



Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio One R11.5 with Avaya Aura® Communication Manager R8.1.3 and Avaya Aura® Application Enablement Services R8.1.3 – 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 to perform a SMS service query to obtain the list of agents and stations configured in Avaya Aura® 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 did not include use of any specific encryption features.

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 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.

- Calabrio is doing split-stream recording using two terminals in independent mode, the minimum release and patch in Communication Manager to support this is in 8.1.3.2.0. This observation to make sure the Communication Manager is running this release or newer otherwise recording using the single step conference method may not work.

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 through Session Border Controller for Enterprise used SIP trunks to connect to the PSTN.

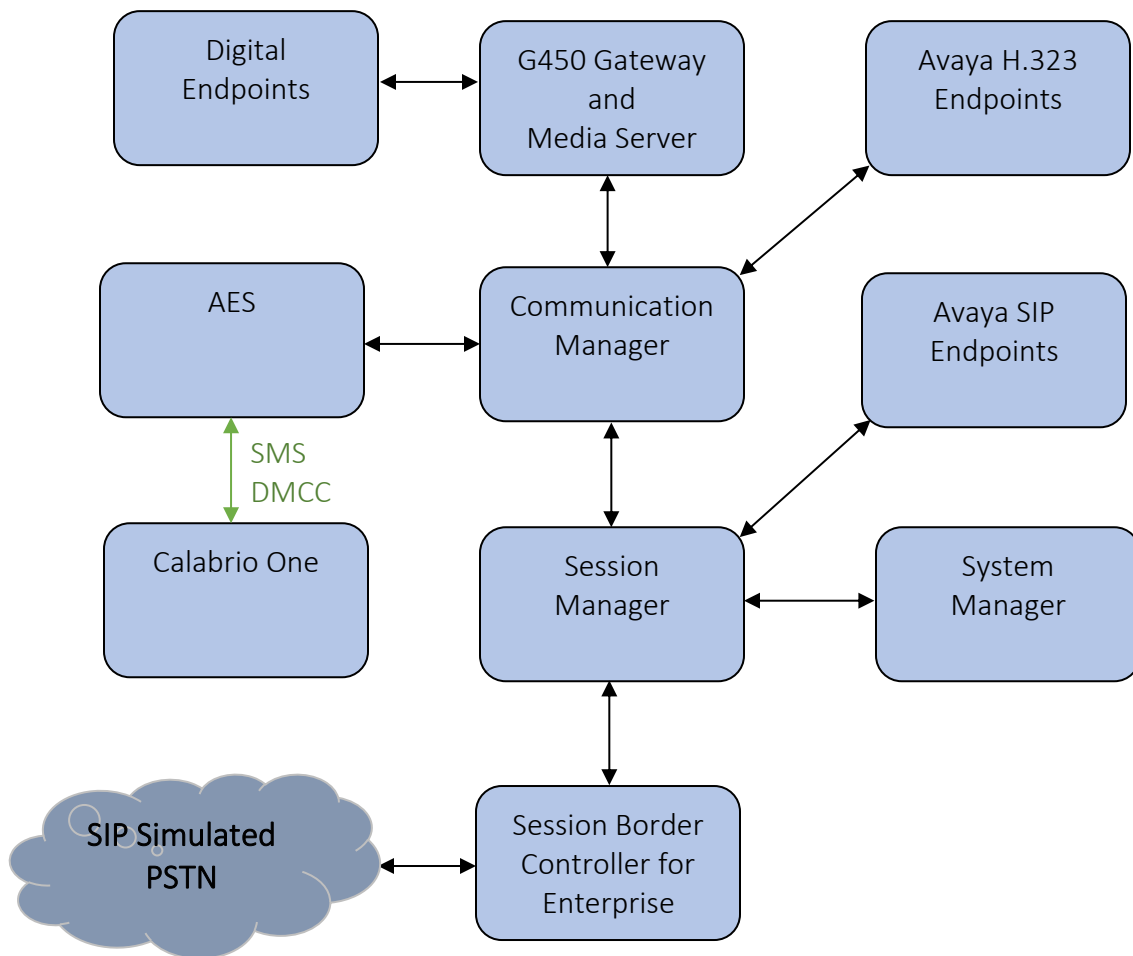


Figure 1 – Calabrio One Compliance Test Configuration

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	8.1.3 8.1.3.2.0.890.26989
Avaya Aura® Application Enablement Services running on virtualized environment	8.1.3 8.1.3.2.0.4-0
Avaya Aura® Session Manager running on virtualized environment	8.1.3 8.1.3.0.813014
Avaya Aura® System Manager running on virtualized environment	8.1.3 8.1.3.0.1011784
Avaya Aura® Media Server running on virtualized environment	8.0 8.0.2.163
Avaya Session Border Controller for Enterprise	8.1.2 8.1.2.0-37-21065
Avaya G450 Media Gateway	41.34.0
Avaya IP Endpoints <ul style="list-style-type: none">• 9608 (H.323)• 9621 (H.323)• 9641GS (SIP)• J189 (SIP)	6.8.304 6.8.304 7.1.9.0.8 4.0.7.1.5
Avaya 9404 Digital Telephone	22.0
Desktop PC running Avaya Agent for Desktop (H.323 and SIP)	2.0.6.0.10
Calabrio ONE Recording and Quality Management running on Windows 2016 Server	11.5

