



Application Notes for VPI EMPOWER Suite with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services Using Multiple Registration – 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 using Multiple Registration. 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 Multiple Registration feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture media associated with the monitored agent stations for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 5.6 to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 using Multiple Registration. 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 stations on Avaya Aura® Communication Manager, and used the Multiple Registration feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture media associated with the monitored agent stations for call recording.

The TSAPI interface is used by VPI EMPOWER Suite to monitor VDNs, skill groups, and agent stations to be recorded, 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 TSAPI interface, and starts the call recording by using the media from the associated virtual IP softphone. The TSAPI event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

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

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.
- 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.

The feature tests also included following call scenarios:

- Basic calls to/from Extensions
- Basic calls to/from Agents
- Basic calls to Hunt Groups (Skills)
- Calls to/from the PSTN
- Hold/Retrieve
- Blind and Supervised Transfers
- Conference Calls

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 via the following means:

- **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 configuration used a single server configuration.

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	12101, 12102
Skill Group	12001, 12003, 12004
Extensions	11001, 11002, 11003, 11251 (H.323 and Digital)
Agents	1101, 1102, 1103, 1251

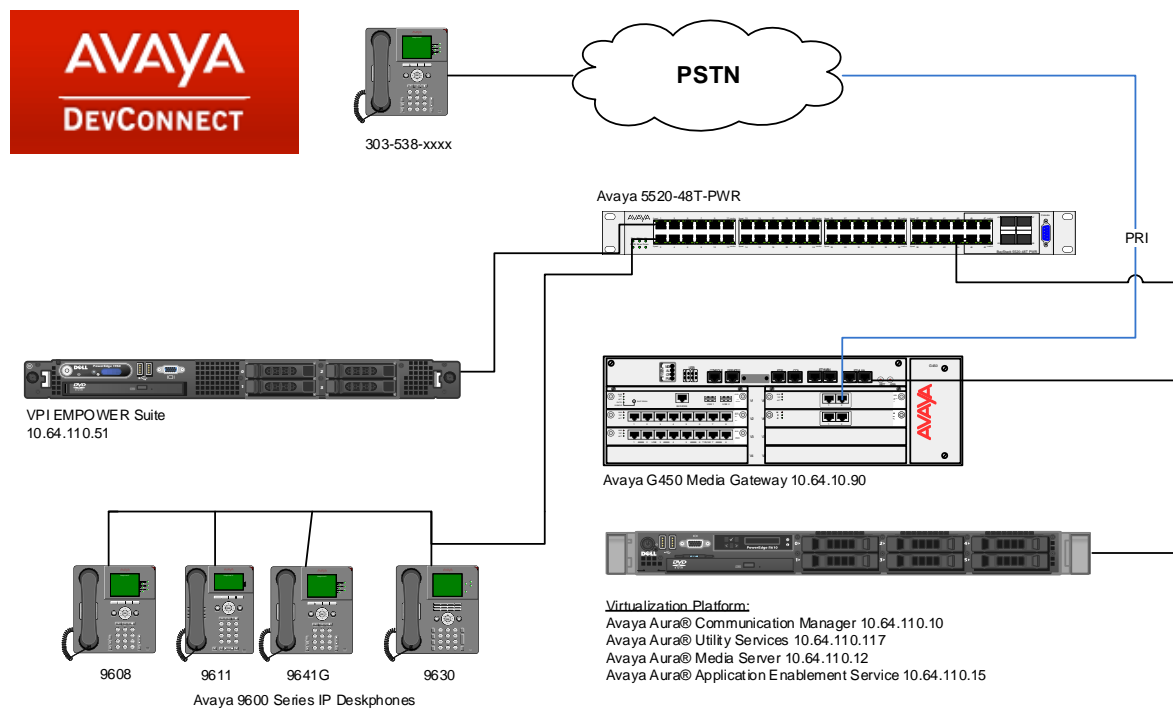


Figure 1: Compliance Testing Configuration

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 with Avaya G430 Media Gateway	7.0 SP1
Avaya Aura® Application Enablement Services	7.0
Avaya one-X® Communicator (H.323)	6.2
Avaya 9611G IP Deskphone (H.323)	6.6
Avaya 9650 IP Deskphone (H.323)	3.25
Avaya 6408D+ Digital Telephone	NA
VPI EMPOWER Suite on Windows Server 2012 <ul style="list-style-type: none">• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC .NET (ServiceProvider.dll)	5.6 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

Please note that all the configuration mentioned in this section is performed via System Access Terminal (SAT).

5.1. Verify License

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	Digital Loss Plan Modification?	y		
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y		
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y		
ATMS?	y				
Attendant Vectoring?	y				

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1	Page 1 of 3
CTI LINK	
CTI Link: 1	
Extension: 19999	
Type: ADJ-IP	
Name: aes	COR: 1

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 UI During Conference/Transfer? n
    Call Classification After Answer Supervision? n
        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 11001                                             Page 1 of 5
                                STATION
Extension: 11001                                         Lock Messages? n                               BCC: 0
    Type: 9650                                           Security Code: 123456                           TN: 1
    Port: S00204                                         Coverage Path 1:                               COR: 1
    Name: IP Station 1                                   Coverage Path 2:                               COS: 1
                                                Hunt-to Station:                               Tests? y

