



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

---

# **Application Notes for TeleApps Admin Assist with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0**

### **Abstract**

These Application Notes describe the procedures for configuring TeleApps Admin Assist to integrate with Avaya Communication Manager and Avaya Application Enablement Services. TeleApps Admin Assist is a web-based application that assists enterprise and call center administrators in managing their users.

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.

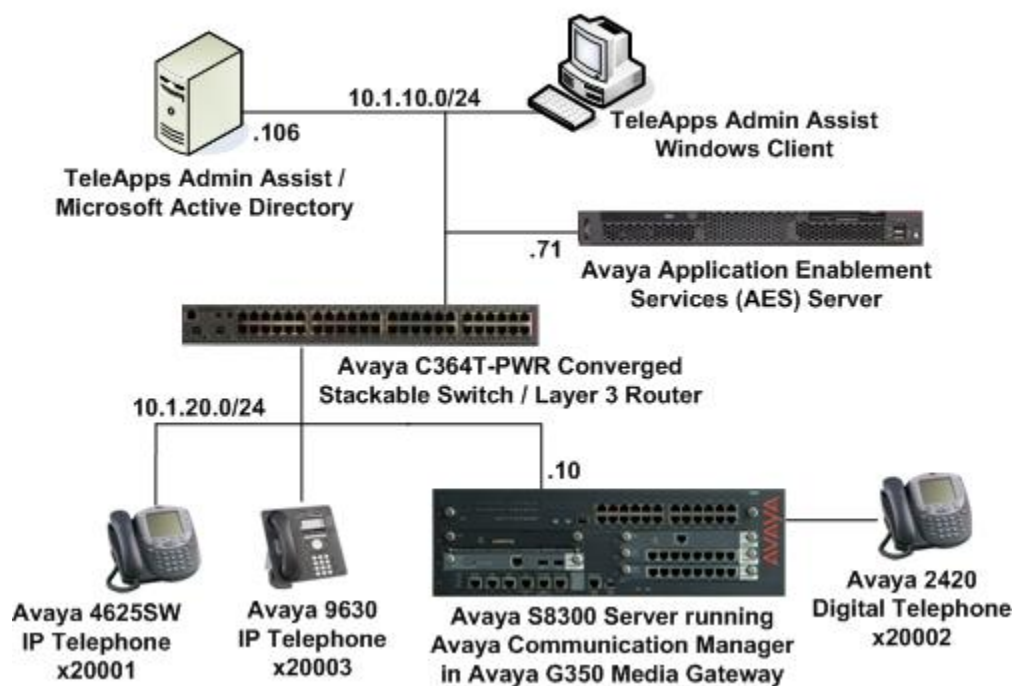
# 1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya Communication Manager, Avaya Application Enablement Services (AES) and TeleApps Admin Assist.

TeleApps Admin Assist is a web-based application that assists enterprise and call center administrators in managing their users. There are two modules in Admin Assist. The first module, PABX Administration, is useful for administrators who are responsible for managing enterprise and call center users of an organization. The second module, Call Center Administration, allows call center supervisors to change their agents' states from their PC.

TeleApps Admin Assist communicates with Avaya AES using the System Management Service (SMS) for PABX Administration and Telephony Services Application Programming Interface (TSAPI) for Call Center Administration. Both SMS and TSAPI Services are provided by the Avaya AES Server.

**Figure 1** illustrates a sample configuration consisting of an Avaya S8300 Server, an Avaya G350 Media Gateway, an Avaya AES Server, Avaya IP and Digital Telephones and Microsoft Windows 2003 Server running TeleApps Admin Assist Server software. A PC was also installed with the TeleApps Admin Assist Client which functions the same way as the web-based Call Center Administration module. An Avaya C364T-PWR Converged Stackable Switch provides network connectivity to all the servers and IP telephones.



**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 S8300 Server	Avaya Communication Manager 5.1.1 (R015x.01.1.415.1) with Service Pack 1 (01.1.415.1-16402)
Avaya G350 Media Gateway - MM712AP DCP Media Module	28.19.0 HW04, FW009
Avaya Application Enablement Services	4.2.1 with Patch 1 (r4-2-1-20-5-0)
Avaya 4625SW IP Telephone	2.9 (H.323)
Avaya 9630 IP Telephone	2.0 (H.323)
Avaya 2420 Series Digital Telephone	-
Avaya C364T-PWR Converged Stackable Switch	4.5.18
TeleApps Admin Assist	1.0
Microsoft Windows Server 2003 Standard Edition	Service Pack 2

## 3. Configure Avaya Communication Manager

This section provides the procedures for configuring the Computer Telephony Integration (CTI) links 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 TeleApps Admin Assist 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 TeleApps Admin Assist. 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
	<div>display system-parameters customer-options<div>Page3 of 11</div></div> <div>OPTIONAL FEATURES</div> <div><div>Abbreviated Dialing Enhanced List? nAudible Message Waiting? n</div><div>Access Security Gateway (ASG)? nAuthorization Codes? y</div><div>Analog Trunk Incoming Call ID? nBackup Cluster Automatic Takeover? n</div><div>A/D Grp/Sys List Dialing Start at 01? nCAS Branch? n</div><div>Answer Supervision by Call Classifier? nCAS Main? n</div><div>ARS? yChange COR by FAC? n</div><div>ARS/AAR Partitioning? yComputer Telephony Adjunct Links? y</div><div>ARS/AAR Dialing without FAC? nCvg Of Calls Redirected Off-net? n</div><div>ASAI Link Core Capabilities? nDCS (Basic)? n</div><div>ASAI Link Plus Capabilities? nDCS Call Coverage? n</div><div>Async. Transfer Mode (ATM) PNC? nDCS with Rerouting? n</div><div>Async. Transfer Mode (ATM) Trunking? n</div><div>ATM WAN Spare Processor? nDigital Loss Plan Modification? n</div><div>ATMS? nDS1 MSP? n</div><div>Attendant Vectoring? nDS1 Echo Cancellation? n</div></div>
2.	<div><div>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.</div><div>add cti-link 1<div>Page1 of 3</div></div><div>CTI LINK</div><div><div>CTI Link: 1</div><div>Extension: 29901</div><div>Type: ADJ-IP</div><div>Name: TSAPI Svcs</div><div>COR: 1</div></div></div>
3.	<div><div>Enter the <b>change node-names ip</b> command. In the compliance-tested configuration, the IP address of the S8300 Server (shown as <b>procr</b>) was utilized for connectivity to Avaya AES.</div><div>change node-names ip<div>Page1 of 2</div></div><div>IP NODE NAMES</div><div><div>NameIP Address</div><div>default0.0.0.0</div><div>procr10.1.20.10</div></div></div>
4.	<div><div>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 contain the node-name <b>procr</b> as shown in <b>Step 3</b>. During the compliance test, the default port was utilized for the <b>Local Port</b> field.</div><div>change ip-services<div>Page1 of 4</div></div><div>IP SERVICES</div><div><div>ServiceEnabledLocalLocalRemoteRemote</div><div>TypeTypeNodeNodeNodePort</div><div>AESVCSyprocr8765</div></div></div>

Step	Description																				
	<p>On Page 4, 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>Page4 of 4</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:																					

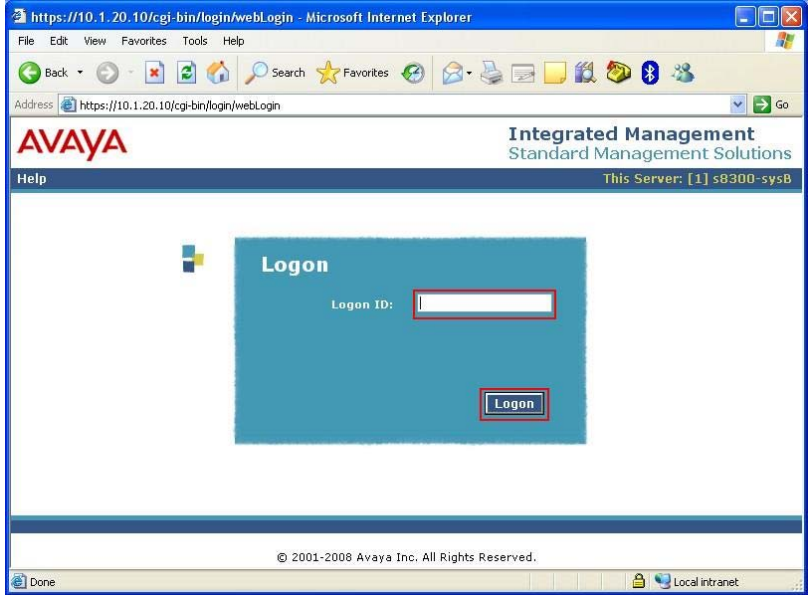
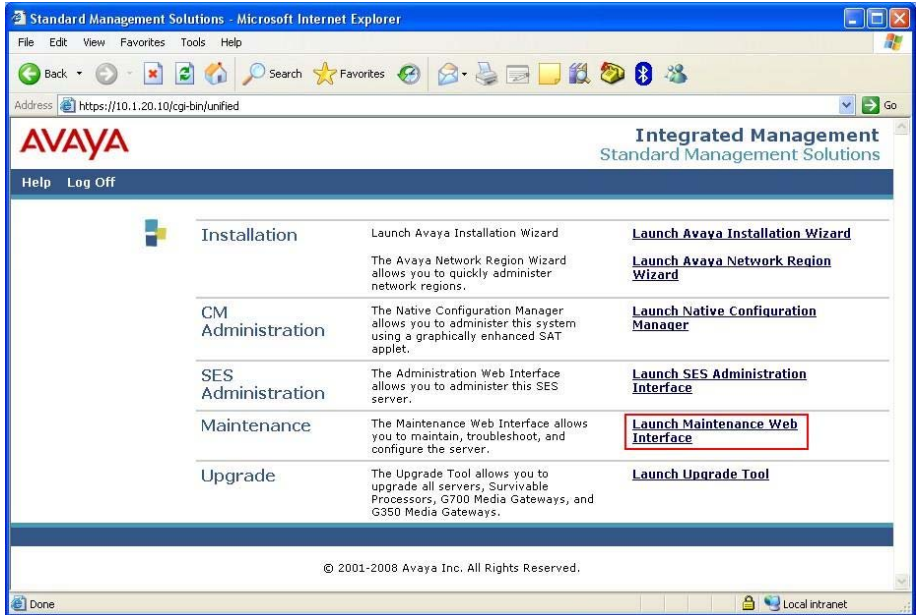
### 3.2. Configure SAT User Profile

