



Avaya Solution & Interoperability Test Lab

Application Notes for HigherGround Calibre with Avaya Aura[®] Communication Manager Using Avaya Aura[®] Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for HigherGround Calibre to interoperate with Avaya Aura[®] Communication Manager using Avaya Aura[®] Application Enablement Services.

HigherGround Calibre is a call recording solution. In the compliance testing, HigherGround Calibre used the Device, Media, and Call Control (DMCC) Service Observing interface from Avaya Aura[®] Application Enablement Services to monitor skill group and agent station extensions on Avaya Aura[®] Communication Manager, and to capture the media associated with the monitored agents 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 (Calibre) to interoperate with Avaya Aura[®] Communication Manager (Communication Manager) using Avaya Aura[®] Application Enablement Services (Application Enablement Services).

Calibre is a call recording solution. In the compliance testing, Calibre used the Device, Media, and Call Control (DMCC) interface from Application Enablement Services to monitor skill group and agent station extensions on Communication Manager.

Calibre starts the call recording by using the Service Observing feature to add a virtual IP softphone to target stations upon successfully registering via DMCC, and to obtain the media when calls connect to the target stations.

When there is an active call on the monitored agent, Calibre is informed of the call via TSAPI event reports from the DMCC interface. The event reports are used to tag recordings with agent, station, caller and called information.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Calibre application, the application uses DMCC to register the virtual IP softphones to Communication Manager, and to request TSAPI monitoring on the skill group and agent station extensions. These virtual stations are then set to Service Observe the target stations using a Service Observe button programmed on the station form.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios. The serviceability test cases were performed manually by disconnecting/reconnecting the network connection to Calibre.

The verification of tests included using the Calibre logs for proper message exchanges and using the Retrieval application for proper logging and playback of the 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 these Application Notes, 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 registration services to register and un-register the virtual IP softphones.
- Use of DMCC monitoring services to monitor skill group, agent stations, and virtual IP softphones.
- Use of DMCC device control services to activate Service Observing for the virtual IP softphones and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous calls, simultaneous 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 the Calibre server.

2.2. Test Results

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

- By design, every time a hold and resume is performed on the agent stations, a new record is created on Calibre.

2.3. Support

Technical support on Calibre can be obtained through the following:

- **Phone:** (818) 456-1600
- **Email:** support@highergroundinc.com

3. Reference Configuration

Calibre can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration shown in **Figure 1**.

Calibre has a Retrieval application that can be used to review and playback the call recordings.

In the compliance testing, the contact center devices consisted of the following.

Device Type	Extension
VDN	31500
Skill/Hunt Group	3100
Agent ID	32000 - 32004
Agent Station (H.323)	30002, 30004
Agent Station (SIP)	30001, 30003, 30006
Agent Station (DCP)	30005
Virtual Station	30050-30055

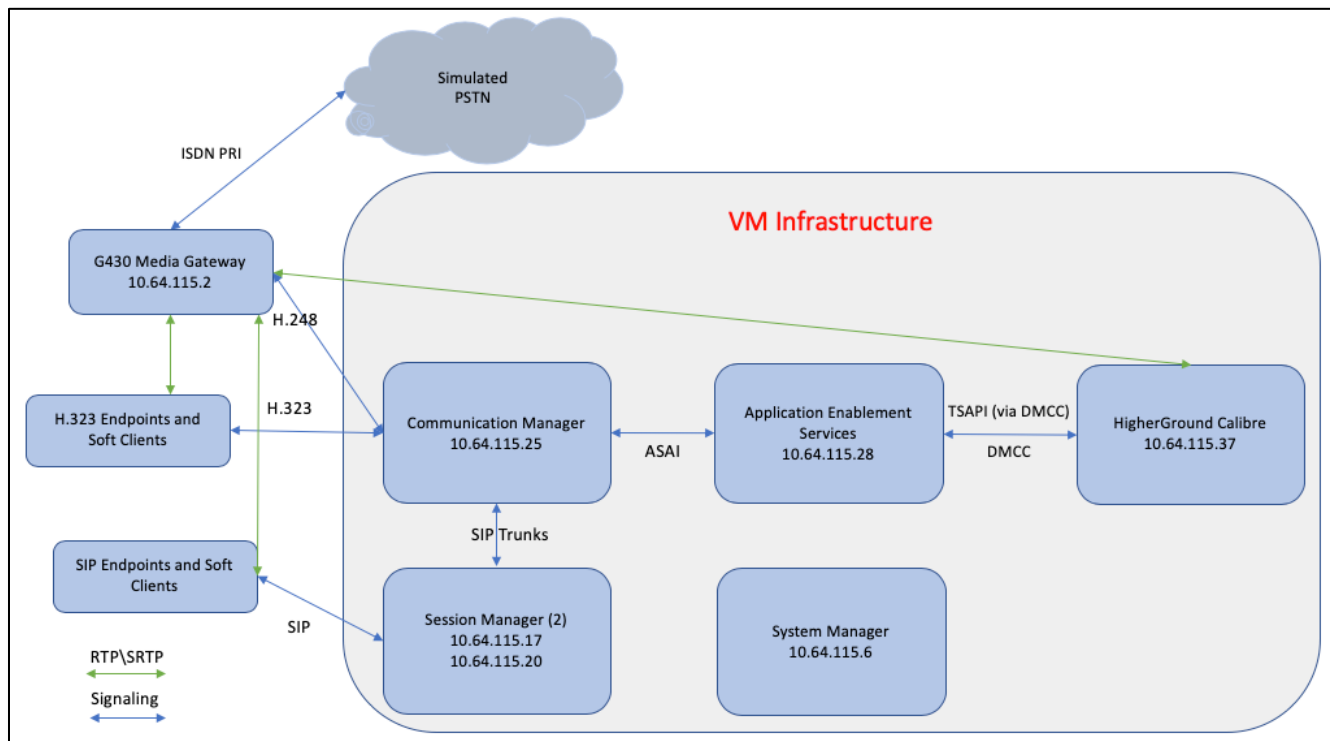


Figure 1: Calibre Test Configuration

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	8.0 (R018x.00.0.822.0)
Avaya G430 Media Gateway	40.10.0
Avaya Aura® System Manager	8.0.0.0.098174
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Aura® Application Enablement Services	8.0.0.0.0.6-0
Avaya 6408D Deskphone (DCP)	n/a
Avaya J169/179 Deskphone (SIP)	3.0.0.1.6
Avaya 9641G Deskphone (SIP)	7.1.1.09
9611G (H.323)	6.6506
9670G (H.323)	3.280A
HigherGround Calibre on Windows 2016 Standard Server	8.1804
• Avaya DMCC .NET (ServiceProvider.dll)	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 IP Services
- Administer CTI link
- Administer system parameters features
- Administer virtual IP softphones

5.1. Verify License

Log in to the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. 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.

