



## DevConnect Program

---

# Application Notes for Enghouse Computer Telephony Integration Connect Version 9 with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for Enghouse Computer Telephony Integration Connect to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the TSAPI interface. Enghouse Connect is a Computer Telephony Integration middleware platform that provides call control and monitoring functionality through various application programming interfaces to end user applications.

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 Avaya DevConnect Program.

# 1. Introduction

These Application Notes describe the configuration steps required for Enghouse Computer Telephony Integration (CTI) Connect to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Telephony Service Application Programming Interface. Enghouse CTI Connect is computer telephony call control server software capable of connecting a variety of TDM and VoIP telephone switches to distributed computer application environments. Its client/server-based CTI package enables the development and running of CTI applications using the CTI Application Programming Interface (API) and manages/monitors/controls a CTI network using the call server. CTI Connect can implement one of two mechanisms to integrate with Avaya Aura® Communication Manager, via Avaya Aura® Application Enablement Services (AES).

- Avaya Telephony Service Application Programming Interface (TSAPI).
- Avaya Adjunct Switch Application Interface (ASAI) protocol.

This document focuses on integration using TSAPI. Enghouse Interactive CTI Connect implements TSAPI to provide Computer Telephony Integration (CTI) call control and monitoring functionality and application programming interfaces to end user business applications.

## 2. General Test Approach and Test Results

The general test approach was to validate the ability of CTI Connect to correctly and successfully connect to Application Enablement Services and handle and control various Communication Manager endpoints in a variety of call scenarios.

CTI Connect use of the Avaya SDK is with the TSAPI protocol in AES. It caters for communication to the Avaya AES (TSAPI and ASAI) entities. AES requires specific licensing to support CTC functions over a TSAPI link:

- To use basic features and call monitoring supported methods, a TSAPI Basic User license is required.
- To use the **CtcRouteChannel.routeCall** method, a TSAPI Advanced User license is required.
- To use the **CtcDeviceChannel.makePredictiveCall** method, a TSAPI Advanced User license is required.

CTCTest is a CTI Connect application that is installed with the CTC server software. CTCTest can be used to perform the sequence of actions an application would take against a supported switch made available with the CTC API software. CTCTest can be used to:

- Test the configuration by sending and receiving data with a switch.
- Check the operation of supported features.
- Validate routine call sequences.
- Isolate problems that occur during development of an application using the Application Programming Interface (API).

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and Enghouse Interactive CTI Connect did not include use of any specific encryption features as requested by Enghouse.

## **2.1. Interoperability Compliance Testing**

Interoperability compliance testing consisted of using CTI Connect to verify successful handling and control of a variety of endpoints as follows:

- Assign and un-assign on devices and call monitor channels.
- Agent Log In/Log Out.
- Set Status for ACD Agents.
- Receive Events which allows Channel Synchronisation and Call States.
- Agent State Synchronization with Agent Telephones.
- Hold/Unhold.
- Transfers: Screened, Unscreened and Immediate Transfer with Disconnect.
- Conferencing: Screened, Unscreened and Immediately Join of calls.
- Associate Data with a call and Pass it to the Switch.
- Customer calls to Agents (Calls to VDN's).
- Virtual Party on a switch to initiate calls.
- Calls from Agent to Agent.
- Calls from Agent to Non-Agent.
- Transmit DTMF Tones.
- Deflect call, Call Forward.
- Set routing for an assigned Route-Point on or off.
- Provide a destination for a call, in response to receipt of Route Request.
- Alternate and Swap of a current call with a call on Consultation Hold.
- Disconnect a specified Party from a call.
- Return ACD Split Information.
- Return the Global Reference Identifier for calls.

- Temporarily Disconnect a party from a call so that the party can no longer hear one or more of the other parties on the call.
- Serviceability Testing.

## 2.2. Test Results

All test cases were executed successfully.

## 2.3. Support

For technical support on Enghouse CTI Connect products, please visit the website at <http://enghouseinteractive.com/> or contact an authorized Enghouse representative at [info.ei@enghouse.com](mailto:info.ei@enghouse.com).

### USA

- Email: [EnvoxSupport@enghouse.com](mailto:EnvoxSupport@enghouse.com)
- Website: <https://www.enghouseinteractive.com/services/support/>
- Phone: +1 800.788.9730 Self-Service
- Phone: +1 800.872.2272 Live-Service

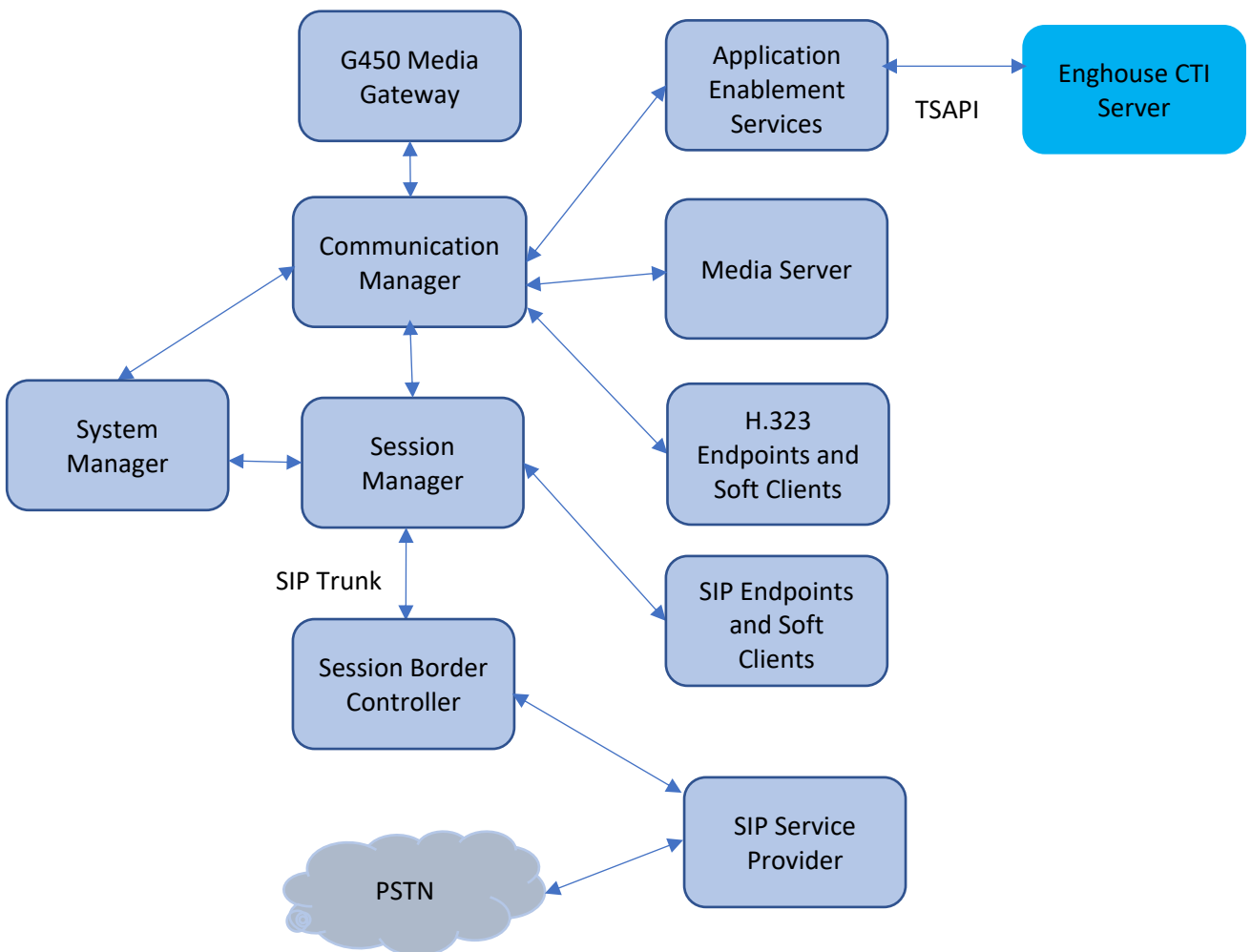
### EMEA

- Email: [uksupport@enghouse.com](mailto:uksupport@enghouse.com)
- Website: <http://www.enghouseinteractive.co.uk/services/support/>
- Phone: +44 870 220 2205

### 3. Reference Configuration

**Figure 1** below shows Avaya Aura® Communication Manager serving both SIP and H.323 endpoints with Avaya Aura® Application Enablement Services providing a TSAPI interface to which the Enghouse Interactive CTI Connect application connects. Avaya Aura® Session Manager provides the point of registration for Avaya SIP endpoints. Avaya Aura® System Manager Server provides a means to manage and configure Session Manager.

