



Avaya Solution & Interoperability Test Lab

Application Notes for Tenfold 3.3 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Salesforce.com – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Tenfold 3.3 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Salesforce.com. Tenfold is a solution that unifies a customer's phone system and CRM platform.

In the compliance testing, Tenfold used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager to provide screen pop, call control, and Click to Dial features from agent desktops that were connected to Tenfold and Salesforce.com.

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 3.3 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Salesforce.com. Tenfold is a solution that unifies a customer's phone system and CRM platform.

In the compliance testing, Tenfold used the Device, Media, and Call Control (DMCC) interface from Application Enablement Services to monitor skill groups and agent stations on Communication Manager to provide screen pop, call control, and Click to Dial features from agent desktops connected to Tenfold and Salesforce.com.

The Tenfold solution consisted of Tenfold Cloud Connect server, Tenfold Cloud hosted on Google Cloud, and Tenfold Embedded UI on Salesforce.com. Tenfold Cloud Connect server is the component that uses DMCC to integrate with Application Enablement Services and resides on a local server provided by Avaya as part of field deployment.

In the compliance testing, each agent desktop used web browser to connect to Tenfold Cloud Connect server, Tenfold Cloud and Salesforce.com.

Upon notification of a call delivered to an agent via DMCC, Tenfold Cloud Connect server shares the information with Tenfold Cloud, which in turn polls the relevant contact record from Salesforce.com and pushes the contact record data onto the agent desktop.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the application, Tenfold automatically used DMCC to monitor skill groups and query agent login information. Upon an agent log in, Tenfold used set agent state to log the agent into the ACD on Communication Manager and requested device monitoring.

For the manual part of testing, incoming ACD calls were placed with available agents that have web browser connections to Tenfold Cloud Connect server, Tenfold Cloud and Salesforce.com. All necessary call actions were initiated from the agent desktops and/or telephones. The Click to Dial calls were initiated by clicking on the contact phone number displayed on the agent desktops from the Salesforce.com web page.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Tenfold Cloud Connect 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 this Application Note, the interface between Avaya systems 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 DMCC logical device services to set agent states, including log in, log out, and work mode changes with support for reason codes and pending aux work.
- Use of DMCC monitoring services to monitor skill groups and agent stations.
- Use of DMCC call control services to support call control and Click to Dial features.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple agents, blind/attended transfer, attended conference, long duration, send DTMF, Click to Dial from contact phone number, pending aux work, and reason codes.

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 Cloud Connect server.

2.2. Test Results

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

- The current Tenfold release does not support SIP agents.
- The current Tenfold release does not support transfer/conference of call to PSTN destination.
- Upon initial log in to the ACD, the Tenfold agent desktop reflected “Unavailable – Meeting” instead of “Unavailable” where “Meeting” is associated with the first configured reason code. This can be resolved by configuration change on the Tenfold Cloud to remove the read-only default setting associated with “Unavailable”.
- By design, Tenfold established two separate DMCC sessions with Application Enablement Services, one for device monitoring and call control and the other for agent state queries.
- By design, after an agent logs out of ACD, Tenfold, and Salesforce.com, Tenfold retained the monitoring on the associated agent station.
- In the conference scenario, when the PSTN party drops from the conference first, each agent desktop continued to reflect connection to the PSTN party.
- After a few Ethernet disruptions to the Tenfold Cloud Connect server, skill group monitors were removed and not re-established. This did not appear to have any negative impact to desktop reflection and handling of subsequent calls.
- For a call that experienced a 60 second Ethernet disruption to the Tenfold Cloud Connect server, the call cannot be dropped from the agent desktop post link recovery. The workaround is to use the agent telephone to drop the active call.
- After a busy out and release of CTI link on Communication Manager, active device monitors were removed on Communication Manager and Application Enablement Services and were not re-established by Tenfold. The workaround is for the administrator to manually restart the tcc.service on the Tenfold Cloud Connect server.

2.3. Support

Technical support on Tenfold can be obtained through the following:

- **Phone:** (415) 599-1170
- **Email:** 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 Application Enablement Services, 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 skill groups and agent stations shown in the table below.

