



Avaya Solution & Interoperability Test Lab

Application Notes for VPI EMPOWER Suite with Avaya Proactive Contact 5.1 with PG230 and Avaya Aura® Application Enablement Services 6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Voice Print International EMPOWER Suite to interoperate with Avaya Proactive Contact 5.1 with PG230 and Avaya Aura® Application Enablement Services 6.3. 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 Event Services interface from Avaya Proactive Contact and the Telephony Services Application Programmer Interface from Avaya Aura® Application Enablement Services to obtain information on calls and agent states, and used the Multiple Registration feature from the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture the media associated with the monitored 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 Proactive Contact 5.1 with PG230 and Avaya Aura® Application Enablement Services 6.3. 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 Event Services interface from Avaya Proactive Contact and the Telephony Services Application Programmer Interface (TSAPI) from Avaya Aura® Application Enablement Services to obtain information on calls and agent states, and used the Multiple Registration feature from the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with the monitored agent stations for call recording.

The Event Services and TSAPI interfaces are used by VPI EMPOWER Suite to monitor the calls and agent states, and the DMCC interface is used by VPI EMPOWER Suite to register a virtual IP softphone against each monitored agent station to pick up the media for call recording. When there is an active call at the monitored agent station, VPI EMPOWER Suite is informed of the call via event reports from the Event Services and/or TSAPI interfaces, and starts the call recording by using the media from the associated virtual IP softphone. The Event Services and/or TSAPI event reports are also used to determine when to stop the call recordings.

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

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the EMPOWER Suite recording application, the application automatically requests monitoring on the agent stations to be recorded using TSAPI, registers the associated virtual IP softphones using DMCC, and obtains current status from Proactive Contact using Event Services.

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

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

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

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

- Handling of Event Services agent states and call events.
- Handling of TSAPI messages in the areas of event notification and value queries.
- Use of DMCC registration services to register and un-register the 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, agent drop, customer drop, hold, reconnect, simultaneous calls, transfer, unsupervised forward work, agent blending, and call blending scenarios.

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. The following were the observations on EMPOWER Suite from the compliance testing.

- Recordings for supervised forward work and conference with supervisor scenarios are not supported in this release of EMPOWER Suite.
- Connections to announcements were included as separate recording entries, and the initial announcement recording entry does not end until the agent receives a call.
- Some recordings include up to ~7 seconds of silence after the agent release the line.

2.3. Support

Technical support on EMPOWER Suite 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

EMPOWER Suite can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration.

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

In the compliance testing, EMPOWER Suite monitored two agent stations with extensions “65001” and “65002” on Communication Manager.

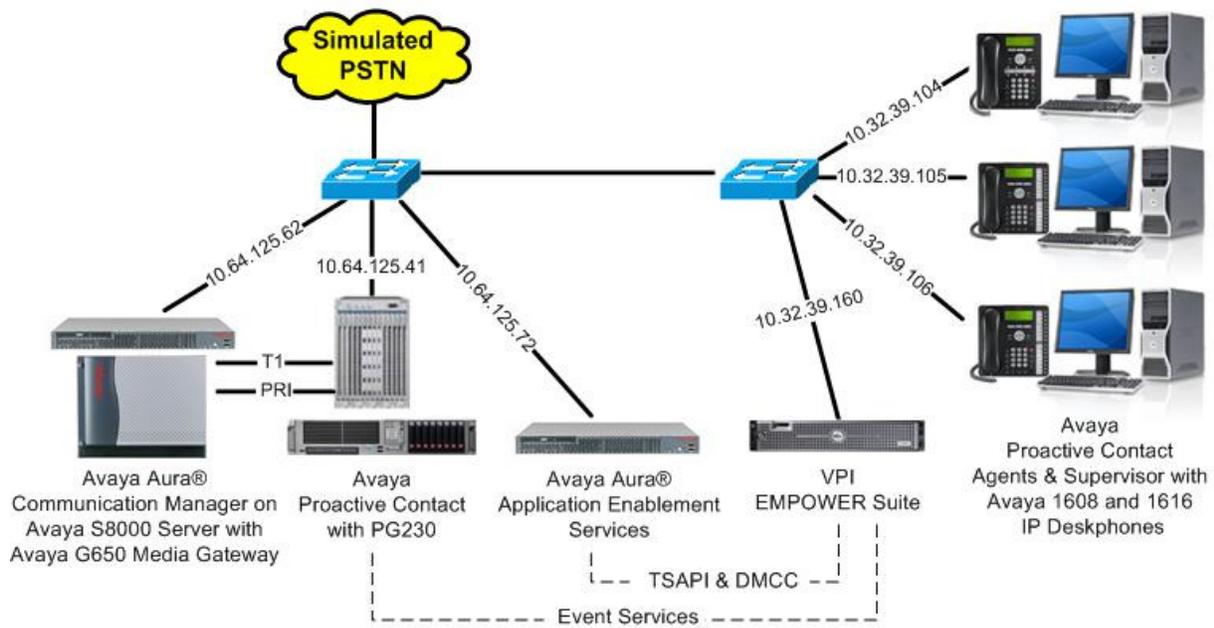


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.2 (R016x.03.0.124.0-21053)
Avaya Aura® Application Enablement Services	6.3.1 (6.3.1.0.19-0)
Avaya Proactive Contact with PG230	5.1
Avaya Proactive Contact Agent	5.1
Avaya Proactive Contact Supervisor	5.1
Avaya 1608 IP Deskphone (H.323)	1.3.4
Avaya 1616 IP Deskphone (H.323)	1.3.4
VPI EMPOWER Suite on Windows Server 2008 <ul style="list-style-type: none">• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC .NET (ServiceProvider.dll)	5.4 SP3 R2 Standard 6.1.0.396 6.1.1.45

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify License

Log in to the System Access Terminal 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? n                                     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? n                             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 2                                                       Page 1 of 3
                                CTI LINK
CTI Link: 1
Extension: 60100
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: 27
```

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
```

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 virtual IP softphone to be registered against the station. Note the value of **Security Code**, which will be used later to configure EMPOWER Suite.

```

change station 65001                                     Page 1 of 4
                                                         STATION
Extension: 65001                                         Lock Messages? n          BCC: 0
Type: 1608                                               Security Code: 65001      TN: 1
Port: S00006                                             Coverage Path 1: 1       COR: 1
Name: VPI Station #1                                    Coverage Path 2:         COS: 1
                                                         Hunt-to Station:         Tests? y

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:
Survivable COR: internal                                   Media Complex Ext:
Survivable Trunk Dest? y                                  IP SoftPhone? 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 agent stations were administered as shown below.

