Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio Call Recording and Quality Management with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Application Enablement Services R6.2 – 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 R6.2 and Avaya Aura® Application Enablement Services R6.2.

Calabrio Call Recording and Quality Management (CRQM) uses the Avaya Aura® Application Enablement Services JTAPI and 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.

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.

©2013 Avaya Inc. All Rights Reserved.

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), Device, Media and Call Control (DMCC), and JTAPI, the recorder is able to register with Avaya Aura® Communication Manager as an IP softphone and use various methods to capture audio from targeted agent's phone, with JTAPI providing call tagging data.

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.

CRQM supports two types of recording methods. For stations that are administered with IP Softphone enabled in Avaya Aura® Communication Manager, CRQM registers with Avaya Aura® Communication Manager using the Independent Registration mode of the DMCC Multiple Registration service. Once DMCC registration is successfully completed, Avaya Aura® Communication Manager will send audio for all calls that originate or terminate on the registered stations to both the phone, and the recorder.

For stations that do not have IP Softphone enabled in Avaya Aura® Communication Manager, including all station types such as SIP, IP, Digital or analog, CRQM uses dedicated, virtual stations in Avaya Aura® Communication Manager to add to calls via the Single Step Conference JTAPI method.

To ensure call records stored in the database are as rich as possible, the application uses the JTAPI capabilities of Avaya Aura® Application Enablement Services to monitor the station activity. This occurs following successful DMCC registrations. If DMCC registration fails, the JTAPI associations are not requested by the application.

©2013 Avaya Inc. All Rights Reserved.

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 as well as four types of codecs (G.711µ, G.711A, G.729, G.729A) 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 with two observations which are described below.

- For some transfer and conferencing tests, though all call legs were recorded, information for originating calling party (calling party number) was not recorded correctly.
- After Communication Manager was rebooted, some DMCC Multiple Registration endpoints were unregistered from Communication Manager. As a result, no subsequent recording could be done for those endpoints. Calabrio has provided a patch which re-registers such endpoints once they have handled a new call. The call that triggers the re-registration will not get recorded though.
- CRQM supports four types of codecs. However, only one is active at a time and a database command is required for a codec change. In addition, the codec used by CRQM needs to be included in the codec set configured at the Communication Manager side. Otherwise, no recording will be generated.

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

©2013 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager R6.2
- Avaya Aura® Application Enablement Services R6.2
- 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.

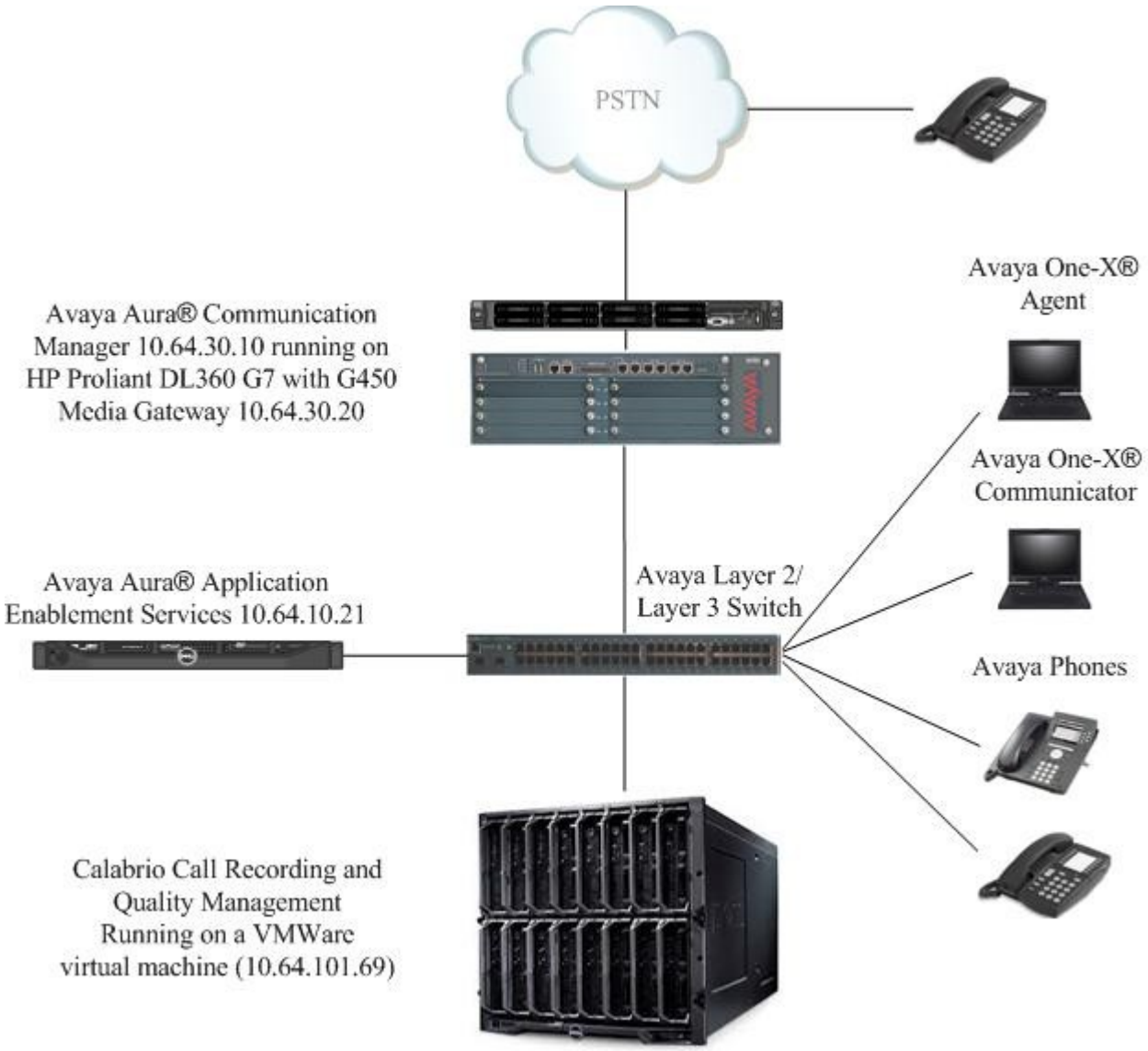


Figure 1 – Calabrio CRQM Compliance Test Configuration

©2013 Avaya Inc. All Rights Reserved.

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	6.2 (0.2.0.823.0) SP5 (patch 20396)
Avaya G450 Media Gateway • 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	6.2 (r6-2-0-18-0) Patch 1
Avaya 9600 Series IP Telephone • 9640 (H.323)	3.1.5
Avaya 96x1 Series IP Telephone • 9641 (H.323)	6.2.2
Avaya 2420 Digital Telephones	-
2500 analog phone	-
Desktop PC running Avaya One-X® Communicator	6.1.7
Desktop PC running Avaya One-X® Agent	2.5
Calabrio Recording and Quality Management running under Windows 2008 R2 Server on a VMWare virtual machine JTAPI/DMCC SDK	9.1 SP1 ES1 6.2

©2013 Avaya Inc. All Rights Reserved.

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**.

©2013 Avaya Inc. All Rights Reserved.

Step	Description
1.	**Verify Feature and License for the integration** Enter the **display system-parameters customer-options** command and ensure that **Computer Telephony Adjunct Links** is set to **y.** Applications that use Application Enablement Services JTAPI/TSAPI must have **Computer Telephony Adjunct Links** enabled on Communication Manager. This Communication Manager feature entitlement is provided with each JTPAI/TSAPI license. JTAPI/TSAPI entitlements must be activated in both the Communication Manager and Application Enablement Services licenses. If this option is not set to **y**, contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                      Page   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  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  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
```

Each recording port or virtual station extension the recorder will use to record agent phones will require an **IP_API_A** license if not licensed on Application Enablement Services.

```
diaplay system-parameters customer-options                      Page  10 of  11
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
AgentSC     *  : 10000          0
IP_API_A    *  : 18000          0
```


©2013 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Administer Communication Manager System Features** Enter the **change system-parameters features** command and ensure that on page 5 **Create Universal Call ID (UCID)** is enabled and a relevant **UCID Network Node ID** (**1** was used in the test) is defined. Also ensure that on page 13 that **Send UCID to ASAI** is set to **y**. CRQM relies on UCID to track complex calls (Transfers and Conferences).

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

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

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

```
change system-parameters features                                Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

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

  ASAI
           Copy ASAI UUI During Conference/Transfer? n
        Call Classification After Answer Supervision? n
                                  Send UCID to ASAI? y
          For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
```


©2013 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Administer IP-Services for Application Enablement Services** Add an IP-Services entry for Application Enablement Services as described below: • Enter the **change ip-services** command. • In the **Service Type** field, type **AESVCS**. • In the **Enabled** field, type **y**. • In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface. • In the **Local Port** field, use the default of **8765**. • Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration. change ip-services Page 1 of 4 IP SERVICES Service Type / Enabled / Local Node / Local Port / Remote Node / Remote Port **AESVCS y procr 8765** On Page 4 of the IP Services form, enter the following values: • In the **AE Services Server** field, type the host name of the Application Enablement Services server. • In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6**, **Step 1**. • In the **Enabled** field, type **y**. change ip-services Page 4 of 4 AE Services Administration Server ID / AE Services Server / Password / Enabled / Status **1: aes6_tr1 xxxxxx y**

©2013 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Administer Computer Telephony Integration (CTI) Link** Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number. • In the **Extension** field, type a valid station extension. • In the **Type** field, type **ADJ-IP**. • In the **Name** field, type a descriptive name. add cti-link 1 Page 1 of 3 CTI LINK **CTI Link: 1** **Extension: 21900** **Type: ADJ-IP** COR: 1 **Name: to AES_10_21**
5.	**Add SMS User Account** CRQM uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application. A privileged user was used in this test; however, a local administrator would want to restrict the user account. This involves creating a user profile at the SAT, and then creating and assigning that user to the profile in the web admin pages. To illustrate, the **add user-profile-by-category 31** command was used to create the profile used in the test as shown below. The **Shell Access**, **Call Center B** and **Stations M** fields were set to **y**. add user-profile-by-category 31 Page 1 of 39 USER PROFILE 31 User Profile Name: Calabrio SMS This Profile is Disabled? n **Shell Access? y** Facility Test Call Notification? n Acknowledgement Required? n Grant Un-owned Permissions? n Extended Profile? n Name Cat Enbl Name Cat Enbl Adjuncts A n Routing and Dial Plan J n **Call Center B y** Security K n Features C n Servers L n Hardware D n **Stations M y** Hospitality E n System Parameters N n IP F n Translations O n Maintenance G n Trunking P n Measurements and Performance H n Usage Q n Remote Access I n User Access R n

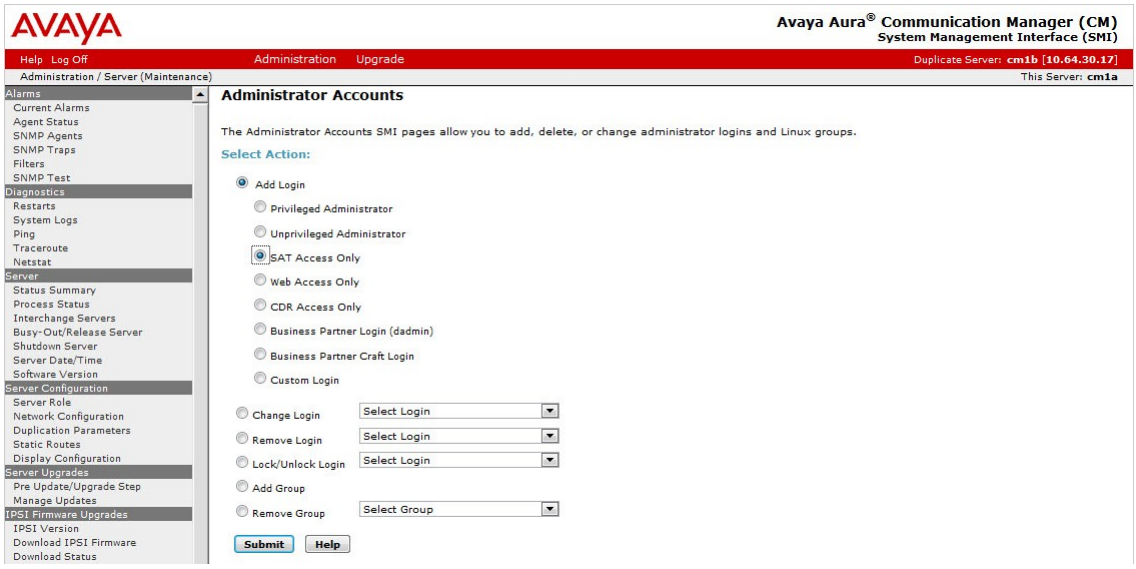
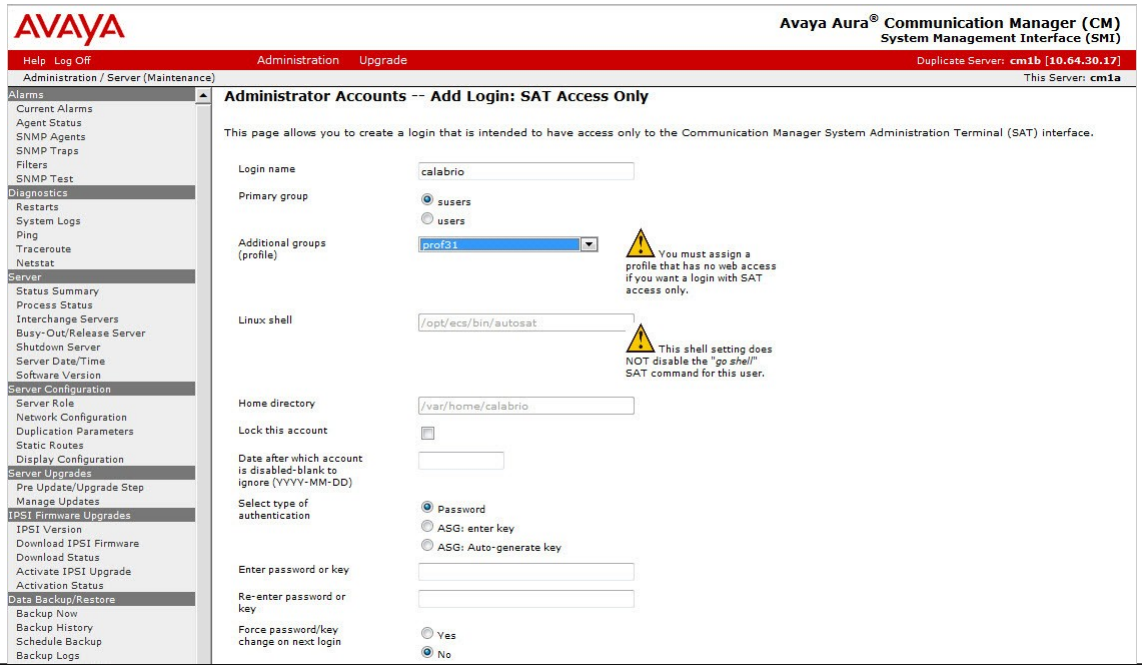
©2013 Avaya Inc. All Rights Reserved.

Step	Description
	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.

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

```
change user-profile-by-category 31                                Page  29 of  39
                    USER PROFILE BY CATEGORY 31
 Set Permissions For Category: M  To: r-       Set All Permissions To:
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                              ess L    --
                    ess clusters L    --
              ess port-networks L    --
                              lsp L    --
                  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-
```


©2013 Avaya Inc. All Rights Reserved.

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**. 

©2013 Avaya Inc. All Rights Reserved.

Step	Description
6.	**Verify Recorded Extensions** 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.

