



## **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 8.9.5 to interoperate with Avaya Aura® Communication Manager 7.0.1 using Avaya Aura® Application Enablement Services 7.0.1.

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 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 0**, 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 8.9.5 to interoperate with Avaya Aura® Communication Manager 7.0.1 using Avaya Aura® Application Enablement Services 7.0.1.

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

When there is an active call on the monitored agent, HigherGround Calibre is informed of the call via event reports from the DMCC interface. HigherGround Calibre starts the call recording by using the Service Observing feature from the DMCC interface to add a virtual IP softphone to the active call 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 the Calibre application, the application automatically uses DMCC to register the virtual IP softphones to Communication Manager, and to request monitoring on the skill groups and agent station extensions.

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 Ethernet 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.

## 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 groups, agent stations, and virtual IP softphones.
- Use of DMCC call 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, transfer and long call duration.

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 hold and resume is used with a new record created in Calibre Recording table. For example, if an agent places a call on hold and then reconnects, there would be two recording entries generated for the call.

## 2.3 Support

Technical support on Calibre can be obtained through the following:

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

### 3 Reference Configuration

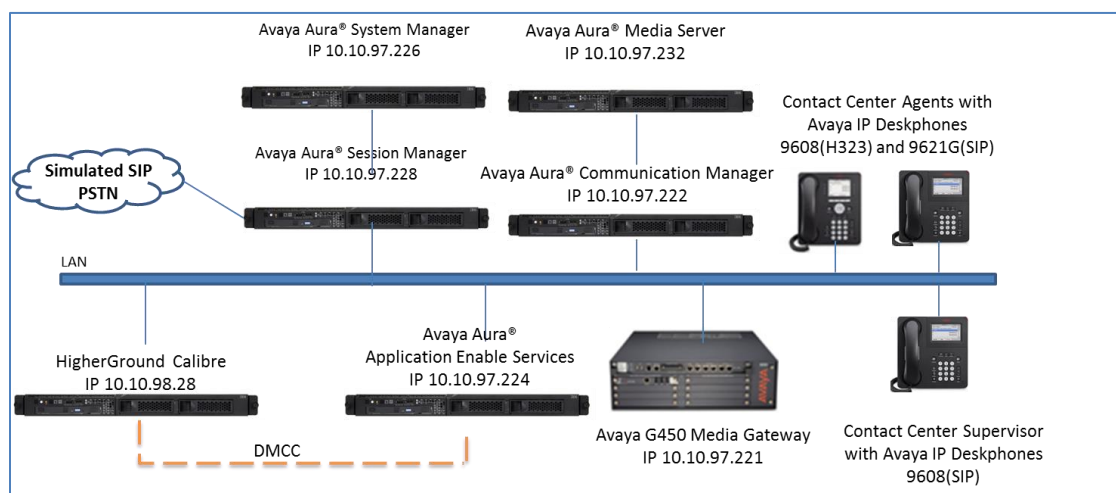
Calibre can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration shown in **Figure 1**.

Calibre has a Retrieval application that can be used to review and playback the call recordings. In the compliance testing, the supervisor has a shortcut to the Retrieval application that physically resides on the Calibre server.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, the contact center devices consisted of two VDNs, two skill groups, one supervisor, and two agents as shown in the table below. Calibre requested monitoring on the skill groups and on both agent station extensions.

Device Type	Extension
VDN	56001, 56010
Skill/Hunt Group	56300, 56303
Agent ID	1000, 1004
Agent Station	56201, 56101
Supervisor Station	56202



**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	7.0.1.1.1 SP1.1
Avaya G450 Media Gateway	7.0.1.1
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 Super Patch 3
Avaya 9608G IP Deskphone (H.323)	6.6229
Avaya 9608, 9621G IP Deskphone (SIP)	7.0.1.1.5
Avaya Aura® Session Manager	7.0.1.1
Avaya Aura® System Manager	7.0.1 SP1
HigherGround Calibre on Windows 2012R2 Server <ul style="list-style-type: none"><li>DMCC Integrator Service</li><li>Avaya DMCC .NET (ServiceProvider.dll)</li></ul>	8.9.5 SP 2 8.95.0.1 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 class of restriction
- Administer CTI link
- Administer system parameters features
- Administer Agent Station
- 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. 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.

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

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

(NOTE: You must logoff & login to effect the permission changes.)
```

Navigate to **Page 7**, and verify **Service Observing (Basic)** is set to “y”.

