



**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.

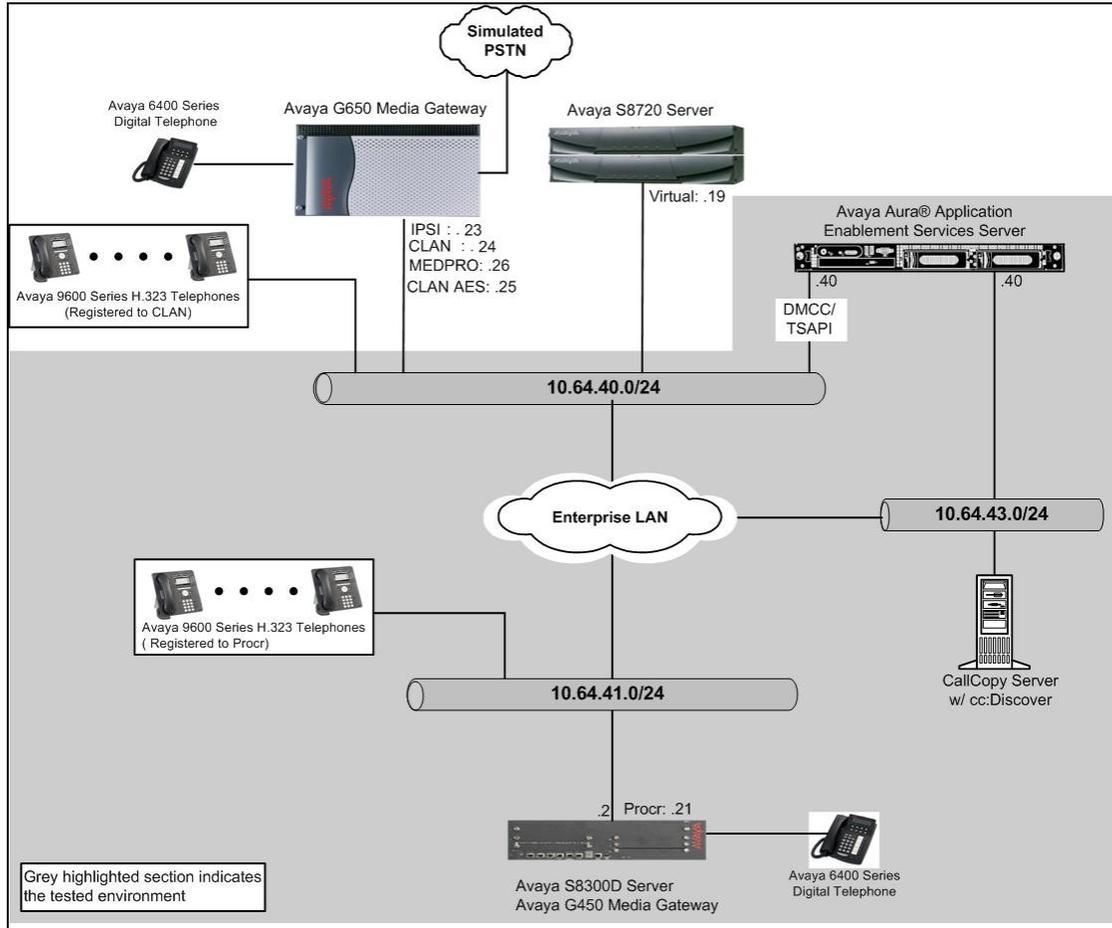


Figure 1: CallCopy cc:Discover with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services

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)	3.1
	9630 (H.323)	3.1
Avaya 9600 Series SIP Telephones		
	9630 (SIP)	2.6.4
	9640 (SIP)	2.6.4
	9650 (SIP)	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:
    Call Handling Preference: skill-level                    Service Objective? n
                                                            Local Call Preference? n

    SN  RL  SL          SN  RL  SL
    1:  88  1          16:
    2:
    3:
    4:
    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 **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 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        Type      Node    Port    Node     Port
AESVCS      y         procr   8765
CDR1        0         procr   0       pcr      5852
CDR2        0         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 Server	Password	Enabled	Status
1:	aes	[REDACTED]	y	idle
2:				
3:				
4:				
5:				
6:				

