Avaya Solution & Interoperability Test Lab

Application Notes for CTIntegrations CT Suite 3.0 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for Voice Integration – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for voice integration. CTIntegrations CT Suite is a 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, to provide screen pop, call control, and click-to-dial features from the agent desktops.

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 3.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for voice integration. CT Suite is a contact center solution.

In the compliance testing, CT Suite used the Device, Media, and Call Control (DMCC) .Net interface from Application Enablement Services to monitor contact center agents on Communication Manager, to provide screen pop, call control, and click-to-dial features from the agent desktops. This compliance testing focused on the integration of voice work items via the Device Manager component of CT Suite.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon an agent log in, the application used DMCC to query device information and agent state, logged the agent into the ACD on Communication Manager if needed, and requested device monitoring.

For the manual part of the testing, incoming ACD calls were placed with available agents that have web browser connections to the CT Suite server. All necessary call actions by agents were initiated from the agent desktops and/or telephones. The click-to-dial calls were initiated by clicking on the phone number in the contact record displayed on the agent desktops.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the CT Suite 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 Application Enablement Services and CT Suite did not include use of any specific encryption features as requested by CTIntegrations.

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 query and set agent states, including log in, log out, and work mode changes with support for pending aux work.

- Use of DMCC monitoring services to monitor agent stations.

- Use of DMCC call control services to support call controls.

- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, conference, transfer, and long duration.

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

2.2. Test Results

All test cases were executed and verified. The following were observations on CT Suite from the compliance testing.

- When Prompt Extension was enabled on the agent template, active call indication disappeared from the agent desktop after the call was answered, with agent needing to use the telephone for subsequent call controls. The workaround is to disable Prompt Extension and use fixed agent extensions.

- By design, the default out of box application does not support screen pop of original calling, original called, and customer contact record at the transfer-to and conference-to agents.

- By design, upon any party drops from a conference, the application does not support update of agent screens to reflect remaining parties.

2.3. Support

Technical support on CT Suite can be obtained through the following:

- **Phone:** (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 resources 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
VDN	60001, 60002
Skill Group	61001, 61002
Agent Station	65001, 66002
Agent ID	65881, 65882
Agent Password	65881, 65882

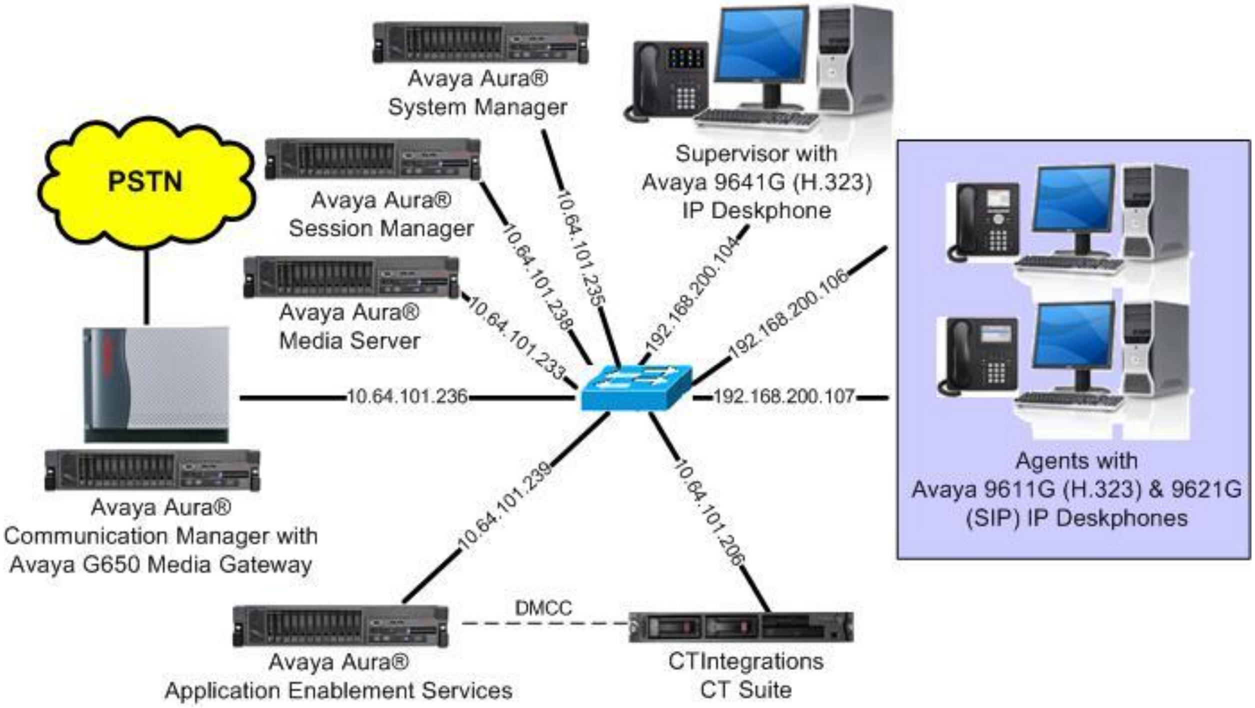

Avaya Aura® System Manager
Supervisor with Avaya 9641G (H.323) IP Deskphone
PSTN
Avaya Aura® Session Manager
Avaya Aura® Media Server
10.64.101.235
10.64.101.238
10.64.101.233
192.168.200.104
192.168.200.106
192.168.200.107
10.64.101.236
Agents with Avaya 9611G (H.323) & 9621G (SIP) IP Deskphones
10.64.101.239
10.64.101.206
Avaya Aura® Communication Manager with Avaya G650 Media Gateway
DMCC
Avaya Aura® Application Enablement Services
CTIntegrations CT Suite

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	7.0.1.2 (7.0.1.2.0.441.23523)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.375
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.4.15-0)
Avaya Aura® Session Manager in Virtual Environment	7.0.1.2 (7.0.1.2.701230)
Avaya Aura® System Manager in Virtual Environment	7.0.1.2 (7.0.1.2.086553)
Avaya 9611G and 9641G IP Deskphones (H.323)	6.6401
Avaya 9621G IP Deskphones (SIP)	7.0.1.4.6
CTIntegrations CT Suite on Microsoft Windows Server 2012 R2 • CT Admin • CT Web Client • CT Device Manager • Avaya DMCC .NET (ServiceProvider.dll)	3.0 Hotfix 1 Standard 3.0.6 3.0.3 3.0.12.17180 7.0.0.38

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify License

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

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

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y               Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                     DCS (Basic)? y
          ASAI Link Core Capabilities? n               DCS Call Coverage? y
          ASAI Link Plus Capabilities? n              DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                         DS1 MSP? y
```

5.2. Administer CTI Link

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

```
add cti-link 1                                                       Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 60111
     Type: ADJ-IP
                                                                         COR: 1
     Name: AES CTI Link
```

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: 27
```

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  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

            Agent/Caller Disconnect Tones? n
          Interruptible Aux Notification Timer (sec): 3
             Zip Tone Burst for Callmaster Endpoints: double

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

5.4. Obtain Reason Codes

For contact centers that use reason codes, enter the “change reason-code-names” command to display the configured reason codes. Make a note of the **Aux Work** reason codes, which will be used later to configure 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  Other
        Reason Code 8:                 /n
        Reason Code 9:                 /n

