Avaya Solution & Interoperability Test Lab

Application Notes for CallCopy cc:Discover with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference and Service Observing for Recordings – 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 using Single Step Conference and Service Observing for Recordings.

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 Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services with Single Step Conferencing and Service Observing, 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 Application Enablement Services 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 or service observing 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.

2. General Test Approach and Test Results

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. For serviceability testing, failures such as cable pulls, busyouts/releases of the trunk group, and resets were applied.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability 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.

2.2. Test Results

The test objectives were verified. For serviceability testing, CallCopy cc:Discover operated properly after recovering from failures such as cable disconnects, and resets of CallCopy cc:Discover, Application Enablement Services and Communication Manager.

2.3. 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

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. CallCopy cc:Discover was connected to the Communication Manager and Application Enablement Services highlighted in grey in the figure below. The other system shown below was used in the execution of various test cases but is not directly part of the solution. As such, it is not included in the configuration described in these Application Notes.

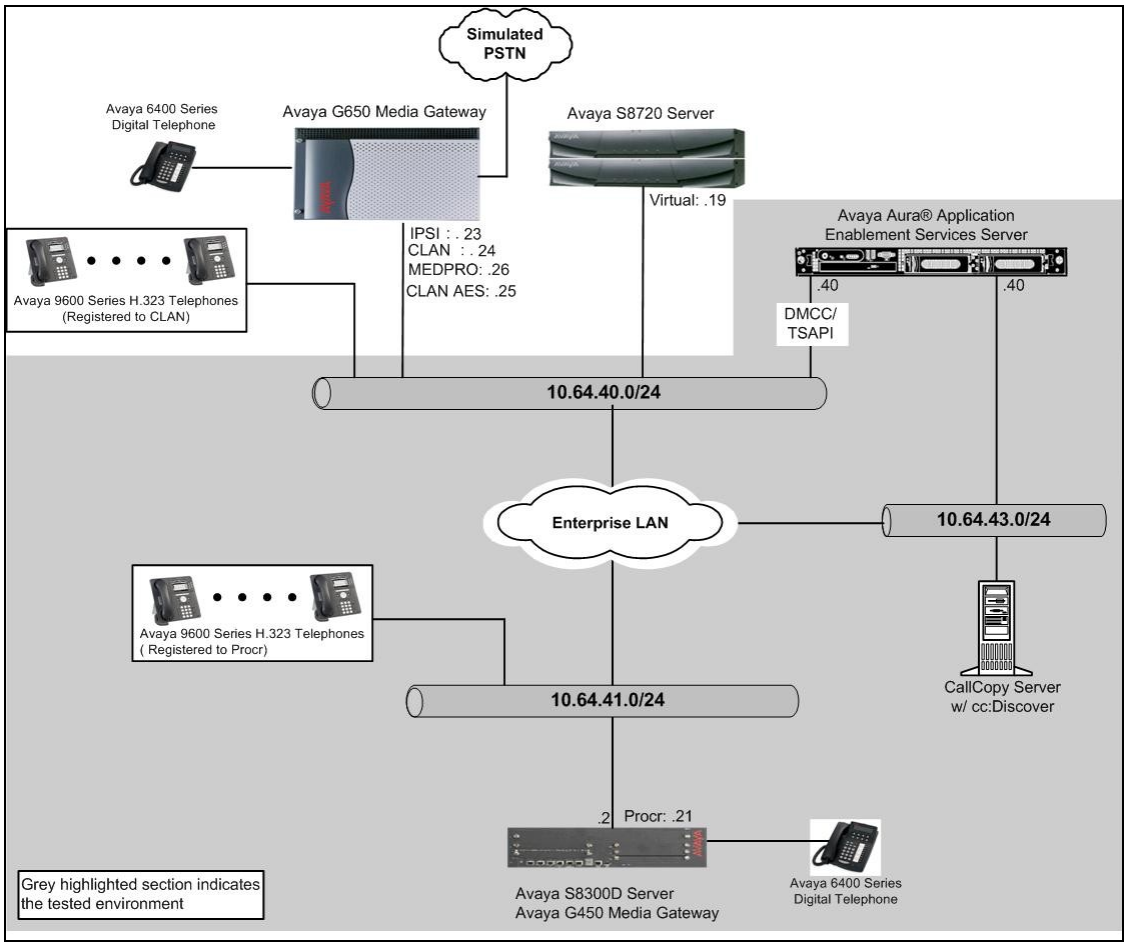


Figure 1: CallCopy cc:Discover with Avaya Aura®Communication Manager and Avaya Aura® Application Enablement Services

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0.1(R016x.00.1.510.1) w/ patch 00.1.510.1-18860
Avaya Aura® Application Enablement Services		6.1 (R6-1-0-20-0)
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones		
	9620 (H.323) 9630 (H.323)	3.1 3.1
Avaya 9600 Series SIP Telephones		
	9630 (SIP) 9640 (SIP) 9650 (SIP)	2.6.4 2.6.4 2.6.4
Avaya 6400 Series Digital Telephones		N/A
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Networks Summit 48		4.1.21
CallCopy cc:Discover		4.5 SP1

5. Configure Avaya Aura® 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 the Computer Telephony Interface (CTI) link in Communication Manager to integrate with cc:Discover. All the configuration changes in 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	72073
Vector	88
Skill group	88
Logical agent IDs	72091, 72092, 72093, 72094, 72095
Recorded stations (IP Telephones)	IP Telephones: 72001, 72002, 72003 DCP Telephone: 72007 IP Agents: 72006
Recording stations (DMCC stations)	72501 - 72059

5.1. 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: 6.0

                                  ACD? y                        Reason Codes? y
                        BCMS (Basic)? y             Service Level Maximizer? n
        BCMS/VuStats Service Level? y            Service Observing (Basic)? y
 BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                  Business Advocate? n              Service Observing (VDNs)? y
                    Call Work Codes? y                          Timed ACW? y
     DTMF Feedback Signals For VRU? y                  Vectoring (Basic)? y
                  Dynamic Advocate? n               Vectoring (Prompting)? y
      Expert Agent Selection (EAS)? y             Vectoring (G3V4 Enhanced)? y
                             EAS-PHD? y              Vectoring (3.0 Enhanced)? y
                Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
             Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
         Lookahead Interflow (LAI)? y                   Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
   Multiple Call Handling (Forced)? y                Vectoring (Holidays)? y
 PASTE (Display PBX Data on Phone)? y               Vectoring (Variables)? y
       (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 88                                               Page   1 of   4
                                    HUNT GROUP

           Group Number: 88                                 ACD? y
             Group Name: hunt-4-Callcopy                  Queue? y
        Group Extension: 72088                           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:
```

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 88                                              Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none




   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? 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 72091                                        Page   1 of   2
                                AGENT LOGINID

               Login ID: 72091                                    AAS? n
                   Name: Agent-1                                 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/SIP Display? n
                                                         Password:
                                                 Password (enter again):
                                                      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
                                           Forced Agent Logout Time:   :

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

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 72091                                        Page   2 of   2
                                  AGENT LOGINID
      Direct Agent Skill:                            Service Objective? n
Call Handling Preference: skill-level              Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 88       1       16:
 2:                  17:
 3:                  18:
 4:                  19:
 5:                  20:
```

Enter the **change 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.

```
change vector 88                                               Page   1 of   6
                                   CALL VECTOR

    Number: 88               Name: Vector-callcopy
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y    Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time     2   secs hearing ringback
02 queue-to      skill 88    pri m
03
```

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 72073 will be routed to VDN 72073, which in turn will invoke the actions specified in vector 88.

```
add vdn 72073                                                  Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                              Extension: 72073
                                  Name*: VDN-Callcopy
                             Destination: Vector Number         88
                    Attendant Vectoring? n
                   Meet-me Conferencing? n
                     Allow VDN Override? n
                                    COR: 1
                                    TN*: 1
                               Measured: none

          VDN of Origin Annc. Extension*:
                              1st Skill*:
                              2nd Skill*:
                              3rd Skill*:
```

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  10
                              FEATURE ACCESS CODE (FAC)

                                Call Center Features
  AGENT WORK MODES
                    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
             Service Observing Listen Only Access Code: 127
             Service Observing Listen/Talk Access Code: 128
                 Service Observing No Talk Access Code: 129
   Service Observing Next Call Listen Only Access Code:
```

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
     01: 124
     02: 125
     03:
     04:
     05:
```

5.2. Recording Ports

The recording ports in this configuration are AES Device, Media, and Call Control (DMCC) stations that essentially appear as IP Softphones to 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
AgentSC         : 2400          0
IP_API_A        : 2400          0
IP_Agent        : 2400          0
IP_NonAgt       : 2400          0
IP_Phone        : 2400          6
IP_ROMax        : 2400          0
IP_Soft         : 2400          0
IP_Supv         : 2400          0
IP_eCons        : 68            0
oneX_Comm       : 2400          0
```

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 and 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.

```
change station 72501                                          Page   1 of   5
                                    STATION

Extension: 72501                       Lock Messages? n              BCC: 0
     Type: 9630                        Security Code: *               TN: 1
     Port: S00078                    Coverage Path 1:                COR: 1
     Name: DMCC-1                    Coverage Path 2:                COS: 1
                                     Hunt-to Station:

STATION OPTIONS
                 Location:                  Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 72501
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                              IP Video Softphone? n
                                 Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

5.3. Recorded Stations

The stations that were recorded during the compliance testing include an Avaya Digital Telephone, Avaya IP Telephones (Avaya 9600 Series), and an Avaya one-X Agent. The extensions used were in the ranges 72001-72009.

```
add station 72001                                          Page   1 of   5
                                    STATION

Extension: 72001                        Lock Messages? n              BCC: 0
     Type: 9620                         Security Code: *               TN: 1
     Port: S00002                     Coverage Path 1:                COR: 1
     Name: S8300-IP-1                 Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                 Location:                  Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 72001
            Speakerphone: 2-way              Mute Button Enabled? y
         Display Language: english
 Survivable GK Node Name:
           Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default
```

5.4. Audio Codec Configuration

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

Note: CallCopy cc:Discover supports G.711 (MU and A) and G.729. During the compliance test, G.711MU was utilized. The codec has to match between 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.711MU            n          2        20
 2:
```

5.5. 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.

