



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Pegasystems Chordiant Foundation Server with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Pegasystems Chordiant Foundation Server to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Pegasystems Chordiant Foundation Server is a customer data and processes management solution.

In the compliance testing, Pegasystems Chordiant Foundation Server used the Java Telephony Application Programming Interface from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and provide screen pops and call control via a thin client web-based agent application.

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 Pegasystems Chordiant Foundation Server to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Pegasystems Chordiant Foundation Server is a customer data and processes management solution.

In the compliance testing, Pegasystems Chordiant Foundation Server used the Java Telephony Application Programming Interface (JTAPI) from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and provide screen pops and call control via a thin client 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.

The compliance test covered the default out-of-the-box Chordiant Unified Desktop, which is a thin client web-based agent application provided by Pegasystems Chordiant Foundation Server. Note that any customized application developed using Pegasystems Chordiant Foundation Server will require separate compliance test.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming calls were placed to the VDNs with available agents running Chordiant Unified Desktop. Manual call controls from the application were exercised to verify proper call handling such as transfer and conference.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cables to Chordiant Foundation Server and to Chordiant Unified Desktop.

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 Chordiant Foundation Server:

- Handling of JTAPI/TSAPI messages in the areas of event notifications, value queries, and set agent states.
- Use of JTAPI/TSAPI call control services to support call control actions such as answer and transfer from the agent desktops.
- Proper handling of call scenarios involving inbound, outbound, ACD, non-ACD, drop, transfer, conference, and multiple agents.

The serviceability testing focused on verifying the ability of the Chordiant Foundation Server to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cables to Chordiant Foundation Server and to Chordiant Unified Desktop.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Chordiant Foundation Server from the compliance testing.

- After dropping from a conference call, the information pertaining to the previous call such as calling and called number may not clear on the agent screen until delivery of the next call, and the timer and customer information may not clear until the end of the next call.
- The application does not support call control actions from the hard phone.
- After the agent transfers an outbound call, the next outbound call can be initiated but will not be reflected on the data screen.
- A separate JTAPI/TSAPI session is established for each agent.
- Negative responses from agent log in attempts, such as agent already logged in and invalid credentials are not reflected on the data screen.
- A TSAPI user credential containing the semicolon character is not supported.
- After a link disruption, agents will receive a pop-up error when trying to use the desktop to control calls established prior to link recovery, and will need to perform a manual recovery. The recovery steps are for the agents to exit from the Chordiant Unified Desktop application manually, use the telephone to log out of the ACD, and to re-launch Chordiant Unified Desktop.

## 2.3. Support

Technical support on Chordiant Foundation Server can be obtained through the following:

- **Phone:** (617) 374-9600
- **Email:** support@chordiant.com
- **Web:** <https://mesh.pega.com>

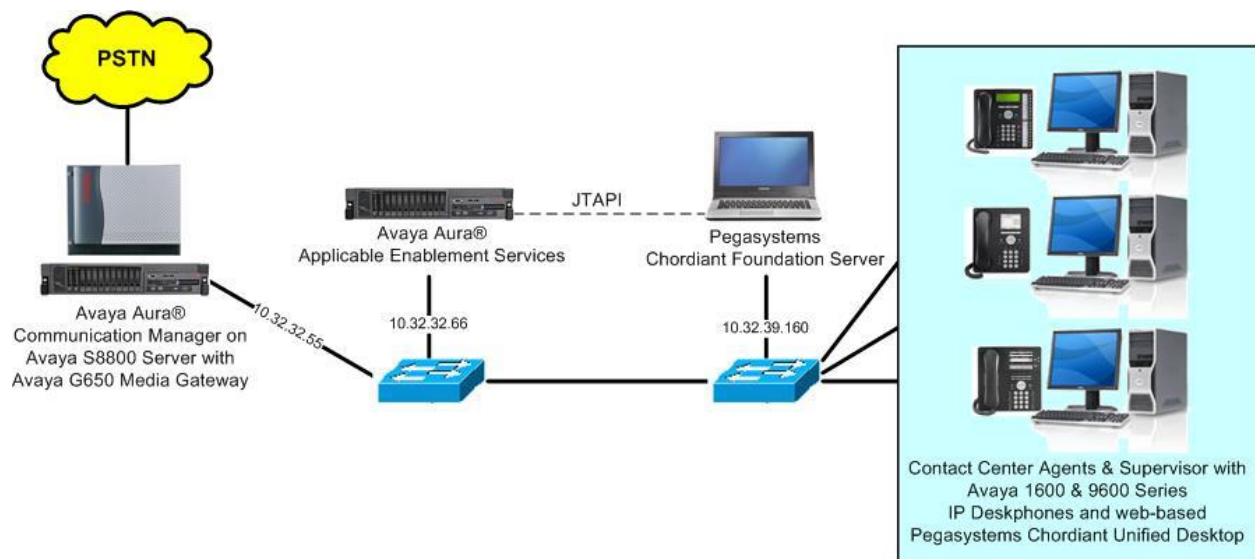
### 3. Reference Configuration

Chordiant Foundation Server can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server configuration.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Chordiant Foundation Server monitored the supervisor and agent station extensions shown in the table below.

Device Type	Extension
VDN	62005, 62006
Skill Group	65555, 65556
Agent Station	65001, 65002
Supervisor Station	65003
Agent ID	65881, 65882, 65883



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP8 (R016x.00.1.510.1-19736)
Avaya G650 Media Gateway <ul style="list-style-type: none"><li>• TN799DP C-LAN Circuit Pack</li><li>• TN2302AP IP Media Processor</li></ul>	HW01 FW040 HW12 FW121
Avaya Aura® Application Enablement Services	6.1.2
Avaya 1616 IP Deskphone (H.323)	1.302S
Avaya 9611G IP Deskphone (H.323)	6.020S
Avaya 9650 IP Deskphone (H.323)	3.1000
Pegasystems Chordiant Foundation Server on Windows 7 Enterprise <ul style="list-style-type: none"><li>• Avaya JTAPI Client (ecsjtapia.jar)</li><li>• BEA WebLogic</li><li>• Oracle</li></ul>	6.7.0 2009 SP1 5.2.0.483 10.3.5 11gR2
Pegasystems Chordiant Unified Desktop	6.7.0

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Obtain agent ID passwords

### 5.1. Verify License

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

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y	
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y	
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y	
ATMS?	y			
Attendant Vectoring?	y			

### 5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page	1 of	3
CTI LINK				
CTI Link: 1				
<b>Extension: 60100</b>				
<b>Type: ADJ-IP</b>				
COR: 1				
<b>Name: TSAPI Link</b>				

### 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 19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name: S8500-SAL
      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

MALICIOUS CALL TRACE PARAMETERS
      Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
      Delay Sending RElease (seconds): 0

SEND ALL CALLS OPTIONS
      Send All Calls Applies to: station      Auto Inspect on Send All Calls? n
      Preserve previous AUX Work button states after deactivation? n

UNIVERSAL CALL ID
      Create Universal Call ID (UCID)? y      UCID Network Node ID: 1
```

### 5.4. Obtain Agent ID Passwords

Use the “display agent-loginID n” command, where “n” is the first agent ID extension from **Section 3**. Make a note of the value in the **Password** field, which will be used later to configure Chordiant Foundation Server.

Repeat this section to obtain the agent ID password for all agent ID extensions in **Section 3**.

