Avaya Solution & Interoperability Test Lab

Application Notes for Hua Pu SmartCom with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Hua Pu SmartCom to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services. Hua Pu SmartCom is a unified communication solution which integrates Communication Manager and Application Enablement Services with Tencent Real Time Exchange (RTX), an instant messaging platform launched by Tencent for enterprises.

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 Hua Pu SmartCom to interoperate with Communication Manager and Application Enablement Services. Hua Pu SmartCom is a unified communication solution which integrates Communication Manager and Application Enablement Services with Tencent Real Time Exchange (RTX), an instant messaging platform launched by Tencent for enterprises. Hua Pu SmartCom communicates with Application Enablement Services using the Telephony Services Application Programming Interface (TSAPI) to provide features such as Click-to-Call, call control and monitoring the phone statuses of other users.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying Hua Pu SmartCom for the following:

- Click-to-Call feature, such as calling the extension or mobile phone of other users using the RTX Client.
- Answering and diverting of incoming calls and making outgoing calls.
- Holding, resuming and hanging up calls.
- Blind and consult transfer of calls.
- Call conference.
- Verifying the phone statuses (idle or busy) of other users.

The serviceability testing focused on verifying the ability of Hua Pu SmartCom to recover from adverse conditions, such as disconnecting the Ethernet cables on the Hua Pu SmartCom server and Application Enablement Services server, and rebooting Communication Manager and Hua Pu SmartCom Server.

1.2. Support

Technical support on Hua Pu SmartCom can be obtained through the following:

- Phone: 4007-06-0023 (within China)
- Email: hotline_tech@huapu.com

2. Reference Configuration

Figure 1 illustrates a test configuration consisting of Communication Manager running on Avaya S8300 Server, an Avaya G350 Media Gateway, an Application Enablement Services server and Avaya 9630 IP Telephones. Hua Pu SmartCom and Tencent RTX are installed on a Microsoft Windows 2003 Server. Hua Pu SmartCom communicates with the TSAPI Service on the Application Enablement Services server using TSAPI. The desktop PCs are running the RTX Client with the Hua Pu SmartCom Plug-in installed. The Avaya C364T-PWR Converged Stackable Switch provides Ethernet connectivity to the servers and IP telephones.

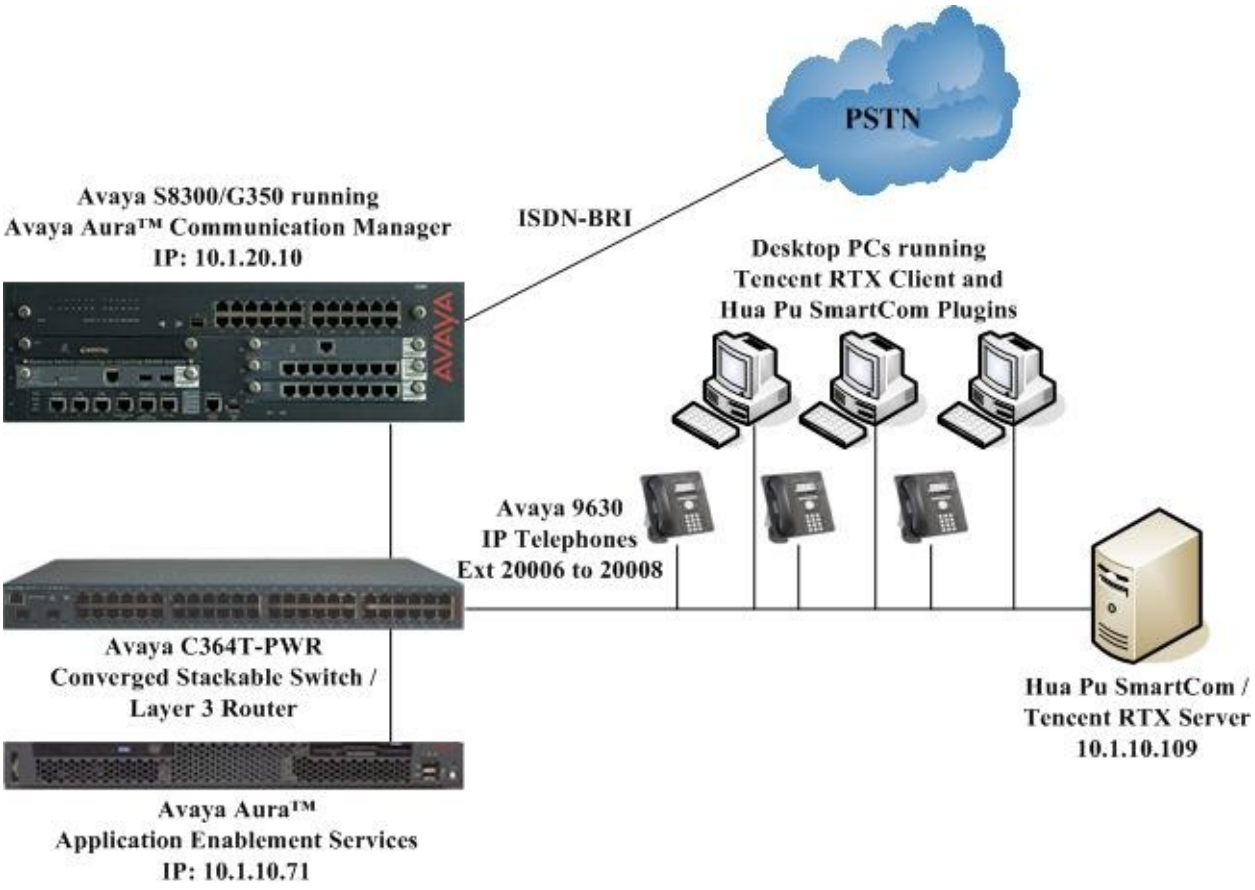


Figure 1: Test Configuration

3. Equipment and Software Validated

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

Equipment/Software	Version
Avaya S8300 Server	Communication Manager 5.2 Service Pack 2.01 (02.0.947.3-17534)
Avaya G350 Media Gateway • MM722AP BRI Media Module	29.24.2 HW01, FW008
Application Enablement Services	4.2.1 (r4-2-1-20-5-0) Patch 3
Avaya C364T-PWR Converged Stackable Switch	4.5.18
Avaya 9630 IP Telephones	3.0 (H.323)
Hua Pu SmartCom	2.0
Hua Pu SmartCom RTX Plug-in (AvayaPlugin)	2.8.2.6
Tencent Real Time Exchange (RTX)	2008

Table 1: Equipment/Software Validated

4. Configure Communication Manager

This section provides the procedures for configuring Computer Telephony Integration (CTI) links on Communication Manager. All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test. Enter the **save translation** command to save the changes to the system after completing this section.