**Note:** For the purposes of the compliance test the CtcTest application was used to validate the functions of CTI Connect.



**Figure 1: Test Configuration Diagram**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1.2.0 FP2 01.0.974.0-27783
Avaya G450 Media Gateway	FW 42.18.0
Avaya Aura® Media Server	10.1.0.125
Avaya Aura® System Manager	10.1.2.0 Feature Pack 2 10.1.2.0.0715476
Avaya Aura® Session Manager	10.1.2.0 Feature Pack 2 10.1.0.02.1012016
Avaya Session Border Controller	10.1.0.0-32-21432
Avaya Aura® Application Enablement Service	10.1.2.0
Avaya 96x1 Series IP Deskphones (H.323)	6.8.5.4
Avaya J100 Series Deskphones (SIP)	4.1.0.0.9
Avaya K155 Vantage Device (SIP)	3.1.1.2 (bld version 0012)
Avaya Workplace for Windows (SIP)	3.32.0.75
Enghouse Interactive CTI Connect	9.0

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure Interface to Avaya Aura® Application Enablement Services.
- Configure Call Center Features.
- Configure Avaya Endpoints for Third Party Call Control.

### 5.1. Configure Interface to Avaya Aura® Application Enablement Services

The following sections illustrate the steps required to create a link between Communication Manager and Application Enablement Services.

#### 5.1.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

<b>display system-parameters customer-options</b>		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	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y	
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y	
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y	
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y	
ATMS?	y			
Attendant Vectoring?	y			

On **Page 10**, see the **ASAI Enhanced Features** that were set during compliance testing. The settings below were set during compliance testing, however, only **Adjunct Routing** and **CTI Stations** are required to be set to **y**.

```
display system-parameters customer-options                               Page 10 of 12
                                ASAI ENHANCED FEATURES

                                Adjunct Routing? y
                                CTI Stations? y
                                Increased Adjunct Route Capacity? y
                                Phantom Calls? y

                                ASAI PROPRIETARY FEATURES

                                Proprietary? y
```

Use the **display system-parameters features** command and on **Page 5**, ensure that **Create Universal Call ID (UCID)** is set to **y** as shown below.

```
display system-parameters features                                     Page 5 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
SYSTEM PRINTER PARAMETERS
  Endpoint:                      Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name: cm10
                                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  Notification using Crisis Alert? n
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station  Auto Inspect on Send All Calls? n
  Send All Calls on Ringing Bridge Leaves Call Ringing on Other Bridges? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y  UCID Network Node ID: 1
  Copy UCID for Station Conference/Transfer? y
```



### 5.1.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr**.

<b>display node-names ip</b>		IP NODE NAMES
Name	IP Address	
AMS1	10.33.1.30	
CMS19	10.33.1.18	
SM10	10.33.1.42	
interopcms	10.33.1.19	
loopback	10.33.1.6	
lsp	10.33.1.7	
<b>procr</b>	<b>10.33.1.43</b>	
( 16 of 18 administered node-names were displayed )		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

### 5.1.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES, use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 5.1.2**.
- **Local Port:** Retain the default value of **8765**.

change ip-services						Page	1 of	4
IP SERVICES								
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	TLS Encryption		
AESVCS	y	procr	8765					

Go to **Page 3** of the **ip-services** form and enter the following values:

- **AE Services Server:** Host name obtained from the AES server, in this case **aes10**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

**Note:** The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** must match the administered name for the AES server; this is created as part of the AES installation and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aes10	*	y	in use

### 5.1.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

<b>change cti-link 1</b>	Page 1 of 3
CTI LINK	
CTI Link: 1	
<b>Extension: 3332</b>	
<b>Type: ADJ-IP</b>	
COR: 1	
Name: AES10	
Unicode Name? n	

## 5.2. Configure Call Center Features

For the purposes of the Predictive Call feature and ACD functionality of CTI Connect, the following must be configured:

- Configure Hunt Group.
- Configure Vector.
- Configure Vector Directory Number (VDN).
- Configure Agents.

### 5.2.1. Configure Hunt Group

Enter the command **add hunt-group x** where **x** is an appropriate hunt group number and configure as follows:

- **Group Number** – this is the Skill Number when configuring the agent and vector.
- **Group Name** – enter an appropriate name.
- **Group Extension** – enter an extension appropriate to the dialplan. This is used for the ACD monitor feature of CTI Connect.
- **Group Type** – set to **ucd-mia**.
- **ACD?** – set to **y**.
- **Queue?** – set to **y**.
- **Vector?** – set to **y**.

<b>change hunt-group 1</b>	Page 1 of 4
HUNT GROUP	
<b>Group Number: 1</b>	<b>ACD? y</b>
<b>Group Name: Skill-1</b>	<b>Queue? y</b>
<b>Group Extension: 3320</b>	<b>Vector? y</b>
<b>Group Type: ucd-mia</b>	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited	
Calls Warning Threshold:	Port:
Time Warning Threshold:	Port:

On **Page 2**, set **Skill** to **y**.

<b>change hunt-group 1</b>	Page 2 of 4
HUNT GROUP	
<b>Skill? y</b>	Expected Call Handling Time (sec): 180
AAS? n	Service Level Target (% in sec): 80 in 20
Measured: both	
Supervisor Extension:	
Controlling Adjunct: none	
VuStats Objective:	
Multiple Call Handling: none	
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n

## 5.2.2. Configure Vector

Enter the command **change vector x** where **x** is the required vector number. Configure as shown below so that calls **queue-to skill 1st**. Skill 1st the hunt group configured in the VDN in **Section 5.2.3**. Ensure that the first entry is **adjunct routing link x** where x is the CTI link configured in **Section 5.1.4**.

<b>change vector 14</b>	Page 1 of 6
CALL VECTOR	
Number: 14	Name: Call Center
Multimedia? n	Attendant Vectoring? n
Basic? y	Meet-me Conf? n
EAS? y	Lock? n
G3V4 Enhanced? y	ANI/II-Digits? y
ASAI Routing? y	Prompting? y
LAI? y	G3V4 Adv Route? y
CINFO? y	BSR? y
Holidays? y	Variables? y
3.0 Enhanced? y	
01 adjunct	routing link 1
02 wait-time	20 secs hearing 1100 then silence
03 queue-to	skill 1 pri m
04 wait-time	100 secs hearing music
05 goto step	3 if unconditionally
06 stop	

### 5.2.3. Configure Vector Directory Number (VDN)

Enter the command **add vdn x** where **x** is the required VDN number appropriate to the dialplan. Configure the VDN to send calls to the vector configured in the previous section as follows:

- **Extension** – note the VDN extension number which will be used to place calls to the Skill vector and on to the Skill.
- **Name** – enter an appropriate name.
- **Destination** – enter the **Vector Number** configured in the previous section.
- **1<sup>st</sup> Skill** – enter the hunt group created in **Section 5.2.1**.

```
change vdn 3340                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
                                                    Extension: 3340                               Unicode Name? n
                                                    Name*: VDN
                                                    Destination: Vector Number          14
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: both          Report Adjunct Calls as ACD*? n
Acceptable Service Level (sec): 20
VDN of Origin Annc. Extension*:
1st Skill*: 1
2nd Skill*:
3rd Skill*:
SIP URI:
```

## 5.2.4. Configure Agents

Agents must be configured with the appropriate Skill Number. Enter the command **add agent-loginID x** where **x** is an agent extension number appropriate to the dialplan and configure as follows:

- **Login ID** – take a note of the configured **Login ID**.
- **Name** – enter an identifying name.
- **Password** – enter a suitable password of the agent.

