



Avaya Solution & Interoperability Test Lab

Application Notes for dvsAnalytics Encore with Avaya Proactive Contact with PG230 and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for dvsAnalytics Encore to interoperate with Avaya Proactive Contact with PG230 and Avaya Aura® Application Enablement Services. dvsAnalytics Encore is a call recording solution.

In the compliance testing, dvsAnalytics Encore used the Event Services interface from Avaya Proactive Contact and the Telephony Services Application Programmer Interface from Avaya Aura® Application Enablement Services to obtain information on agent states and calls, and used the Service Observing feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture the media associated with the monitored agents for call recording.

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

1. Introduction

These Application Notes describe the configuration steps required for dvsAnalytics Encore to interoperate with Avaya Proactive Contact with PG230 and Avaya Aura® Application Enablement Services. dvsAnalytics Encore is a call recording solution.

In the compliance testing, dvsAnalytics Encore used the Event Services interface from Avaya Proactive Contact and the Telephony Services Application Programmer Interface (TSAPI) from Avaya Aura® Application Enablement Services to obtain information on agent states and calls, and used the Service Observing feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with the monitored agents for call recording.

The Event Services and TSAPI interfaces are used by dvsAnalytics Encore to monitor the agent stations and calls, and the DMCC interface is used by dvsAnalytics Encore to register virtual IP softphones to pick up the media for call recording. dvsAnalytics Encore starts the call recording by sending a Service Observing button press from a virtual IP softphone via the DMCC interface to observe the active call. The Event Services and/or TSAPI event reports are also used to determine when to stop the call recordings.

This compliance test covered the recording of calls using the Avaya Proactive Contact with PG230 deployment option.

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 registers virtual IP softphones to Communication Manager using DMCC, requests monitoring on the skill groups and agent stations using TSAPI, and requests monitoring of agent states and call events using Event Services.

For the manual part of the testing, each call was handled manually on the agent station with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the Proactive Contact Agent application to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to Encore. The verification of tests included using the Encore logs for proper message exchanges, and using the Encore web interface for proper logging and playback of calls.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Encore:

- Handling of Event Services agent states and call events.
- Handling of TSAPI messages in the areas of event notification and value queries.
- Use of DMCC registration services to register and un-register virtual IP softphones.
- Use of DMCC physical device services to activate Service Observing for virtual IP softphones to obtain the media.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, agent drop, customer drop, hold, reconnect, simultaneous calls, conference, transfer, unsupervised forward work, agent blending, and call blending scenarios.

The serviceability testing focused on verifying the ability of Encore to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to Encore.

2.2. Test Results

All test cases were executed. The following were the observations on Encore from the compliance testing.

- Recordings for supervised forward work scenarios are not supported in this release of Encore.
- All recordings included the confirmation tone for the Service Observing activation, and may cover up the first couple of seconds of the user conversation.
- The recording playback via the web interface may experience random short loud noise at the end of the recording.
- Short connections to announcements may be included as separate recording entries.
- Held scenario produced two recording entries.
- Recording entries for inbound calls over blend and inbound jobs contained blank DNIS.
- 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.
- Upon each link disruption, a new Event Services connection is created with the old one still in existence. The multiple connections have no harmful effects other than tying up more ports than necessary.
- Upon a link disruption, call before and after the disruption may be merged into one recording.

2.3. Support

Technical support on Encore can be obtained through the following:

- **Phone:** (800) 910-4564
- **Email:** Support@dvsAnalytics.com

3. Reference Configuration

The detailed administration of basic connectivity between Communication Manager and Proactive Contact, between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Encore monitored the skill group and agent station extensions shown in the table below. Note that the skill groups are associated with the inbound ACD for the agent blending mode.

Contact Center Device Type	Extension
Skill Group	41410, 41412
Agent Station	65001, 65002

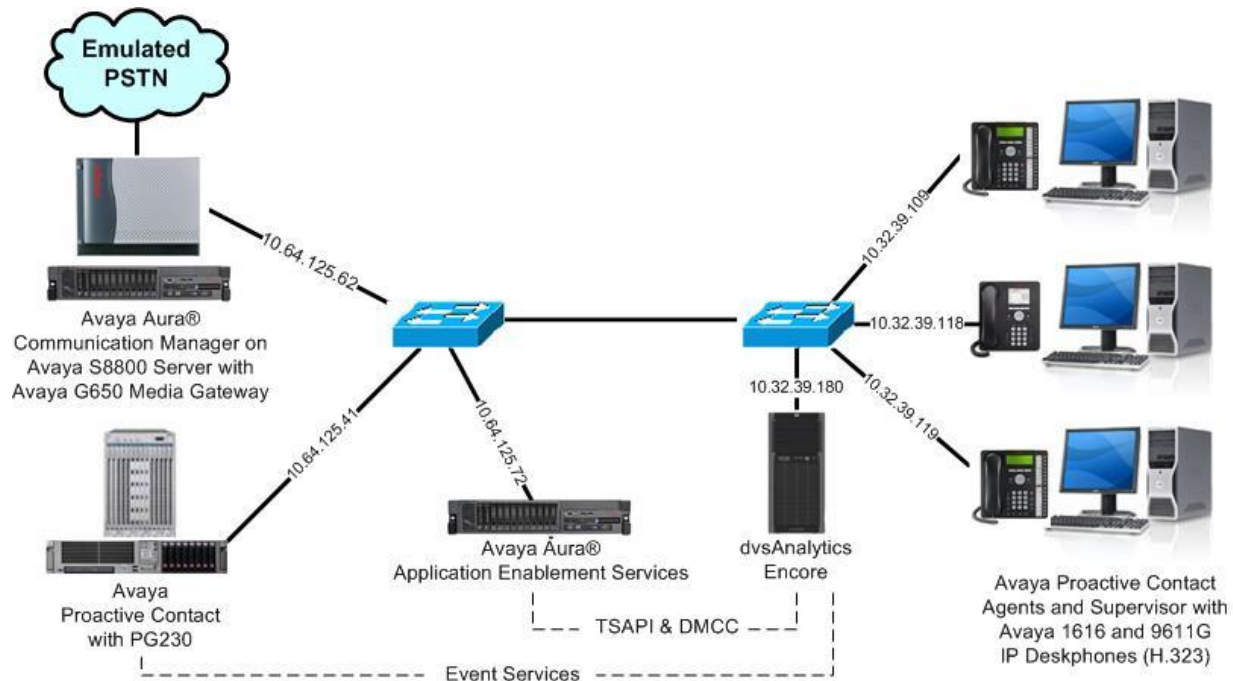


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP7 (R016x.00.1.510.1-19528)
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN799DP C-LAN Circuit Pack• TN2302AP IP Media Processor	HW01 FW040 HW12 FW121
Avaya Aura® Application Enablement Services	6.1.2
Avaya Proactive Contact with PG230	5.0.1
Avaya Proactive Contact Agent	5.0.1
Avaya Proactive Contact Supervisor	5.0.1
Avaya 1616 IP Deskphones (H.323)	1.302S
Avaya 9611G IP Deskphone (H.323)	6.020S
dvsAnalytics Encore on Windows Server 2008 R2 Standard <ul style="list-style-type: none">• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC SDK• Avaya Event Services SDK (TAO.dll)	2.3.3 6.1.1.469 6.2 1.6a_p8