```
display system-parameters customer-options                               Page 7 of 12
CALL CENTER OPTIONAL FEATURES

Call Center Release: 7.0

ACD? y                                Reason Codes? y
BCMS (Basic)? y                      Service Level Maximizer? n
BCMS/VuStats Service Level? y        Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y  Service Observing (Remote/By FAC)? y
Business Advocate? n                 Service Observing (VDNs)? y
Call Work Codes? y                   Timed ACW? y
DTMF Feedback Signals For VRU? y      Vectoring (Basic)? y
Dynamic Advocate? n                  Vectoring (Prompting)? y
Expert Agent Selection (EAS)? y        Vectoring (G3V4 Enhanced)? y
EAS-PHD? y                           Vectoring (3.0 Enhanced)? y
Forced ACD Calls? n                  Vectoring (ANI/II-Digits Routing)? y
Least Occupied Agent? y               Vectoring (G3V4 Advanced Routing)? y
Lookahead Interflow (LAI)? y          Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y  Vectoring (Best Service Routing)? y
Multiple Call Handling (Forced)? y      Vectoring (Holidays)? y
PASTE (Display PBX Data on Phone)? y   Vectoring (Variables)? y
(NOTE: You must logoff & login to effect the permission changes.)
```

## 5.2 Administer Class of Restriction

Use the “change cor n” command, where “n” is the class of restriction (COR) number to be assigned to the target stations that will be recorded, in this case it is 1, set the **Can Be Service Observed** field to “y” as shown below.

During compliance test, the same COR was assigned to the virtual IP softphones used by Calibre, set the **Can Be A Service Observer** field to “y” as shown below.

change cor 1	Page 1 of 23
CLASS OF RESTRICTION	
COR Number: 1	
COR Description:	
FRL: 1	APLT? y
<b>Can Be Service Observed? y</b>	Calling Party Restriction: none
<b>Can Be A Service Observer? y</b>	Called Party Restriction: none
Time of Day Chart: 1	Forced Entry of Account Codes? n
Priority Queuing? n	Direct Agent Calling? n
Restriction Override: all	Facility Access Trunk Test? n
Restricted Call List? n	Can Change Coverage? n
Access to MCT? y	Fully Restricted Service? n
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n
Send ANI for MFE? n	Add/Remove Agent Skills? n
MF ANI Prefix:	Automatic Charge Display? n
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n
Can Be Picked Up By Directed Call Pickup? y	Can Use Directed Call Pickup? y
	Group Controlled Restriction: inactive

## 5.3 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. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1	Page 1 of 3
CTI LINK	
CTI Link: 1	
Extension: 56001	
Type: ADJ-IP	
COR: 1	
Name: DevvmAES	



## 5.4 Administer System Parameters Features

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: 1
```

Navigate to **Page 11**, set **Service Observing: Warning Tone** to the desired setting per customer requirements, and set **Allow Two Observers in Same Call** to “y”.

```
display system-parameters features                                 Page 11 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER SYSTEM PARAMETERS
  EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length:
    Direct Agent Announcement Extension:          Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
    Converse First Data Delay: 0          Second Data Delay: 2
    Converse Signaling Tone (msec): 100    Pause (msec): 70
    Prompting Timeout (secs): 10
    Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
    Available Agent Adjustments for BSR? n
    BSR Tie Strategy: 1st-found
    Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
    Service Observing: Warning Tone? y    or Conference Tone? n
    Allowed with Exclusion: Service Observing? n    SSC? n
    Allow Two Observers in Same Call? y
```

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 UII 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
```

## 5.5 Administer Agent Station

Modify each agent's station to allow the station to be service observed. Use the "change station n" command, where "n" is the station extension, and change the **COR** field to "1" as defined in **Section 5.2**.

Repeat this section for all agent stations. In the interoperability test, two agent stations "56101" and "56201" were modified.

```
display station 56101                                             Page 1 of 5
      STATION
Extension: 56101          Lock Messages? n          BCC: 0
      Type: 9608          Security Code: *          TN: 1
      Port: S00000        Coverage Path 1: 2        COR: 1
      Name: StationNameOneOOne    Coverage Path 2:    COS: 1
      Hunt-to Station:          Tests? y

STATION OPTIONS
      Loss Group: 19          Time of Day Lock Table:
      Speakerphone: 2-way    Personalized Ringing Pattern: 1
      Display Language: english    Message Lamp Ext: 56101
      Survivable GK Node Name:    Mute Button Enabled? y
      Survivable COR: internal    Button Modules: 0
      Survivable Trunk Dest? y    Media Complex Ext:
      Short/Prefixed Registration Allowed: default    IP SoftPhone? y
      Customizable Labels? y    IP Video Softphone? n
```

## 5.6 Administer SIP Agent Station

It is assume that SIP Agent station already in place. In order for third party records media on SIP station, verify SIP station has **Type of 3PCC Enable** set to Avaya as display below.

Note: Proper procedure to update this parameter for SIP Endpoint is on System Manager → User Management.

