



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

---

# **Application Notes for VPI Voice Capture with Avaya Proactive Contact 5.0.1 with PG230 and Avaya Aura® Application Enablement Services 6.1.2 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Voice Print International Voice Capture to interoperate with Avaya Proactive Contact 5.0.1 with PG230 and Avaya Aura® Application Enablement Services 6.1.2. Voice Print International Voice Capture is a call recording solution in the Empower suite.

In the compliance testing, Voice Print International Voice Capture 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 Multiple Registration feature from 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 Voice Print International (VPI) Voice Capture to interoperate with Avaya Proactive Contact 5.0.1 with PG230 and Avaya Aura® Application Enablement Services 6.1.2. Voice Print International Voice Capture is a call recording solution in the Empower suite.

In the compliance testing, VPI Voice Capture 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 Multiple Registration feature from 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 VPI Voice Capture to monitor the agent stations and calls, and the DMCC interface is used by VPI Voice Capture to register a virtual recording device against each monitored station to pick up the media for call recording. When there is an active call at the monitored station, VPI Voice Capture is informed of the call via event reports from the Event Services and/or TSAPI interfaces, and starts the call recording by using the media from the recording device that are associated with the monitored station. 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 Voice Capture application, the application automatically requests monitoring on the stations to be recorded using TSAPI, registers a recording device for each monitored station using DMCC, and obtains the current status on Proactive Contact using Event Services.

For the manual part of the testing, each call was handled manually on the station user 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 Voice Capture.

The verification of tests included using the Voice Capture logs for proper message exchanges, and using the Empower web-based 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 Voice Capture:

- 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 the recording devices.
- Use of DMCC monitoring services and media control events to obtain the media from the recording devices.
- 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 the Voice Capture to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to Voice Capture.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Voice Capture from the compliance testing.

- Recordings for supervised forward work scenarios are not supported in this release of Voice Capture.
- Connections to announcements were included as separate recording entries, and the initial announcement recording entry does not end until the agent receives a call.
- Held scenario produced two recording entries.
- Recording entries for inbound calls over blend and inbound jobs contained blank number dialed.
- The majority of the recordings did not end until ~7 seconds after the agent released the line.
- The server can take up to 7 minutes to be functional to start recording again upon a link restoration.

## 2.3. Support

Technical support on Voice Capture can be obtained through the following:

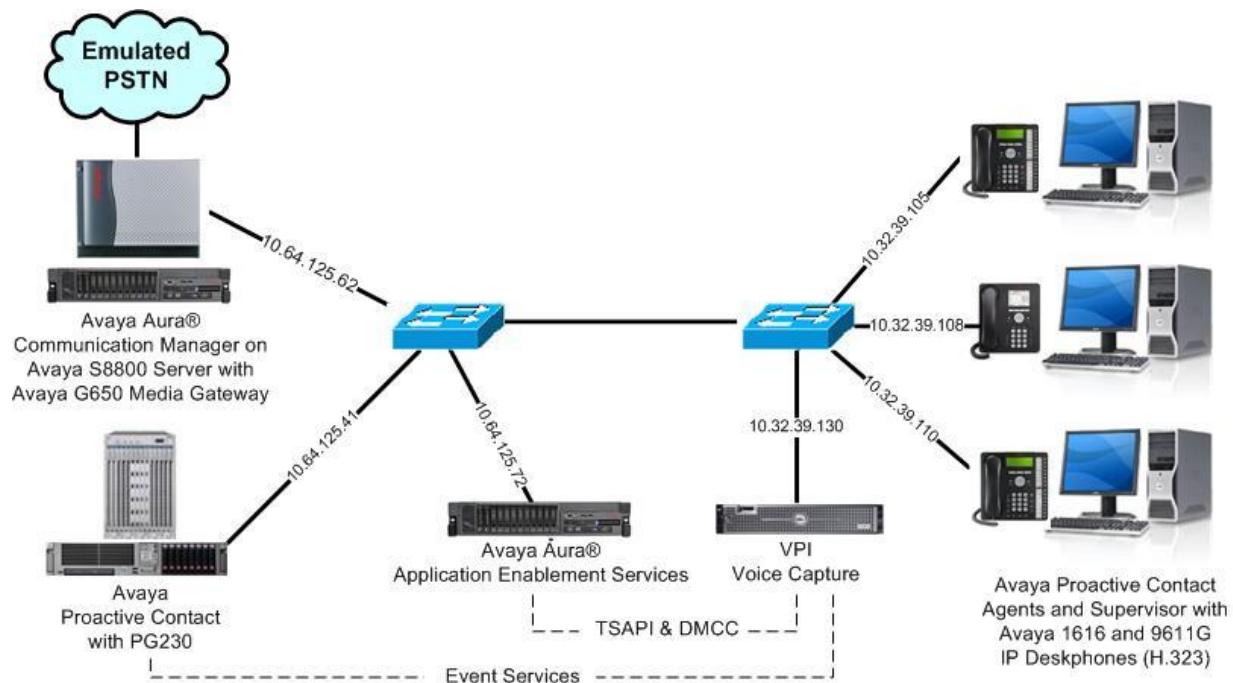
- **Phone:** (805) 389-5201
- **Email:** [support@vpi-corp.com](mailto:support@vpi-corp.com)
- **Web:** <http://www.vpi-corp.com/support.asp>

### 3. Reference Configuration

Voice Capture can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server 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, Voice Capture monitored two agent station extensions “65001” and “65002” on Communication Manager.



**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"><li>TN799DP C-LAN Circuit Pack</li><li>TN2302AP IP Media Processor</li></ul>	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 Deskphone (H.323)	1.301S
Avaya 9611G IP Deskphone (H.323)	6.2013
VPI Voice Capture on Empower Suite and Windows Server 2008 <ul style="list-style-type: none"><li>Avaya TSAPI Windows Client (csta32.dll)</li><li>Avaya DMCC SDK (ServiceProvider.dll)</li></ul>	4.5.0.56 5.3.1.16 R2 Standard SP1 6.1.0.396 6.1.1.45

## 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 system parameters features
- Administer 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	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
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	Digital Loss Plan Modification?	y	
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y	
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y	
ATMS?	y			
Attendant Vectoring?	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 2		Page	1 of	3
CTI LINK				
CTI Link:	2			
<b>Extension:</b>	60100			
<b>Type:</b>	ADJ-IP			
		COR:	1	
<b>Name:</b>	TSAPI Link			

### 5.3. 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 19
      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

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: 27
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Voice Capture.

```
change system-parameters features                                     Page 13 of 19
      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
```



## 5.4. Administer Stations

Use the “change station n” command, where “n” is the first agent station extension from **Section 3**. Enable **IP SoftPhone**, to allow for a recording device to be registered against the station. Note the value of **Security Code**, which will be used later to configure Voice Capture.

