Avaya Solution & Interoperability Test Lab

Application Notes for Presence Technology Presence Suite 8.1 with Avaya Aura® Communication Manager 6.0 and Avaya Aura® Application Enablement Services 5.2.2 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for 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. Presence Suite integrates with the Avaya solution by using the Telephony Services Application Programmer Interface (TSAPI) provided by Avaya Aura® Application Enablement Services 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® Communication Manager with Avaya Aura® Application Enablement Services (AES). Presence Suite is a multi-channel contact management suite able to handle voice, e-mail and web chat contact mechanisms. The Telephony Services Application Programmer Interface (TSAPI) provided by Avaya Aura® Application Enablement Services 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 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 Avaya Aura® 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 Avaya Aura® Application Enablement Services.

2 General Test Approach and Test Results

Testing included validating the correct operation of typical contact centre functions including, inbound and outbound campaign calls. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, and conference. This was carried out for the inbound and outbound campaign calls. Email, Web call back and Web chat were also tested. Additional features such as call capturing, direct agent transfer 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 LAN cables.

2.1 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.

2.2 Test Results

All 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.

2.3 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

3 Reference Configuration

Figure 1 shows the network topology during interoperability testing. Avaya S8800 Server running Communication Manager with an Avaya G650 Media Gateway was used as the hosting PBX. Presence Suite, including Presence Agent PC's, are connected to the LAN and control the Avaya IP telephones via Application Enablement Services using TSAPI.

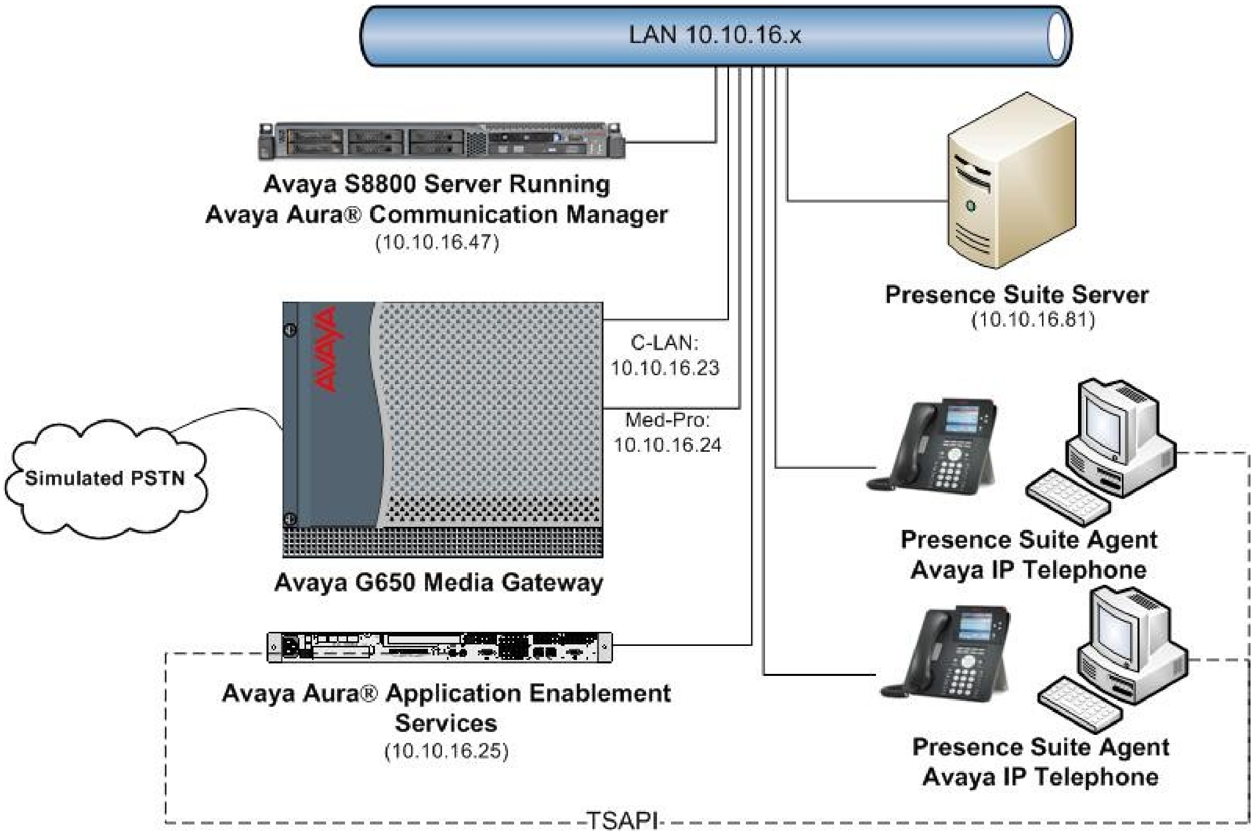


Figure 1: Network Topology

4 Equipment and Software Validated

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

Equipment	**Software**
Avaya S8800 Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.0 Service Pack 01
Avaya G650 Media Gateway CLAN -TN799DP MEDPRO- TN2302AP	 HW 01 FW 024 HW 08 FW 055
Dell 1950 Server running Avaya Aura® Application Enablement Services	Avaya Aura® Application Enablement Services 5.2.2
Avaya 96xx Telephones (H.323)	3.1.1
Presence Suite Server	8.1
Operating System for Presence Agent PC's	Windows XP Professional SP3 Windows Vista Business

Table 1: Hardware and Software Version Numbers

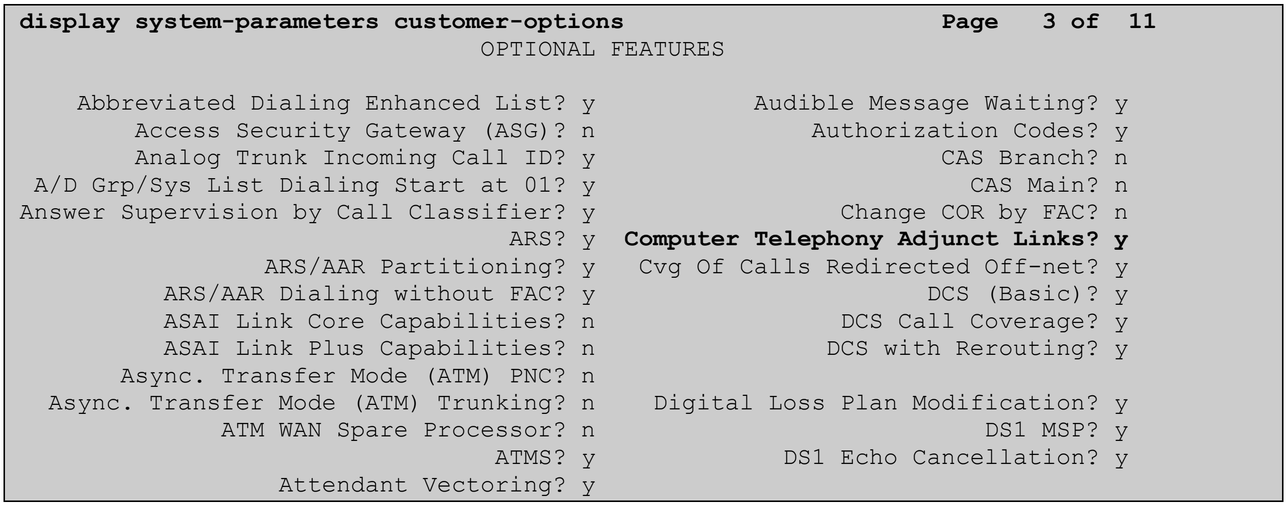
5 Configure Avaya Aura® Communication Manager

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 and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The configuration operations described in this section can be summarized as follows:

- Verify System Features
- Administer SIT Treatment for Call Classification
- Define Feature Access Codes (FAC)
- Administer Trunk Group
- Administer Hunt Groups, Vectors and VDN's
- Administer Class of Restriction
- Administer Agent Logins
- Administer Agent Stations
- Administer CTI Stations
- Configure CLAN for AES Connectivity
- Configure Transport link for AES Connectivity
- Configure CTI Link for TSAPI Service

5.1 Verify System Features

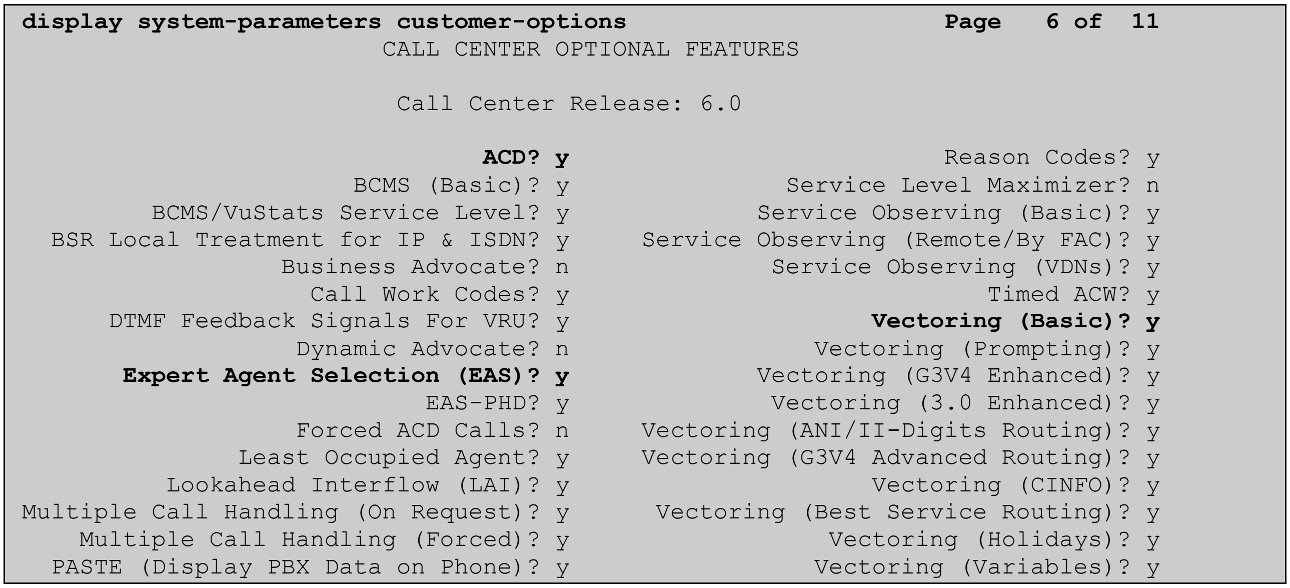
Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.



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

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          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? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

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: 6.0

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

Use the command **display system-parameters features** and 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  19
                        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  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

          Interruptible Aux Notification Timer (sec): 3

  ASAI
            Copy ASAI UUI During Conference/Transfer? y
        Call Classification After Answer Supervision? y
                                   Send UCID to ASAI? y
          For ASAI Send DTMF Tone to Call Originator? y
```

5.2 Administer Special Information Tones Treatment for Call Classification

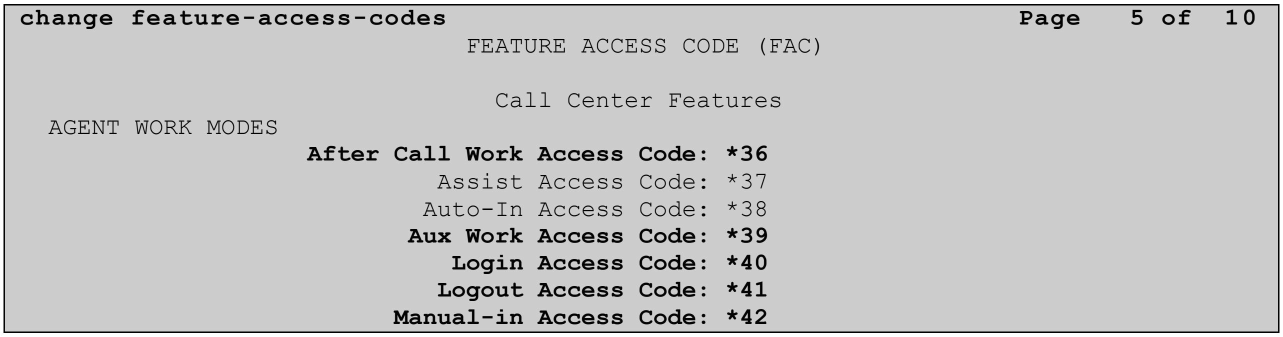
This form is used to specify the treatment of Special Information Tones (SIT) used for outbound call management type calls with USA tone characteristics. Enter the **change sit-treatment** command. Set the **Pause Duration** to **0.8** and **Talk Duration** to **3.0**.

```
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
```

5.3 Define Feature Access Codes (FAC)

Use the **change feature-access-codes** command to define the required access codes. On **Page 5** define a FAC for each of the following:

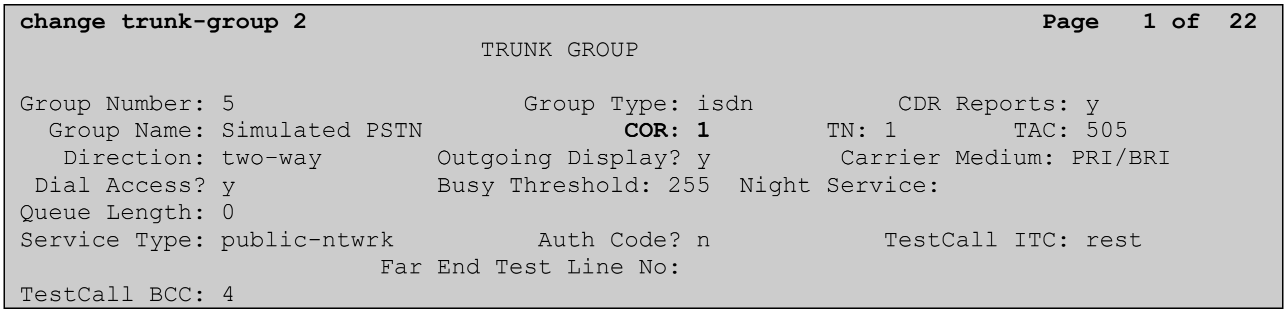
- **Aux Work Access Code:** When activated this feature will set the ACD agent to an Auxilary work state, this is the default state for an agent upon first login.
- **After Call Work Access Code:** When activated this feature will set the ACD agent to an ACW or ‘not ready’ work state, this is the default state for an agent upon call completion when using manual-in.
- **Login Access Code:** This feature allows ACD agents to log in to an extension.
- **Logout Access Code:** This feature allows ACD agents to log out of an extension.
- **Manual-in Access Code:** When activated this feature will set the ACD agent to a state where they are available to handle calls, upon completion of a call the agent will be unavailable until the feature is activated again.



```
change feature-access-codes                                     Page   5 of  10
                               FEATURE ACCESS CODE (FAC)

                                 Call Center Features
  AGENT WORK MODES
                    After Call Work Access Code: *36
                             Assist Access Code: *37
                            Auto-In Access Code: *38
                           Aux Work Access Code: *39
                              Login Access Code: *40
                             Logout Access Code: *41
                          Manual-in Access Code: *42
```

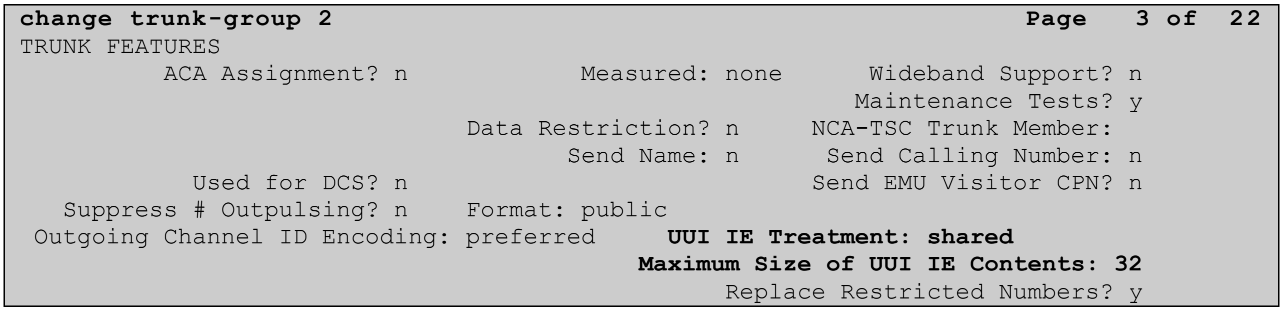
5.4 Administer Trunk

Use the **change trunk group n** command, 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 for interoperability testing is **2**. On **Page 1** set the **COR** (class of restriction) to **1**, this is the COR used for the sample configuration.



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

Group Number: 5                    Group Type: isdn          CDR Reports: y
  Group Name: Simulated PSTN                COR: 1        TN: 1        TAC: 505
   Direction: two-way        Outgoing Display? y         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      Wideband Support? n
                                                         Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: n      Send Calling Number: n
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: public
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: shared
                                           Maximum Size of UUI IE Contents: 32
                                                 Replace Restricted Numbers? y
```

5.5 Administer Hunt Groups, Call Vectors and Vector Directory Numbers

This section describes the configuration required to route calls to the Presence agents. A Vector Directory Numbers (VDN), Vector, Hunt Group and an Agent login ID is required for each contact method used with Presence Suite. Below is a table showing the VDNs, Vectors, Hunt Groups and Agent Login IDs set up for the purpose of interoperability testing. Note that the Suspended row does not have any agents assigned, as this is not used by Presence Suite to route calls but is used instead as a place holder for calls that have been suspended. The Direct Agent row has neither a Skill Group or Agent login ID assigned as this VDN is used to hand control of a call to Presence Suite so that it can deliver the call to the desired destination.

	VDN	Vector	Skill Ext/Hunt Group	Agent Logins
Inbound	1801	1	3091/1	6001 + 6006
Outbound	1802	2	3092/2	6002 + 6007
Email	1803	3	3093/3	6003
Suspended	1804	4	3094/4	N/A
Web Chat & Web Callback	1805	5	3095/5	6005
Direct Agent	1806	6	N/A	N/A

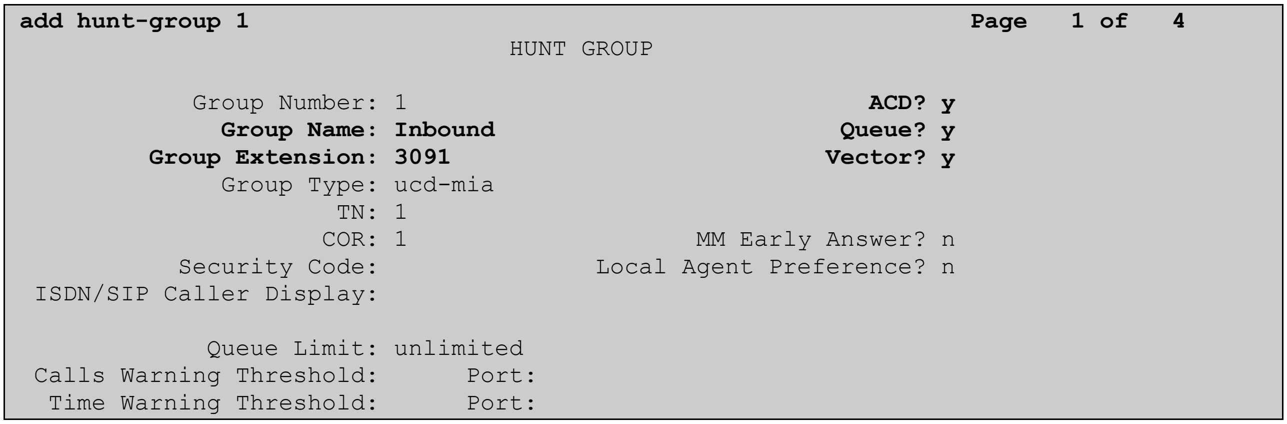
Table 2: Test Agent Details

Note: Unless stated in the Application Notes, the configuration steps for the above VDNs, Vectors, Hunt Groups and Agent Logins are the same. The steps in the following sections may be repeated for each service.

5.5.1 Hunt Groups

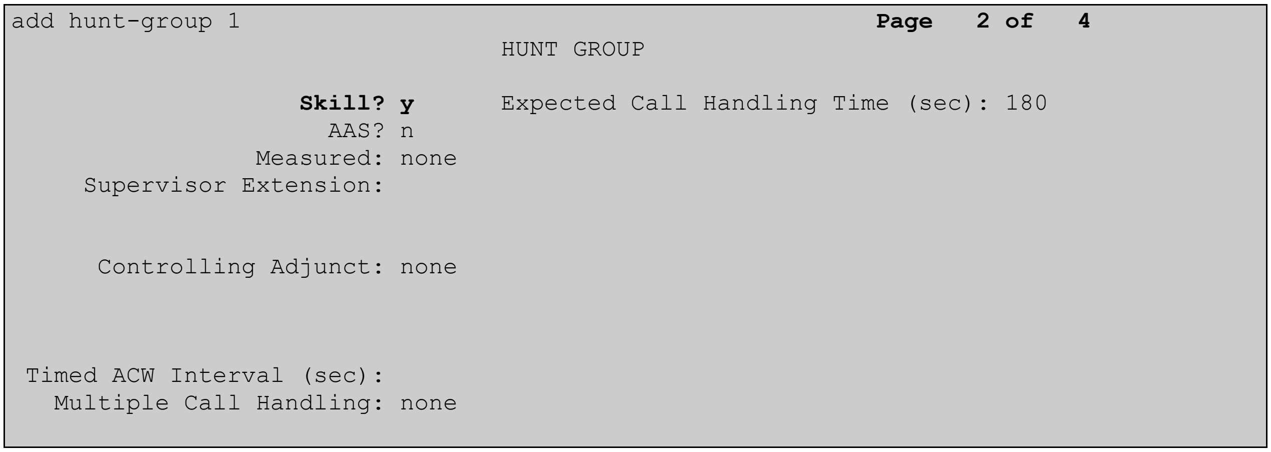
Enter the **add hunt-group n** command where **n** is an available hunt group number. On **Page 1** of the **hunt group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to **y** as shown below.

