



**Application Notes for Geomant Desktop Connect for  
Salesforce.com with Avaya Aura® Communication Manager  
using Avaya Aura® Application Enablement Services 6.3 –  
Issue 1.0**

**Abstract**

These Application Notes describe the configuration steps required for Geomant Desktop Connect for Salesforce.com to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.3. Geomant Desktop Connect for Salesforce.com provides a connector that links Avaya Aura® Communication Manager with cloud-based Customer Relationship Management provider Salesforce.com.

The compliance testing focused on the telephony integration with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Java Telephony Application Programming Interface.

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 for Salesforce.com to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.3. Geomant Desktop Connect for Salesforce.com provides a connector that links Avaya Aura® Communication Manager with cloud-based Customer Relationship Management provider Salesforce.com.

The compliance testing focused on the telephony integration with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Java Telephony Application Programming Interface (JTAPI).

The JTAPI interface is used by Geomant Desktop Connect for Salesforce.com to monitor agent station extensions on Avaya Aura® Communication Manager, and provide login/logout, agent work mode change, screen pop, and click-to-dial via the web-based agent application with Salesforce.com.

JTAPI is a client-side interface to the Telephony Services Application Programmer Interface (TSAPI) on Avaya Aura® Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon agent log in, the application automatically uses JTAPI to query device information, log the agent in, and request device monitoring.

For the manual part of the testing, incoming ACD calls were placed with available agents that have web browser connections to Salesforce.com. All necessary call actions were initiated from the agent telephone, such as answer and drop. The click-to-dial calls were initiated by clicking on the contact phone number displayed on the agent desktop.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the Desktop Connect server and client.

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 interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Desktop Connect:

- Use of TSAPI query service to query agent states.
- Use of TSAPI event report service to monitor agent stations.
- Use of TSAPI set value service to set agent states, including login, logout, and work mode changes.
- Use of TSAPI call control service to support the click-to-dial feature.
- Proper handling of call scenarios involving inbound, outbound, ACD, non-ACD, drop, hold/reconnect, voicemail, transfer, conference, multiple agents, multiple calls, different ANI/DNIS, internal, click-to-dial from contact phone number, pending aux work, pending log out, aux work reason codes.

The serviceability testing focused on verifying the ability of Desktop Connect to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Desktop Connect server and client.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Desktop Connect from the compliance testing.

- The design assumed the maximum length of internal extensions is shorter than the length of calling party numbers received from the PSTN. In the case that the two lengths are the same, then incoming calls from the PSTN will be treated as internal calls, without any database lookup and screen pop.
- When the calling party number isn't available from the PSTN, and the number of characters in the received trunk group data is less than or equal to the maximum length of internal extensions, then the call is treated as internal, without any automatic pop of new contact screen. The agent can subsequently click on the link associated with the "Internal – no match" message to manually pop the new contact screen.
- By design, the transfer-to agent for a blind transfer scenario will receive contact screen pop with the PSTN caller information, whereas the destination agent for all other transfer and conference scenarios will not receive any screen pop.
- Upon a server or client Ethernet disruption, the "Event queue error" will be displayed on the client desktop, and the client will need to manually log out and log back in upon link restoration.
- The application does not support TSAPI user credentials that contained the special character semicolon.

## 2.3. Support

Technical support on Desktop Connect can be obtained through the following:

- **Phone:** +44 1789 766178
- **Email:** [product\\_dc@support.geomant.com](mailto:product_dc@support.geomant.com)

