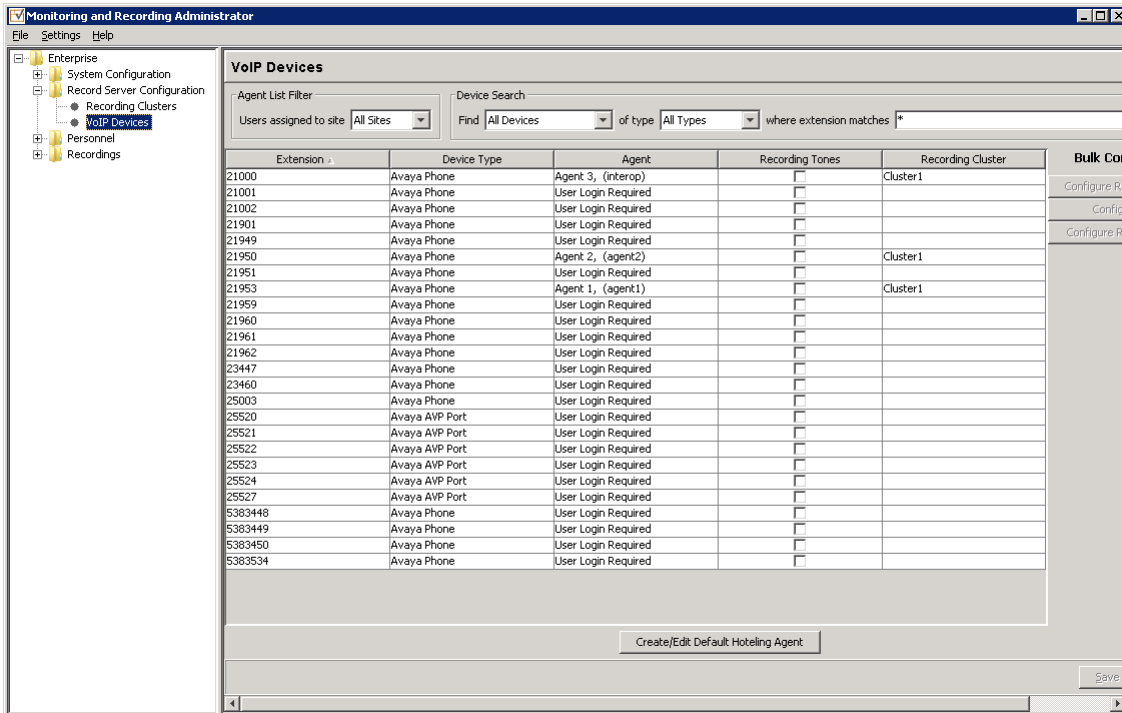


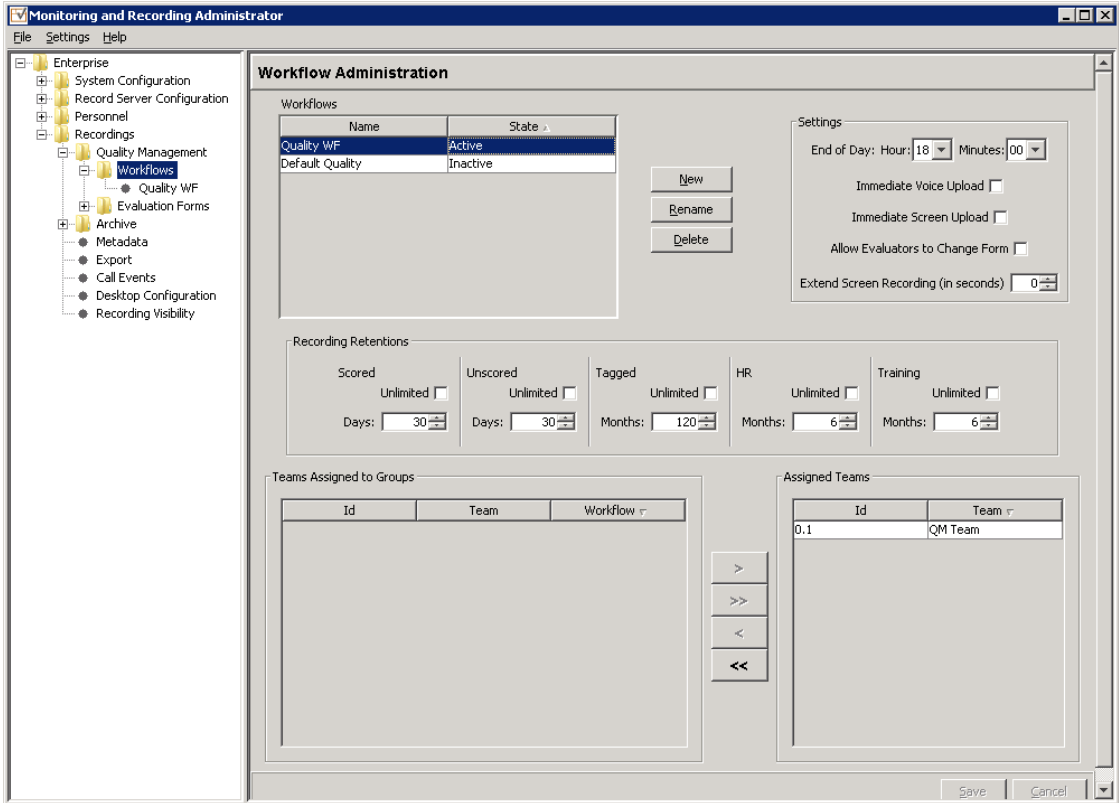
Step	Description																																										
3.	<p><b>Configuration of Users</b></p> <p>Navigate to <b>Enterprise → Personnel → User Administration</b> page to configure users. Once created, users can be statically assigned to a VoIP Device as demonstrated in <b>Step 4</b>.</p>  <table><tr><th>License</th><th>Last Name</th><th>First Name</th><th>User ID</th><th>Assigned Team</th><th></th></tr><tr><td>AQM</td><td>Administrator</td><td></td><td>0.1</td><td></td><td></td></tr><tr><td>AQM</td><td>Agent 1</td><td></td><td>2.5001</td><td>QM Team</td><td>QM</td></tr><tr><td>AQM</td><td>Agent 2</td><td></td><td>2.5002</td><td>QM Team</td><td>QM</td></tr><tr><td>AQM</td><td>Agent 3</td><td></td><td>2.5003</td><td>QM Team</td><td>QM</td></tr><tr><td>AQM</td><td>supervisor</td><td>supervisor</td><td>0.16</td><td>QM Team</td><td>QM</td></tr><tr><td>AQM</td><td>Supervisor</td><td>Joe</td><td>0.15</td><td>QM Team</td><td>QM</td></tr></table>	License	Last Name	First Name	User ID	Assigned Team		AQM	Administrator		0.1			AQM	Agent 1		2.5001	QM Team	QM	AQM	Agent 2		2.5002	QM Team	QM	AQM	Agent 3		2.5003	QM Team	QM	AQM	supervisor	supervisor	0.16	QM Team	QM	AQM	Supervisor	Joe	0.15	QM Team	QM
License	Last Name	First Name	User ID	Assigned Team																																							
AQM	Administrator		0.1																																								
AQM	Agent 1		2.5001	QM Team	QM																																						
AQM	Agent 2		2.5002	QM Team	QM																																						
AQM	Agent 3		2.5003	QM Team	QM																																						
AQM	supervisor	supervisor	0.16	QM Team	QM																																						
AQM	Supervisor	Joe	0.15	QM Team	QM																																						

