



DevConnect Program

Application Notes for Calabrio Quality Management R11 with Avaya Aura® Communication Manager R10.1.3 and Avaya Aura® Application Enablement Services R10.1.3 – Issue 1.0

Abstract

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

Calabrio Quality Management uses 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 Avaya DevConnect Program.

1. Introduction

Calabrio Quality Management (Calabrio) is a contact center and knowledge worker-oriented recording solution that uses 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 the 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.).

The serviceability testing focused on verifying that Calabrio recording server came back into service after re-connecting the Ethernet cable and rebooting the system.

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 these Application Notes, the interface between Avaya systems and Calabrio did not include use of any specific encryption features as requested by Calabrio.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing.

- Inbound and Outbound Calls – Successfully record inbound and outbound calls routed to and from different endpoints such as analog, digital, H.323 and SIP stations.
- Calls to Elite Agents – Successfully record calls to agents logged in to Avaya Agent for Desktop.
- Telephony features – Successfully record hold/resume, mute/unmute, transfer and conference calls.
- Screen recording – Successfully record user's desktops associated with recorded stations.
- Serviceability testing to cover the behavior of Calabrio recording server under different simulated failure conditions.

2.2. Test Results

All test cases successfully passed.

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 consists of 96x1, J100 series and Avaya Agent for Desktop softphones acting like agents.
- Avaya Session Border Controller have SIP trunks that connects to Session Manager and to SIP service provider to provide PSTN calls.
- Calabrio server installed on a standalone machine.

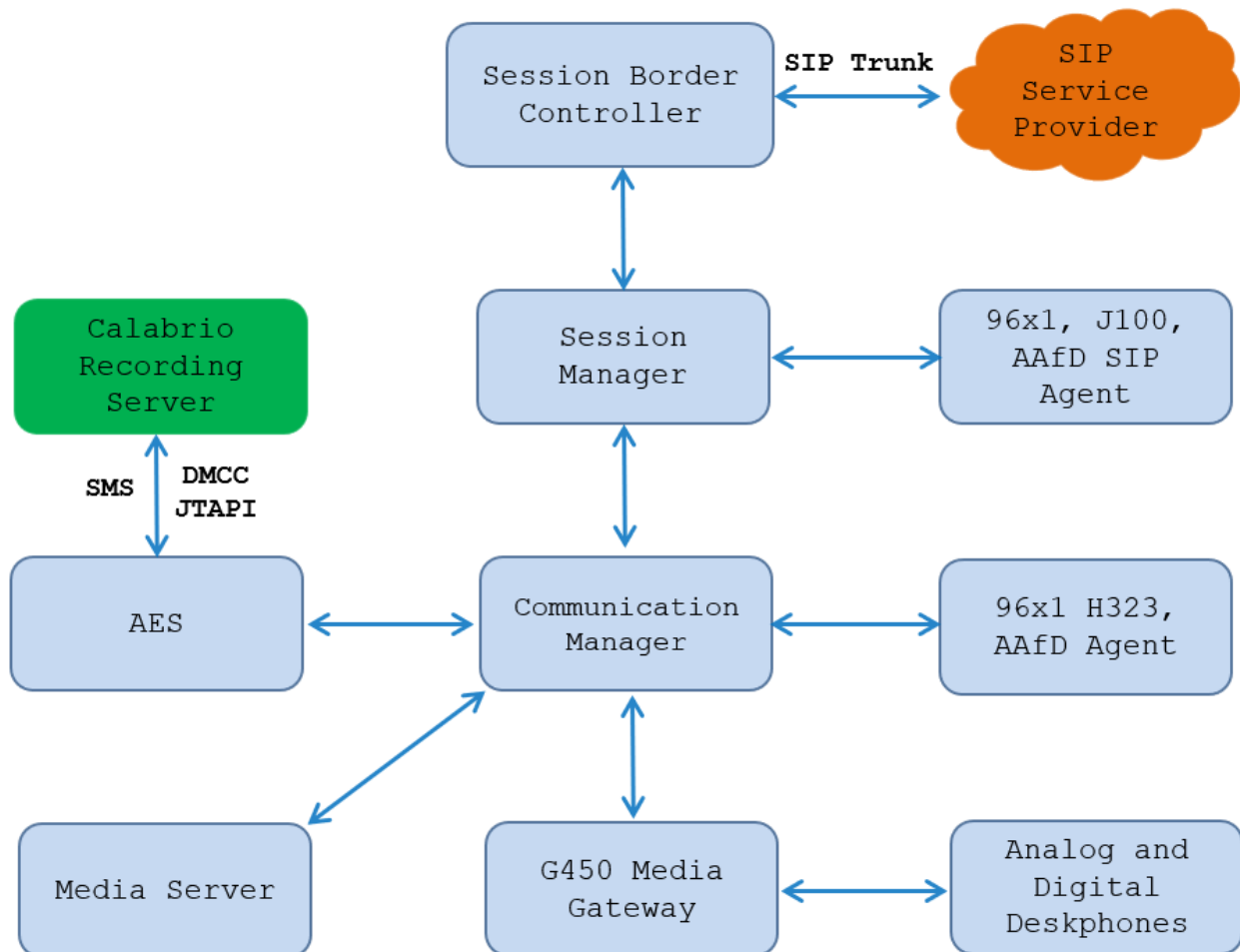


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1.3.1.0-FP3 SP1 01.0.974.0-27937
Avaya G450 Media Gateway	FW 42.24.0
Avaya Aura® Media Server	v.10.1.0.154
Avaya Aura® System Manager	10.1.3.1 Feature Pack 3 SP1 10.1.3.1.0716418
Avaya Aura® Session Manager	10.1.3.1 Feature Pack 3 SP1 10.1.3.1.1013103
Avaya Session Border Controller	10.1.2.0-64-23285
Avaya Aura® Application Enablement Services	10.1.3.0
Avaya J100 Series Deskphones	4.1.2.0.11 (SIP) 6.8.5.4.10 (H.323)
Avaya 96x1 Deskphones	7.1.15 (SIP) 6.8.5.4.10 (H.323)
Avaya Agent for Desktop Softphone	2.0.65
Avaya 9408 Digital Deskphone	2.0
Avaya Analog Deskphone	-
Calabrio One Cloud Platform	11.0.2.X
Calabrio One Data Server running on Windows 2016 Server VM	11.0.2.X