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          Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n     DS1 MSP? y
ATM WAN Spare Processor? n                DS1 Echo Cancellation? y
ATMS? 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 Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 Server	Password	Enabled	Status		
1:	aes81	*	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: 59999			
Type: ADJ-IP			
		COR: 1	
Name: CTI 1			
Unicode Name? n			

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 shown below. Create a user account on Communication Manager by navigating to the **Administrator Accounts** page under **Security** in the left hand pane and selecting the radio button **Add Login** and **Privileged Administrator**. Click **Submit** to continue the process.

The screenshot shows a web interface for system administration. The top navigation bar is red with 'Help' and 'Log Off' links. Below it, a breadcrumb trail reads 'Administration / Server (Maintenance)'. The left sidebar contains a tree view with categories: 'Server' (Status Summary, Process Status, Shutdown Server, Server Date/Time, Software Version), 'Server Configuration' (Server Role, Network Configuration, Static Routes, Display Configuration, Time Zone Configuration, NTP Configuration), 'Server Upgrades' (Manage Updates), 'IPSI Firmware Upgrades' (IPSI Version, Download IPSI Firmware, Download Status, Activate IPSI Upgrade, Activation Status), 'Data Backup/Restore' (Backup Now, Backup History, Schedule Backup, Backup Logs, View/Restore Data, Restore History), and 'Security' (Administrator Accounts, Login Account Policy, Change Password, Login Reports). The 'Administrator Accounts' page is active, showing a title bar 'Administrator Accounts' and a description: 'The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.' Below this is a 'Select Action:' section with 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'. There are also three 'Change Login', 'Remove Login', and 'Lock/Unlock Login' options, each with a 'Select Login' dropdown menu. At the bottom are 'Add Group' and 'Remove Group' options, each with a 'Select Group' dropdown menu. 'Submit' and 'Help' buttons are at the bottom left.

The **Administrator Accounts -- Add Login** screen is displayed. Enter a name in 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	<input type="text" value="calabrio"/>
Primary group	<input type="text" value="susers"/>
Additional groups (profile)	<input type="text" value="prof18"/>
Linux shell	<input type="text" value="/bin/bash"/>
Home directory	<input type="text" value="/var/home/calabrio"/>
Lock this account	<input type="checkbox"/>
SAT Limit	<input type="text" value="none"/>
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
Enter password	<input type="password" value="*****"/>
Re-enter password	<input type="password" value="*****"/>
Force password change on next login	<input checked="" type="radio"/> No <input type="radio"/> Yes

Though a Privileged Administrator account was used, a new 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**.

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 on Session Manager via System Manager.

```
change station 70001                                     Page 1 of 5
                                                         STATION
Extension: 70001                                         Lock Messages? n          BCC: 0
Type: 9641                                               Security Code: *          TN: 1
Port: S000000                                           Coverage Path 1: 98      COR: 1
Name: Black Panther                                     Coverage Path 2:         COS: 1
Unicode Name? n                                         Hunt-to Station:         Tests? y
STATION OPTIONS
Loss Group: 19                                         Time of Day Lock Table:
Personalized Ringing Pattern: 1
Message Lamp Ext: 50001
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
```

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 **virtual**.
- 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**.


add station 3371		Page 1 of 1
STATION		
Extension: 3371		BCC: 0
Type: virtual	Security Code: *	TN: 1
	Coverage Path 1:	COR: 1
Name: DMCC Station 3371	Coverage Path 2:	COS: 1
Unicode Name? n	Map-to Station:	
Time of Day Lock Table:		
Personalized Ringing Pattern: 1		
Survivable COR: internal		
Survivable Trunk Dest? y		

6. Configure Avaya Aura® Application Enablement Services

All administration of Application Enablement Services is performed via a web browser. Enter the IP address of AES 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

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Mon Sep 6 00:03:55 2021 from 10.33.1.64
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.2.0.4-0
Server Date and Time: Thu Sep 23 18:14:55 MDT 2021
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 links to Communication Manager, navigate to the **Communication Manager Interface** → **Switch Connections** page and enter a name for the new switch connection (e.g. **interopcm**) 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 - interopcm

Switch Password: [password field]
Confirm Switch Password: [password field]
Msg Period: 30 Minutes (1 - 72)
Provide AE Services certificate to switch: ☐
Secure H323 Connection: ☐
Processor Ethernet: ☒
Enable TLS Certificate Hostname Validation: ☐
[Apply] [Cancel]

The display returns to the **Switch Connections** screen which shows that the **interopcm** 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
Networking
Security

Switch Connections

[text field] [Add Connection]

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
interopcm	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.

