Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2, Avaya Aura® Application Enablement Services R6.2 and Avaya Proactive Contact R5.0.1 to interoperate with Geomant Unified Agent 1.4 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Geomant Unified Agent 1.4 to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Proactive Contact R5.0.1 using Avaya PG230 Digital Switch. In the compliance testing, Geomant Unified Agent used the Agent API from Avaya Proactive Contact and the Telephony Services Application Programmer Interface from Avaya Aura® Application Enablement Services to provide a custom agent desktop for Communication Manager and/or Avaya Proactive Contact agents for handling of inbound calls delivered by Avaya Aura® Communication Manager and outbound calls delivered by Avaya Proactive Contact or a blend of the two.

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 configuration steps required for Geomant Unified to interoperate with Avaya Aura® Communication Manager and Avaya Proactive Contact using Avaya PG230 Digital Switch and agent blending. In the compliance testing, Geomant Unified Agent used the Agent API from Avaya Proactive Contact and the Telephony Services Application Programmer Interface (TSAPI) from Avaya Aura® Application Enablement Services (AES) to provide a custom agent desktop for Avaya Aura® Communication Manager and/or Avaya Proactive Contact agents, for handling of inbound calls delivered by Avaya Aura® Communication Manager and outbound calls delivered by Avaya Proactive Contact or a blend of the two (Proactive Agent Blend environment).

Geomant Unified Agent is a client which provides a user interface for Avaya Aura® Communication Manager and/or Avaya Proactive Contact call center agents. This is a Google Web Toolkit based application and uses only html pages, web services and javascripts. Geomant Unified Agent is deployed onto a Tomcat application server, and is accessed via a URL from a browser on the agent desktop PC.

Events and activities performed on the Geomant Unified Agent client in relation to the Avaya Aura® Communication Manager Call Center are handled by the Geomant CCI Service via a TSAPI connection to Avaya Aura® Application Enablement Services via Geomant's Contact Centre Integration (CCI) framework.

Events and activities performed on the Geomant Unified Agent client in relation to Avaya Proactive Contact are sent from the Tomcat application to the Geomant APC Service, which handles the connection to the Proactive Contact Agent API via Geomant's Contact Centre Integration (CCI) framework.

In the Proactive Agent Blend (PAB) environment, the inbound calls are delivered to the agents by Avaya Aura® Communication Manager. The TSAPI interface from Avaya Aura® Application Enablement Services is used by Geomant Unified Agent to request call control functions for the inbound calls.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of Unified Agent to carry out call handling functions in a variety of scenarios through its TSAPI and Agent API interface with AES and Proactive Contact respectively. Inbound calls were placed manually via a VDN to agents administered on Communication Manager and handled by agents using the Unified Agent client. Outbound calls from a Proactive Contact calling list were placed automatically based on the configuration and job commencement administered using the Proactive Contact Editor Application and handled by Proactive Contact Agents using the Unified Agent client.

The correct handling of a variety of call scenarios was tested and the Proactive Contact Agent API events were monitored using the agentx_API.trans log file. Communication Manager agents were monitored using the SAT.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The feature testing focused on verifying proper display and handling of calls using the Unified Agent with appropriate options, fields, and values for the following scenarios:

- Outbound and managed jobs
- Inbound ACD calls
- Change ACD agent state
- Proactive Agent Blend
- Log in, join job, go on/off break, leave job, and logoff
- Hold, retrieve, forward work, NVDT call transfer, conference, place manual call, agent drop, release line, hang-up, and finish work
- Set recall and agent owned recall

2.2. Test Results

All test cases were executed and successfully passed with the following observations:

- Where an inbound call is delivered to and ringing on the Unified Agent client, the Drop Call icon is visible but cannot be used and shouldn't be presented.
- Where an inbound call with auto-in and manual-accept configured was received and answered by Unified Agent the info display was not updated when the call ended.
- Where an inbound call from PSTN A is delivered to and answered by a Unified Agent client and subsequently blind transferred to PSTN B the Unified Agent client displays PSTN B transferred to Txxxx. This is logically the reverse of what should be shown, and does not include the original calling party number
- Where a Proactive Contact agent attempts to login using the Unified Agent client with an incorrect or invalid Extension, the info display shows **The server did not respond** for 30 secs and the Proactive Contact agent remains logged in. This prevents further login with the same Proactive Contact agent and the web page must be refreshed or the browser closed and re-opened to clear the Proactive Agent login. Alternatively the Proactive Contact Supervisor menu must be accessed to clear the login.
- Where an outbound call is connected to the Unified Agent client and subsequently transferred by the Unified Agent client, the info display does not update to reflect the successful transfer of the call.
- Where an outbound call is connected to the Unified Agent client and subsequently a conference is created by the Unified Agent client with a 3rd party, the info area does not notify of the conference and where the customer terminates the call the Unified Agent info area displays **Transfer failed! The customer hung up** despite the successful termination.

2.3. Support

Technical Support for the Geomant Unified Agent can be obtained through the following:

- Phone: +44 207 022 4874
- Email: help@geomant.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. In the compliance testing, Unified Agent used the Proactive Contact Agent API to monitor and control outbound calls for the agents, and used TSAPI to monitor and control the inbound calls for the agents. All calls were answered and controlled using the Unified Agent Client.

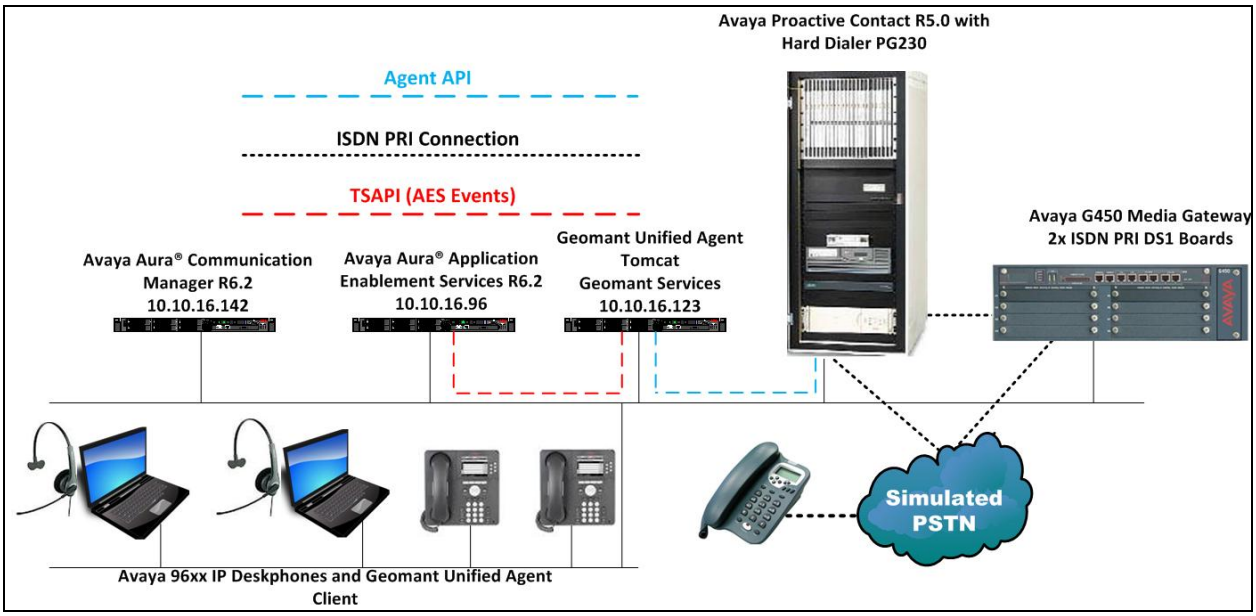


Figure 1: Test Configuration for Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Proactive Contact with Geomant Unified Agent Solution

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communicaiton Manager running on Avaya S8800 Server	R6.2 SP4
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.2
Avaya 9630 IP Deskphone	H323 S3.105S
Avaya Proactive Contact	R5.0.1 with patch 301, 302, 307, 309, 323, 328
Avaya PG230 Digital Switch	Generic Version 15.3.1
Geomant Unified Agent	1.4.4 1.4.4.1 for PAB

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager to support the PG230 integration, CTI connection to Application Enablement Services and the Inbound call center configuration which is also used for Proactive Agent Blend. The procedures include the following areas.

- Configure AE Services
- Configure Inbound ACD
- Configure Avaya Proactive Contact Acquire feature
- Configure ACD agent for Proactive Agent Blend
- Configure feature access codes for Call Centre features
- Configure Trunks to Avaya PG230 Digital Switch

5.1. Configure AE Services

Enter the node **Name** and **IP Address** for AE Services. Take a note of the **procr** node **Name** and **IP Address**.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
procr                   10.10.16.142
CM521                   10.10.16.23
Gateway                 10.10.16.1
IPbuffer                10.10.16.184
Intuition               10.10.16.51
MedPro                  10.10.16.32
Presence                10.10.16.83
RDTT                    10.10.16.185
SESMNGR                 10.10.16.44
SM1                     10.10.16.43
SM61                    10.10.16.201
default                 0.0.0.0
aesserver62             10.10.16.96
```

In order for Communication Manager to establish a connection to AE Services, administer the CTI Link as shown below. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 5899
     Type: ADJ-IP
                                                                      COR: 1
     Name: aesserver62
```

Use the command **change ip-services** to configure IP-Services for the AESVCS service. Use the **procr** node name as noted above as the **Local Node** and set **Enabled** to **y**.

```
change ip-services                                          Page   1 of   4

                                    IP SERVICES
 Service      Enabled      Local        Local       Remote       Remote
  Type                     Node         Port        Node         Port

AESVCS         y          procr          8765
```

On **Page 4**, set the **AE Services Server** hostname and the **Password** that AE Services will use to authenticate with Communication Manager. In this example the hostname and node-name are configured as **aesserver62**. Set **Enabled** to **y**.

```
change ip-services                                          Page   4 of   4
                           AE Services Administration

   Server ID    AE Services       Password          Enabled     Status
                   Server
      1:       aesserver62       Avayapassword1        y        in use
```

5.2. Configure Inbound ACD

For the purposes of proactive agent blend, an inbound vector and VDN must be configured. This is used for delivering inbound calls to ACD agents independent of Proactive Contact. When a call to this VDN is made and queued to skill 2 configured in its vector, Blend Agents (agents which are assigned both skill 2 and skill 1, as described in **Section 5.3**) will automatically be detached from the outbound job, and handle the inbound call. Once the call is complete and there are no more calls queued for the inbound skill, Proactive Contact will acquire the agent for outbound call handling again. Using the command **add vdn xxxx** where **xxxx** is a valid extension, in this case **5812**, administer the VDN as shown below and assign to it a **Name** for identification purposes, and an unassigned **Vector Number.**

```
add vdn 5812                                              Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 5812
                                 Name*: Inbound
                          Destination: Vector Number        2
                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*:
```

VDN 5812 has a destination of Vector Number 2. Enter the command **change vector 2** and configure the vector to **queue-to** an unassigned skill, in this case, **skill 2** with a **priority** of **m.**

```
change vector 2                                           Page   1 of   6
                                  CALL VECTOR

    Number: 2                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 queue-to     skill 2    pri m
02 wait-time    60  secs hearing ringback
```

Calls routed to VDN 5812 will route to skill 2, which is administered as a hunt group. Enter the command **add hunt-group 2** and configure the hunt group with an appropriate **Group Extension** number in the dial plan, and a **Group Name** for identification. Set **ACD, Queue** and **Vector** to **y** (yes), these parameters define that the group is an ACD group, controlled by a vector with queuing enabled.

```
add hunt-group 2                                          Page   1 of   4
                                  HUNT GROUP

           Group Number: 2                                  ACD? y
             Group Name: Inbound                          Queue? y
        Group Extension: 5822                            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 **Skill** to **y** (yes)**.** This tells the ACD that calls routed to this group will be handled by agents assigned with this skill.

```
add hunt-group 2                                          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
```

5.3. Configure Avaya Proactive Contact Acquire feature

In order for Proactive Agent Blend to function, Communication Manager must be configured with a VDN monitored by Proactive Contact. When the agents who belong to the skill to which the Acquire VDN routes are not taking any inbound ACD calls, they are automatically acquired by Proactive Contact to service calls delivered by the outbound job administered in Proactive Contact Editor. Enter the command **add vdn xxxx** where xxxx is a number appropriate to the dialplan. Enter an identifying **Name** and unused **Vector Number**.

```
add vdn 5811                                                  Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 5811
                                 Name*: Dialer Acquire-Out
                           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*:
```

VDN 5811 has a destination of Vector Number 1. Enter the command **change vector 1** and configure an identifying **Name** and a step to **queue-to skill 1** with a priority of **h**.

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

    Number: 1                Name: DialerAcquireOu
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 queue-to     skill 1    pri h
02 wait-time    60  secs hearing ringback
```

As shown in vector 1, skill 1 will be the skill in which the agents required for Proactive Agent Blending will reside. Skill 1 is administered as a hunt group. Enter the command **add hunt-group 1**, specify **Group Name,** and **Group Extension,** and set **ACD, Queue and Vector** to **y.**

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

            Group Number: 1                                    ACD? y
              Group Name: Dialer Acquire-Out                 Queue? y
         Group Extension: 5821                             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 **Skill** to **y.**

```
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
```

5.4. Configure ACD agent for Proactive Agent Blend

In order for the ACD agent to be acquired by Proactive Contact once it has completed taking inbound calls using the Proactive Agent Blend feature, it must be in both the inbound skill (2) and the Acquire skill (1). Using the command **add agent-loginID xxxx** where **xxxx** is a valid extension number in the dialplan, administer a **Name** as shown below.

```
add agent-loginID 5621                                        Page   1 of   3
                                  AGENT LOGINID

               Login ID: 5621                                    AAS? n
                   Name: Agent1                                AUDIX? n
                     TN: 1                               LWC Reception: spe
                    COR: 1                     LWC Log External Calls? n
          Coverage Path:                     AUDIX Name for Messaging:
          Security Code:
                                       LoginID for ISDN/SIP Display? n
                                                           Password:
                                             Password (enter again):
                                                        Auto Answer: station
                                                  MIA Across Skills: system
                                            ACW Agent Considered Idle: system
                                            Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                        Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time:   :

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

On **Page 2** configure the agent in both the inbound skill and the Acquire skill, ensure that the Acquire skill is assigned a higher Skill Level (**SL**) than the Inbound Skill.

```
add agent-loginID 6002                                        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:
 2: 2      2       17:                32:                47:
```

5.5. Configure feature access codes for Call Centre features

Call Center related Feature Access Codes must be administered in order to control the agent state. Enter the command **change feature-access-codes**, on **Page 5** configure **Auto-In Access Code, Login Access Code** and **Logout Access Code** according to the dialplan.

