



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Callray Communications AP Suite Quality Management System with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0**

### **Abstract**

These Application Notes describe the procedures for configuring Callray Communications AP Suite Quality Management System to monitor and record calls placed to and from stations, IP Softphones, and agents on Avaya Communication Manager.

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.

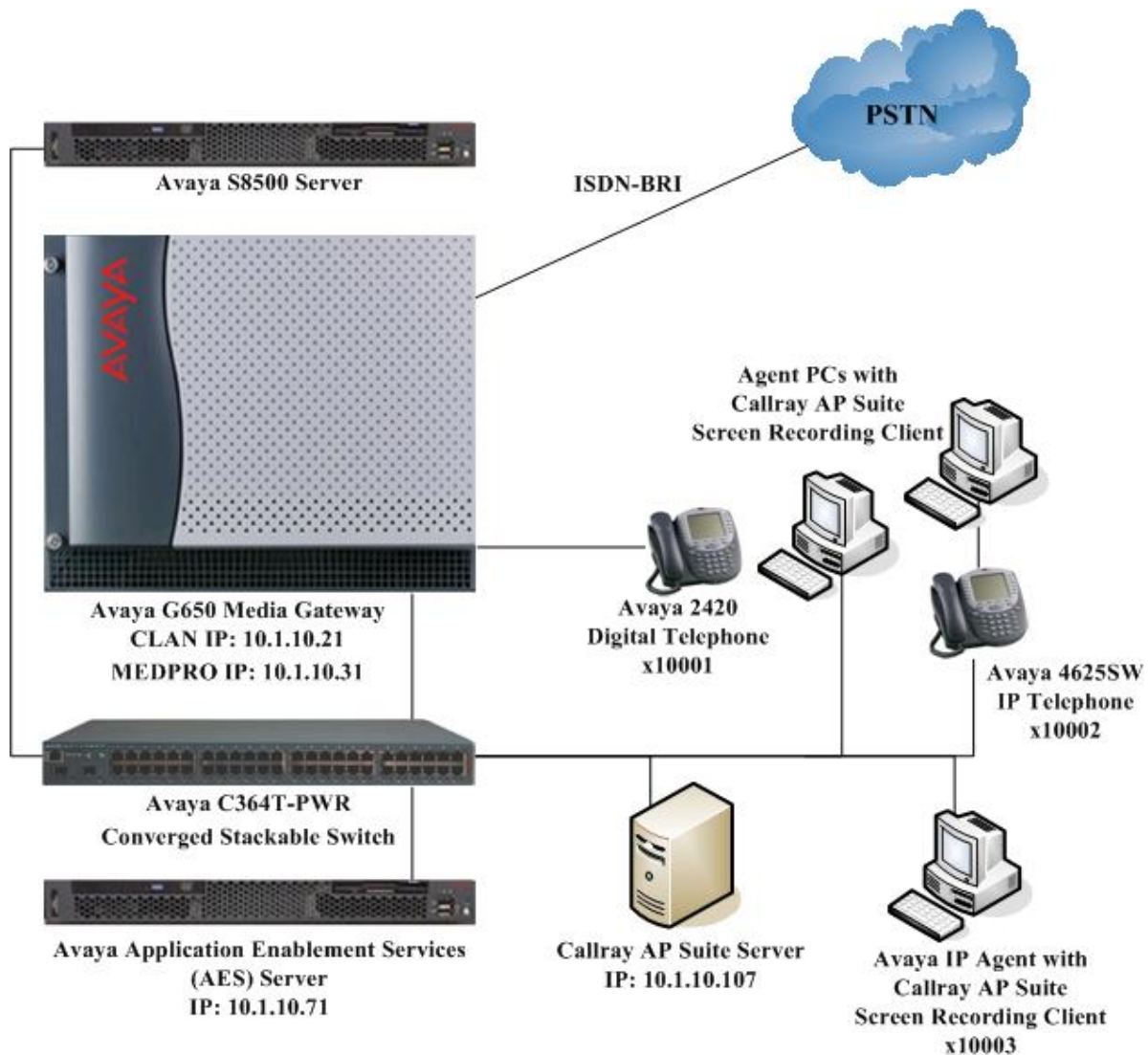
# 1. Introduction

These Application Notes describe a compliance-tested configuration comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) and Callray Communications AP Suite Quality Management System.

Callray AP Suite Quality Management System performs many functions such as the recording, monitoring, retrieving and playing of calls. At the same time, it is also designed to be a management tool for the measurement of agent quality, featuring integrated quality testing, screen capture, assessment, training, and study of agent's performance, forming the overall quality control solution of a call center.

Callray AP Suite communicates with Avaya AES using the Telephony Services Application Programming Interface (TSAPI) and Device, Media and Call Control (DMCC) API (formally known as CMAPI). Callray AP Suite connects to the DMCC Service and registers one DMCC station for every extension to be recorded. When a call starts on an extension to be recorded, the DMCC station will be added to the call using the TSAPI Single Step Conference feature. This causes the Avaya Media Gateway to send the audio packets to Callray AP Suite, which will then record them to the database. Detailed call information obtained using TSAPI are also stored for each call along with the recording.

**Figure 1** illustrates a sample configuration consisting of an Avaya S8500 Server, an Avaya G650 Media Gateway, an Avaya AES Server, Avaya IP and Digital Telephones, an agent PC running Avaya IP Agent and a Windows 2003 Server running Callray AP Suite Server software. The agent PCs were also installed with the Callray AP Suite Screen Recording Client for screen recording. The Callray AP Suite Server registers DMCC stations with Avaya Communication Manager using the Device and Media Control (CMAPI) Service for voice recording. The Callray AP Suite Server also monitors the agent extension using the TSAPI Service to retrieve call related information. Both the DMCC and TSAPI Services are provided by the Avaya AES Server.



**Figure 1: Test Configuration**

## 2. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server	Avaya Communication Manager 5.1 (Service Pack 1 01.0.414.3-15962)

Equipment	Software
Avaya G650 Media Gateway	-
- TN2312BP IP Server Interface	HW07, FW044
- TN799DP C-LAN Interface	HW01, FW026
- TN2602AP IP Media Processor	HW02, FW040
- TN2214CP Digital Line	HW08, FW015
Avaya Application Enablement Services	4.1 with Patch 1
Avaya 4625 Series IP Telephone	2.8.8.7 (H.323)
Avaya 2420 Series Digital Telephone	-
Avaya IP Agent	7.0.25.128
Avaya C364T-PWR Converged Stackable Switch	4.5.18
Callray Communications AP Suite Quality Management System	5.3

### 3. Configure Avaya Communication Manager

This section provides the procedures for configuring Computer Telephony Integration (CTI) links and DMCC stations on Avaya Communication Manager. All the configuration changes in Avaya 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.

#### 3.1. Configure AES and CTI Links

The Avaya AES server forwards CTI requests, responses, and events between Callray AP Suite and Avaya Communication Manager. The Avaya AES server communicates with Avaya Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Callray AP Suite. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI links. See **Section 4** for the details of configuring the AES side of the AES and CTI links.

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

Step	Description												
	<pre>display system-parameters customer-options</pre> <p style="text-align: right;">Page 3 of 11</p> <p style="text-align: center;">OPTIONAL FEATURES</p> <pre> Abbreviated Dialing Enhanced List? n      Audible Message Waiting? n Access Security Gateway (ASG)? n          Authorization Codes? y Analog Trunk Incoming Call ID? n Backup Cluster Automatic Takeover? n A/D Grp/Sys List Dialing Start at 01? n    CAS Branch? n Answer Supervision by Call Classifier? n    CAS Main? n ARS? y                                     Change COR by FAC? n ARS/AAR Partitioning? y Computer Telephony Adjunct Links? y ARS/AAR Dialing without FAC? n Cvg Of Calls Redirected Off-net? n ASAI Link Core Capabilities? n            DCS (Basic)? n ASAI Link Plus Capabilities? n            DCS Call Coverage? n Async. Transfer Mode (ATM) PNC? n         DCS with Rerouting? n Async. Transfer Mode (ATM) Trunking? n ATM WAN Spare Processor? n Digital Loss Plan Modification? n ATMS? n                                  DS1 MSP? n Attendant Vectoring? n                   DS1 Echo Cancellation? n </pre>												
2.	<p>Enter the <b>add cti-link m</b> command, where <b>m</b> is a number between 1 and 64, inclusive. Enter a valid <b>Extension</b> under the provisioned dial plan in Avaya Communication Manager, set the <b>Type</b> field to <b>ADJ-IP</b>, and assign a descriptive <b>Name</b> to the CTI link.</p>												
	<pre>add cti-link 1</pre> <p style="text-align: right;">Page 1 of 2</p> <p style="text-align: center;">CTI LINK</p> <pre> CTI Link: 1 Extension: 19951 Type: ADJ-IP Name: TSAPI Svcs COR: 1 </pre>												
3.	<p>Enter the <b>change node-names ip</b> command. In the compliance-tested configuration, the <b>CLAN-01A02</b> IP address was utilized for registering H.323 endpoints (Avaya IP Telephones and IP Agent softphone, and AES DMCC stations) and for connectivity to Avaya AES.</p>												
	<pre>change node-names ip</pre> <p style="text-align: right;">Page 1 of 2</p> <p style="text-align: center;">IP NODE NAMES</p> <table border="1"> <thead> <tr> <th>Name</th><th>IP Address</th></tr> </thead> <tbody> <tr> <td>CLAN-01A02</td><td>10.1.10.21</td></tr> <tr> <td>MEDPRO-01A13</td><td>10.1.10.31</td></tr> <tr> <td>VAL-01A04</td><td>10.1.10.41</td></tr> <tr> <td>default</td><td>0.0.0.0</td></tr> <tr> <td>procr</td><td>10.1.10.10</td></tr> </tbody> </table>	Name	IP Address	CLAN-01A02	10.1.10.21	MEDPRO-01A13	10.1.10.31	VAL-01A04	10.1.10.41	default	0.0.0.0	procr	10.1.10.10
Name	IP Address												
CLAN-01A02	10.1.10.21												
MEDPRO-01A13	10.1.10.31												
VAL-01A04	10.1.10.41												
default	0.0.0.0												
procr	10.1.10.10												
4.	<p>Enter the <b>change ip-services</b> command. On Page 1, configure the <b>Service Type</b> field to <b>AESVCS</b> and the <b>Enabled</b> field to <b>y</b>. The <b>Local Node</b> field should be pointed to the <b>CLAN-01A02</b> board that was configured previously in <b>Step 3</b>. During the compliance test, the default port was utilized for the <b>Local Port</b> field.</p>												

Step	Description																					
	<div>change ip-services<div>Page1 of 3</div><table><thead><tr><th colspan="7">IP SERVICES</th></tr><tr><th>Service Type</th><th>Enabled</th><th>Local Node</th><th>Local Port</th><th>Remote Node</th><th colspan="2">Remote Port</th></tr></thead><tbody><tr><td>AESVCS</td><td>y</td><td>CLAN-01A02</td><td>8765</td><td></td><td colspan="2"></td></tr></tbody></table></div>	IP SERVICES							Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		AESVCS	y	CLAN-01A02	8765			
IP SERVICES																						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																	
AESVCS	y	CLAN-01A02	8765																			
	<p>On Page 3, enter the hostname of the Avaya AES server for the <b>AE Services Server</b> field. The server name may be obtained by logging in to the Avaya AES server using Secure Shell (SSH), and running the <b>uname -a</b> command. Enter an alphanumeric password for the <b>Password</b> field and set the <b>Enabled</b> field to <b>y</b>. The same password will be configured on the Avaya AES server in <b>Section 4.3 Step 2</b>.</p>																					
	<div>change ip-services<div>Page3 of 3</div><div>AE Services Administration</div><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>aes1</td><td>xxxxxxxxxxxxxxxx</td><td>y</td><td></td></tr><tr><td>2:</td><td></td><td></td><td></td><td></td></tr><tr><td>3:</td><td></td><td></td><td></td><td></td></tr></tbody></table></div>	Server ID	AE Services Server	Password	Enabled	Status	1:	aes1	xxxxxxxxxxxxxxxx	y		2:					3:					
Server ID	AE Services Server	Password	Enabled	Status																		
1:	aes1	xxxxxxxxxxxxxxxx	y																			
2:																						
3:																						

## 3.2. Recording Stations

The recording stations in this configuration are DMCC stations that essentially appear as IP softphones to Avaya Communication Manager. Each DMCC station requires an IP\_API\_A license.