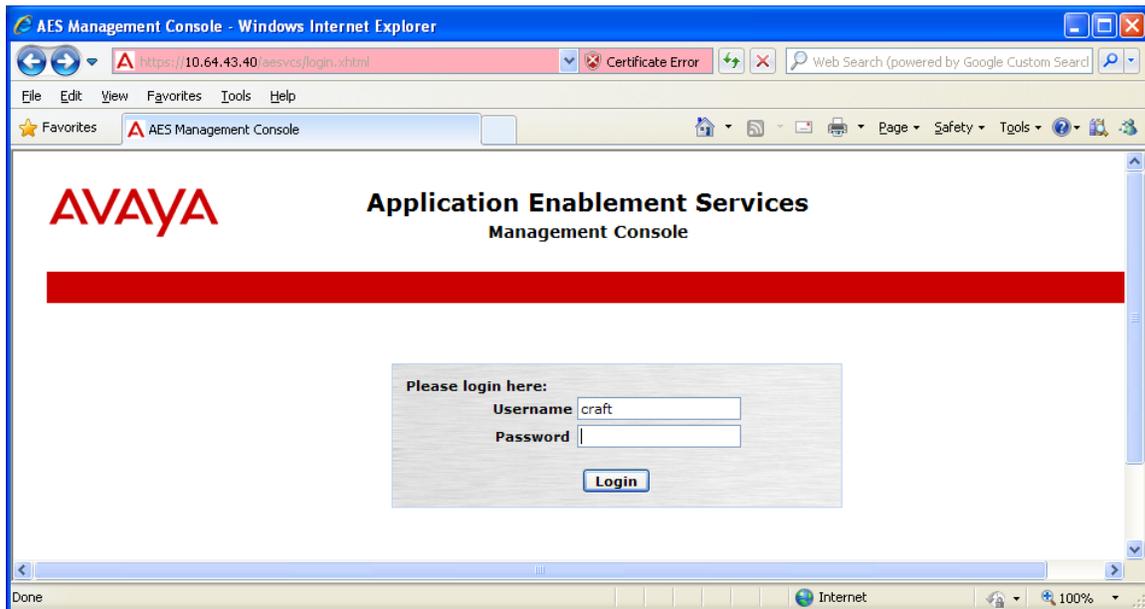
6. Configure Avaya Application Enablement Services

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.

AVAYA Application Enablement Services Management Console

Welcome: User craft
 Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2
 HostName/IP: aes.avaya.com/10.64.43.40
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r6-1-0-20-0

Home | Help | Logout

Home

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

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:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status infomations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

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

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

AVAYA Application Enablement Services Management Console

Welcome: User craft
 Last login: Wed Aug 31 09:39:49 2011 from 10.64.44.2
 HostName/IP: aes.avaya.com/10.64.43.40
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r6-1-0-20-0

Home | Help | Logout

AE Services

- AE Services
 - CVLAN
 - DLG
 - DMCC
 - SMS
 - TSAPI
 - TWS
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

AE Services

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	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	ONLINE	Running	NORMAL MODE	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
 You are licensed to run Application Enablement (CTI) version 6.0

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**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
 Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2
 HostName/IP: aes.avaya.com/10.64.43.40
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r6-1-0-20-0

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

S8300D Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8300D			

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

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**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
 Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2
 HostName/IP: aes.avaya.com/10.64.43.40
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r6-1-0-20-0

Communication Manager Interface | Switch Connections Home | Help | Logout

Connection Details - S8300D

Switch Password [REDACTED]

Confirm Switch Password [REDACTED]

Msg Period 30 Minutes (1 - 72)

SSL

Processor Ethernet

Apply Cancel

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**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
 Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2
 HostName/IP: aes.avaya.com/10.64.43.40
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r6-1-0-20-0

Communication Manager Interface | Switch Connections Home | Help | Logout

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	0

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

AVAYA Application Enablement Services Management Console

Welcome: User craft
 Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2
 HostName/IP: aes.avaya.com/10.64.43.40
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r6-1-0-20-0

Communication Manager Interface | Switch Connections Home | Help | Logout

Name or IP Address	Status
<input type="text" value="10.64.41.21"/>	

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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title 'Application Enablement Services Management Console', and user information: 'Welcome: User craft', 'Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2', 'HostName/IP: aes.avaya.com/10.64.43.40', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r6-1-0-20-0'. The main navigation menu on the left includes 'AE Services', 'Communication Manager Interface', 'Switch Connections', 'Dial Plan', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The 'Switch Connections' page displays a table with the following data:

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8300D	No	30	0

Below the table are several buttons: 'Add Connection', 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper' (highlighted), 'Delete Connection', and 'Survivability Hierarchy'.

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

The screenshot shows the 'Edit H.323 Gatekeeper - S8300D' page in the Avaya Application Enablement Services Management Console. The top navigation bar and user information are the same as in the previous screenshot. The main navigation menu on the left is also the same. The page title is 'Edit H.323 Gatekeeper - S8300D'. Below the title, there is a text input field containing '10.64.41.21' and an 'Add Name or IP' button (highlighted). Below the input field is the label 'Name or IP Address'. At the bottom of the page, there are two buttons: 'Delete IP' and 'Back'.