```
display agent-loginID 65881                                     Page 1 of 3
                        AGENT LOGINID

      Login ID: 65881                                AAS? n
      Name: VPI Agent 65881                            AUDIX? n
      TN: 1                                           LWC Reception: spe
      COR: 1                                           LWC Log External Calls? n
      Coverage Path:                                AUDIX Name for Messaging:
      Security Code:

                                LoginID for ISDN/SIP Display? n
                                Password: 65881
                                Password (enter again): 65881
                                Auto Answer: none
                                MIA Across Skills: system
                                ACW Agent Considered Idle: system
                                Aux Work Reason Code Type: system
                                Logout Reason Code Type: system
                                Maximum time agent in ACW before logout (sec): system
                                Forced Agent Logout Time:      :

WARNING: Agent must log in again before changes take effect
```



## 6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Verify license
- Launch OAM interface
- Administer TSAPI link
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Chordiant user

### 6.1. Verify License


Access the Web License Manager interface by using the URL “https://ip-address:52233/WebLM/ index.jsp” in an Internet browser window, where “ip-address” is the IP address of the license server.

The **Web License Manager** screen is displayed. Log in using the appropriate credentials.

The image shows the Avaya Web License Manager (WebLM v4.6) login interface. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Web License Manager (WebLM v4.6)". The main heading is "Logon". There are two input fields: "User Name:" and "Password:". To the right of the "Password:" field is a dark gray button with a white right-pointing arrow.

The **Web License Manager** screen below is displayed. Select **Licensed Products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

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


Web License Manager (WebLM v4.6)
Logoff

Install License

**Licensed Products**

  APPL\_ENAB

    Application\_Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

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

You are here: Licensed products > Application Enablement (CTI)

License installed on: Dec 6, 2011 5:02:20 PM EST

[View Peak Usage](#)

**Licensed Features**

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2012/12/06	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2012/12/06	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2012/12/06	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2012/12/06	16	0
Product Notes (VALUE_NOTES)	2012/12/06	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; IXP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; IXM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	2012/12/06	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2012/12/06	1000	0
DLG (VALUE_AES_DLG)	2012/12/06	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2012/12/06	1000	1
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2012/12/06	3	0

