Application Notes for Presence Technology Presence Suite with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Presence Technology Presence Suite to successfully interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. Presence Suite is a multi-channel contact management suite which handles voice, text chat, email and web contact mechanisms. Avaya Telephony Service API (TSAPI) interface is used to monitor and control agent stations, and handle routing of external calls.

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

1 Introduction

These Application Notes describe the compliance tested configuration using Presence Suite and Avaya Aura^{TM} Communication Manager with Avaya Aura^{TM} Application Enablement Services (AES). Presence Suite is a multi-channel contact management suite able to handle voice, e-mail and web chat contact mechanisms. Avaya Telephony Service API (TSAPI) interface is used to monitor and control agent stations, generate phantom calls for non-voice contacts, and handle routing of external calls. Presence Suite consists of a number of modules. Only the following modules were compliance tested.

- Presence Voice Outbound
- Presence Voice Inbound
- Presence Messaging
- Presence Internet

Link Failure\Recovery was also tested to ensure successful reconnection on link failure. Upon starting the Presence Server application, the application automatically queries Application Enablement Services for device status and requests monitoring. The Presence Server specifies where to route each call and hence how to handle the calls, based on agent status information that the application tracks from CTI device query results and event reports received from Application Enablement Services.

1.1 Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on verifying Presence Suite handling of TSAPI messages in the areas of routing, call control and event notification. The serviceability testing focused on verifying the Presence Suite ability to recover from adverse conditions, such as stopping the TSAPI Service, taking the CTI link offline and disconnecting the Ethernet cable for the CLAN.

1.2 Support

Technical support can be obtained for Presence Technology Presence Suite as follows:

Email:	support@presenceco.com
Website:	www.presenceco.com
Phone:	+34 93 10 10 300

2 Reference Configuration

Figure 1 shows the network topology during compliance testing. Avaya S8500B Server running Communication Manager with an Avaya G650 Media Gateway was used as the hosting PBX. Presence Suite, including Presence Agent PC's, was connected to the LAN and controlled the Avaya IP telephones via Application Enablement Services using TSAPI.

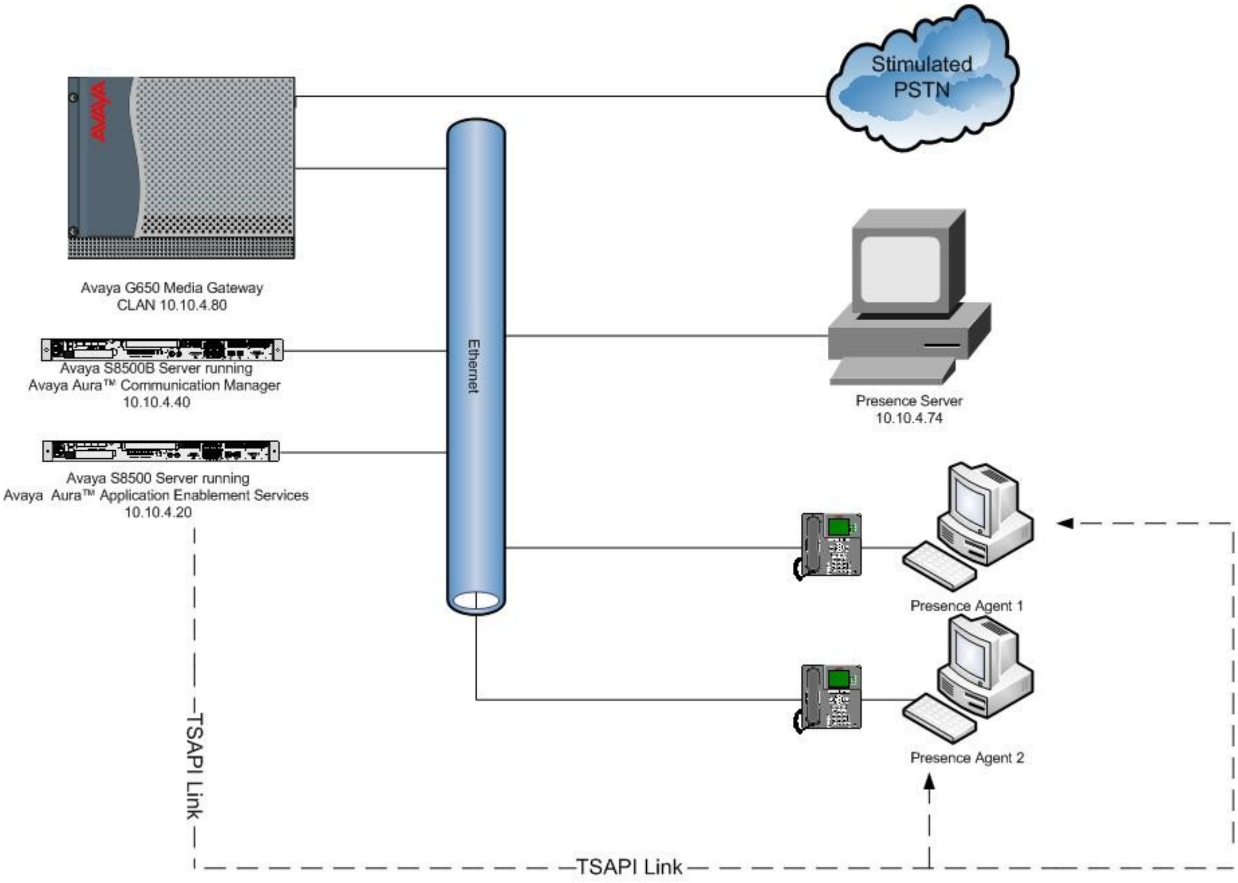


Figure 1: Network Topology

3 Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

Equipment	Software
Avaya S8500B Server running Avaya Aura^{TM} Communication Manager	5.2 (R015x.02.0.947.3-17534)
Avaya G650 Media Gateway - IPSI TN2312BP - CLAN TN799DP - IP Media Processor TN2602AP	 HW15, FM47 HW01, FM32 HW02, FM49
Avaya S8500B Server running Avaya Application Enablement Services	5.2 (Bld 98)
Avaya 96xx Telephones (H.323) - 9630	 3.0
Presence Suite Server	8.0
Operating System for Presence Agent PC's	Windows XP Professional 2002 SP3 Windows Vista Business

Table 1: Hardware and Software Version Numbers

4 Configure Communication Manager

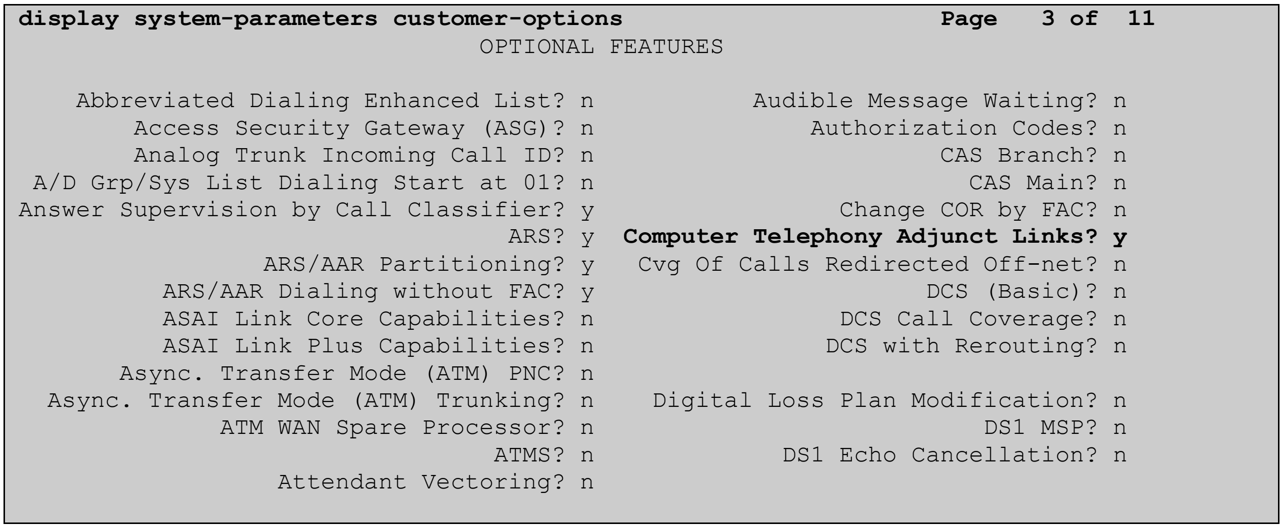
The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- Administer Trunk
- Administer SIT Treatment for Call Classification
- Administer Class of Restriction
- Administer CTI Link for TSAPI Service
- Configure Hunt Groups, Vectors and VDN's
- Administer Agent Logins
- Configure Agent Stations
- Administer Phantom Extensions
- Administer Direct Agent Transfer
- Configure Interface to Application Enablement Services

The configuration of the PRI interface to the PSTN is outside the scope of these Application Notes.

4.1 Verify System Parameters Customer Options

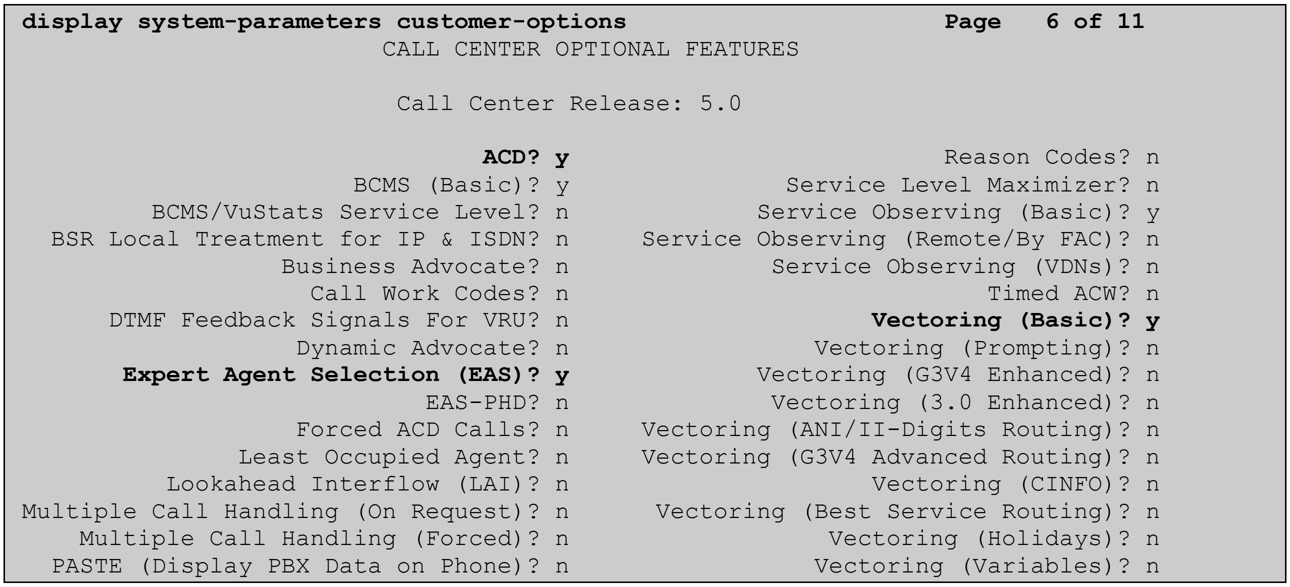
Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.



```
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? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? n
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? 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? n
                  Attendant Vectoring? n
```

On **Page 6**, verify the following customer options are set to **y** as shown below.

- **ACD?** to **y**
- **Vectoring (Basic)?** to **y**
- **Expert Agent Selection (EAS)?** to **y**



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

                          Call Center Release: 5.0

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

Use the command **display system-parameters features** for verification of feature parameters. On **Page 11**, verify that the **Expert Agent Selection (EAS) Enabled?** option is set to **y** as shown below.

```
display system-parameters features                              Page 11 of 17
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                     Delay:
    Message Waiting Lamp Indicates Status For: station
```

On **Page 13**, verify that **Call Classification After Answer Supervision** option is set to **y** as shown below.

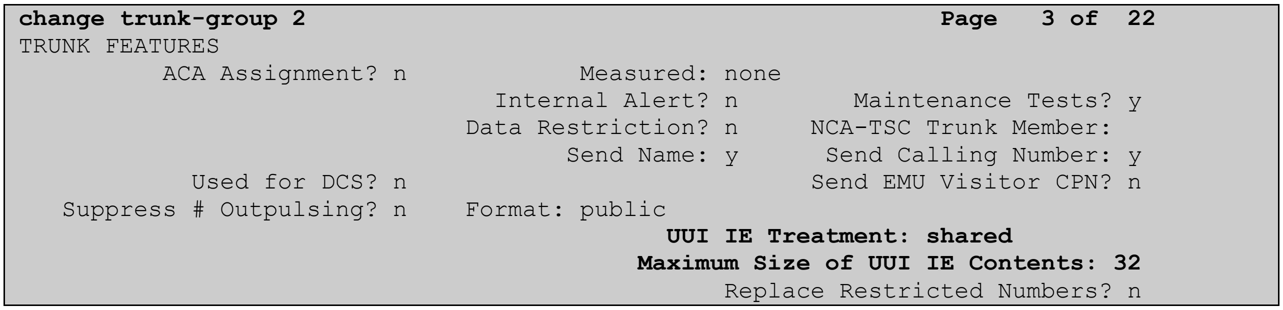
```
display system-parameters features                              Page 13 of 17
                        FEATURE-RELATED SYSTEM PARAMETERS

 CALL CENTER MISCELLANEOUS
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n


  ASAI
            Copy ASAI UUI During Conference/Transfer? n
        Call Classification After Answer Supervision? y
                                   Send UCID to ASAI? n
```

4.2 Administer Trunk

A trunk is set up for inbound and outbound campaign calls. Enter **change trunk group n** where **n** is the trunk group number for the pre-configured ISDN trunk which will be used for inbound and outbound campaign calls. It is assumed that the ISDN trunk and the corresponding signaling group are already configured. The trunk group number used in this case is **2**.

```
change trunk-group 2                                            Page   1 of  22
                                TRUNK GROUP

Group Number: 2                    Group Type: isdn         CDR Reports: y
  Group Name: Inbound                     COR: 1        TN: 1        TAC: 102
   Direction: two-way       Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? y             Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: public-ntwrk         Auth Code? n           TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
```

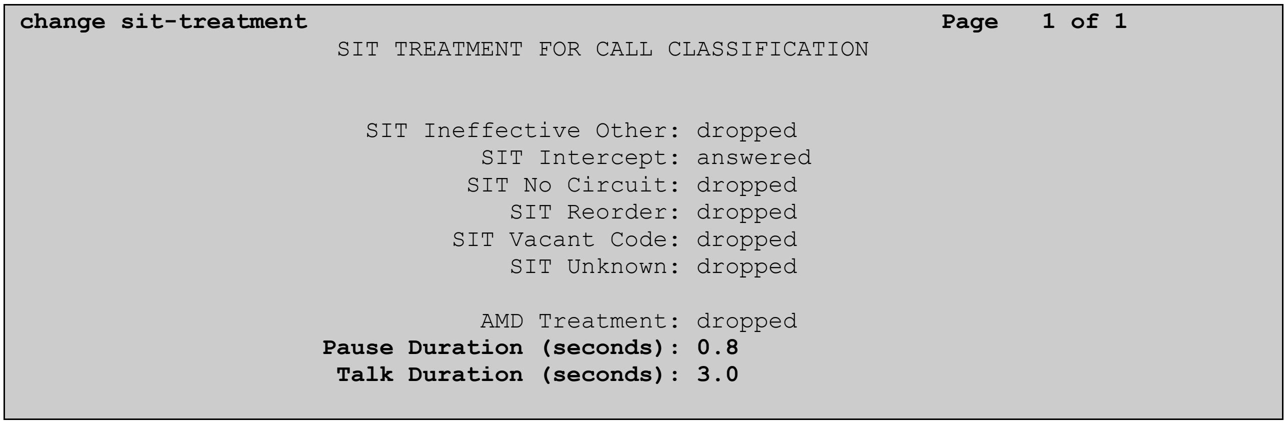
On **Page 3**, set the following values: **UUI IE Treatment** to **shared** and **Maximum Size of UUI IE Contents** to **32**. Default values may be used in the remaining fields.



```
change trunk-group 2                                            Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                 Internal Alert? n        Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: y      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: public
                                             UUI IE Treatment: shared
                                           Maximum Size of UUI IE Contents: 32
                                                 Replace Restricted Numbers? n
```