```

list station 65001 count 2
                                                         STATIONS
Ext/      Port/   Name/      Room/      Cv1/  COR/   Cable/
 Hunt-to  Type   Surv GK NN  Move      Data Ext  Cv2  COS TN Jack
-----
65001    S00006 VPI Station #1  no          1      1      1
          1608
65002    S00049 VPI Station #2  no          1      1      1
          1616

```

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
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Obtain Tlink name
- Administer VPI user
- Enable ports

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 reads "Application Enablement Services Management Console". A red horizontal bar spans the width of the page, with the word "Help" in the top right corner. In the center, there is a login form with the heading "Please login here:". Below this heading are two input fields: "Username" and "Password". Underneath the password field are two buttons: "Login" and "Reset". 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 left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays user information: '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', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. The left sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Welcome to OAM' and contains the following text: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. A bulleted list follows: '• 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'. A final paragraph states: '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' page selected. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays user information: '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', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. The left sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing (expanded), Maintenance, and Networking. Under 'Licensing', the sub-items are: WebLM Server Address, WebLM Server Access (highlighted in blue), and Reserved Licenses. The main content area is titled 'Licensing' and contains the following text: 'If you are setting up and maintaining the WebLM, you need to use the following:'. A bulleted list follows: '• WebLM Server Address'. Below this, it says: 'If you are importing, setting up and maintaining the license, you need to use the following:'. A bulleted list follows: '• WebLM Server Access'. Finally, it says: 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:'. A bulleted list follows: '• 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 are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for device monitoring, and the DMCC license is used for the virtual IP softphones.

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

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

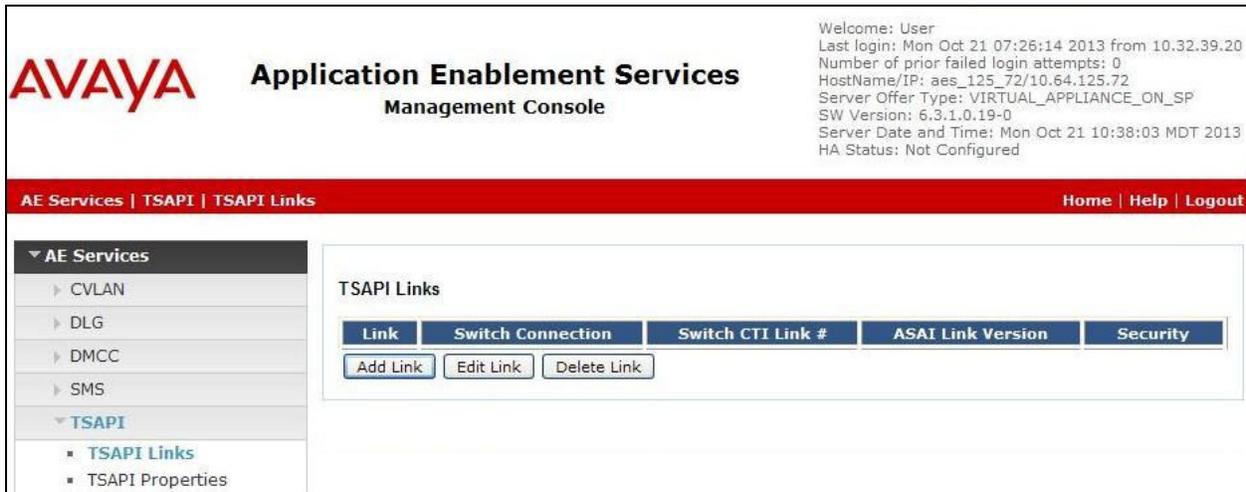
Licensed Features

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_1 LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestricted 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_AES_UNIFIED_CC_DESKTOP,,, CCE (AdvancedUnrestricted, DMCUnrestricted; CSI, AdvancedUnrestricted, DMCUnrestricted; CSI, AdvancedUnrestricted, DMCUnrestricted; AVA 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

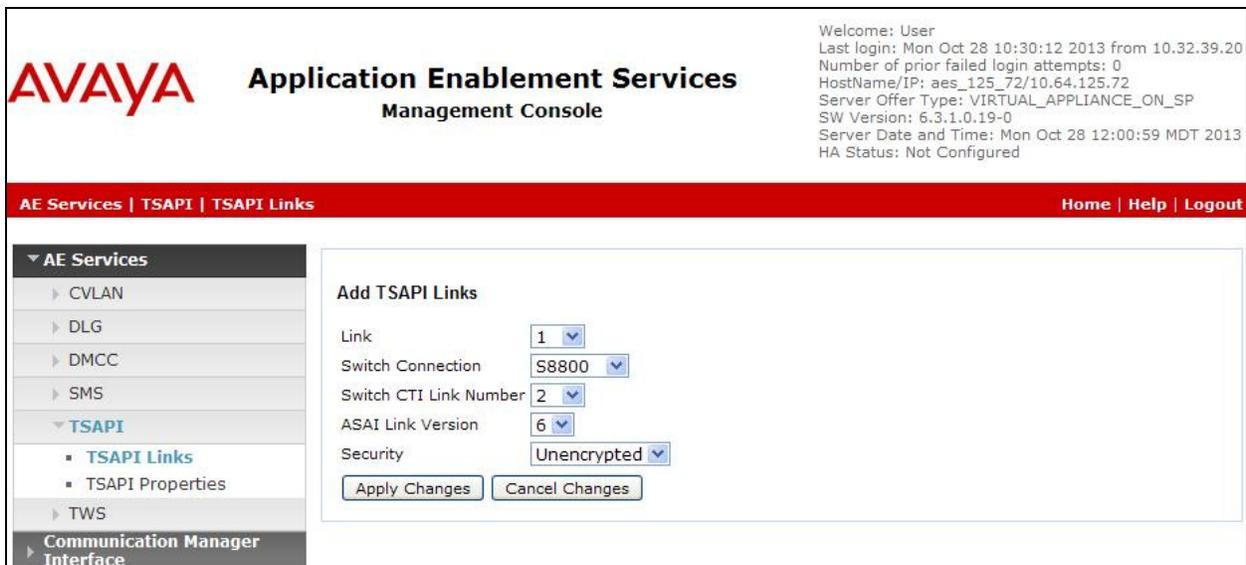
6.3. Administer TSAPI Link

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 **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.



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 top right corner displays user information: "Welcome: User", "Last login: Mon Oct 28 10:30:12 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 28 12:04:20 MDT 2013", and "HA Status: Not Configured". The main navigation bar includes "Communication Manager Interface | Switch Connections" and "Home | Help | Logout". The left sidebar shows a tree view with "Communication Manager Interface" expanded to "Switch Connections". The main content area is titled "Switch Connections" and contains a table with the following data:

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8800	No	30	1

Below the table are several buttons: "Add Connection", "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", "Delete Connection", and "Survivability Hierarchy".

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 the H.323 gatekeeper, in this case “10.64.125.32” as shown below. Click **Add Name or IP**.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Edit H.323 Gatekeeper - S8800" screen. The top right corner displays user information: "Welcome: User", "Last login: Mon Oct 28 10:30:12 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 28 12:04:35 MDT 2013", and "HA Status: Not Configured". The main navigation bar includes "Communication Manager Interface | Switch Connections" and "Home | Help | Logout". The left sidebar shows a tree view with "Communication Manager Interface" expanded to "Switch Connections". The main content area is titled "Edit H.323 Gatekeeper - S8800" and contains a form with the following fields and buttons:

10.64.125.32

Name or IP Address

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title "Application Enablement Services Management Console". The top right shows system information: "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", and "HA Status: Not Configured". A red navigation bar contains "Security | Security Database | Control" and "Home | Help | Logout". The left sidebar lists various services, with "Security Database" expanded to show "Control". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", along with an "Apply Changes" button.

6.6. Restart Services

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays user information: "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", and "HA Status: Not Configured". The main navigation bar includes "Maintenance | Service Controller" and "Home | Help | Logout". The left sidebar lists various service categories, with "Maintenance" expanded to show "Service Controller" selected. The main content area displays a table of services under the heading "Service Controller".

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" 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](#)

Buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, Restart Web Server

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 EMPOWER Suite.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES_125_72”. Note the use of the switch connection “S8800” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title "Application Enablement Services Management Console". The top right shows system information: "Welcome: User", "Last login: Mon Oct 28 10:30:12 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 28 12:05:15 MDT 2013", and "HA Status: Not Configured".

The main navigation bar includes "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar shows 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#S8800#CSTA#AES_125_72" and a "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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: 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. The breadcrumb navigation is User Management | User Admin | Add User. The left sidebar menu includes AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Add User (selected), Change User Password, List All Users, Modify Default Users, Search Users, Utilities, and Help. The main content area is titled 'Add User' and contains a form with the following fields: * User Id (vpi), * Common Name (vpi), * Surname (vpi), * User Password (masked with dots), * Confirm Password (masked with dots), Admin Note (empty), Avaya Role (None), Business Category (empty), Car License (empty), CM Home (empty), Css Home (empty), CT User (Yes), Department Number (empty), Display Name (empty), Employee Number (empty), Employee Type (empty), and Enterprise Handle (empty). A note above the form states 'Fields marked with * can not be empty.'

6.9. Enable Ports

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. Retain the default values in the remaining fields.



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

Networking | Ports
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ 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 Avaya Proactive Contact

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

- Obtain host name
- Obtain permission files

7.1. Obtain Host Name

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

In the compliance testing, the host name of the Proactive Contact server is “lzpds4b”, as shown below.