```
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
                                              Message Lamp Ext: 21949
           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
```


©2013 Avaya Inc. All Rights Reserved.

Step	Description
7.	**Add Virtual Stations** 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 **the add station <n>** command, where **<n>** is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields. • In the **Type** field, enter a station type such as **9640** • In the **Name** field, enter a name containing the **DMCC** string (e.g. **DMCC station 2**). CRQM uses the DMCC string to identify virtual stations. • In the **Security Code** field, enter a desired value. • Set the **IP SoftPhone** field to **y**

```
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
```

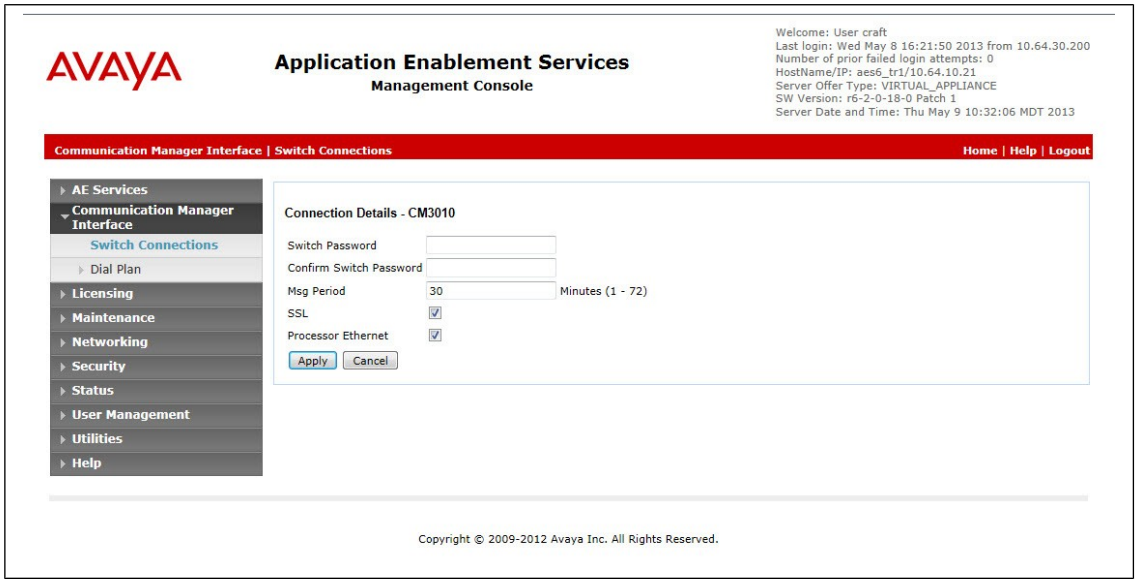
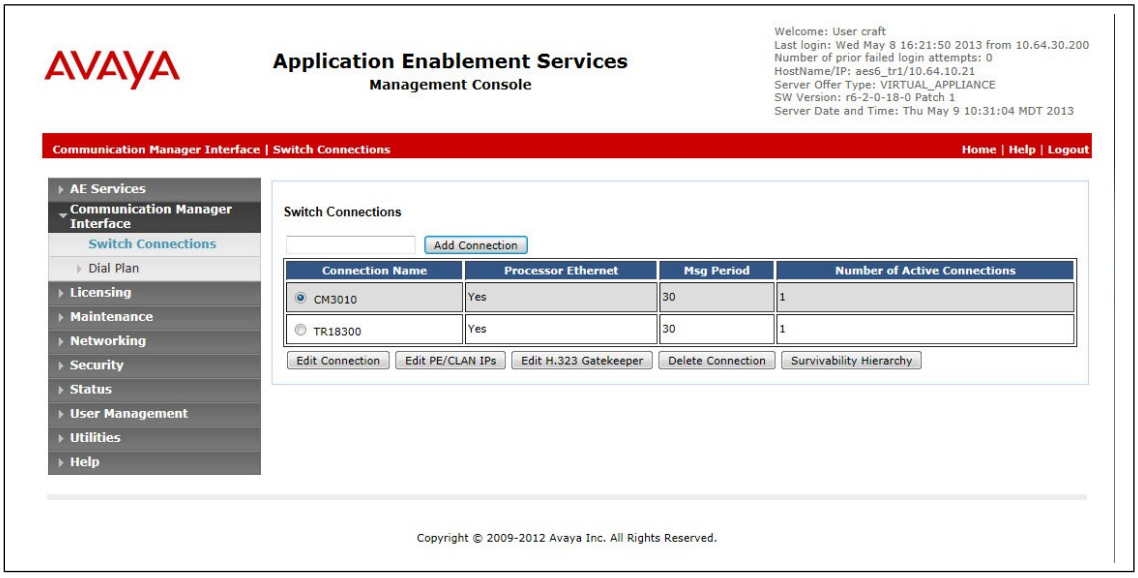

©2013 Avaya Inc. All Rights Reserved.

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.

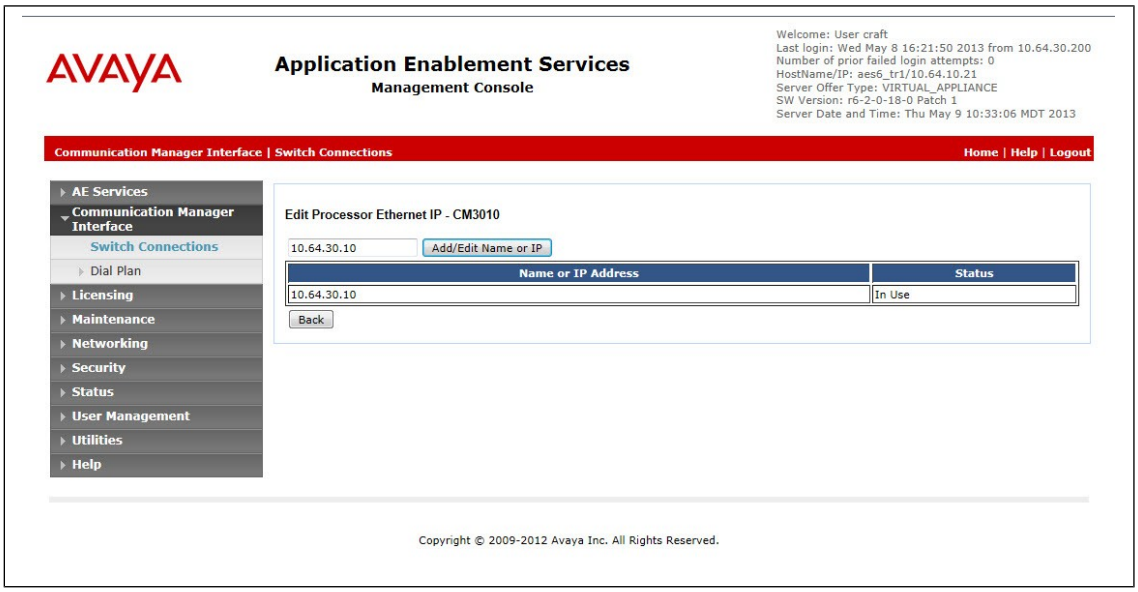
The procedures fall into the following areas:

- 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
- Restart TSAPI Service

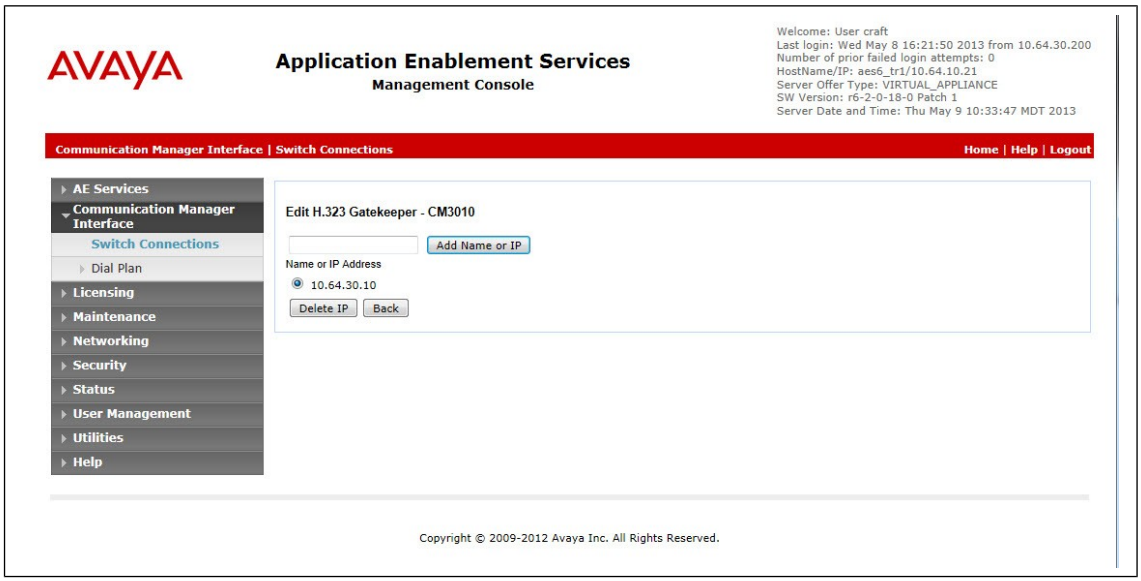
Step	Description
1.	**Configure Communication Manager Switch Connections** To add links to Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection (e.g. **CM3010**) and click the **Add Connection** button (not 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**.  The display returns to the **Switch Connections** screen which shows that the **CM3010** switch connection has been added. 

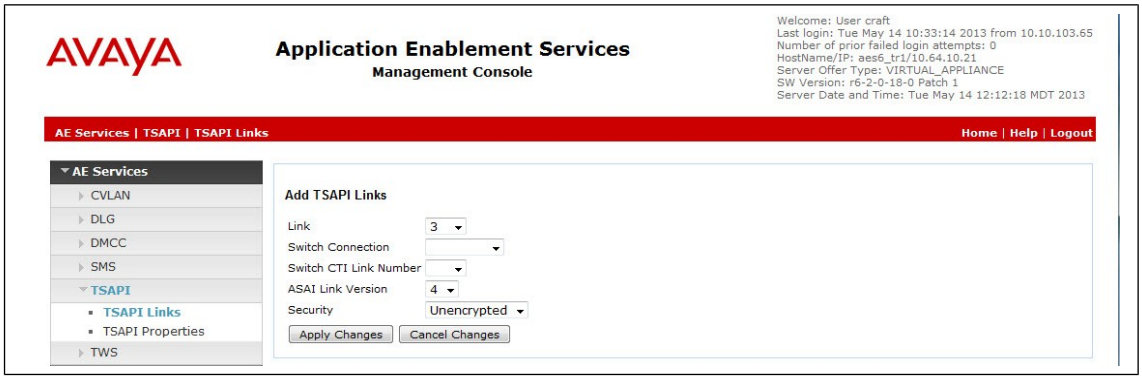
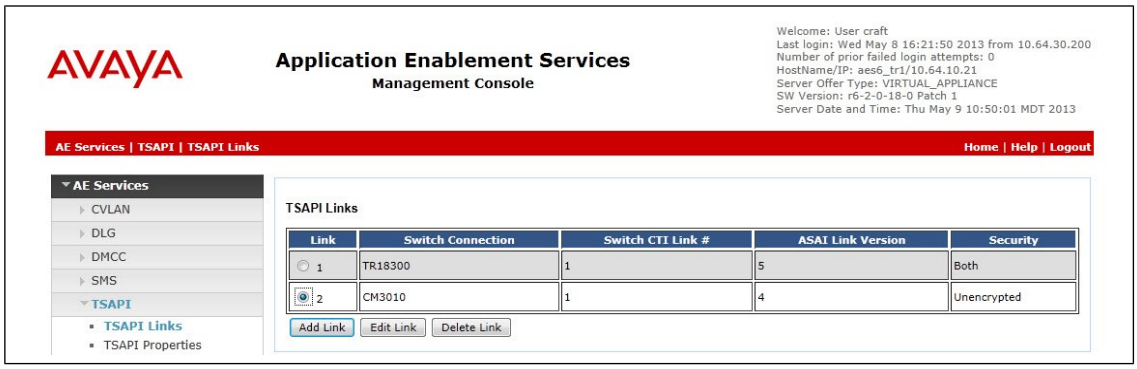
©2013 Avaya Inc. All Rights Reserved.

Step	Description
	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.

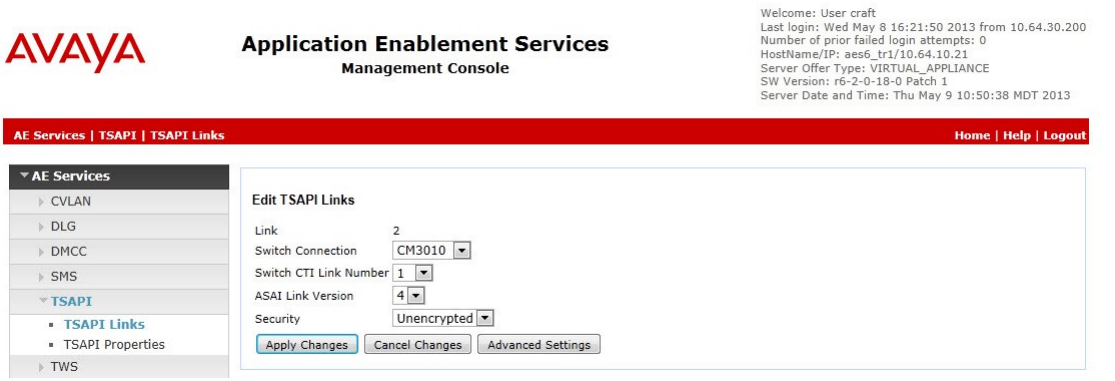
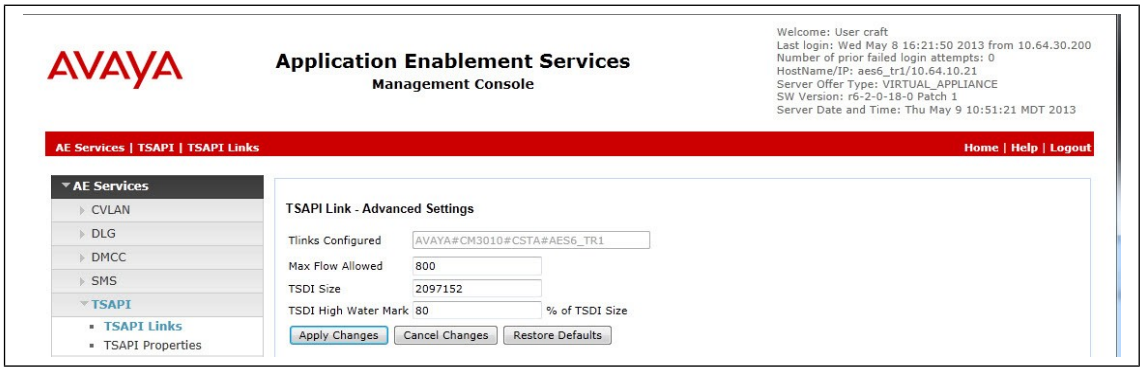


Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.

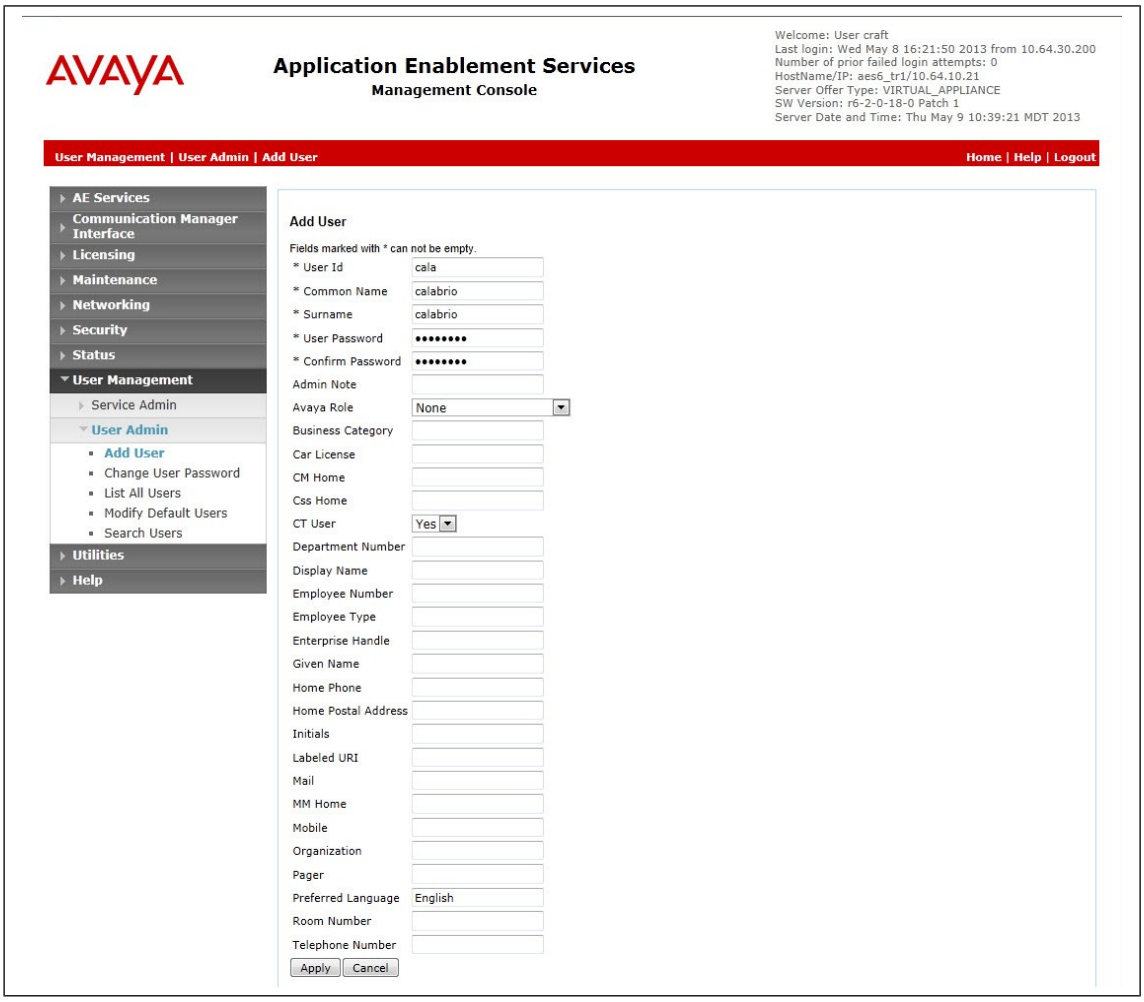


Step	Description
2.	**Add TSAPI Links** Navigate to the **AE Services →TSAPI → TSAPI Links** page to add a TSAPI CTI Link. Click **Add Link** (not shown). Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form in **Section 5**, **Step 4**. Select **Unencrypted** in the **Security** field. Click **Apply Changes**.  It returns to the **TSAPI Links** screen which shows that the **CM3010** link has been added. 