  Default Reason Code:
```

6. Configure Avaya Aura® Application Enablement Services

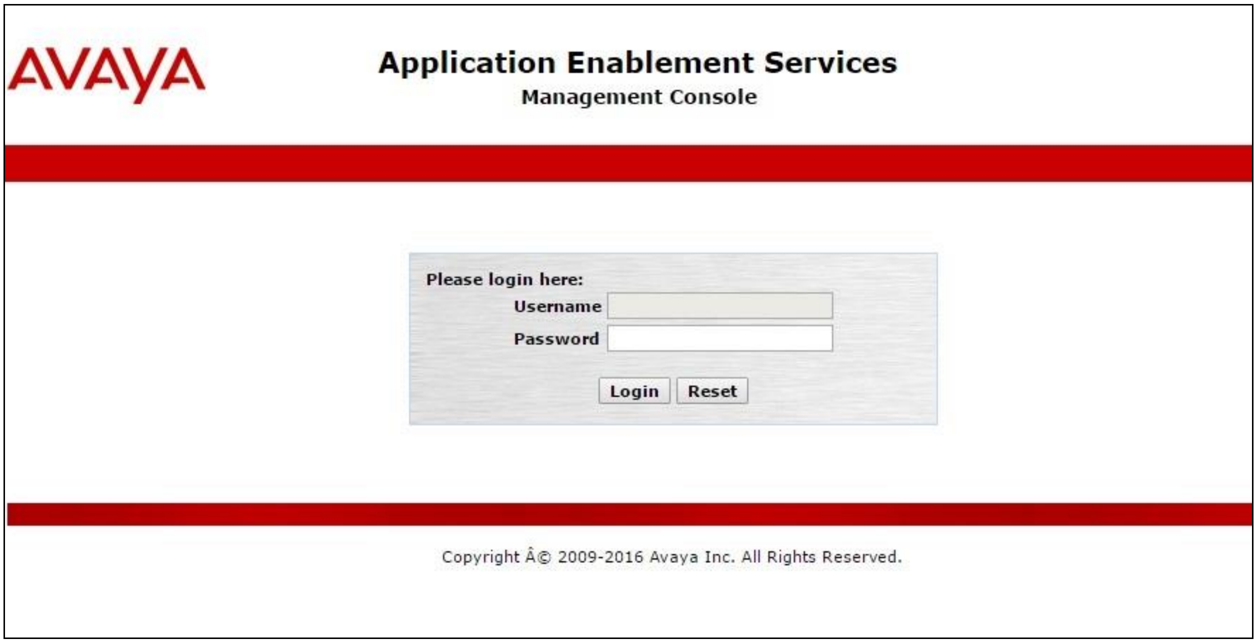
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer CT Suite user
- Administer security database
- Administer ports
- Restart services
- Obtain Tlink name

6.1. Launch OAM Interface

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

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

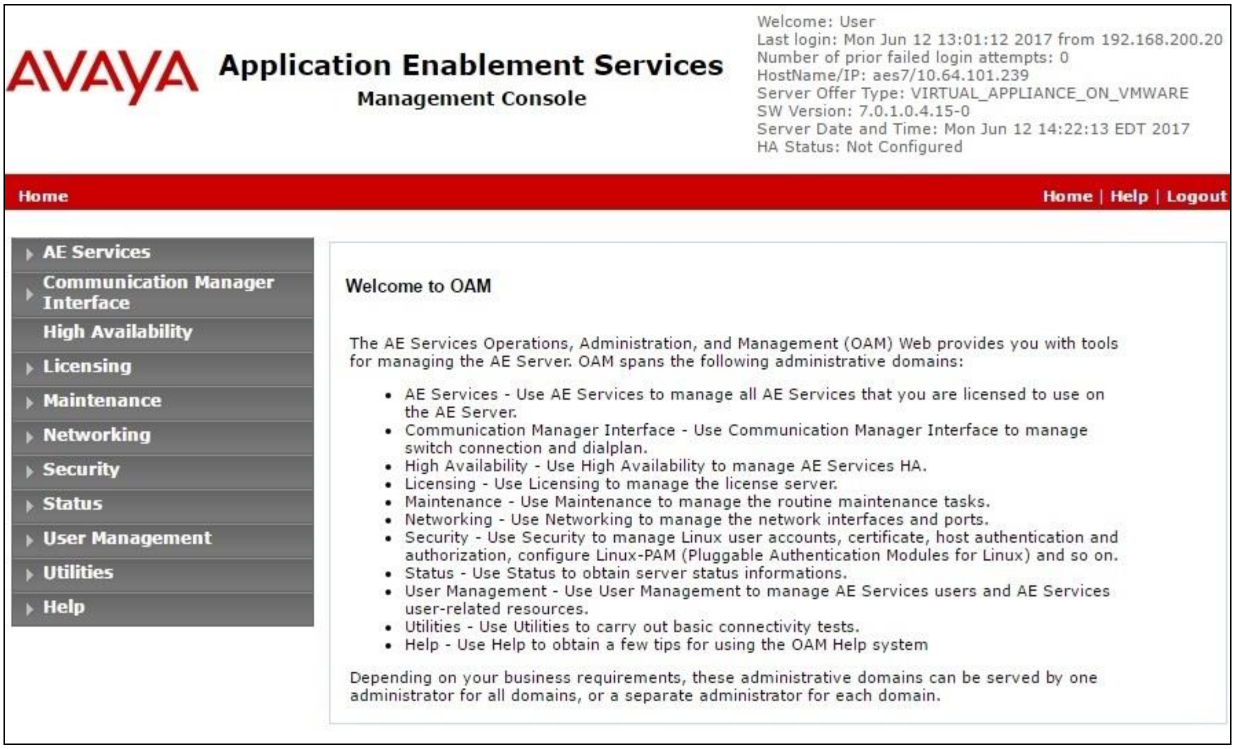


Application Enablement Services
Management Console

Please login here:
Username
Password

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

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



Welcome: User
Last login: Mon Jun 12 13:01:12 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Welcome to OAM

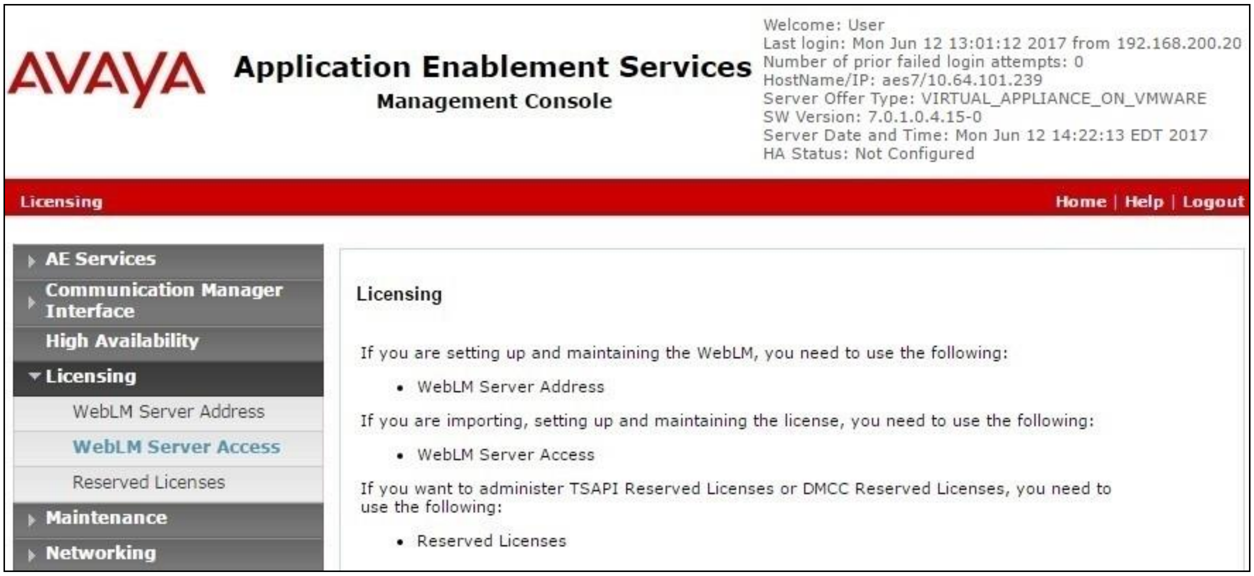
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

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
Last login: Mon Jun 12 13:01:12 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Licensing

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

- WebLM Server Address

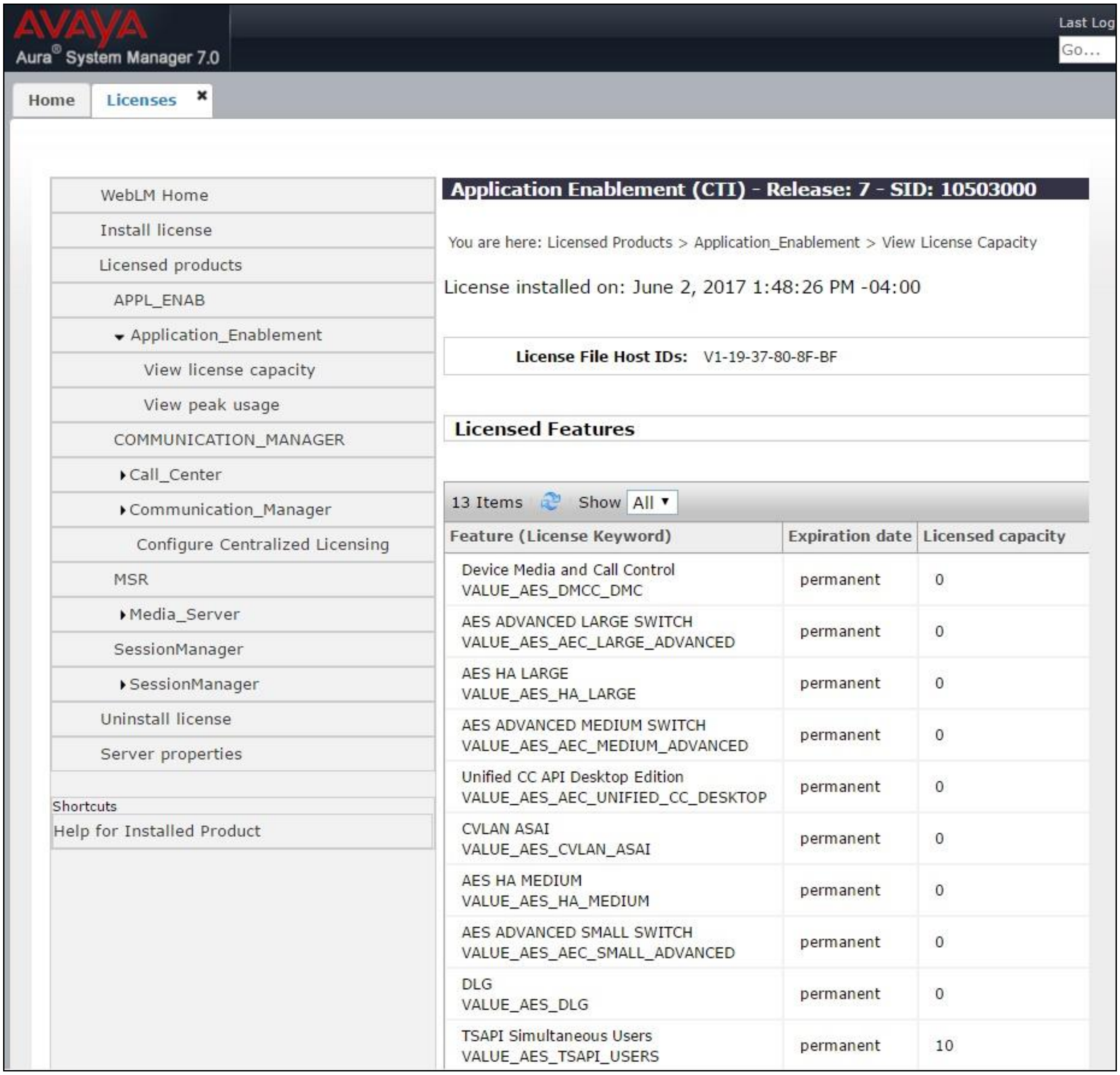
If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

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

- Reserved Licenses

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 agent monitoring and call control via DMCC.



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

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

License installed on: June 2, 2017 1:48:26 PM -04:00

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

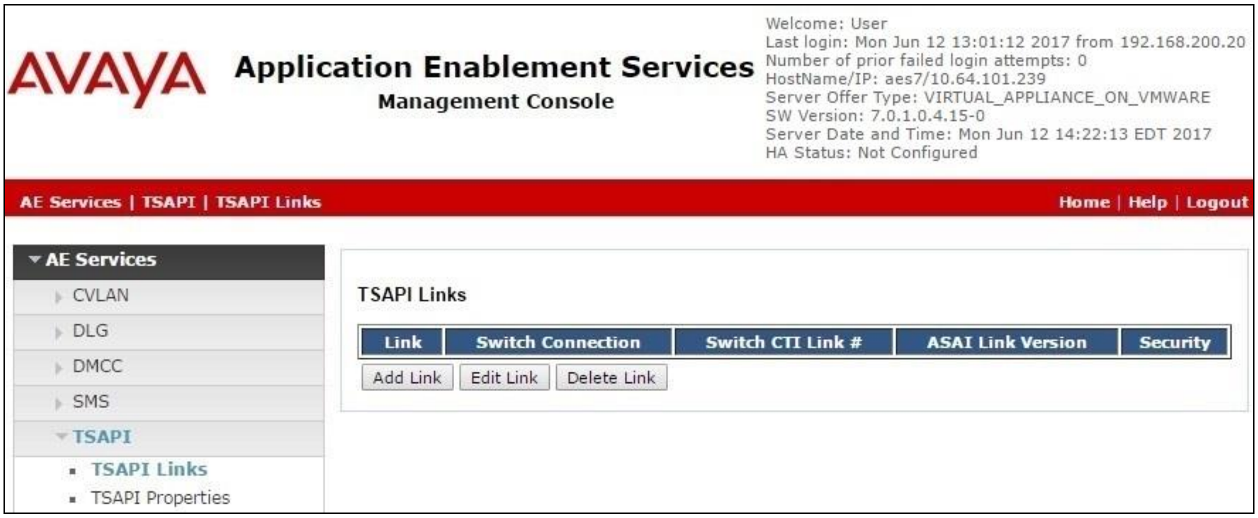
Licensed Features

13 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	0
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	0
AES HA LARGE VALUE_AES_HA_LARGE	permanent	0
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	0
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	0
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	0
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	0
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	0
DLG VALUE_AES_DLG	permanent	0
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10

6.3. Administer TSAPI Link

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



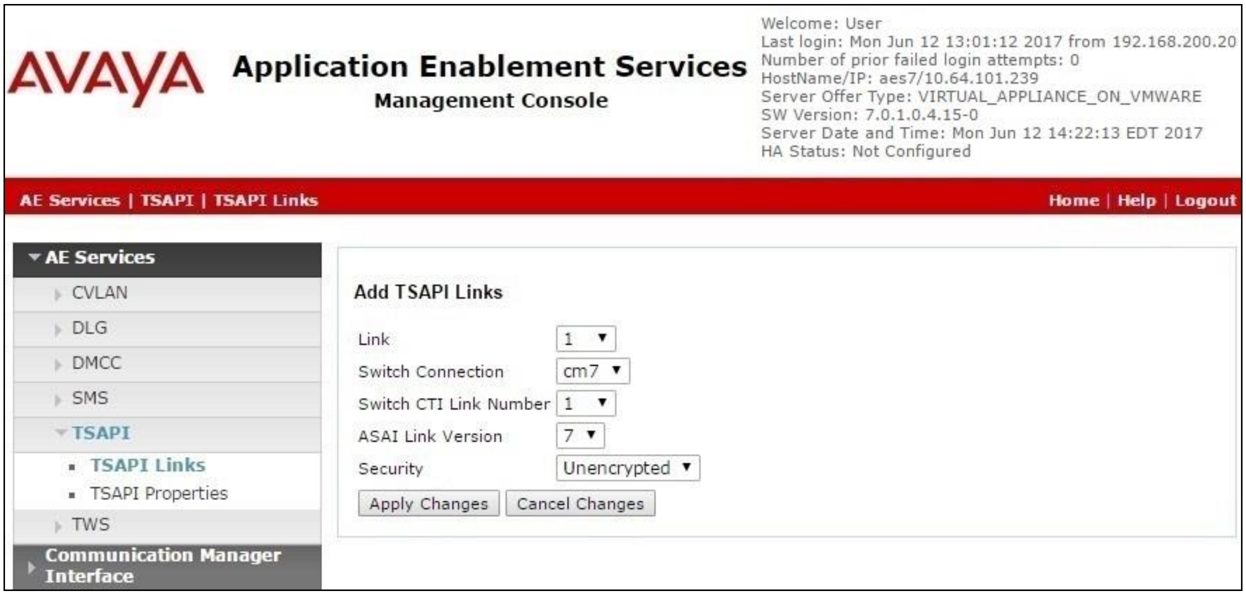
Welcome: User
Last login: Mon Jun 12 13:01:12 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Welcome: User
Last login: Mon Jun 12 13:01:12 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

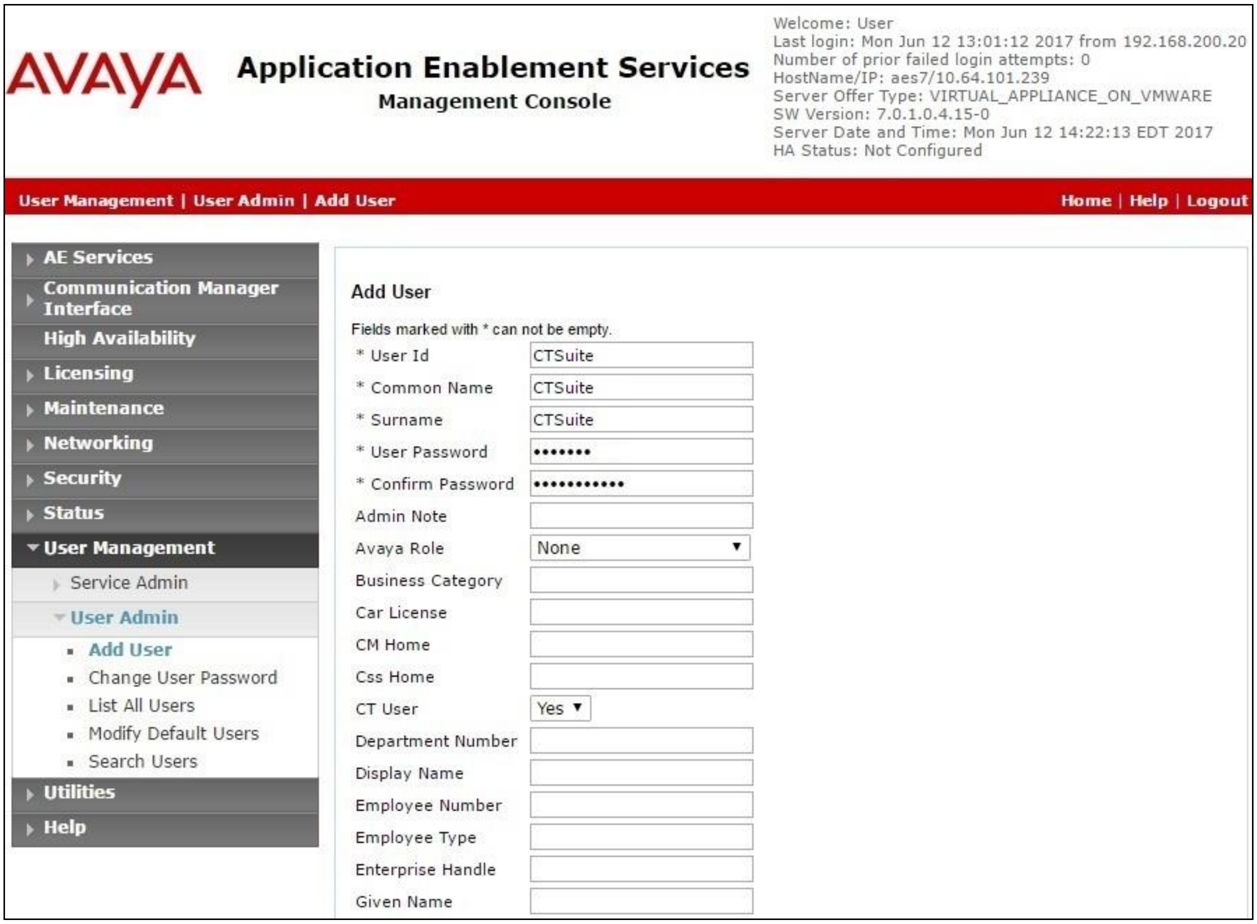
Add TSAPI Links

Link	1 ▾
Switch Connection	cm7 ▾
Switch CTI Link Number	1 ▾
ASAI Link Version	7 ▾
Security	Unencrypted ▾

6.4. Administer CT Suite 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
Last login: Mon Jun 12 13:01:12 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Add User

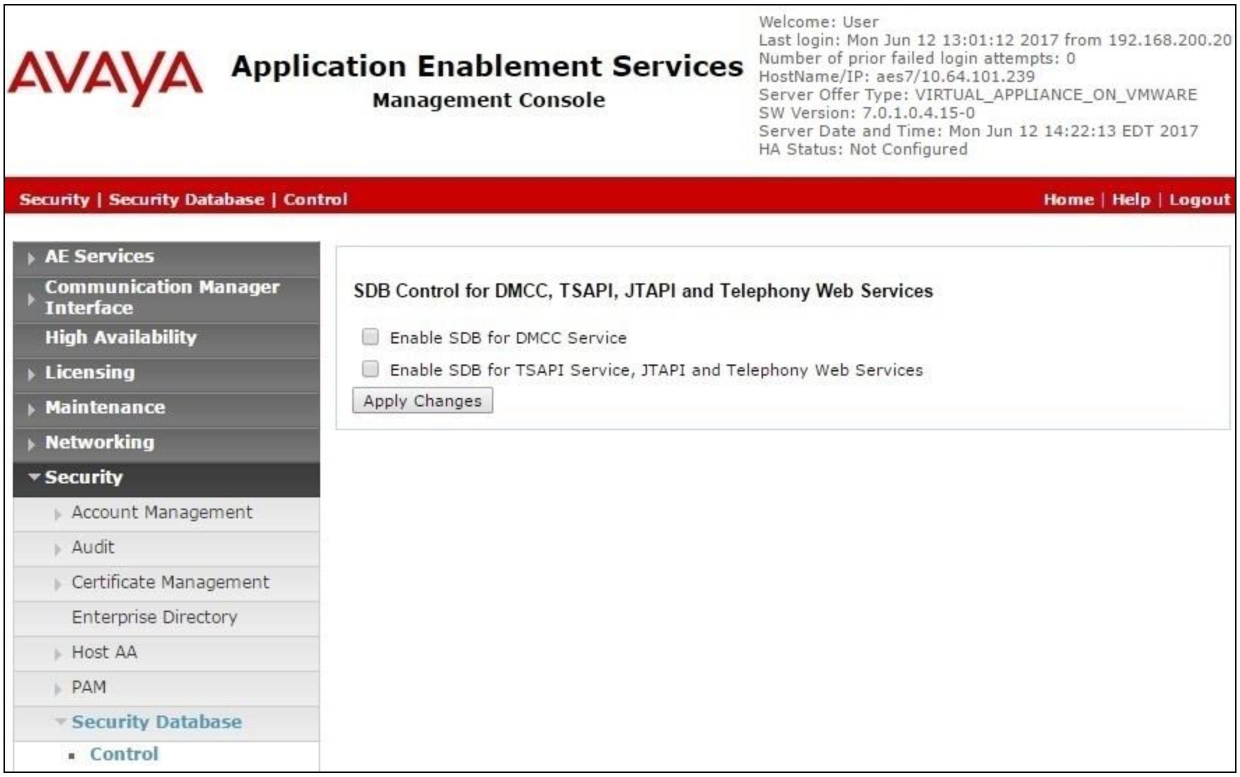
Fields marked with * can not be empty.

* User Id	CTSuite
* Common Name	CTSuite
* Surname	CTSuite
* User Password	•••••••
* Confirm Password	•••••••••••
Admin Note	
Avaya Role	None ▼
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes ▼
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	

6.5. Administer Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

In the event that the parameters are enabled with security database used by the customer, then follow reference [2] to configure access privileges for the CT Suite user from **Section 6.4**.



Welcome: User
Last login: Mon Jun 12 13:01:12 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

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

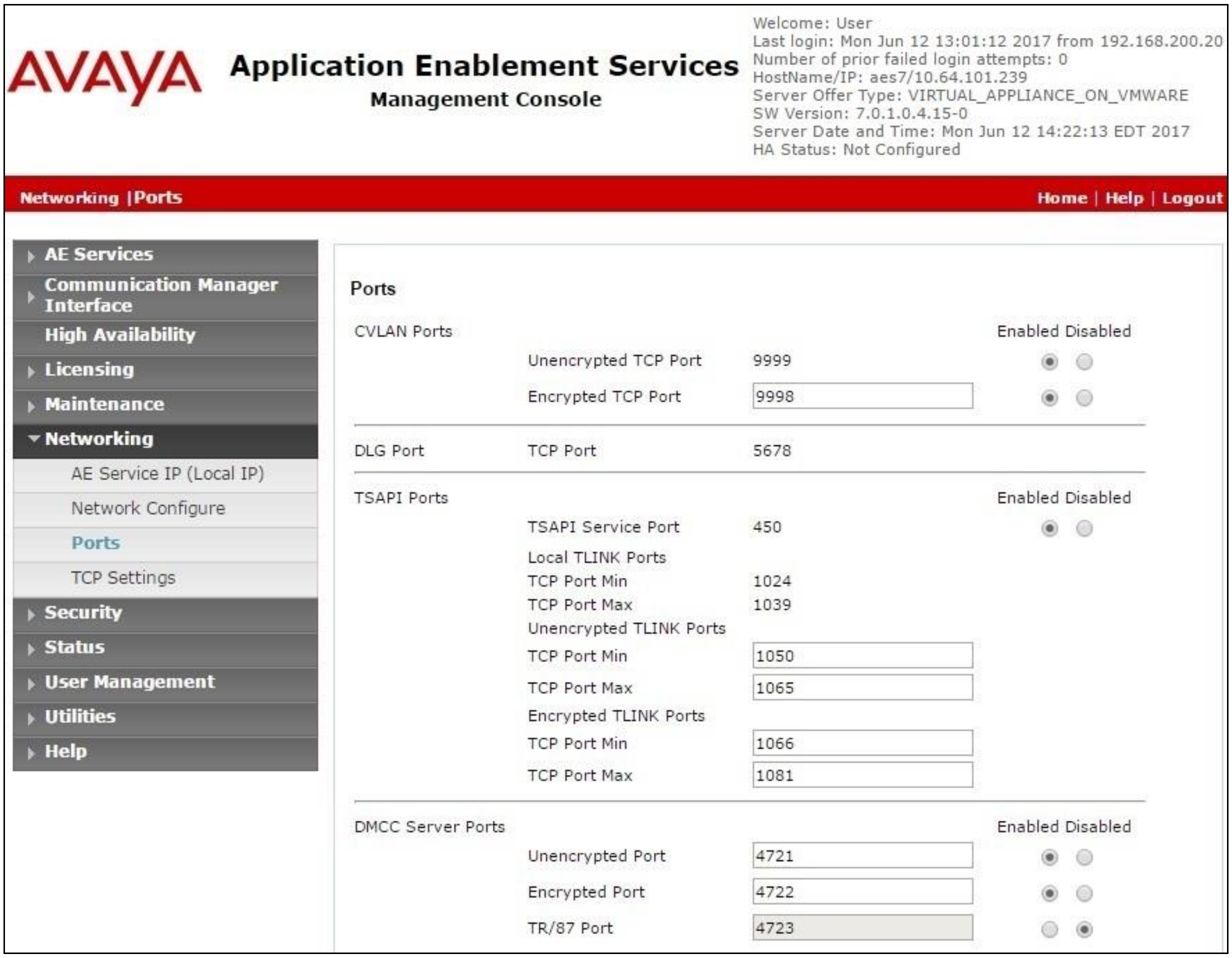
☐ Enable SDB for DMCC Service

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

6.6. 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** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



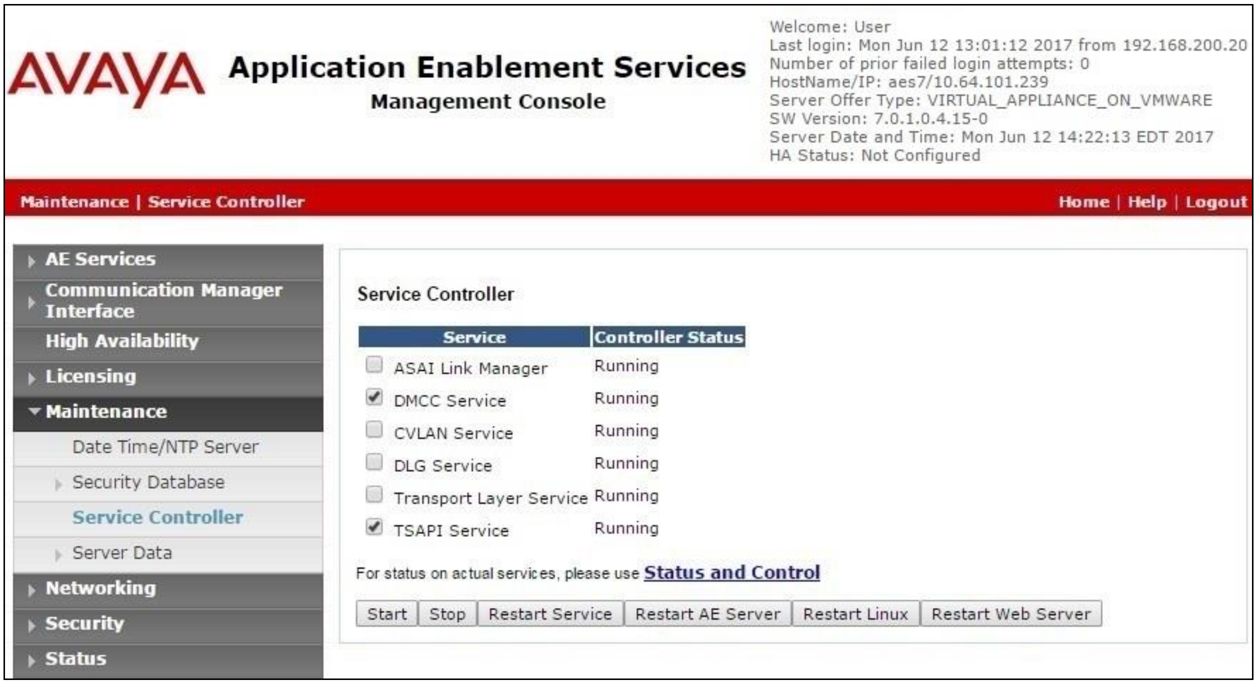
Welcome: User
Last login: Mon Jun 12 13:01:12 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	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				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●

6.7. 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
Last login: Mon Jun 12 13:01:12 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Service Controller

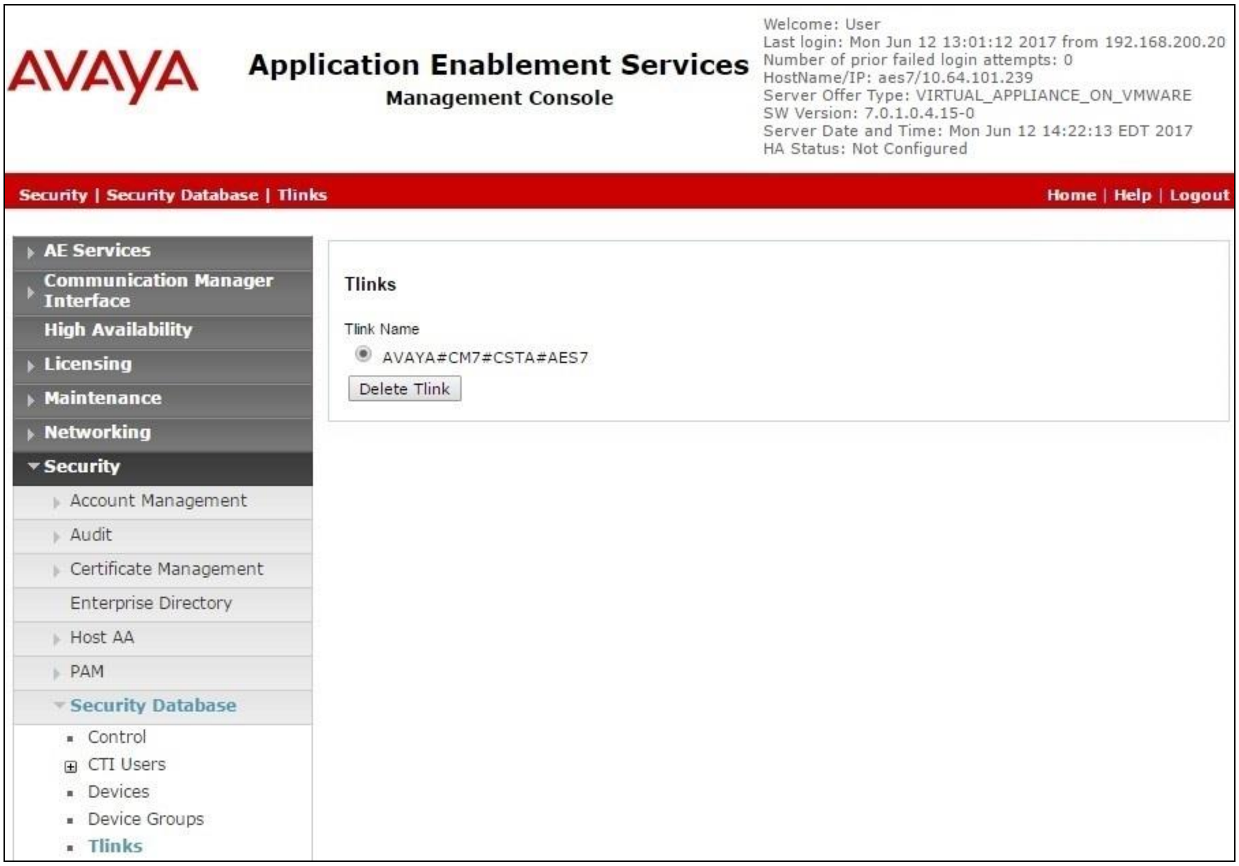
Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.8. Obtain Tlink Name

Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of Tlink names. A new Tlink name is automatically generated for the TSAPI service.

Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring CT Suite.



Welcome: User
Last login: Mon Jun 12 13:01:12 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Tlinks

Tlink Name
● AVAYA#CM7#CSTA#AES7

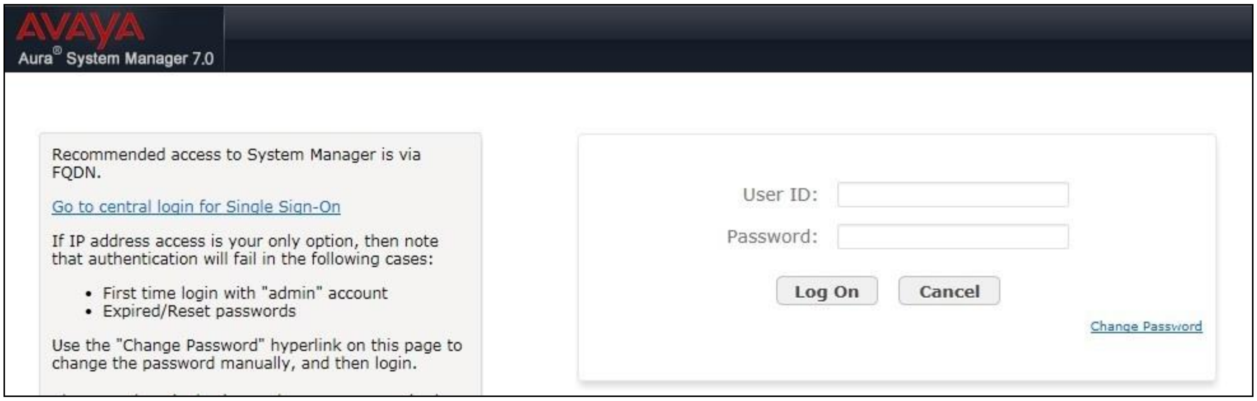
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

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



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

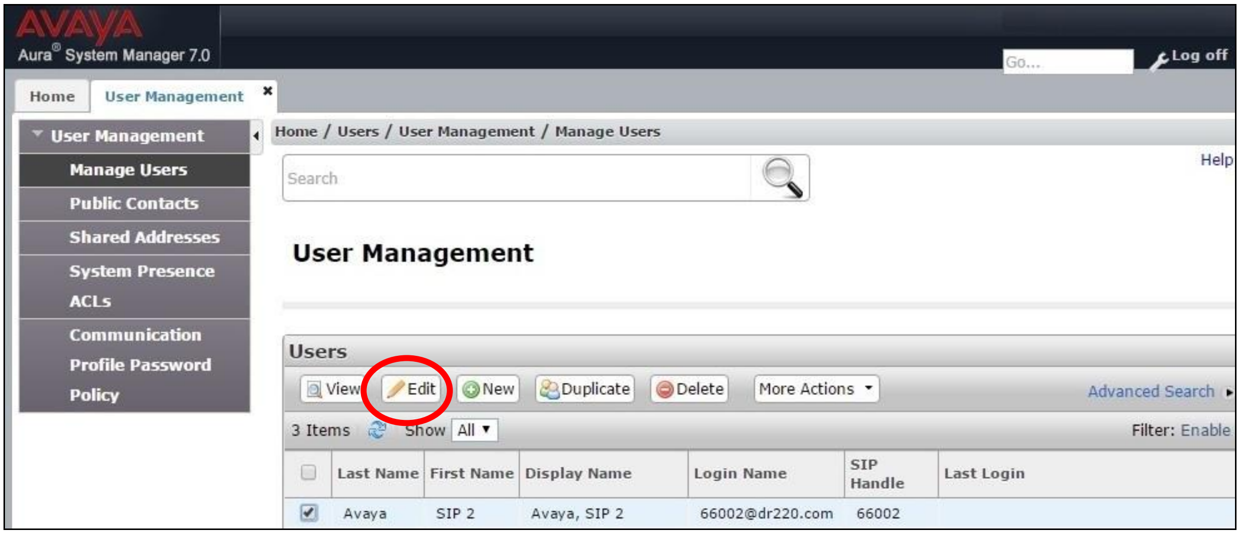
If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

7.2. Administer Users

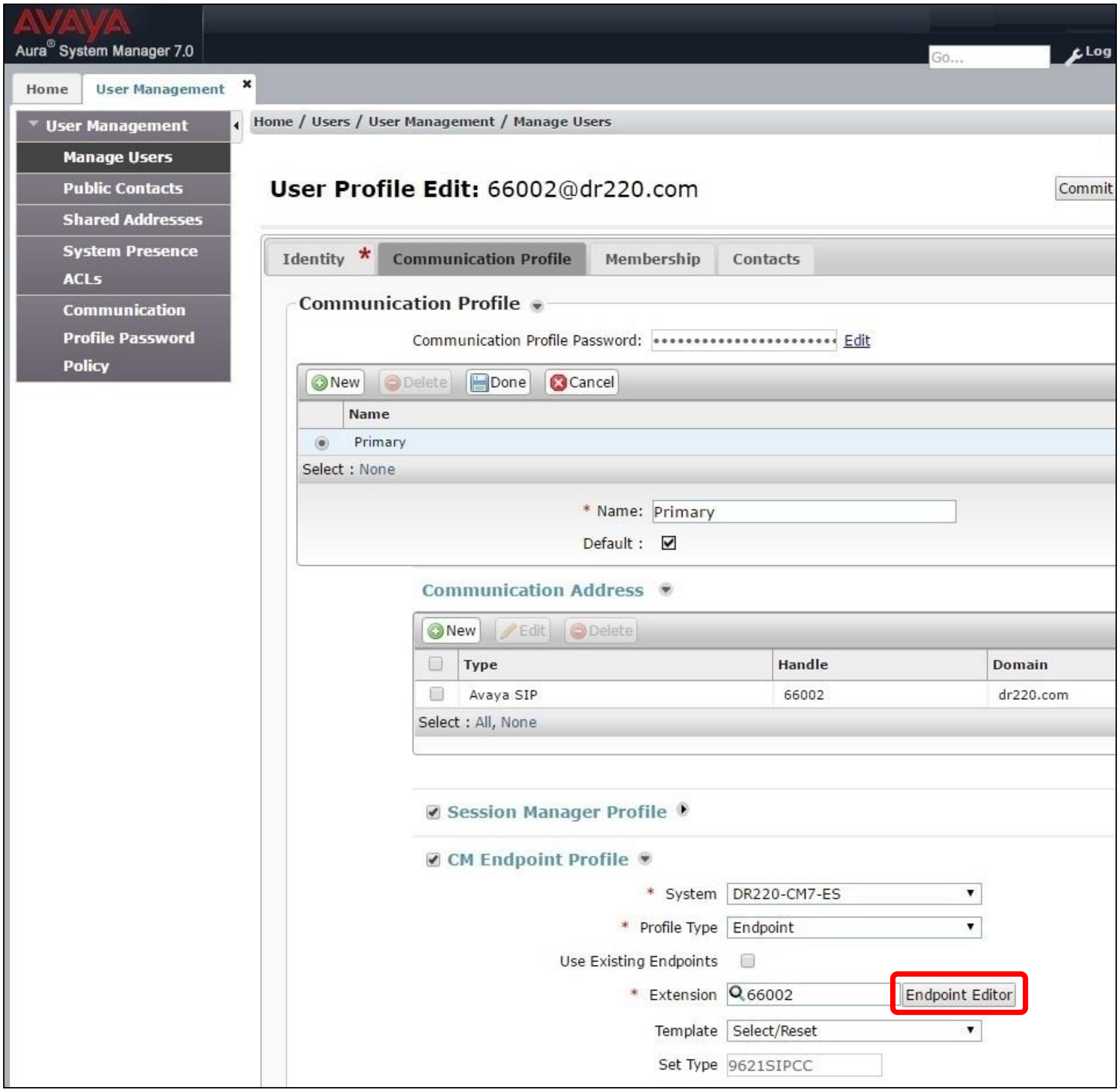
In the subsequent screen (not shown), select **Users → User Management**. Select **User Management → Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.



□	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
☑	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.



Home / Users / User Management / Manage Users

User Profile Edit: 66002@dr220.com

Identity * | Communication Profile | Membership | Contacts

Communication Profile

Communication Profile Password: •••••••••••••••••••••• Edit

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

□	Type	Handle	Domain
□	Avaya SIP	66002	dr220.com

Select : All, None

☑ Session Manager Profile

☑ CM Endpoint Profile

* System DR220-CM7-ES

* Profile Type Endpoint

Use Existing Endpoints □

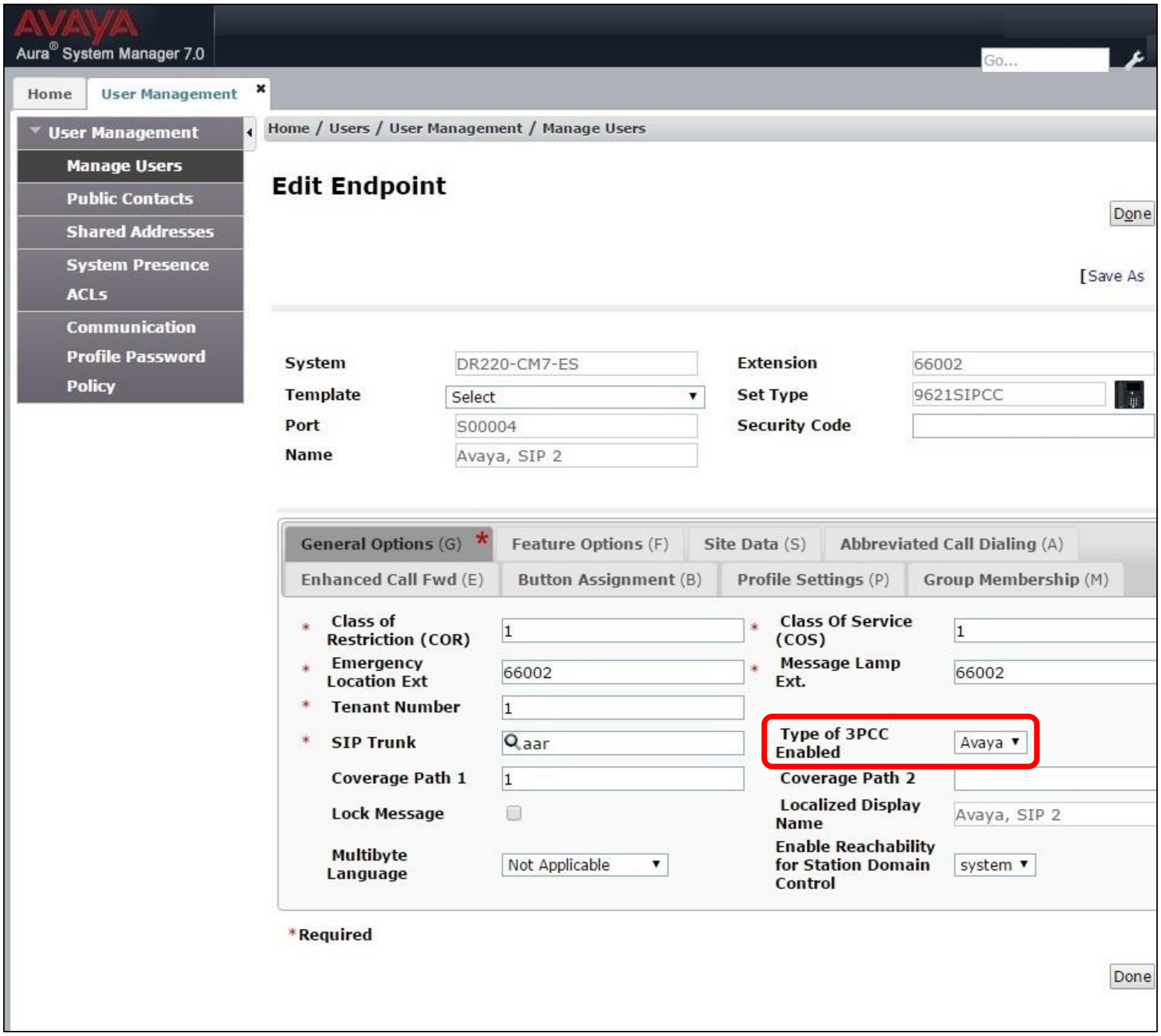
* Extension 66002

Template Select/Reset

Set Type 9621SIPCC

The **Edit Endpoint** screen is displayed. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.



Edit Endpoint

System	DR220-CM7-ES	Extension	66002
Template	Select	Set Type	9621SIPCC
Port	S00004	Security Code	
Name	Avaya, SIP 2		

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

*Required

8. Configure CTIntegrations CT Suite

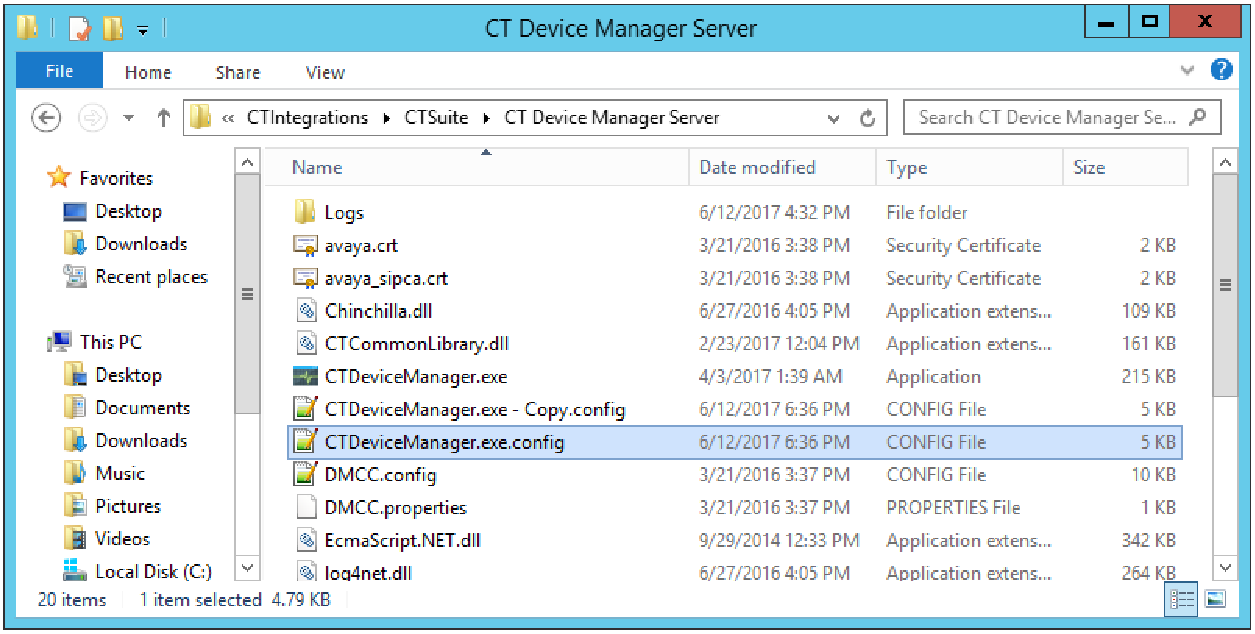
This section provides the procedures for configuring CT Suite. The procedures include the following areas:

- Administer CT Device Manager
- Restart service
- Launch CT Admin interface
- Administer site
- Administer resources
- Administer agent templates

The configuration of CT Suite is typically performed by CTIntegrations system integrators. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Administer CT Device Manager

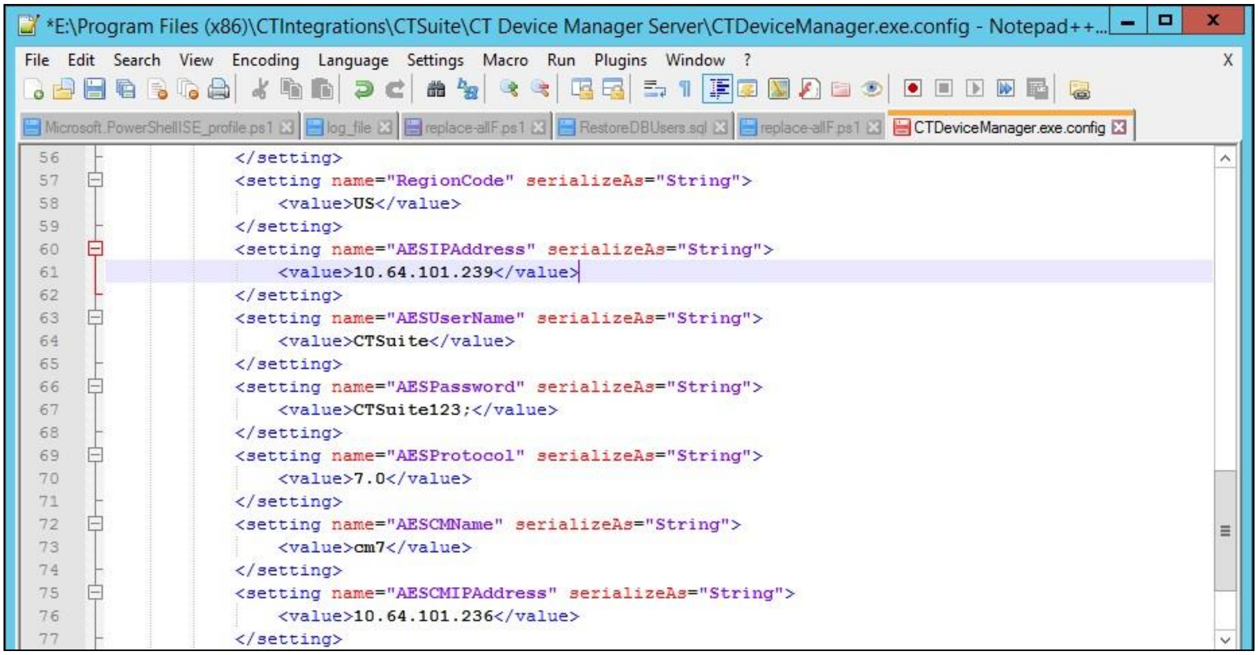
From the CT Suite server, navigate to **E:\Program Files (x86)\CTIntegrations\CTSuite\CT Device Manager Server** to locate the **CTDeviceManager.exe.config** file. Open the file with an application such as NotePad++.



Name	Date modified	Type	Size
Logs	6/12/2017 4:32 PM	File folder	
avaya.crt	3/21/2016 3:38 PM	Security Certificate	2 KB
avaya_sipca.crt	3/21/2016 3:38 PM	Security Certificate	2 KB
Chinchilla.dll	6/27/2016 4:05 PM	Application extens...	109 KB
CTCommonLibrary.dll	2/23/2017 12:04 PM	Application extens...	161 KB
CTDeviceManager.exe	4/3/2017 1:39 AM	Application	215 KB
CTDeviceManager.exe - Copy.config	6/12/2017 6:36 PM	CONFIG File	5 KB
CTDeviceManager.exe.config	6/12/2017 6:36 PM	CONFIG File	5 KB
DMCC.config	3/21/2016 3:37 PM	CONFIG File	10 KB
DMCC.properties	3/21/2016 3:37 PM	PROPERTIES File	1 KB
EcmaScript.NET.dll	9/29/2014 12:33 PM	Application extens...	342 KB
log4net.dll	6/27/2016 4:05 PM	Application extens...	264 KB

Scroll down to the sub-section containing the **AESIPAddress** parameter. Enter the following values for specified fields, and retain the default values for the remaining fields.

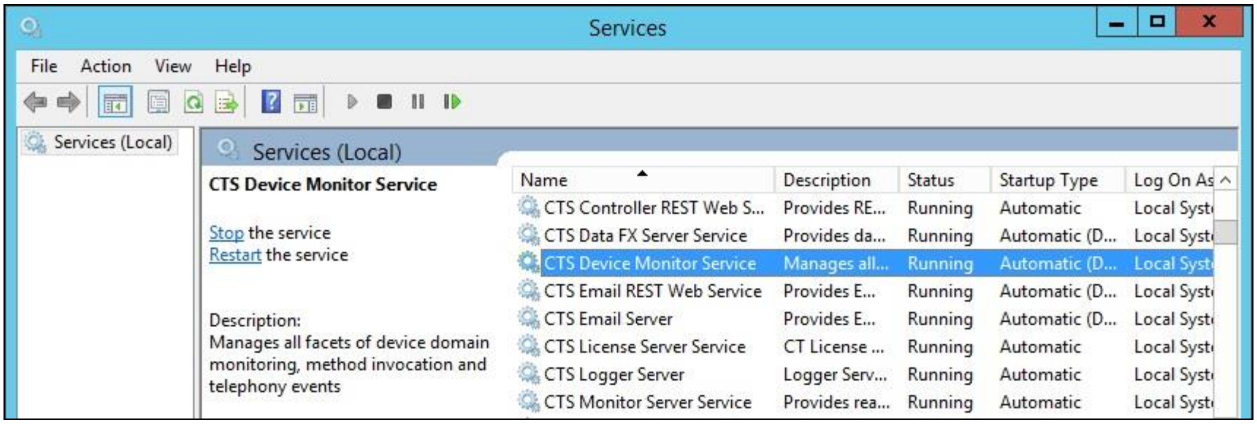
- **AESIPAddress:** IP address of Application Enablement Services.
- **AESUserName:** The CT Suite user credentials from **Section 6.4**.
- **AESPassword:** The CT Suite user credentials from **Section 6.4**.
- **AESCMName:** The switch connection name from **Section 6.3**.
- **AESCMIPAddress:** IP address of Communication Manager from **Section 3**.


*E:\Program Files (x86)\CTIntegrations\CTSuite\CT Device Manager Server\CTDeviceManager.exe.config - Notepad++...
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Microsoft.PowerShellISE_profile.ps1
log_file
replace-allF.ps1
RestoreDBUsers.sql
replace-allF.ps1
CTDeviceManager.exe.config

