



## Avaya Solution & Interoperability Test Lab

---

# **Application Notes for Configuring AMC Technology's DaVinci Premise Server Version 7.0 with Avaya Aura® Application Enablement Services Release 8.1 - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps to integrate AMC Technology's DaVinci Premise Server with Avaya Aura® Application Enablement Services and Call Center Elite of Avaya Aura® Communication Manager to allow various Customer Relationship Management (CRM) applications, using AMC Technology's DaVinci, connection to the Avaya solution.

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 to integrate AMC Technology's DaVinci Premise Server R7.0 with Avaya Aura® Application Enablement Services Release 8.1 with a contact center environment provided by Avaya Aura® Communication Manager in order to allow various Customer Relationship Management (CRM) applications, using AMC Technology's DaVinci Premise Server, connection to the Avaya solution.

AMC Technology's DaVinci CRM integration solution for Avaya provides pre-packaged, server-based integration that delivers real-time connectivity with business applications including Microsoft Dynamics 365, SAPC4C, ServiceNow, Zendesk, Salesforce Oracle Siebel and SAP CRM. Companies can enable full CTI functionality in their CRM desktop including softphone controls, caller identification, and screen population. Agents can place, receive, and transfer customer interactions with full, real-time access to CRM customer data.

AMC Contact Center solutions are built on the AMC DaVinci Platform, which includes DaVinci Premise Server. Through its open architecture, the AMC product suite enables contact centers to integrate a variety of communication channels across different platforms, using new or existing infrastructure, creating a true multi-channel and multi-vendor contact center.

Call center agents and knowledge workers can place, receive, transfer and conference customer interactions with full, real-time access to customer information. Screen Pop is enabled through DaVinci's ability to transfer data from the CTI into an instant, convenient display of customer information in the CRM application.

AMC Technology's DaVinci solution for Avaya Aura® Application Enablement Services contains four (4) main components:

- 1) DaVinci Premise Server.
- 2) AMC Driver, which provides Computer Telephony Integration (CTI) through the Telephony Service Application Program Interface (TSAPI) that enables Call Control, Agent Session Control and Screen Pops.
- 3) AMC Adapter which provides connectivity by directly integrating to premise-based CRM applications.
- 4) AMC DaVinci Premise Gateway, which provides connectivity for cloud-based CRM applications through DaVinci CRM Apps.

**Note:** Integration for cloud-based CRM applications – Microsoft Dynamics 365, Salesforce, SAPC4C, ServiceNow and Zendesk – is through the DaVinci Agent UI and the DaVinci Premise Gateway. DaVinci Agent UI is a browser toolbar component that is embedded within the CRM application iFrame. It connects to DaVinci Premise Server through the DaVinci Premise Gateway, a web service for hybrid deployments.

Integration of premise-based applications – SAP CRM and Oracle Siebel – is through application channel toolbars that connect through adapters that reside on the DaVinci Premise Server, for a pure premise deployment.

## 2. General Test Approach and Test Results

The general test approach was to verify the interoperability of the DaVinci Premise Gateway successfully integrates with Application Enablement Services using TSAPI. The seven different CRM applications were tested during compliance testing: five cloud-based and two premise-based CRMs.

### Cloud-based CRM Applications.

1. Salesforce
2. MS Dynamics 365
3. ServiceNow
4. Zendesk
5. SAP C4C

### Premise-based CRM Applications.

6. Oracle Siebel
7. SAP CRM

Each CRM was tested separately using the same test cases for each CRM/adaptor. The connection to the Avaya solution was identical for each of the seven adaptors that were tested, and the piece of middleware called DaVinci Premise Server was the product compliance tested.

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 systems and the AMC Technology DaVinci Platform did not include the use of any specific encryption features as requested by AMC Technology.

This test was conducted in a lab simulating a basic customer environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The

results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third-party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

## **2.1. Interoperability Compliance Testing**

The interoperability compliance test verified the following feature functionality:

- Logging in and out of a skill/split
- Monitoring agent states (e.g., Ready or Not Ready)
- Agent State synchronization with Agent Telephones
- Establishing calls with other agents and non-monitored devices and verifying the correct call states
- Screen pop consisting of customer or business partner information using ANI for calls
- Basic telephony features such as call hold/resume, blind/supervised transfer, and 3-way conference
- Restarting the AMC DaVinci Premise Server

## 2.2. Test Results

All test cases were executed and passed. The following observation was noted during the compliance test:

### Oracle Siebel experienced the following issues.

1. Some lag in time was experienced on the Siebel toolbar. This was on the AMC side between the premise Siebel server and client so when a call is presented to the phone set it may ring there for up to 5 seconds before the DaVinci softphone shows the incoming call and gets answered. These lag times are consistent with several mitigating factors in the test environment:
  - a. A complex network connection through two VPNs between the AMC-based premise Siebel application server, the DaVinci Premise Server, and the Avaya Application Enablement Services channel services running within the Avaya lab.
  - b. The AMC-based premise Siebel application server is not tuned for production and running on a lab VM environment with limited operating system resources (amount of memory, storage, etc.).
  - c. High local traffic and limited Internet connection bandwidth within the AMC lab environment.
2. The “transfer complete” seemed to take some time lag on the Siebel side, the screen pop was not transferred as a result.

### SAP CRM experienced the following issues.

1. As the agent opens the conference call it cannot drop individual joined party instead of disconnecting itself from the conference by selecting the Hang Up button.
3. Some lag in time was experienced on the SAP Toolbar as agent controls the call. Again, these lag times are consistent with the mitigating factors identified above for the Siebel application integration.