change agent-loginID 1000		Page 1 of 3
AGENT LOGINID		
<b>Login ID: 1000</b>		Unicode Name? n AAS? n
<b>Name: Agent 1000</b>		AUDIX? n
TN: 1		
COR: 1		
Coverage Path:		LWC Reception: spe
Security Code: 1234		LWC Log External Calls? n
Attribute:		AUDIX Name for Messaging:
		LoginID for ISDN/SIP Display? n
		<b>Password: 1234</b>
		Password (enter again): 1234
MWI Served User Type:		Auto Answer: station
AUX Agent Remains in LOA Queue: system		MIA Across Skills: system
AUX Agent Considered Idle (MIA): system		ACW Agent Considered Idle: system
Work Mode on Login: system		Aux Work Reason Code Type: system
		Logout Reason Code Type: forced
Maximum time agent in ACW before logout (sec): system		
		Forced Agent Logout Time: :
WARNING: Agent must log in again before changes take effect		

On **Page 2**, enter the hunt group number configured in **Section 5.2.1** in the **SN** (Skill Number) column and enter an appropriate **SL** (skill level).

change agent-loginID 1000		Page 2 of 3
AGENT LOGINID		
Direct Agent Skill: 1		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
<b>SN</b>	<b>RL SL</b>	
1: 1	1	
2:		
3:		
4:		
16:		
17:		
18:		
19:		
31:		
32:		
33:		
34:		
46:		
47:		
48:		
49:		

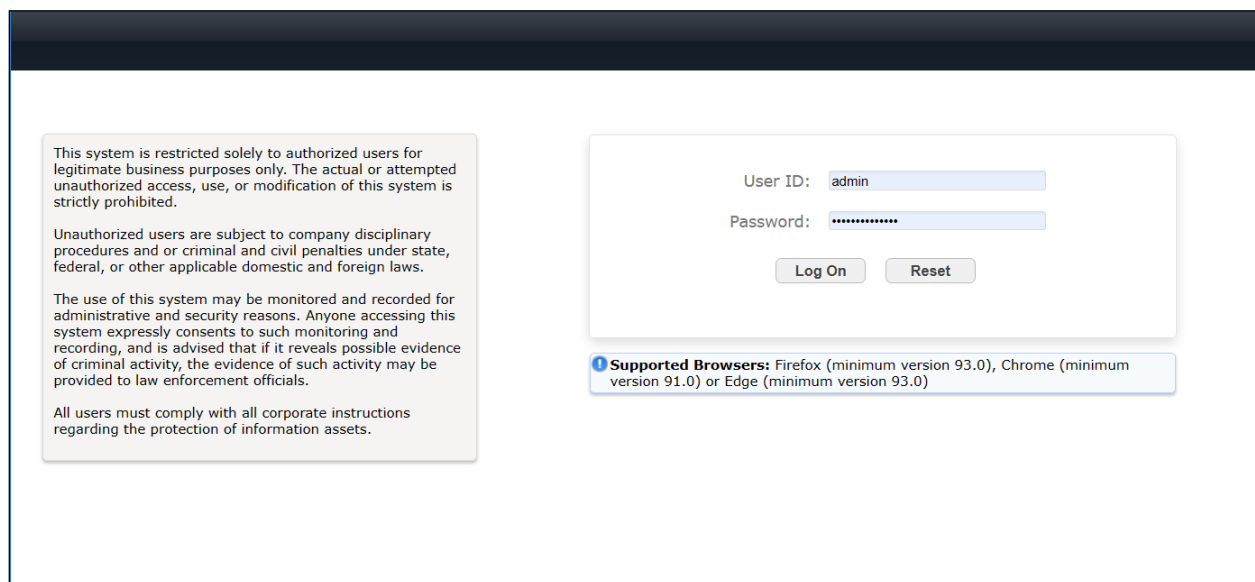
### 5.3. Configure Avaya SIP Endpoints for Third Party Call Control

Each Avaya SIP endpoint or station that needs to be monitored and used for 3<sup>rd</sup> party call control will need to have “Type of 3PCC Enabled” is set to “Avaya”.

Any SIP extension that is to be monitored requires some configuration changes to enable call control. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering

**http://<FQDN >/network-login**, where <FQDN> is the fully qualified domain name of System Manager or **http://<IP Address >/network-login**. Log in using appropriate credentials.

**Note:** The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

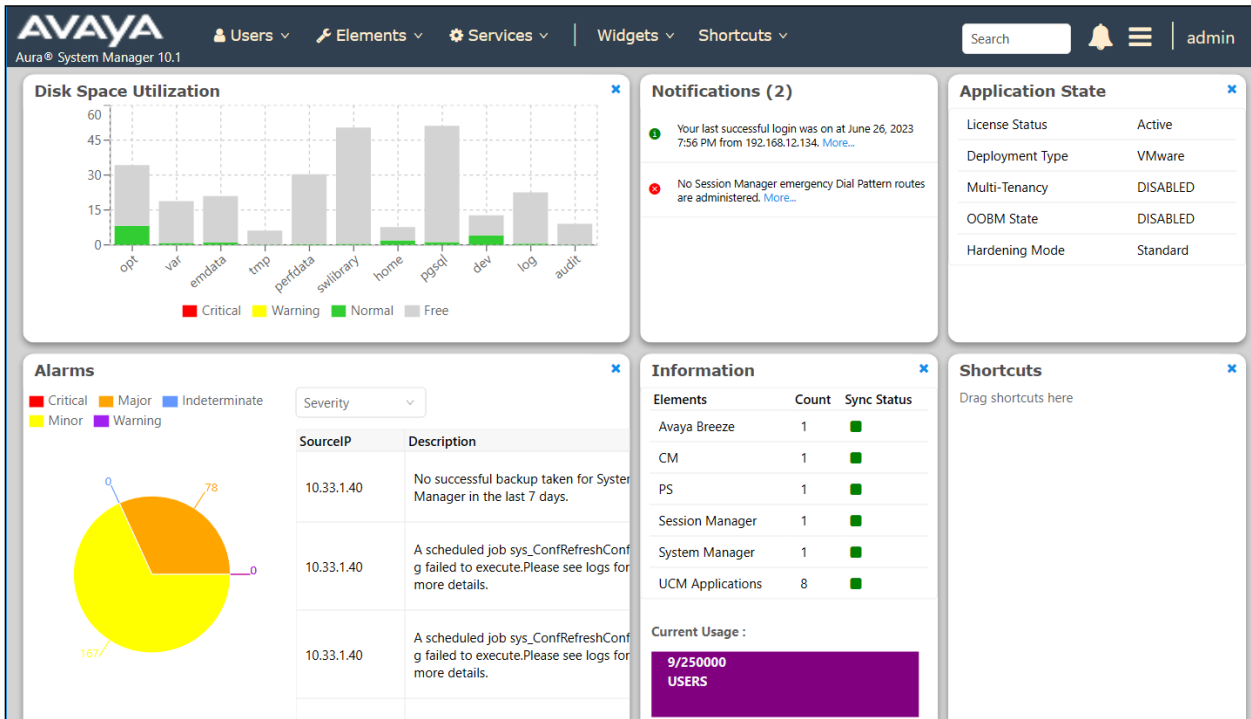
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

**Supported Browsers:** Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0)

From the home page, click on **Users** → **User Management** → **Manage Users**, as shown below.



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.

The screenshot displays the Avaya Aura System Manager 10.1 User Management page. The left sidebar shows the navigation menu with 'Manage Users' selected. The main content area shows a list of users with the following columns: First Name, Surname, and Display Name. The 'Edit' button is highlighted in the top toolbar.

View	First Name	Surname	Display Name
<input type="checkbox"/>	H323 Ext	1000	1000, H323 Ext
<input checked="" type="checkbox"/>	SIP Ext	1100	1100, SIP Ext
<input type="checkbox"/>	J129 SIP	1101	1101, J129 SIP
<input type="checkbox"/>	Equinox Vantage	1102	1102, Equinox Vantage
<input type="checkbox"/>	Agent	Agent	Agent One
<input type="checkbox"/>	Agent	Agent	Agent Two
<input type="checkbox"/>	admin	admin	Default Administrator
<input type="checkbox"/>	SIP	Ext 1150	Ext 1150, SIP
<input type="checkbox"/>	SIP	Ext 1151	Ext 1151, SIP
<input type="checkbox"/>	SIP	Ext 1152	Ext 1152, SIP

Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.

**User Profile | Edit | 1100@devconnect.local**

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya BreezeS Profile ☐

**CM Endpoint Profile ☒**

\* System : cm\$1xvmpg

\* Profile Type : Endpoint

Use Existing Endpoints : ☐

\* Extension : 1100

Template : Start typing...

\* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000002

Voice Mail Number : 6666

Preferred Handle : Select

Calculate Route Pattern : ☐

Sip Trunk : aar

SIP URI : Select

Enhanced Callr-Info Display for 1-line phones : ☐

Delete on Unassign from User or on Delete User : ☒

Override Endpoint Name and Localized Name : ☒

Allow H.323 and SIP Endpoint Dual Registration : ☐

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below. Click on **Done**, at the bottom of the screen, once this is set.

General Options (G) \* Feature Options (F) Site Data (S) Abbreviated Call Dialing (A)

Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

\* Class of Restriction (COR) 1

\* Emergency Location Ext 1100

\* Tenant Number 1

\* SIP Trunk aar

Coverage Path 1

Lock Message ☐

Multibyte Language Not Applicable

\* Class Of Service (COS) 1

\* Message Lamp Ext. 1100

**Type of 3PCC Enabled Avaya**

Coverage Path 2

Localized Display Name 1100, SIP Ext

Enable Reachability for Station Domain Control system

SIP URI

Primary Session Manager

IPv4: 10.10.40.32 IPv6:

Secondary Session Manager



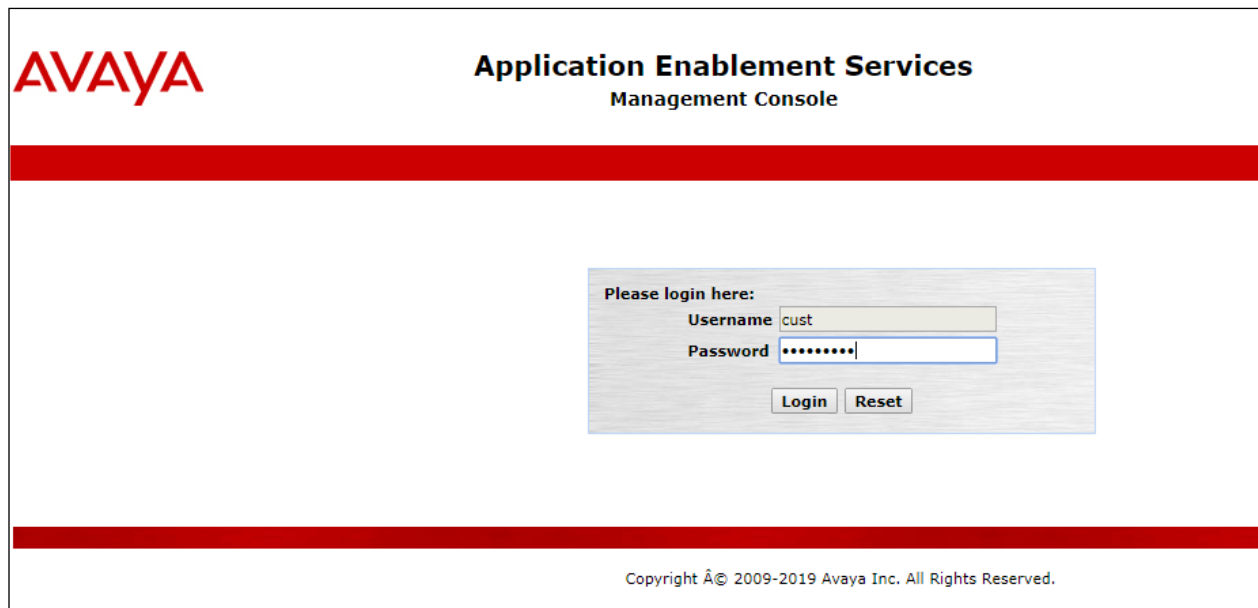
## 6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing.
- Create Switch Connection.
- Administer TSAPI link.
- Identify Tlinks.
- Enable TSAPI Ports.
- Create CTI User.
- Associate Devices with CTI User.

### 6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



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" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a login box with a light gray background. Inside the box, the text "Please login here:" is at the top. Below it are two input fields: "Username" with the text "cust" entered, and "Password" with a series of dots. At the bottom of the box are two buttons: "Login" and "Reset". Another thick red horizontal bar is located at the bottom of the page, just above the footer. The footer text, "Copyright © 2009-2019 Avaya Inc. All Rights Reserved.", is centered at the very bottom.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license.

AE Services

Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▶ TSAPI

▶ TWS

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

AE Services

DLG does not support Encrypted link. In case of GDPR (Data Privacy) enabled systems, use of DLG service will be site responsibility. By default DLG will be in running state

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
Web Telephony Interface(WTI) Service	DOWN	Stopped	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

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

\* WTI will use TSAPI license.  
\* - For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

## 6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

Communication Manager Interface | Switch Connections

Home | Help | Logc

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm10	Yes	30	1

Edit Connection

Edit PE/CLAN IPs

Edit Signaling Details

Delete Connection

Survivability Hierarchy

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.1.3**. The remaining fields should show as below. Click **Apply** to save changes.

Connection Details - cm10

Switch Password

.....

Confirm Switch Password

.....

Msg Period

30

Minutes (1 - 72)

Provide AE Services certificate to switch

☐

Secure H323 Connection

☒

Processor Ethernet

☒

Enable TLS Certificate Validation

☐

Apply

Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button.

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm10	Yes	30	1

Edit Connection

Edit PE/CLAN IPs

Edit Signaling Details

Delete Connection

Survivability Hierarchy

In the resulting screen, enter the IP address of the procr as shown in **Section 5.1.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

Edit Processor Ethernet IP - cm10

10.33.1.43

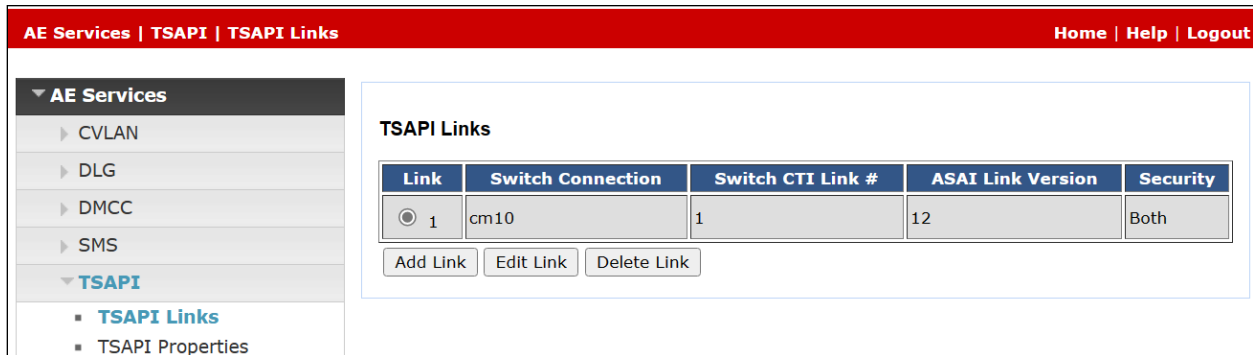
Add/Edit Name or IP

Name or IP Address	Status
10.33.1.43	In Use

Back

### 6.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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

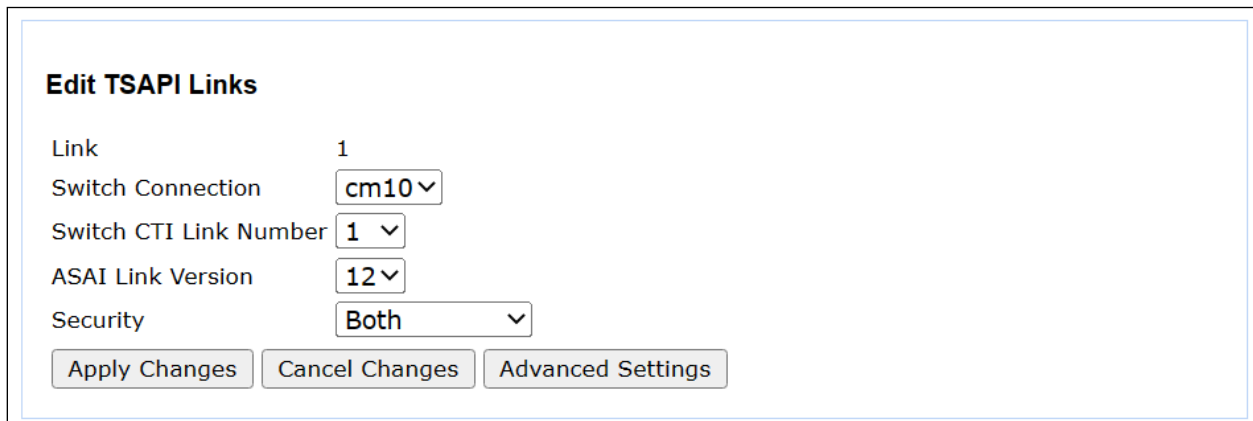
Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm10	1	12	Both

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

On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm10**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.1.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **12**.
- **Security:** This should be set to **Both** allowing both secure and nonsecure connections.