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

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? y           Authorization Codes? y
Analog Trunk Incoming Call ID? y           CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y    CAS Main? n
Answer Supervision by Call Classifier? y    Change COR by FAC? n
ARS? y      Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y      DCS (Basic)? y
ASAI Link Core Capabilities? y      DCS Call Coverage? y
ASAI Link Plus Capabilities? y      DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n      Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n      DS1 MSP? y
ATM WAN Spare Processor? n      DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? y
```

5.2. Administer IP Services

Use the “change ip-services” command to define the service port. The AE Services Server must match the hostname of the AES server, the password will be used later when configuring AES.

change ip-services					Page 1 of 3
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		
change ip-services					Page 3 of 3
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	sildvaes8	*	y	in use	

5.3. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number.

display cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 30099		
Type: ADJ-IP		
Name: AES8		
		COR: 1

5.4. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)** and assign a unique value for **UCID Network 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: SILDenver
      Emergency Extension Forwarding (min): 10
      Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                        COR to Use for DPT: station
      EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
      Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
      Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
      Send All Calls Applies to: station      Auto Inspect on Send All Calls? n
      Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
      Create Universal Call ID (UCID)? y      UCID Network Node ID: 1
```

On **Page 13**, enable **Send UCID to ASAI**. This 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? n
                        Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
      Send Connect Event to ASAI For Announcement Answer? n
      Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.5. Administer Virtual IP Softphones

Add a virtual softphone using 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.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”

add station 30050		Page 1 of 5
STATION		
Extension: 30050	Lock Messages? n	BCC: 0
Type: 9608	Security Code: *	TN: 1
Port: S00017	Coverage Path 1:	COR: 1
Name: DMCC1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 30050	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

Make sure a button is configured with **serv-obsrv**:

add station 30050		Page 4 of 5
STATION		
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3: call-appr	7:	
4: serv-obsrv	8:	
voice-mail		

Repeat this section to administer the desired number of virtual IP softphones, using sequential extension numbers. In the compliance testing, six virtual IP softphones were administered as shown below, to allow for simultaneous recording of all monitored agents in **Section 3**.

```
list station 30050 count 6
```

STATIONS

Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COR/ COS	TN
30050	S00017	DMCC1					1	
	9608		no				1	1
30051	S00020	DMCC2					1	
	9608		no				1	1
30052	S00023	DMCC3					1	
	9608		no				1	1
30053	S00026	DMCC4					1	
	9608		no				1	1
30054	S00029	DMCC5					1	
	9608		no				1	1
30055	S00032	DMCC6					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 Switch Connection
- Administer H.323 Gatekeeper
- Administer TSAPI link
- Disable Security Database
- Restart Services
- Administer Calibre User
- Administer Ports

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 page. At the top, the Avaya logo is on the left, and the title 'Application Enablement Services Management Console' is centered. Below the title is a red horizontal bar. In the center, there is a login box with the text 'Please login here:' followed by a 'Username' label and a text input field. Below the input field is a 'Continue' button. At the bottom of the page, there is a copyright notice: 'Copyright © 2009-2016 Avaya Inc. All Rights Reserved.'

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

The screenshot shows the 'Welcome to OAM' screen of the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message with system details: 'Welcome: User cust', 'Last login: Fri Apr 12 09:44:06 2019 from 10.64.115.42', 'Number of prior failed login attempts: 0', 'HostName/IP: sildvaes8.sildserver.org/10.64.115.28', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.0.0.0.0.6-0', 'Server Date and Time: Wed May 29 12:45:37 MDT 2019', and 'HA Status: Not Configured'. Below the header is a navigation bar with 'Home | Help | Logout'. On the left is a sidebar menu with links to '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 contains a paragraph: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. This is followed by a bulleted list of domains and their functions: '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.', and 'Help - Use Help to obtain a few tips for using the OAM Help system'. A final paragraph states: '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 **Web License Manager** pop-up screen, and log in using the appropriate credentials. In the lab, the license was installed on System Manager.

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 **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for monitoring and call control via DMCC, and the DMCC license is used for the virtual IP softphones.

AVAYA Aura® System Manager 8.0 | Users | Elements | Services | Widgets | Shortcuts | AVAYA DevConnect | Search | admin

Home | Licenses

Licenses

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
- Application_Enablement
 - View license capacity
 - View peak usage
- COMMUNICATION_MANAGER
 - Call_Center
 - Communication_Manager
 - Configure Centralized Licensing
- MSR
 - Media_Server
- SYSTEM_MANAGER
 - System_Manager
- SessionManager
 - SessionManager
- Uninstall license
- Server properties
- Shortcuts
- Help for Licensed products

Application Enablement (CTI) - Release: 8 - SID: 10503000 **Standard License file**

