



Application Notes for AMC Technology DaVinci for Salesforce Service Cloud Voice 7.0 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 0.1

Abstract

These Application Notes describe the configuration steps required for AMC Technology DaVinci for Salesforce Service Cloud Voice 7.0 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. AMC Technology Salesforce Service Cloud for DaVinci is a contact center and CRM integration platform for CRM provider Salesforce.com.

In the compliance testing, AMC Technology DaVinci for Salesforce Service Cloud Voice used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor agent stations on Avaya Aura® Communication Manager to provide screen pop, call control, and Click to Dial features from agent desktops connected to AMC Technology 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 AMC Technology DaVinci for Salesforce Service Cloud Voice (DaVinci) 7.0 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. DaVinci is a contact center and CRM integration platform for CRM provider Salesforce.com.

In the compliance testing, DaVinci used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor agent stations on Communication Manager to provide screen pop, call control, and Click to Dial features from agent desktops connected to AMC Technology and Salesforce.com.

The DaVinci solution consisted of a local DaVinci Premise Gateway, AMC Technology Cloud hosted on Microsoft Azure, and DaVinci App for Salesforce Service Cloud Voice on Salesforce.com. The local DaVinci Premise Gateway is the component that used TSAPI to integrate with Application Enablement Services. The DaVinci App for Salesforce Service Cloud Voice is the component that used the Service Cloud Voice (SCV) API with Salesforce and resided on Salesforce.com.

In the compliance testing, each agent desktop used web browser to connect to DaVinci Premise Gateway, AMC Technology Cloud, and Salesforce.com running the DaVinci App for Salesforce Service Cloud Voice.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon an agent log in, DaVinci requests monitoring on the agent station and uses set agent state to log the agent into the ACD on Communication Manager.

For the manual part of testing, incoming ACD calls were placed with available agents that have web browser connections to DaVinci Premise Gateway, AMC Technology Cloud, and Salesforce.com running the DaVinci App for Salesforce Service Cloud Voice. All necessary call actions were initiated from the agent desktops. The Click to Dial calls were initiated by clicking on the phone numbers displayed on the agent desktops from the Salesforce.com Contacts web page.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the DaVinci Premise Gateway.

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 Application Enablement Services and DaVinci did not include use of any specific encryption features as requested by AMC Technology.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on DaVinci:

- Use of TSAPI monitoring services to monitor agent stations.
- Use of TSAPI query services to query agent states and to set agent states including log in, log out, and work mode changes with support for reason codes.
- Use of TSAPI call control services to support call control and launch of outbound calls for the Click to Dial feature.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple agents, multiple calls via Add Party, blind/attended transfer, attended conference, long duration, Click to Dial from contact phone number, and reason codes.

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

2.2. Test Results

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

- Due to Salesforce SCV limitation, this release of DaVinci does not support features including auto answer, contact record match, and pending work modes.
- Salesforce SCV does not allow for hidden display of presence/work states. As such, the **After Call Work** state will appear on the desktop although shouldn't be selected by agents. Selecting such state will result in an eventual error message of **We can't update your status. Try again later** from Salesforce.
- By Salesforce SCV design, the **Offline** state does not log the agent out of the ACD with agent still able to receive calls. As such, agents should select **Log Out of Phone System** instead. Furthermore, after logging out, the agent desktop will reflect the last unavailable state the agent was in.
- In the Redirection on No Answer (RONA) scenario, after the ACD call was redirected with agent logged out of the ACD by Communication Manager, the agent desktop reflected the last unavailable state the agent was in per Salesforce SCV limitation.
- As another Salesforce SCV limitation, an update of agent presence state may not always succeed. The workaround is to use a two-step process to first change the presence into an unavailable state that differs from the current state, and then into the desired state. For example, if the agent wishes to change from **Available for Voice** to **Lunch**, then select **Meeting** first, followed by **Lunch**. Similarly, when wishing to change from **Lunch** back into **Available for Voice**, then select **Meeting** first, followed by **Available for Voice**.
- DaVinci requires all call control actions such as answer and drop to be initiated via the agent desktop whenever possible.
- Agent desktop reflection of incoming call and presence state change is mostly instantaneous within a couple of seconds. Occasionally, the update can take up to ten seconds in the compliance testing with use of Salesforce development Org that has lower priority than production Org.
- During an Ethernet disruption to the DaVinci Premise Gateway, call control actions from agent desktops received errors such as **We couldn't end your call. Refresh the page and try again**. In some cases, an agent logout and log back in can resolve the desktop display problem post recovery of DaVinci Premise Gateway. If not, then a complete workaround is needed that includes a restart of DaVinci Premise Gateway, complete log out of agents from phone system, Omni-Channel, and Salesforce, clearing of agents' browser privacy settings, and then logging the agents back in. Should an agent experience a presence state change problem after this, simply logout and log back in again. For additional details, contact the AMC Technology Support team.

2.3. Support

Technical support on DaVinci can be obtained through the following:

- **Phone:** (800) 390-4866
- **Email:** support@amctechnology.com
- **Web :** <https://support.amctechnology.com>

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, DaVinci monitored the agent stations shown in the table below.

Device Type	Extension
Agent Station	65000 (H.323), 66002 (SIP)
Agent ID	65881, 65882
Agent Password	65881, 65882

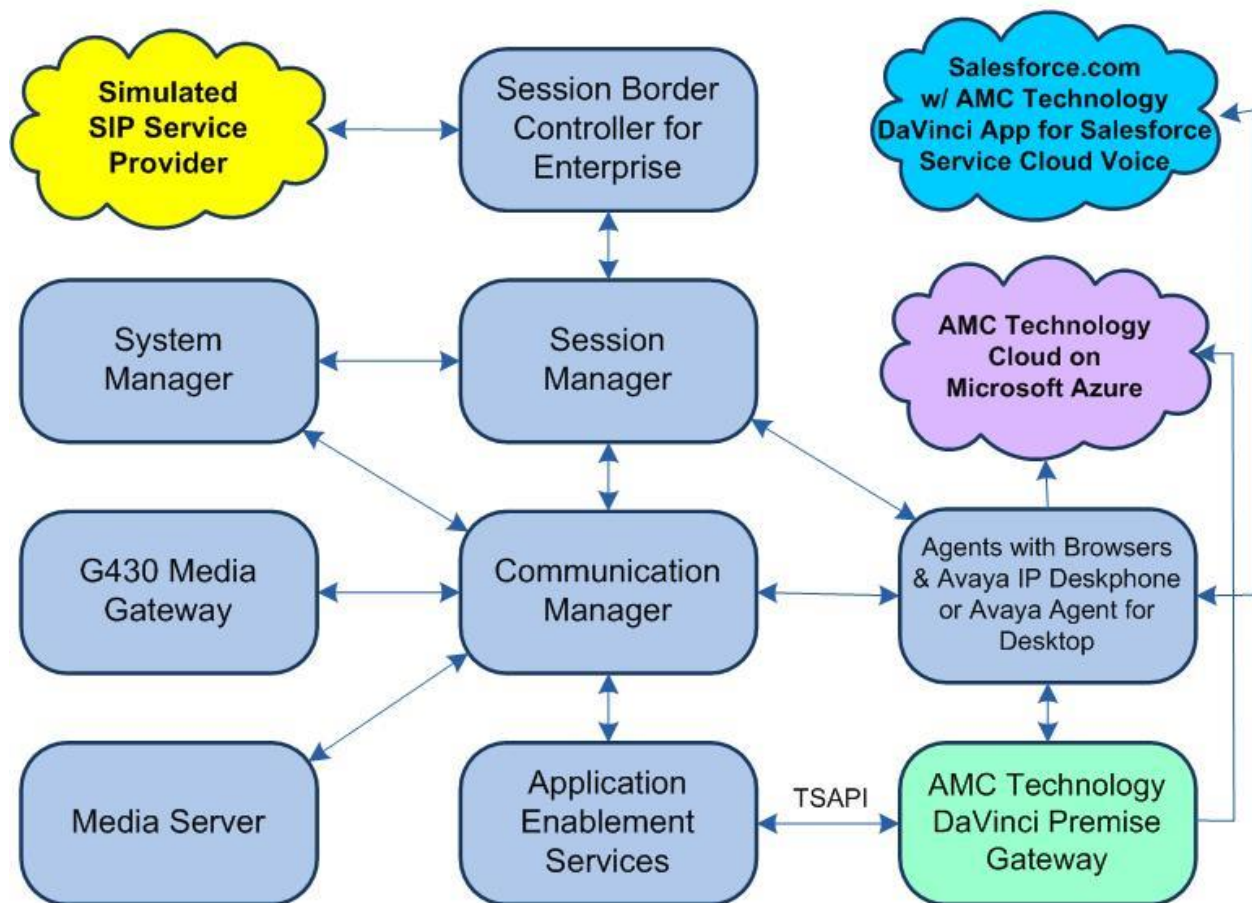


Figure 1: Compliance Testing Configuration

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	8.1.3.4 (8.1.3.4.0.890.27348)
Avaya G430 Media Gateway	41.34.4
Avaya Aura® Media Server in Virtual Environment	8.0.2.218
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.4 (8.1.3.4.0.2-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3.4 (8.1.3.4.813401)
Avaya Aura® System Manager in Virtual Environment	8.1.3.4 (8.1.3.4.1014355)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.3.1 (8.1.3.1-38-21632)
Avaya Agent for Desktop (H.323)	2.0.6.19.3004
Avaya J179 IP Phone (H.323)	6.8511
Avaya J169 IP Phone (SIP)	4.0.11.0.3
AMC Technology DaVinci Premise Gateway on Windows Server 2019 - Avaya TSAPI Windows Client (csta32.dll) - DaVinci Premise	7.0.0.27 Standard 8.1.2 7.0.0.11
AMC Technology Cloud	7.0.0.1
AMC Technology DaVinci App for Salesforce Service Cloud Voice Salesforce.com Salesforce scv-connector-base NPM package	7.0.0.5 Summer 22 3.3.19

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Obtain reason codes

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. Administer System Parameters Features

Log into the System Access Terminal. 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 DaVinci.

```
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 UI During Conference/Transfer? n
  Call Classification After Answer Supervision? y
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.4. 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 DaVinci.