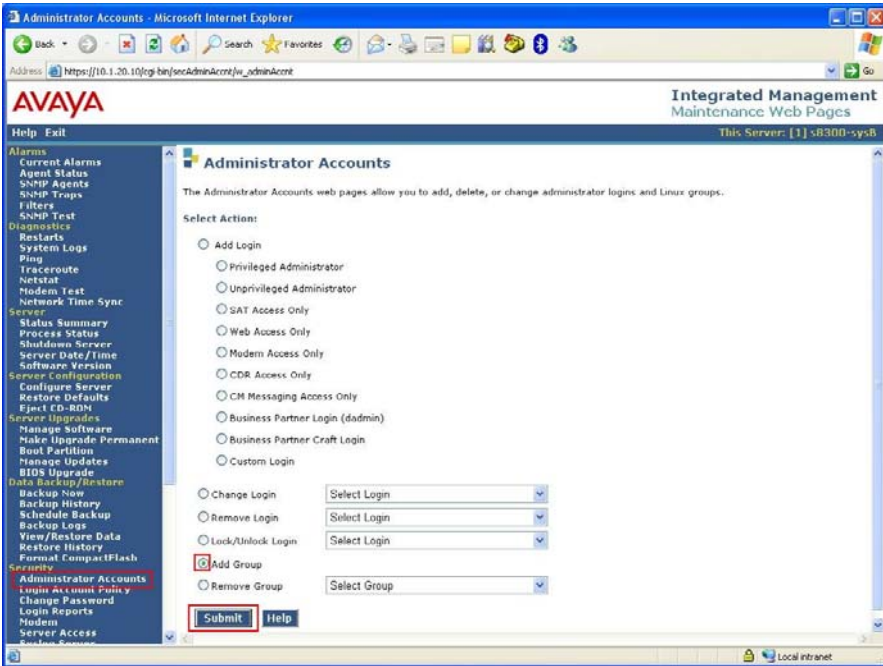
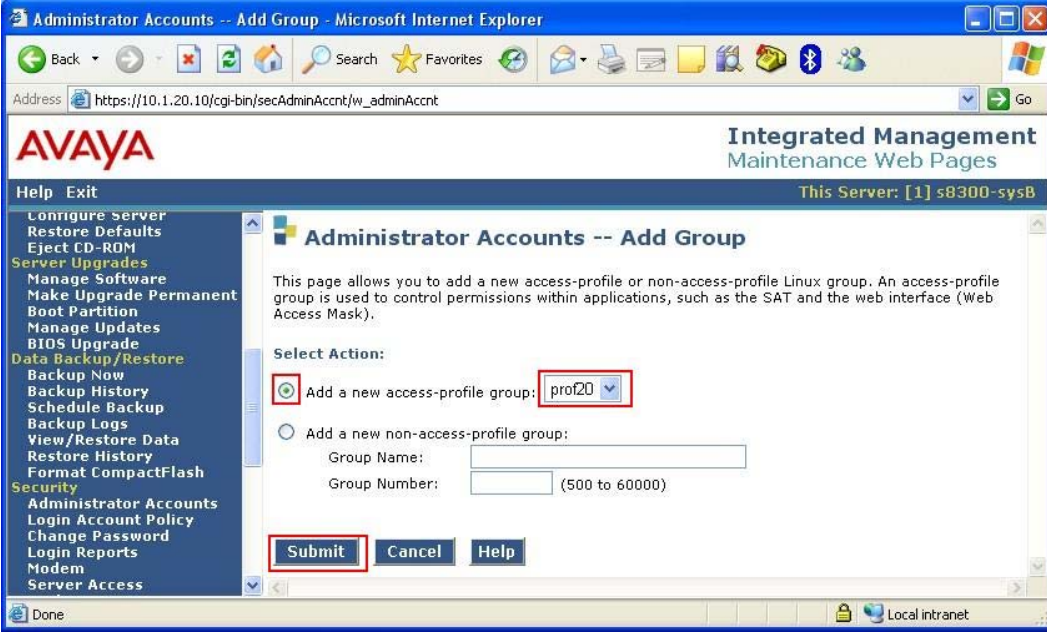
A SAT User Profile specifies which SAT screens may be accessed by the user assigned with the profile and the type of access to each screen. TeleApps Admin Assist logs in to the SAT using the SMS Service to modify station records. Thus, a SAT User Profile with the required permissions is created and assigned to the Admin Assist login account.

Step	Description																																																												
1.	<p>Enter the <b>add user-profile <i>n</i></b> command, where <b><i>n</i></b> is the next unused profile number. Enter a descriptive name for <b>User Profile Name</b> and enable only the category <b>Stations M</b> by setting the <b>Enbl</b> field to <b>y</b>. In this configuration, the user profile 20 is created.</p>																																																												
	<div><div>add user-profile 20</div><div>USER PROFILE 20</div><div>Page 1 of 41</div></div> <p>User Profile Name: <b>Teleapps AdminAssist</b></p> <div><div><div>This Profile is Disabled? n</div><div>Facility Test Call Notification? n</div><div>Grant Un-owned Permissions? n</div></div><div><div>Shell Access? n</div><div>Acknowledgement Required? n</div><div>Extended Profile? n</div></div></div> <table><tr><th>Name</th><th>Cat</th><th>Enbl</th><th>Name</th><th>Cat</th><th>Enbl</th></tr><tr><td>Adjuncts</td><td>A</td><td>n</td><td>Routing and Dial Plan</td><td>J</td><td>n</td></tr><tr><td>Call Center</td><td>B</td><td>n</td><td>Security</td><td>K</td><td>n</td></tr><tr><td>Features</td><td>C</td><td>n</td><td>Servers</td><td>L</td><td>n</td></tr><tr><td>Hardware</td><td>D</td><td>n</td><td>Stations</td><td>M</td><td>y</td></tr><tr><td>Hospitality</td><td>E</td><td>n</td><td>System Parameters</td><td>N</td><td>n</td></tr><tr><td>IP</td><td>F</td><td>n</td><td>Translations</td><td>O</td><td>n</td></tr><tr><td>Maintenance</td><td>G</td><td>n</td><td>Trunking</td><td>P</td><td>n</td></tr><tr><td>Measurements and Performance</td><td>H</td><td>n</td><td>Usage</td><td>Q</td><td>n</td></tr><tr><td>Remote Access</td><td>I</td><td>n</td><td>User Access</td><td>R</td><td>n</td></tr></table>	Name	Cat	Enbl	Name	Cat	Enbl	Adjuncts	A	n	Routing and Dial Plan	J	n	Call Center	B	n	Security	K	n	Features	C	n	Servers	L	n	Hardware	D	n	Stations	M	y	Hospitality	E	n	System Parameters	N	n	IP	F	n	Translations	O	n	Maintenance	G	n	Trunking	P	n	Measurements and Performance	H	n	Usage	Q	n	Remote Access	I	n	User Access	R	n
Name	Cat	Enbl	Name	Cat	Enbl																																																								
Adjuncts	A	n	Routing and Dial Plan	J	n																																																								
Call Center	B	n	Security	K	n																																																								
Features	C	n	Servers	L	n																																																								
Hardware	D	n	Stations	M	y																																																								
Hospitality	E	n	System Parameters	N	n																																																								
IP	F	n	Translations	O	n																																																								
Maintenance	G	n	Trunking	P	n																																																								
Measurements and Performance	H	n	Usage	Q	n																																																								
Remote Access	I	n	User Access	R	n																																																								

### 3.3. Configure Login Group

Create an Access-Profile Group to correspond to the SAT User Profile created in **Section 3.2**.

