Avaya Solution & Interoperability Test Lab

Application Notes for CallCopy cc:Discover with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CallCopy cc:Discover to interoperate with Avaya Communication Manager and Avaya Application Enablement Services.

The cc:Discover is a software-only solution for voice call recording that offers various recording, playback and archiving features and options.

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.

©2007 Avaya Inc. All Rights Reserved.

1. Introduction

CallCopy cc:Discover is a software-only solution for voice call recording that offers various recording, playback and archiving features and options. By combining media redirection from Avaya Communication Manager with single step conferencing, call recording can be achieved without the use of physical connections to the CallCopy server other than standard network connections.

CallCopy cc:Discover uses the Telephony Services API (TSAPI) of the Avaya Application Enablement Services (AES) to receive call related events. CallCopy cc:Discover's internal scheduling algorithm makes the determination on which calls should be recorded based on the events received via the TSAPI link and customer recording requirements.

The cc:Discover's Device Media and Call Control (DMCC) integration works by registering a number of softphone stations (one per channel) and sets the media and media control streams (RTP/RTCP) to go to unique UDP ports on the CallCopy cc:Discover server. When a call is to be recorded, the cc:Discover's TSAPI module performs a single step conference between the extension to be recorded and one of the softphone stations. The recording application then sends a message to the DMCC integration application to begin recording the voice stream coming to that soft phone extension. In this message, the recorder passes along the softphone extension to be recorded along with the location and filename of the recording. All RTP traffic on that softphone's RTP port is captured and written to the file location in CallCopy's proprietary .cca format.

©2007 Avaya Inc. All Rights Reserved.

Figure 1 provides the test configuration used for the compliance testing.

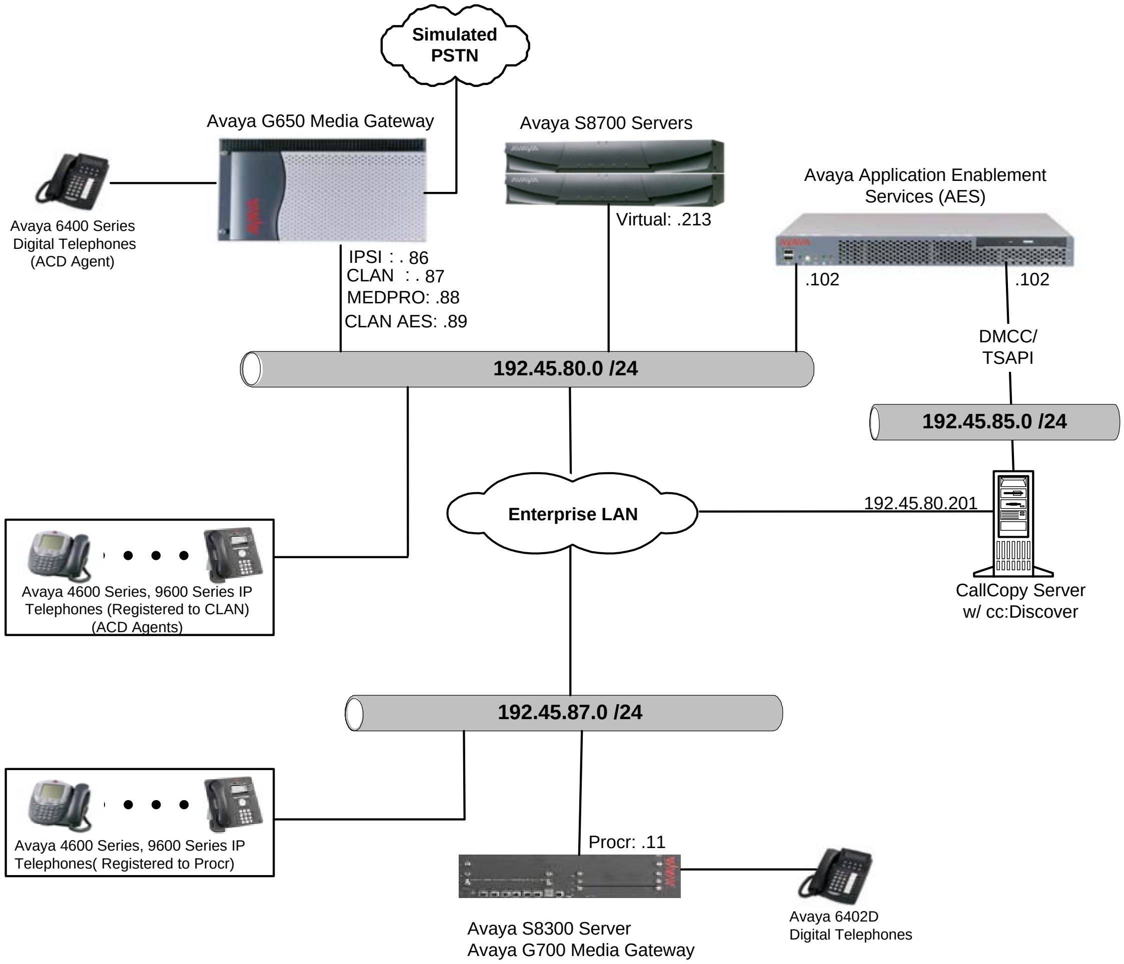


Figure 1: CallCopy cc:Discover with Avaya Communication Manager and Avaya AES

©2007 Avaya Inc. All Rights Reserved.

2. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8700 Servers		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface TN799DP CLAN Interface TN2302AP IP Media Processor	HW11 FW030 HW01 FW017 HW20 FW108
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya Application Enablement Services		4.0 w/ Bundled Offer Build 47.3
Avaya 4600 Series IP Telephones		
	4620 (H.323) 4625 (H.323)	2.8 2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323) 9650 (H.323)	1.5 1.5
Avaya 6400D Series Digital Telephones		N/A
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Networks Summit 48		4.1.21
CallCopy cc:Discover		3.6.0.215

3. Configure Avaya Communication Manager

This section provides the procedures for configuring hunt/skill group, vectors, Vector Directory Numbers (VDN), agents, agent login/logout feature access codes, recording ports and recording (DMCC) stations, recorded stations, IP codec, IP network regions, and Computer Telephony Interface (CTI) link on Avaya Communication Manager to integrate with cc:Discover. 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. For the compliance testing, the following contact center devices were used.

Device Type	Device Number/Extension
VDN	50000
Vector	11
Skill group	11
Logical agent IDs	50021, 50022, 50023, 50024, 20025
Recorded stations (IP Telephones)	IP Telephones: 22001, 22002, 22003 DCP Telephone: 22007 IP Agents: 22008, 22009
Recording stations (DMCC stations)	21001 - 21023

©2007 Avaya Inc. All Rights Reserved.

3.1. Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the **display system-parameters customer-options** command. On **Page 6**, verify that the ACD and Vectoring (Basic) fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options                    Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 3.0

                                ACD? y                          Reason Codes? n
                       BCMS (Basic)? y               Service Level Maximizer? n
         BCMS/VuStats Service Level? n             Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? n     Service Observing (Remote/By FAC)? y
                  Business Advocate? n              Service Observing (VDNs)? n
                    Call Work Codes? n                           Timed ACW? N

      DTMF Feedback Signals For VRU? n                   Vectoring (Basic)? y
                  Dynamic Advocate? n                Vectoring (Prompting)? n
       Expert Agent Selection (EAS)? n             Vectoring (G3V4 Enhanced)? n
                           EAS-PHD? n             Vectoring (3.0 Enhanced)? n
                  Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? n
              Least Occupied Agent? n     Vectoring (G3V4 Advanced Routing)? n
         Lookahead Interflow (LAI)? n                    Vectoring (CINFO)? n
Multiple Call Handling (On Request)? n      Vectoring (Best Service Routing)? n
    Multiple Call Handling (Forced)? n                Vectoring (Holidays)? n
  PASTE (Display PBX Data on Phone)? n               Vectoring (Variables)? n
        (NOTE: You must logoff & login to effect the permission changes.)
```

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the hunt-group form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan. Set the ACD, Queue, and Vector fields to **y**. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.

```
add hunt-group 11                                           Page   1 of   61

                                  HUNT GROUP

            Group Number: 11                                ACD? y
              Group Name: Test                            Queue? y
         Group Extension: 50091                          Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                     MM Early Answer? n
           Security Code:                  Local Agent Preference? n
 ISDN/SIP Caller Display:


             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```


©2007 Avaya Inc. All Rights Reserved.

On **Page 2**, set the Skill field to **y**, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

```
add hunt-group 11                                              Page   2 of   3

                                 HUNT GROUP

                    Skill? y
                      AAS? n
                 Measured: internal
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:



                                      Redirect on No Answer (rings): 3
                                                    Redirect to VDN:
                  Forced Entry of Stroke Counts or Call Work Codes? n
```

Enter the **add agent-loginID p** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1** of the agent-loginID form, enter a descriptive Name and Password.

```
add agent-loginID 50021                                       Page   1 of   2

                                 AGENT LOGINID

                Login ID: 50021                                  AAS? n
                    Name: Agent-50021                          AUDIX? n
                      TN: 1                            LWC Reception: spe
                     COR: 1                   LWC Log External Calls? n
           Coverage Path:                   AUDIX Name for Messaging:
           Security Code:
                                            LoginID for ISDN Display? n
                                                            Password: 1234
                                              Password (enter again): 1234
                                                         Auto Answer: station
                                                   MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system


     WARNING:  Agent must log in again before changes take effect
```


©2007 Avaya Inc. All Rights Reserved.

On **Page 2**, set the Skill Number (SN) to the hunt group number previously created in this section. The Skill Level (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.

```
add agent-loginID 50021                                           Page   2 of   2

                                 AGENT LOGINID
      Direct Agent Skill:
Call Handling Preference: skill-level              Local Call Preference? n

    SN       SL           SN       SL           SN       SL           SN       SL
 1: 11        1       16:                 31:                 46:
 2:                   17:                 32:                 47:
 3:                   18:                 33:                 48:
 4:                   19:                 34:                 49:
 5:                   20:                 35:                 50:
 6:                   21:                 36:                 51:
 7:                   22:                 37:                 52:
 8:                   23:                 38:                 53:
 9:                   24:                 39:                 54:
10:                   25:                 40:                 55:
11:                   26:                 41:                 56:
12:                   27:                 42:                 57:
13:                   28:                 43:                 58:
14:                   29:                 44:                 59:
15:                   30:                 45:                 60:
```

Enter the **add vector q** command, where **q** is an unused vector number. Enter a descriptive Name, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

```
add vector 11                                                      Page   1 of   3

                                 CALL VECTOR

    Number: 11                Name: Queue to skill1
                                             Meet-me Conf? n             Lock? n
     Basic? y    EAS? y    G3V4 Enhanced? n    ANI/II-Digits? n   ASAI Routing? y
 Prompting? n    LAI? n   G3V4 Adv Route? n    CINFO? n    BSR? n    Holidays? n
 Variables? n    3.0 Enhanced? n
01 wait-time    2   secs hearing ringback
02 queue-to     skill 11    pri m
03
04
05
06
07
08
09
10
11

                       Press 'Esc f 6' for Vector Editing
```


©2007 Avaya Inc. All Rights Reserved.

