



**Application Notes for Tenfold with Avaya Aura®  
Communication Manager and Avaya Aura® Application  
Enablement Services using Tenfold Chrome Extension and  
Salesforce.com – Issue 1.0**

**Abstract**

These Application Notes describe the configuration steps required for Tenfold to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Tenfold Chrome Extension and Salesforce.com. Tenfold is a solution that unifies a customer's phone system and CRM platform.

In the compliance testing, Tenfold used the Telephony Services Application Programmer Interface from Avaya Aura® Application Enablement Services to monitor agents on Avaya Aura® Communication Manager, to provide screen pop and Click to Dial features from the agent desktops that were connected to Tenfold and Salesforce.com via Chrome browsers and Tenfold Chrome Extension.

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 Tenfold to interoperate with Avaya Aura® Communication Manager 8.0.1 (Communication Manager) and Avaya Aura® Application Enablement Services 8.0.1 (AES) using Tenfold Chrome Extension with Salesforce.com. Tenfold is a solution that unifies an Avaya Contact Center and a CRM platform.

In the compliance testing, Tenfold used the Telephony Services Application Programmer Interface (TSAPI) from AES to monitor agent stations on Communication Manager, to provide screen pop and Click to Dial features from the agent desktops that were connected to Tenfold and Salesforce.com via Chrome browsers and Tenfold Chrome Extension.

The Tenfold solution consisted of the Tenfold Cloud, Tenfold server with Cloud Connect Server and Cloud Connect Client components, and agent desktops (Windows PCs) with Chrome browser running Tenfold Chrome Extension. The Tenfold Chrome Extension is a plugin that enables call floating UI for agents, and can be downloaded from the Chrome Web Store. The Tenfold Cloud is the component responsible for all business logic, and is required to reside on the Tenfold premise. The Cloud Connect Server is the component that integrates with AES using TSAPI.

In the compliance testing, each agent desktop was connected to the Tenfold server, Tenfold Cloud, and Salesforce.com via the Chrome browser. Upon notification of TSAPI events of a call delivered to an agent, the Tenfold server sends related information to the Tenfold Cloud, which in turn polls the relevant contact record from Salesforce.com and pushes the contact record data onto the Tenfold Chrome Extension running on the agent desktop.

The Tenfold Chrome Extension also examines digits present on all Chrome web pages, and provides indications for digits that meet the criteria and can be dialed as part of the Click to Dial feature. Upon detection of such a click, the Tenfold Chrome Extension passes the information to the Tenfold Cloud, which in turn communicates with the Tenfold server. The Tenfold server then sends a Make Call request to AES, to launch the outbound call on behalf of the agent. All progress tones for the outbound call are played back on the agent telephone.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Upon start of application, Tenfold used TSAPI to query device information and name on the agent stations, and requested monitoring. During the compliance testing Tenfold monitored Avaya H.323 endpoints via TSAPI.

For the manual part of the testing, incoming ACD calls were placed with available agents that have Chrome browser connections to Tenfold and Salesforce.com, along with enabled Tenfold Chrome Extension. All necessary call actions were initiated from the agent telephones. The Click to Dial calls were initiated by clicking on digits from Chrome web pages that were presented as can be dialed.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Tenfold server.

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 AES and Tenfold did not include use of any specific encryption features as requested by Tenfold.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Tenfold:

- Use of TSAPI monitoring services to monitor H.323 agent stations.
- Use of TSAPI call control services to launch outbound calls for the Click to Dial feature.
- Proper handling of call scenarios involving inbound, outbound, ACD, non-ACD, screen pop, drop, hold/resume, multiple agents, long duration, and Click to Dial from Chrome web page.

