Avaya Solution & Interoperability Test Lab

Application Notes for Envision Centricity with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Envision Centricity to monitor and record calls placed to and from stations through a trunk on Avaya Communication Manager.

Envision Centricity is a trunk tap recording solution. The system interfaces with Avaya Communication Manager through the Avaya AES Server, using TSAPI to associate recordings with important CTI information like agent ID and user data.

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 a compliance tested configuration comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) server, and Envision Centricity.

Envision Centricity monitors a trunk, records, stores, and plays back phone calls for verification. Envision Centricity interfaces with the Avaya AES Server, using TSAPI to obtain call control events. The Envision Centricity recording solution supports two recording methods, DMCC w/ TSAPI and Trunk Tap w/ TSAPI. During the compliance test, the Trunk Tap w/ TSAPI solution was tested. The Ai-Logix board, used for recording, was tapped into a T1 ISDN-PRI trunk line.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide an IP trunk between two Avaya Communication Manager systems.

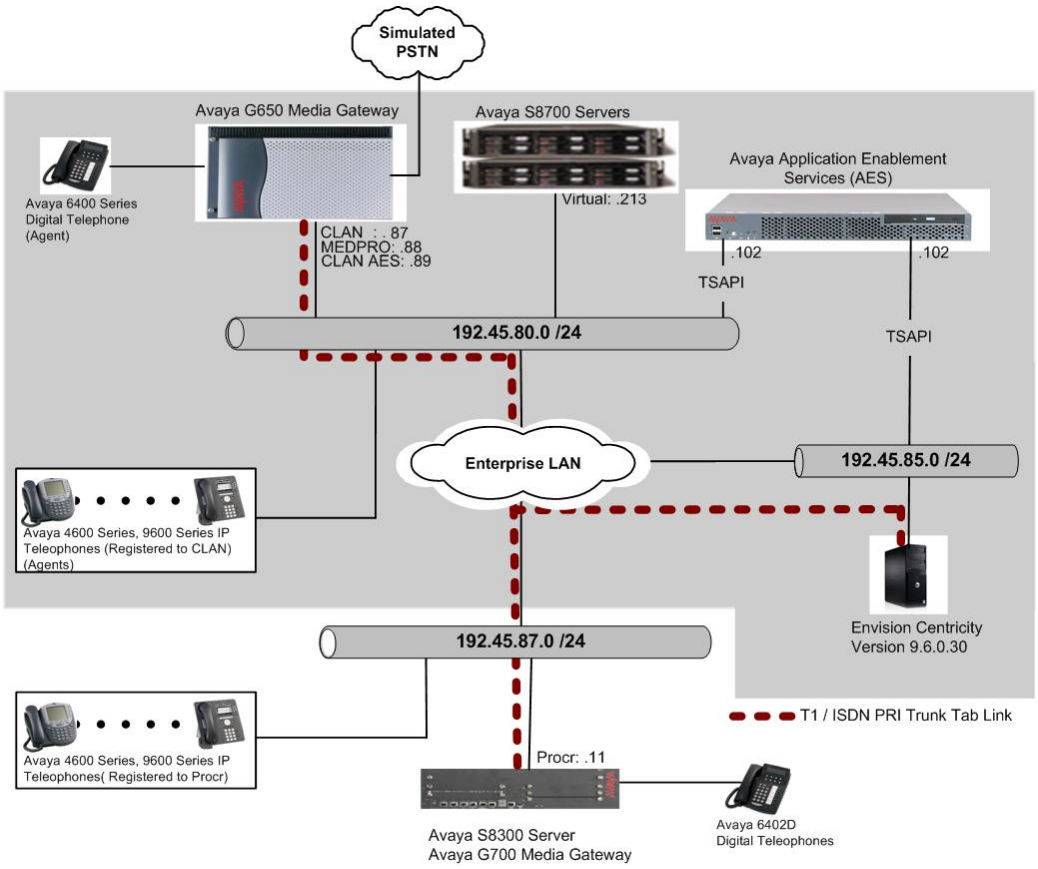


Figure 1: Sample Test Configuration for the Envision Centricity Solution

2. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Servers		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface TN799DP C-LAN Interface TN2302AP IP Media Processor	HW11 FW044 HW01 FW028 HW20 FW118
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya Application Enablement Services Server		4.2 (R4.2.0.19.4)
Avaya 4600 Series IP Telephones		
	4620SW (H.323) 4625SW (H.323)	2.8 2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323) 9650 (H.323)	1.5 1.5
Avaya 6408D+ Digital Telephone		-
Envision Centricity on Microsoft Windows 2003 Server with Service Pack 2		Version 9 (R9.6.0.30)

3. Configure Avaya Communication Manager

This section provides the procedures for configuring an ip-codec-set and ip-network region, a switch connection and Computer Telephony Integration (CTI) links, and recorded stations on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

3.1. System-Parameters Customer-Options for TSAPI

Enter the **display system-parameters customer-options** command. On **Page 3**, verify that the Computer Telephony Adjunct Links field is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.

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

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

3.2. Codec Configuration

Enter the **change ip-codec-set t** command, where **t** is a number between 1 and 7, inclusive.

```
change ip-codec-set 1                                         Page   1 of   2

                         IP Codec Set
   Codec Set: 1

   Audio         Silence      Frames   Packet
   Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2:
```

3.3. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. Avaya IP telephones and an IP agent, used by Envision Centricity, registered with the C-LAN board and were thus also assigned to IP network region 1. The second C-LAN board (CLAN-AES), which is dedicated for the AES server, was assigned to network region 2. The following screen shows only network region 1.

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3929
DIFFSERV/TOS PARAMETERS                RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 0
        Audio 802.1p Priority: 0
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
```

3.4. Configure Switch Connection and CTI Links between Avaya Communication Manager and Avaya Application Enablement Services

The Avaya AES server forwards CTI requests, responses, and events between Envision Centricity and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over a switch connection link. Within the switch connection link, CTI links may be configured to provide CTI services to CTI applications such as Envision Centricity. The following steps demonstrate the configuration of the Avaya Communication Manager side of the switch connection and CTI links. See **Section 4** for the details of configuring the AES side of the switch connection and CTI links.

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to **ADJ-IP**, and assign a descriptive Name to the CTI link.

```
add cti-link 4                                                Page   1 of   2
                                  CTI LINK
 CTI Link: 4
Extension: 20006
     Type: ADJ-IP
                                                                  COR: 1
     Name: TSAPI
```

Enter the **change node-names ip** command. In the compliance tested configuration, the CLAN IP address was used for registering H.323 endpoints (Avaya IP Telephones, and IP Softphones, and AES Device, Media and Call Control API stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
CLAN                   192.45.80.87
CLAN-AES               192.45.80.89
MEDPRO                 192.45.80.88
MEDPRO2                192.45.80.161
S8300G700              192.45.87.11
default                0.0.0.0
procr                  192.45.80.214
```

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was used for the Local Port field.

```
change ip-services                                            Page   1 of   4

                                  IP SERVICES
 Service      Enabled      Local        Local       Remote      Remote
  Type                     Node         Port        Node        Port
AESVCS         y       CLAN-AES         8765
```

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname –a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 4.1**.

```
change ip-services                                            Page   4 of   4
                           AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       server2             xxxxxxxxxxxxxxxx      y        idle
      2:
```

3.5. Recorded Stations

During the compliance test, the following recorded stations were created.

- 22001 (Avaya 4620SW IP)
- 22002 (Avaya 4625SW IP)
- 22003 (Avaya 9630 IP)
- 22007 (Avaya 6408D+)
- 22009 (Avaya IP Agent)

4. Configure Avaya Application Enablement Services

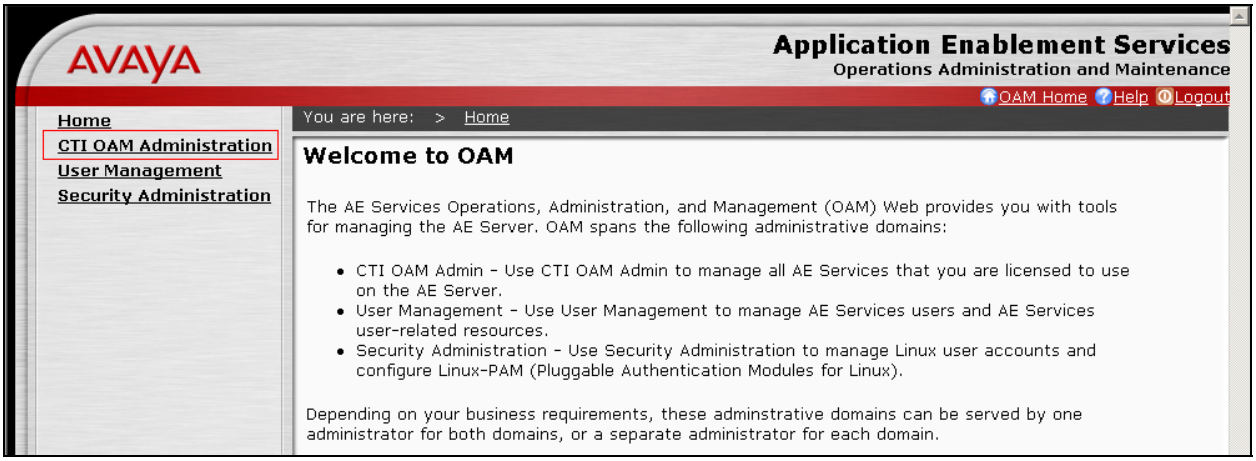
The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a DMCC Server port, and creating a CTI link for TSAPI.

