



Application Notes for Configuring Red Box Recorder's 2600 Series to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps for Red Box Recorder solution with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. Red Box Recorder system is a voice recording solution which can be used to record voice streams for Avaya telephony endpoints.

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 Conferencing recording method on Red Box Recorder 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 solutions, a description of the tests that were performed and a summary of the results of those tests.

Red Box Recorder 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 feature via the Avaya Aura™ Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording.

The application uses the Avaya Aura™ Application Enablement Services DMCC service to register a pool of standalone recording devices. The application uses the Avaya Aura™ Application Enablement Services TSAPI service to monitor the target extension for Established Call events. Whenever the extension joins a call, an Established Call event occurs which triggers the application to use the Single Step Conferencing method to add a recording device to the call. The application receives the call's aggregated RTP media stream via the recording device and records the call.

The Red Box Recorders solution comprises of Red Box Recorder's Server RBR 2610 licensed for Avaya "Active" recording. The RBR 2610 is part of the RBR 2600 series of recorders, all running the same core software, but different hardware builds to suit the individual needs of the customer. The RBR 2610 is ideally suited for Small to Medium Business for use in office environments, remote locations or equipment rooms. The RBR2610 is one of three recorders available from the Red Box Recorders RBR 2600 series, which can provide up to 500 concurrent channels of recording per server.

1.1 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 Avaya Aura™ Communication Manager and inbound and outbound calls from/to the PSTN. The serviceability testing focused on verifying the ability of the Red Box Recorder to recover from disconnection and reconnection of the Avaya solution.

1.2 Support

Technical support can be obtained for Red Box Recorder's RBR 2610 solution as follows:

- Email: support@redboxrecorders.com
- Website: www.redboxrecorders.com
- Phone: +44 (0) 115 9377100

2 Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8500B Server running Communication Manager with Avaya G650 Media Gateway as the PBX. An Avaya S8510 Server hosts the Application Enablement Services software. Avaya 9600 series and 1600 series IP telephones, 2400 series Digital telephones and Avaya analogue telephones are connected to the PBX and used in the testing. The Red Box Recorders RBR 2610 server was used in the compliance test. The system is housed in a Tower based server, fitted with single power supply and RAID1, (mirrored) hard disk drives for resilience. The system supports connectivity for two interface cards offering a maximum of 48 channels of traditional telephony / radio, or 120 channels of Digital Trunks (4 x E1 Trunks). Alternatively, it can support 50 channels of VoIP or up to 50 channels of mixed TDM and VoIP.

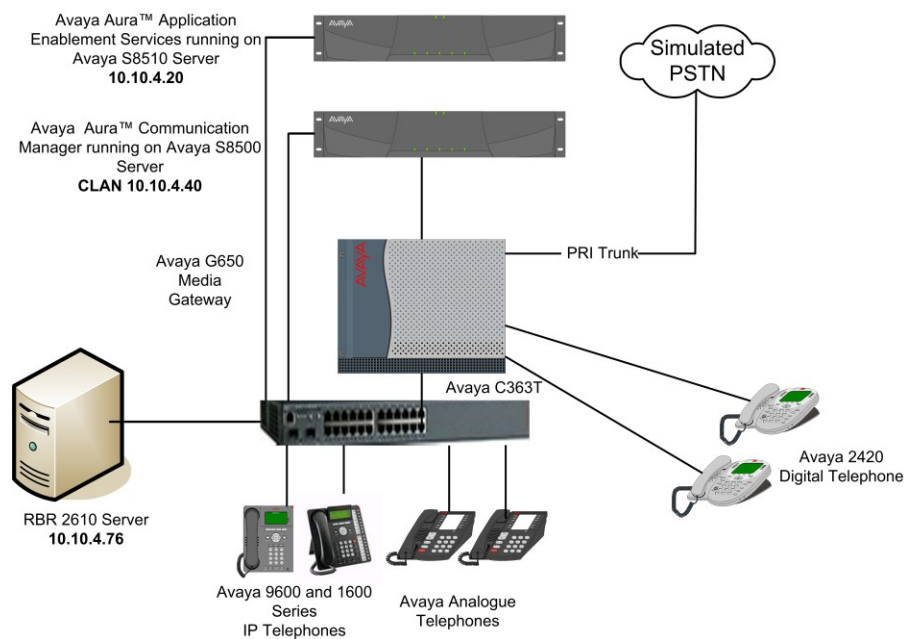


Figure 1: Network Topology

3 Equipment and Software Validated

The following hardware and software were used in the compliance testing.

Equipment	Software Version
Avaya S8500B Server	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya S8510 Server	Avaya Aura™ Application Enablement Services 5.2
Avaya G650 Media Gateway - IPSI TN2312BP - CLAN TN799DP - IP Media Processor TN2602AP - DS1 Interface TN246CP - Analog Line TN793CP - Announcement TN750C	HW15, FW50 HW01, FW38 HW02, FW54 HW02, FW024 HW09, FW10 000014
Avaya 96xx and 16xx Telephones (H.323) - 9620 - 9630 - 1616	3.1 3.1 1.22
Avaya Digital 24xx Telephones - 2420	-
Avaya Analogue Telephones - 2500	-
Avaya C363T-PWR Converged Stackable Switch	4.3.12
Red Box Recorder - RBR 2610 Server	Quantify 1D SP2 AA RAM 120.4603.0

Table 1: Hardware and Software Version Numbers

4 Configuration of 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
- Verify System Parameters Features
- Administer CTI Link for TSAPI Service
- Configure Target Stations to be Recorded
- Configure Button Assignments
- Configure Recording Pool Stations

- Configure the Interface to AES

The configuration of the PRI interface to the PSTN is outside the scope of these application notes.