```
change station 56201                               Page   6 of   6
                                                    STATION
SIP FEATURE OPTIONS
    Type of 3PCC Enabled: Avaya
    SIP Trunk: aar
Enable Reachability for Station Domain Control: s
```

## 5.7 Administer Virtual IP Softphones

Virtual IP softphones are used by Calibre to service observe target stations and capture media. 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 “9620”.
- **Name:** A descriptive name.
- **Security Code:** A desired code, for example: 1234.
- **COR:** Enter COR from **Section 5.2**.
- **IP SoftPhone:** “y”.

```
add station 56114
                                                    STATION
Extension: 56114                               Lock Messages? n           BCC: 0
Type: 9620                                     Security Code: 1234       TN: 1
Port: S00067                                     Coverage Path 1:          COR: 1
Name: Calibre Virtual #1                     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: 56114
Speakerphone: 2-way                             Mute Button Enabled? y
Display Language: english                       Expansion Module? n
                                                    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
```

Navigate to **Page 4**, and configure a **serv-obsrv** button as shown below.

change station 56114		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		4: <b>serv-obsrv</b>	
2: call-appr		5:	
3: call-appr		6:	
voice-mail			

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

list station 56114 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack		
<b>56114</b>	<b>S00067</b>	<b>Calibre Virtual #1</b>				<b>1</b>			
	<b>9620</b>		<b>no</b>			<b>1</b>	<b>1</b>		
<b>56115</b>	<b>S00070</b>	<b>Calibre Virtual #2</b>				<b>1</b>			
	<b>9620</b>		<b>no</b>			<b>1</b>	<b>1</b>		

## 6 Configure Avaya Aura® Application Enablement Services

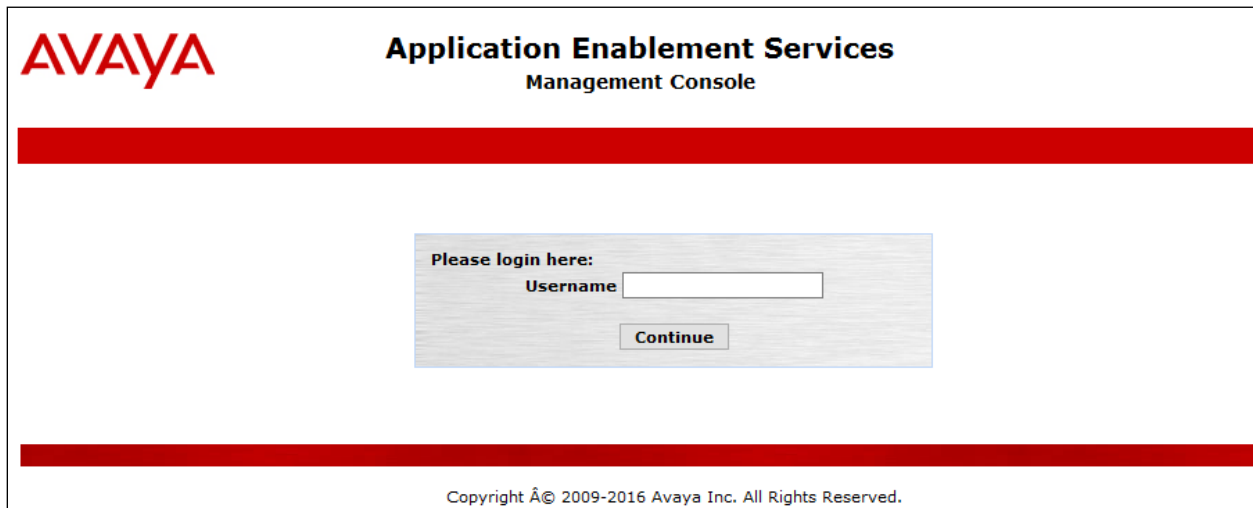
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- 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 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 thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. Another thick red horizontal bar is located at the bottom of the page, just above the footer. The footer text at the very bottom reads "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

The **Welcome to OAM** screen is displayed as below:

The screenshot shows the AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo, the title "Application Enablement Services Management Console", and system information: "Number of prior failed login attempts: 1", "HostName/IP: devvmaes/135.10.97.224", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 7.0.1.0.3.15-0", "Server Date and Time: Wed Mar 22 22:01:33 EDT 2017", and "HA Status: Not Configured". A red navigation bar contains "Home", "Help", and "Logout". On the left, a sidebar lists menu items: 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:" followed by a bulleted list of domains and their functions.

**AVAYA** Application Enablement Services Management Console

Number of prior failed login attempts: 1  
HostName/IP: devvmaes/135.10.97.224  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.3.15-0  
Server Date and Time: Wed Mar 22 22:01:33 EDT 2017  
HA Status: Not Configured

Home | Help | Logout

Home

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.

