



**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 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.

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 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) 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.

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 Single Step Conference 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 group 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 group, agent stations, and virtual IP softphones.
- Use of DMCC call control services to activate Single Step Conference 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:

- Agents are required to log in after Calibre starts.
- Only one skill group can be monitored by Calibre. Agents that do not belong to the monitored skill group can still be monitored with ACD calls recorded, and the recording entries for those calls will be associated with the agent station instead of agent ID extension.
- Non-ACD calls to the agents are recorded and reported using the agent ID extension. The called parameter from those recording entries can be used to identify the non-ACD calls.
- The hold and reconnect scenario with held period under the system MaxRecordSilence interval produced one recording entry, and the same scenario with held period over the MaxRecordSilence interval produced two recording entries with blank call type, calling, called, and answer values in the second recording entry. This is by design, and the MaxRecordSilence parameter is configurable with a default of 15 seconds.
- Two back-to-back calls with inter-call interval below the MaxRecordSilence interval are lumped into one recording entry, with information from the second call used for calling, called, and answer.
- For the transfer scenarios, the recording entry for the transfer-from agent showed call information from the call with the transfer-to destination. In addition, the recording entry for the transfer-to agent contained blank values for calling, called, and answer.
- For the attended transfer scenario, the recording entry associated with the transfer-from agent can have a call type of INTERN or OUT, depending on whether the transfer-to destination is a monitored agent or a non-monitored supervisor respectively. In addition, the recording entry for the transfer-to agent contained blank values for calling, called, and answer.
- For the conference scenarios, the recording entry for the conference-from agent showed call information from the call with the conference-to destination. In addition, the recording entry for the conference-to agent contained blank values for calling, called, and answer.

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 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 shown in the table below. Calibre requested monitoring on the first skill group and on both agent station extensions.

Device Type	Extension
VDN	48001, 48002
Skill Group	48101, 48102
Supervisor	45000
Agent ID	45881, 45882
Agent Station	45001, 45002

