Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Application Enablement Services and Avaya Proactive Contact R5.0 to interoperate with Geomant Desktop Connect – Issue 1.0

Abstract

These Application Notes describe the steps to configure Geomant Desktop Connect to operate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Proactive Contact. The Geomant Desktop Connect solution uses call details presented to a Proactive Contact Agent to integrate with third party applications.

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 Desktop Connect to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services (AES) and Avaya Proactive Contact. Geomant Desktop Connect is used to automate Agent activity based on set criteria defined in up to 999 rules. In the inbound call scenario data presented to the agent by TSAPI is captured by Geomant Desktop Connect using TSAPI. During the outbound call scenario data presented to the Proactive Contact Agent Application is captured by Geomant Desktop Connect using DDE. In the event that the captured data matches one of the rules defined in Geomant Desktop connect, a given action is executed e.g. send keys, launch executable, button presentation, enter URL, toggle between applications, execute another rule. Using the data captured to automate processes is proven to increase productivity in a contact centre environment and increase agent efficiency.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the Desktop Connect to correctly capture the data presented by both inbound ACD calls and outbound Proactive Contact calls.

2.1. Interoperability Compliance Testing

The following tests were performed as part of the compliance testing.

- Outgoing/incoming PSTN call
- DNIS presentation
- ANI presentation
- Call identifier presentation
- Universal call ID presentation
- Redirect presentation
- UUI presentation
- Digit collect presentation
- Proactive Contact Agent field data
- Rule execution
- Button action verification
- Power and network interruption to Geomant server/client, AES and Communication Manager

2.2. Test Results

All functionality and serviceability test cases were completed successfully with the following observation:

- It was not possible to use the PopupAction to display Last Redirect ID information (<LASTREDID>). Though it is possible to provide this through the InfoMessage.

2.3. Support

Technical Support can be obtained for the Geomant products as follows:

- Email: product_dc@support.geomant.com
- Phone: +44 1789 766178

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8800 server running Communication Manager with an Avaya G650 Media Gateway. An Avaya S8800 server hosts Application Enablement Services. Proactive Contact 5 is hosted on an HP Proliant DL385G2 configured to operate with the Avaya PG230 Digital Switch. An Avaya 2420 Digital Hardphone was used by the Agent during the compliance test. The Tomcat application server on which the Geomant Desktop connect configuration is made, was hosted on a Microsoft Windows XP PC along with the Geomant Desktop Connect client, Avaya TSAPI client and Avaya Proactive Contact Agent.

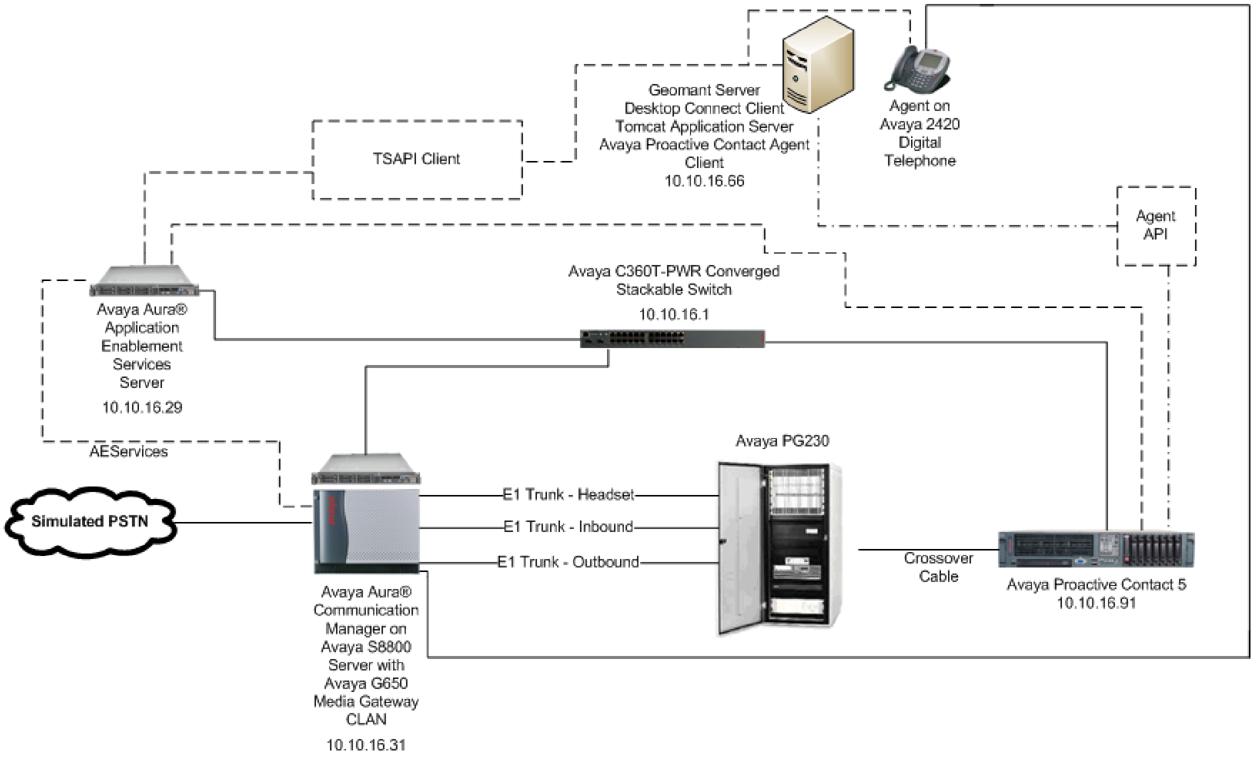


Figure 1: Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Proactive Contact with PG230 and Geomant Desktop Connect Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Media Server	Avaya Aura® Communication Manager R6.0.1 SP4 R16.00.1.510.1-19100
Avaya G650 Media Gateway • TN799DP	 HW 08 FW 040
Avaya S8800 Media Server	Avaya Aura® Application Enablement Services R6.1.1 r6-1-1-30-0
Avaya S8730/HP Proliant DL385G2 Server	Avaya Proactive Contact 5.0 patch 269
Avaya PG230 Digital Switch	Generic Version 15.3.1
Avaya 2420 Digital Telephone	REL 4.00 HWV 1 FWV 4
Generic VMWare Server	VMWare ESXi 4.1 Windows XP SP3 Tomcat 5.5 Geomant Desktop Connect 5.1.6.0 Avaya Proactive Contact Agent 5.0.1 Avaya TSAPI Client 6.1.1

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. The application notes assume trunk connectivity and call routing between Communication Manager and the PG230 digital switch is established, and the relevant licensing and dialplan is administered.

- Define Feature Access Codes
- Administer ACD
- Configure CLAN for Avaya AES Connectivity
- Configure Transport Link for AES Connectivity
- Configure CTI Link for TSAPI Service

5.1. 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
```

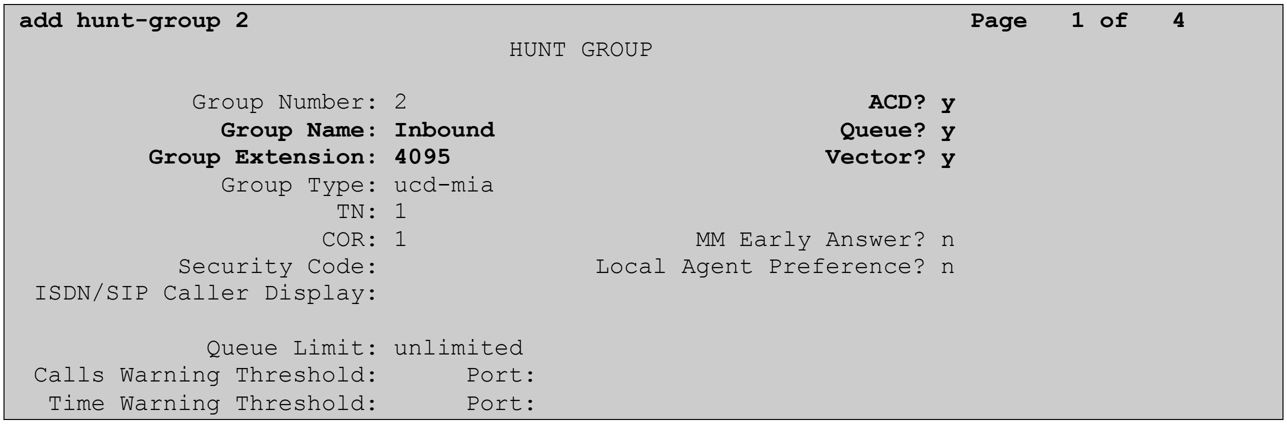
5.2. Administer ACD

In order for ACD calls to be routed to agents, a Hunt Group (skill), Vector and Vector Directory Number (VDN) must be configured. The compliance test covered digit collection, UUI and redirect verification.

5.2.1. Administer Hunt Group

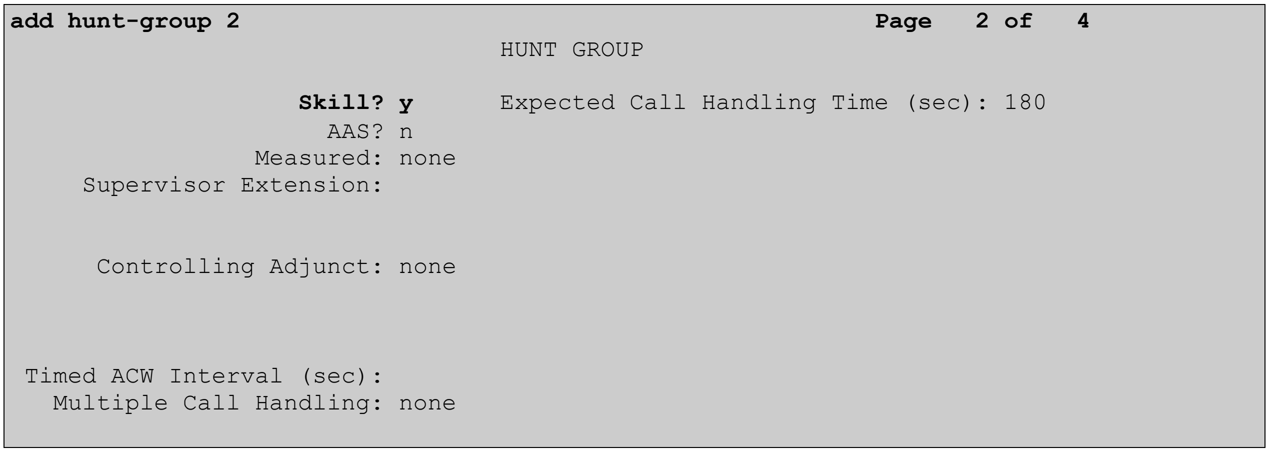
Enter the **add hunt-group n** command where **n** is an available hunt group number. On **Page 1** of the **hunt group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to **y** as shown below.

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



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

            Group Number: 2                               ACD? y
              Group Name: Inbound                       Queue? y
         Group Extension: 4095                         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:
```

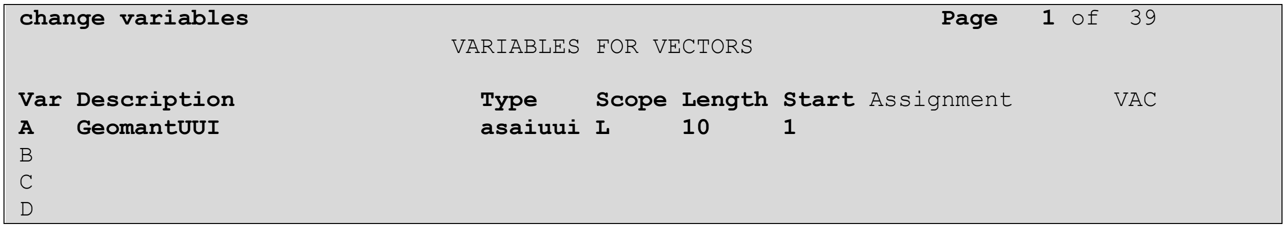
On **Page 2**, set the **Skill** field to **y** as shown below.



```
add hunt-group 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
```

