



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for HigherGround Calibre 9.2022 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 using Single Step Conference – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for HigherGround Calibre 9.2022 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 using Single Step Conference. HigherGround Calibre is a call recording solution.

In the compliance testing, HigherGround Calibre used the Device, Media, and Call Control 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 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 at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required for HigherGround Calibre 9.2022 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 using Single Step Conference. Calibre is a call recording solution.

In the compliance testing, Calibre used the Device, Media, and Call Control (DMCC) .NET interface from Application Enablement Services to monitor skill groups and agent stations on Communication Manager and used the Single Step Conference method to capture media associated with the monitored agent stations for call recording.

When there is an active call at the monitored agent station, Calibre is informed of the call via event reports from the DMCC interface. Calibre starts the call recording 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.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Calibre, the application used DMCC to automatically perform device queries, monitor skill groups and agent stations, and register the virtual IP softphones.

For the manual part of testing, each call was handled manually on the agent station with generation of unique audio content for recording. Necessary user actions such as hold and resume were performed from the agent station to test various call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Calibre.

The verification of tests included use of Application Enablement Services and Calibre logs for proper message exchanges and use of Calibre web interface for proper logging and playback of calls.

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 Calibre did not include use of any specific encryption features as requested by HigherGround.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Calibre:

- 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 serviceability testing focused on verifying the ability of Calibre to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Calibre.

## 2.2. Test Results

All test cases were executed, and the following were observations on Calibre:

- By design, the default Calibre setting ends an active recording upon agent placing the call on hold and starts a new recording upon agent resuming the call. This behavior is controlled by the RecordThroughHold system parameter and is configurable. The compliance testing used the default value of zero for the parameter.
- Calibre only supports the G.711 codec variants in this integration.

## 2.3. Support

Technical support on Calibre can be obtained through the following:

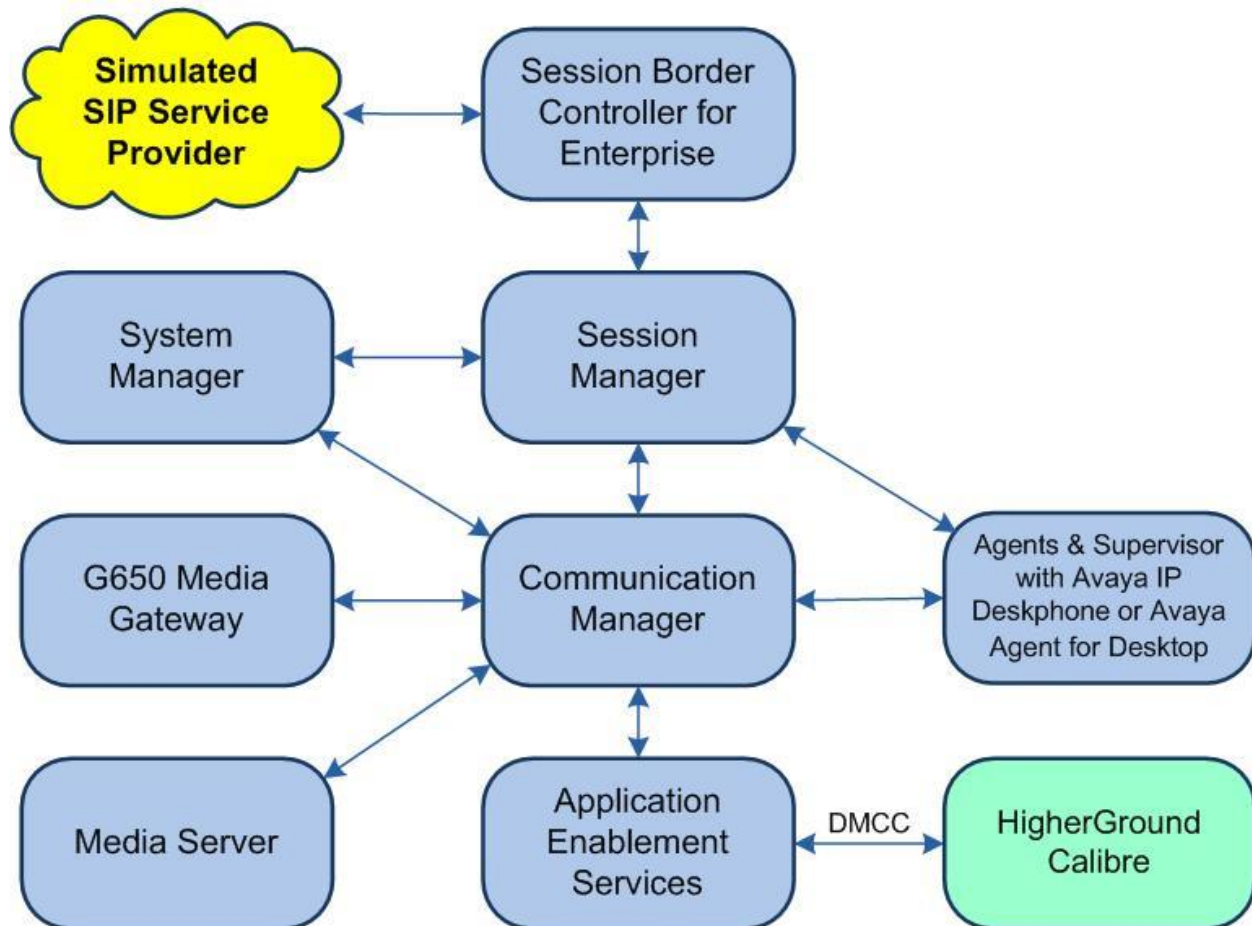
- **Phone:** (818) 456-1600
- **Email:** [support@higherground.com](mailto:support@higherground.com)

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Calibre monitored skill groups and agent stations shown in the table below.

Device Type	Extension
Skill Group	61001, 61002
Agent Station	65001 (H.323), 66002 (SIP)
Agent ID	65881, 65882



**Figure 1: Compliance Testing Configuration**

## 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 in Virtual Environment	10.1 (10.1.0.1.0.974.27372)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1.0.77
Avaya Aura® Application Enablement Services in Virtual Environment	10.1 (10.1.0.1.0.7-0)
Avaya Aura® Session Manager in Virtual Environment	10.1.0.1 (10.1.0.1.1010105)
Avaya Aura® System Manager in Virtual Environment	10.1.0.1 (10.1.0.1.0614394)
Avaya Session Border Controller for Enterprise in Virtual Environment	10.1 (10.1.0.0-32-21432)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.19
Avaya J179 & 9611G IP Phone (H.323)	6.8532
Avaya J169 IP Phone (SIP)	4.0.13.0.6
HigherGround Calibre on Windows 2019 Server <ul style="list-style-type: none"><li>HgDMCC.exe</li><li>Avaya DMCC .NET (ServiceProvider.dll)</li></ul>	9.2022.8323.23020 Standard 9.2022.8425.20884 7.0.0.38

## 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 system parameter features
- Administer virtual IP softphones

### 5.1. Verify License

Log in to 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 set to **y**, then contact the Avaya sales team or business partner for a proper license file.

<b>display system-parameters customer-options</b>		<b>Page</b>	<b>4</b> 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?	y	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 n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field.

Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

<b>add cti-link 1</b>		<b>Page</b>	<b>1</b> of 3
CTI LINK			
CTI Link:	1		
<b>Extension:</b>	<b>60111</b>		
<b>Type:</b>	<b>ADJ-IP</b>		
<b>Name:</b>	<b>AES CTI Link</b>	<b>COR:</b>	1
Unicode Name?	n		

### 5.3. Administer IP Codec Set

Use the **change ip-codec-set n** command, where **n** is an existing codec set number to use for integration with Calibre.

For **Audio Codec**, enter the pertinent G.711 variant as shown below. Note that Calibre only supports the G.711 codec variant in this integration.

For customer network that use encrypted media, make certain that **none** is included for **Media Encryption**, and that **Encrypted SRTP** is set to **best-effort**. These settings are needed for support of non-encrypted media from the virtual IP softphones used by Calibre.

In the compliance testing, this IP codec set was used by the agent stations and by the virtual IP softphones.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP Codec Set

Codec Set: 1

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

Media Encryption                                Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
5:
```

## 5.4. Administer System Parameters Features

Log into the System Access Terminal. Use the **change system-parameters features** command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
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: 27
```

Navigate to **Page 13** and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Calibre.

```
change system-parameters features                                     Page 13 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
  Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

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

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



## 5.5. Administer Virtual IP Softphones

Add a virtual IP softphone 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.

- **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”

<b>add station 65991</b>		Page 1 of 5
STATION		
<b>Extension:</b> 65991	Lock Messages? n	BCC: 0
<b>Type:</b> 9608	<b>Security Code:</b> 123456	TN: 1
Port: IP	Coverage Path 1:	COR: 1
<b>Name:</b> Calibre 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: 65991	
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, two virtual IP softphones were administered as shown below.

list station 65991 count 2										
STATIONS										
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COR/ COS	TN		
65991	S000126	Calibre DMCC 1					1			
	9608		no				1 1			
65992	S000122	Calibre DMCC 2					1			
	9608		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 H.323 gatekeeper
- Administer Calibre 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 the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page, there is a light gray rectangular box containing the text "Please login here:" followed by a label "Username" and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, with the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." centered below it.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title 'Application Enablement Services Management Console'. A red navigation bar at the top contains 'Home', 'Help', and 'Logout' links. On the left, a sidebar lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Welcome to OAM' and provides an overview of the OAM web interface, listing administrative domains and their functions. A welcome message and system information are displayed in the top right corner.

**AVAYA Application Enablement Services Management Console**

Welcome: User  
Last login: Mon Oct 31 08:30:06 2022 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Tue Nov 08 12:26:17 EST 2022  
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).

The screenshot displays the Avaya Application Enablement Services Management Console with the 'Licensing | WebLM Server Access' view selected. The top header and navigation bar are consistent with the previous screenshot. The sidebar now highlights 'Licensing' and lists 'WebLM Server Address', 'WebLM Server Access', and 'Reserved Licenses'. The main content area is titled 'WebLM Server Access' and provides instructions on how to access the WebLM server. A welcome message and system information are displayed in the top right corner.

**AVAYA Application Enablement Services Management Console**

Welcome: User  
Last login: Mon Oct 31 08:30:06 2022 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Tue Nov 08 12:26:17 EST 2022  
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.

**AVAYA**  
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍

Home Licenses

L...

- WebLM Home
- Install license
- Licensed products
- APPL\_ENAB
  - Application\_Enablement
    - View by feature
    - View by local WebLM
    - Enterprise configuration
      - Local WebLM Configuration
      - Usages
      - Allocations
    - Periodic status
  - APS\_CMS\_Connectors
    - APS\_CMS\_Connectors
  - Configure Centralized Licensing
  - ASBCE
    - Session\_Border\_Controller\_E\_AE
  - CCTR

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

You are here: Licensed Products > Application\_Enablement > View by Feature

License installed on: June 10, 2022 9:09:46 PM -04:00

**License File Host IDs:** V5-E1-B3-74-2B-9E-01

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3
DLG (VALUE_AES_DLG)	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16

### 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**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays user information: Welcome: User, Last login: Mon Oct 31 08:30:06 2022 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 10.1.0.1.0.7-0, Server Date and Time: Tue Nov 08 12:26:17 EST 2022, HA Status: Not Configured. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected, and 'TSAPI Links' highlighted. The main content area is titled 'TSAPI Links' and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

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 **cm7**. 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.

The screenshot shows the AVAYA Application Enablement Services Management Console with the 'Add TSAPI Links' screen. The left navigation pane is the same as the previous screenshot. The main content area is titled 'Add TSAPI Links' and contains a form with the following fields: 'Link' (value: 1), 'Switch Connection' (value: cm7), 'Switch CTI Link Number' (value: 1), 'ASAI Link Version' (value: 12), and 'Security' (value: Both). Below the form are buttons for 'Apply Changes' and 'Cancel Changes'.



## 6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with relevant Communication Manager, in this case **cm7**, and select the corresponding radio button. Click **Edit Signaling Details**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The connection 'cm7' is selected with a radio button. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit Signaling Details', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as H.323 gatekeeper, in this case **10.64.101.236** as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - cm7' screen. It features a text input field containing '10.64.101.236' and buttons for 'Add Name or IP' and 'Delete IP'.

## 6.5. Administer Calibre 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.

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

