



## **Application Notes for Red Box Quantify Recording Suite with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Multiple Registration – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Red Box Quantify Recording Suite to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Multiple Registration. Red Box Quantify Recording Suite is a call recording solution.

In the compliance testing, Red Box Quantify Recording Suite used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor skill group and agent station extensions on Avaya Aura® Communication Manager, and capture the media associated with the monitored agents for call recording using the Multiple Registration method.

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

# 1. Introduction

These Application Notes describe the configuration steps required for Red Box Quantify Recording Suite to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.3. Red Box Quantify Recording Suite is a call recording solution.

In the compliance testing, Red Box Quantify Recording Suite used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to monitor skill group and agent station extensions on Avaya Aura® Communication Manager, and used the Multiple Registration feature via the DMCC interface to capture media associated with the monitored agent stations for call recording.

The DMCC interface is used by Red Box Quantify Recording Suite to monitor the skill group and agent stations to be recorded, and to register a virtual IP softphone against each monitored agent station to pick up the media for call recording. When there is an active call at the monitored agent station, Red Box Quantify Recording Suite is informed of the call via event reports from the DMCC interface, and starts the call recording by using the media from the associated virtual IP softphone. The DMCC event reports are also used to determine when to stop the call recordings.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Quantify Recording Suite, the application automatically uses DMCC to register the virtual IP softphones to Communication Manager, and to request monitoring on the skill group and agent station extensions.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios.

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

The verification of tests included using the Quantify Recording Suite logs for proper message exchanges, and using the Quantify Recording Suite web interface for proper logging and playback of the calls.

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

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Quantify Recording Suite:

- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC monitoring services to monitor skill group, agent stations, and virtual IP softphones.
- Use of DMCC call control services to activate Single Step Conference for the virtual IP softphones and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous calls, simultaneous agents, conference, and transfer.

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

## 2.2. Test Results

All test cases were executed, and the following were observations on Quantify Recording Suite:

- Only one skill group can be monitored by Quantify Recording Suite. Agents that do not belong to the monitored skill group can still be monitored with ACD calls recorded, and the recording entries for those calls will display agent station extension instead of agent login ID for Channel Name.
- Non-ACD calls to the agents are recorded and reported using the agent ID extension in Channel Name. The Called Number from those recording entries can be used to identify the non-ACD calls.
- For the multiple calls at an agent scenario, when the agent goes back and forth between two calls using hold and resume, there is a recording entry for each call, and the recording entries contain audio from the other call during the held period.

## 2.3. Support

Technical support on Quantify Recording Suite can be obtained through the following:

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

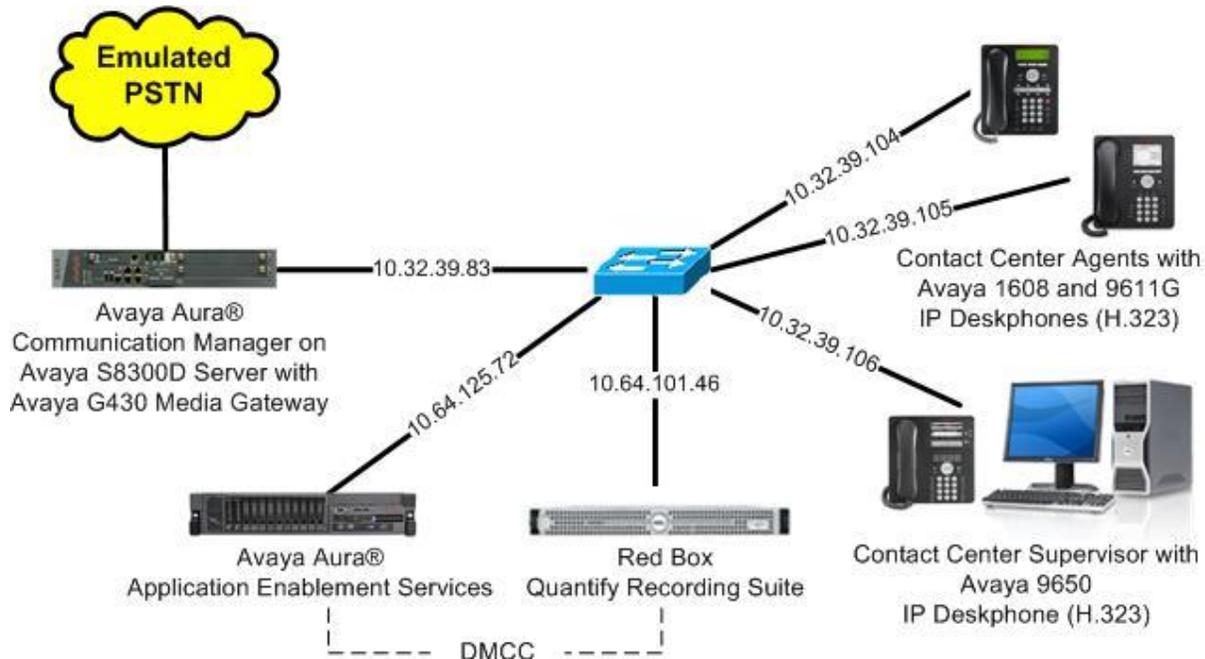
### 3. Reference Configuration

Quantify Recording Suite can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration.

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

In the compliance testing, Quantify Recording Suite monitored the first skill group and two agent station extensions shown in the table below.

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



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8300D Server with Avaya G430 Media Gateway	6.3.2 (R016x.03.0.124.0-21053)
Avaya Aura® Application Enablement Services	6.3.1 (6.3.1.0.19-0)
Avaya 1608 IP Deskphone (H.323)	1.340B
Avaya 9611G IP Deskphone (H.323)	6.3037
Avaya 9650 IP Deskphone (H.323)	3.210A
Red Box Quantify Recording Suite on Windows 2008 Server R2 Enterprise <ul style="list-style-type: none"><li>Avaya DMCC .NET (ServiceProvider.dll)</li></ul>	3A SP2 (Quantify3A_SP2_Build_340) SP 1 6.1.0.37

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Administer agent stations
- Administer class or restriction

### 5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                               Page 3 of 11
                                OPTIONAL FEATURES

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

### 5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                                       Page 1 of 3
                                CTI LINK
CTI Link: 1
Extension: 40001
Type: ADJ-IP
Name: AES CTI Link
                                COR: 1
```

### 5.3. Administer System Parameters Features

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

```
change system-parameters features                               Page 5 of 20
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                        Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                        COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station      Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y      UCID Network Node ID: 1
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Quantify Recording Suite.

```
change system-parameters features                               Page 13 of 20
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
                        Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? y
  Call Classification After Answer Supervision? y
                        Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
```

## 5.4. Administer Agent Stations

Use the “change station n” command, where “n” is the first agent station extension, in this case “45001”.