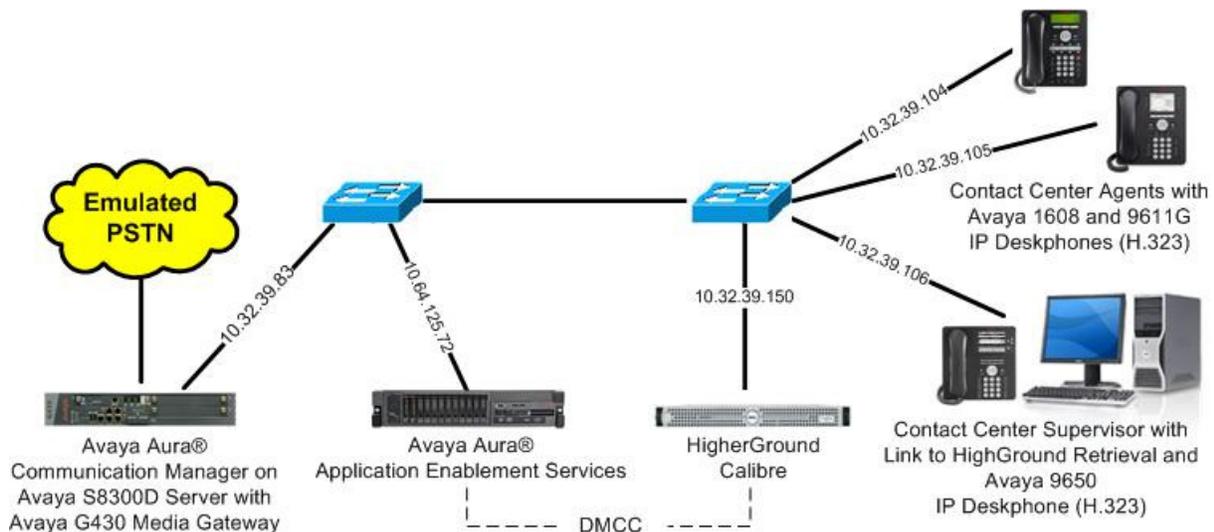


Figure 1: Compliance Testing Configuration

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 on Avaya S8300D Server with Avaya G430 Media Gateway	6.3 SP1 (R016x.03.0.124.0-20850)
Avaya Aura® Application Enablement Services	6.3 (6.3.0.0.212-0)
Avaya 1608 IP Deskphone (H.323)	1.330D
Avaya 9611G IP Deskphone (H.323)	6.2209
Avaya 9650 IP Deskphone (H.323)	3.105S
HigherGround Calibre on Windows 2008 Server <ul style="list-style-type: none">DMCC Integrator ServiceAvaya DMCC .NET (ServiceProvider.dll)	8.1 SP 2 8.1.0.1 6.2.0.29

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer 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. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. 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 3 of 11
                                OPTIONAL FEATURES

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

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. 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: 40001
Type: ADJ-IP
                                COR: 1
Name: CTI Link
```

5.3. 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 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
```

5.4. Administer Virtual IP Softphones

Add a virtual 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 “4620”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”

```

add station 45991                                     Page 1 of 5
                                                    STATION
Extension: 45991                                Lock Messages? n                BCC: 0
Type: 4620                                     Security Code: 45991          TN: 1
Port: IP                                           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: 45991
Speakerphone: 2-way                               Mute Button Enabled? y
Display Language: english                         Expansion Module? n
Survivable GK Node Name:                          Media Complex Ext:
Survivable COR: internal                           IP SoftPhone? y
Survivable Trunk Dest? y                           IP Video Softphone? n
                                                    Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? Y
  
