



Avaya Solution & Interoperability Test Lab

Application Notes for Enhouse Interactive CTI Connect R8.5 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Enhouse Interactive CTI Connect to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the TSAPI interface. Enhouse Interactive CTI Connect is a CTI 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 the 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 Enghouse Interactive CTI Connect to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Telephony Service Application Programming Interface (TSAPI) interface. Enghouse Interactive 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 Computer Telephony Integration (CTI) package enables the development and running of CTI applications using the CTC 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 Interactive CTI Connect products, please visit the website at <http://enghouseinteractive.com/> or contact an authorized Enghouse representative at info.ei@enghouse.com.

USA

- Email: 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
- 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 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.

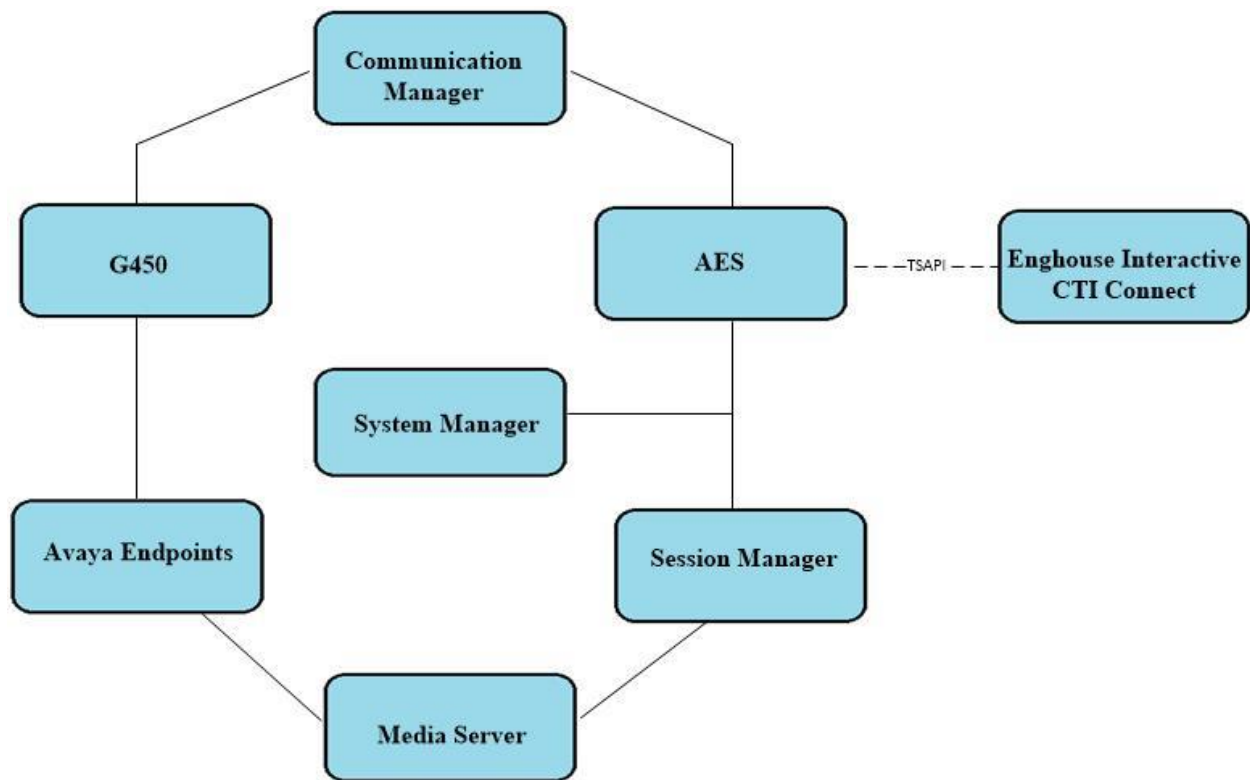


Figure 1: Connection of Enghouse Interactive CTI Connect with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.079880
Avaya Aura® Session Manager	Session Manager R8.1 Build No. – 8.1.0.0.810007
Avaya Aura® Communication Manager	R8.1.0.1.0 – SP1 R018x.01.0.890.0 Update ID 01.0.890.0-25393
Avaya Aura® Application Enablement Services	R8.1 8.1.0.0.9-1
Avaya Aura® Media Server	Appliance Version R8.0.0.12 Media Server 8.0.0.169 Element Manager 8.0.0.169
Avaya 96x1 H323 Deskphone	6.6604
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya J179 H323 Deskphone	6.7.002U
Avaya J129 SIP Deskphone	3.0.0.0.20
Enghouse Equipment	Software / Firmware Version
Enghouse Interactive CTI Connect	8.5.90.0
Enghouse Interactive CtcTest Tool	8.5

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.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	y	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?	y	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		
(NOTE: You must logoff & login to effect the permission changes.)			

