



Avaya Solution & Interoperability Test Lab

Application Notes for Intradiem 9.5 and Avaya Aura® Application Enablement Services 8.1 and Avaya Aura® Communication Manager 8.1 – Issue 1.0

Abstract

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

In the compliance testing, Intradiem application used Device Media and Call Control (DMCC) from Avaya Aura® Application Enablement Services to get events and monitor contact center hunt groups and its agents on Avaya Aura® Communication Manager.

Readers should pay attention to **Section 2.2**, in particular the scope of testing as outlined in **Section 2.2** 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 Intradiem application with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3.

In the compliance testing, Intradiem is a windows application that used Device Media Call Control interface (DMCC) from Avaya Aura® Application Enablement Services to monitor skill/split numbers and VDNs for call and station events on Avaya Aura® Communication Manager and then uses this information to get agent state and update agent state for certain agents based on business rules.

2. General Test Approach and Test Results

The feature test cases were performed manually. Manually perform agent login and logout, agent state changed from the agent's telephones which are included H.323 and SIP IP telephones, verification that events of status changes on agent's telephones are also captured on Intradiem's application.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Intradiem server and restart Application Enablement Services server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Intradiem did not include use of any specific encryption features.

Encryption (TLS/SRTP) was used internally between Avaya products.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Intradiem:

- Monitor and receive agent events such as login, logout, agent state change...etc.
- Creating rules in Intradiem server for agent events to have proper actions such as sending email when agent is logged in/out, changing the agent state from Not Ready to Ready or vice versus.

The serviceability testing focused on verifying the ability of Intradiem Server to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection from Intradiem server and restarting AES server.

2.2. Test Results

All test cases were executed and passed successfully.

2.3. Support

For technical support on the Intradiem, contact Intradiem via phone, email, or internet.

- **Phone:** +1 (888) 566-9457
- **Web:** <http://www.intradiem.com>

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Media Server running on Virtualized Environment, Avaya G450 Media Gateway registers to Communication Manager. The Intradiem server running on Windows 2016 server and connected to Avaya Aura® Application Enablement Service via DMCC port 4721.

