



Avaya Solution & Interoperability Test Lab

Application Notes for CTIntegrations CT Suite 3.3 with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Application Enablement Services 8.0.1 for Voice Integration – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.3 to interoperate with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Application Enablement Services 8.0.1 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 3.3 to interoperate with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Application Enablement Services 8.0.1 for voice integration. CTIntegrations 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	59101
Skill Group	59001
Agent Station	50001, 50002, 50101
Agent ID	55001, 55002, 55003
Agent Password	123456

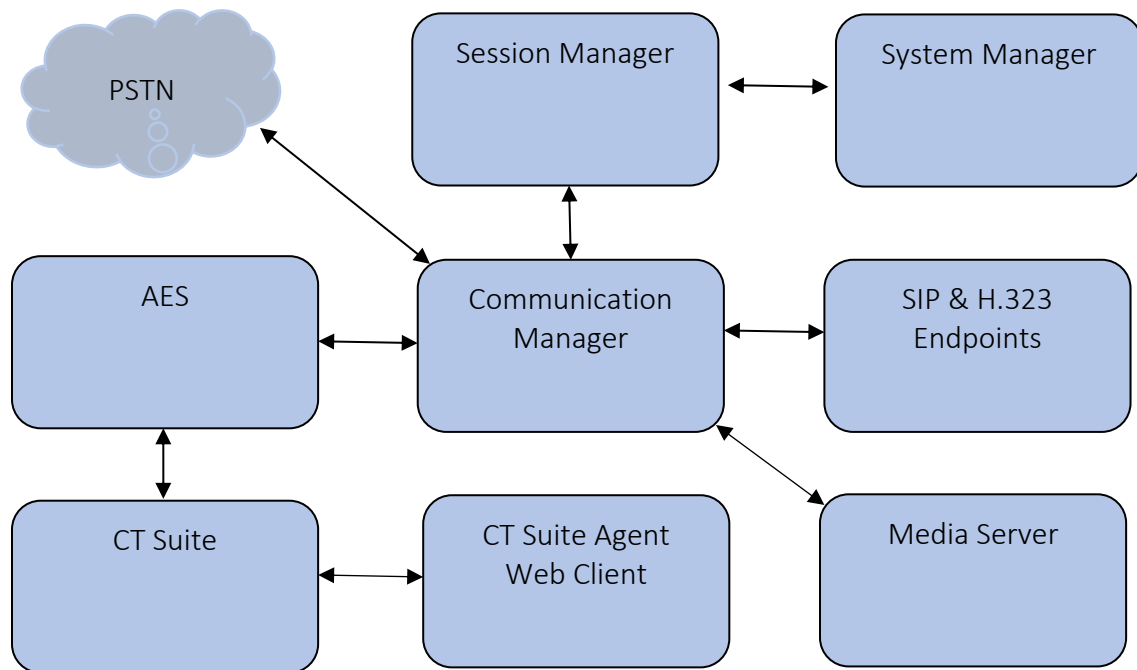


Figure 1: Compliance Testing Configuration

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	8.0.1.1.0-FP1SP1
Avaya Aura® Media Server in Virtual Environment	v.8.0.0.183
Avaya Aura® Application Enablement Services in Virtual Environment	8.0.1.0.2.5-0
Avaya Aura® Session Manager in Virtual Environment	8.0.1.1.801103
Avaya Aura® System Manager in Virtual Environment	8.0.1.1.039340
Avaya 96x1 IP Deskphones (H.323)	6.8102
Avaya 96x1 IP Deskphones (SIP)	7.1.5.0.11
Avaya J169 IP Deskphone (H.323)	6.8102
Avaya Agent for Desktop	1.7.22.1
CTIntegrations CT Suite on Microsoft Windows Server 2016 R2 <ul style="list-style-type: none">• CT Admin• CT Web Client• CT Device Manager• Avaya DMCC .Net SDK	3.3 7.1

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

It is assumed that all extensions are configured as per **Section 3**. Note that for SIP endpoints that are monitored by CT Suite, must have **Type of 3PCC Enabled** to “Avaya.”

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: 59999		
Type: ADJ-IP		
		COR: 1
Name: AES CTI Link 1		
Unicode Name? n		

5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                  Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

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 UI 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.

REASON CODE NAMES		
	Aux Work/ Interruptible?	Logout
Reason Code 1:	Work	/n
Reason Code 2:	Break	/n
Reason Code 3:	Lunch	/n
Reason Code 4:	Training	/n
Reason Code 5:	Water	/n
Reason Code 6:	Bathroom	/n
Reason Code 7:	Dinner	/n
Reason Code 8:	Walk	/n
Reason Code 9:	Run	/n
Default Reason Code: 2		

6. Configure Avaya Aura® Application Enablement Services

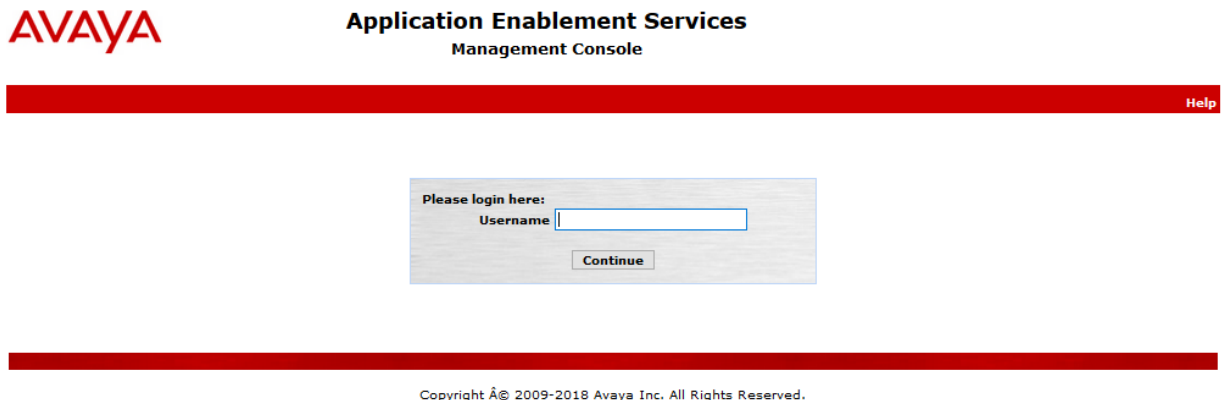
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a login box with the text "Please login here:" and "Username" followed by a text input field. A "Continue" button is located below the input field. At the bottom of the page, a red horizontal bar contains the copyright notice: "Copyright © 2009-2018 Avaya Inc. All Rights Reserved."

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



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri May 24 10:50:55 2019 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes8/10.64.110.132
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.2.5-0
Server Date and Time: Fri May 24 10:52:24 MDT 2019
HA Status: Not Configured

Home

Home | Help | Logout

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

Welcome to OAM


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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status information.
- 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).



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri May 24 10:50:55 2019 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes8/10.64.110.132
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.1.0.2.5-0
Server Date and Time: Fri May 24 10:52:58 MDT 2019
HA Status: Not Configured

Licensing

Home | Help | Logout

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

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 agent monitoring and call control via DMCC.

