



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

---

# **Application Notes for VPI EMPOWER Suite with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 Using Station Tap – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for Voice Print International EMPOWER Suite to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using station tap. Voice Print International EMPOWER Suite provides solutions for interaction recording, quality monitoring, performance management, and eLearning. The compliance testing focused on the recording solution.

In the testing, Voice Print International EMPOWER Suite used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and used the station tap method to capture media associated with the monitored agent 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) EMPOWER Suite to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using station tap. VPI EMPOWER Suite provides solutions for interaction recording, quality monitoring, performance management, and eLearning. The compliance testing focused on the recording solution.

In the testing, VPI EMPOWER Suite used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor VDNs, skill groups, and agent digital stations on Avaya Aura® Communication Manager, and used the station tap method to capture media associated with the monitored agent digital stations for call recording.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the EMPOWER Suite recording application, the application automatically requests monitoring on VDNs, skill groups, and agent stations.

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

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to EMPOWER Suite.

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

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

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on EMPOWER Suite:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, multiple calls, multiple agents, conference, and transfer.

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

## 2.2. Test Results

All test cases were executed and passed.

## 2.3. Support

Technical support on EMPOWER Suite can be obtained through the following:

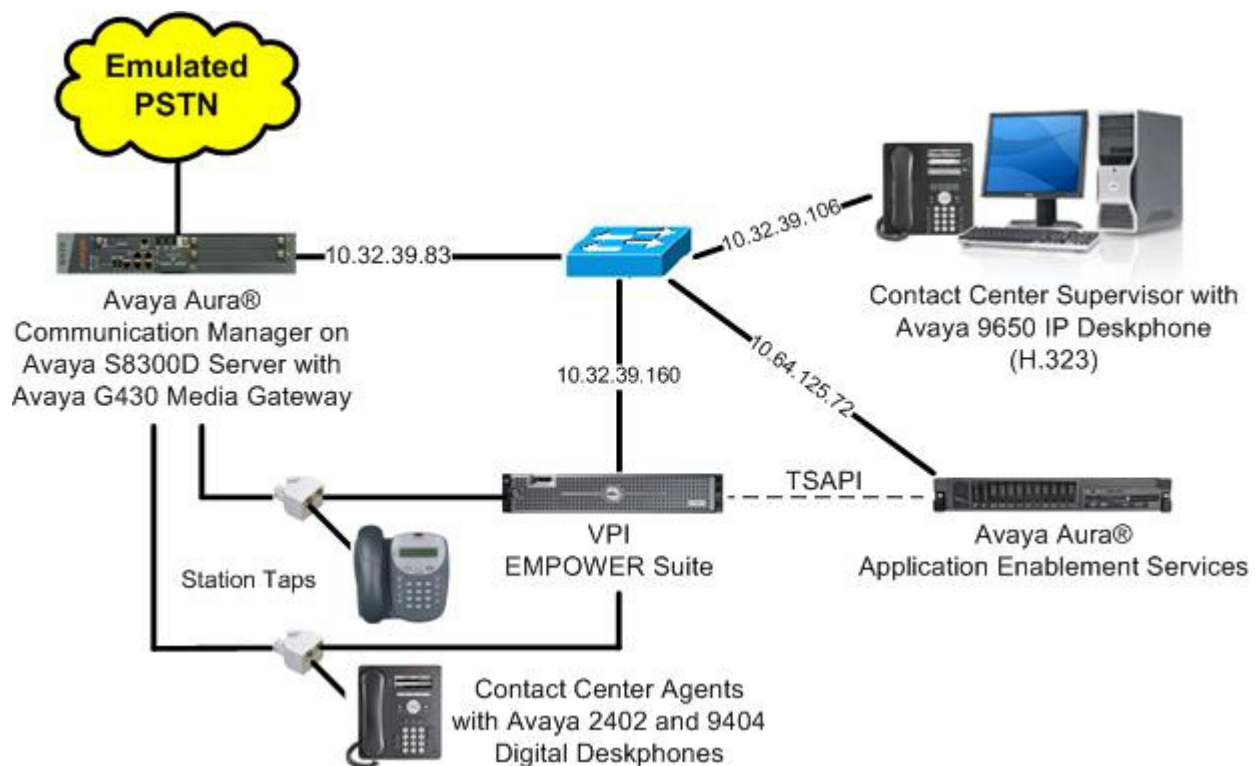
- **Phone:** (805) 389-5201
- **Email:** [support@vpi-corp.com](mailto:support@vpi-corp.com)
- **Web:** <http://www.vpi-corp.com/support.asp>

### 3. Reference Configuration

EMPOWER Suite can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration. In the compliance testing, the RTP streams for agent stations were captured using TDM splitters that replicated all conversations from the agent digital stations to the AudioCodes SmartTAP NGX PCIe board on EMPOWER Suite.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described. In the compliance testing, EMPOWER Suite monitored the contact center devices shown in the table below.

