



Avaya Solution & Interoperability Test Lab

Application Notes for Computer Instruments Screen Pop Premium with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Computer Instruments Screen Pop Premium (SPP) 3.10 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. Computer Instruments Screen Pop Premium integrates with existing CRM solutions to deliver a screen pop, provide phone controls, and other functions to agent desktops. Computer Instruments Screen Pop Premium uses the Telephony Services Application Programming Interface (TSAPI) of Avaya Aura® Application Enablement Services. For the compliance test, a standalone sample SPP client application, provided by Computer Instruments, was used to verify select functions.

Readers should pay attention to **Section 0**, in particular the scope of testing as outlined in **Section 0** 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 to integrate Computer Instruments Screen Pop Premium (SPP) 3.10 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. Computer Instruments Screen Pop Premium integrates with existing CRM solutions to deliver a screen pop, provide phone controls, and other functions to agent desktops. Computer Instruments Screen Pop Premium uses the Telephony Services Application Programming Interface (TSAPI) of Avaya Aura® Application Enablement Services (AES). For the compliance test, a standalone sample SPP client application, provided by Computer Instruments, was used to verify select functions.

In the compliance test, when a call was routed to an agent in the call center, a sample SPP client application on the agent desktop provided a screen pop with information related to a particular caller using Automatic Number Identification (ANI) via a web browser and allowed call control functions, such as answer call, end call, and hold/resume call. In addition, the SPP client application was used to originate outbound calls. The call status was synchronized between the sample SPP application and the desktop phone using AES TSAPI.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. Incoming PSTN calls were made to a VDN or hunt group, which routed the call to an available agent. SPP provided a screen pop with caller information using ANI and allowed the agent to perform call control functions from the sample SPP client application or the agent deskphone. In addition, outbound calls from the SPP application to agents and the PSTN were verified. Serviceability testing focused on verifying that the sample SPP client application recovered after restoring network connectivity and busying out and releasing the CTI link from Communication Manager.

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 Avaya Aura® Application Enablement Services and Computer Instruments Screen Pop Premium used an encrypted TSAPI link.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. Feature testing was limited to verifying the following on Computer Instruments SPP.

- Use of TSAPI call control service to answer call, end call, hold/resume call, and make a call.
- Use of TSAPI query service to query status on skill groups and agent login states.
- Use of TSAPI event report service to monitor VDNs.
- Use of TSAPI monitor service to monitor VDNs and agent stations.
- Use of TSAPI system status service to track TSAPI link status.
- Use of sample SPP application and agent deskphone to perform call control functions to answer call, end call, and hold/resume call to verify that the call state was reflected accurately on both.
- Outbound calls originated from the sample SPP application or agent deskphone to agents and the PSTN.
- Multiple calls to different agents running the sample SPP application.
- Serviceability testing focused on verifying that the sample SPP application came back into service after restoring network connectivity and the TSAPI link.

2.2. Test Results

All test cases passed with the following observations:

- SPP does not support querying for agent states, such as Available (i.e., Auto-In, Manual-In), After Call Work (ACW), Aux Work, etc.
- The sample SPP client application, provided Computer Instruments, did not display agent login status.
- The sample SPP client application, provided Computer Instruments, could not abort a call that was already ringing.
- The sample SPP client application, provided Computer Instruments, did not support call transfers and conference.
- The sample SPP client application, provided Computer Instruments, provided caller information based on a 10-digit number.
- After busying and releasing the TSAPI link from Communication Manager and AES sends a System Status event to SPP, SPP needs to be restarted in order for the SPP client application to reconnect to the SPP server.
- After restoring network connectivity to the agent desktop running the sample SPP client application, the SPP client may have to be manually reconnected to the SPP server.

2.3. Support

Technical support on Computer Instruments Screen Pop Premium can be obtained through the following:

- **Phone:** (888) 451-0851
- **Web:** <https://instruments.com/contact/>

3. Reference Configuration

Figure 1 illustrates the configuration used for the compliance testing. In the compliance testing, SPP monitored the devices shown in the table below.

