Avaya Solution & Interoperability Test Lab

Application Notes for Intradiem 9.5 and Avaya Aura® Application Enablement Services 7.1 – 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 group and its agents on Avaya Aura® Communication Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for Intradiem application with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.1.

In the compliance testing, Intradiem is a Windows application that uses the Device Media Call Control interface (DMCC) from Avaya Aura® Application Enablement Services to monitor and get events of contact center agents on Avaya Aura® Communication Manager. Avaya Agent State is the component that Intradiem uses to trigger agent state events, exposed data and actions. Once started the Intradiem application will connect to the AES server, acquire hunt group extension and VDN number.

2. General Test Approach and Test Results

The feature test cases were performed manually. Agents were manually logged in and out and their states were changed from their telephones, which included H323 and SIP IP telephones. The testing verified that events of status changes on agent's telephones were 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 AES 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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

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

Encryption (TLS/SRTP) was used internal 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 that has PRI/T1 trunk to PSTN. The Intradiem server running on Windows 2012 server and connected to Avaya Aura® Application Enablement Service via DMCC port 4721.

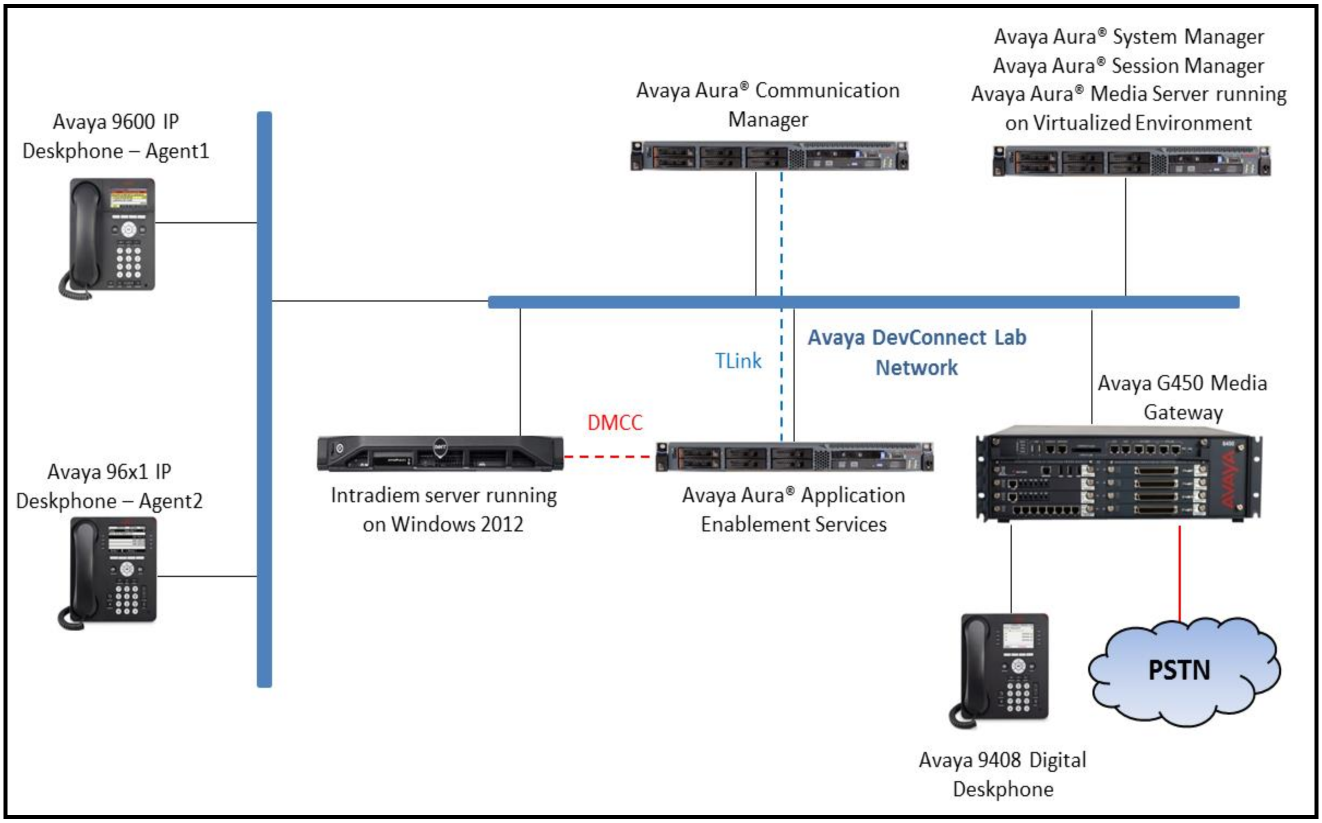

Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya Aura® Media Server running on Virtualized Environment
Avaya Aura® Communication Manager
Avaya 9600 IP Deskphone – Agent1
TLink
Avaya DevConnect Lab Network
Avaya G450 Media Gateway
DMCC
Avaya 96x1 IP Deskphone – Agent2
Intradiem server running on Windows 2012
Avaya Aura® Application Enablement Services
PSTN
Avaya 9408 Digital Deskphone

Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running in Virtual Environment	R017x.00.0.441.0 7.1.3.0.0-FP3
Avaya G450 Media Gateway	39.12.0
Avaya Aura® Media Server running in Virtual Environment	7.8.0.384
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.2
Avaya Aura® System Manager running on Virtualized Environment	7.1.3.0.037763
Avaya Aura® Session Manager running on Virtualized Environment	7.1.3.0.037763
Avaya 9611G IP Deskphone (SIP)	Avaya one-X® Deskphone Release 7.1.2
Avaya 9641G IP Deskphone (H.323)	Avaya one-X® Deskphone Release 6.65
Intradiem running on Windows 2012 Server	9.5.25

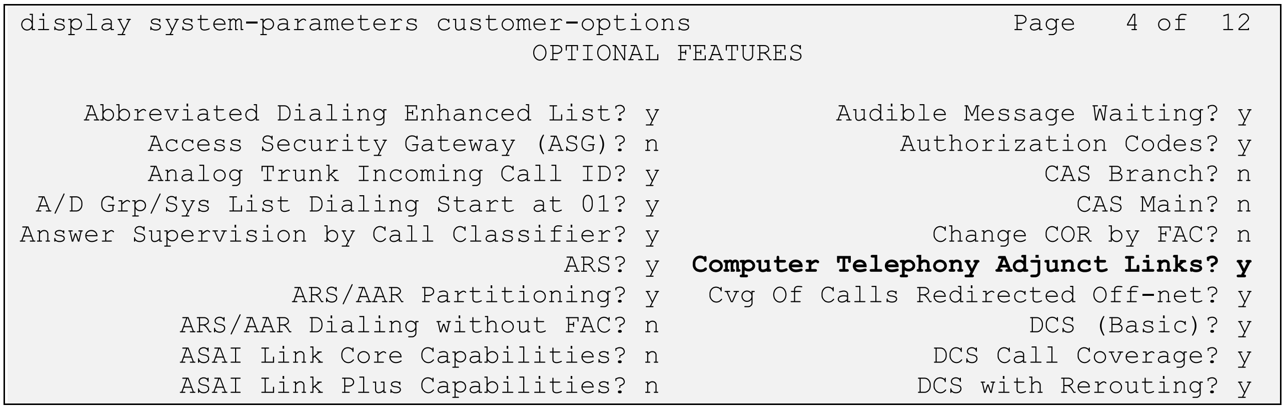
5. Configure Avaya Aura® Communication Manager

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

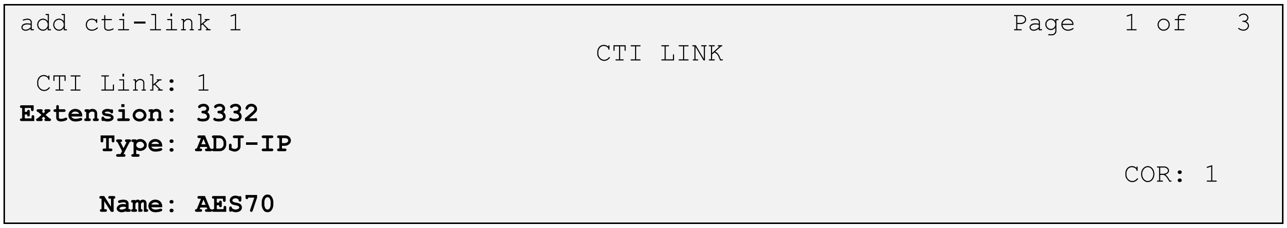
Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.