Device Type	Extension
VDN	48001, 48002
Skill Group	48101, 48102
Agent Station	45001, 45002



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8300D Server	6.3.2 (R016x.03.0.124.0-21053)
Avaya G430 Media Gateway <ul style="list-style-type: none"><li>MM712AP DCP</li></ul>	34.5.0 HW07 FW015
Avaya Aura® Application Enablement Services	6.3.1 (6.3.1.0.19-0)
Avaya 9650 IP Deskphone (H.323)	3.210A
Avaya 2402 Digital Deskphone	NA
Avaya 9404 Digital Deskphone	NA
VPI EMPOWER Suite on Windows Server 2008 <ul style="list-style-type: none"><li>AudioCodes SmartTAP NGX PCIe</li><li>Avaya TSAPI Windows Client (csta32.dll)</li></ul>	5.4 SP3 R2 Standard 05.07.00 Build 1038 6.1.0.396

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features

### 5.1. Verify License

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

```
display system-parameters customer-options                               Page 3 of 11
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? n           Authorization Codes? y
Analog Trunk Incoming Call ID? y           CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y    CAS Main? n
Answer Supervision by Call Classifier? y    Change COR by FAC? n
ARS? y      Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y      DCS (Basic)? y
ASAI Link Core Capabilities? n      DCS Call Coverage? y
ASAI Link Plus Capabilities? n      DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? y    Digital Loss Plan Modification? y
ATM WAN Spare Processor? n            DS1 MSP? y
ATMS? y      DS1 Echo Cancellation? 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: 40001
Type: ADJ-IP
                                                    COR: 1
Name: AES 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 20
      FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

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

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

```
change system-parameters features                                     Page 13 of 20
      FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
      Callr-info Display Timer (sec): 10
      Clear Callr-info: next-call
      Allow Ringer-off with Auto-Answer? n

      Reporting for PC Non-Predictive Calls? n

      Agent/Caller Disconnect Tones? n
      Interruptible Aux Notification Timer (sec): 3
      Zip Tone Burst for Callmaster Endpoints: double

