



## DevConnect Program

---

# Application Notes for CallCabinet SSC Recorder with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required to integrate CallCabinet SSC Recorder 3.0.1.5 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 using Single Step Conference. CallCabinet SSC Recorder is a cloud-based call recording solution.

In this compliance test, CallCabinet SSC Recorder used the Device, Media, and Call Control interface of Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager and used the Single Step Conference method to capture media associated with the monitored agent stations for stereo call recording. The solution supports both mono and stereo call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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.

# 1. Introduction

These Application Notes describe the configuration steps required to integrate CallCabinet SSC Recorder with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference. CallCabinet SSC Recorder is a cloud-based call recording solution.

In this compliance test, CallCabinet SSC Recorder used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager and used the Single Step Conference method to capture media associated with the monitored agent stations for stereo call recording. Stereo call recording is suited for analytics, speech recognition, and transcription applications. The solution supports both mono and stereo call recording.

CallCabinet SSC Recorder is comprised of two applications, the SSC Recorder and the RTP Recorder. When there is an active call at the monitored agent station, SSC Recorder application is informed of the call via event reports from the DMCC interface using an encrypted DMCC link. SSC Recorder starts the stereo call recording(s) by using the Single Step Conference method to add a virtual IP softphone to the active call at the agent to obtain the media. The event reports are also used to determine when to stop the call recordings. The RTP Recorder applications captures the SRTP audio and uploads it to the cloud. Per design, the audio of all active calls on a monitored agent station are captured in the same call recording. The CallCabinet SSC Recorder Portal allows play back of all call recordings logged with call details, such as time, duration, calling and called party, agent ID, queue ID, and more.

In these Application Notes, SSC Recorder refers to the complete call recording solution, not simply the SSC Recorder application mentioned above, unless otherwise specified.

## 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on SSC Recorder using DMCC to perform device queries, monitor skill groups and agent stations, register the virtual IP softphones, and use Single Step Conference for call recordings. Each call to an agent station was recorded in stereo and stored in the cloud and the SSC Recorder Portal allowed the call recordings to be played back. Various call scenarios, such as hold/resume, call transfers, and conferences were exercised to verify proper call recording.

Test verification also included the use of Application Enablement Services and SSC Recorder logs to verify the message exchanges and the use of SSC Recorder Portal to verify the proper logging and playback of calls.

The serviceability testing focused on verifying that SSC Recorder returned to service after busyout and releasing the CTI link between Communication Manager and Application Enablement Services and restarting the DMCC and TSAPI services on Application Enablement Services.

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 CallCabinet SSC Recorder utilized encrypted DMCC and SRTP.

## **2.1. Interoperability Compliance Testing**

Interoperability compliance testing covered the following features and functionality:

- Use of DMCC to monitor skill groups and agent stations, register virtual IP softphones, and activate Single Step Conference.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, forwarding, service observing, auto answer, RONA, long duration, multiple calls, multiple agents, conference, and transfer. The solution supports both G.711 and G.729 for RTP and G.711 for SRTP.
- The use of an encrypted DMCC link between Application Enablement Services and SSC Recorder and stereo call recordings using SRTP. The solution supports both mono and stereo recording.

The serviceability testing focused on verifying the ability of SSC Recorder to recover from adverse conditions, such as restarting the CTI link and the DMCC and TSAPI services on Application Enablement Services.

## **2.2. Test Results**

All test cases passed with the following observation:

- The association of an agent station to Agent ID persists in the SSC Recorder Portal call listing after the agent has logged out.

- The Queue ID in the SSC Recorder Portal call listing shows the hunt group ID when the agent is logged into the ACD queue and is blank when the agent is logged out. The Queue ID is also blank when a direct call (i.e., non-ACD call) is placed to an agent station without the call being routed through a VDN or hunt group or for outgoing calls from an agent station.

## 2.3. Support

Technical support on CallCabinet SSC Recorder may be obtained through the following:

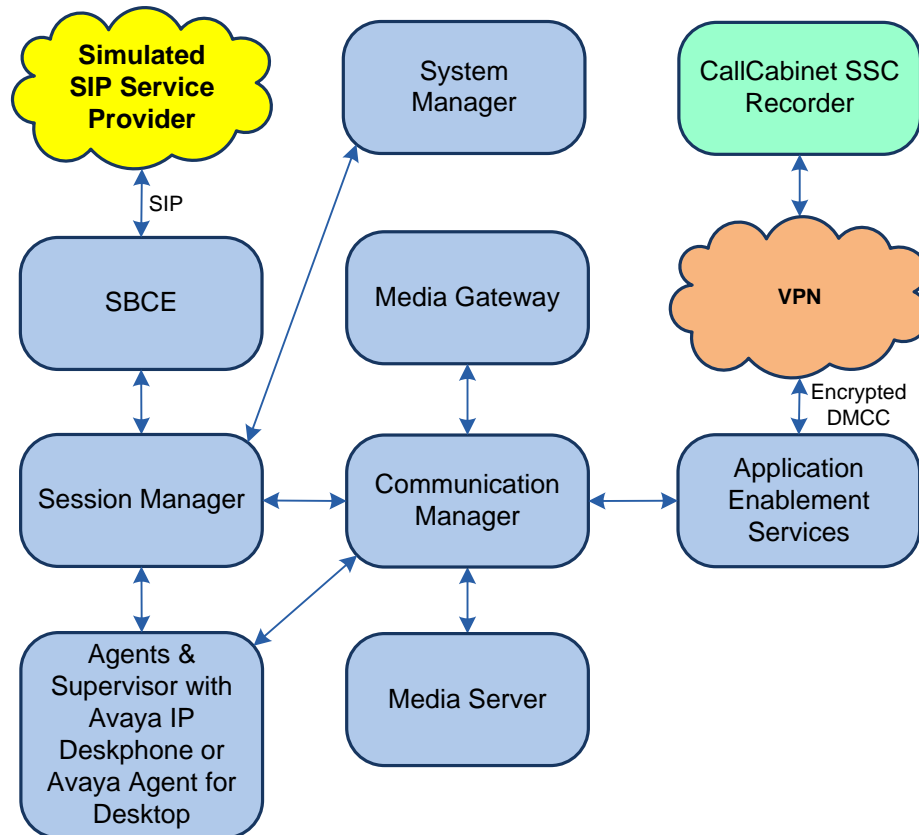
- **Phone:** (800) 653-1389
- **Web:** <https://support.callcabinet.com>

### 3. Reference Configuration

The configuration used for the compliance test is shown in **Figure 1**. The configuration consisted of a basic call center with a skill group and agent stations being monitored by SSC Recorder in the cloud using an encrypted DMCC link and recording two-way, SRTP audio of active calls on monitored agent stations in stereo. The SSC Recorder Portal allowed the logging and play back of call recordings.