```
change ip-network-region 1                                    Page   1 of  20
                            IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    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: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        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
```

5.6. Configure TSAPI CTI Link

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid **Extensio**n 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   3
                                    CTI LINK
 CTI Link: 4
Extension: 72000
     Type: ADJ-IP
                                                                    COR: 1
     Name: TSAPI
```

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

```
change node-names ip                                          Page   1 of   2
                                 IP NODE NAMES
    Name                  IP Address
CLAN                   10.64.40.24
IPOffice               10.64.44.21
SES                    10.64.40.41
SM-1                   10.64.40.42
SM-2                   10.64.21.31
aes                    10.64.43.40
default                0.0.0.0
msgserver-ip           10.64.41.21
pcr                    204.27.235.31
procr                  10.64.41.21
procr6                 ::
```

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 **procr** 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       procr           8765
CDR1                    procr           0        pcr             5852
CDR2                    procr           0        rdtt-1          9004
```

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 Application Enablement Services in **Section 6.1**.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aes                [redacted]          y        idle
      2:
      3:
      4:
      5:
      6:
```

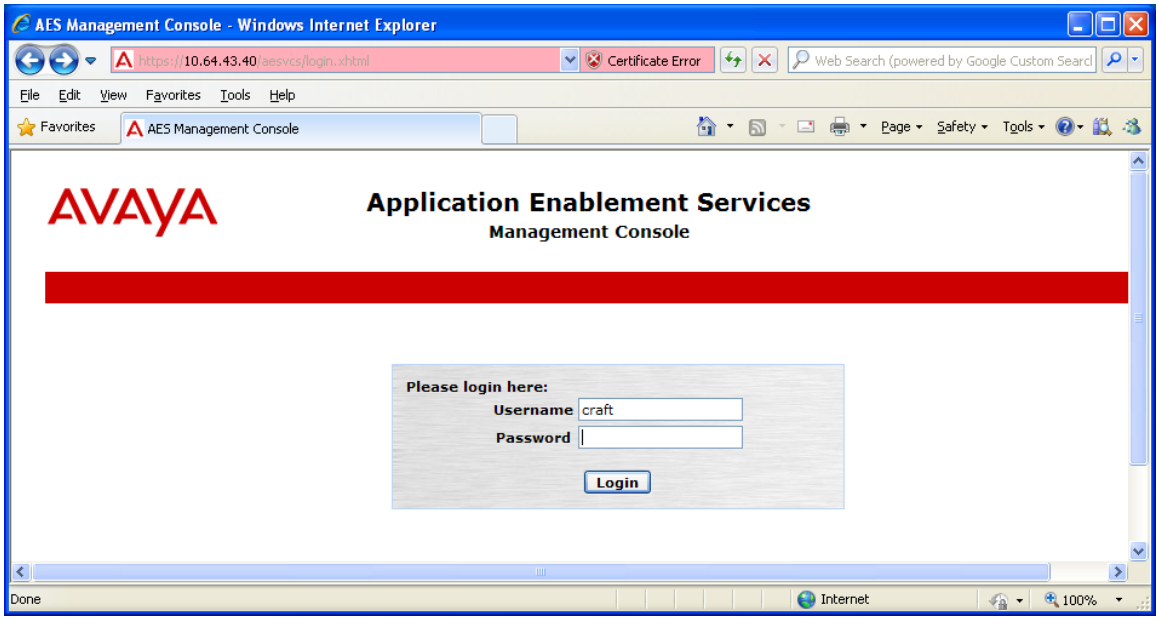
6. Configure Avaya Application Enablement Services

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

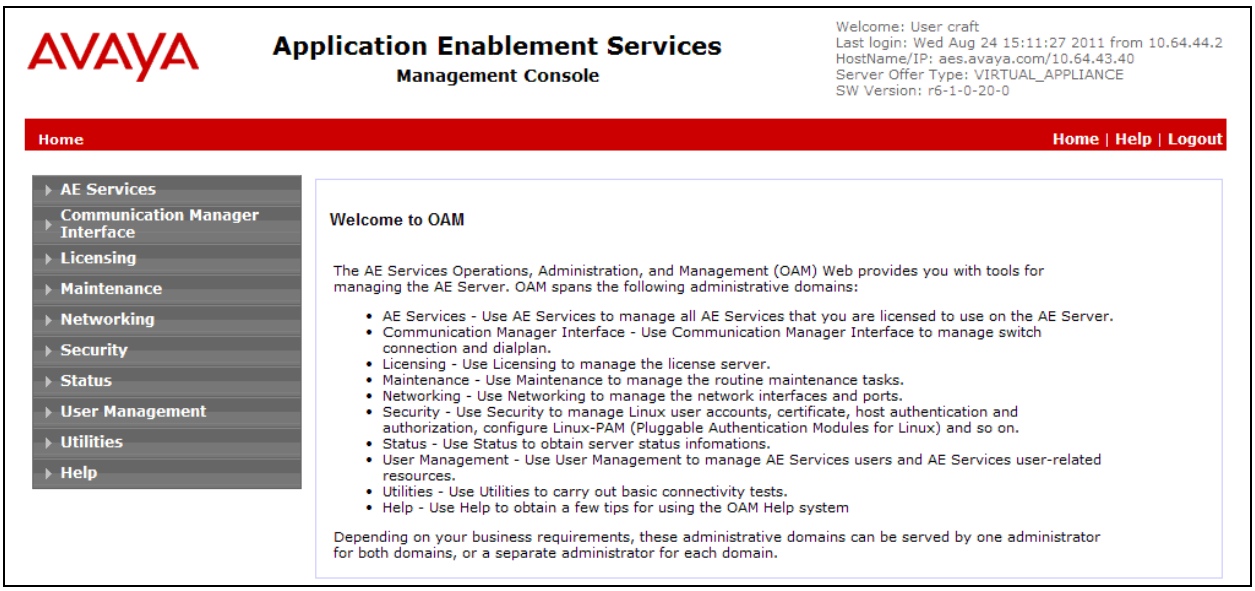
This section assumes that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, creating a CTI link for TSAPI, and a CTI user.

6.1. Configure Switch Connection

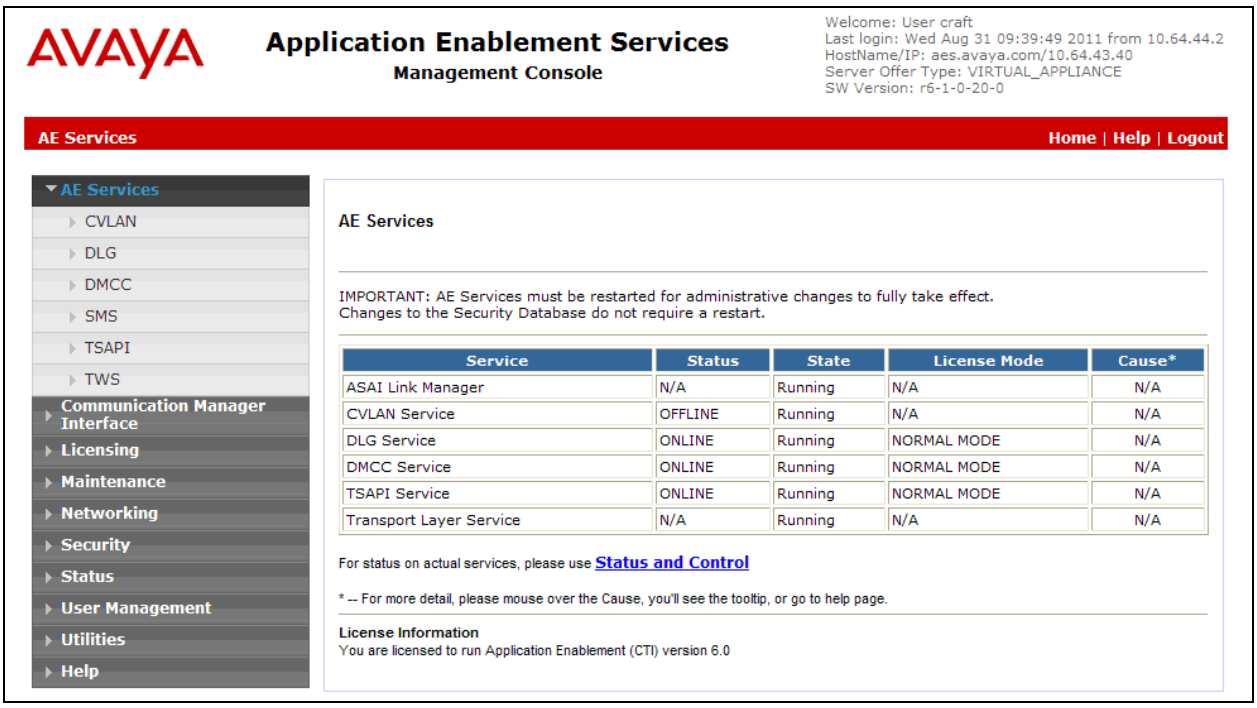
Launch a web browser, enter https://<IP address of AES server> in the URL, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console page.



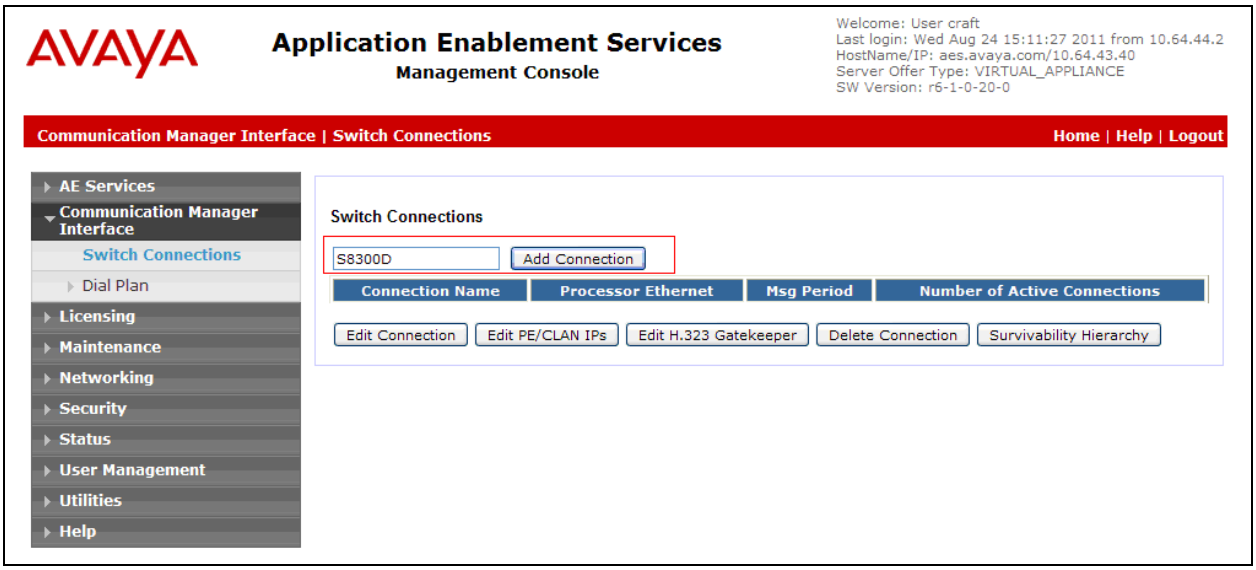
The Welcome to OAM screen is displayed next. Select **AE Services** from the left pane.