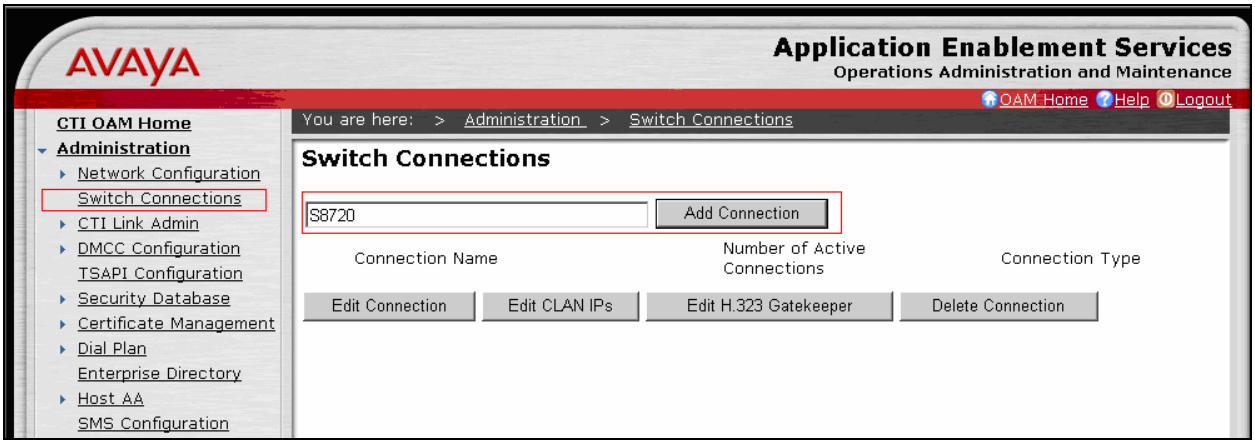
4.1. Configure Switch Connection

Launch a web browser, enter http://<IP address of AES server> in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

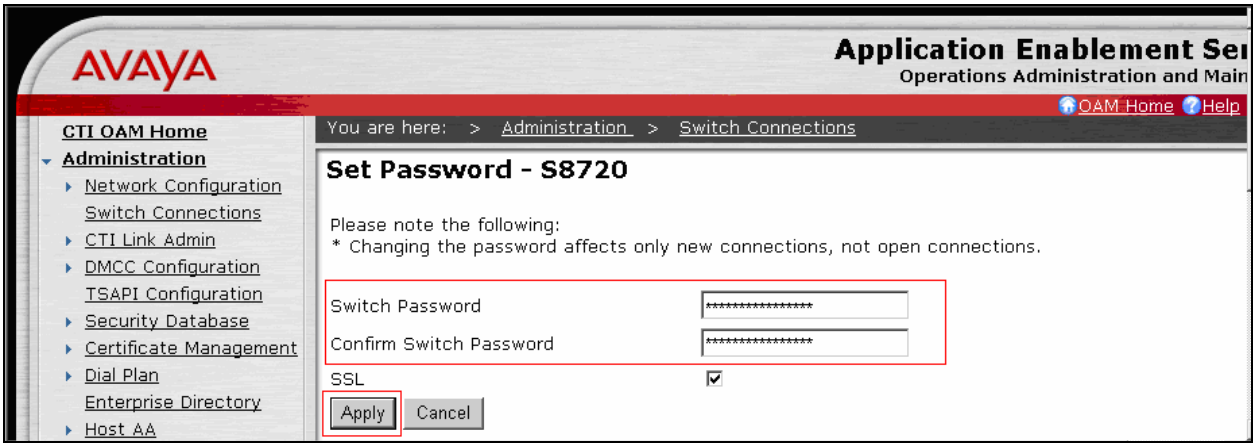
Select the **CTI OAM Administration** link from the left pane of the screen.



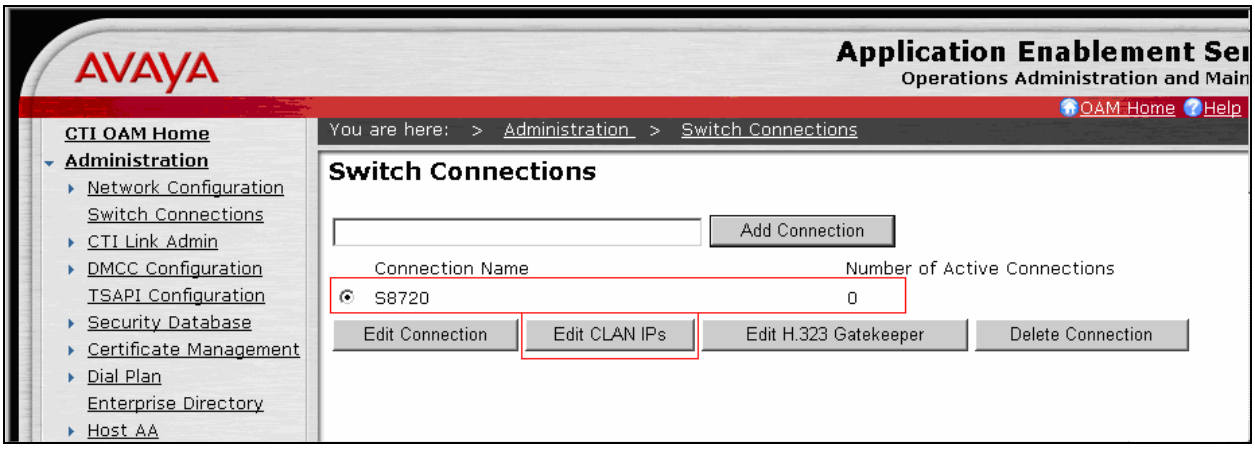
Click on **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



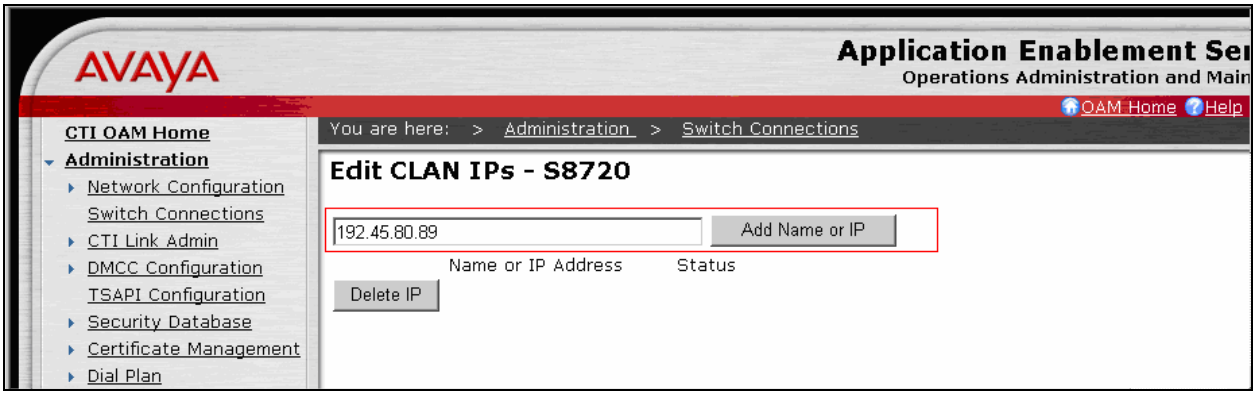
The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 3.4**. Click on **Apply**.



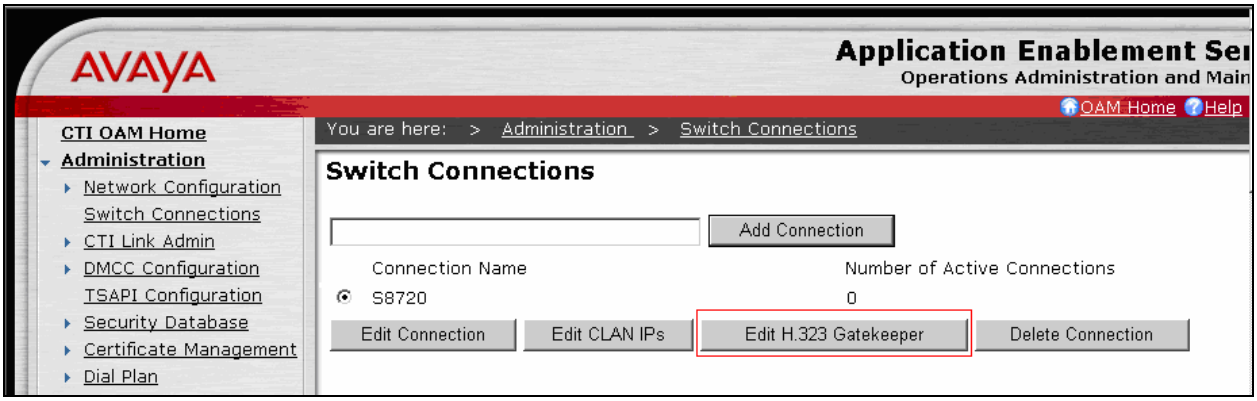
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.



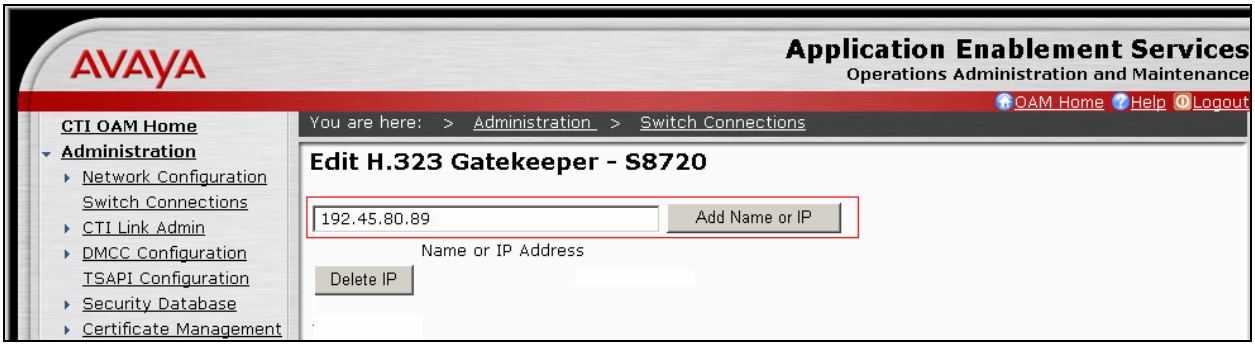
Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 3.4** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



After the completion, navigate back to **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. Click on **Edit H.323 Gatekeeper** for DMCC call control and monitor.

