



Avaya Solution & Interoperability Test Lab

Application Notes for Cacti FocusRecord with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cacti's FocusRecord to interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES). The objective of the test was to evaluate the ability of FocusRecord to issue a Single-Step Conference Request through events acquired from the Telephony Services Application Programming Interface (TSAPI). In the configuration discussed in these Application Notes, Cacti FocusRecord employs Device, Media and Call Control (DMCC) API (formally known as CMAPI) virtual stations as recording ports. During compliance testing, Cacti FocusRecord successfully recorded contact center calls placed to and from stations, as well as calls placed to a hunt group and then redirected to agents.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer Connection Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Cacti FocusRecord Application monitors, records, stores, and plays back phone calls for verification. FocusRecord uses TSAPI with an Application Enablement Services (AES) server to monitor stations, agents, and/or VDNs, i.e., to obtain recording triggers and call information. FocusRecord also uses the Device, Media and Call Control (DMCC) API (formally known as CMAPI) with the AES server to register DMCC softphones that FocusRecord uses as recording ports. When recording of a call is desired, FocusRecord issues a Single Step Conference request through events acquired from TSAPI.

The interoperability of FocusRecord Version 2.45 with Avaya Communication Manager is accomplished through Application Enablement Services. These Application Notes describe the compliance test configuration used to test Cacti's FocusRecord Version 2.45, with Avaya Communication Manager running on an Avaya S8300 Server and an Avaya G350 Media Gateway.

1.1. Interoperability Compliance Testing

The Compliance testing focused on the following areas, covered in the DevConnect Test Plan for Avaya Communication Manager and Application Enablement Services and Cacti's FocusRecord:

Phase 1 Installation & Configuration

Phase 2 FocusRecord/Avaya Feature Functionality Verification

Phase 3 Failover and Serviceability Tests

The installation and configuration testing focused on the setup of all components and the ability to interoperate. It also covered the ability to remove the application from the system.

The functionality testing focused on verifying FocusRecord's ability to use real-time data from Avaya Communication Manager and Application Enablement Services to record contact center calls.

The serviceability testing focused on verifying the ability of FocusRecord to recover from and report on adverse conditions.

1.2. Support

For technical support on FocusRecord, contact Cacti at +1 866 34CACTI or put in a service request at <http://support.cacti-inc.com>.

2. Reference Configuration

The interoperability of FocusRecord with Avaya Communication Manager is accomplished through Application Enablement Services. The compliance test configuration used to test FocusRecord includes the Avaya S8300 Server, the Avaya G350 Media Gateway, Application Enablement Services, Windows 2003 Server running FocusRecord, and telephones. The solution described herein is also extensible to other Avaya Servers and Media Gateways. **Figure 1** provides a high level topology for the configuration used in the compliance test.

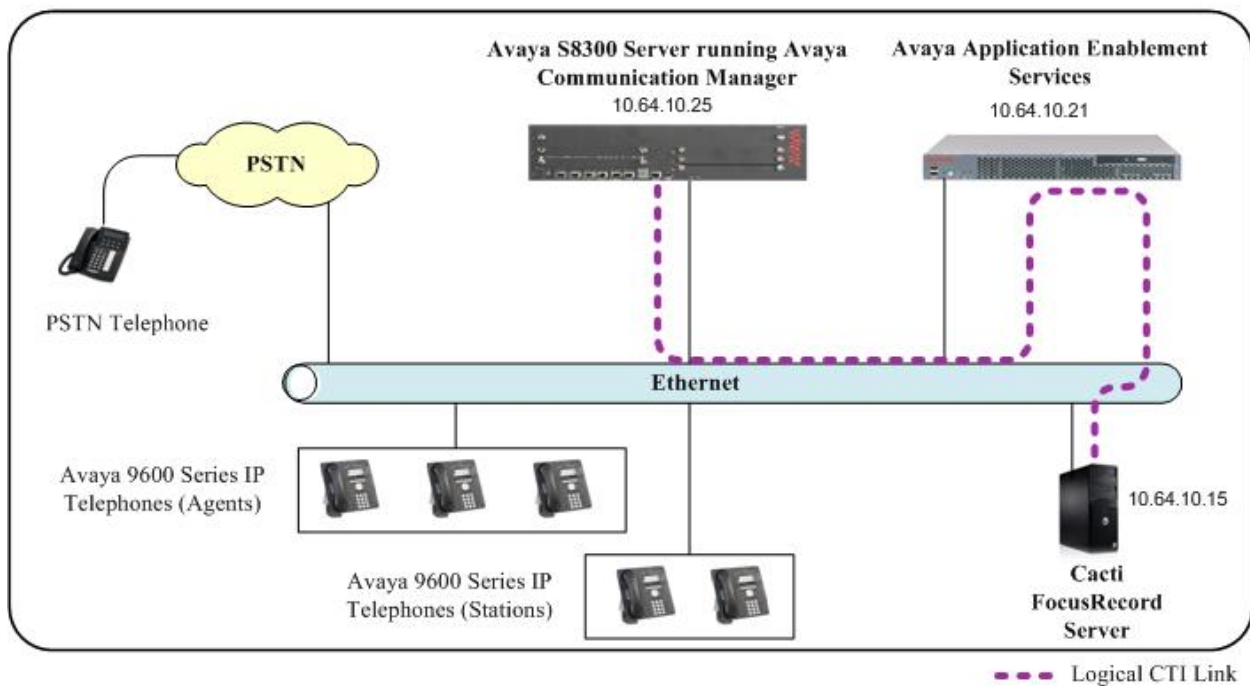


Figure 1: Test Configuration for the Cacti FocusRecord Solution

3. Equipment and Software Validated

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

Hardware/Software Component	Version/Description
Avaya S8300 Server and G350 Media Gateway	Avaya Communication Manager 4.0 (R014x.00.0.730.5) with Service Pack 13566
Avaya Application Enablement Services	Release 4.2
Avaya 9600 Series IP Telephones	9620, 9630, 9640 Terminals R2.0 (H.323)
Avaya IP Agent, Avaya one-X™ Agent	R7.0, R1
Cacti FocusRecord running on Windows 2003 Standard Edition Server	Version 2.45

4. Configure Avaya Communication Manager

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

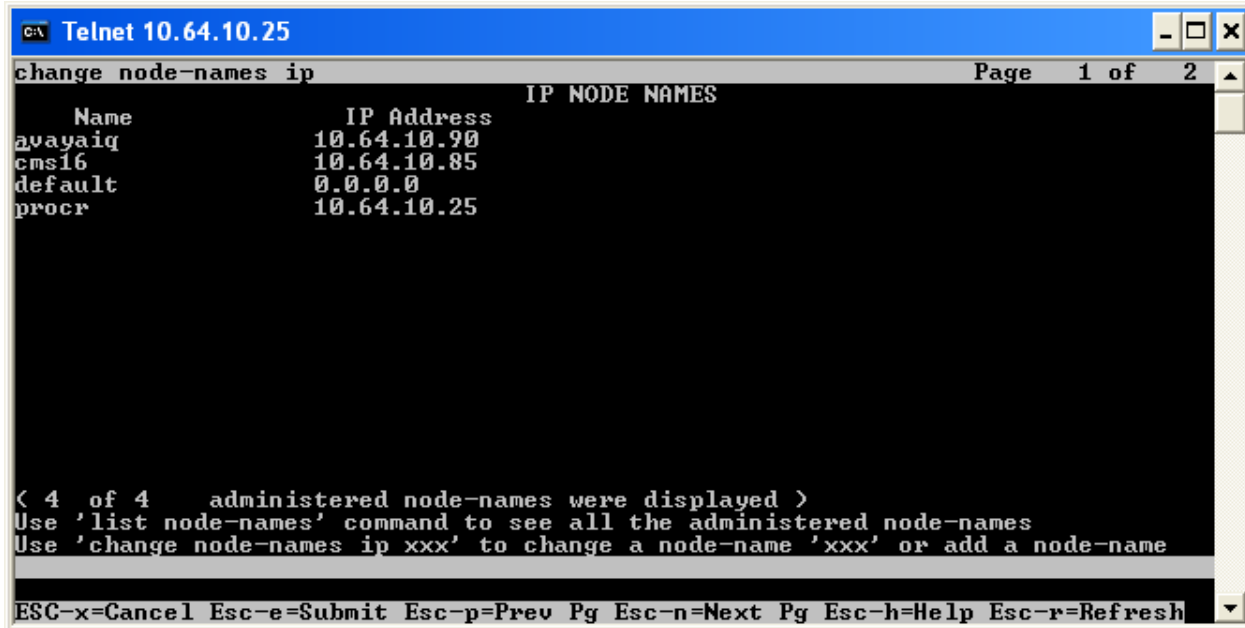
This section provides the procedures for configuring Avaya Communication Manager. The procedures fall into the following areas:

- Administer Processor Ethernet Interface for Application Enablement Services Connectivity
- Configure Hunt/Skill Groups, Agent Logins, and Call Vectoring
- Create Recording Stations
- Create Recorded (Monitored) Stations
- Administer CTI Link

4.1. Administer Processor Ethernet Interface for AES Connectivity

Verify the entry for the Processor Ethernet Interface in the node-names form.