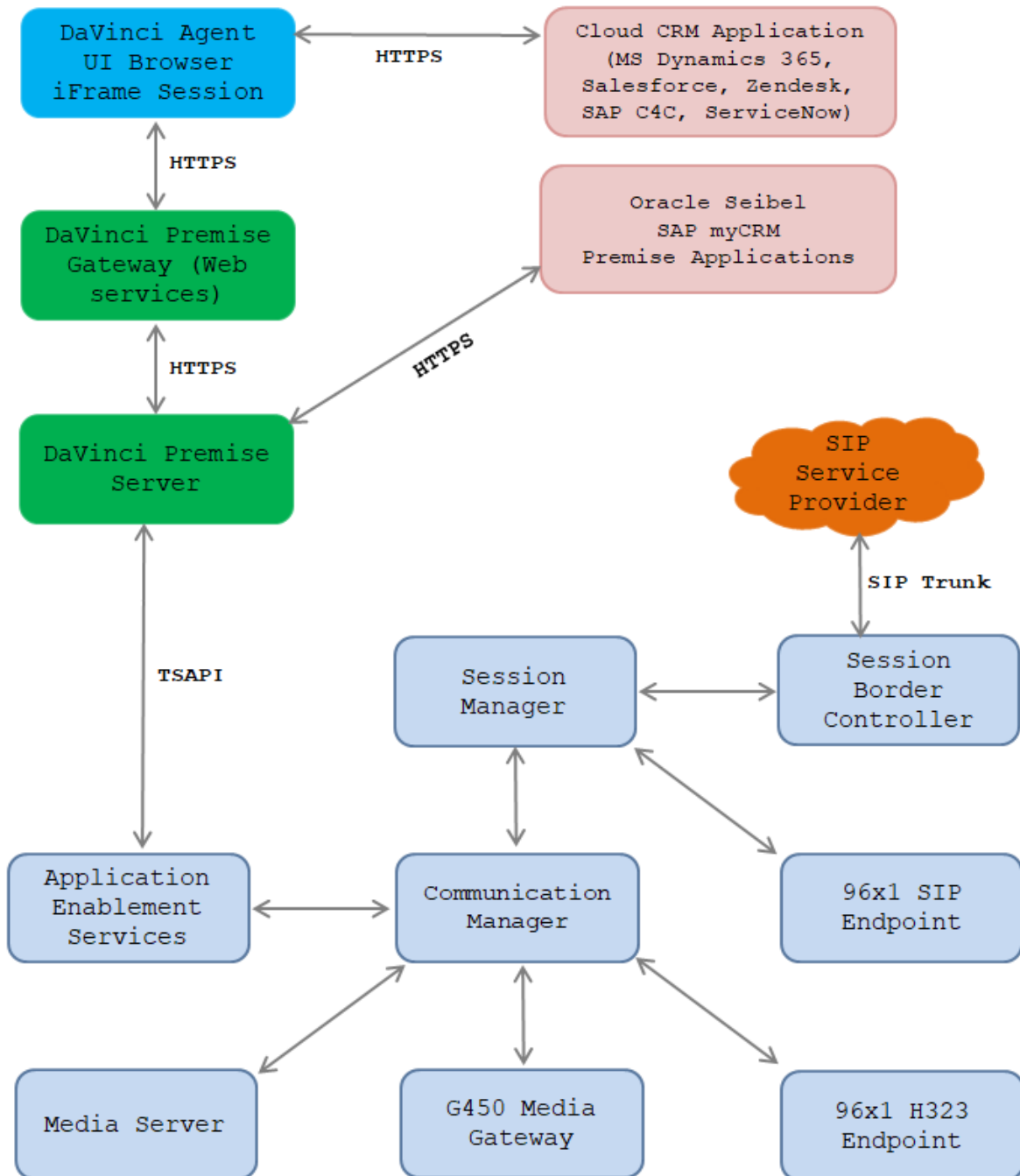
## 2.3. Support

Technical support for AMC Technology can be found as follows:

- Web Portal: <http://www.amctechnology.com/support/>
- Phone contact: +1 804 419 8600 or +1 800 390 4866

### 3. Reference Configuration

The **Figure 1** below illustrates the test configuration diagram for the compliance test. In the test diagram, the DaVinci Premise server established a connection to Application Enablement TSAPI services.



**Figure 1 Test Configuration Diagram**

## 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 running on Virtualized Environment	R8.1.1.0 R018x.01.0.890.0 01.0.890.0-25763
Avaya Aura® System Manager running on Virtualized Environment	System Manager 8.1.1.0 Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.1.0.0310503 Feature Pack 1
Avaya Aura® Session Manager running on Virtualized Environment	R8.1.1.0 Build No. – 8.1.1.0.811021
Avaya Aura® Application Enablement Services	R8.1.1.0 Build No – 8.1.1.0.2.8-0
Avaya Session Border Controller for Enterprise (used to simulate PSTN)	8.1.0.0-14-18490
Avaya Aura® Media Server running on Virtualized Environment	8.0.1.121_2019.04.29
Avaya G450 Media Gateway	41.16.0
Avaya 96x1 IP Deskphones	H323 Release 6.8304 SIP Release 7.1.7.0.11
AMC Technology DaVinci Premise Server (resides on a Windows 2016 64-bit Operating System) AMC Connector <ul style="list-style-type: none"><li>• Salesforce Open CTI</li><li>• Oracle Siebel</li><li>• SAP CRM</li><li>• MS Dynamics 365</li><li>• SAP C4C</li><li>• Service Now</li><li>• Zendesk</li></ul>	DaVinci Premise Server 7.0 DaVinci Driver for Avaya Application Enablement Services  DaVinci Premise Gateway 7.0.0.3 DaVinci Adapter for SAP 7.0 DaVinci Adapter for Siebel 7.0

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager.

### 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	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>		
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y		
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y		
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y		
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y		

### 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					
<b>Extension: 3331</b>					
<b>Type: ADJ-IP</b>					
COR: 1					
Name: AES8					
Unicode Name? n					



### 5.3. 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: 1
    Copy UCID for Station Conference/Transfer? y
```

Navigate to **Page 13** and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to ASAI and it will be used by the TSAPI application.

```
change system-parameters features                                     Page 13 of 20
                                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 UII During Conference/Transfer? y
    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. Administer AE Services

To administer the transport link to AES, use the command “**chang ip-services**”. On **Page 1**, add an entry with the following values. Service Type should be selected as **AESVCS**, enter “**y**” in the **Enabled**, “**procr**” in the **Local Node** and **8765** in the **Local Port**.

change ip-services						Page	1	of	4
IP SERVICES									
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port				
<b>AESVCS</b>	<b>y</b>	<b>procr</b>	<b>8765</b>						

Go to **Page 4**, enter the following values. **AE Services Server** should be the AES host name, enter a password in the **Password** field and select “**y**” in the **Enabled** field.

**Note:** The password entered for **Password** field must match the password on the AES server in the Switch Connection in **Section 6.3**. The **AE Services Server** should match with the host name of the AES server. To obtain the host name of AES server, use the command “**uname -n**” in the Linux command prompt.

change ip-services					Page	4	of	4
AE Services Administration								
Server ID		AE Services Server		Password		Enabled		Status
1:		aes8		*		y		in use
2:		aes81		*		y		in use

## 5.5. Administer Hunt Group

This section provides the Hunt Group configuration for the call center agents. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.8**.

add hunt-group 1	Page 1 of 4
HUNT GROUP	
Group Number: 1	ACD? y
Group Name: Skill-1	Queue? y
Group Extension: 3320	Vector? y
Group Type: ucd-mia	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited	
Calls Warning Threshold:	Port:
Time Warning Threshold:	Port:
SIP URI:	

On **Page 2** of the Hunt Group form, enable the **Skill** option and **Both** in the **Measured** field.

add hunt-group 1	Page 2 of 4
HUNT GROUP	
Skill? y	Expected Call Handling Time (sec): 180
AAS? n	Service Level Target (% in sec): 80 in 20
Measured: both	
Supervisor Extension:	
Controlling Adjunct: none	
VuStats Objective:	
Multiple Call Handling: none	
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n

## 5.6. Administer Vector

Use the command “**change vector n**” while “n” is the vector number from 1-8000. The example of the vector 1 with the basic scripting is shown below. The vector 1 is used for the configuration of VDN in the next step.

```
change vector 1                                     Page 1 of 6
                                           CALL VECTOR
      Number: 1                                Name: Contact Center
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock?
n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing?
y
      Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
      Variables? y      3.0 Enhanced? y
01 wait-time      10      secs hearing 1100      then silence
02 queue-to      skill 1      pri m
03 wait-time      5      secs hearing ringback
04 check      skill 1      pri m if expected-wait      < 30
05 announcement 1104
06 queue-to      skill 1      pri m
07 stop
```