Once completed, select **Apply Changes**.




The screenshot shows the 'Edit TSAPI Links' screen. It contains the following fields and buttons:

- Link:** 1
- Switch Connection:** cm10 (dropdown)
- Switch CTI Link Number:** 1 (dropdown)
- ASAI Link Version:** 12 (dropdown)
- Security:** Both (dropdown)
- Buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

Another screen appears for confirmation of the changes made. Choose **Apply**.

**Apply Changes to Link**  

Warning! Are you sure you want to apply the changes?  
These changes can only take effect when the TSAPI server restarts.

 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

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

**Note: DMCC Service must be restarted for WTI service changes to take effect.**  
For status on actual services, please use [Status and Control](#)

## 6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Enghouse in **Section 7.4**.

The screenshot shows the Avaya DevConnect web interface. The top navigation bar is red with the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. A left-hand sidebar contains a tree view of the application's structure. Under the "Security" section, "Security Database" is expanded, showing a list of items: Control, CTI Users, Devices, Device Groups, **Tlinks** (highlighted in blue), Tlink Groups, and Worktops. The main content area is titled "Tlinks" and contains a "Tlink Name" label. Below this label are two radio button options: "AVAYA#CM10#CSTA#AES10" (which is selected) and "AVAYA#CM10#CSTA-S#AES10". A "Delete Tlink" button is located below the radio buttons. A vertical scrollbar is visible on the right side of the main content area.

Security | Security Database | Tlinks Home | Help | Logout

**Tlinks**

Tlink Name

☒ AVAYA#CM10#CSTA#AES10

☐ AVAYA#CM10#CSTA-S#AES10

Delete Tlink

- 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
    - Devices
    - Device Groups
    - Tlinks**
    - Tlink Groups
    - Worktops

## 6.5. Enable TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking** → **Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

**Networking | Ports**

<ul style="list-style-type: none"> <li>▶ AE Services</li> <li>▶ Communication Manager Interface</li> <li>High Availability</li> <li>▶ Licensing</li> <li>▶ Maintenance</li> <li><b>▼ Networking</b></li> <li>AE Service IP (Local IP)</li> <li>Network Configure</li> <li style="color: blue;"><b>Ports</b></li> <li>TCP/TLS Settings</li> <li>▶ Security</li> <li>▶ Status</li> <li>▶ User Management</li> <li>▶ Utilities</li> <li>▶ Help</li> </ul>	<h3 style="margin-top: 0;">Ports</h3> <hr/> <p><b>CVLAN Ports</b></p> <table style="width: 100%;"> <thead> <tr> <th></th> <th></th> <th>Enabled</th> <th>Disabled</th> </tr> </thead> <tbody> <tr> <td>Unencrypted TCP Port</td> <td>9999</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Encrypted TCP Port</td> <td><input type="text" value="9998"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> <hr/> <p><b>DLG Port</b></p> <table style="width: 100%;"> <thead> <tr> <th>TCP Port</th> <th></th> </tr> </thead> <tbody> <tr> <td>5678</td> <td></td> </tr> </tbody> </table> <hr/> <p><b>TSAPI Ports</b></p> <table style="width: 100%;"> <thead> <tr> <th></th> <th></th> <th>Enabled</th> <th>Disabled</th> </tr> </thead> <tbody> <tr> <td>TSAPI Service Port</td> <td>450</td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Local TLINK Ports</td> <td></td> <td></td> <td></td> </tr> <tr> <td>TCP Port Min</td> <td>1024</td> <td></td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td>1039</td> <td></td> <td></td> </tr> <tr> <td>Unencrypted TLINK Ports</td> <td></td> <td></td> <td></td> </tr> <tr> <td>TCP Port Min</td> <td><input type="text" value="1050"/></td> <td></td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td><input type="text" value="1065"/></td> <td></td> <td></td> </tr> <tr> <td>Encrypted TLINK Ports</td> <td></td> <td></td> <td></td> </tr> <tr> <td>TCP Port Min</td> <td><input type="text" value="1066"/></td> <td></td> <td></td> </tr> <tr> <td>TCP Port Max</td> <td><input type="text" value="1081"/></td> <td></td> <td></td> </tr> </tbody> </table> <hr/> <p><b>DMCC Server Ports</b></p> <table style="width: 100%;"> <thead> <tr> <th></th> <th></th> <th>Enabled</th> <th>Disabled</th> </tr> </thead> <tbody> <tr> <td>Unencrypted Port</td> <td><input type="text" value="4721"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Encrypted Port</td> <td><input type="text" value="4722"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td>TR/87 Port</td> <td><input type="text" value="4723"/></td> <td><input checked="" type="radio"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> <hr/> <p><b>H.323 Ports</b></p> <table style="width: 100%;"> <tbody> <tr> <td>TCP Port Min</td> <td><input type="text" value="20000"/></td> </tr> <tr> <td>TCP Port Max</td> <td><input type="text" value="29999"/></td> </tr> <tr> <td>Local UDP Port Min</td> <td><input type="text" value="20000"/></td> </tr> <tr> <td>Local UDP Port Max</td> <td><input type="text" value="29999"/></td> </tr> </tbody> </table> <div style="text-align: right; margin-top: 10px;">       Enabled Disabled  <input checked="" type="radio"/> <input type="radio"/> </div> <p>Server Media</p>			Enabled	Disabled	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>	Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>	TCP Port		5678				Enabled	Disabled	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>	Local TLINK Ports				TCP Port Min	1024			TCP Port Max	1039			Unencrypted TLINK Ports				TCP Port Min	<input type="text" value="1050"/>			TCP Port Max	<input type="text" value="1065"/>			Encrypted TLINK Ports				TCP Port Min	<input type="text" value="1066"/>			TCP Port Max	<input type="text" value="1081"/>					Enabled	Disabled	Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>	Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>	TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>	TCP Port Min	<input type="text" value="20000"/>	TCP Port Max	<input type="text" value="29999"/>	Local UDP Port Min	<input type="text" value="20000"/>	Local UDP Port Max	<input type="text" value="29999"/>
		Enabled	Disabled																																																																																		
Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>																																																																																		
Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>																																																																																		
TCP Port																																																																																					
5678																																																																																					
		Enabled	Disabled																																																																																		
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>																																																																																		
Local TLINK Ports																																																																																					
TCP Port Min	1024																																																																																				
TCP Port Max	1039																																																																																				
Unencrypted TLINK Ports																																																																																					
TCP Port Min	<input type="text" value="1050"/>																																																																																				
TCP Port Max	<input type="text" value="1065"/>																																																																																				
Encrypted TLINK Ports																																																																																					
TCP Port Min	<input type="text" value="1066"/>																																																																																				
TCP Port Max	<input type="text" value="1081"/>																																																																																				
		Enabled	Disabled																																																																																		
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>																																																																																		
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>																																																																																		
TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>																																																																																		
TCP Port Min	<input type="text" value="20000"/>																																																																																				
TCP Port Max	<input type="text" value="29999"/>																																																																																				
Local UDP Port Min	<input type="text" value="20000"/>																																																																																				
Local UDP Port Max	<input type="text" value="29999"/>																																																																																				

## 6.6. Create CTI User

A user ID and password needs to be configured for the Enghouse to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.

**User Management | User Admin**

**User Admin**

User Admin provides you with the following options for managing AE Services users:

- Add User
- Change User Password
- List All Users
- Modify Default User
- Search Users



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Enghouse setup in **Section 7.4**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with Enghouse setup in **Section 7.4**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.

**AVAYA** Application Enablement Services Management Console

User Management | User Admin | Add User

**Add User**

Fields marked with \* can not be empty.

\* User Id: enghouse

\* Common Name: enghouse

\* Surname: enghouse

\* User Password: .....