```
change reason-code-names                                     Page 1 of 1

                                REASON CODE NAMES

                                Aux Work/      Logout
                                Interruptible?

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:
```

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 DaVinci user
- Administer security database
- Restart services
- 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" 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 Jun 7 11:06:36 2022 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: 8.1.3.4.0.2-0', 'Server Date and Time: Tue Jun 07 11:34:46 EDT 2022', and 'HA Status: Not Configured'. Below the header is a red navigation bar with 'Home | Help | Logout'. The left sidebar contains a menu with options: '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: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. This is followed by a bulleted list: '• 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'. At the bottom of the main content area, a note 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' section selected in the left sidebar. The top header and 'Welcome' message are identical to the previous screenshot. The red navigation bar remains 'Home | Help | Logout'. The left sidebar menu is the same, but 'Licensing' is now highlighted. The main content area is titled 'Licensing' and contains three sections of instructions: 'If you are setting up and maintaining the WebLM, you need to use the following:' followed by a bulleted list with '• WebLM Server Address'; 'If you are importing, setting up and maintaining the license, you need to use the following:' followed by a bulleted list with '• WebLM Server Access'; and 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:' followed by a bulleted list with '• Reserved Licenses'. Below the sidebar menu, the following options are visible: 'WebLM Server Address', 'WebLM Server Access' (highlighted in blue), 'Reserved Licenses', 'Maintenance', and 'Networking'.

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 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍

Home Licenses

L...

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
- ▼ Application_Enablement
 - View license capacity
 - View peak usage
- APS_CMS_Connectors
 - ▶ APS_CMS_Connectors
- Configure Centralized Licensing
- ASBCE
 - ▶ Session_Border_Controller_E_AE
 - ▶ Avaya_Proactive_Contact
- CCTR
 - ▶ ContactCenter
- CMS
 - ▶ CMS
- Configure Centralized Licensing
- COMMUNICATION_MANAGER

>

Application Enablement (CTI) - Release: 8 - SID: 10503000

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

License installed on: May 18, 2022 9:26:13 AM -04:00

License File Host IDs: VE-83-02-2D-26-52-01

Licensed Features

11 Items Show All ▾

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	May 13, 2023	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	May 13, 2023	100
Device Media and Call Control VALUE_AES_DMCC_DMC	May 13, 2023	100
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	May 13, 2023	100
DLG VALUE_AES_DLG	May 13, 2023	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	May 13, 2023	1000

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

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

Buttons: Add Link, Edit Link, Delete Link

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number.

For **Switch Connection**, select the relevant switch connection from the drop-down list, in this case **cm7**. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

Retain the default value for **ASAI Link Version** and set **Security** to the desired value, in this case **Both** was used to allow for both encrypted and non-encrypted connections.

The screenshot shows the Avaya Management Console interface, specifically the "Edit TSAPI Links" screen. The top header and left sidebar are the same as in the previous screenshot. The main content area displays the "Edit TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values are: Link (1), Switch Connection (cm7), Switch CTI Link Number (1), ASAI Link Version (12), and Security (Both). Below the form are buttons for "Apply Changes", "Cancel Changes", and "Advanced Settings".

Link	1
Switch Connection	cm7
Switch CTI Link Number	1
ASAI Link Version	12
Security	Both

Buttons: Apply Changes, Cancel Changes, Advanced Settings

6.4. Administer DaVinci 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 Jun 7 10:48:19 2022 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 07 11:08:26 EDT 2022
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

davinci

* Common Name

davinci

* Surname

davinci

* User Password

.....

* Confirm Password

.....

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

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 the **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** parameter is unchecked, as shown below. In the case that the security database is used by the customer with this parameter enabled, then follow reference [2] to configure access privileges for the DaVinci 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 and system status. A red navigation bar contains the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various service categories, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", followed by an "Apply Changes" button.

Welcome: User
Last login: Tue Jun 7 11:06:36 2022 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 07 11:34:46 EDT 2022
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

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

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

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

6.6. Restart Services

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 Jun 7 11:06:36 2022 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 07 11:34:46 EDT 2022
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
☐ ASAI Link Manager	Running
☐ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☒ 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 pertinent Tlink name, to be used later to configure DaVinci. In this case, the pertinent Tlink name for the non-encrypted connection is **AVAYA#CM7#CSTA#AES7**, as shown below.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". A welcome message and system information are shown in the top right corner. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a list of Tlink names with radio buttons for selection. The first option, "AVAYA#CM7#CSTA#AES7", is selected. A "Delete Tlink" button is also visible.

Welcome: User
Last login: Tue Jun 7 11:06:36 2022 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: 8.1.3.4.0.2-0
Server Date and Time: Tue Jun 07 11:34:46 EDT 2022
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

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

Tlinks

Tlink Name

☒ AVAYA#CM7#CSTA#AES7
☐ AVAYA#CM7#CSTA-S#AES7

Delete Tlink

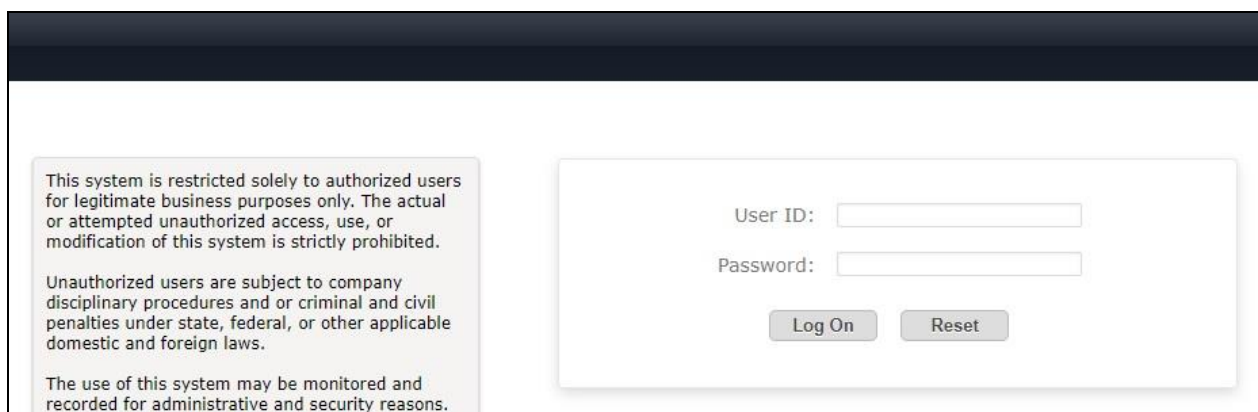
7. Configure Avaya Aura® Session Manager