## 6.2 Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager**.

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Licensing" menu item selected in the sidebar. The top header is identical to the previous screenshot. The red navigation bar now shows "Licensing", "Help", and "Logout". The sidebar menu has "Licensing" highlighted. The main content area is titled "Licensing" and contains instructions for setting up and maintaining the WebLM, including a list of required items: WebLM Server Address, WebLM Server Access, and Reserved Licenses. A red note at the bottom states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page".

**AVAYA** Application Enablement Services Management Console

Welcome: User cust  
Last login: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwddev.com  
Number of prior failed login attempts: 0  
HostName/IP: devvmaes/135.10.97.224  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.2.15-0  
Server Date and Time: Tue Nov 15 13:13:32 EST 2016  
HA Status: Not Configured

Licensing | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
WebLM Server Address  
WebLM Server Access  
Reserved Licenses  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

**Licensing**

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

**NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page**

The screen below is displayed. 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.

WebLM Home

Install license

Licensed products

APPL\_ENAB

▼ Application\_Enablement

View license capacity

View peak usage

CCTR

►ContactCenter

CE

►COLLABORATION\_ENVIRONMENT

CIE

►CIE

COMMUNICATION\_MANAGER

►Call\_Center

►Communication\_Manager

Configure Centralized Licensing

MESSAGING

►Messaging

PRESENCE\_SERVICES

Application Enablement (CTI) - Release: 7 - SID: 10503000

Stat

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

License installed on: October 13, 2015 6:25:48 AM -04:00

License File Host IDs:

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

## 6.3 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 screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays a welcome message for user 'cust' and system information: 'Last login: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwdev.com', 'Number of prior failed login attempts: 0', 'HostName/IP: devvmaes/135.10.97.224', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.1.0.2.15-0', 'Server Date and Time: Tue Nov 15 13:19:29 EST 2016', and 'HA Status: Not Configured'. The main navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded, containing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), 'TSAPI Links' (highlighted), 'TSAPI Properties', and 'TWS'. The main content area is titled 'TSAPI Links' and contains a table with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	DevvmCM	1	7	Both

Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “DevvmCM” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section Error! Reference source not found..**

The screenshot shows the AVAYA Application Enablement Services Management Console with the 'Edit TSAPI Links' screen. The top right corner displays a welcome message for user 'cust' and system information: 'Last login: Mon Nov 21 12:09:40 2016 from 10.10.10.98.75', 'Number of prior failed login attempts: 0', 'HostName/IP: devvmaes/135.10.97.224', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.1.0.2.15-0', 'Server Date and Time: Mon Nov 21 12:58:50 EST 2016', and 'HA Status: Not Configured'. The main navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded, containing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), 'TSAPI Links' (highlighted), 'TSAPI Properties', and 'TWS'. The main content area is titled 'Edit TSAPI Links' and contains the following form fields:

- Link: 1
- Switch Connection: DevvmCM (dropdown)
- Switch CTI Link Number: 1 (dropdown)
- ASAI Link Version: 7 (dropdown)
- Security: Both (dropdown)

Below the form fields are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.



## 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 “DevvmCM”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

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

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, and click **Add Name or IP**. The H.323 gatekeeper used in the compliance testing is shown below.

**Edit H.323 Gatekeeper - DevvmCM**

**Add Name or IP**


Name or IP Address

☒ 10.10.97.222

**Delete IP** **Back**

## 6.5 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**.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Nov 15 13:56:37 2016 from 135.10.98.75  
Number of prior failed login attempts: 0  
HostName/IP: devvmaes/135.10.97.224  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.2.15-0  
Server Date and Time: Tue Nov 15 13:57:21 EST 2016  
HA Status: Not Configured

Security | Security Database | ControlHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service

☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

## 6.6 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**.

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

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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

## 6.7 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).

**User Management | User Admin | List All Users**

**Edit User**

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

## 6.8 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).

<b>High Availability</b>	CVLAN Ports			Enabled Disabled
▶ Licensing	Unencrypted TCP Port	9999		<input checked="" type="radio"/> <input type="radio"/>
▶ Maintenance	Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/> <input type="radio"/>
▼ Networking				
AE Service IP (Local IP)	DLG Port	TCP Port	5678	
Network Configure				
Ports				
TCP/TLS Settings				
▶ Security	TSAPI Ports			Enabled Disabled
▶ Status	TSAPI Service Port	450		<input checked="" type="radio"/> <input type="radio"/>
▶ User Management	Local TLINK Ports			
▶ Utilities	TCP Port Min	1024		
▶ Help	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"/>		
	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

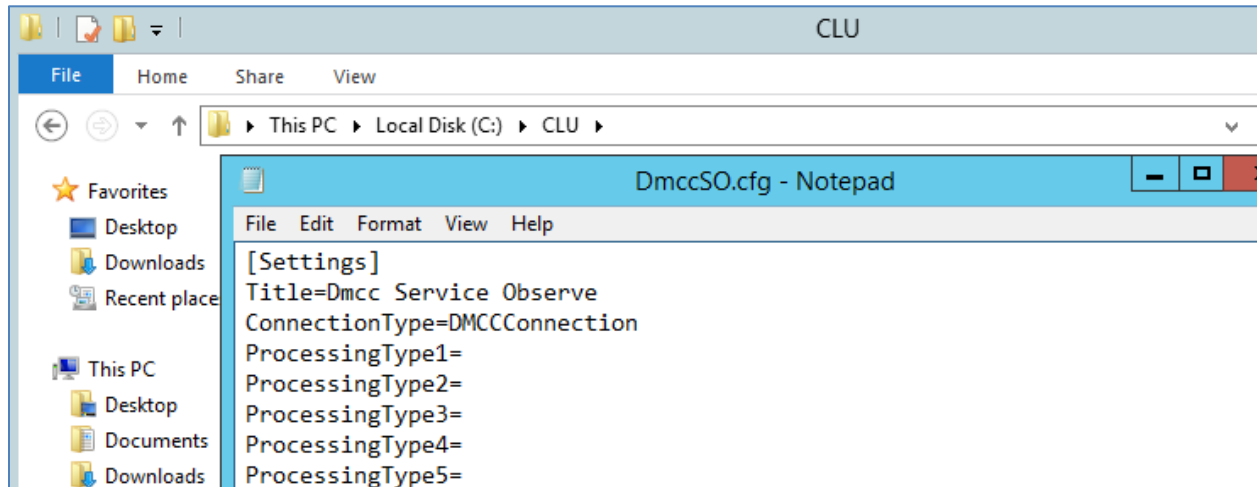
This section provides the procedures for configuring Calibre. The procedures include the following areas:

- Administer DMCC Connector
- 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.

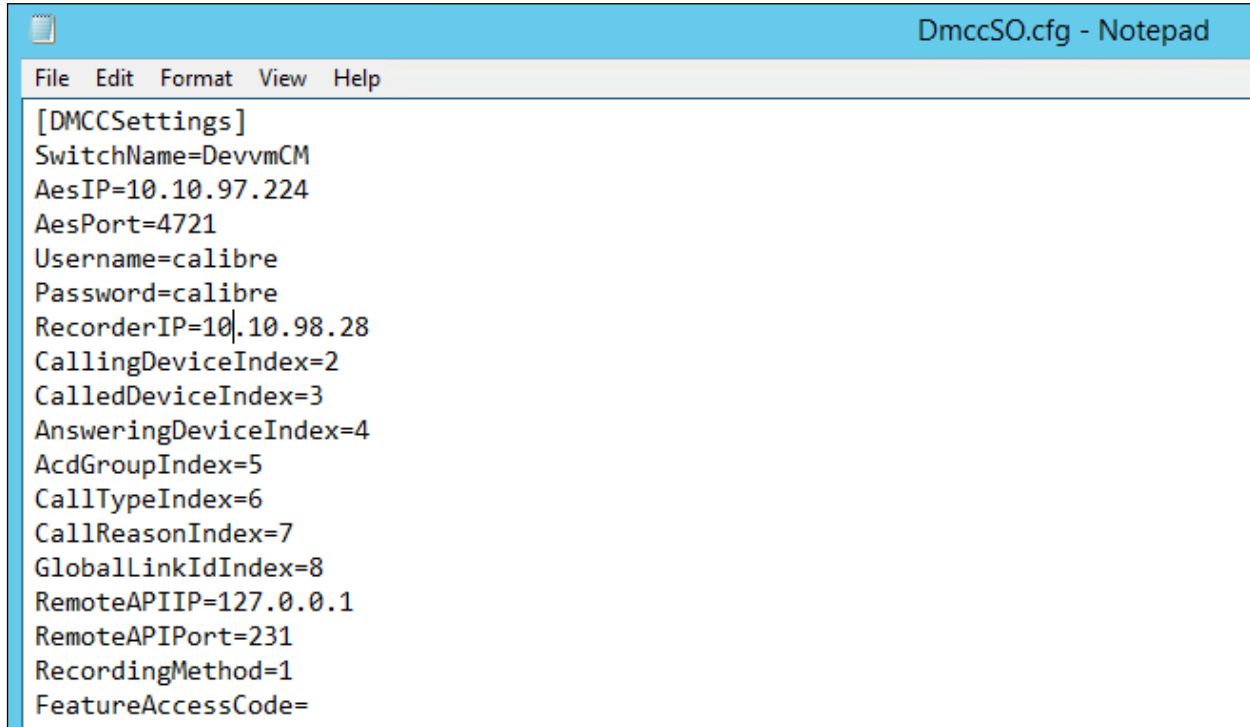
### 7.1 Administer DMCC Connector

On Calibre server, in **C:\clu** folder modify **DmccSO.cfg** using Notepad as shown below. In **[Settings]** section, set **ConnectionType** to “DMCCConnection”.



Navigate to the **[DmccSettings]** section, and set the following:

- **SwitchName:** Enter switch connection name from **Section 6.3**.
- **AesIP:** Enter IP address of Application Enablement Service.
- **AesPort:** Enter DMCC unencrypted port number from **Section 6.8**.
- **Username:** Enter Calibre user name as created in **Section 6.7**.
- **Password:** Enter Calibre user password as created in **Section 6.7**.
- **RecorderIP:** Enter IP address of Calibre server.
- **RecordingMethod:** Enter “1” as Service Observer method.