STATION OPTIONS
    Loss Group: 19                                         Time of Day Lock Table:
    Speakerphone: 2-way                                   Personalized Ringing Pattern: 1
    Display Language: english                             Message Lamp Ext: 11001
    Survivable GK Node Name:                             Mute Button Enabled? y
    Survivable COR: internal                             Button Modules: 0
    Survivable Trunk Dest? y                             Media Complex Ext:
                                                IP SoftPhone? y
                                                IP Video Softphone? n
                                                Short/Prefixed Registration Allowed: default
                                                Customizable Labels? y
```

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
- Restart services
- Obtain Tlink name
- Administer VPI user
- Administer security database
- Verify ports

6.1. Launch OAM Interface

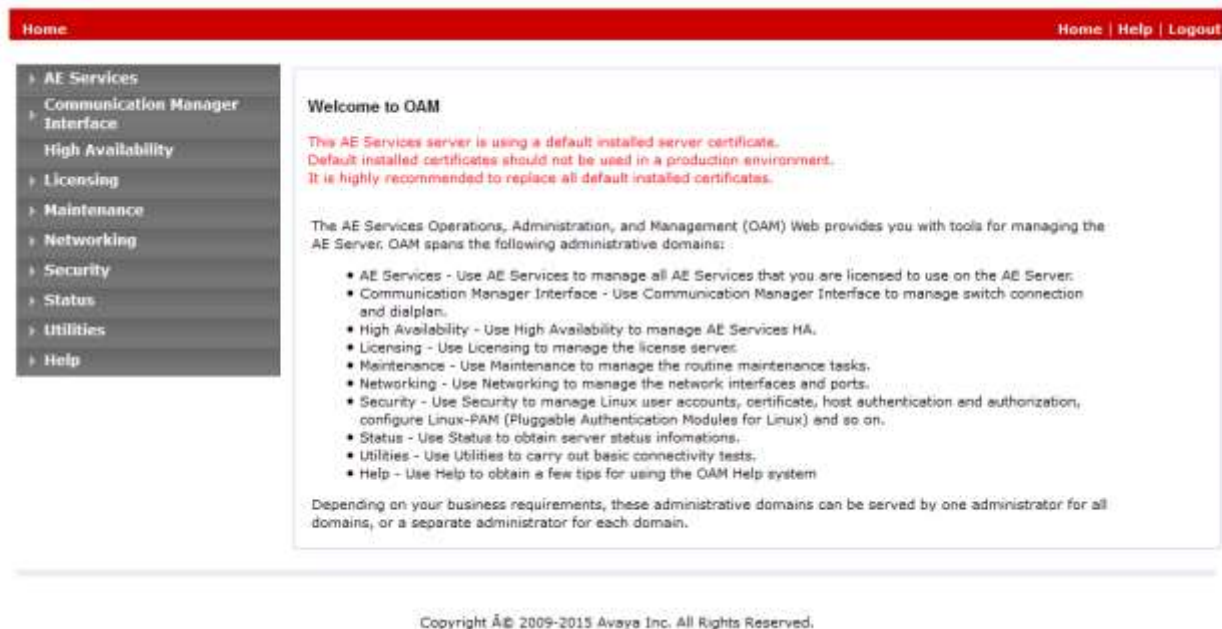
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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 "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. Below this bar is a login box with the text "Please login here:" and "Username" followed by a text input field. A "Continue" button is located below the input field. At the bottom of the page, another red horizontal bar is present, with the copyright notice "Copyright © 2009-2015 Avaya Inc. All Rights Reserved." centered below it.

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



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 **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.

AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16	0
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000	7
DLG VALUE_AES_DLG	permanent	16	0
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000	4

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**.

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm	1	7	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 “cm” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

Add TSAPI Links

Link

1 ▾

Switch Connection

cm ▾

Switch CTI Link Number

1 ▾

ASAI Link Version

1 ▾

Security

Unencrypted ▾

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 “cm”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as the H.323 gatekeeper, in this case “10.64.110.10” as shown below. Click **Add Name or IP**.

