



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring dvsAnalytics Encore and Avaya Aura® Contact Center, Avaya Aura® Application Enablement Service, Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring dvsAnalytics Encore Version 6.0.1 and Avaya Aura® Contact Center 6.4, 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.

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

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

1. Introduction

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. 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 (CCAM), 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 Computer Telephony Integration (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 observations:

- For the conference scenarios, the recording entry for the conference-from agent can contain multiple Service Observing confirmation tones, due to different softphones added for different portions of the conference call.
- In case of a conference call, the recorded party name from TSAPI overwrites the AACC provided agent name.
- The Consultation Call parameter associated with the recording entries applied to the attended transfer and conference scenarios.
- 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/>
- **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.

In the compliance testing, Encore monitored the queue and agent stations shown in the table below.

Device Type	Extension
CDN	4001
Supervisor	53040
Agent Station	53010, 53012

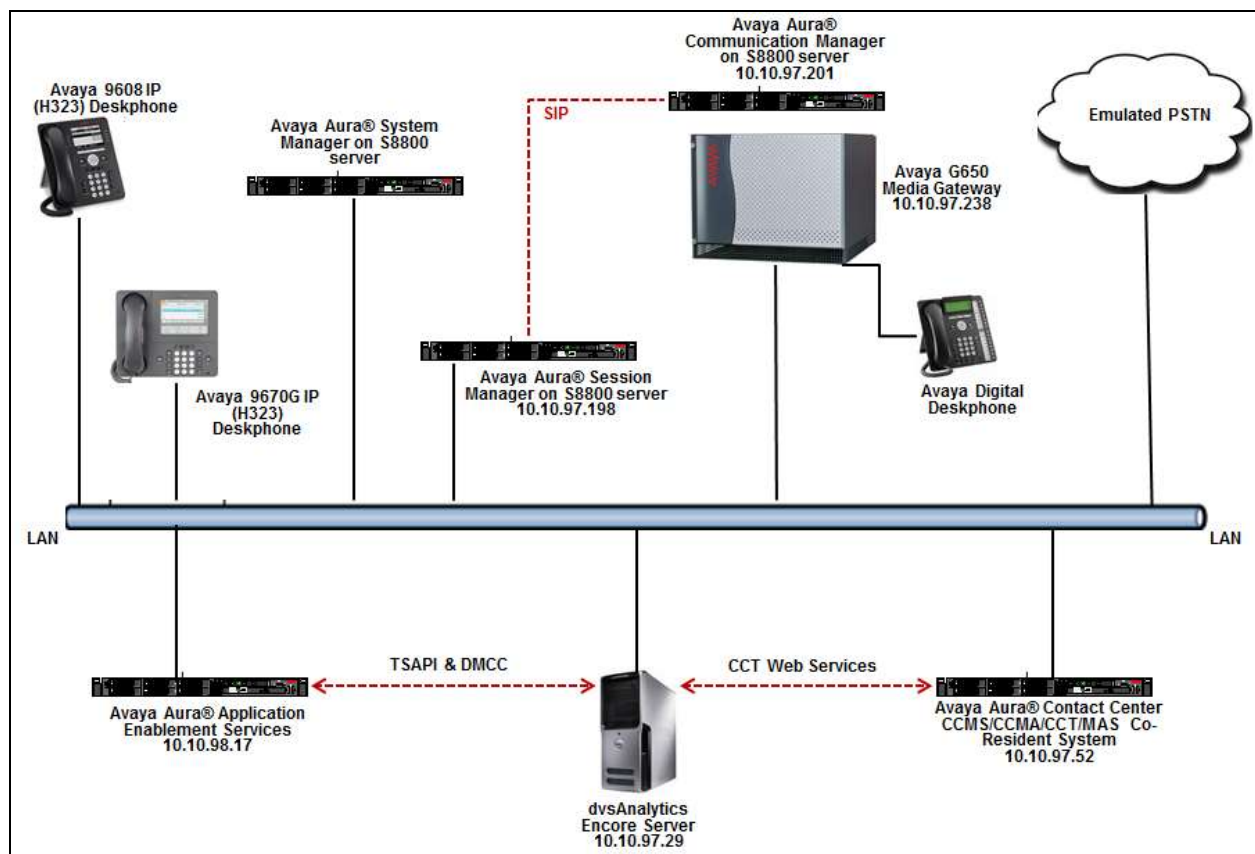


Figure 1: Tested Configuration Diagram

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 on Avaya S8800 Server with Avaya G650Media Gateway	6.3-03.0.124.0 (R016x.03.0.124.0-21588)
Avaya Aura® System Manager running on S8800 Server	6.3
Avaya Aura® Session Manager running on S8800 Server	6.3.10.0.631008
Avaya Aura® Application Enablement Services	6.3.3.1.10-0
Avaya Aura® Contact Center running on S8800 Server Operating System of Avaya Aura® Contact Center server	6.4.213.0 (SP13) Windows Server 64-bit 2008 Standard R2 Service Pack 1
Avaya 9670G IP Deskphone (H.323)	3.220A
Avaya 9608 IP Deskphone (H.323)	6.4014
Avaya 9404 Digital Deskphone	12
dvsAnalytics Encore on Windows Server 2008 R2 Standard SP1 <ul style="list-style-type: none">Encore Web InterfaceAvaya TSAPI Windows Client (csta32.dll)Avaya DMCC XMLAACCBridge.exeAvaya Open Interfaces CCT SDK	6.0.1 3.0.9.6960 6.1.1.469 6.1 2.1.0.7557 6.2

5. Configure Avaya Aura® Communication Manager

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

- Verify License
- Administer CTI Link
- Administer IP Node Name
- 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. Verify License

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

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	

Navigate to **Page 6**, and verify that the **Service Observing (Basic)** customer option is set to “y”.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 6.0		
ACD? y	Reason Codes? y	
BCMS (Basic)? y	Service Level Maximizer? n	
BCMS/VuStats Service Level? y	Service Observing (Basic)? y	
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y	
Business Advocate? n	Service Observing (VDNs)? y	
Call Work Codes? y	Timed ACW? y	
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y	
Dynamic Advocate? n	Vectoring (Prompting)? y	

5.2. Administer CTI Link

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

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 50001		
Type: ADJ-IP		
COR: 1		
Name: AES63		

5.3. Administer IP Node Name

This section describes the steps for configuring IP node names in Communication Manager. Enter the “**change node-names ip**” command, and add a node name for, **CLAN** card and its IP addresses. This will be used later in **Section 6.3**.

change node-names ip		Page 1
NODE NAMES		
Type	Name	IP Address
IP	AES63	10.10.98.17
IP	AVAYARDTT	10.10.98.71
IP	CLAN1	10.10.97.217
IP	CLAN2	10.10.97.238
IP	DevCM3	10.10.4.9

5.4. 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
2:			

5.5. Administer System Parameters Features

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

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

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

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

Navigate to **Page 11**. Set **Service Observing Warning Tone** to the needed setting per customer requirements, and enable **Allow Two Observers in Same Call**, as shown below.

```
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 Threshod: 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 Allowed with Exclusion? n
      Allow Two Observers in Same Call? y
```

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

5.6. Administer Class of Restriction

Enter the “change cor n” command, where “n” is the class of restriction (COR) number used for integration with Encore. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to “y”, as shown below. For the compliance testing, this COR was assigned to the agent stations and virtual IP softphones.

```
change cor 1                                                         Page 1 of 23
                                CLASS OF RESTRICTION

    COR Number: 1
    COR Description:

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

5.7. Administer Agent Stations

Use the “change station n” command, where “n” is the first agent station extension from **Section Error! Reference source not found.** For **COR**, enter the COR number from **Section 5.6**.

