



Application Notes for HigherGround Calibre 9 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for HigherGround Calibre 9 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing. HigherGround Calibre is a call recording solution.

In the compliance testing, HigherGround Calibre used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and used the Service Observing feature to capture media associated with the monitored agent stations for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for HigherGround Calibre 9 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing. Calibre is a call recording solution.

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

When there is an active call at the monitored agent station, Calibre is informed of the call via event reports from the DMCC interface. Calibre starts the call recording by using media via active Service Observing from the virtual IP softphone associated with the agent station. The event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

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

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

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

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and Calibre did not include use of any specific encryption features as requested by HigherGround.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Calibre:

- Use of DMCC to monitor skill groups and agent stations, register virtual IP softphones, and activate Service Observing.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, G.729, forwarding, service observing, long duration, multiple calls, multiple agents, conference, and transfer.

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

2.2. Test Results

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

- By design, the default Calibre setting ends an active recording upon agent placing the call on hold and starts a new recording upon agent resuming the call. This behavior is controlled by the RecordThroughHold system parameter and is configurable. The compliance testing used the default value of zero for the parameter.
- In the attended transfer scenario, the recording entry associated with the remaining conversation between the transfer-to agent and PSTN only contained values for date, duration, agent ID, agent extension, and agent name, with blank values for the remainder parameters.
- When an agent call was observed by the supervisor, the supervisor extension was reported as the answering device in the recording entry.

2.3. Support

Technical support on Calibre can be obtained through the following:

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

3. Reference Configuration

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

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

Device Type	Extension
Skill Group	61001, 61002
Agent Station	65001 (H.323), 66006 (SIP)
Agent ID	65881, 65882

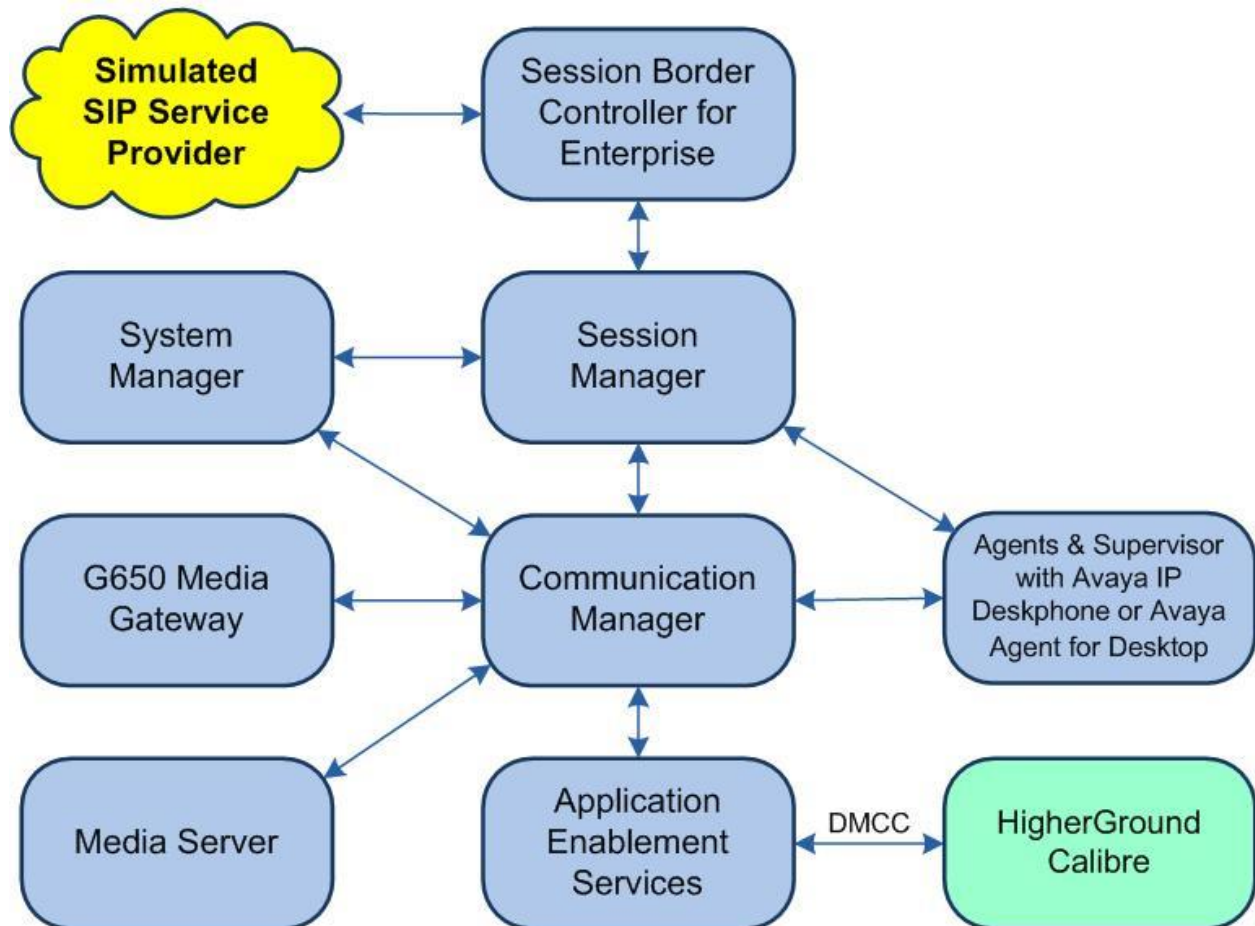


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.1.3 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.0.0.25-0
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.1 (8.1.1.0-19390)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya J179 & 9611G IP Deskphone (H.323)	6.8502
Avaya J169 IP Phone (SIP)	4.0.7.1.5
HigherGround Calibre on Windows 2019 Server <ul style="list-style-type: none">HgDMCC.exeAvaya DMCC .NET (ServiceProvider.dll)	9.2021.7941 Standard 9.2021.7985.15939 7.0.0.38

