AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Geomant Desktop Connect for Salesforce.com 3.1 with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Geomant Desktop Connect for Salesforce.com 3.1 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1. 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.

SJW; Reviewed:
SPOC 1/30/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

1 of 30
Geo-SF-AES71

1. Introduction

These Application Notes describe the configuration steps required for Geomant Desktop Connect for Salesforce.com 3.1 to interoperate with Avaya Aura® Communication Manager 7.1 using Avaya Aura® Application Enablement Services 7.1. 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Desktop Connect for Salesforce did not include use of any specific encryption features as requested by Geomant.

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.

SJW; Reviewed:
SPOC 1/30/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
4 of 30
Geo-SF-AES71

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.
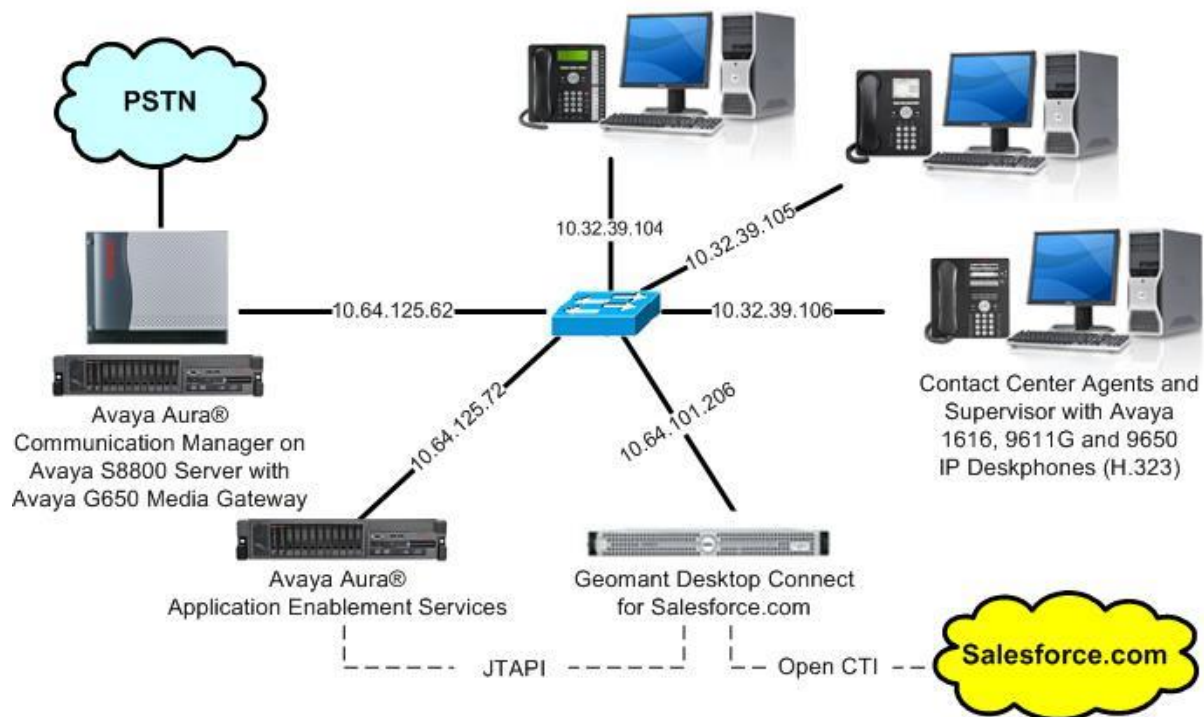
Figure 1: Compliance Testing Configuration

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 a VMware Virtual Machine	CM 7.1.1.0.0.532.23985 Kernel-3.10.0-693.e17.AVI Plat-rhel17.2-0010
Avaya G450 Media Gateway	38.20.1/1
Avaya Media Server	7.8.0.309
Avaya Aura® Application Enablement Services	7.1.0.0.0.17-0
Avaya 9611G IP Deskphone (H.323)	6.6229
Avaya 9641G IP Deskphone (H.323)	6.6229
Geomant Desktop Connect for Salesforce on Microsoft Windows Server 2012 R2 Standard • Avaya JTAPI Windows Client • Apache Tomcat 8.0 • Java SE Runtime Environment x64 1.8	3.1
• Salesforce CRM Classic and Lightning	2017 Winter
Microsoft Windows 10 Enterprise • Internet Explorer 10 • Edge 25+ • Chrome 33+ • Firefox 29+	1709