```
change station 53010
```

Page 1 of 5

STATION		
Extension: 53010	Lock Messages? n	BCC: 0
Type: 9608	Security Code: *	TN: 1
Port: S00004	Coverage Path 1:	COR: 1
Name: H.323 53010	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: 53010
Survivable GK Node Name:	Mute Button Enabled? y
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? y
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default

Repeat this section to administer all agent stations from **Section Error! Reference source not found.** In the compliance testing, two agent stations were administered as shown below.

```
list station 53010 count 3
```

STATIONS								
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack	
53010	S00004 9608	H.323 53010	no			1		
53012	S00119 9670	H.323, 53012	no			1		

5.8. Administer Virtual IP Softphones

Add a virtual IP softphone using the “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.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “9650 or 4620”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.6**.
- **IP SoftPhone:** “y”

add station 53020		Page	1 of 5
STATION			
Extension: 53020	Lock Messages? n	BCC:	0
Type: 9650	Security Code: *	TN:	1
Port: S00102	Coverage Path 1:	COR: 1	
Name: Virtual Ext1	Coverage Path 2:	COS:	1
	Hunt-to Station:	Tests?	y
STATION OPTIONS			
Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern:	1	
	Message Lamp Ext:	53020	
Speakerphone: 2-way	Mute Button Enabled?	y	
Display Language: english	Button Modules:	0	
Survivable GK Node Name:	Media Complex Ext:		
Survivable COR: internal	IP SoftPhone? y		
Survivable Trunk Dest? y	IP Video Softphone?	n	
	Short/Prefixed Registration Allowed:	default	
	Customizable Labels?	y	

Navigate to **Page 4**, and add a “serv-obsrv” button as shown below.

add 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		
2: call-appr		
3: serv-obsrv		

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, four virtual IP softphones were administered as shown below.

list station 53020 count 4										
STATIONS										
Ext/ Hunt-to	Port/ Type	Name/ Surv	GK	NN	Move	Room/ Data	Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack
53020	S00102 9650	Virtual	Ext1		no			1	1	
53021	S00105 4620	Virtual	Ext2		no			1	1	
53022	S00108 4620	Virtual	Ext3		no			1	1	
53023	S00111 4620	Virtual	Ext4		no			1	1	

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM Interface
- Verify License
- Administer TSAPI Link
- Administer H.323 Gatekeeper
- Disable Security Database
- Restart Services
- Obtain Tlink Name
- Administer Encore User
- Enable Ports

6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page, with a "Help" link in the top right corner. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below these fields is a "Login" button. At the bottom of the page, another thick red horizontal bar is present, with the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." centered below it.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "out" with login details. A red navigation bar contains "Home", "Help", and "Logout". The left sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays "Welcome to OAM" with a list of administrative domains and their functions. A copyright notice for 2009-2014 Avaya Inc. is at the bottom.

AVAYA Application Enablement Services Management Console

Welcome! User: out
Last login: Fri Dec 19 18:57:35 2014 from 10.10.96.86
Number of prior failed login attempts: 0
HostName/IP: AES53/10.10.96.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:39:42 EST 2015
HA Status: Not Configured

Home | Help | Logout

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

Welcome to OAM

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

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

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

Copyright © 2009-2014 Avaya Inc. All Rights Reserved.

6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, including details about WebLM Server Address, WebLM Server Access, and Reserved Licenses. A red note at the bottom advises users to disable their pop-up blocker. The top header and navigation bar are identical to the previous screenshot.

AVAYA Application Enablement Services Management Console

Welcome! User: out
Last login: Fri Dec 19 18:57:35 2014 from 10.10.96.86
Number of prior failed login attempts: 0
HostName/IP: AES53/10.10.96.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:48:18 EST 2015
HA Status: Not Configured

Licensing | Home | Help | Logout

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

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

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

Copyright © 2009-2014 Avaya Inc. All Rights Reserved.

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.

Licensed products	License installed on: June 10, 2013 4:44:13 PM -05:00		
APPL_ENAB			
▼ Application_Enablement	License File Host IDs: E4-1F-13-66-48-D8		
View license capacity			
View peak usage			
Uninstall license	Licensed Features		
Server properties			
Manage users			
Shortcuts			
Help for Installed Product			
	10 Items Show ALL ▼		
	Feature (License Keyword)	Expiration date	Licensed capacity
	CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
	Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
	AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
	CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
	Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;del11950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;ur TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_0 AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestrict DMCUnrestricted, AgentEvents;
	AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
	TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
	DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000	

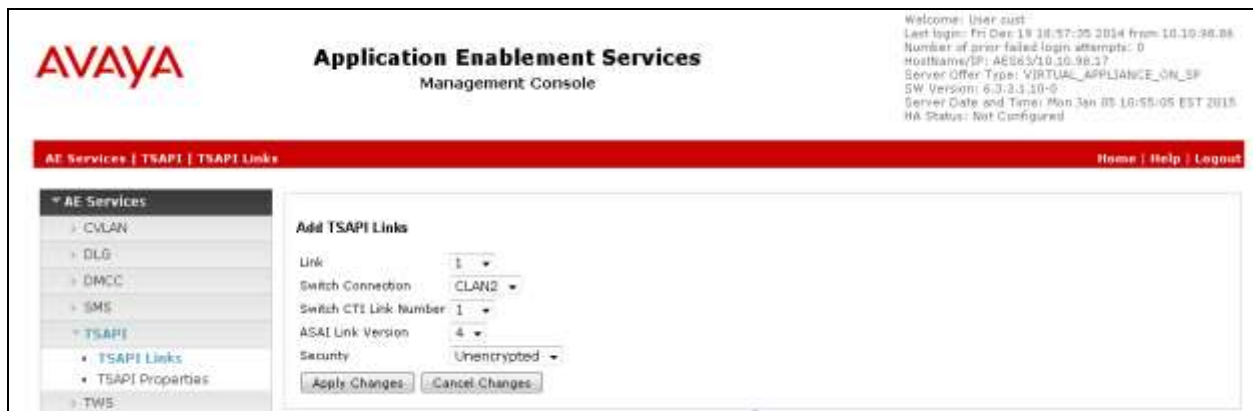
6.3. Administer TSAPI Link

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



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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “CLAN2” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with the relevant Communication Manager, in this case “CLAN2”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Mag Period, and Number of Active Connections. One connection is listed: CLAN2, No, 30, 1. Below the table are buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, and Survivability Hierarchy. The top right corner shows system information: Welcome! User: cust, Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86, Number of prior failed login attempts: 0, HostName/IP: A2563/10.10.98.17, Server Offer Type: VIRTUAL_APPLIANCE_ON_SP, SW Version: 6.3.3.1.10-0, Server Date and Time: Mon Jan 05 18:57:40 EST 2015, HA Status: Not Configured.

Connection Name	Processor Ethernet	Mag Period	Number of Active Connections
CLAN2	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as the H.323 gatekeeper, in this case “10.10.97.201” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - CLAN2' screen. The left navigation pane is the same as the previous screenshot. The main area has a text input field containing '10.10.97.201' and an 'Add Name or IP' button. Below the input field are buttons for 'Delete IP' and 'Back'. The top right corner shows the same system information as the previous screenshot.

6.5. Disable Security Database

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



6.6. Restart Services

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a user status bar on the right indicating a successful login. A red navigation bar below the header shows "Maintenance | Service Controller" and links for "Home | Help | Logout".

The left sidebar contains a tree view with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Data Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status.

The main content area, titled "Service Controller", contains a table with two columns: "Service" and "Controller Status".

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

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

6.7. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Encore

In this case, the associated Tlink name is “AVAYA#CLAN2#CSTA#AES63”. Note the use of the switch connection “CLAN2” from **Section 6.3** as part of the Tlink name.



6.8. Administer Encore User

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

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and system status information such as 'Welcome: user root', 'Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86', and 'Server Date and Time: Mon Jan 05 11:09:24 EST 2015'. A red navigation bar contains the breadcrumb 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'.

The left sidebar shows a tree view of system components, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main content area is titled 'Add User' and contains a form with the following fields:

- * User Id: text input (value: test)
- * Common Name: text input (value: test)
- * Surname: text input (value: test)
- * User Password: password input (masked with asterisks)
- * Confirm Password: password input (masked with asterisks)
- Admin Note: text area
- Avaya Role: dropdown menu (value: None)
- Business Category: text input
- Car License: text input
- CM Home: text input
- Css Home: text input
- CT User: dropdown menu (value: Yes)
- Department Number: text input

A note above the form states: 'Fields marked with * can not be empty.'

6.9. Enable Ports

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

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

AVAYA Application Enablement Services Management Console

Welcome: User: ovt
Last login: Fri Dec 19 18:57:35 2014 from 10.10.30.66
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.10-0
Server Date and Time: Mon Jan 05 11:19:07 EST 2015
HA Status: Not Configured

Networking (Ports) Home | Help | Logout

Ports

CVLAN Ports Enabled Disabled

Unencrypted TCP Port	9999	<input checked="" type="radio"/> <input type="radio"/>
Encrypted TCP Port	9998	<input type="radio"/> <input checked="" type="radio"/>

DLG Port TCP Port 5678

TSAPI Ports Enabled Disabled

TSAPI Service Port	450	<input checked="" type="radio"/> <input type="radio"/>
Local TLINK Ports		
TCP Port Min	1024	
TCP Port Max	1039	
Unencrypted TLINK Ports		
TCP Port Min	1050	
TCP Port Max	1065	
Encrypted TLINK Ports		