The screenshot shows the 'Communication Manager Interface | Switch Connections' page. On the left is a navigation pane with options: AE Services, Communication Manager Interface (selected), Switch Connections (selected), Dial Plan, High Availability, Licensing, and Maintenance. The main content area is titled 'Edit Processor Ethernet IP - interopcm'. It contains a text input field with '10.33.1.6' and an 'Add/Edit Name or IP' button. Below this is a table with two columns: 'Name or IP Address' and 'Status'. The table has one row with '10.33.1.6' and 'In Use'. A 'Back' button is at the bottom left of the main area.

Name or IP Address	Status
10.33.1.6	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.

The screenshot shows the 'User Management | User Admin | Add User' page. On the left is a navigation pane with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (selected), Service Admin, and User Admin (selected). Under User Admin, there are links: Add User (selected), Change User Password, List All Users, Modify Default Users, and Search Users. The main content area is titled 'Add User'. It includes a note: 'Fields marked with * can not be empty.' Below this are several form fields: * User Id (calabrio), * Common Name (calabrio), * Surname (calabrio), * User Password (masked with dots), * Confirm Password (masked with dots), Admin Note (empty), Avaya Role (None), Business Category (empty), Car License (empty), CM Home (empty), Cms Home (empty), CT User (Yes), and Department Number (empty).

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

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

CTI Users

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

EditList 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
Security Database
Control

Edit CTI User

User Profile:	User ID	calabrio
	Common Name	calabrio
	Worktop Name	NONE
	Unrestricted Access	<input checked="" type="checkbox"/>

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	<input type="checkbox"/>

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.

WebLM Home

Install license

Licensed products

APPL_ENAB

▼ Application_Enablement

View license capacity

View peak usage

ASBCE

► Session_Border_Controller_E_AE

CE

► COLLABORATION_ENVIRONMENT

COMMUNICATION_MANAGER

► Call_Center

► Communication_Manager

► Dialog_Designer

MESSAGING

► Messaging

MSR

► Media_Server

ORCHESTRATION_DESIGNER_IDE

► Orchestration_Designer_IDE

POM

► POM

PRESENCE_SERVICES

► Presence_Services

SYSTEM_MANAGER

► System_Manager

Application Enablement (CTI) - Release: 8 - Stand

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

License installed on: July 18, 2019 3:10:38 PM -06:00

License File Host IDs:

Licensed Features

13 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
AES HA LARGE VALUE_AES_HA_LARGE	permanent	100
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	100
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	100

6.4. Obtain DMCC Port and TSAPI Link

To obtain the DMCC port, navigate to **Networking** → **Ports**, make sure the DMCC 4721 port enabled in the DMCC Server Ports section.

Networking Ports			Home Help Logout
Ports			
CVLAN Ports			
Unencrypted TCP Port	9999	Enabled	Disabled
Encrypted TCP Port	9998	Enabled	Disabled
DLG Port			
TCP Port	5678		
TSAPI Ports			
TSAPI Service Port	450	Enabled	Disabled
Local TLINK Ports			
TCP Port Min	1024		
TCP Port Max	1039		
Unencrypted TLINK Ports			
TCP Port Min	1050		
TCP Port Max	1065		
Encrypted TLINK Ports			
TCP Port Min	1066		
TCP Port Max	1081		
DMCC Server Ports			
Unencrypted Port	4721	Enabled	Disabled
Encrypted Port	4722	Enabled	Disabled
TR/87 Port	4723	Enabled	Disabled

To obtain the Tlink, navigate to **Security** → **Security Database** → **Tlinks**. The Tlinks displays in the right-hand side, the Tlink will be used for the configuration in the Calabrio WFM.

Security Security Database Tlinks		Home Help Logout
Tlinks		
Tlink Name		
<input checked="" type="radio"/> AVAYA#INTEROPCM#CSTA#AES8		
<input type="radio"/> AVAYA#INTEROPCM#CSTA-S#AES8		
<button>Delete Tlink</button>		