Edit H.323 Gatekeeper - cm

Name or IP Address

6.5. 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**.

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

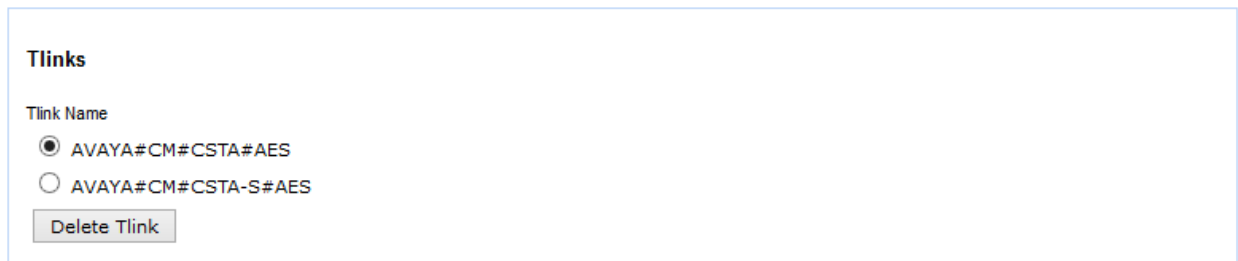
For status on actual services, please use [Status and Control](#)

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#CM#CSTA#AES”. Note the use of the switch connection “cm” from **Section 6.3** as part of the Tlink name.



Tlinks

Tlink Name

☒ AVAYA#CM#CSTA#AES

☐ AVAYA#CM#CSTA-S#AES

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 shows the 'Add User' form within the Avaya User Management application. The top navigation bar is red and contains the text 'User Management | User Admin | Add User' on the left and 'Home | Help | Logout' on the right. A left-hand sidebar menu lists various system categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under 'User Admin', the 'Add User' option is selected and highlighted in blue. The main content area is titled 'Add User' and includes a note: 'Fields marked with * can not be empty.' The form contains the following fields: '* User Id' (text input with 'vpi'), '* Common Name' (text input with 'vpi'), '* Surname' (text input with 'vpi'), '* User Password' (password input with masked dots), '* Confirm Password' (password input with masked dots), 'Admin Note' (text input), 'Avaya Role' (dropdown menu showing 'None'), 'Business Category' (text input), 'Car License' (text input), 'CM Home' (text input), 'Css Home' (text input), 'CT User' (dropdown menu showing 'Yes'), 'Department Number' (text input), and 'Display Name' (text input).

6.8. Administer Security Database

Select **Security** → **Security Database** → **CTI Users** → **List All User**. Edit the user added in **Section 6.7**.

Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

Edit CTI User

User Profile:	User ID	vpi
	Common Name	vpi
	Worktop Name	NONE ▾
	Unrestricted Access	<input checked="" type="checkbox"/>

Call and Device Control:	Call Origination/Termination and Device Status	None ▾
--------------------------	--	--------

Call and Device Monitoring:	Device Monitoring	None ▾
	Calls On A Device Monitoring	None ▾
	Call Monitoring	<input type="checkbox"/>

Routing Control:	Allow Routing on Listed Devices	None ▾