4.3 Administer SIT Treatment for Call Classification

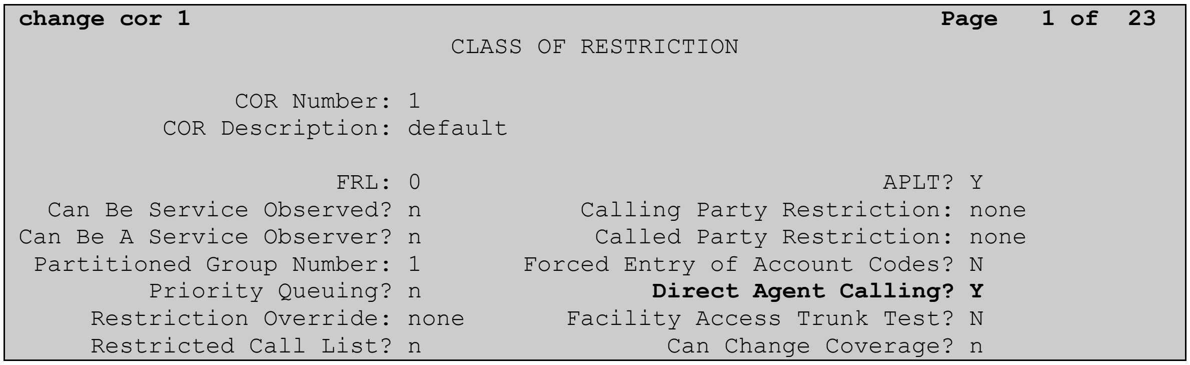
This form is used to specify the treatment of Special Information Tones (SITs) used for Outbound Call Management type calls with USA tone characteristics. Enter the **change sit-treatment** command. Set the **Pause Duration** to **0.8** and **Talk Duration** to **3.0**. Note the values are in seconds.



```
change sit-treatment                                            Page   1 of 1
                      SIT TREATMENT FOR CALL CLASSIFICATION


                        SIT Ineffective Other: dropped
                                SIT Intercept: answered
                               SIT No Circuit: dropped
                                  SIT Reorder: dropped
                              SIT Vacant Code: dropped
                                  SIT Unknown: dropped

                                AMD Treatment: dropped
                     Pause Duration (seconds): 0.8
                      Talk Duration (seconds): 3.0
```

4.4 Administer Class of Restriction

Enter the **change cor 1** command where **1** corresponds to the Class of Restriction assigned to the trunk in **Section 4.2**. On **Page 1**, set the **Direct Agent Calling** to **y**. This will allow agents to be called directly once they are logged in. The COR is also referenced in the agent logins.



```
change cor 1                                                    Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description: default

                      FRL: 0                                APLT? Y
  Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n            Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? N
         Priority Queuing? n                Direct Agent Calling? Y
     Restriction Override: none       Facility Access Trunk Test? N
     Restricted Call List? n                 Can Change Coverage? n
```

4.5 Administer CTI Link with TSAPI Service

Enter **add cti-link n** command where **n** is an available CTI link number. The CTI link number chosen is **10.** Enter an available extension number in the **Extension** field. The **Type** must be set to **ADJ-IP** and enter a descriptive name in the **Name** field in this case **CtiLink1**. The link number specified must be the same value that is used in the **Add / Edit TSAPI Links** configuration screen shown in **Section 5.3** of this document.

```
add cti-link 10                                               Page   1 of   3
                                                 CTI LINK
 CTI Link: 10
Extension: 5002
Type: ADJ-IP
                                                                         COR: 1
     Name: CtiLink1
```

4.6 Administer Hunt Groups, Call Vectors and VDNs

Administer a set of hunt groups, vectors and Vector Directory Numbers (VDNs) per Presence Suite installation documentation. VDNs and vectors were created to allow external calls to be handled by the Presence Suite server. There were five groups of services set up for the purpose of the testing as follows:

- Inbound Service
- Outbound Service (Progressive, Predictive)
- Email Service
- Suspended
- Web Chat & Web Callback Service

Below is a table of the configuration of the VDNs, Vectors, Hunt groups and Agent Login IDs which was set up for the different campaigns for the purpose of the compliance testing.

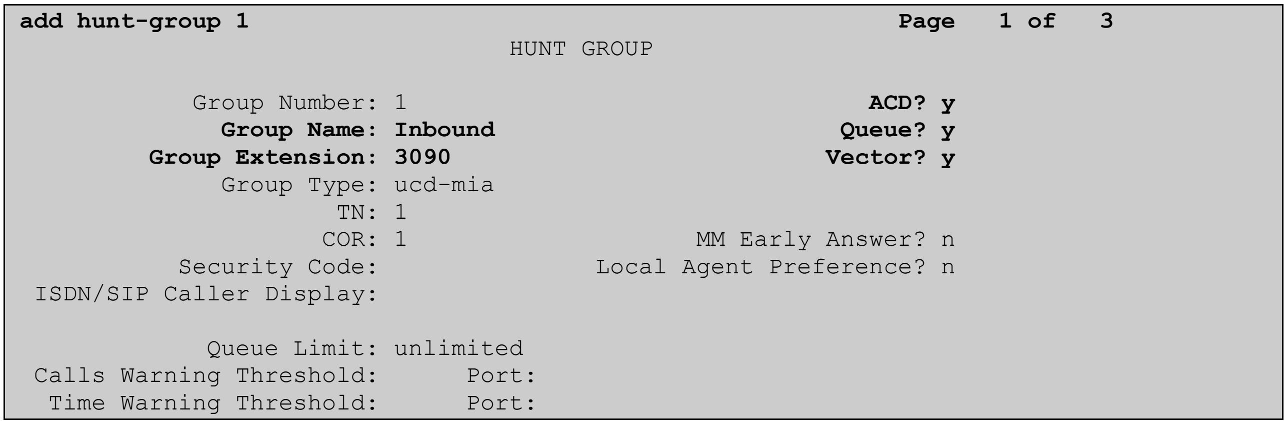
	Inbound	**Outbound**	**Email**	**Suspended**	**Web Chat & Callback**	**Direct Agent**
VDN	1800	1810	1820	1830	1840	1850
VECTOR	1	2	3	4	5	6
SKILL EXT\HUNT GROUP	3090/1	3091/2	3092/3	3093/4	3094/5	
AGENT LOGINS	6001 6005	6002 6006	6003		6004	
Notes		Auto-answer = all		No agent		

Table 2: Test Agent Details

4.6.1 Hunt Groups

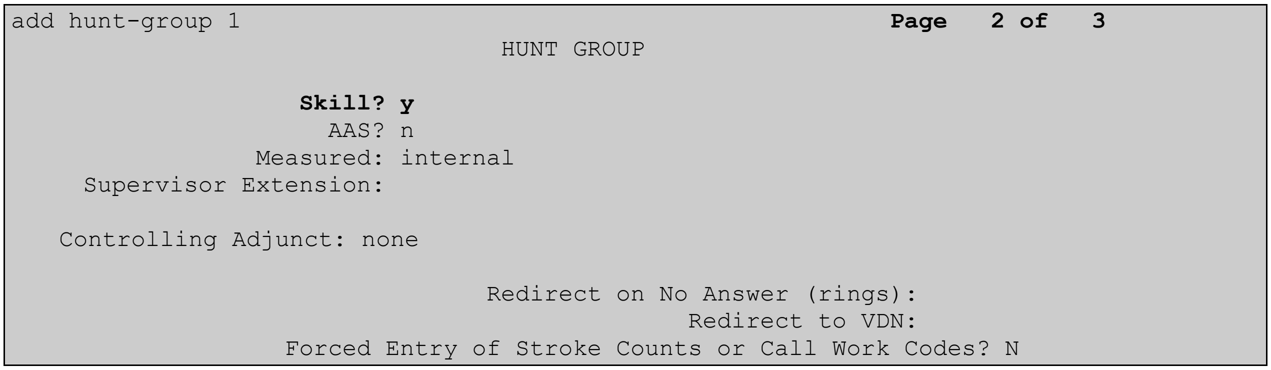
Enter the **add hunt-group n** command where **n** is an unused hunt group number. On **Page 1** of the **hunt group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to **y** as shown below.

- **ACD** to **y**
- **Queue** to **y**
- **Vector** to **y**



```
add hunt-group 1                                             Page   1 of   3
                                  HUNT GROUP

            Group Number: 1                                ACD? y
              Group Name: Inbound                        Queue? y
         Group Extension: 3090                          Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

On **Page 2**, set the **Skill** field to **y** as shown below.



```
add hunt-group 1                                             Page   2 of   3
                                  HUNT GROUP

                    Skill? y
                      AAS? n
                 Measured: internal
     Supervisor Extension:

   Controlling Adjunct: none

                                 Redirect on No Answer (rings):
                                               Redirect to VDN:
                   Forced Entry of Stroke Counts or Call Work Codes? N
```

Repeat the above step and create four more hunt groups with hunt-group extensions 3091 to 3094. The following figure lists **hunt-group** after the five hunt-groups are administered.

```
list hunt-group
                                HUNT GROUPS
Grp  Grp
No.  Name/           Grp     ACD/              No. Cov  Notif/  Dom   Message
     Ext             Type    MEAS Vec MCH  Que Mem Path Ctg Adj Ctrl  Center

1    HG Inbound
     3090            ucd-mia y/N  SK  none y   0        n             n
2    HG Outbound
     3091            ucd-mia y/N  SK  none y   0        n             n
3    HG Email
     3092            ucd-mia y/N  SK  none y   0        n             n
4    HG SuspEmail
     3093            ucd-mia y/N  SK  none y   0        n             n
5    HG WebCallBack
     3094            ucd-mia y/N  SK  none y   0        n             n
```

4.6.2 Vectors

Enter the **change vector n** command, where **n** is set to **1**. Enter the vector steps to queue to the **Skill 1** as shown below.

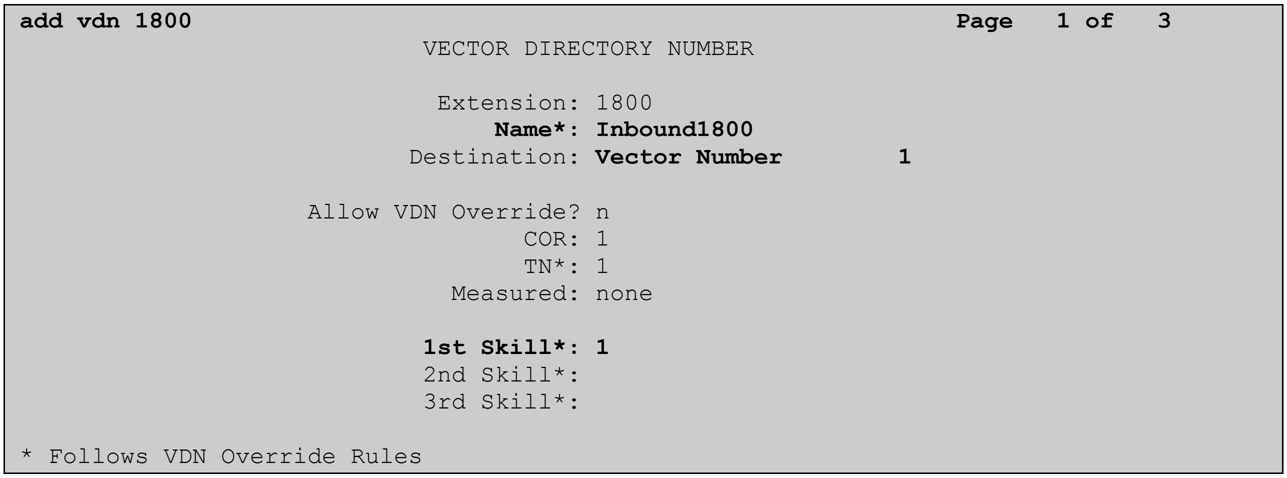
```
change vector 1                                              Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: Inbound
Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? y
 Prompting? n   LAI? n  G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
 Variables? n   3.0 Enhanced? n
01 queue-to     skill 1  pri m
02 wait-time    5   secs hearing silence
03 disconnect   after announcement none
04 stop
05
```

Repeat the above step and configure four more vectors. These vectors will queue the agents to the skills described earlier. Refer to **Table 2** in **Section 4.5**. The following figure lists the vectors after all the vectors are administered.

```
list vector

                                 CALL VECTORS

                               Vector      Name
                               1           Inbound
                               2           Outbound
                               3           Email
                               4           SuspEmail
                               5           WebCallBacK
```

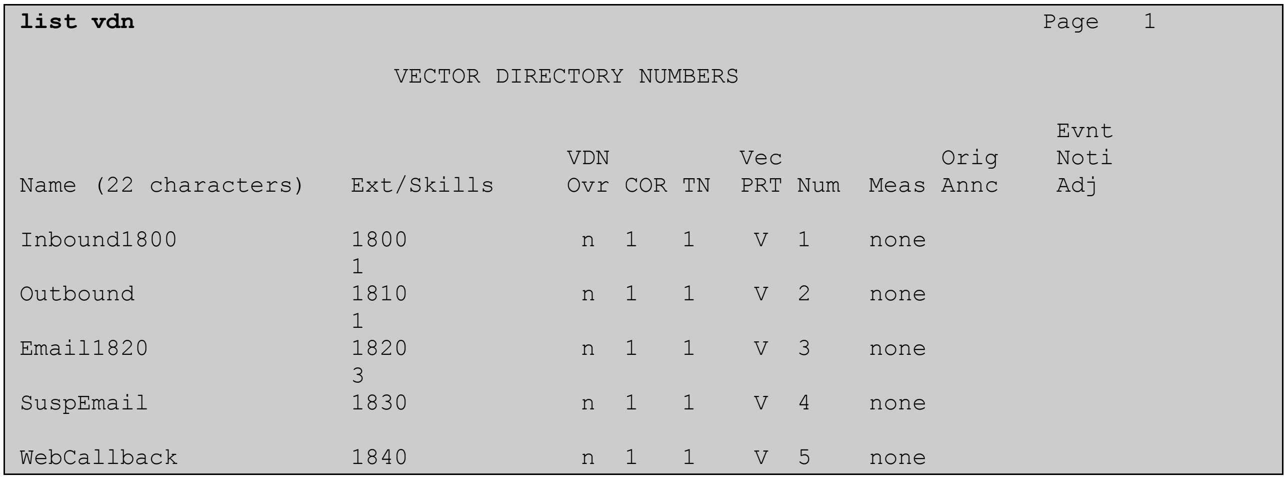
4.6.3 Vector Directory Number (VDN)

Enter the **add vdn n** command, where **n** is an unused VDN number. The VDN chosen is **1800**. On **Page 1** assign a **Name** for the VDN, **Vector Number** as **1** and **1st Skill** to **1**.



```
add vdn 1800                                                     Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 1800
                                 Name*: Inbound1800
                           Destination: Vector Number        1

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

                            1st Skill*: 1
                            2nd Skill*:
                            3rd Skill*:

* Follows VDN Override Rules
```

Repeat the above step and create four more VDNs. These VDNs, vectors and skills created were used for the different types of campaigns during compliance testing. The following figure lists the VDNs after the above administration is completed.

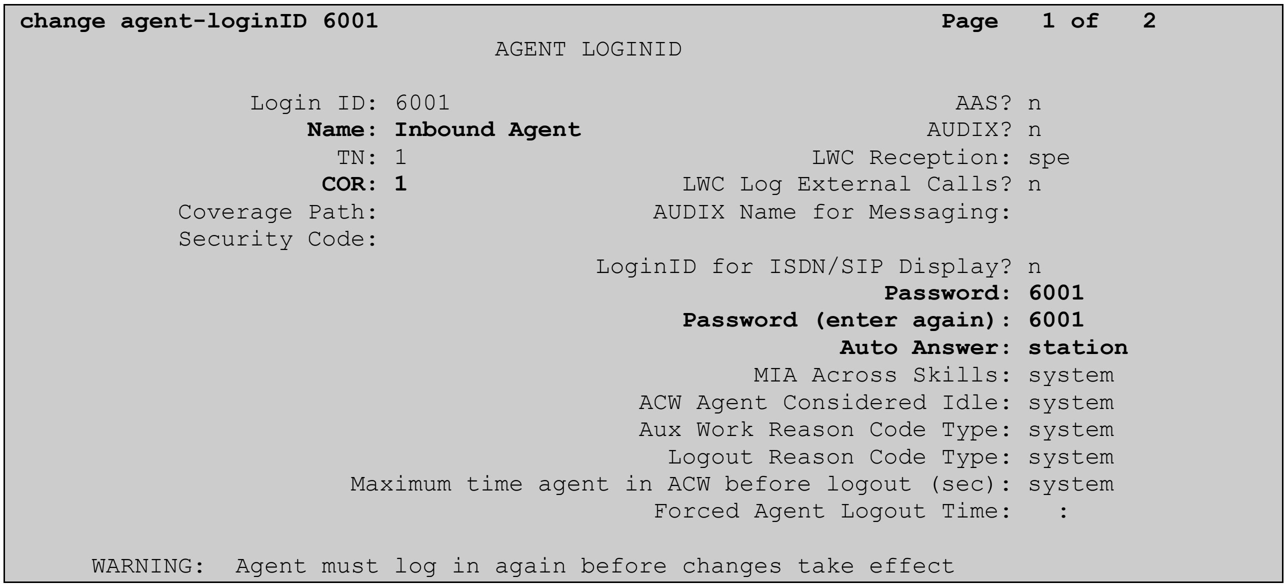


```
list vdn                                                               Page   1

                          VECTOR DIRECTORY NUMBERS

                                                                        Evnt
                                      VDN         Vec           Orig    Noti
Name  (22 characters)  Ext/Skills     Ovr COR TN  PRT Num  Meas Annc    Adj

Inbound1800            1800            n  1   1    V  1    none
                       1
Outbound               1810            n  1   1    V  2    none
                       1
Email1820              1820            n  1   1    V  3    none
                       3
SuspEmail              1830            n  1   1    V  4    none

WebCallback            1840            n  1   1    V  5    none
```

The configuration of Vector 6 and VDN 1850 for Direct Agent Transfer will be covered later in **Section 4.10**.

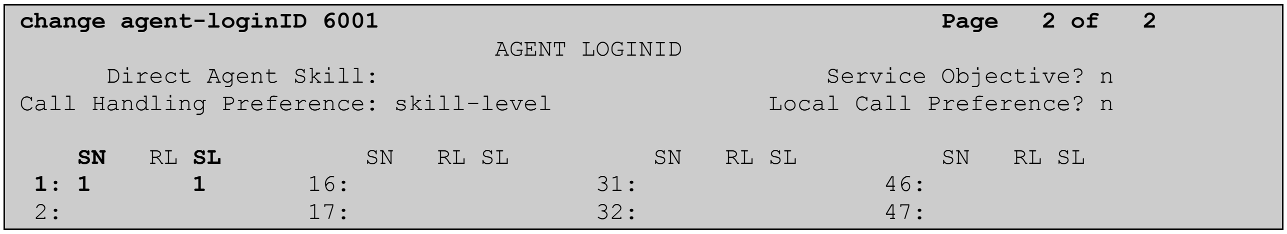
4.7 Administer Agent Logins

Enter the **add agent-loginID n** command; where **n** is a valid extension under the provisioned dial plan. The agent loginID chosen is **6001** and the **Password** is set to **6001**. Enter a descriptive name for the agent in the **Name** field. Ensure the **COR** field is set to **1** which relates to the COR configured in **Section 4.5**. The default value for **Auto Answer** is set to **station**, except for those logins that will be used for progressive/predictive outbound services. In that case, the parameter value will be set to **all**.