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.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title "Application Enablement Services Management Console", and a user welcome message: "Welcome: User craft", "Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2", "HostName/IP: aes.avaya.com/10.64.43.40", "Server Offer Type: VIRTUAL_APPLIANCE", and "SW Version: r6-1-0-20-0". The main navigation bar shows "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar lists "AE Services" with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, TWS, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. The main content area is titled "TSAPI Links" and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are three buttons: "Add Link" (highlighted with a red box), "Edit Link", and "Delete 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 screenshot shows the Avaya Application Enablement Services Management Console with the "Add TSAPI Links" form. The top navigation bar and user welcome message are the same as in the previous screenshot. The left sidebar is the same, with "TSAPI Links" selected. The main content area is titled "Add TSAPI Links" and contains the following fields: "Link" (dropdown menu with "1" selected), "Switch Connection" (dropdown menu with "S8300D" selected, highlighted with a red box), "Switch CTI Link Number" (dropdown menu with "4" selected, highlighted with a red box), "ASAI Link Version" (dropdown menu with "4" selected), and "Security" (dropdown menu with "Both" selected). At the bottom of the form are two buttons: "Apply Changes" (highlighted with a red box) and "Cancel Changes".

The following screen shows the TSAPI CTI link configuration.

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
- ▶ TWS
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8300D	4	4	Both

[Add Link](#) [Edit Link](#) [Delete Link](#)

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.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

User Management | User Admin | Add User Home | Help | Logout

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Service Admin
User Admin
Add User
Change User Password
List All Users
Modify Default Users
Search Users

Add User

Fields marked with * can not be empty.

* User Id callcopy
* Common Name Callcopy123&
* Surname Callcopy123&
* User Password
* Confirm Password

Admin Note
Avaya Role None
Business Category
Car License
CM Home
CSS Home
CT User Yes

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.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes 'Security | Security Database | CTI Users | List All Users' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'Security Database' expanded to 'CTI Users' and 'List All Users' selected. The main content area displays a table of CTI Users:

User ID	Common Name	Worktop Name	Device ID
callcopy	Callcopy123&	NONE	NONE

Below the table are 'Edit' and 'List All' buttons. The 'Edit' button is highlighted with a red box.

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

The screenshot shows the 'Edit CTI User' page in the Avaya Application Enablement Services Management Console. The top navigation bar includes 'Security | Security Database | CTI Users | List All Users' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'Security Database' expanded to 'CTI Users' and 'List All Users' selected. The main content area displays the 'Edit CTI User' form:

Edit CTI User

User Profile:

- User ID: callcopy
- Common Name: Callcopy123&
- Worktop Name: NONE
- Unrestricted Access:

Call and Device Control:

- Call Origination/Termination and Device Status: None

Call and Device Monitoring:

- Device Monitoring: None
- Calls On A Device Monitoring: None
- Call Monitoring:

Routing Control:

- Allow Routing on Listed Devices: None

At the bottom of the form are 'Apply Changes' and 'Cancel Changes' buttons. The 'Apply Changes' button is highlighted with a red box.