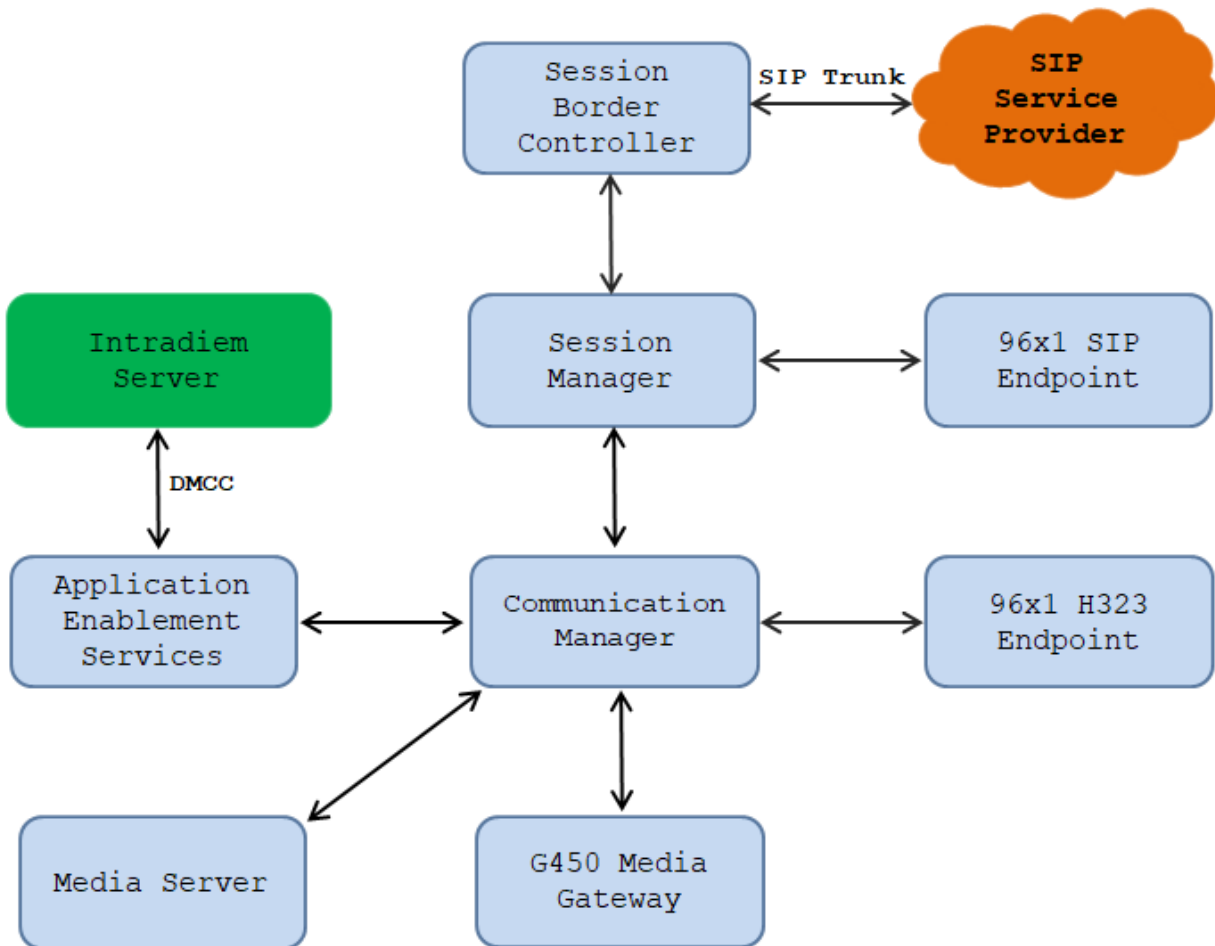


Figure 1: Test Configuration Diagram

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 in a Virtual Environment	8.1.3
Avaya G450 Media Gateway	41.20.0
Avaya Aura® Media Server running in a Virtual Environment	8.0
Avaya Aura® Application Enablement Services in a Virtual Environment	8.1.3
Avaya Aura® System Manager running in a Virtual Environment	8.1.3
Avaya Aura® Session Manager running in a Virtual Environment	8.1.3
Avaya 9611G IP Deskphone (SIP)	Release 7.1.9.0.8
Avaya 9641G IP Deskphone (H.323)	Release 6.8304
Intradiem running on Windows 2016 Server	9.5

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
- Administer IP Node Names
- Administer AE Services
- Administer Hunt Group
- Administer VDN
- Administer Agent Login ID

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has the appropriate permissions for the 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 an appropriate license file.

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

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

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: 3332
      Type: ADJ-IP
                                COR: 1
      Name: AES70
```

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: 01
  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 Intradiem 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 IP Node Names

Use the **change node-names ip** command to administer a Name and IP Address for AES. In the configuration used for compliance testing, the **procr** and **aes70** nodes were utilized to administer a SIP trunk between Communication Manager and Session Manager.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
AMS1	10.33.1.30	
CMS18	10.33.1.20	
aes70	10.33.1.4	
default	0.0.0.0	
interopASM	10.33.1.12	
lsp	10.33.1.17	
procr	10.33.1.6	
procr6	::	

5.5. 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	
AESVCS	y	procr	8765			

Go to **Page 4**, enter the following values. **AE Services Server** should be the AES IP node name that is configured in **Section 5.4** above, 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:	aes70	*	y	in use	

5.6. Administer Hunt Group

This section provides the Hunt Group configuration for the call center agents. This hunt group will later be configured in Avaya POM.

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:
```

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
Measured: Both
Supervisor Extension:

      Controlling Adjunct: none

      Multiple Call Handling: none

Timed ACW Interval (sec):      After Xfer or Held Call Drops? n
```

5.7. Administer VDN

Use the “**add vdn <ext>**” command to add a VDN number. In the **Destination** field, enter **Vector Number** and enter a vector number as shown in the screen below.

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

                               Extension: 3340
                               Name*: Contact Center 1
                               Destination: Vector Number      1
Attendatant 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                SN    RL SL
1: 1      1                    16:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
```

6. Configure Avaya Aura® Application Enablement Services

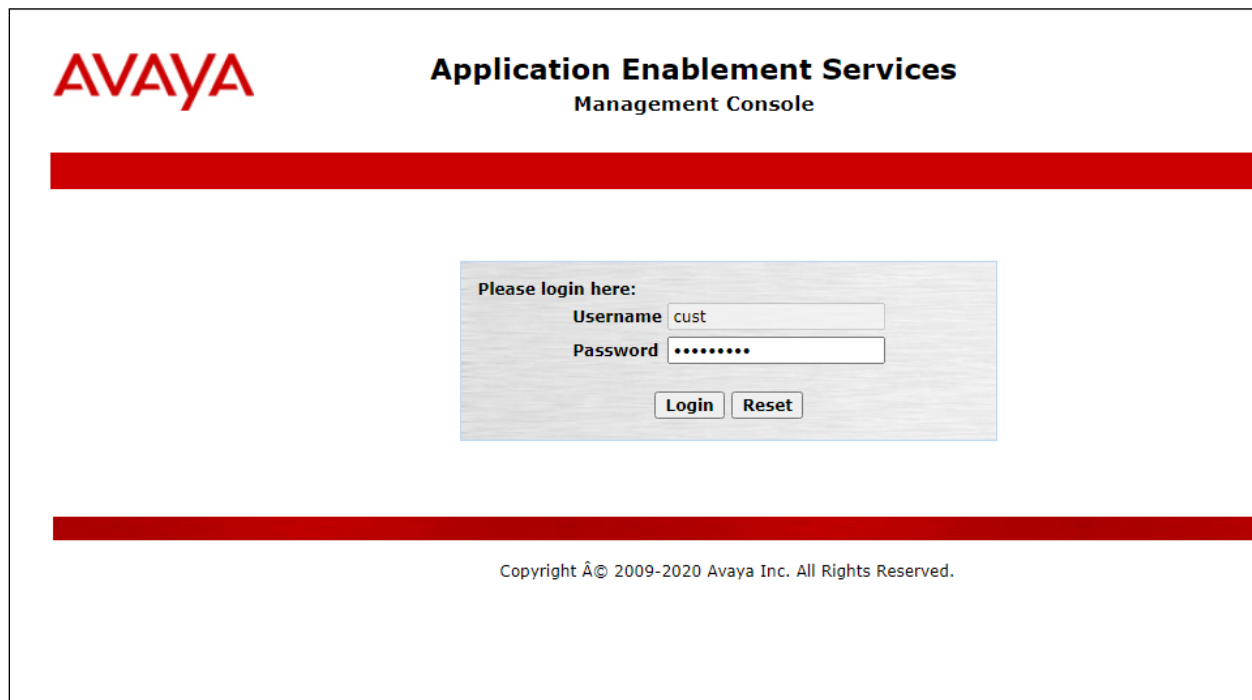
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify License
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user
- Administer Security Database
- Administer Ports
- Restart Services

