



Avaya Solution & Interoperability Test Lab

Application Notes for CDC Software CDC Platform with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Zendesk – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CDC Software CDC Platform to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Zendesk. CDC Software CDC Platform is a middleware solution that connects telephony systems with CRM providers.

In the compliance testing, CDC Software CDC Platform used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, to provide screen pop for agent desktops connected to CRM provider Zendesk.

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 CDC Software CDC Platform (CDC) to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Zendesk. CDC is a middleware solution that connects telephony systems with CRM providers.

In the compliance testing, CDC used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, to provide screen pop for agent desktops connected to CRM provider Zendesk.

The agent desktops are connected to the Zendesk cloud via browser connections. Upon being notified via TSAPI of a call answered on a monitored agent, CDC pushed call information including ANI and DNIS as part of help desk ticket creation to the agent desktop via the Restful API with Zendesk.

The compliance test covered the default out-of-the-box screen pop behavior, which popped help desk ticket creations for inbound ACD calls only. CDC does offer additional features and custom screen pops, which are outside the scope of this compliance test.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon application start up, CDC used TSAPI to query device information for configured agents and requested device monitoring for agents that are logged into the ACD.

For the manual part of testing, incoming ACD calls were placed from PSTN with available agents that have web browser connections to Zendesk. All necessary call actions were initiated from the agent telephones.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the CDC server and to the agent desktops.

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 CDC:

- Handling of TSAPI messages in the areas of event notifications and value queries.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, transfer, conference, and long duration.

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

2.2. Test Results

All test cases were executed and passed. The following is an observation on CDC from the compliance testing.

- CDC requires the SA8702 CDR Enhancements for Network special application to be enabled, which ensures the same UCID across all call segments in a call scenario. However, this special application is not compatible with use of SIP agents, therefore the application cannot support SIP agents in the current release.

2.3. Support

Technical support on CDC can be obtained through the following:

- **Phone:** (570) 309-6827
- **Email:** information@cdcsoftware.com
- **Web :** <http://support.cdcsoftware.com>

3. Reference 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, CDC monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	60001, 60002
Skill Group	61001, 61002
Supervisor	65000
Agent Station	65001, 65002
Agent ID	65881, 65882