- Enter the **change node-names ip** command. In this case, **procr** and **10.64.10.25** are already populated as Name and IP Address for the Processor Ethernet Interface that is used for connectivity to the AES server. The actual IP address may vary. Submit changes.



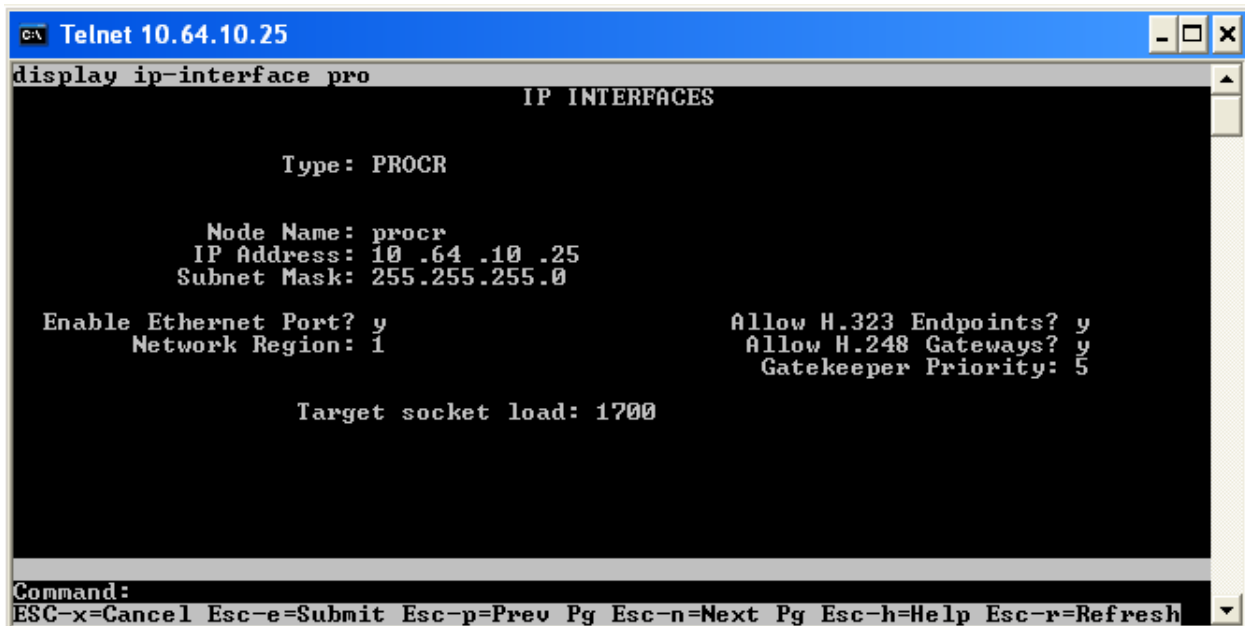
```
C:\ Telnet 10.64.10.25
change node-names ip                                     Page 1 of 2
IP NODE NAMES
Name      IP Address
avayaiaq  10.64.10.90
cms16     10.64.10.85
default   0.0.0.0
procr     10.64.10.25

< 4 of 4 administered node-names were displayed >
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

On an S8300, the Processor Ethernet Interface should already be in the ip-interface list.

- Either the **display ip-interface procr** command or the **list ip-interface all** command will display the parameters of the Processor Ethernet Interface on the S8300.



```
C:\ Telnet 10.64.10.25
display ip-interface pro                                IP INTERFACES

Type: PROCR

Node Name: procr
IP Address: 10 .64 .10 .25
Subnet Mask: 255.255.255.0

Enable Ethernet Port? y
Network Region: 1
Allow H.323 Endpoints? y
Allow H.248 Gateways? y
Gatekeeper Priority: 5

Target socket load: 1700

Command:
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

```

C:\ Telnet 10.64.10.25
list ip-interface all

```

IP INTERFACES									
ON	Type	Slot	Code	Sfx	Node Name/ IP-Address	Subnet Mask	Gateway Address	Net Rgn	ULAN
y	PROCR				10.64.10.25	255.255.255.0	10.64.10.1	1	

```

Command successfully completed
Command:
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

```

Add an entry for IP Services with the following values for fields on **Page 1**, as displayed below:

- 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 the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, retain the default of 8765.

```

C:\ Telnet 10.64.10.25
change ip-services

```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

```

Page 1 of 3
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

```

Go to **Page 3** of the IP Services form, and enter the following values:

- In the **AE Services Server** field, type the name obtained from the AES server, in this case **aesserver2**.
- In the **Password** field, type the same password to be administered on the AES server, in this case **aes1password**.
- In the **Enabled** field, type **y**.

Server ID	AE Services Server	Password	Enabled	Status
1:	aesserver2	aes1password	y	in use
2:				
3:				
4:				
5:				
6:				
7:				
8:				
9:				
10:				
11:				
12:				
13:				
14:				
15:				
16:				

Note that the name and password entered for the **AE Services Server** and **Password** fields must match the hostname and password on the AES server. The administered name for the AES server is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt. The same password entered above will need to be set on the AES server using **Administration -> Switch Connections -> Edit Connection -> Set Password**. For detailed information on AES, see Section 5 Configure Application Enablement Services.

4.2. Configure Hunt/Skill Groups, Agent Logins, and Call Vectoring

Go to **Page 6** of the system-parameters customer-options form, and verify the following values:

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

```
Telnet 10.64.10.25
display system-parameters customer-options Page 6 of 11
CALL CENTER OPTIONAL FEATURES_
Call Center Release: 4.0
ACD? y Reason Codes? y
BCMS <Basic>? y Service Level Maximizer? n
BCMS/UuStats Service Level? n Service Observing <Basic>? y
BSR Local Treatment for IP & ISDN? y Service Observing <Remote/By FAC>? y
Business Advocate? n Service Observing <UDNs>? y
Call Work Codes? n Timed ACW? y
DTMF Feedback Signals For URU? n Vectoring <Basic>? y
Dynamic Advocate? n Vectoring <Prompting>? y
Expert Agent Selection <EAS>? y Vectoring <G3U4 Enhanced>? y
EAS-PHD? n Vectoring <3.0 Enhanced>? y
Forced ACD Calls? n Vectoring <ANI/II-Digits Routing>? y
Least Occupied Agent? y Vectoring <G3U4 Advanced Routing>? y
Lookahead Interflow <LAI>? n Vectoring <CINFO>? n
Multiple Call Handling <On Request>? n Vectoring <Best Service Routing>? y
Multiple Call Handling <Forced>? n Vectoring <Holidays>? y
PASTE <Display PBX Data on Phone>? n Vectoring <Variables>? y
<NOTE: You must logoff & login to effect the permission changes.>
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

Add an entry for a hunt group with the following values as displayed below:

- Enter the **add hunt-group x** command, where **x** is an unused hunt group number.
- On **Page 1**, assign a descriptive **Group Name** and an available **Group Extension**.
- Set the **ACD**, **Queue**, and **Vector** fields to **y**.

```
Telnet 10.64.10.25
add hunt-group 20 Page 1 of 61
HUNT GROUP
Group Number: 20 ACD? y
Group Name: testHunt Queue? y
Group Extension: 5599 Vector? y
Group Type: ucd-mia
IN: 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:
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```


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

A Telnet window titled 'Telnet 10.64.10.25' displays the configuration for a 'HUNT GROUP'. The command 'add hunt-group 20' has been entered. The configuration is on 'Page 2 of 3'. The following fields are visible: 'Skill?' is set to 'y', 'Expected Call Handling Time (sec):' is '180', 'AAS?' is 'n', 'Measured:' is 'none', 'Supervisor Extension:' is blank, 'Controlling Adjunct:' is 'none', 'Timed ACW Interval (sec):' is blank, 'Redirect on No Answer (rings):' is blank, 'Redirect to UDN:' is blank, and 'Forced Entry of Stroke Counts or Call Work Codes?' is 'n'. At the bottom, a legend shows: ESC-x=Cancel, Esc-e=Submit, Esc-p=Prev Pg, Esc-n=Next Pg, Esc-h=Help, Esc-r=Refresh.

```
Telnet 10.64.10.25
add hunt-group 20                                     Page 2 of 3
HUNT GROUP
Skill? y      Expected Call Handling Time (sec): 180
AAS? n
Measured: none
Supervisor Extension:
Controlling Adjunct: none
Timed ACW Interval (sec):
Redirect on No Answer (rings):
Redirect to UDN:
Forced Entry of Stroke Counts or Call Work Codes? n
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

Add entries for agents with the following values as displayed below:

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

A Telnet window titled 'Telnet 10.64.10.25' displays the configuration for an 'AGENT LOGINID'. The command 'add agent-loginID 5325' has been entered. The configuration is on 'Page 1 of 2'. The following fields are visible: 'Login ID:' is '5325', 'Name:' is 'TEST AGENT 1', 'TN:' is '1', 'COR:' is '1', 'Coverage Path:' is blank, 'Security Code:' is blank, 'AAS?' is 'n', 'AUDIX?' is 'n', 'LWC Reception:' is 'spe', 'LWC Log External Calls?' is 'n', 'AUDIX Name for Messaging:' is blank, 'LoginID for ISDN Display?' is 'n', 'Password:' is '5325', 'Password (enter again):' is '5325', 'Auto Answer:' is 'station', 'MIA Across Skills:' is 'system', 'ACW Agent Considered Idle:' is 'system', 'Aux Work Reason Code Type:' is 'system', 'Logout Reason Code Type:' is 'system', 'Maximum time agent in ACW before logout (sec):' is 'system', and 'Forced Agent Logout Time:' is '17:30'. A warning message states: 'WARNING: Agent must log in again before changes take effect'. At the bottom, a legend shows: ESC-x=Cancel, Esc-e=Submit, Esc-p=Prev Pg, Esc-n=Next Pg, Esc-h=Help, Esc-r=Refresh.