```
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
```

5.6. Configure Trunks to Avaya PG230 Digital Switch

It is assumed that the configuration of the PRI trunk between Communication Manager and Proactive Contact is configured, its configuration is not relevant to the interoperation of Unified Agent with the Geomant solution. The **list trust-group** command below shows the trunks configured for use with headsets, inbound, outbound and transfer operations

```
list trunk-group                                                       Page   1

                                TRUNK GROUPS

Grp                                                No.             Out       Que
No.  TAC  Group Type   Group Name                  Mem TN  COR CDR Meas Dsp  Len
21   721  isdn         QSIG to PG230 - Headsets    5   1   1   y   none y    0
22   722  isdn         QSIG to PG230 - Outbound    10  1   1   y   none n    0
23   723  isdn         QSIG to PG230 - Inbound     5   1   1   y   none n    0
24   724  isdn         QSIG to PG230 - Transfer    1   1   1   y   none n    0
```

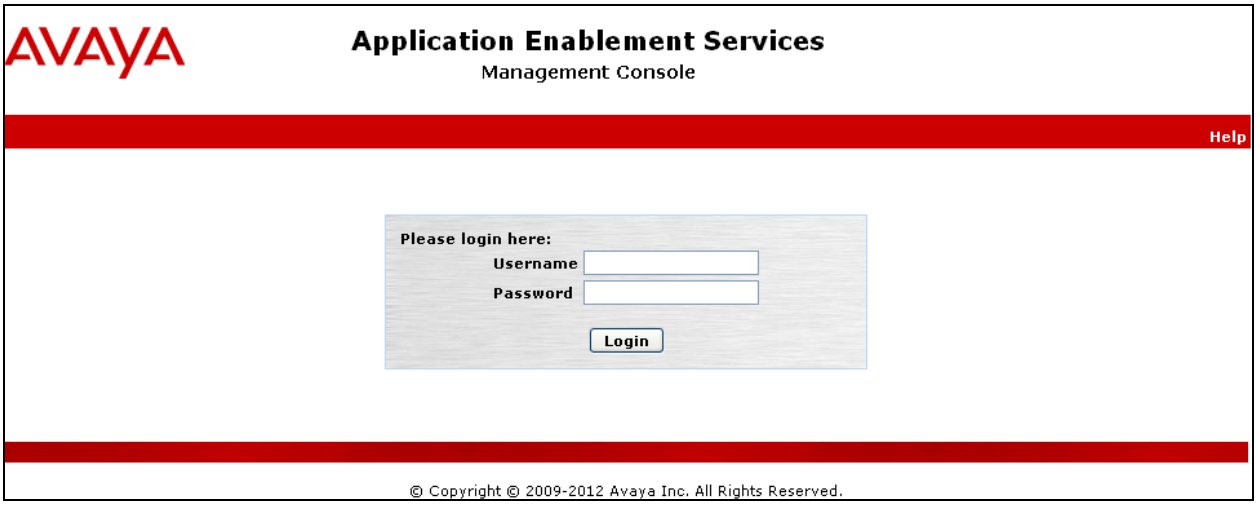
6. Configure Avaya Aura® Application Enablement Services

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

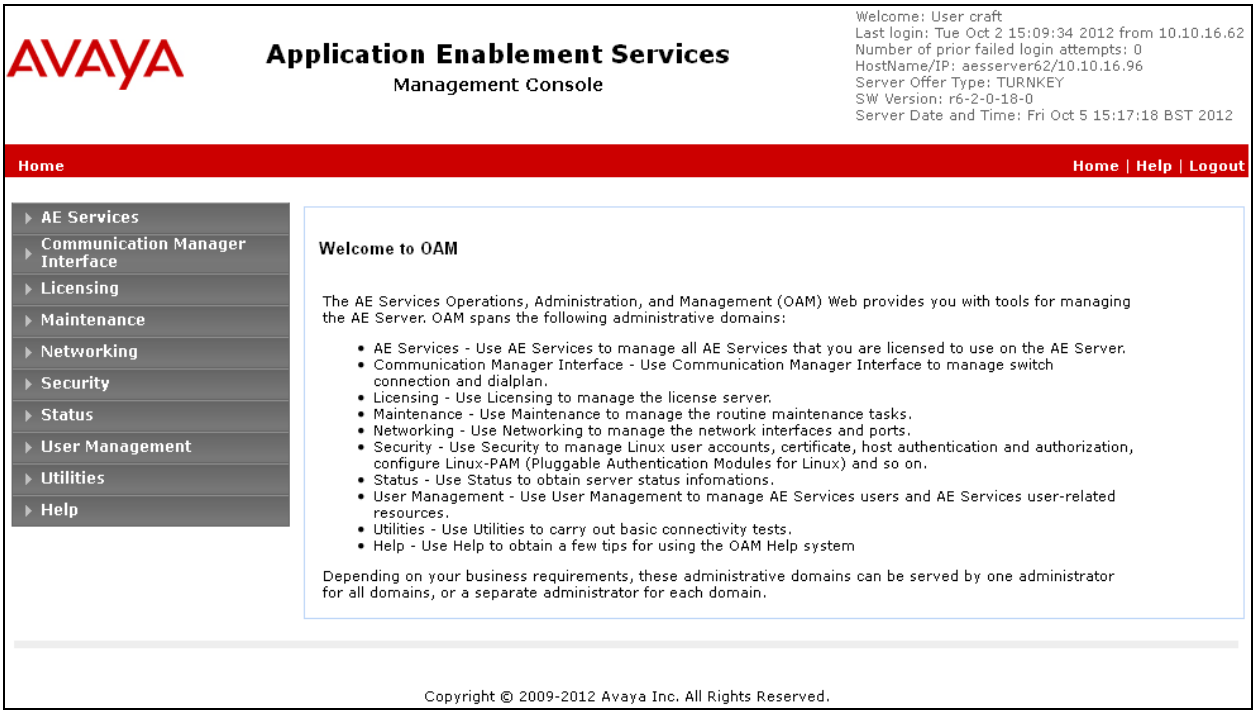
- Launch OAM interface
- Administer the Switch Connection
- Administer TSAPI Link
- Restart TSAPI Service
- Obtain Tlink Name
- Administer Avaya Proactive Contact and Geomant user

6.1. Launch OAM Interface

Access the OAM web-based interface of AES, in this instance using the URL https://10.10.16.96. The Management console is displayed. Login using the appropriate credentials.

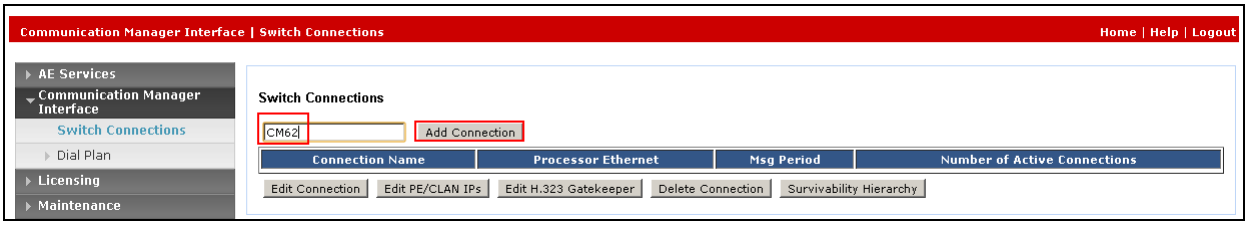


The **Welcome to OAM** screen is displayed next.

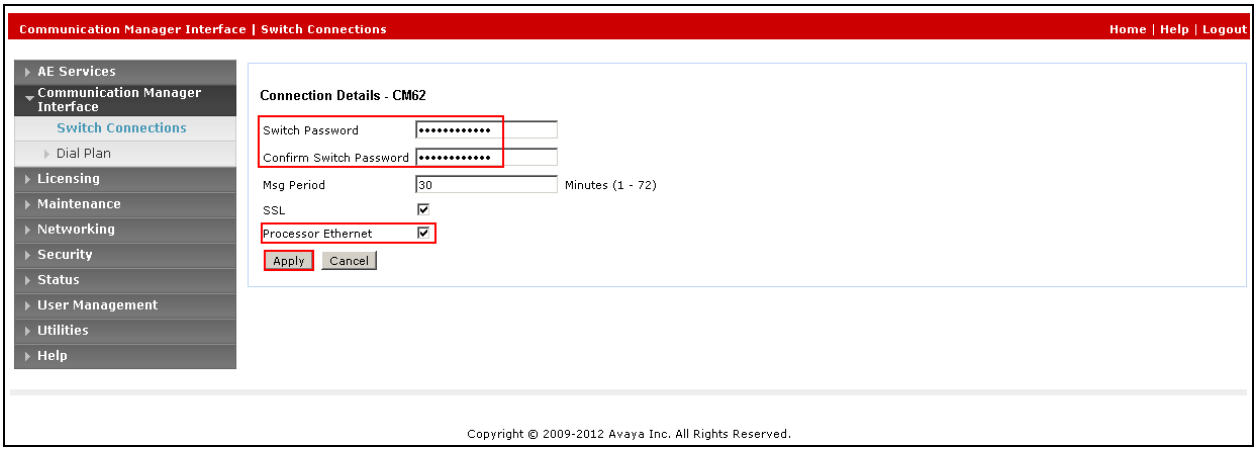


6.2. Administer the Switch Connection

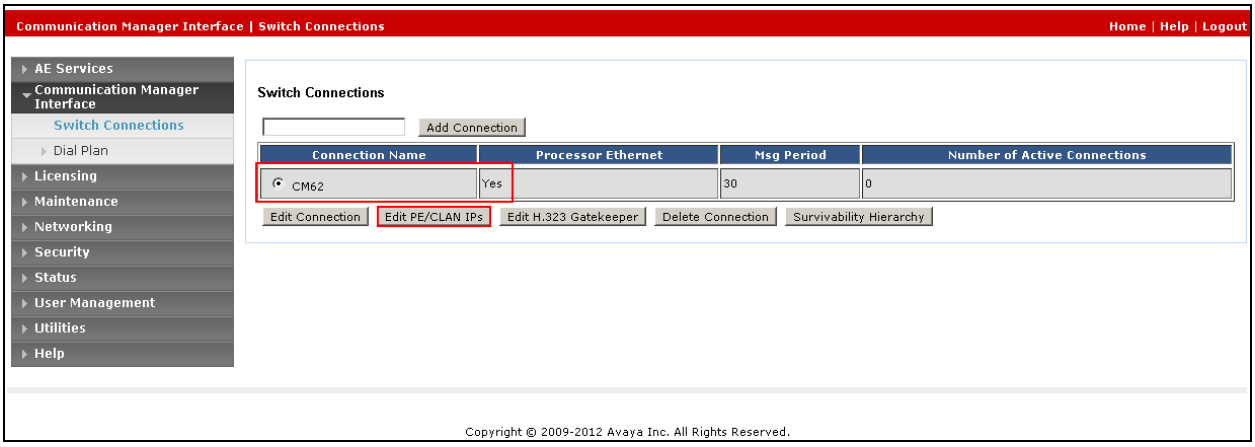
To establish the connection between Communication Manager and AES, click **Communication Manager Interface → Switch Connections**. In the field next to **Add Connection** enter **CM62** and click on **Add Connection**.



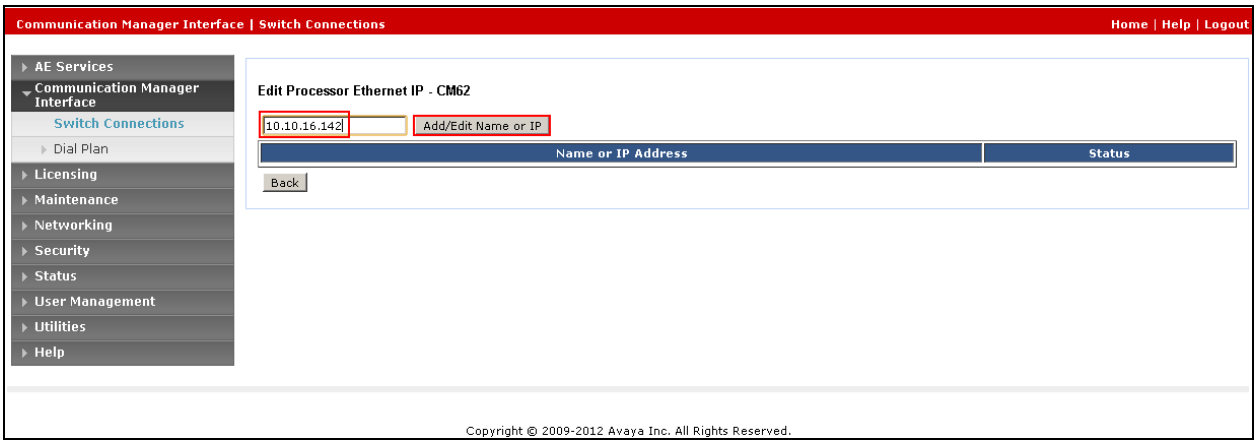
The following screen is displayed. Complete the configuration as shown and enter the password specified in **Section 5.1** when configuring AESVCS in the ip-services form. Click on **Apply** when done.



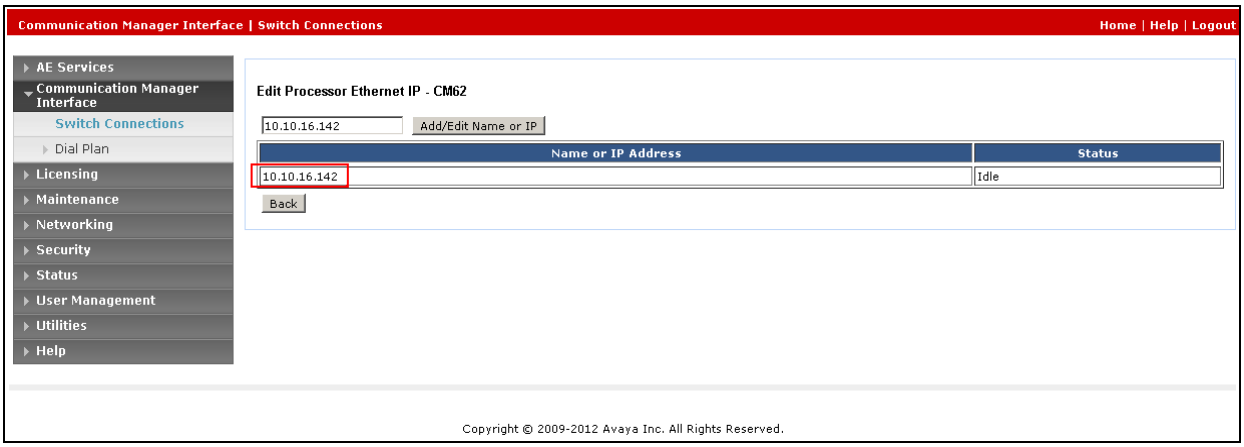
The following screen will be shown displaying the newly added switch connection, click **Edit PE/CLAN IPs**.



The following screen is displayed. Next to **Add/Edit Name or IP,** enter the IP address of the procr as shown below.

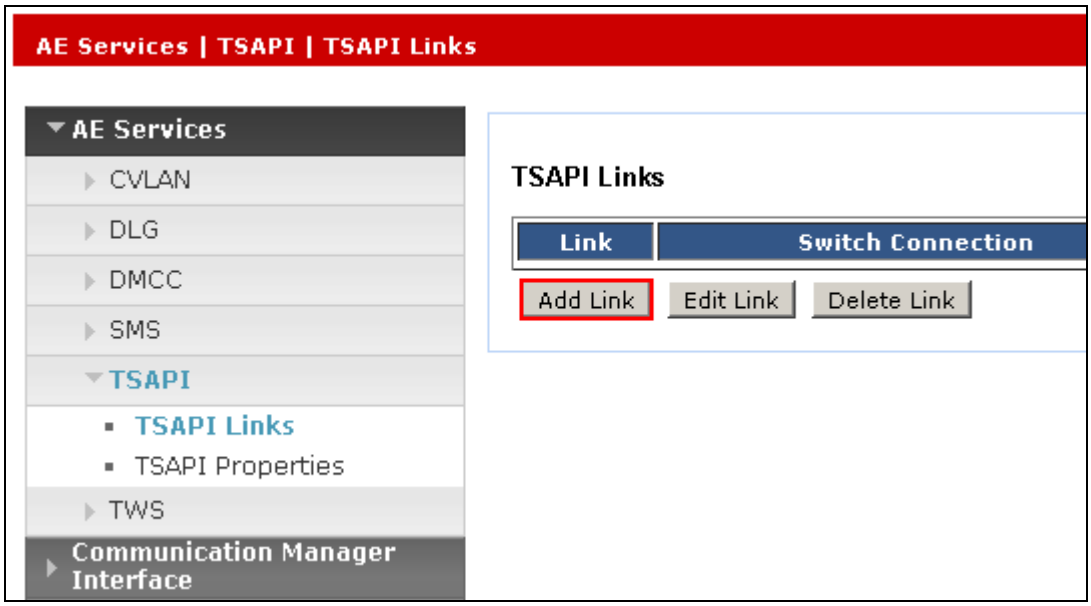


The following screen will now appear displaying the newly added IP address.

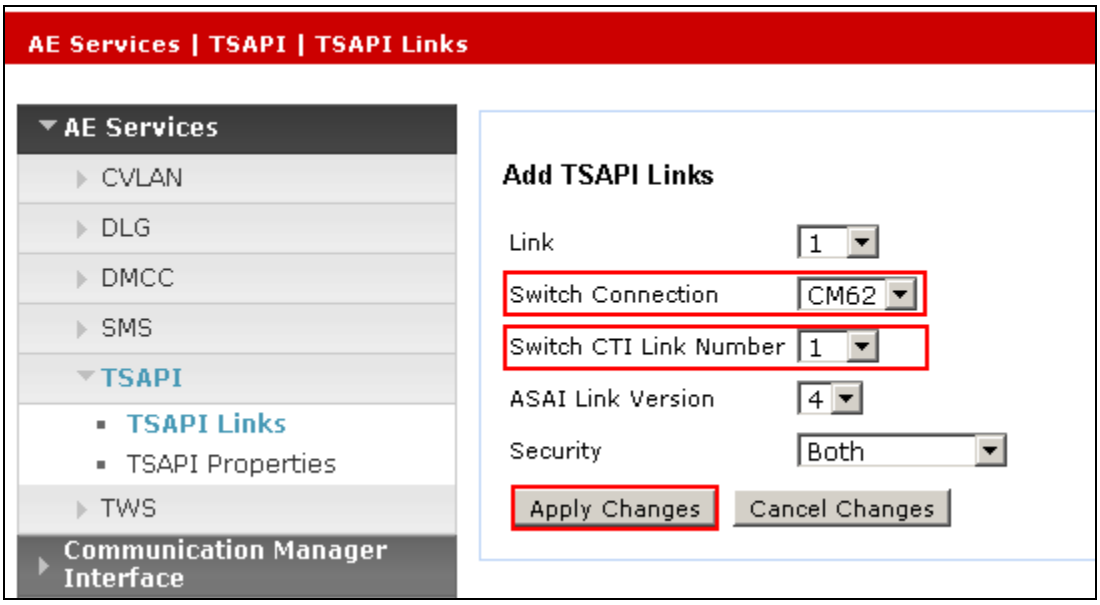


6.3. Administer TSAPI Link

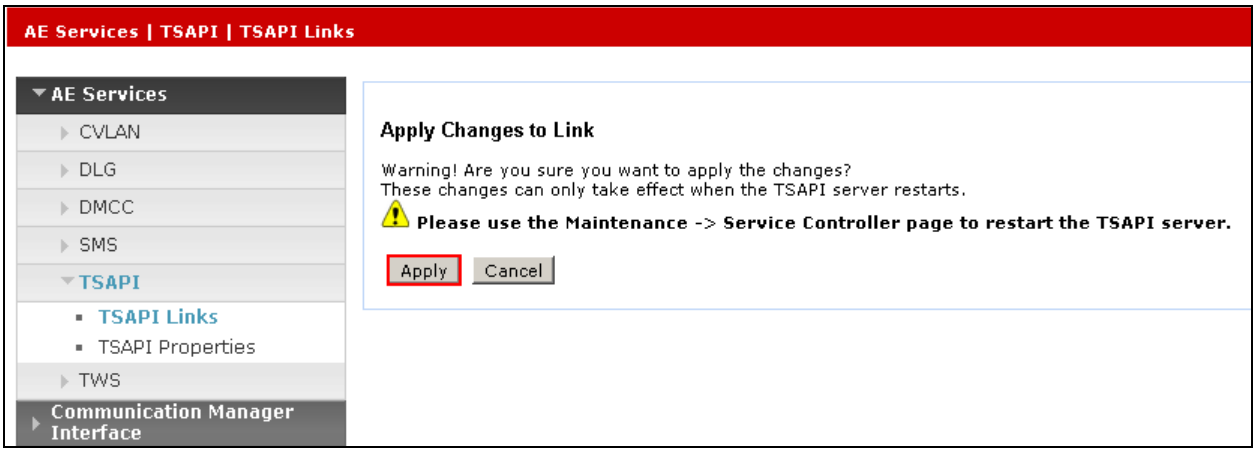
Select **AE Services → TSAPI → TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, click **Add Link**.



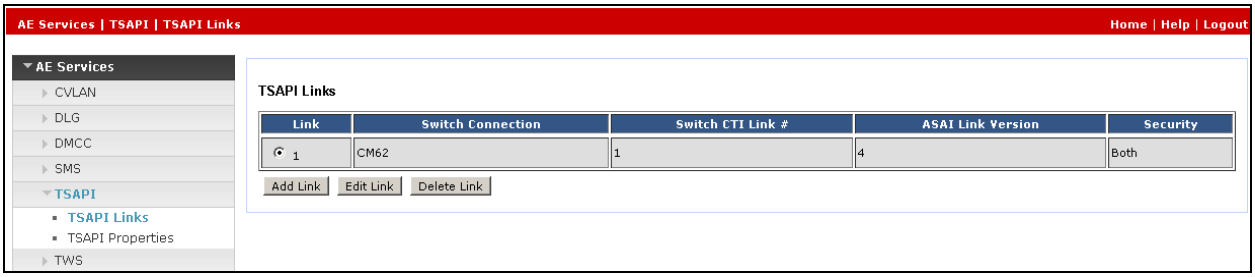