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer system parameters features
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “**display system-parameters customer-options**” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

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? y	DCS (Basic)? y		
ASAI Link Core Capabilities? y	DCS Call Coverage? y		
ASAI Link Plus Capabilities? y	DCS with Rerouting? y		

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

display system-parameters customer-options		Page	7 of 12
CALL CENTER OPTIONAL FEATURES			
Call Center Release: 8.0			
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		

5.2. Administer CTI Link

Add a CTI link using the “**add cti-link n**” command, where “**n**” is an available CTI link number. Enter an available extension number in the **Extension** field.

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

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

5.3. Administer IP Codec Set

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

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

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

```
change ip-codec-set 1                             Page 1 of 2
IP Codec Set
Codec Set: 1
Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt     Size(ms)
1: G.711MU      n           2          20
2: G.729
3:
4:
5:
6:
7:
Media Encryption      Encrypted SRTP: best-effort
1: 1-srtp-aescml28-hmac80
2: aes
3: none
4:
5:
```

5.4. Administer System Parameters Features

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

```
change system-parameters features                                     Page 5 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                  Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 27
```

Navigate to **Page 11**. Set **Service Observing: Warning Tone** to the needed setting per customer requirement, and enable **Allow Two Observers in Same Call**, as shown below.

```
change 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
    Work Mode On Login: aux
  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 Threshod: 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? n    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 UUI During Conference/Transfer? n
    Call Classification After Answer Supervision? y
        Send UCID to ASAI? y
        For ASAI Send DTMF Tone to Call Originator? y
    Send Connect Event to ASAI For Announcement Answer? n
    Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.5. Administer Class of Restriction

Enter the “**change cor n**” command, where “**n**” is the class of restriction (COR) number used for integration with Calibre. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to “**y**”, as shown below. In the compliance testing, this COR was assigned to the agent stations and virtual IP softphones.

If desired, separate COR can be used for enablement of each parameter. The COR with **Can Be Service Observed** enabled needs to be assigned to the agent stations, and the COR with **Can Be A Service Observer** enabled needs to be assigned to the virtual IP softphones.

```
change cor 2                                                         Page 1 of 23
                                CLASS OF RESTRICTION

    COR Number: 2
    COR Description: Calibre

        FRL: 0
    Can Be Service Observed? y
    Can Be A Service Observer? y
        Time of Day Chart: 1
        Priority Queuing? n
        Restriction Override: none
        Restricted Call List? n

        APLT? y
        Calling Party Restriction: none
        Called Party Restriction: none
        Forced Entry of Account Codes? n
        Direct Agent Calling? n
        Facility Access Trunk Test? n
        Can Change Coverage? n
```

5.6. Administer Agent Stations

Use the “**change station n**” command, where “**n**” is the first H.323 agent station extension from **Section 3**. For **COR**, enter the COR number from **Section 5.5**.

Repeat this section to administer all H.323 agent stations from **Section 3**. In the compliance testing, one H.323 agent station was administered as shown below.

change station 65001		Page 1 of 5
STATION		
Extension: 65001	Lock Messages? n	BCC: 0
Type: 9611	Security Code: *	TN: 1
Port: S000106	Coverage Path 1: 1	COR: 2
Name: CM Station 1	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? y

5.7. Administer Virtual IP Softphones

Add a virtual IP softphone using the “**add station n**” command, where “**n**” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “9608”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.5**.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 5
STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 9608	Security Code: 123456	TN: 1
Port: IP	Coverage Path 1:	COR: 2
Name: Calibre DMCC 1	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 65991	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules? 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

Navigate to **Page 4**, and add “**serv-obsrv**” to any available button as shown below.

```

add station 65991
                                     Page 4 of 5

                                     STATION

SITE DATA
  Room:                               Headset? n
  Jack:                               Speaker? n
  Cable:                             Mounting: d
  Floor:                             Cord Length: 0
  Building:                           Set Color:

ABBREVIATED DIALING
  List1:                               List2:                               List3:

BUTTON ASSIGNMENTS
  1: call-appr                        5:
  2: call-appr                        6:
  3: call-appr                        7:
  4: serv-obsrv                     8:

```

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

