Avaya Solution & Interoperability Test Lab

Application Notes for Cacti FocusRecord with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cacti's FocusRecord to interoperate with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} 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 Aura^{TM} Communication Manager is accomplished through Avaya Aura^{TM} Application Enablement Services. These Application Notes describe the compliance test configuration used to test Cacti's FocusRecord Version 2.45, with 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 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 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 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.

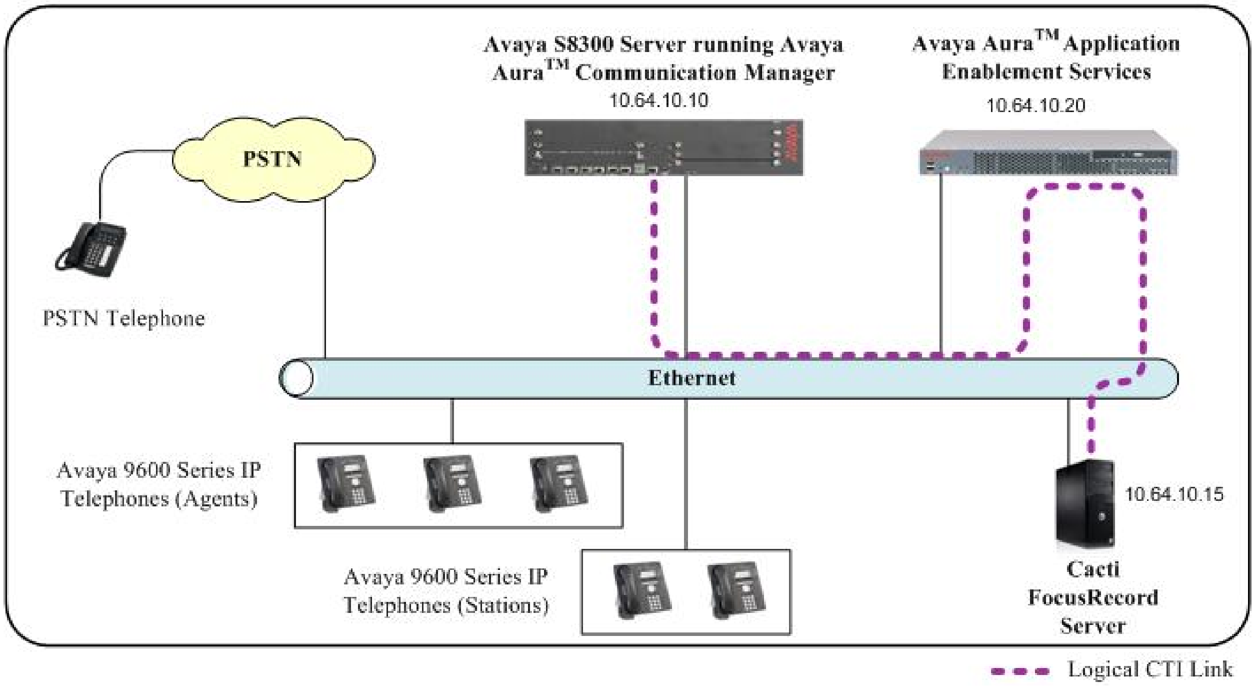

Avaya S8300 Server running Avaya Aura™ Communication Manager
10.64.10.10
Avaya Aura™ Application Enablement Services
10.64.10.20
PSTN
PSTN Telephone
Ethernet
Avaya 9600 Series IP Telephones (Agents)
Avaya 9600 Series IP Telephones (Stations)
10.64.10.15
Cacti FocusRecord Server
Logical CTI Link

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 Aura^{TM} Communication Manager 5.2.1 (R015x.02.1.016.4) with Service Pack 17774
Avaya Aura™ Application Enablement Services	Release 5.2
Avaya 9600 Series IP Telephones	9620, 9630, 9640 Terminals R2.0 (H.323)
Avaya IP Agent, Avaya one-X^{TM} Agent	R7.0, R1
Cacti FocusRecord running on Windows 2003 Standard Edition Server	Version 2.45

4. Configure Avaya Aura™ Communication Manager

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

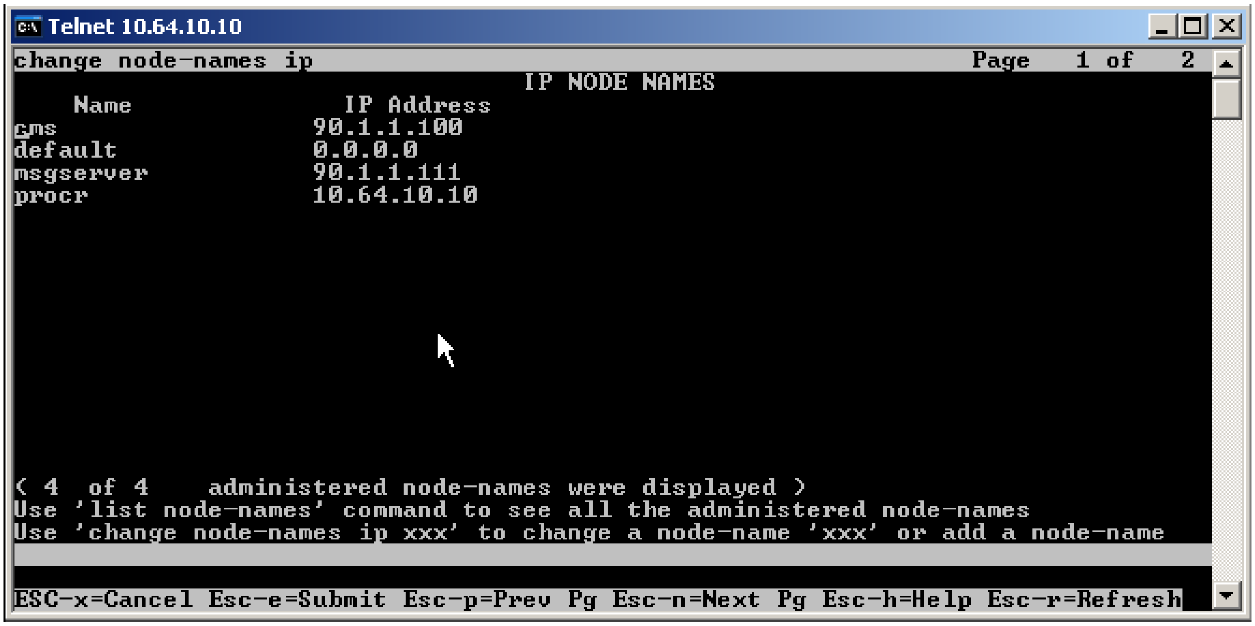
This section provides the procedures for configuring Communication Manager. The procedures fall into the following areas:

- 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.

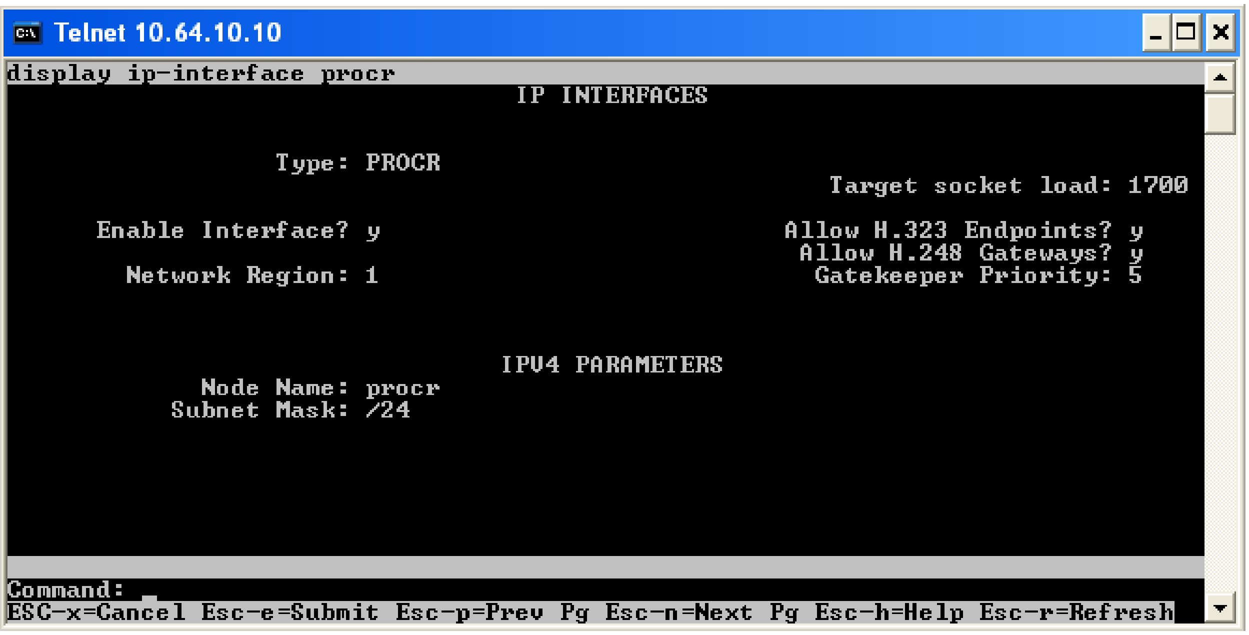
- Enter the **change node-names ip** command. In this case, **procr** and **10.64.10.10** are already populated as Name and IP Address for the Processor Ethernet Interface that is used for connectivity to the AES server. The actual IP address may vary. Submit changes.



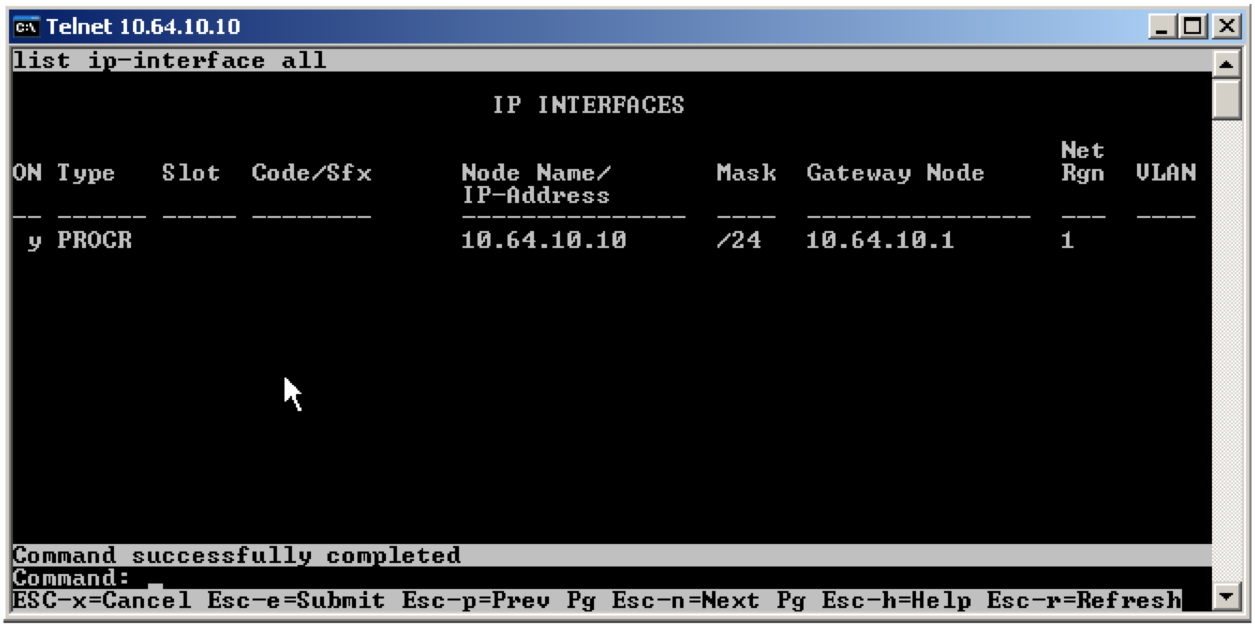
```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
cms                    90.1.1.100
default                0.0.0.0
msgserver              90.1.1.111
procr                  10.64.10.10











( 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.



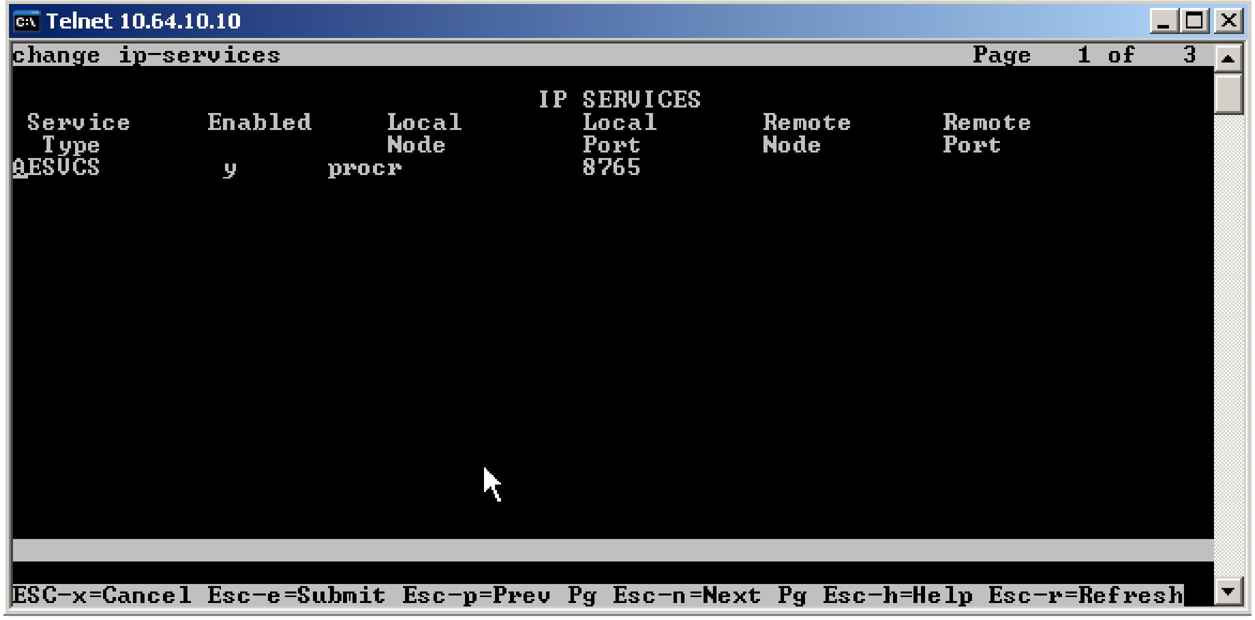
```
display ip-interface procr
                                  IP INTERFACES


                  Type: PROCR
                                                      Target socket load: 1700

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



                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /24






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



```
list ip-interface all

                                   IP INTERFACES

                                                                        Net
ON Type    Slot  Code/Sfx       Node Name/         Mask  Gateway Node    Rgn  VLAN
                                IP-Address
-- ------ ----- ---------       ---------------    ----  --------------- ---  ----
 y PROCR                        10.64.10.10        /24   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:

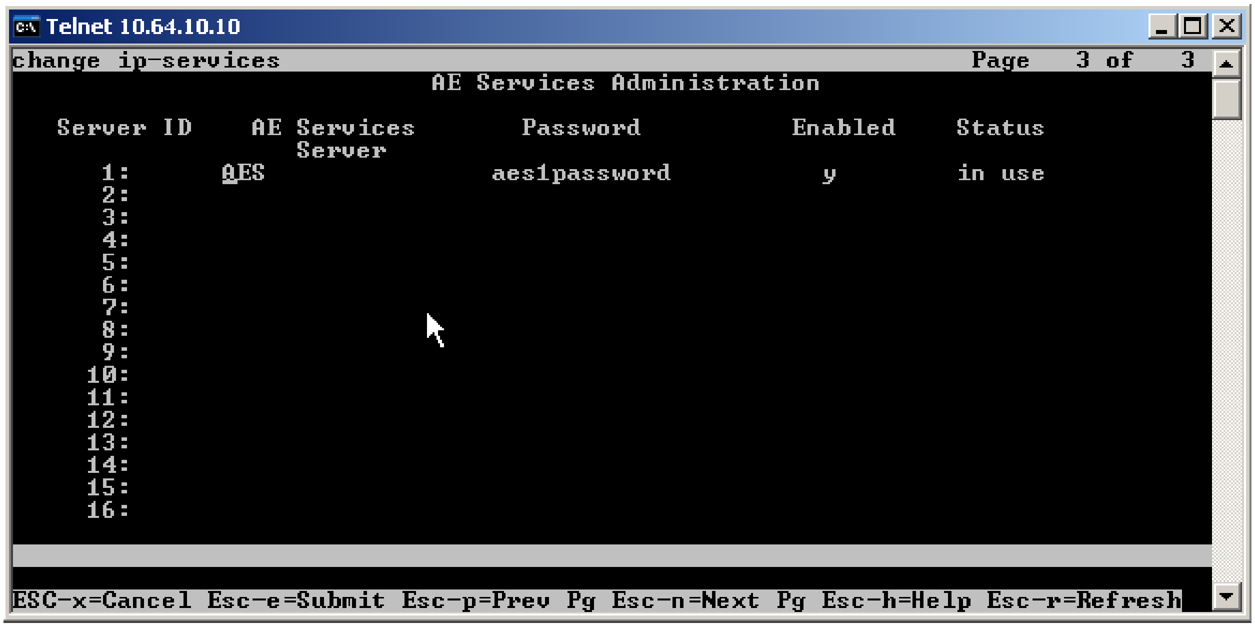
- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, retain the default of 8765.