TCP Port Min	1066	
TCP Port Max	1081	

DMCC Server Ports Enabled Disabled

Unencrypted Port	4721	<input checked="" type="radio"/> <input type="radio"/>
Encrypted Port	4722	<input type="radio"/> <input checked="" type="radio"/>
TR/87 Port	4723	<input type="radio"/> <input checked="" type="radio"/>

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:

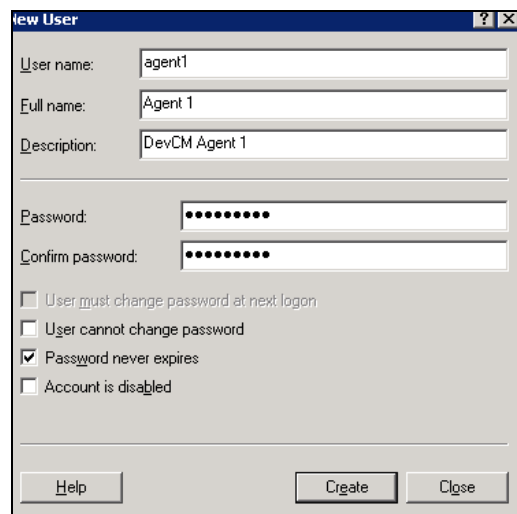
- Configure Windows users.
- Configure CCT Server.

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). Ensure that the Contact Center is equipped with the essential licenses. In Contact Center there are two modes of operation – Corporate and Nodal. The Nodal licenses that would be needed are **LM_CONTACTRECN** and **LM_OIN**. The equivalent Corporate licenses that would be needed are **LM_CONTACTRECC** and **LM_OIC**. During compliance testing, Contact Center used the Corporate licenses.

7.1. 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 screenshot shows the 'New User' dialog box with the following fields and options:

- 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
- Buttons: Help, Create, Close

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



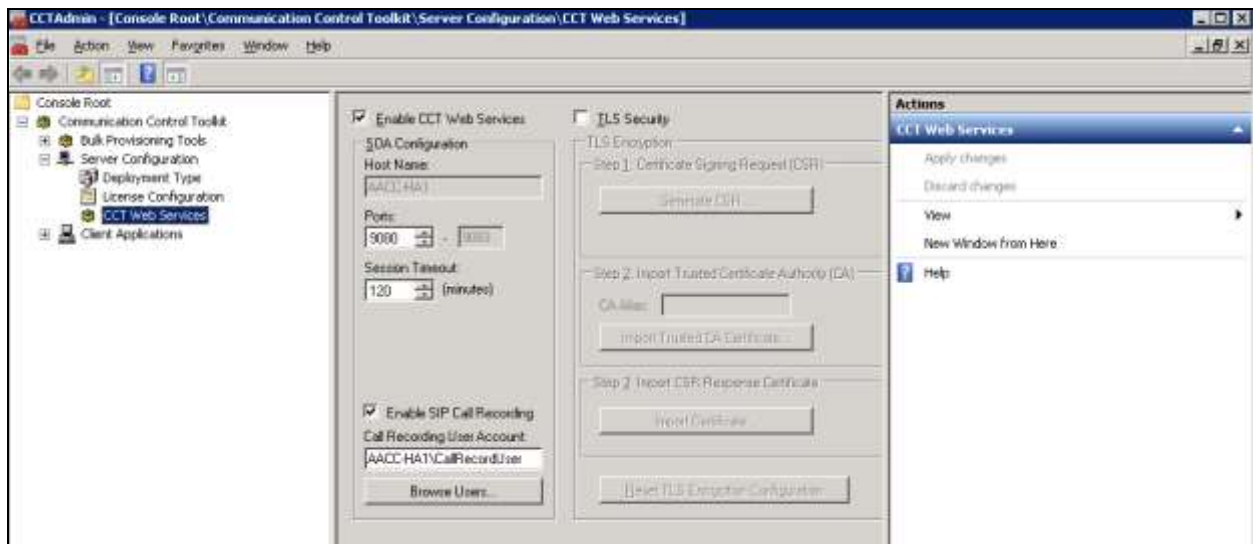
Repeat the same procedure to create “CallRecordUser” that is used for configuring in the CCT Web services for the Encore application.

7.2. 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 “9080”. 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.
- **Enable SIP Call Recording:** Select the box.
- **Call Recording User Account:** Enter the “AACC-HA1\CallRecordUser” as created in **Section 7.1**. 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).

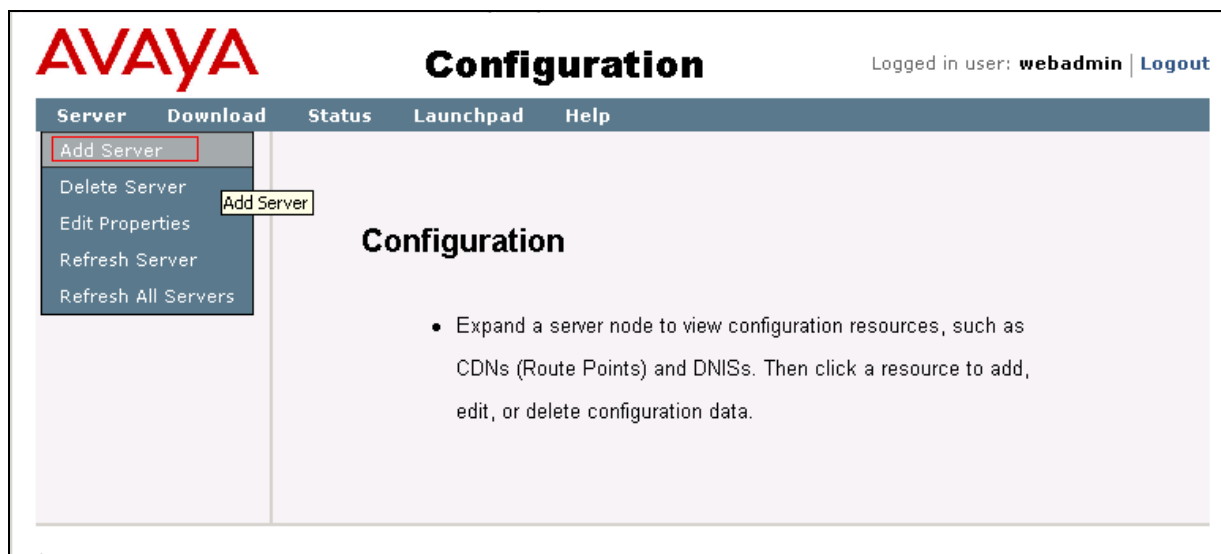
In order to access CCT Administration web page, the CCT server needs to be added into Contact Center Manager Administer (CCMA). Launch CCMA web page, by entering IP address or hostname of CCMA into the address box of a browser as shown below. Note that the IP address of CCMA needs to be added into the **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 screenshot shows the AVAYA Configuration window. On the left, a tree view lists 'AACC-HA1' and 'AACC-HA1-CCT'. The 'Server Properties' form is active, with fields for Type (set to CCT), Server Name (AACC-HA1), IP Address (10.10.97.52), Display Name (AACC-HA1-CCT), Login ID, Password, and DDI Prefix (CCT). A 'Port Number' field is set to 8081. A message states: 'The following ODBC DSN will be automatically created for this system: CCT_135.90.52.52_DSN'. The CCT Website URL is <http://AACC-HA1:8081/AvayaAurac>. On the right, the 'Associated CCMS Servers' section shows 'Server (1)' as AACC-HA1. A 'Submit' button is at the bottom.

The screen below shows the newly added CCT server.

The screenshot shows the AVAYA Configuration window with the 'CCT Administration' section selected. It displays the 'CCT Administration URL' as <http://AACC-HA1:8081/AvayaAurac>. A 'Launch CCT Console' button is visible. The top right corner shows 'Server: AACC-HA1'.

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.

The screenshot shows the AVAYA CCT Administration console. The header includes the AVAYA logo and 'CCT Administration'. A sidebar on the left has links for 'Tools', 'Monitoring', 'Design', and 'Provision'. The main area features the AVAYA logo and the text 'Avaya Aura Contact Center Communication Control Toolkit'. At the bottom, it says 'Manage your Communication Control Toolkit'. The footer indicates 'Version: 8.2' and 'Page 1 of 112'.

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 7.1**.

AVAYA CCT Administration Logged in as: webadmin

Update CCT User

User Details

Login User Name	AAACC-HA1\CallRecordUser
First Name	Call
Last Name	Recorder

Address Assignments

Terminal Assignments

Terminal Group Assignments

Address Group Assignments

Agent Assignments

Save

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.

AVAYA CCT Administration Logged in as: webadmin

Update CCT Provider

Basic Provider Information

Provider Name	Passive
IP Address	10.10.97.52
Port	5060

Provider Type: SIP Contact Center

Provider Configuration

Transport	TCP
-----------	-----

Save

8. Configure dvsAnalytics Encore

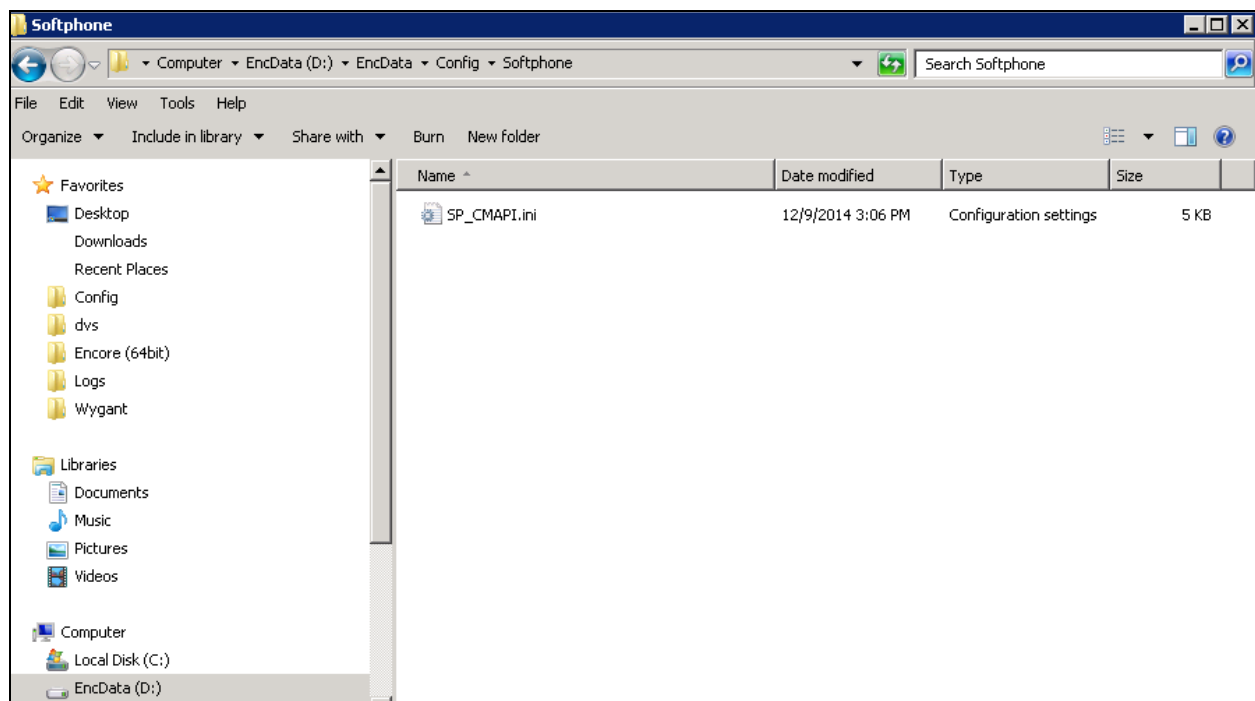
This section provides the procedures for configuring Encore. The procedures include the following areas:

- Administer Softphones
- Administer CTISetup
- Administer CT Gateway
- Administer CTISetup for Contact Center Data Collection
- Administer CT Gateway for Contact Center Data Collection

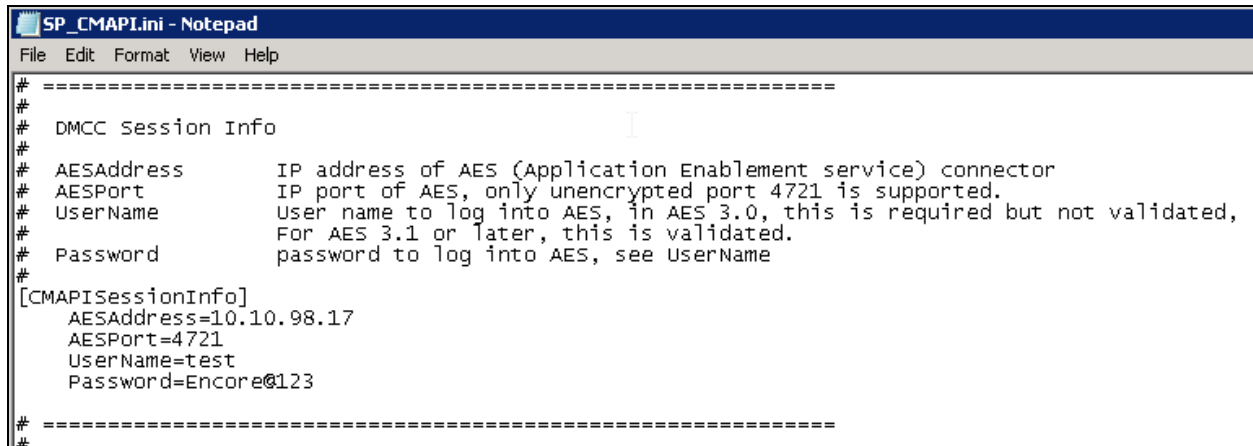
The configuration of Encore is performed by dvsAnalytics installers and dealers. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Administer Softphones

From the Encore server, navigate to the **D:\EncData\Config\Softphone** directory to edit the **SP_CMAPI.ini** file shown below.



Scroll down to the **DMCC Session Info** sub-section. Under **CMAPISessionInfo**, set **AESAddress** to the IP address of the Application Enablement Services server. Set **UserName** and **Password** to the Encore user credentials from **Section 6.8**. Retain the default value for the remaining fields.



