Avaya Solution & Interoperability Test Lab

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

Abstract

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

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

The TSAPI interface is used by VPI Voice Capture to monitor the stations to be recorded, and the DMCC interface is used by VPI Voice Capture to register a virtual recording device against each monitored station to pick up the media for call recording. When there is an active call at the monitored station, VPI Voice Capture is informed of the call via event reports from the TSAPI interface, and starts the call recording by using the media from the recording device associated with the monitored station. The TSAPI event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

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

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

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

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

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

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

2.2. Test Results

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

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

2.3. Support

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

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

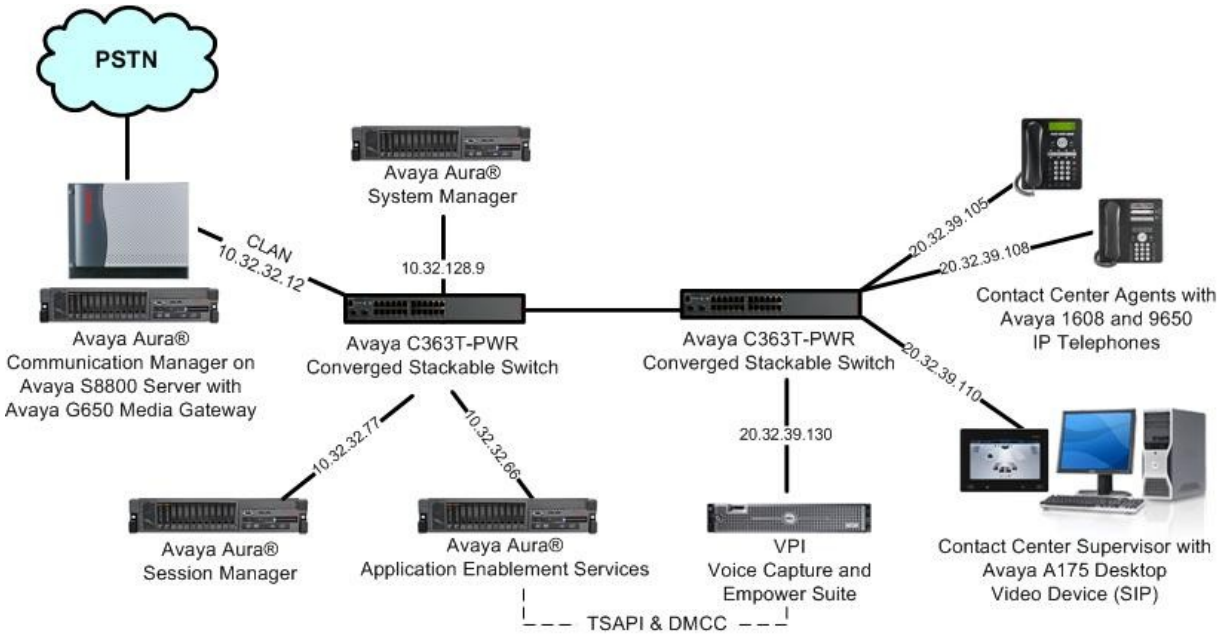
3. Reference Configuration

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

The Avaya Aura® Session Manager was used in the configuration to support Avaya SIP endpoints. The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® System Manager. The detailed administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, VPI Voice Capture monitored the contact center devices shown in the table below.

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



4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP3 (R016x.00.1.510.1-19009)
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor	 HW01 FW038 HW20 FW122
Avaya Aura® Application Enablement Services	6.1
Avaya Aura® Session Manager	6.1 SP2
Avaya Aura® System Manager	6.1 SP2
Avaya 1608 IP Telephones (H.323)	1.3
Avaya 9650 Series IP Telephones (H.323)	3.1
Avaya A175 Desktop Video Device (SIP)	1.0.2
VPI Voice Capture on Windows Server 2008 • Avaya TSAPI Windows Client	4.4.1.46 R2 Standard SP1 6.1.0.396
VPI Empower Suite	5.2.1.22

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify Communication Manager License

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

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

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                         CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                           CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                  ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  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 1                                                  Page   1 of   3
                                     CTI LINK
 CTI Link: 1
Extension: 60100
     Type: ADJ-IP
                                                                   COR: 1
     Name: VPI CTI Link
```

5.3. Administer System Parameters Features

Use the "change system-parameters features" command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name: S8500-SAL
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                              COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
              Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

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

```
change system-parameters features                                Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? y

    Reporting for PC Non-Predictive Calls? n

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

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

5.4. Administer Stations

Use the "change station n" command, where "n" is the first agent station extension from **Section 3**. Enable **IP SoftPhone**, to allow for a recording device to be registered against the station. Note the value of **Security Code**, which will be used later to configure VPI.

```
change station 65001                                          Page   1 of   4
                                     STATION

Extension: 65001                        Lock Messages? n               BCC: 0
     Type: 1608                         Security Code: 65001            TN: 1
     Port: S00000                     Coverage Path 1: 1               COR: 1
     Name: VPI Agent #1               Coverage Path 2:                 COS: 6
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19         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 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         S00000  VPI Agent #1                             1    1
               1608                        no                       1   1
65002         S00045  VPI Agent #2                             1    1
               9650                        no                       1   1
```

6. Configure Avaya Aura® Application Enablement Services

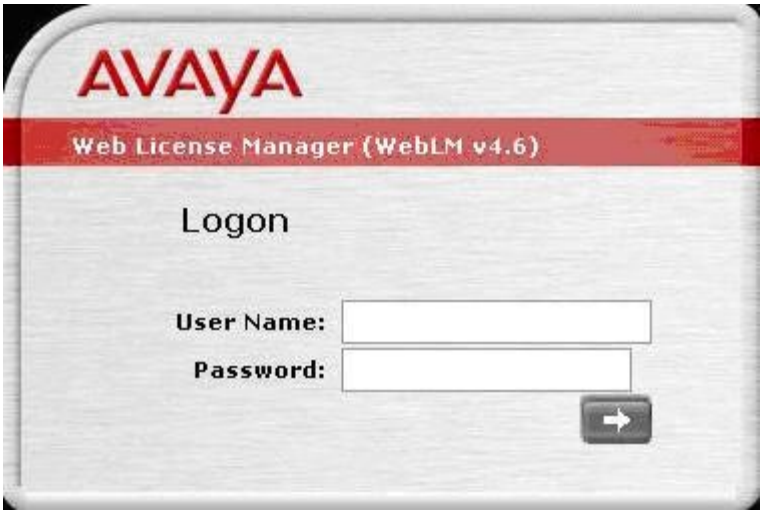
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

- Verify license
- Launch OAM interface
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer VPI user
- Enable DMCC unencrypted port

6.1. Verify License

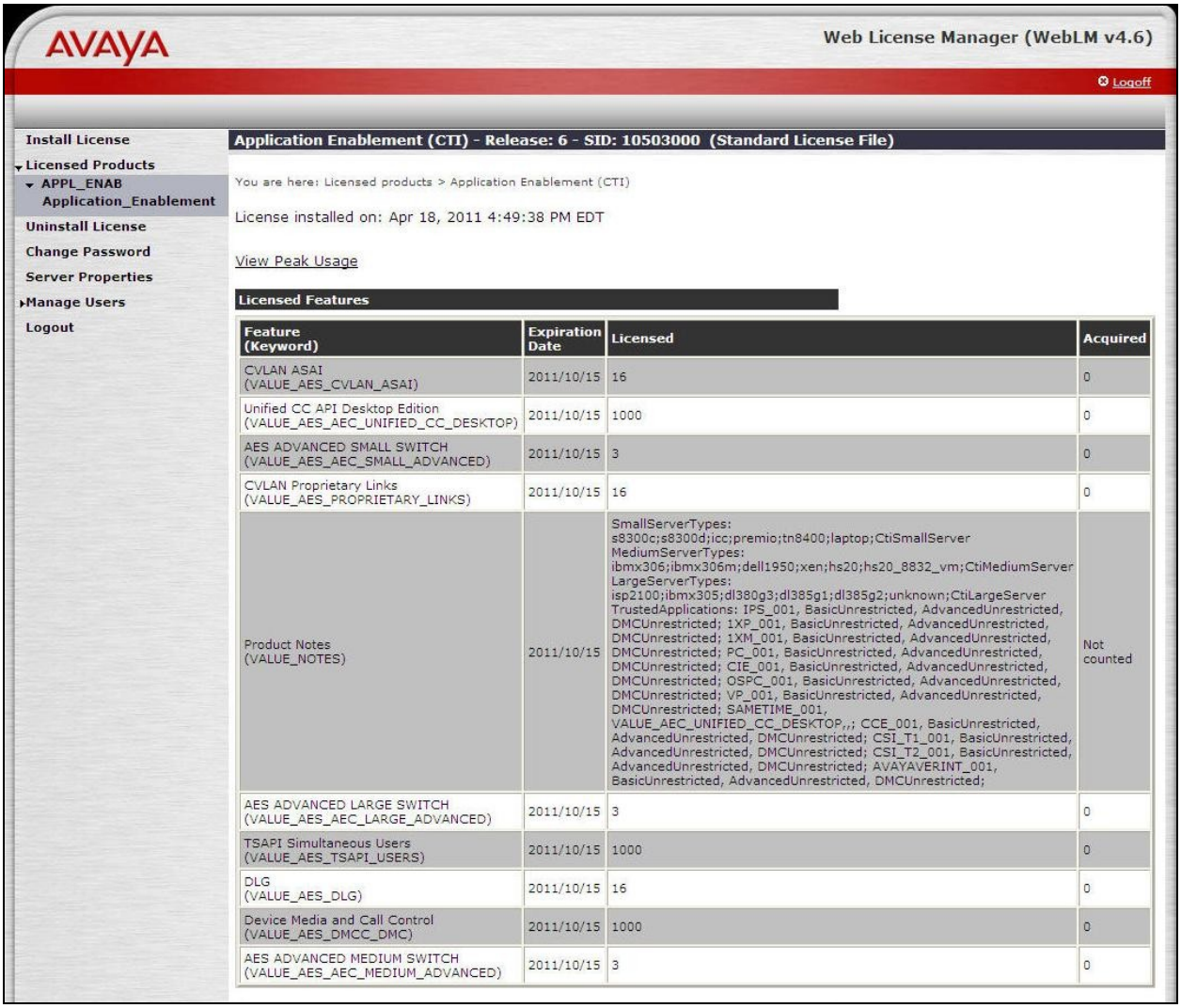
Access the Web License Manager interface by using the URL "https://ip-address:52233/ WebLM/ index.jsp" in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services server.

