Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio One with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

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

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

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

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

1. Introduction

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

Before Calabrio can start recording, it establishes a client connection with AES and performs a SMS service query to obtain the list of agents and stations configured in Avaya Aura® Communication Manager (Communication Manager).

The application uses SMS to populate database information in the Calabrio system. The information collected are, list operation on Agent model, list and display operations on Station model and list operation on Hunt Group model.

The Calabrio DMCC integration works by using two supported DMCC methods, Single Step Conference and Multiple Registration, to capture the media for recording. The Single Step Conference method is used for users with Avaya SIP and Analog telephones, and the Multiple Registration method is used for users with Avaya H.323 and Digital telephones.

2. General Test Approach and Test Results

The compliance test focused on the ability for calls to be recorded. Calls were manually placed from the public switched telephone network (PSTN) directly to and from recorded devices, and to VDN or Skill group extension. For each recorded station in a call, there is one recording generated. Once a call is completed, the recordings are reviewed for their quality, completeness (number of recordings beginning to end, etc.), and accuracy of tagging information (owner, calling party, called party, etc).

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and Calabrio One did not include use of any specific encryption features as requested by Calabrio.

2.1. Interoperability Compliance Testing

The compliance test validated the ability of Calabrio to successfully record calls routed to and from Analog, Digital, and IP endpoints as well as softphone clients. Common call scenarios including hold/resume, mute/unmute, transfer, and conference were exercised during the test. Additional tests included the ability to monitor live calls and to record screen activity associated with a recorded station.

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

2.2. Test Results

All test cases passed with the following observations.

- Calling Number column is populated with the actual Called Number data for a blind conference call recording.

2.3. Support

Technical support on Calabrio can be obtained through the following:

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

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services
- Avaya Endpoints
- Calabrio One server installed on a standalone machine

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

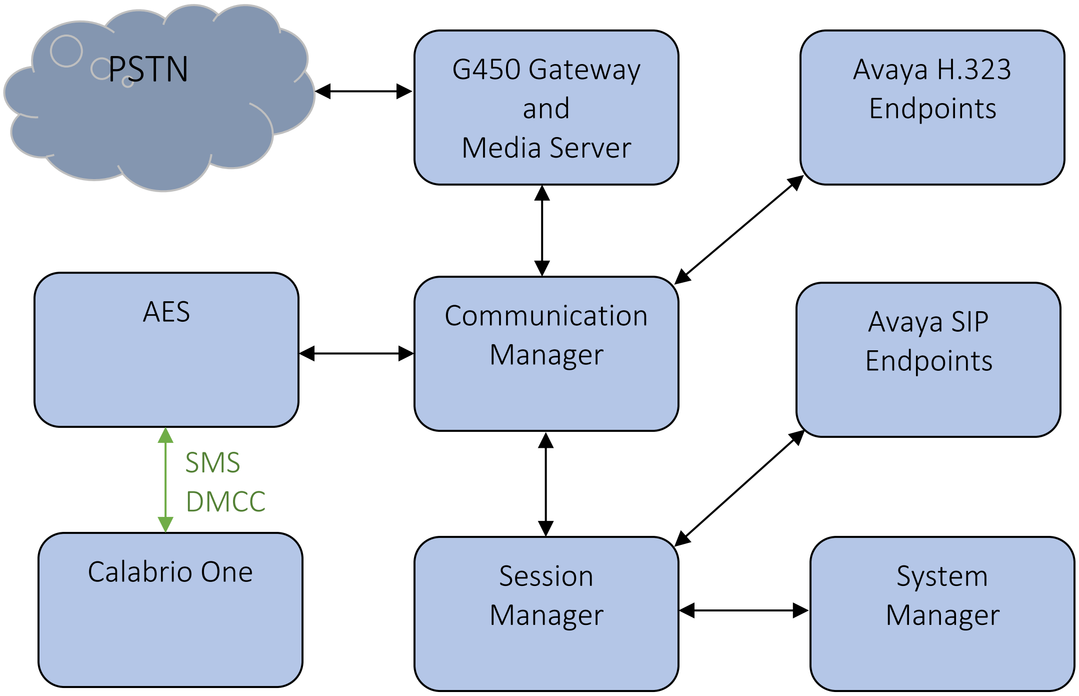


Figure 1 – Calabrio One Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.1.3.3.0-FP3SP3
Avaya Aura® Application Enablement Services running on virtualized environment	7.1.3.3.0.2-0
Avaya Aura® Session Manager running on virtualized environment	7.1.3.3.713307
Avaya Aura® System Manager	7.1.3.3.069127
Avaya Aura® Media Server	7.8.0.384
Avaya G450 Media Gateway	39.20.0
Avaya 96x1 Series IP Deskphone • 9641G (H.323) • 9611G (SIP)	 6.8102 7.1.5
Avaya 1416 Digital Deskphone	FW 1
2500 analog phone	-
Desktop PC running Avaya One-X® Communicator (H.323)	6.2.14 SP14
Desktop PC running Avaya One-X® Agent (H.323)	2.5.13
Calabrio Recording and Quality Management running under Windows 2016 Server • Avaya DMCC SDK 7.0 • Java Development Kit	10.4.18.810 7.0 1.8

5. Configure Avaya Aura® Communication Manager

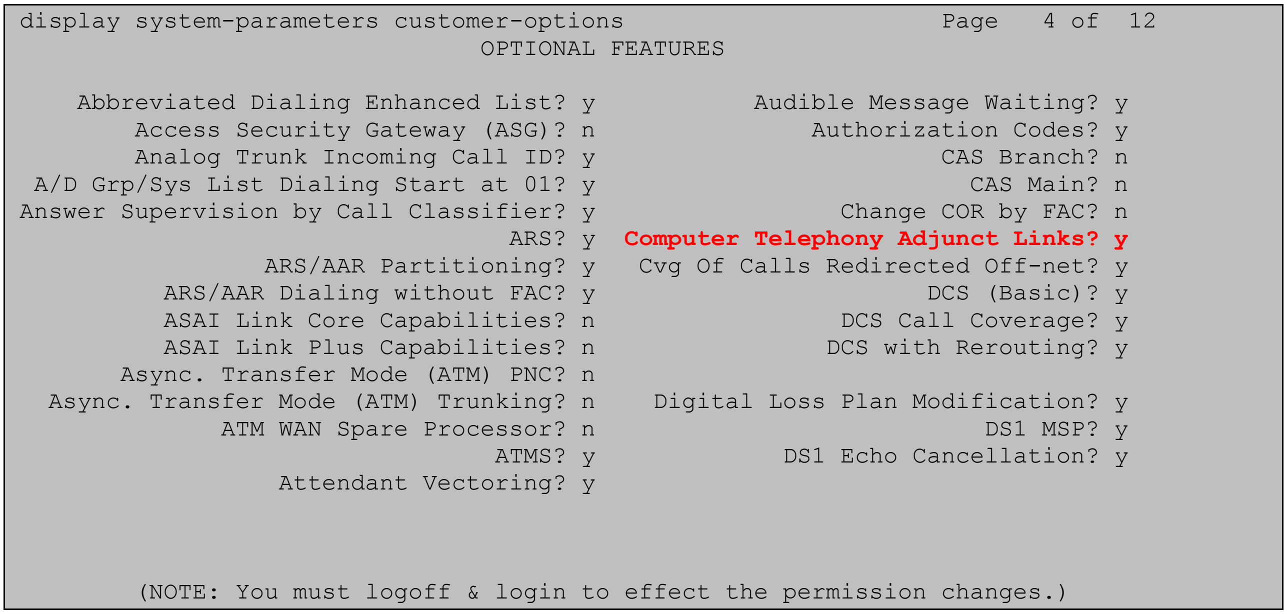
This section provides the procedures for configuring Communication Manager. The procedures fall into the following areas:

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer IP Services for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Add SMS User Account
- Verify Recorded Extensions
- Add Virtual Stations

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation in **Section 10**.

5.1. Verify Feature and License

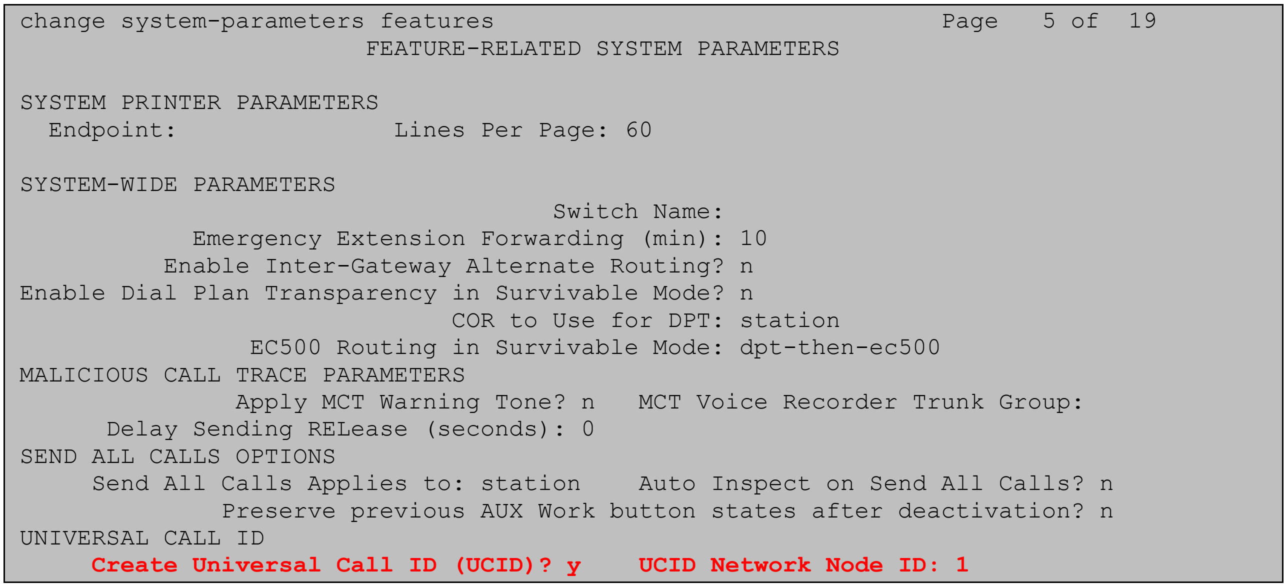
Enter the **display system-parameters customer-options** command and ensure that **Computer Telephony Adjunct Links** is set to **y.** If this option is not set to **y**, contact the Avaya sales team or business partner for a proper license file.



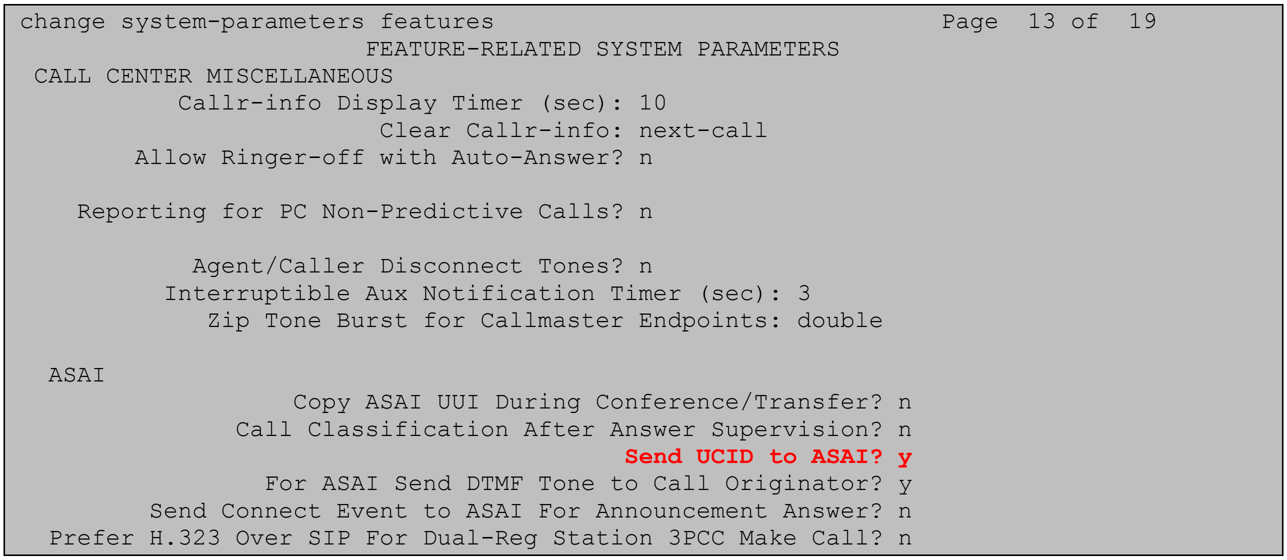
```
display system-parameters customer-options                      Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y            Audible Message Waiting? y
        Access Security Gateway (ASG)? n                Authorization Codes? y
        Analog Trunk Incoming Call ID? y                         CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                           CAS Main? n
Answer Supervision by Call Classifier? y                  Change COR by FAC? n
                                  ARS? y   Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y    Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  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



        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that on page 5 **Create Universal Call ID (UCID)** is enabled and a relevant **UCID Network Node ID** (**1** was used in the test) is defined. Also ensure that on Page 13 that **Send UCID to ASAI** is set to **y**. Calabrio 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
```

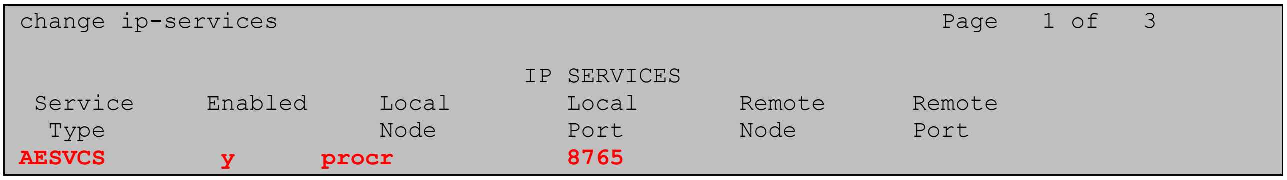


```
change system-parameters features                               Page   13 of   19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? 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
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.3. Administer IP-Services for Application Enablement Services

Add an IP Services entry for Application Enablement Services as described below:

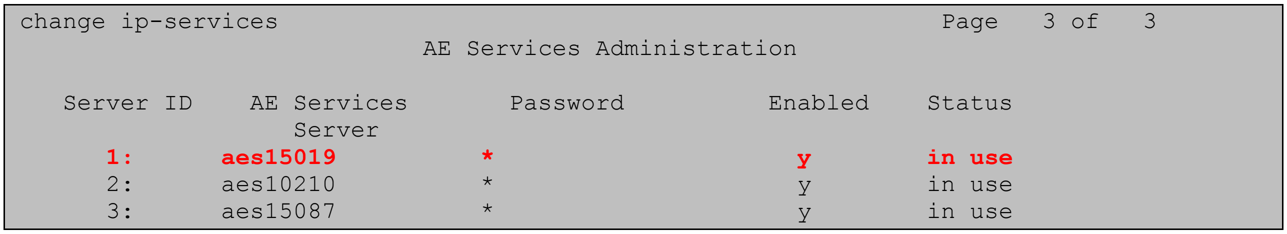
- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration.



