Avaya Solution & Interoperability Test Lab

Application Notes for configuring Enghouse Interactive CTI Connect R8.2 with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 – Issue 1.0

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 Telephony Service API (TSAPI) interface. Enghouse Interactive CTI Connect is a Computer Telephony Integration (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 API (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. Enghouse 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 API (TSAPI) interface.
- 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.

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.

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.
- Agent Ready/Not Ready.
- Agent State Synchronization with Agent Telephones.
- Hold/Unhold.
- Transfers, Blind/Consultative.
- Conferencing.
- Customer calls to Agents (Calls to the Contact Center Skillset).
- Calls from Agent to Agent.
- Calls from Agent to Non Agent.
- Send DTMF.

- Deflect call, Call Forward.
- 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:	http://enghouseinteractive.com/support.php
• Phone:	+1 800.788.9730 Self-Service
• Phone:	+1 800.872.2272 Live-Service

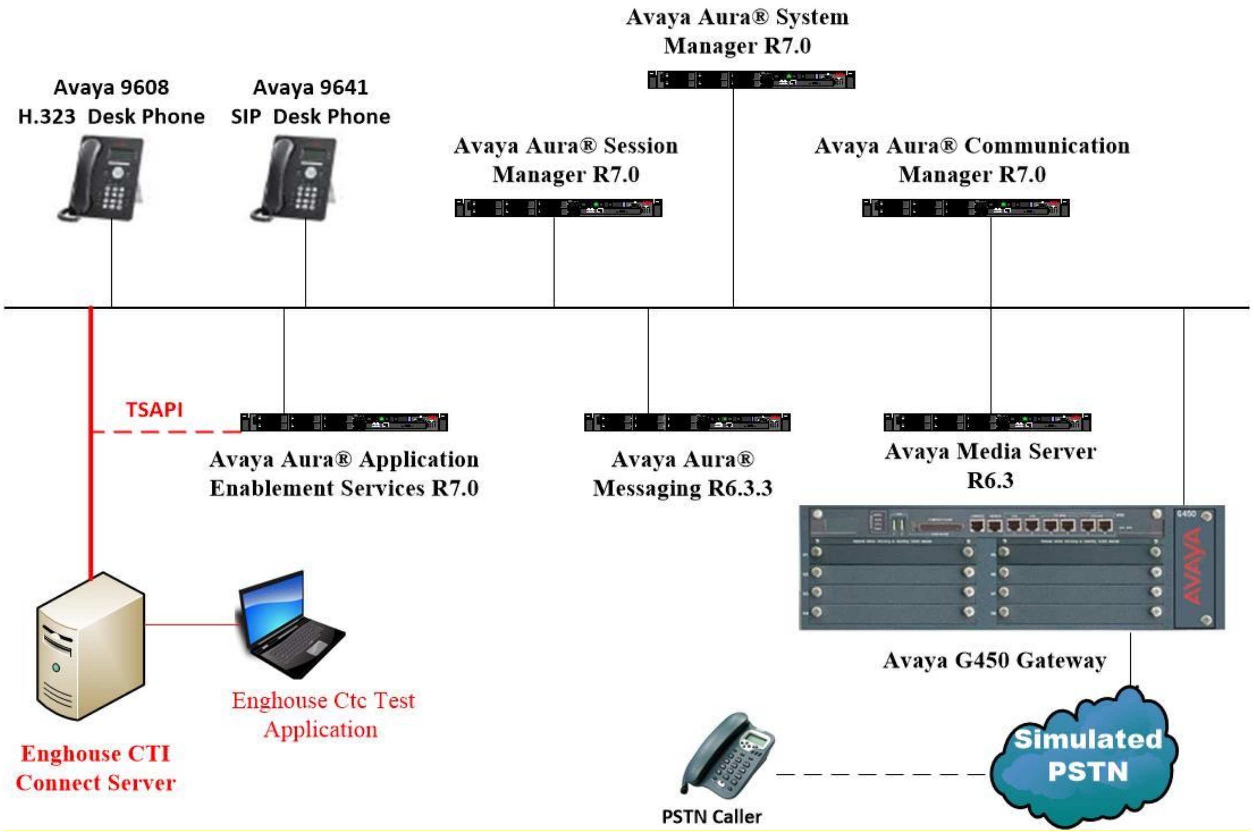
EMEA

• Email:	EnvoxSupport@enghouse.com / SupportEnvox@Syntellect.com
• Website:	http://www.enghouseinteractive.com/services/support/
• Phone:	+44 870 220 2205

3. Reference Configuration

Figure 1 below shows Avaya Aura® Communication Manager R7.0, serving H.323 endpoints with an Avaya G450 Media Gateway and an Avaya Media Server, was configured with Avaya Aura® Application Enablement Services R7.0 hosted on VMware providing a TSAPI interface to which the Enghouse Interactive CTI Connect application connects. Avaya Aura® Session Manager R7.0 provides the point of registration for Avaya SIP endpoints. Avaya Aura® System Manager Server provides a means to manage and configure Session Manager. All of these applications were hosted on VMware ESXi 5.5 infrastructure.

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



Avaya Aura® System Manager R7.0
Avaya 9608 H.323 Desk Phone
Avaya 9641 SIP Desk Phone
Avaya Aura® Session Manager R7.0
Avaya Aura® Communication Manager R7.0
TSAPI
Avaya Aura® Application Enablement Services R7.0
Avaya Aura® Messaging R6.3.3
Avaya Media Server R6.3
Avaya G450 Gateway
Enghouse Ctc Test Application
Enghouse CTI Connect Server
Simulated PSTN
PSTN Caller

Figure 1: Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services with Enghouse Interactive CTI Connect solution

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.0 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.0.064859 Feature Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP1 Build No. – 7.0.1.0.701007
Avaya Aura® Communication Manager running on a virtual server	R7.0 R017x.00.0.441.0 00.0.441.0-23012
Avaya Aura® Application Enablement Services running on a virtual server	R7.0 Build No – 7.0.0.0.1.13
Avaya Media Server running on a virtual server	R6.3
Avaya G450 Gateway	37.19.0 /1
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9608 SIP Deskphone	96x1 SIP Release 7.0.0.39
Enghouse CTI Connect CtcTest Tool	8.2.433.0 8.2.433.0

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:

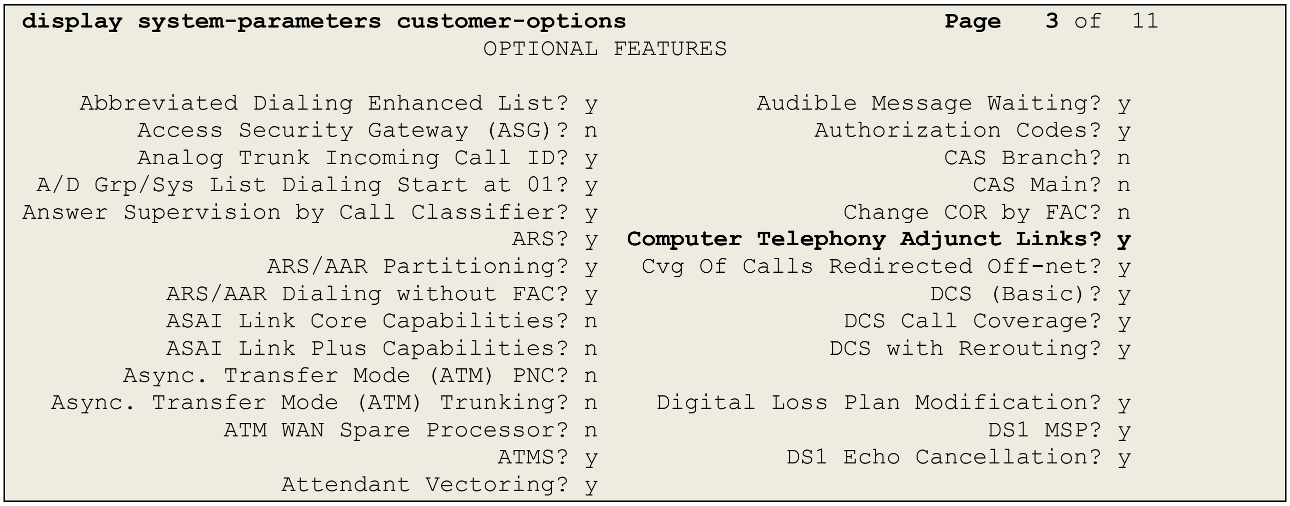
- Configure Interface to Avaya Aura® Application Enablement Services.
- Configure Call Center Features.
- Configure SIP Endpoints for Third Party Call Control.

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 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.



```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? 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** and AES (**aes70vmpg**).

```
display node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.40.12
aes70vmpg           10.10.40.26
default             0.0.0.0
G450                10.10.40.15
procr               10.10.40.13
```

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      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS         y           procr        8765
```

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes70vmpg**.
- **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       Password          Enabled     Status
                    Server
      1:         aes70vmpg         ********          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: 7999
     Type: ADJ-IP
                                                                      COR: 1
     Name: aes70vmpg
```

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: 6900                          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: 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

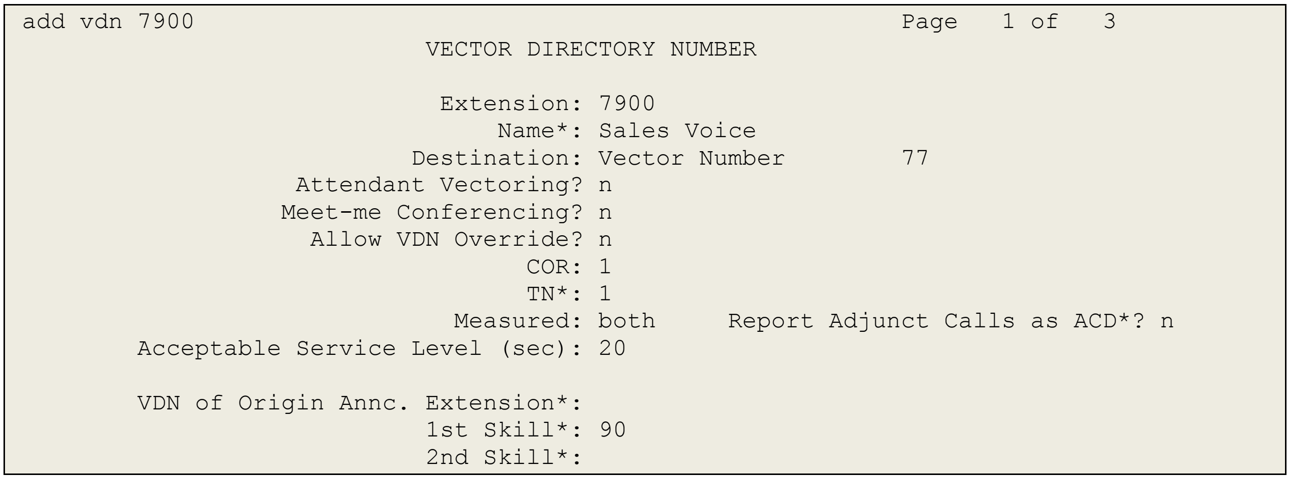
Enter the command **change vector x** where **x** is the required vector number. Configure as shown below so that calls **queue-to skill 1st**. Skill 1st the hunt group configured in the VDN in **Section5.2.3**.

```
change vector 77                                              Page   1 of   6
                                  CALL VECTOR

    Number: 77               Name: EMC Vector
Multimedia? y      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    2   secs hearing ringback
03 queue-to     skill 1st  pri m
04 wait-time    10  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 7900                                                 Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 7900
                                 Name*: Sales Voice
                           Destination: Vector Number        77
                   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*: 90
                            2nd Skill*:
```

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 7700                                          Page   1 of   2
                                 AGENT LOGINID

                Login ID: 7700                                  AAS? n
                    Name: Sales Agent (Dave)                  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:
                                            Password (enter again):
                                                       Auto Answer: station
                                                 MIA Across Skills: system
 AUX Agent Considered Idle (MIA)? system   ACW Agent Considered Idle: 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
```

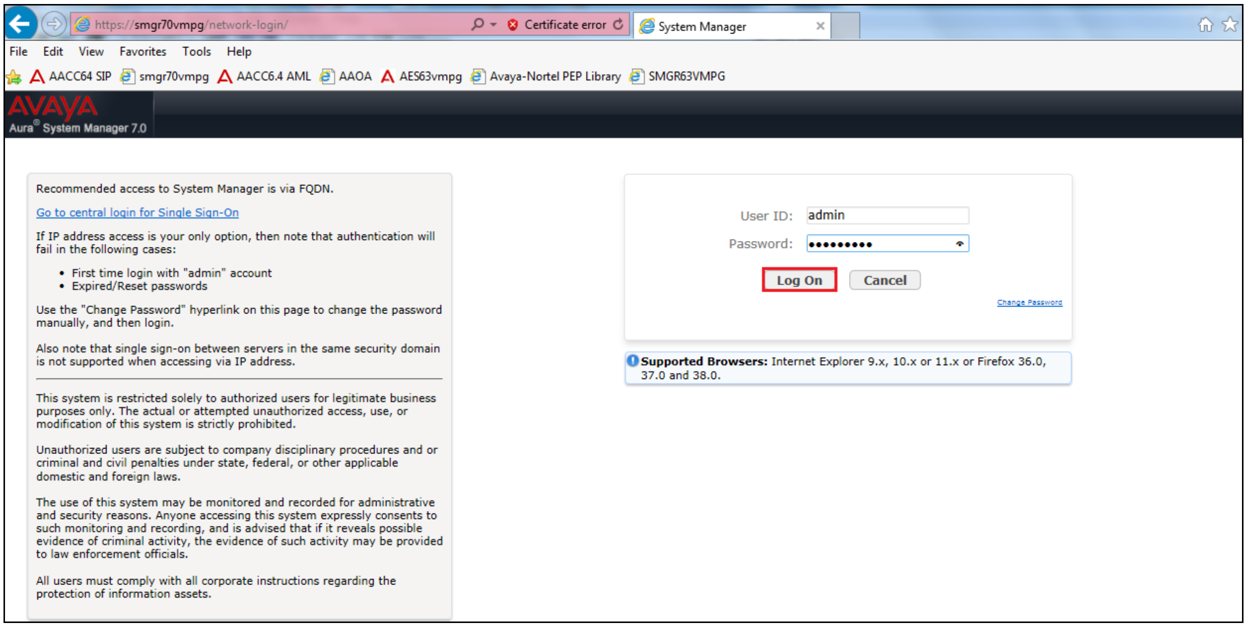
On **Page 2,** enter the hunt group number configured in **Section 5.2.1** in the **SN** (Skill Number) column and enter an appropriate **SL** (skill level).

```
add agent-loginID 7700                                          Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                                Service Objective? n
Call Handling Preference: skill-level                 Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 90      1       16:
 2: 10      1       17:
 3: 20      1       18:
 4: 30      1       19:
 5:                 20:
 6:
 7:
 8:
 9:
10:
```

5.3. Configure SIP Endpoints for Third Party Call Control

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 >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Adddress >/SMGR**. 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.


https://smgr70vmpg/network-login/
Certificate error
System Manager
File Edit View Favorites Tools Help
AACC64 SIP smgr70vmpg AACC6.4 AML AAOA AES63vmpg Avaya-Nortel PEP Library SMGR63VMPG
AVAYA
Aura® System Manager 7.0
Log On
Cancel
Change Password

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.