## 6.2. 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 logo on the left and the title "Application Enablement Services Management Console" in the center. Below the title is a red horizontal bar. In the center of the page is a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below these fields is a "Login" button. At the bottom of the page, below another red horizontal bar, is the copyright notice: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya logo on the left and the title "Application Enablement Services Management Console" in the center. In the top right corner, there is a welcome message: "Welcome: User", "Last login: Wed Aug 8 12:04:10 2012 from 10.32.39.20", "HostName/IP: AES2-S8800/10.32.32.66", "Server Offer Type: VIRTUAL\_APPLIANCE", and "SW Version: r6-1-2-32-0". Below the title is a red horizontal bar with the text "Home" on the left and "Home | Help | Logout" on the right. On the left side of the page is a vertical menu with the following items: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area on the right is titled "Welcome to OAM" and contains the following text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their functions. At the bottom of the main content area, there is a paragraph: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain."

Welcome: User  
Last login: Wed Aug 8 12:04:10 2012 from 10.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-2-32-0

Home | Help | Logout

Home

AE Services  
Communication Manager Interface  
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.
- 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 both domains, or a separate administrator for each domain.

### 6.3. Administer TSAPI Link

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

The screenshot shows the AVAYA Application Enablement Services Management Console. The top navigation bar includes the AVAYA logo, the title "Application Enablement Services Management Console", and a welcome message: "Welcome: User", "Last login: Wed Aug 8 12:04:10 2012 from 10.32.39.20", "HostName/IP: AES2-S8800/10.32.32.66", "Server Offer Type: VIRTUAL\_APPLIANCE", and "SW Version: r6-1-2-32-0". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links" (selected), and "TSAPI Properties". The main content area is titled "TSAPI Links" and contains 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, and click **Apply Changes**.

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (value: 1), "Switch Connection" (value: S8800), "Switch CTI Link Number" (value: 1), "ASAI Link Version" (value: 4), and "Security" (value: Unencrypted). Below the form 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, and click **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two unchecked checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services'. Below these is an 'Apply Changes' button. The top right corner displays user information: 'Welcome: User', 'Last login: Wed Aug 8 12:04:10 2012 from 10.32.39.20', 'HostName/IP: AES2-S8800/10.32.32.66', 'Server Offer Type: VIRTUAL\_APPLIANCE', and 'SW Version: r6-1-2-32-0'. The top navigation bar shows 'Security | Security Database | Control' and links for 'Home | Help | Logout'.

## 6.5. Restart TSAPI Service

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked and 'Running'. Below the table is a link for 'Status and Control' and a row of buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right corner displays the same user information as the previous screenshot. The top navigation bar shows 'Maintenance | Service Controller' and links for 'Home | Help | Logout'.