------------------	---------------------------------	--------

6.9. Verify Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, ensure the radio button for **Unencrypted Port** under the **Enabled** column is selected, as shown below. Note the port value for **Unencrypted Port**, it will be used in for configuring EMPOWER Suite in **Section 7.4**.

DMCC Server Ports		Enabled	Disabled
Unencrypted Port	4721	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	4722	<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	4723	<input checked="" type="radio"/>	<input type="radio"/>

7. Configure VPI EMPOWER Suite

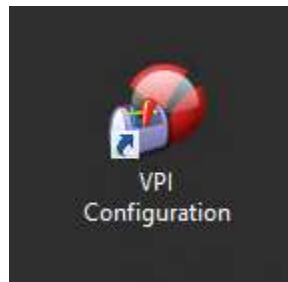
This section provides the procedures for configuring EMPOWER Suite. The procedures include the following areas:

- Launch VPI Configuration
- Administer start/stop events
- Administer TSAPI
- Administer DMCC
- Administer channels
- Launch VPI CLogger Runtime Manager

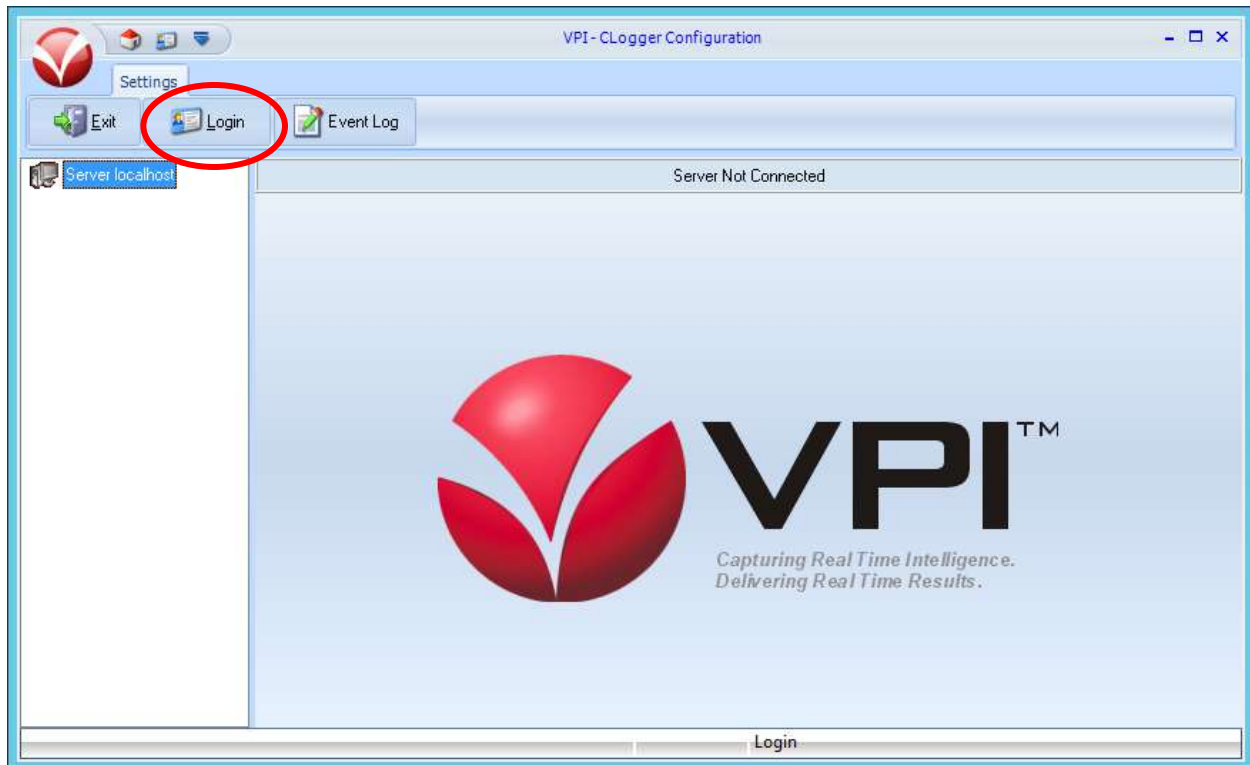
The configuration of EMPOWER Suite is performed by VPI installers. The procedural steps are presented in these Application Notes for informational purposes.

7.1. 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.

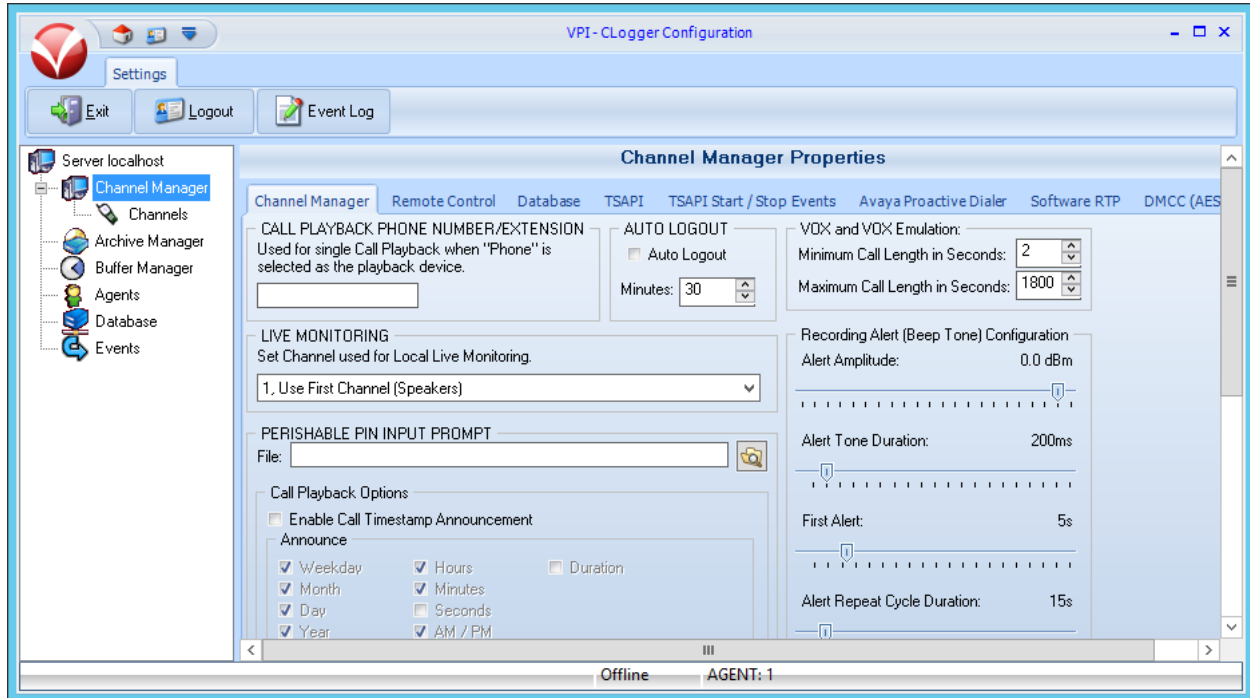


The screen below is displayed next. Log in using the appropriate credentials.

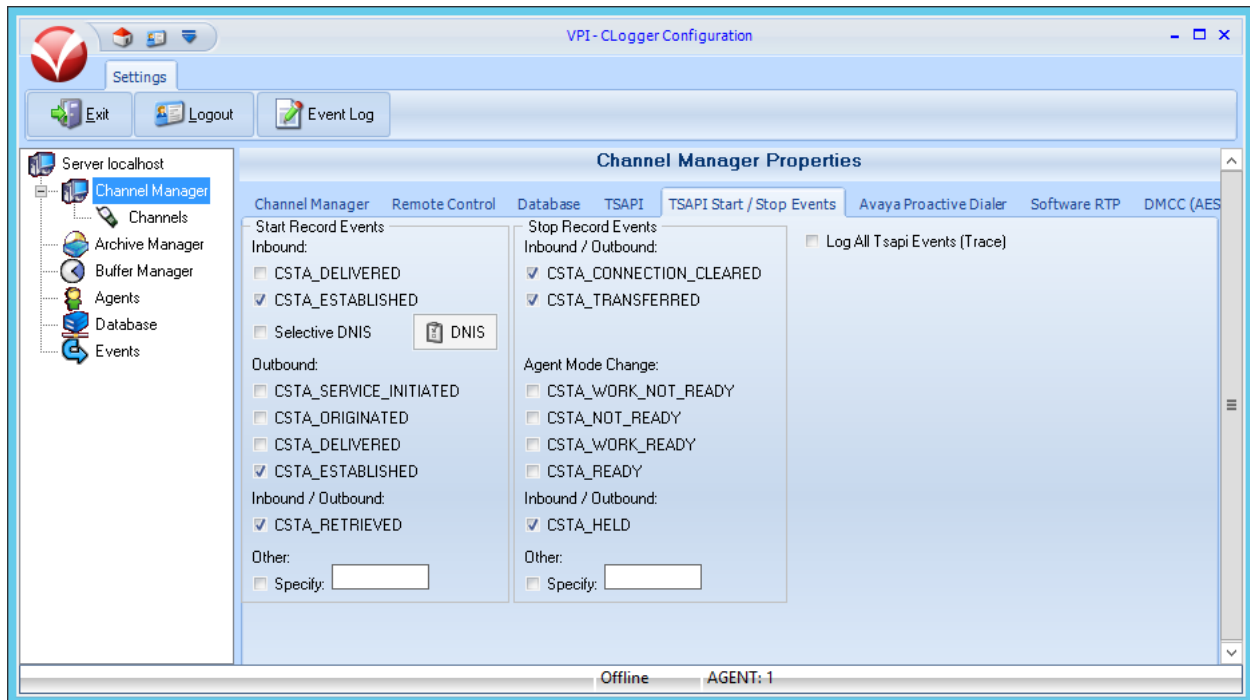


7.2. Administer Start/Stop Events

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 **TSAPI 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.



7.3. Administer TSAPI

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

- **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**.
- **Extensions:** The Station extension from **Section 3**.

The screenshot shows the 'VPI - CLogger Configuration' window. The 'Settings' tab is active, and the 'Channel Manager Properties' section is expanded. The 'TSAPI' tab is selected. The 'TSAPI Server Setup' section contains the following fields:

- Server 1 Machine: AVAYA#CMHCSTAE
- Server 2 Machine: (empty)
- TSAPI Device: (empty)
- Application Username: vpi
- Application Password: (masked)
- Fail to VDX: (unchecked)
- Save All ANI: (unchecked)
- Switch Type: Avaya / Lucent (selected)

The 'General Options' section contains the following fields:

- Record All Agents: (checked)
- Lock Status Lights: (unchecked)
- Use Tsapi Time Stamp: (unchecked)

The 'Additional Monitors' section contains the following fields:

- ACD Groups: 12001, 12002, 12003
- Trunks: (empty)
- VDNs: 12101, 12102
- Extensions: (empty)
- View/Edit: (button)

The 'Service Observe Options' section contains the following fields:

- Monitor Agent Mode Change: (checked)
- Feature Code: (empty)

The 'Dialers Enabled' section contains the following fields:

- DaVox: (unchecked)
- Genesys T-Server: (unchecked)
- IAT: (unchecked)

The 'DN Station Monitors' section contains the following field:

- Minimum Digits: 4

The window has a status bar at the bottom showing 'Offline' and 'AGENT: 1'. The 'Cancel' and 'Apply' buttons are at the bottom right.

7.4. Administer DMCC

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

- **Server IP Address:** IP Address of AES Server.
- **Switch (CLAN) Address:** IP Address of Communication Manager from **Section 6.4**.
- **Server Port:** DMCC Port as configured in **Section 6.9**.
- **Global Ext Password:** Extension password as configured in **Section 5.4**.
- **Session User:** The VPI user credentials from **Section 6.7**.
- **Session Password:** The VPI user credentials from **Section 6.7**.

The screenshot shows the 'VPI-CLogger Configuration' window with the 'DMCC (AES)' tab selected. The window has a sidebar on the left with a tree view containing 'Server localhost', 'Channel Manager', 'Channels', 'Archive Manager', 'Buffer Manager', 'Agents', 'Database', and 'Events'. The main area is titled 'Channel Manager Properties' and contains several tabs: 'Channel Manager', 'Remote Control', 'Database', 'TSAPI', 'TSAPI Start / Stop Events', 'Avaya Proactive Dialer', 'Software RTP', and 'DMCC (AES)'. The 'DMCC (AES)' tab is active, showing 'General Options' and 'TLS (SSL) Options' sections. In 'General Options', the 'Enable' checkbox is checked. The 'Server IP Address' is '10.64.110.15', 'Switch (CLAN) Address' is '10.64.110.10', 'Server Port' is '4721', 'Global Ext Password' is masked with 'xxxxxx', 'Session User' is 'vpi', 'Session Password' is masked with 'xxxxxxxx', and 'Device Instance' is empty. In 'TLS (SSL) Options', the 'Enable' checkbox is checked, 'Version' is 'SSL v2', and 'Allow Older Versions' is unchecked. The 'Certificate File', 'CA File', 'Key File', 'Client CA File', 'CA Path', 'Key Phrase', 'Packet Timeout' (30), 'Connect Timeout' (30), 'Verify Peer' (unchecked), and 'Verify Depth' (30) fields are all empty or have default values. At the bottom right are 'Cancel' and 'Apply' buttons. The status bar at the bottom shows 'Offline' and 'AGENT: 1'.