```
            </setting>
            <setting name="RegionCode" serializeAs="String">
                <value>US</value>
            </setting>
            <setting name="AESIPAddress" serializeAs="String">
                <value>10.64.101.239</value>
            </setting>
            <setting name="AESUserName" serializeAs="String">
                <value>CTSuite</value>
            </setting>
            <setting name="AESPassword" serializeAs="String">
                <value>CTSuite123;</value>
            </setting>
            <setting name="AESProtocol" serializeAs="String">
                <value>7.0</value>
            </setting>
            <setting name="AESCMName" serializeAs="String">
                <value>cm7</value>
            </setting>
            <setting name="AESCMIPAddress" serializeAs="String">
                <value>10.64.101.236</value>
            </setting>
```

8.2. Restart Service

From the CT Suite server, select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Locate and restart the **CTS Device Monitor Service**, as shown below.



CTS Device Monitor Service

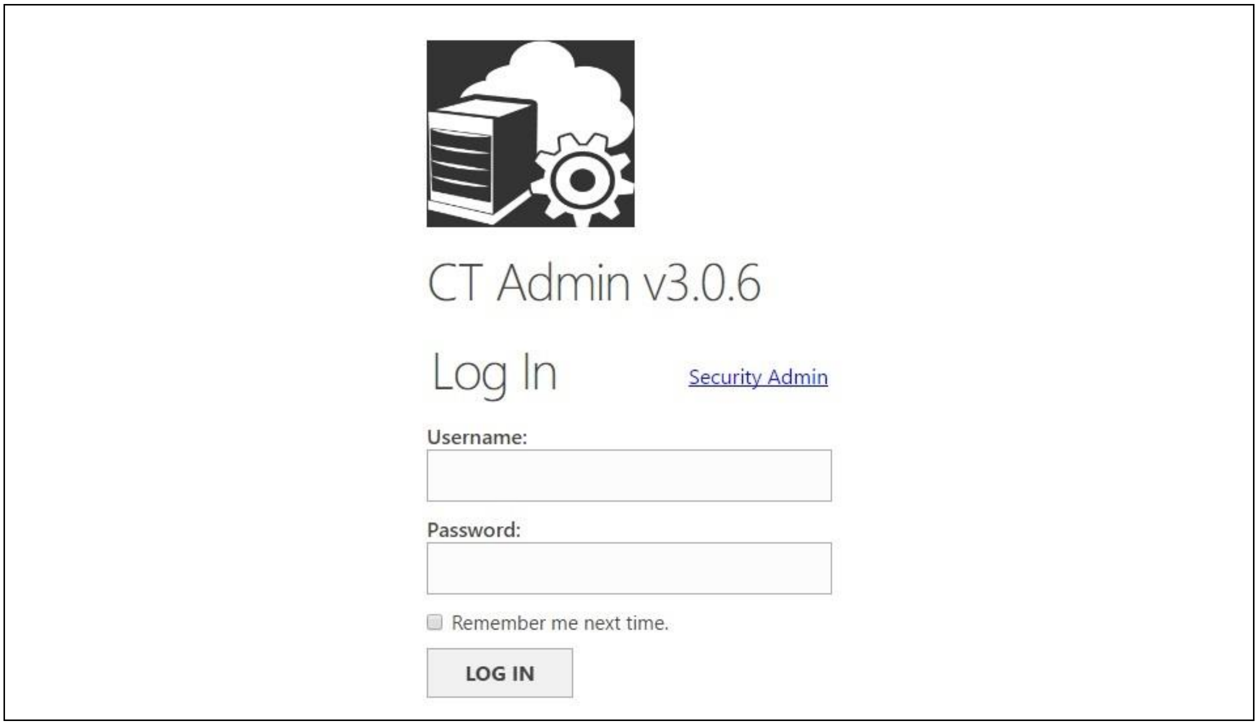
Stop the service
Restart the service

Description:
Manages all facets of device domain monitoring, method invocation and telephony events

Name	Description	Status	Startup Type	Log On As
CTS Controller REST Web S...	Provides RE...	Running	Automatic	Local Syst
CTS Data FX Server Service	Provides da...	Running	Automatic (D...	Local Syst
CTS Device Monitor Service	Manages all...	Running	Automatic (D...	Local Syst
CTS Email REST Web Service	Provides E...	Running	Automatic (D...	Local Syst
CTS Email Server	Provides E...	Running	Automatic (D...	Local Syst
CTS License Server Service	CT License ...	Running	Automatic	Local Syst
CTS Logger Server	Logger Serv...	Running	Automatic	Local Syst
CTS Monitor Server Service	Provides rea...	Running	Automatic	Local Syst

8.3. Launch CT Admin Interface

Access the CT Admin web interface by using the URL “http://ip-address/CTAdmin” in an Internet browser window, where “ip-address” is the IP address of the CT Suite server. The **CT Admin** screen below is displayed. Log in using the administrator credentials.



CT Admin v3.0.6

Log In

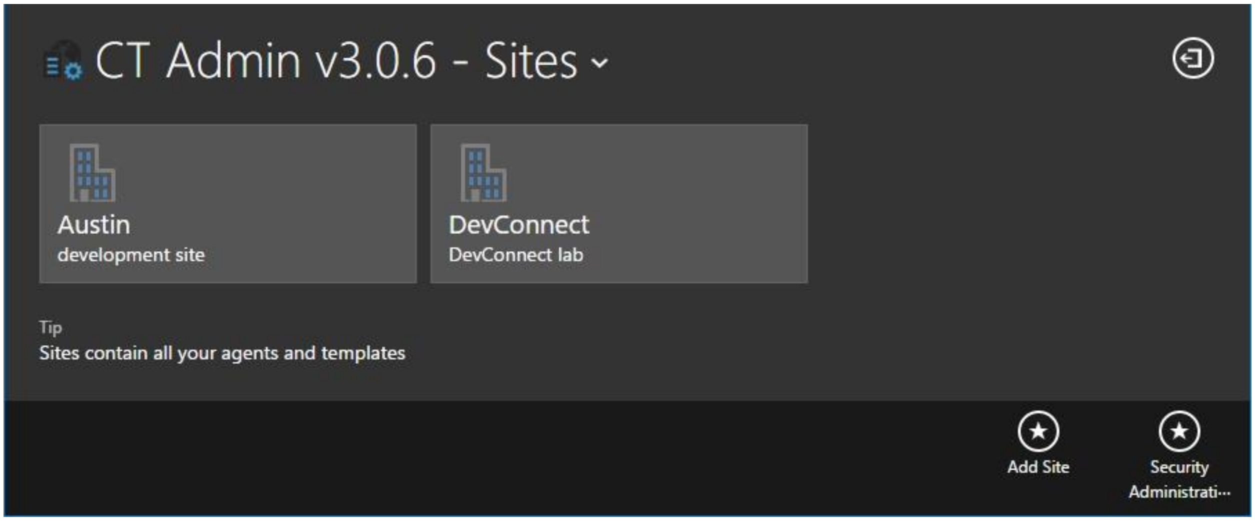
Username:

Password:

□ Remember me next time.

8.4. Administer Site

The **Sites** screen below is displayed next. Select **Add Site** from bottom of screen to add a site. In the compliance testing, the “Austin” and “DevConnect” sites were pre-configured. Select the pertinent newly added site, in this case “DevConnect”.



CT Admin v3.0.6 - Sites

Austin
development site

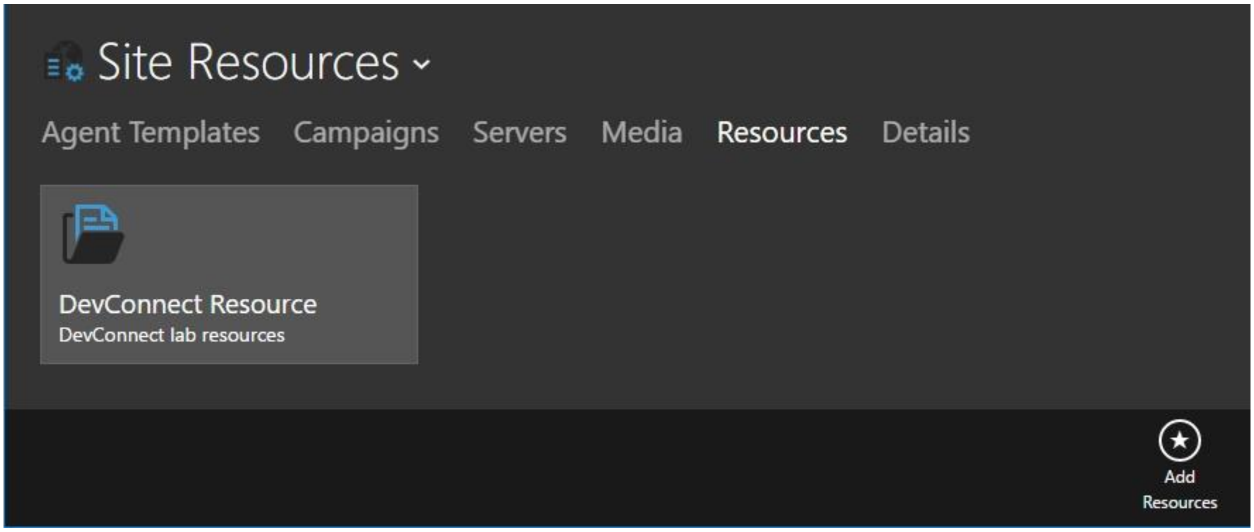
DevConnect
DevConnect lab

Tip
Sites contain all your agents and templates

8.5. Administer Resources

The **Site Resources** screen is displayed. Select **Resources** from the top menu, followed by **Add Resources** from bottom of screen to add a logical group for resources.

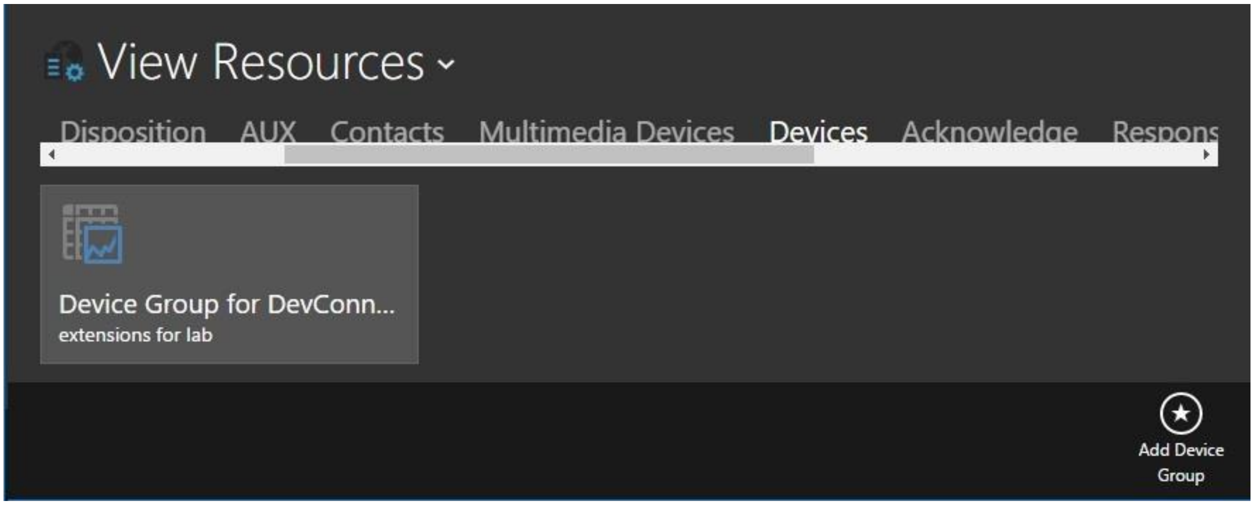
In the compliance testing, the “DevConnect Resource” group was pre-configured. Select the newly added group.



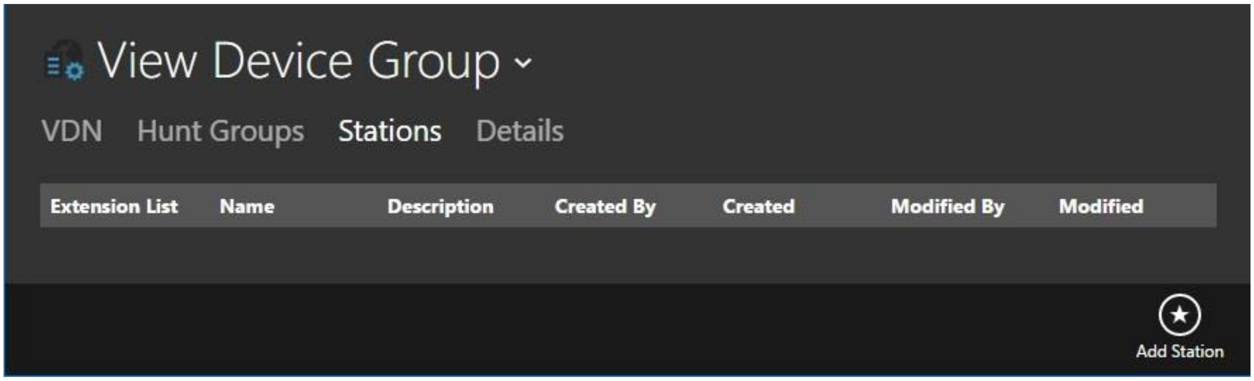
8.5.1. Devices

The **View Resources** screen is displayed next. Scroll the top menu bar as necessary to locate and select **Devices**, followed by **Add Device Group** from bottom of screen to add a logical group for devices.

In the compliance testing, the “Device Group for DevConnect” group was pre-configured. Select the newly added group.

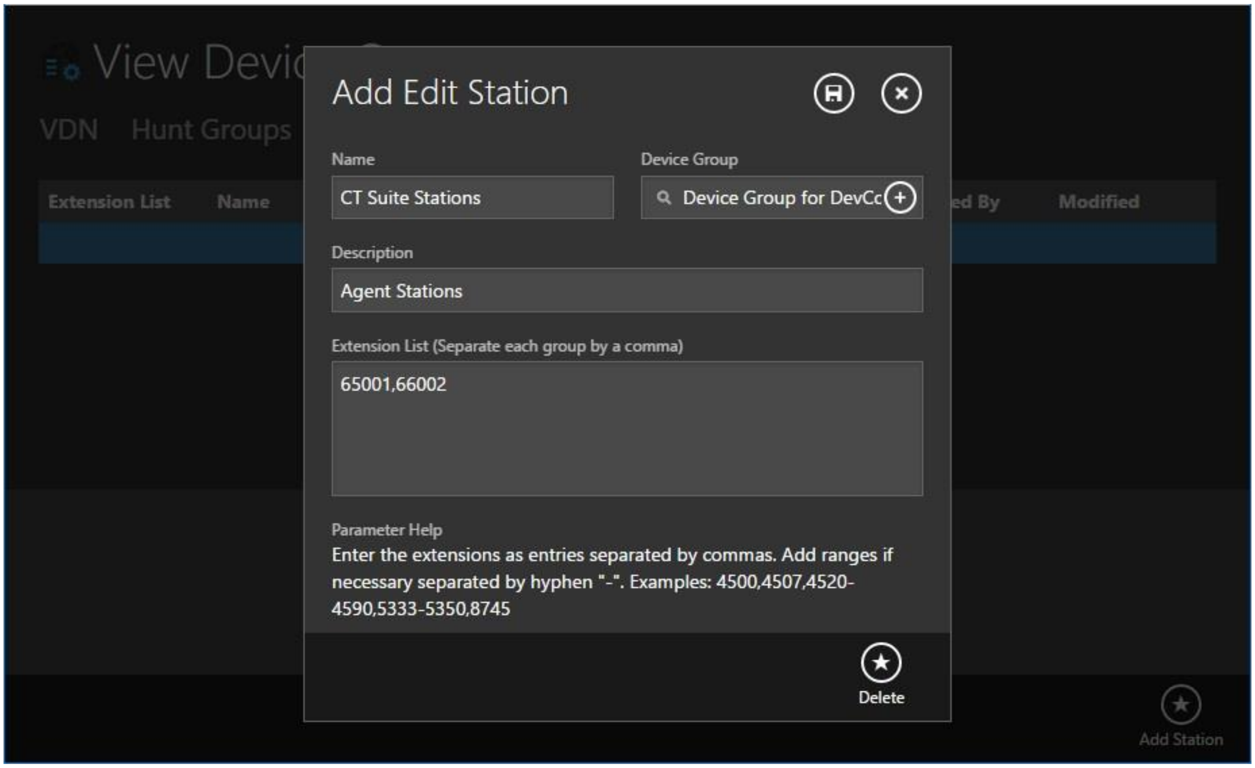


The **View Device Group** screen is displayed. Select **Stations** from the top menu, followed by **Add Station** from bottom of screen.