Step	Description																														
1.	Enter the <b>display system-parameters customer-options</b> command and verify that there are sufficient <b>IP_API_A</b> licenses. If not, contact an authorized Avaya account representative to obtain these licenses.																														
	<div>display system-parameters customer-options<span style="float: right;">Page 10 of 11</span></div> <div>MAXIMUM IP REGISTRATIONS BY PRODUCT ID</div> <table><thead><tr><th>Product ID</th><th>Rel. Limit</th><th>Used</th></tr></thead><tbody><tr><td><b>IP_API_A</b></td><td><b>: 500</b></td><td><b>0</b></td></tr><tr><td>IP_API_B</td><td>: 0</td><td>0</td></tr><tr><td>IP_API_C</td><td>: 0</td><td>0</td></tr><tr><td>IP_Agent</td><td>: 100</td><td>0</td></tr><tr><td>IP_IR_A</td><td>: 100</td><td>0</td></tr><tr><td>IP_Phone</td><td>: 2400</td><td>4</td></tr><tr><td>IP_ROMax</td><td>: 2400</td><td>0</td></tr><tr><td>IP_Soft</td><td>: 100</td><td>0</td></tr><tr><td>IP_eCons</td><td>: 2</td><td>0</td></tr></tbody></table>	Product ID	Rel. Limit	Used	<b>IP_API_A</b>	<b>: 500</b>	<b>0</b>	IP_API_B	: 0	0	IP_API_C	: 0	0	IP_Agent	: 100	0	IP_IR_A	: 100	0	IP_Phone	: 2400	4	IP_ROMax	: 2400	0	IP_Soft	: 100	0	IP_eCons	: 2	0
Product ID	Rel. Limit	Used																													
<b>IP_API_A</b>	<b>: 500</b>	<b>0</b>																													
IP_API_B	: 0	0																													
IP_API_C	: 0	0																													
IP_Agent	: 100	0																													
IP_IR_A	: 100	0																													
IP_Phone	: 2400	4																													
IP_ROMax	: 2400	0																													
IP_Soft	: 100	0																													
IP_eCons	: 2	0																													

Step	Description
2.	<p>Enter the <b>add station t</b> command, where <b>t</b> is an extension valid under the provisioned dial plan. On Page 1, set <b>Type</b> to an IP telephone set type, enter a descriptive <b>Name</b>, specify the <b>Security Code</b>, and set <b>IP SoftPhone</b> to <b>y</b>. The <b>Security Code</b> is used to configure Callray AP Suite in <b>Section 5.2 Step 15</b>. Repeat this as necessary to configure additional DMCC stations. Use the same <b>Security Code</b> for all DMCC stations. For the compliance test, stations from 19901 to 19903 were created for the purpose of recording.</p>
<div>add station 19901<div>Page1 of 4</div><div>STATION</div><div><div><div>Extension: 19901</div><div>Type: 4621</div><div>Port: IP</div><div>Name: AP Suite #1</div></div><div><div>Lock Messages? n</div><div>Security Code: 00000</div><div>Coverage Path 1:</div><div>Coverage Path 2:</div><div>Hunt-to Station:</div></div><div><div>BCC: 0</div><div>TN: 1</div><div>COR: 1</div><div>COS: 1</div></div></div><div>STATION OPTIONS</div><div><div>Loss Group: 19</div><div>Speakerphone: 2-way</div><div>Display Language: english</div><div>Survivable GK Node Name:</div><div>Survivable COR: internal</div><div>Survivable Trunk Dest? y</div></div><div><div>Personalized Ringing Pattern: 1</div><div>Message Lamp Ext: 19901</div><div>Mute Button Enabled? y</div><div>Expansion Module? n</div><div>Media Complex Ext:</div><div>IP SoftPhone? y</div><div>IP Video Softphone? n</div><div>Customizable Labels? y</div></div></div>	

### 3.3. Codec Configuration

Enter the **change ip-codec-set u** command, where **u** is a number between 1 and 7, inclusive. Enter **G.711MU** for **Audio Codec**. In this configuration, only the G.711MU codec is used.

change ip-codec-set 1

Page1 of 2

IP Codec Set

Codec Set: 1

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1:	G.711MU	n	2	20

### 3.4. IP Network Regions

During compliance testing, the C-LAN board was assigned to IP network region 1 for all H.323 endpoint registrations. One MedPro board was also assigned to IP network region 1 to support the RTP voice traffic between all IP telephones, IP Agent and DMCC stations. As such, all the RTP traffic between them is governed by the same codec set as configured in **Section 3.3**.