▼ Application_Enablement	License File Host IDs: VC-3B-2C-EE-93-9D-01		
View license capacity			
View peak usage			
CE	Licensed Features		
► COLLABORATION_ENVIRONMENT			
CMM	13 Items  Show <input type="text" value="All"/>		
► Communication_Manager_Messaging	Feature (License Keyword)	Expiration date	Licensed capacity
Configure Centralized Licensing	Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
COMMUNICATION_MANAGER	AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	8
► Call_Center	AES HA LARGE VALUE_AES_HA_LARGE	permanent	8
► Communication_Manager	AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	8
► Dialog_Designer	Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
IPO	CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	8
► IP_Office	AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	8
MSR	AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	8
► Media_Server	DLG VALUE_AES_DLG	permanent	8
ORCHESTRATION_DESIGNER_IDE	TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
► Orchestration_Designer_IDE	CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	8
POM			
► POM			
SYSTEM_MANAGER			
► System_Manager			

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**.

The screenshot shows the 'TSAPI Links' management interface. On the left is a navigation pane with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), and 'TWS'. Under 'TSAPI', 'TSAPI Links' is selected. The main area is titled 'TSAPI Links' and contains a table with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm8	1	8	Both

Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

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 “cm8” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Select “Both” from the **Security** drop down. Retain the default values in the remaining fields.

The screenshot shows the 'Edit TSAPI Links' form. The left navigation pane is the same as in the previous screenshot. The main area is titled 'Edit TSAPI Links' and contains the following form fields:

- Link: 1
- Switch Connection: cm8 (dropdown)
- Switch CTI Link Number: 1 (dropdown)
- ASAI Link Version: 8 (dropdown)
- Security: Both (dropdown)

At the bottom of the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

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.

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

ctinteg

* Common Name

ctinteg

* Surname

ctinteg

* 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

6.5. Administer Security Database

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the left pane, to display all the users. Select the recently added User and select **Edit**.

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> aessim	aessim	NONE	NONE
<input type="radio"/> ctinteg	ctinteg	NONE	NONE
<input checked="" type="radio"/> ctuser	ctuser	NONE	NONE
<input type="radio"/> interop	interop	NONE	NONE
<input type="radio"/> redsky	redsky	NONE	NONE
<input type="radio"/> spokmcs	spokmcs	NONE	NONE
<input type="radio"/> spokscs	spokscs	NONE	NONE
<input type="radio"/> spokss	spokss	NONE	NONE
<input type="radio"/> sureconnect	sureconnect	NONE	NONE
<input type="radio"/> tenfold	tenfold	NONE	NONE

EditList All

Check box for **Unrestricted Access** for the User.

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

ctuser

ctuser

NONE ▾

☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▾

Call and Device Monitoring:

Device Monitoring

Calls On A Device Monitoring

Call Monitoring

None ▾

None ▾

☐

Routing Control:

Allow Routing on Listed Devices

None ▾

Apply ChangesCancel Changes

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.

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

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**.

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

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

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

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 Unencrypted Tlink name, to be used later for configuring CT Suite.

The screenshot shows the Avaya CT Suite web interface. At the top, a red navigation bar contains the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with various categories: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", and "Security Database". The "Security Database" category is expanded, showing sub-items: "Control", "CTI Users", "Devices", "Device Groups", "Tlinks" (highlighted in blue), and "Tlink Groups". The main content area on the right is titled "Tlinks". It contains a section labeled "Tlink Name" with two radio button options: "AVAYA#CM8#CSTA#AES8" (which is selected) and "AVAYA#CM8#CSTA-S#AES8". Below these options is a button labeled "Delete Tlink".

7. Configure CTIntegrations CT Suite

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

- Launch CT Admin interface
- Administer site
- Administer resources
- Administer agent templates
- Administer AES server

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

7.1. 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 v3.3.0

Log In

[Security Admin](#)

Username:

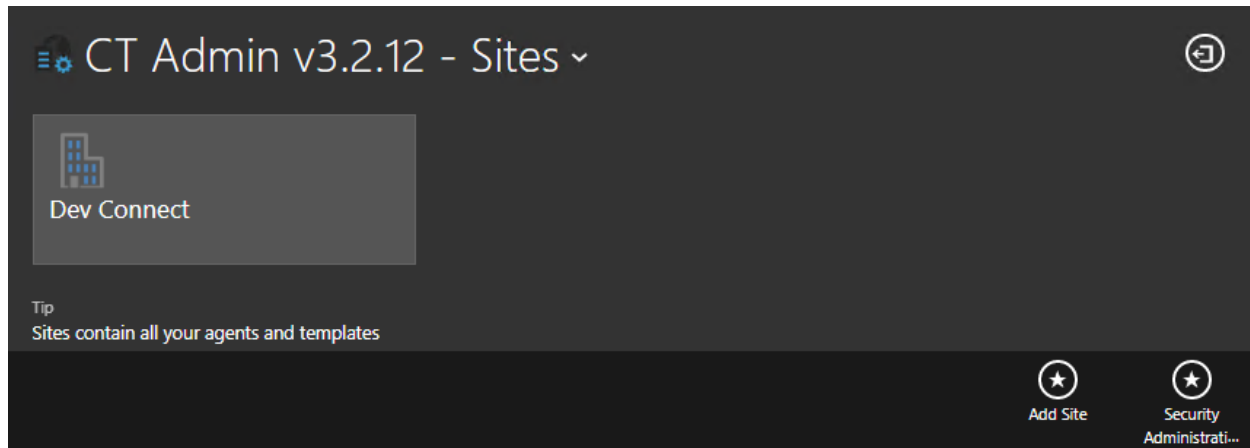
Password:

☐ Remember me next time.

LOG IN

7.2. Administer Site

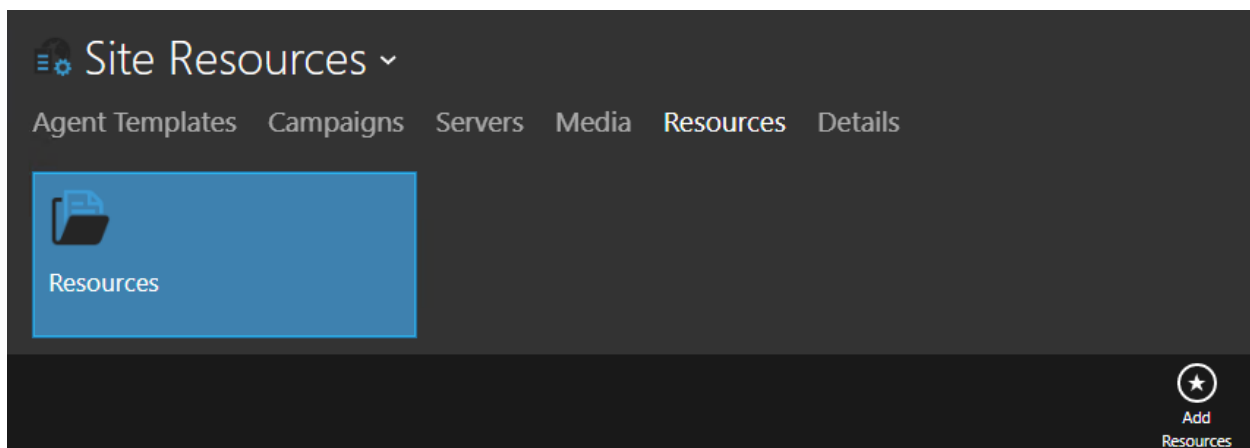
The **Sites** screen below is displayed next. Select **Add Site** from bottom of screen to add a site. In the compliance testing, the “Dev Connect” site was pre-configured. Select the pertinent newly added site, in this case “Dev Connect”.



7.3. 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.