The **Add Edit Station** screen is displayed next. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **Description:** A desired description.
- **Extension List:** The agent station extensions from **Section 3**.


Add Edit Station

Name: CT Suite Stations

Device Group: Device Group for DevCc

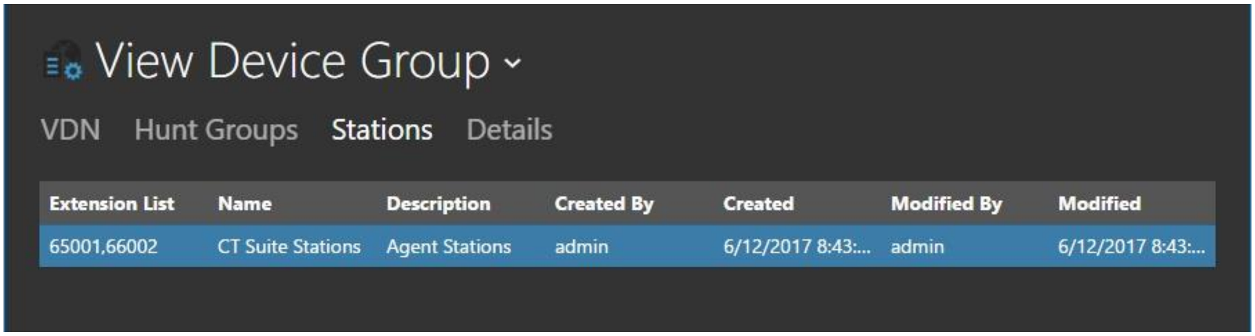
Description: Agent Stations

Extension List (Separate each group by a comma): 65001,66002

Parameter Help

Enter the extensions as entries separated by commas. Add ranges if necessary separated by hyphen "-". Examples: 4500,4507,4520-4590,5333-5350,8745

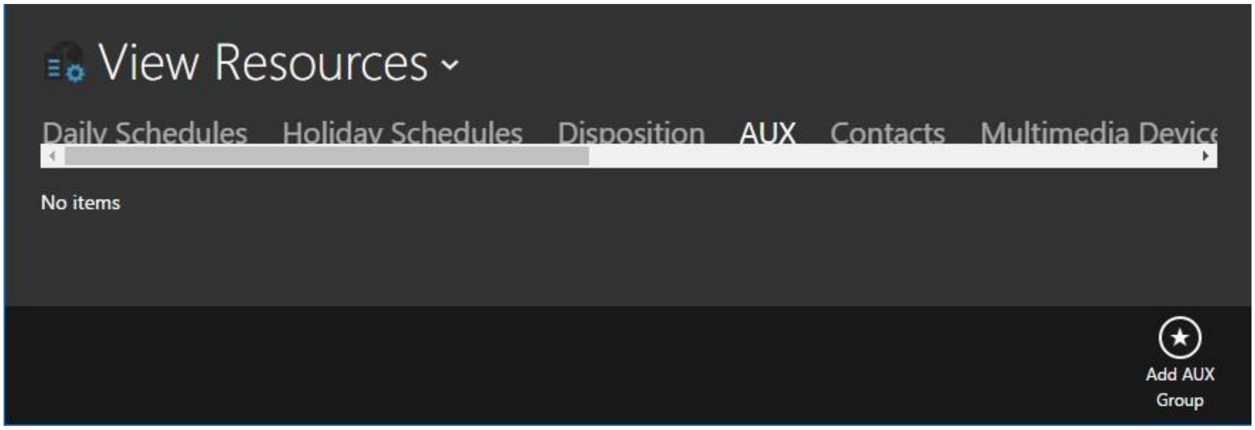
In the compliance testing, two stations **65001** and **66002** were added, as shown below.



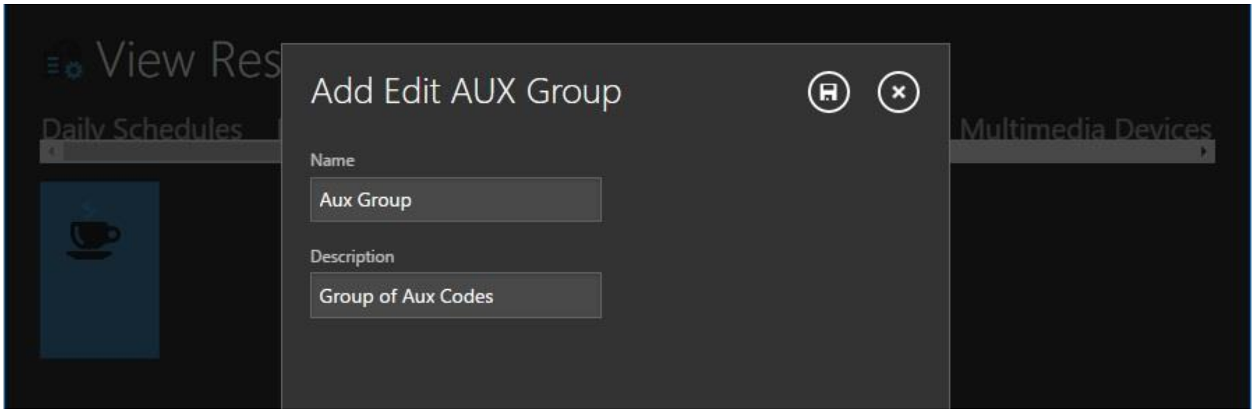
Extension List	Name	Description	Created By	Created	Modified By	Modified
65001,66002	CT Suite Stations	Agent Stations	admin	6/12/2017 8:43:...	admin	6/12/2017 8:43:...

8.5.2. AUX

Navigate back to the **View Resources** screen. Scroll the top menu bar as necessary to locate and select **AUX**, followed by **Add AUX Group** from bottom of screen to add a logical group for aux codes.



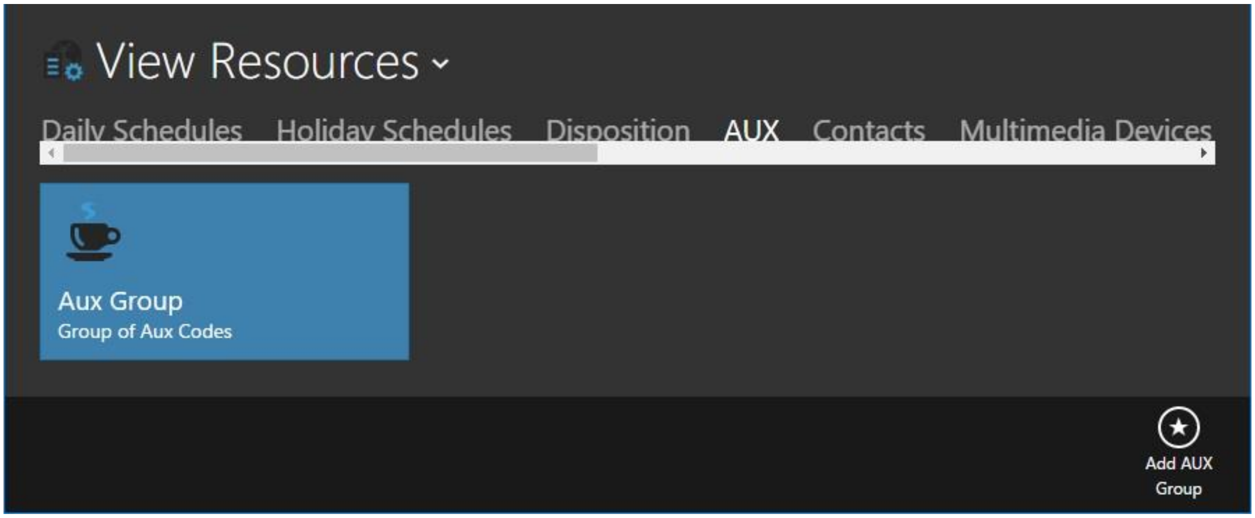
The **Add Edit AUX Group** screen is displayed next. Enter desired values for **Name** and **Description**, as shown below.



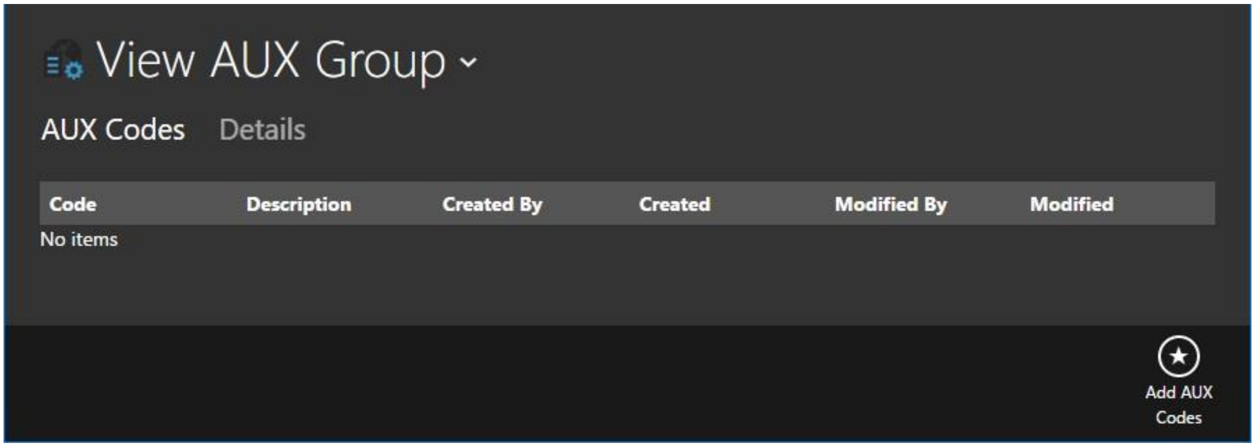
Name: Aux Group

Description: Group of Aux Codes

The **View Resources** screen is displayed again. Select the newly added AUX group, in this case “Aux Group”.



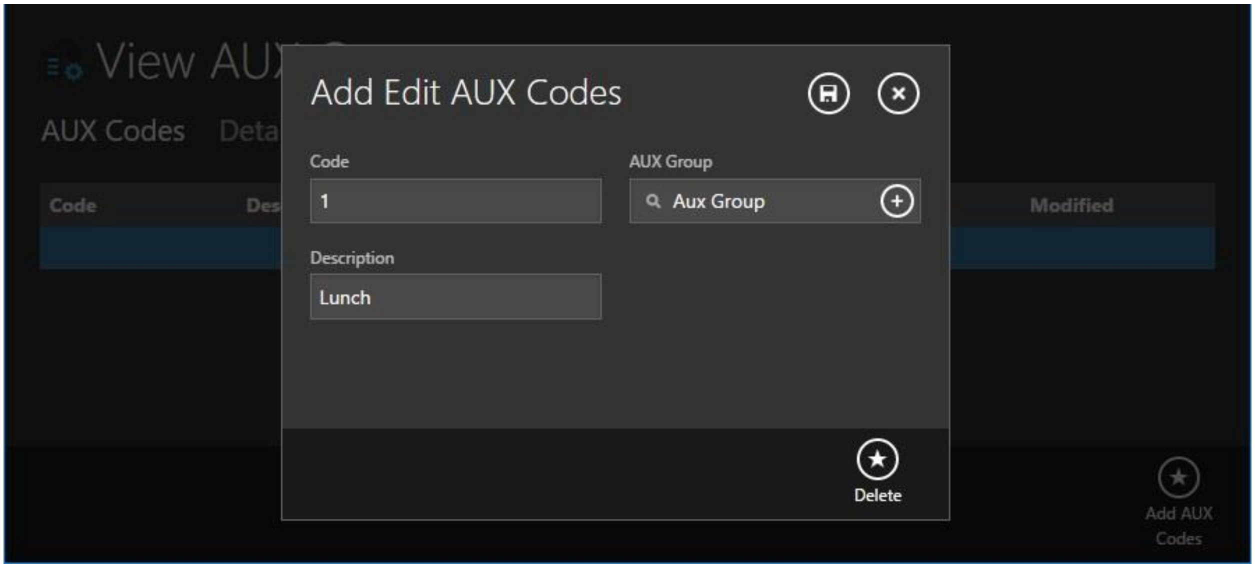
The **View AUX Group** screen is displayed next. Select **Add AUX Codes** from bottom of screen.



Code	Description	Created By	Created	Modified By	Modified
No items					

The **Add Edit AUX Codes** screen is displayed. Enter the following values for specified fields.

- **Code:** The first aux work reason code number from **Section 5.4**.
- **AUX Group:** Select the aux group name created earlier in this section.
- **Description:** The first aux work reason code name from **Section 5.4**.

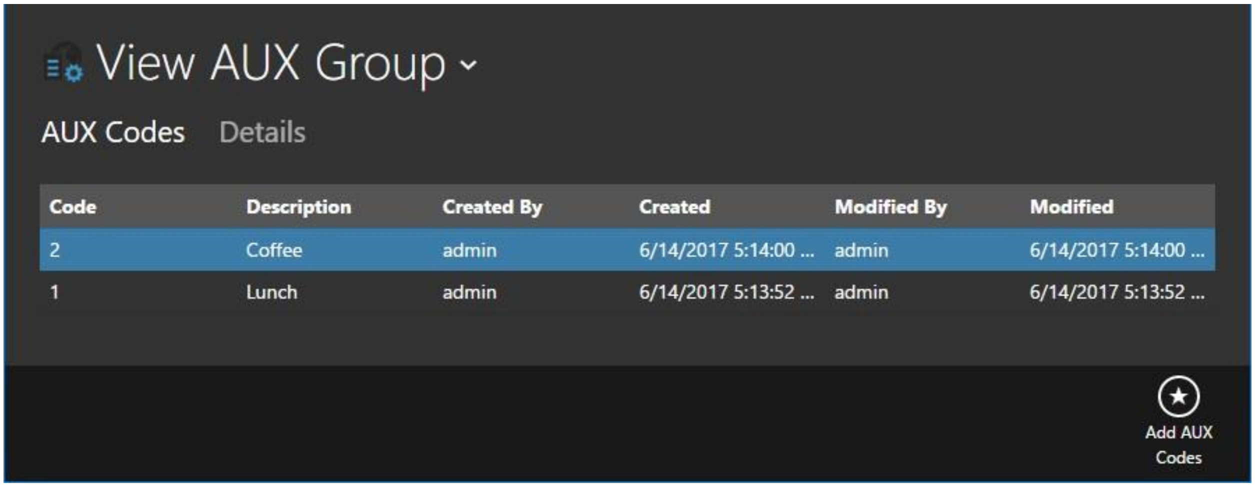


Code: 1

AUX Group: Aux Group

Description: Lunch

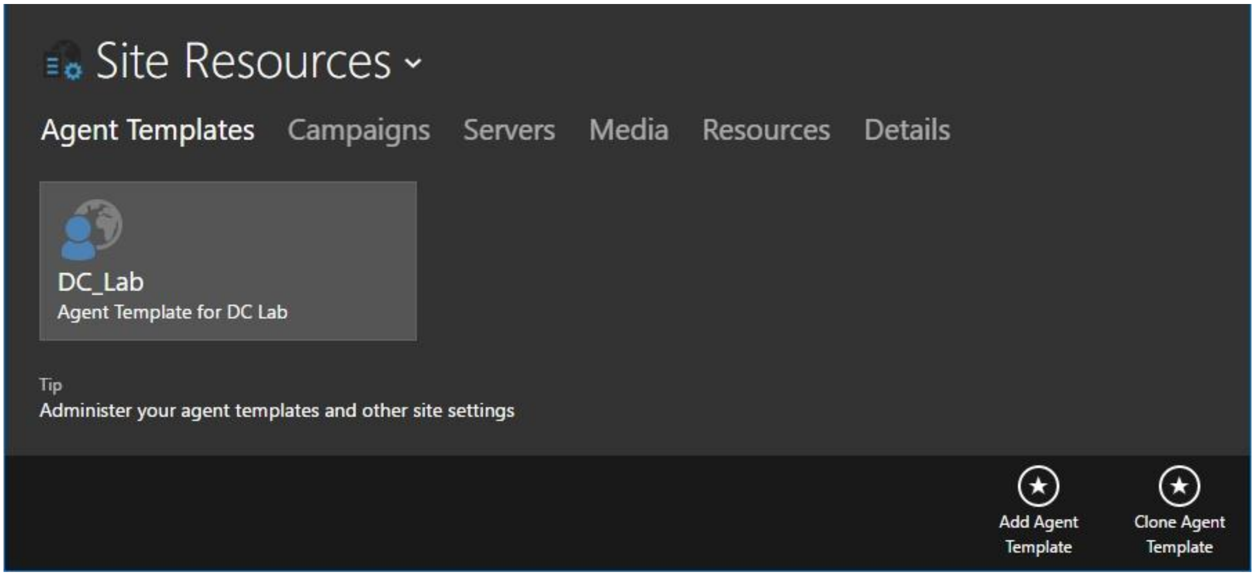
Repeat this section to configure all aux work reason codes from **Section 5.4**. In the compliance testing, two aux work reason codes were configured, as shown below.



Code	Description	Created By	Created	Modified By	Modified
2	Coffee	admin	6/14/2017 5:14:00 ...	admin	6/14/2017 5:14:00 ...
1	Lunch	admin	6/14/2017 5:13:52 ...	admin	6/14/2017 5:13:52 ...

8.6. Administer Agent Templates

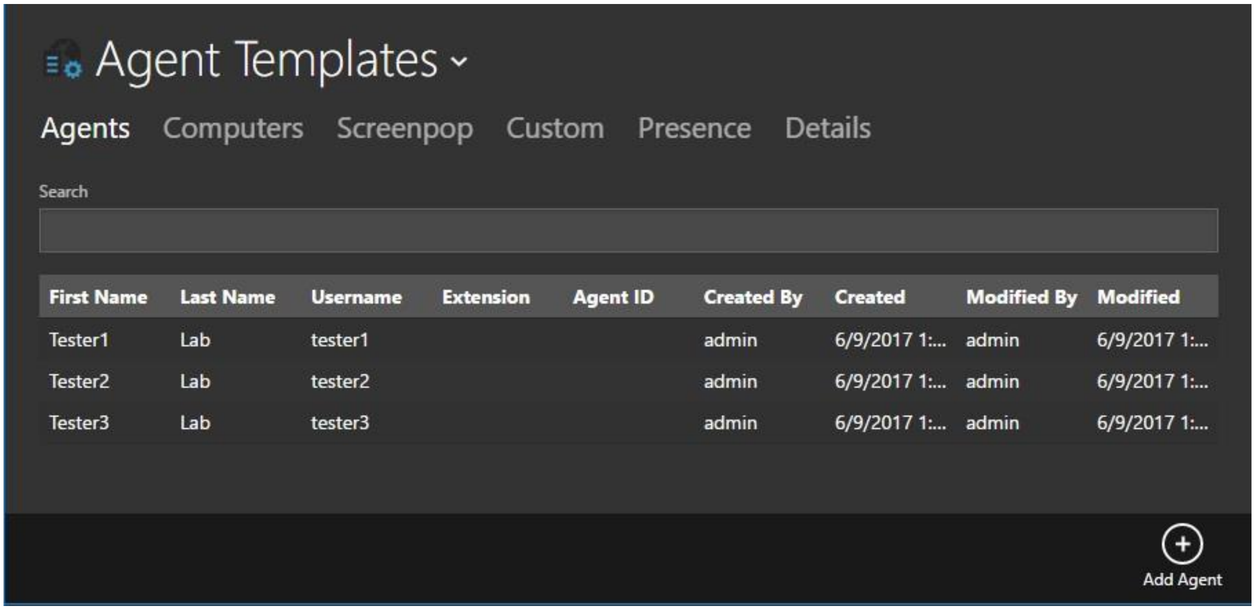
Navigate back to the **Site Resources** screen. Select **Agent Templates** from the top menu, followed by **Add Agent Template** from bottom of screen to add a logical group for agent templates. In the compliance testing, the "DC_Lab" group was pre-configured. Select the newly added group.



Tip
Administer your agent templates and other site settings

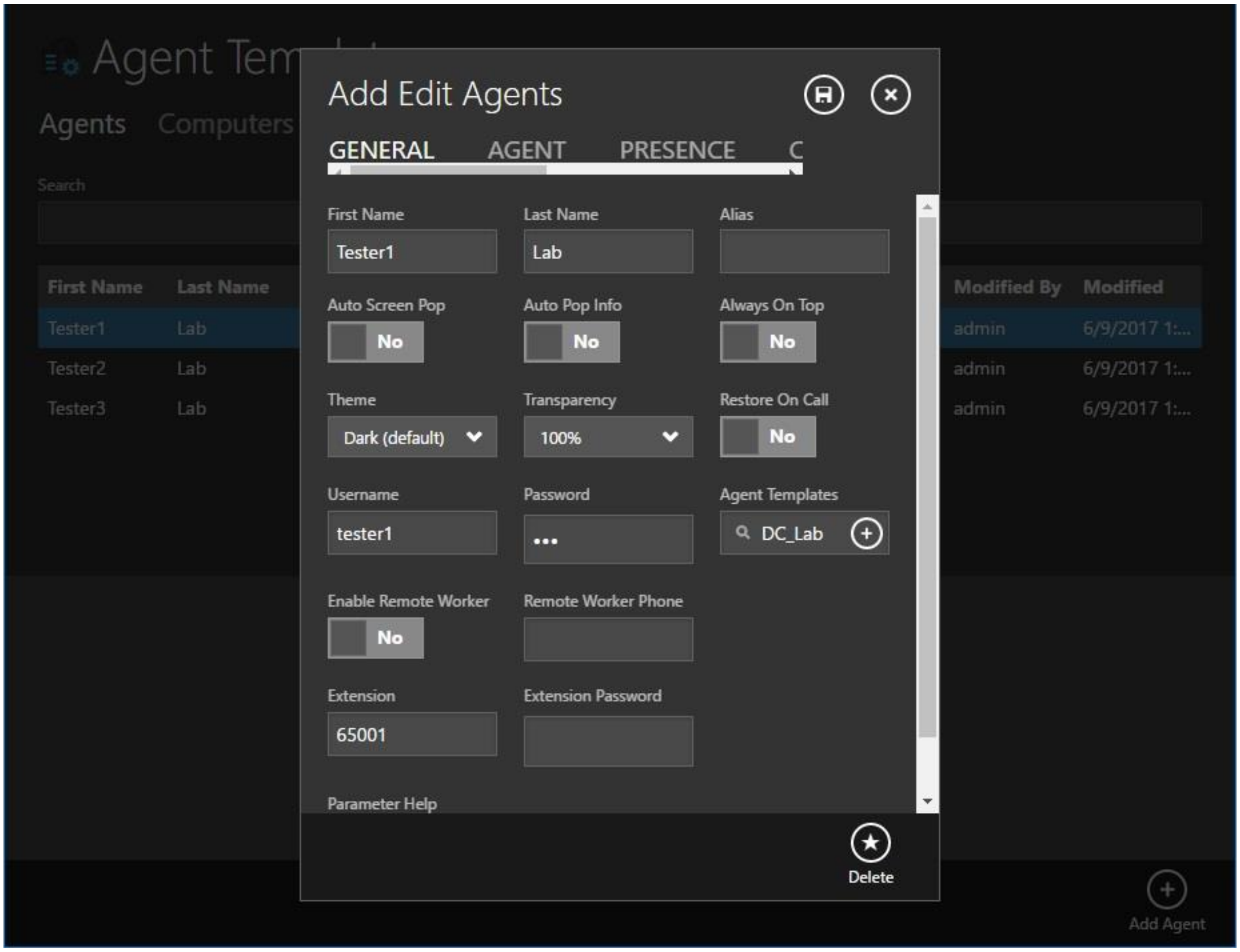
8.6.1. Agents

The **Agent Templates** screen is displayed. Select **Agents** from the top menu, followed by **Add Agent** from bottom of screen to add an agent. In the compliance testing, the three agents shown below were pre-configured. Select the first agent entry, in this case "Tester1".



First Name	Last Name	Username	Extension	Agent ID	Created By	Created	Modified By	Modified
Tester1	Lab	tester1			admin	6/9/2017 1:...	admin	6/9/2017 1:...
Tester2	Lab	tester2			admin	6/9/2017 1:...	admin	6/9/2017 1:...
Tester3	Lab	tester3			admin	6/9/2017 1:...	admin	6/9/2017 1:...

The **Add Edit Agents** screen is displayed. Select the **GENERAL** tab. For **Extension**, enter the relevant agent station extension from **Section 3**. Retain the default values in the remaining fields.



