



Avaya Solution & Interoperability Test Lab

Application Notes for Red Box Quantify 6C with Avaya Aura® Contact Center 7.1.2 and Avaya Aura® Application Enablement Services 10.1 using CCT Open Interfaces and DMCC Multiple Registration – Issue 1.2

Abstract

These Application Notes describe the configuration steps required for Red Box Quantify 6C with Avaya Aura® Contact Center 7.1.2 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® Contact Center 7.1.2 and Avaya Aura® Application Enablement Services 10.1 using CCT Open Interfaces and 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 and Open CCT 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 Avaya Aura® Contact Center 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.
- **Serviceability testing** - The behaviours 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 RedBox Quantify 6C can be obtained through the following:

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

3. Reference Configuration

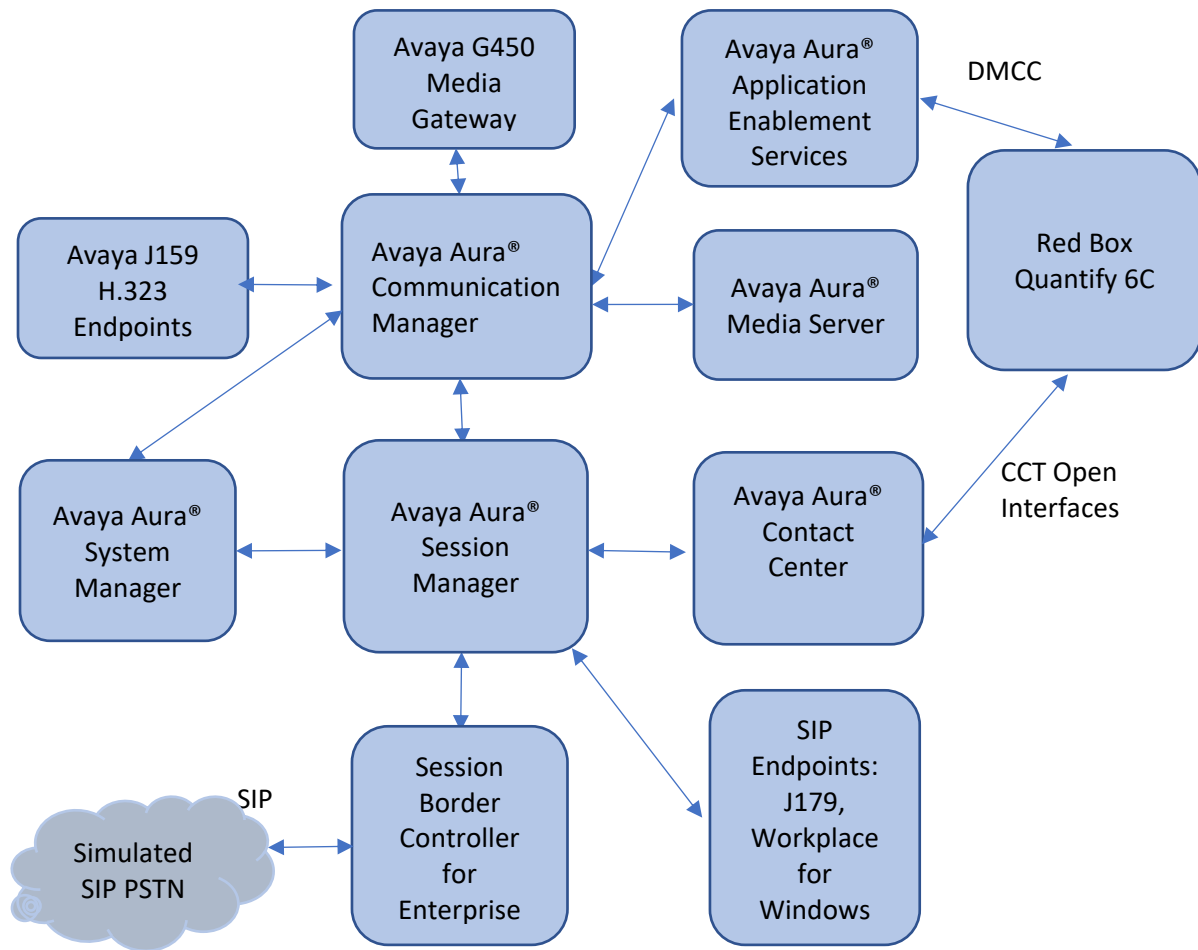


Figure 1: Compliance Testing Configuration

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 Aura® Contact Center	7.1.2
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 Contact Center 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: 1	CTI LINK
Extension: 79999	
Type: ADJ-IP	
Name: aes95	COR: 1

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 8**. 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
Type: 9641	Security Code: 111222
Port: S000004	Coverage Path 1:
Name: H323 Ext1	Coverage Path 2:
	Hunt-to Station:
	BCC: 0
	TN: 1
	COR: 1
	COS: 1
	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:	
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

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

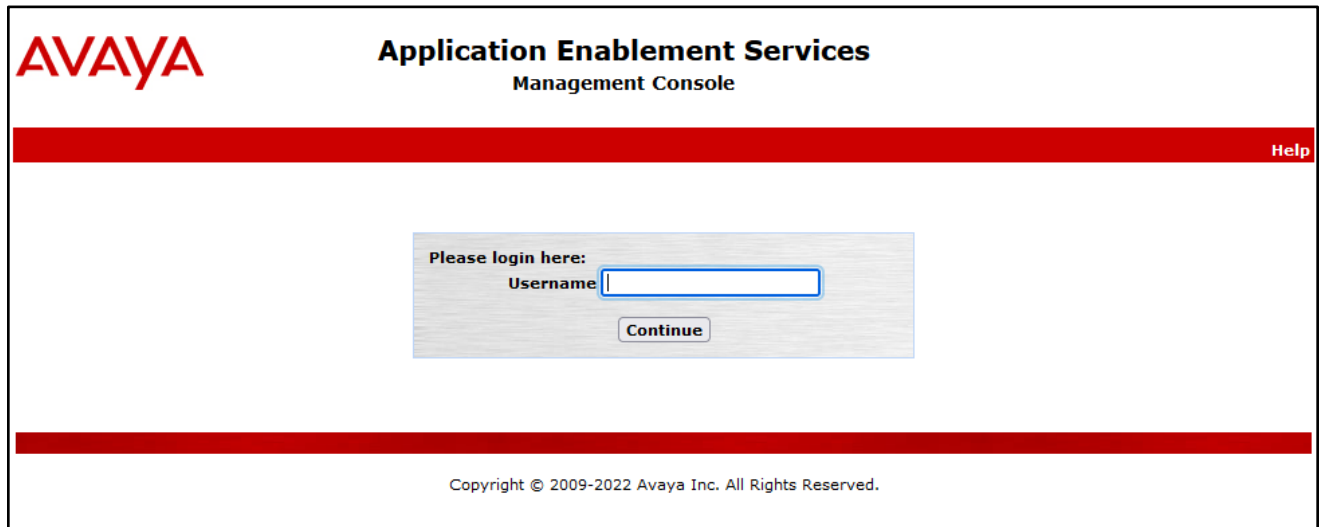
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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 interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with a "Help" link in the top right corner. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." is displayed.