5. Configure Avaya Aura® Communication Manager

This section provides the steps for configuring Communication Manager using the System Access Terminal (SAT). The procedure includes the following areas:

- Verify License
- Administer Communication Manager System Features
- Administer IP-Services
- Administer CTI Link
- Administer SMS User Account
- Administer Recorded Extensions
- Administer Virtual Extensions

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 License

Using the SAT, verify that the **Computer Telephony Adjunct Links** option is enabled on the **system-parameters customer-options** form on **Page 4**. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 4**, ensure **Computer Telephony Adjunct Links** is set to **y**.

```
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? n          DCS (Basic)? y
ASAI Link Core Capabilities? y          DCS Call Coverage? y
ASAI Link Plus Capabilities? y          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: cm10
                                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  Notification using Crisis Alert? n
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Send All Calls on Ringing Bridge Leaves Call Ringing on Other Bridges? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
  Copy UCID for Station Conference/Transfer? y
```

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

  Reporting for PC Non-Predictive Calls? n

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

ASAI
  Copy ASAI UI During Conference/Transfer? y
  Call Classification After Answer Supervision? y
                                Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? y
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.3. Administer IP-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**.

change ip-services					Page 1 of 4	
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	TLS Encryption
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 6.1**.
- In the **Enabled** field, type **y**.

change ip-services		AE Services Administration			Page 4 of 4	
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes10	*	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: 3332	
Type: ADJ-IP	
Name: AES10	COR: 1
Unicode Name? n	

5.5. Administer 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. Login 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.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administration/Server (Maintenance) page. The left-hand navigation pane shows the 'Security' section expanded, with 'Administrator Accounts' selected. The main content area, titled 'Administrator Accounts', provides instructions on adding, deleting, or changing administrator logins and Linux groups. Under the 'Select Action:' heading, there are radio buttons for 'Add Login' (selected), 'Privileged Administrator' (selected), 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. Below these are three groups of options: 'Change Login', 'Remove Login', and 'Lock/Unlock Login', each with a 'Select Login' dropdown menu. At the bottom, there are 'Add Group' and 'Remove Group' options, each with a 'Select Group' dropdown menu. 'Submit' and 'Help' buttons are located at the bottom left of the main content area. The top of the page features the Avaya logo and the title 'Avaya Aura® Communication Manager (CM) System Management Interface (SMI)'. A red header bar contains 'Help Log Off' and 'Administration'. The top right corner indicates 'This Server: cm10'.

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

AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration This Server: cm10

Administration / Server (Maintenance)

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):

Enter password:

Re-enter password:

Force password change on next login: ☐ Yes ☒ No

Submit Cancel Help

5.6. Administer 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 3301		Page 1 of 6
STATION		
Extension: 3301	Lock Messages? n	BCC: 0
Type: 9641	Security Code: *	TN: 1
Port: S000011	Coverage Path 1: 1	COR: 1
Name: John, Anderson	Coverage Path 2:	COS: 15
Unicode Name? n	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: lsp		
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. Administer Virtual Extensions

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 3317		Page 1 of 5
STATION		
Extension: 3317	Lock Messages? n	BCC: 0
Type: 9640	Security Code: *	TN: 1
Port: S000019	Coverage Path 1:	COR: 1
Name: DMCC Station 1	Coverage Path 2:	COS: 1
Unicode Name? n	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 (AES) is performed via a web browser. Enter the ip address of AES in the URL field of a web browser. 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

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Jan 3 22:41:35 E.S.T. 2024 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes10/10.33.1.47
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Sat Jan 06 03:00:04 EST 2024
HA Status: Not Configured

Home

Home | Help | Logout

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

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- 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 a link to Communication Manager, navigate to the **Communication Manager Interface** → **Switch Connections** page and enter a name for the new switch connection (e.g., **cm10**) 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**.

Communication Manager Interface | Switch Connections

Home | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Connection Details - cm10

Switch Password

.....

Confirm Switch Password

.....

Msg Period

30

Minutes (1 - 72)

Provide AE Services certificate to switch

☐

Secure H323 Connection

☐

Processor Ethernet

☒

Enable TLS Certificate Validation

☐

Apply

Cancel

The display returns to the **Switch Connections** screen which shows that the **cm10** switch connection has been added.

Communication Manager Interface | Switch Connections

Home | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm10	Yes	30	1

Edit Connection

Edit PE/CLAN IPs

Edit Signaling Details

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.

Communication Manager Interface | Switch Connections

Home | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

Edit Processor Ethernet IP - cm10

10.33.1.43

Add/Edit Name or IP

Name or IP Address	Status
10.33.1.43	In Use

Back

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.

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

calabrio

* Common Name

Calabrio

* Surname

QM

* User Password

.....

* Confirm Password

.....

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

Department Number

Display Name

Employee Number

Employee Type

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**.

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> calabrio	Calabrio	NONE	NONE
<input type="radio"/> test	Avaya	NONE	NONE

Edit

List All

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).

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▪ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

▪ Device Groups

Edit CTI User

User Profile:

User ID

calabrio

Common Name

Calabrio

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

Apply Changes

Cancel Changes

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.