```

list station 65991 count 2

```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COR/ COS	TN	
65991	S000126	Calibre DMCC 1					2		
	9608		no				1	1	
65992	S000122	Calibre DMCC 2					2		
	9608		no				1	1	

6. Configure Avaya Aura® Application Enablement Services


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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer Calibre user
- Administer security database
- Administer ports
- Restart services

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “**https://ip-address**” in an Internet browser window, where “**ip-address**” is the IP address of the Application Enablement Services server.

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for "User" is displayed, including login details and system information. The left sidebar contains a navigation menu with options like "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area displays the "Welcome to OAM" message, explaining that the OAM Web provides tools for managing the AE Server and listing administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, and Utilities. It also notes that these domains can be served by one administrator for all domains or a separate administrator for each domain.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Mon Nov 8 10:51:48 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Nov 09 10:29:26 EST 2021
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" page, which provides instructions for setting up and maintaining the WebLM. It lists three tasks: setting up and maintaining the WebLM (requiring WebLM Server Address), importing, setting up and maintaining the license (requiring WebLM Server Access), and administering TSAPI Reserved Licenses or DMCC Reserved Licenses (requiring Reserved Licenses).

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Mon Nov 8 10:51:48 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Nov 09 10:29:26 EST 2021
HA Status: Not Configured

Licensing | Home | Help | Logout

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

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

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a tree view with the following structure:

- WebLM Home
- Install license
- Licensed products
 - APPL_ENAB
 - Application_Enablement
 - View by feature
 - View by local WebLM
 - Enterprise configuration
 - Local WebLM Configuration
 - Usages
 - Allocations
 - Periodic status
 - ASBCE
 - Session_Border_Controller_E_AE
 - Avaya_Proactive_Contact
 - CCTR
 - ContactCenter
 - COMMUNICATION_MANAGER

The right pane displays the **Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license)** screen. It includes the following information:

- You are here: Licensed Products > Application_Enablement > View by Feature
- License installed on: August 8, 2019 4:43:51 PM -05:00
- License File Host IDs: VE-83-02-2D-26-52-01

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

6.3. Administer TSAPI Link

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

The screenshot shows the AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar shows a navigation tree with "AE Services" expanded, and "TSAPI" selected. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
------	-------------------	-------------------	-------------------	----------

Buttons: Add Link, Edit Link, Delete Link

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

For **Switch Connection**, select the relevant switch connection from the drop-down list, in this case "cm7". For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

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

The screenshot shows the AVAYA Application Enablement Services Management Console, specifically the "Add TSAPI Links" screen. The left sidebar is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link (1), Switch Connection (cm7), Switch CTI Link Number (1), ASAI Link Version (12), and Security (Both). Below the form are buttons for "Apply Changes", "Cancel Changes", and "Advanced Settings".

Form fields and values:

- Link: 1
- Switch Connection: cm7
- Switch CTI Link Number: 1
- ASAI Link Version: 12
- Security: Both

Buttons: Apply Changes, Cancel Changes, 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 existing switch connections.

Locate the connection name associated with relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows the "Communication Manager Interface" selected, with "Switch Connections" highlighted. The main content area displays the "Switch Connections" table with columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The table lists a connection named "cm7" with "Yes" for Processor Ethernet, "30" for Msg Period, and "1" for Number of Active Connections. Below the table are buttons for "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", "Delete Connection", and "Survivability Hierarchy".

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

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

The screenshot shows the "Edit H.323 Gatekeeper - cm7" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area has a title "Edit H.323 Gatekeeper - cm7" and a text input field containing "10.64.101.236". To the right of the input field is a button labeled "Add Name or IP". Below the input field are two buttons: "Delete IP" and "Back".

6.5. Administer Calibre User

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

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Mon Nov 8 10:51:48 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Nov 09 10:29:26 EST 2021