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



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 27 16:37:37 2022 from 172.16.8.16
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Jul 05 06:22:34 EDT 2022
HA Status: Not Configured

HomeHome | Help | Logout

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

Welcome to OAM

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

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

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

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).

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Jul 5 17:22:35 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Jul 05 07:20:30 EDT 2022
HA Status: Not Configured

Licensing

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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

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.

AVAYA Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Search 🔍

Home Licenses

Licenses

WebLM Home

Install license

Licensed products

APPL_ENAB

Application_Enablement

View license capacity

View peak usage

ASBCE

Session_Border_Controller_E_AE

AVAYA_AURAWEBGATEWAY

AVAYA_AURAWEBGATEWAY

AVP

AVP

CALL_CENTER_ELITE_MULTICHANNEL

Call_Center_Elite_Multichannel

Configure Centralized Licensing

CCTR

Contact_Center

CE

COLLABORATION_ENVIRONMENT

COMMUNICATION_MANAGER

Call_Center

Communication_Manager

Configure Centralized Licensing

Dialog_Designer

IPO

IP_Office

MESSAGING

Application Enablement (CTI) - Release: 10 - SID: 10503000 Standard Li

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: September 6, 2019 4:38:44 PM +07:00

License File Host IDs: V7-67-C3-CF-17-1A-01

Licensed Features

13 Items Show All ▾

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
AES HA LARGE VALUE_AES_HA_LARGE	permanent	100
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	100
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	100

SmallServerTypes:
s8300c;s8300d;icc;premio;tn8400;laptop;CtiS
MediumServerTypes:
ibm306;ibm306m;all1050;ibm306;ibm306m

6.3. Administer TSAPI Link

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

The screenshot shows the 'TSAPI Links' screen in the Management Console. The left navigation pane is expanded to 'TSAPI Links'. The main content area has a red header bar with 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. Below the header, there is a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'. The 'HA Status: Not Configured' message is visible at the top right of the page.

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 **CM93** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.1**. Retain the default values in the remaining fields.

The screenshot shows the 'Edit TSAPI Links' screen in the Management Console. The left navigation pane is expanded to 'TSAPI Links'. The main content area has a red header bar with 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. Below the header, there is a form with fields: Link (1), Switch Connection (CM93), Switch CTI Link Number (1), ASAI Link Version (12), and Security (Both). Below the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'. The 'HA Status: Not Configured' message is visible at the top right of the page.

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.

AVAYA

Application Enablement Services
Management Console

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 15:17:40 ICT 2022
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

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.

AVAYA

Application Enablement Services
Management Console

WELCOME: User: tsk
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
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Account Management

Audit

Certificate Management

Enterprise Directory

Host AA

PAM

Security Database

Control

CTI Users

List All Users

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

Edit List All

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

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

redbox

redbox

NONE

☒

Call and Device Control:

Call Origination/Termination and Device Status

None

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None

None

☐

Routing Control:

Allow Routing on Listed Devices

None

Apply Changes

Cancel Changes

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 header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with system details. A red navigation bar contains the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various service categories, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", along with 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**.

AVAYA

Application Enablement Services
Management Console

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 15:27:30 ICT 2022
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

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

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

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

7. Configure Avaya Aura® Contact Center

It is implied that a working Avaya Aura® Environment, which includes System Manager, Session Manager, Communication Manager, Media Server, and Contact Center, is already in place with the necessary licensing. For all other provisioning information, such as initial installation and configuration, please refer to the product documentation in **Section 11**.

This section shows the steps required to add a new CCT Agent on Avaya Aura® Contact Center. The following sections give step by step instructions on how to add the following.

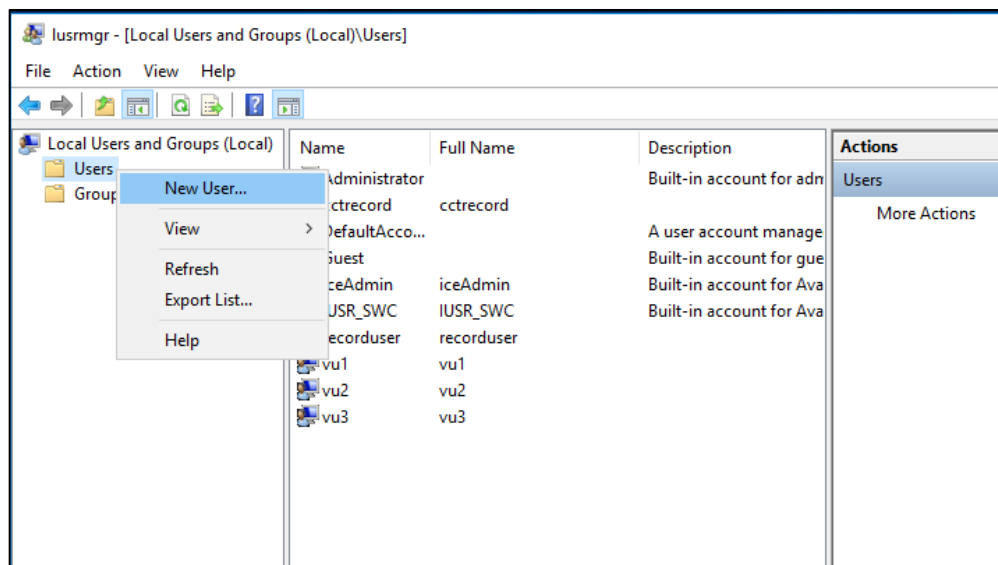
- Create a Windows user on the Avaya Aura® Contact Center Server
- Login to Avaya Aura® Contact Center Manager
- Configure a Contact Center CCT Agent
- Verify CCT User Association
- Verify CCT Web Services

7.1. Create a Windows user on the Avaya Aura® Contact Center Server

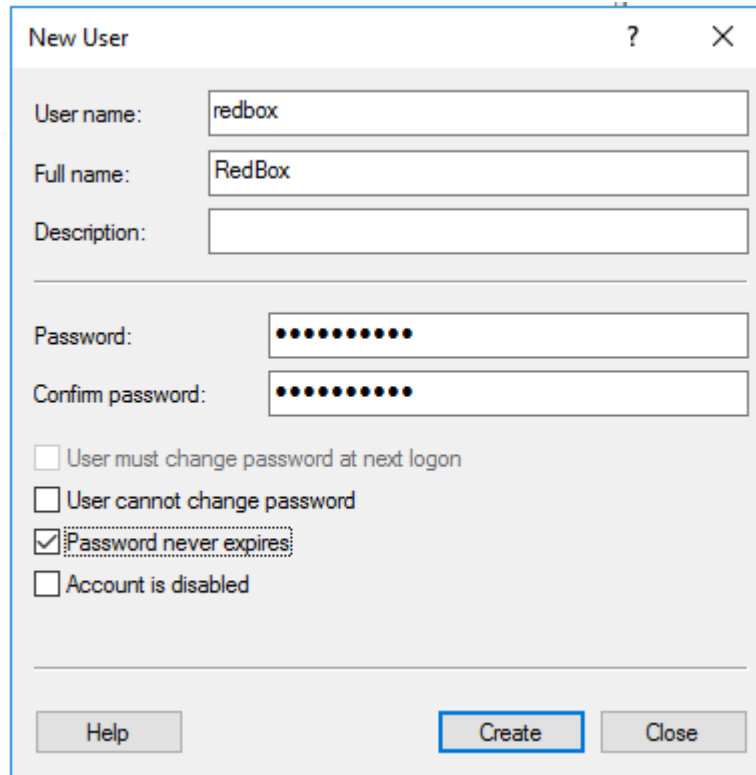
All CCT users must be associated with a user account on Windows Active Directory/Domain User account. When a Contact Center user is created there is an option to create a CCT user and there is an association made there with a Windows domain user, see **Section 7.3**. Users who can access multiple domains can also access the CCT client as long as trust is established between the domains; the user does not have to log on to separate domains to use the CCT client.