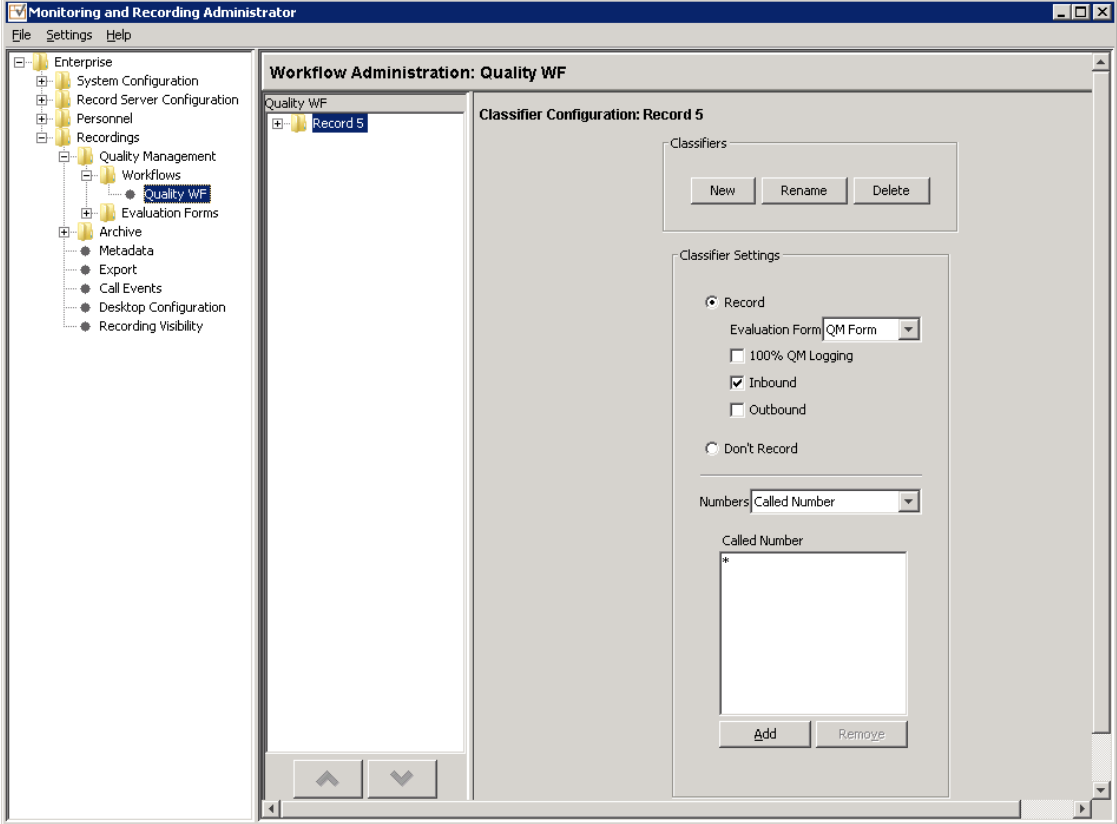
Step	Description
	<p><b>Configuration of Users (Continued)</b></p> <p>Clicking <b>Create User</b> to create a new user. A <b>Create User</b> window pops up. Enter the <b>First Name</b>, <b>Last Name</b>, <b>Windows Login</b>, and <b>QM Password</b>. Click <b>OK</b>.</p> <p>Note: CRQM also automatically populates the Agent list under the <b>Agent</b> tab based upon the agents configured in Communication Manager. The administrator can edit an agent using the <b>Edit User</b> button as an alternative way to create a user.</p> <p>If Screen Recording is required for a user, the <b>Windows Login</b> and <b>QM Password</b> configured for the user have to match the login and password of the PC that the user uses.</p> 