```

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 45991 count 2
                                                    STATIONS
Ext/      Port/   Name/      Room/      Cv1/  COR/   Cable/
Hunt-to   Type    Surv GK NN  Move      Data Ext  Cv2  COS TN Jack
45991    S00036 Calibre Virtual #1          1
           4620                no                1 1
45992    S00039 Calibre Virtual #2          1
           4620                no                1 1
  
```

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- 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 reads "Application Enablement Services Management Console". Below this is a red horizontal bar. The main content area features a login form with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. A "Login" button is positioned below the password field. At the bottom of the page, a red horizontal bar is followed by the copyright notice: "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, there is a user information block: "Welcome: User", "Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes_125_72/10.64.125.72", "Server Offer Type: VIRTUAL_APPLIANCE_ON_SP", "SW Version: 6.3.0.0.212-0", and "Server Date and Time: Tue Sep 3 10:48:28 MDT 2013". Below this is a red navigation bar with "Home | Help | Logout". On the left is a vertical menu with items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and contains the following text: "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: "• 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.", "• 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 infomations.", "• User Management - Use User Management to manage AE Services users and AE Services user-related resources.", "• Utilities - Use Utilities to carry out basic connectivity tests.", "• Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom of the main content area, it 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 (not shown), and log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" page selected. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, there is a user information block: "Welcome: User", "Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes_125_72/10.64.125.72", "Server Offer Type: VIRTUAL_APPLIANCE_ON_SP", "SW Version: 6.3.0.0.212-0", and "Server Date and Time: Tue Sep 3 10:49:22 MDT 2013". Below this is a red navigation bar with "Home | Help | Logout". On the left is a vertical menu with items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security. The "Licensing" item is expanded, showing sub-items: "WebLM Server Address", "WebLM Server Access" (highlighted in blue), and "Reserved