



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

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 to interoperate with Red Box Recorder's Quantify 5B using Single Step Conference – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for Red Box Recorders Quantify 5B solution with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Red Box Recorder's Quantify 5B system is a voice recording solution which can be used to record voice streams for Avaya telephony.

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

The purpose of this document is to describe the compliance testing carried out using the Single Step Conference recording method on Red Box Recorder's Quantify solution with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. It includes a description of the configuration of both the Avaya and the Red Box Recorder's Quantify solutions, a description of the tests that were performed and a summary of the results of those tests.

Quantify is a voice recording system which can be used to record the voice stream of Avaya telephony endpoints. In this compliance test, it uses Avaya Aura® Communication Manager's Single Step Conference feature via the Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to capture the audio and call details for call recording. The application uses the Avaya Aura® Application Enablement Services DMCC service to register virtual extensions that are associated with the extensions to be recorded. When the extension receives an event pertaining to the start of a call, the application opens a conference with the extensions and records the RTP media stream.

The Quantify solution comprises of Red Box Recorder's Server licensed for Avaya "Active" recording.

## 2. General Test Approach and Test Results

The test approach was to verify that the calls placed and recorded using the Quantify solution with Avaya solution functioned correctly with good audio quality received. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, conference, call pick-up, call park, call forward and calls to/from the PSTN. Tests also included ACD Agent Recording. Serviceability testing were also included where the LAN cables were disconnected to AES, Quantify Server and Media Gateway. All tests were successful.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and Quantify did not include use of any specific encryption features as requested by Red Box Recorders.

## **2.1. Interoperability Compliance Testing**

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios to ensure good quality audio recordings were received. Intra-switch calls were made on the Communication Manager and inbound and outbound calls from/to the PSTN. The serviceability testing focused on verifying the ability of Quantify to recover from disconnection and reconnection of the Avaya solution.

## **2.2. Test Results**

All functionality and serviceability test cases were completed successfully with the following observations.

- When a call is transferred using the consult method the recording contained three calls. Quantify shows the initial call, the consult, and the consult and transferred call. The call containing the consult and transferred call displays as being between the called and transferred party and does not indicate there is a call between the caller and transferred party.
- When an initial caller whether internal or external party calls a recorded station, this station makes a blind conference with an internal station which is also recorded, there is no recording for the conference or after the conference maker drops off. This issue is identified by Red Box Recorders and will be fixed with a patch.

