Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio Call Recording and Quality Management with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Calabrio Call Recording and Quality Management solution to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3.

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

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

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

©2016 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 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.

©2016 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. Audio codec support tested for G.711MU. Common call scenarios including hold/resume, mute/unmute, transfer, and conference at Calabrio side were exercised during the test. Additional tests included the ability to monitor live calls and to record screen activity associated with a recorded station.

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

2.2. Test Results

All test cases passed.

2.3. Support

Technical support on Calabrio CRQM can be obtained through the following:

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

©2016 Avaya Inc. All Rights Reserved.

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.

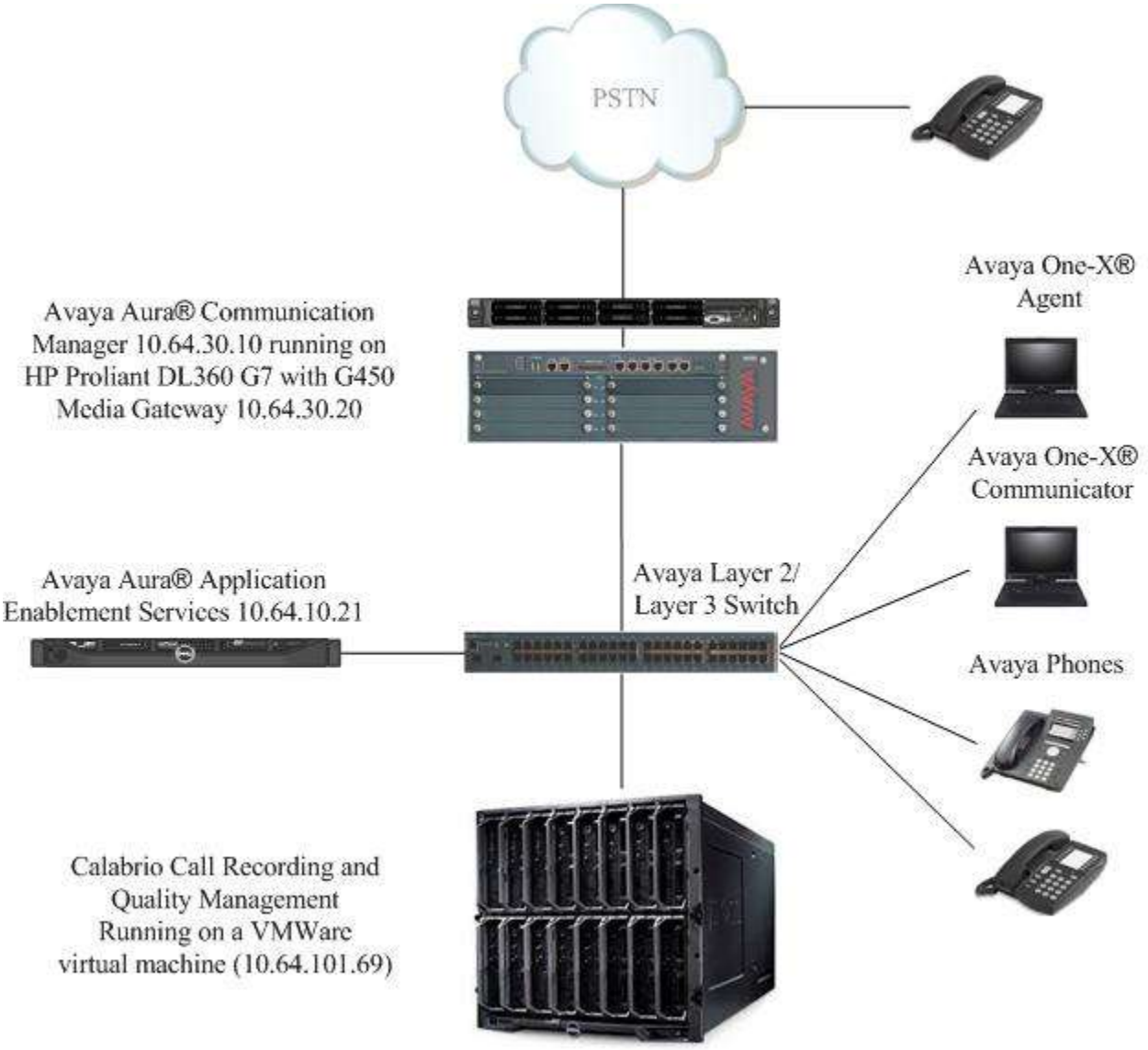


Figure 1 – Calabrio CRQM Compliance Test Configuration

©2016 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	6.3 SP112
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	6.3 SP3
Avaya 9600 Series IP Telephone • 9640 (H.323)	3.2.5
Avaya 96x1 Series IP Telephone • 9641 (H.323)	6.6.0
Desktop PC running Avaya One-X® Communicator	6.3
Calabrio Recording and Quality Management running under Windows 2012 R2 Server on a VMWare virtual machine	9.3

©2016 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:

- 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**.

©2016 Avaya Inc. All Rights Reserved.

Step	Description
1.	**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      Enabled     Local        Local       Remote      Remote
  Type                    Node         Port        Node        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       Password          Enabled    Status
                   Server
      1:        aes10210          xxxxxx              y
```


©2016 Avaya Inc. All Rights Reserved.

Step	Description
2.	**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: 58001
     Type: ADJ-IP
                                                                      COR: 1
     Name: aes10210
```

Step	Description
3.	**Add SMS User Account** CRQM uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application. A privileged user was used in this test; however, a local administrator would want to restrict the user account. This involves creating a user profile at the SAT, and then creating and assigning that user to the profile in the web admin pages. To illustrate, the adding a new user profile, **add user-profile-by-category *n*** command can be used to create the profile.

```
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
```

