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

Abstract

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

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 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 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 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 softphone 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.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on feature functionality, serviceability, and performance. The feature functionality testing evaluated the ability of CallCopy cc:Discover to monitor and record calls placed to and from stations on Communication Manager. The serviceability testing introduced failure conditions to see if cc:Discover could properly resume recording calls after each failure recovery. The performance testing stressed cc:Discover by continuously placing calls over extended periods of time.

The compliance testing validated the monitoring and recording performed by cc:Discover of calls placed to and from analog phones, digital phones, IP phones, softphones, agents, Vector Directory Numbers (VDNs), and hunt groups on an Avaya Aura^{TM} Media Server running Communication Manager.

1.2. Support

Technical support for CallCopy cc:Discover can be obtained by contacting CallCopy at:

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

2. Reference Configuration

The figure below shows the configuration used during compliance testing. Site A is comprised of an Avaya S8500 Media Server with an Avaya G650 Media Gateway. Site B is comprised of an Avaya S8300 Media Server with an Avaya G450 Media Gateway. The two Communication Manager systems are connected to each other via an IP (H.323) trunk and an ISDN-PRI trunk. The various telephones shown are used to generate intra-switch calls (calls between telephones on the same system), outbound/inbound calls to/from the PSTN, and inter-switch calls (calls between the two Communication Manager systems via the two trunks). The CallCopy cc:Discover server is set up to record calls at Site A.

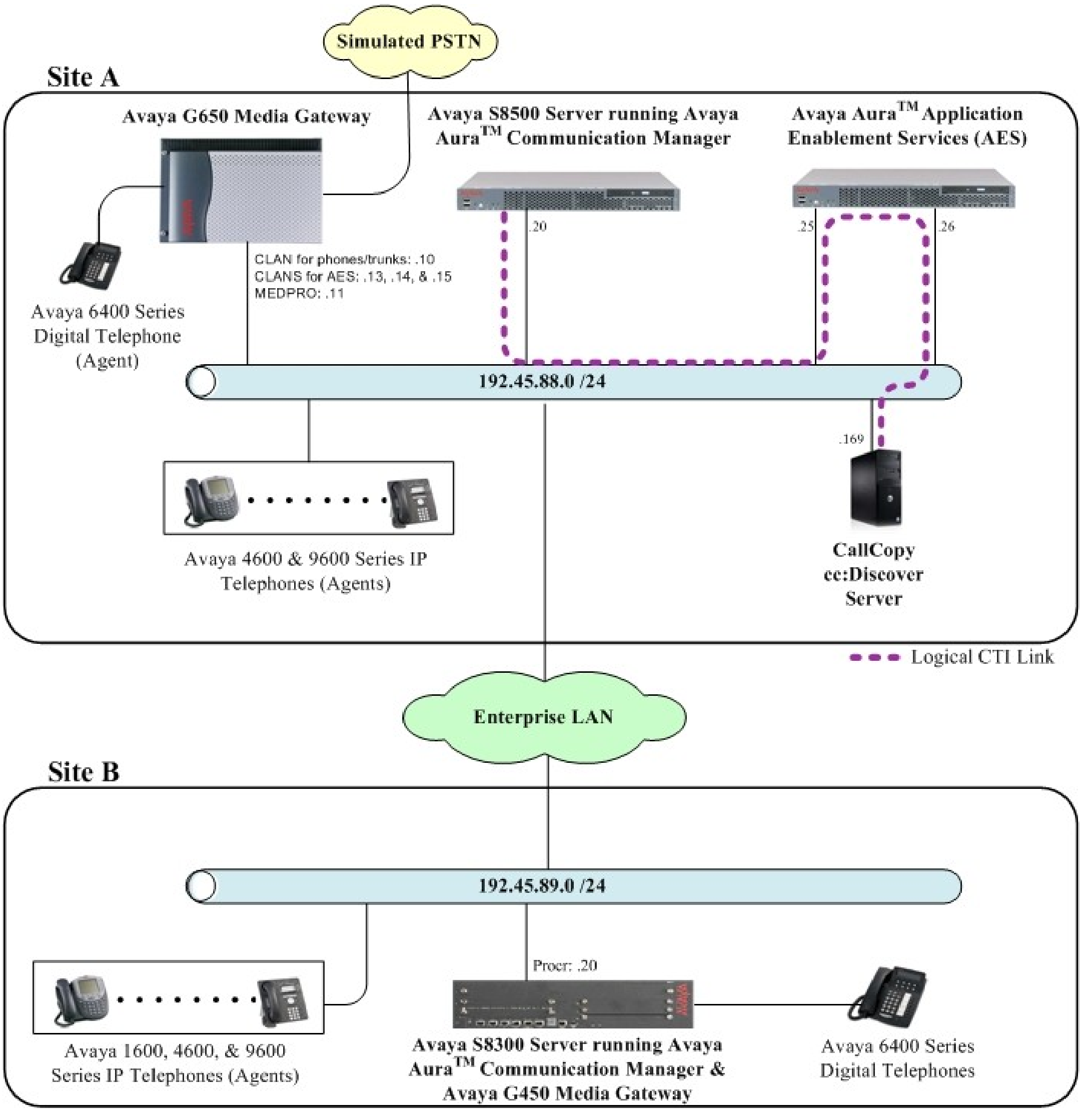

Simulated PSTN
Site A
Avaya G650 Media Gateway
Avaya S8500 Server running Avaya Aura™ Communication Manager
Avaya Aura™ Application Enablement Services (AES)
.20
.25
.26
CLAN for phones/trunks: .10
CLANS for AES: .13, .14, & .15
MEDPRO: .11
Avaya 6400 Series Digital Telephone (Agent)
192.45.88.0 /24
.169
Avaya 4600 & 9600 Series IP Telephones (Agents)
CallCopy cc:Discover Server
Logical CTI Link
Enterprise LAN
Site B
192.45.89.0 /24
Procr: .20
Avaya 1600, 4600, & 9600 Series IP Telephones (Agents)
Avaya S8300 Server running Avaya Aura™ Communication Manager & Avaya G450 Media Gateway
Avaya 6400 Series Digital Telephones

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

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server (w/ G650)	Avaya Aura^{TM} Communication Manager 5.2 (R015x.02.0.947.3)
Avaya S8300 Server (w/ G450)	Avaya Aura^{TM} Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G650 Media Gateway: TN799DP (C-LAN) TN2602AP (MEDPRO) TN2312BP (IPSI)	 HW01, FW026 HW02, FW007 HW15, FW030
Avaya G450 Media Gateway : MM710BP (DS1) MM712AP (DCP)	 HW11, FW044 HW07, FW009
Avaya Aura^{TM} Application Enablement Services (AES) Server	4.2
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Avaya 1600 Series IP Phones : 1608SW (H.323) 1616SW (H.323)	 1.0.3 1.0.3
Avaya 4600 Series IP Phones: 4610SW (H.323) 4620SW (H.323) 4621SW (H.323)	 2.9 2.9 2.9
Avaya 9600 Series IP Phones: 9620 (H.323)	 2.0.0
Avaya 6400 Series Digital Phones	-
CallCopy cc:Discover Server	3.0.0
CallCopy cc:Discover Client	3.0.0

4. Configure Communication Manager

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Communication Manager, refer to the Avaya product documentation, **Reference [1].**

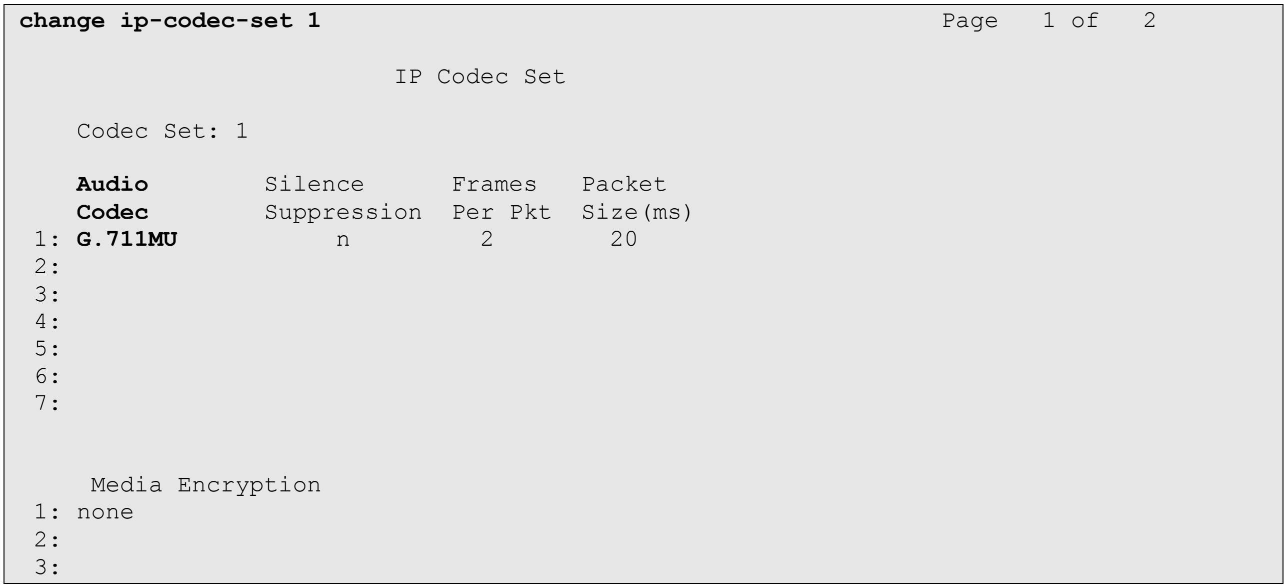
The information shown on the screens throughout this section indicate the values that were used during compliance testing.

4.1. Configure IP Codec Sets & IP-Network Regions

This section provides the steps required for configuring an ip-codec-set and ip-network regions.

1. Enter the **change ip-codec-set <codec set number>** command, where **<codec set number>** is the codec set number to be used with the CallCopy recording solution.

    - In the **Audio Codec** field, type **G.711MU**.



```
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:
 4:
 5:
 6:
 7:


     Media Encryption
 1: none
 2:
 3:
```

2. Enter the **change ip-network-region <region number>**, where **<region number>** is the ip network region number to be used with the CallCopy recording solution.

   - In the **Code Set** field, type **<codec set number>**, where **<codec set number>** is the number of the codec set administered in **Step 1**. The **Codec Set** field reflects the codec set that must be used for connections between phones within this region or between phones and media processor boards within this region.

```
change ip-network-region 1                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: dev8.com
    Name: interop
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: 65535
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 48      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 48       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
```

During compliance testing, two IP Network regions were used. It is best practice for all CLANs dedicated to AE Services to be in a separate network region from those CLANs servicing endpoints (i.e. phones). For compliance testing, a single CLAN in network region 1 was used to service endpoints, while 3 CLANs in network region 2 were dedicated to Application Enablement Services. Both IP network regions were configured to use IP codec set 1.

4.2. Configure Connectivity to AES and Endpoints

This section provides the steps required for configuring connectivity from Communication Manager to Application Enablement Services and endpoints.

The Application Enablement Services server communicates with Communication Manager by using one or more CLANs to create a switch connection. The following steps show only the configuration required in Communication Manager to set up a switch connection. See **Section 5.1** for the configuration steps required in Application Enablement Services to complete the administration of the switch connection.

1. Enter the **change node-names ip** command.

- In the **Name** field, type a descriptive name to assign to a CLAN to be administered.
- In the **IP Address** field, type the IP address that will be assigned to the CLAN.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
8300                192.45.89.20
CLAN                192.45.88.10
CLAN2               192.45.88.13
CLAN3               192.45.88.14
CLAN4               192.45.88.15
LSP-8300            192.45.88.30
Member-CDR          192.168.199.69
RDTT-CDR            192.45.88.45
SES                 192.45.88.50
cf-medpro           192.45.88.11
default             0.0.0.0
ipoffice            192.45.88.40
procr               192.45.88.20
```

Repeat this step for each CLAN.

In the compliance tested configuration, the **CLAN** node was used for registering endpoints and the **CLAN2**, **CLAN3**, and **CLAN4** nodes were used for connectivity to Application Enablement Services.

2. Enter the **add ip-interface <board location>** command, where **<board location>** is the board location for the CLAN, for example: 01A02.

   - In the **Enable Interface** field, type **y**.
   - In the **Network Region** field, type the network region number administered in **Section 4.1**.
   - In the **Node Name** field, type **<CLAN name>**, where **<CLAN name>** is the **Name** from **Step 1**.
   - In the **Ethernet Link** field, type an available Ethernet link number.