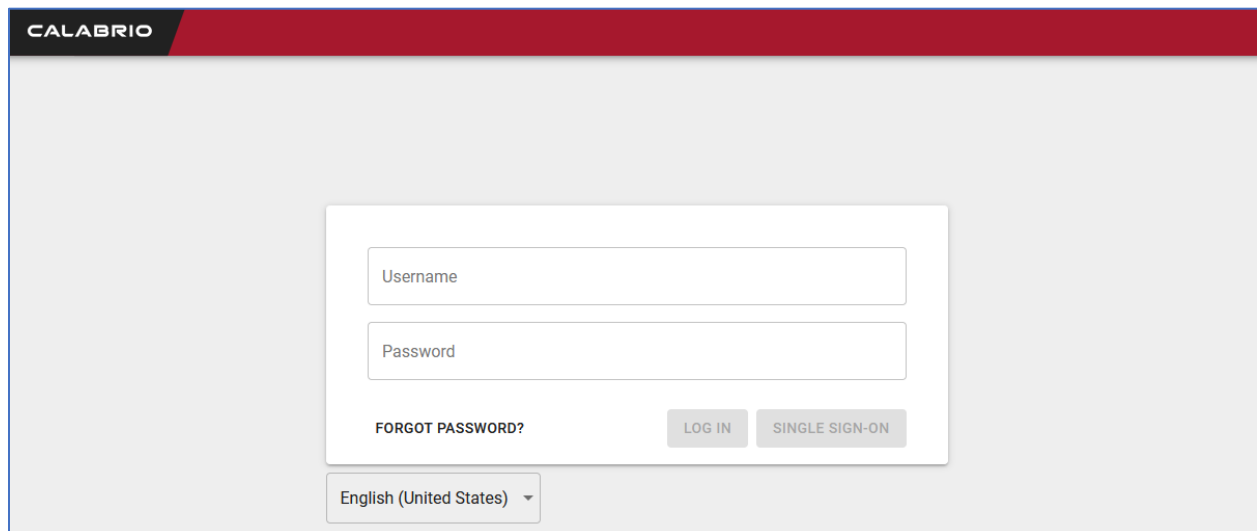
7. Configure Calabrio One

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.



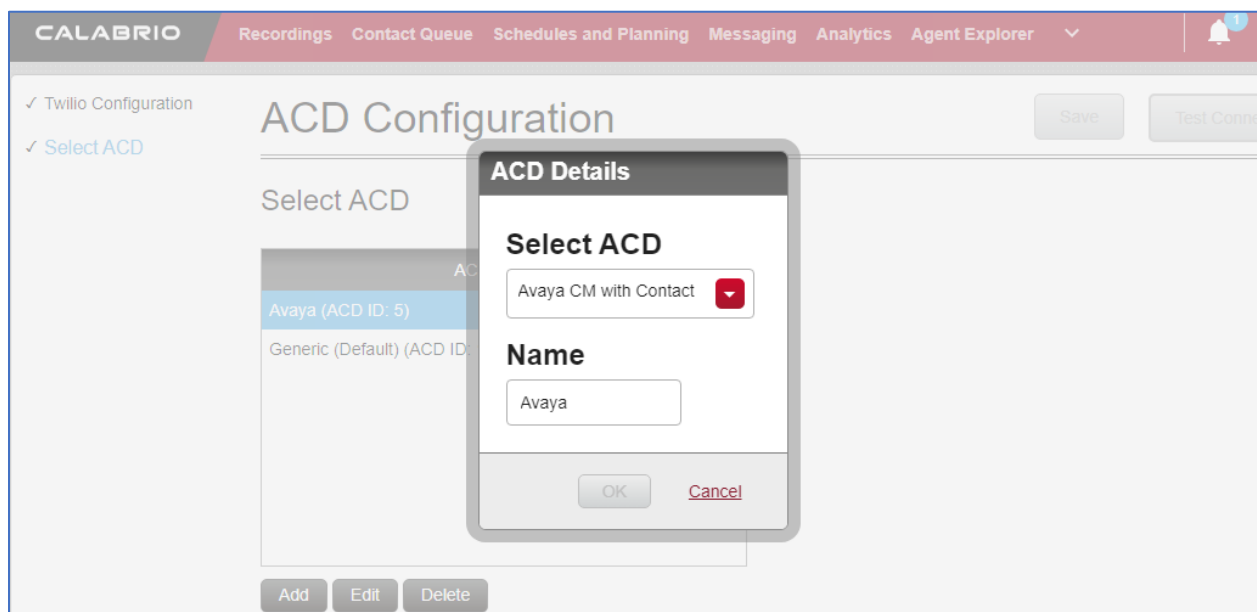
The screenshot shows the Calabrio One web interface. At the top is a dark red header with the word "CALABRIO" in white. Below the header is a light gray background. In the center is a white login box. Inside the box, there are two input fields: "Username" and "Password". Below the "Password" field is a link that says "FORGOT PASSWORD?". To the right of the "FORGOT PASSWORD?" link are two buttons: "LOG IN" and "SINGLE SIGN-ON". Below the login box is a language selection dropdown menu showing "English (United States)" with a downward arrow.

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:

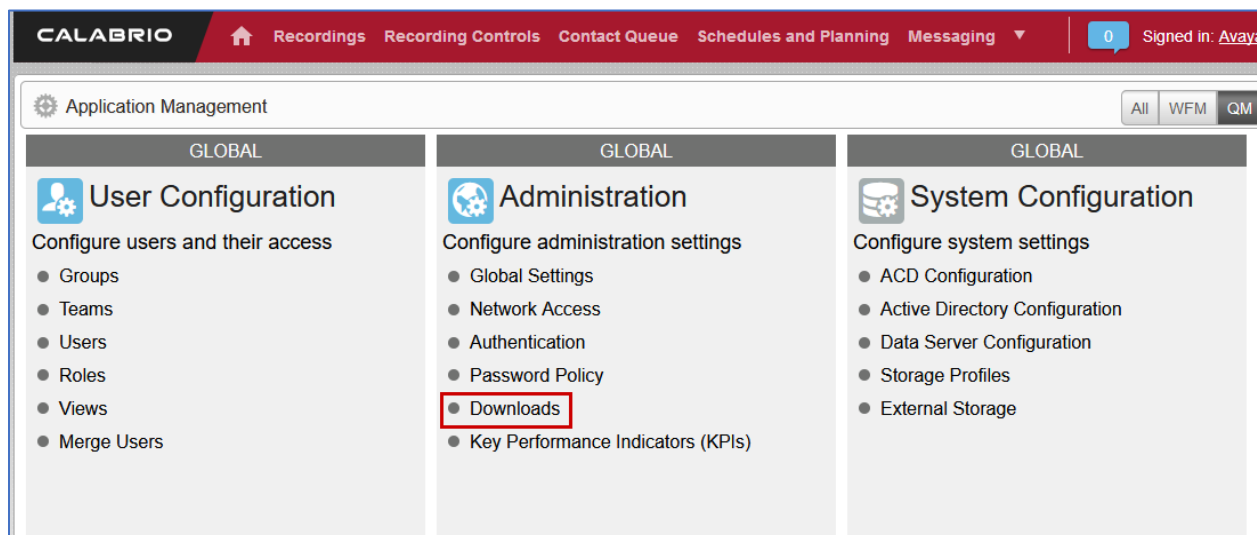
- **SMS SERVER URL:** Type in the SMS Server URL for the AES.
- **COMMUNICATION MANAGER IP ADDRESS:** Communication Manager IP Address
- **COMMUNICATION MANAGER LOGIN & PASSWORD:** As configured in **Section 5.5**
- **VIRTUAL EXTENSION PREFIX:** Type in **DMCC**