Step	Description																																										
	<p><b>Configuration of Users (Continued)</b></p> <p>The user appears in the list. Check one of the checkboxes (e.g. Agent) under the <b>Roles</b> section and select a pre-configured team from the dropdown list of the <b>Assigned Team</b> field.</p>  <p>The screenshot displays the 'Monitoring and Recording Administrator' application. On the left is a tree view with 'Enterprise' expanded, showing 'System Configuration', 'Record Server Configuration', 'Personnel', 'User Administration' (selected), 'Team Administration', 'Group Administration', and 'Recordings'. The main area is titled 'User Administration' and includes buttons for 'Create User', 'License Users', and 'Delete User *'. It shows 'Number Licensed Users: 6'. Below is a tabbed interface with 'Configured Users' selected, displaying a table of users:</p> <table><tr><th>License</th><th>Last Name</th><th>First Name</th><th>User ID</th><th>Assigned Team</th><th>Actions</th></tr><tr><td>AQM</td><td>Administrator</td><td></td><td>0.1</td><td></td><td></td></tr><tr><td>AQM</td><td>Agent 1</td><td></td><td>2.5001</td><td>QM Team</td><td>QM G</td></tr><tr><td>AQM</td><td>Agent 2</td><td></td><td>2.5002</td><td>QM Team</td><td>QM G</td></tr><tr><td>AQM</td><td>Agent 3</td><td></td><td>2.5003</td><td>QM Team</td><td>QM G</td></tr><tr><td>AQM</td><td>supervisor</td><td>supervisor</td><td>0.16</td><td>QM Team</td><td>QM G</td></tr><tr><td>AQM</td><td>Supervisor</td><td>Joe</td><td>0.15</td><td>QM Team</td><td>QM G</td></tr></table> <p>Below the table is the 'User Properties' section for the selected user 'Agent 1'. It includes fields for License (AQM), First Name, Last Name (Agent 1), Assigned Team (QM Team), User ID (2.5001), and Windows Login (agent1). The 'Roles' section has checkboxes for Agent * (checked), Supervisor, Evaluator, Manager, and Archive User. The 'Supervisor's QM Teams' section is empty. Buttons for 'Edit User', 'Add', and 'Remove' are present. A note at the bottom states: '* ACD agents must be created/deleted via ACD, only knowledge workers, non-ACD supervisors and non-ACD teams may be created'.</p>	License	Last Name	First Name	User ID	Assigned Team	Actions	AQM	Administrator		0.1			AQM	Agent 1		2.5001	QM Team	QM G	AQM	Agent 2		2.5002	QM Team	QM G	AQM	Agent 3		2.5003	QM Team	QM G	AQM	supervisor	supervisor	0.16	QM Team	QM G	AQM	Supervisor	Joe	0.15	QM Team	QM G
License	Last Name	First Name	User ID	Assigned Team	Actions																																						
AQM	Administrator		0.1																																								
AQM	Agent 1		2.5001	QM Team	QM G																																						
AQM	Agent 2		2.5002	QM Team	QM G																																						
AQM	Agent 3		2.5003	QM Team	QM G																																						
AQM	supervisor	supervisor	0.16	QM Team	QM G																																						
AQM	Supervisor	Joe	0.15	QM Team	QM G																																						

Step	Description																																										
	<p><b>Configuration of Users (Continued)</b></p> <p>Click the <b>License Users</b> button at the top to display the <b>Licensed/Unlicense Users</b> window. Use the <b>AQM</b> and <b>Unlicensed</b> buttons to set the license mode.</p> <div><div>License/Unlicense Users</div><table><thead><tr><th>AQM ▾</th><th>Unlicensed ▾</th><th>Last Name ▾</th><th>First Name</th><th>Team</th><th>Windows Lo...</th></tr></thead><tbody><tr><td><input checked="" type="radio"/></td><td><input type="radio"/></td><td>Administrator</td><td></td><td></td><td>administrator</td></tr><tr><td><input checked="" type="radio"/></td><td><input type="radio"/></td><td>Agent 1</td><td></td><td>QM Team</td><td>agent1</td></tr><tr><td><input checked="" type="radio"/></td><td><input type="radio"/></td><td>Agent 2</td><td></td><td>QM Team</td><td>agent2</td></tr><tr><td><input checked="" type="radio"/></td><td><input type="radio"/></td><td>Agent 3</td><td></td><td>QM Team</td><td>interop</td></tr><tr><td><input checked="" type="radio"/></td><td><input type="radio"/></td><td>supervisor</td><td>supervisor</td><td>QM Team</td><td>supervisor1</td></tr><tr><td><input checked="" type="radio"/></td><td><input type="radio"/></td><td>Supervisor</td><td>Joe</td><td>QM Team</td><td>supervisor</td></tr></tbody></table><div><div>AQM</div><div>Unlicensed</div><div>OK</div><div>Cancel</div></div></div>	AQM ▾	Unlicensed ▾	Last Name ▾	First Name	Team	Windows Lo...	<input checked="" type="radio"/>	<input type="radio"/>	Administrator			administrator	<input checked="" type="radio"/>	<input type="radio"/>	Agent 1		QM Team	agent1	<input checked="" type="radio"/>	<input type="radio"/>	Agent 2		QM Team	agent2	<input checked="" type="radio"/>	<input type="radio"/>	Agent 3		QM Team	interop	<input checked="" type="radio"/>	<input type="radio"/>	supervisor	supervisor	QM Team	supervisor1	<input checked="" type="radio"/>	<input type="radio"/>	Supervisor	Joe	QM Team	supervisor
AQM ▾	Unlicensed ▾	Last Name ▾	First Name	Team	Windows Lo...																																						
<input checked="" type="radio"/>	<input type="radio"/>	Administrator			administrator																																						
<input checked="" type="radio"/>	<input type="radio"/>	Agent 1		QM Team	agent1																																						
<input checked="" type="radio"/>	<input type="radio"/>	Agent 2		QM Team	agent2																																						
<input checked="" type="radio"/>	<input type="radio"/>	Agent 3		QM Team	interop																																						
<input checked="" type="radio"/>	<input type="radio"/>	supervisor	supervisor	QM Team	supervisor1																																						
<input checked="" type="radio"/>	<input type="radio"/>	Supervisor	Joe	QM Team	supervisor																																						