```
change ip-services                                           Page   1 of   3

                                    IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS           y       procr          8765
```

On Page 3 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6.1**.
- In the **Enabled** field, type **y**.

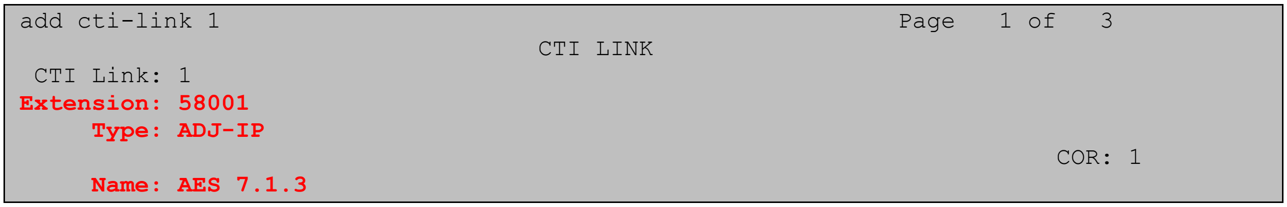


```
change ip-services                                           Page   3 of   3
                           AE Services Administration

   Server ID     AE Services        Password          Enabled     Status
                    Server
      1:       aes15019          *                   y         in use
      2:       aes10210          *                   y         in use
      3:       aes15087          *                   y         in use
```

5.4. Administer Computer Telephony Integration (CTI) Link

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type a valid extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

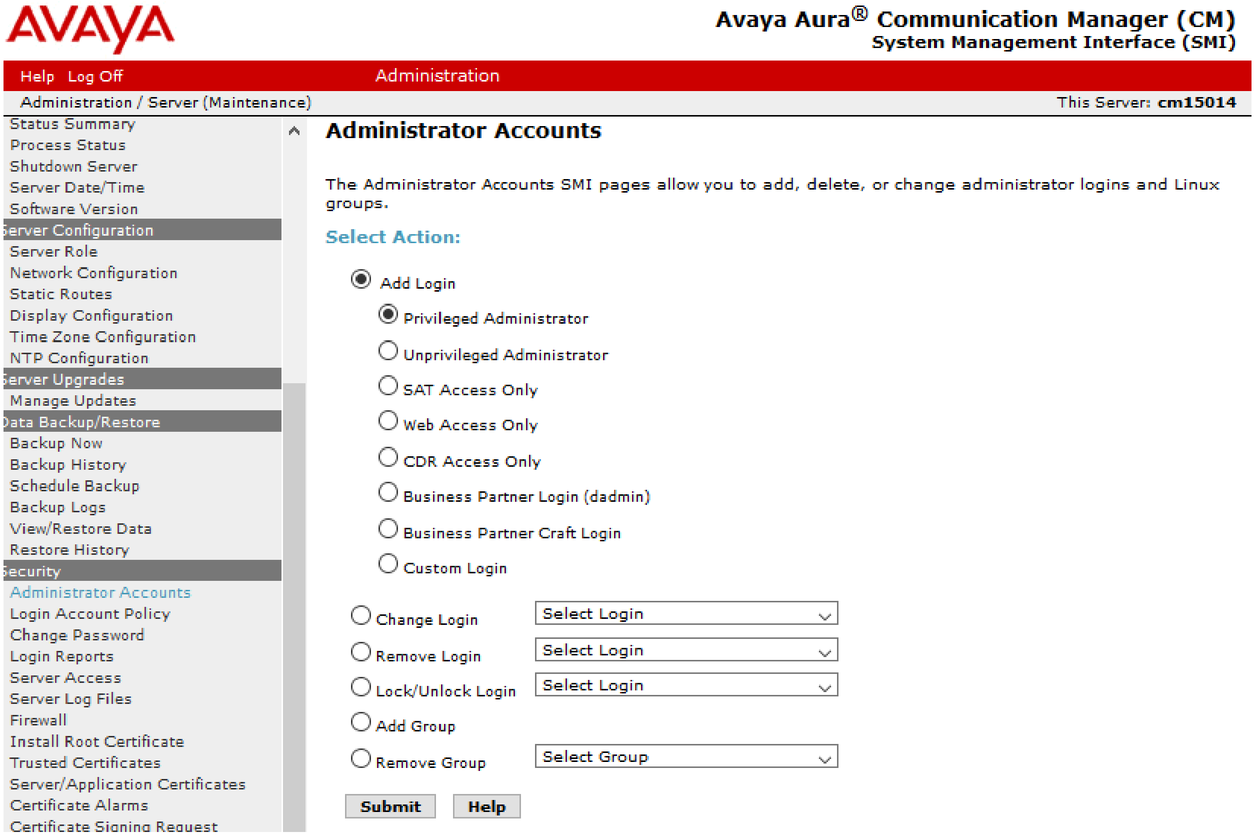


```
add cti-link 1                                             Page   1 of   3
                                     CTI LINK
 CTI Link: 1
Extension: 58001
     Type: ADJ-IP
                                                                     COR: 1

     Name: AES 7.1.3
```

5.5. Add SMS User Account

Calabrio 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. Access the System Management Interface by typing the IP address of Communication Manager in the URL of a web browser. Log in using proper credentials and navigate to **Administration → Server (Maintenance)**. The **Administration/Server (Maintenance)** screen is seen as shown below. Create a user account on Communication Manager by navigating to the **Administer Accounts** page under **Security** from the left hand pane and selecting the radio button **Add Login** and **Privileged Administrator**. Click **Submit** to continue the process.



Administrator Accounts

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

Select Action:

● Add Login
- ● Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

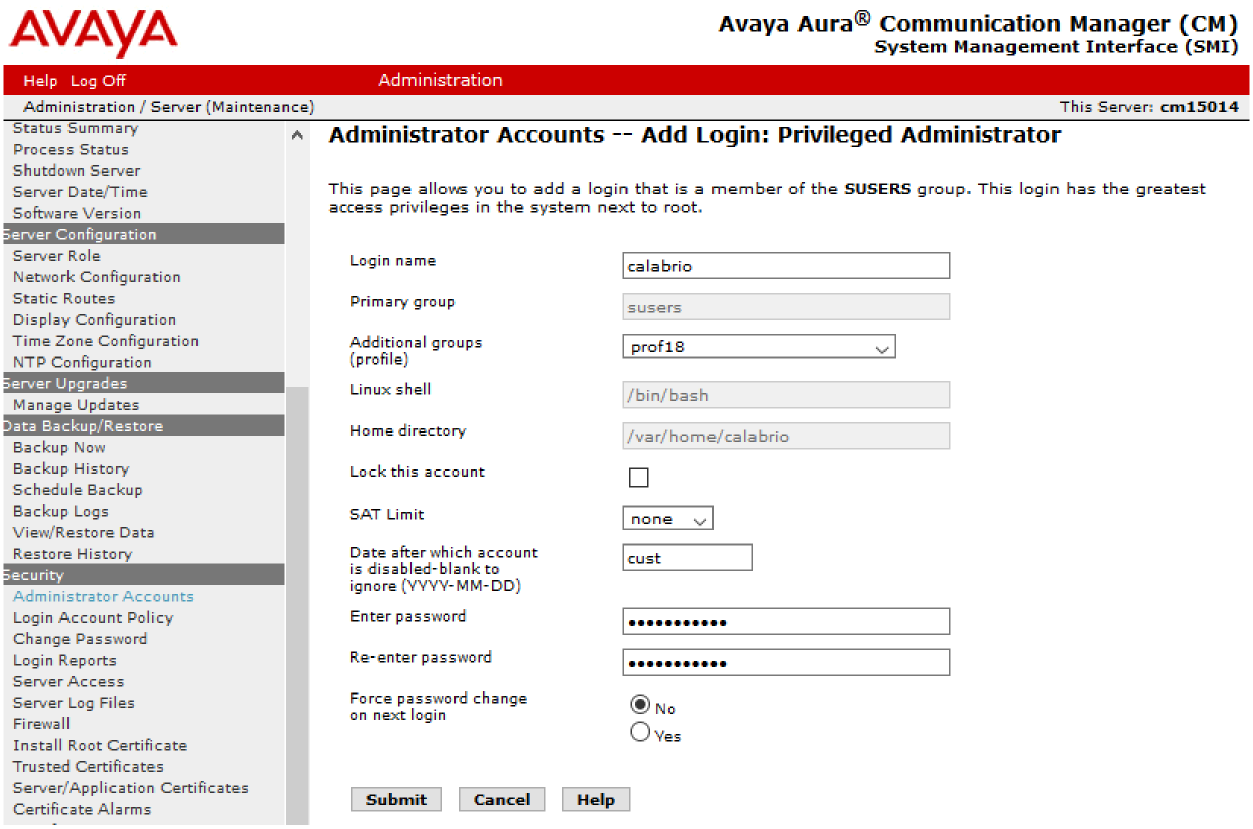
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

The **Administrator Accounts -- Add Login** screen is displayed. Enter a name to the **Login name** field and enter desired password.



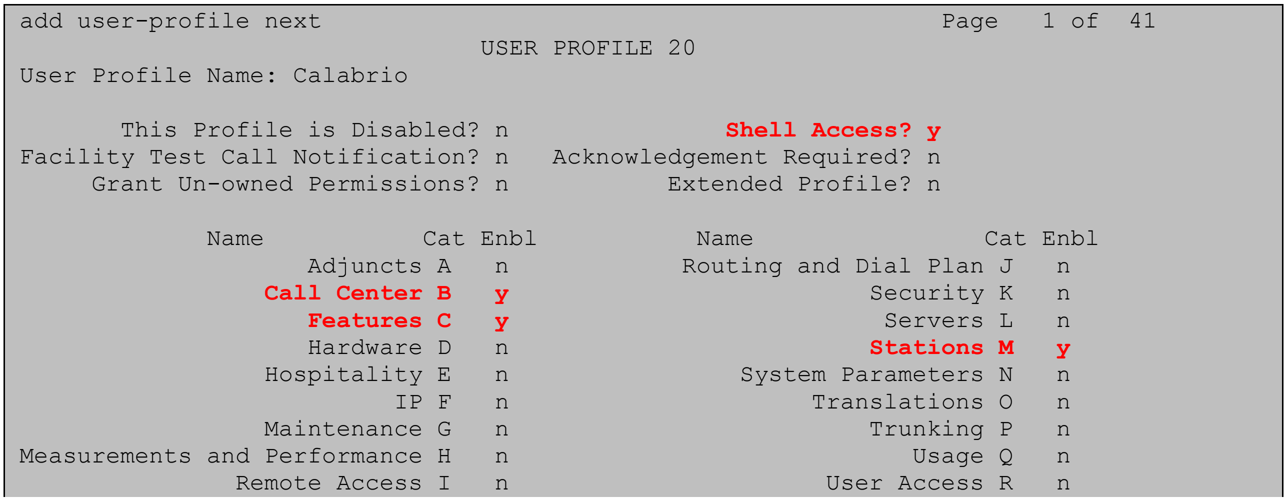
Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name	calabrio
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/calabrio
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	cust
Enter password	•••••••••••
Re-enter password	•••••••••••
Force password change on next login	● No ○ Yes

Submit Cancel Help

Though a Privileged Administrator account was used, a new SMS user profile can be added to limit permissions. Use the **add user-profile next** command to add a new user profile. Set the **Shell Access, Call Center B, Features C,** and **Stations M** to **y.** This profile will need to be assigned to user created above.



```
add user-profile next                                          Page   1 of  41
                                USER PROFILE 20
User Profile Name: Calabrio

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

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

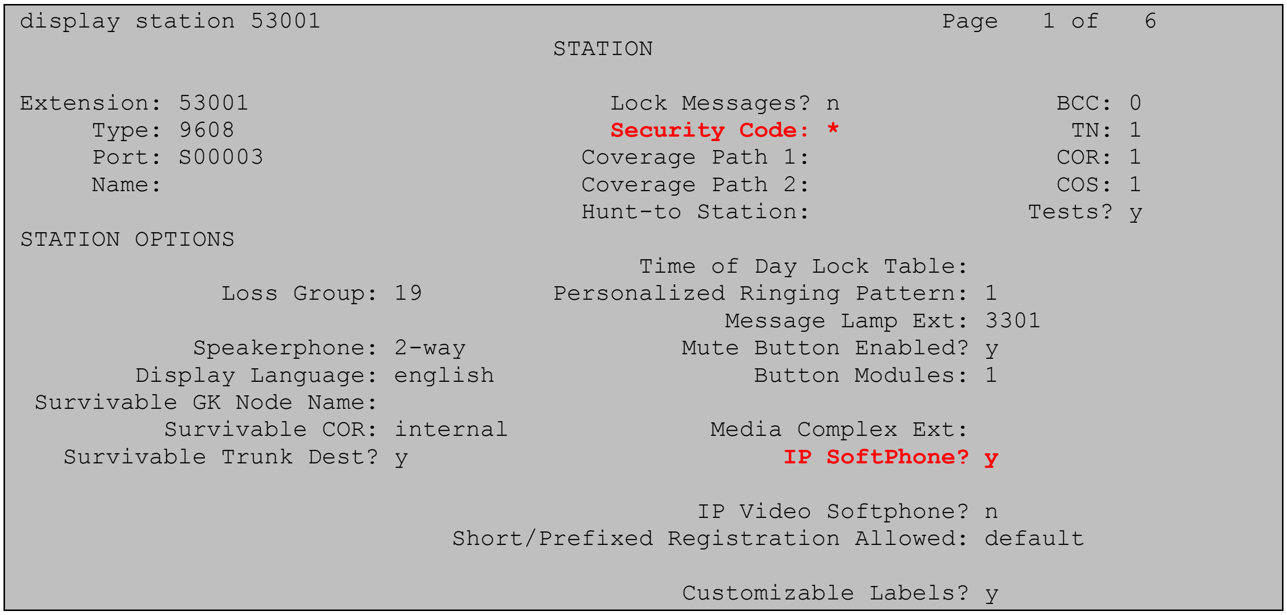
5.6. Verify Recorded Extensions

For H.323 and Digital stations that will be recorded, enable **IP Softphone** as shown below, which will be used by Calabrio to correspond to the Multiple Registration recording method. Calabrio needs to know the **Security Code** in order to successfully register, ensure that security codes are set to the same value for these stations; however, check with Calabrio for alternatives if necessary.

For SIP and Analog stations that will be recorded, leave the **IP Softphone** setting disabled, which will be used by Calabrio to correspond to the Single Step Conference recording method.

Use the **display station n** command to verify information, or **change station n** to make changes if necessary.

Note that all SIP station configurations need to be completed from Session Manager via System Manager.