Enter the **change ip-network-region v** command, where **v** is the number of the IP network region discussed above. Set **Codec Set** to the ip-codec-set number configured in **Section 3.3**.

```
change ip-network-region 1                                     Page 1 of 19
                                                                IP NETWORK REGION
  Region: 1
Location: 1      Authoritative Domain:
  Name: Local
MEDIA PARAMETERS                                           Intra-region IP-IP Direct Audio: yes
  Codec Set: 1                                             Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048                                       IP Audio Hairpinning? n
  UDP Port Max: 7999
DIFFSERV/TOS PARAMETERS                                   RTCP Reporting Enabled? y
  Call Control PHB Value: 46                               RTCP MONITOR SERVER PARAMETERS
  Audio PHB Value: 46                                     Use Default Server Parameters? y
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5                               AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
  H.323 Link Bounce Recovery? n
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

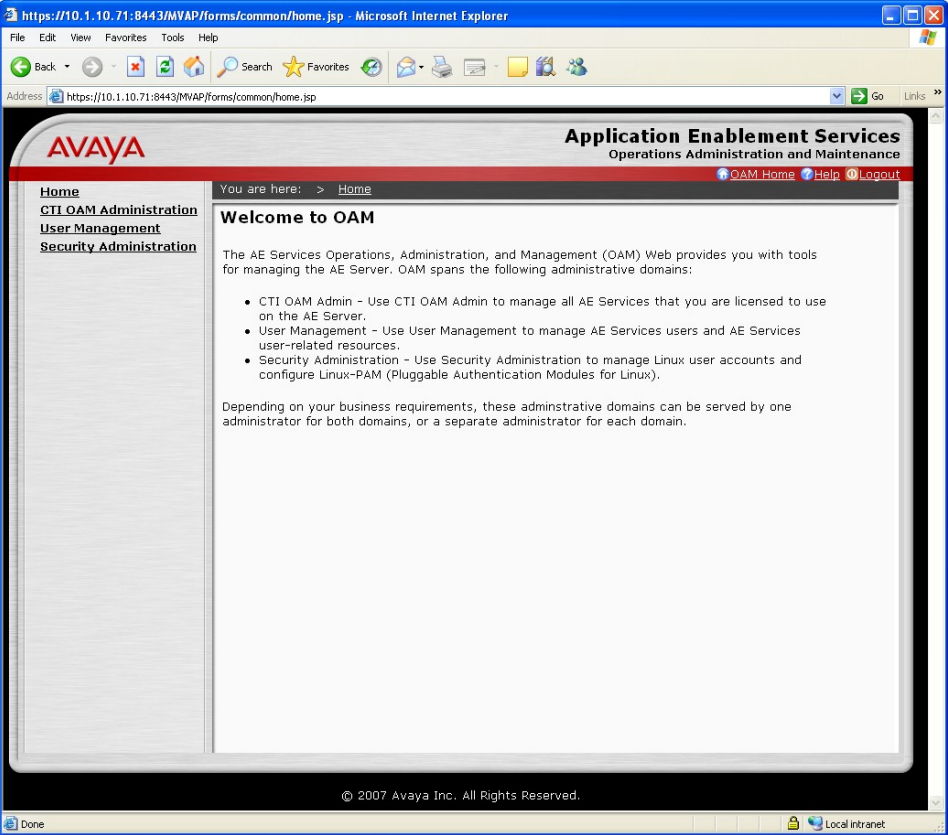
## 4. Configure Avaya Application Enablement Services

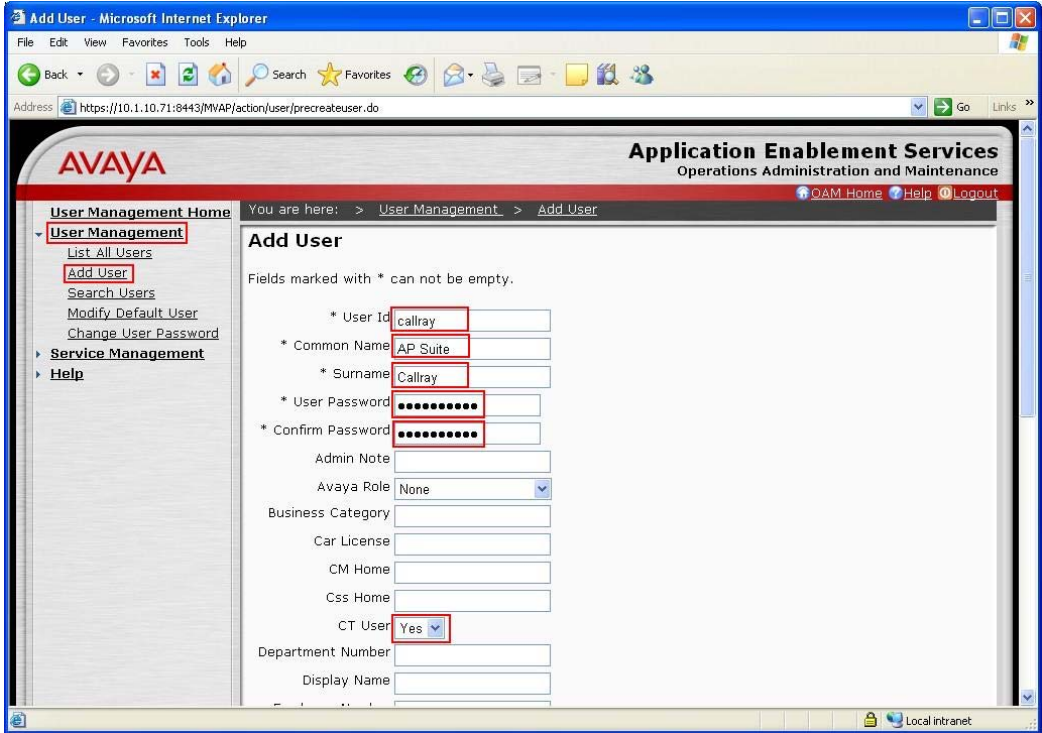
This section provides the procedures for configuring Avaya Application Enablement Services. The procedures fall into the following areas:

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

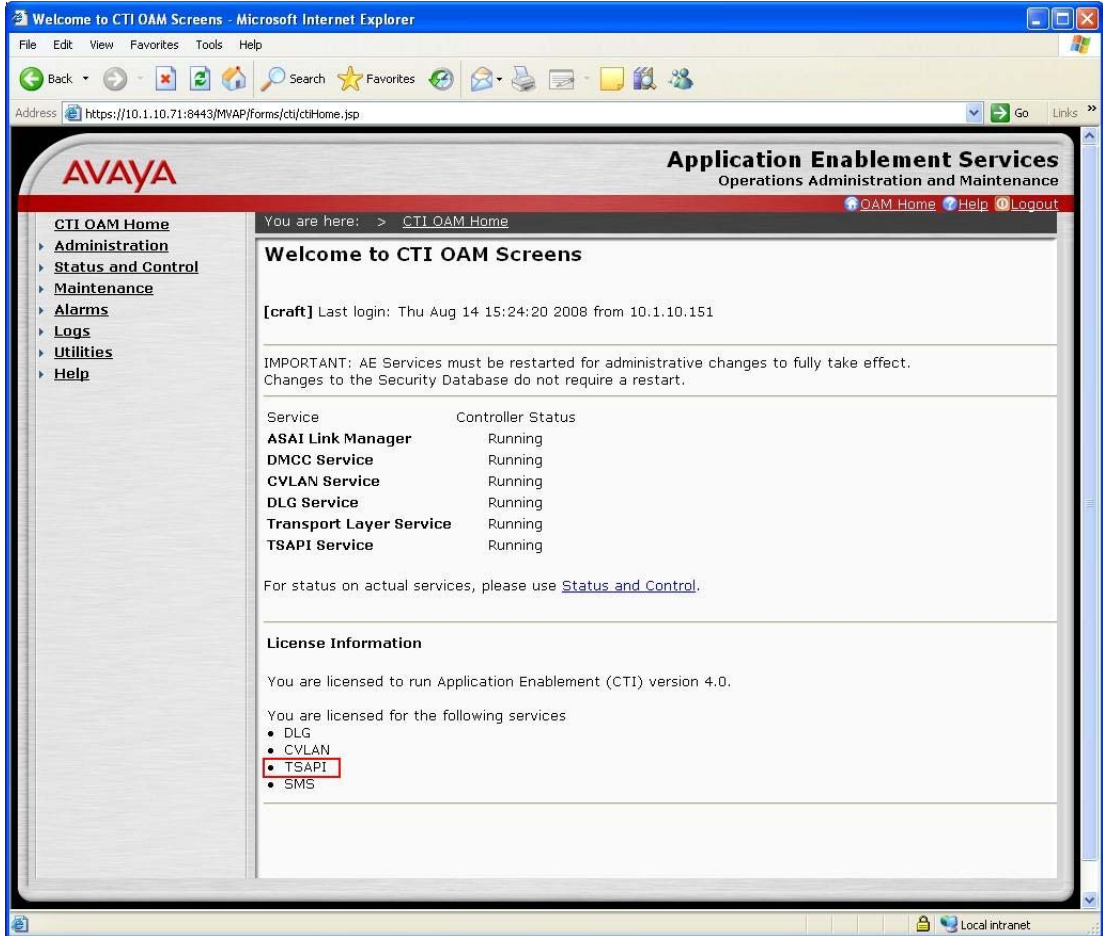


## 4.1. Administer CTI User

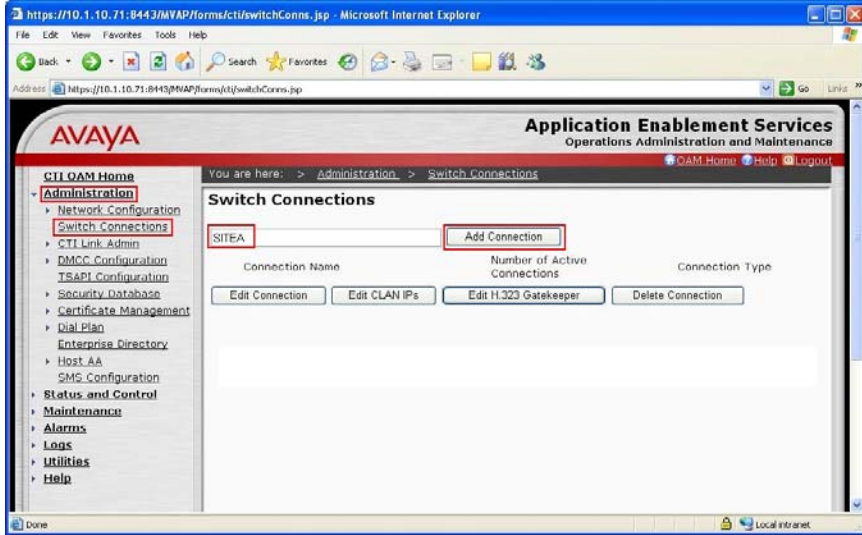
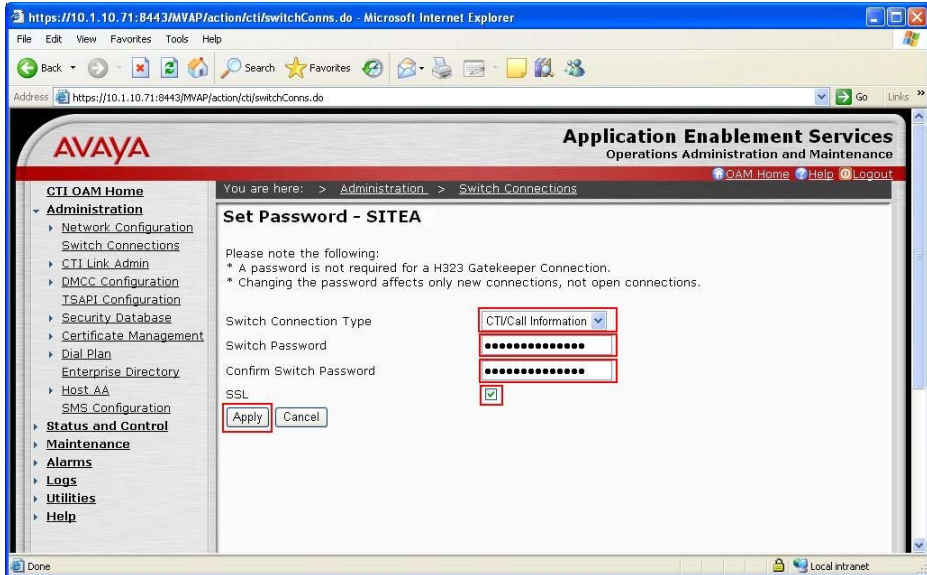
Step	Description
1.	<p>Launch a web browser and enter <b>https://&lt;IP address of AES server&gt;/MVAP/</b> to access the AES OAM web based interface. Log in to AES OAM using an administrative login and password (not shown), and the Welcome To OAM screen will be displayed.</p> 

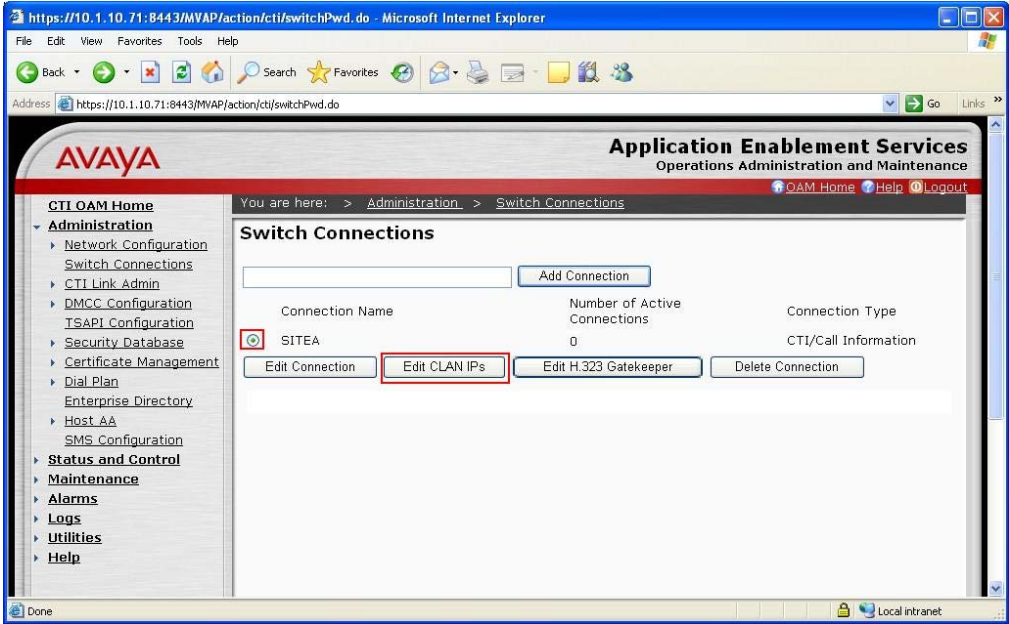
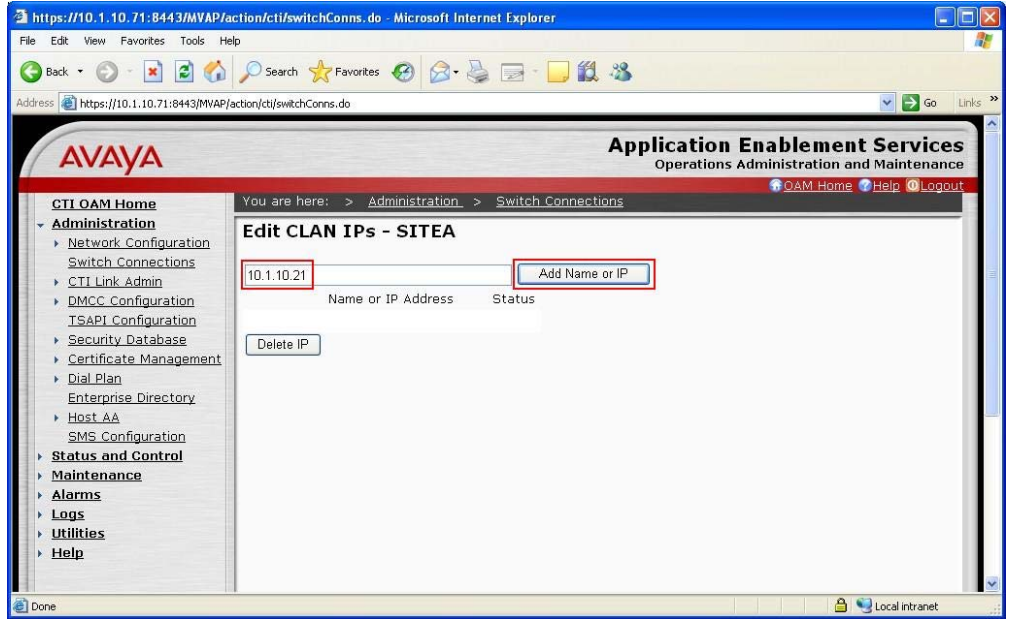
Step	Description
2.	<p>Click <b>User Management</b>, then <b>User Management &gt; Add User</b> in the left pane. Specify a value for <b>User Id</b>, <b>Common Name</b>, <b>Surname</b>, <b>User Password</b> and <b>Confirm Password</b>. Set <b>CT User</b> to <b>Yes</b>. Use the values for <b>User Id</b> and <b>User Password</b> to configure Callray AP Suite in <b>Section 5.2 Step 2</b> and <b>Step 15</b> to access the TSAPI and DMCC Services on the AES server respectively. Scroll down to the bottom of the page and click <b>Apply</b> (not shown).</p> 

## 4.2. Verify Avaya Application Enablement Services License

Step	Description														
1.	<p>Select <b>OAM Home</b>, then click on <b>CTI OAM Administration</b> from the left menu (not shown). From the Welcome to CTI OAM screen, verify that the Avaya 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.