



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

---

# **Application Notes for configuring dvsAnalytics Encore Version 2.3.5 using Digital Tap and Avaya Aura® Contact Center 6.3, Avaya Aura® Application Enablement Service 6.3, Avaya Aura® Session Manager 6.3 and Avaya Aura® Communication Manager 6.3 – Issue 1.0**

### **Abstract**

These Application Notes describe the procedures for configuring dvsAnalytics Encore Version 2.3.5 using Station-side TDM and Avaya Aura® Contact Center 6.3, Avaya Aura® Application Enablement Services 6.3, Avaya Aura® Session Manager 6.3 and Avaya Aura® Communication Manager 6.3. The overall objective of the interoperability compliance testing is to verify calls made from/to a Contact Center agent with Avaya Digital Deskphone can be recorded by dvsAnalytics Encore application.

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

# 1. Introduction

The purpose of the document is to provide the detailed configuration and notes for the compliance test between dvsAnalytics Encore application using Station-side TDM and Avaya Aura® Contact Center (Contact Center), Avaya Aura® Application Enablement Services 6.3 (Application Enablement Services), Avaya Aura® Session Manager 6.3 (Session Manager) and Avaya Aura® Communication Manager 6.3 (Communication Manager) applications. The Avaya Aura® Contact Center system used for the compliance test was a co-resident system that includes Contact Center Manager Server (CCMS), Contact Center Administration Manager, Communication Control Toolkit (CCT) and Media Application Server (MAS). dvsAnalytics Encore (Encore) is a call recording application.

The Station-side TDM method uses a passive tap on the phones connected to Communication Manager to collect audio. These may be analog or digital phone sets. This passive tap is connected to the recording boards in the Encore server. The Application Enablement Services monitors events on Communication Manager and forwards the events to the Application Enablement Services Telephony Server Application Programming Interface (TSAPI) client installed on the Encore server. Based on events received from TSAPI, the Encore server starts and stops recording, collects the audio on the recording boards, and collects the data associated with the call. The CCT Web Services is used by dvsAnalytics Encore to obtain information such as Agent ID, Agent Name, Control Directory Number (CDN) and Skill Set associated with the agent being recorded.

## 2. General Test Approach and Test Results

The compliance test was performed both automatically and manually. The Application Enablement Services monitors events on Communication Manager and forwards the events to the Application Enablement Services TSAPI client installed on the Encore server. Based on events received from TSAPI, the Encore server starts and stops recording, collects the audio on the recording boards, and collects the data associated with the call. The CCT Web Services provides the Agent ID, Name, CDN and Skill Set associated with the recorded call.

For the manual part of the testing, each call was handled manually on the agent with generation of unique audio content for the recordings. Necessary user actions such as hold and un-hold, transfer, conference and forward 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 Encore and stop and start Contact Center bridge services on the Encore server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute a full product performance or feature testing performed by

third party vendors, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a third party solution.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Use of TSAPI calls control services to send events to the Encore server.
- Use of the AudioCodes card to capture audio for digital agent phone.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, abandon, hold and un-hold, ACD, non-ACD, hold, reconnect, simultaneous, conference, forward and transfer.
- Serviceability.

## 2.2. Test Results

All executed test cases passed.

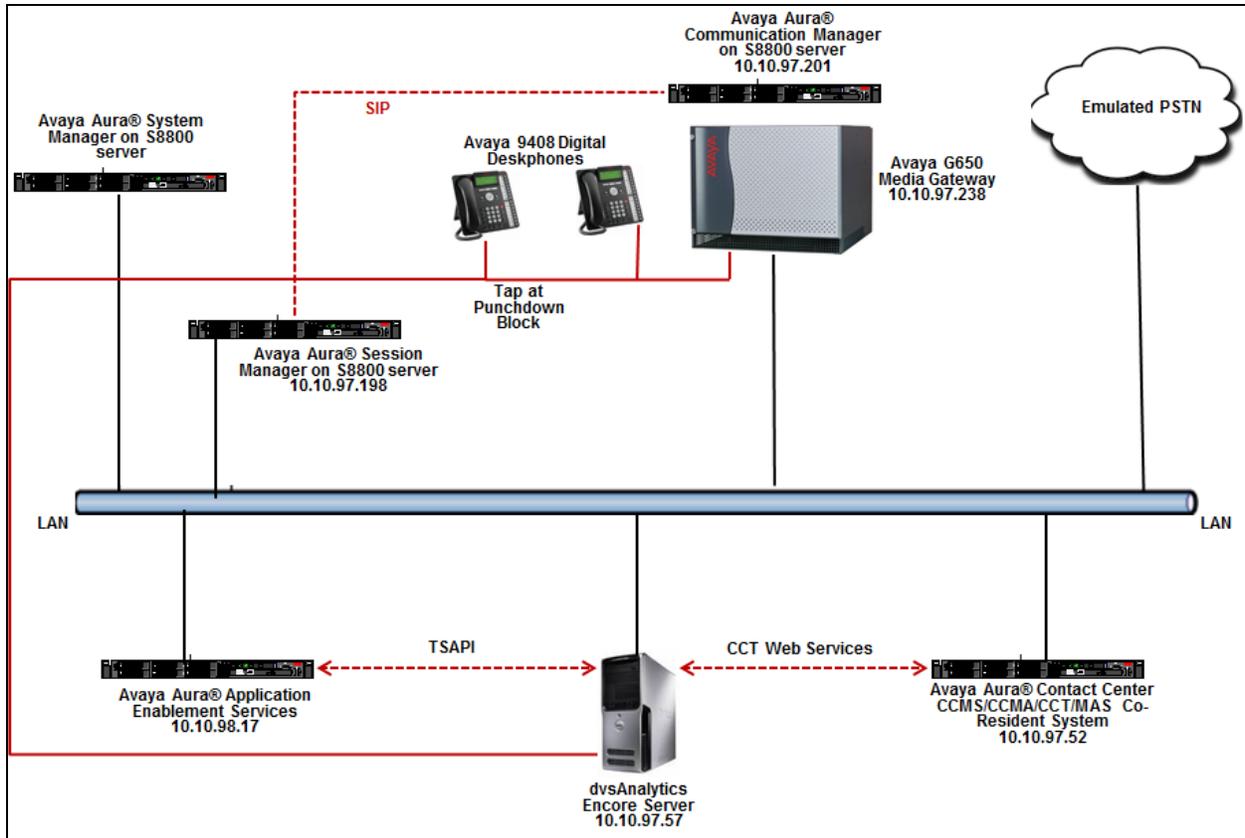
## 2.3. Support

Technical support on dvsAnalytics products can be obtained through the following:

- **Phone:** 800.910.4564
- **Web:** <http://www.dvsanalytics.com/contact.php>
- **Email:** Support@dvsAnalytics.com

### 3. Reference Configuration

**Figure 1** illustrates a configuration consisting of Communication Manager with G650 Media Gateway, Session Manager, System Manager, Application Enablement Services server, Contact Center Co-res system, and Encore server. Assumption is made here that all required configuration between Communication Manager, Session Manager, Application Enablement Services and Contact Center are in place and will not be discussed in this document.