Application Enablement (CTI) - Release: 10 - SID: 10503000 **Standard**

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: April 11, 2023 5:29:59 AM -07:00

License File Host IDs: XXXXXXXXXX

Licensed Features

14 Items  Show **All** ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	512
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	512
AES HA LARGE VALUE_AES_HA_LARGE	permanent	512
AES ADVANCED AGENT VALUE_AES_ADVANCED_AGENT	permanent	512
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	512
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	512
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	512
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	512

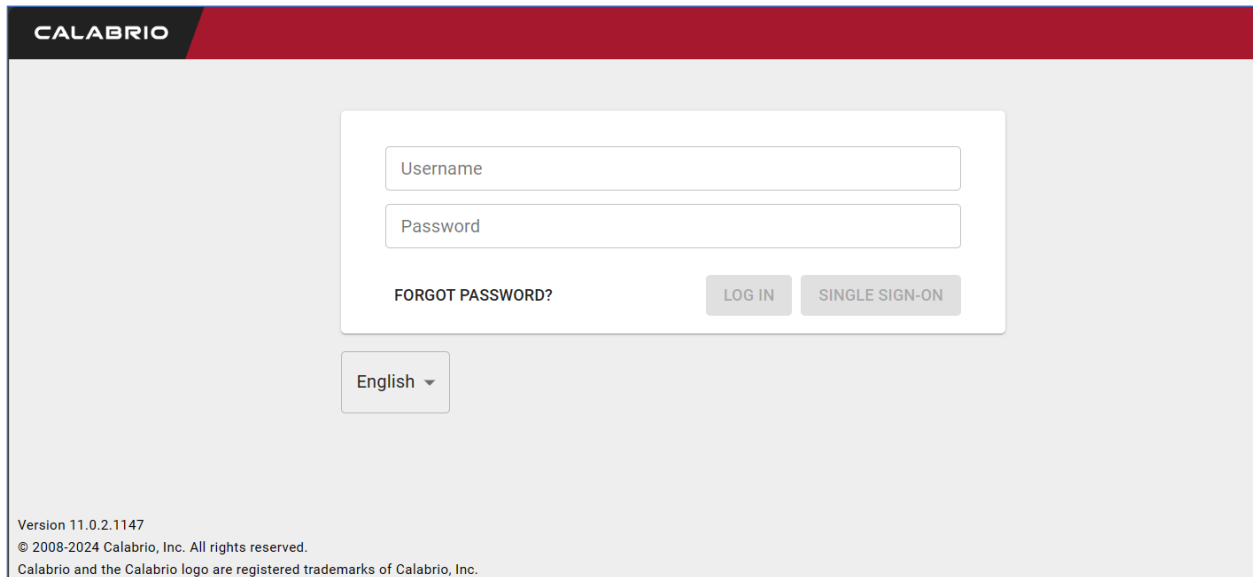
7. Configure Calabrio Quality Management

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 and assumes that the Calabrio platform is installed and operable.

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 web interface. Access the web interface via a browser by entering the URL where Calabrio One tenant is located. Log in using appropriate credentials.



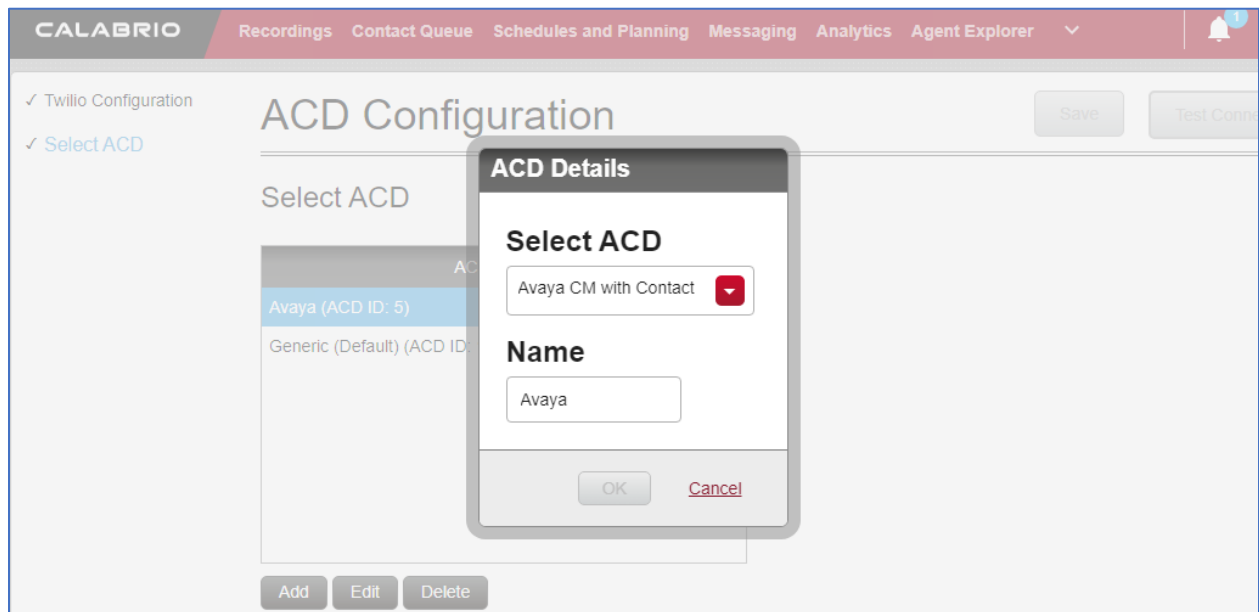
The screenshot shows the Calabrio web interface login page. At the top, there is a dark red header with the 'CALABRIO' logo in white. Below the header, the main content area is light gray. In the center, there is a white login box with the following elements: a 'Username' input field, a 'Password' input field, a 'FORGOT PASSWORD?' link, a 'LOG IN' button, and a 'SINGLE SIGN-ON' button. Below the login box, there is a language selector dropdown menu showing 'English'. At the bottom left of the page, there is small text: 'Version 11.0.2.1147', '© 2008-2024 Calabrio, Inc. All rights reserved.', and 'Calabrio and the Calabrio logo are registered trademarks of Calabrio, Inc.'