5.2.2. Administer UUI

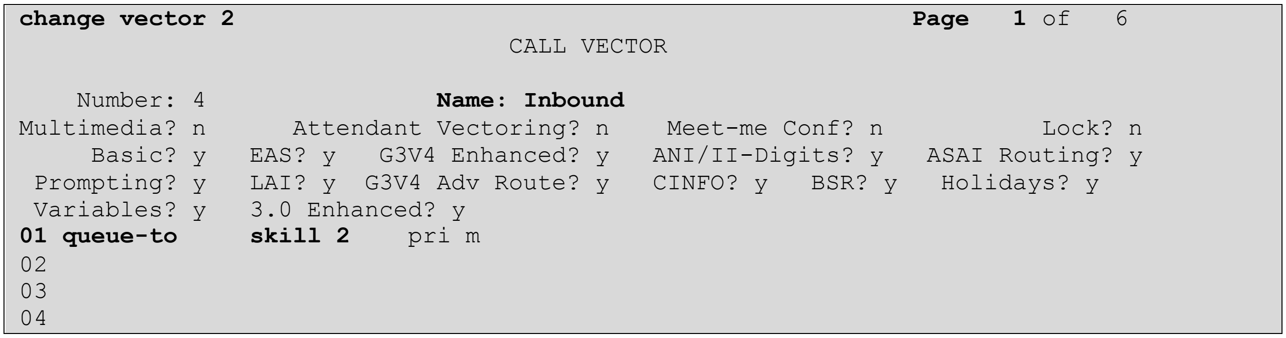
Desktop Connect can use UUI data to run a defined rule. UUI data is presented to the agent via the Vector configured in the **Section 5.2.3**. Enter the command **change variables**, in the first available variable row, in this case **A**, enter a **Description** for the variable, set the **Type** to **asaiuui**, set the **Scope** to **L,** set the variable **Length** accordingly and set the **Start** to **1**.



```
change variables                                            Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                 Type    Scope Length Start Assignment       VAC
A   GeomantUUI                  asaiuui L     10     1
B
C
D
```

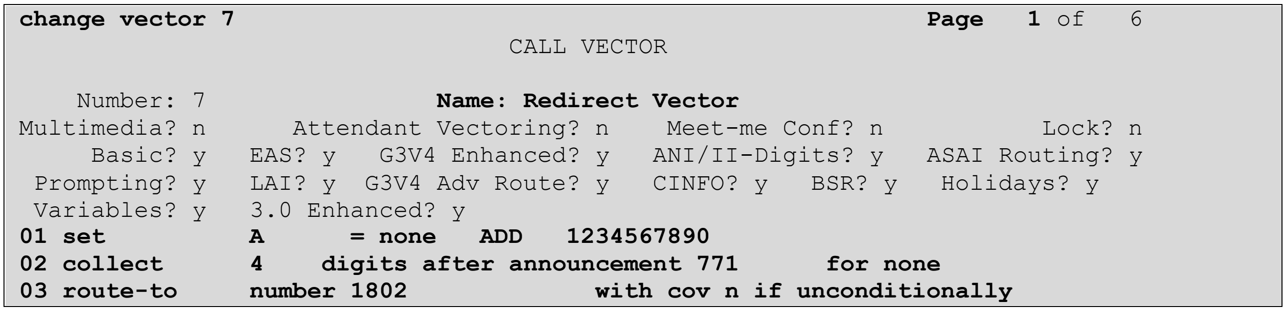
5.2.3. Administer Vector

In order to verify correct redirect VDN information on Destktop Connect, two Vectors must be created. This Section assumes a recording was previously recorded usingannouncement extension number **771**. Enter the **change vector n** command, where **n** is the vector number. Assign a **Name** and enter the vector step to queue to **skill 2** as shown below, leave all other settings default. Skill 2 relates to the skill enabled hunt group configured previously.



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

    Number: 4                 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
03
04
```

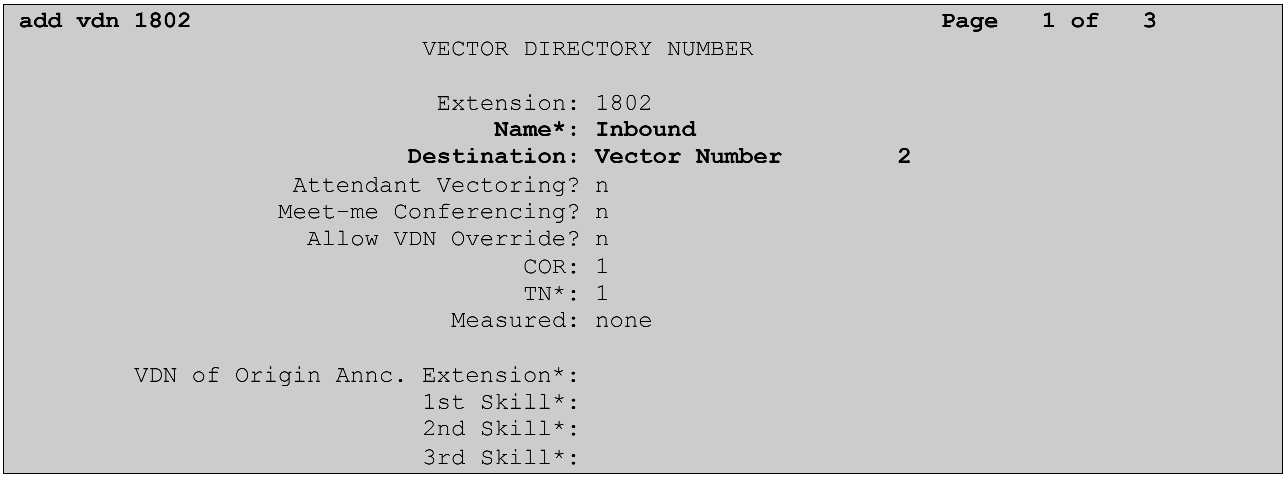
Using the same method, create an additional redirect vector to include digit collection and UUI information. Enter the command **change vector n**, where n is the vector number. Configure step **01** to set variable **A** to **none** and **ADD 1234567890**, configure step **02** to **collect 4 digits after announcement 771**, these digits, entered by an inbound caller, will be presented to the agent using Desktop Connect. Configure step **03** to route to the VDN to configured in **Section 5.2.4**.



```
change vector 7                                            Page   1 of   6
                                  CALL VECTOR

    Number: 7                 Name: Redirect Vector
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 set          A      = none   ADD   1234567890
02 collect      4    digits after announcement 771      for none
03 route-to     number 1802             with cov n if unconditionally
```

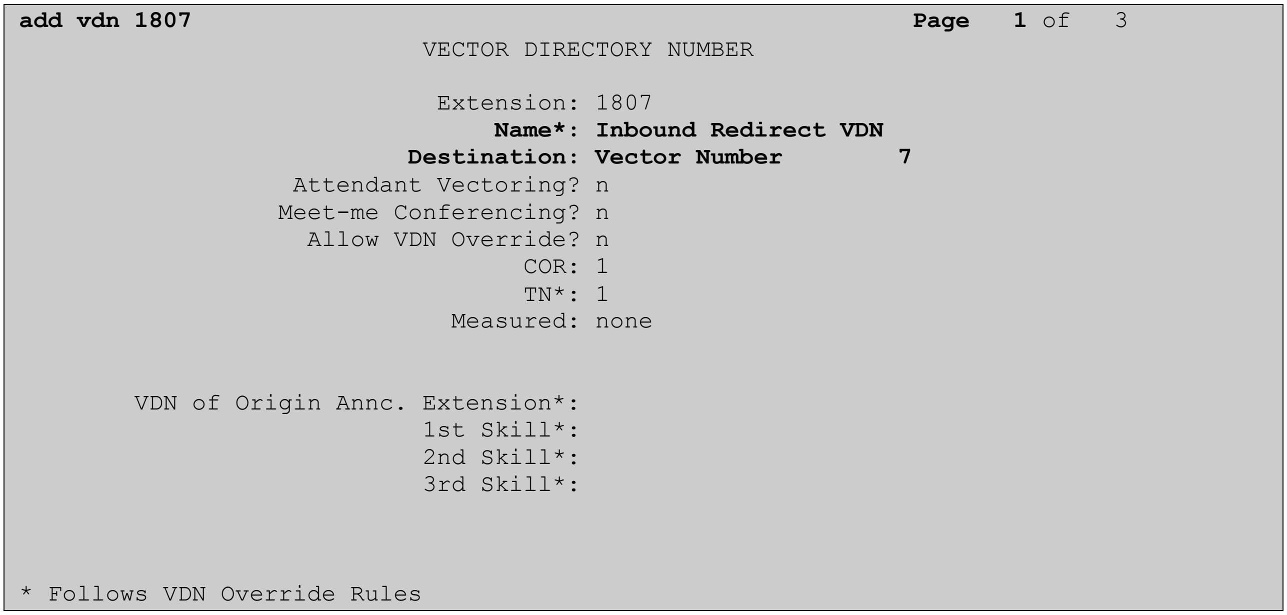
5.2.4. Administer Vector Directory Number (VDN)

Vector 2 and 7 are accessed by calling a Vector Directory Number, 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. The VDN below simply routes calls to **1802** to vector **2**, which in turn, queues callers to skill 2.



```
add vdn 1802                                                    Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 1802
                                 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*:
```

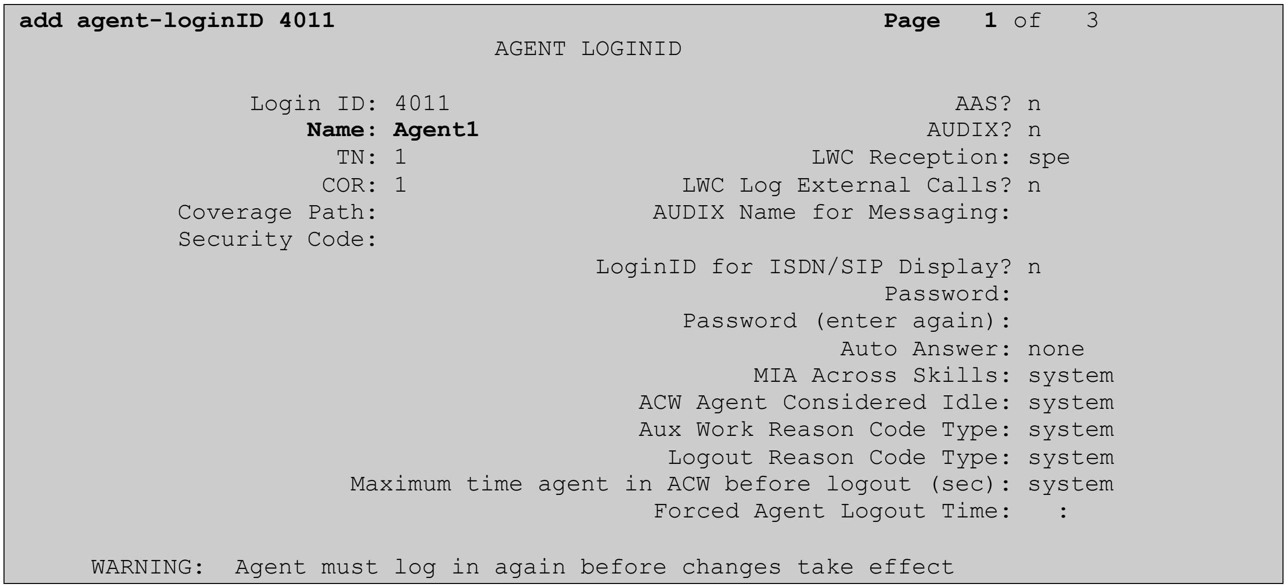
Perform the same to route callers to vector 7. Inbound callers to **1807** will route to vector **7**, this will enter UUI information, collect 4 user entered digits after an announcement, and route the caller to vdn 1802. In order to provide collected digits to Desktop Connect, an intermediate, or redirect vector MUST be used.