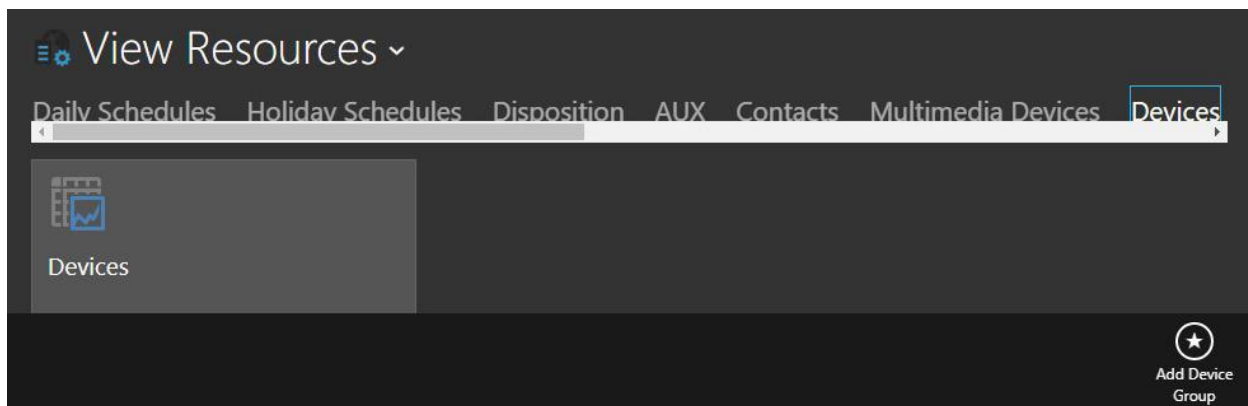
In the compliance testing, the “Resources” group was pre-configured. Select the newly added group.



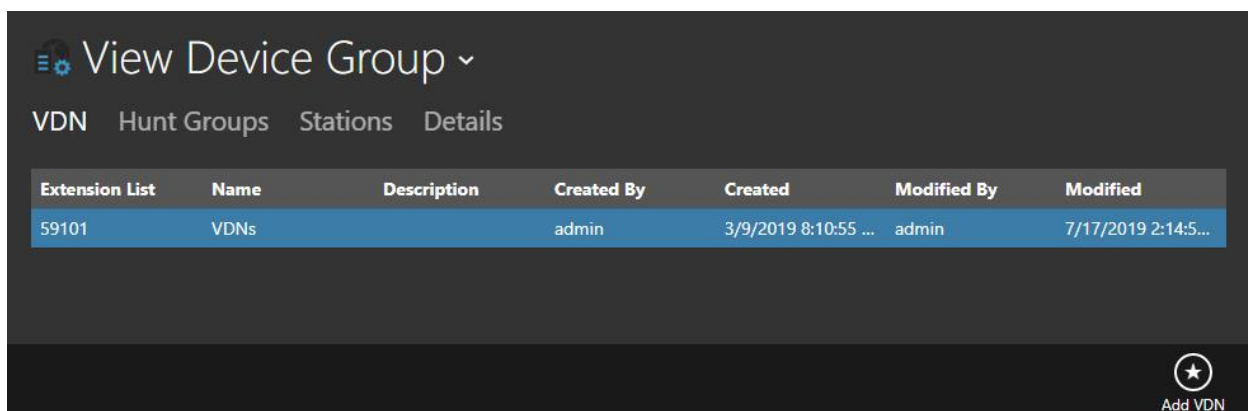
7.3.1. Devices

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 “Devices” group was pre-configured. Select the newly added group.



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



The **Add VDN** 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 description, if desired.
- **Extension List:** The VDN extension from **Section 3**.

The screenshot shows a dark-themed application interface. In the background, there's a 'View Device' screen with a table showing 'Extension List' and 'Name' columns, with one row containing '59101' and 'VDNs'. Overlaid on this is a modal dialog titled 'Add Edit VDN'. The dialog contains the following fields:

- Name:** A text input field containing 'VDNs'.
- Device Group:** A dropdown menu showing 'Devices' with a search icon and a plus button.
- Description:** A large empty text area.
- Extension List (Separate each group by a comma):** A text input field containing '59101'.

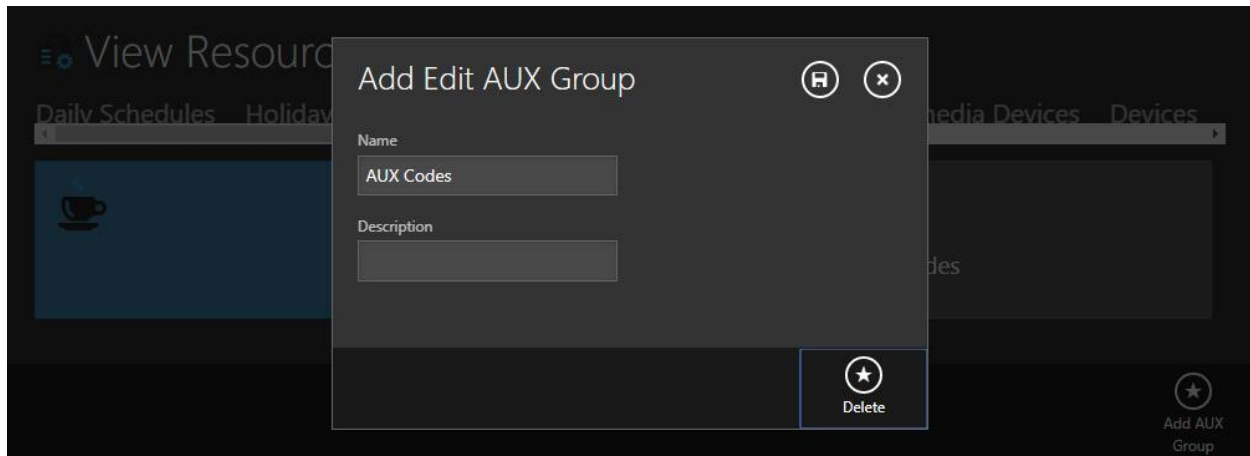
At the bottom of the dialog, there is a 'Delete' button (star icon) and an 'Add VDN' button (star icon). The background also shows a table with 'Modified By' and 'Modified' columns, with one row showing '7/17/2019 2:14:58...'.

7.3.2. AUX

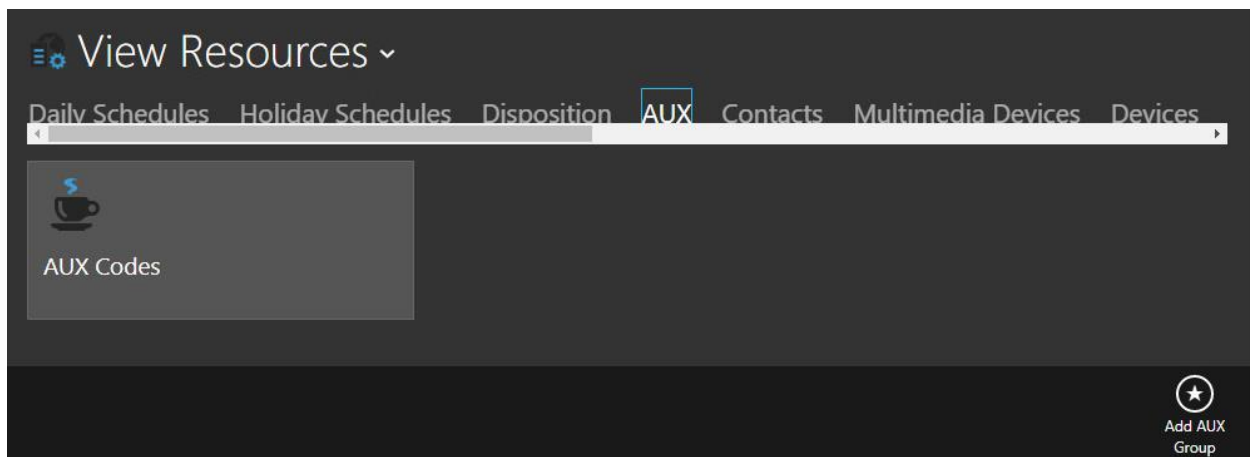
Navigate back to the **View Resources** screen. Scroll the top menu bar as necessary to locate and select **AUX**, followed by **Add AUX Group** from bottom of screen to add a logical group for aux codes.