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

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

5.2. Administer CTI Link

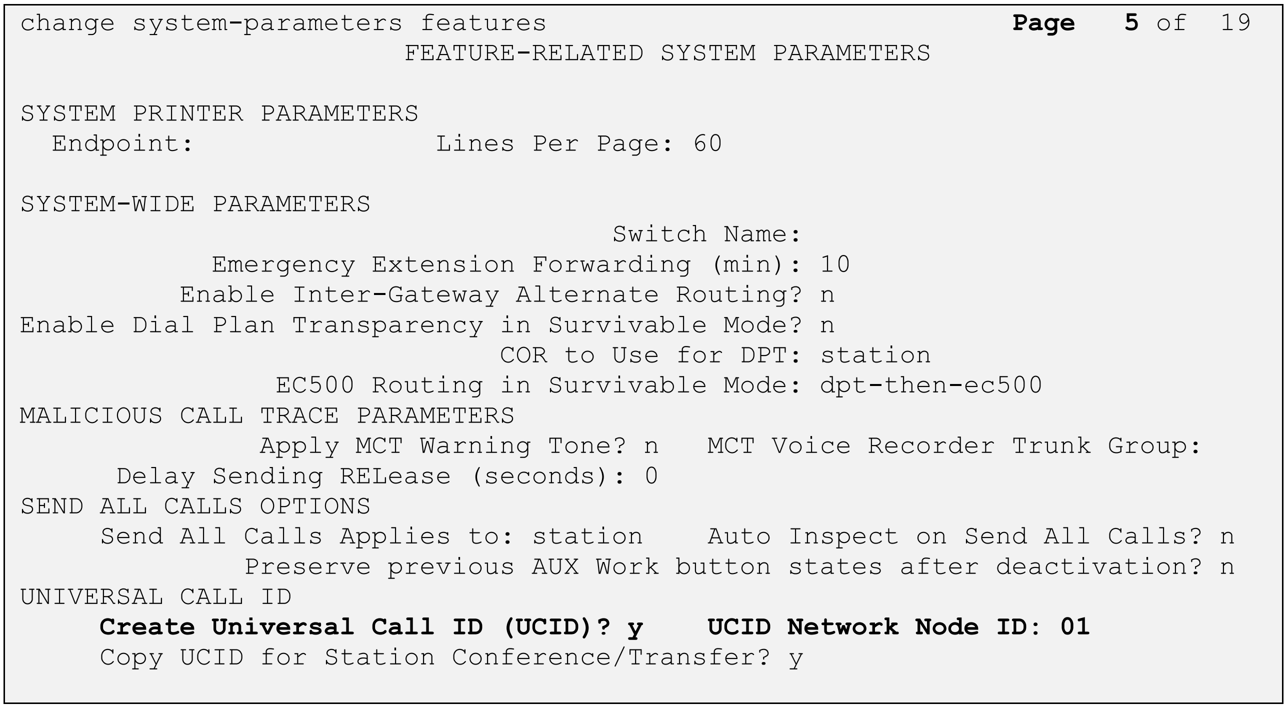
Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. 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
```

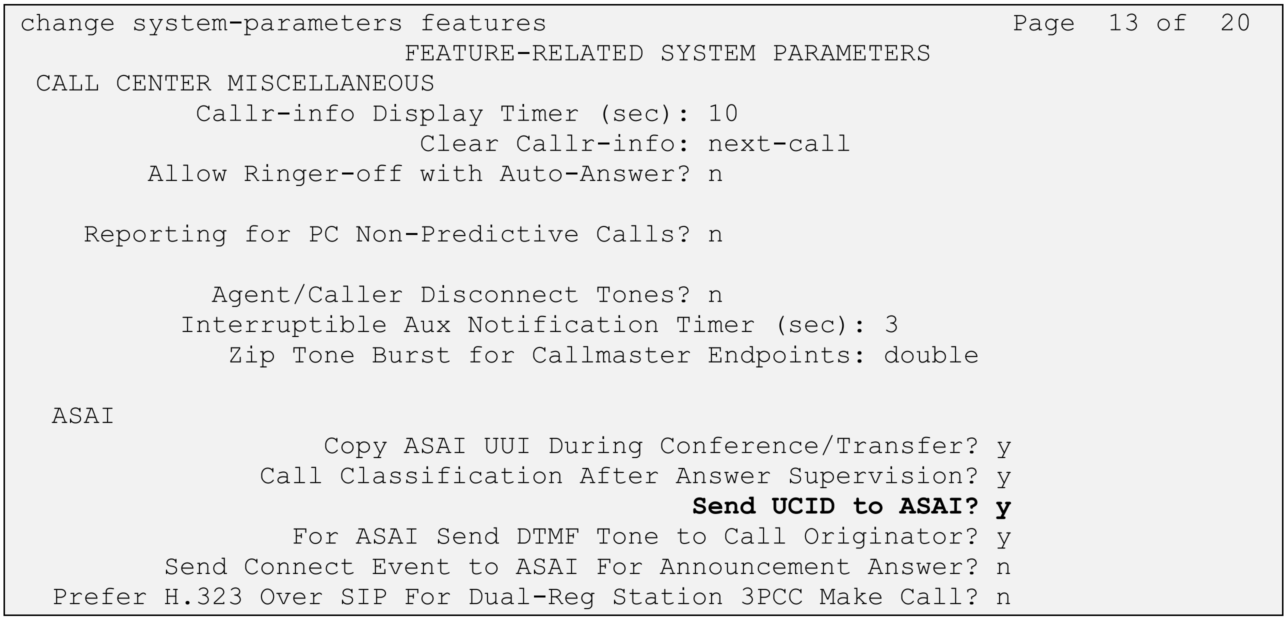
5.3. Administer System Parameters Features

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 UUI 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     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
```

Go to **Page 4**, enter the following values. **AE Services Server** should be the host name of the AES Server. 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       Password          Enabled    Status
                   Server
      1:      aes70            *                      y        in use
```

5.5. 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 5.7**.

```
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
```

5.6. 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.

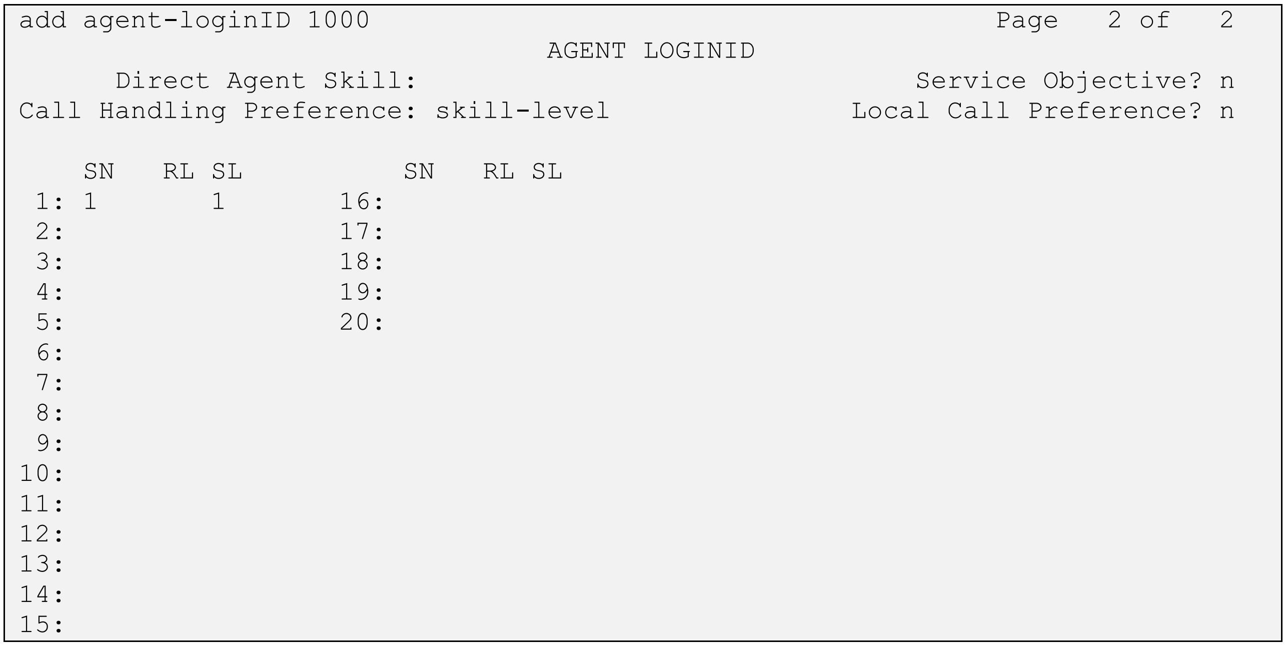
```
add vdn 3340                                                  Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 3340
                                 Name*: Contact Center 1
                           Destination: Vector Number        1
                   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*:
```

5.7. 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:                 17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
```

6. Configure Avaya Aura® Application Enablement Services

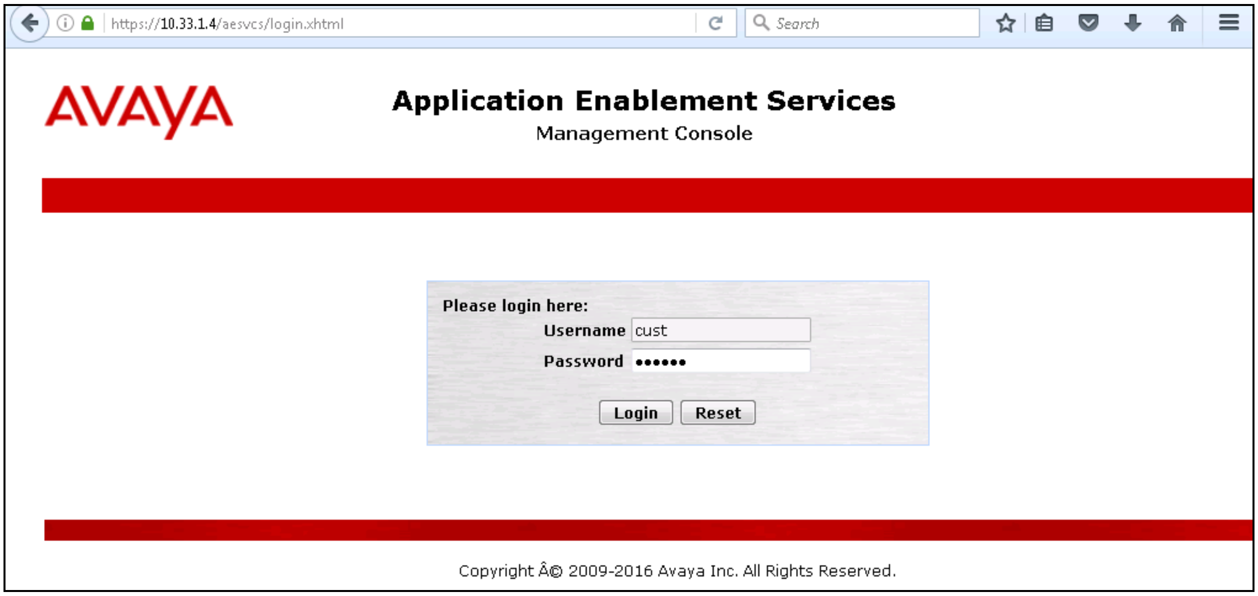
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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.