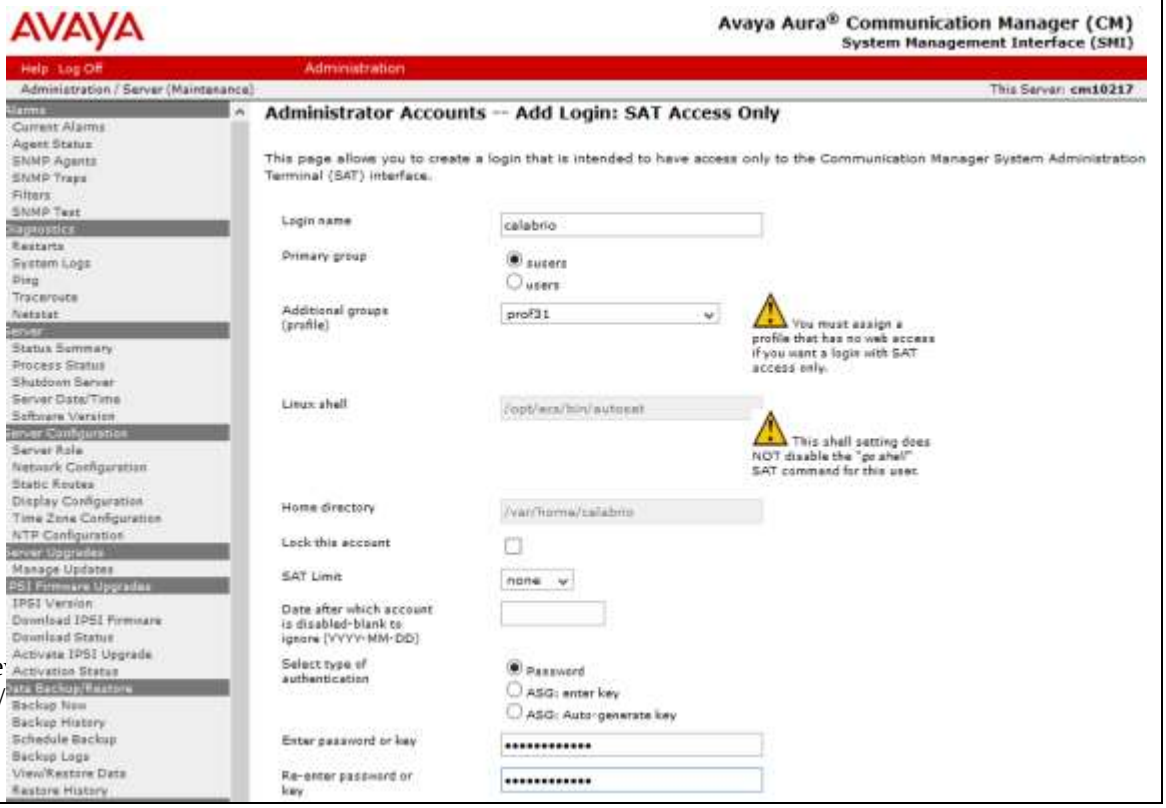

©2016 Avaya Inc. All Rights Reserved.

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-
```


©2016 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**. 

Step	Description
4.	**Verify 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 53001                                        Page   1 of   5
                                    STATION

Extension: 53001                        Lock Messages? n               BCC: 0
     Type: 9608                         Security Code: 123456           TN: 1
     Port: S00000                     Coverage Path 1: 98              COR: 1
     Name: 53001, Station             Coverage Path 2:                 COS: 1
                                      Hunt-to Station:               Tests? y
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 53001
           Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? y

                                           IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                           Customizable Labels? y
```

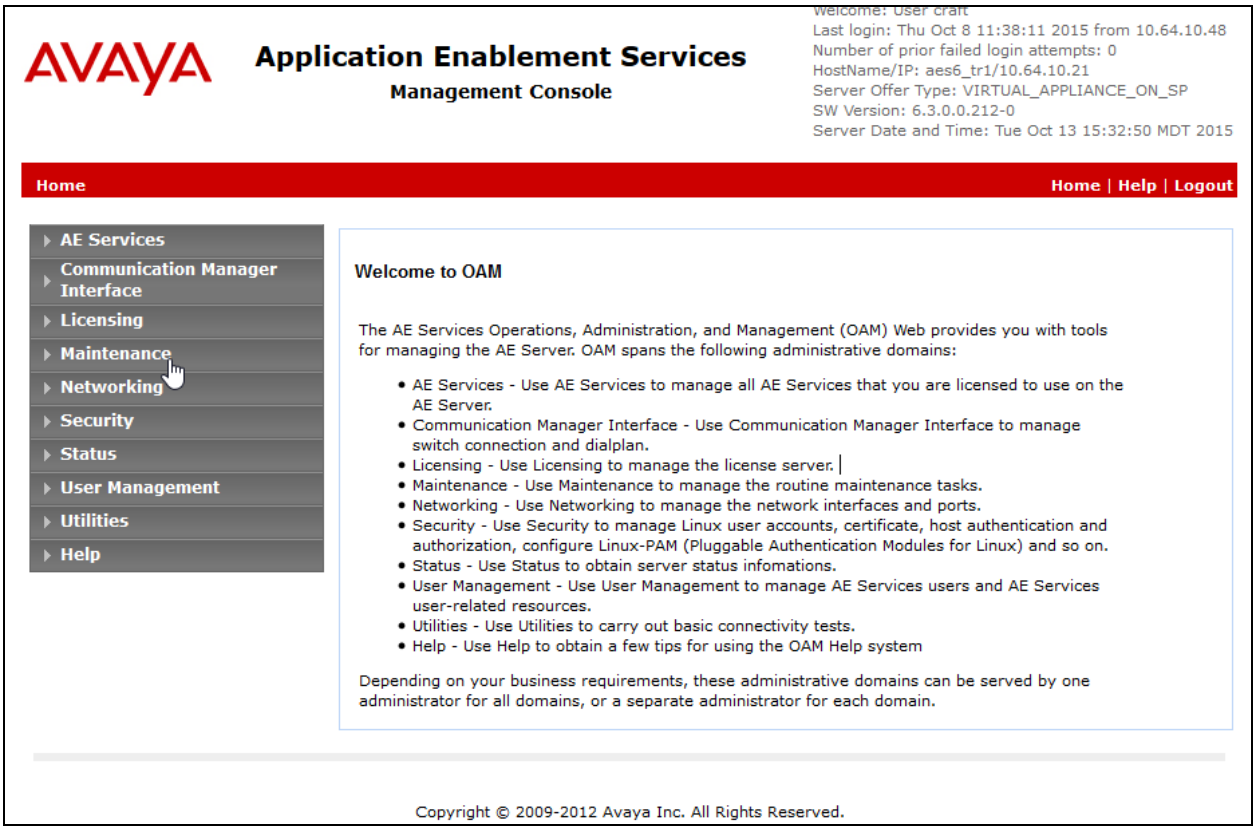

©2016 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Application Enablement Services

