



Avaya Solution & Interoperability Test Lab

Application Notes for Red Box Quantify 6C with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 10.1 using DMCC Multiple Registration – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Red Box Quantify 6C with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. Red Box Quantify 6C is a voice recording solution which can be used to record voice streams for Avaya telephony using Multiple Registration method.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Red Box Quantify 6C to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 using the Multiple Device Registration recording method.

Red Box Quantify 6C 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 Multiple Device Registration feature via Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to capture the audio and call details for call recording. The application uses the Avaya Aura® Application Enablement Services DMCC service to register the extensions that are to be recorded. When the extension receives an event pertaining to the start of a call, the application receives the extensions RTP media stream.

2. General Test Approach and Test Results

The feature test cases were performed manually. Platform to carry out call recording in a variety of scenarios using DMCC Multiple Registration.

For the manual part of the testing, each call was handled manually on the extension 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 Red Box Quantify 6C.

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

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

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

For the testing associated with this Application Notes, the interface between Avaya systems and Red Box Quantify 6C utilized enabled capabilities of secure DMCC interface.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Inbound/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park, Call Pickup, Bridged Appearance and Service Observing.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into Avaya Agent for Desktop.
- **Serviceability testing** - The behavior of Red Box Quantify 6C under different simulated failure conditions.

2.2. Test Results

All test cases were executed and verified successfully.

2.3. Support

Technical support on Red Box Quantify 6C can be obtained through the following:

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

3. Reference Configuration

Red Box Quantify 6C can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration.

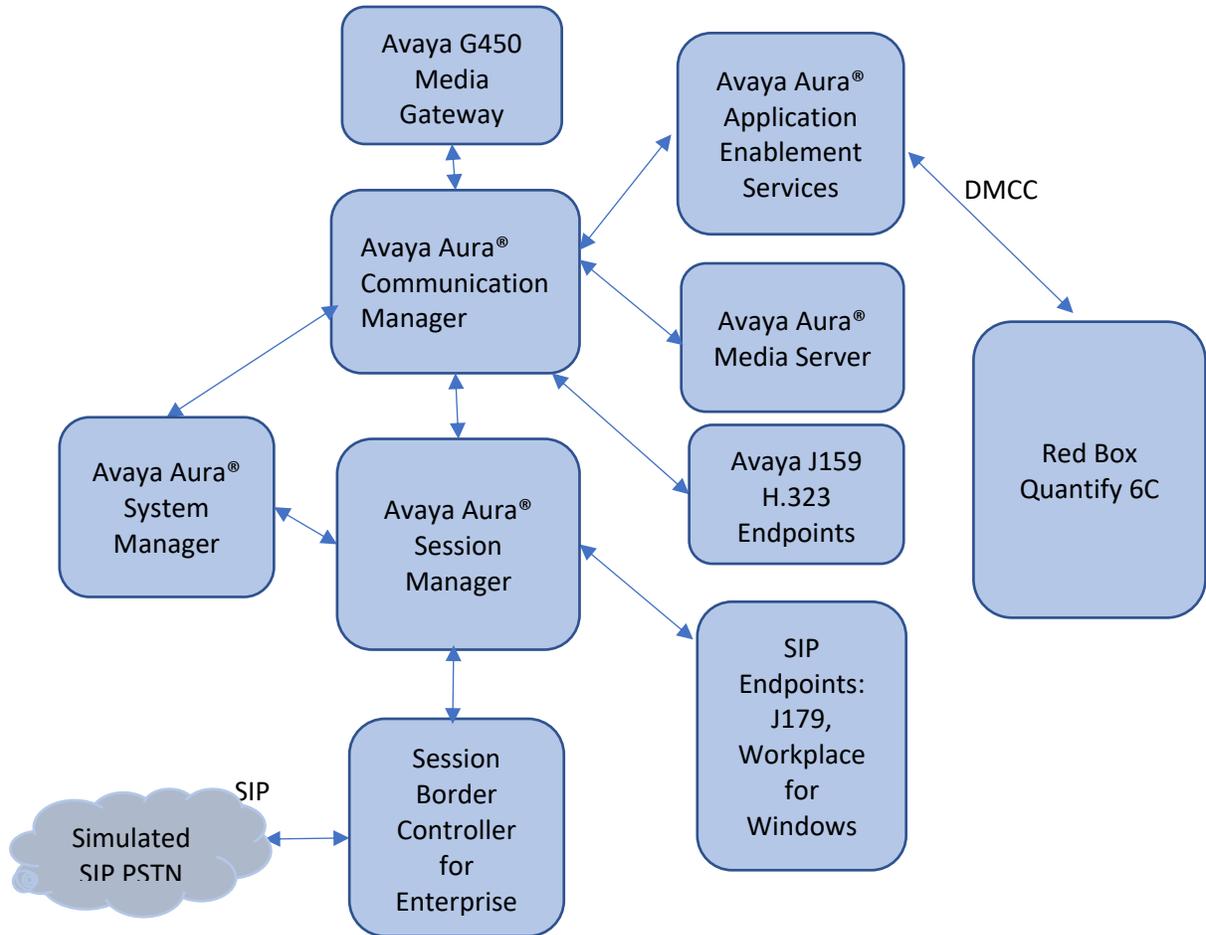


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	10.1.0.0.537353
Avaya Aura® Session Manager in Virtual Environment	10.1.0.1.1010105
Avaya Aura® Communication Manager in Virtual Environment	10.1.0.1 SP1 Build 01.0.974.0-27372
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server in Virtual Environment	10.1.0.77
Avaya Aura® Application Enablement Services in Virtual Environment	10.1.0.1.0.7
Avaya Session Border Controller for Enterprise in Virtual Environment	10.1
Avaya Workplace Client for Windows	3.25.0.73
Avaya J179 IP Phone (SIP)	4.0.12.1
Avaya J159 IP Deskphone (H.323)	6.8.5
Red Box Quantify on Windows Server 2016	6C

5. Configure Avaya Aura® Communication Manager

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

- Administer CTI link
- Configure H.323 Stations for Multi-Registration
- Configure SIP Stations for Multiple Registration

5.1. 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: 79999
Type: ADJ-IP                                     COR: 1
Name: aes155
```

5.2. Configure H.323 Stations for Multi-Registration

All endpoints that are to be monitored by Red Box will need to have IP Softphone set to **y**. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where **x** is the extension number of the station to be monitored. Also, note this extension number for configuration required during the Red Box setup in **Section 7**. Note the Security Code and ensure that **IP Softphone** is set to **y**.