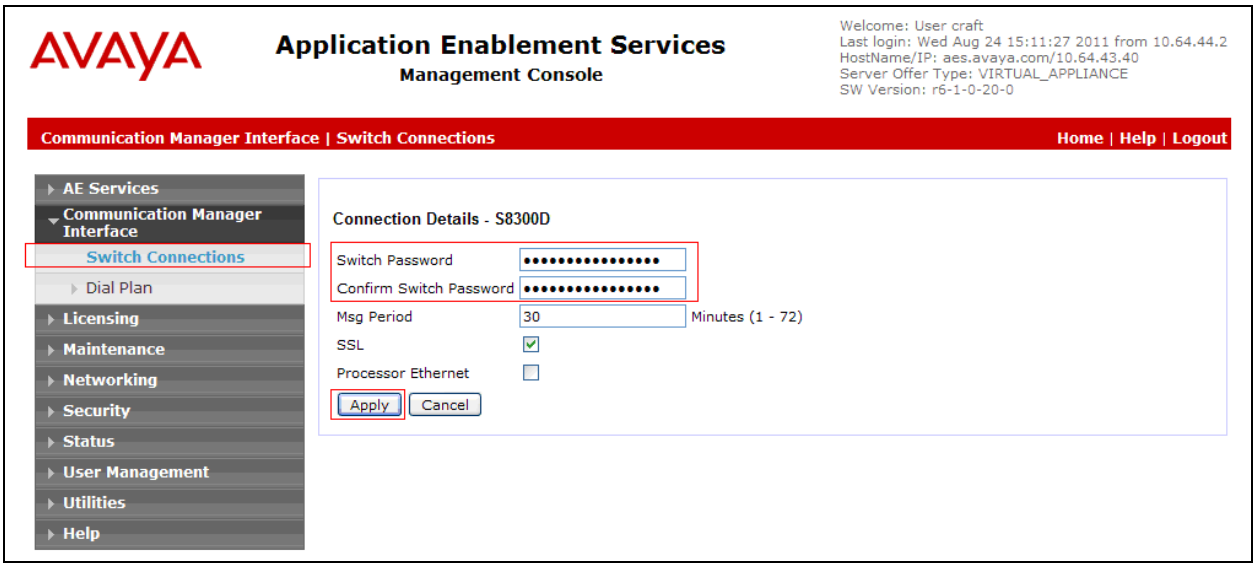
Verify that AES is licensed for the TSAPI service, as shown in the screen below.



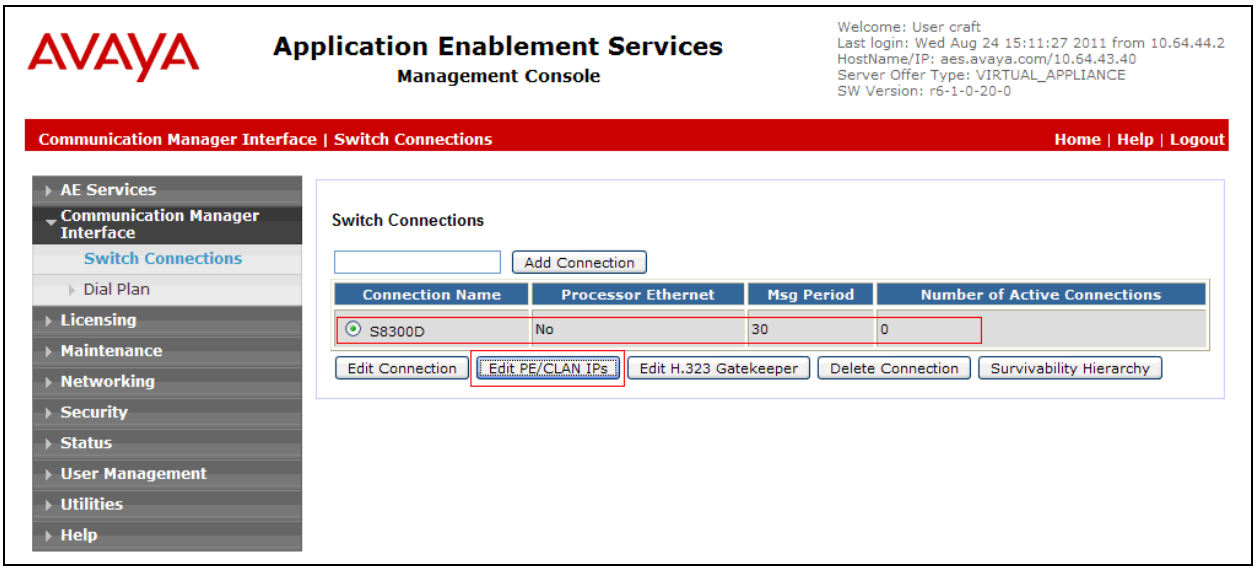
Click on **Communication Manager Interface→ Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click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



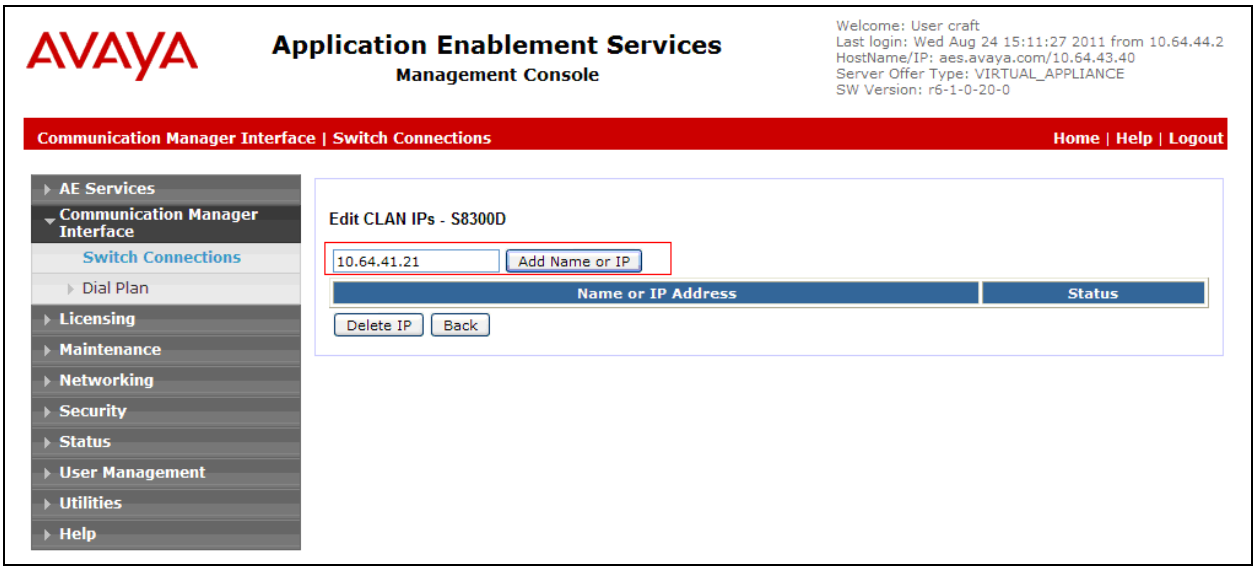
The next window that appears prompts for the Switch Password. Enter the same password that was administered on Communication Manager in **Section 5.6**. Default values may be used in the remaining fields. Click on **Apply**.



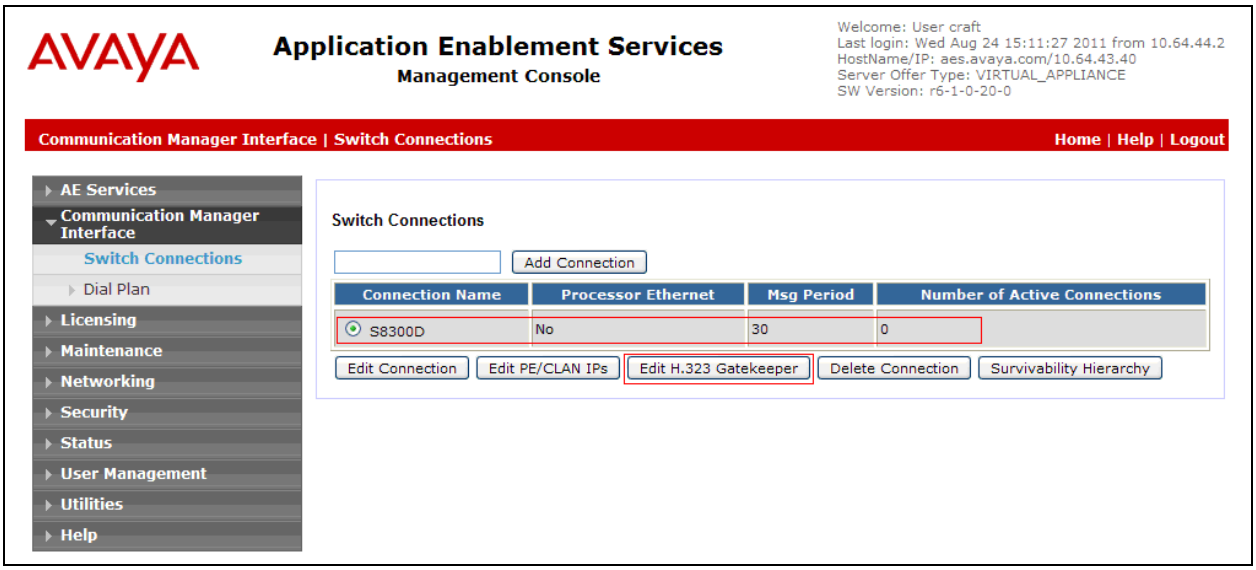
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit PE/CLAN IPs**.