Configure the TSAPI Link using the newly configured **Switch Connection** as shown below where the **Switch CTI Link Number** configured in **Section 5.1** is chosen, and click **Apply Changes**.



The screen below will be displayed with instructions to restart the TSAPI Server. Click **Apply** taking note of the instructions given.

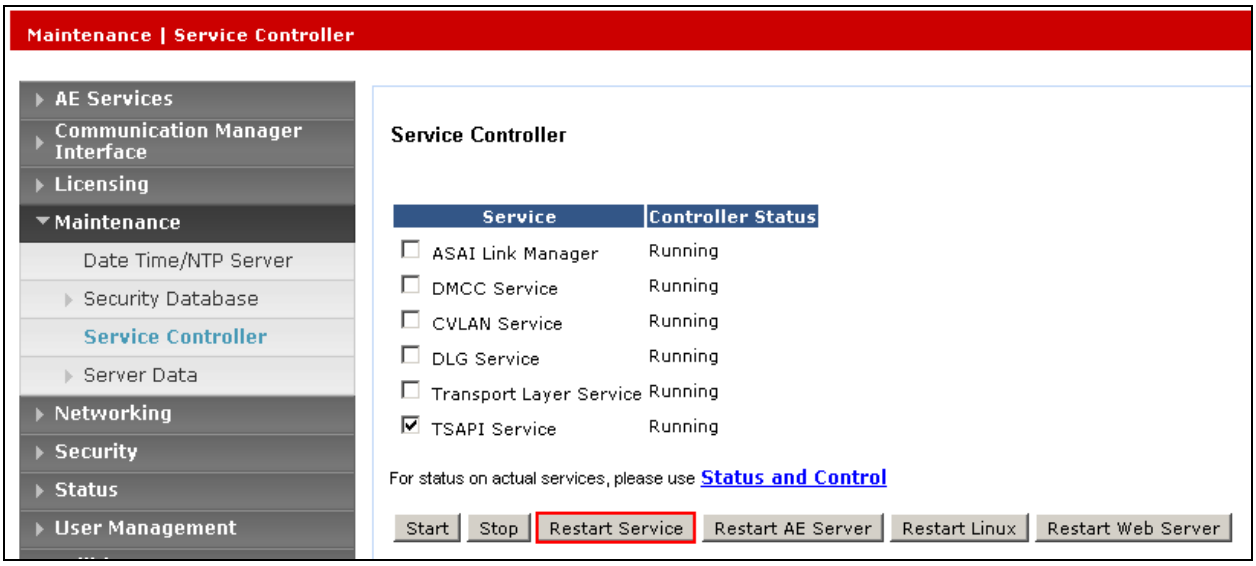


The following screen will be displayed showing the TSAPI Link.



6.4. Restart TSAPI Service

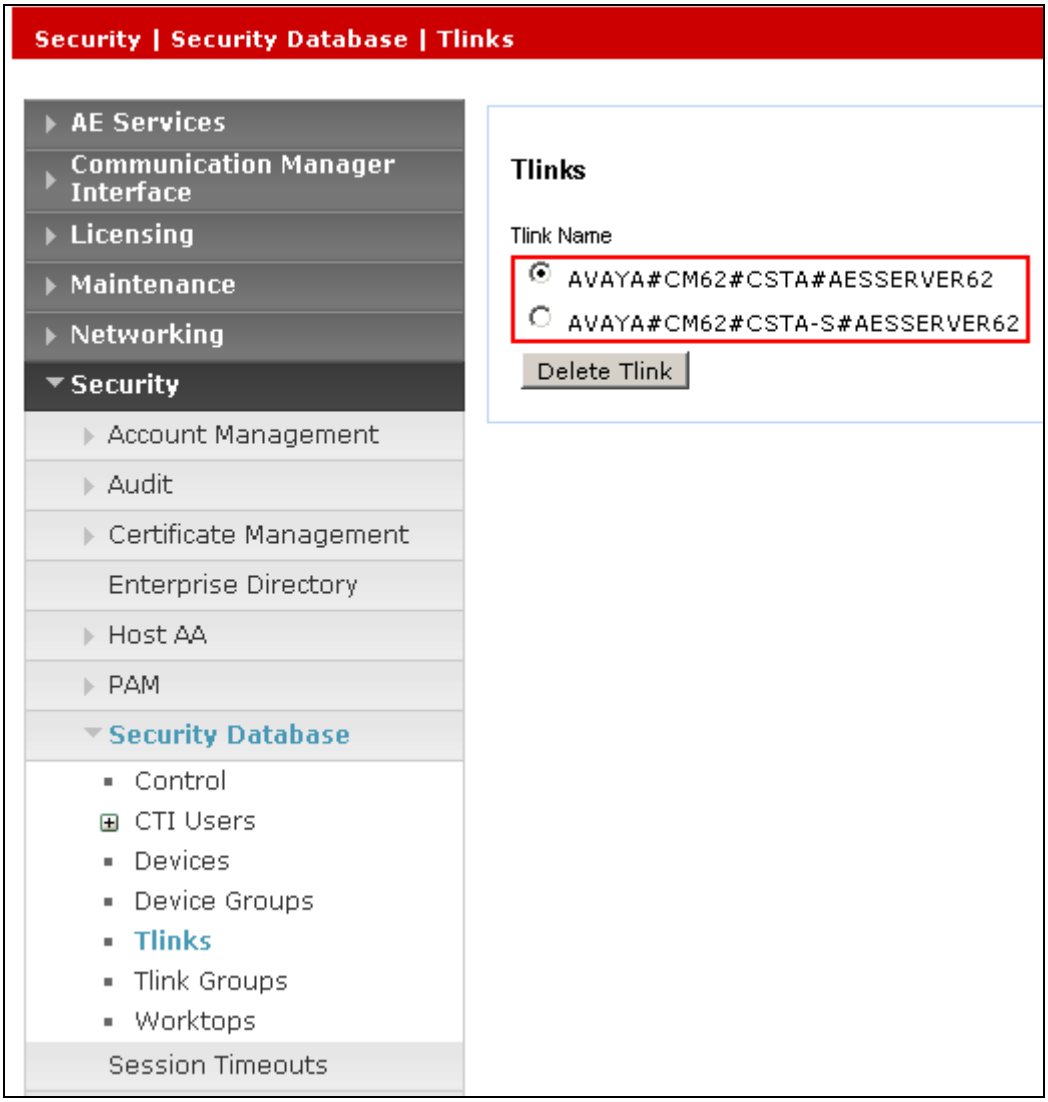
Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service**, and click **Restart Service.**



6.5. Obtain Tlink Name

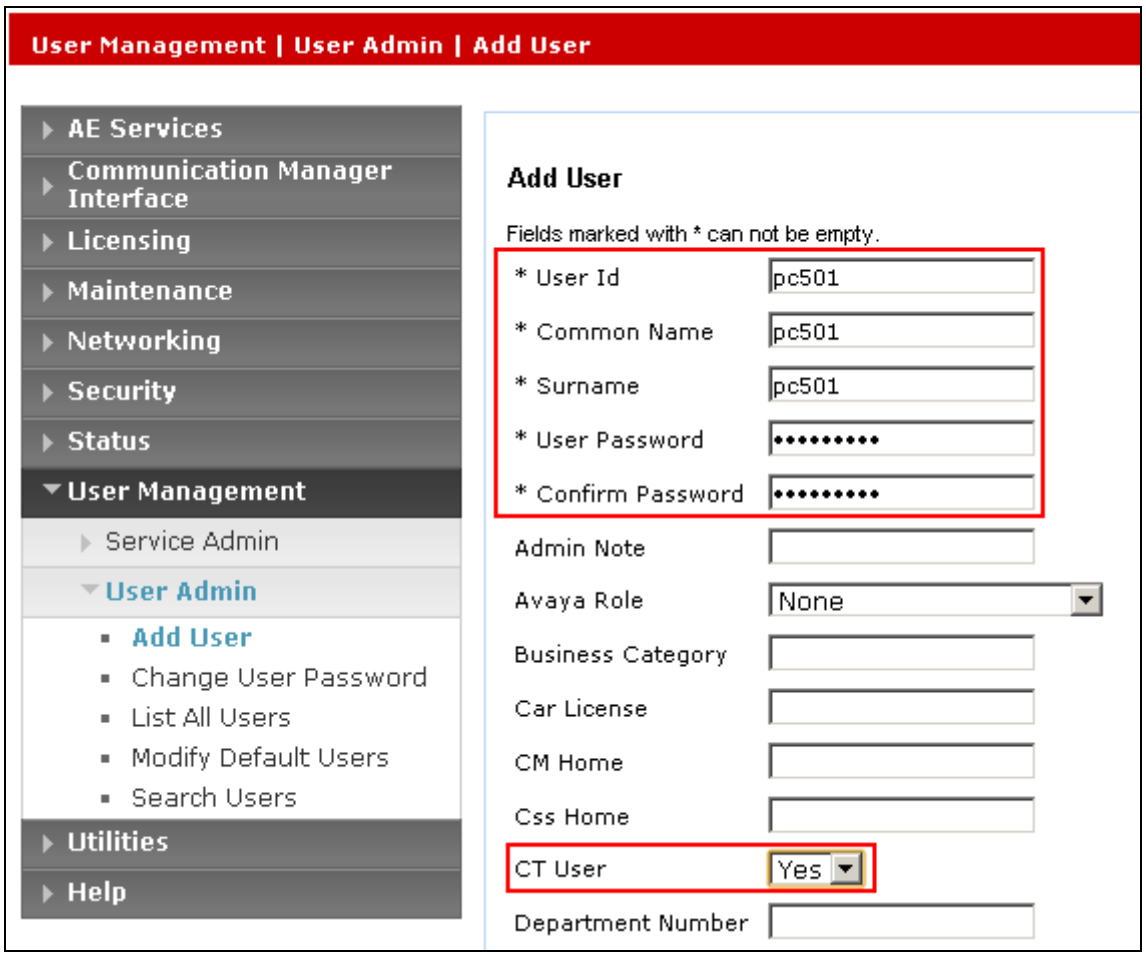
Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name.

Note: The encrypted TSAPI link is used by Proactive Contact and the unencrypted one is used by the GeoCCI Service.

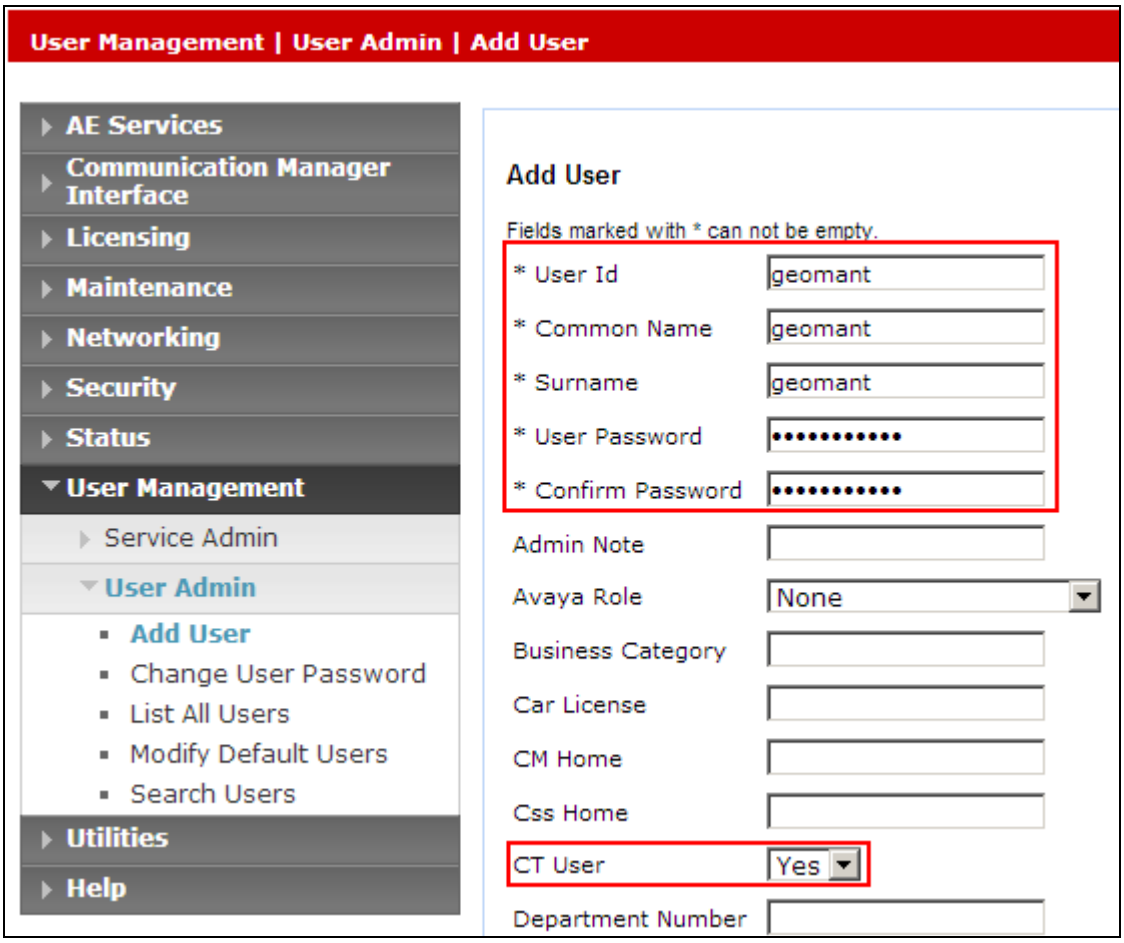


6.6. Administer Avaya Proactive Contact and Geomant User

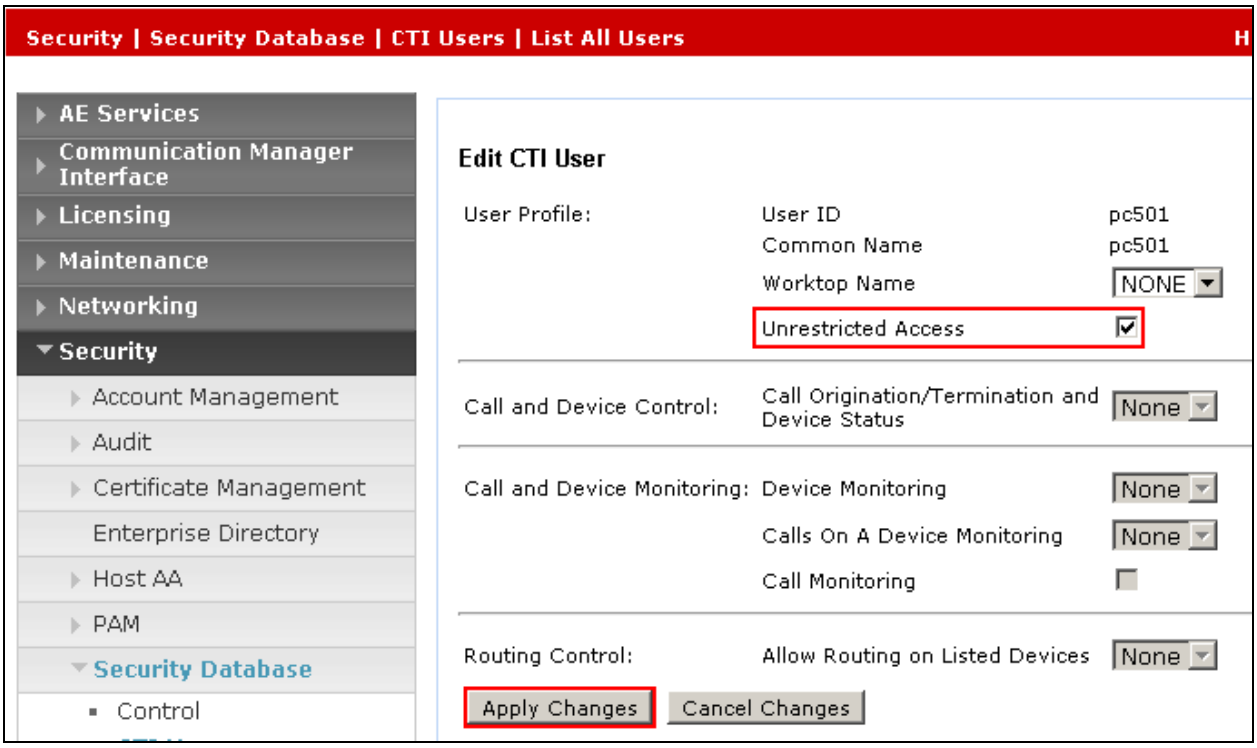
A user must be configured for both Geomant and the Proactive Contact. Select **User Management → User Admin → Add User** from the left pane to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click Apply at the bottom of the screen (not shown below).



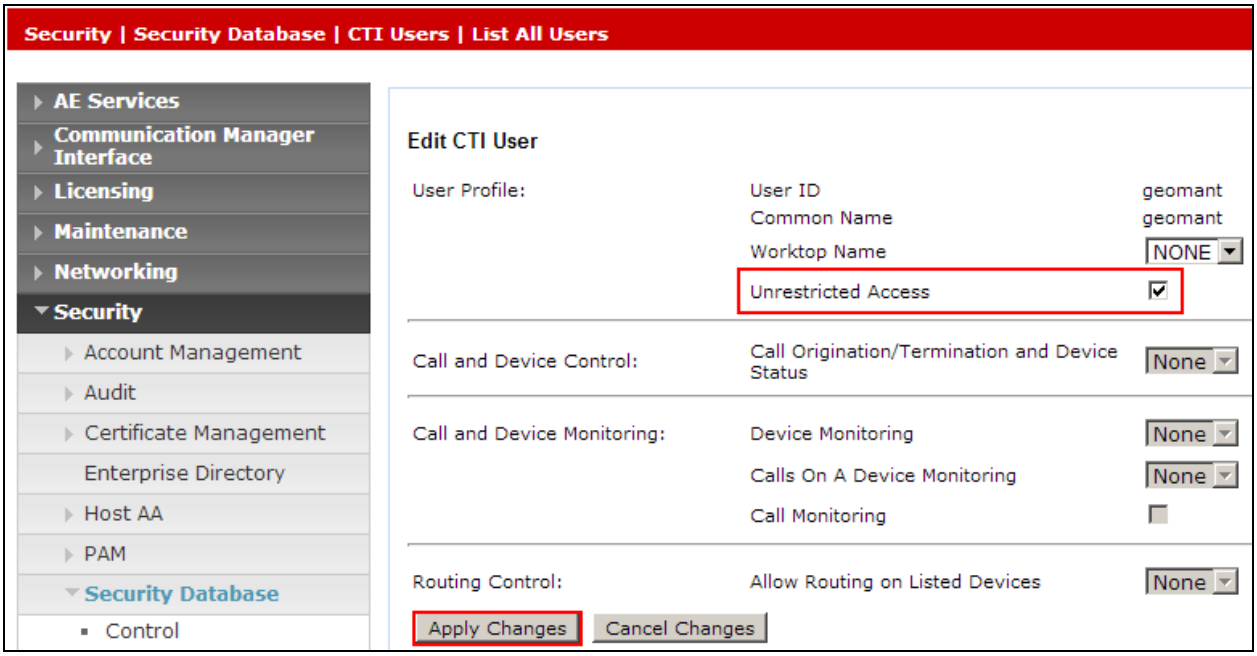
Repeat the steps above to create the Geomant user. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).



In addition, the user which will be used by Proactive Contact and Geomant should be configured as an unrestricted user. Select **Security→ Security Database → CTI Users → List All Users** from the left pane, click on the radio button beside the user created above, in this case, **pc501** and click **Edit.** Place a tick in the box next to **Unrestricted Access**, as shown in the image below. Click **Apply Changes** when done.



Repeat the process for the Geomant user.



7. Configure Avaya Proactive Contact

This section provides the procedures for configuring Proactive Contact. The procedures include the following areas:

- Configure CTI Parameters
- Configure Proactive Agent Blend Domains
- Configure master.cfg
- Configure number format
- Configure the calling list
- Configure Avaya Proactive Contact Administration Software

7.1. Configure CTI Parameters

In order to establish the TSAPI link between Proactive Contact and AES for Proactive Agent Blend enter the following command at the Proactive Contact shell. This will create a cti_passwd.cfg file in /opt/avaya/pab/config/

- **cti_passwd -b** (b denotes the blend option).

When prompted for the password, enter the password administered to the CTI user configured for Proactive Contact earlier on Application Enablement Services, and hit return, re-enter as requested.

For the purposes of Agent Blending, copy the .tslibrc file to the **/opt/avaya/pab/config/** directory by entering the command **cp /opt/avaya/pds/config/.tslibrc /opt/avaya/pab/config/.tslibrc.** Edit the newly copied **.tslibrc** file with the IP address of Application Enablement Services.