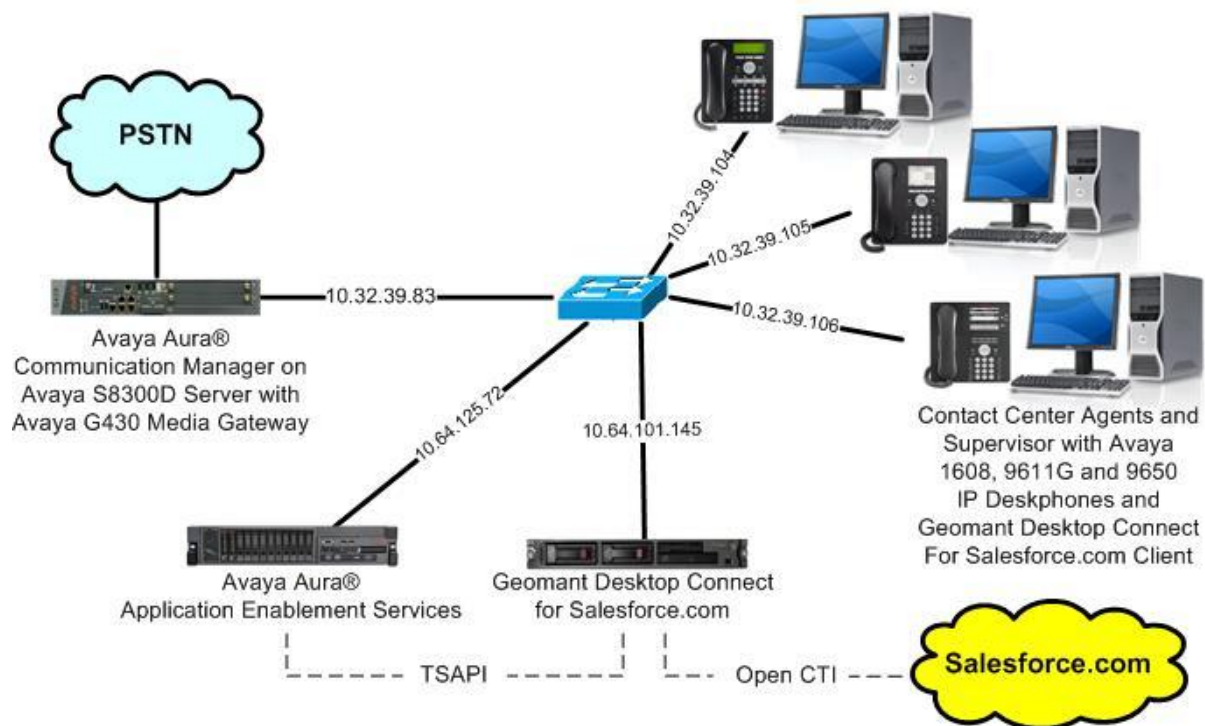
### 3. Reference Configuration

Desktop Connect can be deployed on a single server or with components distributed across multiple servers. The compliance testing used a single server configuration.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described.

The contact center devices used in the compliance testing are shown in the table below. In the compliance testing, Desktop Connect monitored two agent station extensions shown below.

Device Type	Device Number/Extension
VDNs	49001, 49002
Skill groups	48101, 48102
Agent stations	45001, 45002
Agent IDs	45881, 45882
Agent Passwords	45881, 45882
Supervisor station	45000



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8300D Server with Avaya G430 Media Gateway	6.3.4 (R016x.03.0.124.0-21291)
Avaya Aura® Application Enablement Services	6.3.1 (6.3.1.0.19-0)
Avaya 1608 IP Deskphone (H.323)	1.343A
Avaya 9611G IP Deskphone (H.323)	6.3037
Avaya 9650 IP Deskphone (H.323)	3.212A
Geomant Desktop Connect for Salesforce.com on Windows Server 2008 R2 Standard <ul style="list-style-type: none"><li>• Avaya JTAPI Windows Client</li><li>• Salesforce CRM</li><li>• Salesforce.com OpenCTI API</li></ul>	1.1.4  6.1.0.94 Spring 2014 29.0

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Obtain reason codes

### 5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	

### 5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. 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				
<b>Extension:</b> 40001				
<b>Type:</b> ADJ-IP				
COR: 1				
<b>Name:</b> AES CTI Link				

### 5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                               Page 5 of 20
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station      Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y      UCID Network Node ID: 1
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Desktop Connect.

```
change system-parameters features                               Page 13 of 20
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
  Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? y
  Call Classification After Answer Supervision? n
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
```



## 5.4. Obtain Reason Codes

For contact centers that use reason codes, enter the “change reason-code-names” command to display the configured reason codes. Make a note of the **Aux Work** reason code values, which will be used later to configure Desktop Connect.

Note that Desktop Connect supports up to six reason codes for aux work, and none for log out.

change reason-code-names

Page 1 of 1

REASON CODE NAMES

Aux Work/  
Interruptible?

Logout

Reason Code 1: **Lunch** /n

Reason Code 2: **Coffee** /n

Reason Code 3: **Injury** /n

Reason Code 4: **Fire** /n

Reason Code 5: **Flood** /n

Reason Code 6: **Snakes** /n

Reason Code 7: /n

Reason Code 8: /n

Reason Code 9: /n

Default Reason Code:

## 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
- Verify license
- Administer TSAPI link
- Disable security database
- Restart services
- Obtain Tlink name
- Administer Geomant user

### 6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are "Login" and "Reset" buttons. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2013 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message displays user information: "Welcome: User cust", "Last login: Tue Feb 25 12:57:37 2014 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes\_125\_72/10.64.125.72", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP", "SW Version: 6.3.1.0.19-0", "Server Date and Time: Tue Feb 25 12:57:58 MST 2014", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home | Help | Logout". The left sidebar contains a list of menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list of domains and their functions: "AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.", "Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.", "High Availability - Use High Availability to manage AE Services HA.", "Licensing - Use Licensing to manage the license server.", "Maintenance - Use Maintenance to manage the routine maintenance tasks.", "Networking - Use Networking to manage the network interfaces and ports.", "Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.", "Status - Use Status to obtain server status informations.", "User Management - Use User Management to manage AE Services users and AE Services user-related resources.", "Utilities - Use Utilities to carry out basic connectivity tests.", and "Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom, a note states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."