```
$ uname -a  
Linux lzpds4b 2.6.18-308.16.1.e15PAE #1 SMP Tue Sep 18 07:29:37 EDT 2012 i686 athlon  
i386 GNU/Linux
```

7.2. Obtain Permission Files

Use a tool such as WinSCP, to copy the following permission files from the Proactive Contact server, which will be used later to configure EMPOWER Suite.

- /opt/avaya/pds/openssl/certificate/corbaServer_cert.pem
- /opt/avaya/pds/openssl/cacertificate/ProactiveContactCA.pem
- /opt/avaya/pds/openssl/private/corbaServer_key.pem

8. Configure VPI EMPOWER Suite

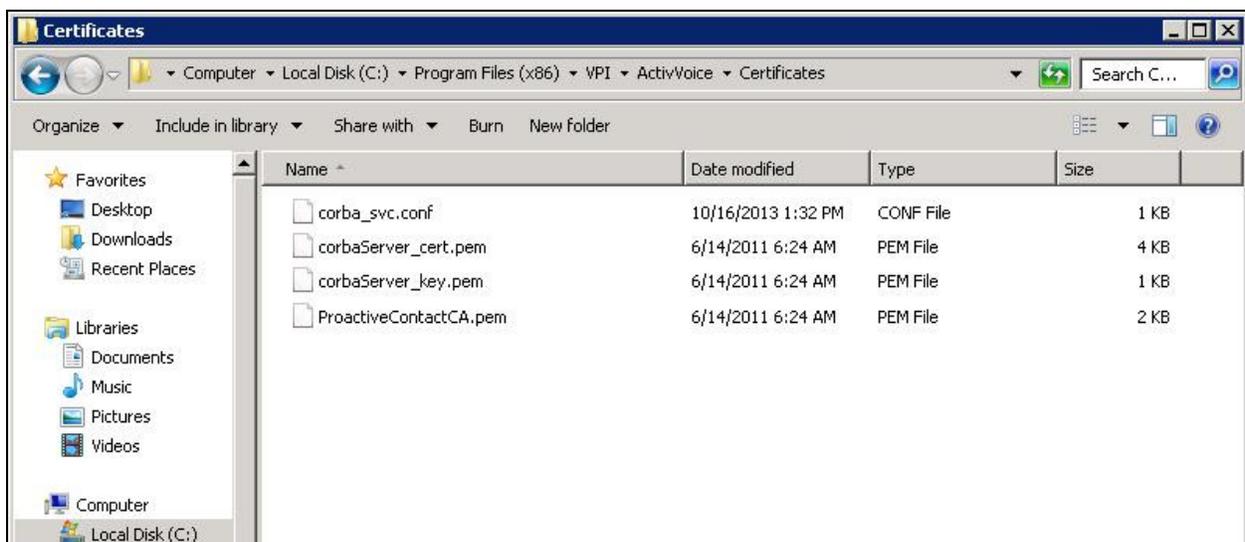
This section provides the procedures for configuring EMPOWER Suite. The procedures include the following areas:

- Copy permission files
- Launch VPI Configuration
- Administer start/stop events
- Administer TSAPI
- Administer proactive dialer
- Administer software RTP
- Administer DMCC
- 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.

8.1. Copy Permission Files

From the EMPOWER Suite server, copy the three permission files from **Section 7.2** to the applicable certificates directory, in this case **C:\Program Files (x86)\VPI\ActivVoice\Certificates**, as shown below. These files will be used for Event Services connection to Proactive Contact.

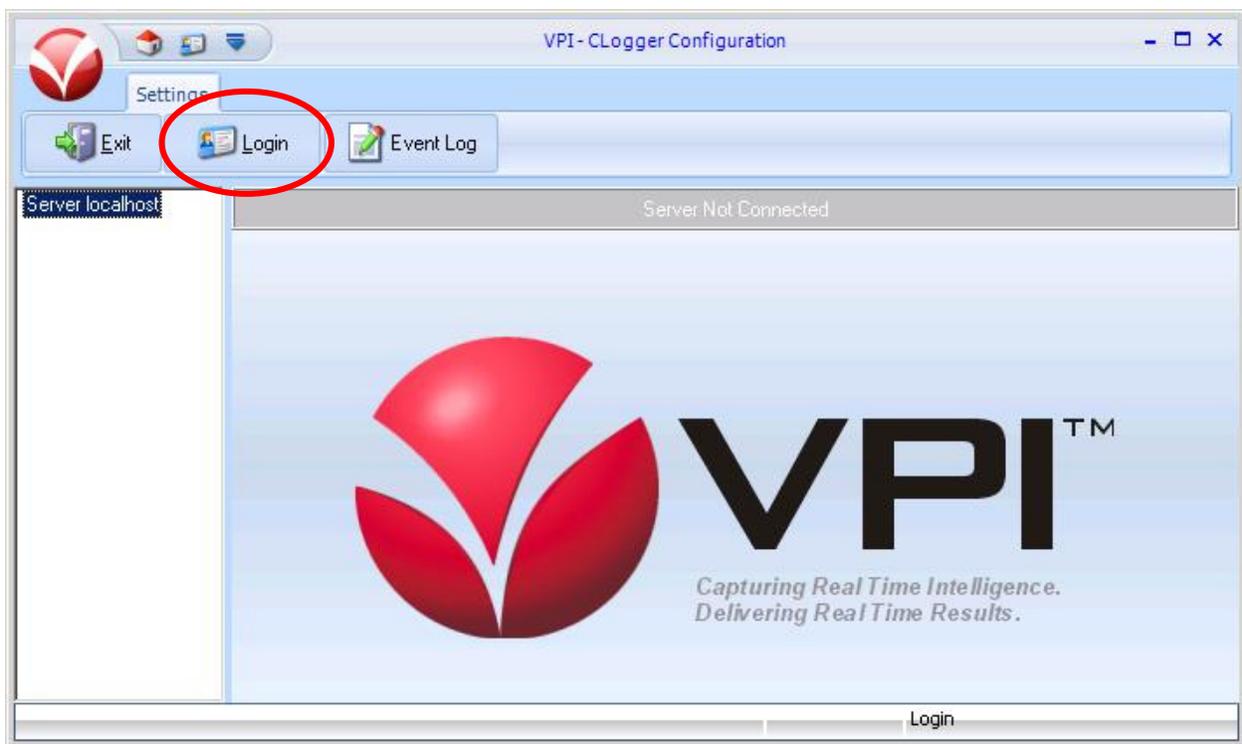


8.2. Launch VPI Configuration

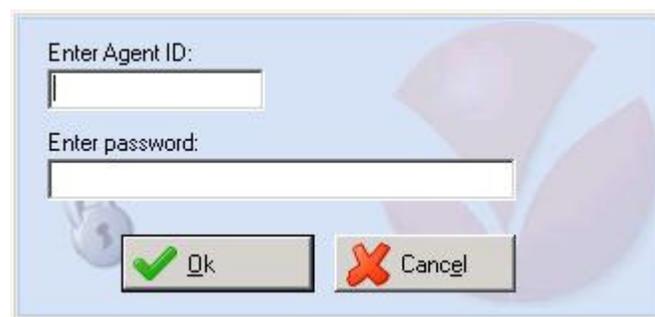
From the EMPOWER Suite server, double-click on the **VPI Configuration** icon shown below, which is created as part of the installation.



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



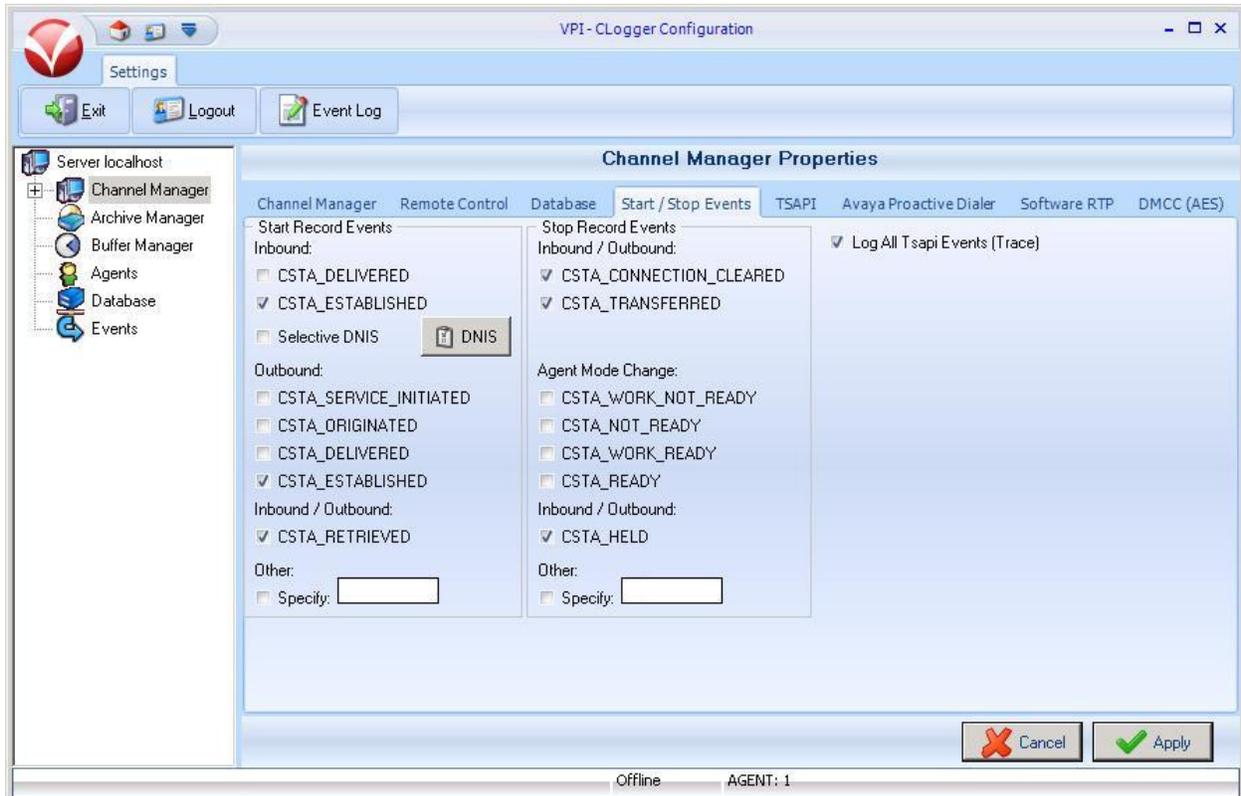
The screen below is displayed next. Log in using the appropriate credentials.



8.3. 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.

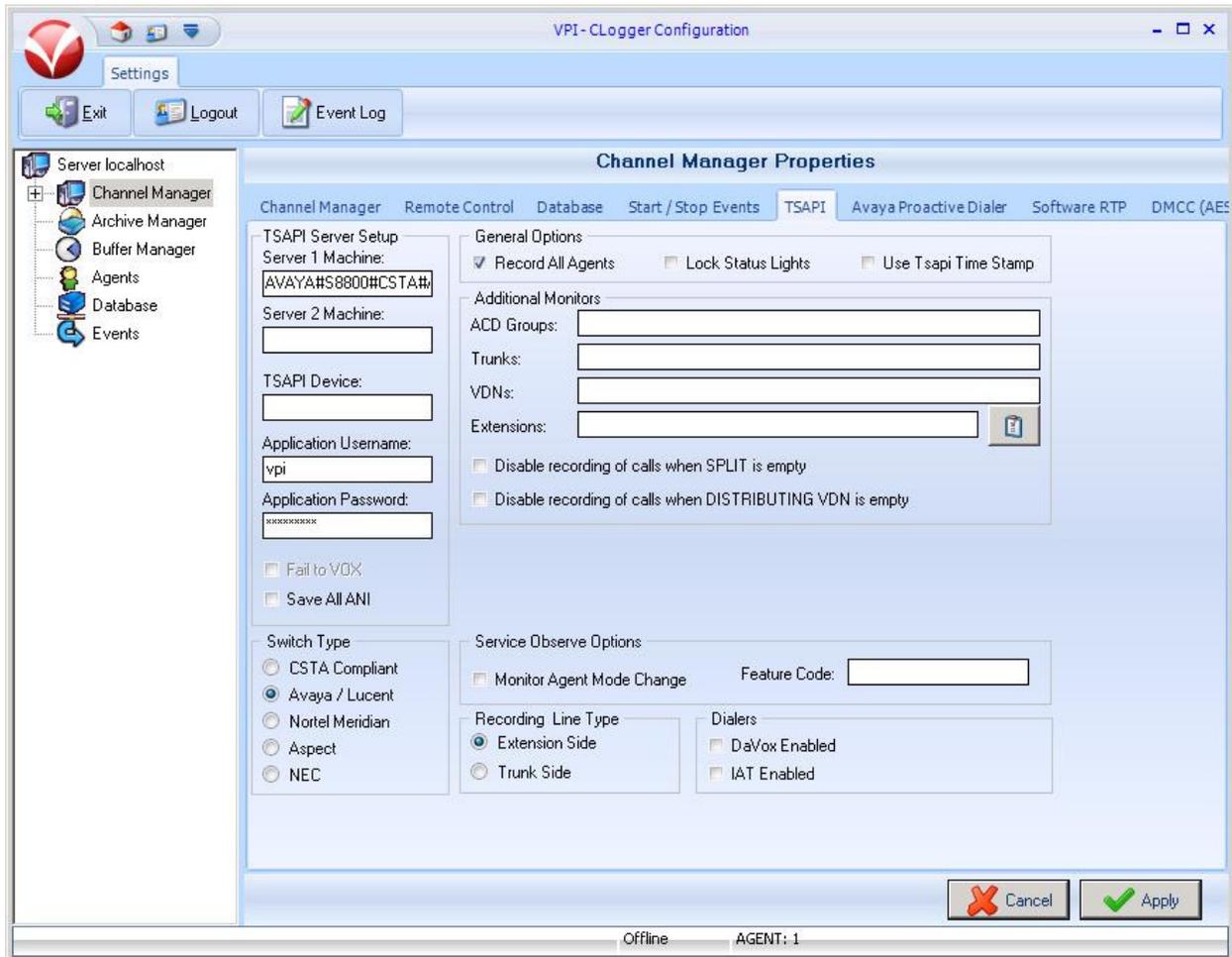
