



Application Notes for Geomant Desktop Connect Unified Agent 2.6.8 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 Unified Agent 2.6.8 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1. Geomant Desktop Connect Unified Agent provides an Agent Desktop that links to Avaya Aura® Communication Manager via Avaya Aura® Application Services.

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 Unified Agent 2.6.8 to interoperate with Avaya Aura® Communication Manager 7.1 using Avaya Aura® Application Enablement Services 7.1. Geomant Desktop Connect Unified Desktop is an agent desktop that connects to Avaya Aura® Communication Manager.

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 Unified Agent 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.

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 Communication Manager. 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 Unified Agent 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 the PSTN caller information, whereas the destination agent for conference scenarios will not.
- 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 the 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 agent desktops were installed with the relevant browser plug-in for integration with Desktop Connect.

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.

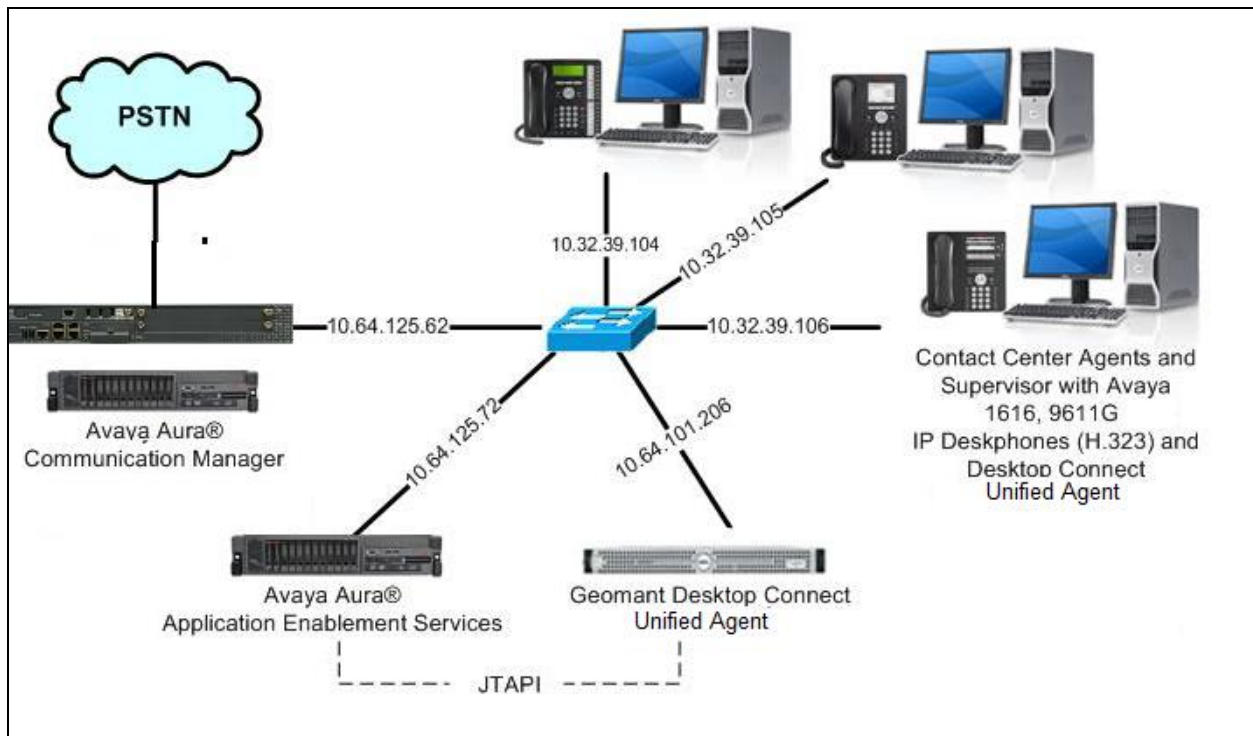


Figure 1: Compliance Testing Configuration

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 Unified Agent on Microsoft Windows Server 2012 R2 Standard <ul style="list-style-type: none">• Avaya JTAPI Windows Client• Apache Tomcat 8.0• Java JRE 1.8	2.6.8