Enter the **add vdn r** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive Name for the VDN and specify the vector configured in the previous step as the Vector Number. In the example below, incoming calls to extension 50000 will be routed to VDN 50000, which in turn will invoke the actions specified in vector 11.

```
add vdn 50000                                               Page   1 of   2

                            VECTOR DIRECTORY NUMBER

                             Extension: 50000
                                  Name: VDN-50000
                         Vector Number: 11

                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                    TN: 1
                              Measured: internal
```

Enter the **change feature-access-codes** command. Define the Auto-In Access Code, Login Access Code, Logout Access Code, and Aux Work Access Code.

```
change feature-access-codes                                    Page   5 of   6
                               FEATURE ACCESS CODE (FAC)

                         Automatic Call Distribution Features

                    After Call Work Access Code: 120
                             Assist Access Code: 121
                            Auto-In Access Code: 122
                           Aux Work Access Code: 123
                              Login Access Code: 124
                             Logout Access Code: 125
                          Manual-in Access Code: 126
      Service Observing Listen Only Access Code: 127
      Service Observing Listen/Talk Access Code: 128
                    Add Agent Skill Access Code: 130
                 Remove Agent Skill Access Code: 131
             Remote Logout of Agent Access Code: 132
```

Enter the **add abbreviated-dialing group g** command, where **g** is the number of an available abbreviated dialing group. In the DIAL CODE list, enter the Feature Access Codes, created previously, for ACD Login and Logout.

```
add abbreviated-dialing group 1                             Page   1 of   1
                        ABBREVIATED DIALING LIST

              Group List: 1        Group Name: Call Center
    Size (multiple of 5): 5       Program Ext:                 Privileged? n
DIAL CODE
     11: 124
     12: 125
     13:
```


©2007 Avaya Inc. All Rights Reserved.

3.2. Recording Ports

The recording ports in this configuration are AES Device, Media, and Call Control (DMCC) stations that essentially appear as IP Softphones to Avaya Communication Manager. Each DMCC station requires an IP_API_A license.

Enter the **display system-parameters customer-options** command and verify that there are sufficient **IP_API_A** licenses. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options                      Page  10 of  11
                    MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit           Used
IP_API_A       : 200             0
IP_API_B       : 0               0
IP_API_C       : 0               0
IP_Agent       : 50              0
IP_IR_A        : 0               0
IP_Phone       : 12000           3
IP_ROMax       : 12000           0
IP_Soft        : 2               0
IP_eCons       : 0               0
               : 0               0
               : 0               0

        (NOTE: You must logoff & login to effect the permission changes.)
```

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, set the Port field to **ip**, enter a descriptive Name, specify the Security Code, and set the IP SoftPhone field to **y**.

Repeat this step as necessary, with the same Security Code, to configure additional DMCC stations.

```
add station 21001                                              Page   1 of   5
                                     STATION

Extension: 21001                         Lock Messages? n               BCC: 0
     Type: 4621                          Security Code: 1234             TN: 1
     Port: ip                      Coverage Path 1:                     COR: 1
     Name: DMCC-1                       Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 21001
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english               Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? y

                                              IP Video Softphone? n

                                             Customizable Labels? y
```


©2007 Avaya Inc. All Rights Reserved.

3.3. Recorded Stations

The stations that were recorded during the compliance testing include an Avaya Digital Telephone, Avaya IP Telephones (Avaya 4600 and 9600 Series), and an Avaya IP Agent. The extensions used were in the ranges 22001-22009.

3.4. Audio Codec Configuration

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

Note: The codec has to match between Avaya Communication Manager and CallCopy cc:Discover (recording codec).

```
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.729A            n         2         20
 2:
 3:
 4:

     Media Encryption
 1: none
 2:
```


©2007 Avaya Inc. All Rights Reserved.

3.5. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. Set the Codec Set field to **1**. The Avaya IP Telephones and Avaya IP Agent, as well as Avaya AES DMCC stations used by the cc:Discover, registered with the C-LAN board (CLAN) and were thus also assigned to IP network region 1. One consequence of assigning the aforementioned Avaya IP Telephones, Avaya IP Agent, Avaya AES DMCC stations, and MedPro boards to a common IP network region is that the RTP traffic between them is governed by the same codec set. The second C-LAN board (CLAN-AES), which was dedicated for the Avaya AES was assigned to the IP network region 2. The following screen shows only IP 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? y
   UDP Port Max: 3028
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: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        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
            Keep-Alive Count: 5
```

On **Page 3**, set the codec set field to **1**, which implies all calls between IP Network Region 1 and IP Network Region 2 utilize the values in IP Codec Set 1.

```
change ip-network-region 1                                      Page   3 of  19

                   Inter Network Region Connection Management

 src dst codec direct   Total          Video                          Dyn
 rgn rgn  set   WAN  WAN-BW-limits  WAN-BW-limits  Intervening-regions  CAC IGAR
 1   1    1
 1   2    1     y        :NoLimit       :NoLimit                             n
 1   3
 1   4
```

©2007 Avaya Inc. All Rights Reserved.

3.6. Configure TSAPI CTI Link

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. Set the Type field to **ADJ-IP** and assign a descriptive Name to the CTI link. Default values may be used in the remaining fields.

```
add cti-link 4                                                Page   1 of   2
                                    CTI LINK
 CTI Link: 4
Extension: 79001
     Type: ADJ-IP
                                                                      COR: 1
     Name: TSAPI
```

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoints (Avaya IP Telephones, Avaya IP Agents, and Avaya AES DMCC stations). The CLAN-AES IP address was used for connectivity to the Avaya AES server.

```
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
S8300G700              192.45.87.11
VAL                    192.45.80.85
default                0.0.0.0
```

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 node-name ip form. During the compliance test, the default port was utilized 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
```


©2007 Avaya Inc. All Rights Reserved.

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 run **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:       server1          xxxxxxxxxxxxxxxx       y        idle
      2:
      3:
```

4. Configure Avaya Application Enablement Services

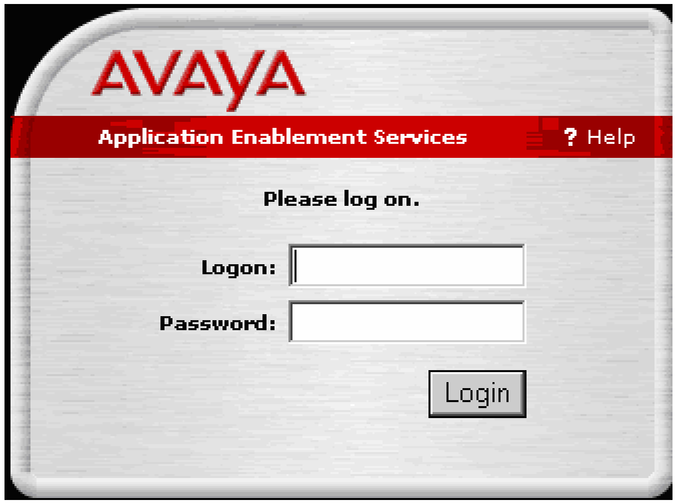
Avaya AES enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. Avaya AES receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, Avaya AES receives responses and events from Avaya 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, creating a CTI link for TSAPI, and a CTI user.

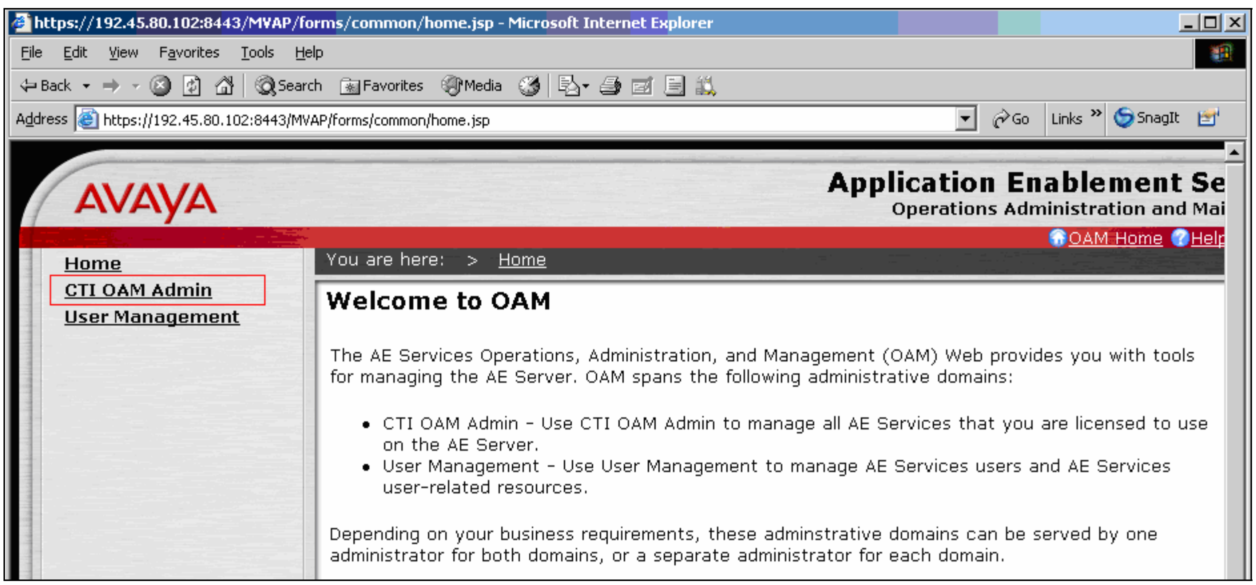
©2007 Avaya Inc. All Rights Reserved.