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

## 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 Chordiant Foundation Server.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES2-S8800”. 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 main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security Database" expanded to show "Tlinks". The main content area, titled "Tlinks", lists a single Tlink named "AVAYA#S8800#CSTA#AES2-S8800" with a "Delete Tlink" button next to it.

**AVAYA** Application Enablement Services Management Console

Welcome: User  
Last login: Wed Aug 8 12:04:10 2012 from 10.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-2-32-0

Security | Security Database | Tlinks Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ Security Database
    - Control
    - ▣ CTI Users
    - Devices
    - Device Groups
    - **Tlinks**

**Tlinks**

Tlink Name

- AVAYA#S8800#CSTA#AES2-S8800

Delete Tlink

## 6.7. Administer Chordiant 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. Click **Apply** at the bottom of the screen (not shown 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: 'Welcome: User', 'Last login: Wed Aug 8 12:04:10 2012 from 10.32.39.20', 'HostName/IP: AES2-S8800/10.32.32.66', 'Server Offer Type: VIRTUAL\_APPLIANCE', and 'SW Version: r6-1-2-32-0'. Below the header is a red navigation bar with 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'. The left sidebar contains a tree view with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under 'User Admin', the 'Add User' option is selected. The main content area shows the 'Add User' form with the following fields: \* User Id (text input, value: chordiant), \* Common Name (text input, value: chordiant), \* Surname (text input, value: chordiant), \* User Password (password input, masked with dots), \* Confirm Password (password input, 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), and Employee Number (text input). A note at the top of the form states: 'Fields marked with \* can not be empty.'

## 7. Configure Pegasystems Chordiant Foundation Server

This section provides the procedures for configuring Chordiant Foundation Server. The procedures include the following areas:

- Administer master.dtd
- Administer TSAPI.PRO
- Administer CTI.xml
- Launch application and web interface
- Administer CTI user accounts
- Administer ACD queues
- Administer station definitions

The configuration of Chordiant Foundation Server is performed by Pegasystems service personnel. The procedural steps are presented in these Application Notes for informational purposes.

Chordiant Foundation Server can be configured on a single server or with components distributed across multiple servers. The solution provides a customizable platform that uses the J2EE framework with either WebSphere or WebLogic as the application server, and either Oracle or DB2 as the database component. For ease of compliance testing, the configuration used a single server hosting all components including WebLogic and Oracle.

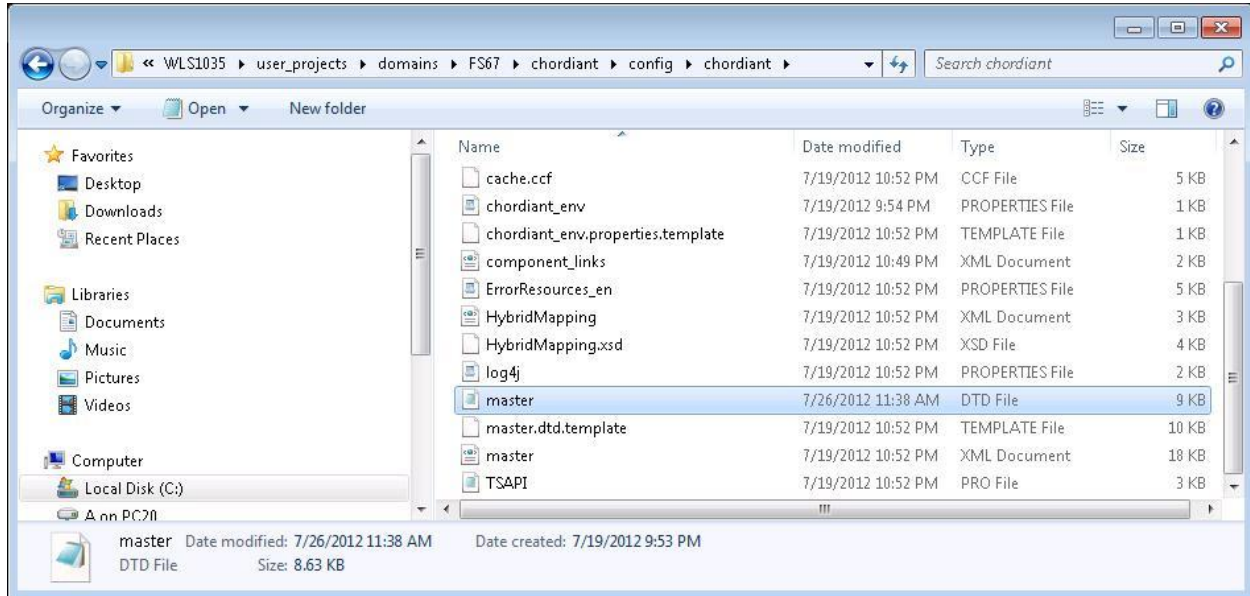
The compliance test covered the default out-of-the-box Chordiant Unified Desktop, which is a thin client web-based agent application provided by Pegasystems Chordiant Foundation Server. Note that any customized application developed using Pegasystems Chordiant Foundation Server will require separate compliance test.

