



Application Notes for Geomant Desktop Connect for Salesforce.com 1.4.1 with Avaya Aura® Communication Manager 6.3.6 and Avaya Aura® Application Enablement Services 6.3.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Geomant Desktop Connect for Salesforce.com 1.4.1 to interoperate with Avaya Aura® Communication Manager 6.3.6 and Avaya Aura® Application Enablement Services 6.3.3. 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.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 1.4.1 to interoperate with Avaya Aura® Communication Manager 6.3.6 using Avaya Aura® Application Enablement Services 6.3.3. 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 contact center devices 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 desktop whenever possible, 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 JTAPI/TSAPI query service to query agent states and device information.
- Use of JTAPI/TSAPI event report service to monitor agent stations, skill groups, and VDNs.
- Use of JTAPI/TSAPI set value service to set agent states, including login, logout, and work mode changes.
- Use of JTAPI/TSAPI call control service to support call control and 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, and 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.

- By design, the destination agent for transfer scenario will receive contact screen pop with PSTN caller information, whereas the destination agent for conference scenarios will not.
- While on an active ACD call, agent can press the Logout icon on the desktop and becomes out of sync with Communication Manager. The workaround is to log back into Desktop Connect, and log out after completing the ACD call.
- In general, mixed use of agent desktop and telephone to perform call control actions are supported. For the transfer and conference features, however, all actions need to start and complete from the same source.
- The application does not support TSAPI user credentials that contained the special character semicolon.
- The VDN parameter on the agent desktop screen will display the associated skill group name for ACD calls.

2.3. Support

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

- **Phone:** +44 1789 766178
- **Email:** 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 the VDNs, skill groups, and agent stations.

Device Type	Extension
VDNs	60001, 60002
Skill Groups	65081, 65082
Supervisor	65000
Agent Stations	65001, 65002
Agent IDs	65881, 65882
Agent Passwords	65881, 65882