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


      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 **Welcome to OAM** screen is displayed next.
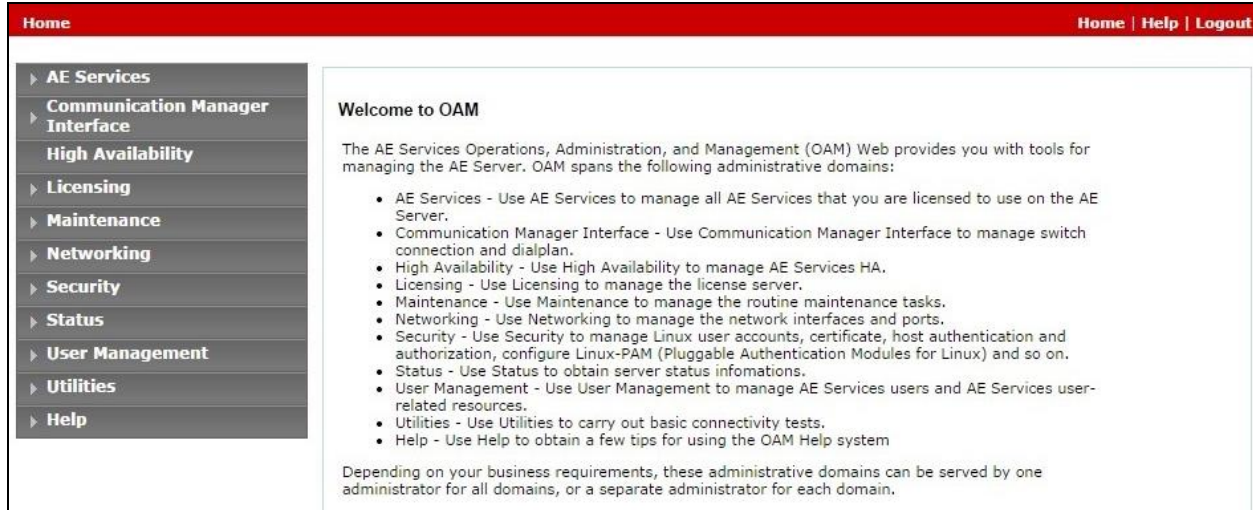
6.2. Verify License

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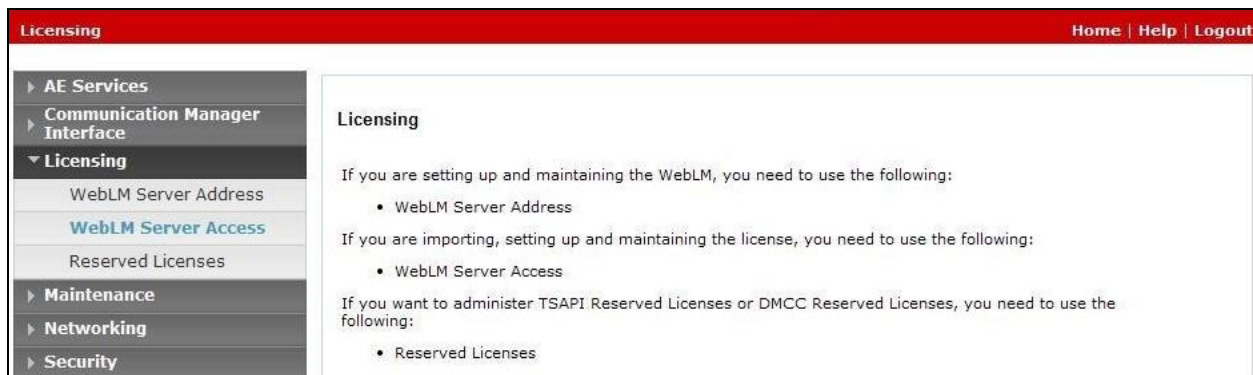
The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

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 **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.

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.

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**.