The **Web License Manager** screen is displayed. Log in using the appropriate credentials.



The **Web License Manager** screen below is displayed. Select **Licensed Products > APPL_ENAB > Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below.

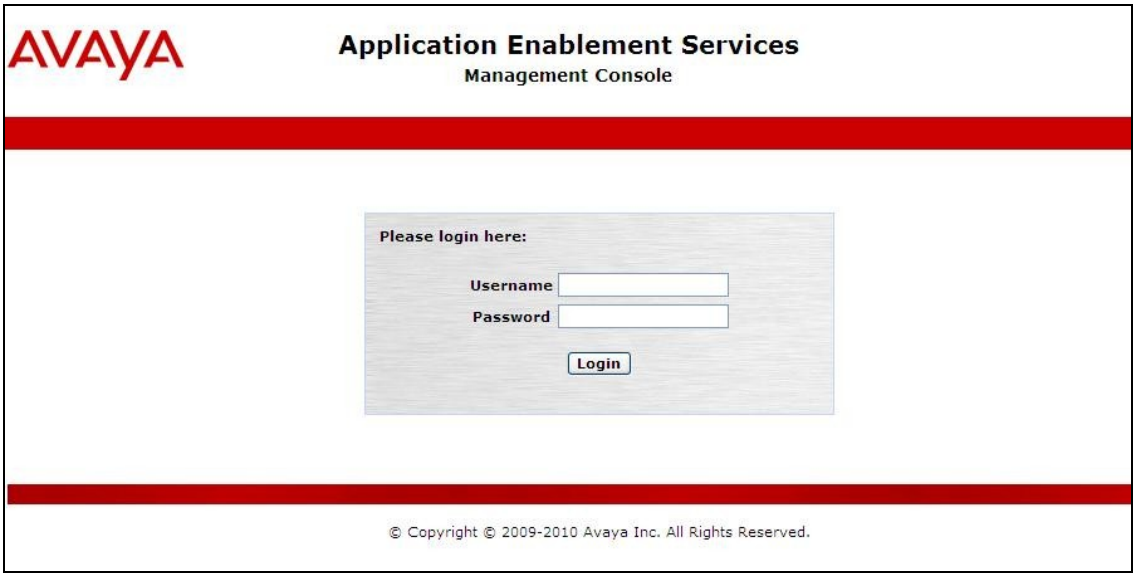


Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2011/10/15	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2011/10/15	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2011/10/15	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2011/10/15	16	0
Product Notes (VALUE_NOTES)	2011/10/15	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	2011/10/15	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2011/10/15	1000	0
DLG (VALUE_AES_DLG)	2011/10/15	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2011/10/15	1000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2011/10/15	3	0

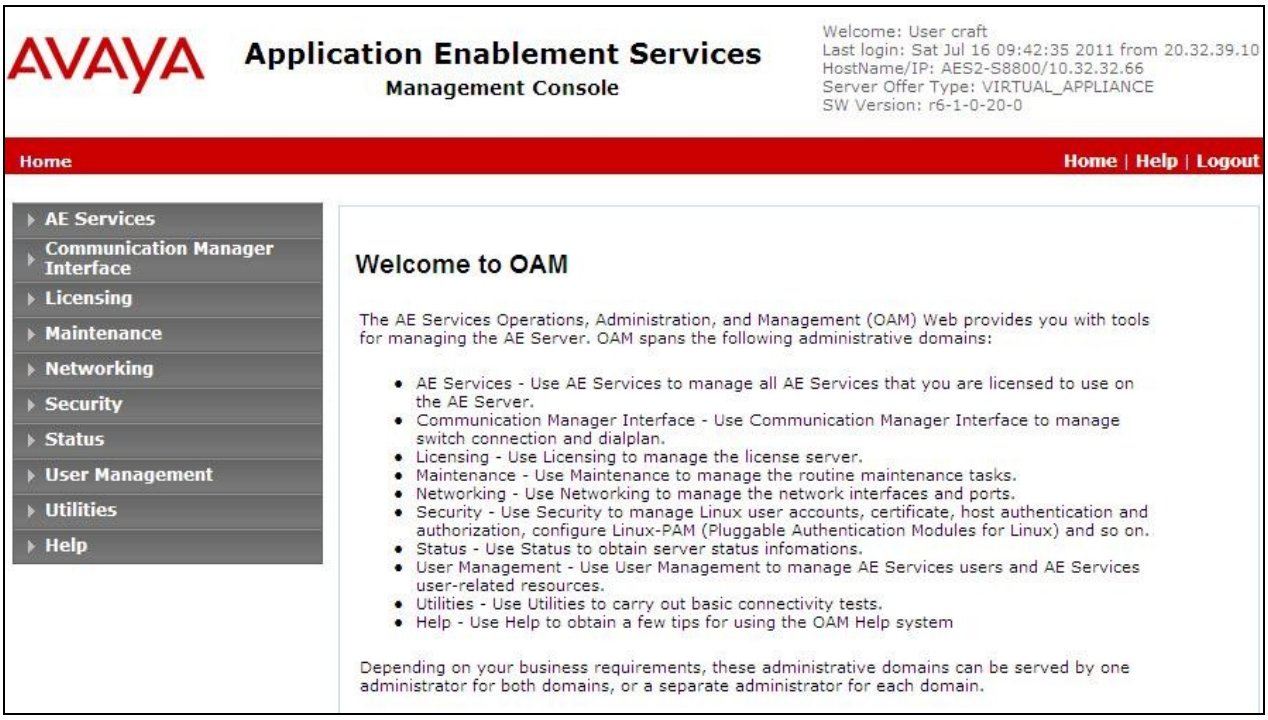
6.2. Launch OAM Interface

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

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

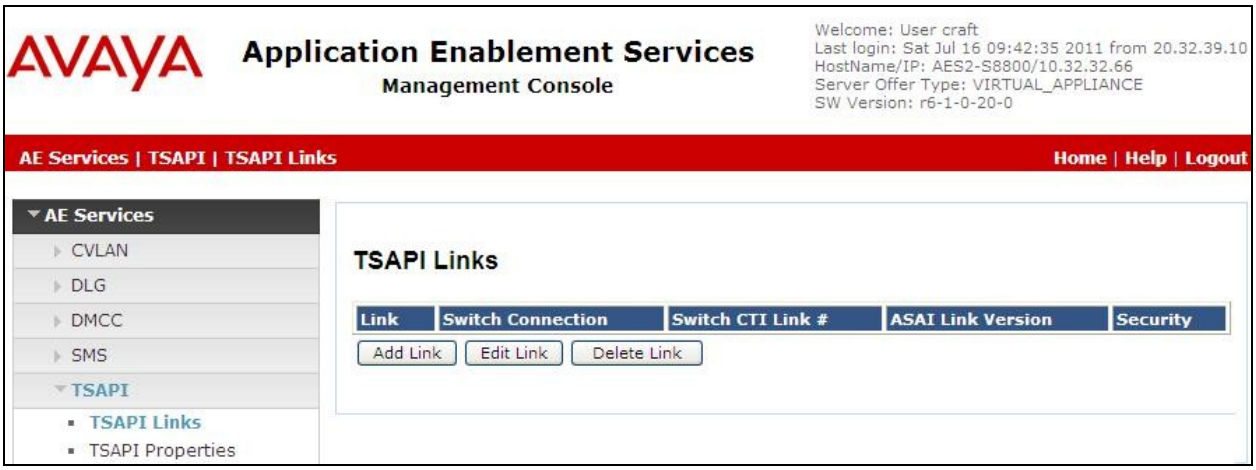


The **Welcome to OAM** screen is displayed next.