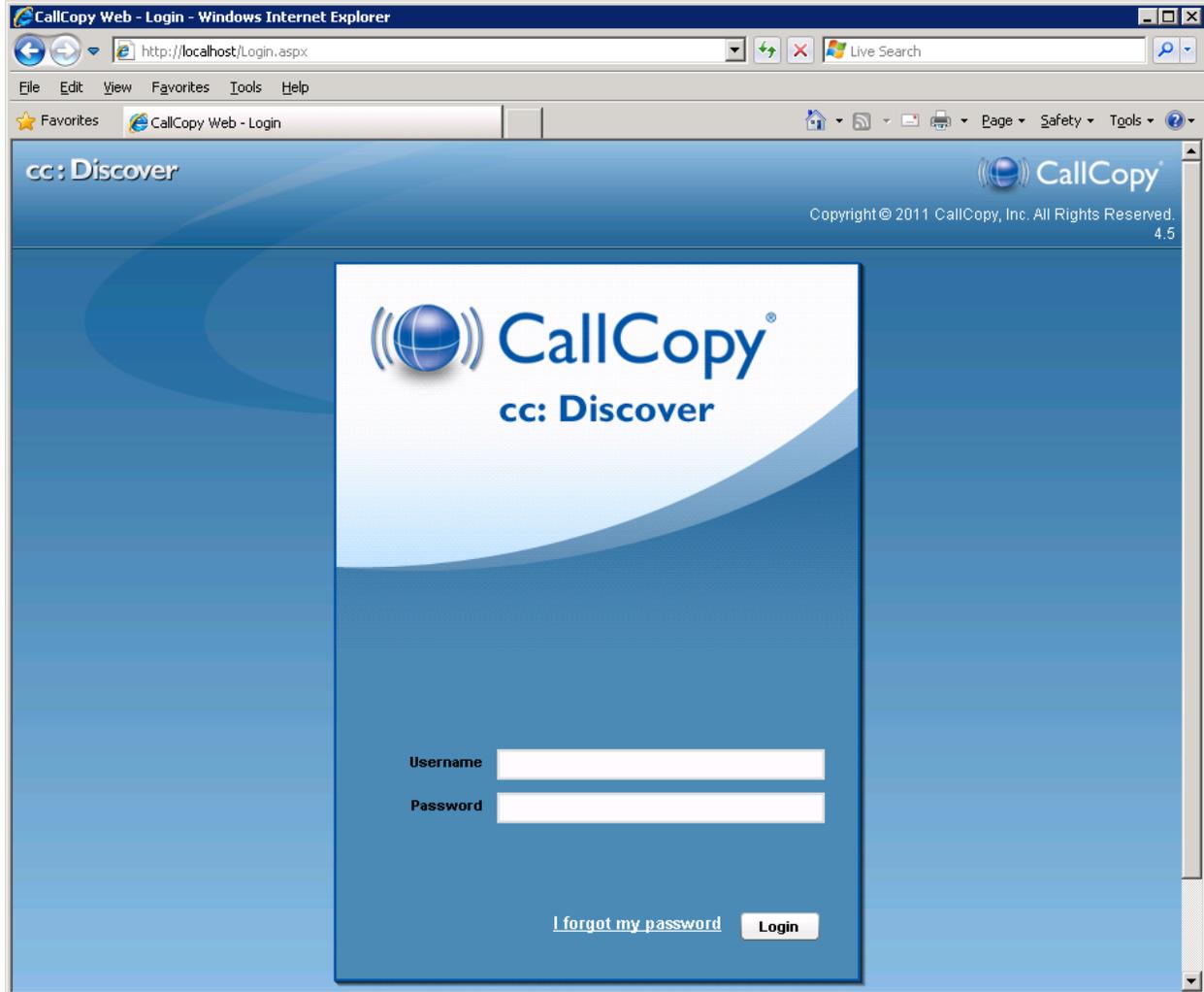
Navigate to the **Security** → **Security Database** → **Tlinks** page and verify the Tlink name. The following screen shows the Tlink used during the compliance test.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and user information: "Welcome: User craft", "Last login: Wed Aug 24 15:11:27 2011 from 10.64.44.2", "HostName/IP: aes.avaya.com/10.64.43.40", "Server Offer Type: VIRTUAL_APPLIANCE", and "SW Version: r6-1-0-20-0". A red navigation bar contains "Security | Security Database | Tlinks" and "Home | Help | Logout". On the left, a sidebar menu shows "Security Database" expanded to "Tlinks". The main content area, titled "Tlinks", shows a "Tlink Name" section with two radio buttons: "AVAYA#S8300D#CSTA#AES" (selected) and "AVAYA#S8300D#CSTA-S#AES". A "Delete Tlink" button is also present.

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 screenshot shows the 'cc: Discover' web interface. The top navigation bar includes 'Home', 'Web Player', 'Coaching', 'Reporting', 'Surveys', and 'Administration'. The user is logged in as 'avaya'. The left sidebar is expanded to 'Settings', with 'CTI Core List' selected. The main content area is titled 'CTI Cores List' and contains a table with the following data:

#	Name
1	Avaya

There is an 'Add Core' button in the top right of the table area.

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 screenshot displays the 'Administration' section of a web application, specifically the 'Settings' page for CTI. The 'Record Method' dropdown is highlighted with a red box and set to 'Single Step Conference'. Other settings include Name: Avaya, Host: 10.64.43.121, Port: 5685, and Monitor Reload Frequency: 300 (s). The 'Related Components' section at the bottom features a table of CTI Modules:

#	Name
1	cc_AvayaTSAPIFx
2	cc_AvayaDMCC

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 screenshot displays the CTI Settings interface. The top navigation bar includes Home, Web Player, Coaching, Reporting, Surveys, and Administration. The left sidebar shows a tree view with categories like Permissions, Settings, Scheduling, and Tools. The main content area is titled 'Settings' and contains various configuration fields. The 'Record Method' dropdown is highlighted with a red box and set to 'Service Observe'. Below the settings is a 'Related Components' section with three columns: Related Boards, Related Core(s), and Related Schedules. At the bottom, a 'CTI Modules' table lists modules, with 'cc_AvayaTSAPIFx' highlighted by a red box.