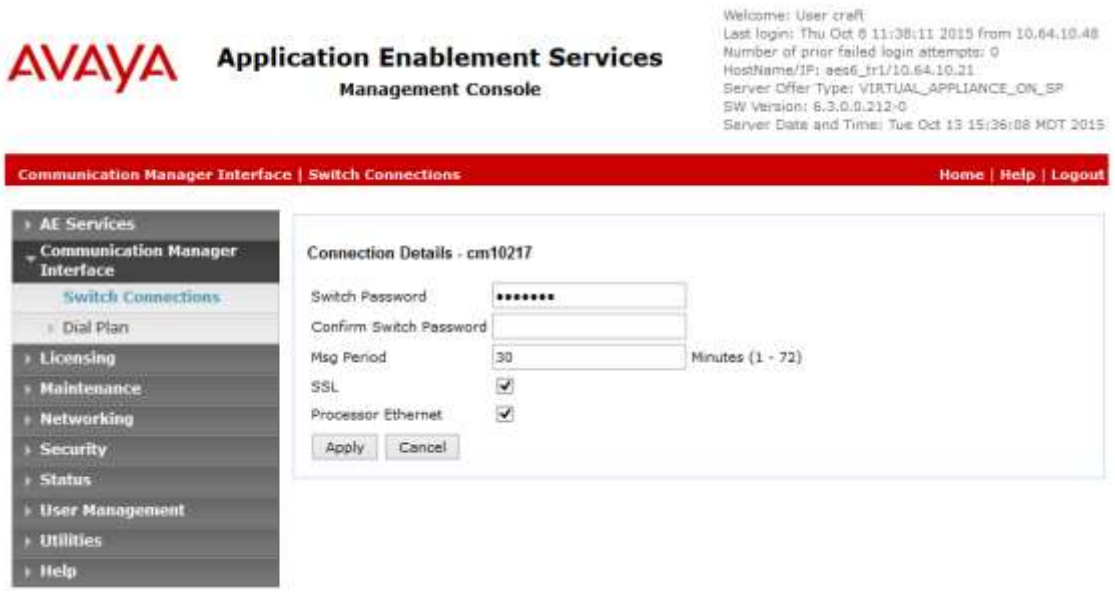
All administration of Application Enablement Services is performed via a web browser. Enter https://<ip-addr> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. Note that all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

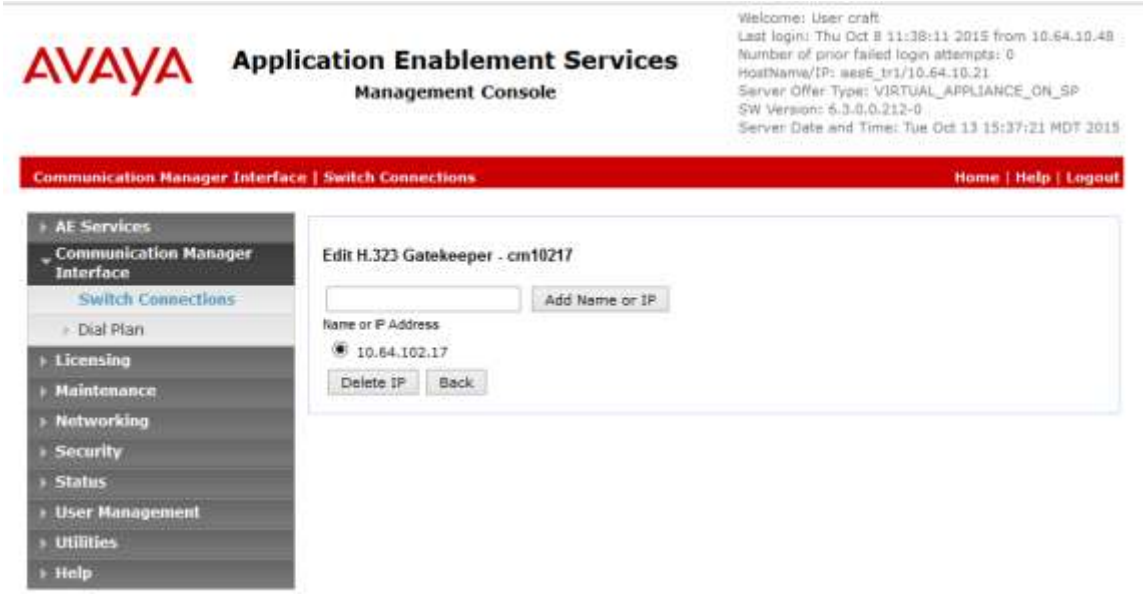
- Configure Communication Manager Switch Connections
- Add TSAPI Links
- Note the TLink Information
- Configure Calabrio User
- Enable Unrestricted Access for Calabrio User



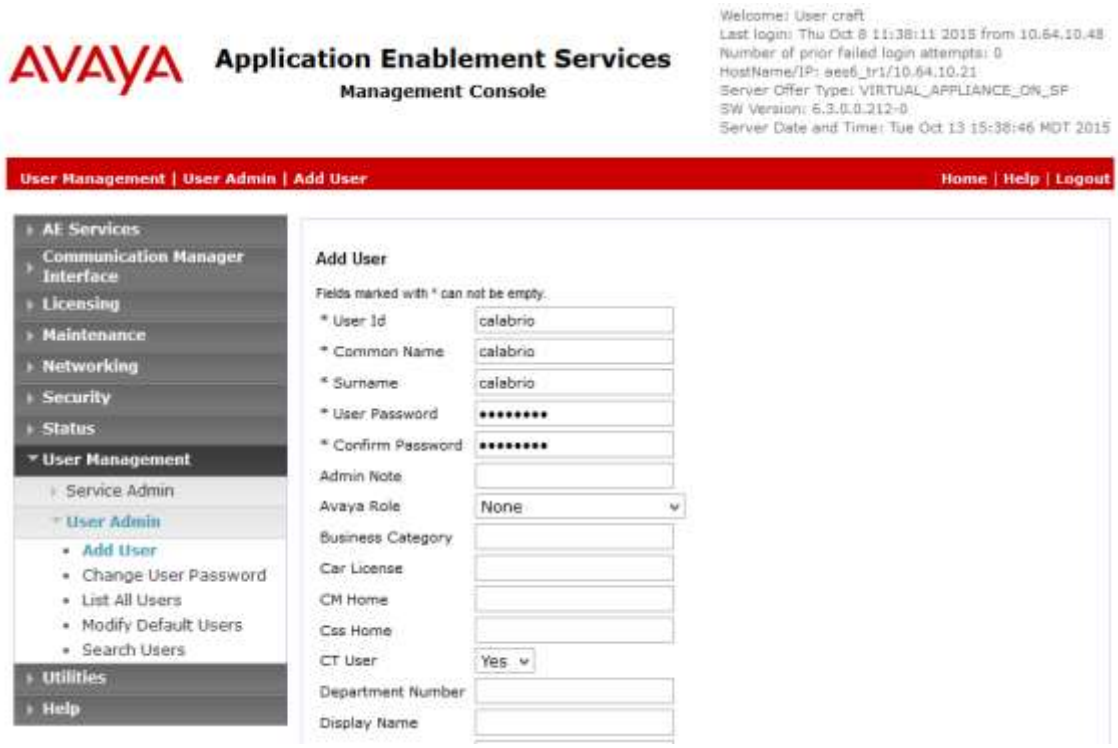
©2016 Avaya Inc. All Rights Reserved.