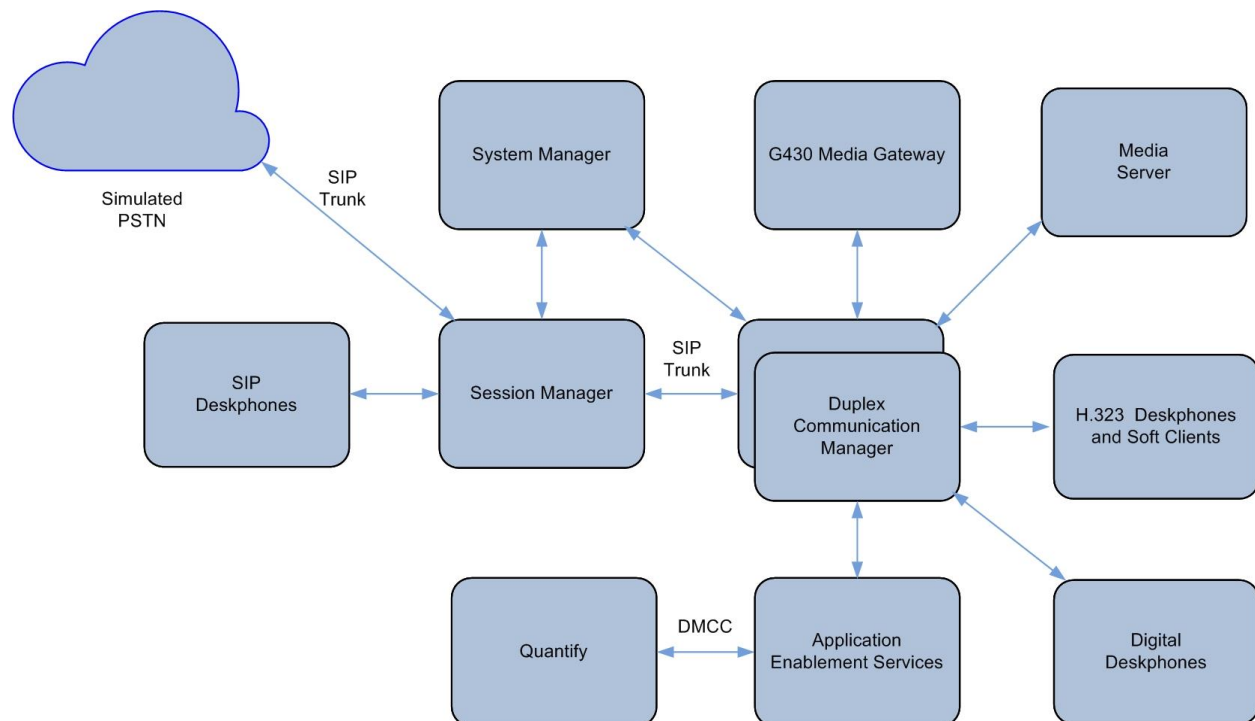
## **2.3. Support**

Technical support can be obtained for Red Box Recorder's solution as follows:

- Email: [support@redboxrecorders.com](mailto:support@redboxrecorders.com)
- Website: [www.redboxrecorders.com](http://www.redboxrecorders.com)
- Phone: +44 (0) 115 9377100

### 3. Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya Aura® Communication Manager with Avaya G430 Media Gateway as the PBX and Avaya Aura® Application Enablement Services. Avaya Vantage (SIP), 96x1 series IP Deskphones (SIP and H.323), 1600 Series IP Deskphones (H.323), J100 series IP Deskphones (SIP and H.323) and 9400 series Digital Deskphones are connected to the PBX and used in the testing. Avaya one-X® Agent (H.323) is setup as softphone. The Quantify server was used in the compliance test. The Quantify system is installed on a Windows 2016 server.



**Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services Server and Red Box Recorder's Quantify 5B Configuration**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration as shown in **Figure 1**.

Equipment	Software
Avaya Aura® System Manager running on a virtual server	System Manager 8.1.1.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.1.0.0310503 Feature Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.1 FP1 Build No. – 8.1.0.0.810015
Avaya Aura® Communication Manager running on Virtual Server	R018x.01.0.890.0 R8.1.0.2.0 – SP2 Update ID 01.0.890.0-25578
Avaya Aura® Application Enablement Services running on Virtual Server	R8.1 Build No – 8.1.0.0.1.9-1
Avaya G430 Media Gateway	41.10.0 /1
Avaya Media Server running on a Virtual Server	R8.0.1.121
Avaya 9608 H323 Deskphone	6.8202
Avaya 1616 -I H323 Deskphone	1.312
Avaya J179 H323 Deskphone	6.8202
Avaya 9641 SIP Deskphone	7.1.6.1.3
Avaya J129 SIP Deskphone	4.0.2.1.3
Avaya Vantage Equinox	3.7.0.104
Avaya 9408 Digital Deskphone	2.0 SP9 (R20)
Avaya one-X® Agent	R2.5.12
Red Box Quantify Recording Suite running on Windows 2016	5B Build 39

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- Configure Virtual Extensions for the Recording Pool
- Configure Interface to AES

### 5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

<b>display system-parameters customer-options</b>		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? y	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	<b>Computer Telephony Adjunct Links? y</b>	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? y		
(NOTE: You must logoff & login to effect the permission changes.)		

## 5.2. Configure virtual stations for the recording pool

Use the **add station** command to configure a station for each of the virtual stations to be used for the recorder channels. Enter in a descriptive **Name** and **Security Code** for each one. The **Security Code** will be referenced by Quantify when setting up the recording extensions. Set the **IP Softphone?** to **y**.

add station 19901		Page 1 of 5
STATION		
Extension: 19901	Lock Messages? n	BCC: 0
Type: 9640	<b>Security Code: *</b>	TN: 1
Port: S000395	Coverage Path 1:	COR: 1
<b>Name: RedBox Virtual #1</b>	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: 19901	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

### 5.3. Configure Interface to Avaya Aura® Application Enablement Services

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Add an available cti-link number which in this case is **3**. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification.

<b>add cti-link 3</b>	Page 1 of 3
CTI LINK	
CTI Link: 3	
Extension: 10093	
Type: ADJ-IP	
COR: 1	
Name: TSAPI Service - AES 8x	
Unicode Name? n	

Obtain the AES server host name from the AES console using the “uname -a” command as below:

```
[cust@aes ~]$ uname -a
Linux aes 3.10.0-1062.1.2.el7.x86_64 #1 SMP Mon Sep 16 14:19:51 EDT 2019 x86_64
x86_64 x86_64 GNU/Linux
[cust@aes ~]$
```

Configure IP-Services for the **AESVCS** service using **change ip-services** command. Using the Local Node name **procr** which means the server processor interface. Set **Enabled** to **y** and leave the **Port** as default.