change station 65001		Page	1 of	4
STATION				
Extension: 65001	Lock Messages? n	BCC:	0	
Type: 1616	<b>Security Code: 65001</b>	TN:	1	
Port: S00006	Coverage Path 1:	COR:	1	
Name: VPI Agent #1	Coverage Path 2:	COS:	1	
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern:	1		
	Message Lamp Ext:	65001		
Speakerphone: 2-way	Mute Button Enabled?	y		
Display Language: english				
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>			
	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	
<b>65001</b>	<b>S00006</b>	<b>VPI Agent #1</b>			<b>1</b>	<b>1</b>			
	<b>1616</b>		<b>no</b>			<b>1</b>	<b>1</b>		
<b>65002</b>	<b>S00031</b>	<b>VPI Agent #2</b>			<b>1</b>	<b>1</b>			
	<b>9630</b>		<b>no</b>			<b>1</b>	<b>1</b>		

## 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 TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer VPI 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 **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](#)

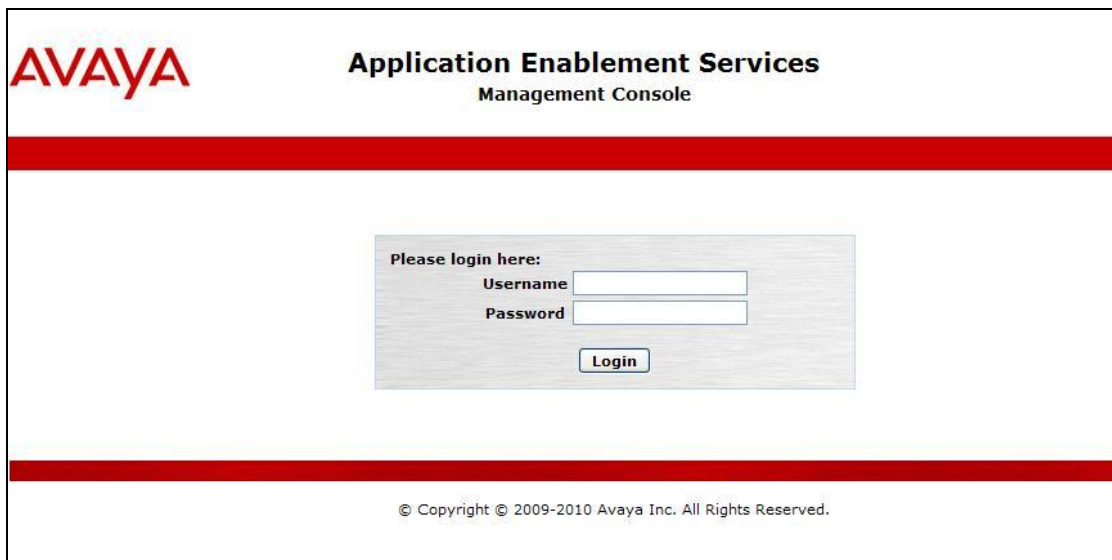
Licensed Features

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

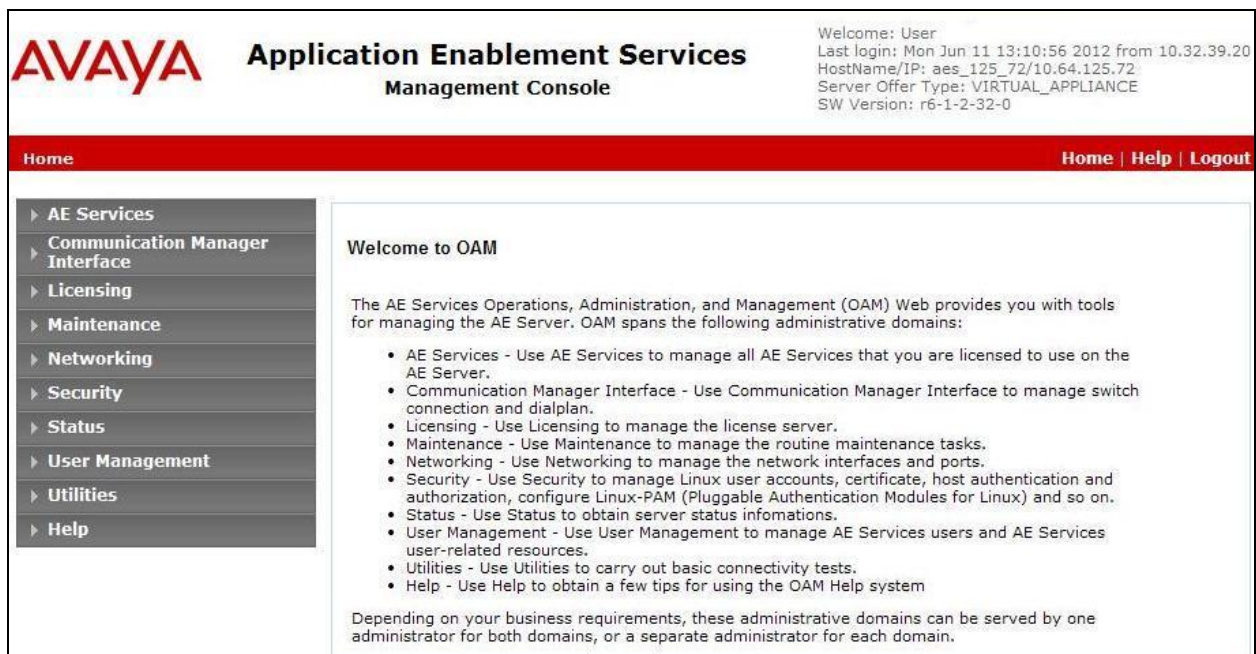
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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



The screenshot shows the Avaya logo on the left and the title "Application Enablement Services Management Console" in the center. Below the title is a red horizontal bar. In the center of the page is a login box with 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, below another red horizontal bar, is the copyright notice: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

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



The screenshot shows the Avaya logo on the left and the title "Application Enablement Services Management Console" in the center. In the top right corner, there is a welcome message: "Welcome: User", "Last login: Mon Jun 11 13:10:56 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 title is a red horizontal bar with the text "Home" on the left and "Home | Help | Logout" on the right. On the left side of the page is a vertical 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:" followed by a bulleted list of domains and their functions. At the bottom of the main content area, there is a paragraph: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain."

Welcome: User  
Last login: Mon Jun 11 13:10:56 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

Home | Help | Logout

Home

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

Welcome to OAM

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

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

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

### 6.3. Administer TSAPI Link

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

The screenshot shows the AVAYA Application Enablement Services Management Console. The left sidebar has a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links' (selected), and 'TSAPI Properties'. The main content area is titled 'TSAPI Links' and contains a table with columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'. The top right of the console displays user information: 'Welcome: User', 'Last login: Mon Jun 11 12:17:42 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 includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'.

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 “S8800” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields, and click **Apply Changes**.

The screenshot shows the AVAYA Application Enablement Services Management Console with the 'Add TSAPI Links' form. The left sidebar is the same as the previous screenshot, but 'Communication Manager Interface' is also visible under 'TSAPI'. The main content area is titled 'Add TSAPI Links' and contains the following fields: 'Link' (dropdown with value 1), 'Switch Connection' (dropdown with value S8800), 'Switch CTI Link Number' (dropdown with value 2), 'ASAI Link Version' (dropdown with value 4), and 'Security' (dropdown with value Unencrypted). At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'. The top right of the console displays the same user information as the previous screenshot. The top navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'.