```
add vdn 1807                                                  Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 1807
                                 Name*: Inbound Redirect VDN
                           Destination: Vector Number        7
                   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*:



* Follows VDN Override Rules
```

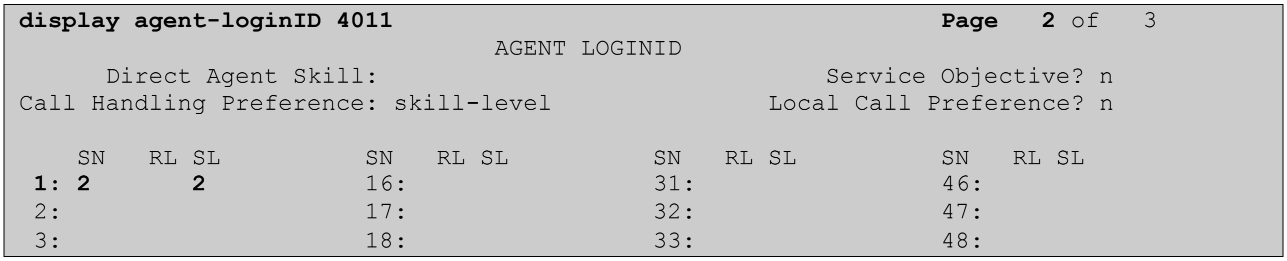
5.2.5. Administer Agent Logins

Skilled Agents must be configured on Communication Manager, 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.



```
add agent-loginID 4011                                      Page   1 of   3
                                 AGENT LOGINID

                Login ID: 4011                                    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: none
                                                   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,** assign a skill to the agent by entering the relevant hunt group number created in **Section 5.2.1** for **SN** and entering a skill level of **2** for **SL**.



```
display agent-loginID 4011                                      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: 2       2            16:                  31:                  46:
 2:                      17:                  32:                  47:
 3:                      18:                  33:                  48:
```

Repeat this task accordingly for any additional inbound agents required.

5.2.6. Configure Agent Stations

It is assumed that stations are configured on Communication Manager, perform the following additional configuration 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.

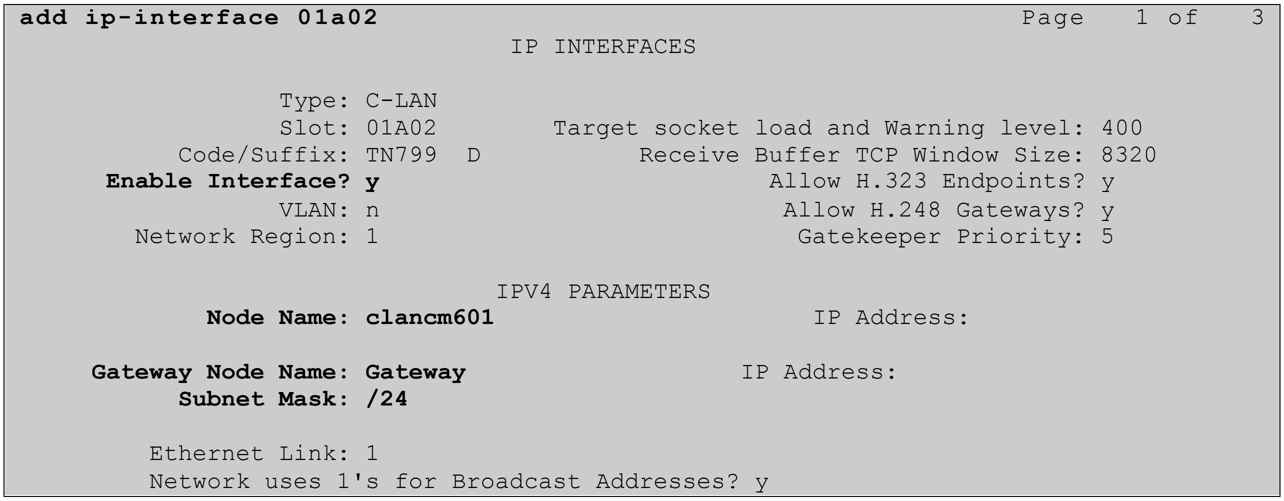
```
change station 4000                                            Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                                Headset? n
       Jack:                                                Speaker? n
      Cable:                                               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::
```

5.3. Configure CLAN for Avaya Aura® Application Enablement Services Connectivity

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

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
devconaes611        10.10.16.29
clancm601           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 Node Name** 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**, 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: clancm601                     IP Address:

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

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

5.4. 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 5.3**
- **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       clancm601          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 **devconaes611**
- **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 or hostname 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:      devconaes611            Avayapassword1        y        in use
      2:      :
```

5.5. 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.

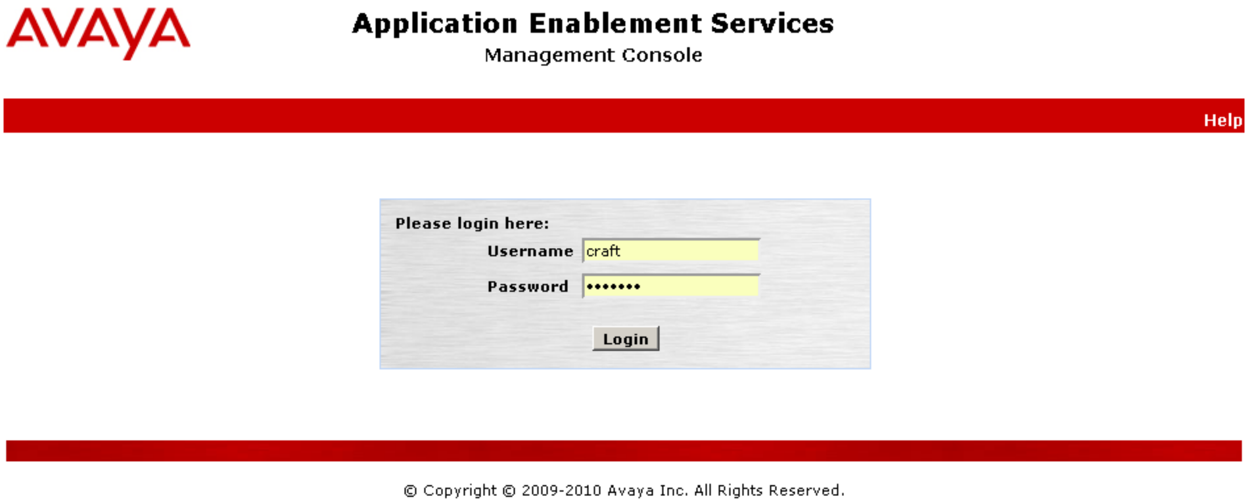
```
add cti-link 1                                                   Page   1 of   3
                                   CTI LINK
 CTI Link: 1
Extension: 4999
     Type: ADJ-IP
                                                                      COR: 1
     Name: devconaes
```

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:

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

All administration in this section is performed from the AES Management Console. Navigate to https://AES_IP_ADDRESS/ in this case http://10.10.16.29 and log in with the relevant credentials.

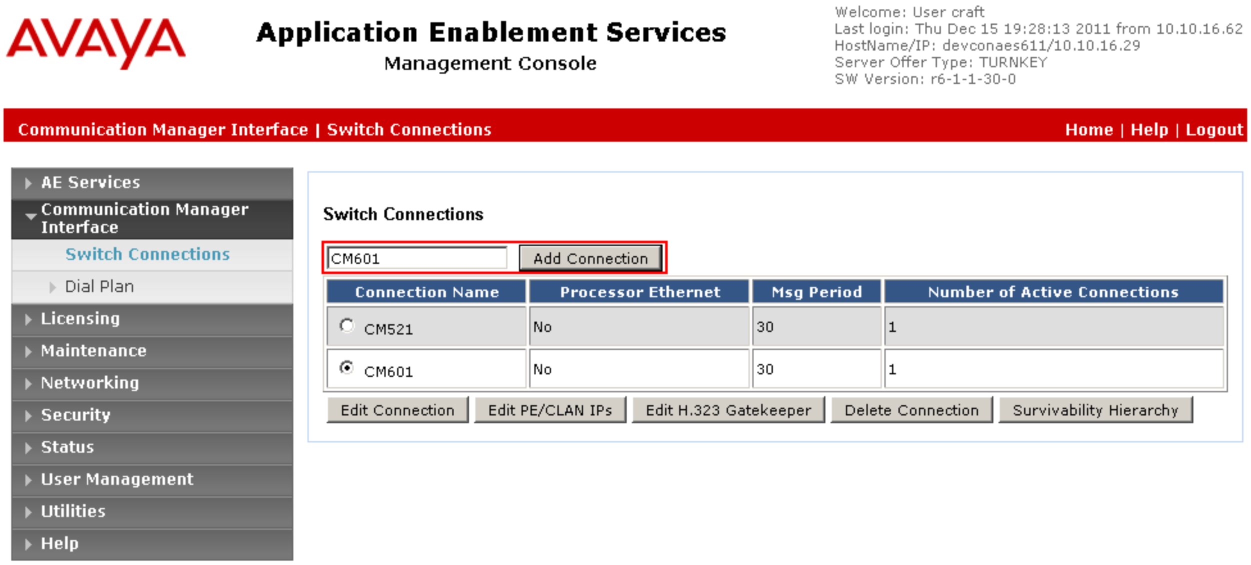

AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Login
© Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

Username: craft

Password: •••••••

6.1. 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.



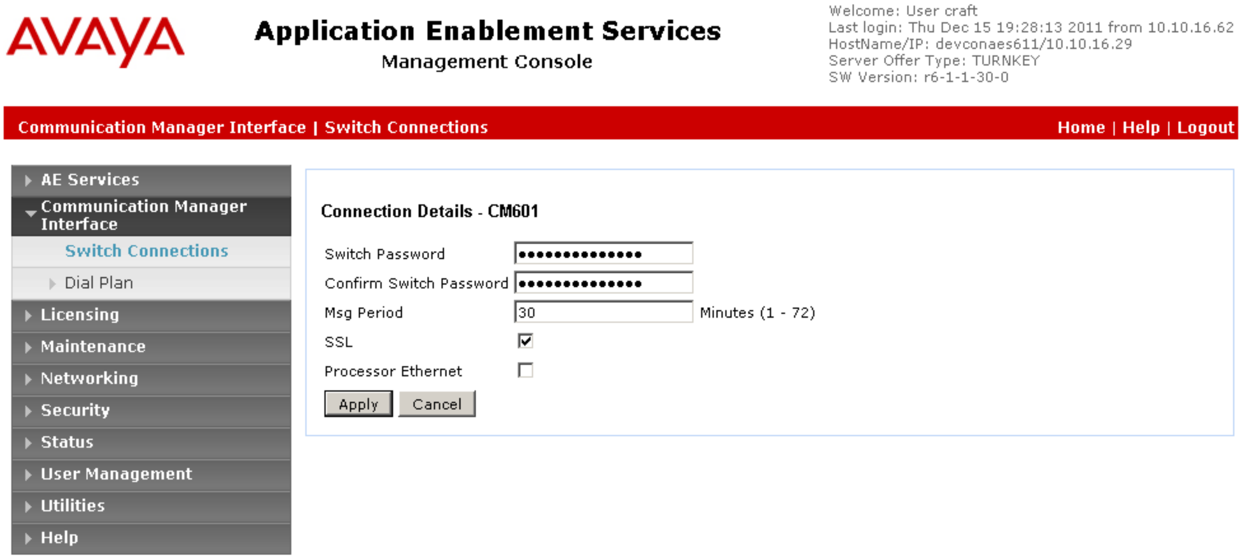
Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

Switch Connections

CM601

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ CM521	No	30	1
● CM601	No	30	1

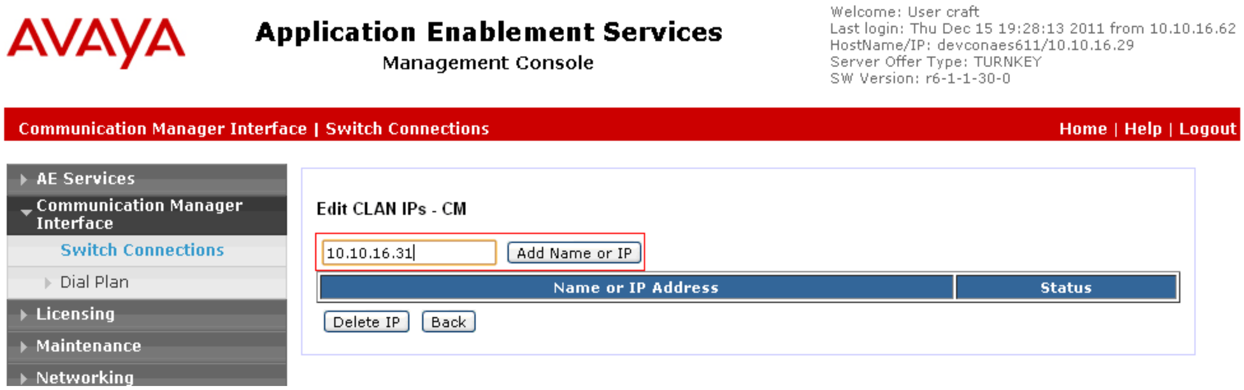
In the resulting screen enter the **Switch Password,** the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.4**. Default values may be accepted for the remaining fields. Click **Apply** to save changes. Select Apply.


AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help
Apply
Cancel

Connection Details - CM601

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

From the **Switch Connections** screen in the above screenshot, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button. 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.



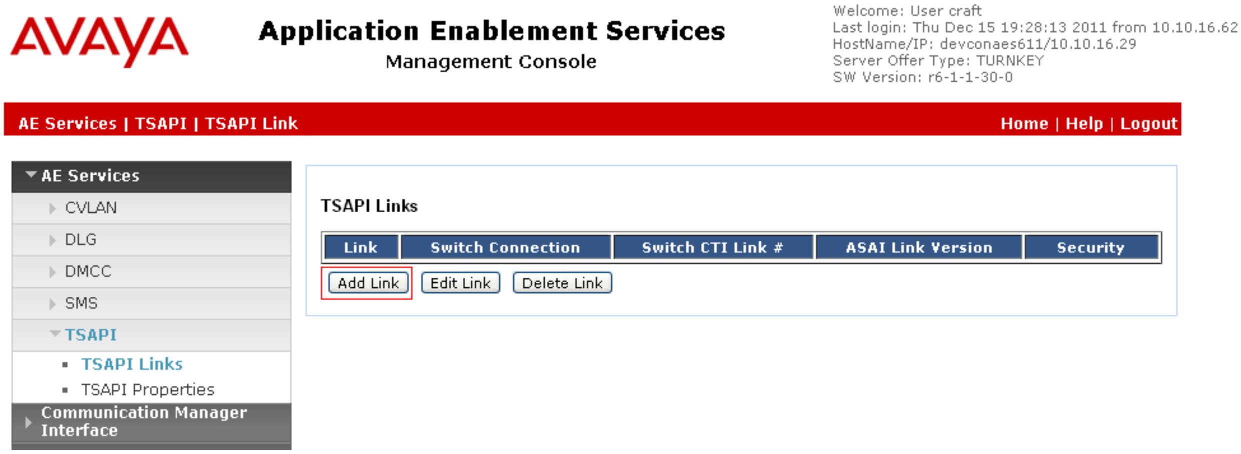
Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

Edit CLAN IPs - CM

10.10.16.31

6.2. 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 Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

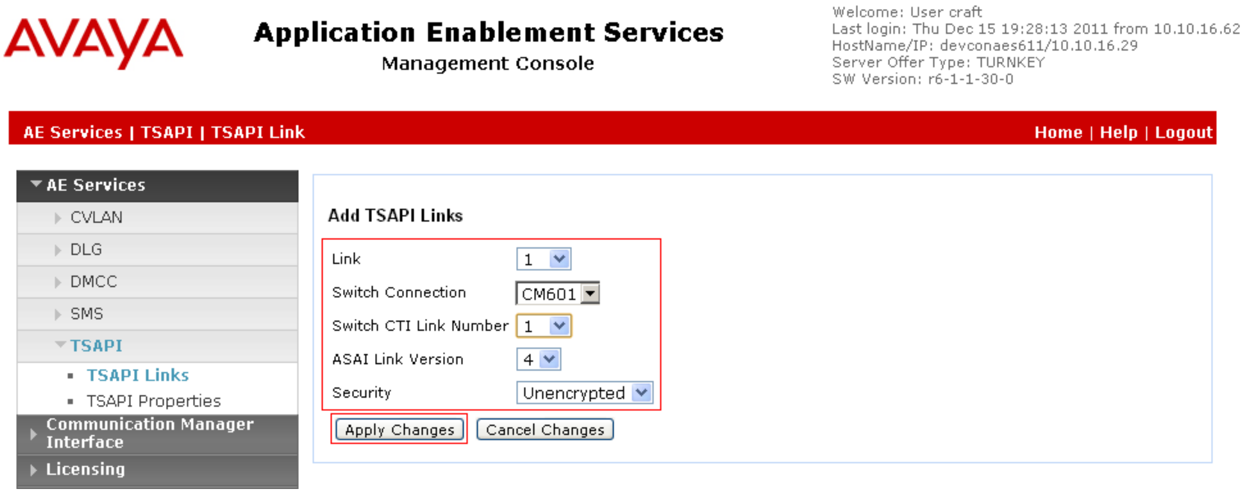
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM**, which has already been configured in **Section 6.1** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.5** 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**.

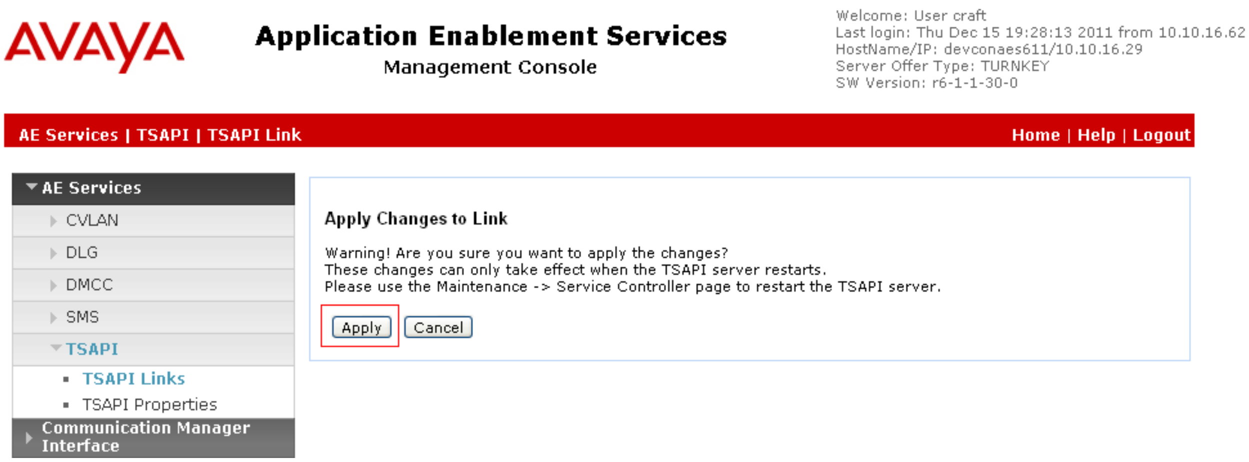


Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

Add TSAPI Links

Link	1
Switch Connection	CM601
Switch CTI Link Number	1
ASAI Link Version	4
Security	Unencrypted

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

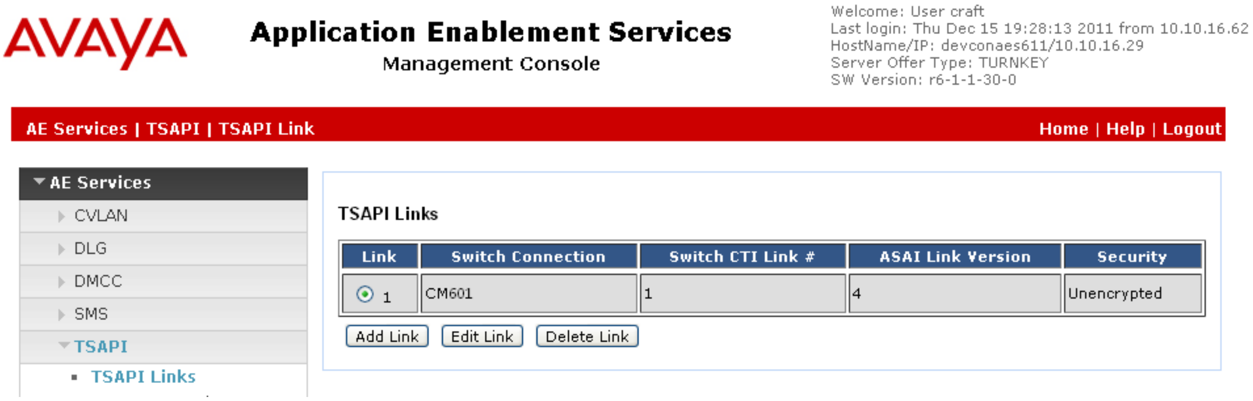


Application Enablement Services
Management Console
Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0
AE Services | TSAPI | TSAPI Link
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
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.

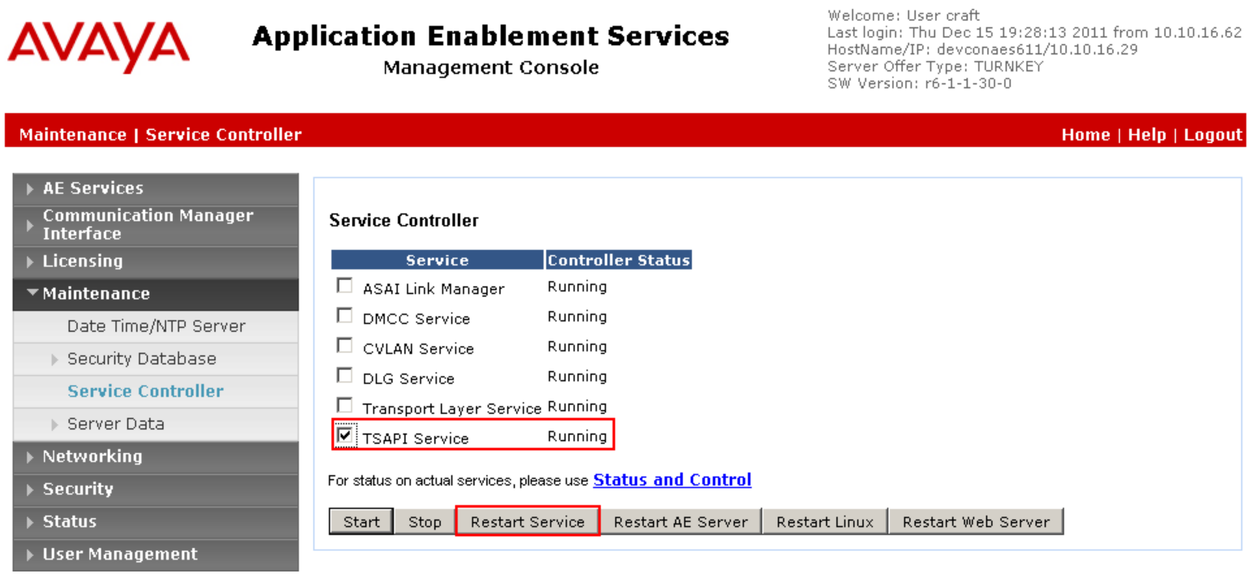


Application Enablement Services
Management Console
Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0
AE Services | TSAPI | TSAPI Link
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
Add Link
Edit Link
Delete Link

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
◉ 1	CM601	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, check the **TSAPI Service** and select **Restart Service**.



Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

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