6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". Below this is a red horizontal bar. In the center, there is a login form with the heading "Please login here:". The form contains two input fields: "Username" with the value "cust" and "Password" with masked characters "*****". Below the password field are two buttons: "Login" and "Reset". At the bottom of the page, there is another red horizontal bar and a copyright notice: "Copyright © 2009-2020 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title "Application Enablement Services Management Console". The top right displays system information: "Welcome: User cust", "Last login: Mon Nov 2 14:30:29 2020 from 10.33.1.200", "Number of prior failed login attempts: 2", "HostName/IP: aes8/10.33.1.4", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.3.0.0.25-0", "Server Date and Time: Thu Nov 19 14:45:59 IST 2020", and "HA Status: Not Configured". A red navigation bar at the top contains "Home" on the left and "Home | Help | Logout" on the right. A left sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their functions. At the bottom of the main content area, it 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 configuration page for "WebLM Server Address". The top navigation bar is red and contains "Licensing | WebLM Server Address" on the left and "Home | Help | Logout" on the right. The left sidebar is the same as in the previous screenshot, with "Licensing" expanded and "WebLM Server Address" selected. The main content area is titled "WebLM Server Address" and contains the following configuration fields: "WebLM IP Address/FQDN" (text input with value "10.33.1.10"), "SSL" (checkbox checked), "WebLM Port" (text input with value "52233"), "Secondary WebLM IP Address/FQDN" (text input), "Secondary SSL" (checkbox checked), and "Secondary WebLM Port" (text input). Below these fields is a section titled "TLS Certificate Hostname Validation" with a "Note: Please refer help page for more details" and a checkbox "Enable Certificate Hostname Validation" which is checked. At the bottom of the configuration area are two buttons: "Apply Changes" and "Restore Defaults".

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 **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a tree view under 'Licenses' with 'APPL_ENAB' selected. The right pane shows the 'Licensed Features' table with 13 items. The table columns are 'Feature (License Keyword)', 'Expiration date', and 'Licensed capacity'. The features listed include 'Device Media and Call Control', 'AES ADVANCED LARGE SWITCH', 'AES HA LARGE', 'AES ADVANCED MEDIUM SWITCH', 'Unified CC API Desktop Edition', 'CVLAN ASAI', 'AES HA MEDIUM', 'AES ADVANCED SMALL SWITCH', 'DLG', 'TSAPI Simultaneous Users', and 'CVLAN Proprietary Links'. All features have an expiration date of 'permanent' and a licensed 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
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	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 5.5** 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.

Welcome: User cust
Last login: Thu Nov 19 14:45:54 2020 from 10.33.100.9
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Thu Nov 19 15:06:59 IST 2020
HA Status: Not Configured

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:
Enable TLS Certificate Hostname Validation:
Apply Cancel

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

Welcome: User cust
Last login: Thu Nov 19 14:45:54 2020 from 10.33.100.9
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Thu Nov 19 15:08:53 IST 2020
HA Status: Not Configured

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.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance
 Networking

Edit Processor Ethernet IP - interopcm

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.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance

Edit H.323 Gatekeeper - interopcm

Name or IP Address

10.33.1.6

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**.

AE Services | TSAPI | TSAPI Links Home | Help | Logout

AE Services
 CVLAN
 DLG
 DMCC
 SMS
 TSAPI
 TSAPI Links
 TSAPI Properties
 TWS

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	interopcm	1	8	Both

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 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.

Welcome: User cust
 Last login: Thu Nov 19 14:45:54 2020 from 10.33.100.9
 Number of prior failed login attempts: 0
 HostName/IP: aes8/10.33.1.4
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 8.1.3.0.0.25-0
 Server Date and Time: Thu Nov 19 15:14:37 IST 2020
 HA Status: Not Configured

AE Services | TSAPI | TSAPI Links Home | Help | Logout

AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ **TSAPI**
 - **TSAPI Links**
 - TSAPI Properties
- ▶ TWS
- ▶ **Communication Manager Interface**

Edit TSAPI Links

Link: 1
 Switch Connection: interopcm
 Switch CTI Link Number: 1
 ASAI Link Version: 8
 Security: Both

Apply Changes | Cancel Changes | Advanced Settings

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 | List All Users Home | 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

Edit User

* User Id: intradiem
 * Common Name: Intradiem
 * Surname: Intradiem
 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:

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. Uncheck both fields below.