In the compliance Test, SSC Recorder monitored skill groups and agent stations shown in the table below.

Device Type	Extension
Skill Group	77500
Agent Stations	77301 (H.323), 78004 (SIP)
Agent IDs	76301, 76302



**Figure 1: Avaya Aura® Call Center with CallCabinet SSC Recorder in the Cloud**

## 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	10.1.2.0.0-FP2
Avaya G430 Media Gateway	FW 42.8.0
Avaya G450 Media Gateway	FW 42.7.0
Avaya Aura® Media Server	10.1.0.77
Avaya Aura® Application Enablement Services	10.1.0.2.0.12-0)
Avaya Aura® System Manager	10.1.2.0 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.2.0.0-071476 Feature Pack 2
Avaya Aura® Session Manager	10.1.2.0.1012016
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series Deskphones	6.8.5.4.10 (H.323)
Avaya J100 Series Telephones	4.0.13.0.6 (SIP)
Avaya Agent for Desktop	2.0.6.25.3006 (SIP)
CallCabinet SSC Recorder	3.0.1.5

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer virtual IP softphones

**Note:** It is assumed that the configuration of a basic call center, including VDN, skill group, agent stations, and agent login IDs, is already in place and will not be covered in these application notes.

### 5.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on **Page 4**. If this option is not enabled, contact an authorized Avaya sales representative to make appropriate changes.

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	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
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	

### 5.2. Administer CTI Link

Add a CTI link using the **add cti-link** command. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page	1 of	3
CTI LINK				
CTI Link:	1			
<b>Extension:</b>	<b>77700</b>			
<b>Type:</b>	<b>ADJ-IP</b>			
<b>Name:</b>	<b>AES TSAPI Link</b>	COR:	1	
Unicode Name?	n			

### 5.3. Administer IP Codec Set

Use the **change ip-codec-set** command to access the **IP Codec Set** form to select the audio codec and media encryption for agents calls and call recording using virtual IP softphones. SSC Recorder supports G.711 with stereo call recording and SRTP using *1-srtp-aescm128-hmac80*. SSC Recorder also supports G.729 with RTP.

change ip-codec-set 1

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711MU	n	2	20
2:			
3:			
4:			
5:			
6:			
7:			

Media Encryption

Encrypted SRTCP: best-effort

1: 1-srtp-aescm128-hmac80

2: 2-srtp-aescm128-hmac32

3: none

4:

5:



## 5.4. Administer Virtual IP Softphones

Add a virtual IP softphone using the **add station** command. Enter the following values for the specified fields and retain the default values for the remaining fields. For the compliance test, eight virtual IP softphones were created with extensions 77951 to 77958. SSC Recorder registers two device instances per virtual IP softphone for stereo call recording and uses Single Step Conference to join one virtual IP softphone to an active call for call recording.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “9608”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”

add station 77951		Page 1 of 5
STATION		
<b>Extension:</b> 77951	Lock Messages? n	BCC: 0
<b>Type:</b> 9608	<b>Security Code:</b> 1234	TN: 1
Port: IP	Coverage Path 1:	COR: 1
<b>Name:</b> SSC Recorder DMCC 1	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: 77951	
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	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? Y	

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, eight virtual IP softphones were administered as shown below.

list station 77951 count 8									
Page 1									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COS	COR/ TN	
77951	S000057 9608	SSC Recorder	DMCC 1	no				1	
77952	S000059 9608	SSC Recorder	DMCC 2	no				1 1	
77953	S000060 9608	SSC Recorder	DMCC 3	no				1 1	
77954	S000061 9608	SSC Recorder	DMCC 4	no				1 1	
77955	S000062 9608	SSC Recorder	DMCC 5	no				1 1	
77956	S000063 9608	SSC Recorder	DMCC 6	no				1 1	
77957	S000064 9608	SSC Recorder	DMCC 7	no				1 1	
77958	S000064 9608	SSC Recorder	DMCC 8	no				1 1	

## 6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Switch Connection
- Administer SSC Recorder user
- Administer security database
- Administer ports
- Restart services

### 6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://<ip-address>” in an Internet browser window, where <ip-address> is the IP address of Application Enablement Services. The login screen is displayed. Log in using the appropriate credentials.



#### Application Enablement Services Management Console


[Help](#)

Please login here:

Username

Copyright © 2009-2022 Avaya Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 09:57:01 EDT 2023  
HA Status: Not Configured

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.

## 6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane to display the applicable WebLM server login screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 10:01:13 EDT 2023  
HA Status: Not Configured

Licensing | WebLM Server Access | Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▼ Licensing
  - WebLM Server Address
  - WebLM Server Access**
  - Reserved Licenses
- ▶ Maintenance
- ▶ Networking

### WebLM Server Access

WebLM Server Access helps you to access the WebLM server specified on the WebLM Server Address page.

- If you are using a local Avaya WebLM server, the AE Services management console redirects you to the Web License Manager page for WebLM configuration.
- If you are using a standalone WebLM server, you must manually log in to the WebLM server for WebLM configuration.

Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **Device Media and Call Control** and **TSAPI Simultaneous Users** as shown below. The DMCC license is used for the virtual IP softphones and the TSAPI license is used for device monitoring.

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

You are here: Licensed Products > Application\_Enablement > View License Capacity

License installed on: May 31, 2022 10:32:15 AM -04:00

**License File Host IDs:** V9-DF-31-89-CD-2A-01

**Licensed Features**

13 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000

Scrolling down to the **Acquired Licenses** section indicates that for eight virtual IP softphones used for stereo call recording, 16 DMCC licenses are used, and to monitor one skill group and two agent stations, three TSAPI licenses are used as shown below.

## Acquired Licenses

2 Items  Show <span>All ▼</span>			
Feature	Acquired by	Acquirer ID	Count
VALUE_AES_DMCC_DMC	DMCC (devcon-aes)	6392456460958976	16
VALUE_AES_TSAPI_USERS	TSAPI (devcon-aes)	devcon-aes:1681483417:2006978:139820032505984:0000	3

### 6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console** to administer a TSAPI link. The **TSAPI Links** screen is displayed as shown below. Click **Add Link**.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 10:03:02 EDT 2023  
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links

Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<a href="#">Add Link</a>	<a href="#">Edit Link</a>	<a href="#">Delete Link</a>		

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number.