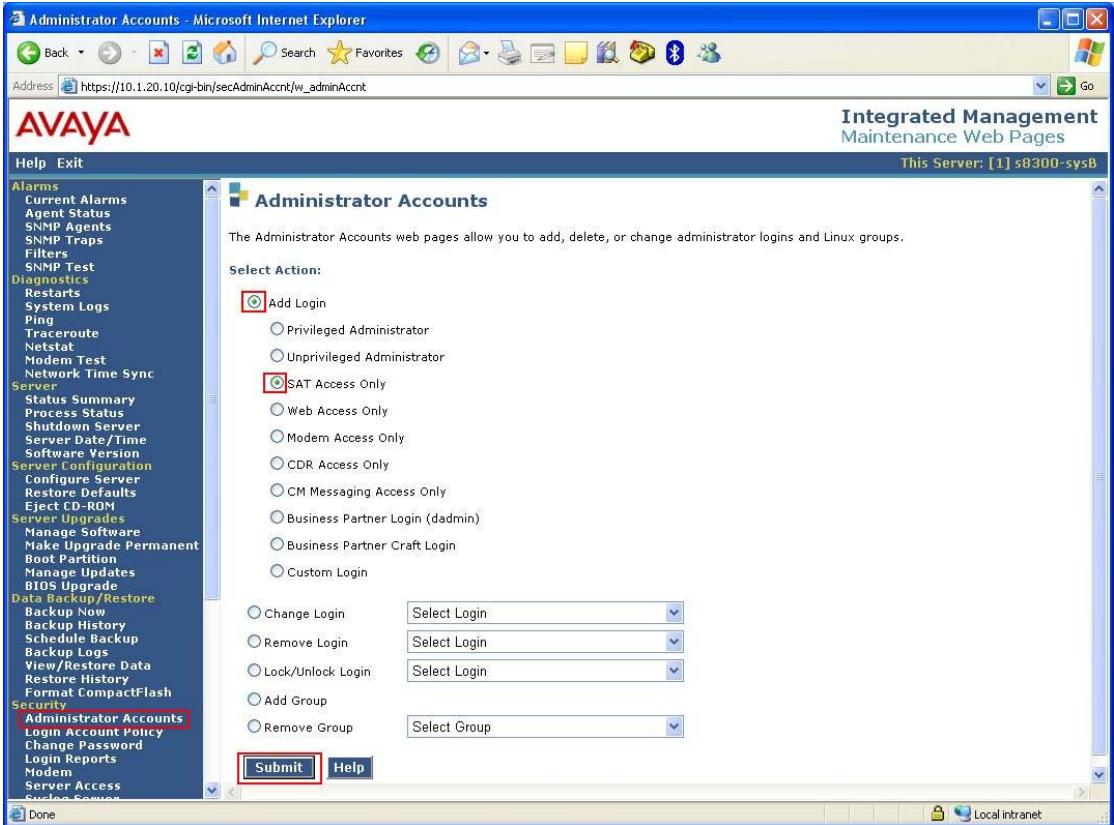
Step	Description
1.	<p>Using a web browser, enter <b>https://&lt;IP address of Avaya Server&gt;</b> to connect to the Avaya Server being configured and log in using appropriate credentials.</p> 
2.	<p>Click <b>Launch Maintenance Web Interface</b>. This will open up the <b>Maintenance Web Pages</b> in a new window that will allow the user to complete the configuration process.</p> 

Step	Description
3.	<p>From the navigation panel on the left side, click <b>Administrator Accounts</b>. Select <b>Add Group</b> and click <b>Submit</b>.</p> 
4.	<p>Select <b>Add a new access-profile group</b> and select <b>prof20</b> from the drop-down box to correspond to the user-profile created in <b>Section 3.2 Step 1</b>. Click <b>Submit</b>. This completes the creation of the login group.</p> 

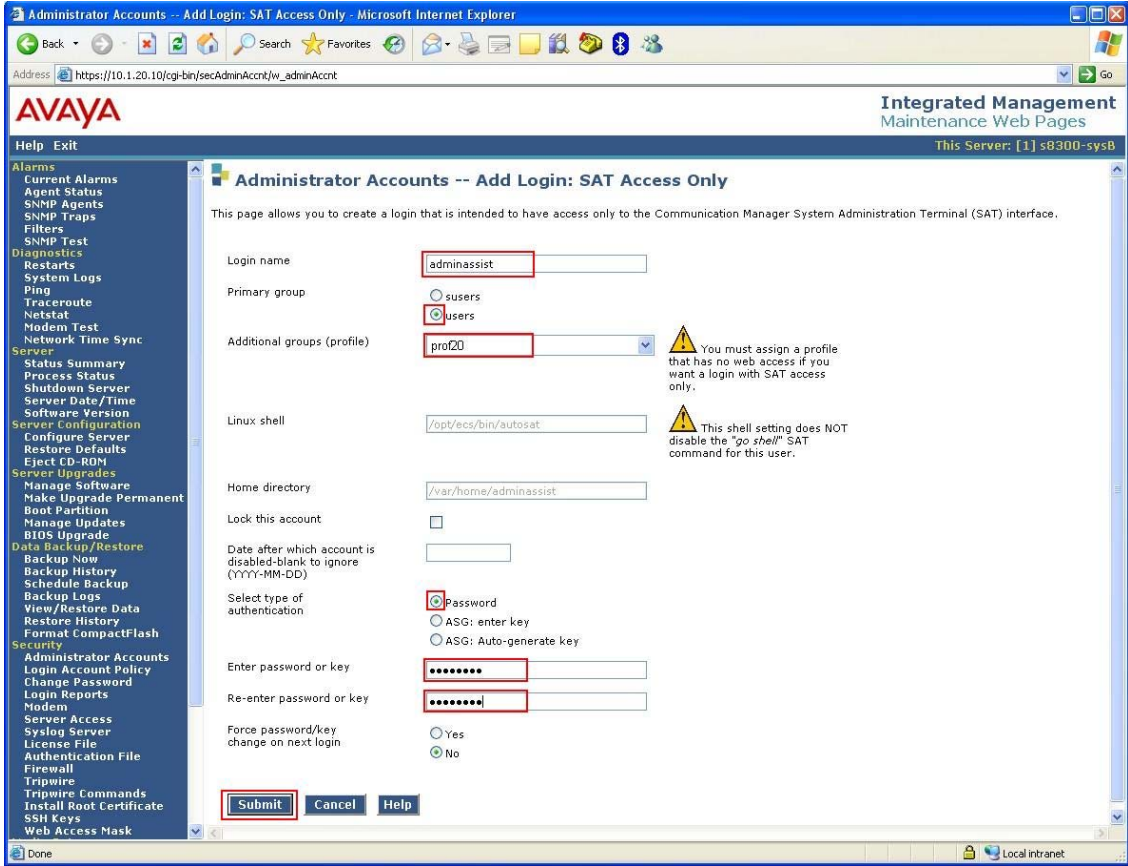


### 3.4. Configure Login

Create a login account for TeleApps Admin Assist to access the SAT using the SMS Service.

Step	Description
1.	<p>From the navigation panel on the left side, click <b>Administrator Accounts</b>. Select <b>Add Login</b> and SAT Access Only to create a new login account with SAT access privileges only. Click <b>Submit</b>.</p> 



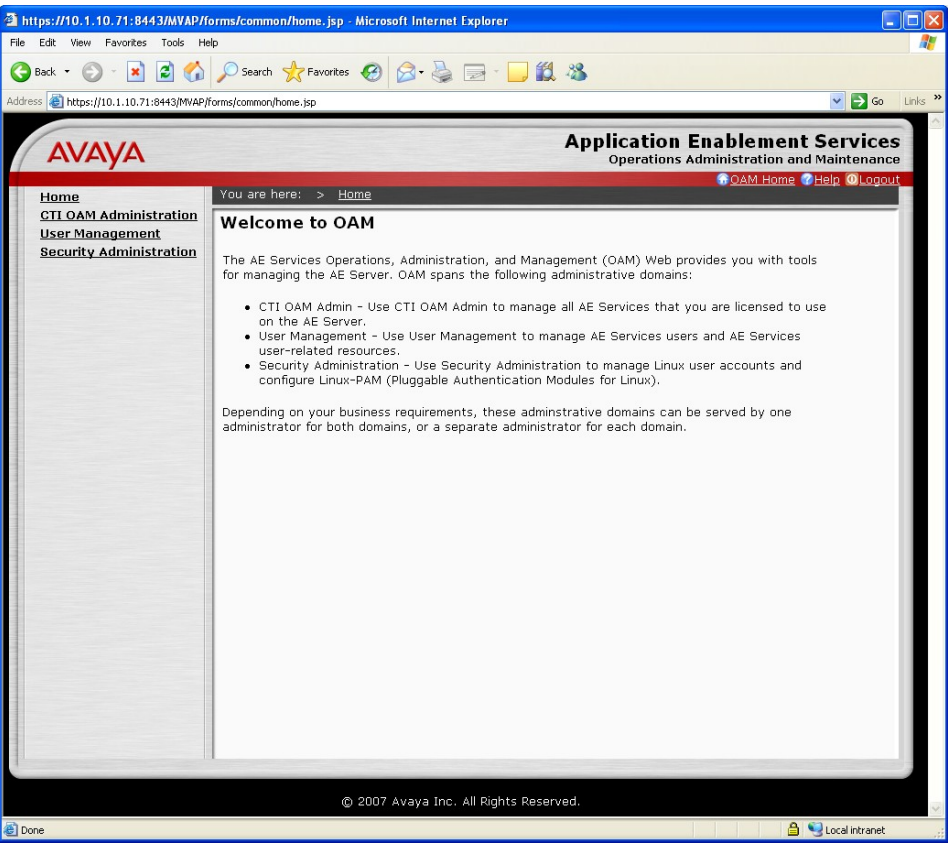
Step	Description
2.	<p>For the field <b>Login name</b>, enter the login to be created. In this configuration, the login <b>adminassist</b> is created. Configure the other parameters for the login as follows:</p> <ul style="list-style-type: none"> <li>• <b>Primary group: users</b> [Limits the permissions of the login]</li> <li>• <b>Additional groups (profile): prof20</b> [Select the login group created in <b>Section 3.3.</b>]</li> <li>• <b>Select type of authentication: Password</b> [Uses a password for authentication.]</li> <li>• <b>Enter password or key / Re-enter password or key</b> [Define the password]</li> </ul> <p>Click <b>Submit</b> to continue. This completes the configuration of the login.</p> 