Step	Description
4.	<p><b>Configuration of Devices</b></p> <p>Navigate to <b>Enterprise → Record Server Configuration → VoIP Devices</b> to configure devices.</p> <p>When the SMS query completes, all stations from Communication Manager are listed on the <b>VoIP Devices</b> page. A device is designated to be recorded by assigning a pre-configured <b>Recording Cluster</b> (e.g. rc1) on the <b>VoIP Devices</b> page, and then assigning an <b>Agent</b> to that device using dropdown lists in each column. The agent dropdown list includes the users configured on the <b>User Administration</b> page in <b>Step 3</b> that have the AQM license assigned.</p> <p>Click <b>Save</b> to complete this step.</p> 

Step	Description
5.	<p><b>Configuration of Recording Schedules (Workflows)</b></p> <p>Navigate to the <b>Recordings → Quality Management → Workflows</b> page. Click the <b>New</b> button to create a Workflow. Enter a name for the new workflow and click <b>OK</b>. To assign the workflow to a team, select a team from the <b>Teams Assigned to Groups</b> list on the bottom left of the page, and click the &gt; button to move that group into the <b>Assigned Teams</b> for the workflow.</p> <p>Click on <b>Save</b> (not shown) to complete this step.</p> 

Step	Description
	<p><b>Configuration of Recording Schedules (Workflows) - Continued</b></p> <p>Click the newly created Workflow in the left pane to edit the details of the schedule. For the Compliance Test, the <b>Inbound</b> and <b>Outbound</b> checkboxes are checked to enable recording for inbound and outbound calls. In addition, the <b>100% QM Logging</b> checkbox is checked to enable screen recording. If an <b>Evaluation Form</b> 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