```
[Telephony Servers]
; This is a list of the servers offering Telephony Services via TCP/IP.
; Either domain name or IP address may be used; default port number is 450
; The form is: host_name=port_number   For example:
;
; tserver.mydomain.com=450
10.10.16.96
;

; This file should be copied to CONFIG directory as .tslibrc.
; See master.cfg for the directory name.

; This entry overrides the [Telephony Servers] section, if any.
```

Navigate to **/opt/avaya/pds/config** – edit **opmon.cfg** as shown below:

```
CFGTIME:15
DIALBACK:1-15:15:1::
DIALBACKNUM:ALL
```

Edit **dgswitch.cfg** as shown below. The format used is based on the location of the ports in the PG230 Digital Switch; therefore Proactive Contact is configured with the same number of Inbound Ports as the number of inbound lines on the PG230 Digital Switch. The inbound ports configured on Proactive Contact correspond to the ports of the inbound trunk group configured on Communication Manager in **Section 5.6**, the same is true for Headset, Outbound and Transfer trunk ports.

```
# Headset Ports
H:1:361:1::#H:15:1:1-1-21-4-2
H:2:362:1::#H:15:1:1-1-21-4-3
H:3:363:1::#H:15:1:1-1-21-4-4
H:4:364:1::#H:15:1:1-1-21-4-5
H:5:365:1::#H:15:1:1-1-21-4-6

# Normal Outbound Trunks
N:1:366:1::#O:10:1:1-1-21-4-7
N:2:367:1::#O:10:1:1-1-21-4-8
N:3:368:1::#O:10:1:1-1-21-4-9
N:4:369:1::#O:10:1:1-1-21-4-10
N:5:370:1::#O:10:1:1-1-21-4-11
N:6:371:1::#O:10:1:1-1-21-4-12
N:7:372:1::#O:10:1:1-1-21-4-13
N:8:373:1::#O:10:1:1-1-21-4-14
N:9:374:1::#O:10:1:1-1-21-4-15
N:10:375:1::#O:10:1:1-1-21-4-16

# Normal Inbound Trunks

N:11:377:1::#I:11:1:1-1-21-4-18
N:12:378:1::#I:11:1:1-1-21-4-19
N:13:379:1::#I:11:1:1-1-21-4-20
N:14:380:1::#I:11:1:1-1-21-4-21
N:15:381:1::#I:11:1:1-1-21-4-22


# Transfer-thru Trunks
T:1:12:1::#T:12:1:1-1-21-4-1
```

Edit only the last 4 lines of **voicemsg.cfg**, this file refers to the announcements recorded on the PG230.

```
250:greeting:1027:Female:Folder4:Voice:Message27
251:inbound:1028:Female:Folder4:Voice:Message28
252:outbound:1029:Female:Folder4:Voice:Message29
253:notLoggedIn:1030:Female:Folder4:Voice:Message30
```

Navigate to the **/opt/avaya/pds/scripts** directory and copy the telephny_hd.spt file to the telephny.spt file using the following command **cp telephny_hd.spt telephny.spt**. This file defines Hard Dialer specific parameters.

Navigate to the **/opt/avaya/pab/config/** directory. Copy and rename the **ctirc.cvct** file, by typing **cp ctirc.cvct ctirc1.** Edit **ctirc1** as shown below.

```
################################################################################
#
# LAST REVISION $Date: 2002/02/20 16:24:55 $
################################################################################
#
# The only configurable line is the 14th line after the comments (third from
# the bottom). There are five fields in this line:
# Field 1: TLINK
# Field 2: Login name for CVCT (run "cti_passwd -b" to setup the encrypted
password)
# Field 3: Application Name (PDS)
# Field 4: TS2 - This is the library version that we used.  Do no change.
0                              # CVCT CEP (switch type)
0x11                           # CEP CHGSVR
0x2015A                        # Supported Events
0                              # Stats and Counts (No MIS for Aspect)
0                              # Appear and Vanish (No LM for Aspect)
0                              # Agent Available, Login, Logout
0                              # per-outstanding-move (N/A for Aspect)
0                              # seconds added to LM (N/A for Aspect)
0                              # seconds added to LC (N/A for Aspect)
Port SupId SupPass
NotUsed
AVAYA#CM62#CSTA-S#AESSERVER62:pc501:PDS:TS2
chgsvr
cep_pway
```

Copy and rename the CBA_procs.example file, type **cp CBA_procs.example CBA_procs** and press **Enter**. Edit **CBA_procs** as shown below with the Proactive Contact server hostname:

```
#########################################################################
#                          |Max Wait|Max Wait|Max Wait|Max Wait|Kill
#                          | Before | Before | Before | Before |Cfg-
# Process|Startup|Shutdown|Shutdown|  Abort | SIGTERM| SIGKILL|Only
#   Type | Order | Order  | Message| Message| Signal | Signal |Mode
#-----------------------------------------------------------------------
# NOTE - Startup Order and Shutdown Order MUST start at the value one(1) and
#        increment WITHOUT any sequence gaps
PROCESS_CONTROL
SOE| 1 | 5 | -1 | -1 | -1 | 25 | 0
USR| 2 | 4 | -1 | -1 | 21 | 24 | 0
CTI| 3 | 3 | 11 | 15 | 24 | 35 | 1
ACD| 4 | 2 |  0 | 5 | 10 | 11 | 1
MSC| 5 | 1 | -1 | -1 | -1 | 25 | 0


#############################################################
# Process | Host | Path | Binary | Parameters
#  Type   | Name |      |  Name  |
#-----------------------------------------------------------
PROCESS_INSTANCE
USR|devconhd501|/opt/avaya/pab/bin/|cbauser|1
CTI|devconhd501|/opt/avaya/pab/bin/|cti|1
ACD|devconhd501|/opt/avaya/pab/bin/|acdmon|1 nocancel min_asa 2sec gen_rel
MSC|devconhd501|/opt/avaya/pab/scripts/|acdsnap_mon|
```

Copy and rename the CBA_cfg.example file, type **cp CBA_cfg.example CBA_cfg** and press **Enter**. This establishes the Application, PBX and Gateway IDs used by Agent Blending.

7.2. Configure Proactive Agent Blend Domains

Proactive Contact needs to be configured with the inbound VDN to be monitored and the acquire VDN for acquiring agents in order to handle calls from the outbound job. The Proactive Contact name for a VDN is Domain. Configured in **/opt/avaya/pab/config/dom_group.data** – this defines an outbound only Domain Group called **NORTH_USA**, an **IB** (inbound) Domain called **5812** with specific reference to **VDN 5812**, and a **TEAM** (acquire) Domain called **5811** with specific reference to **VDN 5811**. Both of these Domains have a Domain Group ID of **NORTH_USA**.