Device Type	Extension
VDNs	77550
Skill Group	77500
Agent Stations	78004, 77301
Agent IDs	76301, 76302

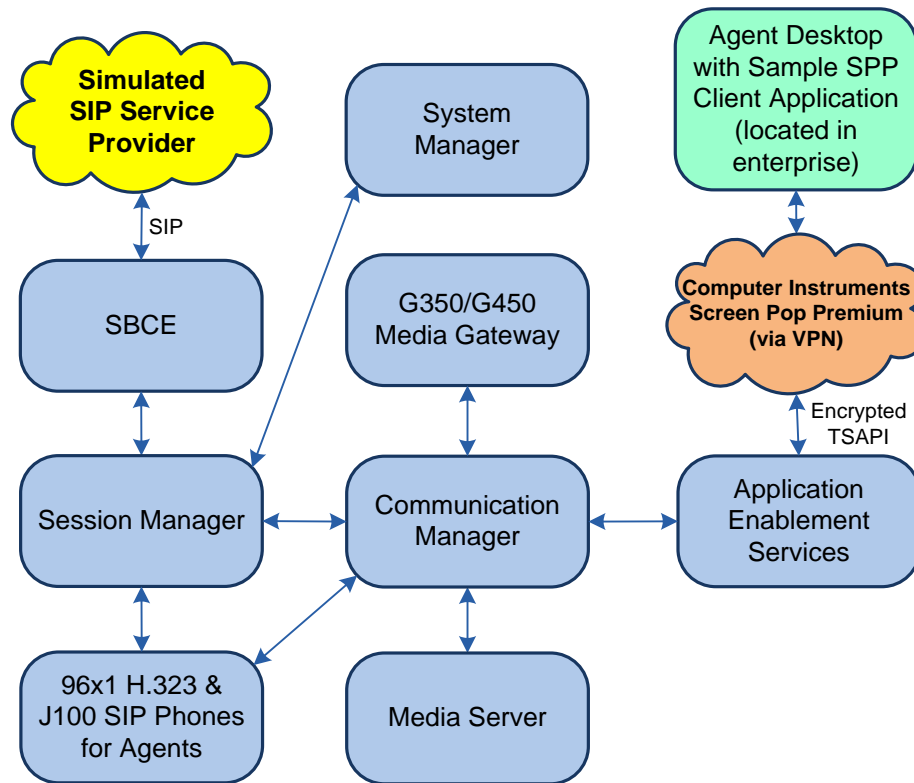


Figure 1: Computer Instruments Screen Pop Premium with Avaya Aura® Suite

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	10.1.0.1.0-SP1
Avaya G430 Media Gateway	FW 42.8.0
Avaya G450 Media Gateway	FW 42.7.0
Avaya Aura® Media Server	v.10.1.0.77
Avaya Aura® Application Enablement Services	10.1.0.1.0.7-0
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.0614394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series Deskphones	6.8.5.3.2 (H.323) 7.1.13.0.4 (SIP)
Avaya J100 Series Deskphones	4.0.13.0.6 (SIP)
Computer Instruments Screen Pop Premium	3.10.8436.27076

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer system parameters features
- Administer CTI link

Note: 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 covered.

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license allows the features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** option is enabled on **Page 4**. If this option is not enabled, then contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                                Page 4 of 12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
    Access Security Gateway (ASG)? n              Authorization Codes? y
    Analog Trunk Incoming Call ID? y              CAS Branch? n
    A/D Grp/Sys List Dialing Start at 01? y      CAS Main? n
    Answer Supervision by Call Classifier? y      Change COR by FAC? n
    ARS? y Computer Telephony Adjunct Links? y
    ARS/AAR Partitioning? y          Cvg Of Calls Redirected Off-net? y
    ARS/AAR Dialing without FAC? n      DCS (Basic)? y
    ASAI Link Core Capabilities? y      DCS Call Coverage? y
    ASAI Link Plus Capabilities? y      DCS with Rerouting? y
    Async. Transfer Mode (ATM) PNC? n
    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

(NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer System Parameters Features

