



Avaya Solution & Interoperability Test Lab

Application Notes for InteractCRM ThinConnect with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for InteractCRM ThinConnect to interoperate with Avaya Communication Manager and Application Enablement Services (AES). ThinConnect is an interaction management application developed using the Java Telephony Application Programming Interface (JTAPI).

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 InteractCRM ThinConnect to interoperate with Avaya Communication Manager and Application Enablement Services (AES). InteractCRM ThinConnect is a desktop Computer Telephony Integration (CTI) solution that provides desktop control over telephony elements. ThinConnect communicates with Avaya Application Enablement Services (AES) using the Java Telephony Application Programming Interface (JTAPI). It provides a desktop CTI Toolbar for screen-pop and other integration requirements.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying InteractCRM ThinConnect for the following:

- Agent login, logout and change work modes.
- Handling incoming and outgoing calls.
- Holding and resuming of calls.
- Blind and consult voice transfers and voice conference.
- Wrap up and aux work reason codes.

The serviceability testing focused on verifying the ability of InteractCRM ThinConnect to recover from adverse conditions, such as disconnecting the Ethernet cables on the ThinConnect Client PC, ThinConnect Server and Avaya AES Server, and resetting the Avaya Communication Manager and ThinConnect Server.

1.2. Support

Technical support on InteractCRM ThinConnect can be obtained through the following:

- Phone: +91-22-40553055
- Email: tcsupport@interactcrm.com

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8500 Server, an Avaya G650 Media Gateway, an Avaya AES Server and Avaya 9630 IP Telephones. InteractCRM ThinConnect Server application is installed on a Windows 2003 Server together with Microsoft SQL Server 2005 for database support. InteractCRM ThinConnect Server communicates with the TSAPI Service on the Avaya AES Server using JTAPI. The agent PCs are running the ThinConnect Client application hosted on the InteractCRM ThinConnect Server using the Microsoft Internet Explorer. Contact related actions such as call answer and transfer are initiated using the ThinConnect Client. The Avaya C364T-PWR Converged Stackable Switch provides Ethernet connectivity to the servers and IP telephones.