ASAI
      Copy ASAI UII During Conference/Transfer? y
      Call Classification After Answer Supervision? y
      Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
      Send Connect Event to ASAI For Announcement Answer? n
```

## 6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Disable security database
- Restart services
- Obtain Tlink name
- Administer VPI user

### 6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are "Login" and "Reset" buttons. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2013 Avaya Inc. All Rights Reserved." is displayed.



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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining that the OAM Web provides tools for managing the AE Server and listing the administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be served by one administrator for all domains or a separate administrator for each domain.

Welcome: User  
Last login: Mon Oct 21 07:26:14 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Mon Oct 21 10:38:03 MDT 2013  
HA Status: Not Configured

Home | Help | Logout

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

**Welcome to OAM**

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status 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 all domains, or a separate administrator for each domain.

## 6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, including the need to use the following: WebLM Server Address, WebLM Server Access, and Reserved Licenses. It also notes that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following: Reserved Licenses.

Welcome: User  
Last login: Mon Oct 21 07:26:14 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Mon Oct 21 10:38:03 MDT 2013  
HA Status: Not Configured

Licensing | Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking

**Licensing**

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

- WebLM Server Address

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


- WebLM Server Access

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

- Reserved Licenses

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there is sufficient license for **TSAPI Simultaneous Users**, as shown below.


**Web License Manager (WebLM v6.3)**
Help | About | Change Password

WebLM Home  
Install license  
Licensed products  
APPL\_ENAB  
▼ Application\_Enablement  
View license capacity  
View peak usage  
Uninstall license  
Server properties  
Manage users  
Shortcuts  
Help for Installed Product