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/		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

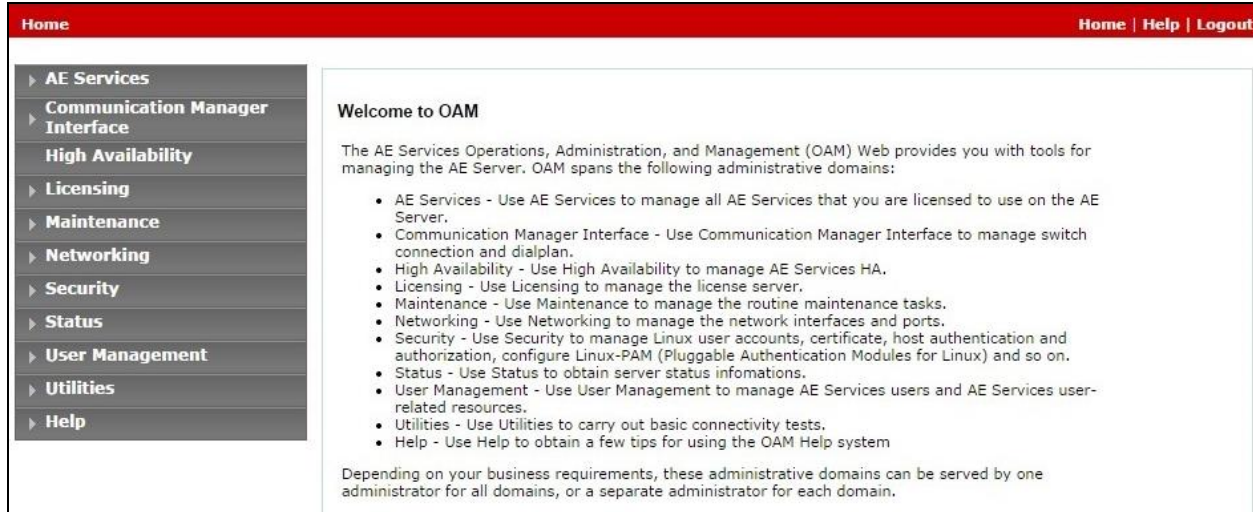
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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



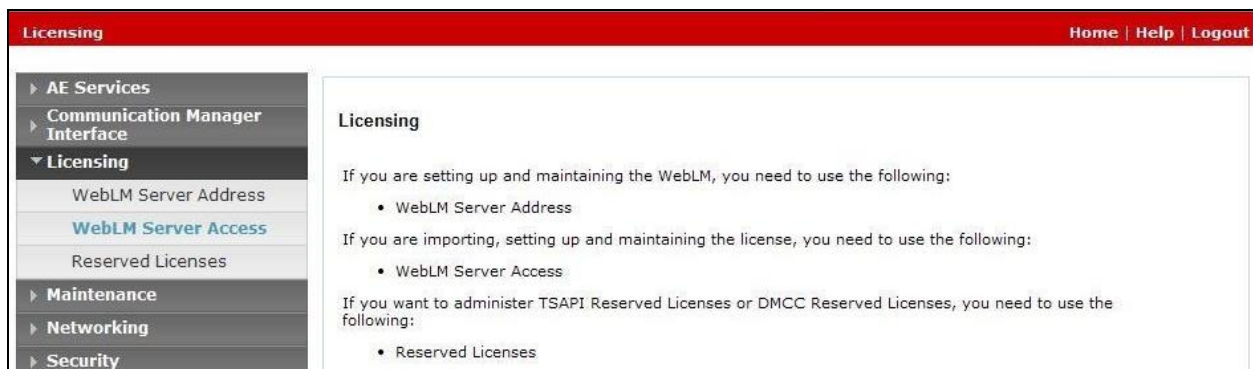
The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page, there is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button.

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.