If there is no Active Directory already in place, then a windows user must be added to the Contact Center server before a CCT user is added. In the example below a new user called agent1 was created on the local Windows Server. To add a new windows user, navigate to Computer Management. On windows 2016 server simply type in Computer Management on the screen and the program will appear.

From Computer Management, in the left window, expand **System Tools → Local Users and Groups → Users** and right click on **Users** and select **New User** as shown below.



Enter the Username and Password noting that this same username and password will be required in configuring the Contact Center CCT Agent. Ensure that Password never expires is ticked. Click on **Create** once the information is filled in correctly.



New User ? X

User name:

Full name:

Description:

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

7.2. Login to Avaya Aura® Contact Center Manager

Launch URL: **http://<IP Address of AACC>** and login to the Contact Center Management Administration with administrative credentials. The Contact Center Launch pad is displayed



7.3. Configure a Contact Center CCT Agent

In the Launch pad, click **Contact Center Management** (not shown). In the left pane, click the Contact Center Manager to which the agent is to be added. On the top menu, select **Add → Agent**. The following highlighted fields were configured:

- **User Type:** Select Agent as User Type.
- **Login ID:** The number the agent enters to logon to the phone. In this case the field is set to the extension (75000).
- **Primary Supervisor:** Select Default Supervisor from the list.
- **Voice URI:** The SIP address of the TR87-controlled terminal dedicated to this agent, in the format sip:agent (use Extension@SIPdomain, where SIPdomain is the CCMS Local SIP Subscriber Domain name. For example, sip:75000@aura.com).
- **Create CCT Agent:** Tick on this check box to associate the agent with CCT. As the **Create CCT Agent** is selected, the **Associate User Account** section will be displayed. Expand this section, select **Search local operating system** and click on **List All** button, it will list all local operating system users including the Windows user **redbox** created in the section above. Select the **redbox**, the **redbox** is now displayed in the **CCT Agent Login Details**.

Click **Contact Types** (not shown), which is then expanded. Select the check box beside each **Contact Type** to assign to the agent (for example, **Voice**).

New Agent Details: **redbox RedBox**

User Details

First Name: **redbox**
Last Name: **RedBox**
Title:
Department:
Language: **English**
Comment:

User Type: **Agent**
Login ID: **75000**
Voice URI: **sip:75000@aura.com**
IM URI: **sip:**

Account Type:
☒ Create CCT Agent

CCT Agent Login Details

Domain: **AACC199**
User ID: **redbox**

Associate User Account

☒ Search local operating system ☐ Search local security server ☐ Search domain users

Search all user accounts where:
Full Name starts with and includes **all users**

User Name	Full Name (11) <input type="button" value="v"/>	Status
<input type="radio"/> iceAdmin	iceAdmin	Available
<input type="radio"/> IUSR_SWC	IUSR_SWC	Available
<input type="radio"/> recorduser	recorduser	Available
<input checked="" type="radio"/> redbox	RedBox	Available
<input type="radio"/> vu1	vu1	Available
<input type="radio"/> vu2	vu2	Available
<input type="radio"/> vu3	vu3	Available

Click the **Skillsets** heading to expand the branch. Click **List All** to list all skillsets configured on the server. From the **Priority** list for each skillset to assign to the agent, select the priority levels (For example select **Voice** and set the priority level 48).

▼ Skillsets

Skillset Name (1)	Contact Type	Priority
Default_Skillset	Voice	48 ▼

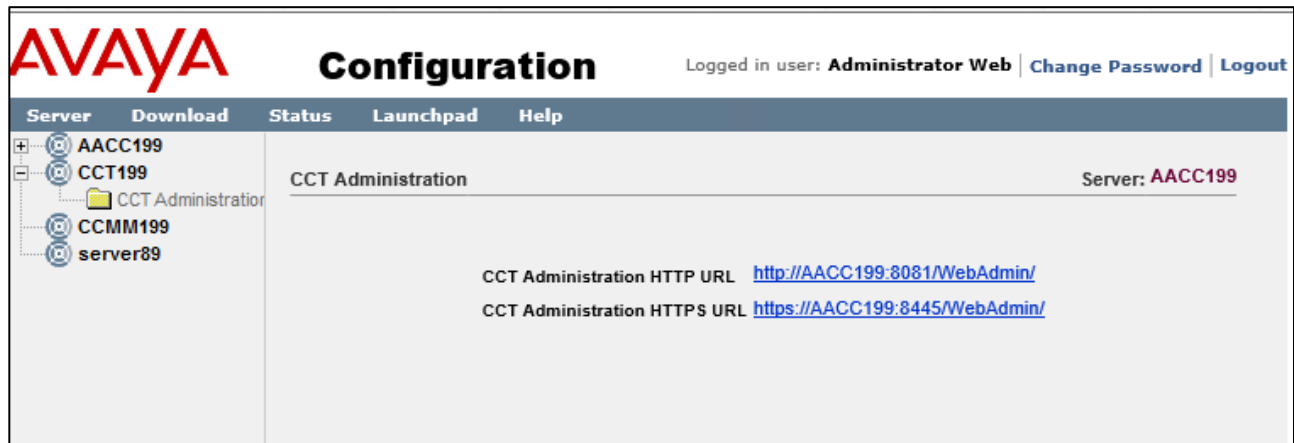
► [Assign Skillsets](#)