## 6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The main content area is titled "Licensing" and contains three sections of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bulleted list with "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bulleted list with "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bulleted list with "Reserved Licenses". The left sidebar menu is expanded to show "WebLM Server Address", "WebLM Server Access" (highlighted in blue), and "Reserved Licenses". The top header and navigation bar are identical to the previous screenshot.

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.


**Web License Manager (WebLM v6.3)**
Help | About | Change Password

WebLM Home  
Install license  
Licensed products  
APPL\_ENAB  
▼ Application\_Enablement  
View license capacity  
View peak usage  
Uninstall license  
Server properties  
Manage users  
Shortcuts  
Help for Installed Product

**Application Enablement (CTI) - Release: 6 - SID: 10503000**
**Standard License file**

You are here: Licensed Products > Application\_Enablement > View License Capacity  
License installed on: May 11, 2012 7:07:47 PM -04:00  
**License File Host IDs:** 00-16-3E-48-ED-82

**Licensed Features**

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,, CCE_001, AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

### 6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" table with one link (ID 1, Switch Connection S8800, Switch CTI Link # 2, ASAI Link Version 6, Security Both). Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	6	Both

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main content area contains form fields for "Link" (value 2), "Switch Connection" (value S8300D), "Switch CTI Link Number" (value 1), "ASAI Link Version" (value 6), and "Security" (value Unencrypted). There are "Apply Changes" and "Cancel Changes" buttons at the bottom.



## 6.4. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. A red navigation bar contains "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various system components, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", followed by an "Apply Changes" button.

Welcome: User cust  
Last login: Tue Feb 25 12:57:37 2014 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Tue Feb 25 12:57:58 MST 2014  
HA Status: Not Configured

**Security | Security Database | Control** Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ **Security**
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ **Security Database**
    - **Control**

**SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services**

☐ Enable SDB for DMCC Service

☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

[Apply Changes](#)

## 6.5. Restart Services

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. A red navigation bar contains "Maintenance | Service Controller" and links for "Home | Help | Logout". The left sidebar lists various system components, with "Maintenance" expanded to show "Service Controller" as the selected option. The main content area, titled "Service Controller", contains a table of services and their statuses. The "TSAPI Service" is checked, and the "Restart Service" button is highlighted. Below the table, there is a link to "Status and Control" and a row of action buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

[Start](#) [Stop](#) [Restart Service](#) [Restart AE Server](#) [Restart Linux](#) [Restart Web Server](#)

## 6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Desktop Connect.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES\_125\_72”. Note the use of the switch connection “S8300D” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a list of three Tlink names, each with a radio button. The first option, "AVAYA#S8300D#CSTA#AES\_125\_72", is selected. A "Delete Tlink" button is located below the list.

AVAYA Application Enablement Services Management Console

Welcome: User cust  
Last login: Tue Feb 25 12:57:37 2014 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Tue Feb 25 12:57:58 MST 2014  
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Account Management  
Audit  
Certificate Management  
Enterprise Directory  
Host AA  
PAM  
Security Database  
Control  
CTI Users  
Devices  
Device Groups  
Tlinks

Tlinks

Tlink Name

- ☒ AVAYA#S8300D#CSTA#AES\_125\_72
- ☐ AVAYA#S8800#CSTA#AES\_125\_72
- ☐ AVAYA#S8800#CSTA-S#AES\_125\_72

Delete Tlink



## 6.7. Administer Geomant User

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.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Feb 25 12:57:37 2014 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Tue Feb 25 12:57:58 MST 2014  
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with \* can not be empty.

