



Avaya Solution & Interoperability Test Lab

Application Notes for VPI Voice Capture with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services 6.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Voice Print International Voice Capture to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.1. Voice Print International Voice Capture is a call recording solution. In the compliance testing, the Voice Print International Voice Capture used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor stations on Avaya Aura® Communication Manager, and used the Multiple Registration feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture the media associated with the monitored stations 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 Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.1. VPI Voice Capture is a call recording solution. In the compliance testing, the VPI Voice Capture used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor stations on Avaya Aura® Communication Manager, and used the Multiple Registration feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with the monitored stations for call recording.

The TSAPI interface is used by VPI Voice Capture to monitor the stations to be recorded, 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 TSAPI interface, and starts the call recording by using the media from the recording device associated with the monitored station. The TSAPI event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the VPI Voice Capture application, the application automatically requests monitoring on the stations to be recorded using TSAPI, and registers a recording device for each monitored station using DMCC.

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 user telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to VPI Voice Capture.

The verification of tests included using the VPI Voice Capture logs for proper message exchanges, and using the VPI Empower Suite web interface for proper logging and playback of the calls.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on VPI Voice Capture:

- 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, internal, external, ACD, non-ACD, hold, reconnect, simultaneous, conference, and transfer.

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

2.2. Test Results

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

- The user will not be able to playback the recording until the associated audio wave appears.
- The server can take up to 8 minutes to be fully functional and starts recording again after a link restoration.

2.3. Support

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

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

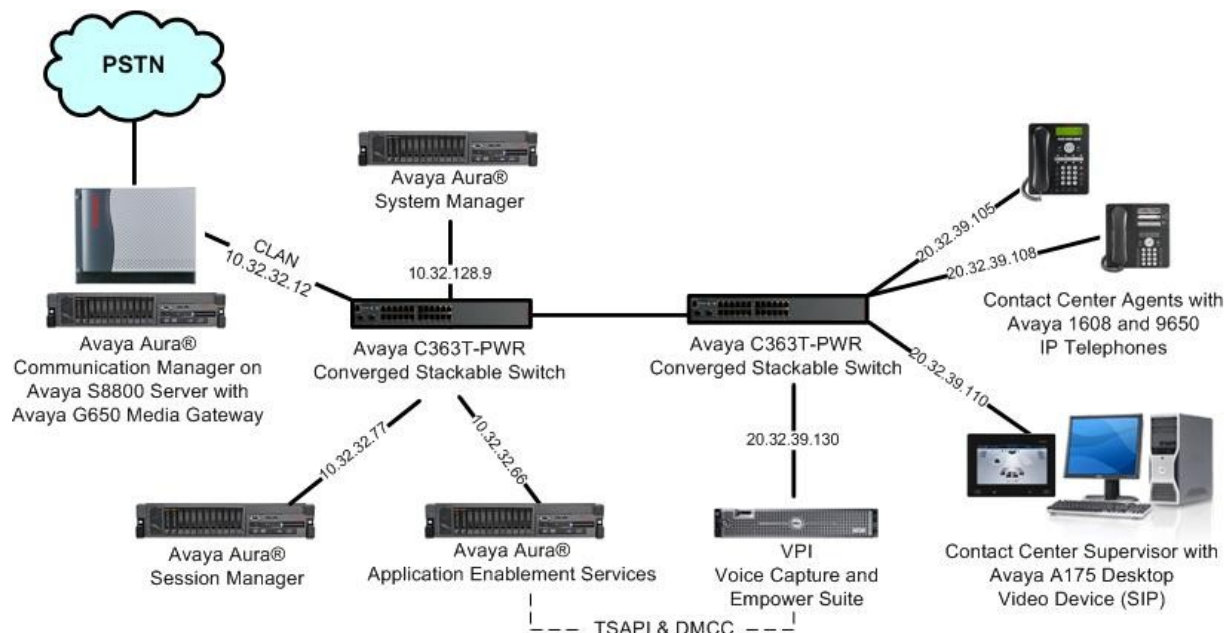
3. Reference Configuration

VPI 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 Avaya Aura® Session Manager was used in the configuration to support Avaya SIP endpoints. The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® System Manager. The detailed administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® 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, VPI Voice Capture monitored the contact center devices shown in the table below.

Device Type	Extension
VDN	65500
Skill Group	65555
Agent Station	65001, 65002



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 SP3 (R016x.00.1.510.1-19009)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media Processor	HW01 FW038 HW20 FW122
Avaya Aura® Application Enablement Services	6.1
Avaya Aura® Session Manager	6.1 SP2
Avaya Aura® System Manager	6.1 SP2
Avaya 1608 IP Telephones (H.323)	1.3
Avaya 9650 Series IP Telephones (H.323)	3.1
Avaya A175 Desktop Video Device (SIP)	1.0.2
VPI Voice Capture on Windows Server 2008 <ul style="list-style-type: none">Avaya TSAPI Windows Client	4.4.1.46 R2 Standard SP1 6.1.0.396
VPI Empower Suite	5.2.1.22

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager License
- Administer CTI link
- Administer system parameters features
- Administer stations

5.1. Verify Communication Manager 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)?	y	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?	n	DCS (Basic)?	y	
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	y	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 1		Page	1 of	3
CTI LINK				
CTI Link:	1			
Extension:	60100			
Type:	ADJ-IP			
		COR:	1	
Name:	VPI CTI 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: S8500-SAL
      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: 1
```

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

      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 VPI.