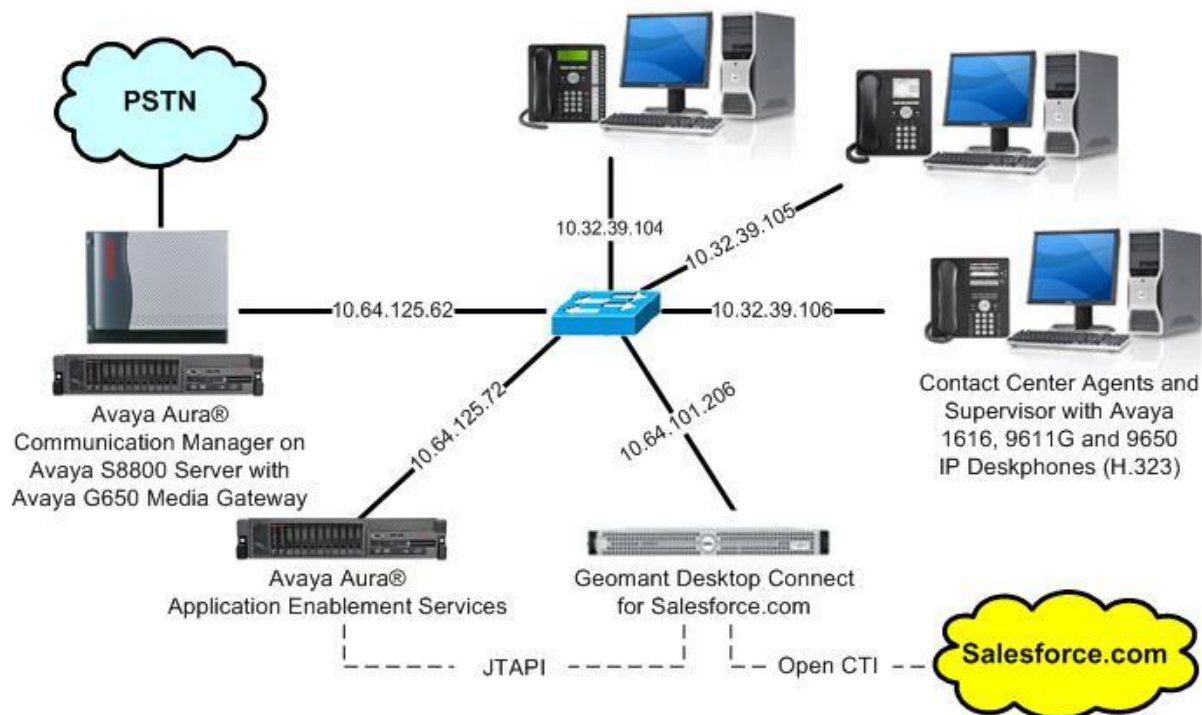


Figure 1: Compliance Testing Configuration

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 S8800 Server with Avaya G650 Media Gateway	6.3.6 (R016x.03.0.124.0-21591)
Avaya Aura® Application Enablement Services	6.3.3 SP1 (6.3.3.1.10-0)
Avaya one-X® Agent	2.5.5 (2.5.50022.0)
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
Avaya 9650 IP Deskphone (H.323)	3.230A
Geomant Desktop Connect for Salesforce.com on Microsoft Windows Server 2008 R2 Standard <ul style="list-style-type: none">• Avaya JTAPI Windows Client• Salesforce.com Open CTI API	1.4.1 6.1.0.94 NA
Salesforce CRM	Winter 2014/2015

