



Avaya Solution & Interoperability Test Lab

Application Notes for configuring dvsAnalytics Encore Version 2.3.5 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 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 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 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.

In the compliance testing, dvsAnalytics Encore used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations on Communication Manager, and used the Service Observing feature via the Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with the monitored stations for call recording.

The TSAPI interface is used by dvsAnalytics Encore to monitor skill groups and agent stations on Communication Manager. The DMCC interface is used by dvsAnalytics Encore to register virtual IP softphones, and for adding softphones to active calls using the Service Observing method. 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.

When there is an active call at the monitored agent, dvsAnalytics Encore is informed of the call via event reports from the TSAPI interface. dvsAnalytics Encore starts the call recording by using the Service Observing feature from the DMCC interface to add a virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings. The CCT Web Services provides the Agent ID, Name, CDN and Skill Set associated with the recorded call.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Encore application, the application automatically requests monitoring on skill groups and agent stations, performs device queries using TSAPI, and registers the virtual IP softphones using DMCC. When there is an active call at the monitored agent, Encore interfaces with Contact Center CCT Web Services to receive CTI information such as Agent ID, Name, CDN and Skill Set.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and resume 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:

- Handling of TSAPI messages in areas of event notification and value queries.
- Use of DMCC registration services to register and un-register virtual IP softphones.
- Use of DMCC monitoring services and media control events to obtain the media from the virtual IP softphones.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, abandon, hold and resume, ACD, non-ACD, hold, reconnect, simultaneous, conference, forward and transfer.
- Serviceability

2.2. Test Results

All executed test cases passed with the following observation,

- The number of softphones to configure need to take into account the small interval of 500ms that a softphone will not be available between recordings.

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.

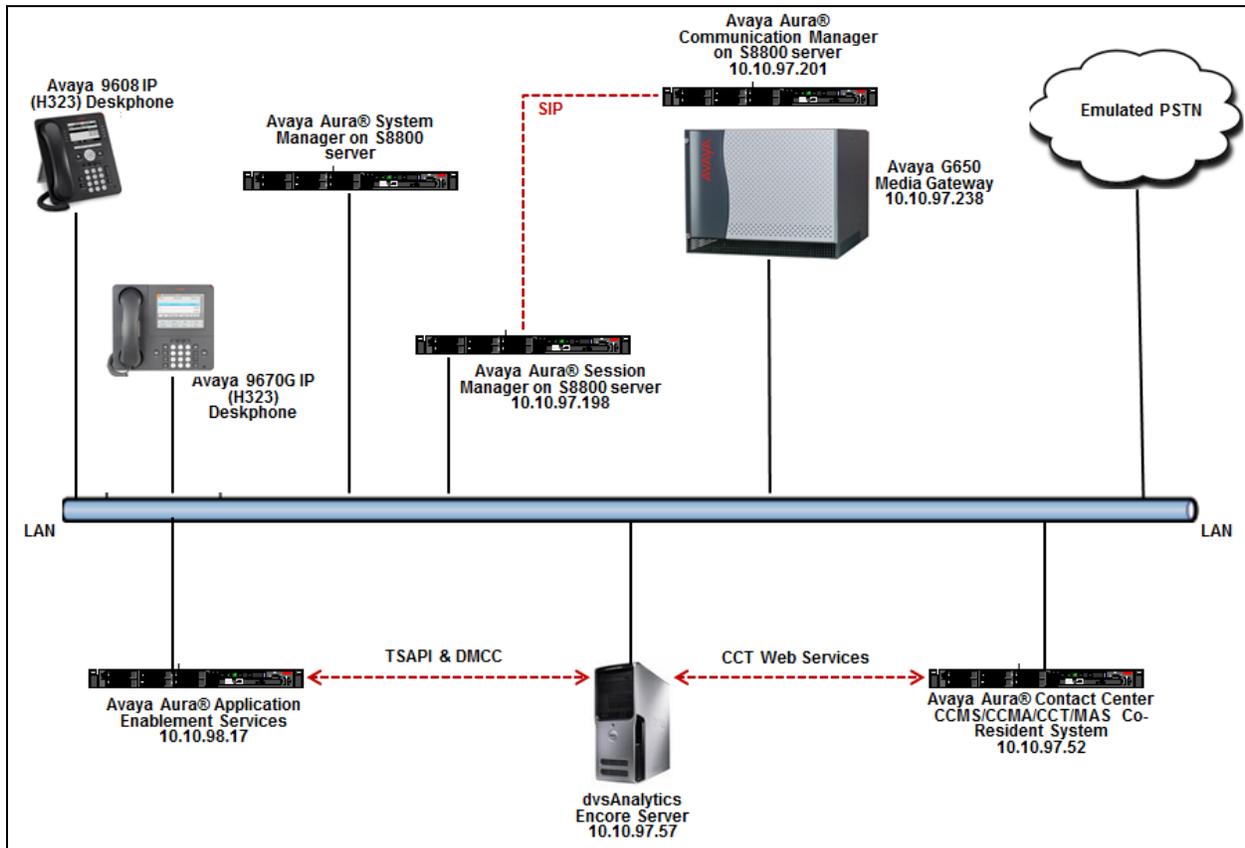


Figure 1: Tested Configuration Diagram

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 Operating System of Avaya Aura® Contact Center server	6.3 Windows 64-bit 2008 Standard R2 Service Pack 1
Avaya 9670G IP Deskphone (H.323)	S3.1
Avaya 9608 IP Deskphone (H.323)	6.2313
dvsAnalytics Encore server Operating System of Encore server <ul style="list-style-type: none">• Encore Web Interface• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC XML• Avaya Open Interfaces CCT SDK	Version 2.3.5 Windows 64-bit 2008 R2 Standard Service Pack 1 3.0.8.5685 6.1.1.469 6.1 6.2

5. Configure Avaya Aura® Communication Manager

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

- Administer CTI link
- Administer IP codec set
- Administer system parameters features
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

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

5.1. Administer CTI Link

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

```
add cti-link 1                                     Page 1 of 3
                                               CTI LINK
CTI Link: 1
Extension: 50001
Type: ADJ-IP
                                               COR: 1
Name: AES62
```

5.2. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Encore. For Audio Codec, enter “G.711MU”, which is the only codec type supported by Encore. In the compliance testing, this IP codec set was assigned to the agents and to the virtual IP softphones used by Encore.

```
Change ip-codec-set 1                             Page 1 of 2
                                               IP Codec Set
Codec Set: 1
Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size (ms)
1: G.711MU      n           2         20
```

5.3. Administer System Parameters Features

To configure Service Observing, use the command “change system-parameters features” to enable two observers in the same call. Navigate to **Page 11** and enable **Allow Two Observers in Same Call** option. The **Service Observing: Warning Tone** option can also be enabled if needed.

```
change system-parameters features                                     Page 11 of 20
                                FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length:
    Direct Agent Announcement Extension:                               Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
    Converse First Data Delay: 0           Second Data Delay: 2
    Converse Signaling Tone (msec): 100     Pause (msec): 70
    Prompting Timeout (secs): 10
    Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
    Available Agent Adjustments for BSR? n
    BSR Tie Strategy: 1st-found
    Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
    Service Observing: Warning Tone? y           or Conference Tone? n
    Service Observing/SSC Allowed with Exclusion? n
    Allow Two Observers in Same Call? y
```

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 UUI 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
```

5.4. Administer Class of Restriction (COR)

Class of Restriction (COR) is used to control features that users can access. There will be two CORs used in the testing, one is assigned to agent stations and the other is assigned to virtual stations that have the Service Observing feature buttons.

To administer a COR that will be used for the agent stations, enter the “change cor n” command, where “n” is available COR number. Enter the following fields and retain other fields at default.

- **COR Description:** Enter a descriptive name, e.g., “For regular ext”.
- **Can Be Service Observed?:** Set to “y”.
- **Can Be A Service Observer?:** Set to “n”.