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id 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

Enterprise Handle

Given Name

6.6. Administer Security Database

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

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is shown, including login details and system information. The main navigation bar at the top contains links for "Security", "Security Database", and "Control". The left sidebar lists various service categories, with "Security" expanded to show sub-options like "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database", and "Control". The "Control" option is selected. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

6.7. Administer Ports

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

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Mon Nov 8 10:51:48 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Nov 09 10:29:26 EST 2021
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

Enabled Disabled

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722


Enabled Disabled

TR/87 Port4723

Enabled Disabled

6.8. Restart Services

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

**Application Enablement Services**
Management Console

Welcome: User
Last login: Mon Nov 8 10:51:48 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Nov 09 10:29:26 EST 2021
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

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

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

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

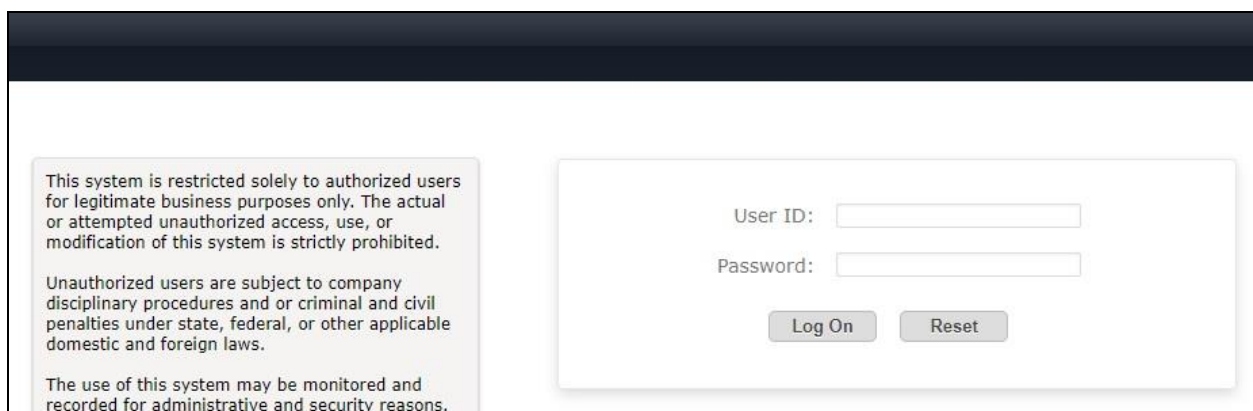
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

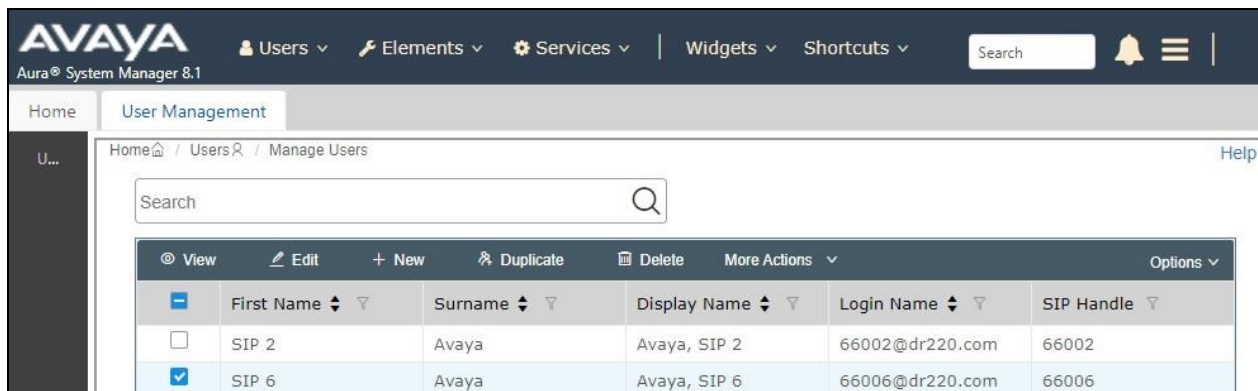
Access the System Manager web interface by using the URL “**https://ip-address**” in an Internet browser window, where “**ip-address**” is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer Users

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

Select the entry associated with the first SIP agent station from **Section 3**, in this case “**66006**”, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
<input checked="" type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006

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

Click on the **Editor** icon shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, a search bar, and menu items for Users, Elements, Services, Widgets, and Shortcuts. The breadcrumb trail indicates the current location: Home > User Management > Manage Users. The main heading is "User Profile | Edit | 66006@dr220.com". Below this are tabs for Identity, Communication Profile, Membership, and Contacts. The Communication Profile tab is active. On the left, under "PROFILES", the "CM Endpoint Profile" is selected with a toggle switch. The main form contains various fields for configuring the user profile, including System (DR-CM), Profile Type (Endpoint), Extension (66006), Set Type (J169CC), Port (S000115), and Voice Mail Number (admin). The "Extension" field has a small blue icon with a pencil, which is highlighted by a red square, indicating it is the "Editor" icon mentioned in the text.

The **Edit Endpoint** pop-up screen is displayed. For **Class of Restriction (COR)**, enter the COR number from **Section 5.5**.

For **Type of 3PCC Enabled**, select “**Avaya**” as shown below.

Repeat this section for all SIP agent stations from **Section 3**. In the compliance testing, one SIP agent station was configured.

AVAYA
Aura® System Manager 8.1

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

Home User Management

Home / Users / Manage Users Help ?

Edit Endpoint

Done [Save As Template]

System	DR-CM	Extension	66006
Template	Select ▾	Set Type	J169CC
Port	S000115	Security Code	
Name	Avaya, SIP 6		

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)

Button Assignment (B) Profile Settings (P) Group Membership (M)

* Class of Restriction (COR)	2	* Class Of Service (COS)	1
* Emergency Location Ext	66006	* Message Lamp Ext.	66006
* Tenant Number	1	* Type of 3PCC Enabled	Avaya ▾
* SIP Trunk	aar	Coverage Path 2	
Coverage Path 1		Localized Display Name	Avaya, SIP 6
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	system ▾
Multibyte Language	Not Applicable ▾		
SIP URI			

8. Configure HigherGround Calibre

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

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

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

8.1. Administer Avaya Recorder

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



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

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

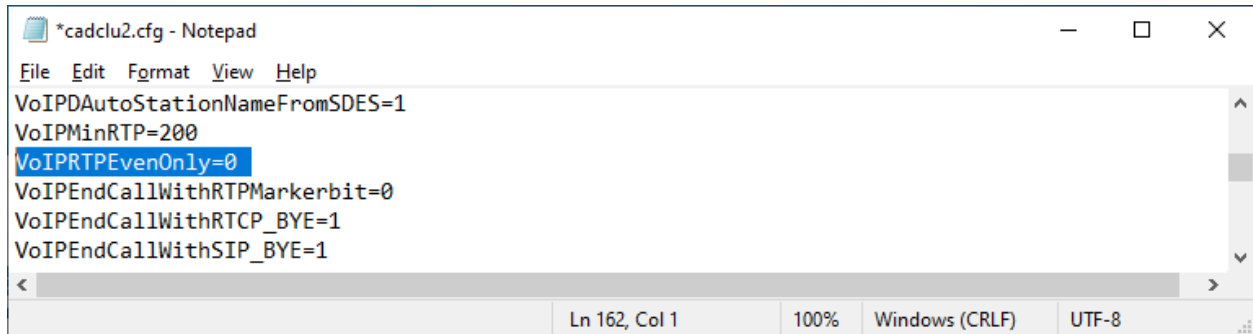
The **HigherGround Avaya Recorder** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **VoIP Type:** “Avaya”
- **VoIP Channel Count:** The number of virtual IP softphones from **Section 5.7**.
- **Minimum Duration:** The desired minimal duration for recordings.

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

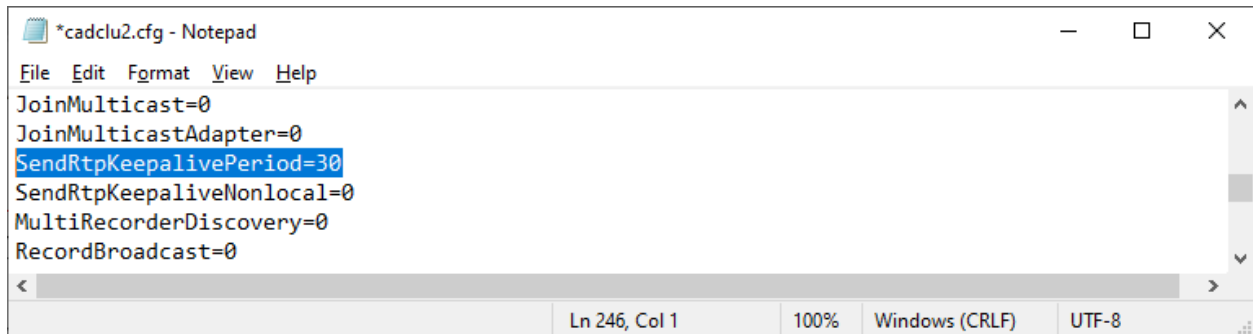
Group	File Name	Title
Important	cadalarm.cfg	Alarm Monitor, HigherGround
Normal	cadarc.cfg	Archive Utility, HigherGround
Normal	cadcfg.cfg	Configuration Manager, HigherGround
Important	cadclu1.cfg	Voice Recorder, HigherGround
Important	cadclu2.cfg	Avaya Recorder, HigherGround
Important	cadcoll.cfg	SMDR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

Locate the **VoIPRTPEvenOnly** parameter and set the value to “0” as shown below. This setting allows for both odd and even RTP ports.