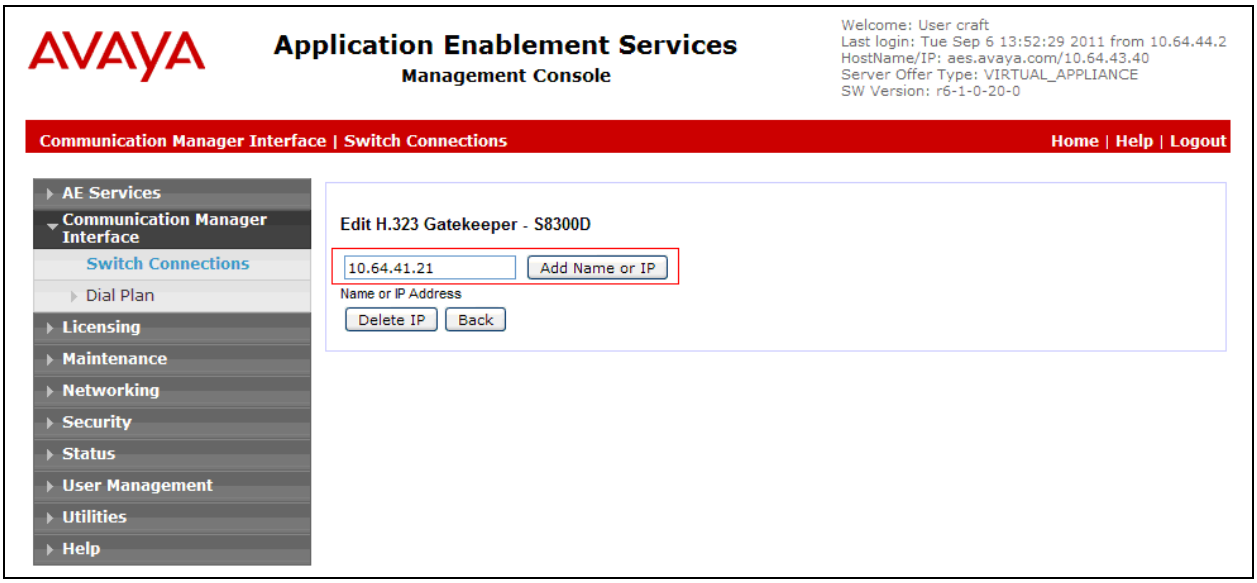
Enter the IP address of Procr used for Application Enablement Services connectivity from **Section 5.6**, and click on **Add Name or IP**.



After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit H.323 Gatekeeper**.

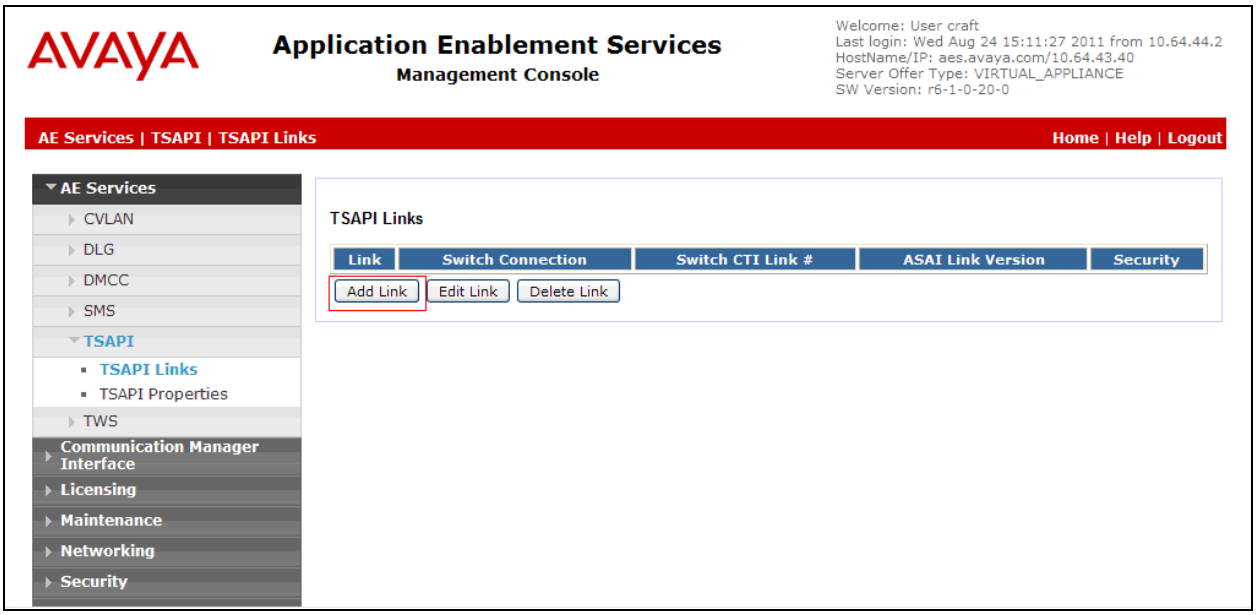


Enter the IP address of Procr used for Application Enablement Services connectivity from **Section 5.6**, and click on **Add Name or IP**.

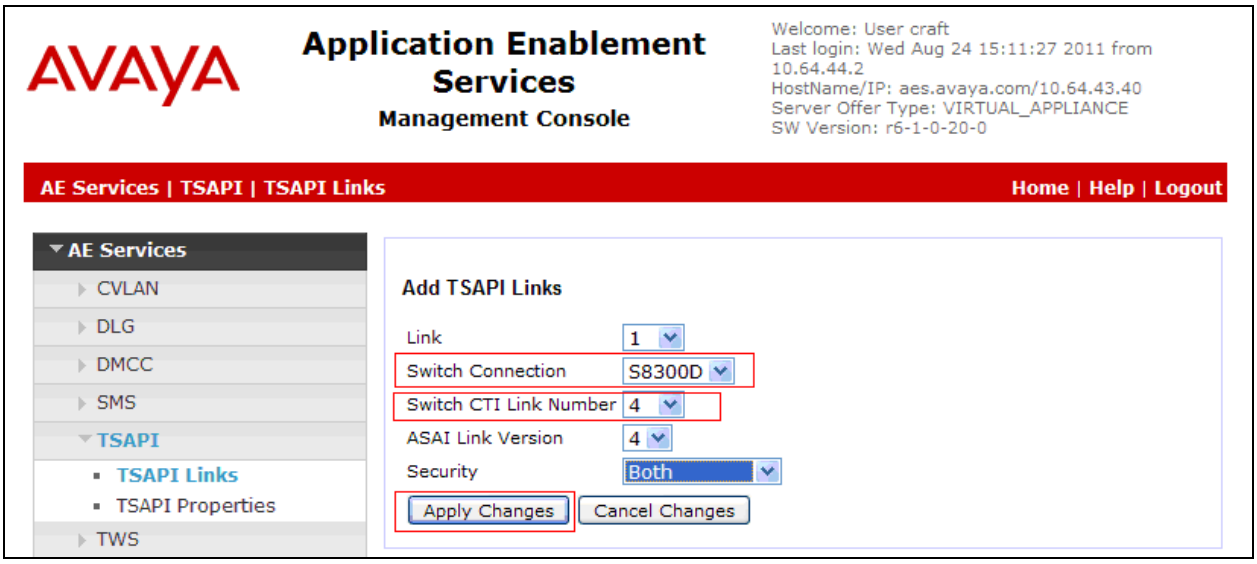


6.2. Configure TSAPI CTI Link

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



Select the switch connection using the drop-down menu. Select the switch connection configured in **Section 6.1**. 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 5.6**. Click **Apply Changes**.



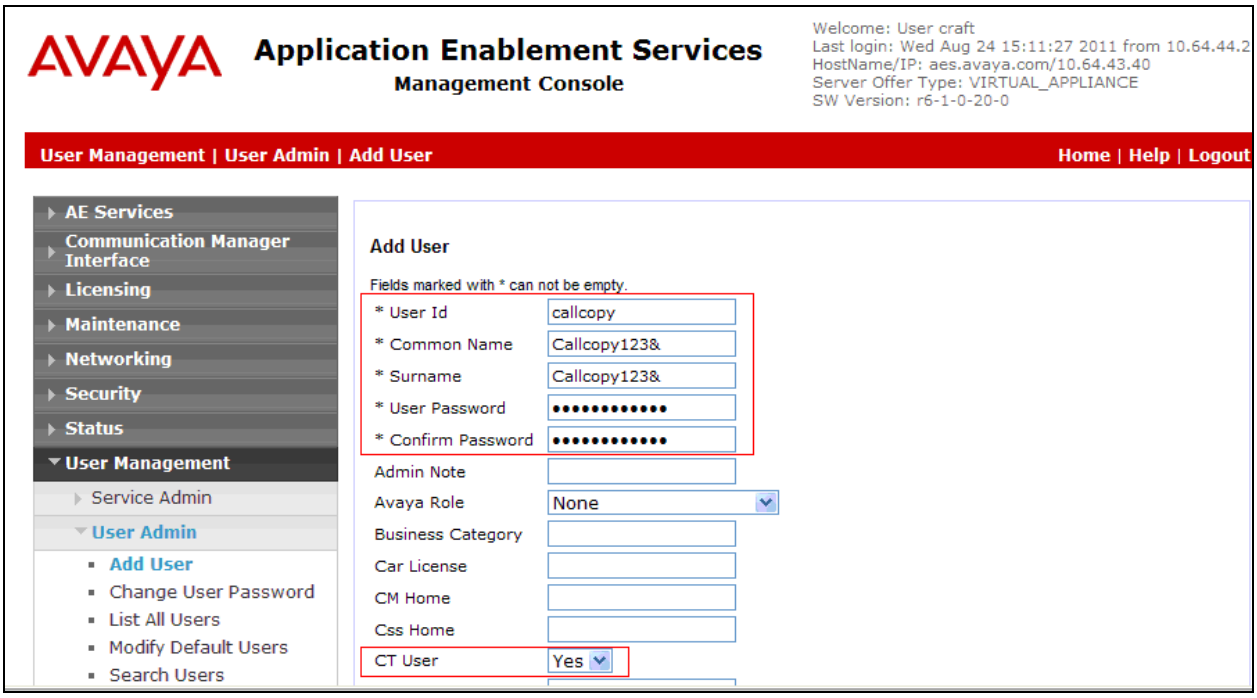
The following screen shows the TSAPI CTI link configuration.