```
change agent-loginID 6001                                       Page   1 of   2
                                 AGENT LOGINID

                Login ID: 6001                                   AAS? n
                    Name: Inbound Agent                        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: 6001
                                              Password (enter again): 6001
                                                         Auto Answer: station
                                                   MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :

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

On **Page 2**, specify the list of skills assigned to the login and the skill level for each of them in the **SN/SL** field as shown below. In this case set the Skill Number, **SN** to **1** and the Skill Level, **SL** to **1**.



```
change agent-loginID 6001                                       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           SN   RL SL           SN   RL SL
 1: 1       1       16:                 31:                 46:
 2:                 17:                 32:                 47:
```

Six agent loginID's were created for the different types of campaigns during compliance testing. This can be shown by entering a **list agent-loginID** command as shown below.

```
list agent-loginID

                               AGENT LOGINID

Login         Name/           Dir Agt COR Ag SO Skil/Lv Skil/Lv Skil/Lv Skil/Lv
ID            Extension       AAS/AUD     Pr

6001          Inbound Agent           1   lvl      1/01     /       /       /
              unstaffed                             /       /       /       /
6002          Outbound Agent          1   lvl      2/02     /       /       /
              unstaffed                             /       /       /       /
6003          Email Agent             1   lvl      3/01     /       /       /
              unstaffed                             /       /       /       /
6004          WebCall Agent           1   lvl      5/01     /       /       /
              unstaffed                             /       /       /       /
6005          InBound Agent2          1   lvl      5/01     /       /       /
              unstaffed                             /       /       /       /
6006          Outbound Agent2         1   lvl      2/02     /       /       /
              unstaffed                             /       /       /       /
```

4.8 Configure Agent Stations

A number of stations were set up and used as agent phones during the compliance testing. The station configuration is not given as it is assumed that they are already administered on Communication Manager. The following buttons were assigned to each agent station as shown below. Enter the command **change station n,** where **n** is the agent phone extension.
On **Page 4** of the station form, configure the following button assignments:

- **aux-work** – Agent is logged in to the ACD but is not available to take a call.
- **manual-in** – Agent is available to accept ACD calls.
- **after-call** – Agent state after the ACD call is completed. The agent is not available.
- **release** – State when the call is dropped.

```
change station 3000                                             Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                             Headset? n
       Jack:                                             Speaker? n
      Cable:  SITE                                      Mounting: d
      Floor:                                         Cord Length:  1
   Building:                                           Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                          5: manual-in         Grp:
 2: call-appr                          6: after-call        Grp:
 3: call-appr                          7: release
 4: aux-work    RC:    Grp:            8:

    voice-mail Number:
```

Feature Access Codes are added for each of the button assignments above on the Communication Manager. Enter the command **change feature-access-codes** and on **Page 5** add codes to the Automatic Call Distribution Features:

After Call Work Access Code	**#8**
Auto-In Access Code	**#2**
Aux Work Access Code	**#4**
Login Access Code	**#6**
Logout Access Code	**#5**
Manual-in Access Code	**#7**

```
change feature-access-codes                                    Page   5 of   8
                              FEATURE ACCESS CODE (FAC)

                        Automatic Call Distribution Features

                    After Call Work Access Code: #8
                             Assist Access Code:
                            Auto-In Access Code: #2
                           Aux Work Access Code: #4
                              Login Access Code: #6
                             Logout Access Code: #5
                          Manual-in Access Code: #7
      Service Observing Listen Only Access Code:
      Service Observing Listen/Talk Access Code:
          Service Observing No Talk Access Code:
                    Add Agent Skill Access Code:
                 Remove Agent Skill Access Code:
             Remote Logout of Agent Access Code:
```

4.9 Administer Phantom Extensions

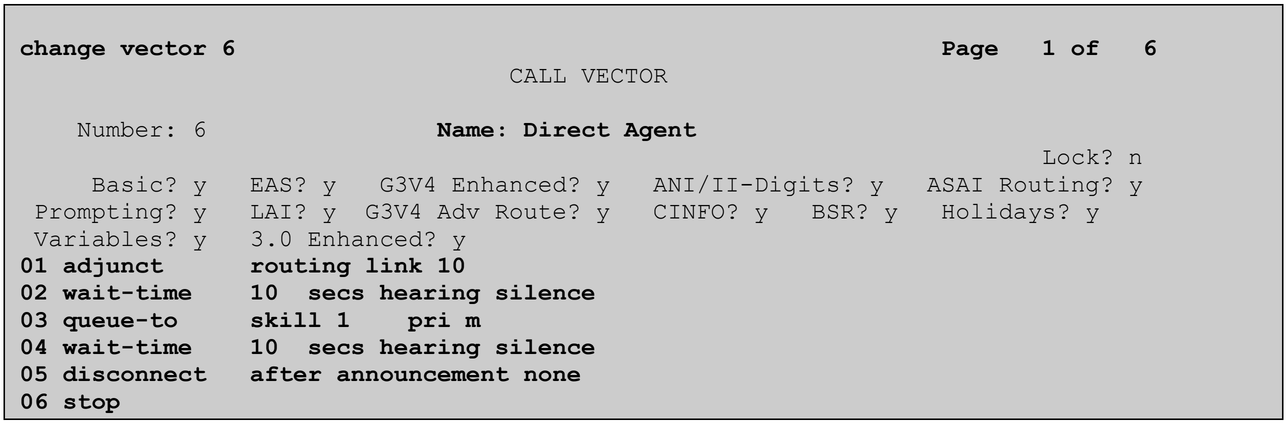
Extensions 3500 and 3510 were created as phantom extensions for outbound preview campaign calls. The configuration for the first of these stations is shown below using the **add station n** command. The station added is **3500** and is named **Phantom1**.

- **Type**: This is set to **CTI**
- **Port**: This is set to **X** (indicates that this is a virtual port)
- **COR**: This is set to **1**

```
add station 3500                                            Page   1 of   5
                                     STATION

Extension: 3500                         Lock Messages? n              BCC: 0
     Type: CTI                          Security Code:                 TN: 1
     Port: X                          Coverage Path 1:                COR: 1
     Name: Phantom1                   Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 1         Personalized Ringing Pattern: 1
             Data Module? n                     Message Lamp Ext: 3500
          Display Module? n

          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y
```

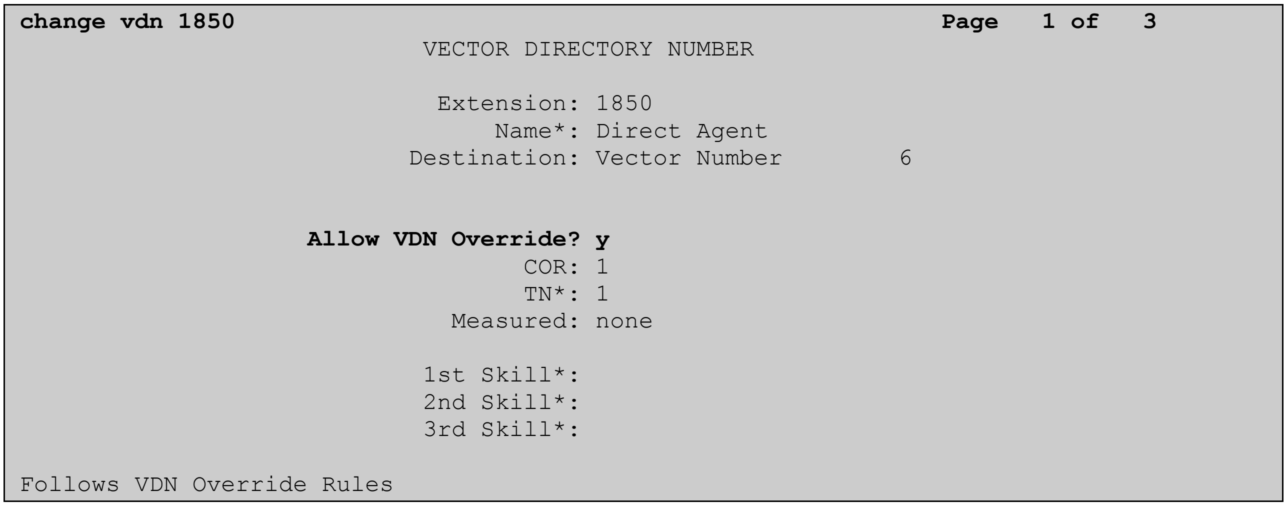
4.10 Administration for Direct Transfer to Agents and Call Capturing

Vector 6 and VDN 1850 are configured for two additional Presence features; Direct Transfer to agents and Call Capturing**.** Direct Agent Calling (DAC) is an Expert Agent Selection (EAS) feature within Communication Manager that allows a call to route directly to the ACD agent. Enter the command **change vector 6.** Set the **Name** as **Direct Agent**. The CTI link configured in **Section 4.5** used by the Presence Server needs to be specified in the vector line 1 (i.e., **01 adjunct routing link 10)**. Line 1 passes control of the call over to the Presence Server so that the Presence Server may transfer it to a specific agent. Lines 3, 4 and 5 provide treatment to the call in case of an unsuccessful routing of the call by the adjunct link.



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

    Number: 6                Name: Direct Agent
                                                                       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 adjunct      routing link 10
02 wait-time    10  secs hearing silence
03 queue-to     skill 1    pri m
04 wait-time    10  secs hearing silence
05 disconnect   after announcement none
06 stop
```

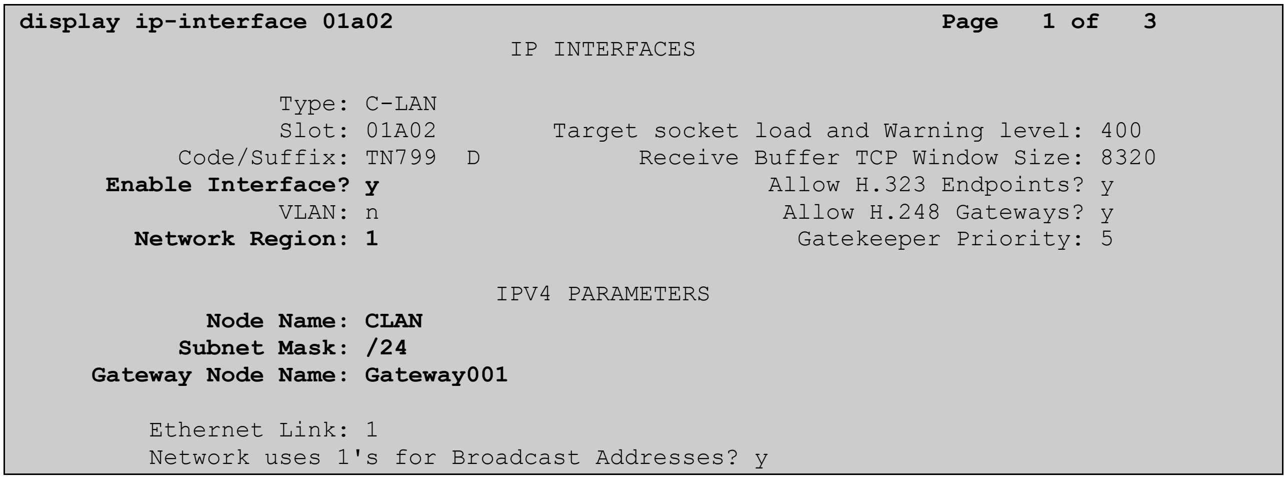
Enter the **change vdn 1850** command. On **Page 1** of the vector directory number form, set the **Allow VDN Override** to **y**. This VDN is used to configure the Direct Agent Transfer.



```
change vdn 1850                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 1850
                                 Name*: Direct Agent
                           Destination: Vector Number        6


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

                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:

Follows VDN Override Rules
```

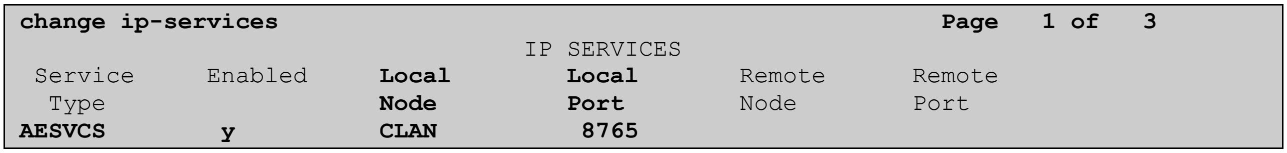
4.11 Configure Interface to Application Enablement Services

The Application Enablement Services server has a TSAPI interface which provides Presence Suite with a means of communicating with Communication Manager to perform telephony operations. Communication Manager requires the configuration parameters shown in this section. Use the **add ip-interface** command to allocate a call control interface. The slot value specified should be the CLAN interface. On **Page 1** the **Node Name** is set to **CLAN** which is defined by the **change node-names ip** command. The **Subnet Mask** and **Gateway Node Name** should be assigned to the values used by the Ethernet network to which the CLAN is attached. The **Enable Interface** is set to **y** and the **Network Region** is set to **1**.



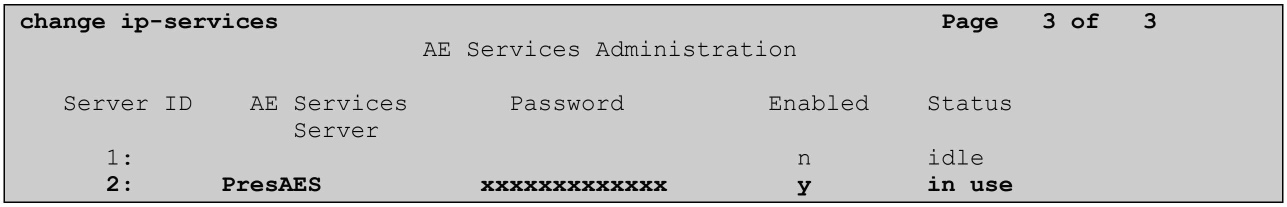
```
display ip-interface 01a02                                          Page   1 of   3
                                  IP INTERFACES

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

                                 IPV4 PARAMETERS
             Node Name: CLAN
           Subnet Mask: /24
     Gateway Node Name: Gateway001

         Ethernet Link: 1
         Network uses 1's for Broadcast Addresses? y
```

Use the **change ip-services** command to set the parameters for **AESVCS** service for the CLAN as shown below. This was defined above to serve as the interface to the Application Enablement Services server. On **Page 1** add **CLAN** as the **Local Node** and accept default of **8765** as **Local Port.**



```
change ip-services                                                  Page   1 of   3
                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y          CLAN          8765
```

On **Page 3**, an entry for the Application Enablement Services server must be made in the list in the screen shown below. The name assigned to the Application Enablement Services server when it was installed must be entered in the **AE Services Server** field for that entry. The **Password** entry must the same as that assigned to the switch connection, as shown in **Section 5.2** of this document.



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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:                                               n        idle
      2:      PresAES           xxxxxxxxxxxxx          y        in use
```

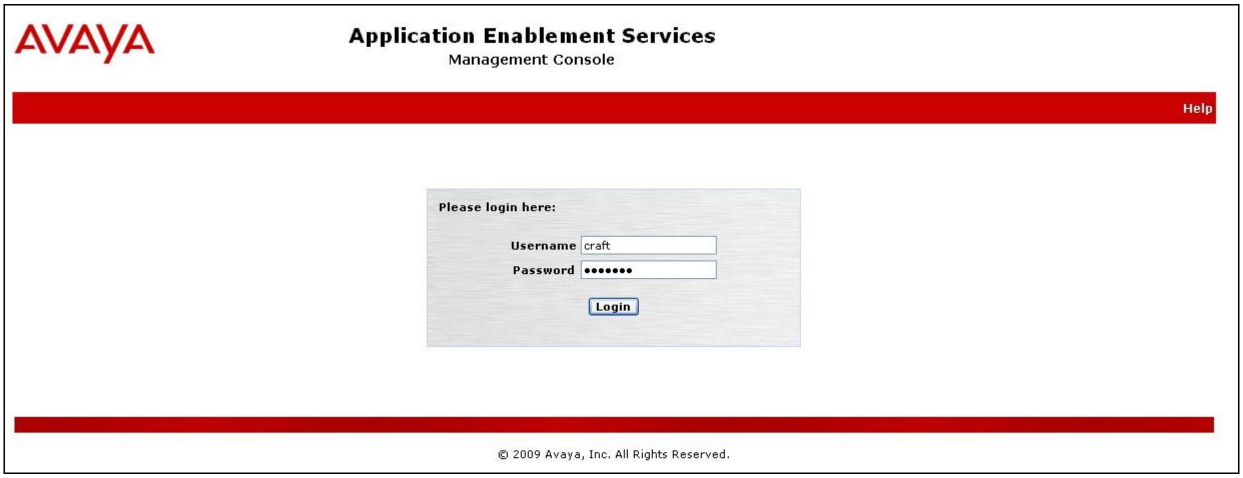
5 Configure Application Enablement Services Server

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable CTI Link User
- Identify Tlinks

5.1 Verify Licensing

Initialize the Application Enablement Services OAM web interface by browsing to http://x.x.x.x, where "x.x.x.x" is the IP address of the Application Enablement Services. Log in as in the screen below.