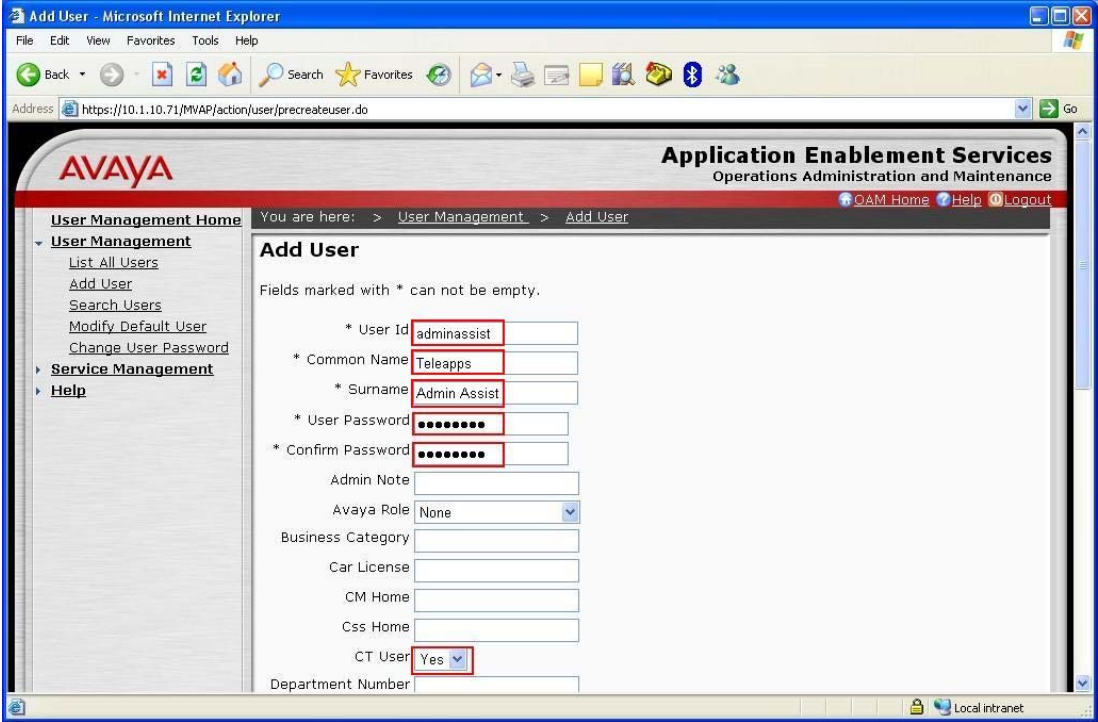
## 4. Configure Avaya Application Enablement Services

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

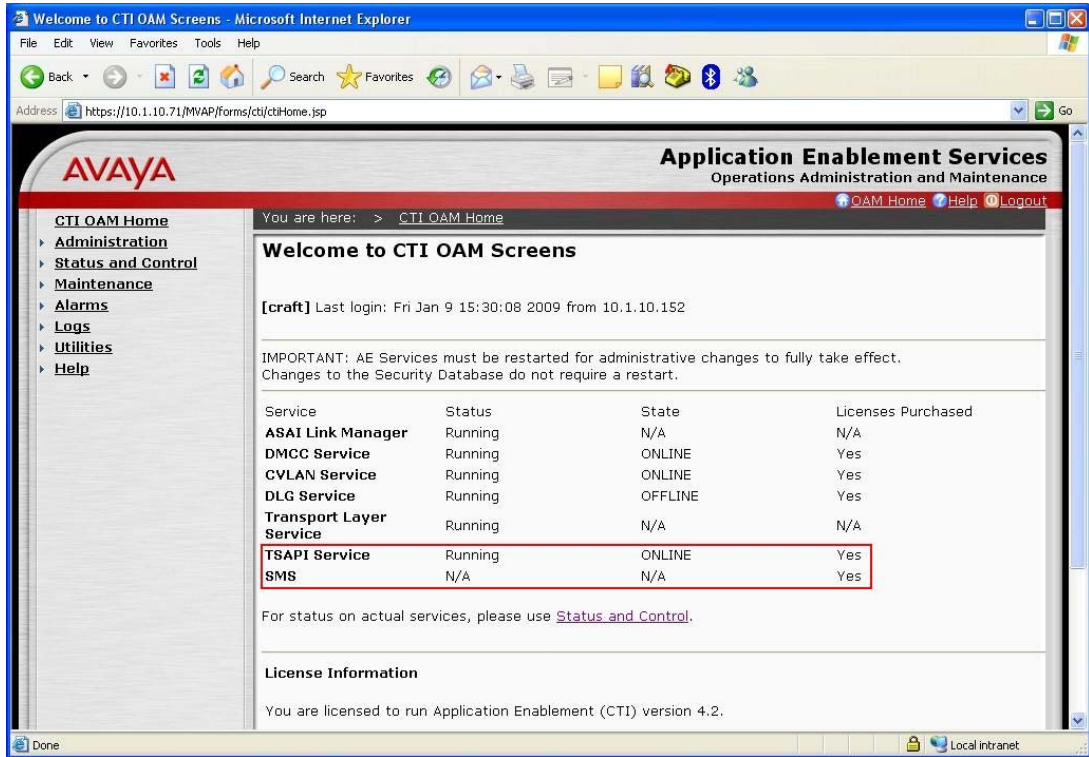
- Administer CTI User
- Verify Avaya Application Enablement Services License
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user permission
- Administer SMS Configuration

### 4.1. Administer CTI User

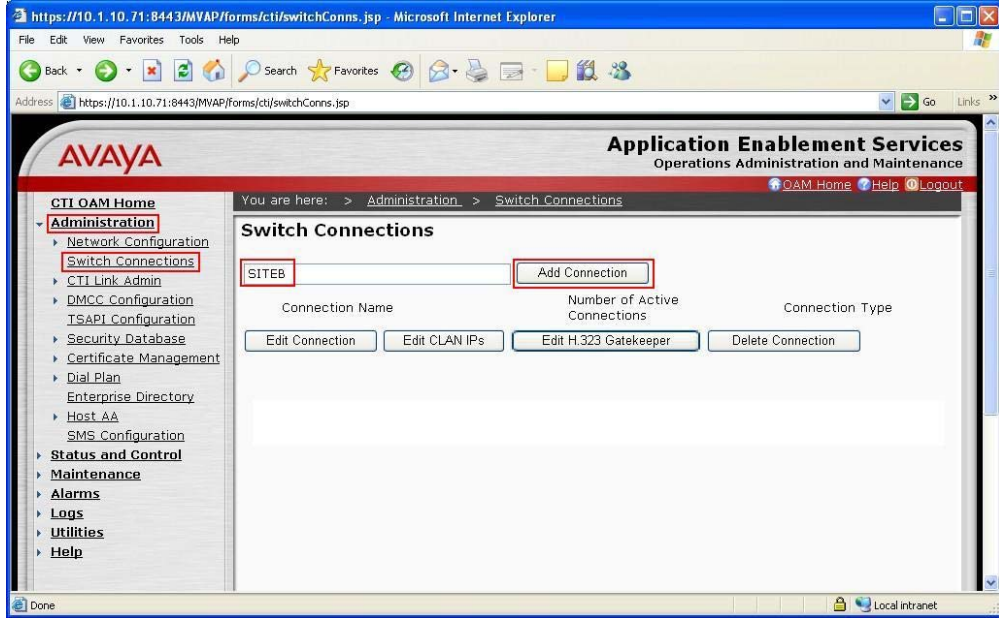
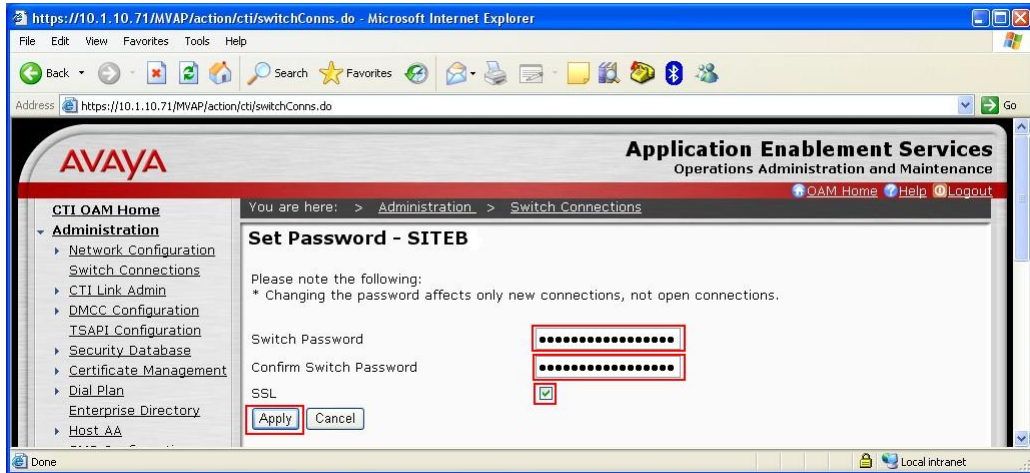
Step	Description
1.	<p>Launch a web browser and enter <b>https://&lt;IP address of AES server&gt;/MVAP/</b> to access the AES OAM web based interface. Log in to AES OAM using an administrative login and password (not shown), and the Welcome To OAM screen will be displayed.</p> 