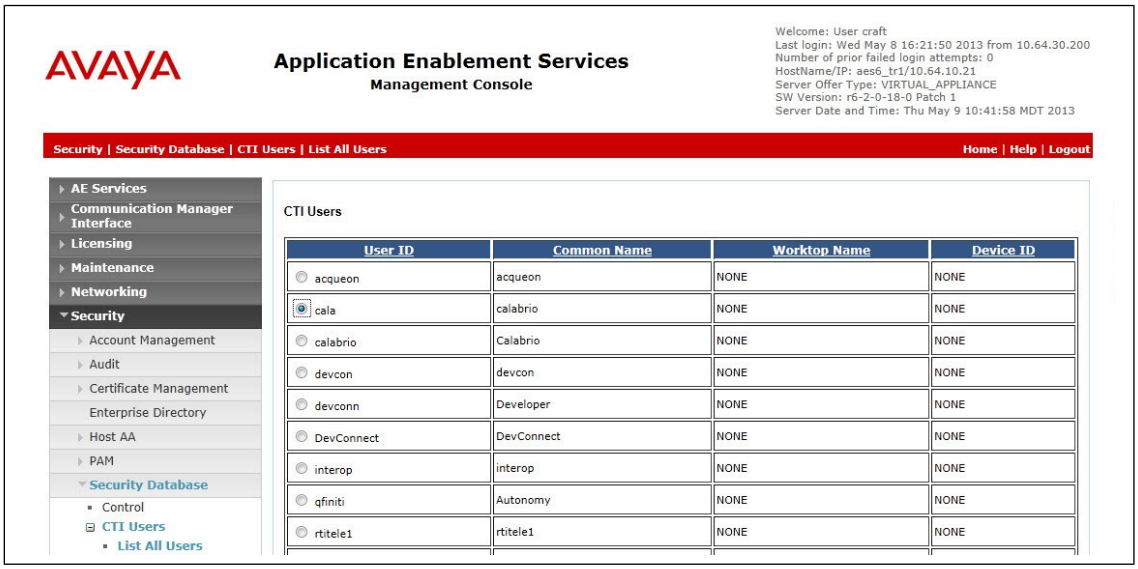
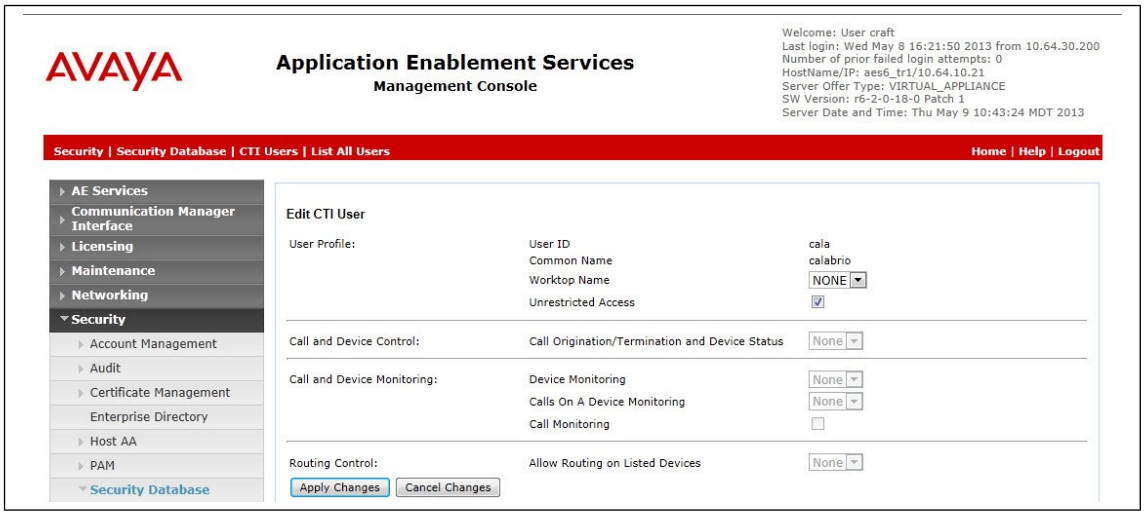
©2013 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Note the TLink Information** Select the **CM3010** TSAPI Link and click **Edit Link**. The **Edit TSAPI Links** screen is displayed.  Click the **Advanced Settings** button. The **TSAPI Link – Advanced Settings** screen is displayed. Note the value in the **Tlinks Configured** field which will be used for CRQM configuration in **Section 7**. 

©2013 Avaya Inc. All Rights Reserved.

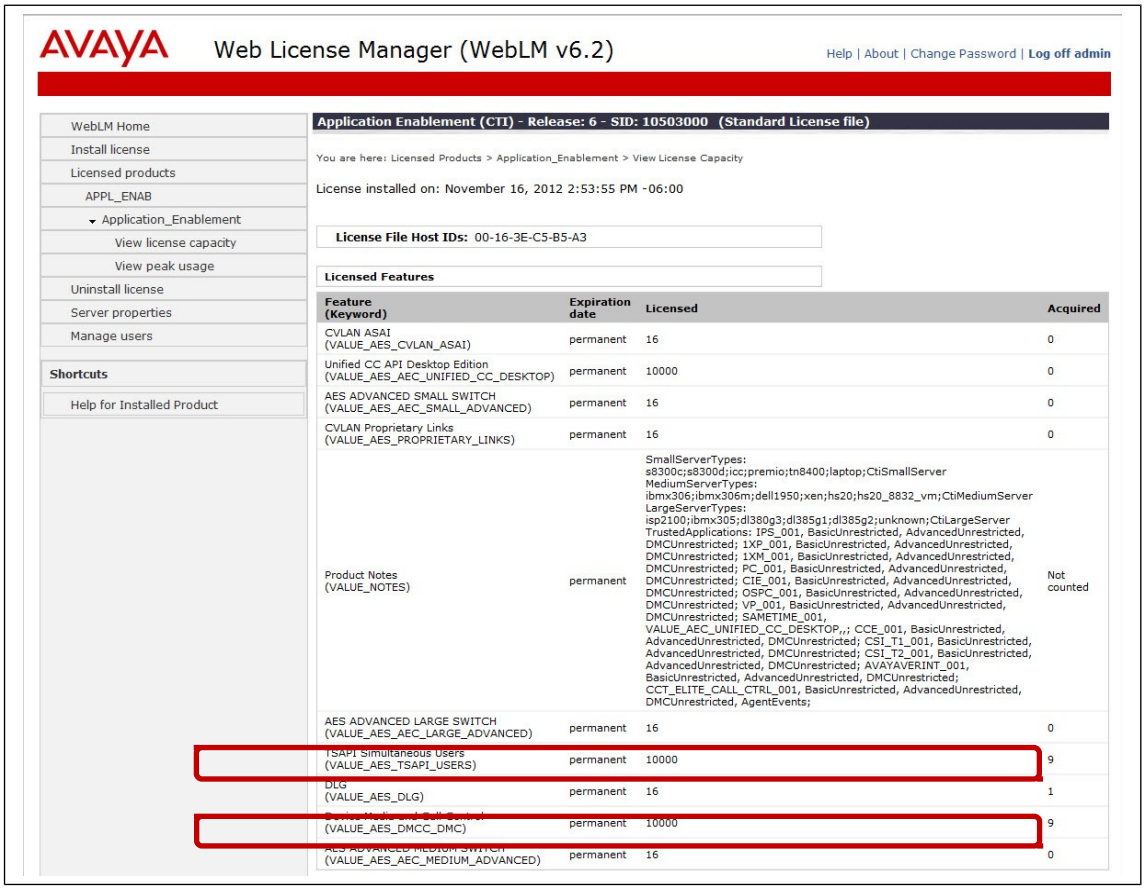
Step	Description
4.	**Configure Calabrio user** In the Navigation Panel, select **User Management → User Admin → Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id, Common Name, Surname,** and **User Password**. Select **Yes** from the **CT User** dropdown list. Click **Apply** at the bottom of the pages to save the entries. 

©2013 Avaya Inc. All Rights Reserved.

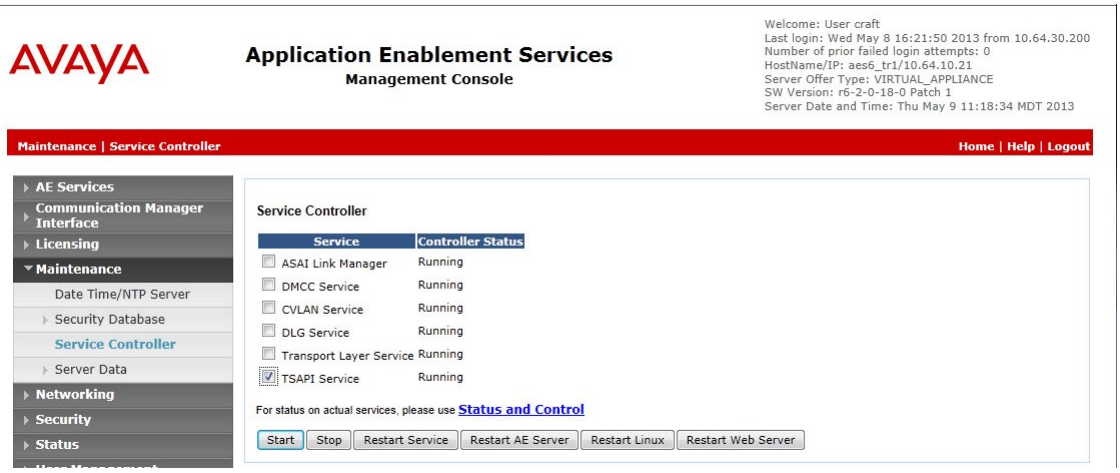
Step	Description
5.	**Enable Unrestricted Access for Calabrio User** If the Security Database (SDB) is enabled on Application Enablement Services, set the calabrio user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step 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. 

©2013 Avaya Inc. All Rights Reserved.

Step	Description
6.	**Confirm TSAPI and DMCC Licenses** CRQM uses a DMCC (**VALUE_AES_DMCC_DMC**) license for each recording port. Additionally, a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license is used for each agent station being monitored. If **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. From the left pane menu on Application Enablement Services Management Console, click **Licensing → WebLM Server Access**. A **Web License Manager** login window is displayed. Enter proper credentials to log in. Click **Licensed products → APPL_ENAB → Application_Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough **VALUE_AES_DMCC_DMC** and **VALUE_AES_TSAPI_USERS** licenses available.



©2013 Avaya Inc. All Rights Reserved.