The screenshot shows a web interface with a red header bar containing the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". On the left is a navigation tree with "Security Database" expanded to "Control". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", along with an "Apply Changes" button.

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 a web interface with a red header bar containing the breadcrumb "Security | Security Database | CTI Users | List All Users" and links for "Home | Help | Logout". On the left is a navigation tree with "Security Database" expanded to "CTI Users" and "List All Users" selected. The main content area is titled "Edit CTI User" and displays configuration for a user named "intradiem". The "User Profile" section shows "User ID" as "intradiem", "Common Name" as "Intradiem", "Worktop Name" as "NONE", and "Unrestricted Access" checked. The "Call and Device Control" section shows "Call Origination/Termination and Device Status" as "None". The "Call and Device Monitoring" section shows "Device Monitoring" as "None", "Calls On A Device Monitoring" as "None", and "Call Monitoring" unchecked. The "Routing Control" section shows "Allow Routing on Listed Devices" as "None". At the bottom 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 **DMCC Server Ports** section, select the radio button for **Unencrypted Port 4721** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

The screenshot shows the 'Networking | Ports' configuration page. The left sidebar lists various system settings, with 'Networking' expanded to show 'Ports'. The main content area is titled 'Ports' and is divided into three sections: CVLAN Ports, DLG Port, and DMCC Server Ports. Each section contains configuration fields and radio buttons for enabling or disabling services.

Section	Service	Value	Enabled	Disabled
CVLAN Ports	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	9998	<input checked="" type="radio"/>	<input type="radio"/>
DLG Port	TCP Port	5678		
TSAPI Ports	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
DMCC Server Ports	Unencrypted Port	4721	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted Port	4722	<input checked="" type="radio"/>	<input type="radio"/>
	TR/87 Port	4723	<input checked="" type="radio"/>	<input type="radio"/>

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 the 'Maintenance | Service Controller' configuration page. The left sidebar lists various system settings, with 'Maintenance' expanded to show 'Service Controller'. The main content area is titled 'Service Controller' and contains a table of services and their controller status.

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](#)

Buttons: Start, Stop, Restart Service, **Restart AE Server**, Restart Linux, Restart Web Server

7. Configure Inradiem

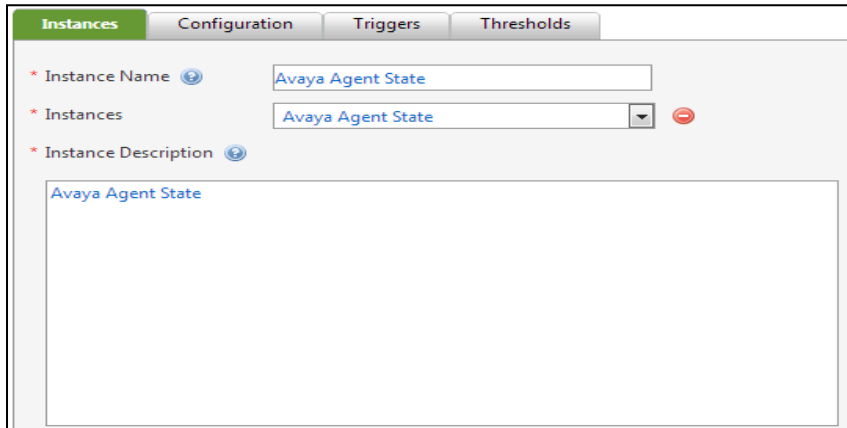
This section provides steps to configure Inradiem application. During the compliance test, the installation and configuration of Inradiem system was performed by Inradiem engineer. This section describes the initial and basic configuration of Inradiem application.