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	Computer Telephony Adjunct Links?	y	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	n	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 2		Page	1 of	3
CTI LINK				
CTI Link:	2			
Extension:	60100			
Type:	ADJ-IP			
		COR: 1		
Name:	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: 27
```

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? y
  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 codes, 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 service
- 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 a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 Avaya Inc. All Rights Reserved." is displayed.

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

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 the user. The left sidebar contains a navigation menu with options: 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 provides an overview of the OAM web interface, listing the administrative domains it manages: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states that these domains can be served by one administrator for all domains or a separate administrator for each domain.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Dec 9 08:04:15 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: 6.3.3.1.10-0
Server Date and Time: Tue Dec 09 08:04:56 MST 2014
HA Status: Not Configured

Home | Help | Logout

Home

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- 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.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for 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 displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area is titled "Licensing" and provides instructions for setting up and maintaining the WebLM, including the WebLM Server Address, WebLM Server Access, and Reserved Licenses. The left sidebar shows the navigation menu with "Licensing" selected, and "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses" listed under it. The main content area also includes a note about administering TSAPI Reserved Licenses or DMCC Reserved Licenses.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Dec 9 08:04:15 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: 6.3.3.1.10-0
Server Date and Time: Tue Dec 09 08:04:56 MST 2014
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security

WebLM Server Address
WebLM Server Access
Reserved Licenses

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:


- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. 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 the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

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 "S8800" 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 displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link: 1, Switch Connection: S8800, Switch CTI Link Number: 2, ASAI Link Version: 6, and Security: Unencrypted. Below the form are buttons for "Apply Changes" and "Cancel Changes".