5. Configure Avaya Aura® Communication Manager

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

- Verify License
- Administer system parameters features
- Administer IP codec set
- Administer class of restriction
- Administer virtual IP softphones
- Administer agent stations

5.1. Verify License

Log in to the System Access Terminal (SAT) 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	

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	

5.2. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Allow Two Observers in Same Call**, which is located on **Page 11**. Set **Service Observing: Warning Tone** as desired.

```
change system-parameters features                                     Page 11 of 19
                                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 Allowed with Exclusion? n
    Allow Two Observers in Same Call? y
```

5.3. 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 7                                             Page 1 of 2
                                IP Codec Set

  Codec Set: 7

  Audio      Silence      Frames      Packet
  Codec      Suppression  Per Pkt   Size(ms)
1: G.711MU    n           2        20
2:
```


5.4. 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 agents and to the virtual IP softphones used by Encore.

change cor 2	Page 1 of 23
CLASS OF RESTRICTION	
COR Number: 2	
COR Description:	
FRL: 0	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? n	Direct Agent Calling? n
Restriction Override: none	Facility Access Trunk Test? n
Restricted Call List? n	Can Change Coverage? n

5.5. Administer Virtual IP Softphones

Add a virtual 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.

- **Type:** “4610”
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **COR:** The class of restriction number from **Section 5.4**.
- **IP SoftPhone:** “y”

add station 65991	Page 1 of 5
STATION	
Extension: 65991	Lock Messages? n
Type: 4610	Security Code: 65991
Port: IP	Coverage Path 1:
Name: Encore Virtual #1	Coverage Path 2:
	Hunt-to Station:
STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
	Personalized Ringing Pattern: 1
Speakerphone: 2-way	Message Lamp Ext: 65991
Display Language: english	Mute Button Enabled? y
Survivable GK Node Name:	
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? y
	IP Video Softphone? n

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

add station 65991		Page 4 of 6
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	7:	
2: call-appr	8:	
3: call-appr	9:	
4: serv-obsrv	10:	
5:	11:	

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 65991 count 4									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack	
65991	S00040	Encore Virtual #1				2			
	4610		no			1	1		
65992	S00043	Encore Virtual #2				2			
	4610		no			1	1		
65993	S00046	Encore Virtual #3				2			
	4610		no			1	1		
65994	S00052	Encore Virtual #4				2			
	4610		no			1	1		

5.6. Administer Agent Stations

Use the “change station n” command, where “n” is the first agent station extension from **Section 3**. For **COR**, enter the class of restriction number from **Section 5.4**.

```
change station 65001
```

		Page	1 of	5
STATION				
Extension: 65001	Lock Messages? n	BCC: 0		
Type: 1616	Security Code: *	TN: 1		
Port: S00006	Coverage Path 1:	COR: 2		
Name: Encore Agent #1	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
Loss Group: 19	Time of Day Lock Table:			
	Personalized Ringing Pattern: 1			
Speakerphone: 2-way	Message Lamp Ext: 65001			
Display Language: english	Mute Button Enabled? y			
Survivable GK Node Name:	Button Modules: 0			
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? n			
	IP Video Softphone? n			
	Short/Prefixed Registration Allowed: default			

Repeat this section to administer all stations to be monitored. In the compliance testing, two stations were administered as shown below.

```
list station 65001 count 2
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack	
65001	S00006	Encore Agent #1				2			
	1616		no			1	1		
65002	S00031	Encore Agent #2				2			
	9620		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:

- Verify license
- Launch OAM interface
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Encore user
- Enable DMCC unencrypted port

6.1. Verify License

Access the Web License Manager interface by using the URL “https://ip-address:52233/WebLM/ index.jsp” in an Internet browser window, where “ip-address” is the IP address of the license server.

The **Web License Manager** screen is displayed. Log in using the appropriate credentials.

The image shows the Avaya Web License Manager (WebLM v4.6) login interface. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Web License Manager (WebLM v4.6)". The main heading is "Logon". There are two input fields: "User Name:" and "Password:". Below the password field is a dark gray button with a white right-pointing arrow.

The **Web License Manager** screen below is displayed. Select **Licensed Products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

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

Web License Manager (WebLM v4.6)
Logoff

Install License

Licensed Products

▼ APPL_ENAB

Application_Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: May 11, 2012 5:07:47 PM MDT

[View Peak Usage](#)

Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_001, BasicUnrestricted, AdvancedUnrestricted; DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted; DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted; DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	16	0

6.2. 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 Management Console' is displayed. Below this, a red horizontal bar spans the width of the page. In the center, there is a light gray box with the text 'Please login here:'. Inside this box, there are two input fields: 'Username' and 'Password', each followed by a text input box. Below these fields is a 'Login' button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice '© Copyright © 2009-2010 Avaya Inc. All Rights Reserved.' is displayed.

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. To its right, the text 'Application Enablement Services Management Console' is displayed. In the top right corner, there is a welcome message: 'Welcome: User', 'Last login: Tue Jul 24 10:24:02 2012 from 10.32.39.20', 'HostName/IP: aes_125_72/10.64.125.72', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r6-1-2-32-0'. Below the header, a red horizontal bar contains the text 'Home | Help | Logout'. On the left side, there is a vertical navigation menu with the following items: 'AE Services', 'Communication Manager Interface', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area on the right 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:'. Below this text is a bulleted list of administrative domains: 'AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.', 'Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.', 'Licensing - Use Licensing to manage the license server.', 'Maintenance - Use Maintenance to manage the routine maintenance tasks.', 'Networking - Use Networking to manage the network interfaces and ports.', 'Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.', 'Status - Use Status to obtain server status informations.', 'User Management - Use User Management to manage AE Services users and AE Services user-related resources.', 'Utilities - Use Utilities to carry out basic connectivity tests.', and 'Help - Use Help to obtain a few tips for using the OAM Help system'. At the bottom of the main content area, there is a note: 'Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain.'

6.3. 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 “S8800”, 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' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The first row shows a connection named 'S8800' with 'No' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The 'Edit H.323 Gatekeeper' button is highlighted.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8800	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 H.323 gatekeeper, in this case “10.64.125.32” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8800' screen. The left navigation pane is the same as the previous screenshot. The main content area has a title 'Edit H.323 Gatekeeper - S8800'. Below the title is a text input field containing '10.64.125.32' and an 'Add Name or IP' button. Below the input field is the label 'Name or IP Address' and two buttons: 'Delete IP' and 'Back'.

6.4. 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, and click **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two unchecked checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services'. Below these is an 'Apply Changes' button. The top right corner displays user information: 'Welcome: User', 'Last login: Tue Jul 24 10:24:02 2012 from 10.32.39.20', 'HostName/IP: aes_125_72/10.64.125.72', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r6-1-2-32-0'. The top navigation bar shows 'Security | Security Database | Control' and 'Home | Help | Logout'.