4.1. Configure AES and CTI Links

Application Enablement Services server forwards CTI requests, responses, and events between Hua Pu SmartCom and Communication Manager. Application Enablement Services server communicates with Communication Manager over an AES link. Within the AES link, CTI links are configured to provide CTI services to CTI applications such as Hua Pu SmartCom. The following steps demonstrate the configuration of the Communication Manager side of the AES and CTI links. See **Section 5** for the details of configuring the Application Enablement Services side of the AES and CTI links.

Step	Description
1.	Enter the **display system-parameters customer-options** command. On Page 3, verify that **Computer Telephony Adjunct Links** is set to **y**. If not, contact an authorized Avaya account representative to obtain the license.

Step	Description
	display system-parameters customer-options Page 3 of 11 OPTIONAL FEATURES Abbreviated Dialing Enhanced List? y Audible Message Waiting? n Access Security Gateway (ASG)? n Authorization Codes? y Analog Trunk Incoming Call ID? n CAS Branch? n A/D Grp/Sys List Dialing Start at 01? n CAS Main? n Answer Supervision by Call Classifier? n Change COR by FAC? n ARS? y Computer Telephony Adjunct Links? **y** ARS/AAR Partitioning? y Cvg Of Calls Redirected Off-net? n ARS/AAR Dialing without FAC? y DCS (Basic)? n ASAI Link Core Capabilities? n DCS Call Coverage? n ASAI Link Plus Capabilities? n DCS with Rerouting? n Async. Transfer Mode (ATM) PNC? n Async. Transfer Mode (ATM) Trunking? n Digital Loss Plan Modification? n ATM WAN Spare Processor? n DS1 MSP? n ATMS? n DS1 Echo Cancellation? n Attendant Vectoring? n
2.	Enter the **add cti-link n** command, where **n** is a number between 1 and 64, inclusive. Enter a valid **Extension** under the provisioned dial plan in Communication Manager, set the **Type** field to **ADJ-IP**, and assign a descriptive **Name** to the CTI link.
	add cti-link 1 Page 1 of 3 CTI LINK CTI Link: 1 Extension: **29901** Type: **ADJ-IP** COR: 1 Name: **TSAPI Services**
3.	Enter the **change node-names ip** command. In the compliance-tested configuration, the processor interface with the node-name **procr** was utilized for connectivity to Application Enablement Services server.
	change node-names ip Page 1 of 2 IP NODE NAMES Name IP Address default 0.0.0.0 msgserver 10.1.20.12 **procr 10.1.20.10**
4.	Enter the **change ip-services** command. On Page 1, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. The **Local Node** field should be set to the processor interface **procr** as shown in **Step 3**. During the compliance test, the default port was utilized for the **Local Port** field.
	change ip-services Page 1 of 4 IP SERVICES Service Type Enabled Local Node Local Port Remote Node Remote Port **AESVCS y procr 8765**

Step	Description
	On Page 4, enter the hostname of the Application Enablement Services server for the **AE Services Server** field. The hostname may be obtained by logging in to the Application Enablement Services server using Secure Shell (SSH), and running the **uname -a** command. Enter an alphanumeric password for the **Password** field and set the **Enabled** field to **y**. The same password will be configured on the Application Enablement Services server in **Section 5.3 Step 2**.

```
change ip-services                                          Page   4 of   4
                          AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:        aes1              xxxxxxxxxxxxxxxx      y
```

4.2. Configure Auto Route Select (ARS) Access Code

The ARS Access Code is configured to allow calls to be routed to external parties through the trunk groups configured in Communication Manager. This is usually configured when the Communication Manager is provisioned. The following describes the steps to determine the ARS Access Code configured.

Step	Description
1.	Enter the **display feature-access-codes** command. On Page 1, note down the feature access code assigned for **Auto Route Selection (ARS) - Access Code 1**, which will be used to configure Hua Pu SmartCom in **Section 6.2 Step 1**.

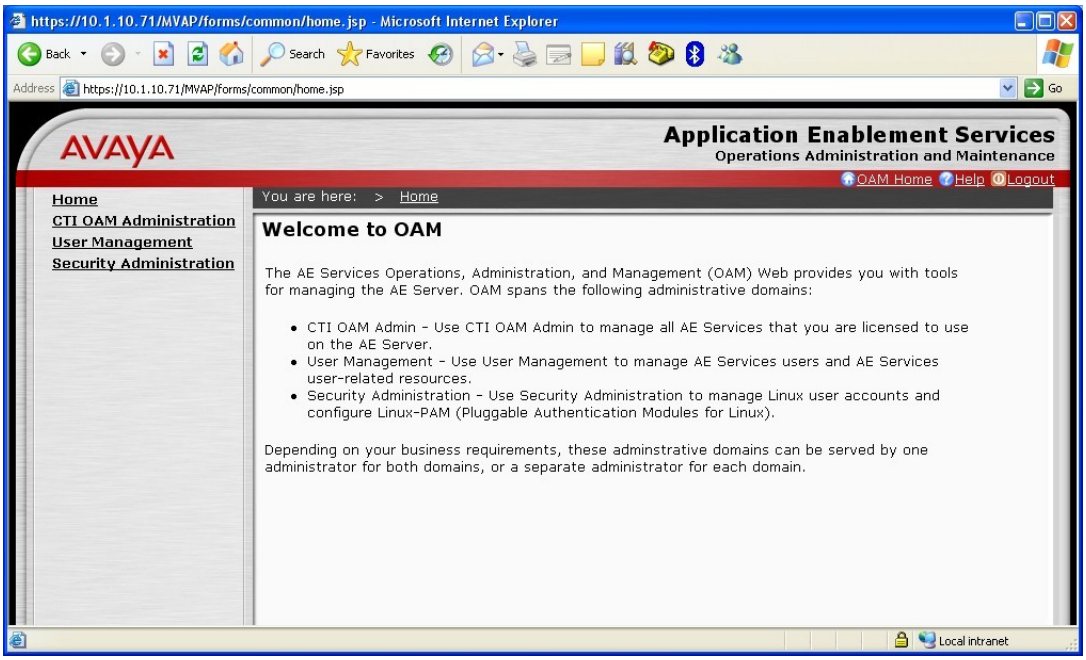
```
display feature-access-codes                                Page   1 of   8
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *00
         Abbreviated Dialing List2 Access Code: *01
         Abbreviated Dialing List3 Access Code: *02
Abbreviated Dial - Prgm Group List Access Code: *03
                      Announcement Access Code: *04
                       Answer Back Access Code: *05

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *06    Deactivation: #06
Call Forwarding Activation Busy/DA: *07    All: *08    Deactivation: #08
   Call Forwarding Enhanced Status: *09    Act: *10    Deactivation: #10
                         Call Park Access Code: *11
                       Call Pickup Access Code: *12
CAS Remote Hold/Answer Hold-Unhold Access Code: *13
                  CDR Account Code Access Code: *14
                       Change COR Access Code:
                  Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code: *17      Close Code: #17
```

