Avaya Solution & Interoperability Test Lab

Application Notes for CTIntegrations CT Suite 2.1.5 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 2.1.5 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. CTIntegrations CT Suite is a CTI based contact center solution.

In the compliance testing, CTIntegrations CT Suite used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager and provide screen pop, click-to-dial, and call control features from the agent desktops running the CTIntegrations CT Desktop application.

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 CTIntegrations CT Suite 2.1.5 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. CT Suite is a CTI based contact center solution.

In the compliance testing, CT Suite used Device, Media, and Call Control (DMCC) .Net from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager and provide screen pop, click-to-dial, and call control features from agent desktops running the CT Desktop application.

The agent desktops used CT Desktop to connect to CT Suite. Upon an agent launching CT Desktop, the application will connect to the CT Suite server and then CT Desktop used DMCC to query device information and requested device monitoring.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon an agent log into CT Desktop, the application will connect to the CT Suite server passing agent desktop Windows username and PC hostname. After successful startup CT Desktop is updated with extension monitored as indicated in the CT Desktop application status bar.

For the manual part of the testing, incoming ACD calls were placed with available agents that have CT Desktop application launched and connected to CT Suite. All necessary call actions were initiated from the agent desktops and/or telephones. The click-to-dial calls were initiated by clicking on the contact phone number displayed on the agent desktop history tab.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the CT Suite server and CT Desktop PC.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on CT Suite:

- Use of DMCC logical device services to set agent states, including log in, log out, and work mode changes with support for reason codes, pending aux work.
- Use of DMCC call control services to support call control and click-to-dial features.
- Use of DMCC monitor and event report services to monitor agent stations and existing calls.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, conference, transfer, long duration, send DTMF, click-to-dial from contact phone number, pending aux work and aux work reason codes.

The serviceability testing focused on verifying the ability of CT Suite to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to CT Suite server and the PC running CT Desktop.

2.2. Test Results

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

- By design, the agent desktop does not support initiation of unattended conference.
- By design, all special characters are not allowed in the Telephone Number field where user enters number to make an outgoing call.
- Upon placing an invalid outbound call from CT Desktop, an End button appears on the desktop when the associated agent telephone type is H.323. However, when the associated agent telephone is SIP, the End button does not appear and the work around is to hang up the call from the agent telephone.
- By default, CT Desktop expects agent telephones to be configured with 3 call appearances. If an agent telephone has only 2 call appearances configured on Communication Manager, then CT Desktop still reflects 3 call appearances.
- For a call that stays up during Ethernet disruption on agent PC, user needs to restart CT Desktop application in order for CT Desktop to reflect current status.
- In the blind transfer scenario, after agent-1 transferred an ACD call from the PSTN to agent-2, the agent-2 desktop continued to reflect agent-1 as the other party on the call instead of the PSTN.
- In the attended conference scenario, after agent-1 conferenced an ACD call from the PSTN with agent-2, agent-1 desktop was updated to reflect the conference whereas agent-2 desktop continued to reflect agent-1 being the other party. Furthermore, after agent-2 dropped from the conference, agent-1 desktop was updated to reflect agent-2 being the other party instead of the PSTN.

- As the application requires a fixed mapping of agent station to agent ID therefore the agent must use a fixed station to log in and not be able to use any other station.

2.3. Support

For technical support on the CTIntegrations CT Suite, contact CTIntegrations via phone, email, or internet.

- **Phone:** +1 877 449 6775
- **Email:** info@ctintegrations.com
- **Web:** http://www.ctintegrations.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, CT Suite monitored the agent stations shown in the table below.

Device Type	Extension
VDNs	56001, 56010
Skill Groups	56300, 56303
Agent Stations	56105, 56204, 54106
Agent IDs	1000, 1002, 1004
Agent Passwords	1234

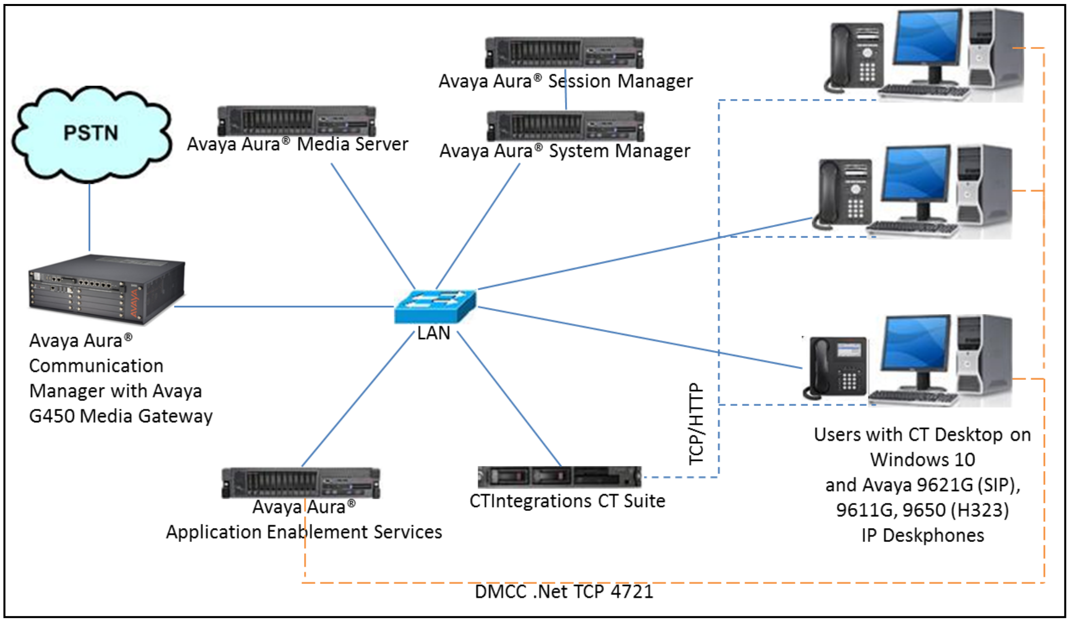

Avaya Aura® Session Manager
PSTN
Avaya Aura® Media Server
Avaya Aura® System Manager
Avaya Aura® Communication Manager with Avaya G450 Media Gateway
LAN
TCP/HTTP
Users with CT Desktop on Windows 10 and Avaya 9621G (SIP), 9611G, 9650 (H323) IP Deskphones
Avaya Aura® Application Enablement Services
CTIntegrations CT Suite
DMCC .Net TCP 4721

Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	R017x.00.0.441.0 7.0.1.0.0-FP1
Avaya G450 Media Gateway	37.19.0
Avaya Aura® Media Server in Virtual Environment	7.7.019 (FP1)
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1.0.2.15
Avaya Aura® System Manager in Virtual Environment	7.0.1.0
Avaya Aura® Session Manager in Virtual Environment	7.0.1.0.701007
Avaya 9621G, IP Deskphone (SIP)	7.0.1
Avaya 9611G IP Deskphone (H.323)	6.6029
Avaya 9650 IP Deskphones (H.323)	3.250A
CTIntegrations CT Suite on Windows Server 2012	2.1.5 R2 Standard
CTIntegrations CT Desktop on Windows 10 Pro • Avaya .Net DMCC	2.5.1.16190 6.3.3.14

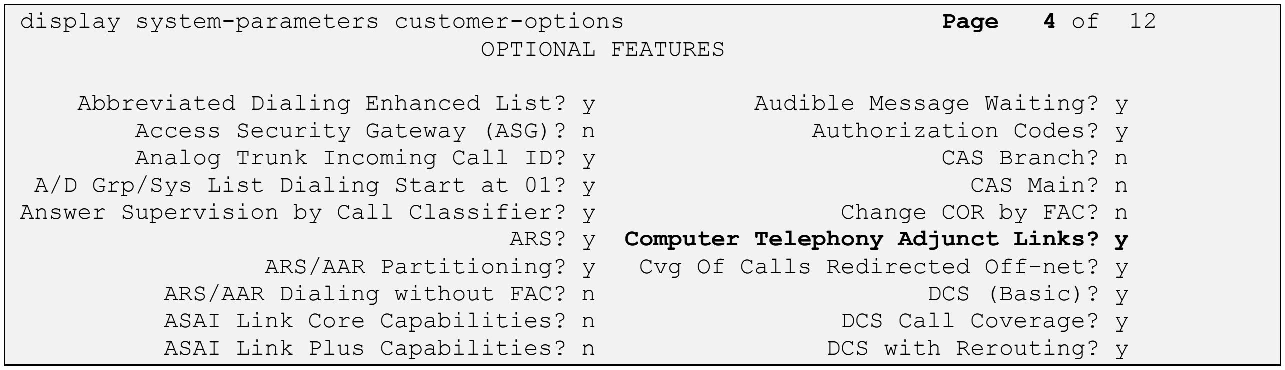
5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Obtain reason codes
- Administer Signaling group for SIP trunk to Session Manager
- Administer Avaya SIP deskphone.

5.1. Verify License

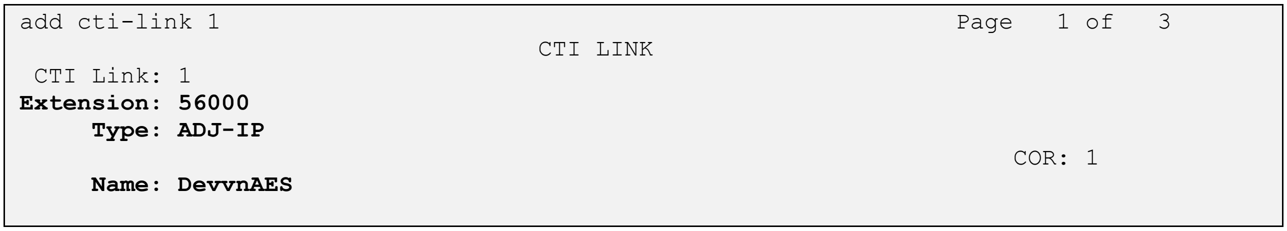
Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Computer Telephony Adjunct Links** customer option is set 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

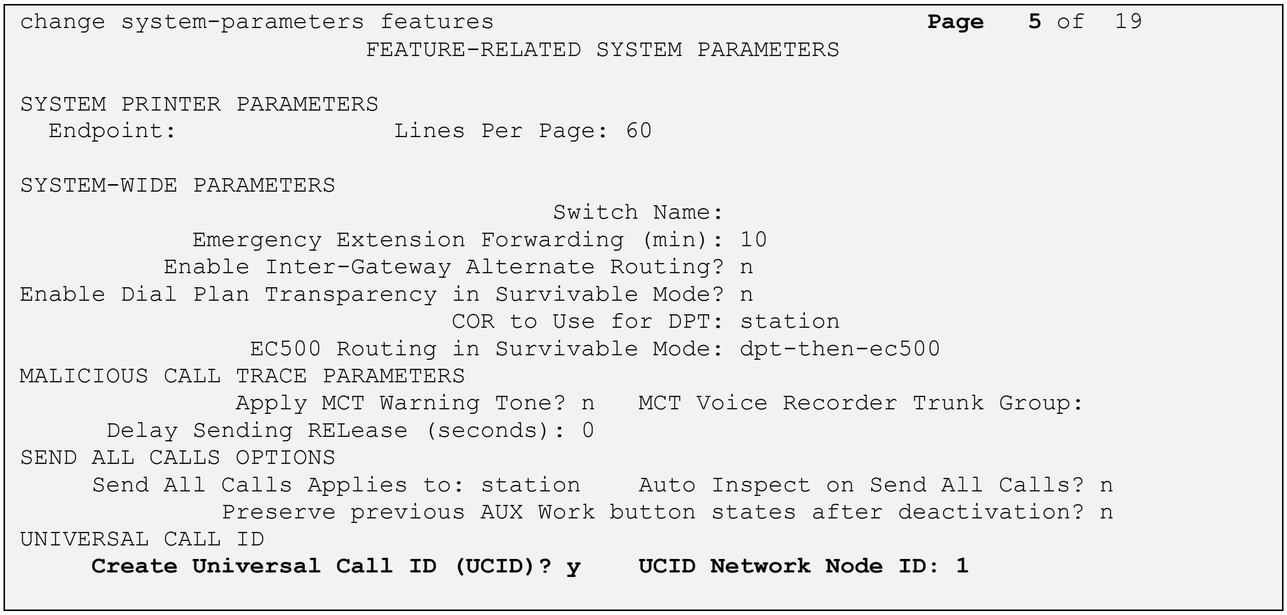
Add a CTI link using the "add cti-link n" command, where "n" is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter "ADJ-IP" in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.



```
add cti-link 1                                                   Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 56000
     Type: ADJ-IP
                                                                     COR: 1

     Name: DevvnAES
```