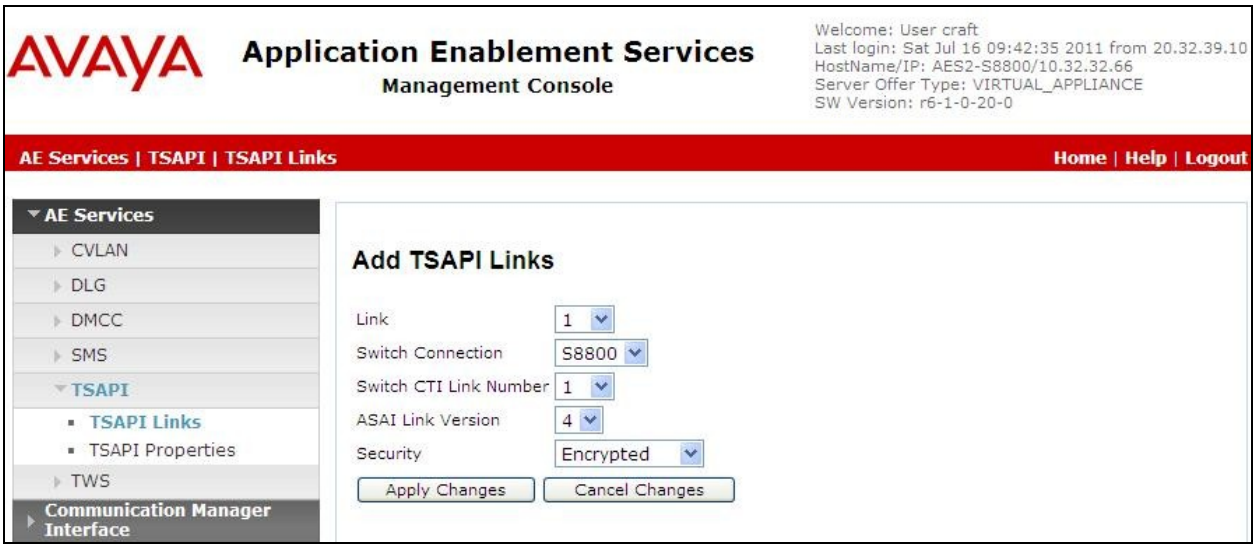
6.3. Administer TSAPI Link

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



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

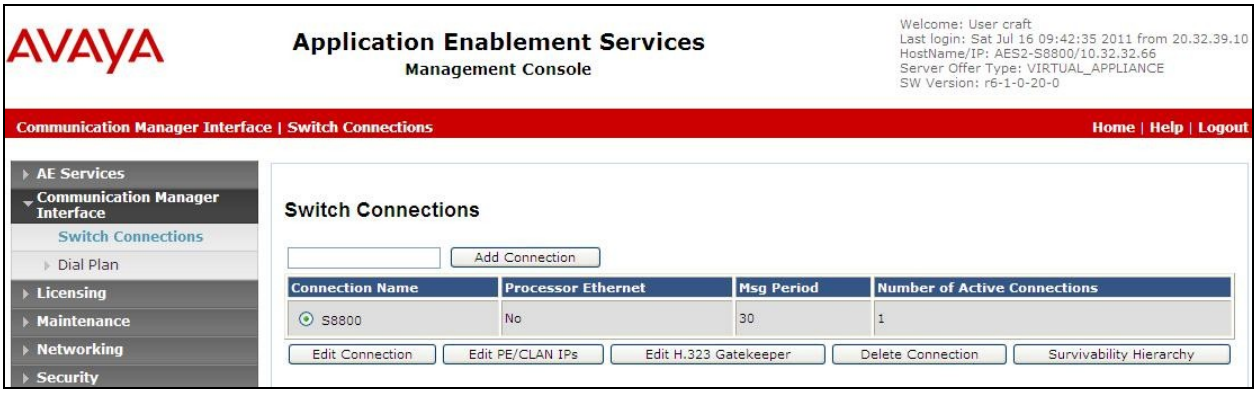
The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8800" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields, and click **Apply Changes**.



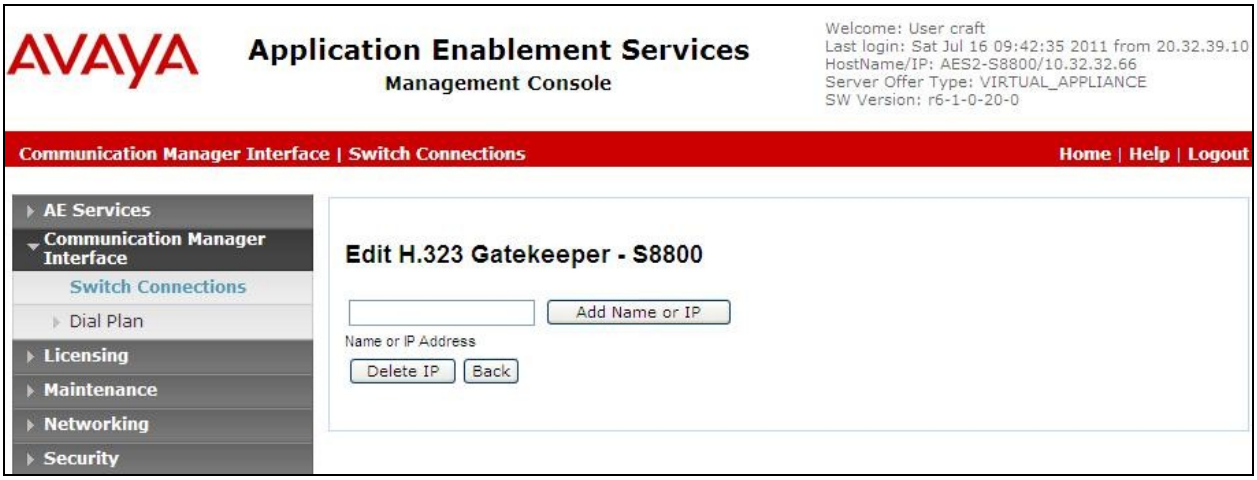
6.4. Administer H.323 Gatekeeper

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 **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, in this case "10.32.32.12" as shown below. Click **Add Name or IP**.

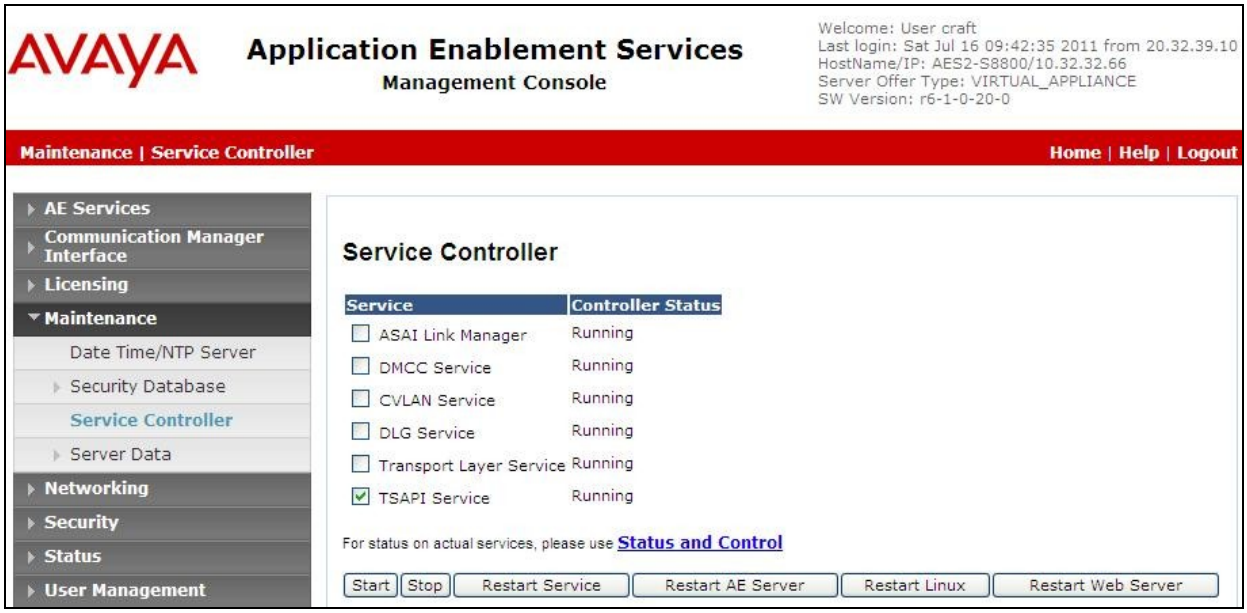


6.5. Disable Security Database

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

6.6. Restart TSAPI Service

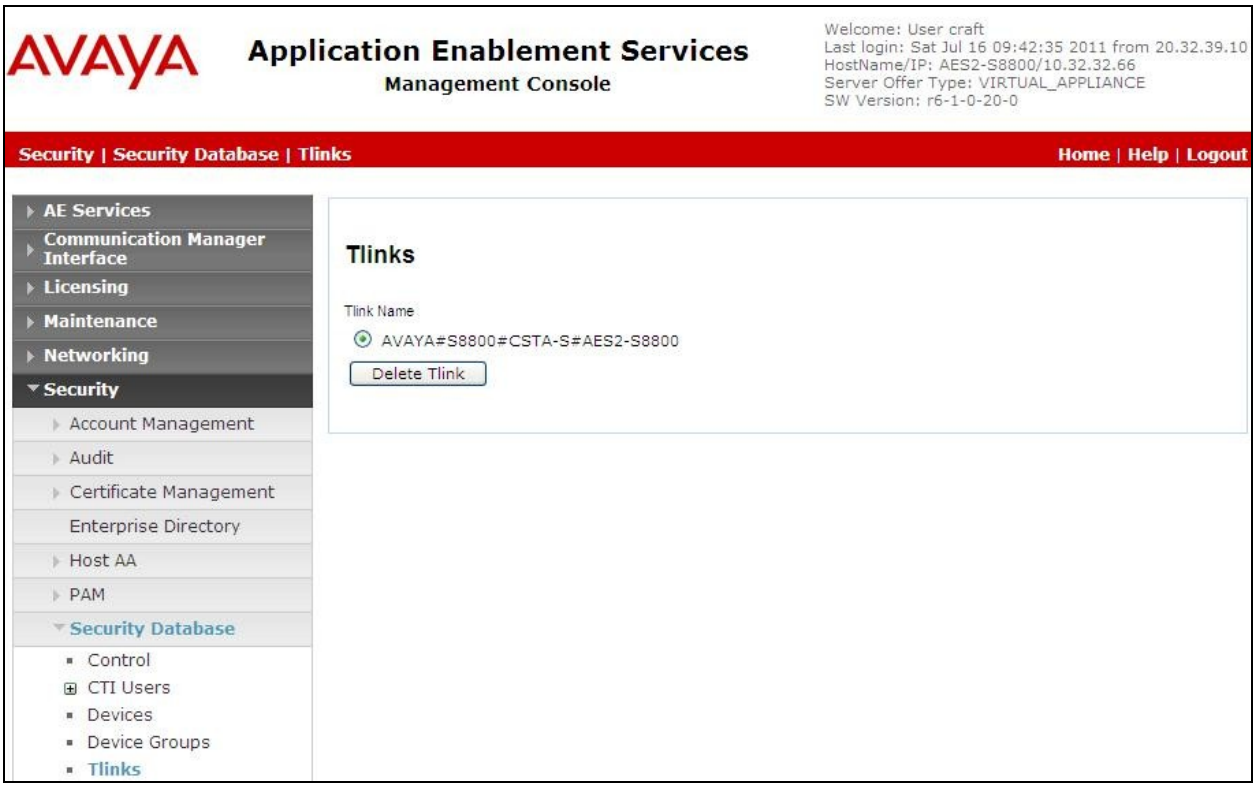
Select **Maintenance > Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service**, and click **Restart Service**.