AVAYA
Application Enablement Services
Management Console
Help

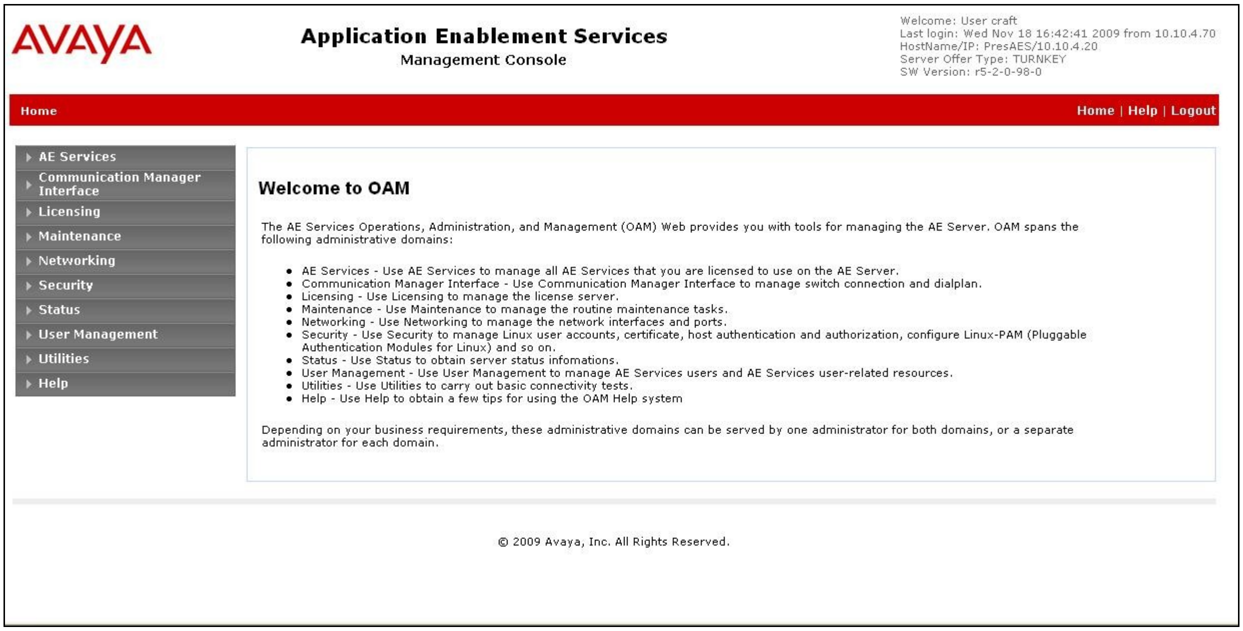
Please login here:

Username craft

Password •••••••

Login
© 2009 Avaya, Inc. All Rights Reserved.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen.



Welcome: User craft
Last login: Wed Nov 18 16:42:41 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Welcome to OAM

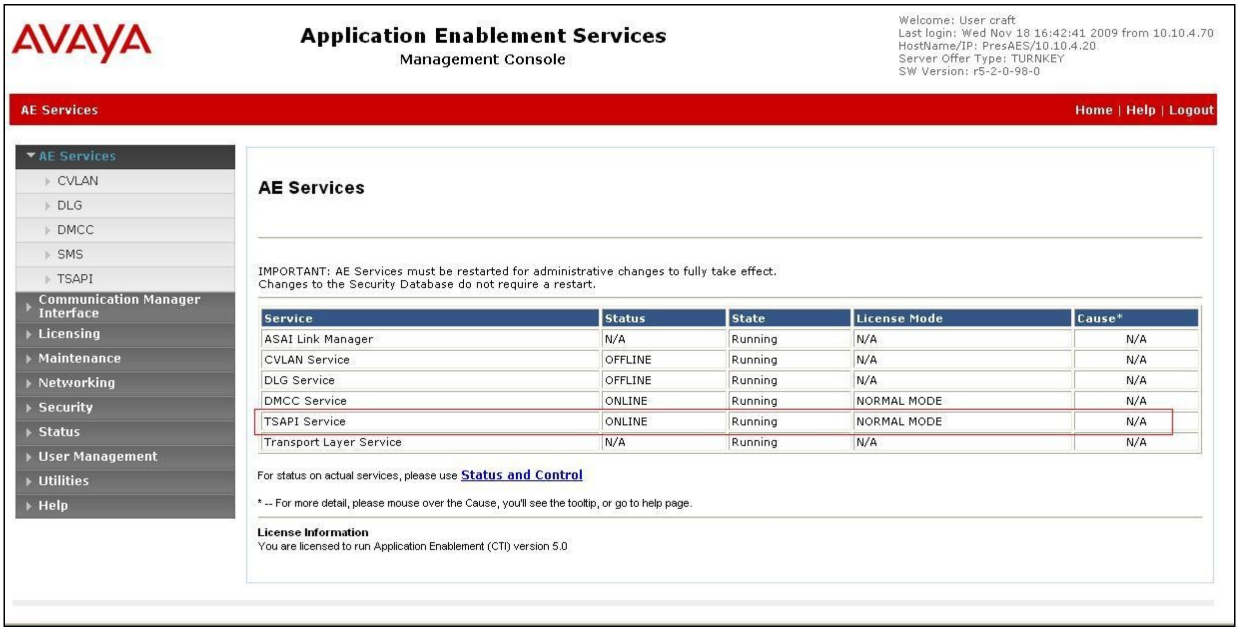
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.



Welcome: User craft
Last login: Wed Nov 18 16:42:41 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
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	OFFLINE	Running	N/A	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

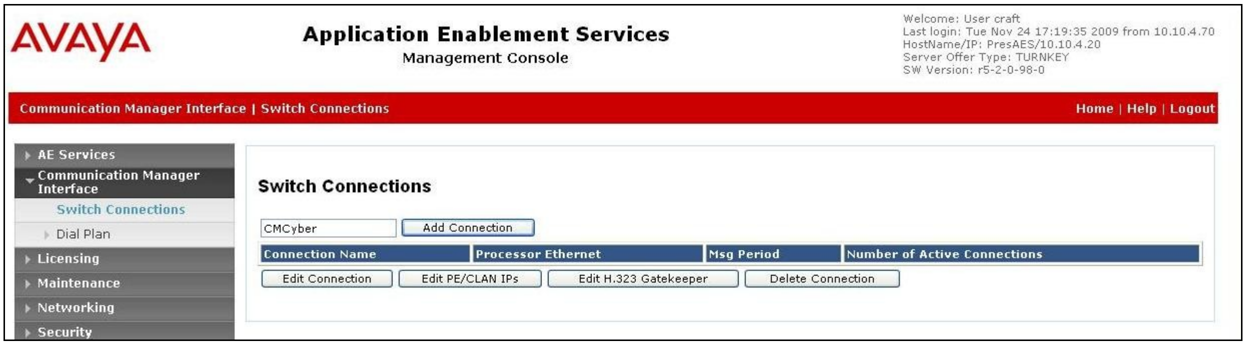
For status on actual services, please use **Status and Control**

* -- 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

5.2 Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface → Switch Connections** to set up a switch connection. Enter in the name of the Switch Connection to be added and click on the **Add Connection** button.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections

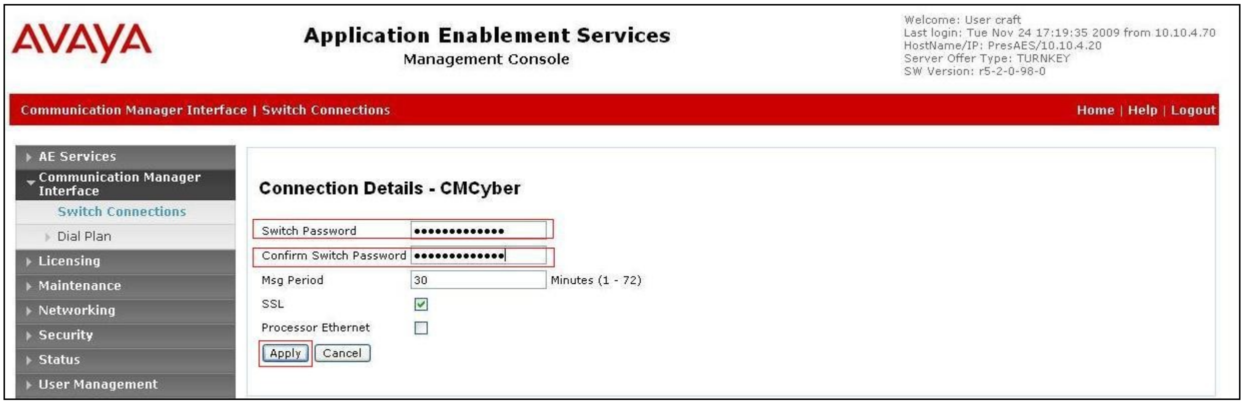
Switch Connections

CMCyber

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

A second screen is displayed as shown below. Enter the screen fields as described below and click the **Apply** button.

- **Switch Password:** The Switch Password must be the same as that entered into Communication Manager AE Services screen via the **change ip-services** command, described in **Section 4.11**.
- **SSL:** This is enabled.



Application Enablement Services
Management Console

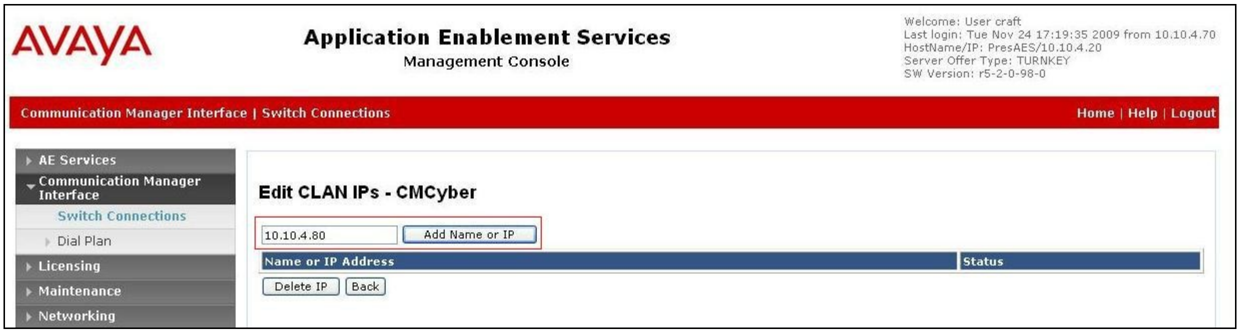
Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections

Connection Details - CMCyber

Switch Password	••••••••••••••
Confirm Switch Password	••••••••••••••
Msg Period	30 Minutes (1 - 72)
SSL	☑
Processor Ethernet	□

The CLAN IP address must then be set on the Application Enablement Services. From the **Communication Manager Interface → Switch Connections** screen (not shown), click the **Edit CLAN IPs** button. Enter the IP address of the CLAN which the Application Enablement Services is to use for communication with Communication Manager as defined in **Section 4.11**. Click the **Add Name or IP** button.

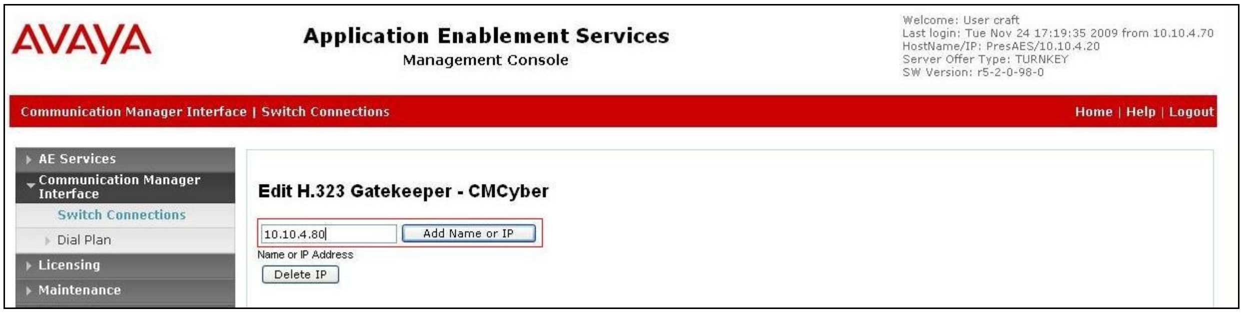

AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Add Name or IP
Delete IP
Back

Edit CLAN IPs - CMCyber

10.10.4.80

Name or IP Address	Status

The H.323 Gatekeeper should be set up to point to the CLAN address on Communication Manager. Navigate to **Communication Manager Interface → Switch Connection → Edit H323 Gatekeeper** to display the screen below. Enter the IP Address and click **Add Name or IP** button as shown below.


AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Add Name or IP
Delete IP

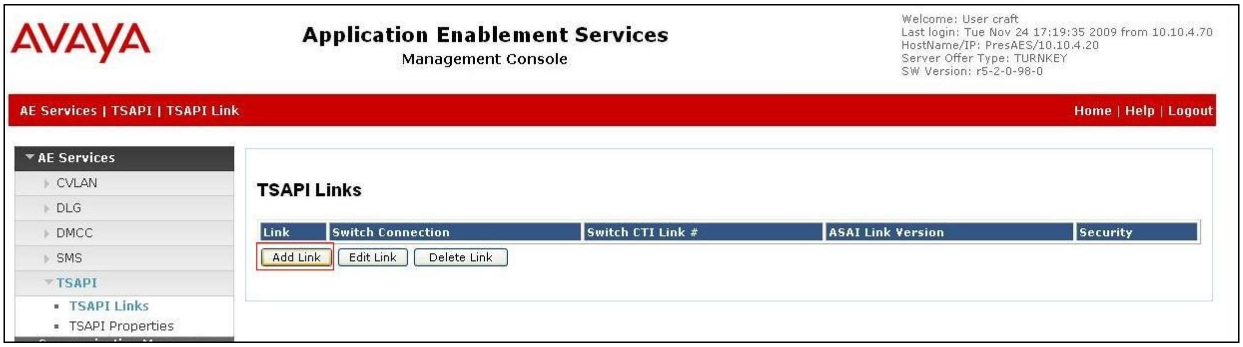
Edit H.323 Gatekeeper - CMCyber

10.10.4.80

Name or IP Address

5.3 Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.


AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
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
Add Link
Edit Link
Delete Link

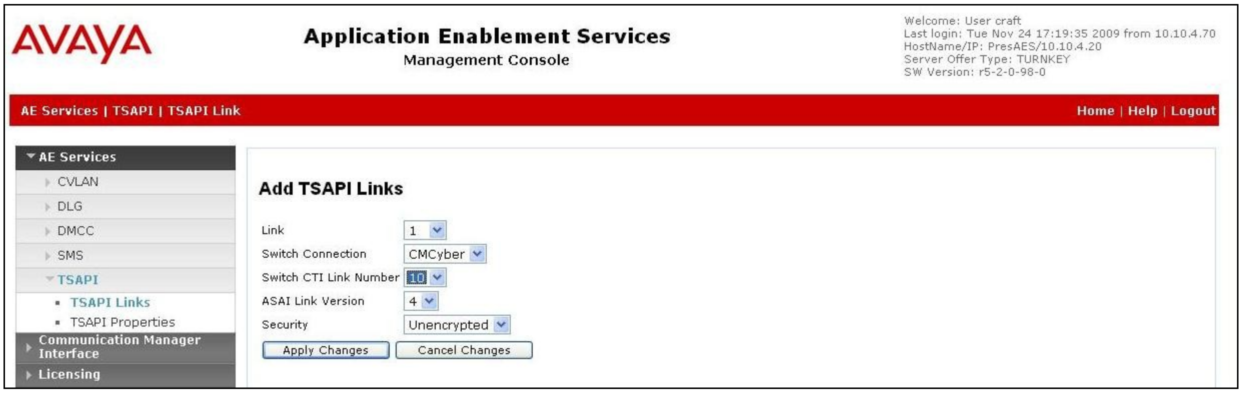
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

On the **Add TSAPI Links** screen, enter the following values:

- **Link** Use the drop-down list to select an unused link number.
- **Switch Connection** Choose the switch connection **CMCyber**, which has already been configured in **Section 5.2**, from the drop-down list.
- **Switch CTI Link Number** Corresponding CTI link number configured in **Section 4.5** which is **10**.
- **ASAI Link Version** This can be left at the default value of **4**.
- **Security: Unencrypted** is the option chosen for this compliance test.

Once completed, select **Apply Changes**.