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

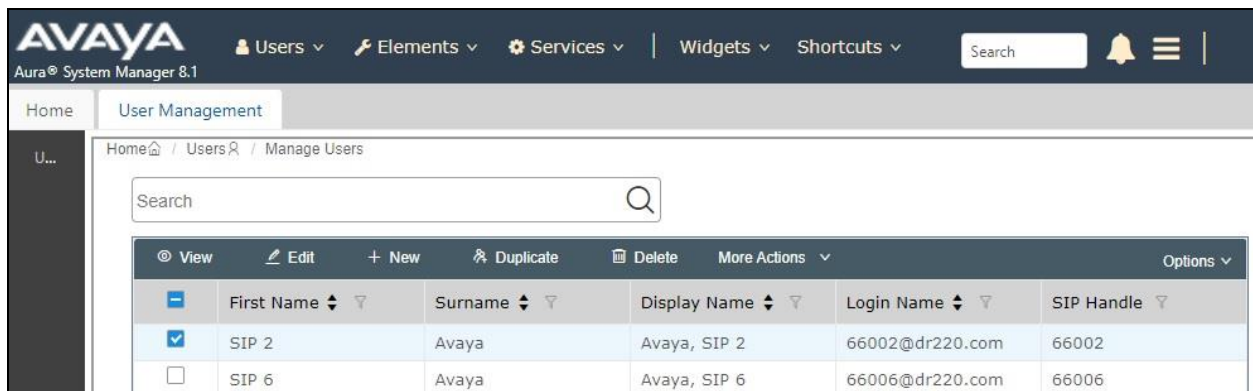
Access the System Manager web interface by using the URL **https://ip-address** in an Internet browser window, where **ip-address** is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section 3**, in this case **66002**, and click **Edit**.



View	Edit	New	Duplicate	Delete	More Actions	Options
☒	☐	☐	☐	☐	☐	☐
SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002		
SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006		

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 8.1", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The main content area is titled "User Profile | Edit | 66002@dr220.com" and features tabs for Identity, Communication Profile, Membership, and Contacts. The Communication Profile tab is active, showing fields for System (DR-CM), Profile Type (Endpoint), Extension (66002), Set Type (J169CC), Port (S000068), and Preferred Handle (Select). The left sidebar shows the "Communication Profile Password" section with a "PROFILE SET : Primary" dropdown and a "Communication Address" field. Below this, the "PROFILES" section includes "Session Manager Profile" (checked), "CM Endpoint Profile" (checked and highlighted), and "Messaging Profile" (unchecked). The "Extension" field (66002) has a blue Editor icon highlighted with a red box.

The **Edit Endpoint** pop-up screen is displayed. For **Type of 3PCC Enabled**, select **Avaya** as shown below.

The screenshot shows the 'Edit Endpoint' configuration page in the Avaya Aura System Manager 8.1 interface. The page is divided into several sections for configuring endpoint settings.

System Information:

- System:** DR-CM
- Template:** J169CC_DEFAULT_CM_8_1
- Port:** S000068
- Name:** Avaya, SIP 2
- Extension:** 66002
- Set Type:** J169CC
- Security Code:** (empty)

Configuration Tabs:

- 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 (M)

General Options (G) * Configuration:

Field	Value
* Class of Restriction (COR)	1
* Emergency Location Ext	66002
* Tenant Number	1
* SIP Trunk	Qaar
Coverage Path 1	
Lock Message	☐
Multibyte Language	Not Applicable
* Class Of Service (COS)	1
* Message Lamp Ext.	66002
Type of 3PCC Enabled	Avaya
Coverage Path 2	
Localized Display Name	Avaya, SIP 2
Enable Reachability for Station Domain Control	system

8. Configure AMC Technology DaVinci for Salesforce Service Cloud Voice

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

- Launch DaVinci Administration Tool
- Administer server
- Administer server profile
- Push server profile
- Administer CRM profile
- Administer agents
- Administer AMC Technology Cloud

Prior to integration, an identity certificate is assumed to be generated and installed on the DaVinci Premise Gateway to support encrypted browser connection from administrator PC within the enterprise to DaVinci web interface for configuration purposes.

The configuration of DaVinci Premise Gateway is performed by AMC Solution Engineers and the procedural steps are presented in these Application Notes for information purpose only.

The detailed configuration of AMC Technology Cloud on Google Cloud is also performed by AMC Solution Engineers and is outside the scope of these Application Notes.

8.1. Launch DaVinci Administration Tool

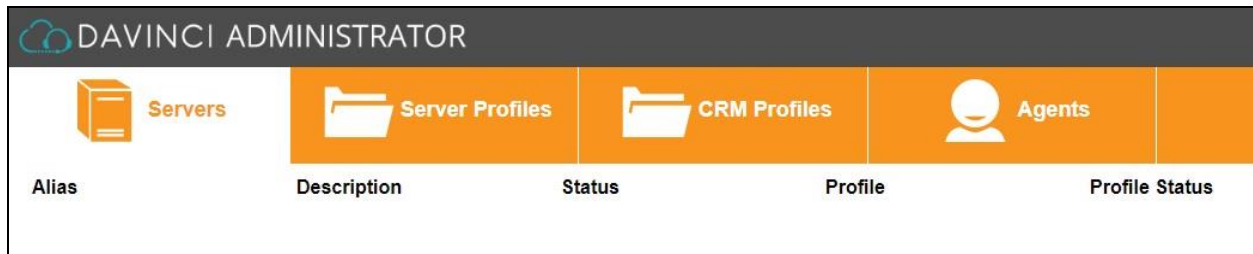
Launch the DaVinci Administration Tool web interface by using the URL **https://hostname/administrationtool** in a browser window, where **hostname** is the host name of the DaVinci Premise Gateway.

The **DAVINCI ADMINISTRATOR** screen below is displayed. Log in using the appropriate credentials.



8.2. Administer Server

The main **DAVINCI ADMINISTRATOR** screen is displayed. Select **Servers** from the top menu, followed by **New** (not shown) in the bottom left of screen to create a new server for integration with Application Enablement Services.



In the updated screen, enter pertinent values associated with the DaVinci Premise Gateway for **Hostname** and **FQDN**. Enter a desired **Description** and select **AES SOAP** as shown below.

The screenshot shows the 'New Server' form in the DAVINCI ADMINISTRATOR. The form has a dark background. On the left, there are three input fields: 'Hostname' with the value 'tlt-w2019', 'FQDN' with the value 'tlt-w2019', and 'Description' with the value 'Avaya AES 8.1'. In the center, there is a 'Choose Profile Template' dropdown menu. The dropdown is open, showing a list of options: 'Build from existing CCS Configuration', 'AACC Remoting', 'AACC SOAP', 'AACC Web', 'AES Routing Remoting', 'AES Routing SOAP', 'AES Routing Web', 'AES Remoting', 'AES SOAP' (which is highlighted), 'AES Web', 'AIC Remoting', 'AIC SOAP', 'Aspect ECS Remoting', 'Aspect ECS SOAP', 'Aspect ECS Web', and 'Aspect UIP Remoting'. On the right, there are two orange buttons: 'SAVE' with a floppy disk icon and 'CANCEL' with an 'X' icon.

8.3. Administer Server Profile

The main **DAVINCI ADMINISTRATOR** screen is displayed again. Select **Server Profiles** from the top menu, followed by the auto created server profile entry shown below, and click **Edit** (not shown) in the bottom left of screen.

DAVINCI ADMINISTRATOR			
 Servers	 Server Profiles	 CRM Profiles	 Agents
Name	Description	Server	Status
tit-w2019 Profile	Profile for tit-w2019	tit-w2019	Active

The screen below is displayed. Select **CTIModule** and click **EDIT**.

DAVINCI ADMINISTRATOR			
 Servers	 Server Profiles	 CRM Profiles	 Agents
 New  Edit  Delete			
Name tit-w2019 Profile		Modules [Global] [ModuleManager] [AgentManager] [DataStore] [EventManager] [StandardizedInterface] [CMGateway] [LicenseManager] [WorkManager] [SoapAdapter] [CTIModule] [AdministrationTool]	EDIT  DELETE  SAVE AS SAVE  CANCEL 
Description Profile for tit-w2019			

The **CTIModule** pane is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **ServerID:** The pertinent Tlink name from **Section 6.7**.
- **UserName:** The DaVinci user credentials from **Section 6.4**.
- **Password:** The DaVinci user credentials from **Section 6.4**.

For **UseAutoIn**, when the setting is at the default value of **1**, DaVinci will request Application Enablement Services to place agent into the **Auto In** state upon agent selection of **Available for Voice** from the desktop. For customers that prefer the **Manual In** state for agents, set the parameter to **0**. Both settings were tested in the compliance test.

The screenshot shows the DAVINCI ADMINISTRATOR interface. The top navigation bar includes 'Servers', 'Server Profiles', 'CRM Profiles', and 'Agents'. The 'Server Profiles' section is active, showing a profile named 'tlt-w2019 Profile' with the description 'Profile for tlt-w2019'. The 'CTIModule' configuration pane is displayed on the right, containing a list of parameters. Two red boxes highlight specific settings: the first box encloses 'ServerID=AVAYA#CM7#CSTA#AES7', '#ExtensionFile=<For Extra Monitoring Ex. VDNs/Path Ex. Program Files\AMC Techno', 'UserName=davinci', and 'Password=DaVinci123!'; the second box encloses 'UseAutoIn=1'.