```
add ip-interface 01a08                                          Page   1 of   3
                                  IP INTERFACES


                  Type: C-LAN
                  Slot: 01A02        Target socket load and Warning level: 400
           Code/Suffix: TN799  D           Receive Buffer TCP Window Size: 8320
      Enable Interface? y                           Allow H.323 Endpoints? y
                  VLAN: n                            Allow H.248 Gateways? y
        Network Region: 1                             Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: CLAN
           Subnet Mask: /24
     Gateway Node Name:

         Ethernet Link: 1
```

Repeat this step for each CLAN

In the compliance tested configuration, the **CLAN** node was assigned to network region 1 and the **CLAN2**, **CLAN3**, and **CLAN4** nodes were assigned to network region 2.

3. Enter the **change ip-services** command.

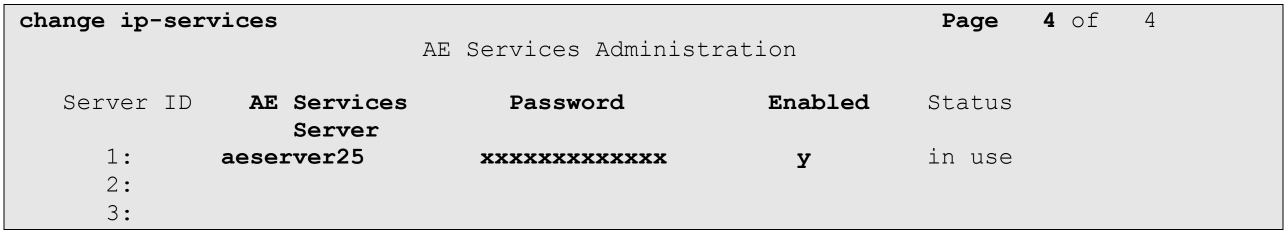
   - In the **Service Type** field, type **AESVCS**.
   - In the **Enabled** field, type **y**.
   - In the **Local Node** field type **<nodename>**, where **<nodename>** is the name of the CLAN board used for connectivity to Application Enablement Services.
   - In the **Local Port** field, accept the default port (**8765**).

```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      CLAN2            8765
AESVCS        y      CLAN3            8765
AESVCS        y      CLAN4            8765
```

Repeat this step for each CLAN used for connectivity to Application Enablement Services.

On **Page 4**,

- In the **AE Services Server** field, type the **<name>** of the Application Enablement Services server. On the Application Enablement Services server, the name can be obtained by typing "uname –n" at the command prompt. The name entered on Communication Manager must match the Application Enablement Services server name exactly.
- In the **Password** field, enter an alphanumeric password. The passwords must exactly match on both Communication Manager and the Application Enablement Services (administered in **Section 5.1**).
- In the **Enabled** field, type **y**.



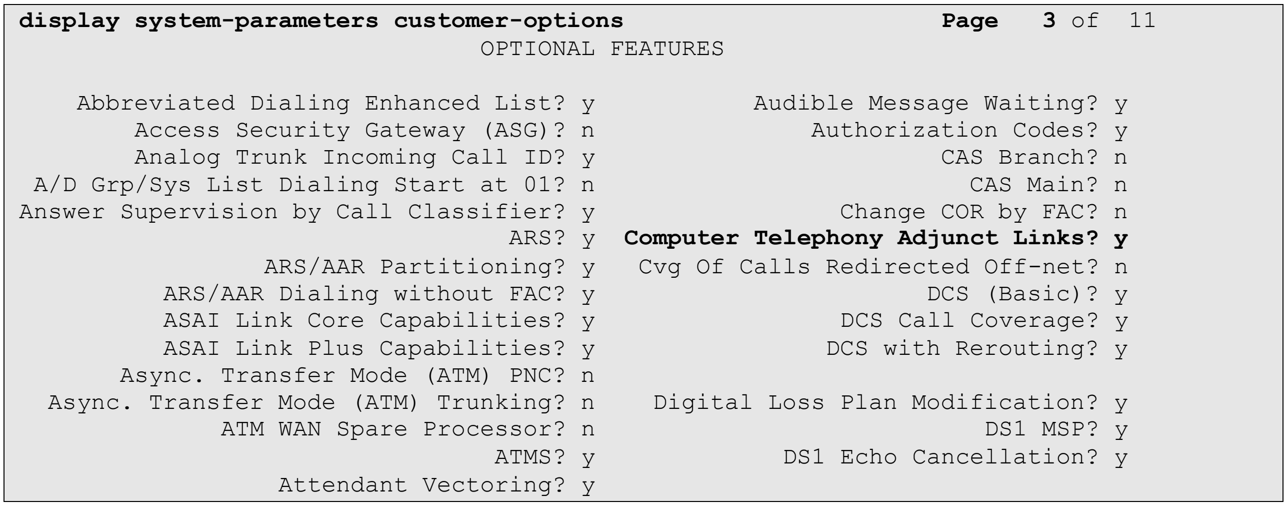
```
change ip-services                                            Page   4 of   4
                           AE Services Administration

   Server ID    AE Services        Password           Enabled    Status
                   Server
      1:      aeserver25       xxxxxxxxxxxxx          y        in use
      2:
      3:
```

4.3. Configure CTI Link

This section provides the steps required for configuring a CTI link on Communication Manager. See **Section 5.3** for the configuration steps required on Application Enablement Services to complete the administration.

1. Enter the **display system-parameters customer-options** command.

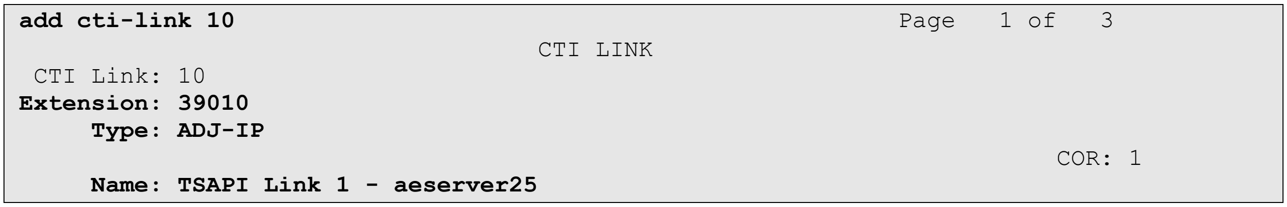
   - On **Page 3**, verify that the **Computer Telephony Adjunct Links** field is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.



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

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                          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? n
          ARS/AAR Dialing without FAC? y                       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
```

2. Enter **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

   - In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
   - In the **Type** field, type **ADJ-IP**.
   - In the **Name** field, type a descriptive name.



```
add cti-link 10                                              Page   1 of   3
                                    CTI LINK
 CTI Link: 10
Extension: 39010
     Type: ADJ-IP
                                                                        COR: 1
     Name: TSAPI Link 1 - aeserver25
```

4.4. Configure Stations (DMCC Recording Devices)

This section provides the steps required for configuring stations on Communication Manager that will function as recording devices for CallCopy cc:Discover.

For the purpose of this document, devices that have been registered using the DMCC service will be called "DMCC devices". When a client application registers itself as a DMCC device at an extension, it can act like an IP softphone to control and monitor physical aspects of the extension (button pushes, lamps, the display, etc.) or access and control the media streams at the extension. For a client application to be able to control the media at an extension, and record calls at that extension, it must register itself as a DMCC device with the media mode set to "Client". Client media mode indicates that the client application will handle the media streams from the DMCC device. DMCC devices that have been registered in Client media mode will be called "DMCC recording devices".

The DMCC recording devices used by CallCopy cc:Discover are administered as IP softphones on Avaya Communication Manager. Each DMCC recording device requires either an "IP_API_A" license on Communication Manager or a "VALUE_DMCC_DMC" license on Application Enablement Services.

Note that these licenses are separate and independent from the Avaya IP Softphone licenses required on Communication Manager for Avaya IP Softphones, but not for DMCC recording devices.

1. Enter the **display system-parameters customer-options** command to verify that there are sufficient **IP_API_A** licenses for the DMCC recording devices. 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       : 1000           0
IP_API_B       : 1000           0
IP_API_C       : 1000           0
IP_Agent       : 1000           0
IP_IR_A        : 0              0
IP_Phone       : 2400           3
IP_ROMax       : 2400           0
IP_Soft        : 2              0
IP_eCons       : 0              0
oneX_Comm      : 2400           0
               : 0              0
```

2. Enter the **add station <extension>** command, where **<extension>** is a valid station extension.

   - In the **Type** field, type an IP telephone set type with configurable buttons; for example, **4620**.
   - In the **Security Code**, type the value entered for **<extension>** (the station extension and security code must match).
   - In the **Name** field, type a descriptive name.
   - In the **IP SoftPhone**, type **y**.

```
add station 31126                                               Page   1 of   5
                                     STATION

Extension: 31126                         Lock Messages? n               BCC: 0
     Type: 4620                          Security Code: 31126            TN: 1
     Port: IP                          Coverage Path 1:                 COR: 1
     Name: DMCC Softphone              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: 31126
            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? n