## 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 “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. A single row is visible with the connection name 'S8800', Processor Ethernet 'No', Msg Period '30', and Number of Active Connections '1'. Below the table are several action buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, and Survivability Hierarchy.

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 text input field containing '10.64.125.32' and an 'Add Name or IP' button. Below the input field is a label 'Name or IP Address' and two buttons: 'Delete IP' and 'Back'.

## 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, 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: Mon Jun 11 13:10:56 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'.

## 6.6. 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 features 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 for 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right corner displays user information: 'Welcome: User', 'Last login: Mon Jun 11 12:17:42 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

## 6.7. 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 Voice Capture.

In this case, the associated unencrypted Tlink name is “AVAYA#S8800#CSTA#AES\_125\_72”. 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". The main content area, titled "Tlinks", lists two Tlink names: "AVAYA#S8800#CSTA#AES\_125\_72" (selected with a radio button) and "AVAYA#S8800#CSTA-S#AES\_125\_72". A "Delete Tlink" button is visible below the list.

**AVAYA** Application Enablement Services Management Console

Welcome: User  
Last login: Mon Jun 11 12:17:42 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

**Tlinks**

Tlink Name

☒ AVAYA#S8800#CSTA#AES\_125\_72  
☐ AVAYA#S8800#CSTA-S#AES\_125\_72

Delete Tlink



## 6.8. Administer VPI 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: Mon Jun 11 12:17:42 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), Utilities, and Help. Under 'User Admin', the 'Add User' option is selected. The main content area is titled 'Add User' and contains a form with the following fields: \* User Id (text input, value: vpi), \* Common Name (text input, value: vpi), \* Surname (text input, value: vpi), \* User Password (password input, masked with dots), \* Confirm Password (password input, masked with dots), Admin Note (text input), Avaya Role (dropdown menu, value: None), Business Category (text input), Car License (text input), CM Home (text input), Csm Home (text input), CT User (dropdown menu, value: Yes), Department Number (text input), Display Name (text input), and Employee Number (text input). A note at the top of the form states: 'Fields marked with \* can not be empty.'

## 6.9. 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: Mon Jun 11 12:17:42 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 Port