```
[CTIModule]
# TraceEnabled=1
TraceLevel=4
TraceMaxSize=50240
DataStore=DataStore
Channel=CTI1
InternalExtLen=5
ServerID=AVAYA#CM7#CSTA#AES7
#ExtensionFile=<For Extra Monitoring Ex. VDNs/Path Ex. Program Files\AMC Techno
UserName=davinci
Password=DaVinci123!
AllowDTMF=Yes
DTMFPause=5
UseAutoIn=1
WorkmodePollInterval=500
BlockAgentStateEventDuringActiveCall=NO
FilterOriginatedEvent=NO
SynchronizeAgentStateInRegister=Yes
#-----
# NULL CONNECTOR
#-----
```

8.4. Push Server Profile

The main **DAVINCI ADMINISTRATOR** screen is displayed again. Select **Servers** from the top menu, followed by the created server entry from **Section 8.2**, and click **Edit** (not shown) from the bottom left of screen.

DAVINCI ADMINISTRATOR				
Servers	Server Profiles	CRM Profiles	Agents	
Alias	Description	Status	Profile	Profile Status
tlit-w2019	Avaya AES 8.1	Running	tlit-w2019 Profile	Pending

In the updated screen, select the **Server Profiles** entry and click **PUSH PROFILE** to push the configuration settings to the DaVinci Premise Gateway.

Hostname	tlit-w2019
FQDN	tlit-w2019
Description	Avaya AES 8.1

Server Profiles
tlit-w2019 Profile

PUSH PROFILE
START ▶
STOP ■
RESTART ↺

The main **DAVINCI ADMINISTRATOR** screen is displayed again with **Profile Status** for the server entry updated to **Active** as shown below.

DAVINCI ADMINISTRATOR				
Servers	Server Profiles	CRM Profiles	Agents	
Alias	Description	Status	Profile	Profile Status
tlit-w2019	Avaya AES 8.1	Running	tlit-w2019 Profile	Active

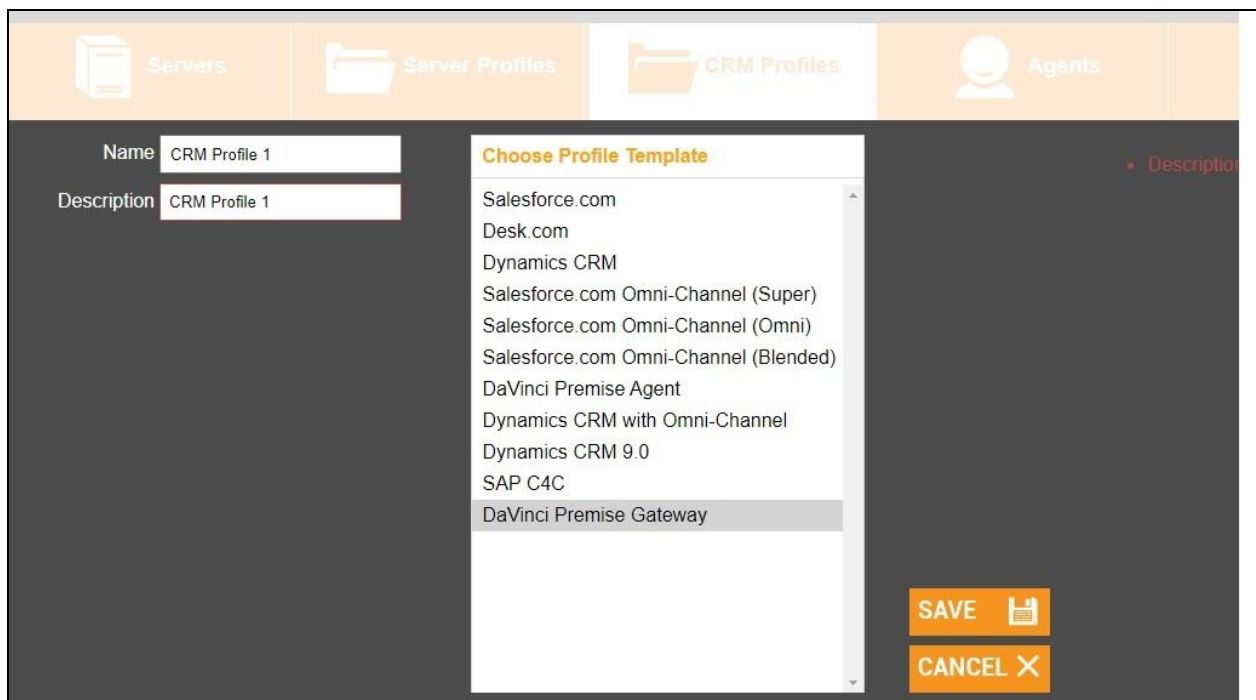
8.5. Administer CRM Profile

The main **DAVINCI ADMINISTRATOR** screen is displayed again. Select **CRM Profiles** followed by **New** (not shown) in the bottom left of screen to create a new profile.



The screenshot shows the DAVINCI ADMINISTRATOR interface. At the top, there's a header with the logo and title. Below it, a navigation bar has four tabs: Servers, Server Profiles, CRM Profiles (which is highlighted), and Agents. Below the navigation bar, there's a table with two columns: Name and Description. The table is currently empty.

In the updated screen, enter desired values for **Name** and **Description**. Select **DaVinci Premise Gateway** profile template as shown below.



The screenshot shows the DAVINCI ADMINISTRATOR interface with the CRM Profiles tab selected. A dialog box titled 'Choose Profile Template' is open in the center. It contains a list of templates: Salesforce.com, Desk.com, Dynamics CRM, Salesforce.com Omni-Channel (Super), Salesforce.com Omni-Channel (Omni), Salesforce.com Omni-Channel (Blended), DaVinci Premise Agent, Dynamics CRM with Omni-Channel, Dynamics CRM 9.0, SAP C4C, and DaVinci Premise Gateway (which is highlighted). To the left of the dialog, there are input fields for 'Name' and 'Description', both containing the text 'CRM Profile 1'. To the right of the dialog, there's a red asterisk and the text 'Description'. At the bottom right of the dialog, there are two buttons: 'SAVE' and 'CANCEL'.

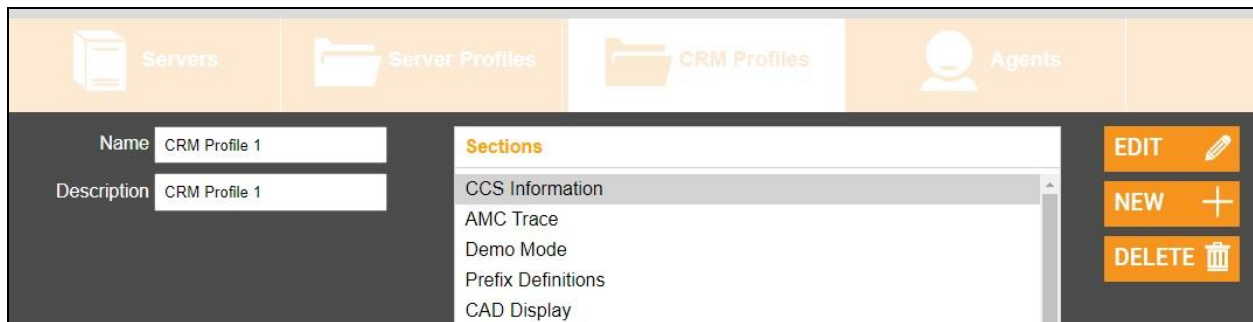
The main **DAVINCI ADMINISTRATOR** screen is displayed again. Select the newly created CRM profile entry and click **Edit** (not shown) from the bottom left of screen.



The screenshot shows the DAVINCI ADMINISTRATOR interface with the CRM Profiles tab selected. Below the navigation bar, there's a table with two columns: Name and Description. The table contains one entry: CRM Profile 1 in the Name column and CRM Profile 1 in the Description column.

