



Avaya Solution & Interoperability Test Lab

Application Notes for VPI Capture Call Logger with Avaya Aura™ Communication Manager Using Avaya Aura™ Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Voice Print International Capture Call Logger to interoperate with Avaya Aura™ Communication Manager using Avaya Aura™ Application Enablement Services 5.2. Voice Print International Capture Call Logger is a call recording solution. In the compliance testing, the Voice Print International Capture Call Logger used the Telephony Services Application Programming Interface from Avaya Aura™ Application Enablement Services to monitor stations on Avaya Aura™ Communication Manager, and used the Single Step Conference 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 Capture Call Logger to interoperate with Avaya Aura™ Communication Manager using Avaya Aura™ Application Enablement Services 5.2. Voice Print International Capture Call Logger is a call recording solution. In the compliance testing, the Voice Print International Capture Call Logger 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 Single Step Conference 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 Capture Call Logger to monitor the stations to be recorded. When there is an active call on the monitored station, the VPI Capture Call Logger is informed of the call via event reports from the TSAPI interface. VPI Capture Call Logger starts the call recording by using the Single Step Conference feature from the DMCC with call control interface to add a virtual IP softphone to the active call, and using the Media Control Events from the DMCC interface to obtain the media from the virtual IP softphone. The TSAPI event reports are also used to determine when to stop the call recordings.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on VPI Capture Call Logger:

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

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

1.2. Support

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

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

2. Reference Configuration

VPI Capture Call Logger can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server configuration, as shown in **Figure 1**. VPI Capture Call Logger also has a VPI Playback Client application that can be used to review and playback the call recordings. In the compliance testing, the VPI Playback Client application was installed on the supervisor PC.

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 Capture Call Logger monitored the contact center devices shown in the table below.

Device Type	Extension
VDN	65500
Skill Group	65555
Supervisor Station	65000
Agent Station	65001, 65002

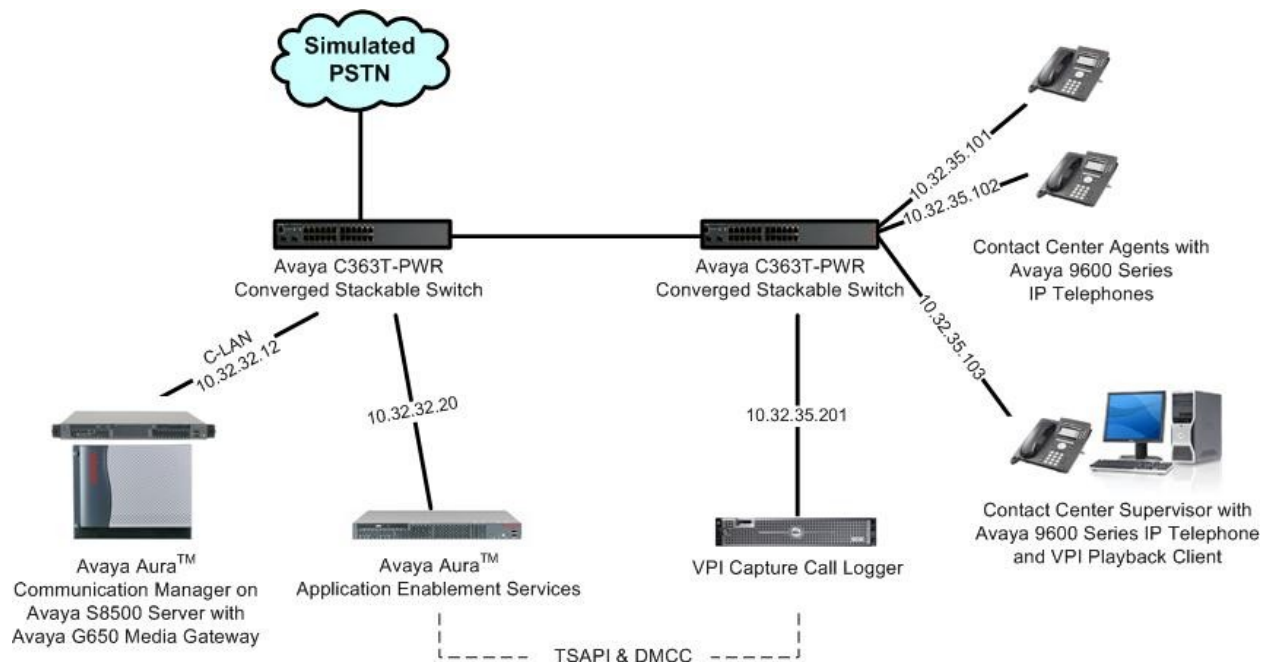


Figure 1: VPI Capture Call Logger with Avaya Aura™ Communication Manager Using Avaya Aura™ Application Enablement Services

3. Equipment and Software Validated

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

Equipment	Software
Avaya Aura™ Communication Manager on Avaya S8500 Server	R015x.02.0.947.3
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media Processor	HW01 FW024 HW20 FW120
Avaya Aura™ Application Enablement Services	5.2
Avaya 9600 Series IP Telephones (H.323)	3.0
VPI Capture Call Logger on Windows 2003 Server with Service Pack 2 <ul style="list-style-type: none">VP ConfigCapturePlayback ClientAvaya TSAPI Windows Client	2.8.4.22 4.3.9.12 4.0.20.0 5.2.1.474

4. 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 virtual IP softphones

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

4.2. 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			

4.3. 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 18
                        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

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 Capture Call Logger.

```
change system-parameters features                               Page 13 of 18
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
                                Clear Callr-info: next-call
      Allow Ringer-off with Auto-Answer? n

      Reporting for PC Non-Predictive Calls? n

                                Interruptible Aux Notification Timer (sec): 3
                                Interruptible Aux Deactivation Threshold (%): 95

ASAI
      Copy ASAI UUI During Conference/Transfer? y
      Call Classification After Answer Supervision? y
                                Send UCID to ASAI? y
```

4.4. Administer Virtual IP Softphones

Add a virtual softphone using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** “4620”
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 5
STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 4620	Security Code: 65990	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: VPI Virtual #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 65991	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
Survivable GK Node Name:	Media Complex Ext:	
Survivable COR: internal	IP SoftPhone? y	
Survivable Trunk Dest? y	IP Video Softphone? n	
	Customizable Labels? y	

Repeat this section to administer the desired number of virtual softphones, using sequential extension numbers and the same security code for all virtual softphones. In the compliance testing, three virtual softphones were administered as shown below, to allow for simultaneous recording of all three monitored stations in **Section 2**.

list station 65991 count 3									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65991	S00002	VPI Virtual #1			1				
	4620		no		1				
65992	S00005	VPI Virtual #2			1				
	4620		no		1				
65993	S00008	VPI Virtual #3			1				
	4620		no		1				

5. 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 TSAPI 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

5.1. Verify TSAPI License

Access the Web License Manager interface by using the URL “https://ip-address/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 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 **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below.