\* Confirm Password: .....

Admin Note:

Avaya Role: None

Business Category:

Car License:

CM Home:

Csx Home:

CT User: Yes

Department Number:

Display Name:

Employee Number:

Employee Type:

Enterprise Handle:

Given Name:

Home Phone:

Home Postal Address:

Initials:

Labeled URI:

Mail:

MM Home:

Mobile:

Organization:

Pager:

Preferred Language: English

Room Number:

Telephone Number:

Apply Cancel

## 6.7. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit**.

Security | Security Database | CTI Users | List All Users

Home | 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

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> enghouse	Enghouse	NONE	NONE
<input type="radio"/> test	test	NONE	NONE

Edit List All

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

Edit CTI User

User Profile:

User ID

Common Name

Worktop Name

Unrestricted Access

enghouse

enghouse

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 Changes

Cancel Changes

Click on **Apply** when asked again to **Apply Changes**.

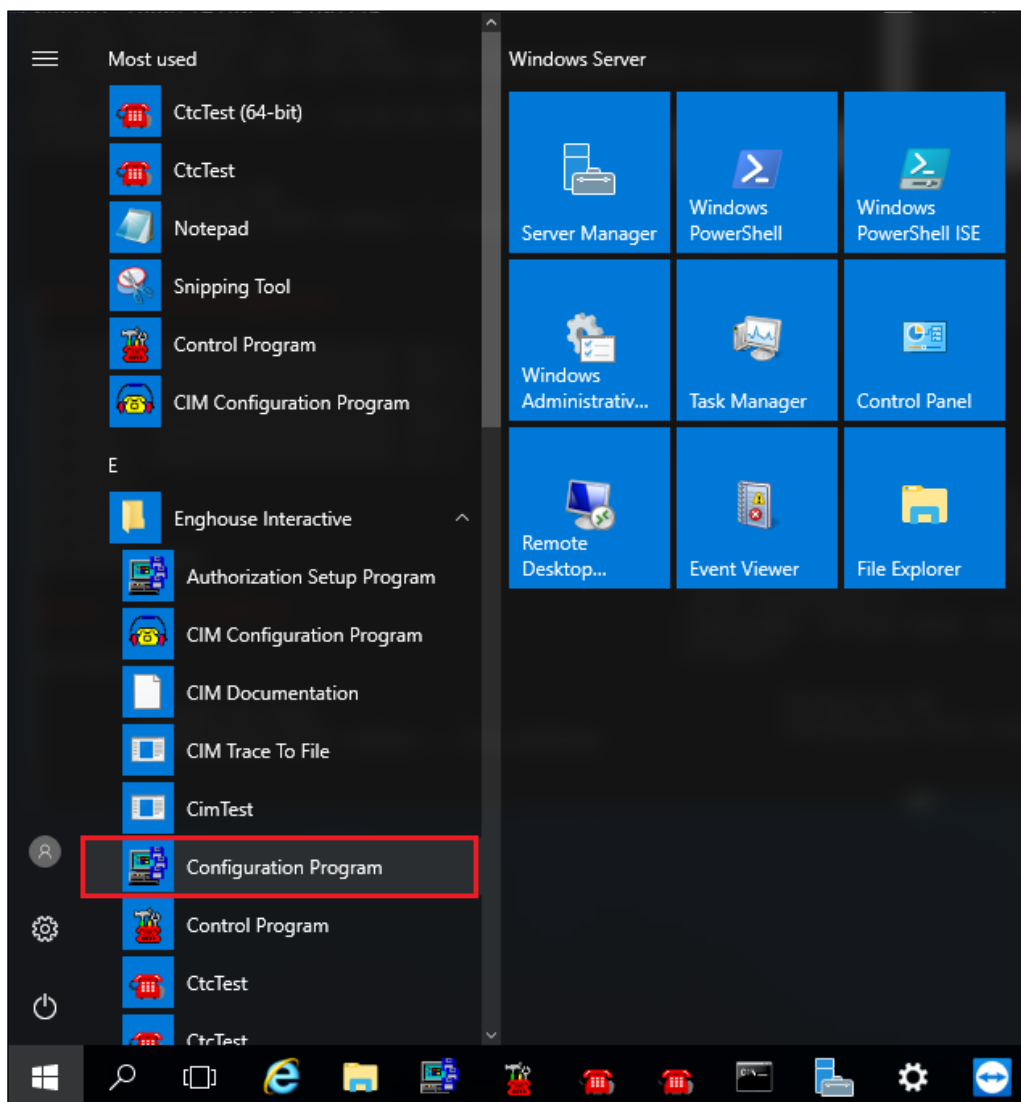
## 7. Configure Enghouse CTI Connect

This section provides the procedures for configuring CTI Connect. The procedures include the following areas:

- Launch configuration program.
- Administer link.
- Administer switch type.
- Administer IP address and link number.

### 7.1. Launch configuration program

CTI Connect uses a GUI based configuration program to configure the TSAPI connection between the CTI Connect server and Application Enablement Services. From the CTI Connect server, launch the configuration program by selecting **Configuration Program** as shown below.



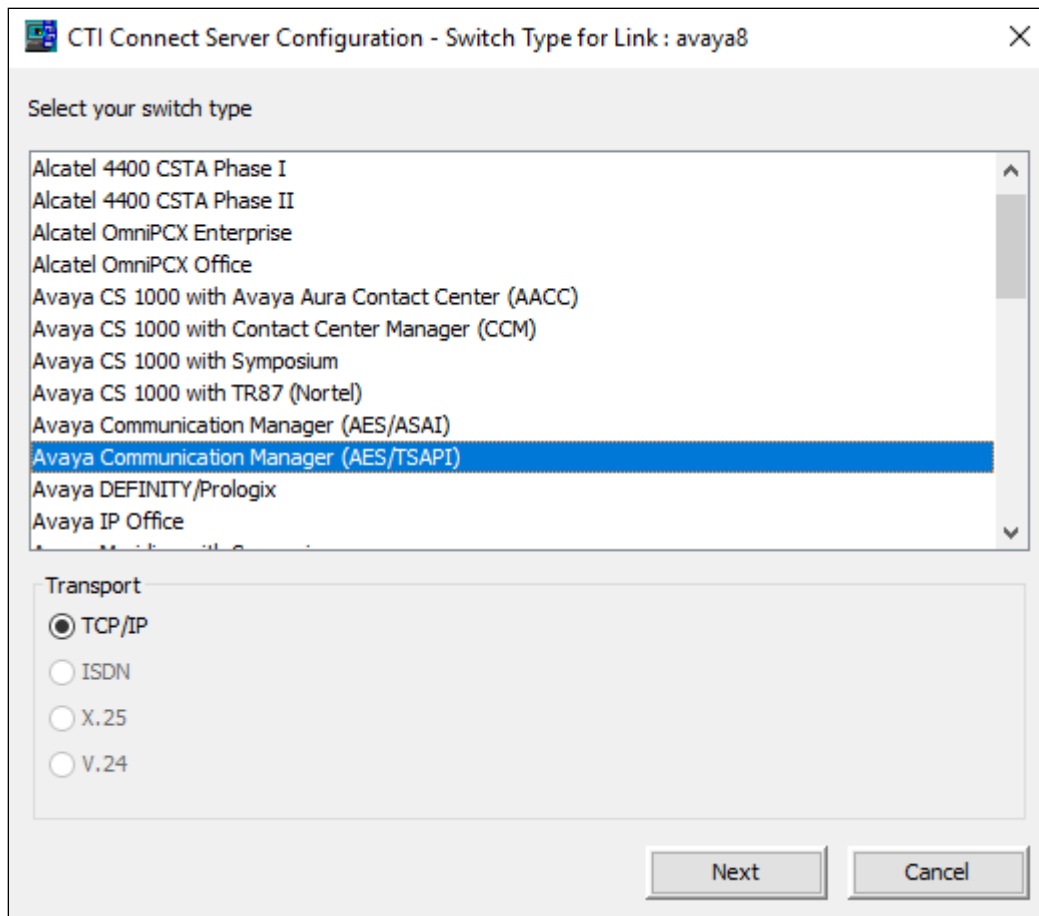
## 7.2. Administer Link

The **CTI Connect Server Configuration** screen is displayed. In the **Enter a Logical Identifier** field, enter a descriptive name, in this case **ctic** and click **Add**.