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

You are here: Licensed Products > Application\_Enablement > View License Capacity

License installed on: May 11, 2012 7:07:47 PM -04:00

**License File Host IDs:** 00-16-3E-48-ED-82

**Licensed Features**

10 Items
Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,, CCE_001, AdvancedUnrestricted, DMCUnrestricted; CSI_001, AdvancedUnrestricted, DMCUnrestricted; CSI_001, AdvancedUnrestricted, DMCUnrestricted; AVA_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

### 6.3. Administer TSAPI Link

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

The screenshot shows the Avaya Management Console interface. 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 "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" table with one link configured. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	6	Both

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 "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot, but "Communication Manager Interface" is also visible. The main content area contains a form with fields for "Link", "Switch Connection", "Switch CTI Link Number", "ASAI Link Version", and "Security". Each field has a dropdown menu. Below the form are "Apply Changes" and "Cancel Changes" buttons.

Link	Switch Connection	Switch CTI Link Number	ASAI Link Version	Security
2	S8300D	1	6	Unencrypted

## 6.4. Disable Security Database

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

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 | Control" as the active path, with links for "Home | Help | Logout". The left sidebar contains a tree view of system components, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

Welcome: User  
Last login: Mon Oct 21 07:26:14 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Mon Oct 21 10:38:03 MDT 2013  
HA Status: Not Configured

**Security | Security Database | Control** [Home](#) | [Help](#) | [Logout](#)

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ **Security**
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - ▶ Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ **Security Database**
    - **Control**

**SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services**


☐ Enable SDB for DMCC Service

☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

[Apply Changes](#)

## 6.5. Restart Services

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