## 5.7. Administer VDN

Use the “**add vdn <ext>**” command to add a VDN number. In the **Destination** field, enter **Vector Number 1** as configured in **Section 5.6** above and keep other fields at their default values.

```
add vdn 3340                                     Page 1 of 3
                                           VECTOR DIRECTORY NUMBER

                                           Extension: 3340
                                           Name*: Contact Center 1
                                           Destination: Vector Number 1
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: both      Report Adjunct Calls as
ACD*? n
Acceptable Service Level (sec): 20
VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:
```

## 5.8. Administer Agent Login ID

To add an **Agent LoginID**, use the command “**add agent-loginID <agent ID>**” for each agent. In the compliance test, three agent login IDs 1000, 1001, and 1002 were created.

add agent-loginID 1000		Page 1 of 2
AGENT LOGINID		
Login ID: 1000	AAS? n	
Name: Agent 1000	AUDIX? n	
TN: 1		
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code: 1234	LWC Log External Calls? n	
Attribute:	AUDIX Name for Messaging:	
LoginID for ISDN/SIP Display? n		
Password:		
Password (enter again):		
Auto Answer: station		
MIA Across Skills: system		
AUX Agent Considered Idle (MIA)? system	ACW Agent Considered Idle: system	
Aux Work Reason Code Type: system		
Logout Reason Code Type: system		
Maximum time agent in ACW before logout (sec): system		
Forced Agent Logout Time: :		
WARNING: Agent must log in again before changes take effect		

On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

add agent-loginID 1000		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:	Service Objective? n	
Call Handling Preference: skill-level	Local Call Preference? n	
SN	RL	SL
1: 1		1
2:		16:
3:		17:
4:		18:
5:		19:
6:		20:
7:		
8:		
9:		
10:		
11:		
12:		
13:		
14:		
15:		

## 6. Configure Avaya Aura® Application Enablement Services


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

- Launch AE web interface
- Verify license
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user
- Administer Security Database
- Administer ports
- Restart services

### 6.1. Launch AE web Interface


Access the AE web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. Another thick red horizontal bar is located at the bottom of the page, just above the footer. The footer text, "Copyright © 2009-2019 Avaya Inc. All Rights Reserved.", is centered at the very bottom.

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

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Thu Feb 27 15:14:53 2020 from 10.33.1.200  
Number of prior failed login attempts: 0  
HostName/IP: aes8/10.33.1.4  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.1.0.2.8-0  
Server Date and Time: Sat Apr 18 23:37:45 IST 2020  
HA Status: Not Configured

HomeHome | Help | Logout

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

### Welcome to OAM

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

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

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

## 6.2. Verify License

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

LicensingHome | Help | Logout

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

### Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

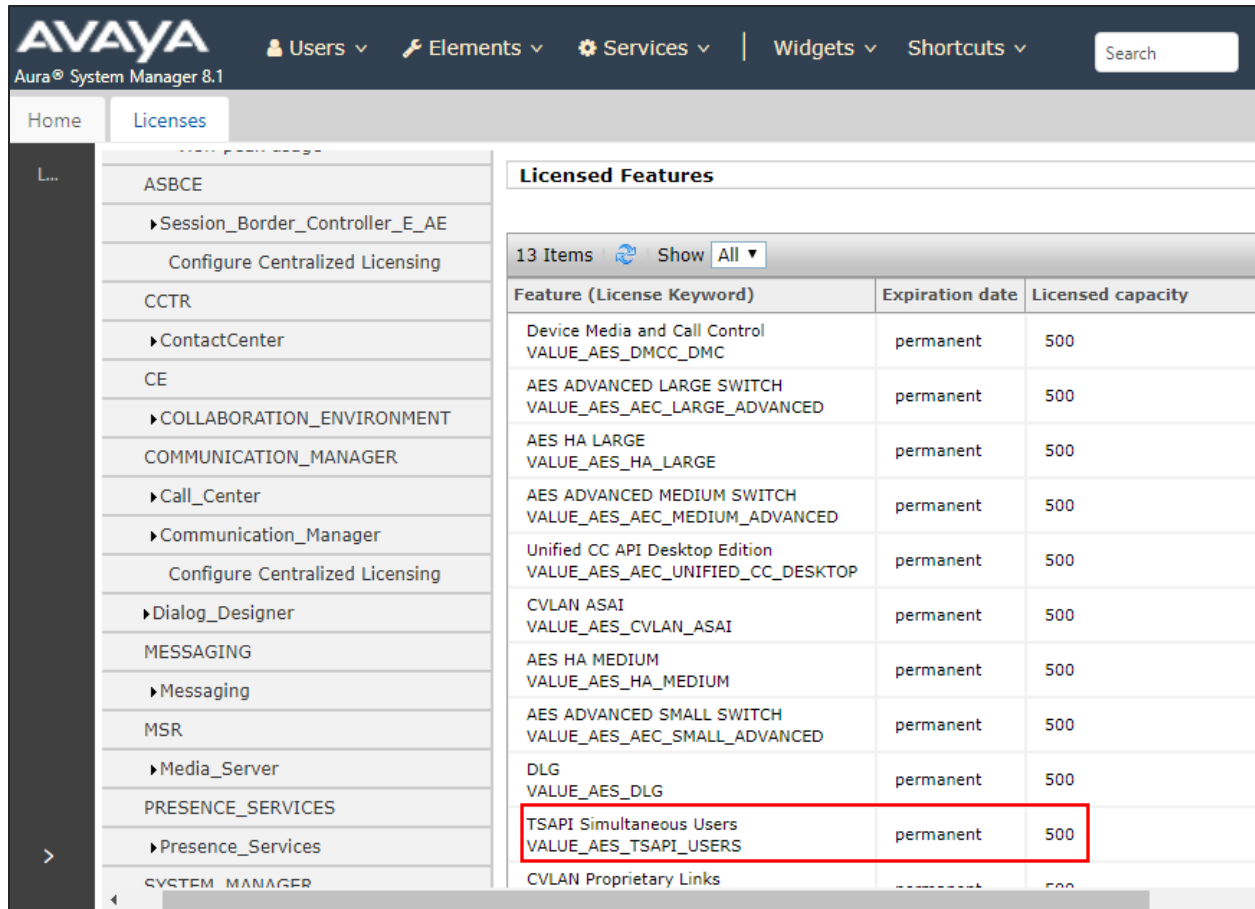
If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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

Select **Licensed products** → **APPL\_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.