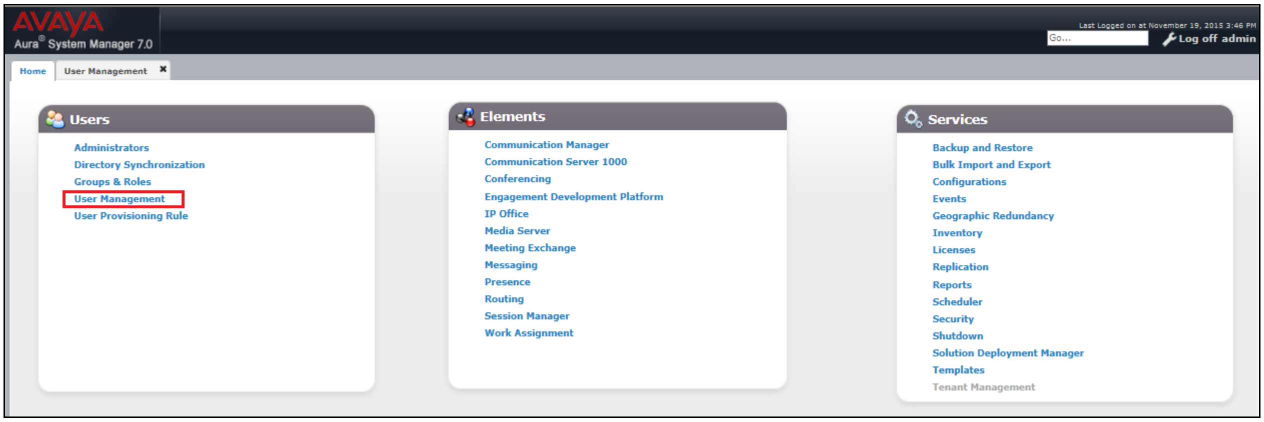
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law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

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

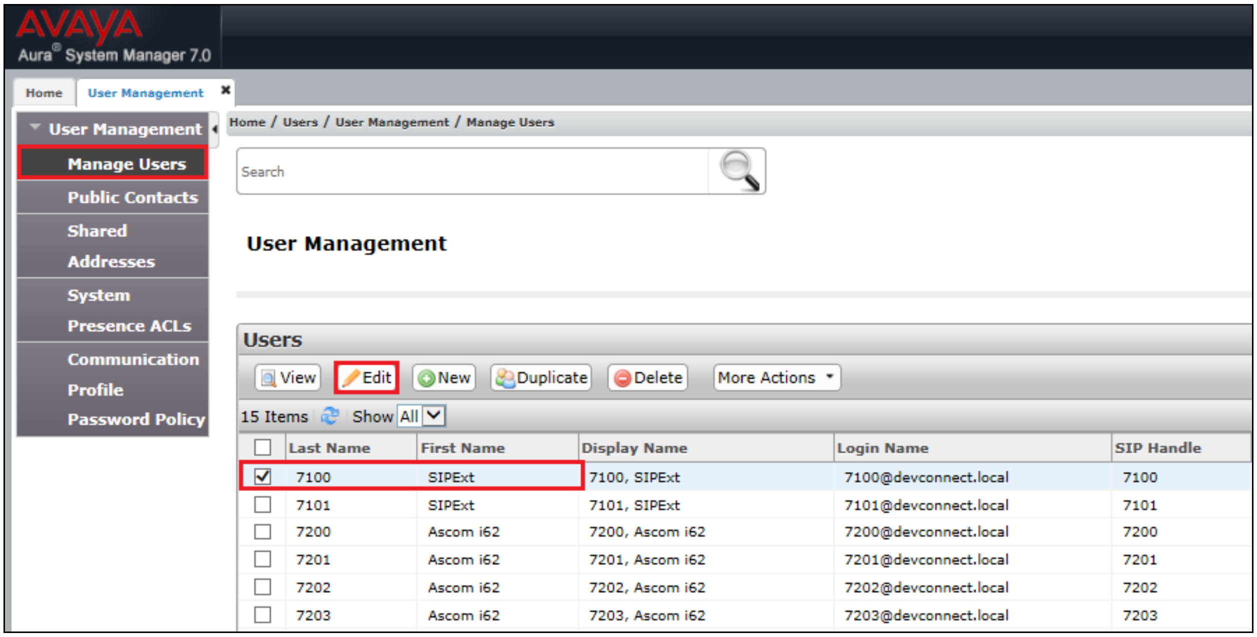
User ID: admin
Password: ●●●●●●●●●

Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

From the home page click on **User Management** highlighted below.



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

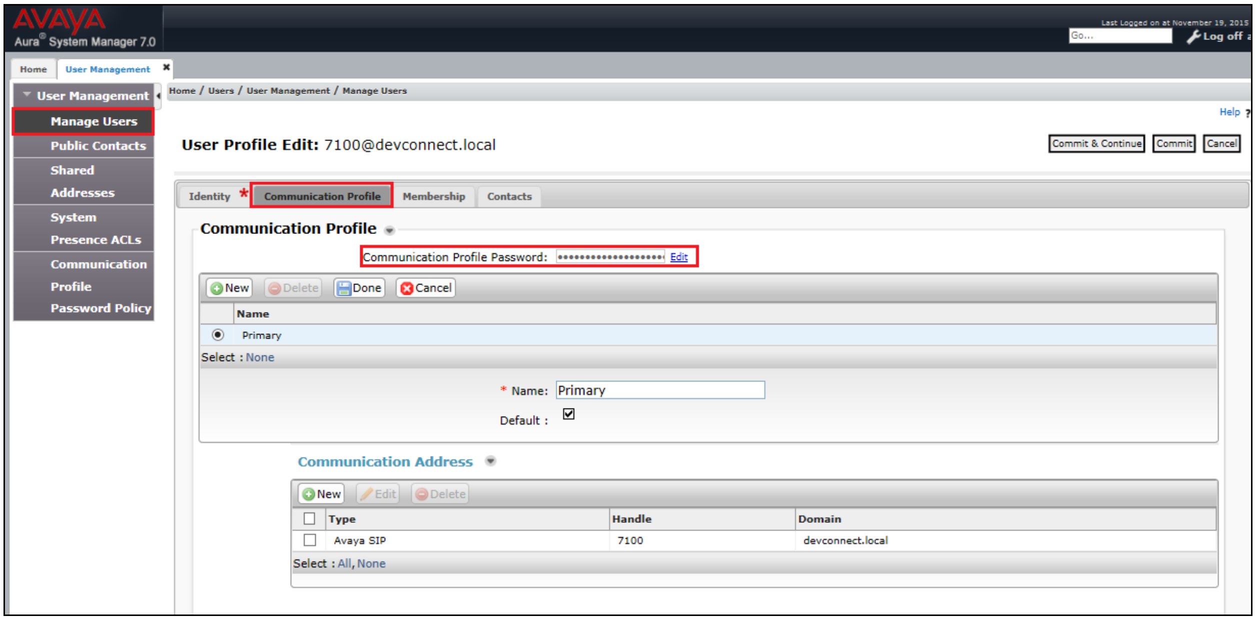


User Management

Users

	Last Name	First Name	Display Name	Login Name	SIP Handle
☑	7100	SIPExt	7100, SIPExt	7100@devconnect.local	7100
□	7101	SIPExt	7101, SIPExt	7101@devconnect.local	7101
□	7200	Ascom i62	7200, Ascom i62	7200@devconnect.local	7200
□	7201	Ascom i62	7201, Ascom i62	7201@devconnect.local	7201
□	7202	Ascom i62	7202, Ascom i62	7202@devconnect.local	7202
□	7203	Ascom i62	7203, Ascom i62	7203@devconnect.local	7203

Click on the **Communication Profile** tab. Ensure that the **Communication Profile Password** is known and if not click on edit to change it.



User Profile Edit: 7100@devconnect.local

Communication Profile

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

	Name
●	Primary

Select : None

* Name: Primary

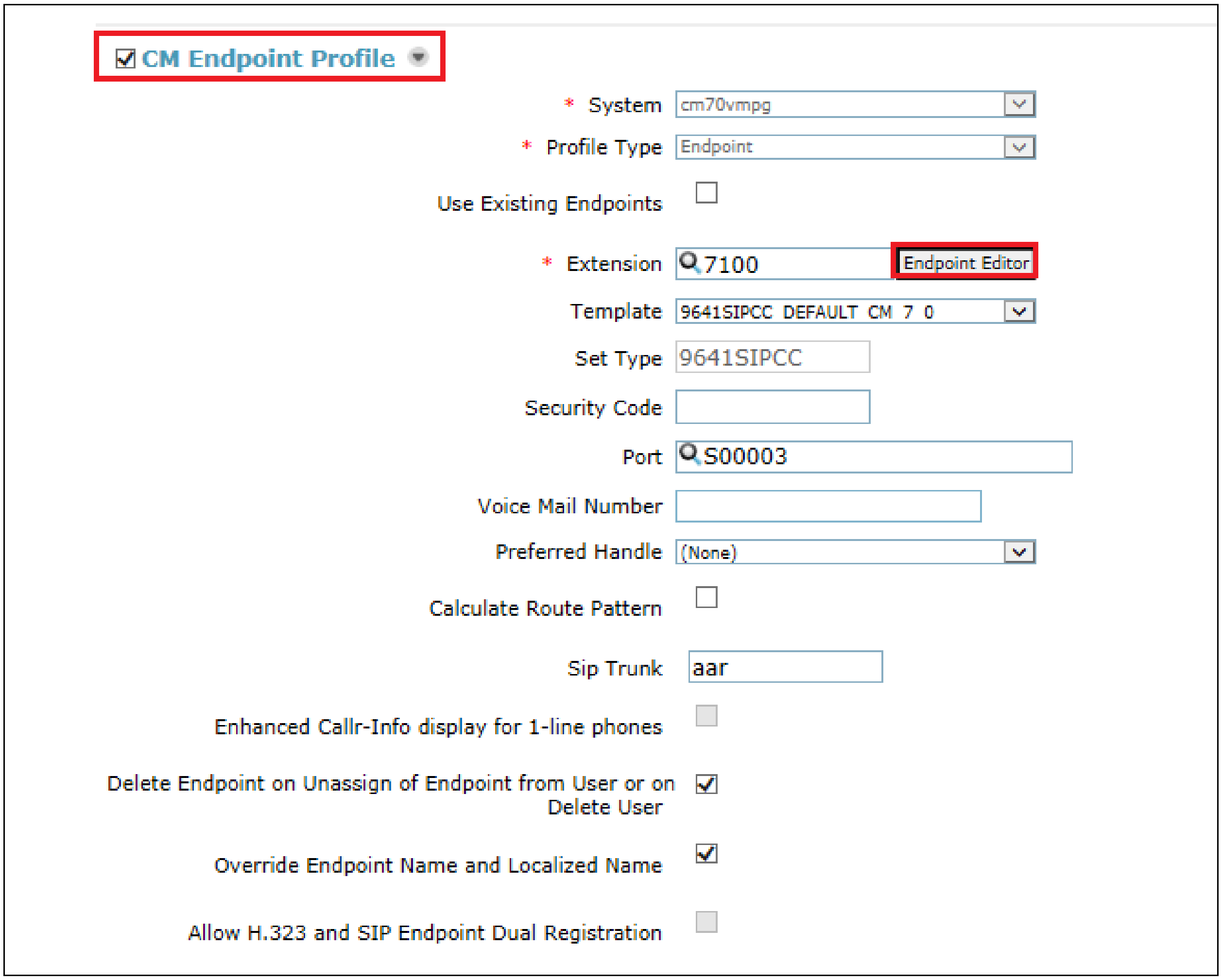
Default : ☑

Communication Address

	Type	Handle	Domain
□	Avaya SIP	7100	devconnect.local

Select : All, None

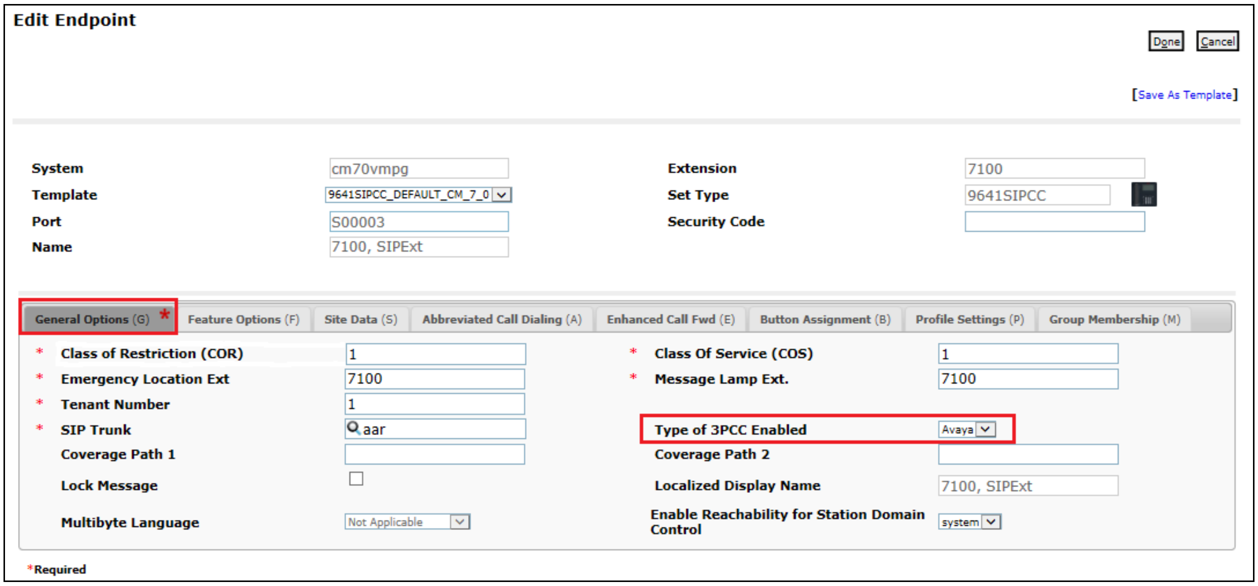
From the same page scroll down to **CM Endpoint Profile** click on **Endpoint Editor** to make further changes.