Licenses". The main content area is titled "Licensing" and contains the following text: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bulleted list: "• WebLM Server Address". Below that, it says: "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bulleted list: "• WebLM Server Access". At the bottom, it says: "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bulleted list: "• Reserved Licenses".

The **Web License Manager** 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.

AVAYA Web License Manager (WebLM v6.3) Help | About | Change Password | Log off admin

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)

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

License installed on: May 11, 2012 7:07:47 PM -04:00

License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001 VALUE_AES_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	16	0

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 user information: "Welcome: User", "Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes_125_72/10.64.125.72", "Server Offer Type: VIRTUAL_APPLIANCE_ON_SP", "SW Version: 6.3.0.0.212-0", and "Server Date and Time: Tue Sep 3 10:53:53 MDT 2013". The 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" (expanded to "TSAPI Links" and "TSAPI Properties"), and "Communication Manager Interface". 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	S8800	2	4	Both

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

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields, and click **Apply Changes**.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The top right corner displays user information: "Welcome: User", "Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes_125_72/10.64.125.72", "Server Offer Type: VIRTUAL_APPLIANCE_ON_SP", "SW Version: 6.3.0.0.212-0", and "Server Date and Time: Tue Sep 3 10:54:31 MDT 2013". The 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" (expanded to "TSAPI Links" and "TSAPI Properties"), "TWS", and "Communication Manager Interface". The main content area is titled "Add TSAPI Links" and contains the following form fields:

- Link: 2
- Switch Connection: S8300D
- Switch CTI Link Number: 1
- ASAI Link Version: 4
- Security: Unencrypted

At the bottom of the form are two buttons: "Apply Changes" and "Cancel Changes".

6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with the relevant Communication Manager, in this case “S8300D”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

Welcome: User
Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Sep 3 10:48:28 MDT 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	1