6.7. Obtain Tlink Name

Select **Security > Security Database > Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring VPI.

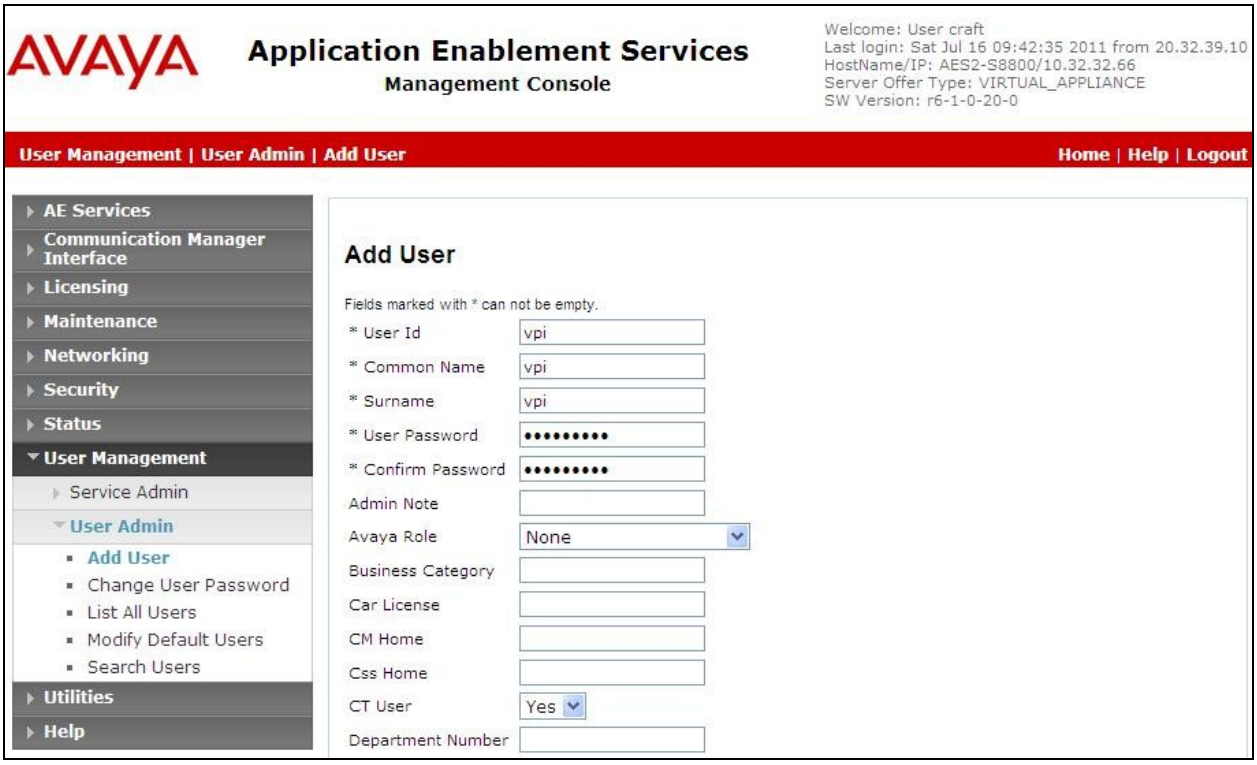
In this case, the associated Tlink name is "AVAYA#**S8800**#CSTA-S#AES2-S8800". Note the use of the switch connection "S8800" from **Section 6.3** as part of the Tlink name.



6.8. Administer VPI User

Select **User Management > User Admin > Add User** from the left pane, to display the **Add User** screen in the right pane.

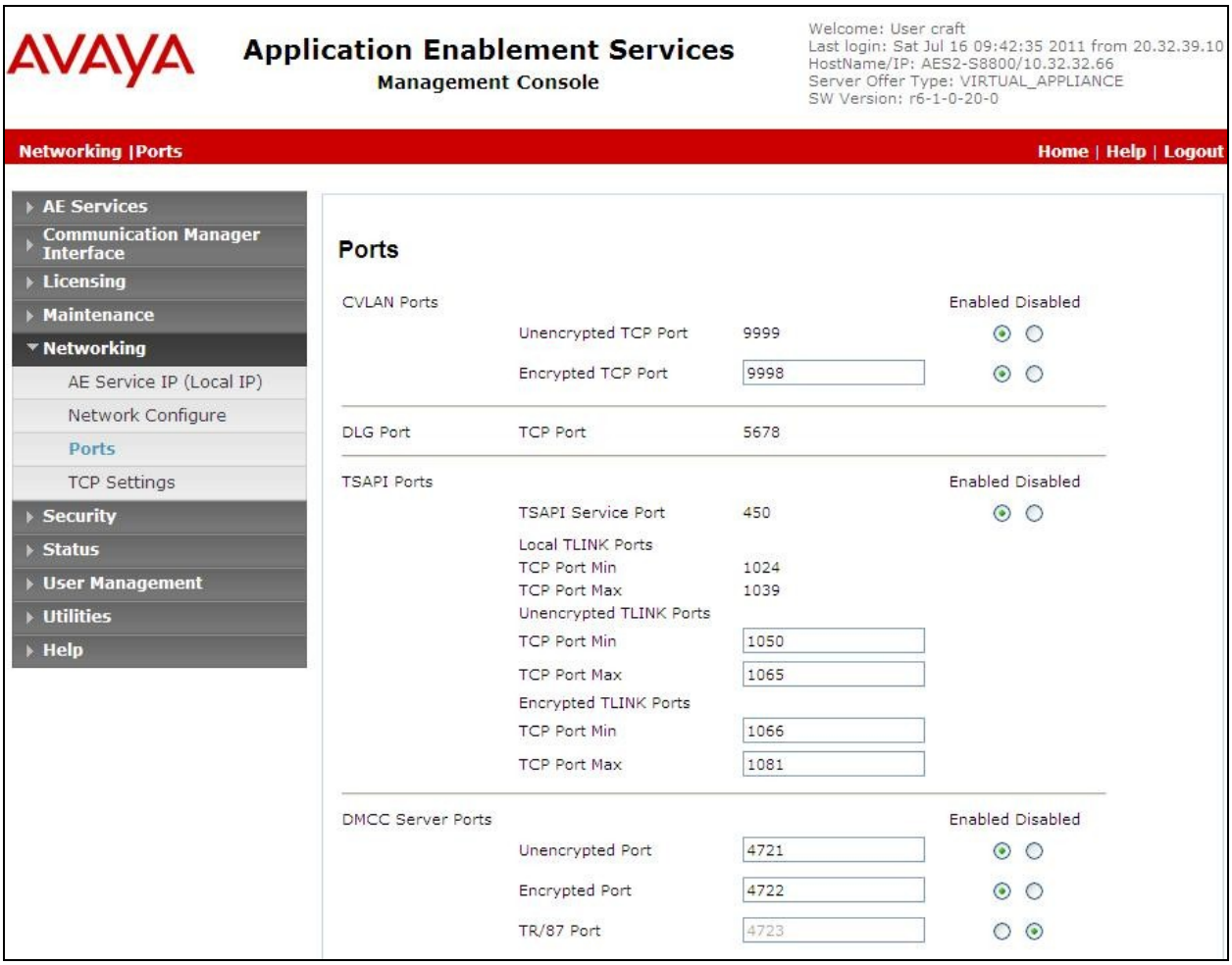
Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "Yes" from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).



6.9. Enable DMCC Unencrypted Port

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

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below.