```
change station 65001
```

Page 1 of 4

STATION		
Extension: 65001	Lock Messages? n	BCC: 0
Type: 1608	Security Code: 65001	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: VPI Agent #1	Coverage Path 2:	COS: 6
	Hunt-to Station:	

STATION OPTIONS

Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 65001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:	Media Complex Ext:	
Survivable COR: internal	IP SoftPhone? y	
Survivable Trunk Dest? y		
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

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	S00000	VPI Agent #1			1	1			
	1608		no			1	1		
65002	S00045	VPI Agent #2			1	1			
	9650		no			1	1		

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Avaya Aura® 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 Application Enablement Services 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:". To the right of 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: Apr 18, 2011 4:49:38 PM EDT

[View Peak Usage](#)

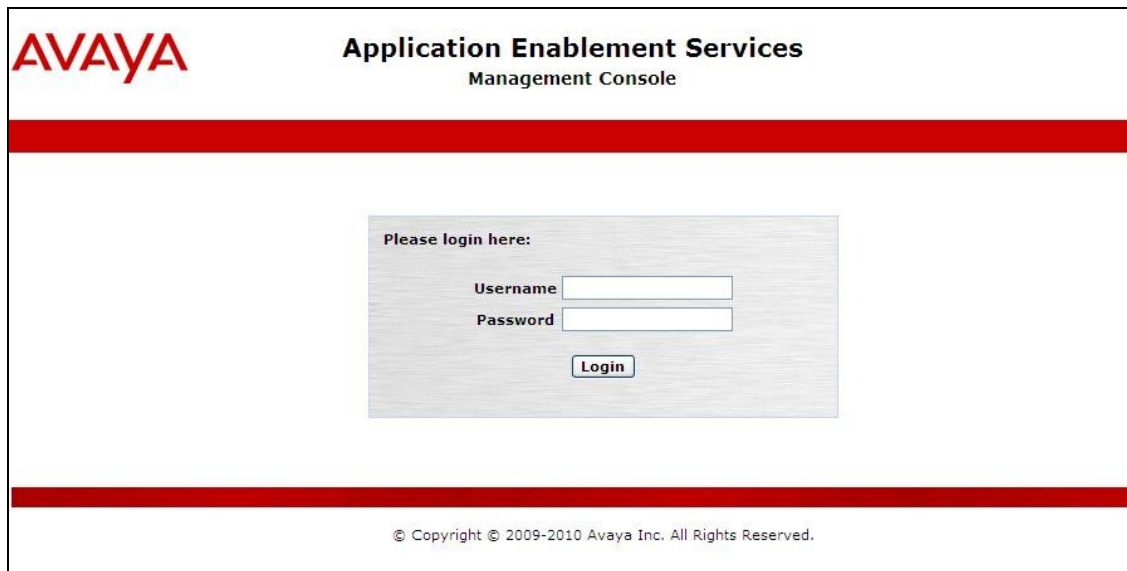
Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2011/10/15	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2011/10/15	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2011/10/15	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2011/10/15	16	0
Product Notes (VALUE_NOTES)	2011/10/15	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; IXP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; IXM_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;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	2011/10/15	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2011/10/15	1000	0
DLG (VALUE_AES_DLG)	2011/10/15	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2011/10/15	1000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2011/10/15	3	0

6.2. Launch OAM Interface

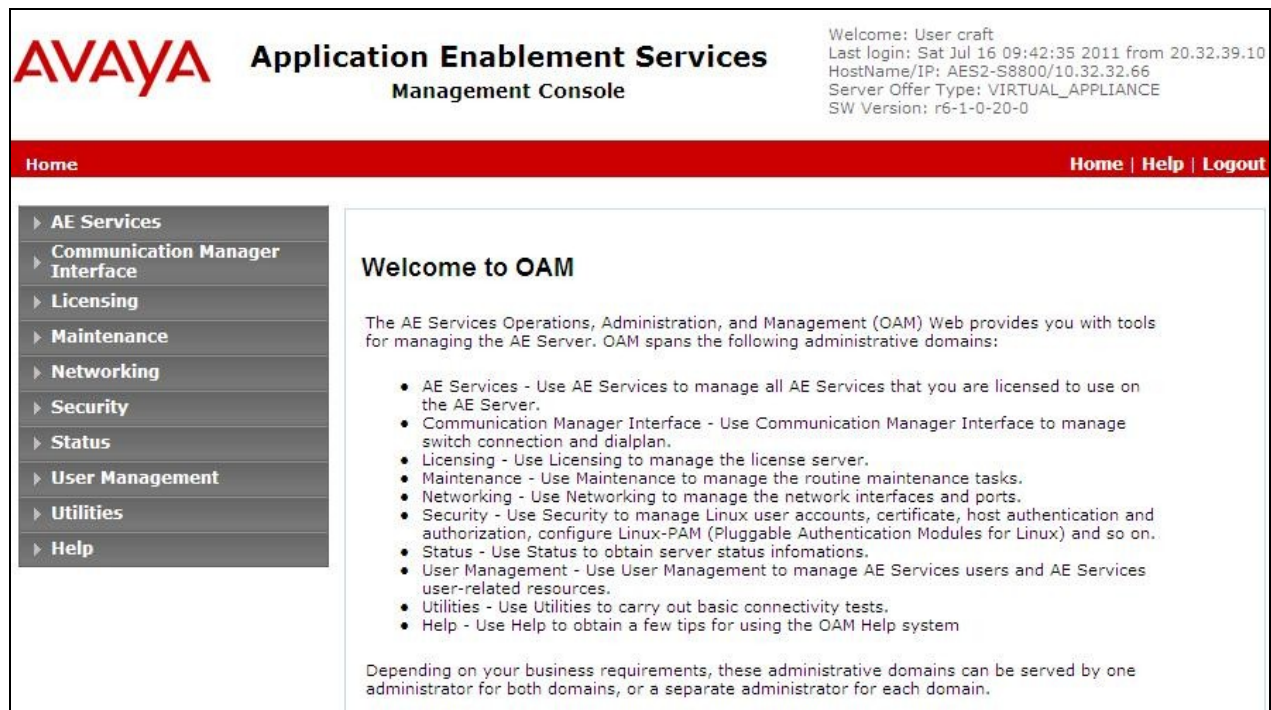
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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" and "Management Console" is displayed. Below this is a red horizontal bar. The main content area contains a light gray box with the text "Please login here:". Inside this box 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, there is a red horizontal bar and a copyright notice: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

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