</p>  <p>The screenshot shows the 'Welcome to CTI OAM Screens' page in a Microsoft Internet Explorer browser. The address bar shows 'https://10.1.10.71:8443/MVAP/forms/cti/ctiHome.jsp'. The page has a red header with the 'AVAYA' logo and 'Application Enablement Services Operations Administration and Maintenance'. A left sidebar contains a menu with 'CTI OAM Home', 'Administration', 'Status and Control', 'Maintenance', 'Alarms', 'Logs', 'Utilities', and 'Help'. The main content area shows the user 'craft' last login on Thu Aug 14 15:24:20 2008 from 10.1.10.151. It includes an important note about restarting AE Services. A table lists services and their controller status: ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, Transport Layer Service, and TSAPI Service, all running. Below this, a 'License Information' section states the user is licensed for version 4.0 and lists services: DLG, CVLAN, TSAPI (highlighted with a red box), and SMS.</p> <table border="1"><thead><tr><th>Service</th><th>Controller Status</th></tr></thead><tbody><tr><td>ASAI Link Manager</td><td>Running</td></tr><tr><td>DMCC Service</td><td>Running</td></tr><tr><td>CVLAN Service</td><td>Running</td></tr><tr><td>DLG Service</td><td>Running</td></tr><tr><td>Transport Layer Service</td><td>Running</td></tr><tr><td>TSAPI Service</td><td>Running</td></tr></tbody></table> <p><b>License Information</b></p> <p>You are licensed to run Application Enablement (CTI) version 4.0.</p> <p>You are licensed for the following services</p> <ul style="list-style-type: none"><li>• DLG</li><li>• CVLAN</li><li>• <b>TSAPI</b></li><li>• SMS</li></ul>	Service	Controller Status	ASAI Link Manager	Running	DMCC Service	Running	CVLAN Service	Running	DLG Service	Running	Transport Layer Service	Running	TSAPI Service	Running
Service	Controller Status														
ASAI Link Manager	Running														
DMCC Service	Running														
CVLAN Service	Running														
DLG Service	Running														
Transport Layer Service	Running														
TSAPI Service	Running														

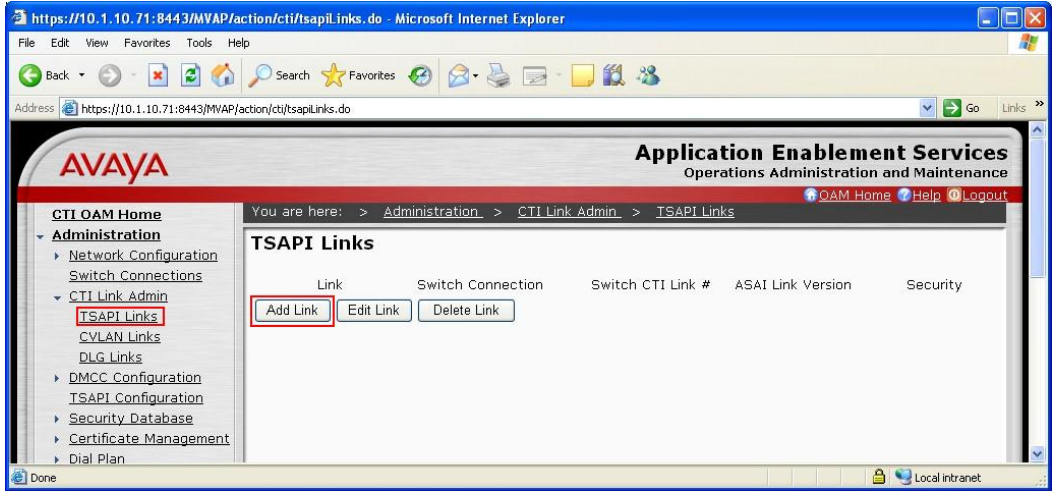
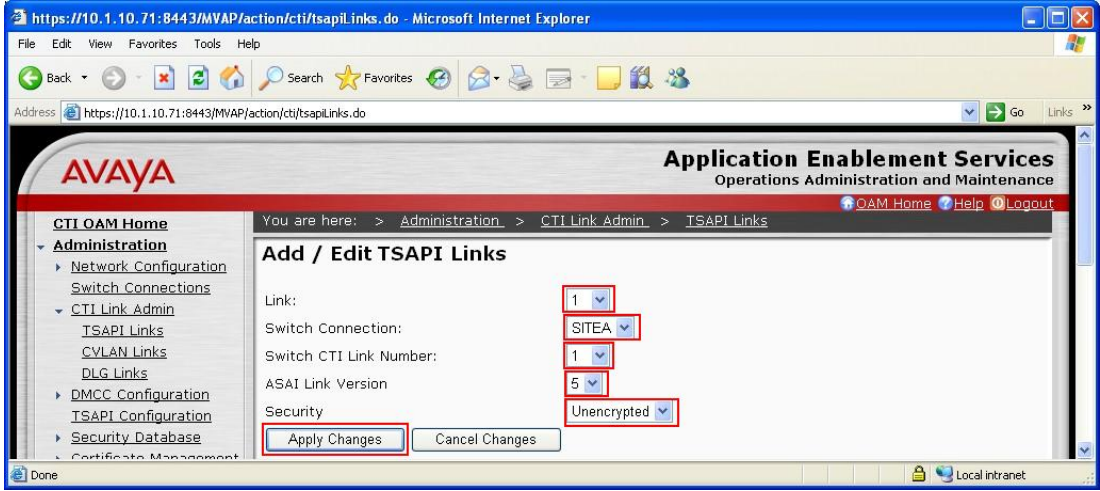
### 4.3. Administer Switch Connection

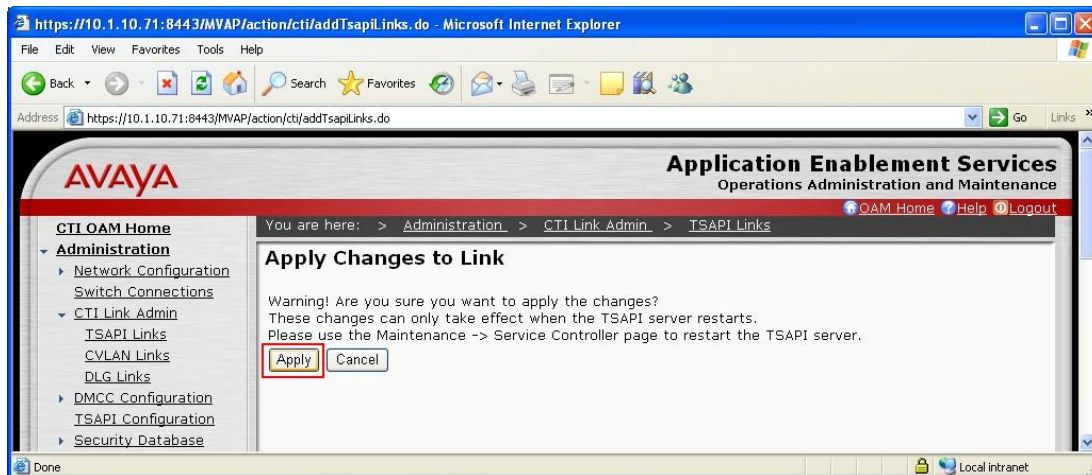
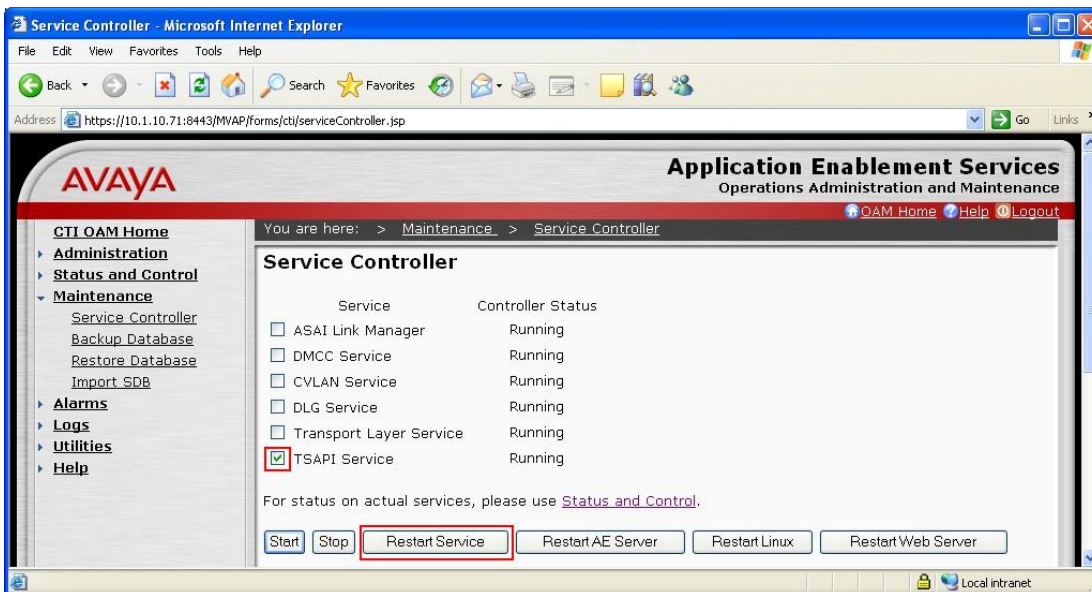
Step	Description
1.	<p>From the CTI OAM Home menu, select <b>Administration &gt; Switch Connections</b>. Enter a descriptive name for the switch connection and click <b>Add Connection</b>. In this case, <b>SITEA</b> is used.</p> 
2.	<p>The Set Password screen is displayed. Select <b>CTI/Call Information</b> for <b>Switch Connection Type</b>. For the <b>Switch Password</b> and <b>Confirm Switch Password</b> fields, enter the password that was administered in Avaya Communication Manager using the IP Services form in <b>Section 3.1 Step 4</b>. The <b>SSL</b> field needs to be checked for the S8500 Server. Click on <b>Apply</b>.</p> 

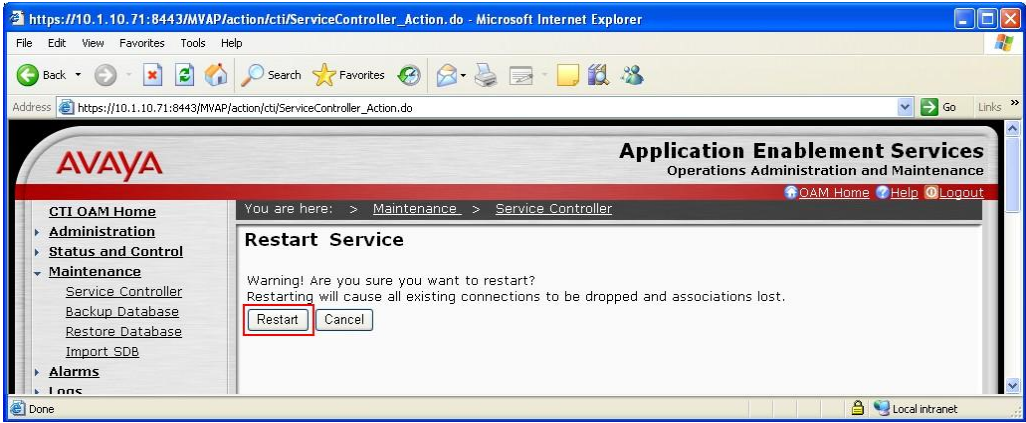
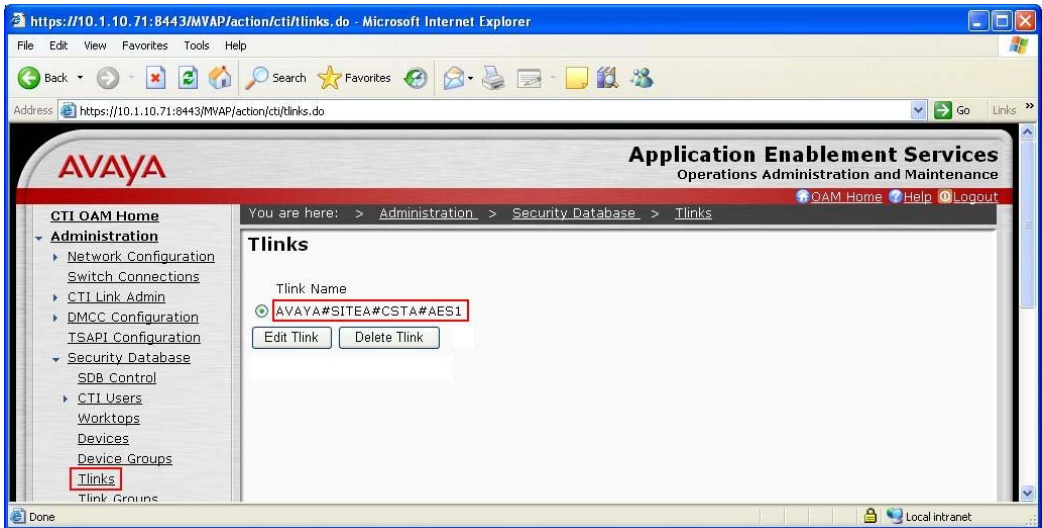
Step	Description
3.	<p>The Switch Connections screen is displayed. Select the newly added switch connection name and click <b>Edit CLAN IPs</b>.</p> 
4.	<p>In the Edit CLAN IPs screen, enter the host name or IP address of the C-LAN used for AES connectivity. In this case, 10.1.10.21 is used, which corresponds to the IP address of the C-LAN administered on Avaya Communication Manager in <b>Section 3.1 Step 3</b>. Click <b>Add Name or IP</b>.</p> 



## 4.4. Administer TSAPI Link

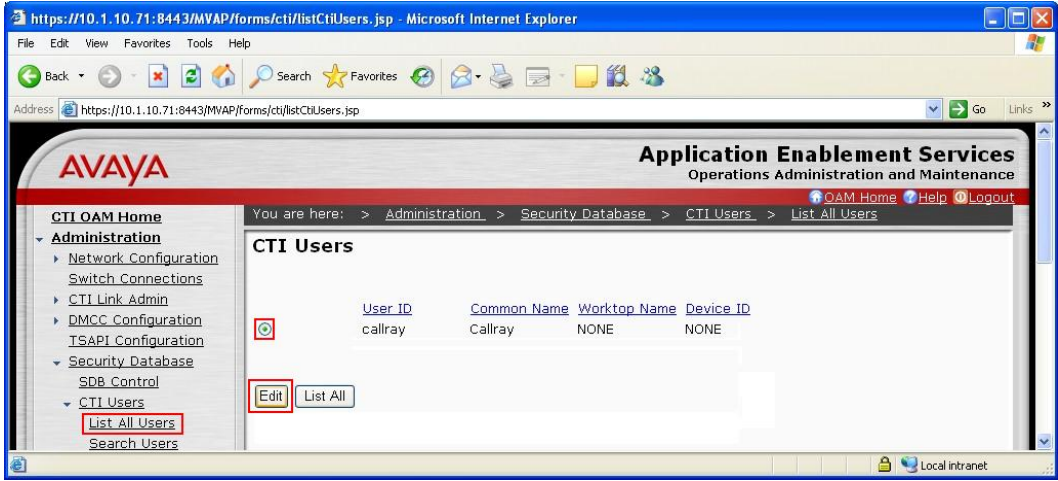
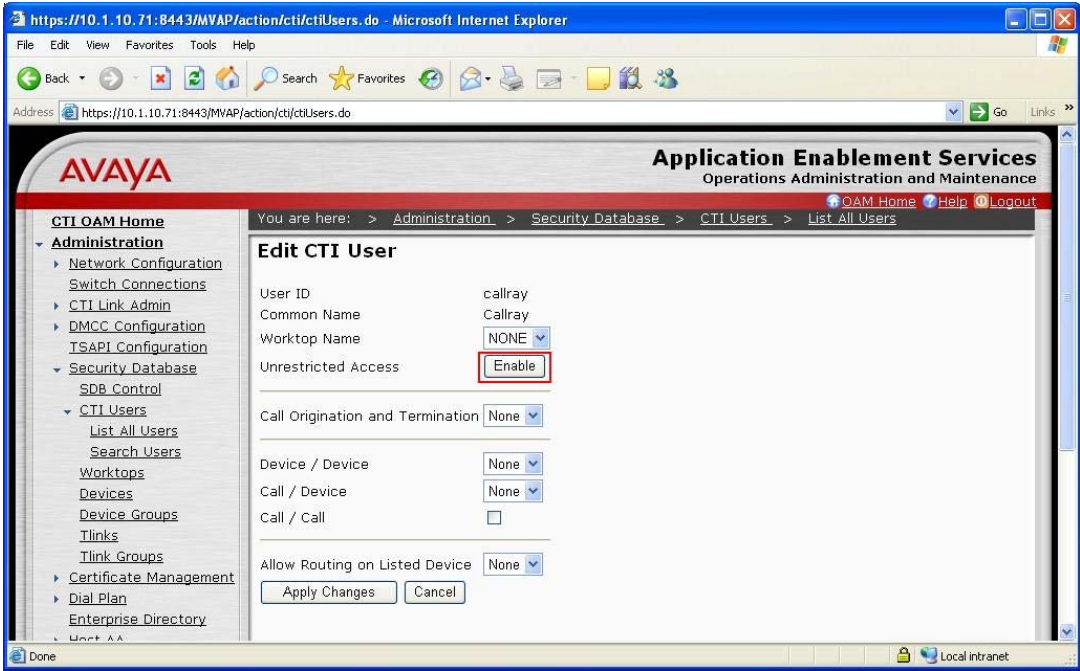
Step	Description
1.	<p>To administer a TSAPI link on AES, select <b>Administration &gt; CTI Link Admin &gt; TSAPI Links</b> from the CTI OAM Home menu. Click <b>Add Link</b>.</p> 