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

## 2.2. Test Results

All test cases were executed, and the following were observations on Tenfold:

- Compliance testing was carried out using H.323 phones only as requested by Tenfold.
- The current release of Tenfold does not support reflection of attended transfer, conference, internal call, and multiple calls.
- If the calling party number was not passed from the PSTN, no indication was provided on the Tenfold Chrome Extension. In cases where PSTN passes “Anonymous”, a no match indication is displayed in the Tenfold Chrome Extension, and this wasn’t verified in the compliance testing.
- For a blind transfer scenario, the Tenfold Chrome Extension on the transfer-to agent showed the full ten digits number associated with the transfer-from agent instead of the number associated with the PSTN caller. The transfer-to agent will need to be aware and recognize when such case occurs, and can manually retrieve the customer contact number by doing a lookup in Salesforce using the populated PSTN caller name from Tenfold Chrome Extension, or by manually collecting the number from the customer.
- After a busy out and release of CTI link commands on Communication Manager, active station monitors were removed on Communication Manager and AES and were not re-established by Tenfold. The workaround is for the administrator to manually restart the services on the Tenfold server.
- When the network connection to the Tenfold server was disrupted, the call duration for an active call in the Tenfold Chrome Extension will continue to increment regardless of when the call was dropped – whether dropped during the disruption or post Tenfold server recovery. Furthermore, the first call to the impacted agent post server recovery continued the duration from the previous call. The duration behavior did return to normal from the second call on for the impacted agent.

## 2.3. Support

Technical support on Tenfold can be obtained through the following:

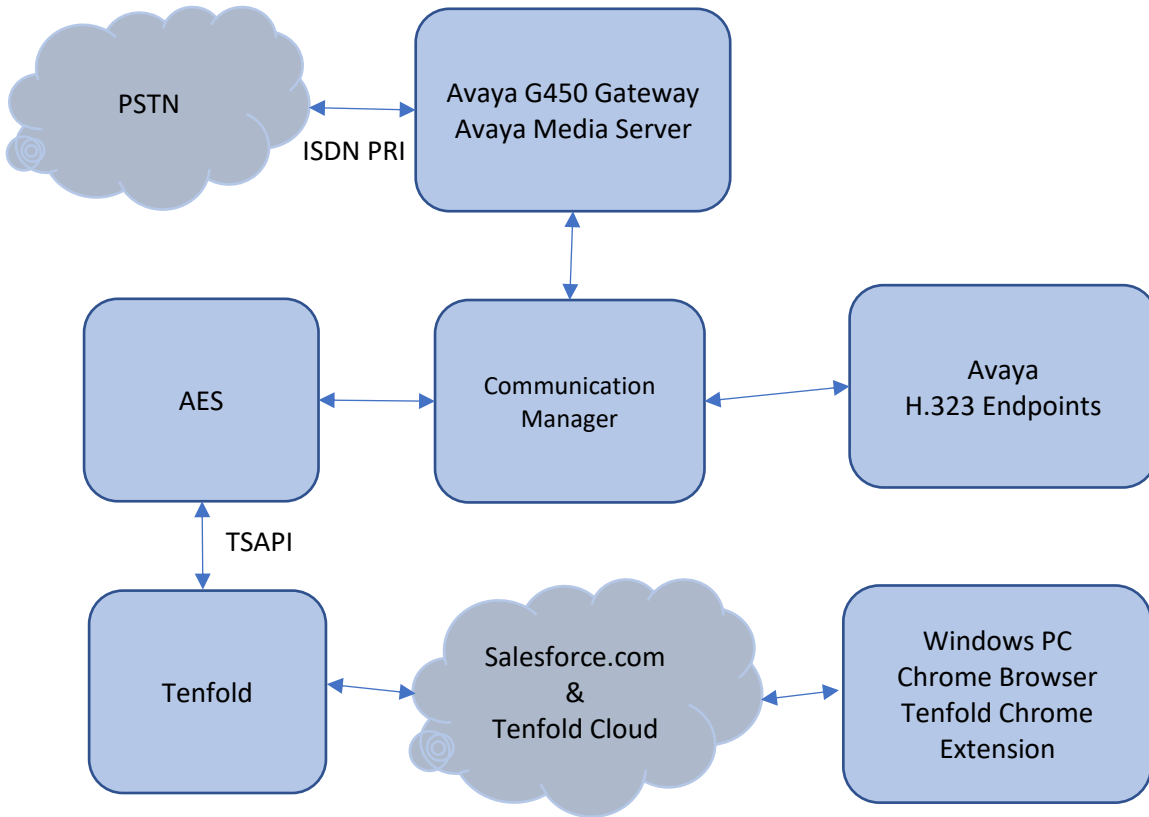
- **Phone:** +1 (415) 599-1170
- **Email:** [support@tenfold.com](mailto:support@tenfold.com)
- **Web:** <https://www.tenfold.com/support-center>

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and AES, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Tenfold monitored the agent stations shown in the table below.