Enable **IP SoftPhone**, to allow for a virtual IP softphone to be registered against the station. Note the **COR** number, to be used in the next section to configure the agent class of restriction.

```
change station 45991                                     Page 1 of 5
                                                         STATION
Extension: 45001                                         Lock Messages? n          BCC: 0
  Type: 1608                                             Security Code: *         TN: 1
  Port: IP                                               Coverage Path 1:         COR: 1
  Name: G430 Station #1                                  Coverage Path 2:         COS: 1
                                                         Hunt-to Station:         Tests: y
STATION OPTIONS
  Loss Group: 19                                         Time of Day Lock Table:
  Speakerphone: 2-way                                   Personalized Ringing Pattern: 1
  Display Language: english                             Message Lamp Ext: 45001
  Survivable GK Node Name:                              Mute Button Enabled? y
  Survivable COR: internal                             Expansion Module? n
  Survivable Trunk Dest? y                             Media Complex Ext:
                                                         IP SoftPhone? y
                                                         IP Video Softphone? n
                                                         Short/Prefixed Registration Allowed: default
                                                         Customizable Labels? Y
```

Repeat this section to administer all stations to be monitored. In the compliance testing, two agent stations were administered as shown below.

```
list station 45001 count 3
                                                         STATIONS
Ext/      Port/   Name/      Room/      Cv1/  COR/   Cable/
 Hunt-to  Type   Surv GK NN  Move      Data Ext  Cv2  COS TN Jack
45001   S00000 G430 Station #1  no      1    1   1
          9608
45002   S00045 G430 Station #2  no      1    1   1
          9611
```

## 5.5. Administer Class of Restriction

Enter the “change cor n” command, where “n” is the first class of restriction (COR) number assigned to the agents from **Section 5.4**. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to “y”, as shown below. Note that these settings are required in order for Quantify Recording Suite to register the virtual IP softphones against the agent stations without use of passwords.

Repeat this section to administer all class of restriction numbers used by the agents. In the compliance testing, the same class of restriction number was assigned to all agent stations.

```
change cor 1                                     Page 1 of 23
                                         CLASS OF RESTRICTION
COR Number: 1
COR Description:
FRL: 0                                         APLT? y
Can Be Service Observed? y                 Calling Party Restriction: none
Can Be A Service Observer? y              Called Party Restriction: none
Time of Day Chart: 1                          Forced Entry of Account Codes? n
Priority Queuing? n                            Direct Agent Calling? n
Restriction Override: none                    Facility Access Trunk Test? n
Restricted Call List? n                       Can Change Coverage? n
```

## 6. Configure Avaya Aura® Application Enablement Services

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

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

### 6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. The title "Application Enablement Services Management Console" is centered at the top. A red horizontal bar spans the width of the page, with a "Help" link on the right side. The main content area features a login form with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are "Login" and "Reset" buttons. At the bottom of the page, a red horizontal bar is present, and the copyright notice "Copyright © 2009-2013 Avaya Inc. All Rights Reserved." is centered below it.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes\_125\_72/10.64.125.72', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP', 'SW Version: 6.3.1.0.19-0', 'Server Date and Time: Wed Nov 6 07:11:40 MST 2013', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. The left sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Welcome to OAM' and contains 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:'. A bulleted list follows: '• 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 infomations.', '• User Management - Use User Management to manage AE Services users and AE Services user-related resources.', '• Utilities - Use Utilities to carry out basic connectivity tests.', '• Help - Use Help to obtain a few tips for using the OAM Help system'. A concluding sentence states: 'Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.'

## 6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' section selected. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes\_125\_72/10.64.125.72', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP', 'SW Version: 6.3.1.0.19-0', 'Server Date and Time: Wed Nov 6 07:11:40 MST 2013', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. The left sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing (expanded), Maintenance, and Networking. Under 'Licensing', the sub-items are: WebLM Server Address, WebLM Server Access (highlighted), Reserved Licenses, and Networking. The main content area is titled 'Licensing' and contains the following text: 'If you are setting up and maintaining the WebLM, you need to use the following:'. A bulleted list follows: '• WebLM Server Address'. Below that, it says: 'If you are importing, setting up and maintaining the license, you need to use the following:'. A bulleted list follows: '• WebLM Server Access'. Finally, it says: 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:'. A bulleted list follows: '• Reserved Licenses'.

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

**AVAYA** Web License Manager (WebLM v6.3) Help | About | Change Password

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

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

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

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

**Licensed Features**

10 Items [Refresh](#) Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_2 LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestrict DMCUnrestricted; 1XM_001, BasicUnrestrict DMCUnrestricted; PC_001, BasicUnrestrict DMCUnrestricted; CIE_001, BasicUnrestrict DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestrict DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE (A AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestrict DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

### 6.3. Administer TSAPI Link

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

Welcome: User  
Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Wed Nov 6 07:11:40 MST 2013  
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

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

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	6	Both

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

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

Welcome: User  
Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Wed Nov 6 07:11:40 MST 2013  
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

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

Add TSAPI Links

Link: 2  
Switch Connection: S8300D  
Switch CTI Link Number: 1  
ASAI Link Version: 6  
Security: Unencrypted

## 6.4. Administer H.323 Gatekeeper

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

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays user information: "Welcome: User", "Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes\_125\_72/10.64.125.72", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP", "SW Version: 6.3.1.0.19-0", "Server Date and Time: Wed Nov 6 07:11:40 MST 2013", and "HA Status: Not Configured". The main navigation pane on the left includes "AE Services", "Communication Manager Interface", "Switch Connections", "Dial Plan", "High Availability", "Licensing", "Maintenance", "Networking", and "Security". The "Switch Connections" section is active, showing a table with the following data:

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

Buttons for "Add Connection", "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", "Delete Connection", and "Survivability Hierarchy" are visible at the bottom of the table.

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, in this case “10.32.39.83” as shown below. Click **Add Name or IP**.