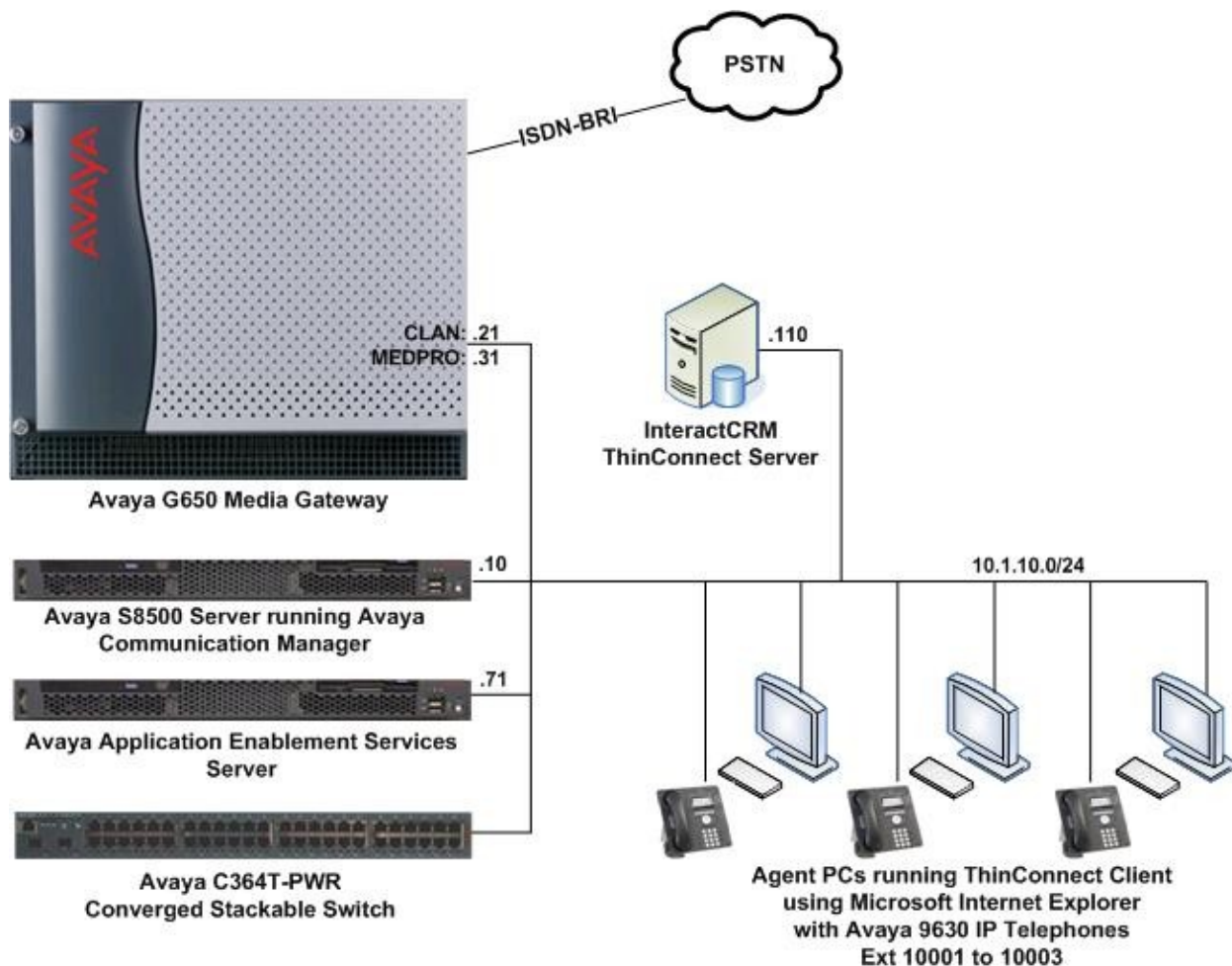


Figure 1: Test Configuration

3. Equipment and Software Validated

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

Equipment/Software	Version
Avaya S8500 Server	Avaya Communication Manager 5.1.2 (Service Pack 01.2.416.4-16770)
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN2312BP IP Server Interface• TN799DP C-LAN Interface• TN2302AP IP Media Processor• TN2185B BRI Trunk	- HW07, FW044 HW01, FW031 HW20, FW118 000004
Avaya Application Enablement Services	4.2.1 (r4-2-1-20-5-0) Patch 1
Avaya C364T-PWR Converged Stackable Switch	4.5.18
Avaya 9630 IP Telephones	2.0 (H.323)
InteractCRM ThinConnect Server on Dell PowerEdge 860	1.0 Microsoft Windows Server 2003, SP2
Microsoft SQL Server	Microsoft SQL Server 2005, SP3
Sun Java SE Development Kit (JDK)	5.0 Update 13
Apache Tomcat	5.5.17

Table 1: Equipment/Software Validated

4. Configure Avaya Communication Manager

This section provides the procedures for configuring 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.

4.1. Configure AES and CTI Links

The Avaya AES server forwards CTI requests, responses, and events between InteractCRM ThinConnect Server 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 InteractCRM ThinConnect. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES and CTI links. See **Section 5** for the details of configuring the AES 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.
	<pre> display system-parameters customer-options Page 3 of 11 OPTIONAL FEATURES 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.	Enter the add cti-link m command, where m is a number between 1 and 64, inclusive. Enter a valid Extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to ADJ-IP , and assign a descriptive Name to the CTI link.
	<pre> add cti-link 1 Page 1 of 3 CTI LINK CTI Link: 1 Extension: 19951 Type: ADJ-IP COR: 1 Name: TSAPI Svcs </pre>