```

change station 70010                                     Page 1 of 5
                                                    STATION
Extension: 70010                                     Lock Messages? n          BCC: 0
Type: 9641                                           Security Code: 111222    TN: 1
Port: S000004                                         Coverage Path 1:         COR: 1
Name: H323 Ext1                                       Coverage Path 2:         COS: 1
                                                    Hunt-to Station:         Tests: y

STATION OPTIONS
                                                    Time of Day Lock Table:
Loss Group: 19                                       Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 70010
Speakerphone: 2-way                                  Mute Button Enabled? y
Display Language: english                            Button Modules: 0
Survivable GK Node Name:                             Media Complex Ext:
Survivable COR: internal                             IP SoftPhone? y
Survivable Trunk Dest? y

                                                    IP Video Softphone? n
Short/Prefixed Registration Allowed: default

                                                    Customizable Labels? Y

```

In the compliance testing, two H323 extensions were administered : **70010** and **70011**

5.3. Configure SIP Stations for Multiple Registration

Each Avaya SIP endpoint or station that needs to be monitored for call recording will need to have **Type of 3PCC Enabled** is set to **Avaya** and **IP Softphone** set to **Yes**. Changes to SIP phones on Communication Manager by enter command **change station x** where **x** is the extension number of the station.

```
change station 70000                                     Page 1 of 6
                                                         STATION
Extension: 70000                                     Lock Messages? n          BCC: 0
Type: J179                                           Security Code: 111222   TN: 1
Port: S000010                                         Coverage Path 1:         COR: 1
Name: SIP Ext1                                       Coverage Path 2:         COS: 1
                                                         Hunt-to Station:        Tests: y

STATION OPTIONS
                                                         Time of Day Lock Table:
Loss Group: 19                                         Personalized Ringing Pattern: 1
                                                         Message Lamp Ext: 70000
Speakerphone: 2-way                                    Mute Button Enabled? y
Display Language: english                             Button Modules: 0
Survivable GK Node Name:
Survivable COR: internal                               Media Complex Ext:
Survivable Trunk Dest? y                               IP SoftPhone? y
                                                         IP Video Softphone? n
Short/Prefixed Registration Allowed: default
                                                         Customizable Labels? Y
```

Go to **Page 6**.

```
change station 70000                                     Page 6 of 6
                                                         STATION
SIP FEATURE OPTIONS
    Type of 3PCC Enabled: Avaya      SIP Trunk: aar
    Enable Reachability for Station Domain Control: s
SIP URI: 70000@aura.com
Primary Session Manager
    IPv4 Address: 10.128.224.18      IPv6 Address:
    IPv4 Node Name: smsip18         IPv6 Node Name:

Secondary Session Manager
    IPv4 Address:                    IPv6 Address:
    IPv4 Node Name:                  IPv6 Node Name:

Third Session Manager
    IPv4 Address:                    IPv6 Address:
    IPv4 Node Name:                  IPv6 Node Name:

Fourth Session Manager
    IPv4 Address:                    IPv6 Address:
    IPv4 Node Name:                  IPv6 Node Name:
```

In the compliance testing, two H323 extensions were administered : **70000** and **70001**

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 redbox user
- Enable CTI User
- Administer security database
- Restart services

6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login screen. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". A red horizontal bar spans the width of the page, with a "Help" link on the right side. In the center, there is a light gray box containing the text "Please login here:" followed by "Username" and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, with the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." centered below it.

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

The screenshot shows the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right is the title 'Application Enablement Services Management Console'. In the top right corner, there is a welcome message and system information: 'Welcome: User cust', 'Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167', 'Number of prior failed login attempts: 0', 'HostName/IP: aes155.aura.com/10.128.226.155', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 10.1.0.1.0.7-0', 'Server Date and Time: Fri Oct 21 17:11:20 ICT 2022', and 'HA Status: Not Configured'. Below this is a red navigation bar with 'Home' on the left and 'Home | Help | Logout' on the right. On the left side, there is a vertical menu with the following items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area 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:'. This is followed by a bulleted list of domains and their uses: 'AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.', 'Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.', 'High Availability - Use High Availability to manage AE Services HA.', 'Licensing - Use Licensing to manage the license server.', 'Maintenance - Use Maintenance to manage the routine maintenance tasks.', 'Networking - Use Networking to manage the network interfaces and ports.', 'Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.', 'Status - Use Status to obtain server status informations.', 'User Management - Use User Management to manage AE Services users and AE Services user-related resources.', 'Utilities - Use Utilities to carry out basic connectivity tests.', and 'Help - Use Help to obtain a few tips for using the OAM Help system'. Below the list, it states: 'Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.' At the bottom of the page, there is a copyright notice: 'Copyright © 2009-2022 Avaya Inc. All Rights Reserved.'

6.2. Verify License

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

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, system information is provided: "Welcome: User cust", "Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes155.aura.com/10.128.226.155", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Fri Oct 21 17:12:08 ICT 2022", and "HA Status: Not Configured".

A red navigation bar contains the word "Licensing" on the left and "Home | Help | Logout" on the right. A left-hand sidebar menu lists various sections: "AE Services", "Communication Manager Interface", "High Availability", "Licensing" (which is expanded to show "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses"), "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help".

The main content area is titled "Licensing" and contains the following text and lists:

- If you are setting up and maintaining the WebLM, you need to use the following:
 - WebLM Server Address
- If you are importing, setting up and maintaining the license, you need to use the following:
 - WebLM Server Access
- If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:
 - Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

At the bottom of the page, a copyright notice reads: "Copyright © 2009-2022 Avaya Inc. All Rights Reserved."

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **Device Media and Call Control**, as shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left navigation pane is expanded to 'Application_Enablement'. The main content area displays the 'Application Enablement (CTI) - Release: 10 - SID: 10503000' page. The page includes a breadcrumb trail: 'You are here: Licensed Products > Application_Enablement > View License Capacity'. Below this, it shows the license installation date: 'License installed on: August 15, 2022 1:54:38 PM +07:00' and the 'License File Host IDs: VC-D4-B4-AD-C9-9F-01'. A section titled 'Licensed Features' contains a table with 14 items. The table has three columns: 'Feature (License Keyword)', 'Expiration date', and 'Licensed capacity'. All features listed have a 'permanent' expiration date and a '5000' licensed capacity.

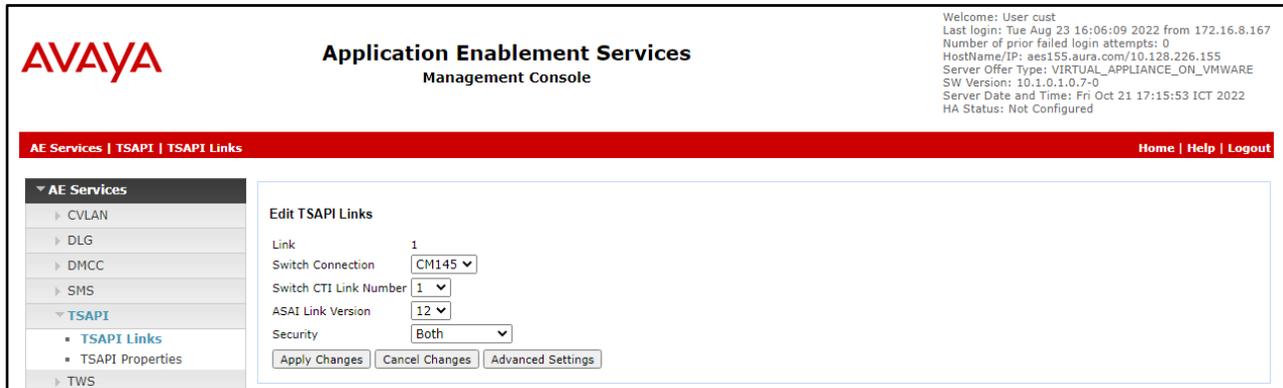
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	5000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	5000
AES HA LARGE VALUE_AES_HA_LARGE	permanent	5000
AES ADVANCED AGENT VALUE_AES_ADVANCED_AGENT	permanent	5000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	5000
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	5000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	5000
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	5000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	5000
DLG VALUE_AES_DLG	permanent	5000
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	5000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	5000

6.3. Administer TSAPI Link

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



The **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 **CM145** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.1**. Retain the default values in the remaining fields.