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

(NOTE: You must logoff & login to effect the permission changes.)
```

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: cm81xvmpeg
      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: 37
```


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** and AES (**aes81xvmpg**).

```
display node-names ip
```

IP NODE NAMES	
Name	IP Address
IPOffice	10.10.40.25
aes81xvmpg	10.10.40.38
ams81vmpg	10.10.40.39
default	0.0.0.0
g430	10.10.40.15
procr	10.10.40.37
procr6	::
sm81xvmpg	10.10.40.32

(8 of 8 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
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

Page 1 of 3

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

- **AE Services Server:** Name obtained from the AES server, in this case **aes81xvmpg**.
- **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 3 of 3
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aes81xvmpg	*****	y	idle
2:				
3:				

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.

add cti-link 1		Page	1 of	3
		CTI LINK		
CTI Link: 1				
Extension: 1990				
Type: ADJ-IP				
		COR: 1		
Name: aes81xvmpg				

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**.

add hunt-group 90		Page 1 of 4
HUNT GROUP		
Group Number: 90	ACD? y	
Group Name: Sales	Queue? y	
Group Extension: 1800	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

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

add hunt-group 90		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: none		
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**.

change vector 1		Page 1 of 6
CALL VECTOR		
Number: 1	Name: Basic Routing	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n Lock? n
Basic? y	EAS? y 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 ringback	
03 queue-to	skill 1st pri m	
04 wait-time	100 secs hearing music	
05 goto step	3 if unconditionally	
06 stop		
07		
08		
09		
10		

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.
- **1st Skill** – enter the hunt group created in **Section 5.2.1**.

add vdn 1900	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 1900	Unicode Name? n
Name*: Sales	
Destination: Vector Number	1
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as ACD*? n
VDN of Origin Annc. Extension*:	
	1st Skill*: 90
	2nd Skill*:
	3rd Skill*:
SIP URI:	
* Follows VDN Override Rules	

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.

add agent-loginID 1400		Page 1 of 2
AGENT LOGINID		
Login ID: 1400	Unicode Name? n	AAS? n
Name: Agent One	AUDIX? n	
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code:	LWC Log External Calls? n	
Attribute:	AUDIX Name for Messaging:	
LoginID for ISDN/SIP Display? n		
Password:1234		
Password (enter again):1234		
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: system	
	Maximum time agent in ACW before logout (sec): system	
	Forced Agent Logout Time: :	
WARNING: Agent must log in again before changes take effect		

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

add agent-loginID 1400		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill: 90		Service Objective? n
Call Handling Preference: skill-level		Local Call Preference? n
SN	RL	SL
1: 90	1	16:
2:		17:
3:		18:
4:		19:
5:		20:
6:		
7:		
8:		

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 3rd 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.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

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

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

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

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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.

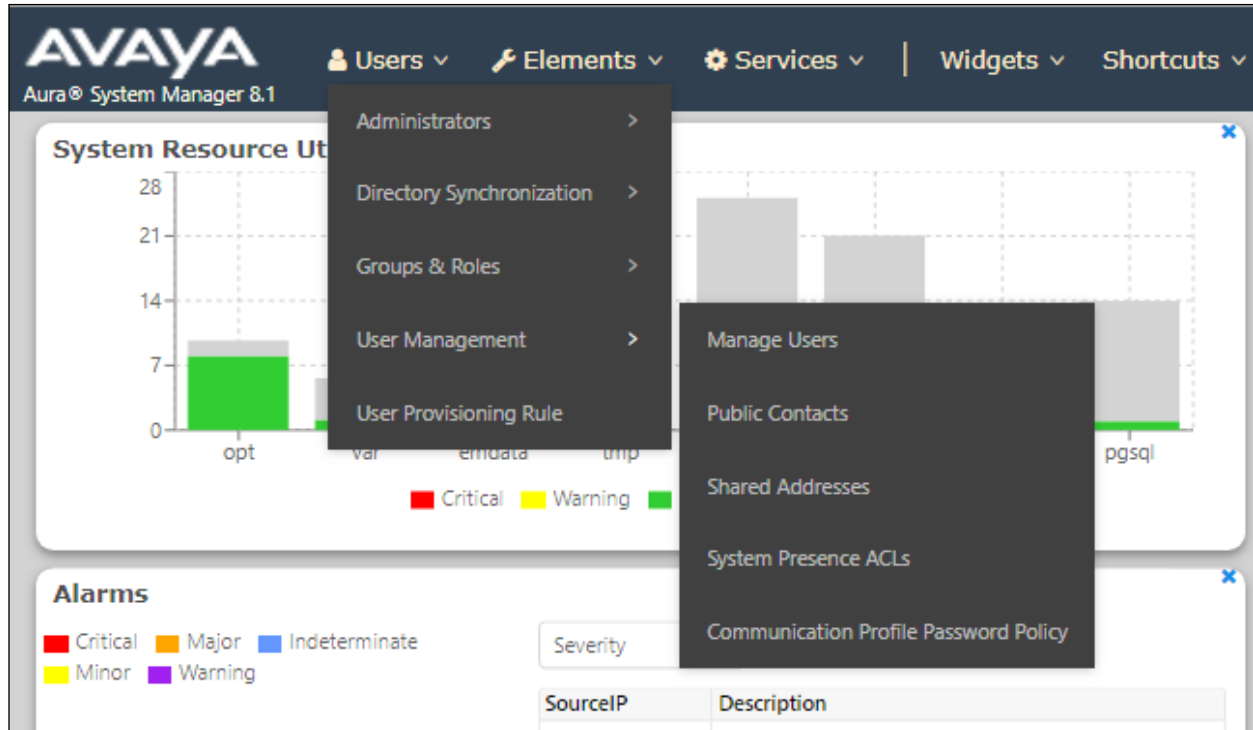
User ID:

Password:

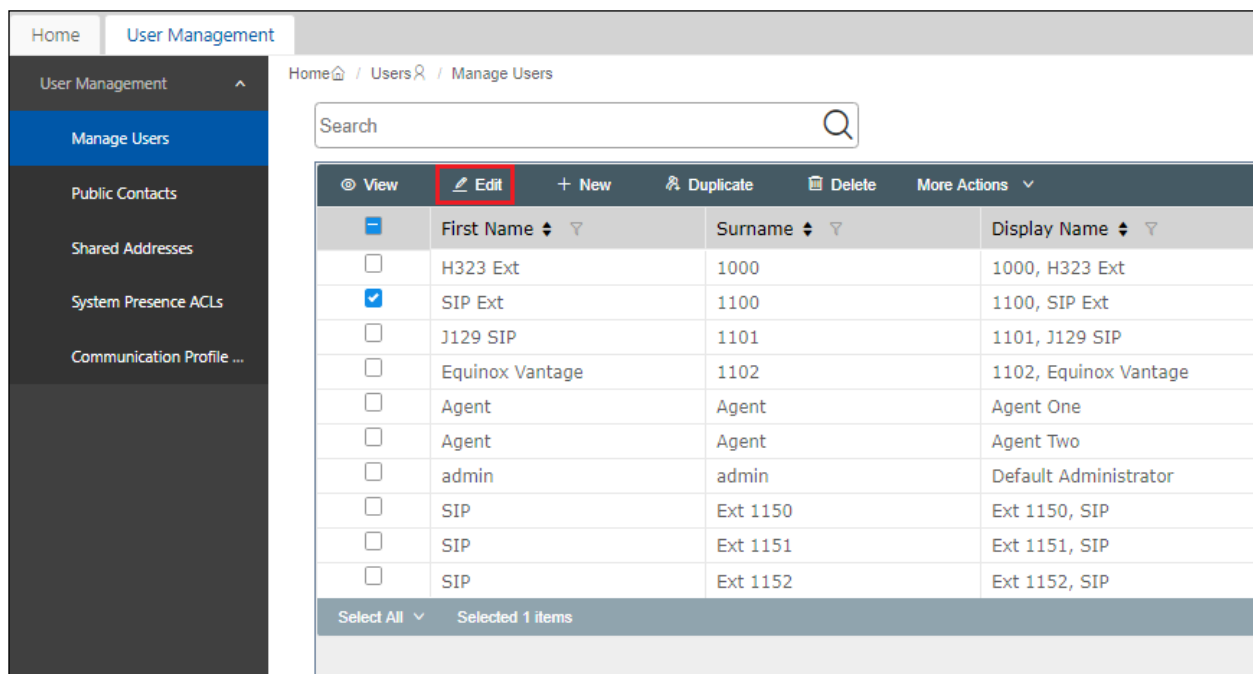
[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

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**.



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

Identity | **Communication Profile** | Membership | Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breeze® 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 : ☐

Commit & Continue | **Commit** | Cancel

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

Click on **Commit** once this is done to save the changes.

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 Breeze® 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 URI :

Select

Sip Trunk :

aar

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 :

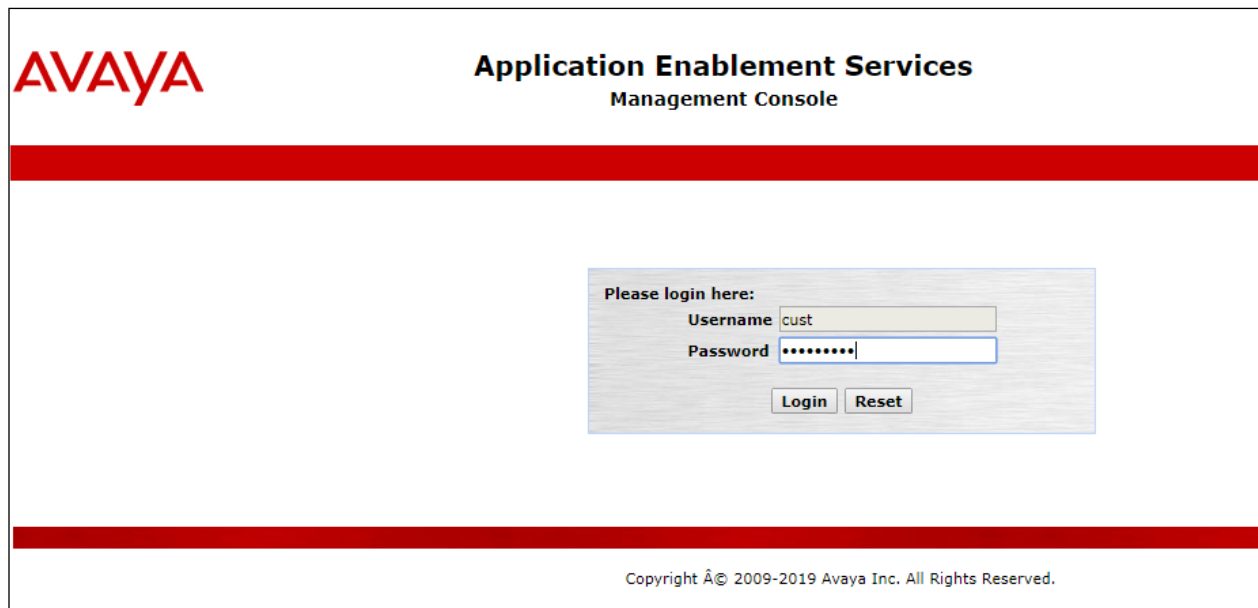
6. Configure Avaya Aura® Application Enablement Services

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 value "cust" and "Password" with masked characters "*****". 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.

The screenshot shows the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'AE Services' and includes an important note: 'IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.' Below this is a table listing services and their status.

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
AE Services HA	Not Configured	N/A	N/A	N/A

Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. Another note says: '* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.' At the bottom, 'License Information' states: 'You are licensed to run Application Enablement (CTI) release 8.x'.