The screenshot shows the 'View Resources' screen with a dark theme. The top navigation bar has a scrollable menu with items: 'Daily Schedules', 'Holiday Schedules', 'Disposition', 'AUX', 'Contacts', 'Multimedia Devices', and 'Devices'. The 'AUX' item is currently selected. Below the menu, the main content area is mostly empty. At the bottom right corner, there is a button with a star icon and the text 'Add AUX Group'.

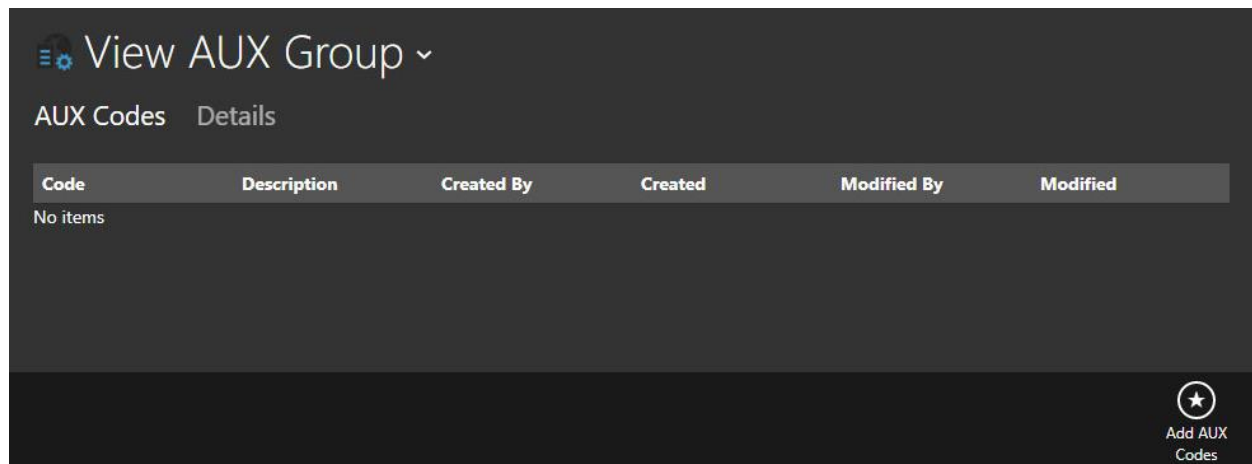
The **Add Edit AUX Group** screen is displayed next. Enter desired values for **Name** and **Description**, as shown below.



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

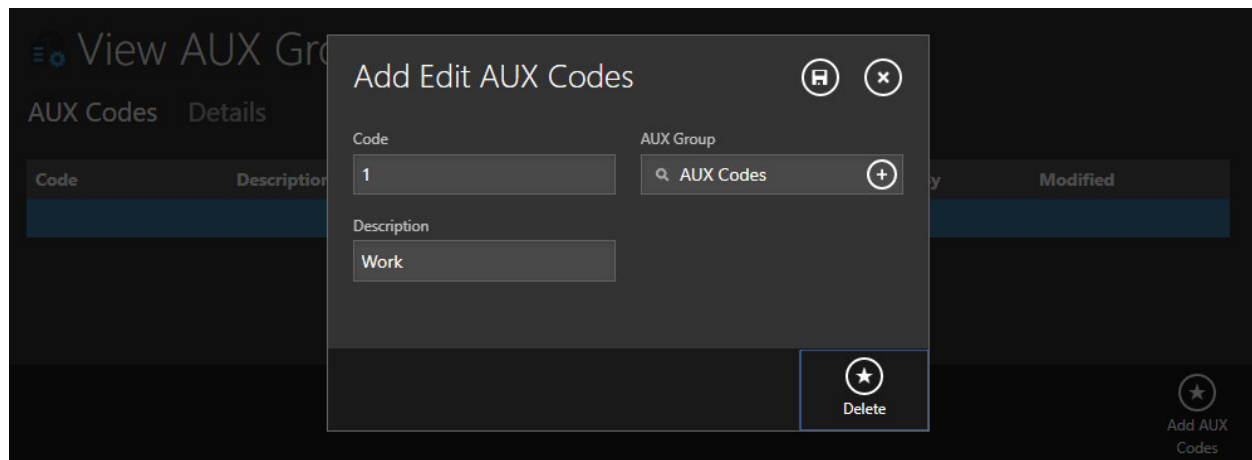


The **View AUX Group** screen is displayed next. Select **Add AUX Codes** from bottom of screen.

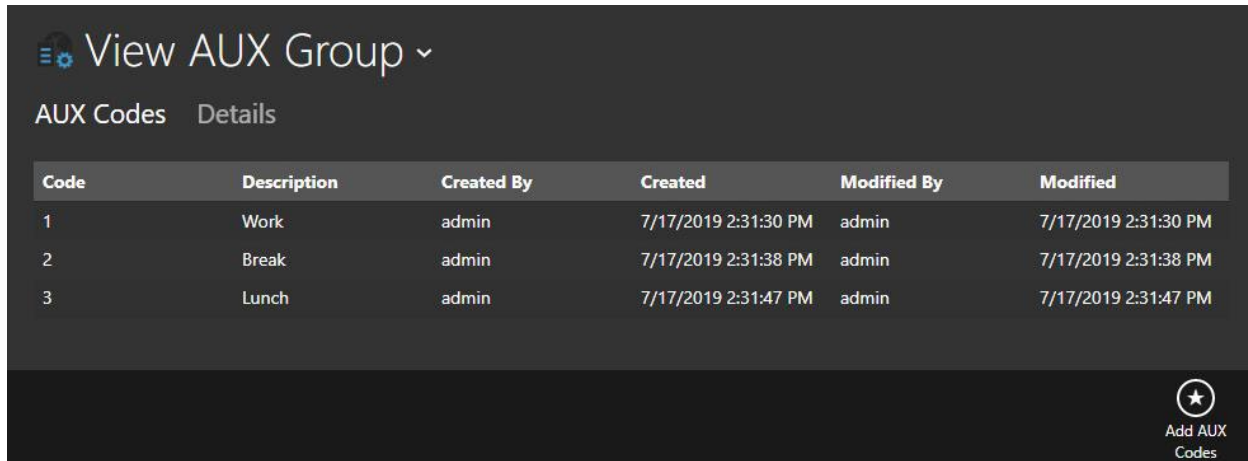


The **Add Edit AUX Codes** screen is displayed. Enter the following values for specified fields.

- **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**.