\* User Idgeomant

\* Common Namegeomant

\* Surnamegeomant

\* User Password\*\*\*\*\*

\* Confirm Password\*\*\*\*\*

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

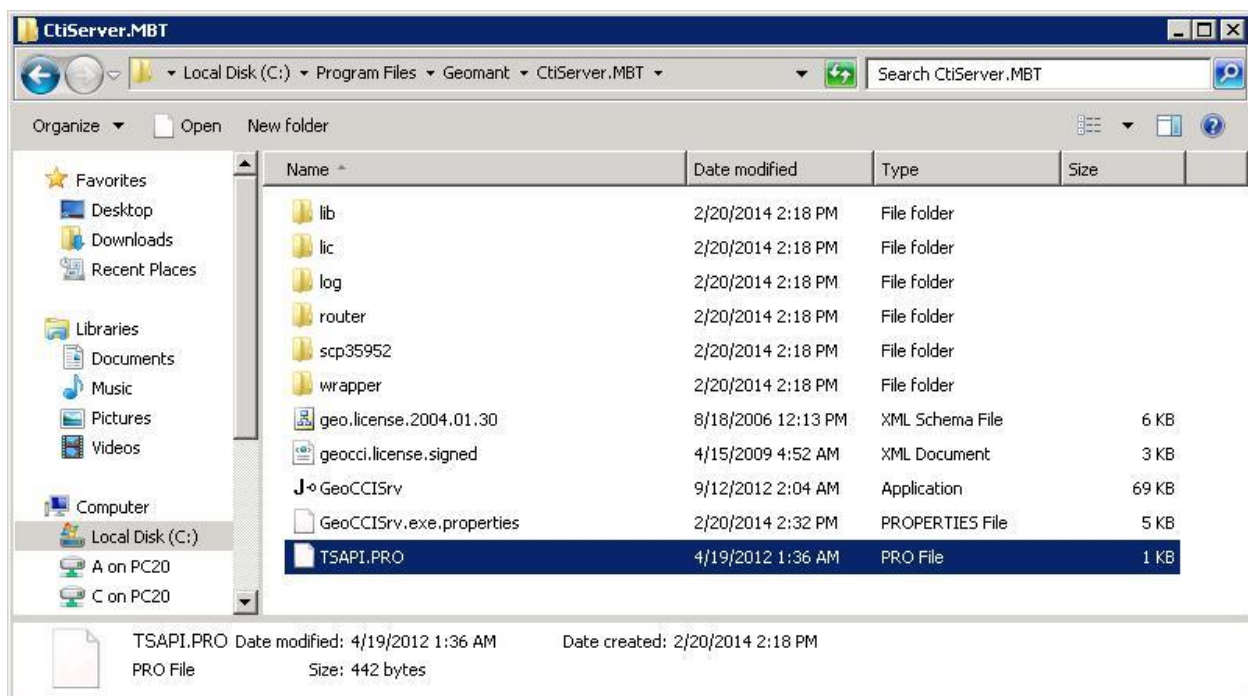
## 7. Configure Geomant Desktop Connect for Salesforce.com

This section provides the procedures for configuring Desktop Connect. The procedures include the following areas:

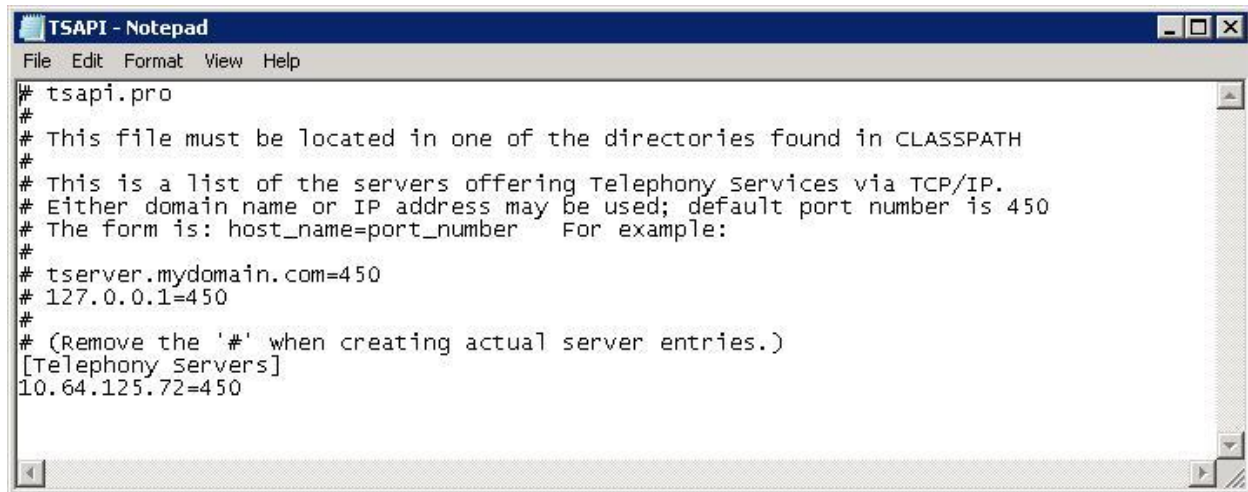
- Administer TSAPI.PRO
- Administer GeoCCISrv.exe.properties
- Administer call center

### 7.1. Administer TSAPI.PRO

From the Desktop Connect server, navigate to the **C:\Program Files\Geomant\CtiServer.MBT** directory to locate the **TSAPI.PRO** file shown below.