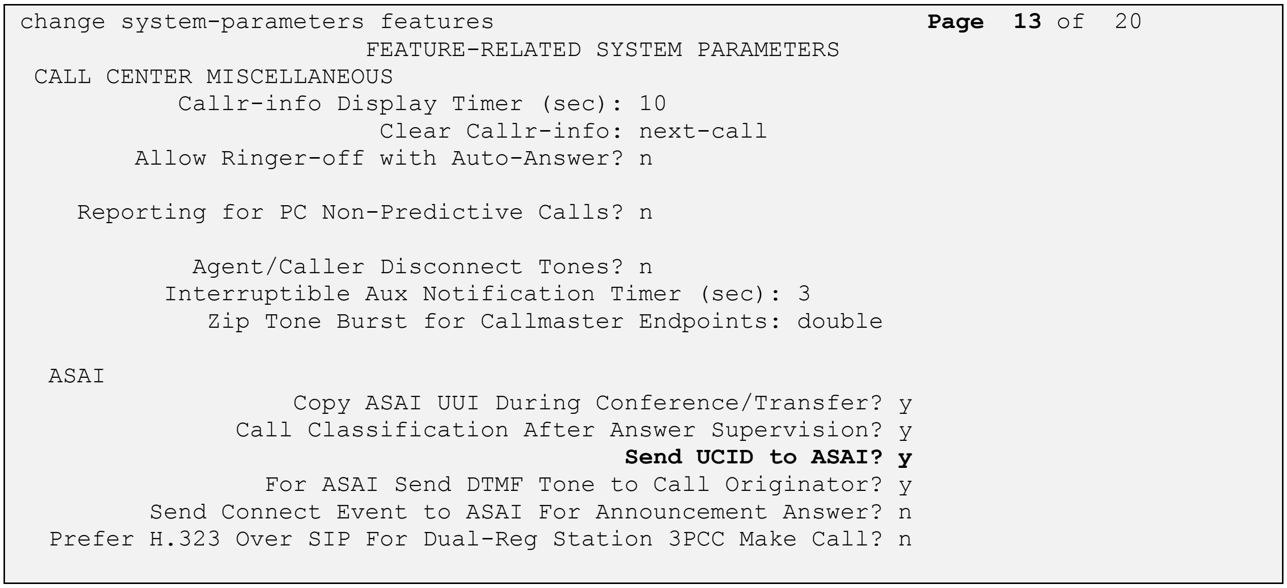
5.3. Administer System Parameters Features

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
```

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



```
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. Obtain VDN

Use the “list vdn” command to display a list of pre-configured VDNs. Make a note of the **Name** for each VDNs from **Section 3**, which will be used later to configure CT Suite. In the compliance testing, the two VDNs shown below were used.

```
list vdn
                          VECTOR DIRECTORY NUMBERS
                                                                       Evnt
                                      VDN         Vec           Orig   Noti
Name (22 characters)   Ext/Skills     Ovr COR TN  PRT Num  Meas Annc   Adj

Basic                  56001           n  1   1    V  1    int
ForSkill3              56010           n  1   1    V  10   int
```

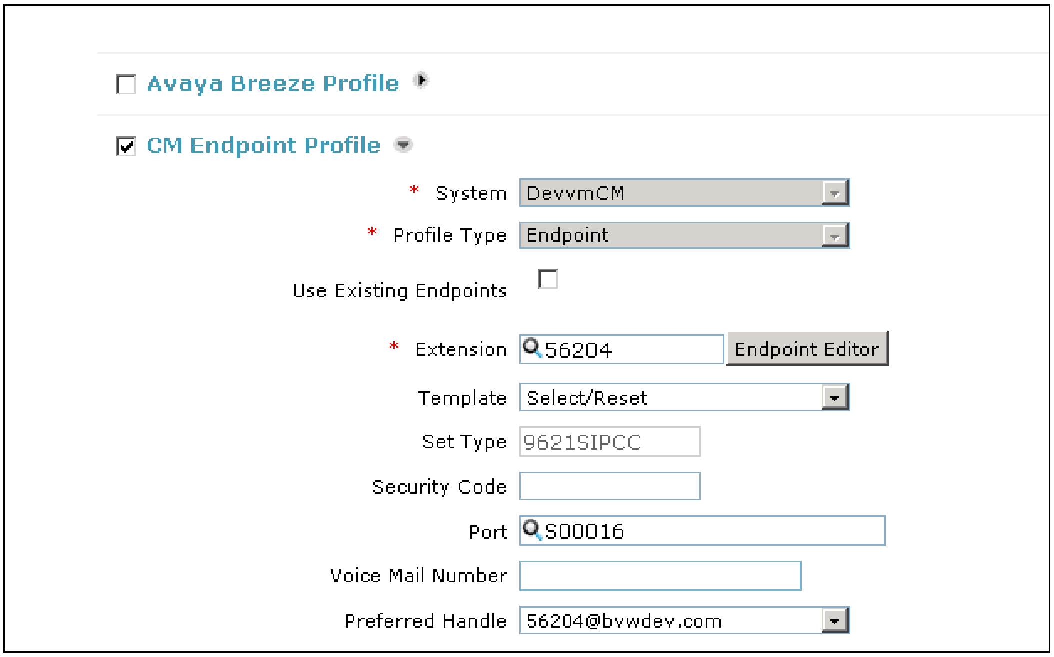
5.5. Obtain Reason Codes

For contact centers that use reason codes, enter the “change reason-code-names” command to display the configured reason codes. Make a note of the reason codes, which will be used later to configure CT Suite.

```
change reason-code-names                                        Page   1 of   1
                                REASON CODE NAMES
                           Aux Work/            Logout
                        Interruptible?

        Reason Code 1: Lunch           /n  Finished Shift
        Reason Code 2: Coffee          /n
        Reason Code 3:                 /n
        Reason Code 4:                 /n
        Reason Code 5:                 /n
        Reason Code 6:                 /n
        Reason Code 7:                 /n
        Reason Code 8:                 /n
        Reason Code 9:                 /n

  Default Reason Code:
```

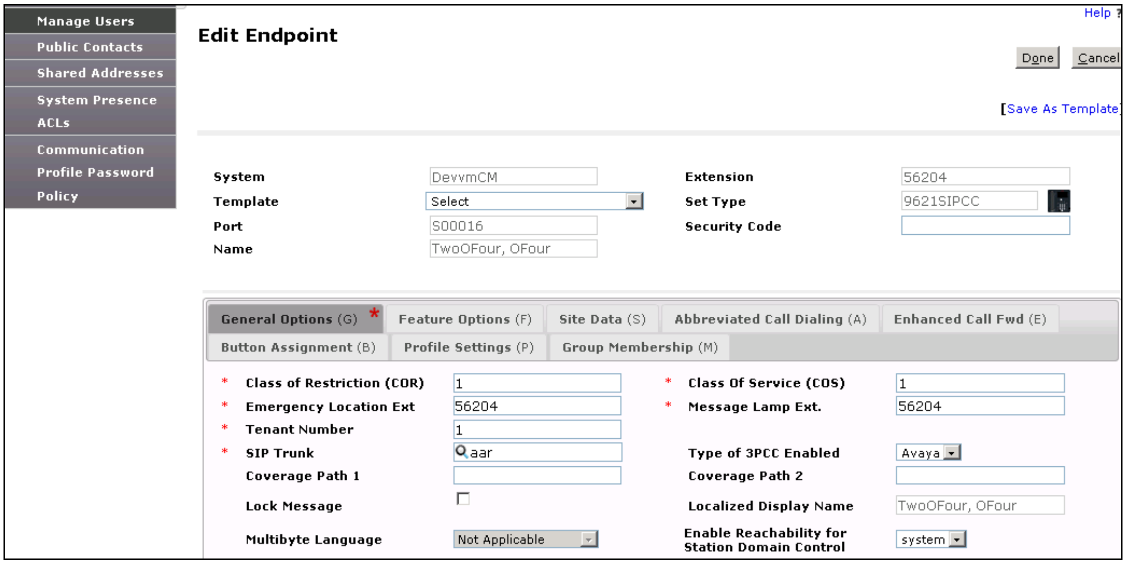
6. Configure Avaya Aura® System Manager

It is assume that SIP user already existed with TLS connection to Session Manager. This section describes steps to set Third Party Control for existing SIP endpoints. On System Manager, select **Users → User Management** (not shown), select existing SIP user, and click on **Endpoint Editor** button shown below:



* System	DevvmCM
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	56204
Template	Select/Reset
Set Type	9621SIPCC
Security Code	
Port	S00016
Voice Mail Number	
Preferred Handle	56204@bvwdev.com

In the **Edit Endpoint** page set **Type of 3PCC Enabled** to “Avaya”, click **Done** and **Commit** (not shown) to save changes.



Edit Endpoint

System	DevvmCM	Extension	56204
Template	Select	Set Type	9621SIPCC
Port	S00016	Security Code	
Name	TwoOFour, OFour		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	56204	* Message Lamp Ext.	56204
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	TwoOFour, OFour
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

7. Configure Avaya Aura® Application Enablement Services

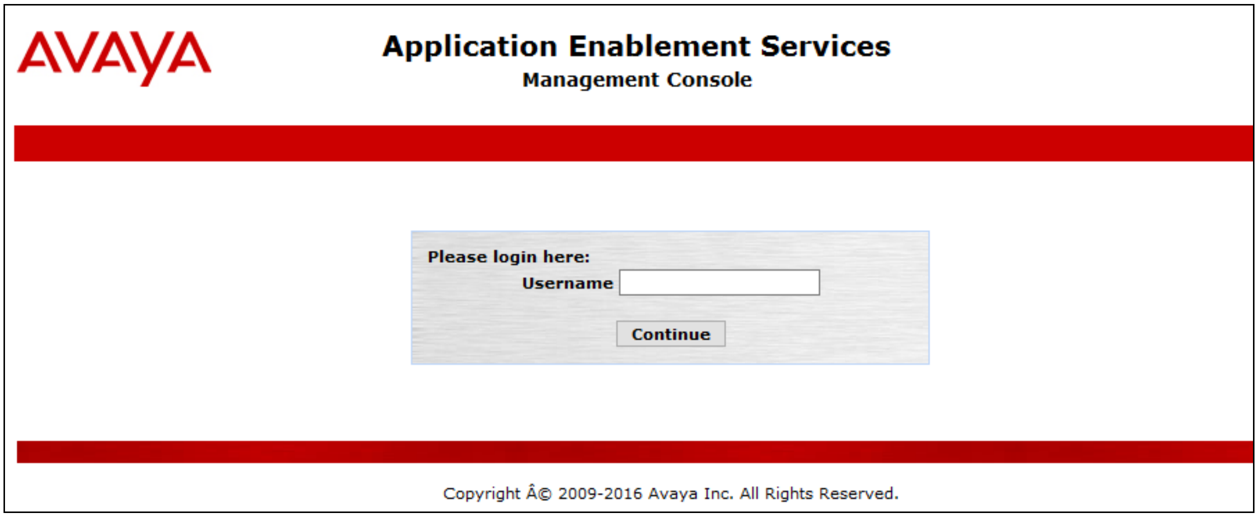
This section provides the procedures for configuring Application Enablement Services. Screenshots for configuration in this section were captured after compliance test for references therefore they are in modify mode instead of create new screen. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer CTIntegrations user
- Disable security database
- Administer ports
- Obtain Tlink information
- Restart services

7.1. 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.