For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection *devcon* is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

Retain the default value for **ASAI Link Version** and set **Security** to the desired value, in this case *Both* to allow for both encrypted and non-encrypted connections.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 10:12:43 EDT 2023  
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links

Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ TWS

Add TSAPI Links

Link

Switch Connection

Switch CTI Link Number

ASAI Link Version


Security

[Apply Changes](#) [Cancel Changes](#)

## 6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a list of existing switch connections.

Locate the connection name associated with relevant Communication Manager, in this case *devcon*, and select the corresponding radio button. Click **Edit Signaling Details**.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 10:14:12 EDT 2023  
HA Status: Not Configured

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"/> devcon	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit Signaling Details Delete Connection Survivability Hierarchy

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of Processor Ethernet on Communication Manager to use as H.323 gatekeeper for registering the virtual IP softphones, in this case *10.64.102.115* as shown below. Click **Add Name or IP**.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Thu Apr 27 12:49:03 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Thu Apr 27 14:26:18 EDT 2023  
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

▶ AE Services  
▼ Communication Manager Interface  
Switch Connections  
▶ Dial Plan  
High Availability  
▶ Licensing  
▶ Maintenance

Switch Connections

Edit H.323 Gatekeeper - devcon

Add Name or IP

Name or IP Address

☒ 10.64.102.115


Delete IP



## 6.5. Administer SSC Recorder User

Select **User Management** → **User Admin** → **Add User** from the left pane to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields.

 **Application Enablement Services**  
**Management Console**

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 10:15:57 EDT 2023  
HA Status: Not Configured

User Management | User Admin | Add UserHome | 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

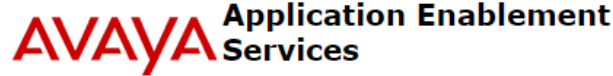
Fields marked with \* can not be empty.

* User Id	<input type="text" value="atmos"/>
* Common Name	<input type="text" value="atmos"/>
* Surname	<input type="text" value="atmos"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>

## 6.6. Administer Security Database

Select **Security → Security Database → Control** from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain that both parameters are unchecked, as shown below.

In the case that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the SSC Recorder user from **Section 6.5**.

**AVAYA** Application Enablement  
Services  
Management Console

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from  
192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 10:16:31 EDT 2023  
HA Status: Not Configured

Security | Security Database | Control

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

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services  
  
☐ Enable SDB for DMCC Service  
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services  
  
Apply Changes

## 6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Encrypted Port** under the **Enabled** column as shown below. Retain the default values in the remaining fields.

**AVAYA** Application Enablement Services  
Management Console

Welcome: User cust  
Last login: Thu Apr 27 12:49:03 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Thu Apr 27 13:43:18 EDT 2023  
HA Status: Not Configured

Networking | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

Enabled Disabled

☒ ☐

Enabled Disabled

☒ ☐

Enabled Disabled

☐ ☒


JAO; Reviewed:  
SPOC 6/3/2023

Avaya DevConnect Application Notes  
©2023 Avaya Inc. All Rights Reserved.

19 of 39  
CallCab-SSC-AES

## 6.8. Restart Services

Select **Maintenance** → **Service Controller** from the left pane to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service** and click **Restart Service**.

 **Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Fri Apr 14 09:18:50 2023 from 192.168.100.251  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 19 10:18:25 EDT 2023  
HA Status: Not Configured

**Maintenance | Service Controller**Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

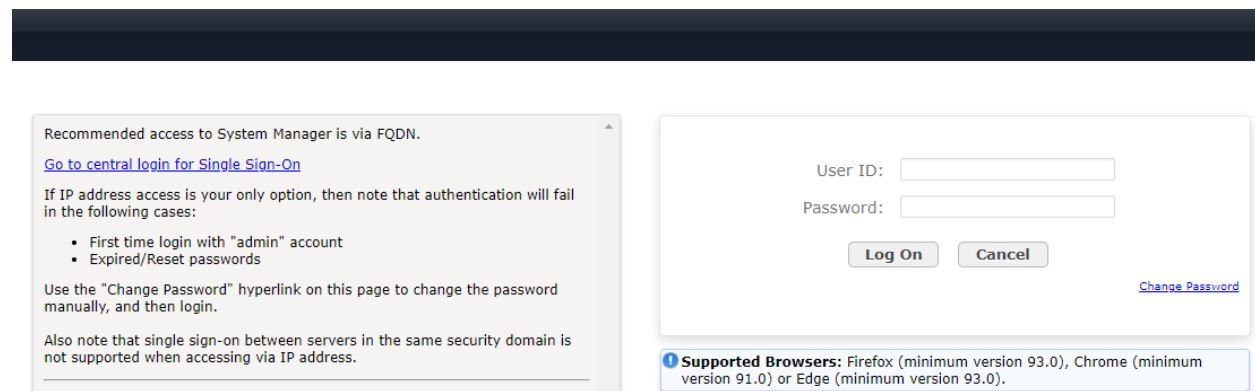
## 7. Configure Avaya Aura® Session Manager

This section covers the configuration of a SIP user on Session Manager so that Application Enablement Services can monitor the station. The SIP user is configured via the System Manager web interface. The procedure includes the following areas:

- Launch System Manager
- Administer SIP Users

### 7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://<ip-address>” in a web browser window, where <ip-address> is the System Manager IP address. Log in using the appropriate credentials.



Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

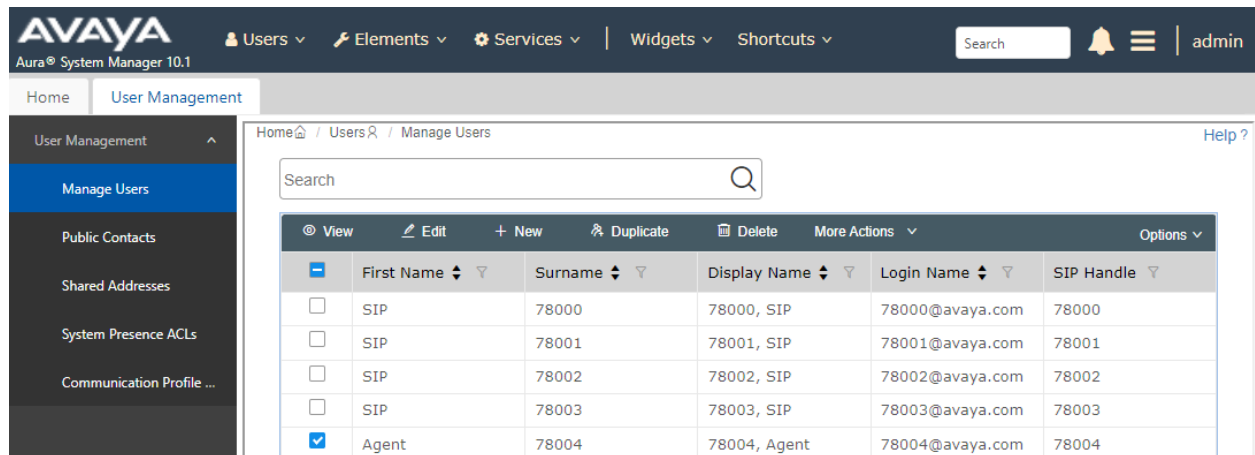
[Change Password](#)

**Supported Browsers:** Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

## 7.2. Administer SIP Users

In the subsequent screen (not shown), select **Users** → **User Management** from the top menu. Select **User Management** → **Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section 3**, in this case *78004*, and click **Edit**.