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.
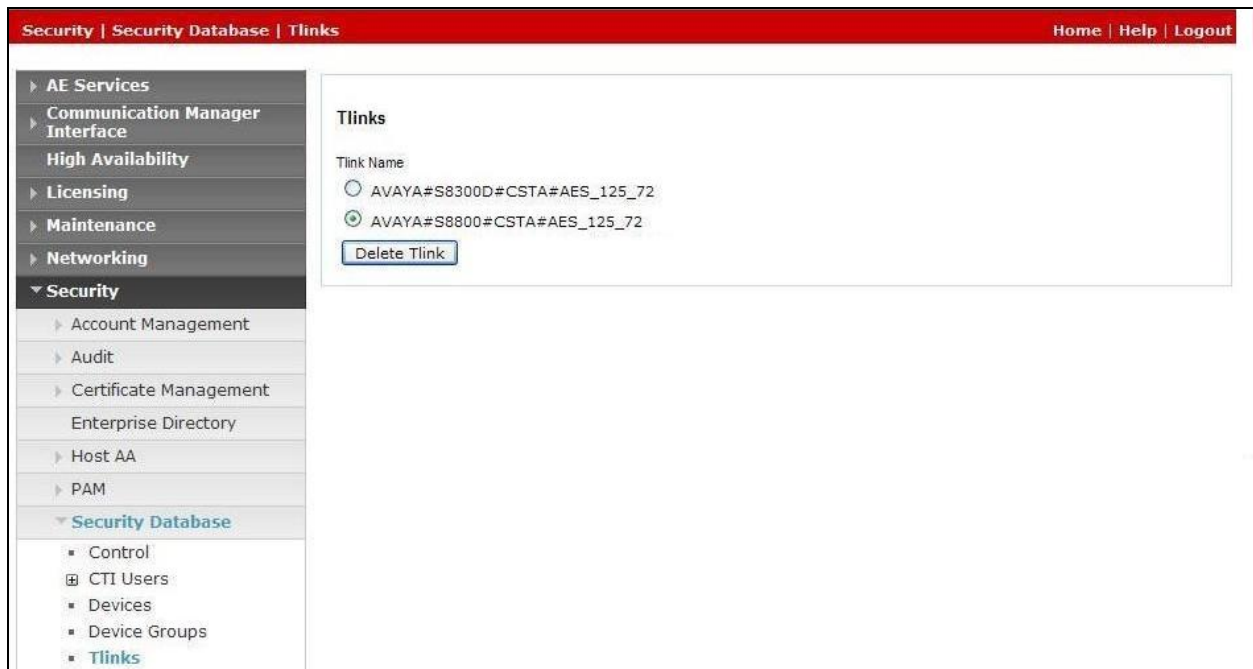
6.7. Administer Geomant User

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.

SJW; Reviewed:
SPOC 1/30/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

18 of 30
Geo-SF-AES71

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
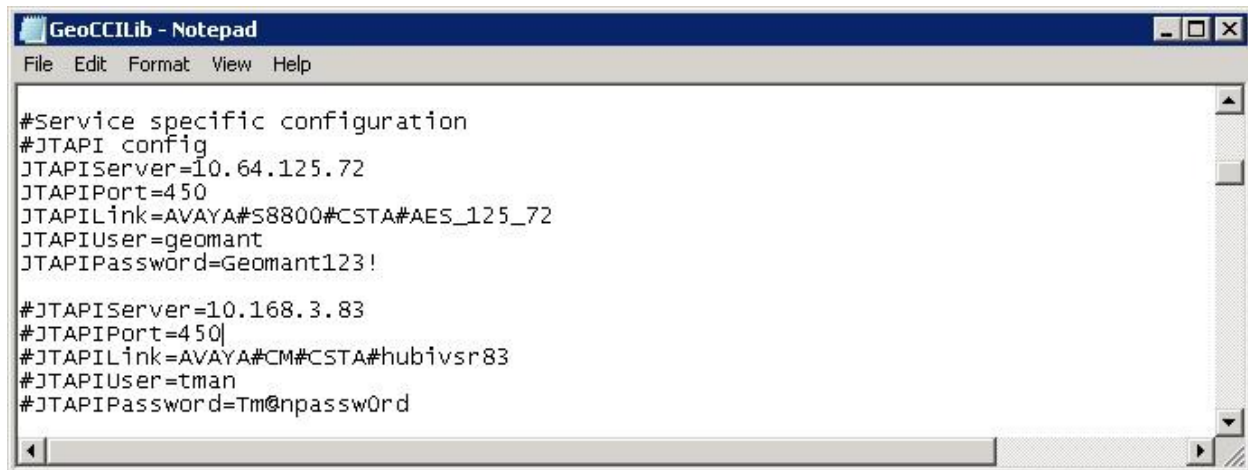
7.1. Administer GeoCCILib

