



Application Notes for Tenfold with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 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 7.1 and Avaya Aura® Application Enablement Services 7.1 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 7.1 and Avaya Aura® Application Enablement Services 7.1 using Tenfold Chrome Extension with 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 (TSAPI) from Application Enablement Services 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 with Chrome browser and enabled Tenfold Chrome Extension. The Tenfold Chrome Extension is a plugin that enables call floating UI for agents, and is 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 Application Enablement Services 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 notified via TSAPI events of a call delivered to an agent, the Tenfold server shares the information with 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 Application Enablement Services, 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.

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 Application Enablement Services 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 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:

- The current release of Tenfold does not support reflection of attended transfer, conference, internal call, and multiple calls.
- By design, agents are required to complete a call with an external party using the assigned extension, in order for the assigned extension to be recognized and associated with the agent. Similarly, when an agent wishes to use a different extension, then the agent's user profile needs to be updated with the new extension along with completion of a call from that extension with an external party.
- In the event that the calling party number was not passed from the PSTN, no indication was provided on the Tenfold Chrome Extension. Tenfold shared that in cases where PSTN passes "Anonymous", then a no match indication can be 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.
- Click to Dial to international destinations were unsuccessful due to no auto insertion of 011 as US exit code. Tenfold shared that this can be made to work as part of an initial onboarding process to configure the required exit code insertion, and the onboarding process wasn't verified in the compliance testing.

- After a busy out and release of CTI link commands on Communication Manager, active station 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 services on the Tenfold server.
- By design, when the Ethernet connection to the Tenfold server was disrupted for 30 seconds, an active call that had stayed up during and post the server recovery was reflected as dropped.
- When the Ethernet connection to the Tenfold server was disrupted for 60 seconds, then 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:** (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 agent stations shown in the table below.

Device Type	Extension
VDNs	60001, 60002
Skill Groups	61001, 61002
Supervisor	65000
Agent Stations	65001, 66002