The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The left sidebar shows the 'User Management' menu with 'Manage Users' selected. The main content area, titled 'Home / Users / Manage Users', features a search bar and a table of users. The table has columns for selection, First Name, Surname, Display Name, Login Name, and SIP Handle. The user 'Agent' with SIP Handle '78004' is selected.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	78000	78000, SIP	78000@avaya.com	78000
<input type="checkbox"/>	SIP	78001	78001, SIP	78001@avaya.com	78001
<input type="checkbox"/>	SIP	78002	78002, SIP	78002@avaya.com	78002
<input type="checkbox"/>	SIP	78003	78003, SIP	78003@avaya.com	78003
<input checked="" type="checkbox"/>	Agent	78004	78004, Agent	78004@avaya.com	78004


The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section and click **Editor** as shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon (admin) are also present. The left sidebar shows the 'User Management' menu with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile ...'. The main content area is titled 'User Profile | Edit | 78004@avaya.com' and features tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section and a 'PROFILES' section with 'Session Manager Profile' and 'CM Endpoint Profile' (which is selected). The 'CM Endpoint Profile' section contains various fields: 'System' (devcon-cm), 'Profile Type' (Endpoint), 'Extension' (78004), 'Set Type' (J179CC), 'Port' (S000020), 'Preferred Handle' (Select), 'Sip Trunk' (aar), 'Security Code' (Enter Security Code), 'Voice Mail Number', 'Template' (Start typing...), 'Use Existing Endpoints' (checkbox), and 'Calculate Route Pattern' (checkbox). The 'Extension' field is highlighted with a red box and a blue 'E' icon.

Select the **General Options** tab. For **Type of 3PCC Enabled**, select *Avaya* as shown below.

Repeat this section for all SIP agent stations from **Section 5.4**. In the compliance test, eight SIP agent stations were configured.

System	devcon-cm	Extension	78004
Template	Select ▼	Set Type	J179CC 
Port	S000020	Security Code	
Name	78004, Agent		

<b>General Options (G) *</b>		Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)		Profile Settings (P)	Group Membership (M)		
* Class of Restriction (COR)	1	* Class Of Service (COS)	1		
* Emergency Location Ext	78004	* Message Lamp Ext.	78004		
* Tenant Number	1				
* SIP Trunk	Qaar	<b>Type of 3PCC Enabled</b>	Avaya ▼		
Coverage Path 1		Coverage Path 2			
Lock Message	<input type="checkbox"/>	Localized Display Name	78004, Agent		
Multibyte Language	Not Applicable ▼	Enable Reachability for Station Domain Control	system ▼		



## 8. Configure CallCabinet SSC Recorder

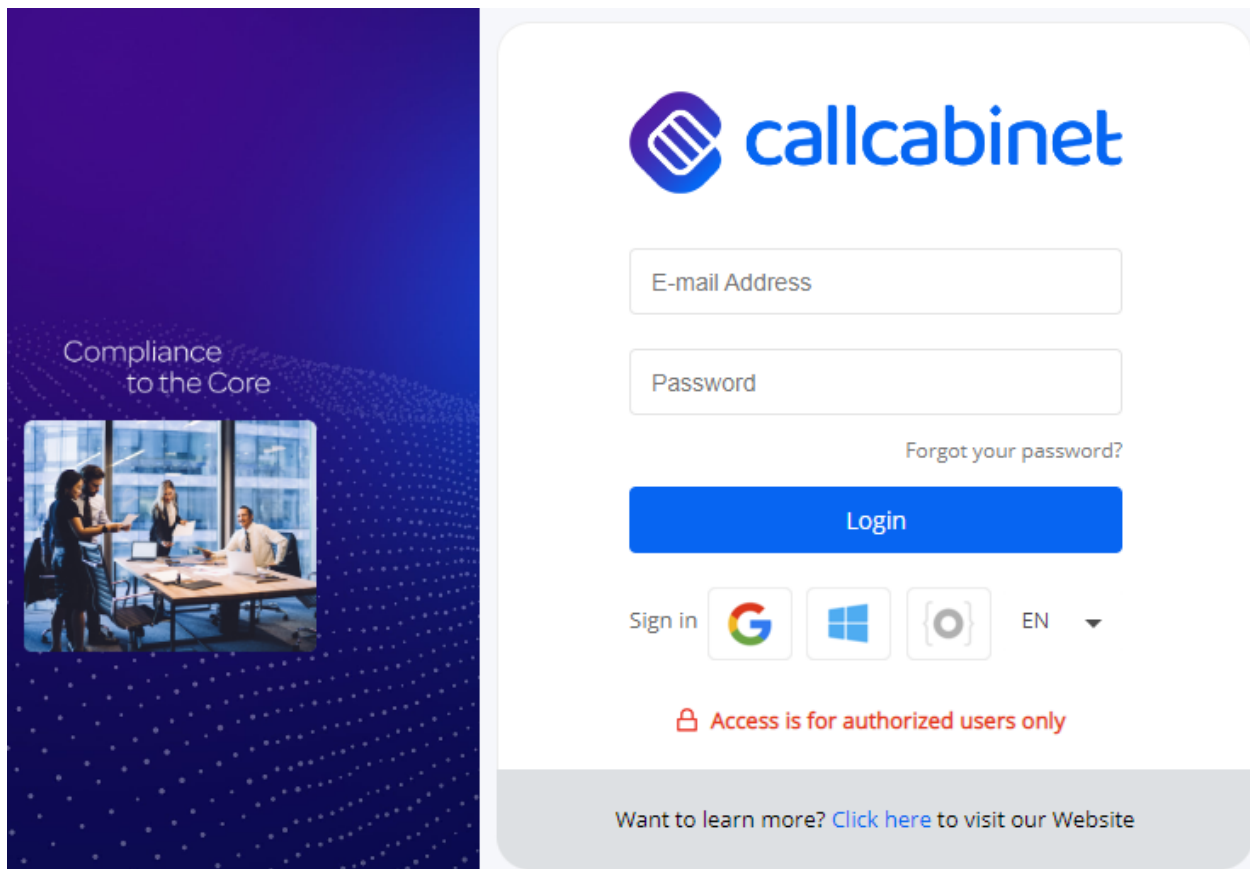
This section covers the configuration of CallCabinet SSC Recorder, which includes the SSC Recorder and RTP Recorder applications.