6.3. Configure CTI User

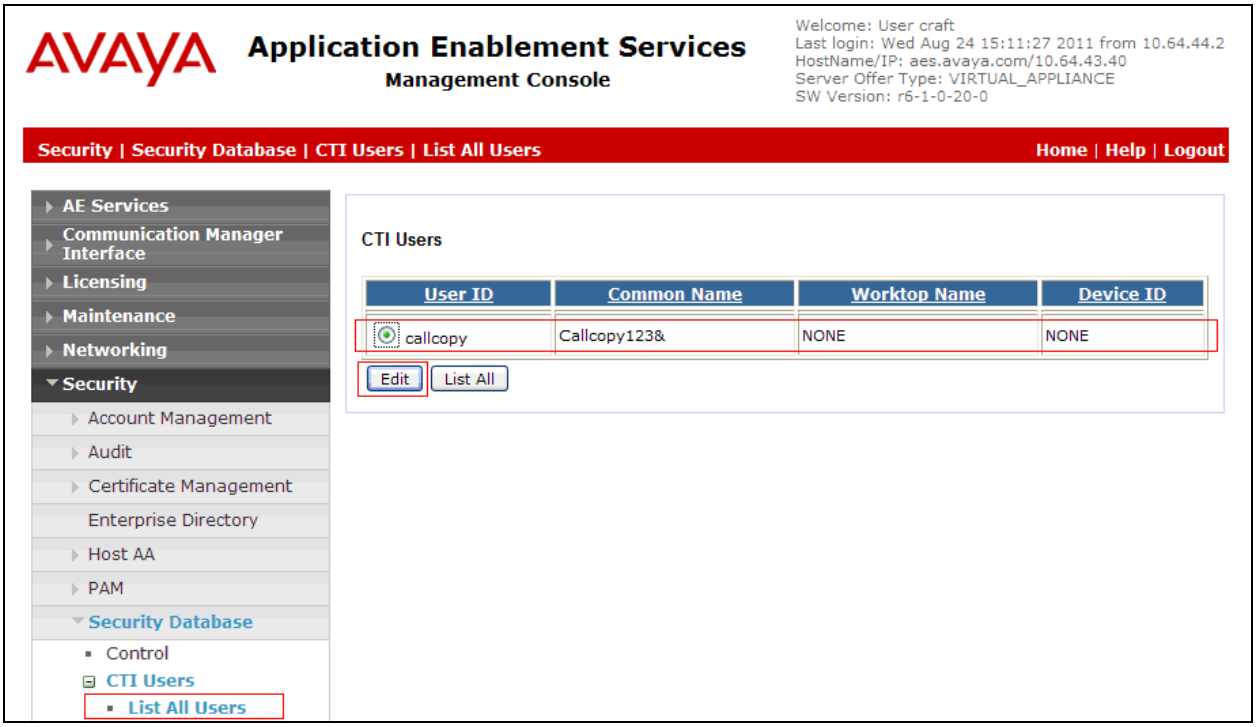
Navigate to **User Management → Add User**. On the Add User page, provide the following information:

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

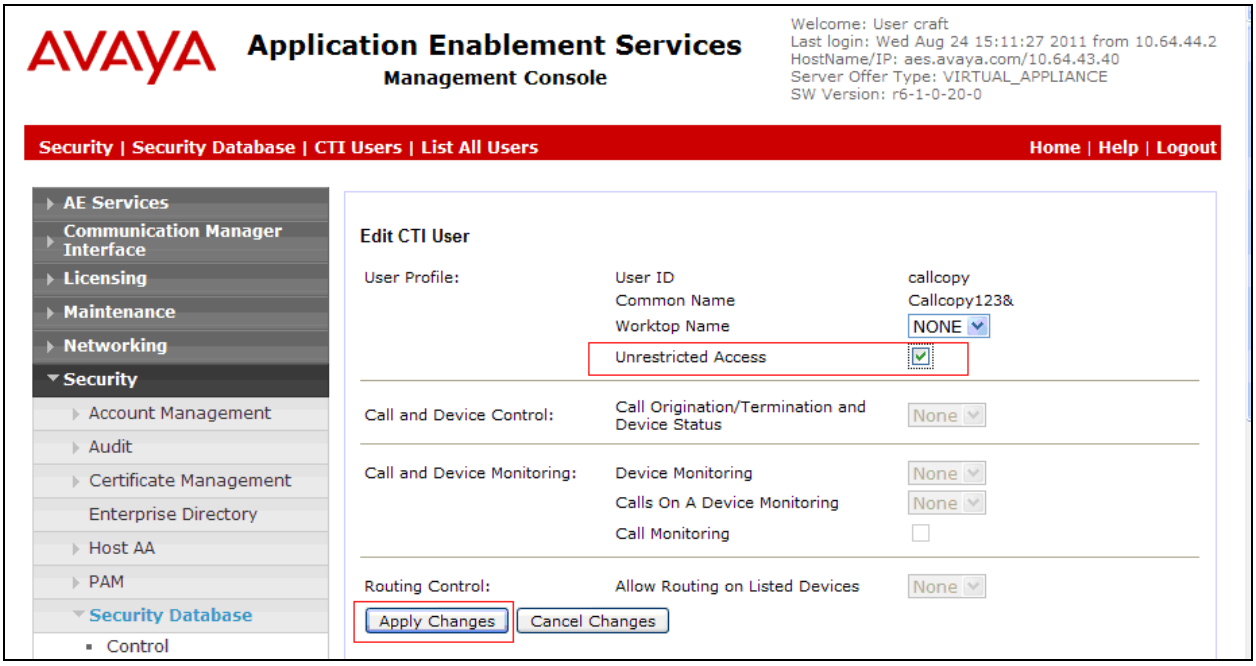
Select **Yes** using the drop-down menu on the **CT User** field. This enables the user as a CTI user. Click the **Apply** button (not shown here) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.



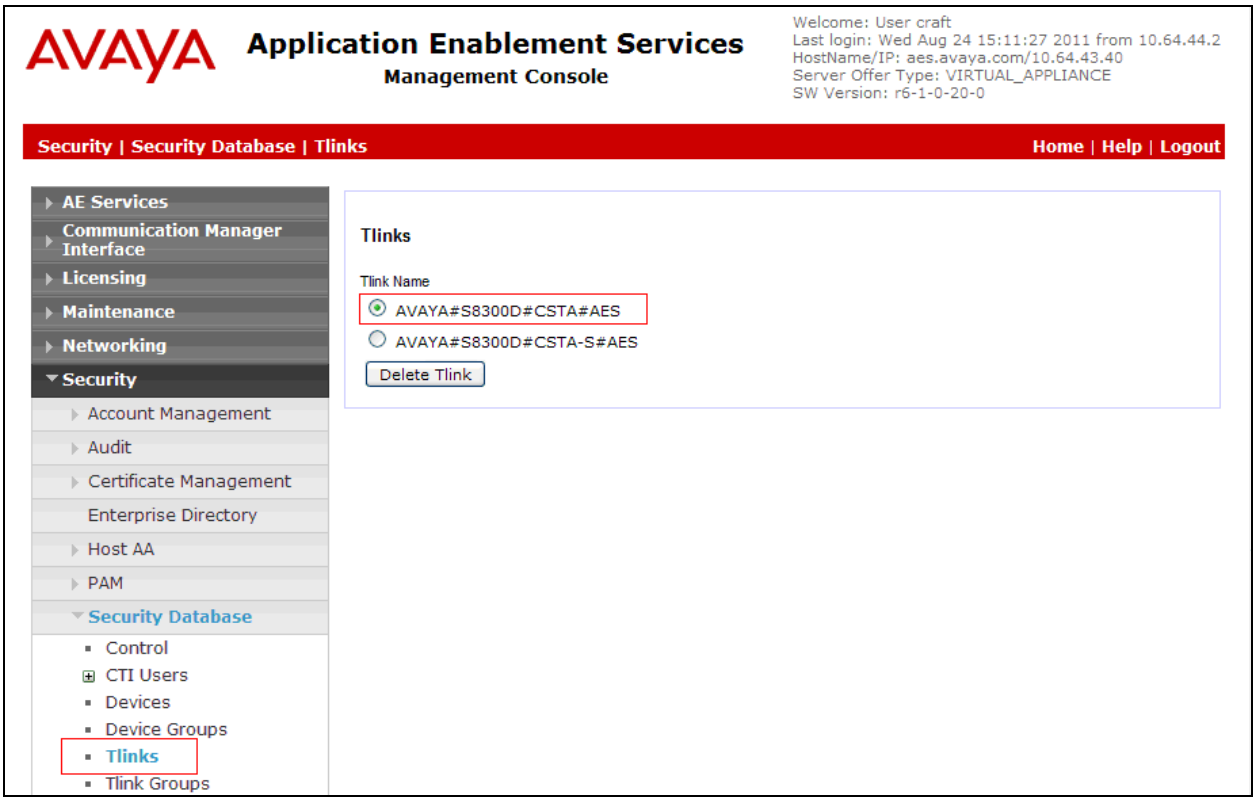
Once the user is created, navigate to the **Security → Security Database → CTI Users → List All Users** page. Select the **User ID** created previously, and click the **Edit** button to set the permission of the user.



Provide the user with unrestricted access privileges by checking the **Unrestricted Access** check box. Click the **Apply Changes** button.