Welcome: User  
Last login: Mon Oct 31 08:30:06 2022 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Tue Nov 08 12:26:17 EST 2022  
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 Idcalibre

\* Common Namecalibre

\* Surnamecalibre

\* User Password\*\*\*\*\*

\* Confirm Password\*\*\*\*\*

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

## 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 Calibre user from **Section 6.5**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner states: "Welcome: User", "Last login: Mon Oct 31 08:30:06 2022 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Nov 08 12:26:17 EST 2022", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected). The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.





## 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**.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Mon Oct 31 08:30:06 2022 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Tue Nov 08 12:26:17 EST 2022  
HA Status: Not Configured

Maintenance | Service ControllerHome | 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

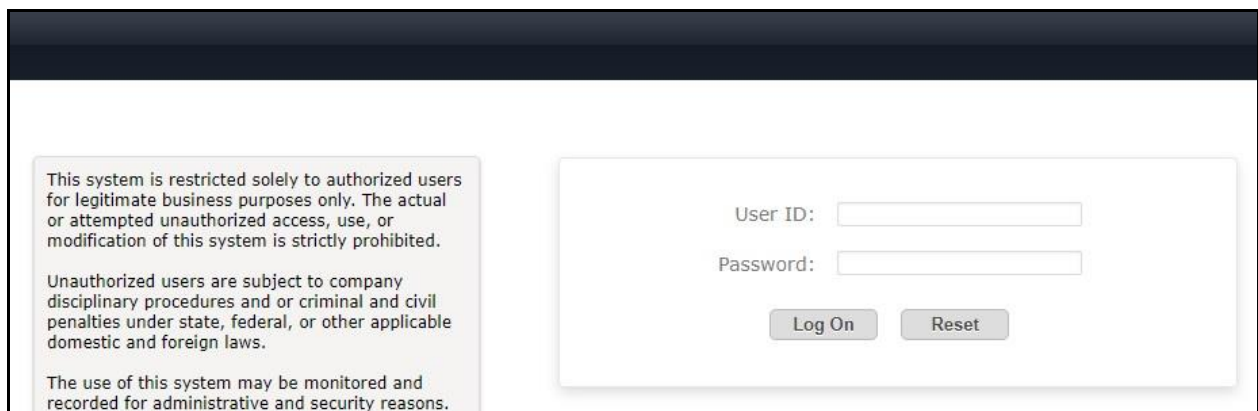
## 7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

### 7.1. Launch System Manager

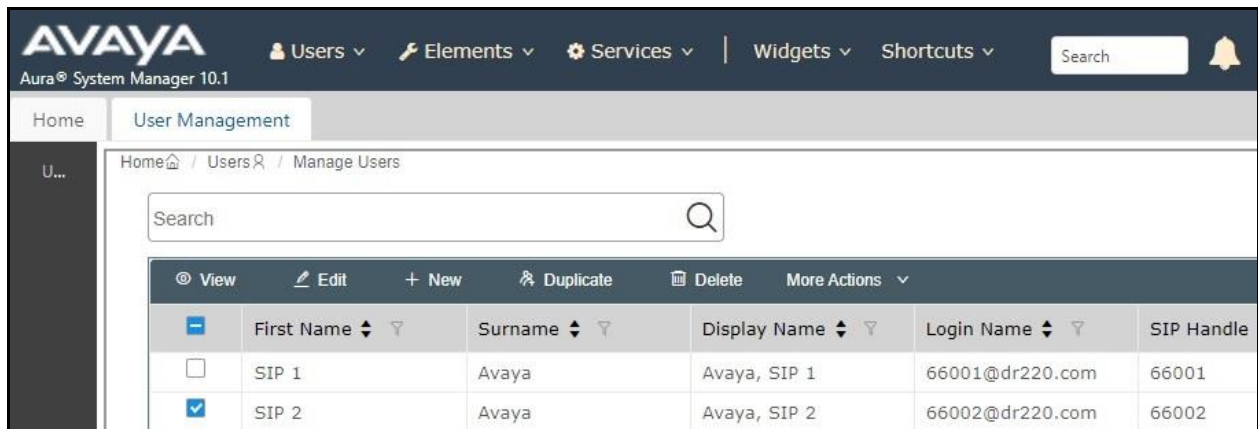
Access the System Manager web interface by using the URL **https://ip-address** in an Internet browser window, where **ip-address** is the IP address of System Manager. Log in using the appropriate credentials.



### 7.2. Administer 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 **66002**, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP 1	Avaya	Avaya, SIP 1	66001@dr220.com	66001
<input checked="" type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002

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

Click on the **Editor** icon 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 notification bell are also present. The main content area is titled 'User Profile | Edit | 66002@dr220.com' and features tabs for Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active, showing a list of profiles on the left: 'Communication Profile Password', 'PROFILE SET : Primary', 'Communication Address', 'PROFILES', 'Session Manager Profile' (disabled), 'CM Endpoint Profile' (enabled), and 'Officelinx Comm Profile' (disabled). The 'CM Endpoint Profile' sub-tab is selected, displaying various configuration fields. The 'Extension' field, containing '66002', has a blue editor icon highlighted with a red square. Other fields include 'System' (DR-CM), 'Profile Type' (Endpoint), 'Set Type' (J169CC), 'Port' (S000068), 'Voice Mail Number' (admin), and 'Sip Trunk' (aar). Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are at the top right.

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 3**. In the compliance testing, one SIP agent station was configured.

System	DR-CM	Extension	66002
Template	J169CC_DEFAULT_CM_8_1	Set Type	J169CC
Port	S000068	Security Code	
Name	Avaya, SIP 2		

<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	66002	* Message Lamp Ext.	66002
* Tenant Number	1	<b>Type of 3PCC Enabled</b>	Avaya
* SIP Trunk	Qaar	Coverage Path 2	
Coverage Path 1		Localized Display Name	Avaya, SIP 2
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	system
Multibyte Language	Not Applicable		

## 8. Configure HigherGround Calibre

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

- Administer Avaya Recorder
- Restart service
- Administer station utility
- Administer VoIP channel
- Administer dmccssc.cfg

The configuration of Calibre is performed by the HigherGround technicians and the procedural steps are presented in these Application Notes for information purposes only.

### 8.1. Administer Avaya Recorder

From the Calibre server, double-click on the **HG4 Configuration Manager** shortcut icon shown below, which was created as part of Calibre installation. Log in using the appropriate credentials in the subsequent screen (not shown).



The **HigherGround Configuration Manager** screen is displayed. Double click on the **Avaya Recorder** entry shown below.

HigherGround Configuration Manager [C:\CLU]		
Group	File Name	Title
Important	cadalarm.cfg	Alarm Monitor, HigherGround
Normal	cadarc.cfg	Archive Utility, HigherGround
Normal	cadcfg.cfg	Configuration Manager, HigherGround
Important	cadclu1.cfg	VoIP Recorder, HigherGround
Important	cadclu2.cfg	Avaya Recorder, HigherGround
Important	cadcoll.cfg	SMDR Data Connector
Normal	caddisp.cfg	Status Display Utility, HigherGround
Important	cadmastr.cfg	Task Master, HigherGround

The **HigherGround Avaya Recorder** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **VoIP Type:** “Avaya”
- **VoIP Channel Count:** The number of virtual IP softphones from **Section 5.5**.
- **Sniff IP:Port:** Check this field.
- **Minimum Duration:** The desired minimal duration for recordings.

**HigherGround Avaya Recorder [C:\CLU\cadclu2.cfg] Type 16**

**Output**

Processing Status File: **CADCLU2.DAT** Title: **HigherGround Avaya Recorder**

Show Devices Level: **Normal**

☒ Save DTMF as Attachments

**CTI Settings**

CTI Application: **Voice Over IP Recorder** ☒ Sniff Passive

**VoIP Type: Avaya** ☒ Sniff IP:Port

Recorder Unit Number: **2** Base Channel Number: **201** Base Station Number: **201**

**VoIP Channel Count: 2**

Virtual Channel Ports:  Base Virtual Channel: **2001** Base Virtual Station: **2001**

☐ Discover VoIP phone addresses ☐ Automatically assign discovered VoIP phones

DDAC Trigger Type: **API**

DDAC Event Log File: **ddac2.log**

Gateways... Light Mask Settings... Routers... DCH Attachments... DCH Triggers...

**Record Settings**

**Minimum Duration: 5** seconds (1-30) Maximum Duration: **7200** seconds (0, 60-6000)

Compression Method: **GSM 6.10 (13000 bps)** Real-Time Loop: **120** seconds (15-3600)

VOX Stop Silence: **5** seconds (5-60)

**Channel Activity Alarms**

Idle Alarm Setting: **WE:0, HD:0, 9-17:1800, 0**

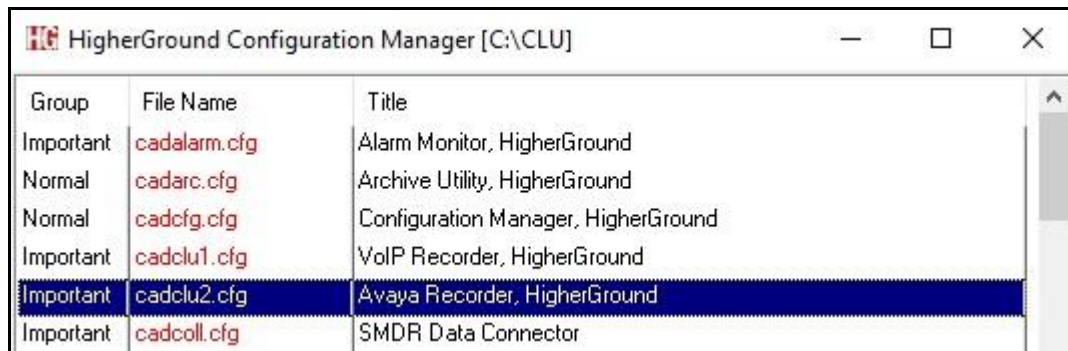
Alarm Repeat Seconds: **3600** Escalate Alarm After: **5** Repeats

☐ Re-launch Recorder on Escalated Idle Alarms

OK Cancel



The **HigherGround Configuration Manager** screen is displayed again. Right click on the **Avaya Recorder** entry and select **Open with Notepad**.



Group	File Name	Title
Important	cadalarm.cfg	Alarm Monitor, HigherGround
Normal	cadarc.cfg	Archive Utility, HigherGround
Normal	cadcfg.cfg	Configuration Manager, HigherGround
Important	cadclu1.cfg	VoIP Recorder, HigherGround
Important	cadclu2.cfg	Avaya Recorder, HigherGround
Important	cadcoll.cfg	SMDR Data Connector

Locate and set the specified fields below with listed values and retain the default values for the remaining fields. Note that only the first two parameters are shown in screenshot below.

- **VoIPRTPEvenOnly:** “0” to allow both odd and even RTP ports.
- **VoIPEndCallWithRTCP\_BYE:** “0”
- **SendRtpKeepalivePeriod:** “30”
- **RTCP:** “0” in both occurrences of this parameter in the file.

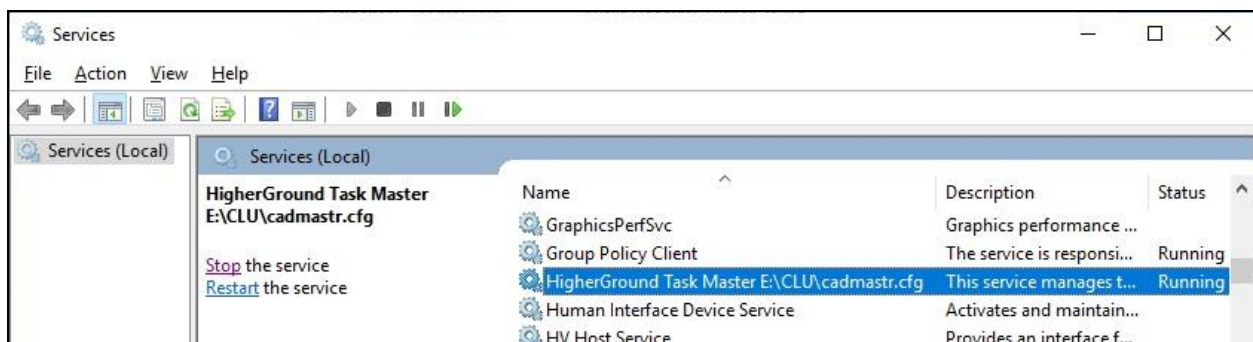