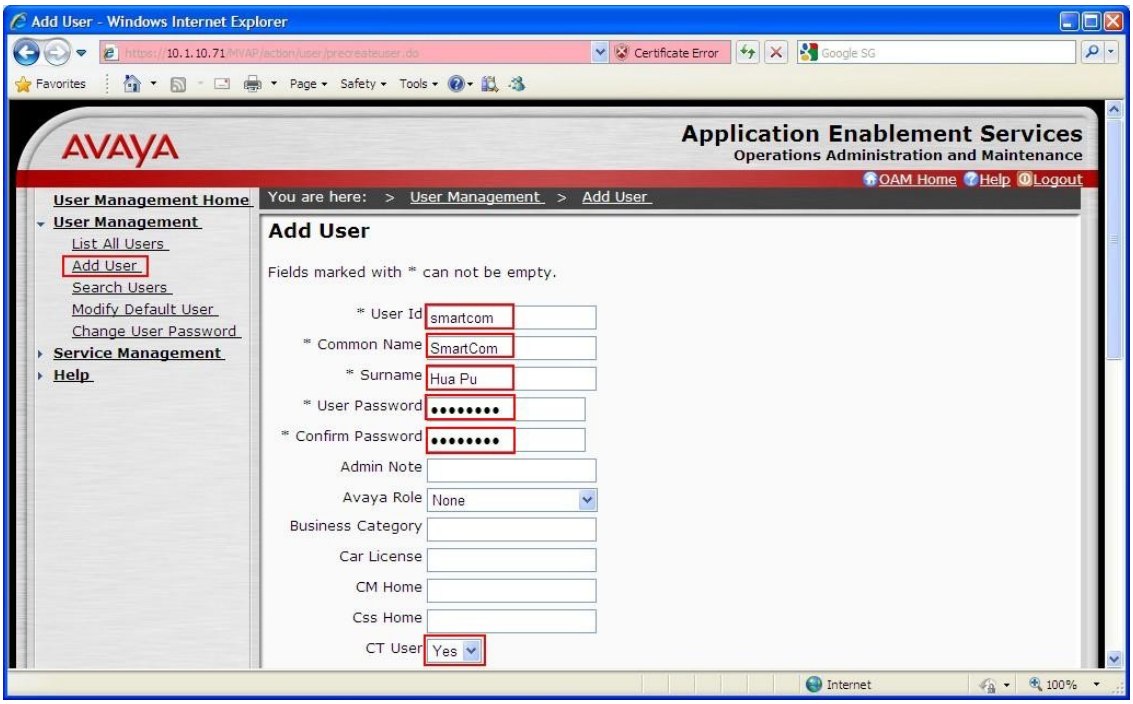
5. Configure Avaya Application Enablement Services

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

- Administer CTI User
- Verify Application Enablement Services License
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user permission

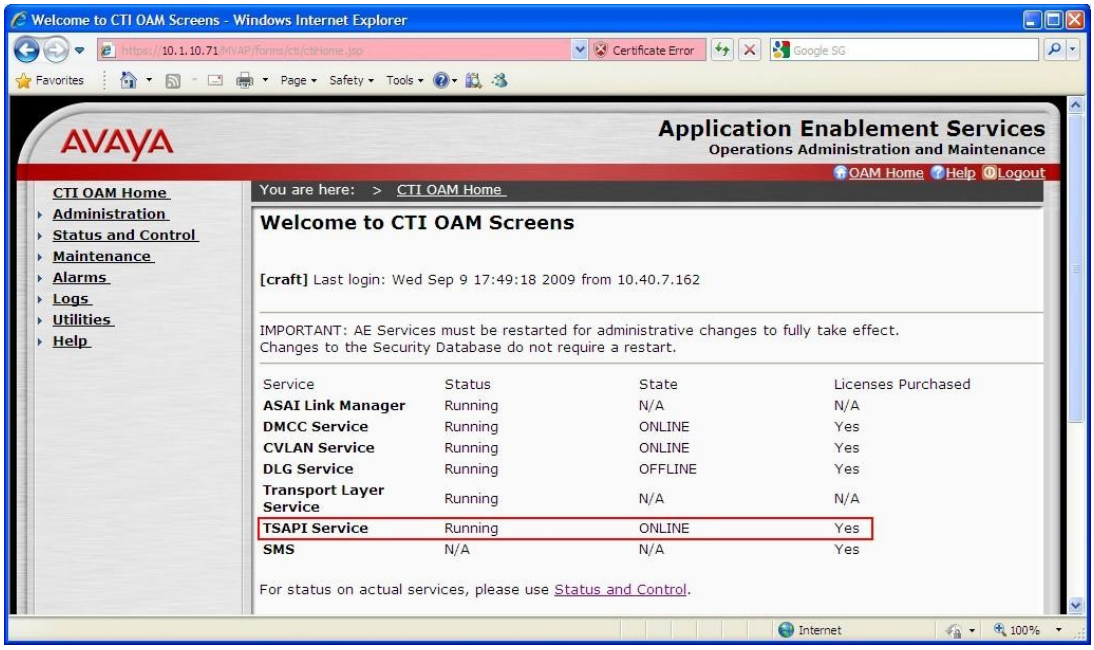
5.1. Administer CTI User

Step	Description
1.	Launch a web browser and enter **https://<IP address of Application Enablement Services server>/MVAP/** to access the OAM web based interface. Log in using an administrative login and password (not shown), and the Welcome To OAM screen will be displayed. 