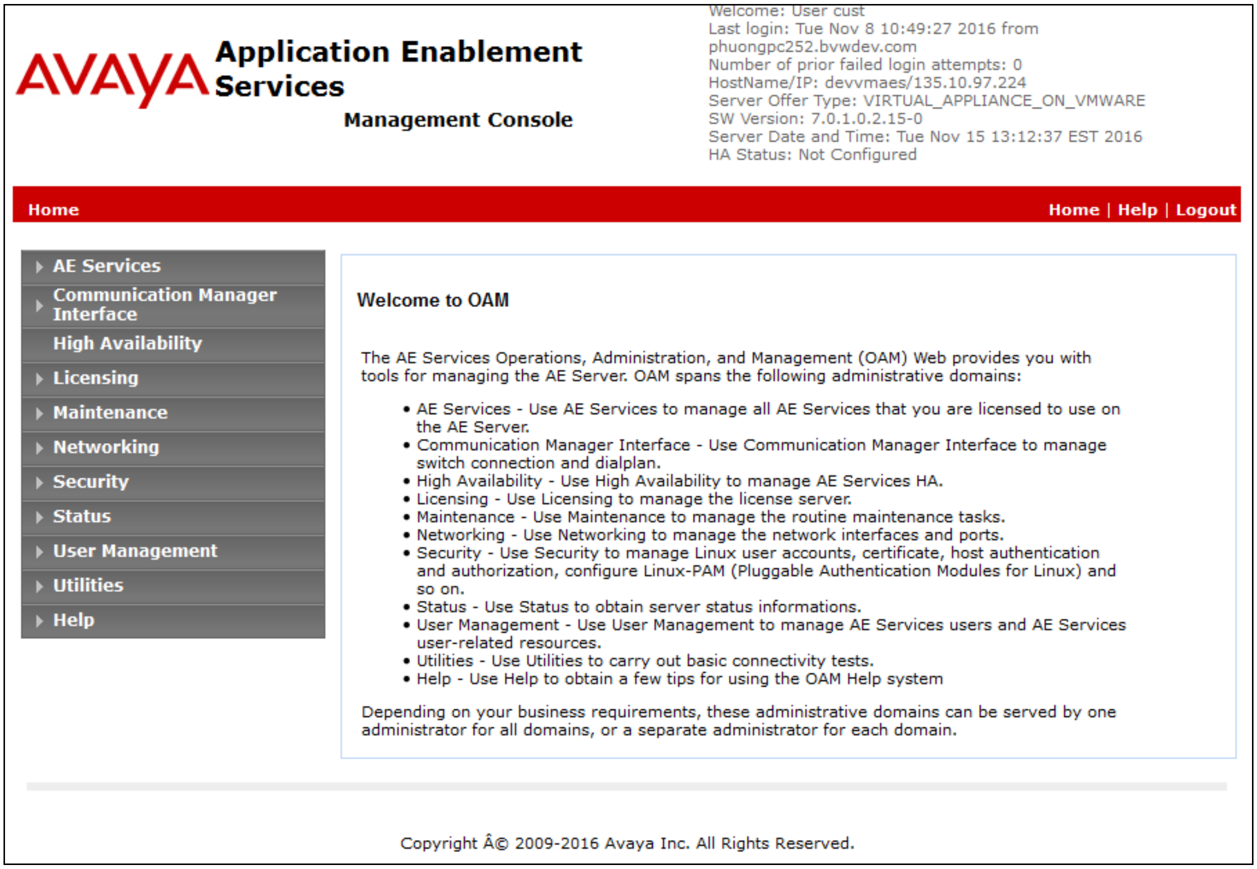


Application Enablement Services
Management Console

Please login here:
Username

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

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



Welcome: User cust
Last login: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwdev.com
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 13:12:37 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:

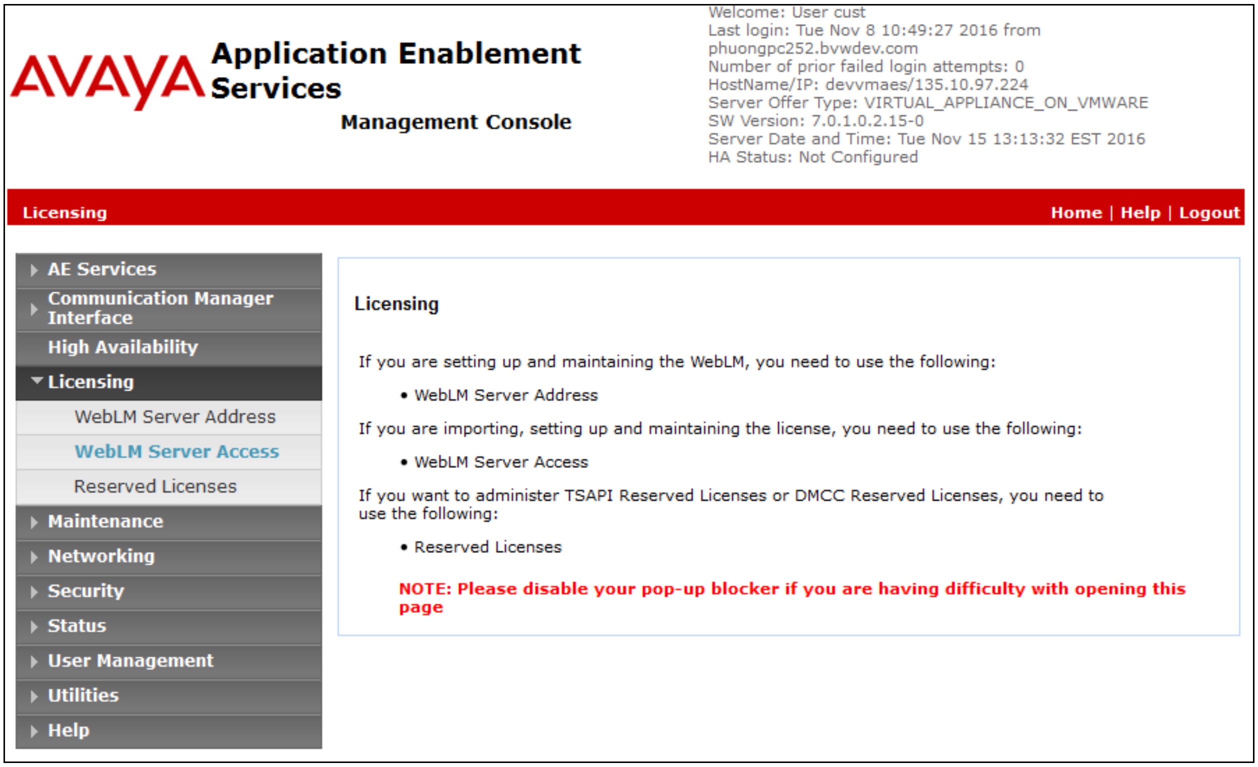
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing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

7.2. 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: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwdev.com
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 13:13:32 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

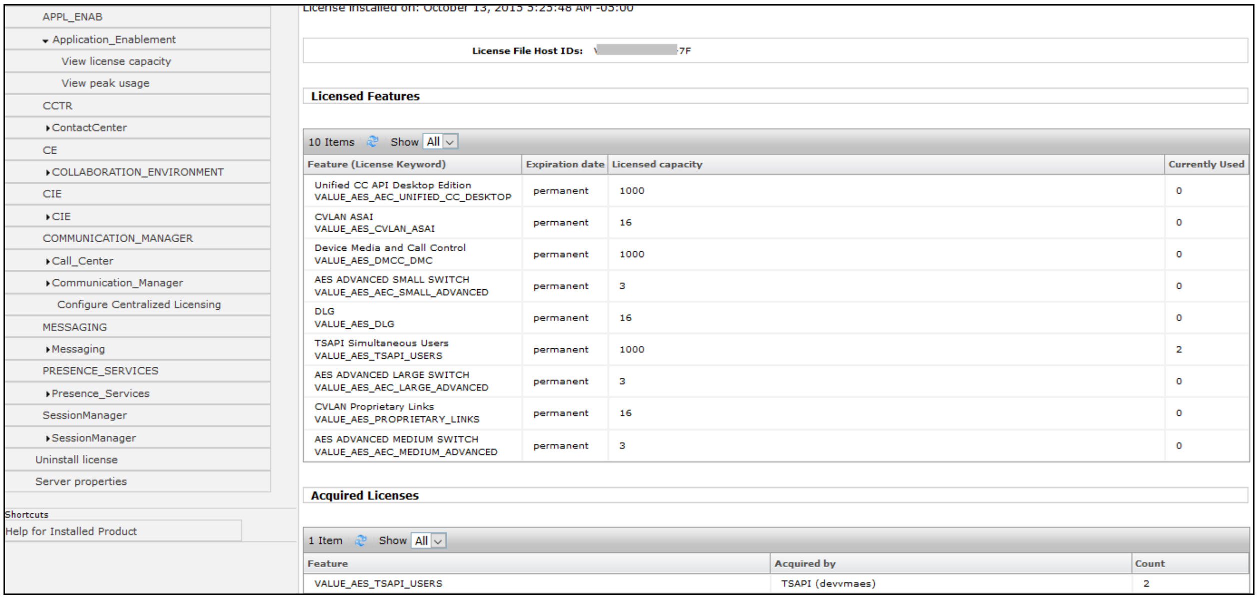
If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- 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. Note that the TSAPI license is used for device monitoring and call control via DMCC, and that no specific DMCC license is required for integration with CT Suite.



License installed on: October 13, 2015 5:23:48 AM -05:00

License File Host IDs: V[redacted]7F

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000	0
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16	0
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000	0
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3	0
DLG VALUE_AES_DLG	permanent	16	0
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000	2
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3	0
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16	0
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3	0

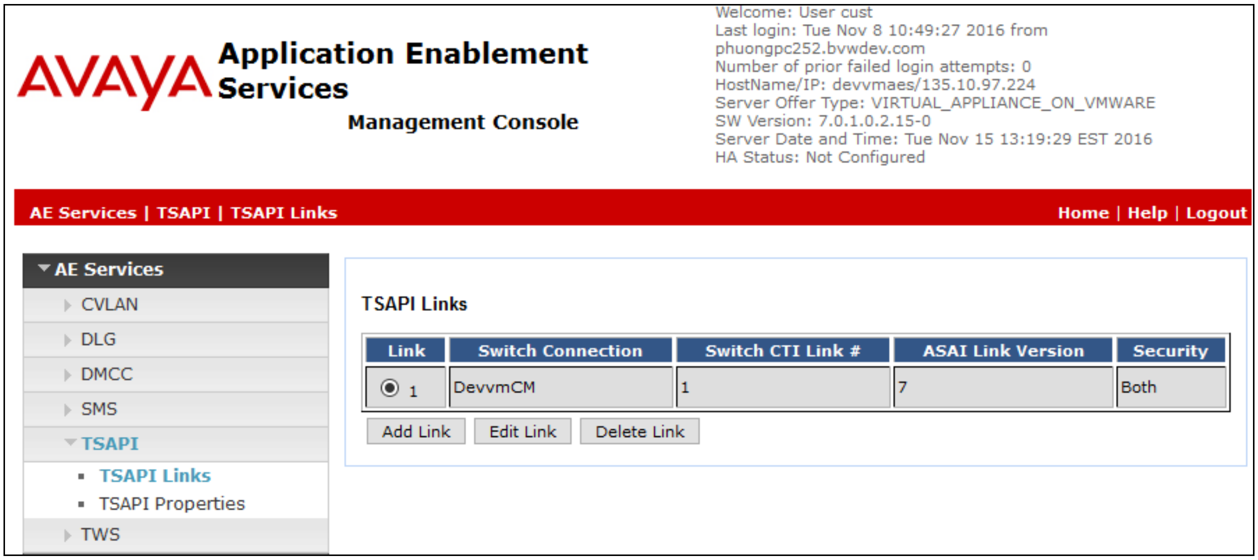
Acquired Licenses

1 Item Show All

Feature	Acquired by	Count
VALUE_AES_TSAPI_USERS	TSAPI (devvmaes)	2

7.3. Administer TSAPI Link

Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link** to create new Link.