Device Type	Extension
Skill Group	61001, 61002
Agent Station	65001, 65002
Agent ID	65881, 65882
Agent Password	65881, 65882

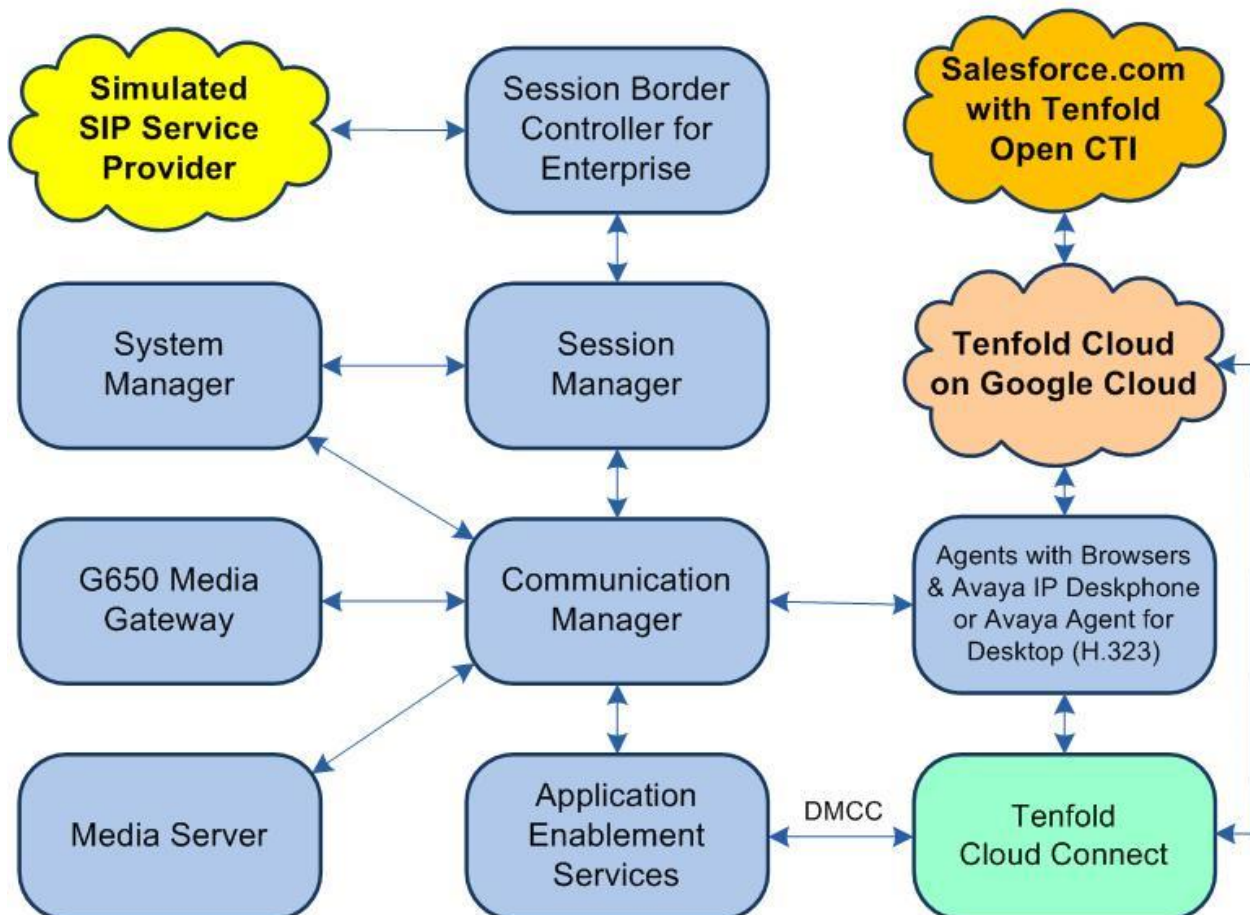


Figure 1: Compliance Testing Configuration

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	8.1.3 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3 (8.1.3.0.0.25-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.2 (8.1.2.0-31-19809)
Avaya Agent for Desktop (H.323)	2.0.6.0.10
Avaya 9611G & J179 IP Deskphone (H.323)	6.8502
Tenfold Cloud Connect on Avaya Linux RedHat <ul style="list-style-type: none">Avaya DMCC XML	3.3.0 8.2.64-AV14EP8 8.0.1
Tenfold Cloud	NA
Tenfold Embedded UI on Salesforce.com	4.60.0 Summer 21

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
- Obtain reason codes
- Obtain skill group data

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?	y	DCS (Basic)?	y		
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y		
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y		

5.2. Administer CTI Link

Add a CTI link using the “**add cti-link n**” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary.