AVAYA 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: 5 - SID: 10503000 (Standard License File)

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

License installed on: Apr 16, 2010 11:27:38 AM EDT

[View Peak Usage](#)

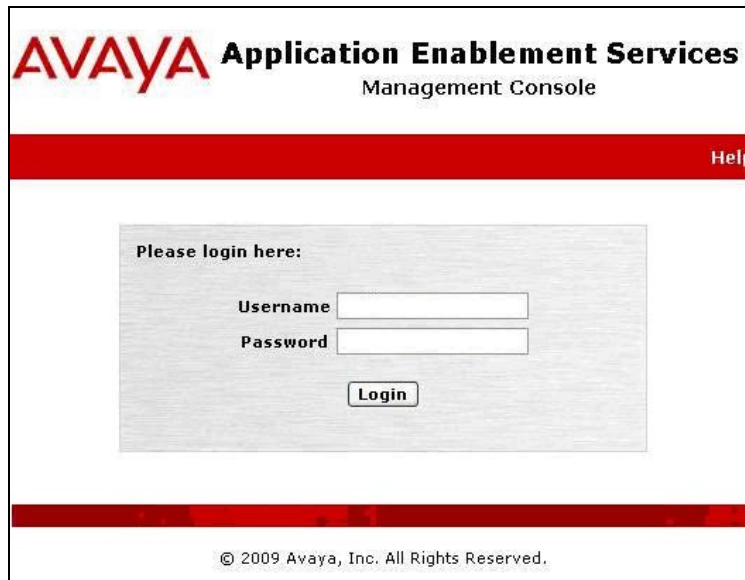
Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	100	0
DLG (VALUE_AES_DLG)	permanent	16	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0

5.2. Launch OAM Interface

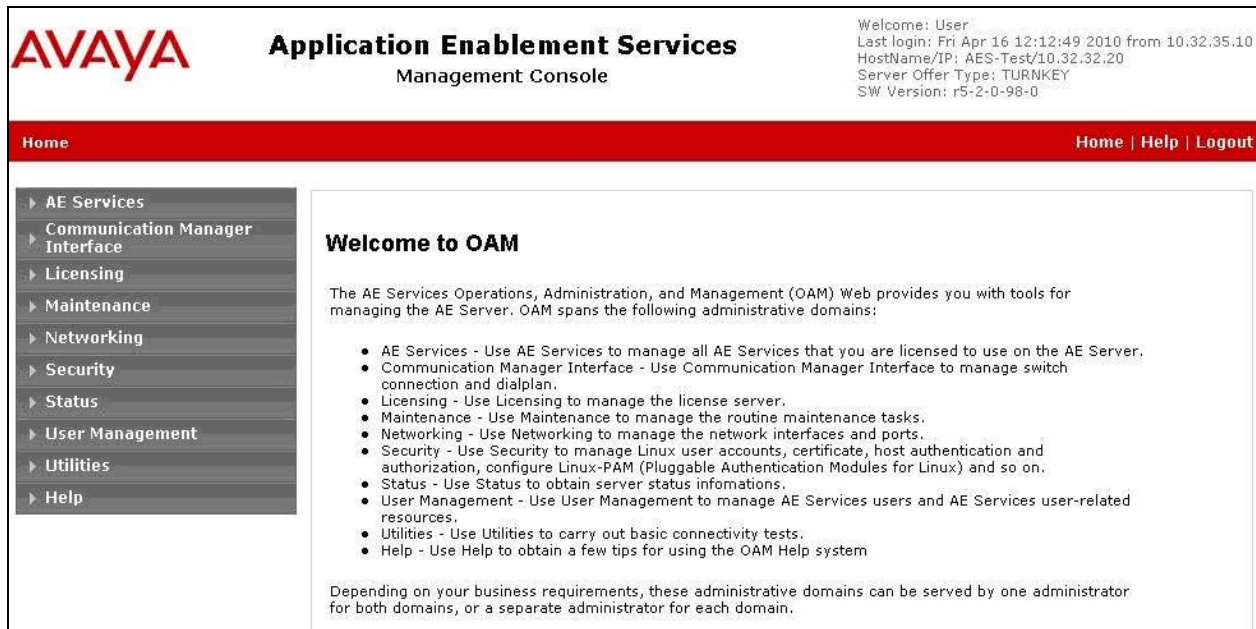
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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



The screenshot shows the login page of the AVAYA Application Enablement Services Management Console. At the top, the AVAYA logo is on the left, and the text "Application Enablement Services Management Console" is on the right. Below this is a red horizontal bar with the word "Help" in white on the right side. The main content area is a light gray box with the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button. At the bottom of the page, there is a red horizontal bar and a copyright notice: "© 2009 Avaya, Inc. All Rights Reserved."

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



The screenshot shows the "Welcome to OAM" screen of the AVAYA Application Enablement Services Management Console. At the top, the AVAYA logo is on the left, and the text "Application Enablement Services Management Console" is on the right. To the right of the header, there is a welcome message: "Welcome: User", "Last login: Fri Apr 16 12:12:49 2010 from 10.32.35.10", "HostName/IP: AES-Test/10.32.32.20", "Server Offer Type: TURNKEY", and "SW Version: r5-2-0-98-0". Below the header is a red horizontal bar with the word "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 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."