```
*cadclu2.cfg - Notepad
File Edit Format View Help
VoIPDAutoStationNameFromSDES=1
VoIPMinRTP=200
VoIPRTPEvenOnly=0
VoIPEndCallWithRTPMarkerbit=0
VoIPEndCallWithRTCP_BYE=1
VoIPEndCallWithSIP_BYE=1
Ln 162, Col 1 100% Windows (CRLF) UTF-8
```

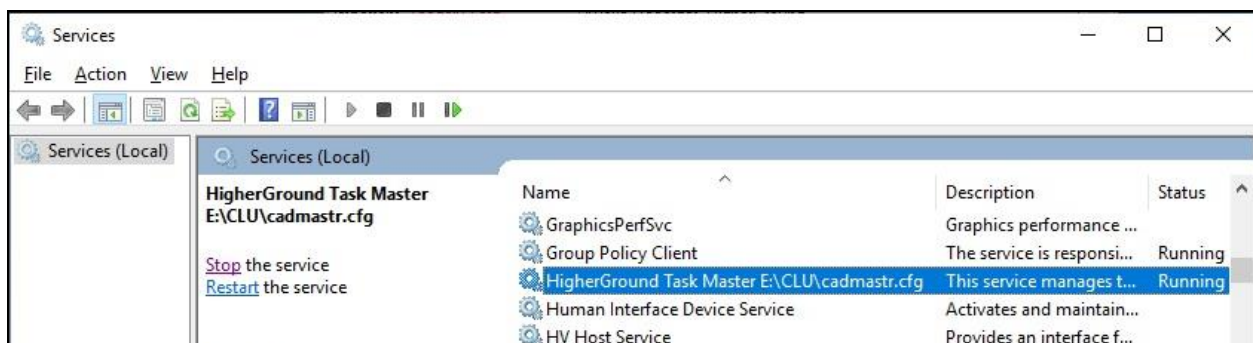
Locate the **SendRtpKeepalivePeriod** parameter and set the value to “30” as shown below.