Enter “**ADJ-IP**” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page	1 of	3
CTI LINK				
CTI Link: 1				
Extension: 60111				
Type: ADJ-IP				
		COR: 1		
Name: AES CTI Link				
Unicode Name? n				

5.3. Obtain Reason Codes

For customers that use reason codes, enter the “**change reason-code-names**” command to display the configured reason codes. Make a note of the **Aux Work** reason codes, which will be used later to configure Tenfold.

change reason-code-names		Page	1 of	1
REASON CODE NAMES				
Aux Work/ Interruptible?		Logout		
Reason Code 1:	Meeting	/n		
Reason Code 2:	Lunch	/n		
Reason Code 3:		/n		
Reason Code 4:		/n		
Reason Code 5:		/n		
Reason Code 6:		/n		
Reason Code 7:		/n	Other	
Reason Code 8:		/n		
Reason Code 9:		/n		
Default Reason Code:				

5.4. Obtain Skill Group Data

Use the “**list hunt-group**” command to display a list of pre-configured hunt and skill groups. Make a note of the **Name** and **Ext** for the skill groups from **Section 3**, which will be used later to configure Tenfold.

list hunt-group		HUNT GROUPS									
Grp No.	Name/ Ext	Grp Type	ACD/ MEAS	Vec	MCH	Que	Mem	Cov Path	Notif/ Ctg Adj	Dom Ctrl	Message Center
1	CM Sales Skill 61001	ucd-mia	y/I	SK	none	y	0		n		n
2	CM Support Skill 61002	ucd-mia	y/I	SK	none	y	0		n		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 Tenfold user
- Administer security database
- Administer ports
- Restart services

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" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot shows the AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo and the title "Application Enablement Services Management Console". On the right, a "Welcome" message displays user information: "Welcome: User", "Last login: Tue May 18 10:00:40 2021 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: 8.1.3.0.0.25-0", "Server Date and Time: Tue May 18 11:06:24 EDT 2021", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home", "Help", and "Logout" links. The left sidebar contains a list of menu items: "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. The list includes: "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.", and "Help - Use Help to obtain a few tips for using the OAM Help system". A final paragraph 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."

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" menu item selected in the left sidebar. The top header and "Welcome" message are identical to the previous screenshot. The red navigation bar also remains the same. The left sidebar now highlights "Licensing" and includes sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area is titled "Licensing" and contains three paragraphs of instructions, each followed by a bulleted list of required actions. The first paragraph states: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by "WebLM Server Address". The second paragraph states: "If you are importing, setting up and maintaining the license, you need to use the following:" followed by "WebLM Server Access". The third paragraph states: "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by "Reserved Licenses".

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. Note that the TSAPI license is used for device monitoring and call control via DMCC, and that no specific DMCC license is required for integration with Tenfold.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a navigation tree with the following items: WebLM Home, Install license, Licensed products, APPL_ENAB, Application_Enablement (expanded), View by feature, View by local WebLM, Enterprise configuration, Local WebLM Configuration, Usages, Allocations, Periodic status, ASBCE, Session_Border_Controller_E_AE, Avaya_Proactive_Contact, CCTR, ContactCenter, and COMMUNICATION_MANAGER. The right pane displays the 'Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license)' screen. It includes a breadcrumb trail: 'You are here: Licensed Products > Application_Enablement > View by Feature'. Below this, it states 'License installed on: August 8, 2019 4:43:51 PM -05:00' and 'License File Host IDs: VE-83-02-2D-26-52-01'. A table lists the features and their license capacities:

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3
DLG (VALUE_AES_DLG)	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16

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".

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 with the "Add TSAPI Links" screen displayed. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. 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. 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 12, and Security is set to Unencrypted. Below the fields are buttons for "Apply Changes" and "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.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue May 18 10:00:40 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue May 18 11:08:38 EDT 2021
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 Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

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 that both parameters are unchecked, as shown below.

In the case that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Tenfold 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". On the right, a welcome message for the user "User" is shown, along with login details: "Last login: Tue May 18 10:00:40 2021 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: 8.1.3.0.0.25-0", "Server Date and Time: Tue May 18 11:06:24 EDT 2021", and "HA Status: Not Configured".

The main navigation bar is red and contains the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various management categories, with "Security" expanded to show sub-items: "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database", and "Control". The "Control" item is 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 checkboxes is an "Apply Changes" button.

6.6. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue May 18 10:00:40 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue May 18 11:06:24 EDT 2021
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port

9999

Enabled Disabled

☒ ☐

Encrypted TCP Port

☒ ☐

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port

450

Enabled Disabled

☒ ☐

Local TLINK Ports

TCP Port Min

1024

TCP Port Max

1039

Unencrypted TLINK Ports

TCP Port Min

TCP Port Max

Encrypted TLINK Ports

TCP Port Min

TCP Port Max

DMCC Server Ports

Unencrypted Port

Enabled Disabled

☒ ☐

Encrypted Port

☒ ☐

TR/87 Port

☒ ☐

6.7. Restart Services

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue May 18 10:00:40 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue May 18 11:06:24 EDT 2021
HA Status: Not Configured

Maintenance | Service ControllerHome | 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 checked="" 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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

7. Configure Tenfold

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

- Administer config.properties
- Restart service

Prior to integration, Tenfold consults with the customer to create needed configuration file depending on customer use of agent status features, dialing rules, internal phone extension lengths, etc.