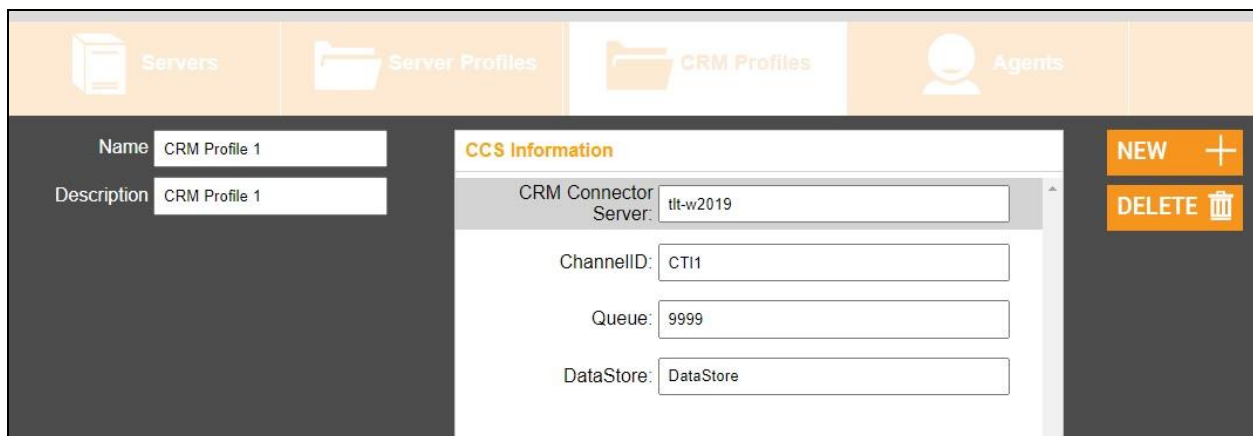
8.5.1. CCS Information

The **Sections** screen is displayed. Select **CCS Information** and click **EDIT**.



The screenshot shows the 'Sections' screen within the 'CRM Profiles' section. The top navigation bar includes 'Servers', 'Server Profiles', 'CRM Profiles', and 'Agents'. On the left, there are input fields for 'Name' and 'Description', both containing 'CRM Profile 1'. The main area is titled 'Sections' and contains a list of options: 'CCS Information', 'AMC Trace', 'Demo Mode', 'Prefix Definitions', and 'CAD Display'. The 'CCS Information' option is selected and highlighted. On the right side, there are three buttons: 'EDIT' with a pencil icon, 'NEW' with a plus icon, and 'DELETE' with a trash can icon.

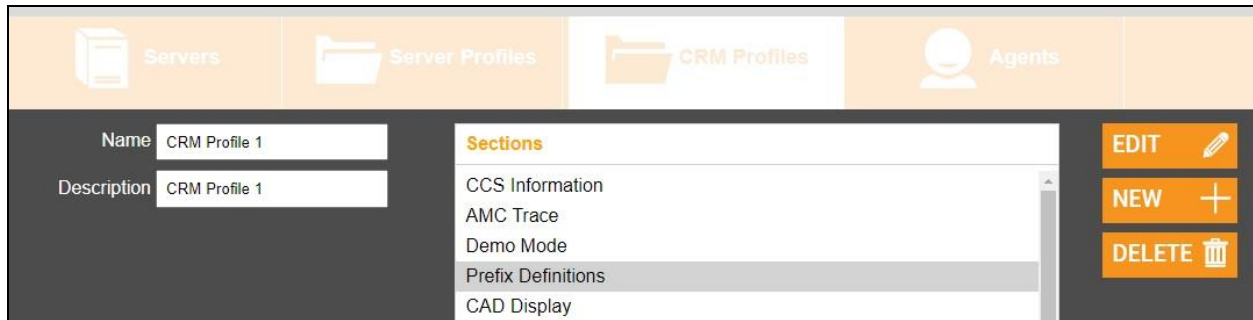
The **CCS Information** screen is displayed next. Enter the hostname of the DaVinci Premise Gateway for **CRM Connector Server** and retain the default values in the remaining fields.



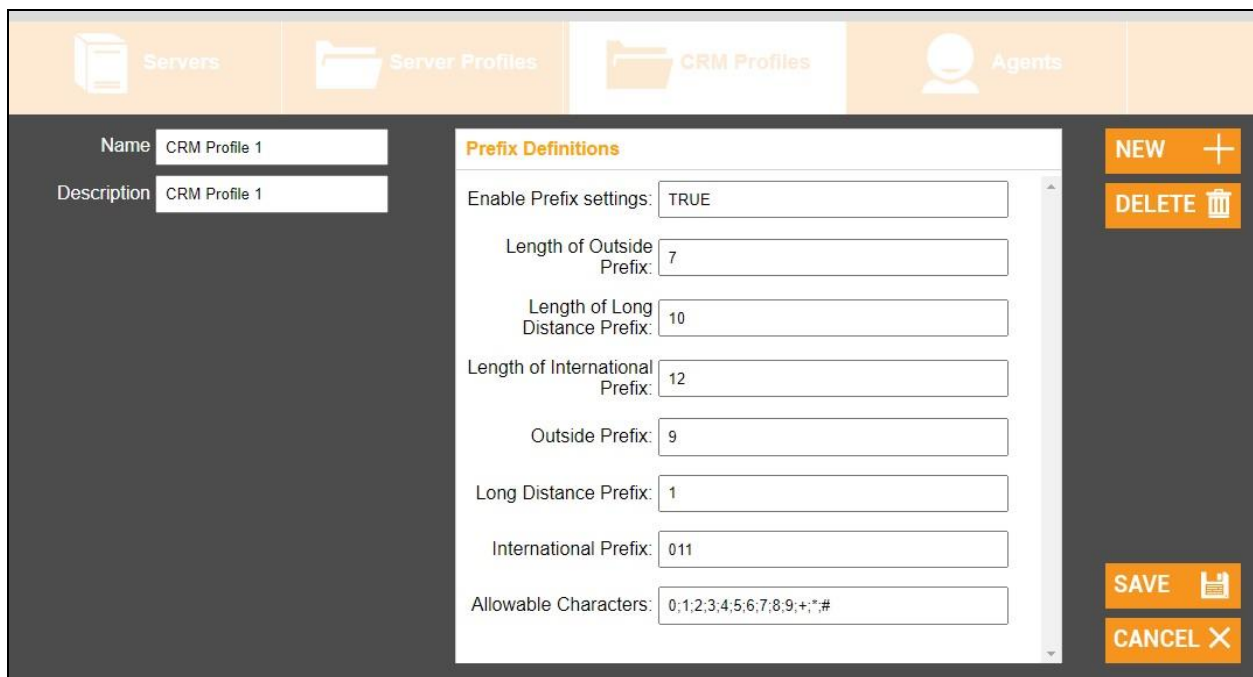
The screenshot shows the 'CCS Information' screen within the 'CRM Profiles' section. The top navigation bar is the same as the previous screen. On the left, the 'Name' and 'Description' fields still contain 'CRM Profile 1'. The main area is titled 'CCS Information' and contains several input fields: 'CRM Connector Server' with the value 'tlt-w2019', 'ChannelID' with the value 'CT11', 'Queue' with the value '9999', and 'DataStore' with the value 'DataStore'. On the right side, there are two buttons: 'NEW' with a plus icon and 'DELETE' with a trash can icon.

8.5.2. Prefix Definitions

The **Sections** screen is displayed again. Select **Prefix Definitions** and click **EDIT**.



The **Prefix Definitions** screen is displayed. Follow reference [x] to configure parameters as appropriate for any needed prefix insertion and processing for outbound calls for the customer network. In the compliance testing, the **Enable Prefix settings** parameter was set to **TRUE** and the remainder parameters were left at default values shown below.



8.5.3. DaVinci to CTI Presence

The **Sections** screen is displayed again. Select **DaVinci to CTI Presence** and click **EDIT**.

The screenshot shows the CRM Profiles configuration interface. The top navigation bar includes 'Servers', 'Server Profiles', 'CRM Profiles', and 'Agents'. The left sidebar shows 'Name' and 'Description' both set to 'CRM Profile 1'. The main area is titled 'Sections' and contains a list of configuration items: Internal Number, Login, CRM Specific Configuration, DTMF, CAD To CTI Mapping, Call Diversion, Call Preview, Channel Operations, Preview Wrapup Codes, Direct Preview Wrapup Codes, Session Timeout, Customization, Advanced, Live Presence, **DaVinci to CTI Presence** (highlighted), and CTI to DaVinci Presence. On the right, there are buttons for 'EDIT', 'NEW', 'DELETE', 'SAVE AS', 'SAVE', and 'CANCEL'.

The **DaVinci to CTI Presence** screen is displayed. Follow reference [x] to create and configure **Not Ready** parameters to match the reason codes from **Section 5.4** as shown below.

The screenshot shows the 'DaVinci to CTI Presence' configuration screen. The top navigation bar and left sidebar are the same as the previous screen. The main area is titled 'DaVinci to CTI Presence' and contains several input fields for configuring presence states: 'Ready' (set to 'Ready'), 'Pending Ready' (set to 'Ready|||pendingready'), 'Pending Not Ready|Lunch' (set to 'NotReady|Lunch|0|pendingnotready'), 'Pending Not Ready|Break' (set to 'NotReady|Break|1|pendingnotready'), 'Pending ACW' (set to 'WorkNotReady|||pendingworknotready'), 'Not Ready|Meeting' (set to 'NotReady|Meeting|1'), and 'Not Ready|Lunch' (set to 'NotReady|Lunch|2'). On the right, there are buttons for 'NEW', 'DELETE', 'SAVE', and 'CANCEL'.