```
change ip-services                                          Page   1 of   3

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









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 **AES**.
- 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**.



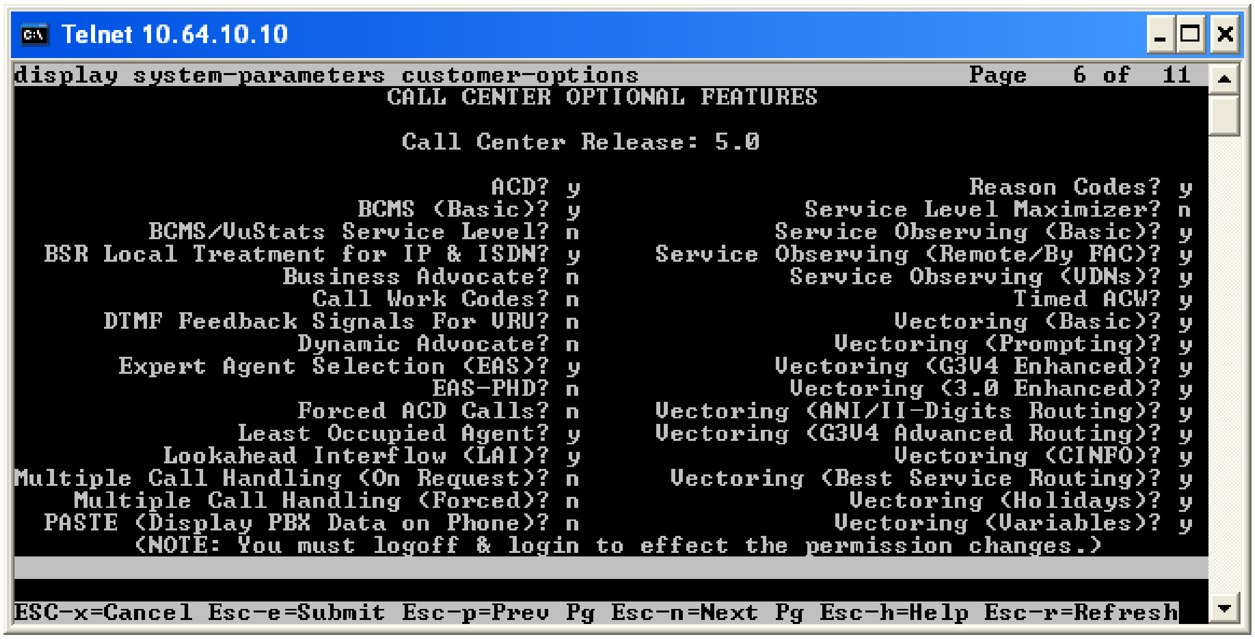
```
change ip-services                                          Page   3 of   3
                              AE Services Administration

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

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

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:

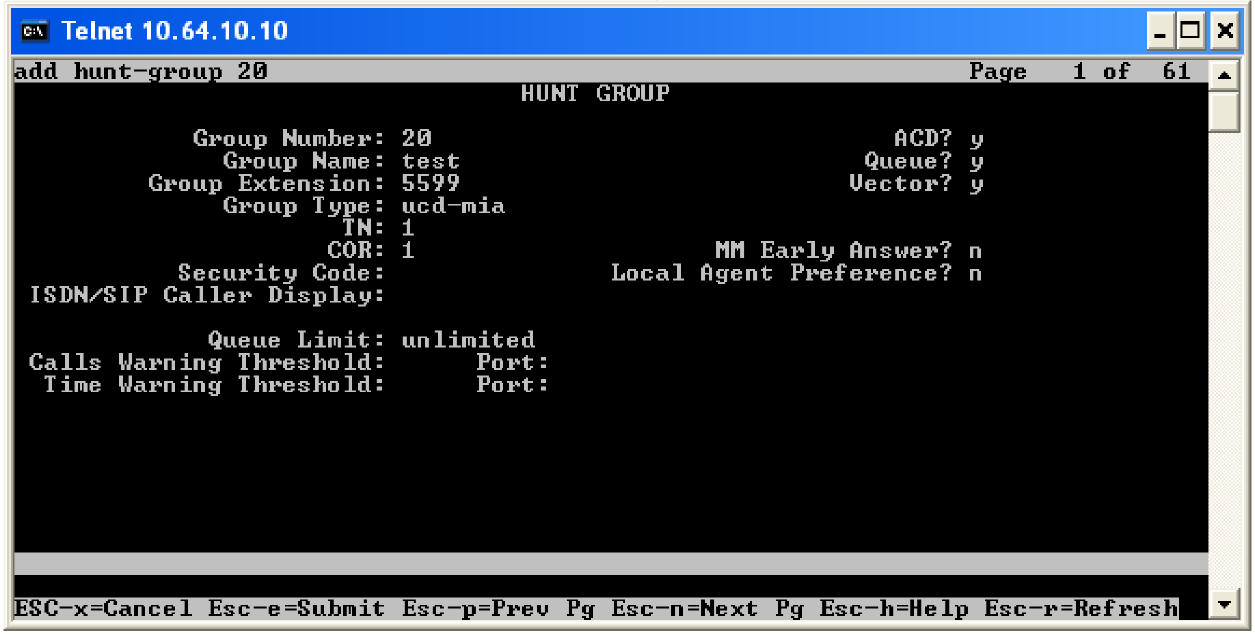
- Enter the **display system-parameters customer-options** command.
- Verify that the **ACD** and **Vectoring (Basic)** fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.



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

                          Call Center Release: 5.0

                                ACD? y                           Reason Codes? y
                       BCMS (Basic)? y                Service Level Maximizer? n
         BCMS/VuStats 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 (VDNs)? y
                    Call Work Codes? n                              Timed ACW? y
      DTMF Feedback Signals For VRU? n                      Vectoring (Basic)? y
                   Dynamic Advocate? n                  Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y              Vectoring (G3V4 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 (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                      Vectoring (CINFO)? y
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
```

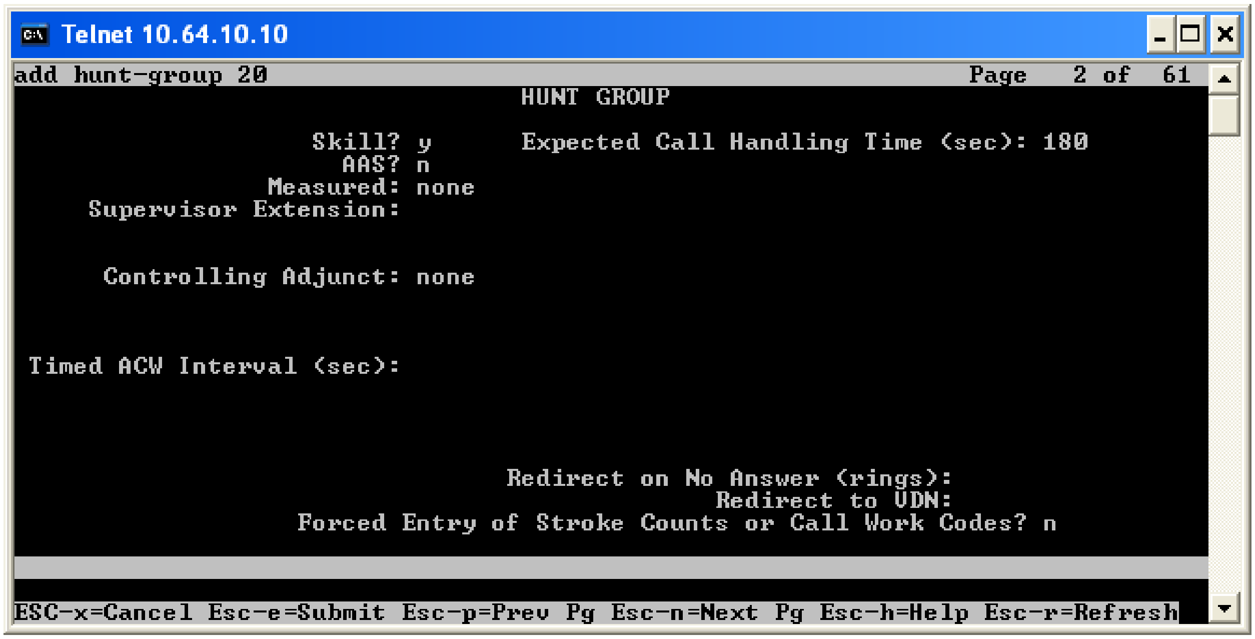
Add an entry for a hunt group with the following values as displayed below:

- 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**.



```
add hunt-group 20                                               Page   1 of  61
                                  HUNT GROUP

            Group Number: 20                               ACD? y
              Group Name: test                           Queue? y
         Group Extension: 5599                          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:







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

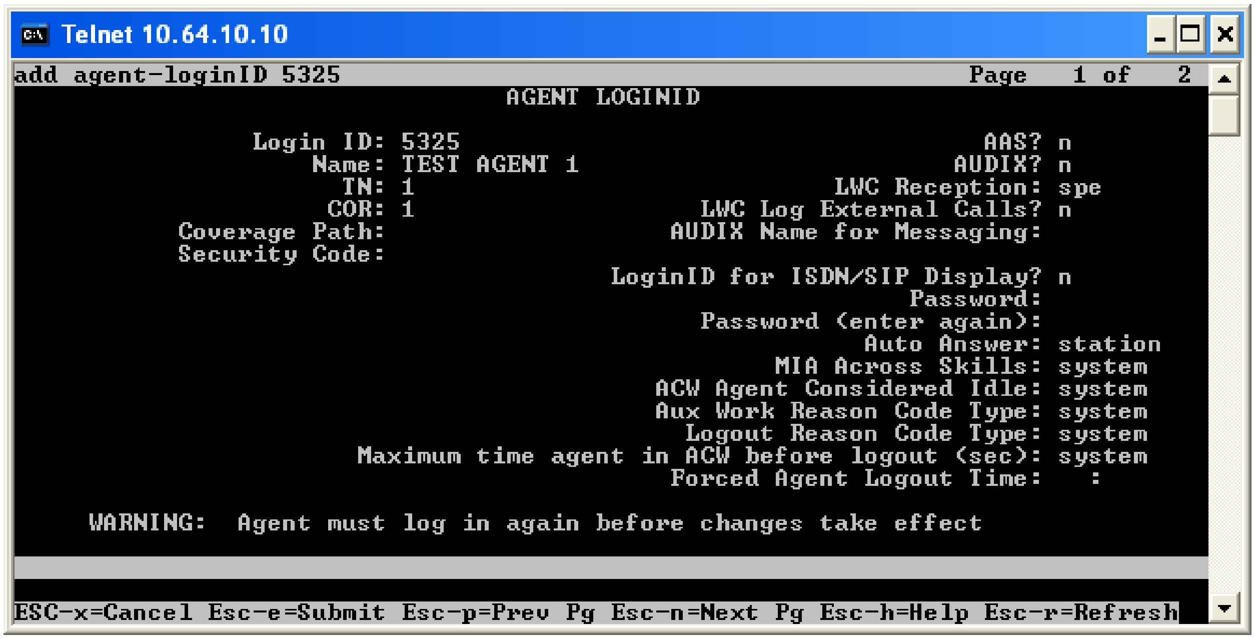
On **Page 2**, set the **Skill** field to **y**, which means that agent membership in the hunt group is based on skills, rather than a pre-programmed assignment to the hunt group.



```
add hunt-group 20                                               Page   2 of  61
                                   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 VDN:
                   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
```

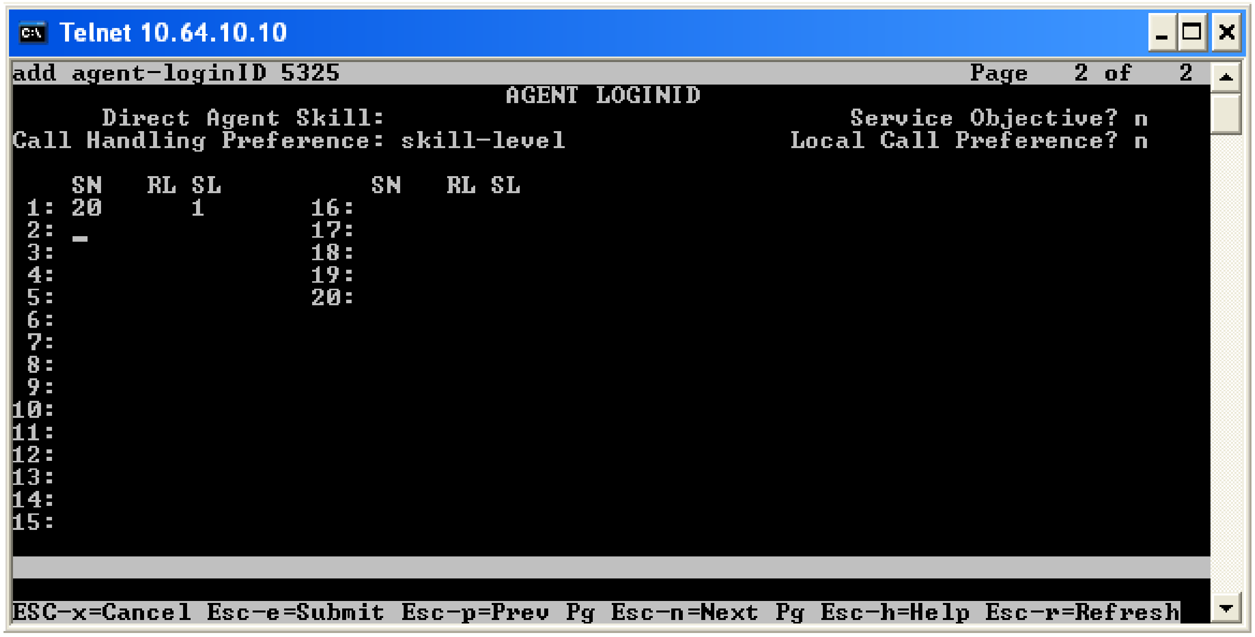
Add entries for agents with the following values as displayed below:

- 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**.