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Fri Apr 16 12:12:49 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Home | Help | Logout

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.

5.3. 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 the user. The left navigation pane shows a tree structure with "AE Services" expanded, containing "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 **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 "S8500" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 4.2**. 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" screen. The left navigation pane is the same as the previous screenshot, but "Communication Manager Interface" and "Licensing" are also visible under "TSAPI". The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (dropdown menu with value 1), "Switch Connection" (dropdown menu with value S8500), "Switch CTI Link Number" (dropdown menu with value 1), "ASAI Link Version" (dropdown menu with value 4), and "Security" (dropdown menu with value Unencrypted). At the bottom of the form are two buttons: "Apply Changes" and "Cancel Changes".

5.4. 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 “S8500”, 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 'S8500' as the connection name, 'No' for Processor Ethernet, '30' for Msg Period, and '0' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', and 'Delete Connection'. The 'Edit H.323 Gatekeeper' button is highlighted in yellow.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8500	No	30	0

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 - S8500' screen. The left navigation pane is the same as the previous screenshot. The main content area has a title 'Edit H.323 Gatekeeper - S8500'. Below the title is a text input field containing '10.32.32.12' and a button labeled 'Add Name or IP'. Below the input field is the label 'Name or IP Address' and a button labeled 'Delete IP'.

5.5. Disable Security Database

Select **Security > Security Database > Control** from the left pane, to display the **SDB Control for DMCC and TSAPI** screen in the right pane. Uncheck **Enable SDB TSAPI Service, JTAPI and Telephony Service**, 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 and TSAPI' and contains two checkboxes: 'Enable SDB for DMCC Service' (checked) and 'Enable SDB TSAPI Service, JTAPI and Telephony Service' (unchecked). An 'Apply Changes' button is at the bottom.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Fri Apr 16 13:22:45 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Security | Security Database | Control

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

SDB Control for DMCC and TSAPI

☒ Enable SDB for DMCC Service
☐ Enable SDB TSAPI Service, JTAPI and Telephony Service

5.6. 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' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' 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'.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Fri Apr 16 12:12:49 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Maintenance | Service Controller

Home | Help | Logout

AE Services
Communication Manager Interface
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status
User Management

Service Controller

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

For status on actual services, please use [Status and Control](#)

5.7. 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#S8500#CSTA#AES-TEST”. Note the use of the switch connection “S8500” from **Section 5.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security Database" expanded to show "Tlinks" selected. The main content area, titled "Tlinks", displays a single Tlink entry with the name "AVAYA#S8500#CSTA#AES-TEST" and buttons for "Edit Tlink" and "Delete Tlink".

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Fri Apr 16 12:12:49 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Security | Security Database | Tlinks Home | Help | Logout

Tlinks

Tlink Name
AVAYA#S8500#CSTA#AES-TEST
Edit Tlink Delete Tlink

5.8. 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: Fri Apr 16 12:12:49 2010 from 10.32.35.10', 'HostName/IP: AES-Test/10.32.32.20', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-0-98-0'. A red navigation bar contains 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'.

The left sidebar shows 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 includes a note: 'Fields marked with * can not be empty.' The form contains the following fields:

- * User Id: vpi
- * Common Name: vpi
- * Surname: vpi
- * User Password: [masked]
- * Confirm Password: [masked]
- Admin Note: [empty text box]
- Avaya Role: None (dropdown menu)
- Business Category: [empty text box]
- Car License: [empty text box]
- CM Home: [empty text box]
- Css Home: [empty text box]
- CT User: Yes (dropdown menu)
- Department Number: [empty text box]

5.9. 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: Fri Apr 16 13:22:45 2010 from 10.32.35.10
HostName/IP: AES-Test/10.32.32.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

▶ 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"/>

6. Configure VPI Capture Call Logger

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

- Launch Voice Print Server Configuration
- Administer TSAPI
- Administer software RTP
- Administer start/stop events
- Administer channels
- Launch Digital Call Logger

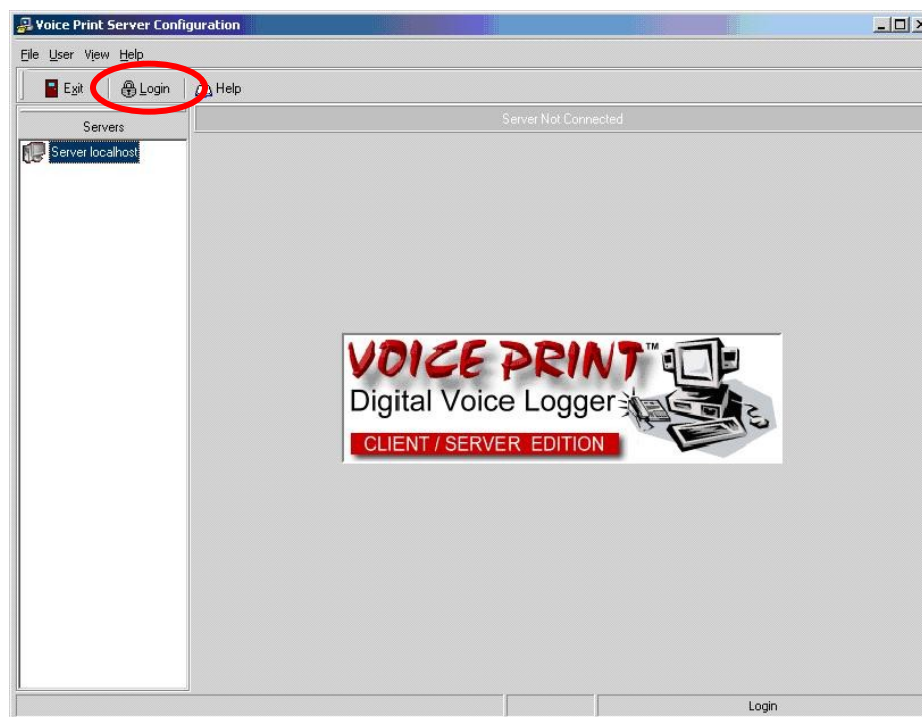
The configuration of VPI Capture Call Logger is performed by VPI installers. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch Voice Print Server Configuration

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



The **Voice Print Server Configuration** screen is displayed. Click on **Login**, as shown below.