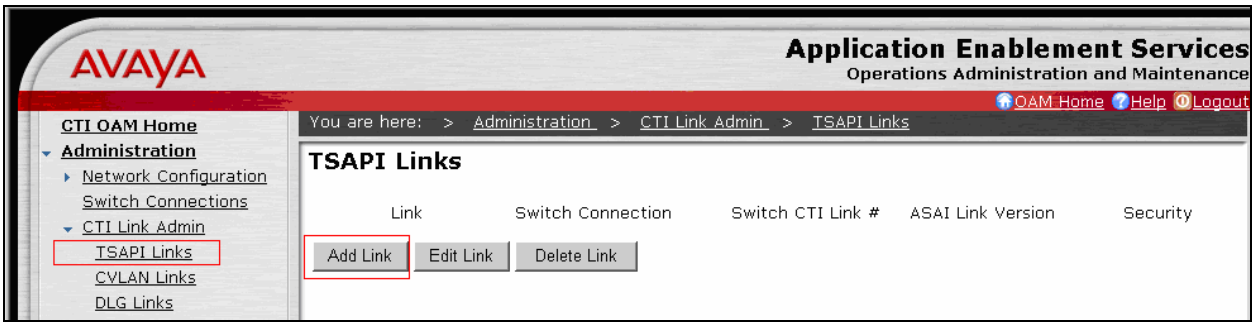


On the **Edit H.323 Gatekeeper – S8720** page, enter the C-LAN IP address which will be used for the DMCC service. During the compliance test, CLAN-AES was used for the DMCC service. Click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

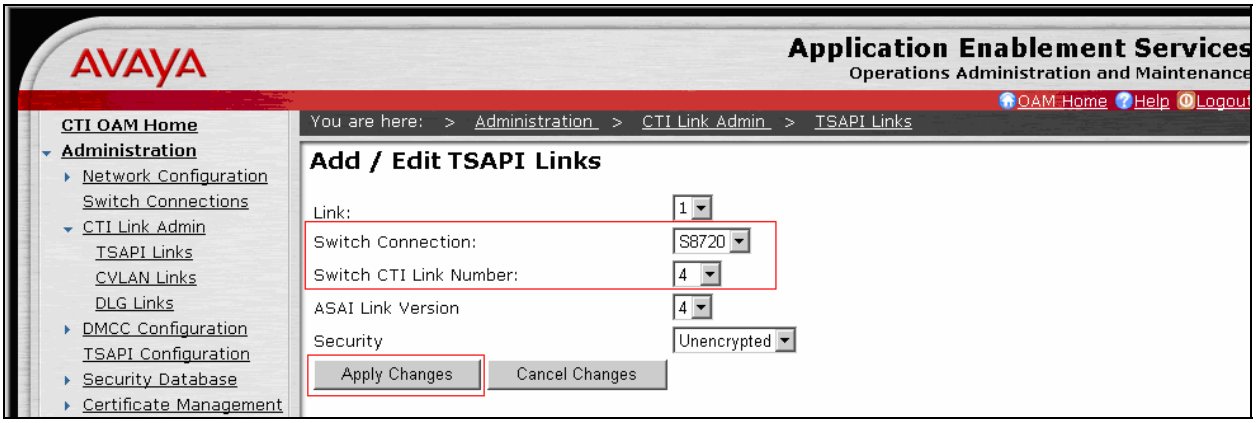


4.2. Configure the TSAPI CTI link

Navigate to **Administration → CTI Link Admin → TSAPI Links** in the left pane, and click on the **Add Link** button to create a TSAPI CTI link.

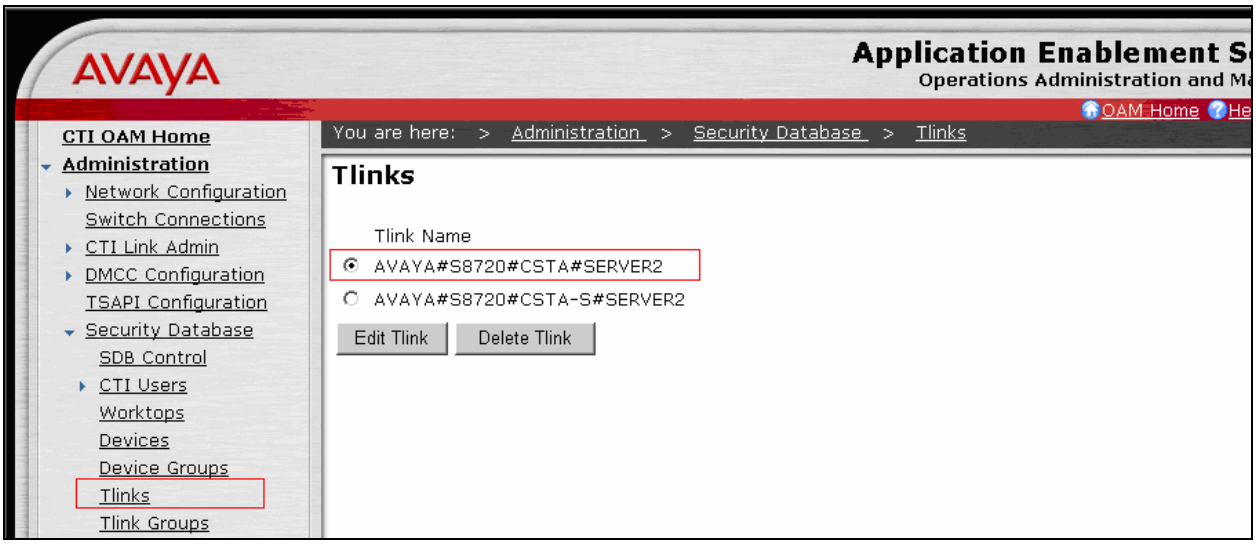


Select a Switch Connection using the drop down menu. The Switch Connection is configured in **Section 4.1**. Select the Switch CTI Link Number using the drop down menu. Switch CTI Link Number should match with the number configured in the cti-link form in **Section 3.4**. Click the **Apply Changes** button. Default values may be used in the remaining fields.



4.3. Configure Tlink

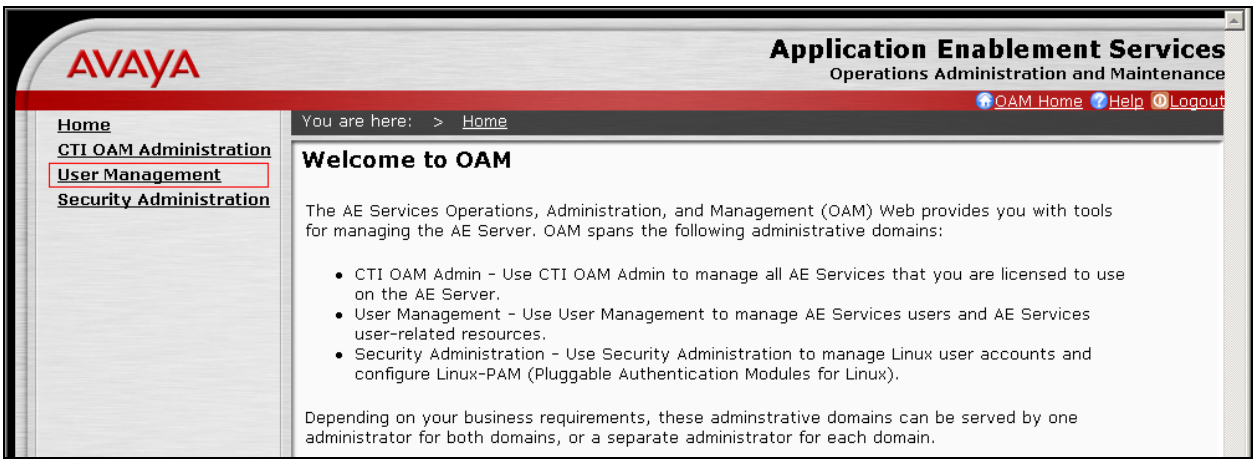
Navigate to **Administration → Security Database → CTI Users → Tlinks**. The Tlink doesn't need to be created manually. The Tlink should be created automatically, once the TSAPI CTI link is created. This section just illustrates how to obtain a Tlink in the AES CTI OAM Home page. The Tlink parameter will be used by the DevConnect member solution.



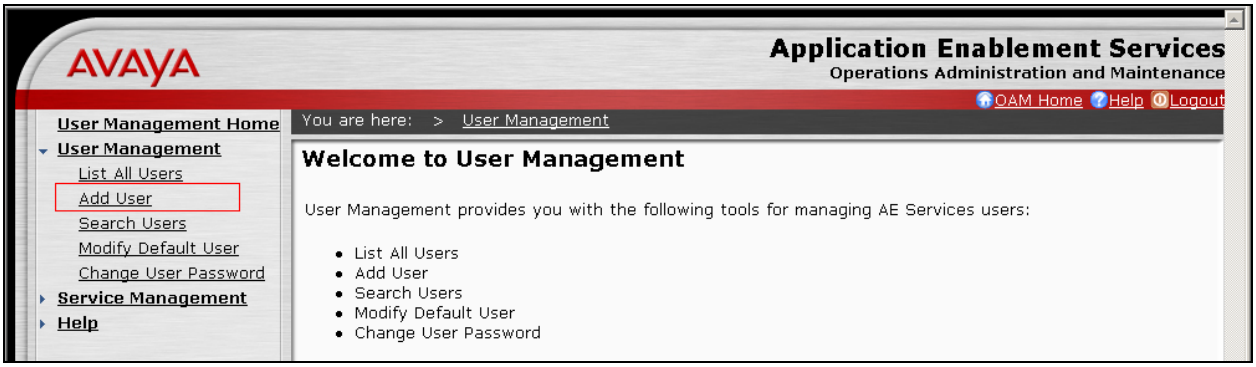
4.4. Configure the CTI Users

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter http://<IP address of AES server> in the URL, and log in with the appropriate credentials to access the relevant administration pages.

The Welcome to OAM page is displayed next. Select **User Management** from the left pane.