7.4. Verify CCT User Association

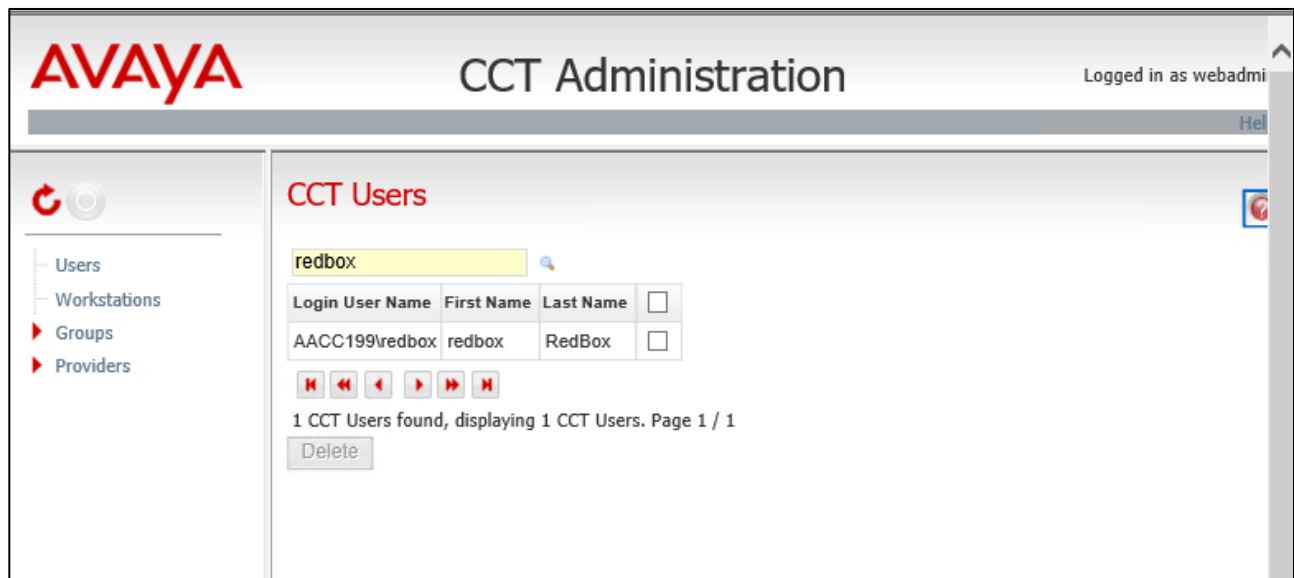
To check to see that the CCT User and Contact Center Agent are associated correctly, navigate to **Configuration** on the Launchpad as shown below.



Expand the CCT Server in the left window and click on **CCT Administration**. Click on **CCT Administration URL** in the main window.



The **CCT Administration** window opens in a separate browser session. Click on **Users** in the left window and double-click on the user added from **Section 7.3**.



Select the agent you require agent metadata for from the column “Agents Available”. In the example agent **75000** is selected.

Update CCT User

User Details

Login User Name

AACC199\redbox

First Name

redbox

Last Name

RedBox

Address Assignments

Terminal Assignments

Terminal Group Assignments

Address Group Assignments

Agent Assignments

Agents available

☐

Agents

20005

20004

20001

50004

50006

<

>

6 Agents found. Page 1 / 1

Agents mapped

☐

Agents

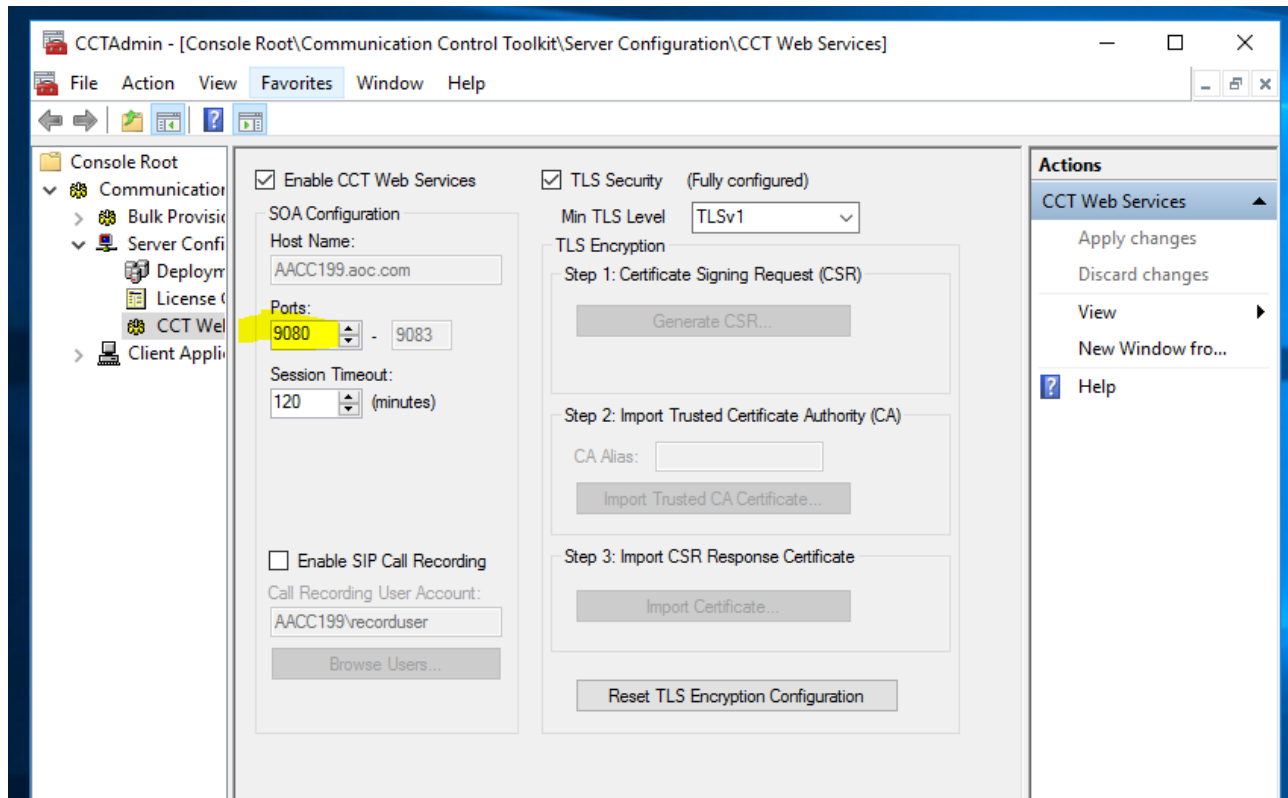
75000

1 Agents found. Page 1 / 1

Save

7.5. Verify CCT User Association

From AACC Window Server, navigate to **Start → Programs → Avaya → Contact Center → Communication Toolkit → CCT Console**. Verify CCT Web Services check box and TLS Security were checked. In this compliance test CCT Webservice uses port **9080**, with **TLS**