4.1 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 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? n	Audible Message Waiting? n	
Access Security Gateway (ASG)? n	Authorization Codes? n	
Analog Trunk Incoming Call ID? n	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? n	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? n	
ARS/AAR Dialing without FAC? y	DCS (Basic)? n	
ASAI Link Core Capabilities? n	DCS Call Coverage? n	
ASAI Link Plus Capabilities? n	DCS with Rerouting? n	
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? n	
ATM WAN Spare Processor? n	DS1 MSP? n	
ATMS? n	DS1 Echo Cancellation? n	
Attendant Vectoring? n		

4.2 Verify System Parameters Features

Universal Call ID is used to uniquely identify calls. On **Page 5** of the system-parameters features form, set **Create Universal Call ID (UCID)?** to **y** and **UCID Network Node ID** to an unassigned node ID.

display system-parameters features		Page 5 of 18
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	
MALICIOUS CALL TRACE PARAMETERS		
	Apply MCT Warning Tone? n	MCT Voice Recorder Trunk Group:
SEND ALL CALLS OPTIONS		
	Send All Calls Applies to: station	Auto Inspect on Send All Calls? n
	Preserve previous AUX Work button states after deactivation? n	
UNIVERSAL CALL ID		

```
Create Universal Call ID (UCID)? y      UCID Network Node ID: 1
```

On Page 13, set **Send UCID to ASAI?** to **y**.

```
display system-parameters features                                     Page 13 of 18
                                FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
                                Clear Callr-info: next-call
                                Allow Ringer-off with Auto-Answer? n

                                Reporting for PC Non-Predictive Calls? n

                                Interruptible Aux Notification Timer (sec): 3
                                Interruptible Aux Deactivation Threshold (%): 95

ASAI
                                Copy ASAI UUI During Conference/Transfer? n
                                Call Classification After Answer Supervision? y
                                Send UCID to ASAI? y
```

4.3 Administer CTI Link for TSAPI Service

Enter **add cti-link n** command where **n** is an available CTI link number. The CTI link number chosen is **10**. Enter an available extension number in the **Extension** field. The **Type** must be set to **ADJ-IP** and enter a descriptive name in the **Name** field, in this case **CtiLink1**. The link number specified is used in the **Add / Edit TSAPI Links** configuration screen shown in **Section 5.3** of this document.

```
add cti-link 10                                                     Page 1 of 3
                                CTI LINK

CTI Link: 10
Extension: 5002
Type: ADJ-IP

                                COR: 1

Name: CtiLink1
```

4.4 Configure Target Stations to be Recorded

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

add station 3000	Page 1 of 5	
STATION		
Extension: 3000	Lock Messages? n	BCC: 0
Type: 2420	Security Code: 3000	TN: 1
Port: 01A0601	Coverage Path 1:	COR: 1
Name: PhoneB	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 2	Time of Day Lock Table:	
Data Option: none	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 3003	
Display Language: english	Mute Button Enabled? y	
	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Customizable Labels? y	

On **Page 2**, ensure that the **Multimedia Mode** is set to **enhanced**.

add station 3000	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	EC500 State: enabled
Multimedia Mode: enhanced	
MWI Served User Type:	Display Client Redirection? n
AUDIX Name:	Select Last Used Appearance? n
	Coverage After Forwarding? s
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y
Emergency Location Ext: 3003	Always Use? n IP Audio Hairpinning? N

4.5 Configure Station Button Assignments

Use the **change station** command to configure the button assignments of the stations to be recorded, as required. Add the appropriate button assignments as shown in the screen on **Page 4** below. In this case there are three call appearance buttons **call-appr**. There are also buttons assigned for the call functions call-pickup, bridged appearance and call park: **call-pkup**, **brdg-appr**, **call-park**.

change station 3000		Page 4 of 5	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	4: call-pkup		
2: call-appr	5: brdg-appr	B:1	E:3005
3: call-appr	6: call-park		

4.6 Configure Recording Pool Stations

A number of stations are added to act as recording pool stations. These are virtual extensions used by the RBR 2610 to record the target stations set up in **Section 4.4**. Use the add station command to add a station with **Type** of **4620**. On **Page 1** ensure that the **IP SoftPhone** parameter is set to **y**. These stations are later configured by the RBR 2610 in **Section 6.2**.

add station 3012		Page 1 of 5	
STATION			
Extension: 3012	Lock Messages? n	BCC: 0	
Type: 4620	Security Code: 1234	TN: 1	
Port: SOOO13	Coverage Path 1:	COR: 1	
Name: Virtual 1	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 19		Time of Day Lock Table:	
Data Option: none	Personalized Ringing Pattern: 1		
Speakerphone: 2-way	Message Lamp Ext: 3003		
Display Language: english	Mute Button Enabled? y		
	Expansion Module? n		
Survivable COR: internal	Media Complex Ext:		
Survivable Trunk Dest? y	IP SoftPhone? y		
	IP Video Softphone? n		
	Customizable Labels? y		