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** drop down menu and type in a **Name** for the ACD.



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**

The following fields are not required for this testing but do require data to be input in order for the ACD Configuration to save successfully:

- Type in C:\Program Files\Common Files\Calabrio ONE\Data Server\gis for the **DIRECTORY** under **AVAYA GIS CONFIGURATION**
- Type in 7003 for **REAL TIME ADHERENCE (RTA) PORT**

No further configuration on this page, such as CMS or CDR, is required for testing. Select **Save** once done.

CALABRIO Recordings Contact Queue Schedules and Planning Messaging Analytics Agent Explorer 1 Hello, Tenant ▼ Help

✓ Twilio Configuration
✓ Select ACD
✓ ACD Filtering
✓ Avaya CM with Contact Center Elite Configuration
✓ Avaya Communication Manager Information
✓ Real Time Adherence (RTA) Port
✓ Synchronization Interval
✓ Avaya GIS Configuration
✓ Avaya Call Management System (CMS) Connection Configuration
✓ CDR Connection Configuration
✓ CDR Parameter Layout

ACD Configuration

Save Test Connection Cancel

Avaya CM with Contact Center Elite Configuration

AE Services SMS Information.

SMS SERVER URL

https://10.33.1.4

Avaya Communication Manager Information

Avaya Communication Manager Information

COMMUNICATION MANAGER IP ADDRESS

10.33.1.6

COMMUNICATION MANAGER LOGIN

calabrio

COMMUNICATION MANAGER PASSWORD

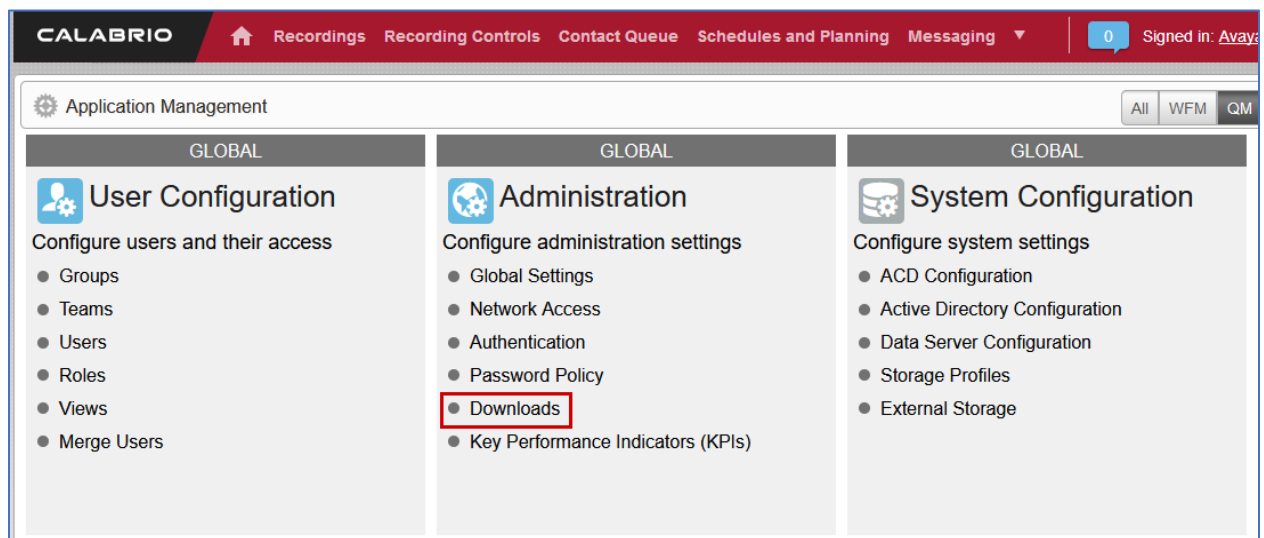
VIRTUAL EXTENSION PREFIX

DMCC

▼ CMS ACD ID

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 software. Install the Data Server on the server prepared to be used as the Calabrio One Data 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.