**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Mon Oct 21 07:26:14 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Mon Oct 21 10:38:03 MDT 2013  
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ 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](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server



## 6.6. 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 EMPOWER Suite.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES\_125\_72”. Note the use of the switch connection “S8300D” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows a list of Tlinks with the first one, "AVAYA#S8300D#CSTA#AES\_125\_72", selected. A "Delete Tlink" button is visible below the list.

Welcome: User  
Last login: Mon Oct 21 07:26:14 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Mon Oct 21 10:38:03 MDT 2013  
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Account Management  
Audit  
Certificate Management  
Enterprise Directory  
Host AA  
PAM  
Security Database  
Control  
CTI Users  
Devices  
Device Groups  
Tlinks

Tlinks

Tlink Name

- ☒ AVAYA#S8300D#CSTA#AES\_125\_72
- ☐ AVAYA#S8800#CSTA#AES\_125\_72
- ☐ AVAYA#S8800#CSTA-S#AES\_125\_72

Delete Tlink

## 6.7. 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.

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 left navigation pane shows a tree structure with 'User Management' expanded, leading to 'User Admin' and then 'Add User'. The main content area contains the 'Add User' form, which includes fields for User Id, Common Name, Surname, User Password, Confirm Password, Admin Note, Avaya Role (set to None), Business Category, Car License, CM Home, Cms Home, CT User (set to Yes), Department Number, Display Name, Employee Number, Employee Type, and Enterprise Handle. A note indicates that fields marked with an asterisk are required.

Welcome: User  
Last login: Mon Oct 21 07:26:14 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Mon Oct 21 10:38:03 MDT 2013  
HA Status: Not Configured

User Management | User Admin | Add User Home | Help | Logout

**Add User**

Fields marked with \* can not be empty.

\* User Id vpi  
\* Common Name vpi  
\* Surname vpi  
\* User Password .....  
\* Confirm Password .....  
Admin Note  
Avaya Role None  
Business Category  
Car License  
CM Home  
Cms Home  
CT User Yes  
Department Number  
Display Name  
Employee Number  
Employee Type  
Enterprise Handle

## 7. Configure VPI EMPOWER Suite

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

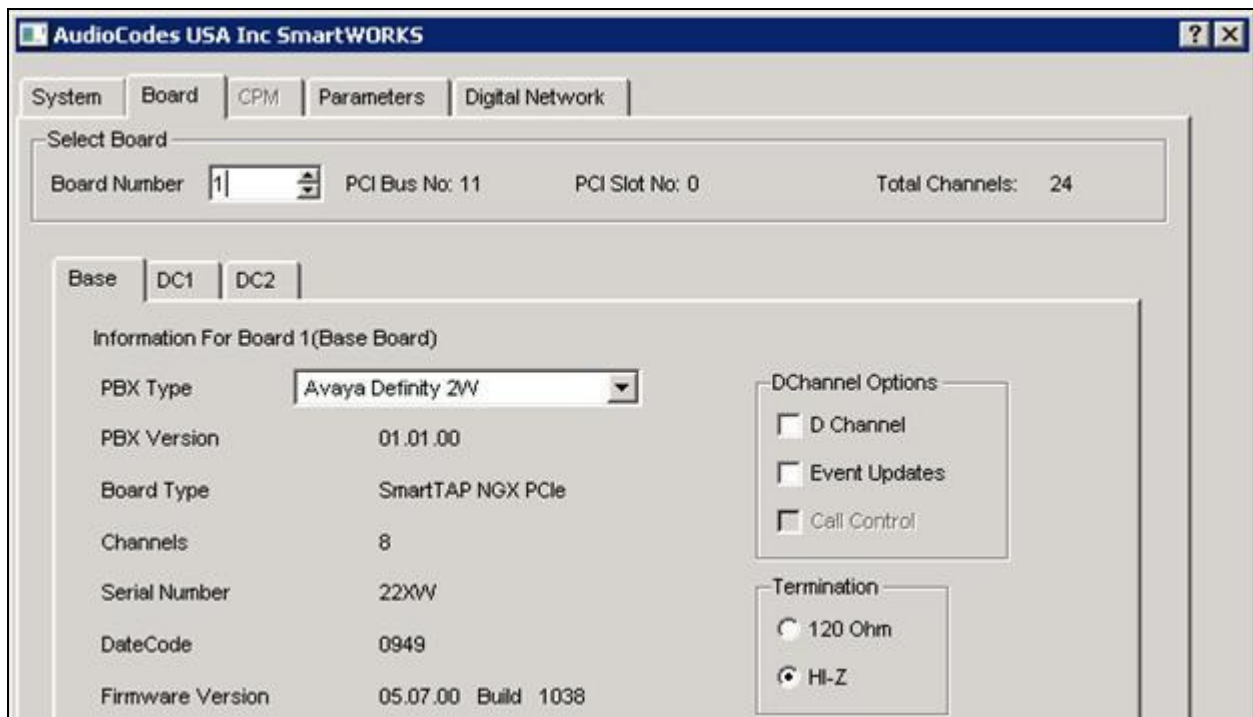
- Administer SmartControl
- Launch VPI Configuration