The screenshot shows the "Edit H.323 Gatekeeper - S8300D" screen. The top right corner displays the same user information as the previous screenshot. The main navigation pane on the left is the same. The "Edit H.323 Gatekeeper - S8300D" section is active, showing a form with the following fields and buttons:

Name or IP Address

## 6.5. Enable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Check both fields below to enable use of SDB. Note that these settings are required in order for Quantify Recording Suite to register the virtual IP softphones against the agent station extensions without use of passwords.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title "Application Enablement Services Management Console". The top right shows system information: "Welcome: User", "Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes\_125\_72/10.64.125.72", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP", "SW Version: 6.3.1.0.19-0", "Server Date and Time: Wed Nov 6 07:11:40 MST 2013", and "HA Status: Not Configured".

The main interface has a red navigation bar with "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. A left-hand navigation pane lists various services, with "Security" expanded to show "Control" selected. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two checked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

## 6.6. Restart Services

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a user welcome message with system details. A navigation bar below the header shows "Maintenance | Service Controller" and "Home | Help | Logout".

The left sidebar contains a tree view of navigation options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (expanded), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, Status, and User Management.

The main content area is titled "Service Controller" and contains a table with the following data:

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

Below the table, there is a note: "For status on actual services, please use [Status and Control](#)". At the bottom of the main content area, there is a row of buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

## 6.7. Administer Quantify User

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

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User, Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20, Number of prior failed login attempts: 0, HostName/IP: aes\_125\_72/10.64.125.72, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP, SW Version: 6.3.1.0.19-0, Server Date and Time: Wed Nov 6 07:12:32 MST 2013, HA Status: Not Configured.

The navigation bar includes **User Management | User Admin | Add User** and **Home | Help | Logout**.

The left sidebar shows a tree view with **User Management** expanded to **User Admin**, where **Add User** is selected.

The main content area is titled **Add User** and contains the following form fields:

- Fields marked with \* can not be empty.
- \* User Id: quantify
- \* Common Name: quantify
- \* Surname: quantify
- \* User Password: [masked]
- \* Confirm Password: [masked]
- Admin Note: [empty]
- Avaya Role: None
- Business Category: [empty]
- Car License: [empty]
- CM Home: [empty]
- Css Home: [empty]
- CT User: Yes
- Department Number: [empty]
- Display Name: [empty]
- Employee Number: [empty]
- Employee Type: [empty]
- Enterprise Handle: [empty]

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the left pane, to display the **CTI Users** screen in the right pane. Select the new Quantify user, and click **Edit**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User, Last login: Fri Nov 8 13:29:05 2013 from 10.32.39.20, Number of prior failed login attempts: 0, HostName/IP: aes\_125\_72/10.64.125.72, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP, SW Version: 6.3.1.0.19-0, Server Date and Time: Mon Nov 11 09:40:24 MST 2013, HA Status: Not Configured.

The breadcrumb navigation is: Security | Security Database | CTI Users | List All Users. The left sidebar shows a tree view with 'Security' expanded to show 'Account Management', 'Audit', 'Certificate Management', and 'Enterprise Directory'. The main content area is titled 'CTI Users' and contains a table with the following data:

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> aesp5	aesp5	NONE	NONE
<input type="radio"/> aesp5h	aesp5h	NONE	NONE
<input type="radio"/> craft	craft	NONE	NONE
<input checked="" type="radio"/> quantify	quantify	NONE	NONE

Below the table are 'Edit' and 'List All' buttons.

The **Edit CTI User** screen is displayed next. Check **Unrestricted Access**, which is required in order for Quantify Recording Suite to register the virtual IP softphones against the agent station extensions without use of passwords.

The screenshot shows the 'Edit CTI User' screen for the 'quantify' user. The top right corner displays system information: Welcome: User, Last login: Fri Nov 8 13:29:05 2013 from 10.32.39.20, Number of prior failed login attempts: 0, HostName/IP: aes\_125\_72/10.64.125.72, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP, SW Version: 6.3.1.0.19-0, Server Date and Time: Mon Nov 11 09:40:38 MST 2013, HA Status: Not Configured.

The breadcrumb navigation is: Security | Security Database | CTI Users | List All Users. The left sidebar shows a tree view with 'Security Database' expanded. The main content area is titled 'Edit CTI User' and contains the following configuration fields:

User Profile: User ID: quantify, Common Name: quantify, Worktop Name: NONE (dropdown), Unrestricted Access:

Call and Device Control: Call Origination/Termination and Device Status: None (dropdown)

Call and Device Monitoring: Device Monitoring: None (dropdown), Calls On A Device Monitoring: None (dropdown), Call Monitoring:

Routing Control: Allow Routing on Listed Devices: None (dropdown)

At the bottom are 'Apply Changes' and 'Cancel Changes' buttons.

## 6.8. Administer Ports

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

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

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 user status area with the following text: "Welcome: User", "Last login: Wed Nov 6 07:07:54 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes\_125\_72/10.64.125.72", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP", "SW Version: 6.3.1.0.19-0", "Server Date and Time: Wed Nov 6 07:11:40 MST 2013", and "HA Status: Not Configured".

The main interface is divided into a left navigation pane and a right content area. The navigation pane includes sections for "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking" (selected), "Security", "Status", "User Management", "Utilities", and "Help". Under "Networking", the "Ports" option is highlighted.

The "Ports" configuration page is titled "Ports" and is divided into three sections:

- CVLAN Ports:** Contains two rows. The first row is "Unencrypted TCP Port" with a value of "9999" and radio buttons for "Enabled" (selected) and "Disabled". The second row is "Encrypted TCP Port" with a value of "9998" and radio buttons for "Enabled" (selected) and "Disabled".
- DLG Port:** Contains one row: "TCP Port" with a value of "5678".
- TSAPI Ports:** Contains several rows. The first row is "TSAPI Service Port" with a value of "450" and radio buttons for "Enabled" (selected) and "Disabled". The following rows are "Local TLINK Ports" with sub-rows for "TCP Port Min" (1024) and "TCP Port Max" (1039). The next section is "Unencrypted TLINK Ports" with sub-rows for "TCP Port Min" (1050) and "TCP Port Max" (1065). The final section is "Encrypted TLINK Ports" with sub-rows for "TCP Port Min" (1066) and "TCP Port Max" (1081).
- DMCC Server Ports:** Contains three rows. The first row is "Unencrypted Port" with a value of "4721" and radio buttons for "Enabled" (selected) and "Disabled". The second row is "Encrypted Port" with a value of "4722" and radio buttons for "Enabled" (selected) and "Disabled". The third row is "TR/87 Port" with a value of "4723" and radio buttons for "Disabled" and "Enabled" (selected).