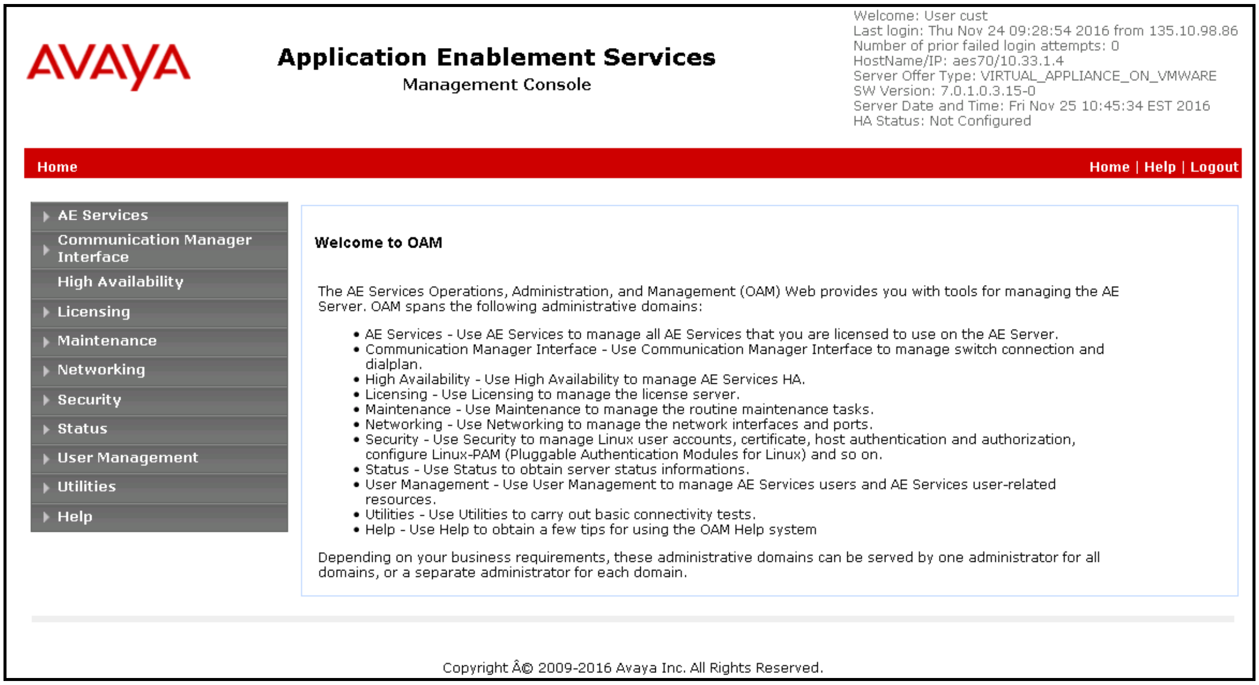


https://10.33.1.4/aesvcs/login.xhtml

Application Enablement Services
Management Console

Please login here:
Username cust
Password ••••••

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



Welcome: User cust
Last login: Thu Nov 24 09:28:54 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 10:45:34 EST 2016
HA Status: Not Configured

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:

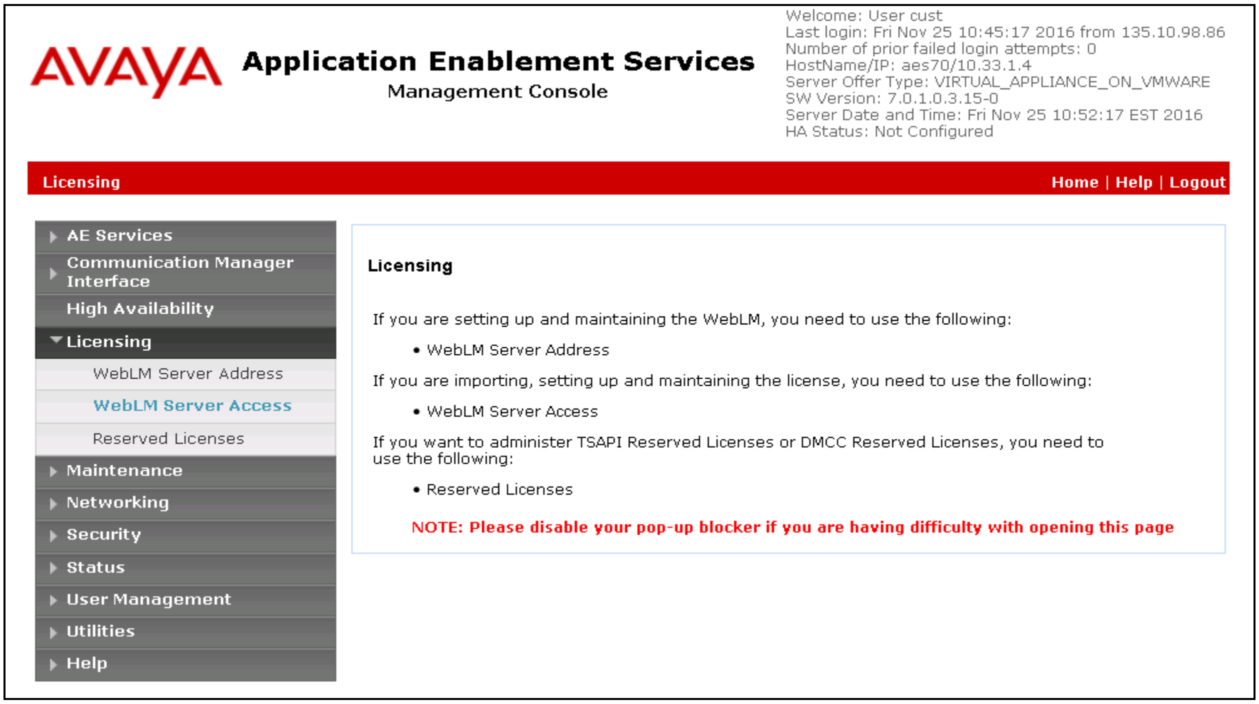
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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.

Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

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).



Welcome: User cust
Last login: Fri Nov 25 10:45:17 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 10:52:17 EST 2016
HA Status: Not Configured

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

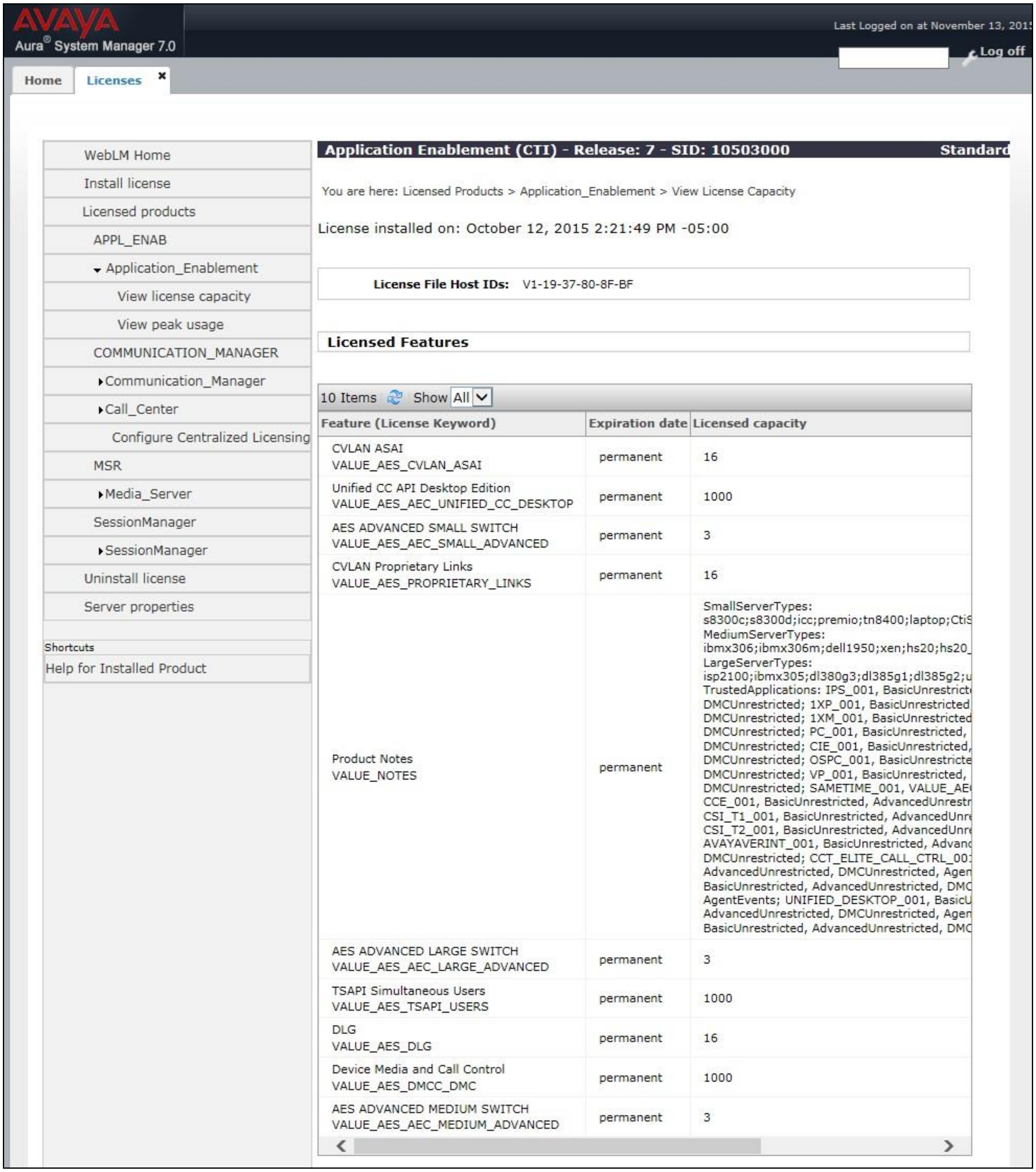
If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- 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.