Select the **Start / Stop Events** tab in the right pane. Check the desired events to trigger the start and stop of call recordings. The screen below shows the selections used for the compliance testing. The **Log All Tsapi Events (Trace)** field was checked in the compliance testing for event verification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



8.4. 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.

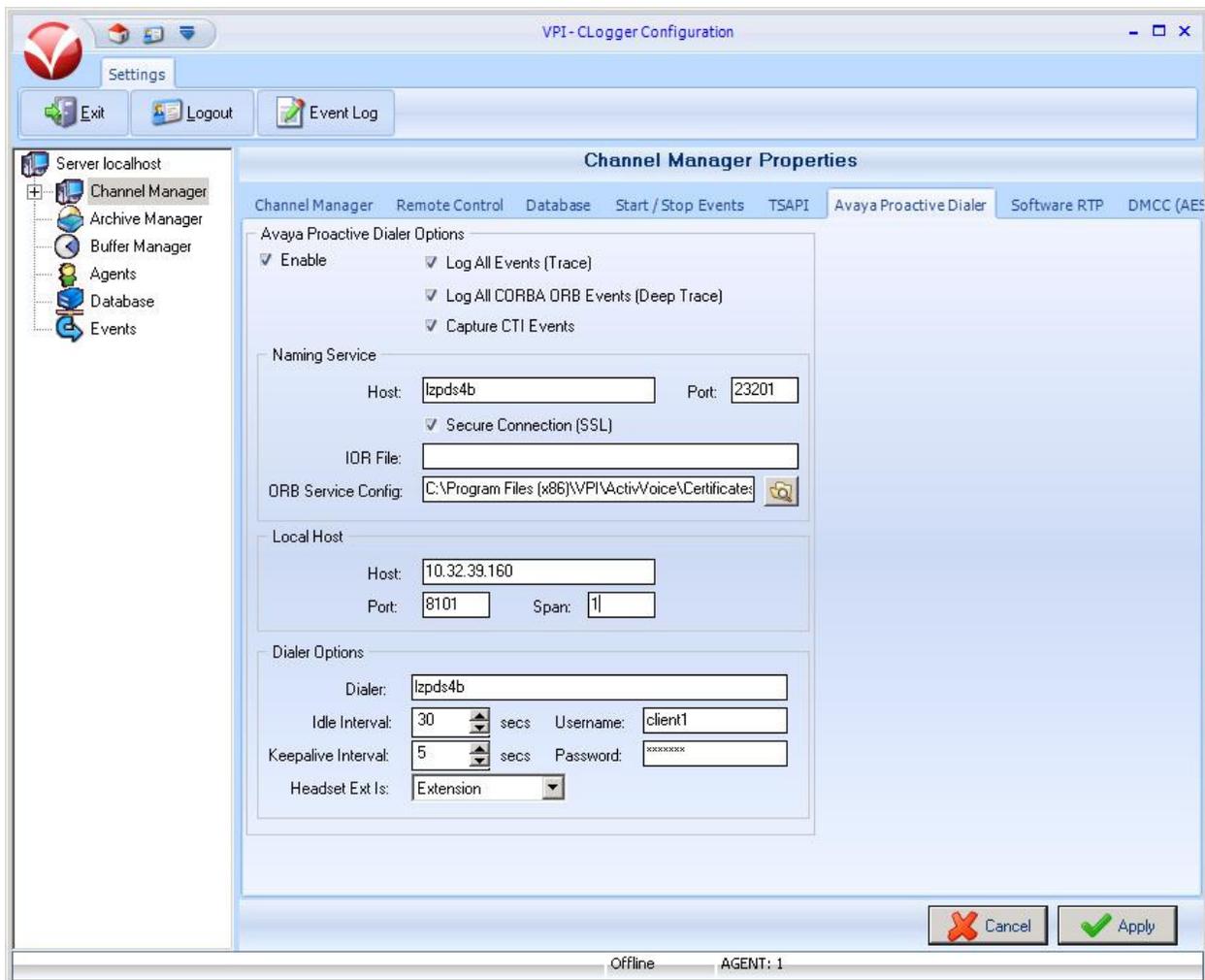
- **Server 1 Machine:** The Tlink name from **Section 6.7**.
- **Application Username:** The VPI user credentials from **Section 6.8**.
- **Application Password:** The VPI user credentials from **Section 6.8**.
- **Switch Type:** “Avaya / Lucent”
- **Recording Line Type:** “Extension Side”



8.5. Administer Proactive Dialer

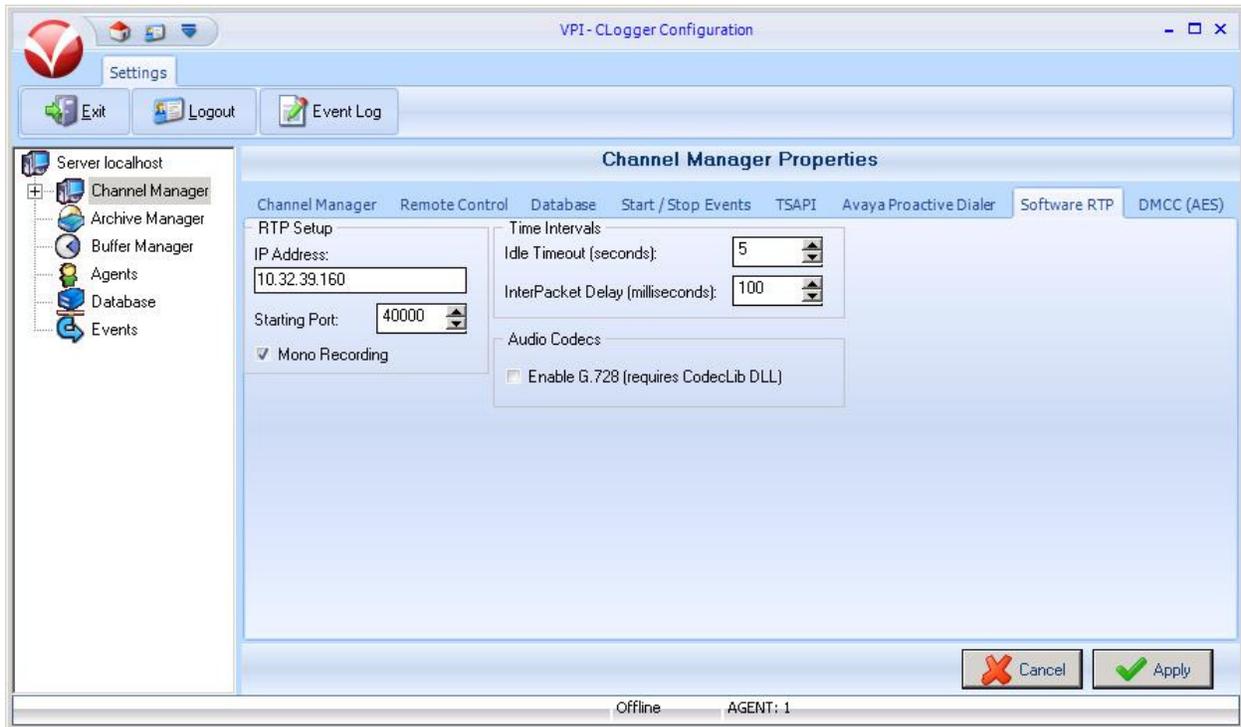
Select the **Avaya Proactive Dialer** tab in the right pane. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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



8.6. Administer Software RTP

Select the **Software RTP** tab in the right pane. For **IP Address**, enter the IP address of the EMPOWER Suite server, in this case “10.32.39.160”. Retain the default values in the remaining fields.



8.7. 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.

- **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-CLogger Configuration' window with the 'DMCC (AES)' tab selected. The 'Channel Manager Properties' section is active, and the 'General Options' group is expanded. The 'Enable' checkbox is checked. The 'Server IP Address' is set to 10.64.125.72, and the 'Switch (CLAN) Address' is set to 10.64.125.32. The 'Server Port' is 4721. The 'Session User' is 'vpi' and the 'Session