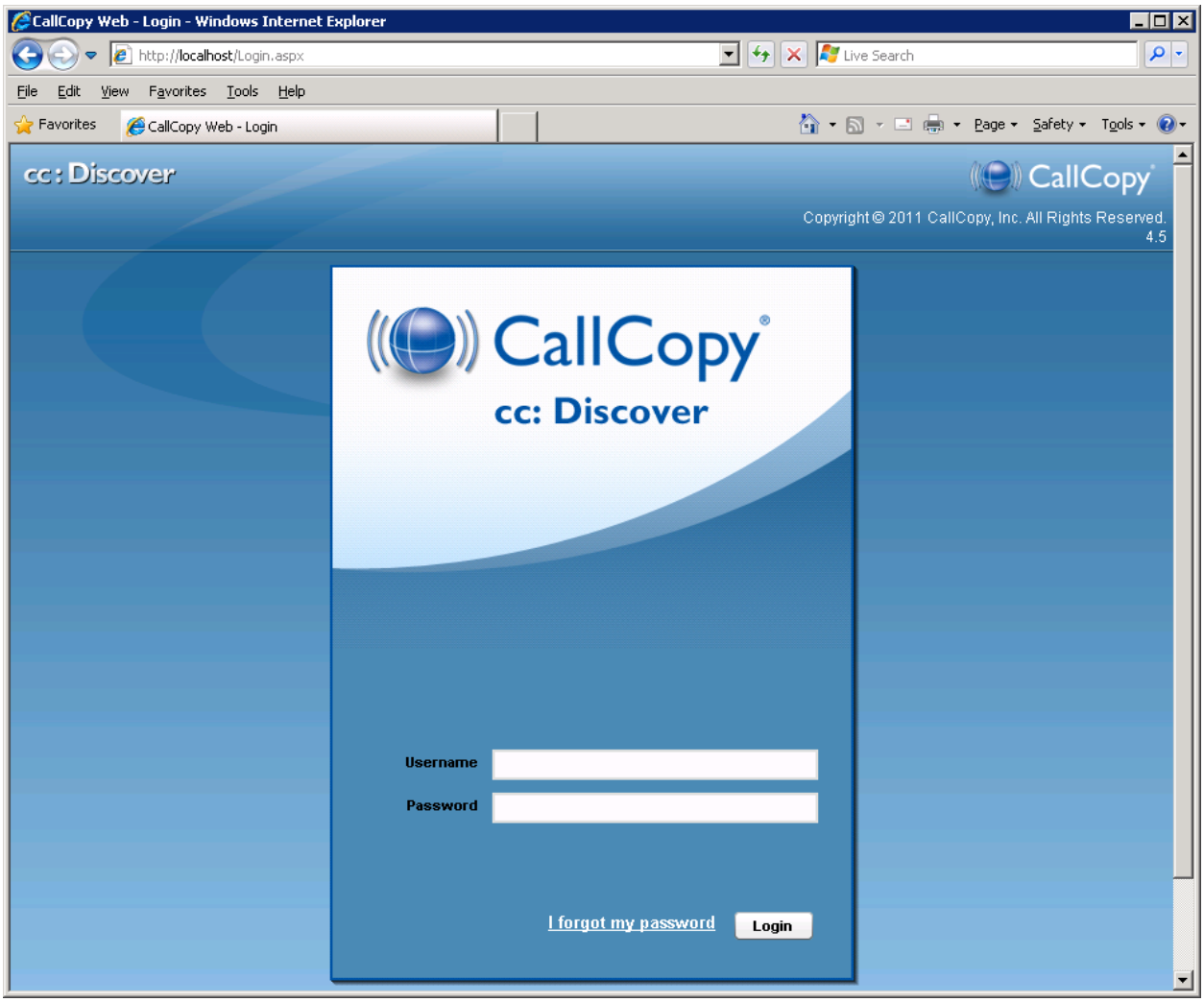
Navigate to the **Security → Security Database → Tlinks** page and verify the Tlink name. The following screen shows the Tlink used during the compliance test.



7. Configure CallCopy cc:Discover

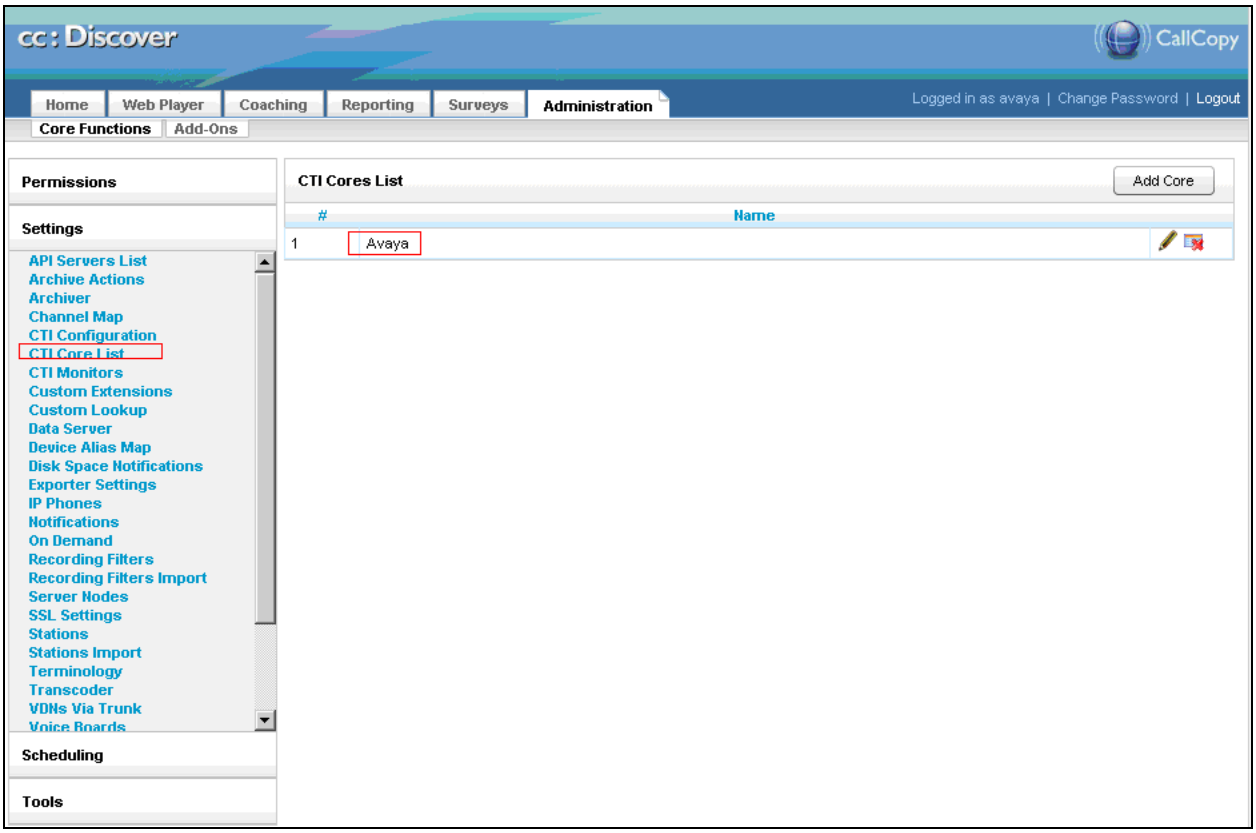
CallCopy installs, configures, and customizes the cc:Discover application for their end customers. This section only describes the interface section of the cc:Discover configuration.

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.

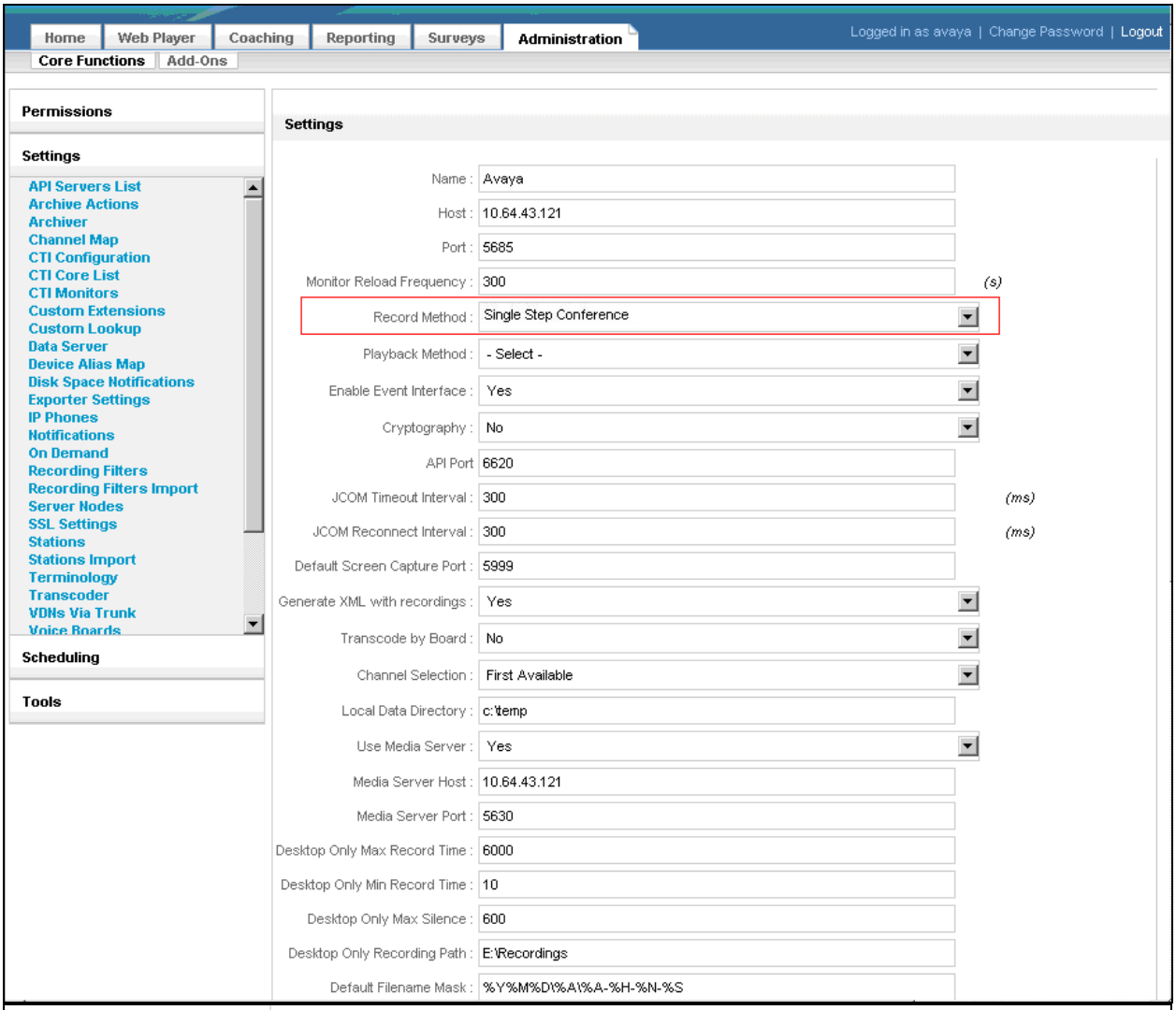


Select **Administration** on the top menu**,** and select the **Settings → CTI Core List** link from the left pane to configure the interface. From the right pane, select **Avaya**.