The screenshot displays the Avaya Aura System Manager 8.1 interface. The left pane shows a tree view with 'L...' expanded, listing various components like ASBCE, Session\_Border\_Controller\_E\_AE, CCTR, CE, COMMUNICATION\_MANAGER, and SYSTEM\_MANAGER. The right pane shows the 'Licensed Features' table, which lists 13 items. The 'TSAPI Simultaneous Users' feature is highlighted with a red box, indicating a permanent license with a capacity of 500.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	500
AES HA LARGE VALUE_AES_HA_LARGE	permanent	500
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	500
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	500
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	500
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	500
DLG VALUE_AES_DLG	permanent	500
<b>TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS</b>	permanent	500
CVLAN Proprietary Links	permanent	500



### 6.3. Administer Switch Connection

Select **Communication Manager Interface** → **Switch Connection** from the left pane of the **Management Console**, enter a name in **Switch Connection** box and click **Add** button (not shown). Enter the password as configured in **Section 5.4** in the **Switch Password** and **Confirm Switch Password** and check on **Processor Ethernet** field if the Processor Ethernet is used in Communication Manager. Click **Apply** button to save the configuration.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

**Connection Details - interopcm**

Switch Password: [password field]  
Confirm Switch Password: [password field]  
Msg Period: 30 Minutes (1 - 72)  
Provide AE Services certificate to switch: ☒  
Secure H323 Connection: ☐  
Processor Ethernet: ☒  
[Apply] [Cancel]

Select the **interopCM** switch connection has been added above and selects **Edit PE/CLAN IPs** to add IP address of switch connection.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

**Switch Connections**

[text field] [Add Connection]

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> interopcm	Yes	30	1

[Edit Connection] [Edit PE/CLAN IPs] [Edit H.323 Gatekeeper] [Delete Connection] [Survivability Hierarchy]

Enter IP address of Processor Ethernet of Communication Manager in the box and click **Add/Edit Name of IP** button to add the IP.

The screenshot shows the 'Communication Manager Interface' with a red header bar containing 'Switch Connections' and links for 'Home | Help | Logout'. A left-hand navigation menu lists various services, with 'Communication Manager Interface' expanded to show 'Switch Connections'. The main content area is titled 'Edit Processor Ethernet IP - interopcm'. It features a text input field containing '10.33.1.6' and an 'Add/Edit Name or IP' button. Below this is a table with two columns: 'Name or IP Address' and 'Status'. The table contains one entry: '10.33.1.6' with a status of 'In Use'. A 'Back' button is located at the bottom left of the main content area.

Name or IP Address	Status
10.33.1.6	In Use

Select **Edit H.323 Gatekeeper** button to add an IP address of gate keeper, the Gatekeeper IP address in this case is also the Processor Ethernet.

The screenshot shows the 'Communication Manager Interface' with a red header bar containing 'Switch Connections' and links for 'Home | Help | Logout'. A left-hand navigation menu lists various services, with 'Communication Manager Interface' expanded to show 'Switch Connections'. The main content area is titled 'Edit H.323 Gatekeeper - interopcm'. It features a text input field and an 'Add Name or IP' button. Below this is a section labeled 'Name or IP Address' with a radio button selected next to '10.33.1.6'. At the bottom, there are 'Delete IP' and 'Back' buttons.

## 6.4. 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 'TSAPI Links' management console. The left sidebar contains a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TWS', 'Communication Manager Interface', 'High Availability', and 'Licensing'. Under 'TSAPI', 'TSAPI Links' is selected. The main content area has a red header bar with 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. Below this is a table with columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is displayed in the right side. 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 “**interopcm**” which is added in the step above. For **Switch CTI Link Number**, select the CTI link number 1 from **Section 5.2**, select **Both** in the **Security** dropdown menu to support both unencrypted and encrypted TSAPI link. Retain the default values in the remaining fields.

The screenshot shows the 'Add TSAPI Links' screen. The left sidebar is the same as the previous screenshot. The main content area has a red header bar with 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. Below this is a form titled 'Add TSAPI Links'. The form contains the following fields: 'Link' (text input with value '1'), 'Switch Connection' (dropdown menu with value 'interopcm'), 'Switch CTI Link Number' (text input with value '1'), 'ASAI Link Version' (text input with value '8'), and 'Security' (dropdown menu with value 'Both'). Below the form are two buttons: 'Apply Changes' and 'Cancel Changes'. In the top right corner, there is a welcome message: 'Welcome: User cust', 'Last login: Sat Apr 18 03:32:50 2020 from 10.33.1.200', 'Number of prior failed login attempts: 0', 'HostName/IP: aes8/10.33.1.4', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 8.1.1.0.2.8-0', 'Server Date and Time: Sun Apr 19 03:44:20 IST 2020', and 'HA Status: Not Configured'.

## 6.5. Administer CTI User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

**User Management | User Admin | Add User**

▶ 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

Premise

\* 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

Home Phone

Home Postal Address

## 6.6. Configure 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. Leave it as default as checked on **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services**.

The screenshot shows the 'Security | Security Database | Control' page. The left navigation pane lists various services, with 'Security Database' expanded to show 'Control'. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' (unchecked) and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services' (checked). An 'Apply Changes' button is located below the checkboxes.

Select **Security → Security Database → CTI Users → List All Users** and select the “test” CTI user which is created in **Section 6.5** and select **Edit** button (not shown). In the **Edit CTI User**, select the check box **Unrestricted Access** and click **Apply Changes** to save the configuration.

The screenshot shows the 'Security | Security Database | CTI Users | List All Users' page. The left navigation pane shows 'CTI Users' expanded to 'List All Users'. The main content area is titled 'Edit CTI User'. It displays the following configuration for a user profile:

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

At the bottom of the form are 'Apply Changes' and 'Cancel Changes' buttons.

## 6.7. 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 **TSAPI Service Port 450** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

**Networking | Ports**Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

**Ports**

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

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

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

H.323 Ports

TCP Port Min20000

TCP Port Max29999

Local UDP Port Min20000

Local UDP Port Max29999

Server Media

RTP Local UDP Port Min\*30000

RTP Local UDP Port Max\*49999

SMS Proxy Ports

Proxy Port Min4101

Proxy Port Max4116

Apply Changes

Restore Defaults

\* Note: The number of RTP ports needs to be double the number of extensions using server media.