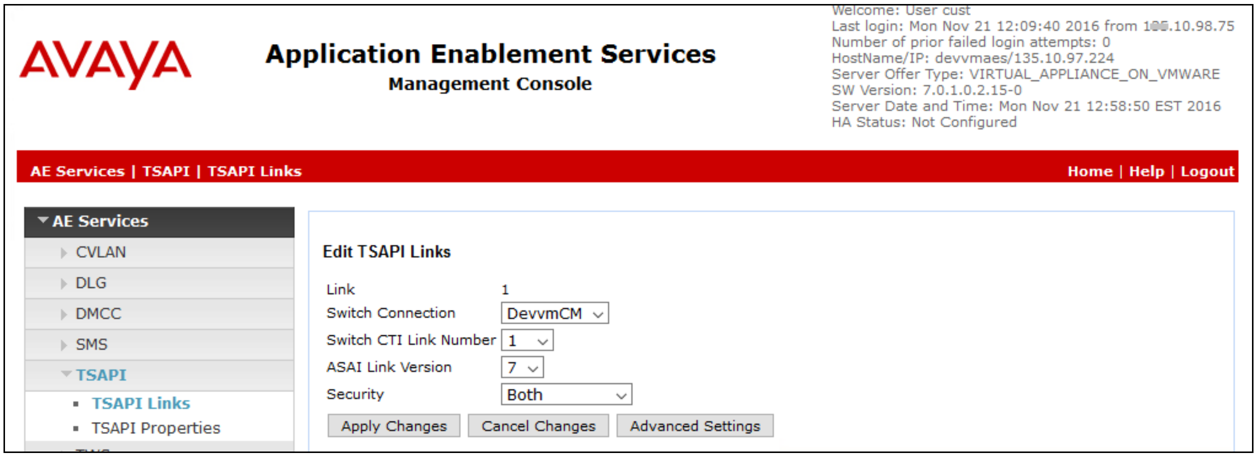
Welcome: User cust
Last login: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwdev.com
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 13:19:29 EST 2016
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
◉ 1	DevvmCM	1	7	Both

The **Add TSAPI Links** screen is displayed next (not shown), below is example of link created during compliance test.

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 "DevvmCM" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Select "7" for **ASAI Link Version** and select "Both" for **Security**.



Welcome: User cust
Last login: Mon Nov 21 12:09:40 2016 from 1[redacted].10.98.75
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Mon Nov 21 12:58:50 EST 2016
HA Status: Not Configured

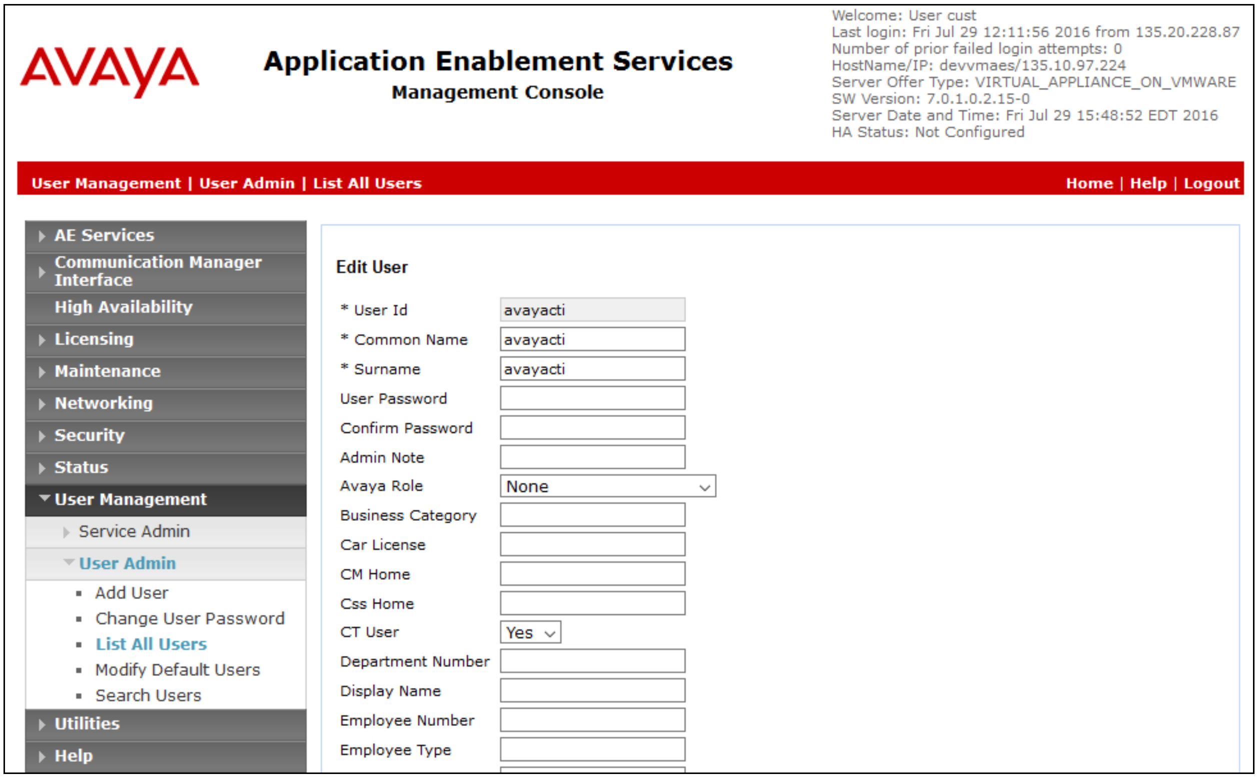
Edit TSAPI Links

Link	1
Switch Connection	DevvmCM
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

7.4. Administer CTIntegrations 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.



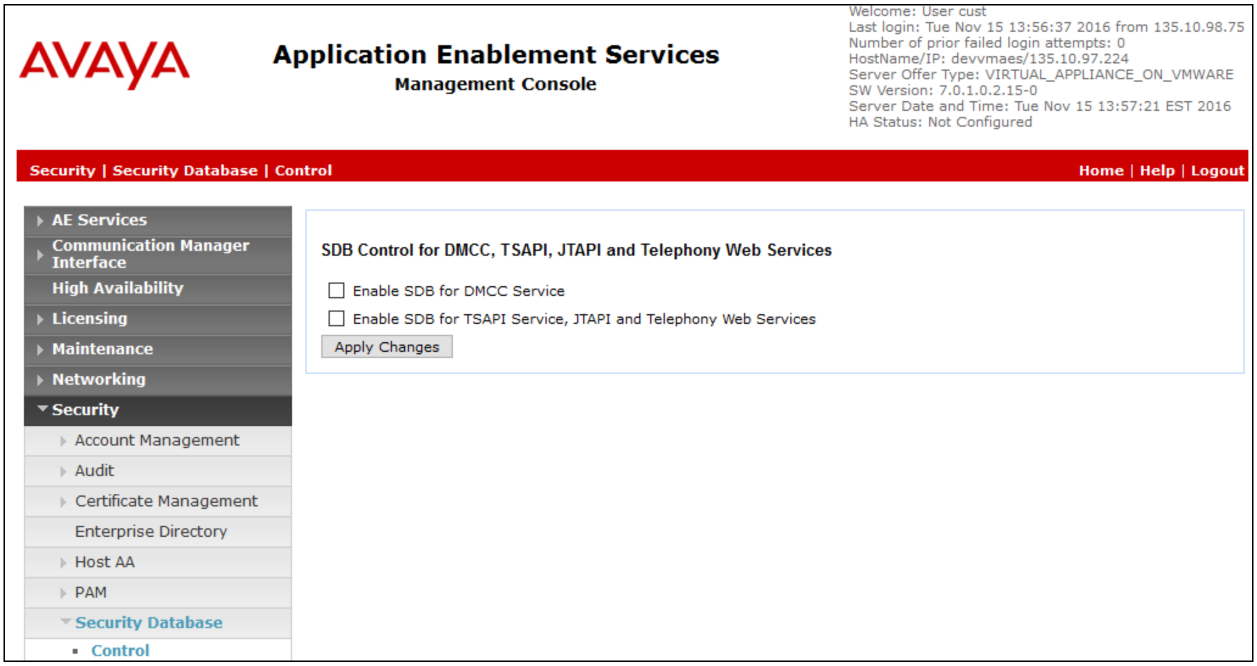
Welcome: User cust
Last login: Fri Jul 29 12:11:56 2016 from 135.20.228.87
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Fri Jul 29 15:48:52 EDT 2016
HA Status: Not Configured

Edit User

* User Id	avayacti
* Common Name	avayacti
* Surname	avayacti
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	

7.5. Disable 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 as shown below.



Welcome: User cust
Last login: Tue Nov 15 13:56:37 2016 from 135.10.98.75
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 13:57:21 EST 2016
HA Status: Not Configured