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 the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control". The right pane shows the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User
Last login: Tue Dec 9 08:04:15 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: 6.3.3.1.10-0
Server Date and Time: Tue Dec 09 08:04:56 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 Service

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**.



Application Enablement Services
Management Console

Welcome: User
Last login: Tue Dec 9 08:04:15 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: 6.3.3.1.10-0
Server Date and Time: Tue Dec 09 08:04:56 MST 2014
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

Service Controller

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#S8800#CSTA#AES_125_72”. Note the use of the switch connection “S8800” 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 the user. The left sidebar contains a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security Database section is expanded, showing sub-items like Control, CTI Users, Devices, Device Groups, and Tlinks. The main content area, titled "Tlinks", shows a list of Tlink names with radio buttons for selection. The selected Tlink is "AVAYA#S8800#CSTA#AES_125_72". A "Delete Tlink" button is also visible.

Welcome: User
Last login: Tue Dec 9 08:04:15 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: 6.3.3.1.10-0
Server Date and Time: Tue Dec 09 08:04:56 MST 2014
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

Tlinks

Tlink Name

☐ AVAYA#S8300D#CSTA#AES_125_72

☒ AVAYA#S8800#CSTA#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
Last login: Tue Dec 9 08:04:15 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: 6.3.3.1.10-0
Server Date and Time: Tue Dec 09 08:06:00 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

Given Name

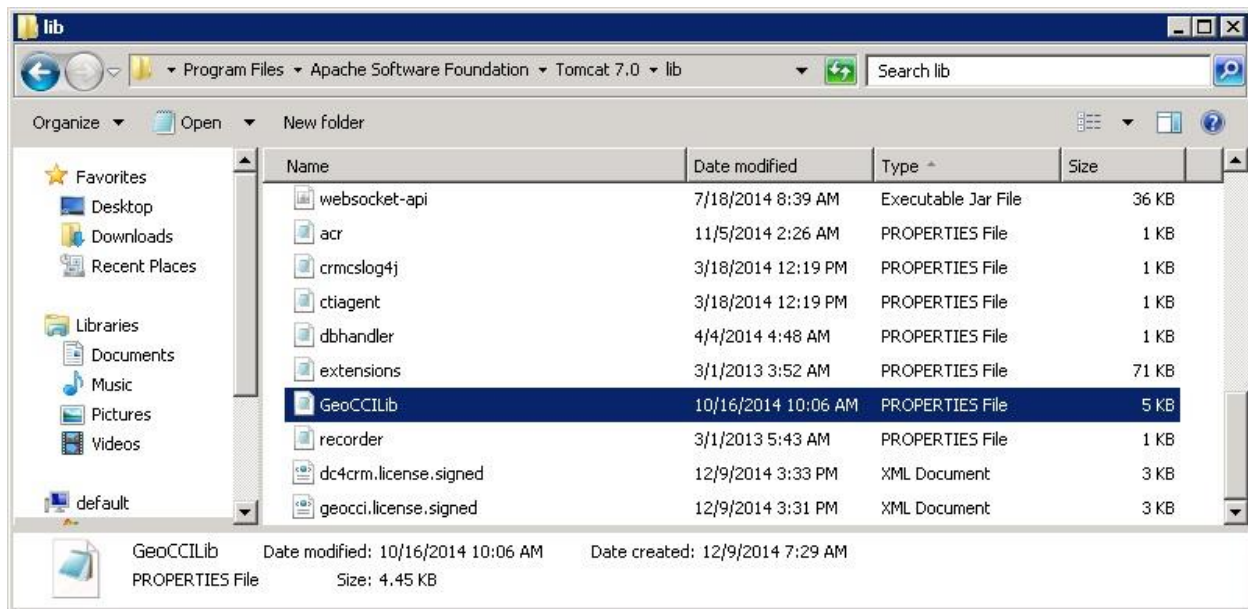
7. Configure Geomant Desktop Connect for Salesforce.com

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

- Administer GeoCCILib
- Administer call center

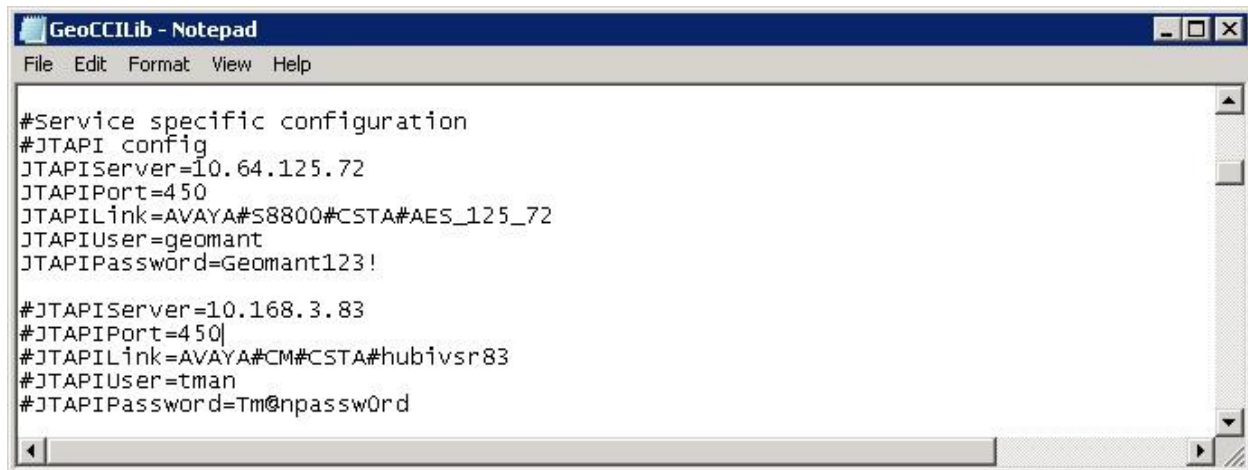
7.1. Administer GeoCCILib

From the Desktop Connect server, navigate to the **C:\Program Files\Apache Software Foundation\Tomcat 7.0\lib** directory to locate the **GeoCCILib** file shown below.



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

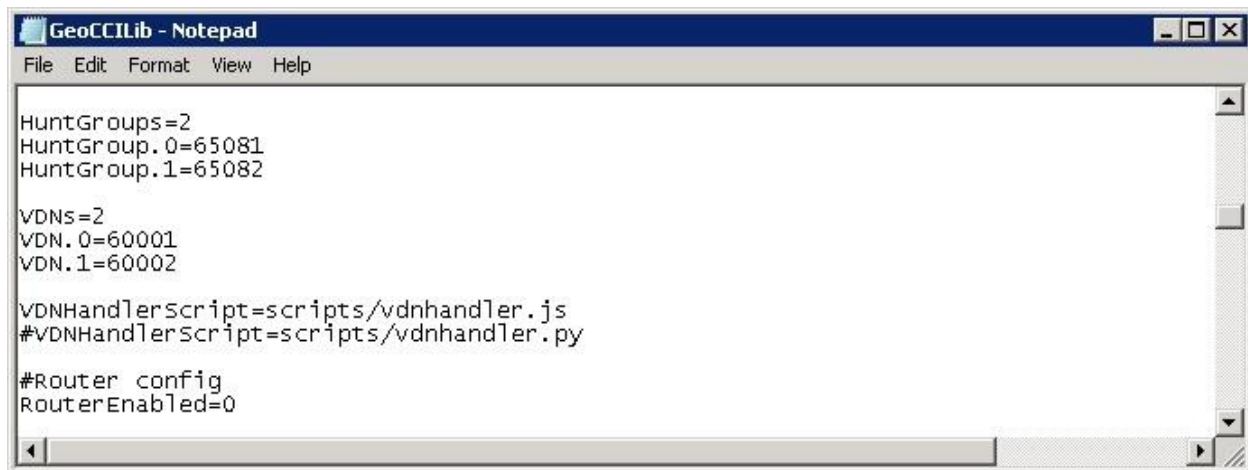
- **JTAPIServer:** IP address of Application Enablement Services.
- **JTAPILink:** The Tlink name from **Section 6.6**.
- **JTAPIUser:** The Geomant user credentials from **Section 6.7**.
- **JTAPIPassword:** The Geomant user credentials from **Section 6.7**.