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 TeleApps Admin Assist in <b>Section 5.2 Step 1</b> to access the TSAPI Service on the AES server. Scroll down to the bottom of the page and click <b>Apply</b> (not shown).</p> 

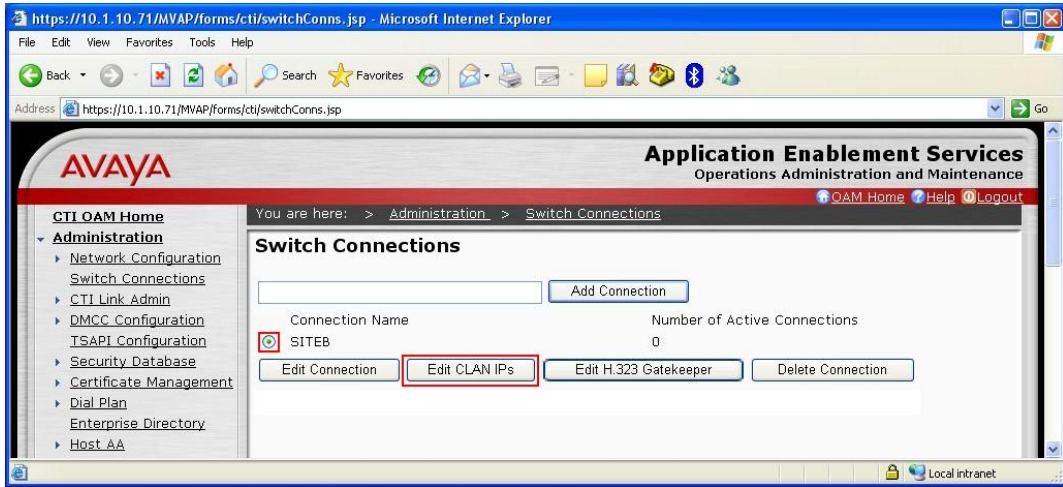
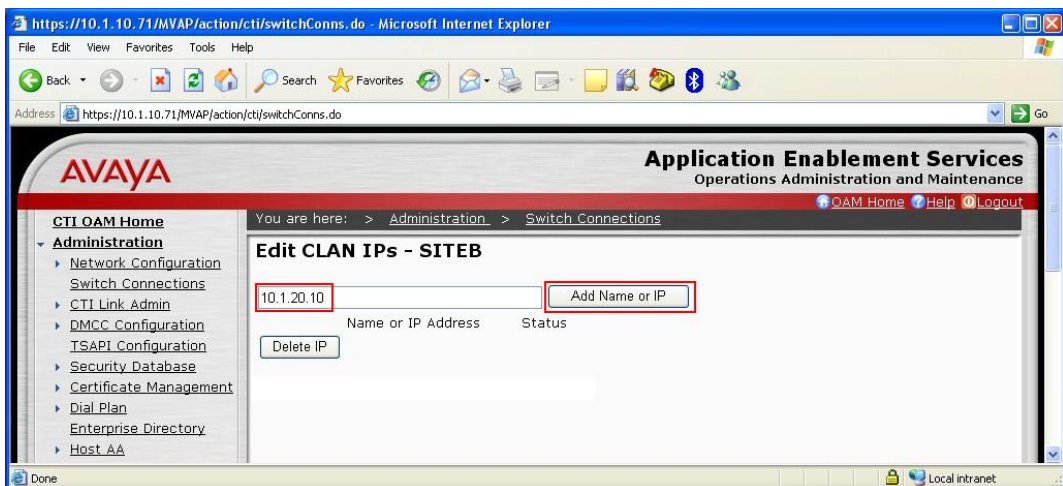
## 4.2. Verify Avaya Application Enablement Services License

Step	Description																																
1.	<p>Select <b>OAM Home</b>, then click on <b>CTI OAM Administration</b> from the left menu (not shown), and the following screen is displayed. Verify that the Avaya Application Enablement Services license has proper permissions for the features illustrated in these Application Notes by ensuring that both TSAPI and SMS services are licensed. If they are not, contact the Avaya sales team or business partner to obtain the required licenses.</p>  <p>The screenshot displays the 'Welcome to CTI OAM Screens' page. On the left is a navigation menu with options: CTI OAM Home, Administration, Status and Control, Maintenance, Alarms, Logs, Utilities, and Help. The main content area shows a welcome message and a table of services. The table has columns: Service, Status, State, and Licenses Purchased. The 'TSAPI Service' and 'SMS' rows are highlighted with a red box, indicating they are licensed. Below the table, there is a note about restarting services and a 'License Information' section stating the user is licensed to run version 4.2.</p> <table><tr><th>Service</th><th>Status</th><th>State</th><th>Licenses Purchased</th></tr><tr><td>ASAI Link Manager</td><td>Running</td><td>N/A</td><td>N/A</td></tr><tr><td>DMCC Service</td><td>Running</td><td>ONLINE</td><td>Yes</td></tr><tr><td>CVLAN Service</td><td>Running</td><td>ONLINE</td><td>Yes</td></tr><tr><td>DLG Service</td><td>Running</td><td>OFFLINE</td><td>Yes</td></tr><tr><td>Transport Layer Service</td><td>Running</td><td>N/A</td><td>N/A</td></tr><tr><td>TSAPI Service</td><td>Running</td><td>ONLINE</td><td>Yes</td></tr><tr><td>SMS</td><td>N/A</td><td>N/A</td><td>Yes</td></tr></table>	Service	Status	State	Licenses Purchased	ASAI Link Manager	Running	N/A	N/A	DMCC Service	Running	ONLINE	Yes	CVLAN Service	Running	ONLINE	Yes	DLG Service	Running	OFFLINE	Yes	Transport Layer Service	Running	N/A	N/A	TSAPI Service	Running	ONLINE	Yes	SMS	N/A	N/A	Yes
Service	Status	State	Licenses Purchased																														
ASAI Link Manager	Running	N/A	N/A																														
DMCC Service	Running	ONLINE	Yes																														
CVLAN Service	Running	ONLINE	Yes																														
DLG Service	Running	OFFLINE	Yes																														
Transport Layer Service	Running	N/A	N/A																														
TSAPI Service	Running	ONLINE	Yes																														
SMS	N/A	N/A	Yes																														