Device Type	Extension
VDNs	59101
Skill Groups	1/59001, 2/59002
Supervisor	51001
Agent Stations	50001 - 50005



**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	8.0.1.1.0-FP1SP1
Avaya G450 Media Gateway	40.20.1
Avaya Aura® Media Server in Virtual Environment	8.0.0.183
Avaya Aura® Application Enablement Services in Virtual Environment	8.0.1.0.2.5-0
Avaya 9611G & 9641G IP Deskphone (H.323)	6.8.1
Tenfold on Microsoft Windows Server 2016 Standard <ul style="list-style-type: none"><li>• Cloud Connect Server</li><li>• Cloud Connect Client</li><li>• Avaya TSAPI Windows Client (csta32.dll)</li></ul>	<ul style="list-style-type: none"><li>• 2-6-12-17161.10644</li><li>• 2-6-12-17161.10644</li><li>• 7.1.1 Build 36</li></ul>
Google Chrome on Microsoft Windows 10 Professional <ul style="list-style-type: none"><li>• Tenfold (Chrome Extension)</li></ul>	73.0.3683.103 <ul style="list-style-type: none"><li>• 3.17.4 (2019.4.10)</li></ul>
Tenfold Cloud	N/A
Salesforce.com	Spring '19

## 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

Note that the connectivity between AES and Communication Manager was pre-configured and was standard in nature. Thus, it is not detailed in this document.