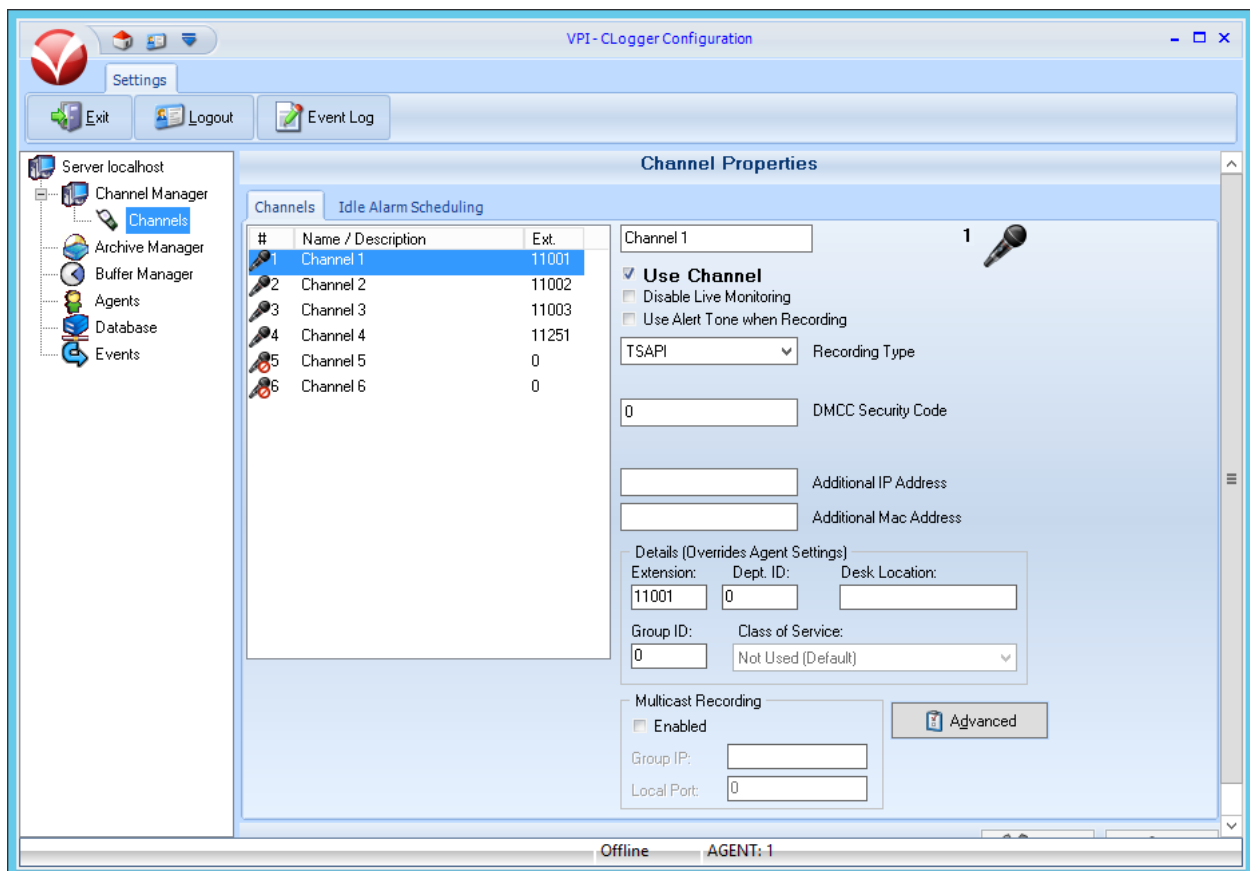
Field	Value
Enable	<input checked="" type="checkbox"/>
Server IP Address	10.64.110.15
Switch (CLAN) Address	10.64.110.10
Server Port	4721
Global Ext Password	xxxxxx
Session User	vpi
Session Password	xxxxxxxx
Device Instance	
TLS (SSL) Options Enable	<input checked="" type="checkbox"/>
Version	SSL v2
Allow Older Versions	<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

7.5. Administer Channels

Select **Server localhost** → **Channel Manager** → **Channels** in the left pane, to display the **Channel Properties** screen. Select the first pertinent channel from the left portion of the **Channel Properties** screen, in this case **Channel 1**, 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 station to be monitored from **Section 3**.

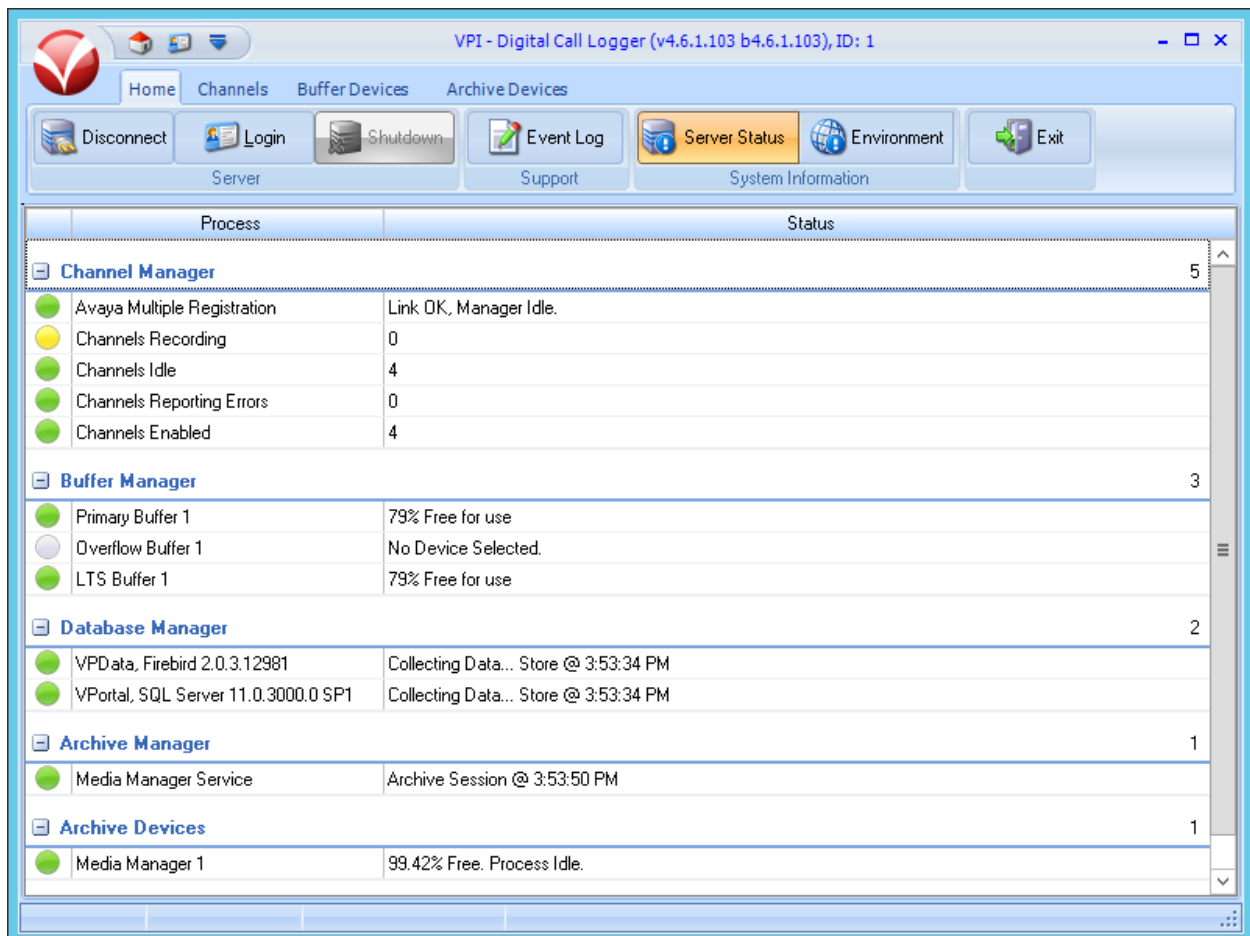


7.6. Launch VPI CLogger Runtime Manager

From the EMPOWER Suite server, double-click on the **VPI CLogger Runtime Manager** 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 6.6**, 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	7	no	aes	established	15	15

Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all extensions configured in **Section 7.5** are displayed along with the IP address of the Application Enablement Services server and **Prod ID** of **IP_API_A**, 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		
11001	9621	IP_Phone	y	10.64.10.238		
	1	6.6115		10.64.110.10		
11001	9621	IP_API_A	y	10.64.110.15		
	1	3.2040		10.64.110.10		
11002	9650	oneX_Comm	y	10.64.10.49		
	1	6.2100		10.64.110.10		
11002	9650	IP_API_A	y	10.64.110.15		
	1	3.2040		10.64.110.10		
11003	9630	IP_Phone	y	10.64.10.91		
	1	3.242A		10.64.110.10		
11003	9630	IP_API_A	y	10.64.110.15		
	1	3.2040		10.64.110.10		
11251	6408D+	IP_API_A	y	10.64.110.15		
	1	3.2040		10.64.110.10		

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**.

TSAPI Link Details

☐ Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm	1	Talking	Tue Nov 17 16:08:43 2015	Online	17	10	15	15	30

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

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

Verify the **User** column shows an active session with the VPI user name from **Section 6.7**, and that the **# of Associated Devices** column reflects the total number of configured VoIP channels from **Section 7.5**.