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

License installed on: November 2, 2018 4:13:54 PM +00:00

License File Host IDs: VF-89-29-16-14-8B-01

Licensed Features

10 Items | Show | All

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

SmallServerTypes:
s8300c;s8300d;jcc;premio;tn8400;laptop;CtiS
MediumServerTypes:
ibmx306;ibmx306m;dell1950;xen;hs20;hs20
LargeServerTypes:
isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u
TrustedApplications: IPS_001, BasicUnrestrict
DMCUnrestricted; 1XP_001, BasicUnrestricted
DMCUnrestricted; 1XM_001, BasicUnrestricted
DMCUnrestricted; PC_001, BasicUnrestricted
DMCUnrestricted; CIE_001, BasicUnrestricted
DMCUnrestricted; OSPC_001, BasicUnrestricted
DMCUnrestricted; VP_001, BasicUnrestricted
DMCUnrestricted; SAMETIME_001, VALUE_AES
CCE_001, BasicUnrestricted, AdvancedUnrestr
CSI_T1_001, BasicUnrestricted, AdvancedUnre
CSI_T2_001, BasicUnrestricted, AdvancedUnre
AVAYAVERINT_001, BasicUnrestricted, Advanc
DMCUnrestricted; CCT_ELITE_CALL_CTRL_001
AdvancedUnrestricted, DMCUnrestricted, Agen
BasicUnrestricted, AdvancedUnrestricted, DMC

6.3. Administer Switch Connection

Select **Communication Manager Interface > Switch Connections** from the left pane. Enter a name for the Switch Connection, **SILDVCM8** was used in this configuration, and click **Add Connection**.

The **Add Switch Connection** screen is displayed next (not shown), below is example of link created during compliance test.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' selected, with 'Switch Connections' highlighted. The main area displays a table of Switch Connections. A table with 4 columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. One entry is visible: SILDVCM8, Yes, 30, 1. Below the table are buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, and Survivability Hierarchy.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
SILDVCM8	Yes	30	1

Next, click the **Edit PE/CLAN IPs** button and enter the IP Address of the Communication Manager and click **Add/Edit Name or IP**.

The screenshot shows the 'Edit Processor Ethernet IP - SILDVCM8' screen. It features a text input field with '10.64.115.25' and an 'Add/Edit Name or IP' button. Below is a table with 2 columns: Name or IP Address and Status. One entry is visible: 10.64.115.25, In Use. A 'Back' button is at the bottom.

Name or IP Address	Status
10.64.115.25	In Use

6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with the relevant Communication Manager, in this case “SILDVCM8”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' selected, with 'Switch Connections' highlighted. The main area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. One connection is listed: SILDVCM8, with Processor Ethernet set to Yes, Msg Period set to 30, and Number of Active Connections set to 1. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
SILDVCM8	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor Ethernet port on Communication Manager to be used as H.323 gatekeeper, in this case “10.64.115.25 as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - SILDVCM8' screen. The left navigation pane is the same as the previous screenshot. The main area has a text input field for 'Name or IP Address' with the value '10.64.115.25' entered. Below the input field are buttons for 'Delete IP' and 'Back'. There is also an 'Add Name or IP' button above the input field.

6.6. Administer TSAPI Link

To administer a TSAPI link, select **AE Services > TSAPI > TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The **Add TSAPI Links** screen is displayed next (not shown), below is example of link created during compliance test.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Jun 10 14:53:11 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvae8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.0.6-0
Server Date and Time: Thu Jun 13 10:08:25 MDT 2019
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
1	SILDVCM8	1	9	Both

Add Link Edit Link Delete Link

For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “**SILDVCM8**” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Select “9” for **ASAI Link Version** and select “Both” for **Security**.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Jun 10 14:53:11 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvae8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.0.6-0
Server Date and Time: Thu Jun 13 10:29:39 MDT 2019
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links

Home | Help | Logout

▼ AE Services

CVLAN

DLG

DMCC

SMS

▼ TSAPI

TSAPI Links

TSAPI Properties

TWS

Edit TSAPI Links

Link1

Switch ConnectionSILDVCM8

Switch CTI Link Number1

ASAI Link Version9

SecurityBoth

Apply Changes Cancel Changes Advanced Settings

6.7. Disable 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. Uncheck both fields below and click **Apply Changes**. This step is optional, the user account can be given unrestricted access instead, as described in **Section 6.9**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with system details. A red navigation bar shows the path "Security | Security Database | Control". The left sidebar lists various system components, with "Security Database" and its "Control" sub-item highlighted. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

Welcome: User cust
Last login: Mon Jun 10 14:53:11 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenvr.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.6-0
Server Date and Time: Thu Jun 13 11:55:21 MDT 2019
HA Status: Not Configured

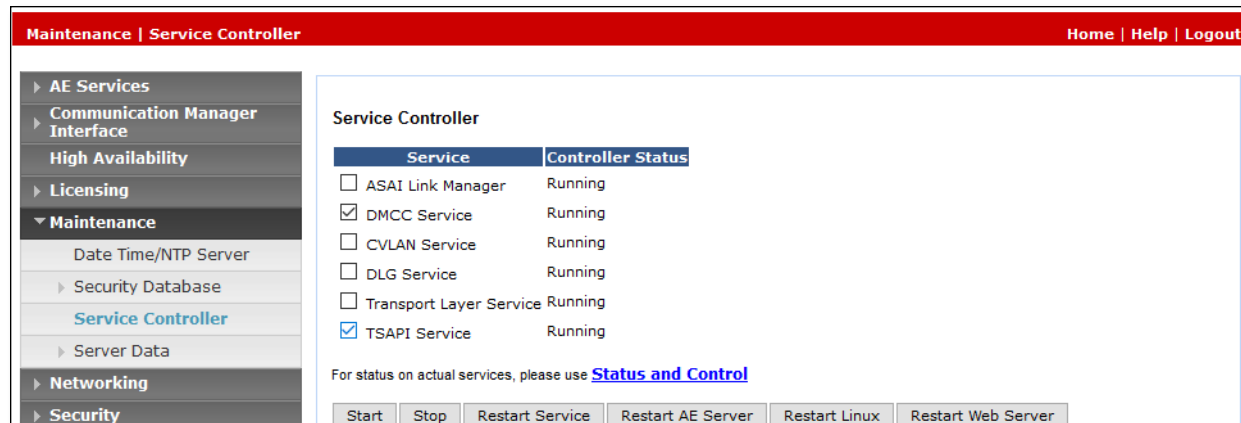
Security | Security Database | Control Home | Help | Logout

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

6.8. 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**.