The configuration of Tenfold is performed by the Tenfold Implementation team and the procedural steps are presented in these Application Notes for information purposes only.

7.1. Administer config.properties

Log in to the Linux shell of Tenfold via SSH. Navigate to the **/opt/tenfold/tcc** directory and open the **config.properties** file with a text editor such as **vi**.

```
[xxxx@dr-tenfold ~]$ cd /opt/tenfold/tcc  
[xxxx@dr-tenfold tcc]# sudo vi config.properties
```

Navigate to the **avayaaes** sub-section. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **skill.extension:** Skill sequence starting with 1 and name and extension from **Section 5.4**.
- **duration:** Recommended session and refresh duration in seconds by Tenfold.
- **callserver:** IP address of Communication Manager.
- **switchname:** The switch connection name from **Section 6.3**.
- **cmapi.server.ip:** IP address of Application Enablement Services.
- **cmapi.username:** The Tenfold user credentials from **Section 6.4**.
- **cmapi.password:** The Tenfold user credentials from **Section 6.4**.
- **access.code:** Comment out these two parameters since not used.
- **reason:** Reason code names from **Section 5.3**.
- **reasoncode:** Reason code values from **Section 5.3**.

```
avayaaes.skill.extension=[{"id":"1","name":"CM Sales Skill","extension":"61001"}, {"id":"2","name":"CM Support Skill","extension":"61002"}]

avayaaes.agentstatus.requested.session.duration=7200
avayaaes.agentstatus.session.refresh.duration=7200
avayaaes=true
avayaaes.callserver=10.64.101.236
avayaaes.switchname=cm7
avayaaes.cmapi.server.ip=10.64.101.239
avayaaes.cmapi.username=tenfold
avayaaes.cmapi.password=Tenfold123!
avayaaes.ignoreexternaladdress=false
#avayaaes.login.agent.feature.access.code=120
#avayaaes.logout.agent.feature.access.code=125
## AE Server client connection port: 4721(non-SSL) or 4722(SSL)
avayaaes.cmapi.server.port=4721
## Legal values for cmapi1.secure are true (for port 4722) and false (for port 4721).
avayaaes.cmapi.secure=false

##conference mode
##mode1 is send a 3 connected event
##mode2 is 2 connected
avayaaes.conferencemode=mode2
#
avayaaes.agentstatus.notready=NotReady
avayaaes.agentstatus.notready.reason=Meeting,Lunch
avayaaes.agentstatus.notready.reasoncode=1,2
avayaaes.agentstatus.logoutstatus=LoggedOut
avayaaes.agentstatus.loginstatus=LoggedIn
avayaaes.agentstatus.wrapupstatus=WorkingAfterCall
avayaaes.agentstatus.userreadystatus=Ready
```

Restart the **tcc.service** as shown below.

```
[xxxx@dr-tenfold tcc]# sudo systemctl restart tcc.service
```

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, 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	Rcvd
1	12	no	aes7	established	1440	1424

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, 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 monitored skill groups and agents that have been logged in from **Section 3**, in this case “**4**”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 28 10:56:43 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 28 11:32:47 EDT 2021
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

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 Sep 28 10:56:03 2021	Online	18	4	1424	1440	30

Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows two active sessions with the Tenfold user name from **Section 6.4** and that the session with “**cmapiApplication**” reflects the number of agents that have been logged in in the **# of Associated Devices**.

Note that the “**cmapiApplication**” session is used by Tenfold for device monitoring and call control, and the “**Tenfold-tcc-aes-cert-org**” session is used by Tenfold for agent state queries.