4.7 Configure Interface to Avaya Aura™ Application Enablement Services

The Application Enablement Services server has a TSAPI interface which provides Red Box Recorder with a means of communicating with Communication Manager to perform telephony operations. Communication Manager requires the configuration parameters shown in this section. Use the **add ip-interface** command to allocate a call control interface. The slot value specified should be the CLAN interface for the G650. On **Page 1** the **Node Name** is set to **CLAN** which is defined by the **change node-names ip** command. The **Subnet Mask** and **Gateway Node Name** should be assigned to the values used by the Ethernet network to which the CLAN is attached. The **Enable Interface** is set to **y** and the **Network Region** is set to **1**.

```
display ip-interface 01a02                                     Page 1 of 3

                                IP INTERFACES

                                Type: C-LAN
                                Slot: 01A02      Target socket load and Warning level: 400
                                Code/Suffix: TN799 D      Receive Buffer TCP Window Size: 8320
                                Enable Interface? y      Allow H.323 Endpoints? y
                                VLAN: n      Allow H.248 Gateways? y
                                Network Region: 1      Gatekeeper Priority: 5

                                IPV4 PARAMETERS

                                Node Name: CLAN
                                Subnet Mask: /24
                                Gateway Node Name: Gateway001
                                Ethernet Link: 1
                                Network uses 1's for Broadcast Addresses? y
```

Use the **change ip-services** command to set the parameters for **AESVCS** service for the CLAN as shown below. This was defined above to serve as the interface to the Application Enablement Services server. On **Page 1**, add **CLAN** as the **Local Node** and accept default of **8765** as **Local Port**.

change ip-services					Page	1 of	3
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	CLAN	8765				

On **Page 3**, an entry for the Application Enablement Services server is inserted as shown in the screen below. The name assigned to the Application Enablement Services server when it was installed must be entered in the **AE Services Server** field for that entry. The **Password** entry must be the same as that assigned to the switch connection, as shown in **Section 5.2** of this document.

change ip-services				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:			n	idle		
2:	PresAES	xxxxxxxxxxxxxx	y	in use		

5 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
- Administer TSAPI link
- Create CTI User
- Enable CTI Link User
- Configure DMCC Port

5.1 Verify Licensing

Access the Application Enablement Services web interface by browsing to `http://x.x.x.x`, where “x.x.x.x” is the IP address of the Application Enablement Services. Log in as in the screen below.

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, a login box contains the text "Please login here:" followed by "Username" and "Password" labels. The username field contains the text "craft" and the password field contains seven dots. A "Login" button is positioned below the password field. At the bottom of the page, a red horizontal bar contains the copyright notice "© 2009 Avaya, Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen.

The screenshot displays the "Welcome to OAM" screen of the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" along with login details. A red navigation bar contains "Home", "Help", and "Logout" links. On the left, a sidebar lists navigation options: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area features a "Welcome to OAM" heading, a brief description of the OAM web interface, a bulleted list of administrative domains and their functions, and a note about administrator roles. The footer includes the copyright notice "© 2009 Avaya, Inc. All Rights Reserved."

Welcome: User craft
Last login: Mon Jun 14 19:12:49 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Home | Help | Logout

AE Services
Communication Manager Interface
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.
- 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 both domains, or a separate administrator for each domain.

© 2009 Avaya, Inc. All Rights Reserved.

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

Application Enablement Services
Management Console

Welcome: User craft
Last login: Mon Jun 14 19:12:49 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services
[Home](#) | [Help](#) | [Logout](#)

AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI
- Communication Manager Interface**
 - Licensing
 - Maintenance
 - Networking
 - Security
 - Status
 - User Management
 - Utilities
 - Help

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	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	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) version 5.0

5.2 Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter in the name of the Switch Connection to be added and click on the **Add Connection** button.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Mon Jun 14 21:57:08 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections
[Home](#) | [Help](#) | [Logout](#)

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

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="button" value="Edit Connection"/>	<input type="button" value="Edit PE/CLAN IPs"/>	<input type="button" value="Edit H.323 Gatekeeper"/>	<input type="button" value="Delete Connection"/>

A second screen is displayed as shown below. Enter the details for each field as described below and click the **Apply** button.

- **Switch Password:** The Switch Password must be the same as that entered into Communication Manager AE Services screen via the **change ip-services** command, described in **Section 4.7**.
- **SSL:** This is enabled.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Mon Jun 14 21:57:08 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status

Connection Details - CM

Switch Password: [password field]
Confirm Switch Password: [password field]
Msg Period: 30 Minutes (1 - 72)
SSL: ☒
Processor Ethernet: ☐
Apply Cancel

The CLAN IP address must then be set on the Application Enablement Services. From the **Communication Manager Interface** → **Switch Connections** screen (not shown), click the **Edit PE/CLAN IPs** button. Enter the IP address of the CLAN which the Application Enablement Services is to use for communication with Communication Manager as defined in **Section 4.7**. Click the **Add Name or IP** button.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Mon Jun 14 21:57:08 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Edit CLAN IPs - CM

10.10.4.80 Add Name or IP
Name or IP Address Status
Delete IP Back

The H.323 Gatekeeper should be set up to point to the CLAN address on Communication Manager. Navigate to **Communication Manager Interface** → **Switch Connection** → **Edit H323 Gatekeeper** to display the screen below. Enter the IP Address and click **Add Name or IP** button as shown below.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Mon Jun 14 19:12:49 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Edit H.323 Gatekeeper - CM

10.10.4.80 Add Name or IP

Name or IP Address
Delete IP

The switch connection set up for CM shows **Number of Active Connections** to be 1.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Tue Jun 15 20:32:23 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM	No	30	1

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

5.3 Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button (not shown). On the **Add TSAPI Links** screen, enter in the following values as shown below:

- **Link** Use the drop-down list to select an unused link number.
- **Switch Connection** Choose the switch connection **CM**, which has already been configured in **Section 5.2**, from the drop-down list.
- **Switch CTI Link Number** This corresponds with the CTI link number configured in **Section 4.3** which is **10**.
- **ASAI Link Version** This can be left at the default value of **4**.
- **Security: Unencrypted** is the option chosen for this compliance test.