- Launch SSC Recorder Portal
- Obtain Customer ID and Site ID
- Configure SSC Recorder Application
- Configure RTP Recorder Application
- Install Trusted Certificate
- Start SSC Recorder Windows Services

The configuration of SSC Recorder is performed by CallCabinet personnel. The following configuration steps are presented for informational purposes only.

### 8.1. Launch SSC Recorder Portal

Access the SSC Recorder Portal by using the URL “<https://<company>.callcabinet.com>” in a web browser window, where <company> is the company URL. Log in using the appropriate credentials.



## 8.2. Obtain Customer ID and Site ID

Navigate to **Settings** → **Site Management** to retrieve the customer information, including the **Customer ID** and **Site ID** shown below. Click the icon to the right to copy the data to the clipboard. This information should be added to the RTP Recorder configuration covered in **Section 8.4**.

The screenshot displays the 'SITE MANAGEMENT' interface. At the top, there's a header with the Avaya logo, the title 'SITE MANAGEMENT', a dropdown menu set to 'Avaya Certification', and a user profile icon. A left sidebar contains various navigation icons. The main content area is titled 'CUSTOMER INFORMATION' and shows the following details:

- Customer Name:** Avaya Certification
- Customer ID:** bc52e108-bfa4-4cc6-8e0e-6b3019ad80f3 (with a copy icon)

Below this, there are three blue buttons: 'ADD NEW SITE', 'PROVISION MICROSOFT TEAMS' (with a Teams icon), and 'PROVISION ZOOM' (with a Zoom icon). A table below these buttons lists site information:

SITE ID	SITE NAME	
2f01a217-248a-4050-87a7-5e10035d5a53	Morristown	

At the bottom of the table, there's a pagination bar showing '1' of 20 items, '1 - 1 of 1 items', and a refresh icon. An 'Edit columns' button is located at the bottom right of the interface.

### 8.3. Configure SSC Recorder Application

The `app.xml` file for the SSC Recorder application, located in the `CallCabinet\CallCabinetSSCRecorder\bin\` directory, should be modified with the following parameter settings:

- **SwitchNameOrIP:** Set to Communication Manager **Switch Connection** name (e.g., *devcon*) from **Section 6.3**.
- **ServerID:** Set to Application Enablement Services IP address (e.g., *10.64.102.119*).
- **UserName:** Set to CT User configured in **Section 6.5**
- **Password:** Set to CT User password in **Section 6.5**.
- **DMCCPort:** Set to encrypted DMCC port (i.e., *4722*) shown in **Section 6.7**.
- **IsEncryptionEnable:** Set to *true* for encrypted DMCC.
- **AesEncryptionProtocol:** Set to *srtplib-aes128-hmac80*.
- **MediaCodec:** Set to *g711u*.
- **IP:** Set to IP address of SSC Recorder server.
- **Extensions:** Specify the agent stations and skill groups to monitor listed in **Section 3**.
- **Softphones:** Specify the virtual IP softphone extensions and passwords from **Section 5.4**. Note that there are two device instances for each virtual IP softphone to support stereo call recordings.

The SSC Recorder `app.xml` file used for the compliance test is displayed on the next page.

```

▼<CallCabinet_SSC>
  ▼<CM_DETAILS>
    <SwitchNameOrIP>devcon</SwitchNameOrIP>
  </CM_DETAILS>
  ▼<AES_DETAILS>
    <ServerID>10.64.102.119</ServerID>
    <UserName>atmos</UserName>
    <Password>Atmos123!</Password>
    <DMCCPort>4722</DMCCPort>
    <AesProtocol>http://www.ecma-international.org/standards/ecma-323/csta/ed3/privD</AesProtocol>
  </AES_DETAILS>
  ▼<SRTP_ENCRYPTION>
    <IsEncryptionEnable>true</IsEncryptionEnable>
    <AesEncryptionProtocol>srtplib-aescm128-hmac80</AesEncryptionProtocol>
    <MediaCodec>g711u</MediaCodec>
  </SRTP_ENCRYPTION>
  ▼<RECORDERS>
    <CRE Index="0" Name="" IP="192.168.120.45" CREIP="127.0.0.1" Port="1701"/>
  </RECORDERS>
  ▼<EXTENSIONS>
    <Ext>77301</Ext>
    <Ext>78004</Ext>
    <Ext>77500</Ext>
  </EXTENSIONS>
  ▼<CRE_CHANNELS>
    <CRE_CHANNEL Channel="0" CRE="0" Port="45000"/>
    <CRE_CHANNEL Channel="1" CRE="0" Port="45002"/>
    <CRE_CHANNEL Channel="2" CRE="0" Port="45004"/>
    <CRE_CHANNEL Channel="3" CRE="0" Port="45006"/>
    <CRE_CHANNEL Channel="4" CRE="0" Port="45008"/>
    <CRE_CHANNEL Channel="5" CRE="0" Port="45010"/>
    <CRE_CHANNEL Channel="6" CRE="0" Port="45012"/>
    <CRE_CHANNEL Channel="7" CRE="0" Port="45014"/>
    <CRE_CHANNEL Channel="8" CRE="0" Port="45016"/>
    <CRE_CHANNEL Channel="9" CRE="0" Port="45018"/>
    <CRE_CHANNEL Channel="10" CRE="0" Port="45020"/>
    <CRE_CHANNEL Channel="11" CRE="0" Port="45022"/>
    <CRE_CHANNEL Channel="12" CRE="0" Port="45024"/>
    <CRE_CHANNEL Channel="13" CRE="0" Port="45026"/>
    <CRE_CHANNEL Channel="14" CRE="0" Port="45028"/>
    <CRE_CHANNEL Channel="15" CRE="0" Port="45030"/>
    <CRE_CHANNEL Channel="16" CRE="0" Port="45032"/>
    <CRE_CHANNEL Channel="17" CRE="0" Port="45034"/>
    <CRE_CHANNEL Channel="18" CRE="0" Port="45036"/>
    <CRE_CHANNEL Channel="19" CRE="0" Port="45038"/>
    <CRE_CHANNEL Channel="20" CRE="0" Port="45040"/>
    <CRE_CHANNEL Channel="21" CRE="0" Port="45042"/>
    <CRE_CHANNEL Channel="22" CRE="0" Port="45044"/>
    <CRE_CHANNEL Channel="23" CRE="0" Port="45046"/>
    <CRE_CHANNEL Channel="24" CRE="0" Port="45048"/>
    <CRE_CHANNEL Channel="25" CRE="0" Port="45050"/>
  </CRE_CHANNELS>
  ▼<SOFTPHONES>
    <SOFTPHONE Extension="77951" Password="1234" CRE_CHANNEL="0" DeviceInstance="0"/>
    <SOFTPHONE Extension="77951" Password="1234" CRE_CHANNEL="1" DeviceInstance="1"/>
    <SOFTPHONE Extension="77952" Password="1234" CRE_CHANNEL="2" DeviceInstance="0"/>
    <SOFTPHONE Extension="77952" Password="1234" CRE_CHANNEL="3" DeviceInstance="1"/>
    <SOFTPHONE Extension="77953" Password="1234" CRE_CHANNEL="4" DeviceInstance="0"/>
    <SOFTPHONE Extension="77953" Password="1234" CRE_CHANNEL="5" DeviceInstance="1"/>
    <SOFTPHONE Extension="77954" Password="1234" CRE_CHANNEL="6" DeviceInstance="0"/>
    <SOFTPHONE Extension="77954" Password="1234" CRE_CHANNEL="7" DeviceInstance="1"/>
    <SOFTPHONE Extension="77955" Password="1234" CRE_CHANNEL="8" DeviceInstance="0"/>
    <SOFTPHONE Extension="77955" Password="1234" CRE_CHANNEL="9" DeviceInstance="1"/>
    <SOFTPHONE Extension="77956" Password="1234" CRE_CHANNEL="10" DeviceInstance="0"/>
    <SOFTPHONE Extension="77956" Password="1234" CRE_CHANNEL="11" DeviceInstance="1"/>
    <SOFTPHONE Extension="77957" Password="1234" CRE_CHANNEL="12" DeviceInstance="0"/>
    <SOFTPHONE Extension="77957" Password="1234" CRE_CHANNEL="13" DeviceInstance="1"/>
    <SOFTPHONE Extension="77958" Password="1234" CRE_CHANNEL="14" DeviceInstance="0"/>
    <SOFTPHONE Extension="77958" Password="1234" CRE_CHANNEL="15" DeviceInstance="1"/>
  </SOFTPHONES>
</CallCabinet_SSC>