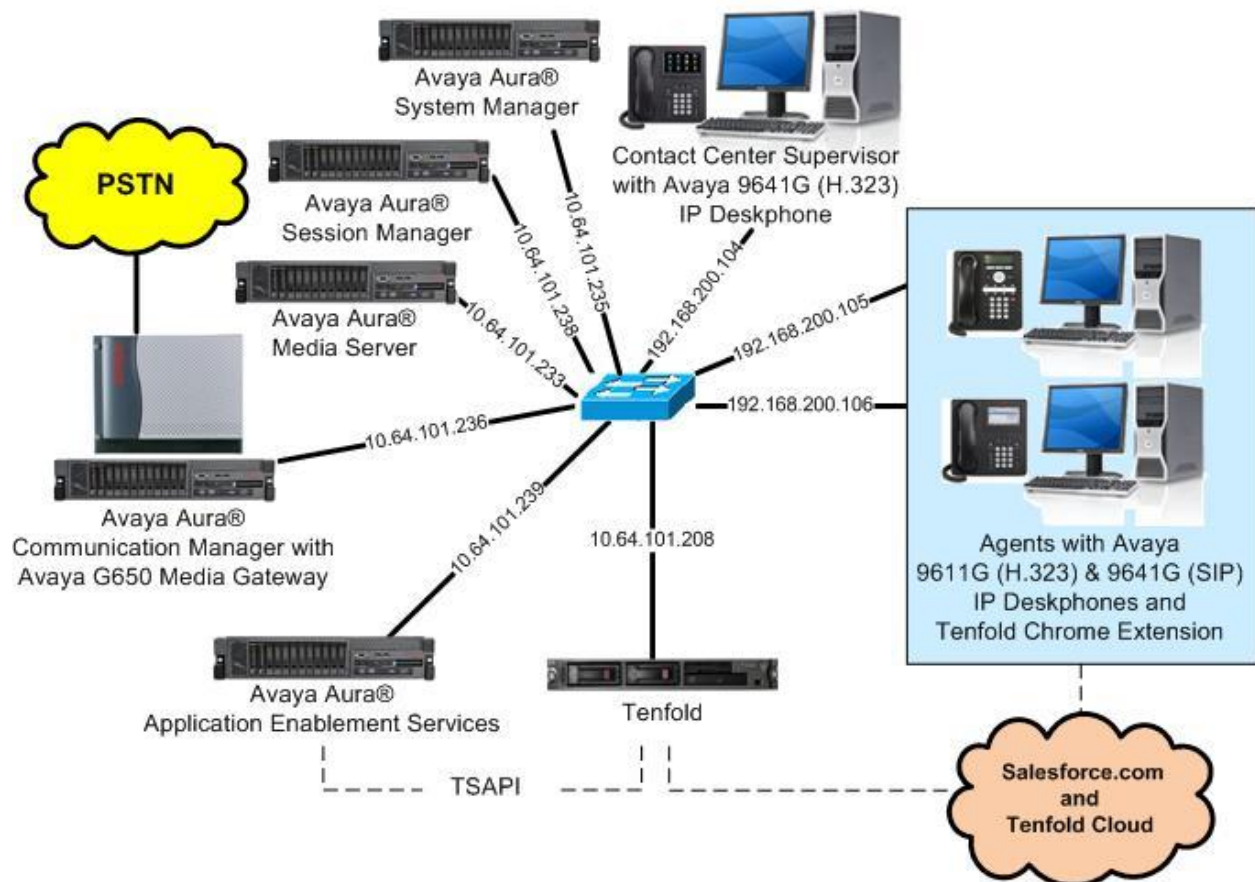


Figure 1: Compliance Testing Configuration

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	7.1.3 (7.1.3.0.0.532.24515)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.8.0.384
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.3 (7.1.3.0.1.7-0)
Avaya Aura® Session Manager in Virtual Environment	7.1.3 (7.1.3.0.713014)
Avaya Aura® System Manager in Virtual Environment	7.1.3 (7.1.3.0.037763)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6604
Avaya 9641G IP Deskphone (SIP)	7.1.1.0.9
Tenfold on Microsoft Windows Server 2012 <ul style="list-style-type: none">Cloud Connect ServerCloud Connect ClientAvaya TSAPI Windows Client (csta32.dll)	NA R2 Standard 2.6.12.17148.9619 1.11.6.0 7.1.1.36
Google Chrome on Microsoft Windows 10 <ul style="list-style-type: none">Tenfold (Chrome Extension)	69.0.3497.100 Pro 3.15.1 (2018.8.290)
Tenfold Cloud	NA
Salesforce.com	Summer 18

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

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: 60111		
Type: ADJ-IP		
COR: 1		
Name: AES CTI Link		

6. Configure Avaya Aura® Application Enablement Services

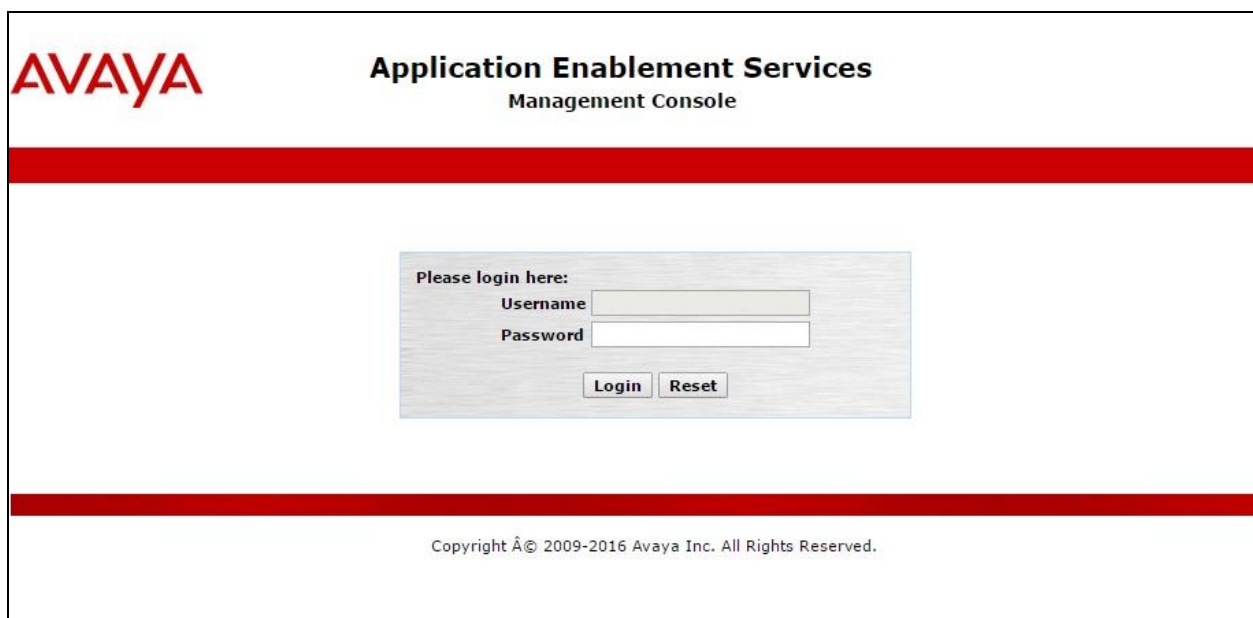
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Tenfold user
- Administer security database
- 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 spans the width of the page below the header. 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 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 Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0", "Server Date and Time: Tue Jul 24 10:52:54 EDT 2018", 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 displays the "Welcome to OAM" message, which 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:" followed by a bulleted list of domains and their functions. At the bottom, it notes that these domains can be served by one administrator for all domains or a separate administrator for each domain.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0
Server Date and Time: Tue Jul 24 10:52:54 EDT 2018
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 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 now shows "Licensing" as the active page, with "Home", "Help", and "Logout" links. The left sidebar highlights "Licensing" and shows sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, import licenses, and administer reserved licenses. It includes a bulleted list of required actions: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses".

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0
Server Date and Time: Tue Jul 24 10:52:54 EDT 2018
HA Status: Not Configured

Licensing | 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

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.

AVAYA
Aura® System Manager 7.1

Last Logged on at: Go...