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

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

License installed on: October 12, 2015 2:21:49 PM -05:00

License File Host IDs: V1-19-37-80-8F-BF

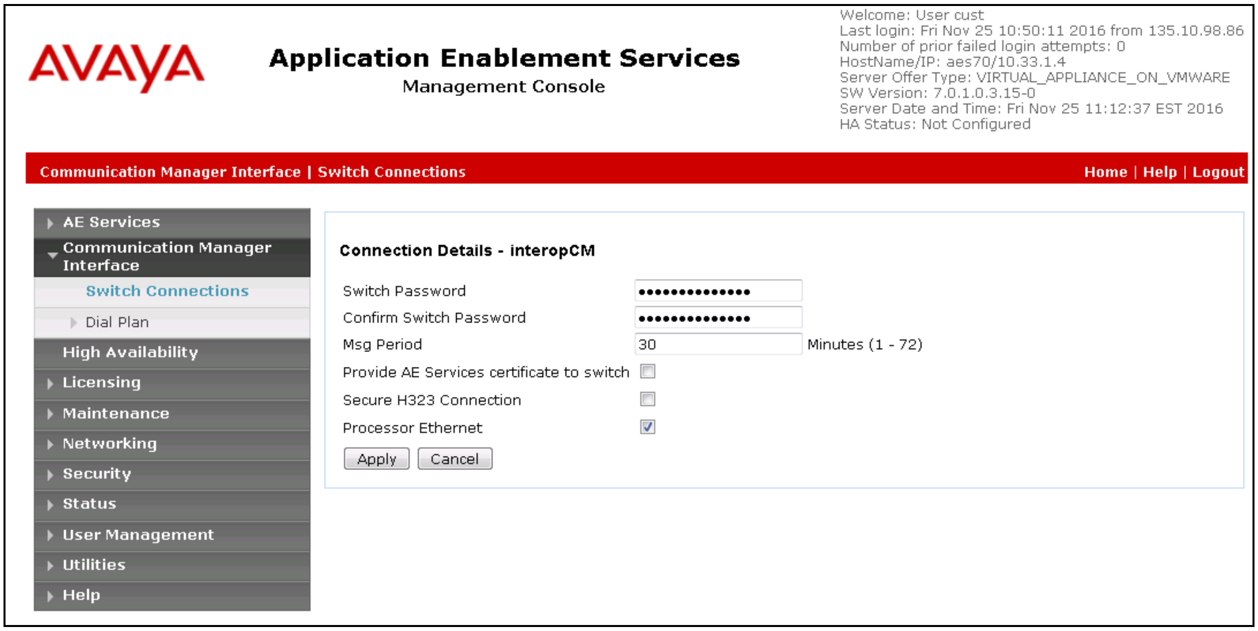
Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;Cti MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricte DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AE CCE_001, BasicUnrestricted, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnr CSI_T2_001, BasicUnrestricted, AdvancedUnr AVAYAVERINT_001, BasicUnrestricted, Advanc DMCUnrestricted; CCT_ELITE_CALL_CTRL_00 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

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.

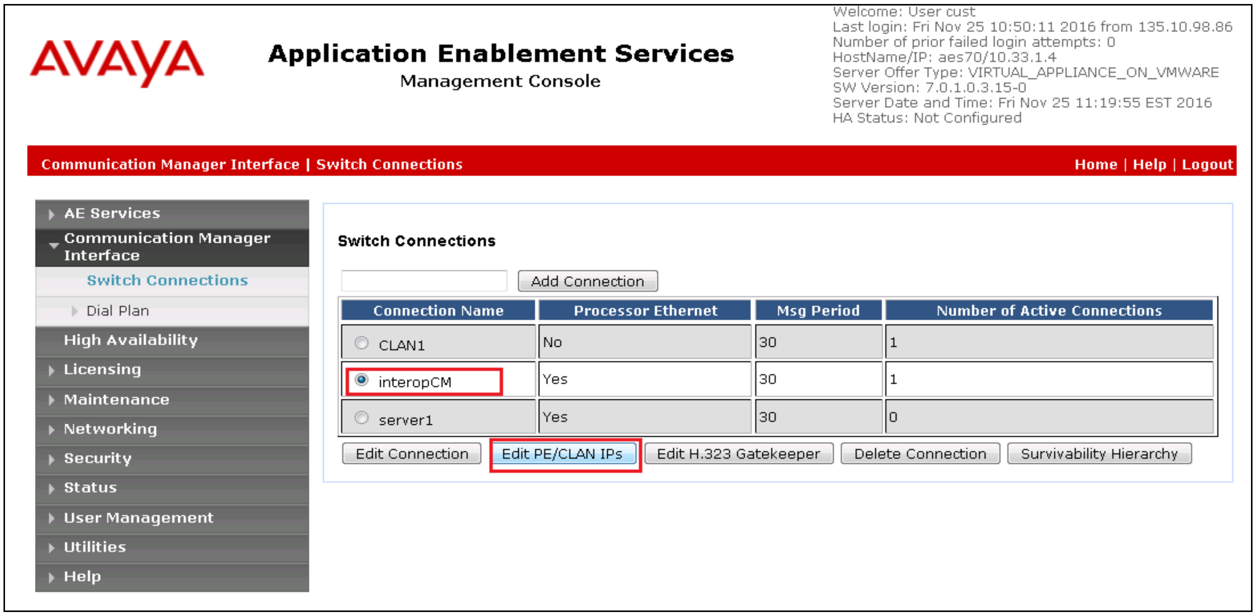


Welcome: User cust
Last login: Fri Nov 25 10:50:11 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 11:12:37 EST 2016
HA Status: Not Configured

Connection Details - interopCM

Switch Password	••••••••••••••
Confirm Switch Password	••••••••••••••
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	□
Secure H323 Connection	□
Processor Ethernet	☑

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

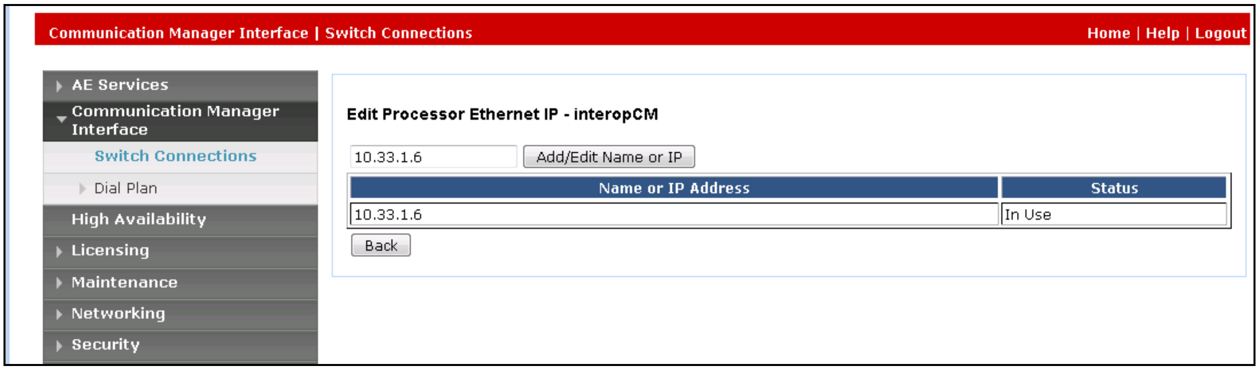


Welcome: User cust
Last login: Fri Nov 25 10:50:11 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 11:19:55 EST 2016
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ CLAN1	No	30	1
● interopCM	Yes	30	1
○ server1	Yes	30	0

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

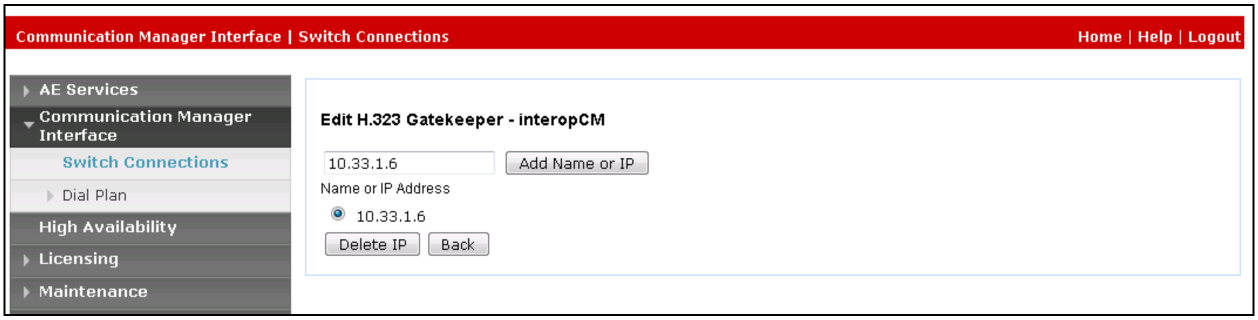


Edit Processor Ethernet IP - interopCM

10.33.1.6

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.



Edit H.323 Gatekeeper - interopCM

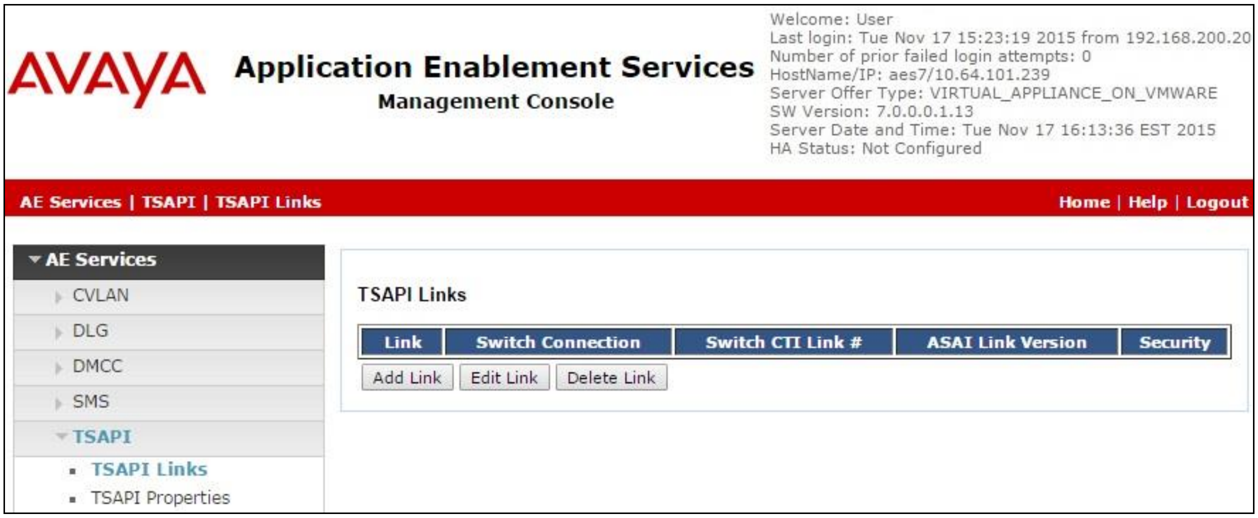
10.33.1.6

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**.