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

The screenshot shows the Calabrio ACD Configuration interface. The top navigation bar includes 'CALABRIO' and various menu items: Recordings, Contact Queue, Schedules and Planning, Messaging, Analytics, Agent Explorer, and a user profile 'Hello, Tenant' with a 'Help' link. A left sidebar lists configuration categories with checkmarks: Twilio Configuration, Select ACD, ACD Filtering, Avaya CM with Contact Center Elite Configuration (highlighted in blue), Avaya Communication Manager Information, Real Time Adherence (RTA) Port, Synchronization Interval, Avaya GIS Configuration, Avaya Call Management System (CMS) Connection Configuration, CDR Connection Configuration, and CDR Parameter Layout. The main content area is titled 'ACD Configuration' and contains a 'Save' button, a 'Test Connection' button, and a 'Cancel' link. Below the title, it says 'Avaya CM with Contact Center Elite Configuration' and 'AE Services SMS Information.' The 'SMS SERVER URL' field is populated with 'https://10.33.1.4'. The 'Avaya Communication Manager Information' section includes fields for 'COMMUNICATION MANAGER IP ADDRESS' (10.33.1.6), 'COMMUNICATION MANAGER LOGIN' (calabrio), 'COMMUNICATION MANAGER PASSWORD' (masked with dots), and 'VIRTUAL EXTENSION PREFIX' (DMCC). At the bottom, there is a dropdown menu for '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.
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.

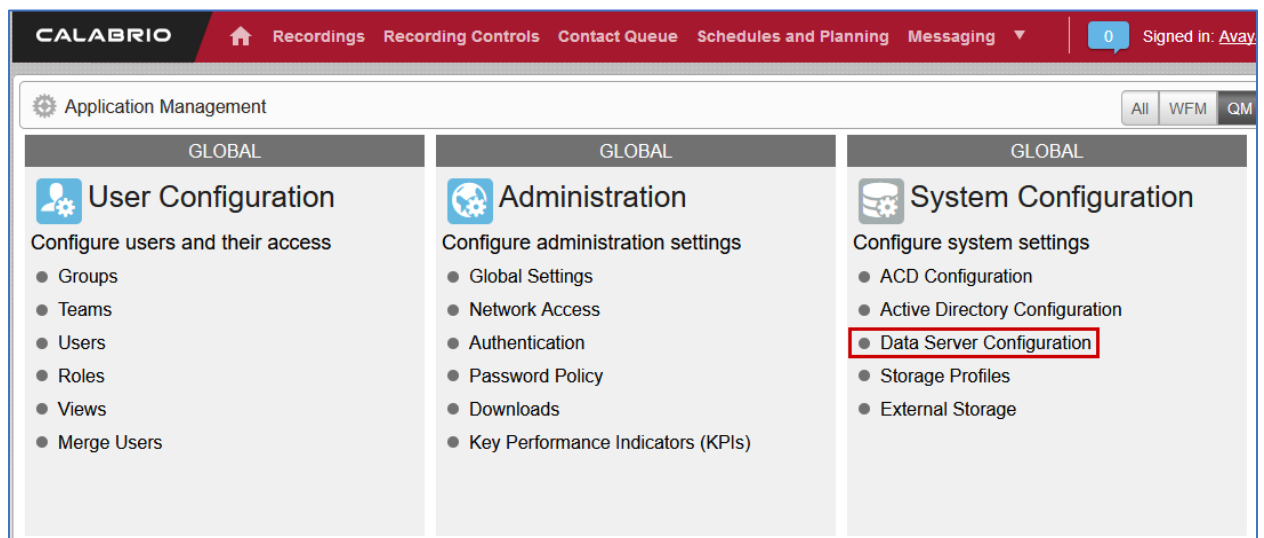
Available Installers

[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 choose the ACD configured in previous step to retrieve the data from.