<input type="radio"/> S8800	No	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

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, in this case “10.32.39.83” as shown below. Click **Add Name or IP**.

Welcome: User
Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Sep 3 10:48:28 MDT 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

Edit H.323 Gatekeeper - S8300D

10.32.39.83 Add Name or IP

Name or IP Address

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**.

Welcome: User
Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Sep 03 10:56:36 MDT 2013

Security | Security Database | Control Home | Help | Logout

▶ AE Services
 ▶ Communication Manager Interface
 ▶ 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

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**.

Welcome: User
Last login: Tue Sep 3 10:41:39 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Sep 3 10:57:59 MDT 2013

Maintenance | Service Controller Home | Help | Logout

▶ AE Services
 ▶ Communication Manager Interface
 ▶ Licensing
 ▼ **Maintenance**
 Date Time/NTP Server
 ▶ Security Database
 Service Controller
 ▶ Server Data
 ▶ Networking
 ▶ Security
 ▶ Status

Service Controller

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

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

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).

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 the user. The main navigation pane on the left shows a tree structure with 'User Management' expanded to 'User Admin', where 'Add User' is selected. The main content area shows the 'Add User' form with the following fields and values:

Field	Value
* User Id	calibre
* Common Name	calibre
* Surname	calibre
* User Password
* Confirm Password
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	

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).



Application Enablement Services

Management Console

Welcome: User
 Last login: Tue Sep 3 10:48:22 2013 from 10.32.39.20
 Number of prior failed login attempts: 0
 HostName/IP: aes_125_72/10.64.125.72
 Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
 SW Version: 6.3.0.0.212-0
 Server Date and Time: Tue Sep 3 11:27:49 MDT 2013

Networking | Ports
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- AE Service IP (Local IP)
- Network Configure
- Ports
- TCP Settings
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Ports

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"/>
DLG Port			
	TCP Port	5678	
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"/>	
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 type="radio"/> <input checked="" type="radio"/>