```
[DMCCSettings]
SwitchName=DevvmCM
AesIP=10.10.97.224
AesPort=4721
Username=calibre
Password=calibre
RecorderIP=10.10.98.28
CallingDeviceIndex=2
CalledDeviceIndex=3
AnsweringDeviceIndex=4
AcdGroupIndex=5
CallTypeIndex=6
CallReasonIndex=7
GlobalLinkIdIndex=8
RemoteAPIIP=127.0.0.1
RemoteAPIPort=231
RecordingMethod=1
FeatureAccessCode=
```

Navigate to the **[DmccExtensions]** section, and set the following:

- **Count:** Enter number of extensions to be recorded, in this case “3”.
- **Extension1:** Enter <physical device>:<recording device>:<password>:<port> where <physical device> is an agent station extension, <recording device> is an available virtual extension created in **Section 5.7**, <password> is the password of the applicable virtual extensions from **Section 5.7**, <port> is the an available recorder port, see screenshot below for configuration used in the compliance testing.
- **Extension2:** Enter <physical device>:<recording device>:<password>:<port>.

```
[DmccExtensions]
Count=3
Extension1=56101:56115:1234:50000
Extension2=56201:56114:1234:50002
Extension3=
```

Navigate to the **[DmccAcidGroups]** section, and set the following:

- **Count:** The number of VDNs in **Section 3**.
- **AcidGroup1:** <vdn>:0:0:0, enter the first VDN extension from **Section 3**.
- **AcidGroup2:** <vdn>:0:0:0, enter the second VDN extension from **Section 3**.

Close the file and save all of the configuration changes.