Home Licenses

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
CIE
► CIE
CMM
► Communication_Manager_Messaging
Configure Centralized Licensing
COMMUNICATION_MANAGER
► Call_Center
► Communication_Manager
Configure Centralized Licensing
MESSAGING
► Messaging
MSR
► Media_Server
SYSTEM_MANAGER
► System_Manager

Application Enablement (CTI) - Release: 7 - SID: 10503000

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: February 23, 2018 7:13:58 PM +00:00

License File Host IDs: V8-7A-42-06-D9-59-01

Licensed Features

10 Items Show All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	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 right corner displays user information: Welcome: User, Last login: Tue Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0, Server Date and Time: Tue Jul 24 10:52:54 EDT 2018, HA Status: Not Configured. The left navigation pane shows the hierarchy: AE Services > TSAPI > TSAPI Links. The main content area is titled "TSAPI Links" and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are 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" form. The left navigation pane shows the hierarchy: AE Services > TSAPI > TSAPI Links. The main content area is titled "Add TSAPI Links" and contains the following fields: Link (dropdown menu with value 1), Switch Connection (dropdown menu with value cm7), Switch CTI Link Number (dropdown menu with value 1), ASAI Link Version (dropdown menu with value 8), and Security (dropdown menu with value 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0
Server Date and Time: Tue Jul 24 10:52:54 EDT 2018
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 event 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 Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0", "Server Date and Time: Tue Jul 24 10:52:54 EDT 2018", and "HA Status: Not Configured".

The main navigation bar is red and contains the links "Security | Security Database | Control" and "Home | Help | Logout". The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected).

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services". It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0
Server Date and Time: Tue Jul 24 10:52:54 EDT 2018
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 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

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#CM7#CSTA#AES7”.

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 is shown, along with login details: "Last login: Tue Jul 24 09:18:47 2018 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: 7.1.3.0.1.7-0", "Server Date and Time: Tue Jul 24 10:52:54 EDT 2018", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks" (selected).

The main content area is titled "Tlinks" and shows a single Tlink entry with the name "AVAYA#CM7#CSTA#AES7". Below the name is a "Delete Tlink" button.

7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:

Password:

[Change Password](#)

7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management**. Select **User Management** → **Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.

AVAYA
Aura® System Manager 7.1

Last Logged on at:

Home / Users / User Management / Manage Users

Search

User Management

Users

3 Items All

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

AVAYA
Aura® System Manager 7.1

Last Logged on at: [] Go...

Home / Users / User Management / Manage Users

User Profile Edit: 66002@dr220.com [Commit & Continue]

Communication Profile

Communication Profile Password: [] [Edit]

[New] [Delete] [Done] [Cancel]

Name

☒ Primary

Select : None

* Name: [Primary]

Default : ☒

Communication Address

[New] [Edit] [Delete]

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	dr220.com

Select : All, None

☒ **Session Manager Profile**

☒ **CM Endpoint Profile**

* System: [DR220-CM7-ES]

* Profile Type: [Endpoint]

Use Existing Endpoints: ☐

* Extension: [66002] [Endpoint Editor]

Display Extension Ranges: []

Template: [Select/Reset]

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.1

Last Logged on at: [] Go...

Home / Users / User Management / Manage Users

Edit Endpoint

System DR220-CM7-ES **Extension** 66002
Template Select **Set Type** 9641SIPCC
Port S00004 **Security Code** []
Name Avaya, SIP 2

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Profile Settings (P)		Group Membership	
* Class of Restriction (COR)	1	* Class Of Service (COS)	1				
* Emergency Location Ext	66002	* Message Lamp Ext.	66002				
* Tenant Number	1	Type of 3PCC Enabled Avaya ▼					
* SIP Trunk	Qaar	Coverage Path 2					
Coverage Path 1	1	Localized Display Name		Avaya, SIP 2			
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control		system ▼			
Multibyte Language	Not Applicable ▼						

*Required

8. Configure Tenfold

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

- Launch Cloud Connect Server Configuration
- Administer telephone system
- Administer extensions
- Assign extensions to users
- Associate user extensions

8.1. Launch Cloud Connect Server Configuration

At the conclusion of installation, the **Cloud Connect Server Configuration** screen is displayed on the Tenfold server. Select **Classic menu**.



8.2. Administer Telephone System

Select **Equipment** → **Avaya Certification** → **Telephone system** from the left pane, where **Avaya Certification** is the pre-created equipment site name. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** “Avaya CM”
- **Trunk access:** The applicable trunk access code for the network, in this case “9”.
- **TSAPI server:** The IP address of Application Enablement Services.
- **TSAPI stream:** The Tlink name from **Section 6.7**.
- **TSAPI username:** The Tenfold user credentials from **Section 6.4**.
- **Password:** The Tenfold user credentials from **Section 6.4**.

Click **Save** to save the configuration, followed by **Start** to start the connectivity.

Cloud Connect Server Configuration

Telephone System

Status: Offline Start

Configuration

Type: Avaya CM

PBX IP address: 1.1.1.1

Username:

Password:

Auto create: ☒ Force now

Trunk access: 9

TSAPI server: 10.64.101.239 [view notes](#)

TSAPI stream: AVAYA#CM7#CSTA#AES7

TSAPI username: tenfold Password:

Two sets of credentials are required. The first is for the telephone system. The second is for the TSAPI server.