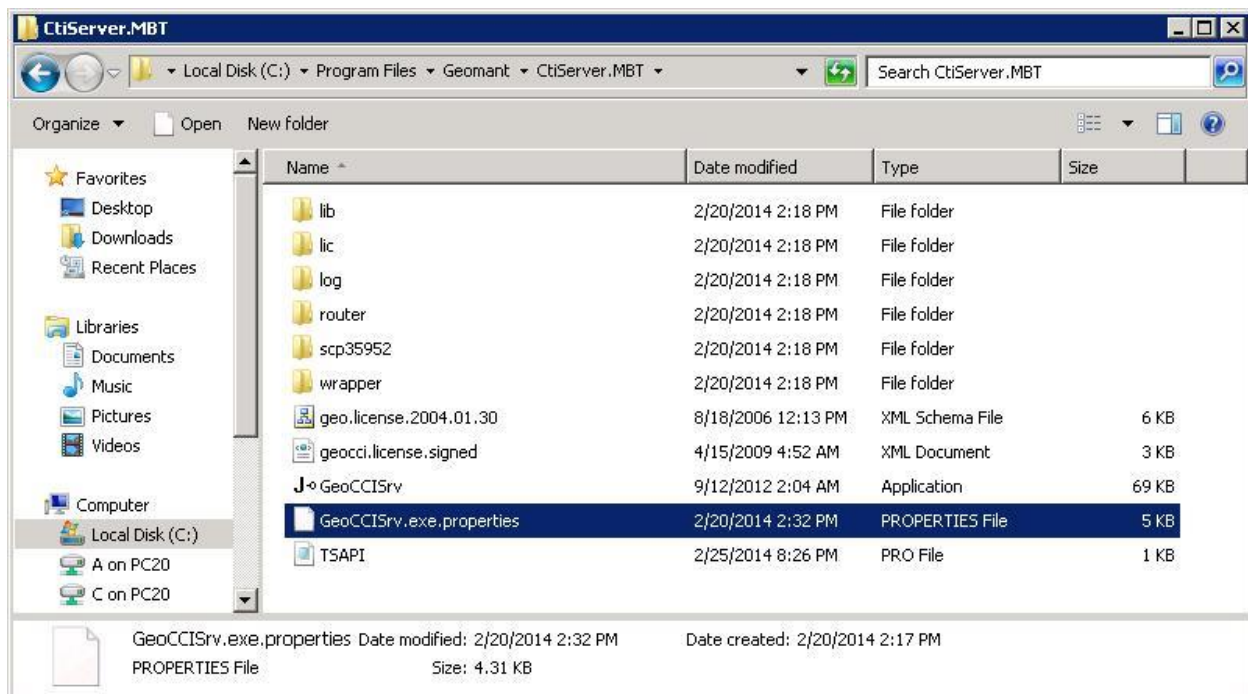
Open the **TSAPI.PRO** file with the Notepad application. Add an entry line shown below, where “10.64.125.72” is the IP address of Application Enablement Services, and “450” is the default port number.



```
# tsapi.pro
#
# This file must be located in one of the directories found in CLASSPATH
#
# 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
# 127.0.0.1=450
#
# (Remove the '#' when creating actual server entries.)
[Telephony Servers]
10.64.125.72=450
```

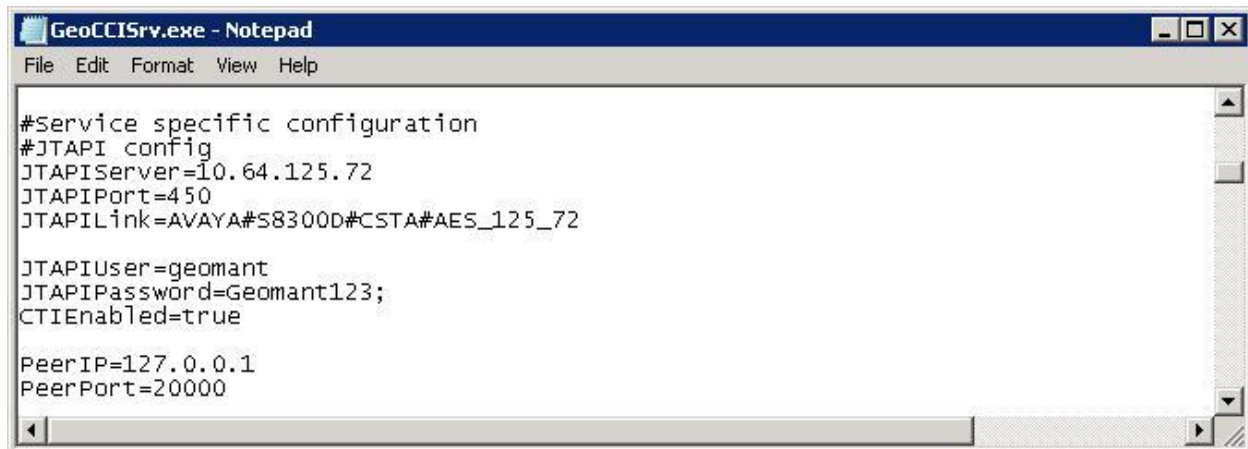
## 7.2. Administer GeoCCISrv.exe.properties

In the same directory, locate the **GeoCCISrv.exe.properties** file.



Open the **GeoCCISrv.exe.properties** file with the Notepad application. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **JTAPIServer:** IP address of Application Enablement Services.
- **JTAPILink:** The Tlink name from **Section 6.6**.
- **JTAPIUser:** The Geomant user credentials from **Section 6.7**.
- **JTAPIPassword:** The Geomant user credentials from **Section 6.7**.



### 7.3. Administer Call Center

Access the web-based interface by using the URL “https://na12.salesforce.com” in an Internet browser window, and log in with the administrator credentials.



The screen below is displayed.