```
*cadclu2.cfg - Notepad
File Edit Format View Help
JoinMulticast=0
JoinMulticastAdapter=0
SendRtpKeepalivePeriod=30
SendRtpKeepaliveNonlocal=0
MultiRecorderDiscovery=0
RecordBroadcast=0
Ln 246, Col 1 100% Windows (CRLF) UTF-8
```

8.2. Restart Service

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



8.3. Administer Station Utility

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



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

The screenshot shows the 'HigherGround Manage - User/Channel Table' window. It has a menu bar with 'Settings', 'Database', 'Table', 'Utility', 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
TLT-W2019	Interactive User	devcon	10001		Admin
TLT-W2019	VoIP Channel	CLU2-201	201		
TLT-W2019	VoIP Channel	CLU2-202	202		

The **HigherGround Manage – Station Utility** screen is displayed next. Create an entry for each agent station extension from **Section 3** with pertinent **Station** extension and desired **Name** value.

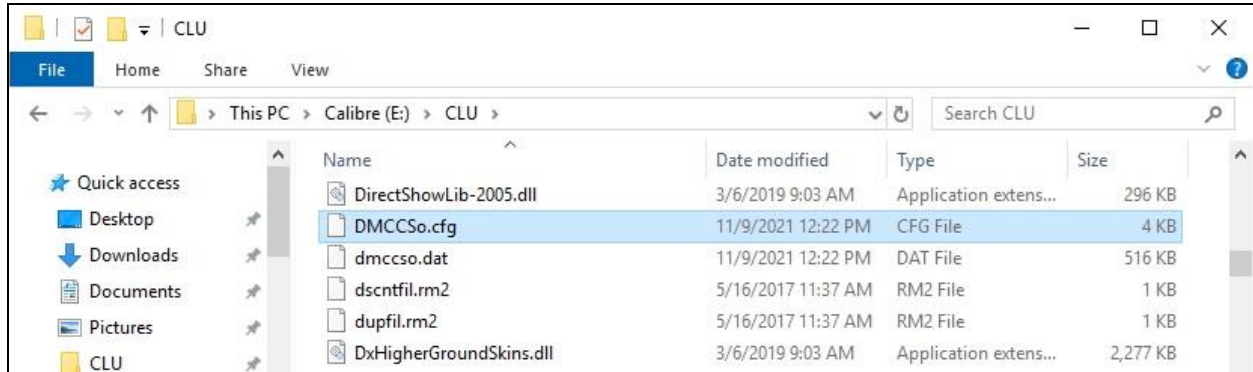
In the compliance testing, two entries were created as shown below.

The screenshot shows the 'HigherGround Manage - Station Utility' window. It has a menu bar with 'Settings', 'Database', 'Table', 'Utility', and 'Run'. Below the menu bar are two checked checkboxes: 'Show expired Stations' and 'Show older versions of Stations'. The main area contains a table with the following data:

System ID	Station	Name	Division	Division Name	Department	Department Name	Building	Room
TLT-W2019	9999	Test Phone	1	UNASSIGNED	101	UNASSIGNED		
TLT-W2019	65001	CM Station 1	0		0			
TLT-W2019	66006	Avaya SIP 6	0		0			

8.5. Administer DMCCso.cfg

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

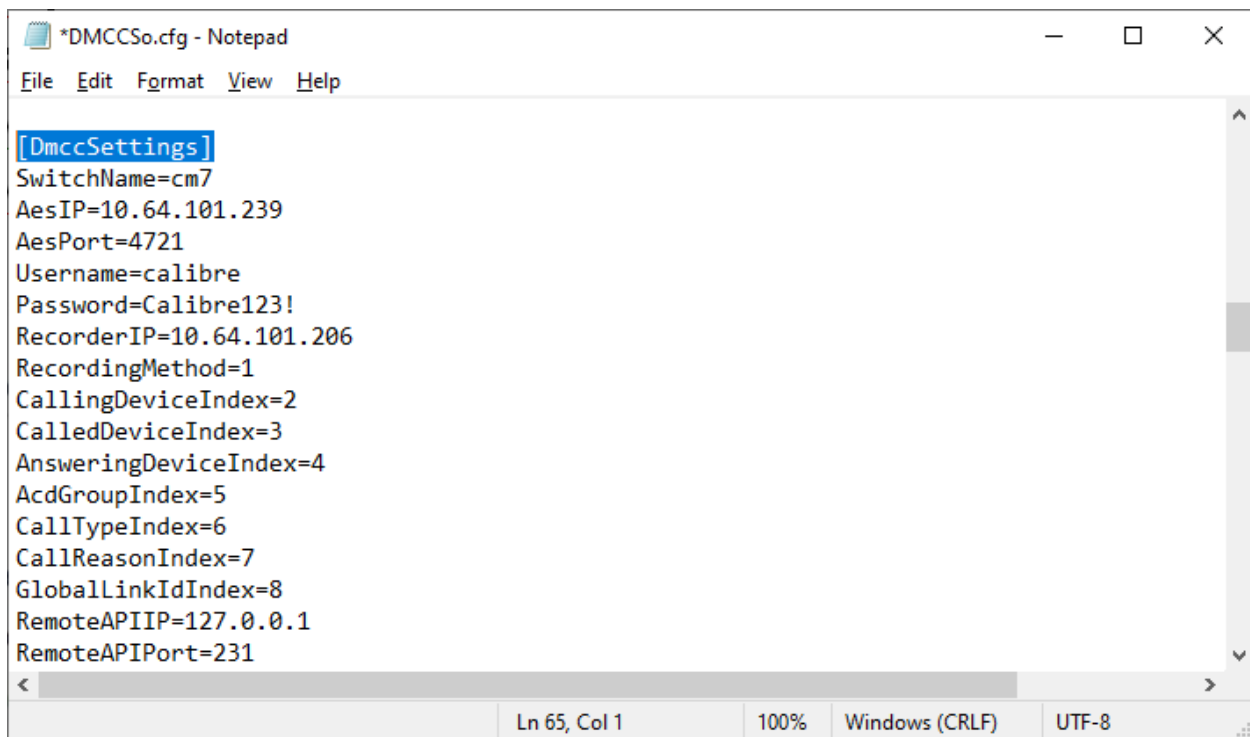


Navigate to the **Settings** sub-section and set **ConnectionType** to “**DMCCConnection**” as show below.



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

- **SwitchName:** The switch connection name from **Section 6.3**.
- **AesIP:** IP address of Application Enablement Services.
- **AesPort:** The DMCC unencrypted port from **Section 6.7**.
- **Username:** The Calibre user credentials from **Section 6.5**.
- **Password:** The Calibre user credentials from **Section 6.5**.
- **RecorderIP:** IP address of the Calibre server.
- **RecordingMethod:** "1" for Service Observing.
- **CallingDeviceIndex:** "2"
- **CalledDeviceIndex:** "3"
- **AnsweringDeviceIndex:** "4"
- **AcdGroupIndex:** "5"
- **CallTypeIndex:** "6"
- **CallReasonIndex:** "7"
- **GlobalLinkIdIndex:** "8"



```
*DMCCSo.cfg - Notepad
File Edit Format View Help

[DmccSettings]
SwitchName=cm7
AesIP=10.64.101.239
AesPort=4721
Username=calibre
Password=Calibre123!
RecorderIP=10.64.101.206
RecordingMethod=1
CallingDeviceIndex=2
CalledDeviceIndex=3
AnsweringDeviceIndex=4
AcdGroupIndex=5
CallTypeIndex=6
CallReasonIndex=7
GlobalLinkIdIndex=8
RemoteAPIIP=127.0.0.1
RemoteAPIPort=231

Ln 65, Col 1    100%    Windows (CRLF)    UTF-8
```


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

For each extension entry, set the value to the station extension associated with a VoIP channel from **Section 8.4**, followed by an available virtual IP softphone extension and security code from **Section 5.7**, and the VoIP channel port number from **Section 8.4**. In the compliance testing, two extension entries were created as shown below.