```
change cor 1                                     Page 1 of 23
                                     CLASS OF RESTRICTION
                                     COR Number: 1
                                     COR Description: For regular ext
                                     FRL: 0
                                     APLT? y
Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? n       Called Party Restriction: none
    Time of Day Chart: 1             Forced Entry of Account Codes? n
    Priority Queuing? y               Direct Agent Calling? n
    Restriction Override: none        Facility Access Trunk Test? y
    Restricted Call List? n           Can Change Coverage? n
                                     Access to MCT? y
                                     Fully Restricted Service? n
Group II Category For MFC: 7         Hear VDN of Origin Annc.? n
    Send ANI for MFE? n              Add/Remove Agent Skills? n
    MF ANI Prefix:                   Automatic Charge Display? n
Hear System Music on Hold? y        PASTE (Display PBX Data on Phone)? n
                                     Can Be Picked Up By Directed Call Pickup? y
                                     Can Use Directed Call Pickup? y
                                     Group Controlled Restriction: inactive
```

Use the same command above to configure a COR for the virtual stations that have the Service Observing feature buttons. Enter the following fields and retain other fields at default.

- **COR Description:** Enter a descriptive name, e.g., “For service observer”.
- **Can Be Service Observed?:** Set to “n”.
- **Can Be A Service Observer?:** Set to “y”.

```

change cor 2                                     Page 1 of 23
                                     CLASS OF RESTRICTION

COR Number: 2
COR Description: For service observer

FRL: 7                                           APLT? y
Can Be Service Observed? n                       Calling Party Restriction: none
Can Be A Service Observer? y                     Called Party Restriction: none
Time of Day Chart: 1                             Forced Entry of Account Codes? n
Priority Queuing? n                               Direct Agent Calling? n
Restriction Override: none                       Facility Access Trunk Test? n
Restricted Call List? n                          Can Change Coverage? n

Access to MCT? y                                 Fully Restricted Service? n
Group II Category For MFC: 7                     Hear VDN of Origin Annc.? n
Send ANI for MFE? n                             Add/Remove Agent Skills? n
MF ANI Prefix:                                  Automatic Charge Display? n
Hear System Music on Hold? y PASTE (Display PBX Data on Phone)? n
Can Be Picked Up By Directed Call Pickup? n
Can Use Directed Call Pickup? n
Group Controlled Restriction: inactive
  
```

5.5. Administer Agent Stations

During the compliance test, the H.323 stations “53018” and “53019” were configured and used as the Contact Center agents with the following requirements.

- A maximum of two Call Appearances per agent station.
- IP Softphone enabled.

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.
- **Security Code:** Enter a desired code.
- **COR:** “1” as configured in **Section 5.5**.
- **IP SoftPhone:** “y”.

```
change station 53012                                     Page 1 of 5
                                                         STATION
Extension: 53012                                         Lock Messages? n          BCC: 0
  Type: 4620                                           Security Code: *       TN: 1
  Port: S00096                                         Coverage Path 1:         COR: 1
  Name: Agent 9608                                     Coverage Path 2:         COS: 1
                                                         Hunt-to Station:        Tests? y
STATION OPTIONS
    Loss Group: 19                                     Time of Day Lock Table:
    Speakerphone: 2-way                               Personalized Ringing Pattern: 1
    Display Language: english                         Message Lamp Ext: 53018
Survivable GK Node Name:                             Mute Button Enabled? y
    Survivable COR: internal                          Expansion Module? n
Survivable Trunk Dest? y                             Media Complex Ext:
                                                         IP SoftPhone? y
                                                         IP Video Softphone? n
                                                         Short/Prefixed Registration Allowed: default
                                                         Customizable Labels? y
```

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

change station 53012	STATION	Page 4 of 5
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3:	7:	
4:	8:	

Repeat the same procedure to create another H323 station “53010”.

5.6. Configure Virtual IP Softphones

For compliance testing create four virtual stations “53020”, “53021”, “53022”, and “53023” that have the Service Observing feature buttons. These virtual softphones were used by the Encore application to record media for calls made from/to agent extensions. Use the “add station n” command, where “n” is an available extension. Enter following fields and retain others at default.

- **Type:** Enter an IP station type.
- **Security Code:** Enter a desired code.
- **Name:** Enter a descriptive name.
- **COR:** “2” as configured in **Section 5.5**.
- **IP SoftPhone?:** “y”.

```
add station 53020                                     Page 1 of 5
                                                    STATION
Extension: 53020                                     Lock Messages? n          BCC: 0
  Type: 4620                                       Security Code: *       TN: 1
  Port: S00102                                       Coverage Path 1:         COR: 2
  Name: Virtual Ext1                               Coverage Path 2:         COS: 1
                                                    Hunt-to Station:         Tests? y
STATION OPTIONS
Loss Group: 19                                       Time of Day Lock Table:
Speakerphone: 2-way                                   Personalized Ringing Pattern: 1
Display Language: english                             Message Lamp Ext: 53020
Survivable GK Node Name:                             Mute Button Enabled? y
Survivable COR: internal                             Expansion Module? n
Survivable Trunk Dest? y                             Media Complex Ext:
                                                    IP SoftPhone? y
                                                    IP Video Softphone? n
Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? y
```

Navigate to **Page 4**, enter two “call-appr” and one “serv-obsrv” buttons.

```
display station 53020                                     Page 4 of 5
                                                    STATION
SITE DATA
  Room:                                     Headset? n
  Jack:                                     Speaker? n
  Cable:                                    Mounting: d
  Floor:                                    Cord Length: 0
  Building:                                 Set Color:

ABBREVIATED DIALING
  List1:                                     List2:                                     List3:

BUTTON ASSIGNMENTS
  1: call-appr                               5:
  2: call-appr                               6:
  3: serv-obsrv                             7:
  4:                                           8:
```

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 DMCC Ports.
- Configure security on Application Enablement Services.
- Administer Tlink.
- Administer CTI User.

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 horizontal bar at the top right contains a "Help" link. In the center, there is a login form with the heading "Please login here:". The form includes two input fields: "Username" and "Password", and a "Login" button below them. At the bottom center, 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" screen. At the top left is the Avaya logo. The title is "Application Enablement Services Management Console". A red horizontal bar at the top right contains "Home | Help | Logout" links. On the left side, there is a navigation menu with the following items: "Home", "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains the following text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list: "• 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 the list, it says: "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 center, there is a copyright notice: "Copyright © 2009-2012 Avaya Inc. All Rights Reserved." In the top right corner, there is a small text box with the following information: "Welcome: User admin", "Last login: Tue Dec 3 10:40:00 2013 from 10.10.96.71", "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", "Server Date and Time: Fri Feb 14 11:37:33 EST 2014".

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** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for device monitoring, and the DMCC license is used for the virtual IP softphones.

Application Enablement (CTI) - Release: 6 - SID: 10S03000 (Standard License file)																																									
WebLM Home																																									
Install license																																									
Licensed products	You are here: Licensed Products > Application_Enablement > View License Capacity																																								
APPL_ENAB	License installed on: June 10, 2013 4:44:13 PM -05:00																																								
Application_Enablement	License File Host IDs: E4-1F-13-66-48-D8																																								
View license capacity																																									
View peak usage																																									
Uninstall license																																									
Server properties																																									
Manage users																																									
Shortcuts																																									
Help for Installed Product																																									
<table border="1"> <thead> <tr> <th>Feature (Keyword)</th> <th>Expiration date</th> <th>Licensed</th> <th>Acquired</th> </tr> </thead> <tbody> <tr> <td>CVLAN ASA1 (VALUE_AES_CVLAN_ASA1)</td> <td>permanent</td> <td>16</td> <td>0</td> </tr> <tr> <td>Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)</td> <td>permanent</td> <td>1000</td> <td>1</td> </tr> <tr> <td>AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)</td> <td>permanent</td> <td>3</td> <td>0</td> </tr> <tr> <td>CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)</td> <td>permanent</td> <td>16</td> <td>0</td> </tr> <tr> <td>Product Notes (VALUE_NOTES)</td> <td>permanent</td> <td></td> <td>Not counted</td> </tr> <tr> <td>AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)</td> <td>permanent</td> <td>3</td> <td>0</td> </tr> <tr> <td>TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)</td> <td>permanent</td> <td>1000</td> <td>0</td> </tr> <tr> <td>DLC (VALUE_AES_DLC)</td> <td>permanent</td> <td>16</td> <td>0</td> </tr> <tr> <td>Device Media and Call Control (VALUE_AES_DMCC_DMC)</td> <td>permanent</td> <td>1000</td> <td>0</td> </tr> </tbody> </table>		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	DLC (VALUE_AES_DLC)	permanent	16	0	Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000	0
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																																						
DLC (VALUE_AES_DLC)	permanent	16	0																																						
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000	0																																						

If the TSAPI and DMCC services are 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 sidebar on the left contains the following navigation items: AE Services (expanded), CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (highlighted), TSAPI Properties, TWS, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, Utilities, and Help. The main configuration area is titled 'Edit TSAPI Links' and contains the following fields:

Link	1
Switch Connection	CLAN2
Switch CTI Link Number	1
ASAI Link Version	4
Security	Both

At the bottom of the configuration area are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

6.3. Administer DMCC Ports

From the Management console, navigate to **Networking** → **Ports**. The following highlighted configurations are needed in **DMCC Server Ports** section:

- **Unencrypted Port**: Enabled and enter the port “4721”. This port is used for Encore server to connect to Application Enablement Services server.

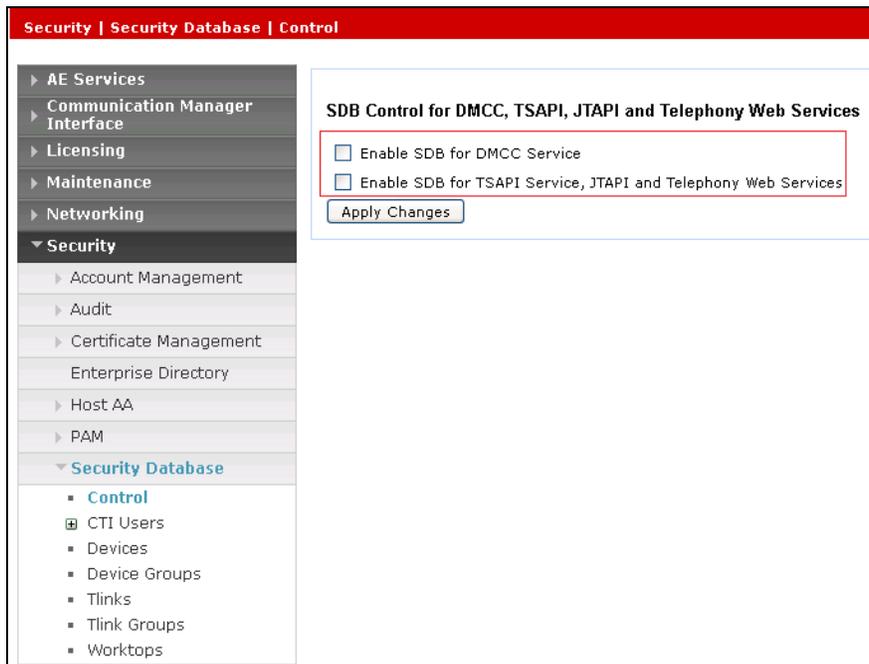
Click on **Apply Changes** and Apply when finished.

The screenshot shows the 'Networking | Ports' configuration page. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking (expanded), AE Service IP (Local IP), Network Configure, Ports (highlighted), TCP Settings, Security, Status, Utilities, and Help. The main content area is titled 'Ports' and is divided into several sections:

- CVLAN Ports**: Includes 'Unencrypted TCP Port' (9999) and 'Encrypted TCP Port' (9998). Both have 'Enabled' radio buttons selected.
- DLG Port**: Includes 'TCP Port' (5678).
- TSAPI Ports**: Includes 'TSAPI Service Port' (450) with 'Enabled' selected, and 'Local TLINK Ports' (1024-1039) with 'Unencrypted TLINK Ports' (1050-1065) and 'Encrypted TLINK Ports' (1066-1081) fields.
- DMCC Server Ports**: Includes 'Unencrypted Port' (4721) with 'Enabled' selected, and 'Encrypted Port' (4722).

6.4. 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 DMCC Service** and **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** boxes are unchecked. Click **Apply Changes** button to complete.



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

Maintenance | Service Controller

▶ AE Services
 ▶ Communication Manager Interface
 ▶ Licensing
 ▼ Maintenance
 Date Time/NTP Server
 ▶ Security Database
 Service Controller
 ▶ Server Data
 ▶ Networking
 ▶ Security
 ▶ Status
 ▶ 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](#)

6.5. 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 9.2**.

Security | Security Database | Tlinks

▶ AE Services
 ▶ Communication Manager Interface
 ▶ Licensing
 ▶ Maintenance
 ▶ Networking
 ▼ Security
 ▶ Account Management
 ▶ Audit
 ▶ Certificate Management
 Enterprise Directory
 ▶ Host AA
 ▶ PAM
 ▼ Security Database
 ▪ Control
 ▣ CTI Users
 ▪ Devices
 ▪ Device Groups
 ▪ **Tlinks**
 ▪ Tlink Groups
 ▪ Worktops

Tlinks

Tlink Name

AVAYA#CLAN2#CSTA#AES63
 AVAYA#CLAN2#CSTA-S#AES63

6.6. 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 9.1**.

The screenshot shows the 'User Management | User Admin | List All Users' interface. On the left is a navigation menu with 'User Management' expanded to 'User Admin', where 'List All Users' is selected. The main area is titled 'Edit User' and contains the following form fields:

* User Id	test
* Common Name	test
* Surname	test
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Cms Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	

7. Configure Avaya Aura® Contact Center

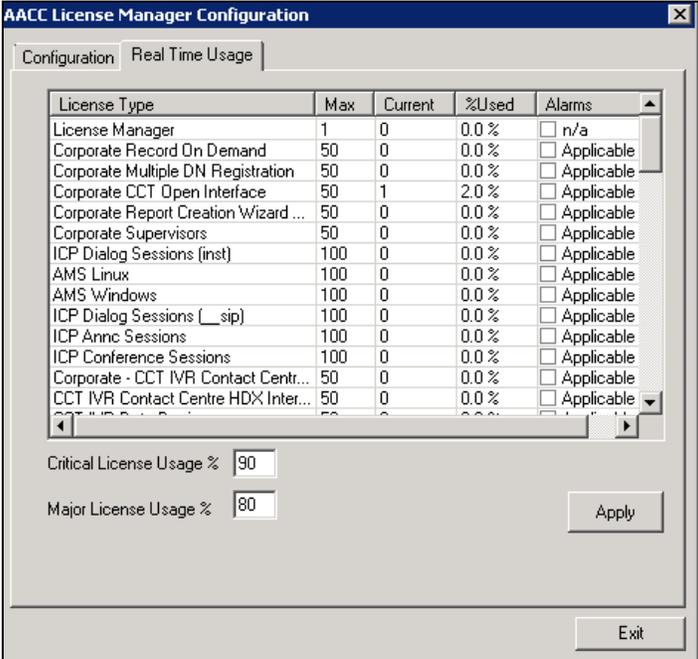
This section provides steps on how to configure Contact Center. This section assumes that Contact Center system is already installed and operational; the section provides steps for configuring the following configurations:

- 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.



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

Critical License Usage %

Major License Usage %

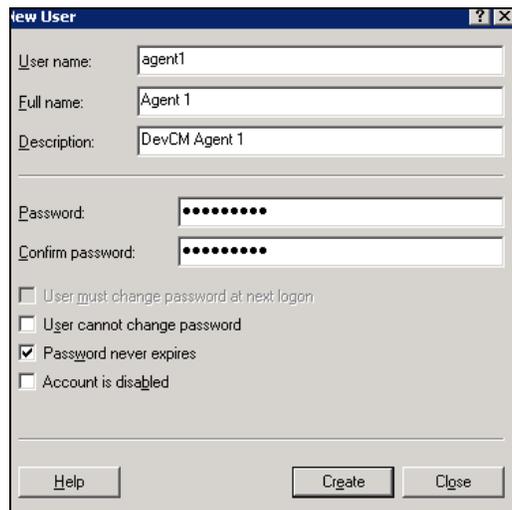
Apply

Exit

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.

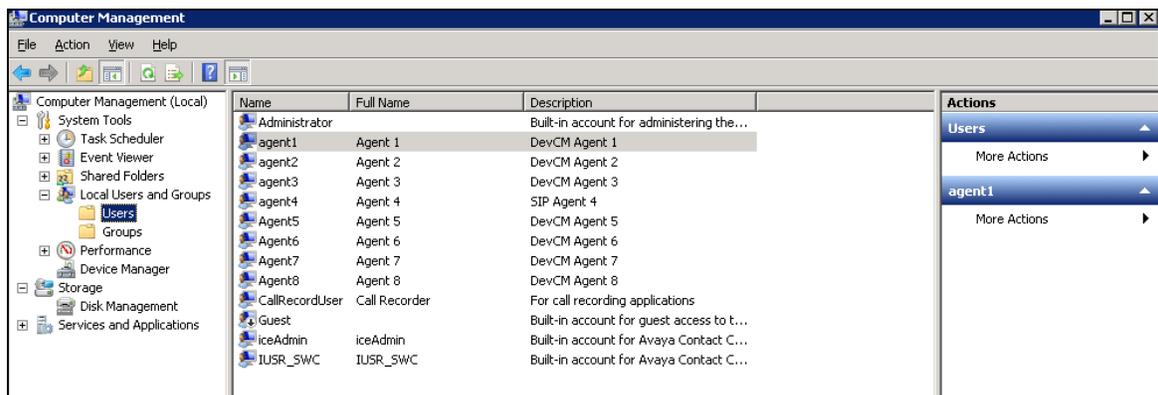
From the Contact Center CCT server, navigate to menu **Start** → **Administrative Tools** → **Computer Management**. The **Computer Management** window is displayed. Right click on **Users** (not shown) folder under **Local Users and Groups** and then select **New**. The **New User** window is displayed;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



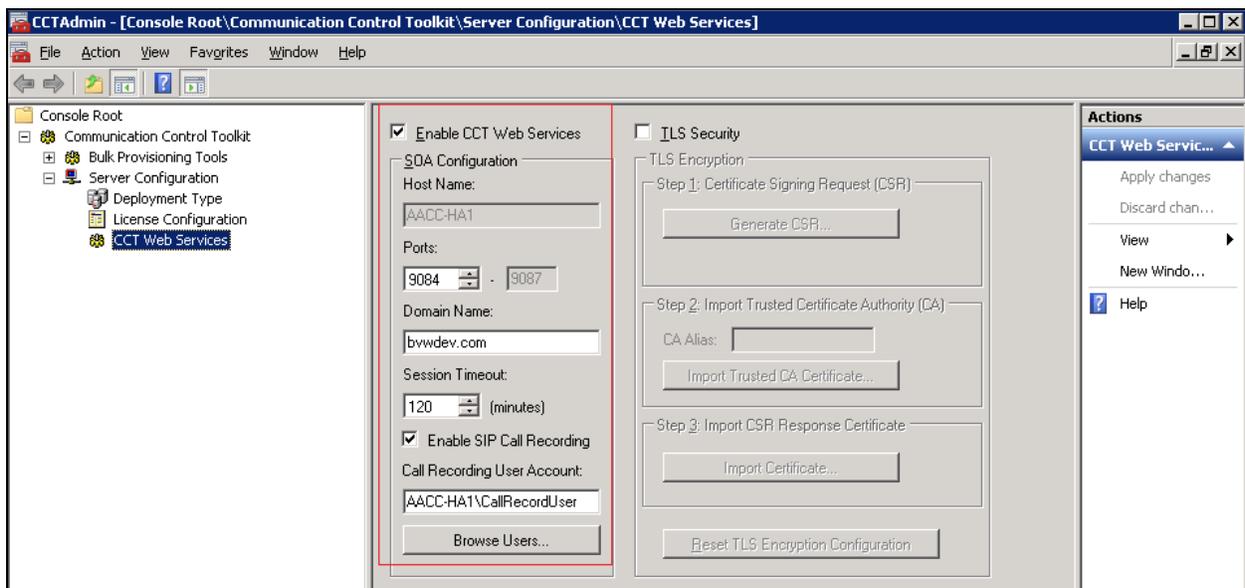
Repeat the same procedure to create “CallRecordUser” that is used for configuring in the CCT Web services for the Encore application.

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**.

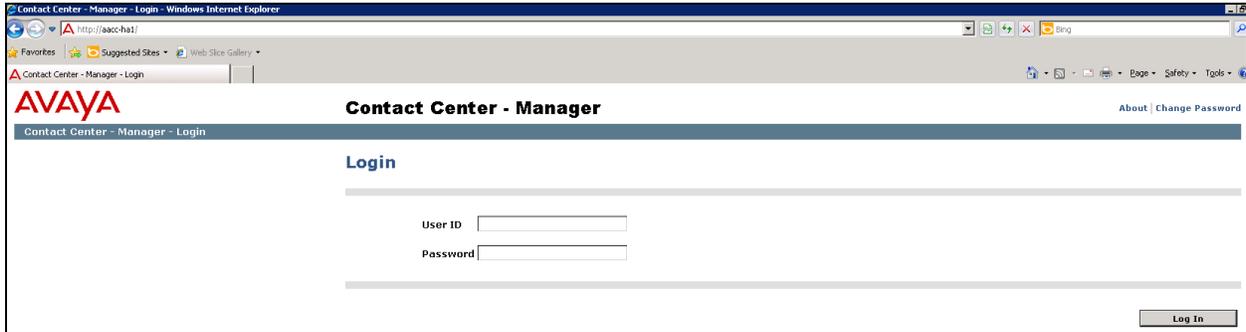
In the middle pane, enter the following highlighted fields:

- **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**. Note to include the local computer name since the user is created as a local Windows user. During compliance testing the local computer name was AACC-HA1.
- **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).

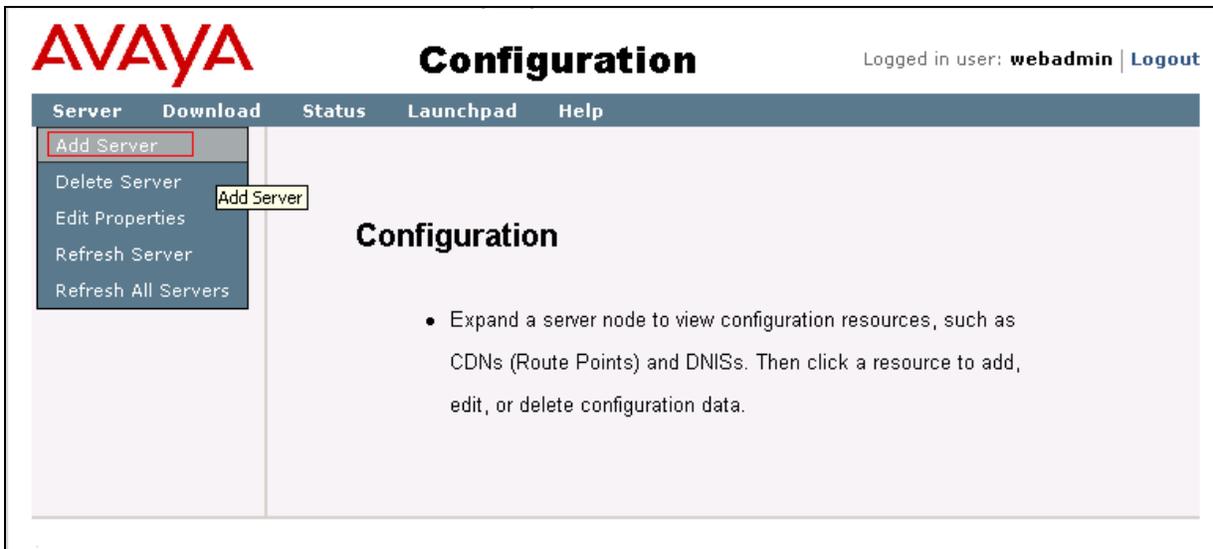
In order to access CCT Administration web page, the CCT server needs to be added into Contact Center Manager Administer (CCMA). Launch CCMA web page, by entering IP address or hostname of CCMA into the address box of a browser as shown below. Note that the IP address of CCMA needs to be added into the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



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



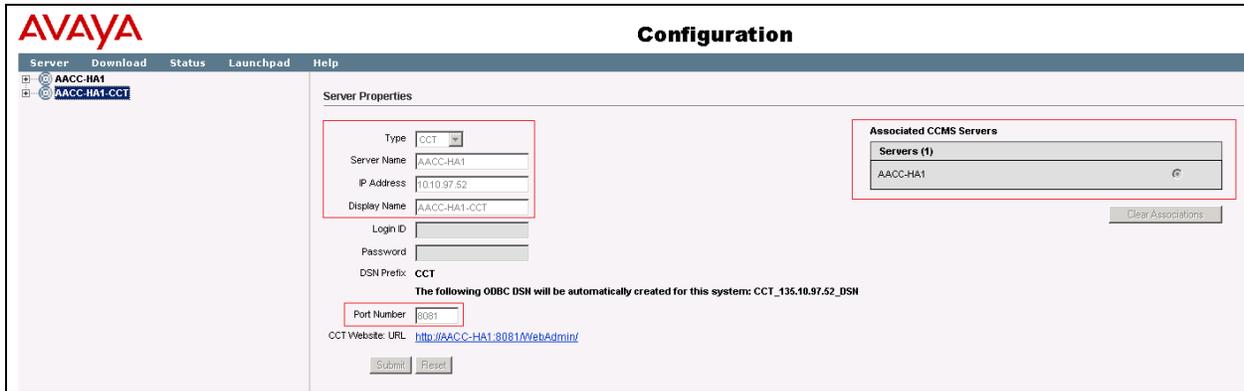
From the **Configuration** page, select **Server** → **Add Server**.



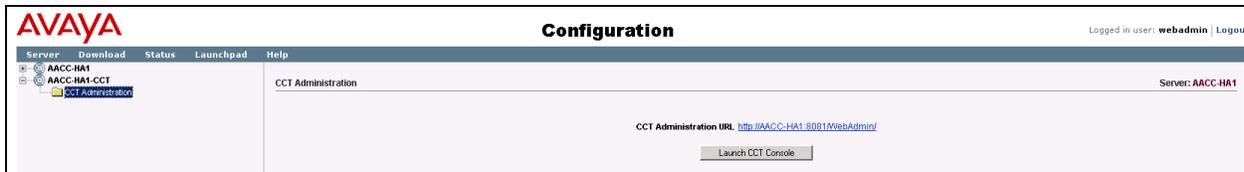
The **Server Properties** window is displayed in the right pane. Enter the following highlighted fields below.

- **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”.

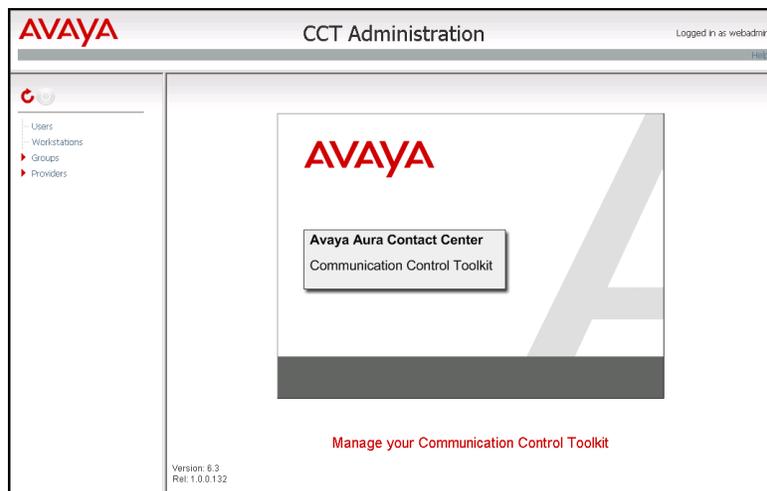
Click **Submit** button to add the CCT Server.



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 left navigation pane has 'Users' highlighted with a red box. 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 form.

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 **Save** button to save changes.

The screenshot shows the AVAYA CCT Administration interface. The left navigation pane has 'Providers' > 'Passive' highlighted with a red box. The main content area is titled 'Update CCT Provider' and contains two sections: 'Basic Provider Information' (with fields for Provider Name: Passive, IP Address: 10.10.97.52, and Port: 5060) and 'Provider Configuration' (with a dropdown menu for Transport set to TCP). A 'Save' button is located at the bottom left of the form.

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.

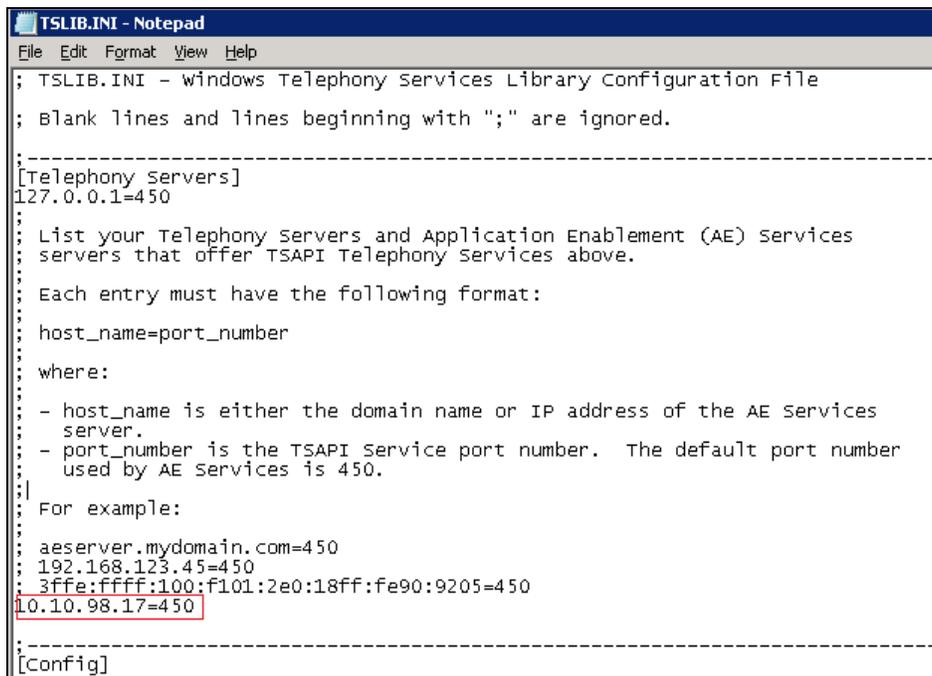
The Encore system integrates with the Avaya system. This integration allows the Encore system to successfully perform the following functions:

- 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 AudioServer Softphones

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 all 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]
```