7.1. Instance Configuration

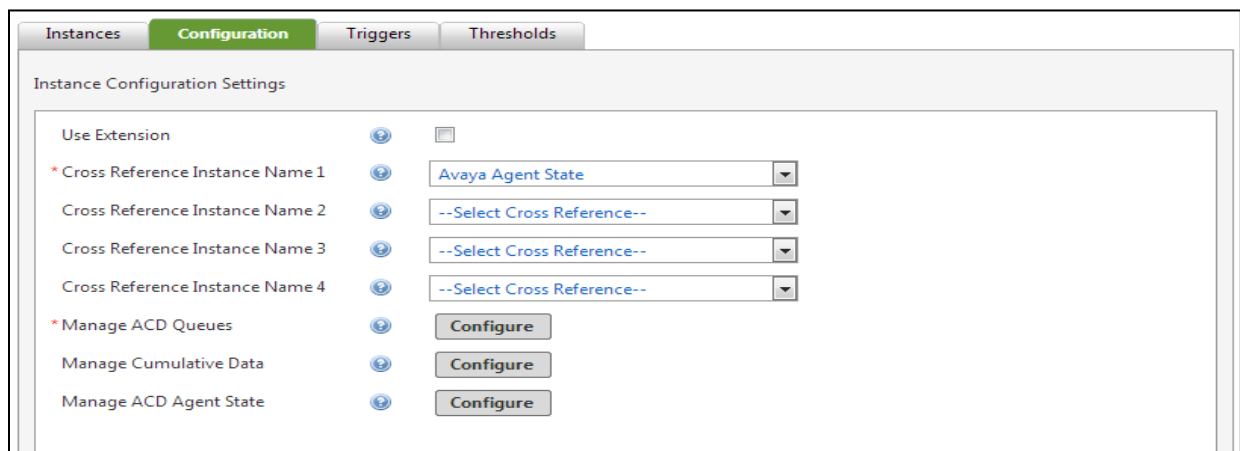
From the Inradiem server, navigate to **Rules → Provider → ACD Provider Category** as shown in the picture below.



Click on Add (+) Button and enter configurations according to the below snapshots.

A screenshot of the 'Instances' configuration page. The 'Instances' tab is selected. The form contains the following fields: 'Instance Name' with the value 'Avaya Agent State', 'Instances' with a dropdown menu showing 'Avaya Agent State' and a red minus button, and 'Instance Description' with a text area containing 'Avaya Agent State'. There are also expand/collapse icons next to the labels.

In the **Configuration** tab, select Avaya Agent State in the **Cross Reference Instance Name1** drop down menu.

A screenshot of the 'Instance Configuration Settings' page. The 'Configuration' tab is selected. The settings include: 'Use Extension' with a checkbox, 'Cross Reference Instance Name 1' with a dropdown menu showing 'Avaya Agent State', 'Cross Reference Instance Name 2' with a dropdown menu showing '--Select Cross Reference--', 'Cross Reference Instance Name 3' with a dropdown menu showing '--Select Cross Reference--', 'Cross Reference Instance Name 4' with a dropdown menu showing '--Select Cross Reference--', and three 'Manage' options: 'Manage ACD Queues', 'Manage Cumulative Data', and 'Manage ACD Agent State', each with a 'Configure' button. There are also expand/collapse icons next to the labels.

Click on **Configure** button in the **Manager ACD Queues** field to enter information of Avaya CM and AES as shown in the screen shot below.

- **ACD/Switch Name:** enter a name of Communication Manager in this case “interopCM”
- **Communication Manger(CM) IP:** enter the IP address of Communication Manger 10.33.1.6
- **Avaya Extension:** enter the hunt group extension **3320** which is configured in **Section 5.6**
- **Application Enablement Services:** enter the IP address 10.33.1.4 of AES
- **AES User Name** and **AES Password:** enter the username “**test**” and its password as configured in **Section 6.5**
- **Port:** enter the DMCC unencrypted port **4721** as configured in **Section 6.7**

Click on **Submit** to save the configuration and **Provider Instance** will be added to the system.