8. Configure Red Box Quantify 6C

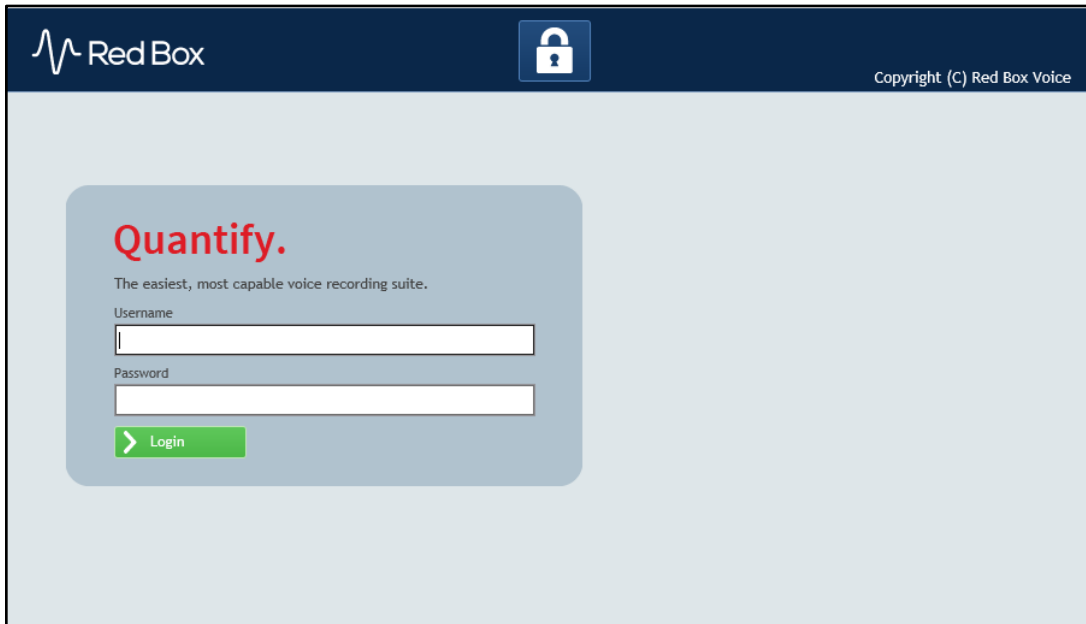
This section provides the procedures for configuring Red Box Quantify 6C. The procedures include the following areas:

- 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.

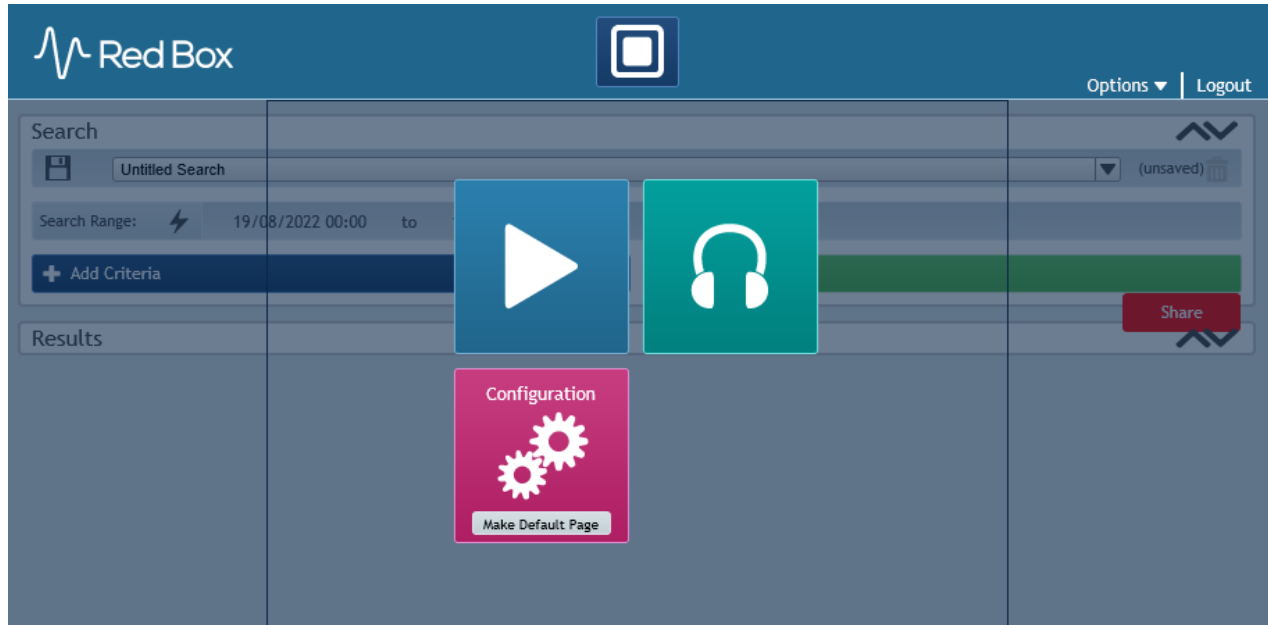
8.1. Administer Register Devices

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.

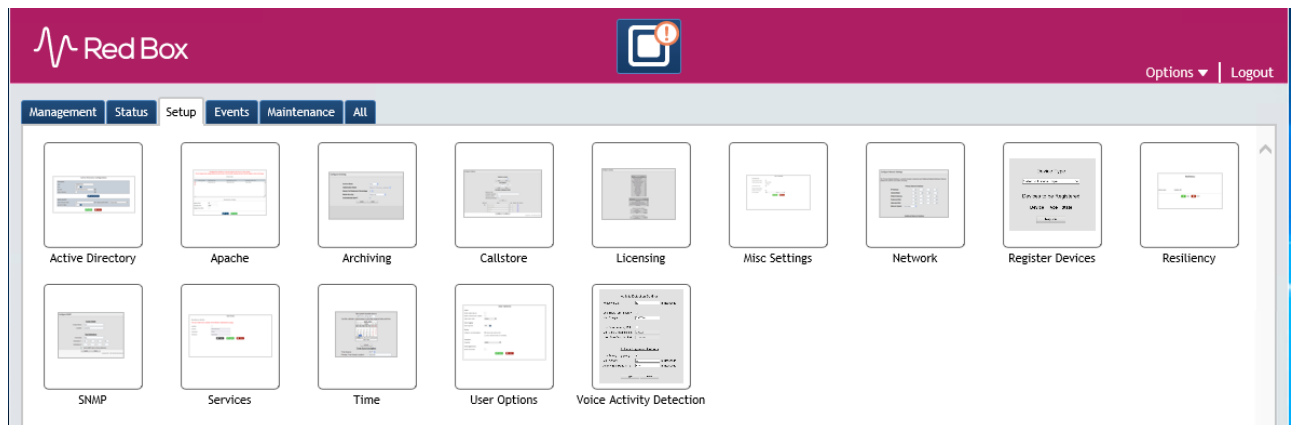


The screenshot shows the Red Box Quantify 6C login page. At the top, there is a dark blue header bar with the Red Box logo on the left, a lock icon in the center, and the text "Copyright (C) Red Box Voice" on the right. Below the header, the main content area is light blue. In the center, there is a white rounded rectangle containing the "Quantify." logo in red, followed by the tagline "The easiest, most capable voice recording suite." Below this, there are two input fields labeled "Username" and "Password". At the bottom of the white box is a green button with a right-pointing arrow and the text "Login".