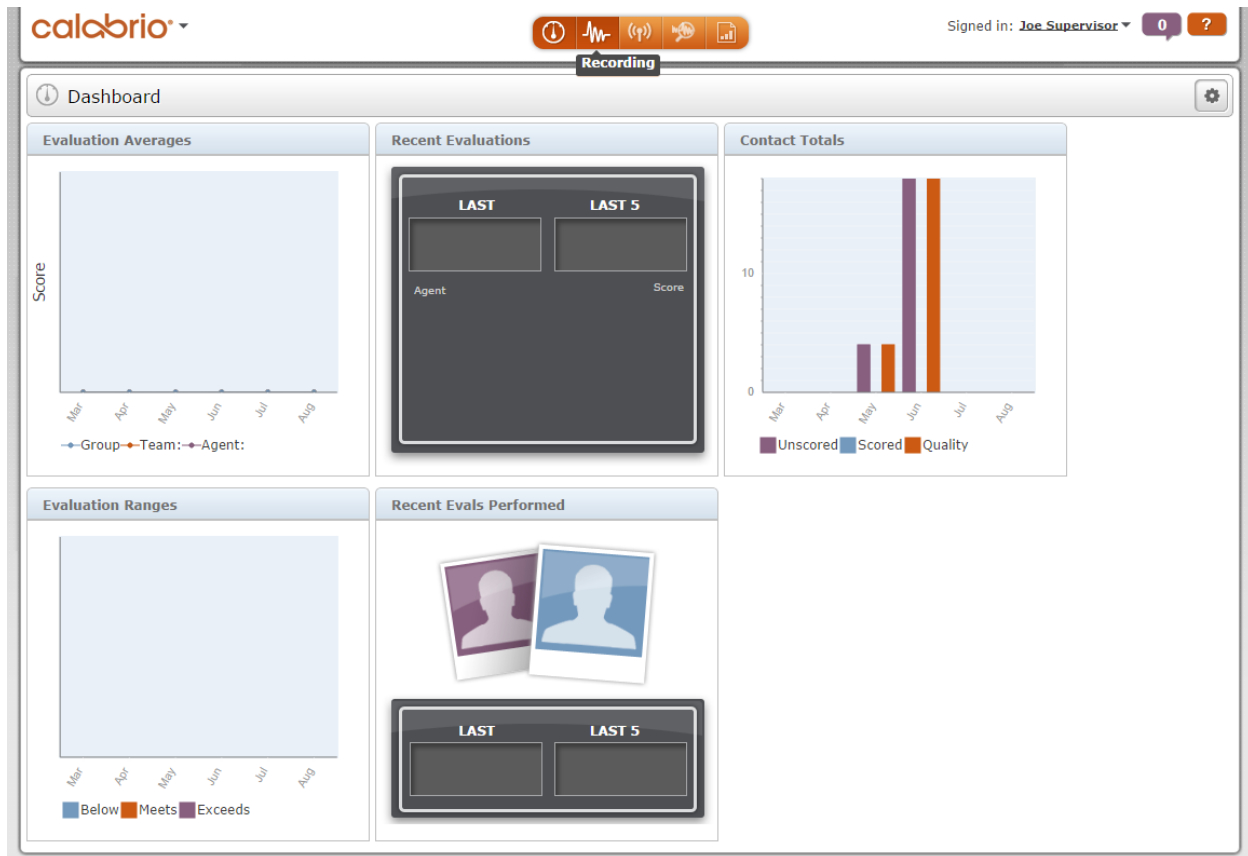
Access the Calabrio web-based user interface using the URL **http://<ip-address>** in a browser window, where **<ip-address>** is the address of the CRQM server. The **Log In** screen is displayed as shown below. Use appropriate credentials to log in.



The image shows the Calabrio login interface. At the top, the Calabrio logo is displayed in orange, followed by the tagline "There's no end to better." and a large orange circle containing the number "1". Below this, there is a login form with two input fields: "Username" with the text "administrator" and "Password" with a single dot. A "Language" dropdown menu is set to "English". At the bottom of the form, there is a link "Validate my PC configuration" with a right-pointing arrow, and a "Login" button.



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.

Signed in: **Joe Supervisor** 0 ?

**Recordings**

AQP:0%

ATT:15 secs

Total:38

New or Refine Search

1 of 2

20

Last Name	First Name	Group Name	Team Name	Contact ID	Calling Number	Called Number	Date	Time	Time Zone	Score
Agent 1		QM Group	QM Team	44	21953	21949	7/17/14	12:47 PM	America/Denver	
Agent 1		QM Group	QM Team	43	21953	21951	7/11/14	01:37 PM	America/Denver	
Agent 1		QM Group	QM Team	42	21953	21949	7/11/14	01:35 PM	America/Denver	
Agent 1		QM Group	QM Team	41	21953	21949	7/9/14	03:04 PM	America/Denver	
Agent 1		QM Group	QM Team	40	7209772637	17209772872	6/26/14	02:34 PM	America/Denver	
Agent 1		QM Group	QM Team	39	7209772637	17209772872	6/26/14	02:34 PM	America/Denver	
Agent 1		QM Group	QM Team	38	7209772637	17209772872	6/26/14	02:33 PM	America/Denver	
Agent 1		QM Group	QM Team	37	7209772637	17209772872	6/26/14	02:33 PM	America/Denver	
Agent 1		QM Group	QM Team	36	7209772636	17209772872	6/26/14	02:31 PM	America/Denver	
Agent 1		QM Group	QM Team	35	7209772637	17209772872	6/26/14	02:25 PM	America/Denver	
Agent 1		QM Group	QM Team	34	21000	21953	6/26/14	02:23 PM	America/Denver	
Agent 3		QM Group	QM Team	33	7209772636	17209772872	6/26/14	02:23 PM	America/Denver	
Agent 3		QM Group	QM Team	32	7209772637	17209772872	6/26/14	12:29 PM	America/Denver	
Agent 3		QM Group	QM Team	31	7209772637	21951	6/26/14	11:55 AM	America/Denver	
Agent 2		QM Group	QM Team	30	7209772637	17209772872	6/26/14	11:55 AM	America/Denver	
Agent 2		QM Group	QM Team	29	7209772637	17209772872	6/26/14	11:54 AM	America/Denver	
Agent 2		QM Group	QM Team	28	7209772637	17209772872	6/26/14	11:53 AM	America/Denver	
Agent 2		QM Group	QM Team	27	7209772636	17209772872	6/26/14	11:50 AM	America/Denver	
Agent 2		QM Group	QM Team	26	7209772637	17209772872	6/26/14	11:36 AM	America/Denver	
Agent 2		QM Group	QM Team	23	T311	17209772872	6/26/14	11:34 AM	America/Denver	