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

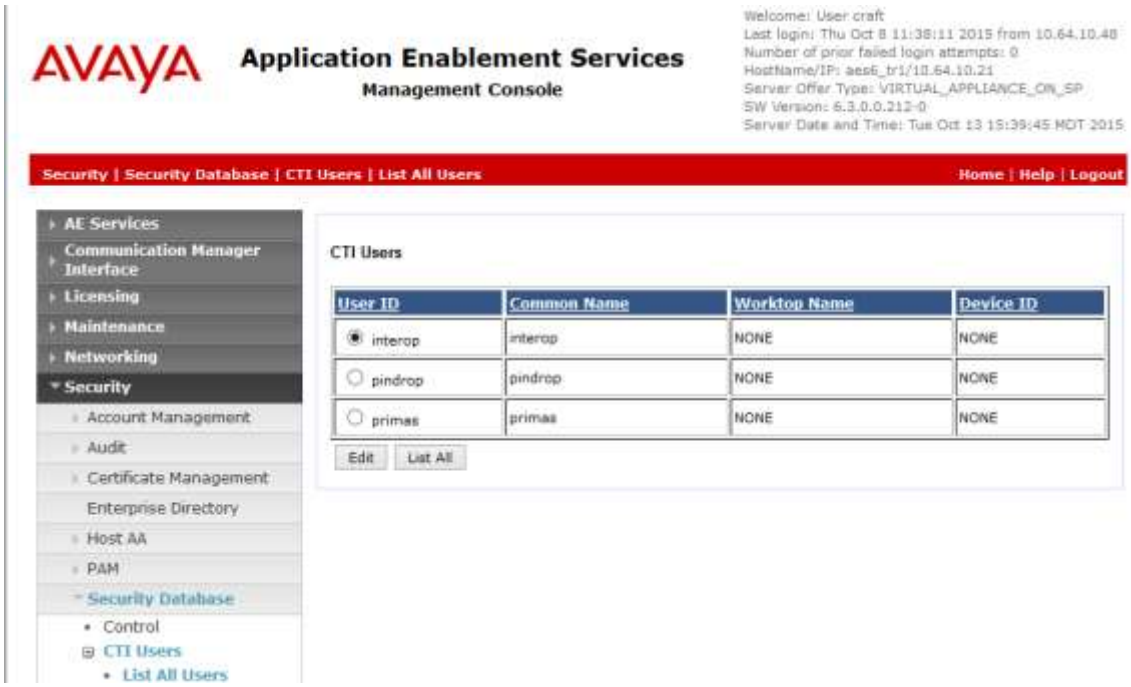
©2016 Avaya Inc. All Rights Reserved.

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. 

©2016 Avaya Inc. All Rights Reserved.

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

©2016 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Enable Unrestricted Access for Calabrio User** If the Security Database (SDB) is enabled on Application Enablement Services, set the calabrio user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration. Navigate to **Security → Security Database → CTI Users → List All Users** and select the **cala** user and click **Edit** (not shown).  On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog.

©2016 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
- 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 → Monitoring and Recording Administrator**. Log in with proper credentials.

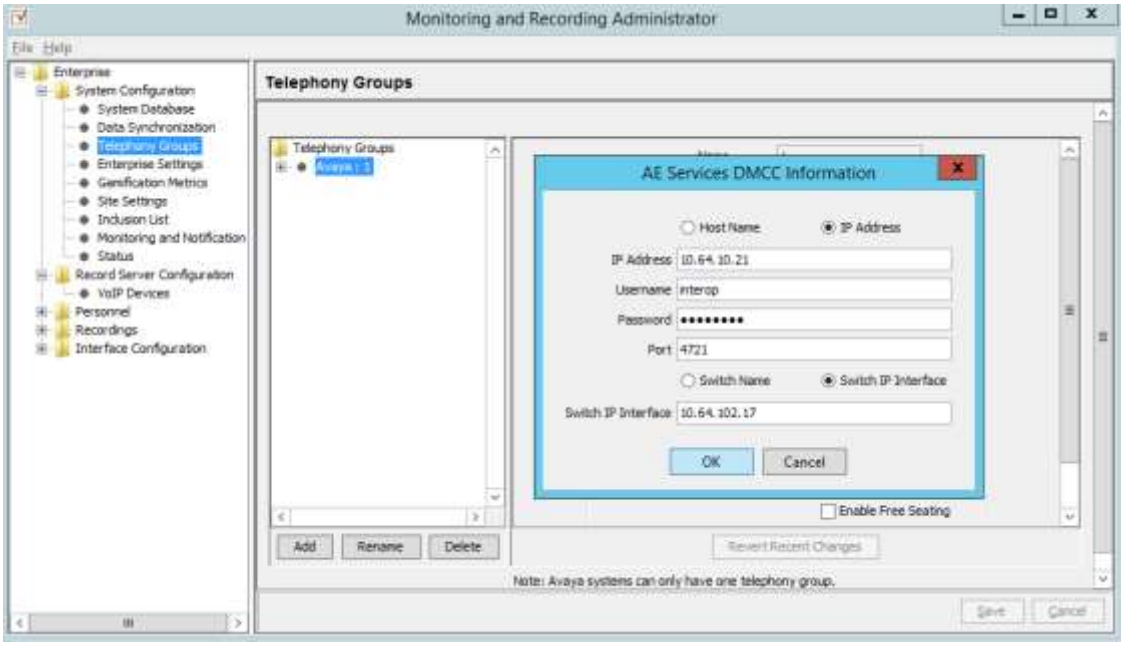
©2016 Avaya Inc. All Rights Reserved.