4.1. Configure Switch Connection

Launch a web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

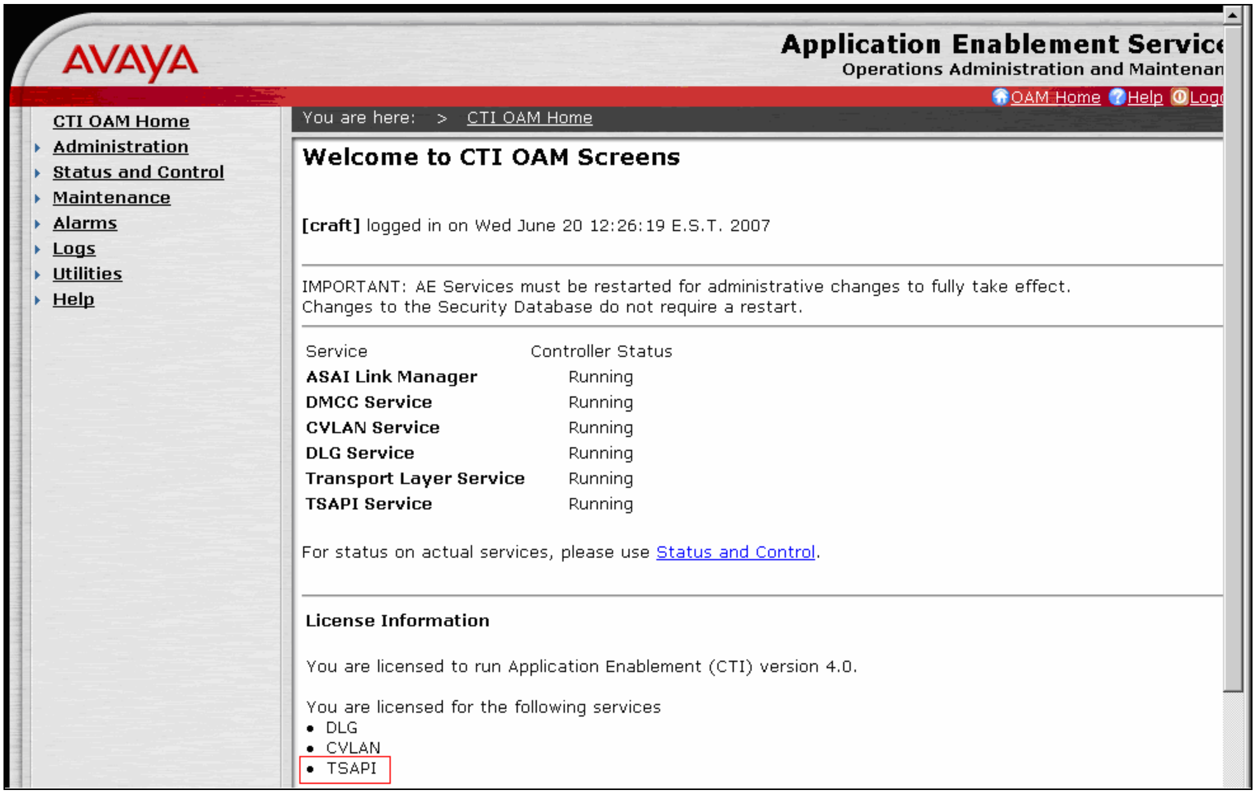


The Welcome to OAM screen is displayed next. Select **CTI OAM Admin** from the left pane.

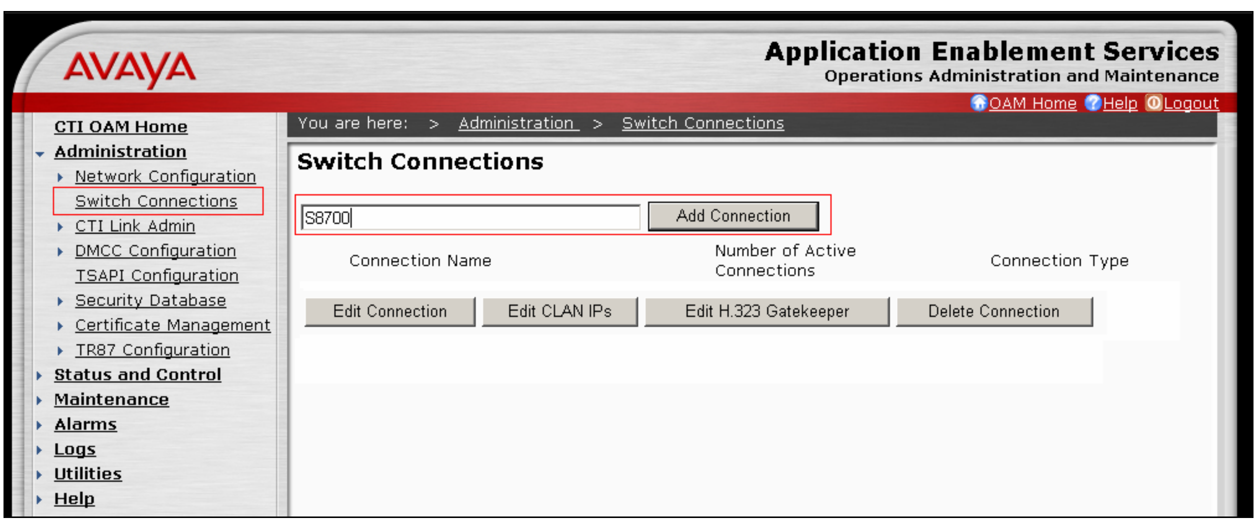


©2007 Avaya Inc. All Rights Reserved.

Verify that AES is licensed for the TSAPI service, as shown in the bottom of the screen below.

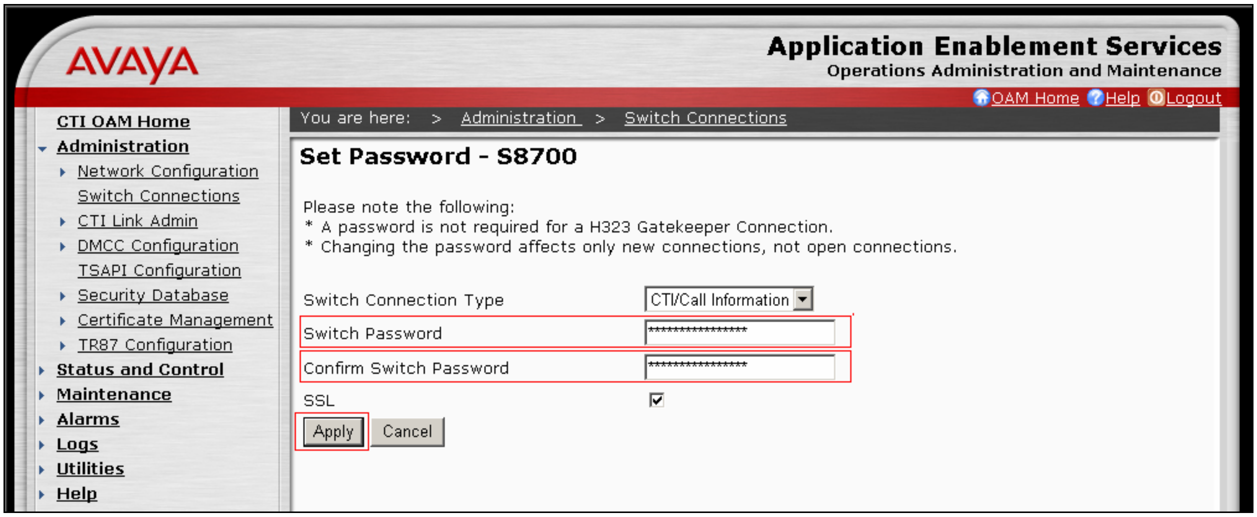


Click on **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the AES server and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

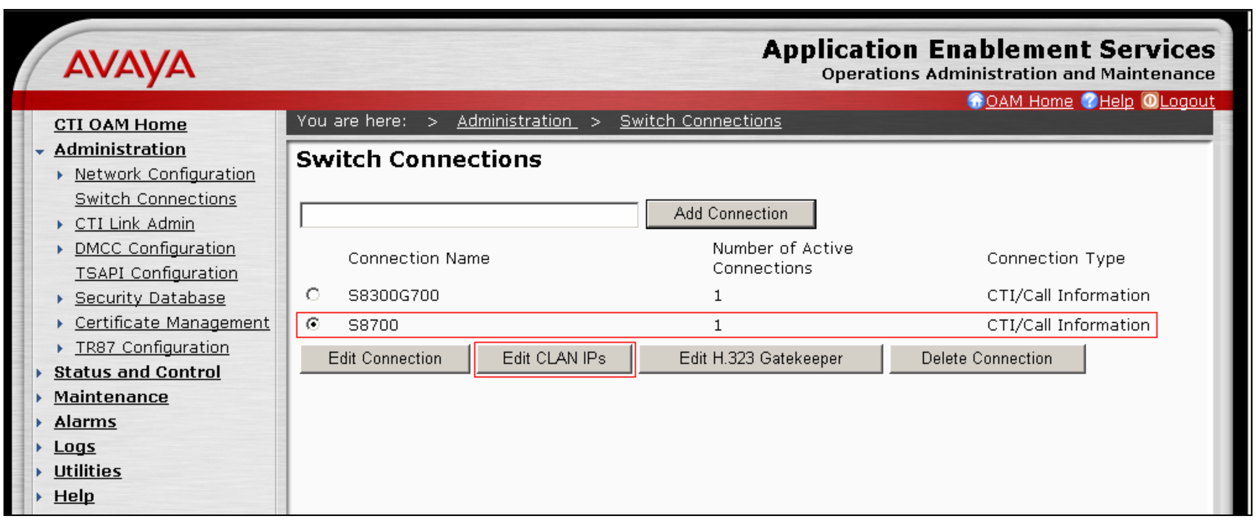


©2007 Avaya Inc. All Rights Reserved.

The next window that appears prompts for the Switch Password. Enter the same password that was administered on Avaya Communication Manager in **Section 3.6**. Default values may be used in the remaining fields. Click on **Apply**.

