Abstract

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 TSAPI interface. Enghouse 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 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: 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:

<table>
<thead>
<tr>
<th>Avaya Equipment</th>
<th>Software / Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® System Manager</td>
<td>System Manager 8.1.0.0&lt;br&gt;Build No. – 8.1.0.0.733078&lt;br&gt;Software Update Revision No: 8.1.0.079880</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>Session Manager R8.1&lt;br&gt;Build No. – 8.1.0.0.810007</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>R8.1.0.1.0 – SP1&lt;br&gt;R018x.01.0.890.0 Update ID 01.0.890.0-25393</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services</td>
<td>R8.1&lt;br&gt;8.1.0.0.0.9-1</td>
</tr>
<tr>
<td>Avaya Aura® Media Server</td>
<td>Appliance Version R8.0.0.12&lt;br&gt;Media Server 8.0.0.169&lt;br&gt;Element Manager 8.0.0.169</td>
</tr>
<tr>
<td>Avaya 96x1 H323 Deskphone</td>
<td>6.6604</td>
</tr>
<tr>
<td>Avaya 96x1 SIP Deskphone</td>
<td>7.1.2.0.14</td>
</tr>
<tr>
<td>Avaya J179 H323 Deskphone</td>
<td>6.7.002U</td>
</tr>
<tr>
<td>Avaya J129 SIP Deskphone</td>
<td>3.0.0.0.20</td>
</tr>
<tr>
<td><strong>Enghouse Equipment</strong></td>
<td><strong>Software / Firmware Version</strong></td>
</tr>
<tr>
<td>Enghouse Interactive CTI Connect</td>
<td>8.5.90.0</td>
</tr>
<tr>
<td>Enghouse Interactive CtcTest Tool</td>
<td>8.5</td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>display system-parameters</th>
<th>Page 10 of 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAI ENHANCED FEATURES</td>
<td></td>
</tr>
<tr>
<td>Adjunct Routing? y</td>
<td></td>
</tr>
<tr>
<td>CTI Stations? y</td>
<td></td>
</tr>
<tr>
<td>Increased Adjunct Route Capacity? y</td>
<td></td>
</tr>
<tr>
<td>Phantom Calls? y</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>display system-parameters</th>
<th>Page 5 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAI PROPRIETARY FEATURES</td>
<td></td>
</tr>
<tr>
<td>Proprietary? y</td>
<td></td>
</tr>
</tbody>
</table>

(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.

<table>
<thead>
<tr>
<th>display system-parameters</th>
<th>Page 5 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEATURE-RELATED SYSTEM PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>SYSTEM PRINTER PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Endpoint:</td>
<td></td>
</tr>
<tr>
<td>Lines Per Page: 60</td>
<td></td>
</tr>
<tr>
<td>SYSTEM-WIDE PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Switch Name: cm8lxvmpg</td>
<td></td>
</tr>
<tr>
<td>Emergency Extension Forwarding (min): 10</td>
<td></td>
</tr>
<tr>
<td>Enable Inter-Gateway Alternate Routing? n</td>
<td></td>
</tr>
<tr>
<td>Enable Dial Plan Transparency in Survivable Mode? n</td>
<td></td>
</tr>
<tr>
<td>COR to Use for DPT: station</td>
<td></td>
</tr>
<tr>
<td>EC500 Routing in Survivable Mode: dpt-then-ec500</td>
<td></td>
</tr>
<tr>
<td>MALICIOUS CALL TRACE PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Apply MCT Warning Tone? n</td>
<td></td>
</tr>
<tr>
<td>MCT Voice Recorder Trunk Group:</td>
<td></td>
</tr>
<tr>
<td>Delay Sending RElease (seconds): 0</td>
<td></td>
</tr>
<tr>
<td>SEND ALL CALLS OPTIONS</td>
<td></td>
</tr>
<tr>
<td>Send All Calls Applies to: station</td>
<td></td>
</tr>
<tr>
<td>Auto Inspect on Send All Calls? n</td>
<td></td>
</tr>
<tr>
<td>Preserve previous AUX Work button states after deactivation? n</td>
<td></td>
</tr>
<tr>
<td>UNIVERSAL CALL ID</td>
<td></td>
</tr>
<tr>
<td>Create Universal Call ID (UCID)? y</td>
<td>UCID Network Node ID: 37</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPOffice</td>
<td>10.10.40.25</td>
</tr>
<tr>
<td>aes81xvmpg</td>
<td>10.10.40.38</td>
</tr>
<tr>
<td>ams81vmpg</td>
<td>10.10.40.39</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>g430</td>
<td>10.10.40.15</td>
</tr>
<tr>
<td>procr</td>
<td>10.10.40.37</td>
</tr>
<tr>
<td>procr6</td>
<td>::</td>
</tr>
<tr>
<td>sm81xvmpg</td>
<td>10.10.40.32</td>
</tr>
</tbody>
</table>