```
# =====
#
# 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=Encore@123
# =====
#
```

Scroll down to the **DMCC softphones** sub-section. Under **Softphone1**, set **Extension** and **Password** to the first virtual IP softphone extension and security code from **Section 5.8**. Set **SwitchAddr** to the IP address of the H.323 Gatekeeper from **Section 6.4**. Set **RTPAddress** to the IP address of the Encore server. Retain the default values for the remaining fields.

Create additional softphone entries as necessary. In the compliance testing, four softphones were configured to correspond to the four virtual IP softphones from **Section 5.8**.

```
SP_CMAPI.ini - Notepad
File Edit Format View Help
# =====
#
# DMCC softphones
# one section per softphone
#
# Extension      extension for the softphone, must be already administered on the switch
# SwitchAddr     IP address of Avaya communication manager (ACM) or CLAN
# SwitchName     symbolic name of ACM (either this or SwitchAddr must be defined)
#                SwitchName is preferred but need requires H.323 Gatekeeper administer on AES.
#                Note that SwitchName is case sensitive.
# Password;      password for softphone, must be administered in ACM.
#                This is the station's "Security code"
# RTPAddress     IP address where AES will direct RTP to.  ie. IP address of computer running
#                the audio server.
# 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=10.10.97.29
Codec=g711U

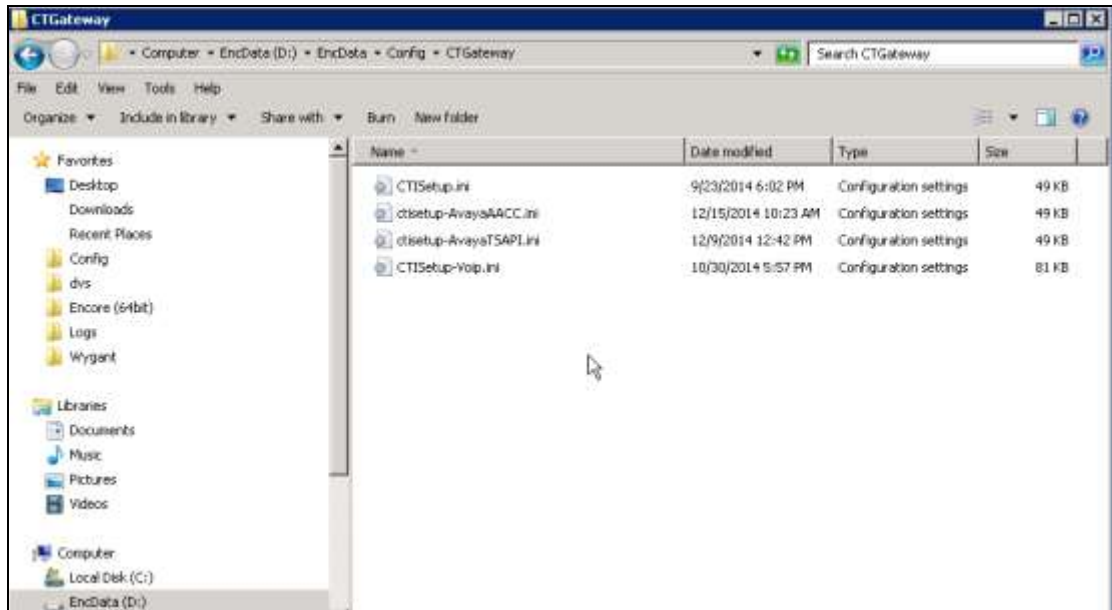
[SoftPhone2]
Extension=53021
Password=1234
# SwitchName=cm
SwitchAddr=10.10.97.201
RTPAddress=10.10.97.29
Codec=g711U

[SoftPhone3]
Extension=53022
Password=1234
# SwitchName=cm
SwitchAddr=10.10.97.201
RTPAddress=10.10.97.29
Codec=g711U

[SoftPhone4]
Extension=53023
Password=1234
# SwitchName=cm
SwitchAddr=10.10.97.201
RTPAddress=10.10.97.29
Codec=g711U
```


8.2. Administer CTISetup

Navigate to the **D:\EncData\Config\CTGateway** directory to edit the **ctisetup-AvayaTSAPI.ini** file.

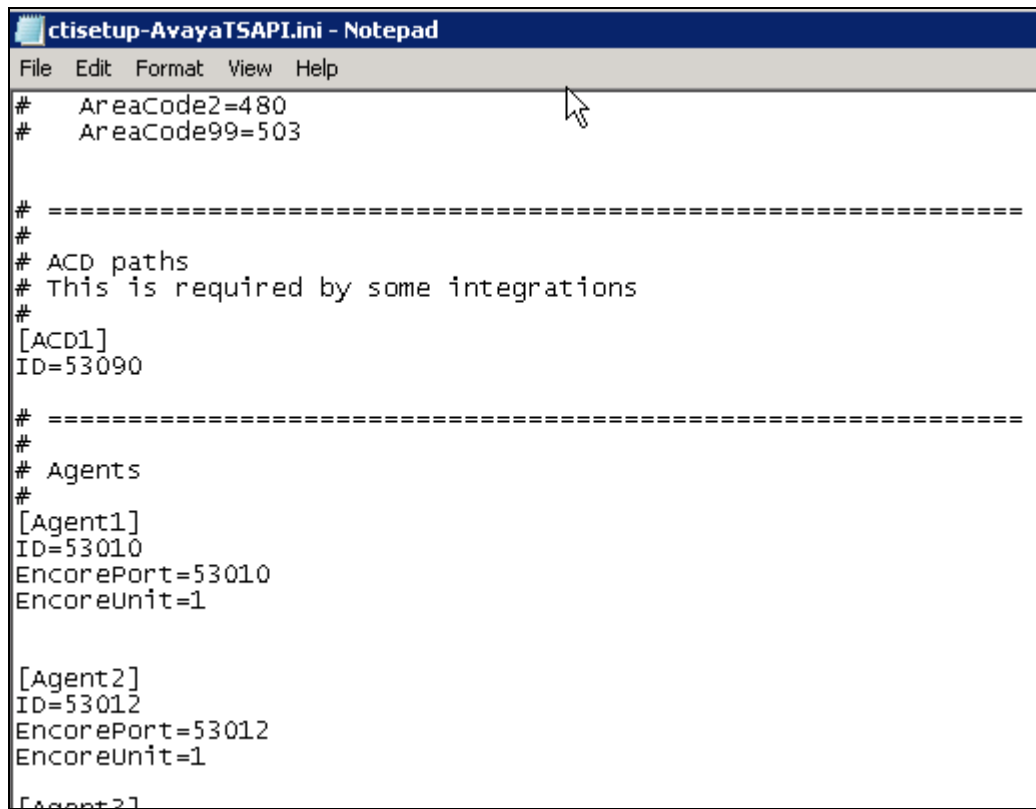


Scroll down to the **Encore ECAPI** sub-section. Under **ECAPI1**, make sure all parameters are set to the default values shown below.

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

# =====
#
# Encore ECAPI
#
[ECAPI1]
    ID=RecEngine
    Address=127.0.0.1
    Port=1503
    Trunk-Field=fldTrunk
    Agent-Field=fldExtension
    ANI-Field=fldANI
    DNIS-Field=fldDNIS
    ID-Field=fldID
    DATA-Field=fldData
    ACD-Field=fldACD
    AgentID-Field=fldAgentLoginID
    NOSTART=NO
    NOSTOP=NO
    AgentEncorePortoverridePort-Field=No
    Port-Field=.AGENT
    DefaultEncoreUnit=1
    TrimPortPrefix=No
#
#
#
```