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) - 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_1 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, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_0 AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestrict 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		

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 'TSAPI Links' management console. The left sidebar contains a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links' (selected), and 'TSAPI Properties'. The main content area is titled 'TSAPI Links' and features a table with columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the table are three buttons: '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' configuration screen. The left sidebar is similar to the previous screen, but 'Communication Manager Interface' is also visible under 'TSAPI'. The main content area is titled 'Add TSAPI Links' and contains five fields with dropdown menus: 'Link' (set to 1), 'Switch Connection' (set to S8800), 'Switch CTI Link Number' (set to 2), 'ASAI Link Version' (set to 6), and 'Security' (set to Unencrypted). At the bottom are two buttons: '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.



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**.



The screenshot shows a web interface for the Service Controller. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (expanded), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, Status, and User Management. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists five services: ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, and Transport Layer Service, all with a status of 'Running'. The 'TSAPI Service' is checked with a green box. Below the table, there is a link to 'Status and Control' and a row of 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

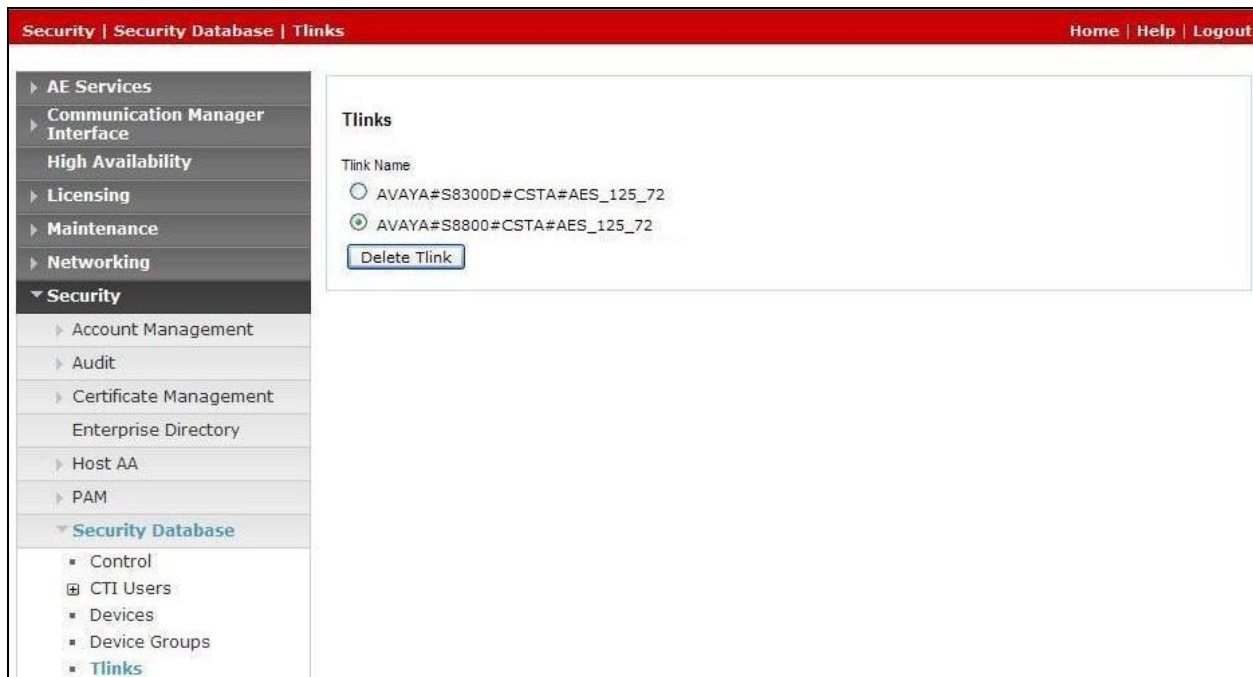
For status on actual services, please use [Status and Control](#)

[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#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.

The screenshot shows the 'Add User' form within the Avaya User Management interface. The left sidebar contains a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. Under 'User Management', 'User Admin' is expanded, showing 'Add User' as the selected option. The main content area is titled 'Add User' and includes a note: 'Fields marked with * can not be empty.' The form contains the following fields: * User Id (text input, value: geomant), * Common Name (text input, value: geomant), * Surname (text input, value: geomant), * User Password (password input, value: masked with dots), * Confirm Password (password input, value: masked with dots), Admin Note (text input), Avaya Role (dropdown menu, value: None), Business Category (text input), Car License (text input), CM Home (text input), Cms Home (text input), CT User (dropdown menu, value: Yes), Department Number (text input), Display Name (text input), Employee Number (text input), Employee Type (text input), Enterprise Handle (text input), and Given Name (text input). The top of the interface has a red header bar with 'User Management | User Admin | Add User' and 'Home | Help | Logout' links.