Use the **change system-parameters features** command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                  Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                               Switch Name:
    Emergency Extension Forwarding (min): 10
    Enable Inter-Gateway Alternate Routing? n
    Enable Dial Plan Transparency in Survivable Mode? n
                               COR to Use for DPT: station
                               EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
    Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
    Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
    Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
    Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
    Create Universal Call ID (UCID)? y    UCID Network Node ID: 27
```

Navigate to **Page 13** and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to SPP.

change system-parameters features	Page 13 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER MISCELLANEOUS	
Callr-info Display Timer (sec): 10	
Clear Callr-info: next-call	
Allow Ringer-off with Auto-Answer? n	
Reporting for PC Non-Predictive Calls? n	
Agent/Caller Disconnect Tones? n	
Interruptible Aux Notification Timer (sec): 3	
Zip Tone Burst for Callmaster Endpoints: double	
ASAI	
Copy ASAI UUI During Conference/Transfer? n	
Call Classification After Answer Supervision? n	
Send UCID to ASAI? y	
For ASAI Send DTMF Tone to Call Originator? y	
Send Connect Event to ASAI For Announcement Answer? n	
Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n	

5.3. Administer CTI Link

Add a CTI link using the **add cti-link** command. 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: 77700	
Type: ADJ-IP	
Name: AES TSAPI Link	COR: 1
Unicode Name? 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 Ports
- Administer Security Database
- Restart Service
- Administer SPP User
- 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 Application Enablement Services. The login screen is displayed. Log in using the appropriate credentials.



Application Enablement Services Management Console


A login form with a light gray background. It contains the text "Please login here:" followed by a label "Username" and a text input field. Below the input field is a button labeled "Continue".

Please login here:

Username

Copyright © 2009-2022 Avaya Inc. All Rights Reserved.

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

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 22 11:51:03 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 12:20:18 EST 2023
HA Status: Not Configured

Home

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 Address** in the left pane to display the applicable WebLM IP address. Log into WebLM using the appropriate credentials.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 22 11:51:03 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 12:22:10 EST 2023
HA Status: Not Configured

Licensing | WebLM Server Address

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▼ Licensing
 - WebLM Server Address
 - WebLM Server Access
 - Reserved Licenses
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

WebLM Server Address

WebLM IP Address/FQDN

SSL ☒

WebLM Port

Secondary WebLM IP Address/FQDN

Secondary SSL ☒

Secondary WebLM Port

TLS Certificate Hostname Validation

Note:Please refer help page for more details

Enable Certificate Hostname Validation ☐