Password' is masked with asterisks. The 'Device Instance' field is empty. The 'TLS (SSL) Options' section is also visible, with 'Enable' unchecked, 'Version' set to 'SSL v2', and 'Allow Older Versions' unchecked. Other fields like 'Certificate File', 'CA File', 'Key File', 'Packet Timeout', 'Connect Timeout', and 'Verify Depth' are also present.

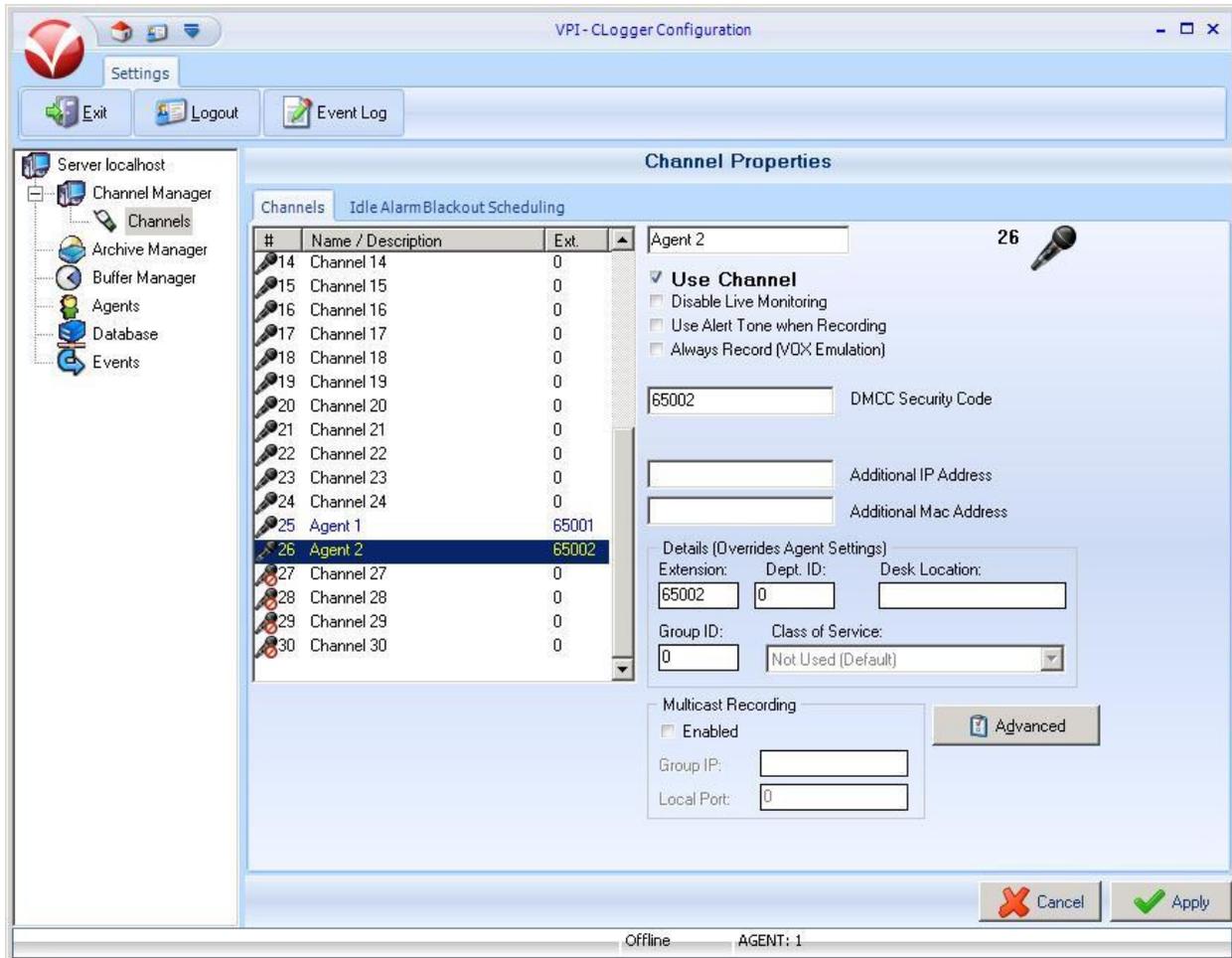
Field	Value
Enable	<input checked="" type="checkbox"/>
Server IP Address	10.64.125.72
Switch (CLAN) Address	10.64.125.32
Server Port	4721
Session User	vpi
Session Password	*****
Device Instance	
Global Ext Password	
Enable (TLS)	<input type="checkbox"/>
Version (TLS)	SSL v2
Allow Older Versions (TLS)	<input type="checkbox"/>
Certificate File	
CA File	
Key File	
Client CA File	
CA Path	
Key Phrase	
Packet Timeout	30
Connect Timeout	30
Verify Peer	<input type="checkbox"/>
Verify Depth	30

8.8. Administer Channels

Select **Server localhost** → **Channel Manager** → **Channels** in the left pane, to display the **Channel Properties** screen. Select the first pertinent VoIP 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.

- **Name / Description:** A desired name for the station to be monitored.
- **Use Channel:** Check this field.
- **DMCC Security Code:** The first agent station security code from **Section 5.4**.
- **Extension:** The first 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**. In the compliance testing, two channels **25-26** were configured as shown below.



8.9. 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.