The screenshot shows the Avaya Application Enablement Services Management Console "Welcome to OAM" screen. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. In the top right corner, there is a welcome message: "Welcome: User craft", "Last login: Sat Jul 16 09:42:35 2011 from 20.32.39.10", "HostName/IP: AES2-S8800/10.32.32.66", "Server Offer Type: VIRTUAL_APPLIANCE", and "SW Version: r6-1-0-20-0". Below this is a red horizontal bar with the text "Home" on the left and "Home | Help | Logout" on the right. The main content area is divided into two sections. On the left is a sidebar with a list of links: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". On the right is the "Welcome to OAM" section, which contains a paragraph: "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 administrative domains and their functions. At the bottom of the page, 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 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 infomations.
- 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 top header includes the AVAYA logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains "AE Services | TSAPI | TSAPI Links" and links for "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links", and "TSAPI Properties". The main content area is titled "TSAPI Links" and features a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "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 "Add TSAPI Links" screen in the AVAYA Application Enablement Services Management Console. The layout is similar to the previous screen, but the main content area is titled "Add TSAPI Links". It contains a form with the following fields: "Link" (value: 1), "Switch Connection" (value: S8800), "Switch CTI Link Number" (value: 1), "ASAI Link Version" (value: 4), and "Security" (value: Encrypted). At the bottom of the form are buttons for "Apply Changes" and "Cancel Changes".

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' > '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. There is one entry with Connection Name 'S8800', Processor Ethernet 'No', Msg Period '30', and Number of Active Connections '1'. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right corner shows user information: 'Welcome: User craft', 'Last login: Sat Jul 16 09:42:35 2011 from 20.32.39.10', 'HostName/IP: AES2-S8800/10.32.32.66', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r6-1-0-20-0'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> 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 “10.32.32.12” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8800' screen. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area has a text input field for 'Name or IP Address' and an 'Add Name or IP' button. Below the input field are 'Delete IP' and 'Back' buttons. The top right corner shows the same user information as the previous screenshot.

6.5. Disable Security Database

Select **Security > Security Database > Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below, 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 craft', 'Last login: Sat Jul 16 09:42:35 2011 from 20.32.39.10', 'HostName/IP: AES2-S8800/10.32.32.66', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r6-1-0-20-0'.

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 contains a table with two columns: 'Service' and 'Controller Status'. The 'TSAPI Service' row is checked. Below the table is a link 'Status and Control' and a row of buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right corner displays the same user information as the previous screenshot.

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 VPI.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA-S#AES2-S8800”. 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 user "craft" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar shows a tree view with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. Under Security, the "Security Database" is expanded, showing sub-items: Control, CTI Users, Devices, Device Groups, and Tlinks. The main content area, titled "Tlinks", shows a single entry with the Tlink Name "AVAYA#S8800#CSTA-S#AES2-S8800" and a "Delete Tlink" button.

Tlinks	
Tlink Name	AVAYA#S8800#CSTA-S#AES2-S8800
	<button>Delete Tlink</button>

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).

AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Jul 16 09:42:35 2011 from 20.32.39.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

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

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 craft
Last login: Sat Jul 16 09:42:35 2011 from 20.32.39.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

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

			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/>	<input type="radio"/>