```
#Service specific configuration
#JTAPI config
JTAPIServer=10.64.125.72
JTAPIPort=450
JTAPILink=AVAYA#S8800#CSTA#AES_125_72
JTAPIUser=geomant
JTAPIPassword=Geomant123!

#JTAPIServer=10.168.3.83
#JTAPIPort=450|
#JTAPILink=AVAYA#CM#CSTA#hubivsr83
#JTAPIUser=tman
#JTAPIPassword=Tm@npassw0rd
```

Scroll down to the **HuntGroups** and **VDNs** sub-sections. For **HuntGroups** and **VDNs**, enter the number of skill groups and VDNs from **Section 3** respectively, and create an entry for each skill group and VDN as shown below.



```
HuntGroups=2
HuntGroup.0=65081
HuntGroup.1=65082

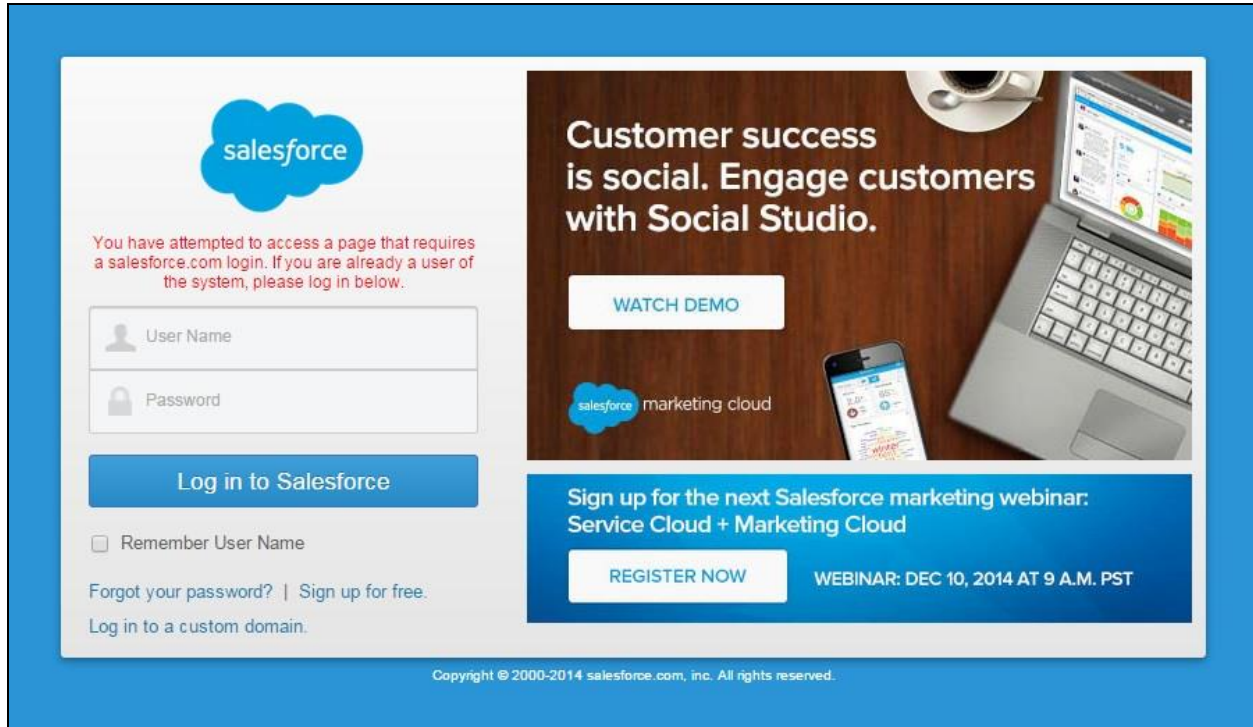
VDNs=2
VDN.0=60001
VDN.1=60002

VDNHandlerScript=scripts/vdnhandler.js
#VDNHandlerScript=scripts/vdnhandler.py

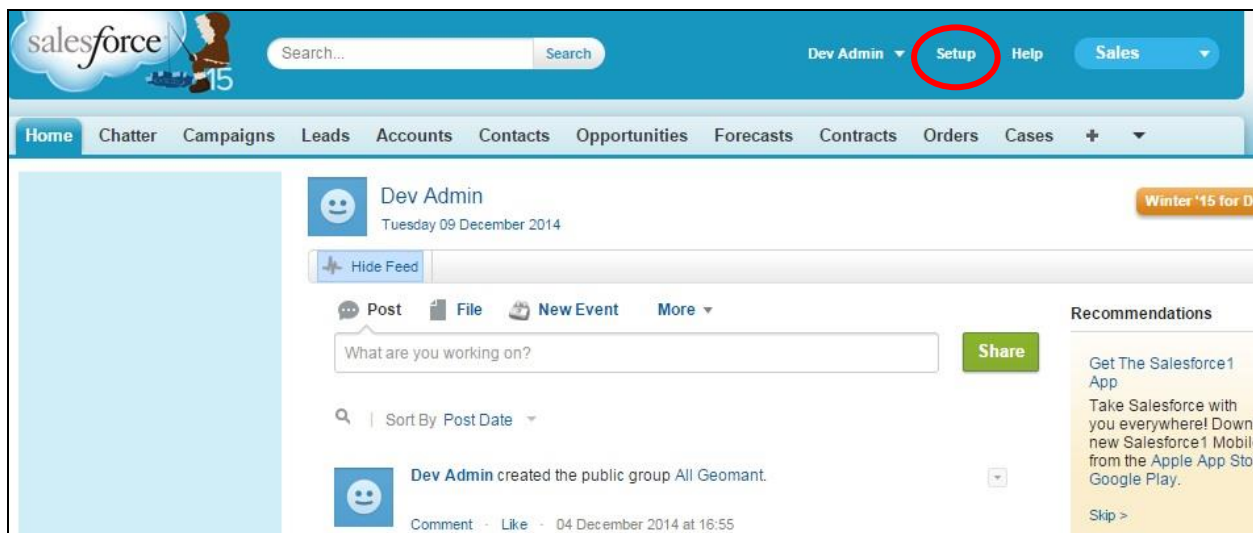
#Router config
RouterEnabled=0
```

7.2. Administer Call Center

Access the web-based interface by using the URL provided by the end customer for Salesforce.com. Log in using the administrator credentials.



In the subsequent screen, click **Setup** as shown below.



Scroll the screen as necessary, and select **Build** → **Customize** → **Call Center** → **Call Centers** from the left pane.

The screenshot shows the Salesforce interface with the left-hand navigation pane expanded to 'Build' → 'Customize' → 'Call Center'. The 'Call Center' sub-menu is open, showing options like 'Call Centers', 'Directory Numbers', and 'SoftPhone Layouts'. The main content area displays 'Recent Items', 'Quick Links' (Tools, Users, App, Security, Data), and 'Community' sections. The right-hand sidebar shows a 'Recommended Apps' section with 'Yesware - Tracking, Sync Sale...' highlighted.