```
add agent-loginID 5325                                          Page   1 of   2
                                  AGENT LOGINID

                Login ID: 5325                                 AAS? n
                    Name: TEST 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


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

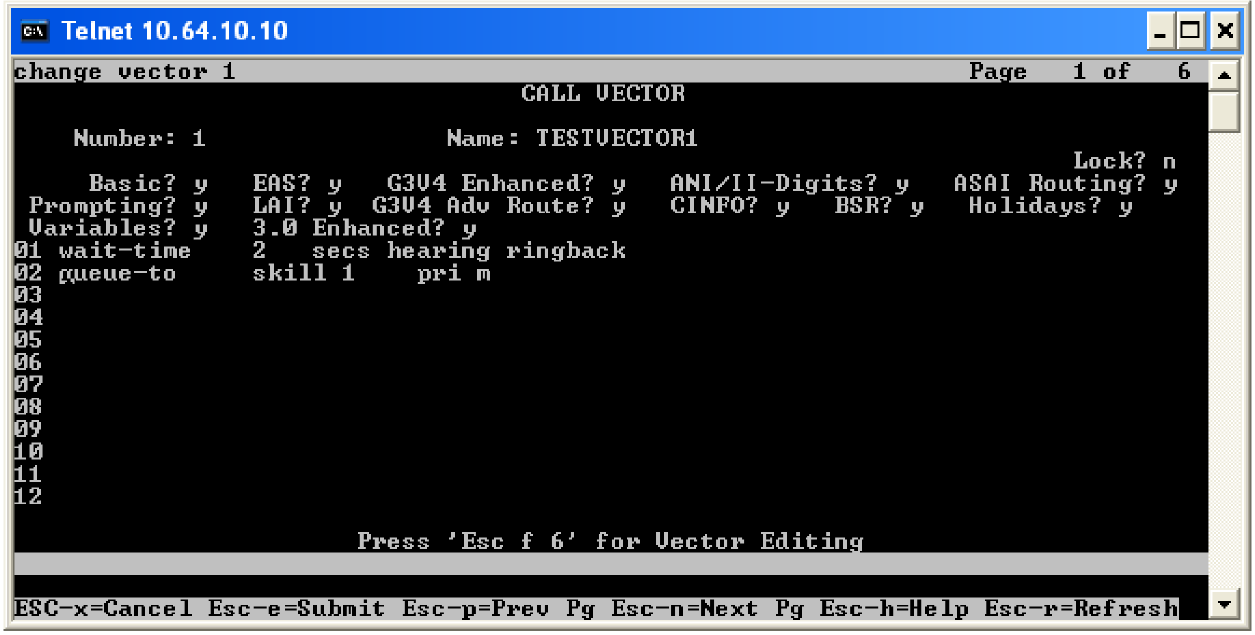
On **Page 2**, set the **Skill Number (SN)** to the hunt group number previously created. The **Skill Level (SL)** may be set according to customer requirements. Repeat this step as necessary to configure additional agent extensions.



```
add agent-loginID 5325                                         Page   2 of   2
                                 AGENT LOGINID
     Direct Agent Skill:                                   Service Objective? n
Call Handling Preference: skill-level                   Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 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:

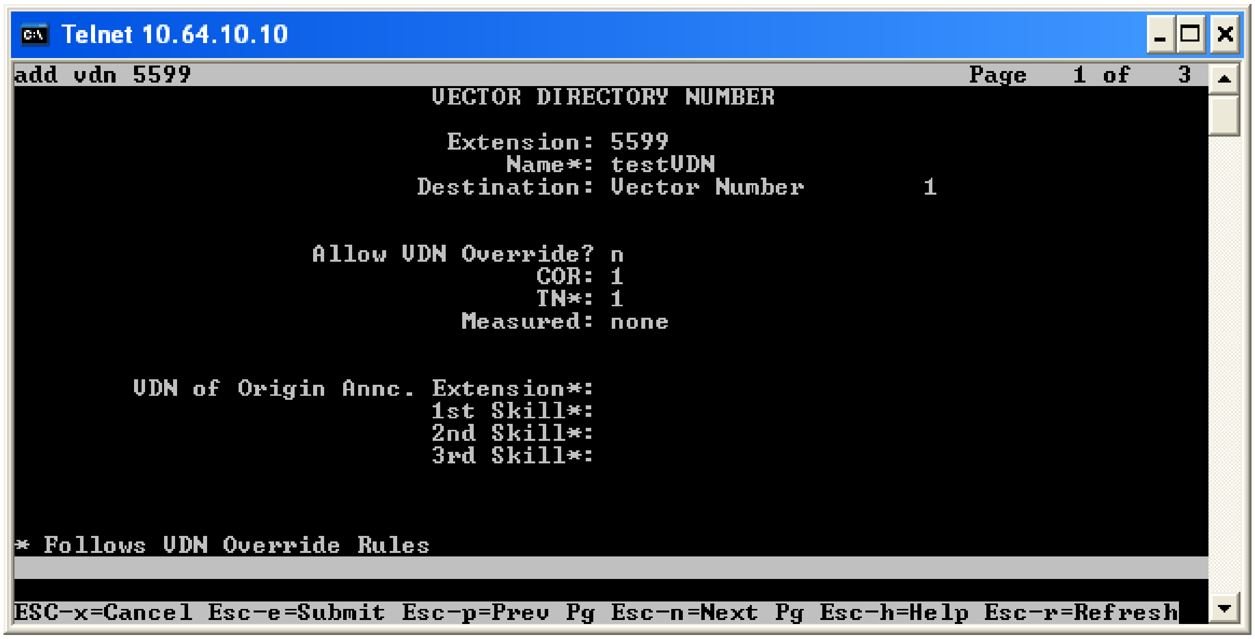
- Enter the **change vector x** command, where **x** is a vector number in the list to be modified.
- Enter a descriptive **Name**, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.



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

    Number: 1                    Name: TESTVECTOR1
                                                                    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 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.



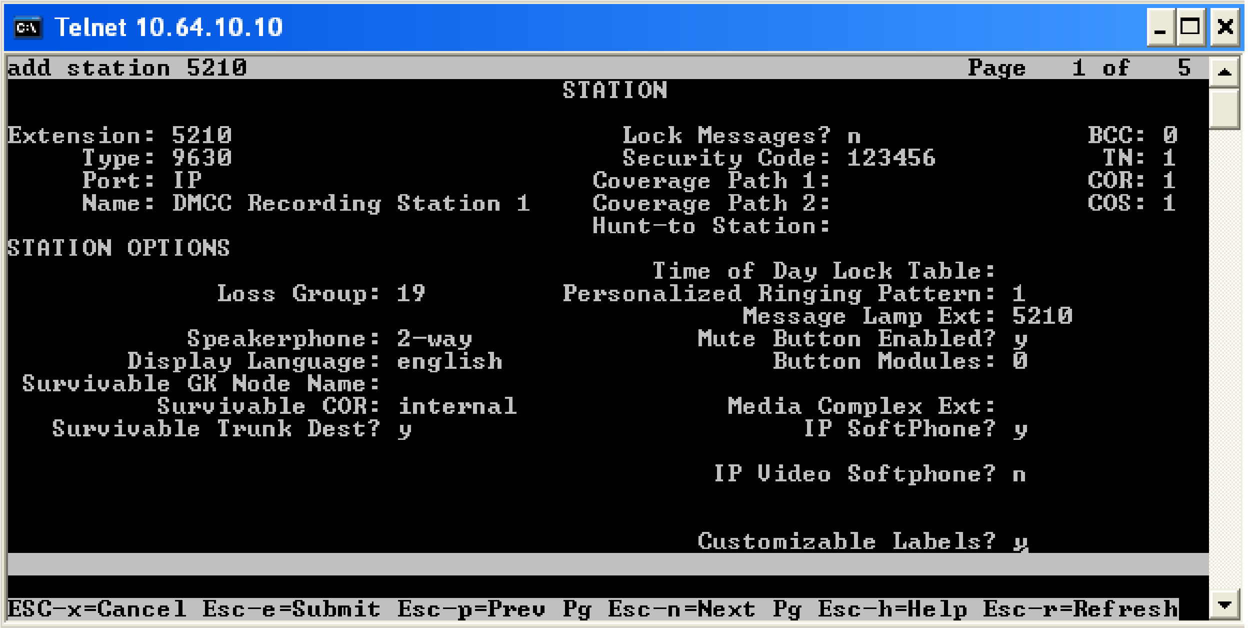
```
add vdn 5599                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 5599
                                 Name*: testVDN
                           Destination: Vector Number        1


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


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


* Follows VDN 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 Communication Manager.

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

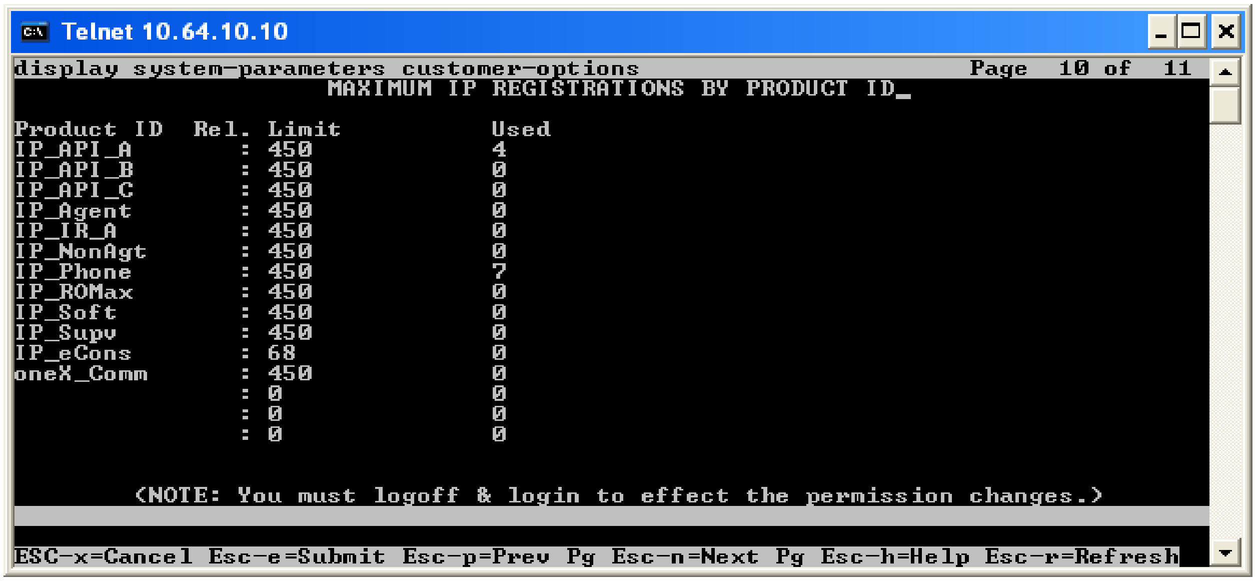
- Enter the **add station x** command, where **x** is a station valid in the dial plan.
- On **Page 1** of the station form, set the **Type** field to an IP telephone set type, enter a descriptive **Name**, and specify the **Security Code**. The security code for all recording stations **MUST** have the same value.
- Set the value for the **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.



```
add station 5210                                                Page   1 of   5
                                     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
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 5210
            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


                                              Customizable Labels? y

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

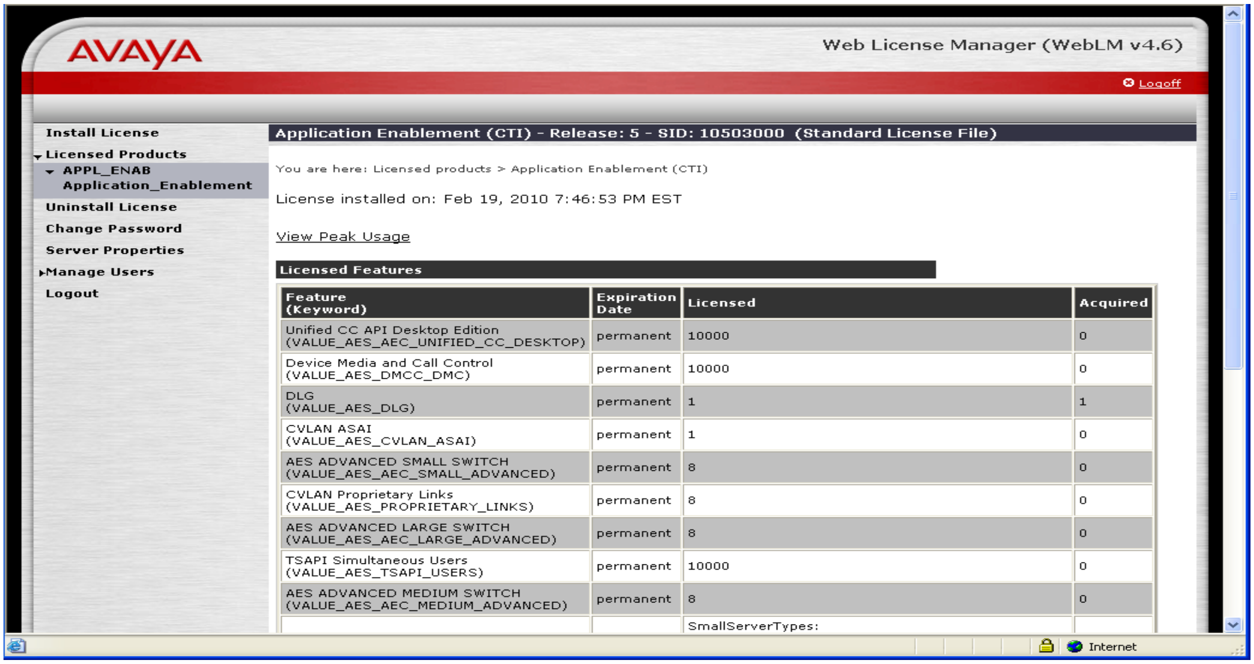
Each DMCC station requires either IP_API_A licenses on Communication Manager or DMCC_DMC licenses through AES.

- On Communication Manager, 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. Ensure the number of licenses **Used** (needed) does not exceed the **Limit**.



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

Product ID   Rel. Limit          Used
IP_API_A        : 450            4
IP_API_B        : 450            0
IP_API_C        : 450            0
IP_Agent        : 450            0
IP_IR_A         : 450            0
IP_NonAgt       : 450            0
IP_Phone        : 450            7
IP_ROMax        : 450            0
IP_Soft         : 450            0
IP_Supv         : 450            0
IP_eCons        : 68             0
oneX_Comm       : 450            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
```

Through AES, licensing can be reviewed after login: **Welcome to OAM -> Licensing -> Licensed Products -> APPL_ENAB -> Application_Enablement – Device Media and Call Control (Value_AES_DMCC_DMC).** If there are not sufficient licenses, contact an authorized Avaya account representative to obtain them. See Section 5 for additional information on AES.