6.4. Administer Redbox 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 header includes the Avaya logo, the title 'Application Enablement Services Management Console', and system information such as 'Welcome: User cust', 'Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167', and 'Server Date and Time: Tue Sep 20 15:17:40 ICT 2022'. A red navigation bar contains 'User Management | User Admin | Add User' and 'Home | Help | Logout'. The left sidebar lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main content area is the 'Add User' form, which includes fields for User Id, Common Name, Surname, User Password, Confirm Password, Admin Note, Avaya Role, Business Category, Car License, CM Home, Css Home, CT User (set to Yes), Department Number, Display Name, Employee Number, and Employee Type. Fields marked with an asterisk are required.

6.5. Enable CTI User

Navigate to the CTI Users screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. In the CTI Users window, select the user that was set up in **Section 6.4** and select the **Edit** option.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: "Welcome: User: cust", "Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes155.aura.com/10.128.226.155", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Tue Sep 27 14:48:50 ICT 2022", and "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 to "CTI Users" and "List All Users" selected. The main content area displays a table of CTI Users:

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> redbox	redbox	NONE	NONE
<input type="radio"/> sestek	sestek	NONE	NONE
<input type="radio"/> tma	tma	NONE	NONE

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

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

The screenshot shows the "Edit CTI User" screen. The "User Profile" section includes: "User ID" (redbox), "Common Name" (redbox), "Worktop Name" (NONE), and "Unrestricted Access" (checked). The "Call and Device Control" section includes: "Call Origination/Termination and Device Status" (None). The "Call and Device Monitoring" section includes: "Device Monitoring" (None), "Calls On A Device Monitoring" (None), and "Call Monitoring" (unchecked). The "Routing Control" section includes: "Allow Routing on Listed Devices" (None). At the bottom are "Apply Changes" and "Cancel Changes" buttons.

6.6. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [4] to configure access privileges for the redbox user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". On the top right, system information is provided: "Welcome: User cust", "Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167", "Number of prior failed login attempts: 0", "HostName/IP: aes155.aura.com/10.128.226.155", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.0.1.0.7-0", "Server Date and Time: Fri Oct 21 17:16:55 ICT 2022", and "HA Status: Not Configured".

A red navigation bar contains "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar menu includes: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users.

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these is an "Apply Changes" button.

6.7. Restart Services

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows a welcome message for user 'cust' and system information including the last login time (Tue Aug 23 16:06:09 2022), IP address (172.16.8.167), and software version (10.1.0.1.0.7-0). The main navigation bar includes 'Maintenance | Service Controller' and 'Home | Help | Logout'. The left sidebar lists various management categories, with 'Maintenance' expanded to show 'Service Controller' as the active selection. The main content area, titled 'Service Controller', contains a table of services and their controller statuses:

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 service control area, there are several buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'.

7. Configure Red Box Quantify 6C

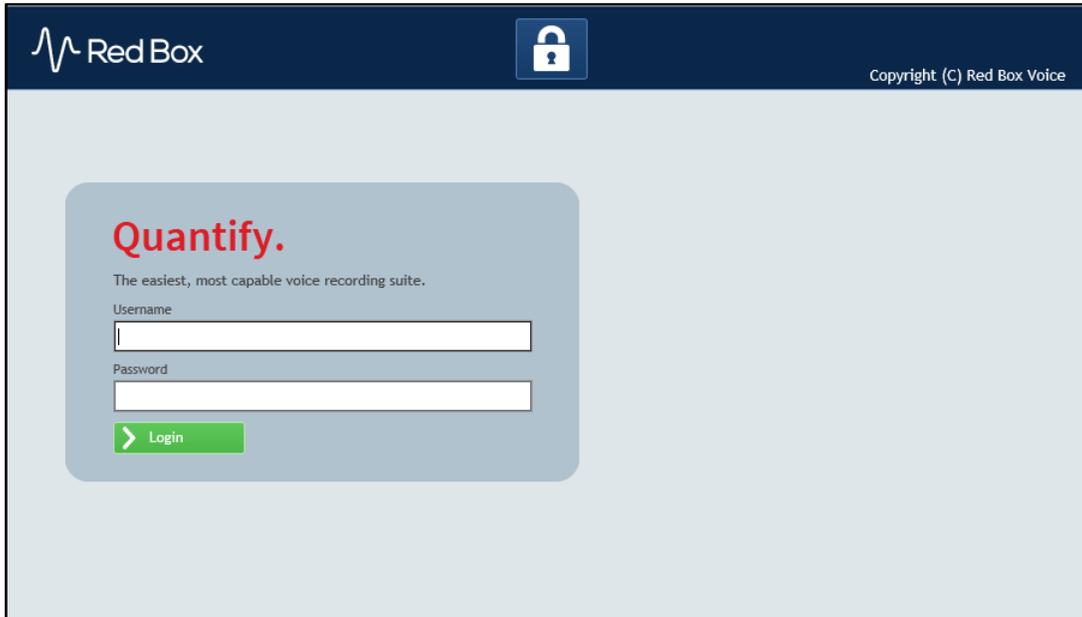
This section provides the procedures for configuring Red Box Quantify 6C. The procedures include the following areas:

- Administer register devices
- Administer CTI server
- Administer recording channels

The configuration of Red Box Quantify 6C is performed by Red Box installation engineers. The procedural steps are presented in these Application Notes for informational purposes.

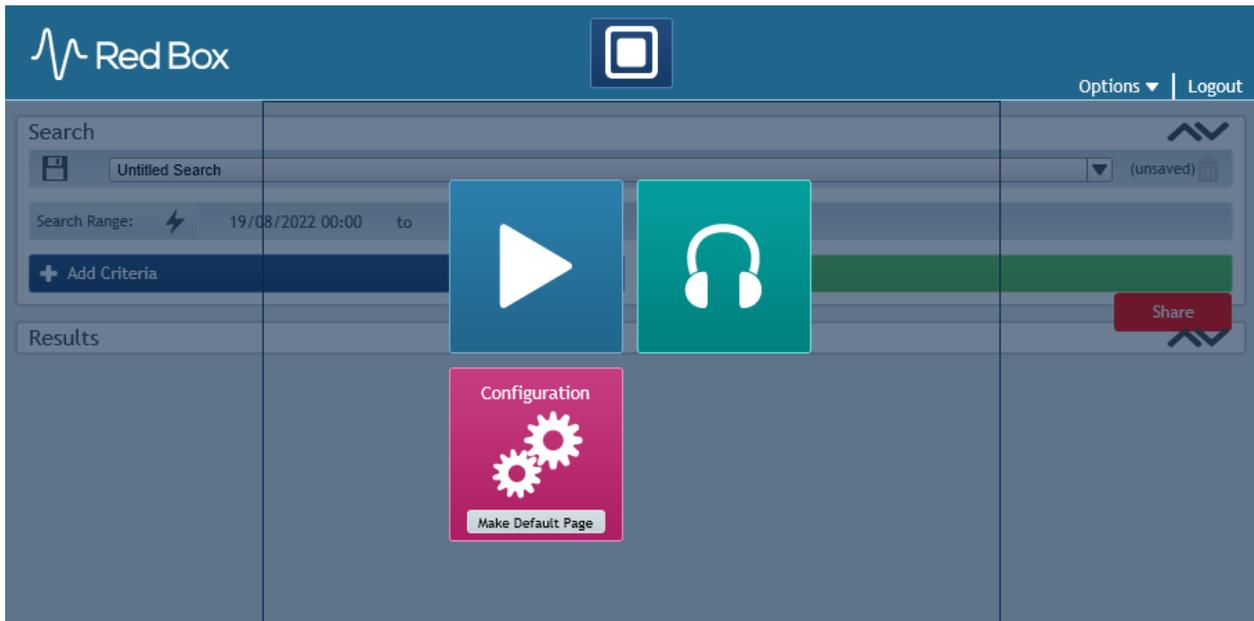
7.1. Administer Register Devices

Access the Red Box Quantify 6C web-based interface by using the URL “http://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Red Box Quantify 6C server. Log in using the appropriate credentials.



The screenshot shows the Red Box Quantify 6C login page. At the top left is the Red Box logo, and at the top right is a lock icon and the text "Copyright (C) Red Box Voice". The main content area features a light blue box with the heading "Quantify." and the tagline "The easiest, most capable voice recording suite." Below this are two input fields: "Username" and "Password". A green "Login" button with a right-pointing arrow is positioned below the password field.

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



The screen below is displayed next. Select **Setup** → **Register Devices**.



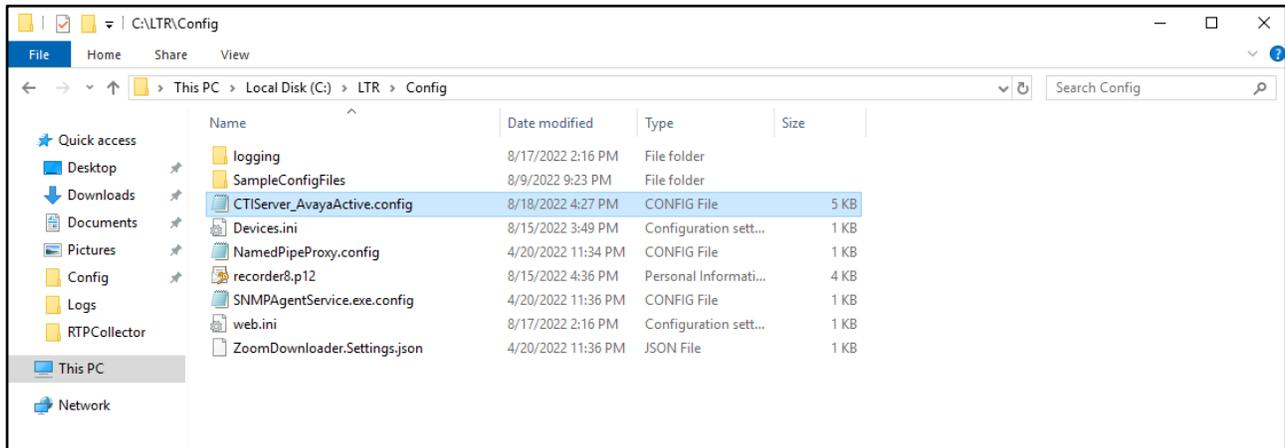
The **Register Devices** screen is displayed. Select **Device Type** as **Avaya Aura (Active)** and then in **Device Options** select **Recording Method** as **Multiple Registration**

Then add devices to register using **Add a Single Device** or **Add a Range of Devices**. After selecting all devices, click **Register**.

Device	Type	State
70000	Avaya Aura (Active)	New
70001	Avaya Aura (Active)	New
70010	Avaya Aura (Active)	New
70011	Avaya Aura (Active)	New

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.
- **dmccPort** Secure DMCC port **4722**
- **username:** The Quantify user credentials from **Section 6.4**.
- **password:** The Quantify user credentials from **Section 6.4**.
- **serverName** FQDN of Application Enablement Services.
- **useSsl** **true**
- **clientCertificateFile** PKCS12 client certificate file
- **clientCertificatePassword** PKCS12 client certificate password