**Figure 1: Tested Configuration Diagram**

## 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 running on S8800 Server with an Avaya G650 Media Gateway	6.3
Avaya Aura® System Manager running on S8800 Server	6.3
Avaya Aura® Session Manager running on S8800 Server	6.3
Avaya Aura® Application Enablement Services running on S8800 Server	6.3
Avaya Aura® Contact Center running on S8800 Server	6.3
Operating System of Avaya Aura® Contact Center server	Windows 64-bit 2008 Standard R2 Service Pack 1
Avaya 9408 Digital Deskphones	NA
dvsAnalytics Encore server	Version 2.3.5
Operating System of Encore server	Windows 64-bit 2008 R2 Standard Service Pack 1
<ul style="list-style-type: none"><li>• Encore Web Interface</li><li>• Avaya TSAPI Windows Client (csta32.dll)</li><li>• Avaya Open Interfaces CCT SDK</li><li>• AudioCodes card</li></ul>	3.0.8.5685 6.1.1.469 6.2 Version 3.0.8.5685

## 5. Configure Avaya Aura® Communication Manager

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

- Administer system parameters features
- Administer CTI link
- Administer agent stations

These steps are performed from the Communication Manager System Access Terminal (SAT) interface.

## 5.1. Administer System Parameters Features

Use the command “change system-parameters features” 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 Encore.

```
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? n
  Call Classification After Answer Supervision? n
                        Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
```

## 5.2. Administer CTI Link

To add a CTI link, use the “add cti-link n” command (not shown), 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: 50001
Type: ADJ-IP
Name: AES62
                                                COR: 1
```

## 5.3. Administer Agent Stations

During the compliance test, digital stations “53040” and “53041” were configured and used as the Contact Center agents with the following requirements.

- A maximum of two Call Appearance lines per agent station.

Issue “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** Enter station type that is being added.
- **Name:** A descriptive name.
- **Port:** The port is physical location of the digital line card that is installed on the G650 media gateway.

```
add station 53040                                 Page 1 of 5
                                                STATION
Extension: 53040                                Lock Messages? n      BCC: 0
Type: 9408                                       Security Code:         TN: 1
Port: 01A0501                               Coverage Path 1:      COR: 1
Name: DCP 53040                              Coverage Path 2:      COS: 1
                                                Hunt-to Station:
STATION OPTIONS
Loss Group: 2                                Time of Day Lock Table:
Data Option: none                            Personalized Ringing Pattern: 1
Speakerphone: 2-way                          Message Lamp Ext: 53040
Display Language: english                    Mute Button Enabled? y
                                                Expansion Module? n
Survivable COR: internal                      Media Complex Ext:
Survivable Trunk Dest? y                     IP SoftPhone? n
                                                Remote Office Phone? n
                                                IP Video Softphone? n
Short/Prefixed Registration Allowed: default
                                                Customizable Labels? y
```

Navigate to **Page 4**, and only assign two “call-appr” buttons.

```
display station 53040                                     Page 4 of 5
                                                         STATION
SITE DATA
  Room:                                         Headset? y
  Jack:                                         Speaker? n
  Cable:                                       Mounting: d
  Floor:                                       Cord Length: 0
  Building:                                    Set Color:

ABBREVIATED DIALING
  List1:                                       List2:                                       List3:

BUTTON ASSIGNMENTS
  1: call-appr                               5: manual-in                               Grp:
  2: call-appr                               6: auto-in                                 Grp:
  3:                                           7: after-call                             Grp:
  4: aux-work   RC:   Grp:                   8: release