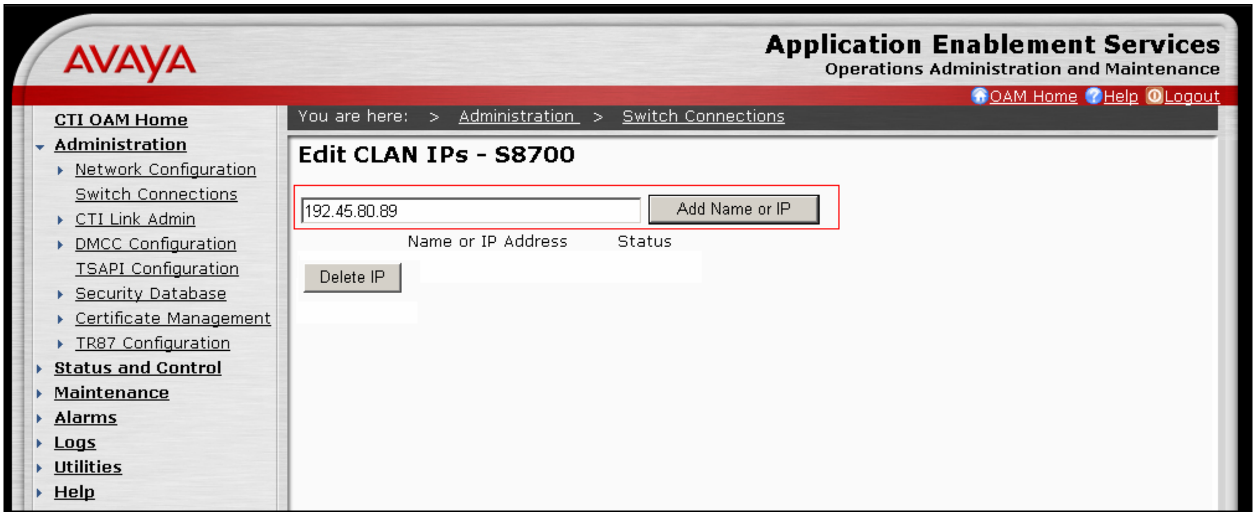


After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.



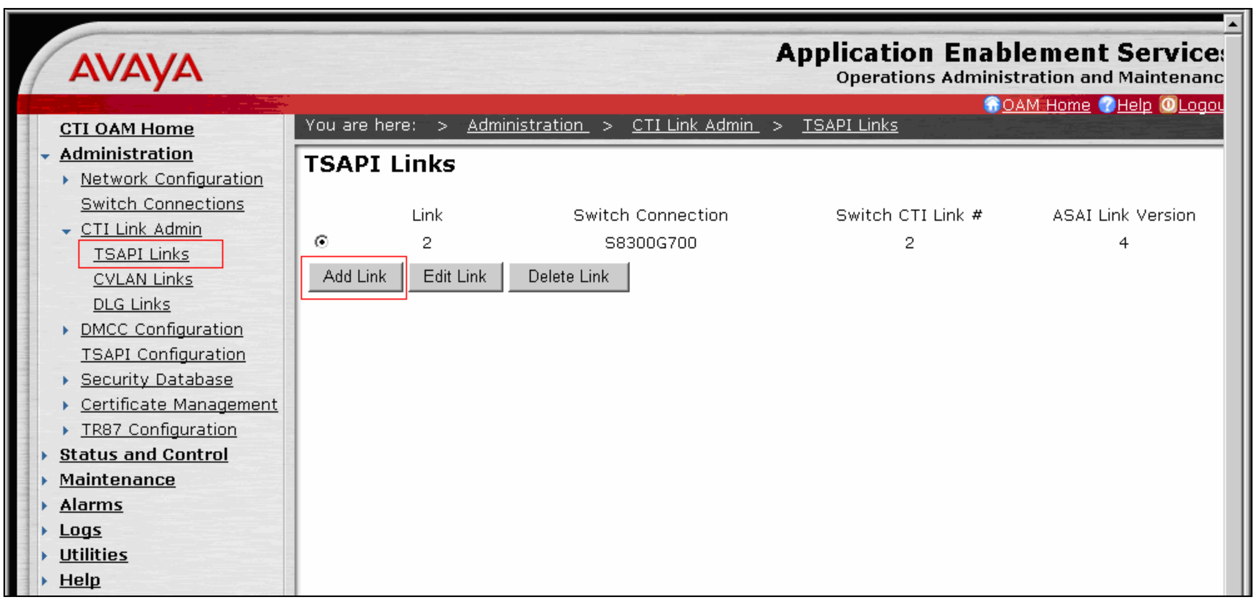
©2007 Avaya Inc. All Rights Reserved.

Enter the IP address of the CLAN used for Avaya AES connectivity from **Section 3.6**, and click on **Add Name or IP**.



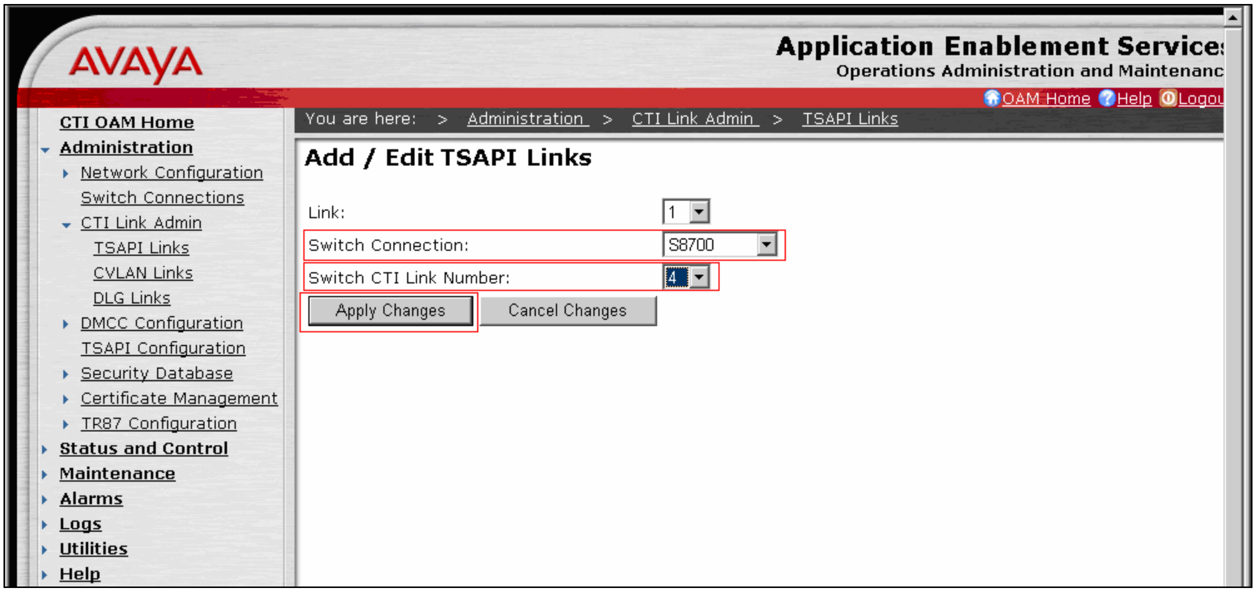
4.2. Configure TSAPI CTI Link

Navigate to **Administration → CTI Link Admin → TSAPI Links** to configure the TSAPI CTI link. Click the **Add Link** button to start configuring the TSAPI link.

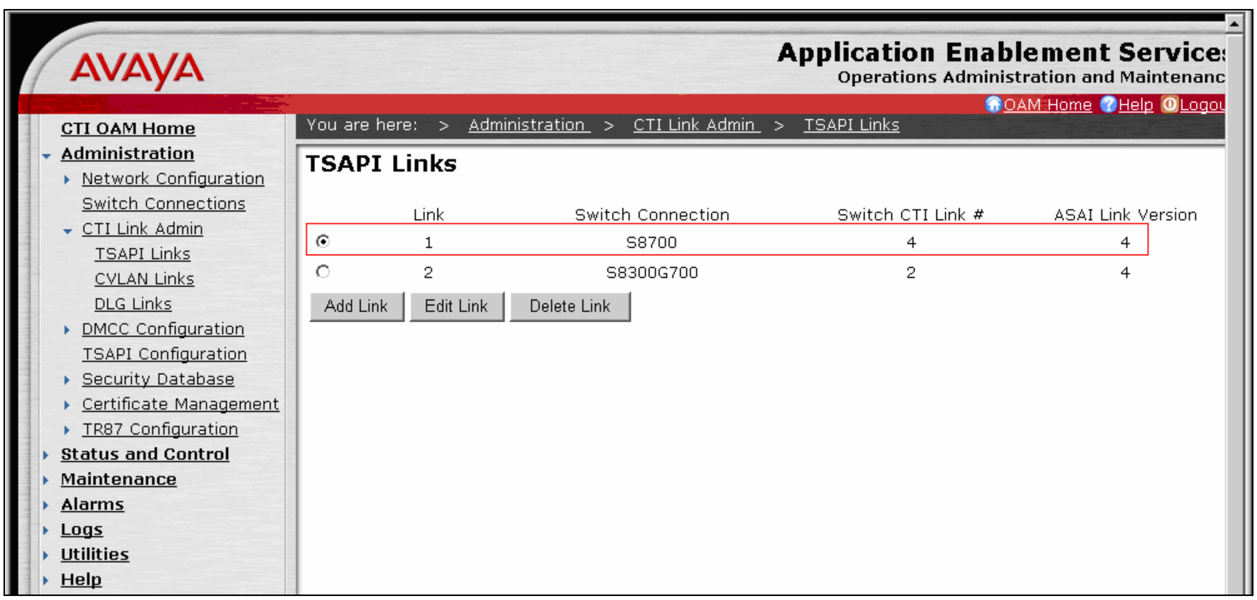


©2007 Avaya Inc. All Rights Reserved.

Select the switch connection using the drop-down menu. Select the switch connection configured in **Section 4.1**. Select the Switch CTI Link Number using the drop-down menu. The CTI link number should match with the number configured in the cti-link form in **Section 3.6**. Select **Apply Changes**.