7. Configure VPI Voice Capture

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

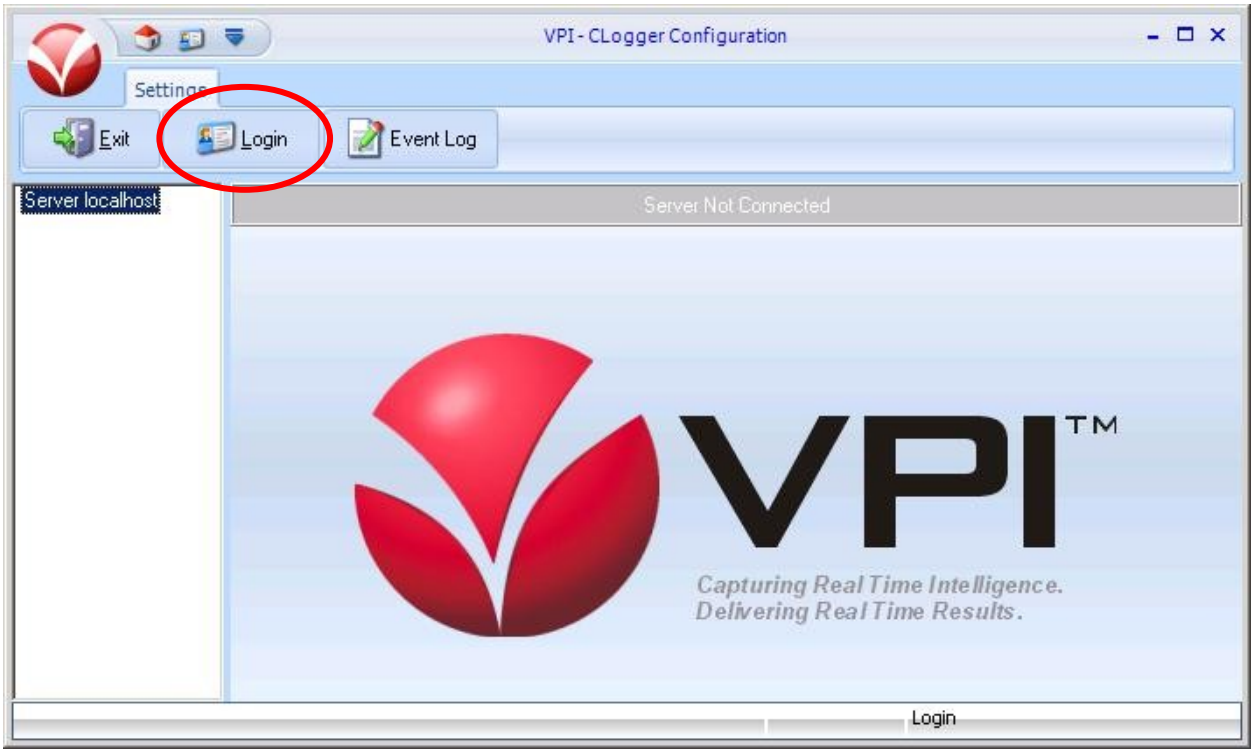
- Launch VPI Configuration
- Administer start/stop events
- Administer TSAPI
- Administer software RTP
- Adminster DMCC
- Administer channels
- Launch Digital Call Logger

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

7.1. Launch VPI Configuration

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

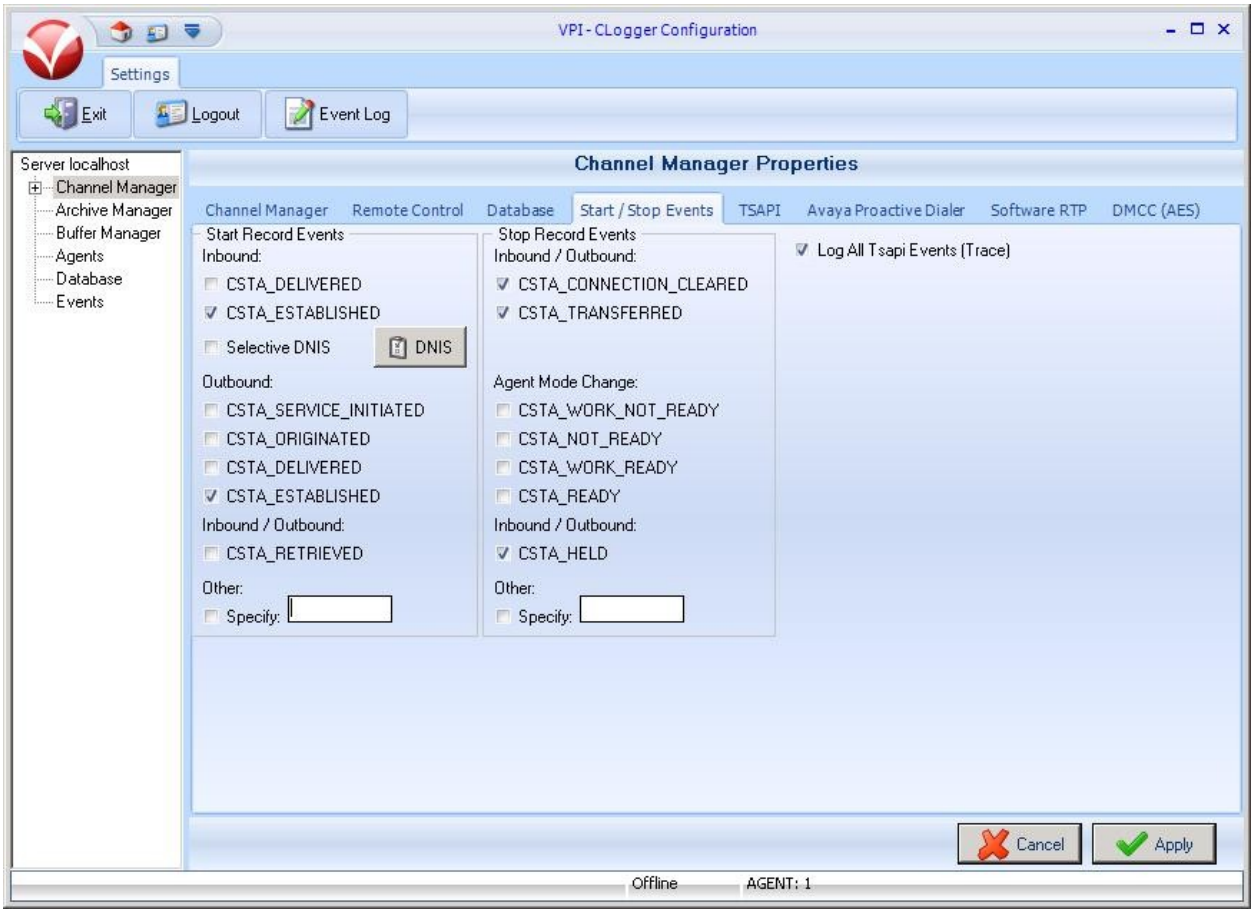
The **VPI - CLogger Configuration** screen is displayed. Click on **Login**, as shown below.



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

7.2. Administer Start/Stop Events

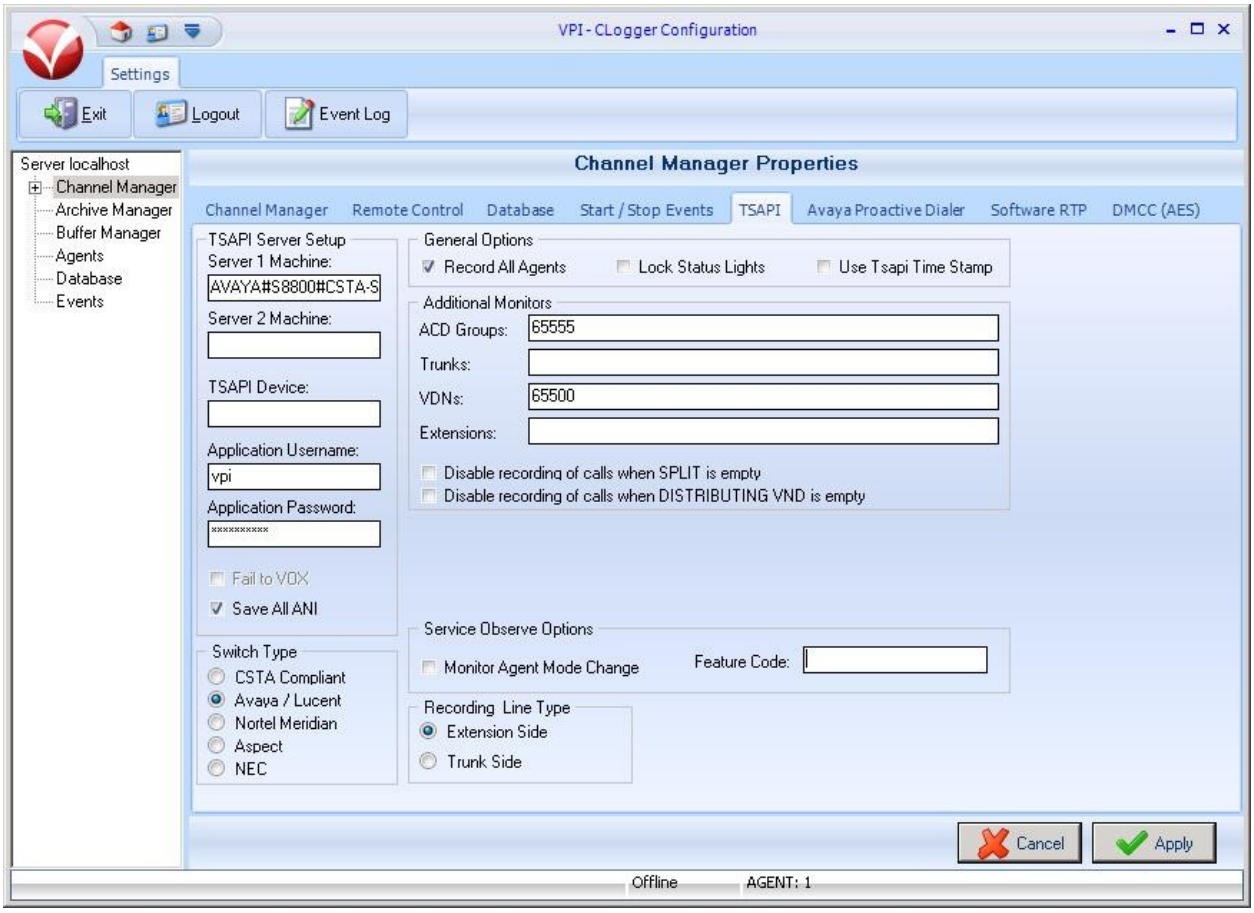
Select the **Start / Stop Events** tab in the right pane. Check the desired events to trigger the start and stop of call recordings. The screen below shows the selections used for the compliance testing. The **Log All Tsapi Events (Trace)** field was checked in the compliance testing for event verification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