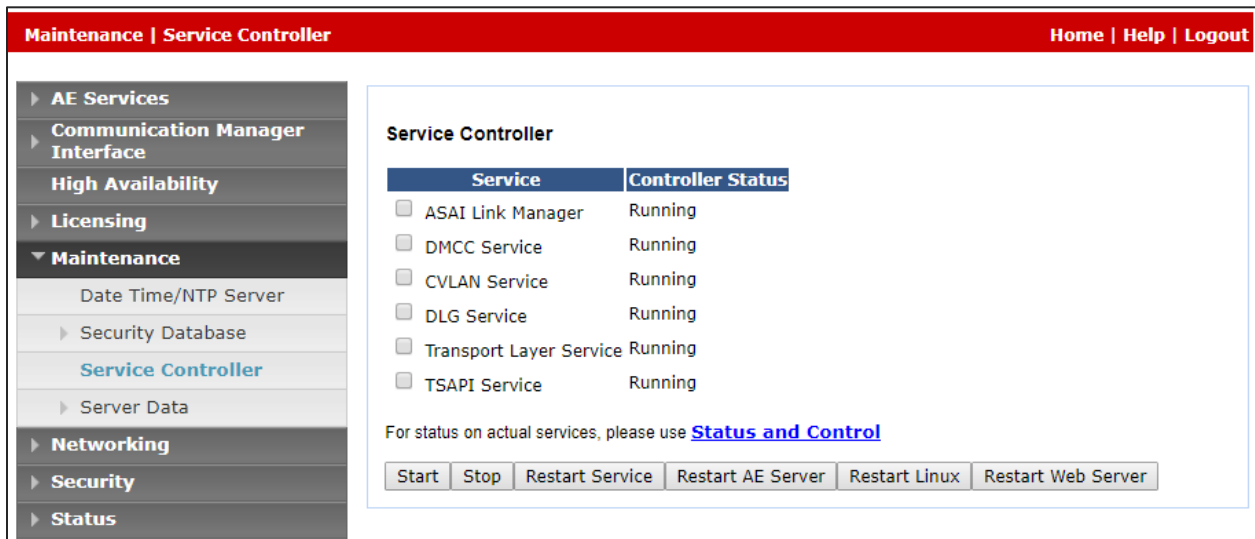
KP; Reviewed:  
SPOC 6/9/2020

Solution & Interoperability Test Lab Application Notes  
©2020 Avaya Inc. All Rights Reserved.

22 of 35  
DaVinci-AES81

## 6.8. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Click **Restart AE Service**.



The screenshot shows a web interface for the Service Controller. The top navigation bar is red with the text "Maintenance | Service Controller" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance" (expanded), "Date Time/NTP Server", "Security Database", "Service Controller" (highlighted in blue), "Server Data", "Networking", "Security", and "Status". The main content area is titled "Service Controller" and contains a table with two columns: "Service" and "Controller Status". The table lists six services, each with a checkbox and a status of "Running". Below the table, there is a link "For status on actual services, please use [Status and Control](#)". At the bottom, there is a row of buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

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 type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

## 7. Configure AMC Technology DaVinci Premise Server

The DaVinci Premise Server (DPS) is configured through server profiles. Server profiles are config.ini files that configure core modules and the channel connector (CTI Module) that connects with and integrates Avaya Application Enablement Services, and the application adapter module which integrates CRM applications.

Three (3) different server profiles were used. Cloud applications (Microsoft Dynamics CRM, Salesforce, SAP C4C, ServiceNow and Zendesk) used the SOAP web services adapter. Siebel used the .NET remoting adapter, which connects using .NET remoting protocol. SAP CRM used the SAP Web adapter, which connects through SAP APIs.

As these differ only in the application adapter configuration, the full Cloud Application SOAP web services profile is listed, and only the adapter configuration differences for SAP CRM and Oracle Siebel are listed. These include difference in the Module Manager, which defines the loadable modules, and the adapter module configuration sections.

### Cloud Application (SOAP) Server Profile [base]

[Global]

Cloud CRM Application & DaVinci Premise Gateway Server Profile

TraceEnabled=1

TraceLevel=4

TraceMaxSize=1024

TracePath=C:\Program Files (x86)\AMC Technology\MCIS\Server\Logs

[ModuleManager]

# TraceEnabled=1

# TraceLevel=4

# TraceMaxSize=1024

ModuleCheckInterval=3000000

CreateDumpOnUnhandledException=True

ModuleTerminateOnStart=CMGateway.exe

ModuleTerminateOnShutdown=CMGateway.exe

ModuleClass=AgentManagerClass,AgentManager.AMCAgentManagerModule

Module=AgentManager,AgentManagerClass

ModuleClass=DataStoreClass,DataStore.AMCMemoryDataStore

Module=DataStore,DataStoreClass

ModuleClass=EventManagerClass,AMCEventManagerModule.AMCEventManagerModule

Module=EventManager,EventManagerClass

ModuleClass=LicenseManagerClass,LicenseManager.AMCLicenseManagerModule

Module=LicenseManager,LicenseManagerClass

ModuleClass=WorkManagerClass,WorkManager.AMCWorkManager

Module=WorkManager,WorkManagerClass



ModuleClass=StandardizedClass,AMCMultiChannelInterface.AMCApplication  
Module=StandardizedInterface,StandardizedClass

ModuleClass=CMGatewayClass,CMGateway.CMGatewayModule  
Module=CMGateway,CMGatewayClass

ModuleClass=SoapAdapter4DotNet\_ProgID,SoapAdapter4DotNet.SoopAdapterModule  
Module=SoapAdapter,SoapAdapter4DotNet\_ProgID

ModuleClass=CentreVuCTI,CentreVuCTI.CentreVuCTIModule  
Module=CTIModule,CentreVuCTI

[AgentManager]  
# TraceEnabled=1  
# TraceLevel=4  
# TraceMaxSize=1024  
TraceMaxSize=50240  
SuppressPendingWorkModeChange=False  
RaiseNewWorkForUnknownWorktops=False  
RaiseWMChangedSynchronous=False  
RaiseNewWorkSynchronous=False  
SynchronizeChannelWorkModes=True

[DataStore]  
# TraceEnabled=1  
# TraceLevel=2  
# TraceMaxSize=1024  
# CleanupInterval=1440  
# DataExpiration=30  
CleanupInterval=240  
DataExpiration=240

[EventManager]  
# TraceEnabled=1  
# TraceLevel=2  
# TraceMaxSize=1024  
# IoPortReadTimeout=3000  
# UseSafeMode=Yes  
ThreadPoolSize=20

[StandardizedInterface]  
# TraceEnabled=1  
# TraceLevel=2  
# TraceMaxSize=1024  
# AgentManager=AgentManager  
ReturnErrorCodes=True

[CMGateway]  
# TraceEnabled=1  
# TraceLevel=2  
# TraceMaxSize=1024  
InstanceName=Default

[LicenseManager]  
# TraceEnabled=1

# TraceLevel=2  
# TraceMaxSize=1024

MCIS=[license key removed]

[WorkManager]  
# TraceEnabled=1  
# TraceLevel=2  
# TraceMaxSize=1024

[SoapAdapter]  
# TraceEnabled=1  
# TraceLevel=4  
# TraceMaxSize=1024  
# MessageLibrary=AMC\_MESSAGES.dll  
TraceMaxSize=50240  
EventManager=EventManager  
# DataStore=DataStoreClient # for distributed data store  
DataStore=DataStore  
AppURL=http://localhost/event-jaxrpc/eventraiser  
EventRaiser=AMCDotNetEventAdapterRaiser.MSMQEventRaiser

[CTIModule]  
# TraceEnabled=1  
TraceLevel=4  
TraceMaxSize=50240  
DataStore=DataStore  
Channel=CTI1  
InternalExtLen=4  
ServerID=AVAYA#INTEROPCM#CSTA#AES8  
ExtensionFile=<For Extra Monitoring Ex. VDNs/Path Ex. Program Files\AMC  
Technology\MCIS\Connectors\Telephony\ACT\Extensions.txt>  
UserName=davinci  
Password=Interop123!  
AllowDTMF=Yes  
DTMFPause=5  
UseAutoIn=1  
WorkmodePollInterval=500  
BlockAgentStateEventDuringActiveCall=NO  
FilterOriginatedEvent=NO  
SynchronizeAgentStateInRegister=Yes