The screenshot displays the Salesforce 14 Home page. The top navigation bar includes the Salesforce logo, a search bar, and user information (Demoadmin Geomant). Below the navigation bar is a main content area with a left sidebar containing links to Home, Chatter, Accounts, Contacts, Cases, Solutions, Reports, Dashboards, and GeoCrm. The main content area includes a 'Quick Find' search bar, a 'Force.com Home' section, a 'System Overview' section with a message, a 'Getting Started' section with a 'Build App' button, and a 'Recent Items' table. The right sidebar contains links to developerforce, Resources, Featured Content, and Events.

**System Overview**

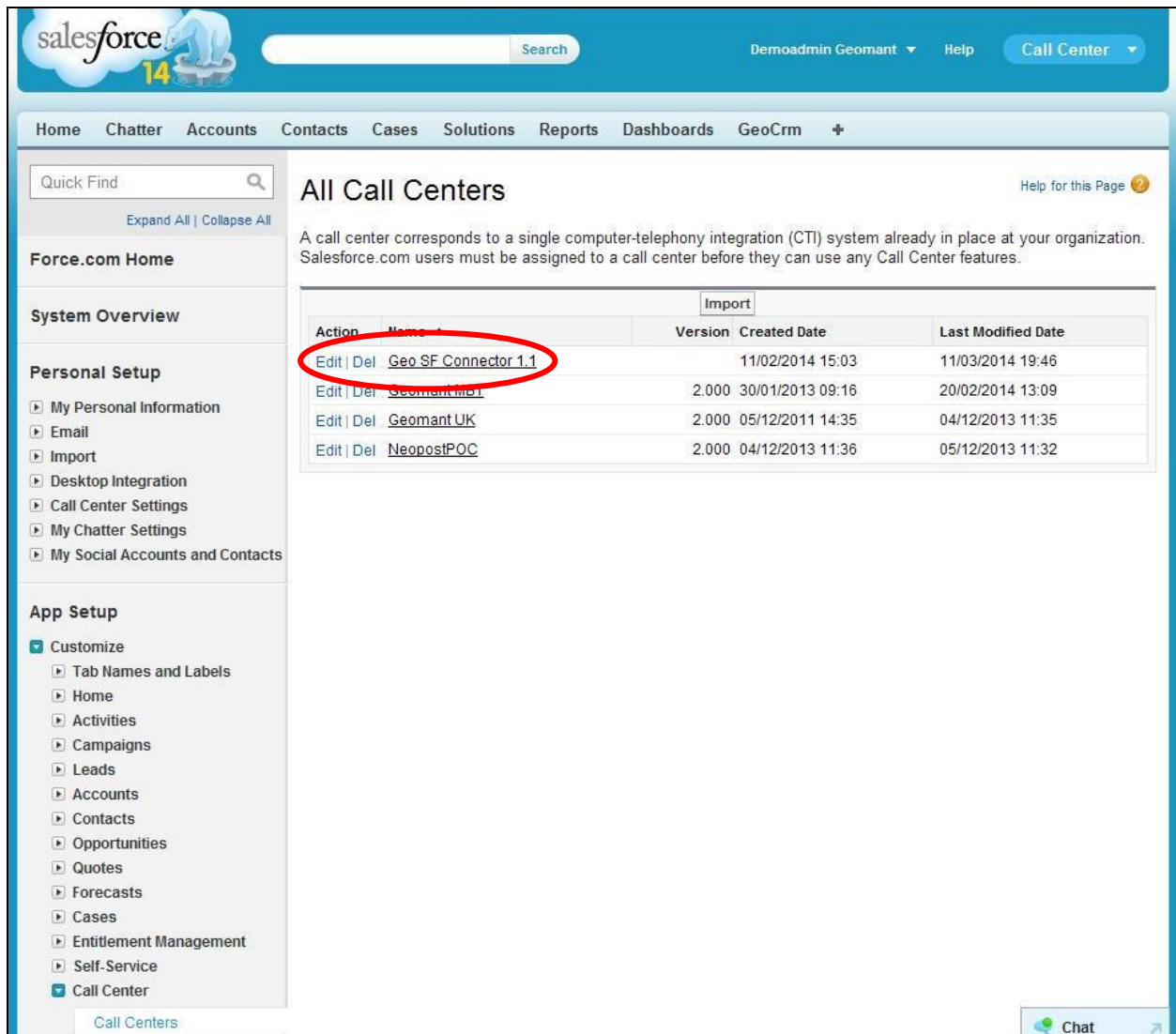
You have a message.  
Expand to see messages or go to the [system overview](#) page to see additional limits.

**Recent Items** beta

Name	Type	Object
Demo2 Demo2	User	
Demoadmin Geomant	User	
User Demo	User	



Select **App Setup** → **Customize** → **Call Center** → **Call Centers** from the left pane, to display a list of pre-configured call centers. Click on the **Edit** button associated with the relevant call center.



**Call Centers**

A call center corresponds to a single computer-telephony integration (CTI) system already in place at your organization. Salesforce.com users must be assigned to a call center before they can use any Call Center features.