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.
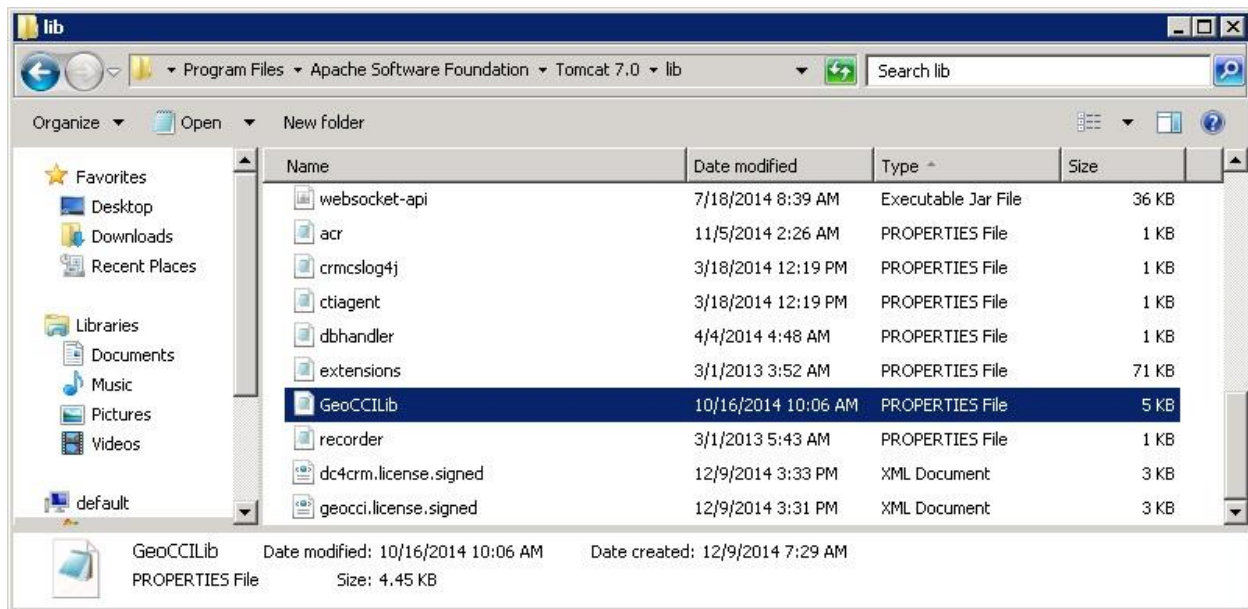
Open the **GeoCCILib** file with the Notepad application. Enter the following values for the specified fields, and retain the default values for the remaining fields.
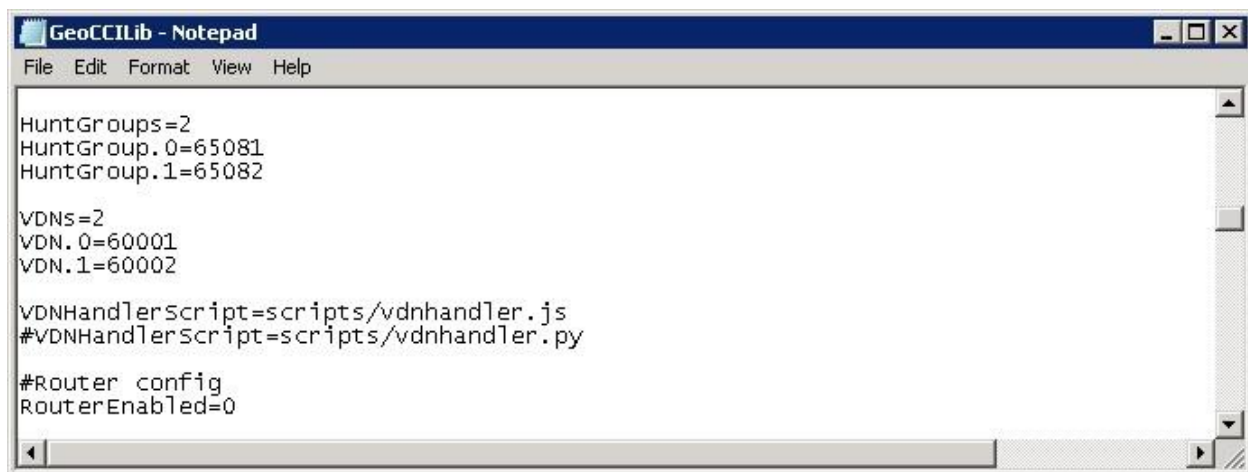
- **JTAPIServer:** IP address of Application Enablement Services.
- **JTAPILink:** The Tlink name from **Section 6.6**.
- **JTAPIUser:** The Geomant user credentials from **Section 6.7**.
- **JTAPIPassword:** The Geomant user credentials from **Section 6.7**.

```
#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 tested 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. Install Managed Package

Desktop Connect for Salesforce 3.1 installs various custom objects and adds custom fields to the Task object. It is permitted to develop workflows and APEX triggers