  voice-mail
```

Repeat the same procedure to create another digital station “53041”.

## 6. Configure Avaya Aura® Application Enablement Services

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

- Verify Application Enablement Services License.
- Administer TSAPI link.
- Administer Tlink.
- Administer CTI User.
- Administer Security

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.

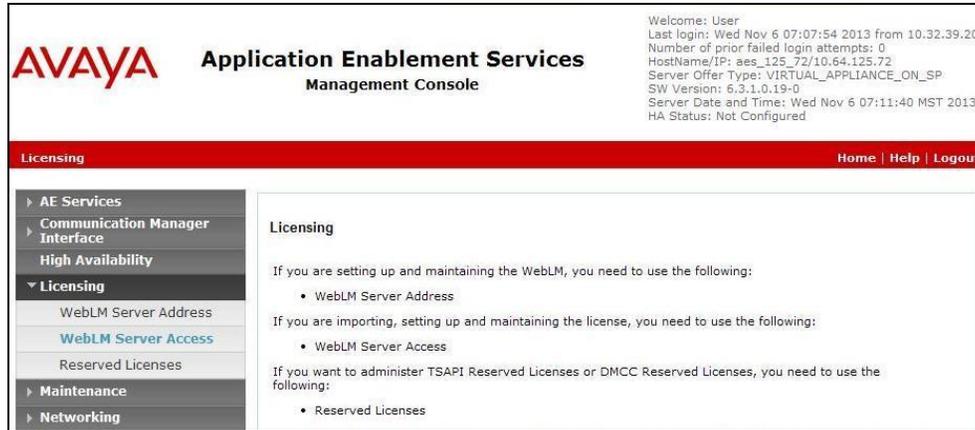
The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. The title is "Application Enablement Services Management Console". A red navigation bar at the top right contains a "Help" link. The main content area features a "Please login here:" prompt with two input fields for "Username" and "Password", and a "Login" button below them. At the bottom, there is a copyright notice: "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console "Welcome to OAM" page. At the top left is the Avaya logo. The title is "Application Enablement Services Management Console". In the top right corner, there is a welcome message for user "admin" and system information: "Welcome: User admin", "Last login: Tue Dec 3 10:40:00 2013 from 10.10.98.71", "Number of prior failed login attempts: 3", "HostName/IP: AES63/10.10.98.17", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP", "SW Version: 6.3.0.0.212-0", and "Server Date and Time: Fri Feb 14 11:37:33 EST 2014". A red navigation bar at the top right contains "Home | Help | Logout" links. On the left side, there is a vertical menu with expandable items: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains a list of administrative domains and their descriptions: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:", "• AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.", "• Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.", "• Licensing - Use Licensing to manage the license server.", "• Maintenance - Use Maintenance to manage the routine maintenance tasks.", "• Networking - Use Networking to manage the network interfaces and ports.", "• Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.", "• Status - Use Status to obtain server status informations.", "• Utilities - Use Utilities to carry out basic connectivity tests.", "• Help - Use Help to obtain a few tips for using the OAM Help system." Below this 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, there is a copyright notice: "Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

## 6.1. Verify Application Enablement Services 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 **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** as shown below. Note that the TSAPI license is used for device monitoring.

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)			
WebLM Home	Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)		
Install license	You are here: Licensed Products > Application_Enablement > View License Capacity		
Licensed products	License installed on: June 10, 2013 4:44:13 PM -05:00		
APPL_ENAB	License File Host IDs: E4-1F-13-66-48-08		
Application_Enablement	Licensed Features		
View license capacity			
View peak usage			
Uninstall license			
Server properties			
Manage users			
Shortcuts			
Help for Installed Product			
Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASA1 (VALUE_AES_CVLAN_ASA1)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	1
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent		Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0
DLG (VALUE_AES_DLG)	permanent	16	0

If the TSAPI service is not licensed, contact the Avaya sales team or business partner for a proper license file.

## 6.2. Administer TSAPI Link

From the Management console, navigate to **AE Services** → **TSAPI** → **TSAPI Links**. The **TSAPI Links** page is displayed in the right (screen not shown), click **Add Link**. Enter the following highlighted values to add the CTI link:

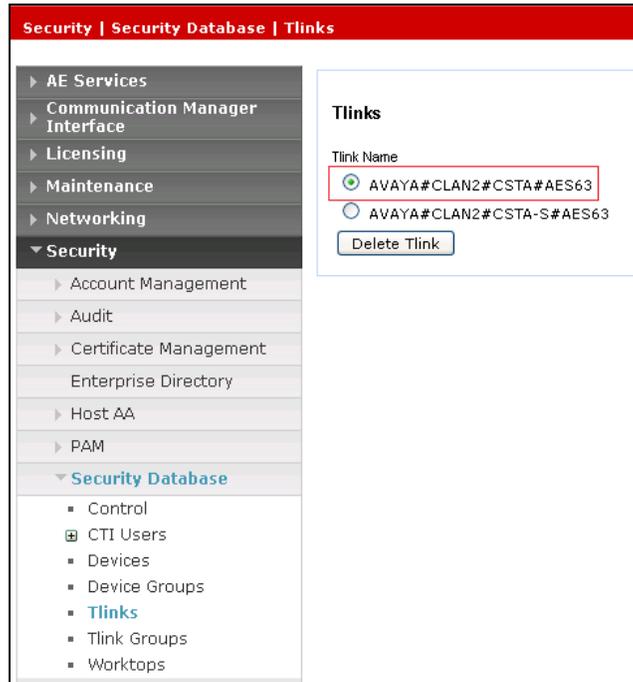
- **Link:** From the drop down menu, select any available link number.
- **Switch Connection:** Select the relevant switch connection from the drop-down list. In this case, the switch connection “CLAN2” is selected **Switch CTI Link Number:** Select the CTI link number from **Section 5.2**.
- **ASAI Link Version:** Select “4” from the drop down menu.
- **Security:** Select “Both” from drop down menu.

Click on **Apply Changes** when finished.

The screenshot shows the 'Edit TSAPI Links' configuration page. The left sidebar contains a navigation menu with the following items: AE Services (expanded), CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, TWS, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, Utilities, and Help. The main content area is titled 'Edit TSAPI Links' and contains a form with the following fields: Link (value: 1), Switch Connection (value: CLAN2), Switch CTI Link Number (value: 1), ASAI Link Version (value: 4), and Security (value: Both). Below the form are three buttons: Apply Changes, Cancel Changes, and Advanced Settings.

### 6.3. Administer Tlink

From the Management Console, navigate to **Security** → **Security Database** → **Tlinks**. The **Tlinks** page is displayed on the right with two Tlinks as shown below. The unsecured Tlink “**AVAYA#CLAN2#CSTA#AES63**” will be used to configure the Encore application in **Section 8.2**.



## 6.4. Administer CTI User

From the Management Console, navigate to **User Management** → **User Admin** → **Add User**. The **Add User** page is displayed on the right (not shown). Enter desired values for **User Id**, e.g. “test”, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields. Click on the **Apply** button to complete (not shown). This user will be used to configure for the Encore application in **Section 8.3**.