9999

Enabled Disabled

Encrypted TCP Port

9998

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port

450

Enabled Disabled

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

Unencrypted Port

4721

Enabled Disabled

Encrypted Port

4722

TR/87 Port

4723

## 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 Voice Capture.

In the compliance testing, the host name of the Avaya Proactive Contact server is “lzpds4b”, 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 [1013]
$
```

## 8. Configure VPI Voice Capture

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

- Launch VPI Configuration
- Administer start/stop events
- Administer TSAPI
- Administer proactive dialer
- Administer software RTP
- Administer DMCC
- Administer channels
- Launch Digital Call Logger

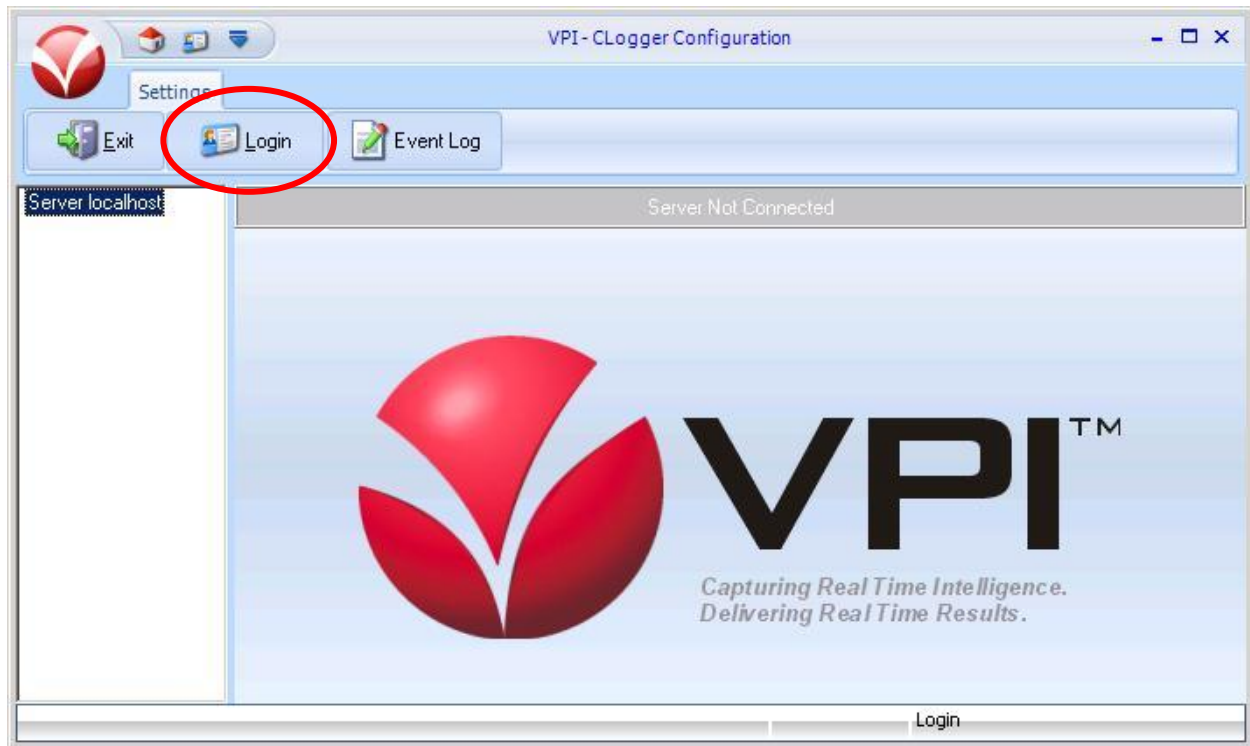
The configuration of Voice Capture is performed by VPI installers. The procedural steps are presented in these Application Notes for informational purposes.

### 8.1. Launch VPI Configuration

From the Voice Capture server, double-click on the **VPI Configuration** icon shown below, which was created as part of installation.



The **VPI - CLogger Configuration** screen is displayed. Click on **Login**, as shown below.

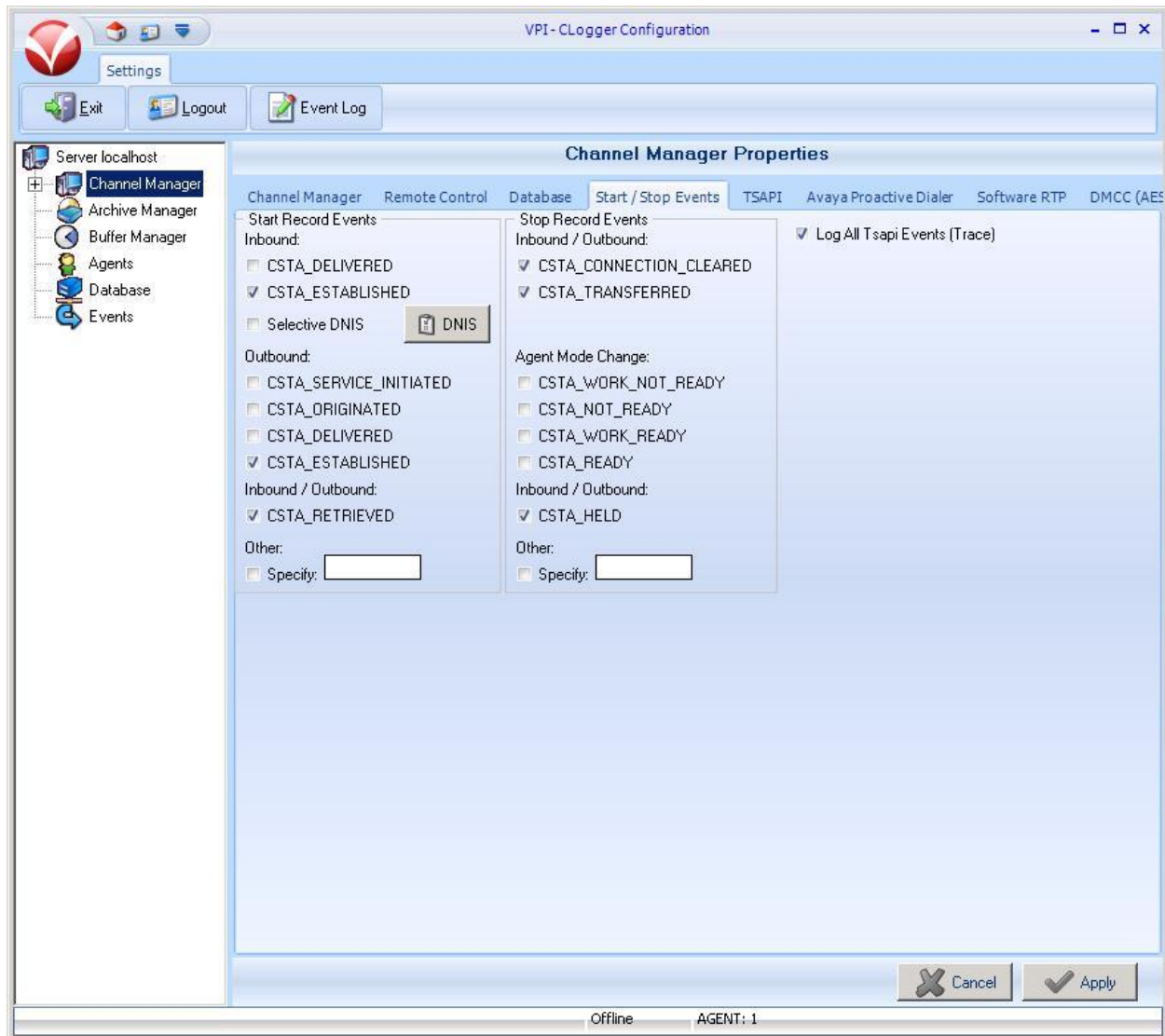


The screen below is displayed next. Log in using the appropriate credentials.

## 8.2. Administer Start/Stop Events

Select **Server localhost** → **Channel Manager** in the left pane, to display the **Channel Manager Properties** screen. Select the **Start / Stop Events** tab in the right pane. Check the desired events to trigger the start and stop of call recordings.

The screen below shows the selections used for the compliance testing. The **Log All Tsapi Events (Trace)** field was checked in the compliance testing for event verification purposes. Click **Apply**.



### 8.3. Administer TSAPI

Select the **TSAPI** tab in the right pane. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Apply**.

- **Server 1 Machine:** The Tlink name from **Section 6.7**.
- **Application Username:** The VPI user credentials from **Section 6.8**.
- **Application Password:** The VPI user credentials from **Section 6.8**.
- **Switch Type:** “Avaya / Lucent”

The screenshot shows the 'VPI-CLogger Configuration' window with the 'TSAPI' tab selected. The window has a menu bar with 'Exit', 'Logout', and 'Event Log'. A left sidebar shows a tree view with 'Server localhost' expanded, containing 'Channel Manager', 'Archive Manager', 'Buffer Manager', 'Agents', 'Database', and 'Events'. The main area is titled 'Channel Manager Properties' and contains several sections:

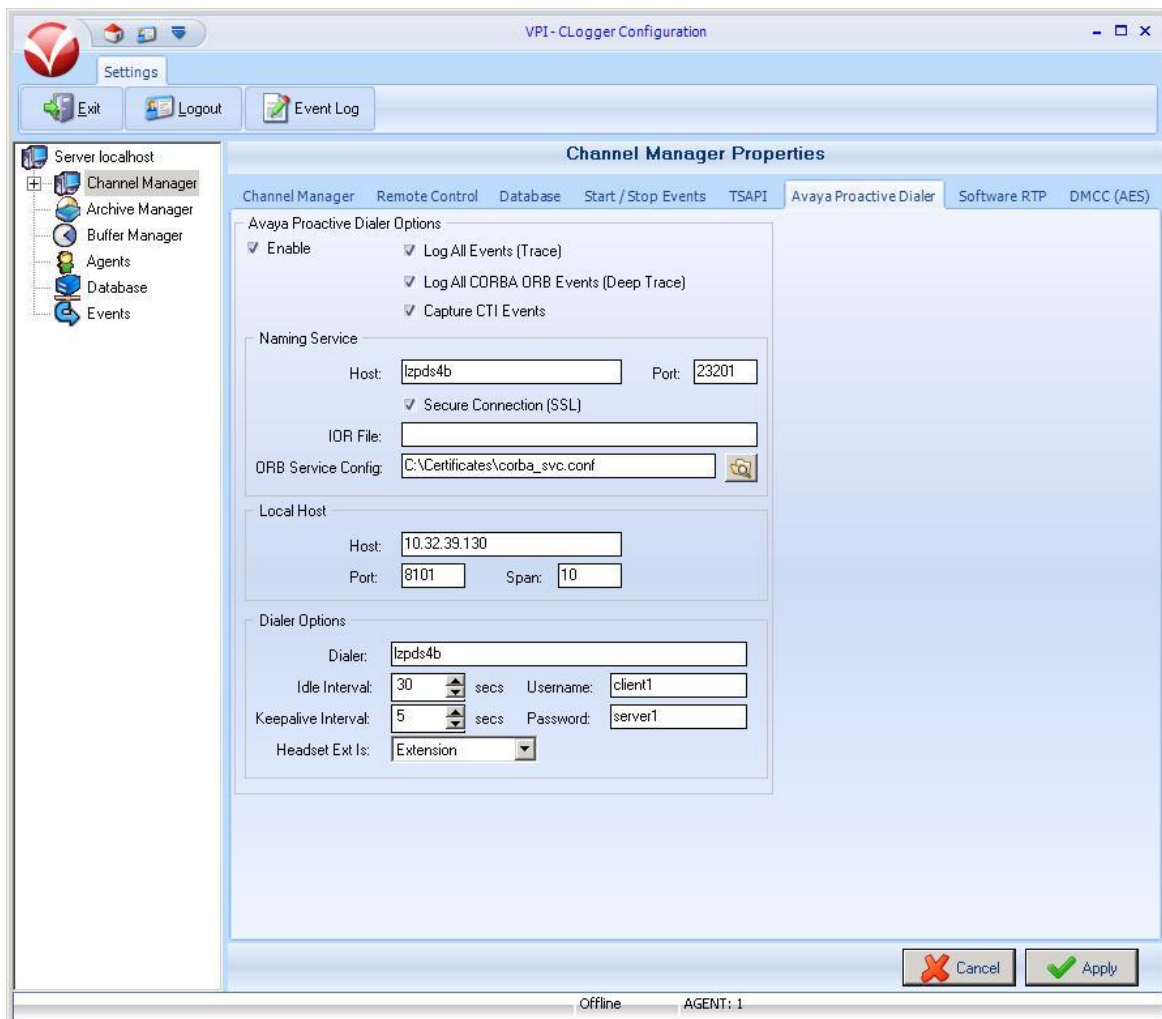
- TSAPI Server Setup:**
  - Server 1 Machine: AVAYA#S8800#CSTA#
  - Server 2 Machine: (empty)
  - TSAPI Device: 10.64.125.72
  - Application Username: vpi
  - Application Password: (masked)
  - ☐ Fail to VDX
  - ☒ Save All ANI
- General Options:**
  - ☒ Record All Agents
  - ☐ Lock Status Lights
  - ☐ Use Tsapi Time Stamp
  - ☐ DaVox Enabled
- Additional Monitors:**
  - ACD Groups: (empty)
  - Trunks: (empty)
  - VDNs: (empty)
  - Extensions: (empty)
  - ☐ Disable recording of calls when SPLIT is empty
  - ☐ Disable recording of calls when DISTRIBUTING VDN is empty
- Switch Type:**
  - ☐ CSTA Compliant
  - ☒ Avaya / Lucent
  - ☐ Nortel Meridian
  - ☐ Aspect
  - ☐ NEC
- Service Observe Options:**
  - ☐ Monitor Agent Mode Change
  - Feature Code: (empty)
- Recording Line Type:**
  - ☒ Extension Side
  - ☐ Trunk Side