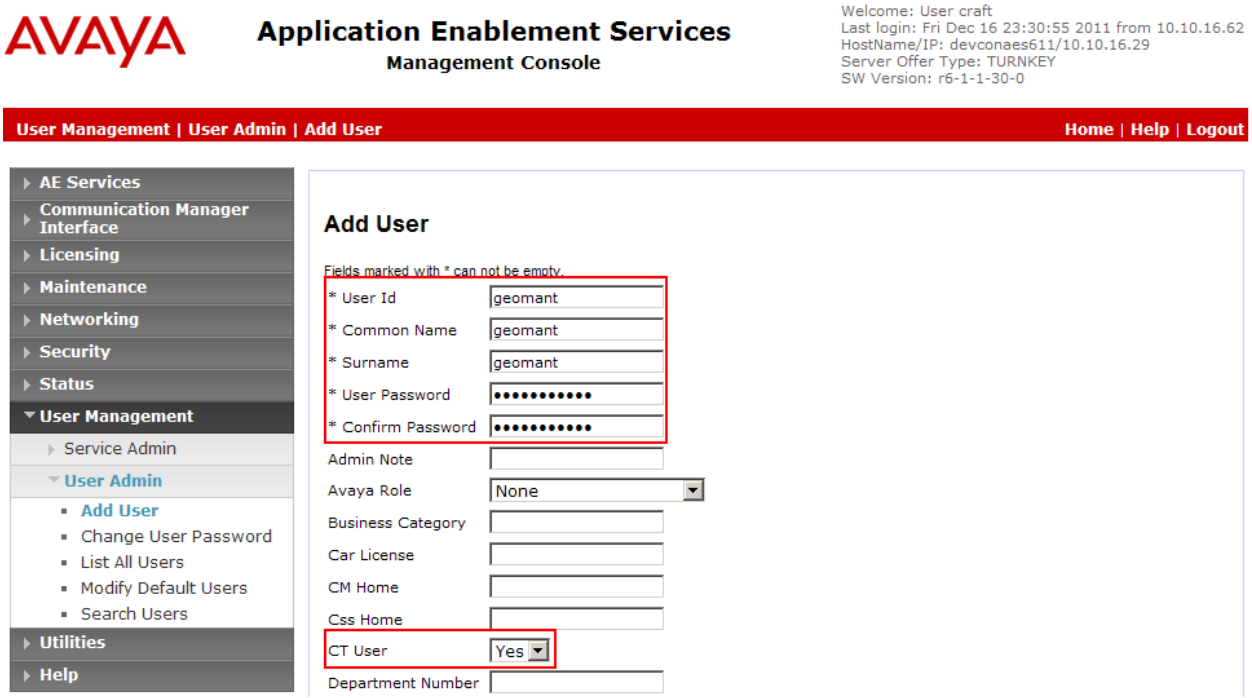
For status on actual services, please use Status and Control

6.3. Create Avaya CTI User

User ID and password needs to be configured for the Desktop Connect 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 Desktop Connect in **Section 8.1.**
- **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 8.1**.
- **CT User -** Select **Yes** from the drop-down menu.

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



Welcome: User craft
Last login: Fri Dec 16 23:30:55 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

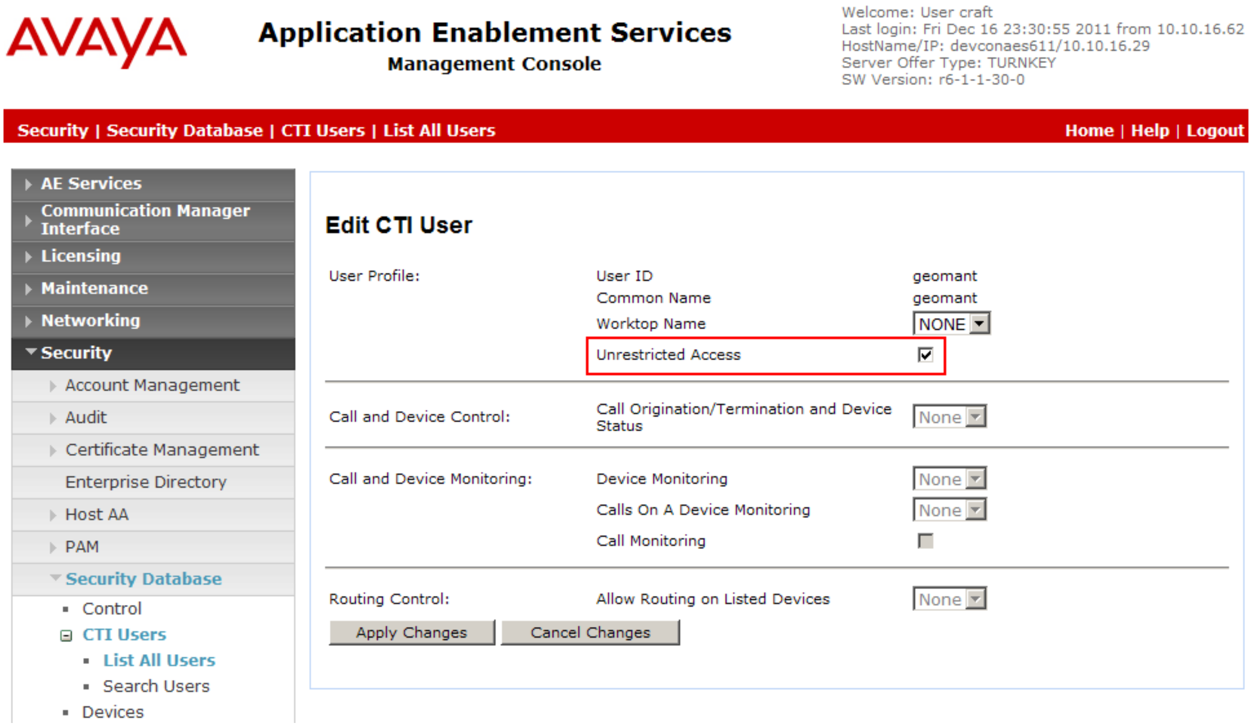
Add User

Fields marked with * can not be empty.

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

6.4. 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 6.3** and select the **Edit** option (not shown). The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and click **Apply Changes** at the bottom of the screen.



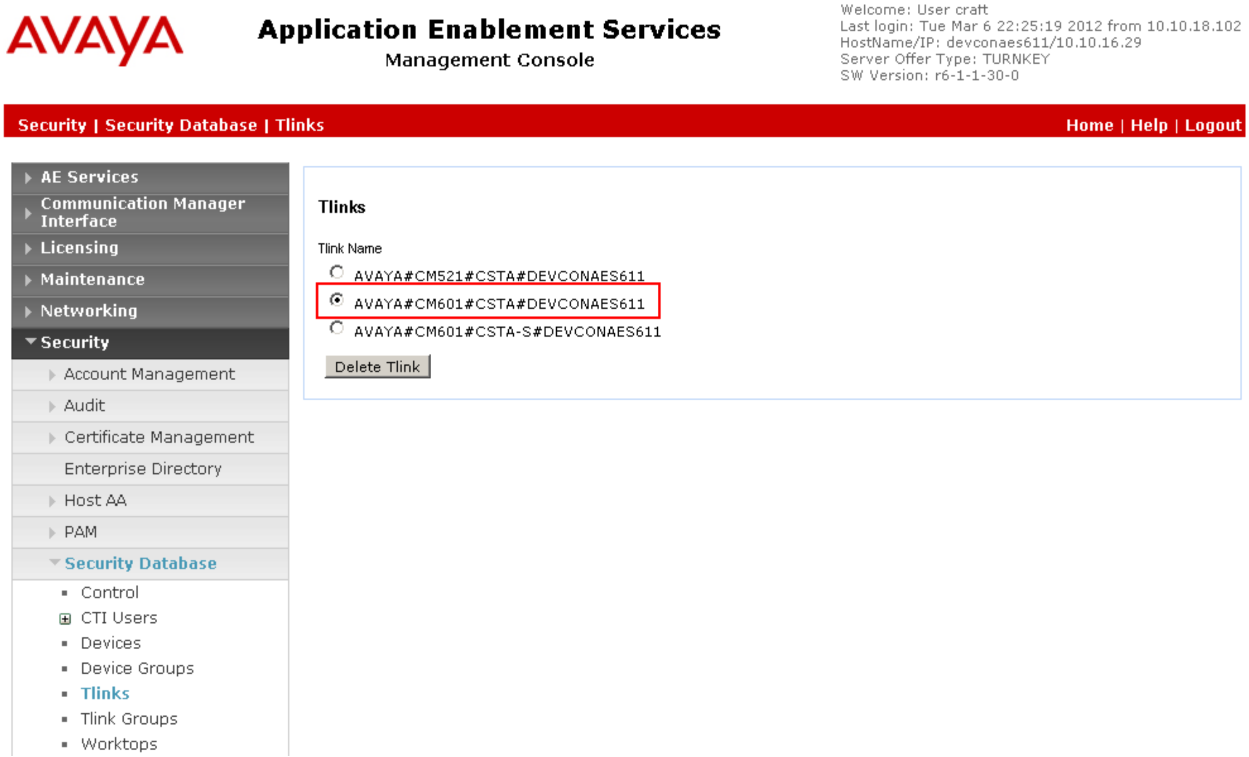
Edit CTI User

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

A screen (not shown) appears to confirm applied changes to CTI User, click **Apply**.

6.5. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Desktop Connect in **Section 8.1**.



Tlinks

Tlink Name

○ AVAYA#CM521#CSTA#DEVCONAES611
● AVAYA#CM601#CSTA#DEVCONAES611
○ AVAYA#CM601#CSTA-S#DEVCONAES611

7. Configure Avaya Proactive Contact and Avaya PG230

The application notes assume Proactive Contact is configured with a job, calling list, and record selection to place outbound calls using the PG230 over ISDN to Communication Manager and on to the PSTN. For the purposes of the compliance test, the **ZIPCODE** field of the calling list was used to activate a Desktop Connect rule. It is assumed Proactive Contact Agent software is installed on the client PC and operational, no special configuration of Proactive Contact Agent is required.

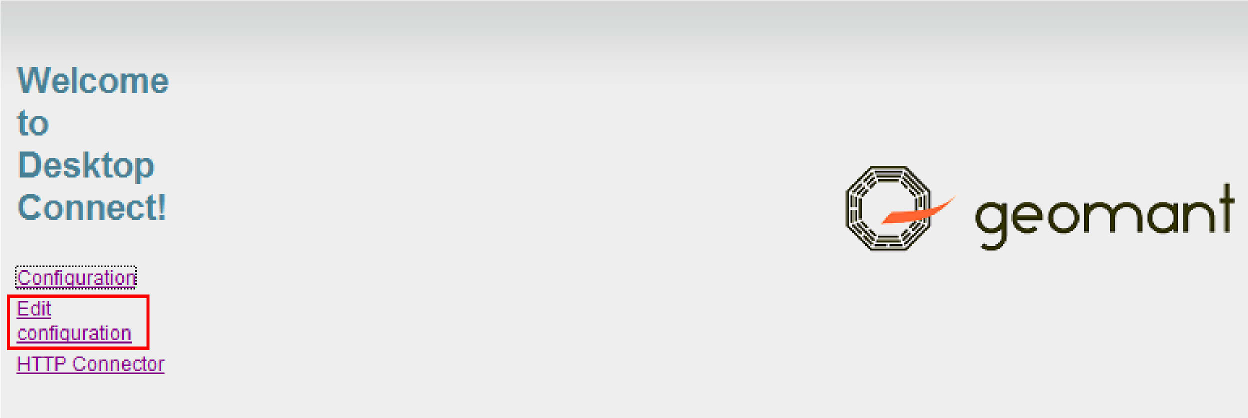
8. Configure Geomant Desktop Connect

For the purposes of the compliance test, the installation and components of Desktop Connect were provided and supported by Geomant. Geomant provided a basic Microsoft Access based CRM database to verify the send key and application popup integration to a third party. Configuration of Desktop Connect is performed via the Tomcat Application server web interface and can be summarized as follows:

- Configure TSAPI Parameters
- Configure ACD Parameters
- Configure Rules

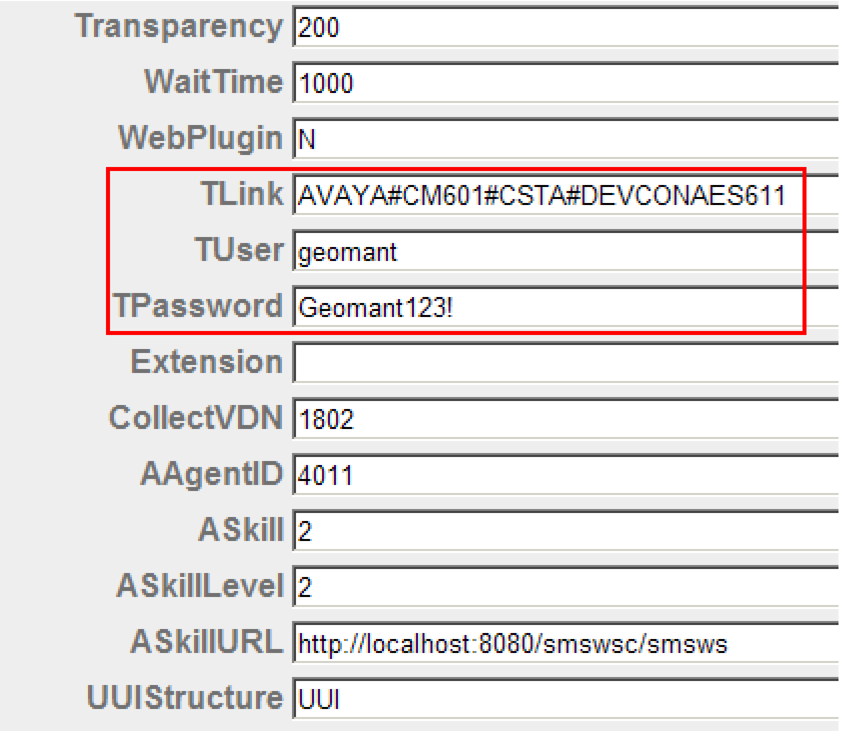
8.1. Configure TSAPI Parameters

Configuration of Desktop Connect is performed via the Tomcat Application server web interface. Browse to http://<ip_of_tomcat_server>:8080/GeoPDI in this case http://10.10.16.66:8080/GeoPDI and click on **Edit configuration**.



Welcome to Desktop Connect!

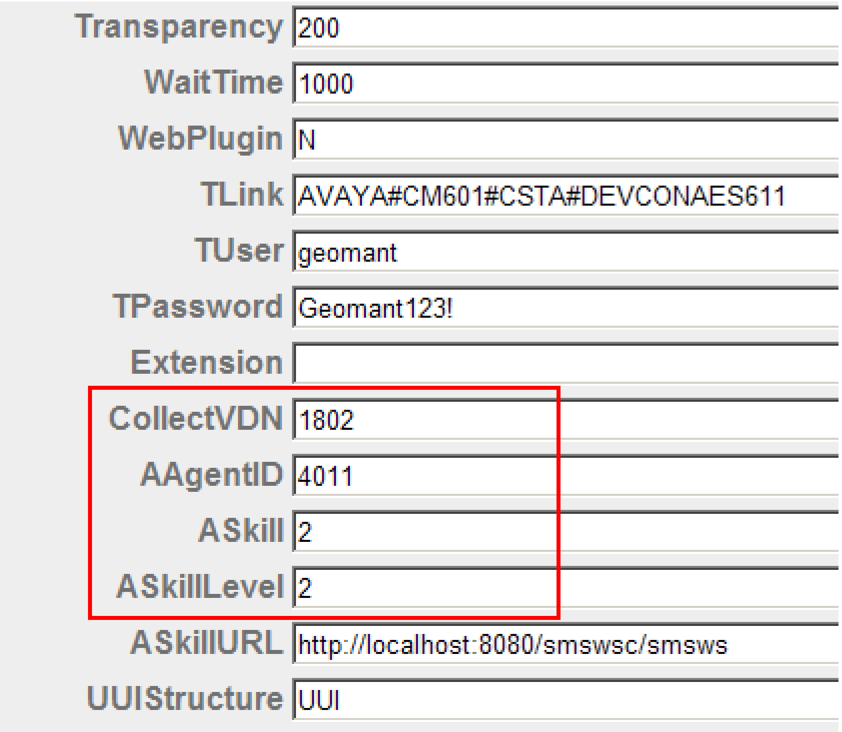
The Desktop Connect Global Configuration is displayed, in the GeoPDI section, enter the **TLink, TUser** and **TPassword** information configured in **Section 6.2, 6.3** and **6.5.**



Transparency	200
WaitTime	1000
WebPlugin	N
TLink	AVAYA#CM601#CSTA#DEVCONAES611
TUser	geomant
TPassword	Geomant123!
Extension	
CollectVDN	1802
AAgentID	4011
ASkill	2
ASkillLevel	2
ASkillURL	http://localhost:8080/smswsc/smsws
UUIStructure	UUI

8.2. Configure ACD Parameters

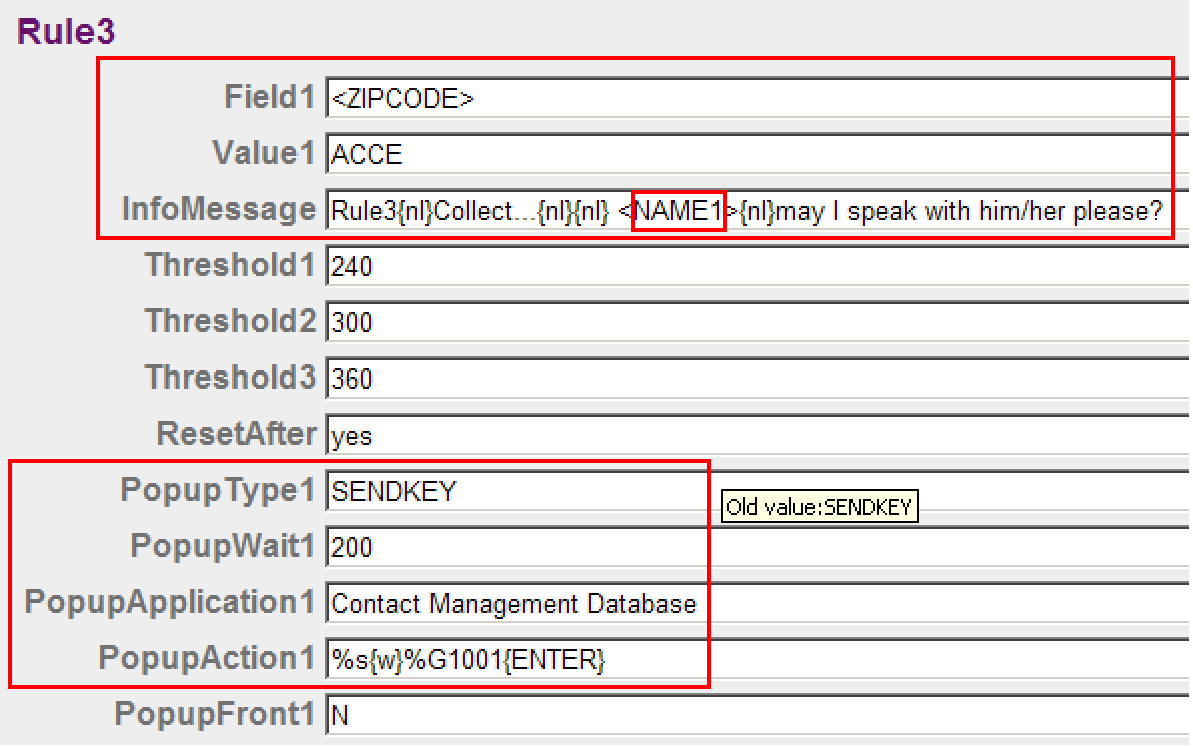
Desktop Connect uses TSAPI to monitor the inbound VDN. Skill and Agent Activity are monitored for the Proactive Contact acquire feature. Enter the **CollectVDN, AAgentID** (agent login ID)**, ASkill** (skill) and **ASkillLevel** configured in **Sections 5** and **6**. Note, the CollectVDN, is the VDN that queues to the skill i.e. 1802, **not** the VDN where the digits are actually collected, i.e. 1807.



Transparency	200
WaitTime	1000
WebPlugin	N
TLink	AVAYA#CM601#CSTA#DEVCONAES611
TUser	geomant
TPassword	Geomant123!
Extension	
CollectVDN	1802
AAgentID	4011
ASkill	2
ASkillLevel	2