The image shows a screenshot of the 'CTI Connect Server Configuration' window. The window has a title bar with the text 'CTI Connect Server Configuration' and standard window controls (minimize, maximize, close). The main content area is divided into two sections: 'New Link' and 'Existing Links'. The 'New Link' section is highlighted with a red rectangular box. Inside this box, there is a text input field labeled 'Enter a logical identifier' containing the text 'ctic', and an 'Add' button to its right. The 'Existing Links' section is located below the 'New Link' section. It contains a dropdown menu labeled 'Select a logical identifier' with 'ctic' selected, and two buttons, 'Modify' and 'Delete', to its right. At the bottom of the window, there are three buttons: 'Server Options', 'Exit', and 'Help'.

### 7.3. Administer switch type

In the **Select your Switch Type** list, select **Avaya Communication Manager (AES/TSAPI)** and click **Next**.



## 7.4. Administer IP address and link number

Enter the following values for the specified fields and retain the default values in the remaining fields. Click **Save** when done.

- **AES Server Address** – enter the IP address of Application Enablement Services, in this case **10.33.1.47**.
- **TSAPI Service Name** - enter the **Tlink Name** obtained in **Section 6.4**.
- **Username** - enter the CT User configured in **Section 6.6**.
- **Password** - enter CT User **Password** configured in **Section 6.6**.

The screenshot shows a configuration window titled "CTI Connect Server Configuration - Link: ctic (Avaya Communication Manager (AES/TSAPI))". The window is divided into several sections:

- Transport**: Contains "AES Server Address" (10.33.1.47) and "Port Number" (450).
- Common**: Contains "Auto Start Link" (checked), "Auto Restart Monitors" (unchecked), "Timestamp" (Server), and "Call Information Manager" (localhost).
- Protocol Specific**: Contains "TSAPI Service Name" (AVAYA#CM10#CSTA#AES10), "Username" (enghouse), and "Password" (Avaya@123).
- Device Level Authorization**: Contains "Authorization" (Off).

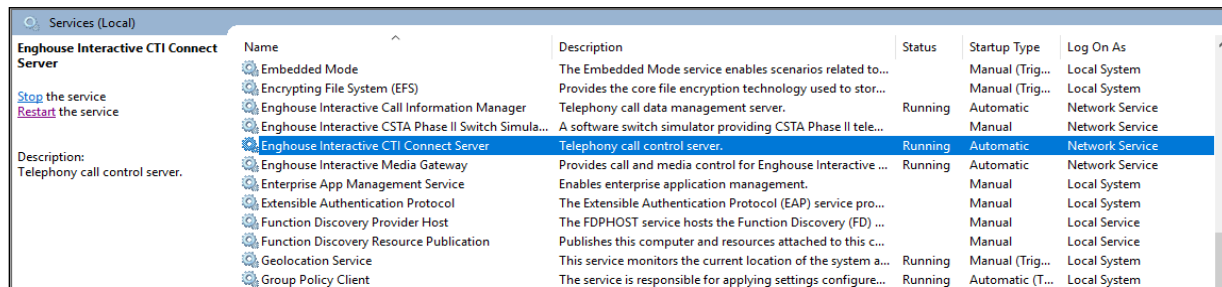
At the bottom, there are buttons for "Advanced", "Trace", "Save", and "Cancel".

## 8. Verification Steps

The correct configuration of the solution can be verified as follows.

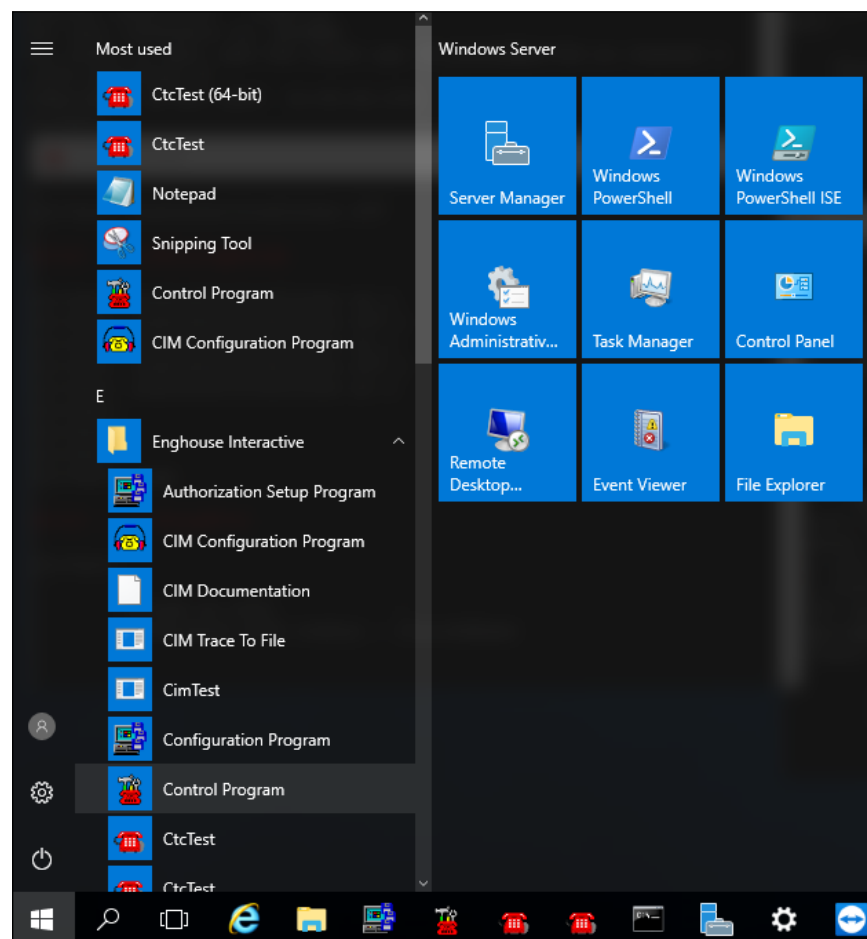
### 8.1. Verify Enghouse Interactive CTI Connect

From the Windows server services, ensure the **Enghouse Interactive CTI Service** is running.

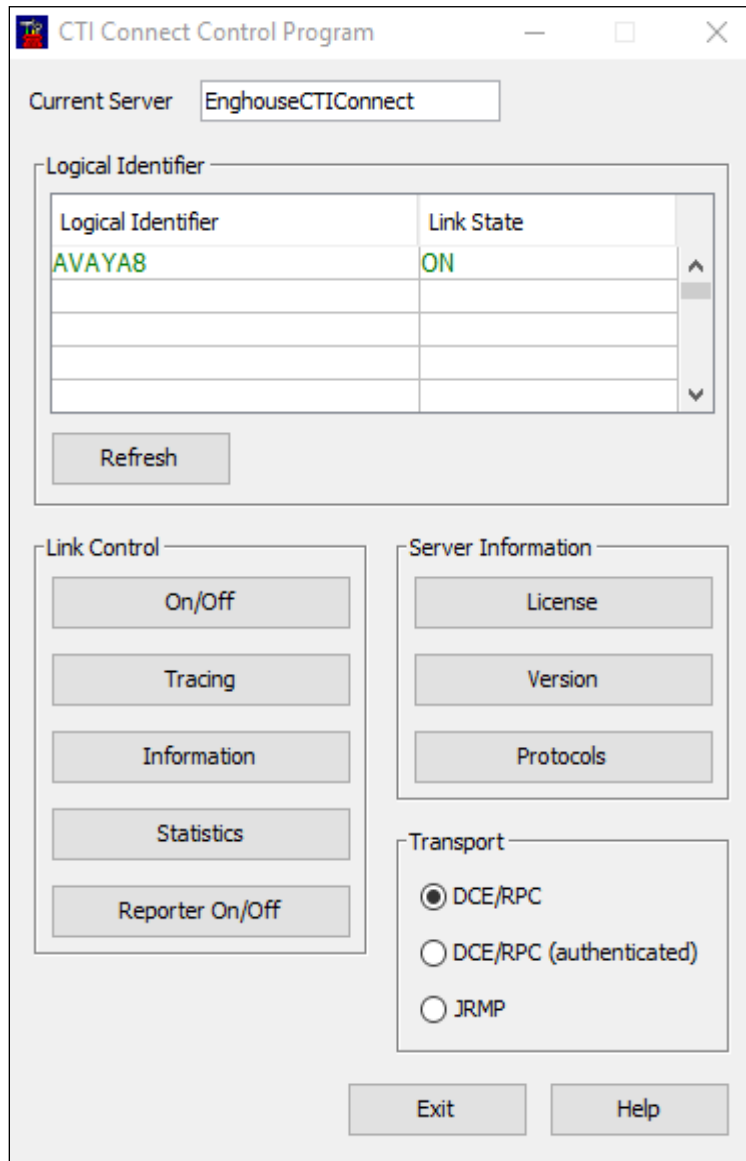


Name	Description	Status	Startup Type	Log On As
Enghouse Interactive CTI Connect Server	Telephony call control server.	Running	Automatic	Network Service

From the CTI Connect server, select **Control Program** from the **Apps** screen as shown below.