DMCC Service Summary - Session Summary
Please do not use back button
☐ Enable page refresh every seconds
Session Summary [Device Summary](#)
Generated on Wed Nov 18 16:57:28 MST 2015
Service Uptime: 2 days, 2 hours 10 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 16
Number of Existing Devices: 4
Number of Devices Created Since Service Boot: 33

<input type="checkbox"/>	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	F3BC98659E034113D 9E6D656437510B5-15	vpi	VoicePrintServer	10.64.110.202	XML Unencrypted	4

Item 1-1 of 1
 Go

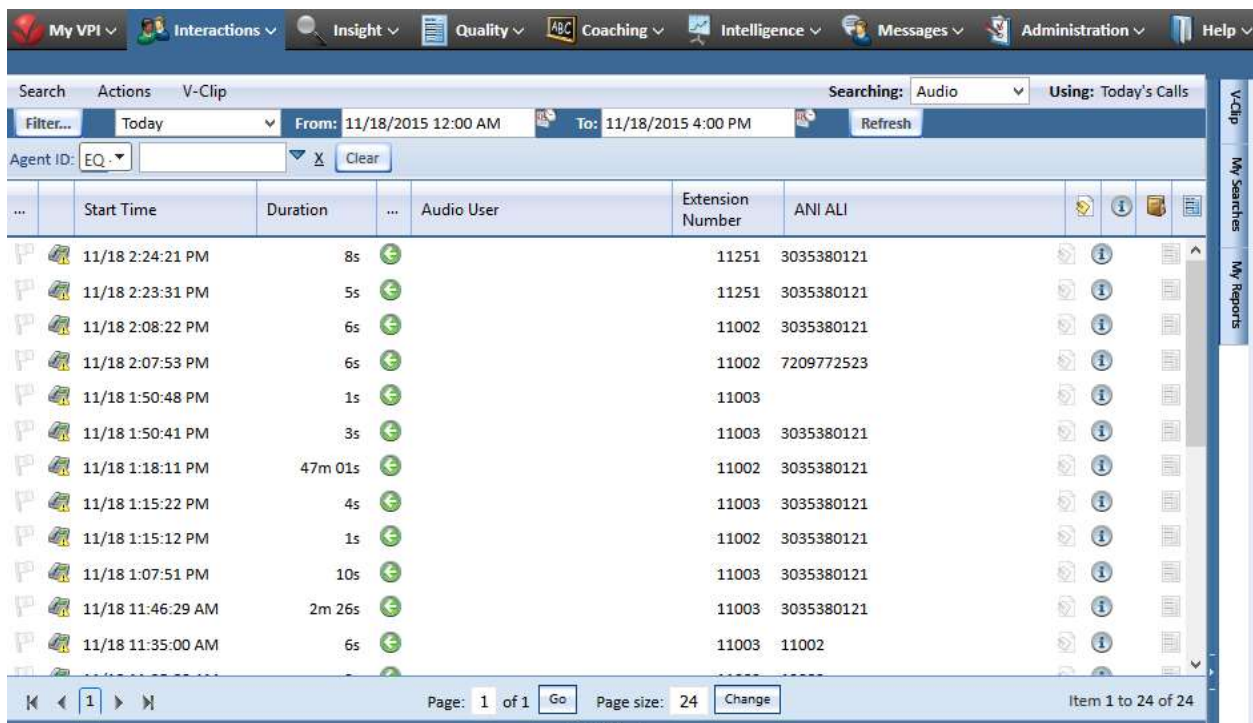
8.3. Verify VPI EMPOWER Suite

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 login screen for the VPI EMPOWER Suite. It features a light blue background with a large, faint VPI logo. In the center, there is a white rounded rectangle containing the login fields. The fields are labeled "User Name:" and "Password:", each followed by a white text input box. Below the password field is a blue "Login" button. To the left of the login fields is a small icon of a padlock. At the bottom of the screen, there is a footer with the text "POWERED BY VPI Version 5.6" on the left and "About VPI EMPOWER Copyright © 2009 - 2015 Voice Print International, Inc. All rights reserved." on the right.

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.



The screenshot shows the VPI EMPOWER Suite interface with a list of call recordings. The top navigation bar includes tabs for My VPI, Interactions, Insight, Quality, Coaching, Intelligence, Messages, Administration, and Help. Below the navigation bar, there is a search and filter section with a "Filter..." button, a "Today" dropdown, and date/time filters for "From: 11/18/2015 12:00 AM" and "To: 11/18/2015 4:00 PM". A "Refresh" button is also present. The main table displays call recordings with columns for Start Time, Duration, Audio User, Extension Number, and ANI ALI. The table is sorted by Start Time in descending order. The bottom of the screen shows a pagination bar with "Page: 1 of 1", "Page size: 24", and "Item 1 to 24 of 24".

...	Start Time	Duration	...	Audio User	Extension Number	ANI ALI			
	11/18 2:24:21 PM	8s			11251	3035380121			
	11/18 2:23:31 PM	5s			11251	3035380121			
	11/18 2:08:22 PM	6s			11002	3035380121			
	11/18 2:07:53 PM	6s			11002	7209772523			