6.5. Restart TSAPI Service

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller'. It contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked and 'Running'. Below the table is a link 'For status on actual services, please use [Status and Control](#)'. At the bottom are buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right corner displays user information: 'Welcome: User', 'Last login: Tue Jul 24 10:24:02 2012 from 10.32.39.20', 'HostName/IP: aes_125_72/10.64.125.72', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r6-1-2-32-0'. The top navigation bar shows 'Maintenance | Service Controller' and 'Home | Help | Logout'.

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

6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. Make a note of the applicable Tlink name, to be used later for configuring Encore.

In this case, the associated encrypted Tlink name is “AVAYA#S8800#CSTA-S#AES_125_72”, which was created as part of the basic connectivity with Proactive Contact. Note the use of the switch connection “S8800” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security Database" expanded to show "Tlinks" selected. The main content area, titled "Tlinks", lists two Tlink names: "AVAYA#S8800#CSTA#AES_125_72" and "AVAYA#S8800#CSTA-S#AES_125_72". The second name is selected with a green radio button. A "Delete Tlink" button is visible below the list.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Fri Jul 27 10:16:14 2012 from 10.32.39.20
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-2-32-0

Security | Security Database | Tlinks Home | Help | Logout

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#S8800#CSTA#AES_125_72
☒ AVAYA#S8800#CSTA-S#AES_125_72

Delete Tlink

6.7. 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. Click **Apply** at the bottom of the screen (not shown below).

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message: 'Welcome: User', 'Last login: Tue Jul 24 10:24:02 2012 from 10.32.39.20', 'HostName/IP: aes_125_72/10.64.125.72', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r6-1-2-32-0'. Below the header is a red navigation bar with 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'. The left sidebar contains a tree view with categories: 'AE Services', 'Communication Manager Interface', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management' (expanded), 'Service Admin', 'User Admin' (expanded), 'Add User' (selected), 'Change User Password', 'List All Users', 'Modify Default Users', 'Search Users', 'Utilities', and 'Help'. The main content area is titled 'Add User' and contains a form with the following fields: '* User Id' (text box with 'encore'), '* Common Name' (text box with 'encore'), '* Surname' (text box with 'encore'), '* User Password' (password box with 8 dots), '* Confirm Password' (password box with 8 dots), 'Admin Note' (text box), 'Avaya Role' (dropdown menu with 'None' selected), 'Business Category' (text box), 'Car License' (text box), 'CM Home' (text box), 'Css Home' (text box), 'CT User' (dropdown menu with 'Yes' selected), 'Department Number' (text box), 'Display Name' (text box), 'Employee Number' (text box), and 'Employee Type' (text box). A note above the form states: 'Fields marked with * can not be empty.'

6.8. Enable DMCC Unencrypted Port

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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jul 24 10:24:02 2012 from 10.32.39.20
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-2-32-0

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

TR/87 Port4723

7. Configure Avaya Proactive Contact

This section provides the procedures for configuring Avaya Proactive Contact.

7.1. Obtain Host Name

Log in to the Linux shell of the Avaya Proactive Contact server. Use the “uname -a” command to obtain the host name, which will be used later for configuring Encore.

In the compliance testing, the host name of the Avaya Proactive Contact server is “lzpds4”, as shown below.

```
$ uname -a
Linux lzpds4b 2.6.18-238.1.1.el5PAE #1 SMP Tue Jan 4 13:53:16 EST 2011 i686 athlon
i386 GNU/Linux
LZPDS4B(admin)/opt/avaya/pds [1001]
$
```

8. Configure dvsAnalytics Encore

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

- Administer softphones
- Administer CTISetup
- Launch CT Gateways
- Administer CT Gateways

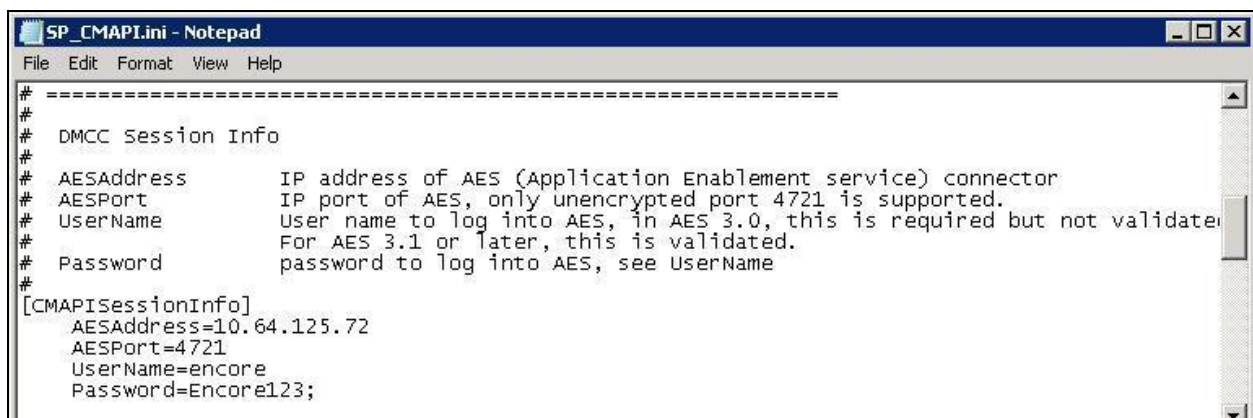
The configuration of Encore is performed by dvsAnalytics installers and dealers. The procedural steps are presented in these Application Notes for informational purposes.

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.