```

*cadclu2.cfg - Notepad
File Edit Format View Help
VoIPDAutoStationNameFromSDES=1
VoIPMinRTP=200
VoIPRTPEvenOnly=0
VoIPEndCallWithRTPMarkerbit=0
VoIPEndCallWithRTCP_BYE=0
VoIPEndCallWithSIP_BYE=1
  
```

## 8.2. Restart Service

From the Calibre server, select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Stop and then start the **HigherGround Task Master** service shown below.



Name	Description	Status
GraphicsPerfSvc	Graphics performance ...	
Group Policy Client	The service is responsi...	Running
HigherGround Task Master E:\CLU\cadmastr.cfg	This service manages t...	Running
Human Interface Device Service	Activates and maintain...	
HV Host Service	Provides an interface f...	



### 8.3. Administer Station Utility

From the Calibre server, double-click on the **HG4 Manage** shortcut icon shown below, which was created as part of Calibre installation. Log in using the appropriate credentials in the subsequent screen (not shown).



The **HigherGround Manage – User/Channel Table** screen is displayed. Select **Utility** → **Station Utility** from the top menu.

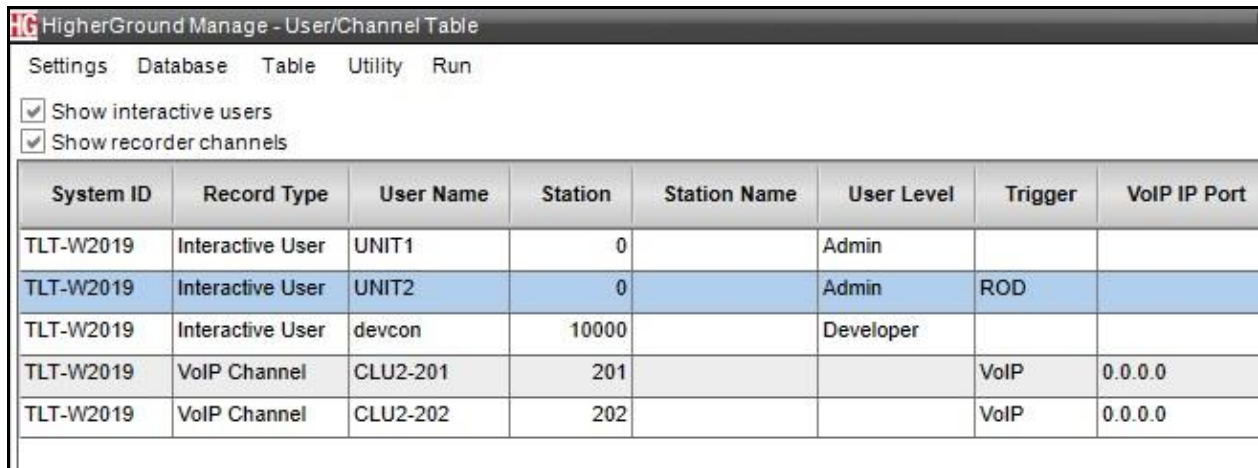
HigherGround Manage - User/Channel Table							
Settings Database Table Utility Run							
<input checked="" type="checkbox"/> Show interactive users							
<input checked="" type="checkbox"/> Show recorder channels							
System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP Port
TLT-W2019	Interactive User	UNIT1	0		Admin		
TLT-W2019	Interactive User	UNIT2	0		Admin	ROD	
TLT-W2019	Interactive User	devcon	10000		Developer		
TLT-W2019	VoIP Channel	CLU2-201	201			VoIP	0.0.0.0
TLT-W2019	VoIP Channel	CLU2-202	202			VoIP	0.0.0.0

The **HigherGround Manage – Station Utility** screen is displayed next. Create an entry for each agent station extension and agent ID from **Section 3** with pertinent **Station** extension and desired **Name** value. In the compliance testing, four entries were created as shown below.

HigherGround Manage - Station Utility							
Settings Database Table Utility Run							
<input checked="" type="checkbox"/> Show expired Stations							
<input checked="" type="checkbox"/> Show older versions of Stations							
System ID	Station	Name	Division	Division Name	Department	Department Name	Building
TLT-W2019	9999	Test Phone	1	UNASSIGNED	101	UNASSIGNED	
TLT-W2019	65001	CM Station 1	0		0		
TLT-W2019	66002	Avaya SIP 2	0		0		
TLT-W2019	65881	Agent 1	0		0		
TLT-W2019	65882	Agent 2	0		0		
<div>&lt; [Progress Bar] &gt;</div>							
<div>Home Save Cancel Add Remove Copy Apply To Report</div>							

## 8.4. Administer VoIP Channel

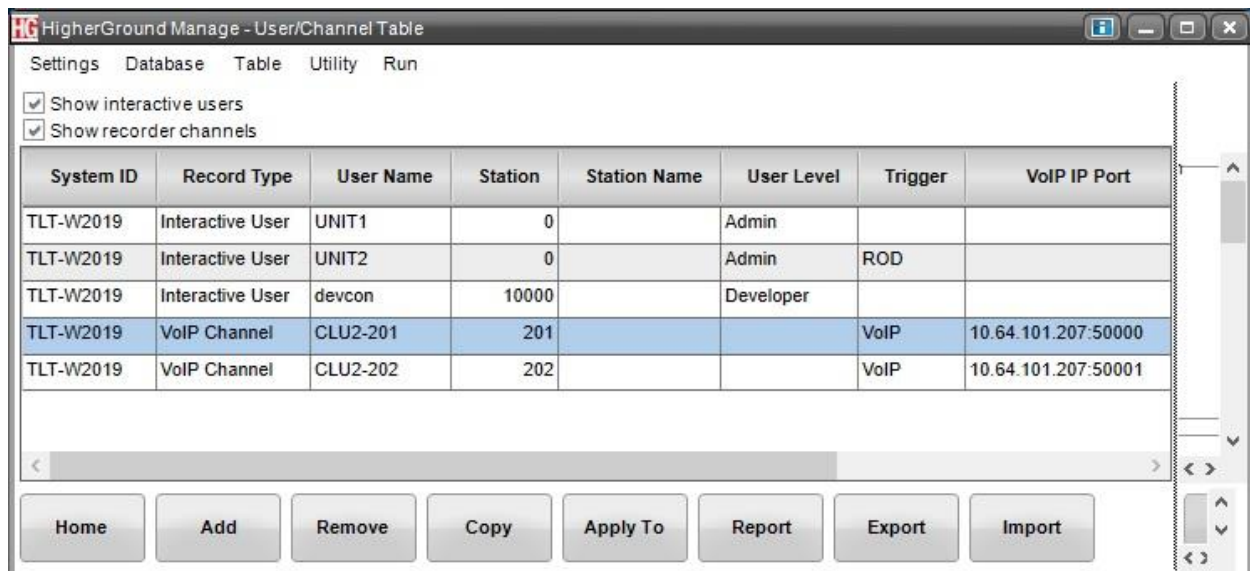