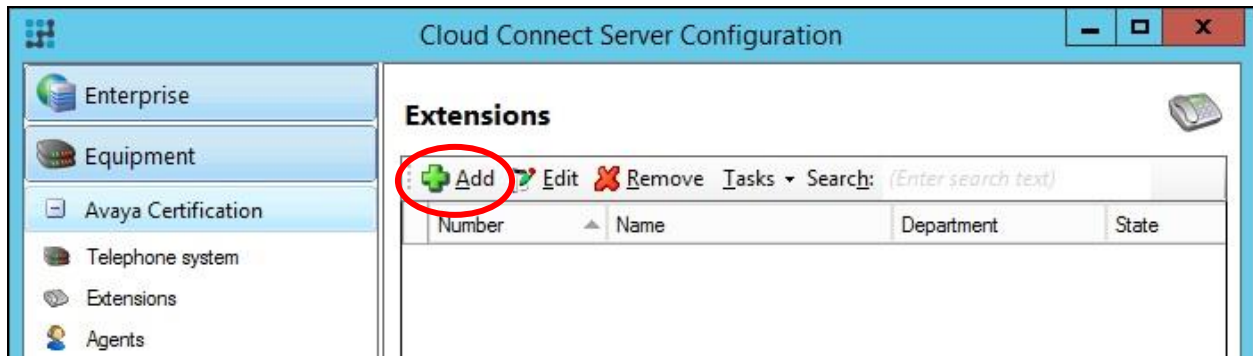
Log: 08:06:39.0 Logging started...

Save Cancel

Version: 2.6.12.17148.9619

8.3. Administer Extensions

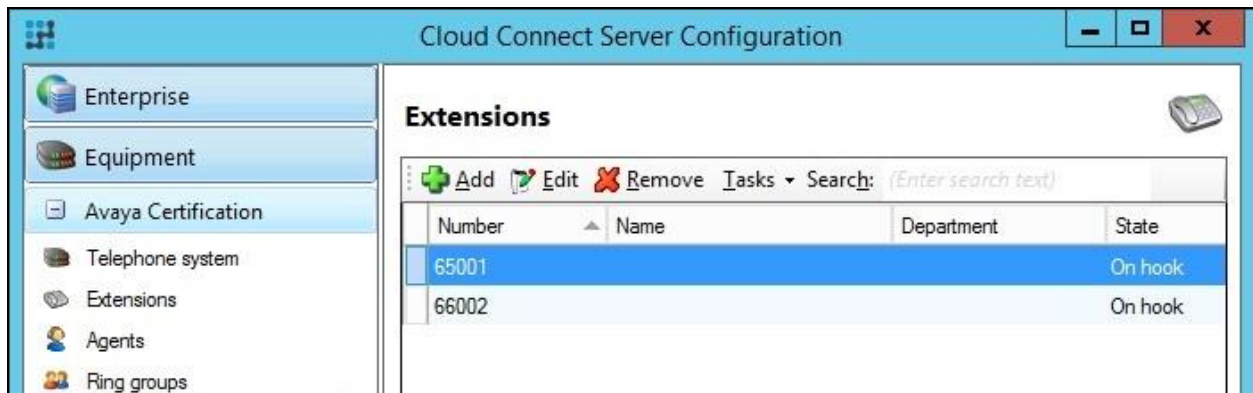
Select **Equipment** → **Avaya Certification** → **Extensions** from the left pane, where **Avaya Certification** is the pre-created equipment site name. Click **Add**.



The **Extension** screen is displayed next. For **Number**, enter the first agent station extension from **Section 3**, and retain the default value in the remaining fields.

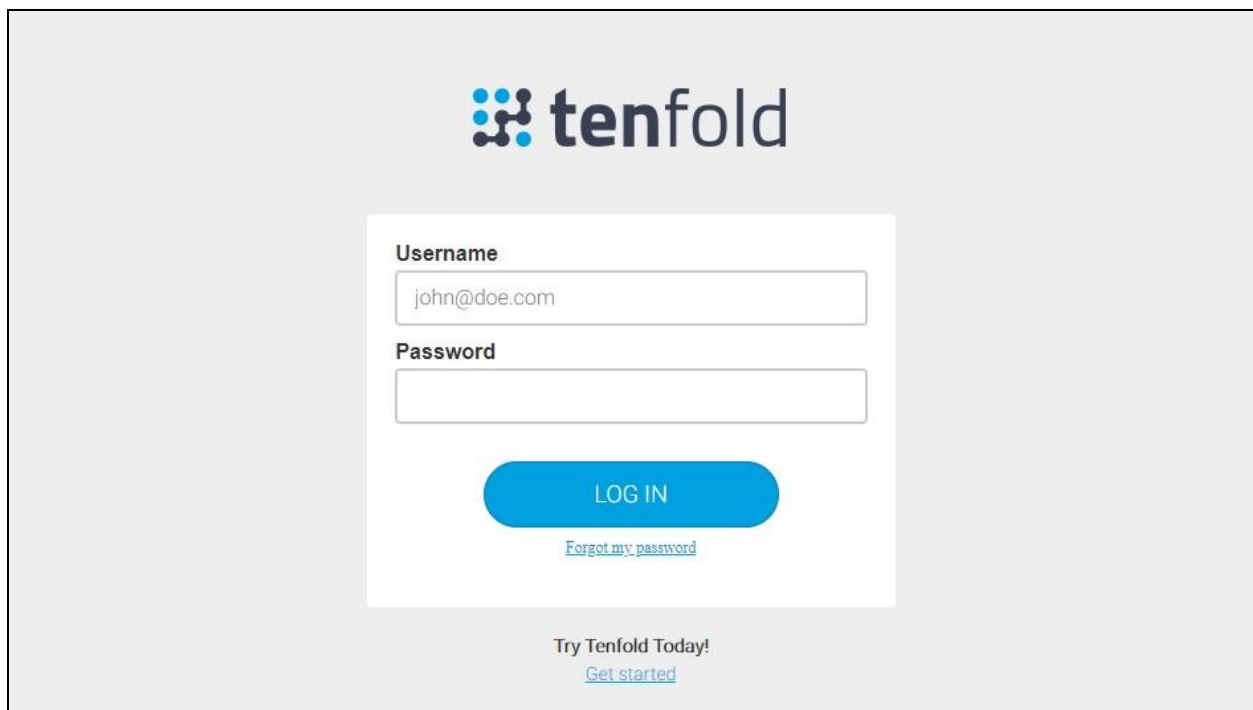
The screenshot shows the 'Extension' configuration dialog box. It has two tabs: 'Extension' and 'Advanced'. The 'Extension' tab is active. It contains several input fields: 'State' (empty), 'Number' (containing '65001'), 'Name' (empty), 'Department' (a dropdown menu), and 'DDI number' (empty). To the right of the 'State' field is a small telephone handset icon. Below these fields is a section titled 'Options' containing eight checkboxes arranged in two columns. The first column has: 'Ignore answer messages', 'Analog handset/Mobex', 'Used as main number', and 'Hide status'. The second column has: 'Do not monitor', 'Use name from telephone system' (which is checked), 'Requires logged in user', and 'Keep call details private'. At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