## 7. Configure Red Box Quantify Recording Suite

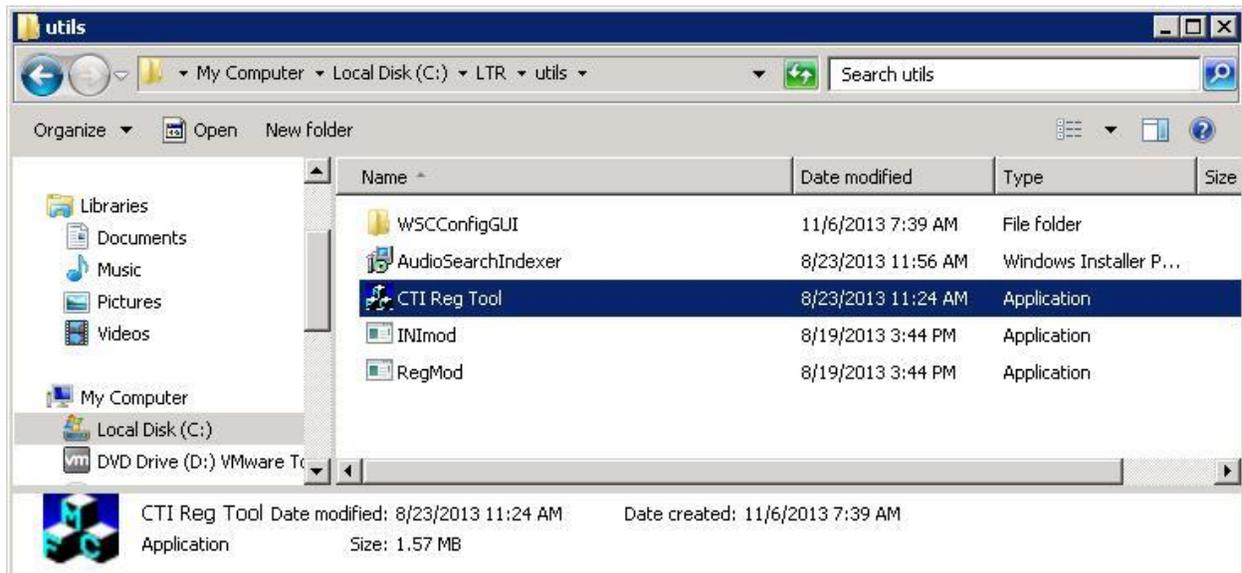
This section provides the procedures for configuring Quantify Recording Suite. The procedures include the following areas:

- Administer CTI registration tool
- Administer CTI server
- Administer recording channels

The configuration of Quantify Recording Suite is performed by Red Box installation engineers. The procedural steps are presented in these Application Notes for informational purposes.

### 7.1. Administer CTI Registration Tool

From the Quantify Recording Suite server, navigate to the **C:\LTR\utils** directory, and double click to launch the **CTI Reg Tool** shown below.



The **CTI Registration Tool** screen is displayed. For **Recorder IP Address**, enter “127.0.0.1”. Enter the appropriate credentials, and click **Connect**.



The screenshot shows the 'CTI Registration Tool' window. It has a title bar with a close button. Below the title bar, there are three input fields: 'Recorder IP Address' containing '127 . 0 . 0 . 1', 'Recorder Username' (empty), and 'Recorder Password' (empty). At the bottom of the window is a 'Connect' button.

Upon successful connection, the **CTI Registration Tool** screen is updated as shown below.

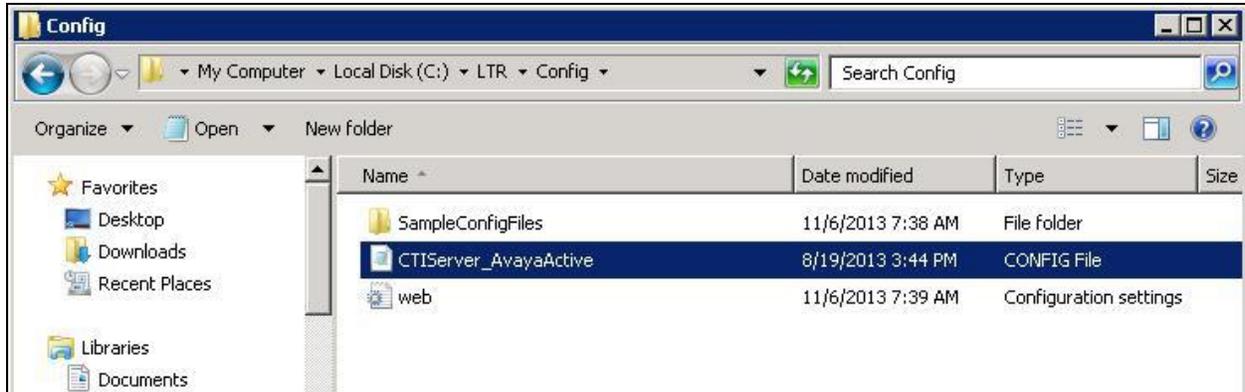
For **Extension or range to register**, enter the range of the agent station extensions from **Section 3**. Select the **Avaya Multiple Registration** radio button, and click **Register**. In the case that the agent station extensions are not consecutive in nature, this step can be repeated to enter one station extension at a time.



The screenshot shows the 'CTI Registration Tool' window after a successful connection. The 'Recorder IP Address' field still contains '127 . 0 . 0 . 1'. The 'Recorder Username' field now contains 'admin' and the 'Recorder Password' field contains '\*\*\*\*\*'. A 'Disconnect' button is now visible. Below this, there is a section for 'Extension or range to register (e.g. 1234 or 1234-1250)' with a text box containing '45001-45002'. There are three radio buttons: 'Avaya Multiple Registration' (selected), 'Avaya Single Step Conferencing', and 'Aastra Active'. A 'Register' button is located below the radio buttons. At the bottom of the window, there is a 'Status' field displaying 'Connected'.