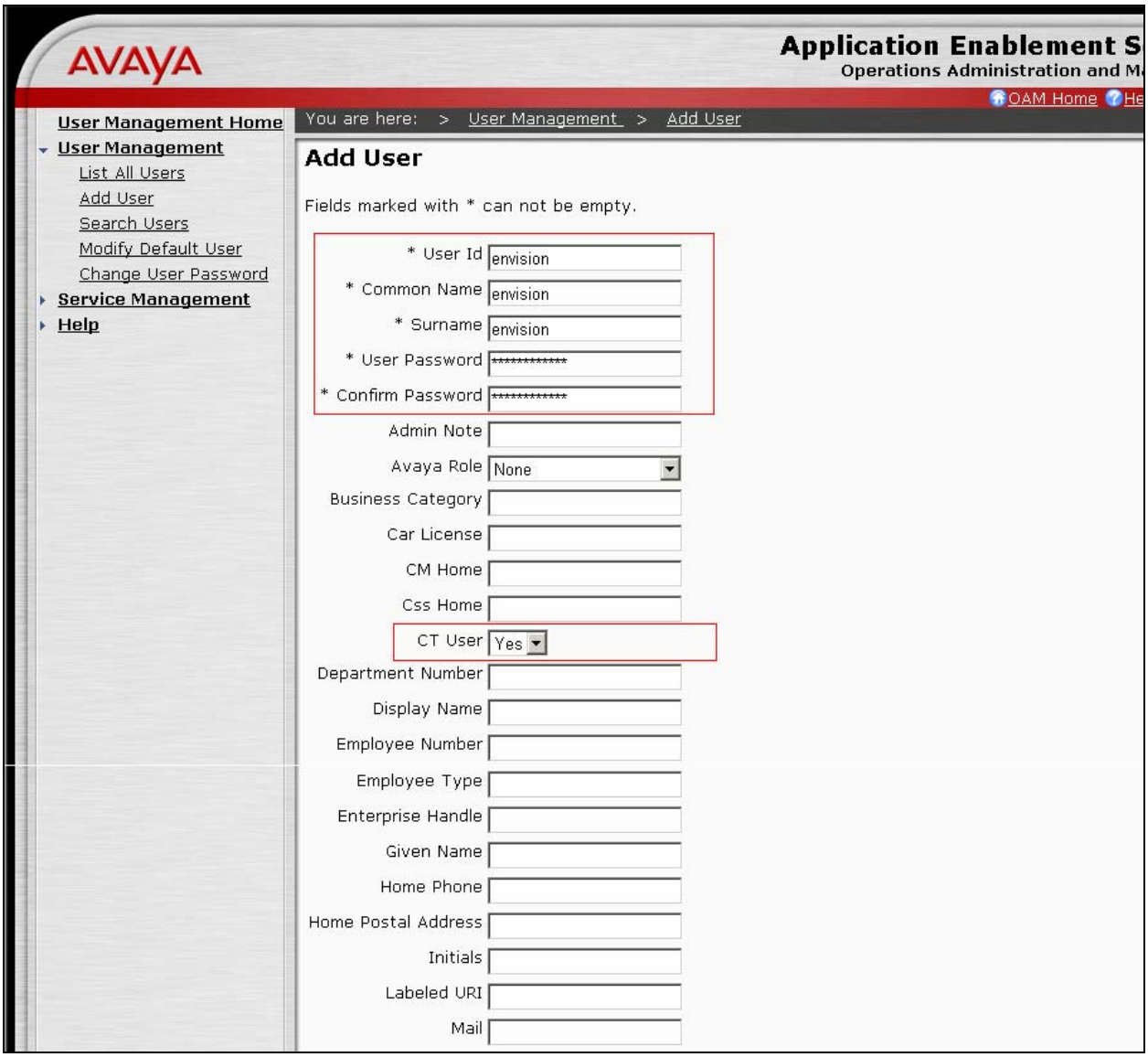
From the Welcome to User Management page, navigate to the **User Management → Add User** page to add a CTI user.



On the Add User page, provide the following information:

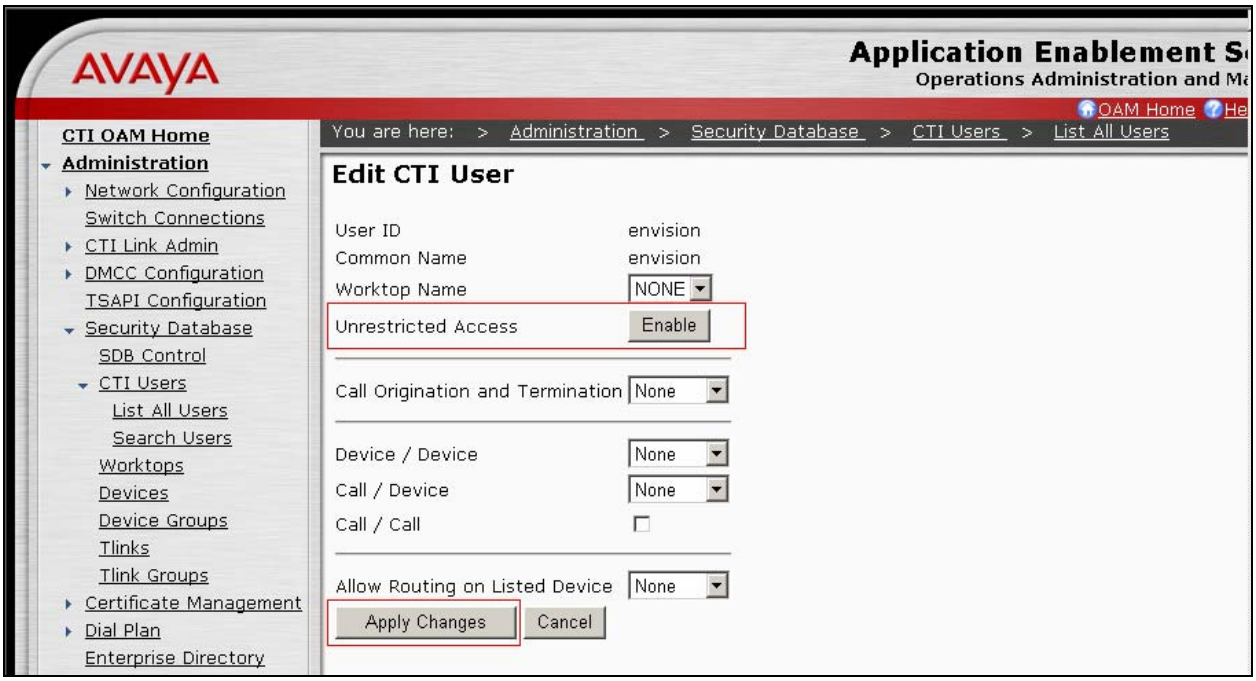
- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the Envision Centricity Configuration page in **Section 5**. Select **Yes** using the drop-down menu on the CT User field. This enables the user as a CTI user. Click the **Apply** button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.



Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Administration → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.

Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.

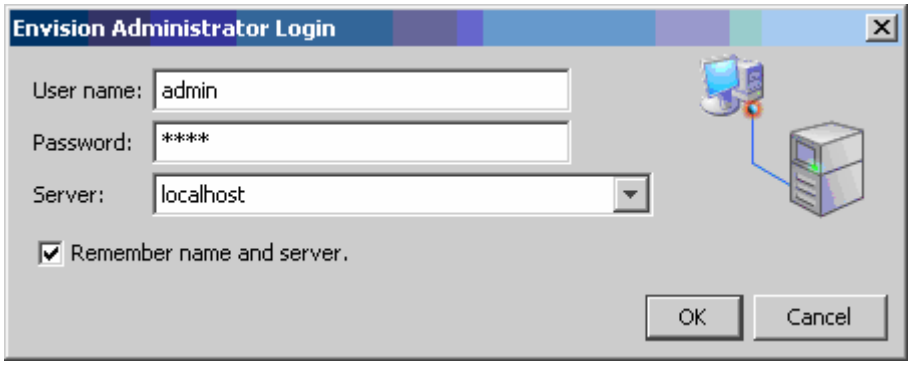


5. Configure Envision Centricity

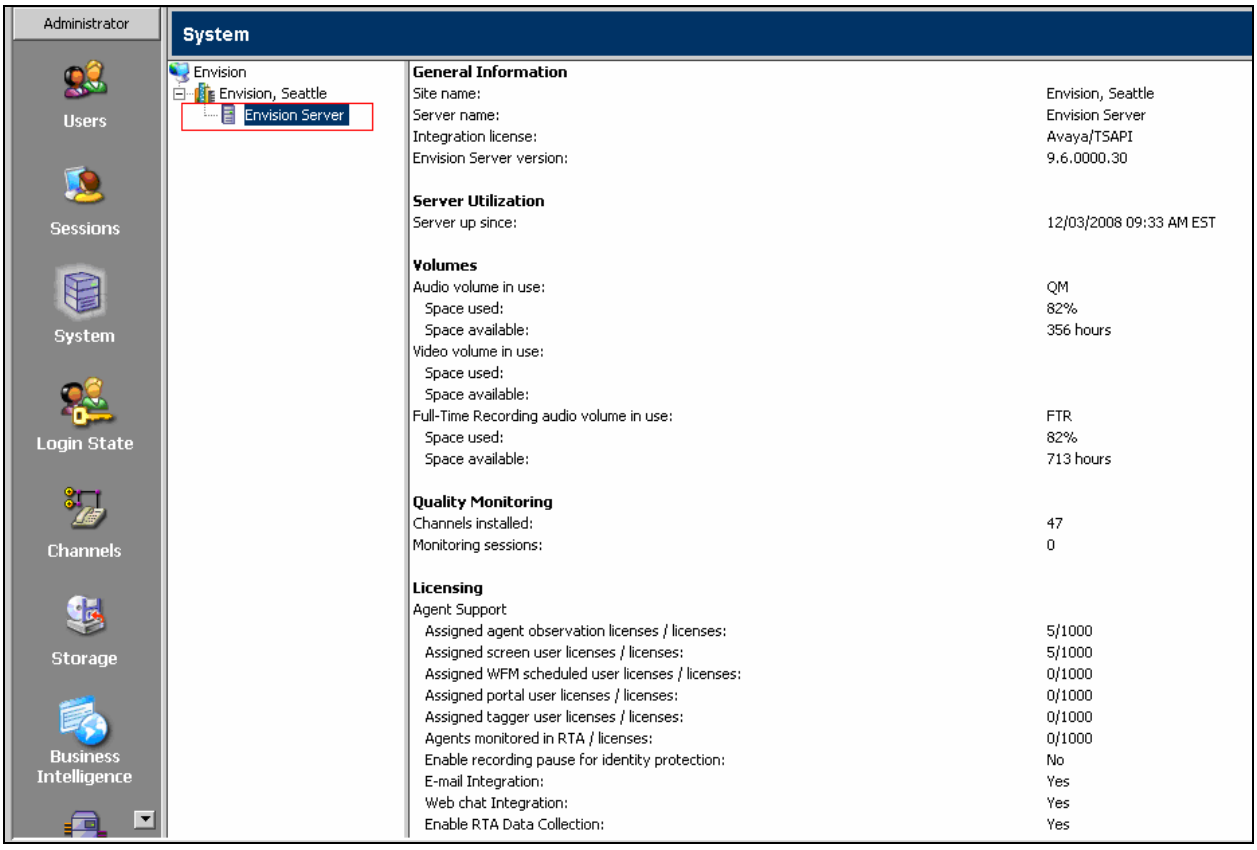
This section only describes the interface configuration for the Envision Centricity application to communicate with Avaya AES and Avaya Communication Manager. The steps in this section describe the configuration of an Ai-Logix for recording, a TSAPI CTI link, extension IDs, agent IDs, and Hunt group and VDN.