From Encore server, navigate to folder **D:\EncData\Config\Softphone**, right-click to the file **SP_CMAPI.ini** and select **Open with Notepad** to edit this file.

In the **CMAPISessionInfo** section, enter the IP address and port of Application Enablement Services server in the **AESAddress** and **AESPort** and **Username** and **Password** as configured in **Section 6.6**. The screens below show the **SP_CMAPI.INI** configuration in the compliance test.

```
SP_CMAPI.ini - Notepad
File Edit Format View Help
# E.G. full extension number=4085551234, set StationPrefix=408
# and set EncorePort in CT gateway INI to 5551234.
# This feature requires SP_CMAPI.DLL 3.5.1000 or later.
# TenDigitsExtension Set this to yes when TenDigitsExtension is set to Yes in CT Gateway
# CTISetup.ini file. StationPrefix is ignored.
# ExtensionAreaCodesFile when TenDigitsExtension=Yes, set this to CTISetup.ini file that
# contains the extension area codes configuration.s

[Options]
SimulatesO=No
OffHookDelayInms=250
OnHookDelayInms=100
InterDigitDelayInms=50
# StationPrefix=
TenDigitsExtension=No
# ExtensionAreaCodesFile=D:\EncData\Config\CTGateway\CTISetup-TSAPI.ini

# =====
# | DMCC Session Info
#
# AESAddress IP address of AES (Application Enablement service) connector
# AESPort IP port of AES, only unencrypted port 4721 is supported.
# UserName User name to log into AES, in AES 3.0, this is required but not validated,
# For AES 3.1 or later, this is validated.
# Password password to log into AES, see UserName
#
[CMAPISessionInfo]
AESAddress=10.10.98.17
AESPort=4721
UserName=test
Password=123456
# =====
#
```