The WebLM screen below is displayed. 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.

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
ASBCE
▶ Session_Border_Controller_E_AE
COMMUNICATION_MANAGER
▶ Call_Center
▶ Communication_Manager
FE
▶ AvayaWorkplace
MESSAGING
▶ Messaging
MSR
▶ Media_Server
OL
▶ OL
SYSTEM_MANAGER
▶ System_Manager
SessionManager
▶ SessionManager
Utility_Services
▶ Utility_Services
VDIA
▶ VDIA

Application Enablement (CTI) - Release: 10 - SID: 10503000Standard License file

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

License installed on: May 31, 2022 9:32:15 AM -05:00

License File Host IDs: V9-DF-31-89-CD-2A-01

Licensed Features

13 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
		SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes:

SPP will use the following license when connected to AES.

Acquired Licenses			
1 Item Show All			
Feature	Acquired by	Acquirer ID	Count
VALUE_AES_TSAPI_USERS	TSAPI (devcon-aes)	devcon-aes:1675866005:1611520:140309635029120:0000	3

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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 22 11:51:03 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 12:29:23 EST 2023
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links

Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ TWS

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	devcon	1	UNKNOWN	Both

Add Link Edit Link Delete Link

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection *devcon* is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Set **Security** to *Encrypted* or *Both* to allow encrypted TSAPI link. Retain the default values in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 22 11:51:03 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 12:33:15 EST 2023
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 1

Switch Connection devcon

Switch CTI Link Number 1

ASAI Link Version 12


Security Both

Apply Changes Cancel Changes

6.4. Administer Ports

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

In the **TSAPI Ports** section, select the radio button for the **Enabled** column as shown below. Retain the default values in the remaining fields.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 22 12:35:27 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 13:27:05 EST 2023
HA Status: Not Configured

Networking | PortsHome | 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 Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

JAO; Reviewed:
SPOC 3/23/2023


Solution & Interoperability Test Lab Application Notes
©2023 Avaya Inc. All Rights Reserved.

13 of 26
CI-SPP-AES10

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. Ensure that both parameters are unchecked as shown below.

In the event that the security database is being used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the SPP user from **Section 0**.

**AVAYA** Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Feb 22 12:35:27 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 13:26:26 EST 2023
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
▶ High Availability
▶ Licensing
▶ Maintenance
▶ Networking
▼ Security
 ▶ Account Management
 ▶ Audit
 ▶ Certificate Management
 Enterprise Directory
 ▶ Host AA
 ▶ PAM
▼ Security Database
 ▪ Control
 ⊞ CTI Users


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

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

Apply Changes

6.6. Restart 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**.