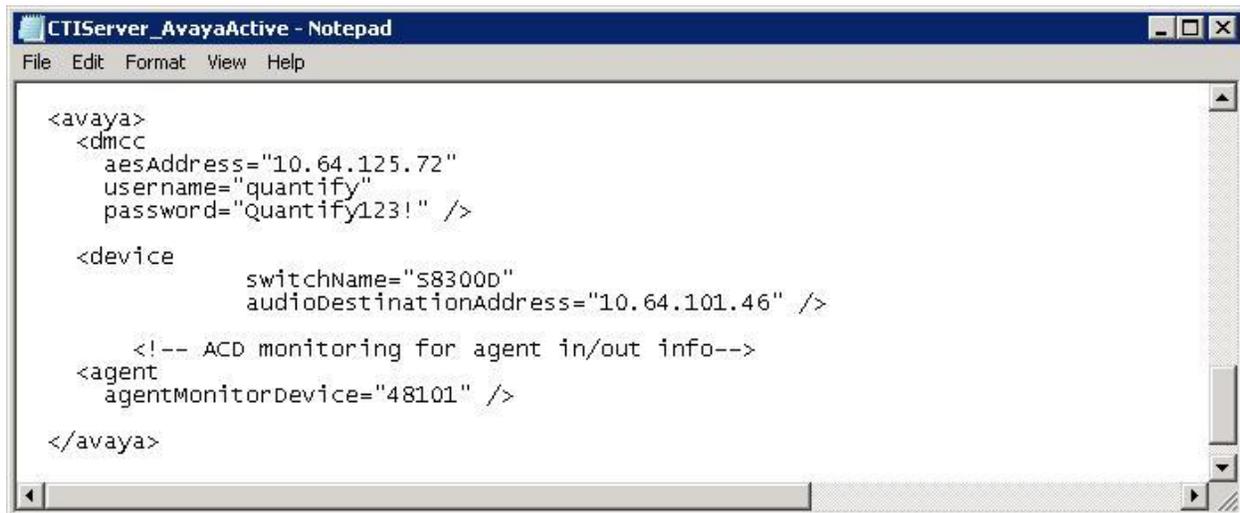
## 7.2. Administer CTI Server

Navigate to the **C:\LTR\Config** directory, and copy the **CTIServer\_AvayaActive** configuration file from the **SampleConfigFiles** directory to the current directory shown below.



Open the **CTIServer\_AvayaActive** file with the Notepad application. Navigate to the **avaya** sub-section, and configure the parameters as shown below.

- **aesAddress:** IP Address of Application Enablement Services.
- **username:** The Quantify user credentials from **Section 6.7**.
- **password:** The Quantify user credentials from **Section 6.7**.
- **SwitchName:** The relevant switch connection name from **Section 6.3**.
- **audioDestinationAddress:** IP address of the Quantify Recording Suite server.
- **agentMonitorDevice:** The first skill group extension from **Section 3**.