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



```
add hunt-group 1                                                Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                                  ACD? y
              Group Name: Inbound                          Queue? y
         Group Extension: 3091                            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   4
                                  HUNT GROUP

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


      Controlling Adjunct: none



 Timed ACW Interval (sec):
   Multiple Call Handling: none
```

Repeat the above steps to create hunt groups for the remaining services. Use the **list hunt-group** command to list all of the configured hunt groups as illustrated below.

```
l list hunt-group                                                          Page   1

                                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    Inbound
     3091             ucd-mia y/N  SK  none y   0        n              n
2    Outbound
     3092             ucd-mia y/N  SK  none y   0        n              n
3    Email
     3093             ucd-mia y/N  SK  none y   0        n              n
4    SuspendEmail
     3094             ucd-mia y/N  SK  none y   0        n              n
5    Web Chat Call Back
     3095             ucd-mia y/N  SK  none y   0        n              n
6    DirectAgent
     3096             ucd-mia y/N  SK  none y   0        n              n
```

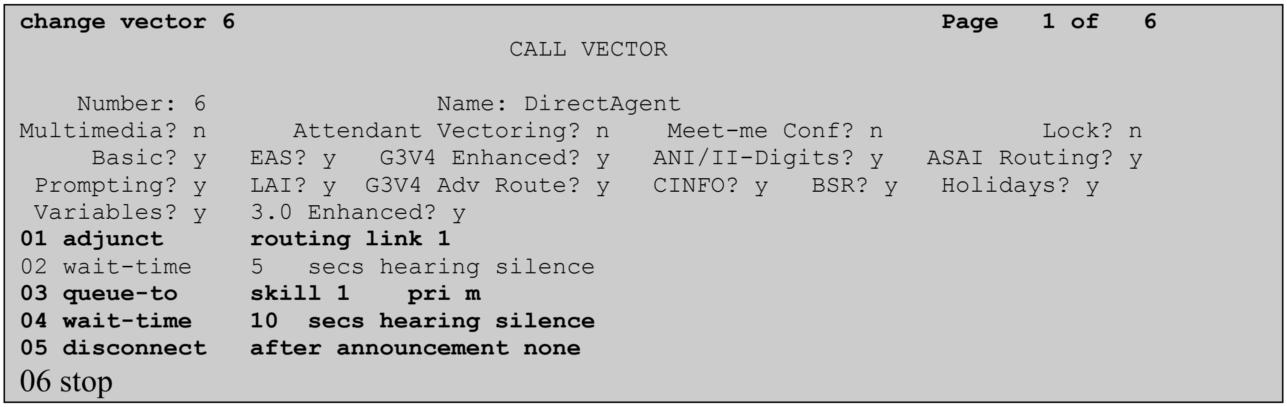
5.5.2 Vectors

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

Note: This is a sample vector, it is possible to provide additional call treatment within the vector such as queue announcements and time of day routing, please see **reference [1]** for further information.

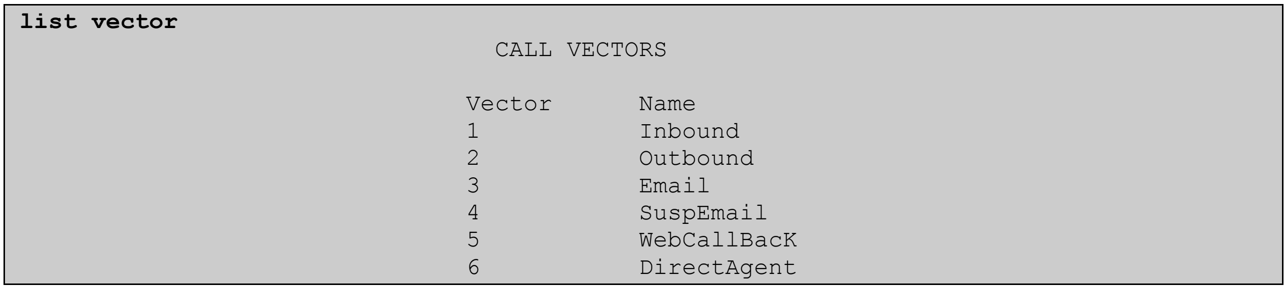
```
change vector 1                                                    Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: Inbound
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    1   secs hearing silence
02 queue-to     skill 1    pri m
03 wait-time    60  secs hearing ringback
04 disconnect   after announcement none
05 stop
```

The above step may be used to create Vectors for the remaining services, except for the Suspend and Direct Agent vectors which requires a different configuration, Vector 6 along with VDN 1806, is used for two additional Presence features; Direct Transfer to agents and Call Capturing**.** Vector 4 along with VDN 1804 is used for suspended Emails. Both vectors require an adjunct routing step. Enter the command **change vector n.** The CTI link configured in **Section 5.12** used by Presence Suite needs to be specified in the vector line 1 (i.e., **01 adjunct routing link 1**). Vector line 1 passes control of the call over to Presence Suite so that Presence Suite may transfer the call to a specific agent. Vector lines 3, 4 and 5 provide treatment to the call in case of an unsuccessful routing attempt of the call by the adjunct link. The Direct agent Vector of 6 is shown below, the configuration of the suspend Vector is the same except line 3 would reference skill 4.



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

    Number: 6               Name: DirectAgent
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 adjunct      routing link 1
02 wait-time    5   secs hearing silence
03 queue-to     skill 1    pri m
04 wait-time    10  secs hearing silence
05 disconnect   after announcement none
06 stop
```

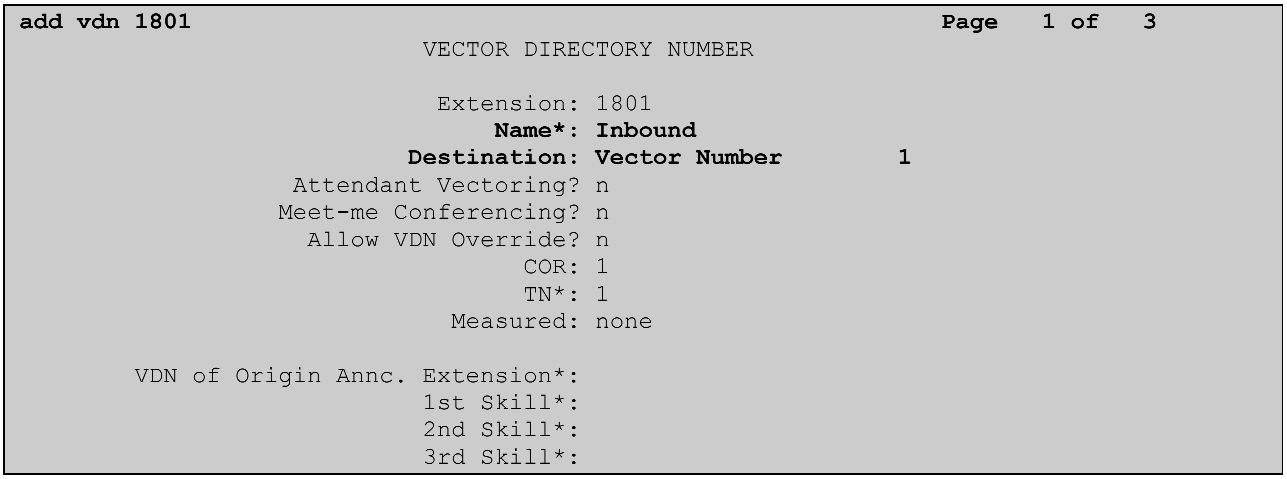
Use the **list vector** command to list all of the configured Vectors as illustrated below.



```
list vector
                                 CALL VECTORS

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

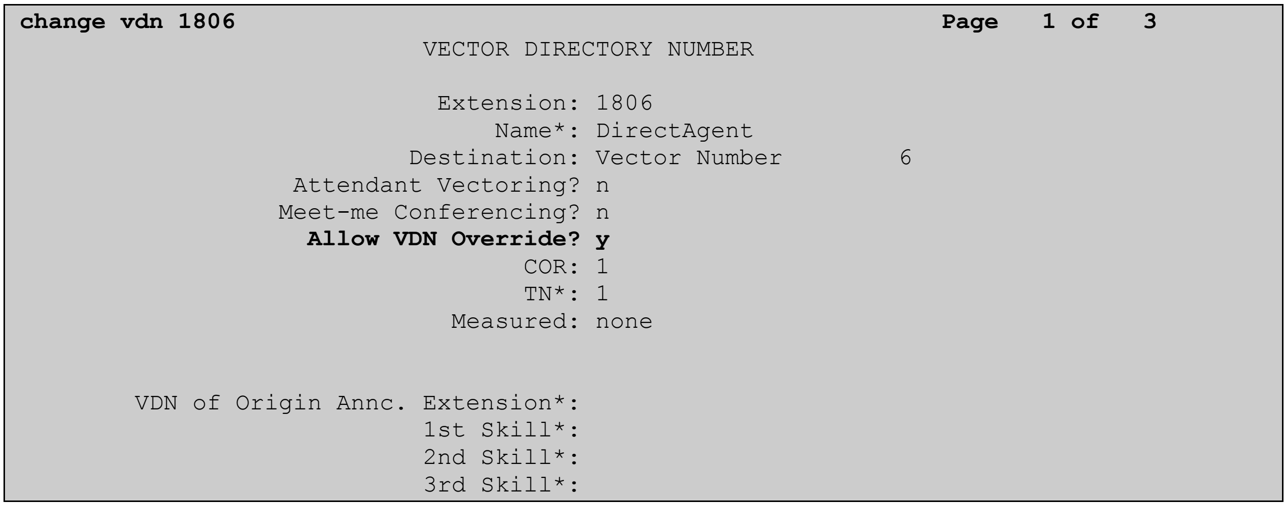
5.5.3 Vector Directory Numbers (VDN)

Enter the **add vdn n** command, where **n** is an available extension number. On **Page 1** assign a **Name** for the VDN and set the **Vector Number** to the relevant vector according to **Table 2** in **Section 5.5**.



```
add vdn 1801                                                    Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 1801
                                 Name*: Inbound
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

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

For the Direct Agent VDN, the **Allow VDN Override** field must be set to **y** as shown in the screen below.



```
change vdn 1806                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 1806
                                 Name*: DirectAgent
                           Destination: Vector Number        6
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? y
                                   COR: 1
                                   TN*: 1
                              Measured: none


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

Use the **list vdn** command to list all of the configured VDNs, illustrated below are the VDNs required for the sample configuration.

```
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

Inbound                1801            n  1   1    V  1    none
Outbound               1802            n  1   1    V  2    none
Email                  1803            n  1   1    V  3    none
SuspEmail              1804            n  1   1    V  4    none
WebCallBack            1805            n  1   1    V  5    none
DirectAgent            1806            y  1   1    V  6    none
```

5.6 Administer Class of Restriction

Enter the **change cor 1** command where **1** corresponds to the Class of Restriction assigned to the trunk group in **Section 5.4** and the agent login IDs in **Section 5.7**. On **Page 1**, set the **Direct Agent Calling** to **y**. This will allow agents to be called directly once they are logged in.

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

               COR Number: 1
          COR Description: Default

                      FRL: 0                                APLT? y
  Can Be Service Observed? y          Calling Party Restriction: none
Can Be A Service Observer? y           Called Party Restriction: none
        Time of Day Chart: 1      Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? y
     Restriction Override: all        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n   n
```

5.7 Administer Agent Logins

Enter the **add agent-loginID n** command; where **n** is an available extension number. 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 5.6**. Define a **Password** for the agent and confirm it in the **Password (enter again)** field. The **Auto Answer** field is set to **station** except for those logins that will be used for outbound services. In that case, the field will be set to **all**.

```
add agent-loginID 6001                                     Page   1 of   3
                                 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
```

On **Page 2,** assign a skill to the agent by entering the relevant hunt group according to **Table 2** in **Section 5.5** for **SN** and entering a skill level of **1** for **SL**.

```
change agent-loginID 6001                                       Page   2 of   3
                                 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:
```

Use the **list agent-loginID** command to list all of the configured agents, illustrated below are the Agents required for the sample configuration. At least one Agent login-id is required for each skill group

```
list agent-loginID
                               AGENT LOGINID
Login ID     Name           Extension     Dir Agt  AAS/AUD        COR Ag Pr SO
               Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

6001         inbound Agent  unstaffed                               1   lvl
                  1/01     /       /       /       /       /       /       /
6002         Outbound Agent unstaffed                               1   lvl
                  2/01     /       /       /       /       /       /       /
6003         Email Agent    unstaffed          3                    1   lvl
                  3/01     /       /       /       /       /       /       /
6005         Webchat Agent  unstaffed                               1   lvl
                  5/01     /       /       /       /       /       /       /
6006         Inbound Agent2 unstaffed                               1   lvl
                  1/01     /       /       /       /       /       /       /
6007         Outbound Agent2unstaffed                               1   lvl
                  2/01     /       /       /       /       /       /       /
```

5.8 Configure Agent Stations

For each station that agents will log in to, enter the command **change station n,** where **n** is the station extension. On **Page 4**, the following buttons must be assigned as shown below:

- **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 1604                                             Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                        Cord Length: 0
   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::
```

5.9 Administer CTI Stations

Presence Suite uses CTI stations via the AES to initiate calls on Communication Manager. The CTI stations will be used to places calls to customers for outbound campaigns as well as to place calls to agents in order to reserve an agent to handle the outbound call. Use the command **add station n**, enter a descriptive name for **Name**, set the **Type** field to **CTI,** enter a **Security Code** that Presence Suite will use to login as the station and enter **X** for the **Port**. Extensions 3500 to 3503 were created as CTI Stations.

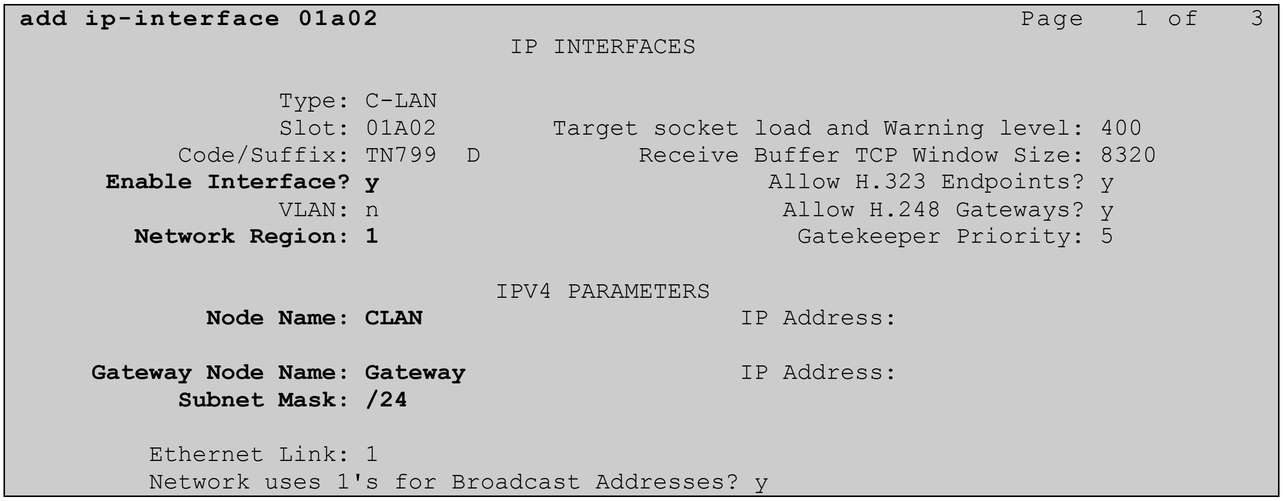
```
add station 3500                                             Page   1 of   5
                                     STATION

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
```

5.10 Configure CLAN for Avaya Aura® Application Enablement Services Connectivity

Define a node name for the CLAN by using the command **change node-names ip** and adding an IP address and node name for the CLAN.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AES522              10.10.16.25
CLAN                10.10.16.31
Gateway             10.10.16.1
```

Add the CLAN to the system configuration using the **add ip-interface n** command where **n** is the CLAN board location. Enter the CLAN node name assigned in the previous step to the **Node Name** field. Enter values for the **Subnet Mask** and **Gateway Address** fields. In this case, **/24** and **Gateway** are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** field to **y**, and use a separate **Network Region** for the CLAN dedicated for AES connectivity. Default values may be used in the remaining fields.

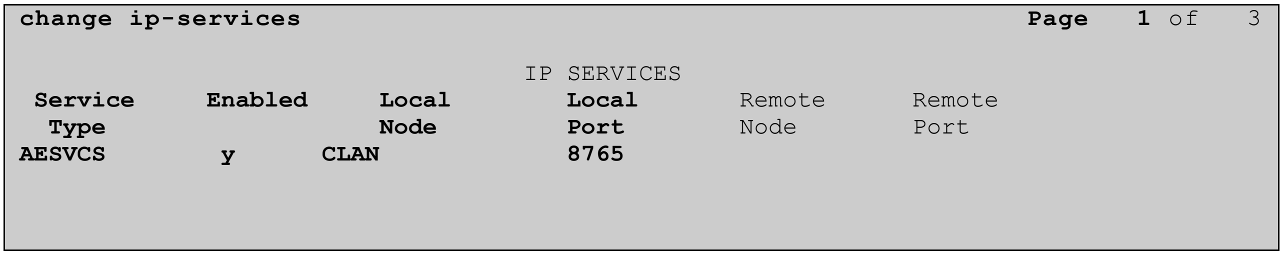


```
add ip-interface 01a02                                            Page   1 of   3
                                   IP INTERFACES

                  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                      IP Address:

    Gateway Node Name: Gateway                   IP Address:
          Subnet Mask: /24

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

5.11 Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**
- **Enabled:** set to **y**
- **Local Node:** set to the node name assigned for the CLAN in **Section 5.10**.
- **Local Port** Retain the default value of **8765**.

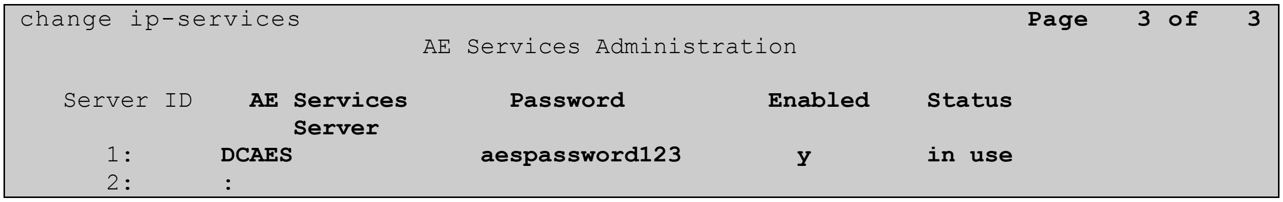


```
change ip-services                                                Page   1 of   3

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

Go to **Page 3** of the ip-services form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **DCAES**
- **Password:** Enter a password to be administered on the AES server
- **Enabled:** Set to **y**

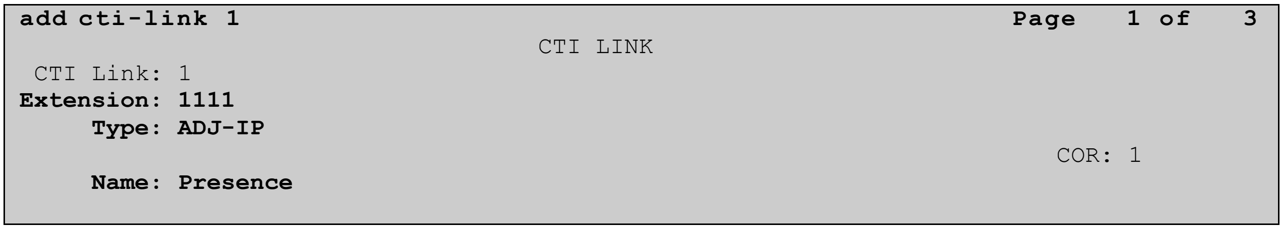
Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.



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

   Server ID    AE Services        Password          Enabled    Status
                   Server
      1:      DCAES             aespassword123        y         in use
      2:      :
```

5.12 Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.



```
add cti-link 1                                                  Page   1 of    3
                                  CTI LINK
 CTI Link: 1
Extension: 1111
     Type: ADJ-IP
                                                                   COR: 1
     Name: Presence
```

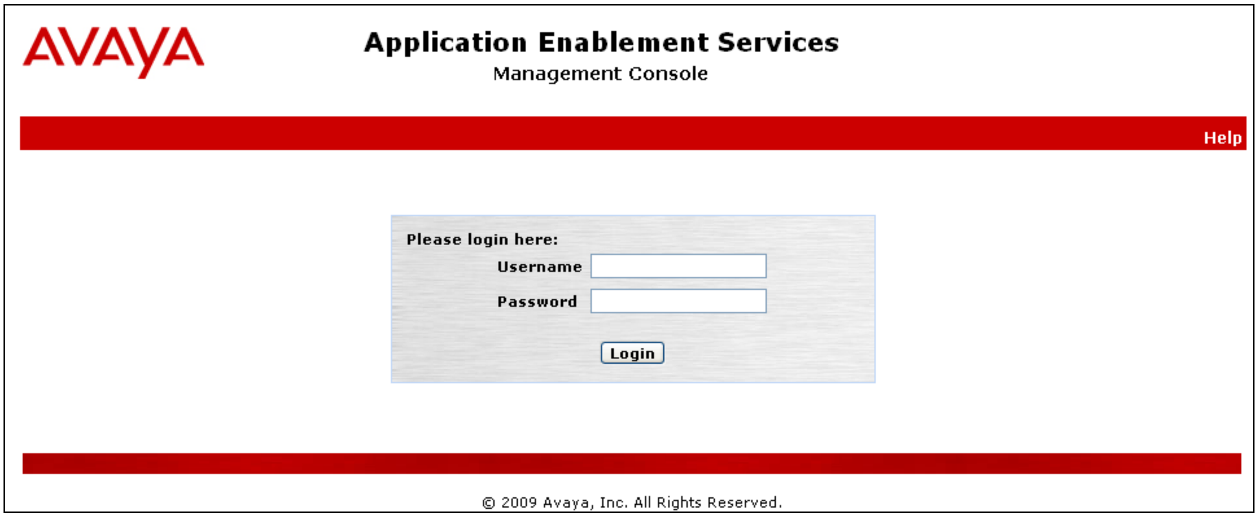
6 Configure Avaya Aura® Application Enablement Services Server

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

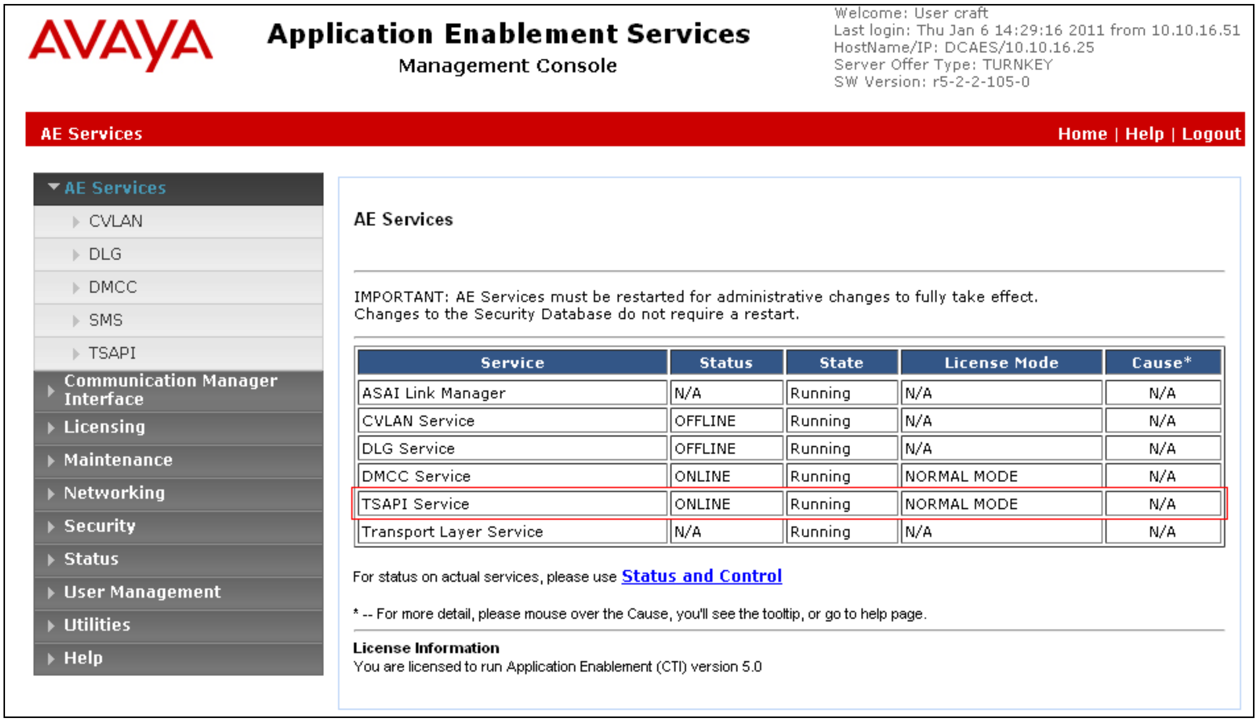
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable CTI Link User
- Identify Tlinks

6.1 Verify Licensing

To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of AES. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Password
Login
© 2009 Avaya, Inc. All Rights Reserved.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). 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, contact an Avaya support representative to acquire the proper license for your solution.



Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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

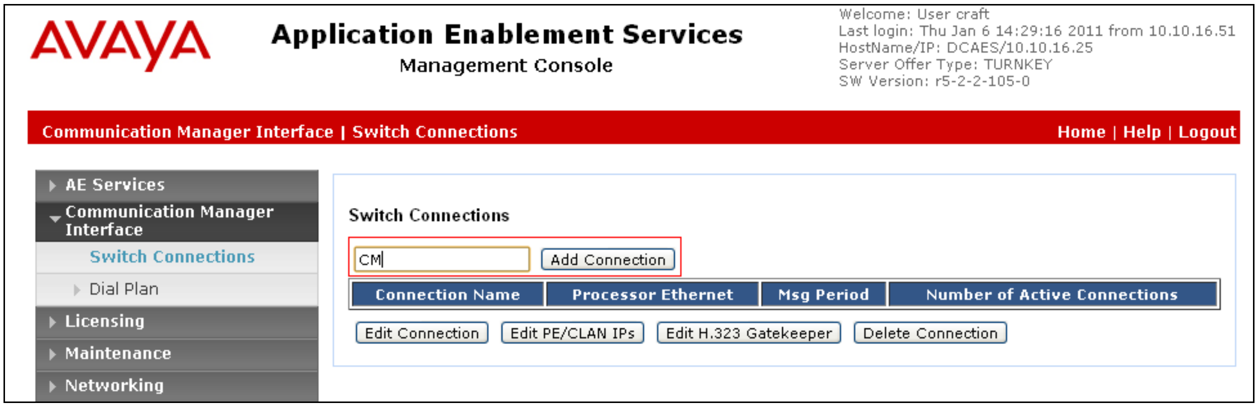
For status on actual services, please use Status and Control

* -- 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

6.2 Create Switch Connection

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



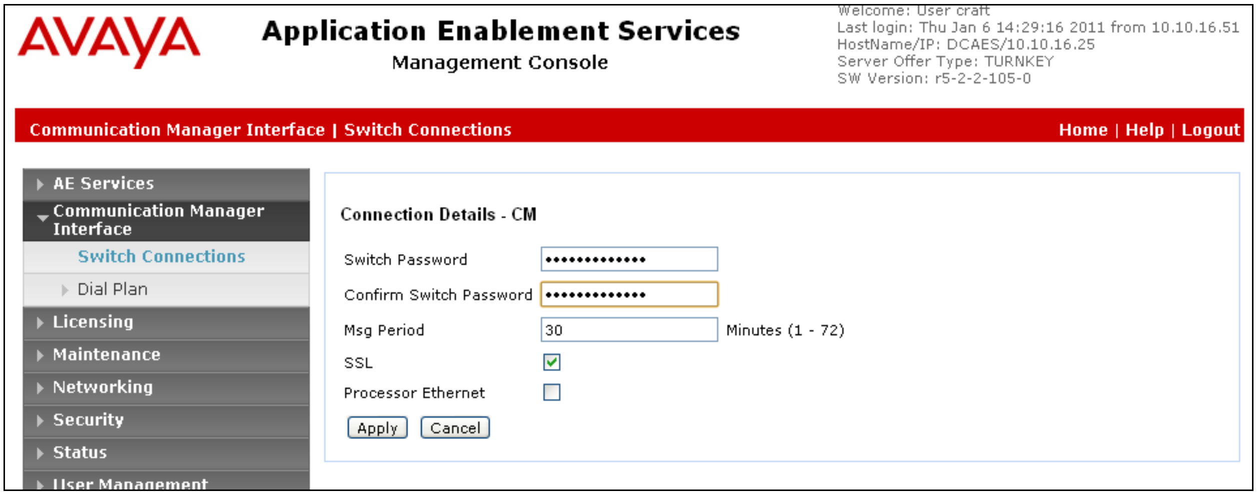
Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Switch Connections

CM

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

In the resulting screen enter the **Switch Password,** the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.11**. default values may be accepted for the remaining fields. Click **Apply** to save changes.

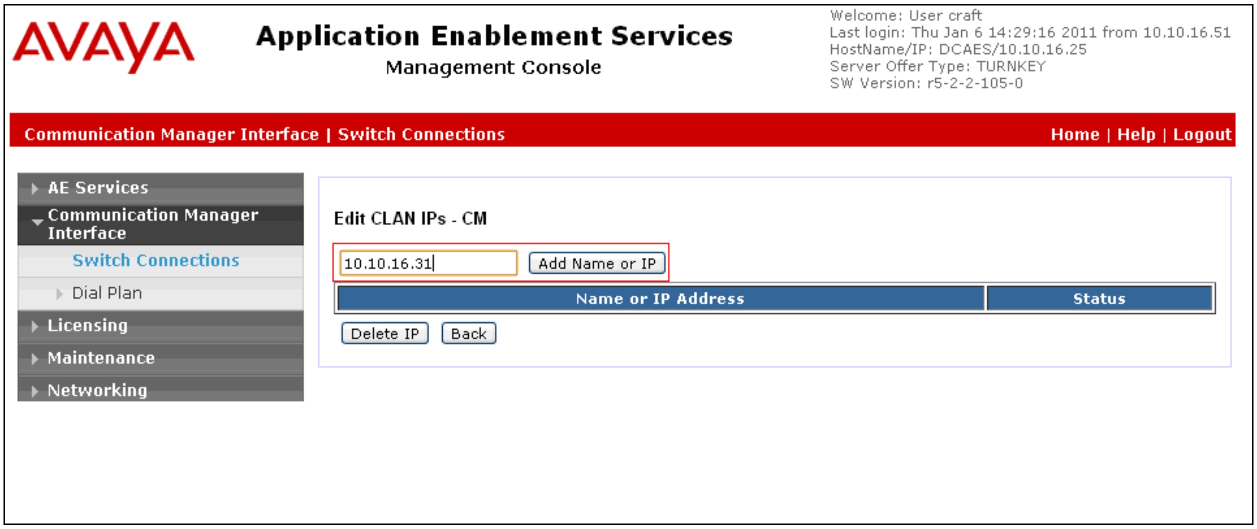


Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Connection Details - CM

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

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the CLAN that will be used for the AES connection and select the **Add Name or IP** button.

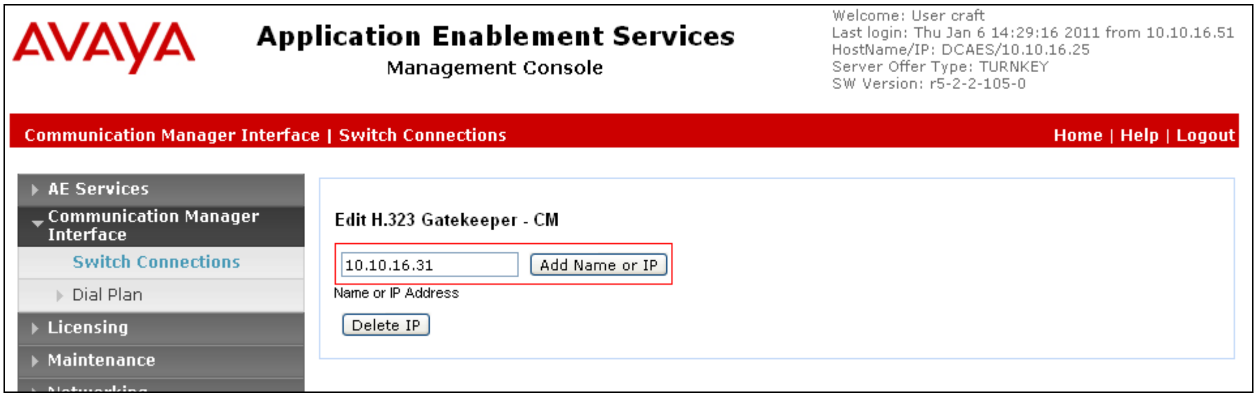


Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Edit CLAN IPs - CM

10.10.16.31

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 H.323 Gatekeeper** to display the screen below. Enter the IP Address and click **Add Name or IP** button as shown below.



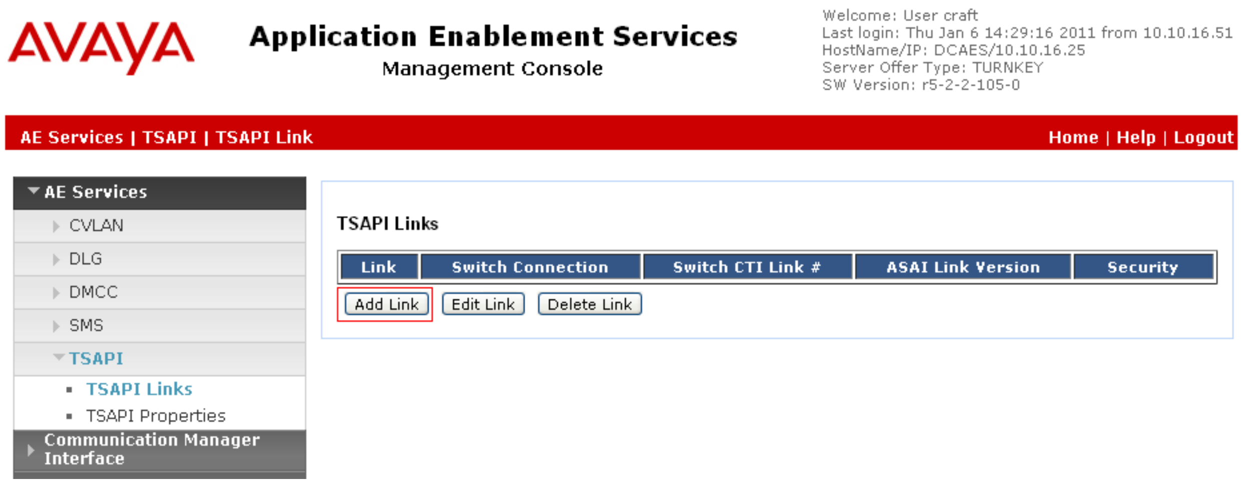
Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Edit H.323 Gatekeeper - CM

10.10.16.31

6.3 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.

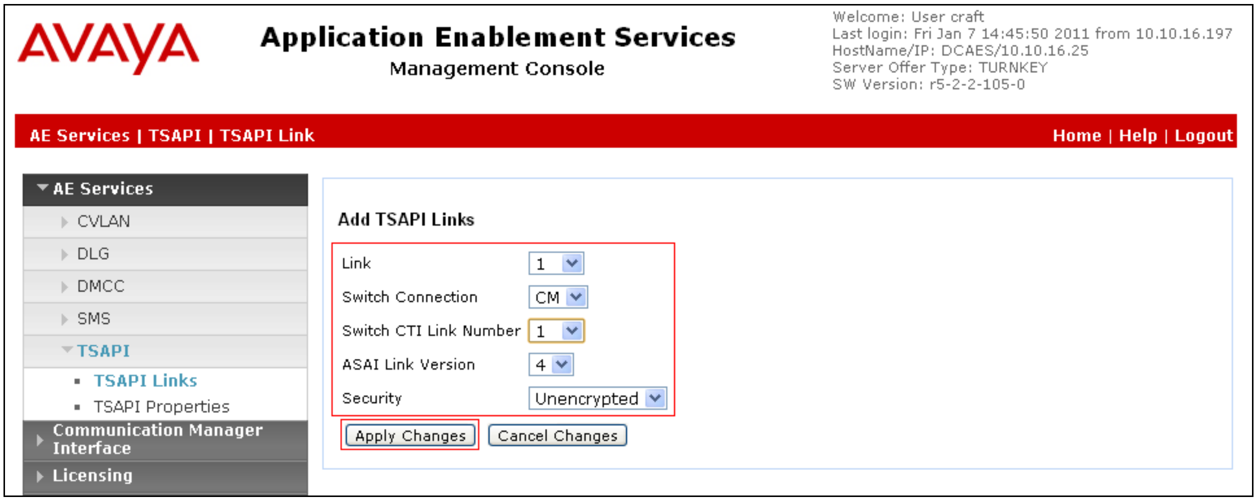


Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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 **CM**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.12** which is **1.**
- **ASAI Link Version:** This can be left at the default value of **4**.
- **Security:** This can be left at the default value of **Unencrypted.**

Once completed, select **Apply Changes**.

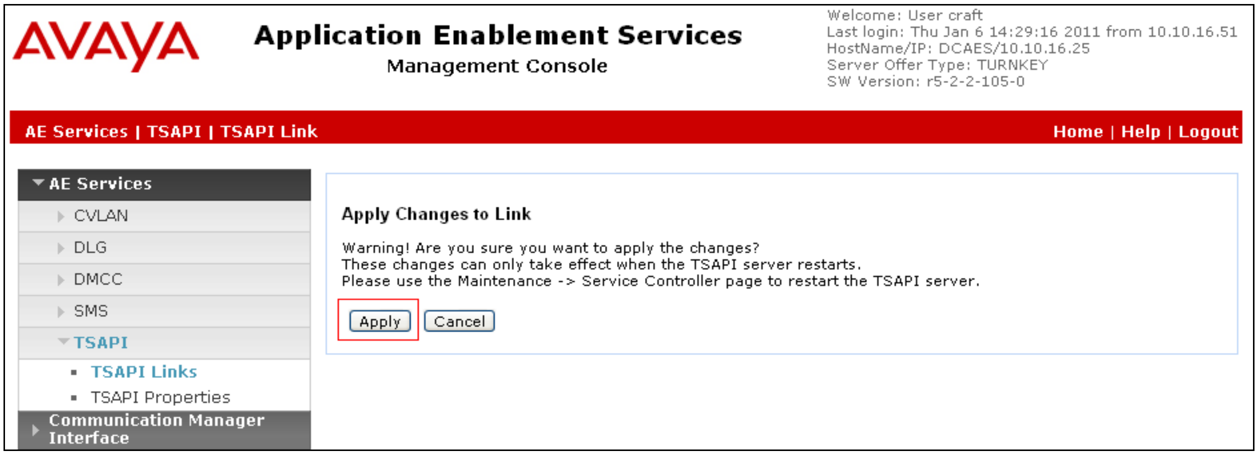


Welcome: User craft
Last login: Fri Jan 7 14:45:50 2011 from 10.10.16.197
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Add TSAPI Links

Link	1
Switch Connection	CM
Switch CTI Link Number	1
ASAI Link Version	4
Security	Unencrypted

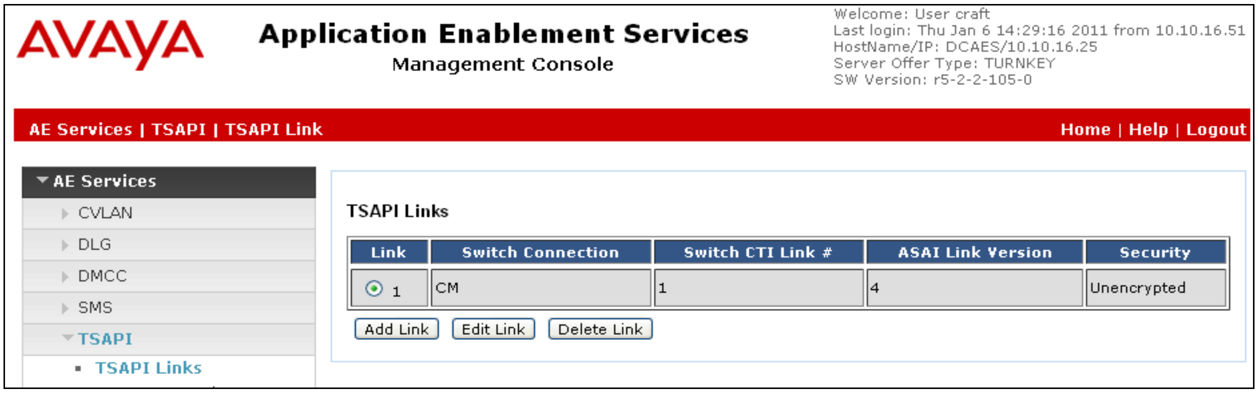
Another screen appears for confirmation of the changes. Choose **Apply**.


AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0
AE Services | TSAPI | TSAPI Link
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
TSAPI Properties
Communication Manager Interface
Apply
Cancel

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.

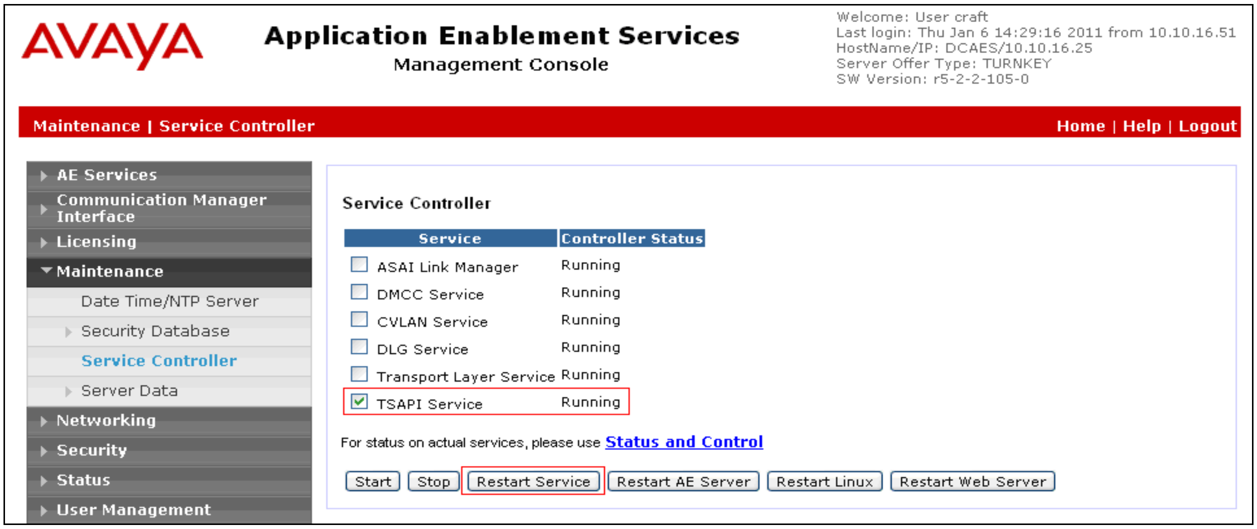
When the TSAPI Link is completed, it should resemble the screen below.


AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0
AE Services | TSAPI | TSAPI Link
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
Add Link
Edit Link
Delete Link

TSAPI Links

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

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



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

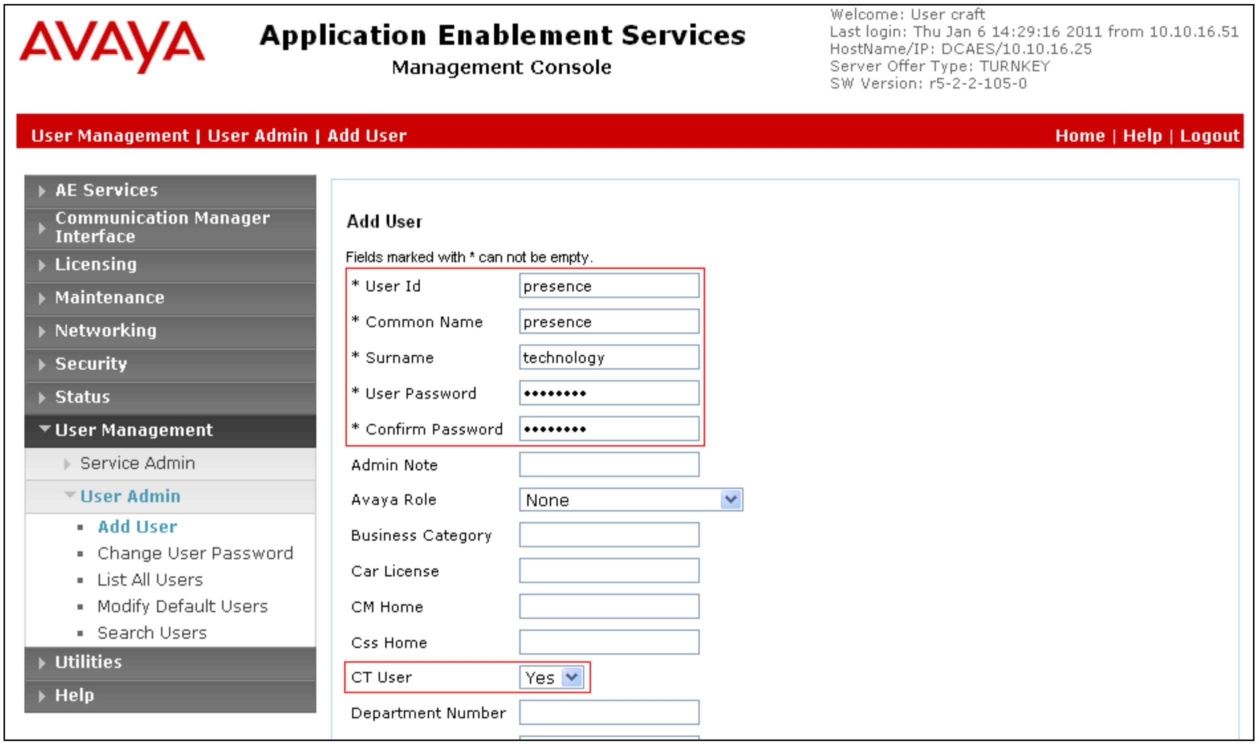
For status on actual services, please use Status and Control

6.4 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 7.1.**
- **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 7.1**.
- **CT User -** Select **Yes** from the drop-down menu.

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



Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Add User

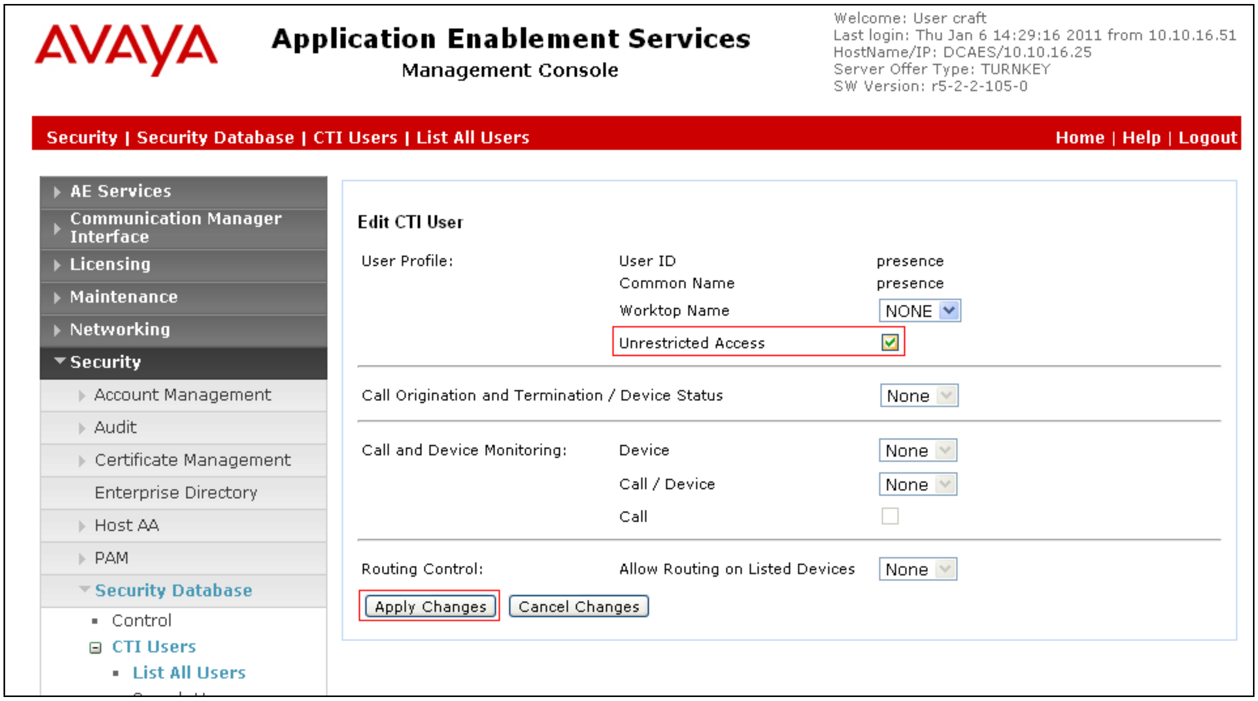
Fields marked with * can not be empty.

* User Id	presence
* Common Name	presence
* Surname	technology
* 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).

6.5 Enable Unrestricted Access for CTI 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 6.4** and select the **Edit** option (not shown). The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

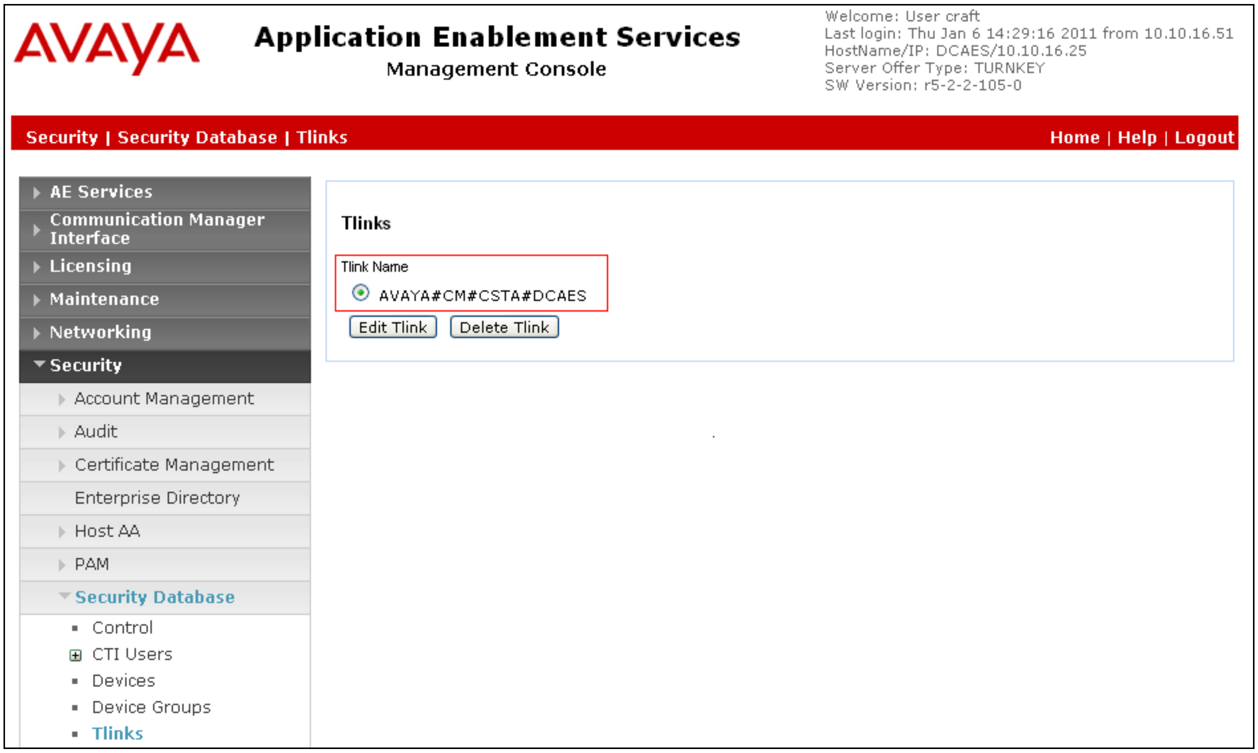
Edit CTI User

User Profile:	User ID	presence
	Common Name	presence
	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.

6.6 Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Presence Suite in **Section 7.1**.



Welcome: User craft
Last login: Thu Jan 6 14:29:16 2011 from 10.10.16.51
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Tlinks

Tlink Name

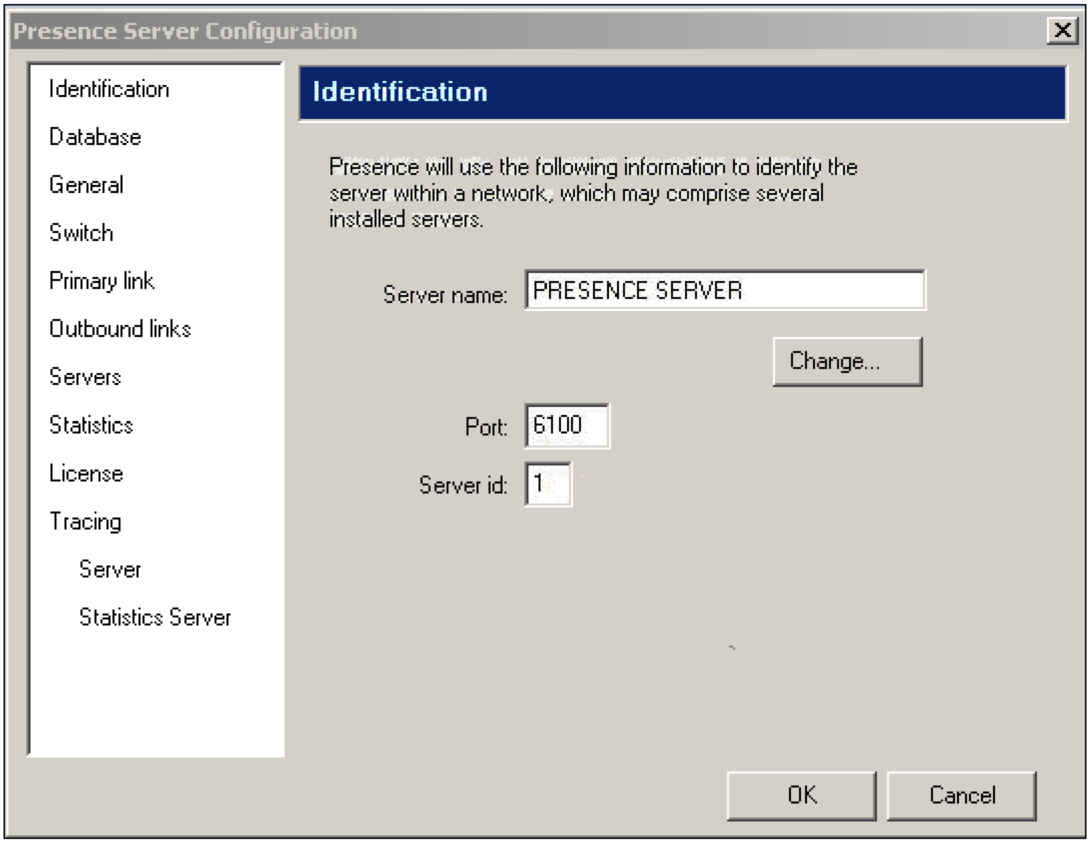
● AVAYA#CM#CSTA#DCAES

7 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.

7.1 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. Select the **Identification** option from 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.



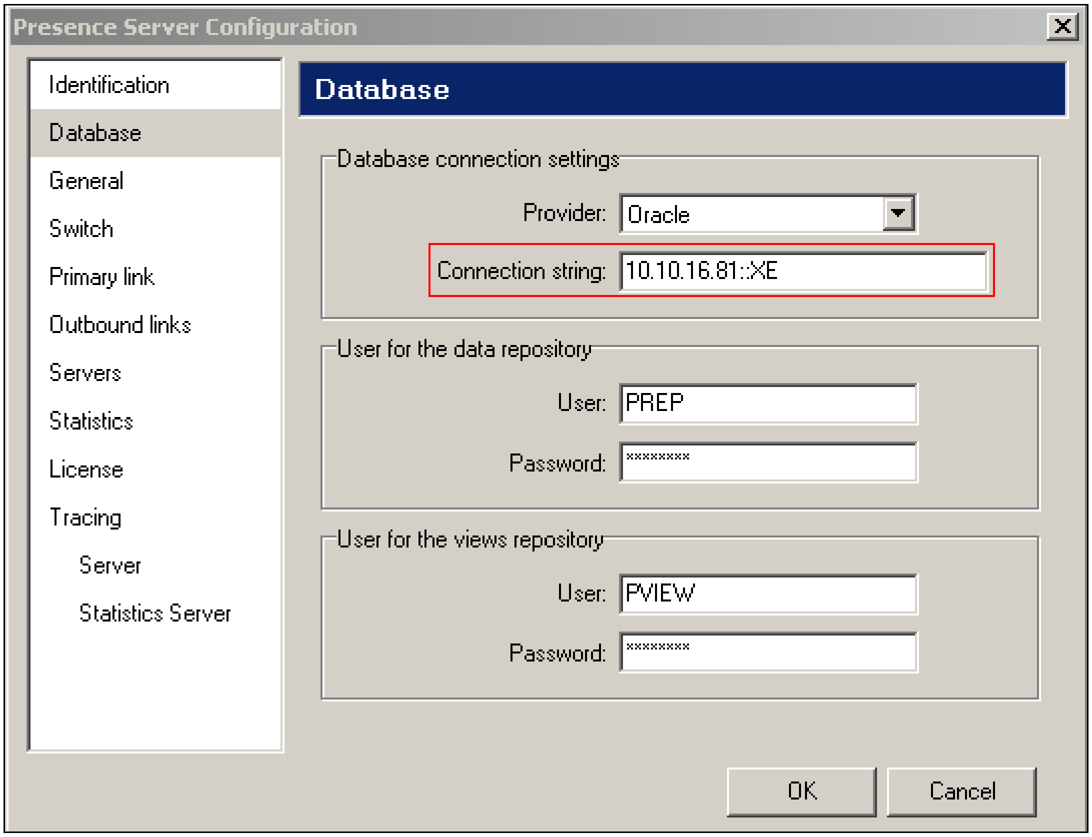
Presence will use the following information to identify the server within a network, which may comprise several installed servers.

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 two colons 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.



Presence Server Configuration

Database

Database connection settings

Provider: Oracle

Connection string: 10.10.16.81::XE

User for the data repository

User: PREP

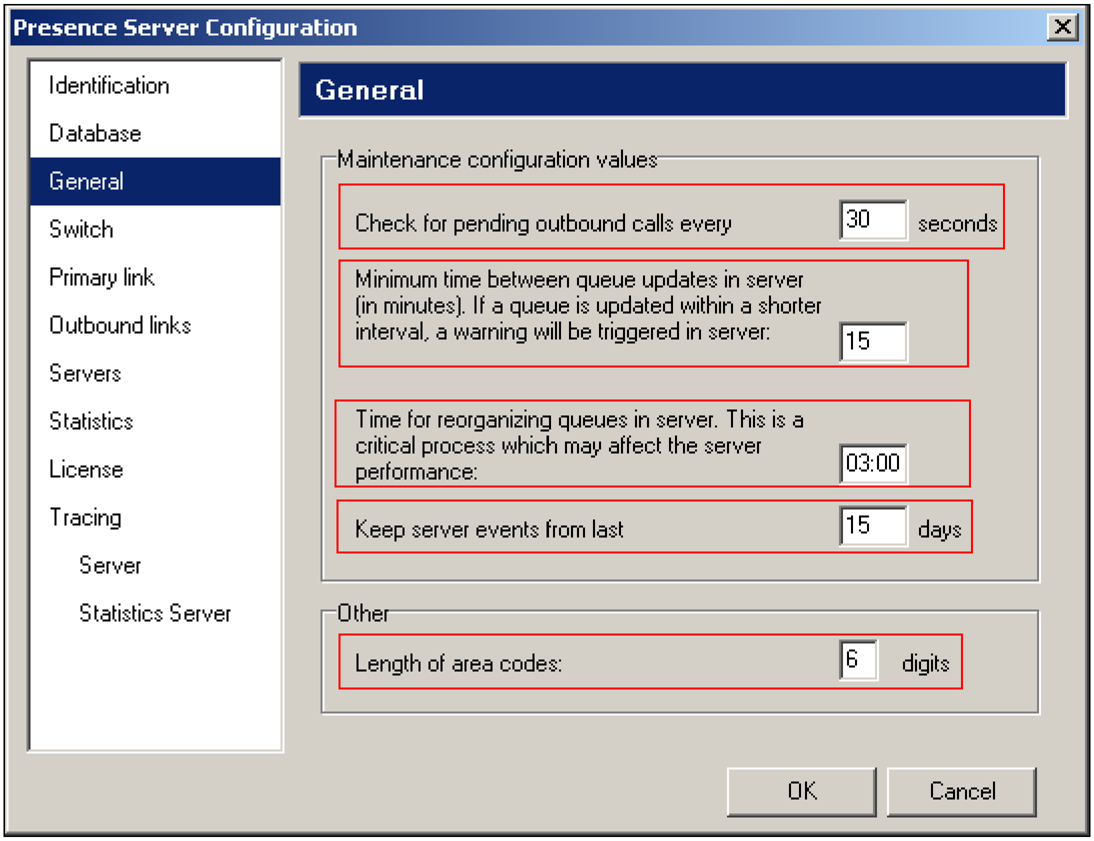
Password: ********

User for the views repository

User: PVIEW

Password: ********

Select **General** from the menu on the left side of the screen. If desired the Maintenance configuration values can be altered here, for the interoperability test the default values were retained.



Maintenance configuration values

Check for pending outbound calls every 30 seconds

Minimum time between queue updates in server (in minutes). If a queue is updated within a shorter interval, a warning will be triggered in server: 15

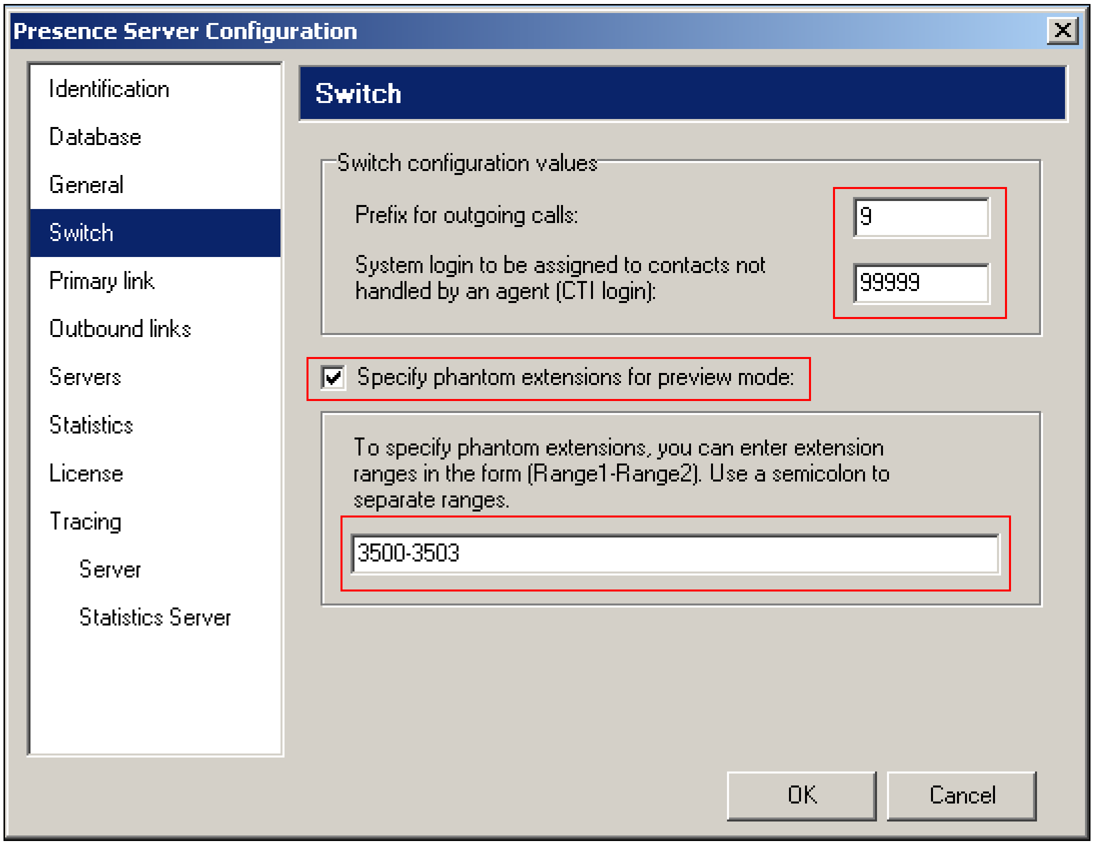
Time for reorganizing queues in server. This is a critical process which may affect the server performance: 03:00

Keep server events from last 15 days

Other

Length of area codes: 6 digits

Select the **Switch** option from the menu on the left side of the screen. If required, enter a value in the **Prefix for outgoing calls** field**,** in this example the ARS feature access code of **9** was used. The **System login to be assigned to contacts not handled by an agent (CTI login)** field should be set to a value supplied by Presence, the value used for this configuration is **99999**. Check the **Specify phantom extension for preview mode** checkbox and enter the phantom extensions configured in **Section 5.9**.