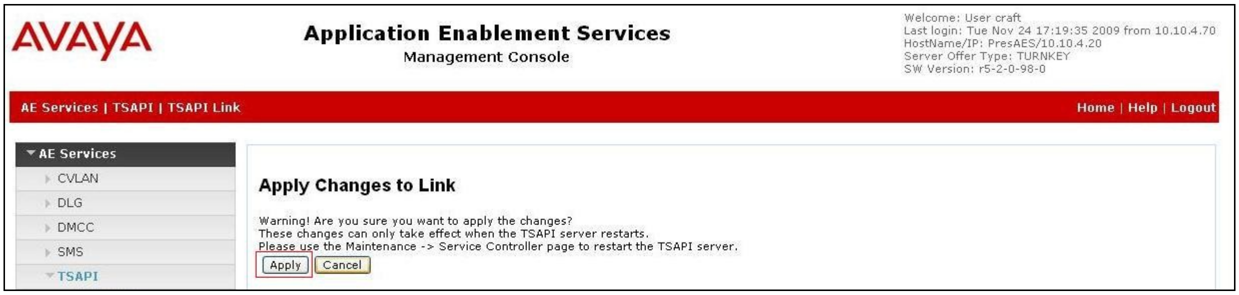


Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Add TSAPI Links

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

Another screen appears for confirmation of the changes. Choose **Apply**.

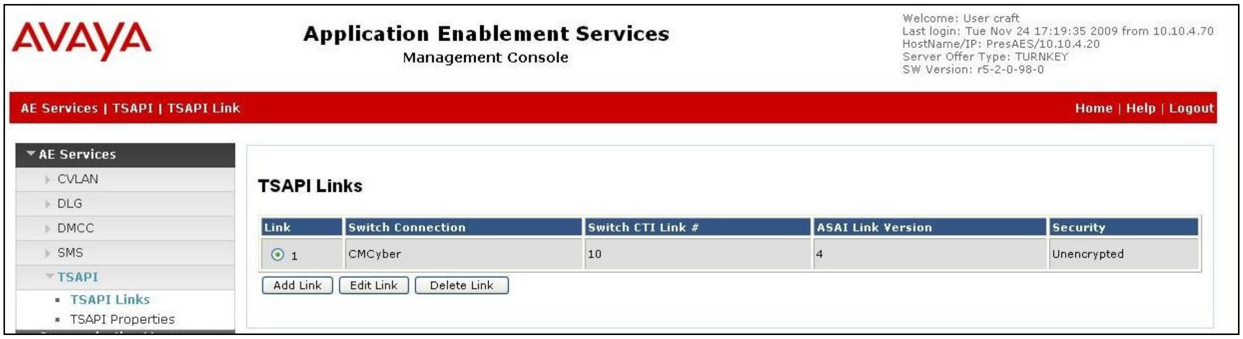


Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
Please use the Maintenance -> Service Controller page to restart the TSAPI server.

When the TSAPI Link is completed it is displayed as in the screen below.

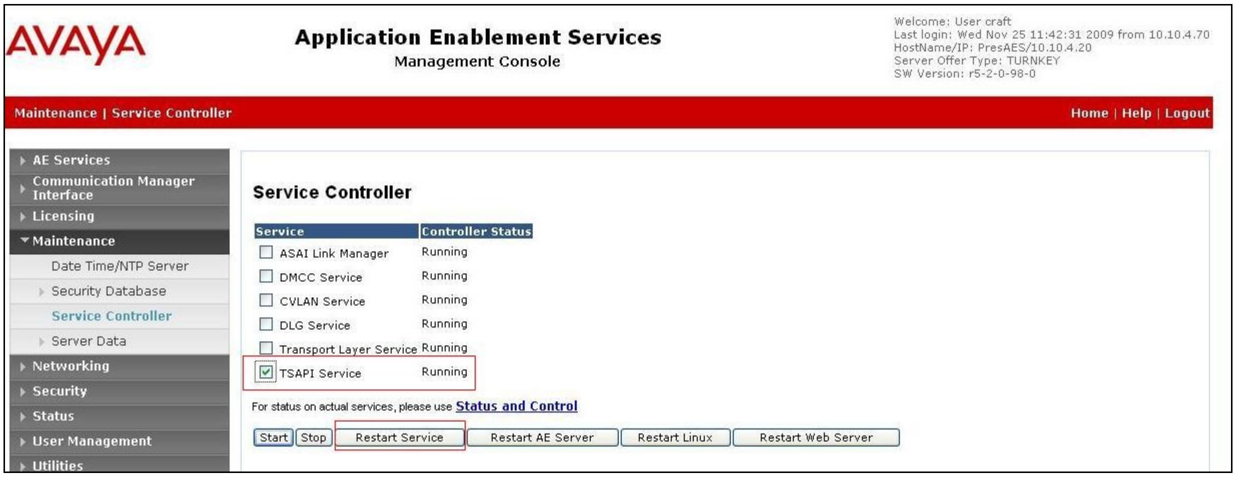


Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	CMCyber	10	4	Unencrypted

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, select **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Nov 25 11:42:31 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Maintenance | Service Controller

Service Controller

Service	Controller Status
☐ ASAI Link Manager	Running
☐ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

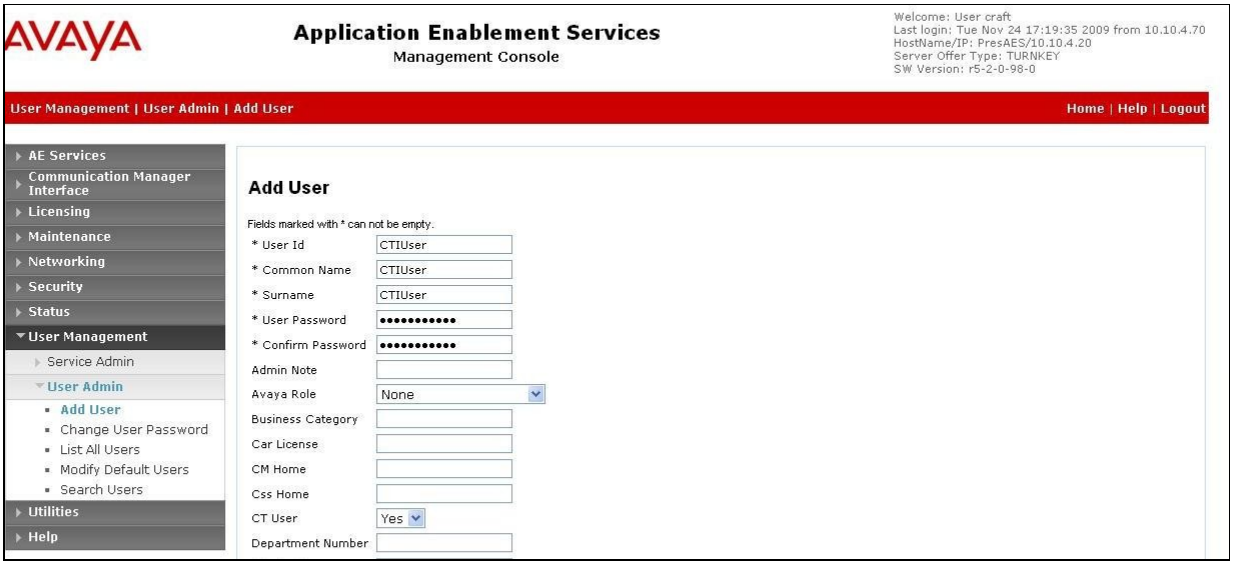
For status on actual services, please use Status and Control

5.4 Create Avaya CTI User

User ID and password needs to be configured for the Presence Suite server to communicate as a TSAPI Client with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option. In the **Add User** screen shown below, enter the following values:

- **User Id -** This will be used by the Presence Suite Server in **Section 6.**
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with the **User Id** in **Section 6**.
- **CT User -** Select **Yes** from the drop-down menu.

Complete the process by choosing the **Apply** at the bottom of the screen (not shown).



Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Nov 24 17:19:35 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

User Management | User Admin | Add User

Add User

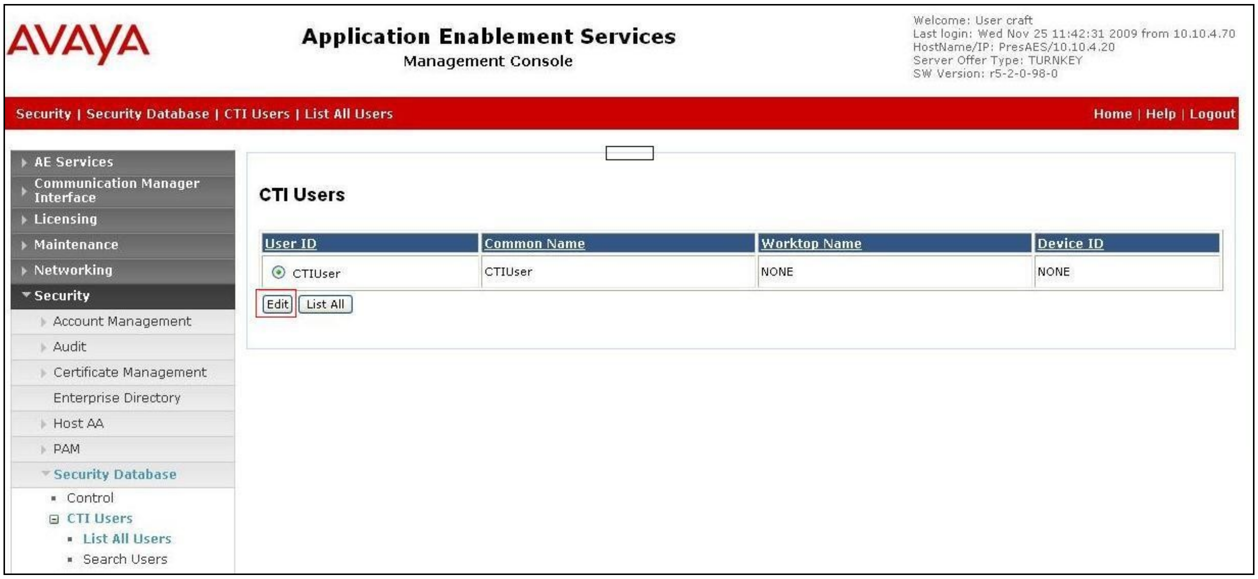
Fields marked with * can not be empty.

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

The next screen will show a message indicating that the user was created successfully (not shown).

5.5 Enable CTI Link User

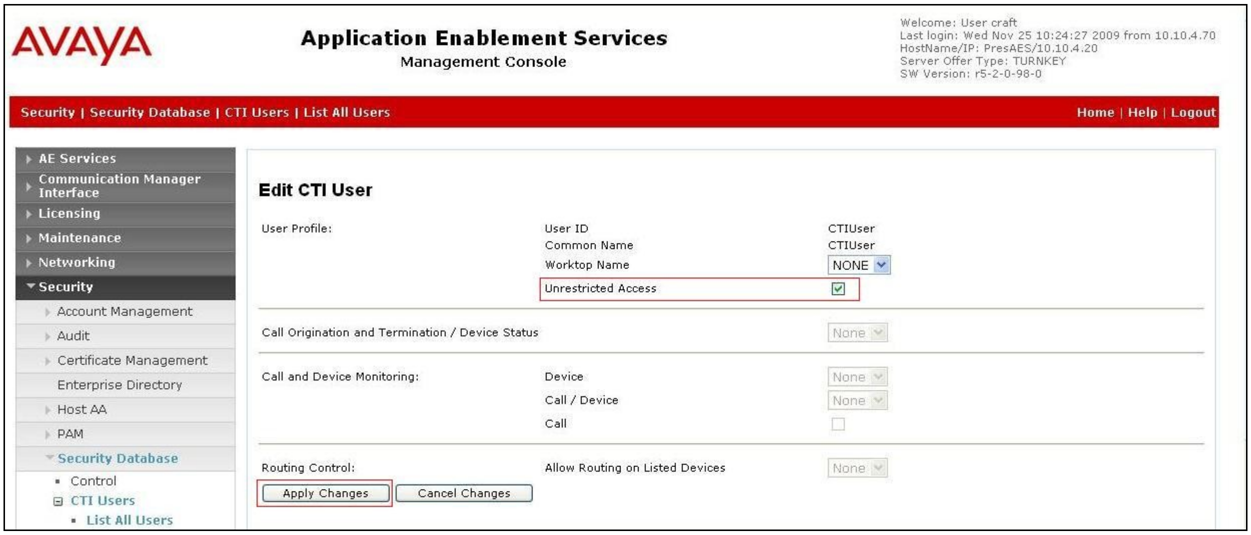
Navigate to the **CTI Users** screen by selecting **Security → Security Database → CTI Users → List All Users**. Select the user that was set up in **Section 5.4** and select the **Edit** option.



CTI Users

User ID	Common Name	Worktop Name	Device ID
● CTIUser	CTIUser	NONE	NONE

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



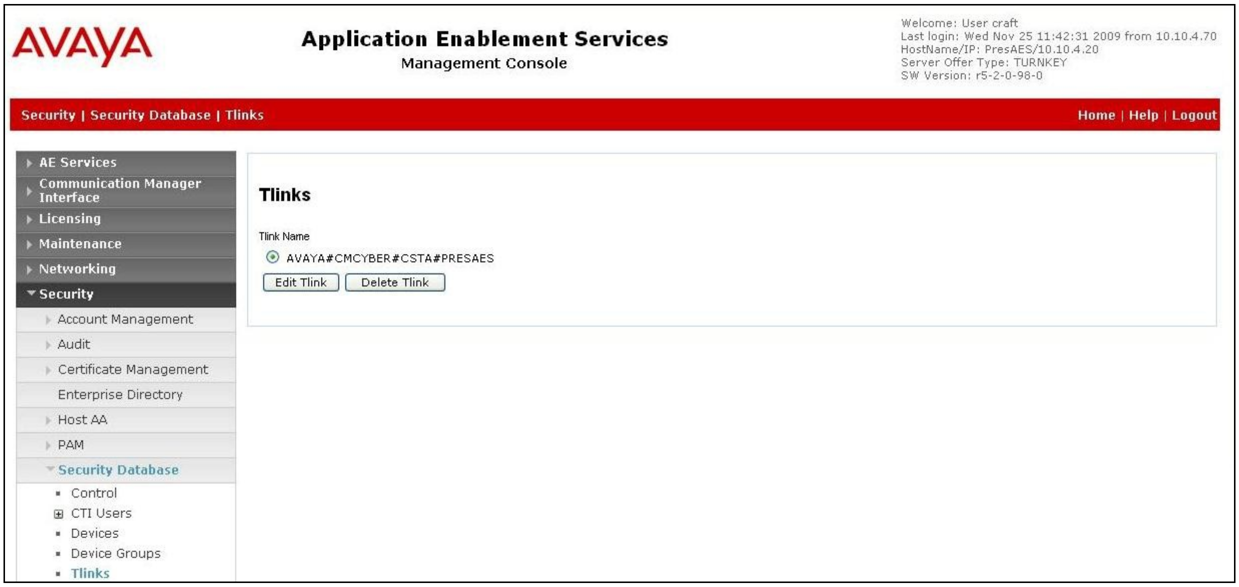
Edit CTI User

User Profile:	User ID	CTIUser
	Common Name	CTIUser
	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

A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

5.6 Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the Tlink name. This will be needed to configure the Presence server in **Section 6.1**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Nov 25 11:42:31 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Security | Security Database | Tlinks

Tlinks

Tlink Name

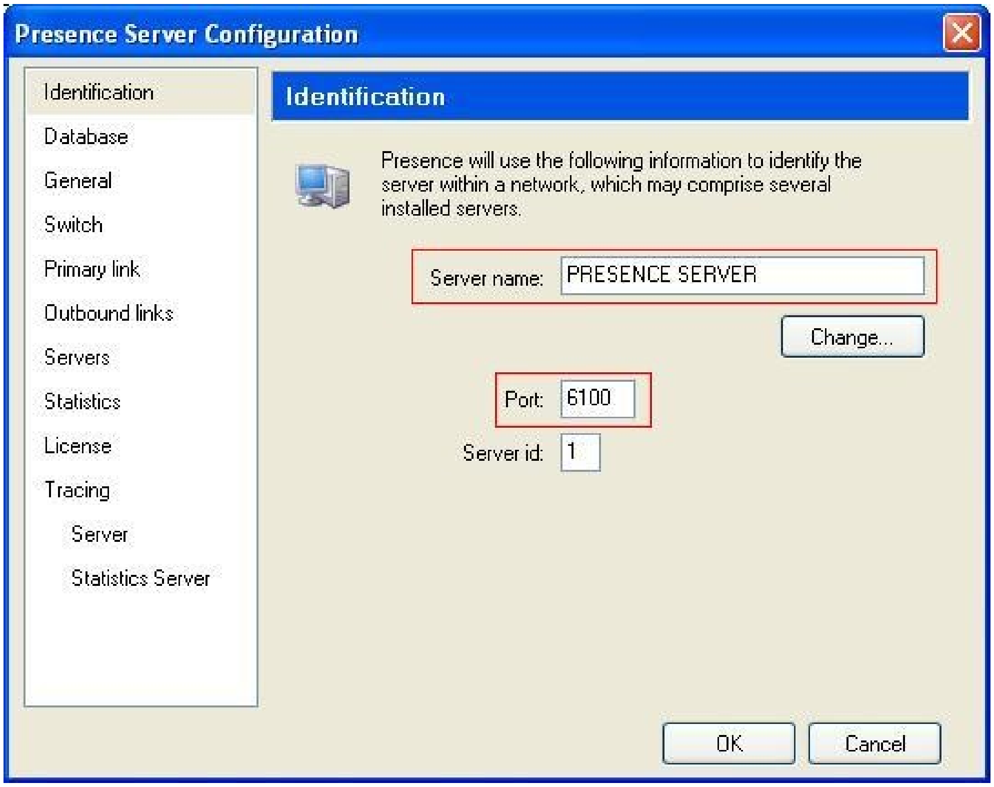
● AVAYA#CMCYBER#CSTA#PRESAES

6 Configure the Presence Suite Server

The Presence Server and the Oracle database were pre-installed on the same machine for convenience, during the compliance testing. The standard practice would be to install the Oracle database on a separate machine.