**User Management | User Admin | List All Users**

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ 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

### Edit User

* User Id	<input type="text" value="test"/>
* Common Name	<input type="text" value="test"/>
* Surname	<input type="text" value="test"/>
User Password	<input type="text"/>
Confirm Password	<input type="text"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Cms Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>

## 6.5. Administer Security

From the Management Console, navigate to expand **Security** → **Security Database** → **Control**. The **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** page is displayed on the right. Make sure **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** boxes are unchecked. Click **Apply Changes** button to complete.

The screenshot displays the Management Console interface. At the top, a red navigation bar contains the text "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. A vertical sidebar on the left shows a tree view of system components, with "Security Database" expanded to show "Control". 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". A red box highlights the second checkbox. Below the checkboxes is an "Apply Changes" button.

DMCC and TSAPI services need to be restarted for the changes take effect. Navigate to **Maintenance** → **Service Controller**. Check on the **TSAPI Service** and click **Restart Service** button to restart the service.

The screenshot shows a web interface for the Service Controller. On the left is a navigation menu with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Security Database, Service Controller, Server Data, Networking, Security, Status, Utilities, and Help. The 'Maintenance' section is expanded, and 'Service Controller' is selected. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, all with a status of 'Running'. The 'TSAPI Service' row is highlighted with a red border, and its checkbox is checked. Below the table, there is a link for 'Status and Control' and a row of buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

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

## 7. Configure Avaya Aura® Contact Center

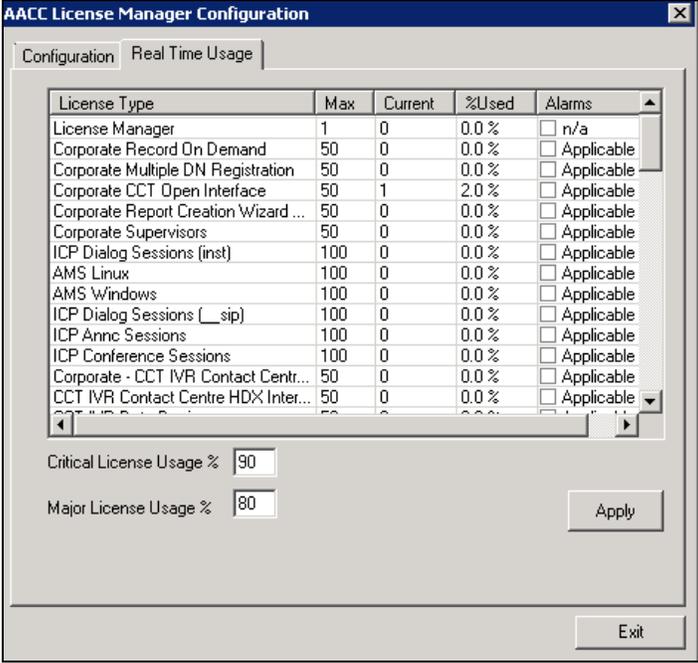
This section provides steps on how to configure Contact Center. This section assumes that Contact Center system is already installed and operational; the section provides steps for configuring the following configurations:

- Verify Contact Center License.
- Configure Windows users.
- Configure CCT Server.

In the compliance test, the Contact Center system used is a co-res system which consists of Contact Center Manager Server, Contact Center Manager Administrator, Contact Center Communication Control Toolkit, Contact Center License Manager, and Media Server Application (MAS).

### 7.1. Verify Contact Center License

From server where the License Manager is installed, navigate to menu **Start → All Programs → Avaya → Contact Center → License Manger → Configuration**. The **AACC License Manager Configuration** window is displayed, make sure there is CCT and ICP presented in the table as below.



The screenshot shows the 'AACC License Manager Configuration' window with the 'Configuration' tab selected. It contains a table with the following data:

License Type	Max	Current	%Used	Alarms
License Manager	1	0	0.0 %	<input type="checkbox"/> n/a
Corporate Record On Demand	50	0	0.0 %	<input type="checkbox"/> Applicable
Corporate Multiple DN Registration	50	0	0.0 %	<input type="checkbox"/> Applicable
Corporate CCT Open Interface	50	1	2.0 %	<input type="checkbox"/> Applicable
Corporate Report Creation Wizard ...	50	0	0.0 %	<input type="checkbox"/> Applicable
Corporate Supervisors	50	0	0.0 %	<input type="checkbox"/> Applicable
ICP Dialog Sessions (inst)	100	0	0.0 %	<input type="checkbox"/> Applicable
AMS Linux	100	0	0.0 %	<input type="checkbox"/> Applicable
AMS Windows	100	0	0.0 %	<input type="checkbox"/> Applicable
ICP Dialog Sessions (_sip)	100	0	0.0 %	<input type="checkbox"/> Applicable
ICP Annc Sessions	100	0	0.0 %	<input type="checkbox"/> Applicable
ICP Conference Sessions	100	0	0.0 %	<input type="checkbox"/> Applicable
Corporate - CCT IVR Contact Centr...	50	0	0.0 %	<input type="checkbox"/> Applicable
CCT IVR Contact Centre HDX Inter...	50	0	0.0 %	<input type="checkbox"/> Applicable

Below the table, there are two input fields: 'Critical License Usage %' set to 90 and 'Major License Usage %' set to 80. There are 'Apply' and 'Exit' buttons at the bottom right of the window.

## 7.2. Configure Windows Users

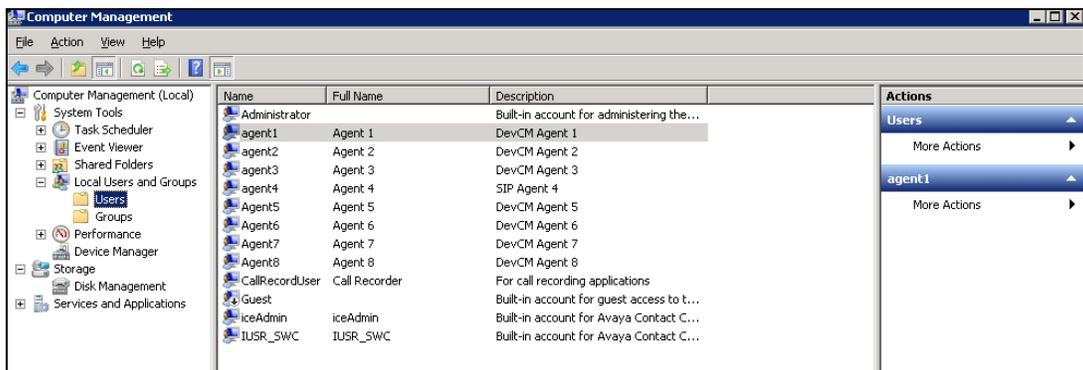
In the compliance test, the Contact Center CCT server is not joined to a Windows domain; therefore, the Windows user used for CCT user login will be created in the local CCT server. In case the CCT server joins a domain, the Windows user needs to be created in the domain controller.

From the Contact Center CCT server, navigate to menu **Start** → **Administrative Tools** → **Computer Management**. The **Computer Management** window is displayed. Right click on **Users** (not shown) folder under **Local Users and Groups** and then select **New**. The **New User** window is displayed; enter information for user as shown below. Click **Create** button to complete.

The 'New User' dialog box contains the following information:

- User name: agent1
- Full name: Agent 1
- Description: DevCM Agent 1
- Password: [masked]
- Confirm password: [masked]
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