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

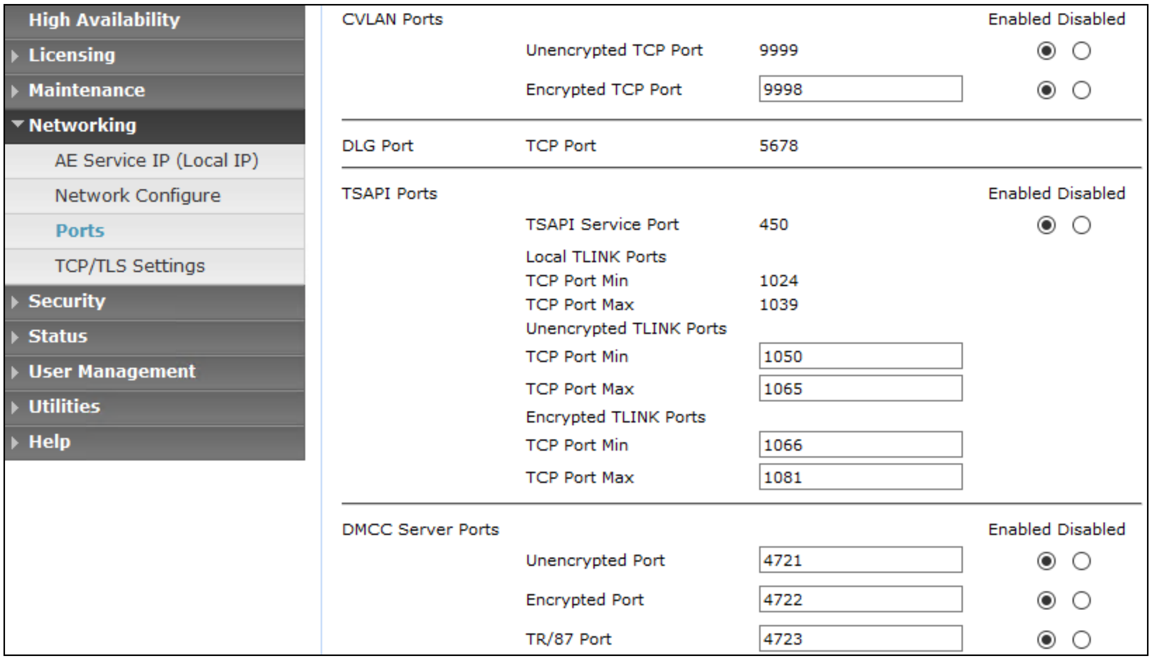
☐ Enable SDB for DMCC Service

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

7.6. Administer Ports

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

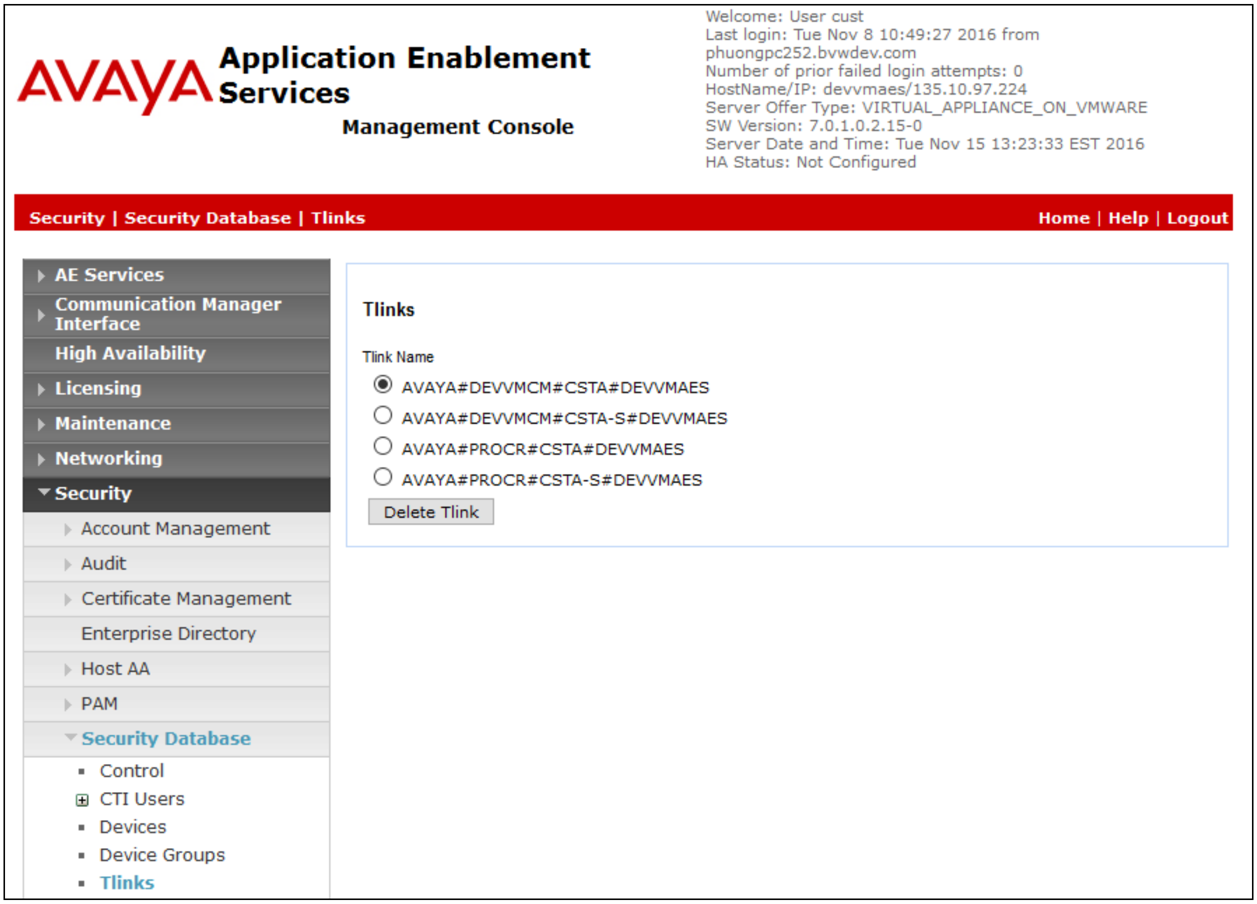
In the **DMCC Ports** section, verify the radio button for **DMCC Server Ports** under the **Enabled** column is checked as shown below. Retain the default values in the remaining fields.



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	●	○

7.7. Obtain Tlink Information

Navigate to **Security → Security Database → Tlinks**. Verify Tlink name, this name is needed to configure CT Suite in **Section 8.1**. Note that the selected Tlink name needs to match the switch connection name used in **Section 7.3**, in this case “DEVVMCM”, as shown below.



Welcome: User cust
Last login: Tue Nov 8 10:49:27 2016 from phuongpc252.bvwdev.com
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Nov 15 13:23:33 EST 2016
HA Status: Not Configured

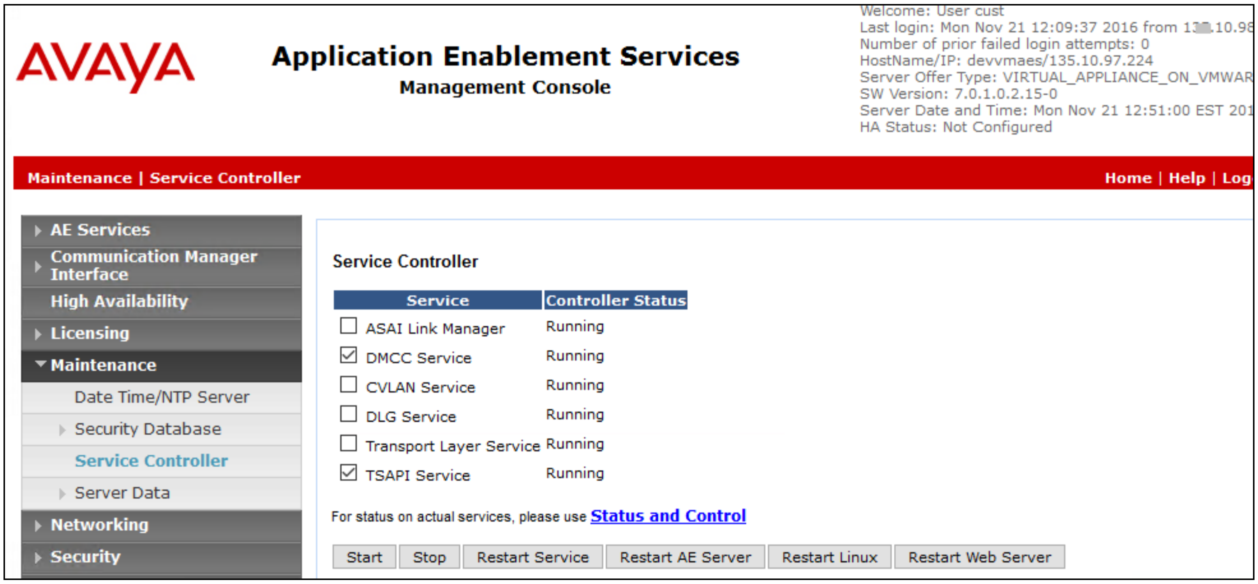
Tlinks

Tlink Name

● AVAYA#DEVVMCM#CSTA#DEVVMAES
○ AVAYA#DEVVMCM#CSTA-S#DEVVMAES
○ AVAYA#PROCR#CSTA#DEVVMAES
○ AVAYA#PROCR#CSTA-S#DEVVMAES

7.8. Restart Services

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and click **Restart Service**.



Welcome: User cust
Last login: Mon Nov 21 12:09:37 2016 from 1[redacted].10.98
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWAR
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Mon Nov 21 12:51:00 EST 201
HA Status: Not Configured

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

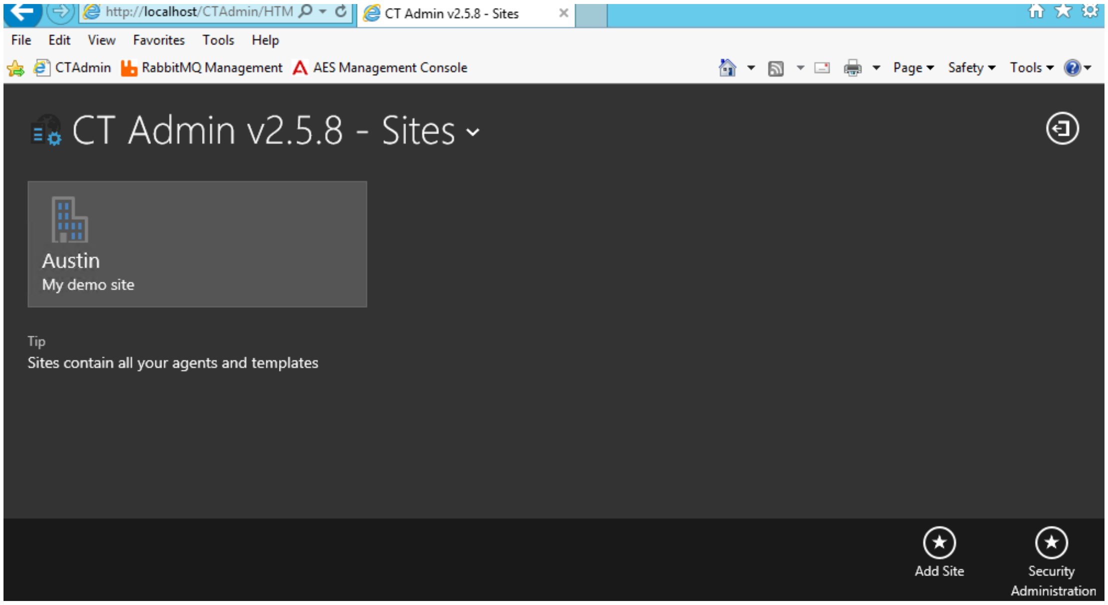
8. Configure CTIntegrations CT Suite

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

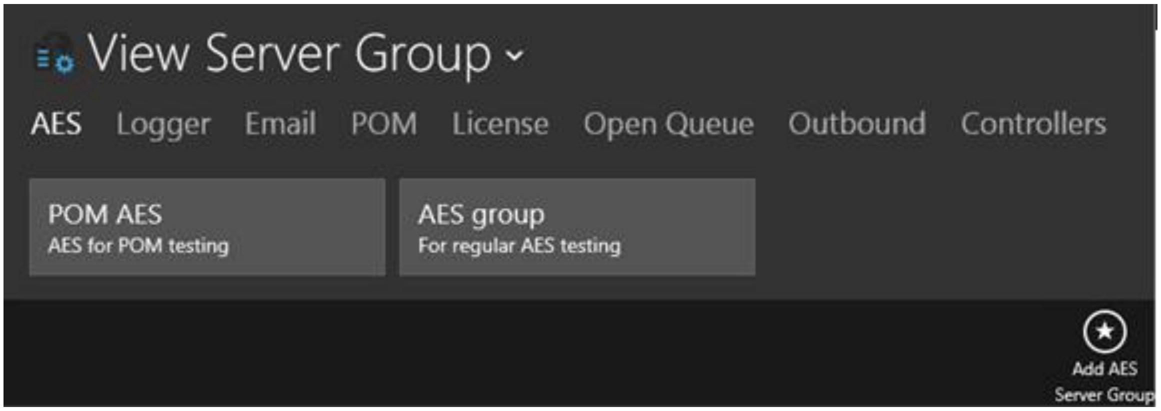
- Configure AES server
- Configure CT Desktop agent account

8.1. Configure AES Server

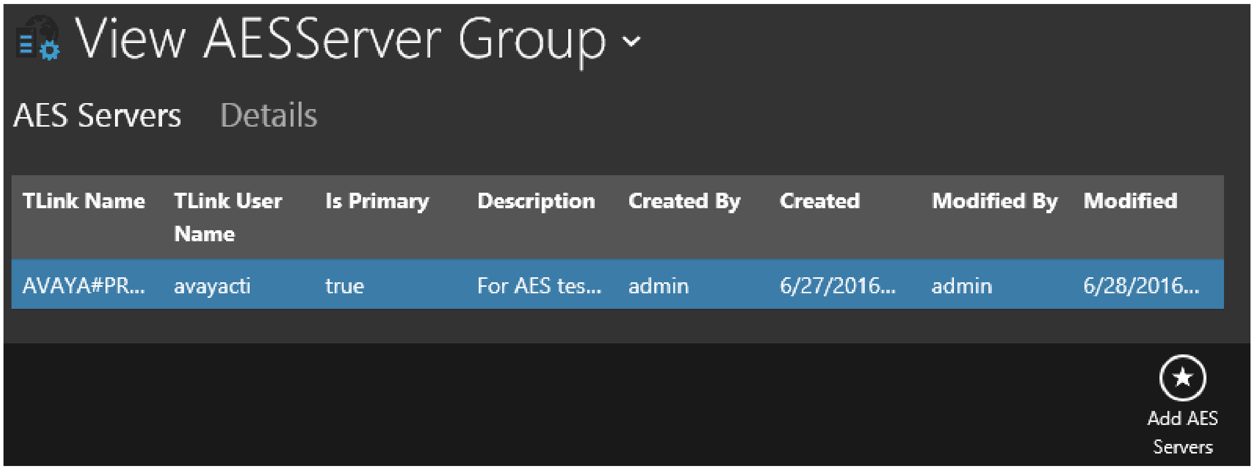
Open a browser and navigate to: http://[ctadmin_server/]/CTAdmin, where [ctadmin_server] is the IP address of CT Suite server, login with proper administrator credentials (not shown). The CT Admin home page is displayed as shown below:



Navigate to **Austin My Demo site** → **Servers** (not shown), there are 2 available groups **POM AES** and **AES group**.