using these custom objects and fields, but unless specifically agreed upon, Geomant is not responsible for the maintenance or correctness of custom code outside the package. It is recommended to notify Geomant before developing such extensions.

The managed package can be installed by accessing the download URL:
https://login.salesforce.com/packaging/installPackage.apexp?p0=04tb00000001YTx

Managed package adds the following objects to Salesforce.com
- Call Center definition required by Desktop Connect for Salesforce.com
- Custom fields required in the phone call activity to store CTI information
- Custom fields required to store the recording playback URL

Package installation requires a Salesforce.com login to access the App Exchange.

On the package install landing page review the package details:
- App Name: Desktop Connect
- Publisher: Geomant
- Version Name: DC4CRM 3.1
- Version Number: 3.3
- View Components: Details the fields and resources that will be added to your Salesforce.com instance
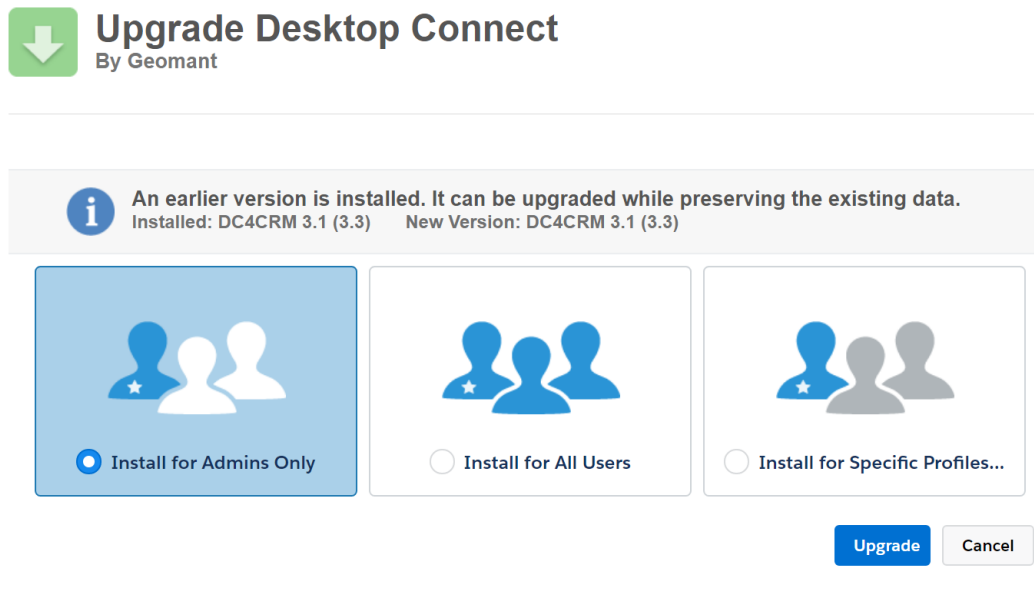
Select **Install for All Users** option as shown on the following screen, and proceed with the installation.

SJW; Reviewed:
SPOC 1/30/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
21 of 30
Geo-SF-AES71

7.3. 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.
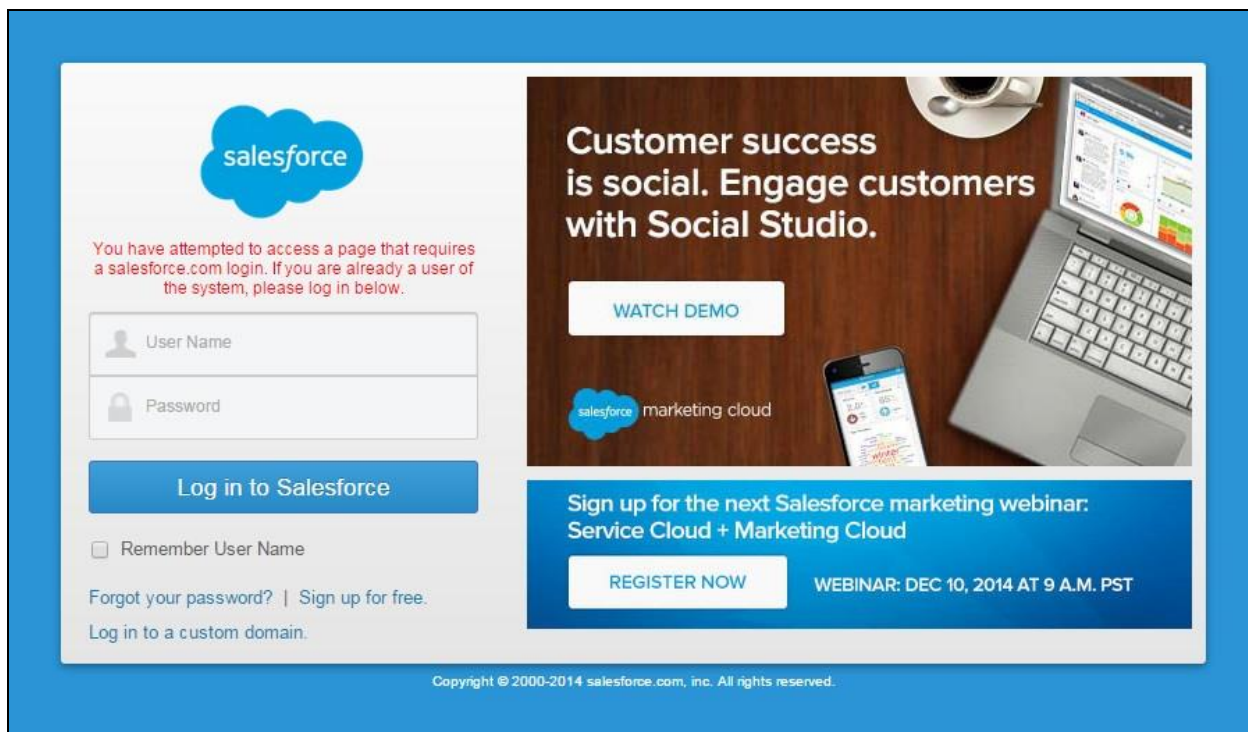
In the subsequent screen, click **Setup** as shown below.
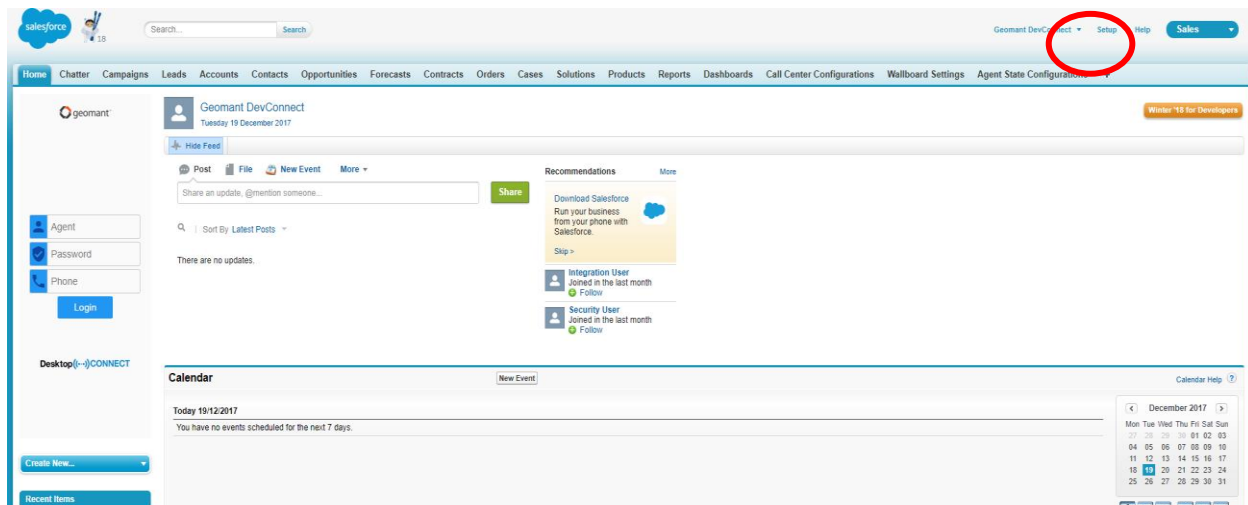
Scroll the screen as necessary, and select **Build → Customize → Call Center → Call Centers** from the left pane.

The **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.

SJW; Reviewed:
SPOC 1/30/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

23 of 30
Geo-SF-AES71