```
CTIServer_AvayaActive - Notepad
File Edit Format View Help
<avaya protocolVersion="http://www.ecma-international.org/standards/ecma-323/csta/ed3/privB">
  <dmcc
    aesAddress="10.128.226.155"
    dmccPort="4722"
    username="redbox"
    password="Avaya1508@RedBox"|
    sessionDuration="180"
    sessionCleanupDelay="60"
    useSsl="true"
    serverName="AES155.aura.com"
    clientCertificateFile="C:\LTR\Config\recorder9.p12"
    clientCertificatePassword="avaya123"
  />
```

Scroll down and configure more parameters as below:

- **SwitchName:** The relevant switch connection name from **Section 6.3**.
- **StationPassword:** The security code for the extensions from **Section 5.2** and **Section 5.3**.



```
CTIServer_AvayaActive - Notepad
File Edit Format View Help

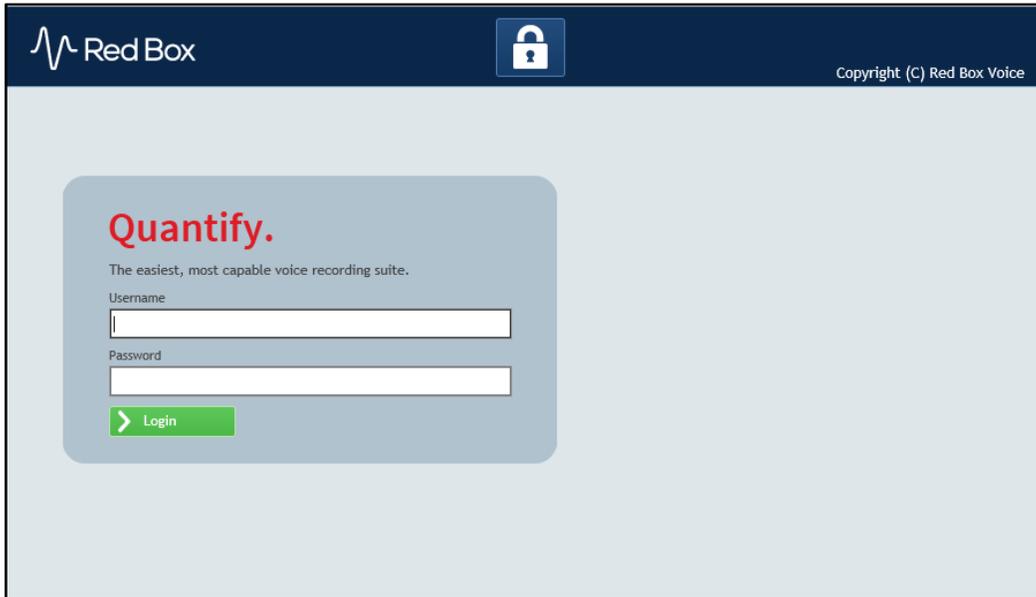
<device
  switchName="CM145"
  controllableByOtherSessions="false"
  instance="4"
  multiRegistrationModeIndependent="true"
  startRecordingOnDeliveredEvent="false"
  startRecordingOnDeliveredEventTimeout="60"
>
  <codecs>
    <add id="g711A"/>
    <add id="g711U"/>
    <add id="g722"/>
    <add id="g729"/>
    <add id="g729A"/>
    <add id="g723"/>
  </codecs>
  <encryptionSuites>
    <add id="srtp-aescm128-hmac80"/>
    <add id="aes"/>
    <add id="none"/>
  </encryptionSuites>
</device>