### 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? n                                     DCS Call Coverage? y
ASAI Link Plus Capabilities? n                                     DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? n                             Digital Loss Plan Modification? Y
ATM WAN Spare Processor? n                                         DS1 MSP? y
ATMS? y                                                             DS1 Echo Cancellation? 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: 59999
Type: ADJ-IP
Name: AES CTI Link 1
Unicode Name? n                                                    COR: 1
```

## 6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Tenfold 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 AES.

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



#### Application Enablement Services Management Console

Help

Please login here:

Username

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.



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

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes 'Home', 'Help', and 'Logout'. The left sidebar contains a menu with items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays a 'Welcome to OAM' message. The message states: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. It lists several domains with brief descriptions: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states: 'Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.'

Welcome: User cust  
Last login: Wed Apr 17 16:14:43 2019 from 10.64.10.203  
Number of prior failed login attempts: 0  
HostName/IP: aes8/10.64.110.132  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.2.5-0  
Server Date and Time: Fri Apr 26 15:14:00 MDT 2019  
HA Status: Not Configured

Home | Help | Logout

Home

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

**Welcome to OAM**

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

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

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

## 6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' page selected. The top navigation bar includes 'Home', 'Help', and 'Logout'. The left sidebar menu is expanded to show 'Licensing' with sub-items: WebLM Server Address, WebLM Server Access, and Reserved Licenses. The main content area displays the 'Licensing' page. It provides instructions for setting up and maintaining the WebLM, including the need to use WebLM Server Address, WebLM Server Access, and Reserved Licenses. A note at the bottom states: 'NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page.'

Welcome: User cust  
Last login: Wed Apr 17 16:14:43 2019 from 10.64.10.203  
Number of prior failed login attempts: 0  
HostName/IP: aes8/10.64.110.132  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.2.5-0  
Server Date and Time: Fri Apr 26 15:15:04 MDT 2019  
HA Status: Not Configured

Home | Help | Logout

Licensing

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

**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

**NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page**

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.

- ▼ Application\_Enablement
  - View license capacity
  - View peak usage
- CE
  - ▶COLLABORATION\_ENVIRONMENT
  - CMM
    - ▶Communication\_Manager\_Messaging
      - Configure Centralized Licensing