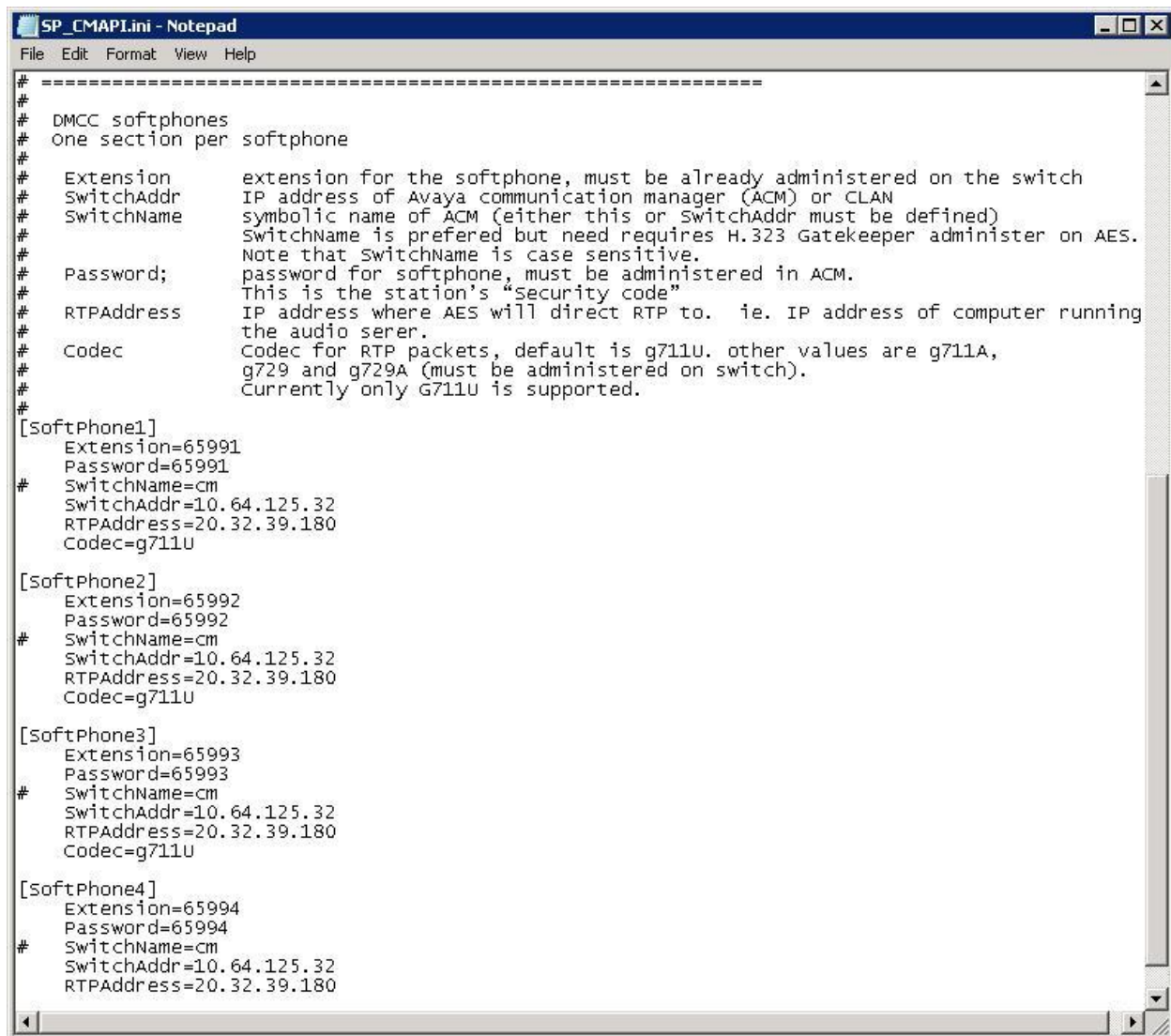


Scroll down to the **DMCC Session Info** section. Under **CMAPISessionInfo**, set **AESAddress** to the IP address of the Application Enablement Services server. Set **UserName** and **Password** to the Encore user credentials from **Section 6.7**. Retain the default value for **AESPort**.



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 5.5**. Set **SwitchAddr** to the IP address of the H.323 Gatekeeper from **Section 6.3**, or set **SwitchName** to the host name of the H.323 Gatekeeper. 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 5.5**.



```
# =====
#
# 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 serer.
# 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=65991
Password=65991
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=20.32.39.180
Codec=g711U

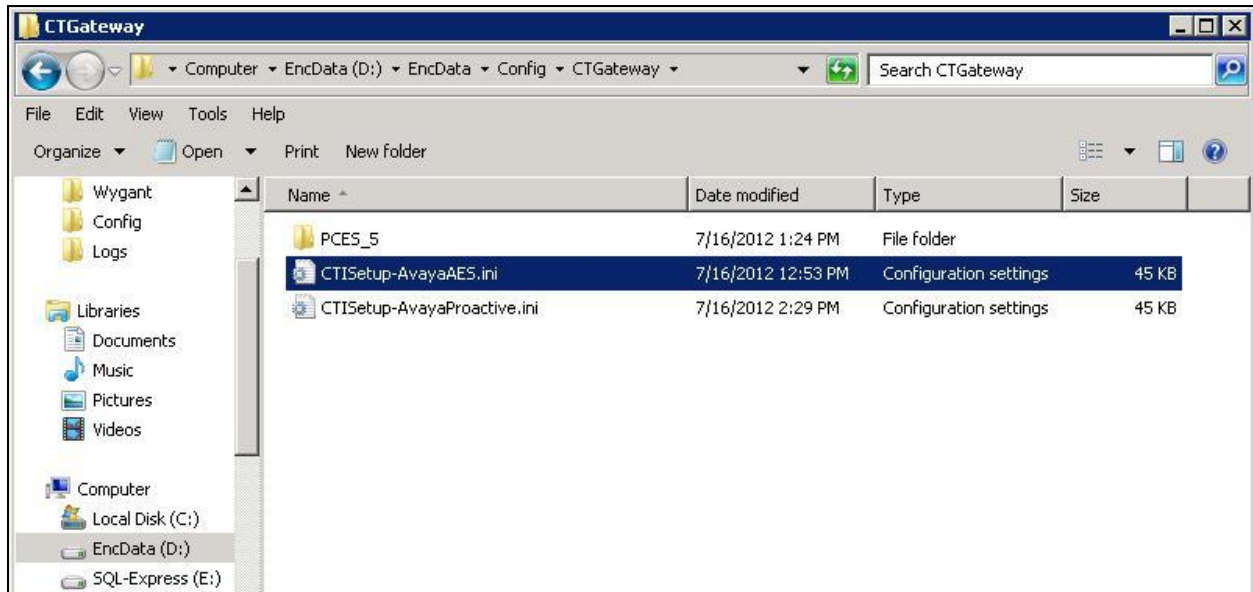
[SoftPhone2]
Extension=65992
Password=65992
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=20.32.39.180
Codec=g711U

[SoftPhone3]
Extension=65993
Password=65993
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=20.32.39.180
Codec=g711U

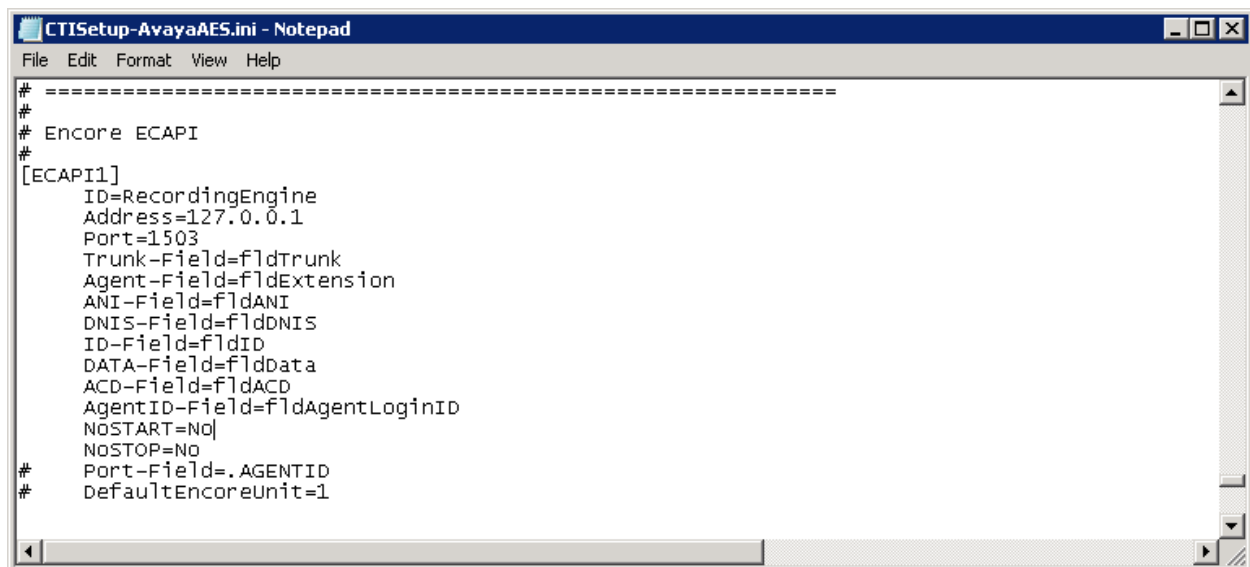
[SoftPhone4]
Extension=65994
Password=65994
# SwitchName=cm
SwitchAddr=10.64.125.32
RTPAddress=20.32.39.180
```