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

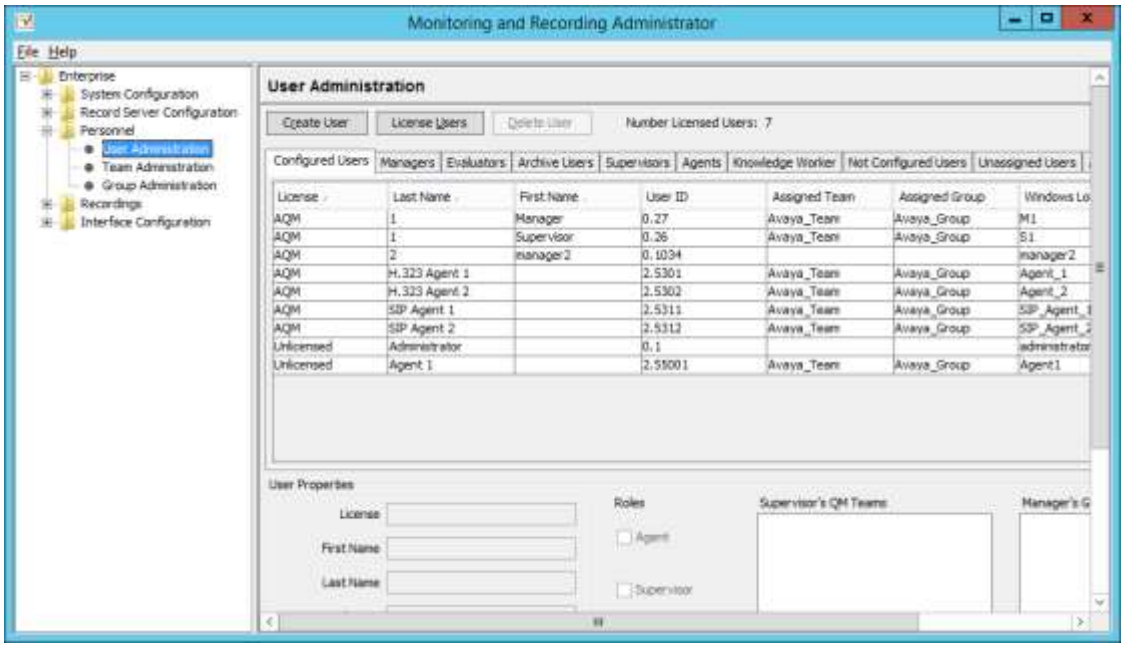
©2016 Avaya Inc. All Rights Reserved.

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**.

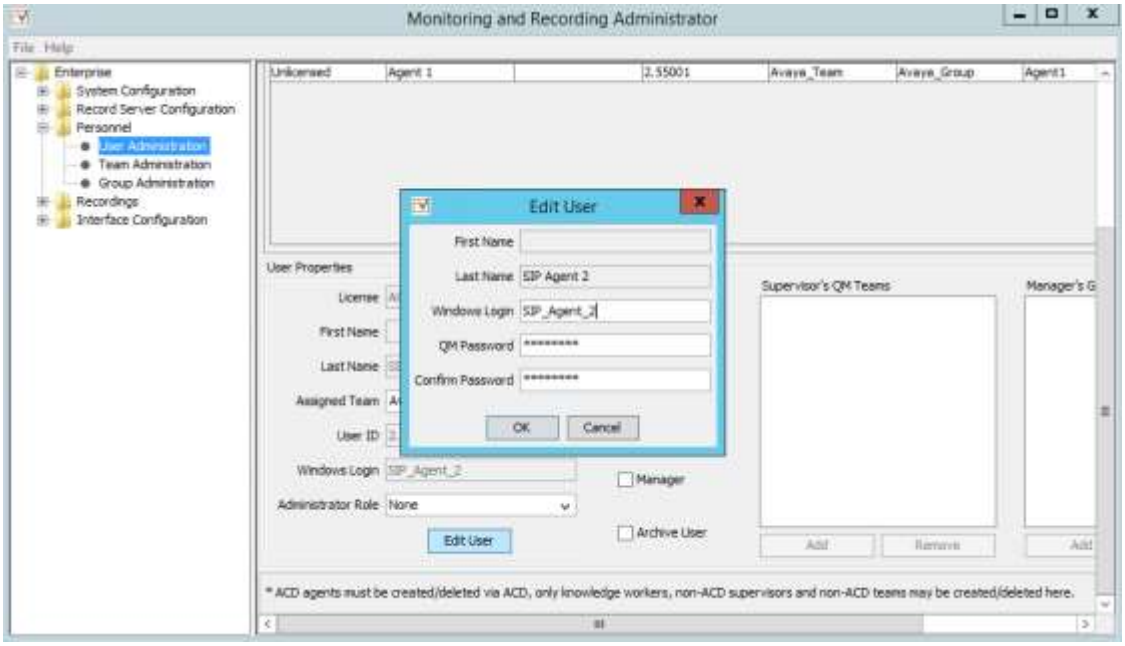
©2016 Avaya Inc. All Rights Reserved.

Step	Description
	Configuration of the Application Enablement Interfaces – DMCC (Continued) The **Avaya Configuration** screen is displayed. In the **AE Services** select **Add**: • **Host Name** or **IP Address** of the **Application Enablement Services** server • **Username** and **Password** (from **Section 6**, **Step 4**) • **4721** as the **port** (the default DMCC listening port) • **Device Password** for the recorded stations (from **Section 5**, **Step 6**). Note that all station passwords must be the same for this solution; however, check with Calabrio for alternatives if necessary. • **Switch Name** or **Switch IP Interface**. Enter the switch name or IP address of Communication Manager. Click **OK** to complete this step. 

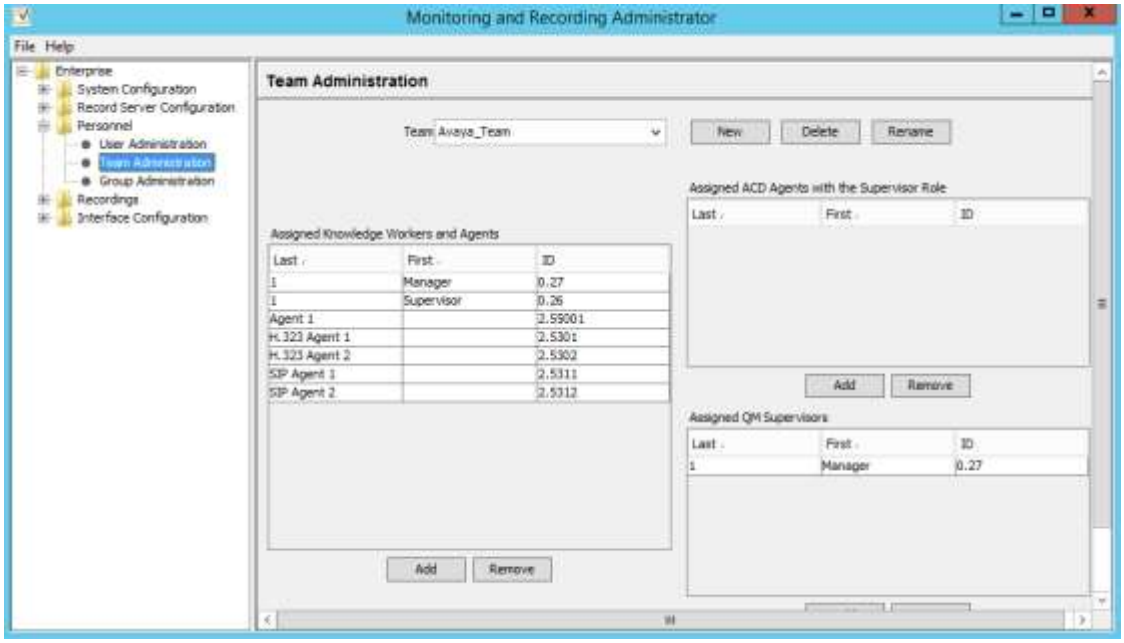
©2016 Avaya Inc. All Rights Reserved.