The screenshot displays the 'Manage ACD Agent State' configuration window. The window is titled 'Manage ACD Agent State' and features a close button (X) in the top right corner. The configuration fields are as follows:

Field Label	Value
* ACD/Switch Name	interopCM
* Communication Manager(CM) IP Address	10.33.1.6
* Avaya Extension	3320
Password of Extension	
* Application Enablement Services (AES) IP Address	10.33.1.4
* AES User Name	test
* AES Password	****
* Port	4721

At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Submit'.

7.2. Configuration

The following sections need to be configured in the Intradiem's server, in order to get instance name from Database and do Host & RIS side configuration.

Host Server

- Update ACD API Service config file and add Avaya Instance name in it.
- Update Agent State Service config file and add Avaya Instance name in it.

RIS Server: update Intradiem Avaya Agent State Service config file with the Avaya instance name.

VDN Setup: update Intradiem Avaya Agent State Service config file on RIS side and update VDN number as below. Also, we can add multiple VDN numbers separate by comma (,) sign.

```
<!--VDN Numbers-->  
<VDNNumbers>3340</VDNNumbers>
```

Start following services on Host and RIS Server:

- Intradiem ACD API Service – Host Side
- Intradiem Agent State Service – Host Side
- Intradiem Avaya Agent State Service – RIS Side

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “**status aesvcs cti-link**” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes70	established	15	15

8.2. Verify Avaya Aura® Application Enablement Services

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

Verify that the **Session ID** is associated with the User “intradium” that was used by Intradium application.

The screenshot shows the web interface for the DMCC Service Summary - Session Summary. The navigation menu on the left includes sections for AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The Status section is expanded to show Alarm Viewer, Logs, Log Manager, and Status and Control. Under Status and Control, the DMCC Service Summary is selected.

The main content area displays the following information:

- DMCC Service Summary - Session Summary**
- Please do not use back button
- Enable page refresh every seconds
- Session Summary [Device Summary](#)
- Generated on Tue Nov 24 14:33:07 IST 2020
- Service Uptime: 36 days, 0 hours 10 minutes
- Number of Active Sessions: 1
- Number of Sessions Created Since Service Boot: 19
- Number of Existing Devices: 1
- Number of Devices Created Since Service Boot: 1

The table below shows the active session details:

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	281E593B79EBB00C2 09084D3353E578F-26	intradium	Intradium Integration	10.33.1.200	XML Unencrypted	1

Below the table, there are buttons for **Terminate Sessions** and **Show Terminated Sessions**. At the bottom, it shows "Item 1-1 of 1" and a "Go" button with the number "1" in a text input field.

8.3. Verify Intradiem

1. Create users with cross reference of Avaya Instance (use the agent ID 1000 & 1001 as cross reference value or any other that are configured).
2. Create rule of Agent State Changed event of Avaya Agent State.

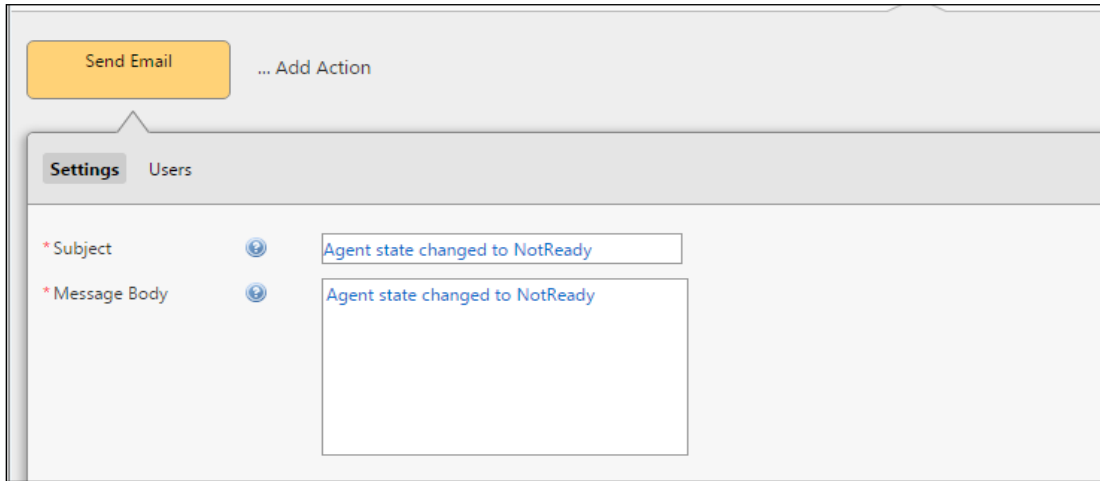
Rule Creation: Create rule following the below snapshot without selecting any condition.