8.5.4. CTI to DaVinci Presence

The **Sections** screen is displayed again. Select **CTI to DaVinci Presence** and click **EDIT**.

The screenshot shows the 'CRM Profiles' section of the application. The 'Name' and 'Description' fields are both set to 'CRM Profile 1'. The 'Sections' list on the right includes the following items: Internal Number, Login, CRM Specific Configuration, DTMF, CAD To CTI Mapping, Call Diversion, Call Preview, Channel Operations, Preview Wrapup Codes, Direct Preview Wrapup Codes, Session Timeout, Customization, Advanced, Live Presence, DaVinci to CTI Presence, and CTI to DaVinci Presence. The 'CTI to DaVinci Presence' item is highlighted. Action buttons on the right include EDIT, NEW, DELETE, SAVE AS, SAVE, and CANCEL.

The **CTI to DaVinci Presence** screen is displayed. Follow reference [x] to create and configure **Not Ready** parameters to match the reason codes from **Section 5.4** as shown below.

The screenshot shows the 'CTI to DaVinci Presence' configuration screen. The 'Name' and 'Description' fields are both set to 'CRM Profile 1'. The configuration parameters are as follows:

Parameter	Value
Ready:	Ready
WorkNotReady:	ACW
NotReady:	Not Ready
OnInteraction:	On an interaction
pendingnotready Lunch	Pending Not Ready Lunch
pendingnotready Break	Pending Not Ready Break
NotReady Meeting 1:	Not Ready Meeting
NotReady Lunch 2:	Not Ready Lunch

Action buttons on the right include NEW, DELETE, SAVE, and CANCEL.

8.6. Administer Agents

The main **DAVINCI ADMINISTRATOR** screen is displayed again. Select **Agents** followed by **New** (not shown) in the bottom left of screen to create an agent.

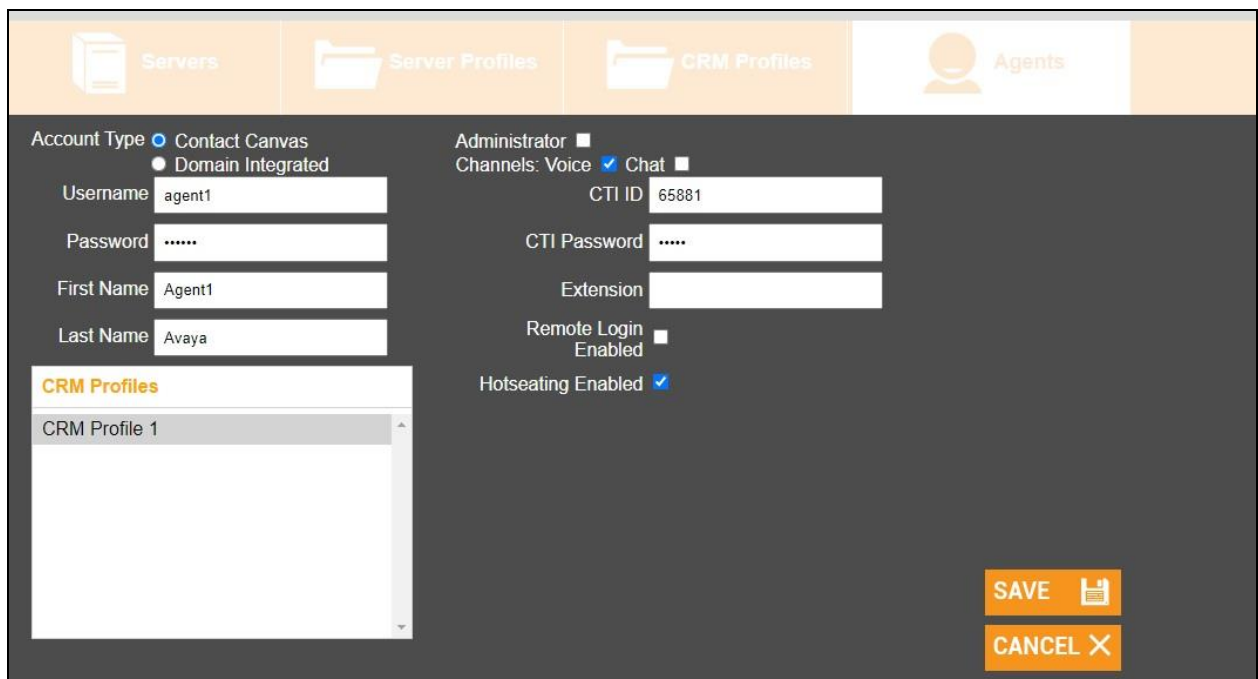


The screenshot shows the DAVINCI ADMINISTRATOR interface. At the top, there's a header with the application name and a navigation bar with five tabs: Servers, Server Profiles, CRM Profiles, Agents (selected), and an empty tab. Below the navigation bar, there's a summary card for the selected agent. The card displays the following information:

Username	Full Name	CRM Profile	Channels	Is Administrator
admin		n/a		☒

The screen below is displayed next. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Username:** The desired credentials for the agent.
- **Password:** The desired credentials for the agent.
- **First Name:** The pertinent first name for the agent.
- **Last Name:** The pertinent last name for the agent.
- **Voice:** Check this channel, which enables additional fields below.
- **CTI ID:** Enter the pertinent agent login ID from **Section 3**.
- **CTI Password:** Enter the pertinent agent login password from **Section 3**.
- **Extension:** Enter the pertinent agent station from **Section 3** when seating is fixed.
- **Hotseating Enabled:** Check this field when agent seating is flexible.



The screenshot shows the agent creation form in the DAVINCI ADMINISTRATOR. The form is divided into several sections:

- Account Type:** Radio buttons for ☒ Contact Canvas and ☐ Domain Integrated.
- Administrator:** A checkbox ☐.
- Channels:** Checkboxes for Voice ☒ and Chat ☐.
- Username:** Text field with value "agent1".
- Password:** Text field with masked characters ".....".