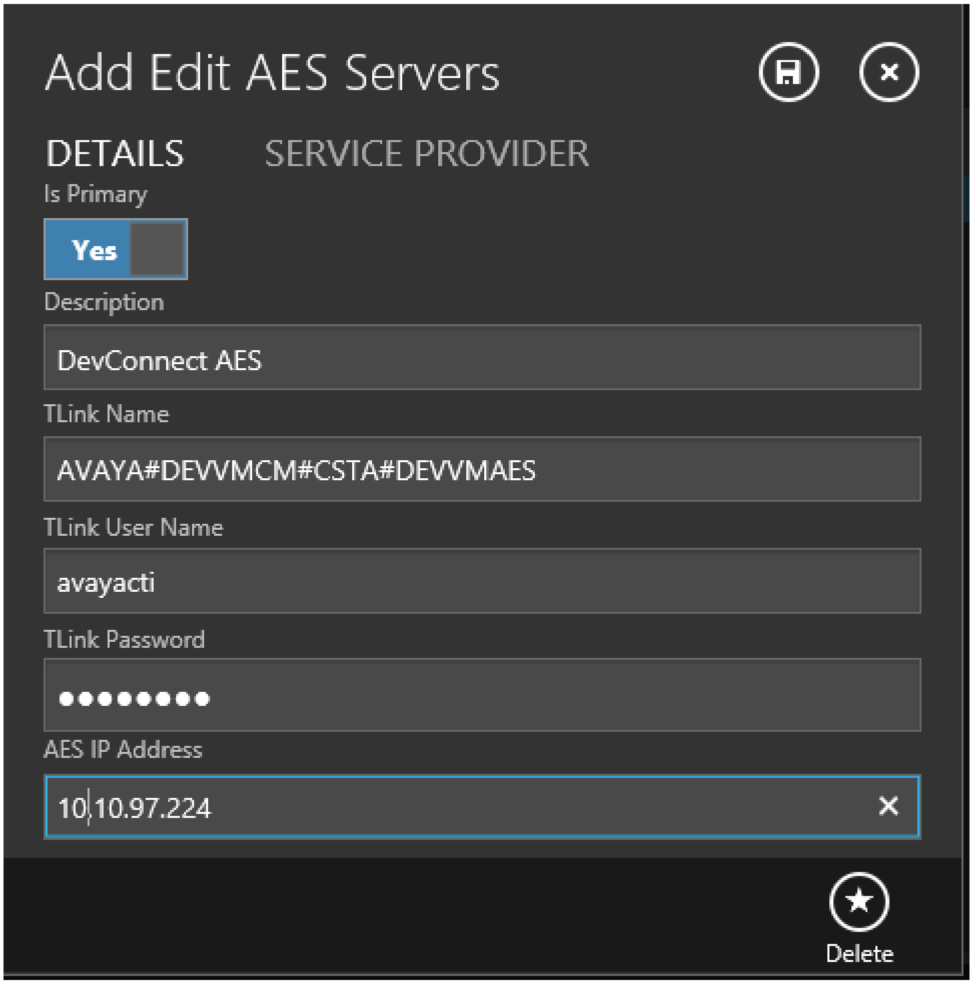
Click on **AES group**, in the **View AESServer Group** page, select an existing AES server entry to view its detail or click **Add AES Servers** to add a new AES server.



TLink Name	TLink User Name	Is Primary	Description	Created By	Created	Modified By	Modified
AVAYA#PR...	avayacti	true	For AES tes...	admin	6/27/2016...	admin	6/28/2016...

Following are details of the **Add Edit AES Servers** settings used in compliance test:

- **Is Primary**: Select **Yes**.
- **Description**: Enter a desired description.
- **TLink Name**: Enter TLink name in **Section 7.7**.
- **TLink User Name**: Enter user name created in **Section 7.4**.
- **TLink Password**: Enter password for username created in **Section 7.4**.
- **AES IP Address**: Enter IP address of Application Enablement Services.



Add Edit AES Servers

Is Primary: Yes

Description: DevConnect AES

TLink Name: AVAYA#DEVVMCM#CSTA#DEVVMAES

TLink User Name: avayacti

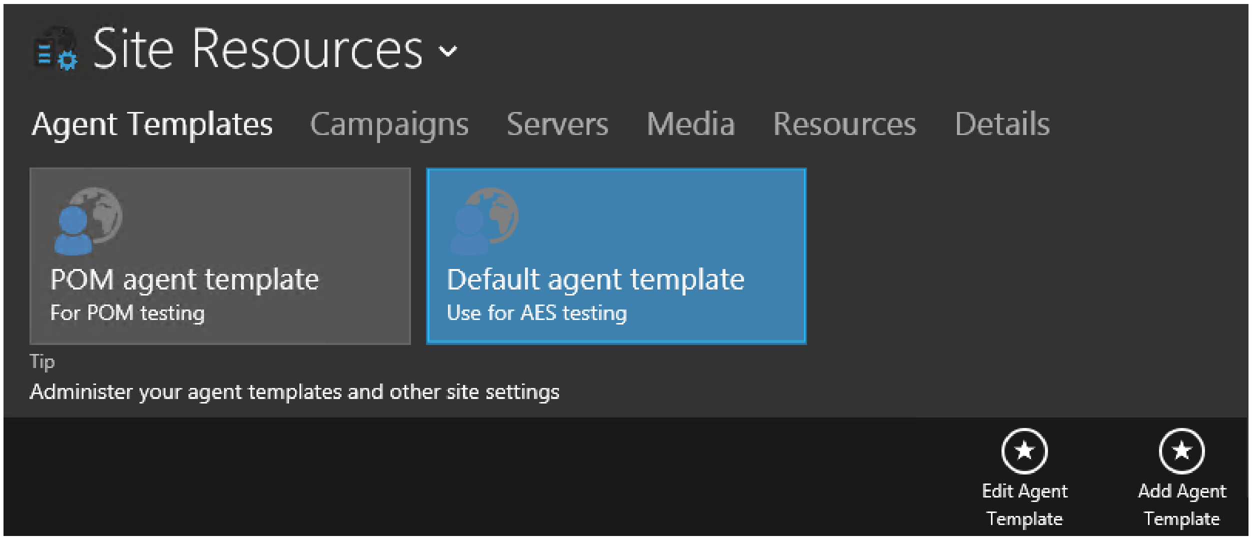
TLink Password: ●●●●●●●●

AES IP Address: 10.10.97.224

8.2. Configure CT Desktop Agent Account

Note: Further agent configuration details are available in the CT Suite Administration Guide in **Section 10**.

Click on the globe icon on the top left of the page to go to the home page. On the **CT Admin** home page, navigate to **Austin (Site) → Agent Templates** and click on **Default agent template**.

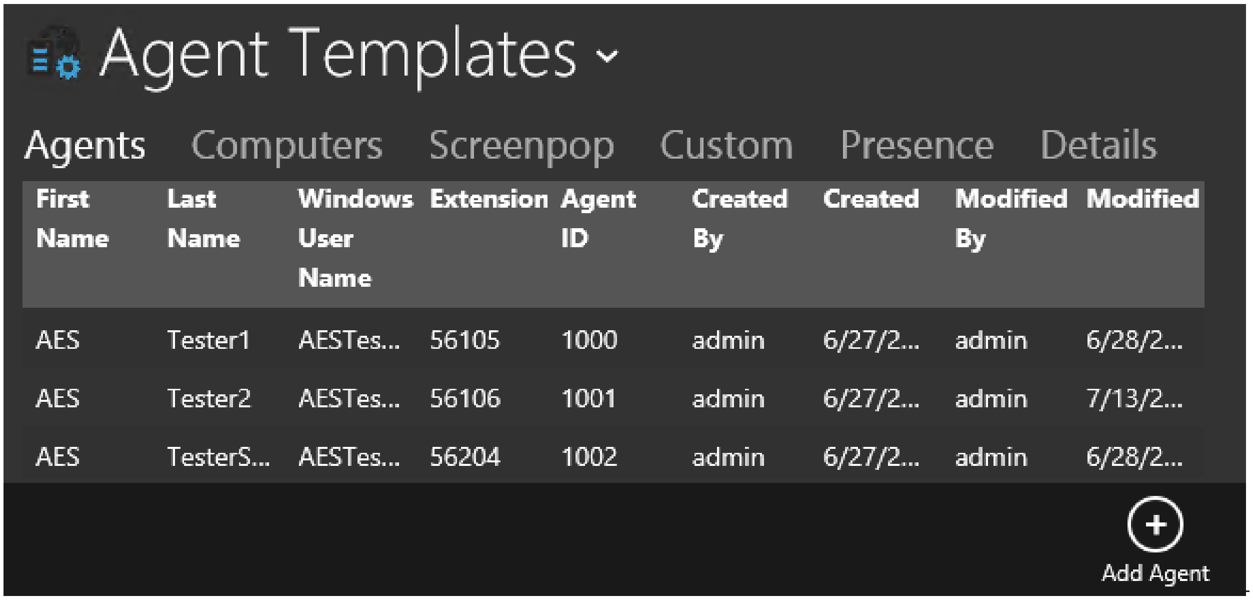


POM agent template
For POM testing

Default agent template
Use for AES testing

Tip
Administer your agent templates and other site settings

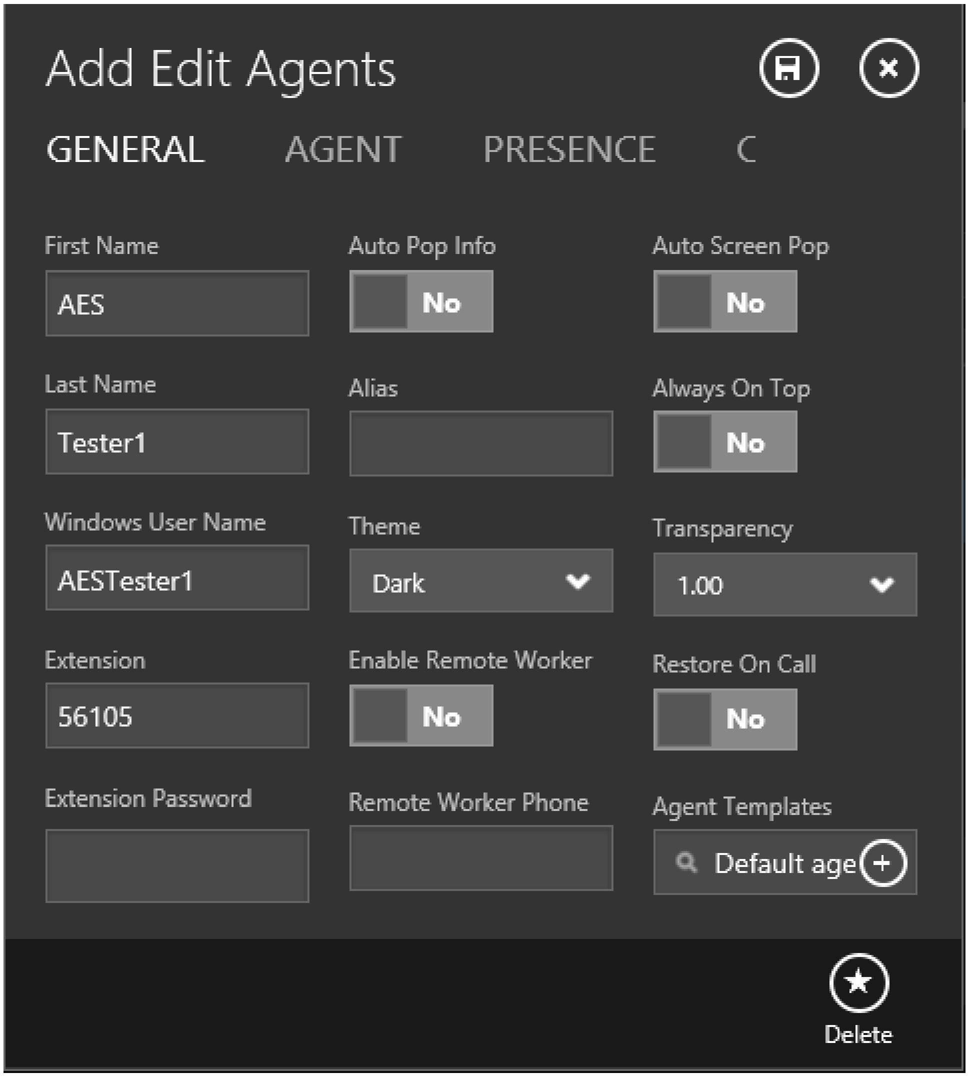
The list of agent used in the compliance testing is shown below. To add an agent, click on the **Add Agent** button.