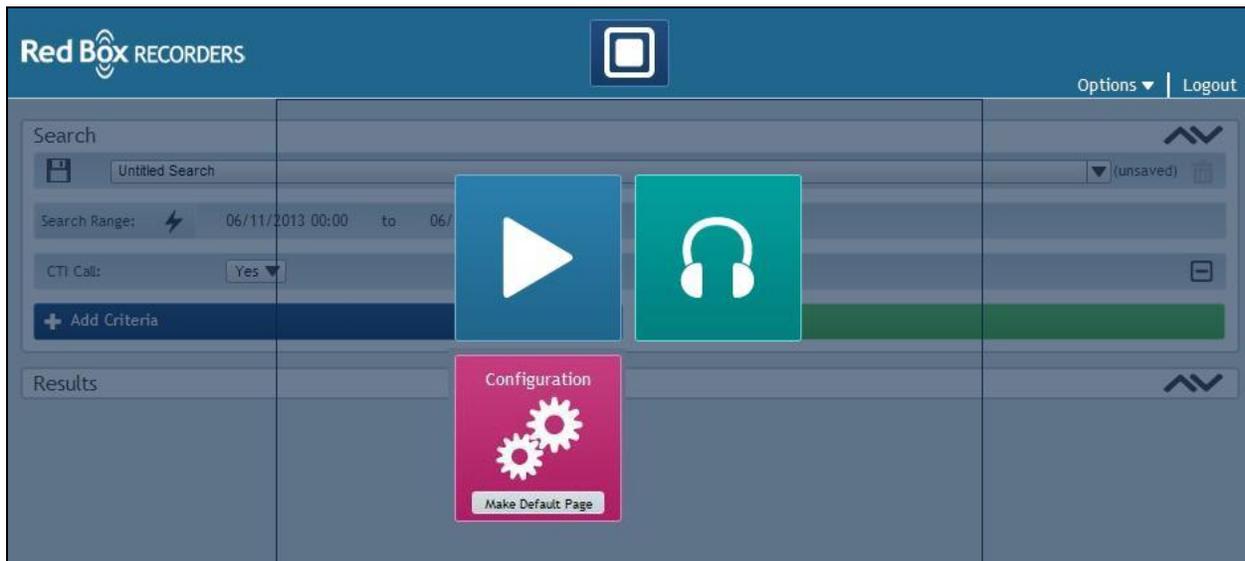


### 7.3. Administer Recording Channels

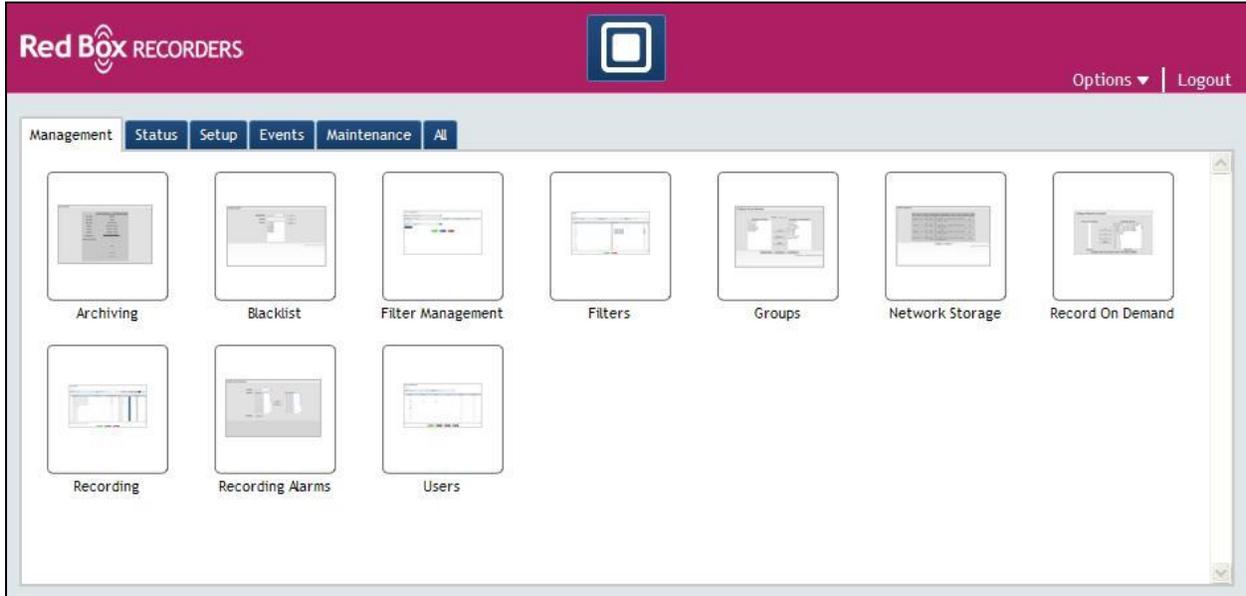
Access the Quantify Recording Suite web-based interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Quantify Recording Suite server. Log in using the appropriate credentials.



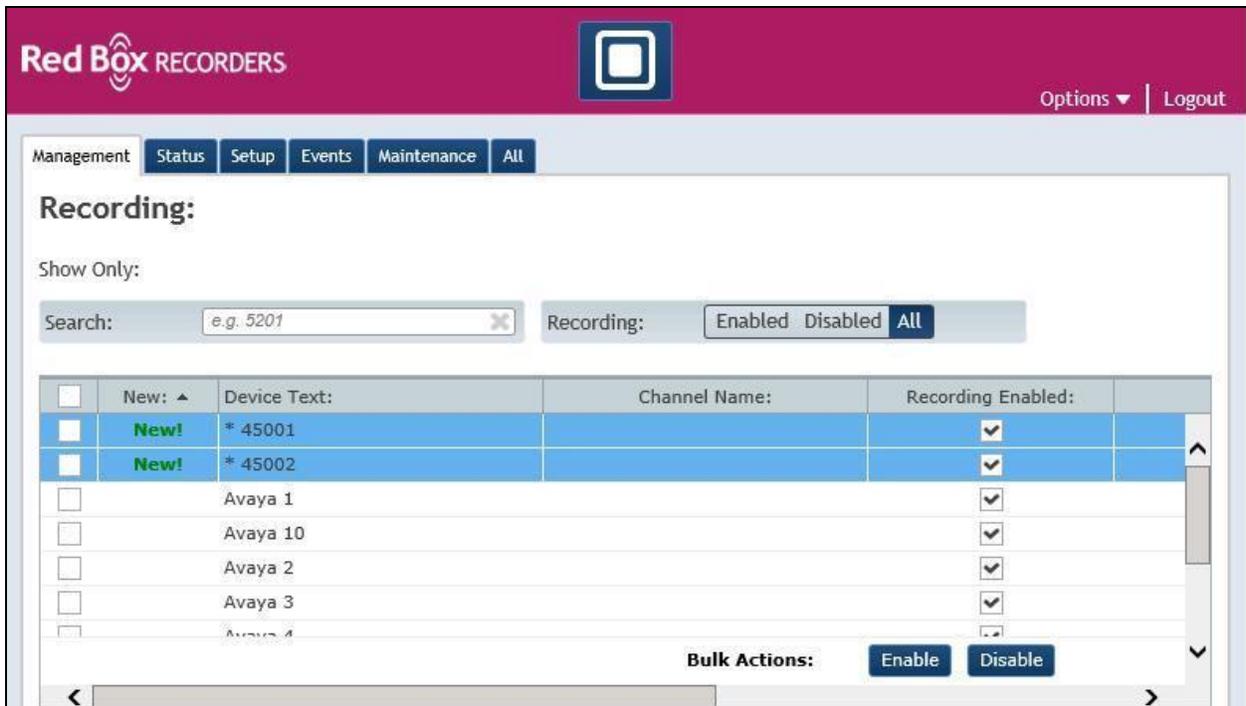
The screen below is displayed. Click on the **Configuration** icon.



The screen below is displayed next. Select **Management** → **Recording**.



The **Recording** screen is displayed. Under the **Recording Enabled** column, check the entries associated with the station agent extensions from **Section 3**. In the compliance testing, two entries with **Device Text** of “45001” and “45002” were checked.