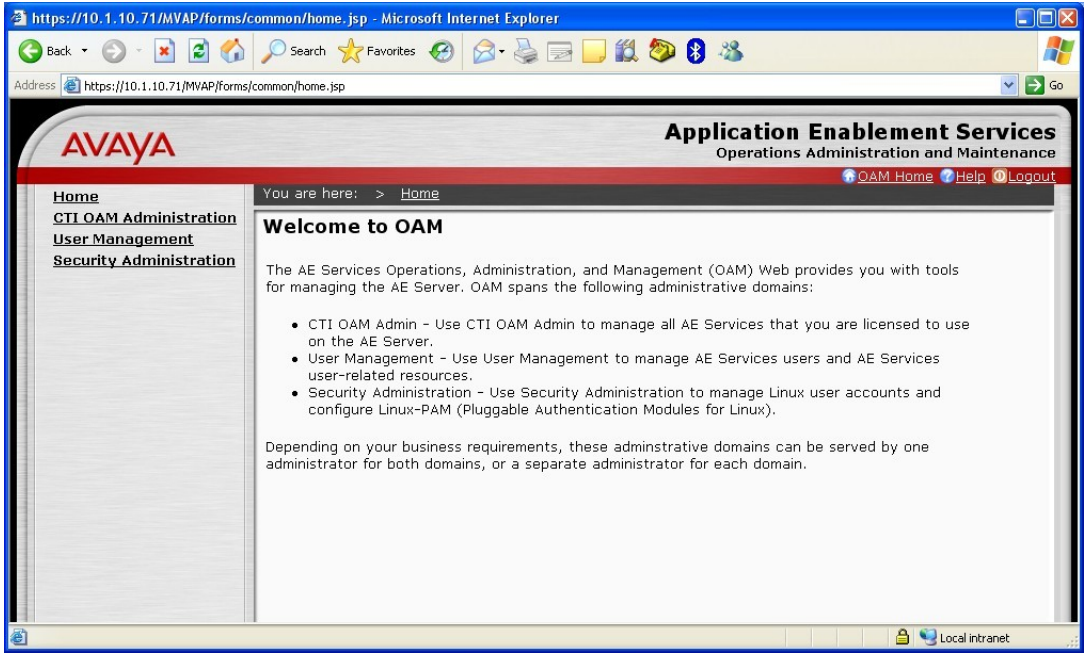
Step	Description																																											
3.	<p>Enter the change node-names ip command. In the compliance-tested configuration, the CLAN board with the node-name CLAN-01A02 was utilized for connectivity to Avaya AES server.</p> <div><div>change node-names ip</div><div>Page1 of2</div><table><tr><th colspan="2">IP NODE NAMES</th></tr><tr><th>Name</th><th>IP Address</th></tr><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></table></div>	IP NODE NAMES		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																													
IP NODE NAMES																																												
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 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 CLAN-01A02 board that was configured previously in Step 3. During the compliance test, the default port was utilized for the Local Port field.</p> <div><div>change ip-services</div><div>Page1 of3</div><table><tr><th colspan="6">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>Remote Port</th></tr><tr><td>AESVCS</td><td>y</td><td>CLAN-01A02</td><td>8765</td><td></td><td></td></tr></table><p>On Page 3, enter the hostname of the Avaya AES server for the AE Services Server field. The server name may be obtained by logging in to the Avaya AES 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 Avaya AES server in Section 5.3 Step 2.</p><div><div>change ip-services</div><div>Page3 of3</div><table><tr><th colspan="5">AE Services Administration</th></tr><tr><th>Server ID</th><th>AE Services Server</th><th>Password</th><th>Enabled</th><th>Status</th></tr><tr><td>1:</td><td>aes1</td><td>xxxxxxxxxxxxxxxxxx</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></table></div></div>	IP SERVICES						Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	AESVCS	y	CLAN-01A02	8765			AE Services Administration					Server ID	AE Services Server	Password	Enabled	Status	1:	aes1	xxxxxxxxxxxxxxxxxx	y		2:					3:				
IP SERVICES																																												
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																																							
AESVCS	y	CLAN-01A02	8765																																									
AE Services Administration																																												
Server ID	AE Services Server	Password	Enabled	Status																																								
1:	aes1	xxxxxxxxxxxxxxxxxx	y																																									
2:																																												
3:																																												
5.	<p>Enter the save translation command to save the changes to the system. This completes the configuration of the Avaya Communication Manager.</p>																																											

5. 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

5.1. Administer CTI User

Step	Description
1.	<p>Launch a web browser and enter https://<IP address of AES server>/MVAP/ 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 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 InteractCRM ThinConnect in Section 6 to access the TSAPI Service on the AES server. Scroll down to the bottom of the page and click Apply (not shown).</p>

Add User - Microsoft Internet Explorer

Address: <https://10.1.10.71/MVAP/action/user/precureuser.do>

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > [User Management](#) > [Add User](#)

User Management Home

- [User Management](#)
 - List All Users
 - Add User**
 - Search Users
 - Modify Default User
 - Change User Password
- Service Management
- Help

Add User

Fields marked with * can not be empty.