Step	Description
7.	**Restart TSAPI Service** Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service**, and click **Restart Services**. 

©2013 Avaya Inc. All Rights Reserved.

7. Configure Calabrio Call Recording and Quality Management

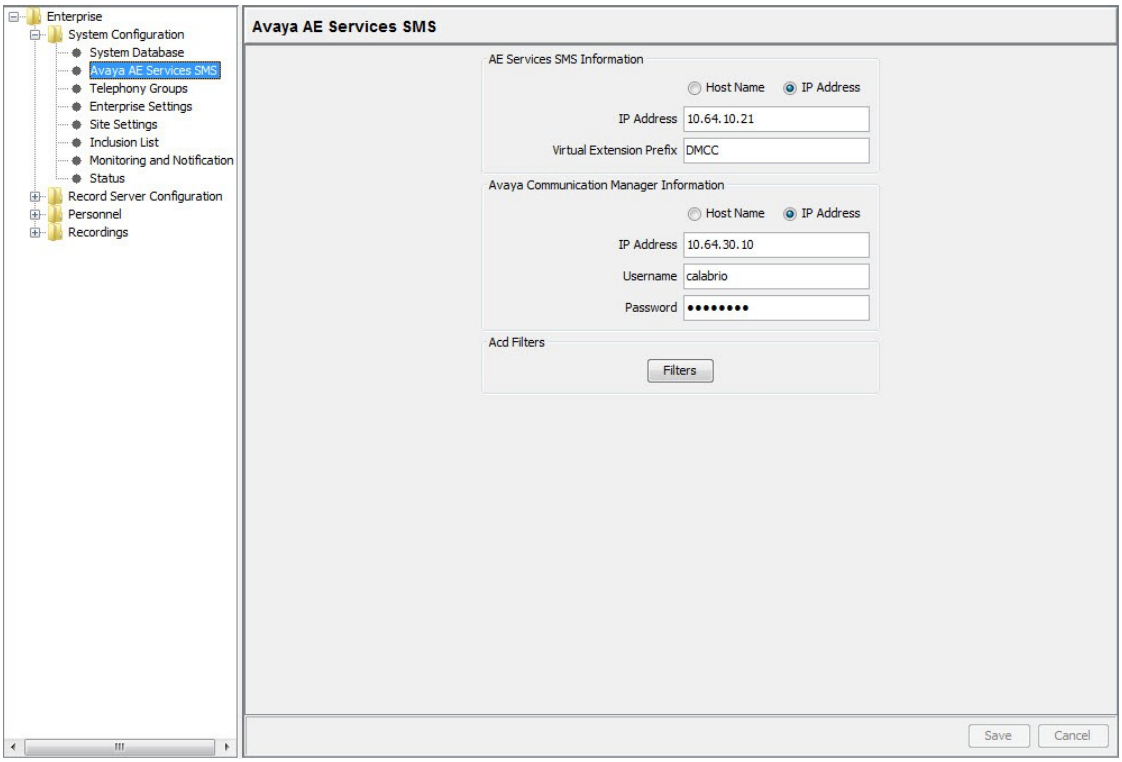
The initial configuration of the CRQM server is typically performed by Calabrio technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the CRQM solution to interoperate with Communication Manager and Application Enablement Services.

The steps include:

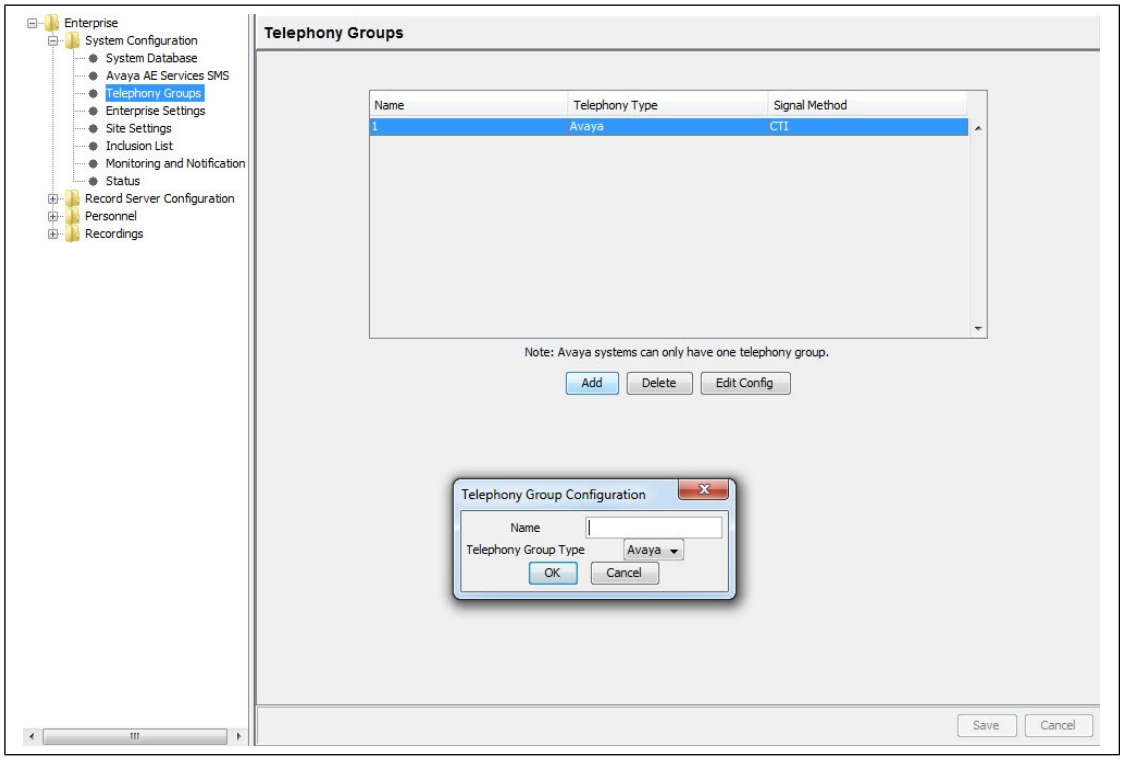
- Configuration of the Application Enablement Interfaces – SMS
- Configuration of the Application Enablement Interfaces – DMCC and JTAPI
- Configuration of Users
- Configuration of Devices
- Configuration of Recording Schedules (Workflows)

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

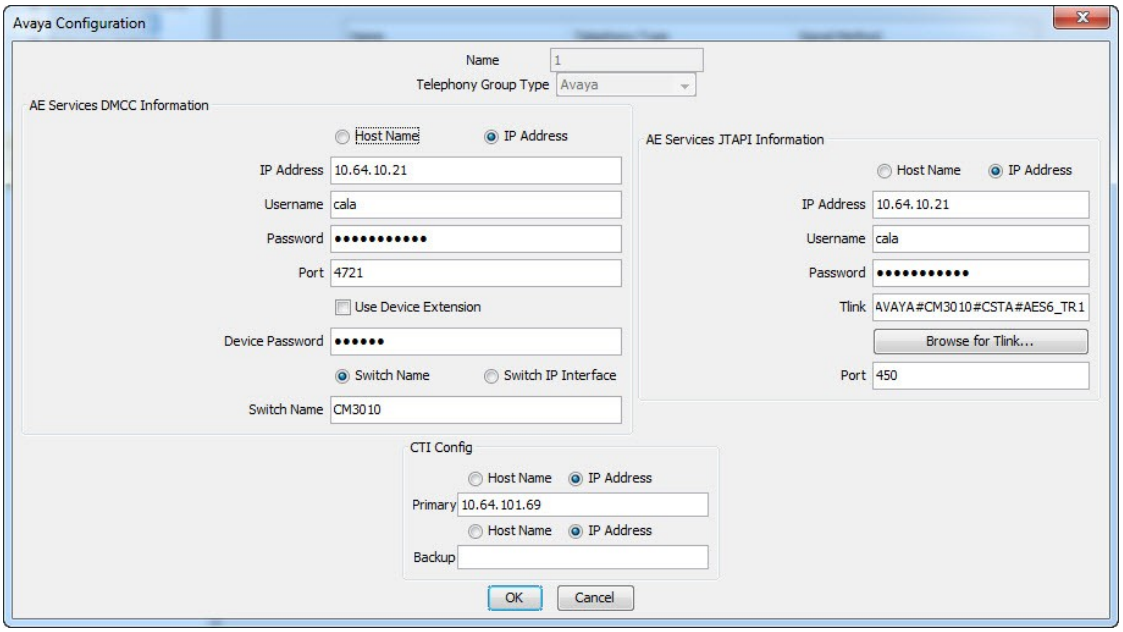
©2013 Avaya Inc. All Rights Reserved.

Step	Description
1.	**Configuration of the Application Enablement Interfaces – SMS** From the left pane, navigate to **Enterprise → System Configuration → Avaya AE Services SMS**. 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**. 

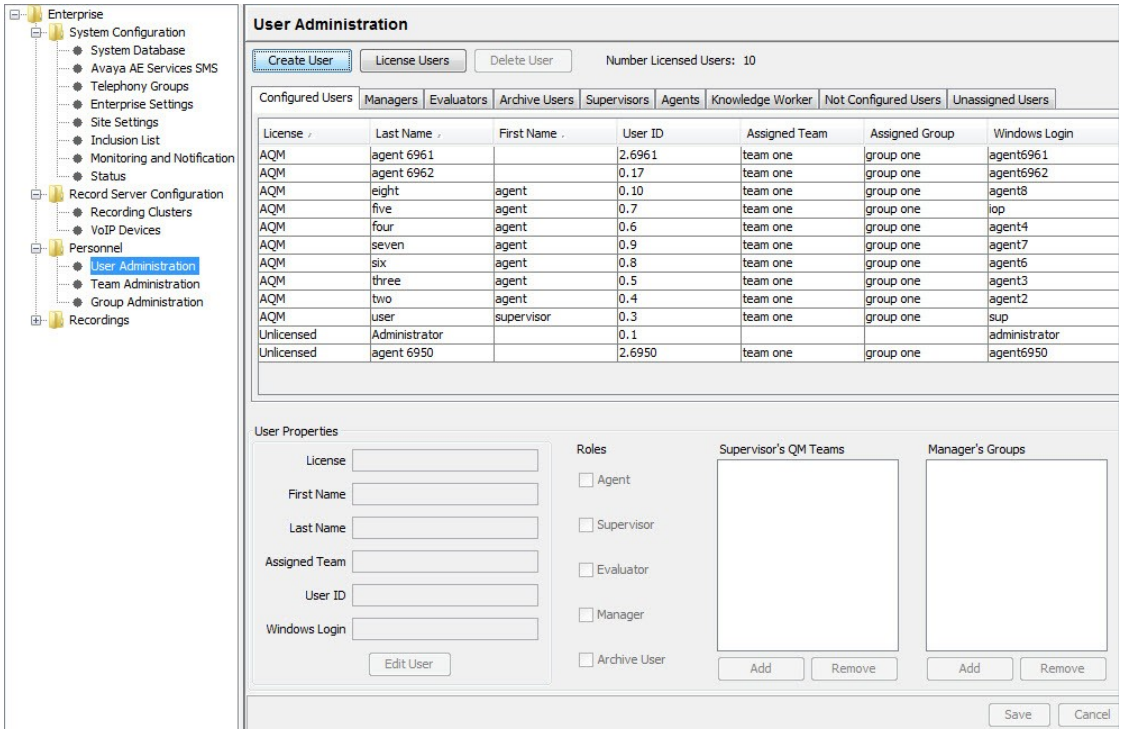
©2013 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Configuration of the Application Enablement Interfaces – DMCC and JTAPI** 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**. 

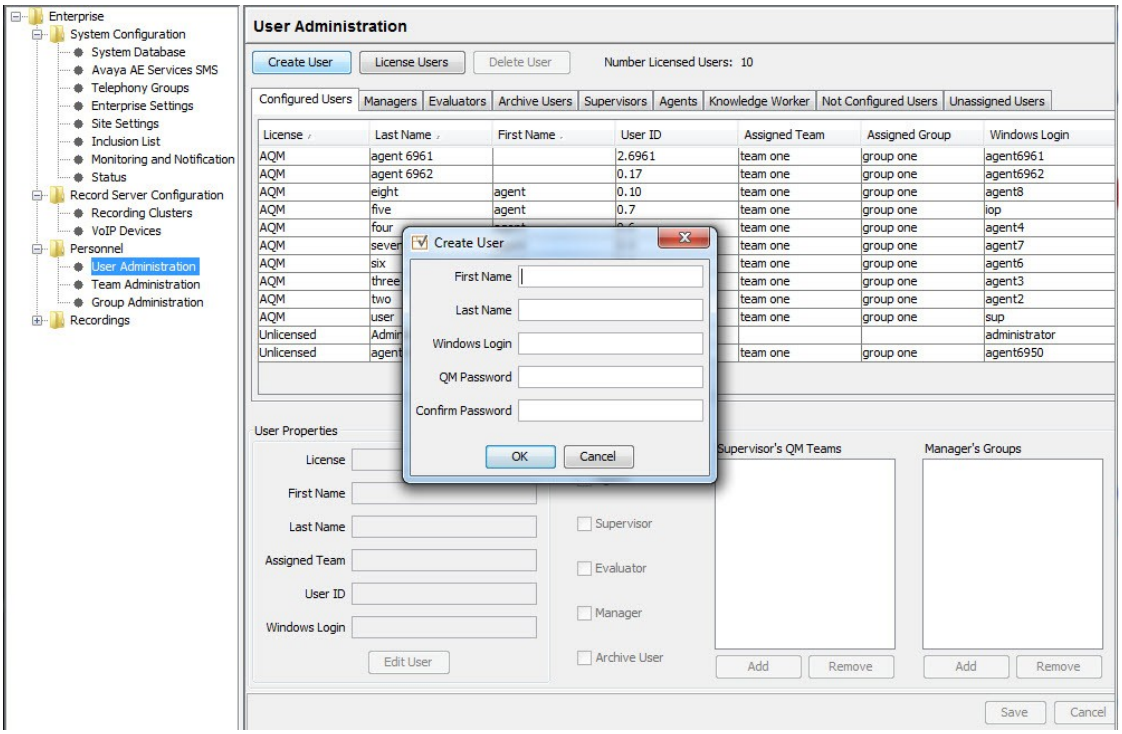
©2013 Avaya Inc. All Rights Reserved.

Step	Description
	Configuration of the Application Enablement Interfaces – DMCC and JTAPI (Continued) The **Avaya Configuration** screen is displayed. In the **AE Services DMCC Information** section, provide: • **Host Name** or **IP Address** of the **Application Enablement Services** server • **Username** and **Password** (from **Section 6**, **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**. This entry must match the configuration in **Section 6**, **Step 1**. **Switch Name** (**CM3010**) is preferred when multiple IP Interfaces are used for H.323 Gatekeepers as it allows Application Enablement Services to manage registrations in a pool. In the **AE Services JTAPI Information** section, provide: • **Host Name** or **IP Address** of the **Application Enablement Services** server. • **Username** and **Password** (from **Section 6**, **Step 4**) • **Tlink** as configured in **Section 6**, **Step 3**. • **450** as the **port** (the default TSAPI service listening port) Click **OK** to complete this step. 