Application Enablement (CTI) - Release: 5 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: Feb 19, 2010 7:46:53 PM EST

View Peak Usage

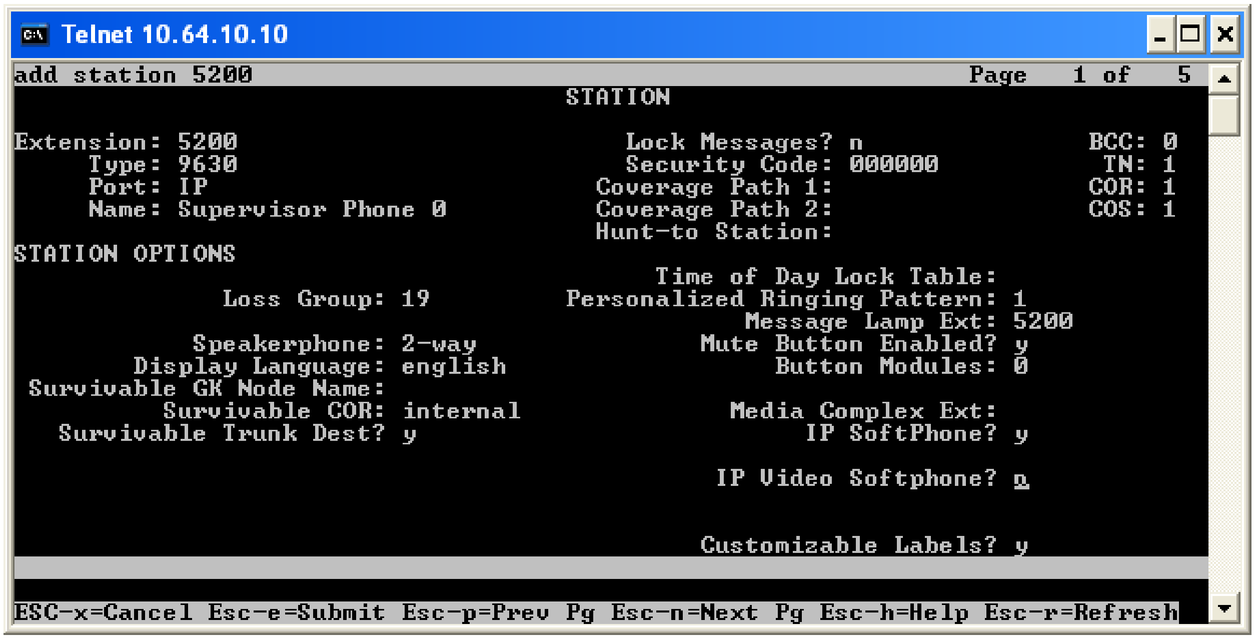
Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	1	1
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	1	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	8	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	8	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	8	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	8	0
		SmallServerTypes:	

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.
- Repeat this procedure as necessary to configure additional monitored stations.



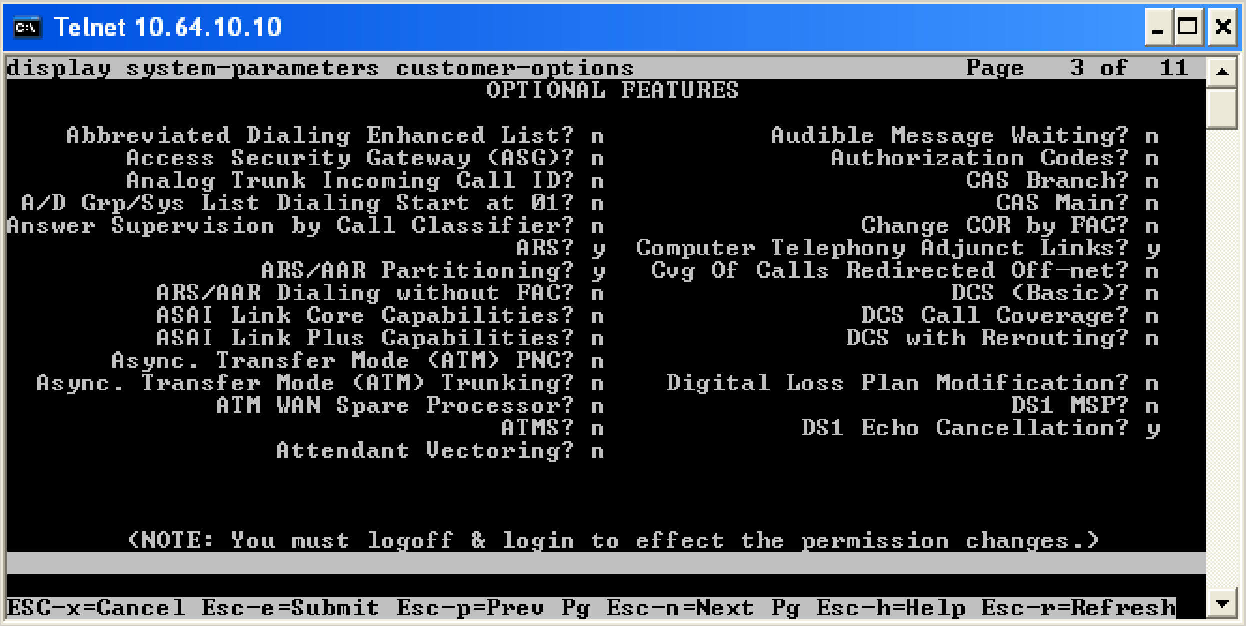
```
add station 5200                                               Page   1 of   5
                                     STATION

Extension: 5200                         Lock Messages? n              BCC: 0
     Type: 9630                         Security Code: 000000          TN: 1
     Port: IP                         Coverage Path 1:                COR: 1
     Name: Supervisor Phone 0         Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19       Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 5200
            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


                                              Customizable Labels? y

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

4.5. Administer Computer Telephony Integration (CTI) Link

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

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

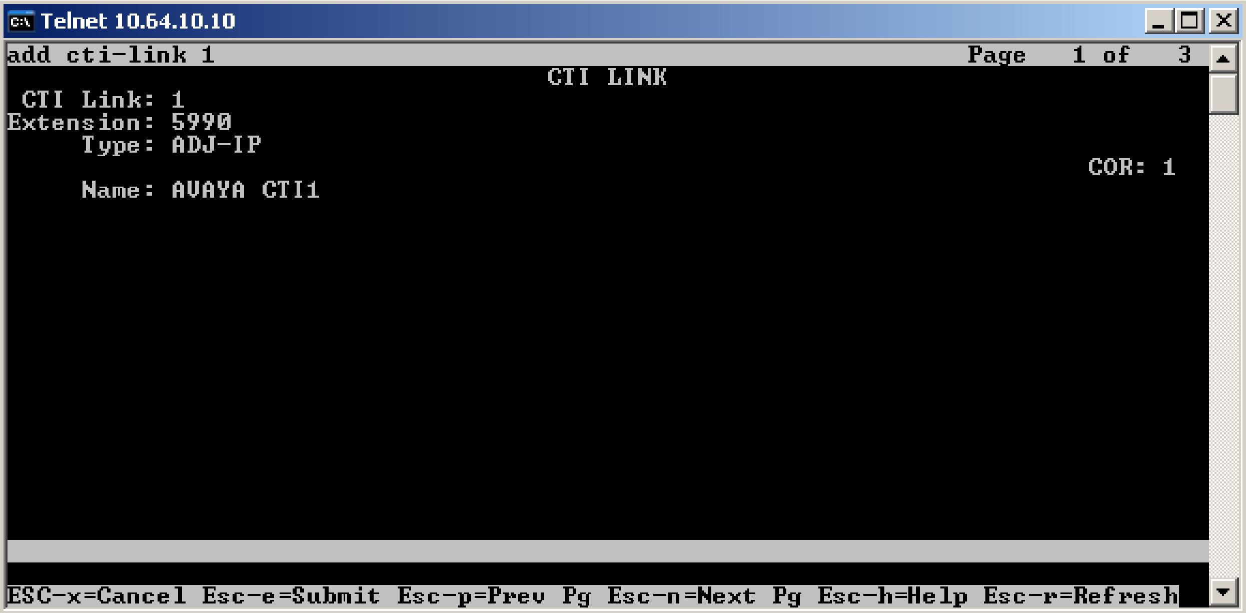
- On **Page 3**, verify that the **Computer Telephony Adjunct Links** field is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.



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

    Abbreviated Dialing Enhanced List? 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? n                DCS Call Coverage? n
          ASAI Link Plus Capabilities? n               DCS with Rerouting? n
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? n
              ATM WAN Spare Processor? n                          DS1 MSP? n
                                 ATMS? n            DS1 Echo Cancellation? y
                  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.

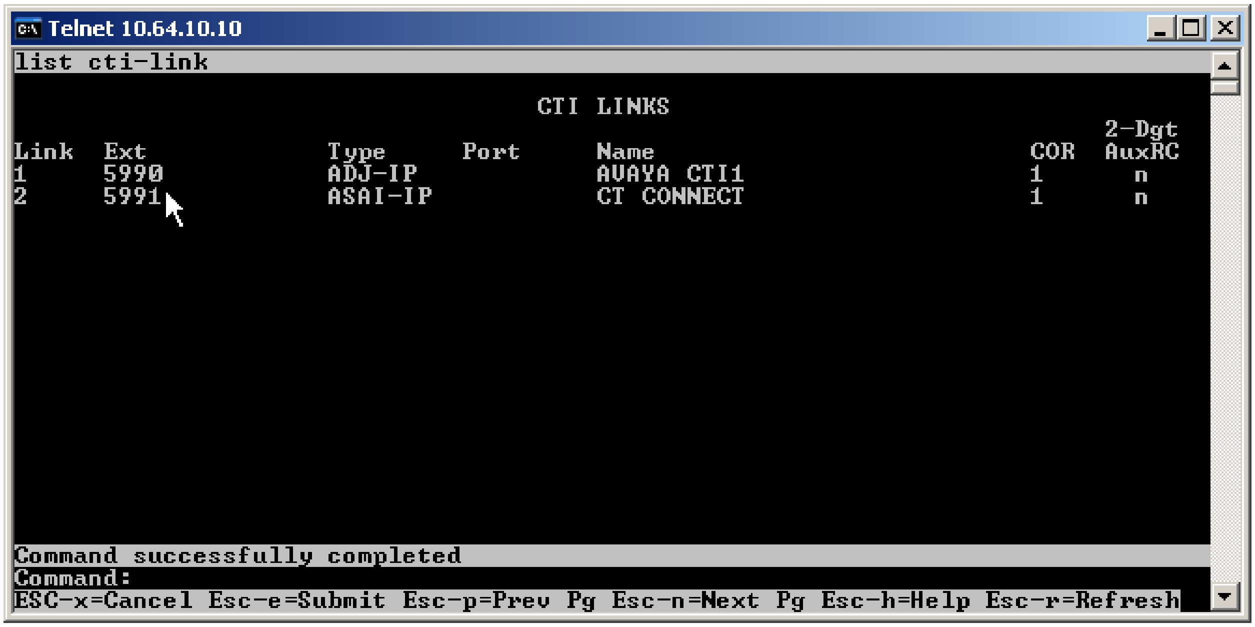
- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.



```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 5990
     Type: ADJ-IP
                                                                    COR: 1
     Name: AVAYA CTI1
```

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

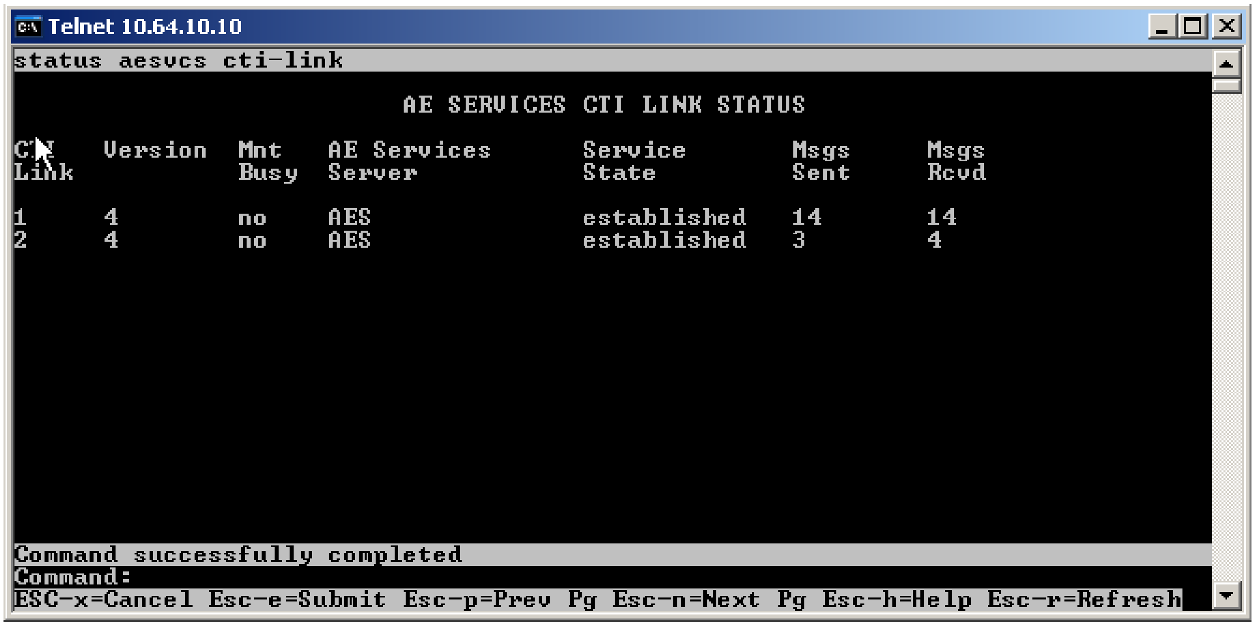
Enter the **list cti-link** command to verify that the CTI Link is correctly configured. In this case, **Link 1** is the link of interest.



```
list cti-link

                                  CTI LINKS
                                                                   2-Dgt
Link  Ext            Type      Port      Name                  COR  AuxRC
1     5990           ADJ-IP              AVAYA CTI1            1      n
2     5991           ASAI-IP             CT CONNECT            1      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**.