```
Telnet 10.64.10.25
add agent-loginID 5325                               Page 1 of 2
AGENT LOGINID
Login ID: 5325
Name: TEST AGENT 1
TN: 1
COR: 1
Coverage Path:
Security Code:
AAS? n
AUDIX? n
LWC Reception: spe
LWC Log External Calls? n
AUDIX Name for Messaging:
LoginID for ISDN Display? n
Password: 5325
Password (enter again): 5325
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: 17:30
WARNING: Agent must log in again before changes take effect
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

On **Page 2**, set the **Skill Number (SN)** to the hunt group number previously created. The **Skill Level (SL)** may be set according to customer requirements. Repeat this step as necessary to configure additional agent extensions.

```

C:\ Telnet 10.64.10.25
add agent-loginID 5325
AGENT LOGINID
Direct Agent Skill:
Call Handling Preference: skill-level
Local Call Preference? n

  SN      SL      SN      SL
1: 20      1      16:
2:         17:
3:         18:
4:         19:
5:         20:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

```

Add entries for vectors with the following values as displayed below:

- Enter the **change vector x** command, where **x** is a vector number in the list to be modified.
- 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.

```

C:\ Telnet 10.64.10.25
change vector 1
CALL VECTOR
Number: 1      Name: Queue to skill1
Basic? y      EAS? y      G3U4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y  LAI? n      G3U4 Adv Route? y      CINFO? n      BSR? y      Holidays? y
Variables? y  3.0 Enhanced? y
01 wait-time  2 secs hearing ringback
02 queue-to   skill 1 pri m
03
04
05
06
07
08
09
10
11
12

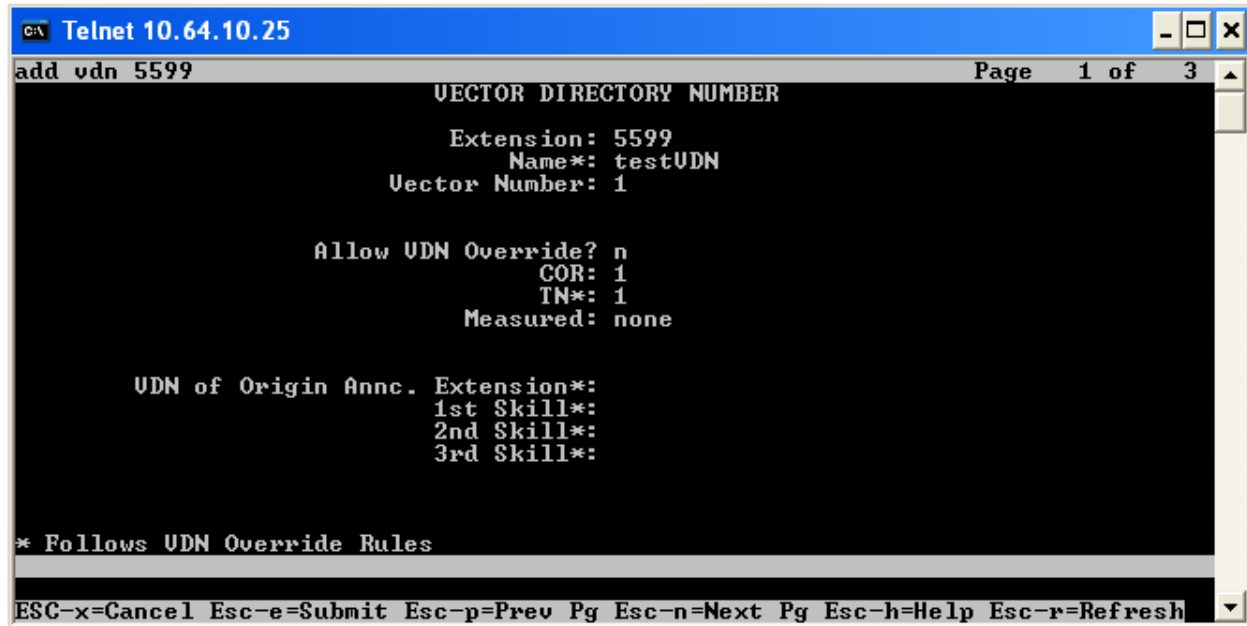
Press 'Esc f 6' for Vector Editing

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

```

Add entries for vdns with the following values as displayed below:

- Enter the **add vdn x** command, where **x** is an extension valid in the dial plan.
- Specify a descriptive **Name** for the VDN and specify the **Destination** as the Vector Number configured in the previous step.
- In the example below, incoming calls to the extension 5599 will be routed to testVDN, which in turn will invoke the actions specified in Vector 1.



```
C:\> Telnet 10.64.10.25
add vdn 5599                                     Page 1 of 3
                                VECTOR DIRECTORY NUMBER
                                Extension: 5599
                                Name*: testUDN
                                Vector Number: 1

                                Allow UDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none

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

* Follows UDN Override Rules

ESC-x=Cancel ESC-e=Submit ESC-p=Prev Pg ESC-n=Next Pg ESC-h=Help ESC-r=Refresh
```

4.3. Create Recording Stations

The recording ports in this configuration are DMCC stations that essentially appear as IP Softphones to Avaya Communication Manager.

Add entries for recording ports with the following values as displayed below:

- Enter the **add station x** command, where **x** is a station valid in the dial plan.
- On **Page 1** of the station form, set the **Type** field to an IP telephone set type, enter a descriptive **Name**, and specify the **Security Code**. The security code for all recording stations **MUST** have the same value.
- Set the value for **IP SoftPhone** to **y**. This value is required for the recording stations.
- Additional default values can be used for these recording stations.
- Repeat this procedure as necessary with the same **Security Code** to configure additional DMCC stations.

The screenshot shows a Telnet window titled "Telnet 10.64.10.25". The command "add station 5210" has been entered. The screen displays the configuration form for a station, labeled "STATION" at the top right. The form is divided into two main sections: "STATION" and "STATION OPTIONS".

STATION

Extension: 5210	Lock Messages? n	BCC: 0
Type: 9630	Security Code: 123456	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: DMCC Recording Station 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	

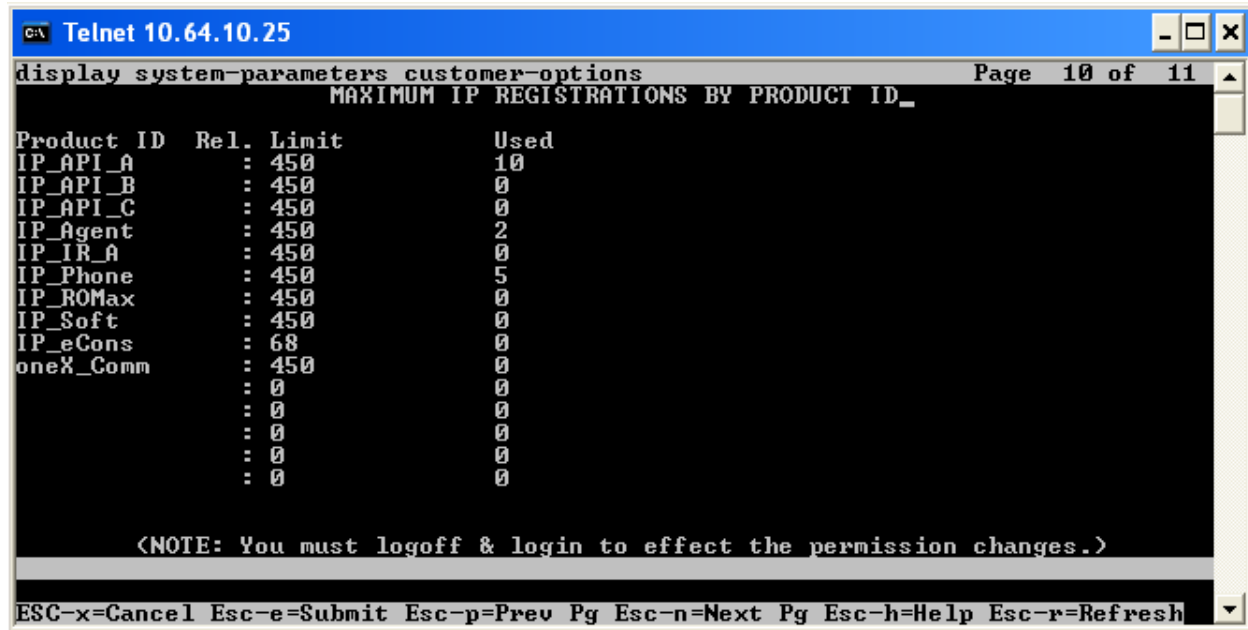
STATION OPTIONS

Loss Group: 19	Time of Day Lock Table:
Speakerphone: 2-way	Personalized Ringing Pattern: 1
Display Language: english	Message Lamp Ext: 5210
Survivable GK Node Name:	Mute Button Enabled? y
Survivable COR: internal	Button Modules: 0
Survivable Trunk Dest? y	Media Complex Ext:
	IP SoftPhone? y
	IP Video Softphone? n
	Customizable Labels? y

At the bottom of the screen, there is a legend for navigation keys: ESC-x=Cancel, Esc-e=Submit, Esc-p=Prev Pg, Esc-n=Next Pg, Esc-h=Help, Esc-r=Refresh.