6.1 Presence Server Configuration

Launch the Presence Server configuration application by double clicking the **pcoservercfg.exe** located in the pre-installed Presence folder on the Presence Server. In the **Identification** option on the menu on the left side of the screen, enter the **Server name:** as **PRESENCE SERVER** as used for the identification of the server. The **Port** can be set to **6100**. Note that the actual value for server port can vary. Press **OK** to continue.



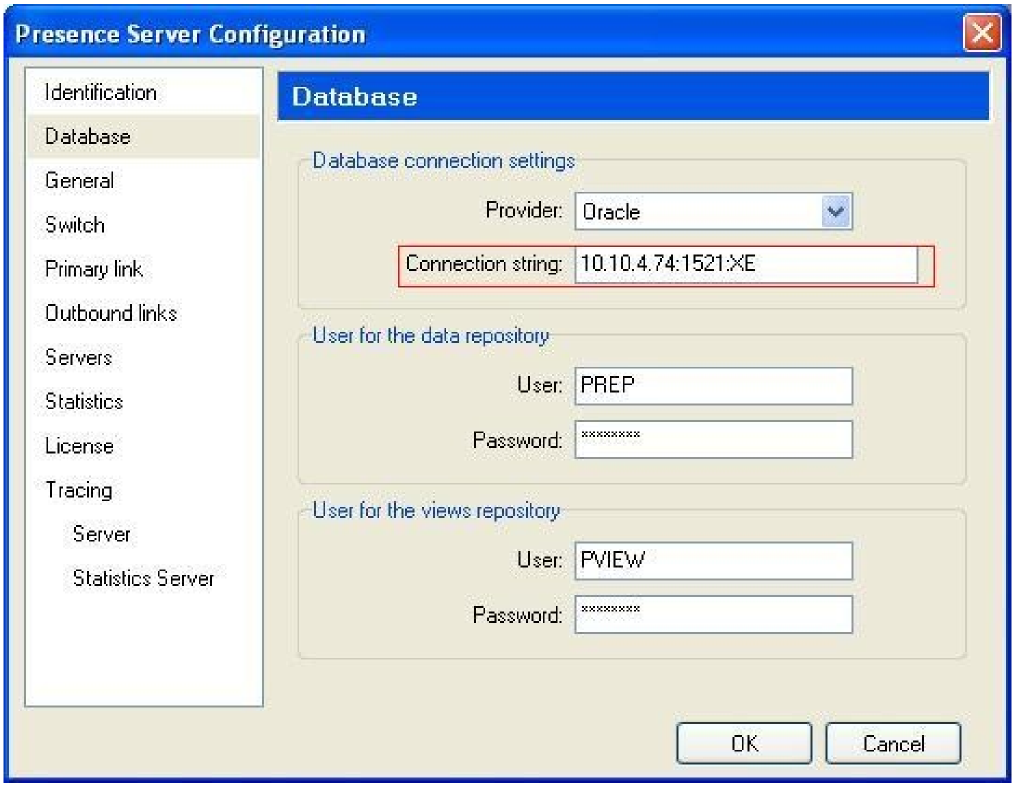
Presence will use the following information to identify the server within a network, which may comprise several installed servers.

Server name: PRESENCE SERVER

Port: 6100

Server id: 1

Select the **Database** option from the menu on the left side of the screen. In the **Connection string:** field, enter the IP address of the Oracle server followed by a colon and then the default port number for the Oracle database **1521**, followed by another colon and then the pre-administered Oracle instance **XE**. The Oracle server is installed on the same server as the Presence application during the compliance test. Enter the appropriate user and password credentials for the Oracle database. Customer calling records were pre-configured on the Presence server for convenience during compliance testing.



Provider: Oracle

Connection string: 10.10.4.74:1521:XE

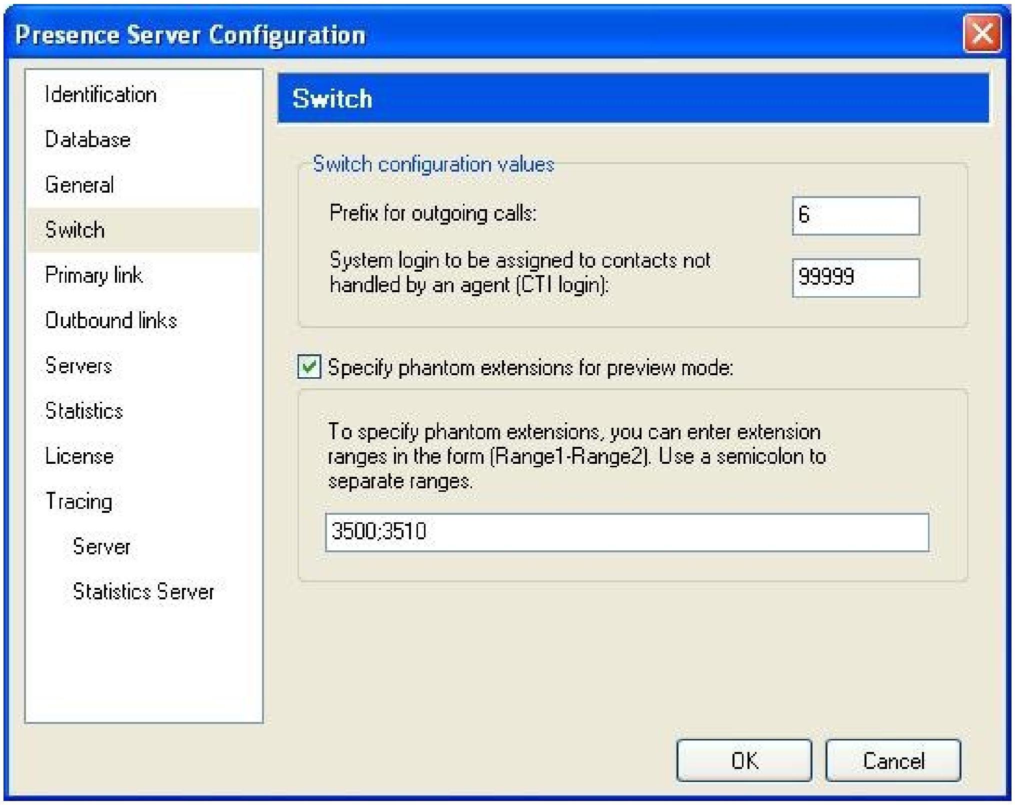
User: PREP

Password: ********

User: PVIEW

Password: ********

Select the **Switch** option on the menu on the left side of the screen. Enter in a value for **Prefix for outgoing calls:** and **System login to be assigned to contacts not handled by an agent (CTI login):**, the values used for this configuration were **6** and **99999**. Enter a tick in the **Specify phantom extension for preview mode** checkbox and enter the phantom extensions configured in **Section 4.9**.



Prefix for outgoing calls: 6

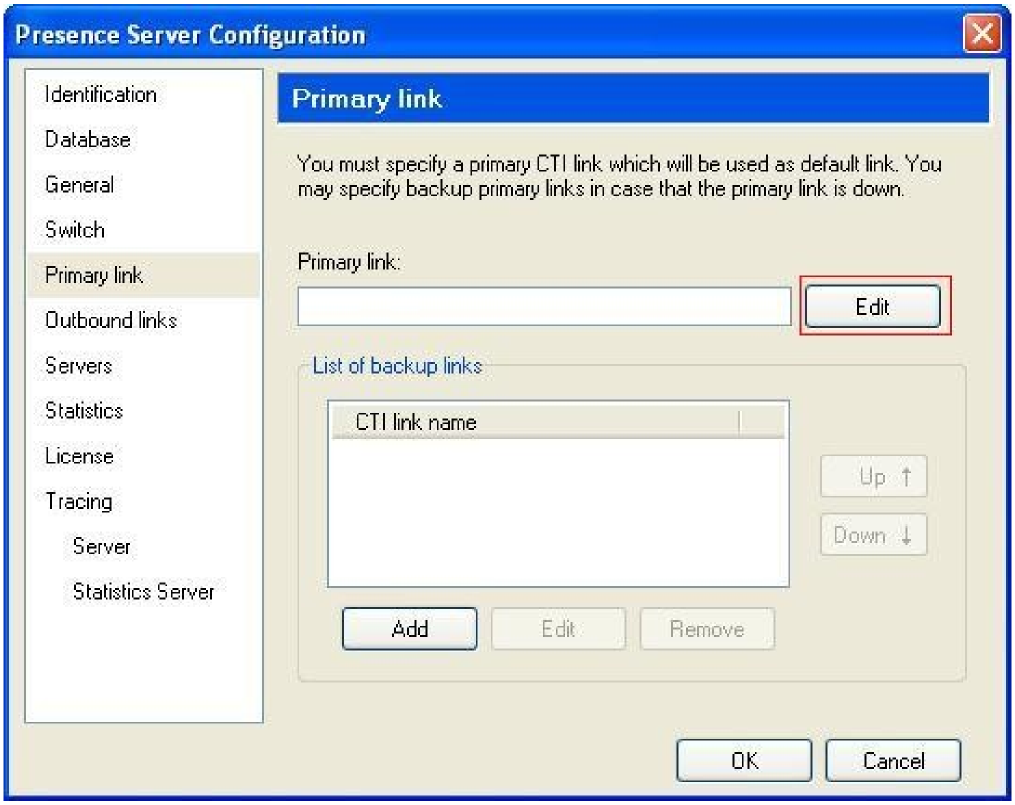
System login to be assigned to contacts not handled by an agent (CTI login): 99999

☑ Specify phantom extensions for preview mode:

To specify phantom extensions, you can enter extension ranges in the form (Range1-Range2). Use a semicolon to separate ranges.

3500;3510

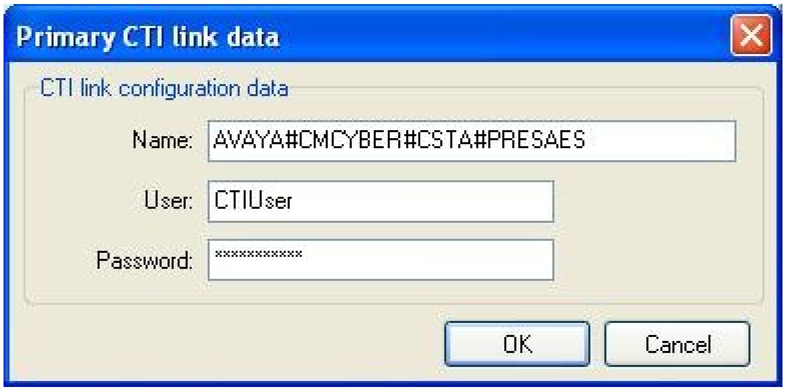
Select the **Primary link** menu on the left side of the screen and choose the **Edit** button to enter in a value.



You must specify a primary CTI link which will be used as default link. You may specify backup primary links in case that the primary link is down.

Primary link:

In the **Name:** field enter the Tlink name on **Section 5.6** and the **User:** name and **Password:** configured in **Section 5.4** on the Application Enablement Services. Click **OK**.

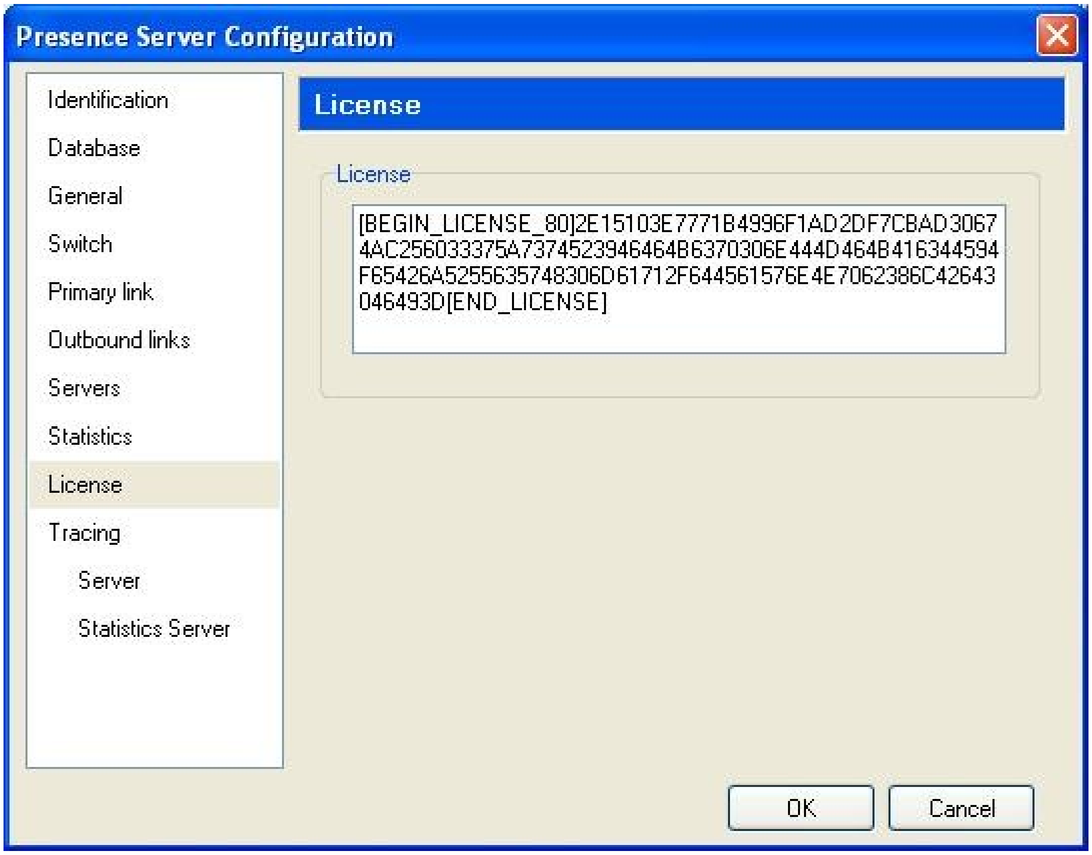


Name: AVAYA#CMCYBER#CSTA#PRESAES

User: CTIUser

Password: ***********

Click on the **License** option on the menu on the left side of the screen and enter a license key. Note a temporary license key was provided by Presence Technology for the duration of the compliance test. Click **OK**.

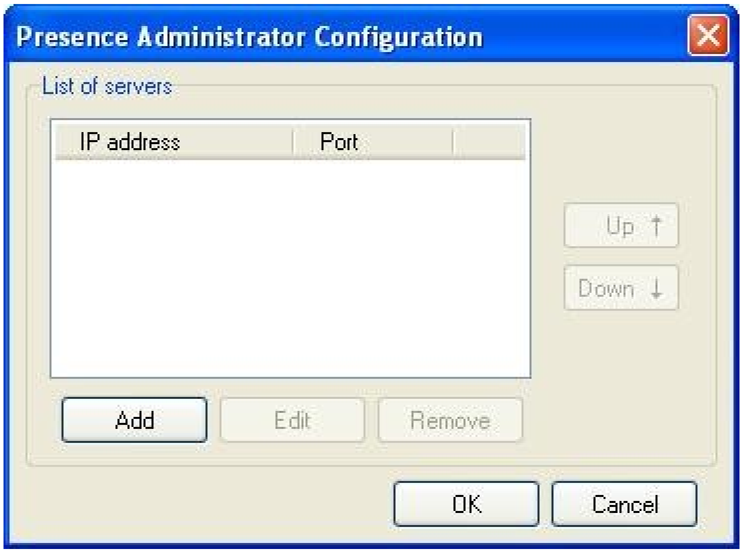


```
[BEGIN_LICENSE_80]2E15103E7771B4996F1AD2DF7CBAD3067
4AC256033375A737452394646 4B6370306E444D464B416344594
F65426A5255635748306D61712F644561576E4E7062386C42643
046493D[END_LICENSE]
```

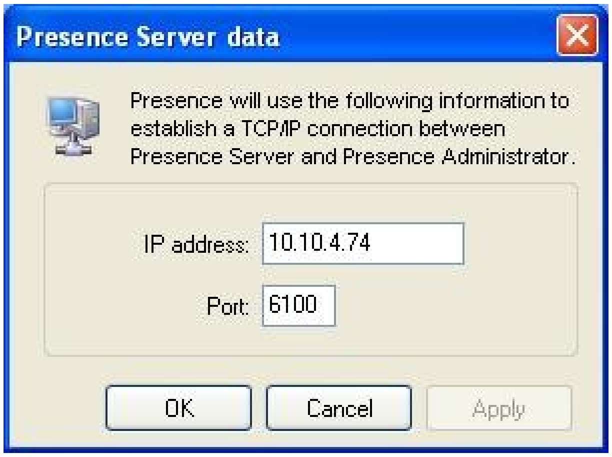
6.2 Presence Administrator Configuration

6.2.1 Configuration of Presence Administrator

Launch the Presence Administrator Configuration application by double clicking the **pcoadmincfg.exe** located in the Presence folder. For testing convenience, the Presence Administrator Configuration Application was also located on the Presence Server machine. Click the **Add** button in the Presence Administrator Configuration screen.



Enter the Presence Server IP Address in the **IP address:** field, in this case **10.10.4.74**. Ensure the Presence Server **Port:** value of **6100** matches the value set in **Section 6.1**. Click **OK**.