5.1. Configure Ai-Logic board for recording a trunk

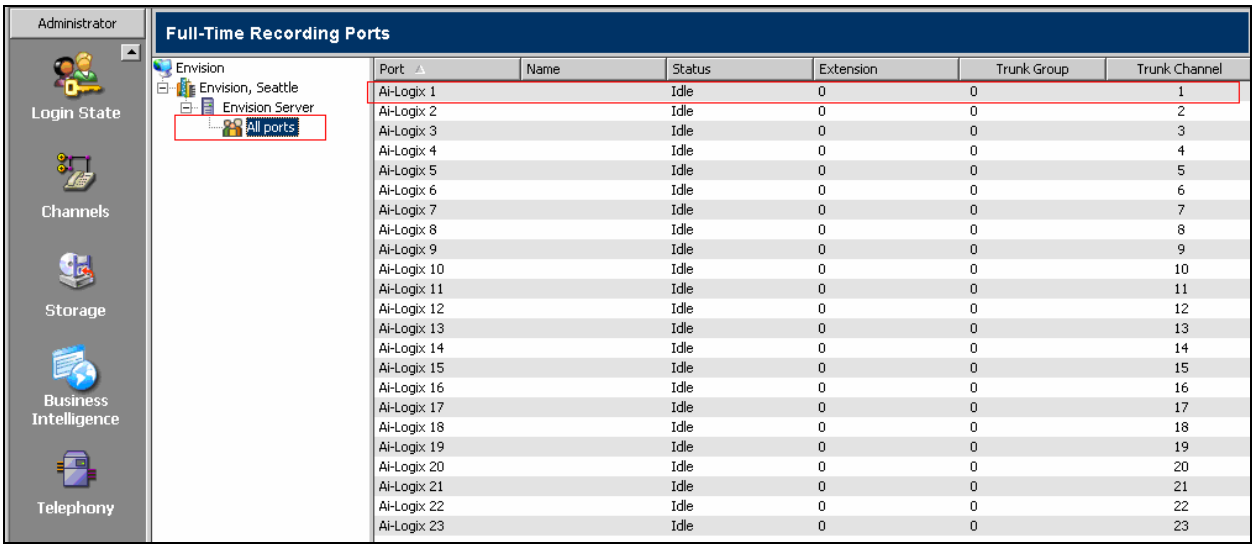
The steps in this section describe the configuration of a trunk setup on an Ai-Logic board. Open the Envision Centricity application by navigating to **Start → All Programs → Envision Telephony → Envision Performance Suite → Administrator**. Provide credentials on the Login window, and click **OK**.



On the System window, select **Envision Server** on the left pane of the window.

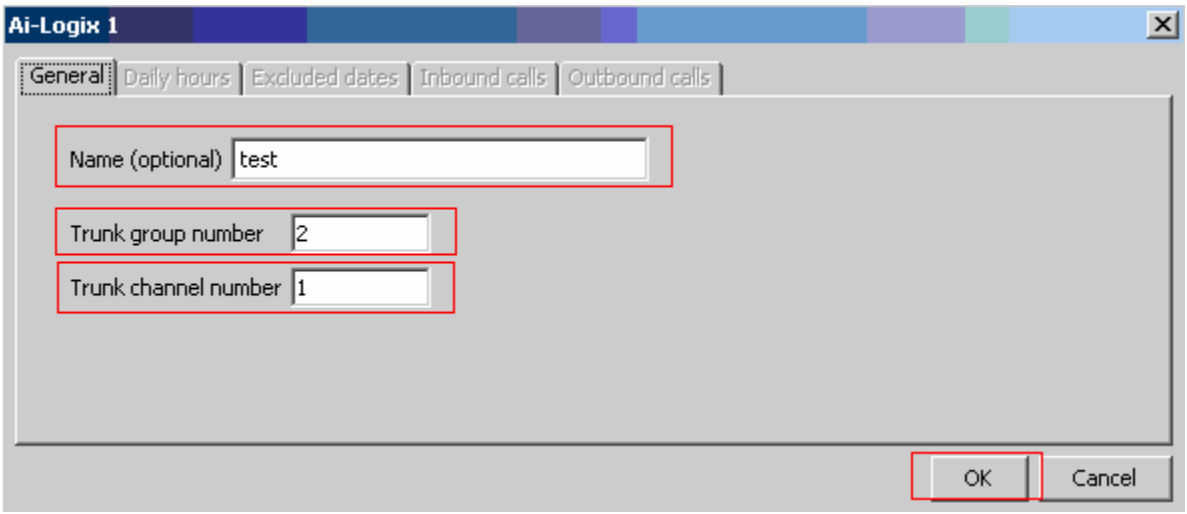


The following window describes how to configure the Ai-Logic board to start monitoring a specific trunk for recording. Click **All Ports** from the left pane of the window, and select a port, in this case Ai-Logix 1, and configure the port by clicking the right mouse button (or double click) the port.



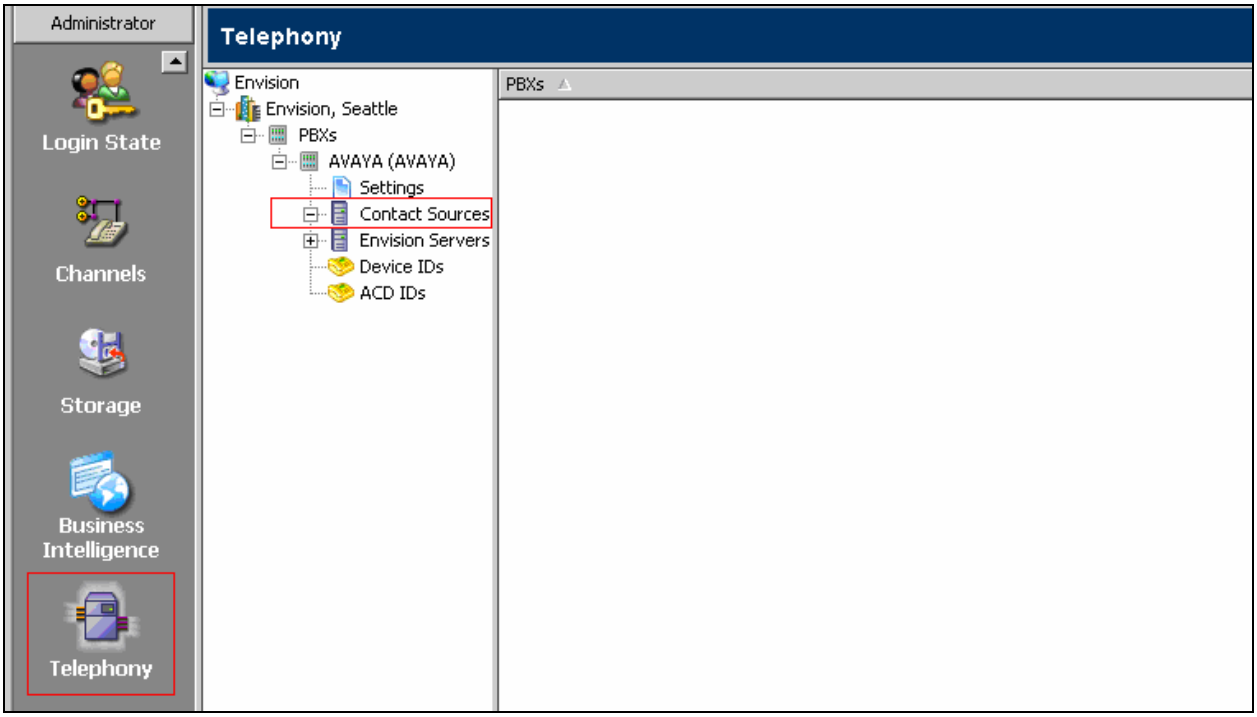
On the Ai-Logix 1 window, provide the following information:

- Name (Optional) – a descriptive name
- Trunk group number – a trunk group that will be monitored for recording.
- Trunk channel number – a trunk channel number that will listen for recording.
- Click on the **OK** button.

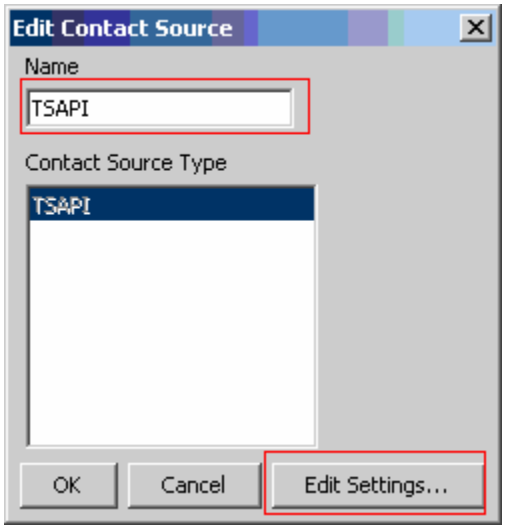


5.2. Configure Contact Sources (TSAPI link)

The steps in this section describe the configuration of a TSAPI CTI link. Click on the Telephony menu under the Administrator section, and navigate to **PBXs → AVAYA (AVAYA) → Contact Sources**. On the right pane of the window, double click to start add a Contact Source.