- CTI ID:** Text field with value "65881".
- First Name:** Text field with value "Agent1".
- CTI Password:** Text field with masked characters ".....".
- Last Name:** Text field with value "Avaya".
- Extension:** Text field.
- Remote Login Enabled:** Checkbox ☐.
- Hotseating Enabled:** Checkbox ☒.
- CRM Profiles:** A dropdown menu showing "CRM Profile 1".
- Buttons:** "SAVE" and "CANCEL" buttons at the bottom right.

Repeat the procedures in this section to create the desired number of agents. In the compliance testing, two agents were created as shown below.

DAVINCI ADMINISTRATOR				
Servers	Server Profiles	CRM Profiles	Agents	
Username	Full Name	CRM Profile	Channels	Is Administrator
admin		n/a		☒
agent1	Agent1 Avaya	CRM Profile 1	Phone	☐
agent2	Agent2 Avaya	CRM Profile 1	Phone	☐

8.7. Administer AMC Technology Cloud

Launch the AMC Technology Cloud web interface by using the URL <https://studio.contactcanvas.com> in a browser window.

The **DAVINCI** screen below is displayed. Log in using the appropriate credentials provided by AMC Technology.


DAVINCI
creators studio

Welcome to DaVinci Creators Studio
Log-in to browse, add, and configure available apps and users.

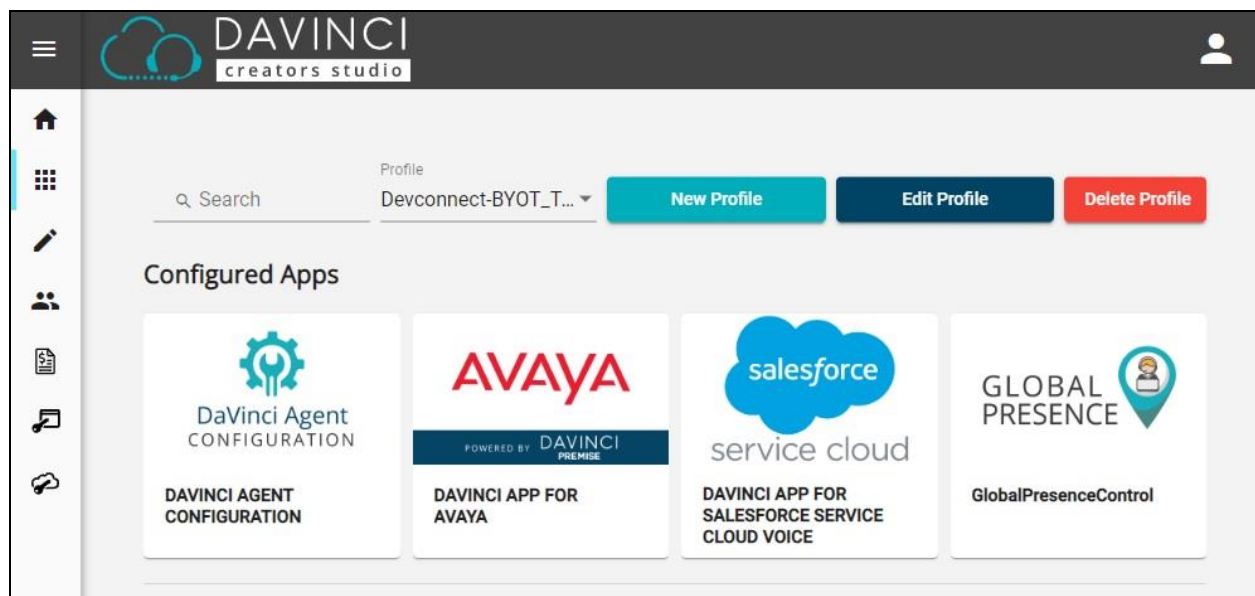
[Need an account? Sign-up for free](#)

In the subsequent screen, select the **Apps** icon from the left pane to display the **Configured Apps** screen below.

Make certain that **Profile** is set to the pertinent pre-configured profile, in this case **DevConnect-BYOT_Test**, and that all four apps shown below are configured for the profile.

In addition, the apps associated with Salesforce Service Cloud and Global Presence need to be configured to have not ready reason codes to match **Section 5.4**.

Select the app associated with Salesforce Service Cloud, in this case **DAVINCI APP FOR SALESFORCE SERVICE CLOUD VOICE**.



8.7.1. Salesforce Service Cloud

The **DAVINCI APP FOR SALESFORCE SERVICE CLOUD VOICE** screen is displayed. Select **Config** from the left pane followed by **PresenceMapping**. Configure a **salesforceToChannel** variable with reason codes from **Section 5.4**, as shown in bottom of screen below.

The screenshot displays the configuration interface for the 'DAVINCI APP FOR SALESFORCE SERVICE CLOUD VOICE'. The left sidebar contains a navigation menu with 'Config' and 'PresenceMapping' selected. The main content area shows the 'PresenceMapping' configuration. A table of variables is visible, with the 'salesforceToChannel' variable highlighted by a red box. This variable is of type 'map' and has two values: 'Lunch' and 'Meeting'.

Name*	Type	Value
channelToSalesforce	map	Key ACW Not Ready Not Ready Not Ready On an inte
salesforceToChannel	map	Key After Call ' Available f Lunch Meeting

8.7.2. Global Presence

From the **Configured Apps** screen in **Section 8.7**, select the app associated with Global Presence, in this case **GlobalPresenceControl**.

The **GlobalPresenceControl** screen is displayed. Select **Config** from the left pane followed by **GlobalPresenceControl** → **ConfiguredPresences** → **Not Ready**. Configure the not ready **reasonCodes** parameter with reason codes from **Section 5.4**, as shown in bottom of screen below.

GLOBAL PRESENCE

Overview
Setup
Config
User Config

GlobalPresenceControl

Configuration

- GlobalPresenceControl
 - ConfiguredPresences
 - Pending Login
 - Not Ready
 - ACW
 - Cases
 - On an interaction
 - Pending Ready
 - Pending Not Ready
 - Pending ACW
 - Pending Parked
 - Ready