Action	Name	Version	Created Date	Last Modified Date
<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Geo SF Connector 1.1</a>		11/02/2014 15:03	11/03/2014 19:46
<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Sequentia 1.1</a>	2.000	30/01/2013 09:16	20/02/2014 13:09
<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Geomant UK</a>	2.000	05/12/2011 14:35	04/12/2013 11:35
<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">NeopostPOC</a>	2.000	04/12/2013 11:36	05/12/2013 11:32

The **Call Center Edit** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Outside Prefix:** The relevant prefix to apply for outbound calls.
- **Long Distance Prefix:** The relevant prefix to apply for long distance calls.
- **International Prefix:** The relevant prefix to apply for international calls.
- **Internal Phone Length:** The maximum length of internal extensions, in this case “5”
- **Aux code Labels:** The aux work reason code values from **Section 5.4**.

**Call Center Edit** Save Cancel

**General Information** ! = Required Information

InternalNameAAA	GeoCRMConnect
Display Name	Geo SF Connector 1.1
CTI Adapter URL	https://devconnect.crm.de
Use CTI API	true
Phone Height	300
Phone Width	500

**Dialing Options**

Outside Prefix	8
Long Distance Prefix	
International Prefix	011
C2D enabled	true
Min Dom Phone Length	7
Internal Phone Length	5

**Aux code Labels**

AUX Code 1	Lunch
AUX Code 2	Coffee
AUX Code 3	Injury
AUX Code 4	Fire
AUX Code 5	Flood
AUX Code 6	Snakes