ASkillURL	http://localhost:8080/smswsc/smsws
UUIStructure	UUI

8.3. Configure Rules

For the purpose of the compliance test **Rule 3, Rule 4** and **Rule 7** were created. In the relevant section of the Global Configuration enter the Rule parameters as shown below for **Rule 3**. In this example, if, when the Proactive Contact Agent is presented with an outbound call, the Proactive Contact Agent screen displays the **ZIPCODE** field populated with the **Value** of **ACCE**, this will match **Rule3** and trigger it to run. Upon activation of the Rule, the pre-defined **InfoMessage** is shown to the agent in Desktop Connect, complete with **NAME1** taken from the Proactive Contact Agent Screen. This uses DDE. Furthermore, the rule is configured to popup (**PopupApplication1)** the running application with a title of **Contact Management Database** and using the **SENDKEY** action defined in **PopupType1** send the **PopupAction1** of **%s{w}%G1001{ENTER}**. Details of the string syntax are available in Desktop Connect documentation. The effect of this particular Rule is to open a predefined record on the Contact Management Database with a record number of 1001. This is adaptable to any given scenario.

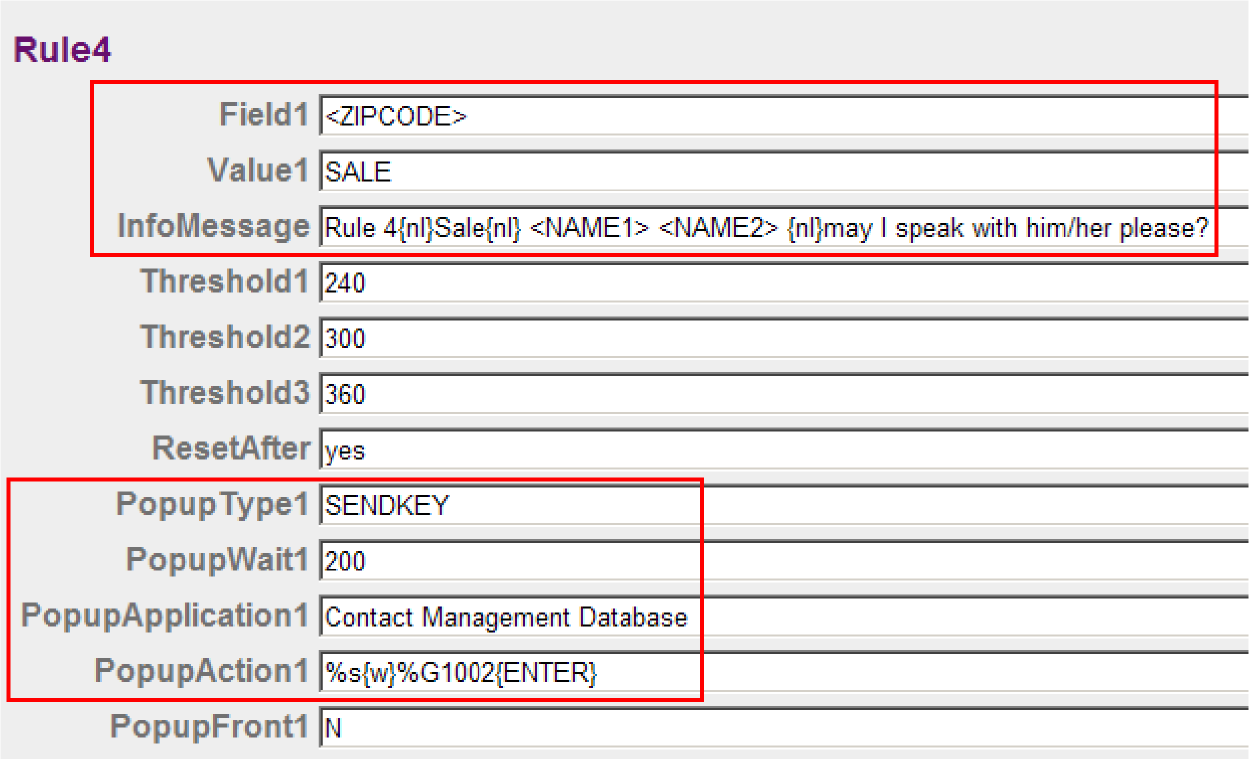


Rule3

Field1	<ZIPCODE>
Value1	ACCE
InfoMessage	Rule3{nl}Collect...{nl}{nl} <NAME1>{nl}may I speak with him/her please?
Threshold1	240
Threshold2	300
Threshold3	360
ResetAfter	yes
PopupType1	SENDKEY
PopupWait1	200
PopupApplication1	Contact Management Database
PopupAction1	%s{w}%G1001{ENTER}
PopupFront1	N

Old value:SENDKEY

Similar principles are applied in **Rule4.**

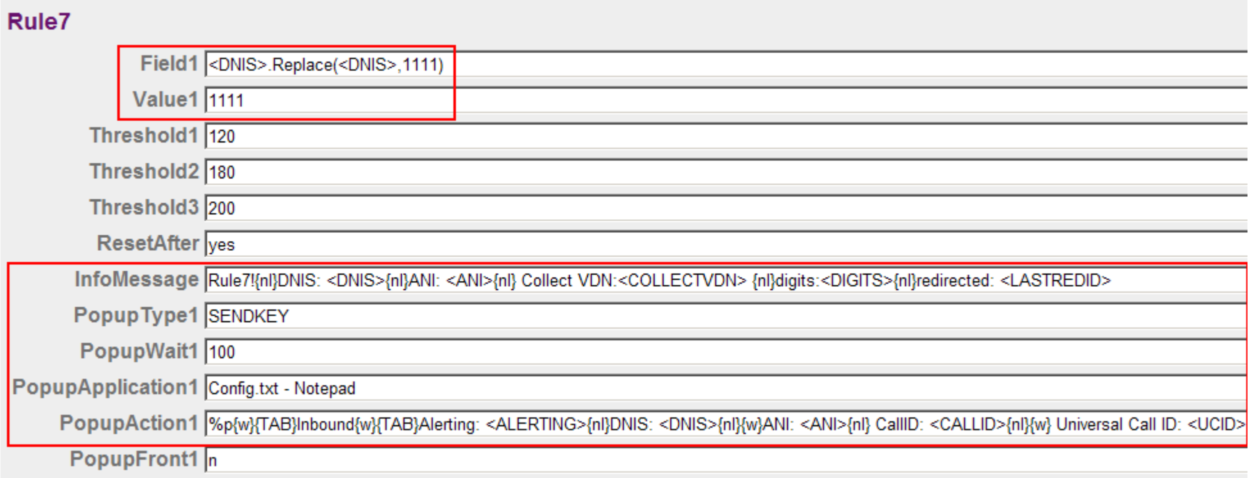


Rule4

Field1	<ZIPCODE>
Value1	SALE
InfoMessage	Rule 4{nl}Sale{nl} <NAME1> <NAME2> {nl}may I speak with him/her please?
Threshold1	240
Threshold2	300
Threshold3	360
ResetAfter	yes
PopupType1	SENDKEY
PopupWait1	200
PopupApplication1	Contact Management Database
PopupAction1	%s{w}%G1002{ENTER}
PopupFront1	N

Rule7 was configured as a “catch all” in the case where no other rules are matched. This is applicable to the inbound calls. **Field1** defines that the **DNIS** presented to Desktop Connect via TSAPI, is replaced with a string of **1111**, **Value1** defines that if the DNIS value is **1111** then the rule is matched, and the **InfoMessage** will be displayed, populated with information captured through the TSAPI monitor and using similar principles to Rule3, an application will popup and the defined keys sent. The full **PopupAction1** string was configured to include UUI, redirect and digit collection information:

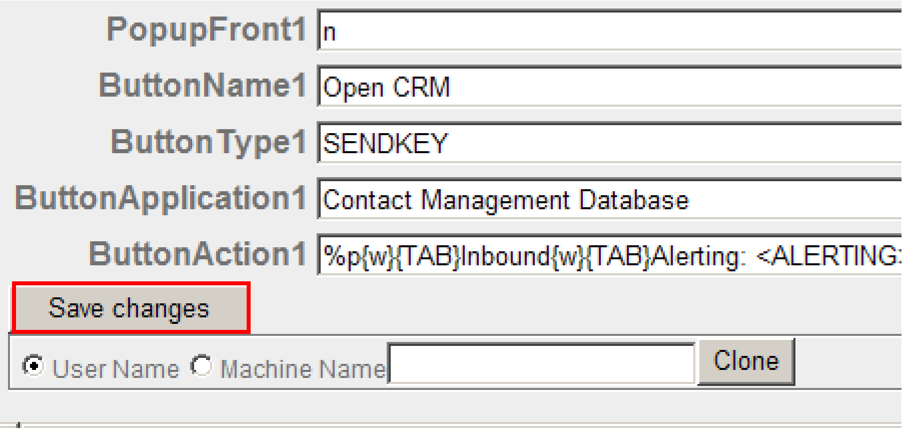
```
%p{w}{TAB}Inbound{w}{TAB}Alerting: <ALERTING>{nl}DNIS: <DNIS>{nl}{w}ANI: <ANI>{nl}
CallID: <CALLID>{nl}{w} Universal Call ID: <UCID>{nl}{nl}{w} User to user information:
<UUI>{nl}{w} Collect digit VDN: <COLLECTVDN>{nl}{w}Collected digits:
<DIGITS>{nl}{w}{w}{w} Last redirecting device: <LASTREDID>{ENTER}
```



Rule7

Field1	<DNIS>.Replace(<DNIS>,1111)
Value1	1111
Threshold1	120
Threshold2	180
Threshold3	200
ResetAfter	yes
InfoMessage	Rule7!{nl}DNIS: <DNIS>{nl}ANI: <ANI>{nl} Collect VDN:<COLLECTVDN> {nl}digits:<DIGITS>{nl}redirected: <LASTREDID>
PopupType1	SENDKEY
PopupWait1	100
PopupApplication1	Config.txt - Notepad
PopupAction1	%p{w}{TAB}Inbound{w}{TAB}Alerting: <ALERTING>{nl}DNIS: <DNIS>{nl}{w}ANI: <ANI>{nl} CallID: <CALLID>{nl}{w} Universal Call ID: <UCID>
PopupFront1	n

Click Select **Save Changes** at the bottom of the page when complete. Any changes to the configuration require a restart of the Desktop Connect Client.



PopupFront1: n

ButtonName1: Open CRM

ButtonType1: SENDKEY

ButtonApplication1: Contact Management Database

ButtonAction1: %p{w}{TAB}Inbound{w}{TAB}Alerting: <ALERTING:

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager CTI Link

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    devconaes611     established   87       61
```