Select **Home** from the bottom of the **HigherGround Manage – Station Utility** screen in **Section 8.3** to display the **HigherGround Manage – User/Channel Table** screen below. Note that two **VoIP Channel** entries were auto created due to the VoIP channel count setting in **Section 8.1**.



System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP Port
TLT-W2019	Interactive User	UNIT1	0		Admin		
TLT-W2019	Interactive User	UNIT2	0		Admin	ROD	
TLT-W2019	Interactive User	devcon	10000		Developer		
TLT-W2019	VoIP Channel	CLU2-201	201			VoIP	0.0.0.0
TLT-W2019	VoIP Channel	CLU2-202	202			VoIP	0.0.0.0

For each **VoIP Channel** entry, set **VoIP IP Port** to the IP address of the Calibre server and an available port number starting with **50000**.

In the compliance testing, two **VoIP Channel** entries were updated as shown below.

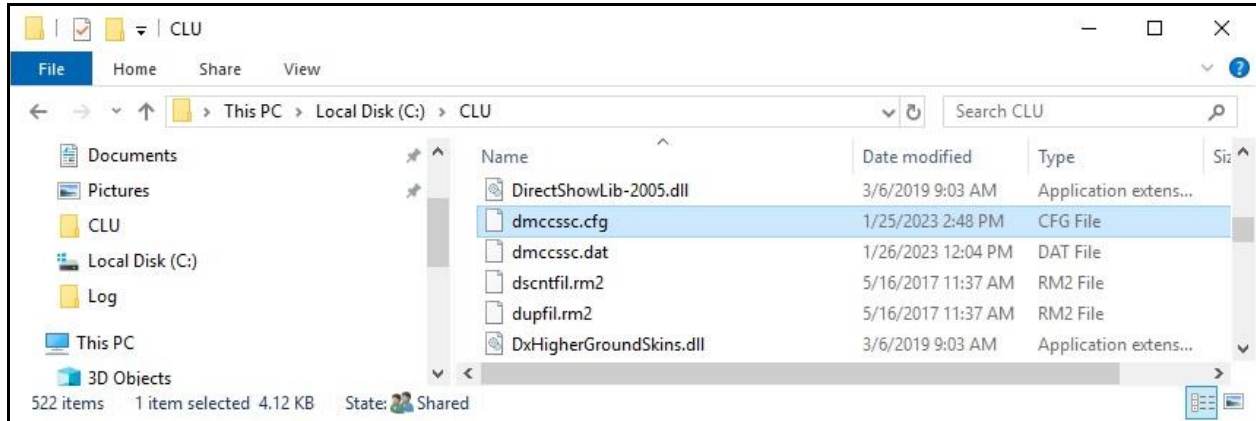


System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP Port
TLT-W2019	Interactive User	UNIT1	0		Admin		
TLT-W2019	Interactive User	UNIT2	0		Admin	ROD	
TLT-W2019	Interactive User	devcon	10000		Developer		
TLT-W2019	VoIP Channel	CLU2-201	201			VoIP	10.64.101.207:50000
TLT-W2019	VoIP Channel	CLU2-202	202			VoIP	10.64.101.207:50001

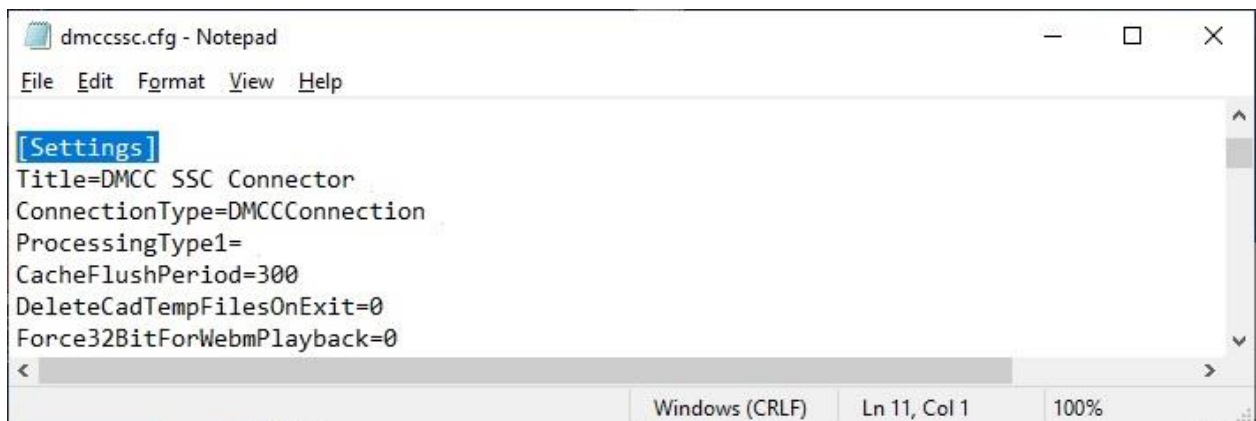
Home Add Remove Copy Apply To Report Export Import

## 8.5. Administer dmccssc.cfg

From the Calibre server, navigate to the Calibre install directory and open the **dmccssc.cfg** file with a text editor such as Notepad.

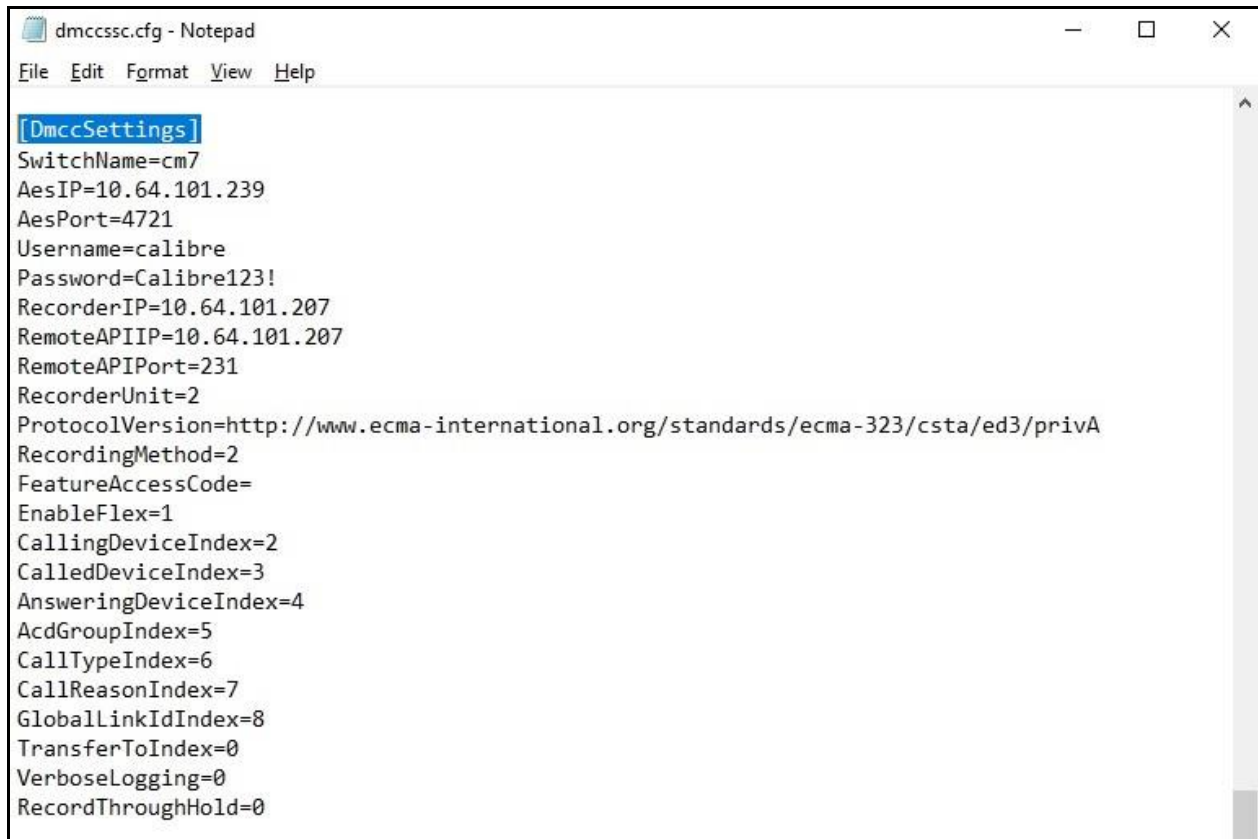


Navigate to the **Settings** sub-section. Set **Title** to **DMCC SSC Connector** and set **ConnectionType** to **DMCCConnection** as show below.



Navigate to the **DmccSettings** sub-section. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **SwitchName:** The switch connection name from **Section 6.3**.
- **AesIP:** IP address of Application Enablement Services.
- **AesPort:** The DMCC unencrypted port from **Section 6.7**.
- **Username:** The Calibre user credentials from **Section 6.5**.
- **Password:** The Calibre user credentials from **Section 6.5**.
- **RecorderIP:** IP address of the Calibre server.
- **RemoteAPIIP:** IP address of the Calibre server.
- **RecordingMethod:** “2” for Single Step Conference.
- **CallingDeviceIndex:** “2”
- **CalledDeviceIndex:** “3”
- **AnsweringDeviceIndex:** “4”
- **AcdGroupIndex:** “5”
- **CallTypeIndex:** “6”
- **CallReasonIndex:** “7”
- **GlobalLinkIdIndex:** “8”

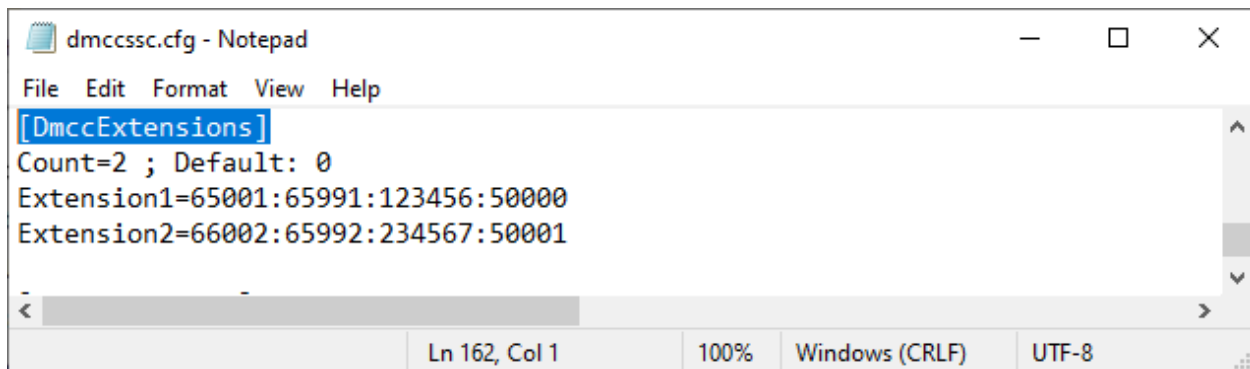


The screenshot shows a Notepad window titled "dmccssc.cfg - Notepad". The menu bar includes File, Edit, Format, View, and Help. The text content of the file is as follows:

```
[DmccSettings]
SwitchName=cm7
AesIP=10.64.101.239
AesPort=4721
Username=calibre
Password=Calibre123!
RecorderIP=10.64.101.207
RemoteAPIIP=10.64.101.207
RemoteAPIPort=231
RecorderUnit=2
ProtocolVersion=http://www.ecma-international.org/standards/ecma-323/csta/ed3/privA
RecordingMethod=2
FeatureAccessCode=
EnableFlex=1
CallingDeviceIndex=2
CalledDeviceIndex=3
AnsweringDeviceIndex=4
AcdGroupIndex=5
CallTypeIndex=6
CallReasonIndex=7
GlobalLinkIdIndex=8
TransferToIndex=0
VerboseLogging=0
RecordThroughHold=0
```

Navigate to the **DmccExtensions** sub-section. Create an extension entry for each VoIP channel from **Section 8.4**. Set the **Count** parameter to the number of extension entries.

For each extension entry, set the value to a station extension from **Section 3**, followed by an available virtual IP softphone extension and security code from **Section 5.5**, and the corresponding VoIP channel port number from **Section 8.4**. In the compliance testing, two extension entries were created as shown below.

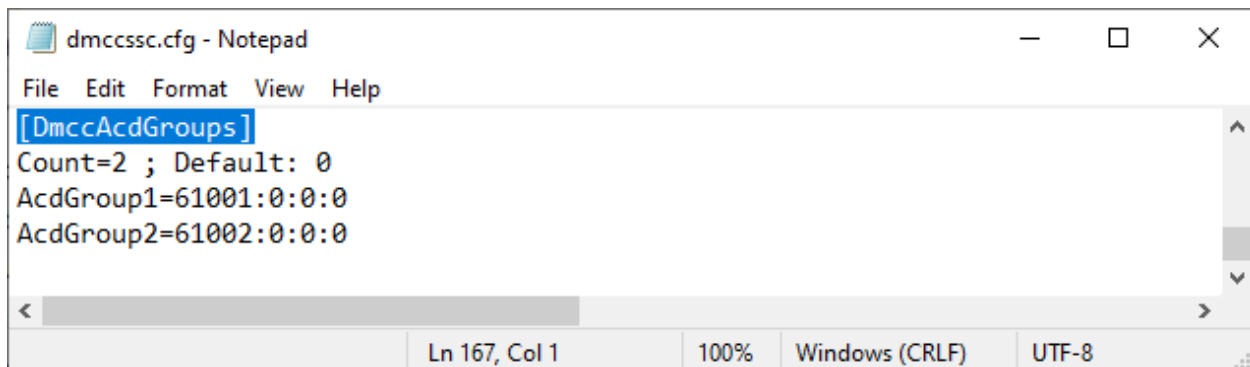