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,
- **Aux code Labels:**   The aux work reason code values from **Section 5.4**.

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    Version  Mnt   AE Services        Service      Msgs    Msgs
Link            Busy  Server             State        Sent    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, in this case "6".

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 7.3**. Log in with the relevant user credentials provided by the end customer.
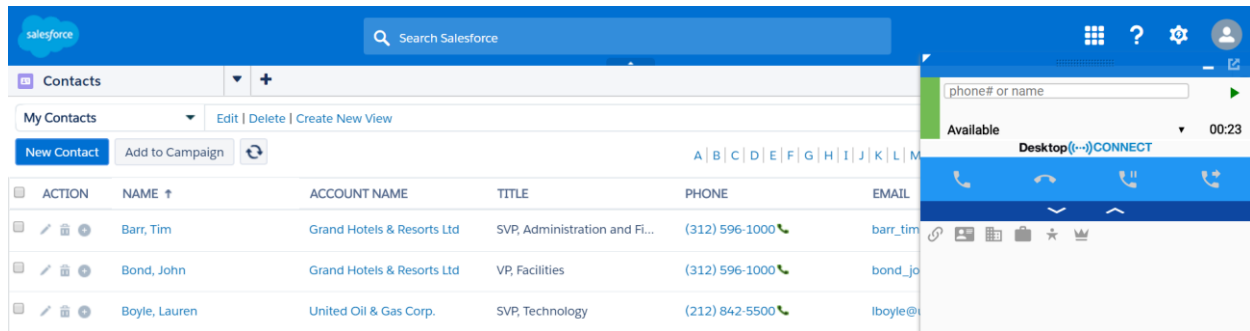
In the left pane, enter the relevant **Agent ID**, agent **Password**, and station **Extension** from **Section 3**, as shown below. Click **Login**.
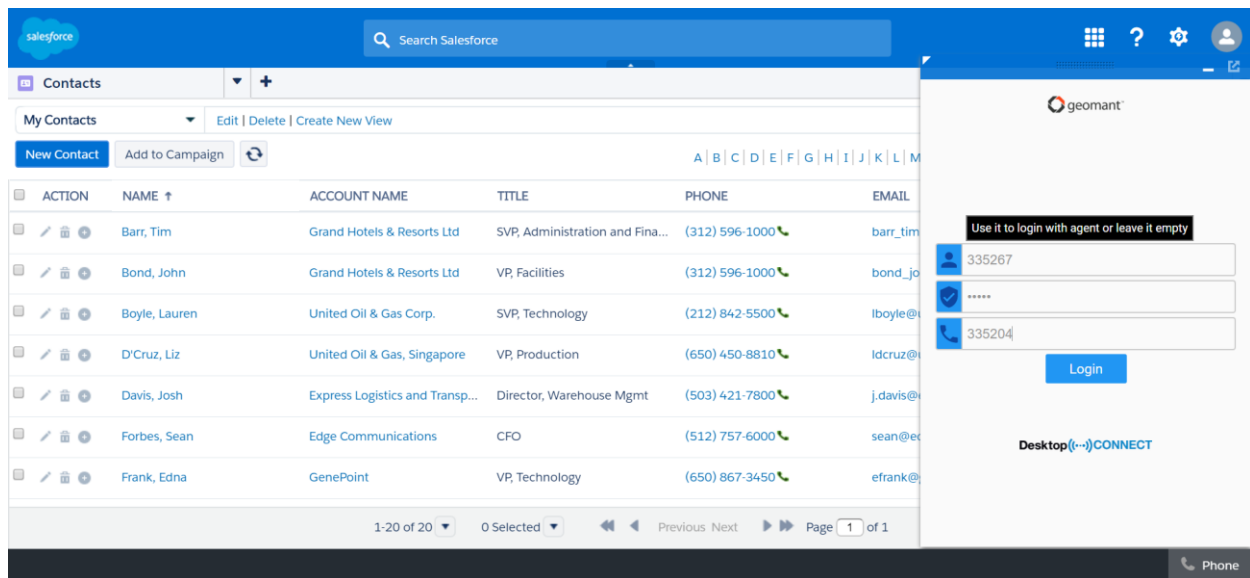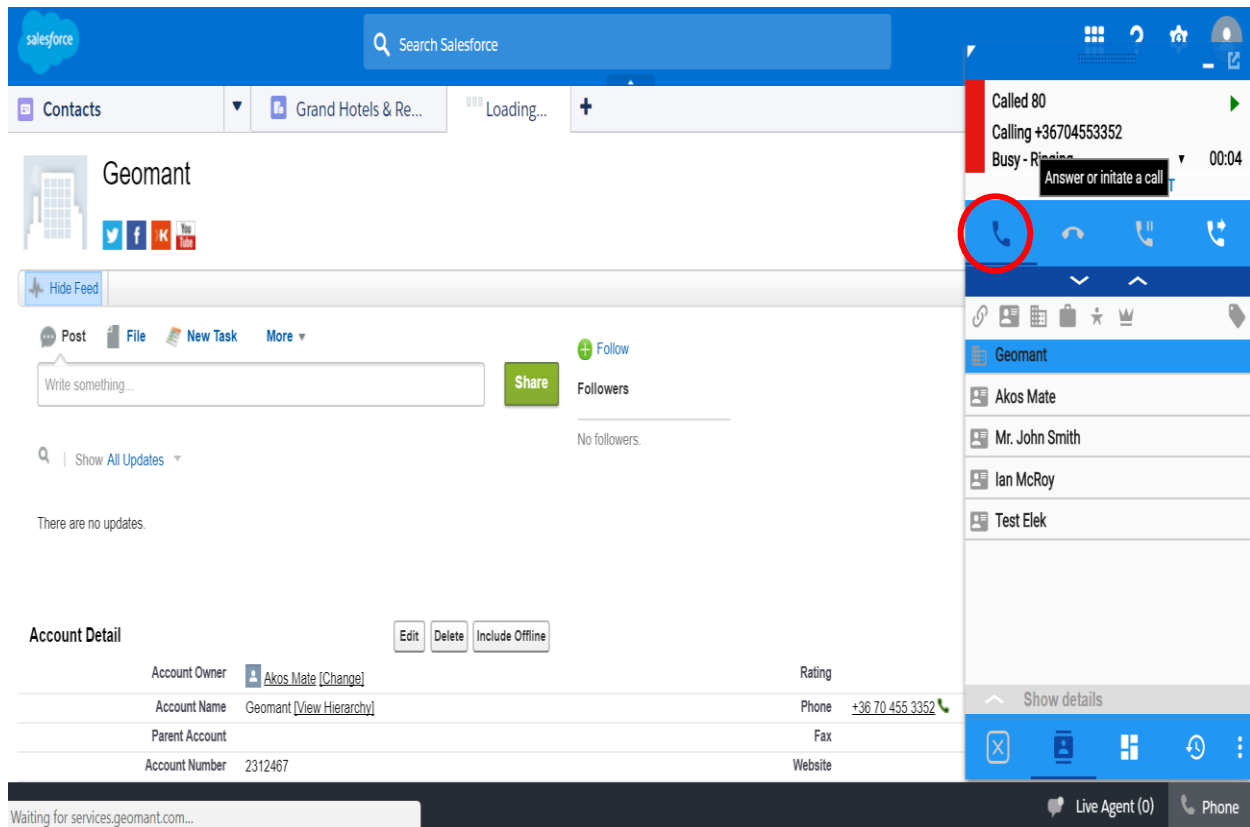