7. Configure HigherGround Calibre

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

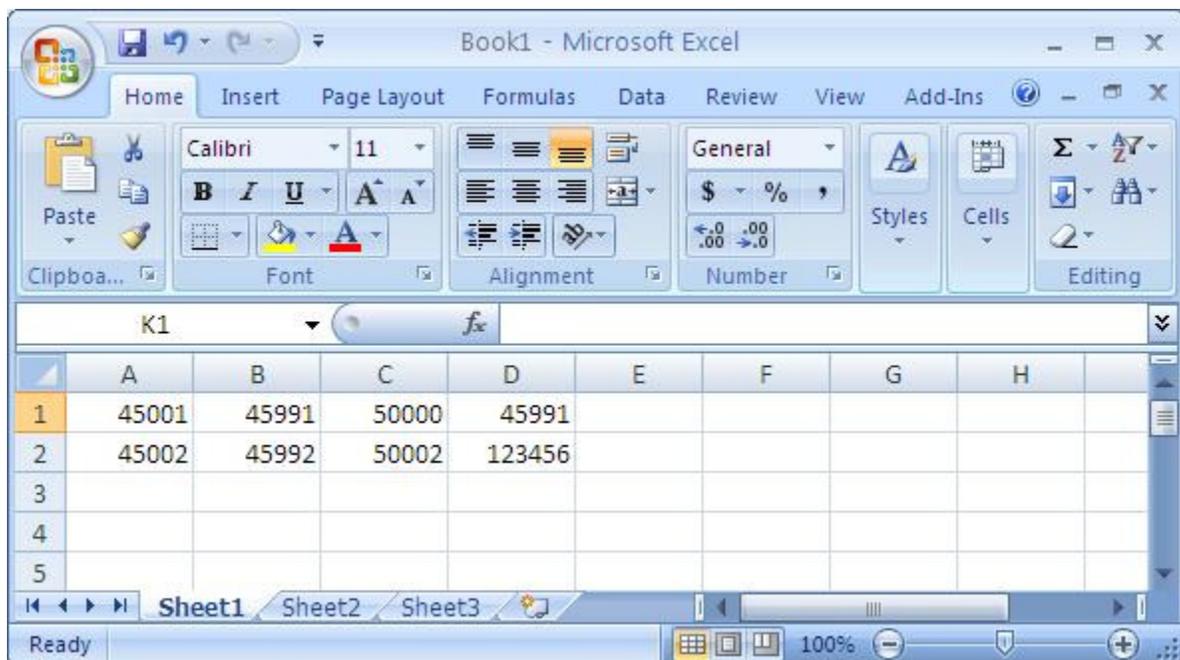
- Administer extensions
- Administer DMCC integrator service
- Administer VoIP channels
- Administer station utility

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

7.1. Administer Extensions

From any PC running the Microsoft Excel application, create a worksheet containing an entry for each monitored agent from **Section 3**. Enter the following values for the specified fields, as shown below.

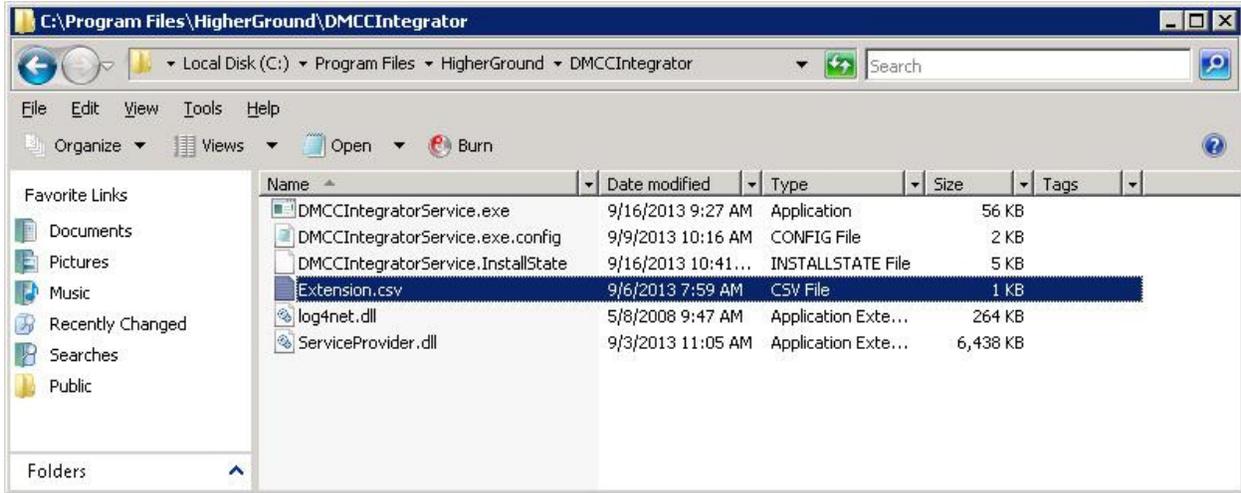
- **Cell A:** The agent station extension from **Section 3**.
- **Cell B:** An available virtual IP softphone extension from **Section 5.4**.
- **Cell C:** An available even RTP port number in the range of 50000-65535.
- **Cell D:** The security code for the available virtual IP softphone from **Section 5.4**.



The screenshot shows a Microsoft Excel window titled "Book1 - Microsoft Excel". The ribbon is set to "Home". The worksheet contains the following data:

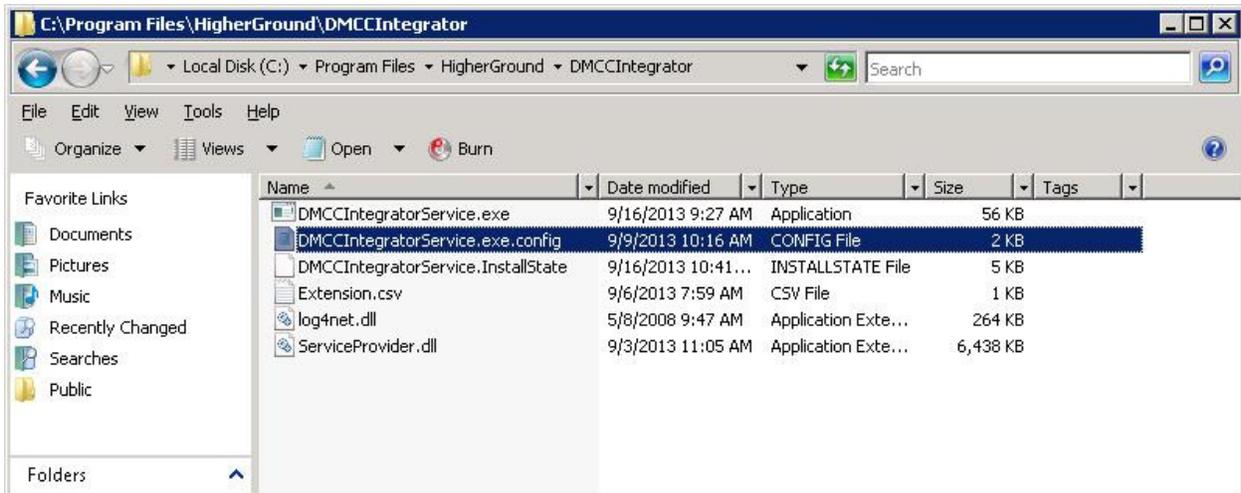
	A	B	C	D	E	F	G	H
1	45001	45991	50000	45991				
2	45002	45992	50002	123456				
3								
4								
5								

Save the worksheet using **Extension** as file name, and **CSV** as file type. Manually copy the resultant **Extension.csv** file to the Calibre server running the Recorder component, in this case under directory **C:\Program Files\HigherGround\DMCCIntegrator**, as shown below.



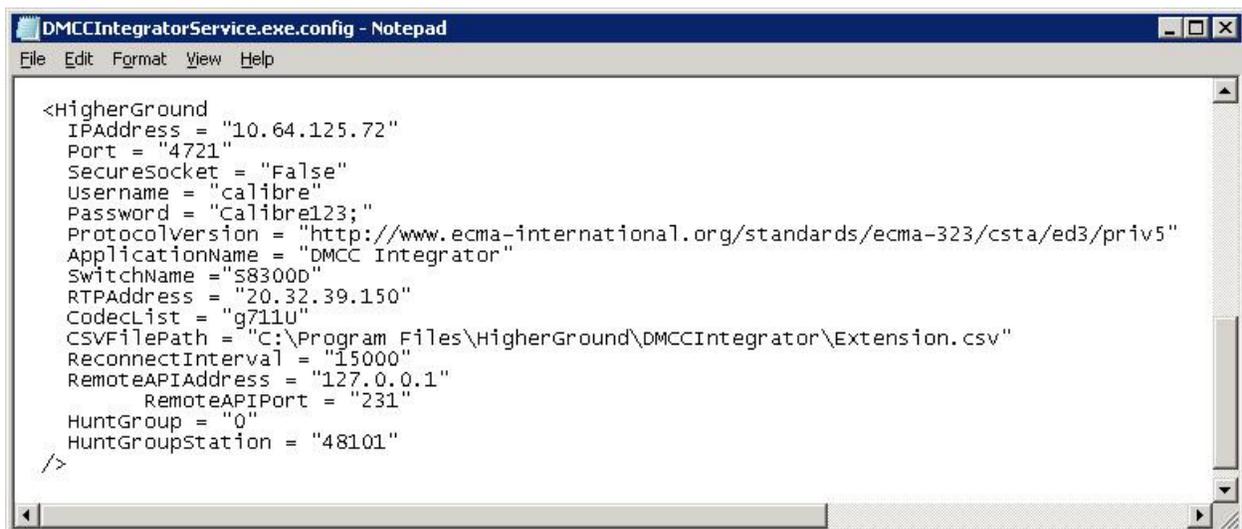
7.2. Administer DMCC Integrator Service

From the Calibre server running the Recorder component, navigate to the **C:\Program Files\HigherGround\DMCCIntegrator** directory to locate the **DMCCIntegratorService.exe.config** file shown below.



Open the **DMCCIntegratorService.exe.config** file with the Notepad application. Navigate to the **HigherGround** sub-section. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **IPAddress:** IP Address of Application Enablement Services.
- **Port:** The DMCC unencrypted port value from **Section 6.8**.
- **Username:** The Calibre user credentials from **Section 6.7**.
- **Password:** The Calibre user credentials from **Section 6.7**.
- **ProtocolVersion:** “<http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv5>”
- **SwitchName:** The relevant switch connection name from **Section 6.3**.
- **RTPAddress:** IP address of Calibre server running the Recorder component.
- **CSVFilePath:** The path to the manually installed Extension.csv file.
- **RemoteAPIAddress:** “127.0.0.1”
- **HuntGroupStation:** The skill group extension to be monitored from **Section 3**.