©2013 Avaya Inc. All Rights Reserved.

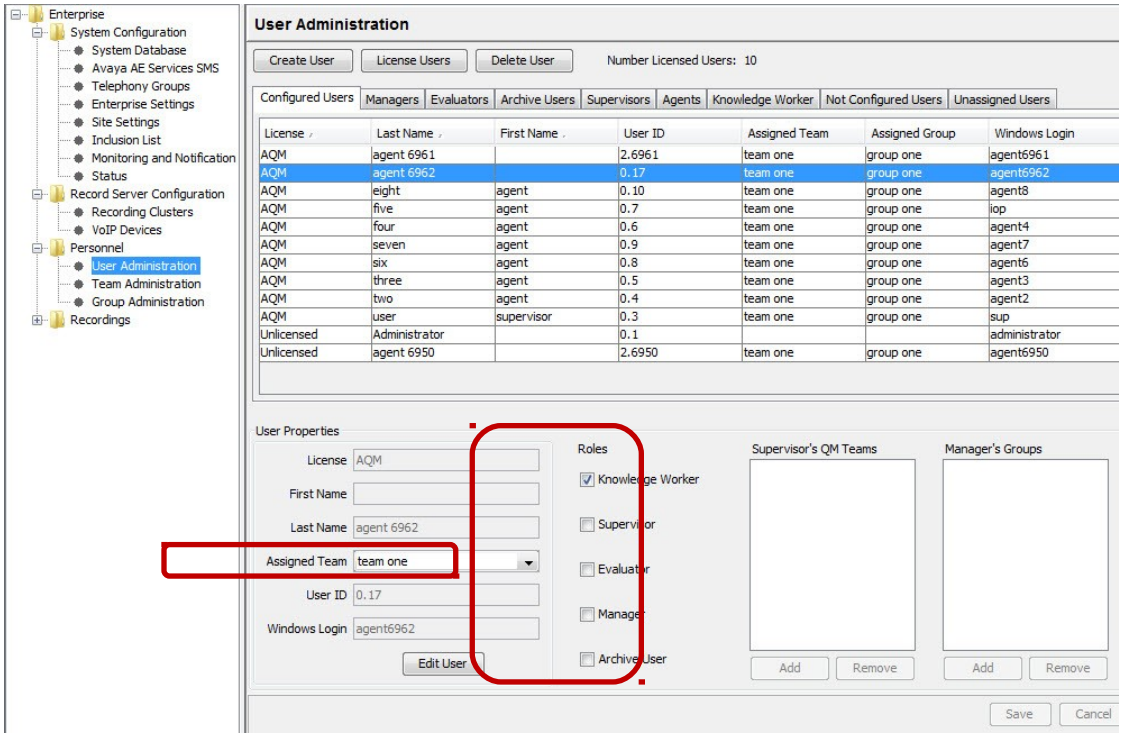
Step	Description
3.	**Configuration of Users** Navigate to **Enterprise → Personnel → User Administration** page to configure users. Once created, users can be statically assigned to a VoIP Device as demonstrated in **Step 4**. 

©2013 Avaya Inc. All Rights Reserved.

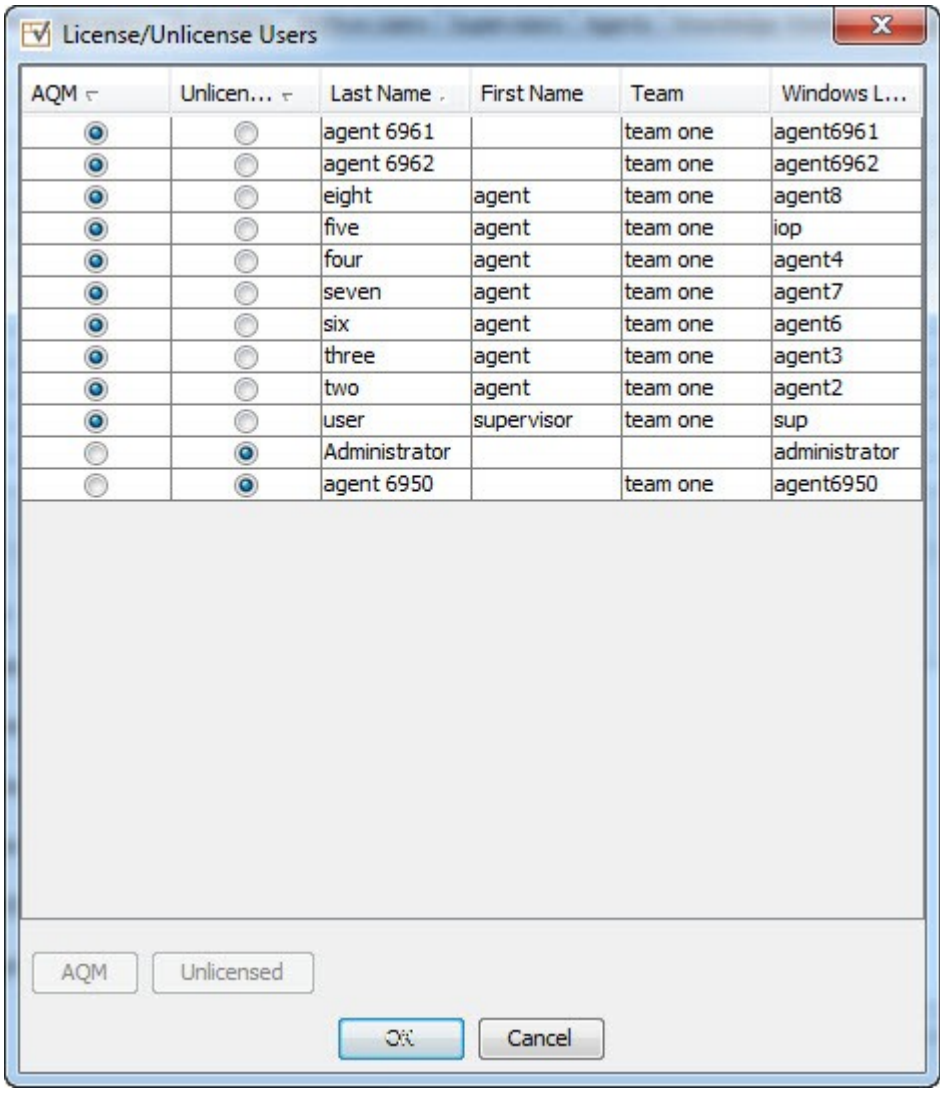
Step	Description
	Configuration of Users (Continued) Clicking **Create User** to create a new user. A **Create User** window pops up. Enter the **First Name**, **Last Name**, **Windows Login**, and **QM Password**. Click **OK**. Note: CRQM also automatically populates the Agent list under the **Agent**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

©2013 Avaya Inc. All Rights Reserved.

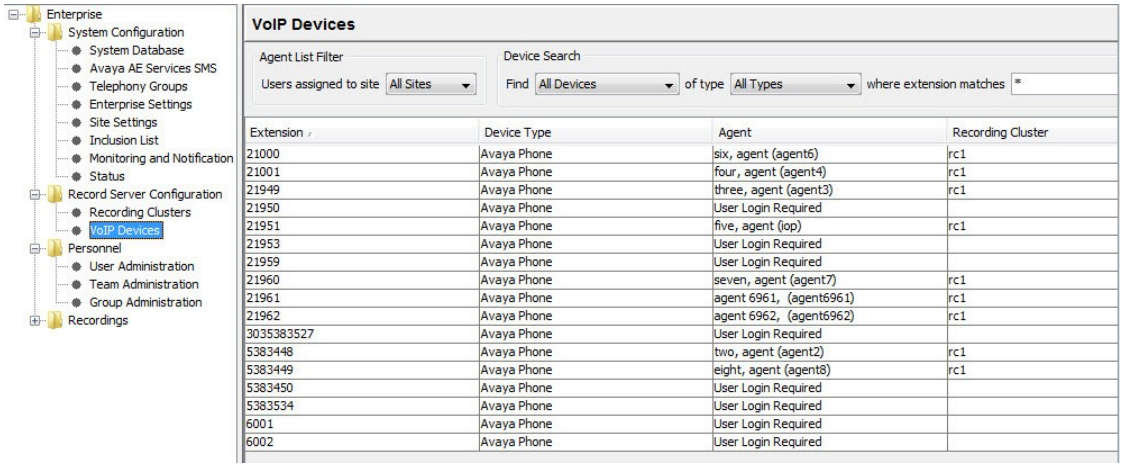
Step	Description
	Configuration of Users (Continued) The user appears in the list. Check one of the checkboxes (e.g. Knowledge Worker) under the **Roles** section and select a pre-configured team from the dropdown list of the **Assigned Team** field.



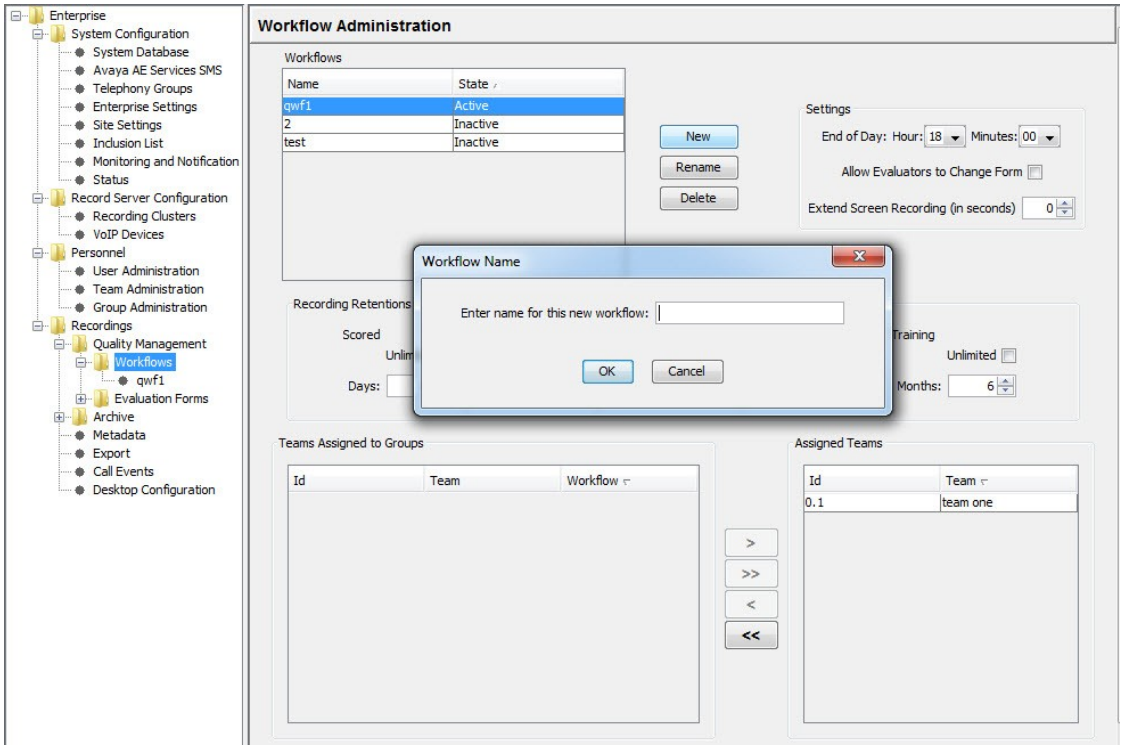
©2013 Avaya Inc. All Rights Reserved.

Step	Description
	Configuration of Users (Continued) 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. 

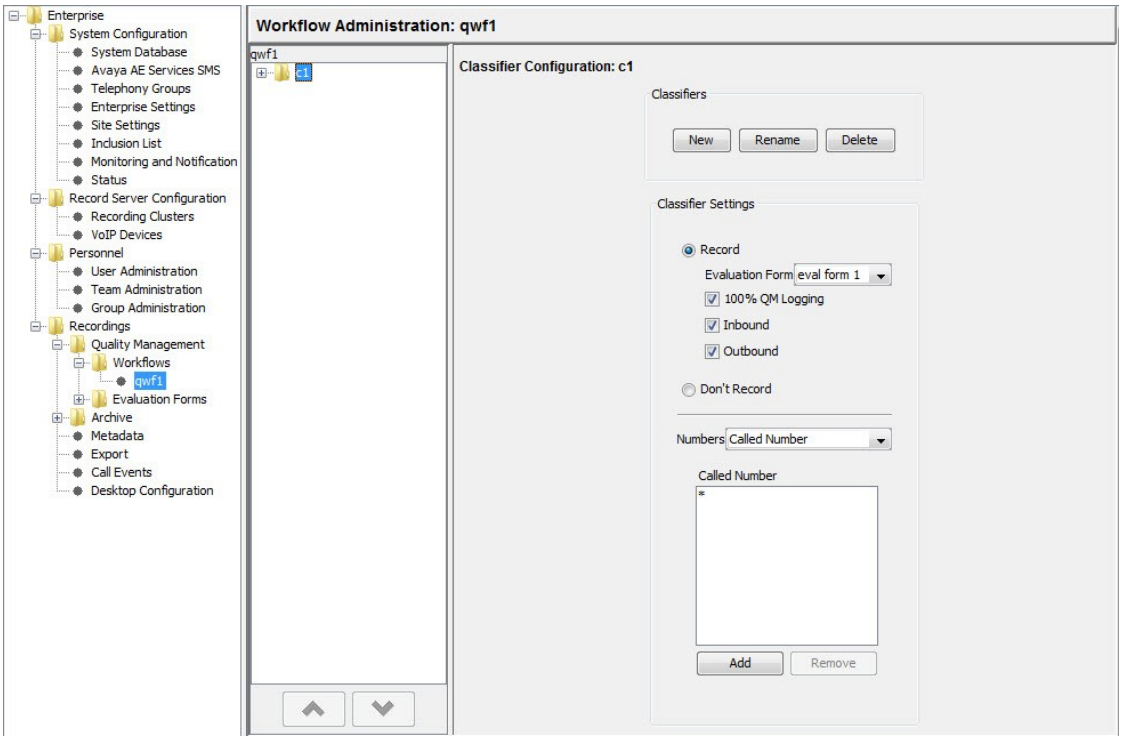
©2013 Avaya Inc. All Rights Reserved.

Step	Description
4.	**Configuration of Devices** Navigate to **Enterprise → Record Server Configuration → VoIP Devices** to configure devices. When the SMS query completes, all stations from Communication Manager are listed on the **VoIP Devices** page. A device is designated to be recorded by assigning a pre-configured **Recording Cluster** (e.g. rc1) on the **VoIP Devices** page, and then assigning an **Agent** to that device using dropdown lists in each column. The agent dropdown list includes the users configured on the **User Administration** page in **Step 3** that have the AQM license assigned. Click **Save** to complete this step.  