Scroll down to the DMCC softphones section. Under **Softphone1**, set **Extension** and **Password** to the first virtual IP softphone extension and security code from **Section 5.7**. Set **SwitchAddr** to the IP address of Communication Manager. During compliance testing the processor IP address was used. Set **RTPAddress** to the IP address of the Encore server. Retain the default values in the remaining fields.

Create additional softphone lines as necessary. In the compliance testing, four softphones were configured to correspond to the four virtual IP softphones from **Section 5.7**.

```
# Codec          Codec for RTP packets, default is g711u. other values are g711A,
#                g729 and g729A (must be administered on switch).
#                Currently only G711U is supported.
#
[SoftPhone1]
  Extension=53020
  Password=1234
#   SwitchName=cm
  SwitchAddr=10.10.97.201
  RTPAddress=10.10.97.57
  Codec=g711U

[SoftPhone2]
  Extension=53021
  Password=1234
#   SwitchName=cm
  SwitchAddr=10.10.97.201
  RTPAddress=10.10.97.57
  Codec=g711U

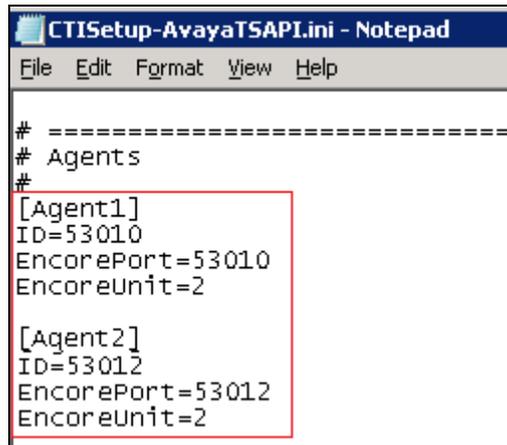
[SoftPhone3]
  Extension=53022
  Password=1234
#   SwitchName=cm
  SwitchAddr=10.10.97.201
  RTPAddress=10.10.97.57
  Codec=g711U

[SoftPhone4]
  Extension=53023
  Password=1234
#   SwitchName=cm
  SwitchAddr=10.10.97.201
  RTPAddress=10.10.97.57
  Codec=g711U
```

8.2. Configure CT Gateway for TSAPI

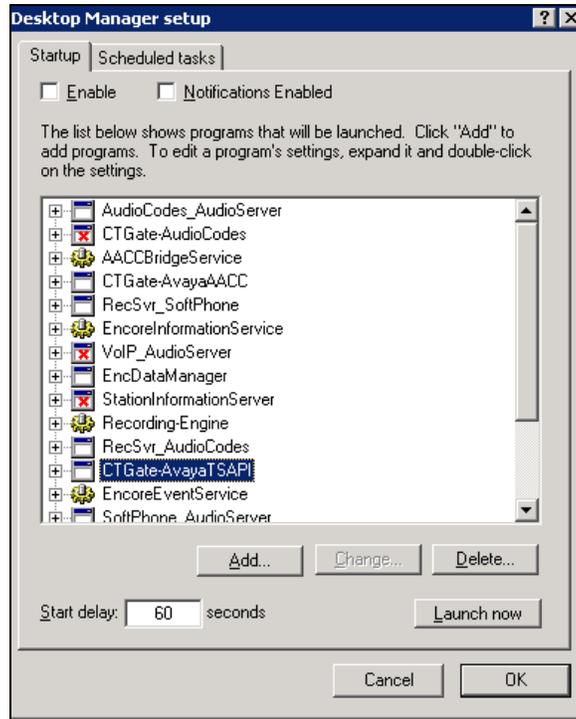
From the Encore server, navigate to D:\EncData\Config\CTGateway. Copy and rename the default **ctisetup.ini** file to **CTIsetup-AvayaTSAPI.ini**. Double click on this file. Locate the following lines in the INI file and verify the values match the example below.

Scroll to the **Agents** section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section 5.6**. **EncoreUnit** is set to the value of the Recording Unit used for DMCC recording. During compliance testing it was on “2”, but will typically be set to “1”. Create additional agent parameter lines as necessary when more than one agent is being monitored.

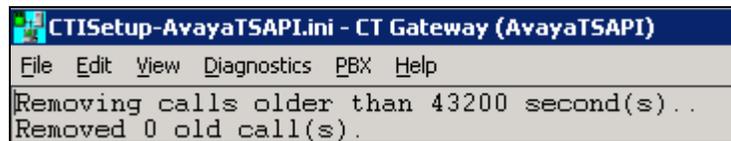


```
# =====  
# Agents  
#  
[Agent1]  
ID=53010  
EncorePort=53010  
EncoreUnit=2  
  
[Agent2]  
ID=53012  
EncorePort=53012  
EncoreUnit=2
```

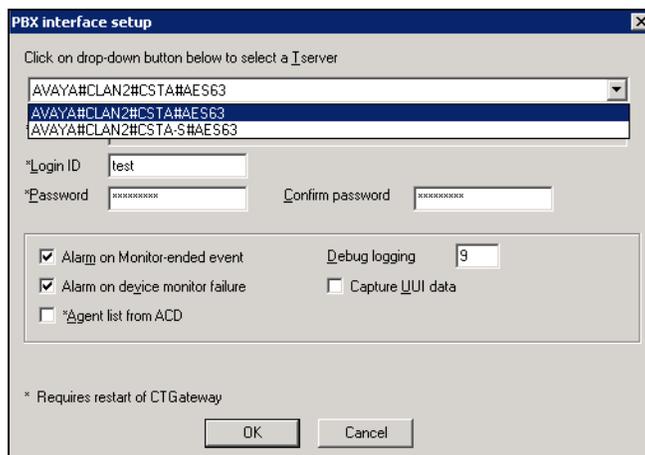
Use the **Desktop Manager setup** tool to launch CT Gateway for Avaya TSAPI. Right-click on the **Desktop Manager** icon in the system tray, select **Configuration** (screen not shown). The **Desktop Manager setup** window is displayed.