At the bottom right are 'Cancel' and 'Apply' buttons. The status bar at the bottom shows 'Offline' and 'AGENT: 1'.

## 8.4. Administer Proactive Dialer

Select the **Avaya Proactive Dialer** tab in the right pane. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Apply**.

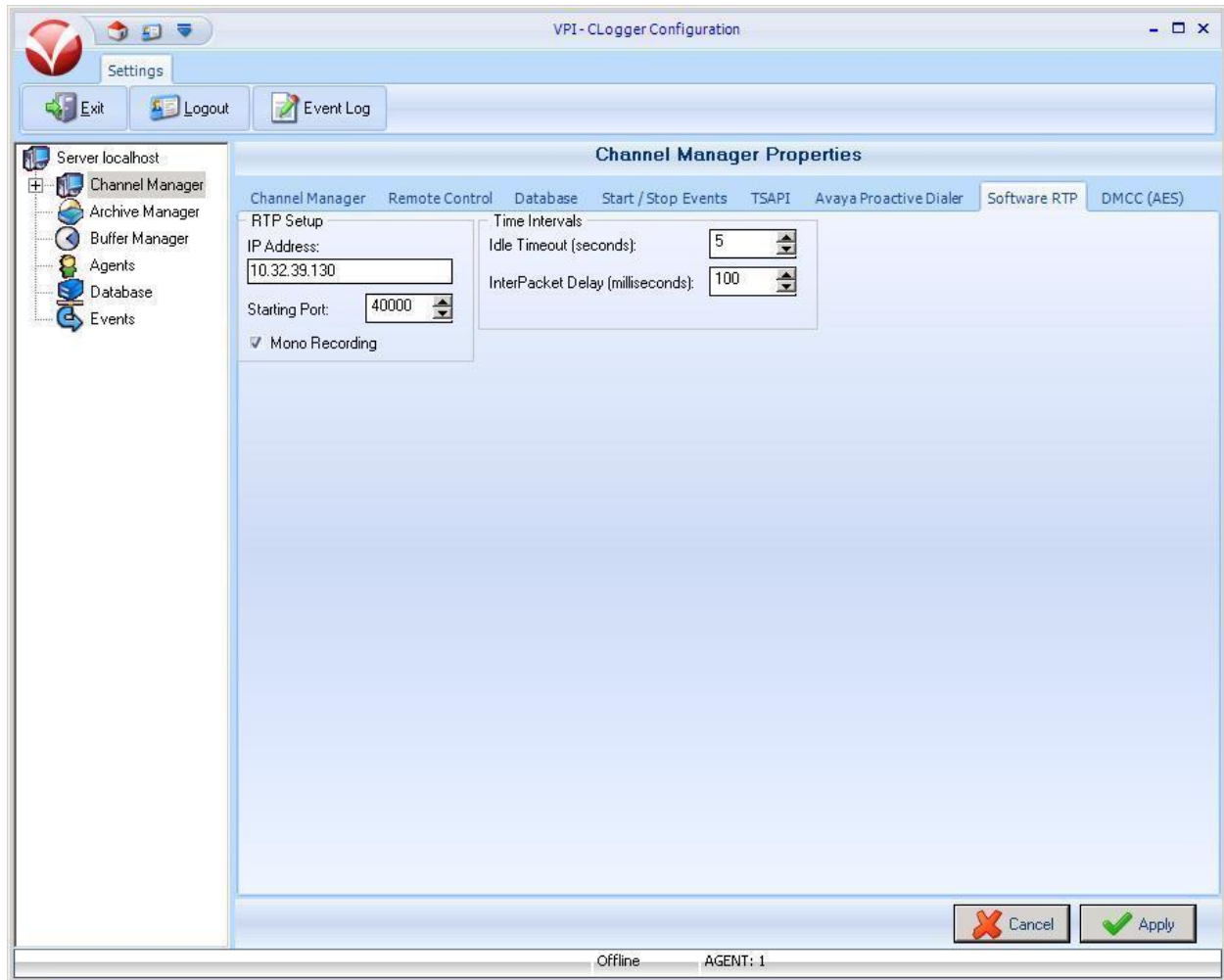
- **Enable:** Check this field.
- **Log All Events (Trace):** Checked during compliance testing for verification purposes.
- **Naming Service Host:** The host name of Avaya Proactive Contact from **Section 7.1**.
- **Naming Service Port:** “23201”
- **Secure Connection (SSL):** Check this field.
- **ORB Service Config:** The location of the installed corba\_svc.conf file.
- **Local Host Host:** The IP address of the Voice Capture server.
- **Local Host Port:** “8101”
- **Dialer:** The host name of Avaya Proactive Contact from **Section 7.1**.
- **Username:** Name of the Avaya Proactive Contact Event Service client.
- **Password:** Password of the Avaya Proactive Contact Event Service client.





## 8.5. Administer Software RTP

Select the **Software RTP** tab in the right pane. For **IP Address**, enter the IP address of the Voice Capture server, in this case “10.32.39.130”. Retain the default values in the remaining fields, and click **Apply**.



## 8.6. Administer DMCC

Select the **DMCC (AES)** tab in the right pane. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Apply**.

- **Enable:** Check this field.
- **Server IP Address:** IP address of the Application Enablement Services server.
- **Session User:** The VPI user credentials from **Section 6.8**.
- **Switch (CLAN) Address:** IP address of the H.323 gatekeeper from **Section 6.4**.
- **Session Password:** The VPI user credentials from **Section 6.8**.

The screenshot shows the 'VPI-CLlogger Configuration' window with the 'DMCC (AES)' tab selected. The window has a menu bar with 'Exit', 'Logout', and 'Event Log'. A left sidebar shows a tree view with 'Server localhost' expanded, containing 'Channel Manager', 'Archive Manager', 'Buffer Manager', 'Agents', 'Database', and 'Events'. The main area is titled 'Channel Manager Properties' and contains two sections: 'General Options' and 'TLS (SSL) Options'. In 'General Options', 'Enable' is checked, 'Server IP Address' is '10.64.125.72', 'Switch (CLAN) Address' is '10.64.125.32', 'Server Port' is '4721', 'Session User' is 'vpi', and 'Session Password' is masked with asterisks. In 'TLS (SSL) Options', 'Enable' is unchecked, 'Version' is 'SSL v2', 'Allow Older Versions' is unchecked, and various certificate and key files are empty. 'Packet Timeout' and 'Connect Timeout' are both '30', and 'Verify Depth' is '30'. At the bottom right are 'Cancel' and 'Apply' buttons. The status bar at the bottom shows 'Offline' and 'AGENT: 1'.

General Options	
<input checked="" type="checkbox"/> Enable	Switch (CLAN) Address: 10.64.125.32
Server IP Address: 10.64.125.72	Server Port: 4721
Session User: vpi	Global Ext Password:
	Session Password:

TLS (SSL) Options	
<input type="checkbox"/> Enable	Version: SSL v2
<input type="checkbox"/> Allow Older Versions	
Certificate File:	Client CA File:
CA File:	CA Path:
Key File:	Key Phrase:
Packet Timeout: 30	Connect Timeout: 30
<input type="checkbox"/> Verify Peer	Verify Depth: 30

## 8.7. Administer Channels

Select **Server localhost** → **Channel Manager** → **Channels** in the left pane, to display the **Channel Properties** screen. Select the first available channel from the left portion of the **Channel Properties** screen, and enter the following values for the specified fields in the right portion of the screen. Retain the default values for the remaining fields.