```
<HigherGround
  IPAddress = "10.64.125.72"
  Port = "4721"
  SecureSocket = "False"
  Username = "calibre"
  Password = "calibre123;"
  ProtocolVersion = "http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv5"
  ApplicationName = "DMCC Integrator"
  SwitchName = "S8300D"
  RTPAddress = "20.32.39.150"
  CodeclList = "g711U"
  CSVFilePath = "C:\Program Files\HigherGround\DMCCIntegrator\Extension.csv"
  ReconnectInterval = "15000"
  RemoteAPIAddress = "127.0.0.1"
    RemoteAPIPort = "231"
  HuntGroup = "0"
  HuntGroupStation = "48101"
/>
```

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

A screenshot of a window titled "HigherGround Calibre Control Tower - User/Channel Table". The window has a menu bar with "Settings", "Database", "Table", "Utility", "Calibre QA", and "Run". Below the menu bar are two checked checkboxes: "Show interactive users" and "Show recorder channels". The main area contains a table with the following data:

System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP
DEVCONNE-841693	Interactive User	ADMIN	99		Admin	ROD DNR	
DEVCONNE-841693	Interactive User	UNIT1	1		Station Only		
DEVCONNE-841693	VoIP Channel	CLU1-001	1			VoIP	0.0.0.0
DEVCONNE-841693	VoIP Channel	CLU1-002	2			VoIP	0.0.0.0
DEVCONNE-841693	VoIP Channel	CLU1-003	3			VoIP	0.0.0.0
DEVCONNE-841693	VoIP Channel	CLU1-004	4			VoIP	0.0.0.0

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:** The corresponding RTP port number for the agent from **Section Error!**
Reference source not found..

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.

System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP
DEVCONN-841693	Interactive User	ADMIN	99		Admin	ROD DNR	
DEVCONN-841693	Interactive User	UNIT1	1		Station Only		
DEVCONN-841693	VoIP Channel	CLU1-001	45001			VoIP	20.32.39.150
DEVCONN-841693	VoIP Channel	CLU1-002	45002			VoIP	20.32.39.150
DEVCONN-841693	VoIP Channel	CLU1-003	3			VoIP	0.0.0.0
DEVCONN-841693	VoIP Channel	CLU1-004	4			VoIP	0.0.0.0

7.4. Administer Station Utility

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

The screenshot shows the 'HigherGround Calibre Control Tower - Station Utility' application window. At the top, there is a menu bar with 'Settings', 'Database', 'Table', 'Utility', 'Calibre QA', 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 data:

System ID	Station	Name	Division	Division Name	Department	Department Name
DEVCONNE-841693	9999	Test Phone	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:** The first agent station extension from **Section 3**.
- **Station Name:** A desired station name.

The screenshot shows the 'HigherGround Calibre Control Tower - Station Utility' application window with the 'General Settings' sub-section expanded. The form contains the following fields and values:

Field	Value
Station No:	45001
Station Name:	Calibre Station 1
Other Station #s:	
Division:	0
Department:	0
Location:	
Equipment:	
Start Date:	
End Date:	
Remarks:	
Division Name:	UNASSIGNED
Department Name:	UNASSIGNED
System ID:	DEVCONNE-841693

Below the General Settings section, there are two other sections: 'Human Resources' and 'Misc.'. The 'Human Resources' section includes fields for Empl. ID, Grad Date, Hire Date, Experience Level (0), and Wage Group (0). The 'Misc.' section includes fields for Cable 1, Cable 2, Cable 3, Cable 4, and Term.

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 Control Tower - Station Utility						
<input type="checkbox"/> Settings <input type="checkbox"/> Database <input type="checkbox"/> Table <input type="checkbox"/> Utility <input type="checkbox"/> Calibre QA <input type="checkbox"/> 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
DEVCONN-841693	9999	Test Phone	0	UNASSIGNED	0	UNASSIGNED
DEVCONN-841693	45001	Calibre Station 1	0	UNASSIGNED	0	UNASSIGNED
DEVCONN-841693	45002	Calibre Station 2	0	UNASSIGNED	0	UNASSIGNED
DEVCONN-841693	45881	Agent1	0	UNASSIGNED	0	UNASSIGNED