```
dmccssc.cfg - Notepad
File Edit Format View Help
[DmccExtensions]
Count=2 ; Default: 0
Extension1=65001:65991:123456:50000
Extension2=66002:65992:234567:50001
Ln 162, Col 1 100% Windows (CRLF) UTF-8
```

Navigate to the **DmccAcdGroups** sub-section. Create an ACD group entry for each skill group from **Section 3**. Set the **Count** parameter to the number of ACD group entries.

For each ACD group entry, set the value to a skill group extension from **Section 3** followed by zeroes. In the compliance testing, two ACD group entries were created as shown below.

Follow the procedures in **Section 8.2** to restart the **HigherGround Task Master** service.



```
dmccssc.cfg - Notepad
File Edit Format View Help
[DmccAcdGroups]
Count=2 ; Default: 0
AcdGroup1=61001:0:0:0
AcdGroup2=61002:0:0:0
Ln 167, Col 1 100% Windows (CRLF) UTF-8
```

## 9. Verification Steps

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

### 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	aes7	established	50	30

Verify registration status of the virtual IP softphones by using the **list registered-ip-stations** command. Verify that all virtual IP softphones from **Section 5.5** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS			
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
65000	9611	IP_Phone	192.168.200.212
tls	1	6.8	10.64.101.236
65001	9611	IP_Phone	192.168.200.179
tls	1	6.8	10.64.101.236
<b>65991</b>	<b>9608</b>	<b>IP_API_A</b>	<b>10.64.101.239</b>
<b>tcp</b>	<b>1</b>	<b>3.2040</b>	<b>10.64.101.236</b>
<b>65992</b>	<b>9608</b>	<b>IP_API_A</b>	<b>10.64.101.239</b>
<b>tcp</b>	<b>1</b>	<b>3.2040</b>	<b>10.64.101.236</b>



## 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 the **User** column shows an active session with the Calibre user name from **Section 6.5** and that the number **# of Associated Devices** reflects the total number of monitored skill groups and agent stations from **Section 3** plus the number of virtual IP softphones from **Section 5.5**, in this case **6** in total.

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

Welcome: User  
Last login: Wed Jan 25 13:09:09 2023 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Thu Jan 26 09:02:26 EST 2023  
HA Status: Not Configured

Status | Status and Control | **DMCC 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

**DMCC Service Summary - Session Summary**

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Jan 26 09:02:21 EST 2023

Service Uptime: 7 days, 19 hours 6 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 5

Number of Existing Devices: 6

Number of Devices Created Since Service Boot: 30

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	6C1C3B3255ED7BC46 312EAF8621C9CAB-4	calibre	HgDMCC	10.64.101.207	XML Unencrypted	6