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.

The screenshot shows the 'Communication Manager Interface | Switch Connections' page. The left navigation menu is similar to the previous screenshot, but 'Switch Connections' is highlighted under 'Communication Manager Interface'. The main content area is titled 'Switch Connections' and features a text input field and an 'Add Connection' button. Below these are several buttons: 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into 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 - cm81xvmpg

Switch Password: [password field]

Confirm Switch Password: [password field]

Msg Period: 30 Minutes (1 - 72)

Provide AE Services certificate to switch: ☐

Secure H323 Connection: ☒

Processor Ethernet: ☒

[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	
<input checked="" type="radio"/> cm81xvmpg	Yes	30	1

[Edit Connection] [Edit PE/CLAN IPs] [Edit H.323 Gatekeeper] [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 - cm81large

10.10.40.34 [Add/Edit Name or IP]

Name or IP Address
10.10.40.34

[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.



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 **cm81xvmpg**, 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 **8**.
- **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' configuration form. It contains the following fields and values: 'Link' is set to 1; 'Switch Connection' is a dropdown menu showing 'cm81xvmpg'; 'Switch CTI Link Number' is a dropdown menu showing 1; 'ASAI Link Version' is a dropdown menu showing 8; and 'Security' is a dropdown menu showing 'Both'. At the bottom of the form are three 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.**

When the TSAPI Link is completed, it should resemble the screen below.

TSAPI Links				
Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm81xvmppg	1	8	Both
<input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/>				

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**.



Application Enablement Services

Management Console

Maintenance | Service Controller

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

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 a web interface for the Avaya Security Database. The top navigation bar is red with the text "Security | Security Database | Tlinks". On the left is a sidebar menu with various categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, Tlinks (highlighted), Tlink Groups, and Worktops. The main content area on the right is titled "Tlinks" and contains a "Tlink Name" section with two radio button options: "AVAYA#CM81XVMGP#CSTA#AES81XVMGP" (selected) and "AVAYA#CM81XVMGP#CSTA-S#AES81XVMGP". Below these options is a "Delete Tlink" button.

Security Security Database Tlinks	
<ul style="list-style-type: none">▶ AE Services▶ Communication Manager Interface▶ High Availability▶ Licensing▶ Maintenance▶ Networking▼ Security<ul style="list-style-type: none">▶ Account Management▶ Audit▶ Certificate ManagementEnterprise Directory▶ Host AA▶ PAM▼ Security Database<ul style="list-style-type: none">▪ Control⊕ CTI Users▪ Devices▪ Device Groups▪ Tlinks▪ Tlink Groups▪ Worktops	<h3>Tlinks</h3> <p>Tlink Name</p> <p><input checked="" type="radio"/> AVAYA#CM81XVMGP#CSTA#AES81XVMGP</p> <p><input type="radio"/> AVAYA#CM81XVMGP#CSTA-S#AES81XVMGP</p> <p><button>Delete Tlink</button></p>

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"> 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			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"/>
	DLG Port	TCP Port	5678	
	TSAPI Ports			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"/>			
DMCC Server Ports			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"/>	
H.323 Ports				
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"/>			
Server Media			Enabled Disabled	
		<input checked="" type="radio"/>	<input type="radio"/>	

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**.



Application Enablement Services Management Console

Security | Security Database | CTI Users | List All Users

▶ 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

CTI Users

User ID	Common Name
<input checked="" type="radio"/> enghouse	enghouse

EditList 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	enghouse
	Common Name	enghouse
	Worktop Name	NONE ▾
	Unrestricted Access	<input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	None ▾
Call and Device Monitoring:	Device Monitoring	None ▾
	Calls On A Device Monitoring	None ▾
	Call Monitoring	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▾
<input checked="" type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

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

AVAYA		Application Enablement Services Management Console
Security Security Database CTI Users List All Users		
<ul style="list-style-type: none">▶ AE Services▶ Communication Manager Interface▶ High Availability▶ Licensing▶ Maintenance▶ Networking▼ Security	Apply Changes to CTI User Properties Warning! Are you sure you want to apply the changes? <input checked="" type="button" value="Apply"/> <input type="button" value="Cancel"/>	