The **Voice Print Login** screen is displayed next. Log in using the appropriate credentials.



6.2. Administer TSAPI

The **Voice Print Server Configuration** screen is displayed again. Select **Server localhost > Channel Manager** in the left pane, to display the **TSAPI** 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 5.7**.
- **Tsapi Device:** IP address of Application Enablement Services server.
- **Application Username:** The VPI user credentials from **Section 5.8**.
- **Application Password:** The VPI user credentials from **Section 5.8**.
- **Switch Type:** “Avaya / Lucent”
- **ACD Groups:** The group extensions to be monitored from **Section 2**.
- **VDNs:** The VDN extensions to be monitored from **Section 2**.
- **Monitor Agent Mode Change:** Uncheck this field.
- **Enable:** Check this field.
- **First Extension:** The starting virtual softphone extension from **Section 4.4**.
- **Extension Password:** The password for the virtual softphones from **Section 4.4**.
- **Server IP Address:** IP address of Application Enablement Services server.
- **Switch (CLAN) Address:** The IP address of the H.323 gatekeeper from **Section 5.4**.
- **Session User:** The VPI user credentials from **Section 5.8**.
- **Password:** The VPI user credentials from **Section 5.8**.

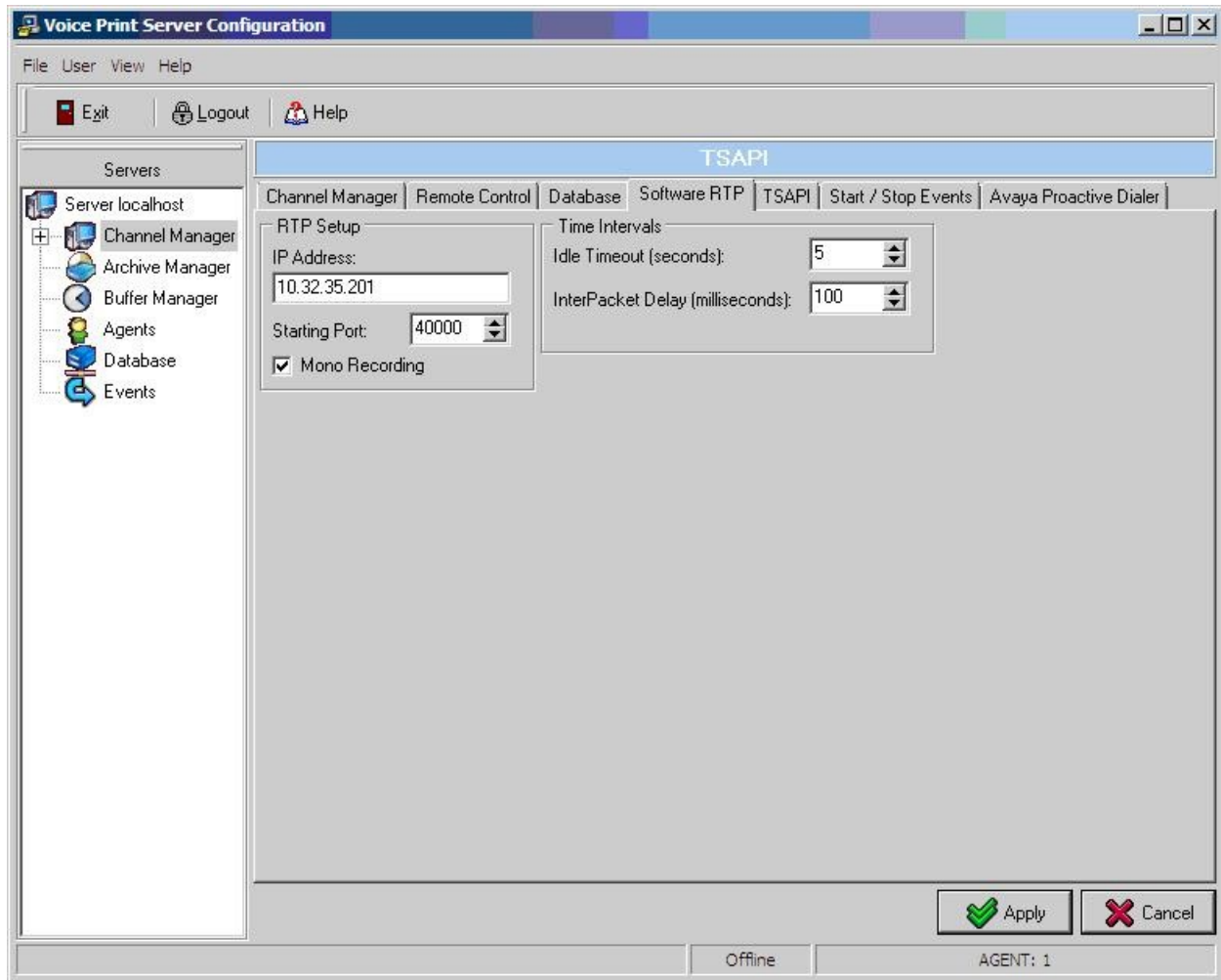
The screenshot shows the 'Voice Print Server Configuration' window with the 'TSAPI' tab selected. The left pane shows a tree view with 'Server localhost' expanded, and 'Channel Manager' selected. The main area contains several configuration sections:

- TSapi Server Setup:**
 - Server 1 Machine: AVAYA#S8500#CSTA#
 - Server 2 Machine: (empty)
 - Tsapi Device: 10.32.32.20
 - Application Username: vpi
 - Application Password: (masked)
 - ☐ Fail to VDX
 - ☒ Save All ANI
- General Options:**
 - ☒ Record All Agents
 - ☐ Lock Status Lights
 - ☐ Use Tsapi Time Stamp
- Additional Monitors:**
 - ACD Groups: 65555
 - Trunks: (empty)
 - VDNs: 65500
 - ☐ Disable recording of calls when SPLIT is empty
 - ☐ Disable recording of calls when DISTRIBUTING VND is empty
- Service Observe Options:**
 - ☐ Monitor Agent Mode Change
 - Feature Code: (empty)
- Switch Type:**
 - ☐ CSTA Compliant
 - ☒ Avaya / Lucent
 - ☐ Nortel Meridian
 - ☐ Aspect
 - ☐ NEC
- CMAPI (AES) Options:**
 - ☒ Enable
 - First Extension: 65991
 - Extension Password: (masked)
 - Server IP Address: 10.32.32.20
 - Server Port: 4721
 - Switch (CLAN) Address: 10.32.32.12
 - Session User: vpi
 - Password: (masked)

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

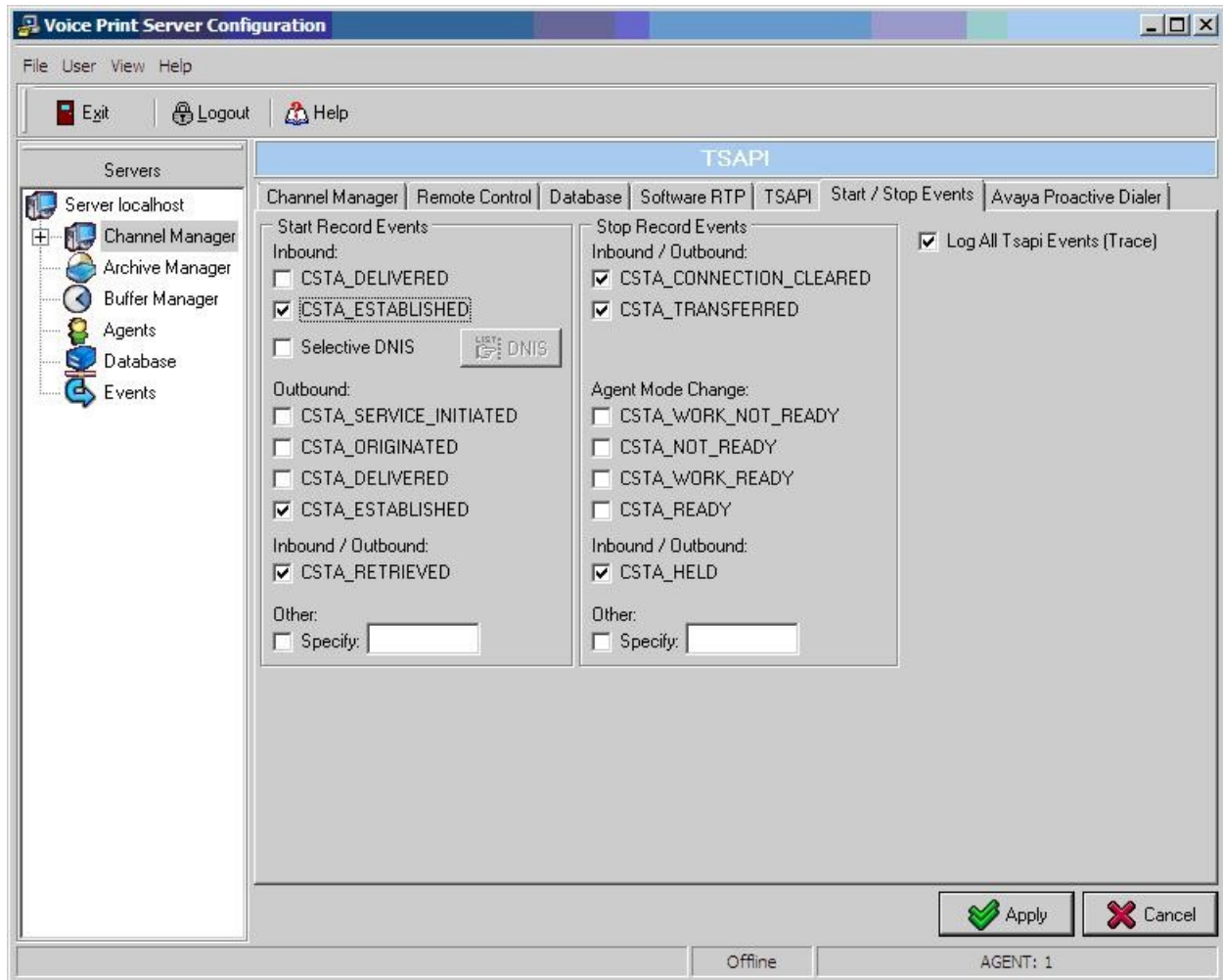
6.3. Administer Software RTP

Select the **Software RTP** tab in the right pane. For **IP Address**, enter the IP address of the VPI Capture Call Logger server, in this case “10.32.35.201”. Retain the default values in the remaining fields, and click **Apply**.



6.4. 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**.



6.5. 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.
- **Extension:** The extension of a station to be monitored from **Section 2**.

Repeat this section to administer a channel for each station to be monitored from **Section 2**, and click **Apply**.

Voice Print Server Configuration

File User View Help

Exit Logout Help

Servers:

- Server localhost
 - Channel Manager
 - Channels**
 - Archive Manager
 - Buffer Manager
 - Agents
 - Database
 - Events

Channel Properties

Channels

#	Name / Description	Ext.
1	Agent1	65001
2	Agent2	65002
3	Supervisor	65000
4	Channel 4	0
5	Channel 5	0

Agent1

☒ **Use Channel**

☐ Disable Live Monitoring

☐ Use Alert Tone when Recording

☐ Always Record (VOX Emulation)

Details (Overrides Agent Settings)

Extension: 65001 Dept. ID: 0 Desk Location:

Group ID: 0 Class of Service: Not Used (Default)

Advanced

Apply Cancel

Offline AGENT: 1

6.6. Launch Digital Call Logger

From the VPI Capture Call Logger 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 (v4.3.9.12 b4.3.9.12), ID: 1

Home Channels Buffer Devices Archive Devices

Login Shutdown Exit Event Log Server Status Environment

Server Support System Information

Process	Status
Channel Manager	5
TSAPI	Link OK, Manager Idle.
Channels Recording	0
Channels Idle	3
Channels Reporting Errors	0
Channels Enabled	3
Buffer Manager	3
Primary Buffer 1	79% Free for use
Overflow Buffer 1	89% Free for use
LTS Buffer 1	76% Free for use
Database Manager	1
Firebird 2.0.3.12981	Collecting Data... Store @ 11:02:22 AM
Archive Manager	1
Network Mass Storage	Sweep Session @ 11:03:38 AM
Archive Devices	1
Archive Device 1, Media ID: 1	96.48% Free. Process Idle.
Clients	0

7. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the VPI Capture Call Logger application, the application automatically registers the virtual IP softphones to Avaya AuraTM Communication Manager using Avaya AuraTM Application Enablement Services DMCC, and requests monitoring on the stations to be recorded using Avaya AuraTM Application Enablement Services TSAPI.