8.2. Administer CTISetup

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

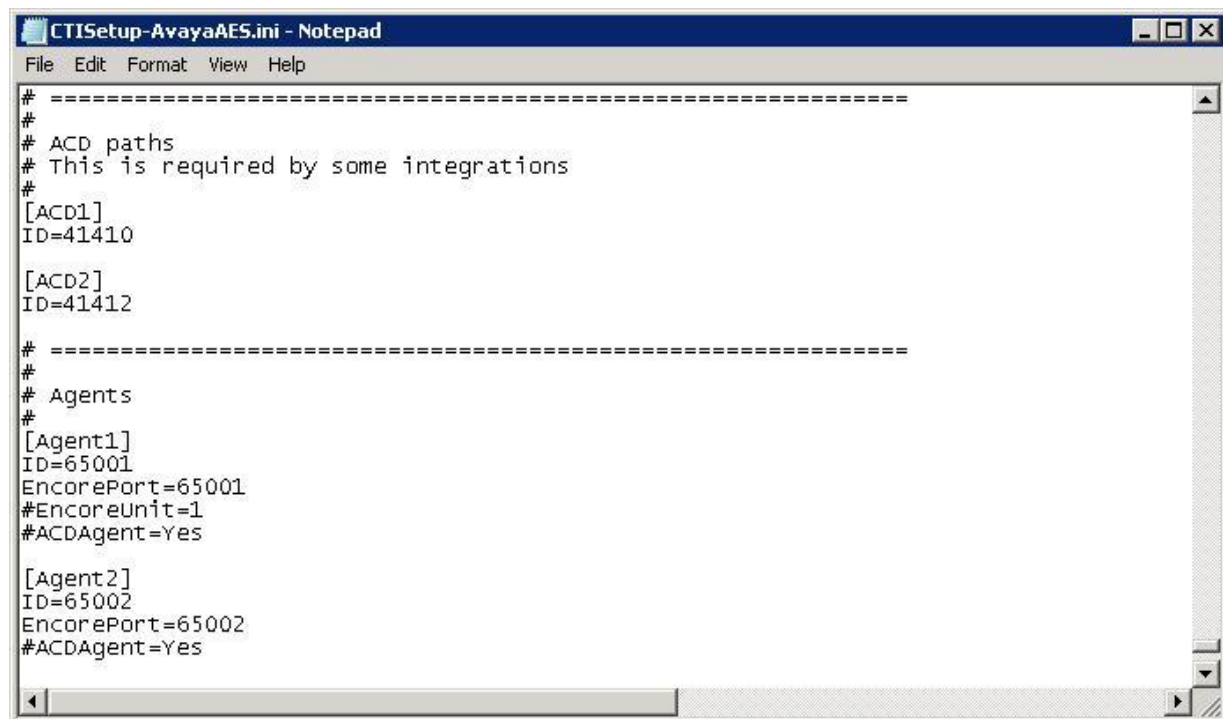


Scroll down to the **Encore ECAPI** section. Under **ECAPI1**, make sure all parameters are set to the default values shown below.



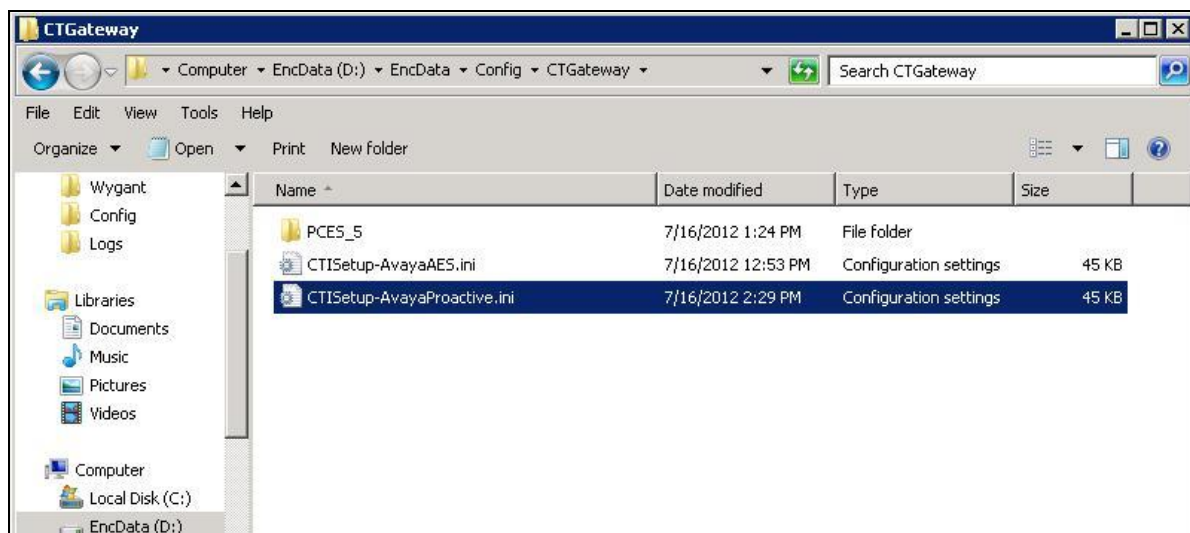
Scroll to the **ACD paths** section. Under **ACD1**, set **ID** to the first skill group extension from **Section 3**. Create additional ACD parameter lines as necessary when more than one skill group is being monitored.

Scroll to the **Agents** section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section 3**. Create additional agent parameter lines as necessary when more than one agent is being monitored.