7.3. Administer TSAPI

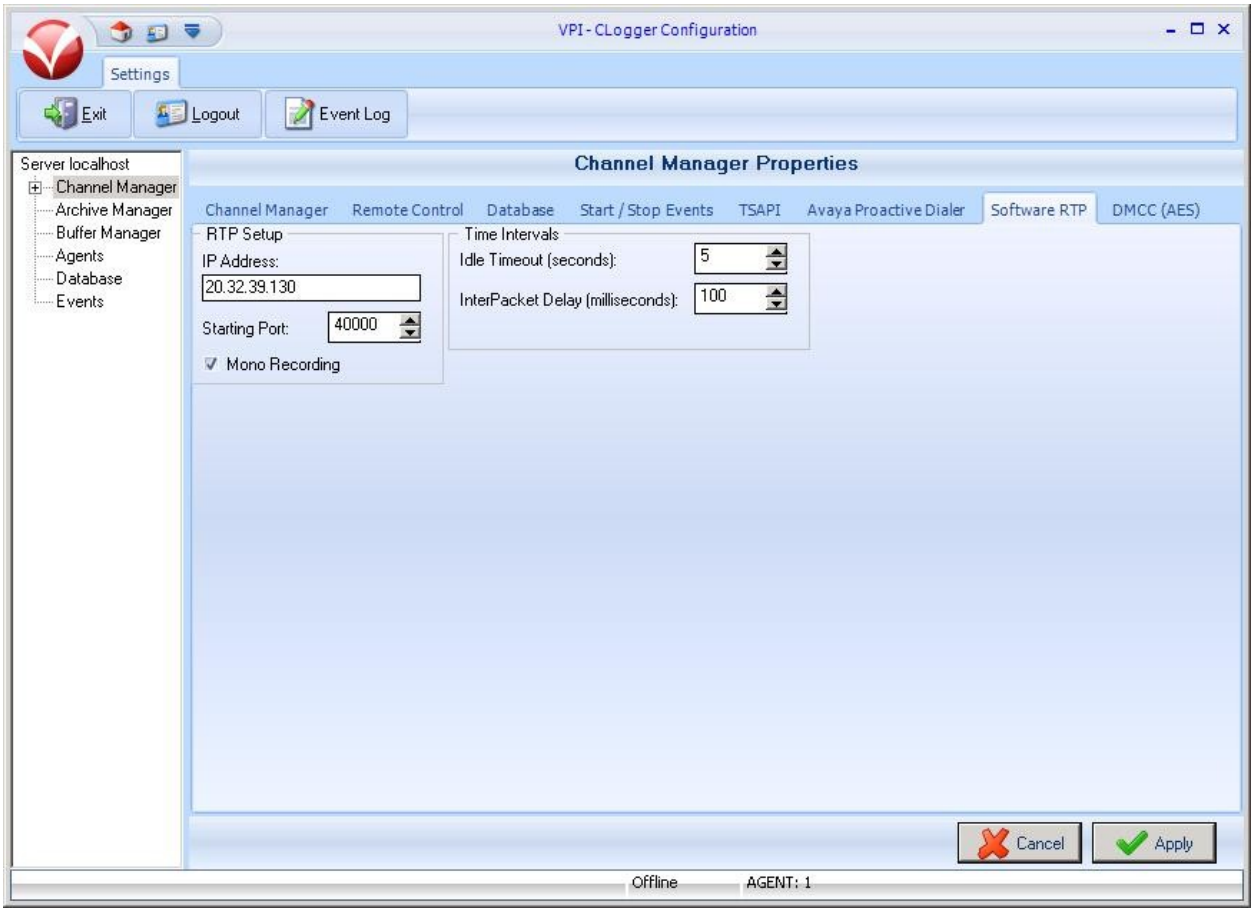
The **VPI - CLogger Configuration** screen is displayed again. Select **Server localhost > Channel Manager** in the left pane, to display the **Channel Manager Properties** screen. Select the **TSAPI** tab in the right pane. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Apply**.

- **Server 1 Machine:** The Tlink name from **Section 6.7**.
- **Application Username:** The VPI user credentials from **Section 6.8**.
- **Application Password:** The VPI user credentials from **Section 6.8**.
- **Switch Type:** "Avaya / Lucent"
- **ACD Groups:** The group extensions to be monitored from **Section 3**.
- **VDNs:** The VDN extensions to be monitored from **Section 3**.



7.4. Administer Software RTP

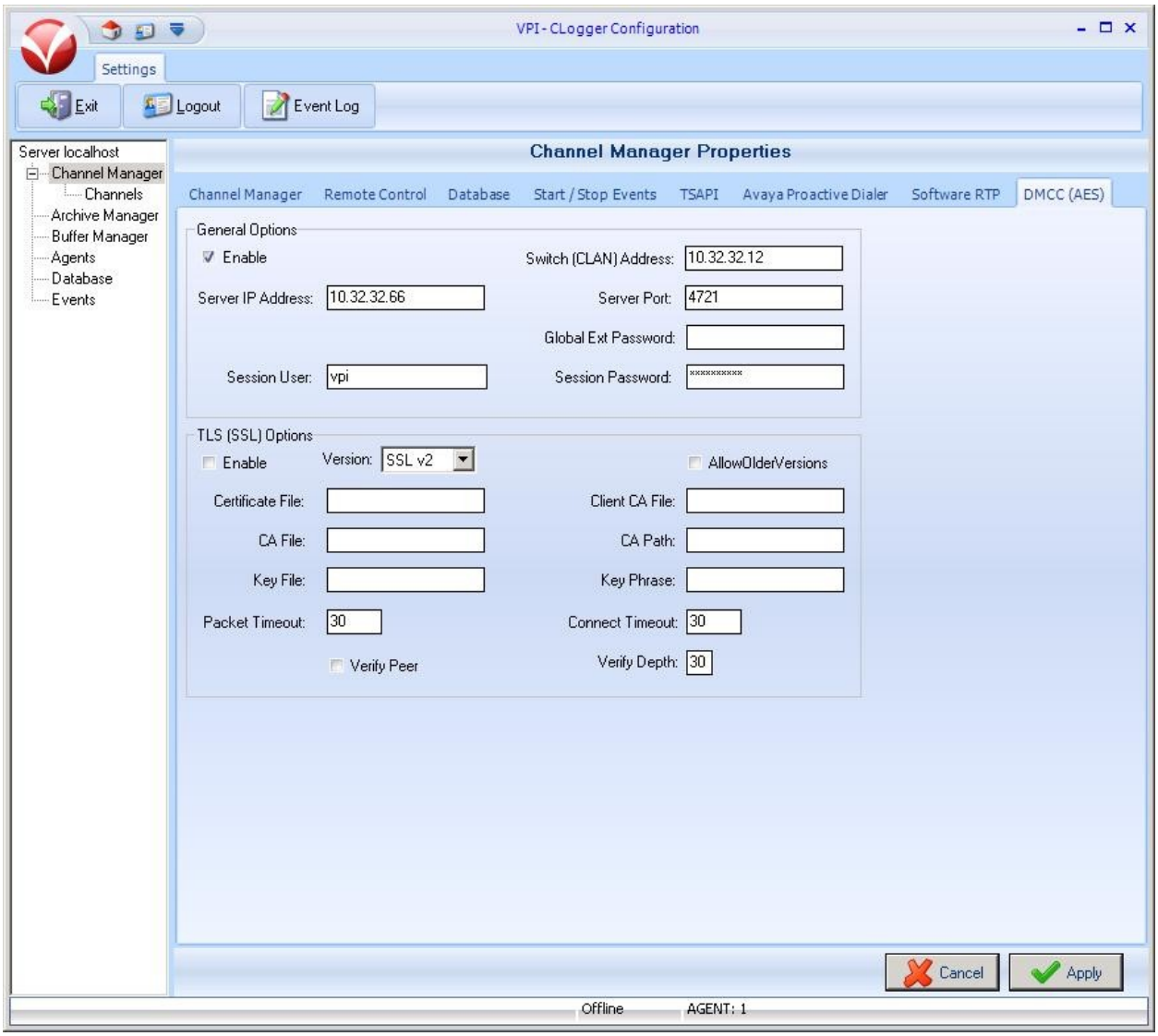
Select the **Software RTP** tab in the right pane. For **IP Address**, enter the IP address of the Voice Capture server, in this case "20.32.39.130". Retain the default values in the remaining fields, and click **Apply**.



7.5. Administer DMCC

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

- **Enable:** Check this field.
- **Server IP Address:** IP address of the Application Enablement Services server.
- **Session User:** The VPI user credentials from **Section 6.8**.
- **Switch (CLAN) Address:** IP address of the H.323 gatekeeper from **Section 6.4**.
- **Session Password:** The VPI user credentials from **Section 6.8**.