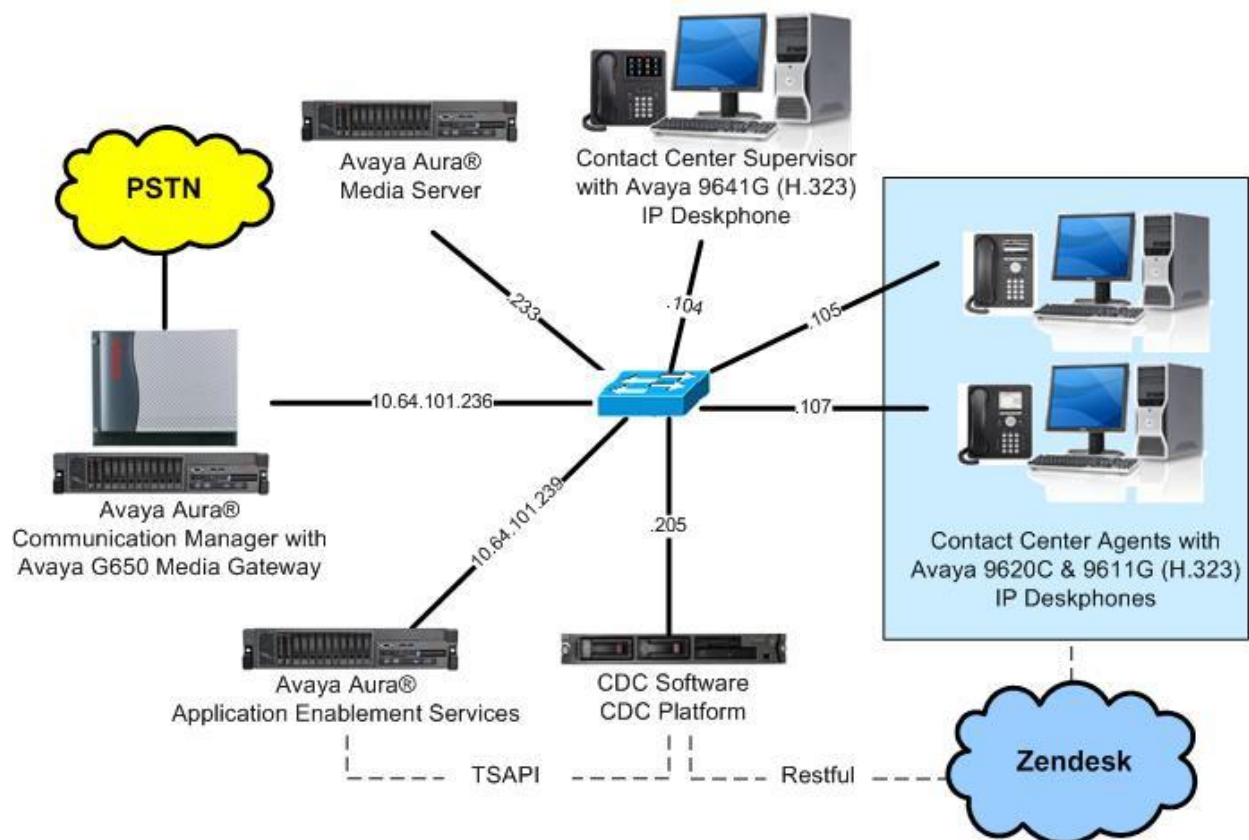


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.0.1.1 (7.0.1.1.0.441.23169)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.2.15-0)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6229
Avaya 9620C IP Deskphone (H.323)	3.270B
CDC Software CDC Platform on Windows Server 2012 R2 <ul style="list-style-type: none">Avaya TSAPI Windows Client (csta32.dll)Zendesk Restful API (ZendeskApi_v2.dll)	1.5.1.4807 Standard 6.2.0.257 3.0.3.0

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
- Verify system parameters special applications
- Administer system parameters features

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 4**. 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 4 of 12
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? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	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		
Extension: 60111		
Type: ADJ-IP		
COR: 1		
Name: AES CTI Link		

5.3. Verify System Parameters Special Applications

Use the “display system-parameters special-applications” command to verify that the **(SA8702) – CDR Enhancements for Network** special application is set to “y” on **Page 5**. This parameter enables the **Copy UCID for Station Conference/Transfer** field to appear on the system parameters features form in **Section 5.4**, which is required by CDC. 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 special-applications                                Page 5 of 10
                                SPECIAL APPLICATIONS

                                (SA8652) - No Hold Consult? n
(SA8654) - Crisis Alert Call Monitoring and Recording? n
                                (SA8661) - Increased Automatic Wakeup Calls? n
                                (SA8662) - Expanded PMS Name & Number? n
                                (SA8684) - PMS Wakeup Message? n
(SA8693) - Connectivity Check for Direct IP Shuffling? n

                                (SA8697) - 3rd Party H.323 Endpoint Support? n
(SA8701) - Net Region Support H.323 Endpoints Behind ALG? n
                                (SA8702) - CDR Enhancements for Network? y
                                (SA8731) - Block Outgoing Bridged Call Display? n
```

5.4. 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. Enable **Copy UCID for Station Conference/Transfer**, which will preserve the UCID associated with a call for the second call legs from station transfer and conference operations on a system wide basis, as required by CDC.