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 Capture Call Logger.

The verification of tests included using the VPI Capture Call Logger logs for proper message exchanges, and using the VPI Playback Client application for proper logging and playback of the calls.

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

- When the VPI server is configured to not use the Held event to start a new recording, then in the attended transfer and blind/attended conference scenarios, the ANI used in the recording entry for the first agent is the transferred-to/conferenced-to destination instead of the original incoming trunk.
- The softphone allocations are dedicated. When the allocated softphone for a monitored station cannot be registered for some reason, then there will be no call recordings for that station.

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 Capture Call Logger.

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 4.2**, 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-Test	established	20	20

Verify the registration status of the virtual softphones by using the “list registered-ip-stations” command. Verify that all extensions from **Section 4.4** are displayed, as shown below.

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

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address	
65000	9640	IP_Phone	y	10.32.35.105	
	1	3.0020		10.32.32.12	
65001	9650	IP_Phone	y	10.32.35.101	
	1	3.0020		10.32.32.12	
65002	9640	IP_Phone	y	10.32.35.106	
	1	3.0020		10.32.32.12	
65991	4620	IP_API_A	y	10.32.32.20	
	1	3.2040		10.32.32.12	
65992	4620	IP_API_A	y	10.32.32.20	
	1	3.2040		10.32.32.12	
65993	4620	IP_API_A	y	10.32.32.20	
	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 5.3**, as shown below.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to **Status and Control > TSAPI Service Summary**. The main content area displays the **TSAPI Link Details** screen. At the top right, a welcome message for 'User' is shown, along with login details and version information. Below the navigation pane, there is a table of TSAPI links. The table has columns: Link, Switch Name, Switch CTI Link ID, Status, Since, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period. The first row shows a link with ID 1, Switch Name S8500, Status Talking, and State Online. Below the table, there are buttons for 'Online' and 'Offline'. At the bottom, there are buttons for 'TSAPI Service Status', 'TLink Status', and 'User Status'.

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	S8500	1	Talking	Fri Apr 16 15:49:31 2010	Online	15	5	21	21	30

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 5.8**, and that the **# of Associated Devices** column reflects the number of virtual softphones from **Section 4.4**.

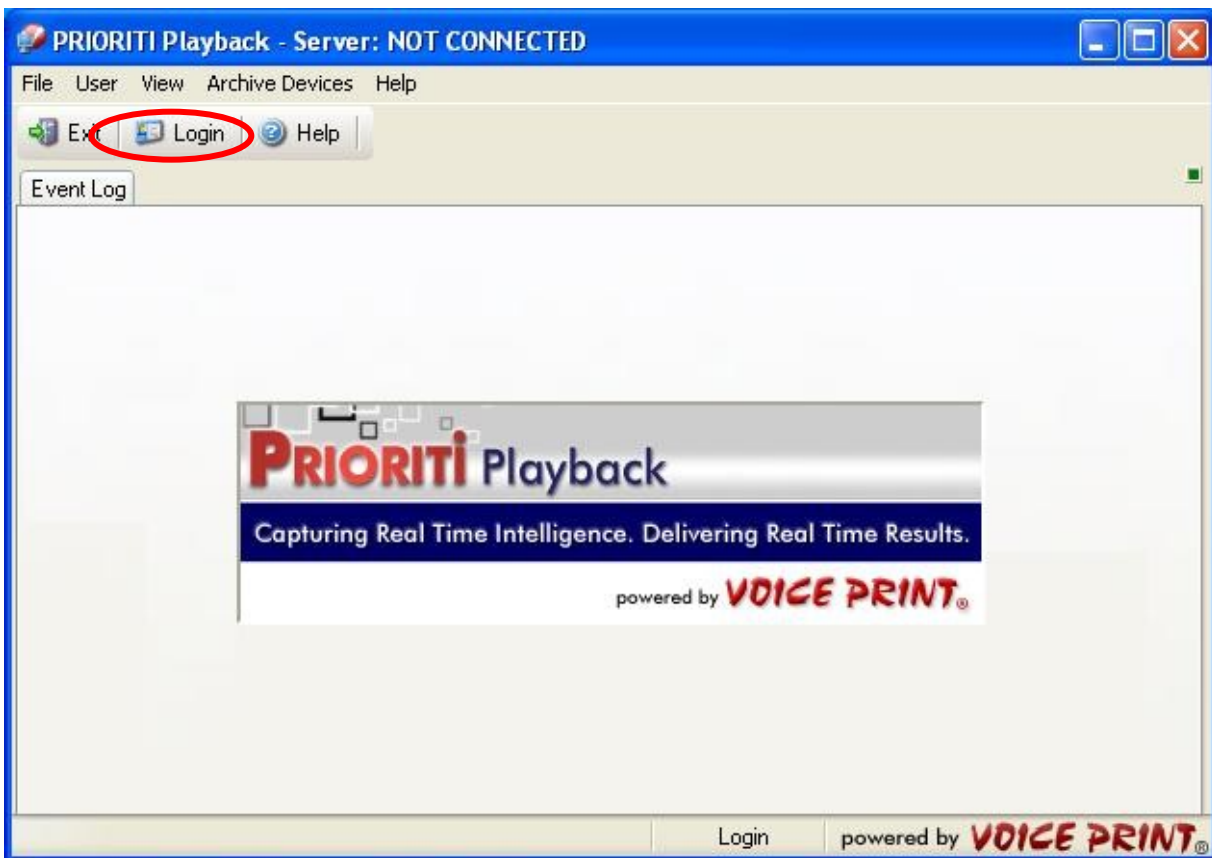
The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to **Status and Control > DMCC Service Summary**. The main content area displays the **DMCC Service Summary - Session Summary** screen. At the top right, a welcome message for 'User' is shown, along with login details and version information. Below the navigation pane, there is a summary of the DMCC service. The summary includes: Session Summary, Device Summary, Generated on Mon Apr 19 11:08:53 EDT 2010, Service Uptime: 2 days, 19 hours 18 minutes, Number of Active Sessions: 1, Number of Sessions Created Since Service Boot: 1, Number of Existing Devices: 3, and Number of Devices Created Since Service Boot: 3. Below the summary, there is a table of sessions. The table has columns: Session ID, User, Application, Far-end Identifier, Connection Type, and # of Associated Devices. The first row shows a session with ID CEF4D9C88B3334777, User vpi, Application VoicePrintServer, Far-end Identifier 10.32.35.201, Connection Type XML Unencrypted, and # of Associated Devices 3. Below the table, there are buttons for 'Terminate Sessions' and 'Show Terminated Sessions'.