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. For the compliance test, recording stations from 5210 to 5219 were created.



```
C:\> Telnet 10.64.10.25
display system-parameters customer-options                                     Page 10 of 11
MAXIMUM IP REGISTRATIONS BY PRODUCT ID_

Product ID  Rel. Limit      Used
IP_API_A   : 450         10
IP_API_B   : 450          0
IP_API_C   : 450          0
IP_Agent   : 450          2
IP_IR_A    : 450          0
IP_Phone   : 450          5
IP_ROMax   : 450          0
IP_Soft    : 450          0
IP_eCons   : 68          0
oneX_Comm  : 450          0
           : 0           0
           : 0           0
           : 0           0
           : 0           0
           : 0           0

<NOTE: You must logoff & login to effect the permission changes.>

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

4.4. Create Recorded (Monitored) Stations

During the compliance test, stations were utilized as monitored and recorded stations.

- Enter the **add station x** command, where x is a station valid in the dial plan.
- On **Page 1** of the station form, set the **Type** field to an IP telephone set type, enter a descriptive **Name**, and specify the **Security Code**. For the compliance test, recorded stations from 5200 to 5209 were created.

The screenshot shows a Telnet window titled "Telnet 10.64.10.25". The command "add station 5200" has been entered, and the system displays the configuration for station 5200. The configuration is presented in a multi-page format, with "Page 1 of 5" indicated at the top right. The configuration details are as follows:

STATION		
Extension: 5200	Lock Messages? n	BCC: 0
Type: 9630	Security Code: 123456	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Station 5200	Coverage Path 2:	COS: 1
	Hunt-to Station:	

STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
Speakerphone: 2-way	Personalized Ringing Pattern: 1
Display Language: english	Message Lamp Ext: 5200
Survivable GK Node Name:	Mute Button Enabled? y
Survivable COR: internal	Button Modules: 0
Survivable Trunk Dest? y	Media Complex Ext:
	IP SoftPhone? y
	IP Video Softphone? n
	Customizable Labels? y

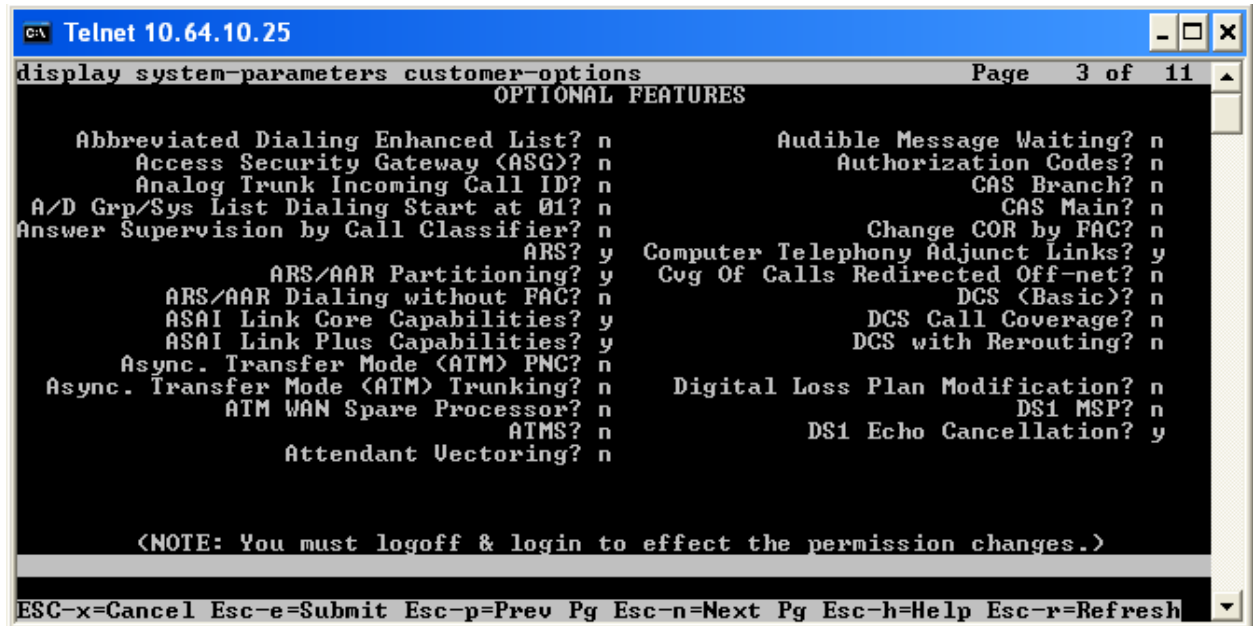
At the bottom of the window, a legend for escape codes is provided: ESC-x=Cancel, Esc-e=Submit, Esc-p=Prev Pg, Esc-n=Next Pg, Esc-h=Help, and Esc-r=Refresh.

4.5. Administer Computer Telephony Integration (CTI) Link

It is assumed that Avaya Communication Manager is enabled with feature licenses for Vectoring, ASAI Link Core Capabilities, and Computer Telephony Adjunct Links. This section provides the steps required for configuring a CTI Link.

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

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



```
Telnet 10.64.10.25
display system-parameters customer-options Page 3 of 11
OPTIONAL FEATURES
Abbreviated Dialing Enhanced List? n Audible Message Waiting? n
Access Security Gateway (ASG)? n Authorization Codes? n
Analog Trunk Incoming Call ID? n CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? n CAS Main? n
Answer Supervision by Call Classifier? n 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? n DCS (Basic)? n
ASAI Link Core Capabilities? y DCS Call Coverage? n
ASAI Link Plus Capabilities? y DCS with Rerouting? n
Async. Transfer Mode (ATM) PNC? n Digital Loss Plan Modification? n
Async. Transfer Mode (ATM) Trunking? n DS1 MSP? n
ATM WAN Spare Processor? n DS1 Echo Cancellation? y
ATMS? n
Attendant Vectoring? n

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

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

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

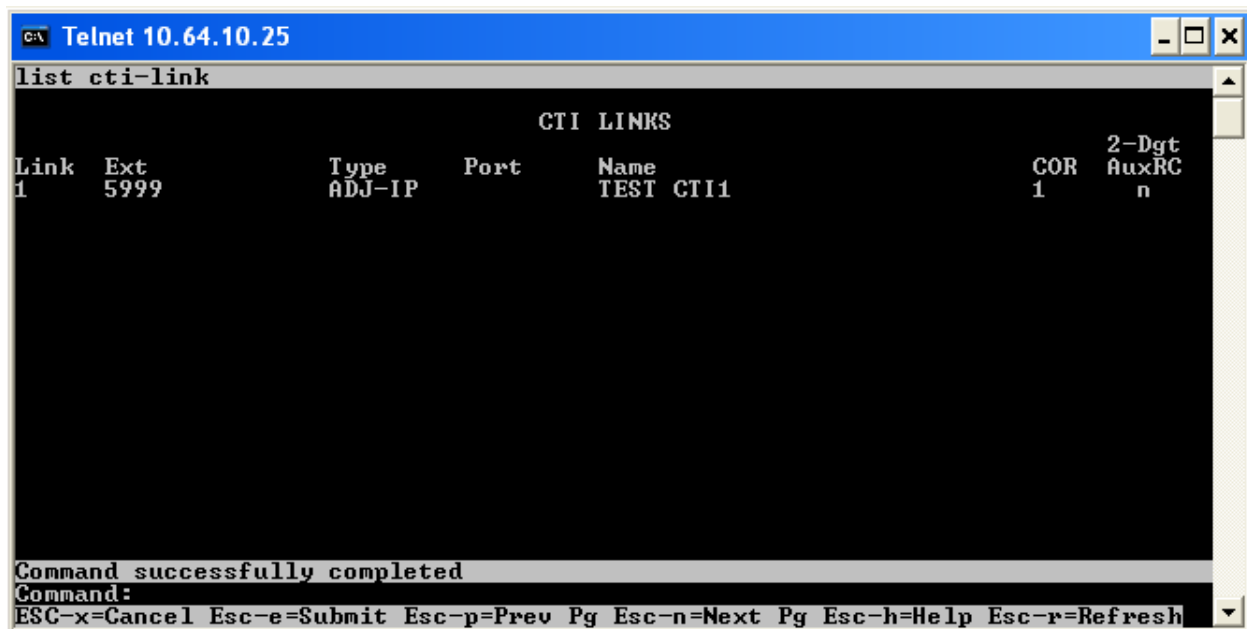
- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.



```
C:\ Telnet 10.64.10.25
add cti-link 1                                     Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 5999
Type: ADJ-IP
Name: TEST CTI1_                                COR: 1

ESC-x=Cancel ESC-e=Submit ESC-p=Prev Pg ESC-n=Next Pg ESC-h=Help ESC-r=Refresh
```