```
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:
                                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
    Copy UCID for Station Conference/Transfer? y
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the UCID to be sent to CDC.

```
change system-parameters features                                     Page 13 of 19
      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
      Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```


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
- Administer CDC user
- Administer security database
- Restart service
- Obtain Tlink name

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 thick red horizontal bar separates the header from the main content area. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login form. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and contains a paragraph explaining the OAM Web's purpose and a bulleted list of administrative domains and their functions. A footer note mentions that these domains can be managed by one or multiple administrators.

Welcome: User
Last login: Tue Nov 22 11:07:14 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 22 14:17:16 EST 2016
HA Status: Not Configured

Home | Help | Logout

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

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the sidebar. The main content area is titled "Licensing" and provides instructions on how to set up, import, and maintain licenses, along with a bulleted list of required actions. The sidebar now highlights "Licensing" and includes sub-items like "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses".

Welcome: User
Last login: Tue Nov 22 11:07:14 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 22 14:17:16 EST 2016
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

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

TLT; Reviewed: Solution & Interoperability Test Lab Application Notes 11 of 24
SPOC 12/20/2016 ©2016 Avaya Inc. All Rights Reserved. CDC-ZD-AES7

6.3. Administer TSAPI Link

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
------	-------------------	-------------------	-------------------	----------