The **Active Call Centers** screen is displayed next, showing a list of pre-configured call centers. Click on the **Edit** button associated with the relevant call center.

The screenshot shows the 'All Call Centers' screen in Salesforce. The left-hand navigation pane is expanded to 'Administer' → 'Manage Users'. The main content area displays a table of call centers. The table has columns for 'Action', 'Name', 'Version', 'Created Date', and 'Last Modified Date'. The first row shows 'Desktop Connect 1.4' with a version of '1.4', created on '01/12/2014 17:22', and last modified on '04/12/2014 11:09'. The 'Edit' button is visible next to the 'Name' column.

Action	Name	Version	Created Date	Last Modified Date
Edit Del	Desktop Connect 1.4	1.4	01/12/2014 17:22	04/12/2014 11:09

The **Call Center Edit** screen is displayed. 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 Desktop Connect 1.4

All Call Centers » Desktop Connect 1.4

Call Center Edit [Save] [Cancel]

General Information ! = Required Information

InternalNameAAA	DesktopConnect
Display Name	Desktop Connect 1.4
CTI Adapter URL	http://dc4cmsrv:8080/dc4cm
Use CTI API	true
Softphone Height	300
Softphone Width	200

Dialing Options

Outside Prefix	9
Long Distance Prefix	1
International Prefix	011
C2D enabled	true
Min Dom Phone Length	11
Internal Phone Length	5
UI Separator	
UI SF ID Position	4

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		no		down	0	0
2	6	no	aes_125_72	established	167	143