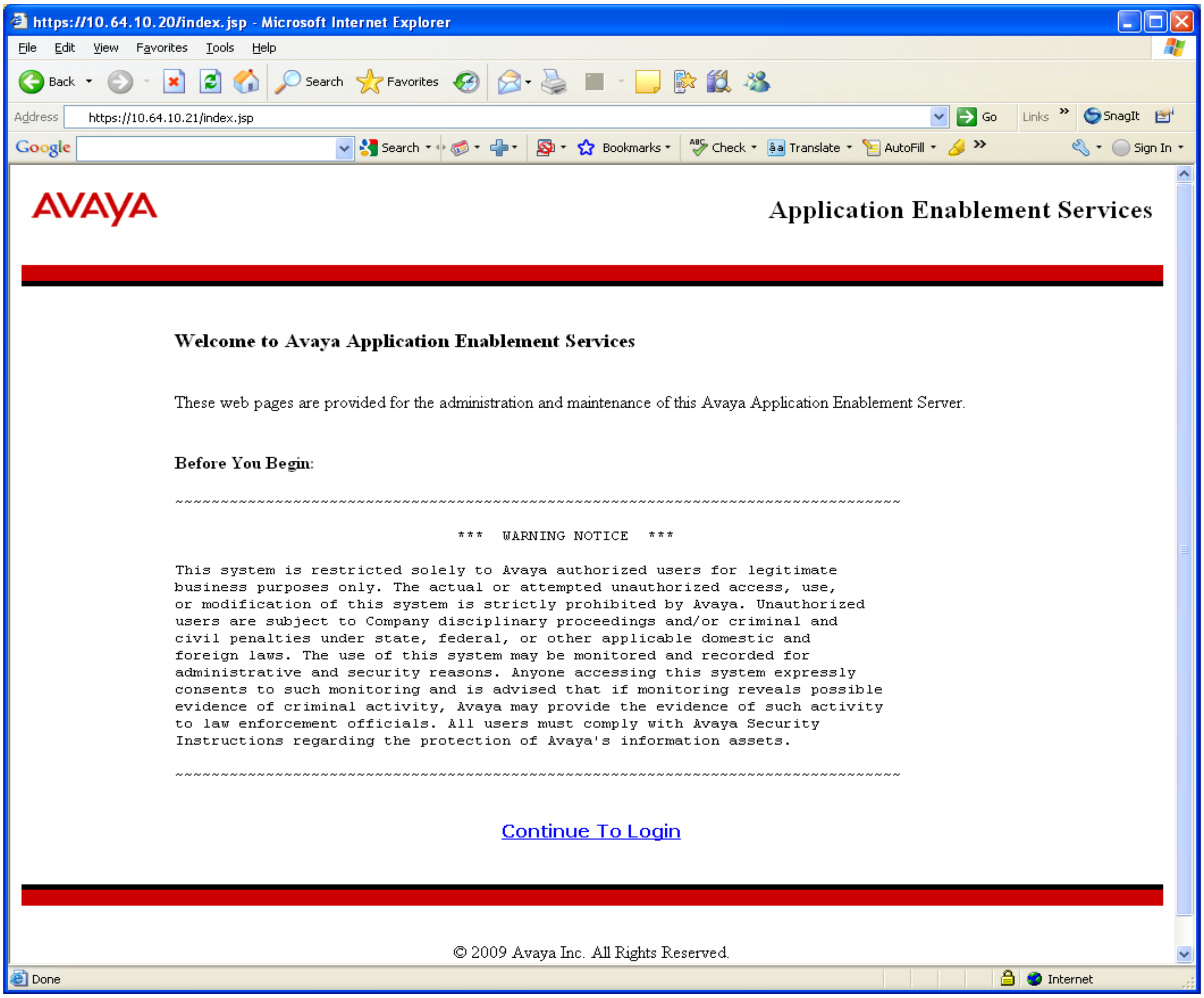
```
status aesvcs cti-link

                              AE SERVICES CTI LINK STATUS

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

1      4          no     AES                established    14        14
2      4          no     AES                established    3         4

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 Application Enablement Services

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

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

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 **Continue to Login** link.


https://10.64.10.20/index.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.64.10.21/index.jsp
Go Links SnagIt
Google Search Bookmarks Check Translate AutoFill Sign In
AVAYA
Done
Internet

Application Enablement Services

Welcome to Avaya Application Enablement Services

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

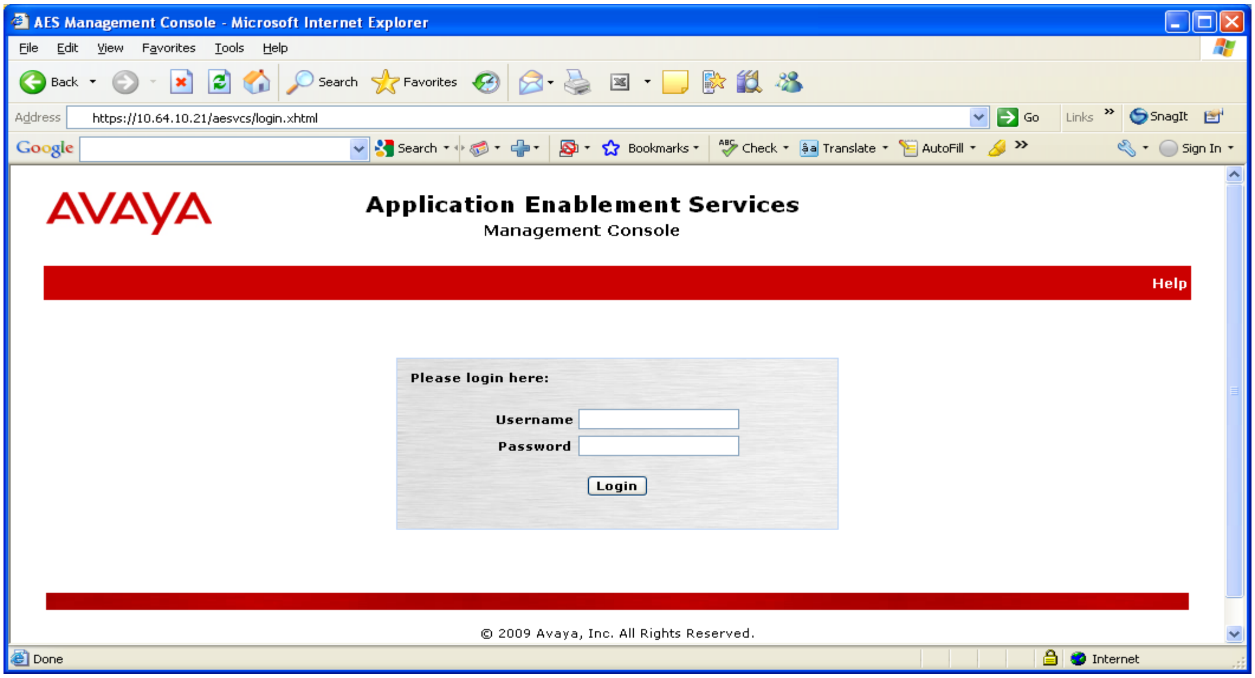
Before You Begin:

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

                  ***   WARNING NOTICE   ***

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

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

Continue To Login

© 2009 Avaya Inc. All Rights Reserved.

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


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.64.10.21/aesvcs/login.xhtml
Go Links SnagIt
Google Search Bookmarks Check Translate AutoFill Sign In
AVAYA
Help
Login
Done
Internet

Application Enablement Services

Management Console

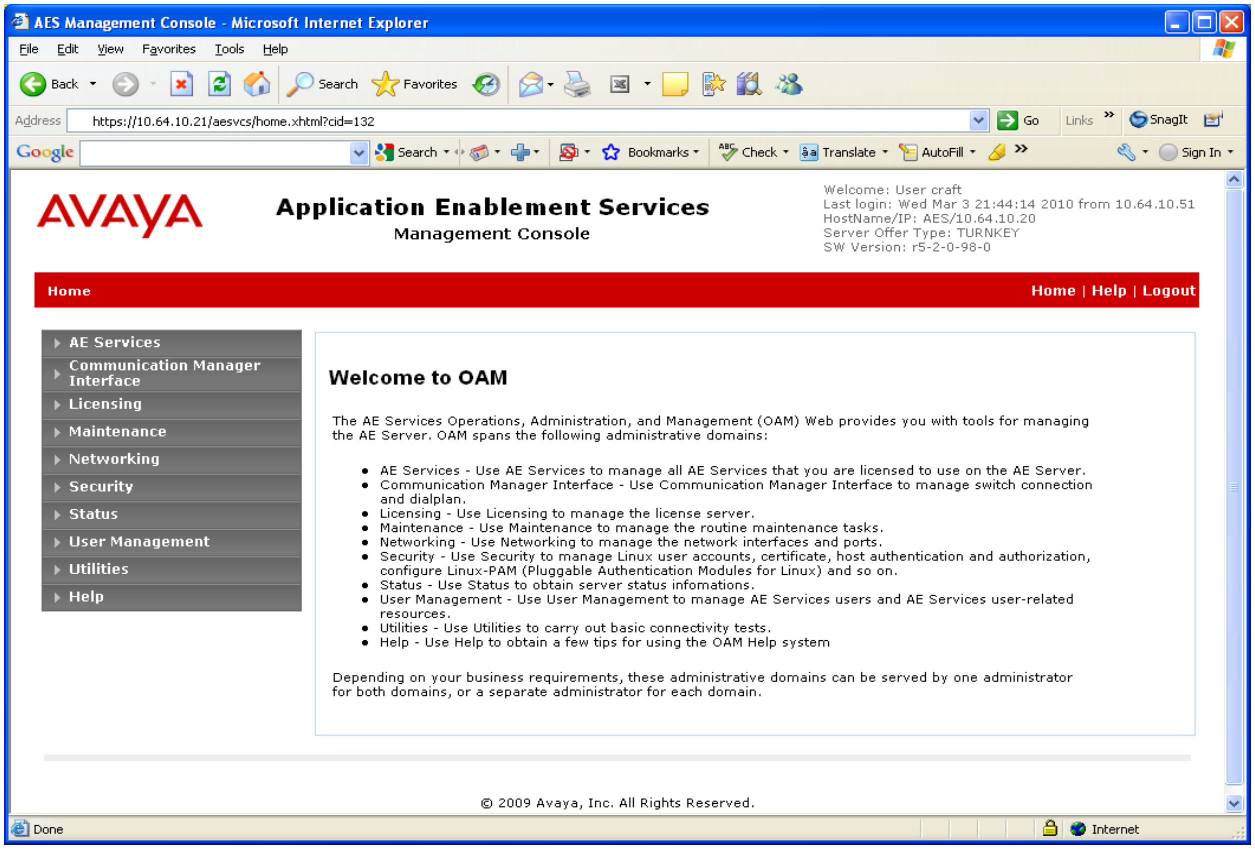
Please login here:

Username

Password

© 2009 Avaya, Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next. Select **AE Services**.


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.64.10.21/aesvcs/home.xhtml?cid=132
Go Links SnagIt
Google Search Bookmarks Check Translate AutoFill Sign In
AVAYA
Home
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help
Done
Internet

Application Enablement Services

Management Console

Welcome: User craft
Last login: Wed Mar 3 21:44:14 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Welcome to OAM

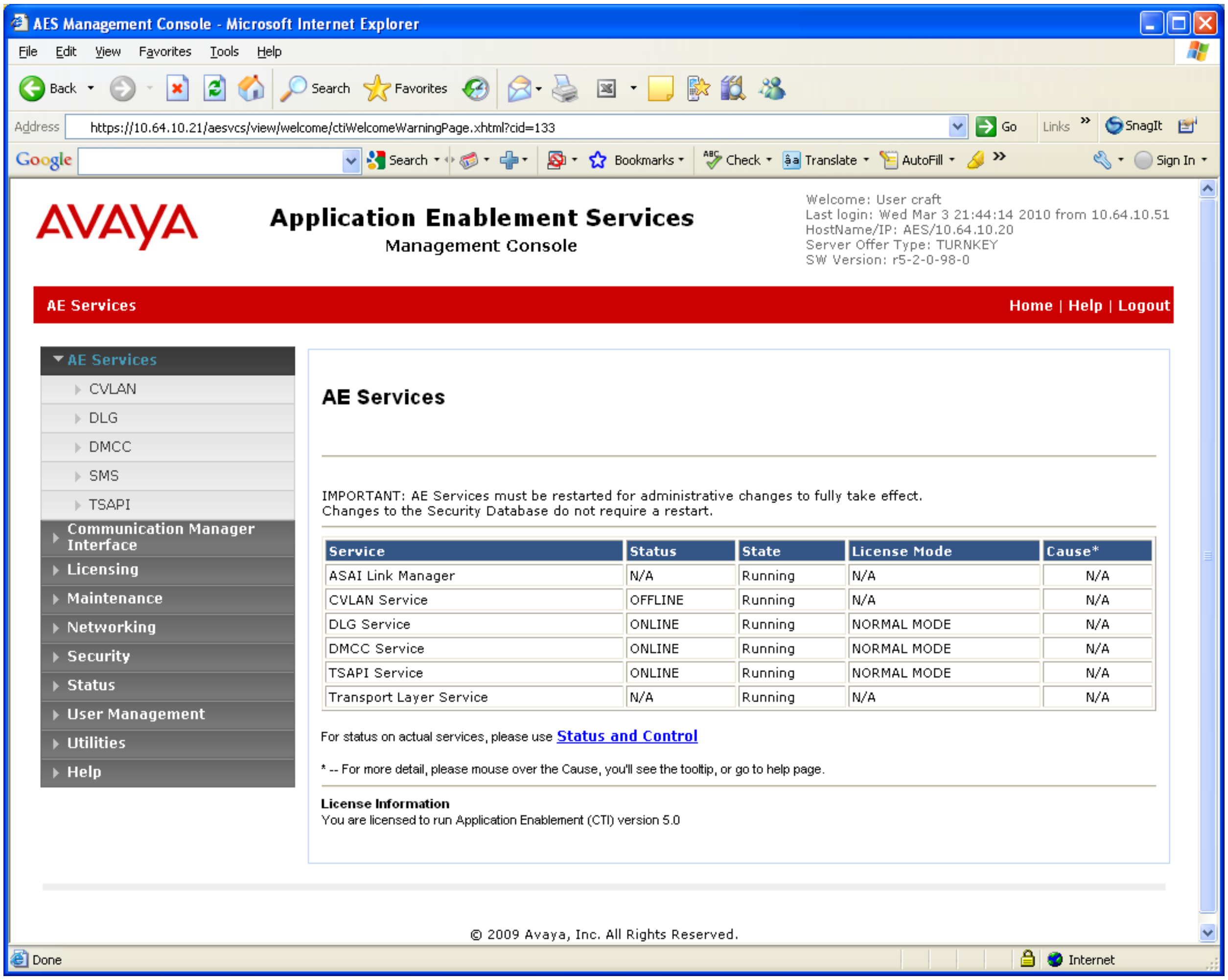
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

© 2009 Avaya, Inc. All Rights Reserved.

The **AE Services** 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.


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.64.10.21/aesvcs/view/welcome/ctiWelcomeWarningPage.xhtml?cid=133 Go Links SnagIt
Google Search Bookmarks Check Translate AutoFill Sign In
AVAYA
Application Enablement Services
Management Console
AE Services
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help
Done
Internet

Welcome: User craft
Last login: Wed Mar 3 21:44:14 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

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

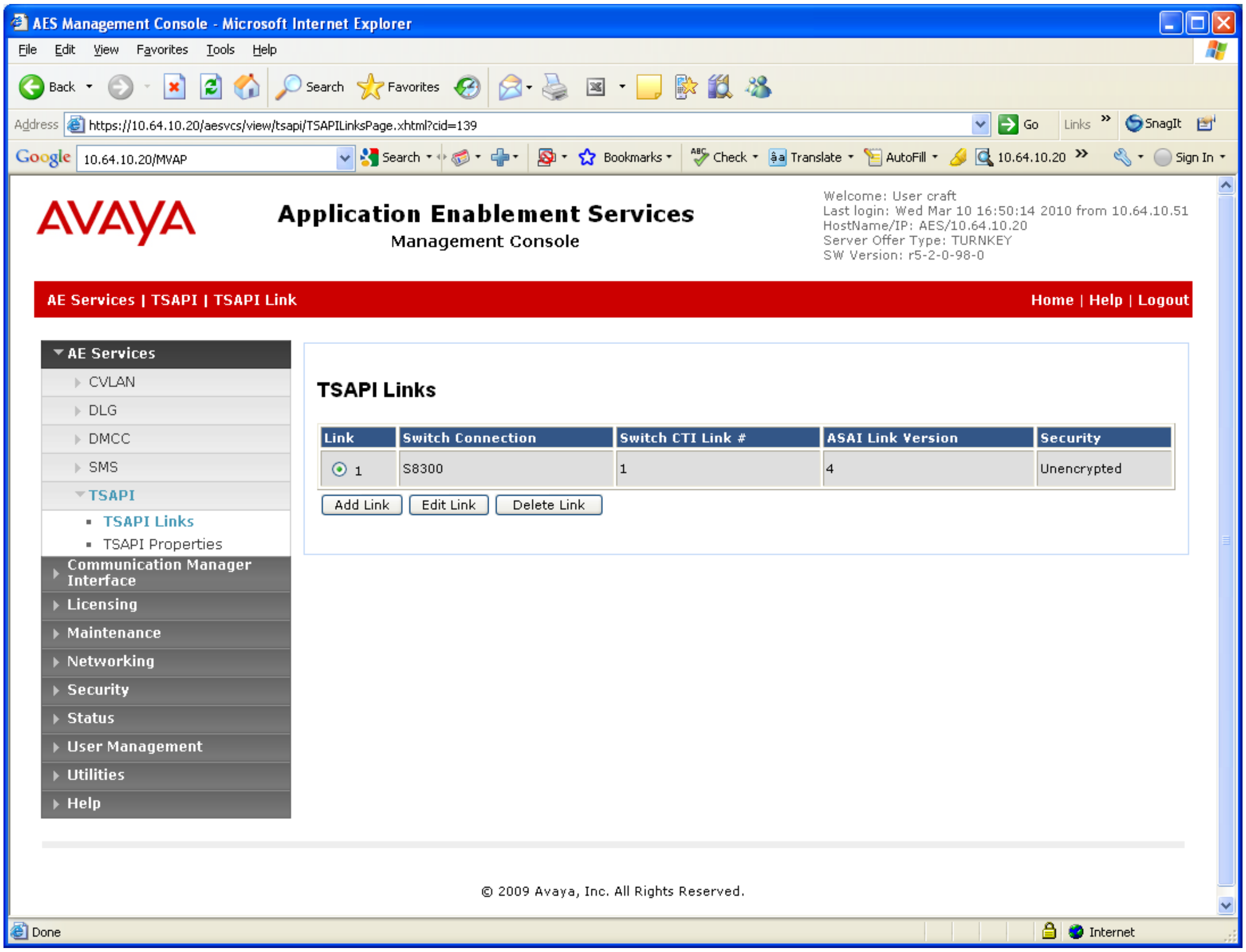
For status on actual services, please use Status and Control

* -- 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 5.0

© 2009 Avaya, Inc. All Rights Reserved.

Navigate to the **AE Services -> TSAPI -> TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**.

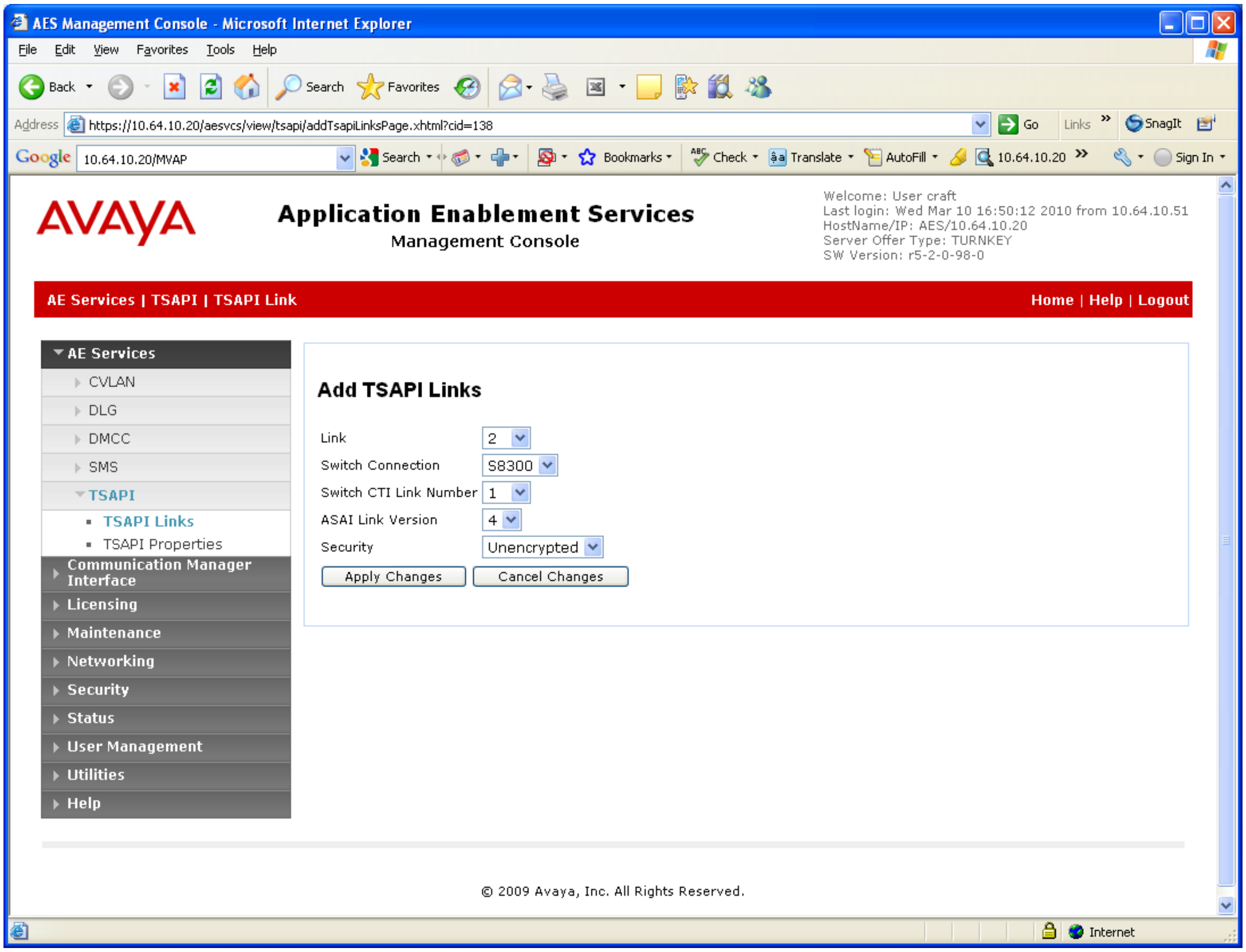


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.64.10.20/aesvcs/view/tsapi/TSAPILinksPage.xhtml?cid=139
Google 10.64.10.20/MVAP
AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Wed Mar 10 16:50:14 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0