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

```
status aesvcs interface

                          AE SERVICES INTERFACE STATUS

Local Node          Enabled?  Number of     Status
                              Connections

clancm601           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**.

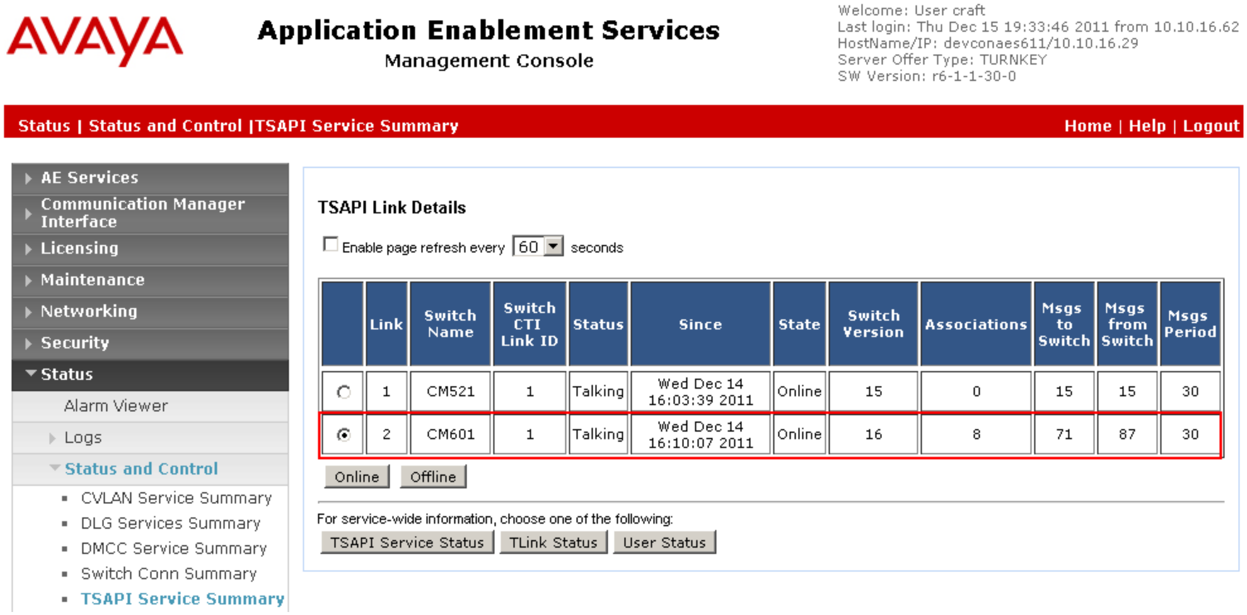
```
status aesvcs link