The screen below shows the **Computer Management** window with a Windows user created as **agent1**. Similarly more users can be created as required.

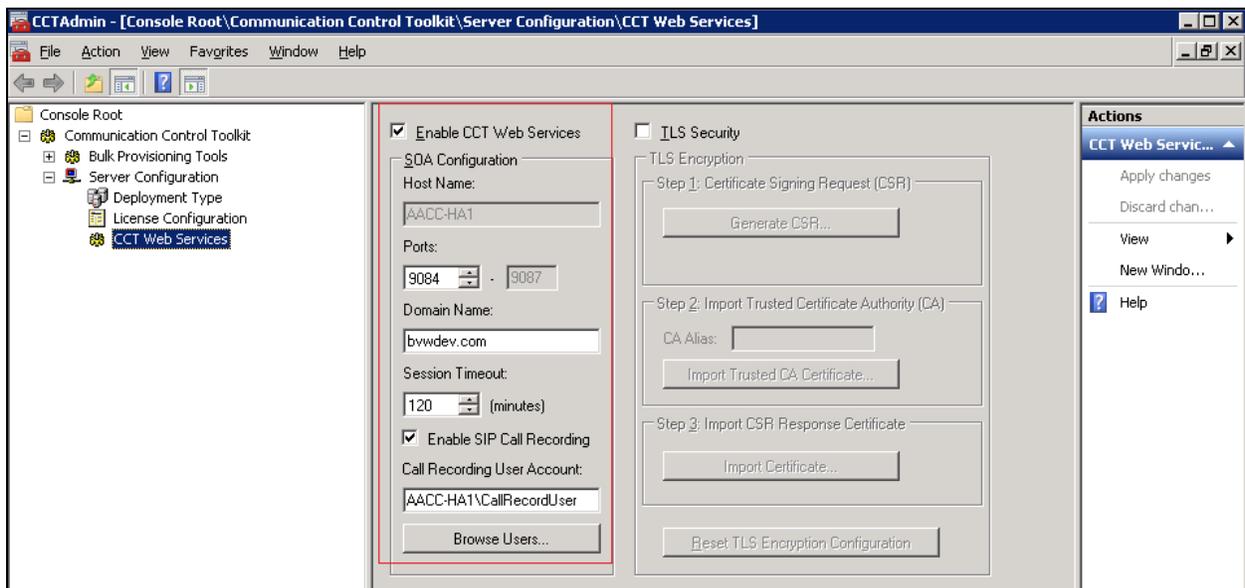


Repeat the same procedure to create “CallRecordUser” that is used for configuring in the CCT Web services for the Encore application.

### 7.3. Configure CCT Web Services

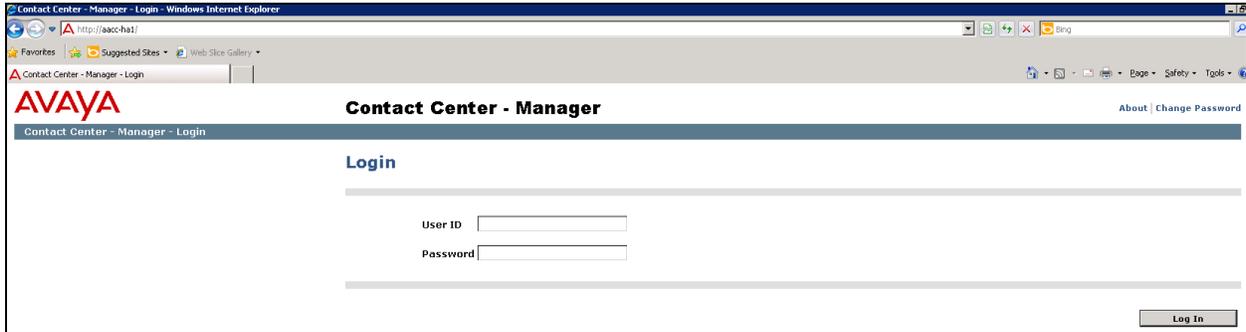
From the Contact Center server, navigate to menu **Start → All Programs → Avaya → Contact Center → Communication Control Toolkit → CCT Console**. The **CCT Admin** window is displayed. In the left navigation pane, select **CCT Web Services** under **Server Configuration**. In the middle pane, enter the following highlighted fields:

- **Enable CCT Web Services:** Select the box.
- **Ports:** Set to “9084”. Note that the **CCT Web Services** range port has to be different than SOA Web Services ports in **WS Open Interface** in the **Server Configuration** of CCMS.
- **Domain Name:** Enter “bvwdev.com”.
- **Enable SIP Call Recording:** Select the box.
- **Call Recording User Account:** Enter the “AACC-HA1\CallRecordUser” as created in **Section 7.2**.
- **TLS Security:** Not used and therefore not selected.



Use **System Control and Monitor Utility** tool to restart CCT services for changes above to take effect (not shown).

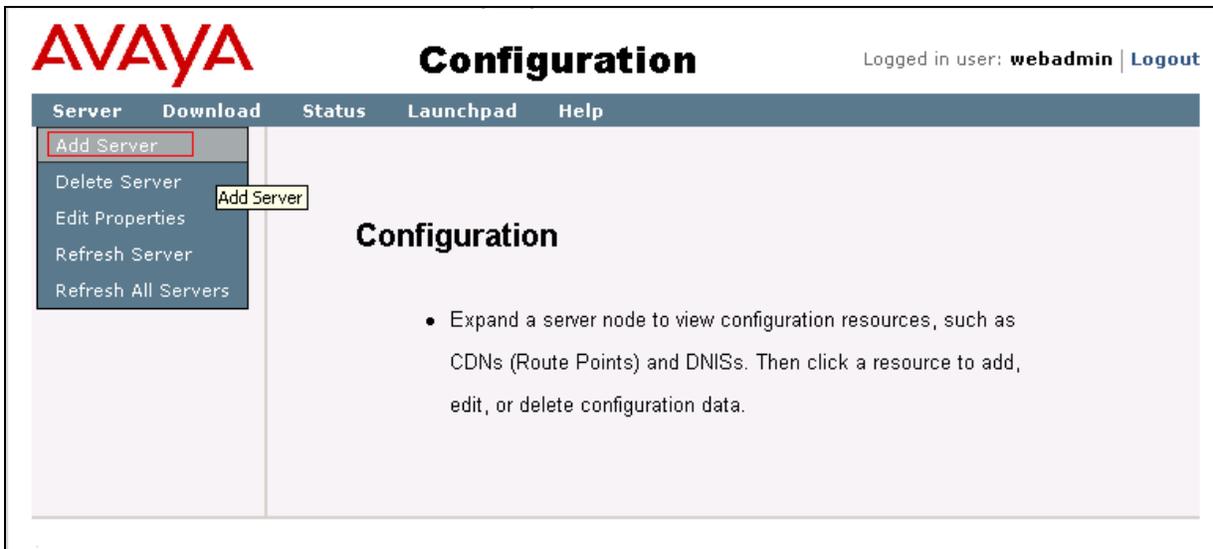
In order to access CCT Administration web page, the CCT server needs to be added into Contact Center Manager Administer (CCMA). Launch CCMA web page, by entering IP address or hostname of CCMA into the address box of a browser as shown below. Note that the IP address of CCMA needs to be added into the **Trusted** sites under **Security** tab of **Internet Options**. Enter the appropriate credentials to access the CCMA webpage.



From the **Launchpad** window in the CCMA web page, select **Configuration**.



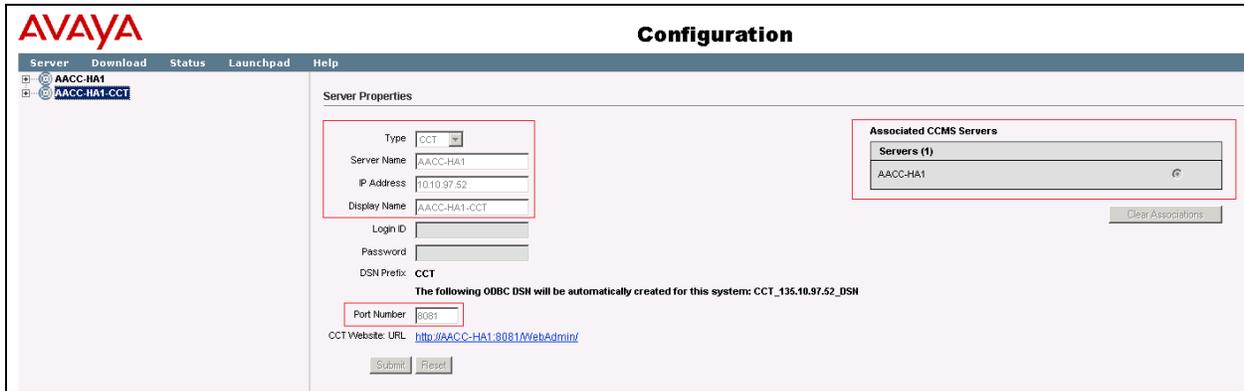
From the **Configuration** page, select **Server** → **Add Server**.



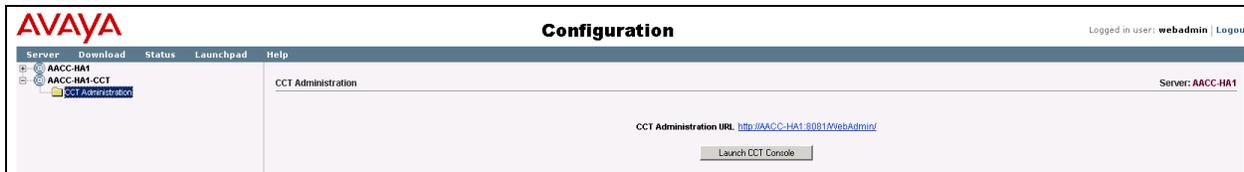
The **Server Properties** window is displayed in the right pane. Enter the following highlighted fields below.

- **Type:** Select “CCT” in the drop down menu.
- **Server Name:** Enter name of CCT server, e.g. “AACC-HA1”.
- **IP Address:** Enter IP address of CCT server, e.g. “10.10.97.52”.
- **Associated CCMS Servers:** Check the radio button of present CCMS.
- **Port Number:** “8081”.

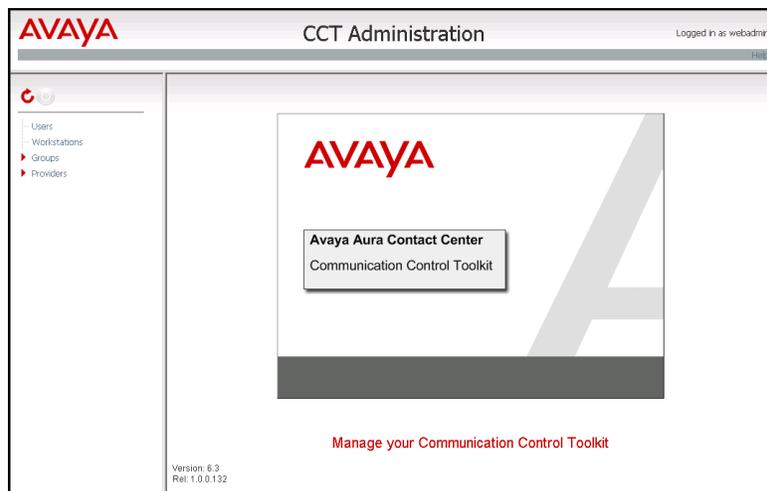
Click **Submit** button to add the CCT Server.



The screen below shows the newly added CCT server.



Click **Launch CCT Console** as seen in the screen above to launch the CCT Administration web-based console, the CCT Administration console is displayed as shown below.



In the left navigation pane, right click on **Users** and **Add new user** (not shown) to add “CallRecordUser” as shown in the screen below. This is the same user configured in **Section 7.2**.

The screenshot shows the AVAYA CCT Administration interface. The top header includes the AVAYA logo, the title "CCT Administration", and the user "Logged in as webadmin". The left navigation pane has "Users" selected. The main content area is titled "Update CCT User" and contains several sections: "User Details" (with fields for Login User Name: AACC-HA1\CallRecordUser, First Name: Call, and Last Name: Recorder), "Address Assignments", "Terminal Assignments", "Terminal Group Assignments", "Address Group Assignments", and "Agent Assignments". A "Save" button is located at the bottom left of the main content area.

In the left navigation pane, expand **Providers** and select **Passive**. The **Update CCT Provider** page is displayed in the right pane, enter the following highlighted fields as shown below and click the **Save** button to save changes.

The screenshot shows the AVAYA CCT Administration interface. The top header includes the AVAYA logo, the title "CCT Administration", and the user "Logged in as webadmin". The left navigation pane has "Providers" > "Passive" selected. The main content area is titled "Update CCT Provider" and contains several sections: "Basic Provider Information" (with fields for Provider Name: Passive, IP Address: 10.10.97.52, and Port: 5060), "Provider Type" (SIP Contact Center), and "Provider Configuration" (with a dropdown for Transport set to TCP). A "Save" button is located at the bottom left of the main content area.

## 8. Configure dvsAnalytics Encore

This document assumes that the Encore system is already installed and configured by dvsAnalytics engineer. This section provides the following steps to configure the Encore system.

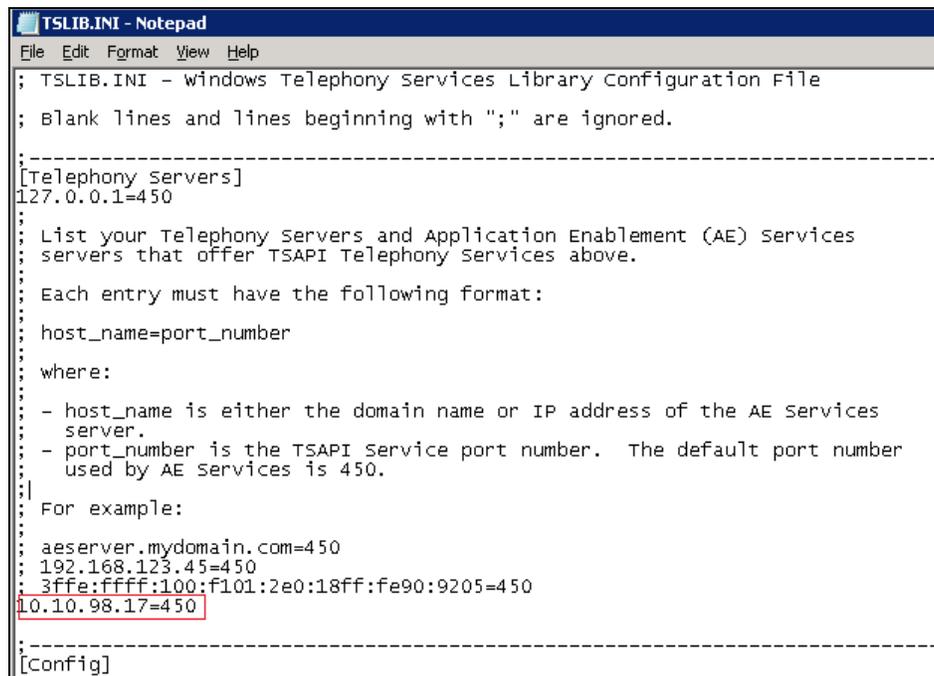
The Encore system integrates with the Avaya system. This integration allows the Encore system to successfully perform the following functions:

- Audio Collection – Capture the audio that needs to be recorded.
- Recording Control – Receive the necessary events that signal when Encore must start and stop recording.
- Data Capture – Receive data associated with the call

### 8.1. Configure the AES TSAPI Client

From Encore server navigate to **Program files\Avaya\AE Services\TSAPI Client**, or using the shortcut **Start → Programs → Avaya AE Services → TSAPI Client**, right-click on the file **TSLIB.INI** and select **Open with Notepad** to edit this file.

In the **Telephony Servers** section, enter the IP address/host name and port number of the Application Enablement Service server where the TSAPI Service is running. In the screen below the IP address is “10.10.98.17” and the port number is “450”, so the entry is shown as “10.10.98.17=450”. Retain default values for other fields. Save the file when finished.

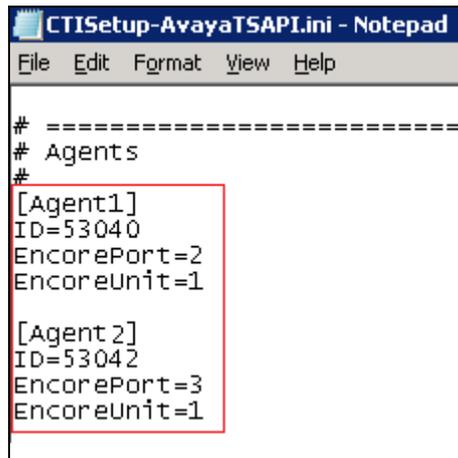