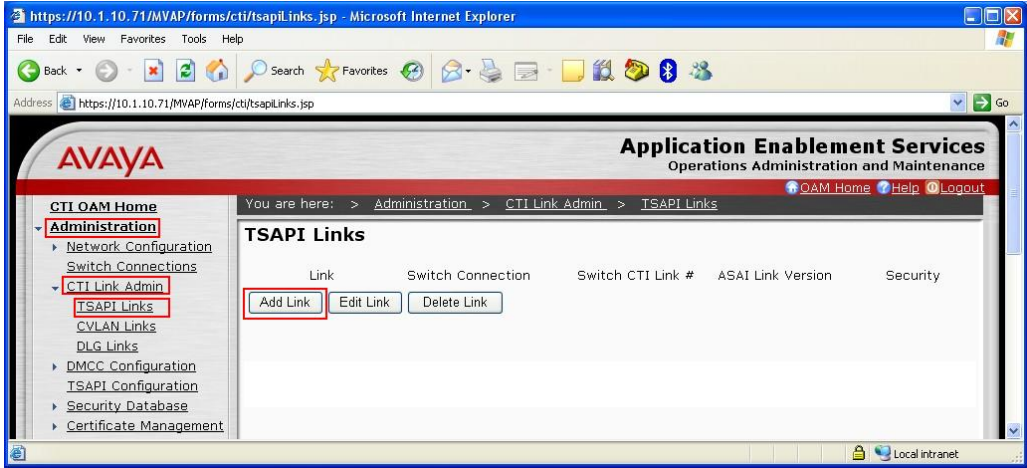
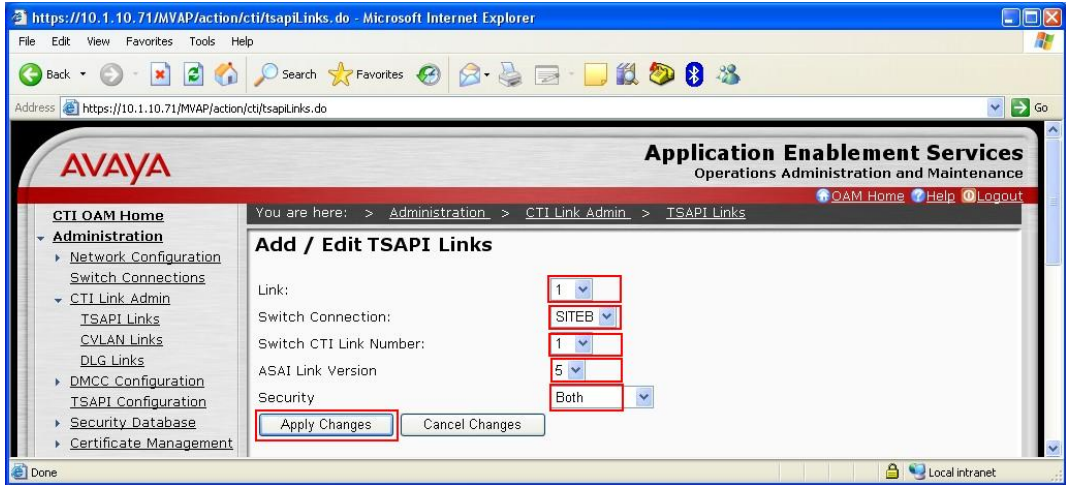
### 4.3. Administer Switch Connection

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>SITEB</b> is used.</p> 
2.	<p>The Set Password screen is displayed. 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 Avaya S8300 Server. Click on <b>Apply</b>.</p> 

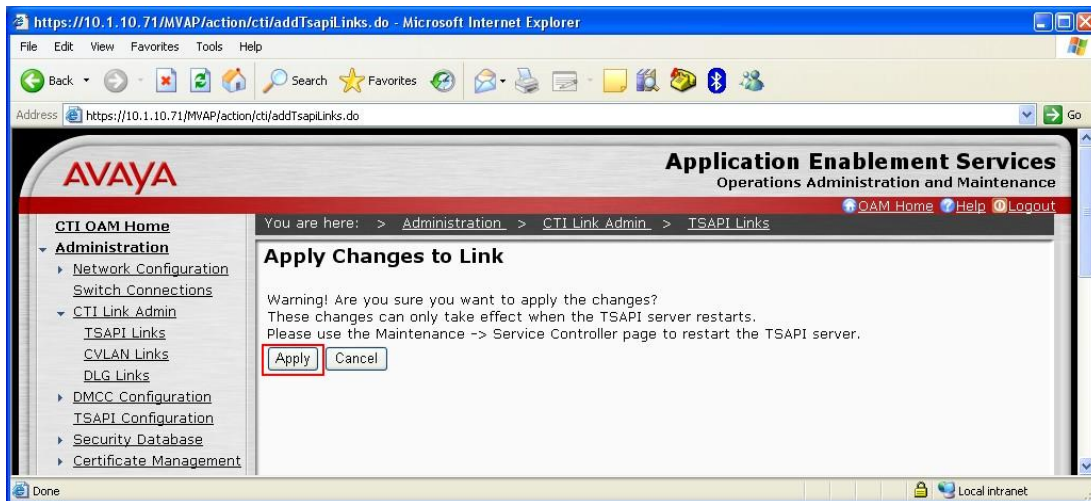
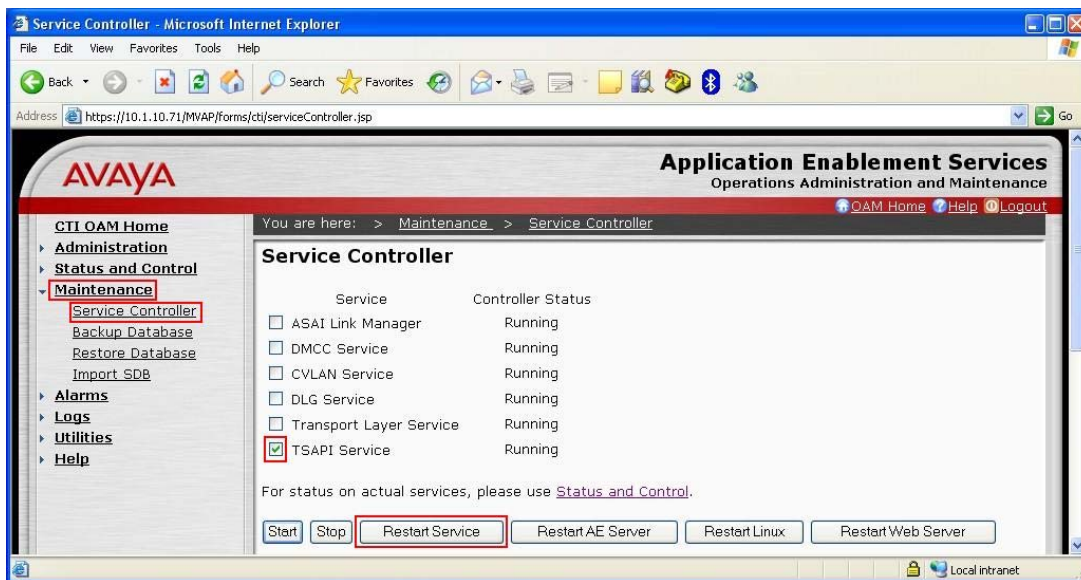



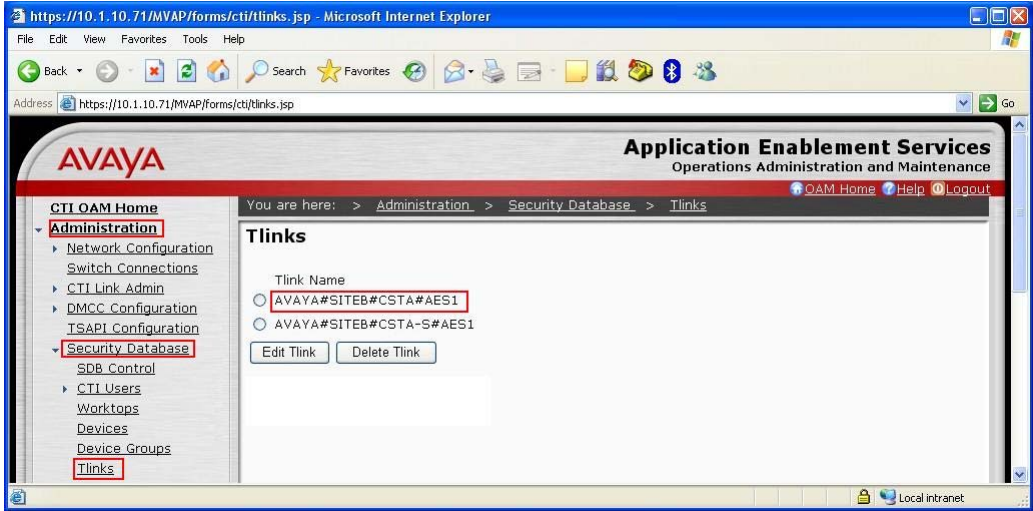
Step	Description
3.	<p>The Switch Connections screen is displayed. Select the newly added switch connection name and click <b>Edit CLAN IPs</b>.</p> 
4.	<p>In the Edit CLAN IPs screen, enter the host name or IP address of the S8300 Server used for AES connectivity, which corresponds to the IP address as shown 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