## 8. Verification Steps

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

### 8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.


```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	6	no	aes_125_72	established	84	78

### 8.2. 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**. Also verify that the **Associations** column reflects the number of agents logged into Desktop Connect, in this case “2”.



# Application Enablement Services Management Console

Welcome: User cust  
Last login: Tue Mar 11 09:03:07 2014 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.1.0.19-0  
Server Date and Time: Tue Mar 11 09:04:32 MDT 2014  
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

### TSAPI Link Details

☐ Enable page refresh every  seconds

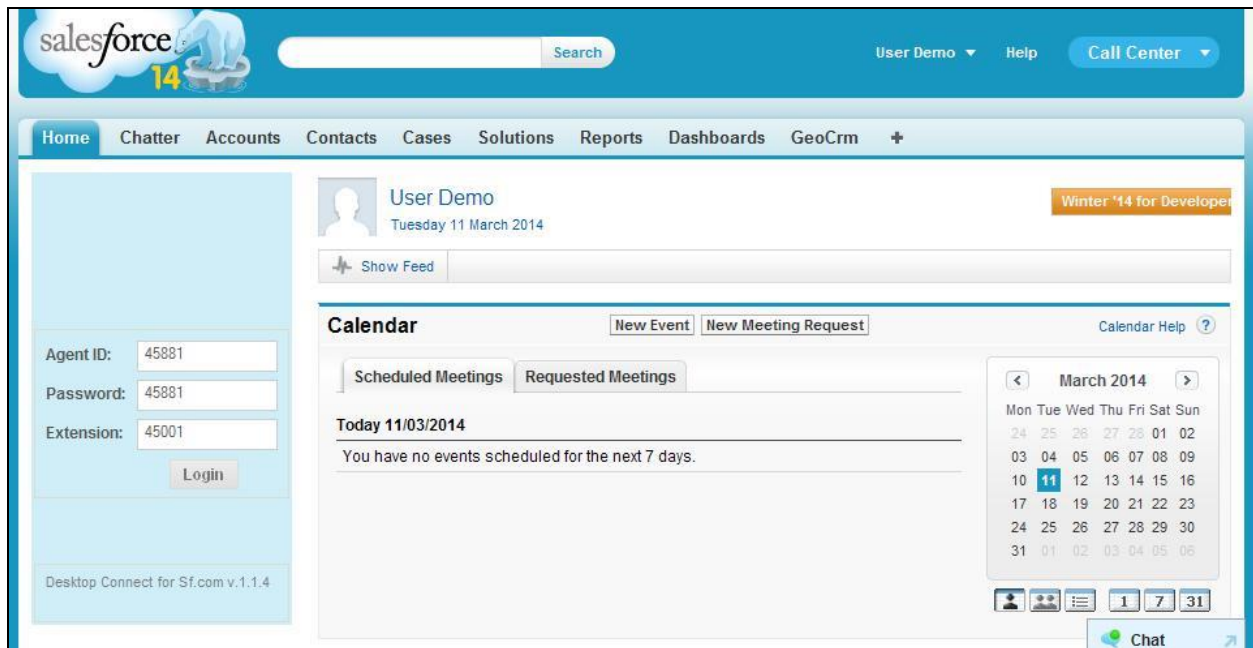
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
○	1	S8800	2	Talking	Mon Nov 25 11:49:35 2013	Online	16	0	15	15	30
●	2	S8300D	1	Talking	Tue Mar 11 07:05:05 2014	Online	16	2	78	84	30



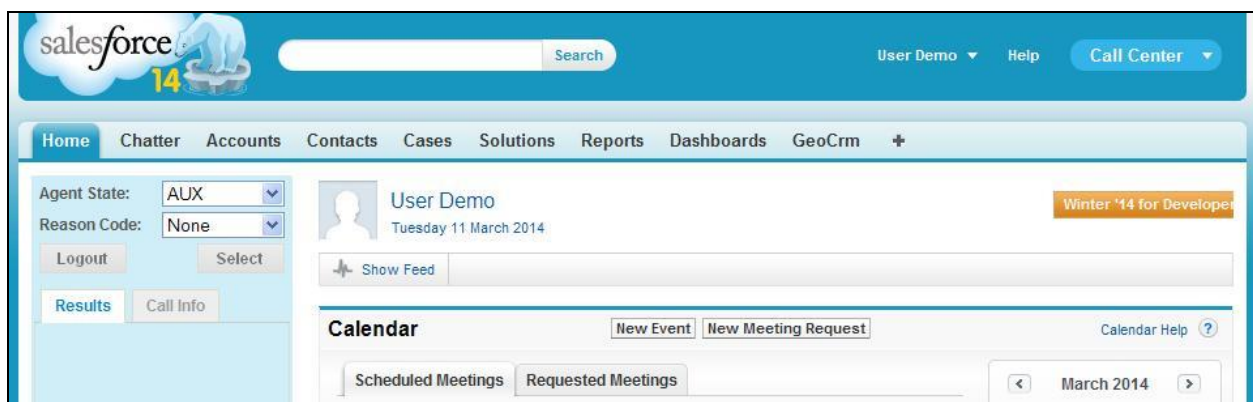
### 8.3. Verify Geomant Desktop Connect for Salesforce.com

From the agent PC, access the web-based interface by using the URL “https://na12.salesforce.com” in an Internet browser window, and log in with the relevant user credentials provided by Geomant. The screen below is displayed.

In the left pane, enter the relevant **Agent ID**, agent **Password**, and station **Extension** from **Section 3**, as shown below. Click **Login**.



Verify that the left pane is updated showing **Agent State** of “AUX”. Select the desired ready state from the **Agent State** drop-down list, such as “Auto-In”, followed by the **Select** button.



Verify that the left pane is updated showing **Agent State** of “Auto-In”, and the message “State changed to AUTO\_IN” in the bottom left pane.

The screenshot shows the Salesforce 14 user interface. The top navigation bar includes the Salesforce logo, a search bar, and links for 'User Demo', 'Help', and 'Call Center'. The main navigation menu has tabs for 'Home', 'Chatter', 'Accounts', 'Contacts', 'Cases', 'Solutions', 'Reports', 'Dashboards', and 'GeoCrm'. The left sidebar shows the 'Agent State' dropdown set to 'Auto-in', with 'Logout' and 'Select' buttons. Below this are 'Results' and 'Call Info' buttons. The main content area displays the user profile for 'User Demo' with the date 'Tuesday 11 March 2014' and a 'Show Feed' button. A 'Calendar' section is visible, showing 'Scheduled Meetings' and 'Requested Meetings' tabs. A message at the bottom left of the sidebar reads 'State change to AUTO\_IN'.

Make an incoming ACD call. Verify that the contact record associated with the PSTN caller is retrieved and displayed, with proper values in the relevant fields. Also verify that the **Agent State** in the left pane changed to “Busy”, as shown below.

The screenshot shows the Salesforce 14 interface with the 'Contacts' tab selected. The left sidebar shows the 'Agent State' dropdown set to 'Busy', with 'Logout' and 'Select' buttons. Below this are 'Results' and 'Call Info' buttons. The main content area displays the contact record for 'Mr. DevConnect908 Avaya'. The contact details include:
 

- Contact Owner: User Demo (Change)
- Name: Mr. DevConnect908 Avaya
- Account Name: Avaya
- Title: (blank)
- Department: Solution Interoperability Lab
- Birthdate: (blank)
- Reports To: (View Org Chart)
- Lead Source: (blank)
- Mailing Address: 211 Mt Airy Rd, Basking Ridge, NJ 07920, USA
- Languages: English
- Created By: User Demo, 26/02/2014 16:12
- Phone: 9088485601
- Home Phone: (blank)
- Mobile: (blank)
- Other Phone: (blank)
- Fax: (blank)
- Email: (blank)
- Assistant: (blank)
- Asst. Phone: (blank)
- Other Address: (blank)
- Level: Primary
- Last Modified By: User Demo, 03/03/2014 18:04

 The bottom left of the sidebar shows 'Recent Items' with links to 'DevConnect908 Avaya' and 'DevConnect732 Avaya'.

## 9. Conclusion

These Application Notes describe the configuration steps required for Geomant Desktop Connect for Salesforce.com to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.3. All feature and serviceability test cases were completed with one observation noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9, Release 6.3, October 2013, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 2, October 2013, available at <http://support.avaya.com>.
3. *Desktop Connect for CRM Deployment and Configuration Guide*, Version 4.0, June 13, 2013, available from Geomant Support.

---

**©2014 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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