<b>change ip-services</b>	Page 1 of 4				
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
<b>AESVCS</b>	<b>y</b>	<b>procr</b>	<b>8765</b>		
CDR1		procr	0	FCSGW	5052
PMS		procr	0	FCSGW	5053

Navigate to **Page 4**, set the **AE Services Server** which is the AES host name above and the **Password** the AES Server will use to authenticate with Communication Manager as created in **Section 6.2**.

<b>change ip-services</b>	Page 4 of 4			
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:				
2:	<b>aes</b>	<b>*</b>	<b>y</b>	in use



## 6. Configuration of Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services (AES). The procedures fall into the following areas:

- Verify Licensing
- Create Switch Connection
- Create CTI User
- Enable CTI User
- Configure DMCC Port

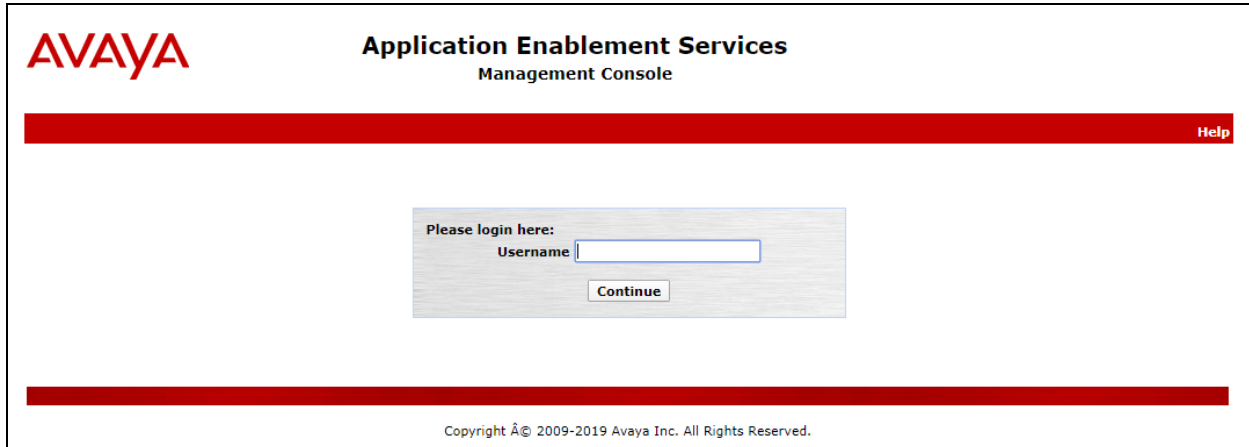
### 6.1. Verify Licensing

Access the Web License Manager used by the Application Enablement Services Server. The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane. Verify that there are sufficient licenses for **Device Media and Call Control**, as shown below. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.

WebLM Home	Application Enablement (CTI) - Release: 8 - SID: 10503000	Standard License file
Install license	You are here: Licensed Products > Application_Enablement > View License Capacity	
Licensed products	License installed on: December 24, 2019 11:05:02 AM +08:00	
APPL_ENAB		
▼ Application_Enablement		
View license capacity	License File Host IDs: VD-1F-D2-AD-7F-5A-01	
View peak usage		
CE		
►COLLABORATION_ENVIRONMENT		
COMMUNICATION_MANAGER		
►Call_Center		
►Communication_Manager		
Configure Centralized Licensing		
MESSAGING		
►Messaging		
MSR		
►Media_Server		
SYSTEM_MANAGER		
►System_Manager		
SessionManager		
►SessionManager		
VSS		
►Voice_Portals		
Uninstall license		
Server properties		
<b>Licensed Features</b>		
13 Items Show All ▼		
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	2500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	0
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	2500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	0
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	2500