  - COMMUNICATION\_MANAGER
    - ▶Call\_Center
    - ▶Communication\_Manager
    - ▶Dialog\_Designer
  - IPO
    - ▶IP\_Office
  - MSR
    - ▶Media\_Server
  - ORCHESTRATION\_DESIGNER\_IDE
    - ▶Orchestration\_Designer\_IDE
  - POM
    - ▶POM
  - SYSTEM\_MANAGER
    - ▶System\_Manager
  - SessionManager

**License File Host IDs:** VC-3B-2C-EE-93-9D-01

**Licensed Features**

13 Items
Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	8
AES HA LARGE VALUE_AES_HA_LARGE	permanent	8
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	8
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	8
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	8
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	8
DLG VALUE_AES_DLG	permanent	8
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	8

SmallServerTypes:

### 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**.

Welcome: User cust  
Last login: Wed Apr 17 16:14:43 2019 from 10.64.10.203  
Number of prior failed login attempts: 0  
HostName/IP: aes8/10.64.110.132  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.2.5-0  
Server Date and Time: Fri Apr 26 15:17:25 MDT 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm8	1	7	Both

Add Link Edit Link Delete Link

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the AES 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.

Welcome: User cust  
Last login: Wed Apr 17 16:14:43 2019 from 10.64.10.203  
Number of prior failed login attempts: 0  
HostName/IP: aes8/10.64.110.132  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.2.5-0  
Server Date and Time: Fri Apr 26 15:21:56 MDT 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ TWS

Add TSAPI Links

Link: 2  
Switch Connection: cm8  
Switch CTI Link Number: 1  
ASAI Link Version: 9  
Security: Unencrypted

Apply Changes Cancel Changes

## 6.4. Administer Tenfold 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.



User Management | User Admin | Add User Home | 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 Id	<input type="text" value="tenfold"/>
* Common Name	<input type="text" value="tenfold"/>
* Surname	<input type="text" value="tenfold"/>
* User Password	<input type="password" value="*****"/>
* Confirm Password	<input type="password" value="*****"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>

## 6.5. Administer Security Database

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the left pane, to display list of the CTI Users. **Edit** the user created in previous section and check box for **Unrestricted Access**.



### Application Enablement Services Management Console

Welcome: User cust  
Last login: Wed Apr 17 16:14:43 2019 from 10.64.10.203  
Number of prior failed login attempts: 0  
HostName/IP: aes8/10.64.110.132  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.2.5-0  
Server Date and Time: Fri Apr 26 15:26:13 MDT 2019  
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users

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
      - List All Users
      - Search Users

#### Edit CTI User

User Profile:	User ID Common Name Worktop Name Unrestricted Access	tenfold tenfold NONE ▾ <input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	None ▾
Call and Device Monitoring:	Device Monitoring Calls On A Device Monitoring Call Monitoring	None ▾ None ▾ <input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▾