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 22 12:35:27 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 13:27:38 EST 2023
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

▶ User Management

▶ Utilities

▶ Help

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. Administer SPP 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 cust
Last login: Wed Feb 22 13:34:07 2023 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 14:36:24 EST 2023
HA Status: Not Configured

User Management | User Admin | Add User


Home | Help | Logout

<ul style="list-style-type: none">▶ AE Services▶ Communication Manager Interface▶ High Availability▶ Licensing▶ Maintenance▶ Networking▶ Security▶ Status▼ User Management<ul style="list-style-type: none">▶ Service Admin▼ User Admin<ul style="list-style-type: none">■ Add User■ Change User Password■ List All Users■ Modify Default Users■ Search Users▶ Utilities▶ Help	<h4>Add User</h4> <p>Fields marked with * can not be empty.</p> <table><tr><td>* User Id</td><td><input type="text" value="cinstruments"/></td></tr><tr><td>* Common Name</td><td><input type="text" value="cinstruments"/></td></tr><tr><td>* Surname</td><td><input type="text" value="cinstruments"/></td></tr><tr><td>* User Password</td><td><input type="password" value="....."/></td></tr><tr><td>* Confirm Password</td><td><input type="password" value="....."/></td></tr><tr><td>Admin Note</td><td><input type="text"/></td></tr><tr><td>Avaya Role</td><td><input type="text" value="None"/></td></tr><tr><td>Business Category</td><td><input type="text"/></td></tr><tr><td>Car License</td><td><input type="text"/></td></tr><tr><td>CM Home</td><td><input type="text"/></td></tr><tr><td>Css Home</td><td><input type="text"/></td></tr><tr><td>CT User</td><td><input type="text" value="Yes"/></td></tr><tr><td>Department Number</td><td><input type="text"/></td></tr><tr><td>Display Name</td><td><input type="text"/></td></tr><tr><td>Employee Number</td><td><input type="text"/></td></tr><tr><td>Employee Type</td><td><input type="text"/></td></tr></table>	* User Id	<input type="text" value="cinstruments"/>	* Common Name	<input type="text" value="cinstruments"/>	* Surname	<input type="text" value="cinstruments"/>	* 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"/>
* User Id	<input type="text" value="cinstruments"/>																																
* Common Name	<input type="text" value="cinstruments"/>																																
* Surname	<input type="text" value="cinstruments"/>																																
* 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"/>																																

6.8. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a list of Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name to be used to configure SPP.

In this case, the associated Tlink name is “AVAYA#DEVCON#CSTA-S#DEVCON-AES”. Note the use of the switch connection “DEVCON” from **Section 0** as part of the Tlink name and “CSTA-S” indicating this is an encrypted TSAPI link.

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 22 13:34:07 2023 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Wed Feb 22 14:37:20 EST 2023
HA Status: Not Configured

Security | Security Database | TlinksHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

▪ Tlink Groups

▪ Worktops

Tlinks

Tlink Name

☒ AVAYA#DEVCON#CSTA#DEVCON-AES

☐ AVAYA#DEVCON#CSTA-S#DEVCON-AES

Delete Tlink

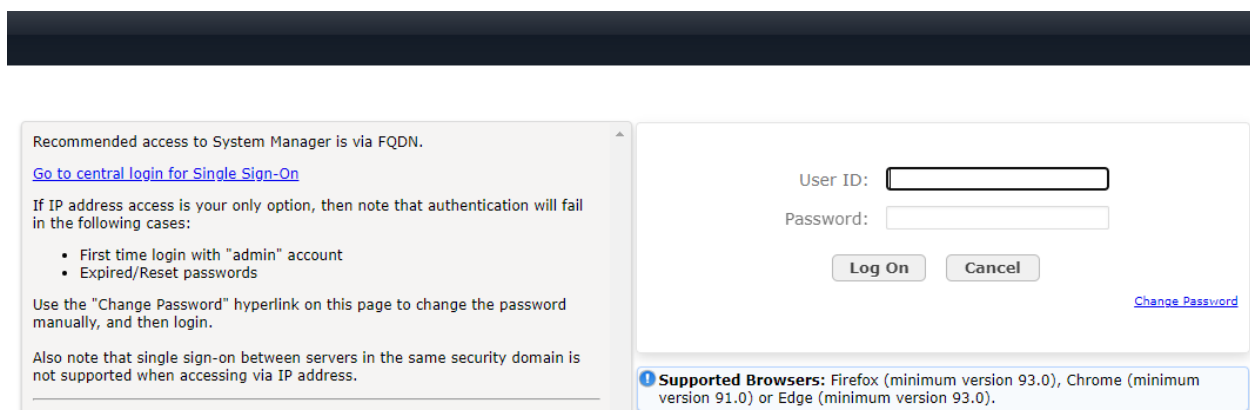