  <mr stationPassword="111222" mediaMode ="Separated" />

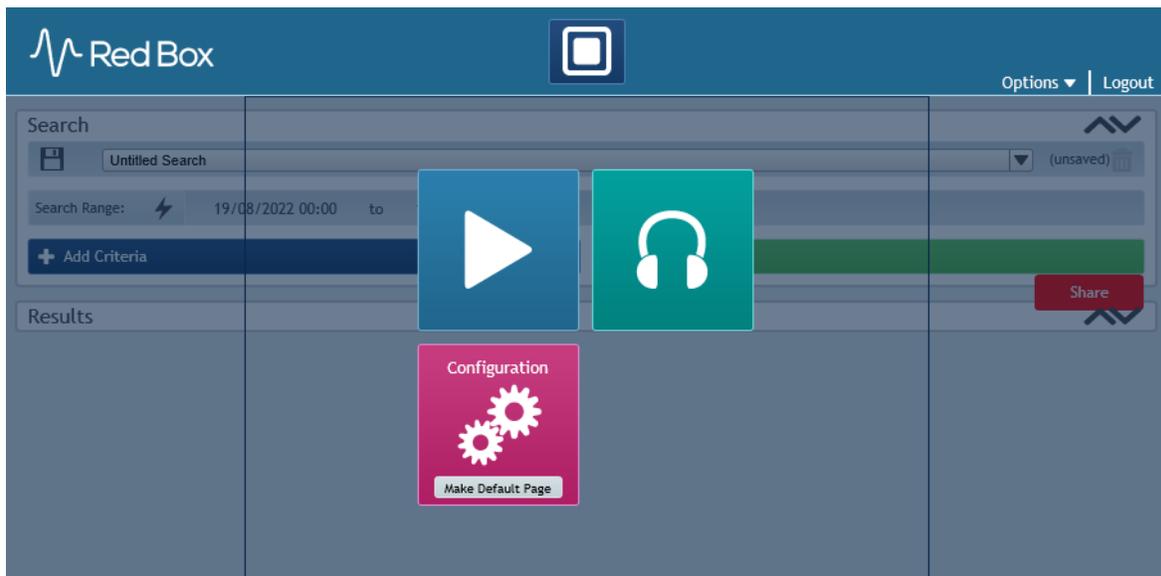
</avaya>
```

7.3. Administer Recording Channels

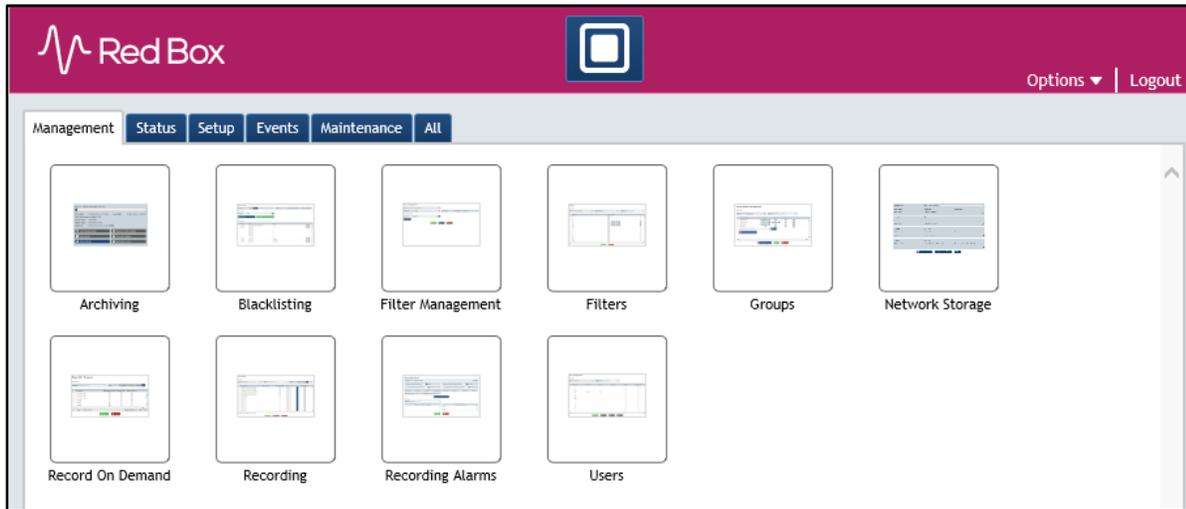
Access the Red Box Quantify 6C web-based interface by using the URL “http://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Red Box Quantify 6C server. Log in using the appropriate credentials.



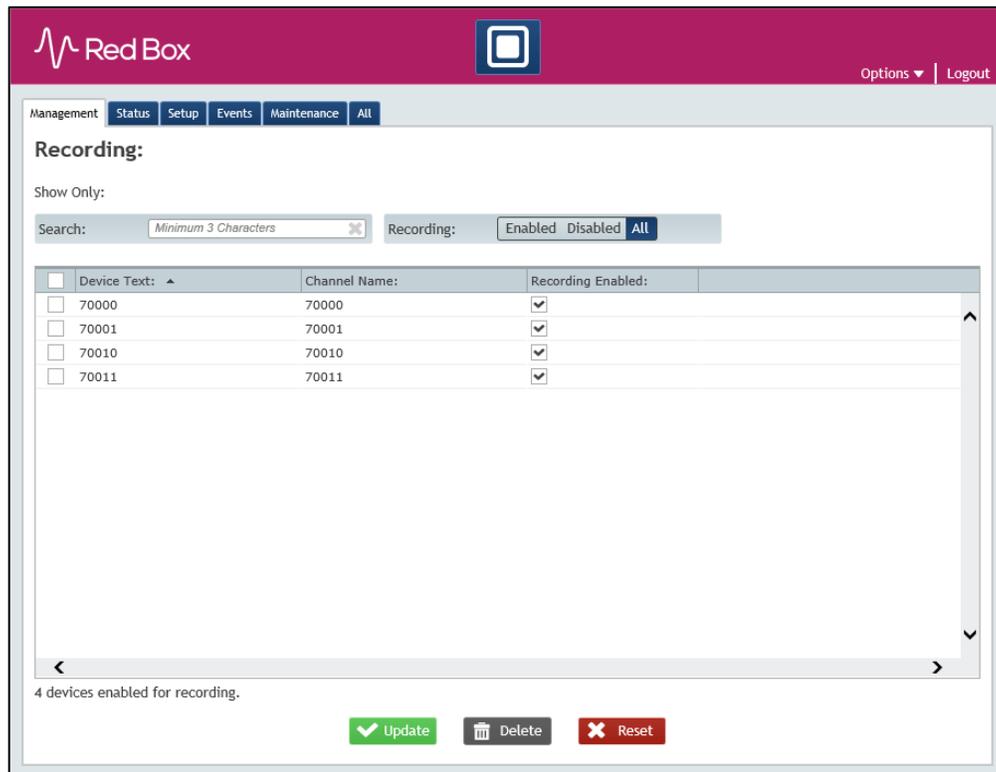
The screen below is displayed. Click on the **Configuration** icon.



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 extensions. In the compliance testing, four entries with **Device Text** of **70000**, **70001**, **70010** and **7011** 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 Red Box Quantify 6C.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.1**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aes155	established	1780	1780

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 extensions from **Section 5.2** and **Section 5.3**.

Welcome: User cust
 Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167
 Number of prior failed login attempts: 0
 HostName/IP: aes155.aura.com/10.128.226.155
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.0.1.0.7-0
 Server Date and Time: Tue Sep 20 16:25:53 ICT 2022
 HA Status: Not Configured

AVAYA Application Enablement Services Management Console

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

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

TSAPI Link Details

Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	CM145	1	Talking	Fri Sep 16 18:29:05 2022	Online	20	9	15	15	30

Online Offline

For service-wide information, choose one of the following:
 TSAPI Service Status TLink Status User Status

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 redbox user name from **Section 6.4**, and that the **# of Associated Devices** column reflects the total number of monitored extensions from **Section 5.2** and **Section 5.3**.



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.16
 Number of prior failed login attempts: 0
 HostName/IP: aes155.aura.com/10.128.226.155
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.0.1.0.7-0
 Server Date and Time: Tue Sep 20 17:59:20 ICT 2022
 HA Status: Not Configured

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

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

DMCC Service Summary - Session Summary

Please do not use back button

Enable page refresh every seconds

Session Summary [Device Summary](#)
 Generated on Tue Sep 20 17:59:00 ICT 2022

Service Uptime:	26 days, 3 hours 44 minutes
Number of Active Sessions:	5
Number of Sessions Created Since Service Boot:	144
Number of Existing Devices:	25
Number of Devices Created Since Service Boot:	205

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	CCDF8E0DD451B1629 8F3679E8348F034-120	redbox	Red Box Recorder	10.128.224.9	XML Encrypted	8
<input type="checkbox"/>	D6E40511CE699FC6E					

Click on active **Session ID** with the redbox username to show number of monitored extensions

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

DMCC Service Summary - Session Detail

Enable page refresh every seconds

Detailed Session View
Generated on Tue Sep 20 18:01:26 ICT 2022

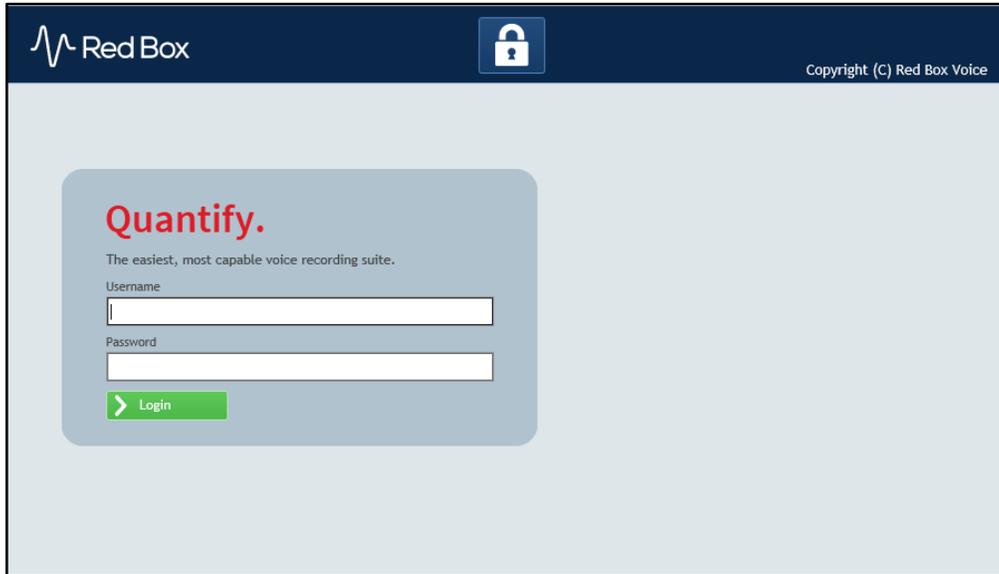
Session ID: CCDF8E0DD451B16298F3679E8348F034-120
 State: Active
 Time Established: Sat, Sep 17, 2022 12:16:05 PM GMT+07:00