 - Missed Call
 - Leads
 - Logout

Node Name
Not Ready

+ Add child node

Variables

	Name*	Type	Value
+			
-	viewOnlyReasonCodes	array	+ Login
-	displayPresence	boolean	True
-	order	number	2
-	icon	string	assets/user_notr
-	reasonCodes	array	+ Lunch Break

9. Verification Steps

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

9.1. 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	9860	9854

9.2. 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 agents from **Section 3** that are logged into the ACD via DaVinci, in this case **2**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Fri Jul 15 09:14:47 2022 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: 8.1.3.4.0.2-0
Server Date and Time: Fri Jul 15 09:58:11 EDT 2022
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

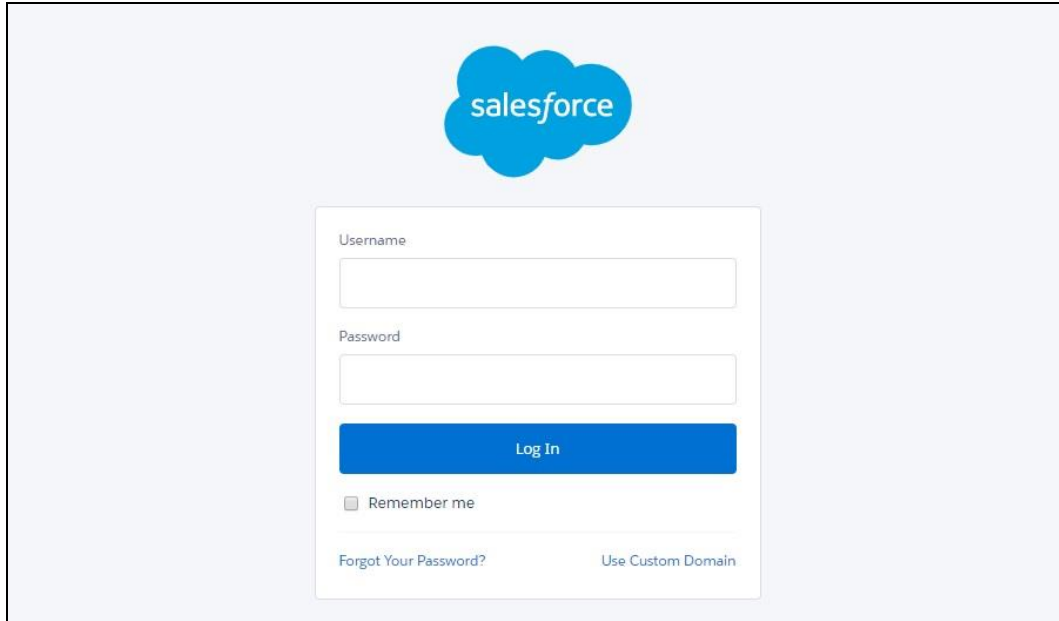
TSAPI Link Details

☐ Enable page refresh every 60 seconds

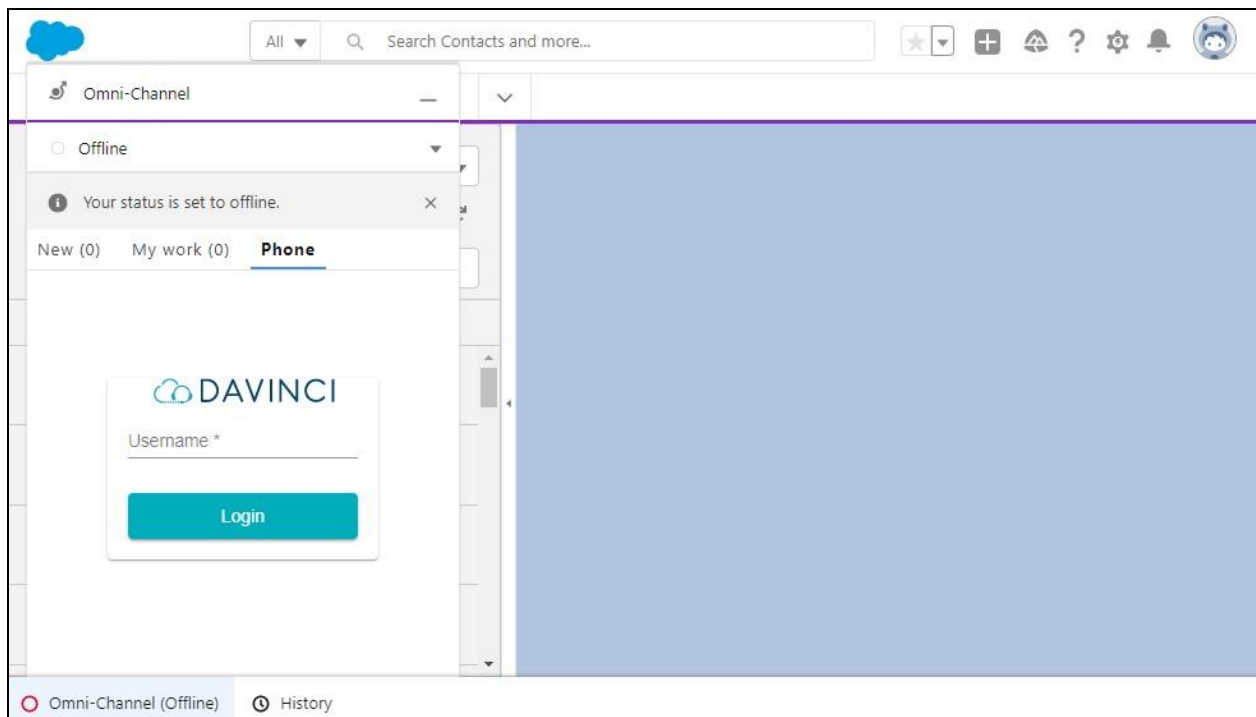
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
☒	1	cm7	1	Talking	Fri Jul 15 09:24:07 2022	Online	18	2	10222	10228	30

9.3. AMC Technology DaVinci for Salesforce Service Cloud Voice

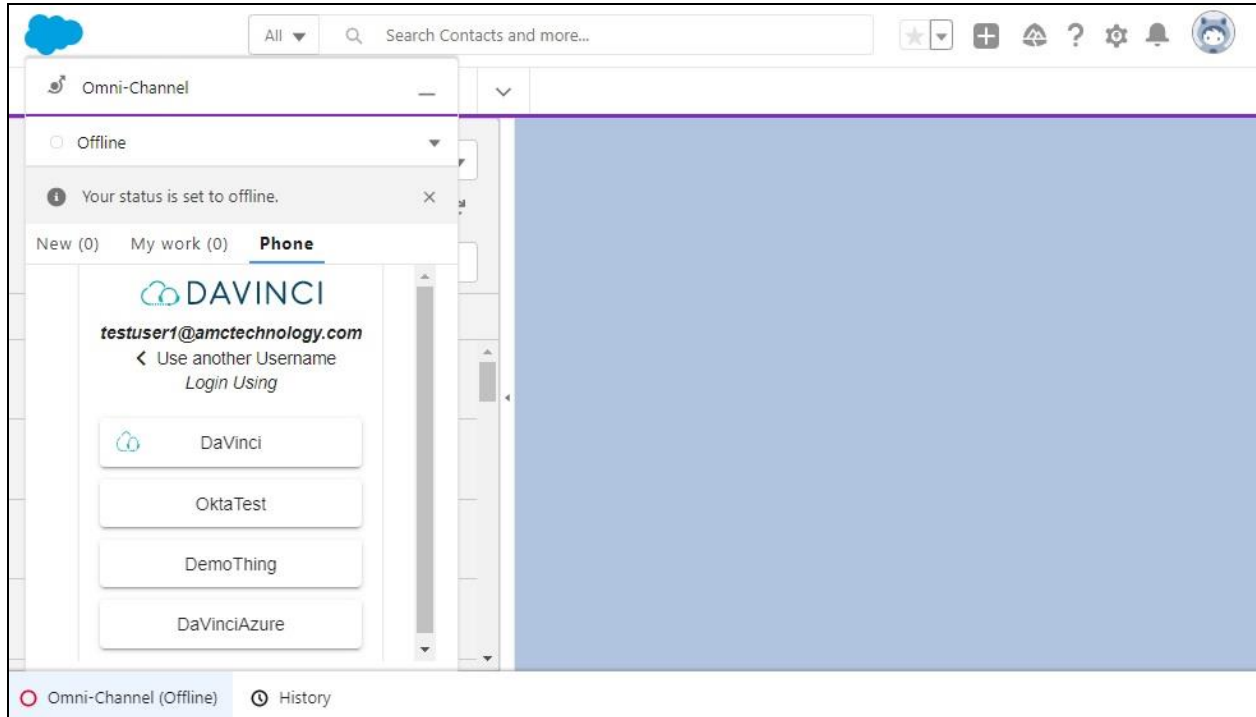
From an agent PC, launch a browser window and enter the URL provided by the end customer for Salesforce.com. Log in with the relevant user credentials provided by the end customer.



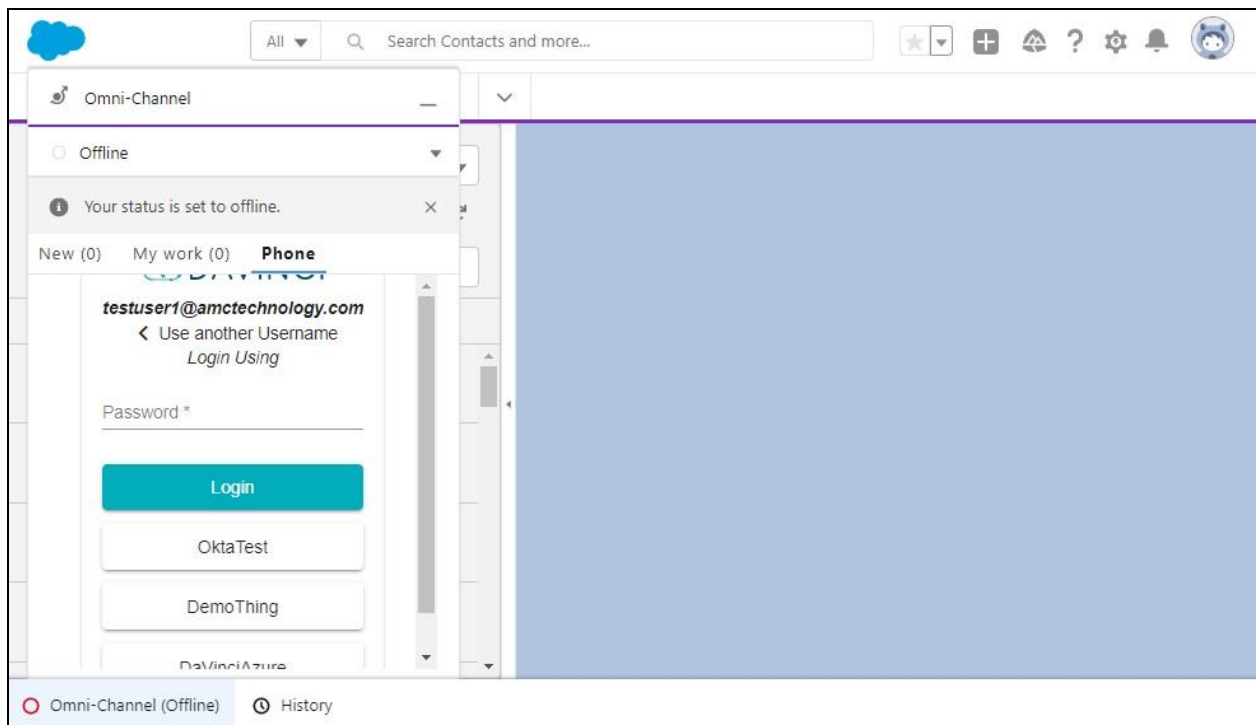
The screen below is displayed next. Log in with a relevant user credential provided by AMC Technology.



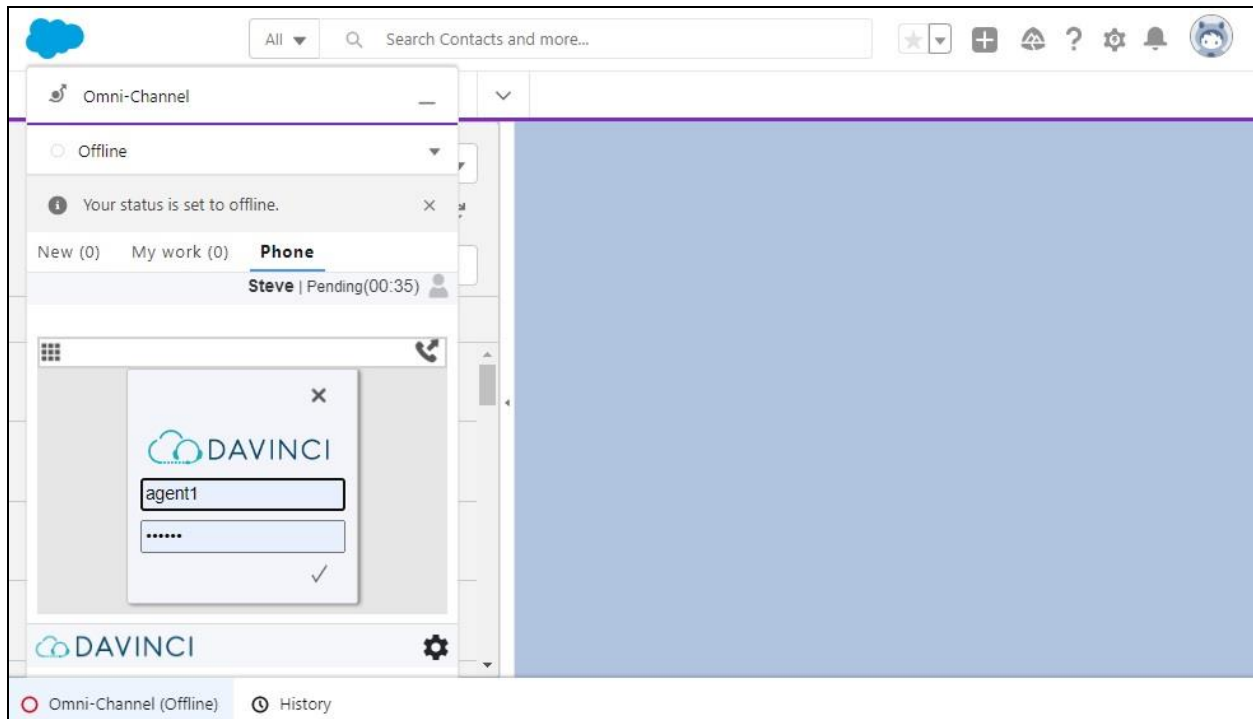
The **Omni-Channel** screen below is displayed. Select **DaVinci**.



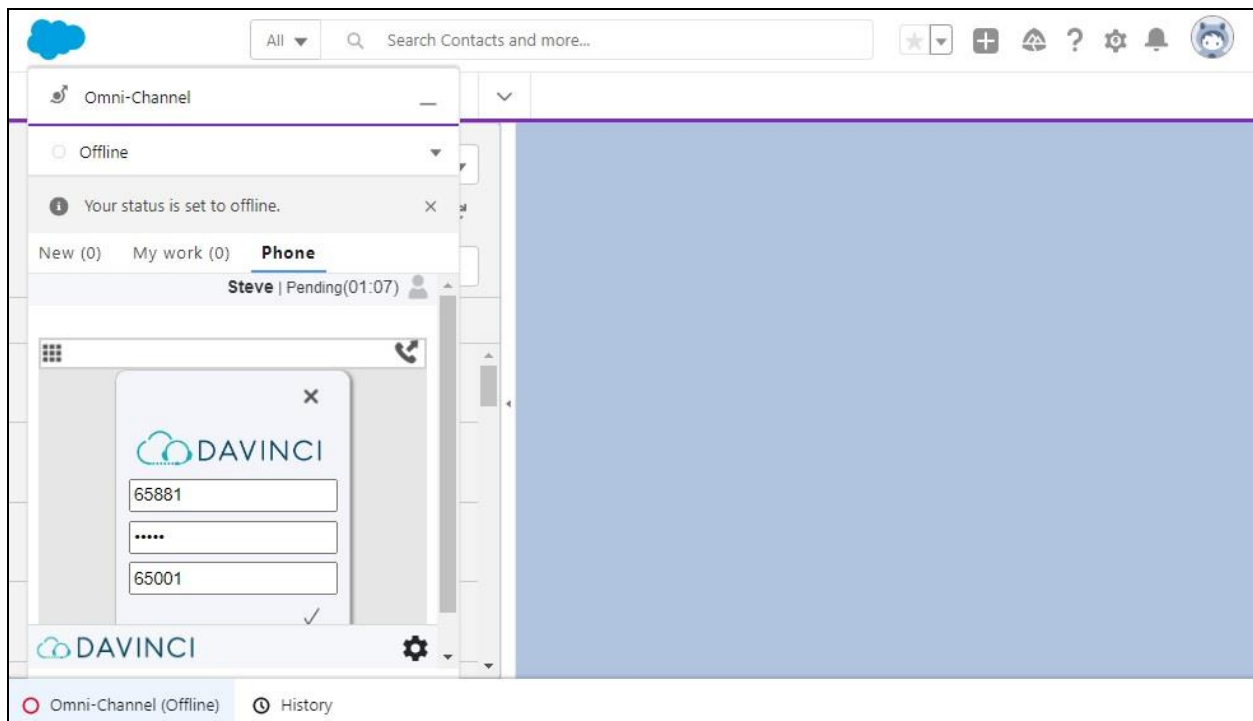
In the updated **Omni-Channel** screen, enter the relevant user password from AMC Technology and select **Login**.



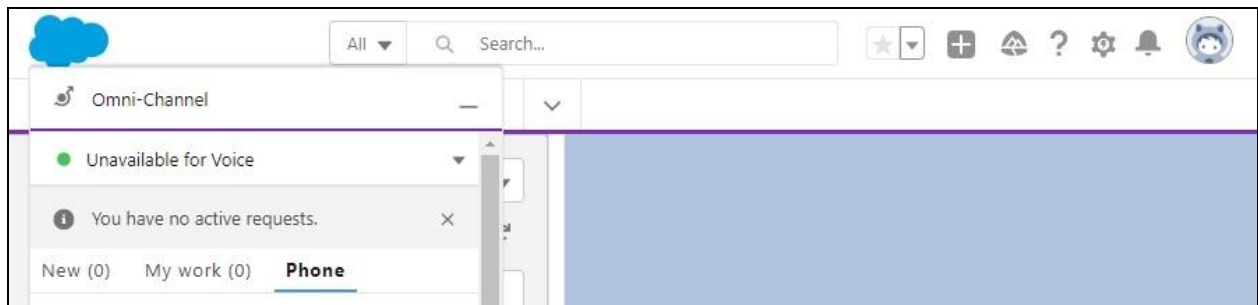
The **Omni-Channel** screen below is displayed next. Enter an agent credential for DaVinci from **Section 8.6** as shown below.



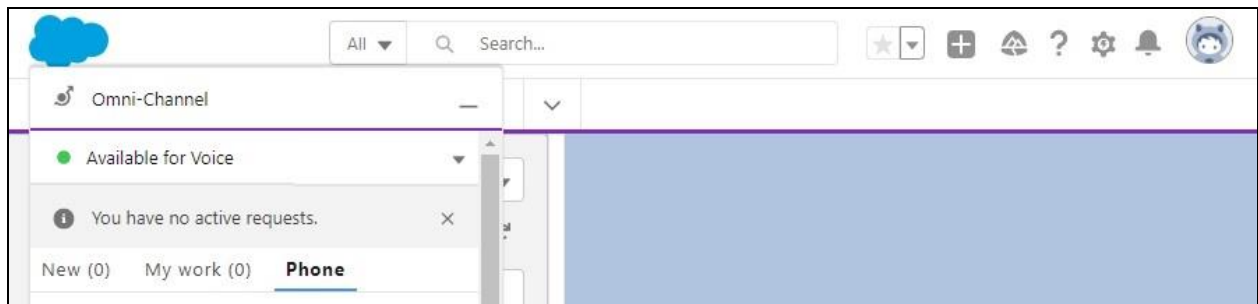
In the updated screen, enter the pertinent agent ID credentials and station extension from **Section 3** as shown below.



Verify that the **Omni-Channel** screen is updated as shown below. Expand the drop-down icon next to **Unavailable for Voice** and select **Available for Voice** (not shown).

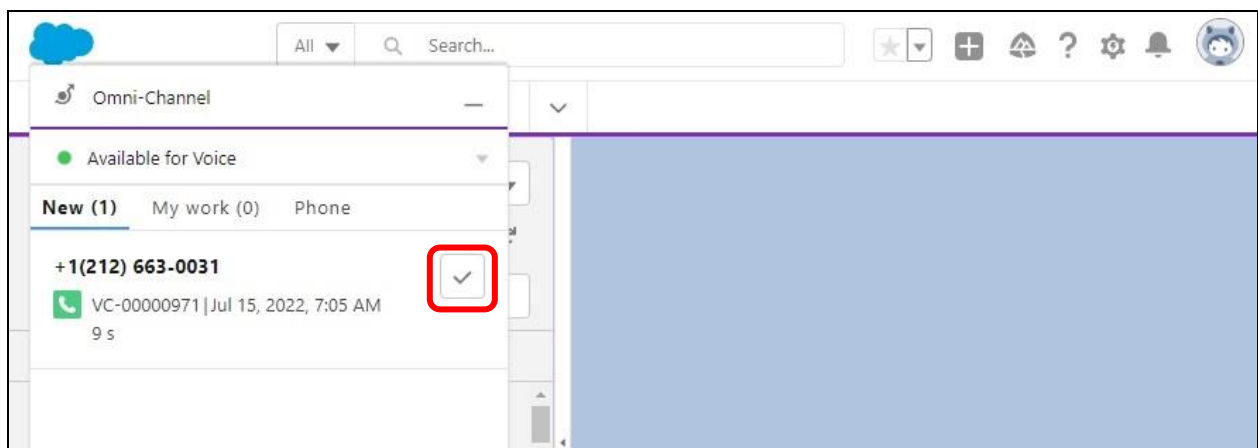


Verify that the **Omni-Channel** screen is updated to reflect **Available for Voice**.

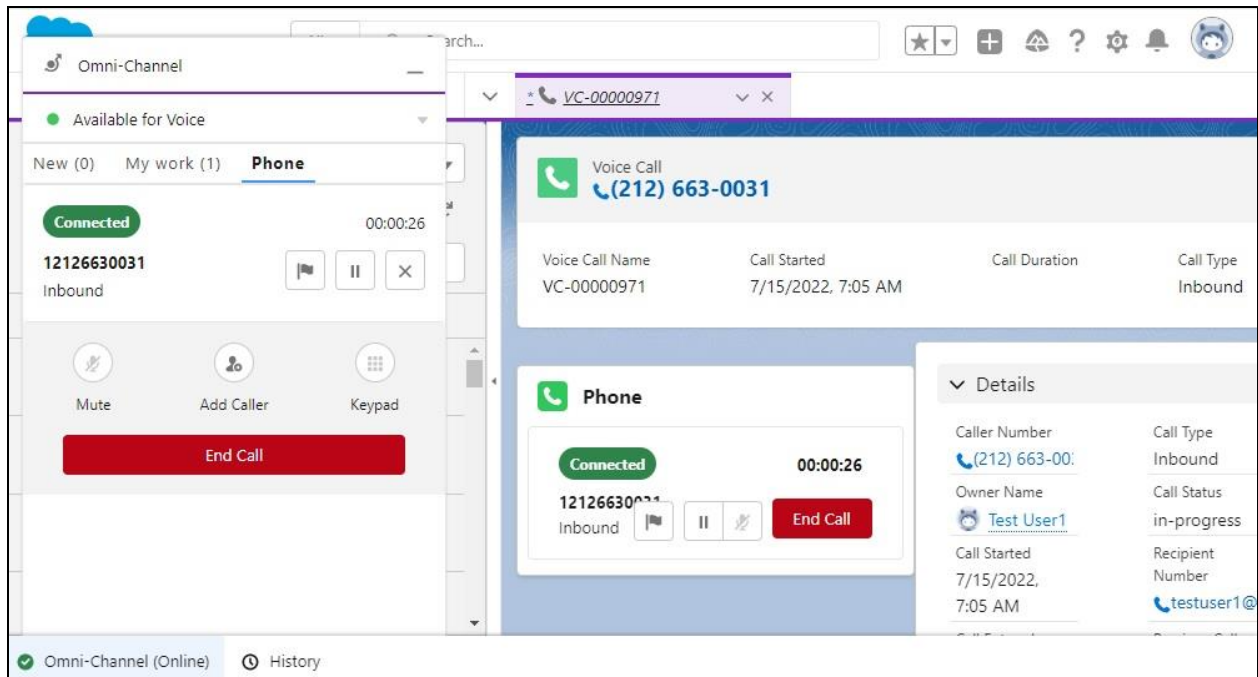


Make an incoming ACD call from the PSTN. Verify that the **Omni-Channel** screen is updated to reflect the incoming call as shown below.

Click on the check mark in the **Omni-Channel** screen to accept the call.



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



10. Conclusion

These Application Notes describe the configuration steps required for AMC Technology DaVinci App for Salesforce Service Cloud Voice 7.0 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. 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 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. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, September 2021, available at <http://support.avaya.com>.
4. *DaVinci for Service Cloud Voice Overview*, **how can readers obtain a copy?**
5. SCV Driver for Avaya Aura Application Enablement Services (AES) Implementation Guide, **should this be referenced, and if so how can readers obtain a copy?**
6. **Is there a user manual equivalent?**

©2022 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.