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**. 

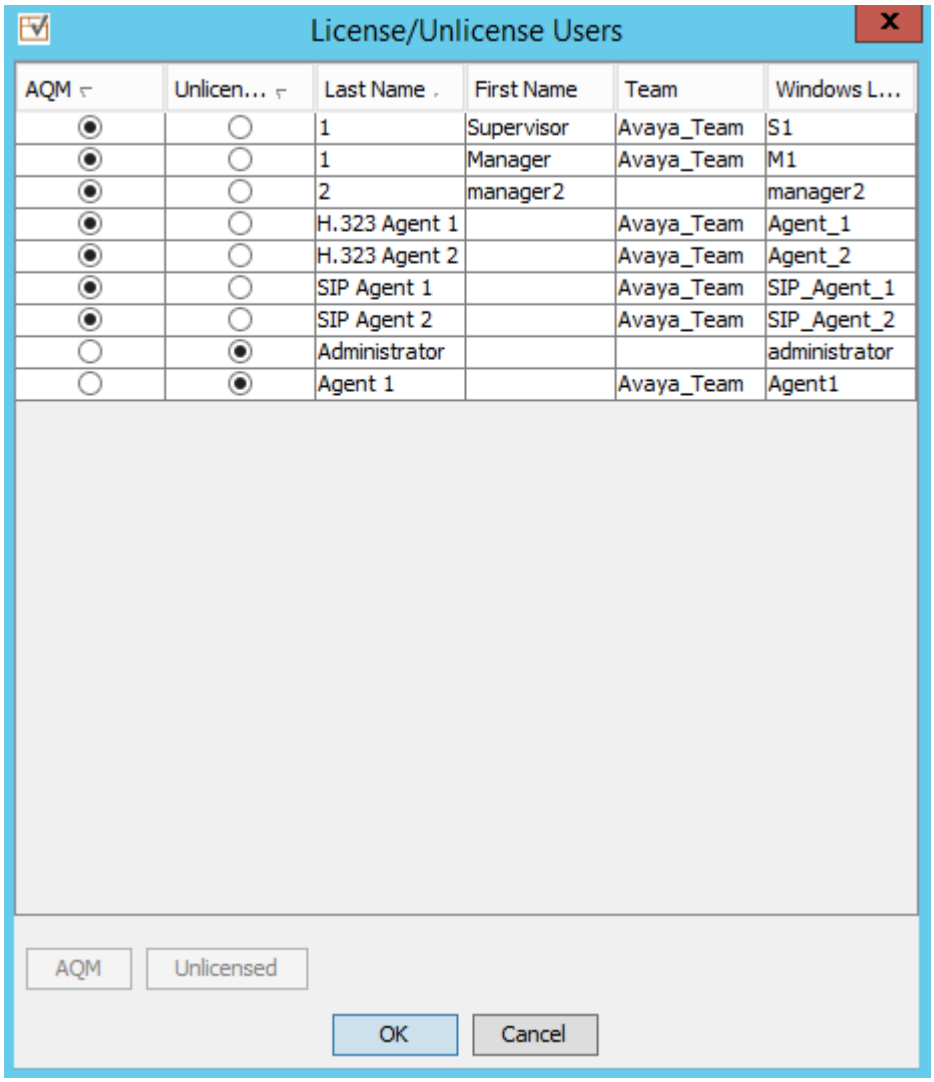
©2016 Avaya Inc. All Rights Reserved.

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 to create a user. 

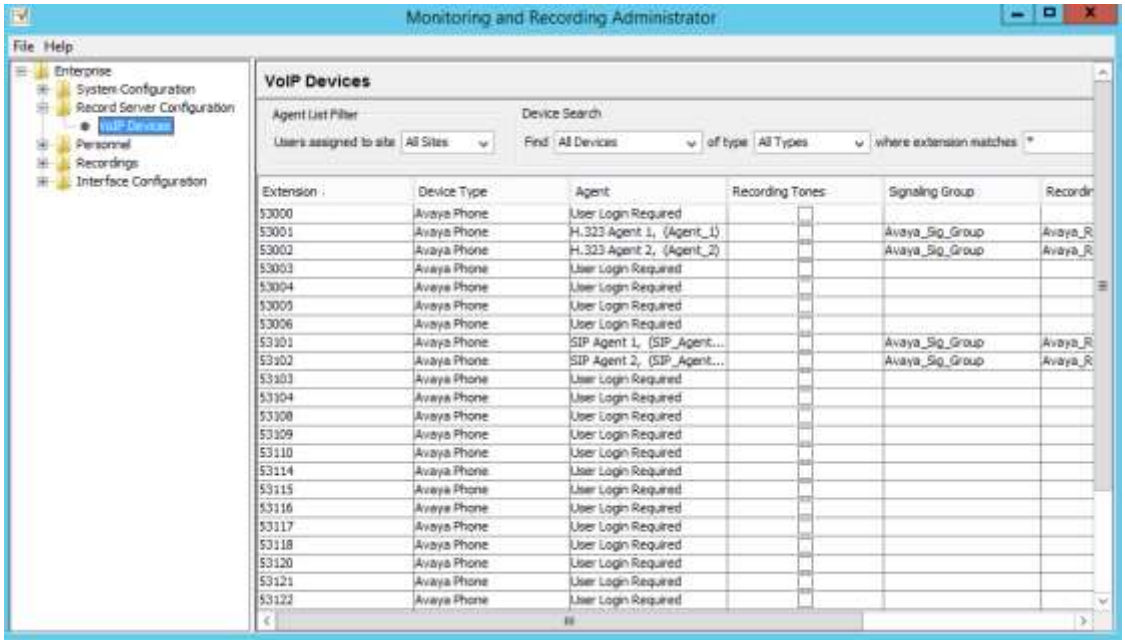
©2016 Avaya Inc. All Rights Reserved.