* User Id:

* Common Name:

* Surname:

* User Password:

* Confirm Password:

Admin Note:

Avaya Role:

Business Category:

Car License:

CM Home:

Cms Home:

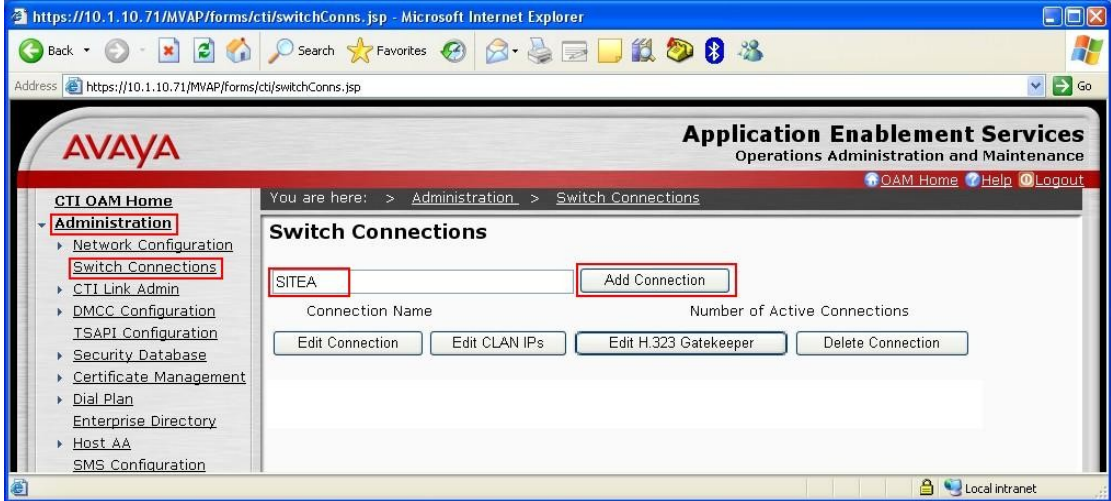
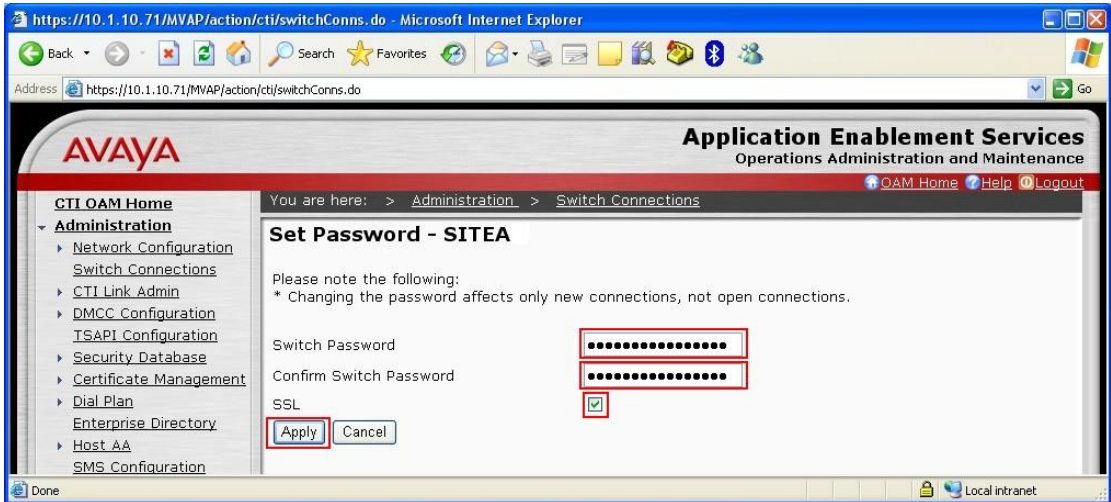
CT User:

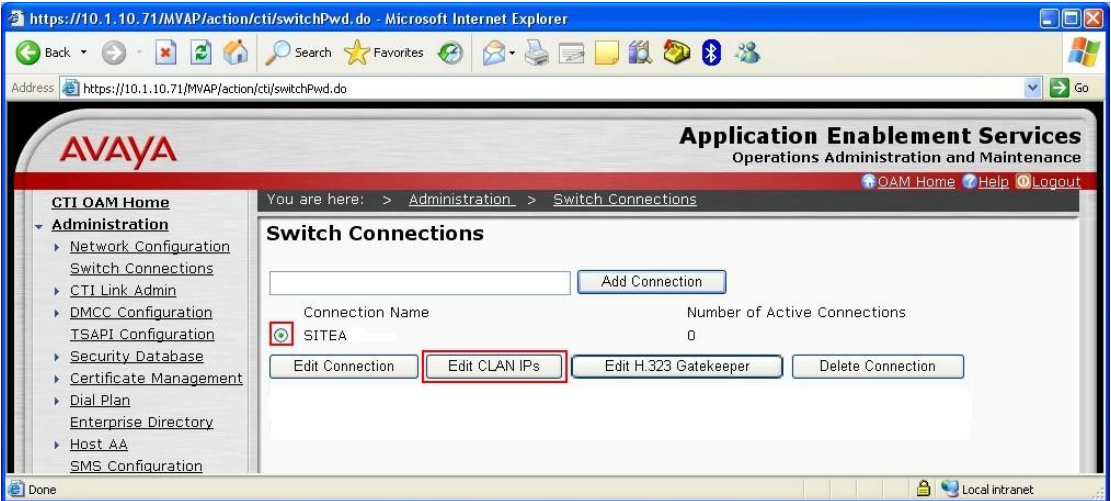
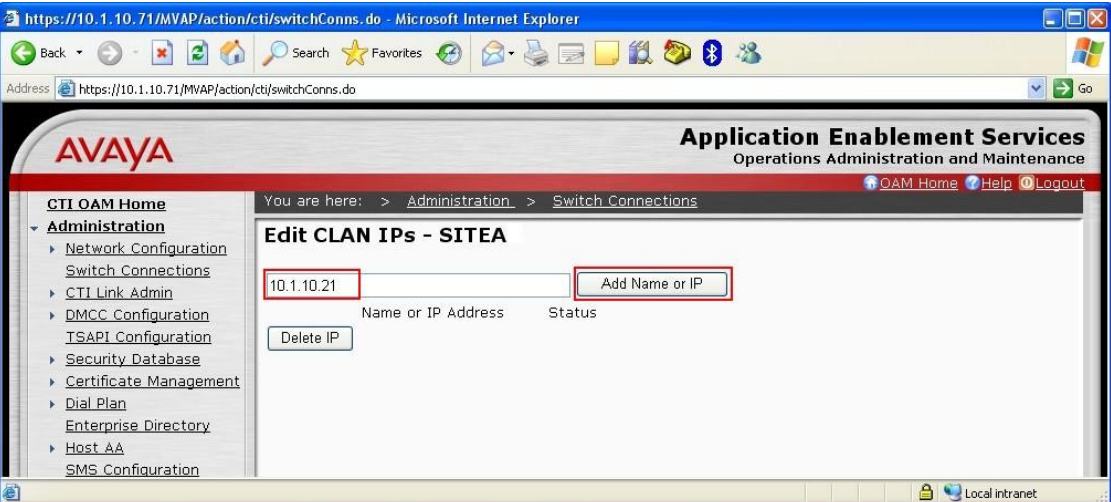
Department Number:

5.2. Verify Avaya Application Enablement Services License

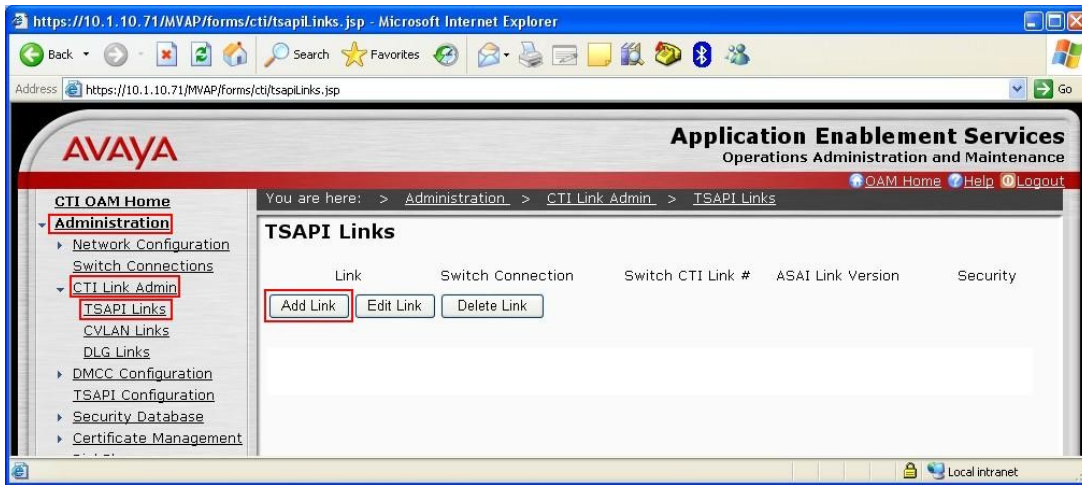
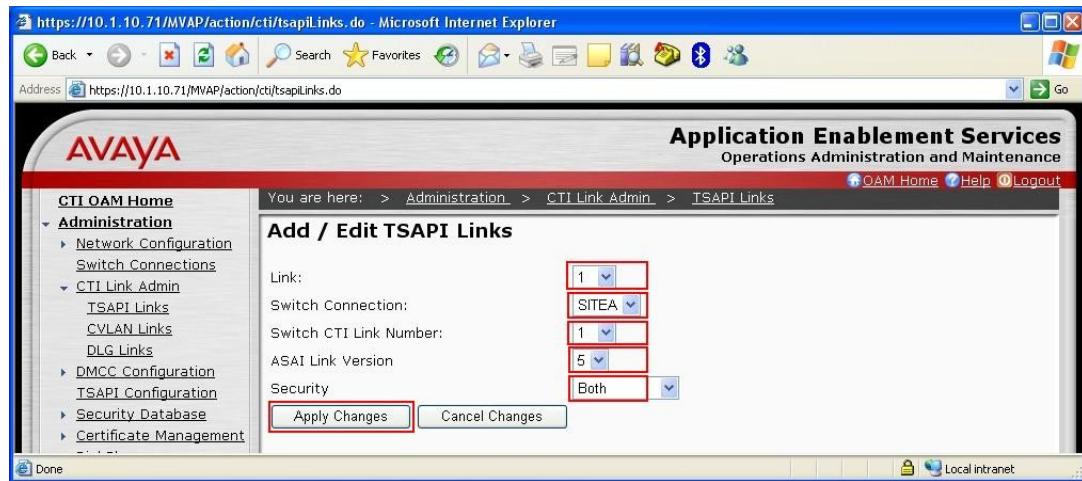
Step	Description
1.	<p>Select OAM Home, then click on CTI OAM Administration from the left menu (not shown). From the Welcome to CTI OAM Screens page, verify that the Avaya Application Enablement Services license has proper permissions for the features illustrated in these Application Notes by ensuring 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>