Switch

Switch configuration values

Prefix for outgoing calls: 9

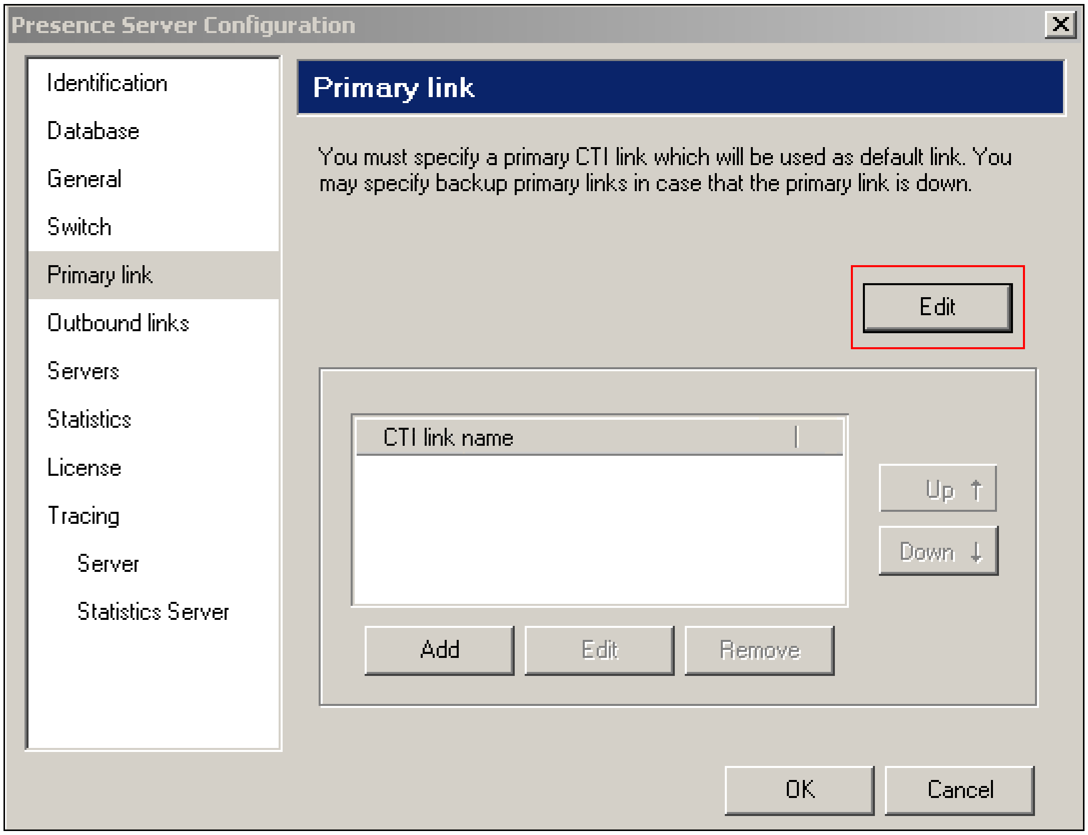
System login to be assigned to contacts not handled by an agent (CTI login): 99999

☑ 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.

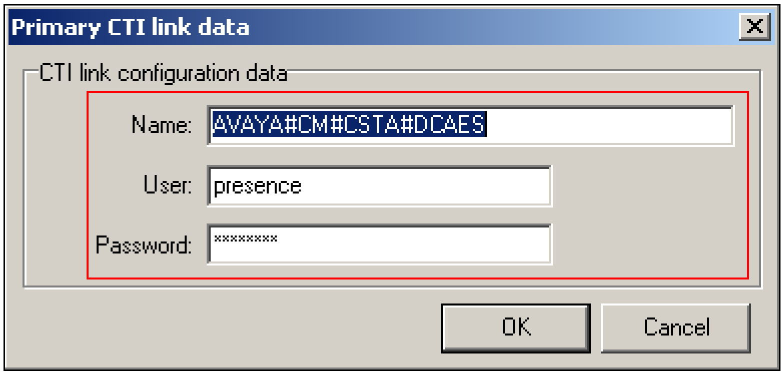
3500-3503

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

In the resulting pop-up box enter the Tlink name from **Section 6.6** in the **Name** field. For the **User** and **Password** fields enter the user name and password configured on the Application Enablement Services in **Section 6.4**. Click **OK**.



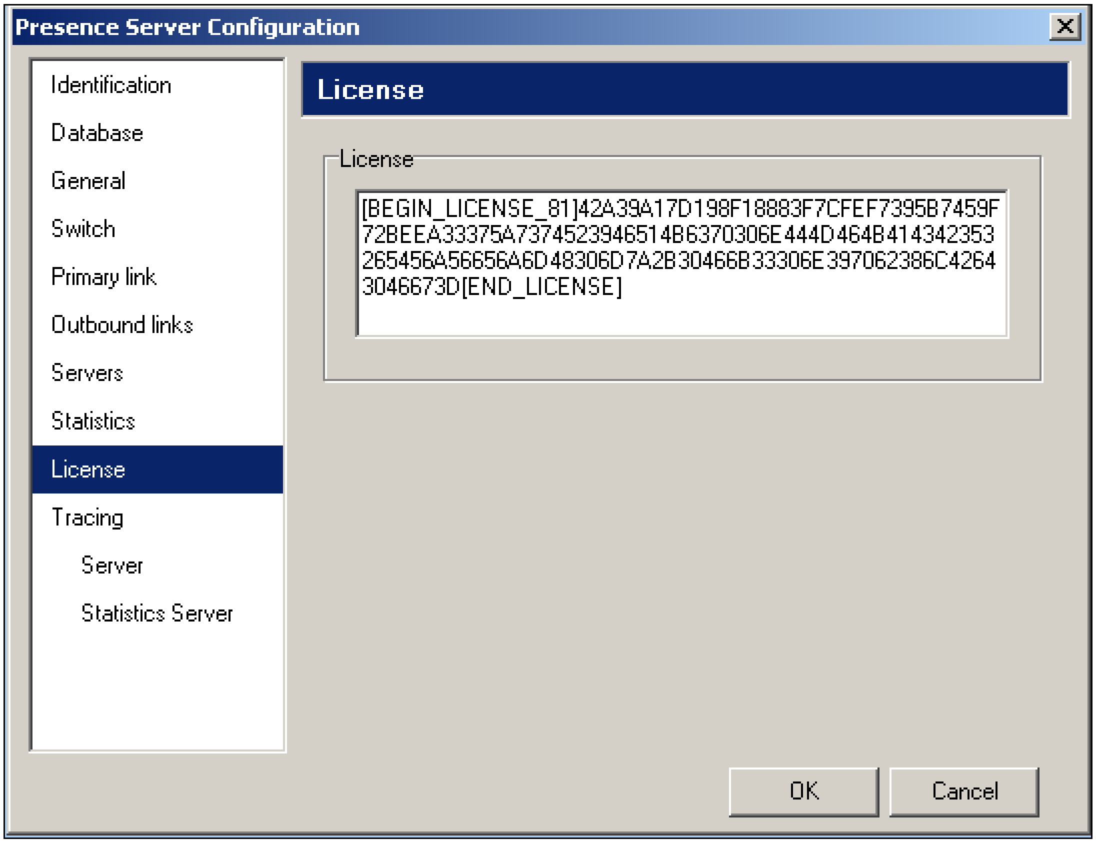
Name: AVAYA#CM#CSTA#DCAES

User: presence

Password: ********

Click on the **License** option on the menu on the left side of the screen and enter a license key.

Note: License keys can be obtained from Presence Technology by using the contact details in **Section 2.3**. Click **OK**.

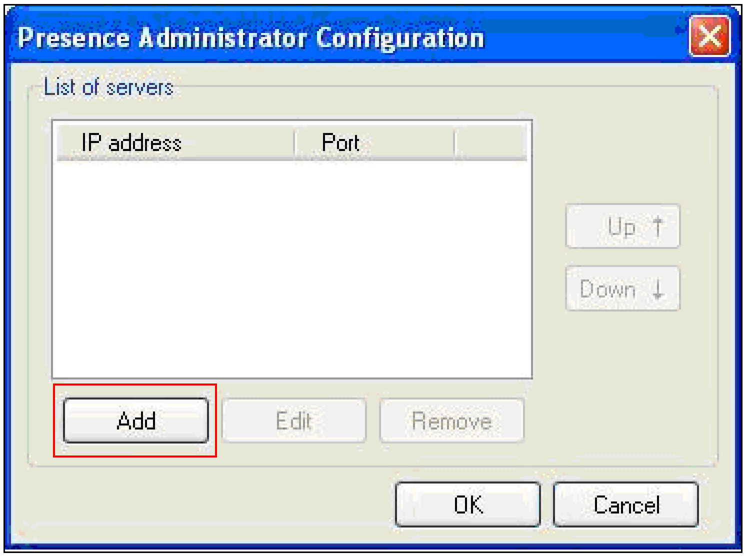


License

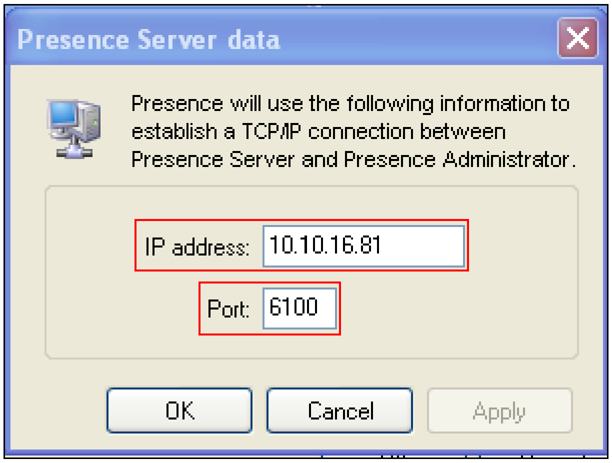
```
[BEGIN_LICENSE_81]42A39A17D198F18883F7CFEF7395B7459F
72BEEA33375A737452394651 4B6370306E444D464B414342353
265456A56656A6D48306D7A2B30466B33306E397062386C4264
3046673D[END_LICENSE]
```

7.2 Presence Administrator Configuration

Launch the Presence Administrator Configuration application by double clicking the **pcoadmincfg.exe** located in the **C:** → **Presence** install folder. Click the **Add** button in the Presence Administrator Configuration screen.



Enter the Presence Server IP Address in the **IP address** field, in this case **10.10.16.81**. Ensure the Presence Server **Port** value of **6100** matches the value set in **Section 7.1**. Click **OK**.



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

IP address: 10.10.16.81

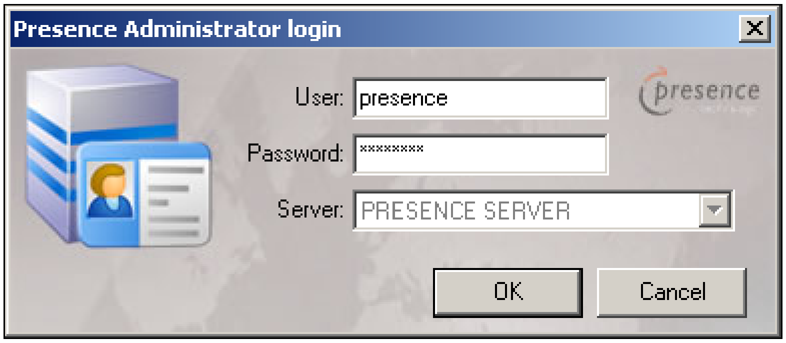
Port: 6100

7.3 Campaign Configuration

A number of services for inbound, outbound, email and internet were configured via the Presence Administrator. This section covers the basic configuration for each type of service. Please refer to **Section 10** for detailed documentation on configuring Presence Suite services.

7.3.1 Logging in to 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.



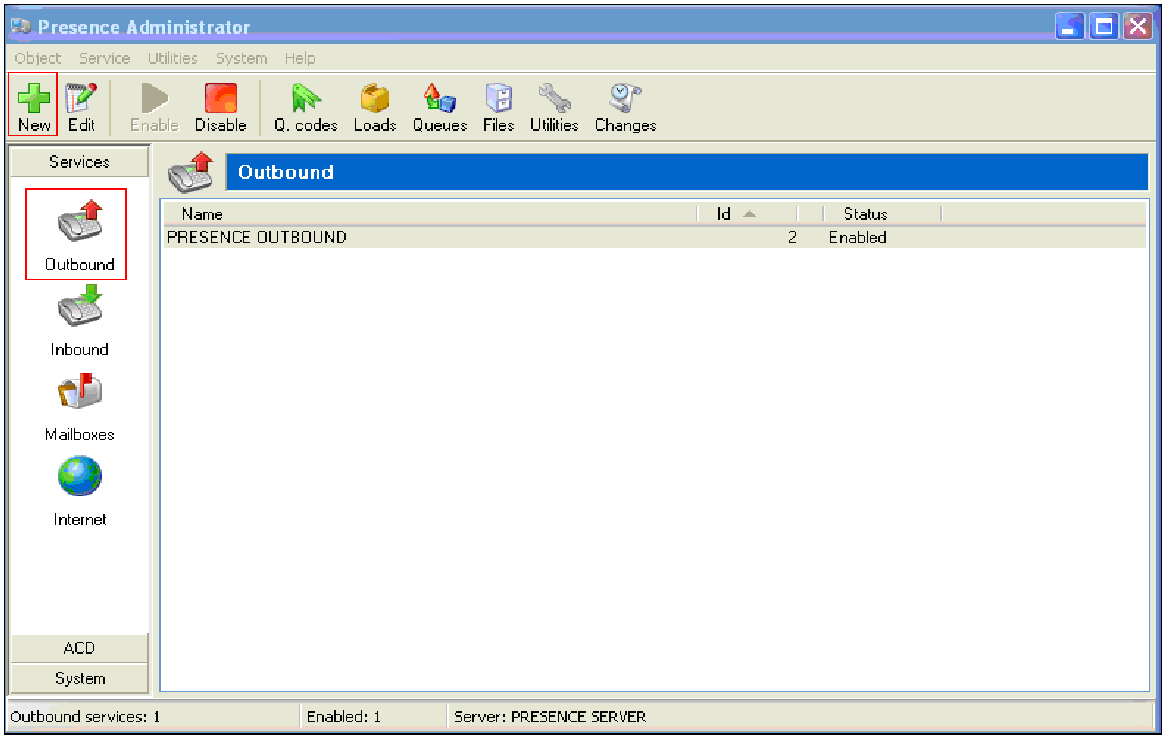
User: presence

Password: ********

Server: PRESENCE SERVER

7.3.2 Outbound Campaign

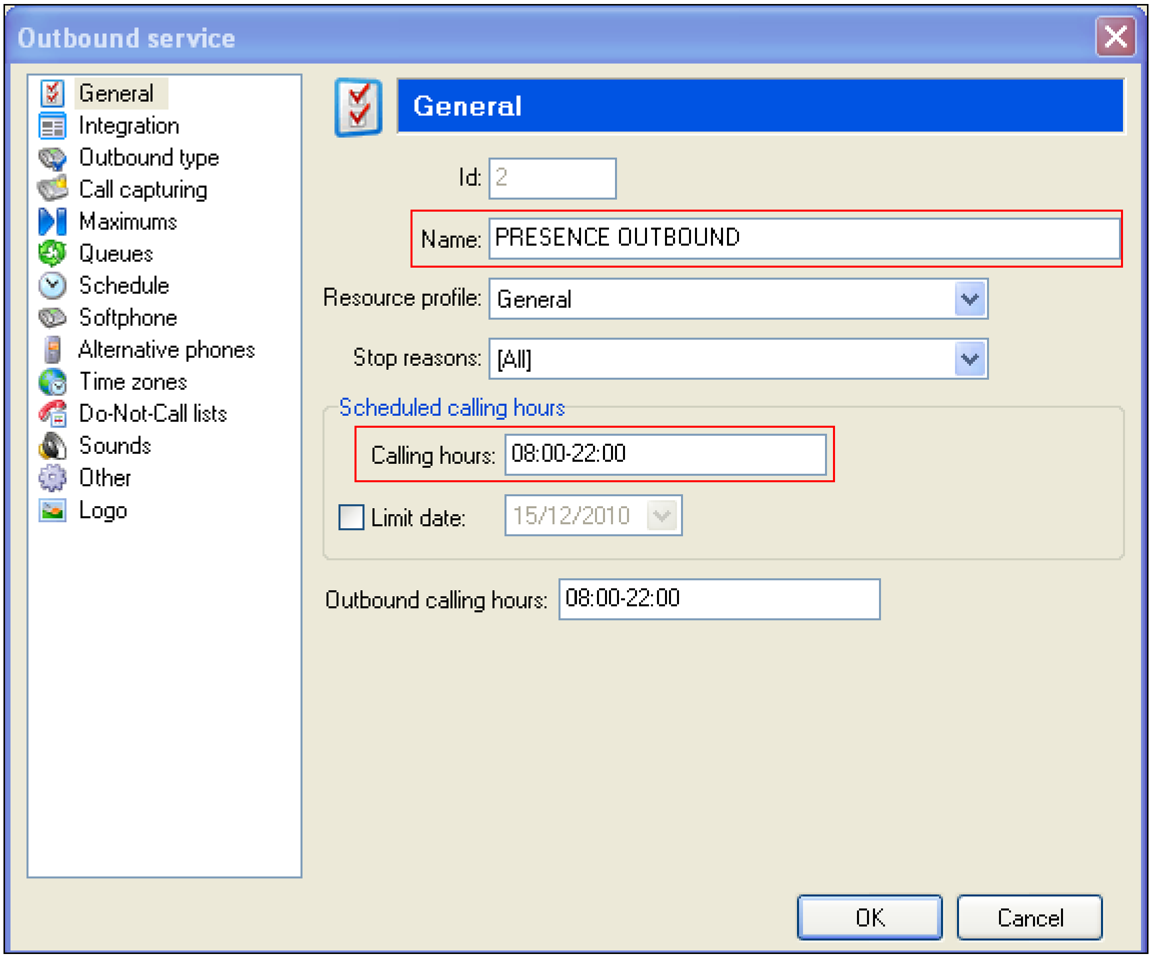
After logging in to Presence Administrator the following screen will be displayed. Select **Services →Outbound** from the Presence Administrator main menu on the left hand side. Click the **New** button to configure an outbound campaign.



Name	Id	Status
PRESENCE OUTBOUND	2	Enabled

Outbound services: 1 | Enabled: 1 | Server: PRESENCE SERVER

In the resulting screen, select general from the menu on the left hand side and enter a **Name** for the outbound campaign. In the **Calling hours** field set the time range for which the outbound Campaign will be active. All other fields are left with their default values.



Id: 2

Name: PRESENCE OUTBOUND

Resource profile: General

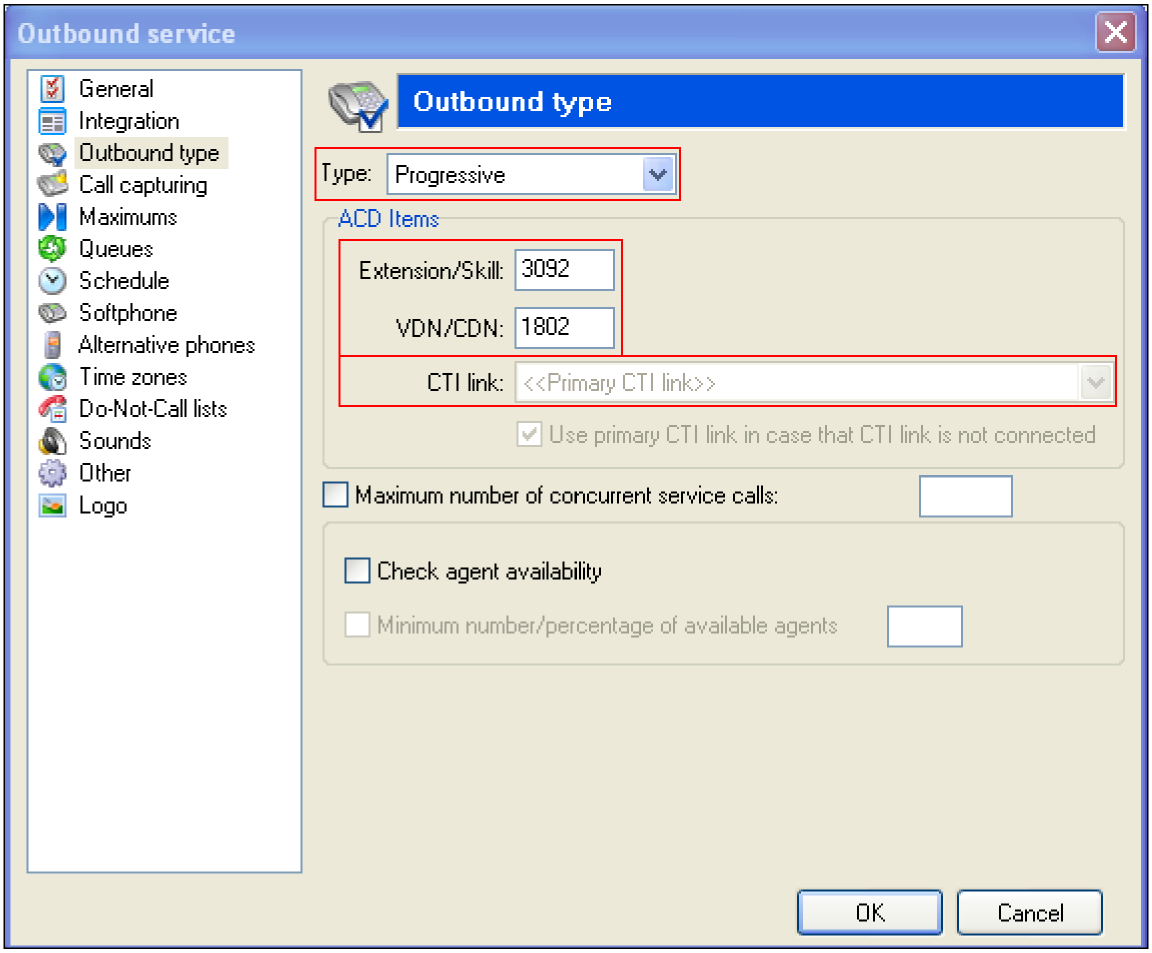
Stop reasons: [All]

Calling hours: 08:00-22:00

□ Limit date: 15/12/2010

Outbound calling hours: 08:00-22:00

Select **Outbound Type** from the left hand side menu and moving to the right, select the **Type** of outbound campaign, this specifies the mode in which the outbound campaign will operate, for further details of the type of outbound campaign available please refer to documentation in **Section 10**. In the **Extension/Skill** field enter the extension number assigned to the outbound skill group defined in **Table 2, Section 5.5**. In the **VDN/CDN** field enter the VDN number assigned to Outbound calls defined in **Table 2, Section 5.5**. In the test configuration only one CTI link was configured so the **CTI Link** filed is set to **<<Primary CTI Link>>** if multiple CTI links exist on the system then the specific CTI link can be specified. All other field may be left at their default values.