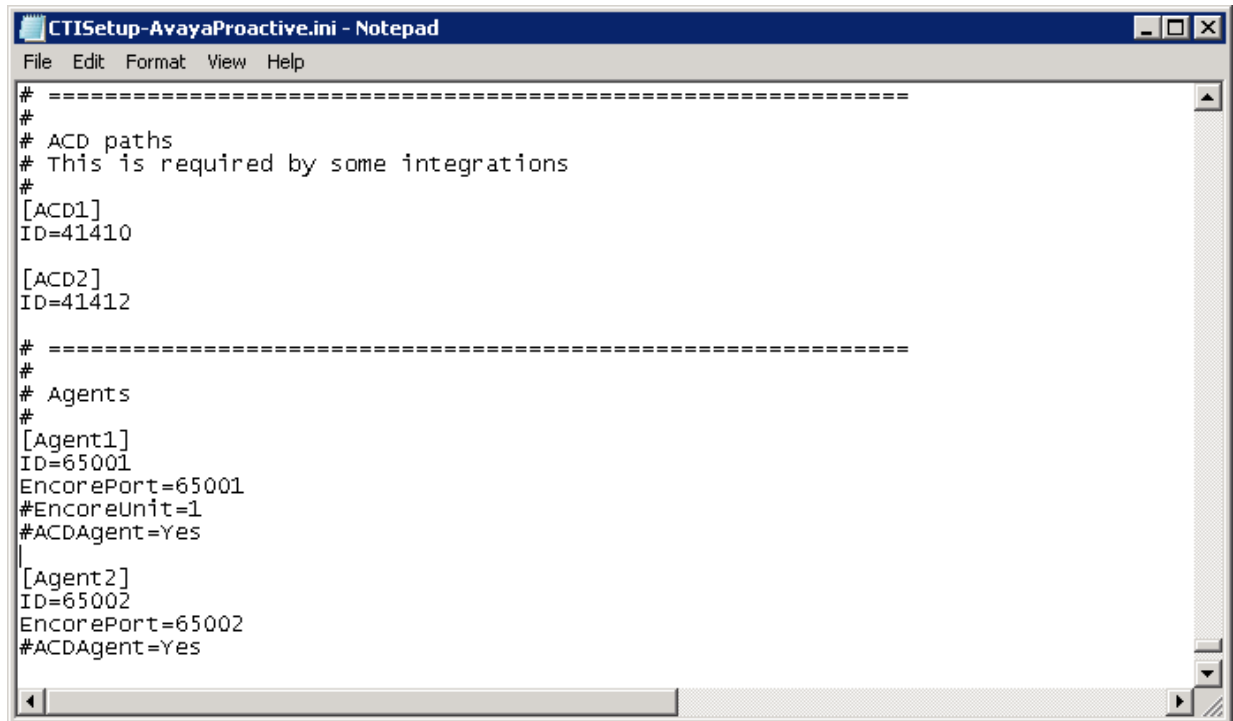


```
# =====  
#  
# ACD paths  
# This is required by some integrations  
#  
[ACD1]  
ID=41410  
  
[ACD2]  
ID=41412  
  
# =====  
#  
# Agents  
#  
[Agent1]  
ID=65001  
EncorePort=65001  
#EncoreUnit=1  
#ACDAgent=Yes  
  
[Agent2]  
ID=65002  
EncorePort=65002  
#ACDAgent=Yes
```

In the same **D:\EncData\Config\CTGateway** directory, edit the **CTISetup-AvayaProactiveContact.ini** file shown below.



Scroll to the **ACD paths** and **Agents** sections, and make the same changes as described above for **CTISetup-AvayaAES.ini**.



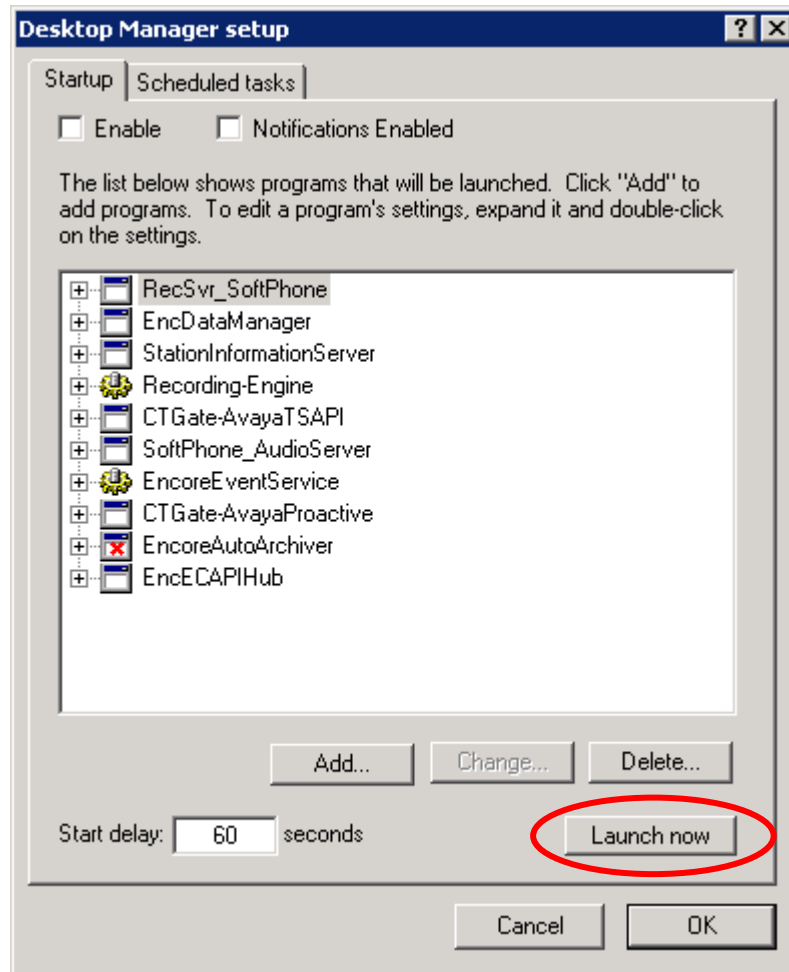
```
# =====  
#  
# ACD paths  
# This is required by some integrations  
#  
[ACD1]  
ID=41410  
  
[ACD2]  
ID=41412  
  
# =====  
#  
# Agents  
#  
[Agent1]  
ID=65001  
EncorePort=65001  
#EncoreUnit=1  
#ACDAgent=Yes  
|  
[Agent2]  
ID=65002  
EncorePort=65002  
#ACDAgent=Yes
```

8.3. Launch CT Gateways

Right click on the **Desktop Manager** icon from the system tray, and select **Configure**.