☑ CM Endpoint Profile

* System	cm70vmpg
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	7100 [Endpoint Editor]
Template	9641SIPCC_DEFAULT_CM_7_0
Set Type	9641SIPCC
Security Code	
Port	S00003
Voice Mail Number	
Preferred Handle	(None)
Calculate Route Pattern	□
Sip Trunk	aar
Enhanced Callr-Info display for 1-line phones	□
Delete Endpoint on Unassign of Endpoint 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.



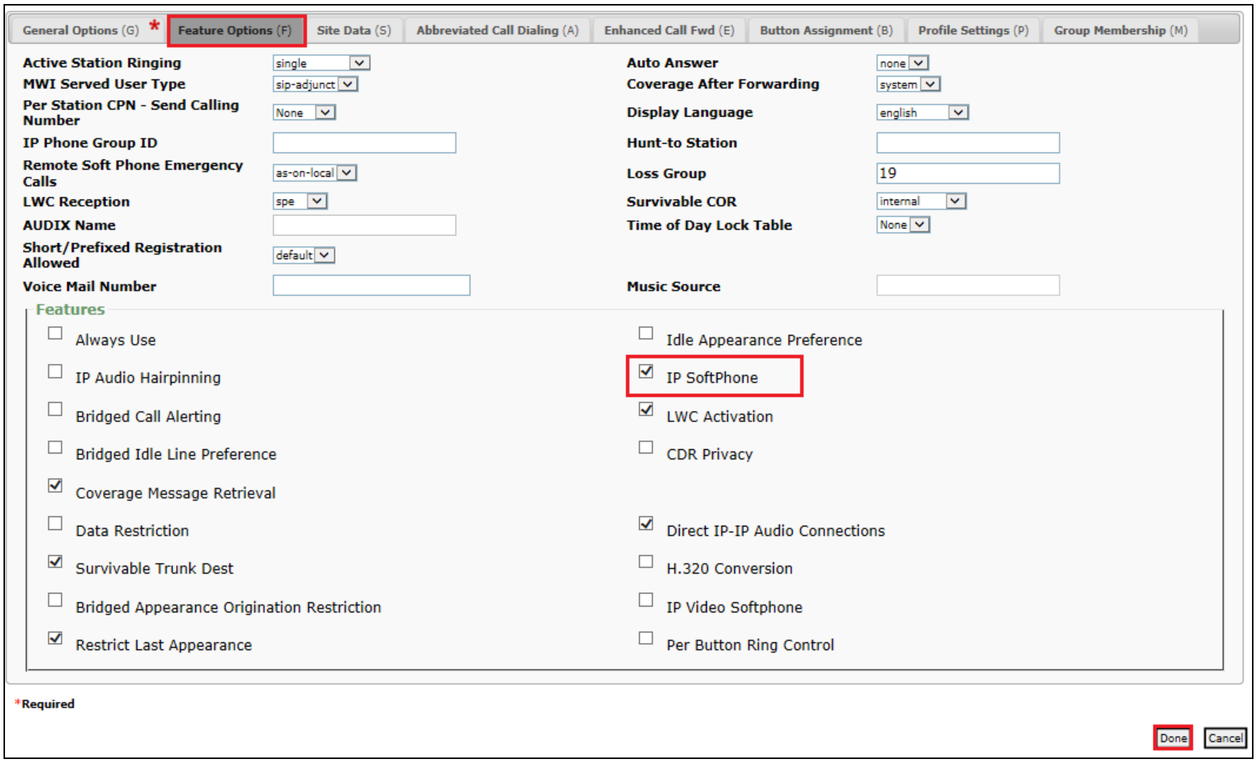
Edit Endpoint

System	cm70vmpg	Extension	7100
Template	9641SIPCC_DEFAULT_CM_7_0	Set Type	9641SIPCC
Port	S00003	Security Code	
Name	7100, SIPExt		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	7100	* Message Lamp Ext.	7100
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	7100, SIPExt
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

*Required

Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done**, at the bottom of the screen, once this is set.



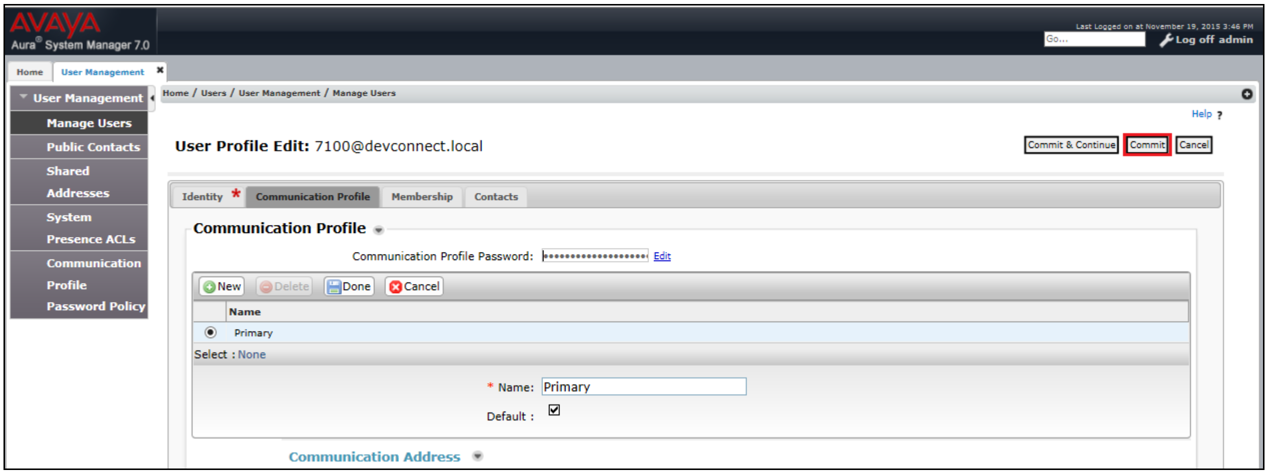
Active Station Ringing	single	Auto Answer	none
MWI Served User Type	sip-adjunct	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
IP Phone Group ID		Hunt-to Station	
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
AUDIX Name		Time of Day Lock Table	None
Short/Prefixed Registration Allowed	default		
Voice Mail Number		Music Source	

Features

□ Always Use	□ Idle Appearance Preference
□ IP Audio Hairpinning	☑ IP SoftPhone
□ Bridged Call Alerting	☑ LWC Activation
□ Bridged Idle Line Preference	□ CDR Privacy
☑ Coverage Message Retrieval	
□ Data Restriction	☑ Direct IP-IP Audio Connections
☑ Survivable Trunk Dest	□ H.320 Conversion
□ Bridged Appearance Origination Restriction	□ IP Video Softphone
☑ Restrict Last Appearance	□ Per Button Ring Control

*Required

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



User Profile Edit: 7100@devconnect.local

Communication Profile

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

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

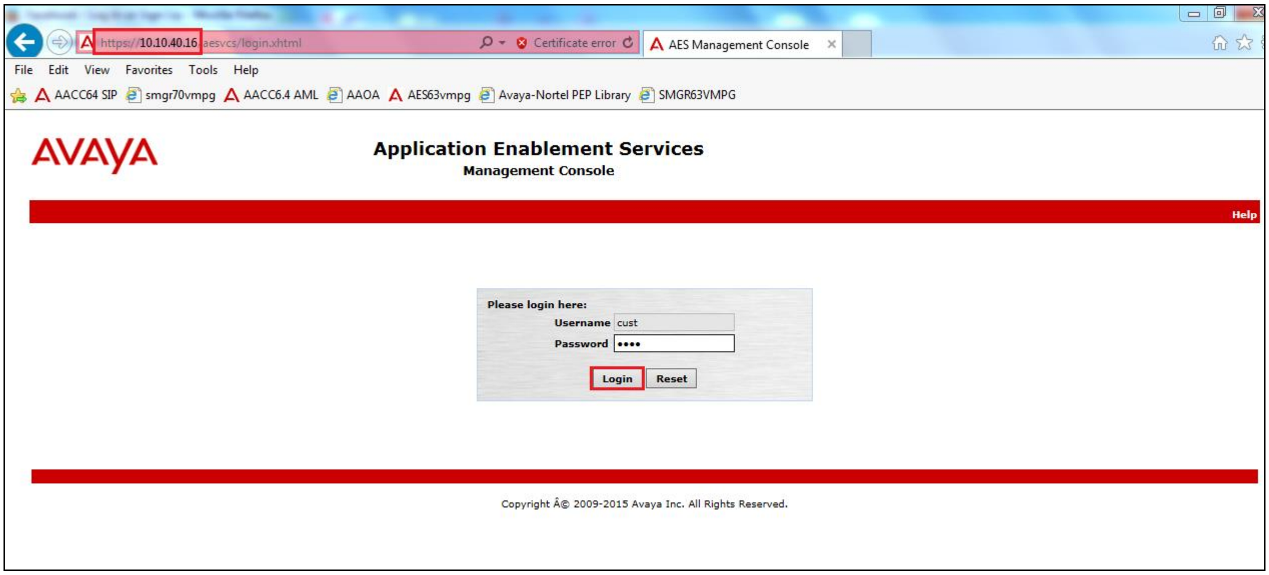
6. Configure Avaya Aura® Application Enablement Services

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 AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



https://10.10.40.16/aesvcs/login.xhtml

Application Enablement Services
Management Console

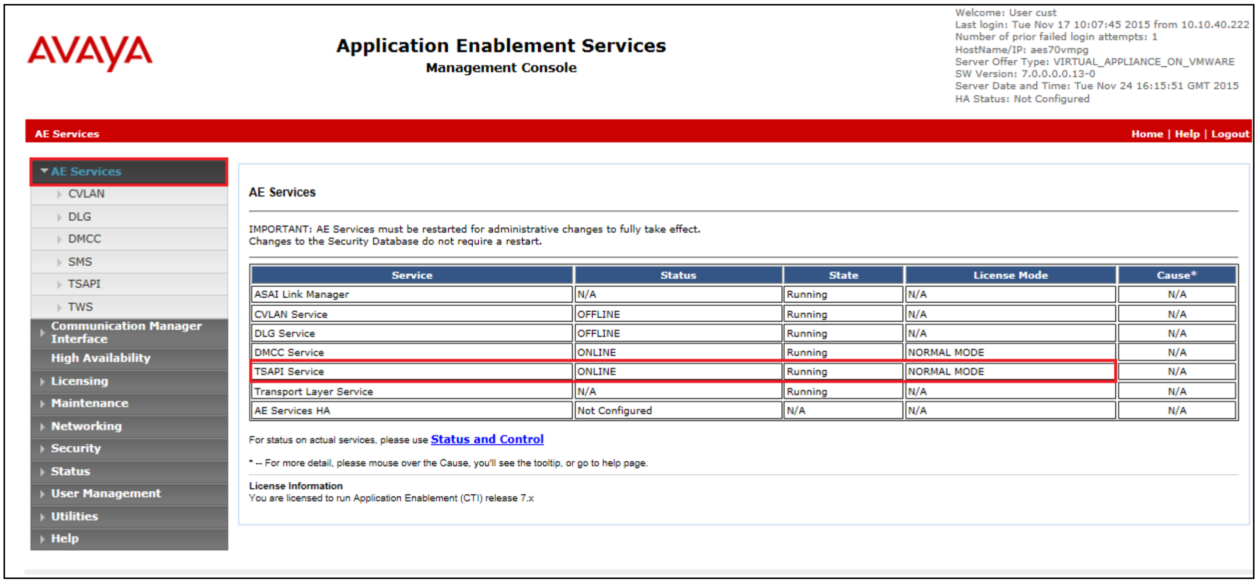
Please login here:

Username cust

Password ••••

Copyright Â© 2009-2015 Avaya Inc. All Rights Reserved.

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.



Welcome: User cust
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222
Number of prior failed login attempts: 1
HostName/IP: aes70vmpg
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-0
Server Date and Time: Tue Nov 24 16:15:51 GMT 2015
HA Status: Not Configured

AE Services

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

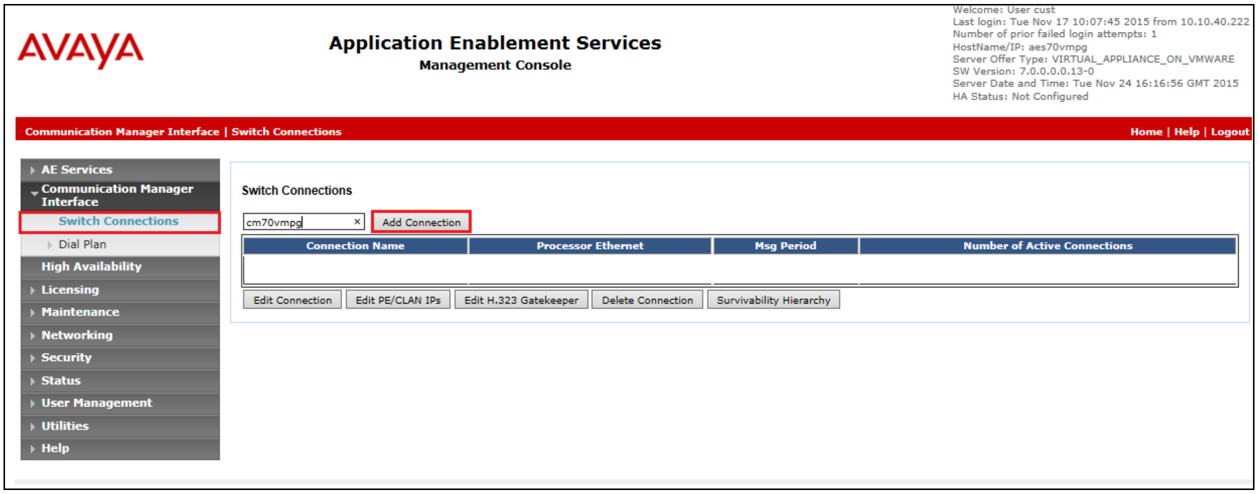
For status on actual services, please use Status and Control

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) release 7.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.