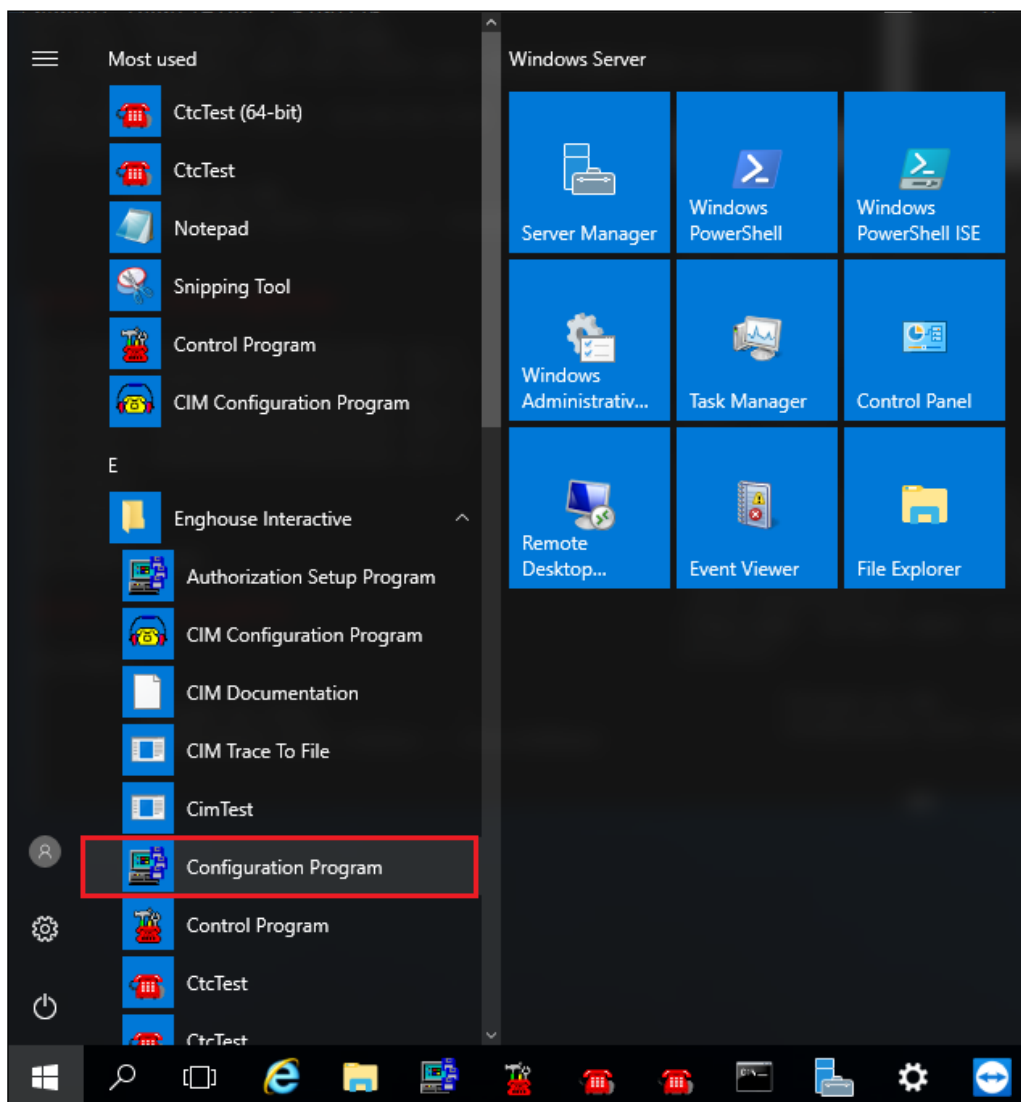
7. Configure EngHouse Interactive CTI Connect

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

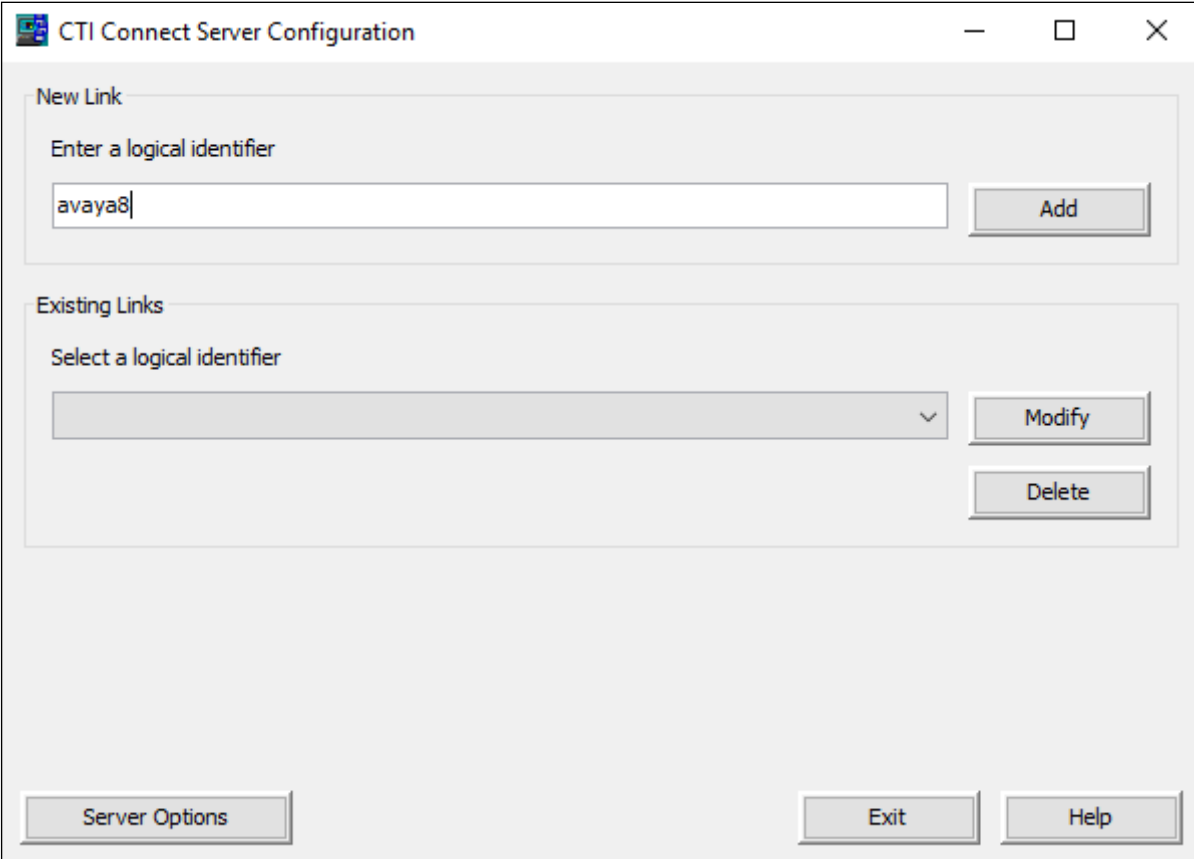
7.1. Launch configuration program

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 **avaya8** and click **Add**.