Enter the **list cti-link** command to verify that the CTI Link is correctly configured.



```
C:\ Telnet 10.64.10.25
list cti-link
CTI LINKS
Link  Ext      Type      Port      Name      COR      2-Dgt
1      5999      ADJ-IP      Port      TEST CTI1      1      AuxRC
n

Command successfully completed
Command:
ESC-x=Cancel ESC-e=Submit ESC-p=Prev Pg ESC-n=Next Pg ESC-h=Help ESC-r=Refresh
```


Check the service state of the link by entering the **status aesvcs cti-link** command. The service state should show **no** for maintenance busy and the Service State should indicate **established**.

```
C:\ Telnet 10.64.10.25
status aesvcs cti-link

      AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services   Service   Msgs   Msgs
Link  Number    Busy Server      State      Sent   Rcvd
-----
1      4        no  aesserver2    established  15     15

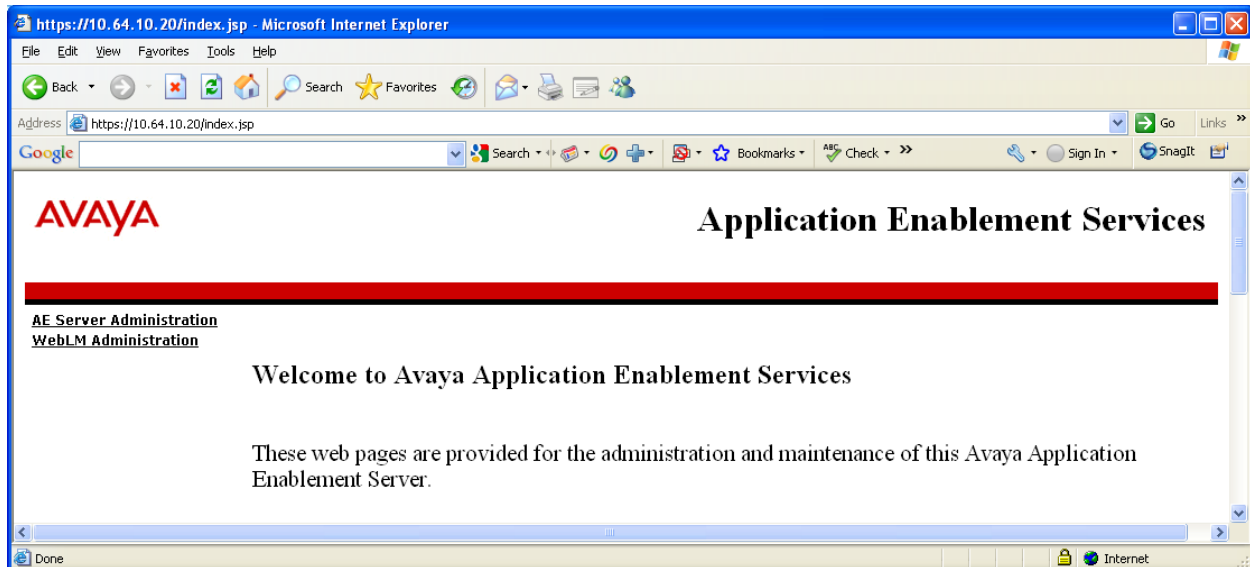
Command successfully completed
Command:
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

5. Configure Avaya Application Enablement Services

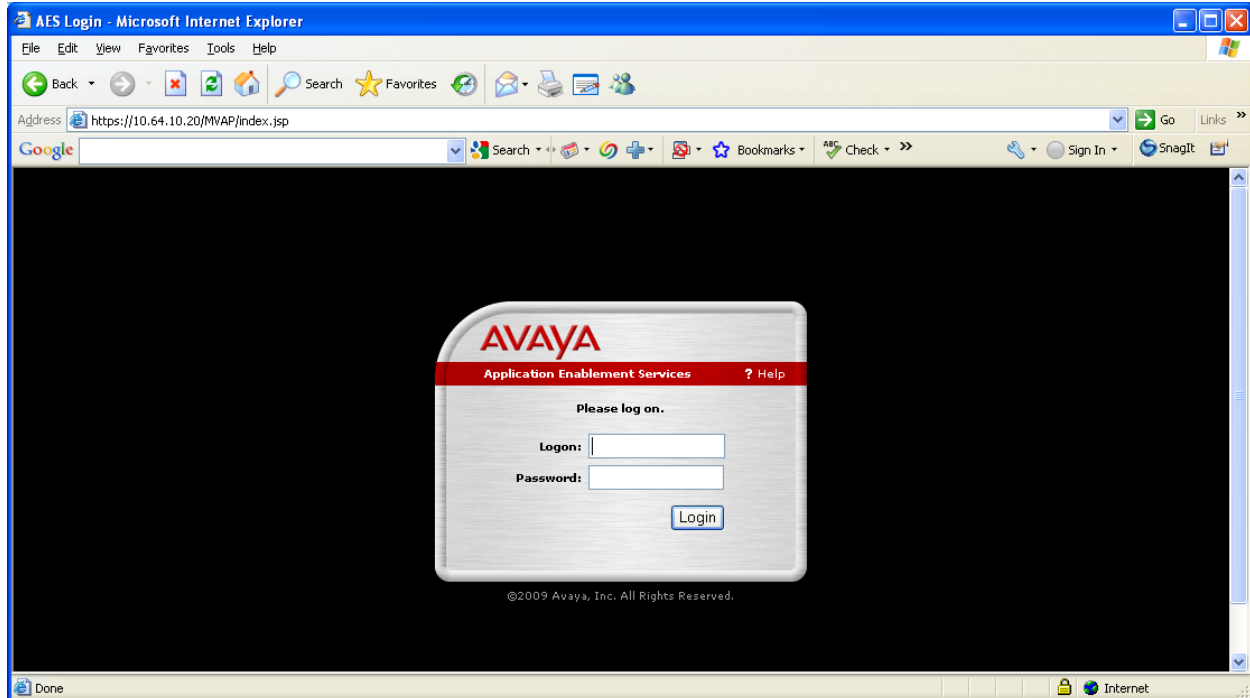
The Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to monitor and control telephony resources on Avaya Communication Manager. The Application Enablement Services server receives requests from CTI applications and forwards them to Avaya Communication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

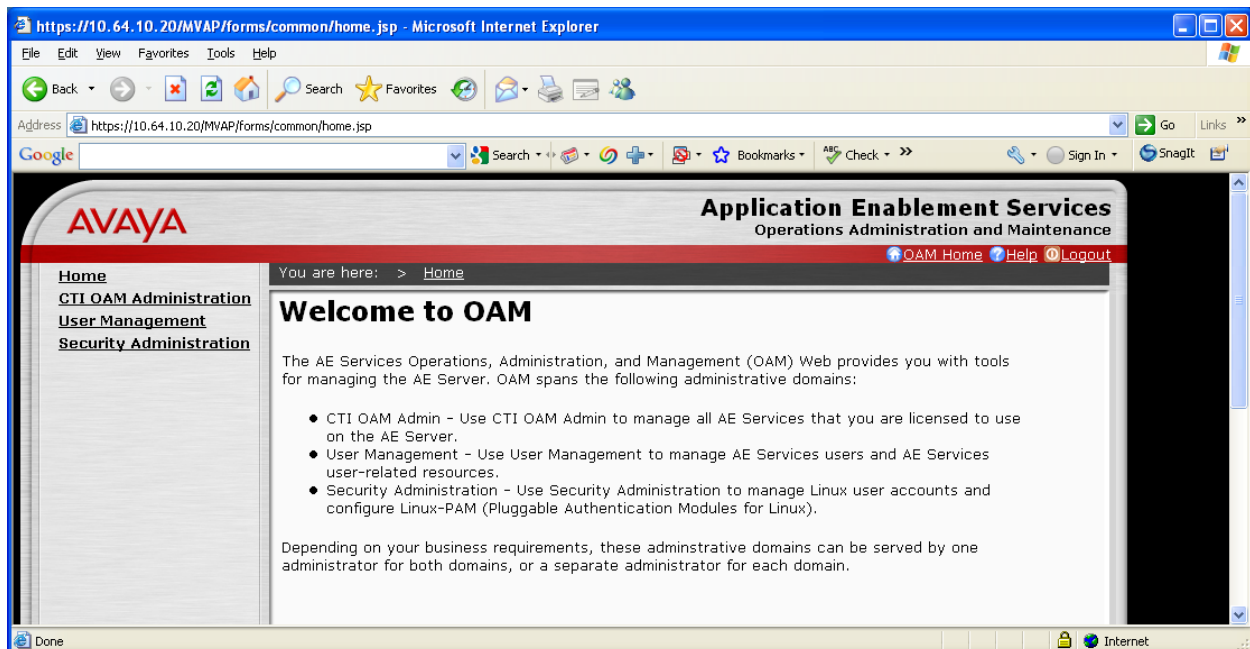
Access the AES OAM web-based interface by using the URL **https://ip-address** in an Internet browser window, where **ip-address** is the IP address of the AES server. Click on the **AE Server Administration** link.



The **Login** screen is displayed as shown below. Log in with the appropriate credentials.



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



The **Welcome to CTI OAM Screens** screen is displayed. Verify that AES is licensed for the TSAPI and DMCC Services, as shown in the screen below. If the TSAPI and DMCC Services are not licensed, contact the Avaya sales team or business partner for a proper license file.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > [CTI OAM Home](#)

Welcome to CTI OAM Screens

[craft] Last login: Mon Nov 2 20:01:05 2009 from 10.64.10.15

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

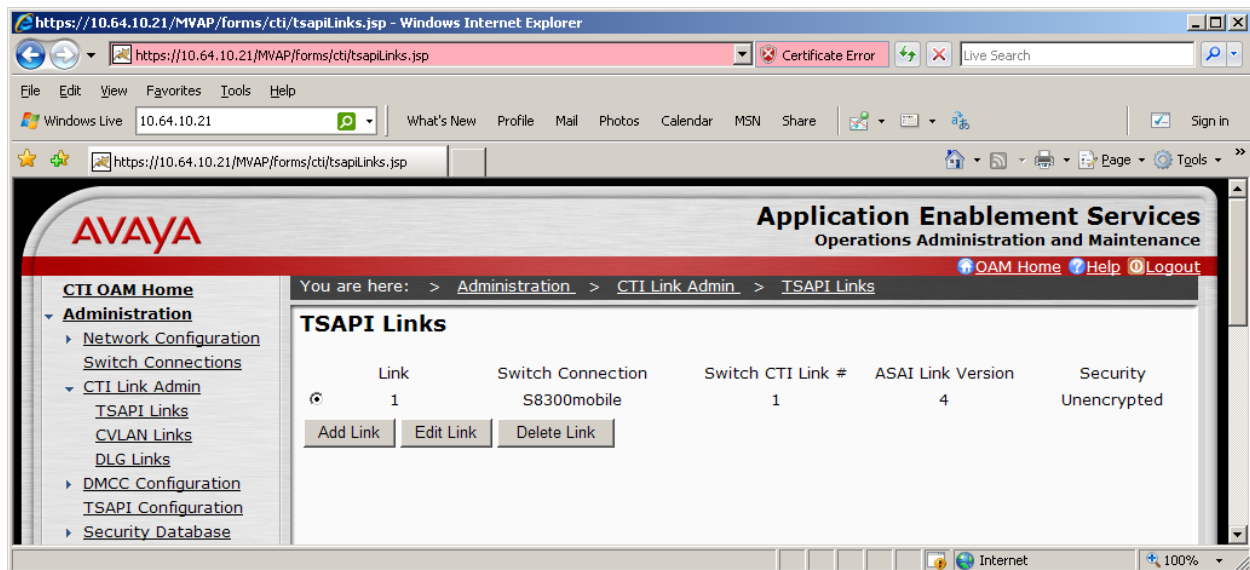
Service	Status	State	Licenses Purchased
ASAI Link Manager	Running	N/A	N/A
DMCC Service	Running	ONLINE	Yes
CVLAN Service	Running	ONLINE	Yes
DLG Service	Running	ONLINE	Yes
Transport Layer Service	Running	N/A	N/A
TSAPI Service	Running	ONLINE	Yes
SMS	N/A	N/A	Yes

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

License Information

You are licensed to run Application Enablement (CTI) version 4.2.

Navigate to **Administration -> CTI Link Admin -> TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**.



Select a Switch Connection using the drop down menu. The Switch Connection is configured in **Section 4.1**. Select the Switch CTI Link Number using the drop down menu. The CTI link number should match the number configured in the cti-link form in **Section 4.5**. Click **Apply Changes**. Default values may be used in the remaining fields.

https://10.64.10.21/MVAP/action/cti/tsapiLinks.do - Windows Internet Explorer

https://10.64.10.21/MVAP/action/cti/tsapiLinks.do Certificate Error Live Search

File Edit View Favorites Tools Help

Windows Live 10.64.10.21 What's New Profile Mail Photos Calendar MSN Share Sign in

https://10.64.10.21/MVAP/action/cti/tsapiLinks.do Page Tools

AVAYA **Application Enablement Services**
Operations Administration and Maintenance

[OAM Home](#) [Help](#) [Logout](#)

You are here: > [Administration](#) > [CTI Link Admin](#) > [TSAPI Links](#)

CTI OAM Home

- Administration
 - Network Configuration
 - Switch Connections
 - CTI Link Admin
 - TSAPI Links**
 - CVLAN Links
 - DLG Links
 - DMCC Configuration
 - TSAPI Configuration
 - Security Database
 - Certificate Management

Add / Edit TSAPI Links

Link: 2

Switch Connection: S8300mobile