```
*DMCCSo.cfg - Notepad
File Edit Format View Help
[DmccExtensions]
Count=2
Extension1=65001:65991:123456:50000
Extension2=66006:65992:234567:50001
```

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

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

Make certain that there is a **RecorderController** sub-section with parameters and default values shown below.

Follow the procedures in **Section 8.2** to stop and start the **HigherGround Task Master** service again.



```
*DMCCSo.cfg - Notepad
File Edit Format View Help
[DmccAcdGroups]
Count=2 ; Default: 0
AcdGroup1=61001:0:0:0
AcdGroup2=61002:0:0:0

[RecorderController]
RecorderName=localhost
RecorderPort=231
RecorderIPV6=0
MaxIdle=120
RecorderName2=
RecorderPort2=0
RecorderIPV62=0
AlarmPeriod=600
```

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aes7	established	45	53

Verify registration status of the virtual IP softphones by using the “**list registered-ip-stations**” command. Verify that all virtual IP softphones from **Section 5.7** are displayed along with the IP address of the Application Enablement Services server, as shown below.

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

REGISTERED IP STATIONS			
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
65000	9611	IP_Phone	192.168.200.179
tls	1	6.8502	10.64.101.236
65001	9611	IP_Phone	192.168.200.212
tls	1	6.8502	10.64.101.236
65991	9608	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236
65992	9608	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236

9.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **User** column shows an active session with the Calibre user name from **Section 6.5** and that the number **# of Associated Devices** reflects the total number of monitored skill groups and agent stations from **Section 3** plus the number of virtual IP softphones from **Section 5.7**, in this case “6”.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Nov 9 11:48:41 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Nov 09 12:04:49 EST 2021
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ **Status**

Alarm Viewer

▶ Logs

▶ Log Manager

▼ **Status and Control**

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ **DMCC Service Summary**

▪ Switch Conn Summary

▪ TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Tue Nov 09 12:04:49 EST 2021

Service Uptime: 1 days, 1 hours 10 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 3

Number of Existing Devices: 6

Number of Devices Created Since Service Boot: 18

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	D45208FB272F3753D 010A4932369F53B-2	calibre	HgDMCC	10.64.101.206	XML Unencrypted	6

Terminate Sessions

Show Terminated Sessions

Item 1-1 of 1
1 Go

Verify status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is “**Talking**” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**, in this case “**4**”.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Tue Nov 9 11:48:41 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Nov 09 12:05:27 EST 2021