                                              Customizable Labels? Y
```

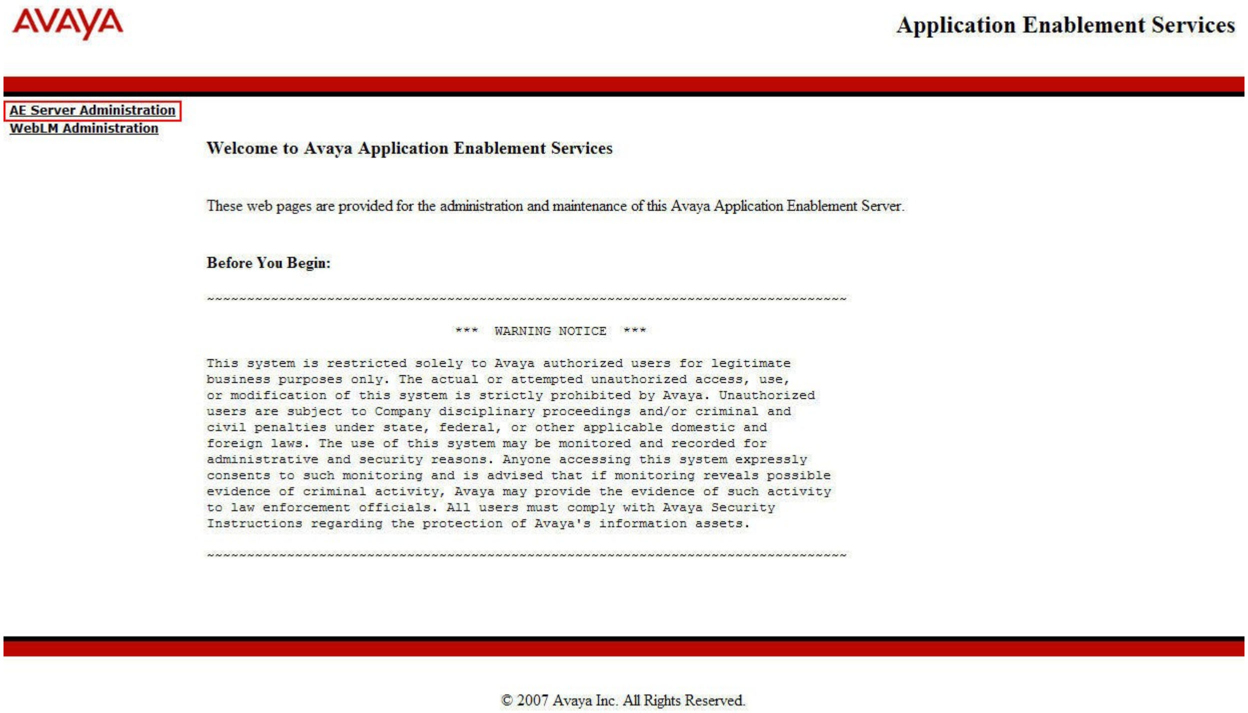
This completes the Avaya Aura^{TM} Communication Manager configuration.

5. Configure Application Enablement Services

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

This section assumes that the installation and basic administration of the Application Enablement Services server has already been performed. For more information on administering Application Enablement Services, refer to the Avaya product documentation, **Reference [2]**.

1. Launch a web browser and enter https://<IP address of AES Server> in the address field. Click **AE Server Administration**.



Welcome to Avaya Application Enablement Services

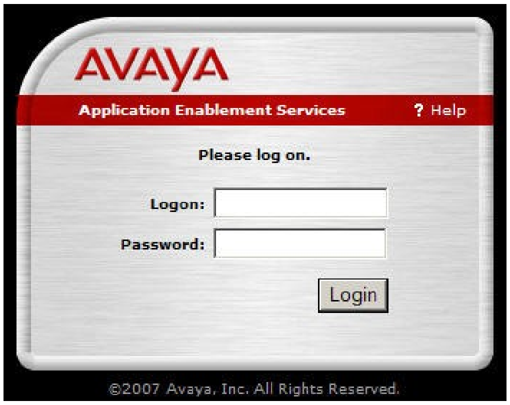
These web pages are provided for the administration and maintenance of this Avaya Application Enablement Server.

Before You Begin:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

                                ***  WARNING NOTICE  ***

This system is restricted solely to Avaya authorized users for legitimate
business purposes only. The actual or attempted unauthorized access, use,
or modification of this system is strictly prohibited by Avaya. Unauthorized
users are subject to Company disciplinary proceedings and/or criminal and
civil penalties under state, federal, or other applicable domestic and
foreign laws. The use of this system may be monitored and recorded for
administrative and security reasons. Anyone accessing this system expressly
consents to such monitoring and is advised that if monitoring reveals possible
evidence of criminal activity, Avaya may provide the evidence of such activity
to law enforcement officials. All users must comply with Avaya Security
Instructions regarding the protection of Avaya's information assets.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

© 2007 Avaya Inc. All Rights Reserved.

2. Log in with the appropriate credentials for accessing the Application Enablement Services CTI OAM web pages.



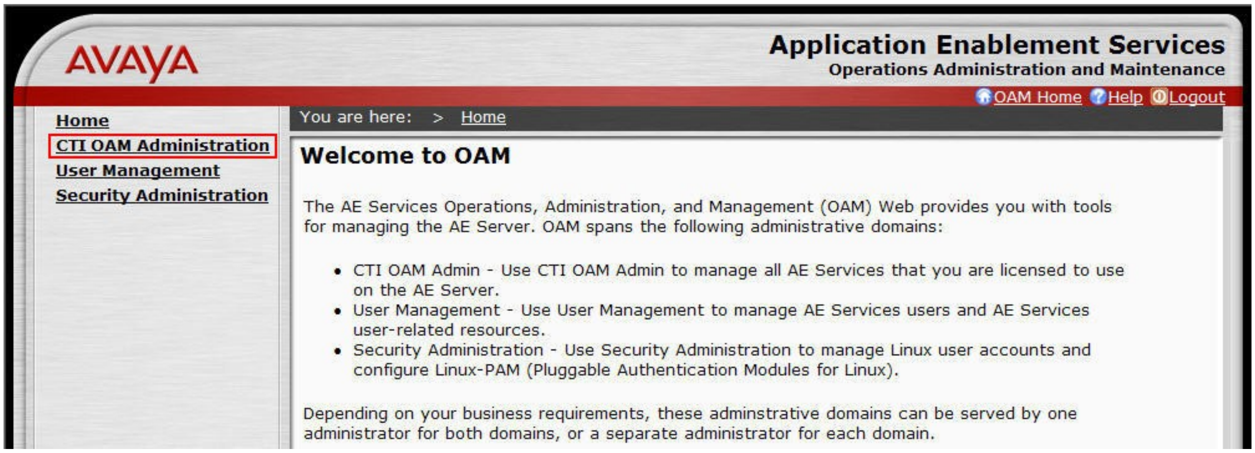
Please log on.

Logon:

Password:

©2007 Avaya, Inc. All Rights Reserved.

3. Click **CTI OAM Administration** in the left pane menu.



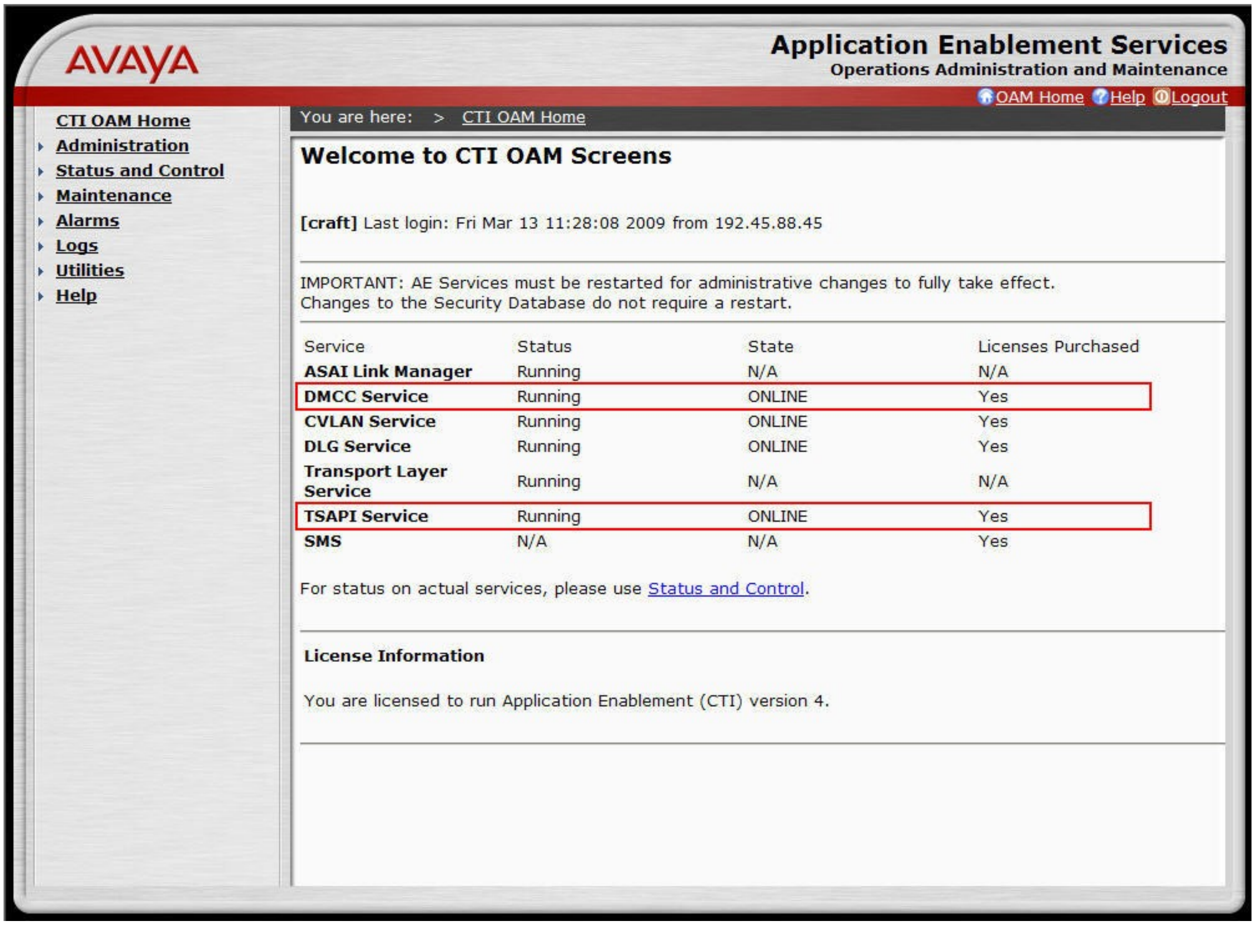
Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Security Administration - Use Security Administration to manage Linux user accounts and configure Linux-PAM (Pluggable Authentication Modules for Linux).

Depending on your business requirements, these adminstrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

4. Verify that Application Enablement Services is licensed for the TSAPI and DMCC services. If these services are not licensed, contact an authorized Avaya account representative to obtain these licenses.



Welcome to CTI OAM Screens

[craft] Last login: Fri Mar 13 11:28:08 2009 from 192.45.88.45

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	Licenses Purchased
ASAI Link Manager	Running	N/A	N/A
DMCC Service	Running	ONLINE	Yes
CVLAN Service	Running	ONLINE	Yes
DLG Service	Running	ONLINE	Yes
Transport Layer Service	Running	N/A	N/A
TSAPI Service	Running	ONLINE	Yes
SMS	N/A	N/A	Yes

For status on actual services, please use Status and Control.

License Information

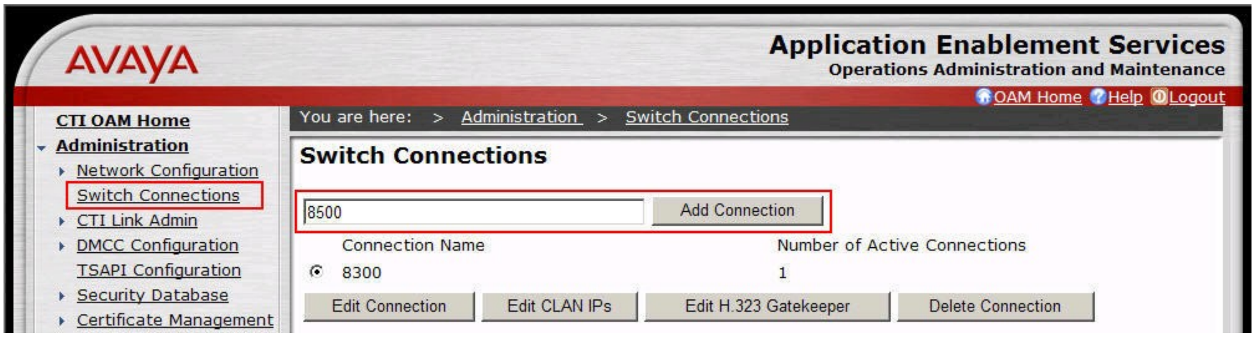
You are licensed to run Application Enablement (CTI) version 4.

5. Each DMCC recording device used by CallCopy cc:Discover requires either an "IP_API_A" license on Avaya Communication Manager or a "VALUE_DMCC_DMC" license on Application Enablement Services. If "VALUE_DMCC_DMC" licenses are being used, log in to the Avaya Web License Manager (WebLM) and verify that there are sufficient licenses for the DMCC recording devices. Additionally, verify there are sufficient TSAPI licenses to monitor and control Communication Manager resources for call events and Single Step Conferencing. If not, contact an authorized Avaya account representative to obtain these licenses.