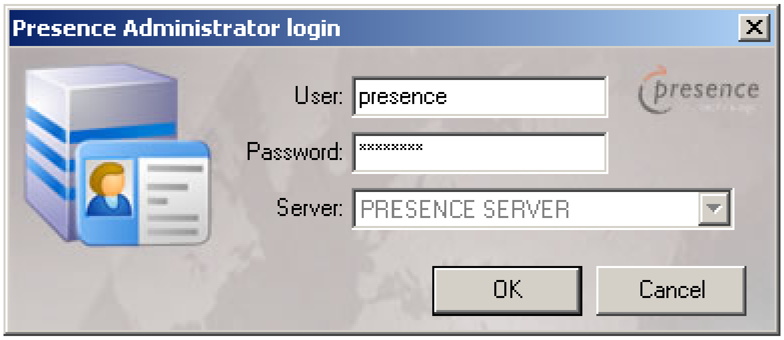
Presence will use the following information to establish a TCP/IP connection between Presence Server and Presence Administrator.

IP address: 10.10.4.74

Port: 6100

6.2.2 Presence Administrator

Launch the Presence Administrator application by double clicking the **pcoadmin.exe** located in the Presence folder. The username and password that appear in the **User:** and **Password** fields are created during the Presence Server installation.



User: presence

Password: ********

Server: PRESENCE SERVER

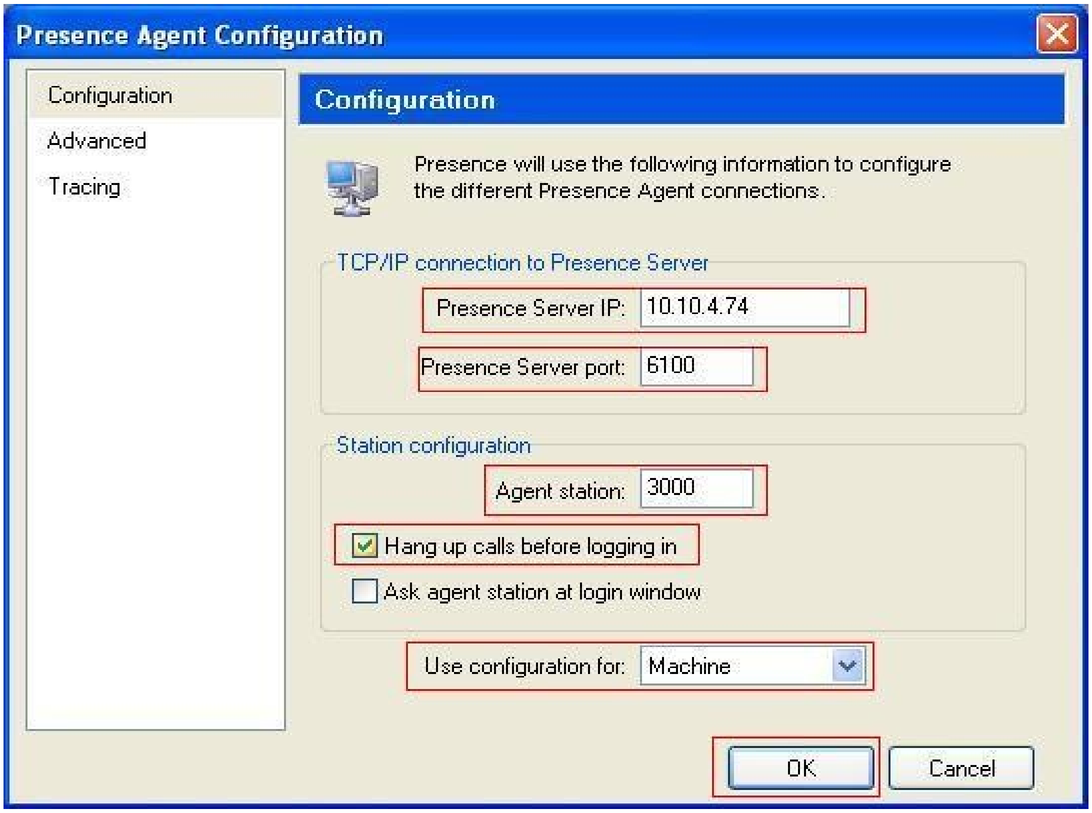
A number of services for inbound, outbound, email and internet were configured via the Presence Administrator and were tested during compliance test. Please refer to **Section 10** for detailed documentation on the configuration of all call services.

6.3 Presence Agent Configuration

The following steps are carried out to configure the Presence Agent.

6.3.1 Configuration of Presence Agent

Launch the Presence agent configuration application by double clicking the **pcoagentcfg.exe** located in the Presence folder. Enter the **Presence Server IP:** address as **10.10.4.74**. The **Presence Server port:** can be left as the default value of **6100**. Enter the agent extension in the **Agent station** field configured on Communication Manager in **Section 4.8**. Check the **Hang up calls before logging in** check box. In the field **Use configuration for:** choose **Machine** from the drop-down menu. Click **OK**. This step is needed for each agent configured; only the agent station field will vary.



Presence will use the following information to configure the different Presence Agent connections.

TCP/IP connection to Presence Server

Presence Server IP: 10.10.4.74

Presence Server port: 6100

Station configuration

Agent station: 3000

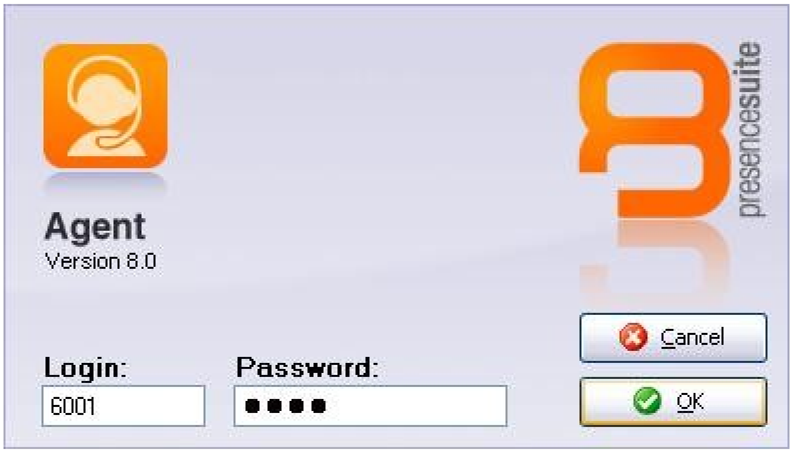
☑ Hang up calls before logging in

□ Ask agent station at login window

Use configuration for: Machine

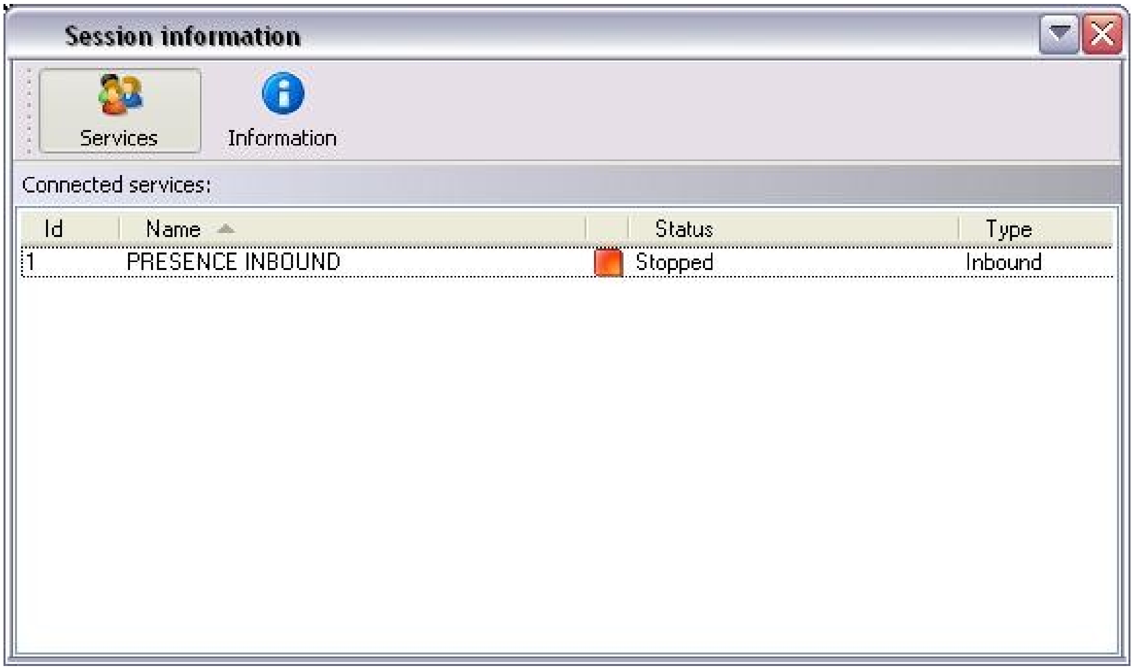
6.3.2 Presence Agent

Prior to installing the Presence agent, ensure that the DBExpress driver (dpexpoda.dll) is located in the **C:\Windows\System32** directory. The DBExpress driver allows the agent application to communicate with the Oracle database. Installing this driver eliminates the need to install the Oracle client. Launch the Presence agent configuration application by double clicking the **pcoagent.exe** located in the Presence folder. Enter the agent **Login** and **Password** configured in **Section 4.7** and click on **OK**.



Login: 6001
Password: ●●●●

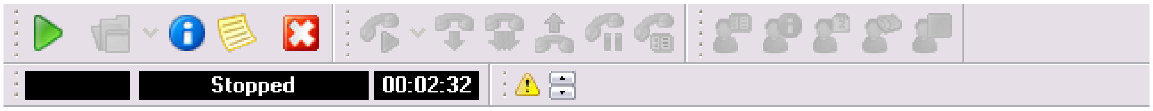
In the screen below, click on the **Services** button in the task bar. The service set up for the agent will be displayed.



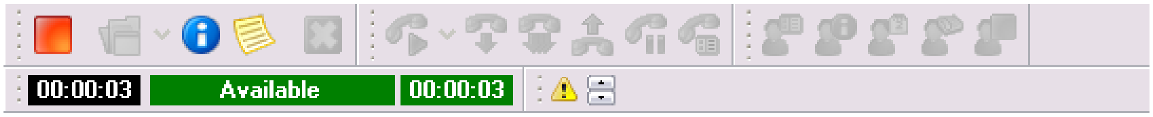
Connected services:

Id	Name	Status	Type
1	PRESENCE INBOUND	🟥 Stopped	Inbound

A task bar is present at the top of the Agent PC. Click on the green arrow to make the agent in an available state.



The information status on the task bar goes to available indicating the agent is ready to receive calls.



7 General Test Approach and Test Results

Testing included validation of correct operation of typical contact centre functions including, inbound voice calls and outbound campaign calls. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, and conference exercised from both the agent application and the agent softphones. This was carried out for the inbound and outbound campaign calls. Email, Web call back and Web collaboration were also tested. Additional features such as call capturing, direct agent transfer calls and malicious calls were tested. The serviceability test cases were performed manually by busying out and releasing the CTI link and by disconnecting and reconnecting the LAN cables.

All the test cases passed successfully. For link failover, as soon as Presence Server identifies the link is down, it automatically re-starts the service, requiring the agents to login again. This is as expected.

8 Verification Steps

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

8.1 Verify Communication Manager

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the TSAPI link status with Application Enablement Services by using the command **status aesvcs cti-link**. The CTI Link is 10. Verify the **Service State** of the TSAPI link is **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              no                     down          0         0
10    4        no    PresAES          established   14        14
```

Use the command **status aesvcs interface** to verify that the status **Local Node CLAN** of Application Enablement Services interface is connected and **listening**.

```
status aesvcs interface

                          AE SERVICES INTERFACE STATUS

Local Node          Enabled?  Number of     Status
                              Connections

CLAN                yes       1             listening
```

Verify that the there is a link with the Application Enablement Services and that messages are being sent and received by using the command **status aesvcs link**.

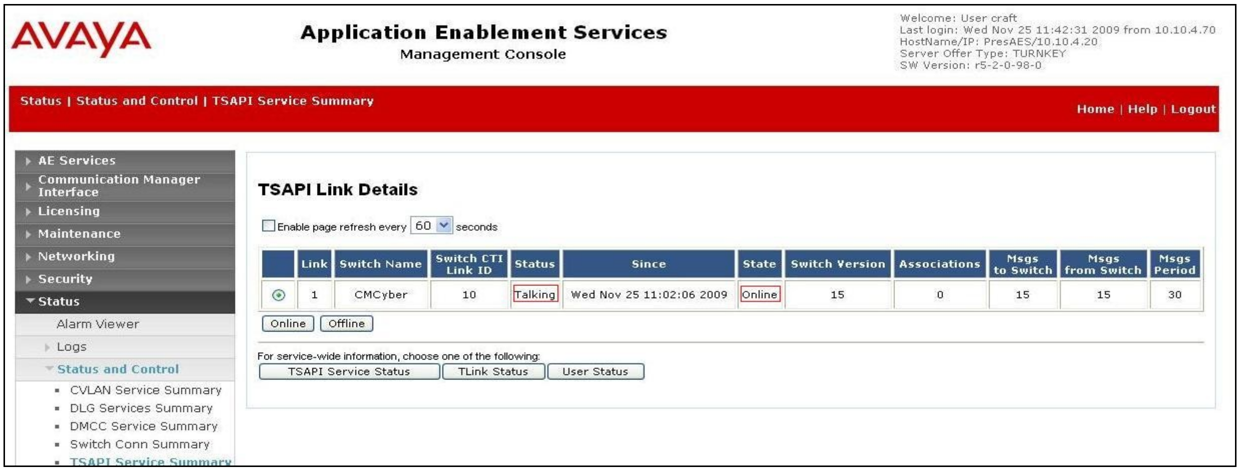
```
status aesvcs link

                            AE SERVICES LINK STATUS

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

01/01  PresAES          10. 10.  4. 20  35199   CLAN            623     610
```

8.2 Verify Application Enablement Services

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly.

8.2.1 TSAPI Link

On the **Application Enablement Services Management Console** verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Nov 25 11:42:31 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Status | Status and Control | TSAPI Service Summary

TSAPI Link Details

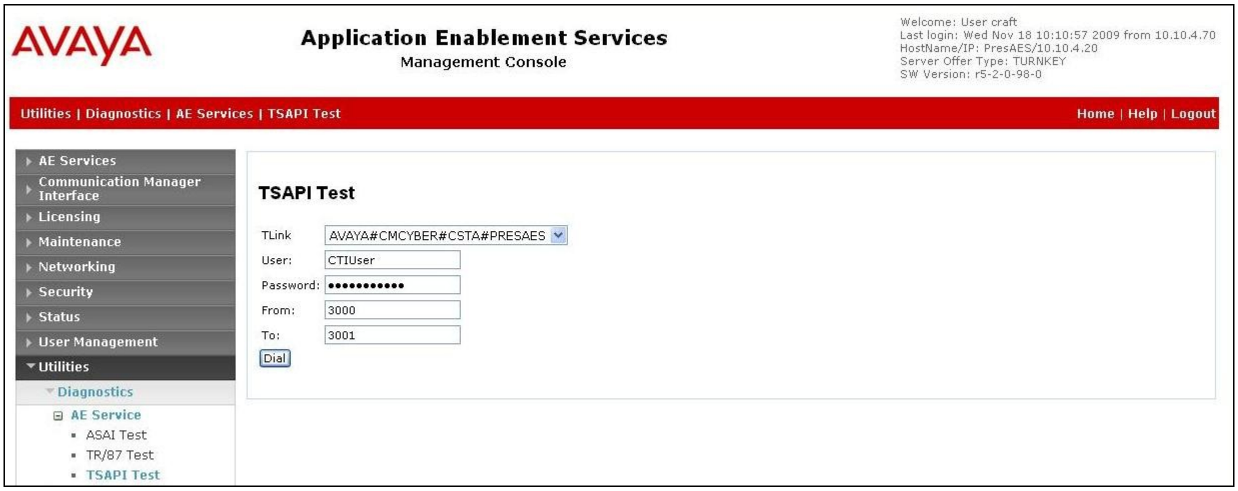
□ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
◉	1	CMCyber	10	Talking	Wed Nov 25 11:02:06 2009	Online	15	0	15	15	30

For service-wide information, choose one of the following:

8.2.2 TSAPI Test

Make a call between two stations on Communication Manager using the TSAPI Link. On the Application Enablement Services **Management Console** navigate to the screen as follows **Utilities → AE Service → TSAPI Test.** Use the username and password set up in **Section 5.4**. Enter in the extension numbers and choose **Dial**.

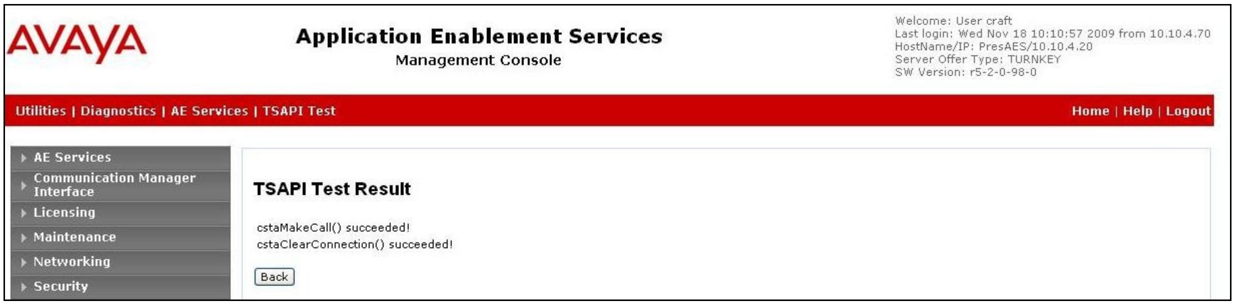


Welcome: User craft
Last login: Wed Nov 18 10:10:57 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

TSAPI Test

TLink: AVAYA#CMCYBER#CSTA#PRESAES
User: CTIUser
Password: ●●●●●●●●●●●
From: 3000
To: 3001

The following screen indicates that the call has been successful.


AVAYA
Application Enablement Services
Management Console
Utilities | Diagnostics | AE Services | TSAPI Test
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Back

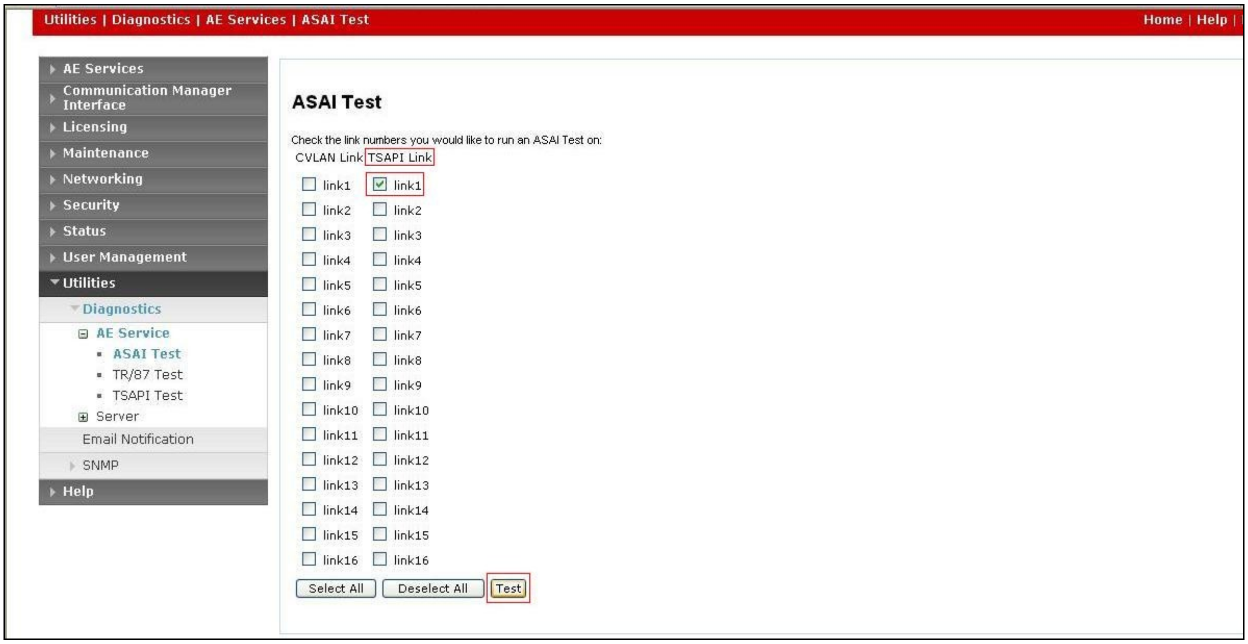
Welcome: User craft
Last login: Wed Nov 18 10:10:57 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

TSAPI Test Result