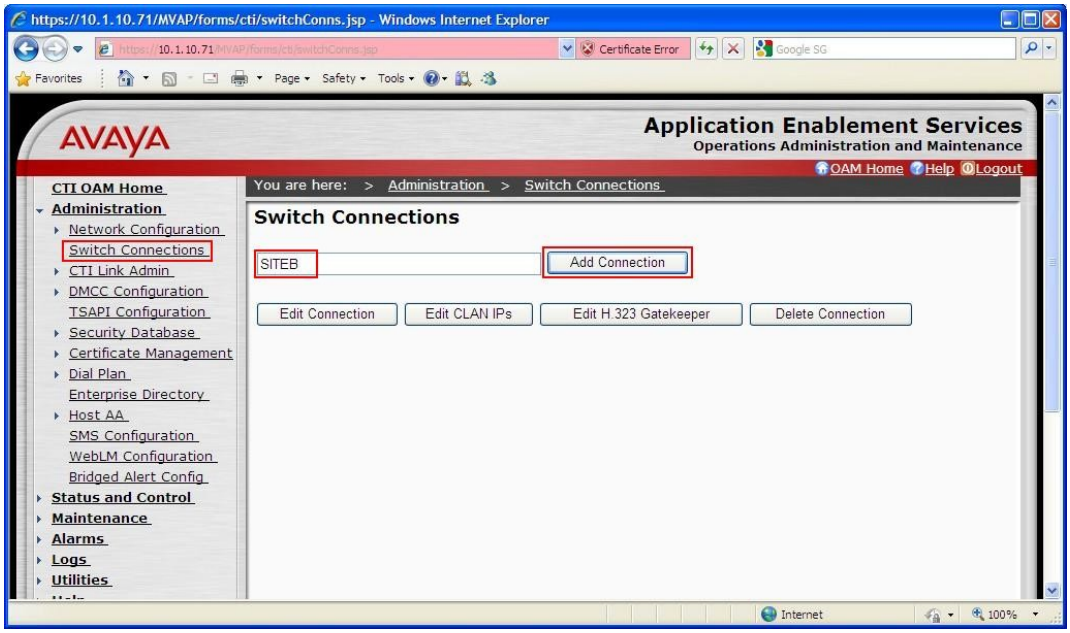
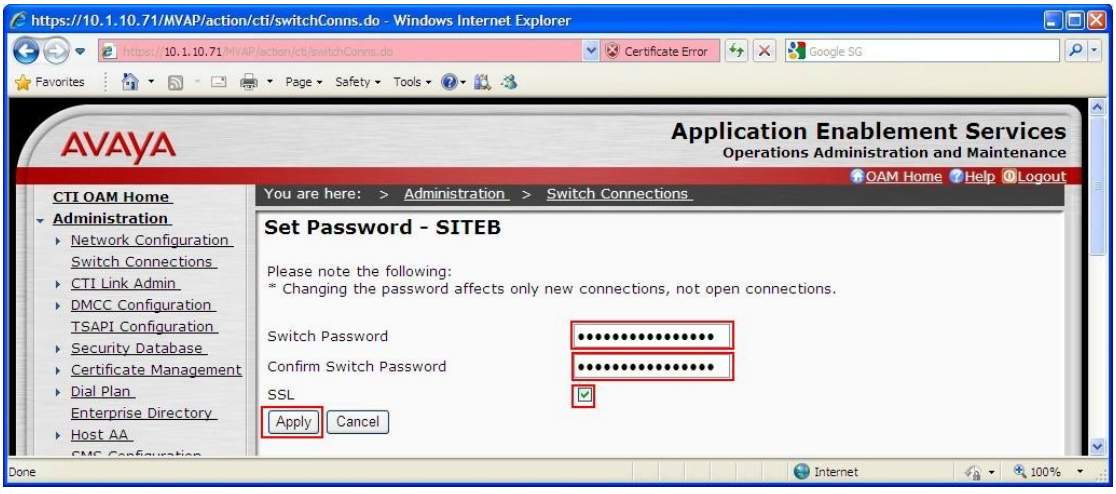
Step	Description
2.	Click **User Management**, then **User Management > Add User** in the left pane. Specify a value for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set **CT User** to **Yes**. Use the values for **User Id** and **User Password** to configure Hua Pu SmartCom in **Section 6.2** to access the TSAPI Service on the Application Enablement Services server. Scroll down to the bottom of the page and click **Apply** (not shown). 