The screenshot shows a web interface for the Service Controller. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, and Security. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists six services: ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, Transport Layer Service, and TSAPI Service. The DMCC Service and TSAPI Service are checked, and all services show a 'Running' status. Below the table, there is a link to 'Status and Control' and a row of buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

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

6.9. 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. Click **Apply** at the bottom of the screen (not shown below).

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text 'Application Enablement Services Management Console'. A red navigation bar contains links for 'User Management', 'User Admin', 'List All Users', 'Home', 'Help', and 'Logout'. The left sidebar lists various system components, with 'User Management' expanded to show 'User Admin' options: 'Add User', 'Change User Password', 'List All Users' (highlighted), 'Modify Default Users', and 'Search Users'. The main content area is titled 'Edit User' and contains a form with the following fields: * User Id (text box with 'Calibre'), * Common Name (text box with 'Calibre'), * Surname (text box with 'Calibre'), User Password (text box), Confirm Password (text box), Admin Note (text box), Avaya Role (dropdown menu with 'None'), Business Category (text box), Car License (text box), CM Home (text box), Csm Home (text box), CT User (dropdown menu with 'Yes'), Department Number (text box), Display Name (text box), Employee Number (text box), Employee Type (text box), Enterprise Handle (text box), Given Name (text box), Home Phone (text box), and Home Postal Address (text box).

Next, navigate to **Security > Security Database > List All Users** and select the Calibre user from the list and click **Edit** (not shown). Check the **Unrestricted Access** radio button and **Apply Changes**.

AVAYA Application Enablement Services

Management Console

Welcome: User cust
Last login: Mon Jun 10 14:53:11 2019 from 10.64.10.210
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.6-0
Server Date and Time: Thu Jun 13 12:20:16 MDT 2019
HA Status: Not Configured

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Account Management

Audit

Certificate Management

Enterprise Directory

Host AA

PAM

Security Database

Control

CTI Users

List All Users

Search Users

Devices

Device Groups

Tlinks

Tlink Groups

Worktops

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

Calibre

Calibre

NONE

☒

Call and Device Control:

Call Origination/Termination and Device Status

None

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None

None

☐

Routing Control:

Allow Routing on Listed Devices

None

Apply Changes

Cancel Changes

6.10. Administer Ports

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

In the **DMCC Server Ports** sub-section, select the radio button for **Unencrypted Port** under the **Enabled** column, and make a note of the port value to be used later to configure Calibre. Retain the default values in the remaining fields. Click **Apply Changes** at the bottom of the screen (not shown below).

High Availability ▶ Licensing ▶ Maintenance ▼ Networking AE Service IP (Local IP) Network Configure Ports TCP/TLS Settings ▶ Security ▶ Status ▶ User Management ▶ Utilities ▶ Help	CVLAN Ports			Enabled	Disabled
		Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
		Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>
	<hr/>				
	DLG Port	TCP Port	5678		
	<hr/>				
	TSAPI Ports			Enabled	Disabled
		TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
		Local TLINK Ports			
		TCP Port Min	1024		
		TCP Port Max	1039		
		Unencrypted TLINK Ports			
		TCP Port Min	<input type="text" value="1050"/>		
		TCP Port Max	<input type="text" value="1065"/>		
		Encrypted TLINK Ports			
		TCP Port Min	<input type="text" value="1066"/>		
		TCP Port Max	<input type="text" value="1081"/>		
	<hr/>				
DMCC Server Ports			Enabled	Disabled	
	Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>	
	Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>	
	TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>	

7. Configure HigherGround Calibre

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

- HigherGround VoIP Recorder Configuration
- DMCC Connector Configuration
- Administer VoIP Channels
- Administer Station Utility

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

7.1. HigherGround VoIP Recorder Configuration

The following settings must be changed in the HigherGround VoIP Voice Recorder's configuration file. On the server, launch the Command Prompt, navigate to the master directory (**E:\clu**), and edit the VoIP Recorder's configuration file (**cadclu#.cfg**).

If the following parameters do not exist, enter them under the **[Settings]** section:

[Settings]

SniffIPPort=1

SendRtpKeepalivePeriod=30

VoIPRTPEvenOnly=0

Setting	Definition
SniffIPPort=1	This tells the recorder to allow channels to be defined to IP:PORT rather than just IP address. This is needed when multiple channels terminate at the same address, but on different fixed port numbers.
SendRtpKeepalivePeriod=30	This tells the recorder to send an RTP “keepalive” packet every 30 seconds to the IP:PORT communicating with each channel that is defined on a local IP address.
VoIPRTPEvenOnly=0	This tells the recorder to allow odd ports to be recorded.

Close the file and save all of the configuration changes.

7.2. DMCC Connector Configuration

The HgDMCC Connector is an extension of the HgConnector, so it uses the same kind of configuration file as HgConnector. You can use a clean G3LogFeed.cfg as the base configuration file for HgDMCC connector.

Request **ServiceProvider.dll** file from the HigherGround support team and place it in the master directory (**E:\clu**) on the server. Open the **E:\clu** folder and copy the **G3LogFeed.cfg** file and rename it to **DmccSO.cfg**. Launch Notepad and open the **DmccSO.cfg** configuration file. Under the **[Settings]** section, set:

ConnectionType=DMCCConnection

Under the **[DmccSettings]** section, set:

SwitchName=<switch name> from **Section 6.3**

AesIP=10.64.115.28

AesPort=4721

Username=<user> from **Section 6.9**

Password=<pw> from **Section 6.9**

RecorderIP=10.64.115.32

RecordingMethod=1

Setting	Definition
AesIP=10.64.115.28	The IP address of the AES server.
AesPort=4721	4721 is the default port number if the customer did not change it.
Username=<user> Password=<pw>	From Section 6.9
RecorderIP=10.64.115.32	This is the IP address of the VoIP recorder.
RecordingMethod=1	1 is the DMCC Service Observe.

Continuing from above, under the **[DmccSettings]**, specify the following parameters:

CallingDeviceIndex=2

CalledDeviceIndex=3

AnsweringDeviceIndex=4

AcdGroupIndex=5

CallTypeIndex=6

CallReasonIndex=7

GlobalLinkIdIndex=8

Setting	Definition
CallingDeviceIndex=2	The calling device is stored to Attach2 .
CalledDeviceIndex=3	The calling device is stored to Attach3 .