## 8. Verification Steps

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

### 8.1. Verify Avaya Aura® Communication Manager

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

```
status aevcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
<b>1</b>	<b>6</b>	<b>no</b>	<b>aes_125_72</b>	<b>established</b>	<b>35</b>	<b>20</b>

Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all agent station extensions from **Section 5.4** are displayed along with the IP address of the Application Enablement Services server, as shown below.

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

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address		
45000	9650 1	IP_Phone 3.210A	y	10.32.39.104 10.32.39.83		
45001	1608 1	IP_Phone 1.340B	y	10.32.39.105 10.32.39.83		
<b>45001</b>	<b>1608</b> <b>1</b>	<b>IP_API_A</b> <b>3.2040</b>	<b>y</b>	<b>10.64.125.72</b> <b>10.32.39.83</b>		
45002	9611 1	IP_Phone 6.3037	y	10.32.39.106 10.32.39.83		
<b>45002</b>	<b>9611</b> <b>1</b>	<b>IP_API_A</b> <b>3.2040</b>	<b>y</b>	<b>10.64.125.72</b> <b>10.32.39.83</b>		

## 8.2. Verify Avaya Aura® Application Enablement Services

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

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



### Application Enablement Services Management Console

Welcome: User  
 Last login: Fri Nov 8 06:47:08 2013 from 10.32.39.20  
 Number of prior failed login attempts: 0  
 HostName/IP: aes\_125\_72/10.64.125.72  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
 SW Version: 6.3.1.0.19-0  
 Server Date and Time: Fri Nov 8 07:29:15 MST 2013  
 HA Status: Not Configured

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

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

#### TSAPI Link Details

Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
○	1	S8800	2	Talking	Fri Nov 8 06:50:48 2013	Online	16	0	15	15	30
●	2	S8300D	1	Talking	Fri Nov 8 07:06:00 2013	Online	16	3	21	37	30

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

Verify the status of the DMCC link by selecting **Status** → **Status and Control** → **DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Quantify user name from **Section 6.7**, and that the **# of Associated Devices** column reflects the total number of monitored skill group and agent station extensions from **Section 3**.

Welcome: User  
 Last login: Fri Nov 8 06:47:08 2013 from 10.32.39.20  
 Number of prior failed login attempts: 0  