Verify that the left pane is updated showing agent state of "Default". Select the desired ready state from the **Agent State** drop-down list, such as "Available".
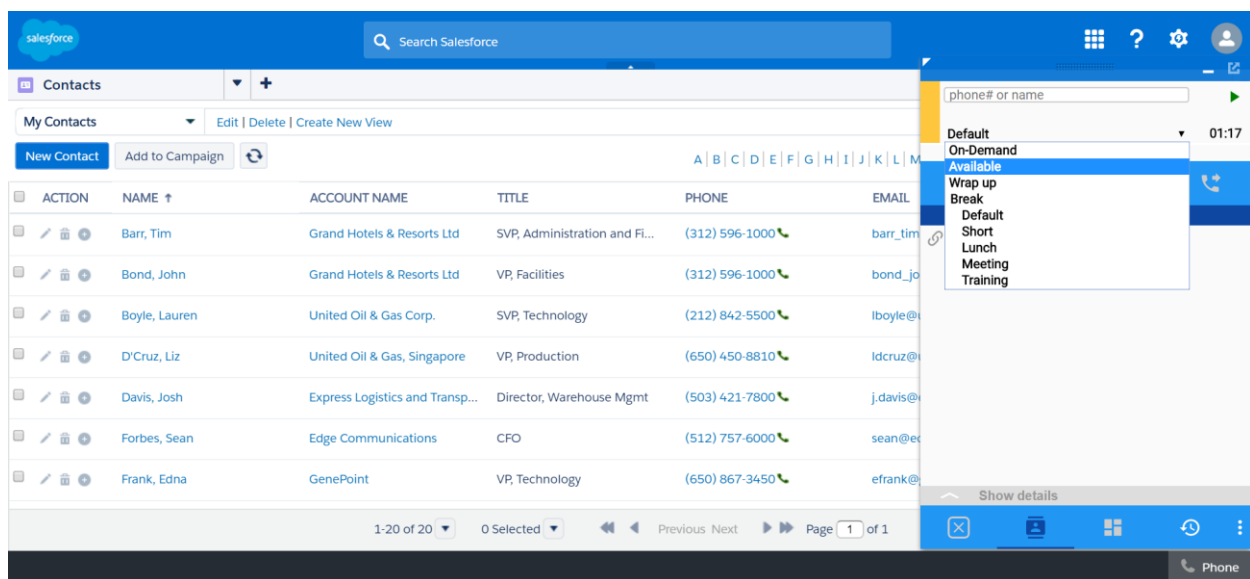
Verify that the left pane is updated showing agent state of "Available", as shown below.

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.

9. Conclusion

These Application Notes describe the configuration steps required for Geomant Desktop Connect for Salesforce.com 3.1 to successfully interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1. 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 71, June 2017 available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.1, 02-300357, June 2017, available at http://support.avaya.com.

3. *Desktop Connect for Salesforce.com Deployment and Configuration Guide*, Version 3.1, September 14, 2017, available as part of Desktop Connect Knowledge Base http://kb.geomant.com/display/DC31.