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**

Red Box

Management Status Setup Events Maintenance All

Device Type

Avaya Aura (Active) ▼

Device Options

Recording Method Multiple Registration ▼

Enable Warning Tones ☐

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

Add a Single Device

Extension 70011

Add

Add a Range of Devices

First Extension Last Extension

Add

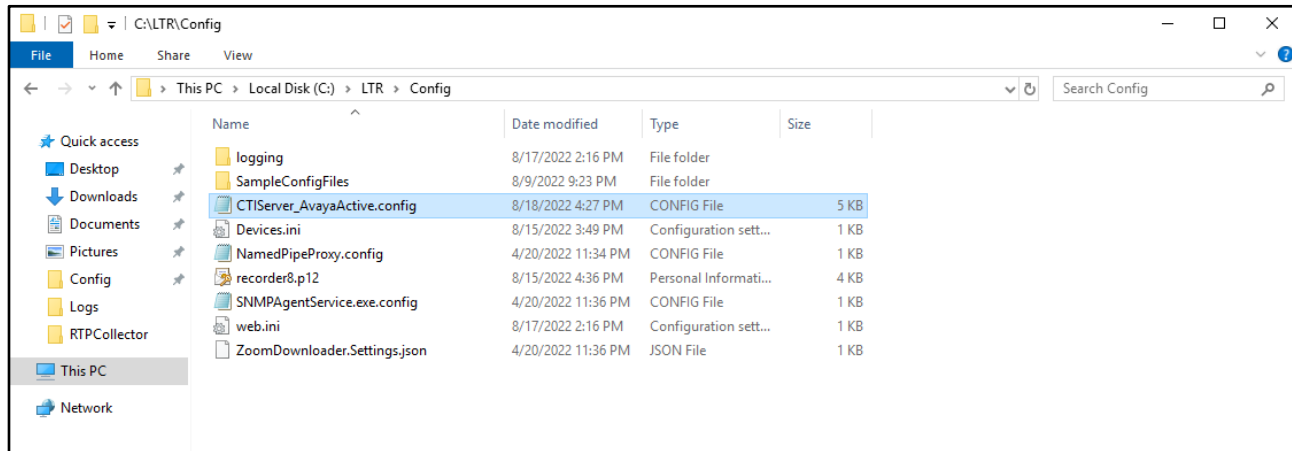
Devices to be Registered

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

Register

8.2. 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



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**.



```
<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>
```

Open the **CTIServer_AvayaACC.config** file with the Notepad application. Navigate to the **aacc** sub-section, and configure the parameters as shown below.

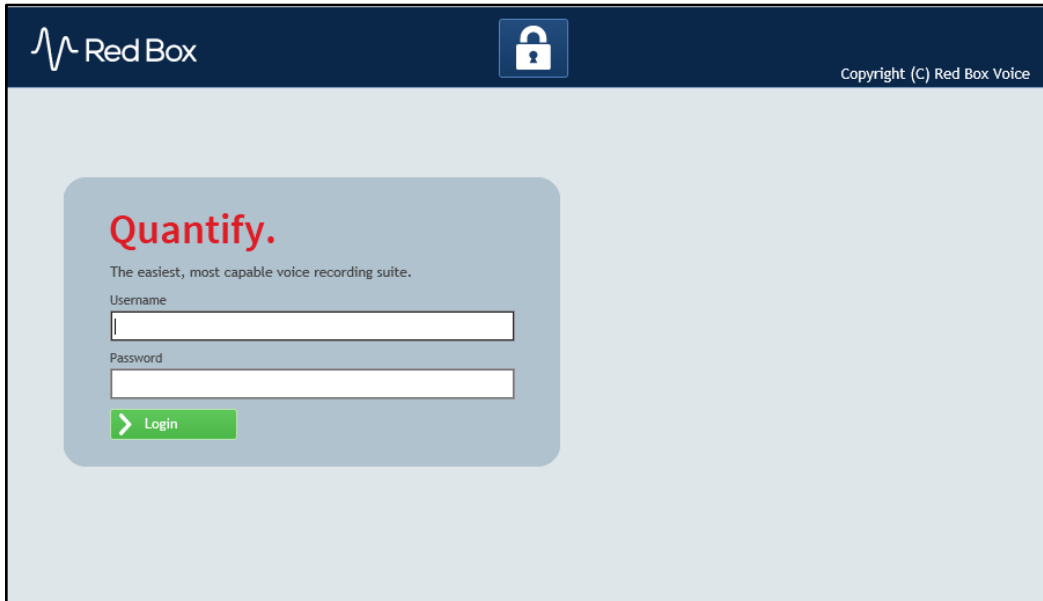
- **primaryServer prefix:** https
- **primaryServer ip** IP Address of Contact Center
- **primaryServer port** 9080
- **loginSettings domain** AACC199
- **username:** The Quantify user credentials from **Section 7.3**.
- **password:** The Quantify user credentials from **Section 7.3**.



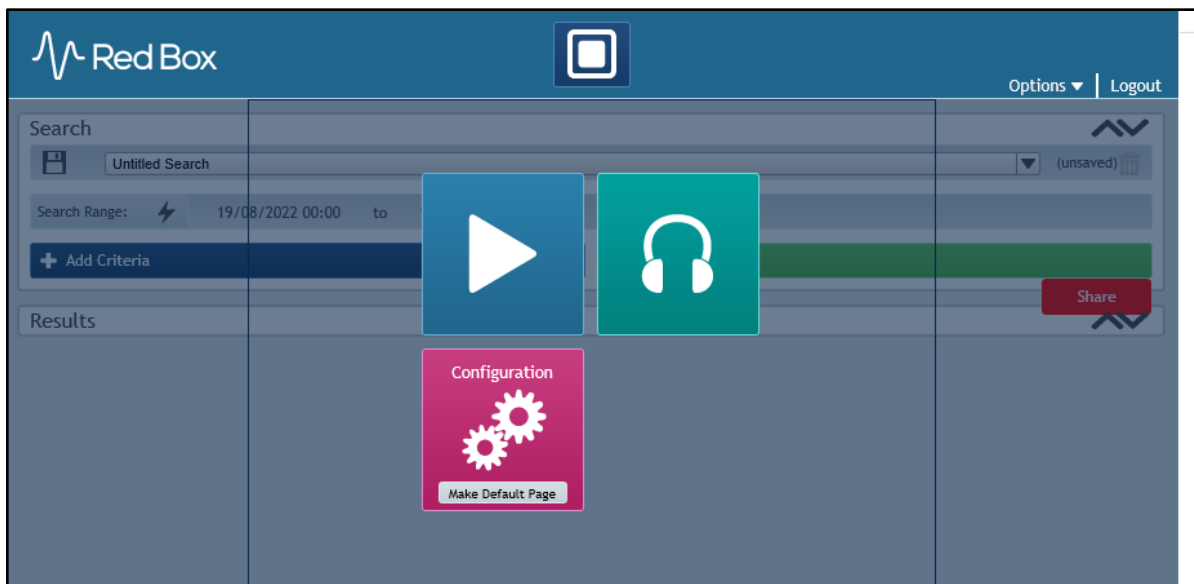
```
<aacc>
  <primaryServer prefix="https" ip="10.30.5.199" port="9080" />
  <notificationConsumers>
    <notificationConsumer>
      <loginSettings domain="AACC199" user="redbox" password="enc:QXZheWExdMjM=" />
      <hostSettings prefix="https" ip="10.128.224.10" port="9081" skipRemoteCertificateVerification="true"
        certificatePath="C:\LTR\Config\Certs\recorder10.pem" certificateKeyPath="C:\LTR\Config\Certs\recorder10.key.pem" />
    </notificationConsumer>
  </notificationConsumers>
  <callStorage storageType="FileAndRecorder" storageOption="./AvayaData.txt" />
</aacc>
</configuration>
```