Extension / Device Type / Agent / Recording Cluster 21000 / Avaya Phone / six, agent (agent6) / rc1 21001 / Avaya Phone / four, agent (agent4) / rc1 21949 / Avaya Phone / three, agent (agent3) / rc1 21950 / Avaya Phone / User Login Required / 21951 / Avaya Phone / five, agent (iop) / rc1 21953 / Avaya Phone / User Login Required / 21959 / Avaya Phone / User Login Required / 21960 / Avaya Phone / seven, agent (agent7) / rc1 21961 / Avaya Phone / agent 6961, (agent6961) / rc1 21962 / Avaya Phone / agent 6962, (agent6962) / rc1 3035383527 / Avaya Phone / User Login Required / 5383448 / Avaya Phone / two, agent (agent2) / rc1 5383449 / Avaya Phone / eight, agent (agent8) / rc1 5383450 / Avaya Phone / User Login Required / 5383534 / Avaya Phone / User Login Required / 6001 / Avaya Phone / User Login Required / 6002 / Avaya Phone / User Login Required /

©2013 Avaya Inc. All Rights Reserved.

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

©2013 Avaya Inc. All Rights Reserved.

Step	Description
	Configuration of Recording Schedules (Workflows) - Continued 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. 

©2013 Avaya Inc. All Rights Reserved.

8. Verification Steps

The following steps may be used to verify the configuration:

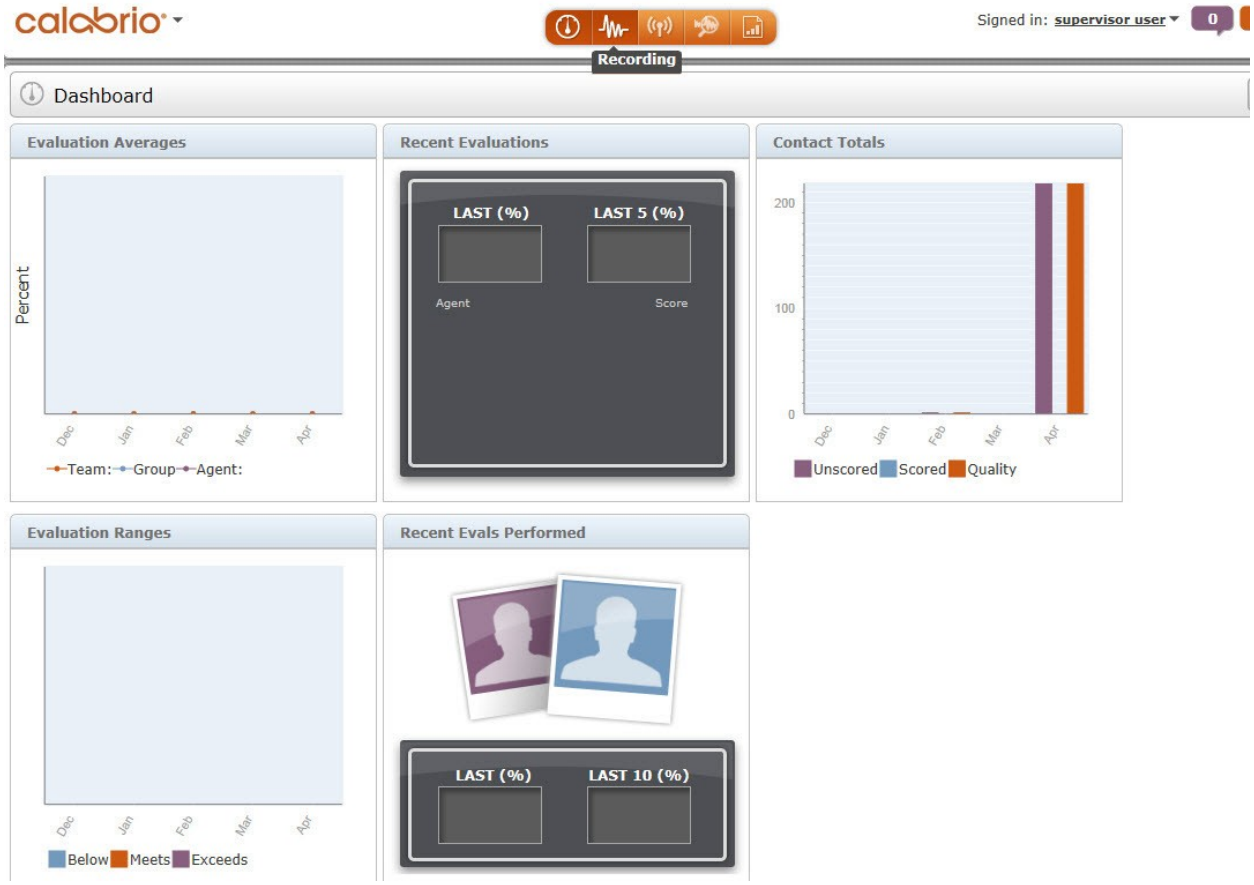
- Verify that the interface on Communication Manager to Application Enablement Services is enabled and in **listening** status (use the **status aesvcs interface** command on the Communication Manager SAT).
- Verify that the link between Communication Manager and Application Enablement Services is transmitting 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

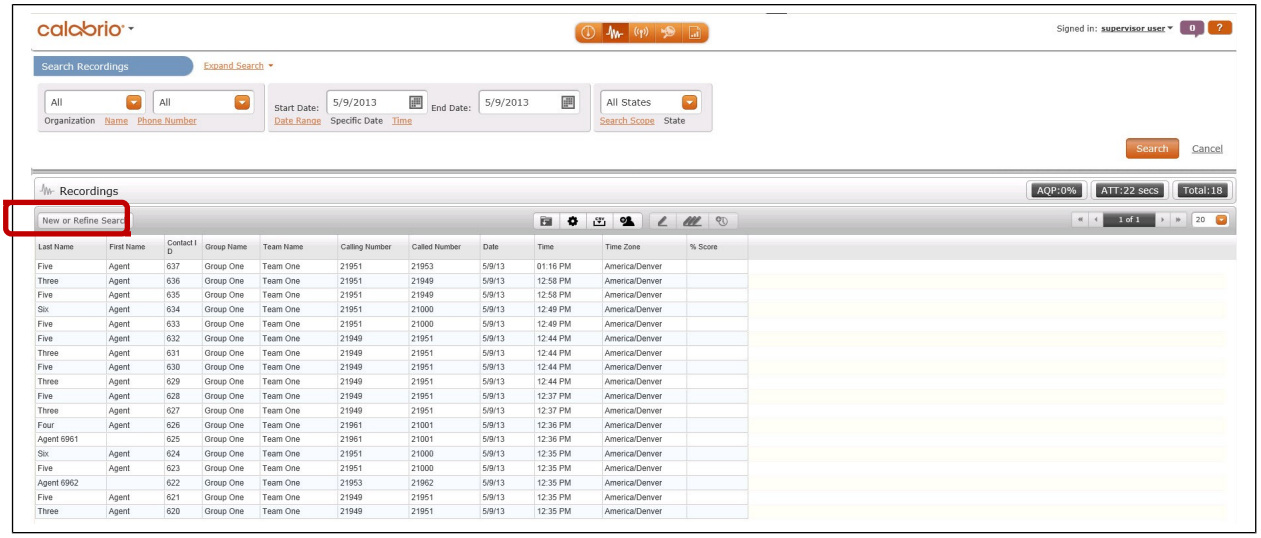
Access the Calabrio web-based user interface using the URL **http://<ip-address>** in a browser window, where **<ip-address>** is the address of the CRQM server. The **Log In** screen is displayed as shown below. Use appropriate credentials to log in.

©2013 Avaya Inc. All Rights Reserved.

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.

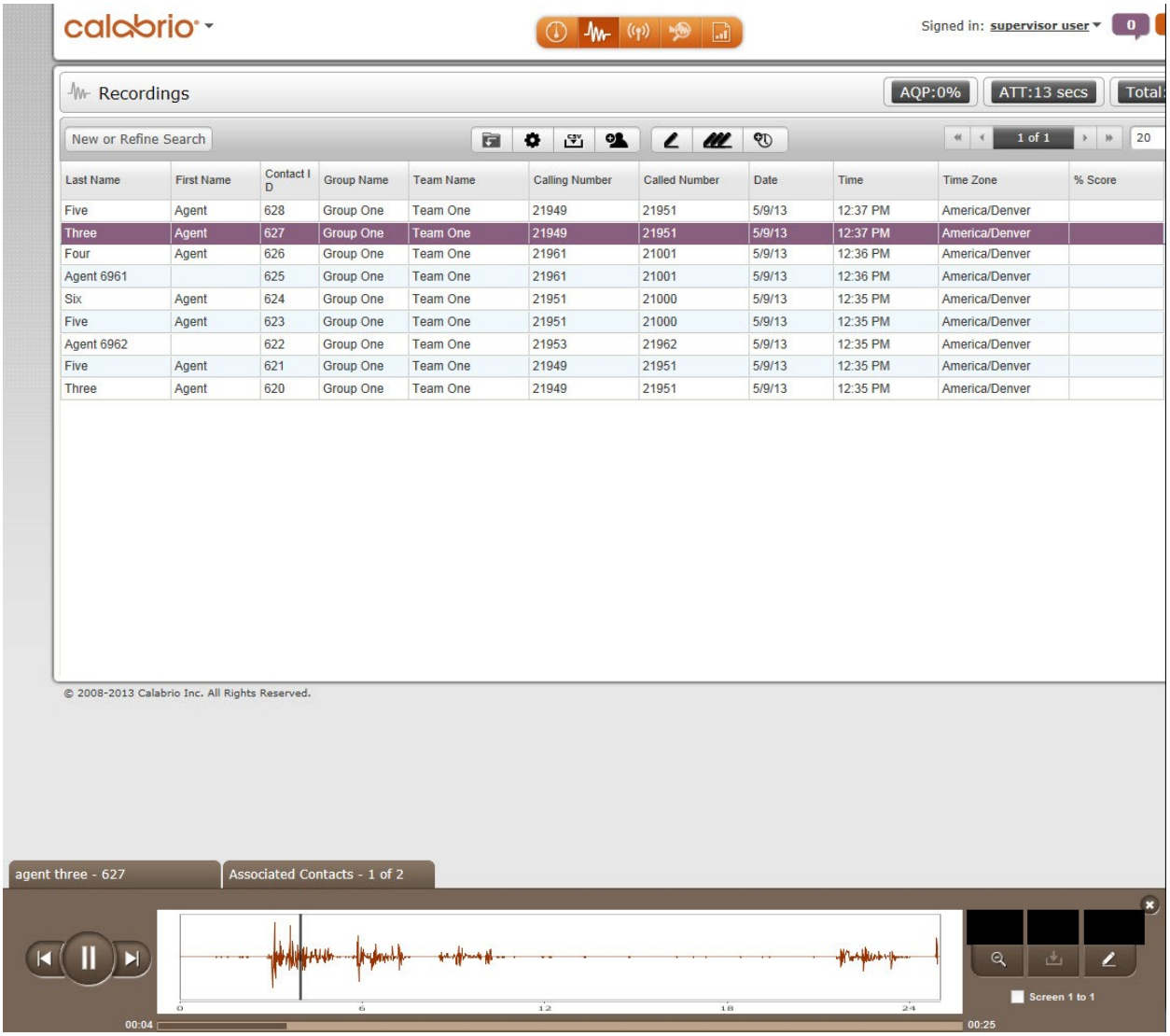