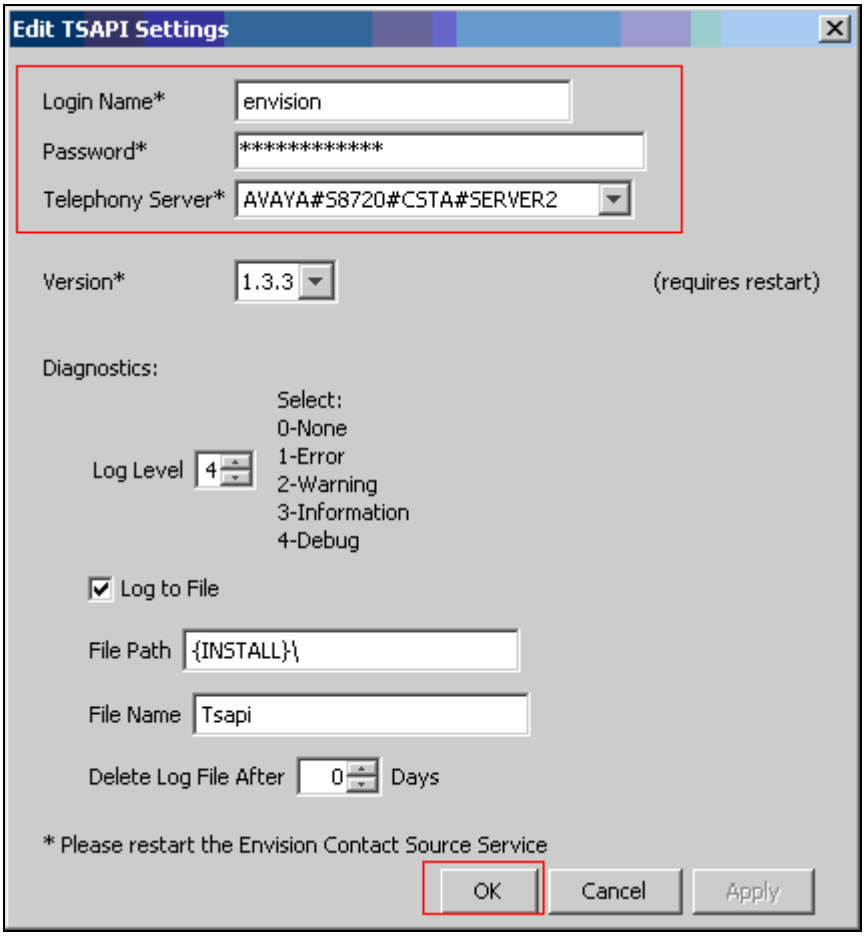


On the Edit Contact Source window, provide a descriptive name for the Contact Source, and click the **Edit Settings** button.



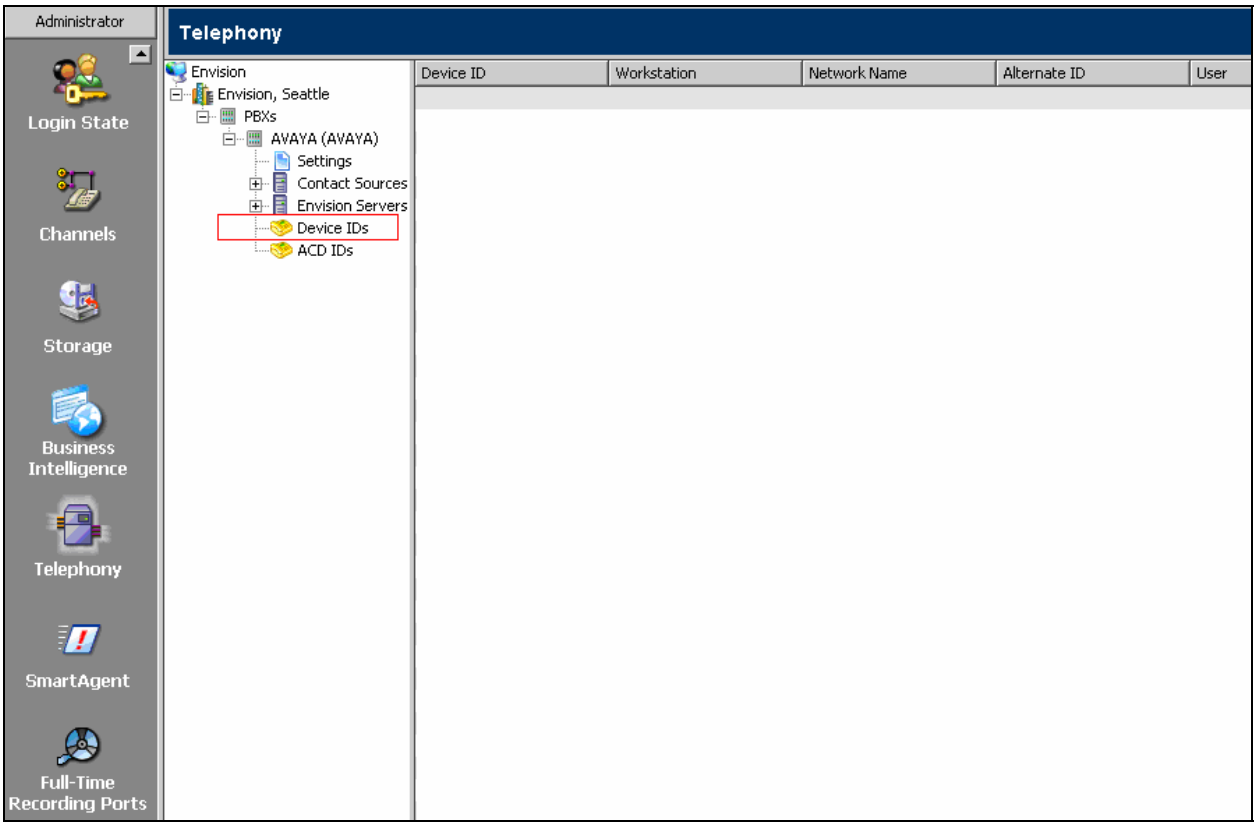
On the Edit TSAPI Settings window, provide the following information:

- Login Name – Enter the User ID created in **Section 4.4**.
- Password – Enter the User Password created in **Section 4.4**.
- Telephony Server – Enter the Tlink Name used for the Switch Connection link in **Section 4.3**.
- Click on the **OK** button.



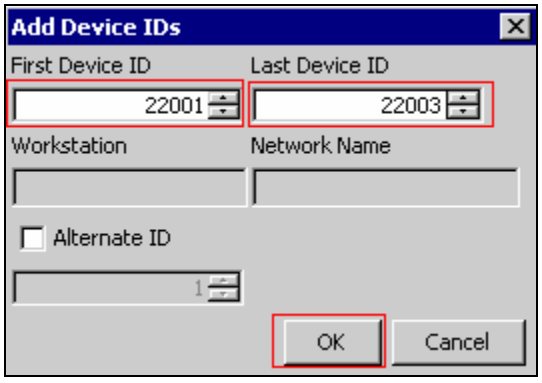
5.3. Configure Device IDs (Extensions)

In the Telephony menu, navigate to **PBXs → AVAYA (AVAYA) → Device IDs**. Double click the right pane of the window to add device.

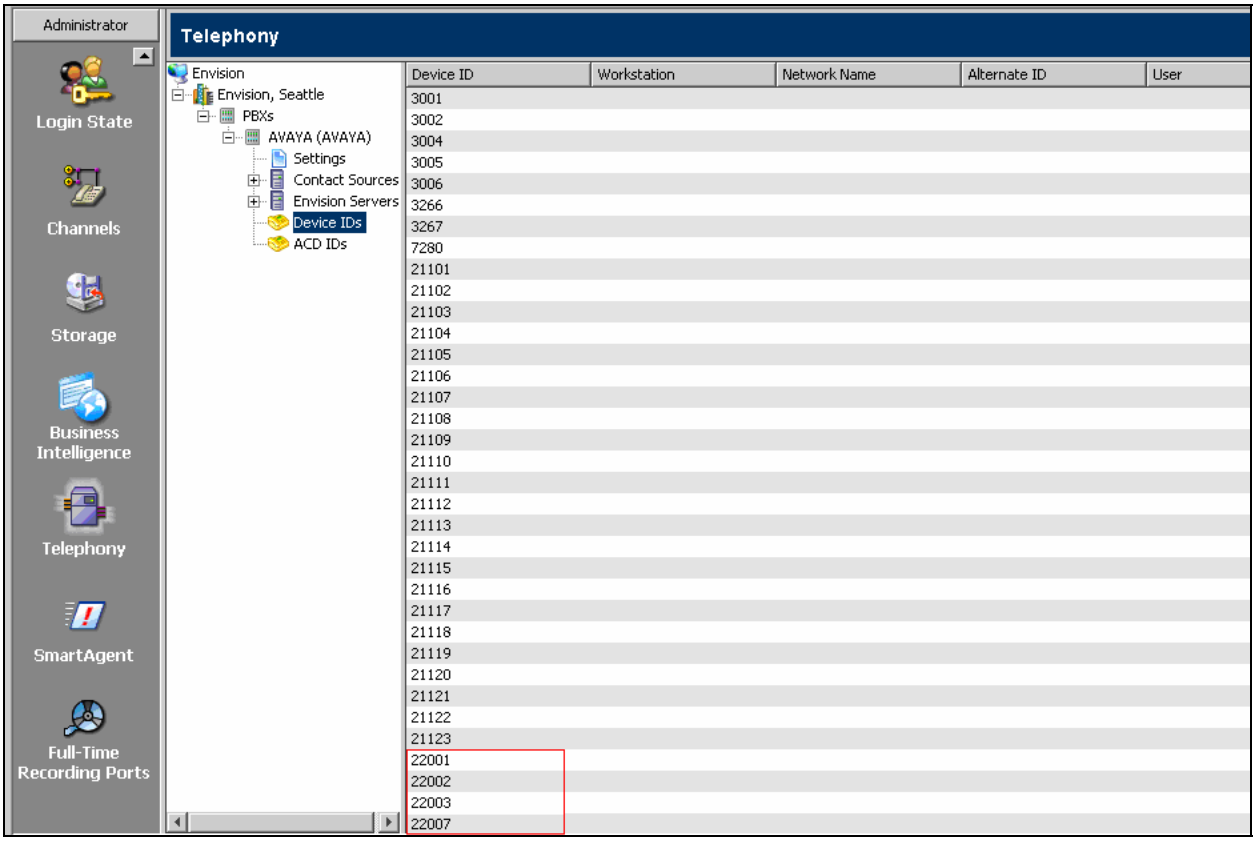


From the Add Device IDs window, provide the range of devices. The following screen shows an example of adding range of recorded devices from 22001 to 22003. Click on the **OK** button.

Repeat this step as necessary to add other devices (extensions) for recording.