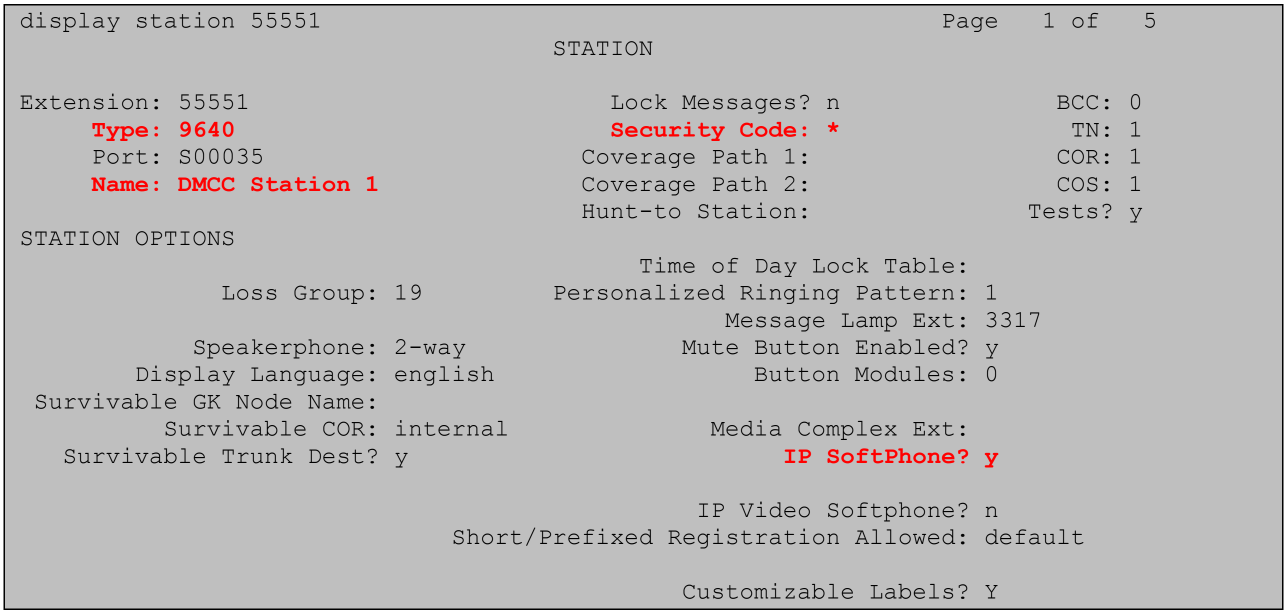


```
display station 53001                                           Page   1 of   6
                                     STATION

Extension: 53001                         Lock Messages? n                BCC: 0
     Type: 9608                          Security Code: *                 TN: 1
     Port: S00003                      Coverage Path 1:                 COR: 1
     Name:                             Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 3301
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 1
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

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

                                              Customizable Labels? y
```

5.7. Add Virtual Stations

Virtual stations are used by Calabrio to do Single Step Conference based call recording for SIP and Analog stations. Add a virtual station using the **add station <n>** command; where **<n>** is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields. Note that the number of virtual stations configured should be equal to the number of stations that will be recorded simultaneously.

- In the **Type** field, enter a station type such as **9640**.
- In the **Name** field, enter a name containing the **DMCC** string (e.g. **DMCC Station 1**). Calabrio uses the DMCC prefix string to identify virtual stations.
- In the **Security Code** field, enter a desired value.
- Set the **IP SoftPhone** field to **y**.



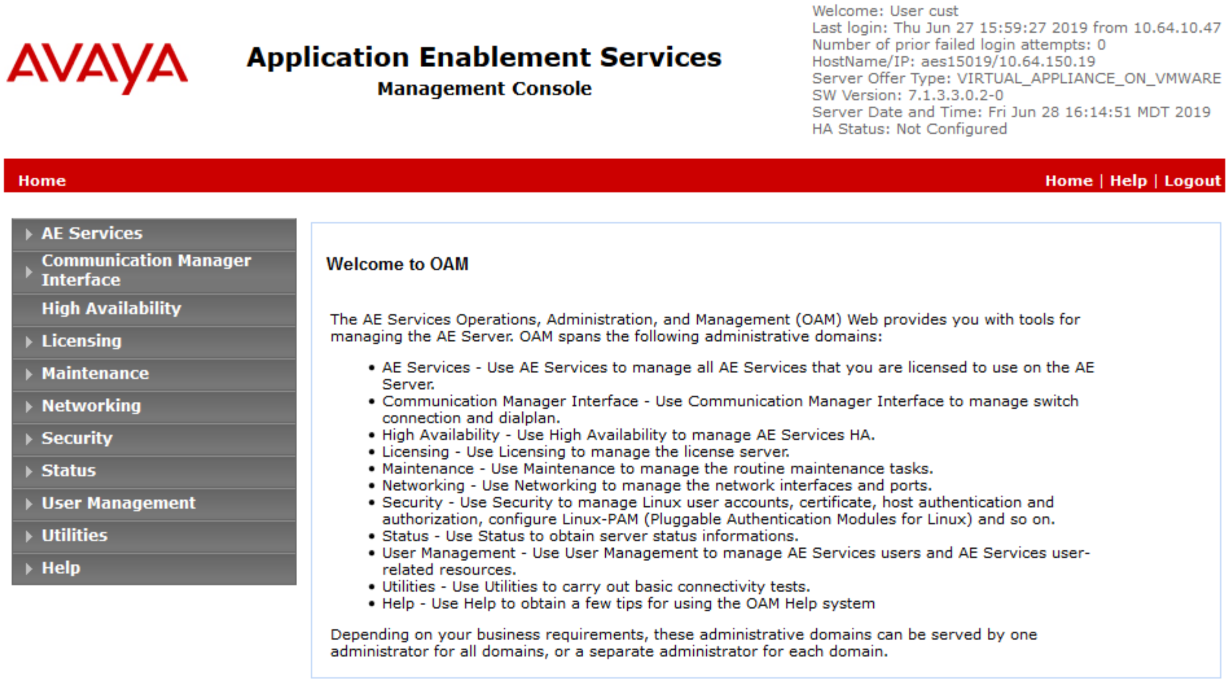
```
display station 55551                                           Page   1 of   5
                                     STATION

Extension: 55551                         Lock Messages? n               BCC: 0
     Type: 9640                          Security Code: *                TN: 1
     Port: S00035                      Coverage Path 1:                 COR: 1
     Name: DMCC Station 1              Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 3317
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                   Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

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

                                              Customizable Labels? Y
```

6. Configure Avaya Aura® Application Enablement Services

All administration of Application Enablement Services is performed via a web browser. Enter https://<ip-addr> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Configure Calabrio User
- Confirm TSAPI and DMCC Licenses



Welcome: User cust
Last login: Thu Jun 27 15:59:27 2019 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.3.0.2-0
Server Date and Time: Fri Jun 28 16:14:51 MDT 2019
HA Status: Not Configured

Welcome to OAM

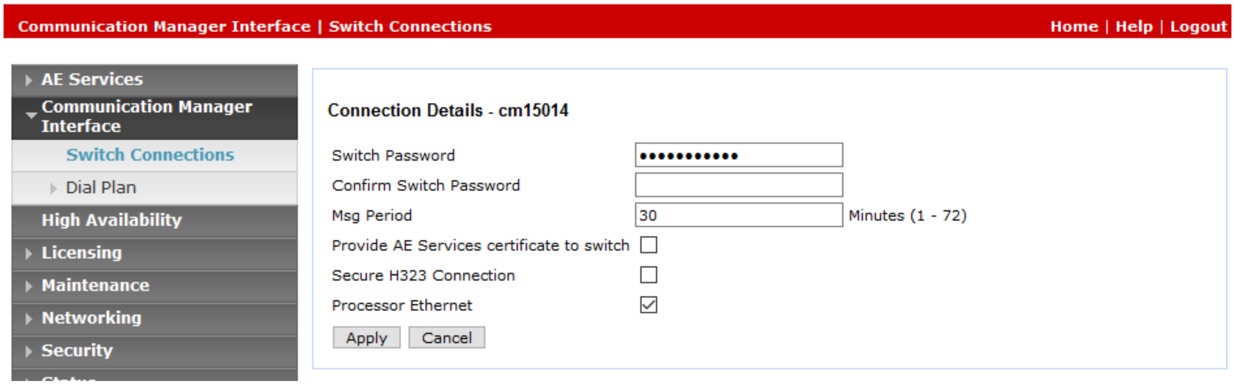
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

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

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

6.1. Configure Communication Manager Switch Connections

To add links to Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection (e.g. **cm15014**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5.3** and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.

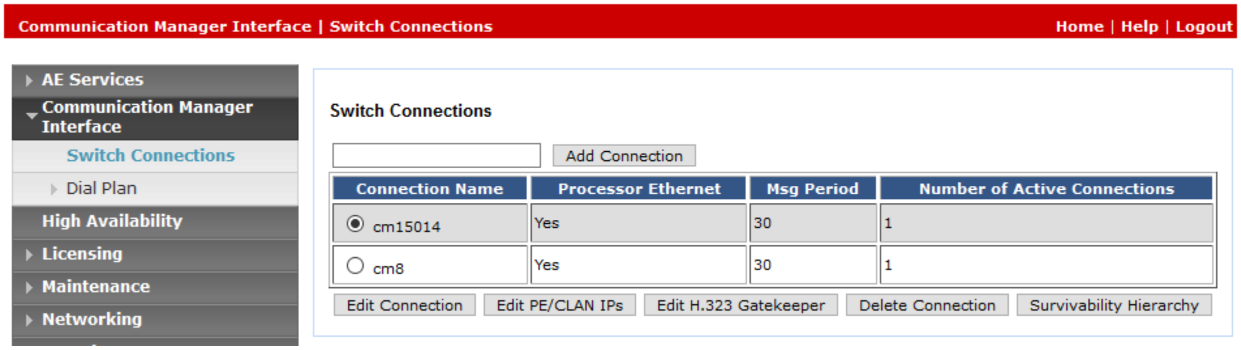


Connection Details - cm15014

Switch Password	••••••••••••	
Confirm Switch Password		
Msg Period	30	Minutes (1 - 72)
Provide AE Services certificate to switch	□	
Secure H323 Connection	□	
Processor Ethernet	☑	

Apply Cancel

The display returns to the **Switch Connections** screen which shows that the **cm15014** switch connection has been added.



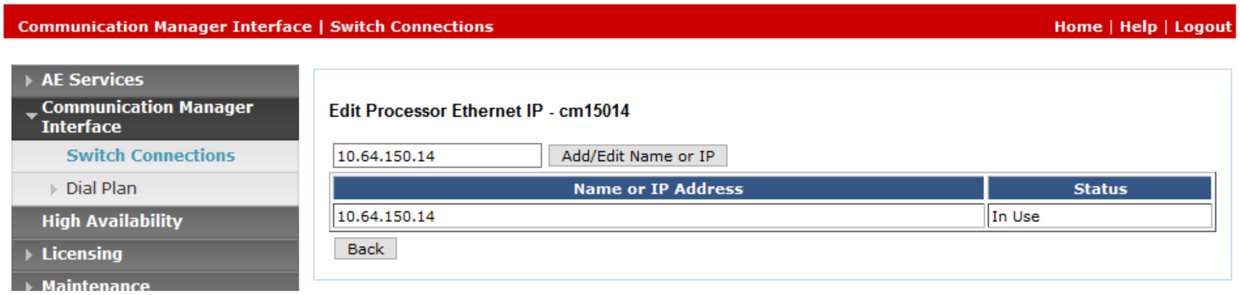
Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm15014	Yes	30	1
○ cm8	Yes	30	1

Edit Connection | Edit PE/CLAN IPs | Edit H.323 Gatekeeper | Delete Connection | Survivability Hierarchy

Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es). The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.



Edit Processor Ethernet IP - cm15014

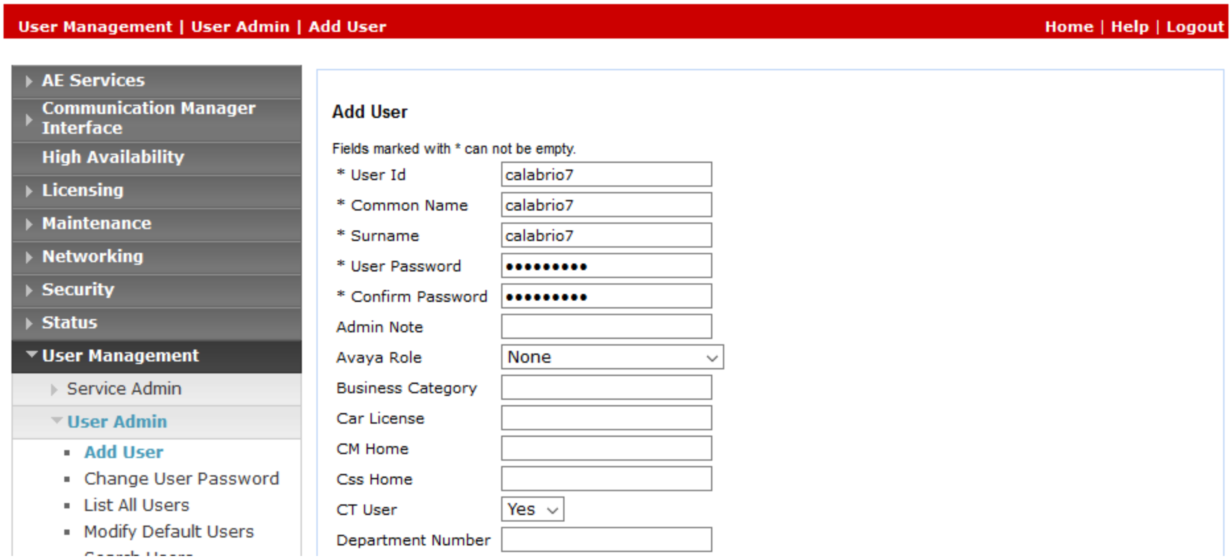
10.64.150.14

Name or IP Address	Status
10.64.150.14	In Use

6.2. Configure Calabrio User

In the Navigation Panel, select **User Management → User Admin → Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list.

Click **Apply** (not shown) at the bottom of the pages to save the entry.



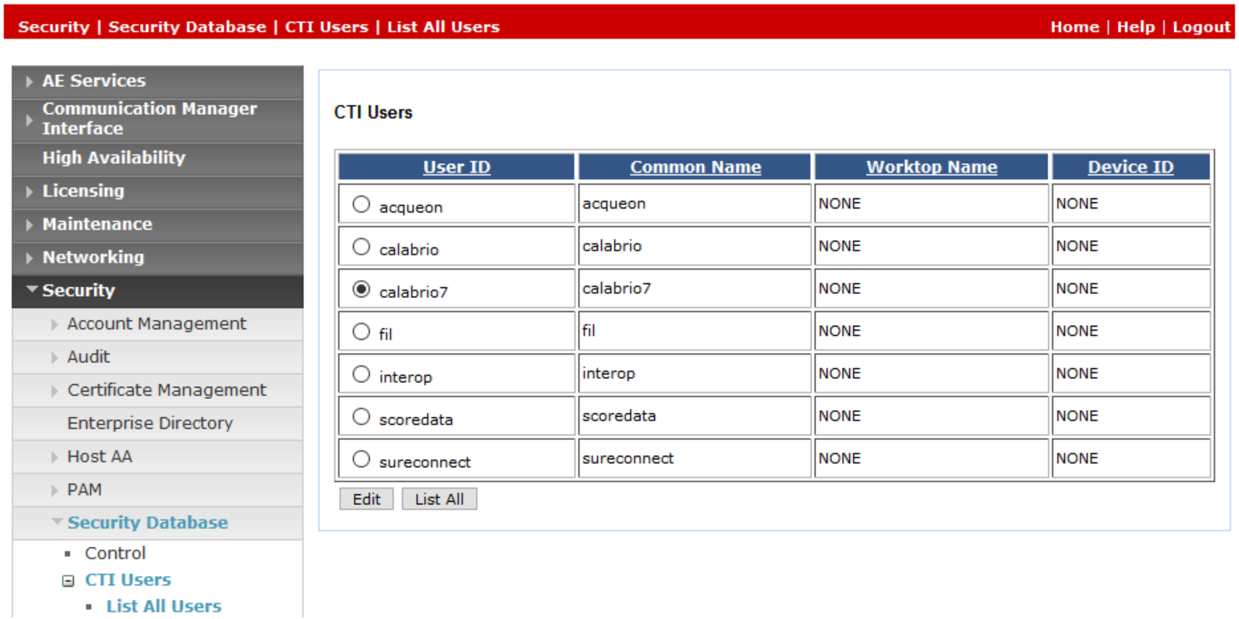
Add User

Fields marked with * can not be empty.