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 (not shown). 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 total number of monitored VDNs, skill groups, and logged in agents from **Section 3**, in this case “6”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Dec 16 10:48:32 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: 6.3.3.1.10-0
Server Date and Time: Tue Dec 16 11:07:42 MST 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

TSAPI Link Details

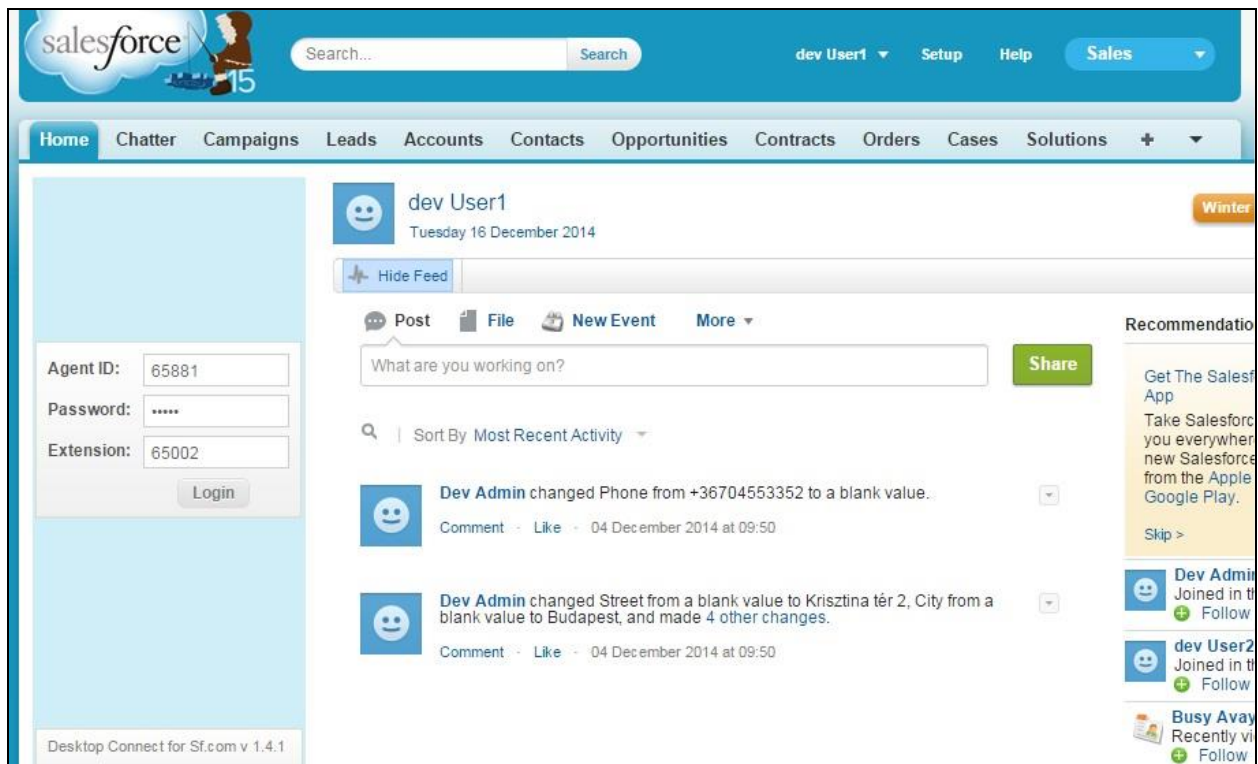
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	S8800	2	Talking	Wed Dec 3 11:19:36 2014	Online	16	6	143	167	30
<input type="radio"/>	2	S8300D	1	Switch Down	Thu Dec 4 15:11:15 2014	Online	16	0	0	0	30

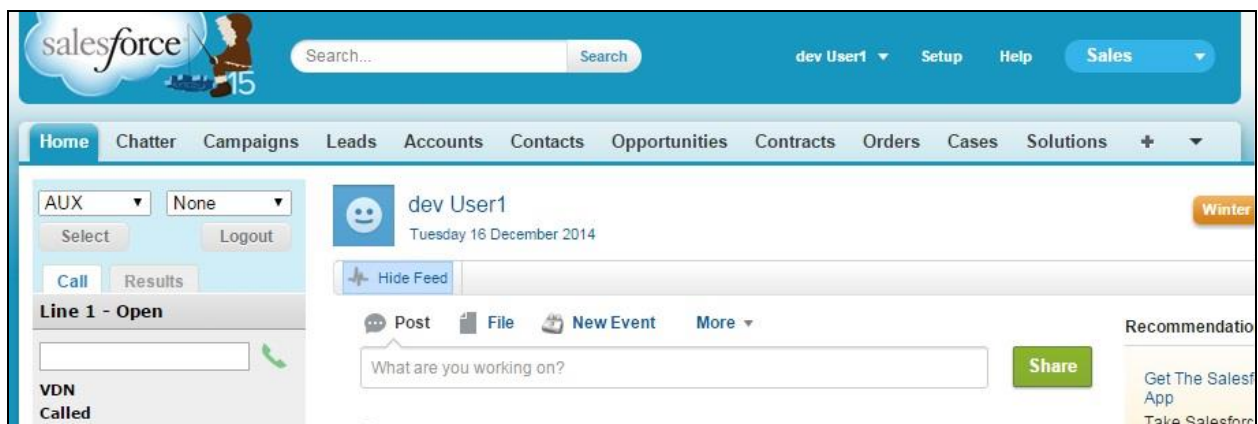
8.3. Verify Geomant Desktop Connect for Salesforce.com

From the agent PC, launch an Internet browser window and enter the same URL from **Section 7.2**. Log in with the relevant user credentials provided by the end customer.

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



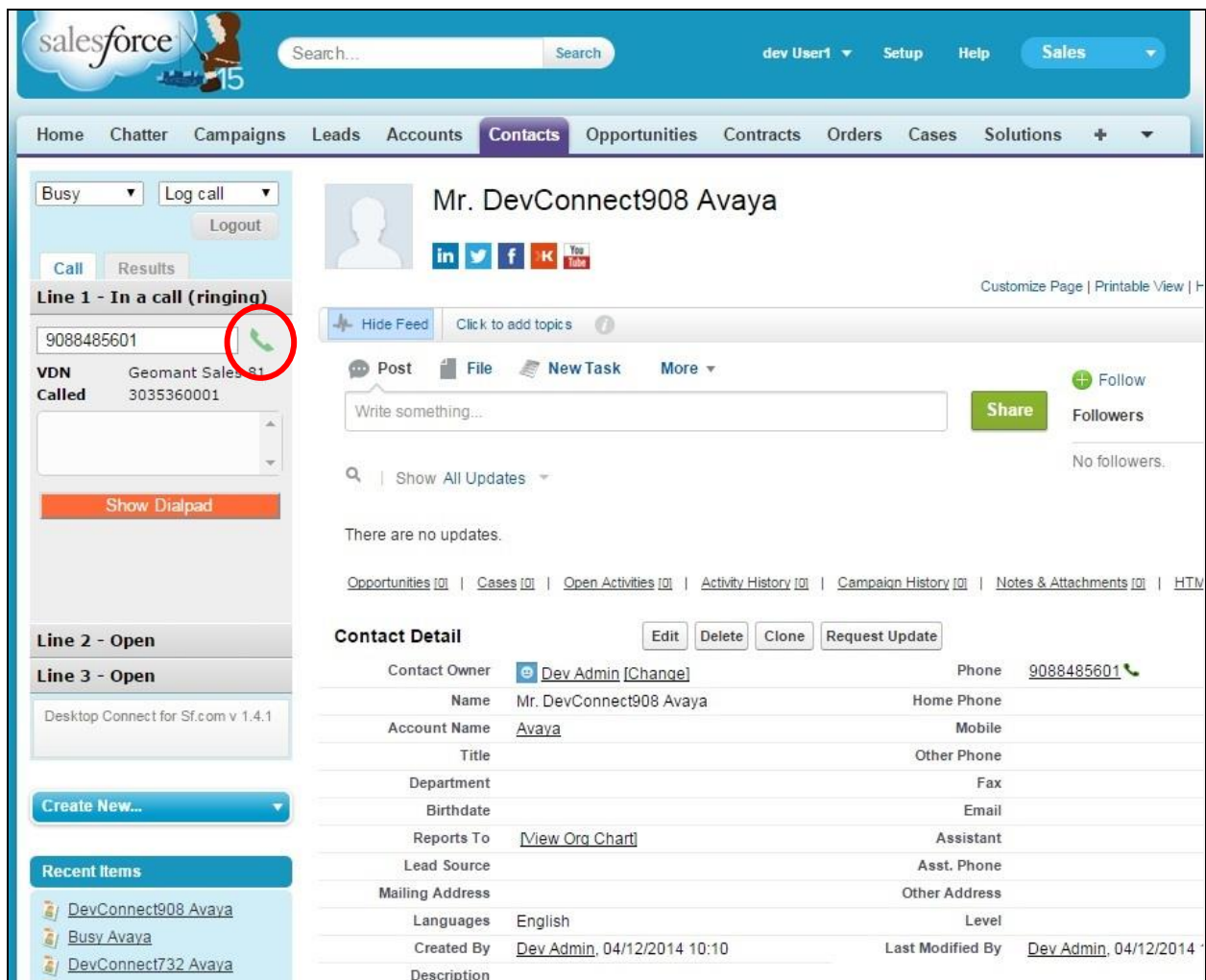
Verify that the left pane is updated showing agent state of “AUX”. Select the desired ready state from the **Agent State** drop-down list, such as “Auto-in”, followed by the **Select** button.



Verify that the left pane is updated showing agent state of “Auto-in”, as shown below.



Make an incoming ACD call. Verify that the matching contact record associated with the PSTN caller is automatically populated, with proper values in the relevant fields. Also verify that the left pane reflects **Busy** and **Line 1 – In a call (ringing)**, as shown below. Click on the answer icon to answer the call.