```

## 8.4. Configure RTP Recorder Application

The app.xml file for the RTP Recorder application, located in the CallCabinet\CallCabinetRTPRecorder\bin\ directory, should be modified with the following parameter settings:

<b>AudioFileFormat:</b>	Specify <i>STEREO</i> for stereo call recording. <i>MONO</i> for mono call recording is also supported.
<b>ClientID:</b>	Set to <b>Customer ID</b> from <b>Section 8.2</b> .
<b>SiteID:</b>	Set to <b>Site ID</b> from <b>Section 8.2</b> .
<b>RecordingCallDirection:</b>	Set to <i>B</i> for recording audio in both directions.

The RTP Recorder app.xml file used for the compliance test is displayed below.

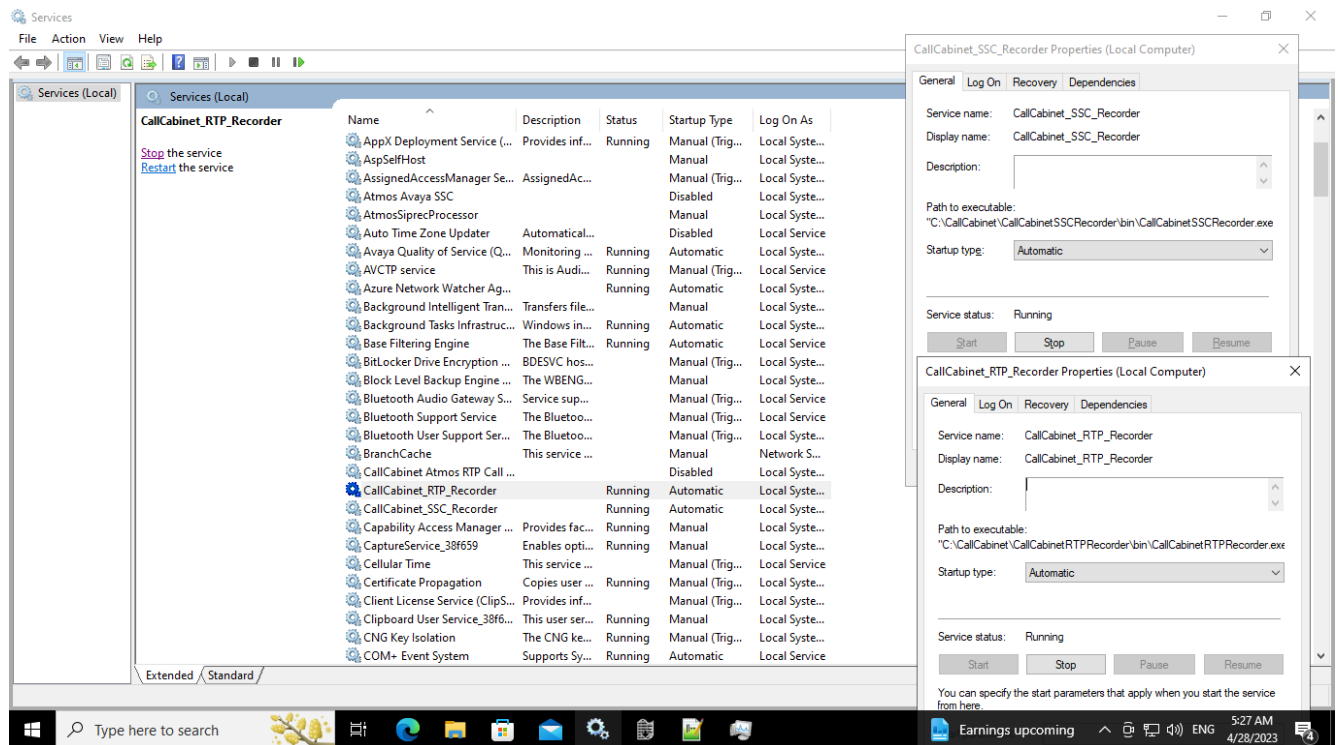
```
▼<CallCabinetConfig>
  ▼<app>
    <AudiofileFormat>STEREO</AudiofileFormat>
    <StoragePath>C:\CallCabinet\CallCabinetRTPRecorder\temp\</StoragePath>
    <NetworkAdapter>\Device\NPF_{8099E182-4C6A-4153-9CF8-8D17FBD78F49}</NetworkAdapter>
    <Port>1701</Port>
    <AudioRepository>C:\CallCabinet\CallCabinetRTPRecorder\from\</AudioRepository>
    <ReprocessDirPath>C:\CallCabinet\CallCabinetRTPRecorder\Reprocess\</ReprocessDirPath>
    <ReprocessIntervalInMinute>10</ReprocessIntervalInMinute>
    <CustomizationType>0</CustomizationType>
    <!-- For Certification -->
    <ClientID>bc52e108-bfa4-4cc6-8e0e-6b3019ad80f3</ClientID>
    <SiteID>2f01a217-248a-4050-87a7-5e10035d5a53</SiteID>
    <RecordingCallDirection>B</RecordingCallDirection>
    <Sftp_Upload>false</Sftp_Upload>
    <Sftp_Ip>[REDACTED]</Sftp_Ip>
    <Sftp_Port>22</Sftp_Port>
    <Sftp_UserName>[REDACTED]</Sftp_UserName>
    <Sftp_Password>[REDACTED]</Sftp_Password>
  </app>
</CallCabinetConfig>
```