- **Name / Description:** A desired name for the station to be monitored.
- **Use Channel:** Check this field.
- **DMCC Security Code:** The corresponding station security code from **Section 5.4**.
- **Extension:** The corresponding station extension from **Section 5.4**.

Repeat this section to administer a channel for each agent station to be monitored from **Section 5.4**, and click **Apply**.

The screenshot shows the VPI-CLogger Configuration window. The left pane contains a tree view with the following items: Server localhost, Channel Manager, Channels (selected), Archive Manager, Buffer Manager, Agents, Database, and Events. The main area is titled 'Channel Properties' and has two tabs: 'Channels' and 'Idle Alarm Blackout Scheduling'. The 'Channels' tab is active, showing a table with the following data:

#	Name / Description	Ext.
1	Agent #1	65001
2	Agent #2	65002
3	Channel 3	0
4	Channel 4	0
5	Channel 5	0
6	Channel 6	0

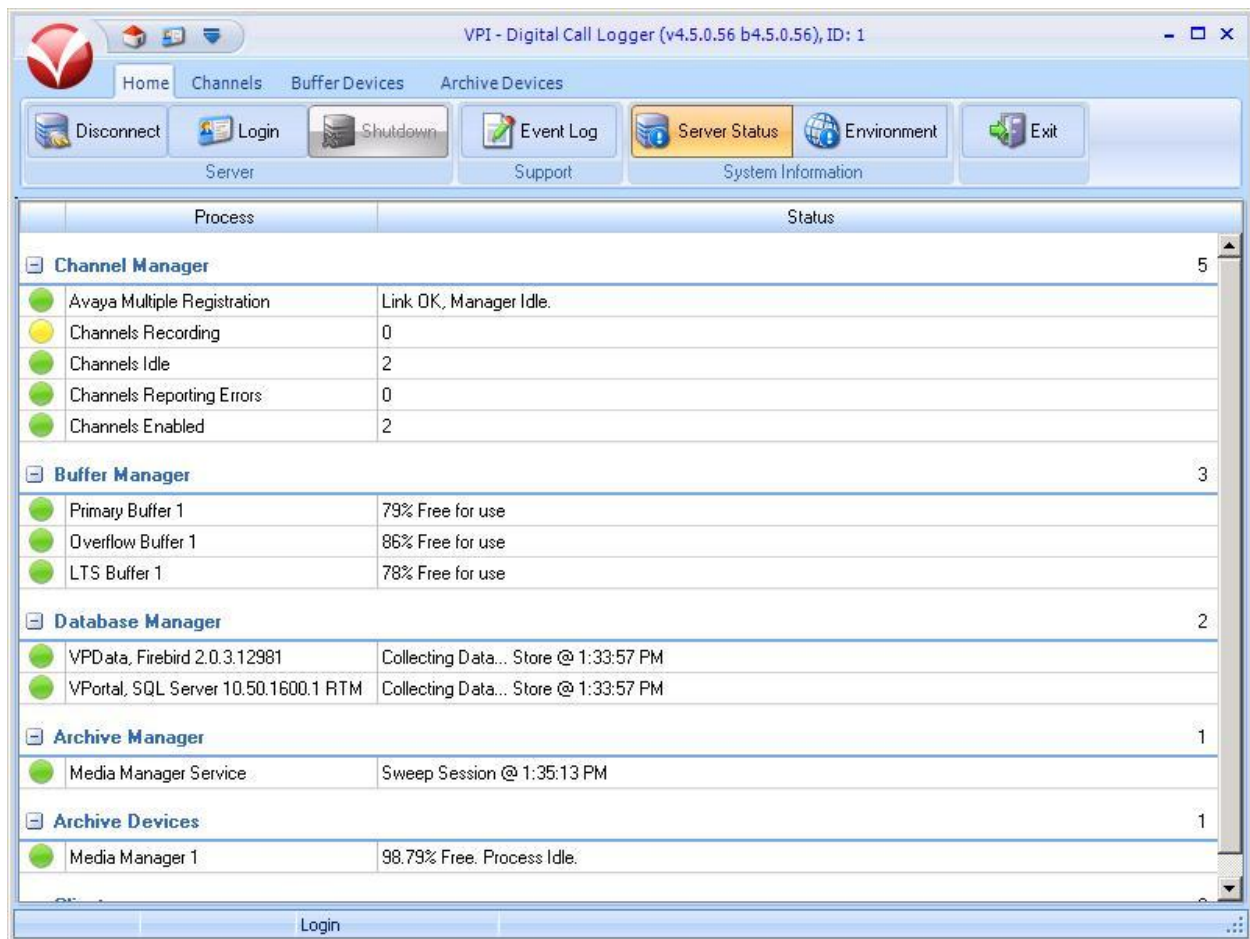
Below the table, the configuration options for 'Agent #1' are displayed. The 'Use Channel' checkbox is checked. Other options include 'Disable Live Monitoring', 'Use Alert Tone when Recording', and 'Always Record (VOX Emulation)'. The 'DMCC Security Code' field is set to '65001'. There are also fields for 'Additional IP Address' and 'Additional Mac Address'. A 'Details (Overrides Agent Settings)' section contains fields for 'Extension' (65001), 'Dept. ID' (0), 'Desk Location', 'Group ID' (0), and 'Class of Service' (Not Used (Default)). A 'Multicast Recording' section has an 'Enabled' checkbox and fields for 'Group IP' and 'Local Port' (0). At the bottom right, there are 'Cancel' and 'Apply' buttons. The status bar at the bottom shows 'Offline' and 'AGENT: 1'.

## 8.8. Launch Digital Call Logger

From the Voice Capture server, double-click on the **Activ! Voice** icon shown below to start the application. Note that the icon was created as part of installation.



The **VPI – Digital Call Logger** screen is displayed. Select **Server Status** from the top portion of the screen. In the **Channel Manager** section, verify that the **Channels Recording** entry has the yellow status, and that all other entries have the green status, as shown below.



Process	Status
<b>Channel Manager</b> 5	
Avaya Multiple Registration	Link OK, Manager Idle.
Channels Recording	0
Channels Idle	2
Channels Reporting Errors	0
Channels Enabled	2
<b>Buffer Manager</b> 3	
Primary Buffer 1	79% Free for use
Overflow Buffer 1	86% Free for use
LTS Buffer 1	78% Free for use
<b>Database Manager</b> 2	
VPData, Firebird 2.0.3.12981	Collecting Data... Store @ 1:33:57 PM
VPortal, SQL Server 10.50.1600.1 RTM	Collecting Data... Store @ 1:33:57 PM
<b>Archive Manager</b> 1	
Media Manager Service	Sweep Session @ 1:35:13 PM
<b>Archive Devices</b> 1	
Media Manager 1	98.79% Free. Process Idle.

## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Proactive Contact, Avaya Aura® Application Enablement Services, and VPI Voice Capture.

### 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	AES_21_46	established	14	14
2	4	no	aes_125_72	<b>established</b>	17	21

Verify the registration status of the recording devices by using the “list registered-ip-stations” command. Verify that there is an entry for each recording channel from **Section 8.7**, with the client IP address of Application Enablement Services as **Station IP Address**, as shown below.