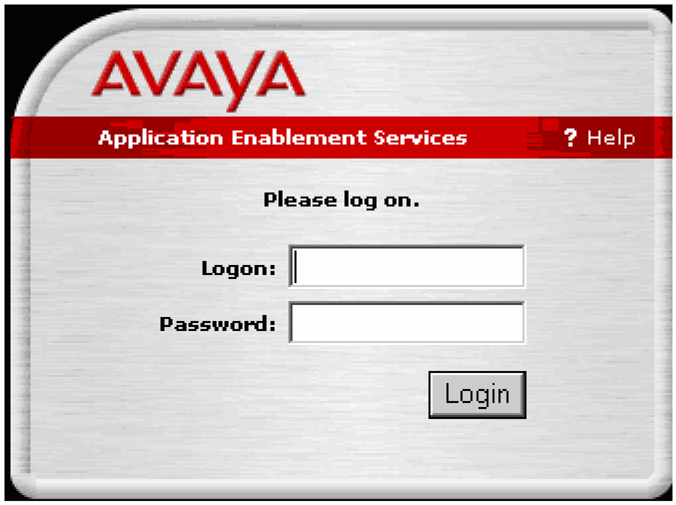
The following screen shows the TSAPI CTI link configuration.



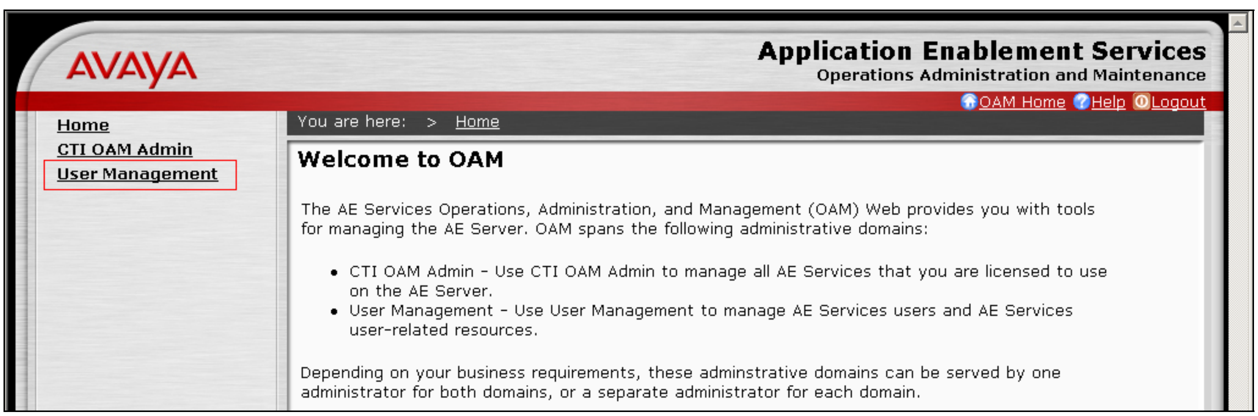
©2007 Avaya Inc. All Rights Reserved.

4.3. Configure CTI User

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials for accessing the OAM Home page.

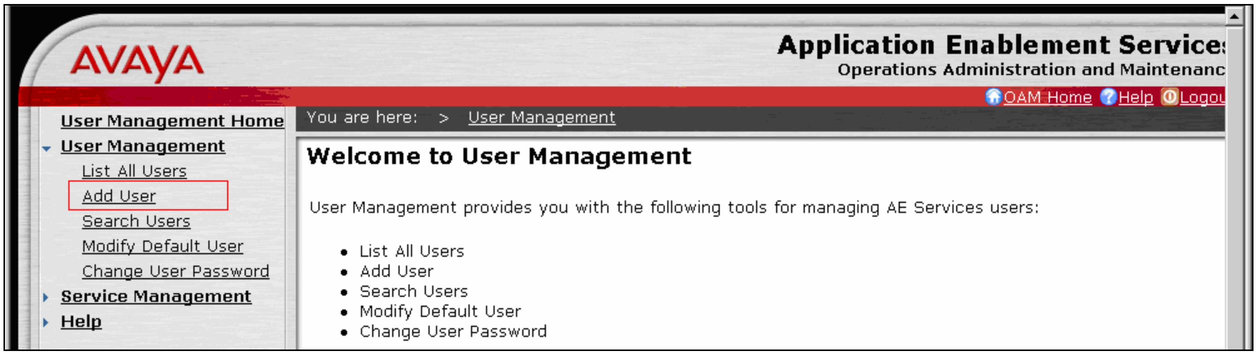


The Welcome to OAM screen is displayed next. Select **User Management** from the left pane.



©2007 Avaya Inc. All Rights Reserved.

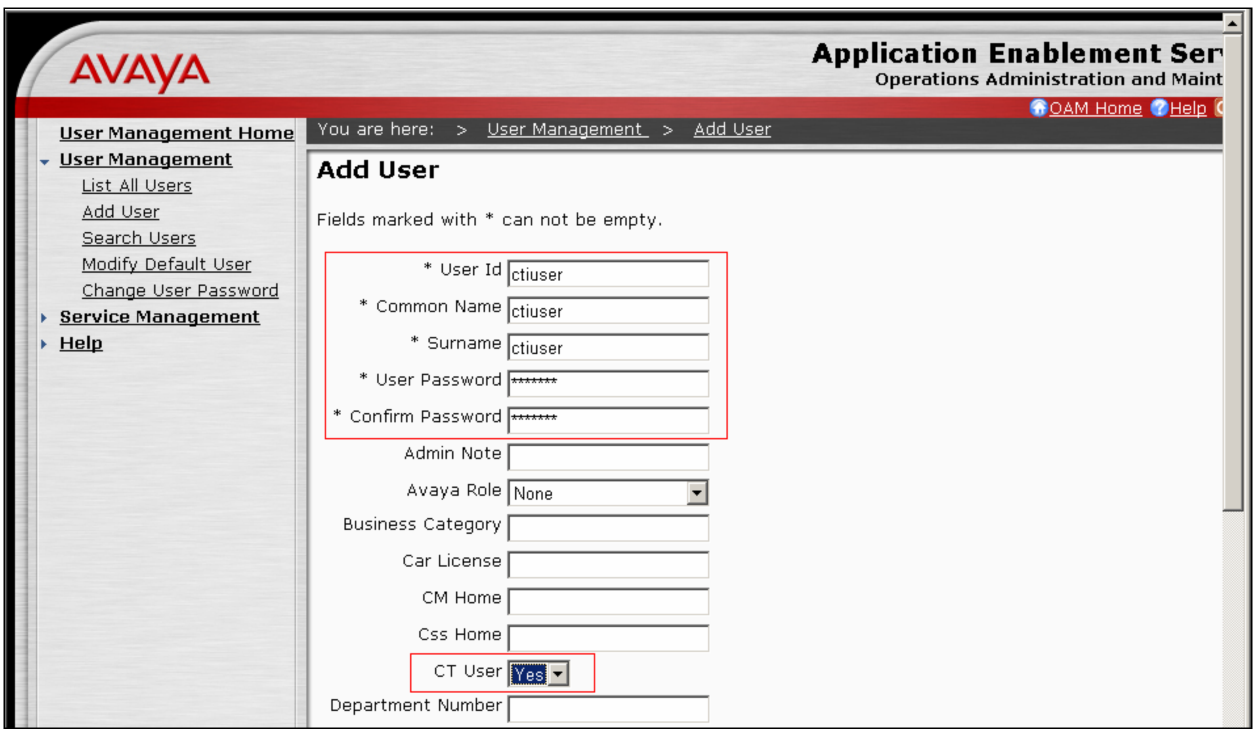
From the Welcome to the User Management Home page, navigate to the **User Management → Add User** page to add a CTI user.



On the Add User page, provide the following information:

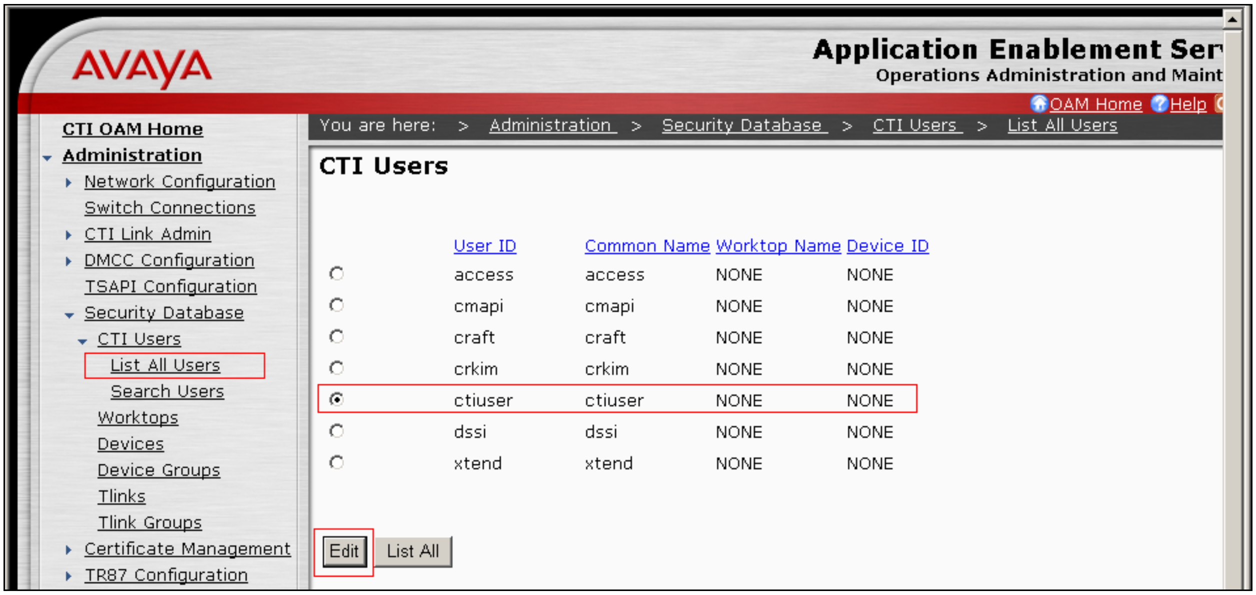
- User Id
- Common Name
- Surname
- User Password
- Confirm Password

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 here) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