Scroll to the **Agents** sub-section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section** Error! Reference source not found.. Create additional agent entries as necessary when more than one agent is being monitored.



```
ctisetup-AvayaTSAPI.ini - Notepad
File Edit Format View Help
# AreaCode2=480
# AreaCode99=503

# =====
#
# ACD paths
# This is required by some integrations
#
[ACD1]
ID=53090

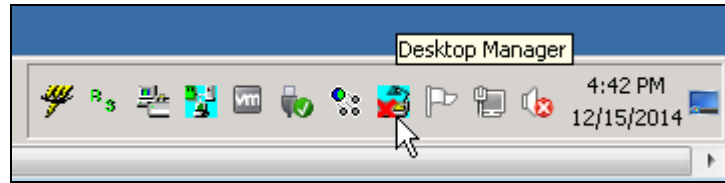
# =====
#
# Agents
#
[Agent1]
ID=53010
EncorePort=53010
EncoreUnit=1

[Agent2]
ID=53012
EncorePort=53012
EncoreUnit=1

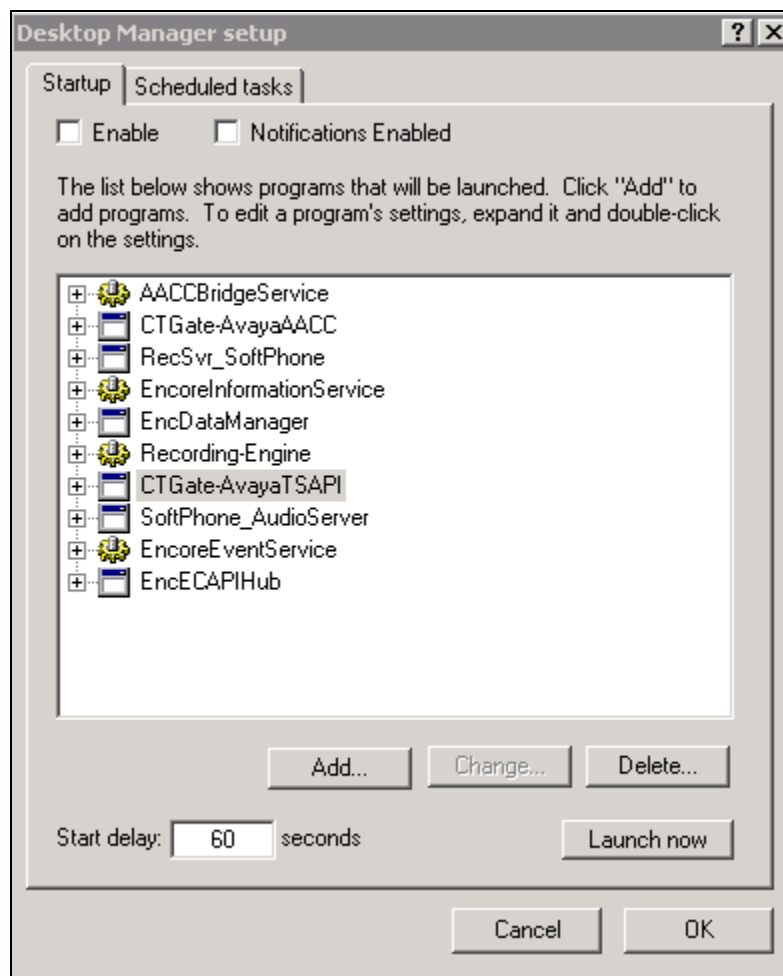
[Agent3]
```

8.3. Administer CT Gateway

Right click on the **Desktop Manager** icon from the system tray, as shown below and choose **Configure** (not shown).



The **Desktop Manager setup** window is displayed as shown below. Select **CTGate-AvayaTSAPI** program from the **Startup** tab and click on the **Launch now** button.



The **CTISetup-AvayaTSAPI.ini** screen is displayed. Select **PBX → Configure** from the top menu.



The **PBX interface setup** screen is displayed. Select the Tlink name from **Section 6.7** from the drop-down list, and enter the Encore user credentials from **Section 6.8** for **Login ID**, **Password**, and **Confirm Password**. Retain the default values in the remaining fields, as shown below.

Click on drop-down button below to select a Tserver

AVAYA#CLAN2#CSTA#AES63

*Tserver: AVAYA#CLAN2#CSTA#AES63

*Login ID test

*Password ***** Confirm password *****

☒ Alarm on Monitor-ended event Debug logging 9

☒ Alarm on device monitor failure ☐ Capture UUI data

☐ *Agent list from ACD

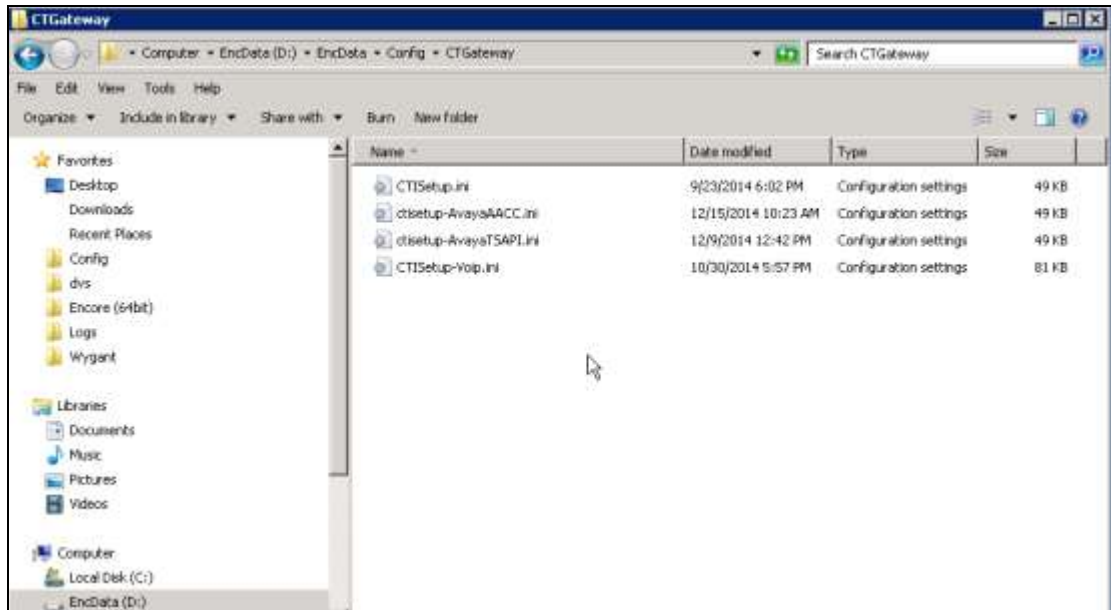
* Requires restart of CTGateway

OK Cancel

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

8.4. Administer CTISetup for Contact Center Data Collection

Navigate to the **D:\EncData\Config\CTGateway** directory to edit the **ctisetup-AvayaAACC.ini** file.