AE Services | TSAPI | TSAPI Link
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
TSAPI Properties
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help
Add Link
Edit Link
Delete Link
© 2009 Avaya, Inc. All Rights Reserved.
Done
Internet

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	S8300	1	4	Unencrypted

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.



AES Management Console - Microsoft Internet Explorer

Address https://10.64.10.20/aesvcs/view/tsapi/addTsapiLinksPage.xhtml?cid=138

Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Mar 10 16:50:12 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services | TSAPI | TSAPI Link

Add TSAPI Links

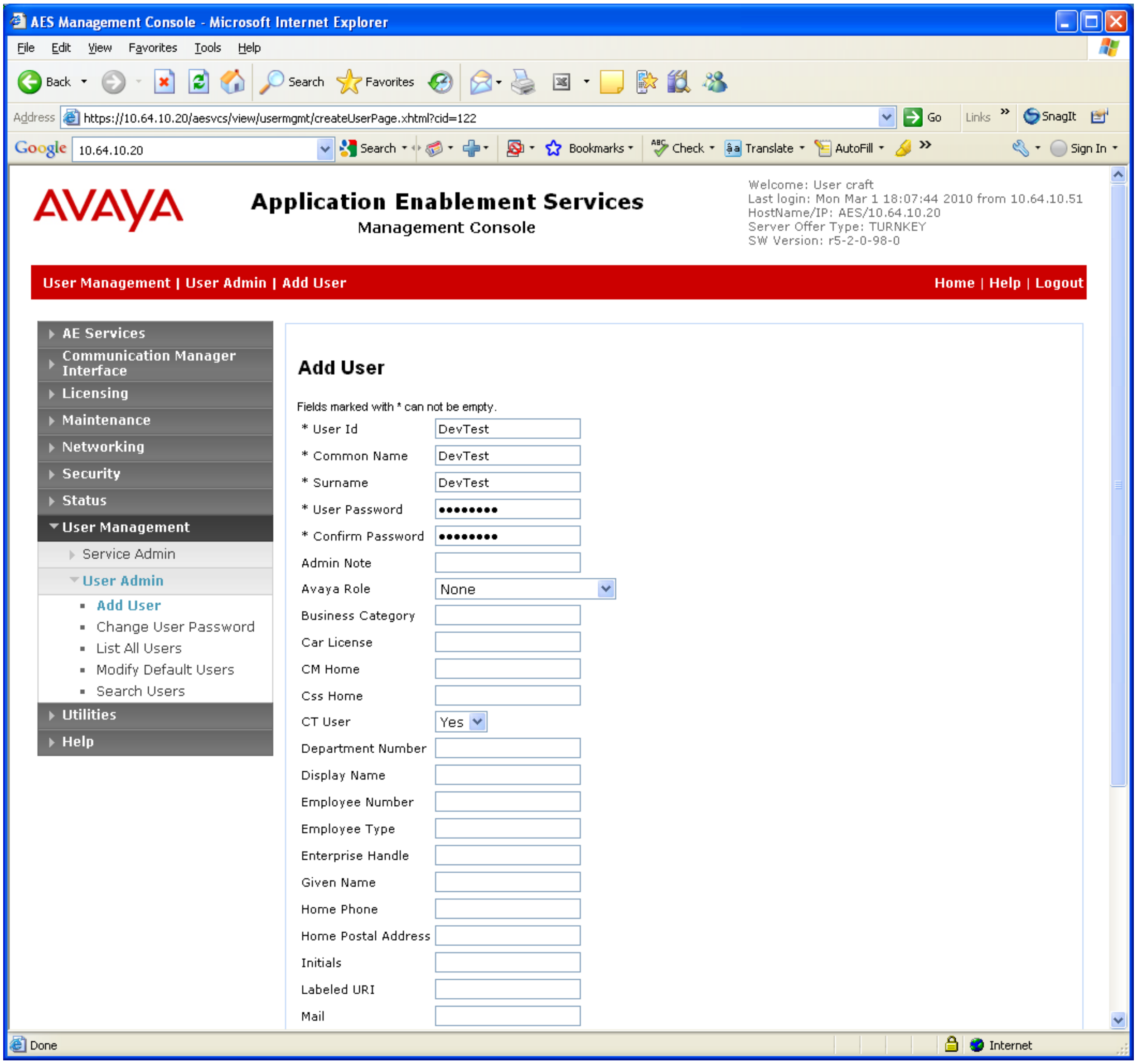
Link	2
Switch Connection	S8300
Switch CTI Link Number	1
ASAI Link Version	4
Security	Unencrypted

© 2009 Avaya, Inc. All Rights Reserved.

Next, add a CTI User, as FocusRecord requires a CTI user to access AES. Select **User Management -> User Admin -> 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).



Address: https://10.64.10.20/aesvcs/view/usermgmt/createUserPage.xhtml?cid=122

Google: 10.64.10.20

Application Enablement Services
Management Console

Welcome: User craft
Last login: Mon Mar 1 18:07:44 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

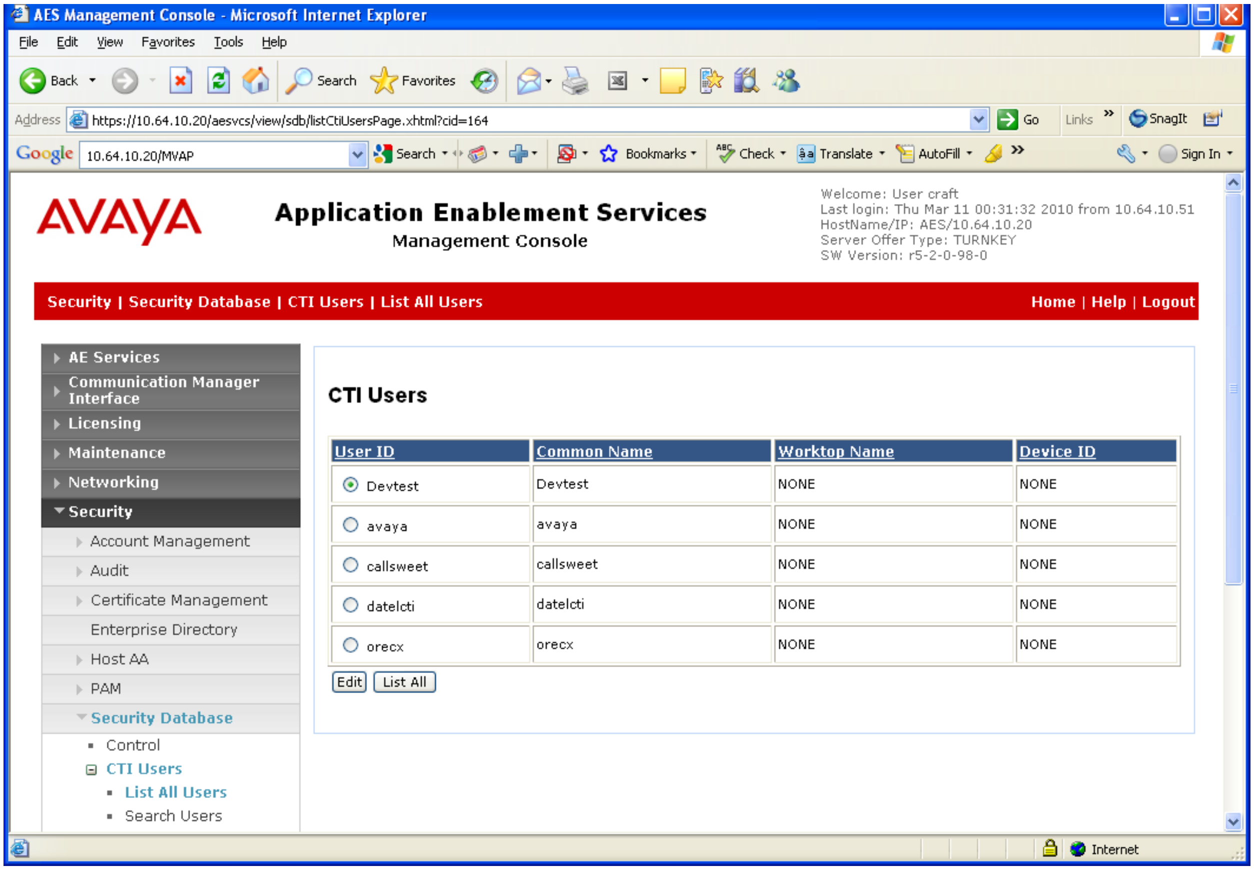
User Management | User Admin | Add User — Home | Help | Logout

Add User

Fields marked with * can not be empty.

* User Id	DevTest
* Common Name	DevTest
* Surname	DevTest
* User Password	••••••••
* Confirm Password	••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	
Mail	

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

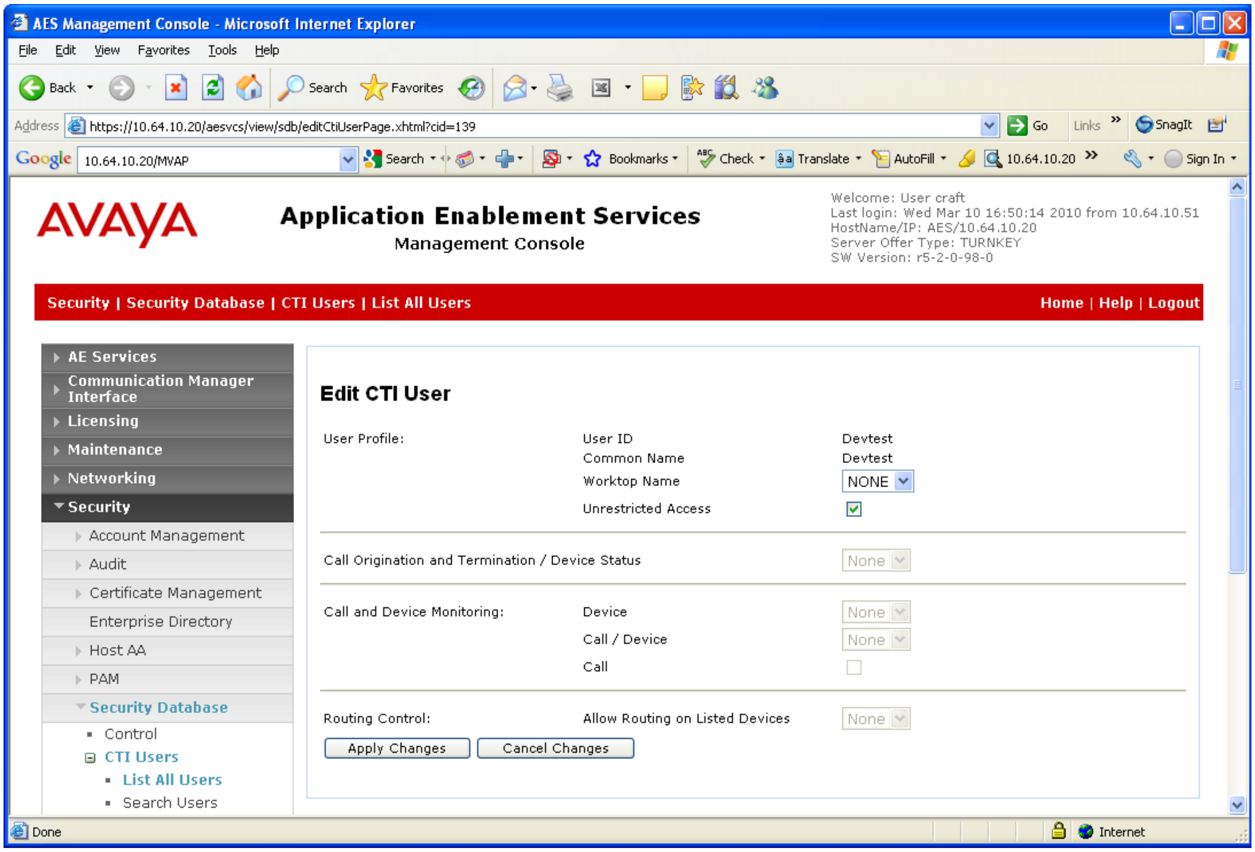

AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.64.10.20/aesvcs/view/sdb/listCtiUsersPage.xhtml?cid=164
AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Thu Mar 11 00:31:32 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0
Security | Security Database | CTI Users | List All Users
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users
Search Users
Internet

CTI Users

User ID	Common Name	Worktop Name	Device ID
● Devtest	Devtest	NONE	NONE
○ avaya	avaya	NONE	NONE
○ callsweet	callsweet	NONE	NONE
○ datelcti	datelcti	NONE	NONE
○ orecx	orecx	NONE	NONE

Edit | List All

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


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.64.10.20/aesvcs/view/sdb/editCtiUserPage.xhtml?cid=139
Google 10.64.10.20/MVAP
AVAYA
Application Enablement Services
Management Console
Security | Security Database | CTI Users | List All Users
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users
Search Users
Done
Internet

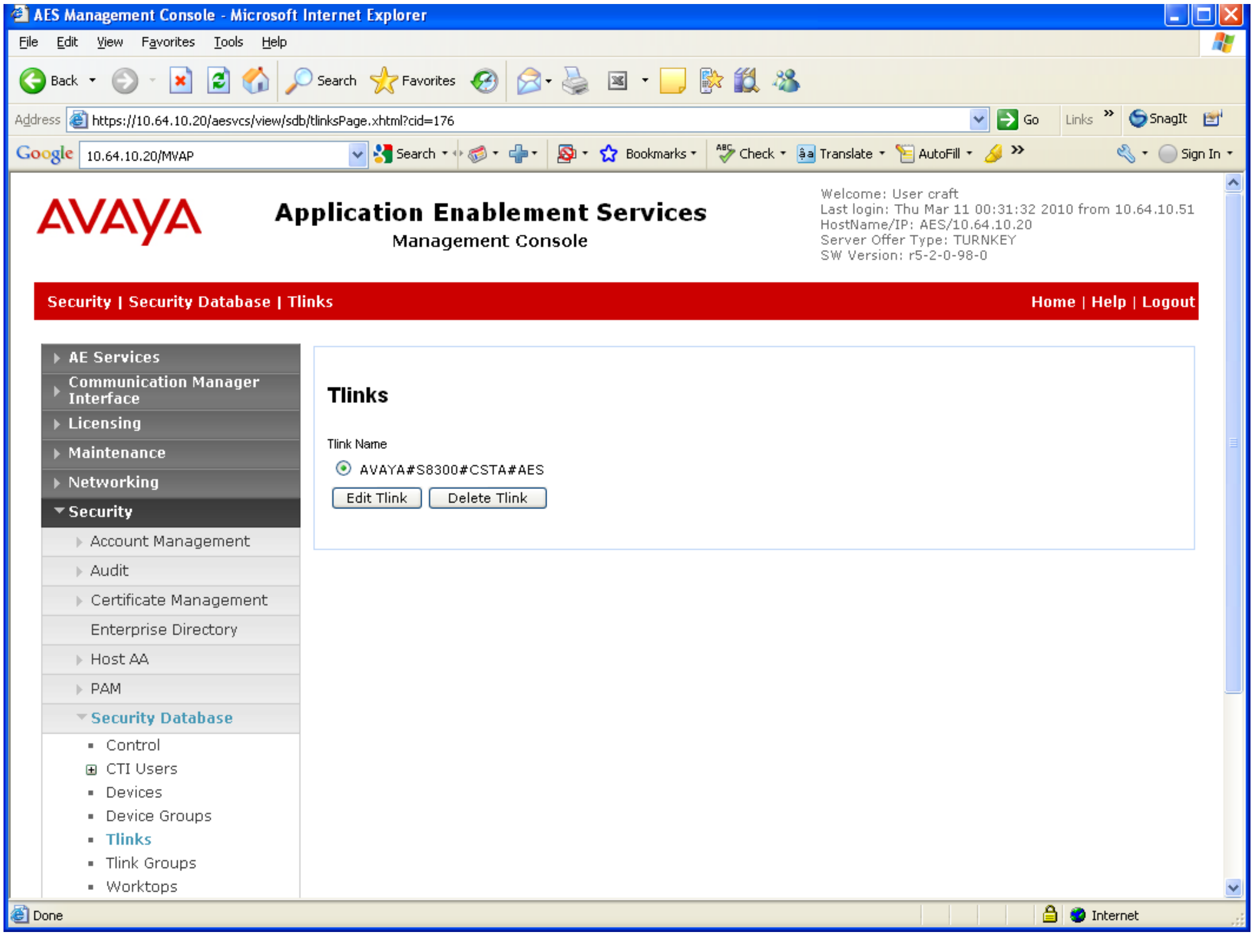
Welcome: User craft
Last login: Wed Mar 10 16:50:14 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Edit CTI User

User Profile:	User ID	Devtest
	Common Name	Devtest
	Worktop Name	NONE
	Unrestricted Access	☑
Call Origination and Termination / Device Status		None
Call and Device Monitoring:	Device	None
	Call / Device	None
	Call	□
Routing Control:	Allow Routing on Listed Devices	None

Apply Changes | Cancel Changes

Select **Security -> Security Database -> 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.


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.64.10.20/aesvcs/view/sdb/tlinksPage.xhtml?cid=176
Go Links SnagIt