On the **Recording** page, click **New or Refined Search,** create search criteria and click **Search** to find recordings.



©2013 Avaya Inc. All Rights Reserved.

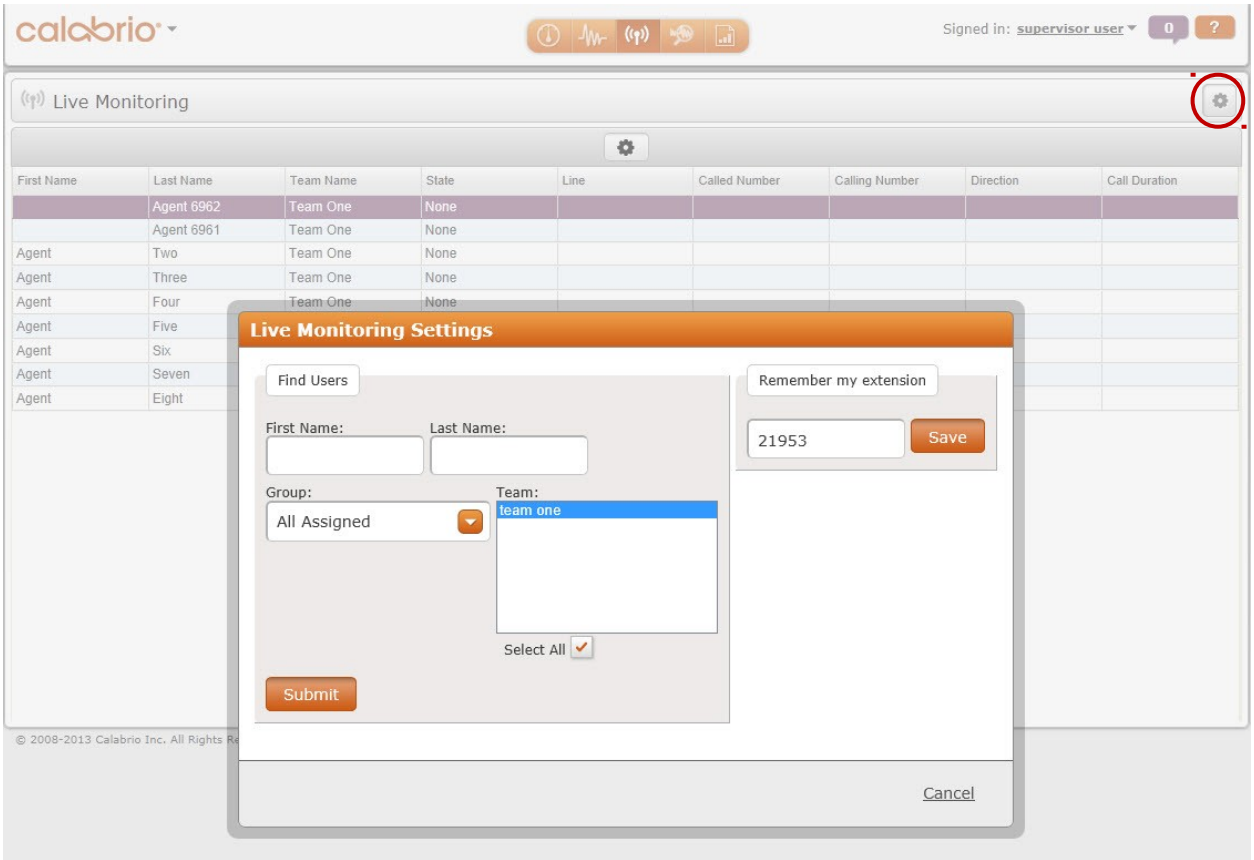
Select a call of interest and double click to launch a playback window as shown below.



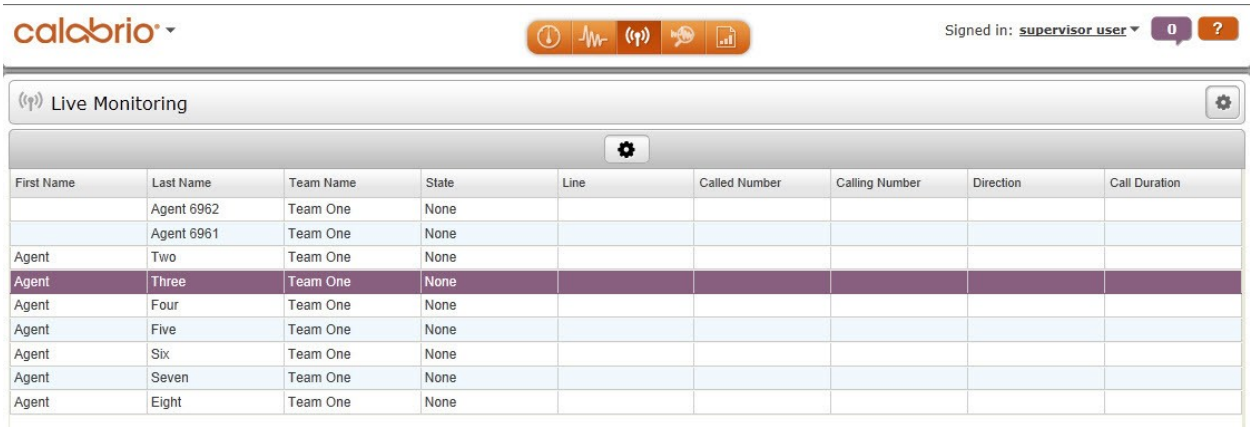
8.2. Verify Live Monitoring

A supervisor can monitor and listen to calls to and from an agent in real-time. To activate the function, click the **Live Monitoring** icon in the orange tool bar.

The **Live Monitoring** page is displayed. Click the **Live Monitoring** icon at the upper right corner. A **Live Monitoring Settings** window pops up. Enter the extension of the phone the supervisor will use to monitor calls and check the **Select All** checkbox in the **Find Users** section. Click **Submit**.

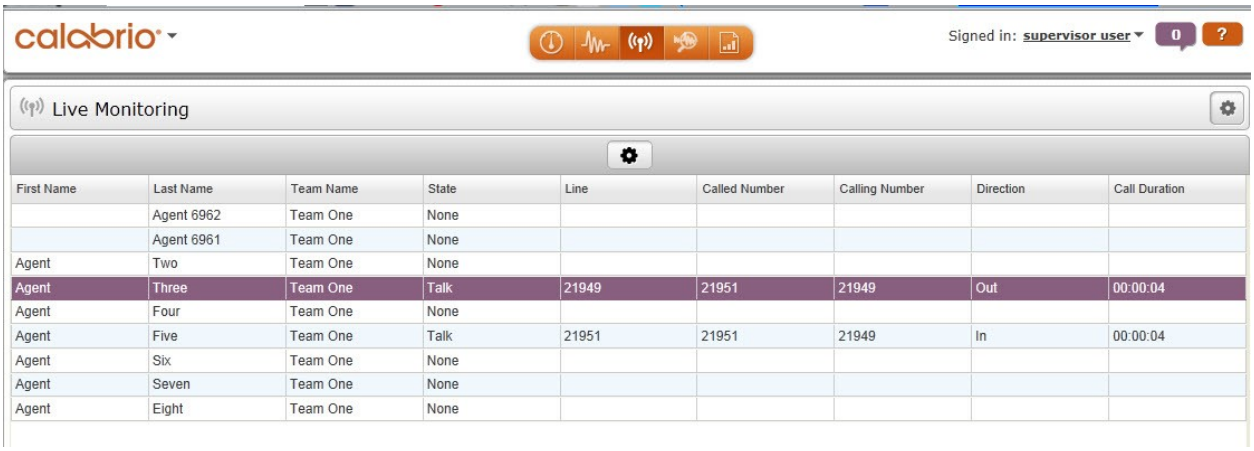


The list of users selected is displayed.



©2013 Avaya Inc. All Rights Reserved.

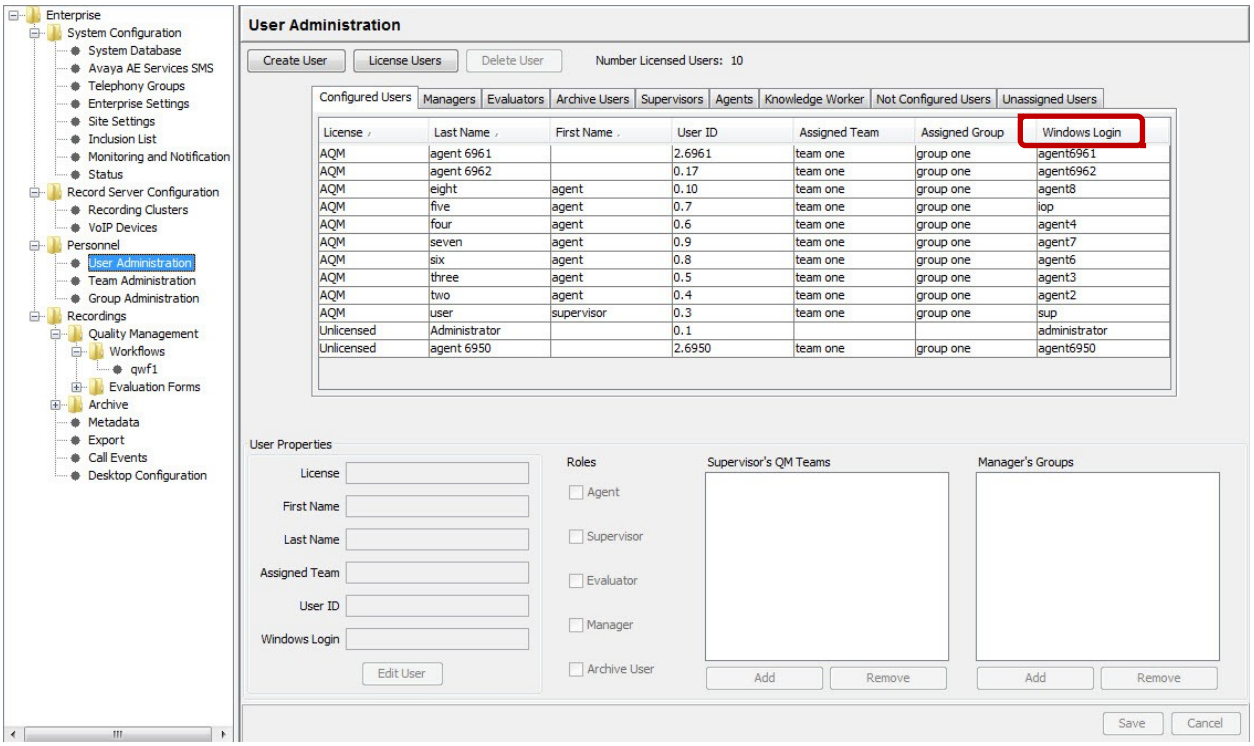
When a user in the monitored list receives or originates a call, call related information is displayed. The supervisor can double click the user line to bridge his/her phone to the call with the phone speaker automatically turned on.



First Name	Last Name	Team Name	State	Line	Called Number	Calling Number	Direction	Call Duration
	Agent 6962	Team One	None					
	Agent 6961	Team One	None					
Agent	Two	Team One	None					
Agent	Three	Team One	Talk	21949	21951	21949	Out	00:00:04
Agent	Four	Team One	None					
Agent	Five	Team One	Talk	21951	21951	21949	In	00:00:04
Agent	Six	Team One	None					
Agent	Seven	Team One	None					
Agent	Eight	Team One	None					

8.3. Verify Screen Recording

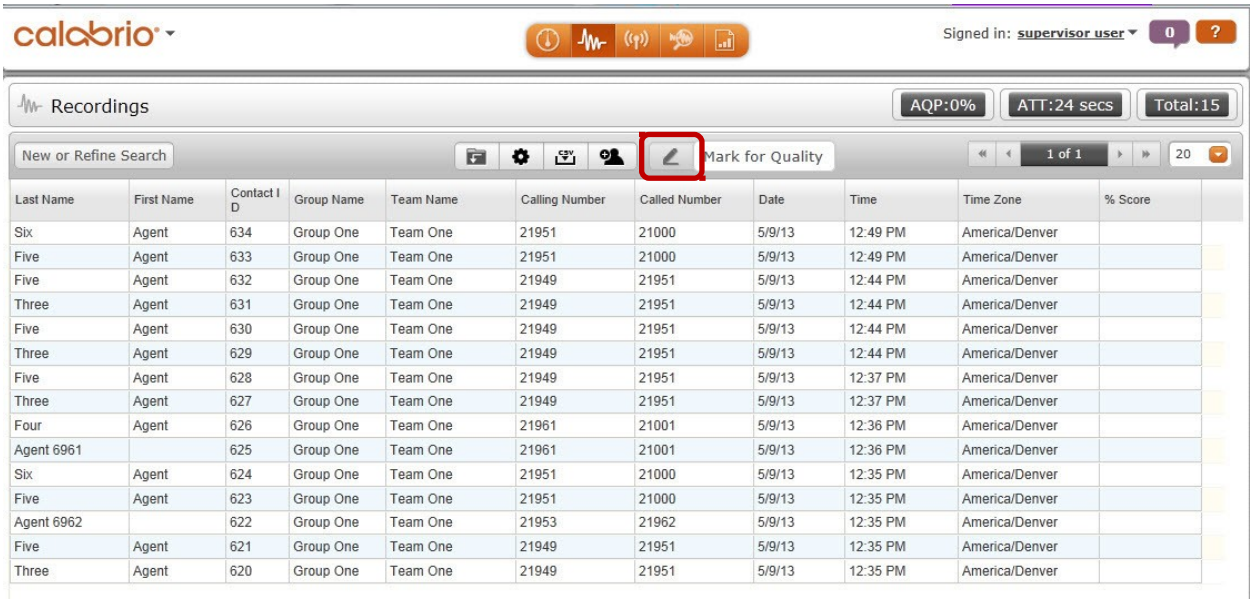
When properly configured, CRQM can perform screen recording at the same time when a call is being recorded. To activate screen recording on an agent's Windows PC, **Calabrio Desktop Recording Service** has to be downloaded and started on the PC. In addition, during User Administration (**Section 7**, **Step 3**) the **Windows Login** and **QM Password** of the user have to be configured to match the login and password of the PC.



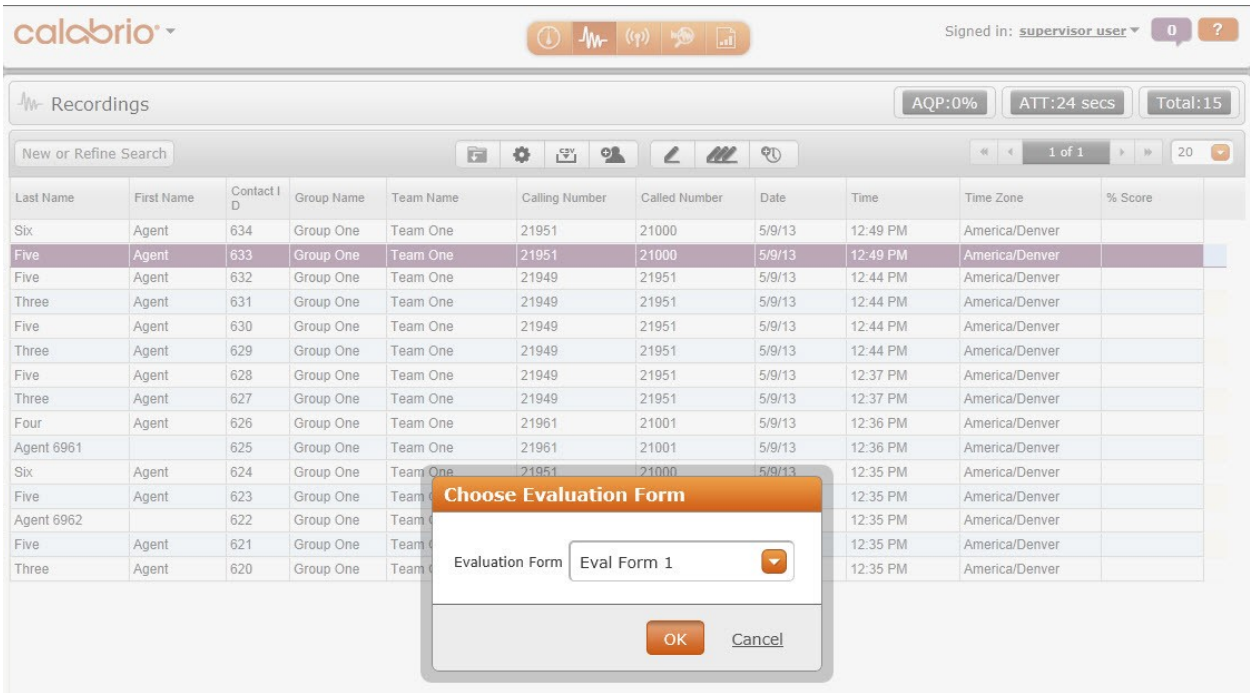
License	Last Name	First Name	User ID	Assigned Team	Assigned Group	Windows Login