Under the **[DmccExtensions]** section, set:

Count=n

Extension1=<physical device>:<recording device>:<password>:<port>

Extension2=<physical device>:<recording device>:<password>:<port>

Extensionnn=<physical device>:<recording device>:<password>:<port>

Setting	Definition
Count=n	n is the number of extensions to be recorded.
Extension1=<physical device>: <recording device>:<password>:<port>	<port> is the recorder port specified on a recording channel. In the screenshot on the next page, it is configured to be 20000 .

The following configurations are needed if the customer has agents logging in and out of the phones.

Under the **[DmccAcdGroups]** section, set:

Count=n

AcdGroup1=<huntgroup>:0:0:0

AcdGroup2=<huntgroup>:0:0:0

Close the file and save all of the configuration changes.

7.3. Administer VoIP Channels

From the Calibre server, double click on the **HigherGround Manage** icon, which was created as part of the installation.



Log in using the appropriate credentials.

A login window titled 'HigherGround Calibre - HgManage Login [DEVCONNE-841693]'. It features the Calibre logo on the left, which consists of a blue stylized head profile and the word 'calibre' in blue, with 'setting the standard' in smaller text below it. On the right, there are two input fields: 'User Name:' and 'Password:'. Below these fields are two buttons: 'Log In' and 'Cancel'.

The **HigherGround Calibre Manage – User/Channel Table** screen is displayed next. Select the first **VoIP Channel** entry on the left portion of the screen.

HigherGround Calibre Manage - User/Channel Table

Settings Database Table Utility Run

☒ Show interactive users
☒ Show recorder channels

System ID	Record Type	User Name	S..	Station Name	Trigger	VoIP IP Port	VoIP MAC
S16-AVAYA	VoIP Channel	CLU1-1001	30001	SIP 30001	VoIP	10.64.115.37:500...	00:00:00:00:00:01
S16-AVAYA	VoIP Channel	CLU1-1002	30002	H323 30002	VoIP	10.64.115.37:500...	00:00:00:00:00:02
S16-AVAYA	VoIP Channel	CLU1-1003	30003	SIP 30003	VoIP	10.64.115.37:500...	00:00:00:00:00:03
S16-AVAYA	VoIP Channel	CLU1-1004	30004	H323 30004	VoIP	10.64.115.37:500...	00:00:00:00:00:04
S16-AVAYA	VoIP Channel	CLU1-1005	30005	DCP 30005	VoIP	10.64.115.37:500...	00:00:00:00:00:05
S16-AVAYA	VoIP Channel	CLU1-1006	30006	SIP 30006	VoIP	10.64.115.37:500...	00:00:00:00:00:06

< >

Home Add Remove Copy Apply To Report Export

In the right portion of the screen shown below, enter the following values for the specified fields in the **Connection** sub-section, and retain the default values for the remaining fields.

- **Station:** The first agent station extension from **Section 3**.
- **VoIP IP:** IP address of Calibre server running the Recorder component.
- **Port:** An RTP port number for the station.

Identification	
Record Type:	VoIP Channel
Recorder Unit:	1
User Name:	CLU1-1002
Channel:	1002
Recording Group:	Automatic
Location:	
System ID:	S16-AVAYA
Connection	
Station:	30002
Picker:	30002
Station Name:	H323 30002
Department Number:	0
Division Number:	0
VoIP IP:	10.64.115.37
Port:	50002 0 0
VoIP MAC:	00:00:00:00:00:00
Record Settings	
Trigger Type:	VOX
<input checked="" type="checkbox"/> Record Incoming	<input type="checkbox"/> Monitor Only
<input checked="" type="checkbox"/> Record Outgoing	
Light Mask:	None
Single Appearance Mask:	None
<input type="checkbox"/> Create Virtual Channels For Line Appearances	
Record Gain:	0
Silence Trunc:	0
VOX Gain:	0
VOX Stop:	0
Centralized Voice Recording	
Record Schedule:	All
Save Cancel Play Monitor History	

Repeat this section to administer a VoIP channel for each agent station extension from **Section 3**. In the compliance testing, VoIP channels were configured as shown below.

HigherGround Calibre Manage - User/Channel Table

Settings Database Table Utility Run

☒ Show interactive users
☒ Show recorder channels

System ID	Record Type	User Name	S...	Station Name	Trigger	VoIP IP Port	VoIP MAC
S16-AVAYA	VoIP Channel	CLU1-1001	30001	SIP 30001	VoIP	10.64.115.37:500...	00:00:00:00:00:0
S16-AVAYA	VoIP Channel	CLU1-1002	30002	H323 30002	VoIP	10.64.115.37:500...	00:00:00:00:00:0
S16-AVAYA	VoIP Channel	CLU1-1003	30003	SIP 30003	VoIP	10.64.115.37:500...	00:00:00:00:00:0
S16-AVAYA	VoIP Channel	CLU1-1004	30004	H323 30004	VoIP	10.64.115.37:500...	00:00:00:00:00:0
S16-AVAYA	VoIP Channel	CLU1-1005	30005	DCP 30005	VoIP	10.64.115.37:500...	00:00:00:00:00:0
S16-AVAYA	VoIP Channel	CLU1-1006	30006	SIP 30006	VoIP	10.64.115.37:500...	00:00:00:00:00:0

< >

Home Add Remove Copy Apply To Report Export

7.4. Administer Station Utility

Select **Utility** → **Station Utility** from the top menu to display the **HigherGround Calibre Manager – Station Utility** screen. Click **Add** in the bottom left portion of the screen.