Switch CTI Link Number: 1

ASAI Link Version: 4

Security: Unencrypted

Internet 100%

Next, add a CTI User, as FocusRecord requires a CTI user to access AES. Select **OAM Home -> User Management -> Add User** from the left pane.

In the **Add User** screen, enter the following values:

- In the **User Id** field, type a meaningful user id.
- In the **Common Name** field, type a descriptive name.
- In the **Surname** field, type a descriptive surname.
- In the **User Password** field, type a password for the user.
- In the **Confirm Password** field, re-enter the same password for the user.
- In the **Avaya Role** field, retain the default of **None**.
- In the **CT User** field, select **Yes** from the dropdown menu.
- Click **Apply** at the bottom of the screen (not shown here).

AVAYA Application Enablement Service
Operations Administration and Maintenance

You are here: > [User Management](#) > [Add User](#)

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Home Phone

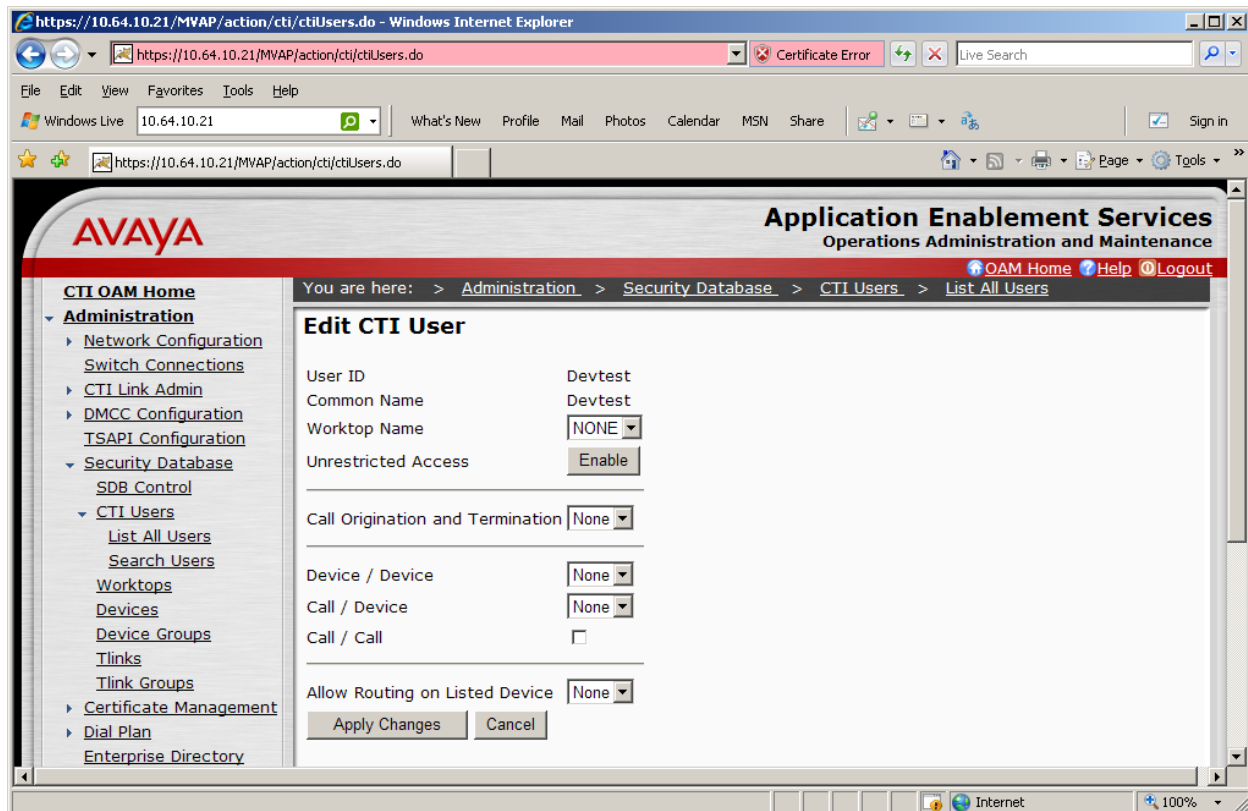
Home Postal Address

Initials

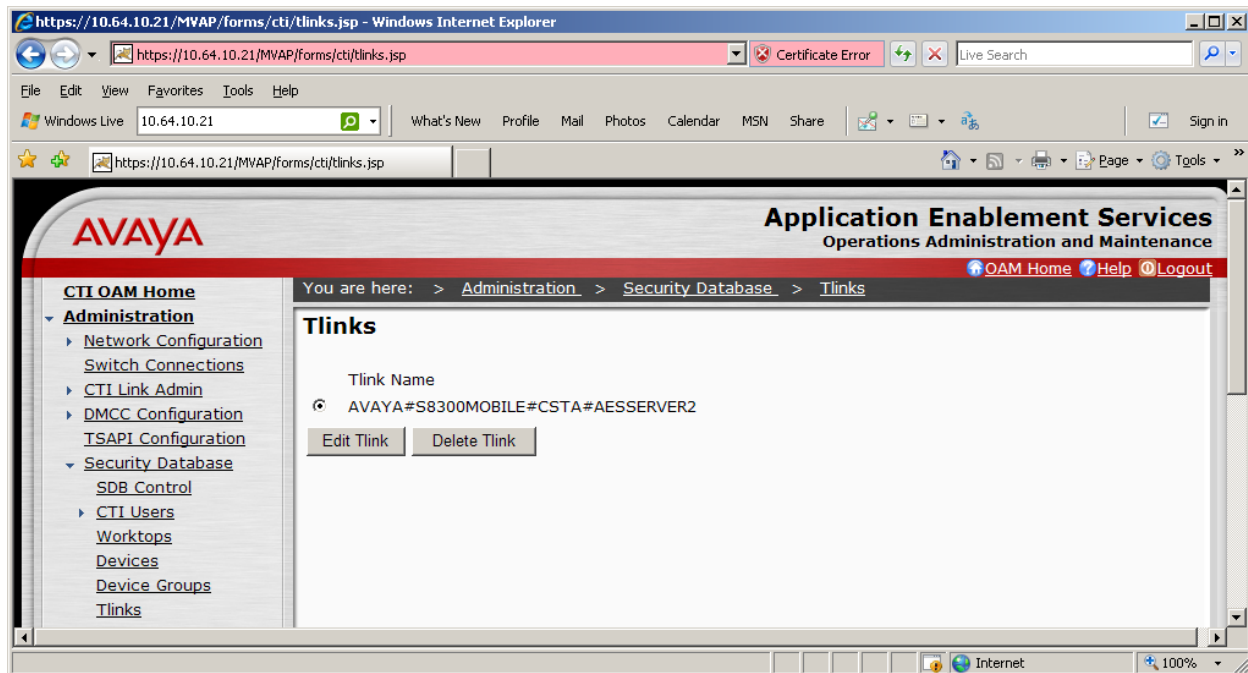
Labeled URI

Next, change the security level for the CTI User as it needs to have unrestricted access privileges. Select **Administration -> Security Database -> CTI Users -> List All Users** from the left pane. Choose the CTI user, and click **Edit**.

Provide the user with unrestricted access privileges by clicking the **Unrestricted Access** button so that it shows **Enable**. Click **Apply Changes**.



Select **Administration -> Security Database -> CTI Users -> Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated by the Application Enablement Services server upon creation of a new switch connection. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring the FocusRecord.



Navigate to the **Administration -> Network Configuration -> Ports** page to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to **Enabled**. Click **Apply Changes** (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > [Administration](#) > [Network Configuration](#) > [Ports](#)

Ports

CVLAN Ports		Enabled	Disabled
Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	9998	<input type="radio"/>	<input checked="" type="radio"/>

DLG Port

TCP Port	Value
TCP Port	5678

TSAPI Ports

Enabled		Disabled	
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
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

Enabled		Disabled	
Unencrypted Port	4721	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	4722	<input type="radio"/>	<input checked="" type="radio"/>
TR/87 Port	4723	<input type="radio"/>	<input checked="" type="radio"/>

6. Configure FocusRecord

Cacti installs, configures, and customizes the FocusRecord application for their end customers. This section only describes the interface configuration for the FocusRecord application to communicate with AES and Avaya Communication Manager.

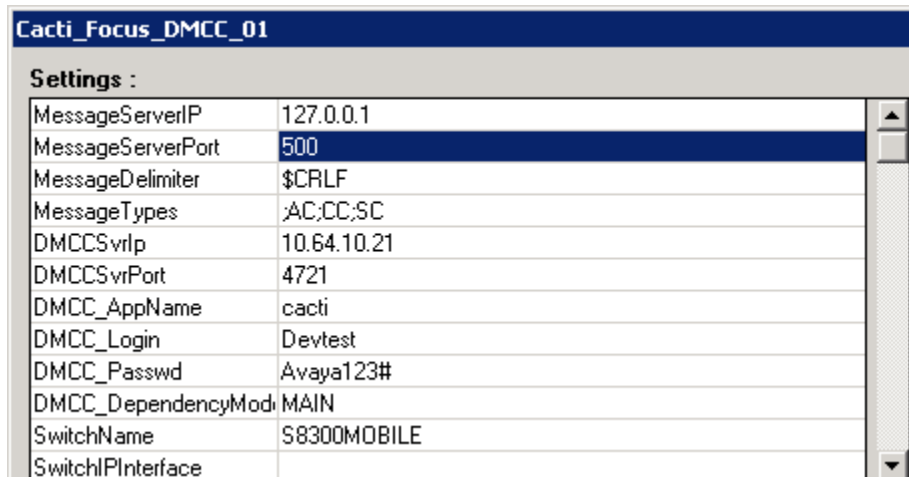
Refer to [3] for configuring the Cacti FocusRecord application.

Navigate to **Start -> Programs -> CAppMan** to access the Cacti_Application_Manager page. In the Cacti_Application_Manager page, select **Cacti_Focus_DMCC_01** and click the **Settings** button.

The following screen shows the Cacti_Focus_DMCC_01 Settings page. Provide the following information:

- **DMCCSvrIp** – Enter the IP address of AES.
- **DMCCSvrPort** – Enter the DMCC port utilized. During the compliance test, the unencrypted, default DMCC port was utilized.
- **DMCC_AppName** – Enter the application name.
- **DMCC_Login** – Enter the user name created in **Section 5**.
- **DMCC_Passwd** – Enter the password created in **Section 5**.
- **SwitchName** – Enter the switch connection name created in **Section 5**.

Click on **Save** to save the changes at the bottom of the screen (not shown here).



Cacti_Focus_DMCC_01	
Settings :	
MessageServerIP	127.0.0.1
MessageServerPort	500
MessageDelimiter	\$CRLF
MessageTypes	:AC;CC;SC
DMCCSvrIp	10.64.10.21
DMCCSvrPort	4721
DMCC_AppName	cacti
DMCC_Login	Devtest