Click **Launch Now** to launch **CT Gateway**. 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 6.5** 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 6.6**. Click **OK** button to complete and shut down the **CTGate-AvayaTSAPI**.

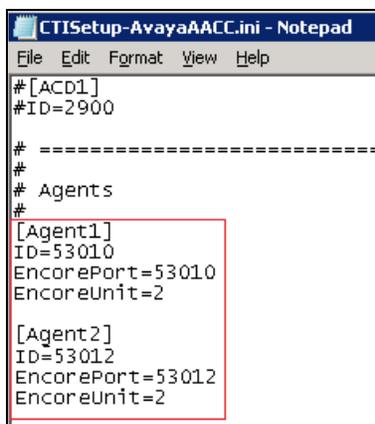


Use the **Desktop Manager Setup** application to launch the **CTGate-AvayaTSAPI** application again.

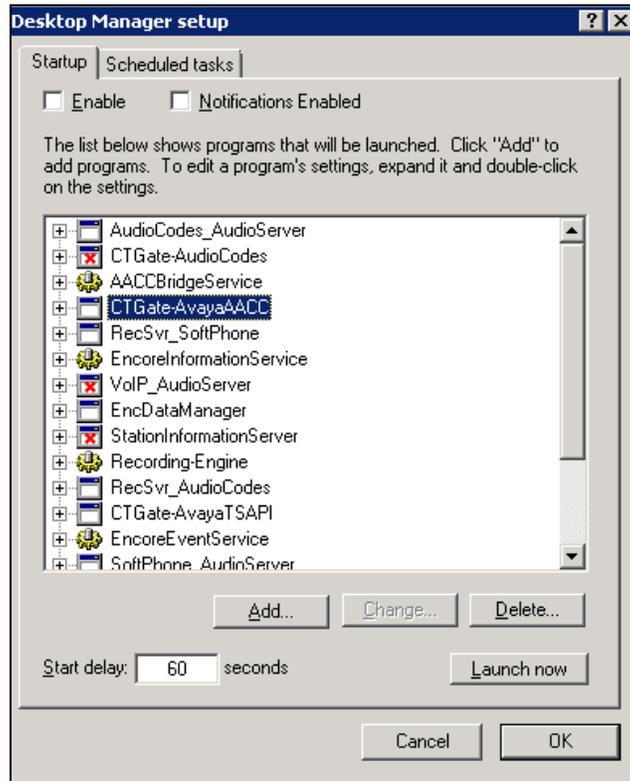
8.3. Configure CT Gateway for Contact Center Data Collection

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:

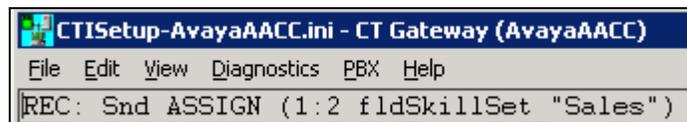
In the **Agents** section, set **ID** and **EncorePort** to the first agent station extension from **Section 5.6**. **EncoreUnit** is set to the value of the Recording Unit used for DMCC recording. During compliance testing it was on “2”, but will typically be set to “1”. Create additional agent parameter 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:** “bvwwdev.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 compliance 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

* Requires restart of CTGateway

Click **OK** button to complete and shut down the **CTGate-AvayaAACC**. Use the **Desktop Manager Setup** application to launch the **CTGateways** 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 connections from Contact Center and Encore servers to Application Enablement Services server by navigating to **Status** → **Status and Control** → **DMCC Service Summary**. The **DMCC Service Summary-Session Summary** window is displayed in the right pane as shown below. Verify the **User** column shows an active session with the CTI user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the number of configured softphones from **Section 8.1**.

AVAYA Application Enablement Services Management Console

Welcome: User admin
 Last login: Mon Nov 25 14:20:41 2013 from 10.10.98.71
 Number of prior failed login attempts: 2
 HostName/IP: AES63/10.10.98.17
 Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
 SW Version: 6.3.0.0.212-0
 Server Date and Time: Tue Dec 03 10:41:34 EST 2013

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

DMCC Service Summary - Session Summary

Enable page refresh every seconds

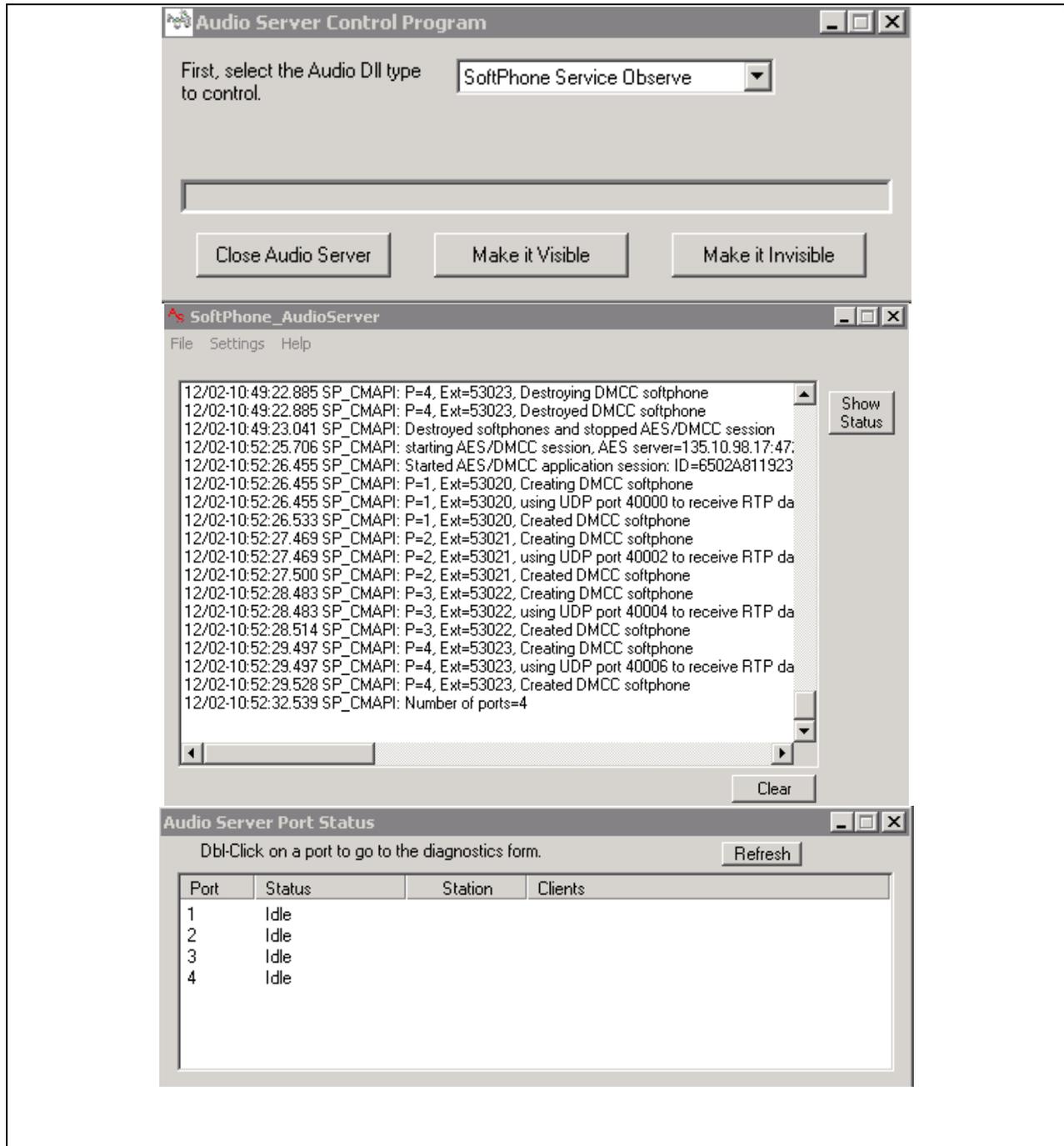
Session Summary [Device Summary](#)
 Generated on Tue Dec 03 10:40:49 EST 2013
 Service Uptime: 35 days, 21 hours 23 minutes
 Number of Active Sessions: 4
 Number of Sessions Created Since Service Boot: 17
 Number of Existing Devices: 4
 Number of Devices Created Since Service Boot: 9