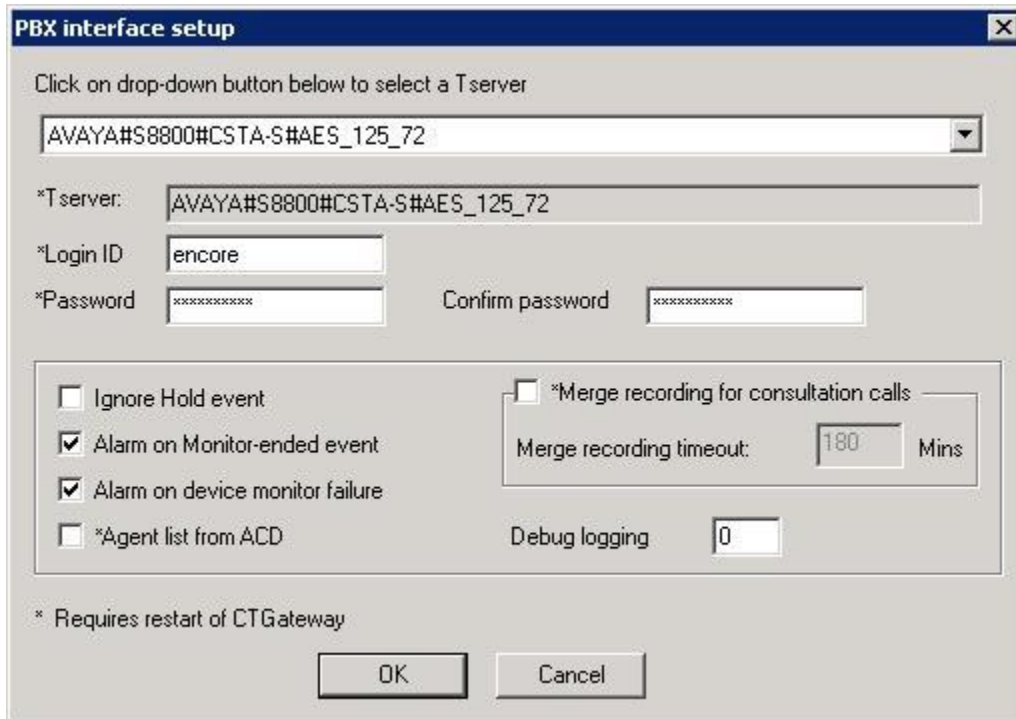
The **Desktop Manager setup** screen is displayed. Click **Launch now** to launch the CT Gateways.



8.4. Administer CT Gateways

The **CT Gateway (AvayaTSAPI)** and **CT Gateway (AvayaProactive)** screens are displayed (not shown). From the **CT Gateway (AvayaTSAPI)** screen, select **PBX > Configure** from the top menu.

The **PBX interface setup** screen below is displayed. Select the Tlink name in **Section 6.6** from the drop-down list. For **Login ID**, **Password**, and **Confirm password**, enter the Encore user credentials from **Section 6.7**. Retain the default values in the remaining fields.



The image shows a 'PBX interface setup' dialog box. At the top, it says 'Click on drop-down button below to select a Tserver'. Below this is a drop-down menu showing 'AVAYA#S8800#CSTA-S#AES_125_72'. Underneath, there are fields for '*Tserver:' (same as the drop-down), '*Login ID' (filled with 'encore'), '*Password' (filled with 'xxxxxxxx'), and 'Confirm password' (filled with 'xxxxxxxx'). A group of checkboxes includes 'Ignore Hold event' (unchecked), 'Alarm on Monitor-ended event' (checked), 'Alarm on device monitor failure' (checked), and '*Agent list from ACD' (unchecked). To the right, there is a checkbox for '*Merge recording for consultation calls' (unchecked) and a 'Merge recording timeout' field set to '180' with 'Mins' next to it. Below these is a 'Debug logging' field set to '0'. At the bottom, a note states '* Requires restart of CTGateway', followed by 'OK' and 'Cancel' buttons.

PBX interface setup

Click on drop-down button below to select a Tserver

AVAYA#S8800#CSTA-S#AES_125_72

*Tserver: AVAYA#S8800#CSTA-S#AES_125_72

*Login ID: encore

*Password: xxxxxxxxxx Confirm password: xxxxxxxxxx

☐ Ignore Hold event

☒ Alarm on Monitor-ended event

☒ Alarm on device monitor failure

☐ *Agent list from ACD

☐ *Merge recording for consultation calls

Merge recording timeout: 180 Mins

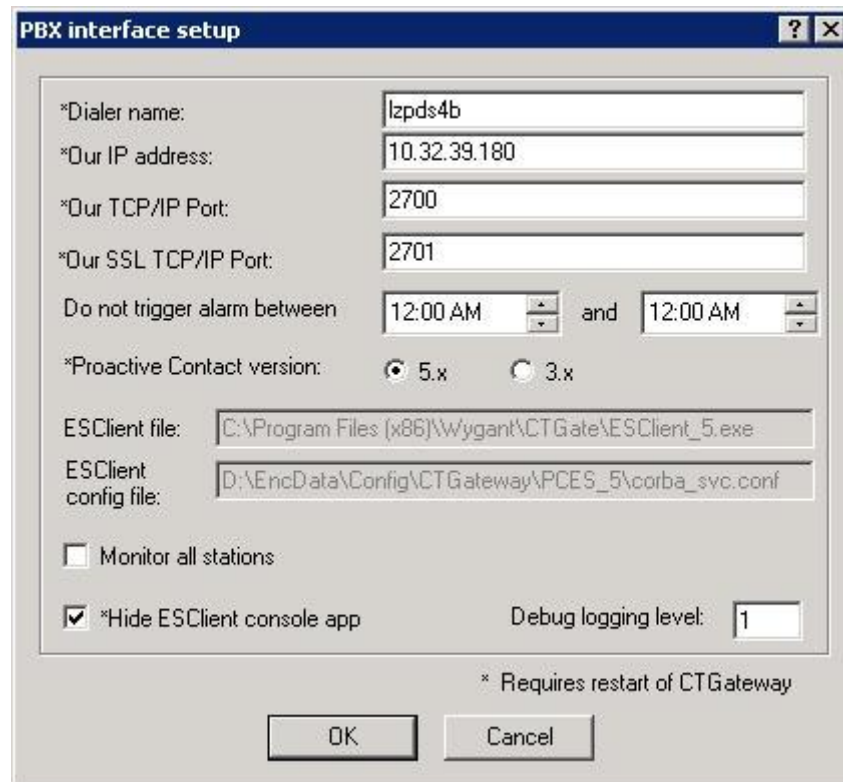
Debug logging: 0

* Requires restart of CTGateway

OK Cancel

From the **CT Gateway (AvayaProactive)** screen (not shown), select **PBX > Configure** from the top menu.

The **PBX interface setup** screen below is displayed. For **Dialer name**, enter the host name of Proactive Contact from **Section 7.1**. For **Our IP address**, enter the IP address of the Encore server. Retain the default values in the remaining fields.



The image shows a Windows-style dialog box titled "PBX interface setup". It contains several input fields and checkboxes. The fields are: "*Dialer name:" with the value "lzpds4b"; "*Our IP address:" with the value "10.32.39.180"; "*Our TCP/IP Port:" with the value "2700"; "*Our SSL TCP/IP Port:" with the value "2701"; "Do not trigger alarm between:" with two time pickers both set to "12:00 AM" and the word "and" between them; "*Proactive Contact version:" with two radio buttons, "5.x" (selected) and "3.x"; "ESClient file:" with the path "C:\Program Files (x86)\Wygant\CTGate\ESClient_5.exe"; "ESClient config file:" with the path "D:\EncData\Config\CTGateway\PCES_5\corba_svc.conf"; a checkbox "Monitor all stations" which is unchecked; a checkbox "*Hide ESClient console app" which is checked; and a "Debug logging level:" field with the value "1". At the bottom right, there is a note "* Requires restart of CTGateway". At the bottom center are "OK" and "Cancel" buttons.