- Administer start/stop events
- Administer TSAPI
- Administer channels
- Launch Activ!Voice

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

### 7.1. Administer SmartControl

From the EMPOWER Suite server, select **Start → Control Panel**, and click on the **SmartControl** icon (not shown below).

The **AudioCodes USA Inc SmartWORKS** screen is displayed. Select the **Board** tab. For **PBX Type**, select the appropriate type to correspond to the digital card on Communication Manager, in this case “Avaya Definity 2W”. Reboot the EMPOWER Suite server.



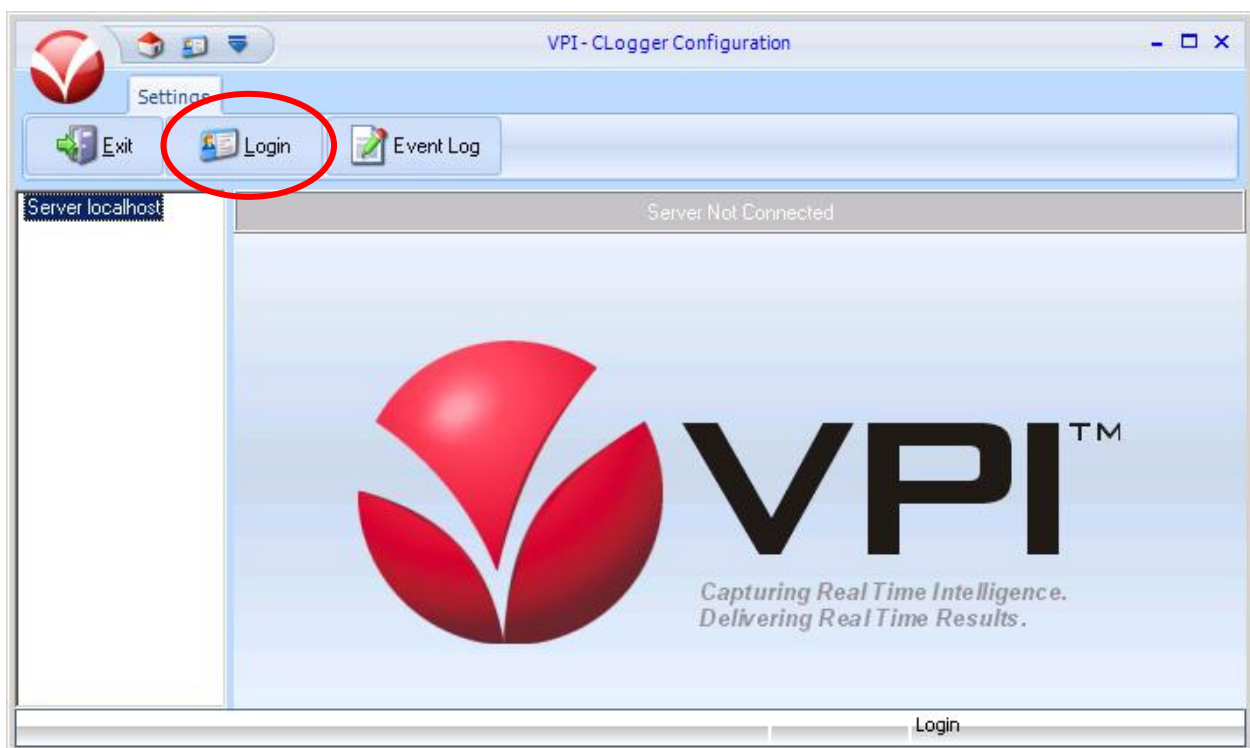


## 7.2. Launch VPI Configuration

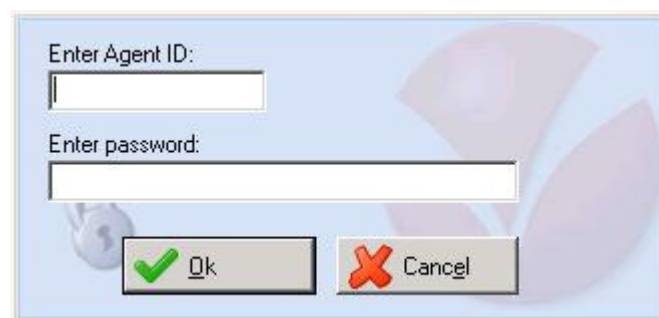
From the EMPOWER Suite server, double-click on the **VPI Configuration** icon shown below, which is created as part of the installation.



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



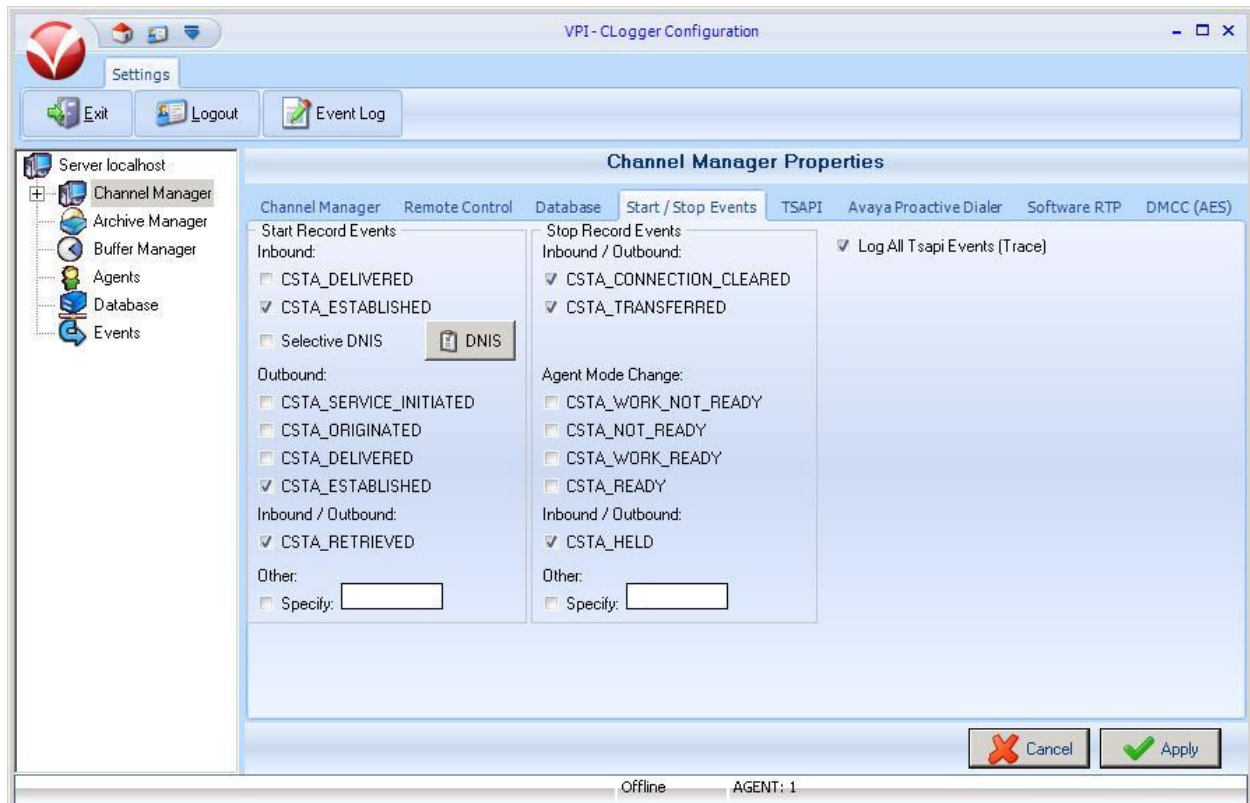
The screen below is displayed next. Log in using the appropriate credentials.



### 7.3. Administer Start/Stop Events

The **VPI - CLogger Configuration** screen is displayed. Select **Server localhost** → **Channel Manager** in the left pane, to display the **Channel Manager Properties** screen.

Select the **Start / Stop Events** tab in the right pane. Check the desired events to trigger the start and stop of call recordings. The screen below shows the selections used for the compliance testing. The **Log All Tsapi Events (Trace)** field was checked in the compliance testing for event verification purposes.



## 7.4. Administer TSAPI

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

- **Server 1 Machine:** The Tlink name from **Section 6.6**.
- **Application Username:** The VPI user credentials from **Section 6.7**.
- **Application Password:** The VPI user credentials from **Section 6.7**.
- **Switch Type:** “Avaya / Lucent”
- **ACD Groups:** The skill group extensions from **Section 3**.
- **VDNs:** The VDN extensions from **Section 3**.
- **Recording Line Type:** “Extension Side”

The screenshot shows the 'VPI-CLogger Configuration' window with the 'TSAPI' tab selected. The left sidebar lists various components: Server localhost, Channel Manager, Archive Manager, Buffer Manager, Agents, Database, and Events. The main area is titled 'Channel Manager Properties' and contains several sections:

- TSAPI Server Setup:**
  - Server 1 Machine: AVAYA#S8300D#CSTA
  - Server 2 Machine: (empty)
  - TSAPI Device: (empty)
  - Application Username: vpi