* User Id	calabrio7
* Common Name	calabrio7
* Surname	calabrio7
* User Password	•••••••••
* Confirm Password	•••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	

If the Security Database (SDB) is enabled on Application Enablement Services, set the Calabrio user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

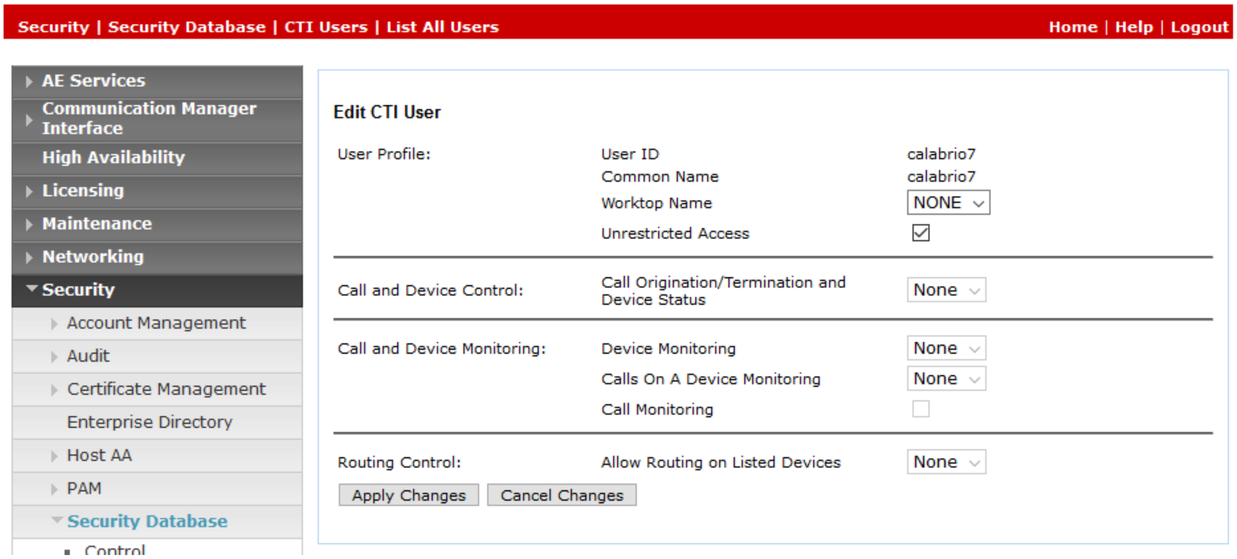
Navigate to **Security → Security Database → CTI Users → List All Users** and select the **calabrio** user and click **Edit**.



CTI Users

User ID	Common Name	Worktop Name	Device ID
○ acqueon	acqueon	NONE	NONE
○ calabrio	calabrio	NONE	NONE
● calabrio7	calabrio7	NONE	NONE
○ fil	fil	NONE	NONE
○ interop	interop	NONE	NONE
○ scoredata	scoredata	NONE	NONE
○ sureconnect	sureconnect	NONE	NONE

On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog (not shown).



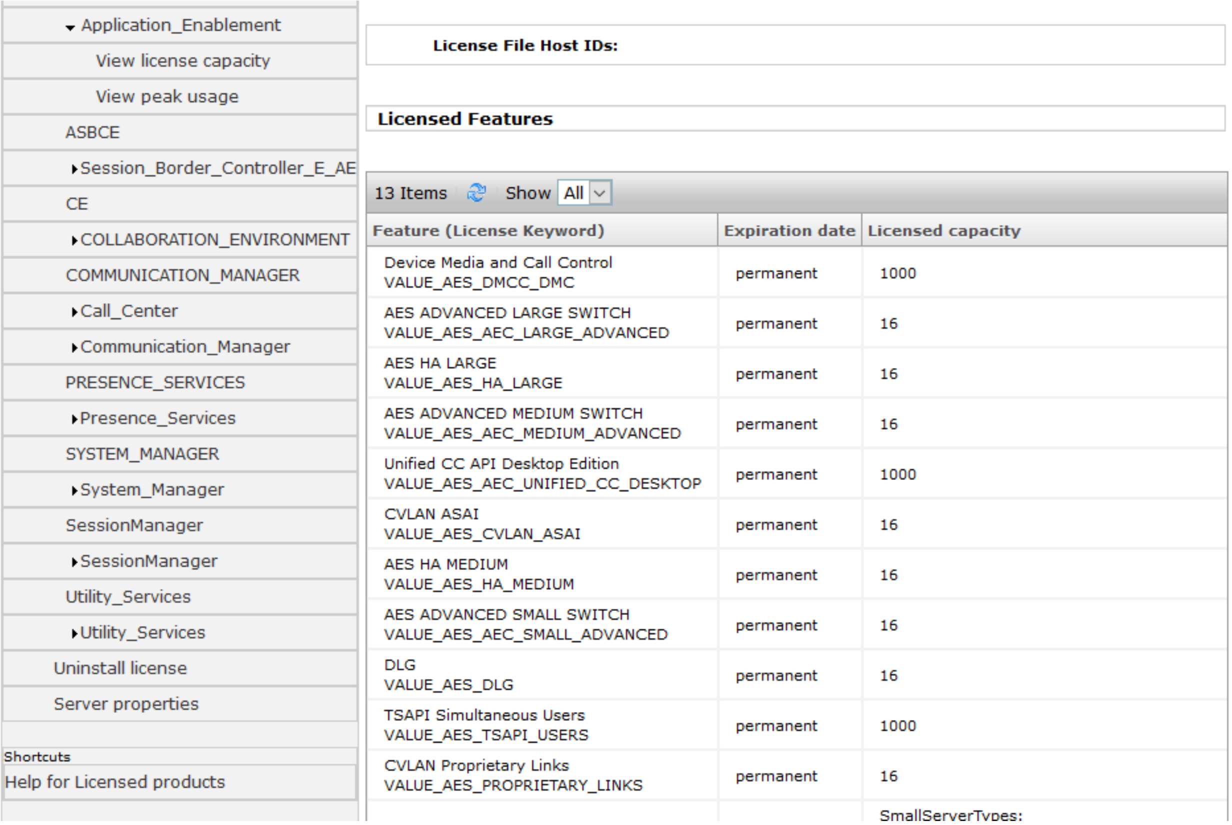
Edit CTI User

User Profile:	User ID	calabrio7
	Common Name	calabrio7
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

6.3. Confirm TSAPI and DMCC Licenses

Calabrio uses a DMCC (**VALUE_AES_DMCC_DMC**) license for each recording port. Additionally, a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license is used for each agent station being monitored. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.

From the left pane menu on Application Enablement Services Management Console, click **Licensing → WebLM Server Access** (not shown). A **Web License Manager** login window is displayed (not shown). Enter proper credentials to log in. Click **Licensed products → APPL_ENAB → Application_Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough **Device Media and Call Control** and **TSAPI Simultaneous Users** licenses available.



Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	16
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	16
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
		SmallServerTypes:

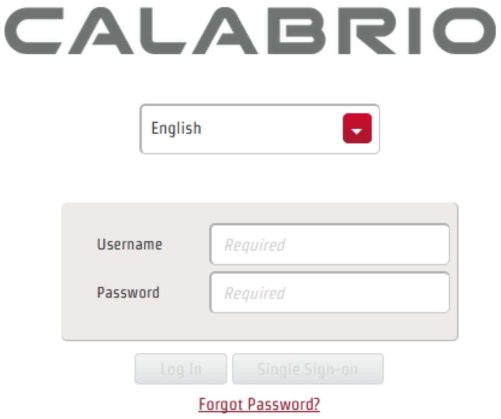
7. Configure Calabrio One

The initial configuration of the Calabrio server is typically performed by Calabrio technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the Calabrio solution to interoperate with Communication Manager and Application Enablement Services. Configuration in this section was performed with the assistance from a Calabrio engineer.

The steps include:

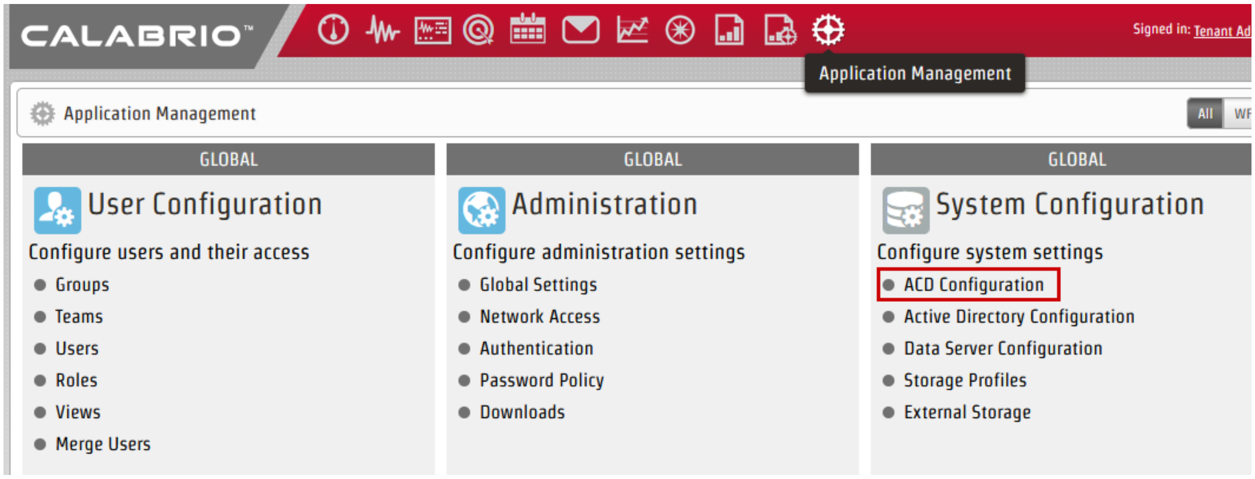
- Configuration of the Application Enablement Interfaces – SMS
- Installation of the Data Server
- Configuration of the Data Server
- Configuration of the Application Enablement Interfaces – DMCC
- Configuration of Device Associations

The configuration of the Calabrio server is performed using Calabrio One web interface. Access the web interface via a browser to the IP Address of Calabrio One server. Log on using appropriate credentials.

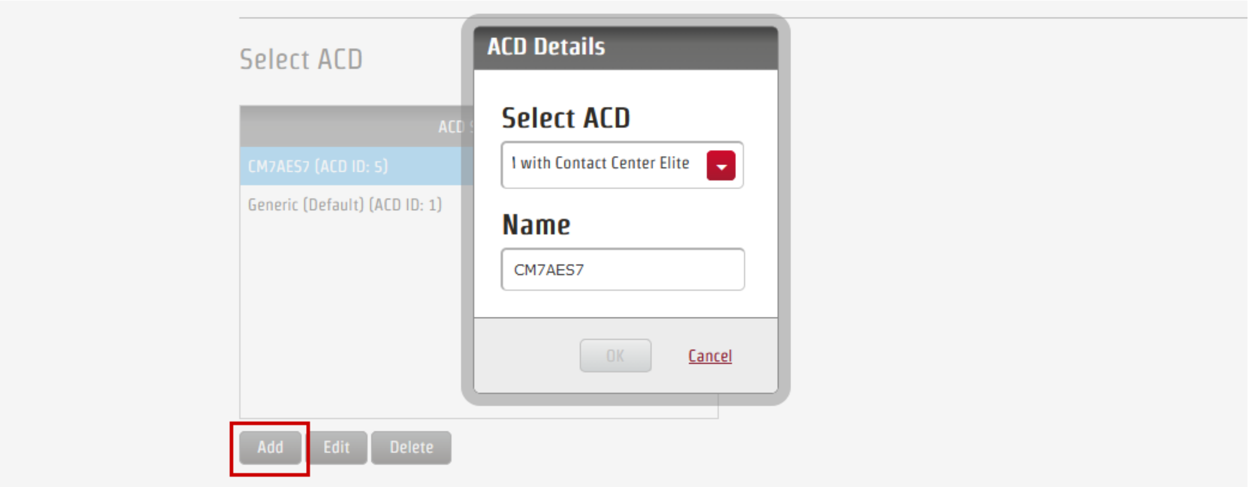


7.1. Configuration of the Application Enablement Interfaces – SMS

From the **Dashboard,** navigate to **Application Management → ACD Configuration.**



On the **ACD Configuration** page, select **Add** to add a new ACD. Select **Avaya CM with Contact Center Elite** from the **Select ACD** drip down menu and type in a **Name** for the ACD.