2.	<p>In the Add / Edit TSAPI Links screen, select the following values:</p> <ul style="list-style-type: none"><li>• <b>Link:</b> Select an available Link number from 1 to 16.</li><li>• <b>Switch Connection:</b> Administered switch connection in <b>Section 4.3 Step 1</b>.</li><li>• <b>Switch CTI Link Number:</b> Corresponding CTI link number in <b>Section 3.1 Step 2</b>.</li><li>• <b>ASAI Link Version:</b> Set to either <b>4</b> or <b>5</b>.</li><li>• <b>Security:</b> <b>Unencrypted</b> TSAPI Links are used.</li></ul> <p>Note that the actual values may vary. Click <b>Apply Changes</b>.</p> 

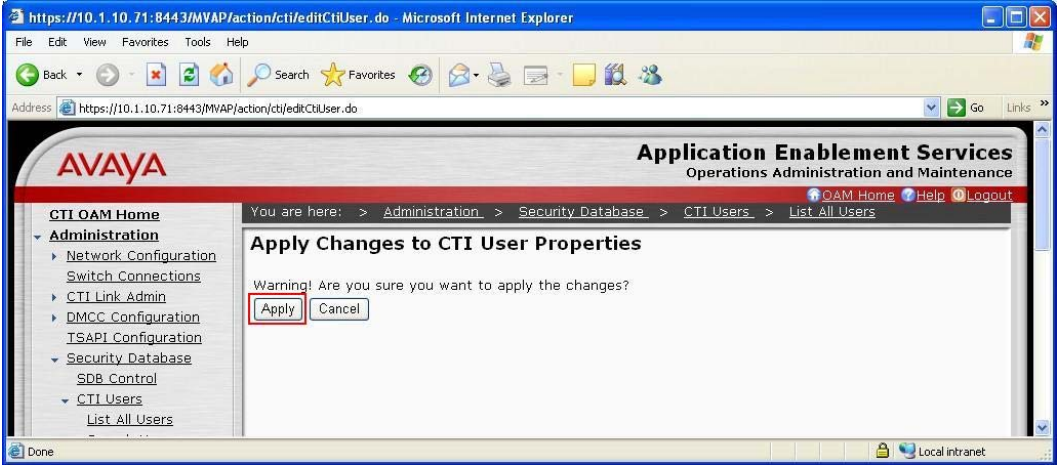
Step	Description
3.	Click <b>Apply</b> to confirm the changes.
	
4.	To restart the TSAPI Service, select <b>Maintenance &gt; Service Controller</b> from the CTI OAM Home menu. Check the <b>TSAPI Service</b> checkbox and click <b>Restart Service</b> .
	

Step	Description
5.	<p>Click <b>Restart</b> to confirm the restart.</p> 
6.	<p>Navigate to the Tlinks screen by selecting <b>Administration &gt; Security Database &gt; Tlinks</b> from the CTI OAM Home menu. Note the value of the <b>Tlink Name</b>, as this will be needed to configure the Callray AP Suite Server in <b>Section 5.2 Step 2</b>. In this configuration, the <b>Tlink Name</b> is <b>AVAYA#SITEA#CSTA#AES1</b>, which is automatically assigned by the AES server.</p> 

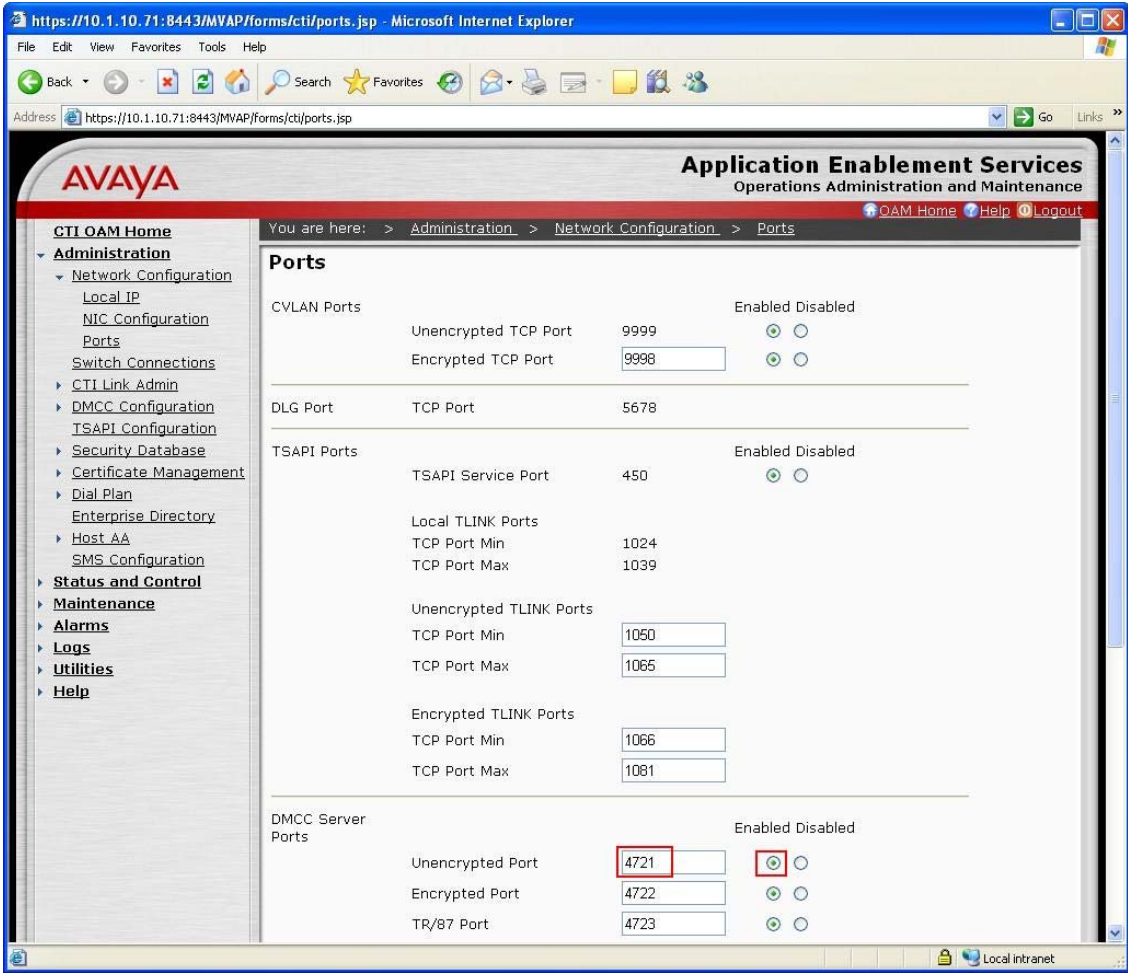


## 4.5. Administer CTI User Permission

Step	Description
1.	<p>Select <b>Administration &gt; Security Database &gt; CTI Users &gt; List All Users</b> from the CTI OAM Home menu. Select the <b>User ID</b> created in <b>Section 4.1 Step 2</b> and click <b>Edit</b>.</p> 
2.	<p>Assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, <b>Unrestricted Access</b> was enabled during compliance testing. If <b>Unrestricted Access</b> is not desired, then consult [1] for guidance on configuring the call/device privileges as well as devices and device groups. Click <b>Enable</b>.</p> 

Step	Description
3.	<p>Click <b>Apply</b> to apply the changes.</p> 

## 4.6. Administer Ports

Step	Description
1.	<p>From the CTI OAM Home menu, select <b>Administration &gt; Network Configuration &gt; Ports</b>. For the DMCC Server Ports, verify that <b>Unencrypted Port</b> is <b>Enabled</b> and note the port value, as this will be needed to configure the Callray AP Suite Server in <b>Section 5.2 Step 15</b>. During the compliance test, the default port values were utilized.</p> 

## 5. Configure Callray AP Suite

Callray installs, configures, and customizes the Callray AP Suite application for their end customers. This section only describes the interface configuration for the Callray AP Suite application to communicate with Avaya AES and Avaya Communication Manager. Refer to [3] and [4] for configuring the Callray AP Suite application.

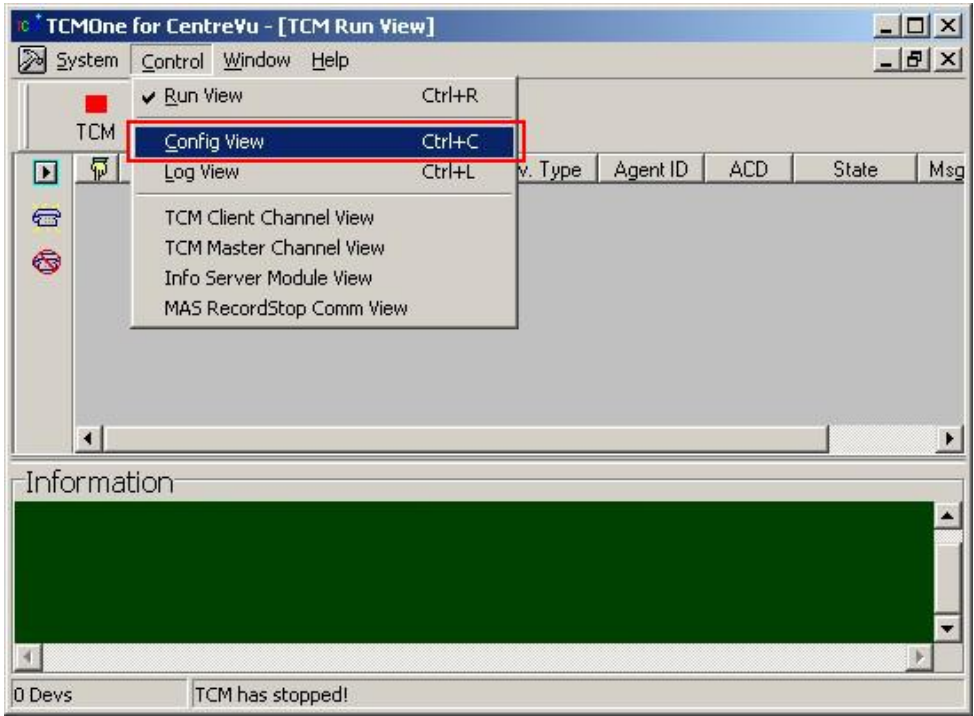
## 5.1. Install Avaya AES TSAPI Client Software

Callray AP Suite uses the Avaya AES TSAPI Client software to communicate with the TSAPI Service on the AES server. The Avaya AES TSAPI Client software will be provided by Callray, or it can also be downloaded from the Avaya Support website (<http://support.avaya.com>).

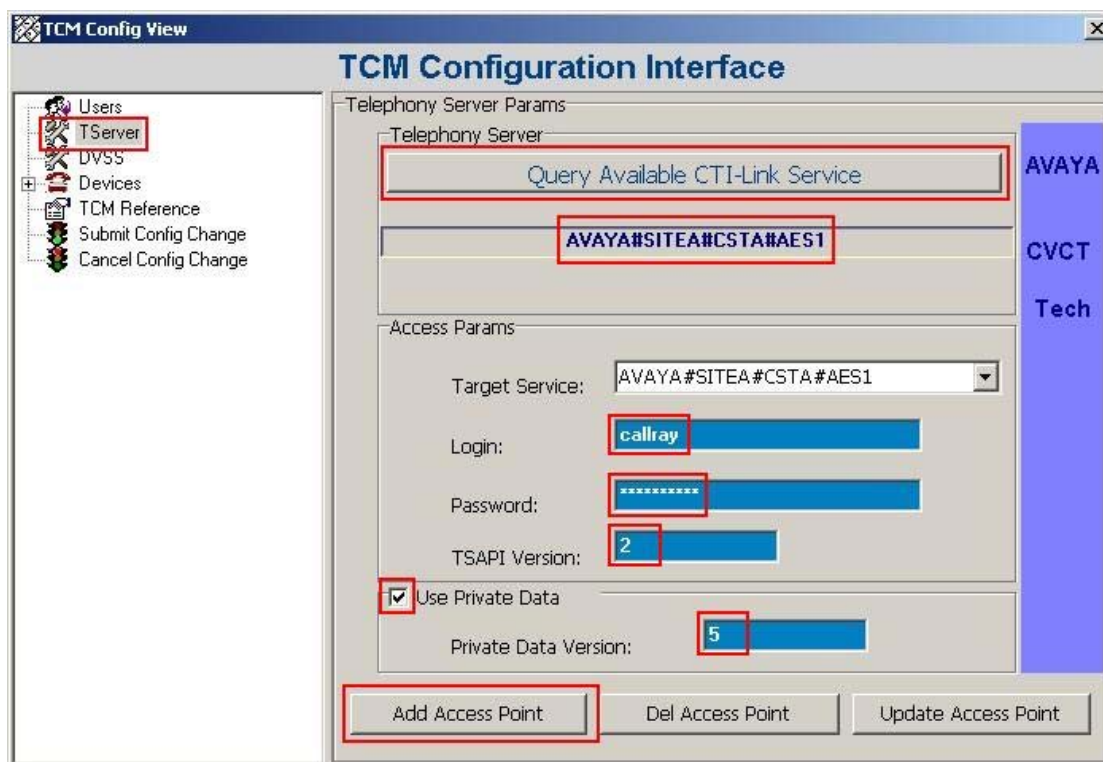
The installation runs through the following steps:

- 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 AES 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**.