```
cstaMakeCall() succeeded!
cstaClearConnection() succeeded!
```

8.2.3 ASAI Test

Additional Tests can be carried out by the using the ASAI Test. Open this screen under **Utilities** → **AE Service** → **ASAI Test**. Run the ASAI Test and check the **TSAPI Link** number on which you would like to run the test. Click on the **Test** button.

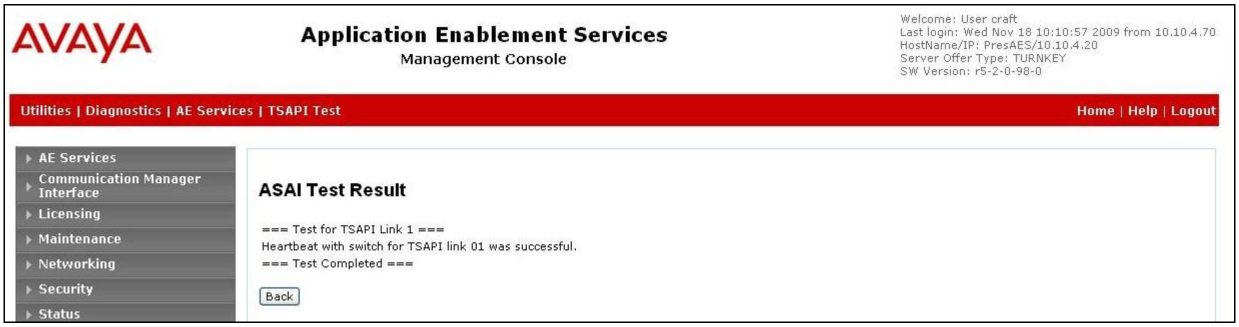


ASAI Test

Check the link numbers you would like to run an ASAI Test on:

CVLAN Link	TSAPI Link
□ link1	☑ link1
□ link2	□ link2
□ link3	□ link3
□ link4	□ link4
□ link5	□ link5
□ link6	□ link6
□ link7	□ link7
□ link8	□ link8
□ link9	□ link9
□ link10	□ link10
□ link11	□ link11
□ link12	□ link12
□ link13	□ link13
□ link14	□ link14
□ link15	□ link15
□ link16	□ link16

The screen **ASAI Test Result** verifies that the TSAPI Link set up in **Section 5.3** is communicating successfully.


AVAYA
Application Enablement Services
Management Console
Utilities | Diagnostics | AE Services | TSAPI Test
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
Back

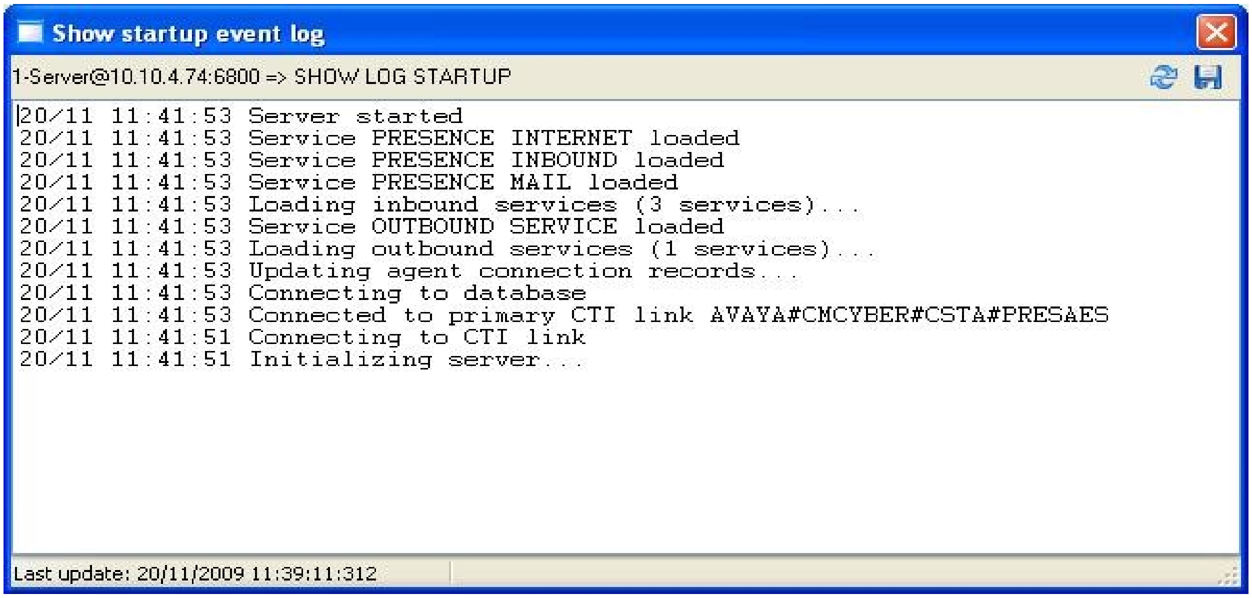
Welcome: User craft
Last login: Wed Nov 18 10:10:57 2009 from 10.10.4.70
HostName/IP: PresAES/10.10.4.20
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

ASAI Test Result

```
=== Test for TSAPI Link 1 ===
Heartbeat with switch for TSAPI link 01 was successful.
=== Test Completed ===
```

8.3 Verify Presence Suite

One of the available features is a startup log. A startup log commences when the Presence Server is trying to load and connect to the Application Enablement Services. The screen below indicates the server has started.

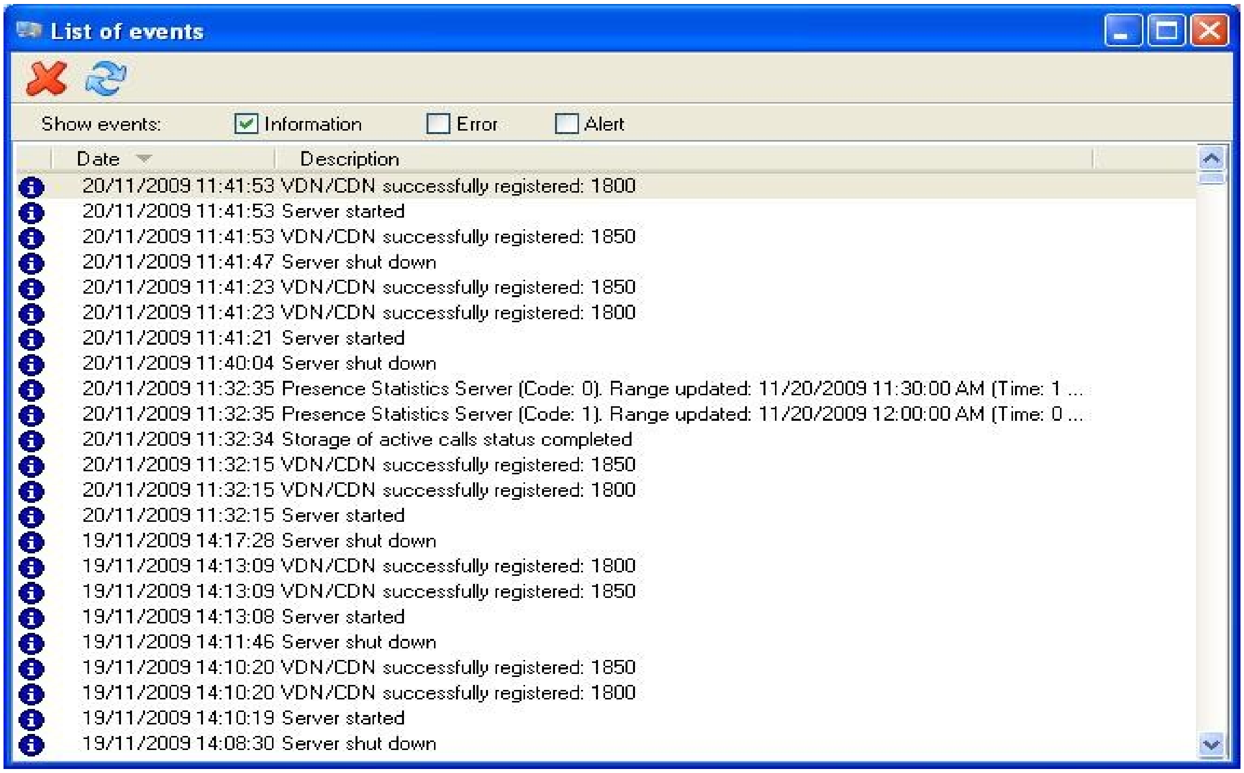


1-Server@10.10.4.74:6800 => SHOW LOG STARTUP

```
20/11 11:41:53 Server started
20/11 11:41:53 Service PRESENCE INTERNET loaded
20/11 11:41:53 Service PRESENCE INBOUND loaded
20/11 11:41:53 Service PRESENCE MAIL loaded
20/11 11:41:53 Loading inbound services (3 services)...
20/11 11:41:53 Service OUTBOUND SERVICE loaded
20/11 11:41:53 Loading outbound services (1 services)...
20/11 11:41:53 Updating agent connection records...
20/11 11:41:53 Connecting to database
20/11 11:41:53 Connected to primary CTI link AVAYA#CMCYBER#CSTA#PRESAES
20/11 11:41:51 Connecting to CTI link
20/11 11:41:51 Initializing server...
```

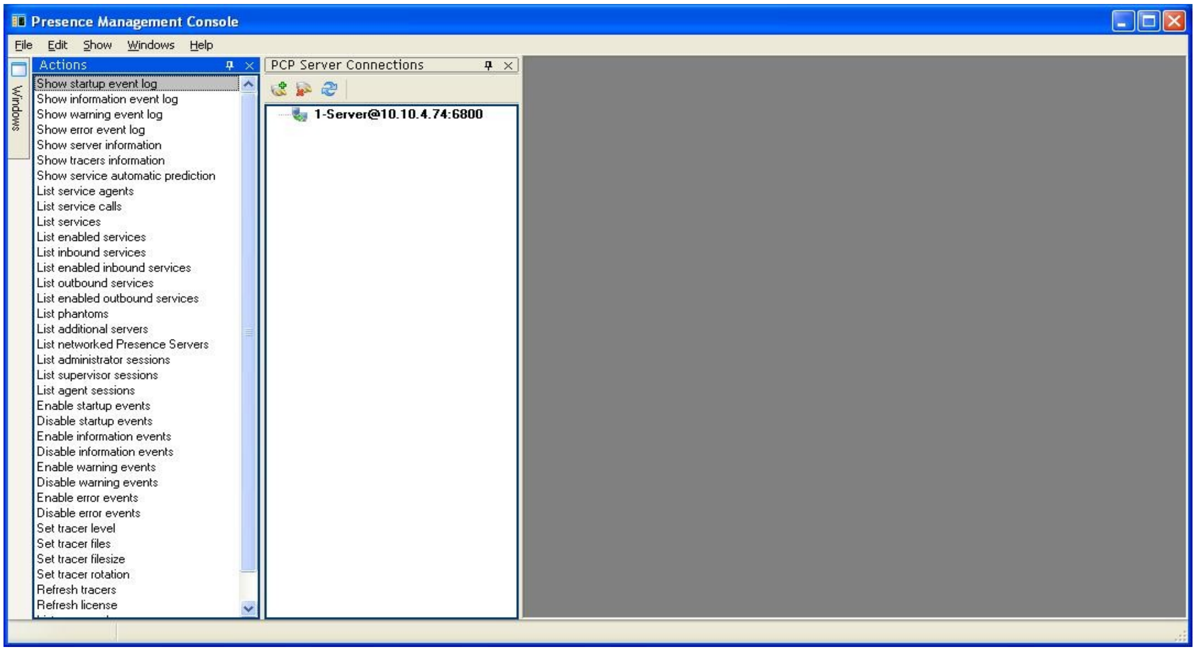
Last update: 20/11/2009 11:39:11:312

The Presence Suite system maintains a log of the events that have occurred in the system. The Events command is located in the Utilities menu in the Presence administrator menu and is used to display and delete the system event log.



```
20/11/2009 11:41:53 VDN/CDN successfully registered: 1800
20/11/2009 11:41:53 Server started
20/11/2009 11:41:53 VDN/CDN successfully registered: 1850
20/11/2009 11:41:47 Server shut down
20/11/2009 11:41:23 VDN/CDN successfully registered: 1850
20/11/2009 11:41:23 VDN/CDN successfully registered: 1800
20/11/2009 11:41:21 Server started
20/11/2009 11:40:04 Server shut down
20/11/2009 11:32:35 Presence Statistics Server (Code: 0). Range updated: 11/20/2009 11:30:00 AM (Time: 1 ...
20/11/2009 11:32:35 Presence Statistics Server (Code: 1). Range updated: 11/20/2009 12:00:00 AM (Time: 0 ...
20/11/2009 11:32:34 Storage of active calls status completed
20/11/2009 11:32:15 VDN/CDN successfully registered: 1850
20/11/2009 11:32:15 VDN/CDN successfully registered: 1800
20/11/2009 11:32:15 Server started
19/11/2009 14:17:28 Server shut down
19/11/2009 14:13:09 VDN/CDN successfully registered: 1800
19/11/2009 14:13:09 VDN/CDN successfully registered: 1850
19/11/2009 14:13:08 Server started
19/11/2009 14:11:46 Server shut down
19/11/2009 14:10:20 VDN/CDN successfully registered: 1850
19/11/2009 14:10:20 VDN/CDN successfully registered: 1800
19/11/2009 14:10:19 Server started
19/11/2009 14:08:30 Server shut down
```

Presence Suite has a ‘pmconsole.exe’ application which is a tool used to aid fault diagnosis in the field.



9 Conclusion

These Application Notes describe the configuration steps required for Presence Suite 8 to successfully interoperate with Avaya Aura™ Communication Manager 5.2 using Avaya Aura™ Application Enablement Services 5.2. All functionality and serviceability test cases were completed successfully.

10 Additional References

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

Product documentation for Avaya products may be found at http://support.avaya.com.

1. Administering Avaya Aura™ Communication Manager, Release 5.2; Document No. 03-300509, May 2009
2. Avaya Aura™ Application Enablement Services Administration and Maintenance Guide; Release 5.2, Document No. 02-300357 ; November 2009
3. Avaya Aura™ Application Enablement Services R5.2 Server and Client Release Notes, November 2009

The following documentation is available on request from Presence: www.presenceco.com

1. ACD Sys Presence Administrator Manual Presence Suite, V8.0
2. Presence Installation Guides Presence Software, V8.0
3. PBX/ACD Requirements Presence Software, V8.0

©2009 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.