Add Edit Agents

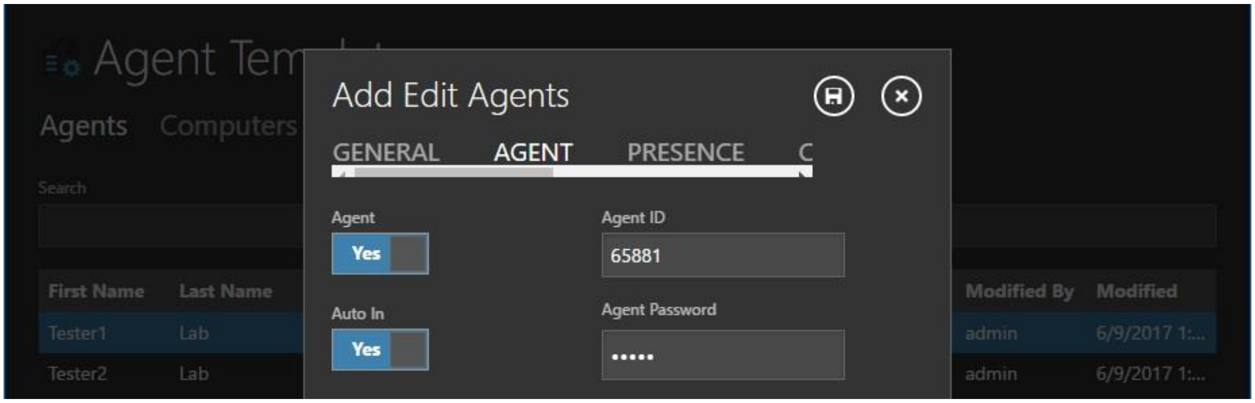
GENERAL AGENT PRESENCE C

First Name: Tester1	Last Name: Lab	Alias:
Auto Screen Pop: No	Auto Pop Info: No	Always On Top: No
Theme: Dark (default)	Transparency: 100%	Restore On Call: No
Username: tester1	Password: •••	Agent Templates: DC_Lab
Enable Remote Worker: No	Remote Worker Phone:	
Extension: 65001	Extension Password:	

Parameter Help

First Name	Last Name	Modified By	Modified
Tester1	Lab	admin	6/9/2017 1:...
Tester2	Lab	admin	6/9/2017 1:...
Tester3	Lab	admin	6/9/2017 1:...

Select the **AGENT** tab. For **Agent ID** and **Agent Password**, enter the relevant agent ID and password from **Section 3**. Retain the default values in the remaining fields.



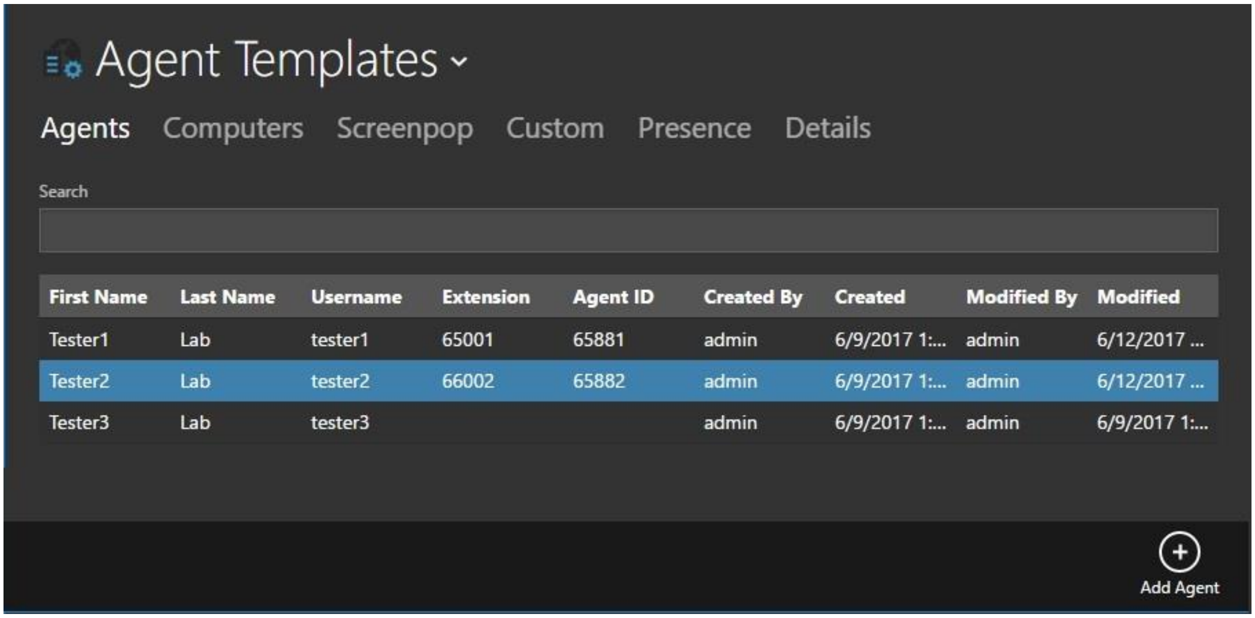
Add Edit Agents

GENERAL AGENT PRESENCE C

Agent: Yes	Agent ID: 65881
Auto In: Yes	Agent Password: •••••

First Name	Last Name	Modified By	Modified
Tester1	Lab	admin	6/9/2017 1:...
Tester2	Lab	admin	6/9/2017 1:...

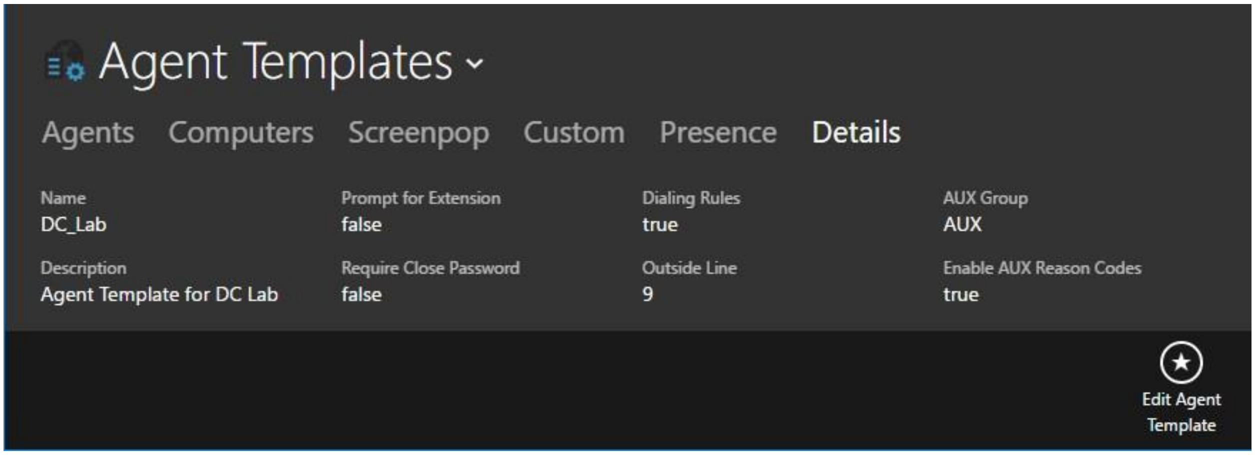
Repeat this section to configure all pertinent agents. In the compliance testing, two agents were configured, as shown below.



First Name	Last Name	Username	Extension	Agent ID	Created By	Created	Modified By	Modified
Tester1	Lab	tester1	65001	65881	admin	6/9/2017 1:...	admin	6/12/2017 ...
Tester2	Lab	tester2	66002	65882	admin	6/9/2017 1:...	admin	6/12/2017 ...
Tester3	Lab	tester3			admin	6/9/2017 1:...	admin	6/9/2017 1:...

8.6.2. Details

Select **Details** from the top menu, followed by **Edit Agent Template** from bottom of screen.



Name
DC_Lab

Description
Agent Template for DC Lab

Prompt for Extension
false

Require Close Password
false

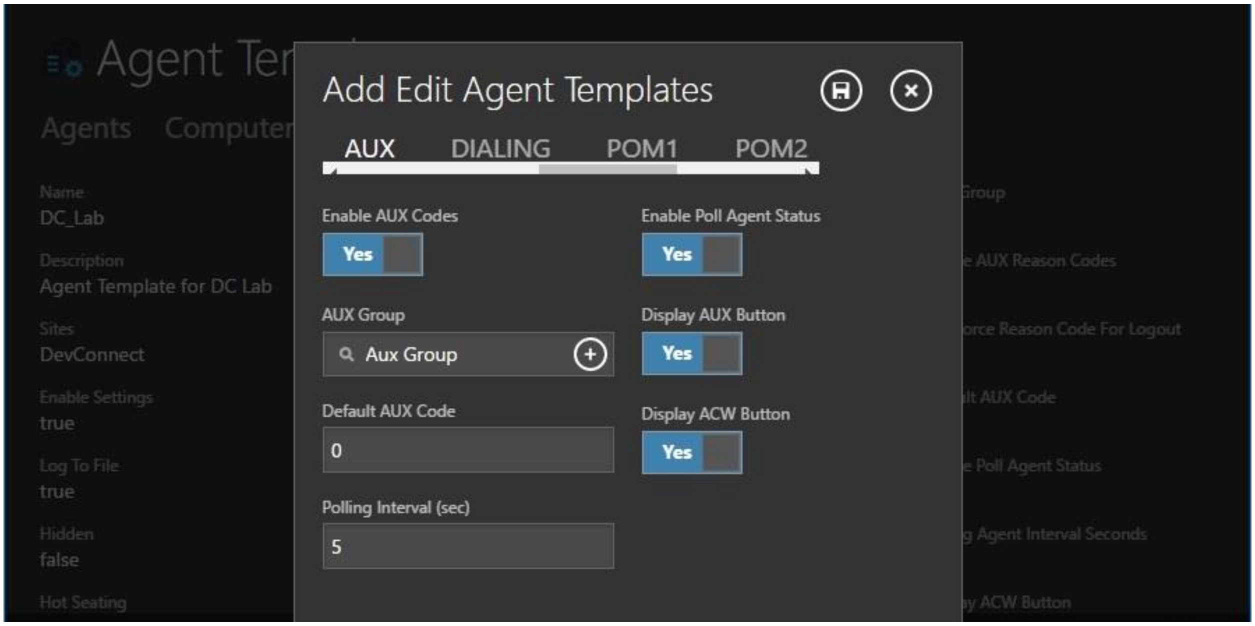
Dialing Rules
true

Outside Line
9

AUX Group
AUX

Enable AUX Reason Codes
true

The **Add Edit Agent Templates** screen is displayed. Scroll the top menu bar as necessary to locate and select the **AUX** tab. Set **Enable AUX Codes** to “Yes”, as shown below. For **AUX Group**, select the aux group from **Section 8.5.2**. Retain the default values in the remaining fields.



Name
DC_Lab

Description
Agent Template for DC Lab

Sites
DevConnect

Enable Settings
true

Log To File
true

Hidden
false

Hot Seating

Add Edit Agent Templates

Enable AUX Codes: Yes

Enable Poll Agent Status: Yes

AUX Group: Aux Group

Display AUX Button: Yes

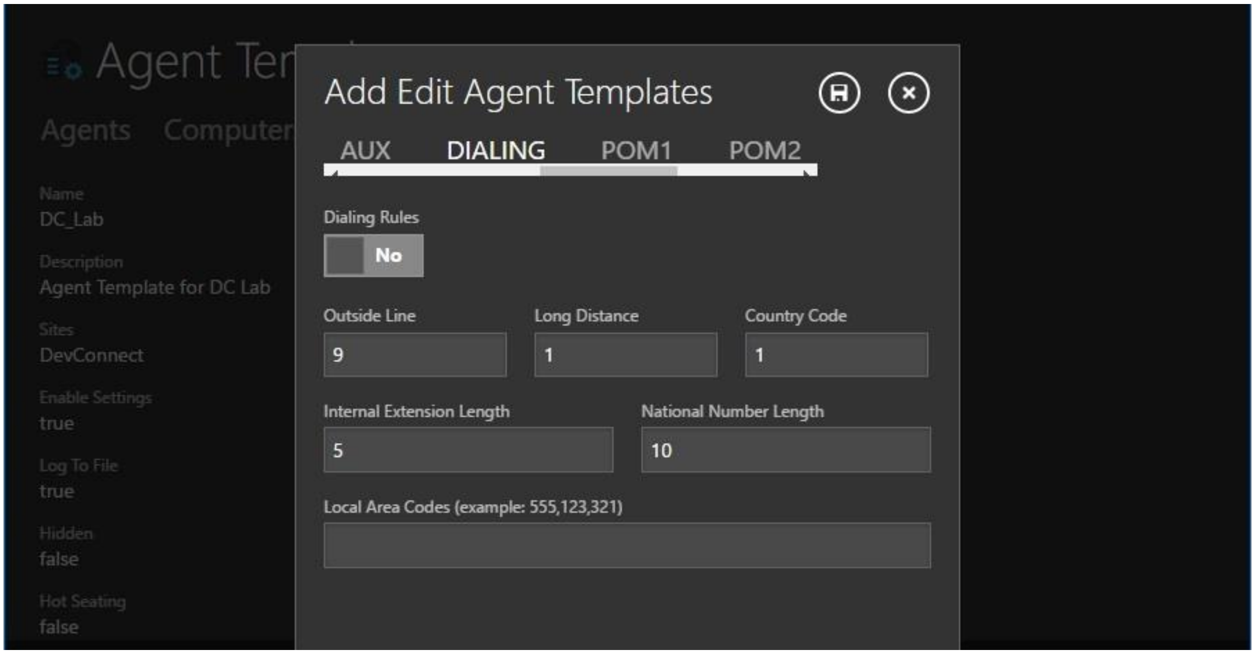
Default AUX Code: 0

Display ACW Button: Yes

Polling Interval (sec): 5

Group
e AUX Reason Codes
orce Reason Code For Logout
lt AUX Code
e Poll Agent Status
g Agent Interval Seconds
y ACW Button

Select the **DIALING** tab. Follow reference [3] to configure parameters to match the customer dialing network. In the compliance testing, **Dialing Rules** was set to “No” for successful testing of click-to-dial for various types of outbound calls, such as international and inter-LATA. With this dialing rules setting, all phone numbers in the contact records were required to be configured with the necessary dialing prefixes.



Name
DC_Lab

Description
Agent Template for DC Lab

Sites
DevConnect

Enable Settings
true

Log To File
true

Hidden
false

Hot Seating
false

Add Edit Agent Templates

Dialing Rules: No

Outside Line: 9

Long Distance: 1

Country Code: 1

Internal Extension Length: 5

National Number Length: 10

Local Area Codes (example: 555,123,321):

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

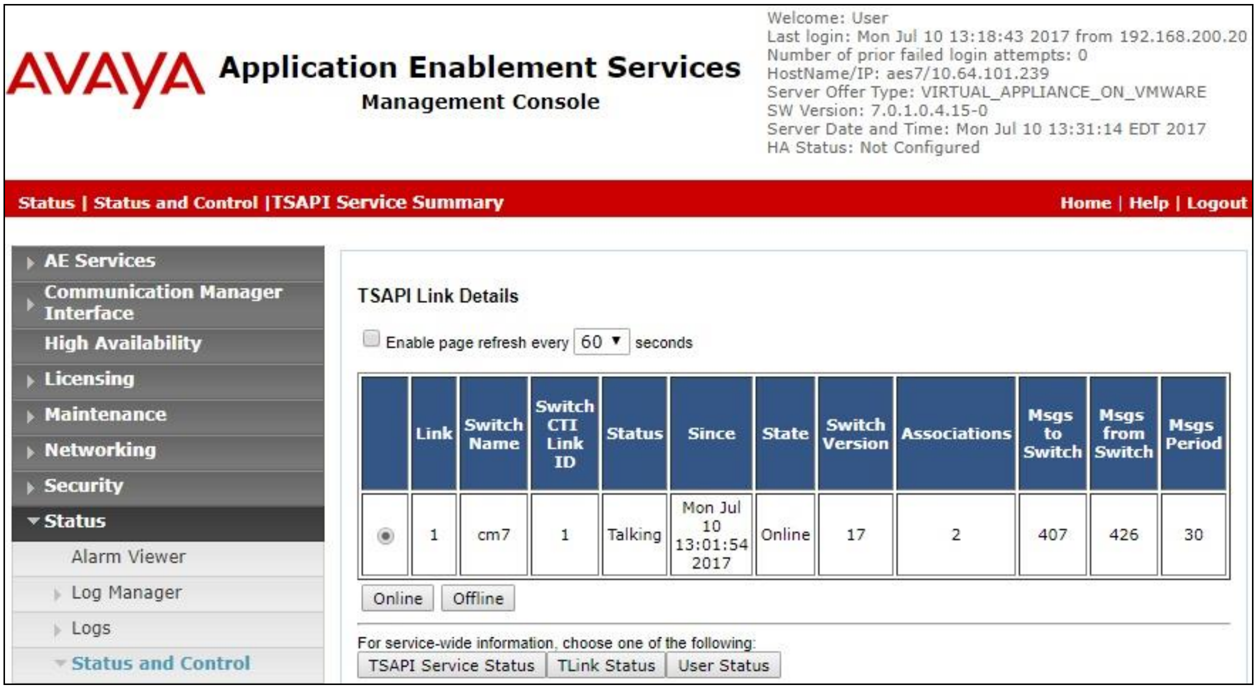
On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
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     aes7              established   418       401
```