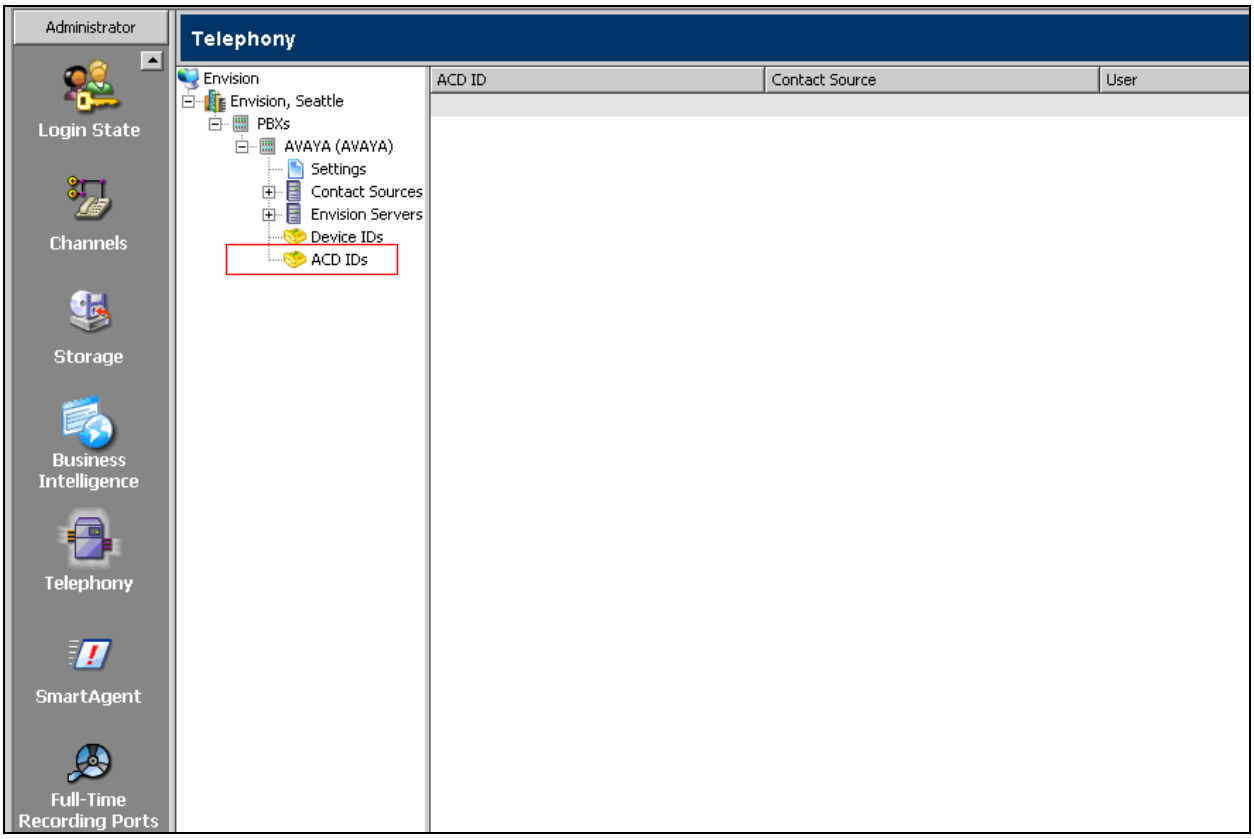


The following screen shows the Device IDs used during the compliance test.

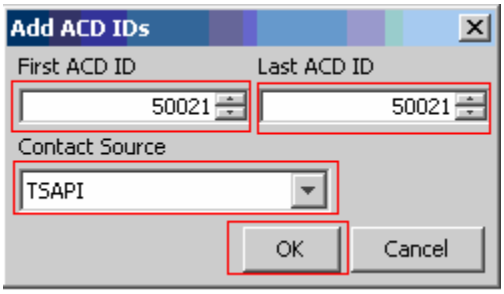


5.4. Configure ACD IDs (Agents)

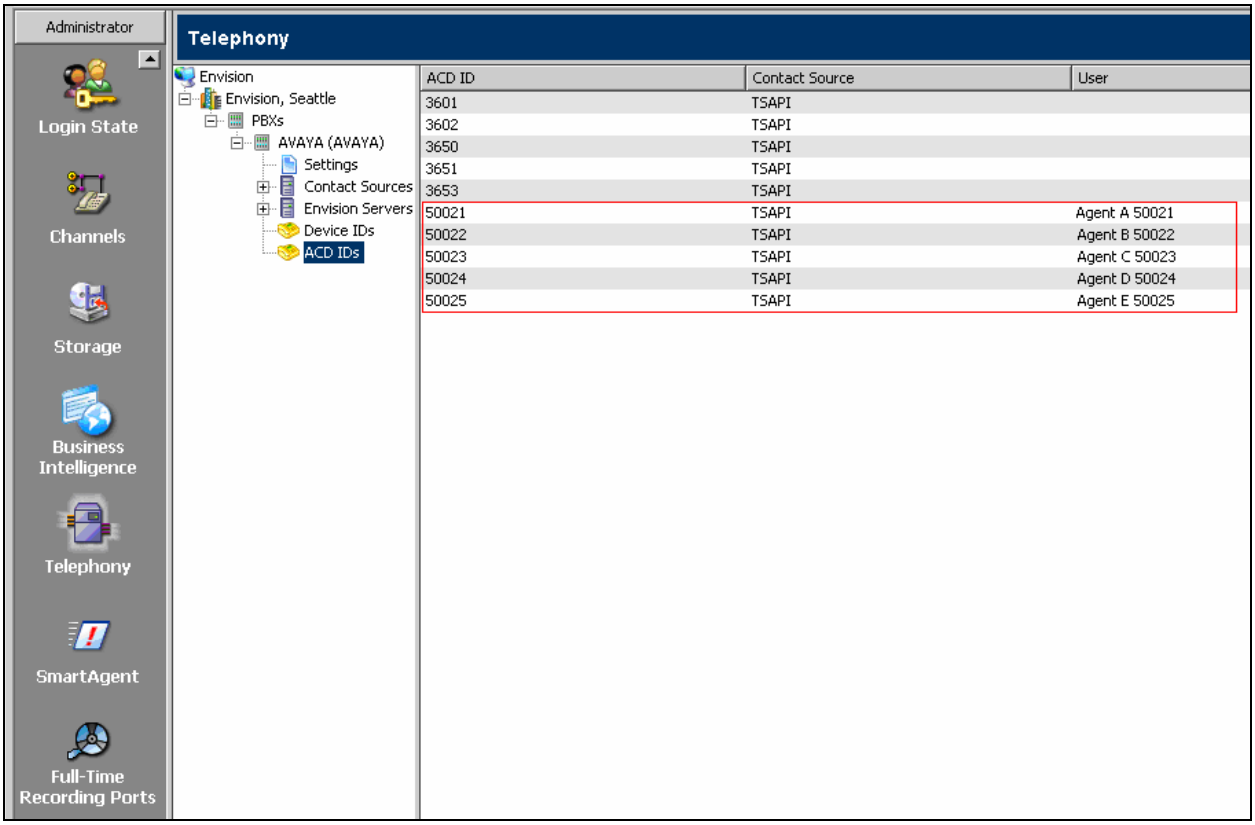
In the Telephony menu, navigate to **PBXs -> AVAYA (AVAYA) -> Envision Servers -> ACD IDs**. Double click the right pane of the window to add a device.



From the Add ACD IDs window, provide the range of devices. The following screen shows an example of adding an agent, 50021. Select **TSAPI** as a Contact Source, using the drop-down menu. Click on the **OK** button.

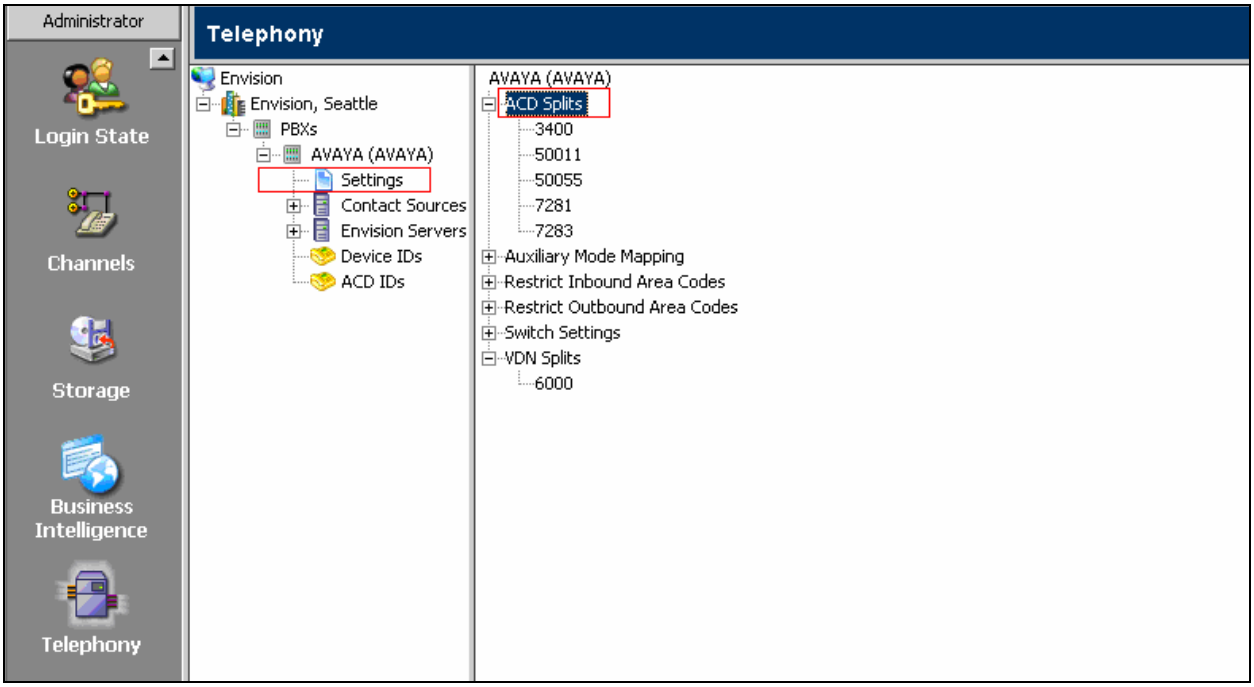


The following screen shows the ACD IDs used during the compliance test.