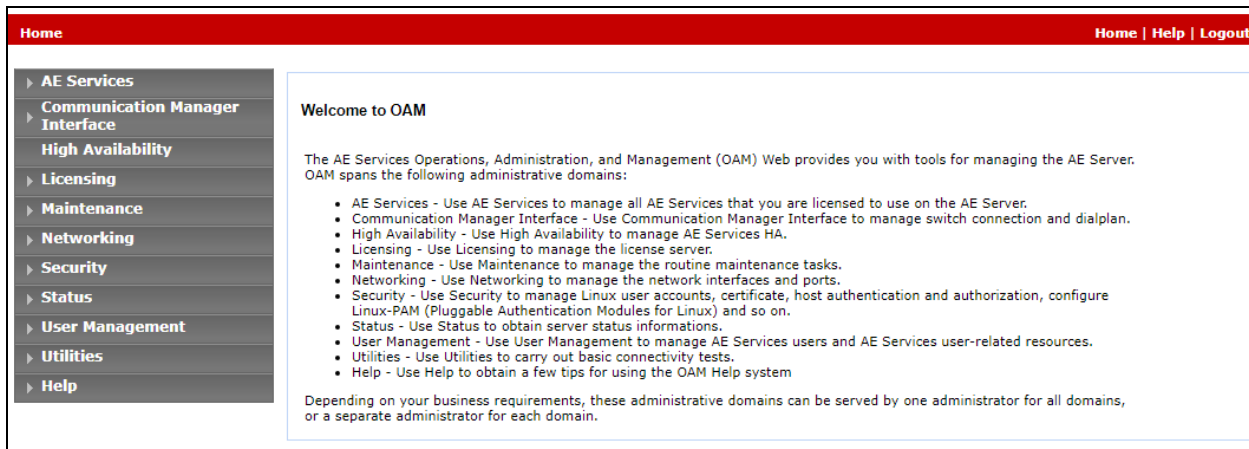
## 6.2. Create Switch Connection

Access the OAM web-based interface of the Application Enablement Services Server, using the URL [https://<Server\\_IP>](https://<Server_IP>). The Management console is displayed, login using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login page. 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, another red horizontal bar is present, with the copyright notice "Copyright © 2009-2019 Avaya Inc. All Rights Reserved." centered below it.

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



The screenshot shows the "Welcome to OAM" screen. At the top, a red horizontal bar contains the "Home" link on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical navigation menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area on the right 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 of domains and their functions. At the bottom of the main content area, there is a paragraph stating: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."

**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.

To establish the connection between Communication Manager and the Application Enablement Services Server, click **Communication Manager Interface** → **Switch Connections**. In the field next to next to **Add Connection**, enter **Duplex** and click on **Add Connection** (not shown), the following screen will be displayed.

**Communication Manager Interface | Switch Connections**

- AE Services
  - Communication Manager Interface
    - Switch Connections
    - Dial Plan
    - High Availability
    - Licensing
    - Maintenance
    - Networking
    - Security

**Connection Details - Duplex**

Switch Password

Confirm Switch Password

Msg Period  Minutes (1 - 72)

Provide AE Services certificate to switch ☒

Secure H323 Connection ☒

Processor Ethernet ☒

Complete the configuration as shown and enter the password specified in **Section 5.3** when configuring AESVCS in ip-services. Enter an appropriate **Switch Password**. Click on **Apply**, the screen below will be displayed.

**Communication Manager Interface | Switch Connections**

- AE Services
  - Communication Manager Interface
    - Switch Connections
    - Dial Plan
    - High Availability
    - Licensing
    - Maintenance
    - Networking

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> Duplex	Yes	30	1
<input type="radio"/> G450	Yes	30	1

Click on **Edit PE/CLAN IPs** (at the bottom of the last screenshot) in order to specify the IP address of the Communication Manager. Next to **Add Name or IP**, enter the IP address of the Communication Manager and click on **Add Name or IP**.

**Communication Manager Interface | Switch Connections** Home | Help | Logout

- AE Services
  - Communication Manager Interface
    - Switch Connections
    - Dial Plan
    - High Availability
    - Licensing

**Edit Processor Ethernet IP - Duplex**

Name or IP Address	Status
10.1.10.230	In Use

Click on **Back** and then click on **Edit H.323 Gatekeeper**. Enter the IP address of the Communication Manager and click on **Add Name or IP**.

**Communication Manager Interface | Switch Connections**

AE Services  
 Communication Manager Interface  
 Switch Connections  
 Dial Plan  
 High Availability  
 Licensing

**Edit H.323 Gatekeeper - Duplex**

Name or IP Address

☒ 10.1.10.230

Select **AE Services** from the left-hand menu and select **DMCC** to verify that the **DMCC Service** is licensed by ensuring that **DMCC Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.

**AE Services** Home | Help | Logout

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	OFFLINE	Running	N/A	N/A
<b>DMCC Service</b>	<b>ONLINE</b>	<b>Running</b>	<b>NORMAL MODE</b>	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

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

\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

**License Information**  
 You are licensed to run Application Enablement (CTI) release 8.x

### 6.3. Create CTI User

A user ID and password needs to be configured for the Red Box recorder to communicate as a DMCC Client with the Application Enablement Services. Select **User Management → User Admin → Add User** from the left-hand menu, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

**User Management | User Admin | Add User**

▶ 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

Redbox

\* Common Name

Redbox

\* Surname

Redbox

\* 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

## 6.4. Enable CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. In the **CTI Users** window, select the user that was set up in **Section 6.3** and select the **Edit** option.