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/> 35F16A5A4F9FB80B 1CC2198CB87BC63-11	sip:53010@bvwddev.com	AACC	10.10.97.52:10.10.97.52	TR-87 Encrypted	1
<input type="checkbox"/> E5186828C0558F546 01826649562E481-17	sip:53040@bvwddev.com	AACC	10.10.97.52:10.10.97.52	TR-87 Encrypted	1
<input type="checkbox"/> E51534AC6444A893D 046933E1E2C22B9-16	sip:53042@bvwddev.com	AACC	10.10.97.52:10.10.97.52	TR-87 Encrypted	1
<input type="checkbox"/> 6502A811923E3CFBA 3E07FAEE8537D78-18	test	SPAS1	10.10.97.57	XML Unencrypted	4

Item 1-4 of 4

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

- Check status of the Audio Server Port and Softphone_AudioServer at the Encore server as shown below. Verify that the ports are created and in idle status.



- Screen below shows the SoftPhone 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 the 'SoftPhone Recording Server' application window. At the top, there is a menu bar with 'File', 'Setup', 'View', 'Diagnostics', and 'Help'. Below the menu is a 'Recording Ports' section with a grid of 10 ports. The first port, '53041', is highlighted in green. Below this is a table showing connection details for 'SoftPhone Audio Server' and 'RecEngine'. The bottom section is a log window titled 'Log: RecSvrSP_25.txt' with a 'Clear' button. The log contains a series of timestamped messages detailing the start and stop of recording sessions for various ports and connections.

Connection Name	Connected	Connection Time	IP Address
SoftPhone Audio Server	Yes	11/25 15:02:36	127.0.0.1
RecEngine	Yes	11/25 15:02:42	127.0.0.1

```

Log: RecSvrSP_25.txt
11/28-13:31:17.010 Rcv<RecEngine>: Start: 2:53012:1 D:\EncData\0H\01Z146ZH.vx8
11/28-13:31:17.010 Snd<AS> MonitorRequest<53012>
11/28-13:31:17.010 Snd<RecEngine>: Start Status: 2:53012:1 {MaxRecTime = 1800} Monitor Request Sent
11/28-13:31:17.697 Rcv<AS><RecEngine><53012><1>: StartedMonitor
11/28-13:31:17.697 Snd<RecEngine>: Asynch Status: 2:53012:1 Start Recording<1>
11/28-13:31:25.481 Rcv<RecEngine>: Stop: 2:53012:1
11/28-13:31:25.481 Snd<AS>: Stop Monitor 53012
11/28-13:31:25.481 Snd<RecEngine>: Stop Status: 2:53012:1 Success
11/28-13:31:37.867 Rcv<RecEngine>: Start: 2:53041:1 D:\EncData\0H\01Z146ZL.vx8
11/28-13:31:37.867 Snd<AS> MonitorRequest<53041>
11/28-13:31:37.867 Snd<RecEngine>: Start Status: 2:53041:1 {MaxRecTime = 1800} Monitor Request Sent
11/28-13:31:37.867 Rcv<RecEngine>: Start: 2:53012:1 D:\EncData\0H\01Z146ZJ.vx8
11/28-13:31:37.867 Snd<AS> MonitorRequest<53012>
11/28-13:31:37.867 Snd<RecEngine>: Start Status: 2:53012:1 {MaxRecTime = 1800} Monitor Request Sent
11/28-13:31:38.554 Rcv<AS><RecEngine><53041><1>: StartedMonitor
11/28-13:31:38.554 Snd<RecEngine>: Asynch Status: 2:53041:1 Start Recording<1>
11/28-13:31:38.554 Rcv<AS><RecEngine><53012><2>: StartedMonitor
11/28-13:31:38.554 Snd<RecEngine>: Asynch Status: 2:53012:1 Start Recording<2>
11/28-13:31:51.018 Rcv<RecEngine>: Stop: 2:53012:1
11/28-13:31:51.018 Snd<AS>: Stop Monitor 53012
11/28-13:31:51.018 Snd<RecEngine>: Stop Status: 2:53012:1 Success
11/28-13:31:51.018 Rcv<RecEngine>: Start: 2:53012:1 D:\EncData\0H\01Z146ZH.vx8
11/28-13:31:51.018 Snd<AS> MonitorRequest<53012>
11/28-13:31:51.034 Snd<RecEngine>: Start Status: 2:53012:1 {MaxRecTime = 1800} {append}Monitor Request Sent
11/28-13:31:51.829 Rcv<AS><RecEngine><53012><3>: StartedMonitor
11/28-13:31:51.829 Snd<RecEngine>: Asynch Status: 2:53012:1 Start Recording<3>
11/28-13:32:26.493 Rcv<RecEngine>: Stop: 2:53012:1
11/28-13:32:26.493 Snd<AS>: Stop Monitor 53012
11/28-13:32:26.493 Snd<RecEngine>: Stop Status: 2:53012:1 Success
11/28-13:32:44.324 Rcv<RecEngine>: Stop: 2:53041:1
11/28-13:32:44.324 Snd<AS>: Stop Monitor 53041
11/28-13:32:44.324 Snd<RecEngine>: Stop Status: 2:53041:1 Success
11/28-13:40:55.662 Rcv<RecEngine>: Start: 2:53041:1 D:\EncData\0K\01Z146ZK.vx8
11/28-13:40:55.662 Snd<AS> MonitorRequest<53041>
11/28-13:40:55.662 Snd<RecEngine>: Start Status: 2:53041:1 {MaxRecTime = 1800} Monitor Request Sent
11/28-13:40:55.927 Rcv<AS><RecEngine><53041><1>: StartedMonitor
  
```

- 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 section shows a navigation pane on the left with categories like Libraries, Shared Playlists, and My Playlists. The main area contains a table of call recordings with columns for Date, Duration, Extension, ACD Number, ACD Name, Skillset, ANI, DNIS, Call Direction, Call Type, Consultation call, Agent Login ID, Other Party Name, and Other Party Number. Below the table is a streaming player for the selected recording, showing a waveform and playback controls. The player status indicates 'Video Unavailable' 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 12:33:38 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 9:34:39 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				54008	53012	Incoming	External	<input type="checkbox"/>			54008	H.323
11/28/2013 9:25:38 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 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 by 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.