Buttons: Add Link, Edit Link, 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 "cm7" 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 Avaya Application Enablement Services Management Console, specifically the "Add TSAPI Links" screen. The left navigation pane is the same as in the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. Each field has a dropdown menu. The "Link" field is set to "1", "Switch Connection" is set to "cm7", "Switch CTI Link Number" is set to "1", "ASAI Link Version" is set to "7", and "Security" is set to "Unencrypted". Below the fields are buttons for "Apply Changes" and "Cancel Changes".

Form fields:

- Link: 1
- Switch Connection: cm7
- Switch CTI Link Number: 1
- ASAI Link Version: 7
- Security: Unencrypted

Buttons: Apply Changes, Cancel Changes

6.4. Administer CDC User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Nov 22 11:07:14 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 22 14:17:16 EST 2016
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idcdc

* Common Namecdc

* Surnamcdc

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.5. Administer 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. Make certain the **Enable SDB for TSAPI Service, JTAPI, and Telephony Web Services** parameter is unchecked, as shown below.

In the event that the security database is used by the customer with the parameter already enabled, then follow reference [2] to configure access privileges for the CDC user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message for the user is shown in the top right corner, including login details and server information. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page. This page contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User
Last login: Tue Nov 22 11:07:14 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 22 14:17:16 EST 2016
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout

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

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

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

6.6. 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 displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title 'Application Enablement Services Management Console'. A welcome message for the user is shown in the top right corner. The main navigation pane on the left lists various sections: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status. The main content area on the right is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, all of which are 'Running'. The 'TSAPI Service' is checked. 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.