```
*VERSION | 1
############################ Defined Domains Groups ########################
# Domain Group Record Layout - To Create a new domain group copy the template
#      below and replace all field holders with appropriate values.
#   NOTE - All fields that retain their place holder values(TR,TT,etc)
#           will be assumed to be empty.
#   NOTE - Line breaks may happen between any fields but not within a field
#   NOTE - Do not change lower case field holders
#
#   WARNING - Remove the "#" comment field indicator to activate the template
#
# TEMPLATE
# ------------------------------------------------------------------------
---
# *DG | DG_NM | dg_id | RTI | CM | MAAS | SC | DSL | MSL |
#  AUT | MAO | TR | TT | ACWT | MQR | afi | rti |
# ------------------------------------------------------------------------
---
#
# Description of fields within a Domain Group
# -----------------------------------------
# *      - Start Of New Record { MUST be in first column of record}
# DG     - Domain Group Record Key   { Always DG}
# DG_NM  - Domain Group Name {Descriptive name use by UI to specify a domain}
# dg_id  - Domain Group ID { FILLED IN BY SYSTEM}
# RTI    - Time Interval (hours)
# CM     - Control Method {ASA-Avg.Spd Answered,SL-Sevice Lvl,OB_ONLY-
Outbound}
# MAAS   - [Target] Average Speed to Answer (seconds)
# SC     - Service Criterion (seconds)
# DSL    - Desired Service Level (%)
# MSL    - Abatement Service Level (%)
# AUT    - Traffic Intensity Threshold (%)
# MAO    - Minimum # of Agents on Outbound (# agents)
# TR     - Initial Traffic Rate (calls/second)
# TT     - Minimum Talk Time (seconds)
# ACWT   - Minimum After Call Work Time (seconds)
# MQR    - Minimum Queued for Release (OB_ONLY groups)
# afi    - Acquisitions From Inbound { FILLED IN BY SYSTEM }
# rti    - Releases To Inbound       { FILLED IN BY SYSTEM }
#

*DG | NORTH_USA | 1 | RTI | OB_ONLY | MAAS | SC |
```

```
      DSL | MSL | AUT | MAO | TR | TT |
      ACWT | 0 | afi | rti |

########################## Defined Domains ########################
# Domain Record Layout - To Create a new domain copy the template below
#    and replace all field holders with appropriate values.
#    NOTE - All notes/warnings from domain group field still apply.
#
# TEMPLATE
# ------------------------------------------------------------------------------
# *DM | DM_ADRS | DM_EXT | DG_NM | dg_id | AP_ID | PBX_ID | GW_ID | DM_TYP |
# ------------------------------------------------------------------------------
#
# Description of fields within a Domain
# ----------------------------------------
# *      - Start Of New Record {MUST be in first column of record}
# DM     - Domain Record Keyword   {Always DM}
#
# DM_ADRS- Domain Address
# DM_EXT - Domain Phone Number
# DG_NM  - Domain Group Name {Descriptive name use by UI to specify a D.G.}
#                     Use TRANS if defining a floating transient domain.
# dg_id  - Domain Group ID {FILLED IN BY SYSTEM}
# AP_ID  - PDS ID
# PBX_ID - PBX ID
# GW_ID  - Gateway ID
# DM_TYP - Domain Type -- one of:
#                     IB          - Inbound,
#                     TRANS   - Transient Acquire,
#                     TEAM    - Team Acquire,
#                           OV_FLOW - Overflow
#

*DM | 5811 | 5811 | NORTH_USA | 1 | 1 | 1 |
      1 | TEAM |

*DM | 5812 | 5812 | NORTH_USA | 1 | 1 | 1 |
      1 | IB |
```

Edit **acd_ext.cfg** – this contains the Communication Manager extension number into which Proactive Agent Blend agents will be logging in, as show below, extension **6000** is the extension onto which agents are logged into in this case:

```
1:6000
```

Agent Blend is a feature add-on for Proactive Contact. Ensure that the PDS service is stopped and as root, enter the command **menu install** which will run a script. When prompted select option **2. Value added products**, and then **2** again for **Install Predictive Agent Blend.** Follow the instructions prompted on screen as shown below. The information presented will display some of that configured previously in this Section.

```
Have you stopped PDS processes: y
Following AES servers are configured:
10.10.16.96 Do you want to add another AES server: n
CTI password seems to be already set in /opt/avaya/pab/config/cti_passwd.cfg
Do you wish to change the CTI password? n
AES_LINK set to AVAYA#CM62#CSTA-S#AESSERVER62
Do you want to change it now?: n
AES_USER set to pc501
Do you want to change it now?: n
Do you wish to configure Domains now?: n
Do you wish to change number of users that can be acquired for outbound
calling now?: n
Now we'll install ACD extensions
Enter q to quit
When prompted, press any key to continue.
Enter 0 to exit, and 0 again
```

7.3. Configure master.cfg

Amendments to the master.cfg file, located in /opt/avaya/pds/etc were made as follows.

```
CALL_BLENDING:YES
DBKGROUP:15,1,1
DBSERVERIP:10.10.16.95
IICB_HOST:devconhd501
INBNDSYS:YES
LINEASSIGN:REG,O=1-10;INB,I=11-15
NAMESERVICEHOST:devconhd501
OPERATORS:5
OPLIMIT:I=5,O=5,B=5,P=5,M=5
PORTS:15
PRIMARY:YES
SWITCHNAME:switch1
SWITCHTESTMODE:NO
SWITCHTYPE:DIGITAL
VISUAL_CPA:YES
WEBLMURL:http,//10.10.16.95,8080/WebLM/LicenseServer:
```

Note: **INBNDSYS** was set to **YES** for the purposes of NVDT testing.

7.4. Configure Number Format

The phonefmt.cfg file located in **/opt/avaya/pds/config** contains details of how Proactive Contact needs to manipulate numbers in the calling list in order to successfully place them. The final line in the file is configured as follows:

```
STD_TO_DIALFMT:*:ALLTYPES:0:::
```

In this instance, of the digits dialed, **0** are deleted and the call is routed to Communication Manager. It is assumed Communication Manager has the necessary configuration required to route the call accordingly.

Proactive Contact is delivered with default calling lists. The author assumes an inbound and outbound calling list is created in Proactive Contact Editor. The administration of calling lists is outside of the scope of this document. For the purposes of the compliance test, calling list 4 (list4) was used.

7.5. Configure Avaya Proactive Contact Supervisor Software

In order for the Proactive Contact Editor application to communicate with the Proactive Contact Server, the PC on which it resides must be configured.

7.5.1. Configure Windows Host File

Edit **%WINDIR%\system32\drivers\etc\hosts** to include the hostname and IP address of the Proactive Contact Server, as follows.