 Uptime: 3 days, 5 hours, 45 minutes, and 21 seconds
 Cleanup Delay Timer: 60 seconds
 Session Duration Timer: 180 seconds
 Time of Most Recent Timer Reset: Tue, Sep 20, 2022 06:00:56 PM ICT
 Reconnect Counter: 0

Devices Associated with Session

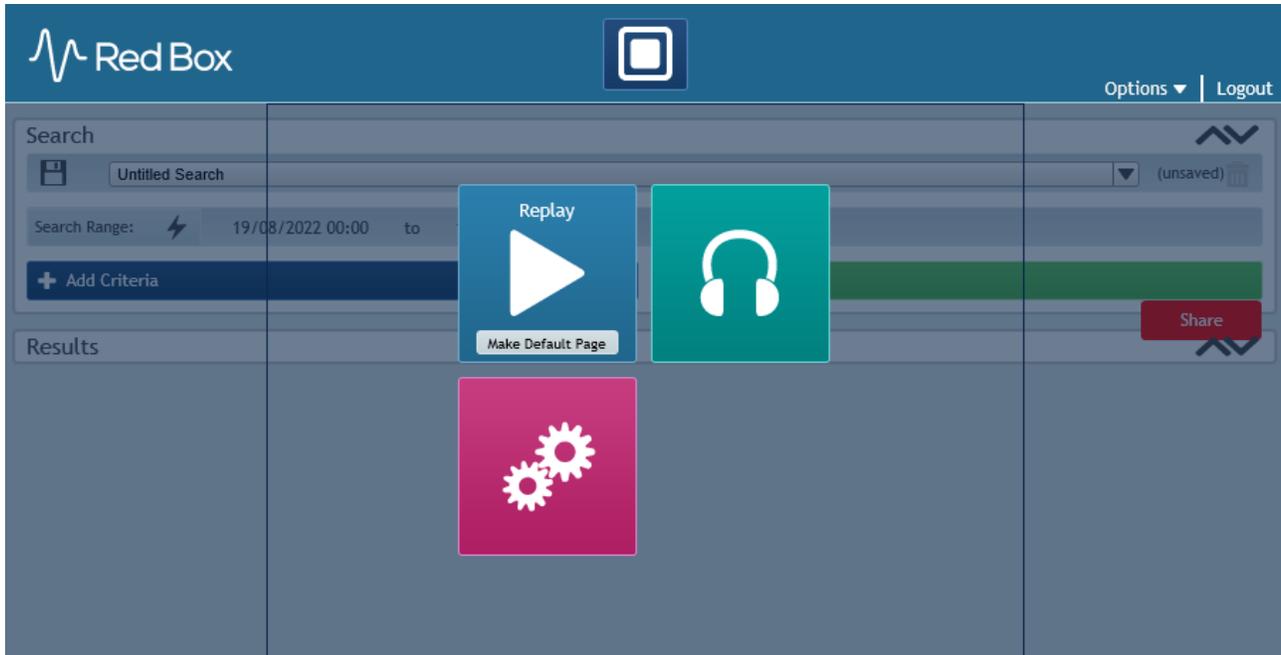
	Device ID	State
<input type="checkbox"/>	70011:CM145:0.0.0.0:4	REGISTERED
<input type="checkbox"/>	70000:CM145:0.0.0.0:5	REGISTERED
<input type="checkbox"/>	70001:CM145:0.0.0.0:5	REGISTERED
<input type="checkbox"/>	70000:CM145:0.0.0.0:4	REGISTERED
<input type="checkbox"/>	70001:CM145:0.0.0.0:4	REGISTERED
<input type="checkbox"/>	70011:CM145:0.0.0.0:5	REGISTERED
<input type="checkbox"/>	70010:CM145:0.0.0.0:5	REGISTERED
<input type="checkbox"/>	70010:CM145:0.0.0.0:4	REGISTERED

8.3. Verify Red Box Quantify 6C

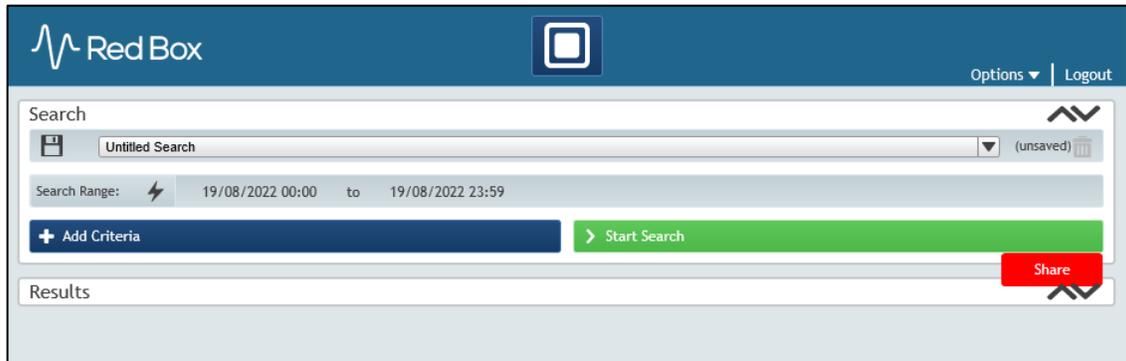
Follow the procedures in **Section 7.3** to log in to the Red Box Quantify 6C web-based interface.



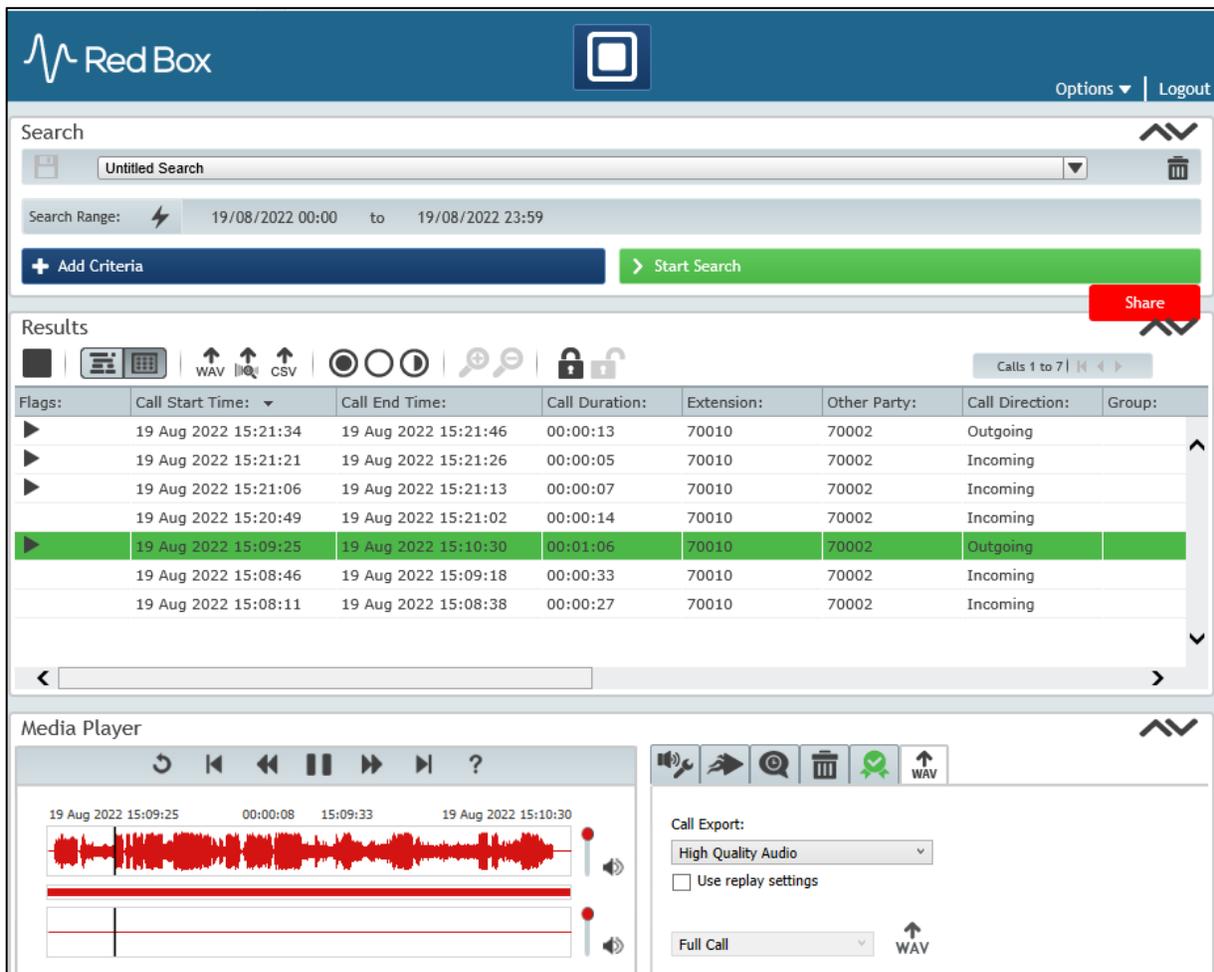
The screen below is displayed. Click on the **Replay** icon.



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 6C to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 10.1 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 Avaya and Red Box Quantify 6C 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*, Release 10.1.x, Issue 1, Dec 2021
2. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022
3. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022
4. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 4, April 2022

Product Documentation for Red Box products may be found at <https://www.redboxvoice.com/>

©2022 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.