The screenshot shows the 'Data Server Configuration' page in the CALABRIO application. The page has a red header bar with navigation links: Recordings, Contact Queue, Schedules and Planning, Messaging, Analytics, and Agent Explorer. A user greeting 'Hello, Tenant' and a 'Help' link are on the right. 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'. The configuration is divided into three sections: 'Select Data Server Configuration' with a dropdown menu showing '10.33.1.64'; '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 filter lists. The 'Available' filter list shows 'Generic (Default)', and the 'Assigned' filter list shows 'Avaya'.

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

Data Server Configuration

Save | Test Connection | Remove | Cancel

Select Data Server Configuration

10.33.1.64

Display Name

10.33.1.64

Regional Data Server ACD Sync Settings

☒ Enable Sync

Basic Filter	Basic Filter
Available	Assigned
Generic (Default)	Avaya

Continuing from above, check box for **Enable Capture (not shown)**, **Enable Device Sync (not shown)**, **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**.

The screenshot shows the 'Data Server Configuration' page in the Calabrio One application. The interface has a dark red header with the 'CALABRIO' logo and navigation tabs: Recordings, Contact Queue, Schedules and Planning, Messaging, Analytics, and Agent Explorer. A user profile 'Hello, Tenant' and a 'Help' link are in the top right. On the left, a sidebar lists various configuration categories, with 'Recording CTI Signaling Server' selected. The main content area is titled 'Data Server Configuration' and includes 'Save', 'Test Connection', 'Remove', and 'Cancel' buttons. It contains two sections: 'Enable CTI Signaling' with a checkbox, a text input for the IP address (10.33.1.64), and a description; and 'Recording Capture Server Settings' with a checkbox for 'Enable Audio Recording', a text input for the IP address (10.33.1.64), and a text input for the directory path (C:\common\TempRecordings).

CALABRIO Recordings Contact Queue Schedules and Planning Messaging Analytics Agent Explorer 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.