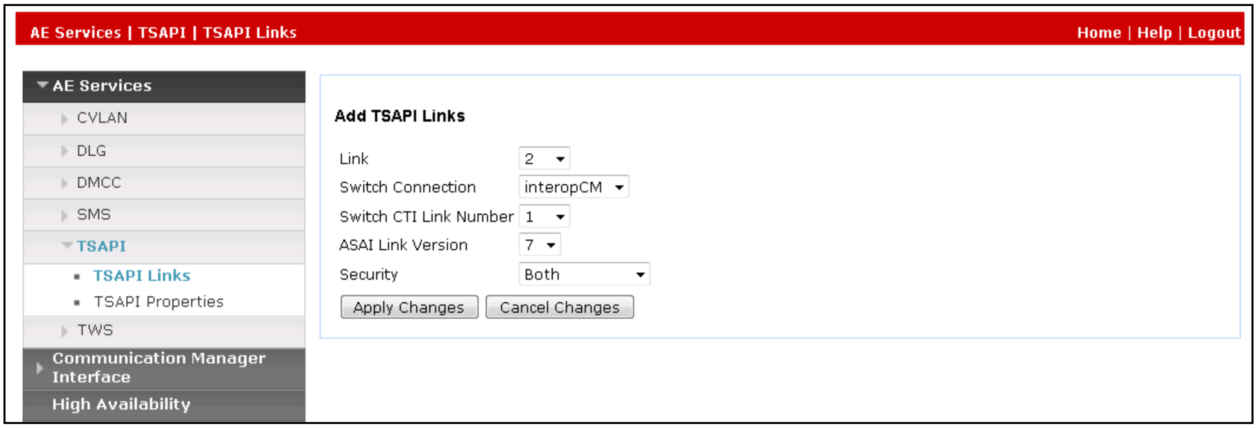


Welcome: User
Last login: Tue Nov 17 15:23:19 2015 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Nov 17 16:13:36 EST 2015
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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.



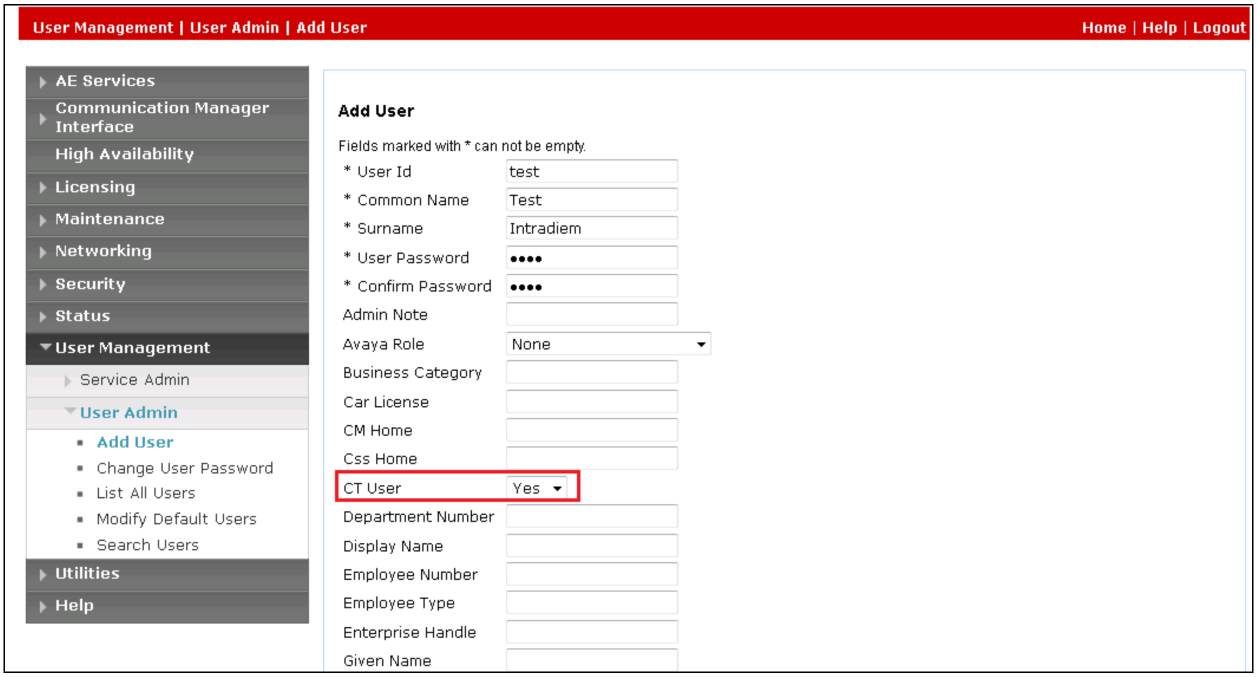
Add TSAPI Links

Link	2
Switch Connection	interopCM
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

Apply Changes | Cancel Changes

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.



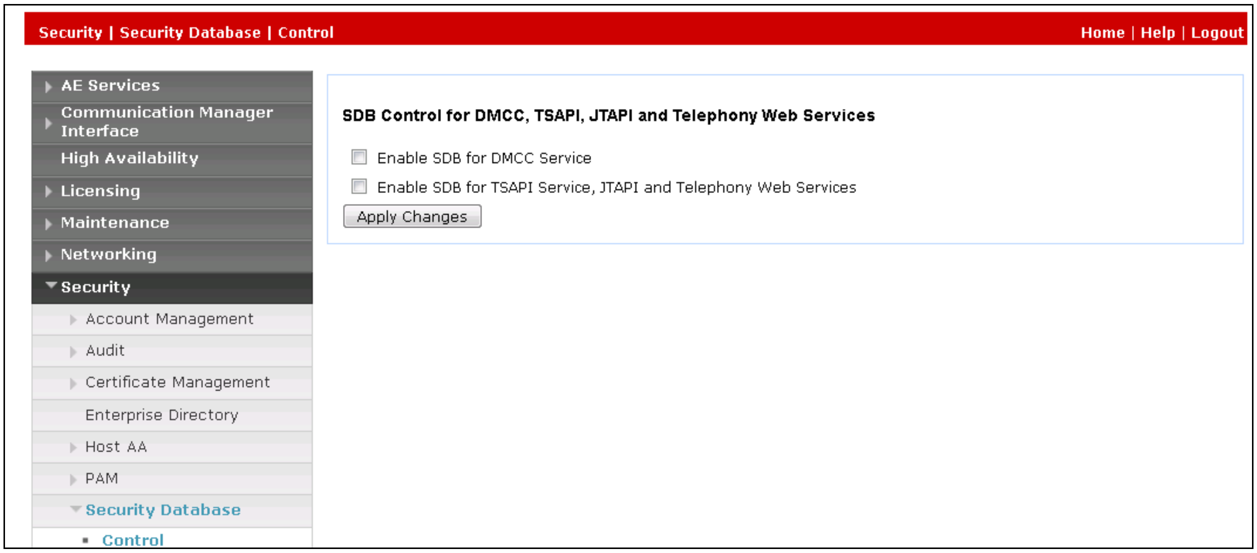
Add User

Fields marked with * can not be empty.

* User Id	test
* Common Name	Test
* 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	
Employee Type	
Enterprise Handle	
Given Name	

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.



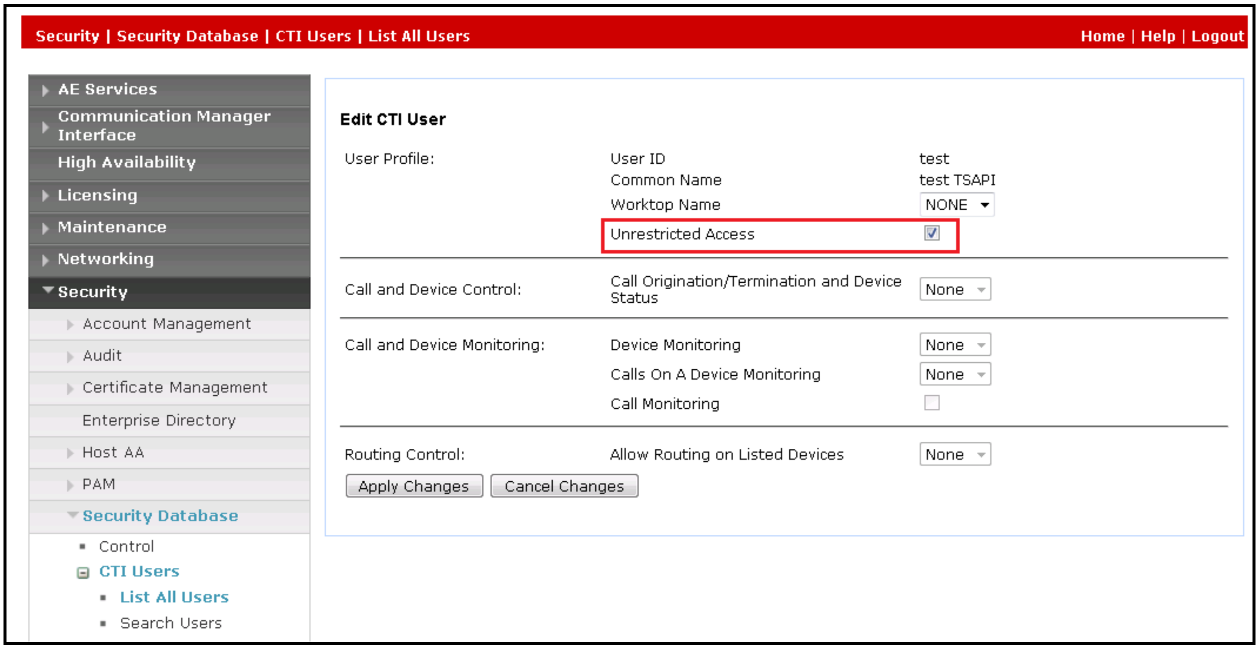
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

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.