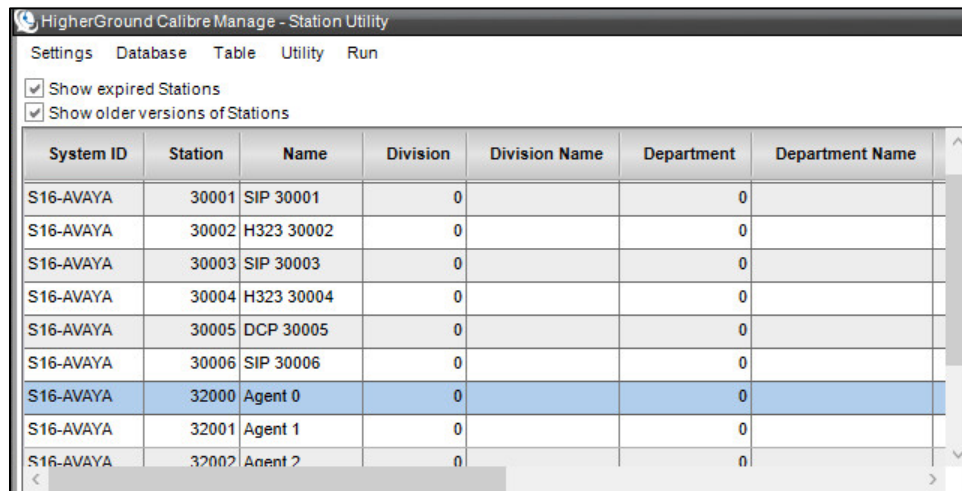
System ID	Station	Name	Division	Division Name	Department	Department Name
S16-AVAYA	30001	SIP 30001	0		0	
S16-AVAYA	30002	H323 30002	0		0	
S16-AVAYA	30003	SIP 30003	0		0	
S16-AVAYA	30004	H323 30004	0		0	
S16-AVAYA	30005	DCP 30005	0		0	
S16-AVAYA	30006	SIP 30006	0		0	

In the right portion of the screen shown below, enter the following values for the specified fields in the **General Settings** sub-section, and retain the default values for the remaining fields.

- **Station No:** The first agent station extension from **Section 3**.
- **Station Name:** A desired station name.

In a similar fashion, create Agents in the same table:

Repeat this section to create an entry for each agent and station from **Section 3**. In the compliance testing, station utility entries were configured as shown below.



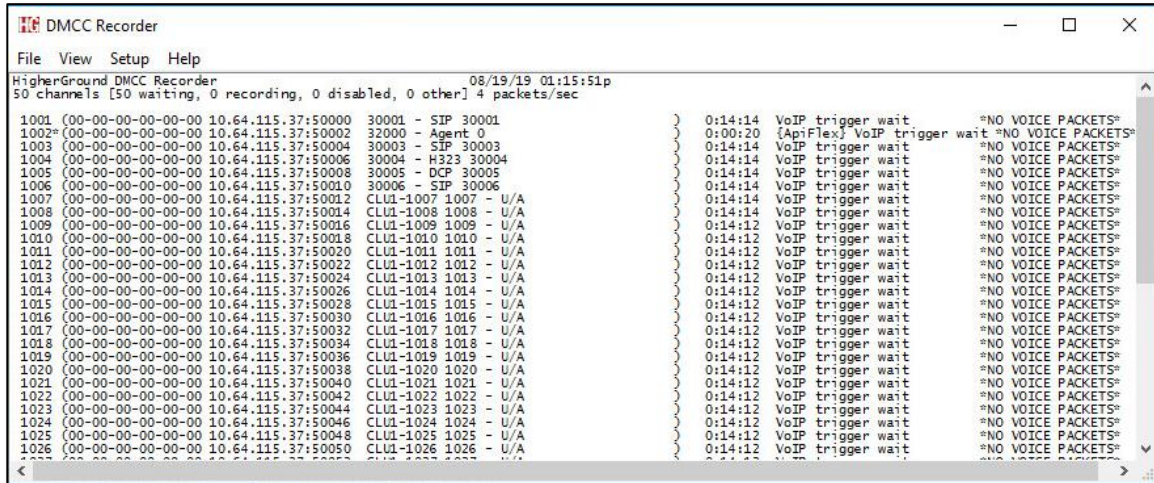
The screenshot shows a software window titled "HigherGround Calibre Manage - Station Utility". It has a menu bar with "Settings", "Database", "Table", "Utility", and "Run". Below the menu bar are two checked checkboxes: "Show expired Stations" and "Show older versions of Stations". The main area contains a table with the following columns: System ID, Station, Name, Division, Division Name, Department, and Department Name. The table lists several entries, with the last three entries (Agent 0, Agent 1, and Agent 2) highlighted in blue. The table is scrollable, as indicated by the vertical scrollbar on the right.

System ID	Station	Name	Division	Division Name	Department	Department Name
S16-AVAYA	30001	SIP 30001	0		0	
S16-AVAYA	30002	H323 30002	0		0	
S16-AVAYA	30003	SIP 30003	0		0	
S16-AVAYA	30004	H323 30004	0		0	
S16-AVAYA	30005	DCP 30005	0		0	
S16-AVAYA	30006	SIP 30006	0		0	
S16-AVAYA	32000	Agent 0	0		0	
S16-AVAYA	32001	Agent 1	0		0	
S16-AVAYA	32002	Agent 2	0		0	