## 8.5. Install Trusted Certificate

For encrypted DMCC link and SRTP support, install the trusted CA certificate used by Application Enablement Services and agent IP stations on the SSC Recorder windows server using Microsoft Management Console (MMC). Avaya Aura® System Manager was used as the certificate authority.

## 8.6. Start SSC Recorder Windows Services

Verify that the following SSC Recorder services, CallCabinet\_SSC\_Recorder and CallCabinet\_RTP\_Recorder, have been started in Windows Services as shown below.



## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and SSC Recorder.

### 9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is *established* for the CTI link number administered in **Section 5.2** as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	devcon-aes	established	895	370

Verify registration status of the virtual IP softphones by using the **list registered-ip-stations** command. Verify that all virtual IP softphones from **Section 5.4** are displayed along with the IP address of the Application Enablement Services server as shown below. Note that for stereo call recording two instances of each virtual IP softphone are registered.

```
list registered-ip-stations ext 77951 count 8
```

Page 1

REGISTERED IP STATIONS			
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
77951	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77951	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77952	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77952	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77953	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77953	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77954	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77954	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115

```
list registered-ip-stations ext 77951 count 8
```

REGISTERED IP STATIONS

Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
77955	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77955	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77956	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77956	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77957	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77957	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77958	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115
77958	9608	IP_API_A	10.64.102.119
tcp	1	3.2040	10.64.102.115

Establish a call with a monitored station and verify the status of the virtual IP softphone using the **status station** command. Verify that the **Service State** is *in-service/off-hook* on **Page 1**.

status station 77955	Page 1 of 10
GENERAL STATUS	
Administered Type: 9608	Service State: <b>in-service/off-hook</b>
Connected Type: N/A	Signal Status: connected
Extension: 77955	Network Region: 1
Port: S000062	Parameter Download: pending
Call Parked? no	SAC Activated? no
Ring Cut Off Act? no	
Active Coverage Option: 1	
EC500 Status: N/A	
Message Waiting:	
Connected Ports: S000207	S000058 T000062
Limit Incoming Calls? no	
User Cntrl Restr: none	
Group Cntrl Restr: none	
CTI Monitoring Active? Yes	



On **Page 5**, verify that the codec used is G.711 as shown below.

status station 77955

Page5 of 10

AUDIO CHANNEL Port: S000062

G.711MU

Switch-End Audio Location: AMS1

IP Address	Port	Node Name	Rgn
Other-End: 10.64.102.118	6138	devcon-ams	1
Set-End: 192.168.120.30	45016		1

Audio Connection Type: ip-tdm

AUDIO CHANNEL Shared Port: S000207

G.711MU

Switch-End Audio Location: AMS1

IP Address	Port	Node Name	Rgn
Other-End: 10.64.102.118	6140	devcon-ams	1
Set-End: 10.64.102.119	45018	devcon-aes	1

Audio Connection Type: ip-tdm

Switch-End Audio Location:

On **Page 7** and subsequent pages (not shown), verify that SRTP is used as shown below.


status station 77955		Page 7 of 10	
SRC PORT TO DEST PORT TALKPATH			
src port: S000062			
S000062:TX:192.168.120.30:45016/g711u/20ms/1-srtp-aescm128-hmac80			
AMS1:RX:10.64.102.118:6138/g711u/20ms/1-srtp-aescm128-h:TX:cnfID:1f0000100000006e			
AMS1:RX:cnfID:1f0000100000006e:TX:10.64.102.118:6140/g711u/20ms/1-srtp-aescm128-h			
S000207:RX:192.168.120.30:45018/g711u/20ms/1-srtp-aescm128-hmac80			

Terminate the call and verify that the **Service State** of the virtual IP softphone returns to *in-service/on-hook*. Call recordings are verified in **Section 9.3**.

## 9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the DMCC service by selecting **Status** → **Status and Control** → **DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify that the **User** column shows an active session with the SSC Recorder username from **Section 6.5**, that the **Connection Type** is encrypted, and that the number **# of Associated Devices** reflects the number of virtual IP softphones. For stereo call recording, two device instances per virtual IP softphone is used so the **# of Associated Devices** is *16*.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Wed Apr 26 09:23:12 2023 from 192.168.100.250  
Number of prior failed login attempts: 0  
HostName/IP: devcon-aes/10.64.102.119  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.2.0.12-0  
Server Date and Time: Wed Apr 26 10:24:56 EDT 2023  
HA Status: Not Configured

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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Wed Apr 26 10:24:46 EDT 2023

Service Uptime: 11 days, 23 hours 41 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 28

Number of Existing Devices: 16

Number of Devices Created Since Service Boot: 330

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	E575506F3A4F128D0 1A7B5013E2B8388-27	atmos	AtmosAvayaSSC	192.168.120.30	XML Encrypted	16

Terminate Sessions Show Terminated Sessions

Item 1-1 of 1

1 Go

Click on the **Session ID** in the screen on previous page to display the devices associated with the session.