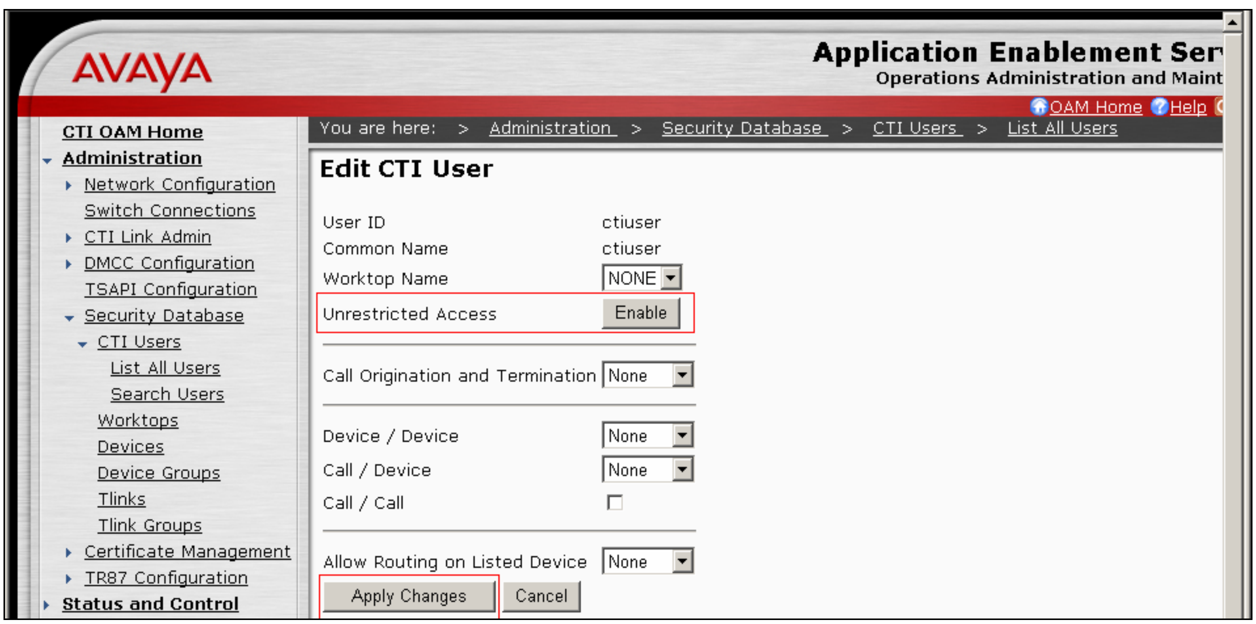


©2007 Avaya Inc. All Rights Reserved.

Once the user is created, select **OAM Home** in upper right and navigate to the **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.

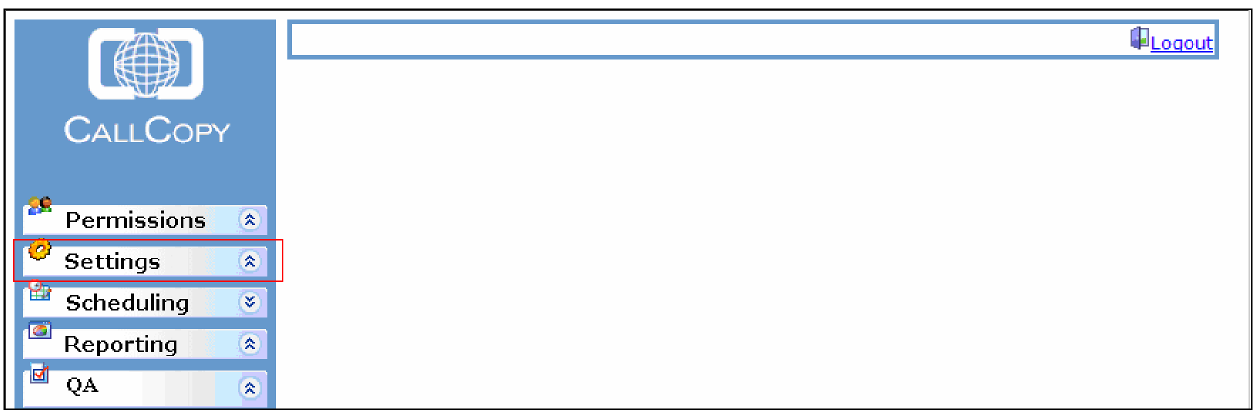


5. Configure CallCopy cc:Discover

CallCopy installs, configures, and customizes the cc:Discover application for their end customers. This section only describes the interface section of the cc:Discover configuration.

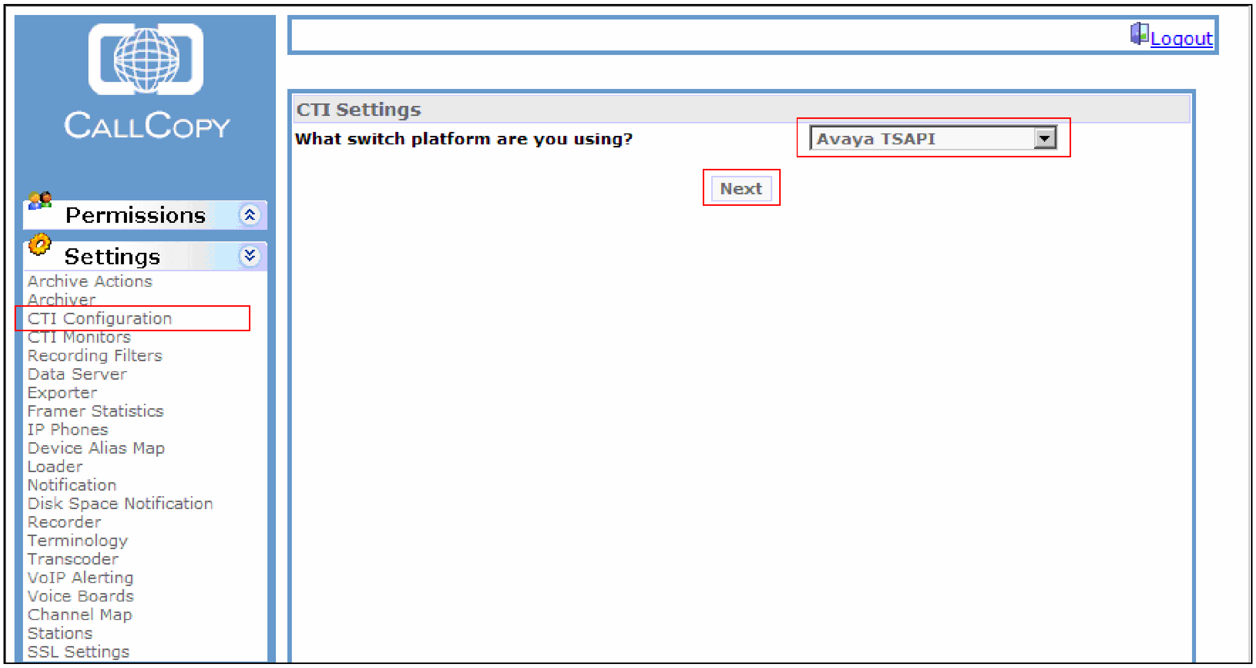
Launch a web browser, enter http://<IP address of CallCopy server> in the URL, and log in with the appropriate credentials for accessing the CallCopy cc:Discover main pages.

Select the **Settings → CTI Configuration** link from the left pane to configure the interface.

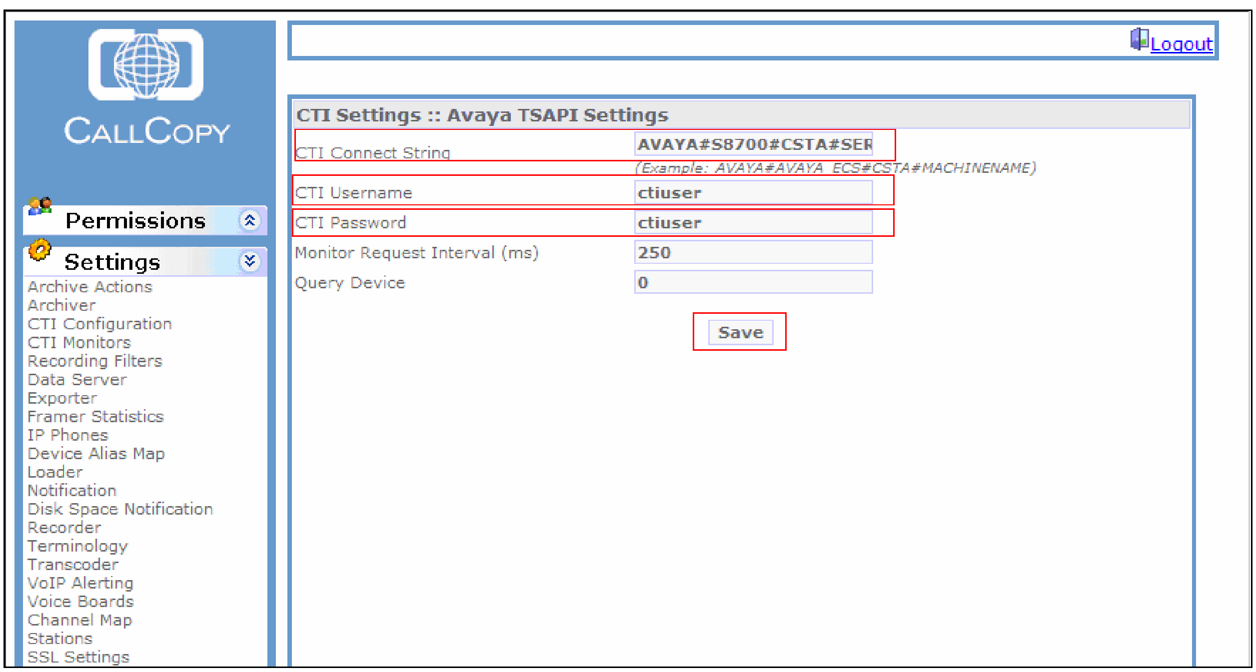


©2007 Avaya Inc. All Rights Reserved.

The following shows the CTI Settings screen. Using the drop-down menu, select **Avaya TSAPI**. Click the **Next** button.