 HostName/IP: aes\_125\_72/10.64.125.72  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
 SW Version: 6.3.1.0.19-0  
 Server Date and Time: Fri Nov 08 07:29:25 MST 2013  
 HA Status: Not Configured

**AVAYA Application Enablement Services Management Console**

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

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

**DMCC Service Summary - Session Summary**

Enable page refresh every 60 seconds

Session Summary [Device Summary](#)  
 Generated on Fri Nov 08 07:29:25 MST 2013

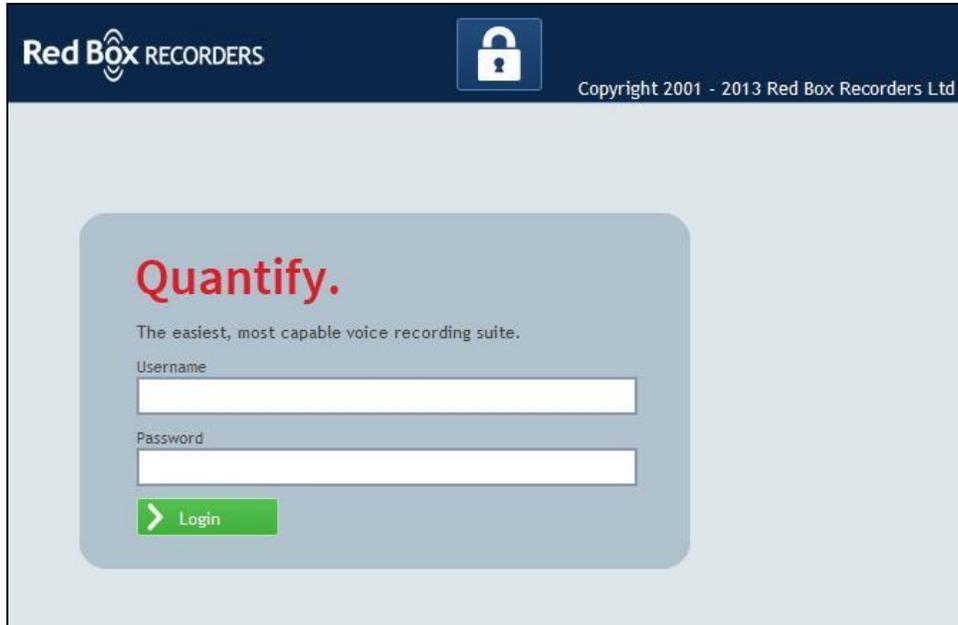
Service Uptime: 0 days, 0 hours 37 minutes  
 Number of Active Sessions: 1  
 Number of Sessions Created Since Service Boot: 2  
 Number of Existing Devices: 3  
 Number of Devices Created Since Service Boot: 4

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	E08E343CC2CC6E909 5C2C6859CEC4942-1	quantify	Red Box Recorder	10.64.101.46	XML Unencrypted	3

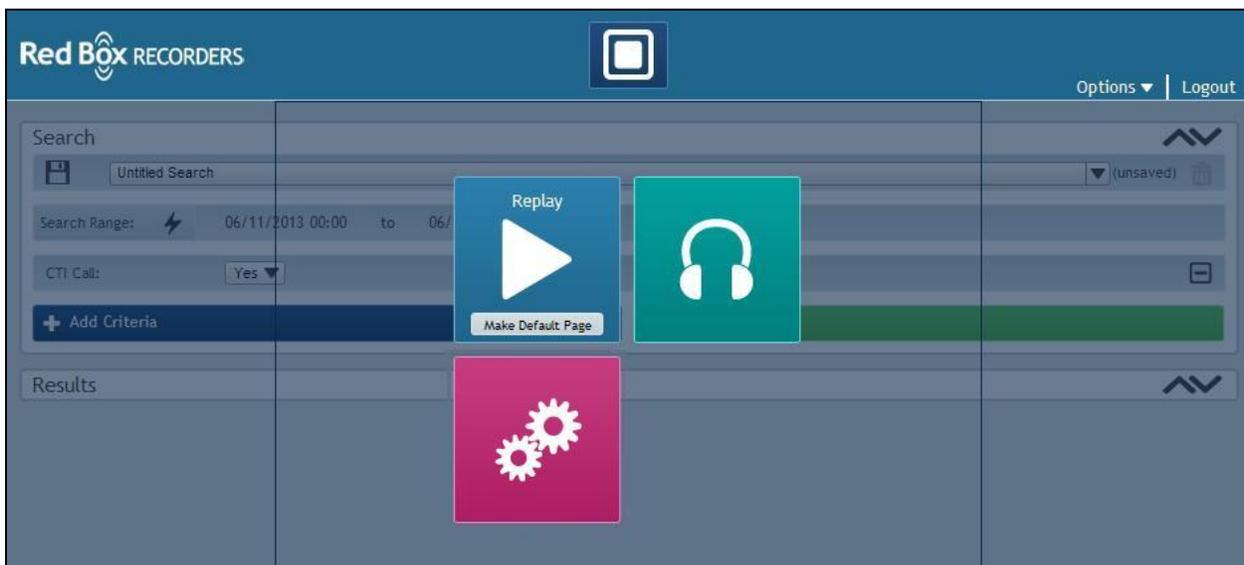
Item 1-1 of 1  
 Go

### 8.3. Verify Red Box Quantify Recording Suite

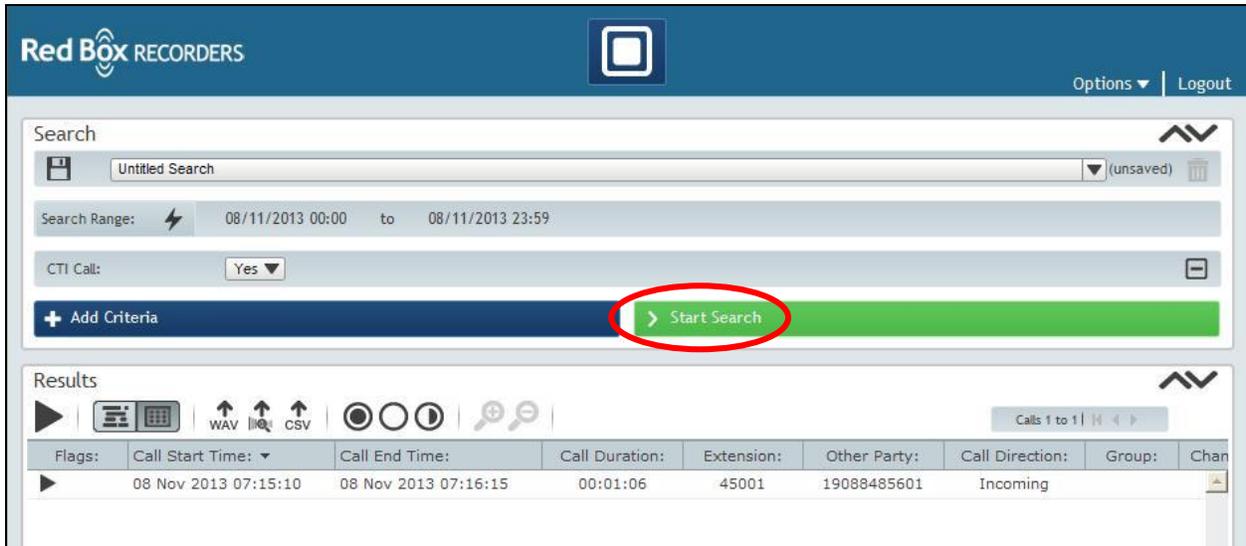
Log an agent in to the skill group to handle and complete an ACD call. Follow the procedures in **Section 7.3** to log in to the Quantify Recording Suite web-based interface.



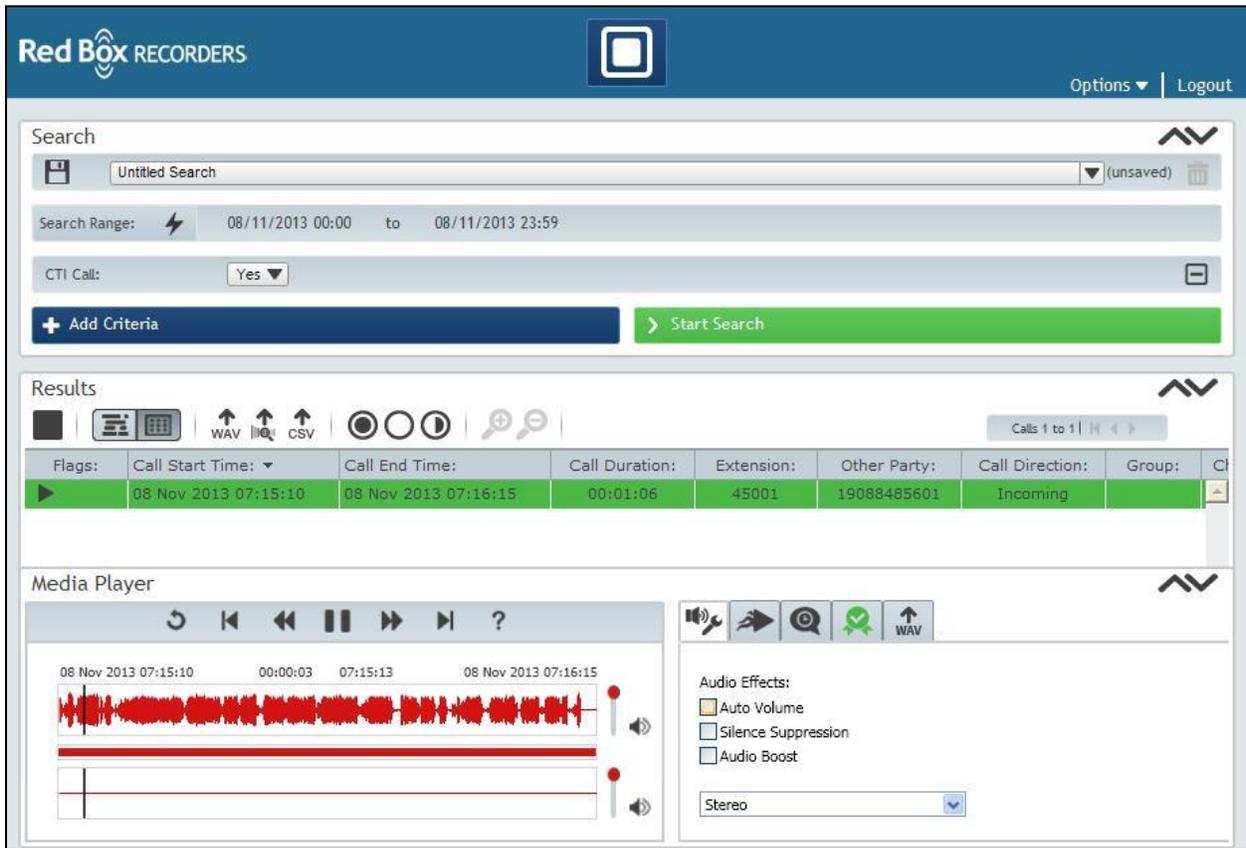
The screen below is displayed. Click on the **Replay** icon.



The **Search** screen is displayed. Click **Start Search** to obtain a listing of all recording entries for the current day. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.



Double click on the entry to listen to the playback. Verify that call recording is played back.



## 9. Conclusion

These Application Notes describe the configuration steps required for Red Box Quantify Recording Suite to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Multiple Registration. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9, Release 6.3, October 2013, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 2, October 2013, available at <http://support.avaya.com>.
3. *White-paper on Security in Avaya Aura® Application Enablement Services*, Document Rev 4.0.0, February 2013, available at <http://support.avaya.com>.
4. *Quantify Administration Manual, Release 3A SP1, September 2013*, available on the Quantify software CD.
5. *Quantify User Manual, Release 3A SP1, May 2013*, available on the Quantify software CD.

---

**©2014 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).