5.1. Configure a Switch Connection

This section provides the steps required for configure a Switch Connection. A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager.

1. Select **Administration > Switch Connections** from the left pane menu. In the **Add Connection** field, type a descriptive name and click **Add Connection**.

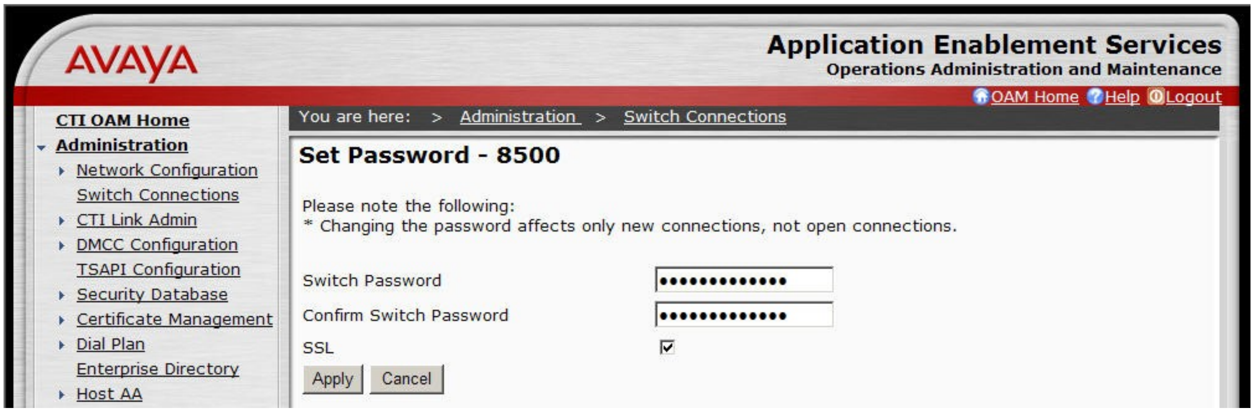


Switch Connections

8500

	Connection Name	Number of Active Connections
●	8300	1

2. In the **Switch Password** field, type the password that was entered during **Step 3** of **Section 4.2**. Re-type the password in the **Confirm Switch Password** field. Leave **SSL** checked if using a secure connection to Communication Manager. Click **Apply**.



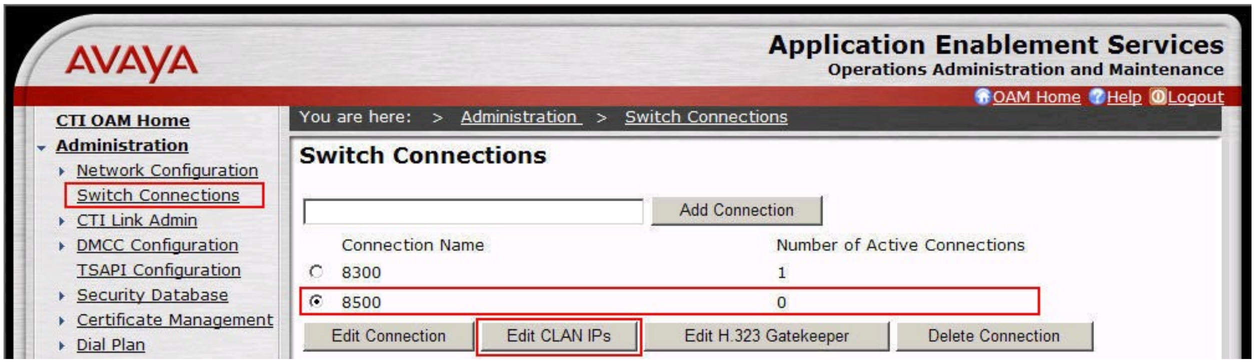
Set Password - 8500

Please note the following:
* Changing the password affects only new connections, not open connections.

Switch Password ••••••••••••••
Confirm Switch Password ••••••••••••••
SSL ☑

OAM adds the switch connection and returns to the "Switch Connections" page.

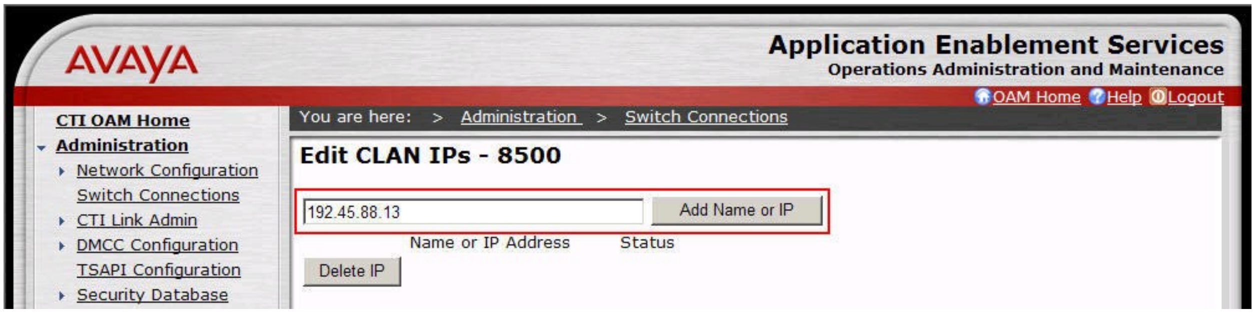
3. From the "Switch Connections" page, select the newly added switch connection, and click **Edit CLAN IPs**.



Switch Connections

	Connection Name	Number of Active Connections
○	8300	1
●	8500	0

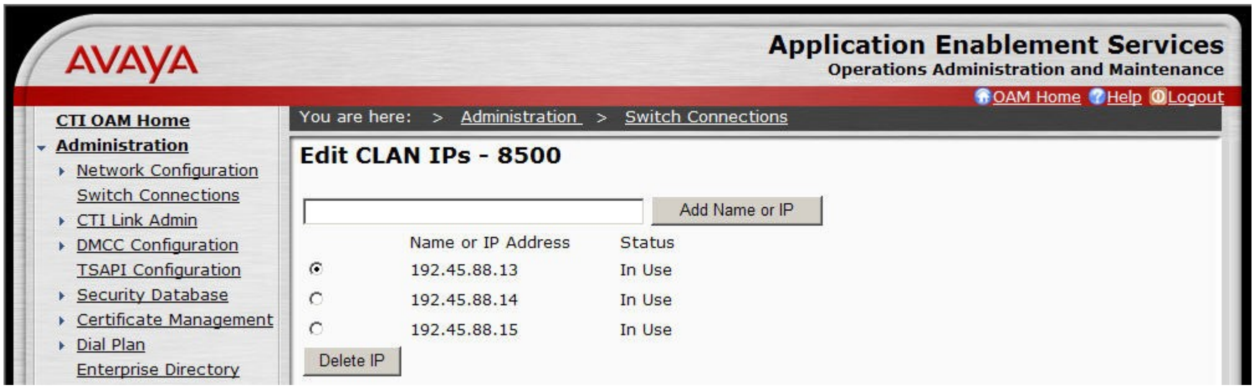
4. In the **Add Name or IP** field, type the **<Host Name>** or the **<IP Address>** of the CLAN, and click **Add Name or IP** (use the Host Name or IP address of the CLAN that was administered for Application Enablement Services connectivity in **Section 4.2**).



Edit CLAN IPs - 8500

192.45.88.13

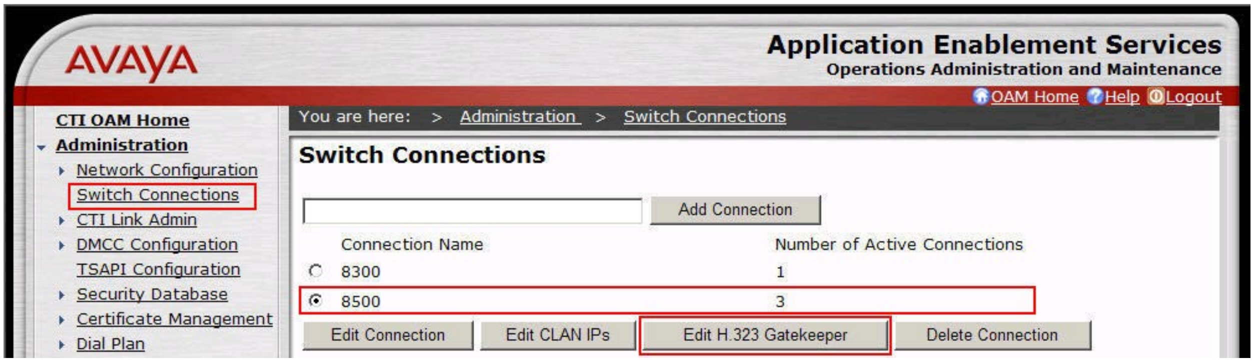
Repeat this step for each CLAN. The screen below shows the CLANs that were used during compliance testing.



Edit CLAN IPs - 8500

	Name or IP Address	Status
●	192.45.88.13	In Use
○	192.45.88.14	In Use
○	192.45.88.15	In Use

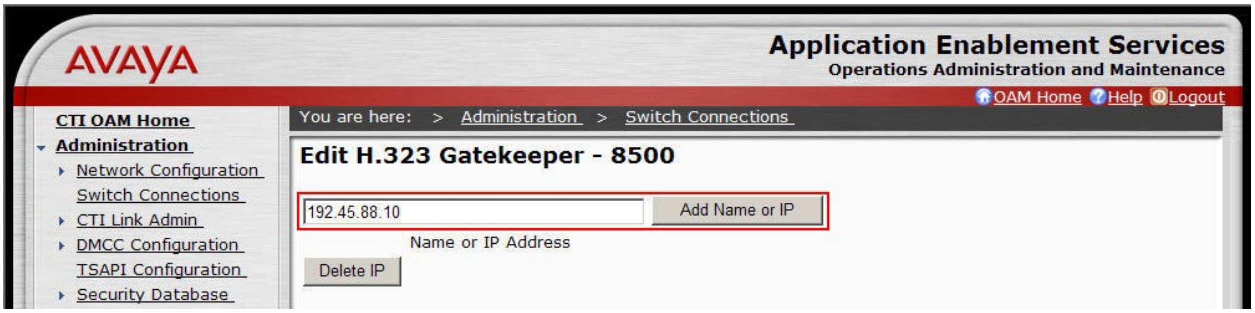
5. Navigate back to **Administration > Switch Connections**. Select the switch connection, and click **Edit H.323 Gatekeeper**.



Switch Connections

	Connection Name	Number of Active Connections
○	8300	1
●	8500	3

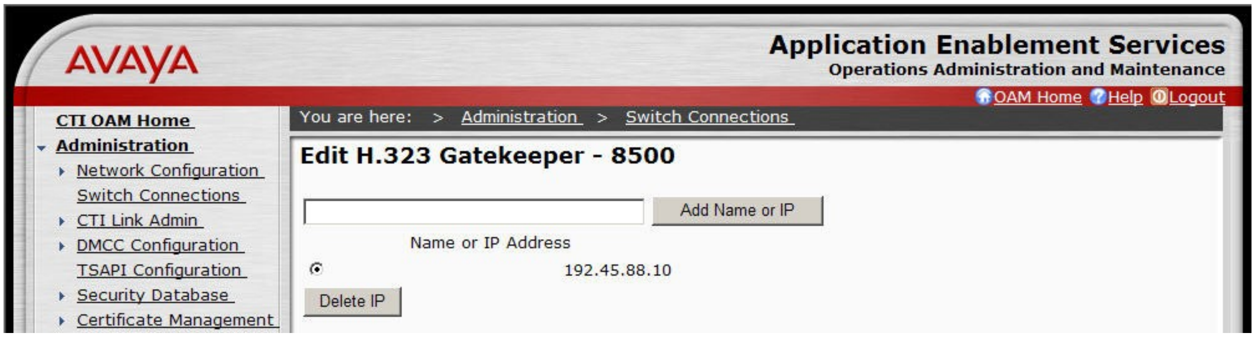
6. In the **Add Name or IP** field, type the **<Host Name>** or **<IP address>** of the CLAN to be used. Click **Add Name or IP**.



Edit H.323 Gatekeeper - 8500

192.45.88.10

Repeat this step as necessary to add multiple H.323 Gatekeepers. The screen below shows the CLANs that were used during compliance testing.



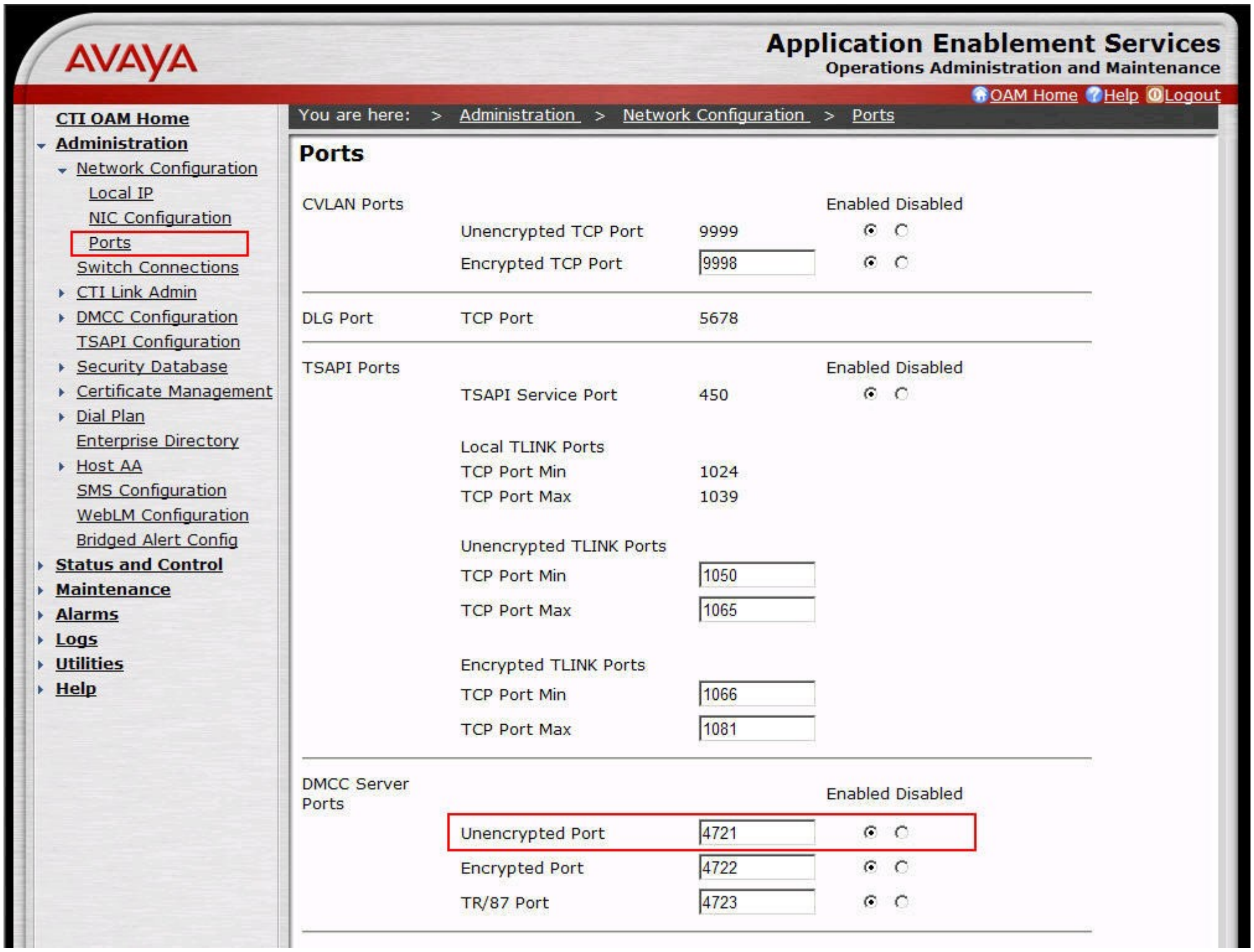
Edit H.323 Gatekeeper - 8500

	Name or IP Address
●	192.45.88.10

5.2. Configure DMCC Server Ports

This section provides the steps required for configuring DMCC server ports.

1. Navigate to the **CTI OAM Home > Administration > Ports** page. During compliance testing, the default port values shown in the screen below were utilized. Since the unencrypted port was utilized during the compliance test, set the **Unencrypted Port** field to **Enabled**. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



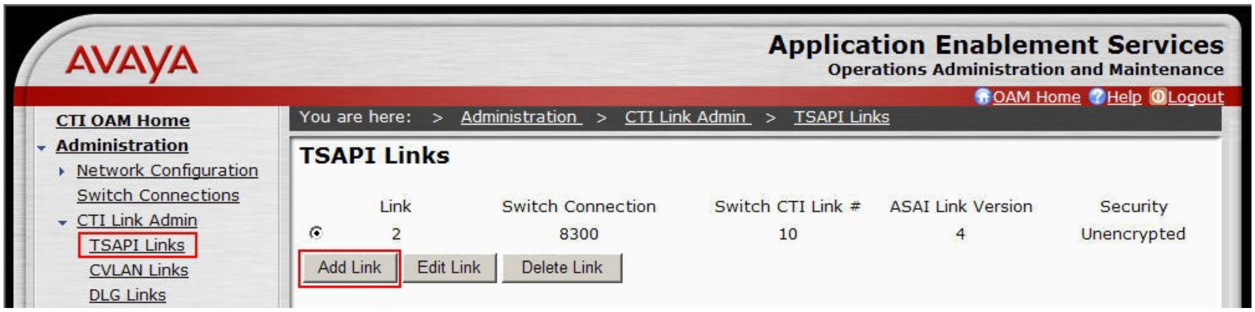
Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

5.3. Configure TSAPI Link

This section provides the steps required for configuring a TSAPI Link.

1. From the CTI OAM main menu select **Administration > CTI Link Admin > TSAPI Links**. Click **Add Link**.

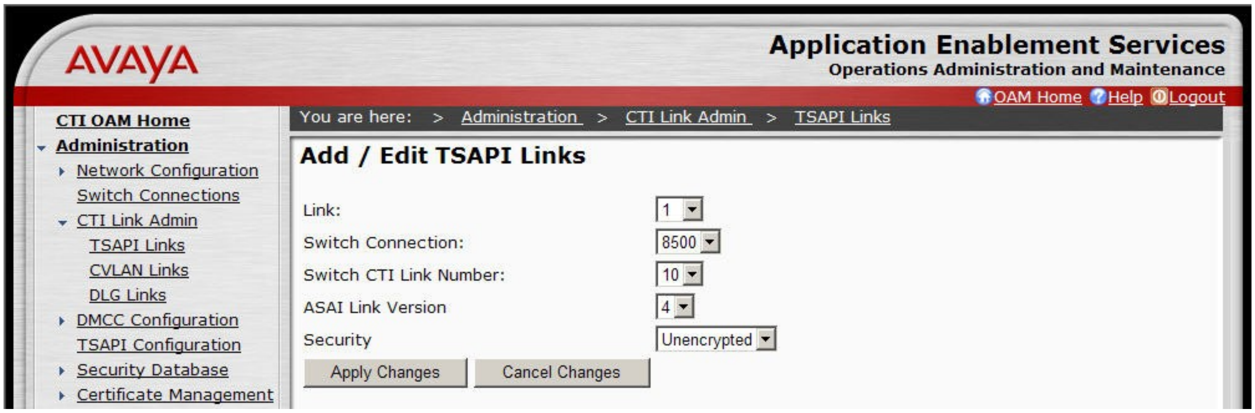


TSAPI Links

	Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
●	2	8300	10	4	Unencrypted

2. Complete the "Add / Edit TSAPI Links" page as follows:

- In the **Link** field, select an available link number.
- In the **Switch Connection** field, select the switch connection configured in **Section 5.1**.
- In the **Switch CTI Link Number** field, select the CTI link number that was administered on Communication Manager in **Step 2** of **Section 4.3**.
- In the **ASAI Link Version** field, select the default value, **4**.
- In the **Security** field, select the appropriate encryption option for connectivity to the CallCopy cc:Discover server.



Add / Edit TSAPI Links

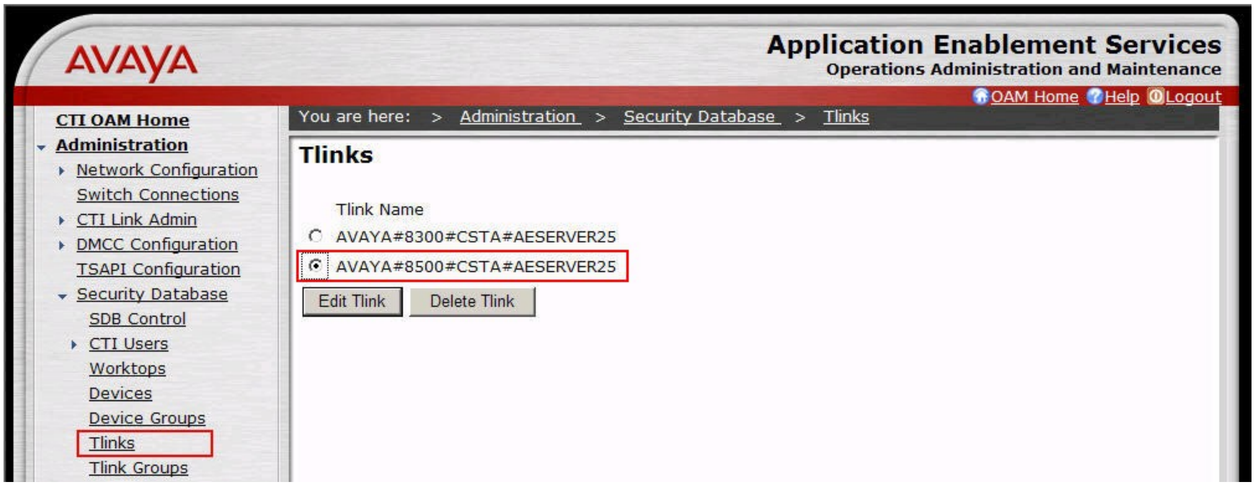
Link:	1
Switch Connection:	8500
Switch CTI Link Number:	10
ASAI Link Version	4
Security	Unencrypted

5.4. Display Tlink

This section provides the steps required to display Tlinks.

Tlinks are service identifiers (names) dynamically created by the TSAPI Service. Tlinks are created automatically once the TSAPI CTI links are created. The appropriate Tlink name will be needed during the configuration of the CallCopy cc:Discover server. This section just illustrates how to obtain the Tlink name.

1. Navigate to **Administration > Security Database > CTI Users > Tlinks**.



	Tlink Name
○	AVAYA#8300#CSTA#AESERVER25
●	AVAYA#8500#CSTA#AESERVER25

To identify the correct Tlink, note that a Tlink has the following format:

AVAYA#switch_connection_name#service_type#AE_server_name

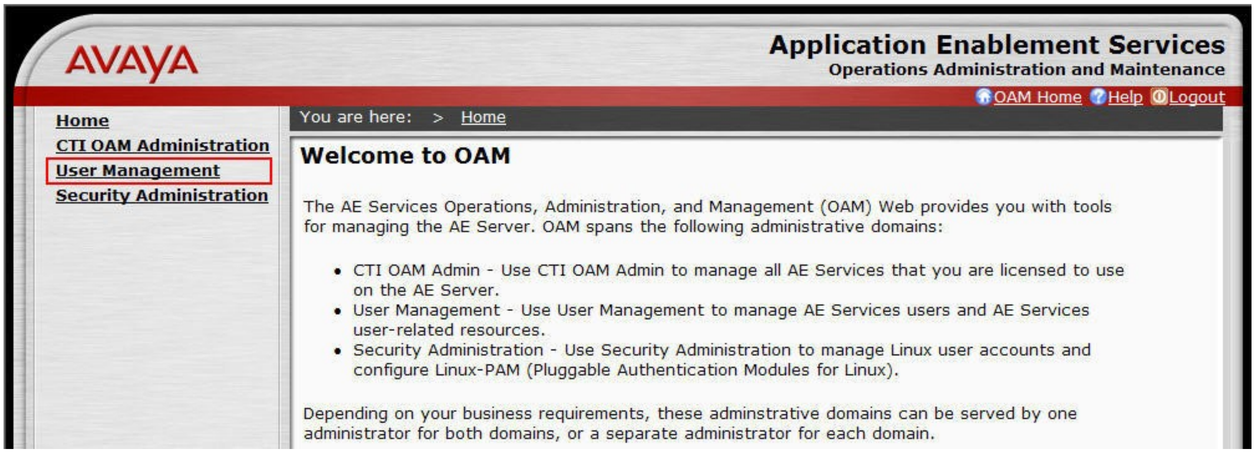
where:

- **AVAYA** is a fixed constant.
- **switch_connection_name** represents the Switch Connection name administered in **Section 5.1**.
- **service_type** refers to the CSTA service type. It can be either of the following:
  - **CSTA**, if the TSAPI Link was administered as unencrypted in **Section 5.3**.
  - **CSTA-S**, if the TSAPI Link was administered as encrypted in **Section 5.3**.
- **AE_server_name** represents the Application Enablement Services Server name.

5.5. Configure CTI Users

This section provides the steps required to configure a CTI user. If necessary, log in to the Application Enablement Services server again with the appropriate credentials for accessing the "User Management" pages.

1. Navigate to the "OAM Home" page. Select **User Management** from the left pane menu.



Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

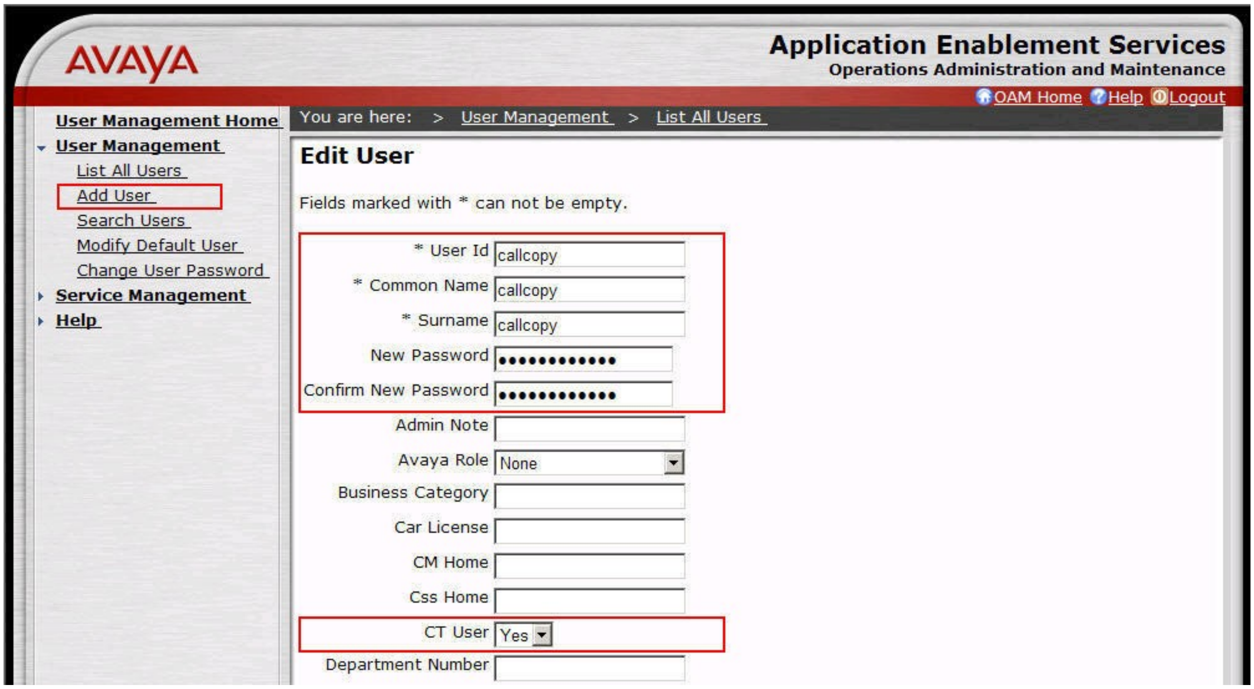
- CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Security Administration - Use Security Administration to manage Linux user accounts and configure Linux-PAM (Pluggable Authentication Modules for Linux).

Depending on your business requirements, these adminstrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

2. Navigate to the **User Management > Add User**. On the "Add User" page, provide the following information:

- In the **User Id** field, type the user ID being assigned to the user.
- In the **Common Name** field, enter the name the user prefers to use.
- In the **Surname** field, type the surname**.**
- In the **User Password** field, type the password being assigned to the user.
- In the **Confirm Password** field, re-type the assigned password.
- In the **CT User field,** select **Yes** to add the user as a member of the Security Database (SDB).

Click the **Apply** button (not shown) at the bottom of the screen.

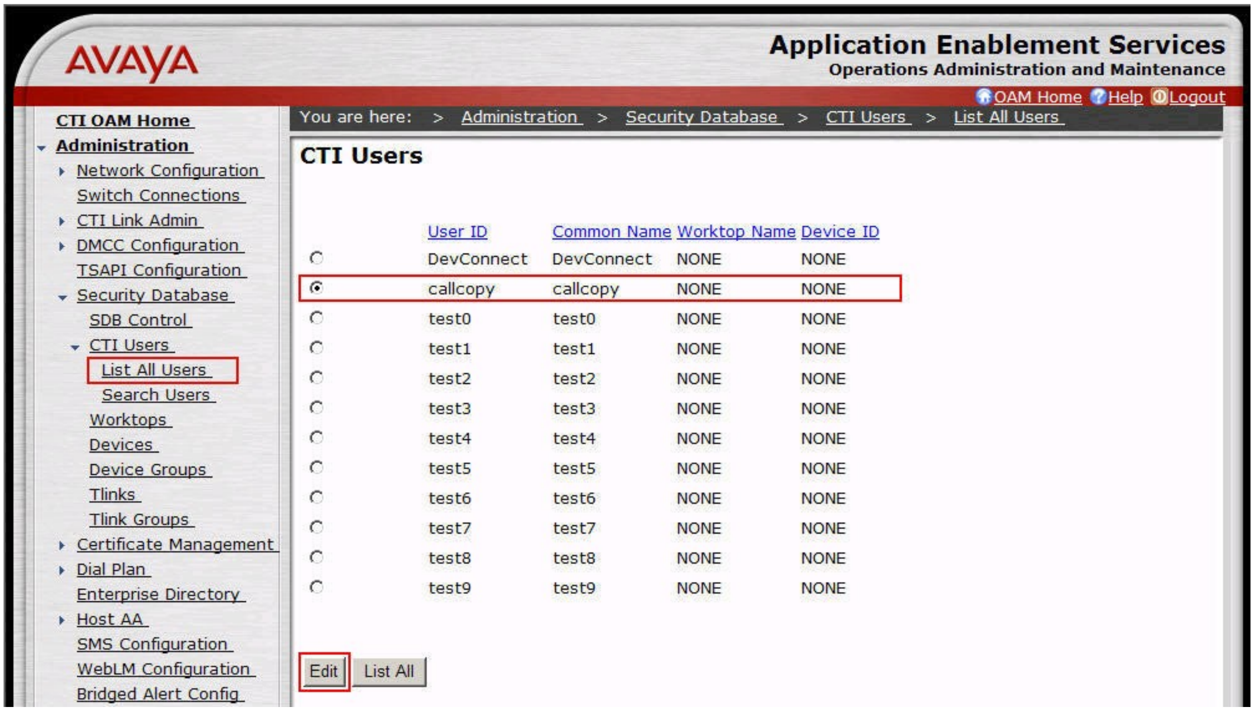


Edit User

Fields marked with * can not be empty.

* User Id	callcopy
* Common Name	callcopy
* Surname	callcopy
New Password	●●●●●●●●●●●●
Confirm New Password	●●●●●●●●●●●●
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	

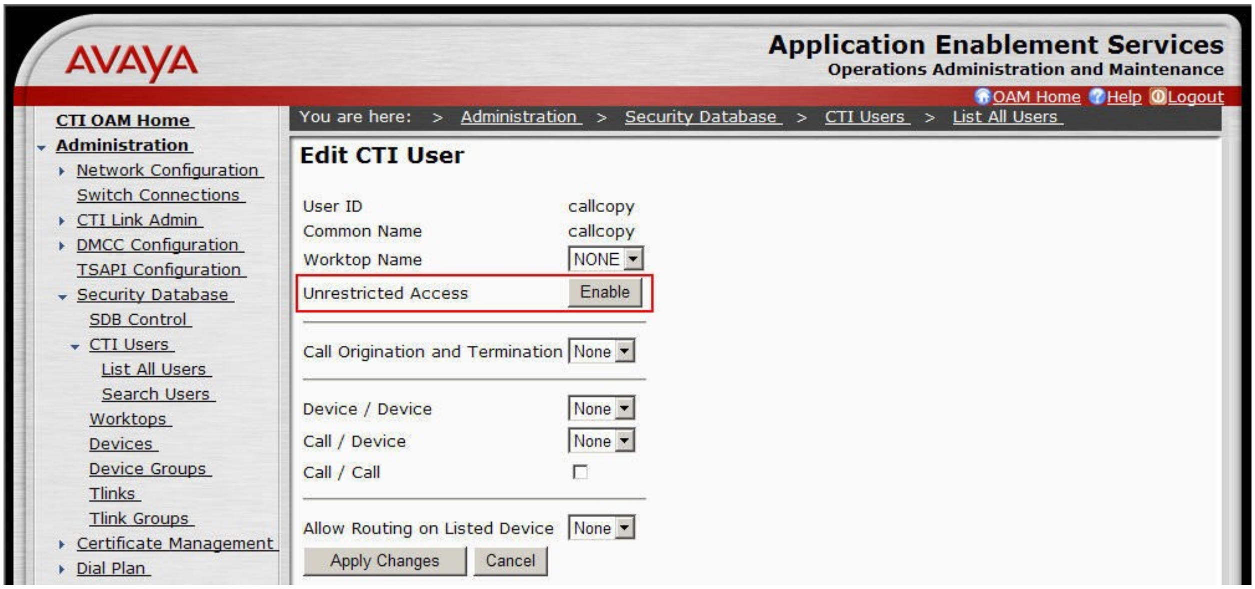