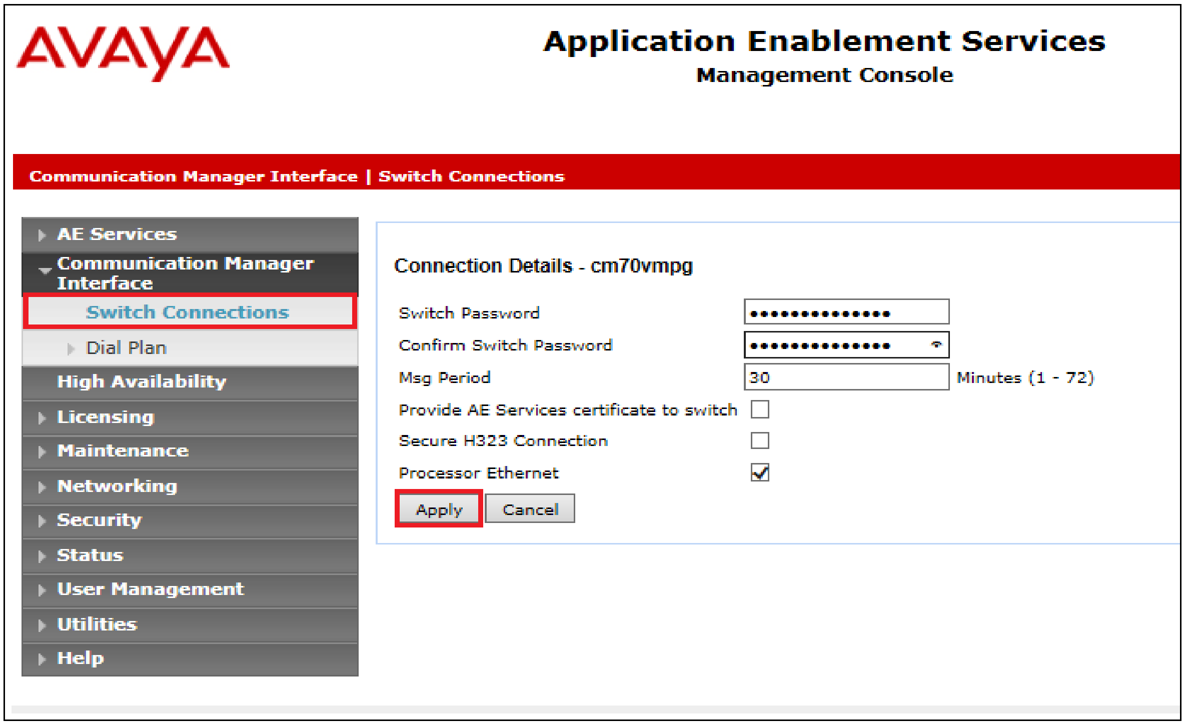
Welcome: User cust
Last login: Tue Nov 17 10:07:45 2015 from 10.10.40.222
Number of prior failed login attempts: 1
HostName/IP: aes70vmpg
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-0
Server Date and Time: Tue Nov 24 16:16:56 GMT 2015
HA Status: Not Configured

Switch Connections

cm70vmpg

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

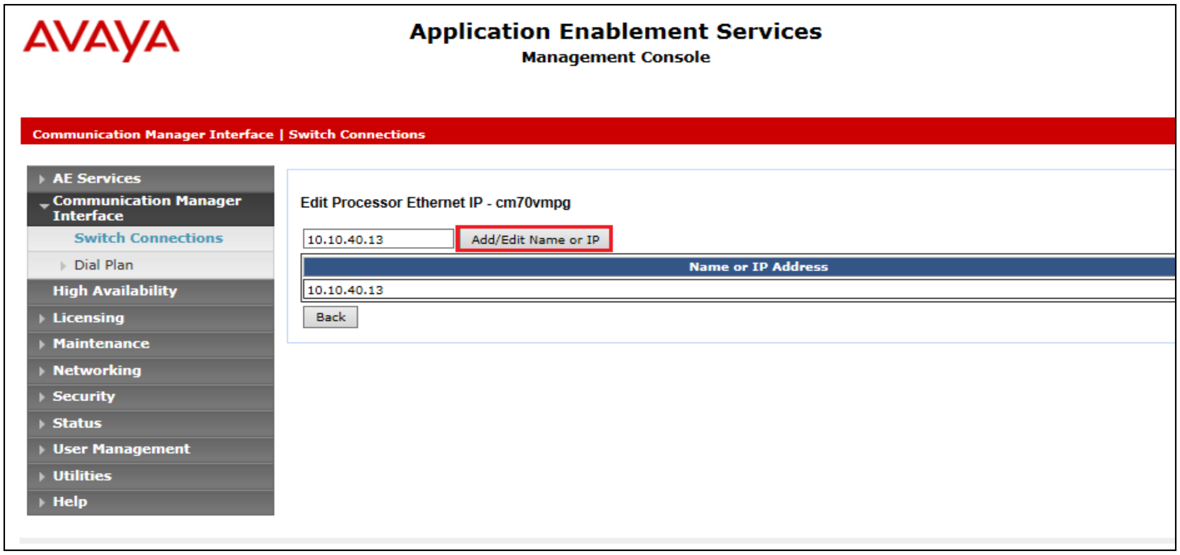
In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. The remaining fields should show as below. Click **Apply** to save changes.



Connection Details - cm70vmpg

Switch Password	••••••••••••••
Confirm Switch Password	••••••••••••••
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	□
Secure H323 Connection	□
Processor Ethernet	☑

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown, see screen at the bottom of the previous page. 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.



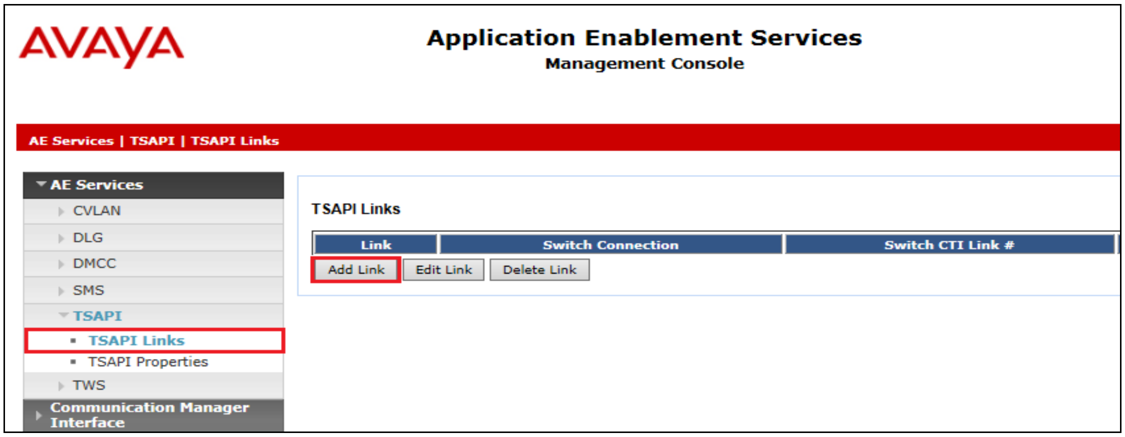
Edit Processor Ethernet IP - cm70vmpg

10.10.40.13

Name or IP Address
10.10.40.13

6.3. Administer TSAPI link

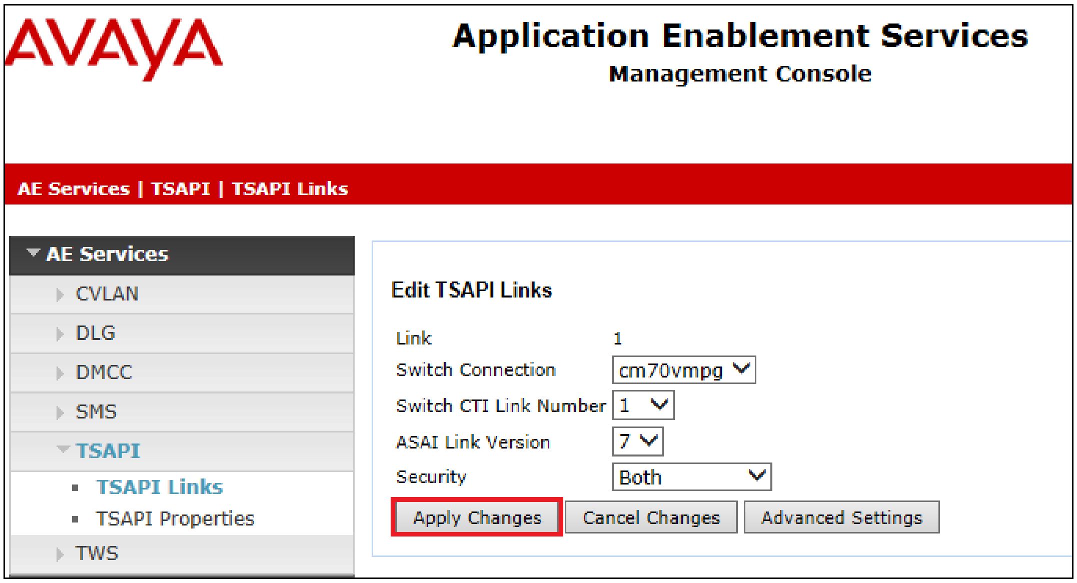
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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 **cm70vmpg**, 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 **7**.
- **Security:** This can be left at the default value of **both**.

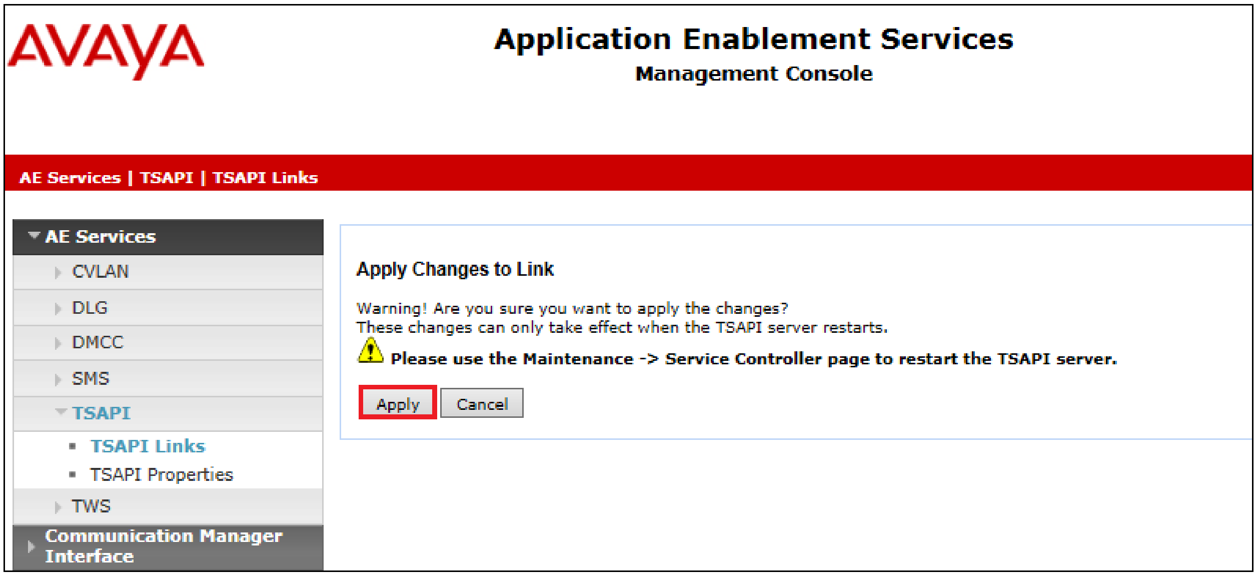
Once completed, select **Apply Changes**.



Edit TSAPI Links

Link	1
Switch Connection	cm70vmpg
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

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

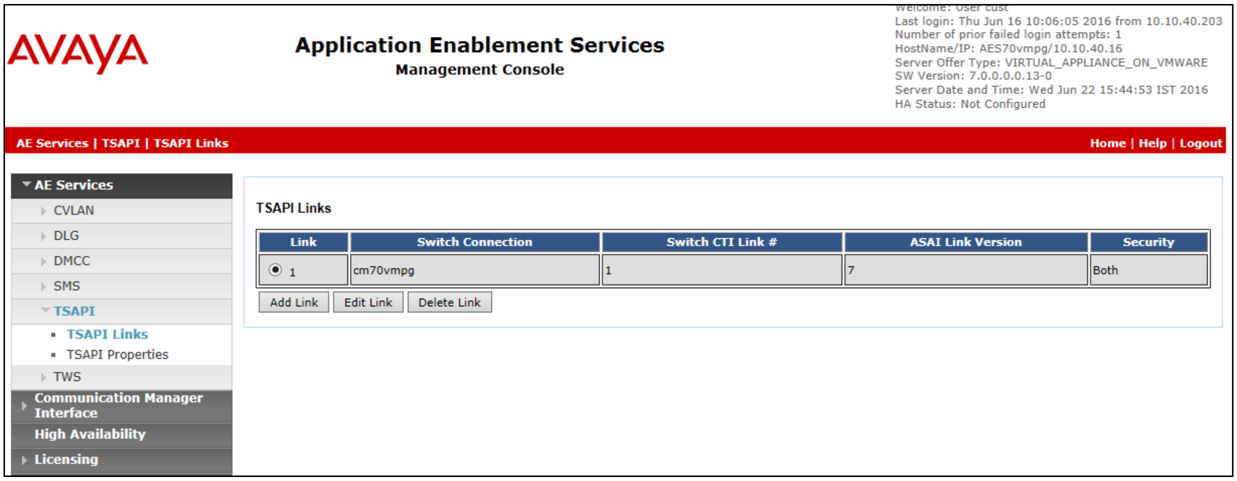

AVAYA
Application Enablement Services
Management Console
AE Services | TSAPI | TSAPI Links
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
TSAPI Properties
TWS
Communication Manager Interface
Apply
Cancel

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.