```
TSLIB.INI - Notepad
File Edit Format View Help
; TSLIB.INI - windows Telephony Services Library Configuration File
; Blank lines and lines beginning with ";" are ignored.
-----
[Telephony servers]
127.0.0.1=450
;
; List your Telephony Servers and Application Enablement (AE) Services
; servers that offer TSAPI Telephony Services above.
;
; Each entry must have the following format:
;
; host_name=port_number
;
; where:
;
; - host_name is either the domain name or IP address of the AE Services
;   server.
; - port_number is the TSAPI Service port number. The default port number
;   used by AE Services is 450.
;
; For example:
;
; aeserver.mydomain.com=450
; 192.168.123.45=450
; 3ffe:ffff:100:f101:2e0:18ff:fe90:9205=450
10.10.98.17=450
-----
[Config]
```

## 8.2. Configure CT Gateway for TSAPI

From the Encore server, navigate to **D: \EncData\Config\CTGateway**. Copy and rename the default **ctisetaup.ini** file to **CTIsetup-AvayaTSAPI.ini**. Double click on this file. Locate the following lines in the INI file and verify the values match the example below:

Scroll to the **Agents** section. Under **Agent1**, set **ID** to the first agent station extension from **Section 5.3. EncorePort** is set to a unique value for each agent that corresponds to the physical port where the passive tap for this extension is terminated. **EncoreUnit** is set to the value of the Recording Unit used for passive recording. During compliance testing it was set to "1". Create additional agent parameter lines as necessary when more than one agent is being monitored.

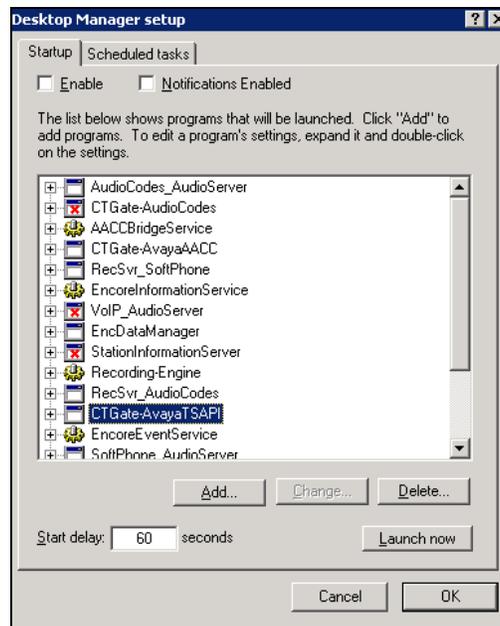