The detailed administration of user profiles is not the focus of these Application Notes and will not be described. This section assumes the necessary user profiles have been pre-configured.



## 7.1. Administer master.dtd

From the Chordiant Foundation Server, navigate to the directory containing the **master.dtd** file, in this case **C:\WLS1035\user\_projects\domains\FS67\chordiant\config\chordiant**.

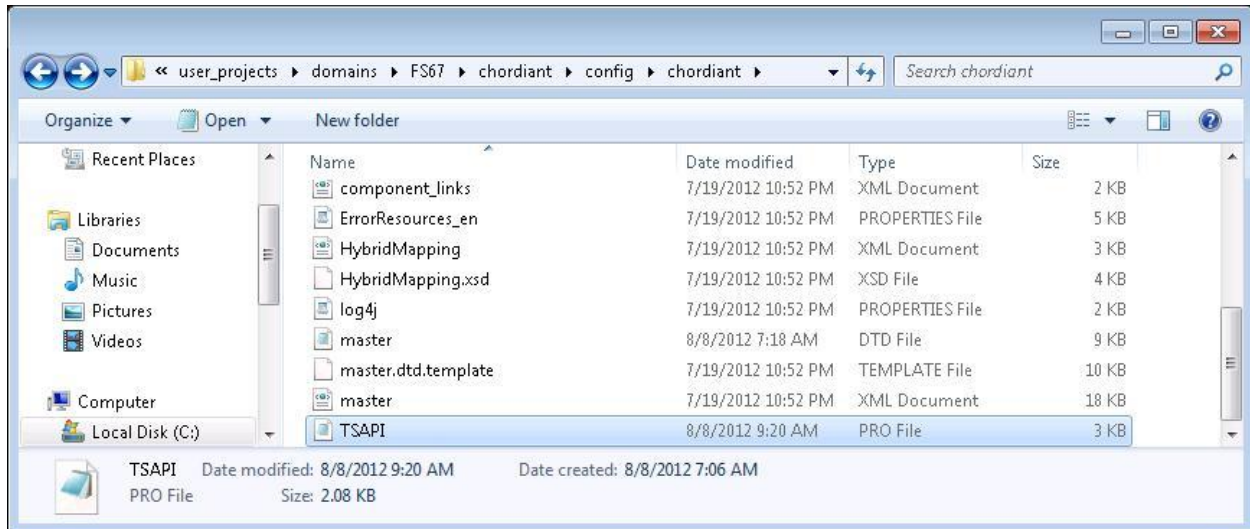


Open the **master.dtd** file with the Notepad application, and scroll down to the **CTI entities** section. Set **CTI\_MIDDLEWARE\_SERVER** to the Tlink name from **Section 6.6**. Set **NUMBER\_OF\_CTI MANAGERS** to the total number of monitored supervisors and agents from **Section 3**.

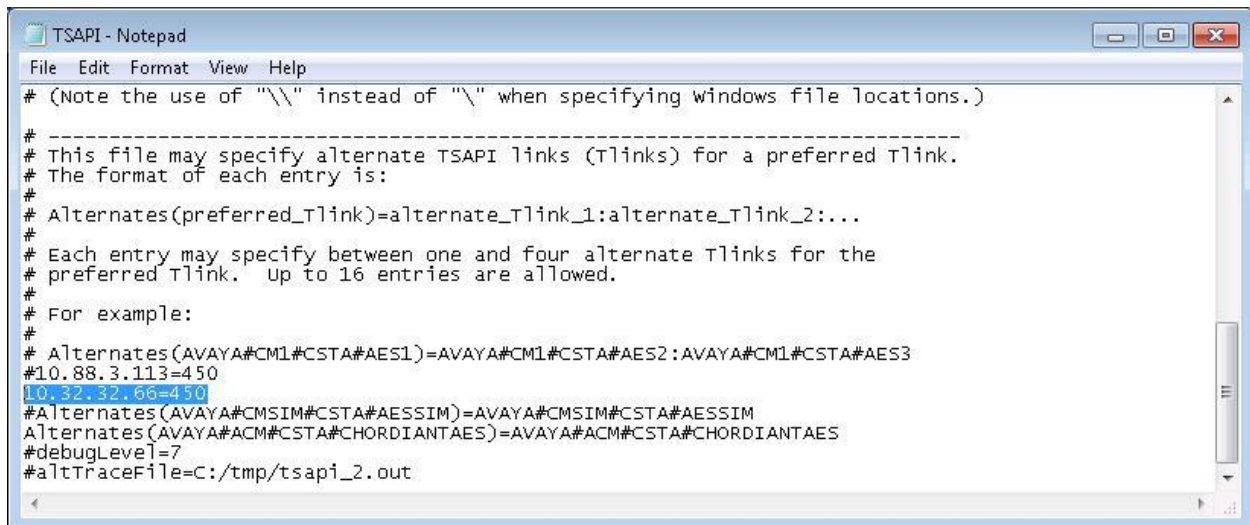


## 7.2. Administer TSAPI.PRO

In the same directory, edit the **TSAPI.PRO** file shown below.

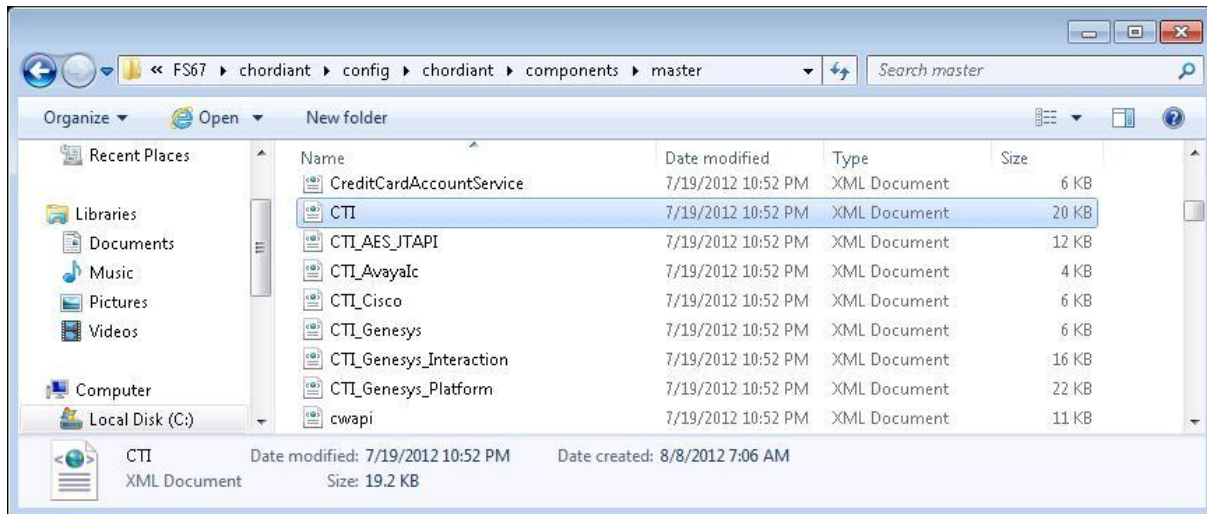


Scroll to the bottom of the file, and add a line as shown below, where “10.32.32.66” is the IP address of Application Enablement Services.

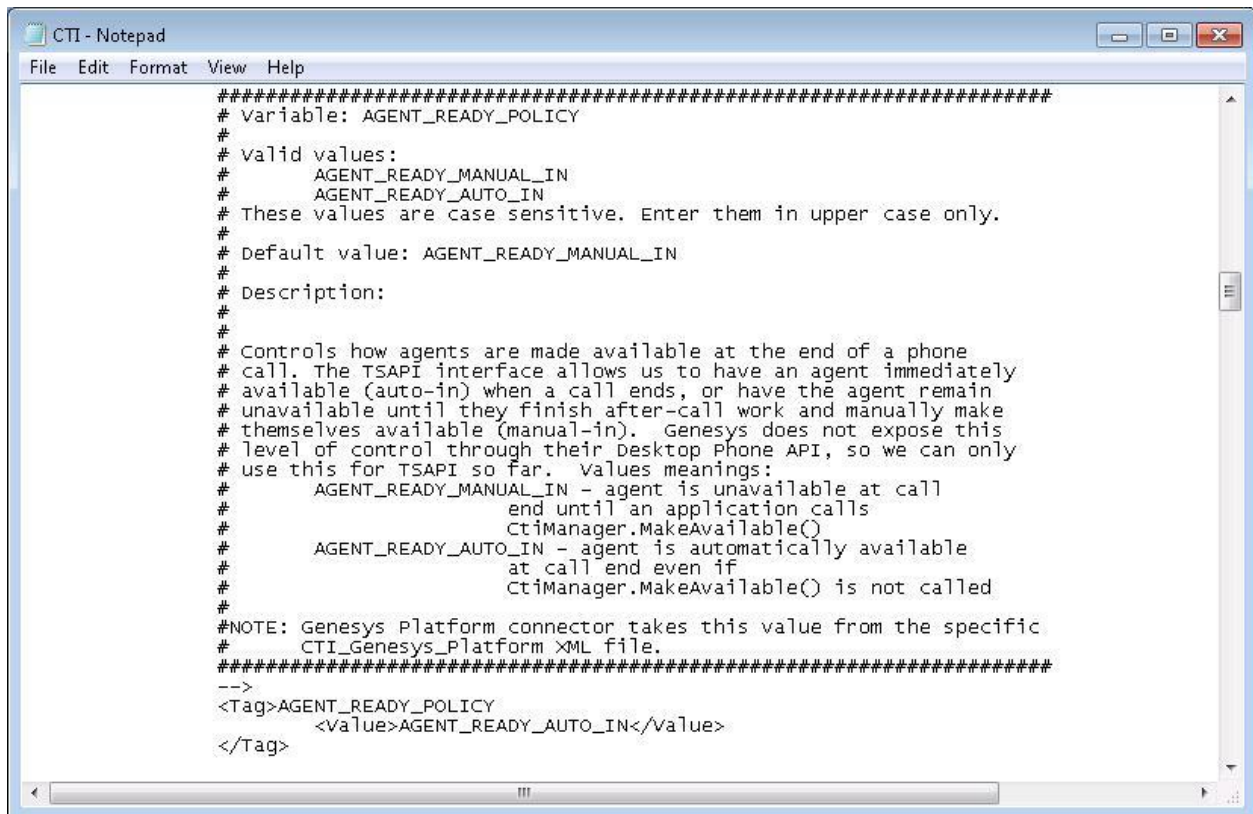


### 7.3. Administer CTI.xml

Navigate to the directory containing the **CTI.xml** file, in this case **C:\WLS1035\user\_projects\domains\FS67\chordiant\config\chordiant\components\master**.



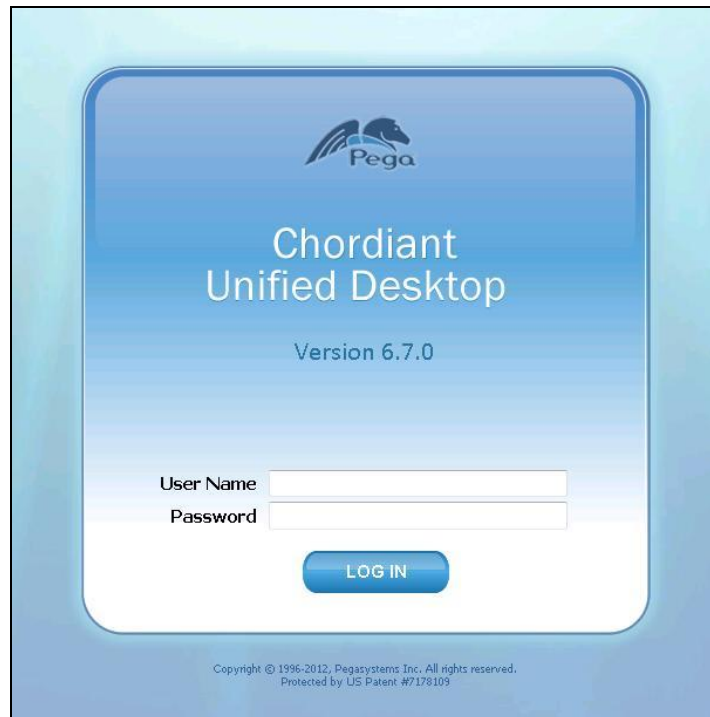
Open the **CTI.xml** file with the Notepad application, and scroll down to the **AGENT\_READY\_POLICY** section to set the desired agent availability mode. In the compliance testing, the policy was set to **AGENT\_READY\_AUTO\_IN** shown below.



## 7.4. Launch Application and Web Interface

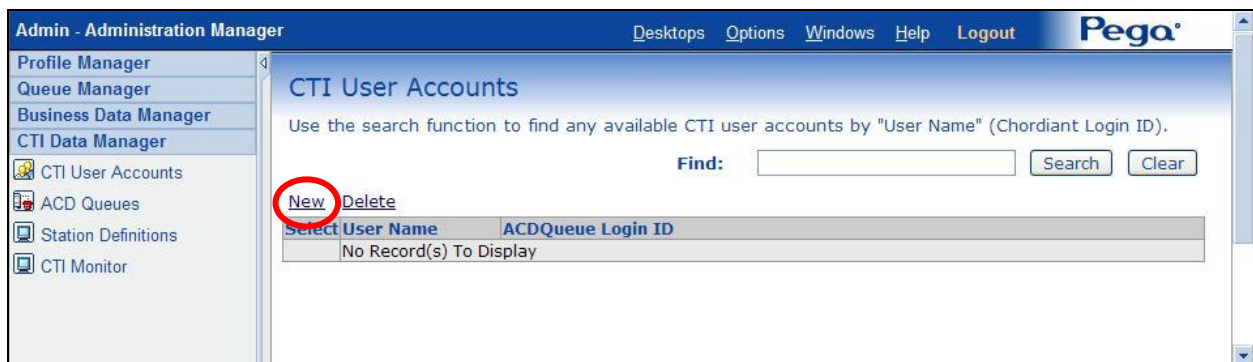
From the Chordiant Foundation Server, navigate to the directory containing the **setChordiantParam.cmd** file, in this case **C:\WLS1035\user\_projects\domains\FS67\bin**, and double-click to launch the application.

After launching the application, start the web interface from a PC by using the URL <http://ip-address:7001/Advisor/advisor.htm> in an Internet browser window, where “ip-address” is the IP address of Chordiant Foundation Server. Log in using the administrator credentials.



## 7.5. Administer CTI User Accounts

The **Admin – Administration Manager** screen is displayed. Select **CTI Data Manager** → **CTI User Accounts** from the left plane, to display the **CTI User Accounts** screen in the right pane. Click **New** to add a new user account.





The screen below is displayed. For **User Name**, click the flashlight icon and select the appropriate user profile from the subsequent pop-up window (not shown). For the **ACDQueue** fields, enter the first agent ID credentials from **Section 5.4**. For the **Middleware** fields, enter the Chordiant user credentials from **Section 6.7**.

**Admin - Administration Manager** Desktops Options Windows Help Logout Pega

**CTI User Account : New**

General

Save Cancel

User Name: \* ccagent1

ACDQueue Login ID: \* 65881

ACD Queue Login Password: .....

Re-Type ACD Queue Password: .....

Middleware Login ID: chordiant

Middleware Login Password: .....

Re-Type Middleware Login Password: .....

Cisco ICM Peripheral ID:

Repeat this section to create a user account for each monitored supervisor and agent from **Section 3**. Note that if transfer/conference of data screens is desired for supervisors, then Chordiant Foundation Server requires the supervisors to be configured and logged in as agents. In the compliance testing, three user accounts were created as shown below.

**Admin - Administration Manager** Desktops Options Windows Help Logout Pega

**Information**

CTI User added successfully

**CTI User Accounts**

Use the search function to find any available CTI user accounts by "User Name" (Chordiant Login ID).

Find: Search Clear

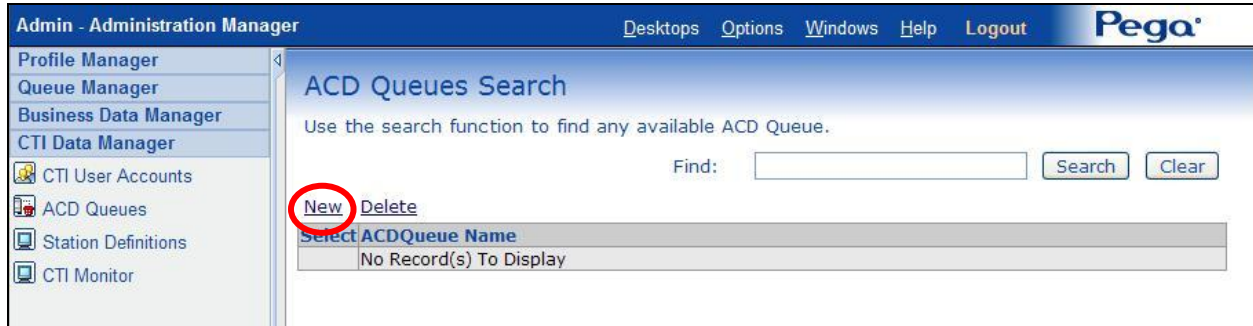
New Delete

Select All Select None

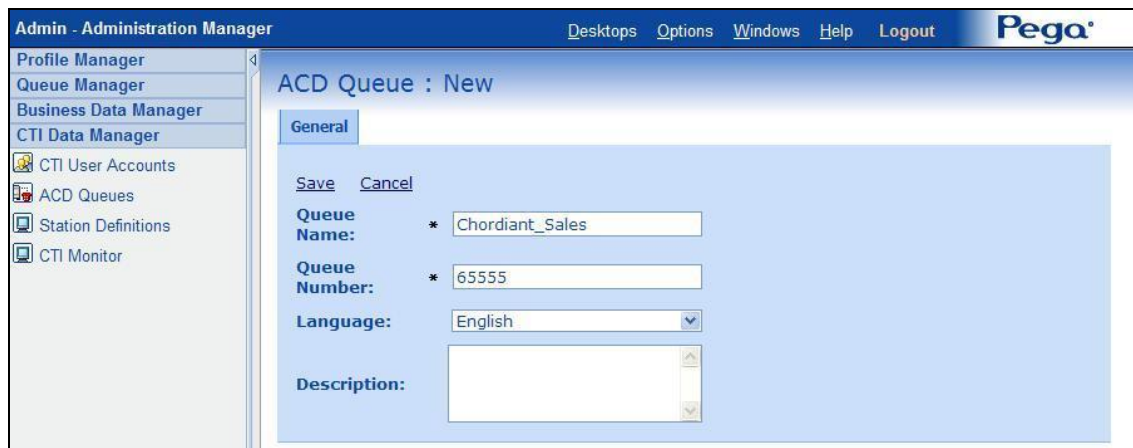
Select	User Name	ACDQueue Login ID
<input type="checkbox"/>	ccagent1	65881
<input type="checkbox"/>	ccagent2	65882
<input type="checkbox"/>	ccmanager	65883

## 7.6. Administer ACD Queues

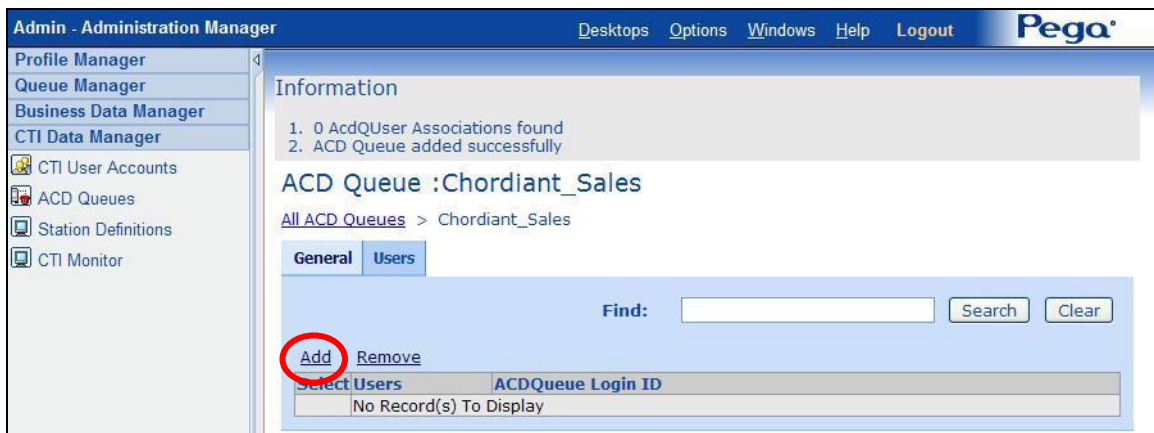
Select **CTI Data Manager** → **ACD Queues** from the left plane, to display the **ACD Queues Search** screen in the right pane. Click **New** to add a new ACD queue.



The screen below is displayed next. For **Queue Name**, enter a desired name without blanks. For **Queue Number**, enter the first skill group extension from **Section 3**. For **Language**, select a desired language, in this case “English”. Click **Save**.



The screen is updated with a new **Users** tab, as shown below. Click **Add** to add a user.



In the subsequent screen (not shown), click the flashlight icon followed by **Search** to display a list of available users (not shown), and select the desired user to add to the queue. Repeat these steps to add all desired users to the queue. In the compliance testing, all three users from **Section 7.5** were added to the queue, as shown below.

The screenshot shows the 'Admin - Administration Manager' interface. The left sidebar contains a navigation menu with the following items: Profile Manager, Queue Manager, Business Data Manager, CTI Data Manager, CTI User Accounts, ACD Queues, Station Definitions, and CTI Monitor. The main content area is titled 'Information' and displays a message: 'User is successfully assigned to the acd queue.' Below this, the title 'ACD Queue :Chordiant\_Sales' is shown, followed by a breadcrumb link 'All ACD Queues > Chordiant\_Sales'. There are two tabs: 'General' and 'Users', with 'Users' being the active tab. A search bar with 'Find:' and buttons for 'Search' and 'Clear' is present. Below the search bar, there are links for 'Add' and 'Remove'. A table with the following data is displayed:

Select	Users	ACDQueue Login ID
<input type="checkbox"/>	ccagent1	65881
<input type="checkbox"/>	ccagent2	65882
<input type="checkbox"/>	ccmanager	65883

Repeat this section to create an ACD queue for each skill group extension from **Section 3**. In the compliance testing, two ACD queues were created as shown below.

The screenshot shows the 'Admin - Administration Manager' interface. The left sidebar contains the same navigation menu as the previous screenshot. The main content area is titled 'ACD Queues Search' and displays a message: 'Use the search function to find any available ACD Queue.' Below this, there is a search bar with 'Find:' and buttons for 'Search' and 'Clear'. There are links for 'New' and 'Delete'. A table with the following data is displayed:

Select	ACDQueue Name
<input type="checkbox"/>	Chordiant_Sales