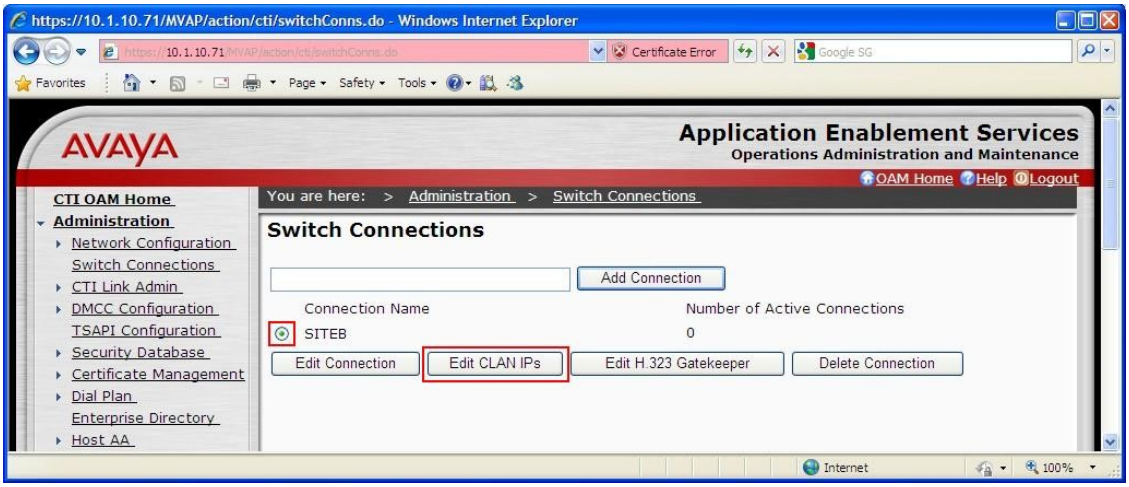
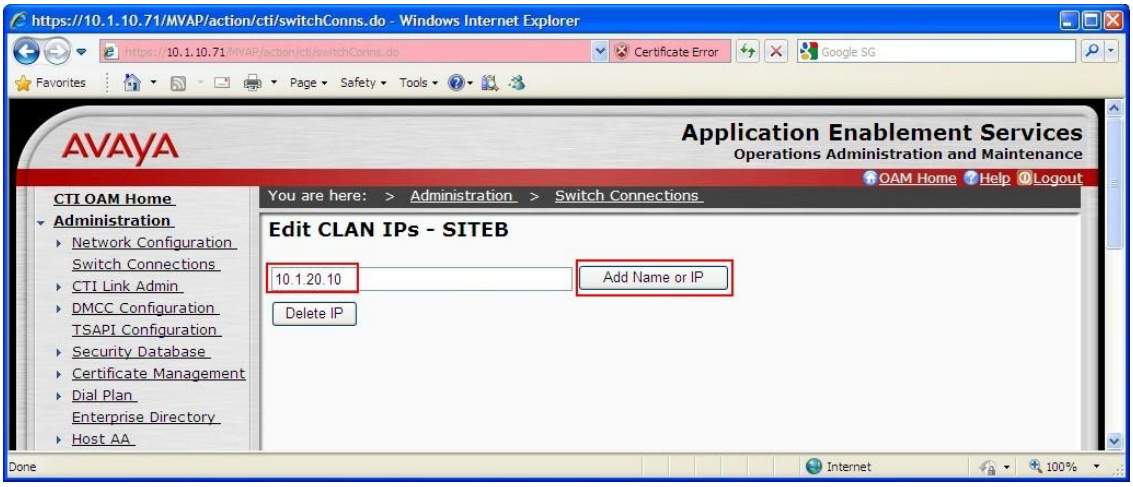
5.2. Verify Application Enablement Services License

Step	Description
1.	Select **OAM Home**, then click on **CTI OAM Administration** from the left menu (not shown). From the Welcome to CTI OAM Screens page, verify that the Application Enablement Services license has proper permissions for the features illustrated in these Application Notes by ensuring the TSAPI Service is licensed. If the TSAPI Service is not licensed, then contact the Avaya sales team or business partner for a proper license file.

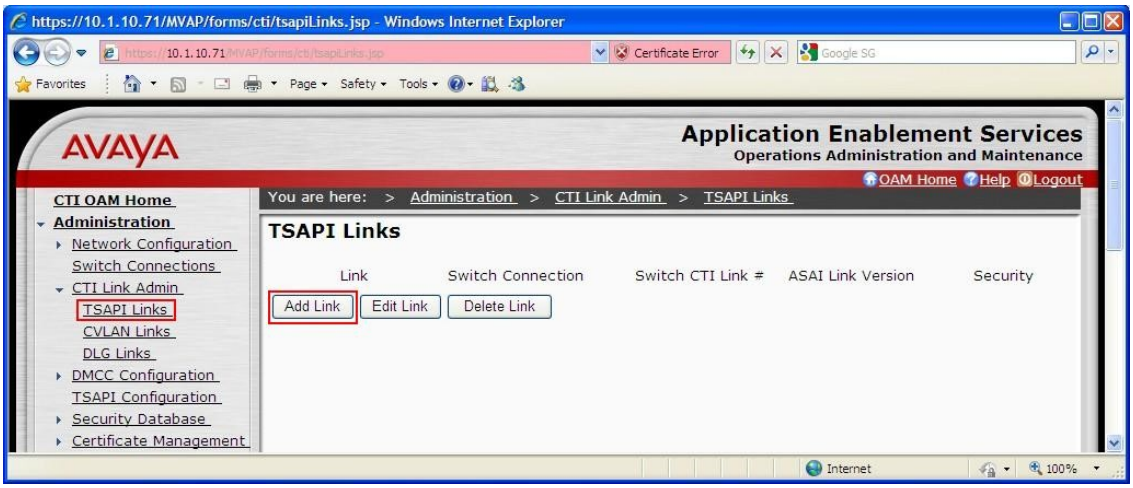
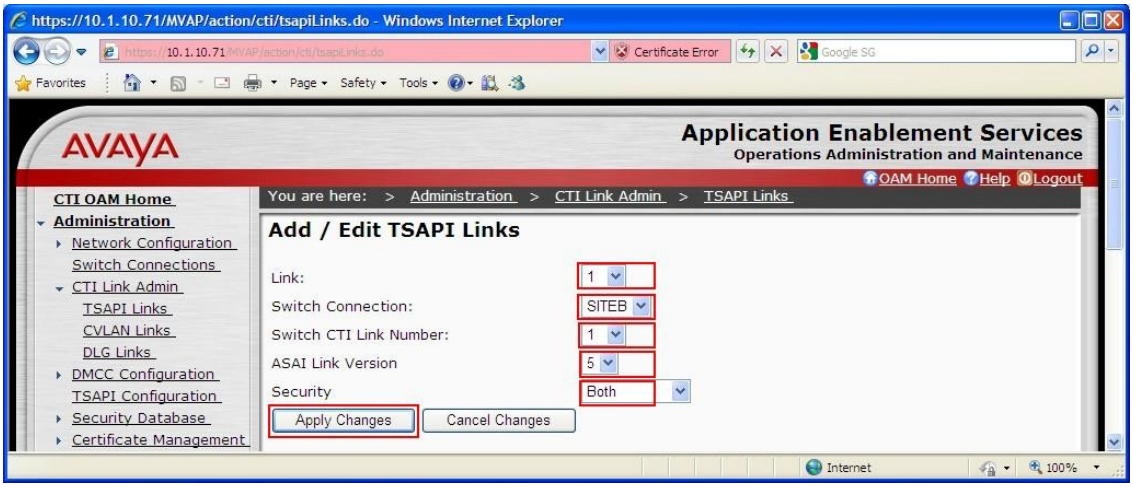