The screenshot shows the VPI - Digital Call Logger application window. The title bar reads "VPI - Digital Call Logger (v4.6.0.69 b4.6.0.69), ID: 1". The interface includes a navigation menu with "Home", "Channels", "Buffer Devices", and "Archive Devices". Below this is a toolbar with buttons for "Disconnect", "Login", "Shutdown", "Event Log", "Server Status", "Environment", and "Exit". The main area is a table with columns for "Process" and "Status".

Process	Status
Channel Manager 5	
Avaya Multiple Registration	Link OK, Manager Idle.
Channels Recording	0
Channels Idle	26
Channels Reporting Errors	0
Channels Enabled	26
Buffer Manager 3	
Primary Buffer 1	79% Free for use
Overflow Buffer 1	No Device Selected.
LTS Buffer 1	75% Free for use
Database Manager 2	
VPData, Firebird 2.0.3.12981	Collecting Data... Store @ 9:31:26 AM
VPortal, SQL Server 11.0.3000.0 SP1	Collecting Data... Store @ 9:31:26 AM
Archive Manager 1	
Media Manager Service	Archive Session @ 9:31:36 AM
Archive Devices 1	
Media Manager 1	95.44% Free. Process Idle.

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
2	6	no	aes_125_72	established	21	18

Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all extensions from **Section 8.8** are displayed along with the IP address of the Application Enablement Services server, as shown below.

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

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper	IP Address
65000	1616 1	IP_Phone 1.340B	y	10.32.39.106 10.64.125.62	
65001	1608 1	IP_Phone 1.340B	y	10.32.39.104 10.64.125.62	
65001	1608 1	IP_API_A 3.2040	y	10.64.125.72 10.64.125.32	
65002	1616 1	IP_Phone 1.340B	y	10.32.39.105 10.64.125.62	
65002	1616 1	IP_API_A 3.2040	y	10.64.125.72 10.64.125.32	

9.2. 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays user information: Welcome: User, Last login: Mon Oct 28 11:50:49 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 28 13:24:57 MDT 2013, HA Status: Not Configured.