Application Enablement Services
 Management Console

Welcome: User
 Last login: Tue Sep 28 10:48:04 2021 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: 8.1.3.0.0.25-0
 Server Date and Time: Tue Sep 28 11:06:35 EDT 2021
 HA Status: Not Configured

Status | Status and Control | **DMCC Service Summary**
Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ **Status**

Alarm Viewer

▶ Logs

▶ Log Manager

▼ **Status and Control**

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ **DMCC Service Summary**

▪ Switch Conn Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Tue Sep 28 11:06:30 EDT 2021

Service Uptime:
0 days, 0 hours 9 minutes

Number of Active Sessions:
2

Number of Sessions Created Since Service Boot:
5

Number of Existing Devices:
0

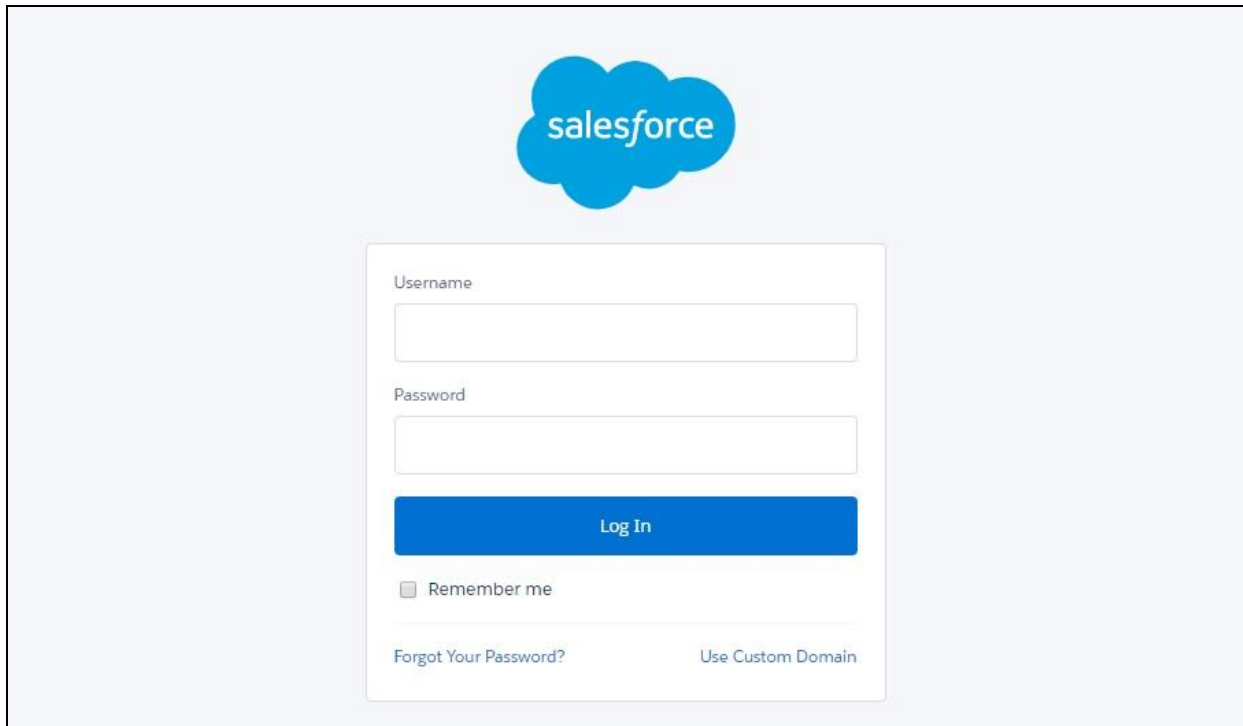
Number of Devices Created Since Service Boot:
0

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	E950D61FC17BBBE8E 29552FD7EB35A16-3	tenfold	cmapiApplication	10.64.101.205	XML Unencrypted	2
<input type="checkbox"/>	10DB819C066D95999 BD25F19BAD61260-4	tenfold	Tenfold-tcc-aes-cert-org	10.64.101.205	XML Unencrypted	0