<input type="checkbox"/>	Chordiant_Support

## 7.7. Administer Station Definitions

Select **CTI Data Manager** → **Station Definitions** from the left plane, to display the **Station Definitions Search** screen in the right pane. Click **New** to add a new station definition.

Admin - Administration Manager

Desktops Options Windows Help Logout Pega

Profile Manager  
Queue Manager  
Business Data Manager  
CTI Data Manager  
CTI User Accounts  
ACD Queues  
Station Definitions  
CTI Monitor

Station Definitions Search

Use the search function to find any available Station.

Find:  Search Clear

New Delete

Select Name

No Record(s) To Display

The screen below is displayed next. Enter a desired **Name** and click **Save**.

Admin - Administration Manager

Desktops Options Windows Help Logout Pega

Profile Manager  
Queue Manager  
Business Data Manager  
CTI Data Manager  
CTI User Accounts  
ACD Queues  
Station Definitions  
CTI Monitor

Station: New

General

Save Cancel

Name: \*  Chordiant agent 1

Effective Date:

Expiry Date:

The screen is updated with a new **Devices** tab, as shown below. Click **New** to add a device.

Admin - Administration Manager

Desktops Options Windows Help Logout Pega

Profile Manager  
Queue Manager  
Business Data Manager  
CTI Data Manager  
CTI User Accounts  
ACD Queues  
Station Definitions  
CTI Monitor

Station: Chordiant agent 1

All Stations > Chordiant agent 1

General Devices

New Delete

Select Device Name Device Type Device ID

No Record(s) To Display



The screen below is displayed. For **Device ID**, enter the first agent station extension from **Section 3**. Enter a desired **Device Name**.

The screenshot shows the 'Admin - Administration Manager' interface with the 'Devices: New' form. The left sidebar contains a navigation menu with items like Profile Manager, Queue Manager, Business Data Manager, CTI Data Manager, CTI User Accounts, ACD Queues, Station Definitions, and CTI Monitor. The main area has a 'General' tab with fields for Device Type (set to 'Telephone'), Device ID (65001), Device Name (agent 1), Description, Primary Middleware Host, Primary Middleware Port, Secondary Middleware Host, and Secondary Middleware Port. Buttons for 'Save' and 'Cancel' are at the top left of the form area.

Repeat this section to create a station definition for each agent and supervisor station extension from **Section 3**. In the compliance testing, three station definitions were created as shown below.

The screenshot shows the 'Admin - Administration Manager' interface with the 'Station Definitions Search' screen. The left sidebar is the same as the previous screenshot. The main area shows 'Information' with '5 Stations found.' and a 'Station Definitions Search' section. It includes a search bar with a 'Find:' label, 'Search' and 'Clear' buttons, and a table of results. The table has columns for 'Select' and 'Name'. The results are: Chordiant agent 1, Chordiant agent 2, and Chordiant supervisor 1. There are also 'New' and 'Delete' buttons above the table.

Select	Name
<input type="checkbox"/>	Chordiant agent 1
<input type="checkbox"/>	Chordiant agent 2
<input type="checkbox"/>	Chordiant supervisor 1

## 8. Verification Steps

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