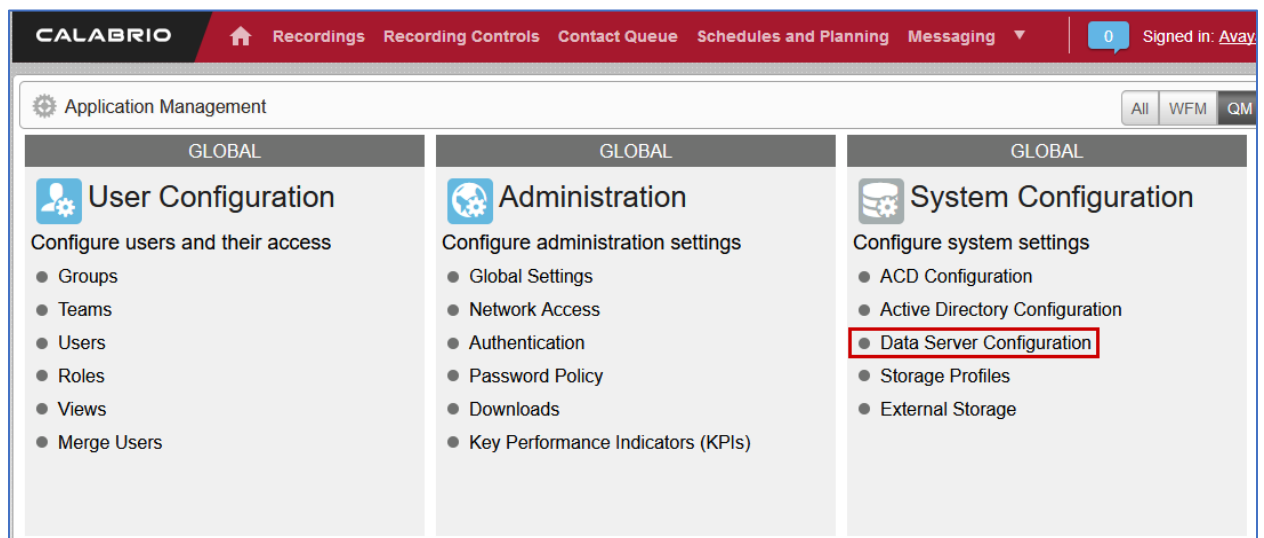
Available Installers

[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, which should be the IP address of the server where the Data Server software was installed. Check the box for **Enable Sync** and choose the ACD configured in the previous step to retrieve the user data from.

The screenshot shows the 'Data Server Configuration' page in the Calabrio application. The page has a red header with the Calabrio logo and navigation links: Recordings, Contact Queue, Schedules and Planning, Messaging, Analytics, and Agent Explorer. On the right of the header, there is a user profile 'Hello, Tenant' and a 'Help' link. A left sidebar contains a list of configuration categories, with 'Select Data Server Configuration' highlighted. The main content area is titled 'Data Server Configuration' and includes buttons for 'Save', 'Test Connection', 'Remove', and 'Cancel'. Below the title, there are three sections: 'Select Data Server Configuration' with a text input field containing '10.33.1.64' and a red dropdown arrow; 'Display Name' with a text input field containing '10.33.1.64'; and 'Regional Data Server ACD Sync Settings' which includes a checked 'Enable Sync' checkbox and two tables. The first table, under 'Available', has a 'Basic Filter' and a dropdown menu showing 'Generic (Default)'. The second table, under 'Assigned', has a 'Basic Filter' and a dropdown menu showing 'Avaya'.

Basic Filter
Available
Generic (Default)

Basic Filter
Assigned
Avaya

Continuing from above, check the box for **Enable Device Sync (not shown)** and **Enable CTI Signaling** then type in the IP Address of Data Server being configured. Check the box for **Enable Audio Recording**. Enter the IP Address of the Recording server and the file path location where recordings will be temporarily stored on the Data Server being configured.

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 a single server.

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

The screenshot shows the 'Data Server Configuration' page in the CALABRIO application. The left sidebar contains a list of configuration categories, with 'Recording CTI Signaling Server' selected. The main content area is divided into two sections. The first section, 'Data Server Configuration', has a 'Save' button and a 'Test Connection' button. It includes a checkbox for 'Enable CTI Signaling' which is checked, followed by a text input field containing '10.33.1.64'. The second section, 'Recording Capture Server Settings', has a 'Remove' button and a 'Cancel' button. It includes a checkbox for 'Enable Audio Recording' which is checked, followed by a text input field containing '10.33.1.64' and another text input field containing 'C:\common\TempRecordings'.

CALABRIO Recordings Contact Queue Schedules and Planning Messaging Analytics Agent Explorer 1 Hello, Tenant ▼ Help

✓ Select Data Server Configuration

✓ Display Name

✓ Regional Data Server ACD Sync Settings

✓ Regional Data Server ACD Capture Settings

✓ Regional Data Server Real-Time Event Settings

✓ Regional Data Server Staged Upload Settings

✓ Regional Data Server Reconciliation Settings

✓ Active Directory Sync

✓ Data Server Device Sync Settings

✓ Recording SIPREC Signaling Server Settings

✓ Recording CTI Signaling Server

Data Server Configuration

Save Test Connection Remove Cancel

☒ 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.

10.33.1.64

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.