Once completed, select **Apply Changes**.

The following screen shows the completed entries.

AVAYA **Application Enablement Services** Management Console

Welcome: User craft
Last login: Mon Jun 14 21:57:08 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services | TSAPI | TSAPI Link Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
- ▶ Communication Manager Interface
- ▶ Licensing

Add TSAPI Links

Link: 1
Switch Connection: CM
Switch CTI Link Number: 10
ASAI Link Version: 4
Security: Unencrypted

Another screen appears for confirmation of the changes. Choose **Apply**.

AVAYA **Application Enablement Services** Management Console

Welcome: User craft
Last login: Mon Jun 14 21:57:08 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services | TSAPI | TSAPI Link Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
Please use the Maintenance -> Service Controller page to restart the TSAPI server.

When the TSAPI Link is completed, it is displayed as in the screen below.

AVAYA**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Tue Jun 15 00:18:21 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services | TSAPI | TSAPI Link

Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM	10	4	Unencrypted

Add Link Edit Link Delete Link

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, select **Maintenance** → **Service Controller**. On the Service Controller screen, tick the **TSAPI Service** box and select **Restart Service**.

AVAYA**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Mon Jun 14 21:57:08 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ Maintenance
 - Date Time/NTP Server
 - ▶ Security Database
 - Service Controller
 - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management

Service Controller

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

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

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

5.4 Create CTI User

A user ID and password needs to be configured for the Red Box recorder to communicate as a TSAPI Client with the Application Enablement Services. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option. In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Red Box recorder in **Section 6.2**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** in **Section 6.2**.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing the **Apply** button at the bottom of the screen (not shown).

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message: 'Welcome: User craft', 'Last login: Tue Jun 15 00:18:21 2010 from 10.10.4.70', 'HostName/IP: PresAES/192.11.13.6', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-0-98-0'. A red navigation bar contains 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'.

The left sidebar shows a tree view with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under 'User Admin', the 'Add User' option is selected.

The main content area is titled 'Add User'. It includes a note: 'Fields marked with * can not be empty.' Below this, a red box highlights the required fields: '* User Id' (text input with 'CTIUser'), '* Common Name' (text input with 'CTIUser'), '* Surname' (text input with 'CTIUser'), '* User Password' (password input with dots), and '* Confirm Password' (password input with dots). Other fields include 'Admin Note' (text input), 'Avaya Role' (dropdown menu with 'None' selected), 'Business Category' (text input), 'Car License' (text input), 'CM Home' (text input), 'Css Home' (text input), 'CT User' (dropdown menu with 'Yes' selected), 'Department Number' (text input), and 'Display Name' (text input).

The next screen will show a message indicating that the user was created successfully (not shown).

5.5 Enable CTI Link User

Navigate to the users screen by selecting **User Management → User Admin → List All Users**. Select the user that was set up in **Section 5.4** and select the **Edit** option.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Tue Jun 15 00:18:21 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

User Management | User Admin | List All Users Home | Help | Logout

List All Users

User Id	Common Name	Surname
<input checked="" type="radio"/> CTIUser	CTIUser	CTIUser
<input type="radio"/> avaya	avaya	avaya
<input type="radio"/> craft	craft	craft
<input type="radio"/> cust	cust	cust
<input type="radio"/> cust1	cust1	cust1
<input type="radio"/> genericdap1	genericdap1	genericdap1
<input type="radio"/> genericdap2	genericdap2	genericdap2
<input type="radio"/> replicator1	replicator1	replicator1
<input type="radio"/> tsc	tsc	tsc

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

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Wed Jun 9 18:21:32 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

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

Edit CTI User

User Profile:

User ID: CTIUser
Common Name: CTIUser
Worktop Name: NONE
Unrestricted Access: ☒

Call Origination and Termination / Device Status: None

Call and Device Monitoring:

Device: None
Call / Device: None
Call: ☐

Routing Control: Allow Routing on Listed Devices: None

A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

5.6 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 following screen. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