The screenshot shows a configuration interface for selecting an event. At the top, there is a green button labeled 'Select Event' and a link that says '... or Set Frequency'. Below this, there are three main sections: 'Provider Category', 'Provider Instance', and 'Event'. Under 'Provider Category', 'ACD' is selected. Under 'Provider Instance', 'Avaya1' is selected. Under 'Event', 'Agent State Changed' is selected. Other options in the 'Event' list include 'Time in Current State Threshold Met', 'User Logged In', and 'User Logged Out'.

In the event of **Agent State Changed** section, select a state of agent for example “**agentNotReady**” and keep other fields at default. Click Next (not shown) to go to next step.

The screenshot shows the 'Settings' configuration screen for the 'Agent State Changed' event. At the top, there is a green button labeled 'Agent State Changed' and a link that says '... or Set Frequency'. Below this, there is a 'Settings' section with a 'Back to List' link. The settings include: '* Agent State Changed To' with a dropdown menu set to 'agentNotReady'; 'AUX Code' with an empty text input field; '* User List' with a dropdown menu set to 'All Users'; and two unchecked checkboxes: 'Who are also assigned to any of these Queues:' and 'Who are also assigned to any of these Staffing Groups:'. At the bottom, there is an unchecked checkbox for 'Set Schedule'.

Select the **Send Email** in the **Action** section (not shown), the Send Email window displays enter a subject in the **Subject** field and content in the **Message Body**.



The screenshot shows a configuration window for a 'Send Email' action. At the top, there is a yellow button labeled 'Send Email' and a link to '... Add Action'. Below this, there are two tabs: 'Settings' (selected) and 'Users'. Under the 'Settings' tab, there are two required fields: '* Subject' and '* Message Body'. Both fields contain the text 'Agent state changed to NotReady'. There are also small circular icons next to each field.

The screenshot below is the summary of the newly created rule. Intradium application gets the agent state change to not ready as matched with rule above they will send out the email to pre-configured email address.



The screenshot shows a 'Rule Summary' window. It displays a rule flow: 'IF' (white box) -> 'Agent State Changed' (green box) -> 'THEN' (white box) -> 'Send Email' (yellow box). At the bottom right, there are buttons for '< Previous' and 'Submit'. There is also a hamburger menu icon in the top right corner.

Rule Execution

1. Login agent 1000 on any extension number.
2. Change Agent State as 'agentNotReady'
3. Agent state is changed to 'Agent Not Ready' and rule should trigger
4. Verify the action on email inbox.

9. Conclusion

These Application Notes describe the configuration steps required for Intradiem 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 any observations noted in **Section** Error! Reference source not found.

10. Additional References

This section references the product documentation that is relevant to these Application Notes. Documentation for Avaya products may be obtained via <http://support.avaya.com>

- [1] Administering Avaya Aura® Communication Manager, Release 8.1, Document 03-300509, Issue 10, June 2020
- [2] Administering Avaya Aura® Session Manager, Release 8.1, Issue 7, Jan 2020
- [3] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 8.1, Document 02-300357, Jan 2020.

Documentation related to Intradiem may directly be obtained from Intradiem.

©2021 Avaya Inc. All Rights Reserved.

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

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