8.3. Administer Recording Channels

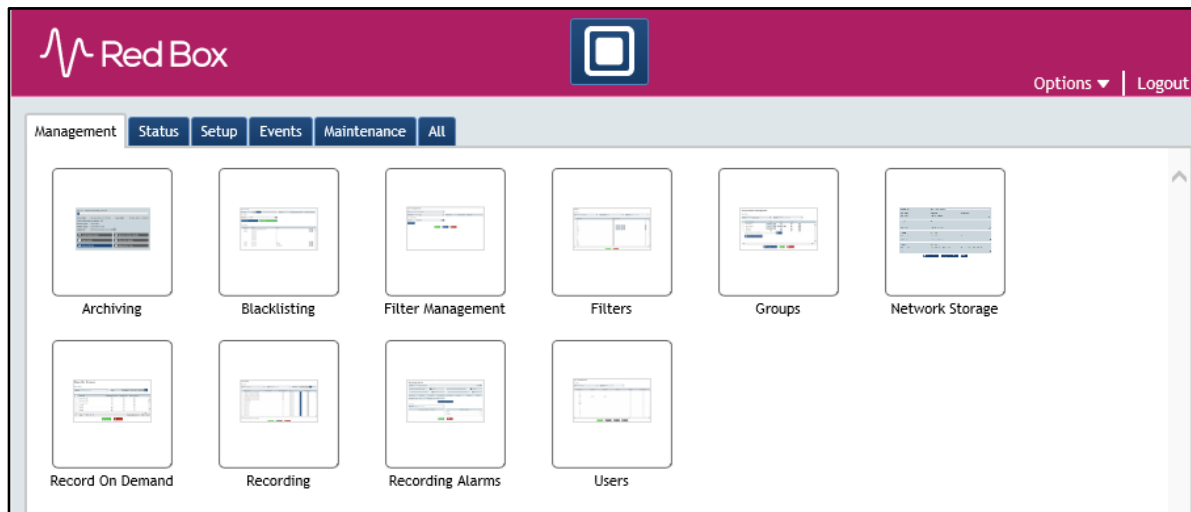
Access the Red Box Quantify 6C web-based interface by using the URL “http://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Red Box Quantify 6C server. Log in using the appropriate credentials.



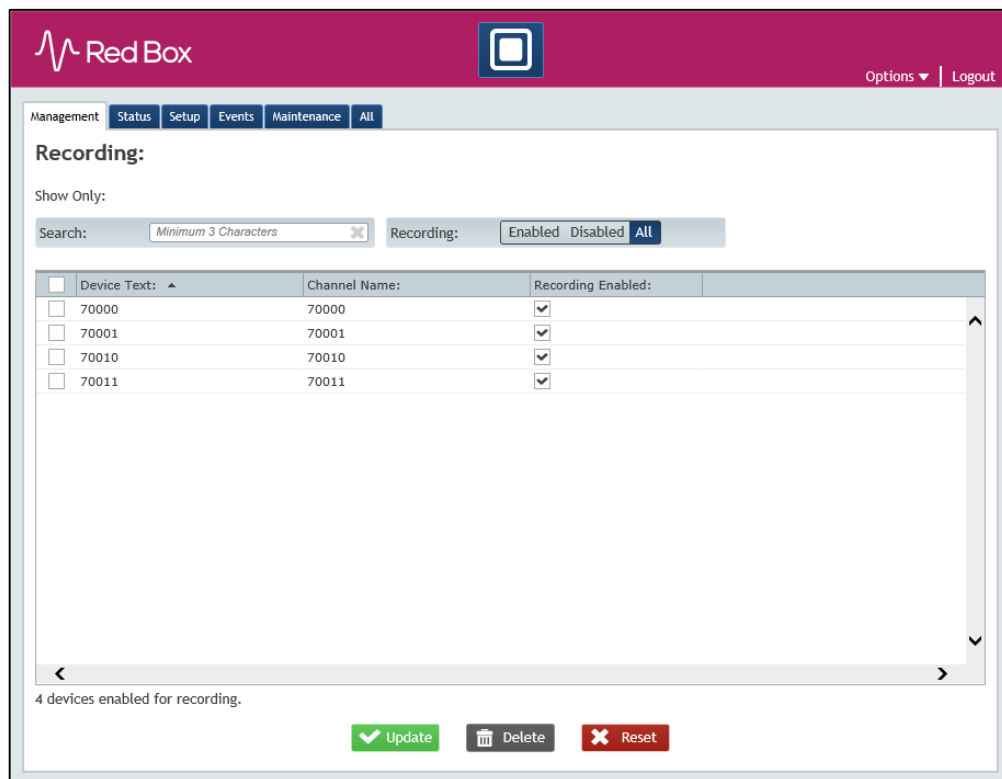
The screen below is displayed. Click on the **Configuration** icon.



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 agent extensions. In the compliance testing, four entries with **Device Text** of **70000**, **70001**, **70010** and **7011** were checked.



9. 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.

9.1. 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 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	aes95	established	1780	1780

9.2. 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**.

AVAYA

Application Enablement Services
Management Console

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

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 172.16.8.167
 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: Mon Oct 17 18:43:58 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**

▪ Switch Conn Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Mon Oct 17 18:43:58 ICT 2022

Service Uptime: 53 days, 4 hours 29 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 214

Number of Existing Devices: 11

Number of Devices Created Since Service Boot: 328

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	4EA3C633F96188DC6 39EA3E349ADC6AB-211	redbox	Red Box Recorder	10.128.224.10	XML Encrypted	8
<input type="checkbox"/>	AFE4E926F1C8A5E79 1E38CAB6F7851AA-214	sestek	SestekFalconRecorder	10.103.1.50	XML Encrypted	3