<ul style="list-style-type: none"> Communication Manager Interface Licensing Maintenance Networking <ul style="list-style-type: none"> AE Service IP (Local IP) Network Configure Ports Security Status User Management Utilities Help 		<h3>Ports</h3> <table> <tr> <td colspan="2">CVLAN Ports</td> <td colspan="2">Enabled Disabled</td> </tr> <tr> <td>Unencrypted TCP Port</td> <td>9999</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Encrypted TCP Port</td> <td><input type="text" value="9998"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td colspan="4"><hr/></td> </tr> <tr> <td>DLG Port</td> <td>TCP Port</td> <td>5678</td> <td></td> </tr> <tr> <td colspan="4"><hr/></td> </tr> <tr> <td colspan="2">TSAPI Ports</td> <td colspan="2">Enabled Disabled</td> </tr> <tr> <td>TSAPI Service Port</td> <td>450</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td colspan="4">Local TLINK Ports</td> </tr> <tr> <td>TCP Port Min</td> <td>1024</td> <td></td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td>1039</td> <td></td> <td></td> </tr> <tr> <td colspan="4">Unencrypted TLINK Ports</td> </tr> <tr> <td>TCP Port Min</td> <td><input type="text" value="1050"/></td> <td></td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td><input type="text" value="1065"/></td> <td></td> <td></td> </tr> <tr> <td colspan="4">Encrypted TLINK Ports</td> </tr> <tr> <td>TCP Port Min</td> <td><input type="text" value="1066"/></td> <td></td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td><input type="text" value="1081"/></td> <td></td> <td></td> </tr> <tr> <td colspan="4"><hr/></td> </tr> <tr> <td colspan="2">DMCC Server Ports</td> <td colspan="2">Enabled Disabled</td> </tr> <tr> <td>Unencrypted Port</td> <td><input type="text" value="4721"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Encrypted Port</td> <td><input type="text" value="4722"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>TR/87 Port</td> <td><input type="text" value="4723"/></td> <td><input type="radio"/></td> <td><input checked="" type="radio"/></td> </tr> <tr> <td colspan="4"><hr/></td> </tr> <tr> <td colspan="2">H.323 Ports</td> <td colspan="2"></td> </tr> </table>		CVLAN Ports		Enabled Disabled		Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>	Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>	<hr/>				DLG Port	TCP Port	5678		<hr/>				TSAPI Ports		Enabled Disabled		TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>	Local TLINK Ports				TCP Port Min	1024			TCP Port Max	1039			Unencrypted TLINK Ports				TCP Port Min	<input type="text" value="1050"/>			TCP Port Max	<input type="text" value="1065"/>			Encrypted TLINK Ports				TCP Port Min	<input type="text" value="1066"/>			TCP Port Max	<input type="text" value="1081"/>			<hr/>				DMCC Server Ports		Enabled Disabled		Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>	Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>	TR/87 Port	<input type="text" value="4723"/>	<input type="radio"/>	<input checked="" type="radio"/>	<hr/>				H.323 Ports			
CVLAN Ports		Enabled Disabled																																																																																																	
Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>																																																																																																
Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>																																																																																																
<hr/>																																																																																																			
DLG Port	TCP Port	5678																																																																																																	
<hr/>																																																																																																			
TSAPI Ports		Enabled Disabled																																																																																																	
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>																																																																																																
Local TLINK Ports																																																																																																			
TCP Port Min	1024																																																																																																		
TCP Port Max	1039																																																																																																		
Unencrypted TLINK Ports																																																																																																			
TCP Port Min	<input type="text" value="1050"/>																																																																																																		
TCP Port Max	<input type="text" value="1065"/>																																																																																																		
Encrypted TLINK Ports																																																																																																			
TCP Port Min	<input type="text" value="1066"/>																																																																																																		
TCP Port Max	<input type="text" value="1081"/>																																																																																																		
<hr/>																																																																																																			
DMCC Server Ports		Enabled Disabled																																																																																																	
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>																																																																																																
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>																																																																																																
TR/87 Port	<input type="text" value="4723"/>	<input type="radio"/>	<input checked="" type="radio"/>																																																																																																
<hr/>																																																																																																			
H.323 Ports																																																																																																			

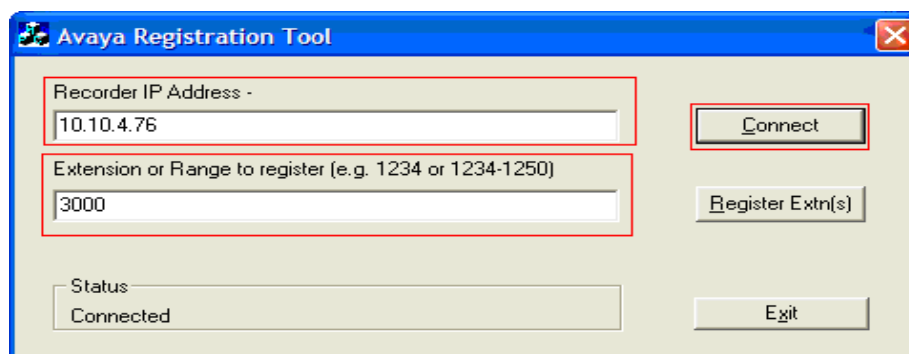
6 Configuration of Red Box Recorder

The Quantify 1D, Service Pack 2 software will already have been installed onto the RBR 2610 server. It now needs to be assigned an IP address. There are two main components to configure the recording solution as follows:

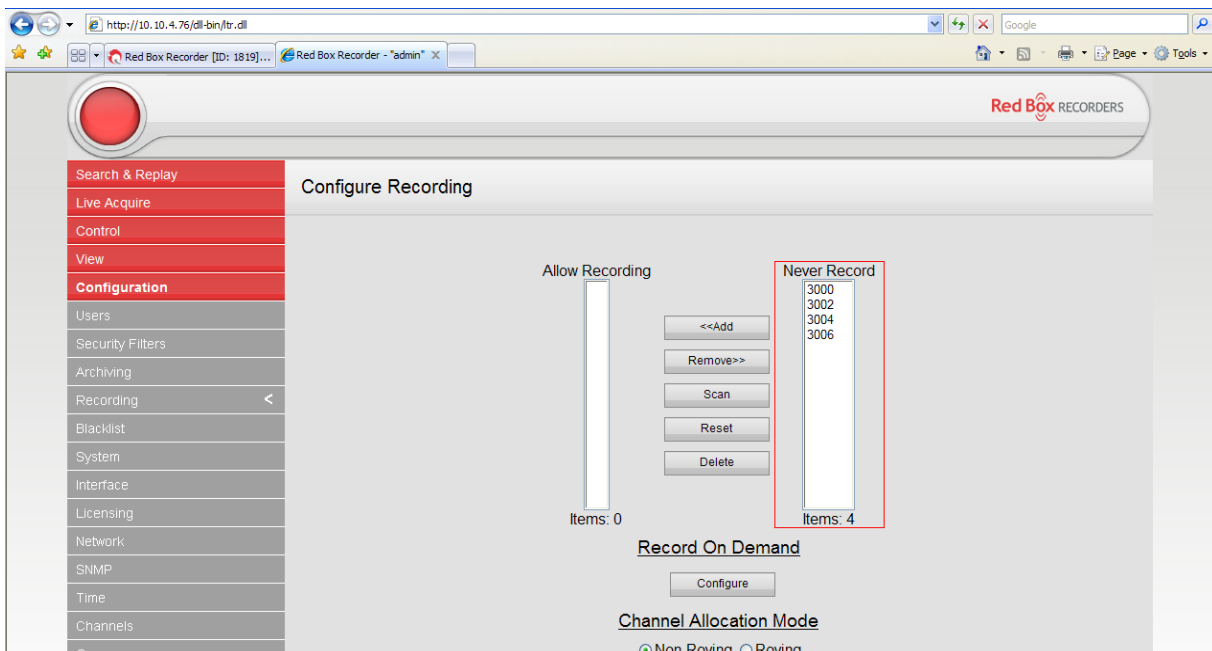
- Register extensions to RBR 2610
- Configure RBR 2610 to AES