DMCC_Passwd	Avaya123#
DMCC_DependencyMod	MAIN
SwitchName	S8300MOBILE
SwitchIPInterface	

The following screen shows the second part of DMCC Configuration.

- **IpPhoneDevicePasswd** – Enter the recording (DMCC stations) extension password, created in **Section 4.3**. This should be identical for all recording stations.
- **RtpIpAddress** – Enter the IP address of the recording device server, in this case, FocusRecord on the Windows 2003 server.
- **RtpStartPort** – Choose an appropriate starting port, in this case, 6000.
- **CodecType** – Enter the audio codec type. This must match the value in the IP Codec Set form used in the IP Network Region form.
- **MaxFilterDevices** – Set this value to cover the number of devices.
- **PhoneExtensionFilter** – Set this range for monitored stations previously created.

Click on **Save** to save the changes at the bottom of the screen (not shown here).

The screenshot shows a web-based configuration interface titled "Cacti_Focus_DMCC_01". Below the title is a section labeled "Settings :". It contains a table with various configuration parameters and their values. A vertical scrollbar is visible on the right side of the table.

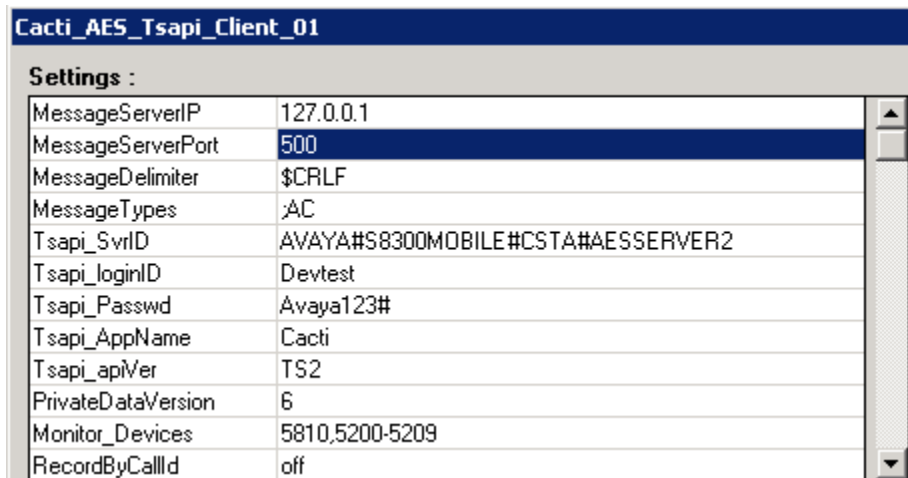
IpPhoneDevicePassword	123456
RtpPortMode	OnDemand
RtpIpAddress	10.64.10.15
RtpStartPort	6000
CodecType	g711U
MaxFilterDevices	100
PhoneExtensionFilter	5200-5209
MaxDevicesOnCallId	2
RecorderId	01
ChannelExtended	
DSN_Connection	
AutoRestartTime	00:30

To configure for the TSAPI service, navigate to **Start -> Programs -> CAppMan** to access the Cacti_Application_Manager page. In the Cacti_Application_Manager page, select **Cacti_AES_Tsapi_Client_01** and click the **Settings** button.

The following screen shows the Cacti_AES_Tsapi_Client_01 Settings page. Provide the following information:

- **Tsapi_SvrID** – Enter the Tlink name used. The Tlink name can be obtained by accessing AES through the web, and navigate to **Administration -> Security Database -> Tlinks** as described in **Section 5**.
- **Tsapi_loginID** – Enter the user name created in **Section 5**.
- **Tsapi_Passwd** – Enter the password created in **Section 5**.
- **Tsapi_AppName** – Enter the switch, application, or company name. This is used for logging purposes, and does not have a pairing in AES.
- **Monitor_Devices** – Enter the monitored (recorded) extension range created in **Section 4.4**.

Click on **Save** to save the changes at the bottom of the screen (not shown here).



Settings :	
MessageServerIP	127.0.0.1
MessageServerPort	500
MessageDelimiter	\$CRLF
MessageTypes	:AC
Tsapi_SvrID	AVAYA#S8300MOBILE#CSTA#AESERVER2
Tsapi_loginID	Devtest
Tsapi_Passwd	Avaya123#
Tsapi_AppName	Cacti
Tsapi_apiVer	TS2
PrivateDataVersion	6
Monitor_Devices	5810,5200-5209
RecordByCallId	off

7. General Test Approach and Test Results

All feature functionality test cases were performed manually to verify proper operation. The following scenarios were tested using the test configuration diagram shown in **Figure 1**.

The installation test cases were covered with the setup of Avaya Communication Manager, Application Enablement Services, and FocusRecord. The clean removal of the application was also covered in this section.

The functionality test cases were performed manually. Various calls were placed including incoming PSTN calls to the hunt groups, and incoming and outgoing personal calls from the agents. Recordings were verified, per the test cases.

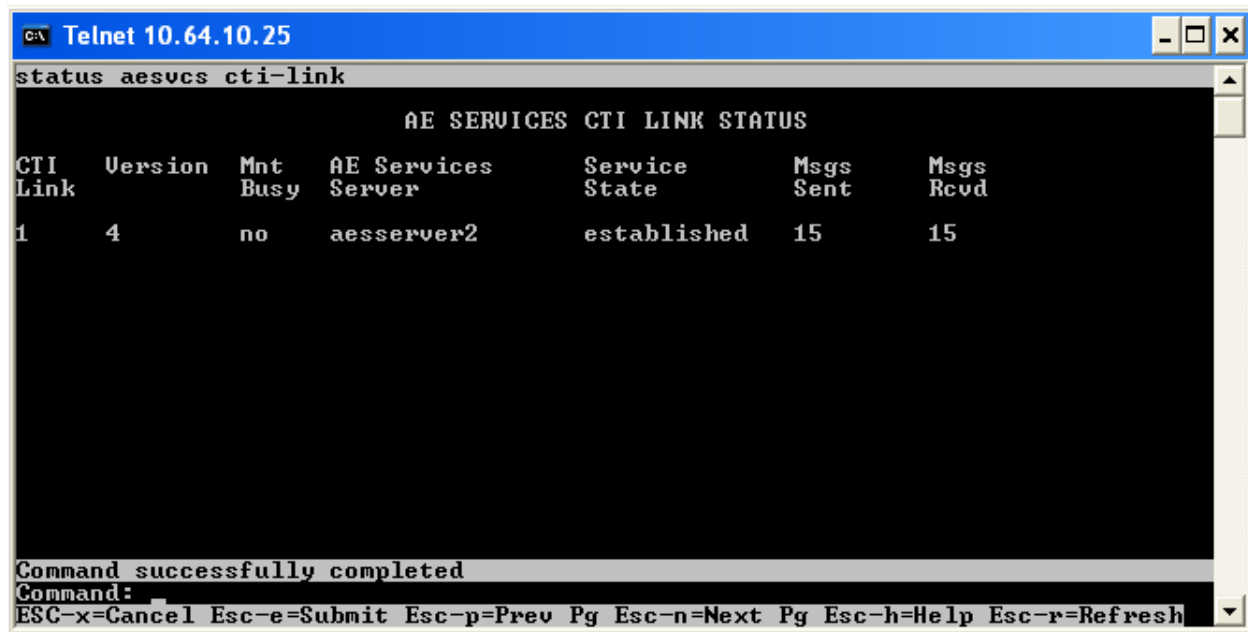
The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to the FocusRecord server and Avaya Communication Manager, stopping the CTI service, and pulling power from Avaya Communication Manager.

All test cases passed. No errors were detected.

8. Verification Steps

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

For Avaya Communication Manager, check the CTI Link status with the **status aevcs cti-link** command. The service state should show **no** for maintenance busy and the Service State should indicate **established**.