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of agents that are logged in, in this case “2”.



Welcome: User
Last login: Mon Jul 10 13:18:43 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jul 10 13:31:14 EDT 2017
HA Status: Not Configured

TSAPI Link Details

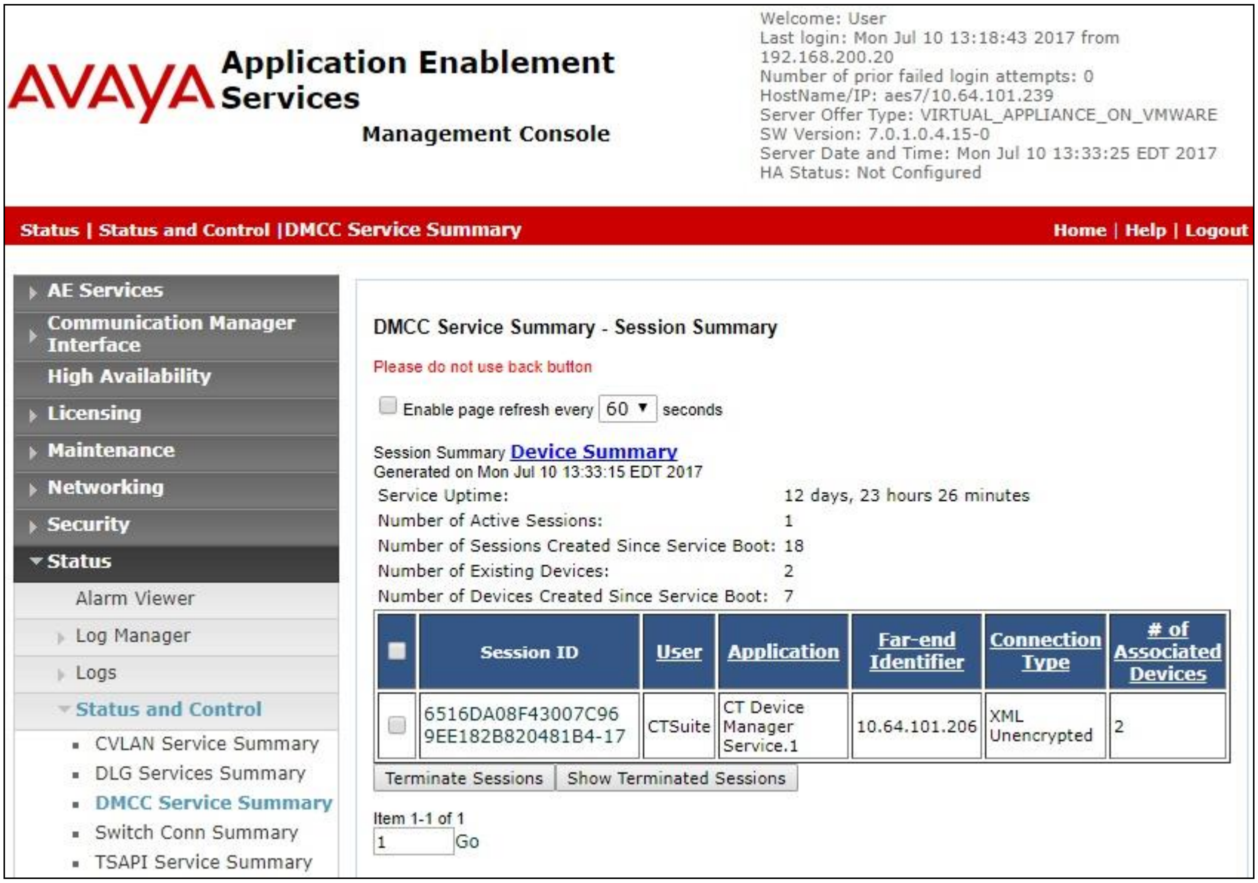
□ Enable page refresh every 60 ▾ seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Mon Jul 10 13:01:54 2017	Online	17	2	407	426	30

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

Verify the status of the DMCC connection 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 an active session with the CT Suite user name from **Section 6.4**, and that the **# of Associated Devices** column reflects the total number of agents that are logged in, in this case "2".