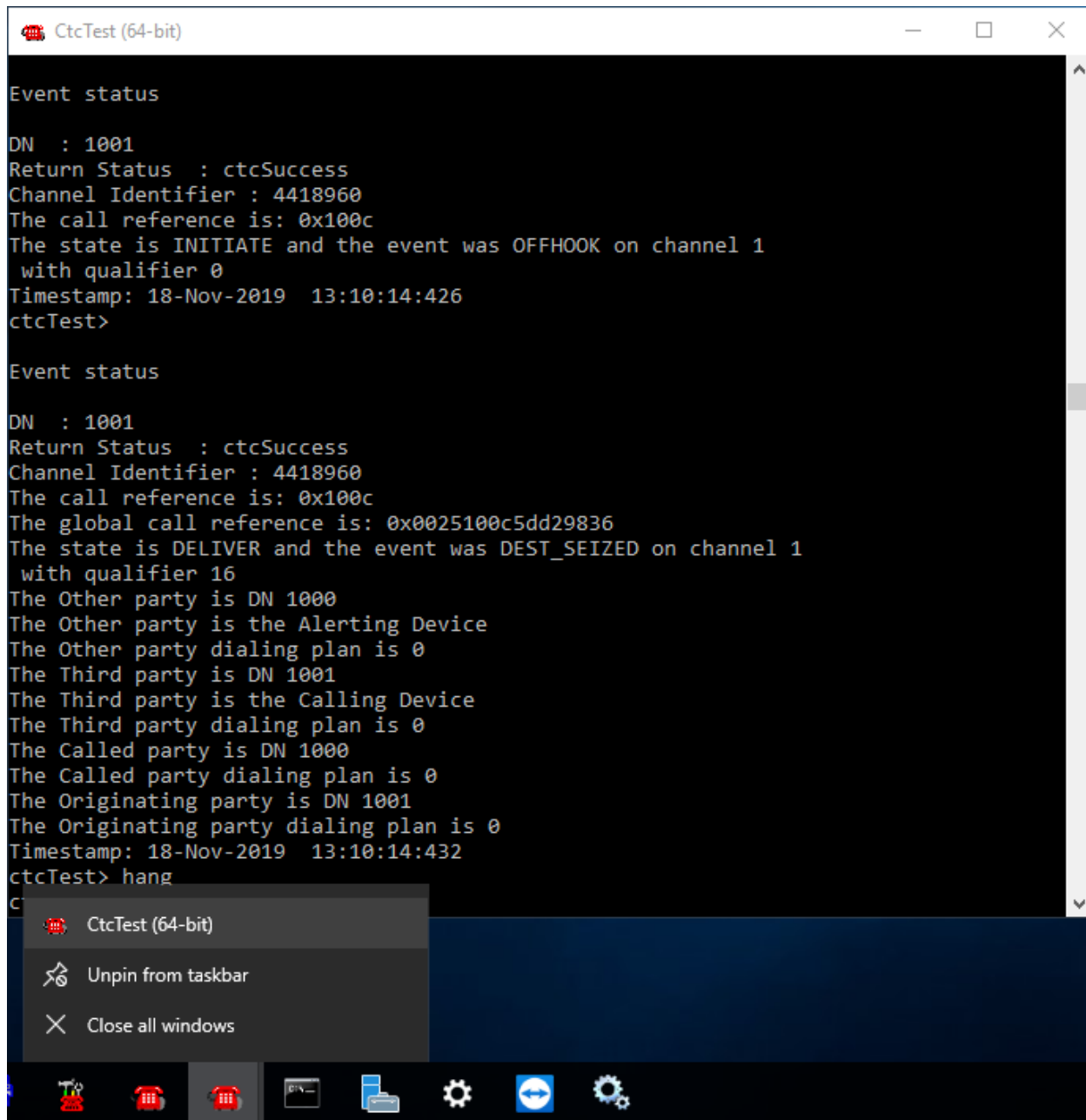


Ensure that the **Link State** associated with the administered **Logical Identifier** from **Section 7.2** in this case **AVAYA8** is **ON**.





Using the **CtcTest** tool, create a monitor on the required endpoint, in this case **1001**. Place a call to another station, in this case **1000**, from the monitored endpoint. Use the CtcTest tool to answer the call by executing the **answer** command and to hang up the call using the **hangup** command. Ensure that the call is answered and CtcTest can be used to complete the full variety of supported call control scenarios.



The screenshot shows the CtcTest (64-bit) application window. The main text area displays two event status messages. The first message shows the state as INITIATE and the event as OFFHOOK on channel 1. The second message shows the state as DELIVER and the event as DEST\_SEIZED on channel 1, with additional details about the parties involved. A context menu is open over the application window, showing options: 'CtcTest (64-bit)', 'Unpin from taskbar', and 'Close all windows'. The Windows taskbar is visible at the bottom with several icons.

```
Event status
DN : 1001
Return Status : ctcSuccess
Channel Identifier : 4418960
The call reference is: 0x100c
The state is INITIATE and the event was OFFHOOK on channel 1
with qualifier 0
Timestamp: 18-Nov-2019 13:10:14:426
ctcTest>

Event status
DN : 1001
Return Status : ctcSuccess
Channel Identifier : 4418960
The call reference is: 0x100c
The global call reference is: 0x0025100c5dd29836
The state is DELIVER and the event was DEST_SEIZED on channel 1
with qualifier 16
The Other party is DN 1000
The Other party is the Alerting Device
The Other party dialing plan is 0
The Third party is DN 1001
The Third party is the Calling Device
The Third party dialing plan is 0
The Called party is DN 1000
The Called party dialing plan is 0
The Originating party is DN 1001
The Originating party dialing plan is 0
Timestamp: 18-Nov-2019 13:10:14:432
ctcTest> hang
C
```

## 8.2. Verify TSAPI Connection Status

Using the Application Enablement Services web interface, click **Status** → **Status and Control** → **TSAPI Service Summary**. Select the appropriate **Switch Name** and click on **User Status**.

**Status | Status and Control | TSAPI 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**

**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
<input checked="" type="radio"/>	1	cm10	1	Talking	Tue Apr 11 08:04:41 2023	Online	20	0	15	15	30

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

The **CTI User Status** should show the “enghouse” user that was created in **Section 6.6**.

**CTI User Status**

☐ Enable page refresh every **60** seconds

CTI Users

Open Streams 1

Closed Streams 13

**Open Streams**

Name	Time Opened	Time Closed	Tlink Name
enghouse	Thu 11 May 2023 12:31:45 PM MDT		AVAYA#CM10#CSTA#AES10

### 8.3. Verify monitoring from Communication Manager

There are commands that can be used to show that certain stations or hunt groups are being monitored. The “List Monitor” command can be used to display any stations are being currently monitored.

list monitored-station															
MONITORED STATION															
Associations:		1		2		3		4		5		6		7	
		CTI		CTI		CTI		CTI		CTI		CTI		CTI	
Station Ext		Lnk	CRV	Lnk	CRV	Lnk	CRV	Lnk	CRV	Lnk	CRV	Lnk	CRV	Lnk	CRV
-----															
1000		1	0005												
1001		1	0003												

## 9. Conclusion

These Application Notes describe the compliance testing of Enghouse Interactive CTI Connect with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All test cases were executed successfully.

## 10. Additional References

This section references the product documentations that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 10.1
- [4] *Administering Avaya Aura® Session Manager*, Release 10.1

Product documentation for CTI Connect can be found by contacting Enghouse as per **Section 2.3**.

---

**©2023 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](mailto:devconnect@avaya.com).