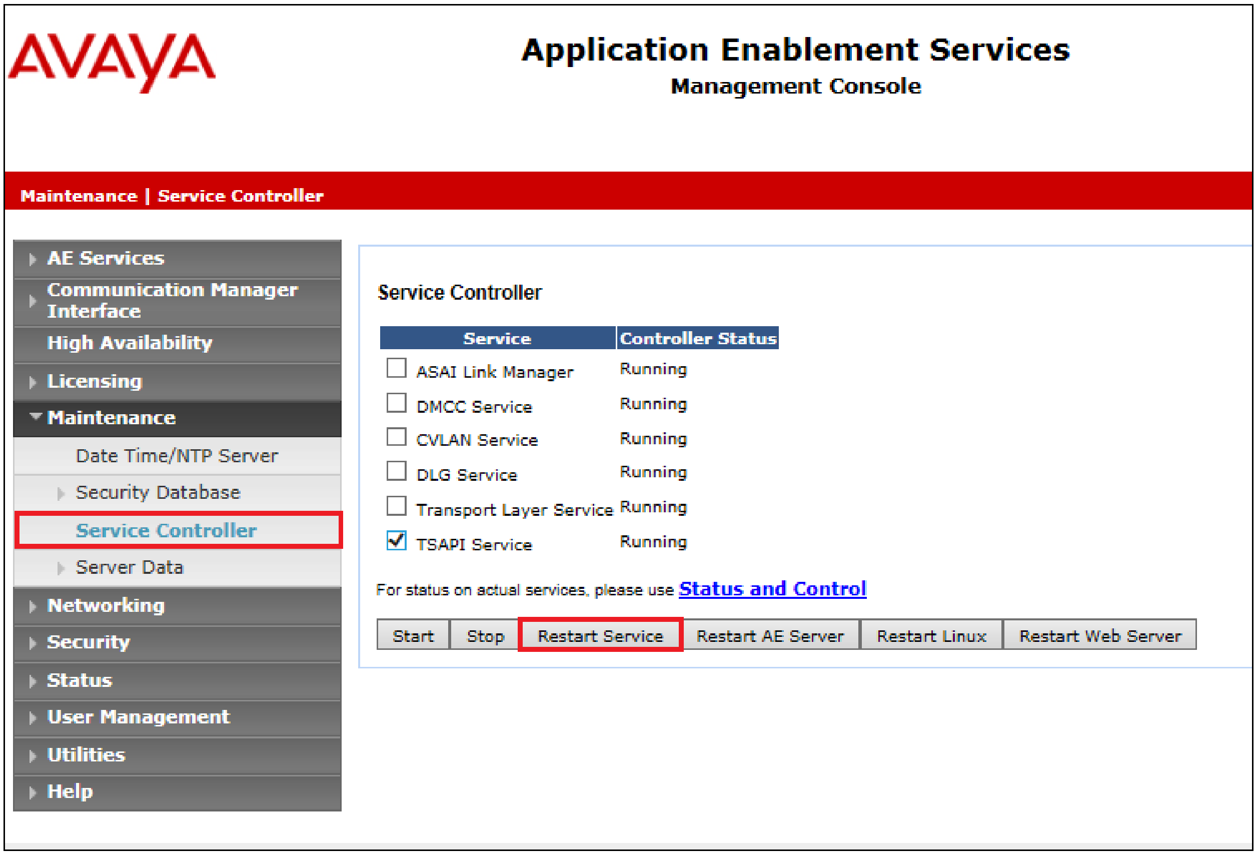


Welcome: User cust
Last login: Thu Jun 16 10:06:05 2016 from 10.10.40.203
Number of prior failed login attempts: 1
HostName/IP: AES70vmpg/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-0
Server Date and Time: Wed Jun 22 15:44:53 IST 2016
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	cm70vmpg	1	7	Both

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**.



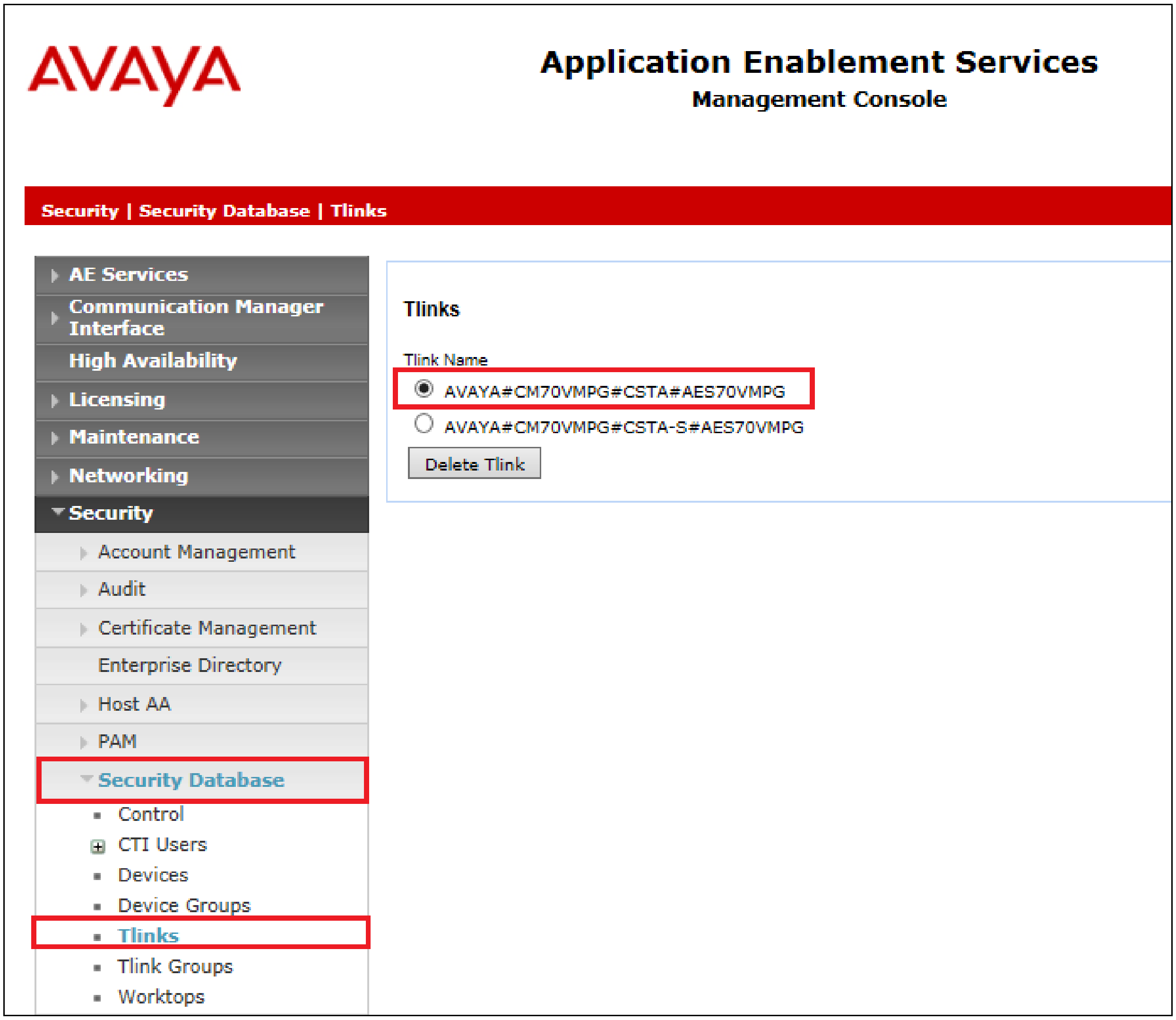
Service Controller

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

For status on actual services, please use Status and Control

6.4. 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**.



Tlinks

Tlink Name

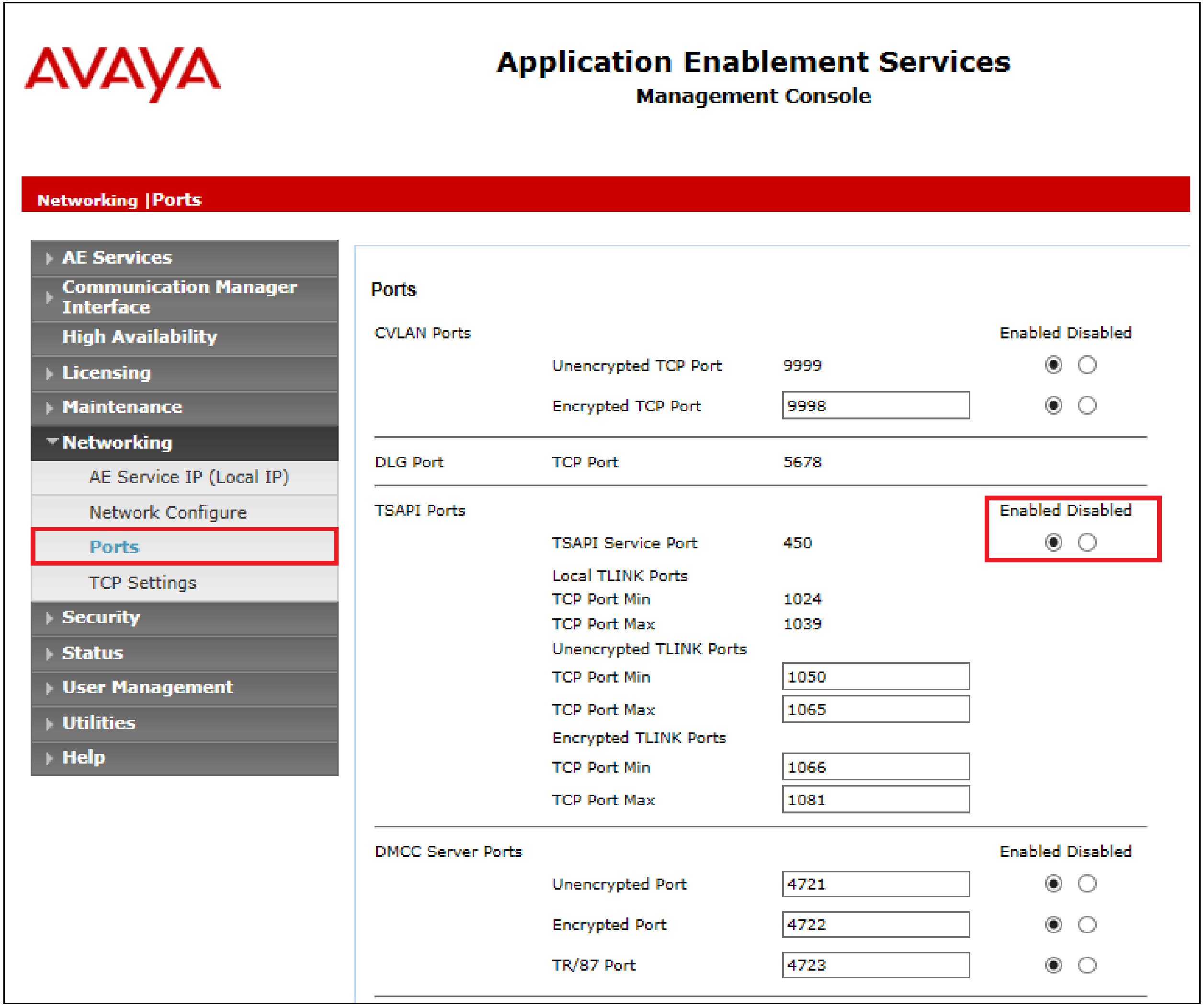
● AVAYA#CM70VMPG#CSTA#AES70VMPG

○ AVAYA#CM70VMPG#CSTA-S#AES70VMPG

Delete Tlink

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.