First Name	Last Name	Windows User Name	Extension	Agent ID	Created By	Created	Modified By	Modified
AES	Tester1	AESTes...	56105	1000	admin	6/27/2...	admin	6/28/2...
AES	Tester2	AESTes...	56106	1001	admin	6/27/2...	admin	7/13/2...
AES	TesterS...	AESTes...	56204	1002	admin	6/27/2...	admin	6/28/2...

In the **Add Edit Agent** screen, select the **GENERAL** tab, and enter the following information:

- **First Name**: Enter any descriptive name.
- **Last Name**: Enter any descriptive name.
- **Window User Name**: Enter the Window user name for the agent, this user name is used to login CT Desktop from the agent desktop. In this example it is "AESTester1".
- **Extension**: Enter the corresponding agent station extension as listed in **Section 3**.



Add Edit Agents

GENERAL AGENT PRESENCE C

First Name: AES

Auto Pop Info: No

Auto Screen Pop: No

Last Name: Tester1

Alias:

Always On Top: No

Windows User Name: AESTester1

Theme: Dark

Transparency: 1.00

Extension: 56105

Enable Remote Worker: No

Restore On Call: No

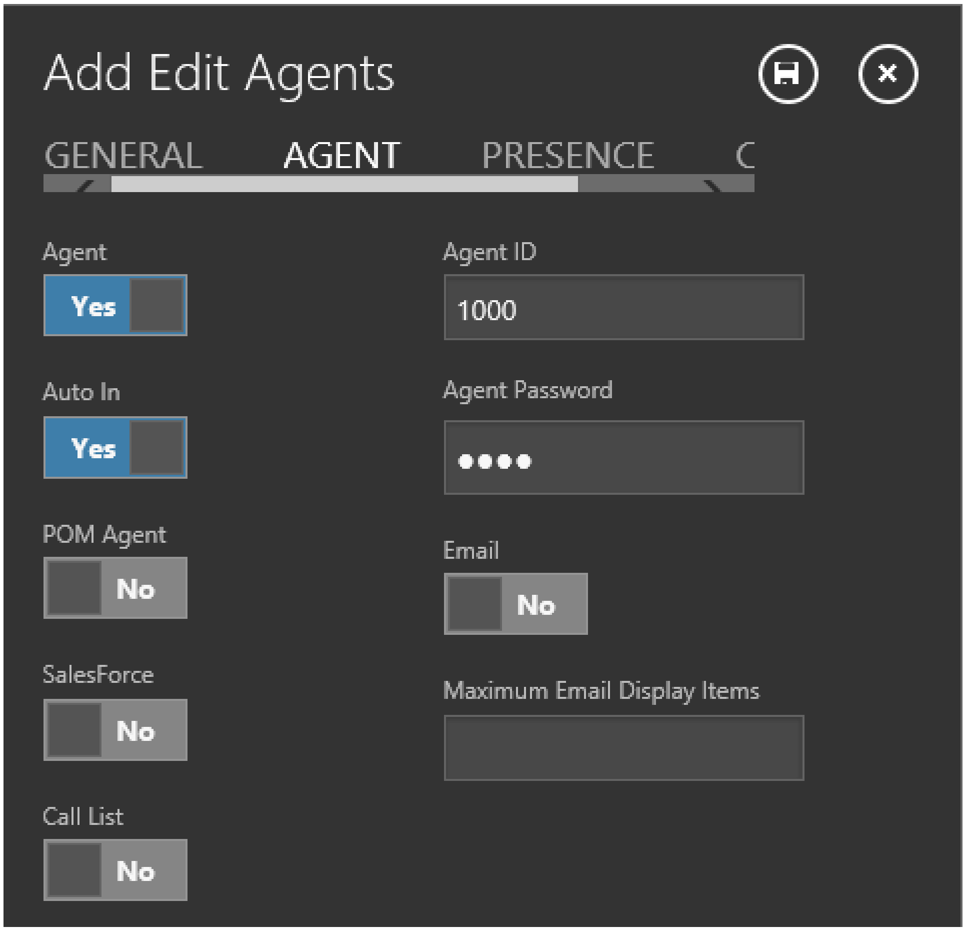
Extension Password:

Remote Worker Phone:

Agent Templates: Default age

Select the **AGENT** tab, and enter the following information:

- **Agent**: Select **Yes**.
- **Auto In**: Select **Yes**.
- **Agent ID**: Enter the corresponding Agent ID as listed in **Section 3**.
- **Agent Password**: Enter Agent Password as listed in Section **3**.



Add Edit Agents

Agent: Yes

Agent ID: 1000

Auto In: Yes

Agent Password: ●●●●

POM Agent: No

Email: No

SalesForce: No

Maximum Email Display Items:

Call List: No

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

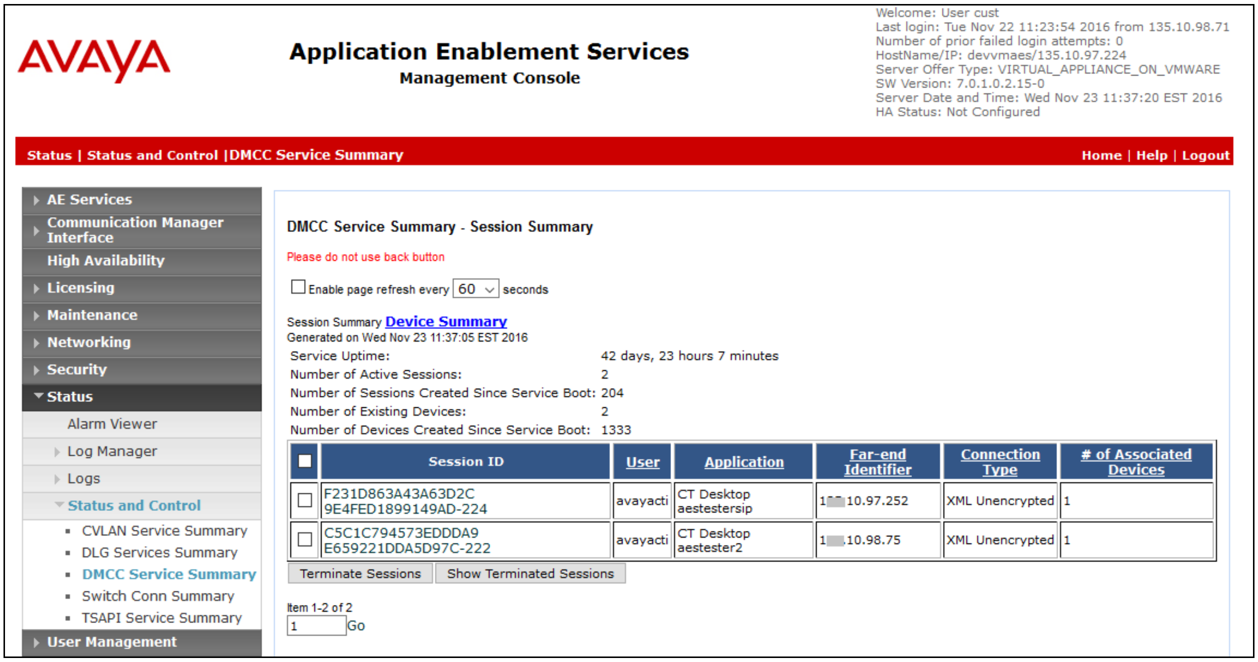
On Communication Manager, verify the status of the administered CTI link by using the "status aesvcs cti-link" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**, as shown below.

```
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    devvmaes         established   28       24
```

9.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **User** column shows active sessions with the CT Desktop Windows User Name from **Section 8.2**.



Welcome: User cust
Last login: Tue Nov 22 11:23:54 2016 from 135.10.98.71
Number of prior failed login attempts: 0
HostName/IP: devvmaes/135.10.97.224
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Wed Nov 23 11:37:20 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 Wed Nov 23 11:37:05 EST 2016

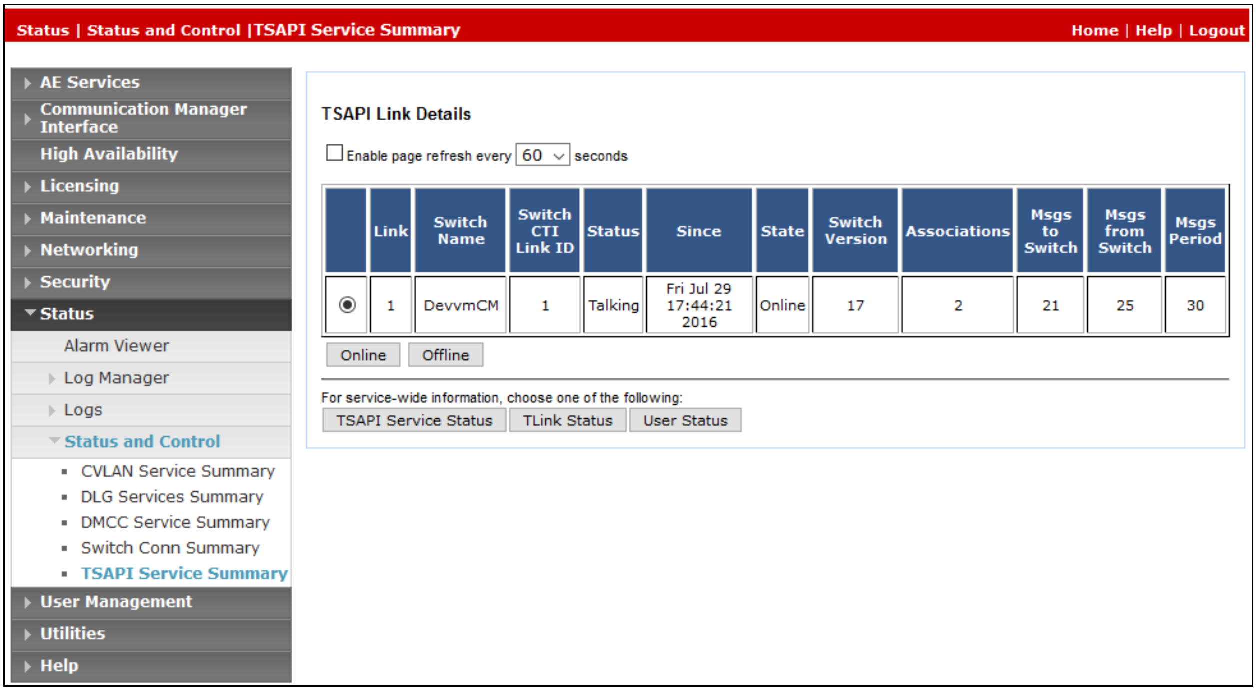
Service Uptime:	42 days, 23 hours 7 minutes
Number of Active Sessions:	2
Number of Sessions Created Since Service Boot:	204
Number of Existing Devices:	2
Number of Devices Created Since Service Boot:	1333

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	F231D863A43A63D2C 9E4FED1899149AD-224	avayacti	CT Desktop aestestersip	1[redacted]10.97.252	XML Unencrypted	1
□	C5C1C794573EDDDA9 E659221DDA5D97C-222	avayacti	CT Desktop aestester2	1[redacted].10.98.75	XML Unencrypted	1

Item 1-2 of 2
1

Verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is "Talking" for the TSAPI link administered in **Section 5.2** and that the **Associations** column reflects the number of agents from **Section 3** that are currently logged into CT Desktop and therefore monitored, in this case "2".