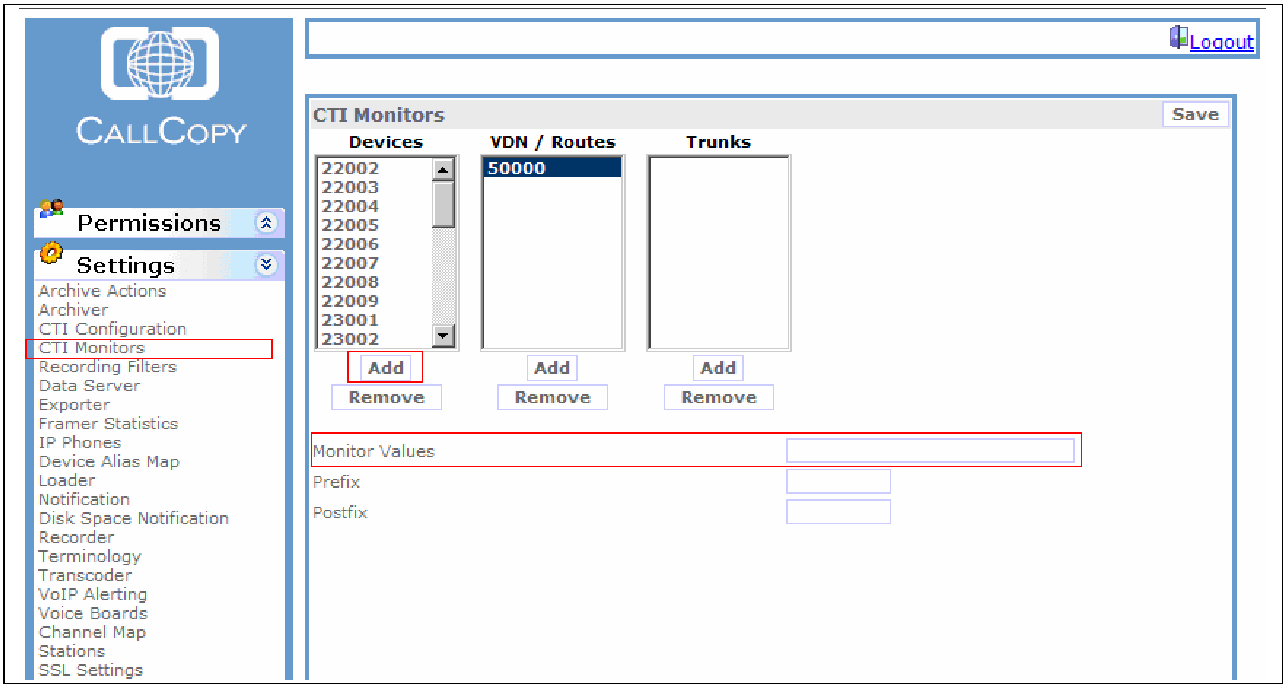


From the Avaya TSAPI Settings screen, provide the TLink name used in AES for the CTI Connect String field. Provide an appropriate CTI username and password that were created in **Section 4.3**. Click the **Save** button.



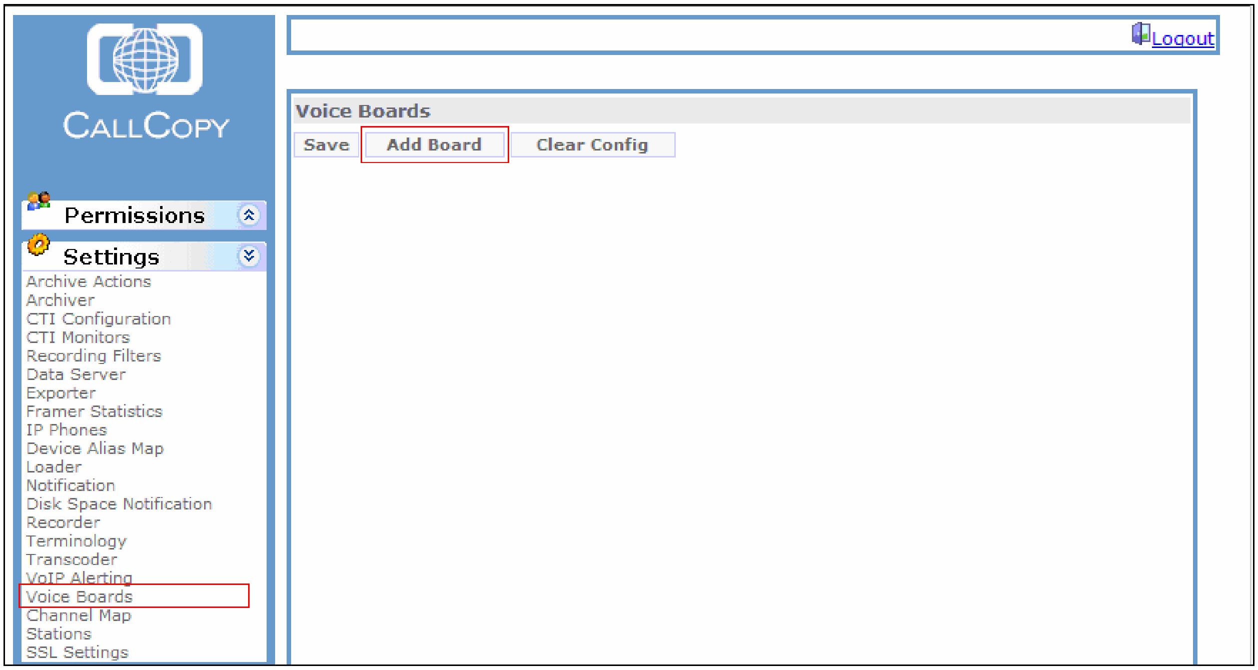
©2007 Avaya Inc. All Rights Reserved.

Select **CTI Monitor** link under the Settings section. To add any device to be monitored for recording, enter the extension in the Monitor Values field, and click the **Add** button under the Devices section. Same procedures apply for monitoring VDN/Routes and Trunks.
After completion of entering monitors, click the **Save** button at the bottom of the screen (not shown here).

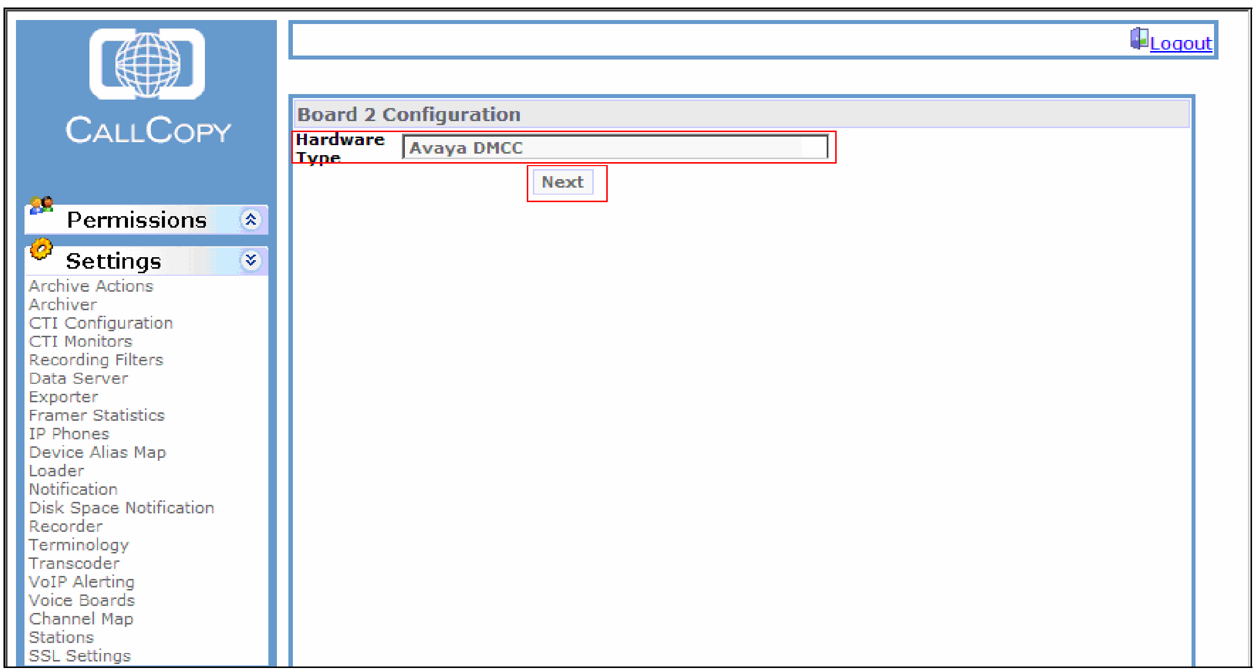


©2007 Avaya Inc. All Rights Reserved.

Select **Voice Boards** link under the Settings section. To add a new board, click **Add Board**.



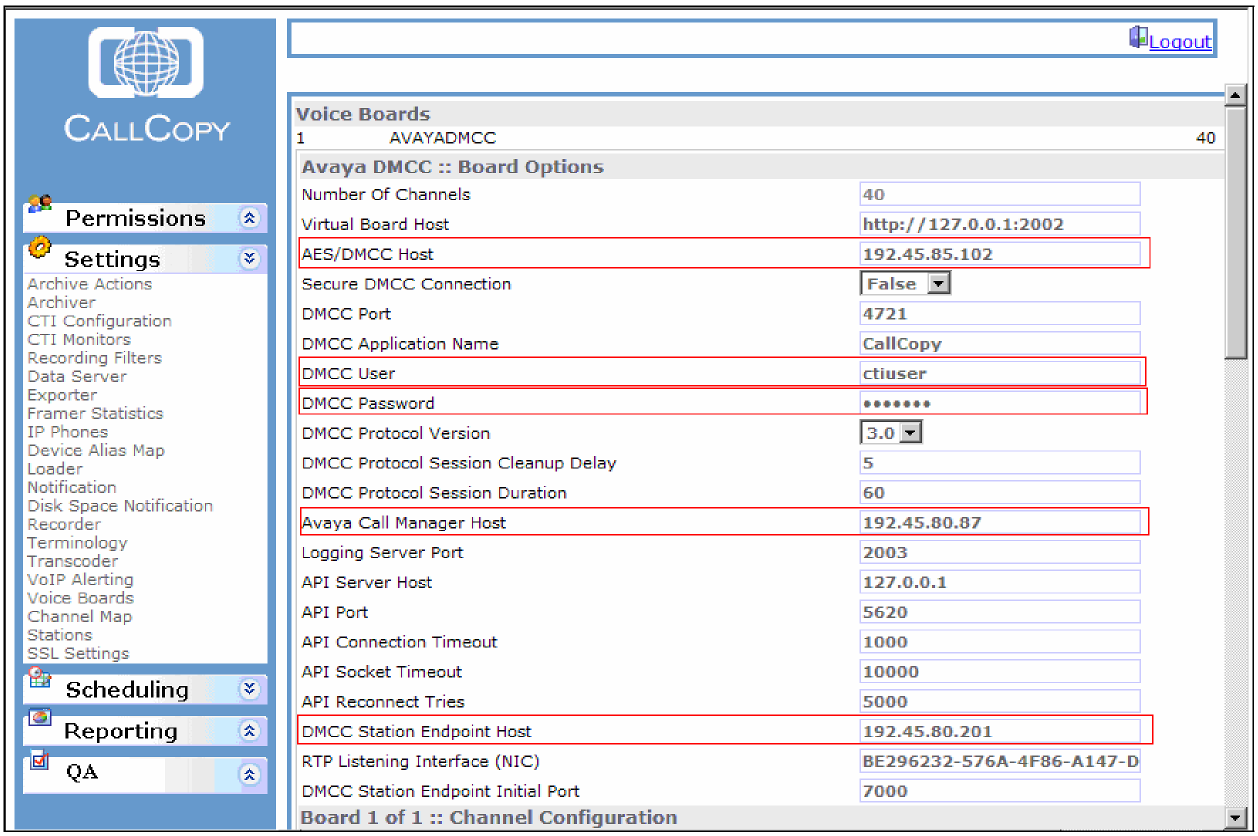
Enter a descriptive Name for the Hardware Type field, and click **Next**.