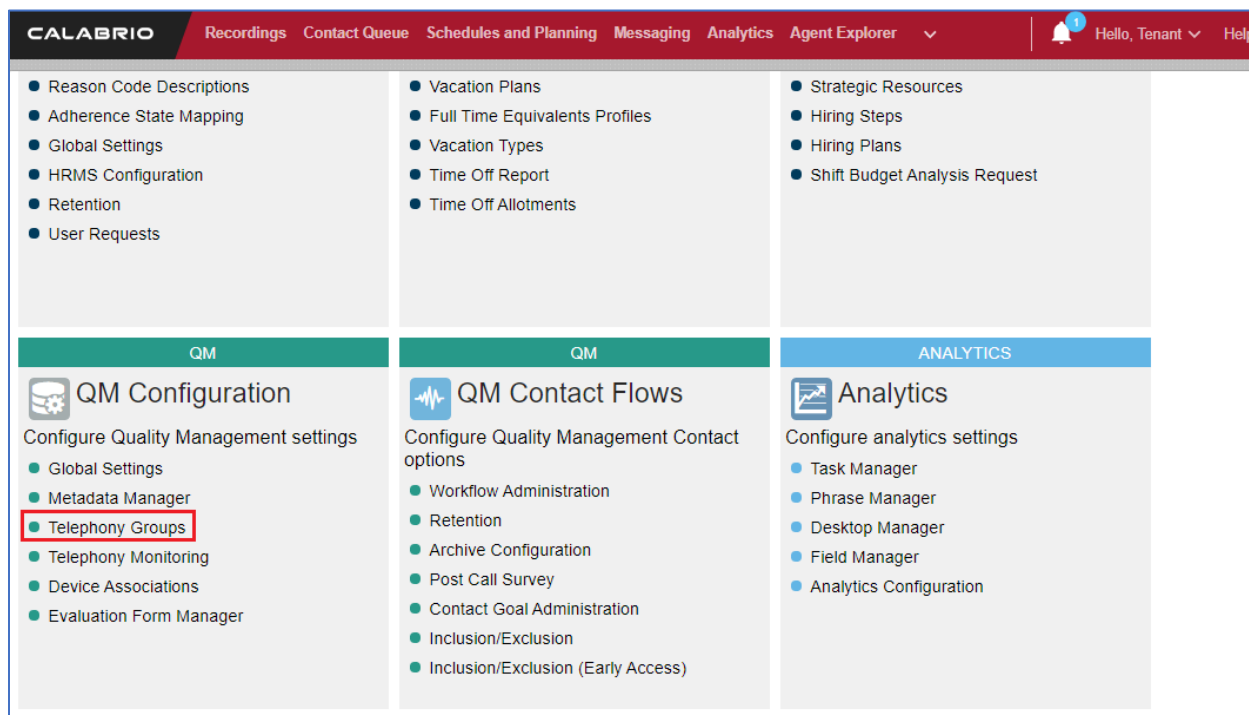
10.33.1.64

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 'Telephony Groups' configuration page. The page has a sidebar with 'Telephony Groups', 'Signaling Groups', and 'Recording Groups'. The main content area is titled 'Telephony Groups' and contains a description: 'Telephony Groups provide the structure used to create the recording infrastructure. Use this page to create Telephony Groups, Signaling Groups, and Recording Groups'. Below the description is a table with two columns: 'Name' and 'Type'. The table has one row with 'Avaya CM' in the 'Name' column and 'Avaya Communication Manager' in the 'Type' column. Below the table is a form with two fields: 'TELEPHONY GROUP NAME' and 'TELEPHONY GROUP PLATFORM TYPE'. The 'TELEPHONY GROUP NAME' field has a label 'Enter a unique name for the group.' and a text input field containing 'AvayaCM'. The 'TELEPHONY GROUP PLATFORM TYPE' field has a label 'Select the type of platform for this telephony group' and a dropdown menu with 'Avaya Communication Manager' selected. At the bottom of the form 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 previous section.
- Select a **DEVICE SYNCHRONIZATION DATA SERVER**. This Data Server was pre-configured.

The screenshot shows the 'Telephony Groups' configuration page in the CALABRIO system. The page has a red header bar with navigation links: Recordings, Contact Queue, Schedules and Planning, Messaging, Analytics, and Agent Explorer. A user greeting 'Hello, Tena' is visible in the top right. On the left, a 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' and several configuration options: 'DEVICE PASSWORD' with radio buttons for 'Use Device Extension', 'Use Static Password' (selected), and 'Use Custom Pattern'; a password input field with four dots; 'ASSOCIATED AVAYA ACD' with a dropdown menu showing 'Avaya (ACD ID: 5)'; an unchecked 'Enable Free Seating' checkbox; 'RECORDING SKILL HUNT GROUP' with a text input for 'Extension'; and 'DEVICE SYNCHRONIZATION DATA SERVER' with a dropdown menu showing '10.33.1.64'. 'Save' and 'Delete' buttons are located at the top right of the configuration area.

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 as shown in **Section 6.4**.

The screenshot shows the 'Telephony Groups' configuration page. The 'Application Enablement Services Information' section contains the following fields and options:

- SWITCH CONNECTION NAME**: interopcm
- HOSTNAME / IP ADDRESS**: 10.33.1.4
- PORT**: 4721
- ☐ Use Secure Connection

The 'User Credentials' section contains:

- USER NAME**: calabrio
- PASSWORD**: (masked with dots)

At the bottom, there is a message: 'This saves the changes to this server. Use the save above to save the whole form.' and buttons for '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 page with the 'Signaling' tab selected. The 'Signaling Groups' section contains a table with the following data:

Name	Telephony Group
SG 1	Avaya CM

Below the table is an empty input field for adding a new signaling group. The 'Previous' and 'Next' buttons are visible at the top right of the section.