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

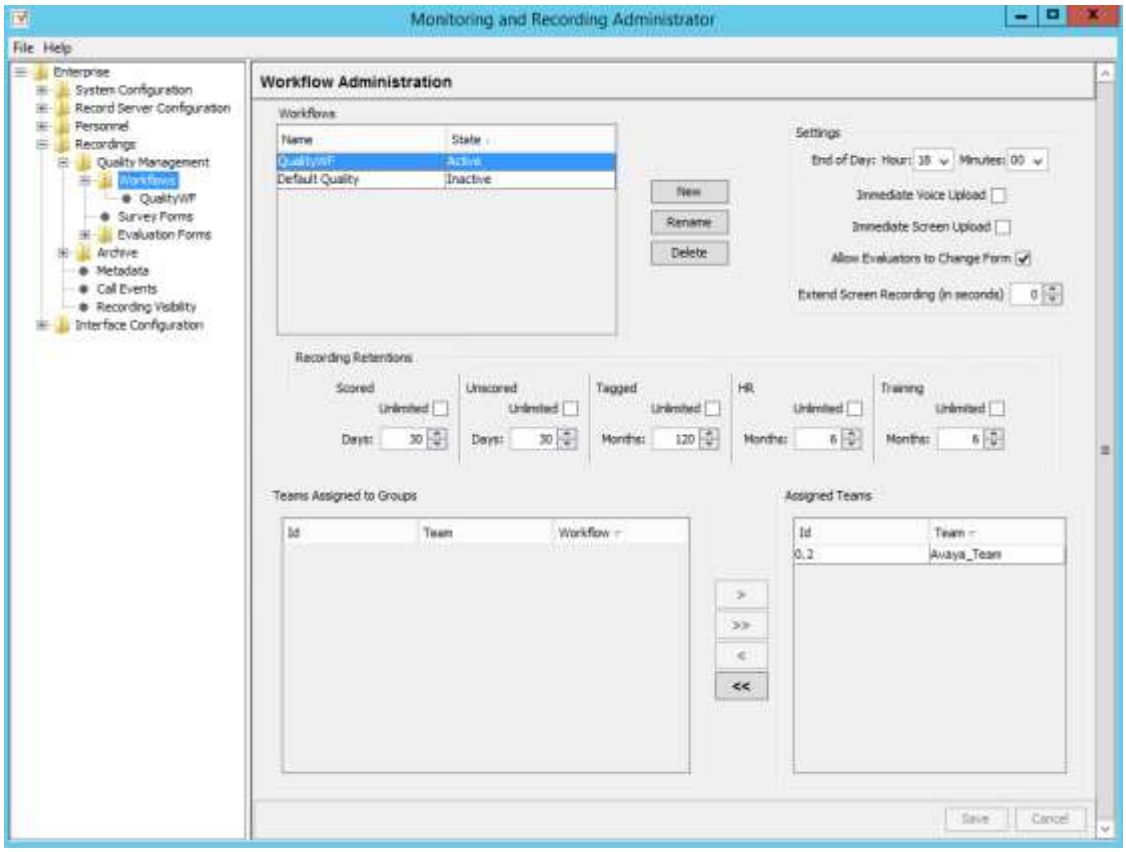
©2016 Avaya Inc. All Rights Reserved.

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. 

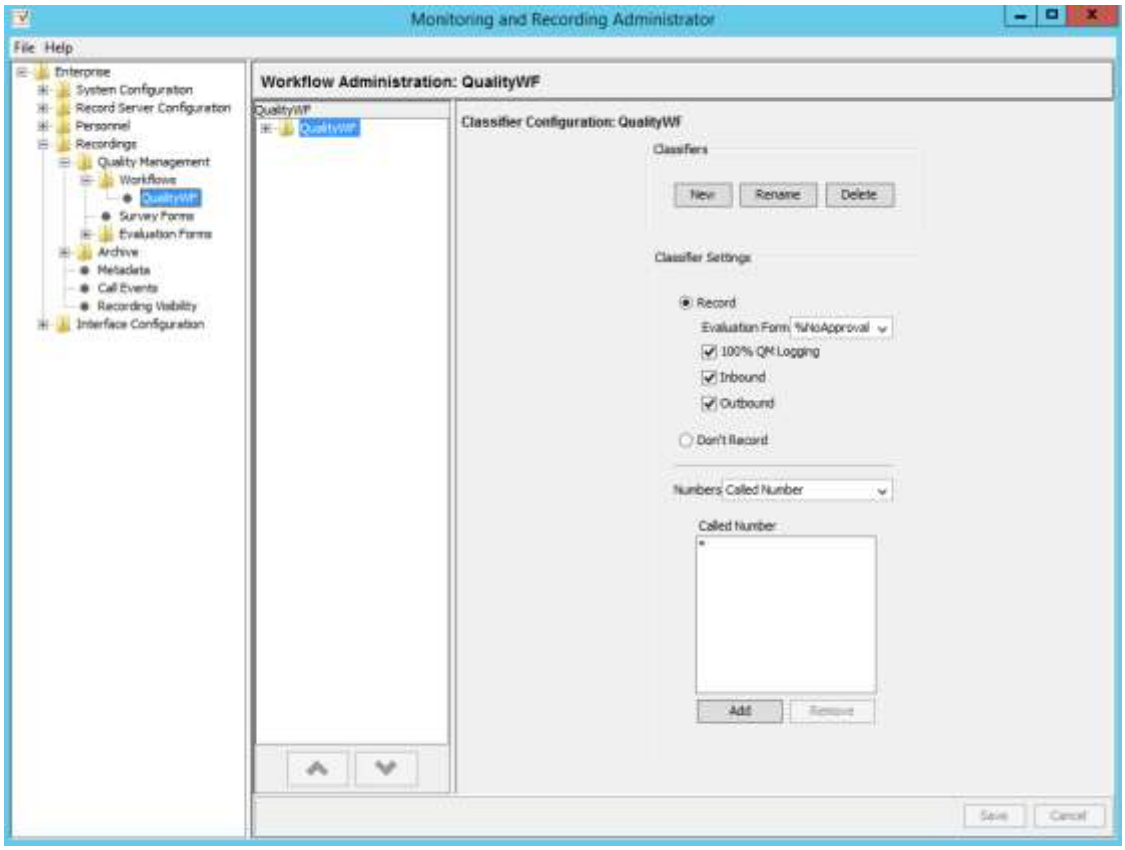
©2016 Avaya Inc. All Rights Reserved.

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. 

©2016 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. 

©2016 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. 