7. Configure Avaya Aura® Session Manager

This section provides the procedure for configuring a SIP user on Session Manager, which is performed via the web interface of System Manager. The procedure includes the following areas:

- Launch System Manager
- Administer users

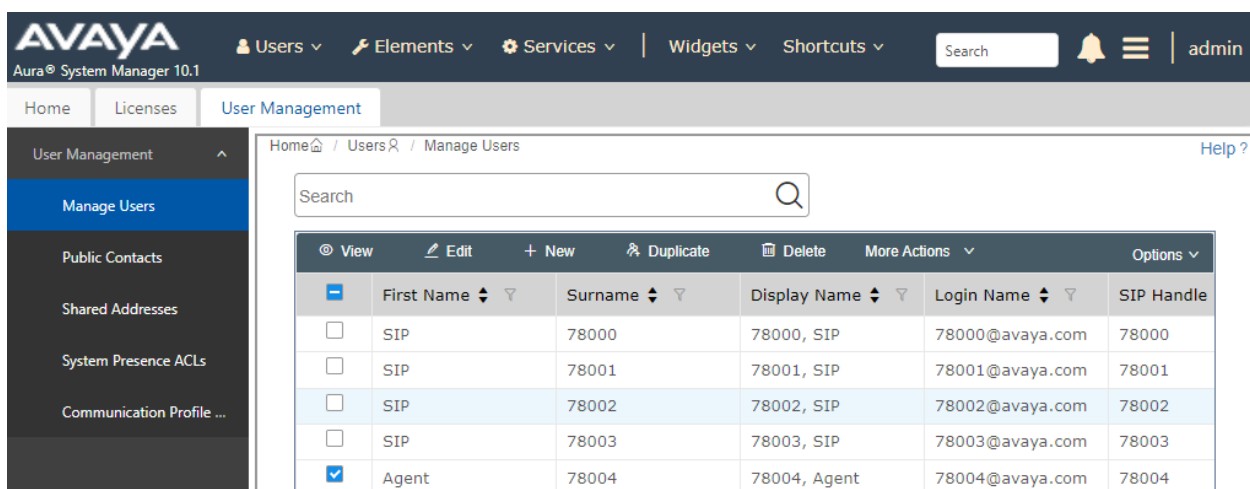
7.1. Launch System Manager

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



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 SIP agent station from **Section 3**, in this case **78004**, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	78000	78000, SIP	78000@avaya.com	78000
<input type="checkbox"/>	SIP	78001	78001, SIP	78001@avaya.com	78001
<input type="checkbox"/>	SIP	78002	78002, SIP	78002@avaya.com	78002
<input type="checkbox"/>	SIP	78003	78003, SIP	78003@avaya.com	78003
<input checked="" type="checkbox"/>	Agent	78004	78004, Agent	78004@avaya.com	78004

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**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The 'User Management' section is expanded, and the 'Manage Users' sub-section is selected. The 'User Profile | Edit | 78004@avaya.com' screen is displayed. The 'Communication Profile' tab is active, and the 'CM Endpoint Profile' sub-section is selected. The 'Extension' field is highlighted with a red box.

The **New 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.

The screenshot shows the 'Edit Endpoint' screen in the Avaya Aura System Manager 10.1 interface. The 'General Options (G)' tab is selected. The 'Type of 3PCC Enabled' dropdown is set to 'Avaya'. The 'Extension' field is 78004, and the 'Set Type' is J179CC.

8. Configure Computers Instruments Screen Pop Premium

The configuration of SPP is performed by Computer Instruments technical personnel. For provisioning, Computer Instruments would require the call center devices to be monitored, such as VDNs, skill groups, agent login IDs, and agent stations. In addition, the AES Tlink name is also required.

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager


On Communication Manager, verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is *established* for the CTI link number administered in **Section 5.3**, 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	12	no	devcon-aes	established	860	861

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify that the **Status** is *Talking* for the TSAPI link administered in **Section 0**.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Feb 14 09:43:33 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Tue Feb 14 11:27:59 EST 2023
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

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

User Management

Utilities

Help

TSAPI Link Details

☐ Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	devcon	1	Talking	Wed Feb 1 11:42:16 2023	Online	20	5	74	127	30

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

Click on the **User Status** button to verify that the SPP user has opened an AES connection as shown below.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Feb 14 09:43:33 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.2.0.12-0
Server Date and Time: Tue Feb 14 11:30:21 EST 2023
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

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

User Management

Utilities

Help

CTI User Status

Enable page refresh every

60

seconds

CTI Users

All Users

Submit

Open Streams

1

Closed Streams

16