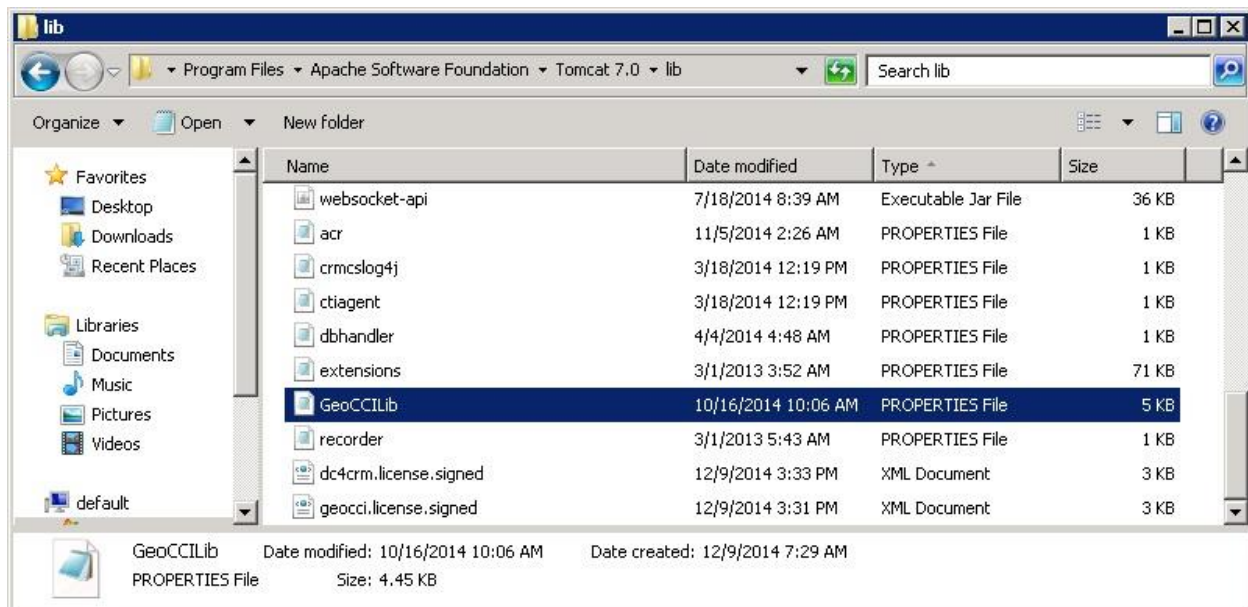
7. Configure Geomant Desktop Connect Unified Agent