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

Telephony Groups

Save Delete Cancel

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

Telephony Groups

✓ Telephony Groups

✓ Signaling Groups

✓ Recording Groups

Telephony Groups

Save Delete Cancel

1. Telephony

2. Signaling

3. Recording

Previous Next

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

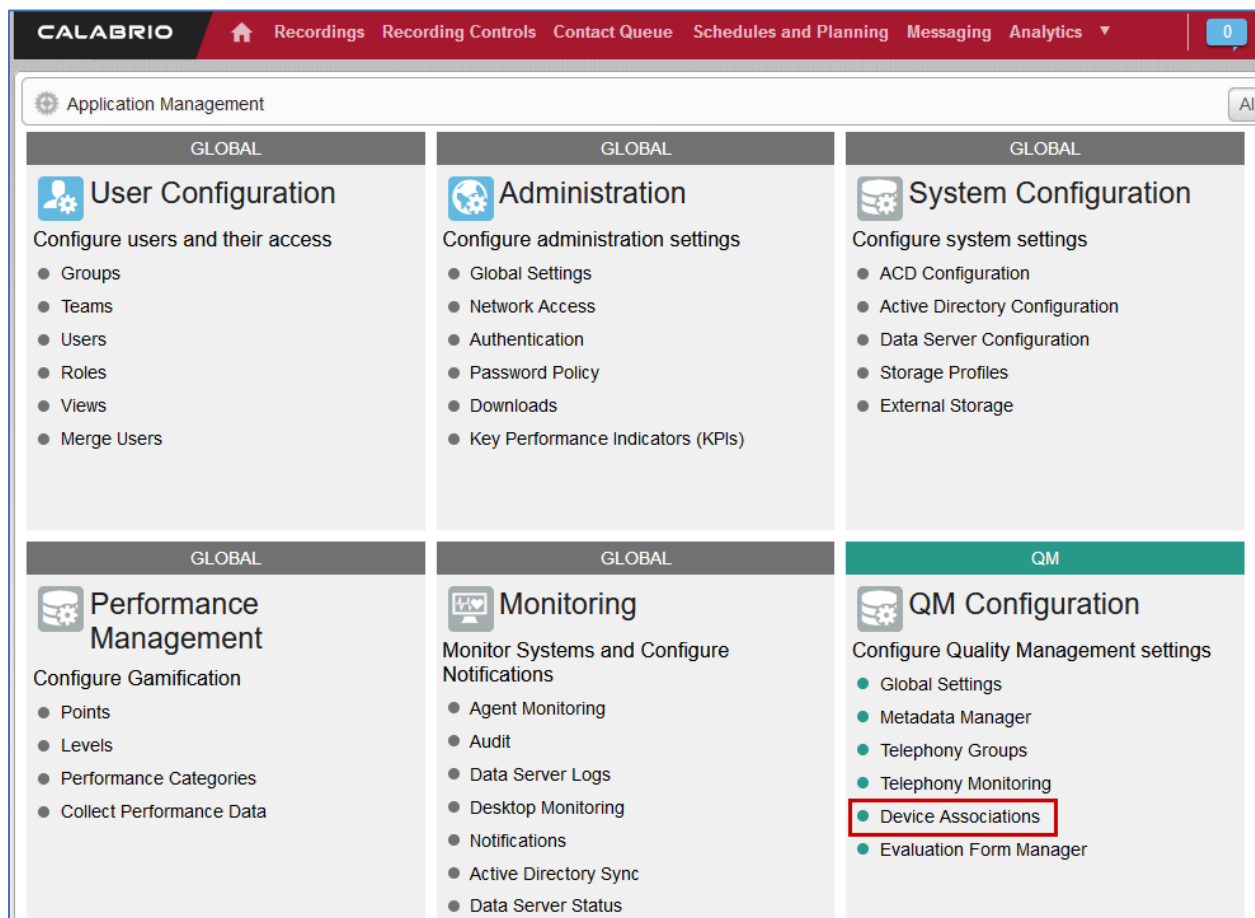
Add Update Delete Reset Recording Group

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. 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>										
<div>Device Associations</div> <div>Associate devices from your ACD with users, recording groups, and recording types</div> <div> CANCEL SAVE </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	Signaling 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 covers the steps that can be performed to verify the proper configuration of Application Enablement Services, Communication Manager, and Calabrio One.

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.

The screenshot shows the 'DMCC Service Summary - Session Summary' page. The left sidebar contains a navigation menu with 'Status' selected. The main content area displays session summary statistics and a table of active sessions.

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Fri Sep 24 03:42:16 MDT 2021

Service Uptime: 27 days, 23 hours 18 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 13

Number of Existing Devices: 15

Number of Devices Created Since Service Boot: 10520

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	C2954098AD4C1F951 4053094FD1717DE-48	calabrio	cmapiApplication	10.33.1.64	XML Unencrypted	15

[Terminate Sessions](#) [Show Terminated Sessions](#)

Item 1-1 of 1
1 Go

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	
Station	Ext	CTI		CTI		CTI		CTI		CTI		CTI		CTI		CTI	
		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														

8.1. Verify Calabrio One

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

CALABRIO							
Recordings Contact Queue Schedules and Planning Messaging Analytics Agent Explorer Reporting Data Explorer							
Recordings							
(1) Active		AQP: 0%, ATT: 00:03:28 Results per page 40 1-40 of 68					
Contact ID	Last Name	First Name	Group Name	Team Name	Calling Number	Called Number	
164	Agent 1002	Agent 1002	Default Group	Default Team	4305	3401	
163	Agent 1002	Agent 1002	Default Group	Default Team	3401	4305	
162	VP Agent 1	VP Agent 1	Default Group	Default Team	3311	3302	
161	Agent 1001	Agent 1001	Default Group	Default Team	3311	3302	
160	Agent 1000	Agent 1000	Default Group	Default Team	6139675085	5872330371	
159	Agent 1002	Agent 1002	Default Group	Default Team	3402	3401	
158	Agent 1003	Agent 1003	Default Group	Default Team	6139675085	3402	
157	Agent 1002	Agent 1002	Default Group	Default Team	3301	3401	
156	Agent 1000	Agent 1000	Default Group	Default Team	6139675085	5872330371	
155	Agent 1000	Agent 1000	Default Group	Default Team	3402	3301	
154	Agent 1003	Agent 1003	Default Group	Default Team	6139675085	3402	
153	Agent 1003	Agent 1003	Default Group	Default Team	3402	3340	
152	Agent 1000	Agent 1000	Default Group	Default Team	4305	3301	
151	Agent 1003	Agent 1003	Default Group	Default Team	4305	3402	
150	Agent 1003	Agent 1003	Default Group	Default Team	6139675189	3402	

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

CALABRIO

Recordings Contact Queue Schedules and Planning Messaging Analytics Agent Explorer Reporting

Hello, Tenant Help

Contact 155 Agent 1000 Agent 1000 09/12/2021 11:02 PM

1x 00:00 / 01:15

Details

(2) Associated Contacts

Contact Information

Contact

Contact ID 155

Calling Number 3402

Called Number 3301

Call Duration 00:01:15

Reason Archive

HR No

Training No

State Unscored

Audio

00:00

Evaluation

Choose Evaluation

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 8.1.x, Issue 12, July 2021.
- [2] Administering Avaya Aura® Session Manager, Release 8.1.x, Issue 10, September 2021.
- [3] Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 11, June 2021

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

©2021 Avaya Inc. All Rights Reserved.

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

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