## 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 shows the Avaya Application Enablement Services Management Console. The top navigation bar includes "Maintenance | Service Controller" and "Home | Help | Logout". The left sidebar shows a tree view with "Maintenance" expanded to "Service Controller". The main content area displays the "Service Controller" page with a table of services and their statuses.

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](#)

Buttons: 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 Tenfold.

In this case, the associated Tlink name is “AVAYA#CM8#CSTA#AES8”.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar shows a tree view with "Security" expanded to "Security Database" and "Tlinks" selected. The main content area displays the "Tlinks" page with a list of Tlink names and a "Delete Tlink" button.

Tlink Name

- AVAYA#CM8#CSTA#AES8
- AVAYA#CM8#CSTA-S#AES8

Buttons: Delete Tlink

## 7. Configure Tenfold

All configuration for Tenfold is performed by Tenfold engineers. As such, the information is not provided in this document.

## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, AES, and Tenfold.

### 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	8	no	aes8	established	18	19

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

On AES, verify status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) from the left pane. 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 number of agent stations from **Section 3** that are monitored by Tenfold, in this case “2”.



### Application Enablement Services Management Console

Welcome: User cust  
 Last login: Fri Apr 26 15:13:59 2019 from 10.64.10.203  
 Number of prior failed login attempts: 0  
 HostName/IP: aes8/10.64.110.132  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 8.0.1.0.2.5-0  
 Server Date and Time: Fri Apr 26 15:45:40 MDT 2019  
 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
  - ▶ Logs
  - ▶ Log Manager

#### TSAPI Link Details

Enable page refresh every  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	cm8	1	Talking	Fri Apr 26 15:18:28 2019	Online	18	1	19	18	30

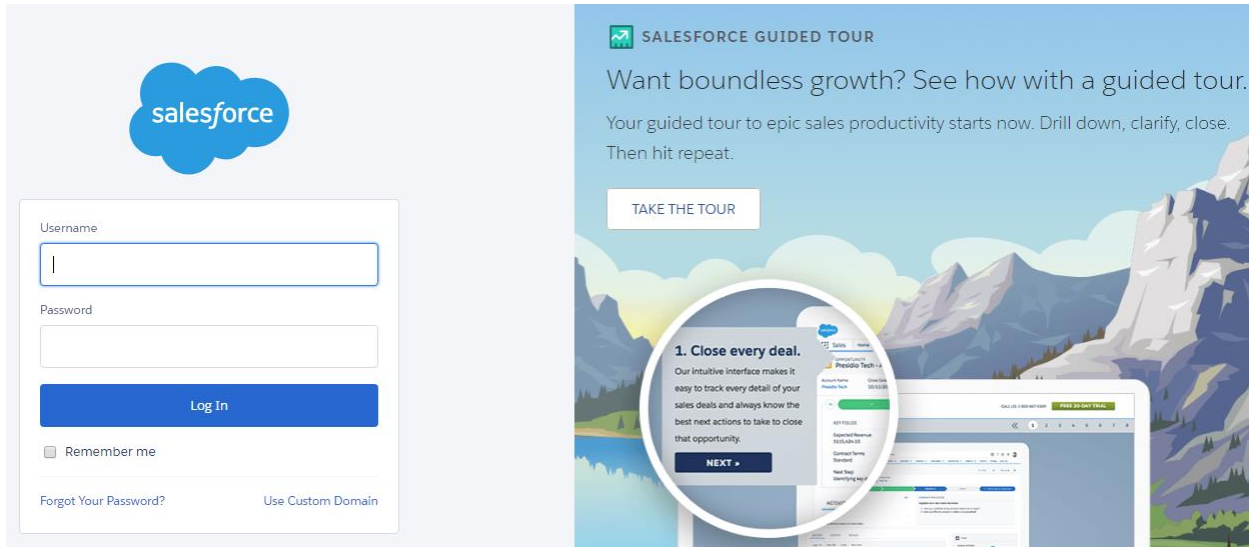
---

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

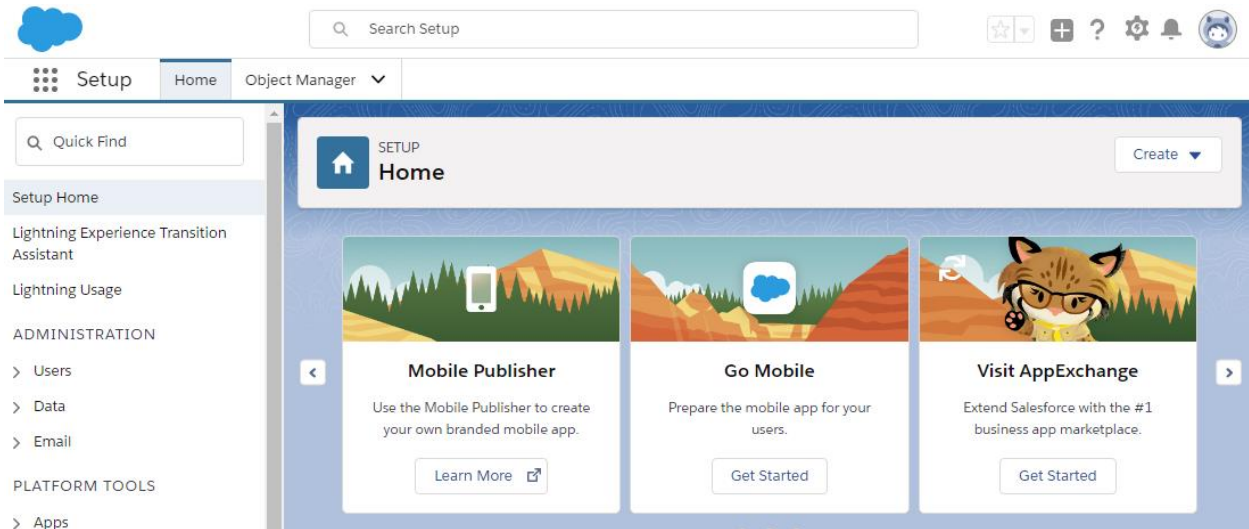


### 8.3. Verify Tenfold

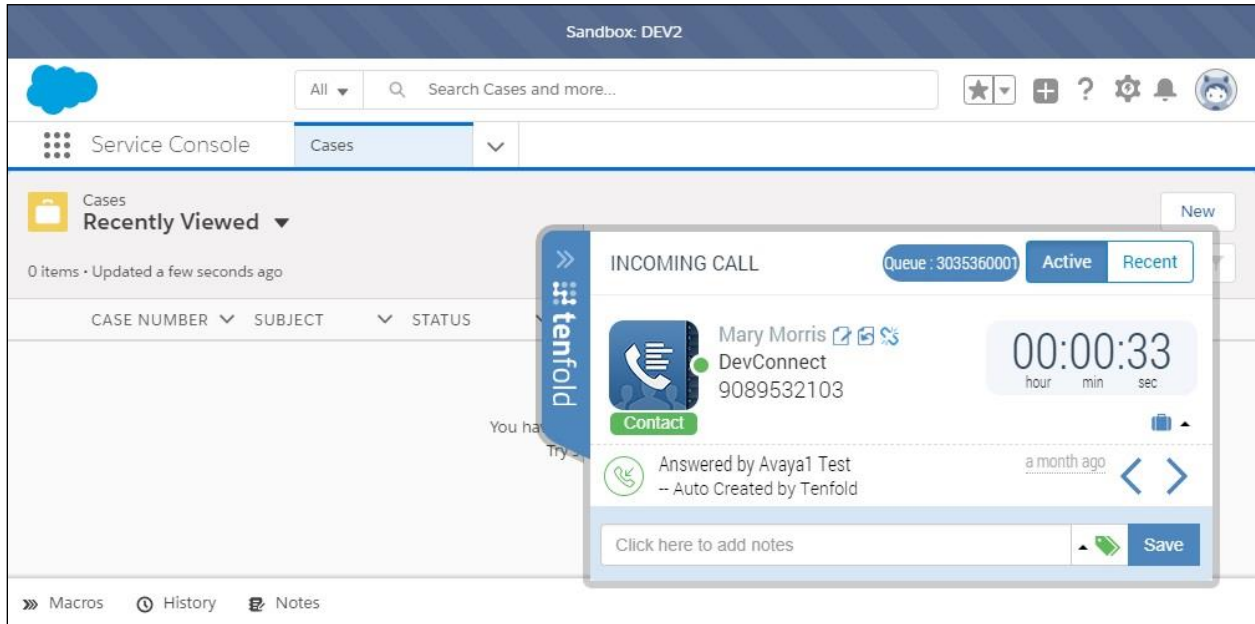
From an agent PC, launch a Chrome browser window and enter the URL provided by Tenfold. Log in with the relevant user credentials provided by Tenfold.



The screen below is displayed next.



Answer the call from the agent telephone. Verify that the call status on Tenfold Chrome Extension is updated to a green dot to reflect answered, as shown below.



## 9. Conclusion

These Application Notes describe the configuration steps required for Tenfold to successfully interoperate with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Application Enablement Services 8.0.1 using Chrome browser and Tenfold Chrome Extension with Salesforce.com. 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 ID 03-300509
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
3. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 8.0*
4. *Avaya AES Integration Overview*, available upon request to Tenfold Support.
5. *User Documentation*, available upon request to Tenfold Support.

---

**©2019 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).