```
list 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	10.32.39.110
	1	1.302S		10.64.125.62
65001	1616	IP_Phone	y	10.32.39.105
	1	1.302S		10.64.125.62
<b>65001</b>	<b>1616</b>	<b>IP_API_A</b>	<b>y</b>	<b>10.64.125.72</b>
	<b>1</b>	<b>3.2040</b>		<b>10.64.125.32</b>
65002	9620	IP_Phone	y	10.32.39.108
	1	6.020S		10.64.125.62
<b>65002</b>	<b>9620</b>	<b>IP_API_A</b>	<b>y</b>	<b>10.64.125.72</b>
	<b>1</b>	<b>3.2040</b>		<b>10.64.125.32</b>

### 9.2. Verify Avaya Proactive Contact

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

tcp	0	0	lzpds4b:enserver_ssl	lzpds4b:11101	ESTABLISHED
<b>tcp</b>	<b>0</b>	<b>0</b>	<b>lzpds4b:enserver_ssl</b>	<b>10.32.39.130:49711</b>	<b>ESTABLISHED</b>

### 9.3. 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**, as shown below.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to **Status and Control**, with **TSAPI Service Summary** selected. The main content area displays the **TSAPI Link Details** screen. At the top, there is a welcome message and login information. Below this, there is a checkbox for "Enable page refresh every 60 seconds". A table lists the TSAPI link details:

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="checkbox"/>	1	S8800	2	Talking	Mon Jun 4 10:09:07 2012	Online	16	4	21	17	30

Below the table, there are buttons for "Online" and "Offline". At the bottom, there is a section for "For service-wide information, choose one of the following:" with buttons for "TSAPI Service Status", "TLink 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. In the lower portion of the screen, verify that the **User** column shows an active session with the VPI user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of recording devices/channels from **Section 8.7**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to **Status and Control**, with **DMCC Service Summary** selected. The main content area displays the **DMCC Service Summary - Session Summary** screen. At the top, there is a welcome message and login information. Below this, there is a checkbox for "Enable page refresh every 60 seconds". The screen shows session summary statistics:

Session Summary [Device Summary](#)  
Generated on Wed Jun 20 08:24:26 MDT 2012  
Service Uptime: 13 days, 22 hours 53 minutes  
Number of Active Sessions: 1  
Number of Sessions Created Since Service Boot: 19  
Number of Existing Devices: 2  
Number of Devices Created Since Service Boot: 55

A table lists the session details:

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	E988BA45D125EB16F CC94693F6049C79-23	vpi	VoicePrintServer	20.32.39.130	XML Unencrypted	2

Below the table, there are buttons for "Terminate Sessions" and "Show Terminated Sessions".



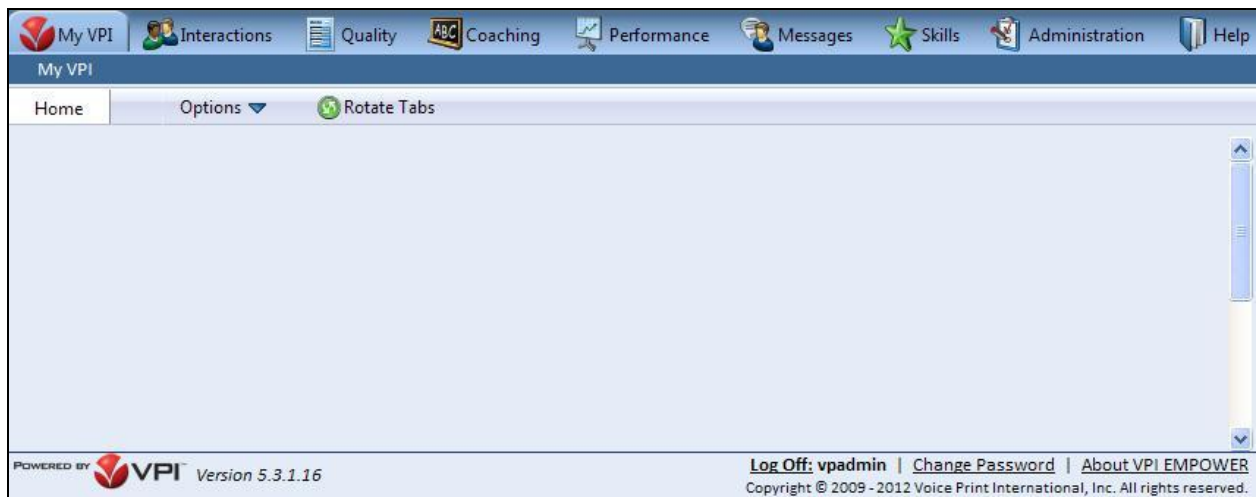
## 9.4. Verify VPI Voice Capture

Start a job on Proactive Contact, and log an agent in to handle and complete a call. Access the Voice Capture web-based interface by using the URL “https://ip-address/VPortal” in an Internet browser window, where “ip-address” is the IP address of the Voice Capture server. Log in using the appropriate credentials.