Welcome: User
Last login: Tue Nov 22 11:07:14 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 22 14:17:16 EST 2016
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status

Service Controller

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

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

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

6.7. 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 CDC.

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” 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 pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows the "Tlinks" page with a single Tlink named "AVAYA#CM7#CSTA#AES7" and a "Delete Tlink" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Nov 22 11:07:14 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 22 14:17:16 EST 2016
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

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

Tlinks

Tlink Name
AVAYA#CM7#CSTA#AES7
Delete Tlink

7. Configure CDC Software CDC Platform

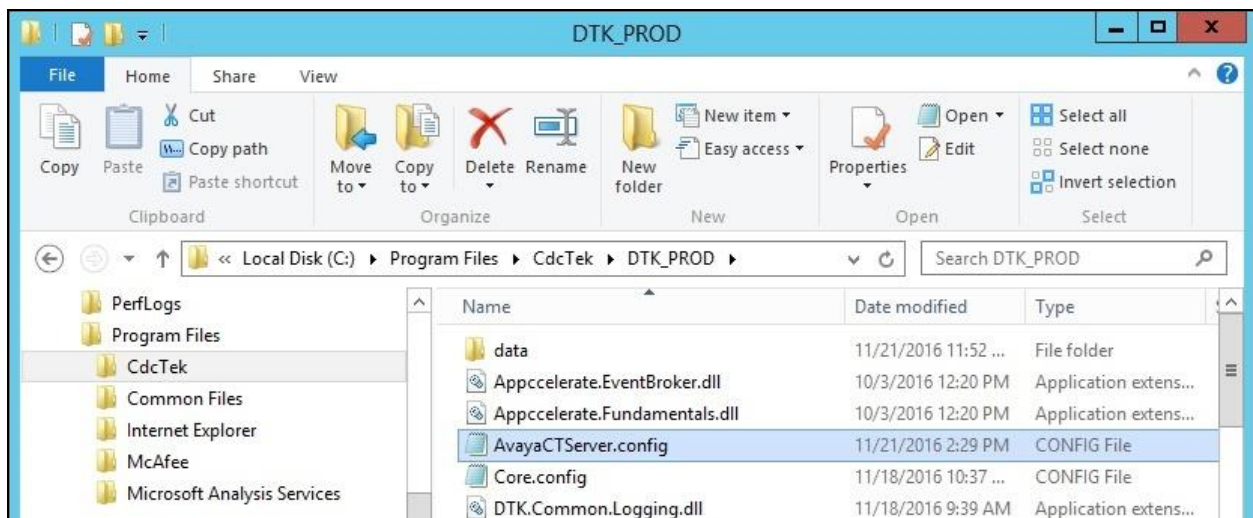
This section provides the procedures for configuring CDC. The procedures include the following areas:

- Administer AvayaCTServer.config
- Administer Zendesk.config

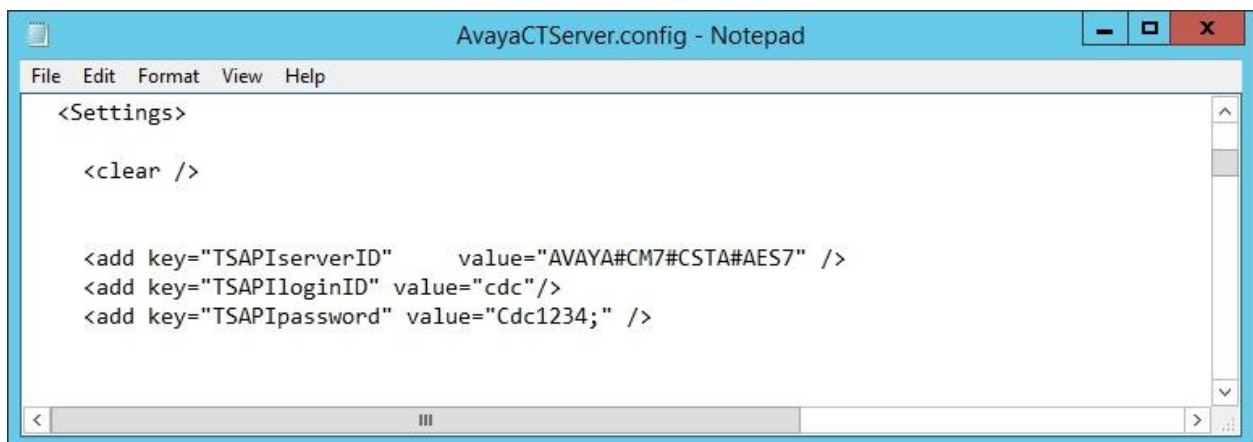
The configuration of CDC is performed by CDC technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Administer AvayaCTServer.config

From the CDC server, navigate to the **C:\Program Files\CdcTek** directory to edit the **AvayaCTServer.config** file shown below.

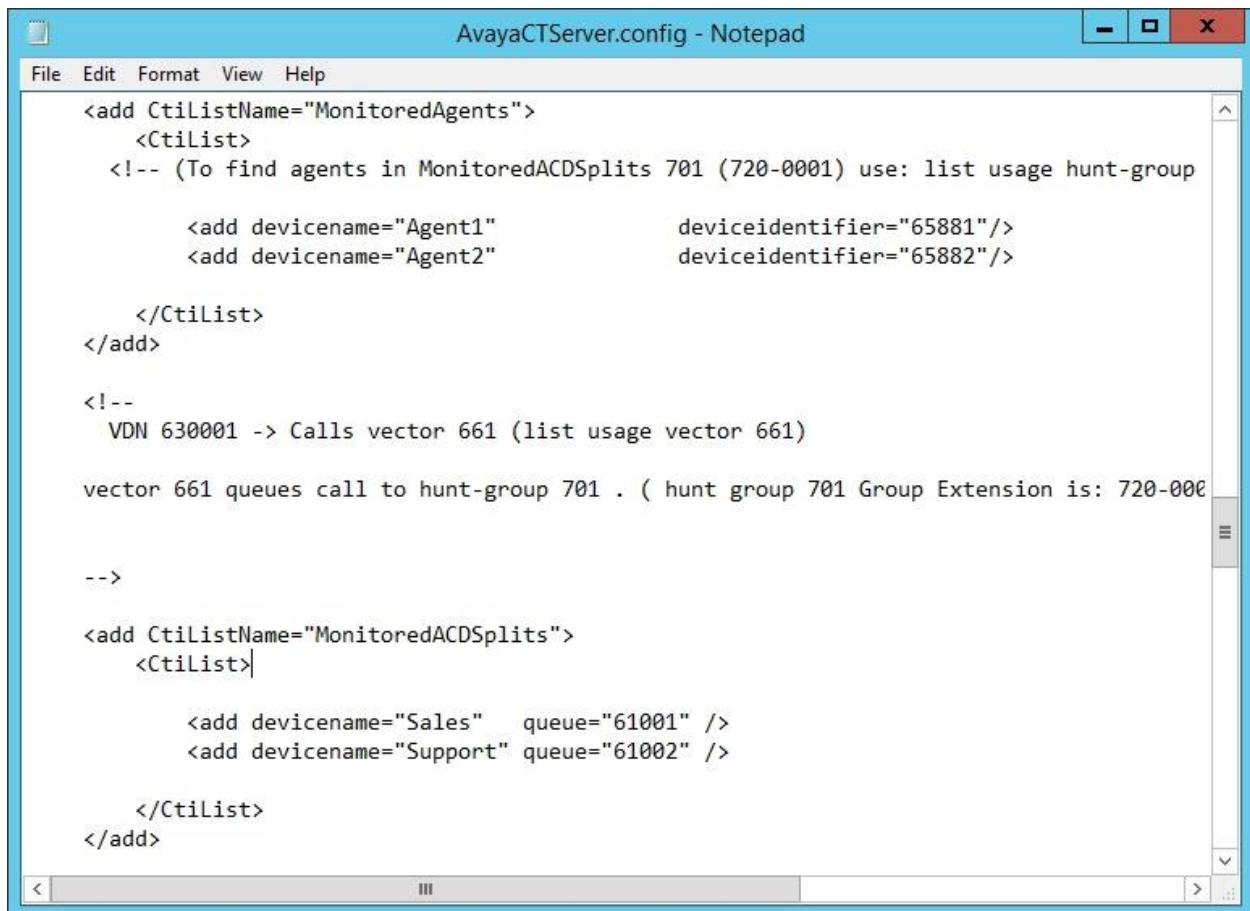


Scroll down to the **Settings** sub-section. Set **TSAPIserverID** to the Tlink name from **Section 6.7**. Set **TSAPIloginID** and **TSAPIpassword** to the CDC user credentials from **Section 6.4**.



Scroll down to the **MonitoredAgents** sub-section. For each agent ID from **Section 3**, add an entry line with a descriptive **devicename**, and the agent ID value as **deviceidentifier**, as shown below.

Scroll down to the **MonitoredACDSplits** sub-section. For each skill group from **Section 3**, add an entry line with a descriptive **devicename**, and the skill group extension value as **queue**, as shown below.