#### DMCC Service Summary - Session Detail

☐ Enable page refresh every  seconds

##### Detailed Session View

Generated on Thu Apr 27 13:13:27 EDT 2023

Session ID: D83D94A7FAA8D23A2AD57D802E56FD42-44

State: Active

Time Established: Thu, Apr 27, 2023 10:32:13 AM GMT-05:00

Uptime: 0 days, 2 hours, 41 minutes, and 13 seconds

Cleanup Delay Timer: 5 seconds

Session Duration Timer: 180 seconds

Time of Most Recent Timer Reset: Thu, Apr 27, 2023 01:13:22 PM EDT

Reconnect Counter: 0

[Terminate Sessions](#)

##### Devices Associated with Session


<input type="checkbox"/>	Device ID	State
<input type="checkbox"/>	77953:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77953:devcon:0.0.0.0:0	REGISTERED
<input type="checkbox"/>	77958:devcon:0.0.0.0:0	REGISTERED
<input type="checkbox"/>	77958:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77955:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77955:devcon:0.0.0.0:0	REGISTERED
<input type="checkbox"/>	77956:devcon:0.0.0.0:0	REGISTERED
<input type="checkbox"/>	77952:devcon:0.0.0.0:0	REGISTERED
<input type="checkbox"/>	77954:devcon:0.0.0.0:0	REGISTERED
<input type="checkbox"/>	77957:devcon:0.0.0.0:0	REGISTERED
<input type="checkbox"/>	77952:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77957:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77954:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77956:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77951:devcon:0.0.0.0:1	REGISTERED
<input type="checkbox"/>	77951:devcon:0.0.0.0:0	REGISTERED

[Terminate Selected Devices](#) [Back](#)

Item 1-16 of 16

Verify status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is **Talking** for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**, in this case 3.



**Application Enablement Services**  
 Management Console

Welcome: User cust  
 Last login: Thu Apr 27 09:41:29 2023 from 192.168.100.250  
 Number of prior failed login attempts: 0  
 HostName/IP: devcon-aes/10.64.102.119  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 10.1.0.2.0.12-0  
 Server Date and Time: Thu Apr 27 13:12:54 EDT 2023  
 HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary
Home | 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**

### TSAPI Link Details

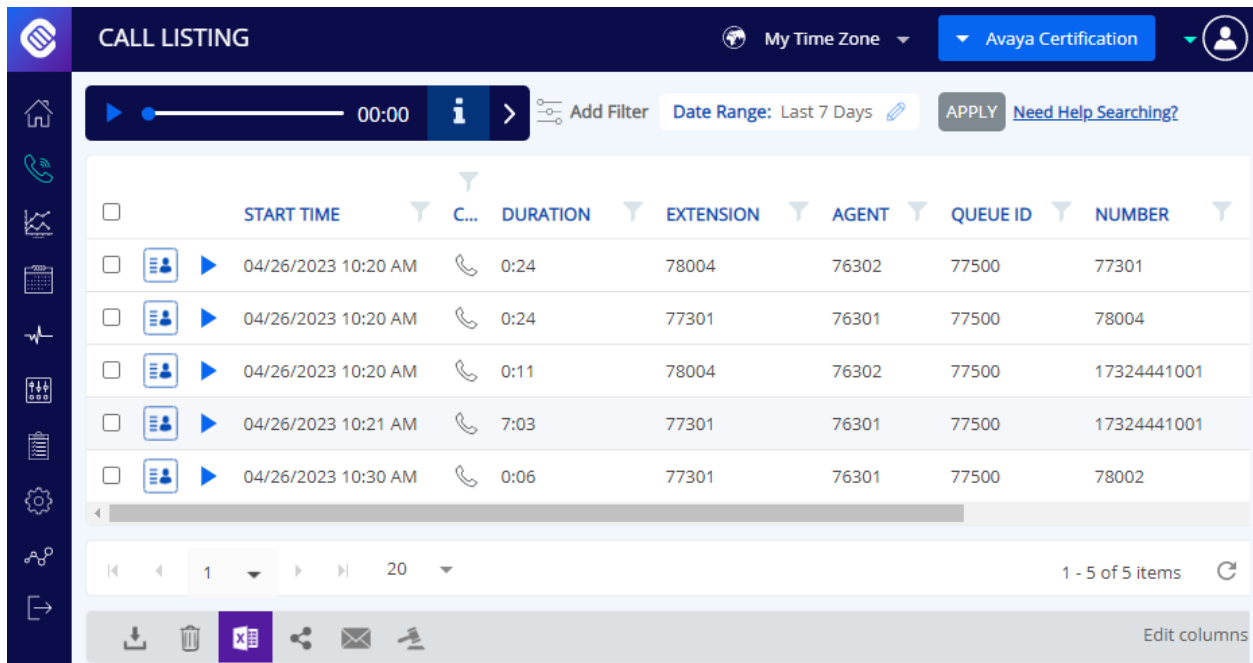
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	devcon	1	Talking	Wed Apr 26 09:56:39 2023	Online	20	3	24	24	30

For service-wide information, choose one of the following:

### 9.3. Verify CallCabinet SSC Recorder

Log in an agent to handle and complete an ACD call. Access the SSC Recorder Portal as described in **Section 8.1** and log in using the appropriate credentials. Navigate to **Call Listing** to view a listing of call recordings. Verify that there is an entry for the last call with proper values in the relevant fields as shown below. Verify that the recording can be played back.



The screenshot displays the 'CALL LISTING' interface. At the top, there's a header with a logo, 'CALL LISTING', 'My Time Zone', 'Avaya Certification', and a user profile icon. Below the header is a toolbar with a play button, a progress bar at 00:00, an information icon, and an 'Add Filter' button. A 'Date Range' dropdown is set to 'Last 7 Days', with an 'APPLY' button and a 'Need Help Searching?' link. The main area contains a table with columns: START TIME, C... (likely Call ID), DURATION, EXTENSION, AGENT, QUEUE ID, and NUMBER. The table lists six call entries. The bottom of the interface shows a pagination bar with '1' selected out of 20 items, and a footer with icons for download, delete, export, share, email, and print, along with an 'Edit columns' link.

	START TIME	C...	DURATION	EXTENSION	AGENT	QUEUE ID	NUMBER
<input type="checkbox"/>	04/26/2023 10:20 AM		0:24	78004	76302	77500	77301
<input type="checkbox"/>	04/26/2023 10:20 AM		0:24	77301	76301	77500	78004
<input type="checkbox"/>	04/26/2023 10:20 AM		0:11	78004	76302	77500	17324441001
<input type="checkbox"/>	04/26/2023 10:21 AM		7:03	77301	76301	77500	17324441001
<input type="checkbox"/>	04/26/2023 10:30 AM		0:06	77301	76301	77500	78002

## 10. Conclusion

These Application Notes describe the configuration steps required to integrate CallCabinet SSC Recorder with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference. Stereo call recordings were logged and played back successfully. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

## 11. Additional References

This section references the Avaya and CallCabinet documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 2, September 2022, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 5, September 2022, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 4, September 2022, available at <http://support.avaya.com>.
- [4] *Avaya Aura® AE Services Device, Media, and Call Control .NET API Programmer's Guide*, Release 8.x – 10.x, Aug 2022.
- [5] *CallCabinet Atmos User Guide*, available at <https://www.callcabinet.com/atmos-user-guide/>.

---

**©2023 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](mailto:devconnect@avaya.com).