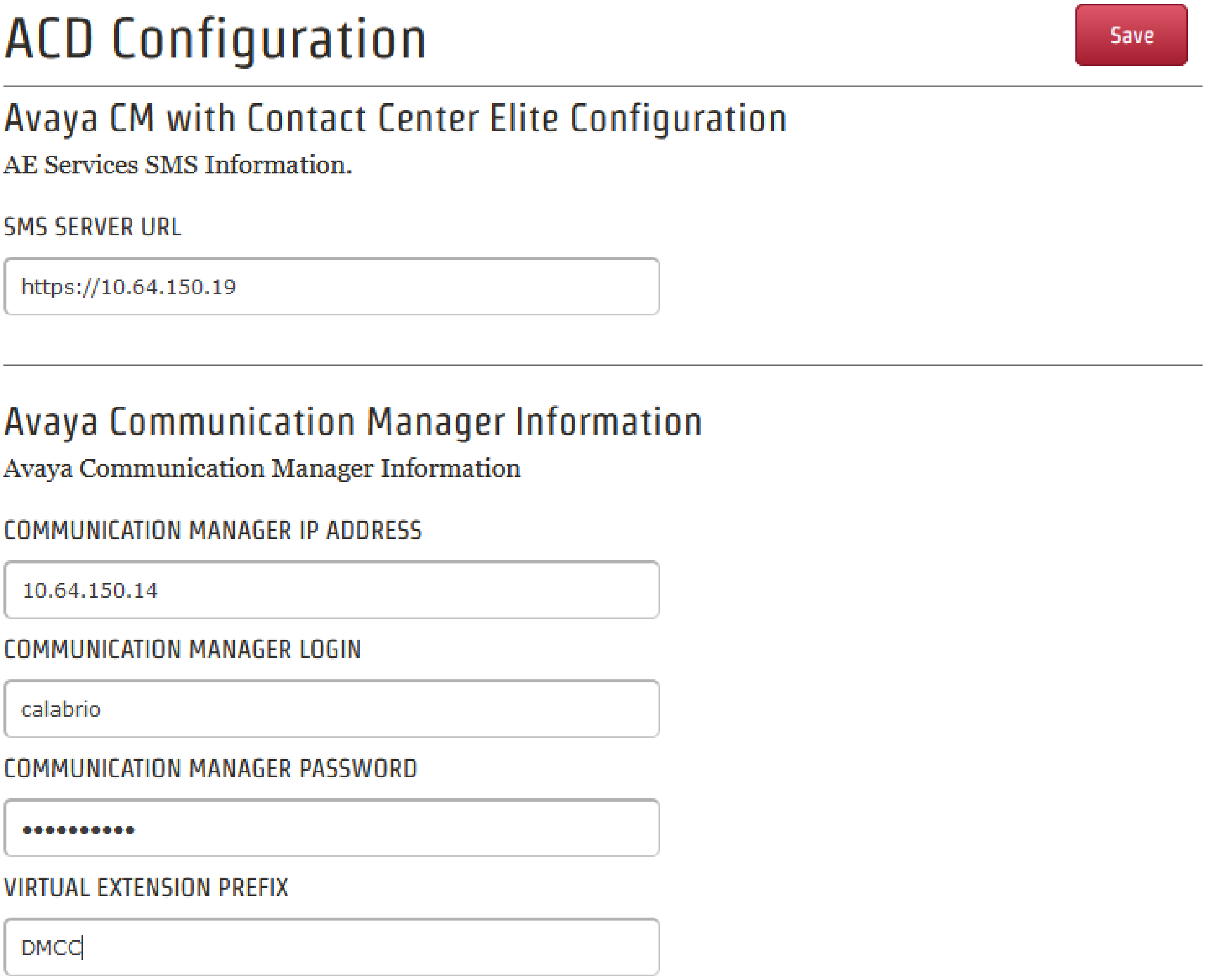
Select ACD: l with Contact Center Elite

Name: CM7AES7

Configure the ACD as shown below:

- **SMS SERVER URL:** Type in the SMS Server URL for the AES.
- **COMMUNICATION MANAGER IP ADDRESS:** Communication Manager IP Address
- **COMMUNICATION MANAGER LOGIN & PASSWORD:** As configured in **Section 5.5**
- **VIRTUAL EXTENSION PREFIX:** Type in **DMCC**

Add the other configuration as instructed by a Calabrio. Select **Save** once done.



ACD Configuration

Avaya CM with Contact Center Elite Configuration

AE Services SMS Information.

SMS SERVER URL: https://10.64.150.19

Avaya Communication Manager Information

Avaya Communication Manager Information

COMMUNICATION MANAGER IP ADDRESS: 10.64.150.14

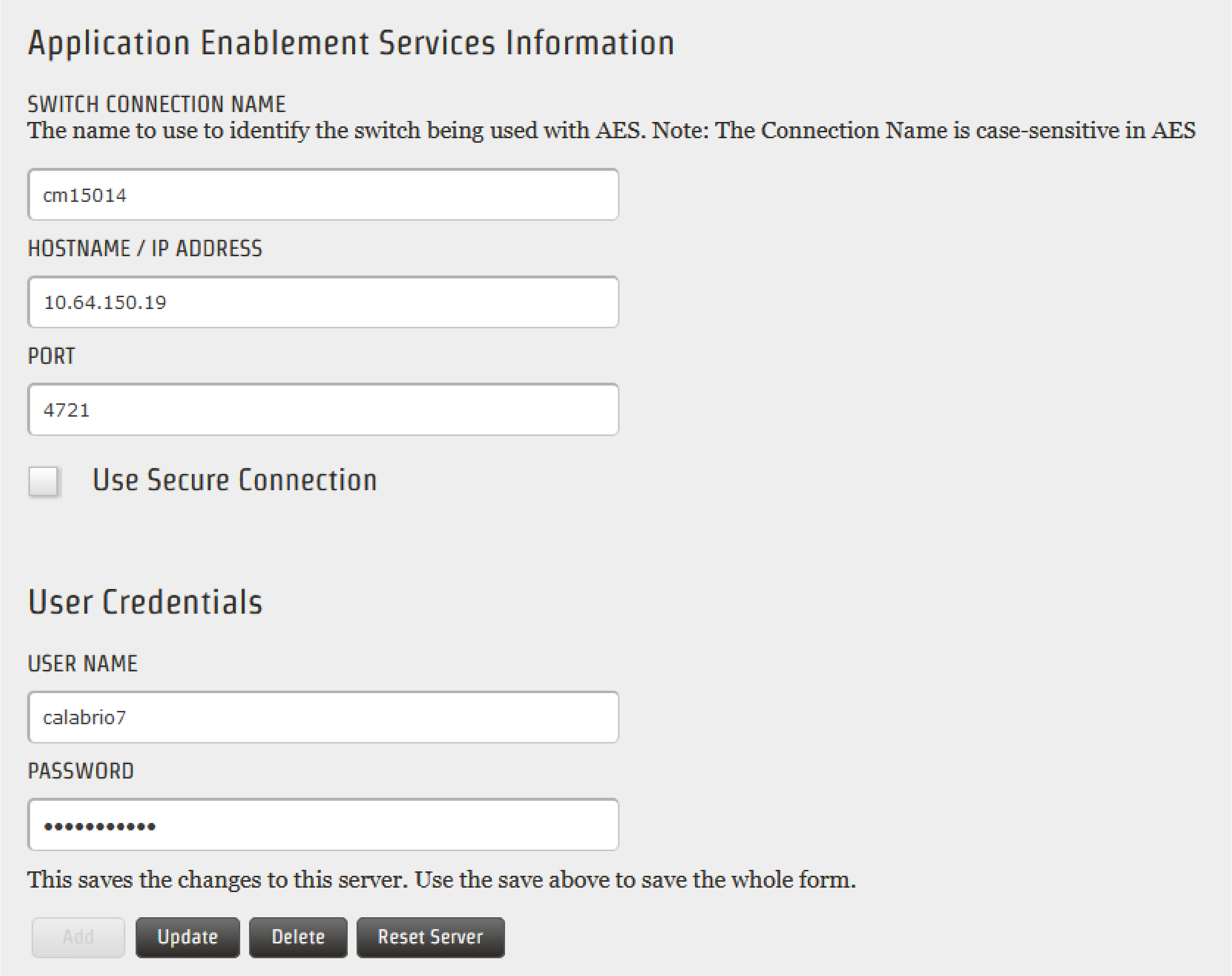
COMMUNICATION MANAGER LOGIN: calabrio

COMMUNICATION MANAGER PASSWORD: ••••••••••

VIRTUAL EXTENSION PREFIX: DMCC

In the **Application Enablement Services Information** section:

- Type in the hostname of Communication Manager in **SWITCH CONNECTION NAME**
- FOR **HOSTNAME / IP ADDRESS,** type in the IP Address of AES
- Configure the default DMCC Port in the **PORT** field, 4721



Application Enablement Services Information

SWITCH CONNECTION NAME
The name to use to identify the switch being used with AES. Note: The Connection Name is case-sensitive in AES

cm15014

HOSTNAME / IP ADDRESS

10.64.150.19

PORT

4721

□ Use Secure Connection

User Credentials

USER NAME

calabrio7

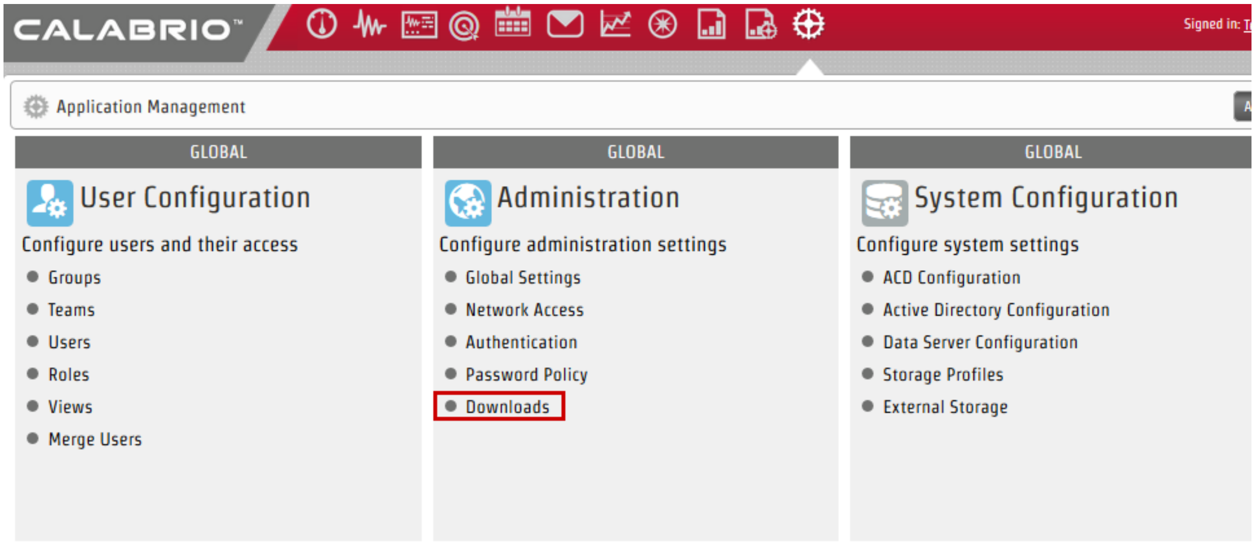
PASSWORD

••••••••••••

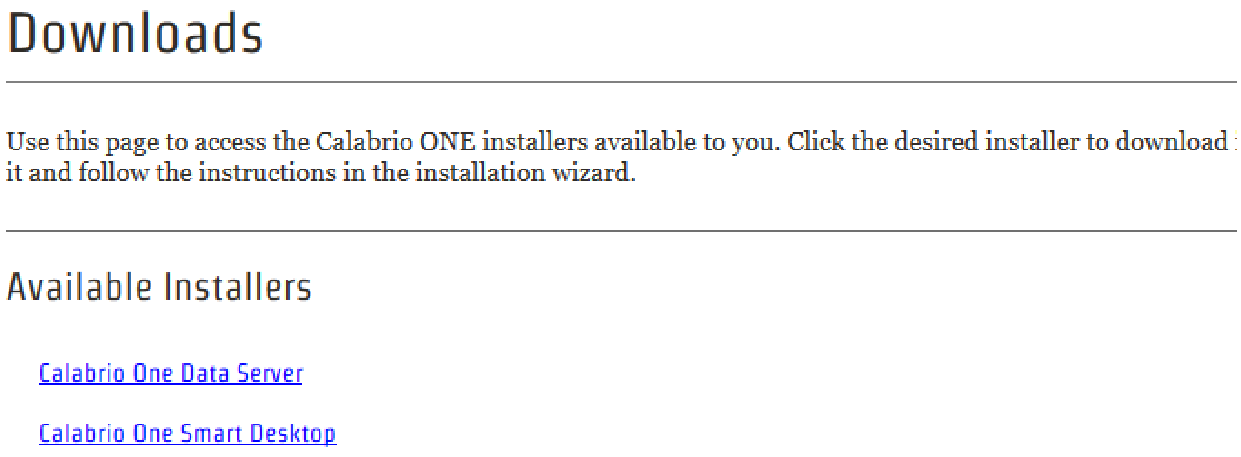
This saves the changes to this server. Use the save above to save the whole form.

7.2. Installation of the Data Server

From the **Application Management** page, select **Downloads.**



From the **Downloads** page, select **Calabrio One Data Server** to download the Data Server. Install the Data Server on the Calabrio One server.



Downloads

Use this page to access the Calabrio ONE installers available to you. Click the desired installer to download it and follow the instructions in the installation wizard.