The image shows a Windows-style application window titled "CTI Connect Server Configuration". The window has a standard title bar with minimize, maximize, and close buttons. The main content area is divided into two sections. The top section, labeled "New Link", contains a text input field with the placeholder "Enter a logical identifier" and the text "avaya8" entered. To the right of the input field is an "Add" button. The bottom section, labeled "Existing Links", contains a dropdown menu with the placeholder "Select a logical identifier". To the right of the dropdown are "Modify" and "Delete" buttons. At the bottom of the window, there are three buttons: "Server Options", "Exit", and "Help".

CTI Connect Server Configuration

New Link

Enter a logical identifier

avaya8

Add

Existing Links

Select a logical identifier

Modify

Delete

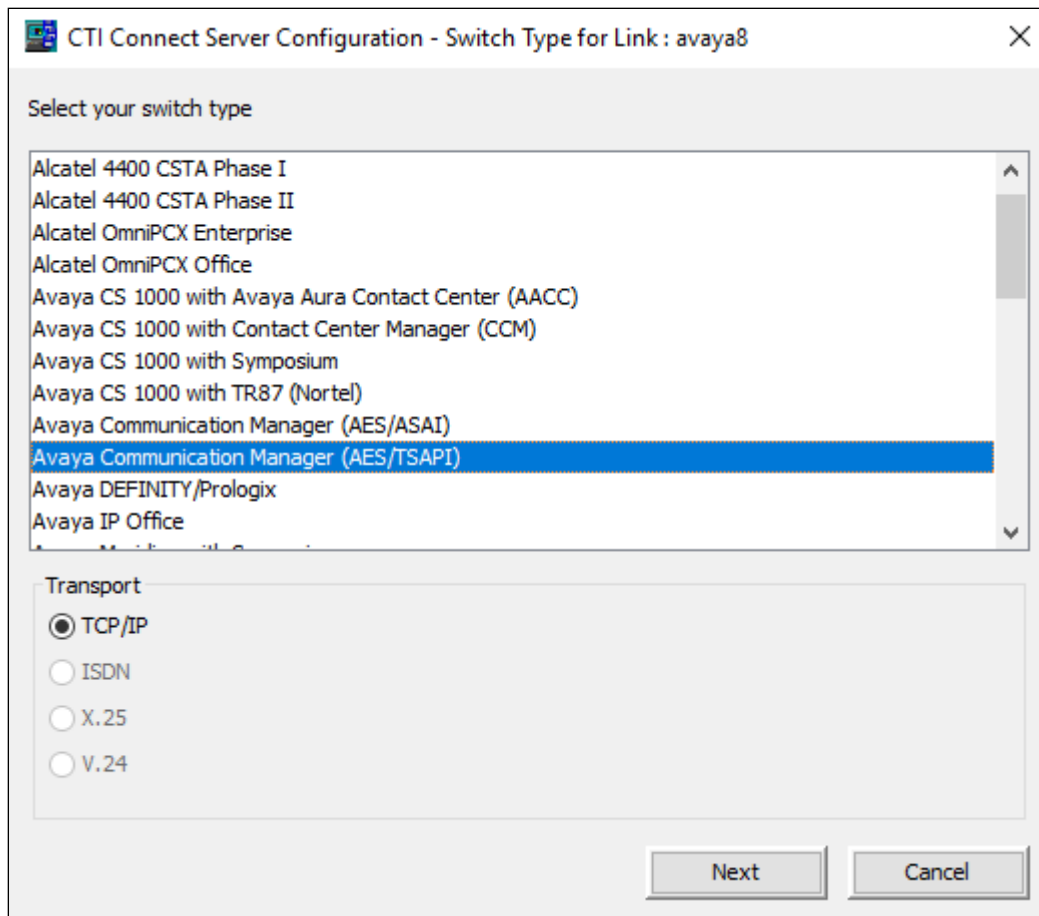
Server Options

Exit

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 **10.10.40.38**.
- **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**.

CTI Connect Server Configuration - Configuring Link : avaya8

Transport

AES Server Address: 10.10.40.38

Port Number: 450

Common

☒ Auto Start Link

☐ Auto Restart Monitors

Timestamp: Server

Call Information Manager: localhost

Protocol Specific

TSAPI Service Name: AYA#CM81XVMPG#CSTA#AES81XVMPG

Username: Enghouse

Password: Avaya123&

Device Level Authorization

Authorization: Off

Advanced Trace Save 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.

Services (Local)