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
CEF4D9C88B3334777 3F179D042724018-1482	vpi	VoicePrintServer	10.32.35.201	XML Unencrypted	3

8.3. Verify VPI Capture Call Logger

Log an agent in to the Skill group to handle and complete an ACD call. From the PC running the VPI Client Playback application, select **Start > Programs > VPI > VPI Playback Client** to launch the **VPI Playback Client** application.

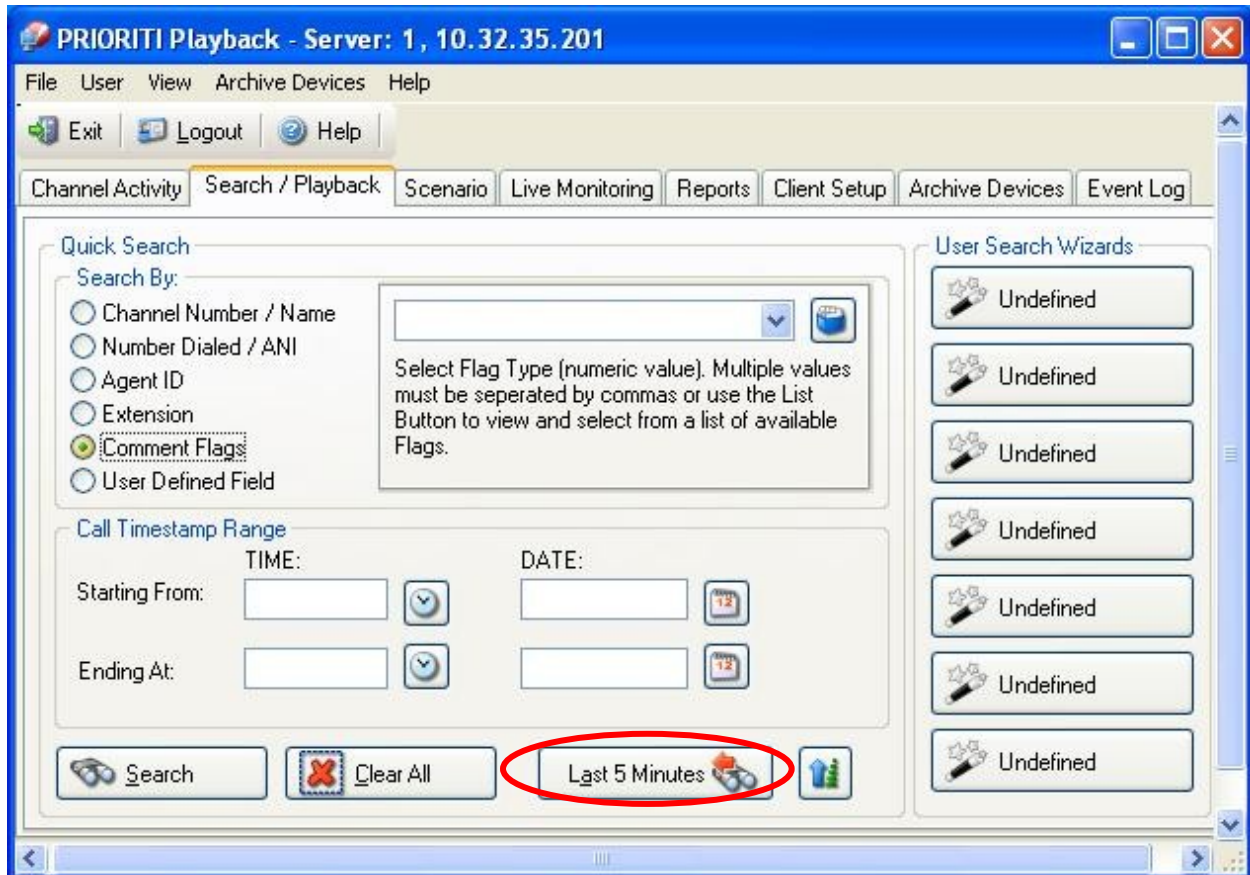
The **PRIORITI Playback** screen is displayed. Click Login.