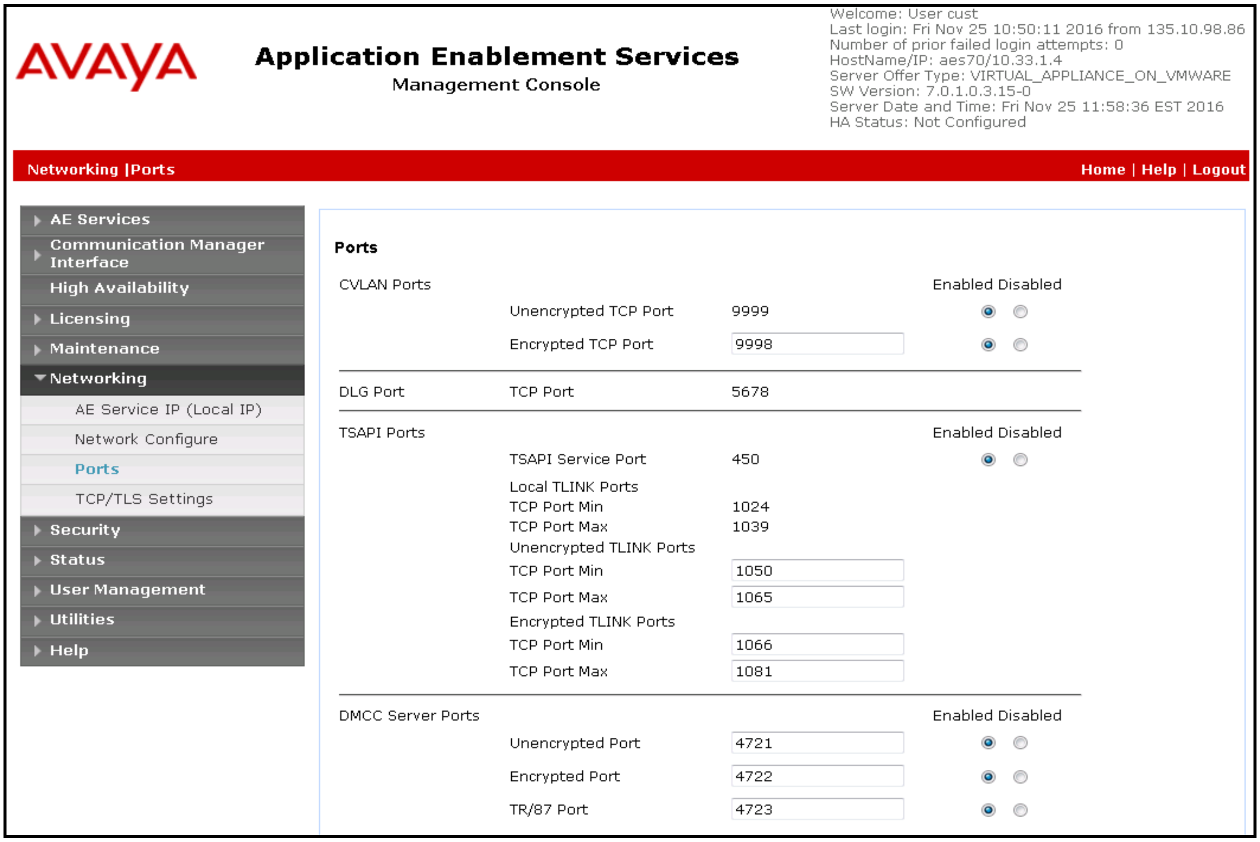
Edit CTI User

User Profile:	User ID	test
	Common Name	test TSAPI
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

Apply Changes | Cancel Changes

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.



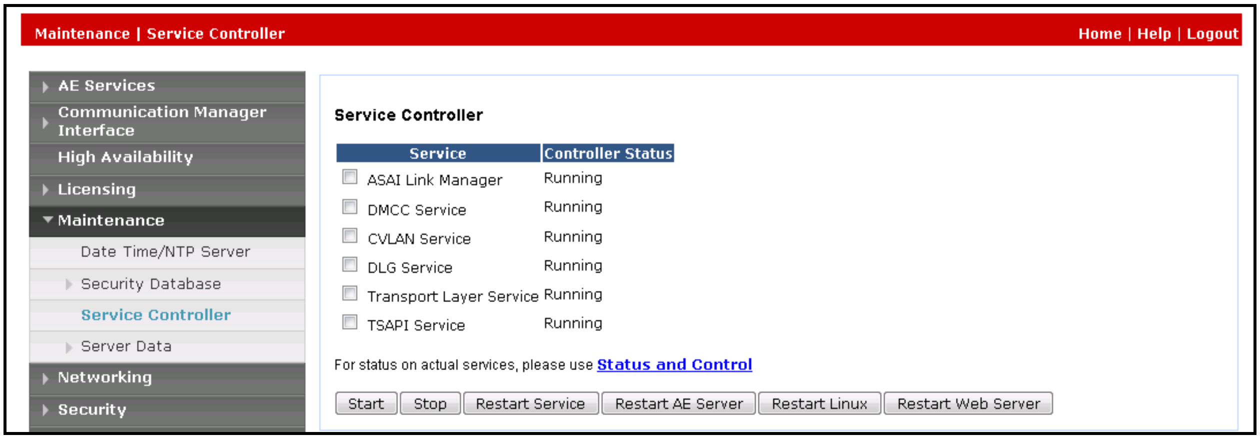
Welcome: User cust
Last login: Fri Nov 25 10:50:11 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 11:58:36 EST 2016
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

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**.



Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
□ TSAPI Service	Running

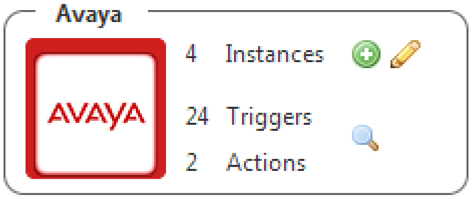
For status on actual services, please use Status and Control

7. Configure Intradiem System

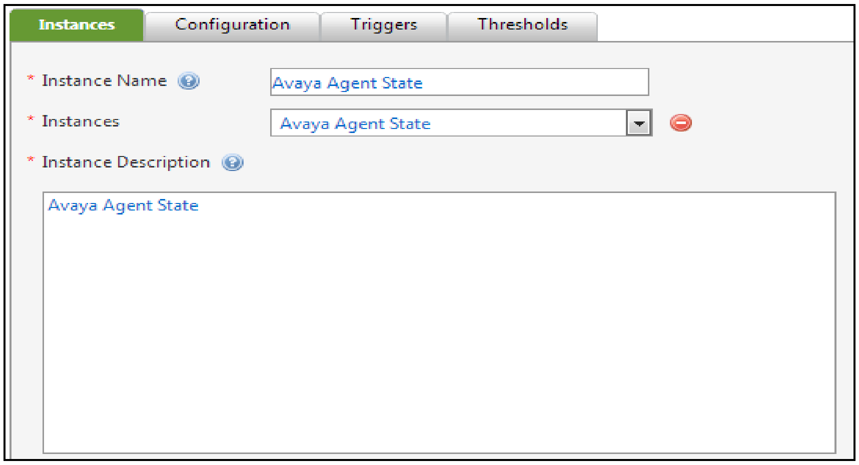
This section provides steps to configure Intradiem application. During the compliance test, the installation and configuration of Intradiem system was performed by Intradiem engineer. This section describes the initial and basic configuration of Intradiem application.

7.1. Instance Configuration

From the Intradiem 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.