Outbound type

Type: Progressive

ACD Items

Extension/Skill: 3092

VDN/CDN: 1802

CTI link: <<Primary CTI link>>

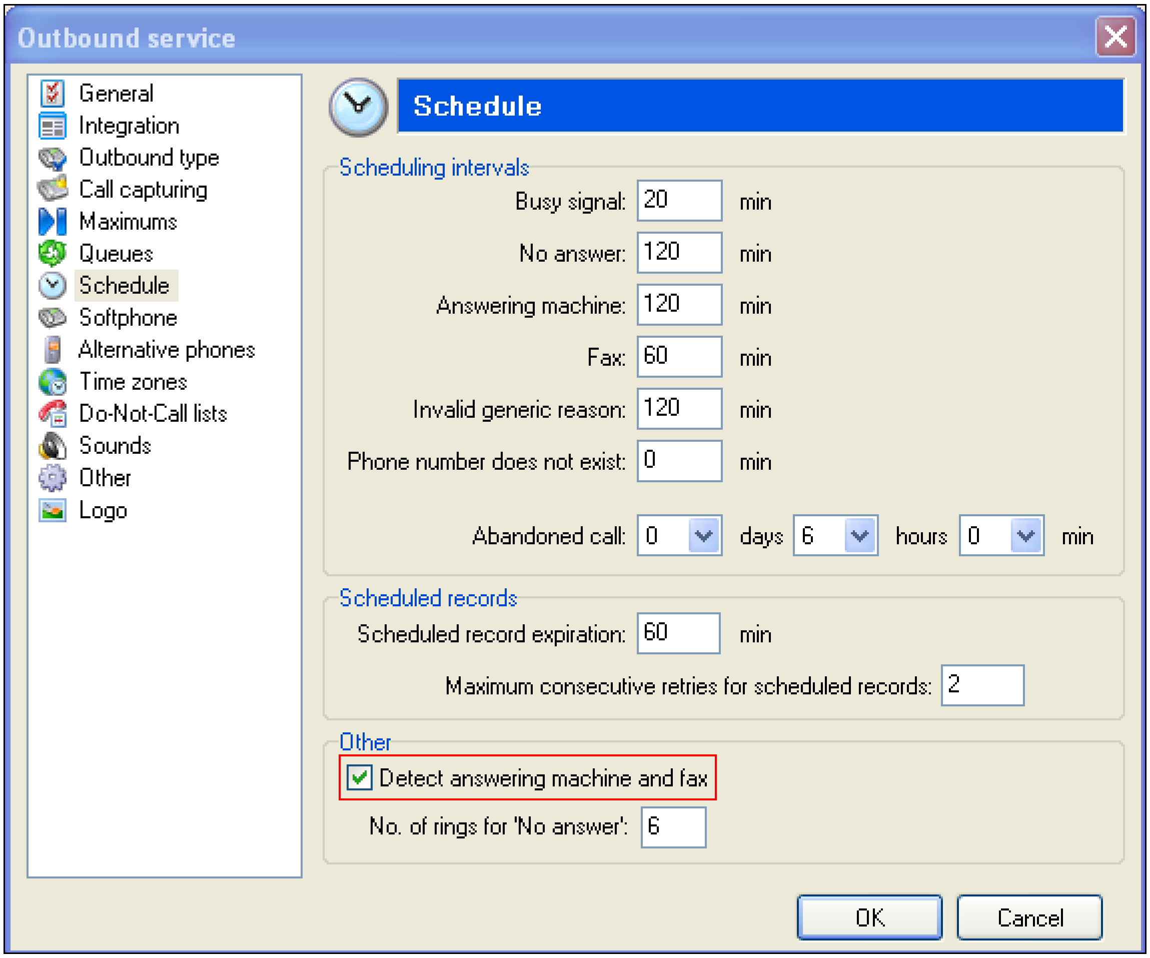
☑ Use primary CTI link in case that CTI link is not connected

□ Maximum number of concurrent service calls:

□ Check agent availability

□ Minimum number/percentage of available agents

Select **Schedule** from the left hand side menu. The fields in the right hand side define how the outbound campaign should behave following an un-successful attempt at contacting the customer. For testing, the **Detect answering machine and fax** box was checked with default values accepted for all other fields, as shown in the screen below. Click **OK** to complete the outbound campaign configuration.



Schedule

Scheduling intervals

Busy signal: 20 min

No answer: 120 min

Answering machine: 120 min

Fax: 60 min

Invalid generic reason: 120 min

Phone number does not exist: 0 min

Abandoned call: 0 days 6 hours 0 min

Scheduled records

Scheduled record expiration: 60 min

Maximum consecutive retries for scheduled records: 2

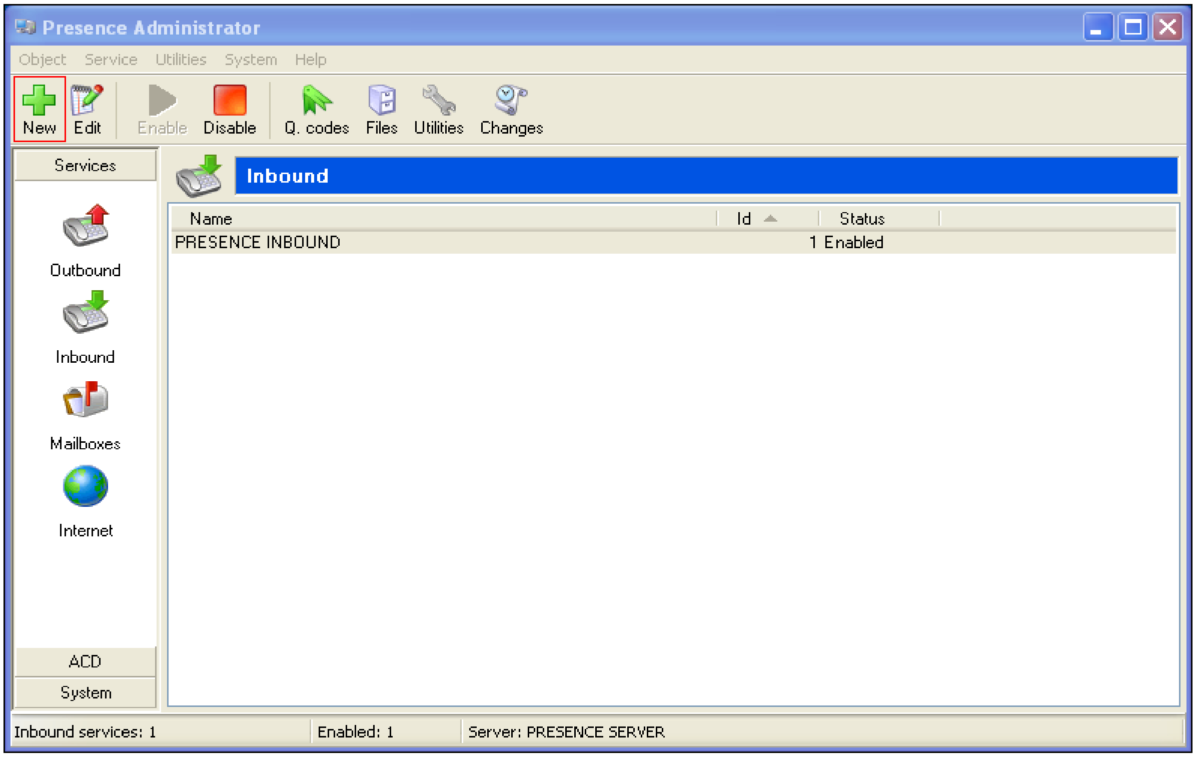
Other

☑ Detect answering machine and fax

No. of rings for 'No answer': 6

7.3.3 Inbound Campaign

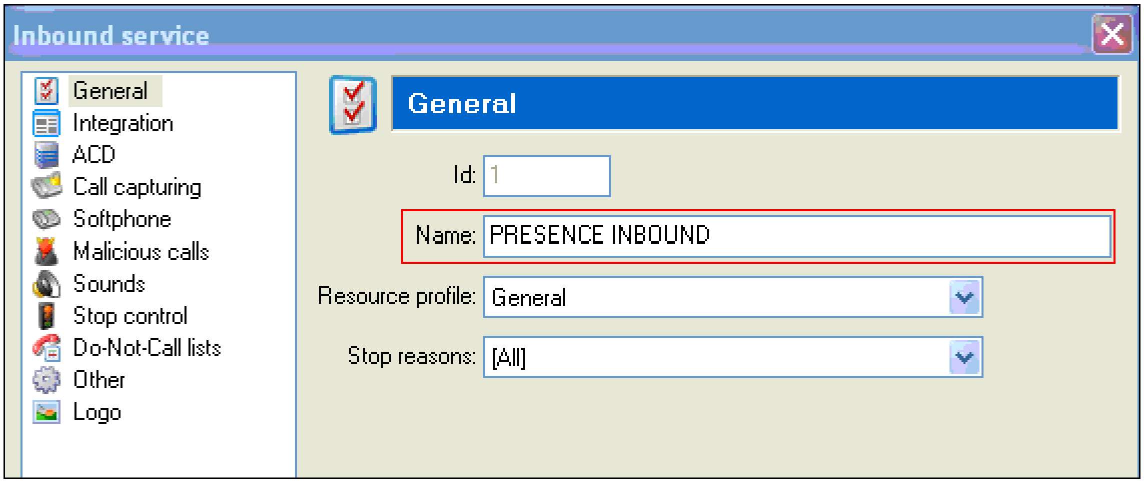
To configure an inbound campaign, from the left hand side select **Services →Inbound** from the Presence Administrator main menu. Click the **New** button.



Name	Id	Status
PRESENCE INBOUND	1	Enabled

Inbound services: 1 Enabled: 1 Server: PRESENCE SERVER

In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the inbound campaign. All other fields are left with their default values.



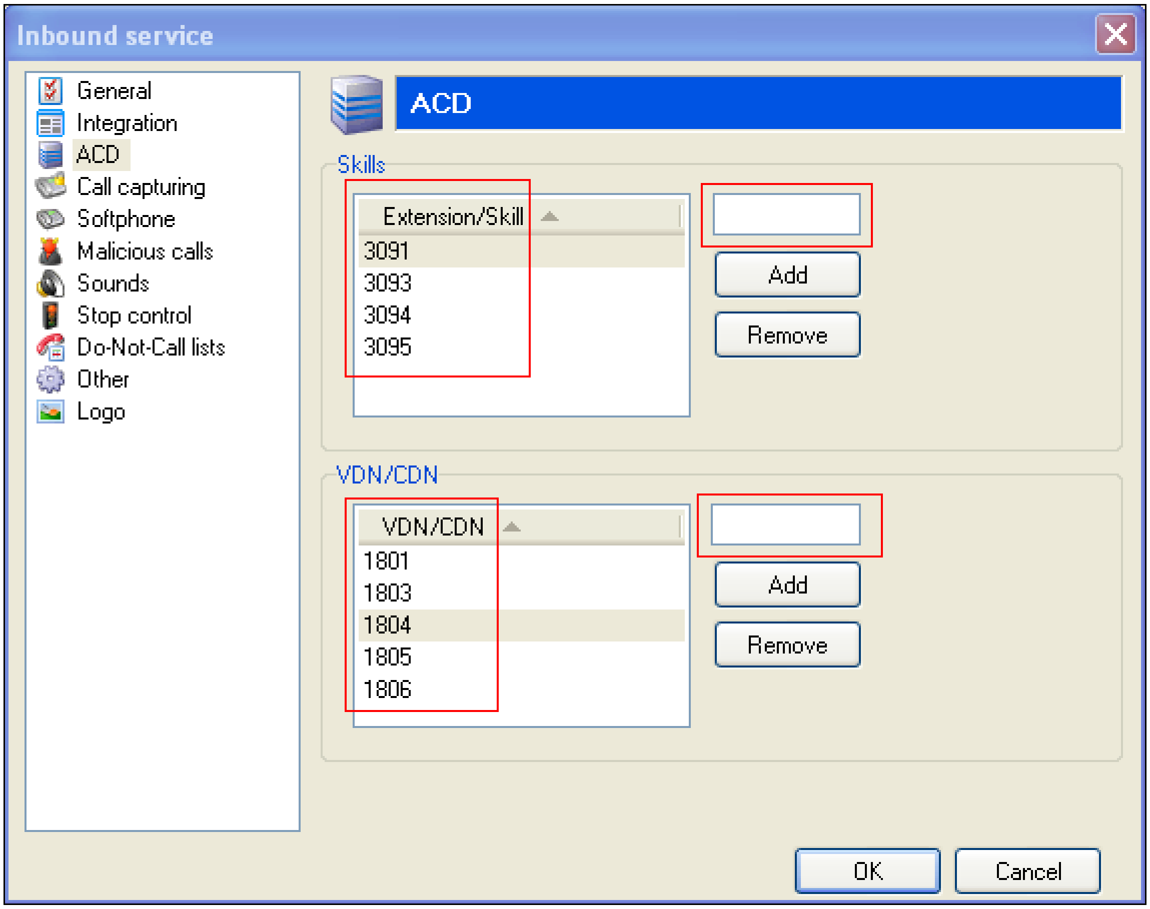
Id: 1

Name: PRESENCE INBOUND

Resource profile: General

Stop reasons: [All]

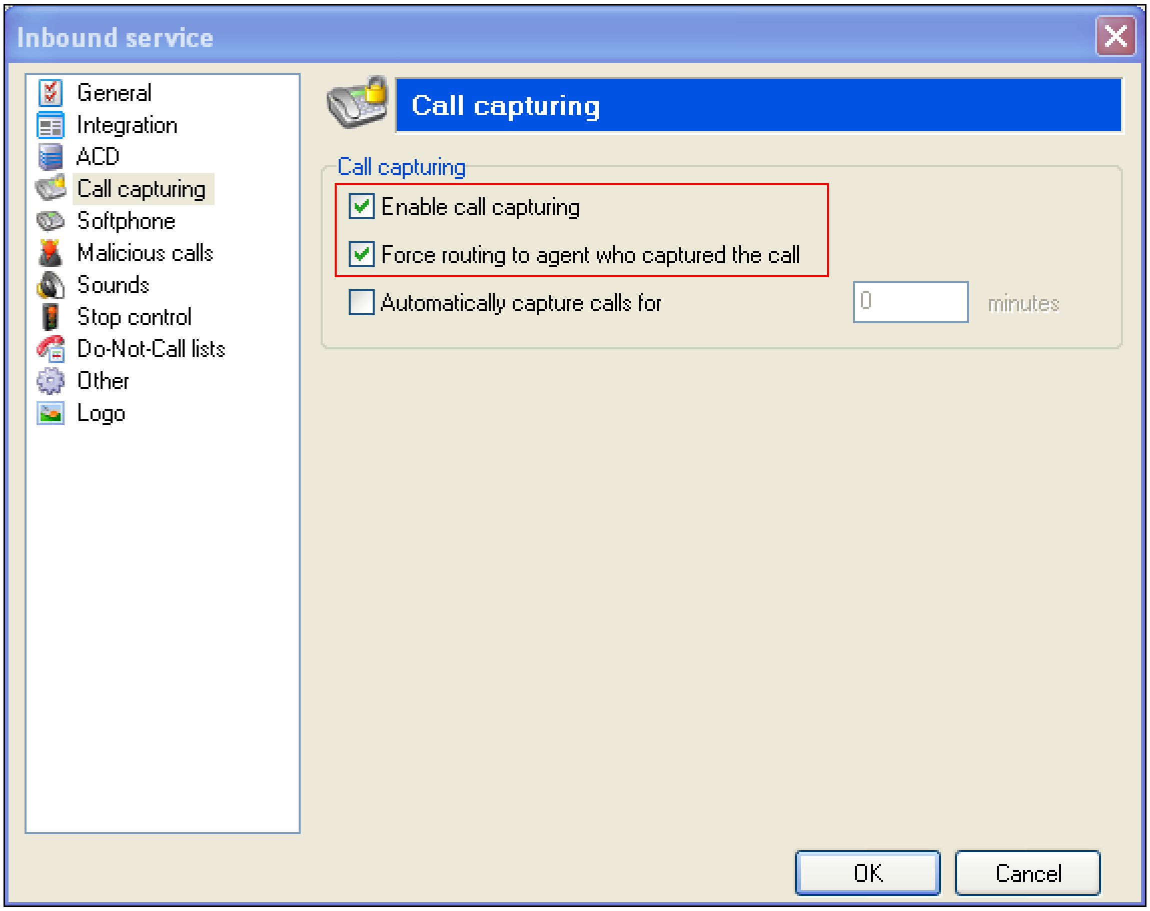
Select **ACD** from the left hand side menu and moving to the right, under the heading **Skills** enter the skill group extensions that will handle inbound calls in the untitled box (this includes email and web chat call types) and click **Add**. The skill group extensions will then appear to the left in the **Extension/Skill** box. Under the heading **VDN/CDN** enter the agent login IDs that will handle inbound calls in the untitled box and click **Add.** The agent login IDs will then appear to the left in the **VDN/CDN** box.



Extension/Skill
3091
3093
3094
3095

VDN/CDN
1801
1803
1804
1805
1806

Select **Call capturing** from the left hand side menu and moving to the right, select the **Enable call capturing** and **Force routing to agent who captured the call** check box's. These options allow an agent to mark an inbound call so that if the caller rings back while that agent is logged on the call will be routed again to the agent who tagged the call.



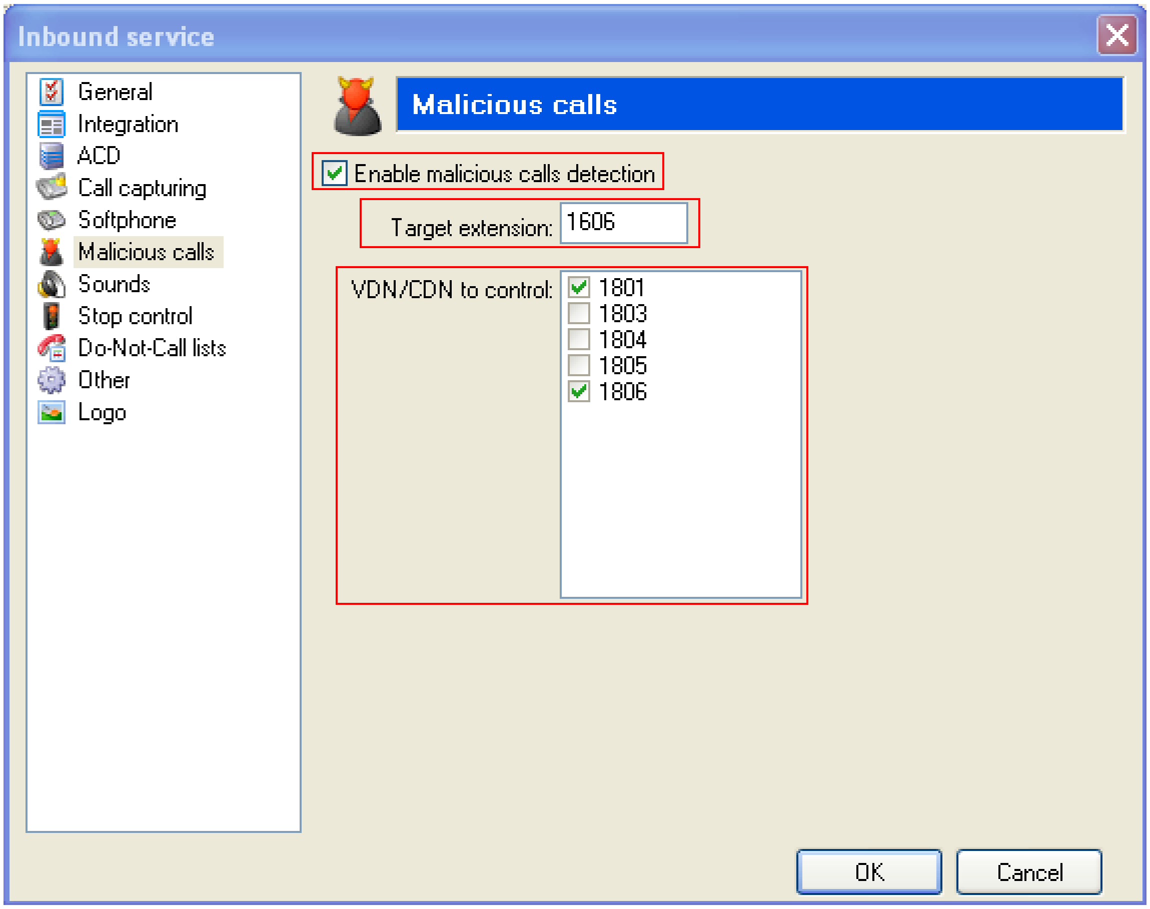
Call capturing

☑ Enable call capturing

☑ Force routing to agent who captured the call

□ Automatically capture calls for 0 minutes

Select **Malicious calls** from the left hand side menu and moving to the right, select the **Enable malicious calls detection** check box**.** This option allows agents to mark calls as malicious, so that the caller can be directed to another location such as a supervisor position if they call back again. In the **Target extension** field enter the extension that any malicious calls will be re-directed to. In the **VDN/CDN to control** field select the VDNs this option will be available on.