```
C:\ Telnet 10.64.10.25
status aevcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI Link  Version  Mnt  AE Services  Service  Msgs  Msgs
Link      Number   Busy Server      State    Sent   Rcvd
-----
1         4       no  aesserver2   established  15    15

Command successfully completed
Command:
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

For AES, the TSAPI and DMCC Services should show as **Running, ONLINE, and Yes**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > CTI OAM Home

Welcome to CTI OAM Screens

[craft] Last login: Mon Nov 2 20:01:05 2009 from 10.64.10.15

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 4.2.

For FocusRecord, after a few calls are made, the client page will show recordings that can be listened to and verified.

The screenshot displays the ObserveCTI WS web interface. The top navigation bar includes links for Start Page, Reports, Send Message, Training Video Recorder, Designer, and Logout. A welcome message for the Administrator is visible. The main content area shows search results for recordings, with a table listing details such as Date/Time, Channel, Duration, AgentID, AgentName, AgentGroup, Type, Comment, VDN/DNIS, and Custom fields. The left sidebar contains navigation options like Sites, Search, Recordings, Personnel, Dashboards, and Rules. The Recordings section is expanded, showing filters for From, To, Min Dur, Max Dur, Channel, AgentID, AgentGroup, CallType, Comments, VDN/DNIS, Custom-J, Custom-K, Custom-L, Nth_Call, and Location. A Saved Queries section is also present, listing Queries, Recordings, Agents5thPast7, and Evaluations.

Date/Time	Channel	Duration	AgentID	AgentName	AgentGroup	Type	Comment	VDN/DNIS	S	V	Custom-J	Custom-K	Custom-L
02/22/2010 10:18:11	R01C001	00:01:22	5205	Ext 5205	extensions	in	Unreviewed				a...	5203	
02/22/2010 10:18:11	R01C002	00:01:22	5203	Ext 5203	extensions	out	Unreviewed				a..5205		
02/22/2010 10:34:51	R01C003	00:01:22	5203	Ext 5203	extensions	in	Unreviewed				a...	5205	
02/22/2010 10:34:51	R01C004	00:01:22	5205	Ext 5205	extensions	out	Unreviewed				a..5203		
02/22/2010 10:38:15	R01C005	00:00:28	5913	Agent 5913	agents	in	Unreviewed	5913			a...	5205	
02/22/2010 10:38:15	R01C006	00:00:28	5205	Ext 5205	extensions	out	Unreviewed				a..5913		
02/22/2010 10:48:00	R01C007	00:01:00	5913	Agent 5913	agents	in	Unreviewed	5913			a...	5205	
02/22/2010 10:48:00	R01C008	00:00:59	5205	Ext 5205	extensions	out	Unreviewed				a..5913		

9. Conclusion

FocusRecord was compliance tested with Avaya Communication Manager and Avaya Application Enablement Services. FocusRecord successfully recorded calls for agents and hunt groups. All test cases completed successfully.

10. Additional References

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

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

[1] *Administrator Guide for Avaya Communication Manager*, Doc ID: 03-300509, February 10, 2007

[2] *Application Enablement Services Administration and Maintenance Guide*, Doc ID: 02-300357, May 5, 2008

[3] *Cacti FocusRecord Workstation Users Guide v2.45*

©2010 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.