```
[DmccAcidGroups]
Count=2
AcidGroup1=56001:0:0:0
AcidGroup2=56010:0:0:0
```

## 7.2 Administer VoIP Channels

From the Calibre server running the Control Tower application, double click on the **HigherGround Control Tower** icon, which was created as part of installation.



The **HigherGround Calibre** screen is displayed. Log in using the appropriate credentials.

The login window has a title bar with the text "HigherGround Calibre - HgManage Login [DEVCONNE-841693]". On the left is the Calibre logo, which consists of a blue stylized head profile with a white earpiece and the word "calibre" in blue, with the tagline "setting the standard" below it. On the right, there are two input fields: "User Name:" and "Password:". Below these fields are two buttons: "Log In" and "Cancel".

Field	Value
User Name	
Password	

The **HigherGround Calibre Manage – User/Channel Table** screen is displayed next. Select the first **VoIP Channel** entry on the left portion of the screen. For security reasons, the public IP addresses are masked in the screen below.

HigherGround Calibre Manage - User/Channel Table								
Settings Database Table Utility Run								
<input 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	VoIP MAC
2012PC4	VoIP Channel	CLU1-001	56101	Extension 1		VoIP	1 6.10.98.28:50000	00:00:00:00:00:00
2012PC4	VoIP Channel	CLU1-002	56201	Extension 2		VoIP	1 6.10.98.28:50002	00:00:00:00:00:00
2012PC4	VoIP Channel	CLU1-003	3			VoIP	1 6.10.98.28:50004	00:00:00:00:00:00
2012PC4	VoIP Channel	CLU1-004	4			VoIP	1 6.10.98.28:50006	00:00:00:00:00:00
2012PC4	VoIP Channel	CLU1-005	5			VoIP	1 6.10.98.28:50008	00:00:00:00:00:00
2012PC4	VoIP Channel	CLU1-006	6			VoIP	1 6.10.98.28:50010	00:00:00:00:00:00



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:** Enter agent station extension from **Section 3**.
- **VoIP IP:** IP address of Calibre server running the Recorder component.
- **Port:** The corresponding RTP port number for the agent from **Section 7.1**.

The screenshot shows the 'Connection' configuration window. It includes the following fields and values:

- Station:** 56101
- Station Name:** Extension 1
- Department Number:** 0
- Division Number:** 0
- VoIP IP:** 10.10.98.28
- VoIP MAC:** 00:00:00:00:00:00
- Port:** 50000, 0, 0
- Picker:** 56101

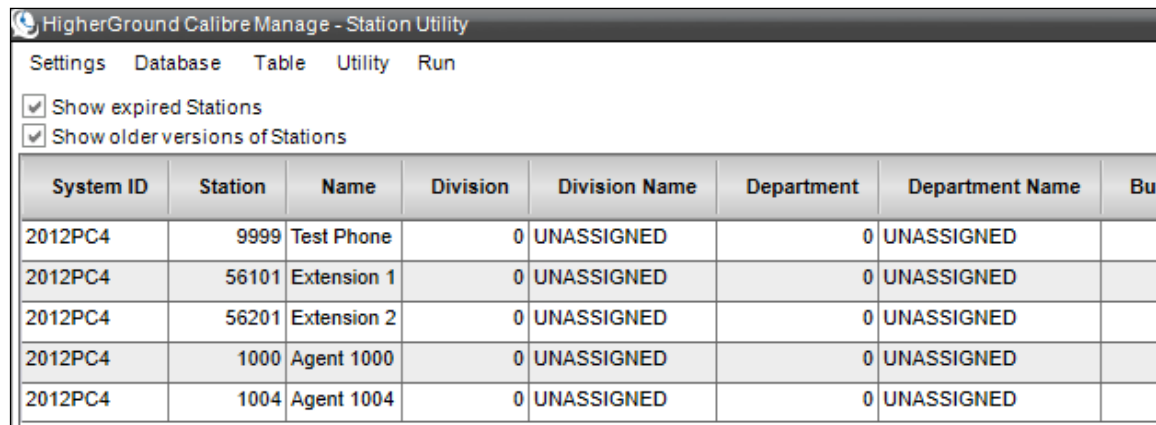
Repeat this section to administer a VoIP channel for each agent station extension from **Section 3**. In the compliance testing, two VoIP channels were configured as shown below.

The screenshot shows the 'HigherGround Calibre Manage - User/Channel Table' window. The table contains the following data:

System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP Port	VoIP MAC
2012PC4	VoIP Channel	CLU1-001	56101	Extension 1		VoIP	10.10.98.28:50000	00:00:00:00:00:00
2012PC4	VoIP Channel	CLU1-002	56201	Extension 2		VoIP	10.10.98.28:50002	00:00:00:00:00:00

### 7.3 Administer Station Utility

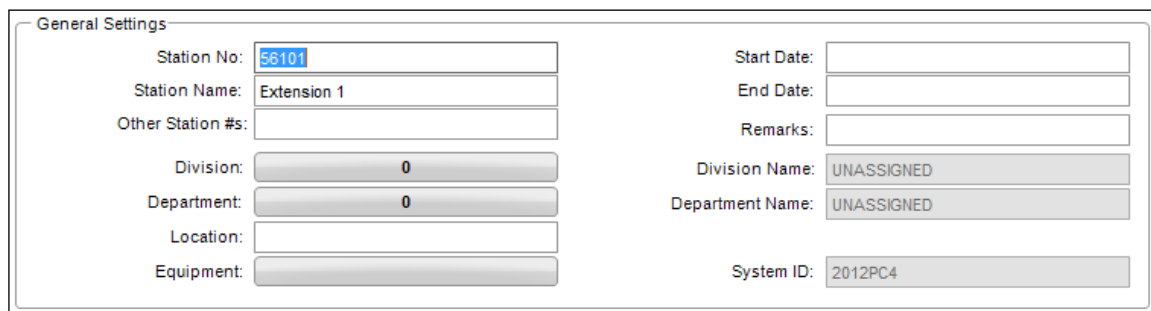
Select **Utility → Station Utility** from the top menu to display the **HigherGround Calibre Manage – Station Utility** screen. Click **Add** in the bottom left portion of the screen (not shown).



System ID	Station	Name	Division	Division Name	Department	Department Name	Bu
2012PC4	9999	Test Phone	0	UNASSIGNED	0	UNASSIGNED	
2012PC4	56101	Extension 1	0	UNASSIGNED	0	UNASSIGNED	
2012PC4	56201	Extension 2	0	UNASSIGNED	0	UNASSIGNED	
2012PC4	1000	Agent 1000	0	UNASSIGNED	0	UNASSIGNED	
2012PC4	1004	Agent 1004	0	UNASSIGNED	0	UNASSIGNED	

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:** Enter agent station extension listed in **Section 3**.
- **Station Name:** A desired station name.



General Settings	
Station No: 56101	Start Date:
Station Name: Extension 1	End Date:
Other Station #s:	Remarks:
Division: 0	Division Name: UNASSIGNED
Department: 0	Department Name: UNASSIGNED
Location:	
Equipment:	System ID: 2012PC4

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

HigherGround Calibre 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	Room	Emp
2012PC4	9999	Test Phone	0	UNASSIGNED	0	UNASSIGNED			
2012PC4	56101	Extension 1	0	UNASSIGNED	0	UNASSIGNED			
2012PC4	56201	Extension 2	0	UNASSIGNED	0	UNASSIGNED			
2012PC4	1000	Agent 1000	0	UNASSIGNED	0	UNASSIGNED			
2012PC4	1004	Agent 1004	0	UNASSIGNED	0	UNASSIGNED			

## 8 Verification Steps

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