DLG Port

	TCP Port			
	5678			

TSAPI Ports

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

DMCC Server Ports

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

7. Configure VPI Voice Capture

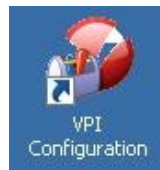
This section provides the procedures for configuring VPI Voice Capture. The procedures include the following areas:

- Launch VPI Configuration
- Administer start/stop events
- Administer TSAPI
- 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.

7.1. Launch VPI Configuration

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



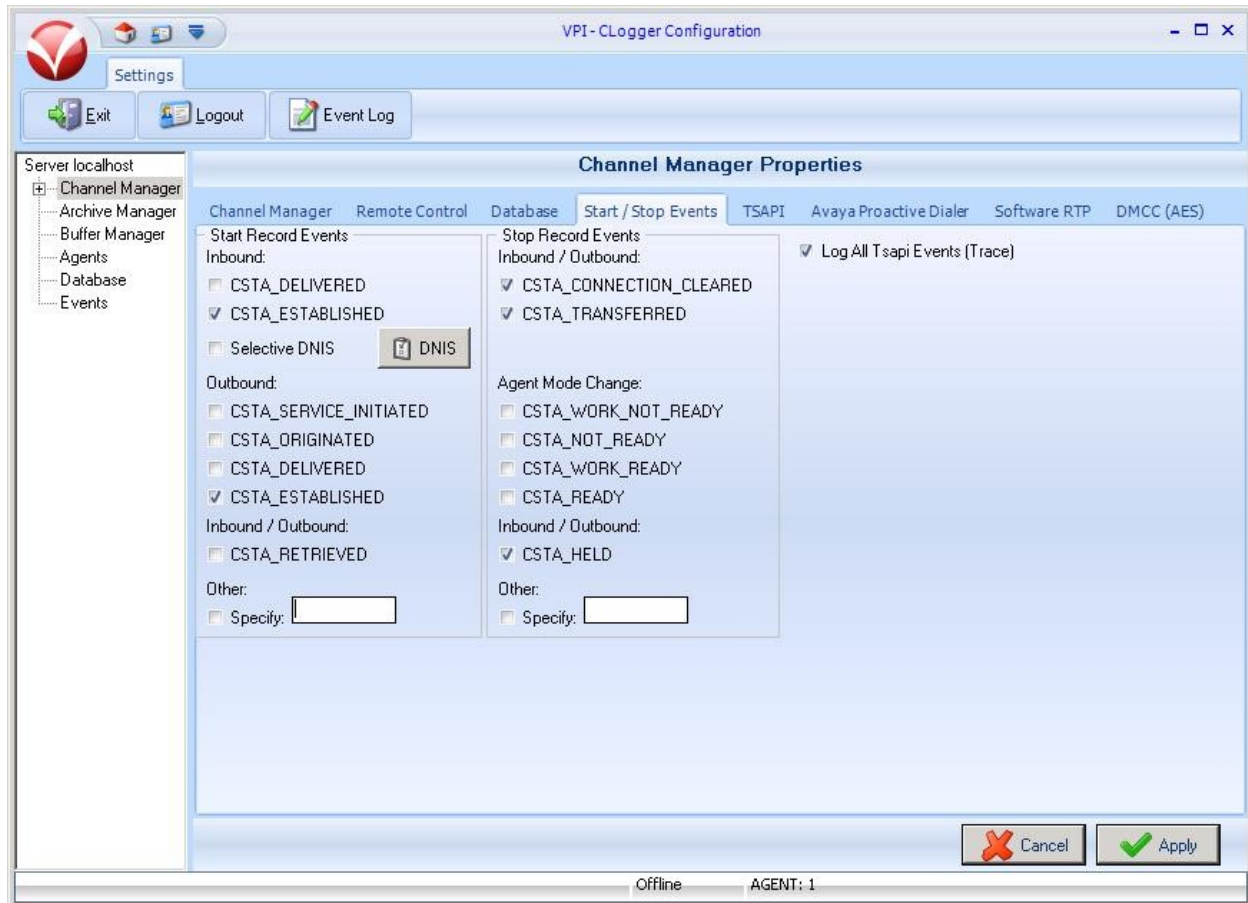
The **VPI - CLogger Configuration** screen is displayed. Click on **Login**, as shown below.



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

7.2. Administer Start/Stop Events

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**.



7.3. Administer TSAPI

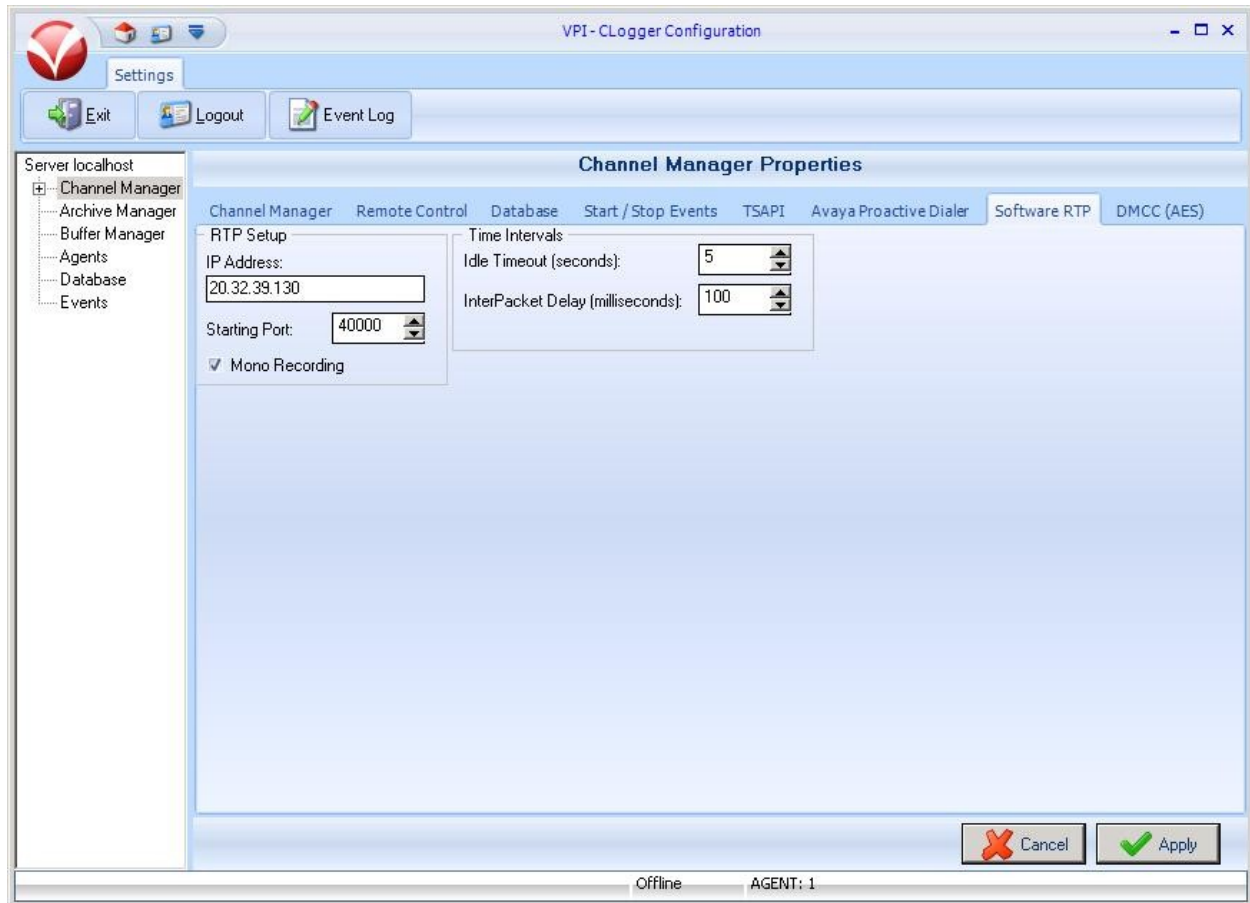
The **VPI - CLogger Configuration** screen is displayed again. Select **Server localhost > Channel Manager** in the left pane, to display the **Channel Manager Properties** screen. Select the **TSAPI** tab in the right pane. Enter the following values for the specified fields, and retain the default 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”
- **ACD Groups:** The group extensions to be monitored from **Section 3**.
- **VDNs:** The VDN extensions to be monitored from **Section 3**.

The screenshot shows the 'VPI - CLogger Configuration' window. On the left, a tree view shows 'Server localhost' expanded, with 'Channel Manager' selected. The main area displays the 'Channel Manager Properties' dialog box with the 'TSAPI' tab active. The 'TSAPI Server Setup' section contains fields for 'Server 1 Machine' (filled with 'AVAYA#S8800#CSTA-S'), 'Server 2 Machine' (empty), 'TSAPI Device' (empty), 'Application Username' (filled with 'vpi'), and 'Application Password' (masked with 'XXXXXXXX'). Below these are checkboxes for 'Fail to VOX' (unchecked) and 'Save All ANI' (checked). The 'Switch Type' section has radio buttons for 'CSTA Compliant', 'Avaya / Lucent' (selected), 'Nortel Meridian', 'Aspect', and 'NEC'. The 'General Options' section includes 'Record All Agents' (checked), 'Lock Status Lights' (unchecked), and 'Use Tsapi Time Stamp' (unchecked). The 'Additional Monitors' section has fields for 'ACD Groups' (filled with '65555'), 