  - Application Password: (masked with asterisks)
  - ☐ Fail to VDX
  - ☐ Save All ANI
- General Options:**
  - ☒ Record All Agents
  - ☐ Lock Status Lights
  - ☐ Use Tsapi Time Stamp
- Additional Monitors:**
  - ACD Groups: 48101, 48102
  - Trunks: (empty)
  - VDNs: 48001, 48002
  - Extensions: (empty)
  - ☐ Disable recording of calls when SPLIT is empty
  - ☐ Disable recording of calls when DISTRIBUTING VDN is empty
- Switch Type:**
  - ☐ CSTA Compliant
  - ☒ Avaya / Lucent
  - ☐ Nortel Meridian
  - ☐ Aspect
  - ☐ NEC
- Service Observe Options:**
  - ☐ Monitor Agent Mode Change
  - Feature Code: (empty)
- Recording Line Type:**
  - ☒ Extension Side
  - ☐ Trunk Side

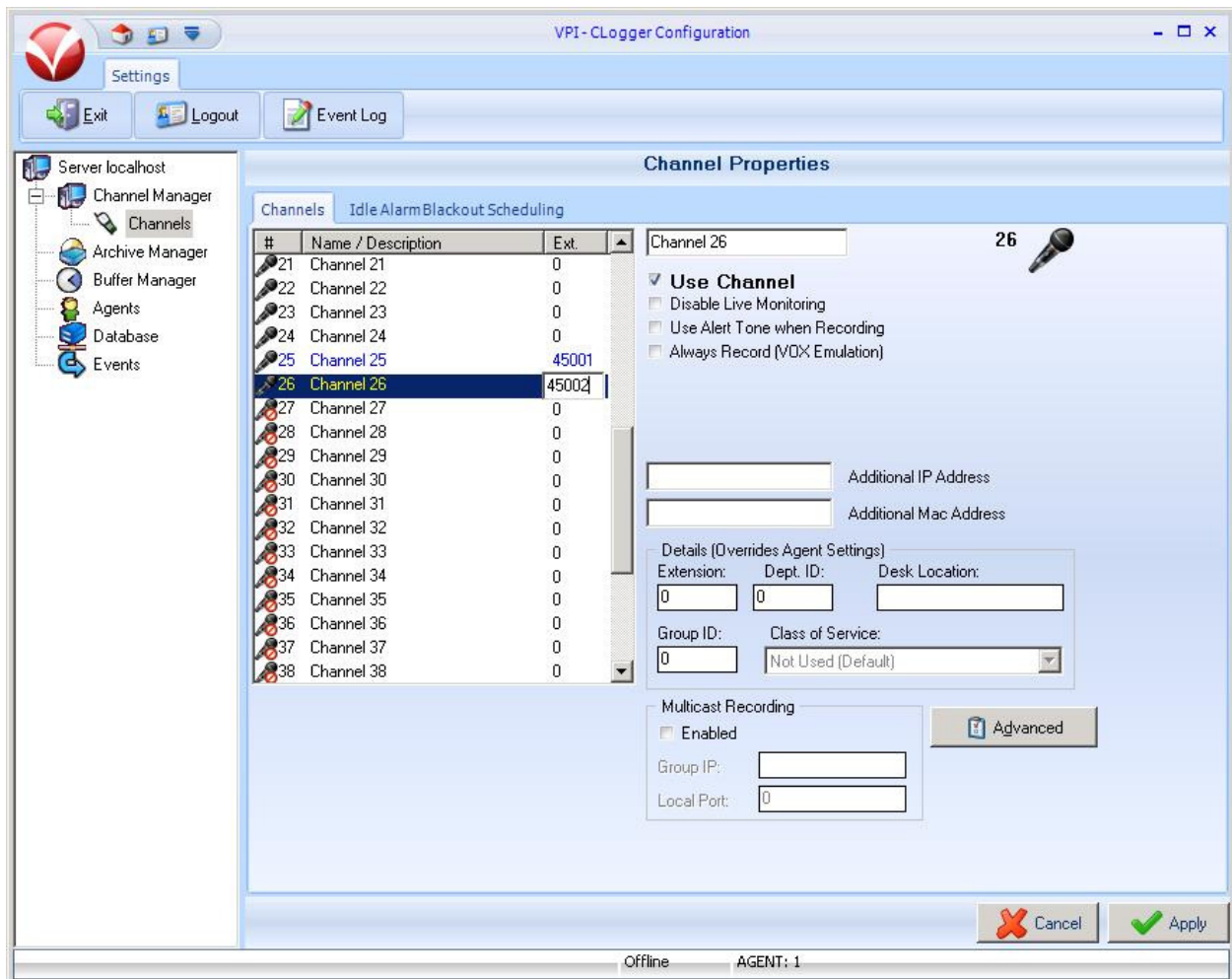
At the bottom right are 'Cancel' and 'Apply' buttons. The status bar at the bottom shows 'Offline' and 'AGENT: 1'.

## 7.5. Administer Channels

Select **Server localhost** → **Channel Manager** → **Channels** in the left pane, to display the **Channel Properties** screen. Select the first pertinent digital channel from the left portion of the **Channel Properties** screen, in this case **Channel 25**, and enter the following values for the specified fields in the right portion of the screen. Retain the default values for the remaining fields.

- **Use Channel:** Check this field.
- **Extension:** The first station extension from **Section 3**.

Repeat this section to administer a channel for each agent digital station to be monitored from **Section 3**. In the compliance testing, two channels **25** and **26** were configured as shown below.

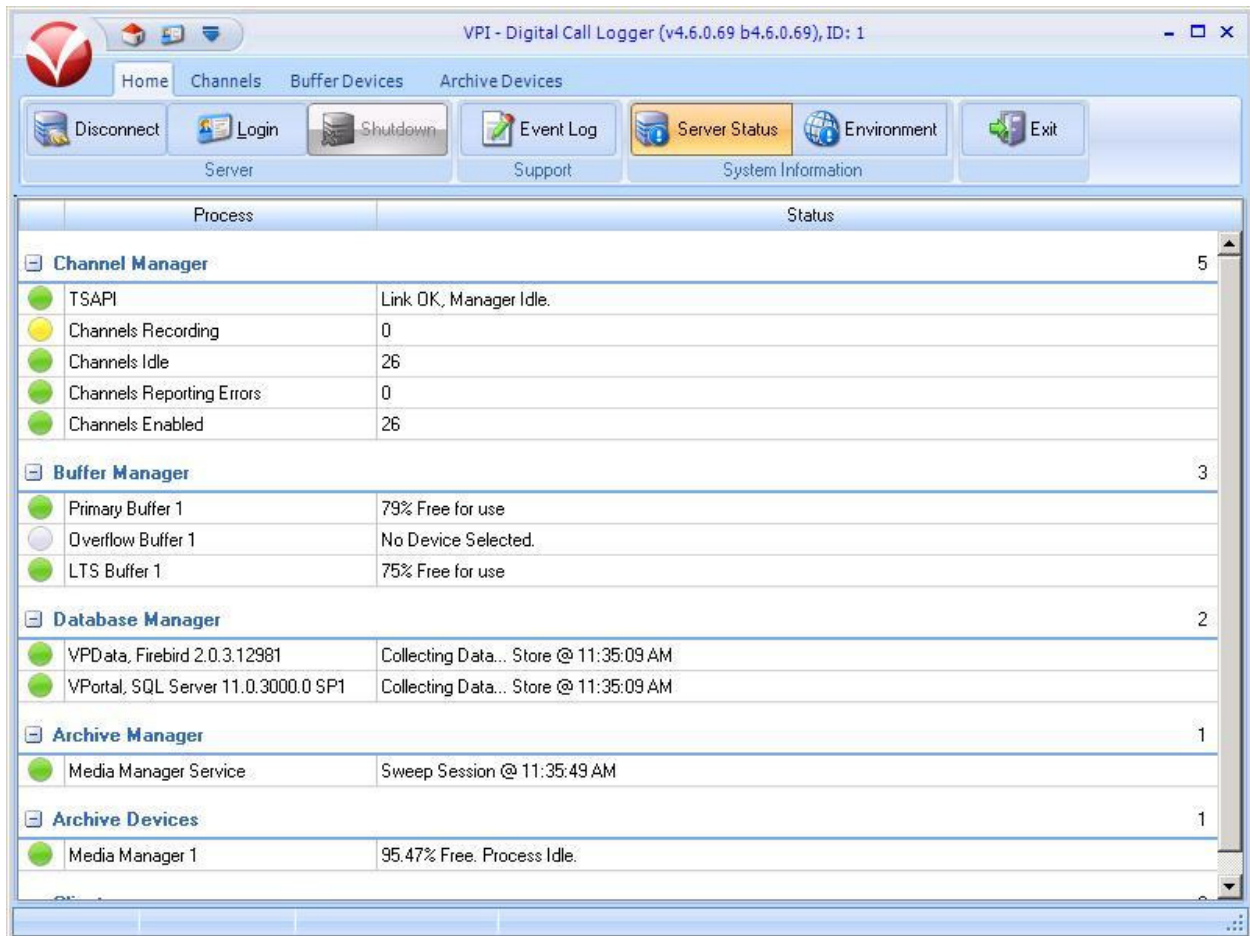


## 7.6. Launch Activ!Voice

From the EMPOWER Suite 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. 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.





## 8. Verification Steps

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

### 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	6	no	aes_125_72	established	43	21

### 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**, and that the **Associations** column reflects the total number of monitored contact center devices from **Section 3**.



**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Oct 22 12:06:09 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Tue Oct 22 12:36:35 MDT 2013  
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
ⓘ	1	S8800	2	Talking	Thu Oct 17 07:55:05 2013	Online	16	0	15	15	30
ⓘ	2	S8300D	1	Talking	Tue Oct 22 07:32:52 2013	Online	16	6	30	52	30

Online Offline

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