[AdministrationTool]  
AdminToolHost=localhost  
WebServiceHost=localhost  
MCISName=localhost  
#AdminRemotingPort=65372  
#SMTPServer=<smtpserver>  
TraceLevel=5  
TraceMaxSize=1000000  
TracePath=C:\Program Files (x86)\AMC Technology\MCIS\Server\Logs\  
TraceFileName=AdministrationTool.log

### **Siebel CRM Server Profile** [differences for adapter configuration only]

[ModuleManager]

# TraceEnabled=1

# TraceLevel=4

# TraceMaxSize=1024

ModuleCheckInterval=3000000

CreateDumpOnUnhandledException=True

ModuleTerminateOnStart=CMGateway.exe

ModuleTerminateOnShutdown=CMGateway.exe

ModuleClass=AgentManagerClass,AgentManager.AMCAgentManagerModule

Module=AgentManager,AgentManagerClass

ModuleClass=DataStoreClass,DataStore.AMCMemoryDataStore

Module=DataStore,DataStoreClass

ModuleClass=EventManagerClass,AMCEventManagerModule.AMCEventManagerModule

Module=EventManager,EventManagerClass

ModuleClass=LicenseManagerClass,LicenseManager.AMCLicenseManagerModule

Module=LicenseManager,LicenseManagerClass

ModuleClass=WorkManagerClass,WorkManager.AMCWorkManager

Module=WorkManager,WorkManagerClass

ModuleClass=StandardizedClass,AMCMultiChannelInterface.AMCApplication

Module=StandardizedInterface,StandardizedClass

ModuleClass=CMGatewayClass,CMGateway.CMGatewayModule

Module=CMGateway,CMGatewayClass

ModuleClass=RemotingEndpointClass,AMCDotNetAdapterRemotingLibrary.RemotingModule

Module=RemotingEndpoint,RemotingEndpointClass

ModuleClass=CentreVuCTI,CentreVuCTI.CentreVuCTIModule

Module=CTIModule,CentreVuCTI

[RemotingEndpoint]

TraceLevel=4

TraceMaxSize=50240

RemotingPort=5623

# EventBroadcastPort=4555

# DataStore=DataStore

DataStore=CTIModule

### **SAP CRM Server Profile** [differences for adapter configuration only]

[ModuleManager]

# TraceEnabled=1

# TraceLevel=4

```

# TraceMaxSize=1024
ModuleCheckInterval=3000000
CreateDumpOnUnhandledException=True

ModuleTerminateOnStart=CMGateway.exe
ModuleTerminateOnShutdown=CMGateway.exe

ModuleClass=AgentManagerClass,AgentManager.AMCAgentManagerModule
Module=AgentManager,AgentManagerClass

ModuleClass=DataStoreClass,DataStore.AMCMemoryDataStore
Module=DataStore,DataStoreClass

ModuleClass=EventManagerClass,AMCEventManagerModule.AMCEventManagerModule
Module=EventManager,EventManagerClass

ModuleClass=LicenseManagerClass,LicenseManager.AMCLicenseManagerModule
Module=LicenseManager,LicenseManagerClass

ModuleClass=WorkManagerClass,WorkManager.AMCWorkManager
Module=WorkManager,WorkManagerClass

ModuleClass=StandardizedClass,AMCMultiChannelInterface.AMCApplication
Module=StandardizedInterface,StandardizedClass

ModuleClass=CMGatewayClass,CMGateway.CMGatewayModule
Module=CMGateway,CMGatewayClass

ModuleClass=ICIAdapterClass,ICIAdapter.ICIAdapterModule
Module=IciAdapter,IciAdapterClass

ModuleClass=CentreVuCTI,CentreVuCTI.CentreVuCTIModule
Module=CTIModule,CentreVuCTI

[IciAdapter]
TraceLevel=6
TraceMaxSize=50240
CTIChannel=CTI1
ConfigDBHost=PETDaVinci7\SQLExpress
ConfigServerName=petdavinci7
# ConfigDBUser=<If using Named Authorization, SQL user with proper Authorization>fd
# ConfigDBPass=<Password for above SQL User>
EventHandlingLevel=5
NewHandleOnWarmTransfer=False
NewHandleOnConference=False
WaitForCallStateUpdateDelay=1500
DropCreatedItemAfterFailedDial=True
DropCreatedItemAfterFailedConsult=True
CheckCallStateAfterDial=True
CheckCallStateAfterConosult=True
WaitCallStateAfterDial=200
LetDropEventCleanItem=True
FilterDropForTransferredCall=False

```

```

# RejectQueue=<Rejection Queue number>
DataStore=CTIModule
ContactDataKeyName=CAD
ListenForImmediateChannelArrivalEvent=True
ListenForNewWorkEvent=False
UpdateTransferHandleTelephony=True
AllowWorkCenterList=False
PostImmediateChannelArrivalDelay=1 000
WrapupMode=1
#      WorkCenterMode=3
#      WorkCenterMode=2,100
NotReadyReasonACWLAN=ZH|EN|DE|FR
NotReadyReasonCode=3,Break ZH|Break|Pause|Pause FR
NotReadyReasonCode=4,LunchZH|Meeting|Mittag| Mittag FR
ACWText=After Call ZH|After Call|After Call DE|After Call FR
InboundDispositionCode=3012,WIB-Task Completed ZH|WIB-Task Completed|WrapupIB-Task
Completed DE|WIB-Task Completed FR
InboundDispositionCode=3013,WIB-Hang Up/Transfer ZH|WIB-Hang Up/Transfer|WIB-Hang
Up/Transfer DE|WIB-Hang Up/Transfer FR
OutboundDispositionCode=3015,WOB-Contacted ZH|WOB-Contacted|WOB-Contacted DE|WOB-
Contacted FR
OutboundDispositionCode=3016,WOB-Left Message ZH|WOB-Left Message|WOB-Left Message
DE|WOB-Left Message FR
NotReadyReasonCode=9999,-- Select -- ZH|-- Select --|-- Select -- DE|-- Select -- FR
ShowSelectForFailedWorkMode=True
EnablePreviewWrapup=False
EnableCallDisposition=False
EnablePreviewWrapupNumericCode=False
EnableCallDispositionNumericCode=False
PreviewANIFromCADField=PhoneNumber
CallTypeForPreviewPopup=Inbound
EnablePhantomInboundPopup=False
# NumberTranslationFile=D:\Program Files\AMC Technology\Application Adapters\SAP Web
Client Adapter\Default.tfs
# NumberTranslationANIRule=Strip000|Replace00w86|ADD_PLUS
#
NumberTranslationDialingRule=StripPLUS|Add000IfGreaterThanSeven|Replace00086With00|Repl
ace00000w00
# DialerConnectedStatusText=PDS CALL
# ContactDataOnReadScript=
# ANITranslationScript=

```

## 8. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

### 8.1. Verify AES Connection

Verify the status of the **TSAPI Service Summary** service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** is displayed in the right pane. The status should be in “**Talking**” in the **Status** column.