TSAPI Link Details

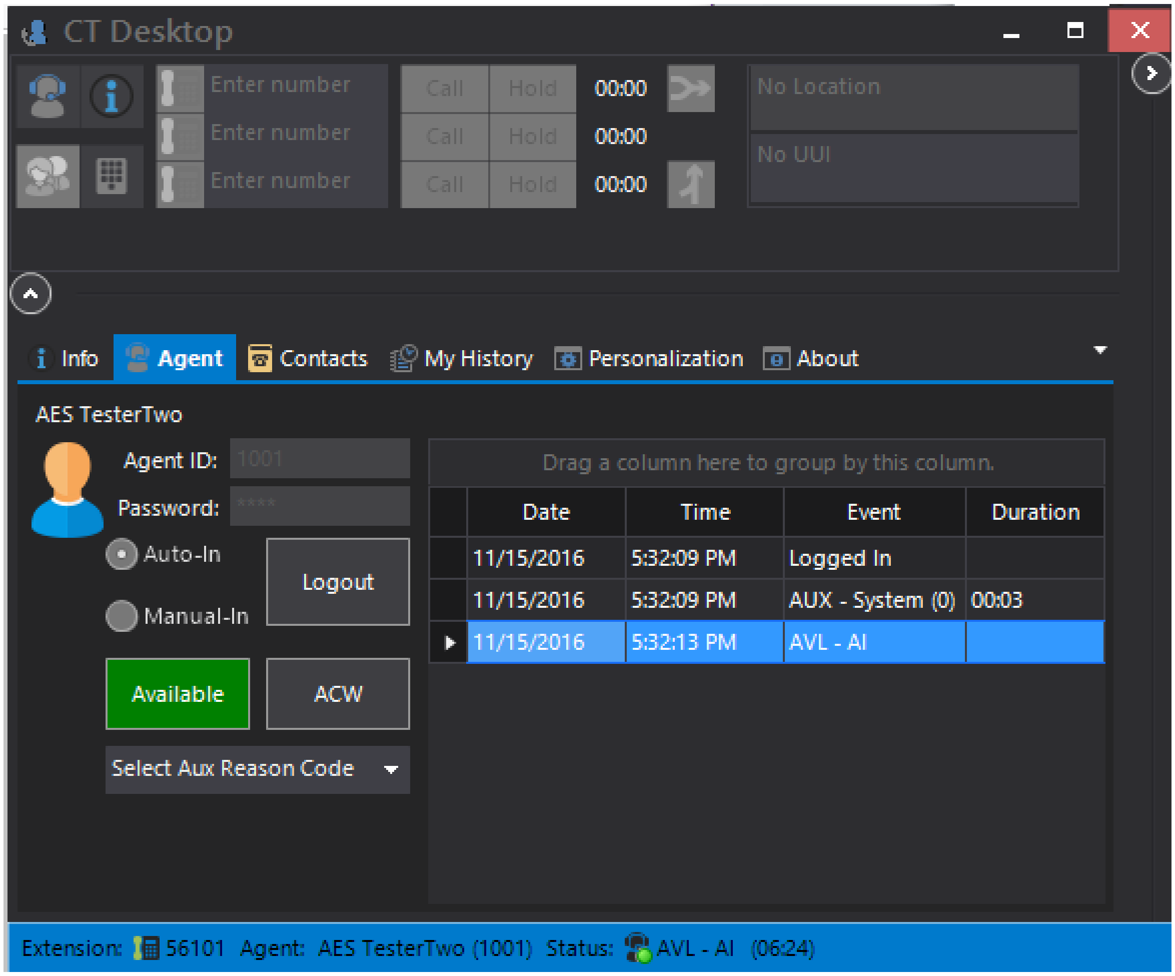
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	DevvmCM	1	Talking	Fri Jul 29 17:44:21 2016	Online	17	2	21	25	30

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

9.3. Verify CTIntegrations CT Suite

From the agent PC, launch the CT Desktop application via **Start → CTIntegrations → CTSuite → CT Desktop**, once started the CT Desktop application will connect to the CT Suite server passing agent desktop Windows user name, in this case it is **AES TesterTwo** as configured in **Section 8.2**. CT Suite then monitors the agent deskphone in this case it is **56101** as configured in **Section 8.2**, click on **Login** button (not shown). Change agent status to available for incoming ACD call by click on the **Available** button. Agent successfully logged in and is available as displayed in the CT Desktop application status bar in the bottom of the screen.



00:00
00:00
00:00

No Location
No UUI

AES TesterTwo

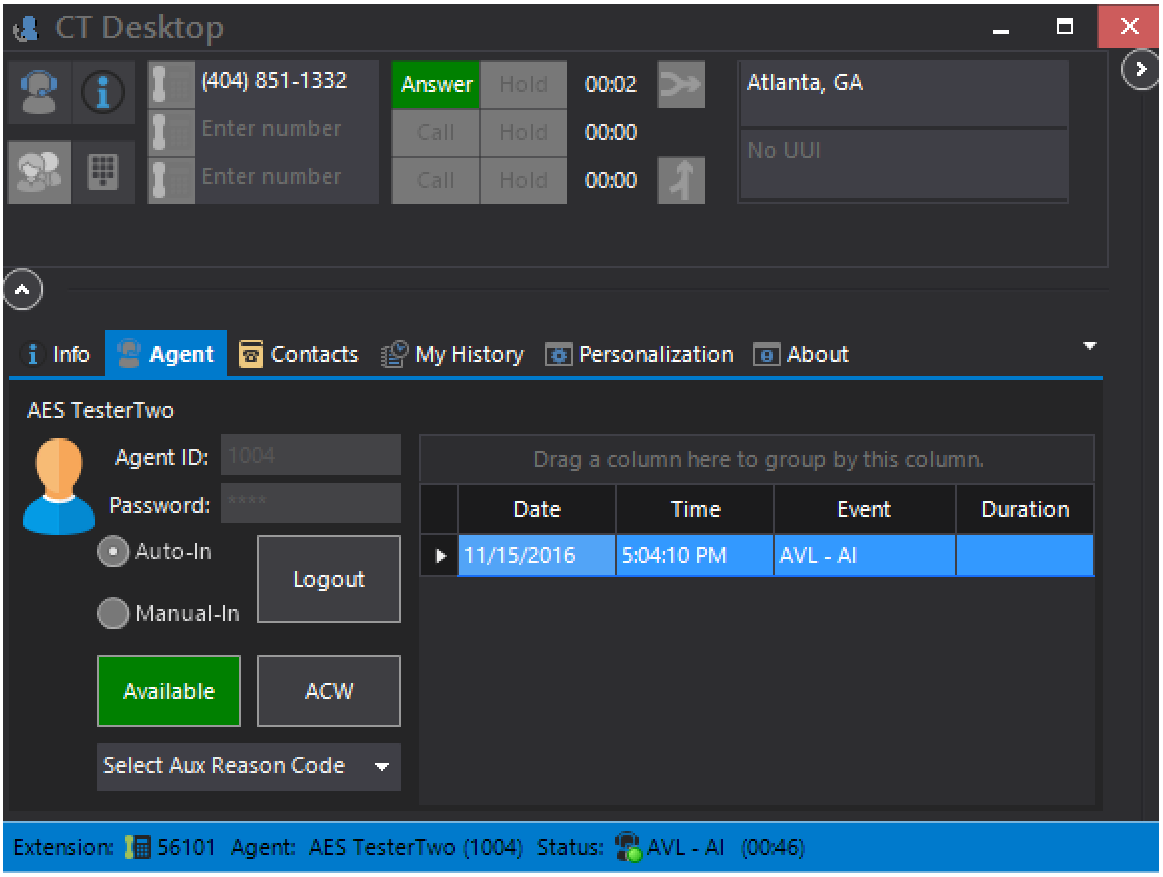
Agent ID: 1001
Password: ****

● Auto-In
○ Manual-In

Date	Time	Event	Duration
11/15/2016	5:32:09 PM	Logged In	
11/15/2016	5:32:09 PM	AUX - System (0)	00:03
11/15/2016	5:32:13 PM	AVL - AI	

Extension: 56101 Agent: AES TesterTwo (1001) Status: AVL - AI (06:24)

Make an incoming ACD call. Verify that the top pane is updated to display an incoming call. Click the **Answer** button.



(404) 851-1332 00:02

Enter number 00:00

Enter number 00:00

Atlanta, GA

No UUI

AES TesterTwo

Agent ID: 1004

Password: ****

● Auto-In

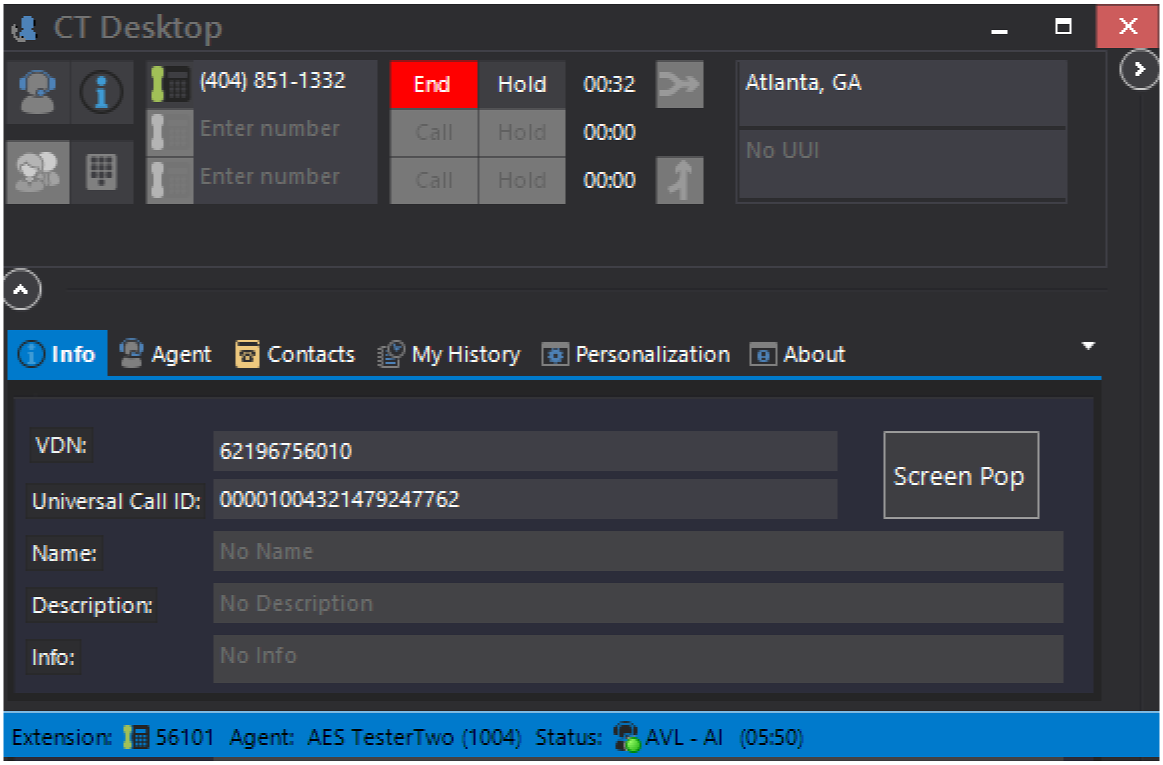
○ Manual-In

Drag a column here to group by this column.

Date	Time	Event	Duration
11/15/2016	5:04:10 PM	AVL - AI	

Extension: 56101 Agent: AES TesterTwo (1004) Status: AVL - AI (00:46)

Click on the **Info** tab to see details of **VDN** and **Universal Call ID** as shown below. Verify that the agent is connected to PSTN callller with two-way talk paths and that the upper pane is updated with **End** and **Hold**, as shown below.



(404) 851-1332 00:32
Atlanta, GA
No UUI

VDN: 62196756010
Universal Call ID: 00001004321479247762
Name: No Name
Description: No Description
Info: No Info

Extension: 56101 Agent: AES TesterTwo (1004) Status: AVL - AI (05:50)

10. Conclusion

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 2.1.5 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. 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, June 2016.

[2] Administering Avaya Aura® Session Manager, Release 7.0, Issue 7, Jan 2016.

[3] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 7.0, Document 02-300357, Jan 2016.

Documentation related to CTIntegrations may directly be obtained from CTIntegrations:

[4] CT Suite Desktop Guide R2.

[5] CT Suite Admin Guide R2.

[6] CT Desktop installation R2.5 update 2 document

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.