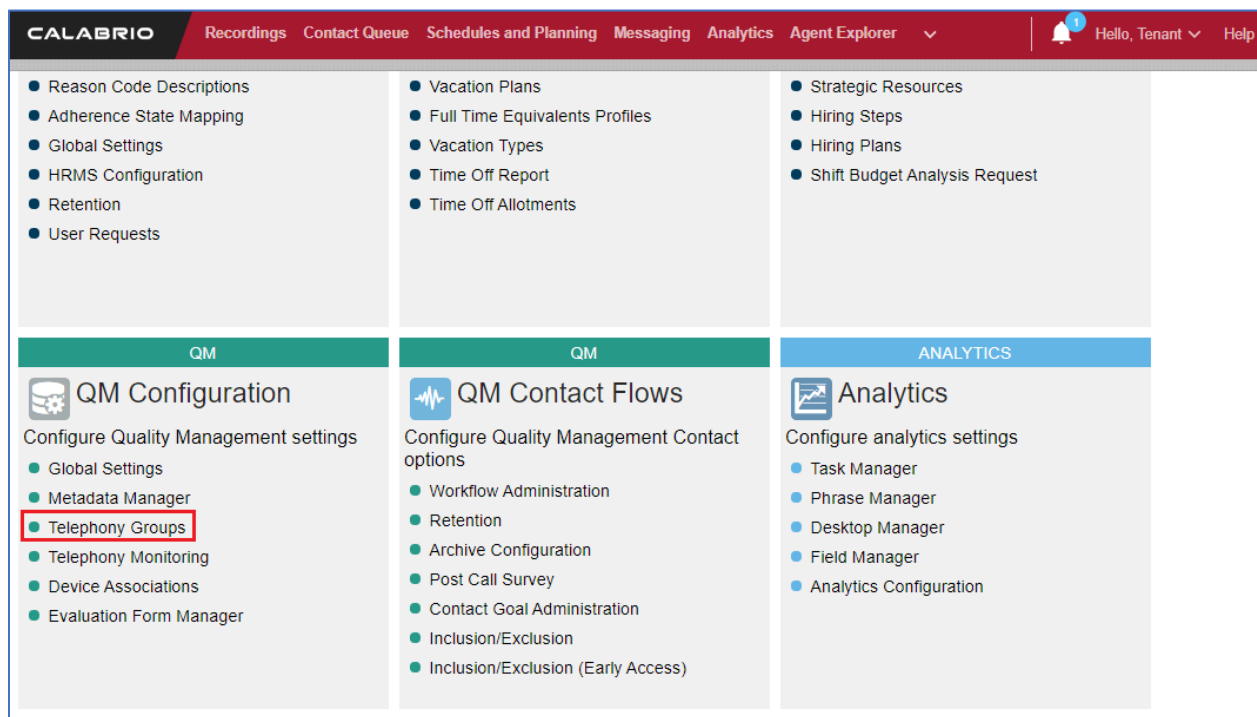
10.33.1.64

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:\common\TempRecordings

7.4. Configuration of the Application Enablement Interfaces – DMCC

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



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**.

The screenshot shows the 'Telephone Groups' configuration page. The page has a sidebar with links for 'Telephone Groups', 'Signaling Groups', and 'Recording Groups'. The main content area is titled 'Telephone Groups' and contains a table with the following data:

Name	Type
Avaya CM	Avaya Communication Manager

Below the table, there are two sections:

TELEPHONY GROUP NAME
Enter a unique name for the group.
AvayaCM

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

At the bottom, there are three buttons: 'Add', 'Update', and 'Reset Telephony Group'.

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 **Section 7.1**.
- Select a **DEVICE SYNCHRONIZATION DATA SERVER** which will be the name of the Data Server configured in **Section 7.3**.

The screenshot shows the 'Telephony Groups' configuration page in the CALABRIO application. The left sidebar lists 'Telephony Groups', 'Signaling Groups', and 'Recording Groups', with 'Telephony Groups' selected. The main content area is titled 'Telephony Groups' and contains the 'Avaya Telephony Platform Configuration' section. This section includes 'Telephony Group Global Settings' with the following fields: 'DEVICE PASSWORD' (with radio buttons for 'Use Device Extension', 'Use Static Password' (selected), and 'Use Custom Pattern', and a password input field showing four asterisks); 'ASSOCIATED AVAYA ACD' (a dropdown menu showing 'Avaya (ACD ID: 5)'); 'Enable Free Seating' (an unchecked checkbox); 'RECORDING SKILL HUNT GROUP' (a label and an 'Extension' input field); and 'DEVICE SYNCHRONIZATION DATA SERVER' (a dropdown menu showing '10.33.1.64'). 'Save' and 'Delete' buttons are located at the top right of the configuration area. The top navigation bar includes links for Recordings, Contact Queue, Schedules and Planning, Messaging, Analytics, and Agent Explorer, along with a user greeting 'Hello, Tena'.

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 of 4721 in the **PORT** field

In the **User Credentials** section:

- Type in the Login name of the user account created in **Section 6.2** in **USER NAME**
- Type in the password for the above user account in **PASSWORD**

The screenshot shows the 'Telephony Groups' configuration window with the 'Application Enablement Services Information' tab selected. The window has 'Save', 'Delete', and 'Cancel' buttons at the top right. The 'Application Enablement Services Information' section contains the following fields:

- SWITCH CONNECTION NAME**: A text field with the value 'interopcm'. Below it is a note: 'The name to use to identify the switch being used with AES. Note: The Connection Name is case-sensitive in AES'.
- HOSTNAME / IP ADDRESS**: A text field with the value '10.33.1.4'.
- PORT**: A text field with the value '4721'.
- Use Secure Connection**: A checkbox that is currently unchecked.

The 'User Credentials' section contains the following fields:

- USER NAME**: A text field with the value 'calabrio'.
- PASSWORD**: A password field with masked characters '*****'.

At the bottom, there is a message: 'This saves the changes to this server. Use the save above to save the whole form.' and four buttons: 'Add', 'Update', 'Delete', and 'Reset Server'.

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

The screenshot shows the 'Telephony Groups' configuration window with the 'Signaling Groups' tab selected. The window has 'Save', 'Delete', and 'Cancel' buttons at the top right. On the left, there is a sidebar with three tabs: 'Telephony Groups', 'Signaling Groups', and 'Recording Groups', all of which are checked. The main area shows a progress bar with three steps: '1. Telephony', '2. Signaling' (which is the active step), and '3. Recording'. Below the progress bar, there is a 'Previous' button and a 'Next' button. The 'Signaling Groups' section contains a table with two columns: 'Name' and 'Telephony Group'. The table has one row with the values 'SG 1' and 'Avaya CM'. Below the table, there is an empty text field for adding a new signaling group.

- **PRIMARY QM SIGNALING DATA SERVER:** Select the IP Address of Calabrio One Data Server configured in **Section 7.3** from the dropdown menu
- **AES SERVER:** Select the IP Address of the AES configured in **Application Enablement Services Information** Telephony Group configuration from the dropdown menu

Telephony Groups

SaveDeleteCancel

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

10.33.1.64

AES SERVER
Select the primary AES server for this Signaling Group

10.33.1.4

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**.

Under **Recording Groups Assignment**, Select the **Recording Group** that is being configured from the dropdown menu and set **Priority** to **Primary**. Select **Save** once completed.