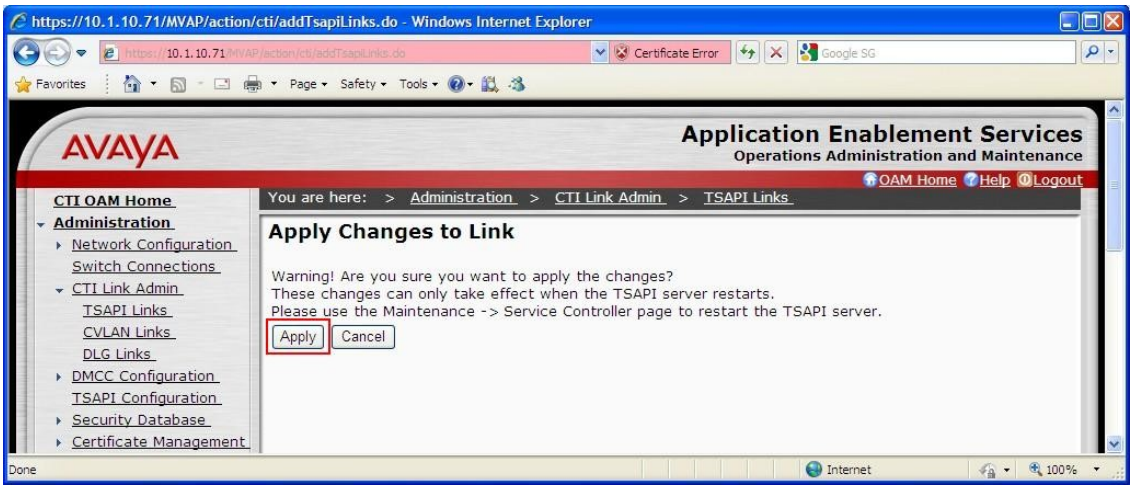
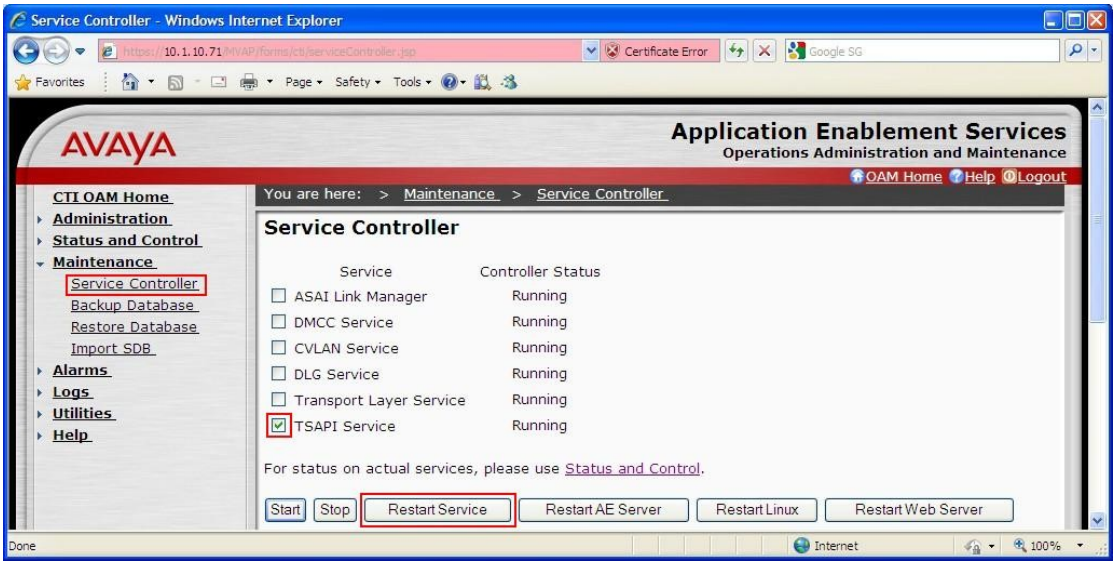
5.3. Administer Switch Connection

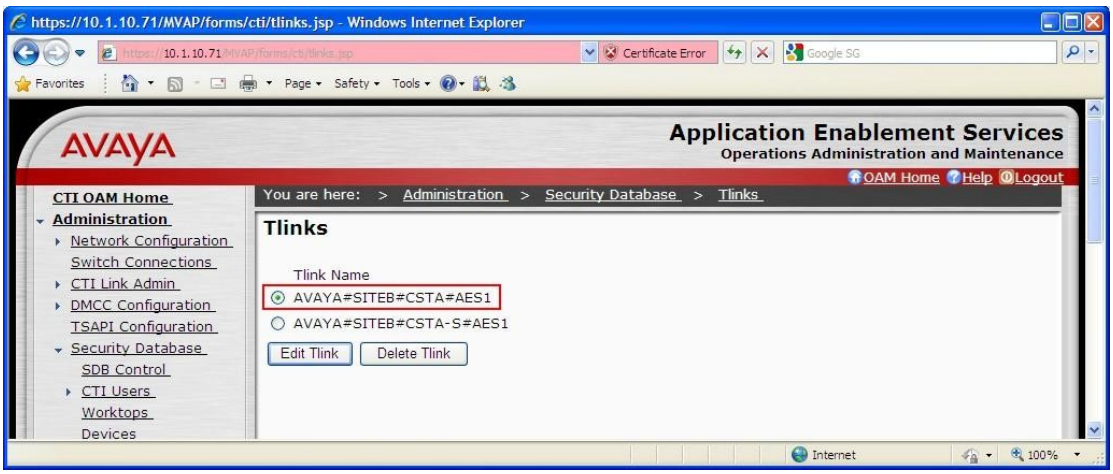
Step	Description
1.	From the CTI OAM Home menu, select **Administration > Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this configuration, **SITEB** is used. 
2.	The Set Password – SITEB screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Communication Manager using the IP Services form in **Section 4.1 Step 4**. The **SSL** field needs to be checked. Click on **Apply**. 

Step	Description
3.	The Switch Connections screen is displayed. Select the newly added switch connection name and click **Edit CLAN IPs**. 
4.	In the Edit CLAN IPs – SITEB screen, enter the host name or IP address of the processor interface as shown on the Communication Manager in **Section 4.1 Step 3**, which is **10.1.20.10**. Click **Add Name or IP**. 