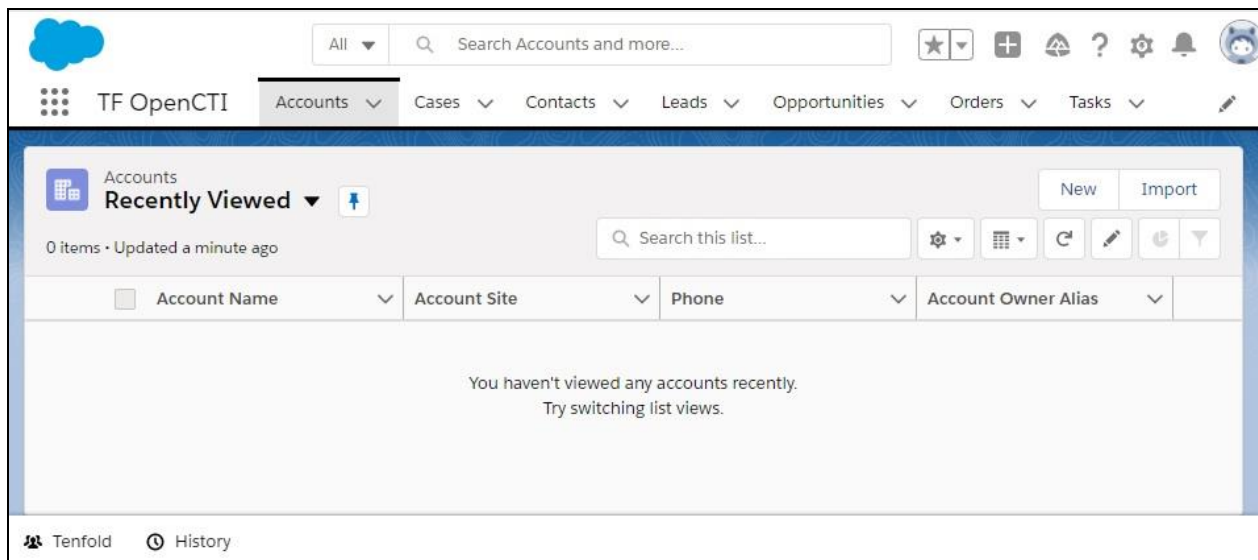
Terminate Sessions
Show Terminated Sessions

8.3. Verify Tenfold

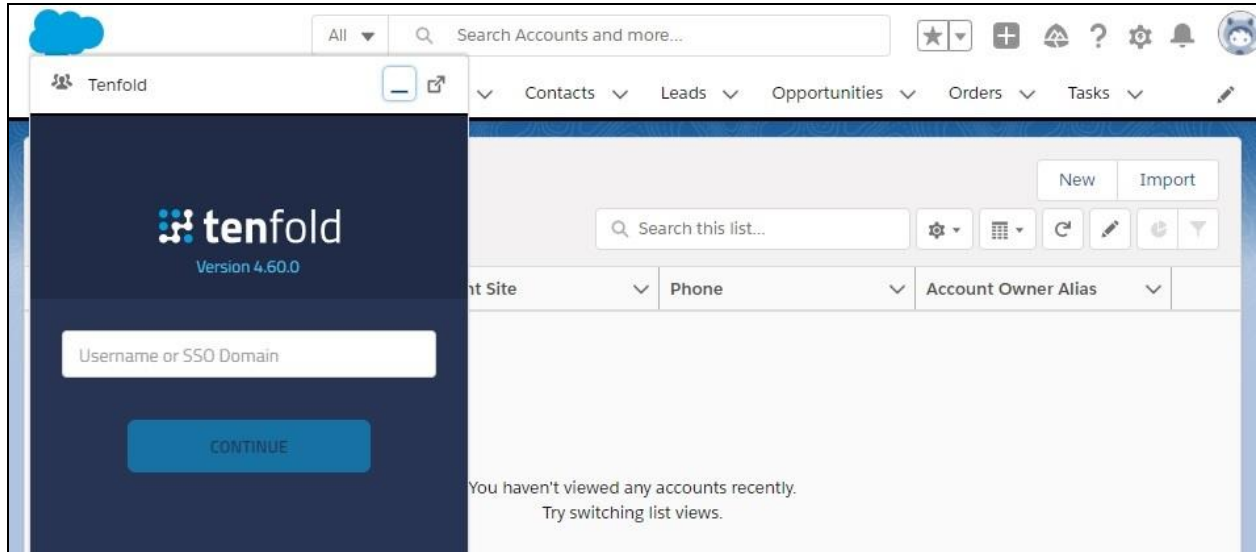
From an agent PC, launch an Internet browser window and enter the URL provided by the end customer for Salesforce.com. Log in with the relevant user credentials provided by the end customer.