©2016 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

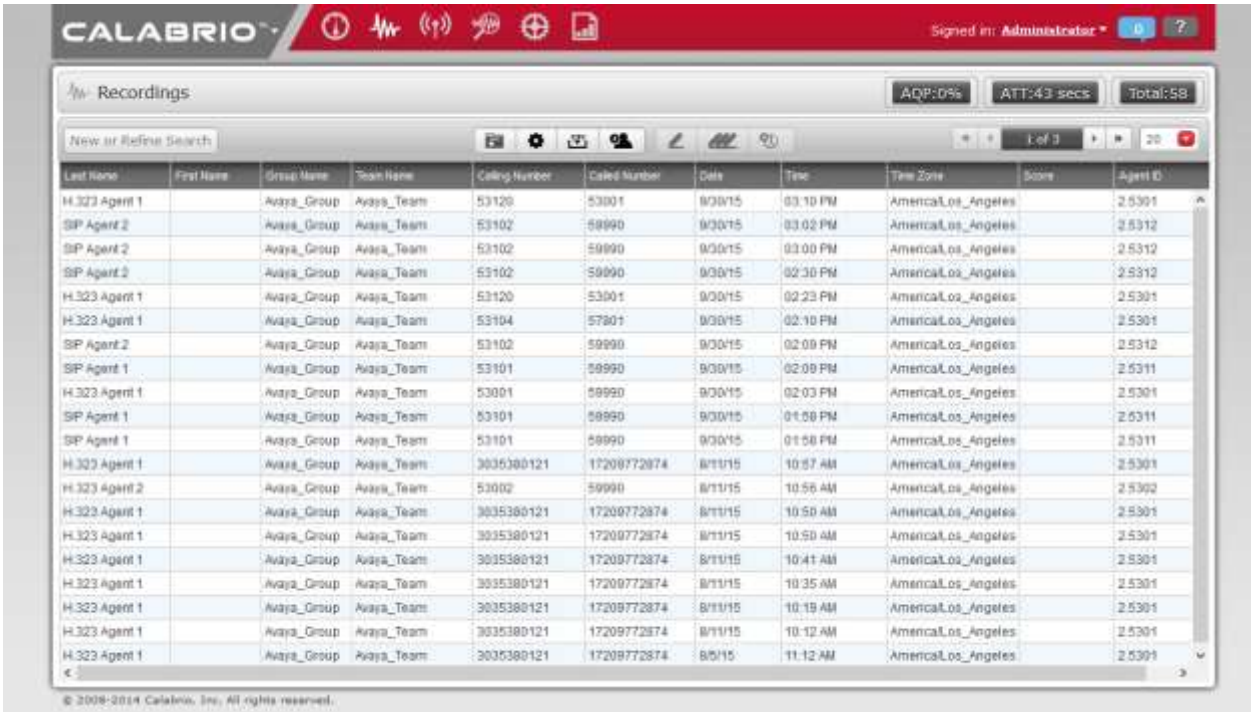
Access the Calabrio web-based user interface using the URL **http://<ip-address>** in a browser window, where **<ip-address>** is the address of the CRQM server. The **Log In** screen is displayed as shown below. Use appropriate credentials to log in.

©2016 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.

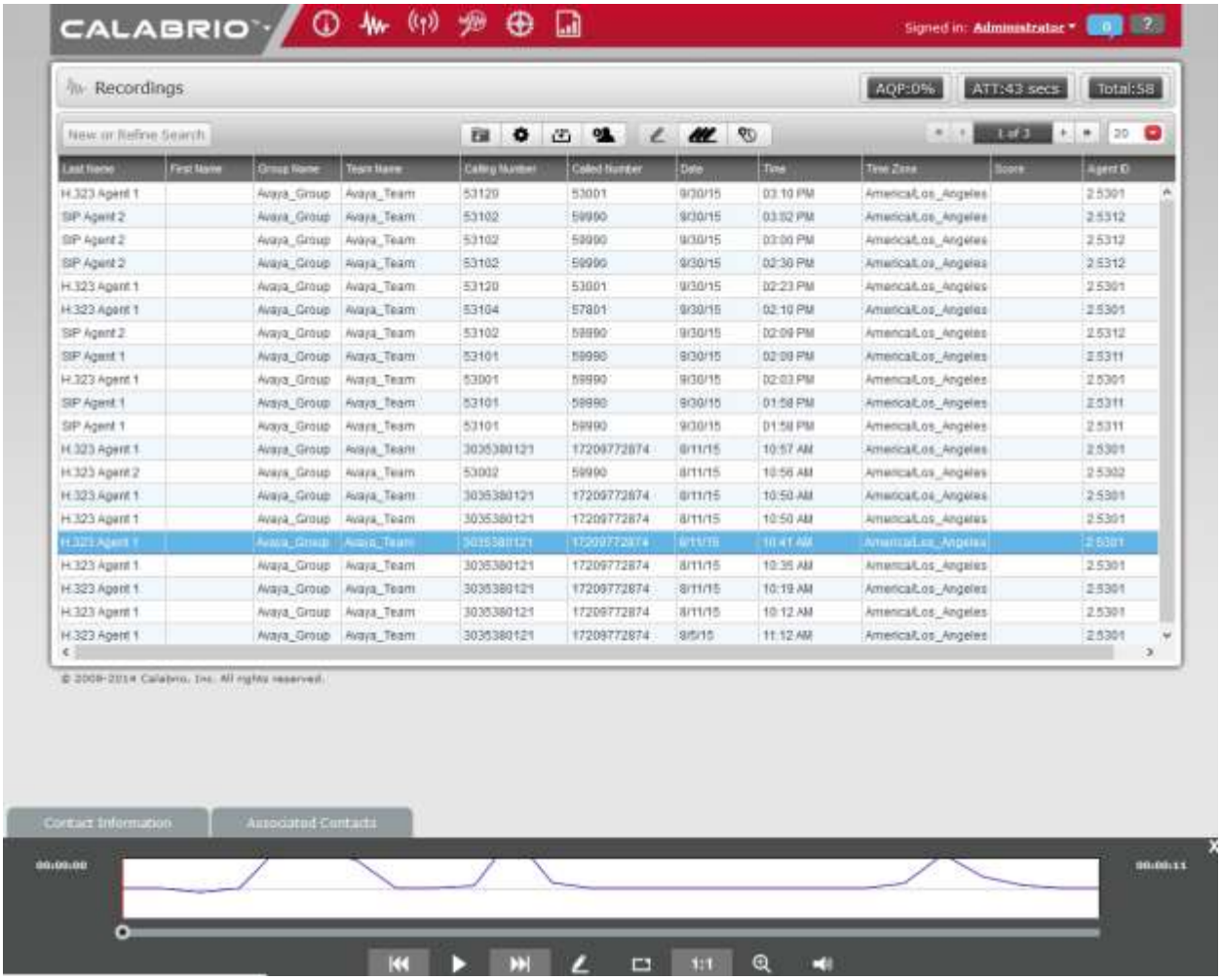
©2016 Avaya Inc. All Rights Reserved.

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



©2016 Avaya Inc. All Rights Reserved.

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



©2016 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.

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

©2016 Avaya Inc. All Rights Reserved.

©2016 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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

©2016 Avaya Inc. All Rights Reserved.