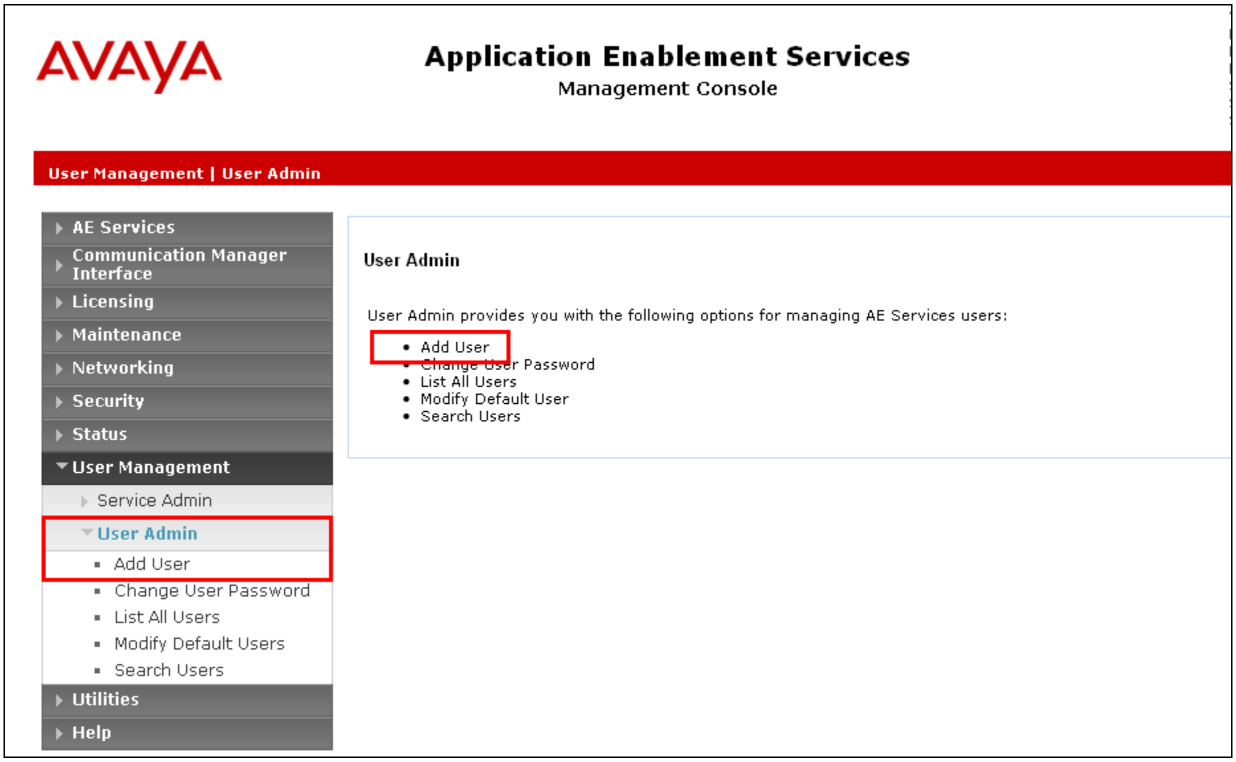


Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

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 Admin

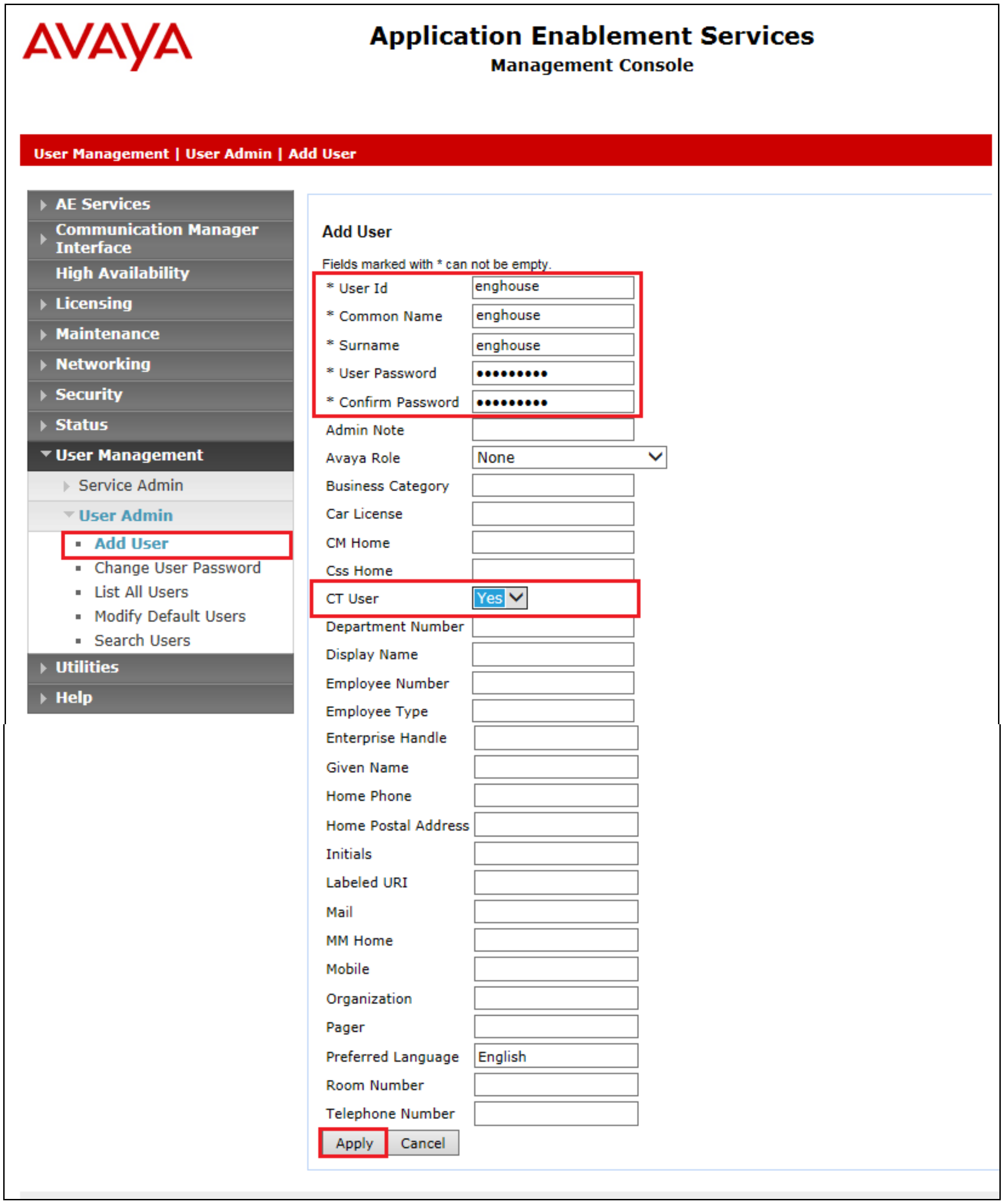
User Admin provides you with the following options for managing AE Services users:

- 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.



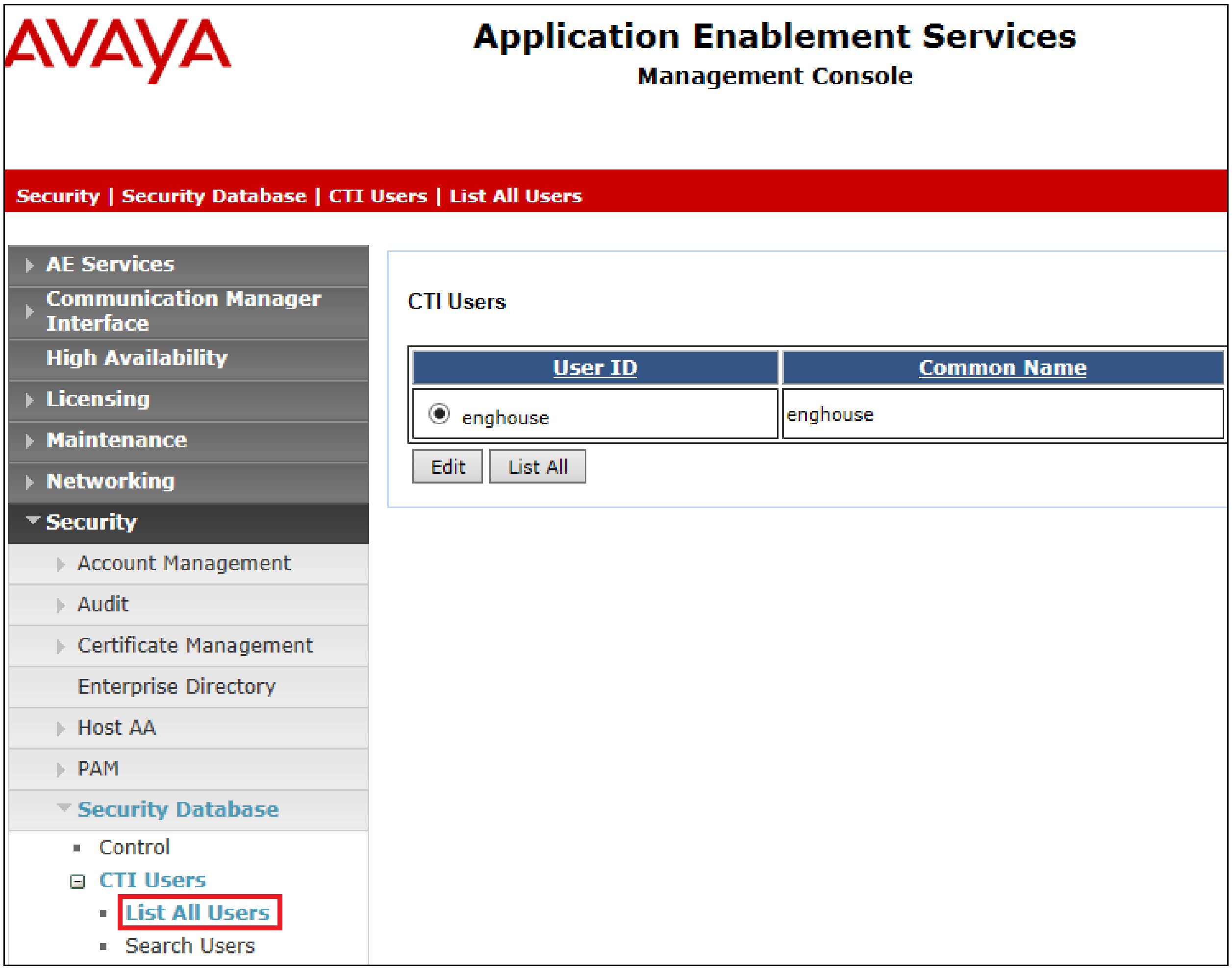
Add User

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	
Css 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	

6.7. Associate Devices with CTI User

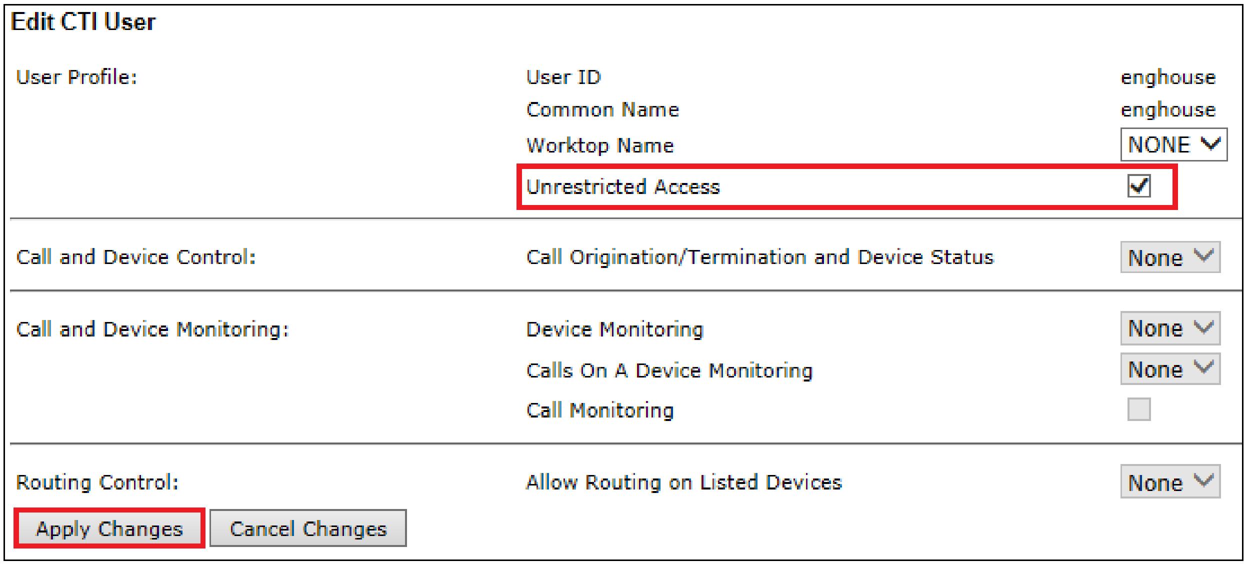
Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit**.



CTI Users

User ID	Common Name
● enghouse	enghouse

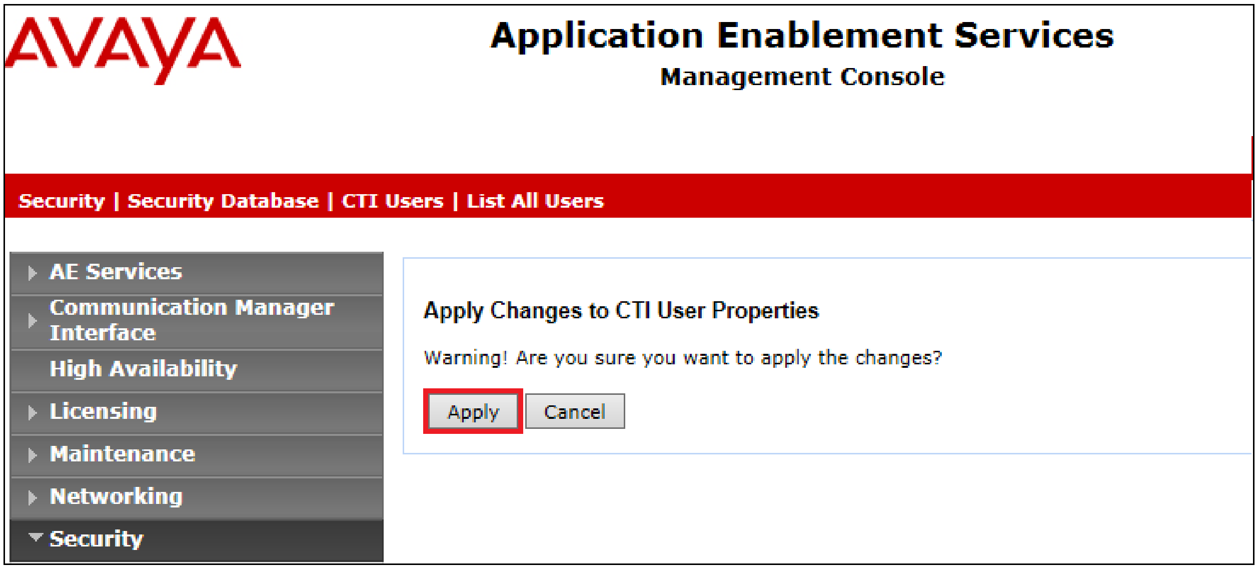
In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.



Edit CTI User

User Profile:	User ID	enghouse
	Common Name	enghouse
	Worktop Name	NONE
	Unrestricted Access	☑
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	□
Routing Control:	Allow Routing on Listed Devices	None

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



Application Enablement Services

Management Console

Security | Security Database | CTI Users | List All Users

Apply Changes to CTI User Properties

Warning! Are you sure you want to apply the changes?

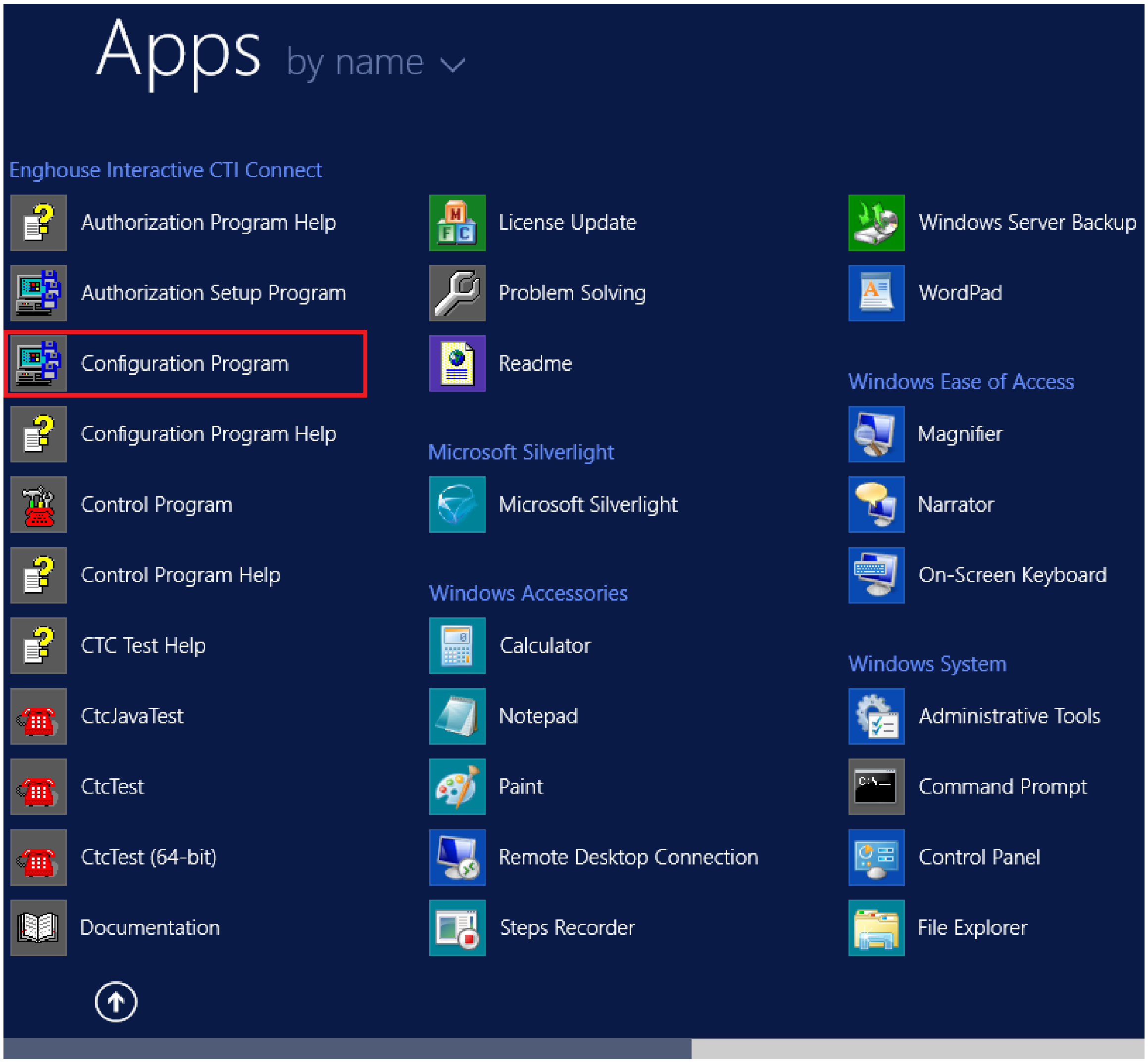
7. Configure EngHouse Interactive CTI Connect

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.