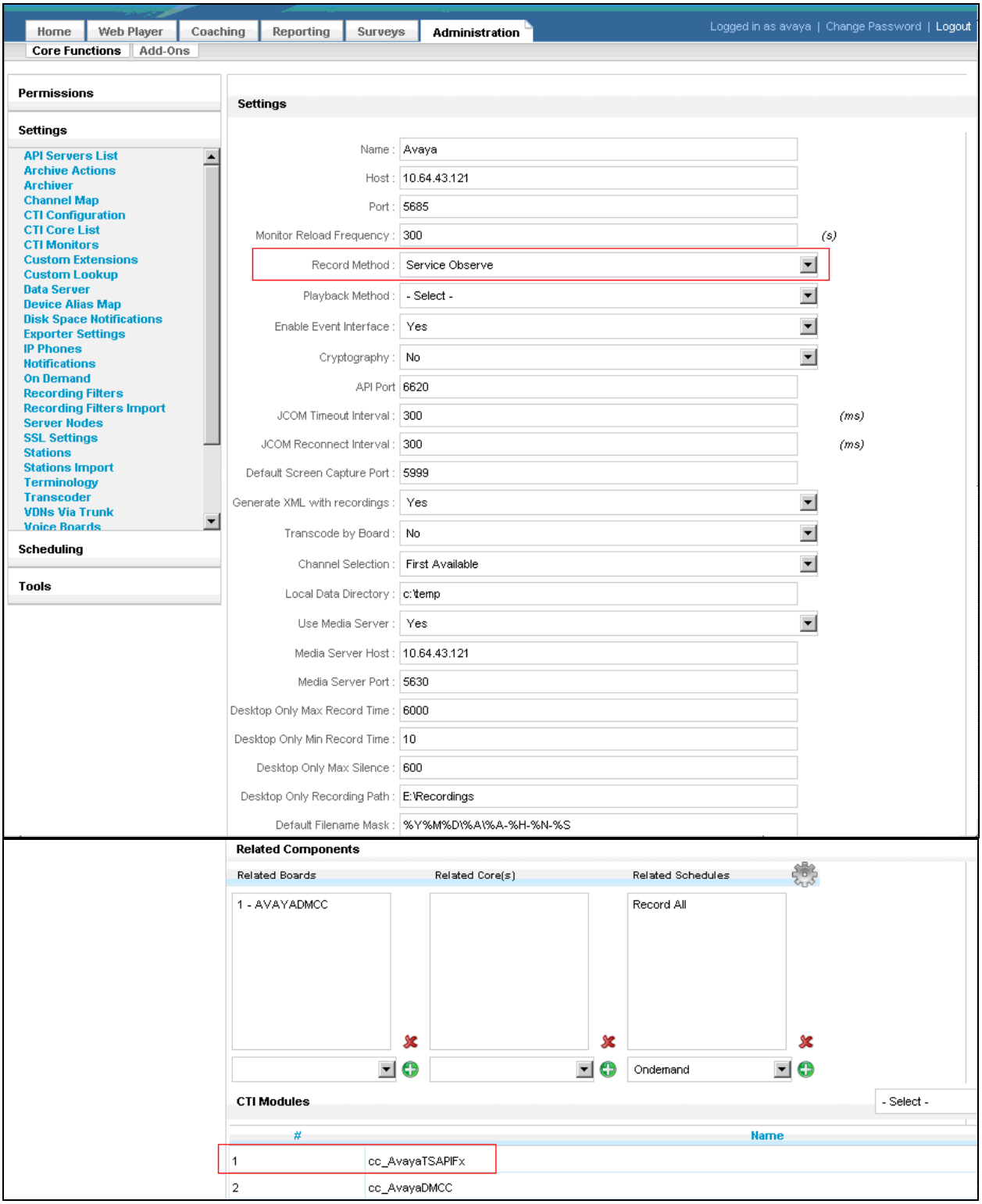
Note: *Avaya (CTI Core List) was created by a CallCopy engineer prior to the actual test.*



The following two screens show the CTI Settings screen for Single Step Conference recording solution. Select **Single Step Conference** as the **Record Method**, using the drop down list. In the second screen, double click **cc_AvayaTSAPIFx**.



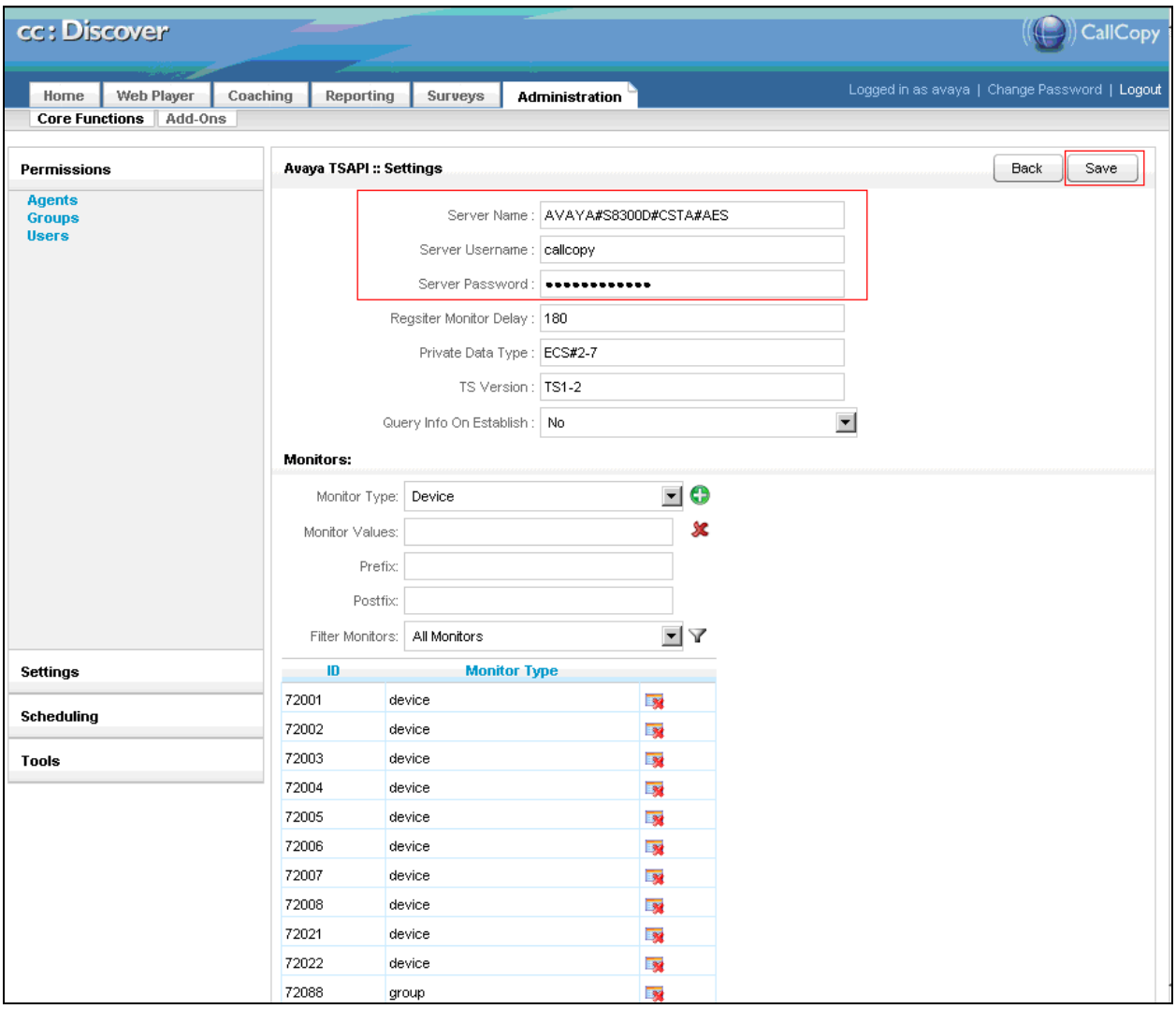
The following two screens show the CTI Settings screen for the Service Observe recording solution. Select **Service Observe** as the **Record Method**, using the drop down list. In the second screen, double click **cc_AvayaTSAPIFx**.



The following screen displays the **Avaya TSAPI:: Settings** page. Provide the following information:

- **Server Name –** Enter the **TLink** name used in Application Enablement Services for the CTI Connect String field.
- **Server Username** – Enter an appropriate CTI username that was created in **Section 6.3**.
- **Server Password** – Enter an appropriate CTI password that was created in **Section 6.3**.