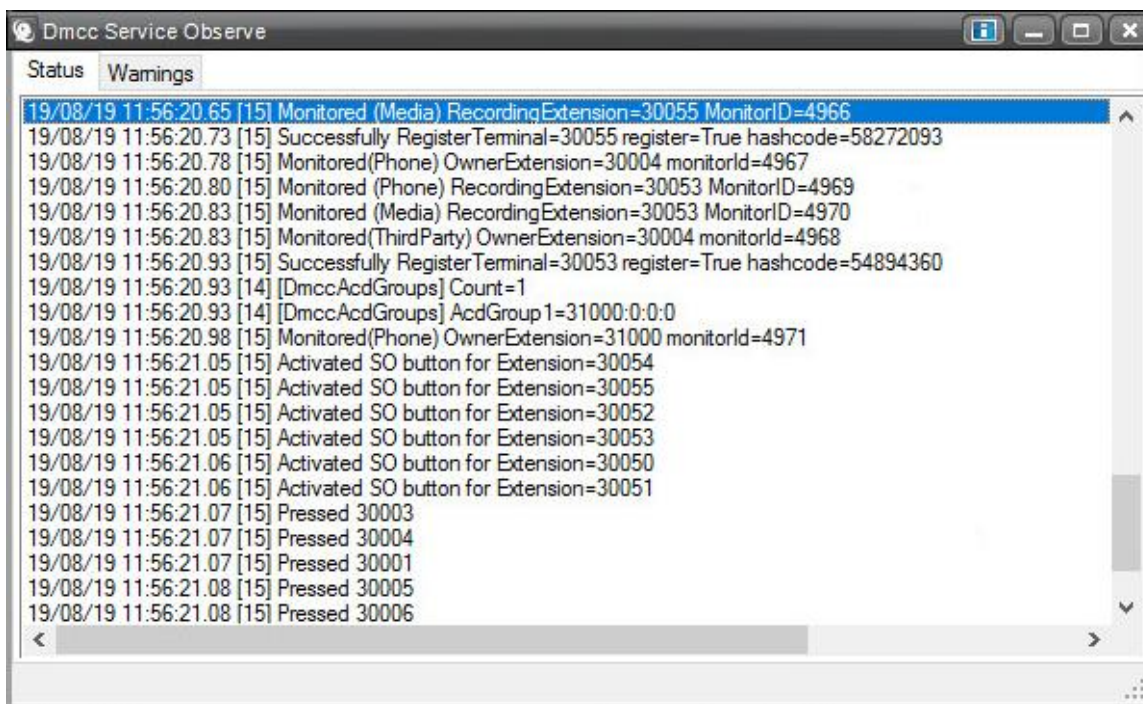
8. Verification Steps

8.1. Higher Ground Calibre

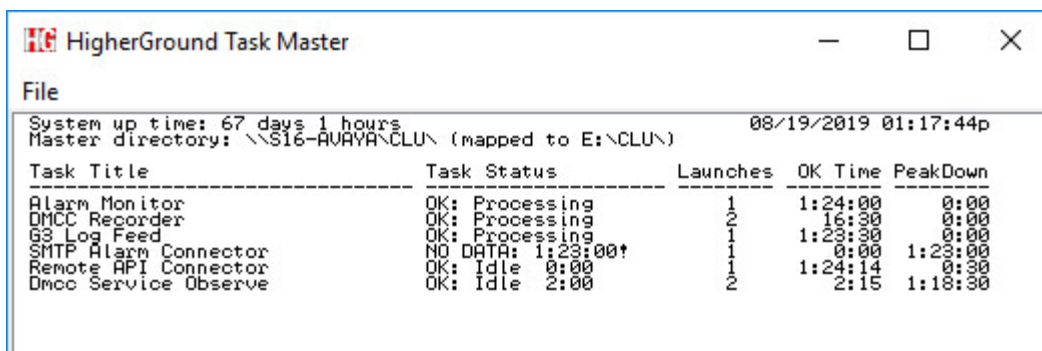
On the HigherGround Calibre server, the **DMCC Recorder** application as shown below will summarize the status of recording ports. If an Agent is logged in to a station, the Agent name will appear in place to the station. In this view, Agent 0 is logged in to station 30002, the remaining stations have no logged in agent.



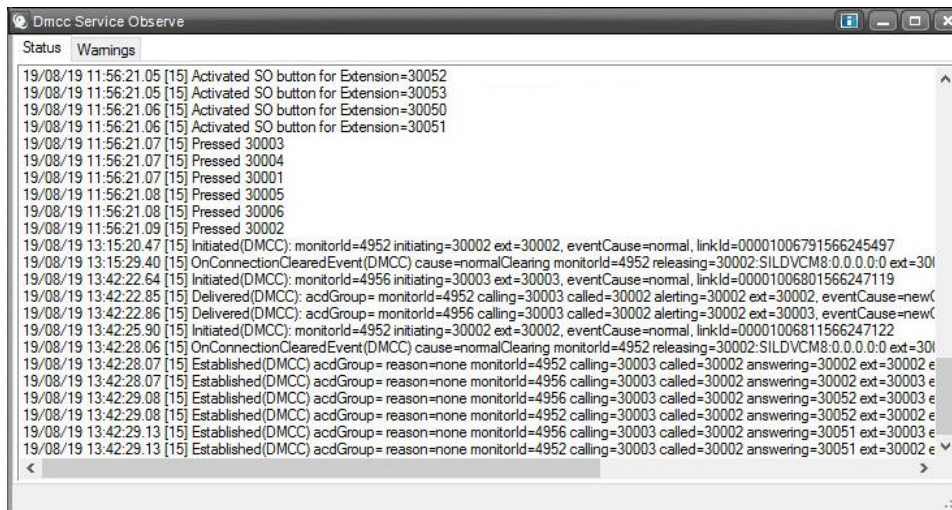
The **DMCC Service Observe** application window will show recent DMCC activity.



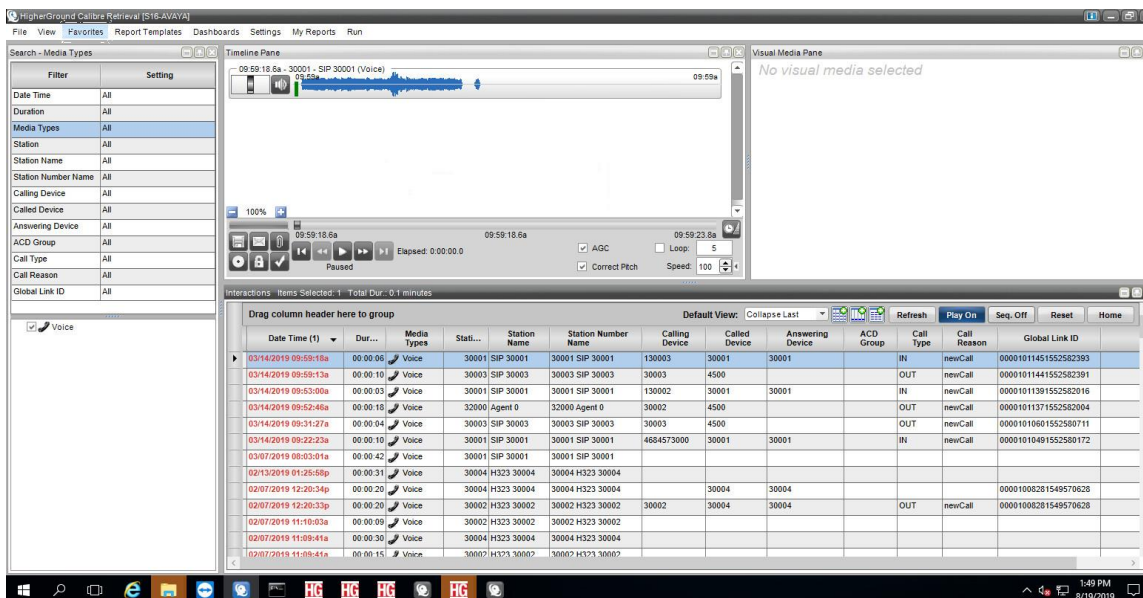
The **HigherGround Task Master** is an application that shows the health of all of the recorder processes, and acts as a watchdog to restart any failed processes.