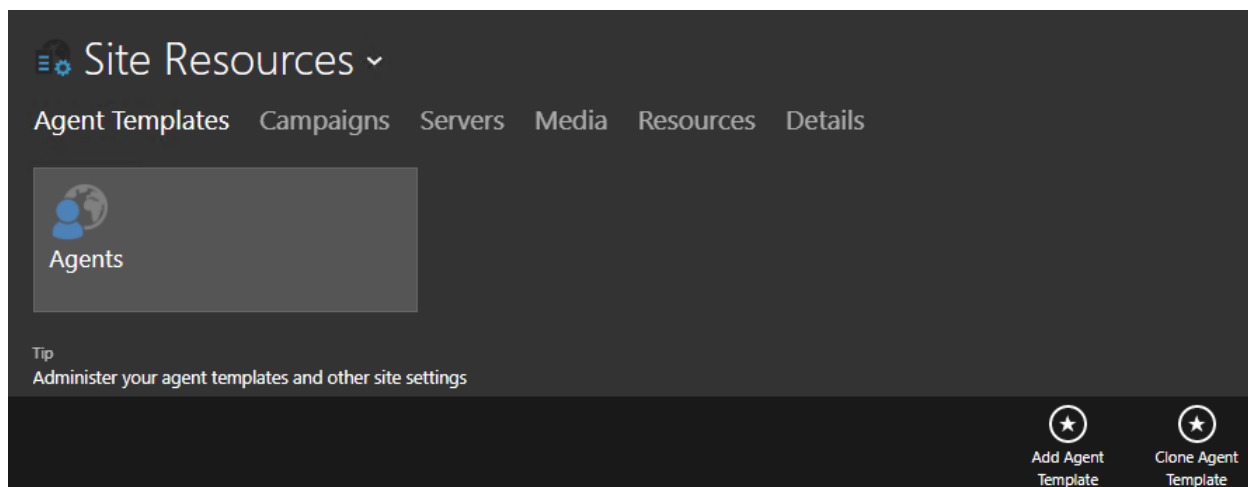
Repeat this section to configure all aux work reason codes from **Section 5.4**. In the compliance testing, first three aux work reason codes were configured, as shown below.

A screenshot of the 'View AUX Group' interface. At the top, there's a header 'View AUX Group' with a dropdown arrow. Below it are two tabs: 'AUX Codes' (selected) and 'Details'. The main content is a table with six columns: 'Code', 'Description', 'Created By', 'Created', 'Modified By', and 'Modified'. The table contains three rows of data. At the bottom right, there is a circular button with a star icon and the text 'Add AUX Codes'.

Code	Description	Created By	Created	Modified By	Modified
1	Work	admin	7/17/2019 2:31:30 PM	admin	7/17/2019 2:31:30 PM
2	Break	admin	7/17/2019 2:31:38 PM	admin	7/17/2019 2:31:38 PM
3	Lunch	admin	7/17/2019 2:31:47 PM	admin	7/17/2019 2:31:47 PM

7.4. 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 “Agents” group was pre-configured. Select the newly added group.

A screenshot of the 'Site Resources' interface. At the top, there's a header 'Site Resources' with a dropdown arrow. Below it are several tabs: 'Agent Templates' (selected), 'Campaigns', 'Servers', 'Media', 'Resources', and 'Details'. The main content area shows a large grey box with a globe icon and the text 'Agents'. Below this box is a 'Tip' section with the text 'Administer your agent templates and other site settings'. At the bottom right, there are two circular buttons with star icons: 'Add Agent Template' and 'Clone Agent Template'.

Site Resources

Agent Templates Campaigns Servers Media Resources Details

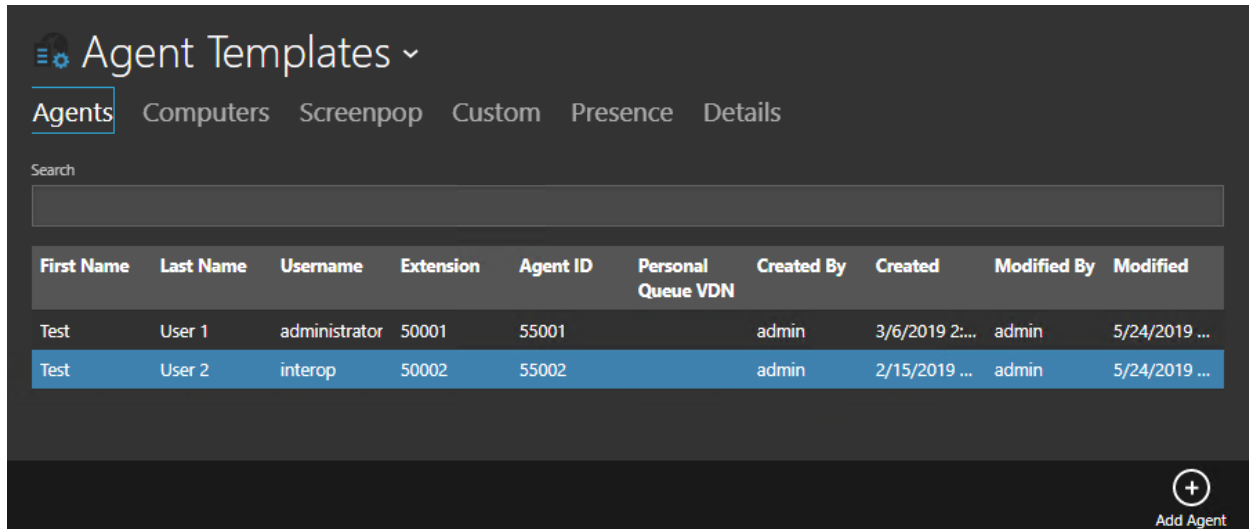
Agents

Tip
Administer your agent templates and other site settings

Add Agent Template Clone Agent Template

7.4.1. 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 two agents shown below were pre-configured. Select the first agent entry, in this case “Test User 1”.



The screenshot shows the 'Agent Templates' interface. At the top, there is a header 'Agent Templates' with a dropdown arrow. Below it, a navigation bar contains tabs: 'Agents' (highlighted), 'Computers', 'Screenpop', 'Custom', 'Presence', and 'Details'. A search bar is located below the tabs. The main area displays a table of agents. The table has columns: 'First Name', 'Last Name', 'Username', 'Extension', 'Agent ID', 'Personal Queue VDN', 'Created By', 'Created', 'Modified By', and 'Modified'. Two agents are listed: 'Test User 1' (administrator, 50001, 55001) and 'Test User 2' (interop, 50002, 55002). The second agent is highlighted. At the bottom right, there is a button with a plus icon and the text 'Add Agent'.

First Name	Last Name	Username	Extension	Agent ID	Personal Queue VDN	Created By	Created	Modified By	Modified
Test	User 1	administrator	50001	55001		admin	3/6/2019 2:...	admin	5/24/2019 ...
Test	User 2	interop	50002	55002		admin	2/15/2019 ...	admin	5/24/2019 ...

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.

The screenshot shows the 'Add Edit Agents' dialog box with the 'GENERAL' tab selected. The fields are as follows:

Field	Value
First Name	Test
Last Name	User 1
Alias	
Auto Screen Pop	No
Auto Pop Info	No
Always On Top	No
Theme	Dark
Transparency	100%
Restore On Call	No
Username	administrator
Password	...
Agent Templates	Agents
Enable Remote Worker	No
Remote Worker Phone	
Language	English
Extension	50001
Extension Password

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.