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

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> eicc	eicc	NONE	NONE
<input type="radio"/> psadmin	psadmin	NONE	NONE
<input checked="" type="radio"/> Redbox	Redbox	NONE	NONE
<input type="radio"/> Test	Test	NONE	NONE

[Edit](#) [List All](#)

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

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

Edit CTI User

User Profile:

User ID: Redbox  
Common Name: Redbox  
Worktop Name: NONE ▼  
**Unrestricted Access** ☒

Call and Device Control: Call Origination/Termination and Device Status: None ▼

Call and Device Monitoring:

Device Monitoring: None ▼  
Calls On A Device Monitoring: None ▼  
Call Monitoring: ☐

Routing Control: Allow Routing on Listed Devices: None ▼

[Apply Changes](#) [Cancel Changes](#)

## 6.5. Configure DMCC Port

On the AES Management Console navigate to **Networking → Ports** to set the DMCC server port. During the compliance test, the **Unencrypted Port** set to **4721** was **Enabled** as shown in the screen below. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

The screenshot shows the 'Networking | Ports' configuration page in the AES Management Console. The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking (selected), AE Service IP (Local IP), Network Configure, Ports (highlighted), TCP/TLS Settings, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Ports' and contains several sections:

- CVLAN Ports:** Includes 'Unencrypted TCP Port' (9999) and 'Encrypted TCP Port' (9998), each with 'Enabled' and 'Disabled' radio buttons. The 'Unencrypted TCP Port' is currently selected.
- DLG Port:** Includes 'TCP Port' (5678).
- TSAPI Ports:** Includes 'TSAPI Service Port' (450), 'Local TLINK Ports' (1024), 'TCP Port Min' (1039), 'Unencrypted TLINK Ports' (1050), 'TCP Port Max' (1065), 'Encrypted TLINK Ports' (1066), and 'TCP Port Max' (1081). Each has 'Enabled' and 'Disabled' radio buttons.
- DMCC Server Ports:** Includes 'Unencrypted Port' (4721), 'Encrypted Port' (4722), and 'TR/87 Port' (4723). Each has 'Enabled' and 'Disabled' radio buttons. The 'Unencrypted Port' is currently selected and highlighted with a red box.

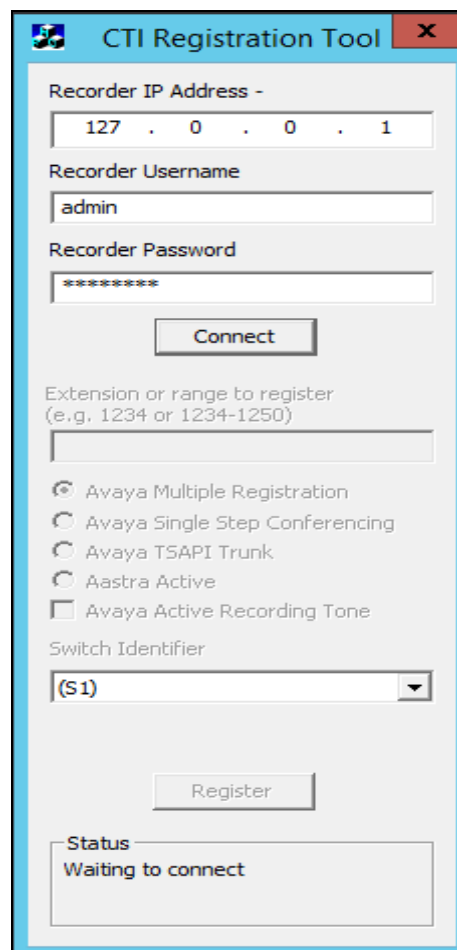
## 7. Configuration of Quantify

The Quantify Server is provided pre-installed with Quantify 5B. Administering an IP address on Microsoft Windows is outside of the scope of this document. There are two main components to configure the recording solution as follows.

- Register extensions to Quantify
- Configure Quantify to connect to Application Enablement Services

### 7.1. Register Extensions to Quantify

Run the **CTI Reg Tool**, located in **C:\LTR\utils** on the Red Box Recorder Server, the **CTI Reg Tool** is used to access the Red Box Recorder server and assign extensions which are to be recorded. Accept the default **Recorder IP Address**, **Recorder Username** and **Recorder Password** and click **Connect**. Select the radio button **Avaya Single Step Conferencing** and enter the extension numbers to be recorded in the **Extension or Range to register** field. Click **Register** and the devices are registered with the recorder. Select **Disconnect** button when complete and close down the **CTI Registration Tool** dialog box.