DEVCONN-841693	45882	Agent2	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 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	aes_125_72	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 5.4** are displayed, as shown below.

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

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Gatekeeper	IP Address/ IP Address	
45000	9650 1	IP_Phone 3.105S	y	10.32.39.104	10.32.39.83	
45001	1608 1	IP_Phone 1.330D	y	10.32.39.105	10.32.39.83	
45002	9611 1	IP_Phone 6.2209	y	10.32.39.106	10.32.39.83	
45991	4620 1	IP_API_A 3.2040	y	10.64.125.72	10.32.39.83	
45992	4620 1	IP_API_A 3.2040	y	10.64.125.72	10.32.39.83	

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 group and agent station extensions from **Section 3**.

Welcome: User
 Last login: Mon Sep 16 12:06:22 2013 from 10.32.39.20
 Number of prior failed login attempts: 0
 HostName/IP: aes_125_72/10.64.125.72
 Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
 SW Version: 6.3.0.0.212-0
 Server Date and Time: Mon Sep 16 12:44:01 MDT 2013

AVAYA Application Enablement Services Management Console

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

▶ AE Services
 ▶ Communication Manager Interface
 ▶ 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**
 ▶ User Management
 ▶ Utilities
 ▶ Help

TSAPI Link Details

Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
○	1	S8800	2	Talking	Mon Aug 19 09:35:30 2013	Online	16	0	15	15	30
⊕	2	S8300D	1	Talking	Mon Sep 16 11:17:41 2013	Online	16	3	23	23	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.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User, Last login: Mon Sep 16 12:06:22 2013 from 10.32.39.20, Number of prior failed login attempts: 0, HostName/IP: aes_125_72/10.64.125.72, Server Offer Type: VIRTUAL_APPLIANCE_ON_SP, SW Version: 6.3.0.0.212-0, and Server Date and Time: Mon Sep 16 12:44:10 MDT 2013.

The navigation bar includes **Status | Status and Control | DMCC Service Summary** and **Home | Help | Logout**. The left sidebar shows a tree view with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, Status and Control, User Management, Utilities, and Help. The **Status and Control** category is expanded, showing sub-items like CVLAN Service Summary, DLG Services Summary, **DMCC Service Summary**, Switch Conn Summary, and TSAPI Service Summary.

The main content area displays the **DMCC Service Summary - Session Summary** page. It includes a checkbox for "Enable page refresh every 60 seconds" and a link for "Device Summary". Below this, it shows session statistics: Service Uptime: 12 days, 1 hours 18 minutes; Number of Active Sessions: 1; Number of Sessions Created Since Service Boot: 25; Number of Existing Devices: 5; and Number of Devices Created Since Service Boot: 128.

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	897C642DAA1EDC5DF FBEF5AC1FD7020C-24	calibre	DMCC Integrator	20.32.39.150	XML Unencrypted	5

Below the table are buttons for "Terminate Sessions" and "Show Terminated Sessions", and a status indicator "Item 1-1 of 1".

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.



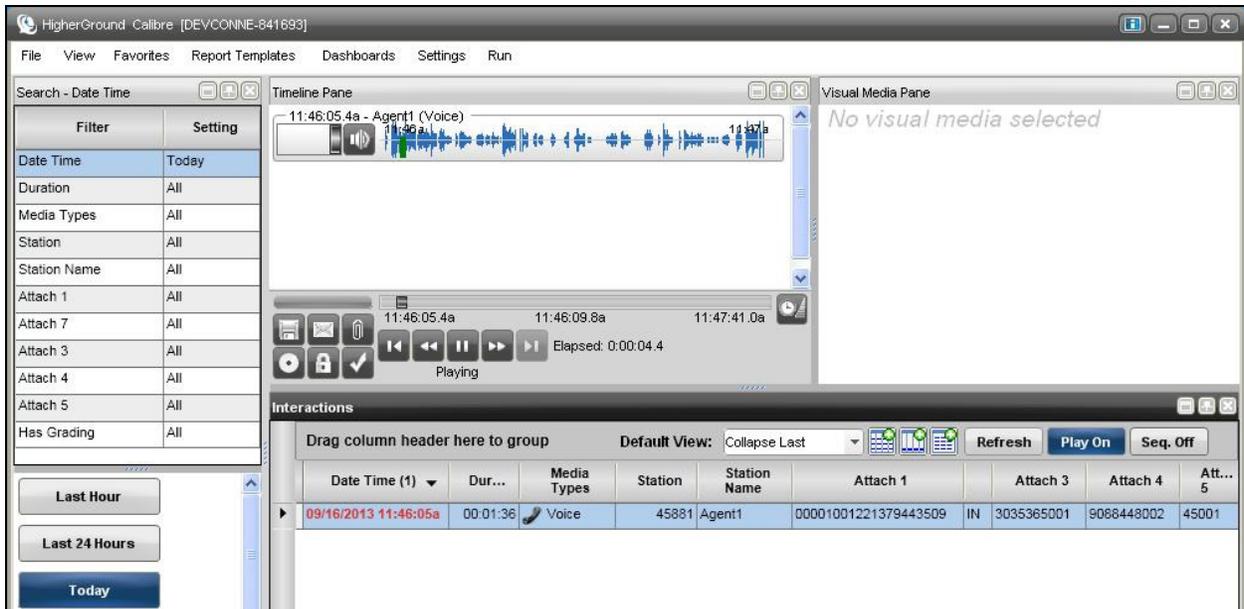
The screen below is displayed briefly while the forms are loading.



The **HigherGround Calibre** 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.



9. Conclusion

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

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 8, Release 6.3, May 2013, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 1, May 2013, available at <http://support.avaya.com>.
3. *Calibre Administrator Manual, Version 8.1*, available as part of Calibre installation.
4. *Avaya DMCC Based Call Monitoring Installation Manual, Version 1.1, 4/2009*, Version v.2.1, 2013, available as part of Calibre installation.
5. *Calibre User Manual*, Version v.2.1, 2013, available as part of Calibre installation.

©2013 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.