The screenshot shows the 'TSAPI Link Details' page. The left navigation pane has 'Status' expanded, showing 'Status and Control' as the selected option. The main content area displays a table of TSAPI link details. The status of the link is 'Talking'.

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	interopcm	1	Talking	Fri Feb 14 17:25:44 2020	Online	18	2	197	202	30

Below the table, there are buttons for 'Online' and 'Offline'. A note states: 'For service-wide information, choose one of the following: TSAPI Service Status | TLink Status | User Status'.

Select the **User Status** button in the **TSAPI Link Details** page above to show the status of CTI user used for TSAPI service. The **CTI User Status** displays the *davinci* CTI user name with the time of the connection established.

The screenshot shows the 'CTI User Status' page. The left navigation pane has 'Status' expanded, showing 'Status and Control' as the selected option. The main content area displays a table of CTI user status. The status of the user is 'Talking'.

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Fri 14 Feb 2020 05:26:27 PM IST		AVAYA#INTEROPCM#CSTA#AES8
DMCCLCSUserDoNotModify	Fri 14 Feb 2020 05:26:27 PM IST		AVAYA#INTEROPCM#CSTA#AES8
DMCCLCSUserDoNotModify	Fri 14 Feb 2020 05:26:31 PM IST		AVAYA#INTEROPCM#CSTA-S#AES8
davinci	Sun 19 Apr 2020 04:35:43 PM IST		AVAYA#INTEROPCM#CSTA#AES8

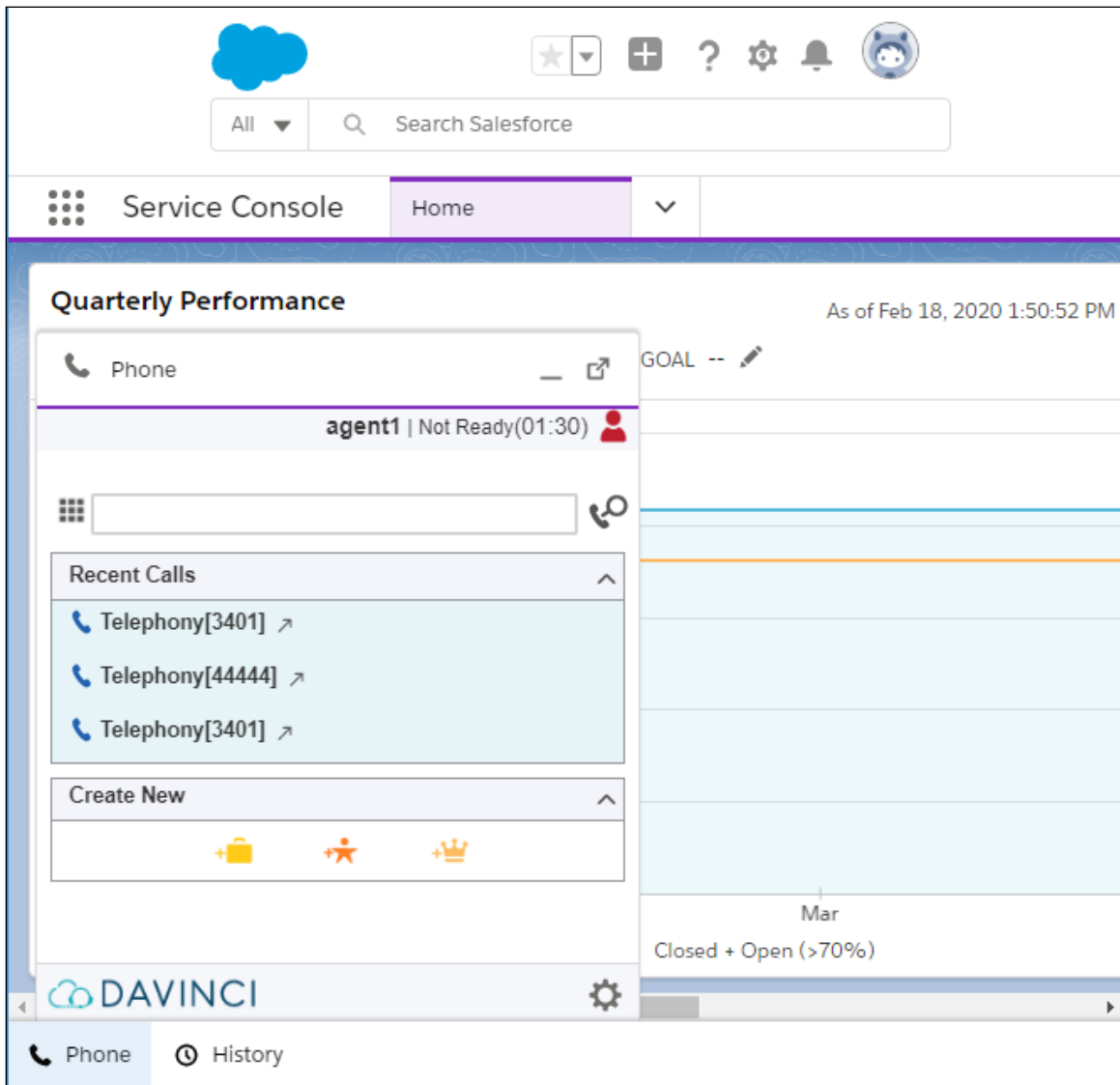
Below the table, there are buttons for 'Show Closed Streams', 'Close All Opened Streams', and 'Back'.

## 8.2. Verify CTI CRM

This section shows typical CRM applications that were used during the compliance test.