*Dialer name:	lzpds4b
*Our IP address:	10.32.39.180
*Our TCP/IP Port:	2700
*Our SSL TCP/IP Port:	2701
Do not trigger alarm between	12:00 AM and 12:00 AM
*Proactive Contact version:	<input checked="" type="radio"/> 5.x <input type="radio"/> 3.x
ESClient file:	C:\Program Files (x86)\Wygant\CTGate\ESClient_5.exe
ESClient config file:	D:\EncData\Config\CTGateway\PCES_5\corba_svc.conf
<input type="checkbox"/> Monitor all stations	
<input checked="" type="checkbox"/> *Hide ESClient console app	
Debug logging level:	1

* Requires restart of CTGateway

OK Cancel

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that **Service State** is “established” for the relevant CTI link, 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	AES_21_46	established	15	15
2	4	no	aes_125_72	established	203	67

Verify the registration status of virtual IP softphones by using the “list registered-ip-stations” command. Verify that all softphone extensions from **Section 5.5** are displayed, as shown below.

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

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address	
65000	1616	IP_Phone	y	10.32.39.119	
	1	1.302S		10.64.125.62	
65001	1616	IP_Phone	y	10.32.39.109	
	1	1.302S		10.64.125.62	
65002	9620	IP_Phone	y	10.32.39.118	
	1	6.020S		10.64.125.62	
65991	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	
65992	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	
65993	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	
65994	4610	IP_API_A	y	10.64.125.72	
	1	3.2040		10.64.125.32	

9.2. Verify Avaya Proactive Contact


Log in to the Linux shell of the Proactive Contact server, and issue the “netstat | grep enservice” command. Verify that there is an entry showing an **ESTABLISHED** connection between Proactive Contact and Encore, as shown below.

tcp	0	0	lzpds4b:enservice_ssl	10.32.39.180:49716	ESTABLISHED
tcp	0	0	lzpds4b:enservice_ssl	lzpds4b:29292	ESTABLISHED

9.3. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify 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 that **Status** is “Talking” for the relevant TSAPI link, as shown below.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Fri Jul 27 07:31:20 2012 from 10.32.39.20
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-2-32-0

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ **TSAPI Service Summary**

TSAPI Link Details


☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
	1	S8800	2	Talking	Mon Jun 4 10:09:07 2012	Online	16	6	66	199	30

For service-wide information, choose one of the following:

Verify 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.

In the lower portion of the screen, verify that there is an active session with the Encore user name from **Section 6.7**, and that **# of Associated Devices** reflects the number of softphones from **Section 8.1**.


Application Enablement Services
Management Console

Welcome: User
Last login: Fri Jul 27 07:31:20 2012 from 10.32.39.20
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-2-32-0

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

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

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Fri Jul 27 09:42:18 MDT 2012

Service Uptime: 51 days, 0 hours 11 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 49
Number of Existing Devices: 4
Number of Devices Created Since Service Boot: 166

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	7C16DA1797C2CCBAE 50678376374EC85-56	encore	SPAS1	20.32.39.180	XML Unencrypted	4

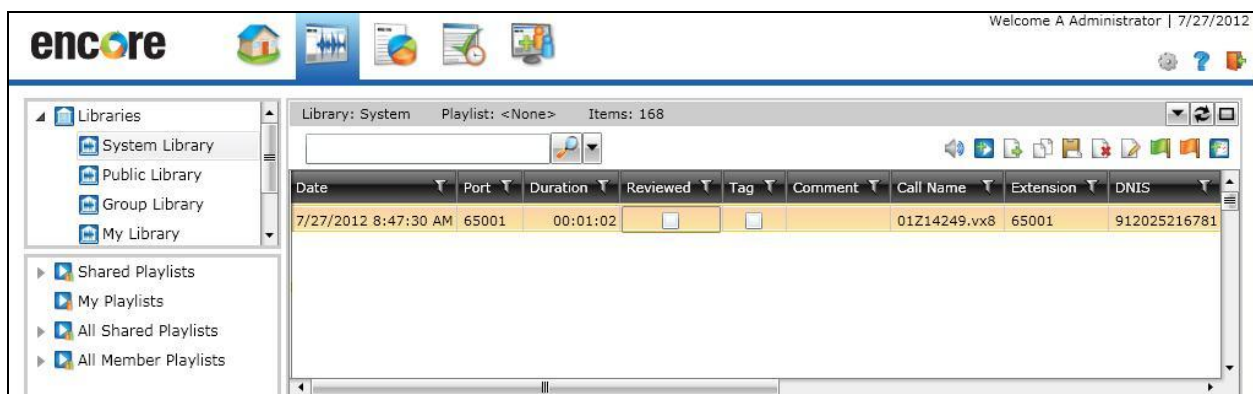
Item 1-1 of 1

9.4. Verify dvsAnalytics Encore

Start a job on Proactive Contact, and log an agent in to handle and complete a 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.



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 Encore PC5 application interface. At the top, the 'encore' logo is on the left, and a 'Welcome A Administrator | 7/27/2012' message is on the right. Below the header, there is a navigation pane on the left with 'Libraries' (System Library, Public Library, Group Library, My Library) and 'Shared Playlists' (My Playlists, All Shared Playlists, All Member Playlists). The main area shows a table of call recordings. The table has columns: Date, Port, Duration, Reviewed, Tag, Comment, Call Name, Extension, and DNIS. A single row is visible with the following data: 7/27/2012 8:47:30 AM, 65001, 00:01:02, [checkbox], [checkbox], [empty], 01Z14249.vx8, 65001, 912025216781. Below the table, a 'Streaming Player' section shows '01Z14249.vx8' and 'Position: 0:00:04.648 Recording Length: 0:01:00.802'. A waveform visualization is shown, and a 'Video Unavailable' message is on the left. At the bottom, there is a playback control bar with buttons for play, pause, stop, previous, next, and a volume slider.

Date	Port	Duration	Reviewed	Tag	Comment	Call Name	Extension	DNIS
7/27/2012 8:47:30 AM	65001	00:01:02	<input type="checkbox"/>	<input type="checkbox"/>		01Z14249.vx8	65001	912025216781

10. Conclusion

These Application Notes describe the configuration steps required for dvsAnalytics Encore to successfully interoperate with Avaya Proactive Contact with PG230 and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011, available at <http://support.avaya.com>.
3. *Administering Avaya Proactive Contact*, Release 5.0, April 2012, available at <http://support.avaya.com>.
4. *Avaya Aura™ Communication Manager TSAPI Integration Guide*, Release 2.3.3, April 18, 2012, available from dvsAnalytics Support.
5. *Avaya Aura™ Communication Manager TSAPI Installation Addendum*, Release 2.3.3, April 30, 2012, available from dvsAnalytics Support.
6. *Avaya Proactive Contact Dialer Integration Guide*, Release 2.3.3, April 30, 2012, available from dvsAnalytics Support.
7. *Avaya Proactive Contact Dialer Installation Addendum*, Release 2.3.3, April 30, 2012, available from dvsAnalytics Support.

©2012 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.