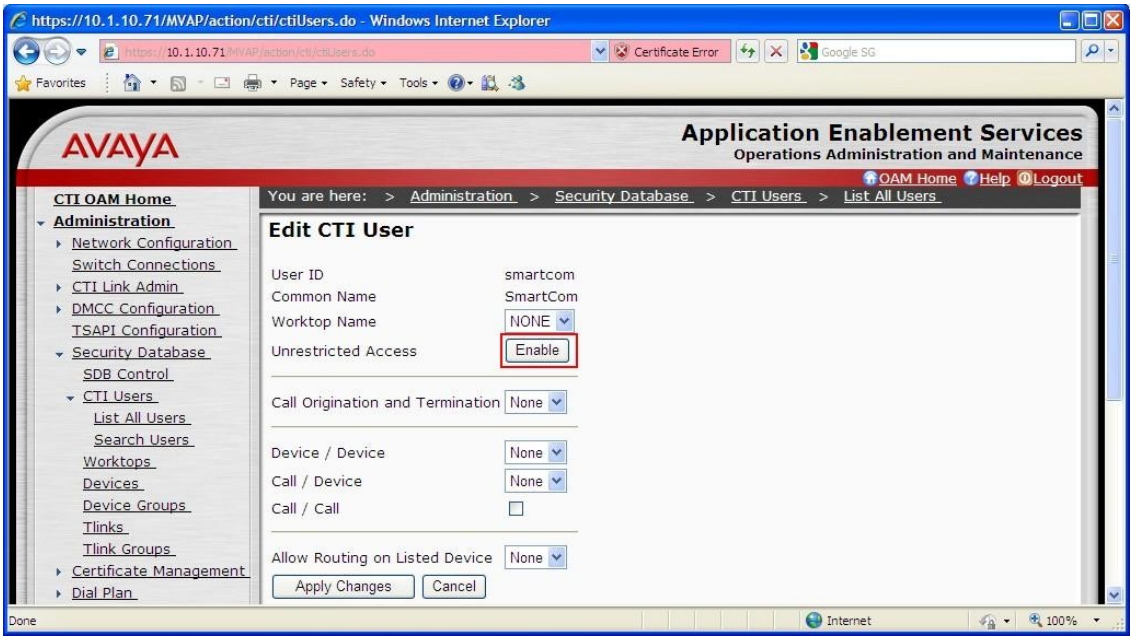
5.4. Administer TSAPI Link

Step	Description
1.	To administer a TSAPI link, select **Administration > CTI Link Admin > TSAPI Links** from the CTI OAM Home menu. Click **Add Link**. 
2.	In the Add / Edit TSAPI Links screen, select the following values: • **Link:** Select an available Link number from 1 to 16. • **Switch Connection:** Administered switch connection in **Section 5.3 Step 1**. • **Switch CTI Link Number:** Corresponding CTI link number in **Section 4.1 Step 2**. • **ASAI Link Version:** Set to **5**. • **Security:** Set to **Both** so that both encrypted and unencrypted TSAPI Links can be used. Note that the actual values may vary. Click **Apply Changes**. 

Step	Description
3.	Click **Apply** to confirm the changes. 
4.	To restart the TSAPI Service, select **Maintenance > Service Controller** from the CTI OAM Home menu. Check **TSAPI Service** and click **Restart Service**. 

Step	Description
5.	Click **Restart** to confirm the restart. 
6.	Navigate to the Tlinks screen by selecting **Administration > Security Database > Tlinks** from the CTI OAM Home menu. Note the value of the **Tlink Name**, as this will be needed to configure Hua Pu SmartCom Server in **Section 6.2**. In this configuration, the unencrypted **Tlink Name AVAYA#SITEB#CSTA#AES1** is used. 

5.5. Administer CTI User Permission

Step	Description
1.	Select **Administration > Security Database > CTI Users > List All Users** from the CTI OAM Home menu. Select the **User ID** created in **Section 5.1 Step 2** and click **Edit**. 
2.	Assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, **Unrestricted Access** privilege was enabled during compliance testing. If **Unrestricted Access** is not desired, then consult [1] for guidance on configuring the call/device privileges as well as devices and device groups. Click **Enable**. 

Step	Description
3.	Click **Apply** to apply the changes. This completes the configuration for Application Enablement Services. 
4.	Select **Administration > Security Database > SDB Control** from the CTI OAM Home menu. Uncheck **Enable SDB TSAPI Service, JTAPI and Telephony Service** and click **Apply Changes**. For simplicity in configuration, The SDB was not enabled for TSAPI Service during compliance testing. If this is not desired, then consult [1] for guidance on configuring the devices and device groups. 

6. Configure Hua Pu SmartCom

Hua Pu installs, configures and customizes Hua Pu SmartCom for their end customers. This section describes only the interface configuration for Hua Pu SmartCom to communicate with Application Enablement Services and Communication Manager. Refer to [3] and [4] for the detail configuration of Hua Pu SmartCom.

6.1. Install Application Enablement Services TSAPI Client Software

Hua Pu SmartCom uses the Application Enablement Services TSAPI Client software to communication with the TSAPI Service on the Application Enablement Services server. The TSAPI Client software will be provided by Hua Pu, or it can also be downloaded from Avaya Support website (http://support.avaya.com).

The installation runs through the following steps:

a. A welcome window will be displayed. Click **Next** to continue.

b. Accept the **Destination Folder** and click **Next**.

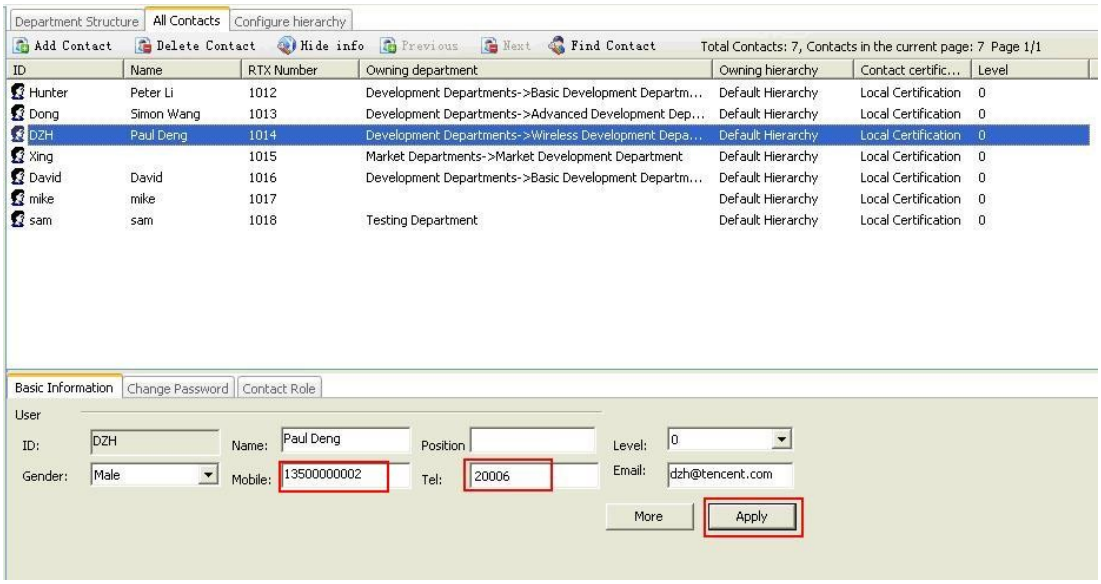
c. In the **Host Name or IP Address** field, enter the IP address of the Application Enablement Services server and click **Add to List**. In this configuration, enter **10.1.10.71**. Click **Next**.