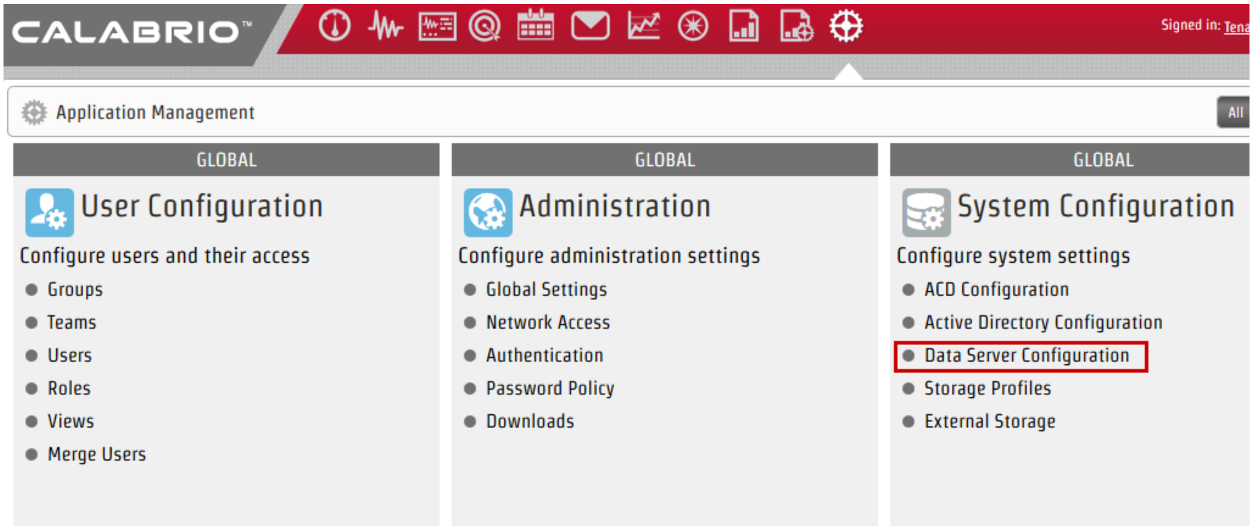
Available Installers

Calabrio One Data Server

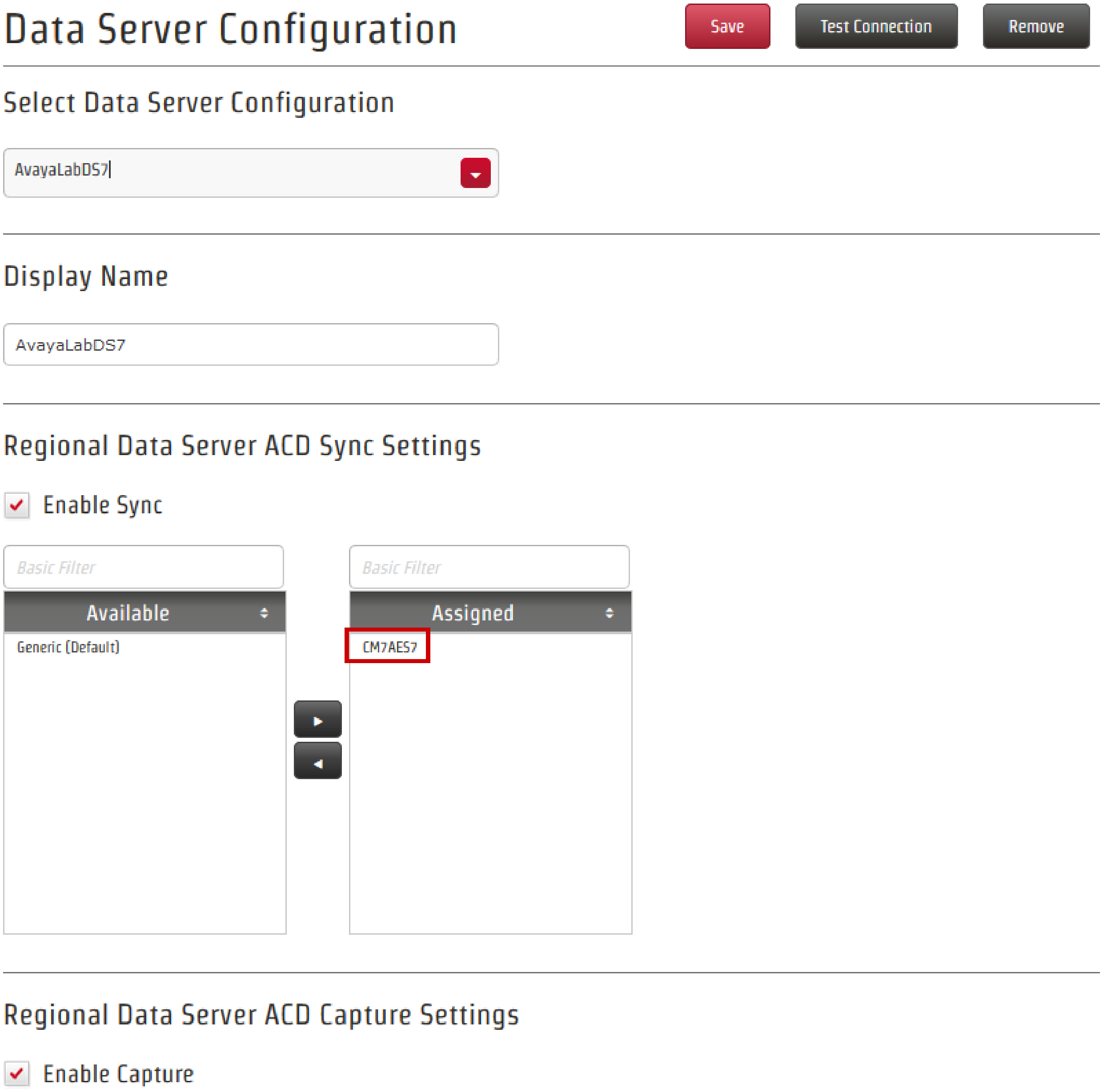
Calabrio One Smart Desktop

7.3. Configuration of the Data Server

Navigate to **Application Management → Data Server Configuration.**



On the **Data Server Configuration** page, select the name of the Data Server to be configured**.** Check box for **Enable Sync** and **Enable Capture** (not shown) and choose the ACD configured in previous step to retrieve the data from.



Data Server Configuration

Select Data Server Configuration

AvayaLabDS7

Display Name

AvayaLabDS7

Regional Data Server ACD Sync Settings

☑ Enable Sync

Assigned: CM7AES7

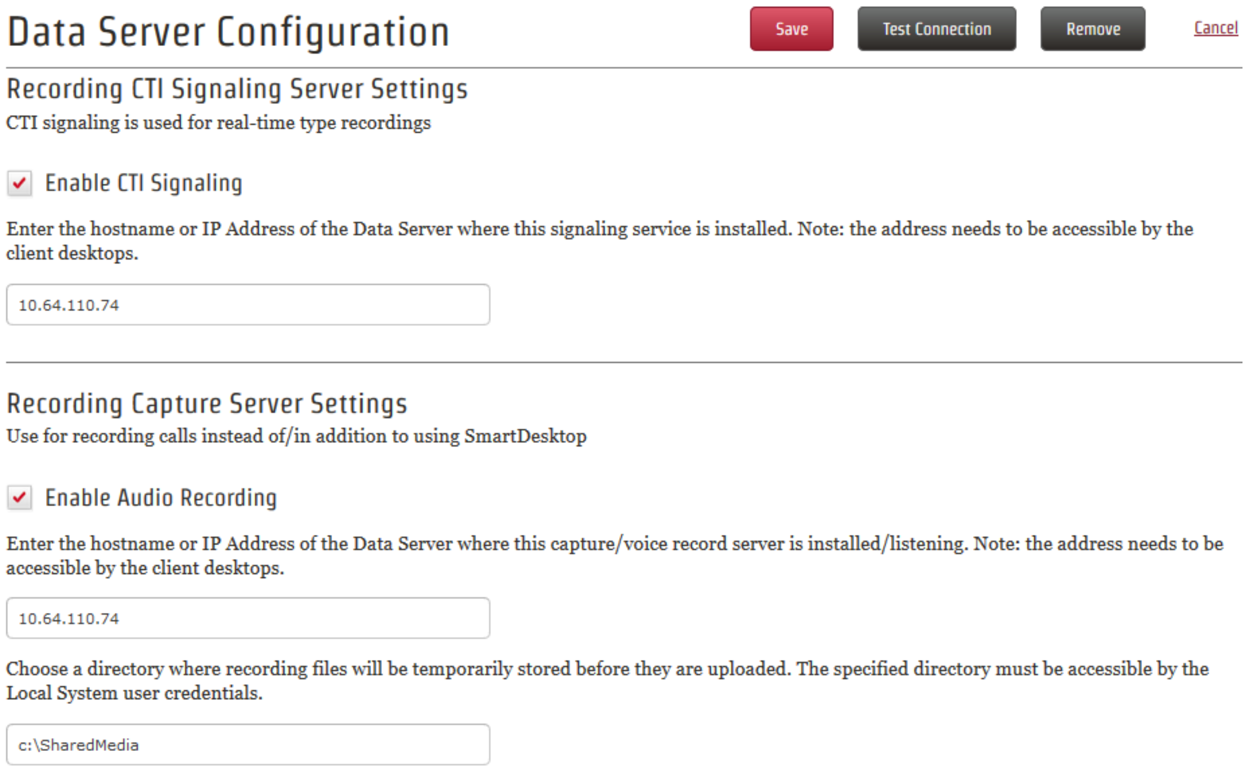
Regional Data Server ACD Capture Settings

☑ Enable Capture

Continuing from above, check box for **Enable CTI Signaling** and type in the IP Address of Data Server being configured. Check box for **Enable Audio Recording**. Enter the IP Address of the Recording server and the path to where recordings should be sent to for processing.

Note: The Data Server can be installed on multiple machines and the functions split between them to increase performance. For this testing, the Data Server was installed on the same server running Calabrio One.

Select **Test Connection** to test this configuration, followed by **Save.**



Data Server Configuration

Recording CTI Signaling Server Settings

CTI signaling is used for real-time type recordings

☑ Enable CTI Signaling

Enter the hostname or IP Address of the Data Server where this signaling service is installed. Note: the address needs to be accessible by the client desktops.

10.64.110.74

Recording Capture Server Settings

Use for recording calls instead of/in addition to using SmartDesktop

☑ Enable Audio Recording

Enter the hostname or IP Address of the Data Server where this capture/voice record server is installed/listening. Note: the address needs to be accessible by the client desktops.

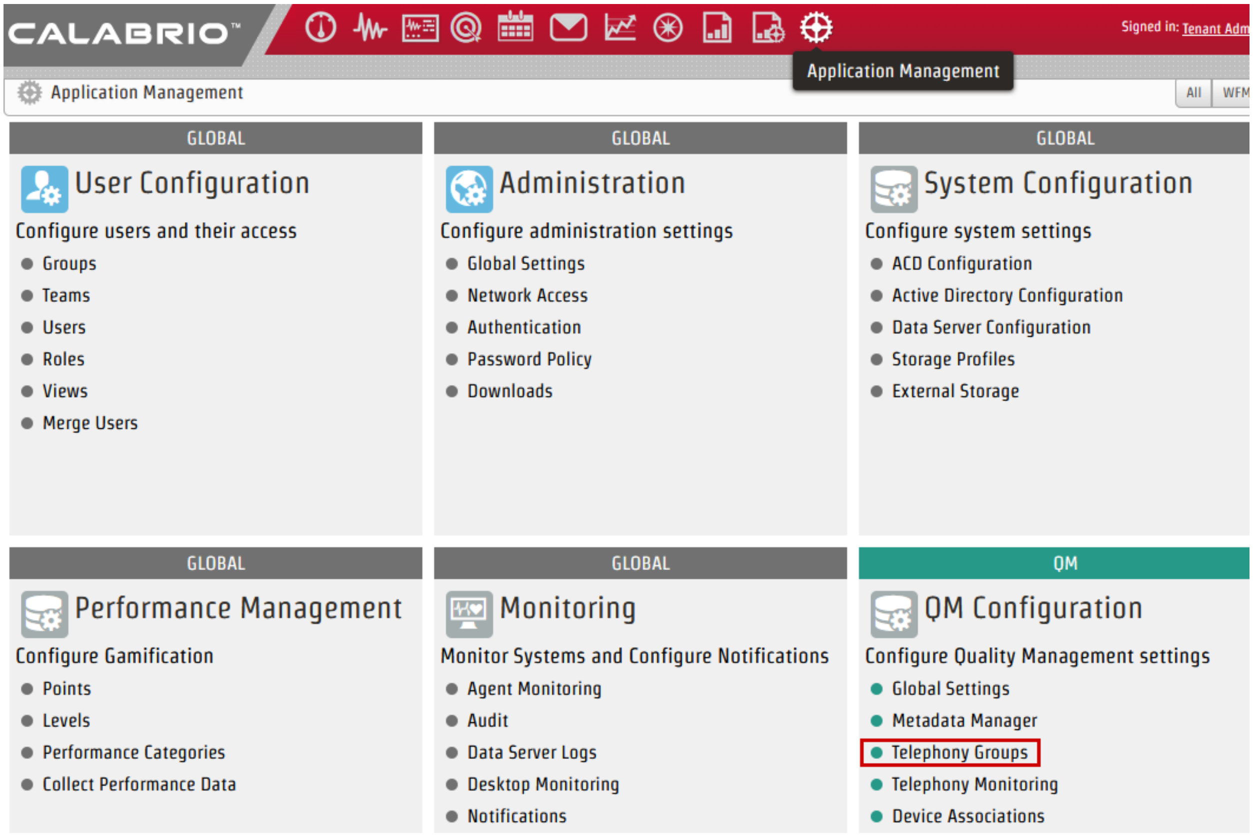
10.64.110.74

Choose a directory where recording files will be temporarily stored before they are uploaded. The specified directory must be accessible by the Local System user credentials.

c:\SharedMedia

7.4. Configuration of the Application Enablement Interfaces – DMCC

From the **Application Management** page, select **Telephony Groups.**

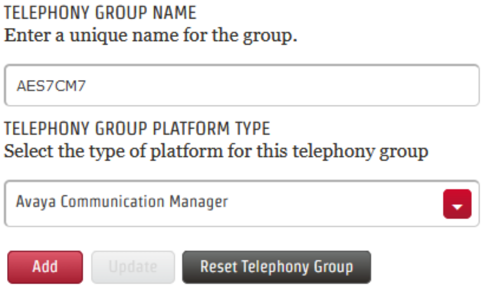


Signed in: Tenant Adm

Application Management

GLOBAL	GLOBAL	GLOBAL
User Configuration Configure users and their access ● Groups ● Teams ● Users ● Roles ● Views ● Merge Users	**Administration** Configure administration settings ● Global Settings ● Network Access ● Authentication ● Password Policy ● Downloads	**System Configuration** Configure system settings ● ACD Configuration ● Active Directory Configuration ● Data Server Configuration ● Storage Profiles ● External Storage
GLOBAL	GLOBAL	QM
Performance Management Configure Gamification ● Points ● Levels ● Performance Categories ● Collect Performance Data	**Monitoring** Monitor Systems and Configure Notifications ● Agent Monitoring ● Audit ● Data Server Logs ● Desktop Monitoring ● Notifications	**QM Configuration** Configure Quality Management settings ● Global Settings ● Metadata Manager ● Telephony Groups ● Telephony Monitoring ● Device Associations

On the **Telephone Groups** page, Type in a **TELEPHONY GROUP NAME** and select **Avaya Communication Manager** from the **TELEPHONY GROUP PLATFORM TYPE** drop down menu. Select **Add.**



TELEPHONY GROUP NAME
Enter a unique name for the group.

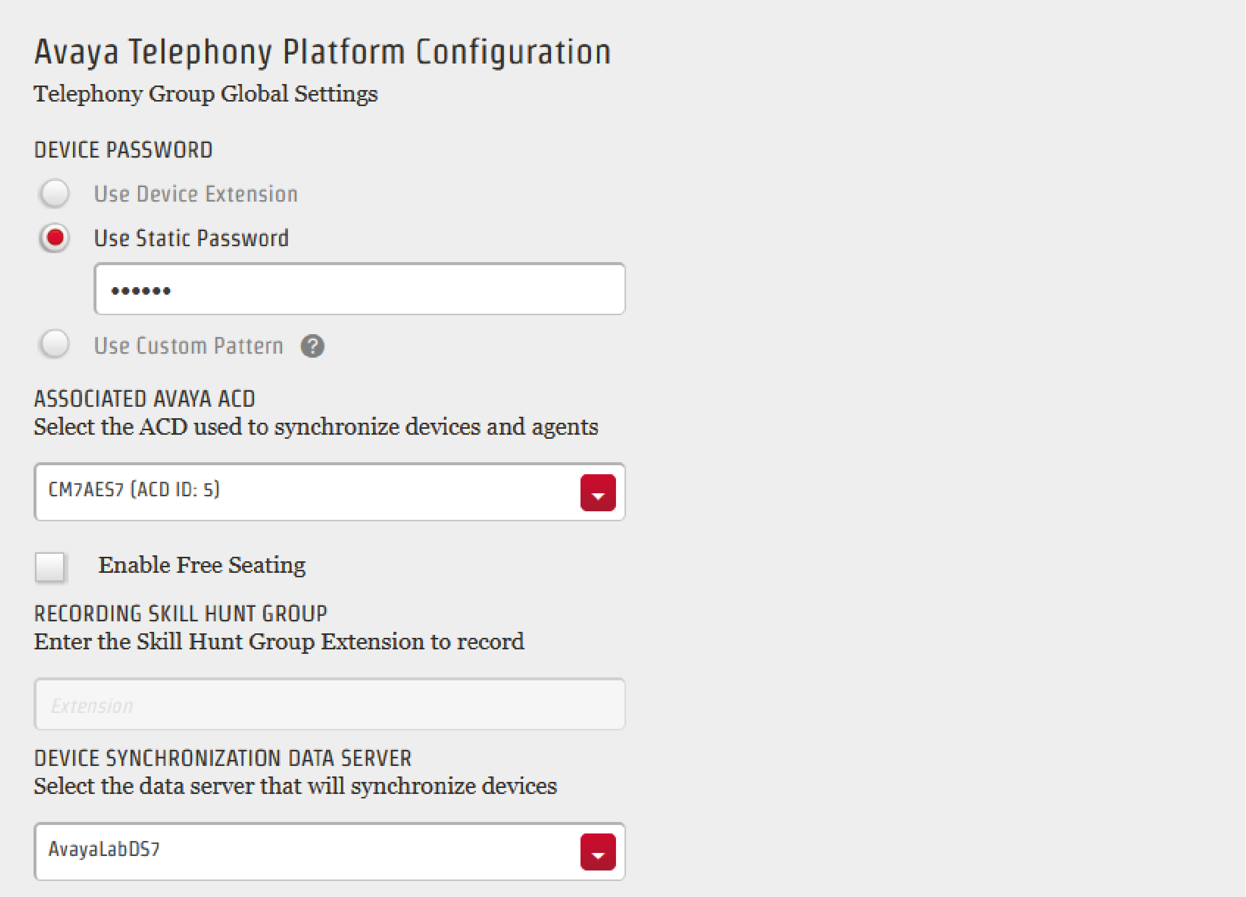
AES7CM7

TELEPHONY GROUP PLATFORM TYPE
Select the type of platform for this telephony group

Avaya Communication Manager

In the **Avaya Telephony Platform Configuration** section:

- Select **Use Static Password** radio button and type in the password from **Section 5.6.**
- Select the **ASSOCIATED AVAYA ACD** as configured in previous section.
- Select a **DEVICE SYNCHRONZATION DATA SERVER.** This Data Server was pre-configured.