```
CTIsetup-AvayaTSAPI.ini - Notepad
File Edit Format View Help

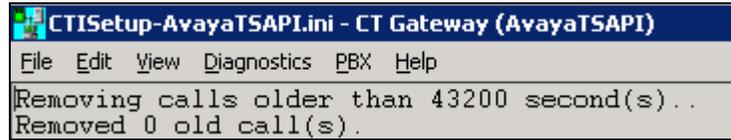
# =====
# Agents
#
[Agent1]
ID=53040
EncorePort=2
EncoreUnit=1

[Agent2]
ID=53042
EncorePort=3
EncoreUnit=1
```

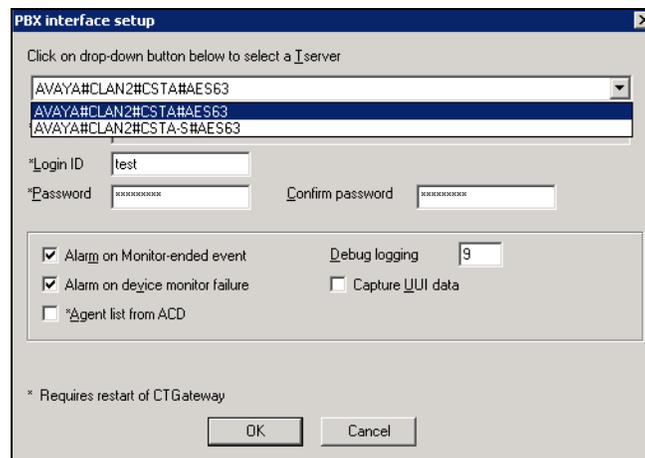
Use the **Desktop Manager setup** tool to launch CT Gateway for AvayaTSAPI. Right-click on the **Desktop Manager** icon in the system tray, select **Configuration** (screen not shown). The **Desktop Manager setup** window is displayed.



Click **Launch Now** to launch **CT Gateways**. The **CTISetup-AvayaTSAPI.ini-CTI Gateway (AvayaTSAPI)** window is displayed as seen below.



From the above screen, continue to navigate to **PBX → Configuration** (not shown). The **PBX interface setup** window is displayed. Select the Tlink **AVAYA#CLAN2#CSTA#AES63** as configured in **Section 6.3** in the dropdown menu. Enter “test” in the **Login ID** box and its password in the **Password** and **Confirm Password** boxes. The ID “test” is configured in **Section 6.4**. Click **OK** button to complete and shut down the **CTGate-AvayaTSAPI**.

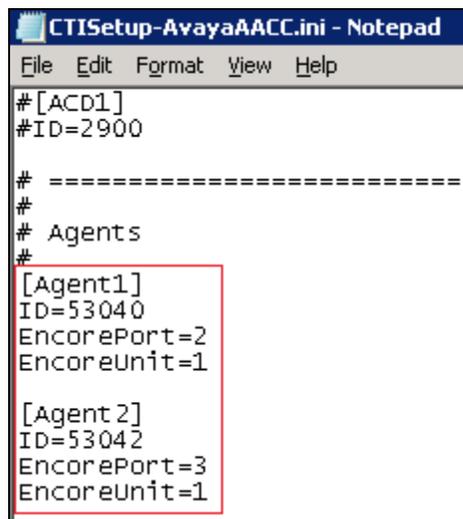


Use the **Desktop Manager Setup** application to launch the **CTGate-AvayaTSAPI** application again.

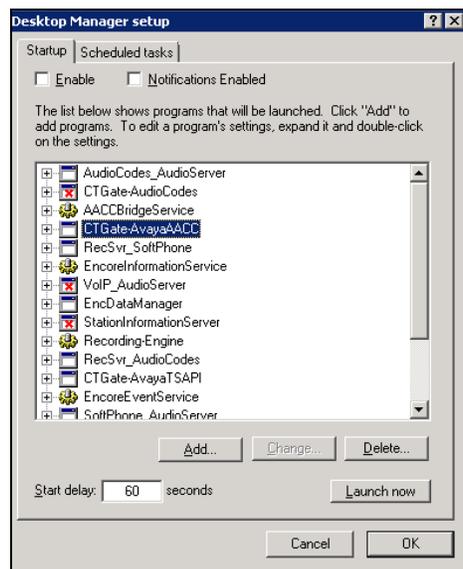
### 8.3. Configure CT Gateway for Contact Center Data Collection

From the Encore server navigate to \EncData\Config\CTGateway. Copy and rename the default **ctisetup.ini** file to **CTISetup-AvayaAACC.ini**. If no **ctisetup.ini** exists, find the default file in the **SampleINI** folder. Double-click on the **CTISetup-AvayaAACC.ini** file to edit. Locate the following lines in the INI file and verify the values match the example below.

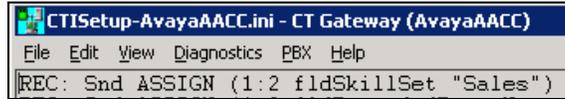
In the **Agents** section, set **ID** to the first agent station extension from **Section 5.3**. Set **EncorePort** to a unique value per agent that corresponds to the physical port where the passive tap for this extension is terminated. **EncoreUnit** is set to the value of the Recording Unit used for passive recording. During compliance testing it was set to "1". Create additional agent parameter lines as necessary when more than one agent is being monitored.



Use the **Desktop Manager Setup** tool to launch the **CTGate-AvayaAACC** application.



The **CTISetup-AvayaAACC.ini-CT Gateway (AvayaAACC)** window is displayed as seen below.



From the above screen, continue to navigate to **PBX → Configuration** (not shown). The **PBX interface setup** window is displayed. Enter the values as highlighted in the screen below.

**AACC Communication Control ToolKit (CCT) Web services section:**

- **CCT Server name/IP address:** Enter IP address of CCT server “10.10.97.52”
- **CCT web services port:** “9084” as configured in **Section 7.3**
- **AACC SIP Domain:** “bvwdev.com” as configured in **Section 7.3.**
- **CCT web service user ID:** “AACC-HA1\CallRecordUser” as configured in **Section 7.2.**
- **CCT web service user password:** The password that was configured in **Section 7.2.**
- **Confirm CCT web service user password:** Same as above.

**AACC Contact Center Manager Administrator (CCMA) web services section.**

- **CCMA Server name / IP Address:** Enter the IP address of CCMA server which is “10.10.97.52”.
- **CCMA web service user ID:** Enter the appropriate user ID to login to CCMA
- **CCMA web service user password:** Enter the password valid for the above user.
- **Confirm CCMA web service user password:** Same as above.

Retain default values for other fields in this section.

**Encore AACC Bridge Windows service section.**

- **Server name / IP address:** Enter the IP address of Encore server “10.10.97.57” that was used during cmlpace testing.

Retain default values for other fields in this section.

**PBX interface setup** [?] [X]

**AACC Communication Control ToolKit (CCT) Web services**

\*CCT Server name / IP address: 10.10.97.52

\*CCT web services port: 9084

\*AACC SIP Domain: bvwdev.com

\*CCT web service user ID: AACC-HA1\CallRecordUse

\*CCT web service user password: \*\*\*\*\*

Confirm CCT web service user password: \*\*\*\*\*

---

**AACC Contact Center Manager Administration (CCMA) web services**

\*CCMA Server name / IP address: 10.10.97.52

\*CCMA web services port: 80

\*CCMA web service user ID: [REDACTED]

\*CCMA web service user password: \*\*\*\*\*

Confirm CCMA web service user password: \*\*\*\*\*

---

**Encore AACC Bridge Windows service**

\*Server name / IP address: 10.10.97.57

CT Gateway connects to this IP Port: 1566

AACC connects to one of these IP Ports (2702 - 2706): 2705

---

\*Delay events by 500 ms

Debug logging level: 0 [Add memo to log file...]

\* Requires restart of CTGateway

OK Cancel

Click **OK** button to complete and shut down the **CTGate-AvayaAACC**. Use the **Desktop Manager Setup** application to launch the **CTGateway** for the **CTGate-AvayaAACC** application again.

## 9. Verification Steps

The following are typical steps to verify the integration between Encore application and Contact Center, Application Enablement Services, Session Manager and Communication Manager.

- Check status of the AudioCodes Recording at the Encore server. Screen below shows the AudioCodes Recording Server in the process of a recording. Verify that the port is busy and the proper status of the recording is seen.

The screenshot displays two windows. The top window, titled "Audio Server Control Program", has a dropdown menu set to "AudioCodes" and three buttons: "Close Audio Server", "Make it Visible", and "Make it Invisible". The bottom window, titled "AudioCodes Recording Server : unit 1", contains a "Recording Ports" table, a connection log table, and a log viewer.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24

Connection Name	Connected	Connection Time	IP Address
RecEngine	Yes	11/25 15:02:31	127.0.0.1

Log: RecSvrAC\_25.txt Clear