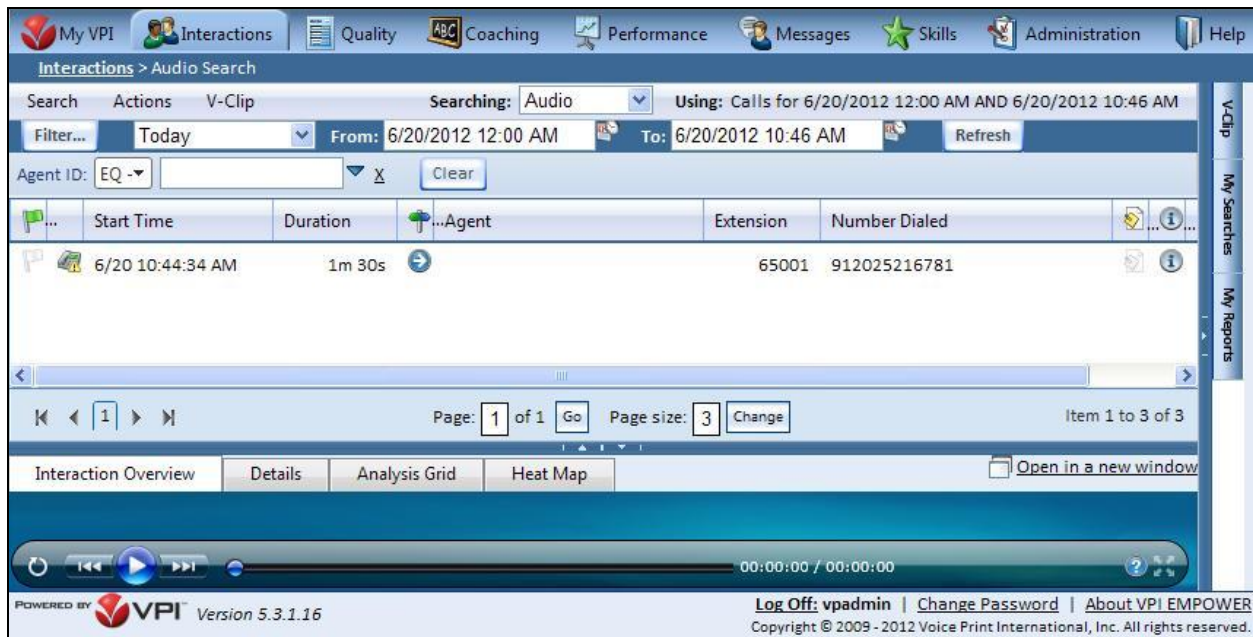


The image shows a web-based login interface for VPI Voice Capture. It features a light blue background with a central login box. Inside the box, there are two input fields: "User Name:" and "Password:". To the right of the password field is a "Login" button. A small lock icon is visible in the bottom left corner of the login box. At the bottom of the page, there is a footer that reads "POWERED BY VPI Version 5.3.1.16" and "About VPI EMPOWER Copyright © 2009 - 2012 Voice Print International, Inc. All rights reserved."

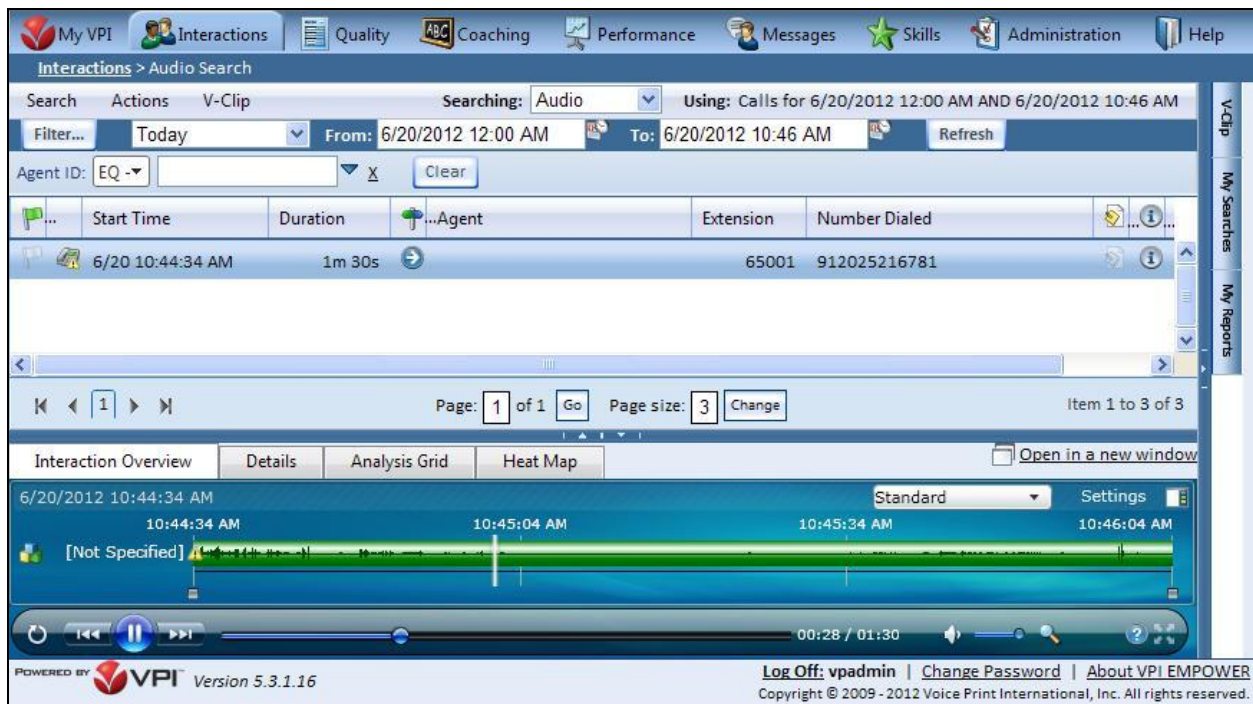
The screen below is displayed next. Select **Interactions** → **Audio Search** from the top menu.



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



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





## 10. Conclusion

These Application Notes describe the configuration steps required for VPI Voice Capture to successfully interoperate with Avaya Proactive Contact 5.0.1 with PG230 and Avaya Aura® Application Enablement Services 6.1.2. 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. *VPI Empower Channel Manager Reference Guide*, May 2012, available on the VPI Voice Capture server as part of installation.

---

**©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](mailto:devconnect@avaya.com).