d. At the end of installation process click **Finish**.

6.2. Configure Hua Pu SmartCom Server

Step	Description
1.	On the Hua Pu SmartCom Server, edit the file **TeleServer.ini** located in the folder **C:\HuaPu\RTX-AES\TeleServer** using Notepad. Configure the following fields below required for the integration to the Application Enablement Services TSAPI Service. • **ServerName**: Tlink Name as shown in **Section 5.4 Step 6**, in this case is **AVAYA#SITEB#CSTA#AES1**. • **UserName**: CTI User created in **Section 5.1 Step 2**, in this case is **smartcom**. • **Password**: CTI User password created in **Section 5.1 Step 2**. (Note: Password field is configured as clear text. When the SmartCom Server application is run for the first time, it will convert the value to cipher text.) • **DialPre**: Enter the ARS Access Code from **Section 4.2**.
2.	Deploy the Hua Pu SmartCom Plug-in **avayaplugin.rpi** located in the folder **C:\HuaPu\RTX-AES** to all the RTX Clients. This is accomplished by using the Auto Upgrade tool in Tencent RTX Manager so that the RTX Clients will be prompted to install the plug-in the next time they logged in. Refer to [5] for more details.

Step	Description
3.	Using Tencent RTX Manager, configure phone extensions and mobile number for all RTX Users in the **Tel** and **Mobile** fields respectively and click **Apply**.



7. General Test Approach and Test Results

The feature test cases were performed manually. Using Tencent RTX clients with the Hua Pu Plug-in installed, incoming and outgoing calls were placed on Communication Manager. Features provided by Hua Pu SmartCom such as Click-to-Call, call control, call transfers and conference were tested. The phone statuses of other users (e.g. idle or busy) were also verified during testing.

The serviceability test cases were performed manually by disconnecting the Ethernet cables on the Hua Pu SmartCom server and Application Enablement Services server, rebooting of the Communication Manager and Hua Pu SmartCom server.

All feature and serviceability test cases were executed and passed.

8. Verification Steps

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

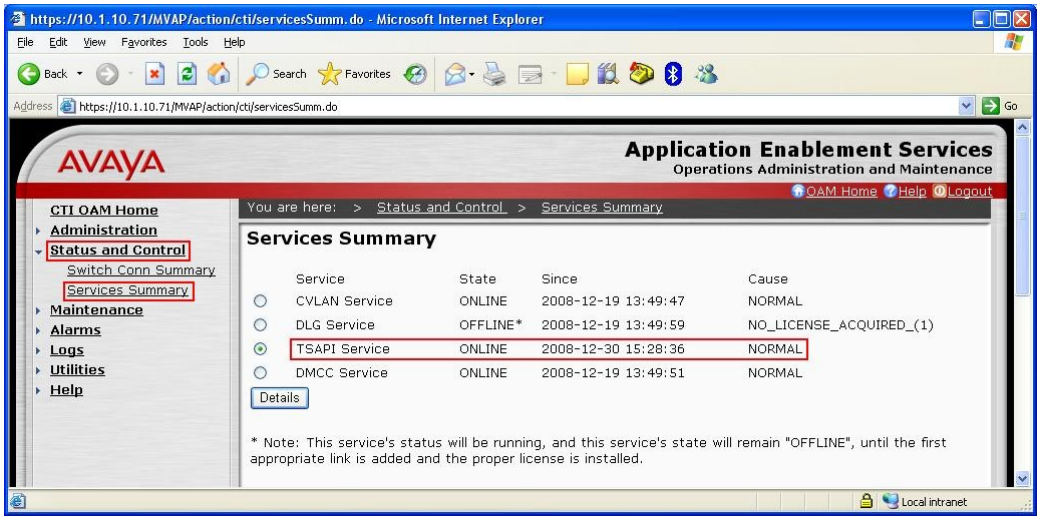
8.1. Verify Communication Manager

Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command. The **Service State** field should display **established**.

```
status aesvcs cti-link

                        AE SERVICES CTI LINK STATUS

CTI    Version  Mnt    AE Services      Service       Msgs     Msgs
Link            Busy   Server           State         Sent     Rcvd

1      5        no     aes1             established   67       85
```

8.2. Verify Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI Service by selecting **Status and Control > Services Summary** from the left pane. The **State** field for the **TSAPI Service** should display **ONLINE**.



8.3. Verify Hua Pu SmartCom

Using the Tencent RTX client, place a Click-to-Call to another user using the Contact List. For the user receiving the call, click the Answer button to answer the call. Verify that the call is set up successfully and the RTX Client window shows the correct phone statuses for the users as shown below.

9. Conclusion

These Application Notes describe the configuration steps required for Hua Pu SmartCom to interoperate with Communication Manager and Application Enablement Services using the Telephony Services Application Programming Interface (TSAPI). All feature and serviceability test cases were completed successfully.

10. Additional References

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

The following Avaya product documentations can be found at http://support.avaya.com.

[1] *Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide*, Release 4.2, Document ID 02-300357, Issue 10, May 2008.
[2] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Issue 7, Release 5.2, May 2009, Document Number 555-245-205.

The following product documentations are available from Hua Pu.

[3] *Hua Pu SmartCom Inc R2.0 User Guide*.
[4] *Hua Pu SmartCom Server R2.0 Installation Guide*.

The following product documentations are available from Tencent Technology.

[5] *RTX Administrator's Manual*, Version 2008, October 2007.

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.