Welcome: User
Last login: Mon Jul 10 13:18:43 2017 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: 7.0.1.0.4.15-0
Server Date and Time: Mon Jul 10 13:33:25 EDT 2017
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 Jul 10 13:33:15 EDT 2017

Service Uptime:	12 days, 23 hours 26 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	18
Number of Existing Devices:	2
Number of Devices Created Since Service Boot:	7

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	6516DA08F43007C96 9EE182B820481B4-17	CTSuite	CT Device Manager Service.1	10.64.101.206	XML Unencrypted	2

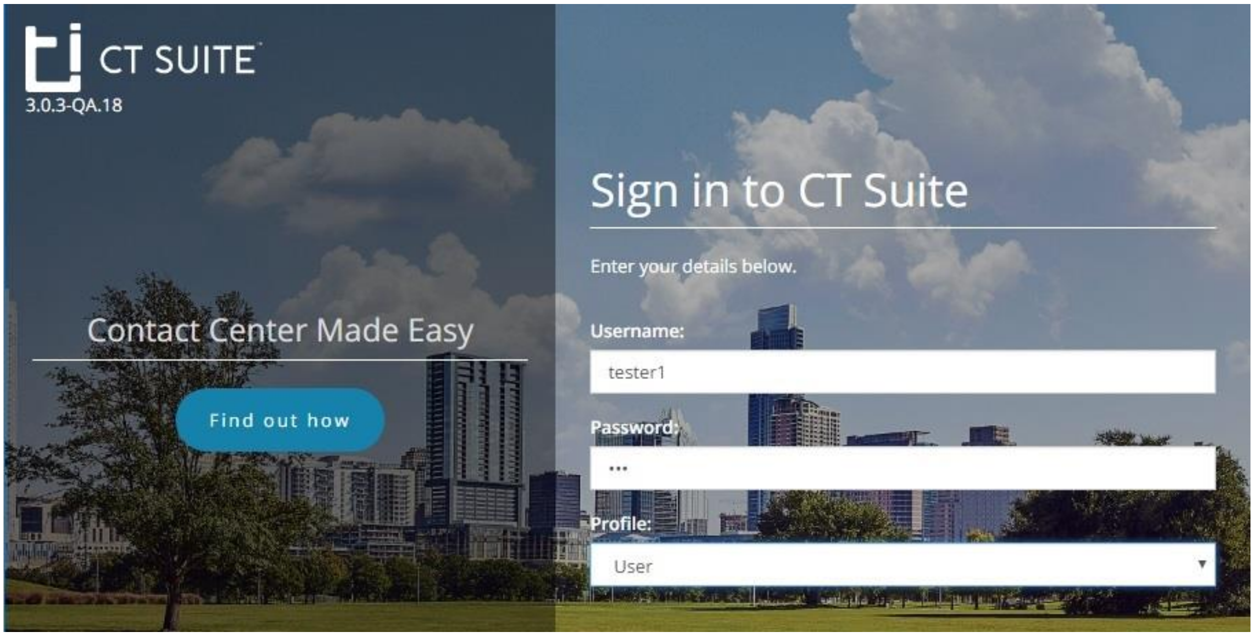
Terminate Sessions | Show Terminated Sessions

Item 1-1 of 1
1 Go

9.3. Verify CTIntegrations CT Suite

From an agent PC, launch an Internet browser window and enter the URL "http://ip-address:8081", where "ip-address" is the IP address of the CT Suite server.

The **Sign in to CT Suite** screen is displayed. For **Username** and **Password**, enter an applicable agent credentials from **Section 8.6.1**, and retain the default value in the remaining field.



Sign in to CT Suite

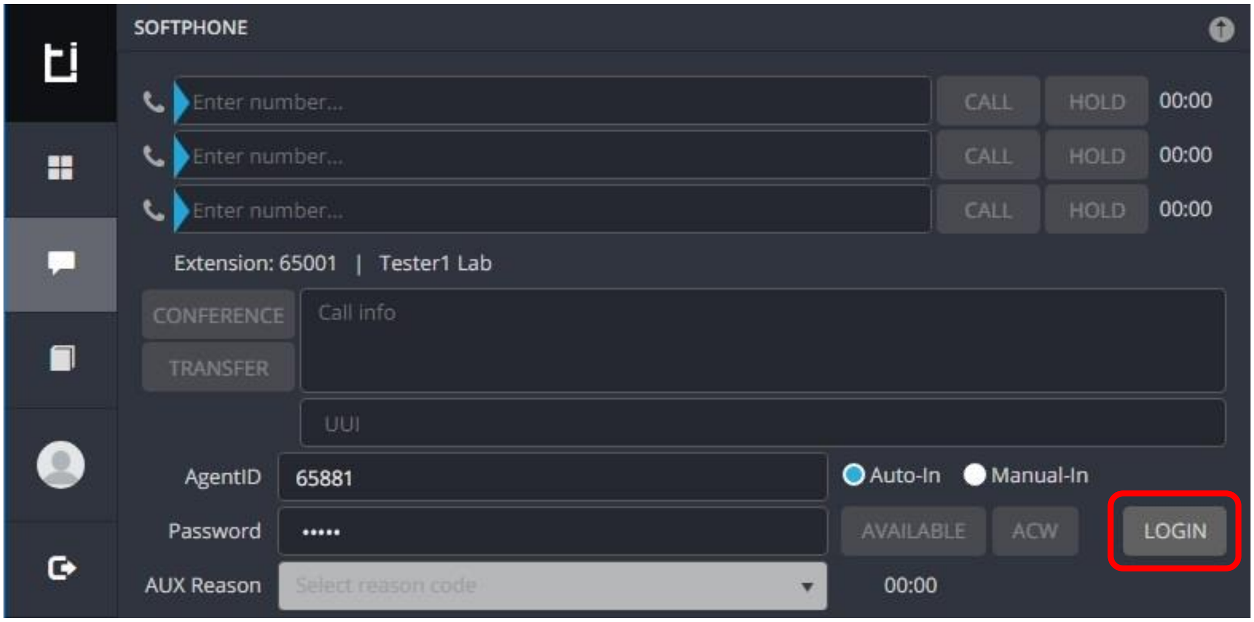
Enter your details below.

Username: tester1

Password: •••

Profile: User

The agent screen below is displayed next. Retain the default values, and select **LOGIN** to log the agent into the ACD on Communication Manager.



Extension: 65001 | Tester1 Lab

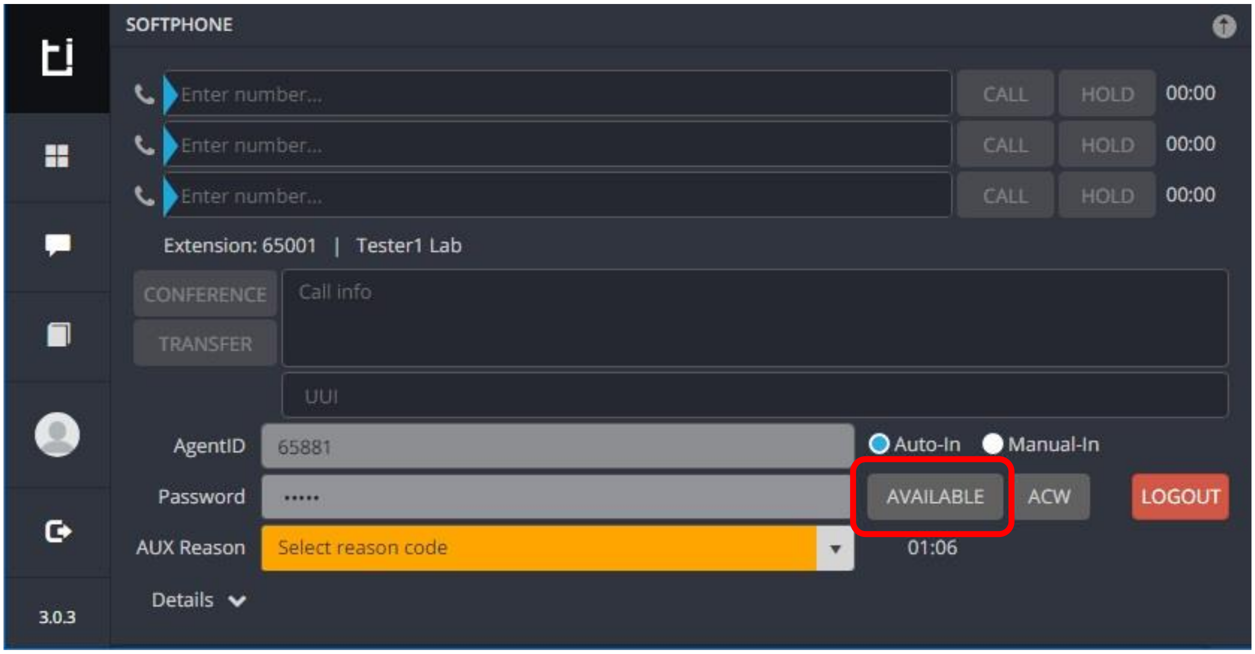
AgentID: 65881

● Auto-In ○ Manual-In

Password: •••••

AUX Reason: Select reason code

The agent screen is updated, as shown below. Click **AVAILABLE**.



Extension: 65001 | Tester1 Lab

AgentID: 65881

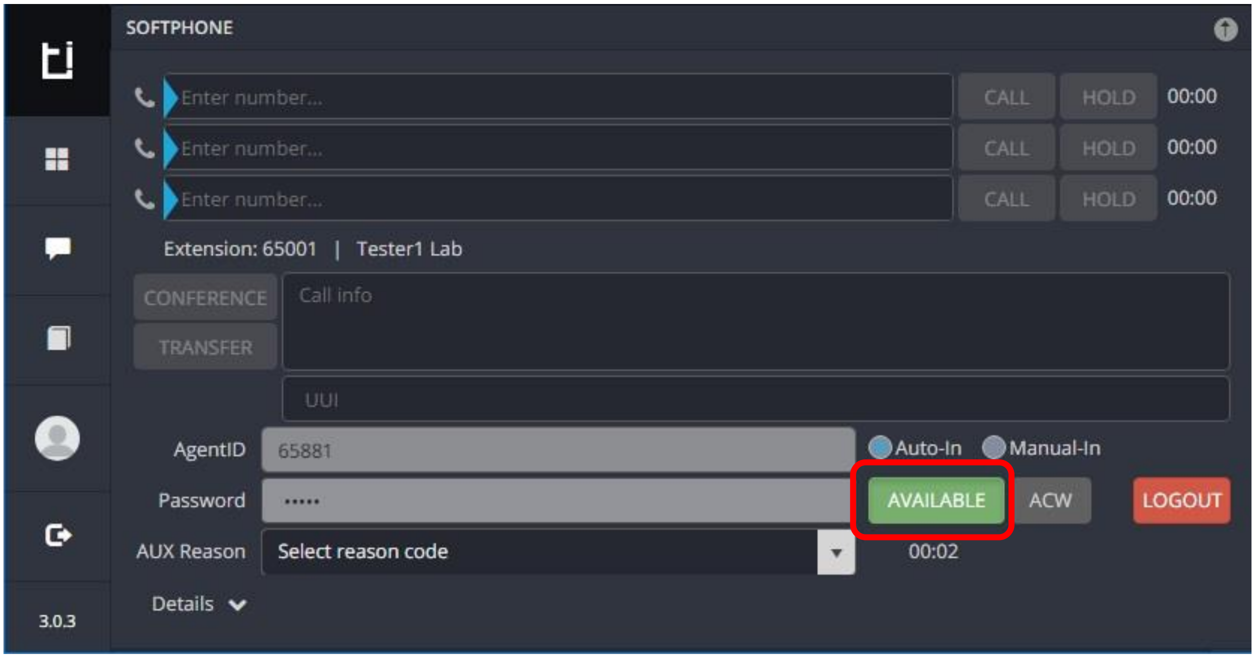
● Auto-In ○ Manual-In

Password: •••••

AUX Reason: Select reason code

01:06

Verify that the agent screen is updated, with the **AVAILABLE** icon shown in green below.



Extension: 65001 | Tester1 Lab

AgentID: 65881

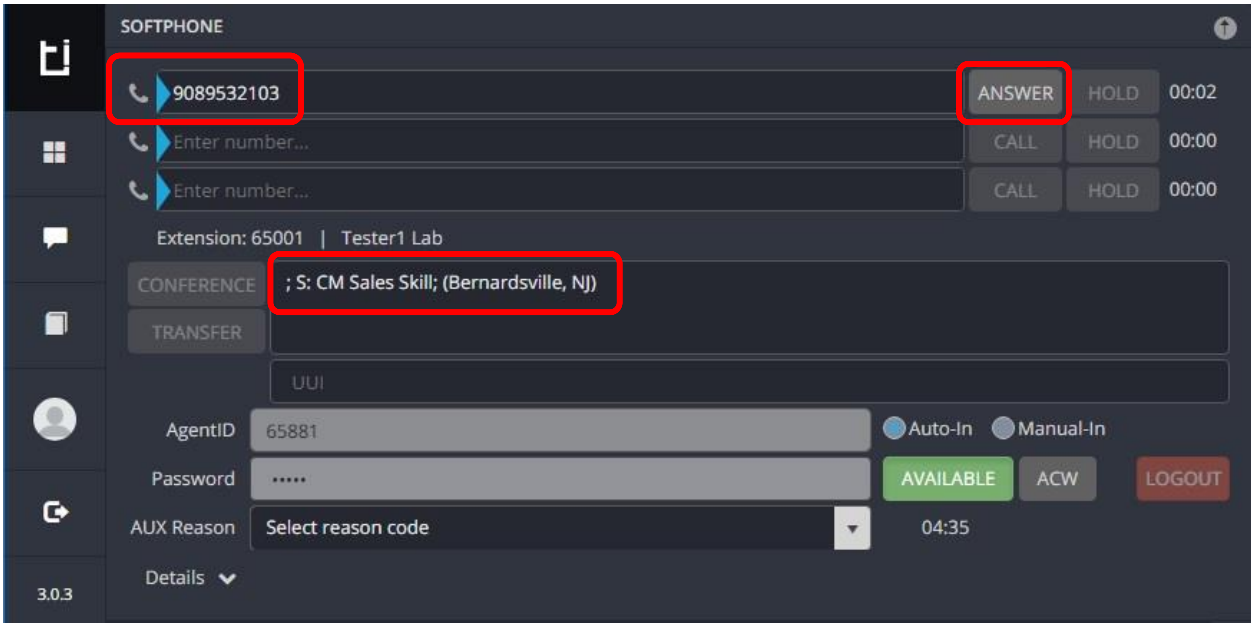
● Auto-In ● Manual-In

Password: •••••

AUX Reason: Select reason code

00:02

Make an incoming ACD call. Verify that the top section of the available agent's screen is updated to reflect the calling party number and name of skill group associated with the called number. In the compliance testing, the pertinent skill group name is "CM Sales Skill". Click **ANSWER**.



9089532103 00:02
Enter number... 00:00
Enter number... 00:00

Extension: 65001 | Tester1 Lab

; S: CM Sales Skill; (Bernardsville, NJ)

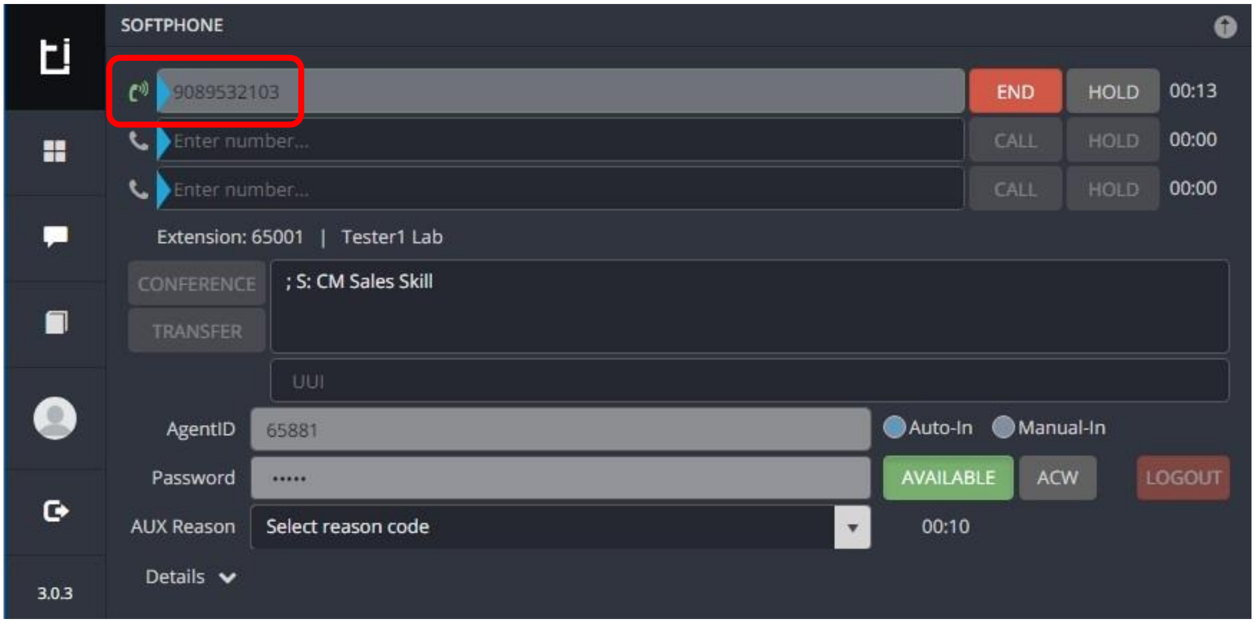
UUI

AgentID 65881

Password •••••

AUX Reason Select reason code 04:35

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



9089532103 00:13
Enter number... 00:00
Enter number... 00:00

Extension: 65001 | Tester1 Lab

; S: CM Sales Skill

UUI

AgentID 65881

Password •••••

AUX Reason Select reason code 00:10

10. Conclusion

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.0 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for voice integration. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at http://support.avaya.com.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at http://support.avaya.com.

3. *CT Admin Administrator's Guide*, CT Suite v3.0, 5/30/17, available at https://www.ctintegrations.com/docs.

4. *CT Suite Web Client*, Web Client User Guide, CT Suite R3.0, 5/30/17, available at https://www.ctintegrations.com/docs.

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.