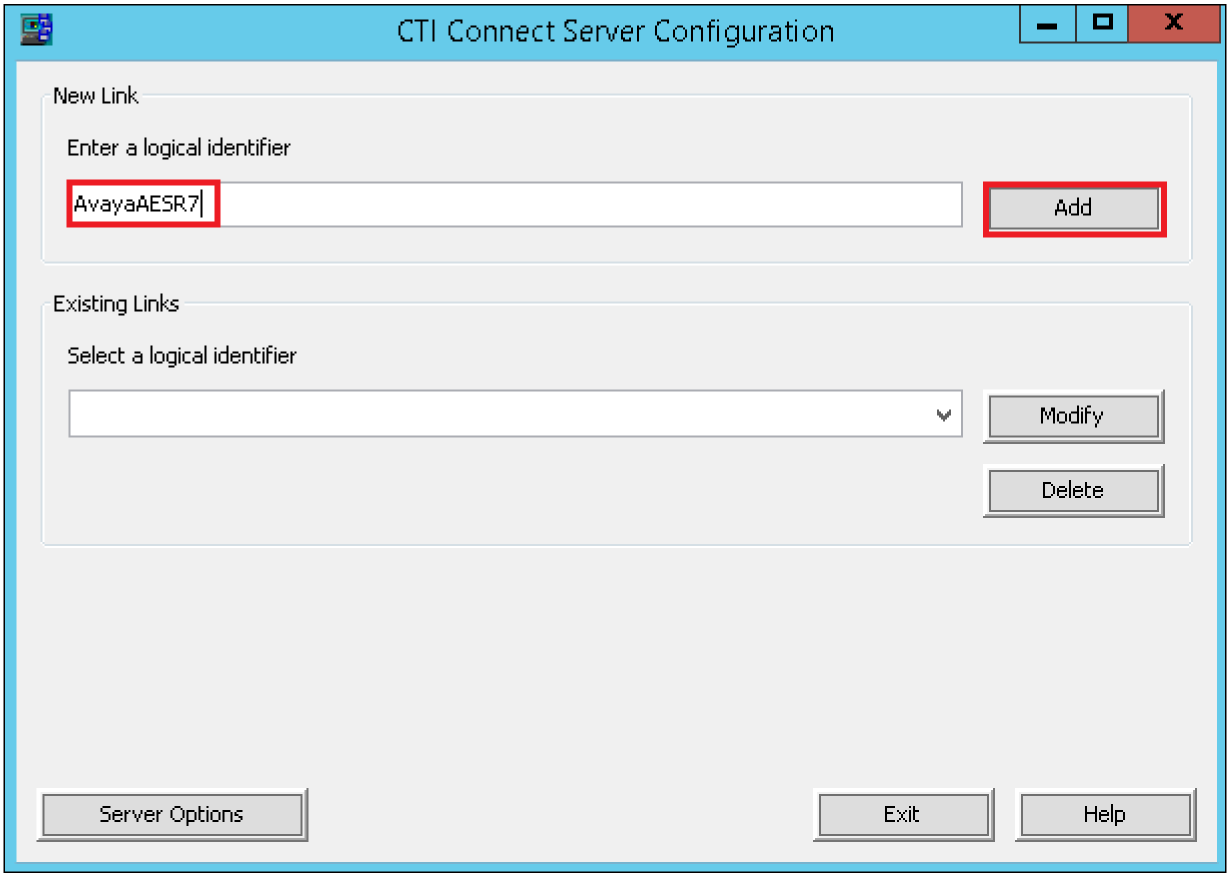
7.1. Launch configuration program

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.



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 **AvayaAESR7** and click **Add**.



CTI Connect Server Configuration

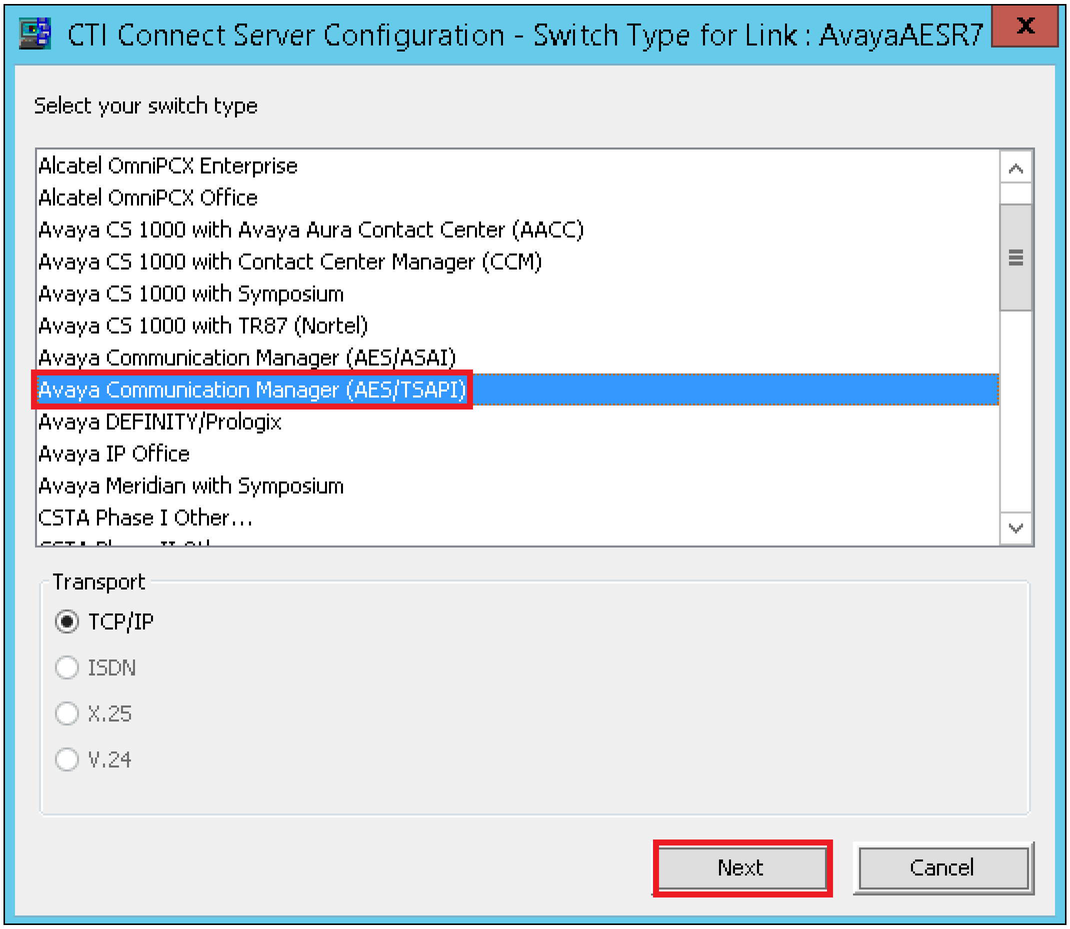
New Link

Enter a logical identifier

AvayaAESR7

7.3. Administer switch type

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



CTI Connect Server Configuration - Switch Type for Link : AvayaAESR7

Select your switch type

- Alcatel OmniPCX Enterprise
- Alcatel OmniPCX Office
- Avaya CS 1000 with Avaya Aura Contact Center (AACC)
- Avaya CS 1000 with Contact Center Manager (CCM)
- Avaya CS 1000 with Symposium
- Avaya CS 1000 with TR87 (Nortel)
- Avaya Communication Manager (AES/ASAI)
- Avaya Communication Manager (AES/TSAPI)
- Avaya DEFINITY/Prologix
- Avaya IP Office
- Avaya Meridian with Symposium
- CSTA Phase I Other...

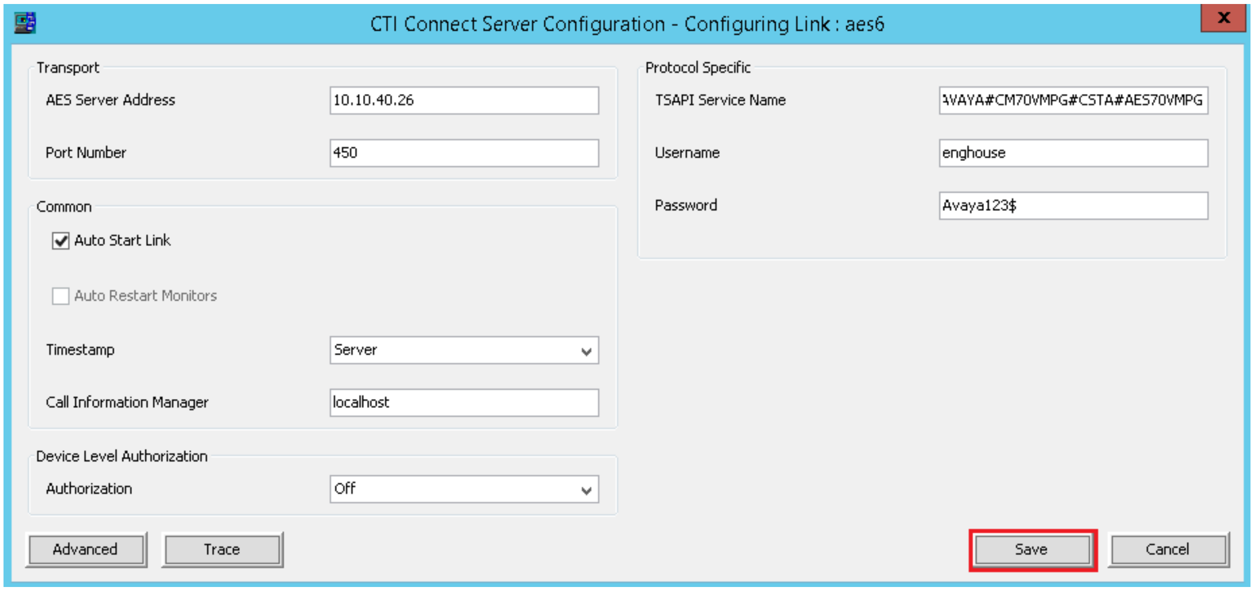
Transport

● TCP/IP
○ ISDN
○ X.25
○ V.24

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 **10.10.40.26**.
- **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 : aes6

Transport

AES Server Address: 10.10.40.26

Port Number: 450

Common

☑ Auto Start Link

□ Auto Restart Monitors

Timestamp: Server

Call Information Manager: localhost

Device Level Authorization

Authorization: Off

Protocol Specific

TSAPI Service Name: AVAYA#CM70VMPG#CSTA#AES70VMPG

Username: enghouse

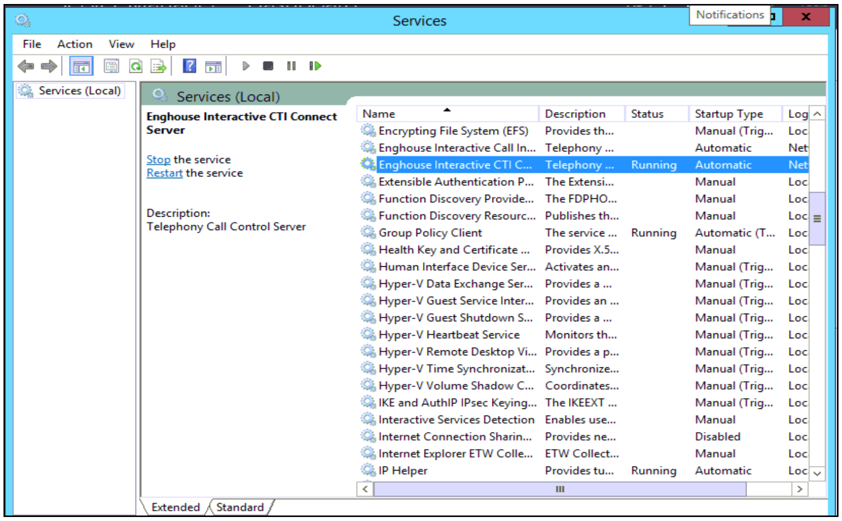
Password: Avaya123$

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)