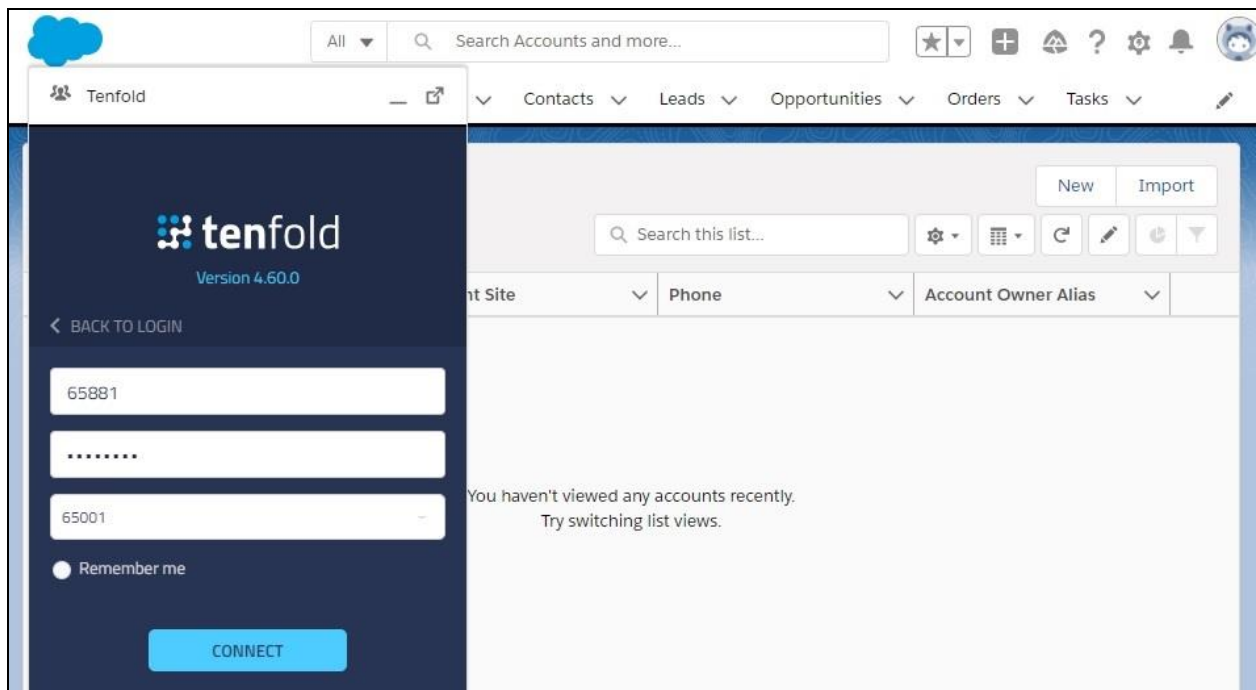
The screen below is displayed next. Select **Tenfold** from the bottom of screen.



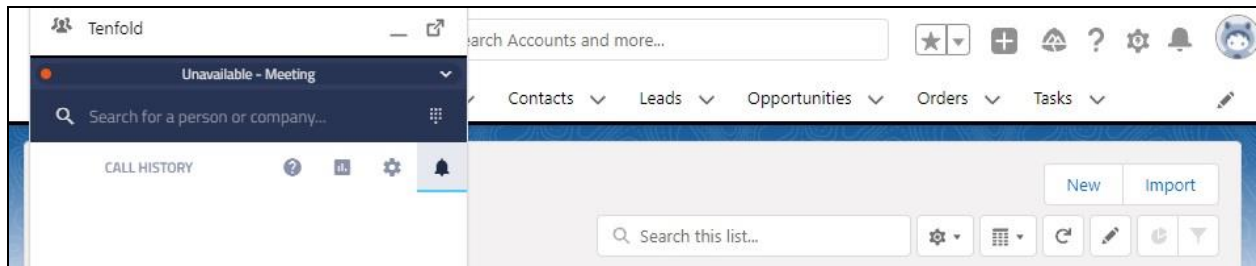
The **Tenfold** screen is displayed. Log in with the appropriate credentials provided by Tenfold.



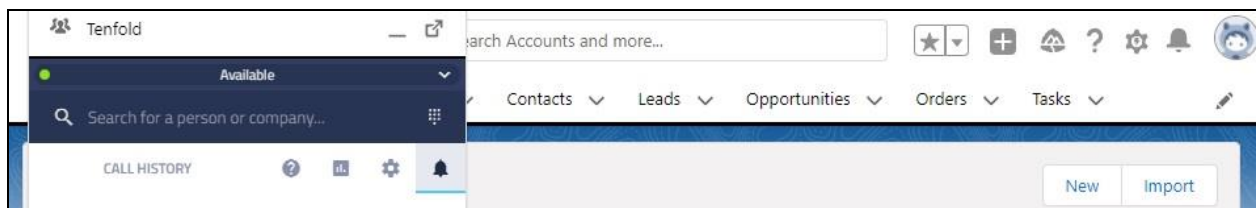
The **Tenfold** screen below is displayed next. Enter the relevant agent ID, agent password, and station extension from **Section 3** and click **CONNECT**.



Verify that the **Tenfold** screen is updated as shown below. Expand the drop-down icon next to **Unavailable – Meeting** and select **Available** (not shown).