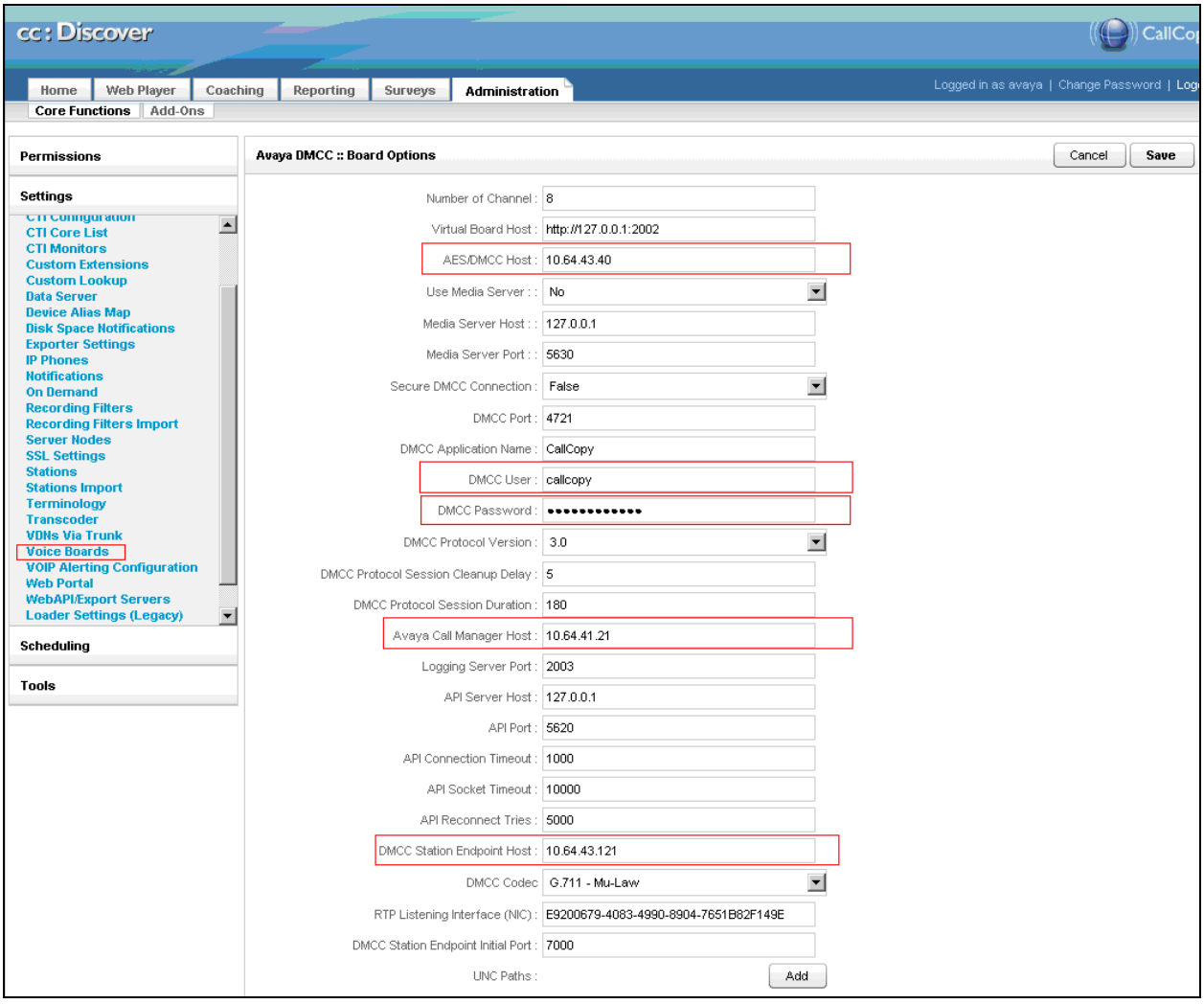
Click the **Save** button.



Select the **Voice Boards** link under the **Settings** section. To add a new board, click **Add Board** (not shown). From the **New Board** page, select **AVAYACMCC** as a Hardware Type, and click **Next** button (not shown). Provide the following information:

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

Click the **Save** button.
Default values may be used for all other fields.



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

Board1 of 1 :: Channel Configuration

#	Assign	Station	Password	Name
1	Anything	72501	1234	
2	Anything	72502	1234	
3	Anything	72503	1234	
4	Anything	72504	1234	
5	Anything	72505	1234	
6	Anything	72506	1234	
7	Anything	72507	1234	
8	Anything	72508	1234	

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and Application Enablement Services.

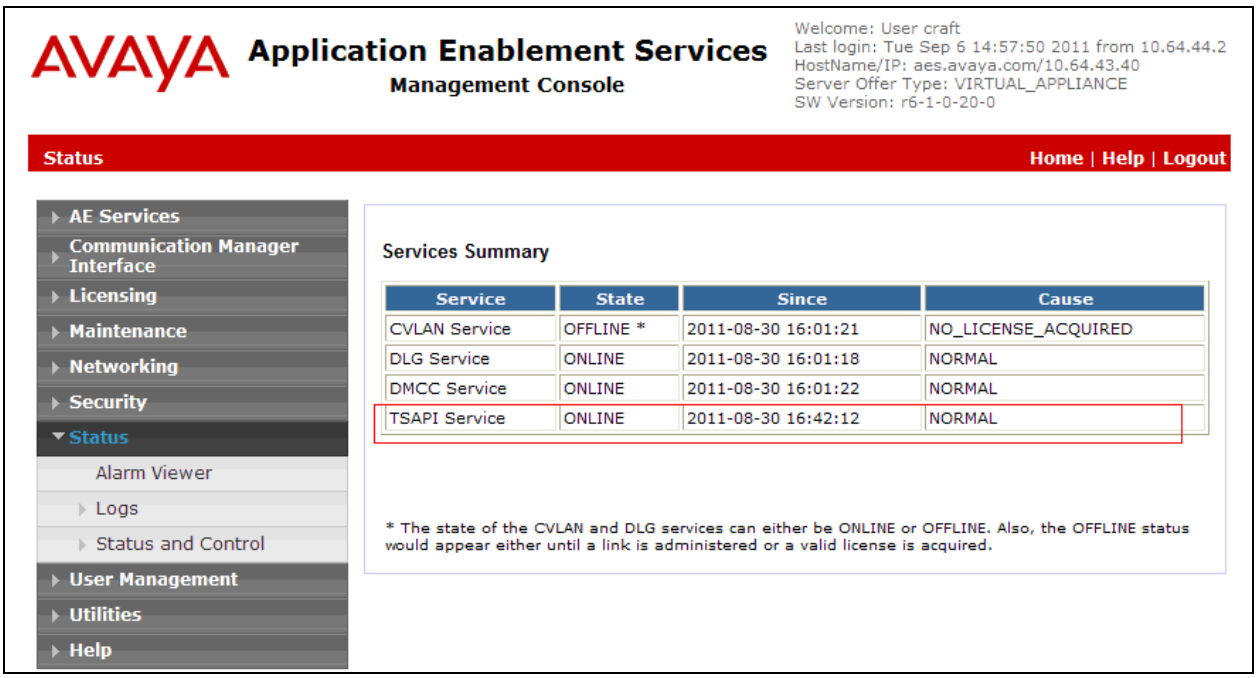
8.1. Verify Avaya Aura® Communication Manager

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 5.6**, as shown below.

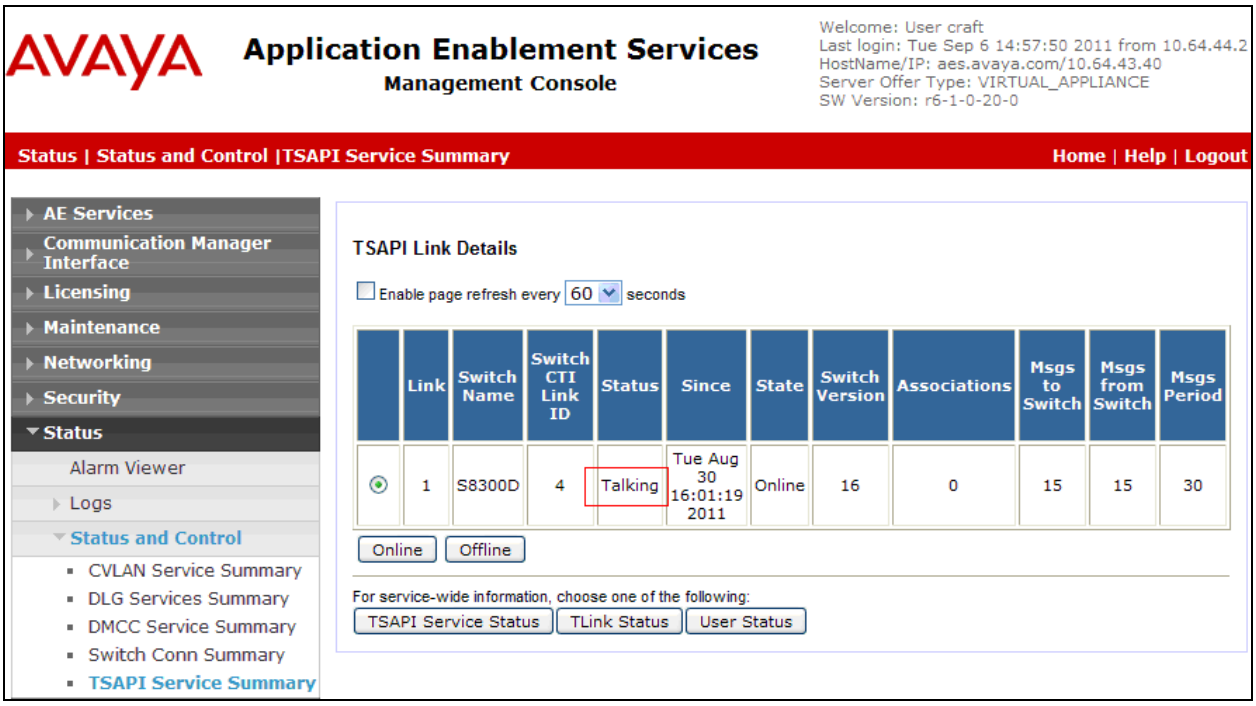
```
status aesvcs cti-link

                        AE SERVICES CTI LINK STATUS

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

1               no                      down           0        0
4      4        no     aes              established    15       15
```

8.2. Verify Avaya Aura® Application Enablement Services

From the Application Enablement Services Management Console web pages, verify the state of the TSAPI Service is set to **ONLINE** by selecting **Status** from the left pane.



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



9. Conclusion

These Application Notes describe the configuration steps required for CallCopy cc:Discover (Version 4.5 SP1) to interoperate with Avaya Aura® Communication Manager 6.0.1 and Avaya Application Enablement Services 6.1. 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] *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, June 2010 available at http://support.avaya.com.
[2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 20011 available at http://support.avaya.com
[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.