6.1 Register Extensions to RBR 2610

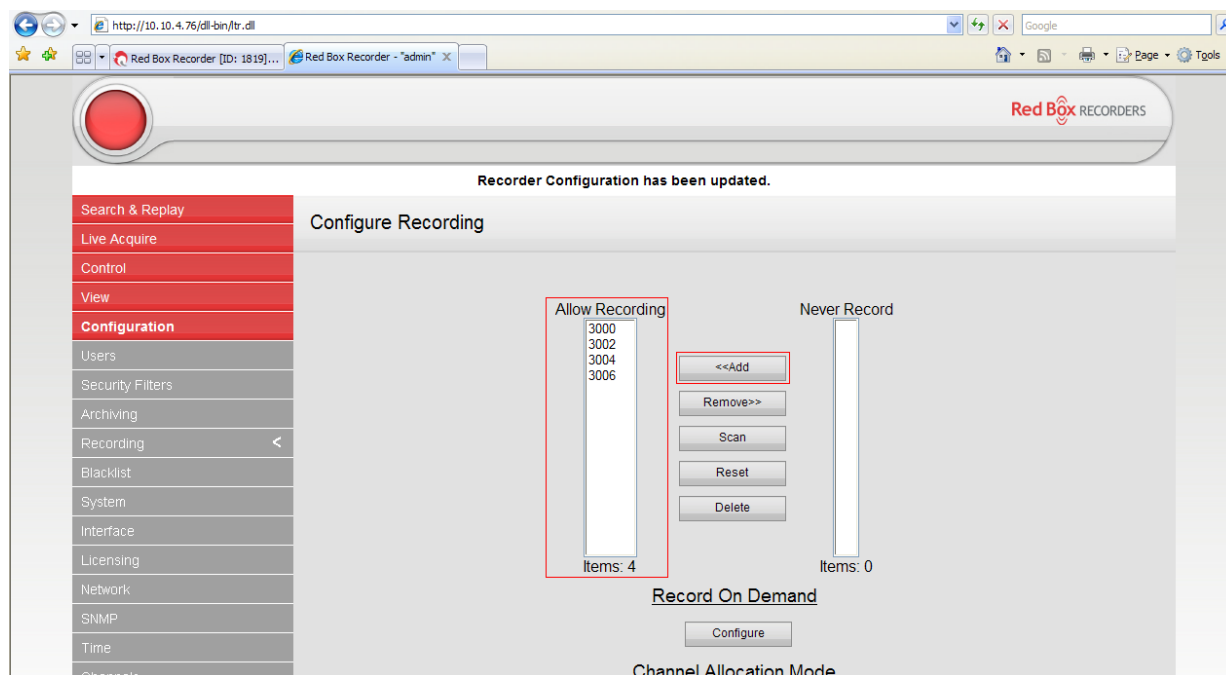
The **Avaya Registration Tool** is used to access the RBR 2610 server and assign extensions. Enter in the **Recorder IP Address** followed by the extension numbers to be recorded in the **Extension or Range to register (e.g. 1234 or 1234-1250)** field. Choose **Connect**.



The web interface is used to configure the extensions. Use ***http://10.10.4.76*** to access the **Configure Recording** screen. The extensions which were added above appear in the **Never Record** column as shown below.