'Trunks' (empty), 'VDNs' (filled with '65500'), and 'Extensions' (empty). Below these are checkboxes for 'Disable recording of calls when SPLIT is empty' (unchecked) and 'Disable recording of calls when DISTRIBUTING VND is empty' (unchecked). The 'Service Observe Options' section includes 'Monitor Agent Mode Change' (unchecked) and a 'Feature Code' field (empty). The 'Recording Line Type' section has radio buttons for 'Extension Side' (selected) and 'Trunk Side' (unchecked). At the bottom right are 'Cancel' and 'Apply' buttons. The status bar at the bottom shows 'Offline' and 'AGENT: 1'.

7.4. 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 “20.32.39.130”. Retain the default values in the remaining fields, and click **Apply**.



7.5. 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 'Settings', 'Exit', 'Logout', and 'Event Log'. A left sidebar shows a tree view with 'Server localhost' expanded, containing 'Channel Manager', 'Channels', 'Archive Manager', 'Buffer Manager', 'Agents', 'Database', and 'Events'. The main area is titled 'Channel Manager Properties' and contains several tabs: 'Channel Manager', 'Remote Control', 'Database', 'Start / Stop Events', 'TSAPI', 'Avaya Proactive Dialer', 'Software RTP', and 'DMCC (AES)'. The 'DMCC (AES)' tab is active, showing 'General Options' and 'TLS (SSL) Options' sections. In 'General Options', 'Enable' is checked, 'Server IP Address' is '10.32.32.66', 'Switch (CLAN) Address' is '10.32.32.12', 'Server Port' is '4721', 'Session User' is 'vpi', and 'Session Password' is masked. In 'TLS (SSL) Options', 'Enable' is unchecked, 'Version' is 'SSL v2', 'AllowOlderVersions' 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 very bottom shows 'Offline' and 'AGENT: 1'.

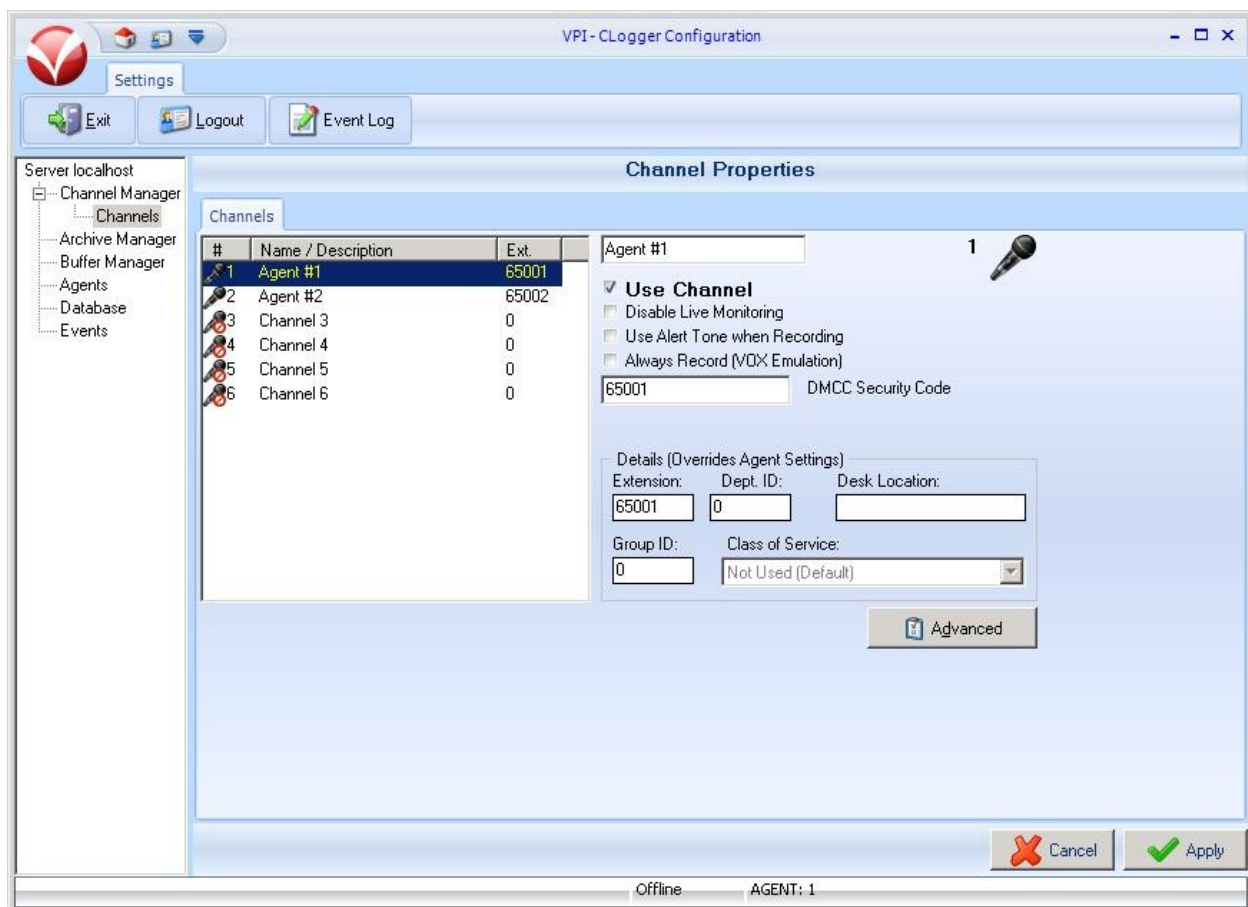
Field	Value
Enable	<input checked="" type="checkbox"/>
Server IP Address	10.32.32.66
Switch (CLAN) Address	10.32.32.12
Server Port	4721
Session User	vpi
Session Password	[Masked]
Global Ext Password	[Empty]
TLS (SSL) Options - Enable	<input type="checkbox"/>
TLS (SSL) Options - Version	SSL v2
TLS (SSL) Options - AllowOlderVersions	<input type="checkbox"/>
Certificate File	[Empty]
Client CA File	[Empty]
CA File	[Empty]
CA Path	[Empty]
Key File	[Empty]
Key Phrase	[Empty]
Packet Timeout	30
Connect Timeout	30
Verify Peer	<input type="checkbox"/>
Verify Depth	30

7.6. 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 agent station security code from **Section 5.4**.