Enghouse Interactive CTI Connect Server

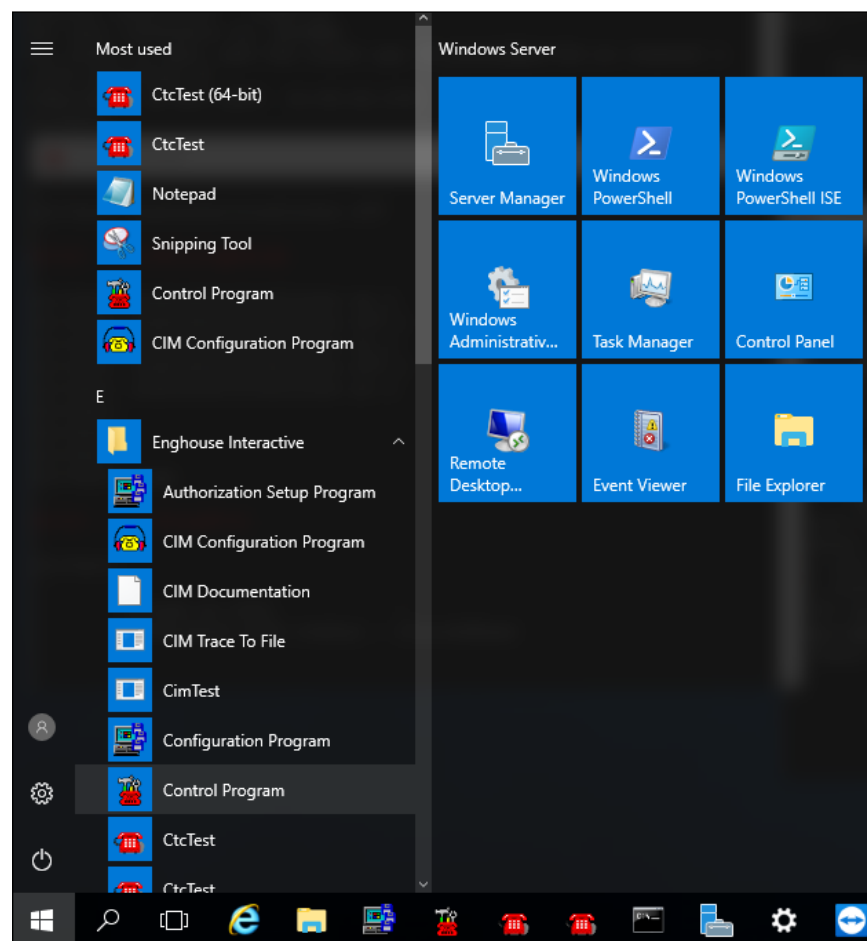
Stop the service

Restart the service

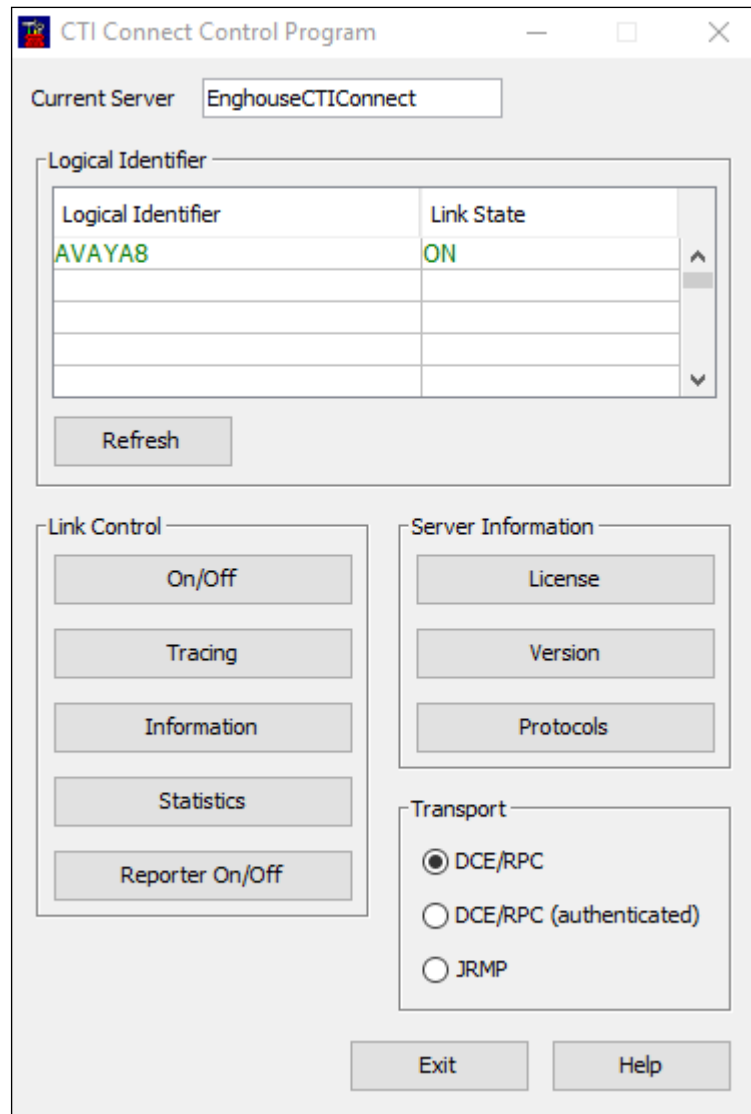
Description:
Telephony call control server.

Name	Description	Status	Startup Type	Log On As
Embedded Mode	The Embedded Mode service enables scenarios related to...		Manual (Trig...	Local System
Encrypting File System (EFS)	Provides the core file encryption technology used to stor...		Manual (Trig...	Local System
Enghouse Interactive Call Information Manager	Telephony call data management server.	Running	Automatic	Network Service
Enghouse Interactive CSTA Phase II Switch Simula...	A software switch simulator providing CSTA Phase II tele...		Manual	Network Service
Enghouse Interactive CTI Connect Server	Telephony call control server.	Running	Automatic	Network Service
Enghouse Interactive Media Gateway	Provides call and media control for Enghouse Interactive ...	Running	Automatic	Network Service
Enterprise App Management Service	Enables enterprise application management.		Manual	Local System
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service pro...		Manual	Local System
Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) ...		Manual	Local Service
Function Discovery Resource Publication	Publishes this computer and resources attached to this c...		Manual	Local Service
Geolocation Service	This service monitors the current location of the system a...	Running	Manual (Trig...	Local System
Group Policy Client	The service is responsible for applying settings configure...	Running	Automatic (T...	Local System