The main navigation bar includes **Status | Status and Control | TSAPI Service Summary** and **Home | Help | Logout**.

The left sidebar contains the following menu items:

- ▶ 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**

The main content area displays the **TSAPI Link Details** screen. It includes a checkbox for "Enable page refresh every 60 seconds" and a table of link details:

	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	4	15	301	30

Below the table are buttons for **Online** and **Offline**. At the bottom, there is a section for service-wide information with buttons for **TSAPI Service Status**, **TLink Status**, and **User Status**.

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify 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 total number of configured VoIP channels from **Section 8.8**.

Welcome: User
 Last login: Mon Oct 28 11:50:49 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 28 13:25:19 MDT 2013
 HA Status: Not Configured

AVAYA Application Enablement Services Management Console

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

DMCC Service Summary - Session Summary

Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
 Generated on Mon Oct 28 13:25:19 MDT 2013

Service Uptime: 11 days, 5 hours 27 minutes
 Number of Active Sessions: 1
 Number of Sessions Created Since Service Boot: 24
 Number of Existing Devices: 2
 Number of Devices Created Since Service Boot: 69

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	082CB103E9C3809D6 DB230F81C693F8F-27	vpi	VoicePrintServer	20.32.39.160	XML Unencrypted	2

Item 1-1 of 1
 Go

9.3. Verify Avaya Proactive Contact

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