3. Select **OAM Home** in upper right and navigate to the **CTI OAM Administration → Security Database → CTI Users → List All Users** page. Select the **User ID** created in **Step 2**, and click the **Edit** button to set the permissions of the user.



CTI Users

	User ID	Common Name	Worktop Name	Device ID
○	DevConnect	DevConnect	NONE	NONE
●	callcopy	callcopy	NONE	NONE
○	test0	test0	NONE	NONE
○	test1	test1	NONE	NONE
○	test2	test2	NONE	NONE
○	test3	test3	NONE	NONE
○	test4	test4	NONE	NONE
○	test5	test5	NONE	NONE
○	test6	test6	NONE	NONE
○	test7	test7	NONE	NONE
○	test8	test8	NONE	NONE
○	test9	test9	NONE	NONE

4. Provide the user with unrestricted access privileges by clicking the **Enable** button on the **Unrestricted Access** field. A Warning screen will be displayed (not shown). Click **Apply**.



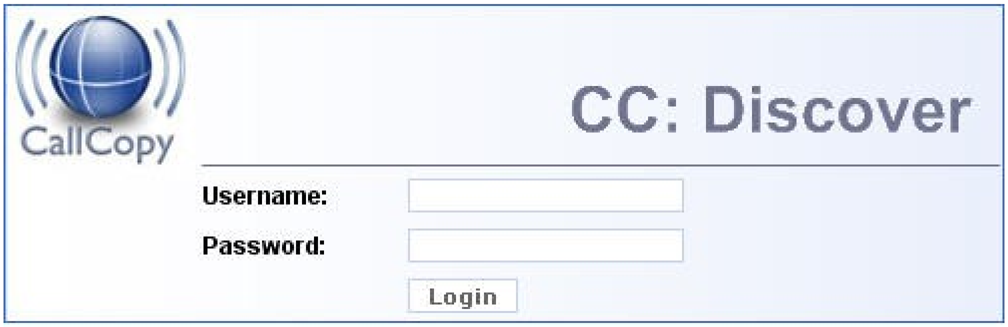
Edit CTI User

User ID	callcopy
Common Name	callcopy
Worktop Name	NONE
Unrestricted Access	Enable
Call Origination and Termination	None
Device / Device	None
Call / Device	None
Call / Call	□
Allow Routing on Listed Device	None

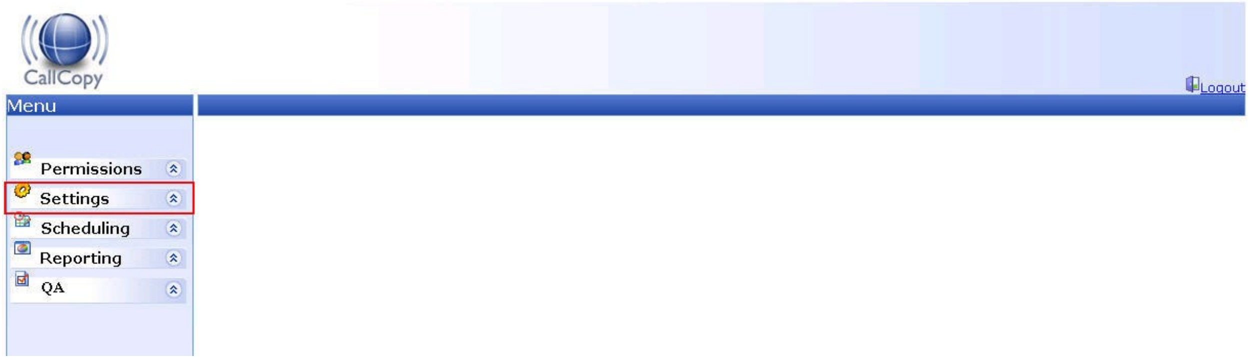
6. Configure CallCopy cc:Discover

This section describes the configuration required for the CallCopy cc:Discover server to interface with Application Enablement Services and Communication Manager.

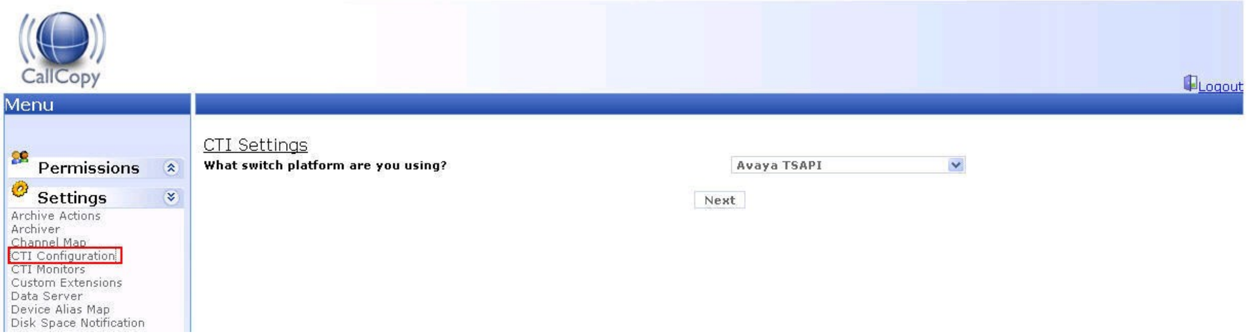
CallCopy installs, configures, and customizes the cc:Discover application for their end customers. This section only describes the interface section of the cc:Discover configuration. Launch a web browser, enter http://<IP address of CallCopy server> in the URL, and log in with the appropriate credentials for accessing the CallCopy cc:Discover main pages.



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



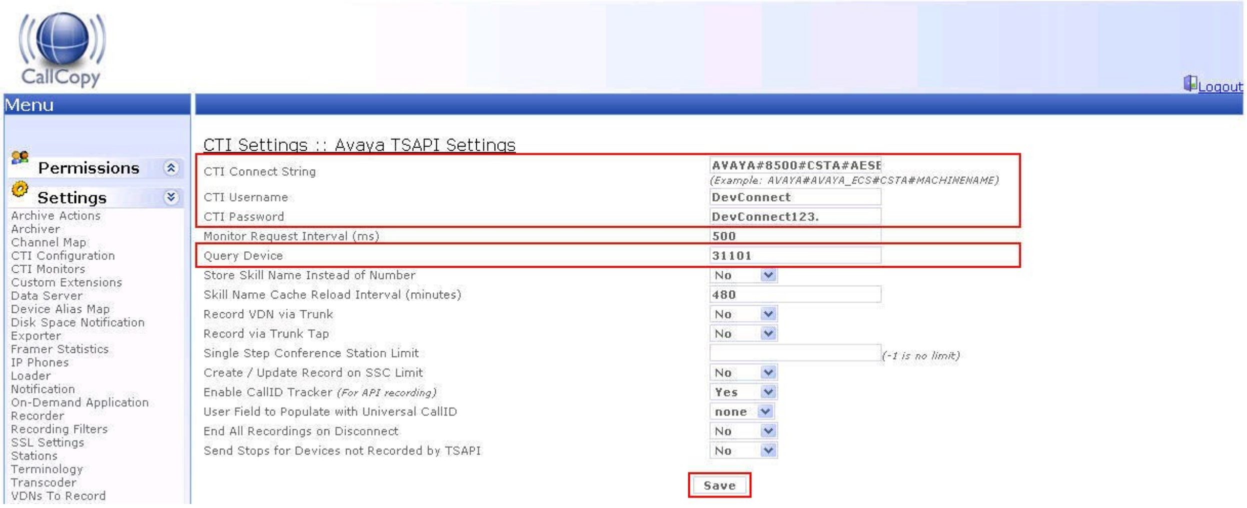
The following shows the **CTI Settings** screen. Use the drop-down menu to select **Avaya TSAPI**. Click the **Next** button.



CTI Settings

What switch platform are you using? Avaya TSAPI

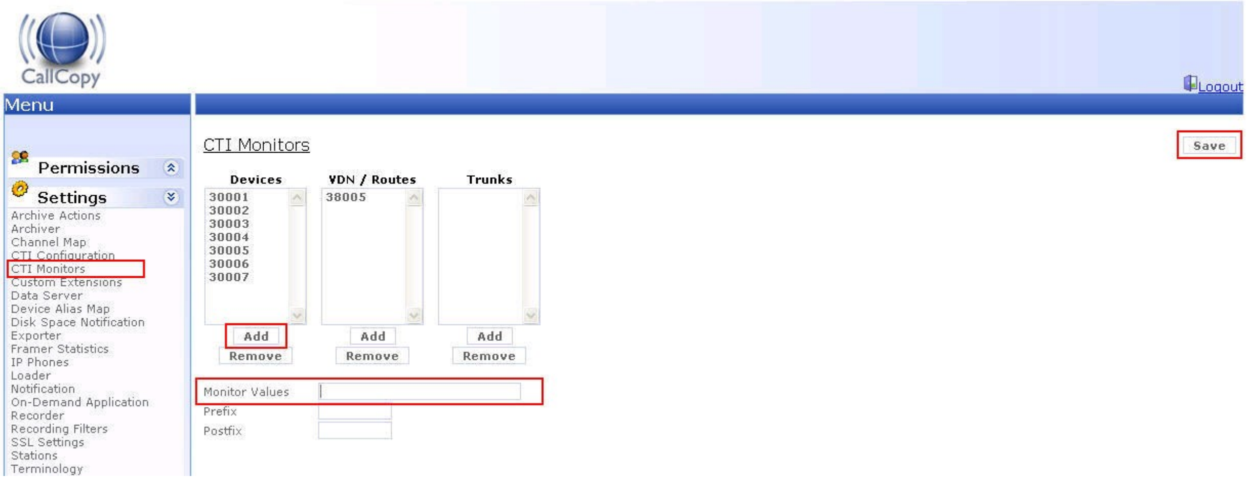
From the **Avaya TSAPI Settings** screen, provide the TLink name used in AES for the **CTI Connect String** field. Provide an appropriate **CTI Username** and **CTI Password** that were created in **Section 5.5**. Enter the extension of one of the DMCC devices for the **Query Device** field. Click the **Save** button.



CTI Settings :: Avaya TSAPI Settings

CTI Connect String	AVAYA#8500#CSTA#AESE *(Example: AVAYA#AVAYA_ECS#CSTA#MACHINENAME)*
CTI Username	DevConnect
CTI Password	DevConnect123.
Monitor Request Interval (ms)	500
Query Device	31101
Store Skill Name Instead of Number	No
Skill Name Cache Reload Interval (minutes)	480
Record VDN via Trunk	No
Record via Trunk Tap	No
Single Step Conference Station Limit	*(-1 is no limit)*
Create / Update Record on SSC Limit	No
Enable CallID Tracker *(For API recording)*	Yes
User Field to Populate with Universal CallID	none
End All Recordings on Disconnect	No
Send Stops for Devices not Recorded by TSAPI	No

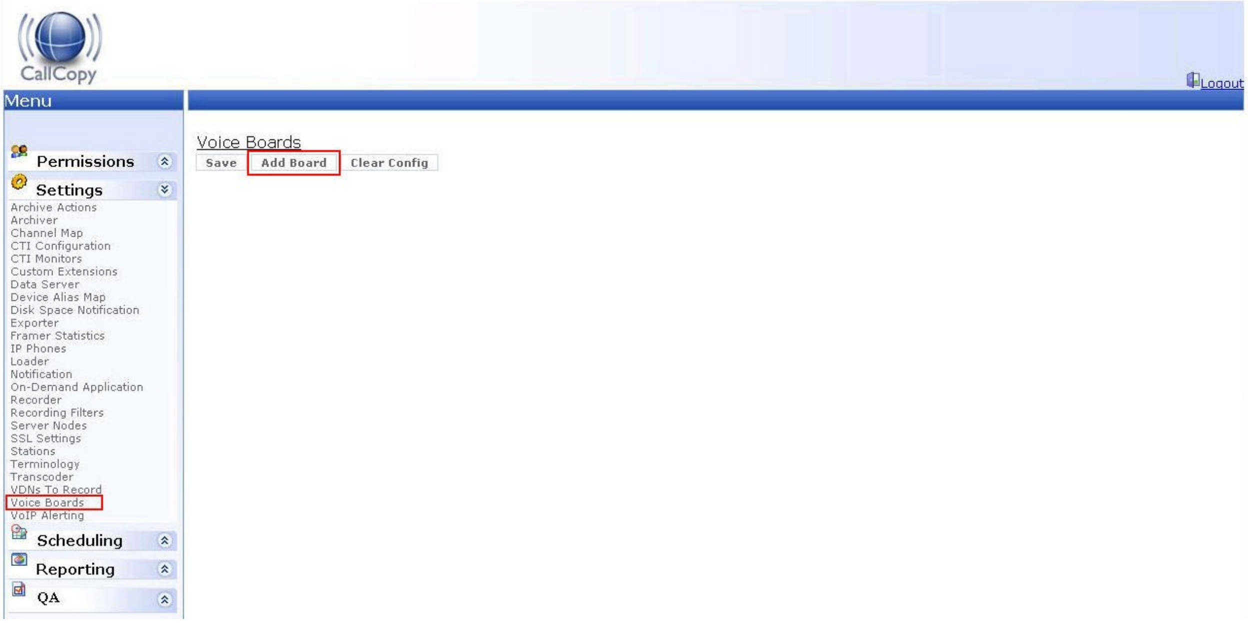
Select **CTI Monitor** link under the **Settings** section. To add any device to be monitored for recording, enter the extension in the **Monitor Values** field, and click the **Add** button under the **Devices** section. Same procedures apply for monitoring **VDN/Routes** and **Trunks**.
After completion of entering monitors, click the **Save** button.



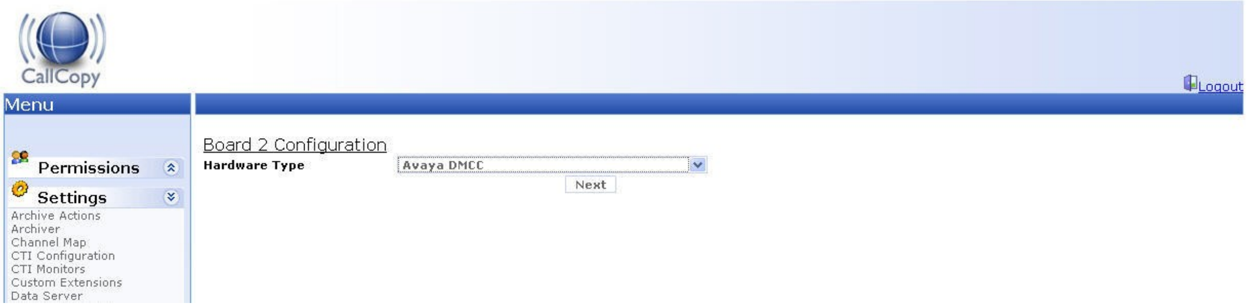
Devices: 30001, 30002, 30003, 30004, 30005, 30006, 30007

VDN / Routes: 38005

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



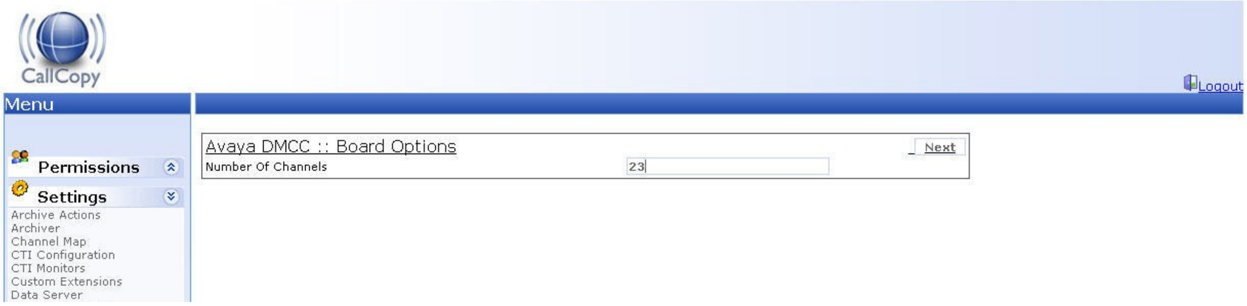
Select **Avaya DMCC** from the pull down menu for the **Hardware Type** field, and click **Next**.