When calls arrive at target stations, call event data will appear in the **DMCC Service Observe** application window.



Use a web browser to login to the **HigherGround Calibre Retrieval** interface to query for, and replay recordings.



8.2. Communication Manager

On Communication Manager, use the **list monitored-station** command to confirm TSAPI that the application is registered for event notification on agent stations.

```
list monitored-station

MONITORED STATION

Associations:      1      2      3      4      5      6      7      8
                   CTI     CTI     CTI     CTI     CTI     CTI     CTI     CTI
Station Ext      Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV
-----
30001             1  000A
30002             1  0006
30003             1  0008
30004             1  000D
30005             1  0001
30006             1  0004

Command successfully completed
Command:
ESC-x=Cancel ESC-e=Submit ESC-p=Prev Pg ESC-n=Next Pg ESC-h=Help ESC-r=Refresh
```

Use the **status station** command to view RTP connections and codecs with an active call. The display below illustrates a call connected to the Calibre server (10.64.115.37) on port 50004 with g711 mulaw and no encryption. The station is connected to the media gateway (10.64.115.2) with g729a and SRTP.

```
status station 30002                                     Page 9 of 11
SRC PORT TO DEST PORT TALKPATH
src port: S00005
S00005:TX:10.64.115.36:2982/g729a/20ms/1-ertp-aescm128-hmac80
001V012:RX:10.64.115.2:2052/g729/20ms/1-ertp-aescm128-hmac80;TX:ctxID:280
001V011:RX:ctxID:280;TX:10.64.115.2:2056/g711u/20ms
S00023:RX:10.64.115.37:50004/g711u/20ms

dst port: S00023

ESC-x=Cancel ESC-e=Submit ESC-p=Prev Pg ESC-n=Next Pg ESC-h=Help ESC-r=Refresh
```

Note that to view RTP connections with a SIP station, use the status trunk commands.

8.3. Application Enablement Services

On Application Enablement Services, navigate to the **Status > Status and Control > DMCC Service Summary**. On the **Device Summary** page, verify the recorder has registered for events on agent stations (state will display **IDLE**), and virtual extensions for recording:

The screenshot shows the AVAYA Application Enablement Services Management Console. The top navigation bar includes 'Status | Status and Control | DMCC Service Summary' and 'Home | Help | Logout'. The left sidebar lists various services, with 'Status and Control' expanded to show 'DMCC Service Summary'. The main content area displays the 'DMCC Service Summary - Device Summary' page. It includes a 'Please do not use back button' warning, a refresh button, and a 'Session Summary' section. The 'Session Summary' section shows the service uptime and statistics. Below this is a table of devices with columns for Device ID, Gatekeeper IP address, State, and Associated Sessions.

Device ID	Gatekeeper IP address	State	Associated Sessions
30001:SILDVCM8:0.0.0.0:0	N/A	IDLE	1
30002:SILDVCM8:0.0.0.0:0	N/A	IDLE	1
30003:SILDVCM8:0.0.0.0:0	N/A	IDLE	1
30004:SILDVCM8:0.0.0.0:0	N/A	IDLE	1
30005:SILDVCM8:0.0.0.0:0	N/A	IDLE	1
30006:SILDVCM8:0.0.0.0:0	N/A	IDLE	1
30050:SILDVCM8:0.0.0.0:0	10.64.115.25	REGISTERED	1
30051:SILDVCM8:0.0.0.0:0	10.64.115.25	REGISTERED	1
30052:SILDVCM8:0.0.0.0:0	10.64.115.25	REGISTERED	1
30053:SILDVCM8:0.0.0.0:0	10.64.115.25	REGISTERED	1
30054:SILDVCM8:0.0.0.0:0	10.64.115.25	REGISTERED	1
30055:SILDVCM8:0.0.0.0:0	10.64.115.25	REGISTERED	1
31000:SILDVCM8:0.0.0.0:0	N/A	IDLE	1

On the **Session Summary** page, the Calibre user can be confirmed, in this case using an unencrypted XML session with the DMCC service.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top navigation bar includes 'Status | Status and Control | DMCC Service Summary' and 'Home | Help | Logout'. The left sidebar lists various services, with 'Status and Control' expanded to show 'DMCC Service Summary'. The main content area displays the 'DMCC Service Summary - Session Summary' page. It includes a 'Please do not use back button' warning, a refresh button, and a 'Session Summary' section. The 'Session Summary' section shows the service uptime and statistics. Below this is a table of sessions with columns for Session ID, User, Application, Far-end Identifier, Connection Type, and # of Associated Devices.

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
0466745BCDCF8074 2AC0CBC75DE911F-659	calibre	HgDMCC	10.64.115.37	XML Unencrypted	13

9. Conclusion

These Application Notes describe the configuration steps required for HigherGround Calibre to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services to record audio calls. The solution passed all compliance test cases successfully, please refer to **Section 2.2** for results and any observations.

10. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at <http://support.avaya.com>.

Avaya:

1. *Administering Avaya Aura® Communication Manager*, Release 8.0.x Issue 4, May 2019
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.0.x Issue 3, August 2019

©2019 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.