#	Name
1	cc_AvayaTSAPIFx
2	cc_AvayaDMCC

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.

The screenshot shows the 'Avaya TSAPI :: Settings' page. The 'Server Name' field is highlighted with a red box and contains 'AVAYA#S8300D#CSTA#AES'. The 'Server Username' field contains 'callcopy' and the 'Server Password' field contains a masked password. Other fields include 'Register Monitor Delay' (180), 'Private Data Type' (ECS#2-7), 'TS Version' (TS1-2), and 'Query Info On Establish' (No). The 'Monitors' section shows a table with columns 'ID' and 'Monitor Type'.

ID	Monitor Type
72001	device
72002	device
72003	device
72004	device
72005	device
72006	device
72007	device
72008	device
72021	device
72022	device
72088	group

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 IP address 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 screenshot displays the 'Avaya DMCC :: Board Options' configuration page. The interface includes a navigation menu on the left with 'Voice Boards' highlighted. The main area contains the following configuration fields:

- Number of Channel: 8
- Virtual Board Host: http://127.0.0.1:2002
- AES/DMCC Host: 10.64.43.40
- Use Media Server: No
- Media Server Host: 127.0.0.1
- Media Server Port: 5630
- Secure DMCC Connection: False
- DMCC Port: 4721
- DMCC Application Name: CallCopy
- DMCC User: callcopy
- DMCC Password: [Masked]
- DMCC Protocol Version: 3.0
- DMCC Protocol Session Cleanup Delay: 5
- DMCC Protocol Session Duration: 180
- Avaya Call Manager Host: 10.64.41.21
- 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: 10.64.43.121
- DMCC Codec: G.711 - Mu-Law
- RTP Listening Interface (NIC): E9200679-4083-4990-8904-7651B82F149E
- DMCC Station Endpoint Initial Port: 7000

UNC Paths: [Add]

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 <input type="text" value="72501"/>	1234 <input type="text"/>	<input type="text"/>
2	Anything <input type="text" value="72502"/>	1234 <input type="text"/>	<input type="text"/>
3	Anything <input type="text" value="72503"/>	1234 <input type="text"/>	<input type="text"/>
4	Anything <input type="text" value="72504"/>	1234 <input type="text"/>	<input type="text"/>
5	Anything <input type="text" value="72505"/>	1234 <input type="text"/>	<input type="text"/>
6	Anything <input type="text" value="72506"/>	1234 <input type="text"/>	<input type="text"/>
7	Anything <input type="text" value="72507"/>	1234 <input type="text"/>	<input type="text"/>
8	Anything <input type="text" value="72508"/>	1234 <input type="text"/>	<input type="text"/>

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 Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs 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.

Welcome: User craft
Last login: Tue Sep 6 14:57:50 2011 from 10.64.44.2
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-0-20-0

AVAYA Application Enablement Services Management Console

Status [Home](#) | [Help](#) | [Logout](#)

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status**
- Alarm Viewer
- Logs
- Status and Control
- User Management
- Utilities
- Help

Service	State	Since	Cause
CVLAN Service	OFFLINE *	2011-08-30 16:01:21	NO_LICENSE_ACQUIRED
DLG Service	ONLINE	2011-08-30 16:01:18	NORMAL
DMCC Service	ONLINE	2011-08-30 16:01:22	NORMAL
TSAPI Service	ONLINE	2011-08-30 16:42:12	NORMAL

* The state of the CVLAN and DLG services can either be ONLINE or OFFLINE. Also, the OFFLINE status would appear either until a link is administered or a valid license is acquired.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes 'Status | Status and Control | TSAPI Service Summary' and 'Home | Help | Logout'. The left sidebar lists various services, with 'Status' expanded to show 'TSAPI Service Summary'. The main content area displays 'TSAPI Link Details' with a table of link information. The 'Status' column for the first link is highlighted with a red box and shows 'Talking'. Below the table are buttons for 'Online' and 'Offline', and a section for service-wide information with buttons for 'TSAPI Service Status', 'TLink Status', and 'User Status'.

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	S8300D	4	Talking	Tue Aug 30 16:01:19 2011	Online	16	0	15	15	30

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 2011 available at <http://support.avaya.com>
- [3] *CallCopy Avaya DMCC Integration*.
- [4] *CallCopy Avaya TSAPI Integration*.

©2011 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.