© 2008-2014 Calabrio, Inc. All rights reserved.

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

calabrio®

Signed in: Joe Supervisor 0 ?

Recordings AQP:0% ATT:15 secs Total:38

New or Refine Search

Last Name	First Name	Group Name	Team Name	Contact ID	Calling Number	Called Number	Date	Time	Time Zone	Score
Agent 1		QM Group	QM Team	44	21953	21949	7/17/14	12:47 PM	America/Denver	
Agent 1		QM Group	QM Team	43	21953	21951	7/11/14	01:37 PM	America/Denver	
Agent 1		QM Group	QM Team	42	21953	21949	7/11/14	01:35 PM	America/Denver	
Agent 1		QM Group	QM Team	41	21953	21949	7/9/14	03:04 PM	America/Denver	
Agent 1		QM Group	QM Team	40	7209772637	17209772872	6/26/14	02:34 PM	America/Denver	
Agent 1		QM Group	QM Team	39	7209772637	17209772872	6/26/14	02:34 PM	America/Denver	
Agent 1		QM Group	QM Team	38	7209772637	17209772872	6/26/14	02:33 PM	America/Denver	
Agent 1		QM Group	QM Team	37	7209772637	17209772872	6/26/14	02:33 PM	America/Denver	
Agent 1		QM Group	QM Team	36	7209772636	17209772872	6/26/14	02:31 PM	America/Denver	
Agent 1		QM Group	QM Team	35	7209772637	17209772872	6/26/14	02:25 PM	America/Denver	
Agent 1		QM Group	QM Team	34	21000	21953	6/26/14	02:23 PM	America/Denver	
Agent 1		QM Group	QM Team	33	7209772636	17209772872	6/26/14	02:23 PM	America/Denver	
Agent 3		QM Group	QM Team	32	7209772637	17209772872	6/26/14	12:29 PM	America/Denver	
Agent 3		QM Group	QM Team	31	7209772637	21951	6/26/14	11:55 AM	America/Denver	
Agent 2		QM Group	QM Team	30	7209772637	17209772872	6/26/14	11:55 AM	America/Denver	
Agent 2		QM Group	QM Team	29	7209772637	17209772872	6/26/14	11:54 AM	America/Denver	
Agent 2		QM Group	QM Team	28	7209772637	17209772872	6/26/14	11:53 AM	America/Denver	
Agent 2		QM Group	QM Team	27	7209772636	17209772872	6/26/14	11:50 AM	America/Denver	
Agent 2		QM Group	QM Team	26	7209772637	17209772872	6/26/14	11:36 AM	America/Denver	
Agent 2		QM Group	QM Team	23	T311	17209772872	6/26/14	11:34 AM	America/Denver	

© 2008-2014 Calabrio, Inc. All rights reserved.

Contact Information Associated Contacts

00:00:00 00:00:05

Play/Pause

⏮ ⏪ ⏩ ⏭ 🔍 1:1 🔊

## 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, June 2014, Document Number 03-300509.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014

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

---

**©2014 Avaya Inc. All Rights Reserved.**

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

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