Repeat this section to add an extension for each agent station from **Section 3**. In the compliance testing, two extensions were added as shown below.

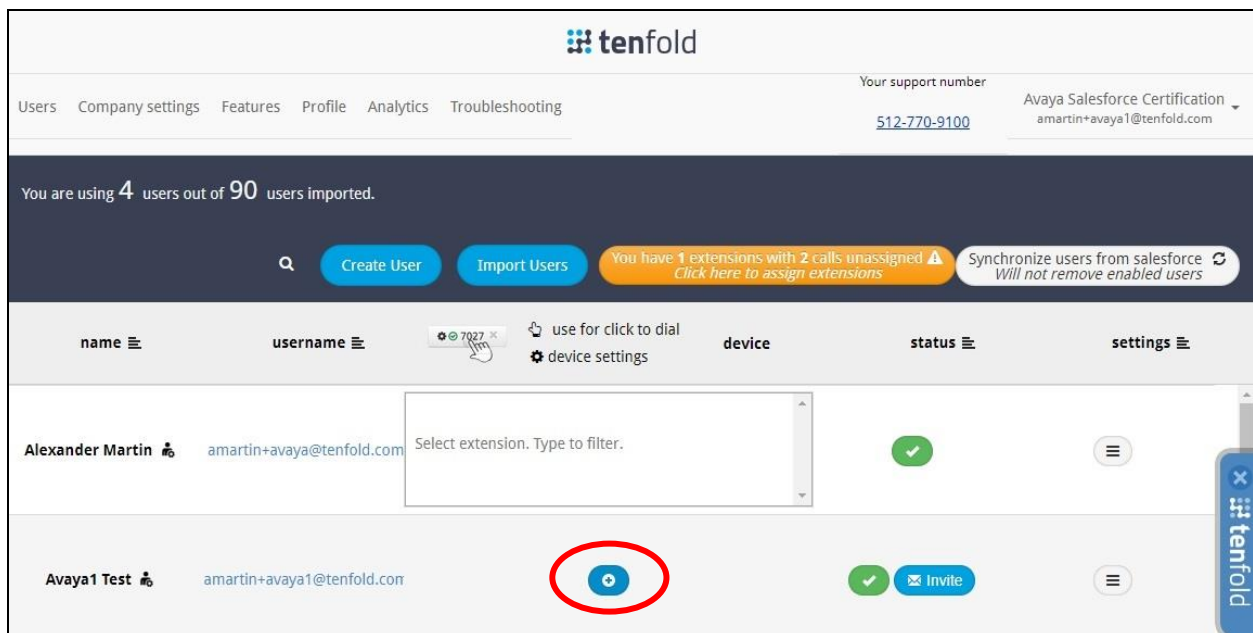


8.4. Assign Extensions to Users

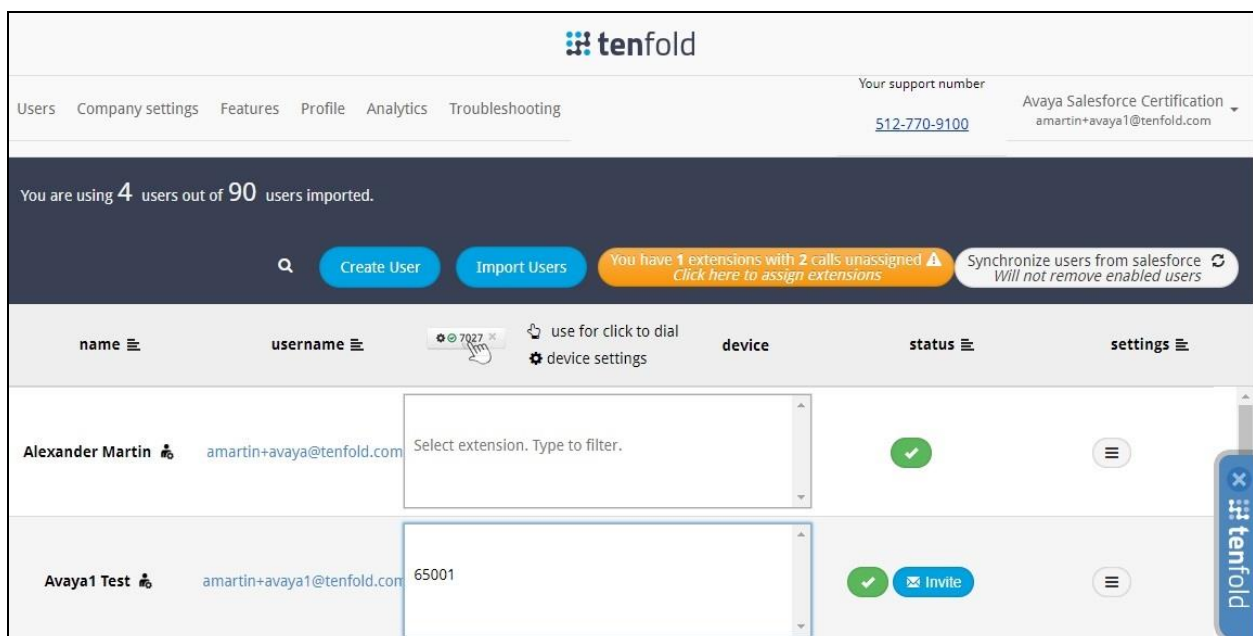
Access the Tenfold web-based interface by using the URL “https://dashboard.tenfold.com” in an Internet browser window. The screen below is display. Log in using an administrative credential from Tenfold.



In the subsequent screen, select **Users** from the top menu to display a list of pre-configured users. Locate the first pre-created user that will be used by the agents, in this case user “Avaya1Test”. Click on the add icon associated with the user, as shown below.



The screen is updated with an extension box for the user. Enter the relevant extension from **Section 8.3** that will be used by the user, in this case “65001”.



Repeat this section to assign extensions to all agent users. In the compliance testing, extensions were assigned to two agent users, as shown below.

The screenshot shows the Tenfold user management interface. At the top, there's a navigation bar with links: Users, Company settings, Features, Profile, Analytics, Troubleshooting. On the right, it shows 'Your support number' as 512-770-9100 and 'Avaya Salesforce Certification' with the email amartin+avaya1@tenfold.com. Below this, a status bar indicates 'You are using 4 users out of 90 users imported.' and buttons for 'Create User', 'Import Users', and 'Synchronize users from salesforce'. A warning message states 'You have 1 extensions with 2 calls unassigned. Click here to assign extensions.' The main table lists two users: 'Avaya1 Test' with username 'amartin+avaya1@tenfold.com' and extension '65001', and 'Avaya2 Test' with username 'amartin+avaya2@tenfold.com' and extension '66002'. Each user row has a green checkmark, an 'Invite' button, and a settings icon.

8.5. Associate User Extensions

Each agent is required to complete a call with an external party, in order for the assigned extension to be recognized and associated for the agent user. Once associated, then the assigned extensions are updated as shown below.

This screenshot shows the same Tenfold user management interface as the previous one, but with the extension numbers updated. The 'Avaya1 Test' user now has extension '65001' and the 'Avaya2 Test' user has extension '66002'. The interface elements, including the navigation bar, status bar, and warning message, are identical to the previous screenshot. The table shows the updated extension numbers for both users, and each row still has a green checkmark, an 'Invite' button, and a settings icon.

9. Verification Steps

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

9.1. 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	aes7	established	24	26

9.2. 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 agent stations from **Section 3** that are monitored by Tenfold, in this case “2”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Fri Sep 7 09:50:33 2018 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: 7.1.3.0.1.7-0
Server Date and Time: Fri Sep 07 11:00:34 EDT 2018
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

▼ 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	Mon Jun 11 10:48:28 2018	Online	17	2	27	25	30