AQM	agent 6961		2.6961	team one	group one	agent6961
AQM	agent 6962		0.17	team one	group one	agent6962
AQM	eight	agent	0.10	team one	group one	agent8
AQM	five	agent	0.7	team one	group one	iop
AQM	four	agent	0.6	team one	group one	agent4
AQM	seven	agent	0.9	team one	group one	agent7
AQM	six	agent	0.8	team one	group one	agent6
AQM	three	agent	0.5	team one	group one	agent3
AQM	two	agent	0.4	team one	group one	agent2
AQM	user	supervisor	0.3	team one	group one	sup
Unlicensed	Administrator		0.1			administrator
Unlicensed	agent 6950		2.6950	team one	group one	agent6950

©2013 Avaya Inc. All Rights Reserved.

To activate screen recording playback, the supervisor has to download a Calabrio Screen Player plug-in for Internet Explorer. Screen recording will be available for playback after a scheduled upload time, usually end of the day. If an immediate upload is required, the supervisor can select the corresponding call recording and click the **Mark for Quality** button.

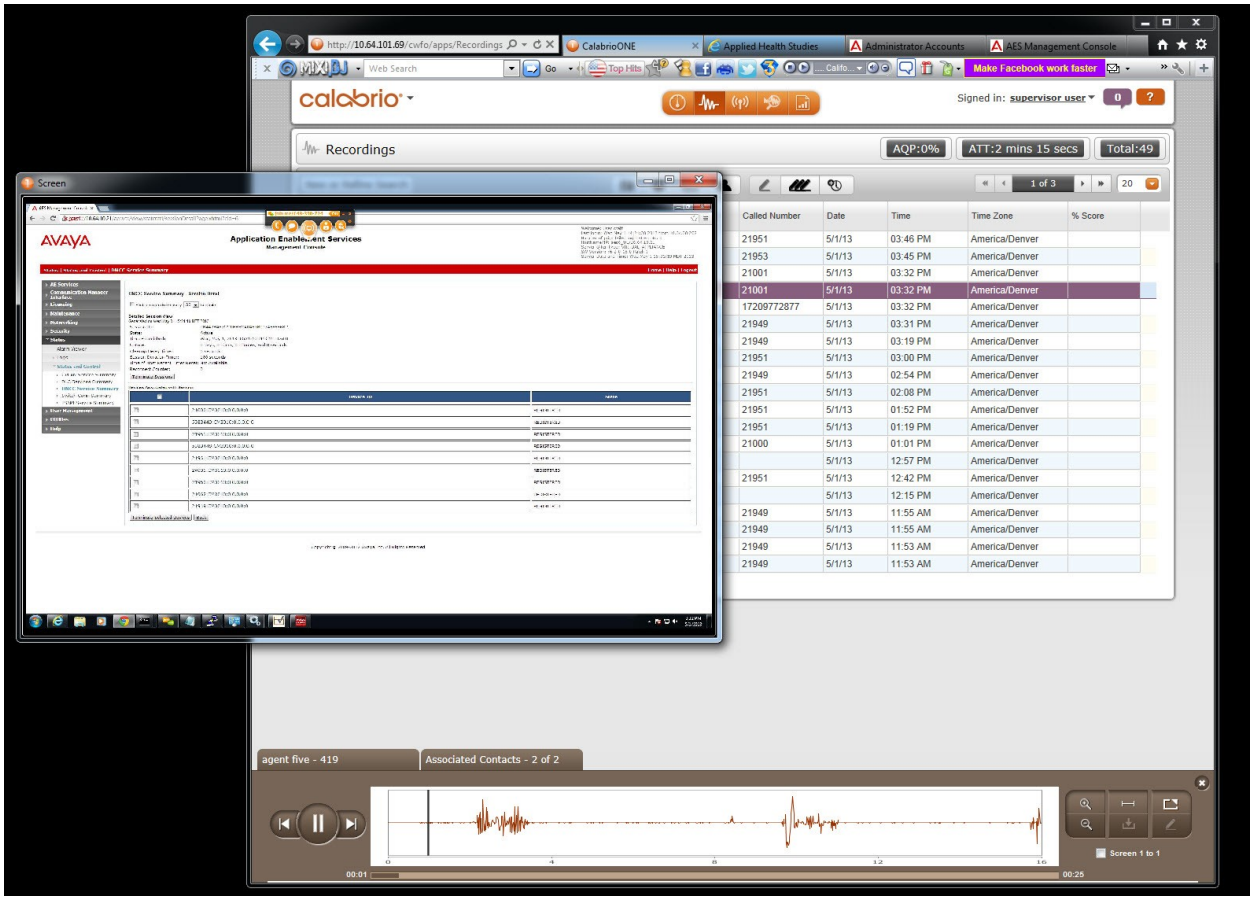


The **Choose Evaluation Form** window is displayed. Select a pre-configured evaluation form and click **OK**.



©2013 Avaya Inc. All Rights Reserved.

Once the screen recording is uploaded, a screen recording will be played when the corresponding call recording is played.



©2013 Avaya Inc. All Rights Reserved.

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.

- *Administering Avaya Aura® Communication Manager*, Release 6.2, Issue 7.0, July 2012, Document Number 03-300509.
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.2, Issue 11, July 2012
- *Avaya Aura® Application Enablement Services Device, Media and Call Control API Java Programmers Guide Release 6.2*, Issue 1, June 2012, Document Number 02-300359

Product information for Calabrio products can be found at http://calabrio.com/about-calabrio/services/

- *Calabrio Call Recording and Quality Management Application User Guide*, Version 9.1, Last Modified January 25, 2013
- *Calabrio Monitoring and Recording Services Administrator User Guide for Avaya*, Version 9.1, Last Modified January 25, 2013

©2013 Avaya Inc. All Rights Reserved.

©2013 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.