```
<add CtiListName="MonitoredAgents">
  <CtiList>
    <!-- (To find agents in MonitoredACDSplits 701 (720-0001) use: list usage hunt-group

        <add devicename="Agent1"          deviceidentifier="65881"/>
        <add devicename="Agent2"          deviceidentifier="65882"/>

    </CtiList>
  </add>

  <!--
    VDN 630001 -> Calls vector 661 (list usage vector 661)

vector 661 queues call to hunt-group 701 . ( hunt group 701 Group Extension is: 720-000

-->

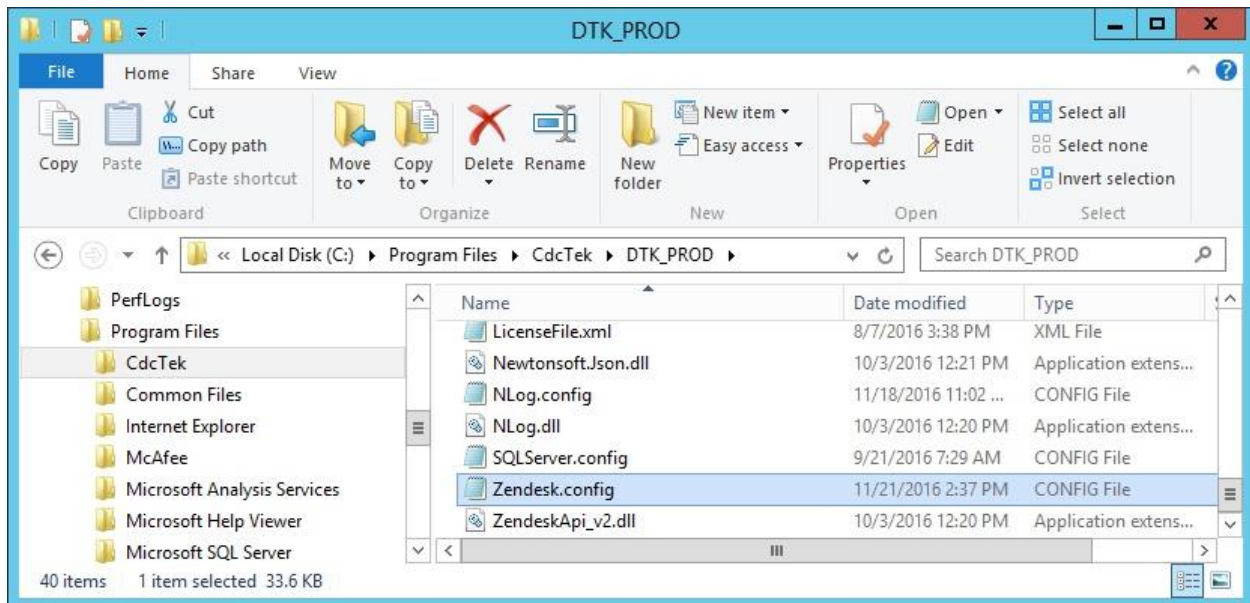
<add CtiListName="MonitoredACDSplits">
  <CtiList>

    <add devicename="Sales"  queue="61001" />
    <add devicename="Support" queue="61002" />