Telephony Groups

- ✓ Telephony Groups
- ✓ Signaling Groups
- ✓ Recording Groups

Telephony Groups

SaveDeleteCancel

1. Telephony
2. Signaling
3. Recording

PreviousNext

Recording Groups Settings

Record Group	Signaling Group	Telephony Group
RG 1	SG 1	Avaya CM

RECORDING GROUP NAME
Enter a unique name for the group

RG 1

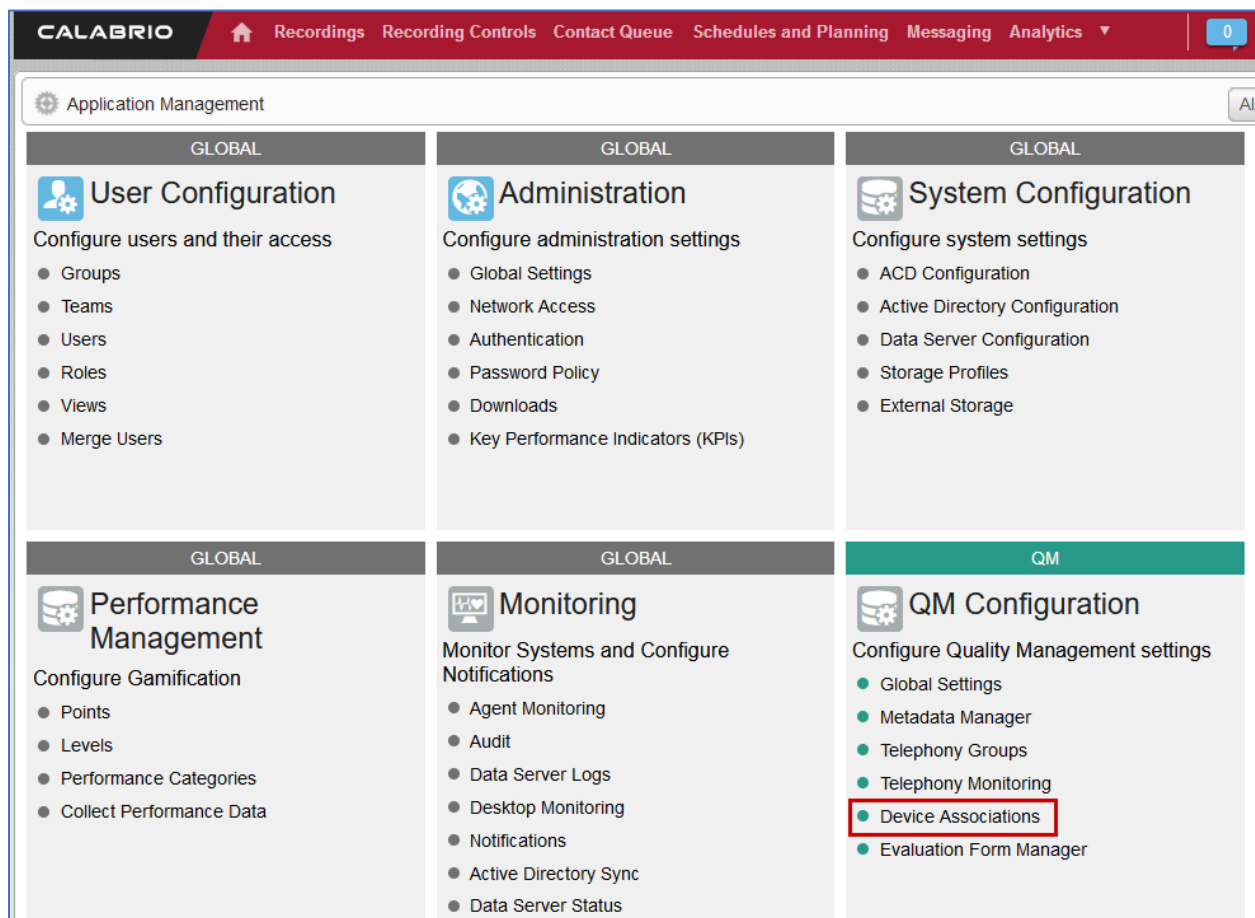
AddUpdateDeleteReset Recording Group

Recording Groups Assignment

Hostname	Recording Group	Priority
10.33.1.64	RG 1	Primary

7.5. Configuration of Device Associations

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



Configure the device association as needed based on the particular call scenario tests. For example, some scenarios require Free Seating to be configured under Telephony Groups configuration and the agent to be unassigned from the station in Device Associations. For assistance with specific recording scenarios, please contact Calabrio for further information.

- All devices to be recorded must have:
 - A **Recording Group** assigned, which should be the one configured in **Section 7.4**
 - A **Recording Type** configured depending on the station type
 - **Single Step Conference** stations require a **Virtual Extension** to be configured
 - An **Agent** assigned with a Role that contains the **Record Voice** permission
 - **Stereo** checkbox enabled if dual channel, stereo recording is desired and configured in CM/AES

During the compliance test, the following extensions were configured to be recorded.

<div>CALABRIO</div> <div> Recordings Contact Queue Schedules and Planning Messaging Analytics Agent Explorer Reporting Data Explorer </div> <div> Hello, Tenant Help </div>										
Device Associations										CANCEL SAVE
Associate devices from your ACD with users, recording groups, and recording types										
<div> <div> <div></div> <div></div> </div> <div>Results per page 10 1-6 of 6</div> </div>										
Configured	Recording Tones	Stereo	Device Type	Extension	Virtual Extension	Agent	Telephony Group	Signalling Group	Recording Group	Recording Type
Yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avaya Phone Device	3402	3372	Age...	Avaya CM	SG 1	RG 1	Sin...
Yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avaya Phone Device	3302		Age...	Avaya CM	SG 1	RG 1	Mul...
Yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avaya Phone Device	3311	3317	Age...	Avaya CM	SG 1	RG 1	Sin...
Yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avaya Phone Device	3401	3371	Age...	Avaya CM	SG 1	RG 1	Sin...
Yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avaya Phone Device	3301		Age...	Avaya CM	SG 1	RG 1	Mul...
Yes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Avaya Phone Device	3312	3318	Age...	Avaya CM	SG 1	RG 1	Sin...