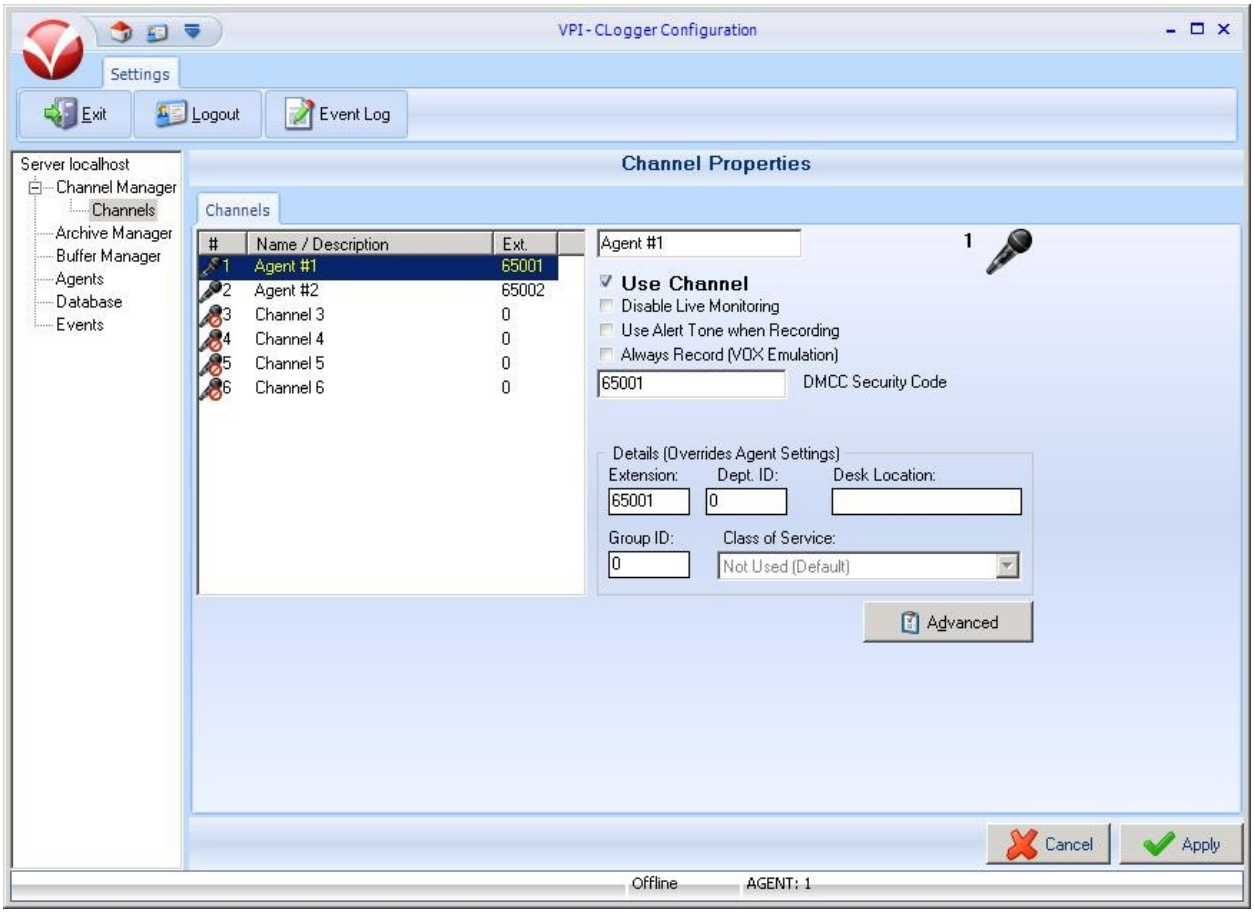


7.6. Administer Channels

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

- **Name / Description:** A desired name for the station to be monitored.
- **Use Channel:** Check this field.
- **DMCC Security Code:** The agent station security code from **Section 5.4**.
- **Extension:** The agent station extension from **Section 5.4**.

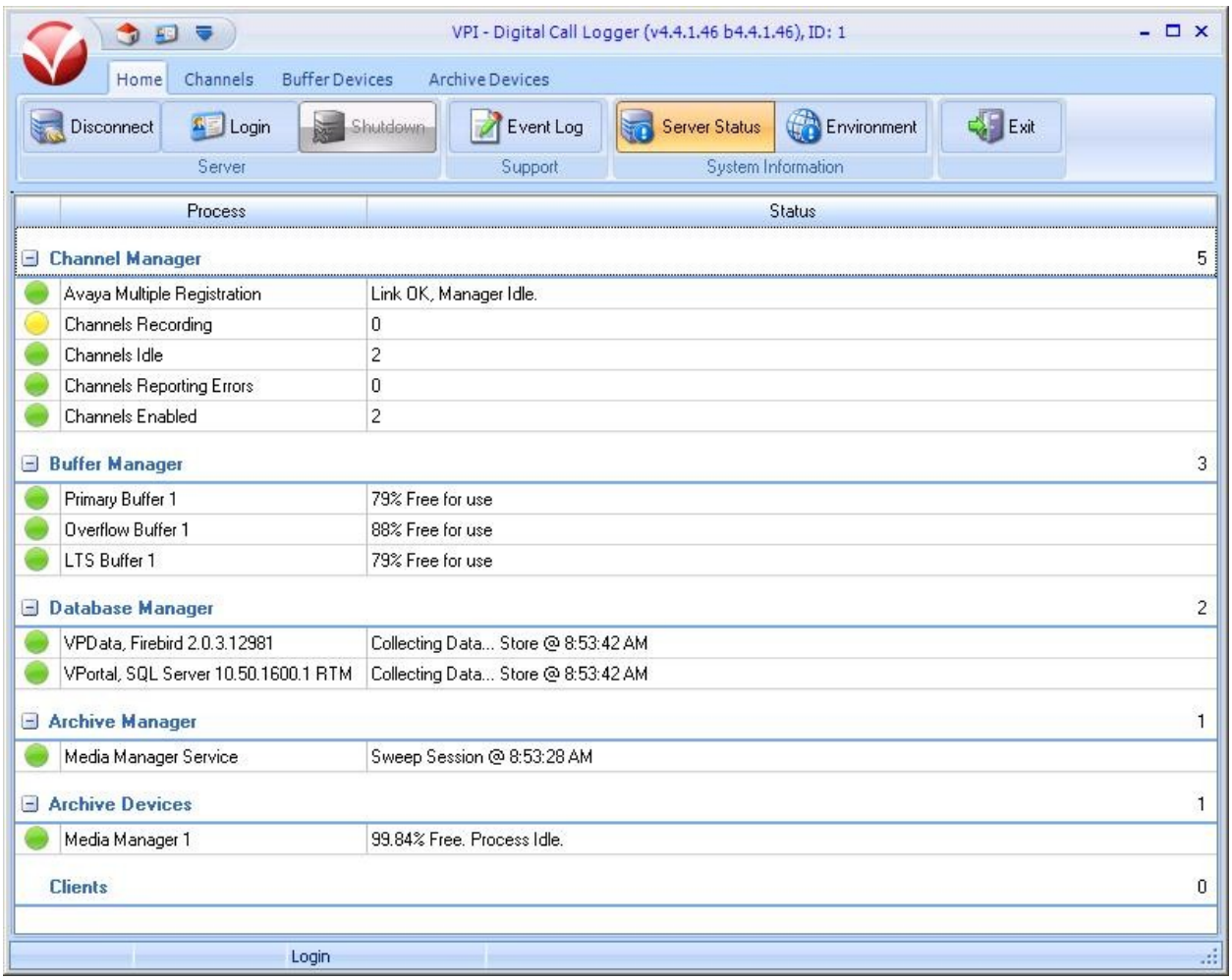
Repeat this section to administer a channel for each agent station to be monitored from **Section 5.4**, and click **Apply**.



7.7. Launch Digital Call Logger

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

The **VPI – Digital Call Logger** screen is displayed. Select **Server Status** from the top portion of the screen. In the **Channel Manager** section, verify that the **Channels Recording** entry has the yellow status, and that all other entries have the green status, as shown below.



8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     4        no    AES2-S8800       established   103      32
```

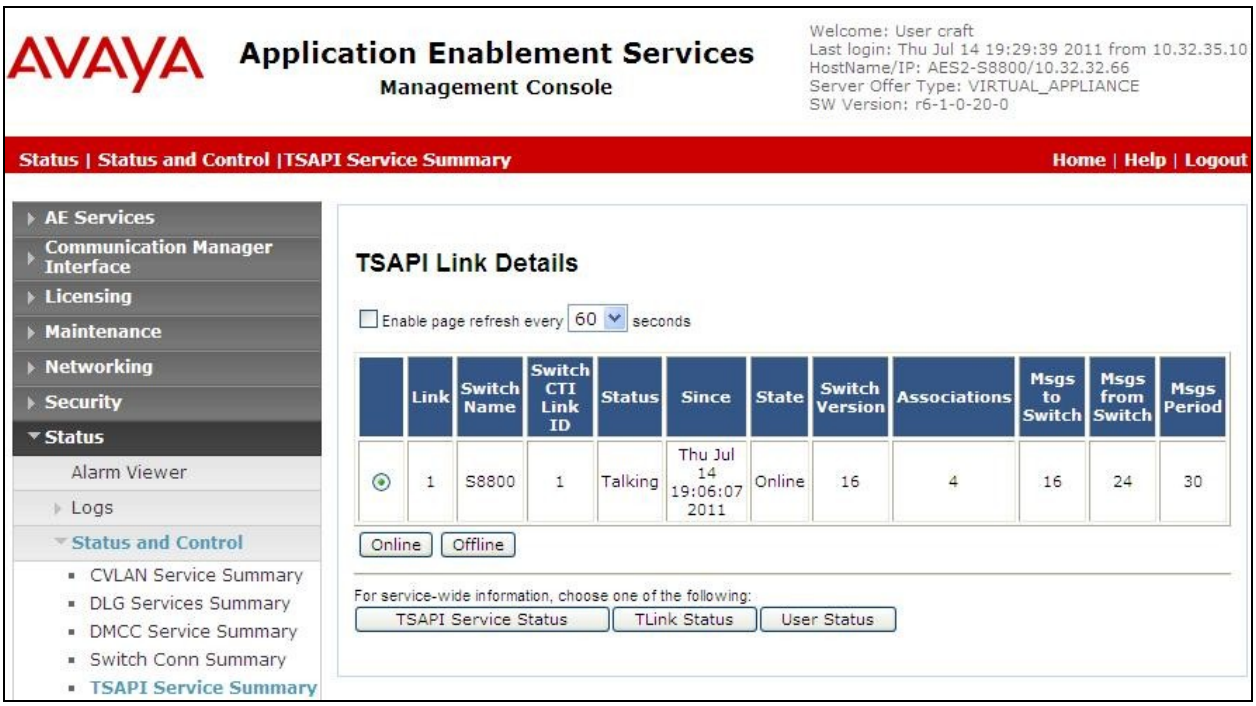
Verify the registration status of the recording devices by using the "list registered-ip-stations" command. Verify that there is an entry for each recording channel from **Section 7.6**, with the client IP address of Avaya Aura® AES as **Station IP Address**, as shown below.