Open Streams

Name	Time Opened	Time Closed	Link Name
cstruments	Tue 14 Feb 2023 11:16:51 AM EST		AVAYA#DEVCON#CSTA-S#DEVCON-AES

Show Closed Streams

Close All Opened Streams

Back

9.3. Verify Computer Instruments Screen Pop Premium

Start the SPP client application on the agent desktop. Right-click on SPP icon in the Windows task bar to display the following pop-up menu.

Configuration

Color Style

Status

Phone Display

Client Chat

Contacts

Connect

About

Exit

Select **Configuration** (from the previous page) to configure the SPP server IP address, port, extension, and SPP credentials as shown below. In this example, extension **78004** is monitored.

SPP Premium Client Configuration

Server Connection

Server IP Address: ☒ Auto Connect

Server Port:

My Extension:

SPP User ID:

SPP User Pwd:

CRM Configuration

User ID: Password:

Default Contact Manager

☐ Microsoft Outlook ☐ Dynamics

☐ SalesForce ☐ Generic

☒ None

Client Screen Pop Options

Minimum digits needed for Call Info pop:

Screen Pop Options

URL / Command:

☐ ScreenPop on Answer ☐ ScreenPop On Ring ☒ No ScreenPop

Desktop Options

☐ Open Documents automatically upon call notification

☐ Use voice announcements

Phone Pad Options

☒ Display Phonepad on Ring ☐ Do not display Phonepad

☐ Display Phonepad on Answer

Call Info Window Options

☐ Inbound ☐ Minimize on Pop

☒ Inbound/Outbound ☒ Open Call Info on Answer

☐ Outbound

Check which detail windows to pop automatically


☐ Caller Emails ☐ Document History

☐ Sent Emails ☐ Open Document List

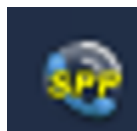
Transfer Options

Backup Extension: ☐ Transfer to backup if on a call

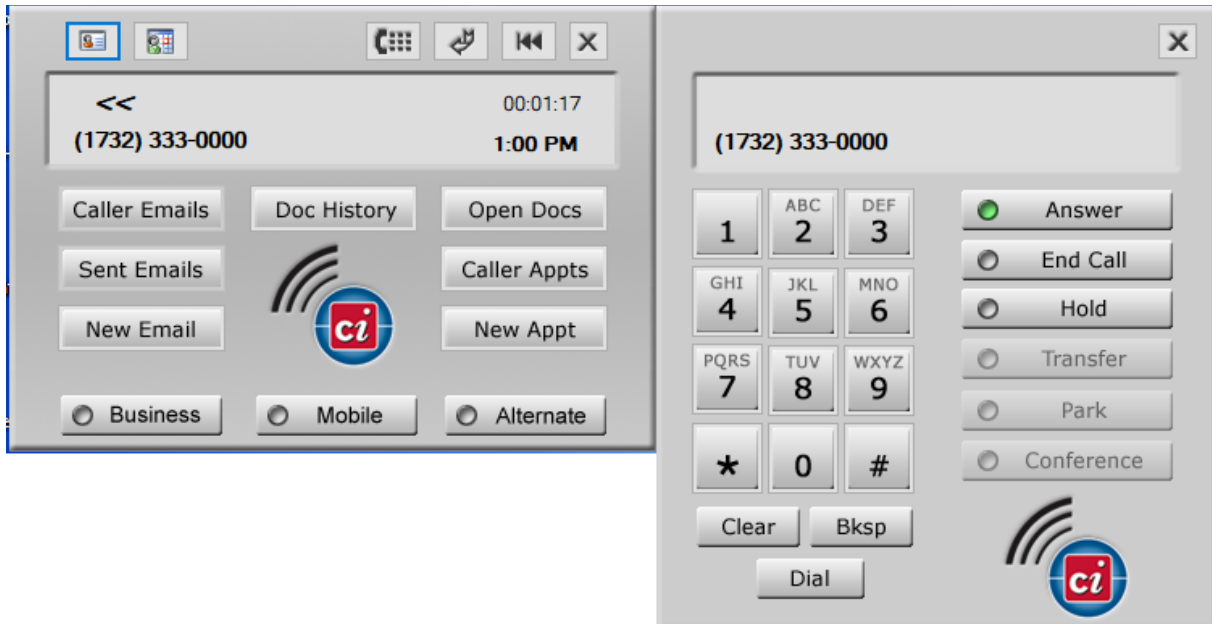
Transfer Message:



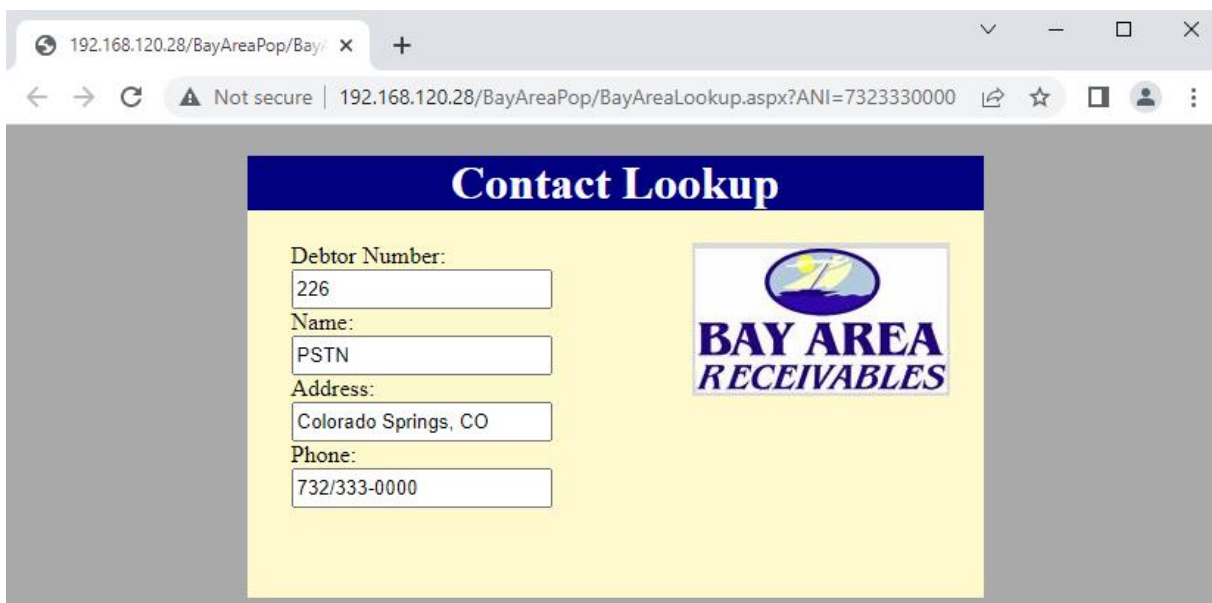
Next, right-click on the SPP icon in the Windows task bar and select **Connect** to connect to the SPP server. Once the SPP client application is connected to the SPP server, the SPP icon would turn green as shown below.



Lastly, right-click on the SPP icon again and select **Phone Display**. Place a call to the agent associated with extension 78004. The incoming call is displayed in the SPP client application as shown below. Click the **Answer** button to answer the call. Verify that the call is connected to the agent desk phone.



Also, verify that a screen pop with caller information is displayed in a Web browser as shown below.



On the SPP Phone Display, click **End Call** to terminate the call. From the SPP Phone Display, an outbound call may also be established.

10. Conclusion

These Application Notes describe the configuration steps required to integrate Computer Instruments Screen Pop Premium (SPP) with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. SPP was able to deliver a screen pop with caller information based on ANI, provide call control functions, and establish outbound calls using Telephony Services Application Programming Interface (TSAPI) of Avaya Aura® Application Enablement Services. 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 10.1.x, Issue 2, September 2022, available at <http://support.avaya.com>.
2. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 5, September 2022, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 7, September 2022, available at <http://support.avaya.com>.
4. *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 4, September 2022, available at <http://support.avaya.com>.

©2023 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.