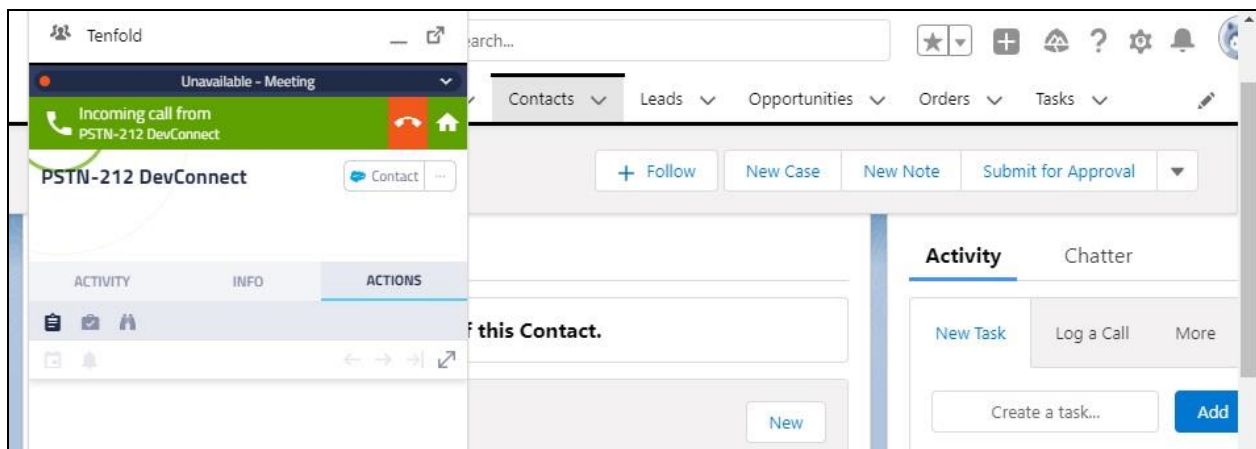


Verify that the **Tenfold** screen is updated to reflect **Available**.

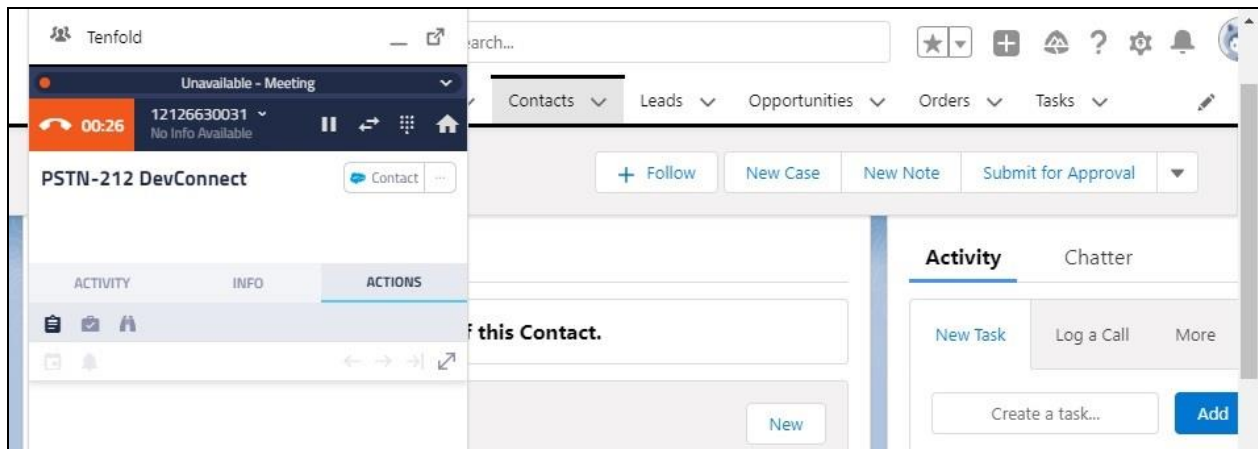


Make an incoming ACD call from the PSTN. Verify that the **Tenfold** screen is updated to reflect the incoming call. Also verify that the name obtained from the uniquely matching contact record associated with the PSTN caller number is displayed as shown below, in this case **"PSTN-212 DevConnect"**.

Click on the green incoming call area on the **Tenfold** screen to answer the call.



Verify that the agent is connected to the PSTN caller with two-way talk path, and that the **Tenfold** screen is updated to reflect a connected call along with the number of the PSTN caller as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Tenfold 3.3 to successfully interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3 using 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*, Release 8.1.x, Issue 8, November 2020, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at <http://support.avaya.com>.
3. *Avaya AES Integration Overview*, available upon request to Tenfold Support.
4. *User Documentation*, available upon request to Tenfold Support.

©2021 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.