```
list registered-ip-stations

                             REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ----------------------------------------
65001         1608      IP_Phone    y  20.32.39.105
              1         1.3000         10.32.32.12
65001         1608      IP_API_A    y  10.32.32.66
              1         3.2040         10.32.32.12
65002         9650      IP_Phone    y  20.32.39.108
              1         3.1000         10.32.32.12
65002         9650      IP_API_A    y  10.32.32.66
              1         3.2040         10.32.32.12
```

8.2. Verify Avaya Aura® Application Enablement Services

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

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



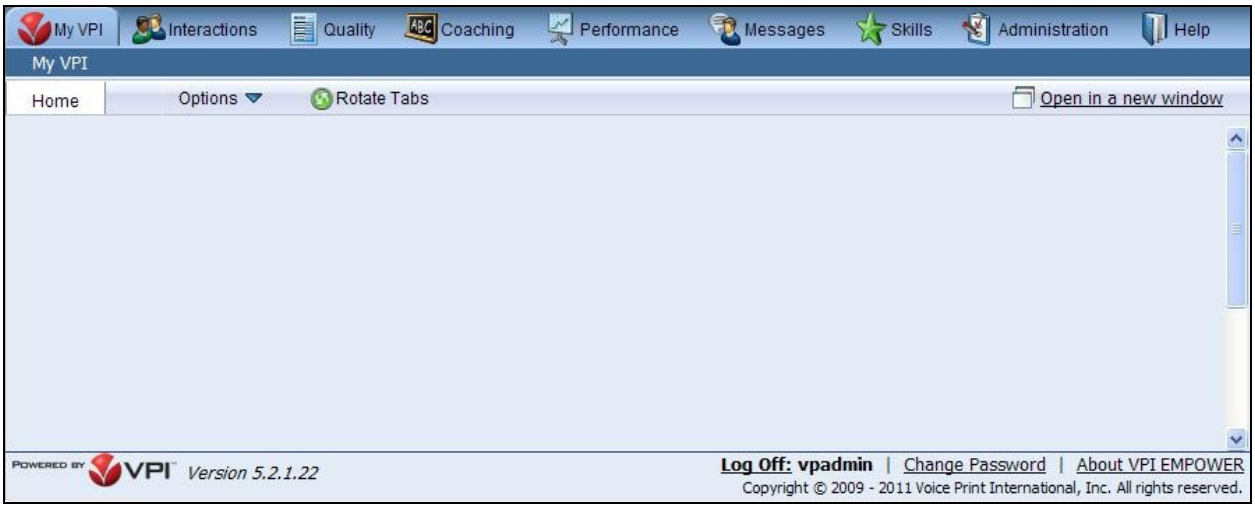
Verify the status of the DMCC link by selecting **Status > Status and Control > DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

In the lower portion of the screen, verify that the **User** column shows an active session with the VPI user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of recording devices/channels from **Section 7.6**.

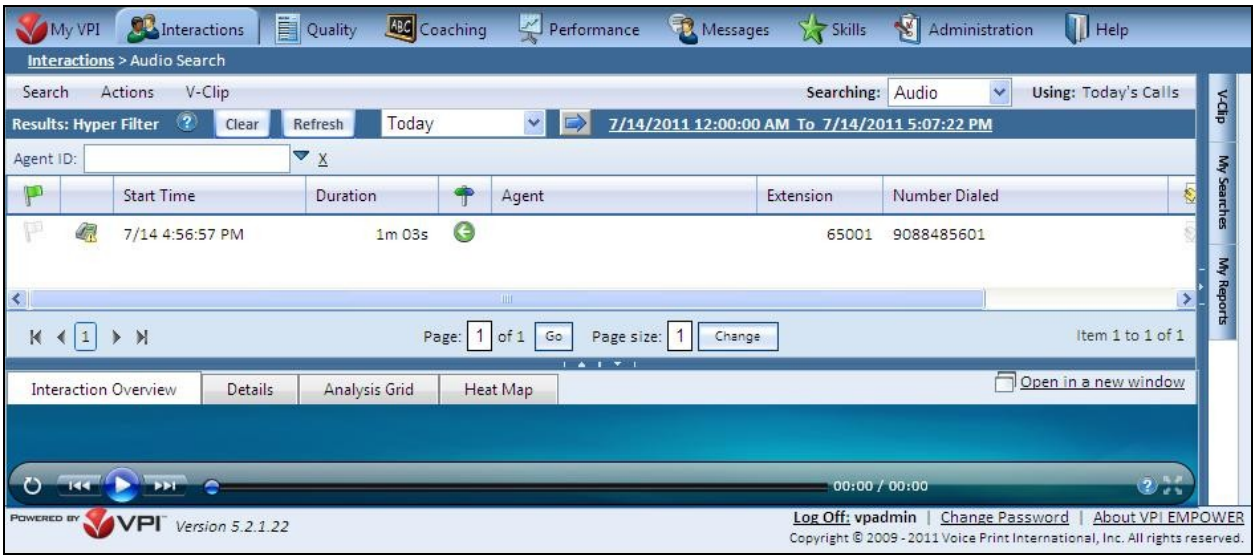
8.3. Verify VPI Voice Capture

Log an agent in to the skill group to handle and complete an ACD call. Access the Voice Capture web-based interface by using the URL "https://ip-address/VPortal" in an Internet browser window, where "ip-address" is the IP address of the Voice Capture server. Log in using the appropriate credentials.

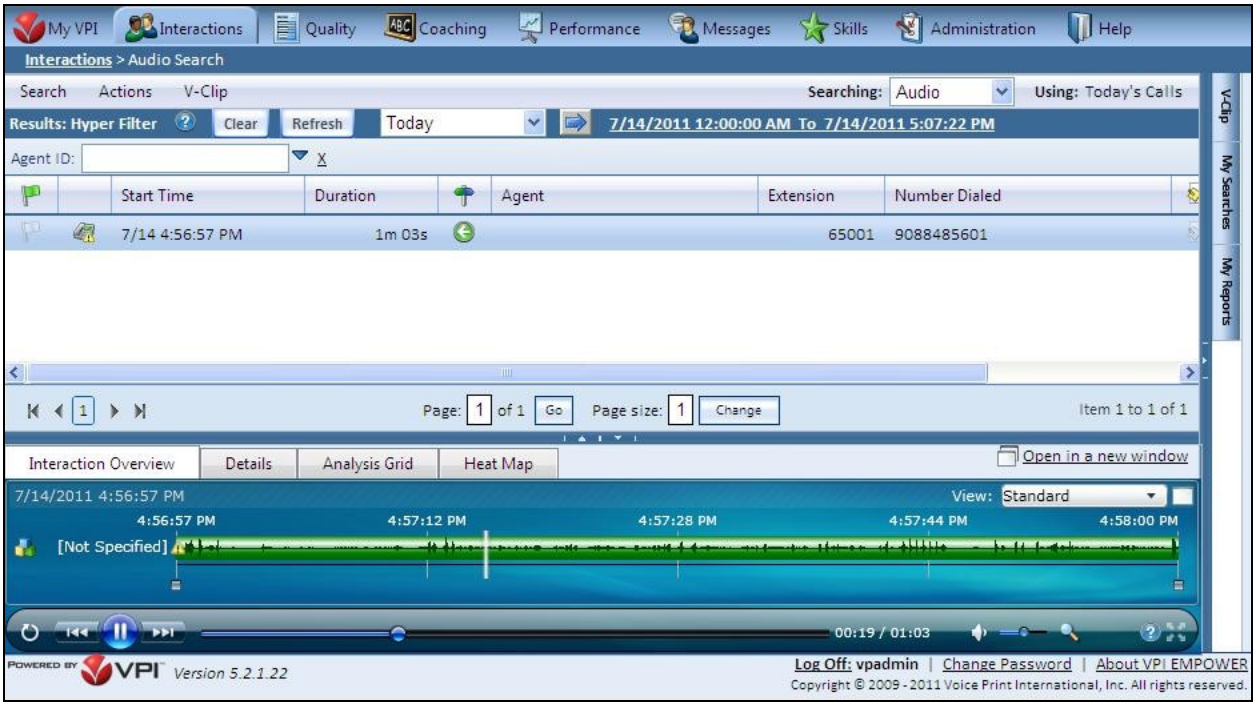
The screen below is displayed next. Select **Interactions > Audio Search** from the top menu.



The screen is updated with a list of the call recordings. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.



Double click on the entry to listen to the playback. Verify that the screen is updated and that the call recording is played back.



9. Conclusion

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

10. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011, available at http://support.avaya.com.

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

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.