- **Extension:** The agent 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 shows a tree view with 'Server localhost' expanded, and 'Channel Manager' > 'Channels' selected. The main area is titled 'Channel Properties' and contains a table of channels and configuration options for the selected channel, 'Agent #1'.

#	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

Configuration options for 'Agent #1':

- ☒ **Use Channel**
- ☐ Disable Live Monitoring
- ☐ Use Alert Tone when Recording
- ☐ Always Record (VOX Emulation)
- DMCC Security Code: 65001
- Details (Overrides Agent Settings):
 - Extension: 65001
 - Dept. ID: 0
 - Desk Location:
 - Group ID: 0
 - Class of Service: Not Used (Default)

Buttons: Cancel, Apply, Advanced

7.7. Launch Digital Call Logger

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

VPI - Digital Call Logger (v4.4.1.46 b4.4.1.46), ID: 1

Home Channels Buffer Devices Archive Devices

Disconnect Login Shutdown Event Log Server Status Environment Exit

Server Support System Information

Process	Status
Channel Manager 5	
Avaya Multiple Registration	Link OK, Manager Idle.
Channels Recording	0
Channels Idle	2
Channels Reporting Errors	0
Channels Enabled	2
Buffer Manager 3	
Primary Buffer 1	79% Free for use
Overflow Buffer 1	88% Free for use
LTS Buffer 1	79% Free for use
Database Manager 2	
VPData, Firebird 2.0.3.12981	Collecting Data... Store @ 8:53:42 AM
VPortal, SQL Server 10.50.1600.1 RTM	Collecting Data... Store @ 8:53:42 AM
Archive Manager 1	
Media Manager Service	Sweep Session @ 8:53:28 AM
Archive Devices 1	
Media Manager 1	99.84% Free. Process Idle.
Clients 0	

Login

8. Verification Steps

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

8.1. 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	AES2-S8800	established	103	32

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 7.6**, with the client IP address of Avaya Aura® AES as **Station IP Address**, 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		
65001	1608	IP_Phone	y	20.32.39.105		
	1	1.3000		10.32.32.12		
65001	1608	IP_API_A	y	10.32.32.66		
	1	3.2040		10.32.32.12		
65002	9650	IP_Phone	y	20.32.39.108		
	1	3.1000		10.32.32.12		
65002	9650	IP_API_A	y	10.32.32.66		
	1	3.2040		10.32.32.12		

8.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, as shown below.

AVAYA **Application Enablement Services**