```

11/29-10:04:01 Snd<RecEngine>: Stop Status: 1:2:1 Success
12/02-10:14:48 Rcv<RecEngine>: Start: 1:2:1 D:\EncData\0D\01Z1471D.vw8
12/02-10:14:48 Snd<RecEngine>: Start Status: 1:2:1 {MaxRecTime = 1800} Recording Started
12/02-10:14:55 Rcv<RecEngine>: Stop: 1:2:1
12/02-10:14:55 Snd<RecEngine>: Stop Status: 1:2:1 Success
12/02-10:16:08 Rcv<RecEngine>: Start: 1:1:1 D:\EncData\0E\01Z1471E.vw8
12/02-10:16:08 Snd<RecEngine>: Start Status: 1:1:1 {MaxRecTime = 1800} Recording Started
    
```

- To verify information and play back for the call recording above, from workstation PC with sound card and speaker equipped launch a browser and enter the link below: <http://10.10.97.57/Encore> in the browser where “10.10.97.57” is the IP address of the Encore server. The screen below shows the detailed information of the call recordings. Verify the call data of the recording call such as Agent Login ID, ACD number, Skillset, and Agent name... etc. Click **Play** button at the bottom to check the audio quality of the recorded call.

The screenshot displays the Encore application interface. The top navigation bar includes the Encore logo and a user profile for 'Welcome A Administrator | 12/3/2013'. The main area is divided into a left sidebar with a tree view of libraries and playlists, and a central table of call recordings. The table has columns for Date, Duration, Extension, ACD Number, ACD Name, Skillset, ANI, DNIS, Call Direction, Call Type, Consultation call, Agent Login ID, Other Party Name, Other Party Number, and Record. Below the table is a playback player for a selected recording, showing a waveform and playback controls. The player indicates 'Streaming Player: 012146YU.vx8' and 'Recording Length: 0:00:18.102'.

Date	Duration	Extension	ACD Number	ACD Name	Skillset	ANI	DNIS	Call Direction	Call Type	Consultation call	Agent Login ID	Other Party Name	Other Party Number	Record
11/28/2013 12:34:03 PM	00:00:15	53012				53012	53113	Outgoing	Internal	<input checked="" type="checkbox"/>			53113	H.323
11/28/2013 12:33:28 PM	00:00:21	53012	4002		Sales	4002	53012	Incoming	External	<input type="checkbox"/>	53012		4002	Agent
11/28/2013 9:40:42 AM	00:00:40	53012	4002		Sales	4002	53012	Incoming	External	<input type="checkbox"/>	53012		4002	Agent
11/28/2013 9:35:37 AM	00:00:16	53012	4002		Sales	4002	53012	Incoming	External	<input type="checkbox"/>	53012		4002	Agent
11/28/2013 9:26:44 AM	00:00:09	53012	4002		Sales	4002	53012	Incoming	External	<input type="checkbox"/>	53012		4002	Agent
11/28/2013 9:25:36 AM	00:00:10	53012				53113	53012	Incoming	Internal	<input type="checkbox"/>			53113	H.323
11/28/2013 9:24:56 AM	00:00:10	53012				53012	54008	Outgoing	External	<input type="checkbox"/>			54008	H.323
11/28/2013 9:24:19 AM	00:00:07	53012				53012	53113	Outgoing	Internal	<input type="checkbox"/>			53113	H.323
11/28/2013 9:19:50 AM	00:00:08	53012				53012	54008	Outgoing	External	<input type="checkbox"/>			54008	H.323
11/28/2013 9:16:56 AM	00:00:08	53012	4002		Sales	4002	53012	Incoming	External	<input type="checkbox"/>	53012		4002	Agent
11/27/2013 11:45:48 AM	00:00:09	53041				53113	53041	Incoming	Internal	<input type="checkbox"/>			53113	DCP 5
11/27/2013 11:42:21 AM	00:00:13	53041				53113	53041	Incoming	Internal	<input type="checkbox"/>			53113	DCP 5
11/27/2013 11:36:59 AM	00:00:11	53041				53041	53012	Outgoing	Internal	<input type="checkbox"/>		H.323, 53012	53012	DCP 5
11/27/2013 11:36:59 AM	00:00:11	53012				53041	53012	Incoming	Internal	<input type="checkbox"/>		DCP 53041	53041	H.323
11/27/2013 11:35:21 AM	00:00:12	53041				53113	53041	Incoming	Internal	<input type="checkbox"/>			53113	DCP 5
11/27/2013 9:16:20 AM	00:00:05	53012				4002	53012	Incoming	External	<input type="checkbox"/>			4002	H.323
11/27/2013 9:12:20 AM	00:00:07	53012				4002	53012	Incoming	External	<input type="checkbox"/>			4002	H.323

## 10. Conclusion

All test cases in the test plan were executed and passed. The dvsAnalytics Encore application Version 2.3.5 using Station-side TDM is considered to successfully integrate with Avaya Aura® Contact Center Release 6.3, Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3.

## 11. Additional References

The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, October 2013, Release 6.3 Document 03-300509 Issue 9.
- [2] *Administering Avaya Aura® Session Manager*, October 2013, Release 6.3, Document 03-603324.
- [3] *Administering Avaya Aura® System Manager*, October 2013, Release 6.3.
- [4] *Avaya Communication Installation and Commissioning*, Doc# NN43041-310, Issue 05.04, Date May 2011.
- [5] *Avaya Aura® Contact Center SIP Commissioning*, Doc# NN44400-511.
- [6] *Avaya Aura® Contact Center Configuration – Avaya Aura Unified Communications Platform Integration*, Doc# NN44400-521.
- [7] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 2, October 2013

The following product documentation is available on contacting dvsAnalytics.

- [1] *Avaya Aura™ Communication Manager TSAPI Integration Guide*, Release 2.3.5, November 18, 2013
- [2] *Avaya Aura™ Communication Manager TSAPI Installation Addendum*, Release 2.3.5, November 19, 2013

---

**©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).