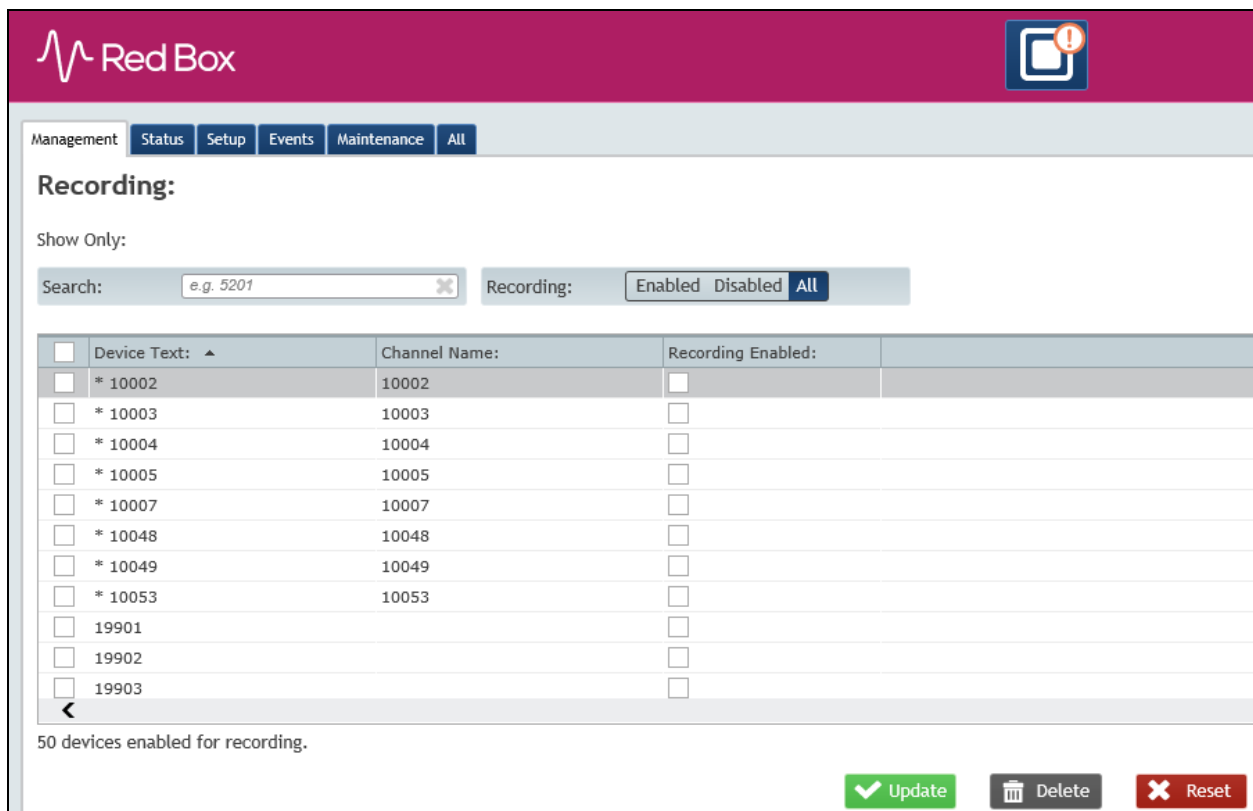


The screenshot shows the 'CTI Registration Tool' window. It has a title bar with a standard Windows icon and a close button. The main area contains several fields and controls:

- Recorder IP Address -**: A text field containing '127 . 0 . 0 . 1'.
- Recorder Username**: A text field containing 'admin'.
- Recorder Password**: A text field containing '\*\*\*\*\*'.
- Connect**: A button located below the password field.
- Extension or range to register**: A text field with a placeholder '(e.g. 1234 or 1234-1250)'.
- Registration Options**: A group of radio buttons and a checkbox:
  - ☒ Avaya Multiple Registration
  - ☐ Avaya Single Step Conferencing
  - ☐ Avaya TSAPI Trunk
  - ☐ Aastra Active
  - ☐ Avaya Active Recording Tone
- Switch Identifier**: A dropdown menu showing '(S1)'.
- Register**: A button located below the switch identifier.
- Status**: A text area showing 'Waiting to connect'.



The web interface is used to configure the extensions. Use **http://<server IP>** to access the **Recording** screen of the Red Box Recorder. The extensions which were added earlier in this section should appear in the **Recording** screen as shown below.