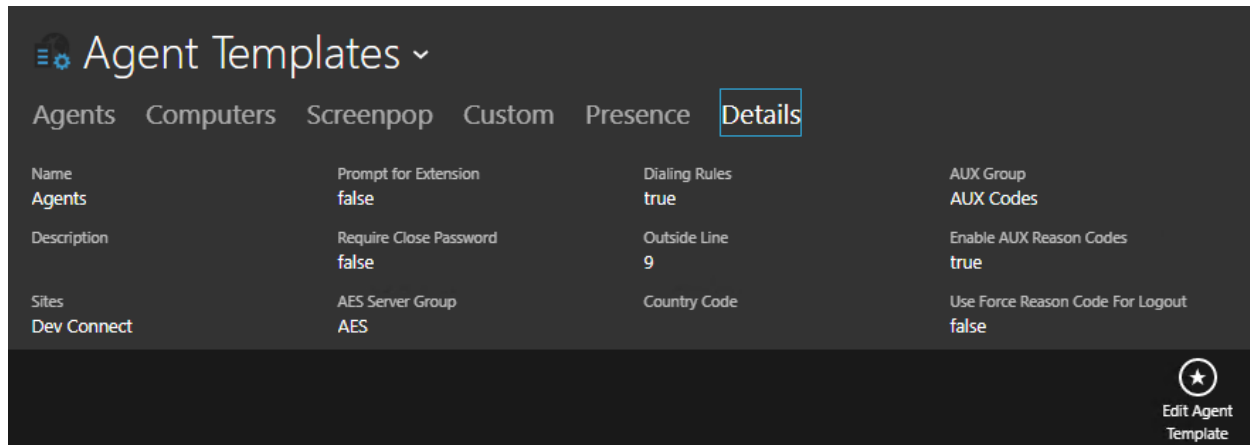
The screenshot shows the 'Add Edit Agents' dialog box with the 'AGENT' tab selected. The fields are as follows:

Field	Value
Agent	Yes
Agent ID	55001
Auto In	Yes
Agent Password

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

7.4.2. Details

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

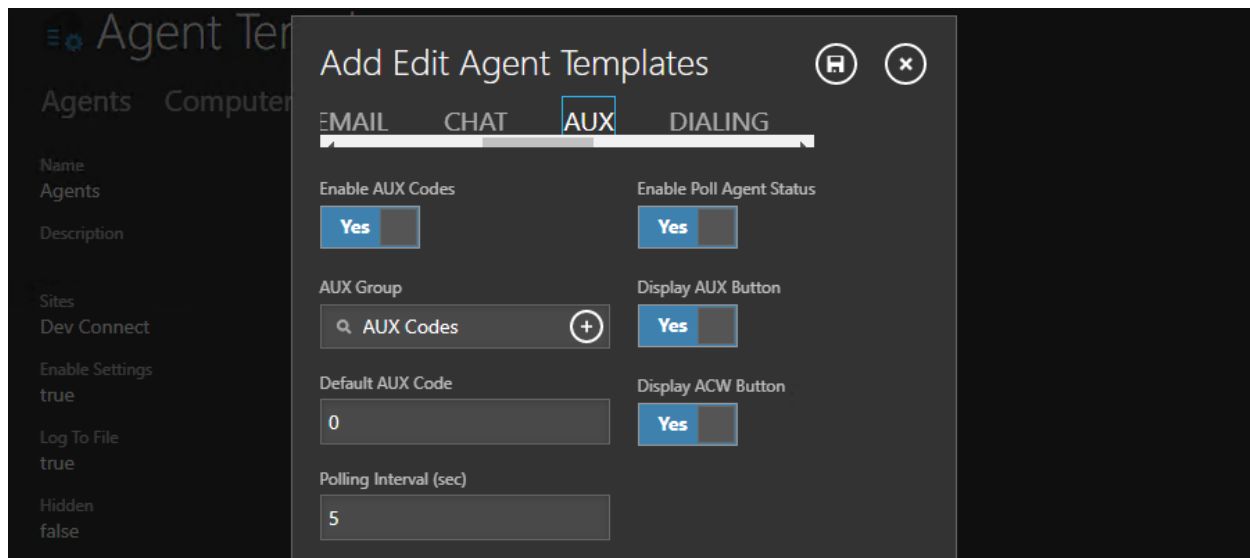


The screenshot shows the 'Agent Templates' interface with the 'Details' tab selected. The interface is dark-themed. At the top, there's a header 'Agent Templates' with a dropdown arrow. Below it, a navigation bar contains tabs: 'Agents', 'Computers', 'Screenpop', 'Custom', 'Presence', and 'Details' (which is highlighted with a blue box). The main area displays a table of settings for the 'Agents' template. The settings are organized into four columns:

Setting	Value
Name	Agents
Description	
Sites	Dev Connect
Prompt for Extension	false
Require Close Password	false
AES Server Group	AES
Dialing Rules	true
Outside Line	9
Country Code	
AUX Group	AUX Codes
Enable AUX Reason Codes	true
Use Force Reason Code For Logout	false

At the bottom right, there is a button labeled 'Edit Agent Template' with a star icon.

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 7.3.2**. Retain the default values in the remaining fields.



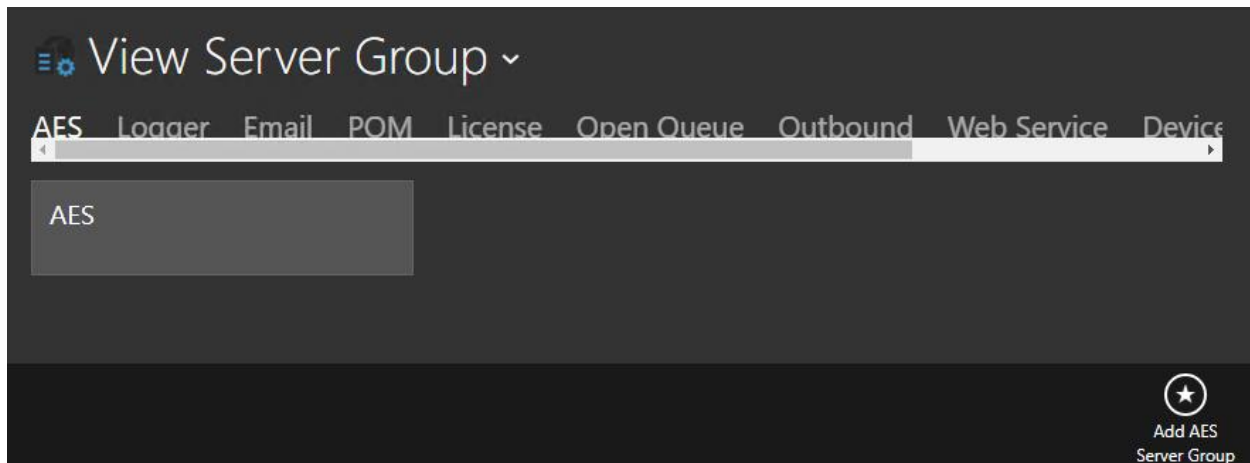
The screenshot shows the 'Add Edit Agent Templates' dialog box. The dialog has a title bar with a close button (X) and a maximize button. Below the title bar, there's a tabbed interface with four tabs: 'EMAIL', 'CHAT', 'AUX' (which is selected and highlighted with a blue box), and 'DIALING'. The 'AUX' tab contains the following settings:

Setting	Value
Enable AUX Codes	Yes
Enable Poll Agent Status	Yes
AUX Group	AUX Codes
Display AUX Button	Yes
Default AUX Code	0
Display ACW Button	Yes
Polling Interval (sec)	5