Board 2 Configuration

Hardware Type: Avaya DMCC

Enter a number for the **Number of Channels** field, and click **Next**.



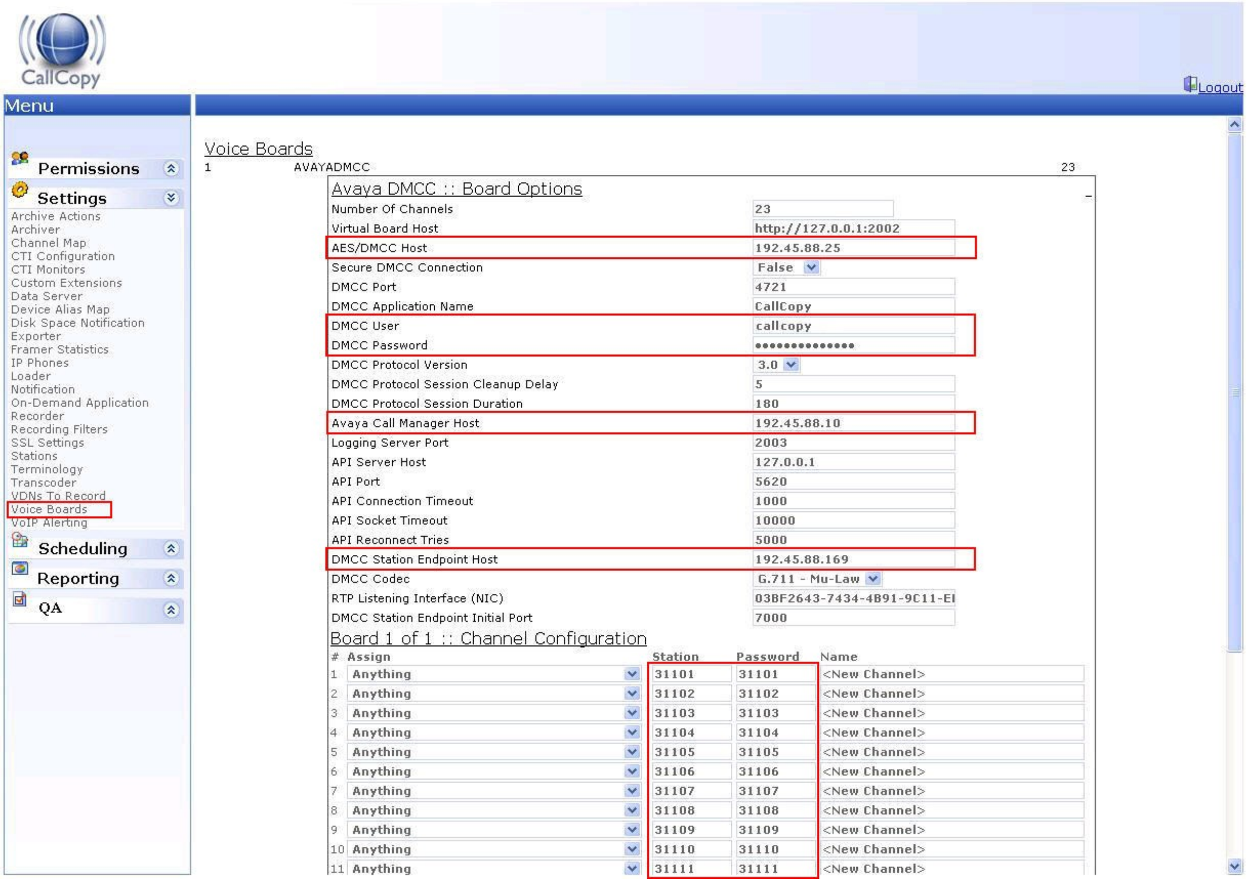
Avaya DMCC :: Board Options

Number Of Channels: 23

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 AES during the DMCC session startup.
- **DMCC Password** - DMCC password used for authenticating with AES during the DMCC session startup.
- **Avaya Call Manager Host** - CLAN (or procr) IP address of 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.
- **Station** and **Password** - Enter all recording stations and the password for each station.

Default values may be used for all other fields.



Voice Boards

1 AVAYADMCC 23

Avaya DMCC :: Board Options

Number Of Channels	23
Virtual Board Host	http://127.0.0.1:2002
AES/DMCC Host	192.45.88.25
Secure DMCC Connection	False
DMCC Port	4721
DMCC Application Name	CallCopy
DMCC User	callcopy
DMCC Password	●●●●●●●●●●●●●●
DMCC Protocol Version	3.0
DMCC Protocol Session Cleanup Delay	5
DMCC Protocol Session Duration	180
Avaya Call Manager Host	192.45.88.10
Logging Server Port	2003
API Server Host	127.0.0.1
API Port	5620
API Connection Timeout	1000
API Socket Timeout	10000
API Reconnect Tries	5000
DMCC Station Endpoint Host	192.45.88.169
DMCC Codec	G.711 - Mu-Law
RTP Listening Interface (NIC)	03BF2643-7434-4B91-9C11-EI
DMCC Station Endpoint Initial Port	7000

Board 1 of 1 :: Channel Configuration

#	Assign	Station	Password	Name
1	Anything	31101	31101	<New Channel>
2	Anything	31102	31102	<New Channel>
3	Anything	31103	31103	<New Channel>
4	Anything	31104	31104	<New Channel>
5	Anything	31105	31105	<New Channel>
6	Anything	31106	31106	<New Channel>
7	Anything	31107	31107	<New Channel>
8	Anything	31108	31108	<New Channel>
9	Anything	31109	31109	<New Channel>
10	Anything	31110	31110	<New Channel>
11	Anything	31111	31111	<New Channel>

7. General Test Approach and Test Results

The general test approach was to place calls and use basic telephony operations to verify that CallCopy cc:Discover could properly record the calls, associate the calls with the correct stations and agents, and to confirm that quality recordings could be retrieved and played back. The test cases were broken down into three categories: feature testing, serviceability testing, and performance testing.

For feature testing, several types of calls were placed, including:

- Internal calls
- Inbound trunk calls
- Outbound trunk calls
- Transfer and Conference calls

The calls were placed to and from various endpoints, including: stations, agents, VDNs, and hunt groups.

For serviceability testing, failure conditions were introduced into the test configuration, such as network cable pulls, CTI link busyouts, and server resets to verify that CallCopy cc:Discover could properly resume operation after failure recovery.

For performance testing, a sustained volume of calls were generated for an extended period of time to verify that CallCopy cc:Discover could record all the calls during that time period.

All test cases were executed and passed.

8. Verification Steps

This section provides the steps that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and CallCopy cc:Discover.

8.1. Verify Communication Manager

This section provides the steps required to verify the status of the link(s) to Application Enablement Services and the CTI link.

1. Enter the **status aesvcs link** command. Verify the **Remote IP** is the IP address of the Application Enablement Services server, the **Local Node** displays each CLAN used for connectivity to Application Enablement Services, and that there is appropriate message traffic over the links (**Msgs Sent** and **Msgs Rcvd**).