                                AE SERVICES LINK STATUS

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

01/01   devconaes611     10.10.16.29        45883    clancm601         683      665
```

9.2. Verify Avaya Aura® Application Enablement Services CTI Connection

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

9.2.1. 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: Thu Dec 15 19:33:46 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

TSAPI Link Details

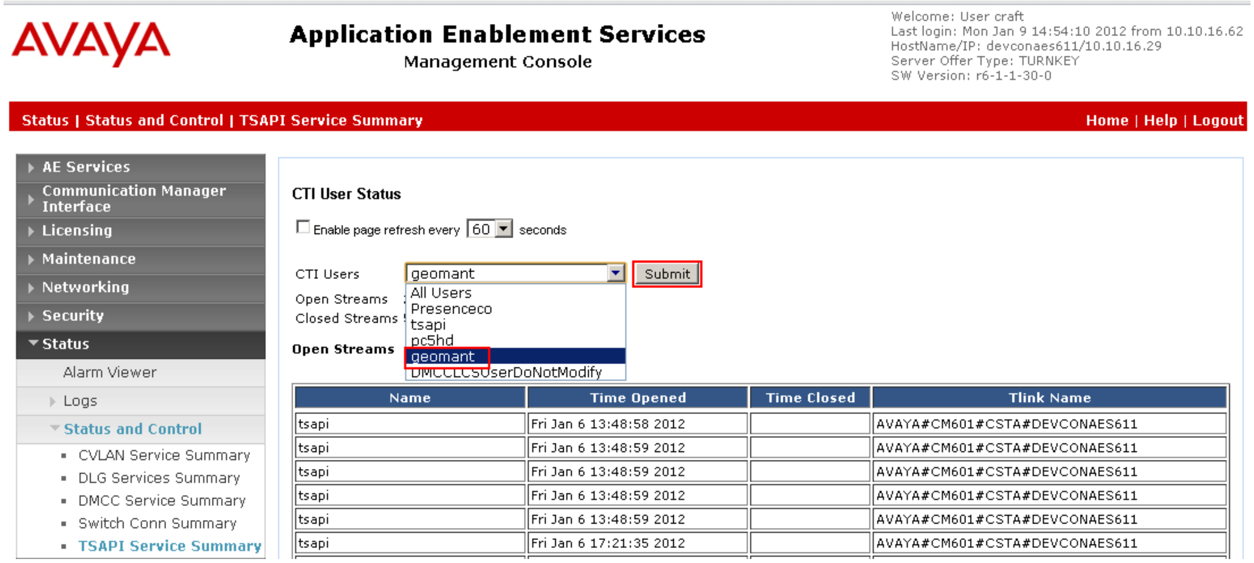
□ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
○	1	CM521	1	Talking	Wed Dec 14 16:03:39 2011	Online	15	0	15	15	30
●	2	CM601	1	Talking	Wed Dec 14 16:10:07 2011	Online	16	8	71	87	30

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

9.2.2. TSAPI User Status

On the Application Enablement Services Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary → CTI User Status** to display the **CTI User Status** page. Select the CTI user created in **Section 6.3** from the drop down list and click on **Submit.**



Welcome: User craft
Last login: Mon Jan 9 14:54:10 2012 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

CTI User Status

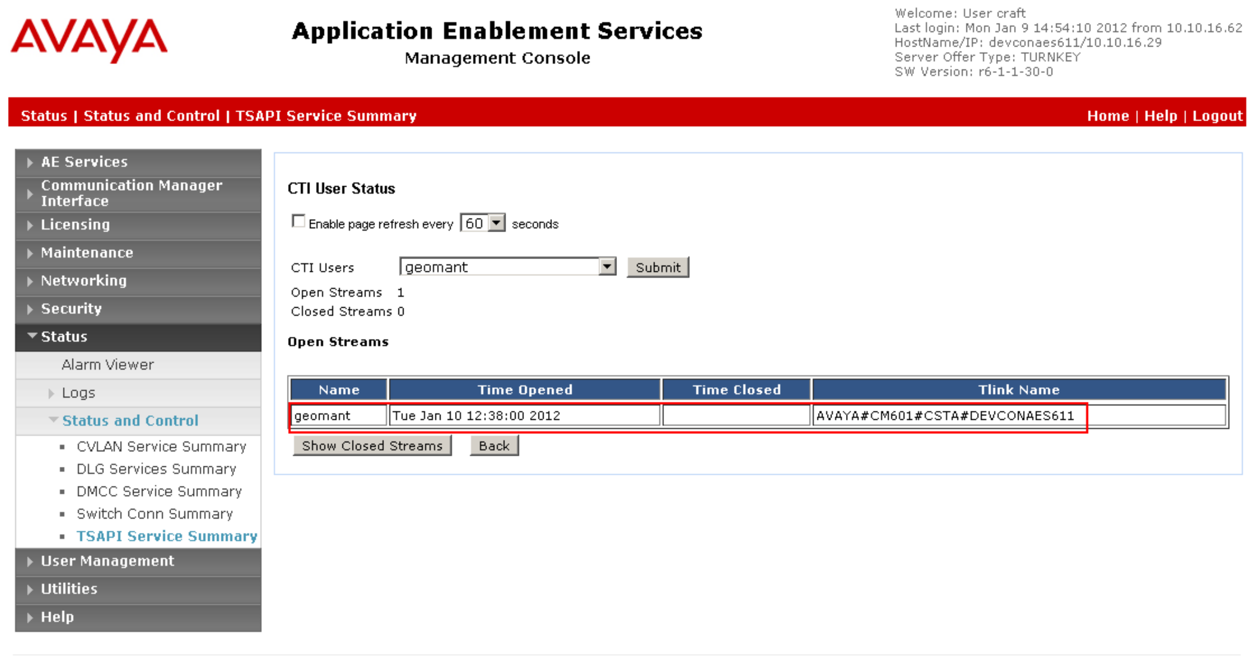
☐ Enable page refresh every 60 seconds

CTI Users: geomant
Open Streams
Closed Streams

Open Streams

Name	Time Opened	Time Closed	Tlink Name
tsapi	Fri Jan 6 13:48:58 2012		AVAYA#CM601#CSTA#DEVCONAES611
tsapi	Fri Jan 6 13:48:59 2012		AVAYA#CM601#CSTA#DEVCONAES611
tsapi	Fri Jan 6 13:48:59 2012		AVAYA#CM601#CSTA#DEVCONAES611
tsapi	Fri Jan 6 13:48:59 2012		AVAYA#CM601#CSTA#DEVCONAES611
tsapi	Fri Jan 6 13:48:59 2012		AVAYA#CM601#CSTA#DEVCONAES611
tsapi	Fri Jan 6 17:21:35 2012		AVAYA#CM601#CSTA#DEVCONAES611

Verify a corresponding open stream containing the configured **Tlink Name** and CTI User **Name**. Confirm a value in **Time Opened** and that there is no entry in **Time Closed.**



Welcome: User craft
Last login: Mon Jan 9 14:54:10 2012 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users: geomant
Open Streams 1
Closed Streams 0

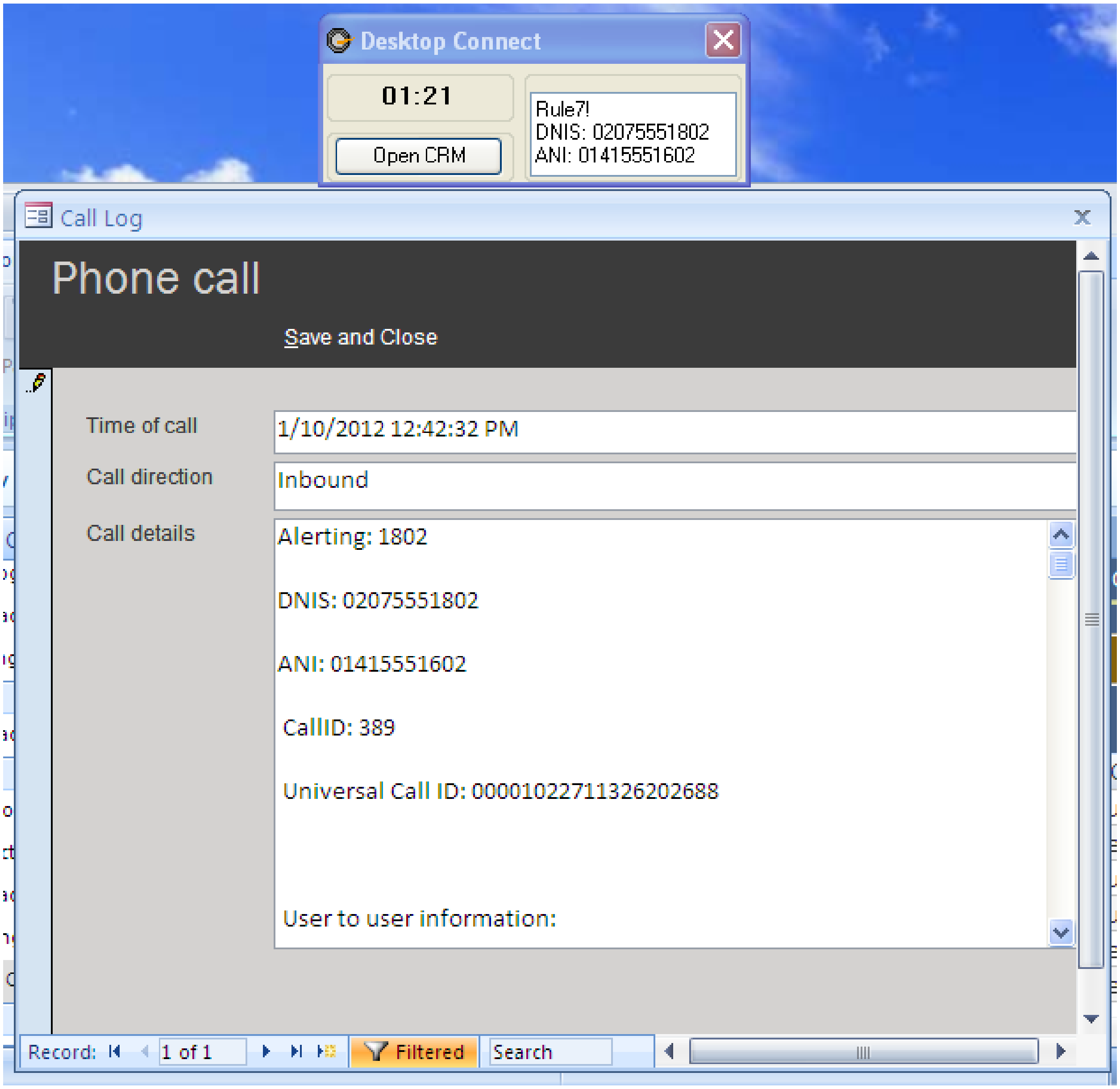
Open Streams

Name	Time Opened	Time Closed	Tlink Name
geomant	Tue Jan 10 12:38:00 2012		AVAYA#CM601#CSTA#DEVCONAES611

9.3. Verify Geomant Desktop Connect Client

9.3.1. ACD Configuration

Place an incoming call from the PSTN to the corresponding VDN, in this example **1802**, verify that the relevant rule is observed and the correct screen pop information is presented defined by the **Rule**7. See **Section 8.3** for information about **Rule 7**.



Rule7!
DNIS: 02075551802
ANI: 01415551602

Time of call: 1/10/2012 12:42:32 PM

Call direction: Inbound

Call details:

Alerting: 1802

DNIS: 02075551802

ANI: 01415551602

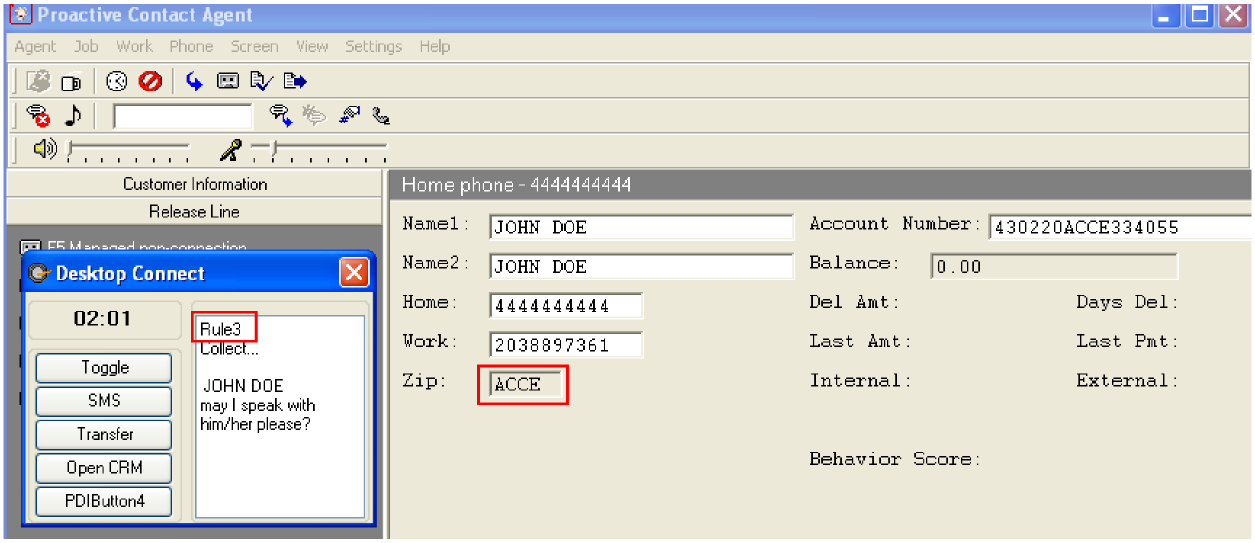
CallID: 389

Universal Call ID: 00010227113262O2688

User to user information:

9.3.2. Proactive Contact Configuration

Using the Proactive Contact agent, login to the relevant job, upon delivery of an outbound call verify that the relevant rule is observed and the correct screen pop information is presented. In this case, **Rule 3** configured in **Section 8.3** is triggered as the **ZIP** field matches a value of **ACCE**. Note: On the configured agent screen, the field name is **ZIP**, however Desktop Connect uses the actual value of the field name in the Calling List.



02:01

Rule3
Collect...

JOHN DOE
may I speak with him/her please?

Home phone - 4444444444

Name1: JOHN DOE
Name2: JOHN DOE
Home: 4444444444
Work: 2038897361
Zip: ACCE
Account Number: 430220ACCE334055
Balance: 0.00
Del Amt:
Days Del:
Last Amt:
Last Pmt:
Internal:
External:
Behavior Score:

10. Conclusion

These Application Notes describe the configuration steps required for the Geomant Desktop Connect application to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Proactive Contact. All functionality and serviceability test cases were completed successfully.

11. Additional References

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

[1] Administering Avaya Aura® Communication Manager – Release 6.0, Issue 6.0, June 2010

[2] Administering Proactive Contact – Release 5 – July 2011

Product documentation for Geomant Products can be found at http://www.geomant.com

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.