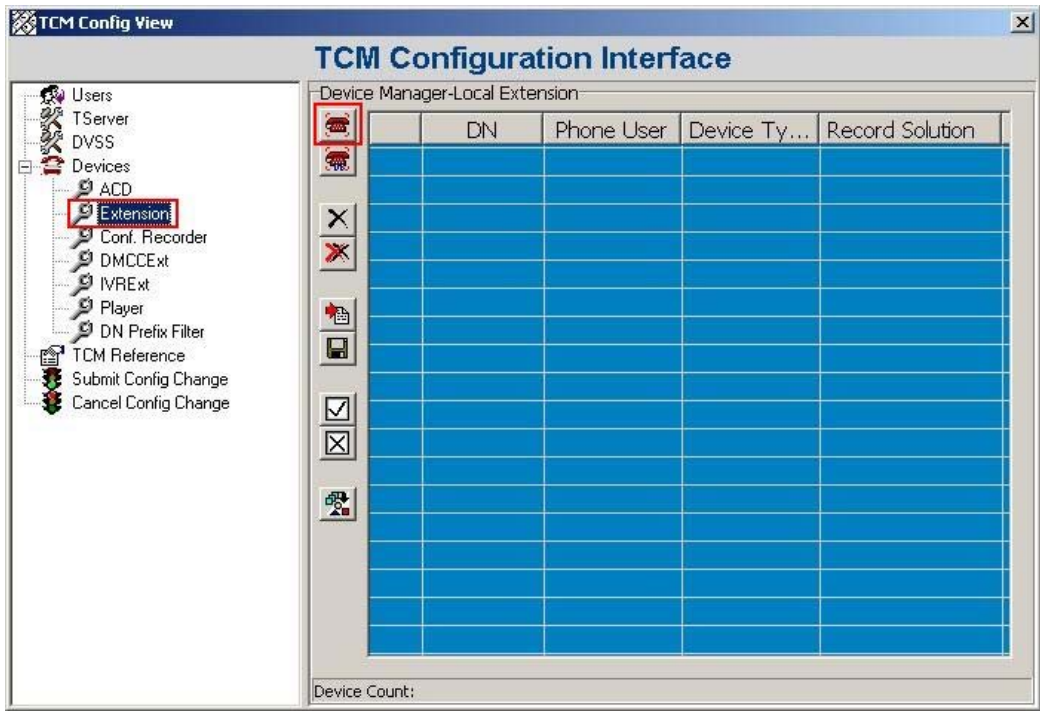
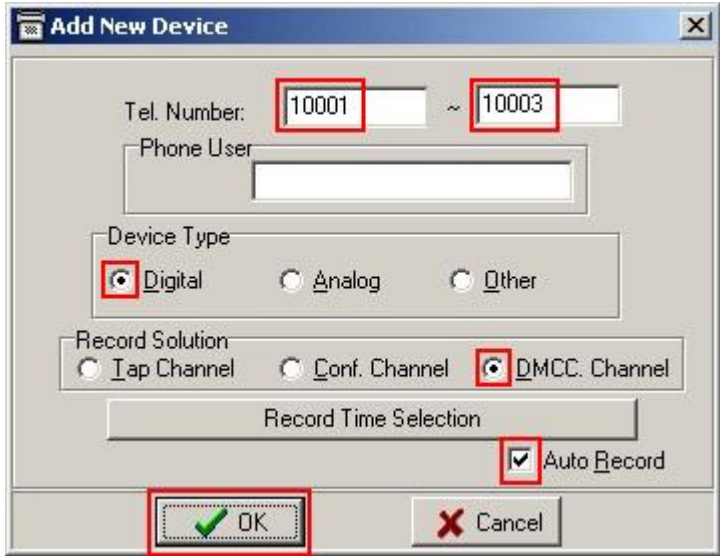
## 5.2. Configure Callray AP Suite


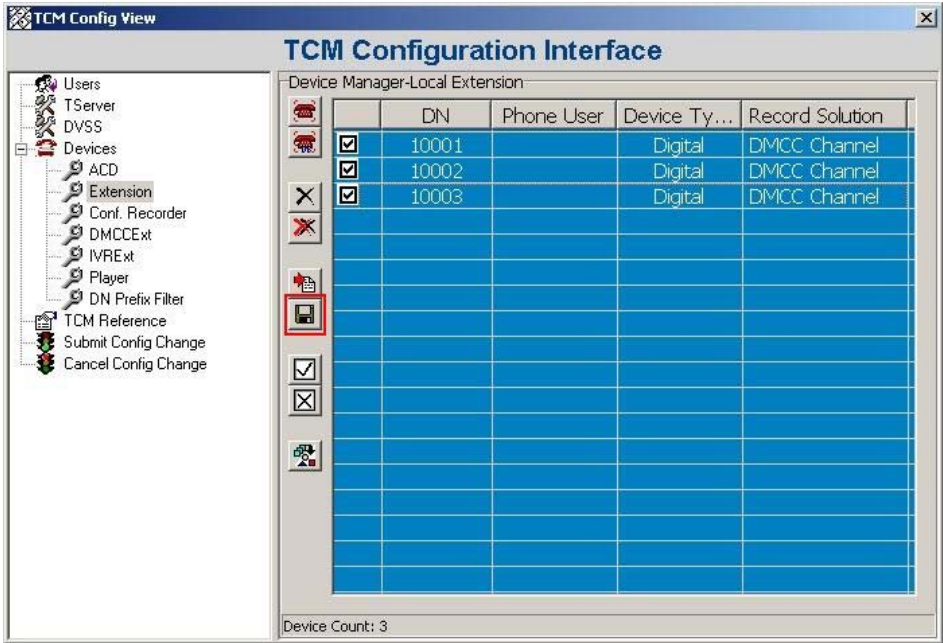

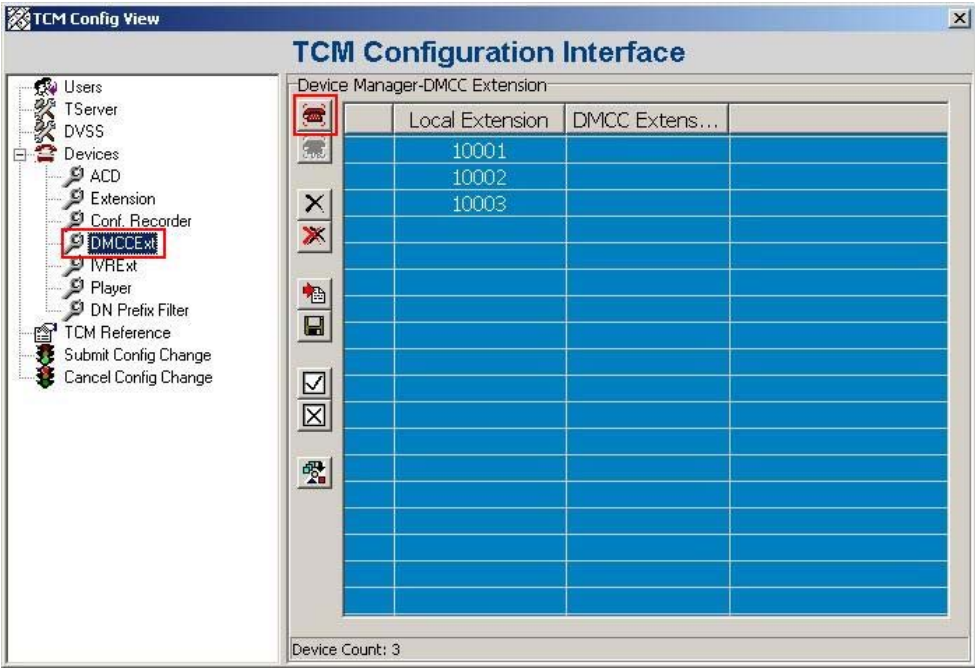
Step	Description
1.	<p>On the Callray AP Suite Server, click <b>Start &gt; Run</b>. Browse to the <b>C:\DVS\TCMOne\</b> folder and select the file <b>TCMOne.exe</b>. Click <b>OK</b> to launch it (not shown). Click <b>Control &gt; Config View</b> to open the configuration window.</p> 

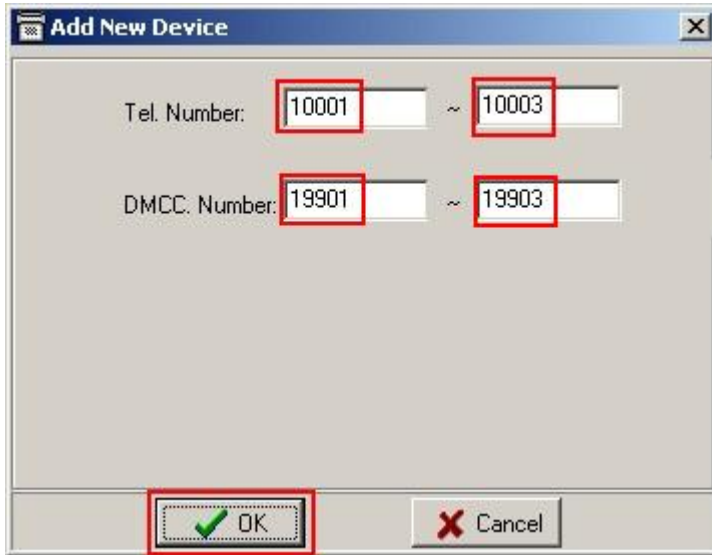

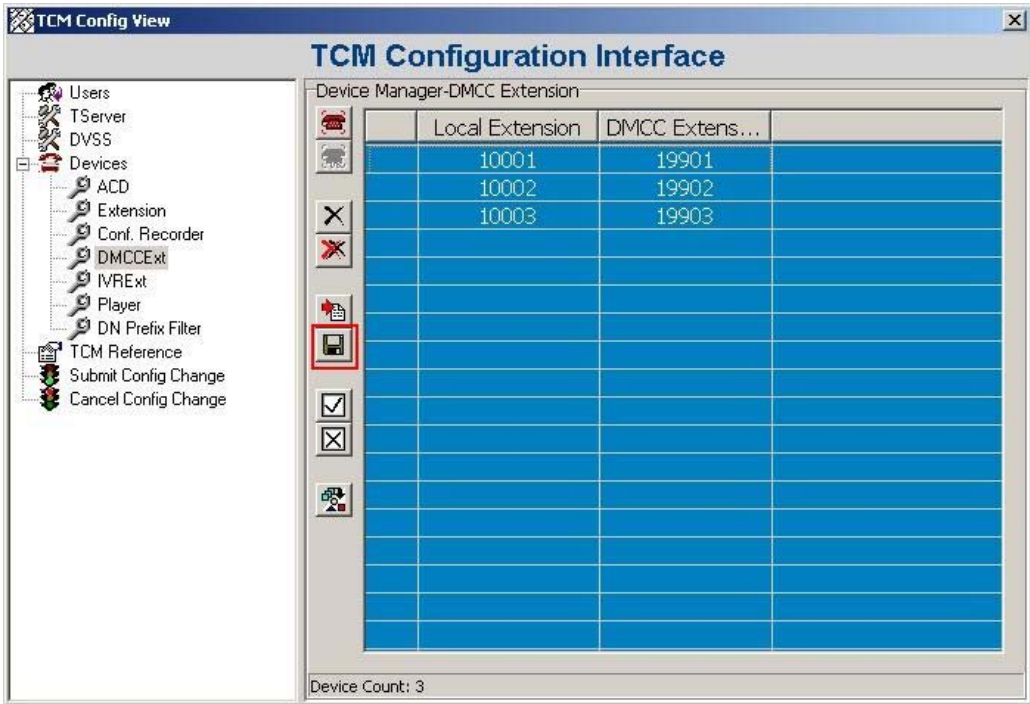
Step	Description
2.	<p>From the TCM Config View window, select <b>TServer</b> on the left pane to configure the Telephony Server parameters. Click <b>Query Available CTI-Link Service</b> to query for the available TSAPI Links. Select the TSAPI Link noted down in <b>Section 4.4 Step 4</b>. For <b>Login</b> and <b>Password</b>, enter the values configured in <b>Section 4.1 Step 2</b>. Set <b>TSAPI Version</b> to <b>2</b>, check <b>Use Private Data</b> and set <b>Private Data Version</b> to <b>5</b>. Click <b>Add Access Point</b> to continue.</p>




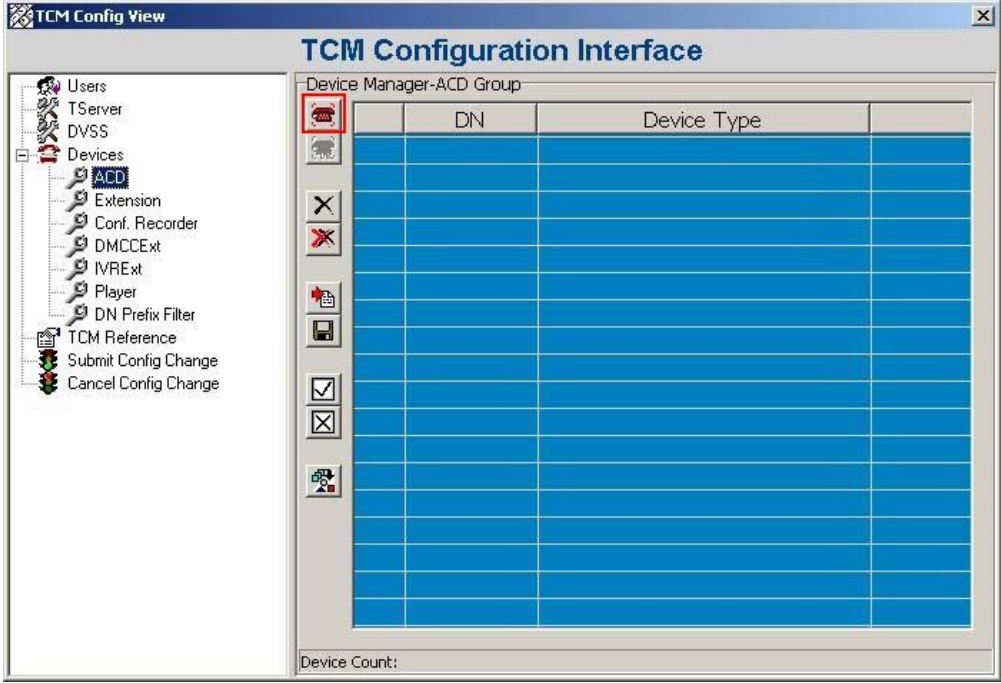
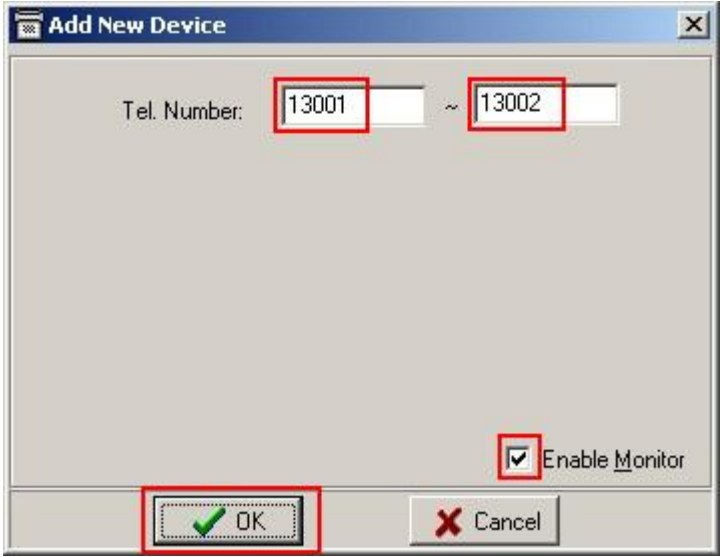



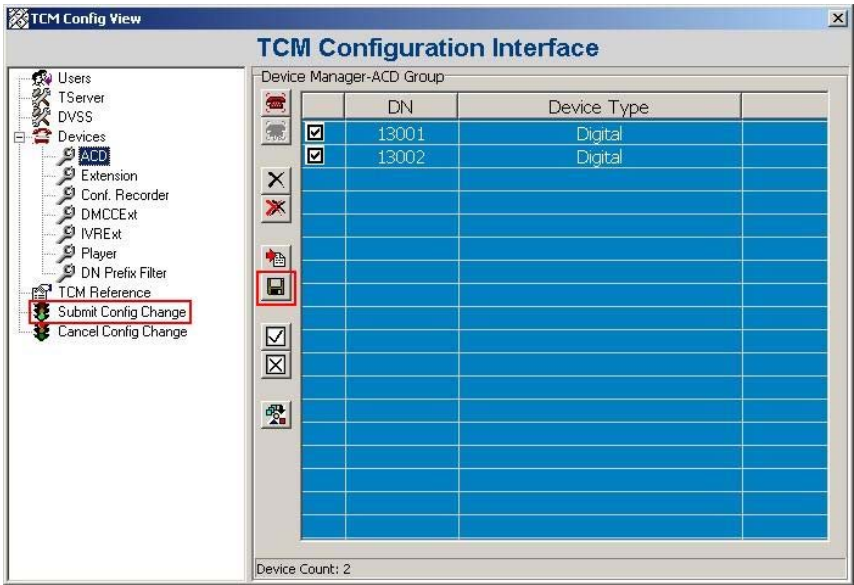
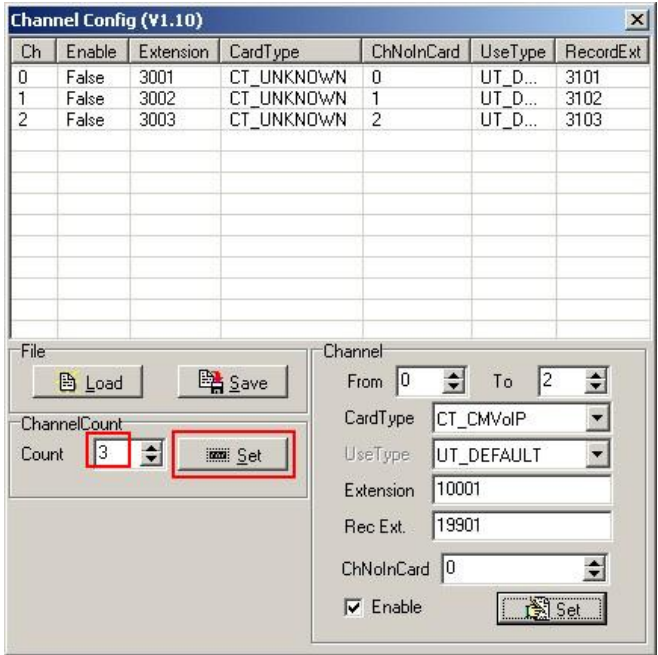
Step	Description
3.	<p>Select <b>Devices &gt; Extension</b> on the left pane to configure the extensions to be recorded. Click  (Add a new device).</p> 
4.	<p>From the Add New Device window, enter the extensions to be recorded for <b>Tel Number</b>. In this configuration, extensions 10001 to 10003 will be recorded. Select <b>Digital</b> for <b>Device Type</b>, <b>DMCC Channel</b> for <b>Record Solution</b> and check <b>Auto Record</b>. Click <b>OK</b>.</p> 

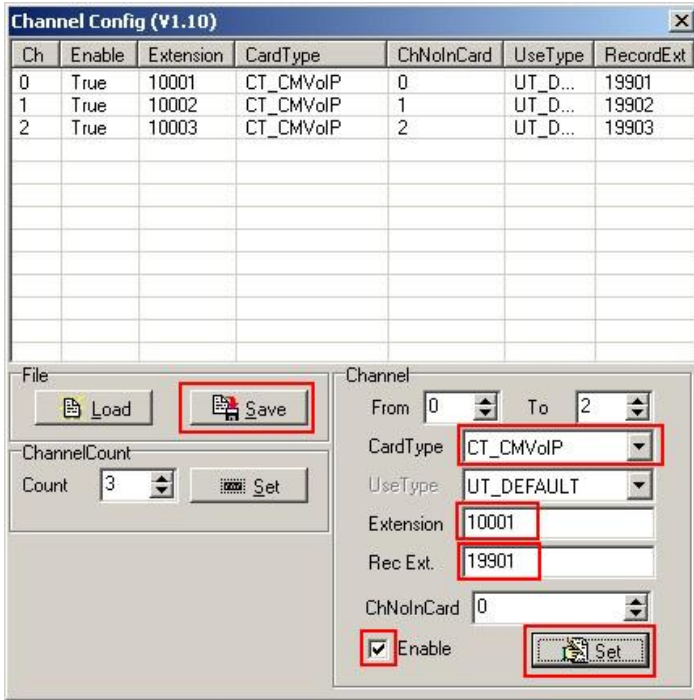

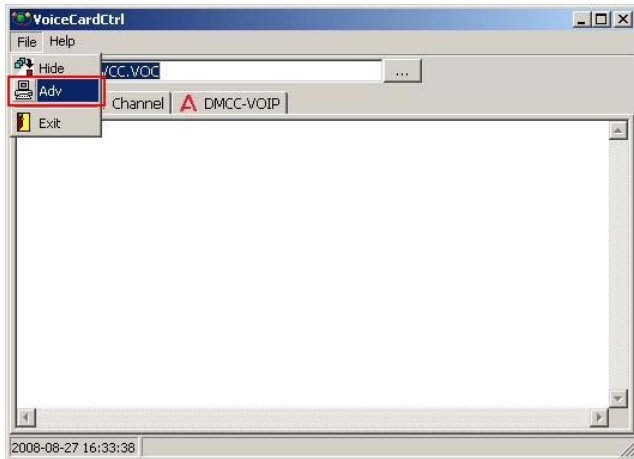
Step	Description
5.	<p>Click  (Save device configuration) to save the changes.</p>  <p>The screenshot shows the 'TCM Configuration Interface' window. On the left, a tree view has 'DMCCExt' selected under the 'Devices' category. The main area displays a table titled 'Device Manager-Local Extension' with columns: DN, Phone User, Device Ty..., and Record Solution. The table contains three rows with DN values 10001, 10002, and 10003, all of type 'Digital' and solution 'DMCC Channel'. The 'Save' icon (a floppy disk) in the left toolbar is highlighted with a red box. The status bar at the bottom indicates 'Device Count: 3'.</p>
4.	<p>Select <b>Devices &gt; DMCCExt</b> on the left pane to assign a DMCC station for each extension to be recorded. Click  (Add a new device).</p>  <p>The screenshot shows the 'TCM Configuration Interface' window. In the left tree view, 'DMCCExt' is selected under 'Devices'. The main area displays a table titled 'Device Manager-DMCC Extension' with columns: Local Extension, DMCC Extens..., and an empty column. The table contains three rows with 'Local Extension' values 10001, 10002, and 10003. The 'Add' icon (a telephone handset) in the left toolbar is highlighted with a red box. The status bar at the bottom indicates 'Device Count: 3'.</p>

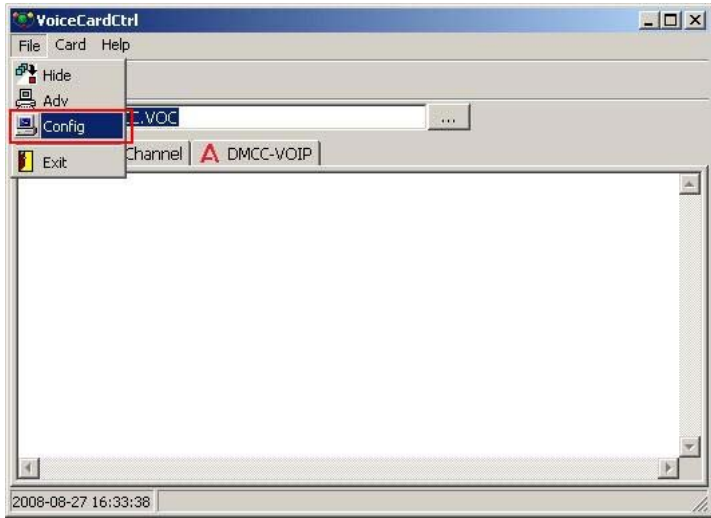
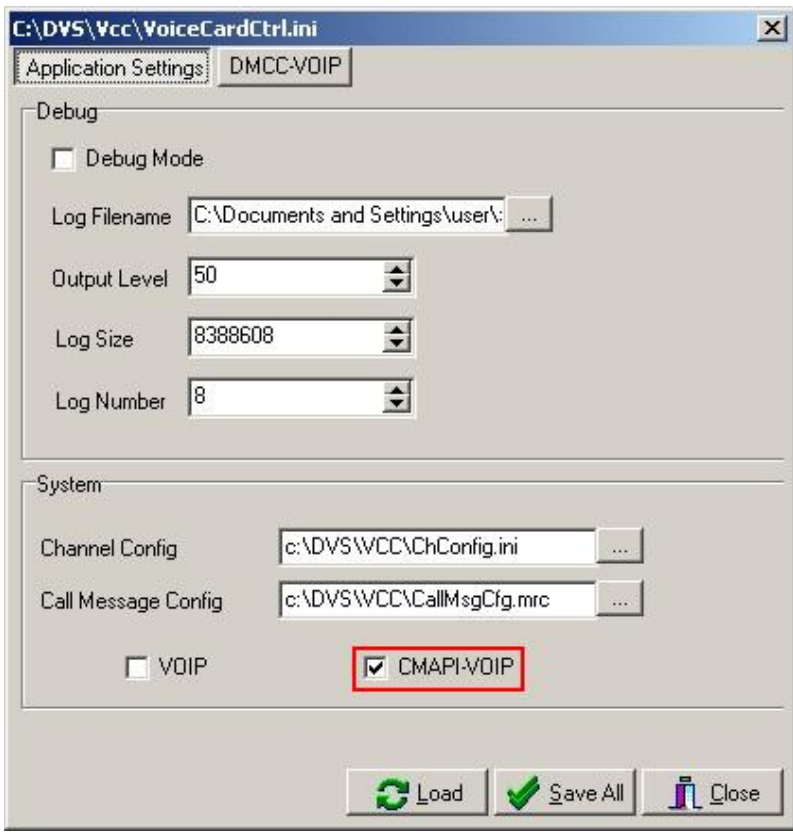
Step	Description