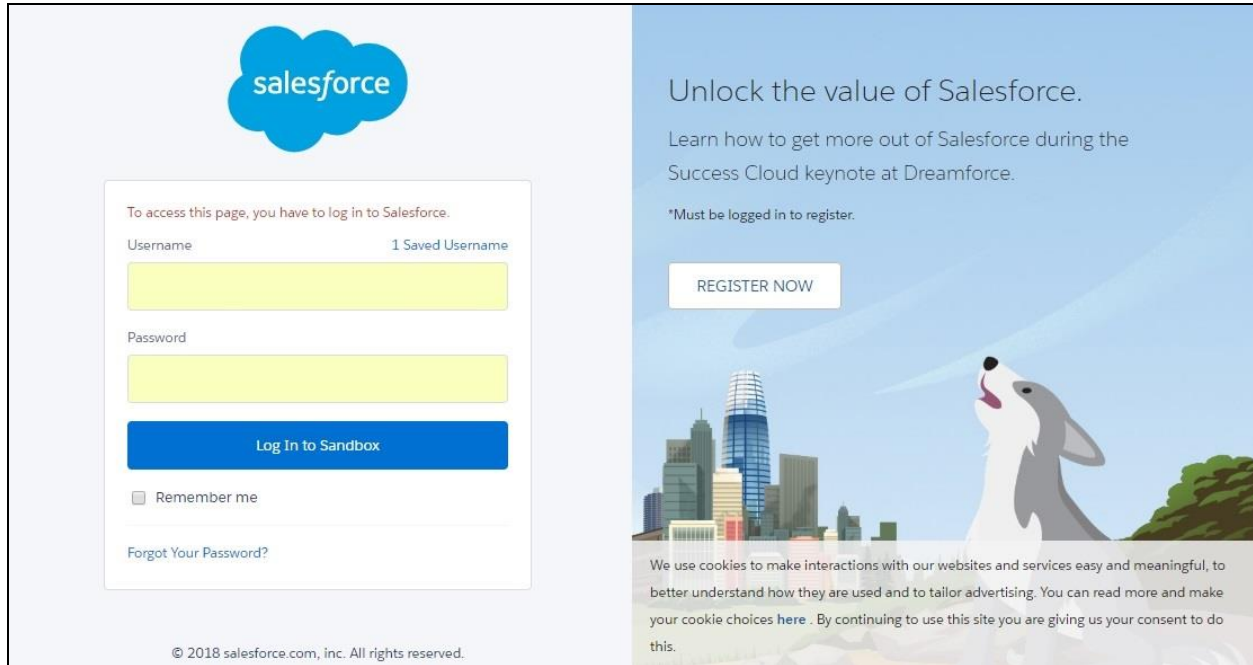
Online Offline

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

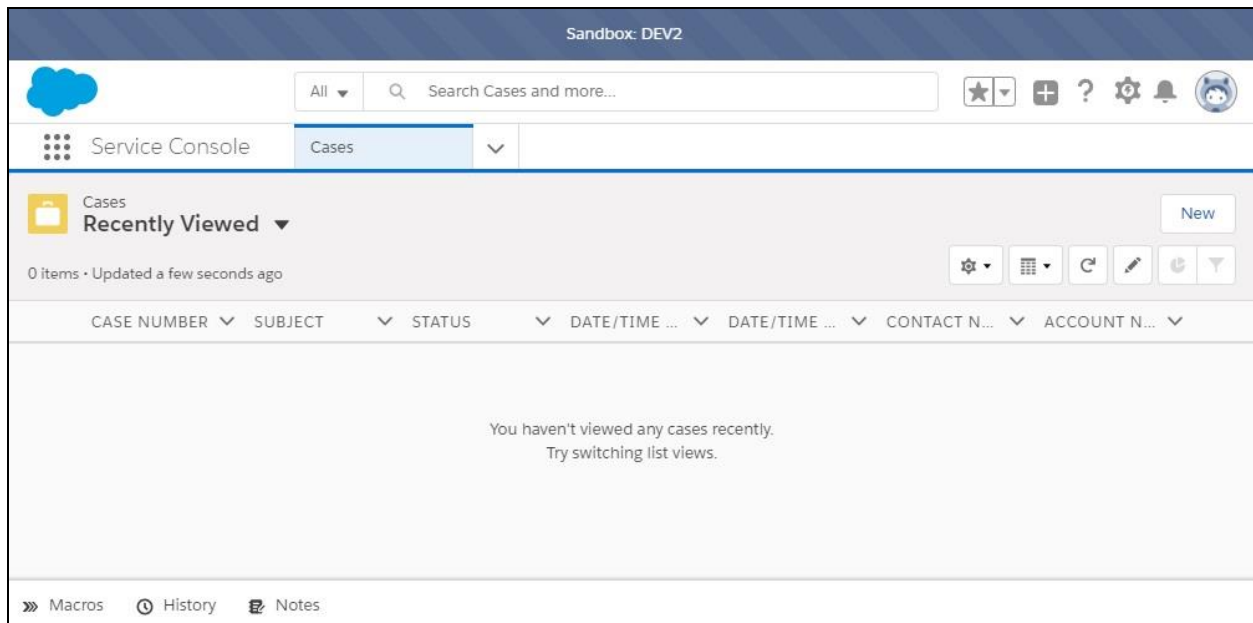
TSAPI Service Status TLink Status User Status