The highlighted fields on the following screen were configured for the compliance test.

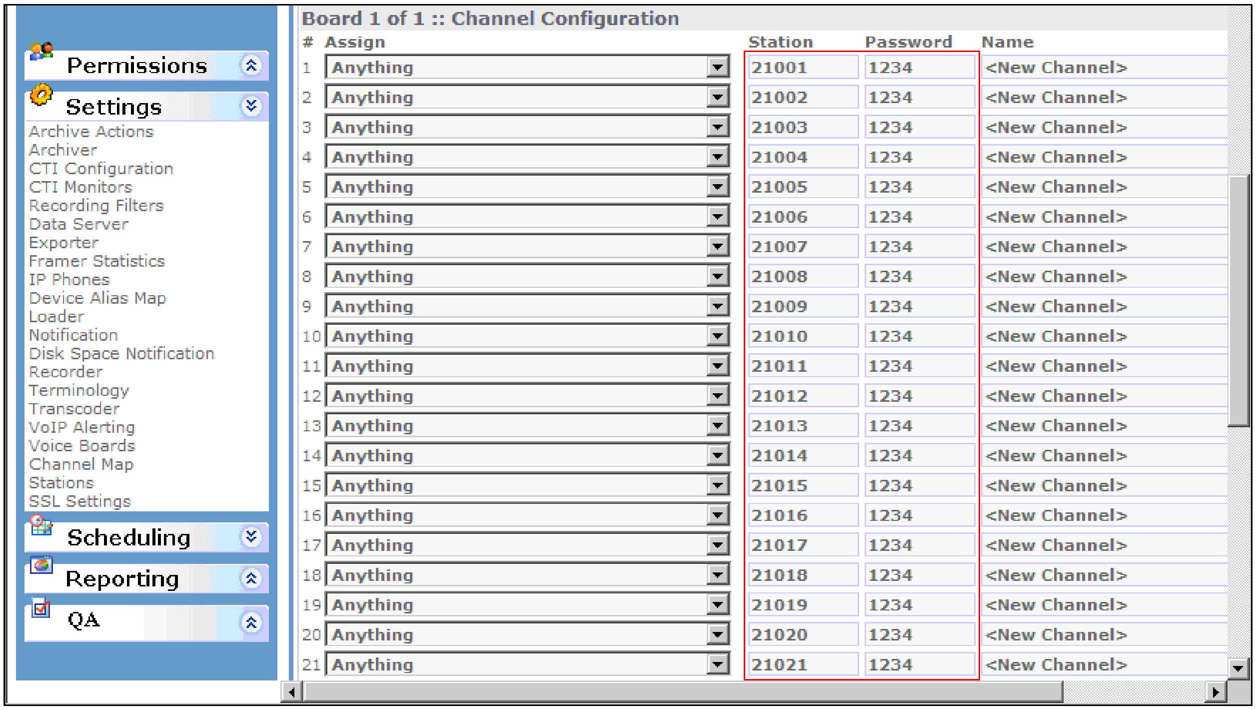
- AES/DMCC Host - IP address of the AES/DMCC host.
- DMCC User - DMCC username used for authenticating with Avaya AES during the DMCC session startup.
- DMCC Password - DMCC password used for authenticating with Avaya AES during the DMCC session startup.
- Avaya Call Manager Host - CLAN (or procr) IP address of Avaya Communication Manager.
- DMCC Station Endpoint Host - IP address that will be receiving the RTP/RTCP traffic from the Call Manager. This will be the server running the Avaya DMCC Integration (usually the CallCopy Server). You must enter the actual IP address of the server – do not use localhost or 127.0.0.1.

Default values may be used for all other fields.



©2007 Avaya Inc. All Rights Reserved.

The following screen is a continuation of the previous screen. Enter all recording stations and a password for each station.



6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability, and performance testing. The feature testing evaluated the ability of CallCopy cc:Discover to monitor and record calls placed to and from stations and agents. The serviceability testing introduced failure scenarios to see if CallCopy cc:Discover could resume recording after failure recovery. The performance testing stressed CallCopy cc:Discover by continuously placing calls over extended periods of time.

6.1. General Test Approach

All test cases were performed manually. The general approach was to place various types of calls to and from stations, and agents. These trunk calls were then monitored and recorded using CallCopy cc:Discover. The recordings were verified for each call. For feature testing, the types of calls included inbound and outbound trunk calls, transferred calls, bridged calls, and conferenced calls. Performance tests verified that CallCopy cc:Discover could record calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, busyouts/releases of the trunk group, and resets were applied.

©2007 Avaya Inc. All Rights Reserved.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

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

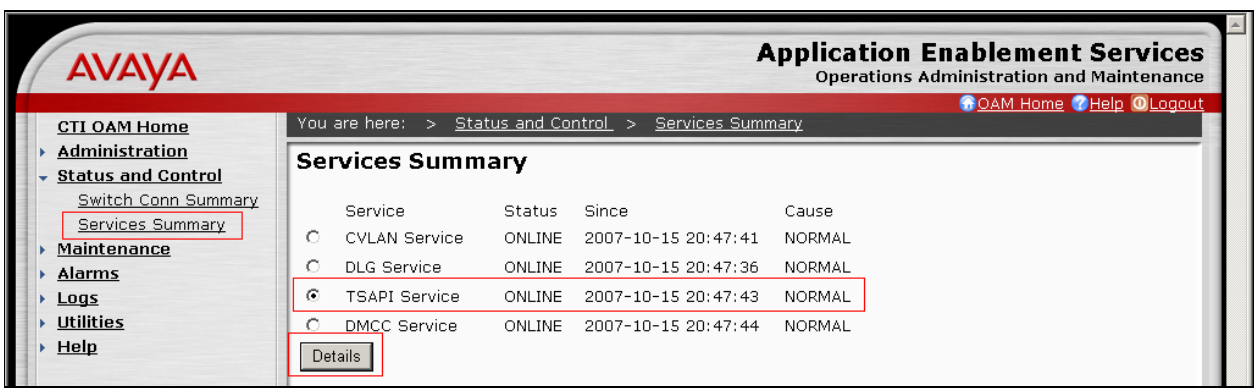
7.1. Verify Avaya Communication Manager

Verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify the Service State is "**established**" for the CTI link number administered in **Section 3.6**, 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              no                     down         0        0
2              no    server1          restarting   15       15
3              no                     down         0        0
4     4        no    server1          established  15       15
5              no                     down         0        0
6              no                     down         0        0
```

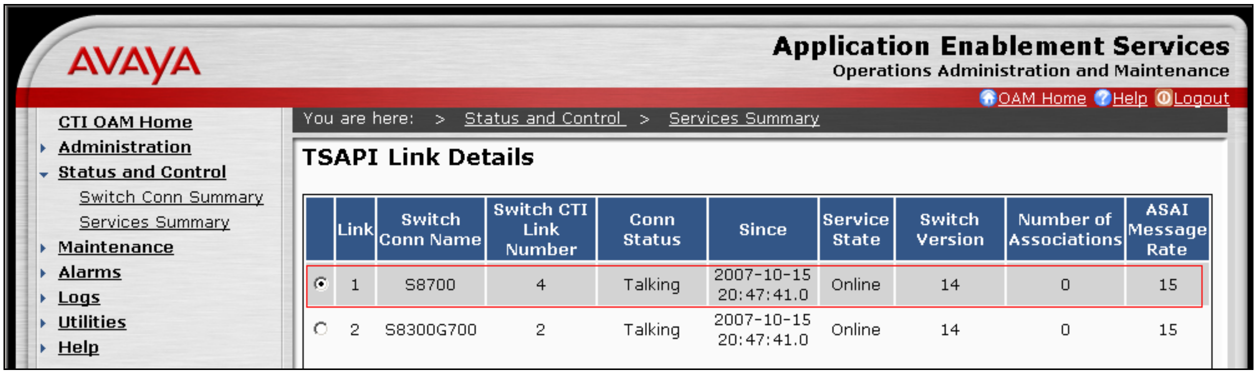
7.2. Verify Avaya Application Enablement Services

From the AES CTI OAM Admin web pages, verify the status of the TSAPI link by selecting **Status and Control → Services Summary** from the left pane. Select the radio button for TSAPI Service, and click **Details**.



©2007 Avaya Inc. All Rights Reserved.

The **TSAPI Link Details** screen is displayed. Verify that the **Conn Status** is "Talking", as shown below.



8. Support

Technical support on the cc:Discover can be obtained through the following:

- **Phone:** (888) 922-5526 (Option 2)
- **Web:** http://support.callcopy.com or http://www.callcopy.com/support

9. Conclusion

These Application Notes describe the configuration steps required for CallCopy cc:Discover (Version 3.6.0.215) to interoperate with Avaya Communication Manager 4.0.1 (R014x.00.1.731.2) and Avaya Application Enablement Services 4.0 (Bundled Offer Build 47.3). All feature and serviceability test cases were completed.

10. Additional References

This section references the Avaya and CallCopy product documentation that is relevant to these Application Notes.

[1] *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 3.1, February 2007, available at http://support.avaya.com.
[2] *CallCopy Avaya DMCC Integration.*
[3] *CallCopy Avaya TSAPI Integration.*

©2007 Avaya Inc. All Rights Reserved.

©2007 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.