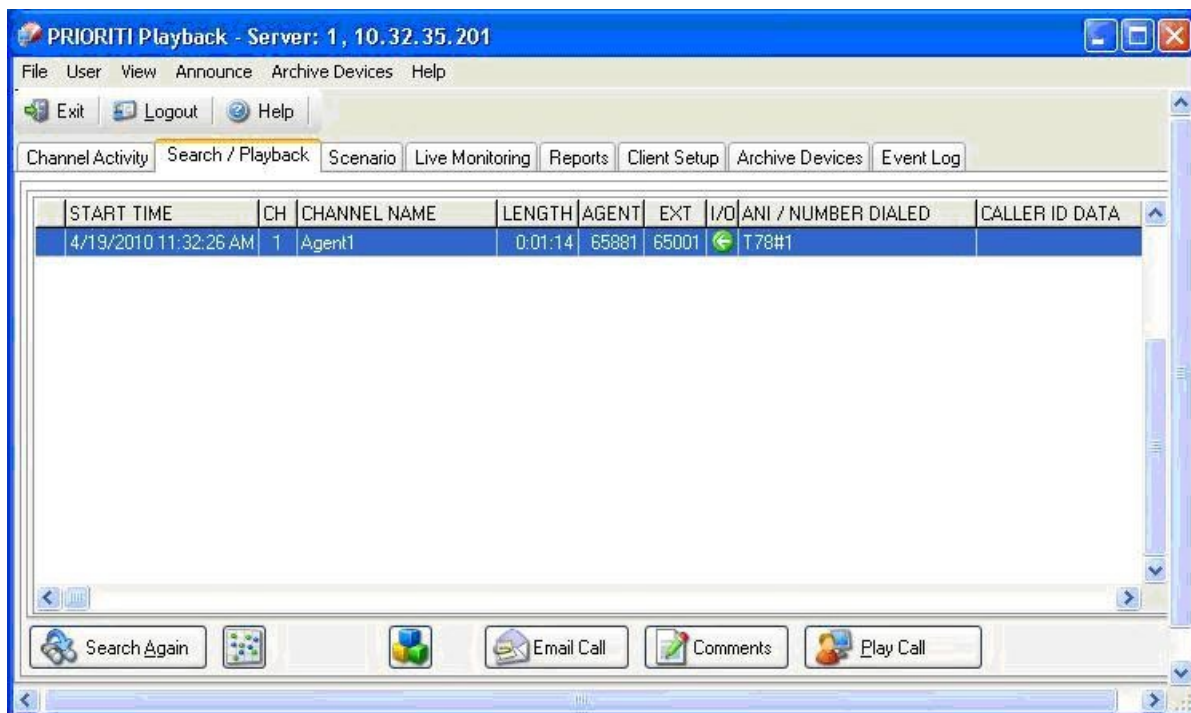
The **Voice Print Login** screen is displayed next. Retain the default value in the **Connect to** field, and enter the appropriate credentials to log in.



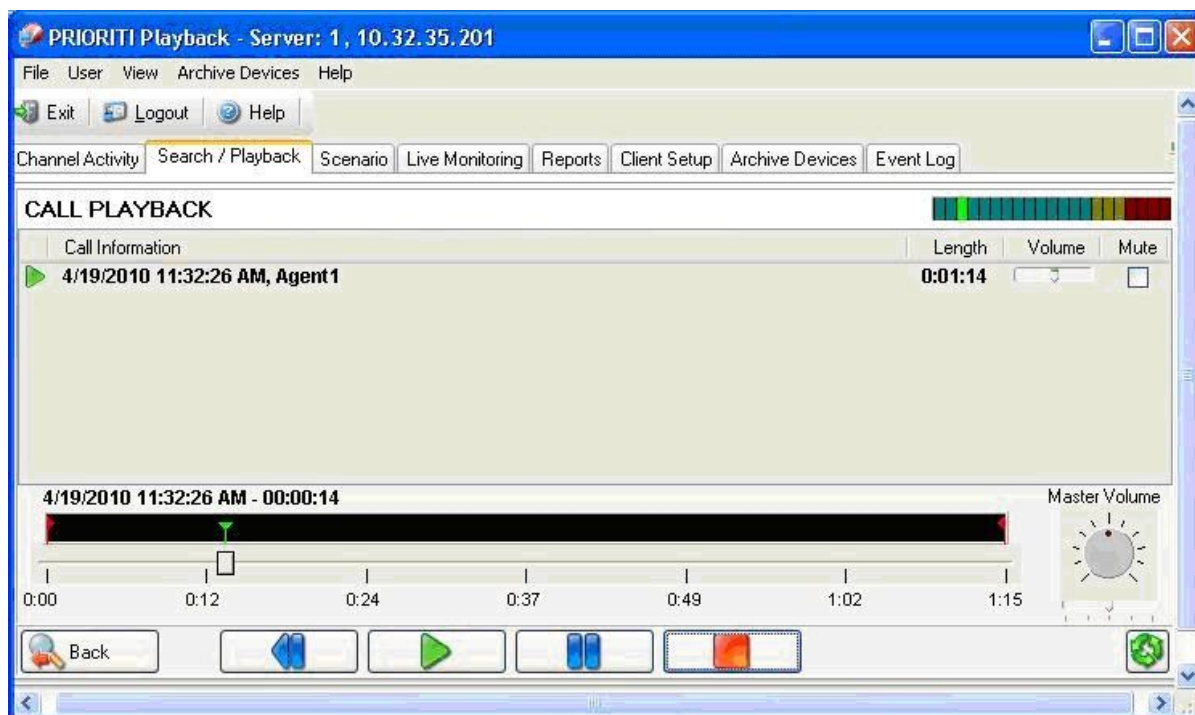
The **PRIORITI Playback** screen is displayed again and updated. Select the **Search / Playback** tab. Retain the default values, and click on **Last 5 Minutes**. If more than five minutes have elapsed since the call, then select the appropriate values for **Call Timestamp Range** and click **Search**.



The **PRIORITI Playback** screen is updated with a list of the call recordings from the last five minutes. 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 Capture Call Logger to successfully interoperate with Avaya Aura™ Communication Manager using Avaya Aura™ Application Enablement Services 5.2. All feature and serviceability test cases were completed with observations noted in **Section 7**.

10. Additional References

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

1. *Administrator Guide for Avaya Aura™ Communication Manager*, Document 03-300509, Issue 5.0, Release 5.2, May 2009, available at <http://support.avaya.com>.
2. *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Release 5.2, Document ID 02-300357, Issue 11, November 2009, available at <http://support.avaya.com>.
3. *VPI Activ! Voice Configuration Guide (VPConfig)*, Version 4.0, available on the VPI Capture Call Logger server as part of installation.

©2010 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.