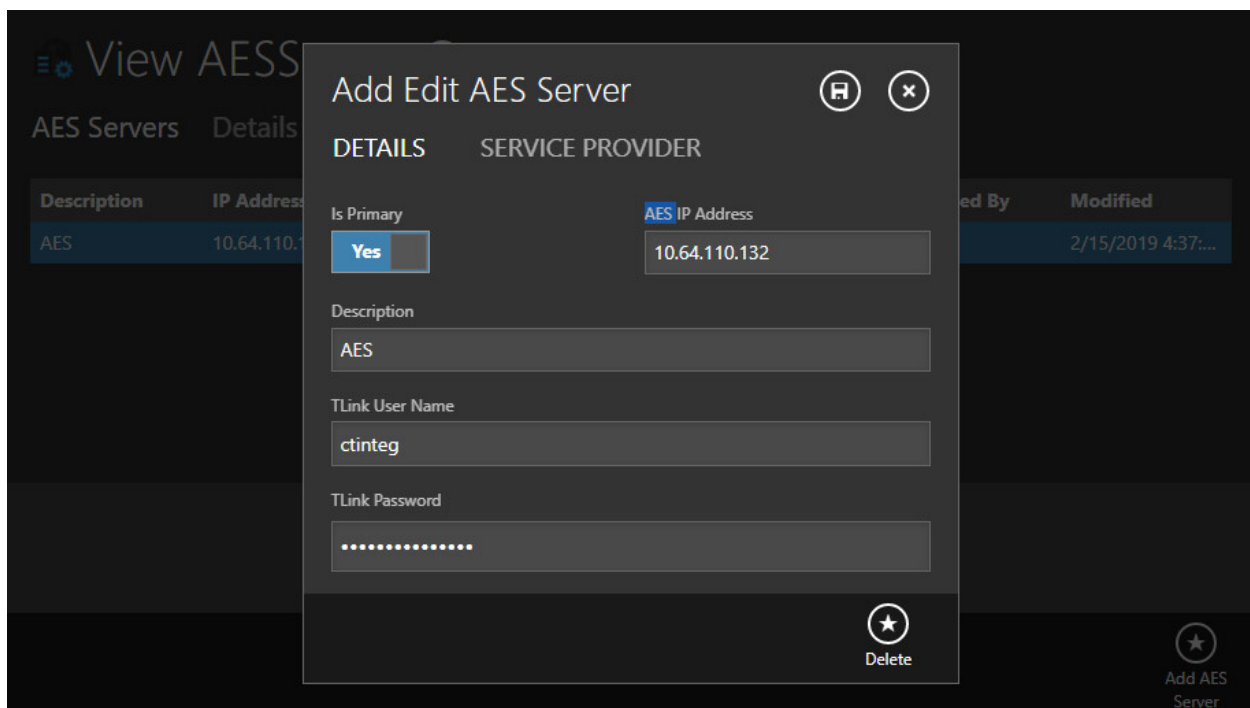
The background shows a partial view of the 'Agent Templates' interface with the 'Agents' tab selected.

7.5. Administer AES Server

To add AES configuration navigate to **Site → Server → Server Group → AES**. Select **AES** from the top menu, followed by **Add AES Server Group** from bottom of screen to add a logical group. In the compliance testing, the “AES” group was pre-configured. Note that an AES server group is required to be configured.



The **Add Edit AES Server** screen is displayed. Type in the **AES IP Address** and configured the credentials as per **Section 6.4**.



8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	8	no	aes8	established	370	370

8.2. 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**.

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ **Status**

Alarm Viewer

▶ Logs

▶ Log Manager

▼ **Status and Control**

■ CVLAN Service Summary

TSAPI Link Details

☐ Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm8	1	Talking	Tue May 21 10:51:19 2019	Online	18	0	373	373	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**.

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
 - Alarm Viewer
 - ▶ Logs
 - ▶ Log Manager
 - ▼ **Status and Control**
 - CVLAN Service Summary
 - DLG Services Summary
 - **DMCC Service Summary**
 - Switch Conn Summary
 - TSAPI Service Summary
 - ▶ User Management
 - ▶ Utilities
 - ▶ Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Fri May 24 16:20:17 MDT 2019

Service Uptime: 18 days, 6 hours 35 minutes
Number of Active Sessions: 2
Number of Sessions Created Since Service Boot: 18
Number of Existing Devices: 4
Number of Devices Created Since Service Boot: 28

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	C96BC35A9DBF13780 1858721B6023C01-4	ctinteg	CT Device Manager Server 1@WIN-UOQFTD9JOP2	10.64.110.169	XML Unencrypted	2
<input type="checkbox"/>	D67B1ED70163260C9 35E5DFC56C4BB46-3	ctinteg	CT Monitor Server 1@WIN-UOQFTD9JOP2	10.64.110.169	XML Unencrypted	3

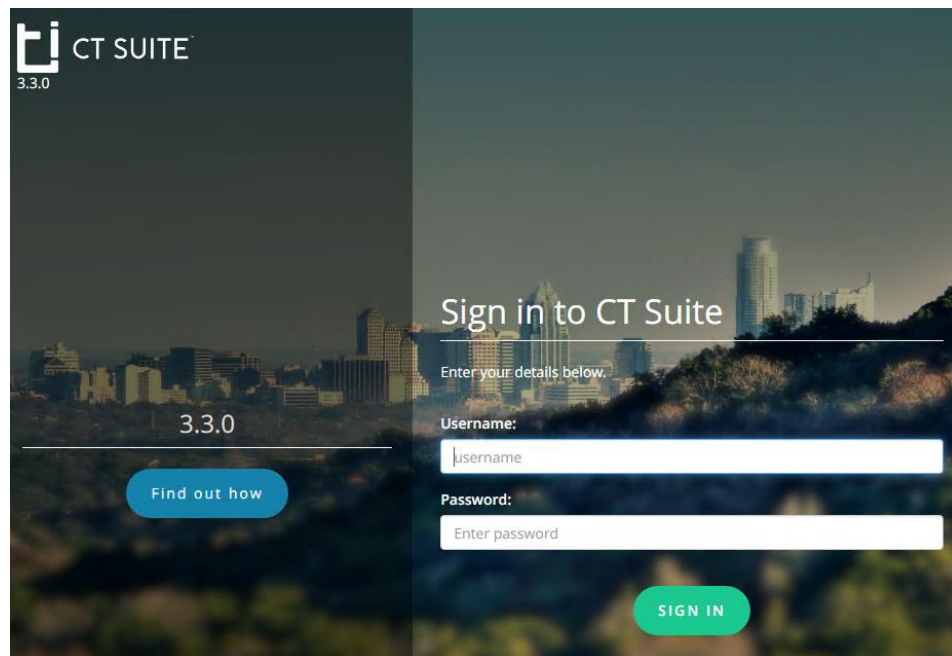
Terminate Sessions
Show Terminated Sessions