```
status aesvcs link

                            AE SERVICES LINK STATUS

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

01/01  aeserver25      192. 45. 88. 25  56300   CLAN2           207     192
01/02  aeserver25      192. 45. 88. 25  56302   CLAN4           180     180
01/03  aeserver25      192. 45. 88. 25  56304   CLAN3           180     180
```

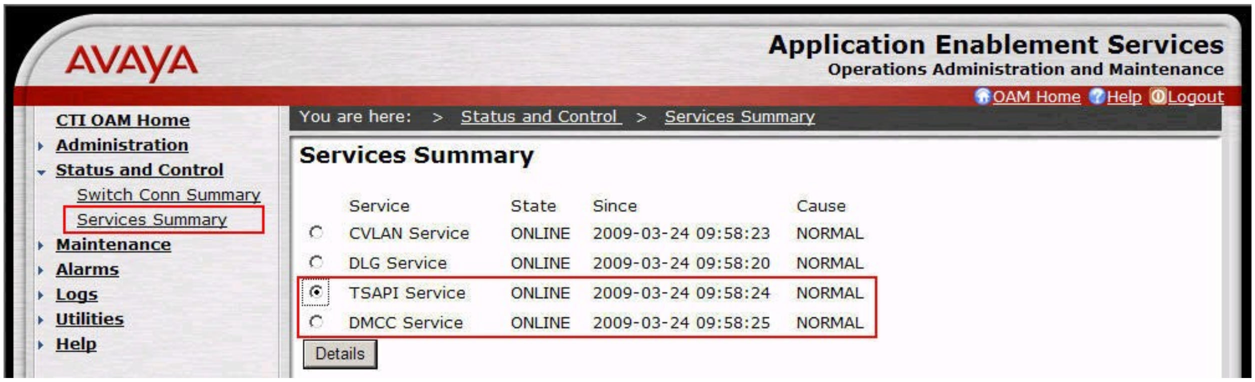
2. Enter the **status aesvcs cti-link** command. Verify the **Service State** is **established** for the CTI link number administered in **Section 4.3**.

```
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                     down          0        0
3              no                     down          0        0
4              no                     down          0        0
5              no                     down          0        0
6              no                     down          0        0
7              no                     down          0        0
8              no                     down          0        0
9              no                     down          0        0
10    4        no    aeserver25       established   15       15
```

8.2. Verify Application Enablement Services

This section provides the steps required to verify the status of the TSAPI and DMCC services.

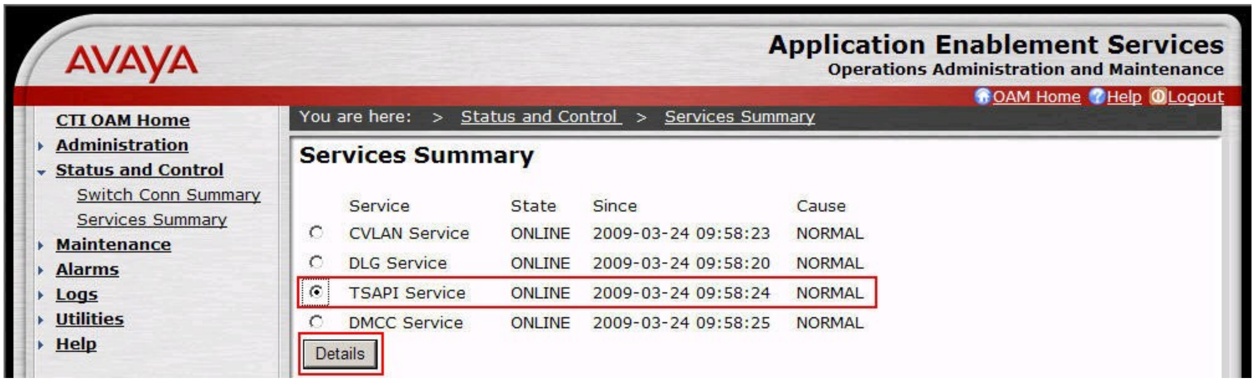
1. From the Application Enablement Services "CTI OAM Admin" web pages, navigate to **Status and Control > Services Summary** in the left pane menu. Verify that the **State** of the **TSAPI Service** and the **DMCC Service** is **ONLINE**.



Services Summary

	Service	State	Since	Cause
○	CVLAN Service	ONLINE	2009-03-24 09:58:23	NORMAL
○	DLG Service	ONLINE	2009-03-24 09:58:20	NORMAL
●	TSAPI Service	ONLINE	2009-03-24 09:58:24	NORMAL
○	DMCC Service	ONLINE	2009-03-24 09:58:25	NORMAL

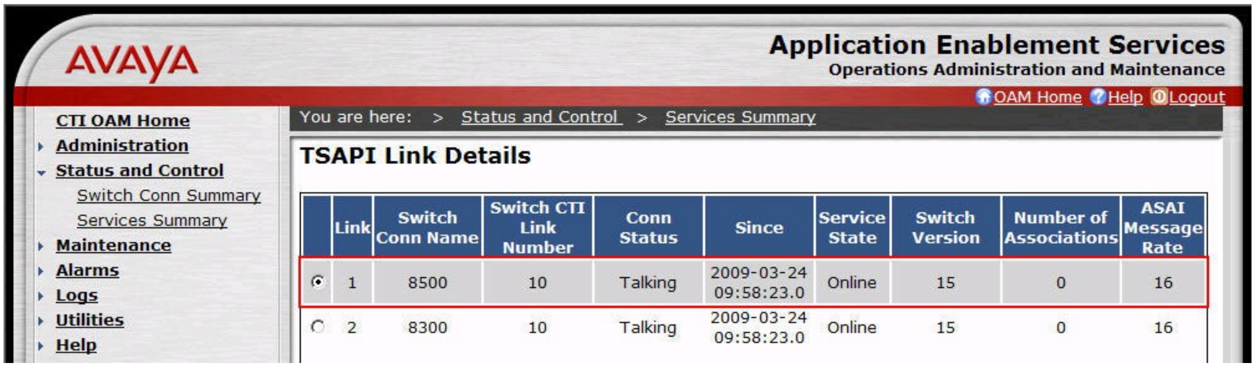
2. Select the radio button for **TSAPI Service**, and click **Details**.



Services Summary

	Service	State	Since	Cause
○	CVLAN Service	ONLINE	2009-03-24 09:58:23	NORMAL
○	DLG Service	ONLINE	2009-03-24 09:58:20	NORMAL
●	TSAPI Service	ONLINE	2009-03-24 09:58:24	NORMAL
○	DMCC Service	ONLINE	2009-03-24 09:58:25	NORMAL

3. Verify that the **Conn Status** is **Talking** for the TSAPI link administered in **Section 5.3**.



TSAPI Link Details

	Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
●	1	8500	10	Talking	2009-03-24 09:58:23.0	Online	15	0	16
○	2	8300	10	Talking	2009-03-24 09:58:23.0	Online	15	0	16

9. Conclusion

These Application Notes describe the configuration steps required for CallCopy cc:Discover 3.8 to interoperate with Avaya Aura^{TM} Communication Manager 5.2 and Avaya Aura^{TM} Application Enablement Services 4.2. All feature, serviceability, and performance test cases were completed and passed.

10. Additional References

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

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

[1] *Administering Avaya Aura™ Communication Manager,* Doc ID: 03-300509, Issue 5.0, Release 5.2, May 2009
[2] *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*, Doc ID: 02-300357, Release 4.2, Issue 10, May 2008

The following CallCopy product documentation was used during installation and configuration:

[3] *CallCopy Avaya DMCC Integration*
[4] *CallCopy Avaya TSAPI Integration*

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.