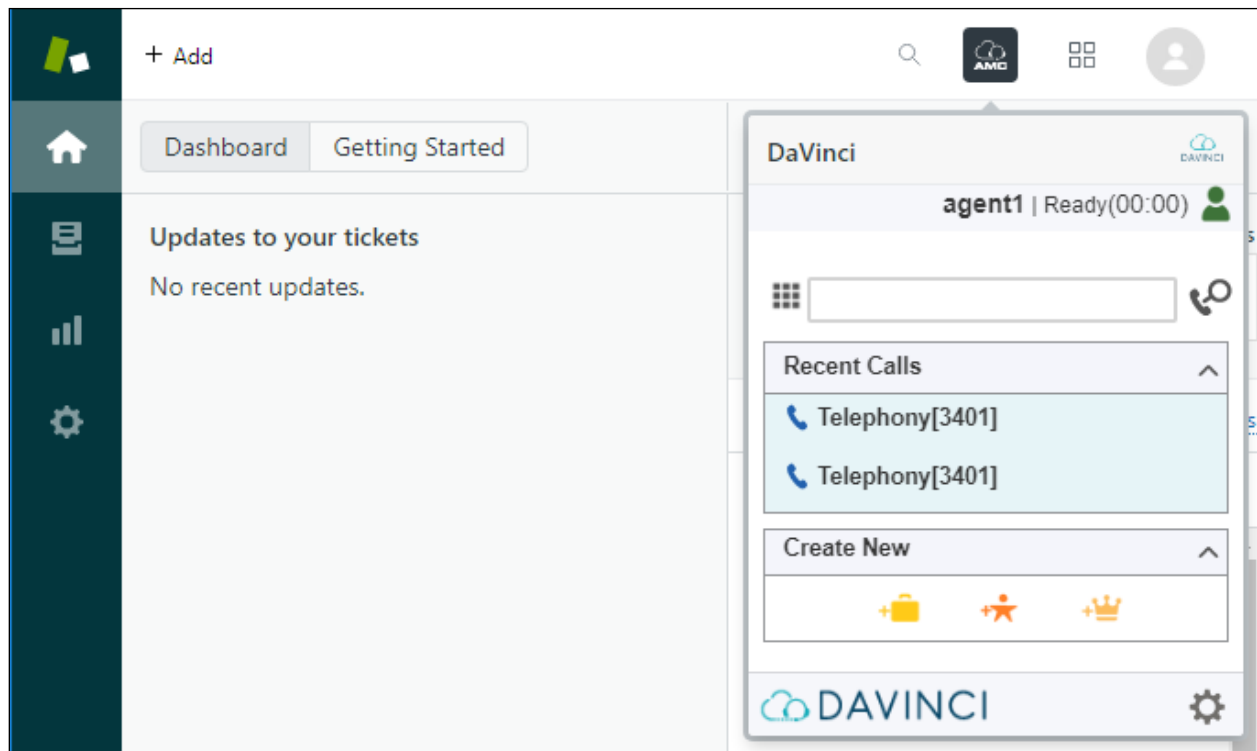
### 8.2.1. Salesforce CRM

The screen below shows the DaVinci Agent UI logs in to Salesforce CRM and placed in **Not Ready** mode.



### 8.2.2. Zen Desk CRM

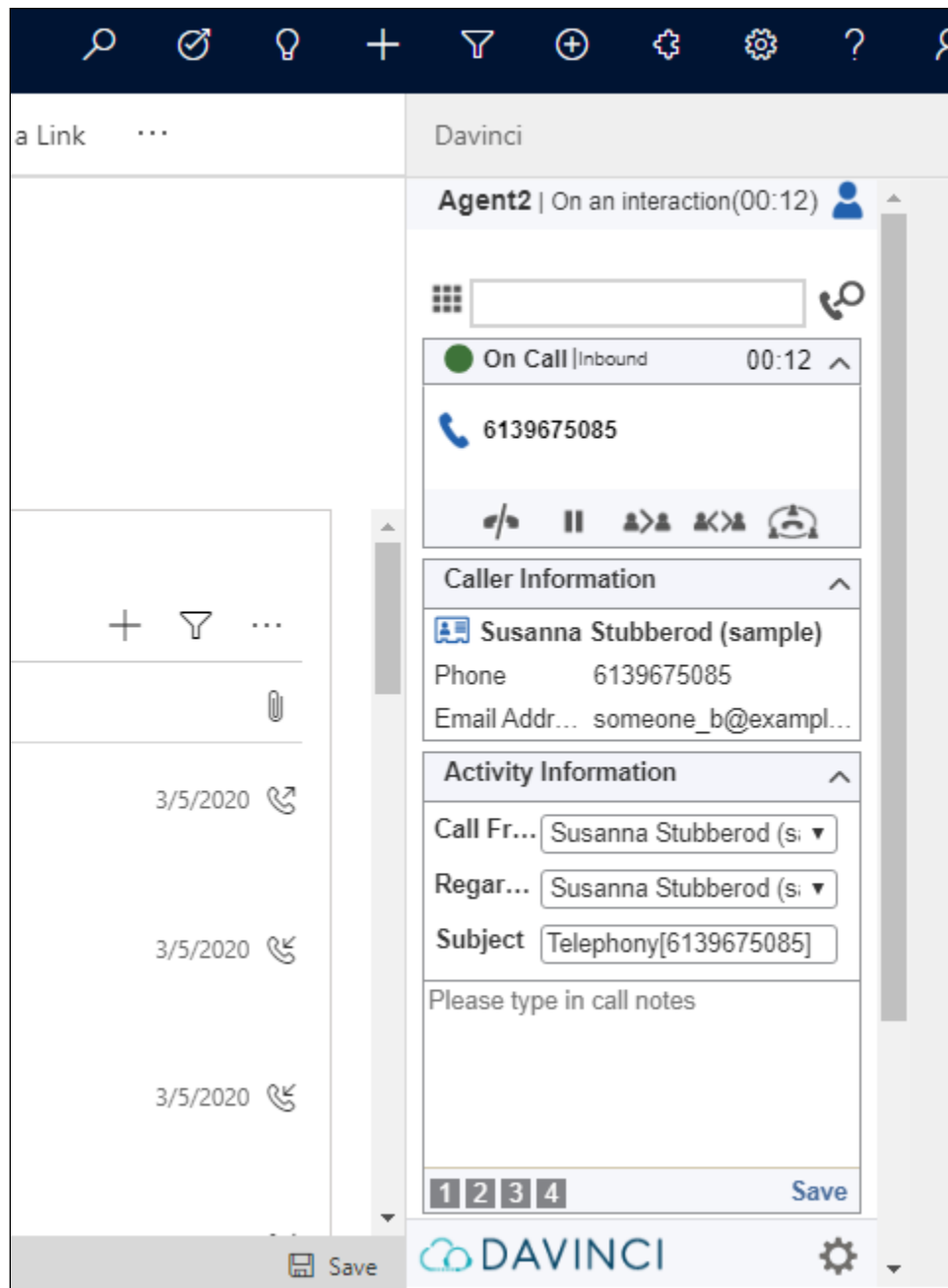
The screen below shows the DaVinci Agent UI is integrated with Zendesk CRM and placed in the **Ready** mode.





### 8.2.3. Microsoft Dynamics 365 CRM

The screen below shows the DaVinci Agent UI is integrated with MS Dynamics 365 and answers an inbound call.



## 9. Conclusion

These Application Notes describe the configuration steps required for AMC Technology DaVinci Premise Server Version 7.0 to successfully interoperate with Avaya Aura® Application Enablement Services release 8.1. All feature and serviceability test cases were completed with observations noted in **Section** Error! Reference source not found..

## 10. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Deploying Avaya Aura® applications from System Manager*, Release 8.1, October 2019
- [2] *Deploying Avaya Aura® Communication Manager*, Release 8.1, October 2019
- [3] *Administering Avaya Aura® Communication Manager*, Release 8.1, October 2019
- [4] *Deploying Avaya Aura® Session Manager*, Release 8.1 October 2019
- [5] *Upgrading Avaya Aura® Session Manager* Release 8.1, October 2019
- [6] *Administering Avaya Aura® Session Manager* Release 8.1, October 2019
- [7] *Deploying Avaya Session Border Controller for Enterprise Release 8.1*, February 2020
- [8] *Upgrading Avaya Session Border Controller for Enterprise Release 8.1*, February 2020
- [9] *Administering Avaya Session Border Controller for Enterprise Release 8.1*, February 2020

---

**©2020 Avaya Inc. All Rights Reserved.**

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

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