### 8.1 Verify Avaya Aura® Communication Manager

On Communication Manager, verify the 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 5.3**, 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	7	no	devaes	established	26	20

Verify the registration status of the virtual softphones by using the “list registered-ip-stations” command. Verify that all extensions from **Section 5.7** are displayed, as shown below.

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

Page 1

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Skt Gatekeeper IP Address			
56101	9608	IP Phone	tcp 10.33.5.29			
	1	6.6229	10.10.97.222			
56114	9620	IP_API_A	tcp 10.10.97.224			
	1	3.2040	10.10.97.222			
56115	9620	IP_API_A	tcp 10.10.97.224			
	1	3.2040	10.10.97.222			

## 8.2 Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of monitored skill groups, softphones and agent station extensions as listed in **Section 3**.

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

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ 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	DevvmCM	1	Talking	Thu Jan 5 17:29:30 2017	Online	17	6	76	92	30

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

Verify the status of the DMCC link 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 6.7**, and that the **# of Associated Devices** column reflects the number of monitored skill group, agent station extensions, and virtual IP softphone extensions.

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- High Availability
- ▶ Licensing
- ▼ Status
  - Alarm Viewer
  - ▶ Log Manager
  - ▶ Logs
  - ▼ Status and Control
    - CVLAN Service Summary
    - DLG Services Summary
    - DMCC Service Summary
    - Switch Conn Summary

### DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every  seconds

Session Summary [Device Summary](#)

Generated on Thu Jan 26 16:02:29 EST 2017

Service Uptime: 20 days, 22 hours 32 minutes

Number of Active Sessions: 8

Number of Sessions Created Since Service Boot: 92

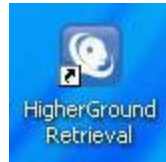
Number of Existing Devices: 12

Number of Devices Created Since Service Boot: 90

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	47F909090A91A590F E5C9740569C313E-93	calibre	HgDMCC	10.10.98.28	XML Unencrypted	6

### 8.3 Verify HigherGround Calibre

Log an agent in to the monitored skill group to handle and complete an ACD call. From the agent PC, double click on the shortcut for the HighGround Retrieval application that resides on the Calibre server.



The screen below is displayed. Log in using the appropriate credentials.



The screen below is displayed next with a list of the call recordings for today. Verify that there is an entry reflecting the last call, with proper values in the relevant fields. Select the entry and verify that the call recording can be played back.

A screenshot of the HigherGround Calibre application interface. The top menu bar includes 'File', 'View', 'Favorites', 'Report Templates', 'Dashboards', 'Settings', 'My Reports', and 'Run'. The left sidebar contains a 'Filter' section with a list of fields like 'Date Time', 'Duration', 'Media Types', etc., and a 'Setting' section. Below the filter is a 'Last Hour' button and a 'Last 12 Hours' button. The main area is divided into a 'Timeline Pane' at the top showing a call recording timeline with a play button and a 'Visual Media Pane' on the right showing 'No visual media selected'. At the bottom, there is a table of call recordings with columns for 'Date Time (1)', 'Dur...', 'Media Types', 'St...', 'Station Name', 'Alt Station', 'Alt Station Name', 'Calling Device', 'Called Device', 'Answering Device', 'Accl...', 'Call Type', 'Call Reason', and 'GlobalLinkId'. The table shows three entries for 01/26/2017. Below the table is a 'Default View: Collapse Last' button.

## 9 Conclusion

These Application Notes describe the configuration steps required for HigherGround Calibre 8.9.5 to successfully interoperate with Avaya Aura® Communication Manager 7.0.1 using Avaya Aura® Application Enablement Services 7.0.1. All feature and serviceability test cases were completed with observations noted in **Section0**.

## 10 Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1 555-245-205 Issue 3 October 2016.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.0.1 Issue 2 August 2016.

Contact HigherGround, Inc for Calibre documents:

3. *Calibre v.8.9 User Manual*.
4. *Calibre v.8.9 Administrator Manual*.
5. *Avaya DMCC Service Observe Integration Manual* Jan 26, 2017



---

**©2017 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).