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

- Administer GeoCCILib
- Administer call center

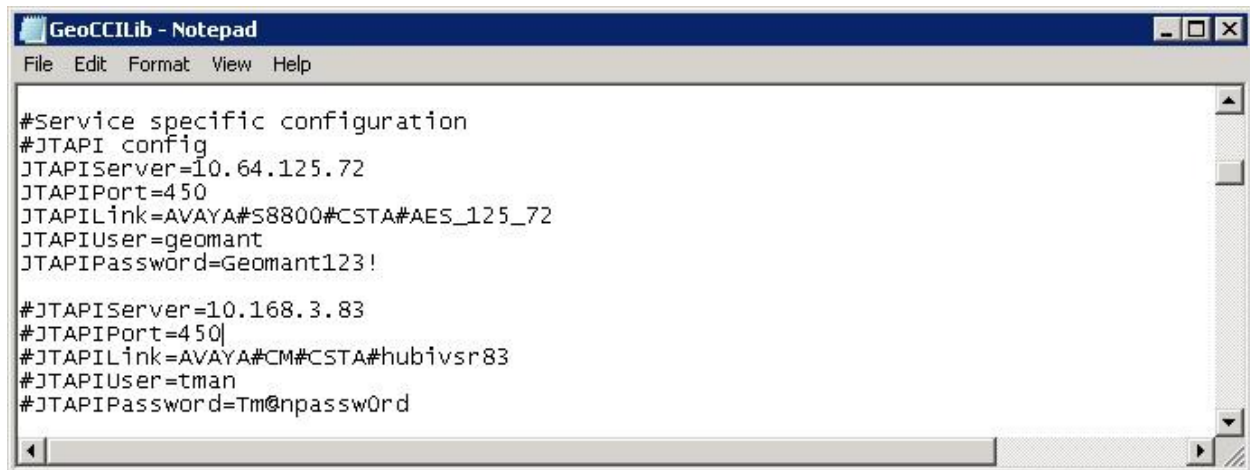
7.1. Administer GeoCCILib

From the Desktop Connect server, navigate to the **C:\Program Files\Apache Software Foundation\Tomcat 8.0\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.

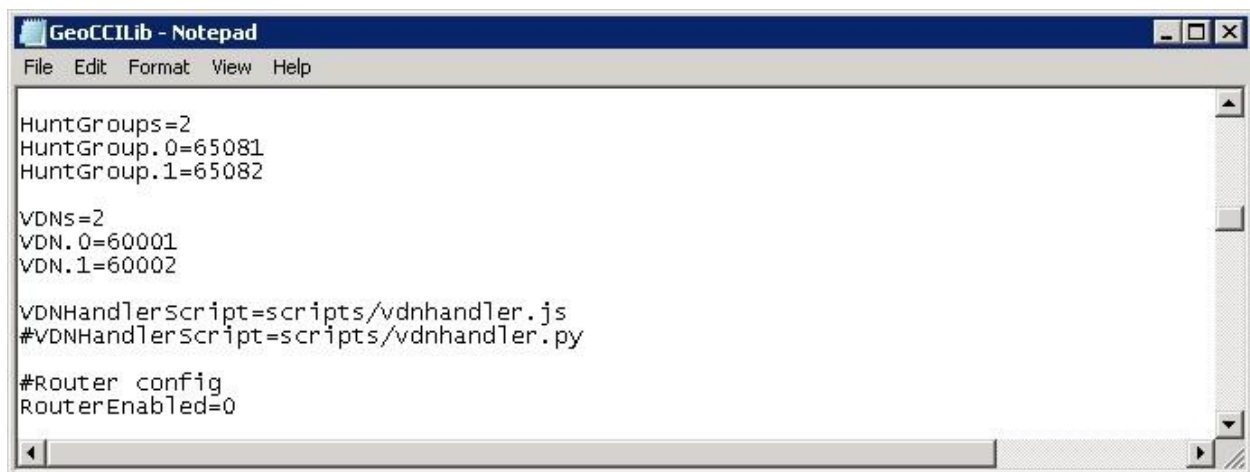
- **JTAPIServer:** IP address of Application Enablement Services.
- **JTAPILink:** The Tlink name from **Section 6.6**.
- **JTAPIUser:** The Geomant user credentials from **Section 6.7**.
- **JTAPIPassword:** The Geomant user credentials from **Section 6.7**.



```
#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 used for testing 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
```

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	101	98

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”.

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	98	101	30
<input type="radio"/>	2	S8300D	1	Switch Down	Thu Dec 4 15:11:15 2014	Online	16	0	0	0	30

Online

Offline

8.3. Verify Geomant Desktop Connect Unified Agent

From the agent PC, launch an Internet browser window and enter the Unified Agent URL and Log in with the relevant user credentials provided by the end customer.

9. Conclusion

These Application Notes describe the configuration steps required for Geomant Desktop Connect Unified Agent 2.6.8 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 7.1, 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 Unified Agent - Deployment and Configuration Guide*, Version 2.6.8, available as part of Desktop Connect Unified Agent Knowledge Base <http://kb.geomant.com/display/DC31/Desktop+Connect+v3.1>.

©2018 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.