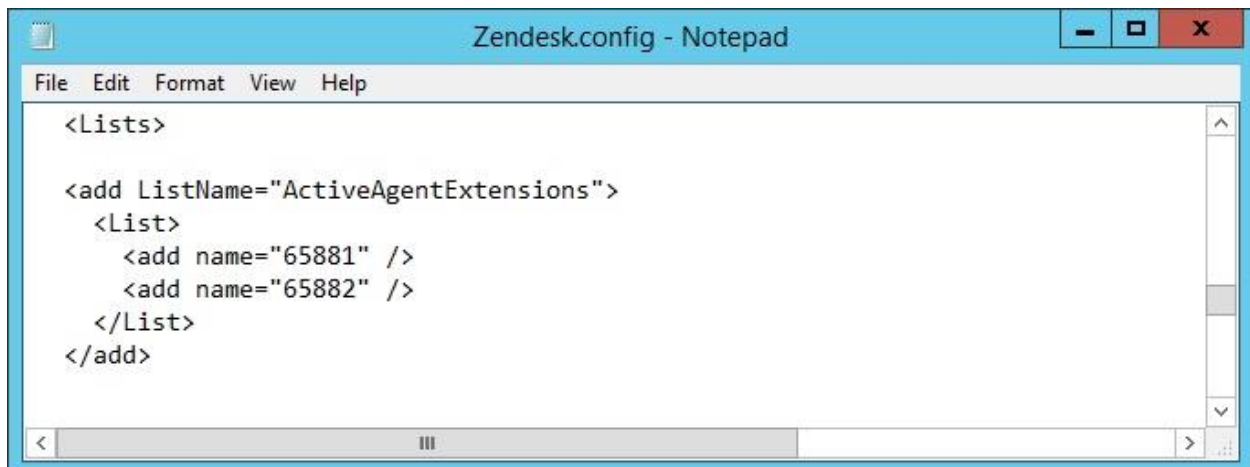
  </CtiList>
</add>
```

7.2. Administer Zendesk.config

Under the same directory, edit the **Zendesk.config** file.



Scroll down to the **ActiveAgentExtensions** sub-section. Add an entry line or each agent ID from **Section 3**, as shown below.



8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify 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	7	no	aes7	established	15	15

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 that the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and logged in agents from **Section 3**, in this case “4”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Nov 22 14:16:55 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 22 15:04:15 EST 2016
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

TSAPI Link Details

☐ Enable page refresh every 60 seconds

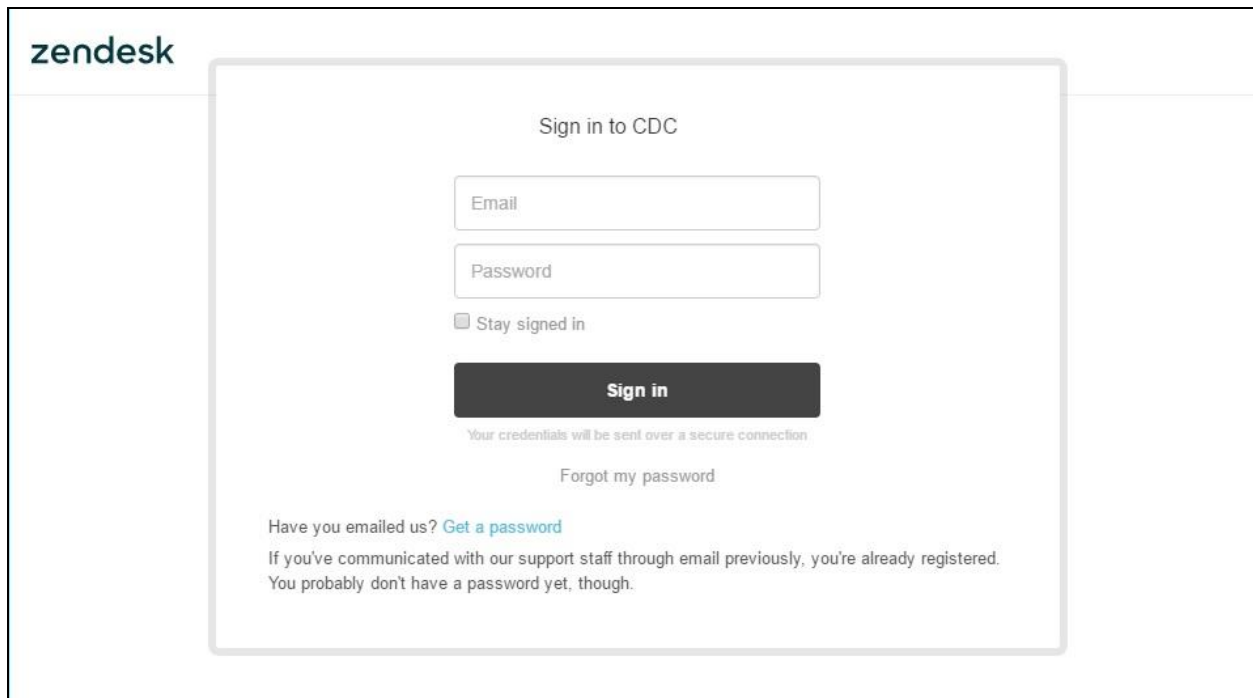
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Tue Nov 15 16:47:55 2016	Online	17	4	15	15	30

Online Offline

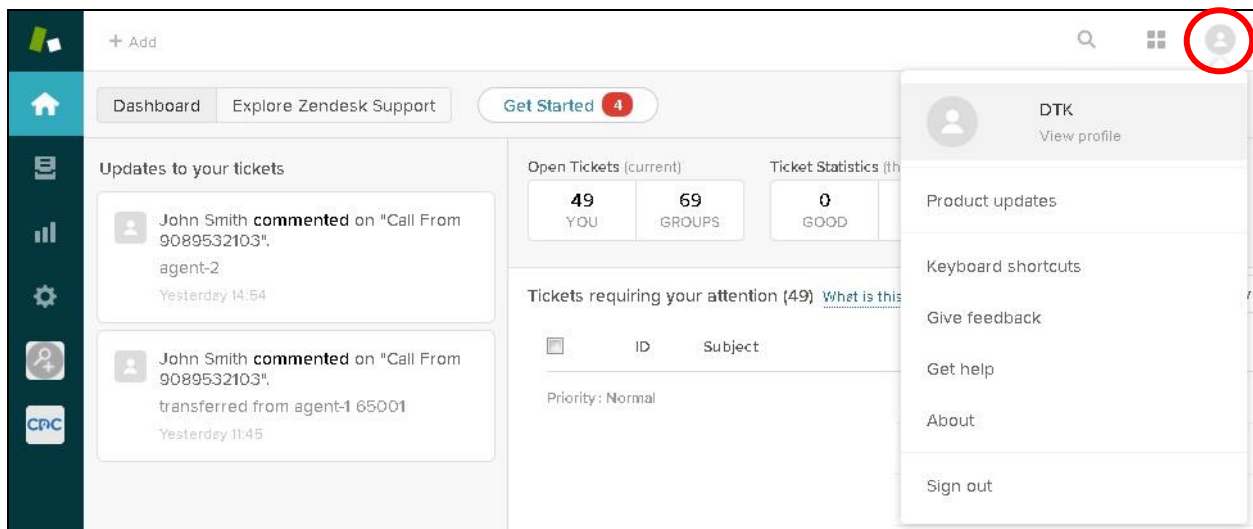
For service-wide information, choose one of the following:
TSAPI Service Status TLink Status User Status

8.3. Verify CDC Software CDC Platform

Use the agent telephone to log an agent into the ACD. From the agent desktop, launch an Internet browser window and enter the URL provided by the end customer for Zendesk. Log in with the relevant user credentials provided by CDC.



The screen below is displayed. Click on the user icon from the upper right portion of the screen, and select **View profile** from the top of the list.



The screen is updated as shown below. Scroll down the left pane to the **Telephony Id Avaya AES** sub-section, and enter the pertinent agent ID from **Section 3**, in this case “65881”.

The screenshot shows the DTK interface with the following details:

- Left Pane:**
 - Home icon
 - Menu icon
 - Bar chart icon
 - Gears icon
 - Person icon
 - CDC logo
- Top Bar:**
 - DTK (selected)
 - + Add
 - Search icon
 - Grid icon
 - Profile icon
- Main Content Area:**