```
10.10.16.95 devconhd501
```

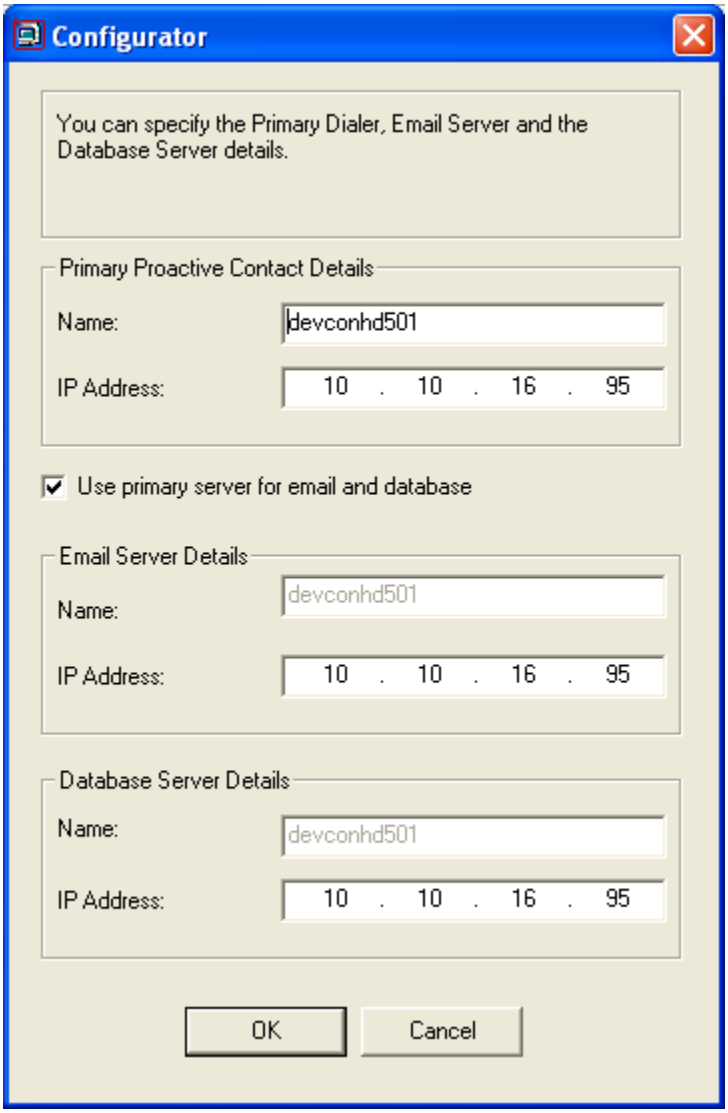
7.5.2. Check Avaya Proactive Contact Services

Ensure all necessary services are running on the Proactive Contact Server. The following commands start, check and stop the db, mts, and pds services, which must be stopped and started in the order shown. All services must be started before proceeding.

start_db
start_mts
start_pds
check_db
check_mts
check_pds
stop_pds
stop_mts
stop_db

7.5.3. Configure Avaya Proactive Contact Supervisor Software

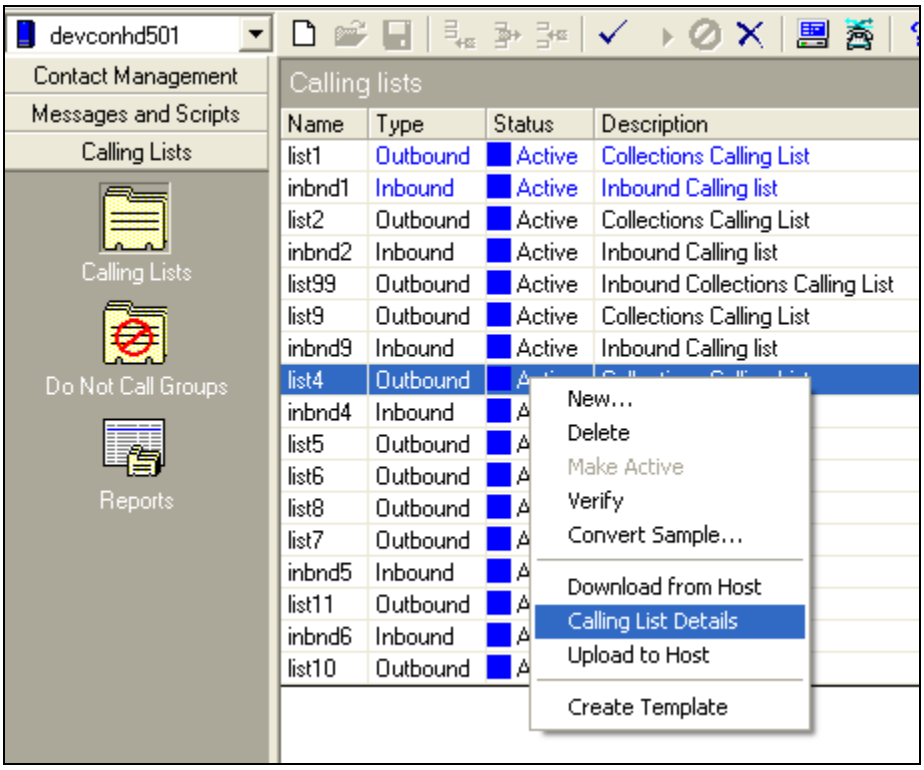
Double click on the Health Manager icon on the desktop. The Screen below will be presented, complete it as shown with the Proactive Contact IP address and hostname



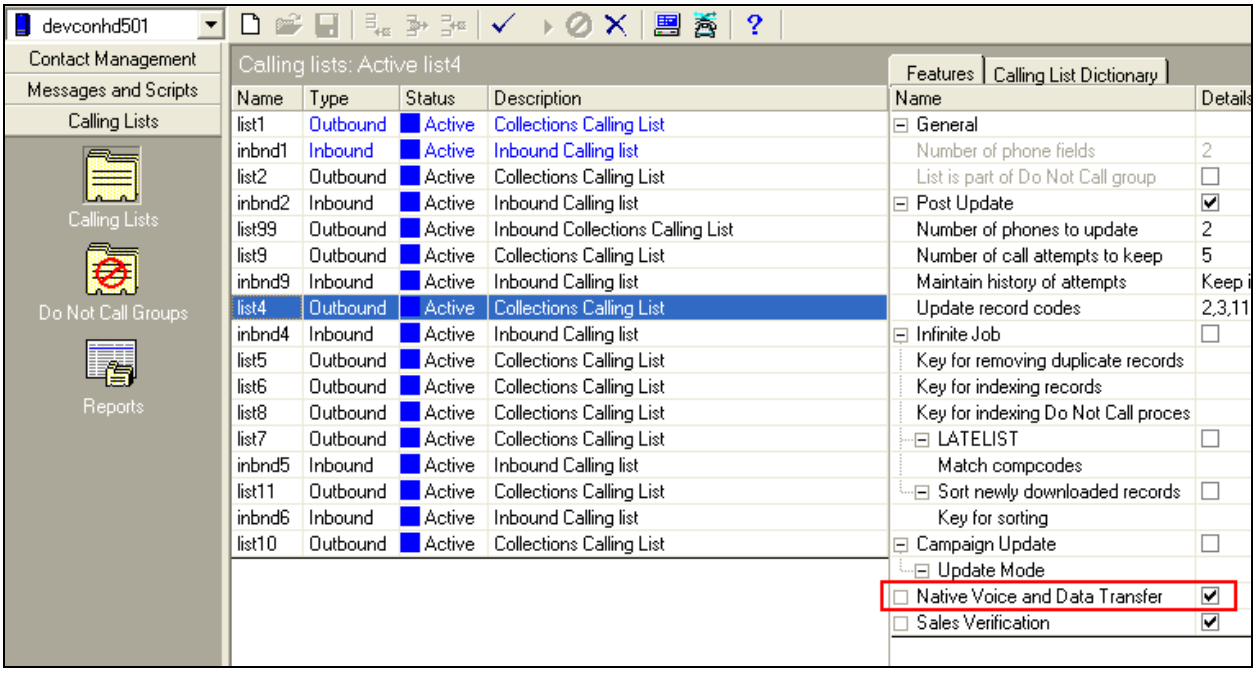
It is now possible to log in to the Health Manager with the sysadm login credentials. Close Health Manager and double click on the Editor icon on the desktop. Log in with the sysadm login credentials.

7.5.4. Configure Native Voice and Data Transfer Parameters (NVDT)

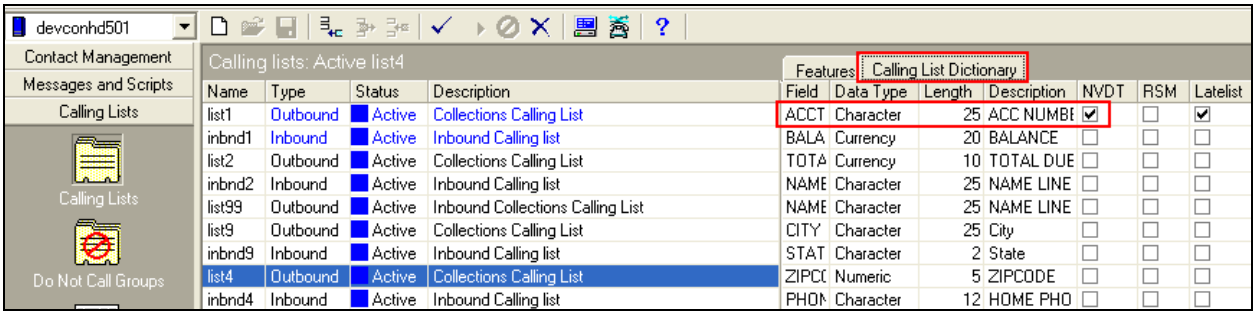
NVDT is the feature used when transferring caller details from the outbound job to the inbound job. In this instance, an agent logged into the inbound job will receive the account number as well as the voice path. These parameters are configured in the calling list, as shown below. In the left hand pane click **Calling Lists → Calling Lists,** right click on **list4** and select **Calling List Details.**



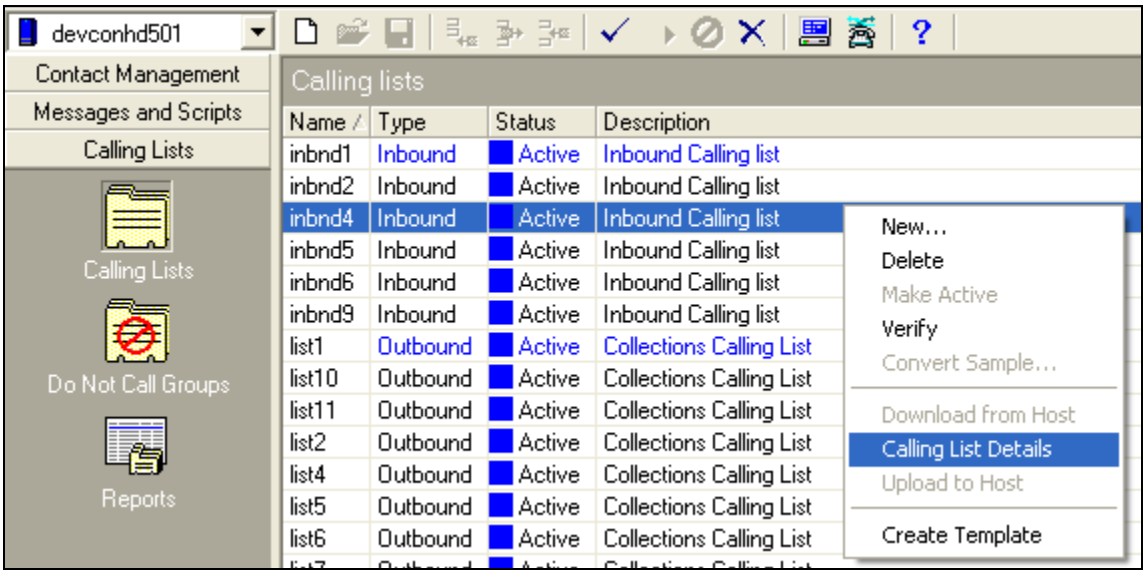
Click to place a tick in the field to enable NVDT (**Native Voice and Data Transfer**).



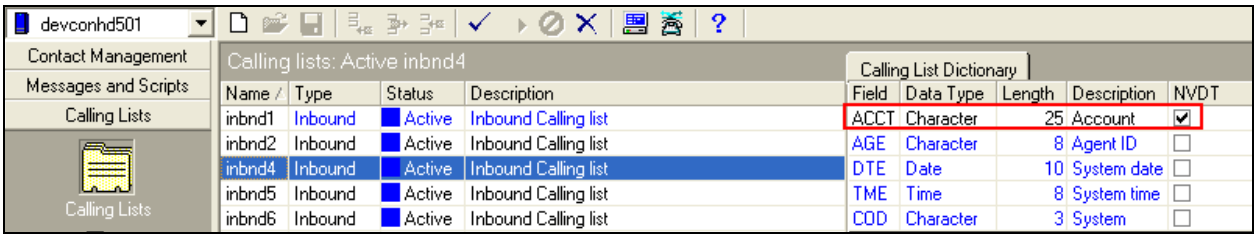
Click on the **Calling List Dictionary** Tab, and click to place a tick in the **NVDT** column next to **ACCTNUM**. Ensure the **Length** field is set to **25**. Save when completed.



The same needs to be performed for the **inbnd4** list. Right click on **inbnd4** and select **Calling List Details.**

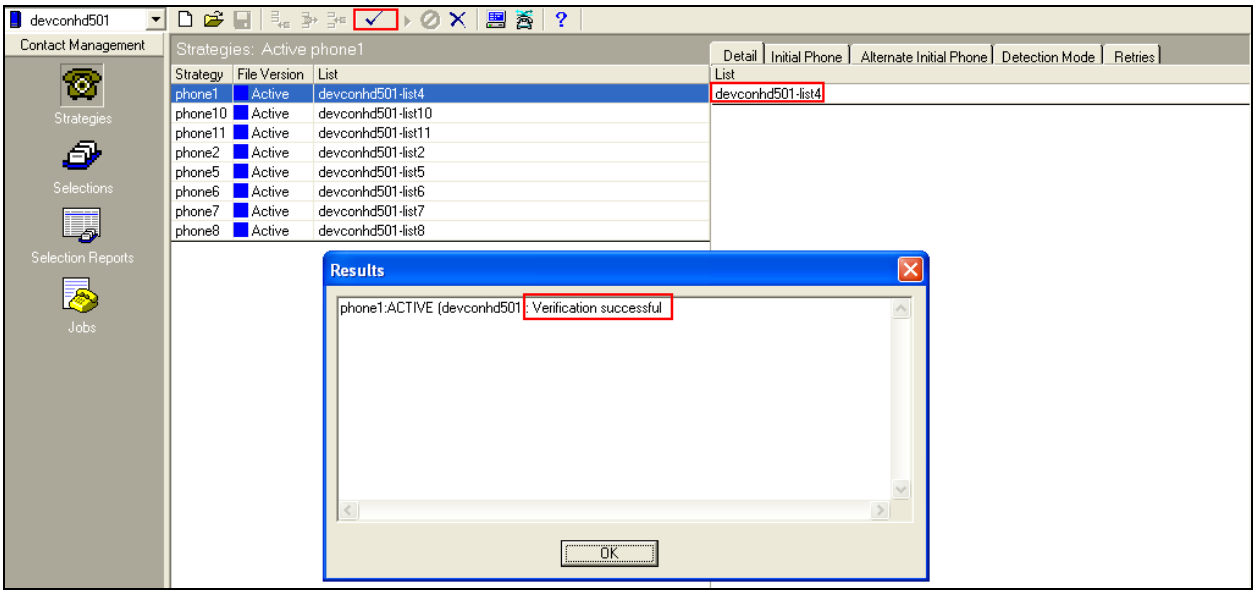


Click to place a tick in the **NVDT** column next to **ACCTNUM**. Ensure the **Length** field is set to **25**. Save when completed.



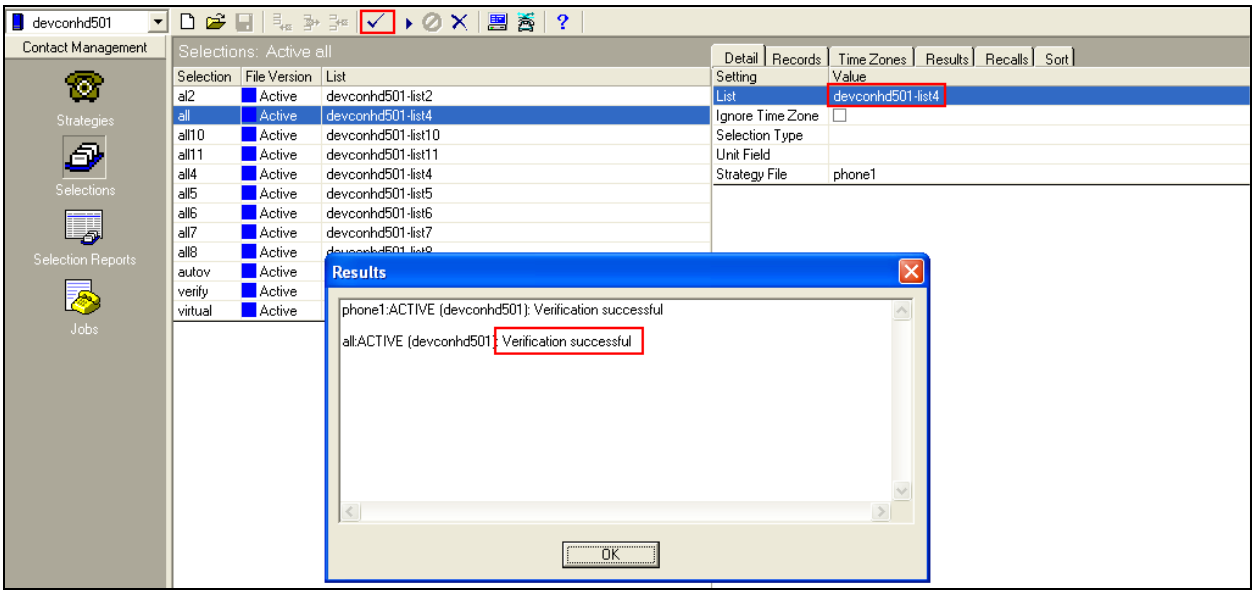
7.5.5. Configure Strategy

Assuming that strategy **phone1** and calling list **list4** (as specified in the previous section), are being used, configure editor as shown below. Click verify and ensure verification is successful.

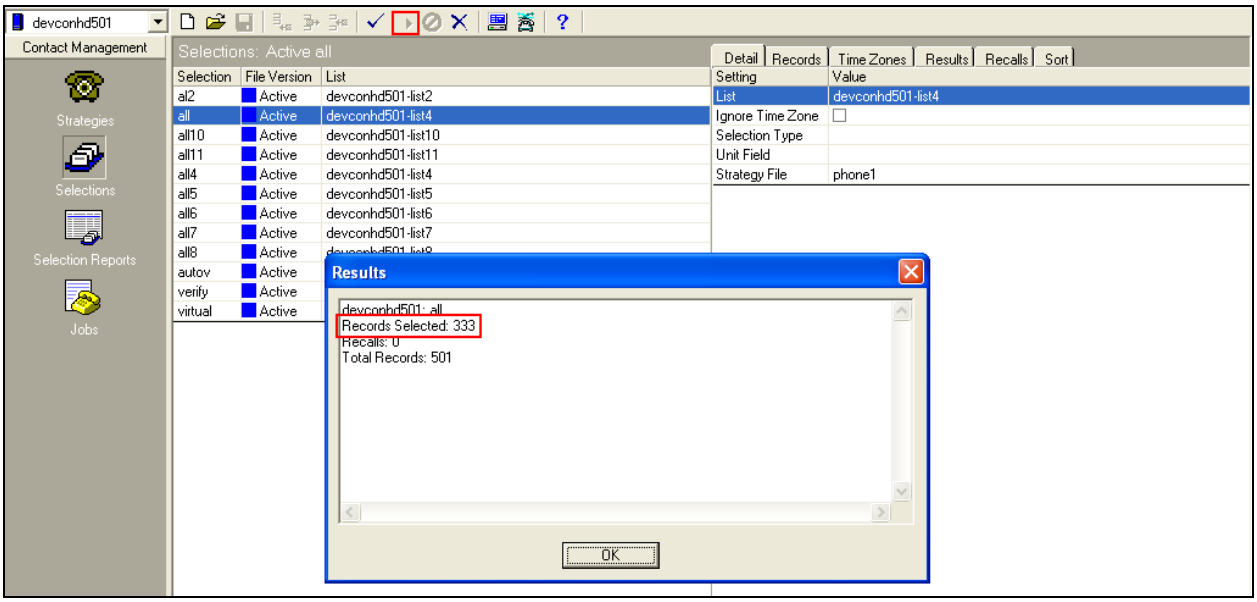


7.5.6. Configure Selections

Click **Selections**, select **all**, and specify calling list **list4**, click verify and ensure verification is successful.

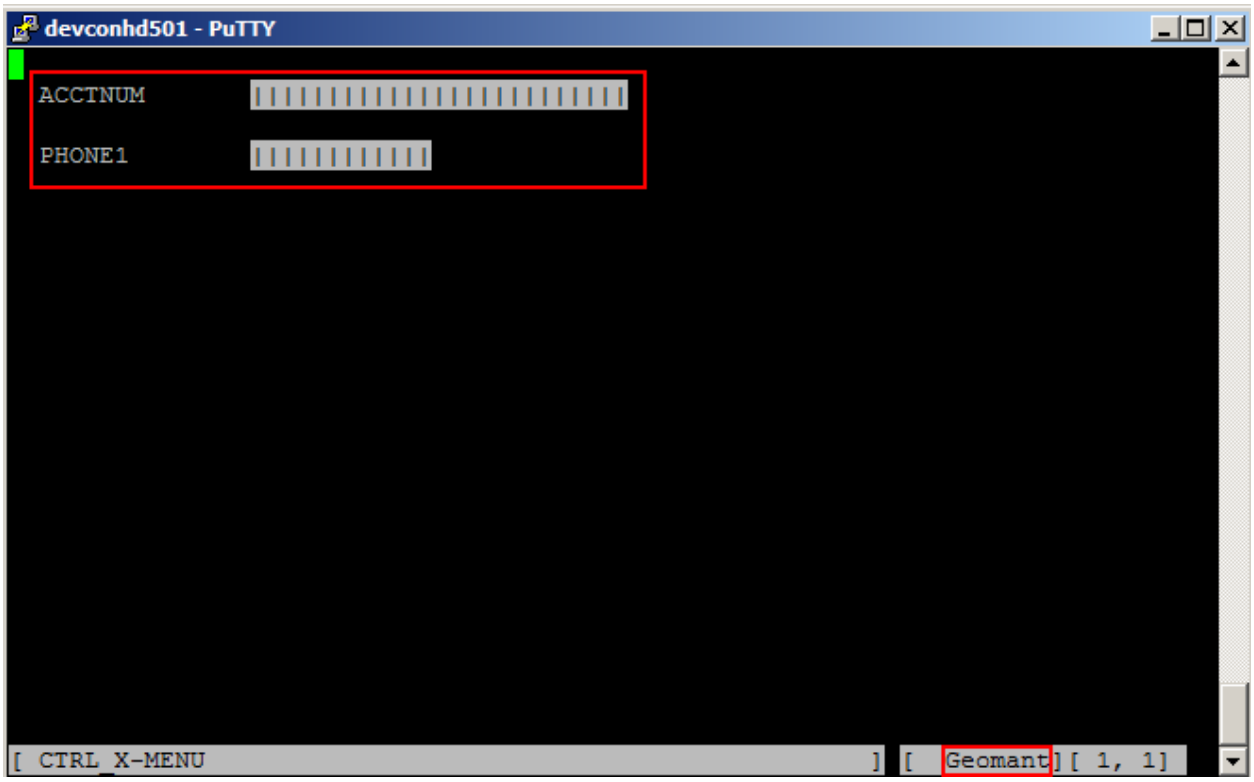


Click run , and ensure that the selection selected includes some records.



7.5.7. Configure Agent Screen

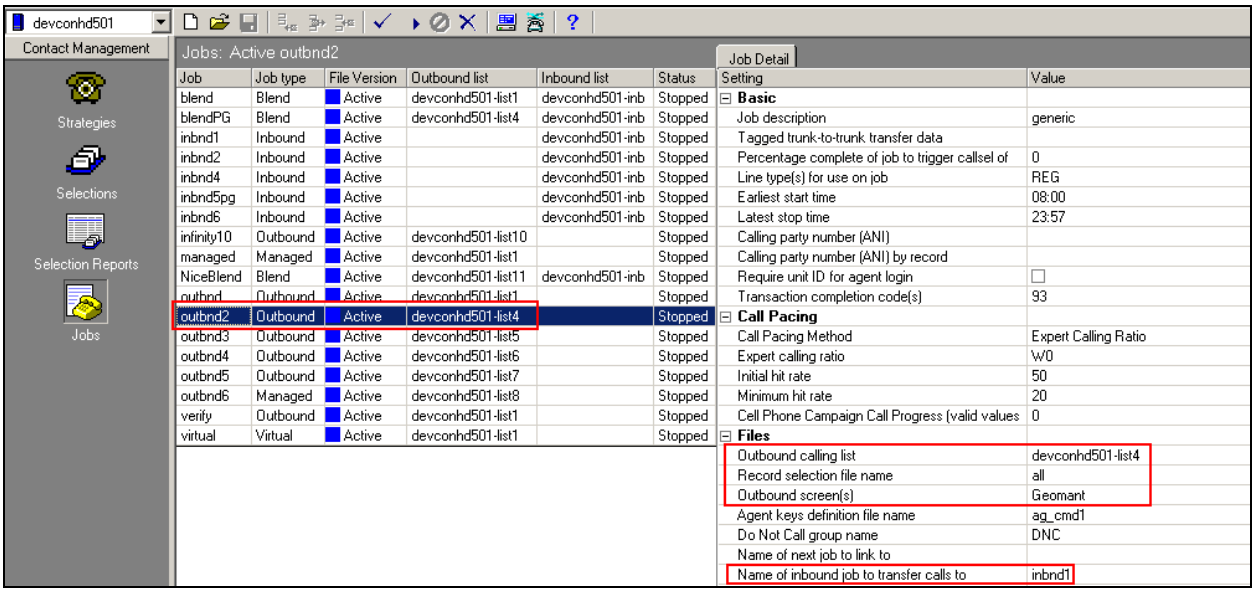
An agent screen must be configured. This defines the information presented to the agent from the calling list when an outbound call is delivered to an agent. From the Proactive Contact command line enter the command **menu system**, choose option **2. Calling lists** followed by option **6. Build screens** to build a screen with the required information to be presented to the agent. In the screenshot shown below the **ACCTNUM** and **PHONE1** fields have been chosen and the screen is named as **Geomant**.



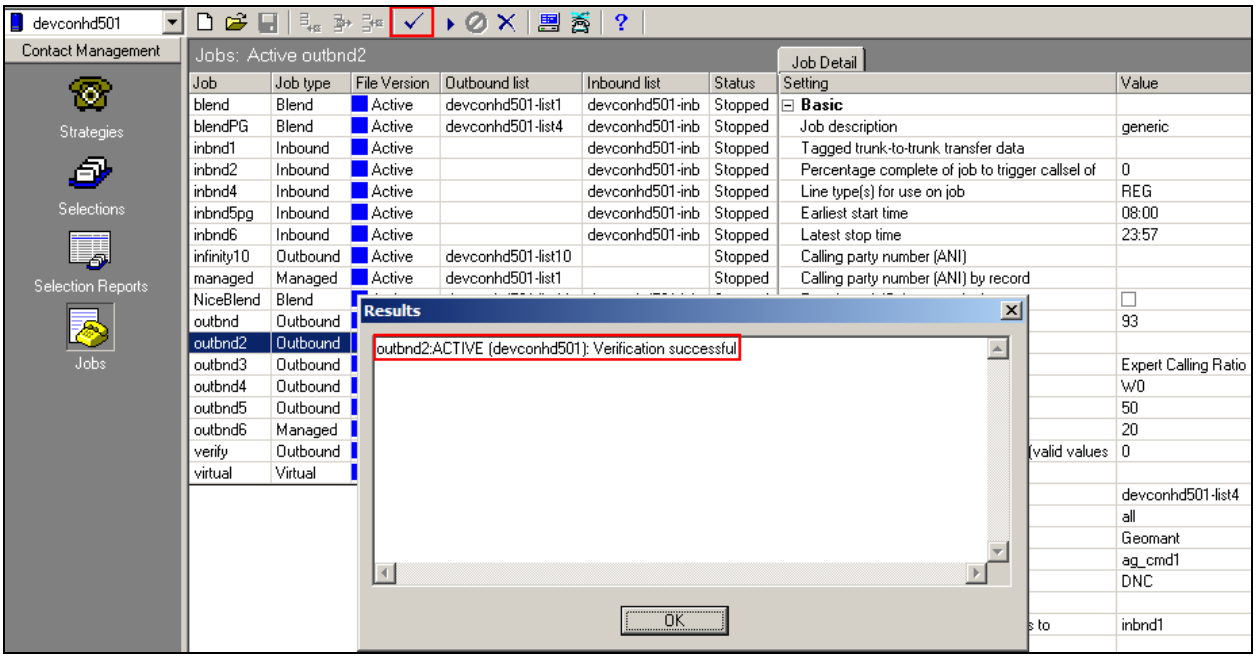
7.5.8. Configure Outbound Job

Click **Jobs,** select **outbnd2** and configure as shown with **Outbound calling list list4**. Set the **Record selection file name** to **all** and the **Outbound screen(s)** to **Geomant.**

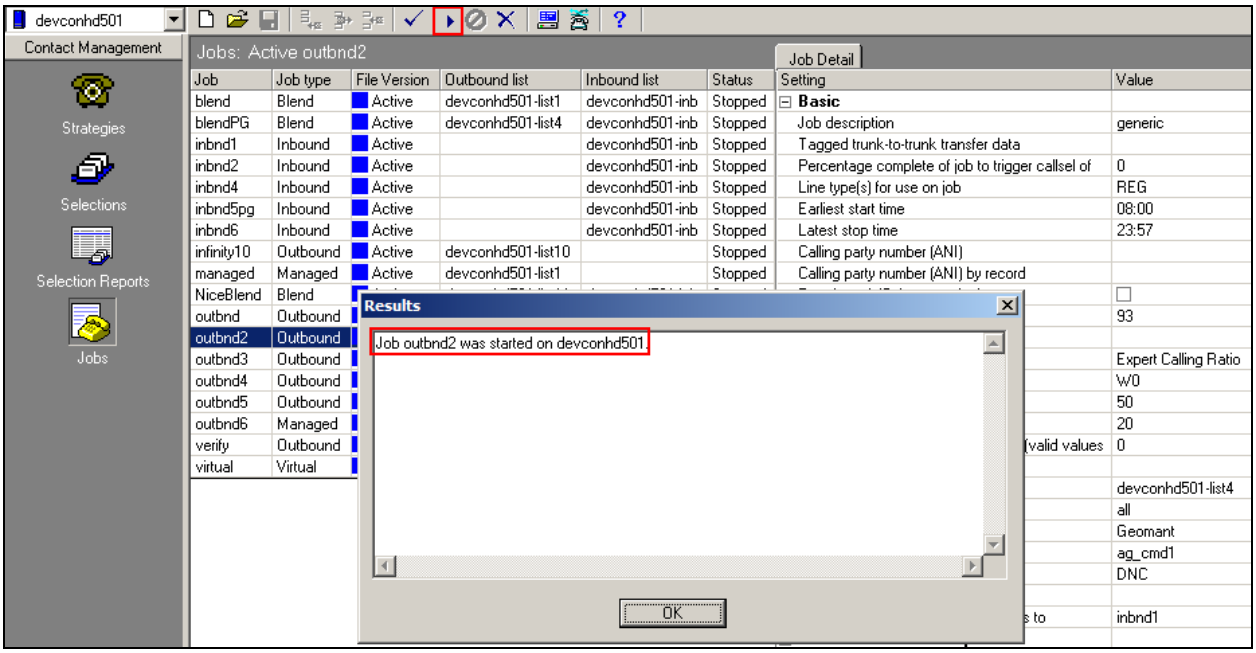
Note: Name of inbound job to transfer calls to is set to **inbnd1** - this relates to the NVDT feature.



Click verify and ensure verification completes successfully.



Start the job by clicking  .

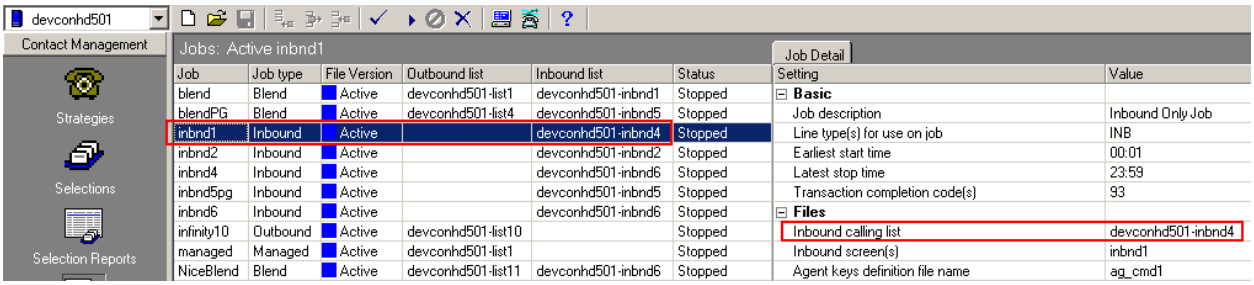


The outbound job is now running, and Proactive Contact will be initiating outbound calls to Proactive Contact Agents, once logged in.

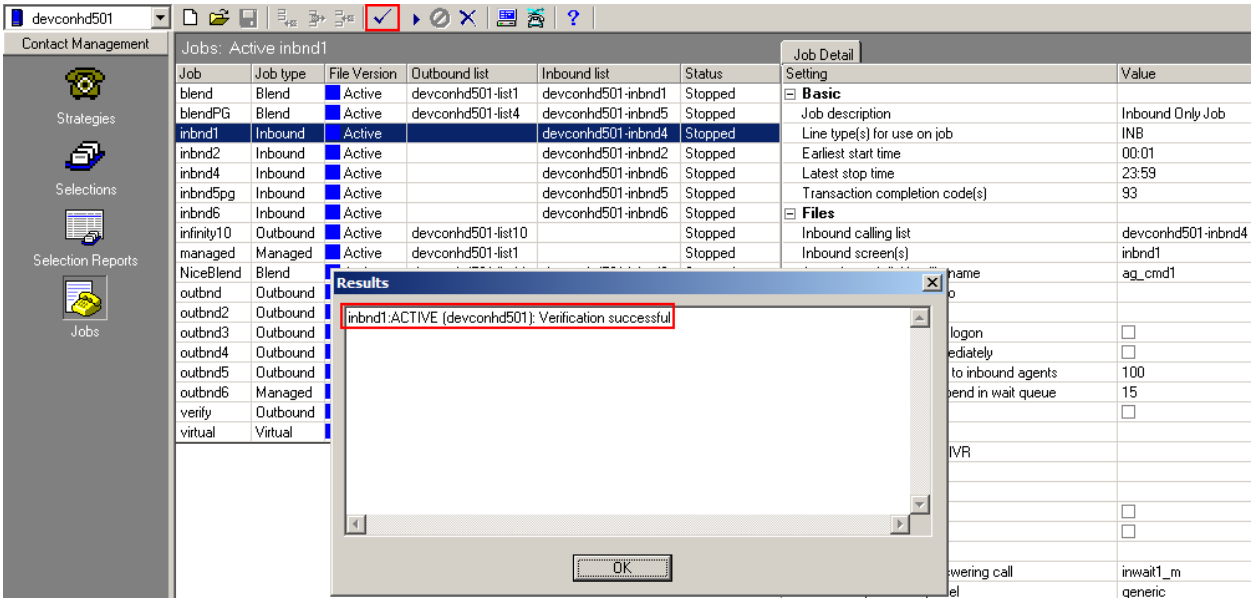
7.5.9. Configure Inbound Job

7.5.10. Configure Inbound Job

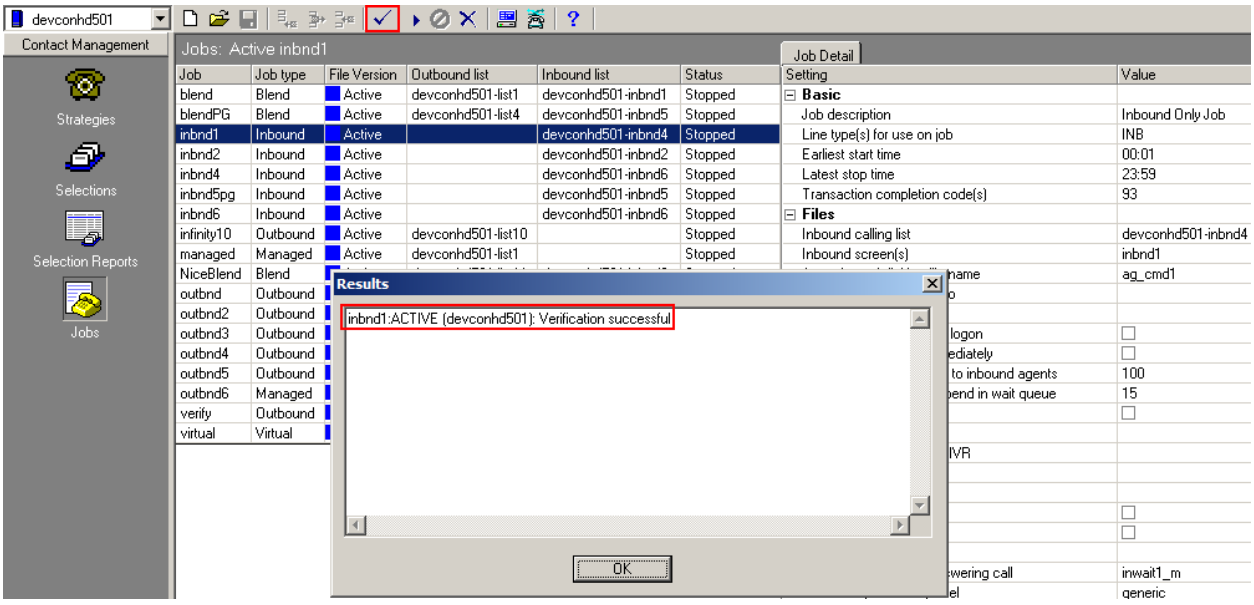
Click **Jobs** select **inbnd1** and configure as shown. This is the job used to for the NVDT feature as noted above.



Click verify  and ensure verification completes successfully.



Start the job by clicking  .



If the job fails to run as expected, ensure the job file within the **/opt/avaya/pds/job/** directory has the following parameters set:

```
TESTMODE::
TESTOPER::
```

8. Configure Geomant Unified Agent

The installation, configuration and commissioning of Unified Agent is managed and facilitated by the Geomant Delivery team and involves the full installation, configuration and deployment of all components of the Unified Agent solution.. This section provides the procedures for configuring Unified Agent to interoperate with the Avaya solution. The process can be summarized as follows:

- Configure CTI Connection
- Configure Dialer Connection
- Configure Acquire VDN

8.1. Configure CTI Connection

Unified Agent uses the Geomant CCI service to connect with Application Enablement Services using a TSAPI connection. Using an appropriate text editor to open the **GeoCCISrv.exe.properties** file, which by default is located in the **C:\Program Files\GeoCCI** directory on the Unified Agent server and configure the following:

- **JTAPIServer** – enter IP address of Application Enablement Services
- **JTAPILink** – enter the Tlink name obtained in **Section 6.5**
- **JTAPIUser** – enter the CTI User configured for Geomant in **Section 6.6**
- **JTAPIPassword** – enter the CTI User password configured for Geomant in **Section 6.6**

As shown in the extract below.

```
#Service specific configuration
#JTAPI config
JTAPIServer=10.10.16.96
JTAPIPort=450
JTAPILink=AVAYA#CM62#CSTA#AESSERVER62
JTAPIUser=geomant
JTAPIPassword=Geomant123!
```

8.2. Configure Dialer Connection

Unified Agent uses the Geomant APC service to connect with the Proactive Contact Agent API. Using an appropriate text editor to open the **GeoCCIAPCServer.exe.config** file, which by default is located in the **C:\Program Files\GeoCCIAPC** directory on the Unified Agent server and configure the following:

- **Dialer.[number].Address** – enter IP address of Proactive Contact
- **Dialer.[number].Port** – enter the port the Proactive Contact Agent API uses (default 22700)

As shown in the extract below.

```
    <add key="Dialer.0.Name" value="LAB_DIALLER"/>
    <add key="Dialer.0.Address" value="10.10.16.95"/>
    <add key="Dialer.0.Port" value="22700"/>
```

The **apcdialer.properties** file contains the settings for the Unified Agent Tomcat Application auto-update functionality. The Unified Agent Tomcat Application performs a daily download of the .job and .ky files located on the dialer at a defined time. The download process involves the use of SFTP protocol to perform this transfer. The user configured in this file needs to have privileges for remote file transfer, in this instance the admin user was used. Using an appropriate text editor to open the **apcdialer.properties** file, the location of which depends on the implementation, and configure the following:

- DialerIP – IP address of Proactive Contact
- DialerPort – SSH port for connection to Proactive Contact for SFTP transfer
- DialerUser – username for SSH connection
- DialerPass – password for user.