	11/18 1:50:48 PM	1s			11003				
	11/18 1:50:41 PM	3s			11003	3035380121			
	11/18 1:18:11 PM	47m 01s			11002	3035380121			
	11/18 1:15:22 PM	4s			11003	3035380121			
	11/18 1:15:12 PM	1s			11002	3035380121			
	11/18 1:07:51 PM	10s			11003	3035380121			
	11/18 11:46:29 AM	2m 26s			11003	3035380121			
	11/18 11:35:00 AM	6s			11003	11002			

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 Search & Discovery web application. The top navigation bar includes tabs for My VPI, Interactions, Insight, Quality, Coaching, Intelligence, Messages, Administration, and Help. The main search area shows filters for 'Today', 'From: 11/18/2015 12:00 AM', and 'To: 11/18/2015 2:25 PM'. A table of search results is shown below, with columns for Start Time, Duration, Agent Name, and Events. The bottom section of the interface provides a detailed view of a selected call, including a timeline of events such as 'Sensitive Audio', 'Call Held', and 'Call Retrieved'. The playback controls at the bottom indicate the call duration is 00:00 / 00:08.

Start Time	Duration	Agent Name	Events
11/18 1:50:41 PM	8s		
11/18 1:18:11 PM	47m 01s		
11/18 1:15:22 PM	4s		
11/18 1:15:12 PM	1s		
11/18 1:07:51 PM	10s		
11/18 11:46:29 AM	2m 26s		
11/18 11:34:46 AM	20s		
11/18 11:14:48 AM	30s		
11/18 11:14:25 AM	14s		
11/18 11:00:51 AM	4s		
11/18 10:57:53 AM	19s		
11/18 10:52:17 AM	8s		

Interaction Overview | Details | AnalysisGrid | Heat Map | Maps | Open in a new window

11/18/2015 1:50:41 PM

1:50:41 PM

[Not Specified]

Sensitive Audio

11/18/2015 1:50:41 PM

Direction: Inbound

Number: 3035380121

Name: none

Validation (Success)

1:50:43 PM

Call Held

11/18/2015 1:50:44 PM

1:50:47 PM

Call Retrieved

11/18/2015 1:50:47 PM

1:50:49 PM

00:00 / 00:08

Powered by VPI Version 5.6

Log Off: vpadmin | Change Password | About VPI EMPOWER

Copyright © 2009 - 2015 Voice Print International, Inc. All rights reserved.

8.4. 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 using Multiple Registration. All feature and serviceability test cases were completed.

9. 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 7.0, August 2015, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
3. *VPI EMPOWER Avaya Channel Manager Guide*, September 2015, available on the VPI EMPOWER Suite server as part of installation.

©2016 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.