Google 10.64.10.20/MVAP Search Bookmarks Check Translate AutoFill Sign In
AVAYA
Application Enablement Services
Management Console
Security | Security Database | Tlinks
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks
Tlink Groups
Worktops
Edit Tlink
Delete Tlink
Done
Internet

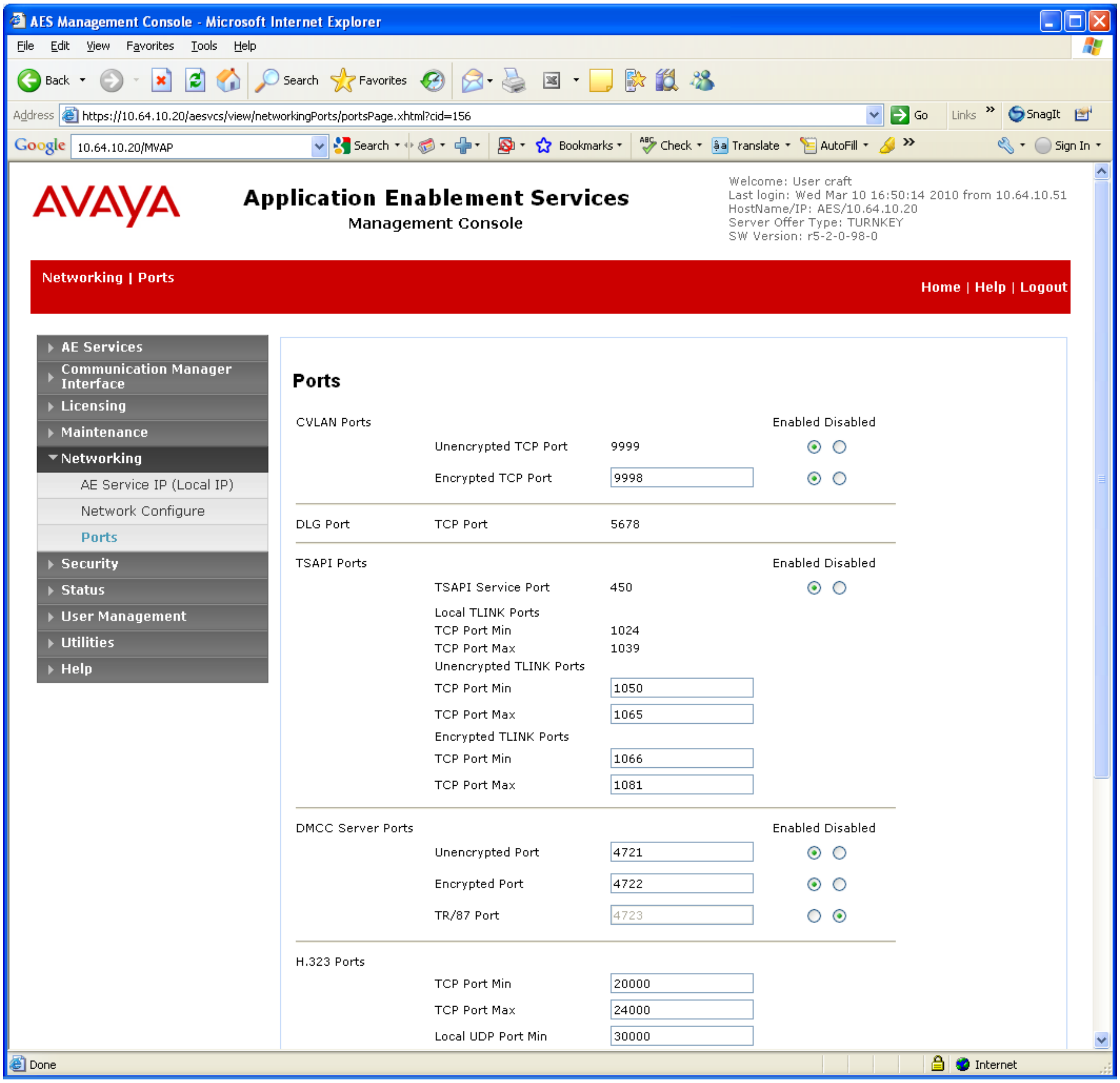
Welcome: User craft
Last login: Thu Mar 11 00:31:32 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Tlinks

Tlink Name

● AVAYA#S8300#CSTA#AES

Navigate to the **Networking -> 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.


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.64.10.20/aesvcs/view/networkingPorts/portsPage.xhtml?cid=156
Go Links SnagIt
Google 10.64.10.20/MVAP
Search Bookmarks Check Translate AutoFill Sign In
AVAYA
Networking | Ports
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
AE Service IP (Local IP)
Network Configure
Ports
Security
Status
User Management
Utilities
Help
Done
Internet

Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Mar 10 16:50:14 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●
H.323 Ports				
	TCP Port Min	20000		
	TCP Port Max	24000		
	Local UDP Port Min	30000		

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 communicates with AES and Communication Manager.

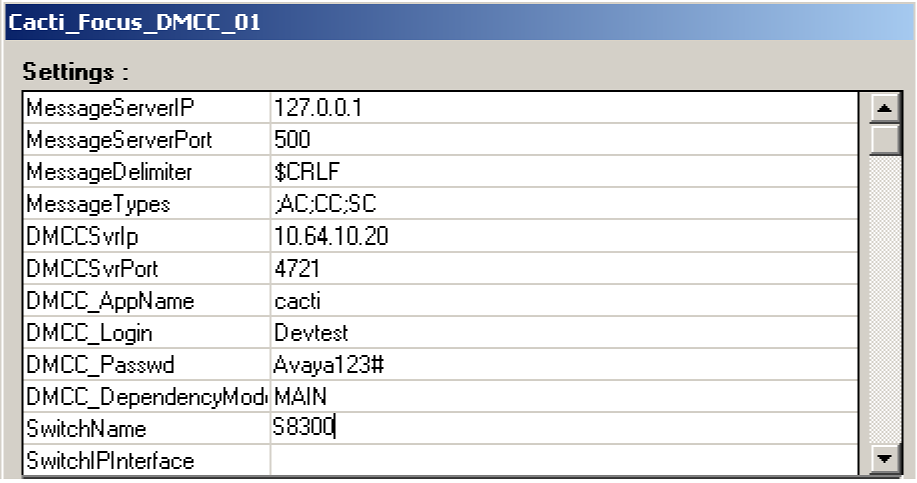
Refer to [3] for configuring the Cacti FocusRecord application.

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

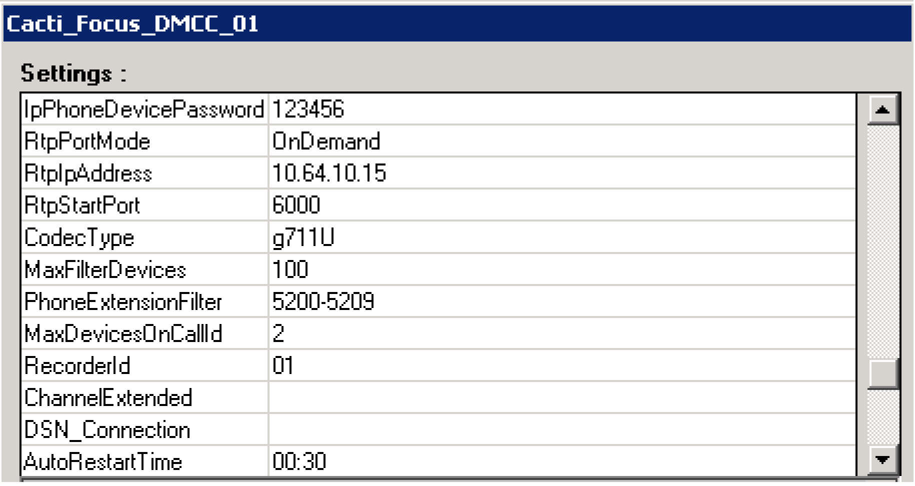
Settings :

MessageServerIP	127.0.0.1
MessageServerPort	500
MessageDelimiter	$CRLF
MessageTypes	;AC;CC;SC
DMCCSvrIp	10.64.10.20
DMCCSvrPort	4721
DMCC_AppName	cacti
DMCC_Login	Devtest
DMCC_Passwd	Avaya123#
DMCC_DependencyMod	MAIN
SwitchName	S8300
SwitchIPInterface	

The following screen shows the second part of DMCC Configuration.

- **IpPhoneDevicePasswd** – Enter the recording (DMCC stations) extension Security Code, 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).



Cacti_Focus_DMCC_01

Settings :

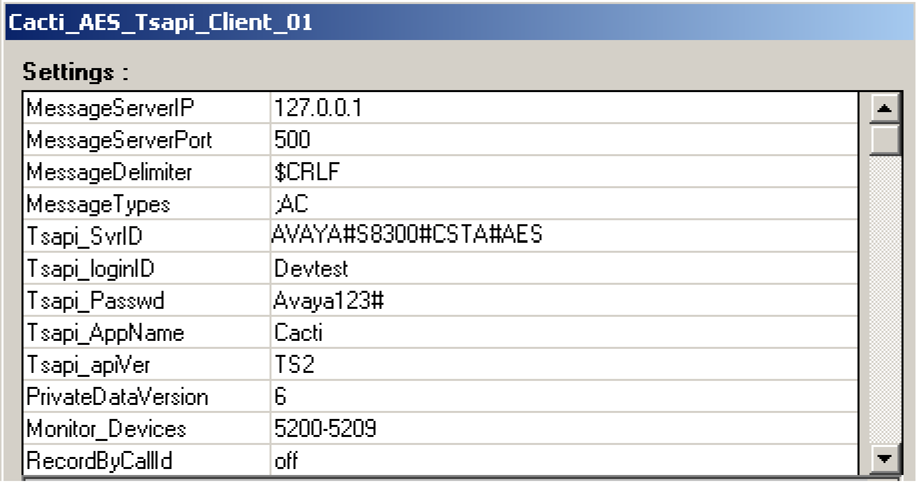
IpPhoneDevicePassword	123456
RtpPortMode	OnDemand
RtpIpAddress	10.64.10.15
RtpStartPort	6000
CodecType	g711U
MaxFilterDevices	100
PhoneExtensionFilter	5200-5209
MaxDevicesOnCallId	2
RecorderId	01
ChannelExtended	
DSN_Connection	
AutoRestartTime	00:30

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).



Cacti_AES_Tsapi_Client_01

Settings :

MessageServerIP	127.0.0.1
MessageServerPort	500
MessageDelimiter	$CRLF
MessageTypes	;AC
Tsapi_SvrID	AVAYA#S8300#CSTA#AES
Tsapi_loginID	Devtest
Tsapi_Passwd	Avaya123#
Tsapi_AppName	Cacti
Tsapi_apiVer	TS2
PrivateDataVersion	6
Monitor_Devices	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 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.

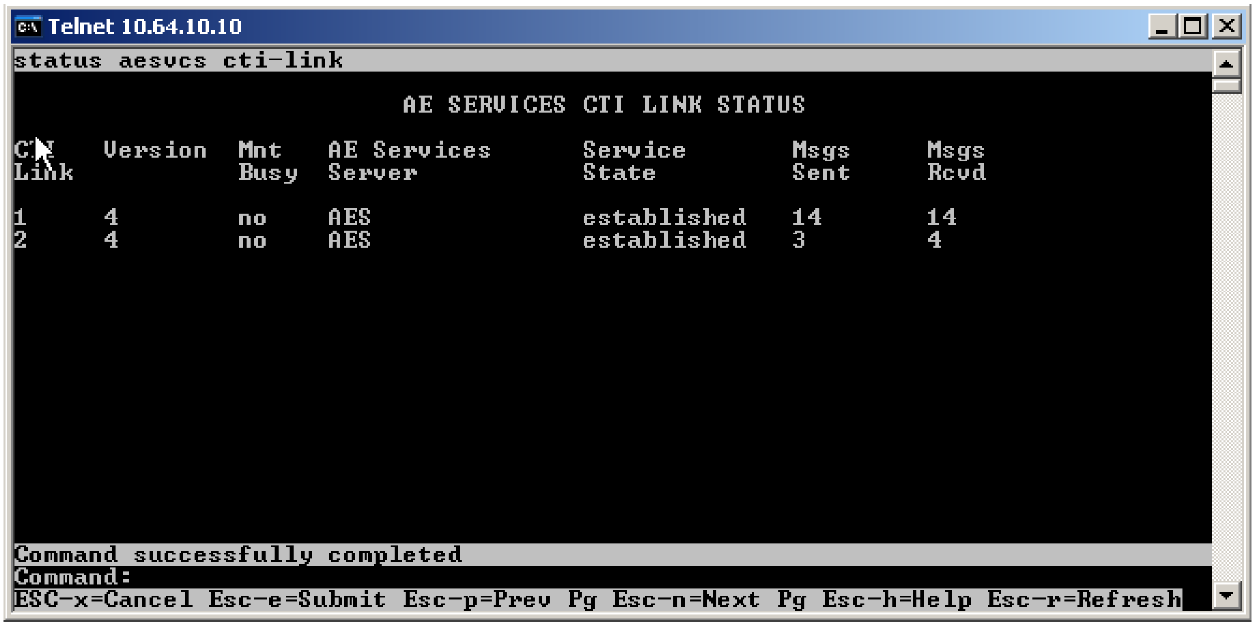
The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to the FocusRecord server and Communication Manager, stopping the CTI service, and pulling power from Communication Manager.

All test cases passed. No errors were detected.

8. Verification Steps

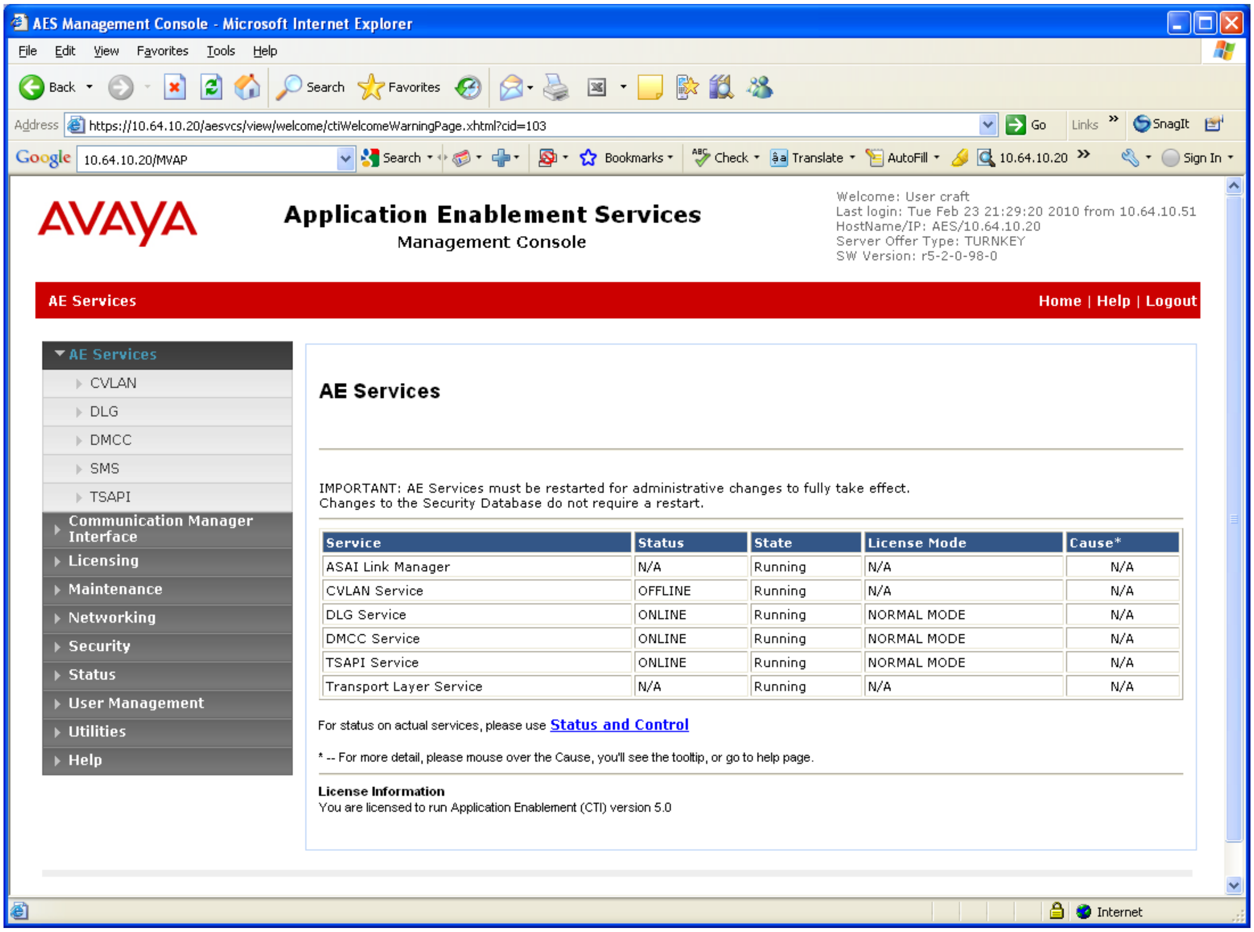
This section provides the tests that can be performed to verify proper configuration of Communication Manager, AES, and FocusRecord.

For Communication Manager, check the CTI Link status with the **status aesvcs cti-link** command (Link 1 for this configuration). The service state should show **no** for maintenance busy and the Service State should indicate **established**.