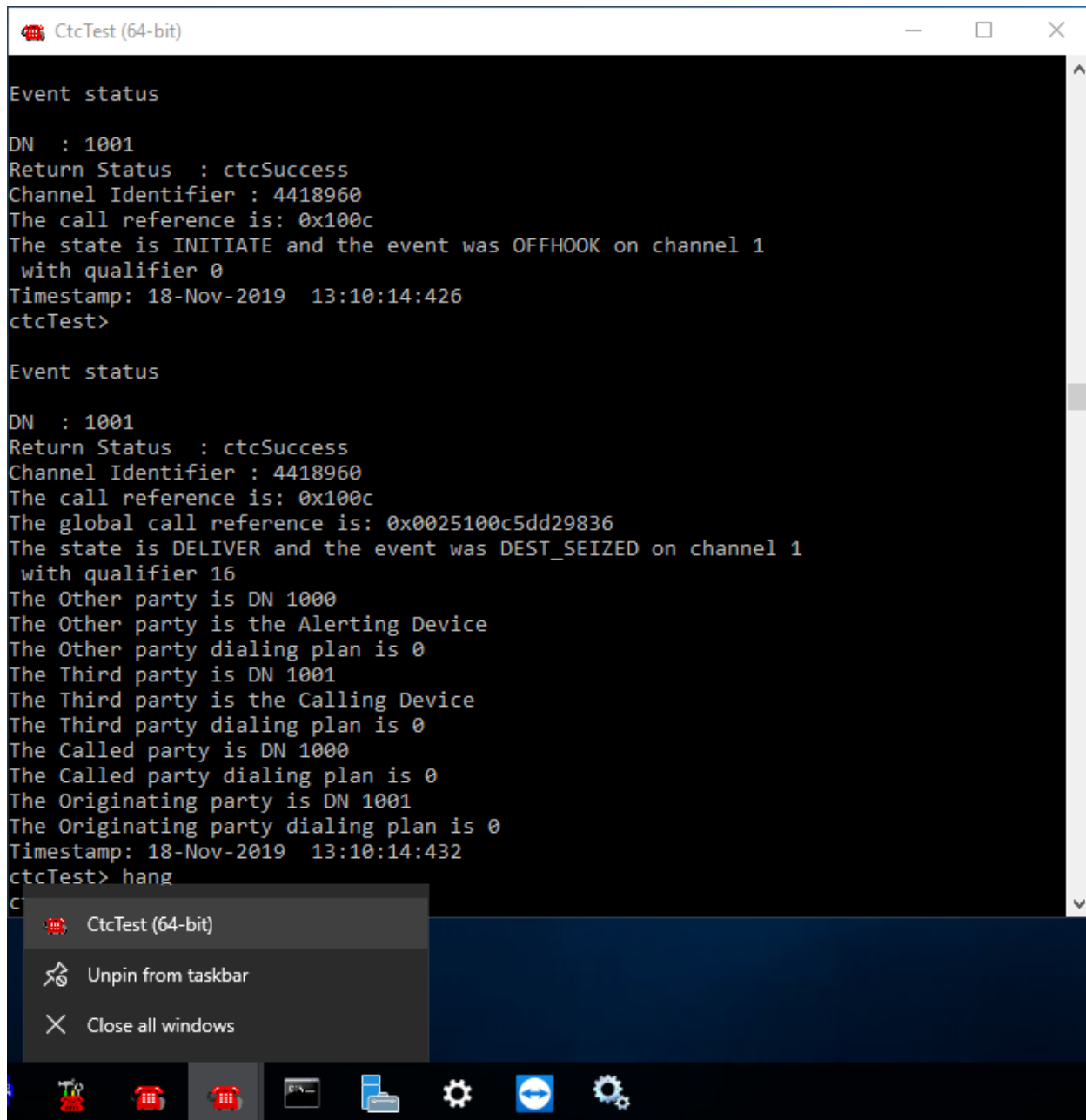
From the CTI Connect server, select **Control Program** from the **Apps** screen as shown below.



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 is for DN 1001, showing a successful call initiation (OFFHOOK) on channel 1. The second message is for DN 1001, showing a successful call delivery (DEST_SEIZED) on channel 1, with detailed information about the other party (DN 1000), third party (DN 1001), and called party (DN 1000). The user has entered the 'hang' command at the prompt. 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, showing several icons including the Start button, taskbar search, and several application 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
```

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

▶ 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
<input checked="" type="radio"/>	1	cm81xvmpg	1	Talking	Wed Nov 13 09:35:55 2019	Online
<input type="radio"/>	2	cm81large	1	Talking	Wed Nov 13 09:35:52 2019	Online

Online Offline

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

TSAPI Service Status TLink Status **User Status**

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 All Users Submit

Open Streams 5

Closed Streams 9

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Wed 02 Oct 2019 09:06:57 AM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 02 Oct 2019 09:06:58 AM IST		AVAYA#CM81LARGE#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 02 Oct 2019 09:06:58 AM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 02 Oct 2019 09:06:58 AM IST		AVAYA#CM81LARGE#CSTA#AES81XVMPG
Enghouse	Wed 13 Nov 2019 08:50:02 AM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG

Show Closed Streams Close All Opened Streams Back

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.

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 with observations noted in **Section 2.2**.

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 8.1
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 8.1
- [4] *Administering Avaya Aura® Session Manager*, Release 8.1

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

©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.