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Calabrio Quality Management with Communication Manager and Application Enablement Services.

8.1. Verify Application Enablement Services

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.

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

▶ User Management

▶ Utilities

▶ Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Mon Jan 08 01:27:08 EST 2024

Service Uptime: 33 days, 23 hours 20 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 7

Number of Existing Devices: 13

Number of Devices Created Since Service Boot: 152652

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	A064D211343C625B2D9DC9B83FCBD67F-6	calabrio	cmapiApplication	10.33.1.64	XML Unencrypted	13

Terminate Sessions

Show Terminated Sessions

Item 1-1 of 1

1Go

8.2. Verify Communication Manager

Via SAT, use the **list monitored-station** command to verify the Calabrio is successfully monitoring the configured station.

list monitored-station									
MONITORED STATION									
Associations:	1	2	3	4	5	6	7	8	
	CTI	CTI	CTI	CTI	CTI	CTI	CTI	CTI	
Station Ext	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	Lnk CRV	
-----	-----	-----	-----	-----	-----	-----	-----	-----	
3302	1 0100								
3311	1 0117								
3312	1 0111								
3317	1 0116								
3318	1 0115								
3371	1 010D								
3372	1 0104								
3401	1 010E								
3402	1 0106								

8.3. Verify Calabrio One

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

CALABRIO

Recordings

Contact Queue

Schedules and Planning

Messaging

Analytics

Agent Explorer

Reporting

Data Explorer

Add-Ons

Hello, Khanh

Help

Filters

Searching in America/Chicago

Filter Set

+

ADD FILTER

RESET

DATE RANGE

Today

×

SEARCH SCOPE

All Evaluations

×

CANCEL

APPLY

Recordings

(2) Active

ATT: 00:00:42

Results per page 80

1-24 of 24

<

>

<div><input type="checkbox"/></div>	Contact ID	Last Name	First Name	Group Name	Team Name	Calling Number
<div><input type="checkbox"/></div>	115	Agent 1001	Agent 1001	Default Group	Default Team	3401
<div><input type="checkbox"/></div>	114	Agent 1004	Agent 1004	Default Group	Default Team	3303
<div><input type="checkbox"/></div>	113	Agent 1009	Agent 1009	Default Group	Default Team	6139674300
<div><input type="checkbox"/></div>	112	Agent 1004	Agent 1004	Default Group	Default Team	6139674300
<div><input type="checkbox"/></div>	111	Agent 1001	Agent 1001	Default Group	Default Team	6139674300
<div><input type="checkbox"/></div>	110	Agent 1009	Agent 1009	Default Group	Default Team	6139674300
<div><input type="checkbox"/></div>	109	Agent 1001	Agent 1001	Default Group	Default Team	3301
<div><input type="checkbox"/></div>	108	Agent 1009	Agent 1009	Default Group	Default Team	3407
<div><input type="checkbox"/></div>	107	Agent 1009	Agent 1009	Default Group	Default Team	3303
<div><input type="checkbox"/></div>	106	Agent 1008	Agent 1008	Default Group	Default Team	3407
<div><input type="checkbox"/></div>	105	Agent 1008	Agent 1008	Default Group	Default Team	3303
<div><input type="checkbox"/></div>	104	Agent 1008	Agent 1008	Default Group	Default Team	3303
<div><input type="checkbox"/></div>	103	Agent 1008	Agent 1008	Default Group	Default Team	3407
<div><input type="checkbox"/></div>	102	Agent 1004	Agent 1004	Default Group	Default Team	6139674305
<div><input type="checkbox"/></div>	101	Agent 1004	Agent 1004	Default Group	Default Team	3401
<div><input type="checkbox"/></div>	100	Agent 1003	Agent 1003	Default Group	Default Team	3407
<div><input type="checkbox"/></div>	99	Agent 1003	Agent 1003	Default Group	Default Team	3407

© 2008-2023 Calabrio, Inc. All rights reserved.

Version 11.0.2.1142

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

The screenshot displays the CALABRIO application interface for a call playback window. The top navigation bar includes links for Recordings, Contact Queue, Schedules and Planning, Messaging, Analytics, Agent Explorer, Reporting, Data Explorer, and Add-Ons. The user is logged in as 'Hello, Khanh'.

The main interface is divided into several sections:

- Details:** Shows contact information for Contact 116, including Contact ID, Calling Number, Called Number, Call Duration, Reason, HR, Training, State, and Contact Type.
- Transcription:** Displays a timeline of the call with various segments labeled, such as '161.', '224461 conference conference.', '112256 hang up now on the.', and '671-2256.'.
- Audio:** A central audio waveform player with a red play button and a progress bar.
- Evaluation (Unscored):** A section for evaluating the call performance, including a 'Choose Evaluation' dropdown, a 'NoApproval_Percentage' field, and a 'GREET' section with evaluation questions and their corresponding scores.

The evaluation questions and their scores are as follows:

Question	Score	Percentage
1.1 Immediate attention to customer?	20.00%	
1.2 Proper identification of company?	20.00%	
1.3 Proper company greeting?	20.00%	

9. Conclusion

These Application Notes describe the procedures for configuring Calabrio Quality Management 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 successfully.

10. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at support.avaya.com. Calabrio Quality Management documentation is available through the application via online help.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 12, September 2023, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at <http://support.avaya.com>.
- [4] *Administering Avaya Aura® Application Management*, Release 10.1.x, Issue 5, October 2023, available at <http://support.avaya.com>.

©2024 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.