Terminate Sessions | Show Terminated Sessions

Item 1-1 of 1  
1 Go

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 **4**.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Wed Jan 25 13:09:09 2023 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Thu Jan 26 09:01:58 EST 2023  
HA Status: Not Configured

Status | Status and Control | TSAPI 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**

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	cm7	1	Talking	Wed Jan 18 13:54:31 2023	Online	20	4	30	49	30

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

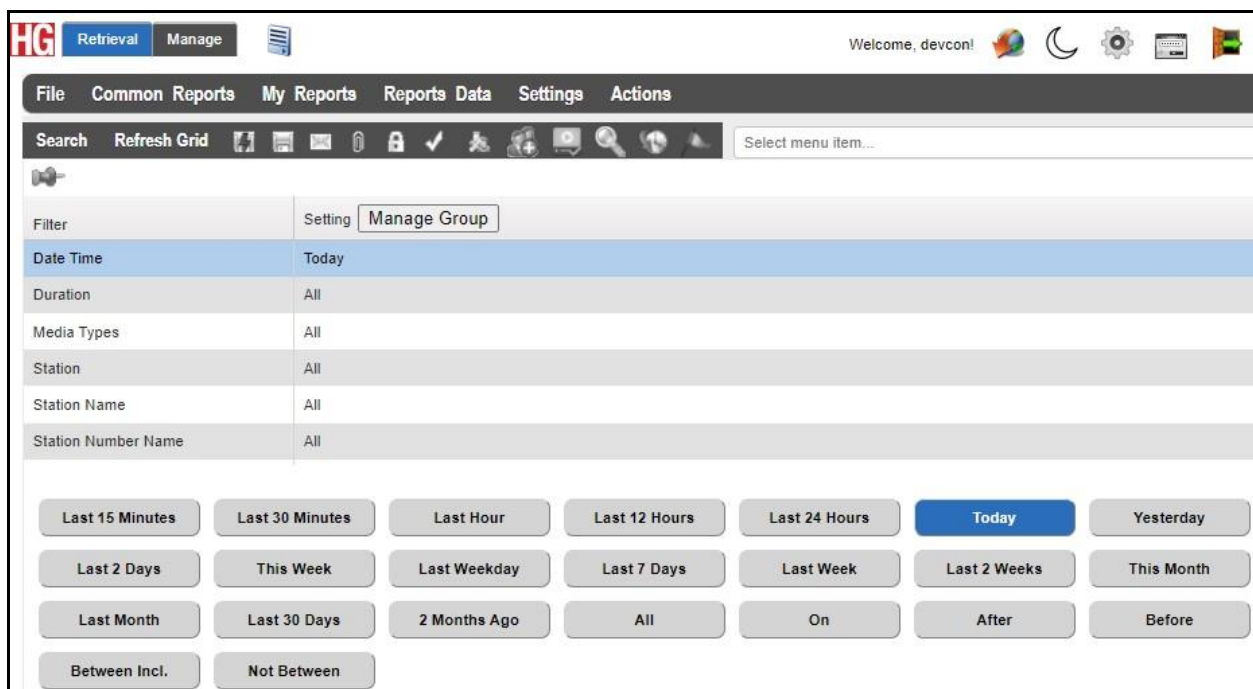


### 9.3. Verify HigherGround Calibre

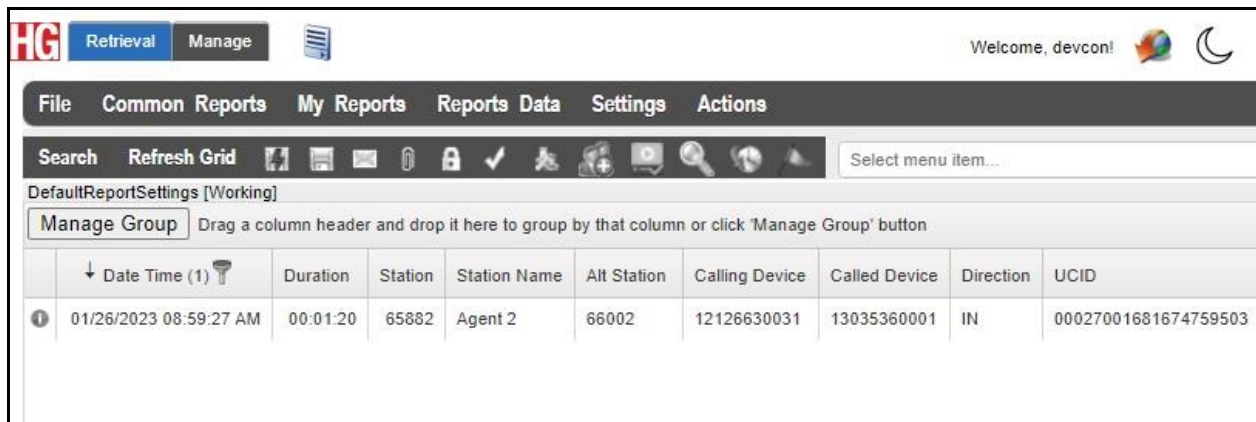
Log an agent in to handle and complete an ACD call. Access the Calibre web interface by using the URL **http://ip-address/WBI** where **ip-address** is the IP address of the Calibre server. Log in using the appropriate credentials.



The screen below is displayed. Select the **Retrieval** tab followed by **Search** then **Today**. Select **Refresh Grid**.

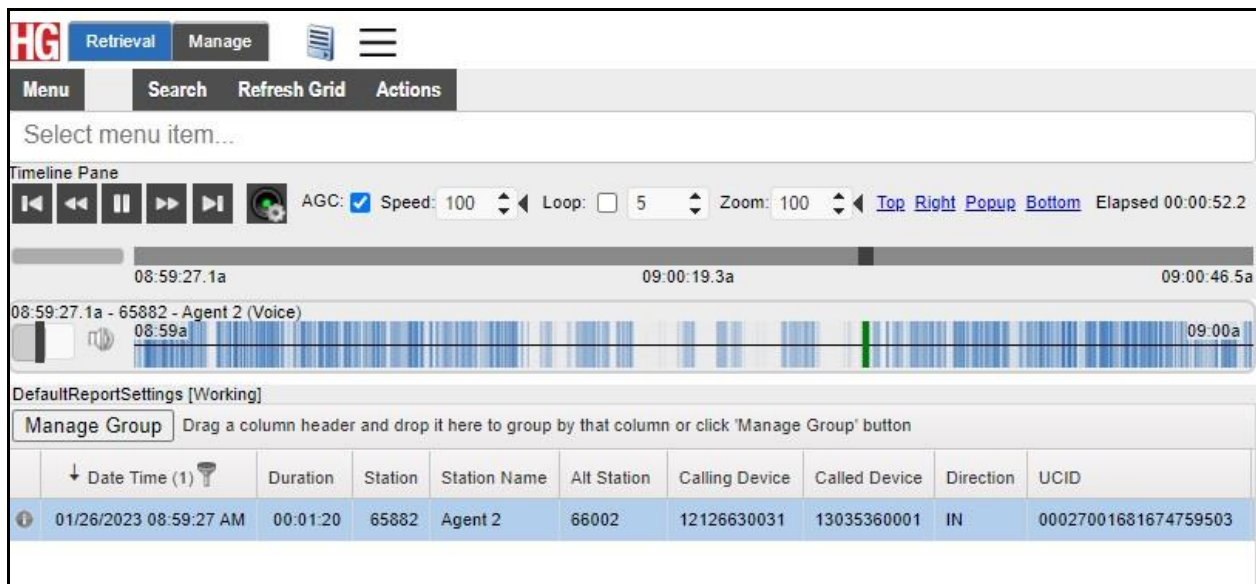


The screen is updated with a list of call recordings for today. Verify that there is an entry for the last call with proper values in the relevant fields as shown below.



↓ Date Time (1)	Duration	Station	Station Name	Alt Station	Calling Device	Called Device	Direction	UCID
01/26/2023 08:59:27 AM	00:01:20	65882	Agent 2	66002	12126630031	13035360001	IN	00027001681674759503

Select the entry followed by the **Play** icon in the updated screen. Verify that the recording can be played back as shown below.



Timeline Pane

AGC: ☒ Speed: 100 Loop: ☐ 5 Zoom: 100 Top Right Popup Bottom Elapsed 00:00:52.2

08:59:27.1a 09:00:19.3a 09:00:46.5a

08:59:27.1a - 65882 - Agent 2 (Voice)

08:59a 09:00a

↓ Date Time (1)	Duration	Station	Station Name	Alt Station	Calling Device	Called Device	Direction	UCID
01/26/2023 08:59:27 AM	00:01:20	65882	Agent 2	66002	12126630031	13035360001	IN	00027001681674759503

## 10. Conclusion

These Application Notes describe the configuration steps required for Calibre 9.2022 to successfully interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 using Single Step Conference. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 11. Additional References

This section references the product 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. *HG4 Web UI Installation Manual*, v.9.2022, available as part of Calibre installation.
5. *HG4 Admin Manual*, v.9.2022, available as part of Calibre installation.
6. *HG4 User Manual*, v.9.2022, available as part of Calibre installation.

---

**©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).