Terminate Sessions
Show Terminated Sessions

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

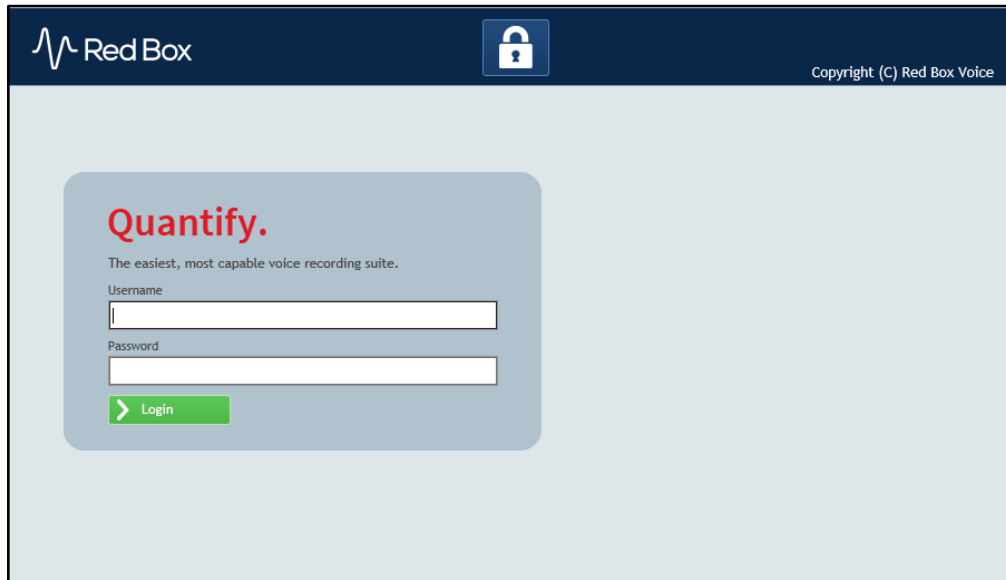
Detailed Session View
Generated on Mon Oct 17 18:44:20 ICT 2022
Session ID: 4EA3C633F96188DC639EA3E349ADC6AB-211
State: Active
Time Established: Sat, Oct 15, 2022 12:14:56 PM GMT+07:00
Uptime: 2 days, 6 hours, 29 minutes, and 24 seconds
Cleanup Delay Timer: 60 seconds
Session Duration Timer: 180 seconds
Time of Most Recent Timer Reset: Mon, Oct 17, 2022 06:43:45 PM ICT
Reconnect Counter: 0

Devices Associated with Session

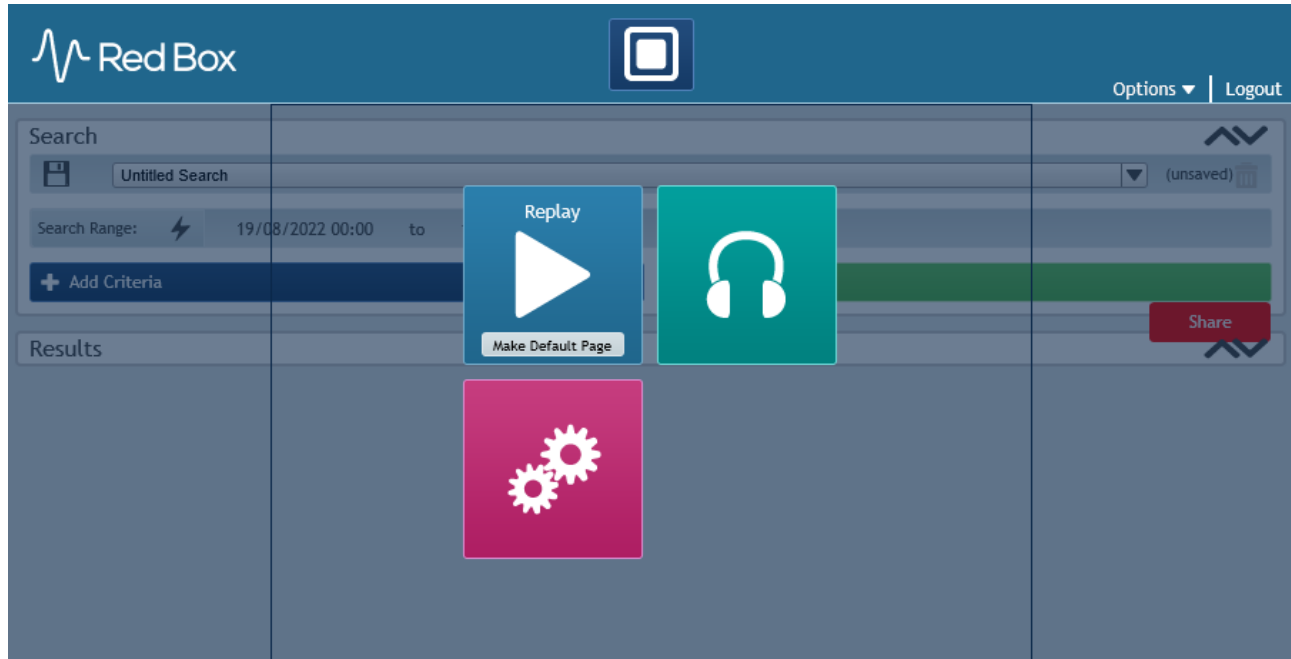
	Device ID	State
<input type="checkbox"/>	70011:CM145:0.0.0.0:3	REGISTERED
<input type="checkbox"/>	70001:CM145:0.0.0.0:3	REGISTERED
<input type="checkbox"/>	70011:CM145:0.0.0.0:2	REGISTERED
<input type="checkbox"/>	70001:CM145:0.0.0.0:2	REGISTERED
<input type="checkbox"/>	70000:CM145:0.0.0.0:3	REGISTERED
<input type="checkbox"/>	70000:CM145:0.0.0.0:2	REGISTERED
<input type="checkbox"/>	70010:CM145:0.0.0.0:3	REGISTERED
<input type="checkbox"/>	70010:CM145:0.0.0.0:2	REGISTERED

9.3. 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.

Red Box

Options | Logout

Search

Untitled Search (unsaved)

Search Range: 19/08/2022 00:00 to 19/08/2022 23:59

+ Add Criteria Start Search Share

Results

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

Red Box

Options | Logout

Search

Untitled Search

Search Range: 19/08/2022 00:00 to 19/08/2022 23:59

+ Add Criteria Start Search Share

Results

Flags: Call Start Time: Call End Time: Call Duration: Extension: Other Party: Call Direction: Group:

▶	19 Aug 2022 15:21:34	19 Aug 2022 15:21:46	00:00:13	70010	70002	Outgoing	
▶	19 Aug 2022 15:21:21	19 Aug 2022 15:21:26	00:00:05	70010	70002	Incoming	
▶	19 Aug 2022 15:21:06	19 Aug 2022 15:21:13	00:00:07	70010	70002	Incoming	
▶	19 Aug 2022 15:20:49	19 Aug 2022 15:21:02	00:00:14	70010	70002	Incoming	
▶	19 Aug 2022 15:09:25	19 Aug 2022 15:10:30	00:01:06	70010	70002	Outgoing	
	19 Aug 2022 15:08:46	19 Aug 2022 15:09:18	00:00:33	70010	70002	Incoming	
	19 Aug 2022 15:08:11	19 Aug 2022 15:08:38	00:00:27	70010	70002	Incoming	

Media Player

19 Aug 2022 15:09:25 00:00:08 15:09:33 19 Aug 2022 15:10:30

Call Export: High Quality Audio Use replay settings Full Call WAV

10. Conclusion

These Application Notes describe the configuration steps required for Red Box Quantify 6C to successfully interoperate with Avaya Aura® Contact Center 7.1.2 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**.

11. 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 RedBox products may be found at <https://www.redboxvoice.com/>

©2024 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.