5.	<p>From the Add New Device window, enter the extensions configured in <b>Step 4</b> for <b>Tel Number</b>. Assign the corresponding DMCC stations to be used in <b>DMCC Number</b>. In this configuration, DMCC stations 19901 to 19903 are used. Click <b>OK</b>.</p> 
6.	<p>Click  (Save device configuration) to save the changes.</p> 

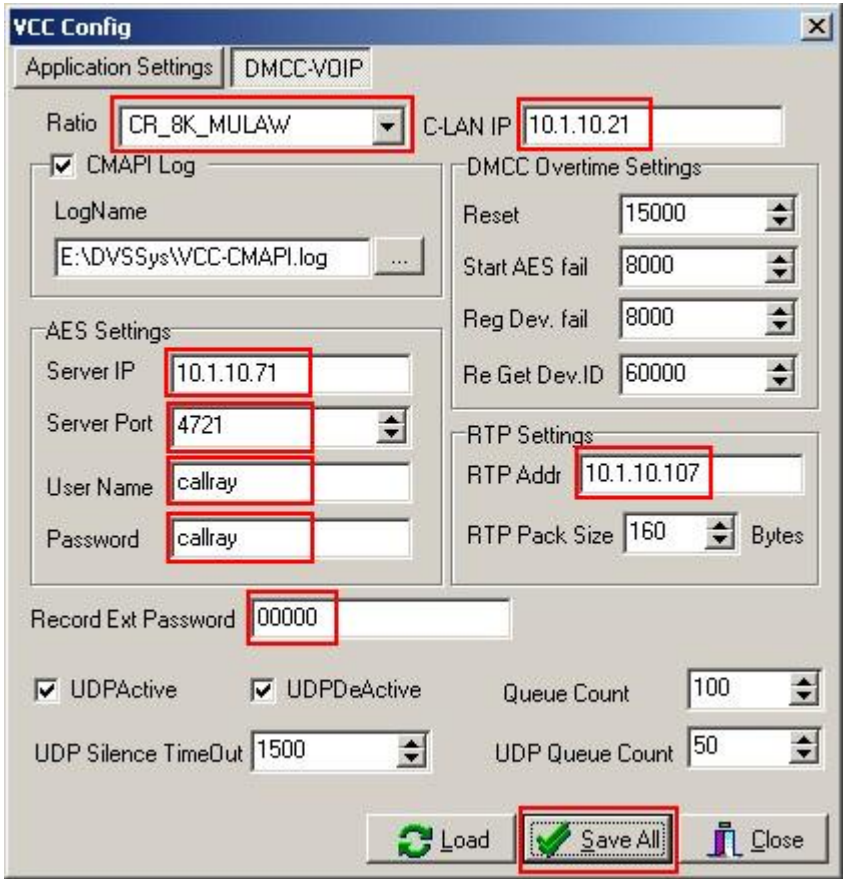


Step	Description
7.	<p>Select <b>Devices &gt; ACD</b> on the left pane to configure the Hunt Group extensions that Callray AP Suite monitors for agents logging in / out of the ACD. Click  (Add a new device).</p> 
8.	<p>From the Add New Device window, enter the Hunt Group extensions to be monitored for <b>Tel Number</b> and check <b>Enable Monitor</b>. In this configuration, agents logged into two Hunt Groups with group extensions 13001 and 13002. Click <b>OK</b>.</p> 

Step	Description
9.	<p>Click  (Save device configuration) to save the changes. Then, click <b>Submit Config Change</b> to close the TCM Config View window and complete the configuration</p> 
10.	<p>Click <b>Start &gt; Run</b>. Browse to the <b>C:\DVS\VCC\</b> folder and select the file <b>ChConfig.exe</b>. Click <b>OK</b> to launch it (not shown). From the Channel Config window, set <b>Count</b> to the number of extensions to be recorded configured in <b>Step 4</b> and click <b>Set</b>.</p> 

Step	Description
11.	<p>To configure the channels with the right values, set the <b>CardType</b> to <b>CT_CMVoIP</b> and check <b>Enable</b>. Set <b>Extension</b> to the first extension to be recorded and <b>Rec Ext</b> to the first DMCC station. These values correspond to those configured in <b>Step 5</b>. Click <b>Set</b>. Then click <b>Save</b> and save the configuration to the file <b>ChConfig.ini</b> in the <b>C:\DVS\VCC\</b> folder (not shown).</p> 
12.	<p>Click <b>Start &gt; Run</b>. Browse to the <b>C:\DVS\VCC\</b> folder and select the file <b>VoiceCardCtrl.exe</b>. Click <b>OK</b> to launch it (not shown). Click on the icon  in the Taskbar to open the VoiceCardCtrl window. To reveal the <b>Config</b> option, click on <b>File &gt; Adv</b> and enter the correct password (not shown).</p> 

Step	Description
13.	<p>Click on <b>File &gt; Config</b> to continue.</p> 
14.	<p>Click on <b>Application Settings</b> and check <b>CMAPI-VOIP</b>.</p> 

Step	Description
15.	<p>Click on <b>DMCC-VOIP</b> tab. Configure the parameters required by Callray AP Suite for DMCC as follows:</p> <ul style="list-style-type: none"> <li>• <b>Ratio:</b> Set to <b>CR_8K_MULAW</b> to correspond to the Codec settings configured on Avaya Communication Manager in <b>Section 3.3</b>.</li> <li>• <b>C-LAN IP:</b> IP address of the CLAN configured in <b>Section 3.1 Step 3</b> for the DMCC stations to register to Avaya Communication Manager.</li> <li>• <b>Server IP:</b> IP address of the AES server.</li> <li>• <b>Server Port:</b> Set to 4721 for the DMCC Unencrypted Port. See <b>Section 4.6</b>.</li> <li>• <b>User Name:</b> Enter the value for <b>User Id</b> configured in <b>Section 4.1 Step 2</b>.</li> <li>• <b>Password:</b> Enter the value for <b>User Password</b> configured in <b>Section 4.1 Step 2</b>.</li> <li>• <b>Record Ext Password:</b> Use the Security Code configured in <b>Section 3.2 Step 2</b>.</li> <li>• <b>RTP Addr:</b> IP address of Callray AP Suite.</li> </ul> <p>Consult [3] for the explanation of other parameters. Click <b>Save All</b>.</p> 