Scroll to the **Agents** sub-section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section Error! Reference source not found.** Create additional agent entries as necessary when more than one agent is being monitored.

```
ctisetup-AvayaAACC.ini - Notepad
File Edit Format View Help

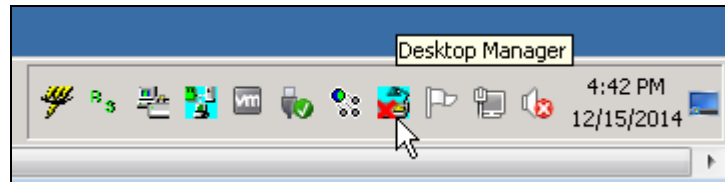
# =====
#
# ACD paths
# This is required by some integrations
#
#[ACD1]
#ID=2900

# =====
#
# Agents
#
[Agent1]
ID=53010
EncorePort=53010
EncoreUnit=1

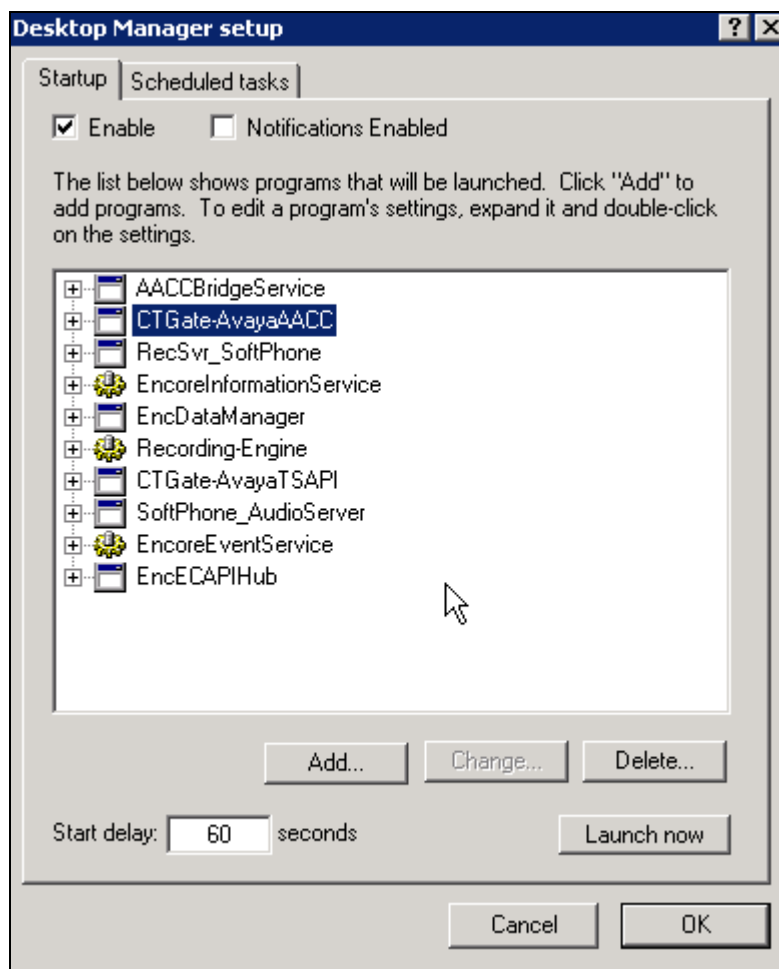
[Agent2]
ID=53012
EncorePort=53012
EncoreUnit=1
```

8.5. Administer CT Gateway for Contact Center Data Collection

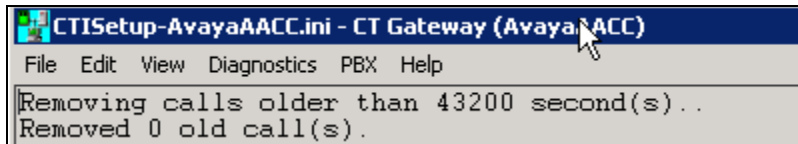
Right click on the **Desktop Manager** icon from the system tray, as shown below and choose **Configure** (not shown).



The **Desktop Manager setup** window is displayed as shown below. Select **CTGate-AvayaAACC** program from the **Startup** tab and click on the **Launch now** button.



The **CTISetup-AvayaAACC.ini-CT Gateway (AvayaAACC)** screen is displayed. Select **PBX** → **Configure** from the top menu.



The **PBX interface setup** window is displayed. Enter the values as shown 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:** “9080” as configured in **Section 7.2**.
- **AACC SIP Domain:** “bvwddev.com” was configured on the AACC.
- **CCT web service user ID:** “AACC-HA1\CallRecordUser” as configured in **Section 7.1**.
- **CCT web service user password:** The password that was configured in **Section 7.1**.
- **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 “10.10.97.29” 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: 9080

*AACC SIP Domain: bvwdev.com

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

*CCT web service user password: xxxxxxxxxxxx

Confirm CCT web service user password : xxxxxxxxxxxx

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: [REDACTED]

Confirm CCMA web service user password : [REDACTED]

Encore AACC Bridge Windows service

*Server name / IP address: 10.10.97.29

CT Gateway connects to this IP Port: 1566

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

☒ *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 CTGateways for the **CTGate-AvayaAACC** application again.

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	AES63	established	21	21

Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone extensions from **Section 5.88** are displayed along with the IP address of the Application Enablement Services server, as shown below.

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

Page 2

REGISTERED IP STATIONS						
Station or Orig	Ext Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper	IP Address
53015		4620	IP_Phone	y	10.10.5.12	
		1	2.300		10.10.97.201	
53016		9620	IP_Phone	y	10.10.5.3	
		1	6.3116		10.10.97.201	
53018		4620	IP_Phone	y	10.10.5.61	
		1	6.4014		135.10.97.201	
53020		9650	IP_API_A	y	10.10.98.17	
		1	3.2040		10.10.97.201	
53021		4620	IP_API_A	y	10.10.98.17	
		1	3.2040		10.10.97.201	
53022		4620	IP_API_A	y	10.10.98.17	
		1	3.2040		10.10.97.201	
53023		4620	IP_API_A	y	10.10.98.17	
		1	3.2040		10.10.97.201	

9.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section Error! Reference source not found.**

The screenshot displays the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user 'cst' with login details. A red status bar indicates the current page is "Status | Status and Control | TSAPI Service Summary".

The left sidebar contains a tree view of navigation options: All Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The Status section is expanded, showing sub-items like Alarm Viewer, Log Manager, Logs, Status and Control, and various service summaries (CVLAN, DLG, DMCC, Switch Conn, and TSAPI Service Summary).

The main content area is titled "TSAPI Link Details" and includes a refresh toggle set to 60 seconds. Below this is a table with the following data:

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Misses to Switch	Misses from Switch	Misses Period
@	1	CLAN2	1	Talking	Fri Dec 19 10:44:44 2014	Online	16	3	21	21	30

Below the table are "Online" and "Offline" buttons. A section for "For service-wide information, choose one of the following" contains buttons for "TSAPI Service Status", "Link Status", and "User Status".

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

Verify the **User** column shows an active session with the Encore user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of configured softphones from **Section 8.1**.