### 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	4	no	AES2-S8800	established	30	30

### 8.2. Verify Avaya Aura® Application Enablement Services

Log at least one agent into the ACD as described in **Section 8.3**. On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of supervisors and agents logged into the ACD.

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Wed Aug 8 12:04:10 2012 from 10.32.39.20  
HostName/IP: AES2-S8800/10.32.32.66  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-2-32-0

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
	1	S8800	1	Talking	Wed Jun 13 13:29:46 2012	Online	16	1	42	47	30

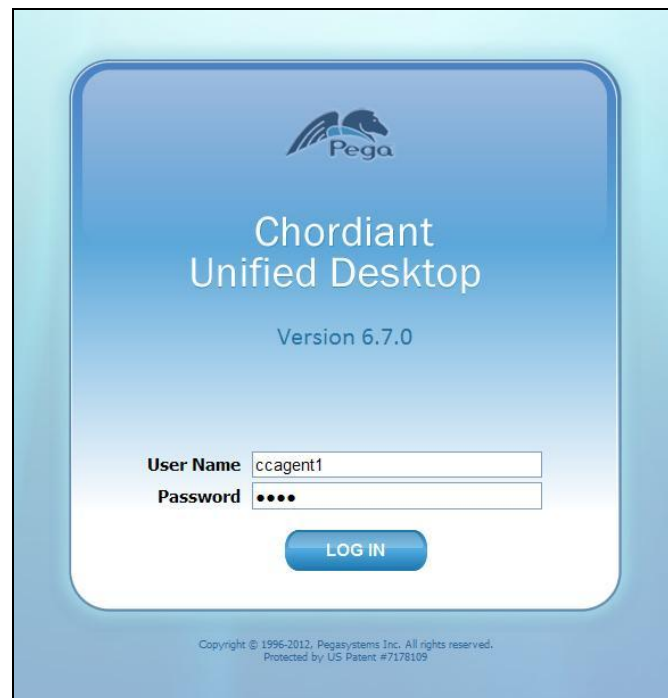
Online Offline

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

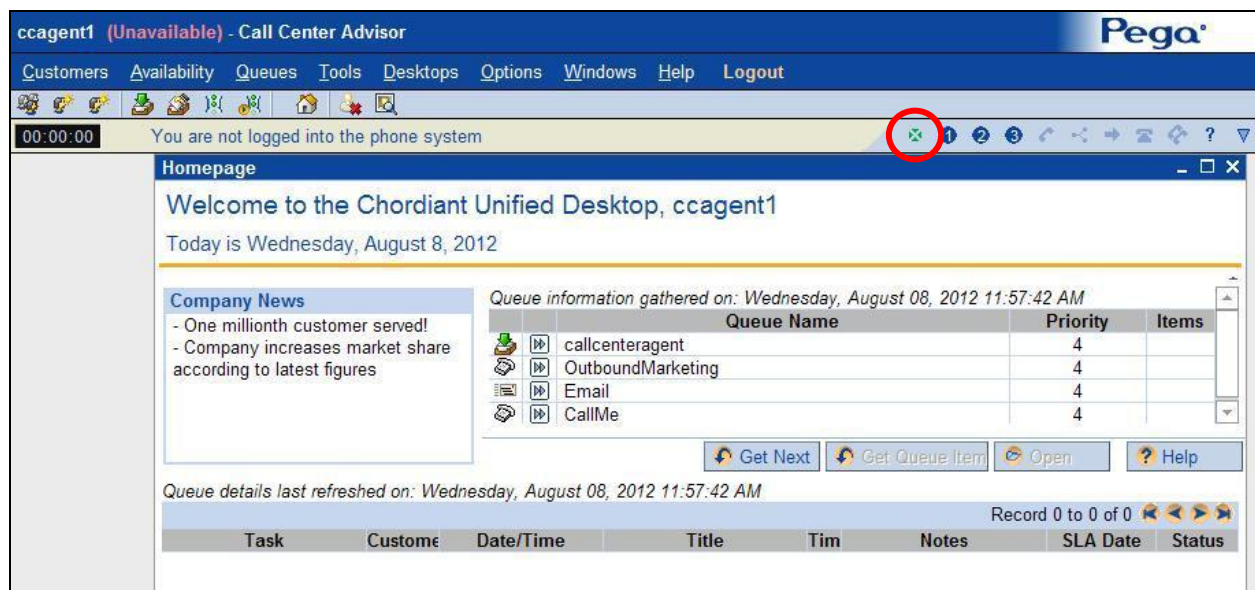
TSAPI Service Status TLink Status User Status

### 8.3. Verify Pegasystems Chordiant Foundation Server

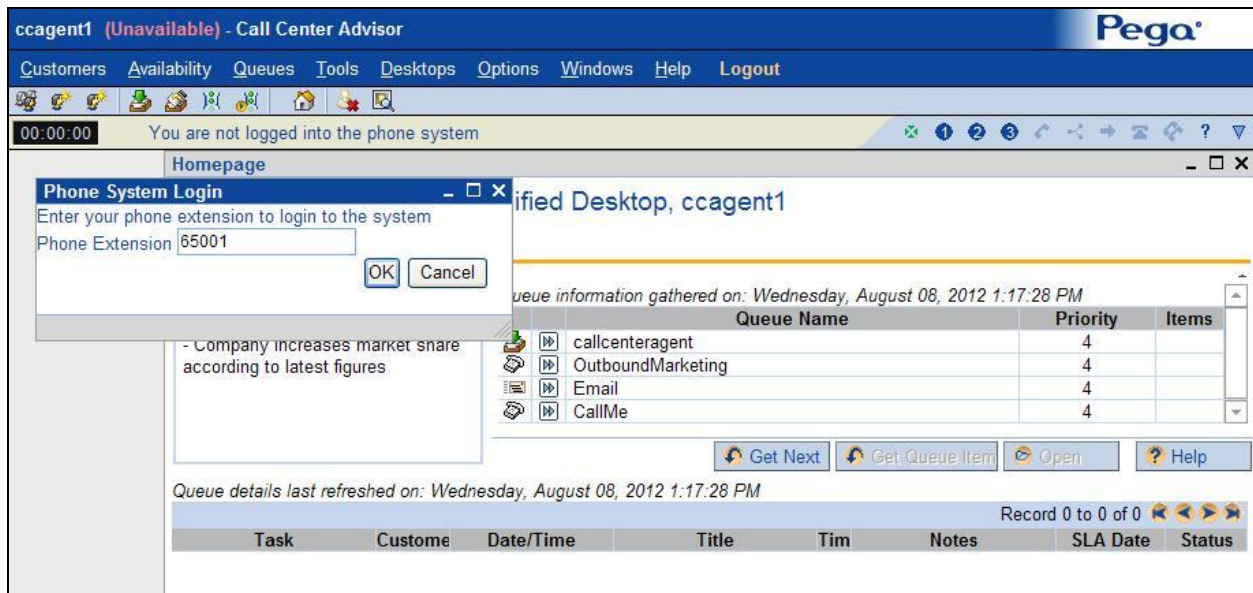
From the agent PC, follow the procedures in **Section 7.4** to launch the Chordiant web-based interface, and log in using the appropriate user credentials.



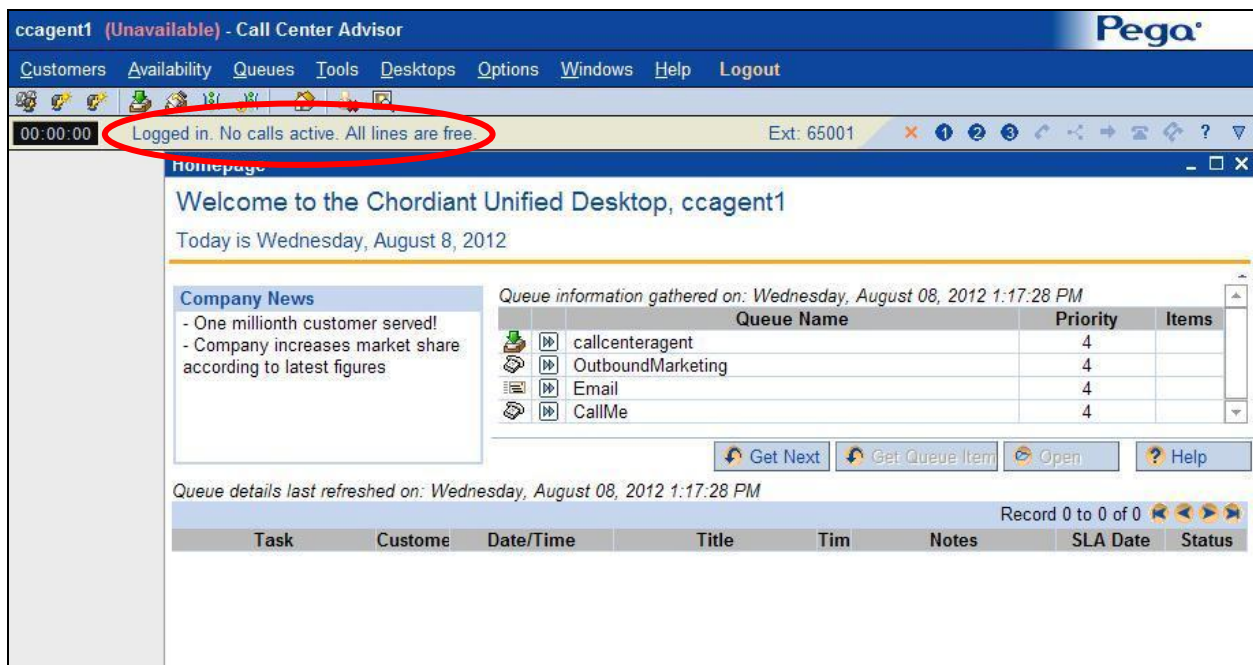
The screen below is displayed next. Click on the **Login to phone system** icon below.



The **Phone System Login** pop-up box is displayed. Enter the agent's station extension, in this case "65001".

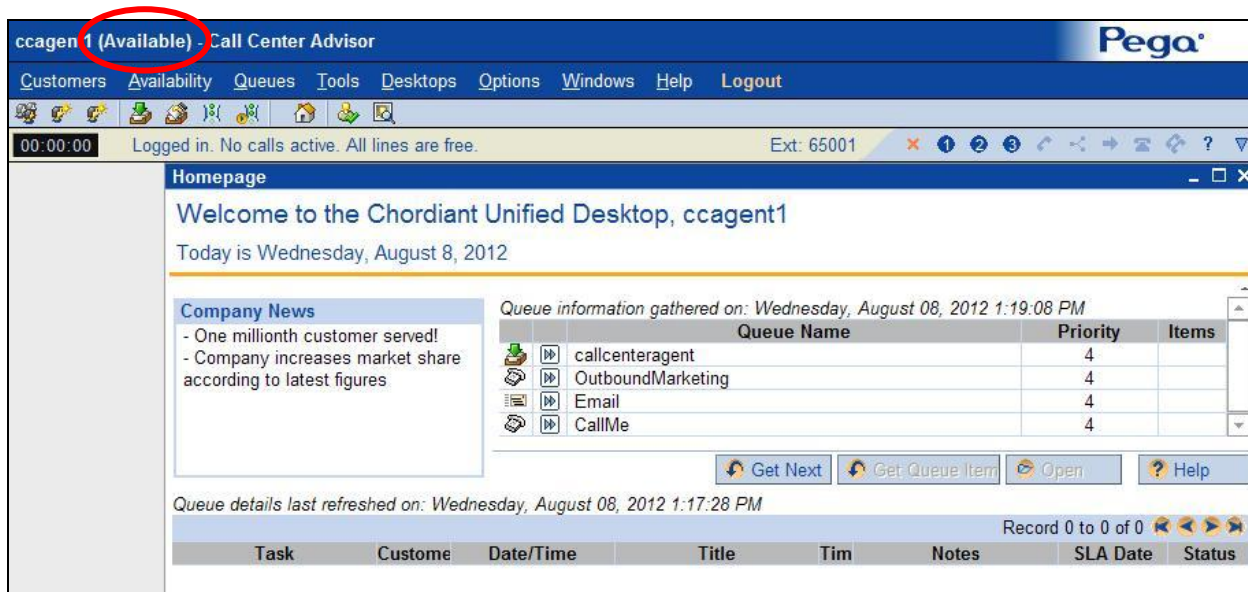


Verify that the screen is updated with log in status, as shown below. Select **Availability** → **Availability** from the top menu.



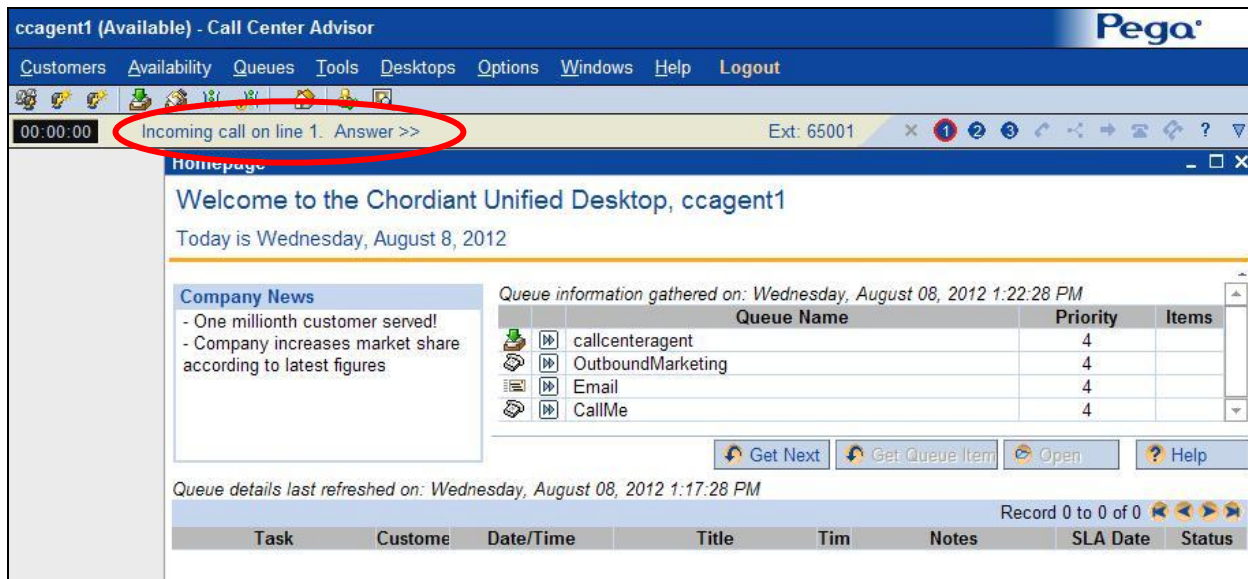


Verify the agent mode changes to **Available**, as shown below.



Make an incoming ACD call from the PSTN. Verify the call is ringing at the agent's telephone, and that the agent screen is updated to reflect the incoming call.

Click on **Answer** or the icon corresponding to the ringing call appearance.



Verify the agent is connected to the PSTN with two-way talk path, and that the agent screen is updated with the calling and called party information, as shown below.

ccagent1 (Available) - Call Center Advisor Pega®

Customers Availability Queues Tools CaseManagement Desktops Options Windows Help Logout

00:00:20 Unknown ? 9088445002 7328862005 Ext: 65001

### Homepage

Welcome to the Chordiant Unified Desktop, ccagent1

Today is Thursday, July 5, 2012

#### Company News

- One millionth customer served!
- Company increases market share according to latest figures

Queue information gathered on: Thursday, July 05, 2012 9:57:54 AM

Queue Name	Priority	Items
callcenteragent	4	
OutboundMarketing	4	
Email	4	
CallMe	4	

Get Next Get Queue Item Open Help

Queue details last refreshed on: Thursday, July 05, 2012 9:54:32 AM

Record 0 to 0 of 0

Task	Custome	Date/Time	Title	Tim	Notes	SLA Date	Status
------	---------	-----------	-------	-----	-------	----------	--------

Filter Remove Filter Re-queue Open Comment Refresh Help

## 9. Conclusion

These Application Notes describe the configuration steps required for Pegasystems Chordiant Foundation Server to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. 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 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011, available at <http://support.avaya.com>.
3. *Chordiant Foundation Server Telephony Integration Guide*, Release 6.7, May 2012, available at <https://mesh.pegasystems.com>.

---

**©2012 Avaya Inc. All Rights Reserved.**

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

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