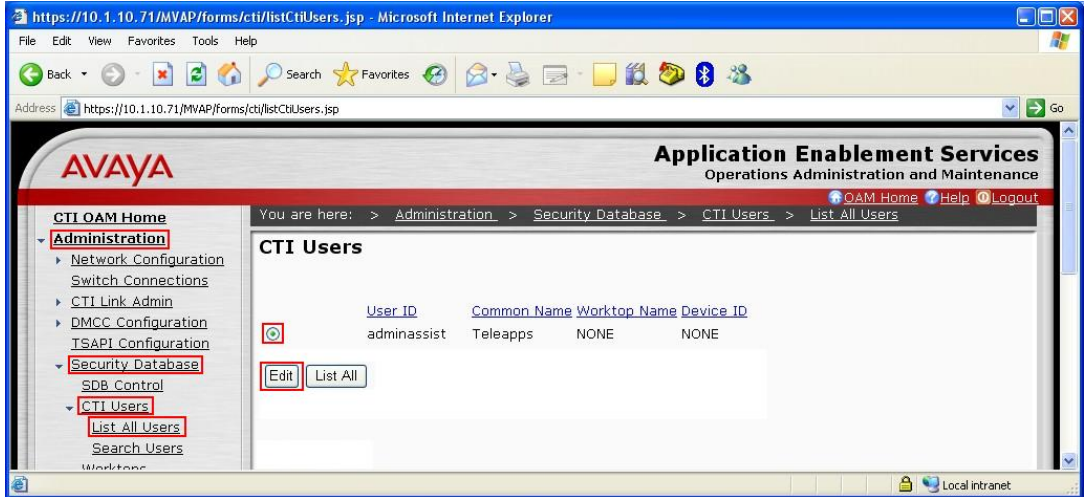
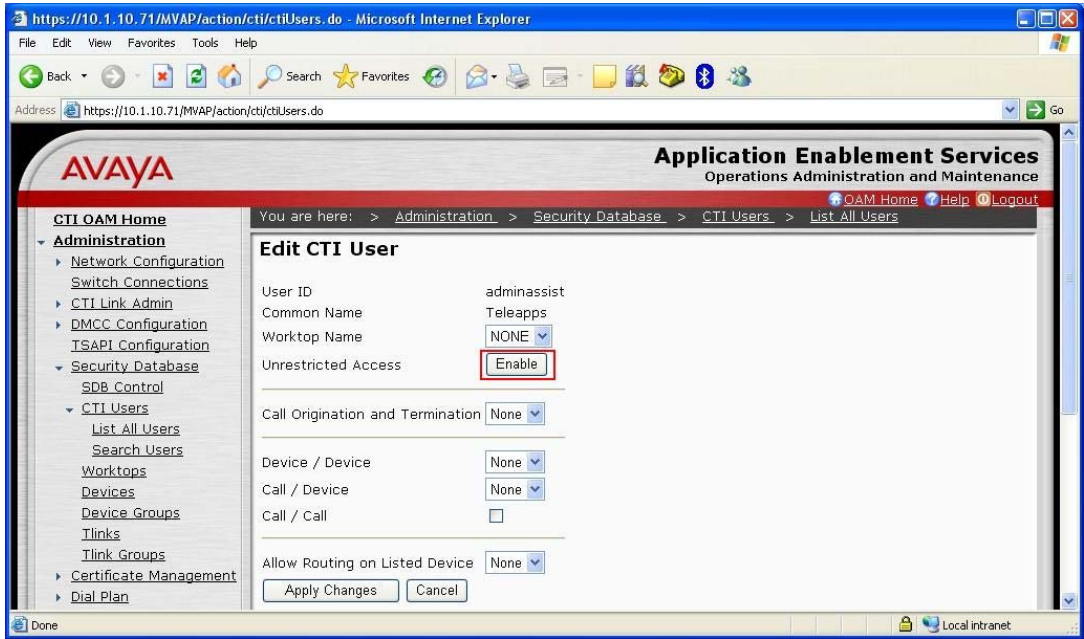
Step	Description
1.	<p>To administer a TSAPI link on AES, select <b>Administration &gt; CTI Link Admin &gt; TSAPI Links</b> from the CTI OAM Home menu. Click <b>Add Link</b>.</p> 
2.	<p>In the Add / Edit TSAPI Links screen, select the following values:</p> <ul style="list-style-type: none"><li>• <b>Link:</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 <b>5</b>.</li><li>• <b>Security:</b> Set to <b>Both</b> to allow both encrypted and unencrypted TSAPI Links.</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 TeleApps Admin Assist Server in <b>Section 5.2 Step 1</b>. In this configuration, the <b>Tlink Name</b> is <b>AVAYA#SITEB#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.	Click <b>Apply</b> to apply the changes.

## 4.6. Administer SMS Configuration

Step	Description
1.	From the CTI OAM Home menu, select <b>Administration &gt; SMS Configuration</b> . Set <b>Default CM Host Address</b> to the IP Address of the S8300 Server, <b>Default CM Admin Port</b> to <b>5022</b> and <b>CM Connection Protocol</b> to <b>SSH</b> . The remaining fields can be left at their default values. Click <b>Apply Changes</b> . These values will be used to configure the TeleApps Admin Assist Server in <b>Section 5.2 Step 1</b> .



## 5. Configure TeleApps Admin Assist

TeleApps installs, configures, and customizes the TeleApps Admin Assist application for their customers. This section only describes the interface configuration required for the TeleApps Admin Assist application to communicate with Avaya AES and Avaya Communication Manager.

Refer to [3] for configuring the TeleApps Admin Assist application.

### 5.1. Install Avaya AES TSAPI Client Software

TeleApps Admin Assist uses the Avaya AES TSAPI Client software to communicate with the TSAPI Service on the AES server. Install the AES TSAPI Client software on both the TeleApps Admin Assist Server and all PCs running the TeleApps Admin Assist Client.

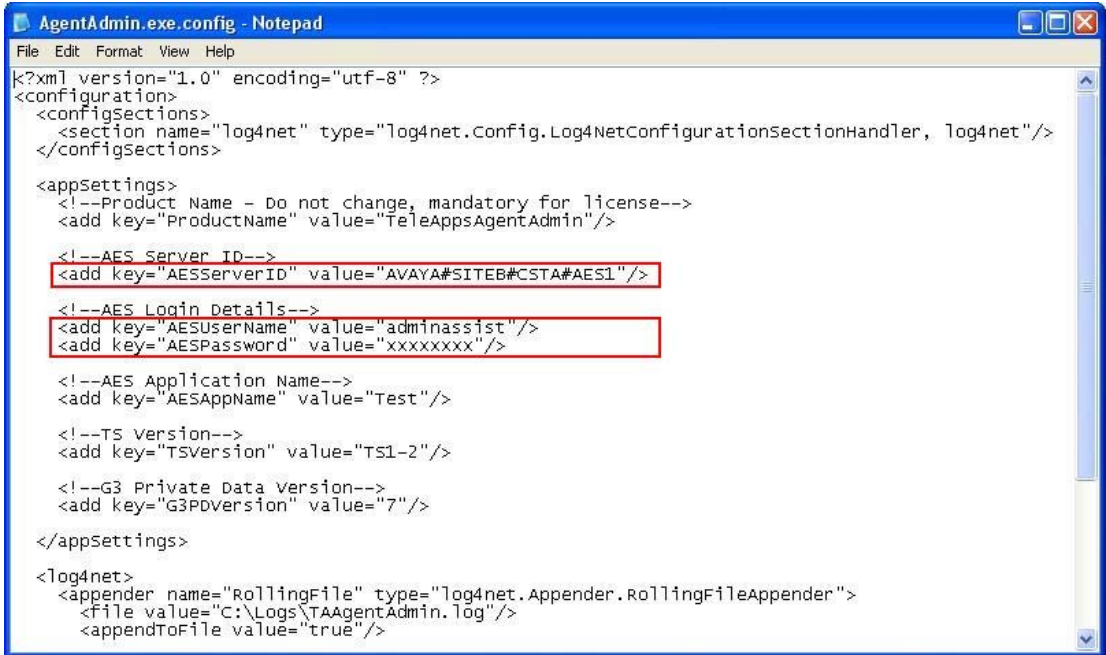
The Avaya AES TSAPI Client software will be provided by TeleApps, or it can also be downloaded from the Avaya Support website (<http://support.avaya.com>).

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 TeleApps Admin Assist

Step	Description
1.	<p>On the TeleApps Admin Assist Server, edit the file <b>web.config</b> located in the <b>C:\Inetpub\wwwroot\TeleAppsAdminAssist\</b> folder using Notepad. In the <b>&lt;appSettings&gt;</b> section, configure the following settings required for the TSAPI and SMS Services:</p> <p><u>TSAPI Service</u></p> <pre>&lt;add key="AESServerID" value="AVAYA#SITEB#CSTA#AES1" /&gt; &lt;add key="AESUserName" value="adminassist" /&gt; &lt;add key="AESPassword" value="Encrypt(xxxxxxxx)" /&gt;</pre> <p>The values are obtained from <b>Section 4.4 Step 6</b> and <b>Section 4.1 Step 2</b> respectively.</p> <p><u>SMS Service</u></p> <pre>&lt;add key="SMSService.SystemManagement" value="http://10.1.10.71/sms/SystemManagementService.php" /&gt; &lt;add key="SMSUserName" value="Encrypt(adminassist@10.1.20.10:5022)" /&gt; &lt;add key="SMSPassword" value="Encrypt(yyyyyyyy)" /&gt;</pre> <p><b>10.1.10.71</b> is the IP address of the AES Server. The other values are obtained from <b>Section 3.4 Step 2</b>.</p> 

Step	Description
2.	<p>On the PC installed with the TeleApps Admin Assist Client, edit the file <b>AgentAdmin.exe.config</b> located in the <b>C:\Program Files\TeleApps\TAAgentAdmin\</b> folder using Notepad. In the &lt;appSettings&gt; section, configure the following settings required for the TSAPI Service:</p> <pre>&lt;add key="AESServerID" value="AVAYA#SITEB#CSTA#AES1" /&gt; &lt;add key="AESUserName" value="adminassist" /&gt; &lt;add key="AESPassword" value="xxxxxxx" /&gt;</pre> <p>The values are obtained from <b>Section 4.4 Step 6</b> and <b>Section 4.1 Step 2</b> respectively. This completes the configuration of TeleApps Admin Assist.</p> 

## 6. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of TeleApps Admin Assist to list, add, modify and delete users and stations from both the Microsoft Active Directory and Avaya Communication Manager. The feature also evaluated the ability of TeleApps Admin Assist to query and change the states of agents. The serviceability testing introduced failure scenarios to see if TeleApps Admin Assist can resume recording after failure recovery.