```
Dialer=LAB_DIALLER
DialerIP=10.10.16.95
DialerPort=22
DialerUser=admin
DialerPass=xxxxx
DialerPath=/opt/avaya/pds/
```

8.3. Configure Acquire VDN

The **ctiagent.properies** file contains settings related to the Unified Agent Tomcat Application CTI integration, including the address and port used for internal communication with the Geomant CCI Server, extension number ranges and length, the prefix for external dialing and the Acquire VDN to be monitored for the PAB feature. Using an appropriate text editor to open the **ctiagent.properties** file, the location of which depends on the implementation, and configure the following:

- OutsideNumPrefix – set this to the number used to dial externally
- InsideNumLength – set this according to the extension number and length used by agents
- BlendSkills - set this to the VDN of the aquire skill used by PAB as configured in **Section 5.3**

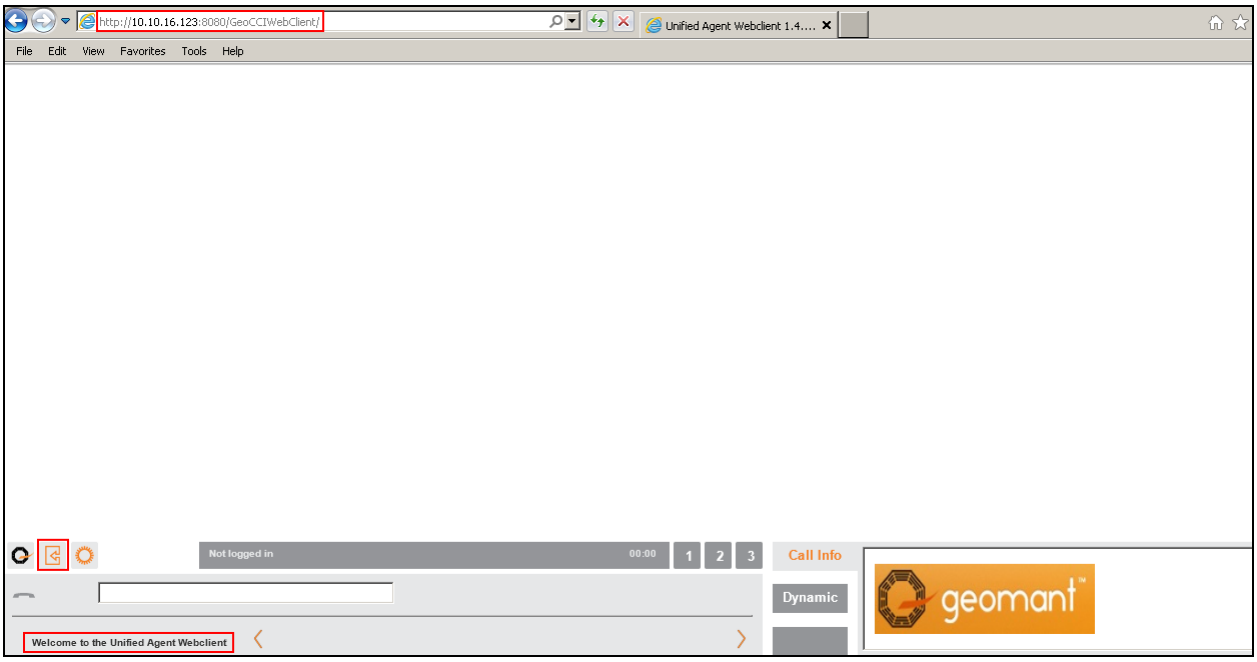
```
OutsideNumPrefix=9
InsideNumLength=4|6
ReasonCodes=1|Away from Desk;2|In a Meeting;3|At Lunch;4|Do not disturb;5|On
a break;6|Manual Outbound;7|At a training session;8|Post
#ForceAccept values: empty, autoaccept, manualaccepty
ForceAccept=
#ConferenceEnabled values: 1 - enabled, 0 - disabled
ConferenceEnabled=1
ClientTimeout=30000
BlendSkills=5811
```

9. Verification Steps

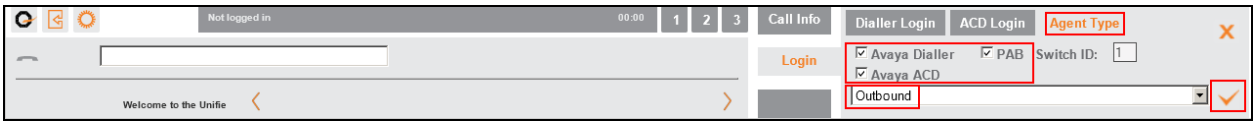
This section provides the tests that can be performed to verify proper configuration of Unified Agent, Proactive Contact, and Application Enablement Services. Prior to verification, start an outbound job on Proactive Contact.

9.1. Verify Geomant Unified Agent

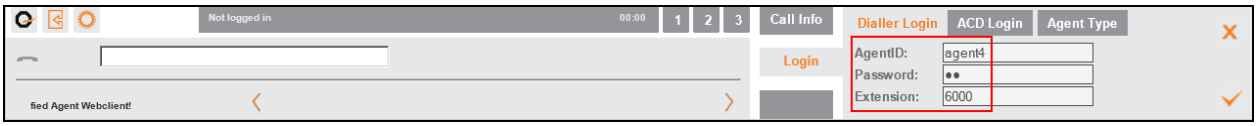
From the agent PC navigate to the URL of the Unified Agent web client, in this case http://10.10.16.123:8080/GeoCCIWebClient/, the info area will display a welcome message, click the **login** icon.



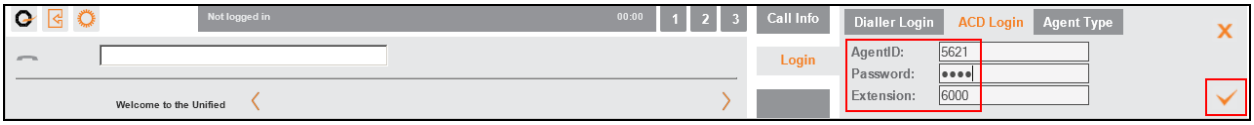
Click the **Agent Type** tab and enter the agent type as required. In the example below, **Outbound** is selected from the drop down list, and the **Avaya Dialler**, **PAB** and **Avaya ACD** tick boxes are checked – this configuration pertains to logging in an agent for a Proactive Agent Blend scenario.



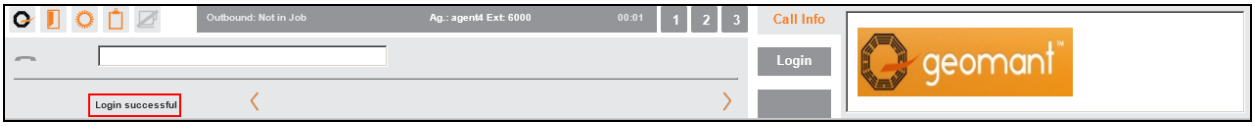
Click on the **Dialler Login** tab and enter the Proactive Contact **AgentID** and **Password**. Enter the **Extension** number for the endpoint on which calls will be handled.



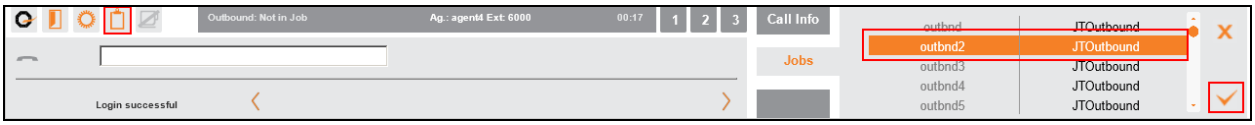
Click the **ACD Login** tab and enter the **AgentID** and **Password** configured on Communication Manager. The **Extension** number is auto-populated with what is entered on the **Dialler Login** tab. Click the orange tick when done.



If the login is successful, the **Login successful** message will appear in the info area.



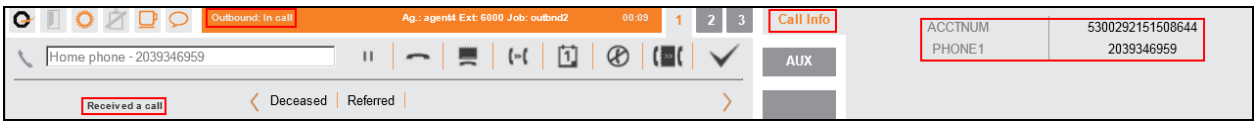
Click the **Join Job** icon and select the job to be joined on the right hand side of the screen, click the orange tick to join the job.



The acquire call will be placed to the agent extension, in this case 6000. Once answered the agent will be acquired for the outbound dialer job. The info area will update with a message to this affect. The status bar will show **On Break**. Click the **off break** button to begin handling outbound calls.

Outbound calls will be placed by the dialer. Once an outbound call is answered verify that the call is connected to the agent, the record information will appear in the **Call Info** area, the info area will update with **Received a call** and the status bar will update with **In call**.

Note: the information displayed in the **Call Info** area matches the fields configured in the Agent Screen in **Section 7.5.7**.



Place a call to the inbound VDN configured in **Section 5.2**. Once the outbound call has been completed, verify that the agent is moved to inbound mode and the inbound call can be answered using the Unified Agent web client.

9.2. Verify Avaya Aura® Communication Manager Trunks

Following on from the previous section, handle an outbound call using the Unified Agent web client, and enter the command **status trunk x** where **x** is the Outbound or Headset trunk shown in **Section 5.6**. Verify that the **Service State** of the trunk members are **in-service**. In the example below where an outbound call is connected to an agent, the **Service State** of the trunk member is **in-service/active.**

```
status trunk 8

                              TRUNK GROUP STATUS

Member    Port      Service State       Mtce Connected Ports
                                        Busy

0008/001  001V806   in-service/idle     no
0008/002  001V807   in-service/idle     no
0008/003  001V808   in-service/idle     no
0008/004  001V809   in-service/idle     no
0008/005  001V810   in-service/idle     no
0008/006  001V811   in-service/idle     no
0008/007  001V812   in-service/idle     no
0008/008  001V813   in-service/active   no    S00041    S00007
0008/009  001V814   in-service/idle     no
0008/010  001V815   in-service/idle     no
```

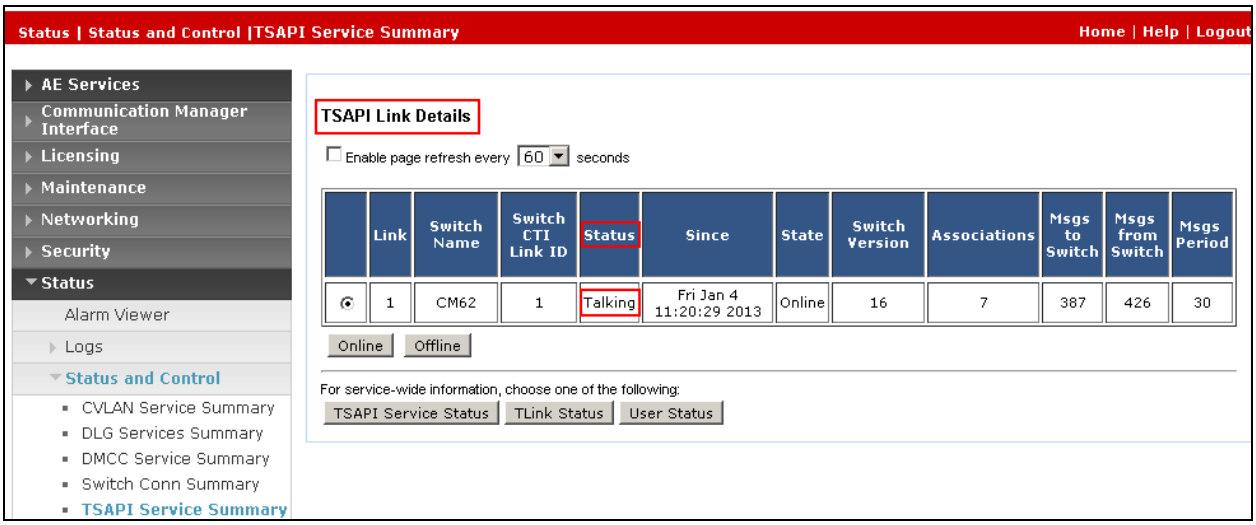
9.3. Verify Proactive Contact Job Status

From Proactive Contact shell, type the command **jobmon** to verify an agent is logged into the job outbnd2 and handling a call:

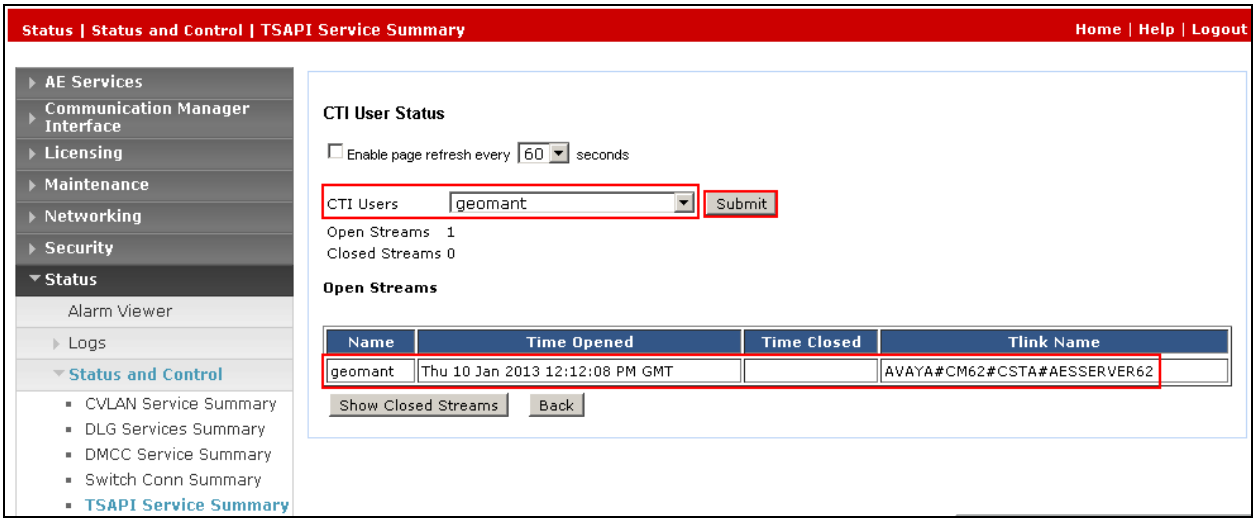
```
[STANDARD]                          Job Activity
[ALLID]
                                Summary Statistics
                  Job: [outbnd2][1478]
                  Start time: 07.45.02  Current time: 14.58.49
  Agent Activity                        Line Usage
  ----------------------------------  ----------------------------------------
              All Outb    ACD      PTP  Outbound Lines          Cur  Avg  Peak
  Logged in:    1    1      0        0   Demand       :           1    0     1
  Assigned :    1    1                   Available    :           9
  On Phone :    1    1                   Total Lines  :          10


  Calling Activities
  ------------------------------------------------------------------------------
  Outbound Phone Calls
    Records Selected:        419
    Phone Calls made:          6
    Cur/Run Hit Rate:         65/66 %
    Agent Connects  :          3
    Queue           :          0
    Recalls         :          0
    Phone Calls Left:        305
```

9.4. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify the **Status** is **Talking** for the TSAPI link administered in **Section 6.3**, as shown below.



Click on **User Status** and select the configured Geomant CTI user from the **CTI Users** drop down list and click **Submit**. Verify an Open Stream is displayed against the Geomant CTI user with the Tlink name configured in **Section 8.1**.



10. Conclusion

These Application Notes describe the configuration steps required for Geomant Unified Agent to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Proactive Contact with Avaya PG230 Digital Switch. All feature test cases were completed successfully with observations note in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Proactive Contact*, Release 5.0, April 2012, available at http://support.avaya.com.
2. *Geomant Unified Agent Implementation Guide*, Version 1.4.0, November 2012

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.