## 6. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of Callray AP Suite to monitor and record calls placed to and from stations and agents. The serviceability testing introduced failure scenarios to see if Callray AP Suite can resume recording after failure recovery.

### 6.1. General Test Approach

The general approach was to place various types of calls to and from stations, agents, and Vector Directory Numbers (VDNs), monitor and record them using Callray AP Suite, and verify the recordings. Some of the recorded calls included both the voice conversation and agent PC screen capture. For feature testing, the types of calls included internal calls, inbound and outbound trunk calls, transferred calls, and conferenced calls. For serviceability testing, failures such as disconnecting the LAN cable to the Callray AP Suite Server and Avaya AES Server, and resetting the Callray AP Suite Server and Avaya Communication Manager were applied.

### 6.2. Test Results

All test cases were executed and passed.

## 7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Application Enablement Services and Callray AP Suite.

### 7.1. Verify Avaya Communication Manager

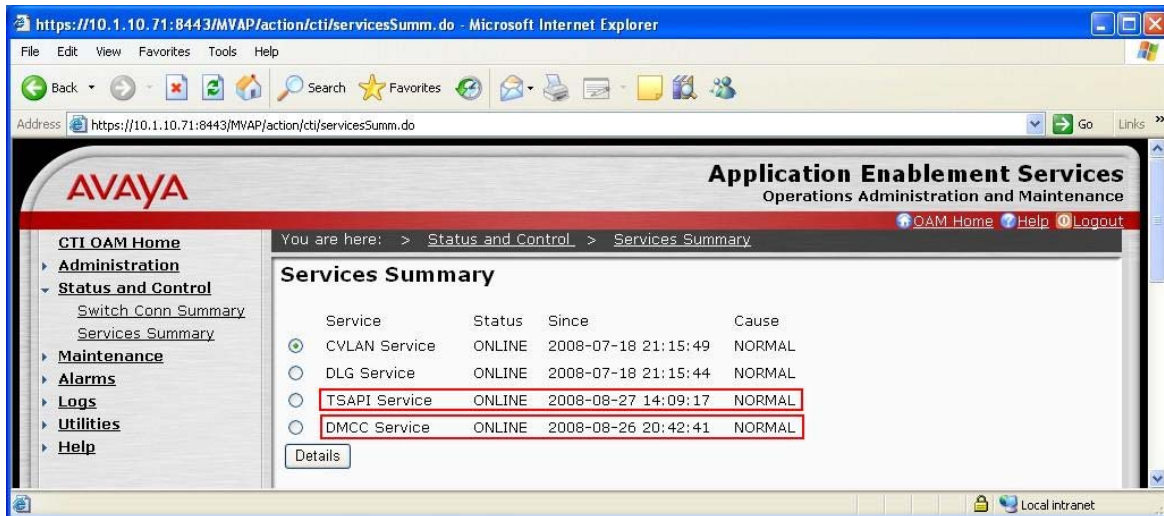
Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command. The **Service State** field should display **established**.

<b>status aesvcs cti-link</b>						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	5	no	aes1	established	47	53

### 7.2. Verify Avaya Application Enablement Services

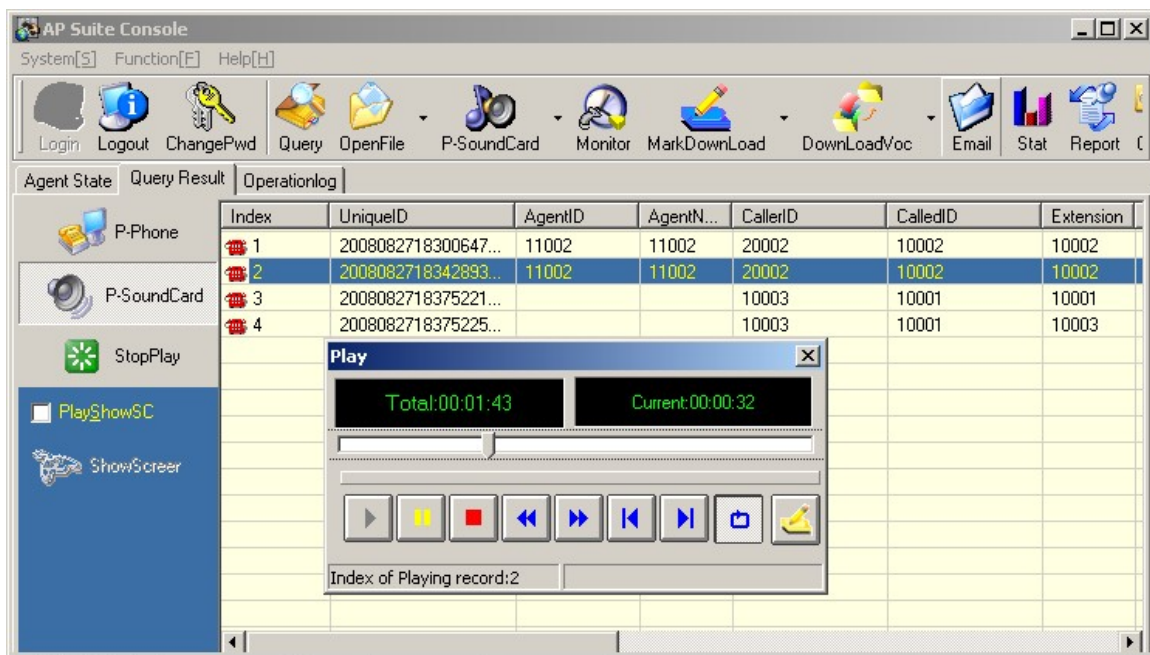
From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services by selecting **Status and Control > Services Summary** from the left pane. The **Status** field for both **TSAPI Service** and **DMCC Service** should display **ONLINE**.





### 7.3. Verify Callray AP Suite

Place a test call to an extension being recorded and hang up after 10 seconds. From the Callray AP Suite Server, launch the AP Suite Console application. Query for the recording of the test call. Verify that the recording is played back correctly and the call information is accurate.



## 8. Support

For technical support on Callray AP Suite, contact Callray Communications at:

- Phone: + 86-755-26649500 Extension 219
- Email: [service@callray.com.cn](mailto:service@callray.com.cn)

## 9. Conclusion

These Application Notes illustrate the procedures for configuring Callray Communications AP Suite Quality Management System to monitor and record calls placed to and from stations and VDNs on an Avaya Communication Manager system. In the configuration described in these Application Notes, Callray AP Suite uses the TSAPI and DMCC Services of Avaya Application Enablement Services to perform recording. All test cases were completed successfully.

## 10. Additional References

This section references the Avaya and Callray documentation that is relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide*, Release 4.1, Document ID 02-300357, Issue 9, February 2008.

[2] *Feature Description and Implementation for Avaya Communication Manager*, Issue 5, February 2007, Document Number 555-245-205.

The following product documentation is available from Callray Communications.

[3] *AP Suite – DVS Installation and Maintenance Guide (Avaya DMCC IP Recording Solution)*

[4] *AP Suite – TCMOne Operations Guide*



---

**©2008 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).