Management Console

Welcome: User craft
Last login: Thu Jul 14 19:29:39 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

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	1	Talking	Thu Jul 14 19:06:07 2011	Online	16	4	16	24	30

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

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 7.6**.


Application Enablement Services
Management Console

Welcome: User craft
Last login: Thu Jul 14 19:29:39 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

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

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Thu Jul 14 20:22:26 EDT 2011

Service Uptime: 71 days, 22 hours 52 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 28
Number of Existing Devices: 2
Number of Devices Created Since Service Boot: 167

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	F51455DA5AC3BA952 5DA21AB12CA62A6-45	vpi	VoicePrintServer	20.32.39.130	XML Unencrypted	2

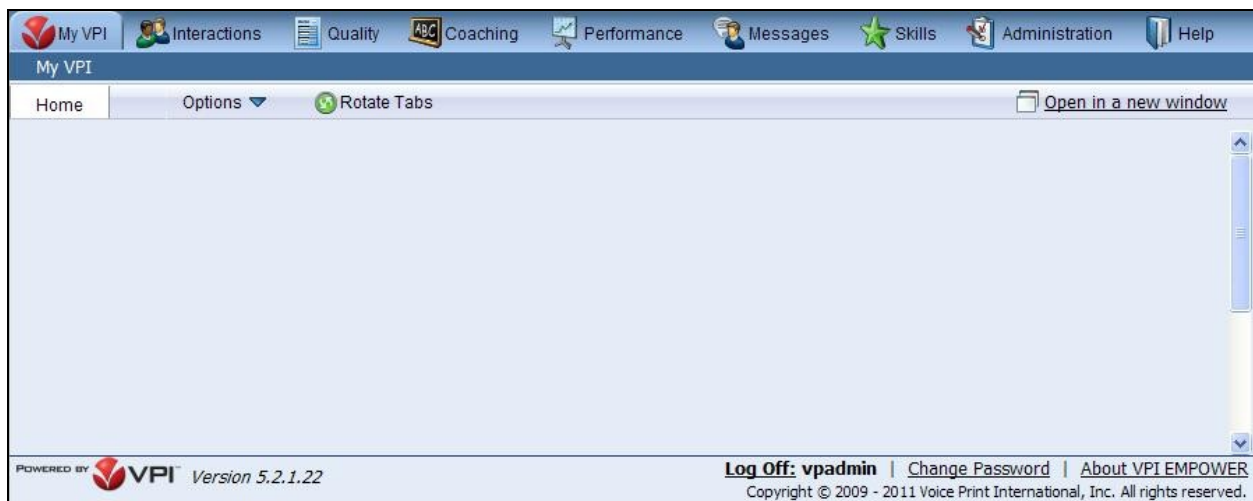
8.3. Verify VPI Voice Capture

Log an agent in to the skill group to handle and complete an ACD 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.

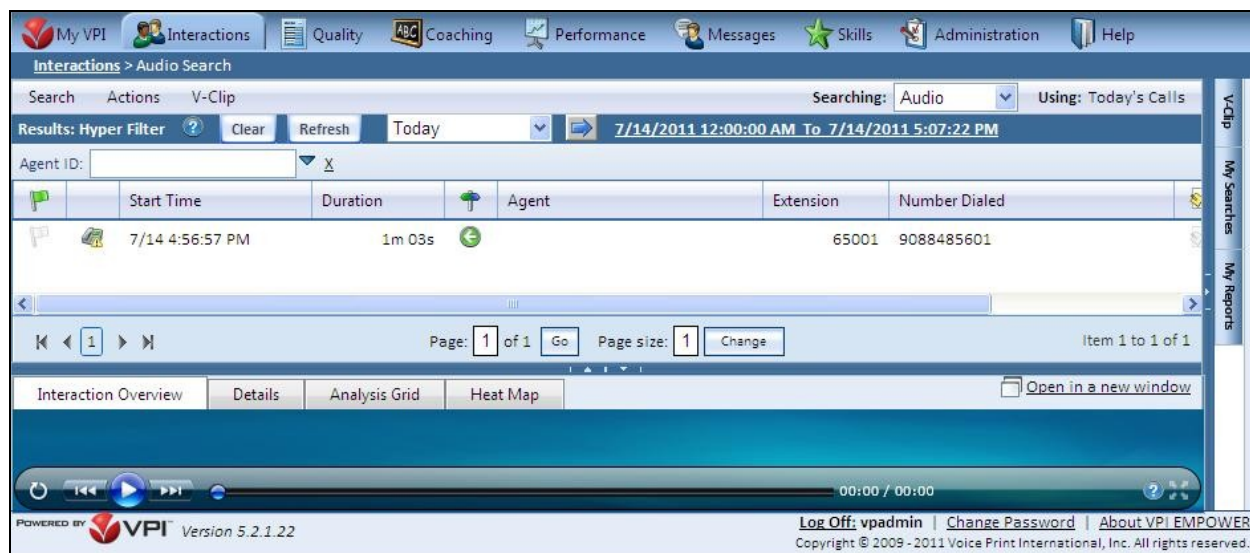


The image shows a web-based login interface for VPI Voice Capture. It features a central login box with two input fields: "User Name:" and "Password:". Below the password field is a "Login" button. To the left of the input fields is a small icon of a key. The background is light blue with a faint VPI logo. At the bottom, there is a footer area that includes the text "POWERED BY VPI Version 5.2.1.22" on the left, "About VPI EMPOWER" as a link in the center, and "Copyright © 2009 - 2011 Voice Print International, Inc. All rights reserved." on the right.

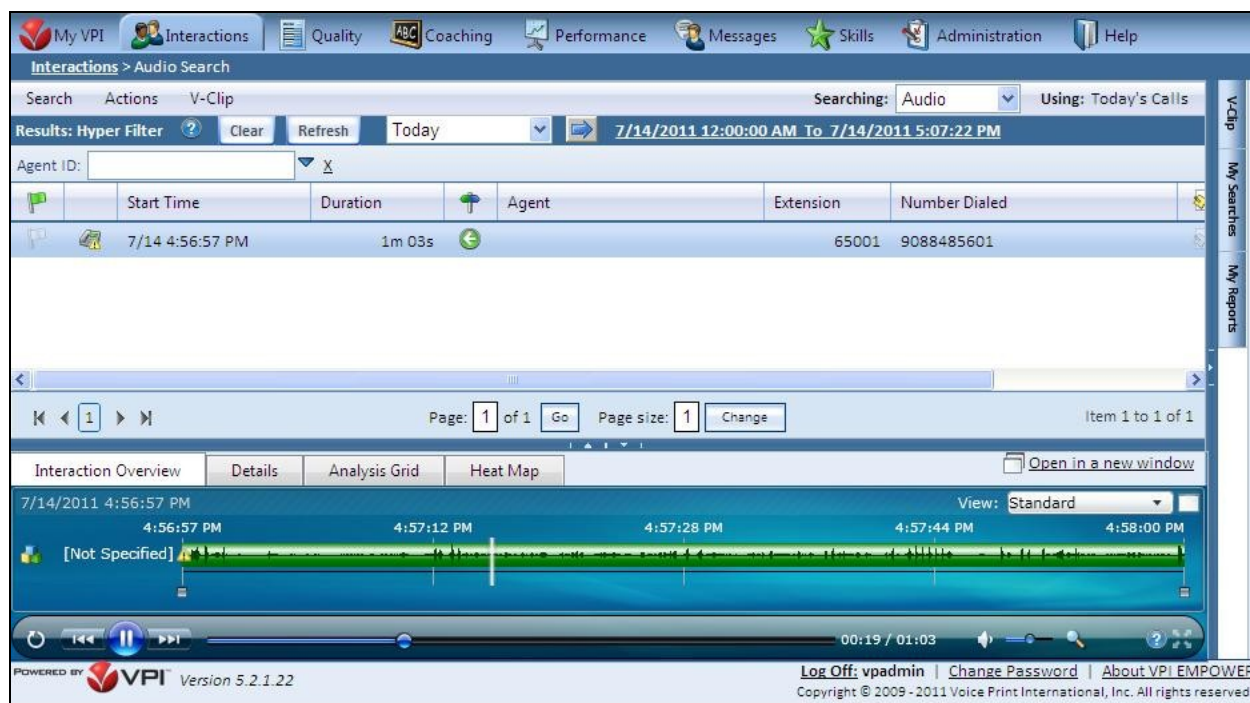
The screen below is displayed next. Select **Interactions > Audio Search** from the top menu.



The screen is updated with a list of the 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.



9. Conclusion

These Application Notes describe the configuration steps required for VPI Voice Capture to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. 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. *Avaya Multiple Registration Channel Manager Reference Guide*, July 2011, available on the VPI Empower Suite installation CD.

©2011 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.