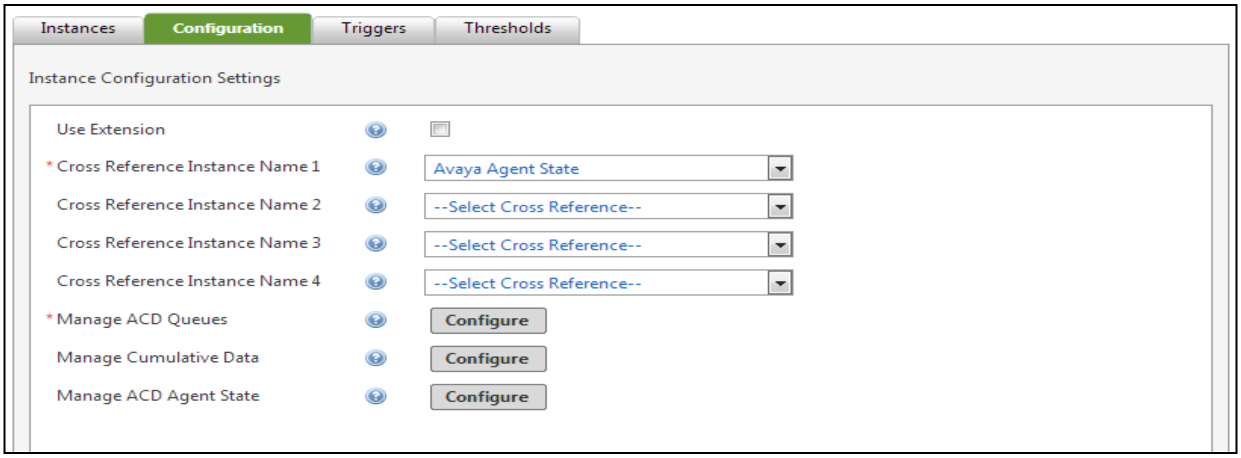


* Instance Name: Avaya Agent State

* Instances: Avaya Agent State

* Instance Description: Avaya Agent State

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



Instance Configuration Settings

Use Extension □

* Cross Reference Instance Name 1: Avaya Agent State

Cross Reference Instance Name 2: --Select Cross Reference--

Cross Reference Instance Name 3: --Select Cross Reference--

Cross Reference Instance Name 4: --Select Cross Reference--

* Manage ACD Queues

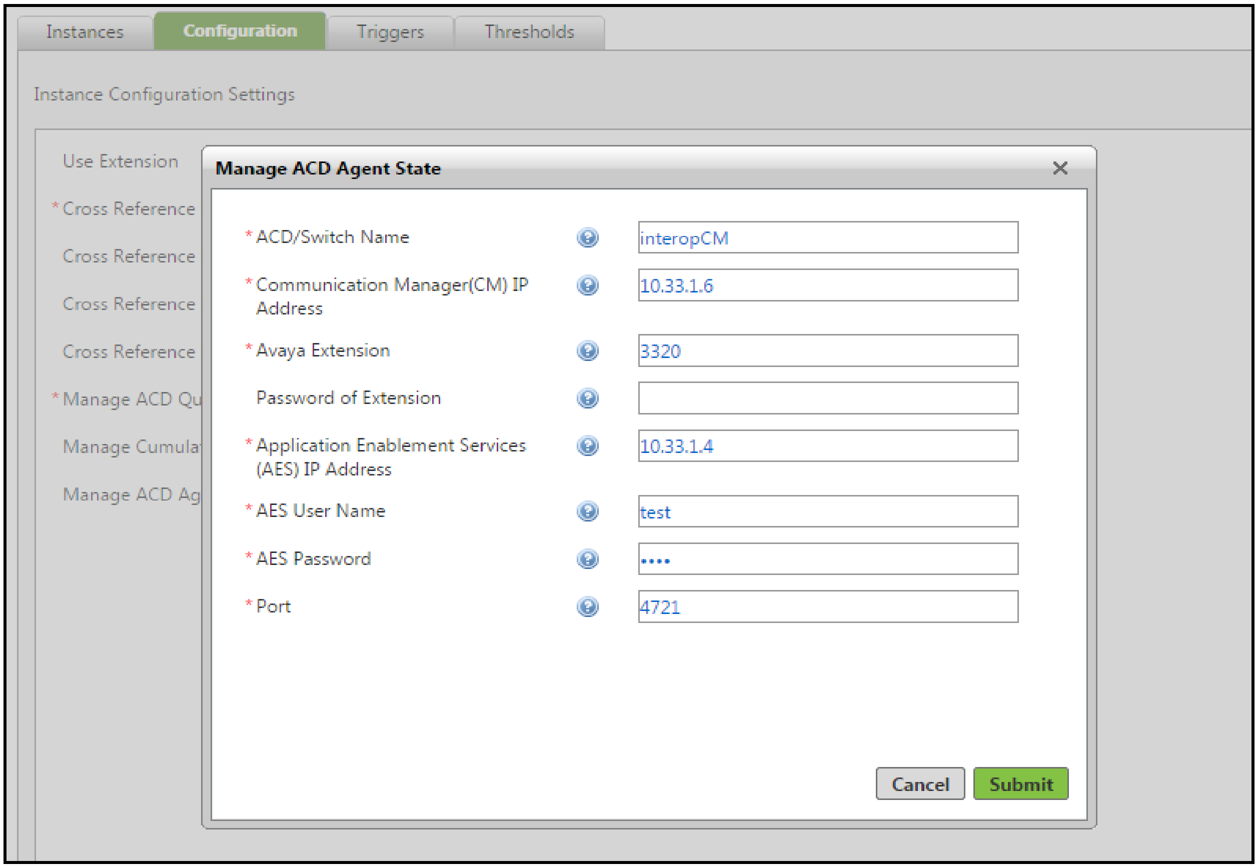
Manage Cumulative Data

Manage ACD Agent State

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.



Manage ACD Agent State

* 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

7.2. Configuration

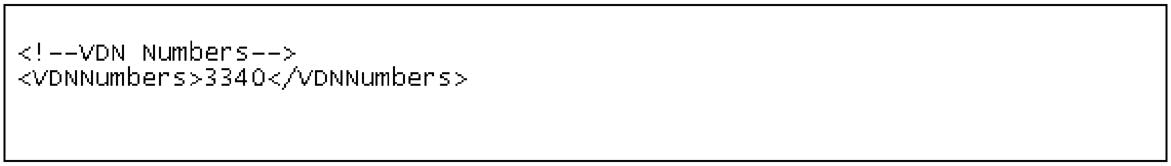
Get instance name from Database and do Host & RIS side configuration

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 Intradiem.

8.1. Verify Avaya Aura® Communication Manager

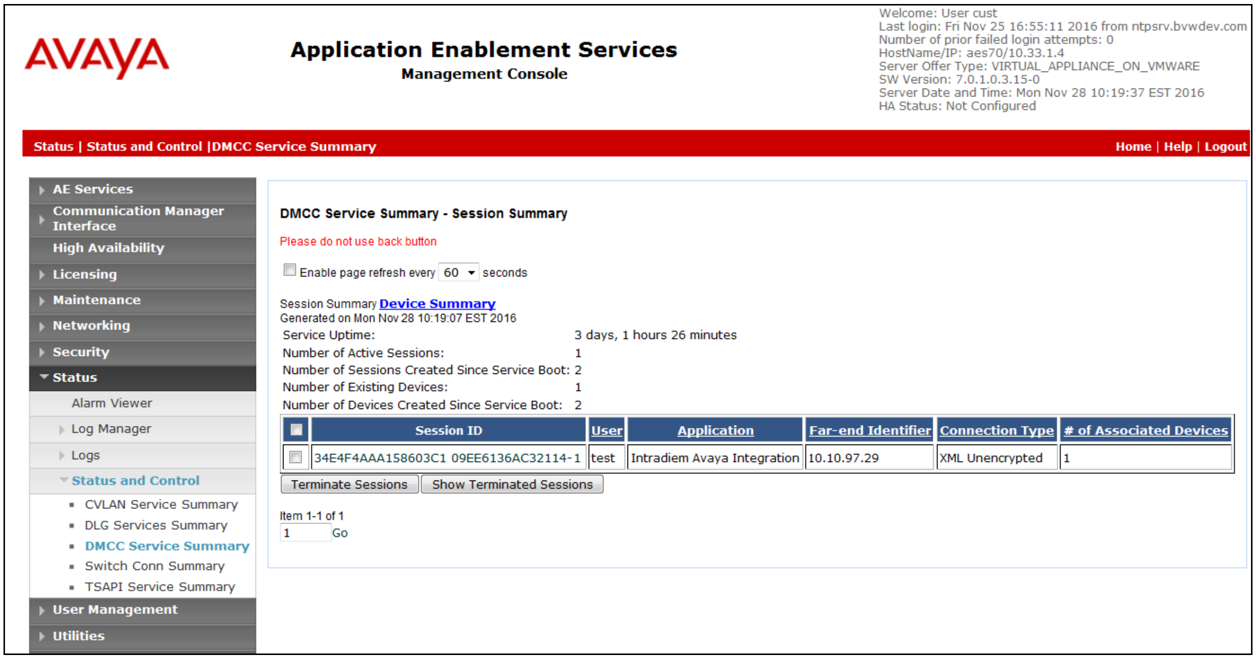
On Communication Manager, verify the status of the administered CTI link by using the "**status aesvcs cti-link**" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     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 **test** that was used by Intradiem application.



Welcome: User cust
Last login: Fri Nov 25 16:55:11 2016 from ntpsrv.bvwdev.com
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Mon Nov 28 10:19:37 EST 2016
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Mon Nov 28 10:19:07 EST 2016

Service Uptime:	3 days, 1 hours 26 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	2
Number of Existing Devices:	1
Number of Devices Created Since Service Boot:	2

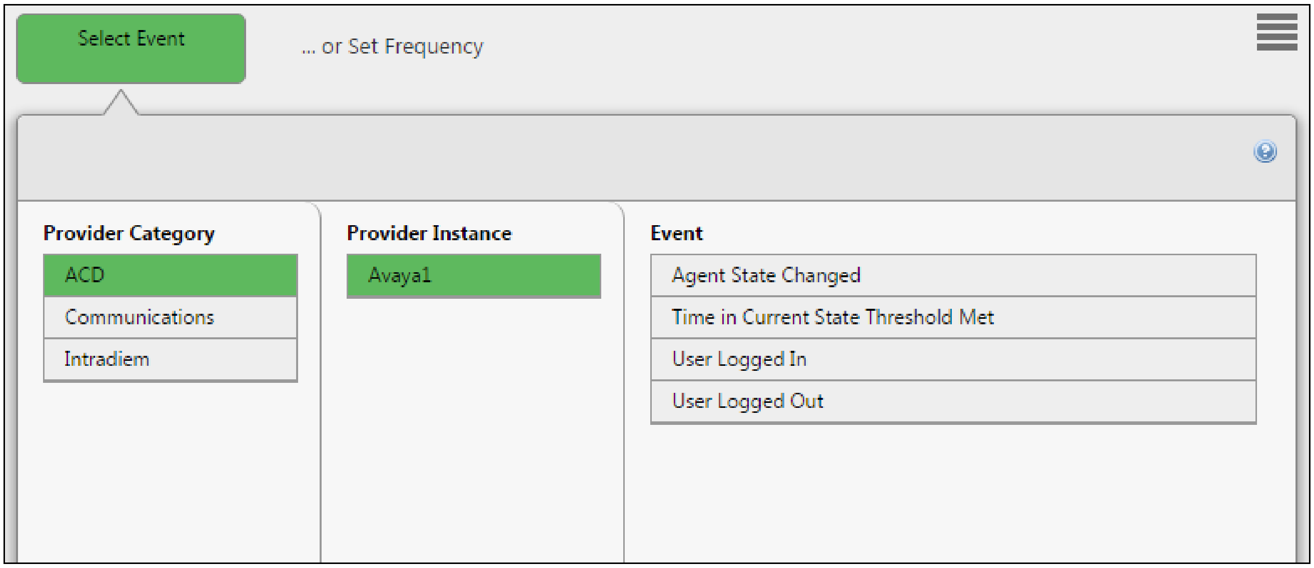
□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	34E4F4AAA158603C1 09EE6136AC32114-1	test	Intradiem Avaya Integration	10.10.97.29	XML Unencrypted	1