Avaya Telephony Platform Configuration

Telephony Group Global Settings

DEVICE PASSWORD

○ Use Device Extension

● Use Static Password

••••••

○ Use Custom Pattern

ASSOCIATED AVAYA ACD

Select the ACD used to synchronize devices and agents

CM7AES7 (ACD ID: 5)

□ Enable Free Seating

RECORDING SKILL HUNT GROUP

Enter the Skill Hunt Group Extension to record

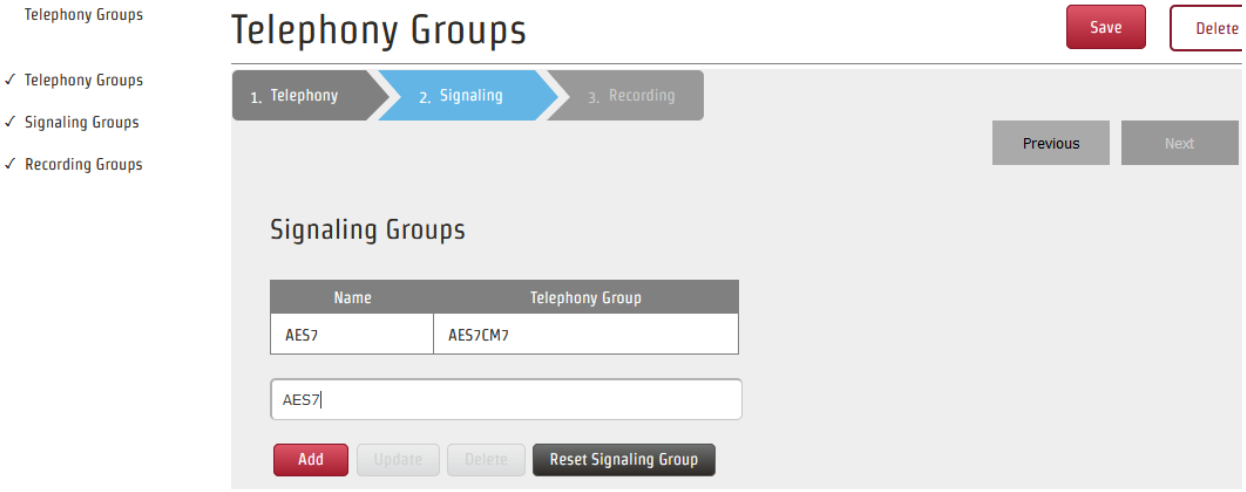
Extension

DEVICE SYNCHRONIZATION DATA SERVER

Select the data server that will synchronize devices

AvayaLabDS7

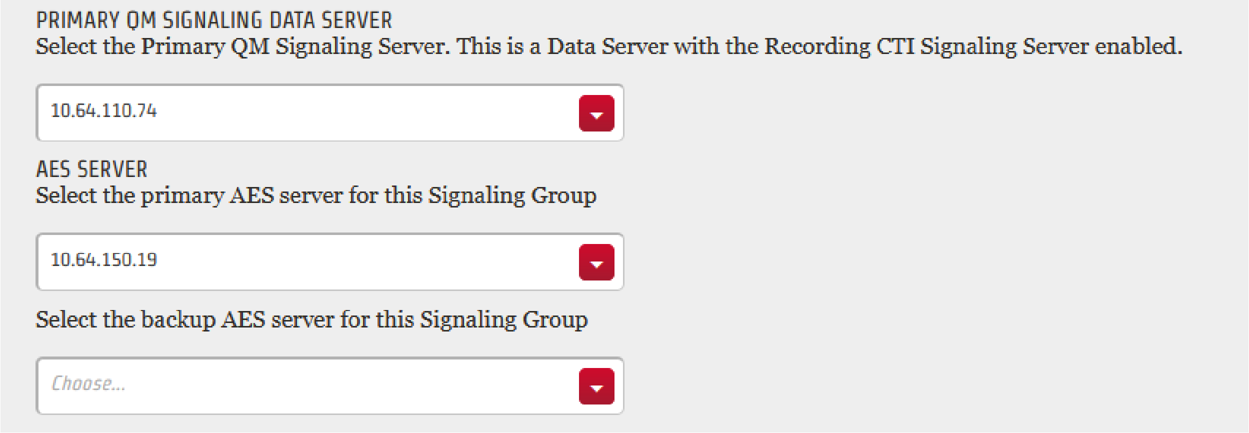
Select the **Signaling** tab, type in a name for a **Signaling Group** and select **Add.**



Name	Telephony Group
AES7	AES7CM7

AES7

- **PRIMARY QM SIGNALING DATA SERVER:** Type in the IP Address of Calabrio One server
- **AES SERVER:** Type in the IP Address of AES



PRIMARY QM SIGNALING DATA SERVER
Select the Primary QM Signaling Server. This is a Data Server with the Recording CTI Signaling Server enabled.

10.64.110.74

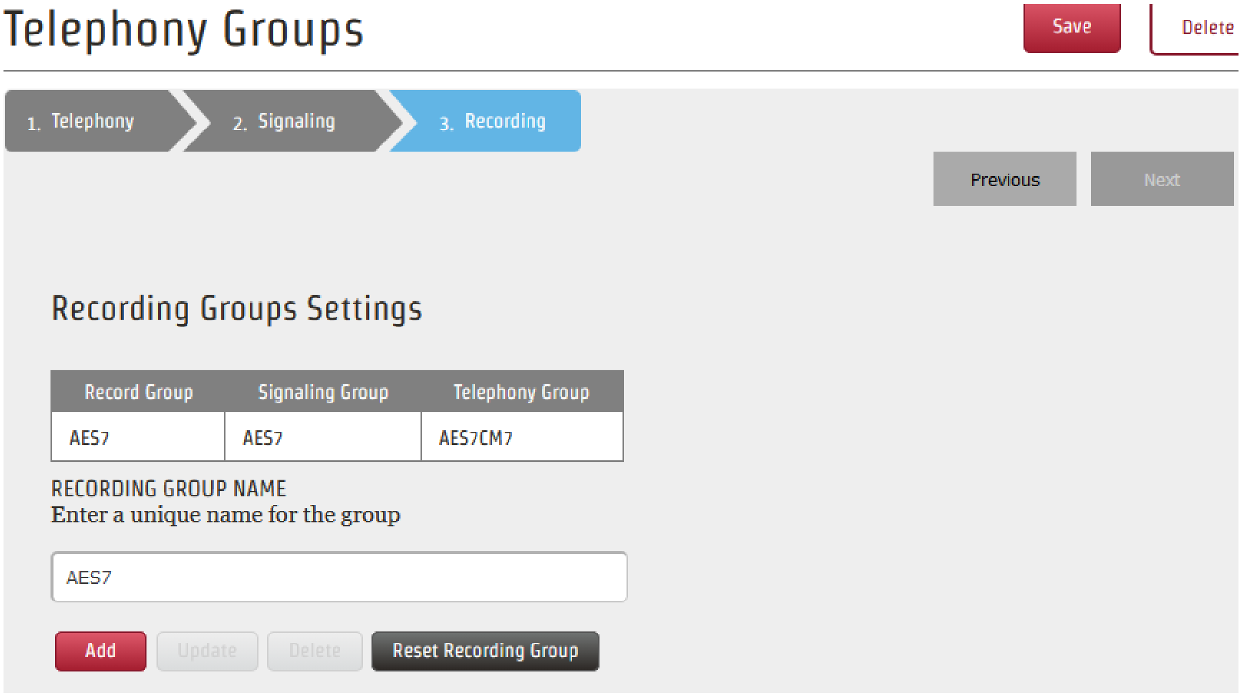
AES SERVER
Select the primary AES server for this Signaling Group

10.64.150.19

Select the backup AES server for this Signaling Group

Choose...

Select the **Recording** tab, type in a name for a **Recording Group** and select **Add.**



Telephony Groups

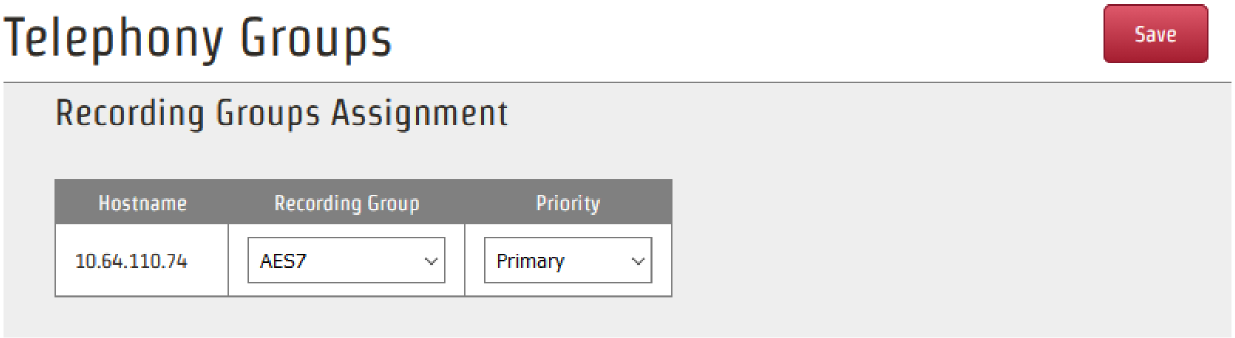
Recording Groups Settings

Record Group	Signaling Group	Telephony Group
AES7	AES7	AES7CM7

RECORDING GROUP NAME
Enter a unique name for the group

AES7

Select the **Recording Group** from that is being configured and set **Priority** to **Primary.** Select **Save** once done.



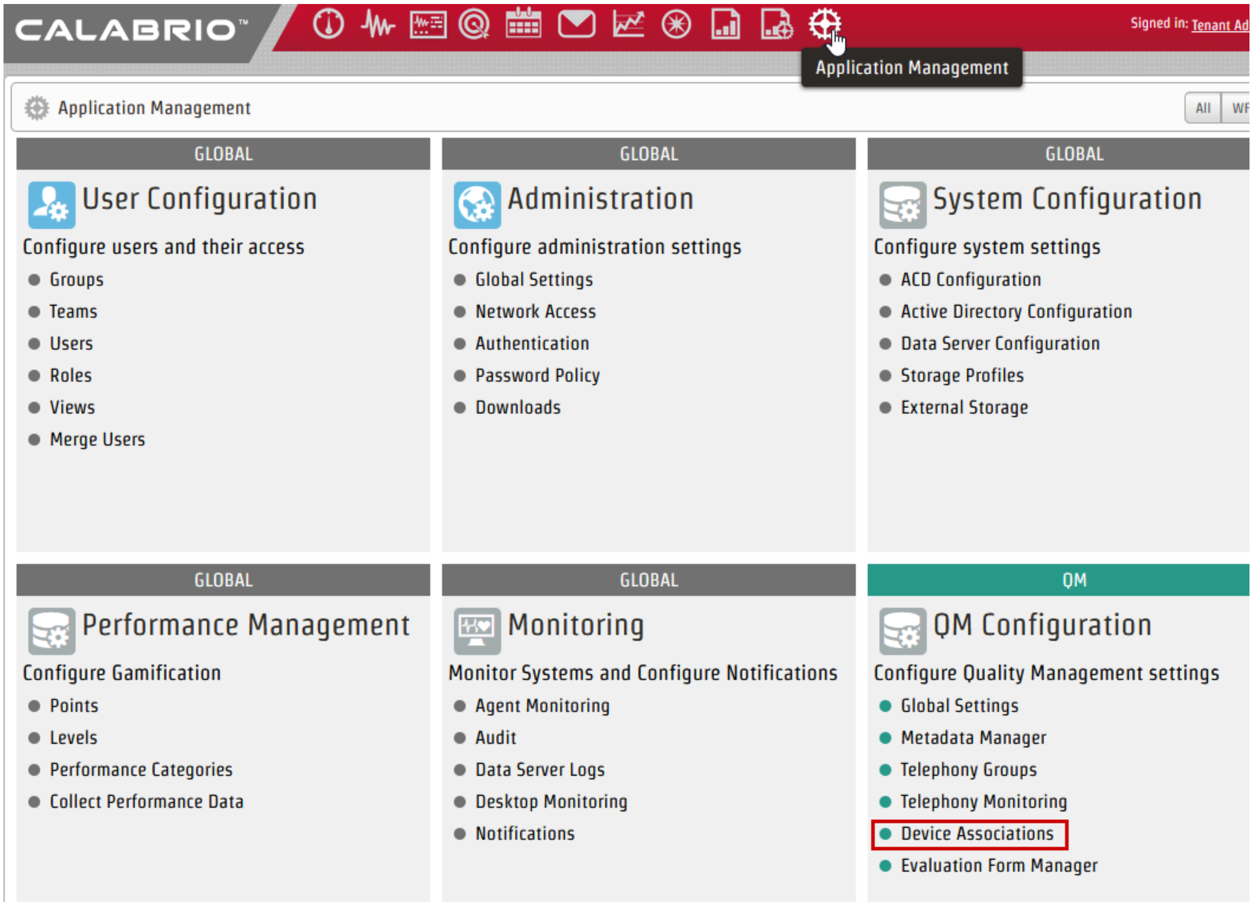
Telephony Groups

Recording Groups Assignment

Hostname	Recording Group	Priority
10.64.110.74	AES7	Primary

7.5. Configuration of Device Associations

Navigate to **Application Management → Device Assosications.**



CALABRIO™

Signed in: Tenant Ad

Application Management

Application Management

All WF

GLOBAL

User Configuration

Configure users and their access

- Groups
- Teams
- Users
- Roles
- Views
- Merge Users

GLOBAL

Administration

Configure administration settings

- Global Settings
- Network Access
- Authentication
- Password Policy
- Downloads