```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1      4         no    AES              established    14        14
2      4         no    AES              established    3         4











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 **ONLINE, Running**, and **NORMAL MODE**.


AES Management Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.64.10.20/aesvcs/view/welcome/ctiWelcomeWarningPage.xhtml?cid=103
Go Links SnagIt
Google 10.64.10.20/MVAP
Search Bookmarks Check Translate AutoFill 10.64.10.20 Sign In
AVAYA
AE Services
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help
Internet

Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Feb 23 21:29:20 2010 from 10.64.10.51
HostName/IP: AES/10.64.10.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

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.

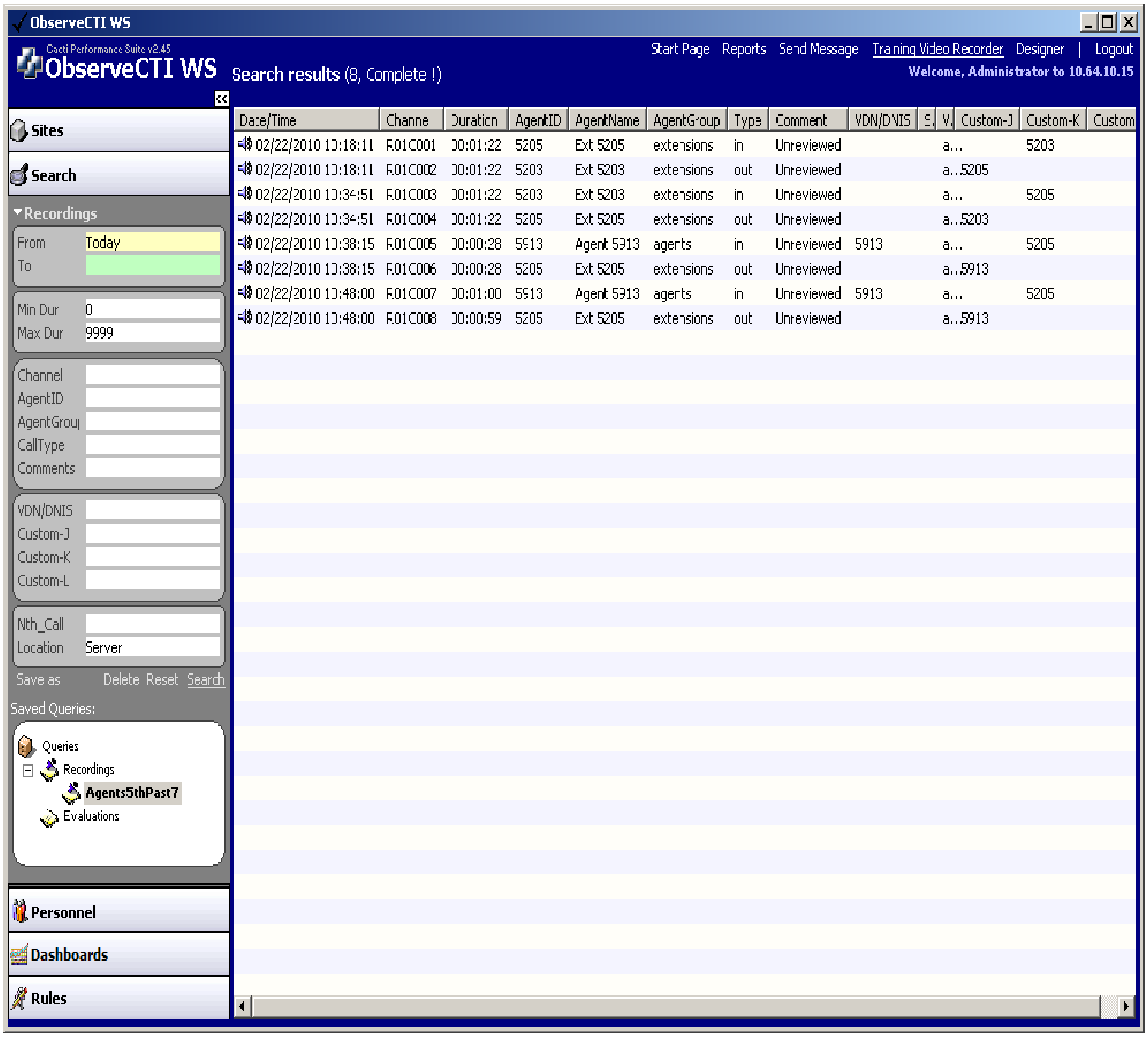
Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	ONLINE	Running	NORMAL MODE	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

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 5.0

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



Search results (8, Complete !)

From	Today
To	
Min Dur	0
Max Dur	9999
Channel	
AgentID	
AgentGrou	
CallType	
Comments	
VDN/DNIS	
Custom-J	
Custom-K	
Custom-L	
Nth_Call	
Location	Server

Date/Time	Channel	Duration	AgentID	AgentName	AgentGroup	Type	Comment	VDN/DNIS	S.	V.	Custom-J	Custom-K	Custom
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 Communication Manager and 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] *Administering Avaya Aura^{TM} Communication Manager*, Doc ID: 03-300509, May 4, 2009

[2] *Avaya Aura^{TM} Application Enablement Services Administration and Maintenance Guide*, Doc ID: 02-300357, November 20, 2009

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

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.