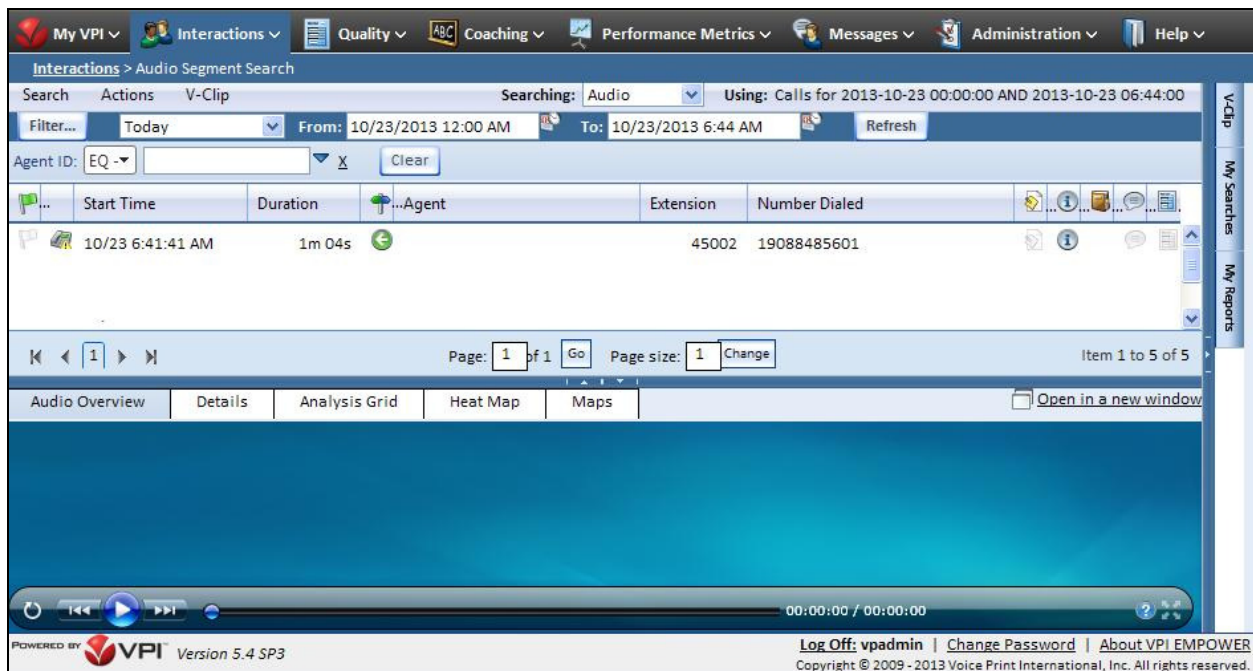
TSAPI Service Status TLink Status User Status

### 8.3. Verify VPI EMPOWER Suite

Log an agent in to the skill group to handle and complete an ACD call. Access the EMPOWER Suite 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 EMPOWER Suite server. Log in using the appropriate credentials.



The screen below is displayed next, with a list of the call recordings for the current day. 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.

The screenshot displays the VPI Interactions Audio Segment Search interface. The top navigation bar includes tabs for My VPI, Interactions, Quality, Coaching, Performance Metrics, Messages, Administration, and Help. The main header shows 'Interactions > Audio Segment Search'. Below this, a search bar is set to 'Searching: Audio' with a date range filter for '10/23/2013 12:00 AM' to '10/23/2013 6:44 AM'. A table lists search results with columns for Start Time, Duration, Agent, Extension, and Number Dialed. The first entry is for '10/23 6:41:41 AM' with a duration of '1m 04s' and extension '45002'. Below the table, a playback control interface is visible, showing a timeline from 6:41:41 AM to 6:42:45 AM. The playback controls include a play button, a progress bar, and a volume slider. The bottom of the screen shows the VPI logo and version information: 'Version 5.4 SP3'.

Start Time	Duration	Agent	Extension	Number Dialed
10/23 6:41:41 AM	1m 04s		45002	19088485601

Page: 1 of 1 Go Page size: 1 Change Item 1 to 5 of 5

Audio Overview Details Analysis Grid Heat Map Maps Open in a new window

10/23/2013 6:41:41 AM Standard Settings

6:41:41 AM 6:41:57 AM 6:42:13 AM 6:42:29 AM 6:42:45 AM

[Not Specified]

00:11 / 01:04

POWERED BY VPI Version 5.4 SP3

Log Off: vpadmin | Change Password | About VPI EMPOWER  
Copyright © 2009 - 2013 Voice Print International, Inc. All rights reserved.



## 9. Conclusion

These Application Notes describe the configuration steps required for VPI EMPOWER Suite to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3. All feature and serviceability test cases were completed.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9, Release 6.3, October 2013, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 2, October 2013, available at <http://support.avaya.com>.
3. *VPI EMPOWER Avaya Channel Manager Guide*, September 2013, available on the VPI EMPOWER Suite server as part of installation.

---

**©2013 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).