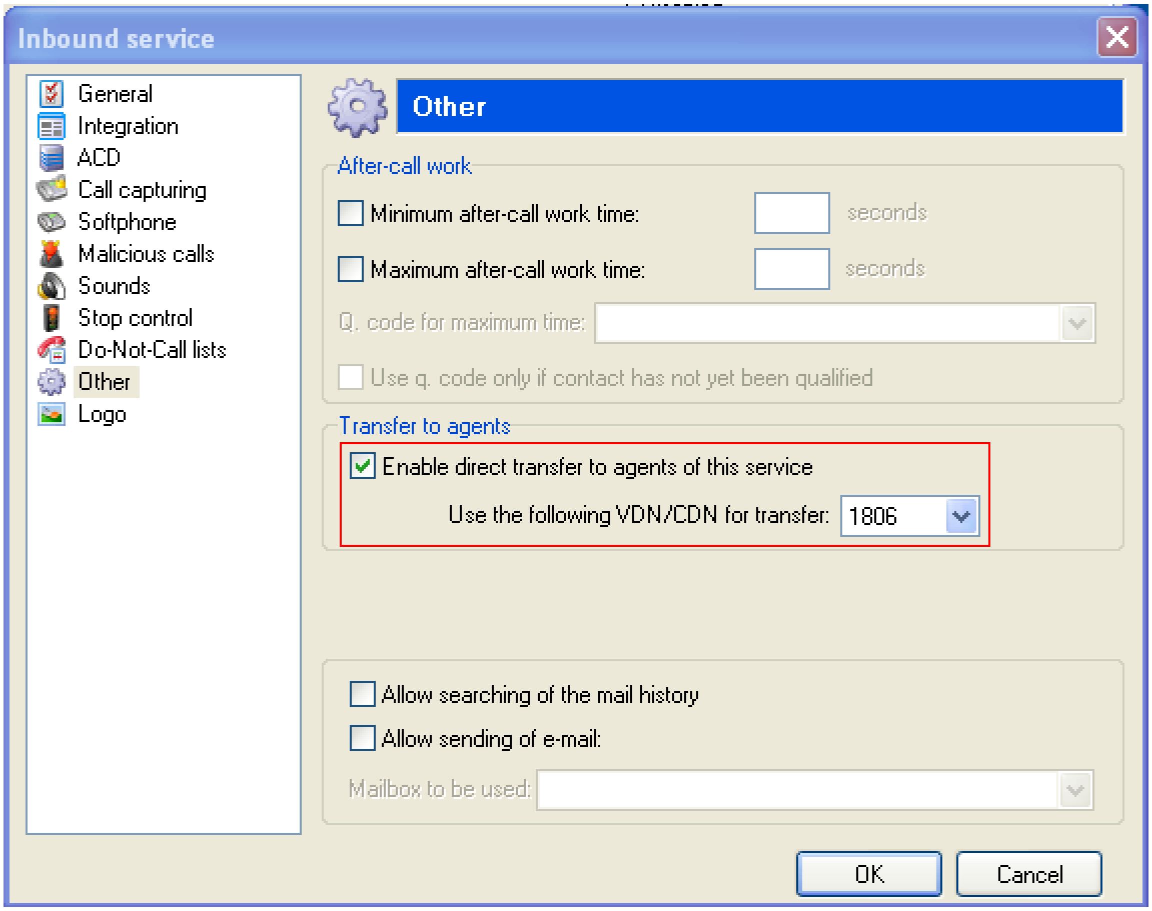


☑ Enable malicious calls detection

Target extension: 1606

VDN/CDN to control:
☑ 1801
☐ 1803
☐ 1804
☐ 1805
☑ 1806

Select **Other** from the left hand side menu and moving to the right, select the **Enable direct transfer to agents of this service** check box. Enter the direct agent transfer VDN assigned in **Table 2, Section 5.5** in the **Use the following VDN/CDN for transfer** field. Click **OK** to complete the inbound campaign configuration**.**



Other

After-call work

☐ Minimum after-call work time: seconds

☐ Maximum after-call work time: seconds

Q. code for maximum time:

☐ Use q. code only if contact has not yet been qualified

Transfer to agents

☑ Enable direct transfer to agents of this service

Use the following VDN/CDN for transfer: 1806

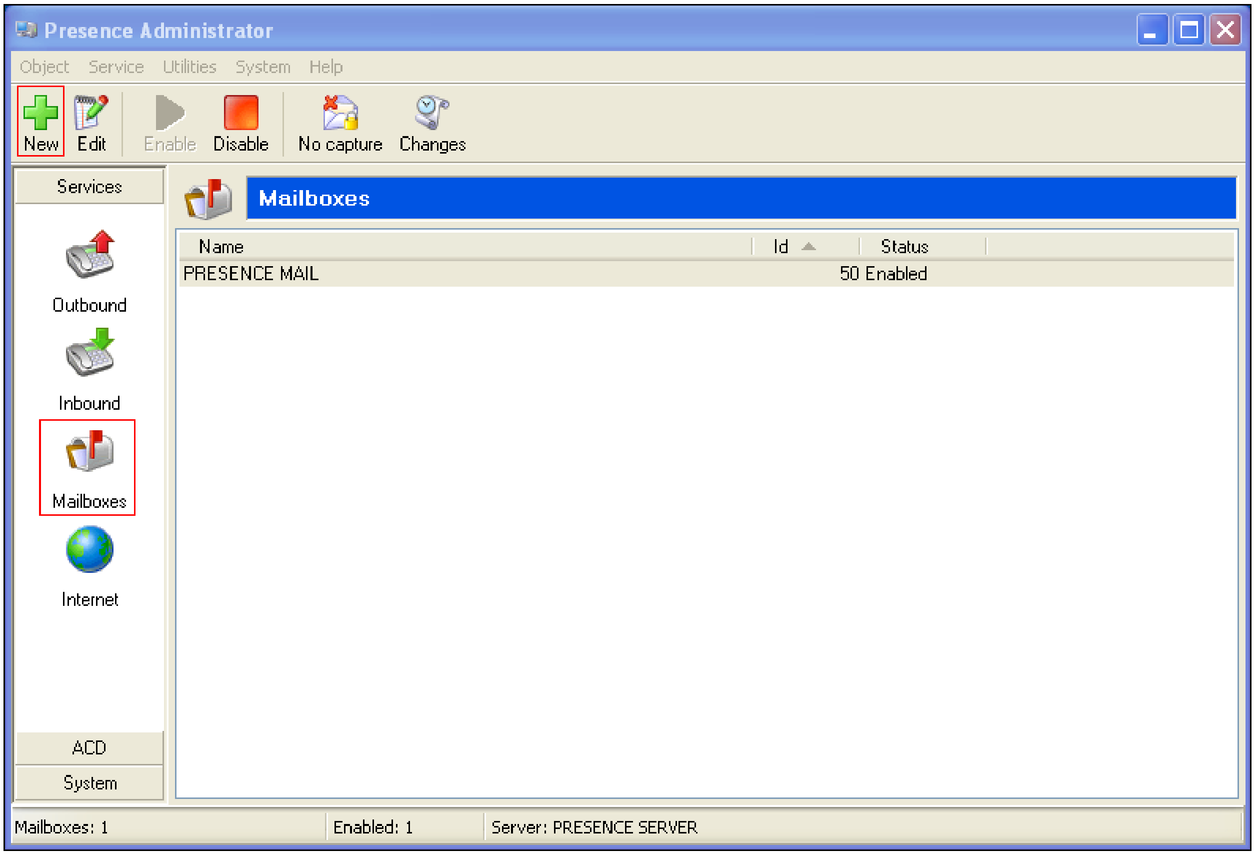
☐ Allow searching of the mail history

☐ Allow sending of e-mail:

Mailbox to be used:

7.3.4 Email Campaign

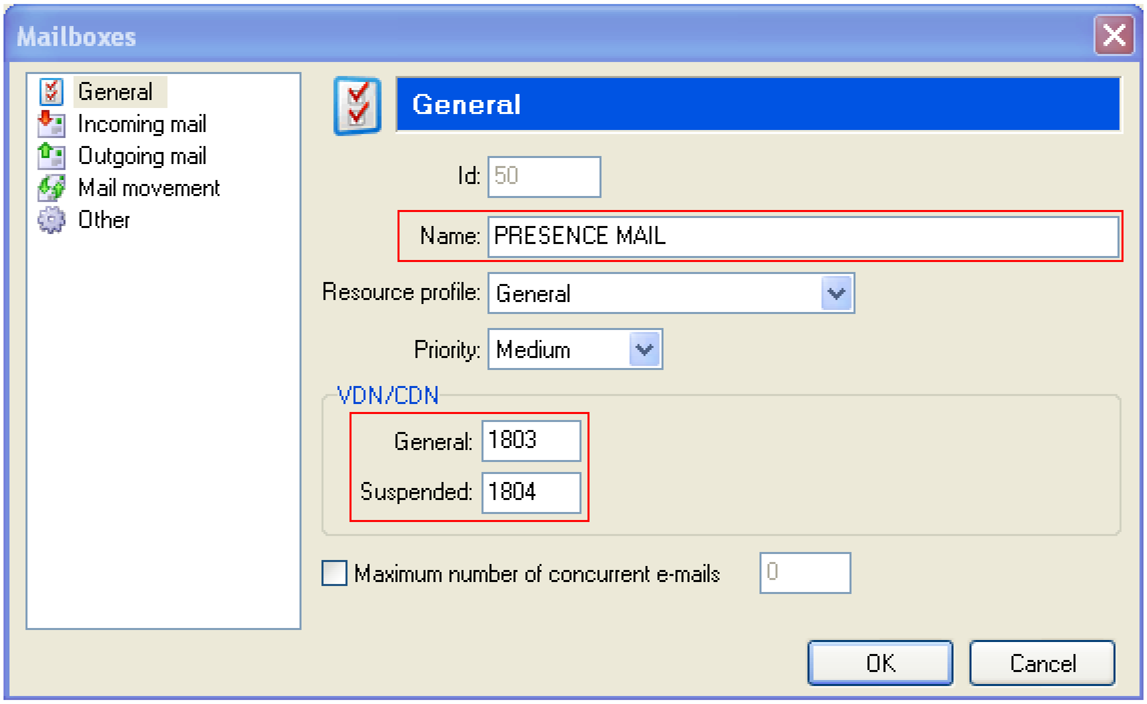
To configure an email campaign, from the left hand side select **Services → Mailboxes** from the Presence Administrator main menu. Click the **New** button.



Name	Id	Status
PRESENCE MAIL	50	Enabled

Mailboxes: 1 | Enabled: 1 | Server: PRESENCE SERVER

In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the email campaign. Referring to **Table 2, Section 5.5,** under the heading **VDN/CDN** in the **General** field enter the VDN assigned for email and enter the VDN assigned for suspended emails in the **Suspended** field.



Id: 50

Name: PRESENCE MAIL

Resource profile: General

Priority: Medium

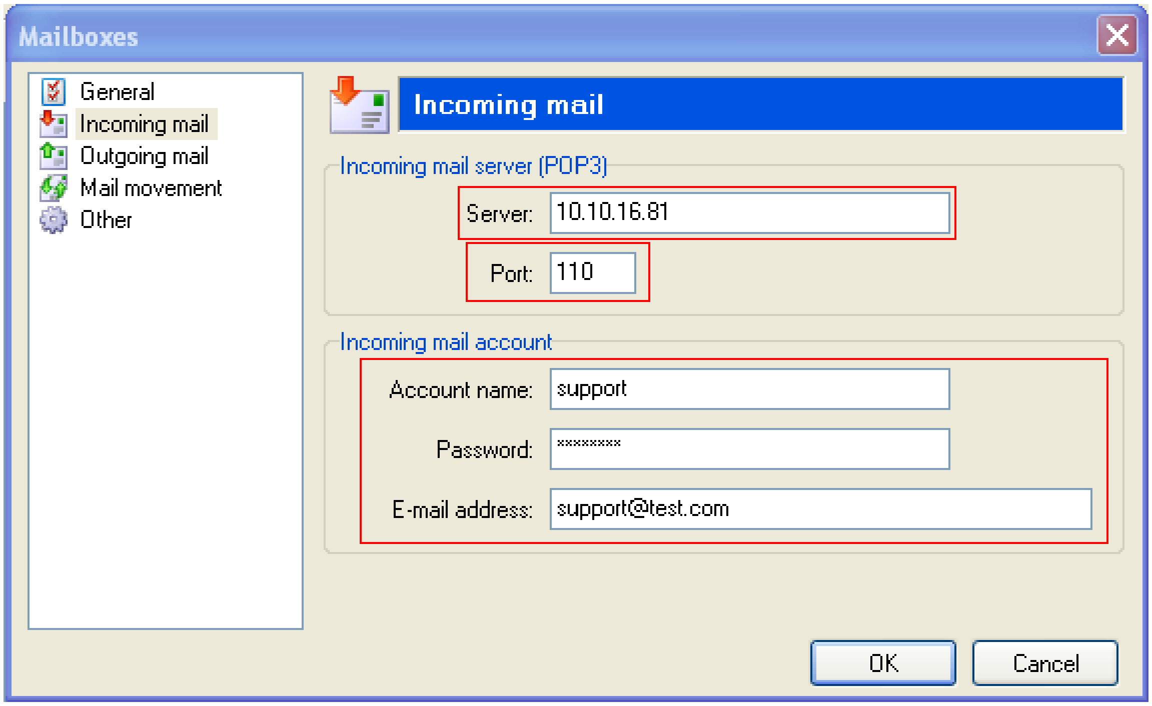
VDN/CDN

General: 1803

Suspended: 1804

□ Maximum number of concurrent e-mails 0

Select **Incoming mail** from the left hand side menu. This window allows you to specify the POP3 server and account from which to download incoming mails. In the **Server** field enter the POP3 mail server address, for the interoperability testing this was the same IP address as the Presence Server. The default POP3 port of **110** is entered into the **Port** field. Under the **Incoming mail account** heading enter the **Account name, Password** and **E-mail address** associated with the POP3 mail account.



Incoming mail server (POP3)

Server: 10.10.16.81

Port: 110

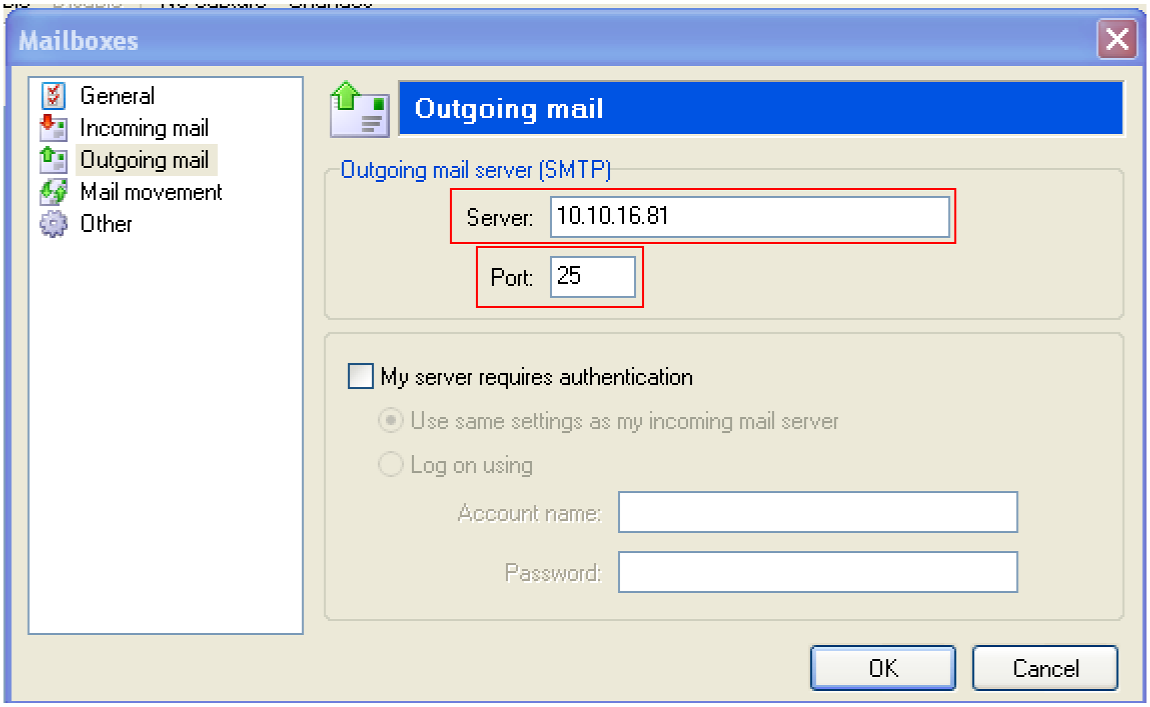
Incoming mail account

Account name: support

Password: *********

E-mail address: support@test.com

Select **Outgoing mail** from the left hand side menu and moving to the right, define the SMTP server that will be used to send response emails from Presence agents. Enter an IP address in the server field. For the interoperability testing this was the same IP address as the Presence Server. The default SMTP port of **25** is entered into the **Port** field. Click **OK** to complete the email campaign configuration.



Outgoing mail server (SMTP)

Server: 10.10.16.81

Port: 25

□ My server requires authentication

● Use same settings as my incoming mail server

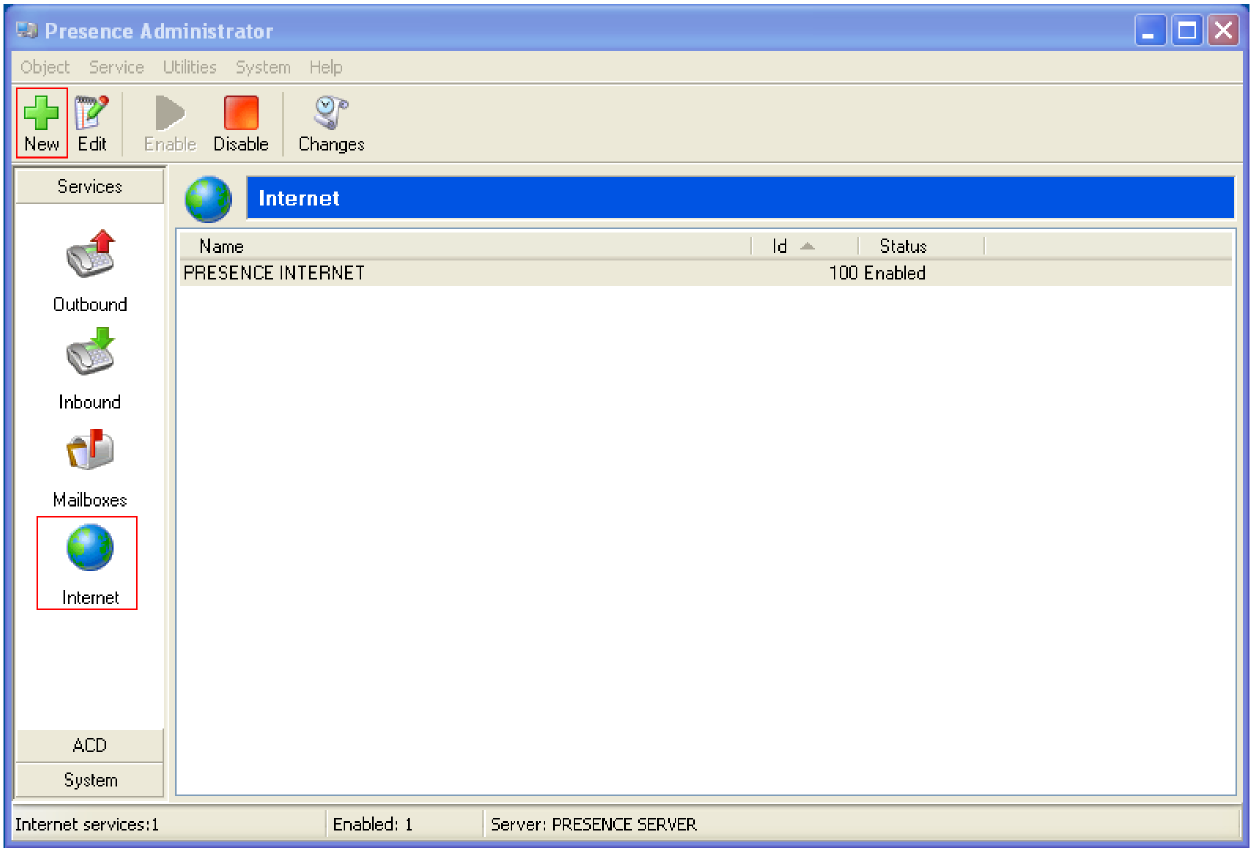
○ Log on using

Account name:

Password:

7.3.5 Web Chat / Web Call Back

To configure a web campaign, from the left hand side select **Services → Internet** from the Presence Administrator main menu. Click the **New** button.



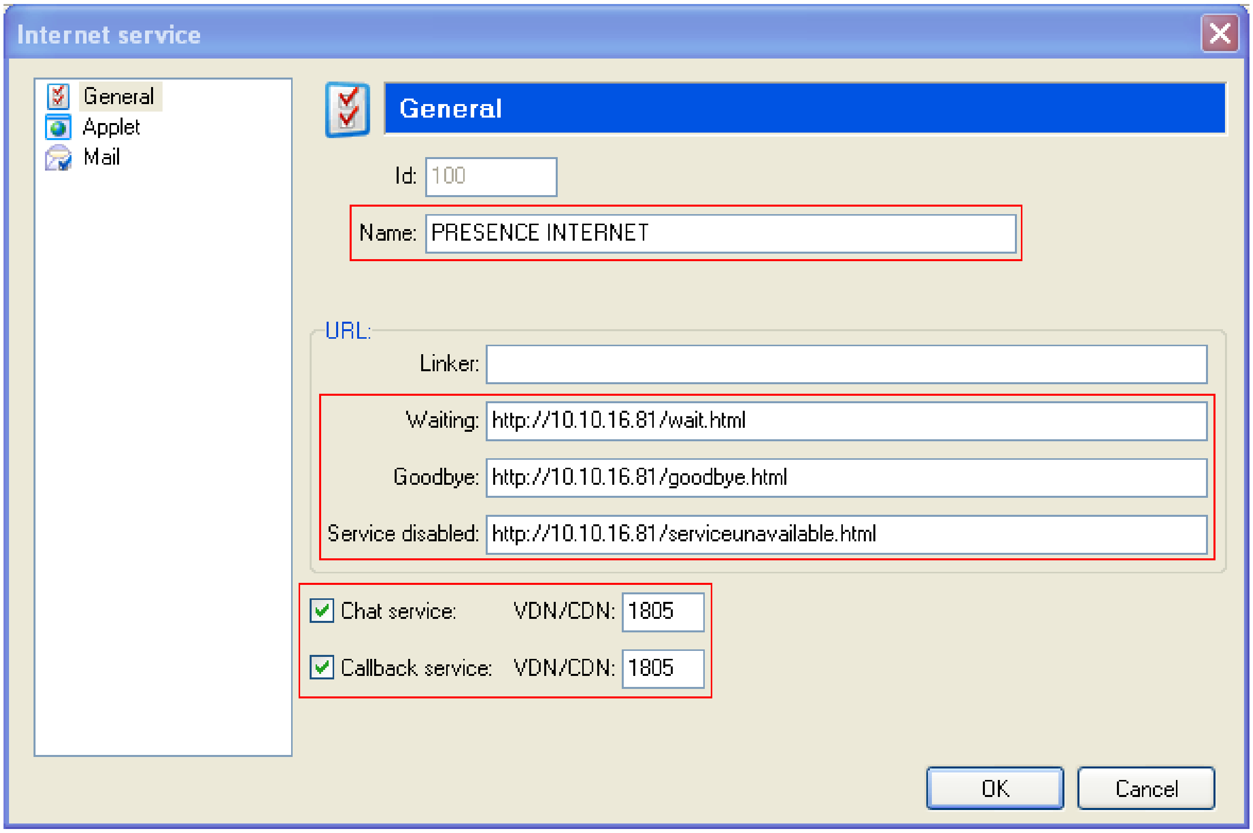
Name	Id	Status
PRESENCE INTERNET	100	Enabled

Internet services:1 | Enabled: 1 | Server: PRESENCE SERVER

In the resulting screen, select **General** from the menu on the left hand side and enter a **Name** for the web campaign. Under the **URL** heading three campaigns are defined:

- The **Waiting** URL is the URL that is presented to the customer if no agents are available.
- The **Goodbye** URL is the URL that is presented to the customer when the web callback or web chat session ends.
- The **Service disabled** URL is the URL that is presented to the customer if the service has been disabled for any reason.