GLOBAL

System Configuration

Configure system settings

- ACD Configuration
- Active Directory Configuration
- Data Server Configuration
- Storage Profiles
- External Storage

GLOBAL

Performance Management

Configure Gamification

- Points
- Levels
- Performance Categories
- Collect Performance Data

GLOBAL

Monitoring

Monitor Systems and Configure Notifications

- Agent Monitoring
- Audit
- Data Server Logs
- Desktop Monitoring
- Notifications

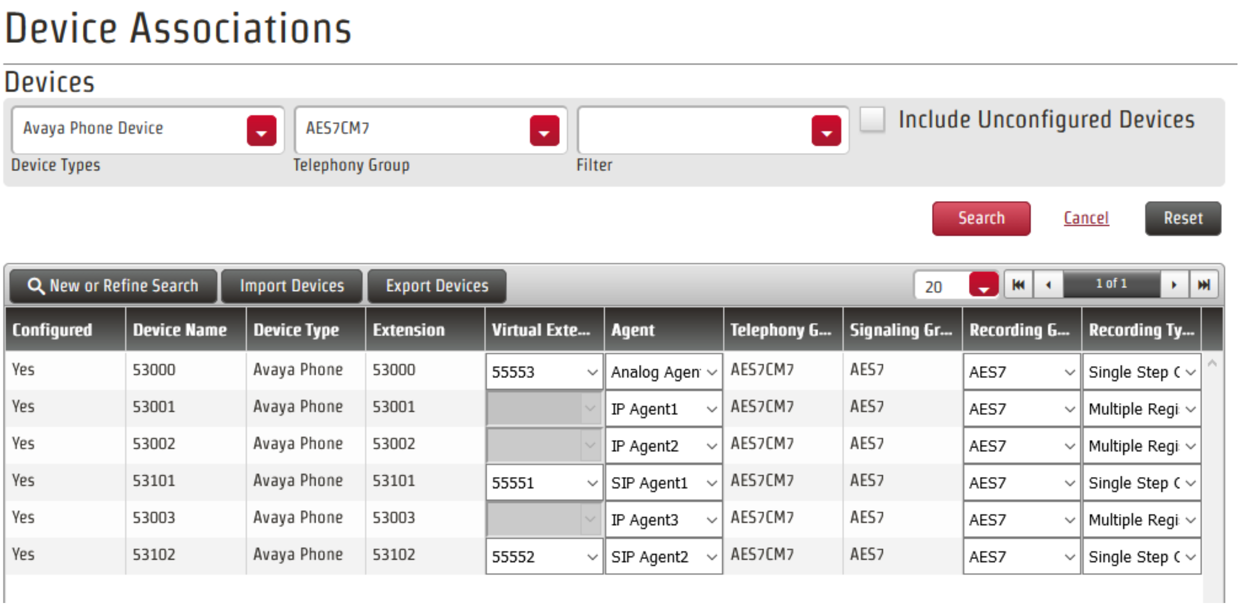
QM

QM Configuration

Configure Quality Management settings

- Global Settings
- Metadata Manager
- Telephony Groups
- Telephony Monitoring
- Device Associations
- Evaluation Form Manager

Configure the device association as needed. During the compliance test, the following extensions were configured to be recorded.



Device Associations

Devices

Device Types: Avaya Phone Device

Telephony Group: AES7CM7

Filter:

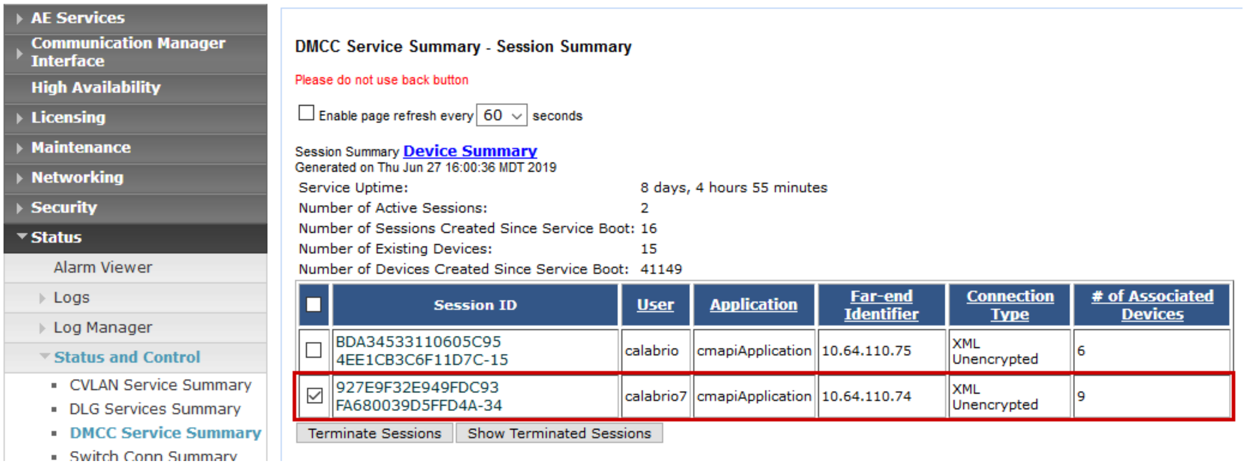
□ Include Unconfigured Devices

Configured	Device Name	Device Type	Extension	Virtual Exte...	Agent	Telephony G...	Signaling Gr...	Recording G...	Recording Ty...
Yes	53000	Avaya Phone	53000	55553	Analog Agen	AES7CM7	AES7	AES7	Single Step (
Yes	53001	Avaya Phone	53001		IP Agent1	AES7CM7	AES7	AES7	Multiple Regi
Yes	53002	Avaya Phone	53002		IP Agent2	AES7CM7	AES7	AES7	Multiple Regi
Yes	53101	Avaya Phone	53101	55551	SIP Agent1	AES7CM7	AES7	AES7	Single Step (
Yes	53003	Avaya Phone	53003		IP Agent3	AES7CM7	AES7	AES7	Multiple Regi
Yes	53102	Avaya Phone	53102	55552	SIP Agent2	AES7CM7	AES7	AES7	Single Step (

8. Verification Steps

8.1. Verify AES

From the AES OAM page, navigate to **Status → Status and Control → DMCC Service Summary.** Verify the user configured in **Section 6.2** is successfully connected to AES.



DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

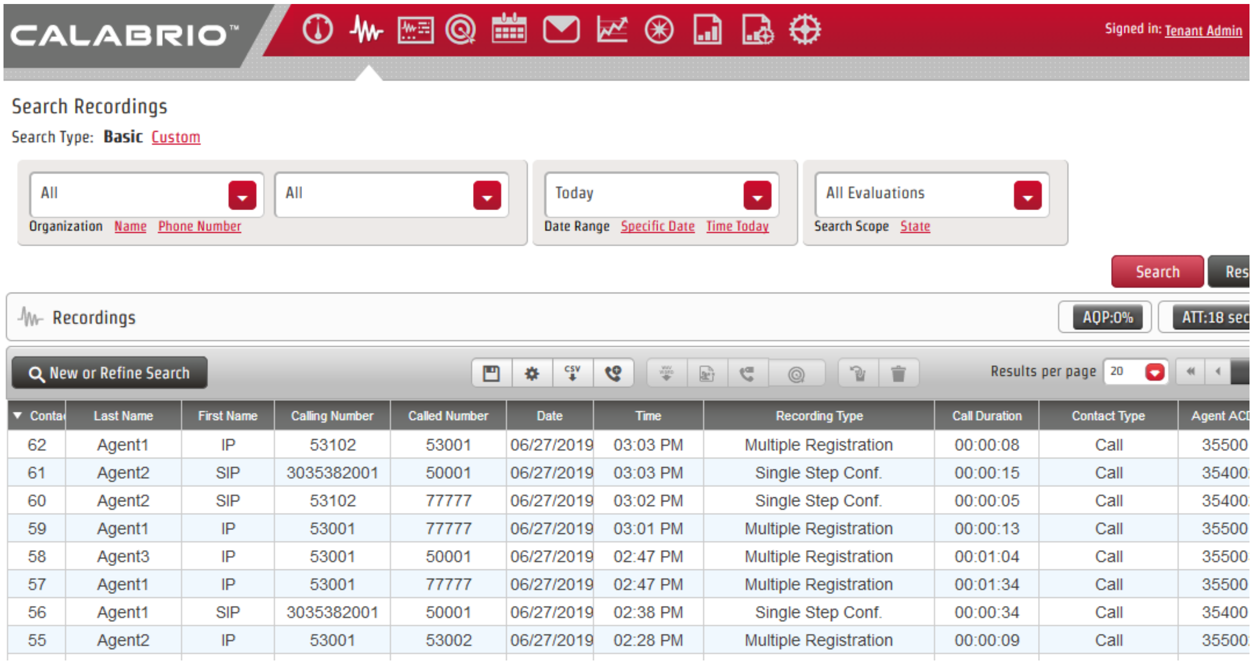
Session Summary Device Summary
Generated on Thu Jun 27 16:00:36 MDT 2019

Service Uptime:	8 days, 4 hours 55 minutes
Number of Active Sessions:	2
Number of Sessions Created Since Service Boot:	16
Number of Existing Devices:	15
Number of Devices Created Since Service Boot:	41149

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	BDA34533110605C95 4EE1CB3C6F11D7C-15	calabrio	cmapiApplication	10.64.110.75	XML Unencrypted	6
☑	927E9F32E949FDC93 FA680039D5FFD4A-34	calabrio7	cmapiApplication	10.64.110.74	XML Unencrypted	9

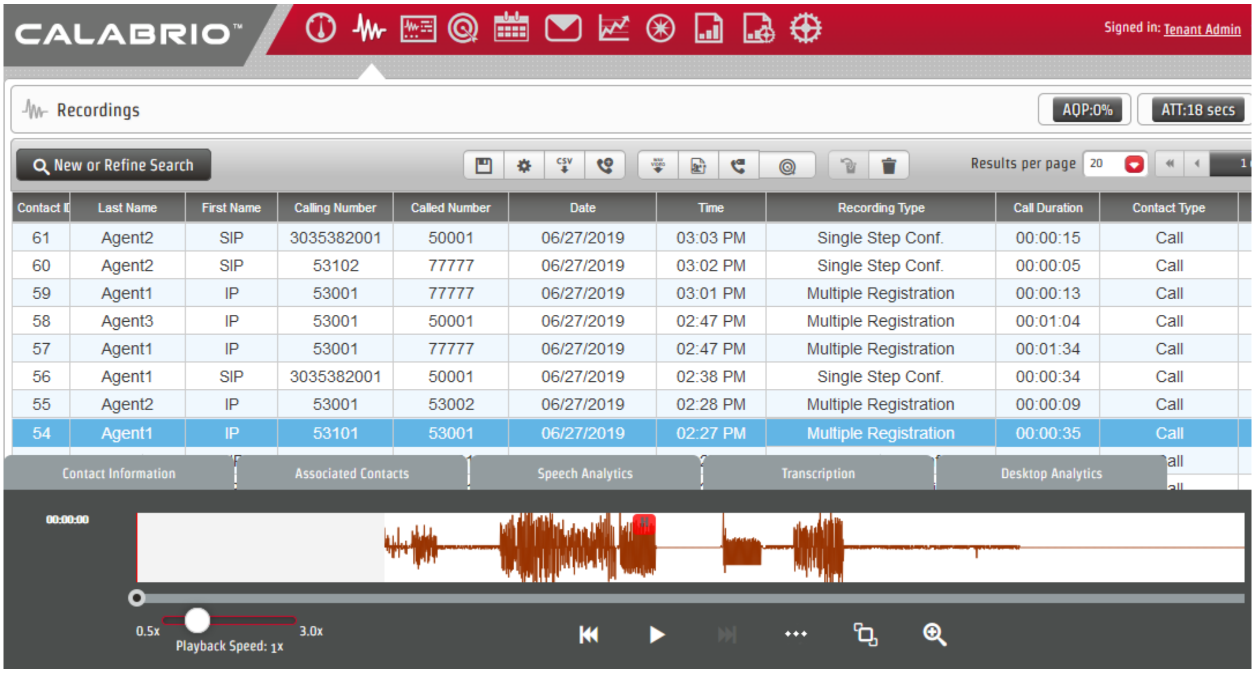
8.2. Verify Calabrio One

Place a few calls between recorded extensions. Verify the recordings are available on the Calabrio One web interface.



Conta	Last Name	First Name	Calling Number	Called Number	Date	Time	Recording Type	Call Duration	Contact Type	Agent ACD
62	Agent1	IP	53102	53001	06/27/2019	03:03 PM	Multiple Registration	00:00:08	Call	35500
61	Agent2	SIP	3035382001	50001	06/27/2019	03:03 PM	Single Step Conf.	00:00:15	Call	35400
60	Agent2	SIP	53102	77777	06/27/2019	03:02 PM	Single Step Conf.	00:00:05	Call	35400
59	Agent1	IP	53001	77777	06/27/2019	03:01 PM	Multiple Registration	00:00:13	Call	35500
58	Agent3	IP	53001	50001	06/27/2019	02:47 PM	Multiple Registration	00:01:04	Call	35500
57	Agent1	IP	53001	77777	06/27/2019	02:47 PM	Multiple Registration	00:01:34	Call	35500
56	Agent1	SIP	3035382001	50001	06/27/2019	02:38 PM	Single Step Conf.	00:00:34	Call	35400
55	Agent2	IP	53001	53002	06/27/2019	02:28 PM	Multiple Registration	00:00:09	Call	35500

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



Contact I	Last Name	First Name	Calling Number	Called Number	Date	Time	Recording Type	Call Duration	Contact Type
61	Agent2	SIP	3035382001	50001	06/27/2019	03:03 PM	Single Step Conf.	00:00:15	Call
60	Agent2	SIP	53102	77777	06/27/2019	03:02 PM	Single Step Conf.	00:00:05	Call
59	Agent1	IP	53001	77777	06/27/2019	03:01 PM	Multiple Registration	00:00:13	Call
58	Agent3	IP	53001	50001	06/27/2019	02:47 PM	Multiple Registration	00:01:04	Call
57	Agent1	IP	53001	77777	06/27/2019	02:47 PM	Multiple Registration	00:01:34	Call
56	Agent1	SIP	3035382001	50001	06/27/2019	02:38 PM	Single Step Conf.	00:00:34	Call
55	Agent2	IP	53001	53002	06/27/2019	02:28 PM	Multiple Registration	00:00:09	Call
54	Agent1	IP	53101	53001	06/27/2019	02:27 PM	Multiple Registration	00:00:35	Call

9. Conclusion

These Application Notes describe the procedures for configuring Calabrio One to monitor and record calls placed to and from agents and phones on Avaya Aura® Communication Manager. In the configuration described in these Application Notes, Calabrio uses the Device and Media Control Services and System Management Service of Avaya Aura® Application Enablement Services to perform recording. All feature and serviceability test cases were completed and passed with the observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.
2. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.1.

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

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.