Verify that the agent is connected to the PSTN caller with two-way talk paths, and that the left pane is updated to reflect **Line 1 – In a call (talking)**, as shown below.

The screenshot shows the Salesforce interface for a contact named Mr. DevConnect908 Avaya. The left sidebar indicates the agent is in a call on Line 1. The main content area shows the contact's profile and a table of contact details.

Contact Detail	
Contact Owner	Dev Admin [Change]
Name	Mr. DevConnect908 Avaya
Account Name	Avaya
Title	
Department	
Birthdate	
Reports To	View Org Chart
Lead Source	
Mailing Address	
Languages	English
Created By	Dev Admin, 04/12/2014 10:10
Description	
Phone	9088485601
Home Phone	
Mobile	
Other Phone	
Fax	
Email	
Assistant	
Asst. Phone	
Other Address	
Level	
Last Modified By	Dev Admin, 04/12/2014

9. Conclusion

These Application Notes describe the configuration steps required for Geomant Desktop Connect for Salesforce.com 1.4.1 to successfully interoperate with Avaya Aura® Communication Manager 6.3.6 and Avaya Aura® Application Enablement Services 6.3.3. All feature and serviceability test cases were completed with observations 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 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *Desktop Connect for Salesforce.com Deployment and Configuration Guide*, Version 1.4, November 5, 2014, available as part of Desktop Connect ISO package.

©2015 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.