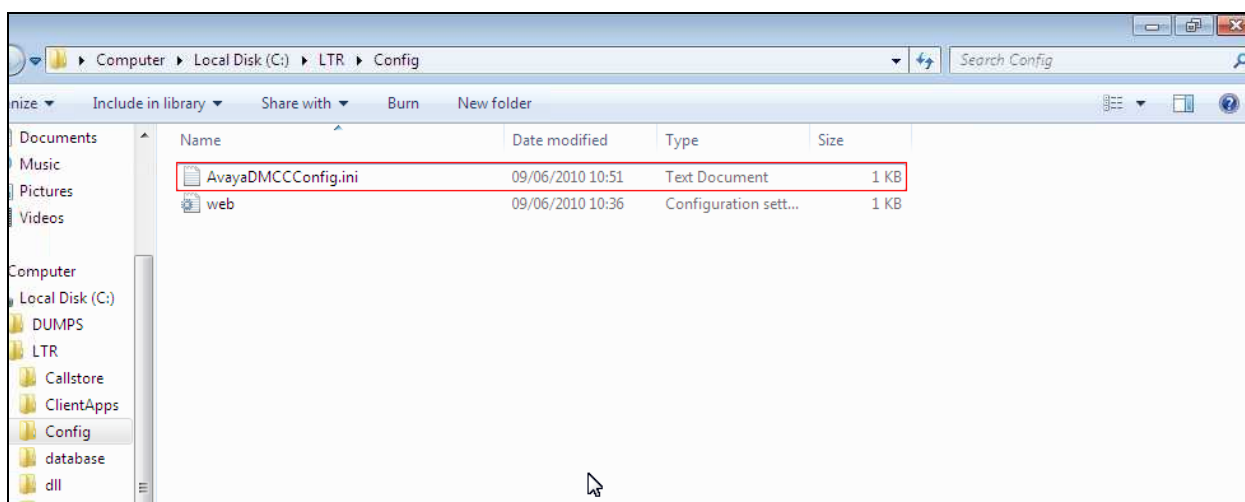


Use the **Add** button to configure these extensions for recording. Highlight the extensions and select **Add**. The extensions will then be transferred to the **Allow Recording** column.



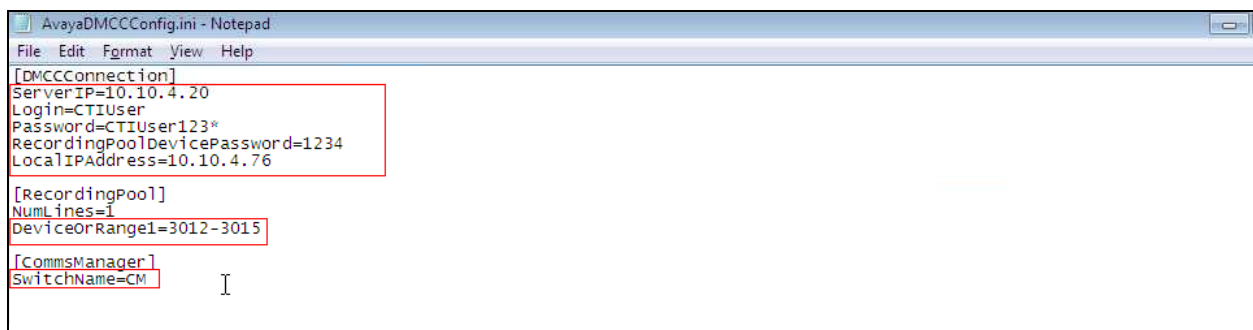
6.2 Configure RBR 2610 to Avaya Aura™ Application Enablement Services

Use the ini file **AvayaDMCCConfig.ini** placed in default location of **C:\LTR\Config** to configure AES to Red Box Recorder solution.



Open the file and enter in the following values:

- **ServerIP:** Set this to **10.10.4.20** which is the AES IP Address
- **Login:** Set this to the CTI user name that was set in **Section 5.4**.
- **Password:** Set this to the CTI user password set in **Section 5.4**.
- **RecordingPoolDevicePassword:** This is the common extension password set for each of the stations on the Communication Manager assigned to the recording device pool. These have been set up in **Section 4.6**.
- **LocalIPAddress:** Enter in the IP address that was assigned to the Red Box Recorder.
- **DeviceOrRange1:** The extension numbers that were assigned as the recording pool devices are set here; in this case a range of was set.
- **SwitchName:** This is the name of the switch connection as set in **Section 5.2**.



```
AvayaDMCCConfig.ini - Notepad
File Edit Format View Help
[DMCCConnection]
ServerIP=10.10.4.20
Login=CTIUser
Password=CTIUser123*
RecordingPoolDevicePassword=1234
LocalIPAddress=10.10.4.76
[RecordingPool]
NumLines=1
DeviceOrRange1=3012-3015
[CommsManager]
SwitchName=CM
```

Save the file. Restart the recorder. The RBR 2610 should now be configured to the Application Enablement Services.

7 General Test Approach and Test Results

The test approach was to verify that the calls placed and recorded using the Red Box Recorder 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 and calls to/from the PSTN. Tests also included calls to voicemail. The tests were all functional in nature and performance testing was not included. Overall the compliance test was successful.

The serviceability tests were performed by disconnecting the RBR 2610 server from the network and ensuring successful recording of calls and good audio quality on re-connection. These tests were repeated for the Avaya solution by disconnecting and reconnecting both Communication Manager and Application Enablement Services.

It should be noted that on rebooting the Communication Manager, either the Application Enablement Services or the Red Box Recorder RBR 2610 needs to be re-started in order to re-establish the connection with the recorder and continue call recording.

8 Verification Steps

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

8.1 Verify Avaya Aura™ Communication Manager

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the TSAPI link status with Application Enablement Services by using the command **status aesvcs cti-link**. The CTI Link is 10. Verify the **Service State** of the TSAPI 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
1		no		down	0	0
10	4	no	PresAES	established	14	14

Use the command **status aesvcs interface** to verify that the status **Local Node** named **CLAN** of the Application Enablement Services interface is connected and the **Status** is set to **listening**.

status aesvcs interface			
AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
CLAN	yes	1	listening

Verify that there is a link with the Application Enablement Services and that messages are being sent and received by using the command **status aesvcs link**. The resulting record shows details for the **AE Services Server** called **PresAES**.

status aesvcs link						
AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	PresAES	10. 10. 4. 20	35199	CLAN	623	610

8.2 Verify Avaya Aura™ Application Enablement Services

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.