Item 1-2 of 2
1 Go

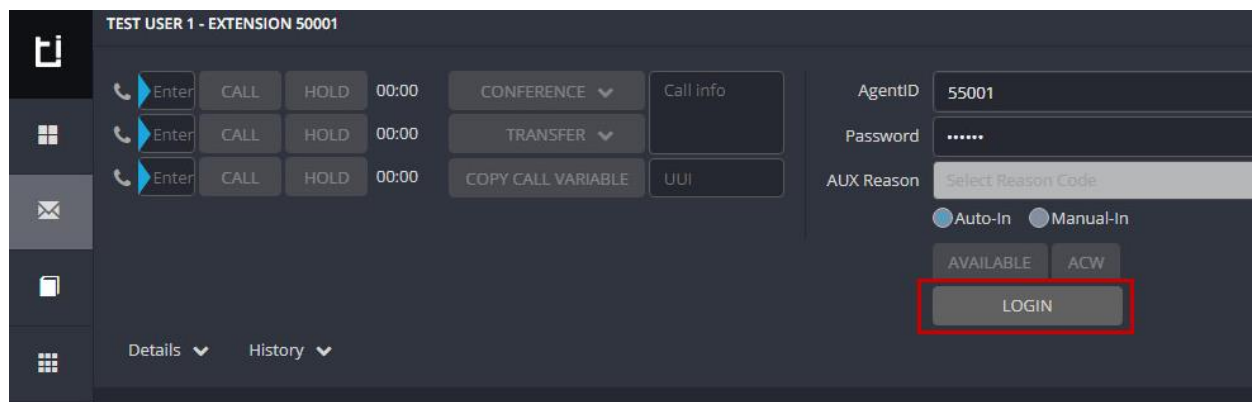
8.3. Verify CTIntegrations CT Suite

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.

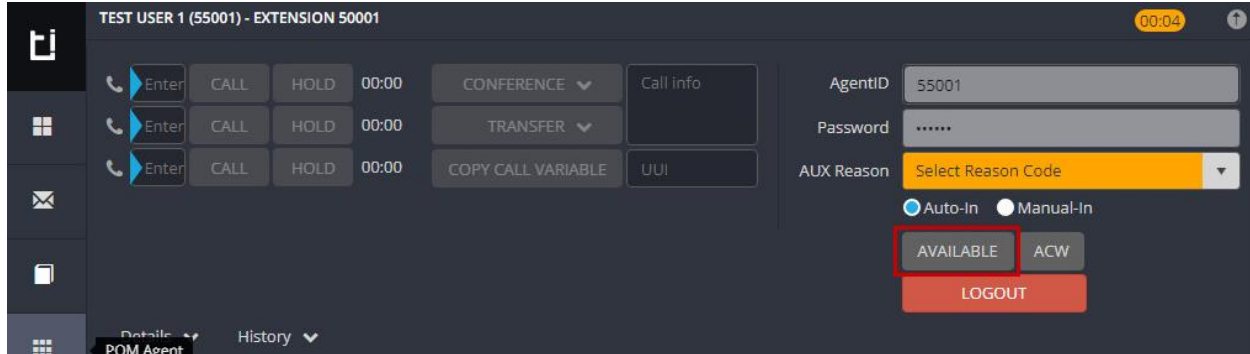
The **Sign in to CT Suite** screen is displayed. For **Username** and **Password**, enter an applicable agent credentials from **Section 7.3.1**, and retain the default value in the remaining field.



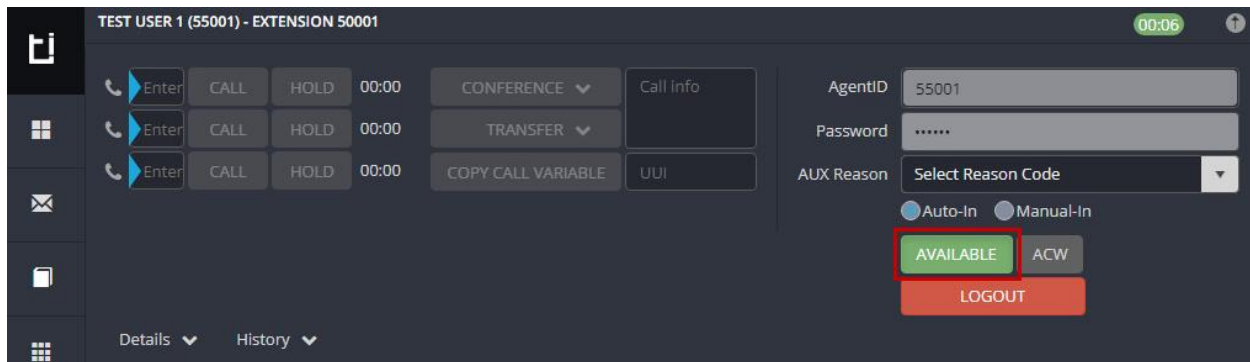
The agent screen below is displayed next. Retain the default values, and select **LOGIN** to log the agent into the ACD on Communication Manager.



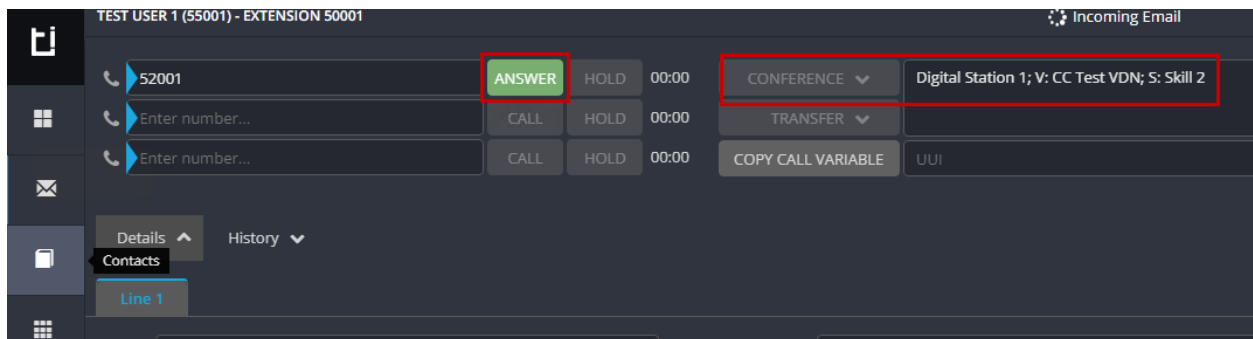
The agent screen is updated, as shown below. Click **AVAILABLE**.



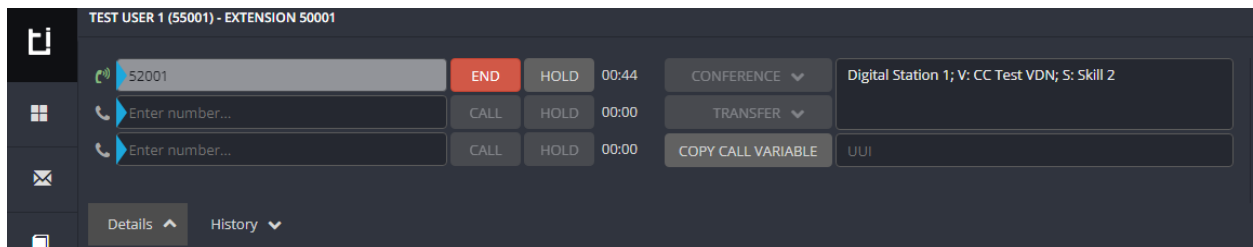
Verify that the agent screen is updated, with the **AVAILABLE** icon shown in green below.



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. Click **ANSWER**.



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



9. Conclusion

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.3 to successfully interoperate with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Application Enablement Services 8.0.1 for voice integration. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.0.x, Issue 4, May 2019.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 8.0.1, Issue 2, December 2018.

Documentation related to CT Desktop may directly be obtained from CTIntegrations.

3. CTIntegrations CT Suite Admin User Guide, User Guides v3.2

©2019 Avaya Inc. All Rights Reserved.

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

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