Red Box

Management Status Setup Events Maintenance All

**Recording:**

Show Only:


Search:  Recording: Enabled Disabled All

<input type="checkbox"/>	Device Text: ▲	Channel Name:	Recording Enabled:
<input type="checkbox"/>	* 10002	10002	<input type="checkbox"/>
<input type="checkbox"/>	* 10003	10003	<input type="checkbox"/>
<input type="checkbox"/>	* 10004	10004	<input type="checkbox"/>
<input type="checkbox"/>	* 10005	10005	<input type="checkbox"/>
<input type="checkbox"/>	* 10007	10007	<input type="checkbox"/>
<input type="checkbox"/>	* 10048	10048	<input type="checkbox"/>
<input type="checkbox"/>	* 10049	10049	<input type="checkbox"/>
<input type="checkbox"/>	* 10053	10053	<input type="checkbox"/>
<input type="checkbox"/>	19901		<input type="checkbox"/>
<input type="checkbox"/>	19902		<input type="checkbox"/>
<input type="checkbox"/>	19903		<input type="checkbox"/>

50 devices enabled for recording.

Update Delete Reset

Tick the checkbox under column **Recording Enabled** to configure these extensions for recording. Select **Update** (not shown) below and the extensions will be enabled for recording.



Management
Status
Setup
Events
Maintenance
All

### Recording:

Show Only:

Search:
Recording:
Enabled
Disabled
All

<input type="checkbox"/>	Device Text: ▲	Channel Name:	Recording Enabled:
<input type="checkbox"/>	10002		<input checked="" type="checkbox"/>
<input type="checkbox"/>	10003	10003	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10004		<input checked="" type="checkbox"/>
<input type="checkbox"/>	10005	10005	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10007	10007	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10048		<input checked="" type="checkbox"/>
<input type="checkbox"/>	10049		<input checked="" type="checkbox"/>
<input type="checkbox"/>	10053		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19901		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19902		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19903		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19904		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19905		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19906		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19907		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19908		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19909		<input checked="" type="checkbox"/>
<input type="checkbox"/>	19910		<input checked="" type="checkbox"/>

## 7.2. Configure Red Box Recorder to connect to the Avaya Aura® Application Enablement Services

Use the config file **CTIServer\_AvayaActive.config** placed in default location of **C:\LTR\Config** to configure AES to Red Box Recorder solution. Open the file in text editor and enter in the following values. See below sample config file.

- **aesAddress:** Set this to **10.1.10.70** which is the AES IP Address
- **username:** Set this to the CTI username that was set in **Section 6.3**
- **password:** Set this to the CTI user password set in **Section 6.3**
- **switchName:** This is the name of the switch connection as set in **Section 6.2**
- **audioDestinationAddress:** Enter in the IP address that was assigned to the Red Box Recorder

Under **<!-- the ssc section is only required if Single Step Conferencing is required-->**

- **<ssc stationPassword="\*\*\*\*\*">** Enter the Virtual Station password set in **Section 5.2**
- **add start:** Set this to the range of associated extensions

Under **<!--To Add a range of recording devices -->**

- **<add start="first Extension" end="last Extension":** Enter the range of Virtual Extensions added in **Section 5.2**

```
<avaya>
<dmcc
  useSsl="false"
  aesAddress="10.1.10.70"
  username="Redbox"
  password="Redbox#1"
  dmccPort="4721"
  sessionDuration="180"
  sessionCleanupDelay="60" />

<device
  switchName="Duplex"
  audioDestinationAddress="10.1.10.125"
  multiRegistrationModelIndependent="true" />

  <!-- ACD monitoring for agent in/out info-->
<agent
  agentMonitorDevice="10003" />
<mr stationPassword="111222" />

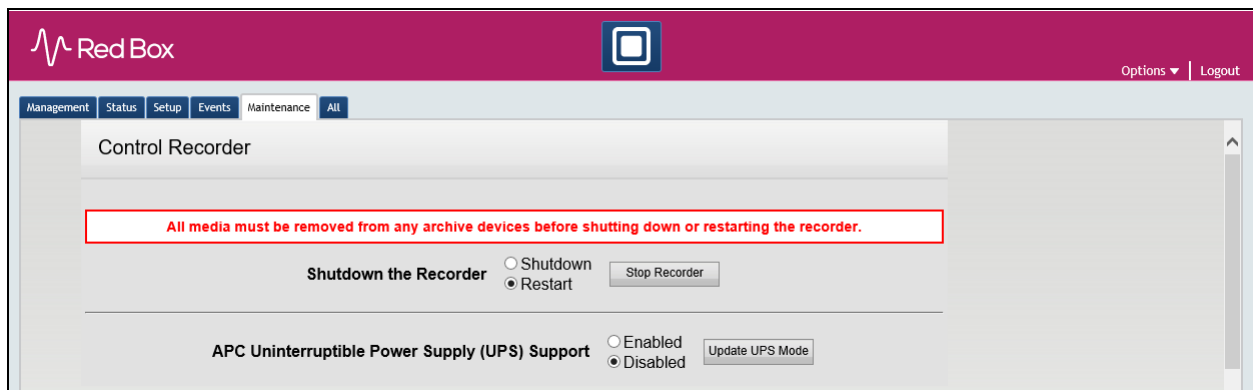
  <!-- the ssc section is only required if Single Step Conferencing is required-->
  <ssc stationPassword="*****">
</devices>
  <!-- To add a single recording device -->
  <!-- add device="8230001" / -->
```

```
<!-- add device="8237001"/ -->

<!-- To add a range of recording devices -->
<add start="19901" end="19910"/>
</devices>
</ssc>
</avaya>
```