8.2.1 TSAPI Link

On the **Application Enablement Services Management Console** verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top navigation bar includes "Status | Status and Control | TSAPI Service Summary" and "Home | Help | Logout". The left sidebar lists various services, with "Status" expanded to show "Status and Control". The main content area is titled "TSAPI Link Details" and features a table with the following data:

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	CM	10	Talking	Wed Jun 9 00:31:06 2010	Online	15	0	15	15	30

Below the table, there are buttons for "Online" and "Offline". A section for "For service-wide information, choose one of the following:" includes buttons for "TSAPI Service Status", "TLink Status", and "User Status".

8.2.2 TSAPI Test

Make a call between two stations on Communication Manager using the TSAPI Link. On the **Application Enablement Services Management Console** navigate to the screen as follows **Utilities** → **Diagnostics** → **AE Service** → **TSAPI Test**. Use the username and password set up in **Section 5.4**. Enter in the extension numbers of the stations in the **From** and **To** fields and choose **Dial**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top navigation bar includes "Utilities | Diagnostics | AE Services | TSAPI Test" and "Home | Help | Logout". The left sidebar lists various services, with "Utilities" expanded to show "Diagnostics". The main content area is titled "TSAPI Test" and contains the following fields:

- TLink: AVAYA#CM#CSTA#PRESAES (dropdown menu)
- User: CTIUser (text field)
- Password: (password field)
- From: 3000 (text field)
- To: 3004 (text field)
- Dial: (button)

The following screen indicates that the call has been successful.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Jun 9 00:27:54 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-96-0

Utilities | Diagnostics | AE Services | **TSAPI Test**
Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▶ Status

TSAPI Test Result

cstaMakeCall() succeeded!
cstaClearConnection() succeeded!

[Back](#)

8.2.3 DMCC Service

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. It shows a connection to the Red Box Recorder Server, IP address **10.10.4.76**. The **Application** is set to **Redbox** and the **Far-end Identifier** is given as the IP address **10.10.4.76** as expected.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Jun 9 18:21:32 2010 from 10.10.4.70
HostName/IP: PresAES/192.11.13.6
Server Offer Type: TURNKEY
SW Version: r5-2-0-96-0

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

▶ AE Services
▶ Communication Manager Interface
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▼ **Status**
 Alarm Viewer
 ▶ Logs
 ▼ **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

☐ Enable page refresh every seconds

Session Summary [Device Summary](#)
Generated on Wed Jun 09 19:31:47 IST 2010

Service Uptime: 0 days, 0 hours 1 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 1
Number of Existing Devices: 8
Number of Devices Created Since Service Boot: 8

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	B1001F0F3D961C3F0 B4360364558C43F-0	CTIUser	Redbox	10.10.4.76	XML Unencrypted	8

[Terminate Sessions](#) [Show Terminated Sessions](#)

Item 1-1 of 1

8.3 Verify RBR 2610

The following steps can be performed to verify the basic operation of the system components:

- Check status page of the Red Box Recorder to verify that there are no alarms running. If all is functioning as expected the status page should appear as in the screen below. This page loads once logged in to the recorder.

The screenshot shows the 'Recorder Status' page of the Red Box Recorder. The left sidebar contains a menu with options: Search & Replay, Live Acquire, Control, View (highlighted), Channel Activity, Recorder Status, Logged In Users, Statistics, Version Information, Database Details, Media List, Configuration, Diagnostics, Event Logs, User Settings, Downloads, and Logout. The main content area displays the Recorder Status information in a table:

Item	Status
Recorder ID	1819
Recorder Status	Recording
System Type	Standalone
Active Alarms	0
Unarchived Data	<div><div></div></div> 0 %
Recorder Utilization	<div><div></div></div> 0 %
Calls Being Recorded	0

Below the table, there are two buttons: 'Drive 1' and 'Drive 2', both labeled 'No Media'. At the bottom, it states 'The current recorder time is: 13:53:47 on 09 Jun 2010'.

- Choose the **Version Information** tab on the recorder screen to check the version numbers of the recorder to ensure that the **AA RAM** version is as expected.

The screenshot shows the 'Version Information' page of the Red Box Recorder. The left sidebar menu is the same as in the previous screenshot, but 'Version Information' is now highlighted. The main content area displays the 'Recorder System Release' information in a table:

Component	Version
Recorder	7.43.4603
Active Recording PP	1.4.4603
AA RAM	1.20.4603.0
RAInterface	7.16.4603
RIConverter	1.13.4603
Quantify	1.00.549
BUI	7.28.4603
Templates	7.14.4607
Upload Manager	1.0
Update Manager	5.42
SNMP Agent	4.0.4603
Support Manager	2.3

9 Conclusion

These Application Notes describe the configuration steps required for the Red Box Recorder solution to successfully interoperate with an Avaya solution using Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. All functionality and serviceability test cases were completed successfully.

10 Additional References

This section references the Avaya and Red Box Recorder product documentation that are relevant to these Application Notes.

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

1. *Administering Avaya Aura™ Communication Manager*, Document No 03-300509, May 2009
2. *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*; Release 5.2, Document No. 02-300357; November 2009
3. *Avaya Aura™ Application Enablement Services R5.2 Server and Client Release Notes*, November 2009
4. *Developing Client-side IP Recording Applications using Avaya Application Enablement Services*, An Avaya DevConnect Application Note, October 2008

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

Log into the partner portal to access the following documents:

1. *Red Box Recorder User Manual*, Release 9
2. *Quantify Manual*, Version 1.0.451
3. *Avaya Aura™ AES/DMCC Integration*

©2010 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.