### 6.1. General Test Approach

The general approach was to add, modify or delete users with different station types, such as Avaya 2400 Series Digital Telephones and 4600 and 9600 Series IP Telephones, and to verify that the stations were added, modified or deleted on Avaya Communication Manager. Agents in different states such as logout, ready, after-call-work (ACW) and aux-work (AUX) were also



verified and changed between the different states using TeleApps Admin Assist. For serviceability testing, failures such as disconnecting the LAN cable to the TeleApps Admin Assist and Avaya AES Server, and resetting the TeleApps Admin Assist Server and Avaya Communication Manager were applied.

## 6.2. Test Results

All test cases were executed and passed. The following observations were noted:

- The fields that are shown are restricted to the ones that are commonly used. In addition, only the values for these fields can be changed. To change the values for other fields, the administrator will need to use the SAT user interface on Avaya Communication Manager.
- The field **User logon name (pre-Windows 2000)** under the **Account** tab in Microsoft Active Directory was not set properly during testing. TeleApps will provide the fix in a future patch.
- The button assignments on the station currently have the following restrictions. TeleApps will provide the enhancement in a future patch.
  - Only the first 6 buttons can be assigned.
  - Features that can be assigned are limited to those without additional data, (e.g. call-appr, auto-cback) or when the additional data is optional (e.g. call-fwd, send-calls).

## 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 TeleApps Admin Assist.

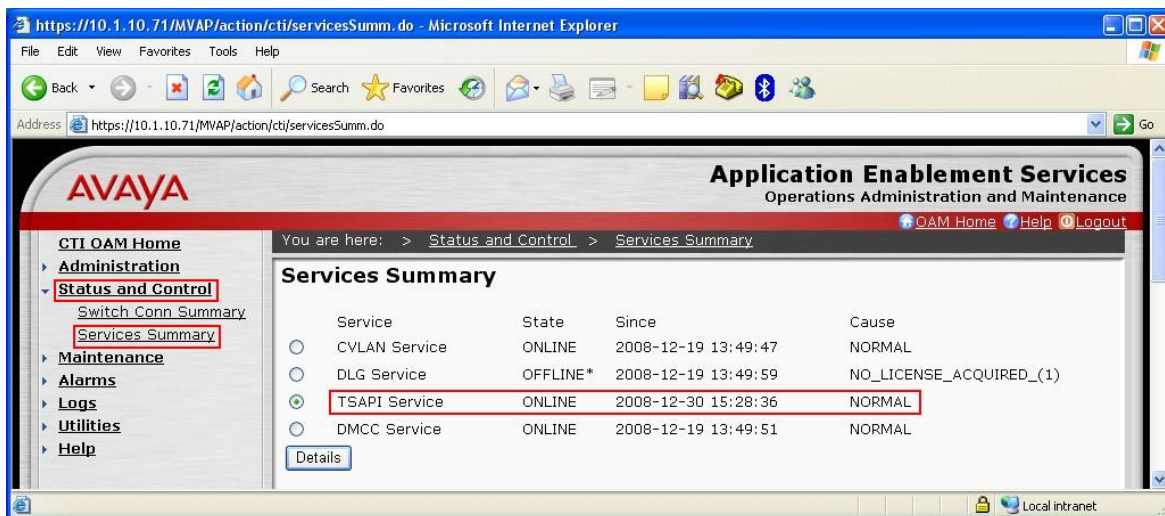
### 7.1. Verify Avaya Communication Manager

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

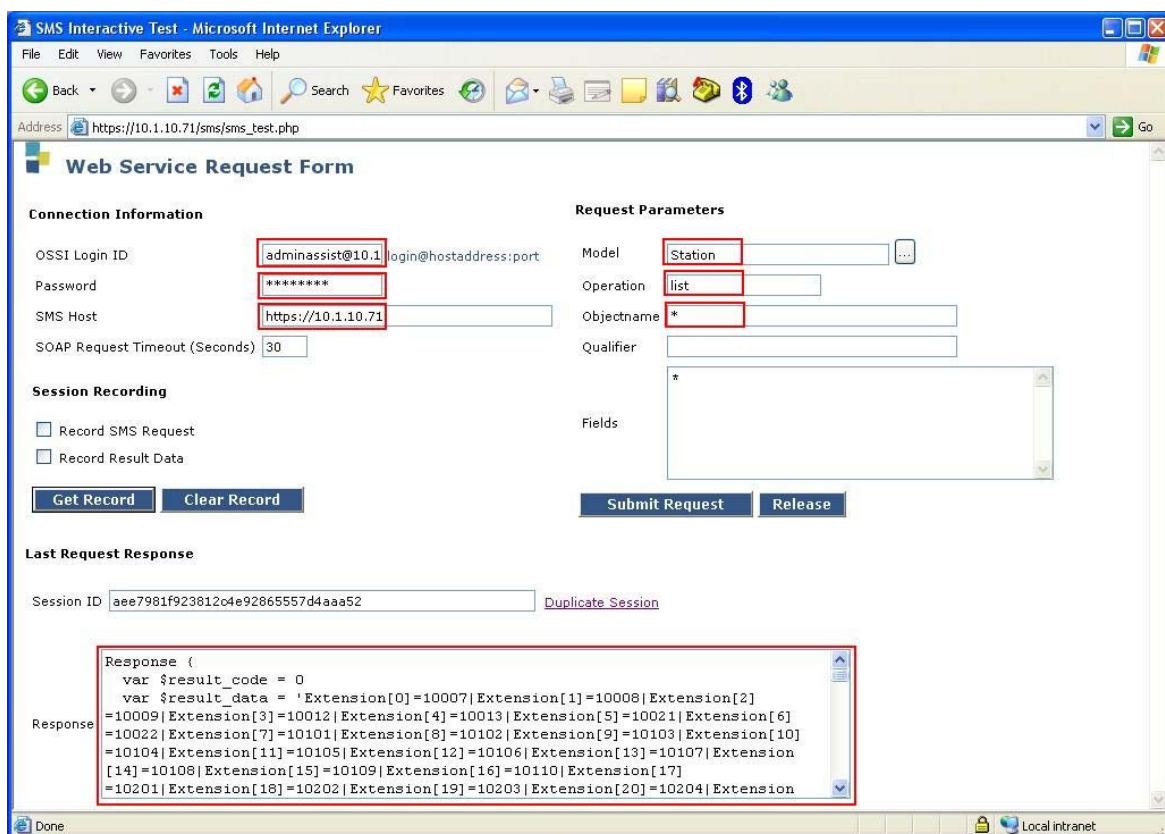
status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	5	no	aes1	established	47	53

### 7.2. Verify Avaya Application Enablement Services

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



Browse to the SMS Service test page **https://<IP address of AES>/sms/sms\_test.php**. Using the login information for Admin Assist in **Section 3.4 Step 2**, verify that a listing of the station records on Avaya Communication Manager can be retrieved successfully.



### 7.3. Verify TeleApps Admin Assist

Add a new user using TeleApps Admin Assist. Verify that the user is created in Microsoft Active Directory and the user extension is created in Avaya Communication Manager.

**TeleApps Admin Assist**

**Add New User**

First Name: John  
 Last Name: Doe  
 Logon Name: johndoe  
 Password: .....  
 Confirm Password: .....  
 Message Lamp Extension: 20015  
 E-mail Alias: .....  
 Description: John Doe  
 Port: IP  
 Extension: 20015  
 Template: Template1.xml  
 Emergency location Extension: 20015

☐ User Must change the Password on next logon  
☒ Password Never Expires  
☐ Create Mail Box  
☒ User Cannot Change the Password  
☐ Disable User account

**Add User** **Cancel**

Obtain the status of an agent using TeleApps Admin Assist and verify that the status corresponds to that observed on the telephone.

**TeleApps Admin Assist**

**Current Status**

Agent ID: 11001 Agent Name: Agent 1

**Set New Status**

Agent Status: ACW

**Get Current State**

Additional Info: (In case of Login/AUX)

Login: .....  
 Extension: 20003  
 Agent Password: 000000  
 AUX Mode: .....  
**Set Agent Status** **Cancel**

## 8. Support

For technical support on TeleApps Admin Assist, contact the TeleApps support team at:

- Phone: +61 2 8205 0529
- Email: support@teleapps.com.au

## 9. Conclusion

These Application Notes illustrate the procedures for configuring TeleApps Admin Assist to interoperate with Avaya Application Enablement Services and Avaya Communication Manager. In the configuration described in these Application Notes, TeleApps Admin Assist uses the TSAPI and SMS Services of Avaya Application Enablement Services to perform its tasks. All test cases were completed successfully.

## 10. Additional References

This section references the Avaya and TeleApps 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 6, January 2008, Document Number 555-245-205.

The following product documentation is available from TeleApps.

- [3] *TeleApps Admin Assist 1.0 User Guide*, Version 1.0, December 2008

---

**©2009 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).