Item 1-1 of 1
1

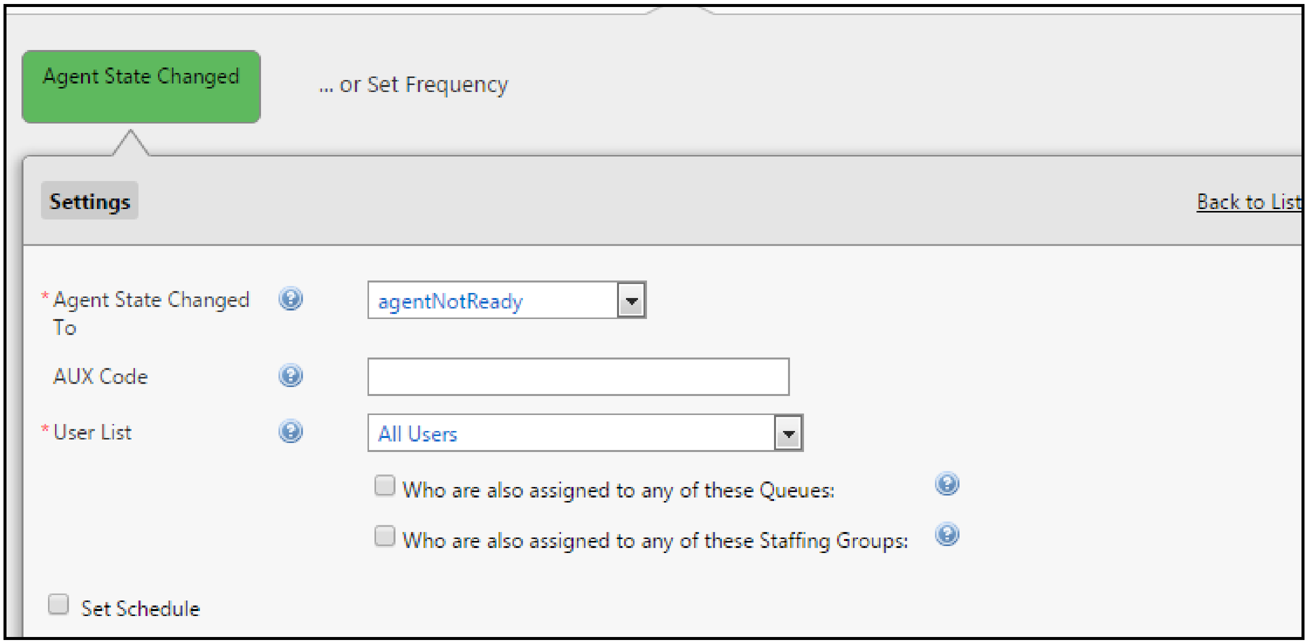
8.3. Verify Intradiem

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.



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.



* Agent State Changed To: agentNotReady

AUX Code:

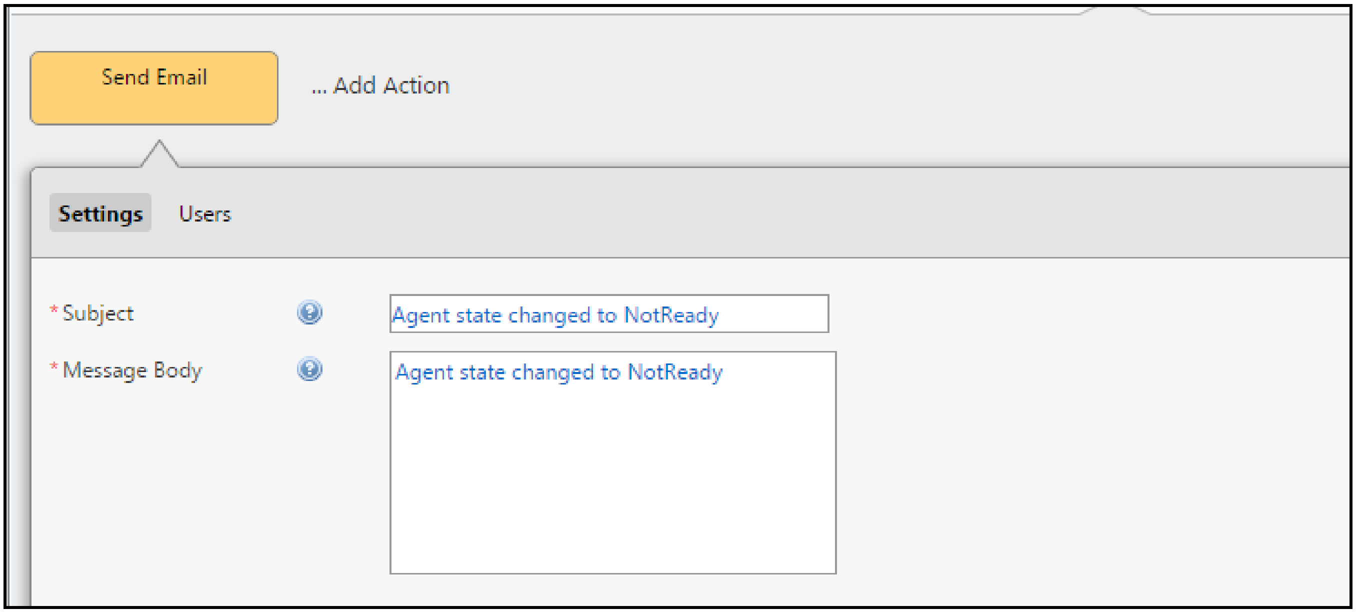
* User List: All Users

□ Who are also assigned to any of these Queues:

□ Who are also assigned to any of these Staffing Groups:

□ Set Schedule

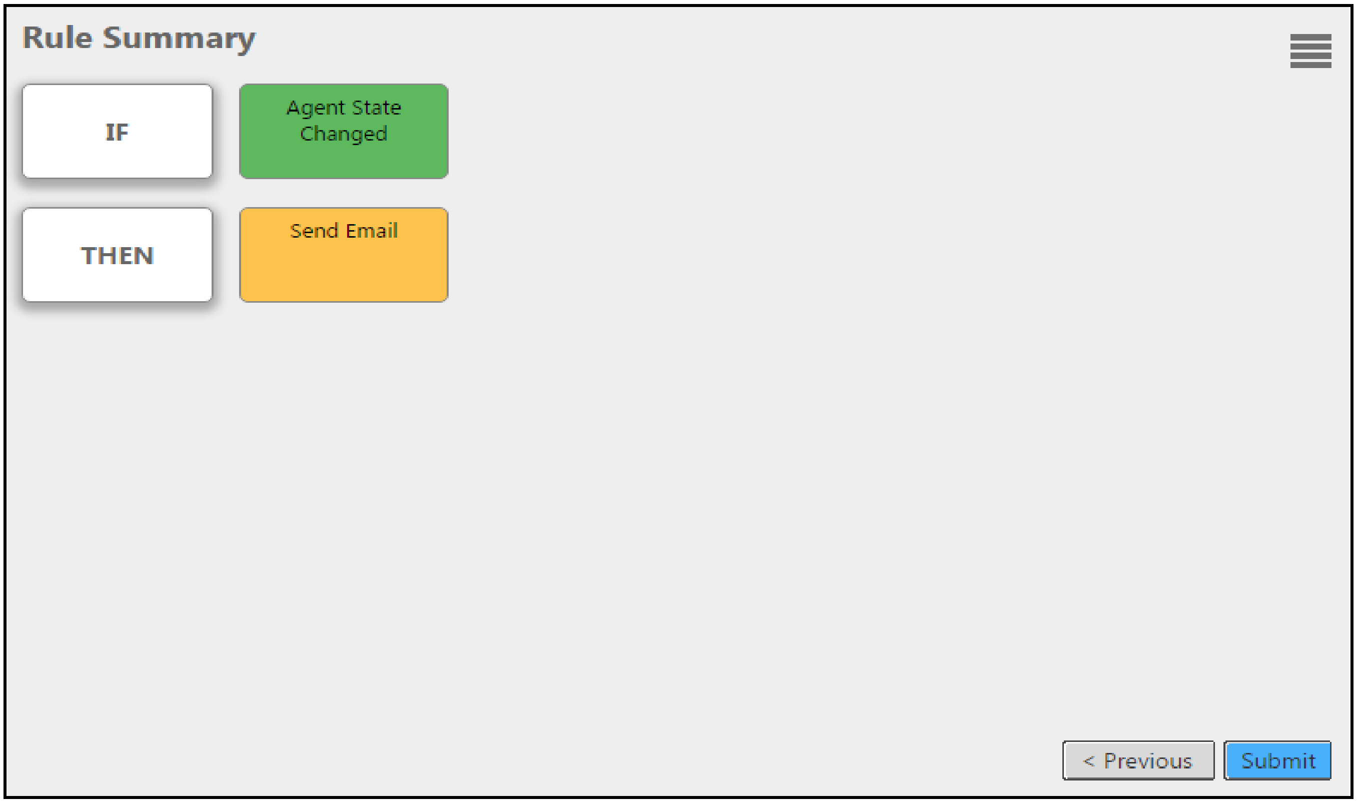
Select the **Send Email** in the **Action** section (not shown), the Send Email window displays enter a subject in the Subject field and content in the Message Body.



* Subject: Agent state changed to NotReady

* Message Body: Agent state changed to NotReady

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



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 7.1 and Avaya Aura® Application Enablement Services 7.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

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 7.0.3, Document 03-300509, Issue 10, May 2018.

[2] Administering Avaya Aura® Session Manager, Release 7.0, Issue 7, May 2018.

[3] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 7.0, Document 02-300357, May 2018.

Documentation related to Intradiem may directly be obtained from Intradiem

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.