9.3. Verify Tenfold

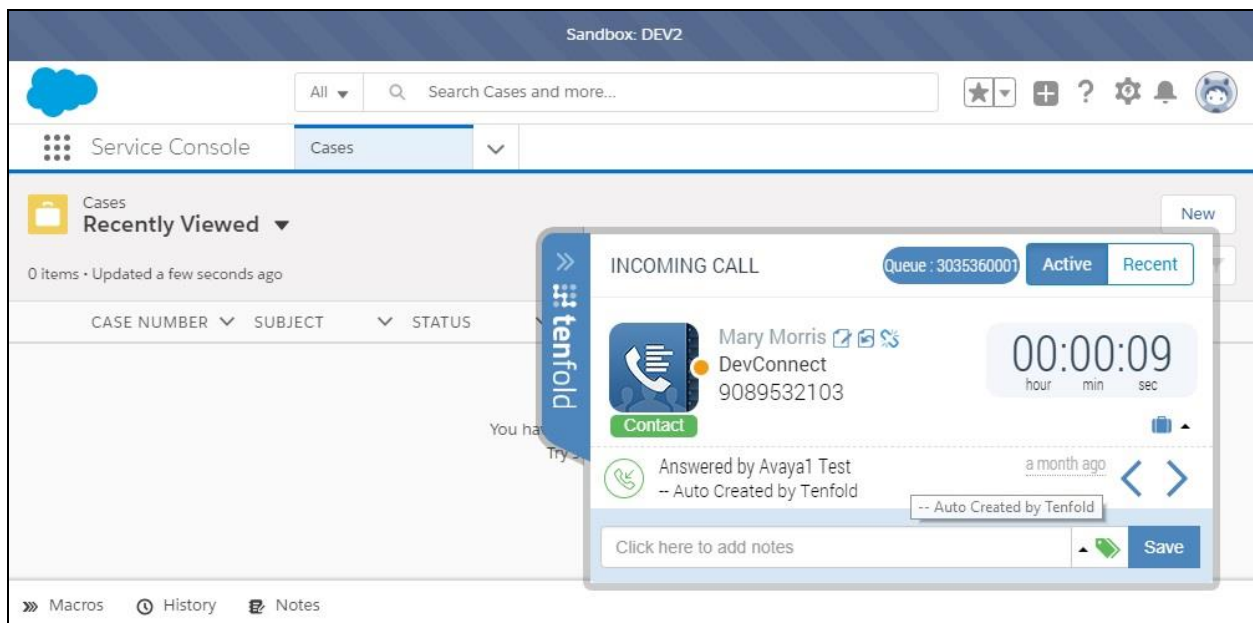
From an agent PC, launch a Chrome browser window and enter the URL provided by Tenfold. Log in with the relevant user credentials provided by Tenfold.



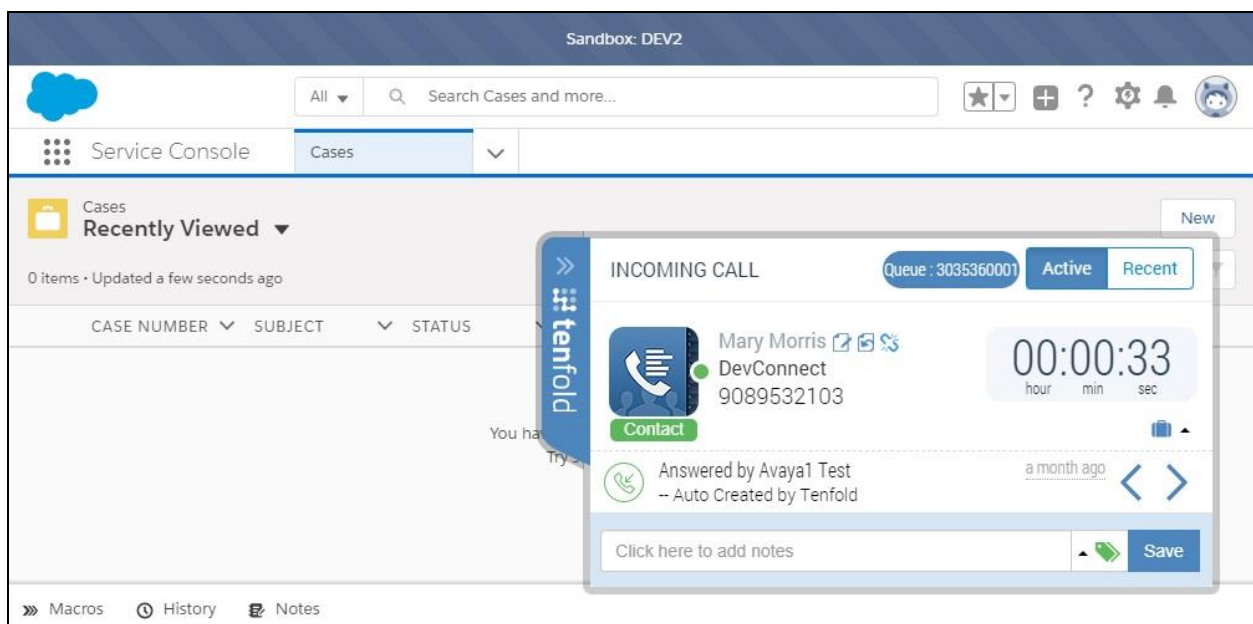
The screen below is displayed next.



Make an incoming ACD call from the PSTN. Verify that the Tenfold Chrome Extension screen appears, and is populated with the matching contact record associated with the PSTN caller number. Also verify that the ringing call status is indicated by an amber dot, as shown below.



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.



10. Conclusion

These Application Notes describe the configuration steps required for Tenfold to successfully interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 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**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.3, Issue 7, May 2018, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.3, Issue 5, May 2018, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 7.1.3, Issue 5, July 2018, available at <http://support.avaya.com>.
4. *Avaya AES Integration Overview*, available upon request to Tenfold Support.
5. *User Documentation*, available upon request to Tenfold Support.

©2018 Avaya Inc. All Rights Reserved.

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

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