The **Chat service** and **Callback service** check box's should be selected and the relevant VDN for each entered into the **VDN/CDN** field. Refer to **Table 2, Section 5.5.**



Id: 100

Name: PRESENCE INTERNET

Linker:

Waiting: http://10.10.16.81/wait.html

Goodbye: http://10.10.16.81/goodbye.html

Service disabled: http://10.10.16.81/serviceunavailable.html

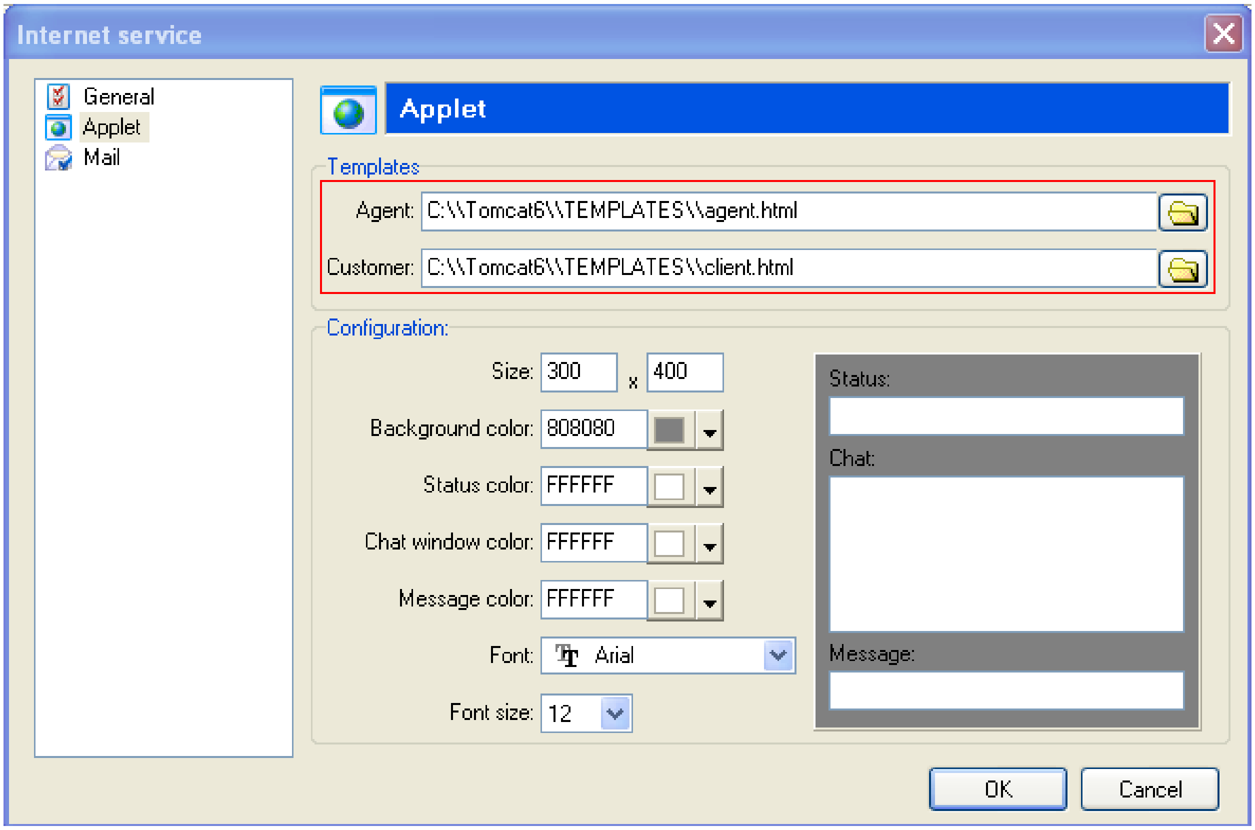
☑ Chat service: VDN/CDN: 1805

☑ Callback service: VDN/CDN: 1805

Select **Applet** from the left hand side menu. This window is used to configure the applet that is presented to the customer and to the agent when a web chat or web callback requests is made. Under the **Templates** heading, two HTML templates are defined:

- The **Agent** HTML template is used to load the applet that is used by the agent.
- The **Customer** HTML template is used to load the applet that is used by the customer.

Under the **Configuration** heading the display parameters for the applet such as size and window colour can be altered, for the interoperability test the default values were accepted. Click **OK** to complete the web chat/web callback campaign.



Templates

Agent: C:\\Tomcat6\\TEMPLATES\\agent.html

Customer: C:\\Tomcat6\\TEMPLATES\\client.html

Configuration:

Size: 300 x 400

Background color: 808080

Status color: FFFFFF

Chat window color: FFFFFF

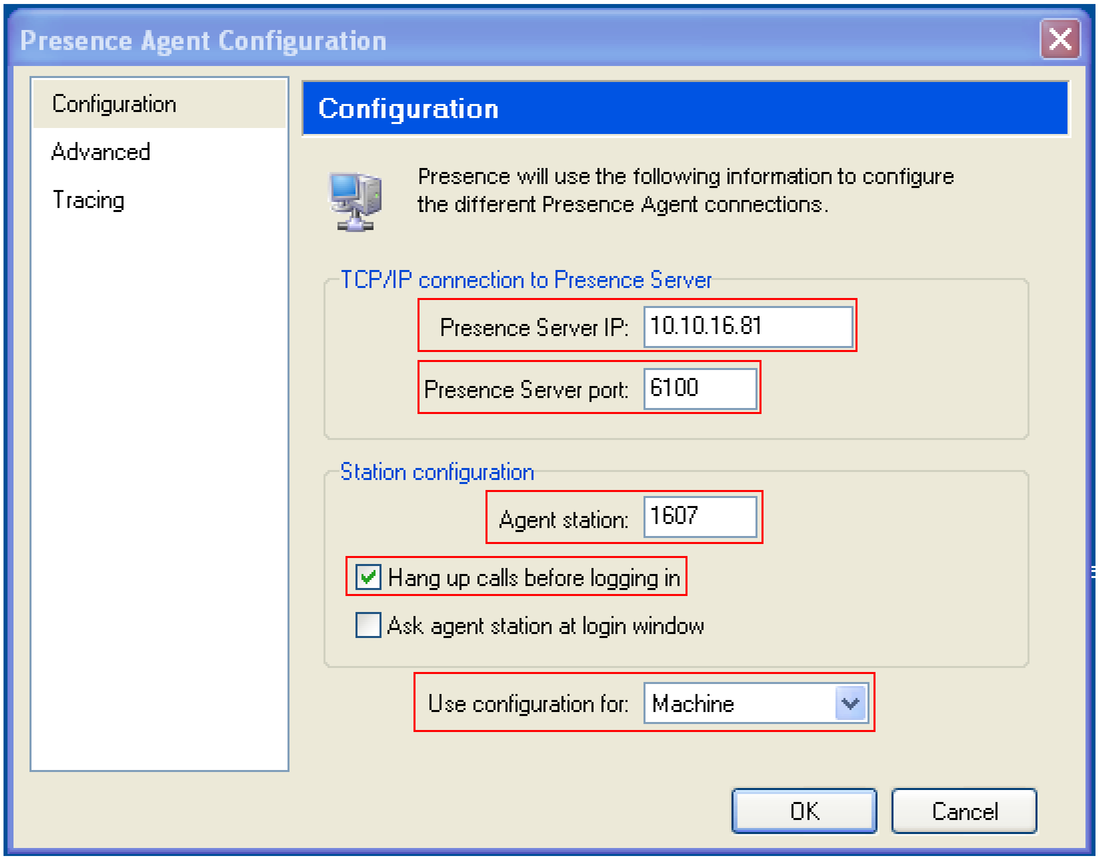
Message color: FFFFFF

Font: Arial

Font size: 12

7.4 Presence Agent Configuration

The following steps are carried out to on the Presence Suite Agent PC. 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 **pcoagentcfg.exe** located in the **C: → Presence** folder. Enter the **Presence Server IP:** address as **10.10.16.81**. The **Presence Server port** can be left as the default value of **6100**. Enter the extension of the agent that will be using this workstation in the **Agent station** field. 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: 10.10.16.81

Presence Server port: 6100

Station configuration

Agent station: 1607

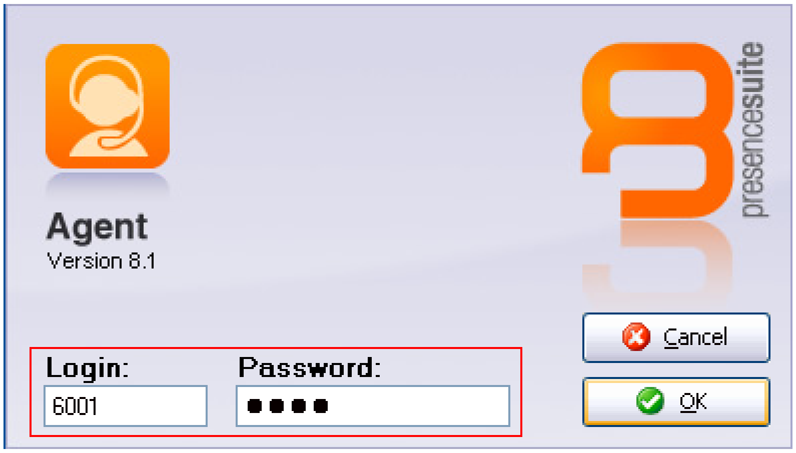
☑ Hang up calls before logging in

☐ Ask agent station at login window

Use configuration for: Machine

7.4.1 Logging in Presence Agent

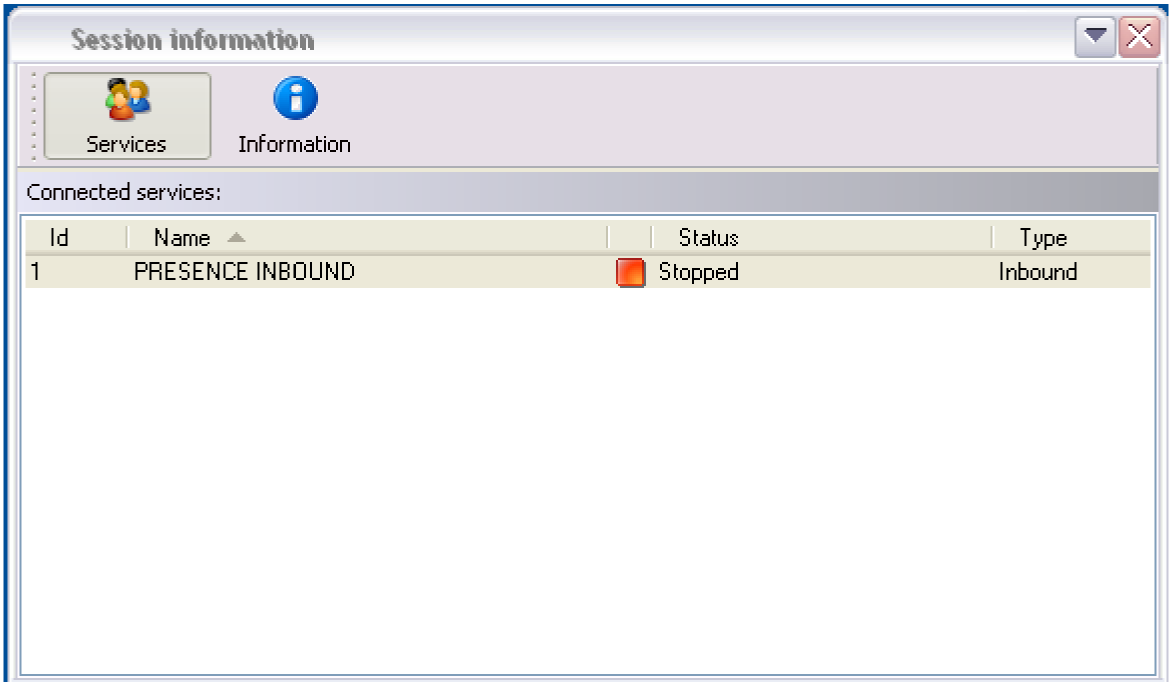
Launch the Presence agent configuration application by double clicking the **pcoagent.exe** located in the Presence folder. Enter the agent **Login** and **Password** configured in **Section 5.7** and click on **OK**.



Login: 6001

Password: ●●●●

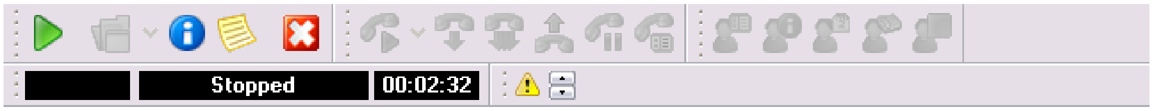
In the next screen, click on the **Services** button in the task bar. The service set up for the agent will be displayed.



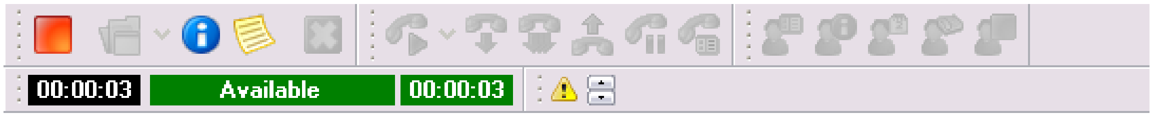
Connected services:

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 put the agent in to an available state.



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



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 Avaya Aura® 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**. 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     4        no    DCAES            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**.

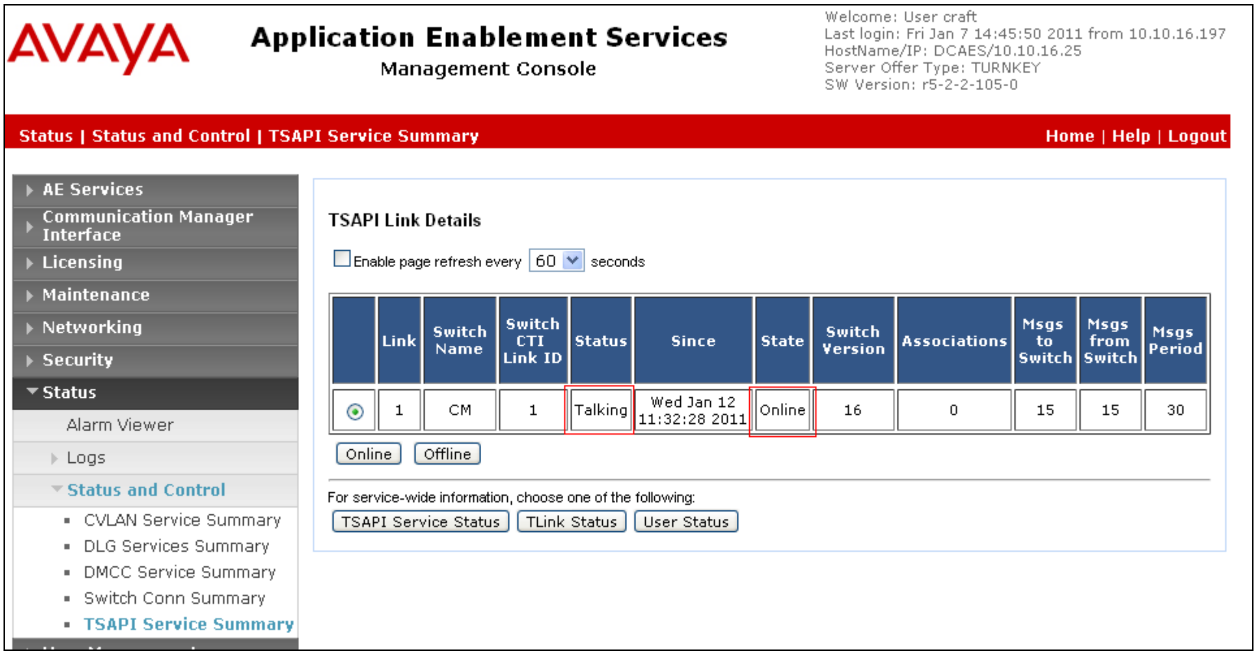
```
status aesvcs link

                                AE SERVICES LINK STATUS

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

01/01   DCAES             10.10.16.25        58744    CLAN             626      611
```

8.2 Verify Avaya Aura® 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**.



Welcome: User craft
Last login: Fri Jan 7 14:45:50 2011 from 10.10.16.197
HostName/IP: DCAES/10.10.16.25
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

TSAPI Link Details

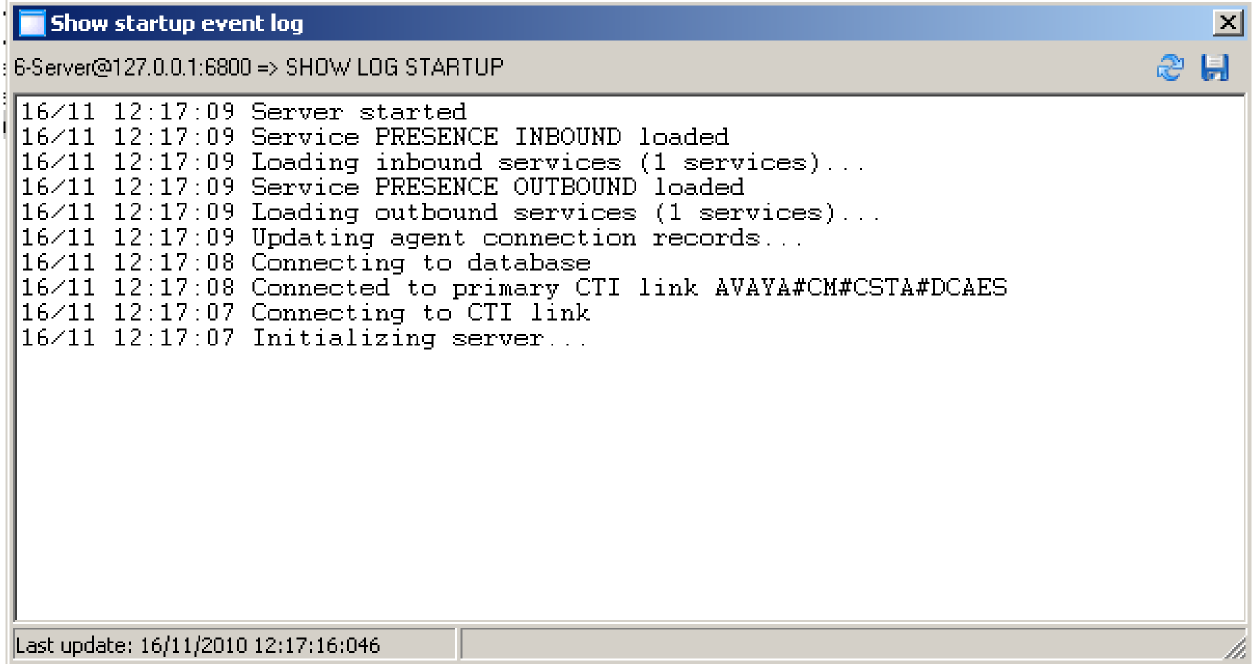
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	CM	1	Talking	Wed Jan 12 11:32:28 2011	Online	16	0	15	15	30

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

8.3 Verify Presence Suite

One of the available methods to confirm correct startup is a startup log which can be accessed from Presence Administrator by navigating to **Utilities →Events**. 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.

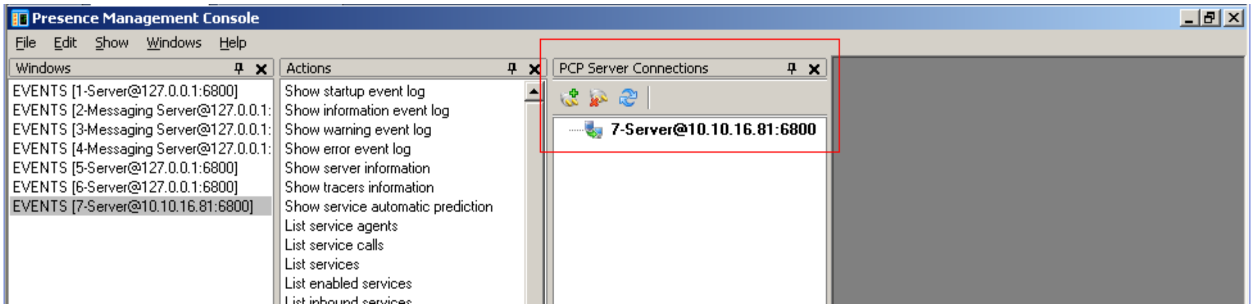


6-Server@127.0.0.1:6800 => SHOW LOG STARTUP

```
16/11 12:17:09 Server started
16/11 12:17:09 Service PRESENCE INBOUND loaded
16/11 12:17:09 Loading inbound services (1 services)...
16/11 12:17:09 Service PRESENCE OUTBOUND loaded
16/11 12:17:09 Loading outbound services (1 services)...
16/11 12:17:09 Updating agent connection records...
16/11 12:17:08 Connecting to database
16/11 12:17:08 Connected to primary CTI link AVAYA#CM#CSTA#DCAES
16/11 12:17:07 Connecting to CTI link
16/11 12:17:07 Initializing server...
```

Last update: 16/11/2010 12:17:16:046

Presence Suite has a **pmconsole.exe** system which is a tool used to aid fault diagnosis. Verify that the Presence Suite server is visible in the PCP Server Connections column.


Presence Management Console
File Edit Show Windows Help
Windows
EVENTS [1-Server@127.0.0.1:6800]
EVENTS [2-Messaging Server@127.0.0.1:
EVENTS [3-Messaging Server@127.0.0.1:
EVENTS [4-Messaging Server@127.0.0.1:
EVENTS [5-Server@127.0.0.1:6800]
EVENTS [6-Server@127.0.0.1:6800]
EVENTS [7-Server@10.10.16.81:6800]
Actions
Show startup event log
Show information event log
Show warning event log
Show error event log
Show server information
Show tracers information
Show service automatic prediction
List service agents
List service calls
List services
List enabled services
List inbound services
PCP Server Connections
7-Server@10.10.16.81:6800

9 Conclusion

These Application Notes describe the configuration steps required for Presence Suite 8.1 to successfully interoperate with Avaya Aura® Communication Manager 6.0 using Avaya Aura® Application Enablement Services 5.2.2. All feature 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; Document No. 03-300509, 9th August 2010
2. Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Document No. 02-300357; 20th November 2009

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

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

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.