Save the file.

Restart the recorder from the web interface, click on **Configuration → Recorder (Maintenance) icon**. Select the **Restart** radio button and click **Stop Recorder** as shown below. The Red Box Recorder will restart and is now configured to the Application Enablement Services.



## 8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya and Red Box Recorder solution.

### 8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the AESVCS link status with Application Enablement Services by using the command **status aesvcs cti-link**. The CTI Link is 3. Verify the **Service State** of the CTI link is **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
3	10	no	aes	established	15	15

### 8.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. The **Application** is set to **Red Box Recorder** and the **Far-end Identifier** is given as the IP address of the Quantify server.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Jan 14 15:22:27 2020 from 192.168.100.18  
Number of prior failed login attempts: 0  
HostName/IP: aes/10.1.10.70  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.1.9-1  
Server Date and Time: Tue Jan 14 16:05:17 SGT 2020  
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

User Management

Utilities

Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Jan 14 16:05:02 SGT 2020

Service Uptime: 4 days, 1 hours 52 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 1

Number of Existing Devices: 18

Number of Devices Created Since Service Boot: 18

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
E85EE564DF11C2B76 DA354709BD2BC90-0	Redbox	Red Box Recorder	10.1.10.125	XML Unencrypted	18

Item 1-1 of 1

1 Go

### 8.3. Verify Quantify Configuration

The following steps can be performed to verify the basic operation of the system components. Click on **Configuration → Recorder Status (Status) icon**. The Recorder Status page of the Quantify Recorder will show any alarms running. Note **Calls Being Recorded** will show number of calls currently being recorded. This page loads once logged into the recorder. See below screenshot.

**Recorder Status**

Date and Time	Alarm Details
10 Jan 2020 15:15:05	No 'Active Recording PP' packets have been detected by the recorder for the timeout period (120 seconds). Lack of packets suggests that recordings may be lost or of poor quality. Check that the system is recording and that your span is correctly configured to send traffic to the Recorder.
10 Jan 2020 11:07:30	Windows UAC is enabled. The Recorder may not function correctly. There is a potential risk for recording outages and loss of functionality. It is strongly recommended to switch UAC off using the registry settings described in the manual.
10 Jan 2020 11:06:42	The Recorder software license version is out of date. An old version of software licensing was detected. Future releases of the Recorder software may cause this license to be disabled. Check with support before upgrading your Recorder.

Item	Status
Recorder ID	125
Recorder Status	Recording
System Type	Standalone
Active Alarms	3
Unarchived Data	<div><div></div></div> 0 %
Recorder Utilization	<div><div></div></div> 0 %
Calls Being Recorded	0
Calls Being Discarded	0

No Archive Devices are licensed.

The current recorder time is:  
16:08:22, 14 Jan 2020

Choose the **Version Information** icon on the recorder screen to check the version numbers of the recorder to ensure that the version is as expected.

**Version Information**

Recorder System Release  
Quantify5B\_Build\_39

Component	Version
Recorder	5.3.1.39
Active Recording PP	5.3.3.39
CTI Only PP	5.3.4.39
Avaya Active CTI	5.3.1.39
Named Pipe Proxy	5.3.1.39
RAInterface	5.3.2.39
Quantify	5.3.39
BUI	5.3.1.39
Templates	5.3.0.39
Upload Manager	1.0
Update Manager	5.42
Support Manager	2.3

## 9. Conclusion

These Application Notes describe the configuration steps required for the Red Box Recorder's Quantify 5B to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All functionality and serviceability test cases were completed successfully with observations shown in **Section 2.2**.

## 10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 3, dated October 2019.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 3, dated August 2019.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.1.1, Issue 2, dated October 2019.

Product documentation for Red Box Recorder can be found at <http://www.redboxrecorders.com>

---

**©2020 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).