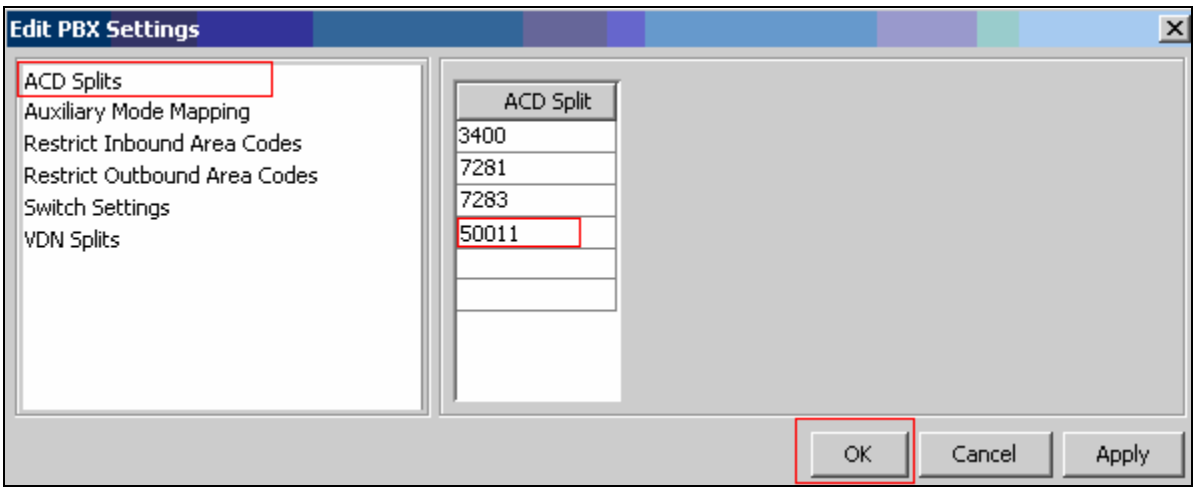


5.5. Configure Splits (Hunt Group and VDN)

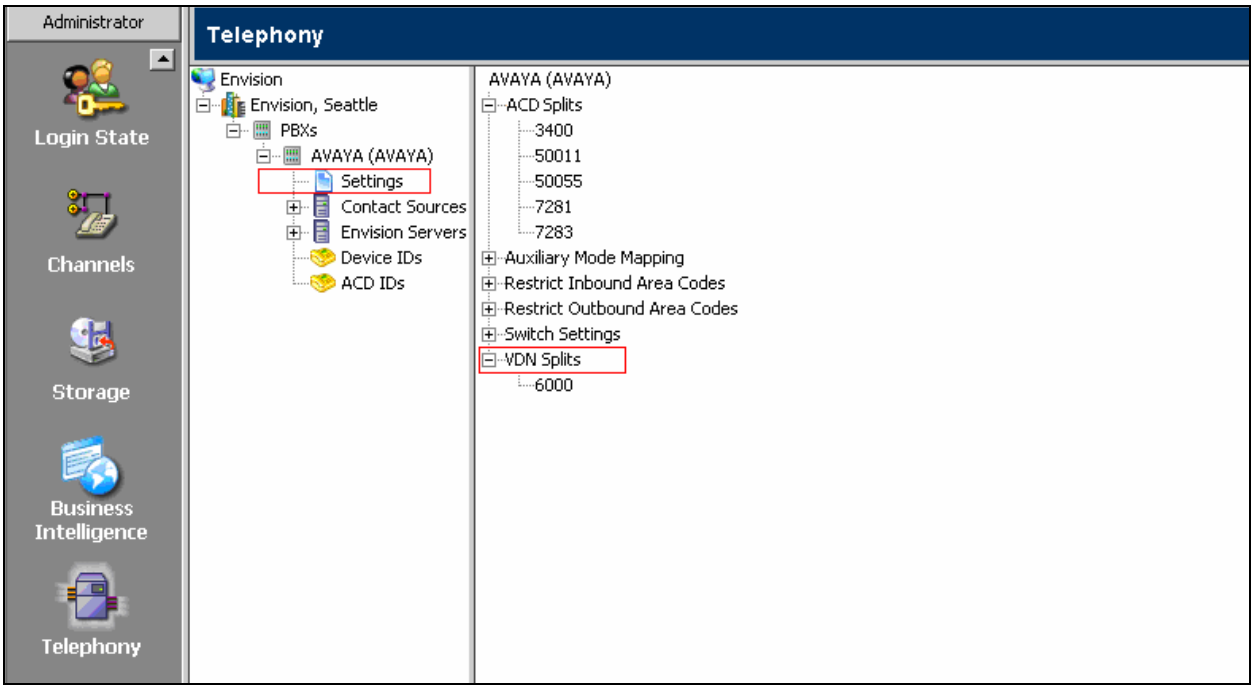
In the Telephony menu, navigate to **PBXs -> AVAYA (AVAYA) -> Settings**. In the right pane of the window, select **ACD Splits**. The ACD Splits field is used to add hunt groups for recording.



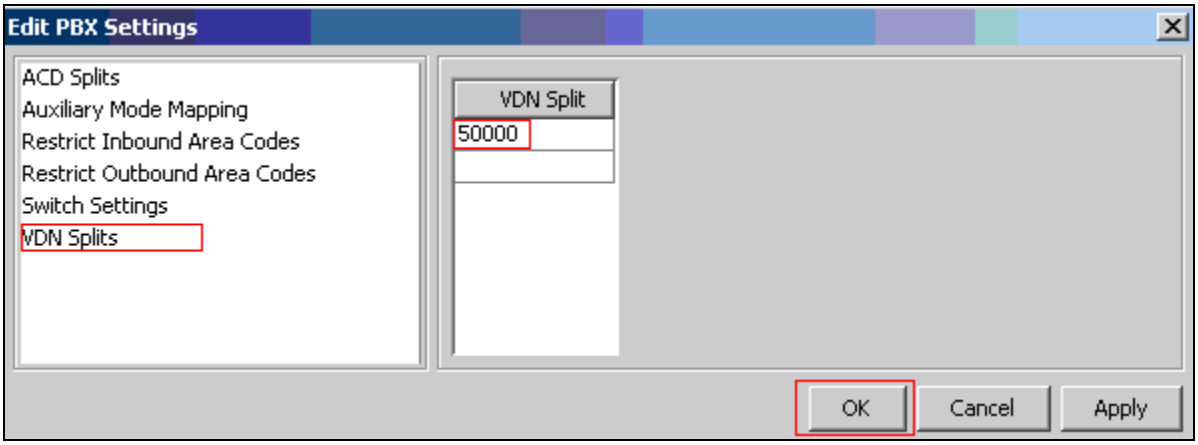
From the Edit PBX Settings window, select **ACD Splits** on the left pane of the window. On the right pane of the window, click the empty slot and enter a hunt group extension. The following screen shows an example of adding a hunt group extension, 50011. Click on the **OK** button.



Under the Telephony menu, navigate to **PBXs -> AVAYA (AVAYA) -> Settings**. In the right pane of the window, select **VDN Splits**. VDN Splits field is utilized to add VDNs for recording.



From the Edit PBX Settings window, select **VDN Splits** on the left pane of the window. On the right pane of the window, click the empty slot and enter a VDN extension. The following screen shows an example of adding a VDN extension, 50000. Click on the **OK** button.



6. Interoperability Compliance Testing

The interoperability compliance test included basic trunk recording, serviceability, and performance testing. The basic recording testing evaluated the ability of Envision Centricity to monitor and record calls placed to and from stations through a trunk. The serviceability testing introduced failure scenarios to see if Envision Centricity can resume recording after failure recovery. The performance testing stressed Envision Centricity by continuously placing calls over extended periods of time.

6.1. General Test Approach

The general approach was to manually place calls to and from stations through a trunk, monitor and record them using Envision Centricity, and verify the recordings. The types of calls included inbound and outbound trunk calls (station calls, agent calls, VDN, hunt group), conference calls and transferred calls through a trunk. Performance tests verified that Envision Centricity could record calls during a sustained volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the steps that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES.

7.1. Verify Avaya Communication Manager

Verify the status of the administered AES link by using the **status aesvcs link** command.

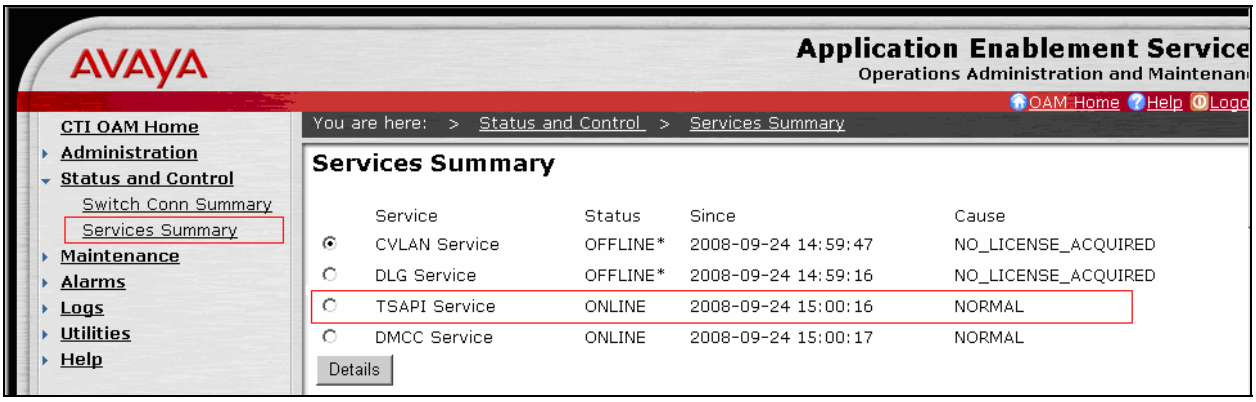
```
status aesvcs link

                              AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                          Port                    Sent    Rcvd

01/01  server2         192. 45. 80.103  60336   CLAN-AES        208     197
```

Verify the Service State field of the administered TSAPI CTI link is in **established** state, by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link

                           AE SERVICES CTI LINK STATUS

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

4     4        no    server2          established   15       15
```

7.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services are ONLINE, by selecting **Status and Control → Services Summary** from the left pane.



8. Support

Technical support on Envision Centricity can be obtained via email at http://www.envisioninc.com/custom_form.cfm?custom_form_id=32023 or by calling 206-225-0800 ext 600.

9. Conclusion

These Application Notes illustrate the procedures for configuring an Envision Centricity trunk tap call recording solution to monitor and record calls placed to and from stations through a trunk on an Avaya Communication Manager system. During compliance testing, Envision Centricity successfully monitored events and recorded calls placed to and from stations. Envision Centricity was also able to record calls under continuous call volume over an extended period of time.

10. Additional References

This section references the Avaya and Envision documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com .

[1] *Administrator Guide for Avaya Communication Manager*, Issue 4, January 2008, Document Number 03-300509

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 4.1, Issue 9, February 2008, Document Number 02-300357

The Envision Centricity Administrator User Guide was used during the configuration. Customers are provided a copy of this guide at the time of installation.

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.