 - Details:**
 - Notes
 - Telephony Id Avaya AES:**
 - 65881
 - Outbound Dialing Region: United States of America - US
 - Created: Aug 03 10:49
 - DTK Profile:**
 - + New Ticket
 - Tickets (49)
 - Security Settings
 - Assigned tickets (49):**

ID	Subject	Requester	Requested	Updated
Status: Open				

Make an incoming ACD call from the PSTN and answer the call on the agent telephone. Verify that the agent desktop is populated with a new ticket incident, in this case “1525”, along with proper call information, as shown below.

The screenshot shows the DTK interface with a new ticket incident #1525. The ticket is titled "Call From 9089532103" and includes the following details:

- Top Bar:**
 - DTK (selected)
 - Call From 9089532103 #1525
 - + Add
 - Search icon
 - Grid icon
 - Profile icon
- Main Content Area:**
 - Organization (create):** NewUser-9089532103
 - Incident #1525** (open)
 - Assignee:** Support/DTK
 - CCs:** search name or contact info
 - Form:** Default Ticket Form
 - Tags:** ctk
 - Type:** Incident
 - Priority:** Normal
 - Linked problem:** -
 - Wrap-Up:** -
 - talk time:** -
 - Call Details:**
 - Call From 9089532103
 - Today 16:37 • NewUser-9089532103 9089532103 via DTK
 - [change] • Via [Phone Number]
 - Public reply / Internal note:** your comment is sent to the ticket requester
 - Conversations:** All 1
 - DTK Today 16:37 NEW:**
 - DTK generated:
 - ANI: 9089532103
 - VDN: 3035360001
 - Agent: 65881
 - Answering Extension: 65001
 - Call ID: 00027013611479846871
 - UCID: 00027013611479846871
 - ACDSplit: 61001
 - Bottom Bar:**
 - Close tab
 - Submit as Open

9. Conclusion

These Application Notes describe the configuration steps required for CDC Software CDC Platform to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Zendesk. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at <http://support.avaya.com>.
3. *Administration and Configuration (Avaya and CRM)*, Version 1.5.1, November 17, 2016, available at <http://support.cdcsoftware.com>.

©2016 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.