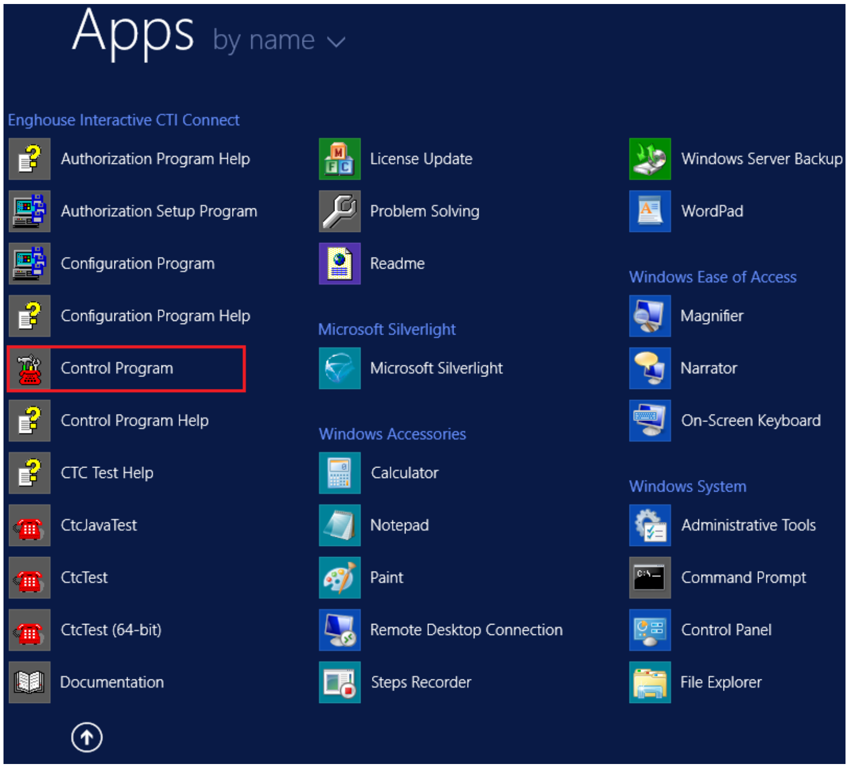
Enghouse Interactive CTI Connect Server

Stop the service
Restart the service

Description:
Telephony Call Control Server

Name	Description	Status	Startup Type	Log
Encrypting File System (EFS)	Provides th...		Manual (Trig...	Loc
Enghouse Interactive Call In...	Telephony ...		Automatic	Net
Enghouse Interactive CTI C...	Telephony ...	Running	Automatic	Net
Extensible Authentication P...	The Extensi...		Manual	Loc
Function Discovery Provide...	The FDPHO...		Manual	Loc
Function Discovery Resourc...	Publishes th...		Manual	Loc
Group Policy Client	The service ...	Running	Automatic (T...	Loc
Health Key and Certificate ...	Provides X.5...		Manual	Loc
Human Interface Device Ser...	Activates an...		Manual (Trig...	Loc
Hyper-V Data Exchange Ser...	Provides a ...		Manual (Trig...	Loc
Hyper-V Guest Service Inter...	Provides an ...		Manual (Trig...	Loc
Hyper-V Guest Shutdown S...	Provides a ...		Manual (Trig...	Loc
Hyper-V Heartbeat Service	Monitors th...		Manual (Trig...	Loc
Hyper-V Remote Desktop Vi...	Provides a p...		Manual (Trig...	Loc
Hyper-V Time Synchronizat...	Synchronize...		Manual (Trig...	Loc
Hyper-V Volume Shadow C...	Coordinates...		Manual (Trig...	Loc
IKE and AuthIP IPsec Keying...	The IKEEXT ...		Manual (Trig...	Loc
Interactive Services Detection	Enables use...		Manual	Loc
Internet Connection Sharin...	Provides ne...		Disabled	Loc
Internet Explorer ETW Colle...	ETW Collect...		Manual	Loc
IP Helper	Provides tu...	Running	Automatic	Loc

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



Apps by name

Enghouse Interactive CTI Connect
- Authorization Program Help
- Authorization Setup Program
- Configuration Program
- Configuration Program Help
- Control Program
- Control Program Help
- CTC Test Help
- CtcJavaTest
- CtcTest
- CtcTest (64-bit)
- Documentation
- License Update
- Problem Solving
- Readme

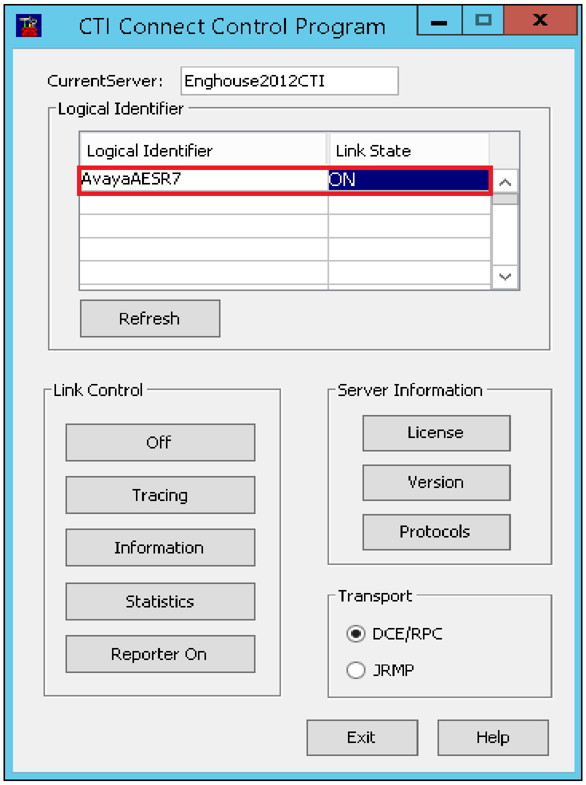
Microsoft Silverlight
- Microsoft Silverlight

Windows Accessories
- Calculator
- Notepad
- Paint
- Remote Desktop Connection
- Steps Recorder
- Windows Server Backup
- WordPad

Windows Ease of Access
- Magnifier
- Narrator
- On-Screen Keyboard

Windows System
- Administrative Tools
- Command Prompt
- Control Panel
- File Explorer

Ensure that the **Link State** associated with the administered **Logical Identifier** from **Section 7.2** in this case **AvayaAESR7** is **ON**.



CurrentServer: Enghouse2012CTI

Logical Identifier

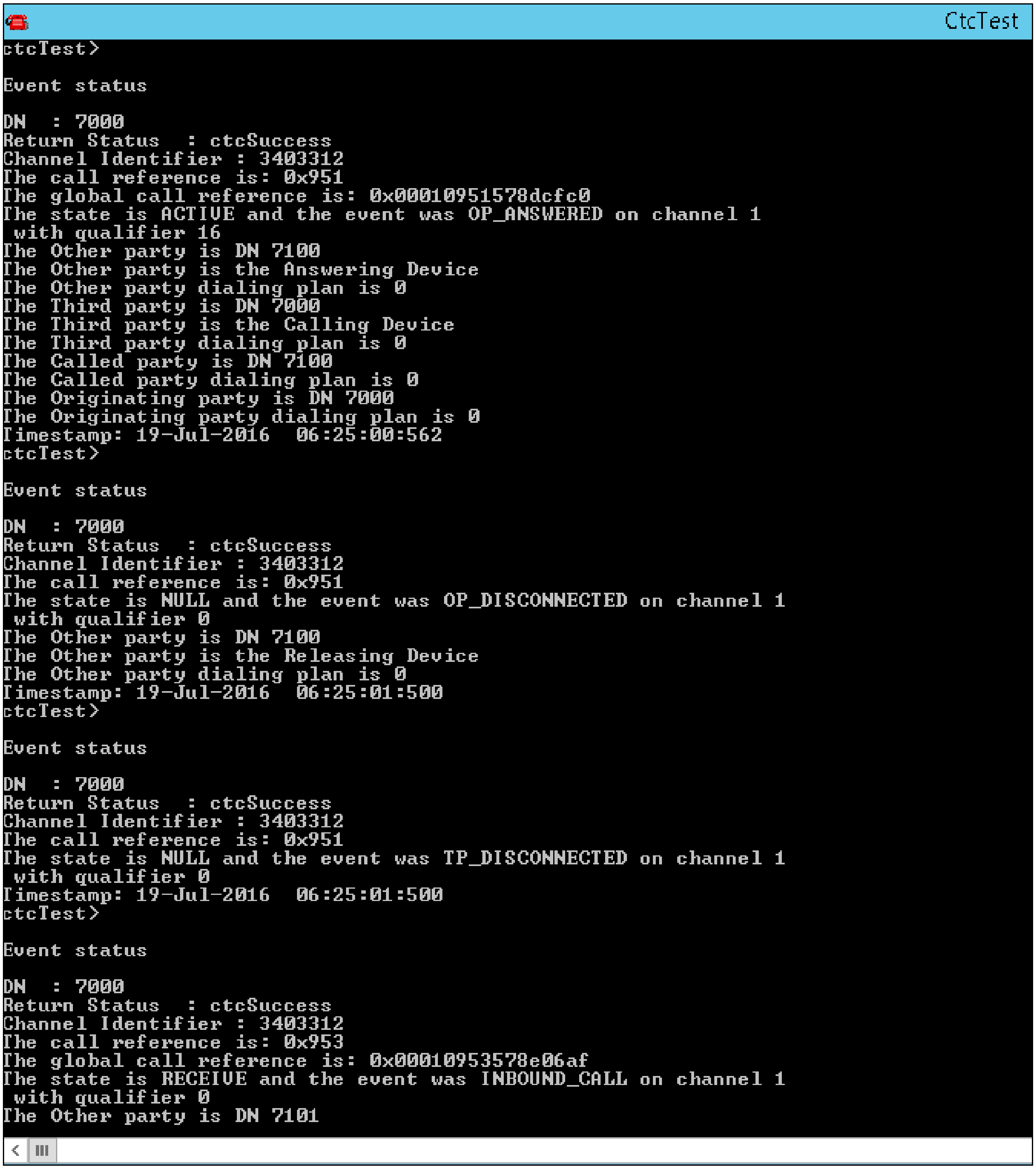
Logical Identifier	Link State
AvayaAESR7	ON

Transport

● DCE/RPC

○ JRMP

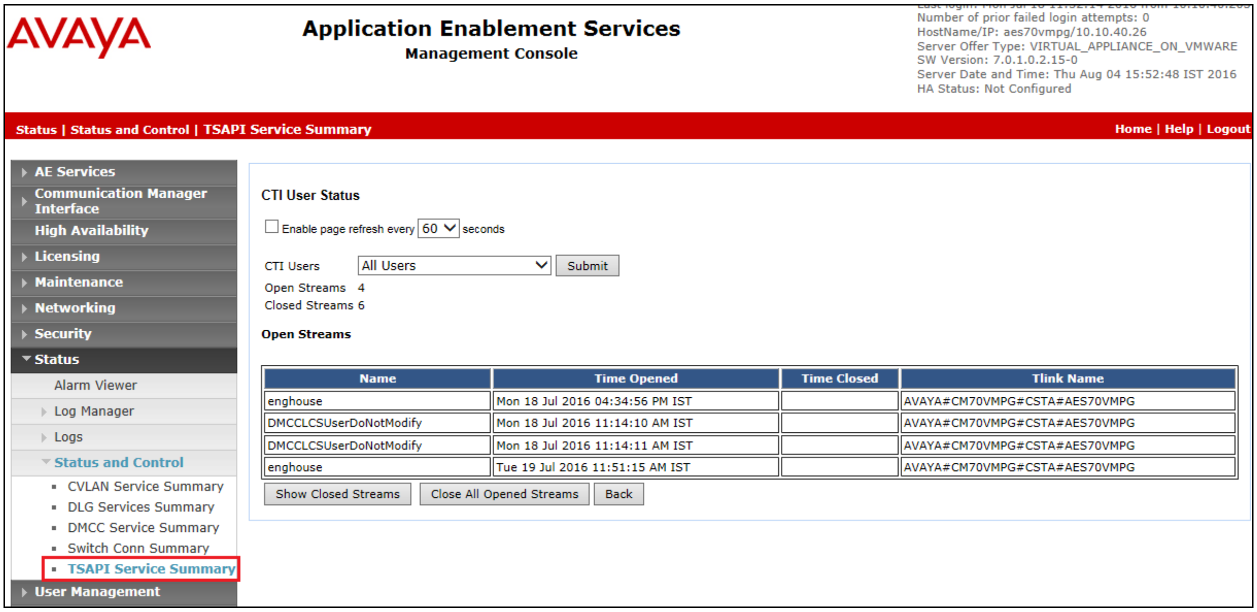
Using the CtcTool, create a monitor on the required endpoint, in this case **7000**. Place a call to the monitored endpoint from another endpoint, in this case **7100**. Use the CtcTest tool to answer the call by executing the **ans** command. Ensure that the call is answered and CtcTest can be used to complete the full variety of call control scenarios.



```
ctcTest>

Event status

DN   : 7000
Return Status   : ctcSuccess
Channel Identifier : 3403312
The call reference is: 0x951
The global call reference is: 0x00010951578dcfc0
The state is ACTIVE and the event was OP_ANSWERED on channel 1
 with qualifier 16
The Other party is DN 7100
The Other party is the Answering Device
The Other party dialing plan is 0
The Third party is DN 7000
The Third party is the Calling Device
The Third party dialing plan is 0
The Called party is DN 7100
The Called party dialing plan is 0
The Originating party is DN 7000
The Originating party dialing plan is 0
Timestamp: 19-Jul-2016  06:25:00:562
ctcTest>

Event status

DN   : 7000
Return Status   : ctcSuccess
Channel Identifier : 3403312
The call reference is: 0x951
The state is NULL and the event was OP_DISCONNECTED on channel 1
 with qualifier 0
The Other party is DN 7100
The Other party is the Releasing Device
The Other party dialing plan is 0
Timestamp: 19-Jul-2016  06:25:01:500
ctcTest>

Event status

DN   : 7000
Return Status   : ctcSuccess
Channel Identifier : 3403312
The call reference is: 0x951
The state is NULL and the event was TP_DISCONNECTED on channel 1
 with qualifier 0
Timestamp: 19-Jul-2016  06:25:01:500
ctcTest>

Event status

DN   : 7000
Return Status   : ctcSuccess
Channel Identifier : 3403312
The call reference is: 0x953
The global call reference is: 0x00010953578e06af
The state is RECEIVE and the event was INBOUND_CALL on channel 1
 with qualifier 0
The Other party is DN 7101
```

8.2. Verify TSAPI Connection Status

Using the Application Enablement Services web interface, click **Status → Status and Control → TSAPI Service Summary → User Status** and select the Enghouse CT User configured in **Section 6.5** from the **CTI Users** drop down box and click **Submit**. Verify the number of **Open Streams** listed accurately reflects the number of endpoints being monitored and controlled by CTI Connect.



Number of prior failed login attempts: 0
HostName/IP: aes70vmpg/10.10.40.26
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Thu Aug 04 15:52:48 IST 2016
HA Status: Not Configured

CTI User Status

□ Enable page refresh every 60 seconds

CTI Users: All Users [Submit]
Open Streams 4
Closed Streams 6

Open Streams

Name	Time Opened	Time Closed	Tlink Name
enghouse	Mon 18 Jul 2016 04:34:56 PM IST		AVAYA#CM70VMPG#CSTA#AES70VMPG
DMCCLCSUserDoNotModify	Mon 18 Jul 2016 11:14:10 AM IST		AVAYA#CM70VMPG#CSTA#AES70VMPG
DMCCLCSUserDoNotModify	Mon 18 Jul 2016 11:14:11 AM IST		AVAYA#CM70VMPG#CSTA#AES70VMPG
enghouse	Tue 19 Jul 2016 11:51:15 AM IST		AVAYA#CM70VMPG#CSTA#AES70VMPG

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*, Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 7.0

[4] *Avaya Aura® Session Manager Overview*, Doc # *03603323Avaya Aura ® Contact Centre SIP Commissioning*, Doc # NN44400-511, Release 7.0

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.