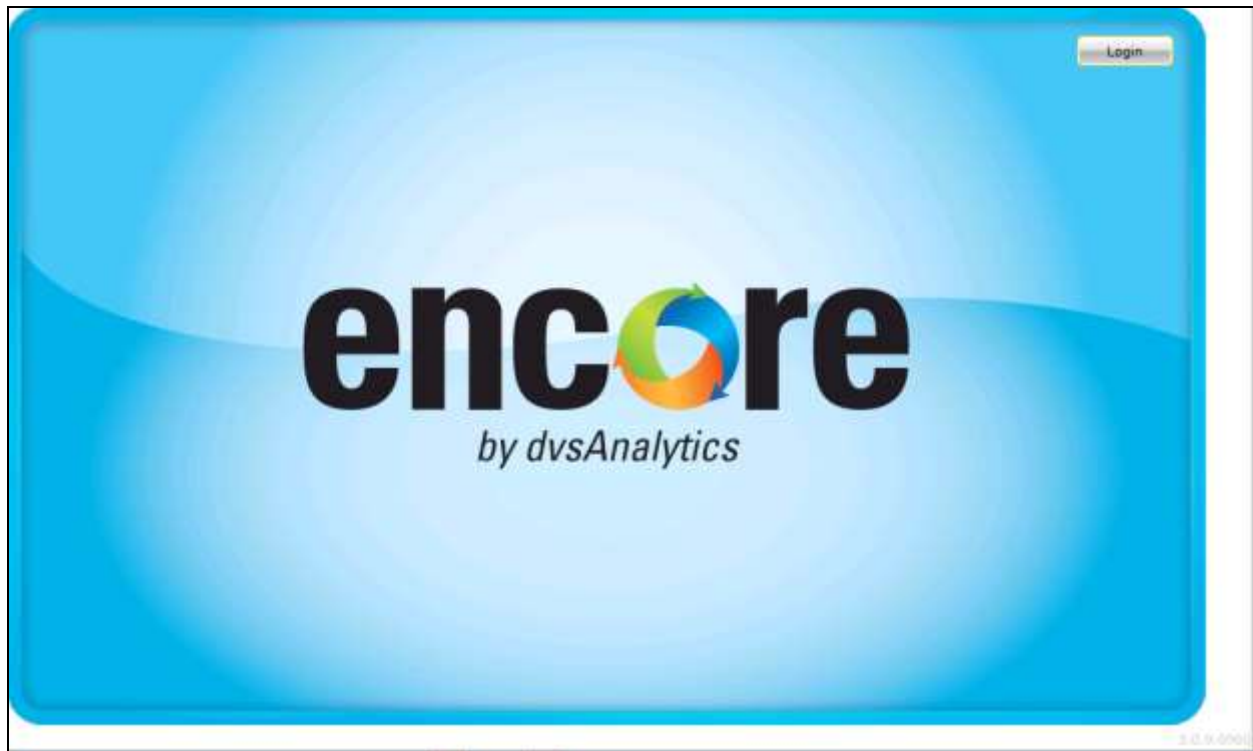
The screenshot displays the Avaya Application Enablement Services Management Console. The left navigation pane shows the 'Status' menu expanded, with 'Status and Control' selected. The main content area is titled 'DMCC Service Summary - Session Summary'. It includes a 'Please do not use back button' warning, a refresh timer set to 60 seconds, and session statistics: Service Uptime (16 days, 16 hours 40 minutes), Number of Active Sessions (1), Number of Sessions Created Since Service Boot (1), Number of Existing Devices (4), and Number of Devices Created Since Service Boot (4). A table lists the active session details.

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
88F53731642024871:2825507C0224C25-0	test	SPAS1	10.10.97.29	XML Unencrypted	4

Below the table are buttons for 'Terminate Sessions' and 'Show Terminated Sessions'. A pagination bar at the bottom indicates 'Page 1 of 1' and '1' of '00'.

9.3. Verify dvsAnalytics Encore

Log an agent into the skill group to handle and complete an ACD call. Access the Encore web interface by using the URL “http://ip-address/encore” in an Internet browser window, where “ip-address” is the IP address of the Encore server. The **encore** screen is displayed. Click **Login** and log in using the appropriate credentials.



The **encore** screen is updated with a list of call recordings. Verify that there is an entry in the right pane reflecting the last call, with proper values in the relevant fields.

Date	Time	Duration	Extension	AM	DMES	Call Direction	Call Type	Consultation call	Recorded Party Name	Recorded Party Number	Other Party Name	Other Party Number
1/15/2015	4:05:50 PM	00:00:48	53010	4081	53010	Incoming	External	<input type="checkbox"/>	H.323 53010	53009		4081
1/15/2015	4:05:47 PM	00:00:12	53012	4081	53010	Incoming	External	<input type="checkbox"/>	H.323 53012	53002		4081
1/15/2015	4:03:19 PM	00:00:09	53000	4081	53010	Incoming	External	<input type="checkbox"/>	Agent 1	53009		4081
1/15/2015	5:59:42 PM	00:00:25	53012	4081	53010	Incoming	External	<input type="checkbox"/>	H.323 53012	53002		4081
1/15/2015	3:08:42 PM	00:00:11	53002	40810	53012	Outgoing	Internal	<input checked="" type="checkbox"/>	H.323 53012	53009	H.323 53012	53010
1/15/2015	3:08:25 PM	00:00:11	53000	4081	53010	Incoming	External	<input type="checkbox"/>	Agent 1	53009		4081
1/15/2015	3:04:44 PM	00:00:18	53012	4081	53010	Incoming	External	<input type="checkbox"/>	H.323 53012	53002		4081
1/15/2015	3:04:18 PM	00:00:12	53000	4081	53010	Incoming	External	<input type="checkbox"/>	Agent 1	53009		4081

Right click on the entry and select **Play** to listen to the playback. Verify that the screen is updated and that the call recording is played back.

The screenshot displays the AACP interface. The top section is a table listing call recordings. The bottom section shows a playback control bar with a waveform and various playback controls.

Time	Call ID	Call Type	Direction	Agent	Call Status	Call Duration	Call Start Time	Call End Time	Call Recording Length
1/19/2015 4:03:47 PM	33012	90-08-12	33012	4801	33010	Incoming	External		H.323, 33012
1/19/2015 4:03:49 PM	33018	90-08-08	33018	4801	33010	Incoming	External		Agent 1
1/19/2015 3:58:42 PM	33012	90-08-08	33012	4801	33010	Incoming	External		H.323, 33012
1/19/2015 3:58:42 PM	33018	90-08-11	33018	33018	33012	Outgoing	Internal		H.323, 33018
1/19/2015 3:58:25 PM	33018	90-08-11	33018	4801	33010	Incoming	External		Agent 1
1/19/2015 3:54:48 PM	33012	90-08-18	33012	4801	33018	Incoming	External		H.323, 33012
1/19/2015 3:54:28 PM	33018	90-08-12	33018	4801	33010	Incoming	External		Agent 1
1/19/2015 3:49:44 PM	33012	90-08-21	33012	4801	33010	Incoming	External		H.323, 33012
1/19/2015 3:49:44 PM	33018	90-08-10	33018	33018	33012	Outgoing	Internal		H.323, 33018
1/19/2015 3:49:30 PM	33018	90-08-08	33018	4801	33010	Incoming	External		Agent 1
1/19/2015 3:43:38 PM	33018	90-08-10	33018	33018	33010	Outgoing	Internal		H.323, 33018
1/19/2015 3:42:50 PM	33012	90-08-08	33012	4801	33010	Incoming	External		Agent 1
1/19/2015 3:38:15 PM	33018	90-08-23	33018	6149754403	10980450018	Incoming	External		H.323, 33018
1/19/2015 3:37:36 PM	33018	90-08-01	33018	4801	33010	Incoming	External		Agent 1
1/19/2015 3:32:30 PM	33018	90-08-11	33018	33018	33010	Outgoing	Internal		H.323, 33018
1/19/2015 3:32:09 PM	33018	90-08-11	33018	4801	33010	Incoming	External		Agent 1
1/19/2015 3:27:30 PM	33018	90-08-19	33018	4801	33010	Incoming	External		Agent 1

Recording Player: 33018(33018)
 Status: 0:08:30.000 Recording Length: 0:08:30.000

Video Unavailable

Playback controls: Play, Stop, Previous, Next, Full Screen, Volume, and a progress bar.

10. Conclusion

These Application Notes describe the configuration steps required for dvsAnalytics Encore to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Contact Center using Service Observing and CCT web services. All feature and serviceability test cases were completed with observations noted in **Section Error! Reference source not found..**

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02-300357, Release 6.3.
3. *Administering Avaya Aura® Session Manager*, Issue 7, Release 6.3.
4. *Administering Avaya Aura® System Manager*, Issue 6, Release 6.3.
5. *Avaya Aura® Contact Center SIP Commissioning*, Doc# NN44400-511.
6. *Avaya Aura® Contact Center Configuration – Avaya Aura Unified Communications Platform Integration*, 44400-52, Issue 05.03, Release 6.4.

The following product documentation is available by contacting dvsAnalytics.

Avaya AuraTM Communication Manager TSAPI Integration Guide, Encore Version 6.0.1, October 3, 2014, available from dvsAnalytics Support.

Avaya AuraTM Communication Manager TSAPI Installation Addendum, Release 2.3.5, October 20, 2014, available from dvsAnalytics Support.

©2015 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.