```

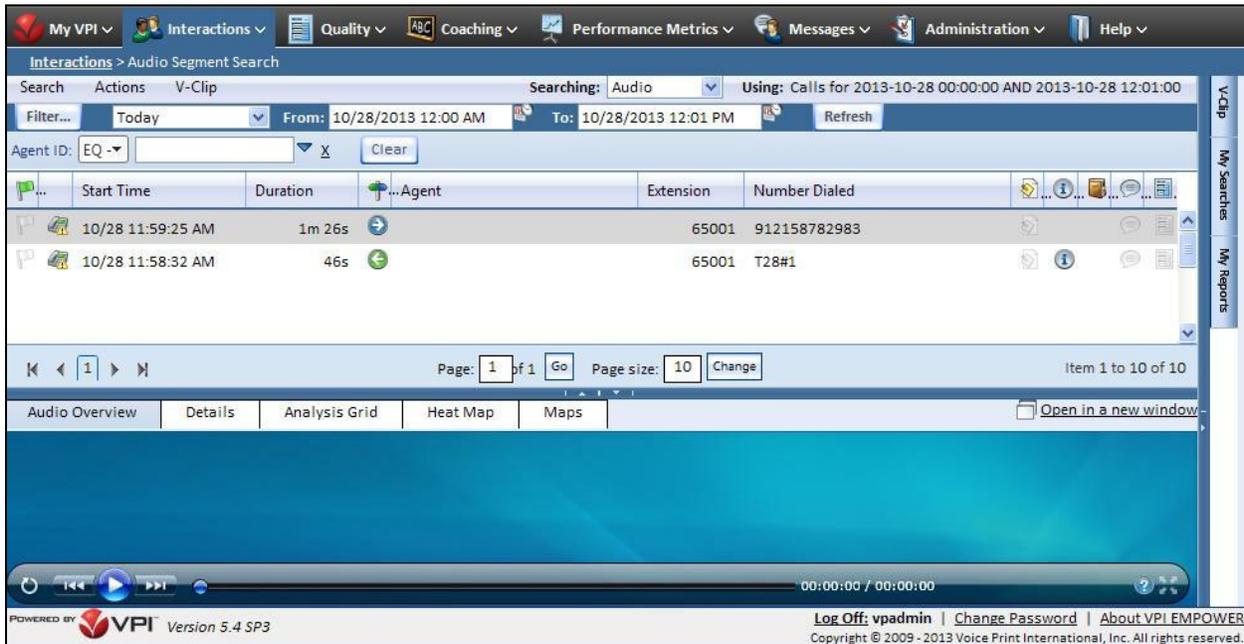
tcp        0      0 lzpds4b:enserver_ssl  10.32.39.160:49337  ESTABLISHED
tcp        0      0 lzpds4b:enserver_ssl  lzpds4b:62177      ESTABLISHED
tcp        0      0 lzpds4b:62177         lzpds4b:enserver_ssl ESTABLISHED
  
```

9.4. Verify VPI EMPOWER Suite

Start a job on Proactive Contact, and log an agent in to handle and complete a call. Access the EMPOWER Suite web-based interface by using the URL “https://ip-address/VPportal” 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 EMPOWER software interface. At the top, there is a navigation menu with options: My VPI, Interactions, Quality, Coaching, Performance Metrics, Messages, Administration, and Help. Below this is the 'Interactions > Audio Segment Search' section. It includes a search bar with 'Searching: Audio' and 'Using: Calls for 2013-10-28 00:00:00 AND 2013-10-28 12:01:00'. There are filters for 'Filter...' (Today), 'From:' (10/28/2013 12:00 AM), and 'To:' (10/28/2013 12:01 PM), along with a 'Refresh' button. An 'Agent ID:' field contains 'EQ' and a 'Clear' button. Below the search filters is a table with columns: Start Time, Duration, Agent, Extension, and Number Dialed. The table contains two entries:

Start Time	Duration	Agent	Extension	Number Dialed
10/28 11:59:25 AM	1m 26s	[Agent Icon]	65001	912158782983
10/28 11:58:32 AM	46s	[Agent Icon]	65001	T28#1

Below the table is a pagination bar showing 'Page: 1 of 1', 'Page size: 10', and 'Item 1 to 10 of 10'. The main area is divided into tabs: Audio Overview, Details, Analysis Grid, Heat Map, and Maps. The 'Audio Overview' tab is active, showing a timeline for the call on 10/28/2013 from 11:59:25 AM to 12:00:29 PM. A green bar represents the audio waveform, and a vertical line indicates the current playback position at 11:59:46 AM. The playback controls at the bottom show a play button, a progress bar at 00:10 / 01:26, and a volume icon. The footer includes 'POWERED BY VPI Version 5.4 SP3' and 'Log Off: vpadmin | Change Password | About VPI EMPOWER Copyright © 2009 - 2013 Voice Print International, Inc. All rights reserved.'

10. Conclusion

These Application Notes describe the configuration steps required for VPI EMPOWER Suite to successfully interoperate with Avaya Proactive Contact 5.1 with PG230 and Avaya Aura® Application Enablement Services 6.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 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. *Administering Avaya Proactive Contact*, Release 5.1, April 2013, available at <http://support.avaya.com>.
4. *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.