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

TSAPI Link Details

☐ Enable page refresh every 60 seconds

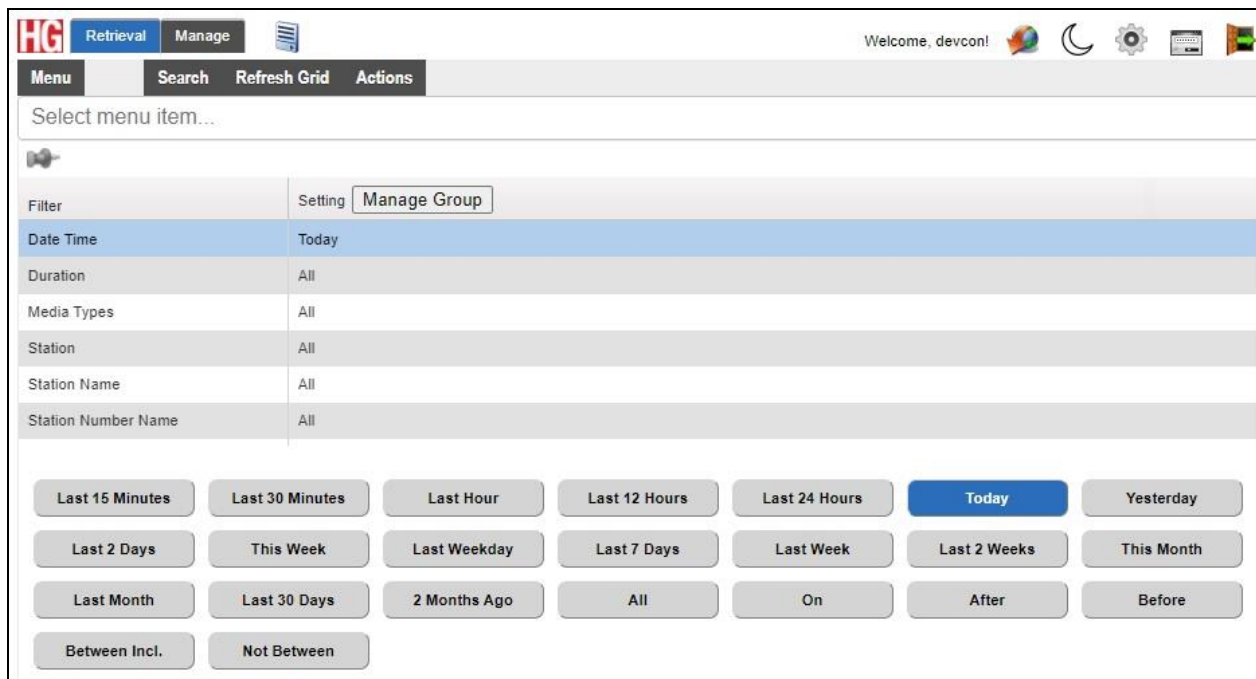
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Mon Nov 8 10:53:44 2021	Online	18	4	53	45	30

9.3. Verify HigherGround Calibre

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



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



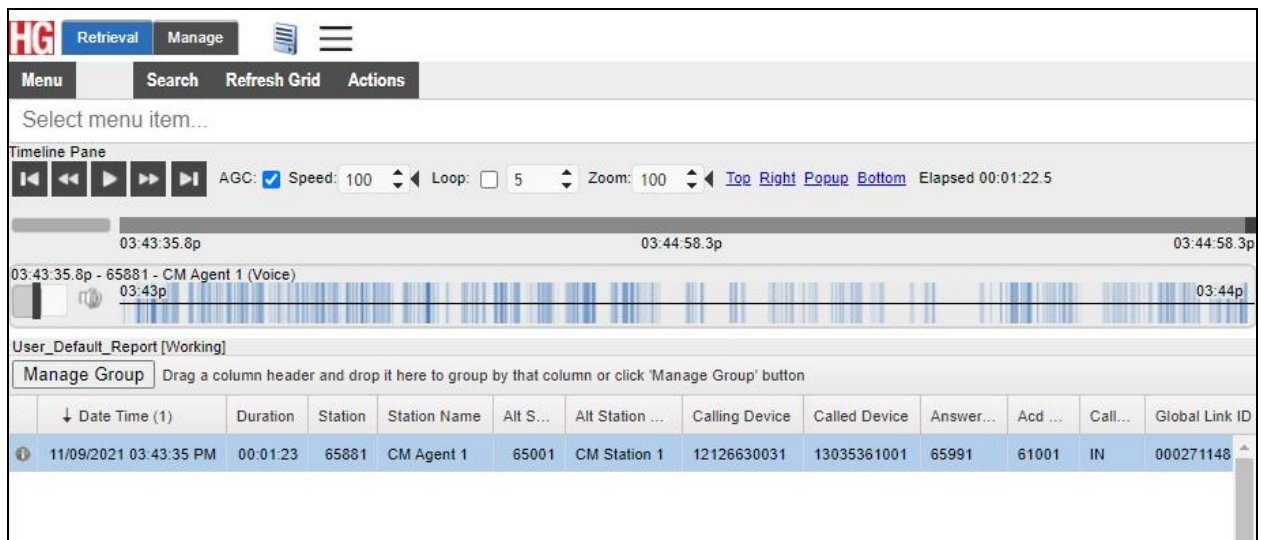
The screen is updated with a list of call recordings for today. Verify that there is an entry for the last call with proper values in the relevant fields as shown below.



The screenshot shows a web application interface with a top navigation bar containing 'Retrieval' and 'Manage' buttons. Below this is a menu bar with 'Menu', 'Search', 'Refresh Grid', and 'Actions'. A search bar is present with the text 'Select menu item...'. Below the search bar is a section titled 'User_Default_Report [Working]' with a 'Manage Group' button and a instruction: 'Drag a column header and drop it here to group by that column or click 'Manage Group' button'. The main content is a table of call recordings.

	↓ Date Time (1)	Duration	Station	Station Name	Alt S...	Alt Station ...	Calling Device	Called Device	Answer...	Acid ...	Call...	Global Link ID
1	11/09/2021 03:43:35 PM	00:01:23	65881	CM Agent 1	65001	CM Station 1	12126630031	13035361001	65991	61001	IN	00027114811

Double click on the entry, and verify that the recording can be played back.



The screenshot shows the same web application interface as the previous one, but with the 'Timeline Pane' open. The timeline pane displays a waveform of the call recording. The timeline starts at 03:43:35.8p and ends at 03:44:58.3p. The waveform is labeled '03:43:35.8p - 65881 - CM Agent 1 (Voice)'. The timeline pane also includes playback controls: a play button, a speed slider set to 100, a loop button, a zoom slider set to 100, and buttons for 'Top Right Popup' and 'Bottom'. The 'Elapsed' time is 00:01:22.5. Below the timeline pane is the same 'User_Default_Report [Working]' section with the 'Manage Group' button and the table of call recordings.

	↓ Date Time (1)	Duration	Station	Station Name	Alt S...	Alt Station ...	Calling Device	Called Device	Answer...	Acid ...	Call...	Global Link ID
1	11/09/2021 03:43:35 PM	00:01:23	65881	CM Agent 1	65001	CM Station 1	12126630031	13035361001	65991	61001	IN	000271148

10. Conclusion

These Application Notes describe the configuration steps required for Calibre 9 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, November 2020, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, February 2021, available at <http://support.avaya.com>.
4. *HG4 Installation Manual*, v.9.2021, available as part of Calibre installation.
5. *HG4 Admin Manual*, v.9.2020, available as part of Calibre installation.
6. *HG4 User Manual*, v.9.2020, available as part of Calibre installation.

©2021 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.