(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

<table>
<thead>
<tr>
<th>Service</th>
<th>Enabled</th>
<th>Local Node</th>
<th>Local Port</th>
<th>Remote Node</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AESVCS</td>
<td>y</td>
<td>procr</td>
<td>8765</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
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.

<table>
<thead>
<tr>
<th>Server ID</th>
<th>AE Services Server</th>
<th>Password</th>
<th>Enabled</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>aes81xvmpg</td>
<td>********</td>
<td>y</td>
<td>idle</td>
</tr>
</tbody>
</table>

### 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
```

**CTI LINK**

**CTI Link**: 1  
**Extension**: 1990  
**Type**: ADJ-IP  
**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
```

<table>
<thead>
<tr>
<th>HUNT GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Number: 90</td>
</tr>
<tr>
<td>Group Name: Sales</td>
</tr>
<tr>
<td>Group Extension: 1800</td>
</tr>
<tr>
<td>Group Type: ucd-mia</td>
</tr>
<tr>
<td>TN: 1</td>
</tr>
<tr>
<td>COR: 1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Queue Limit: unlimited</td>
</tr>
<tr>
<td>Calls Warning Threshold: Port:</td>
</tr>
<tr>
<td>Time Warning Threshold: Port:</td>
</tr>
</tbody>
</table>
On Page 2, set Skill to y.

add hunt-group 90

HUNT GROUP

Skill? y
AAS? n
Expected Call Handling Time (sec): 180
Service Level Target (% in sec): 80
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

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

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
AGENT LOGINID

Login ID: 1400
Name: Agent One
TN: 1
COR: 1
Coverage Path: LWC Reception: spec
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
AUX Agent Considered Idle (MIA): system
Work Mode on Login: system
Max 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
AGENT LOGINID

Direct Agent Skill: 90
Call Handling Preference: skill-level
Service Objective? n
Local Call Preference? n

SN RL SL 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” 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.
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.

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

### 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.
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](image)

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](image)

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](image)
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 cm81xvmph, 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.
Another screen appears for confirmation of the changes made. Choose **Apply**.

![Apply Changes to Link](image)

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

![TSAPI Links](image)

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

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

![Configuration Program Launch](image_url)
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.
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**.
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
<th>Log On As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enghouse Interactive CTI Connect Server</td>
<td>Enghouse Interactive Call Information Manager</td>
<td>Running</td>
<td>Manual (Trg.)</td>
<td>Local System</td>
</tr>
<tr>
<td>Enghouse Interactive Media Gateway</td>
<td>Provides call and media control for Enghouse interactive media gateway</td>
<td>Running</td>
<td>Manual (Trg.)</td>
<td>Local System</td>
</tr>
<tr>
<td>Function Discovery Provider</td>
<td>The Function Discovery Provider hosts the Function Discovery (FD) service.</td>
<td>Manual</td>
<td>Manual (Trg.)</td>
<td>Local System</td>
</tr>
<tr>
<td>Function Discovery Resource Publication</td>
<td>Publishes this computer and resources attached to this computer.</td>
<td>Manual</td>
<td>Manual (Trg.)</td>
<td>Local System</td>
</tr>
<tr>
<td>Geolocation Service</td>
<td>The service monitors the current location of the system and provides location services.</td>
<td>Manual</td>
<td>Manual (Trg.)</td>
<td>Local System</td>
</tr>
<tr>
<td>Group Policy Client</td>
<td>The service is responsible for applying settings configured in the Group Policy service.</td>
<td>Manual</td>
<td>Manual (Trg.)</td>
<td>Local System</td>
</tr>
</tbody>
</table>

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 answercall 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.
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 and Control TSAPI Service Summary](image)

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

![CTI User Status](image)
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](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.