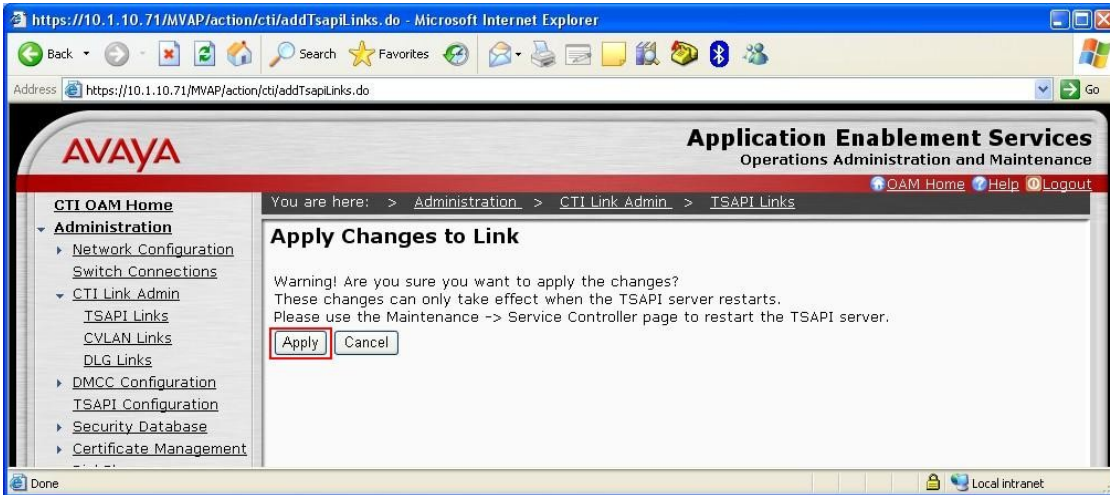

5.3. Administer Switch Connection


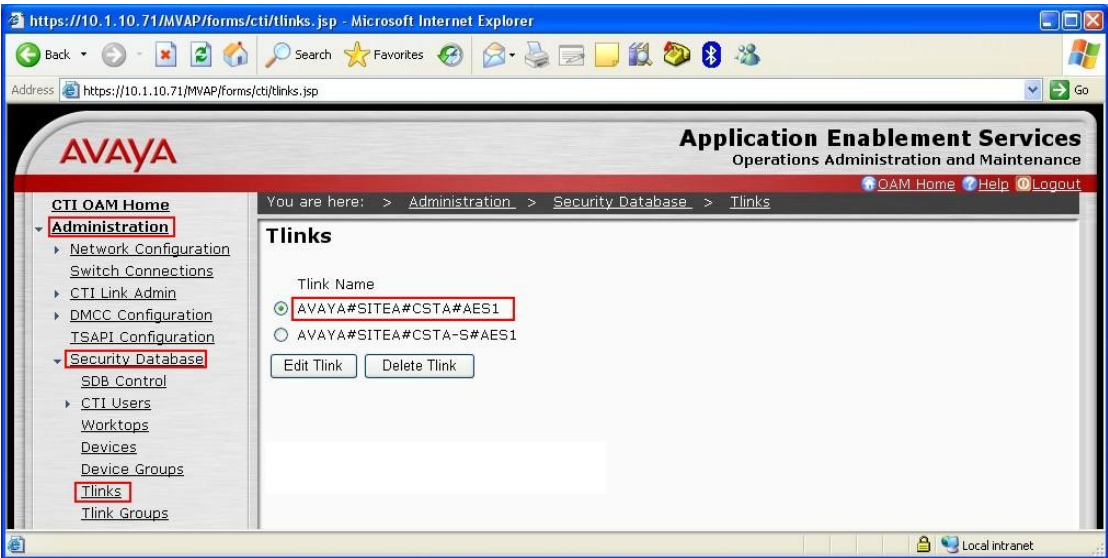
Step	Description
1.	<p>From the CTI OAM Home menu, select Administration > Switch Connections. Enter a descriptive name for the switch connection and click Add Connection. In this configuration, SITEA is used.</p> 
2.	<p>The Set Password – SITEA screen is displayed. Select CTI/Call Information for Switch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

Step	Description
3.	<p>The Switch Connections screen is displayed. Select the newly added switch connection name and click Edit CLAN IPs.</p> 
4.	<p>In the Edit CLAN IPs – SITEA 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 the Avaya Communication Manager in Section 4.1 Step 3. Click Add Name or IP.</p> 

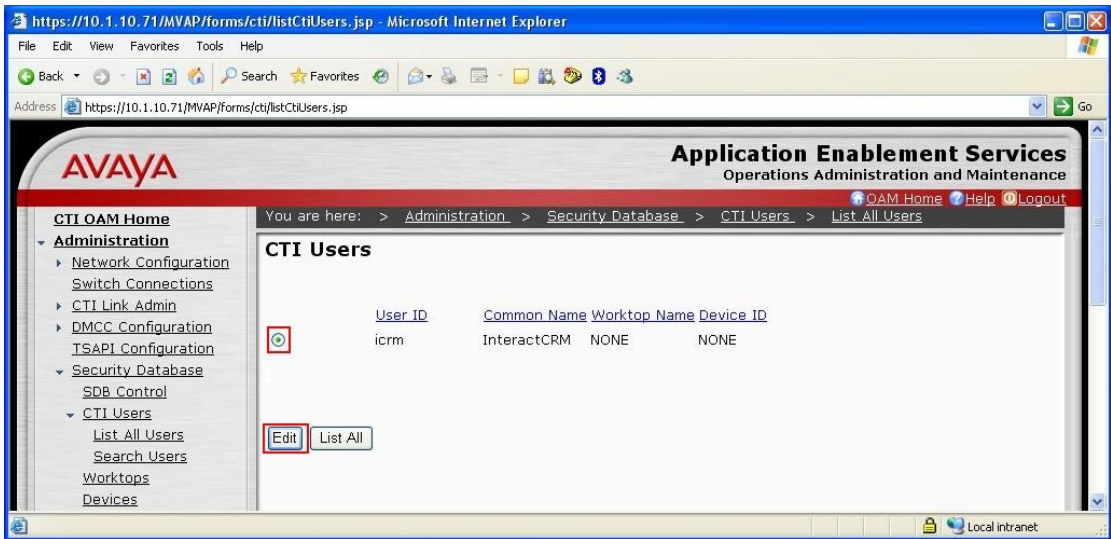
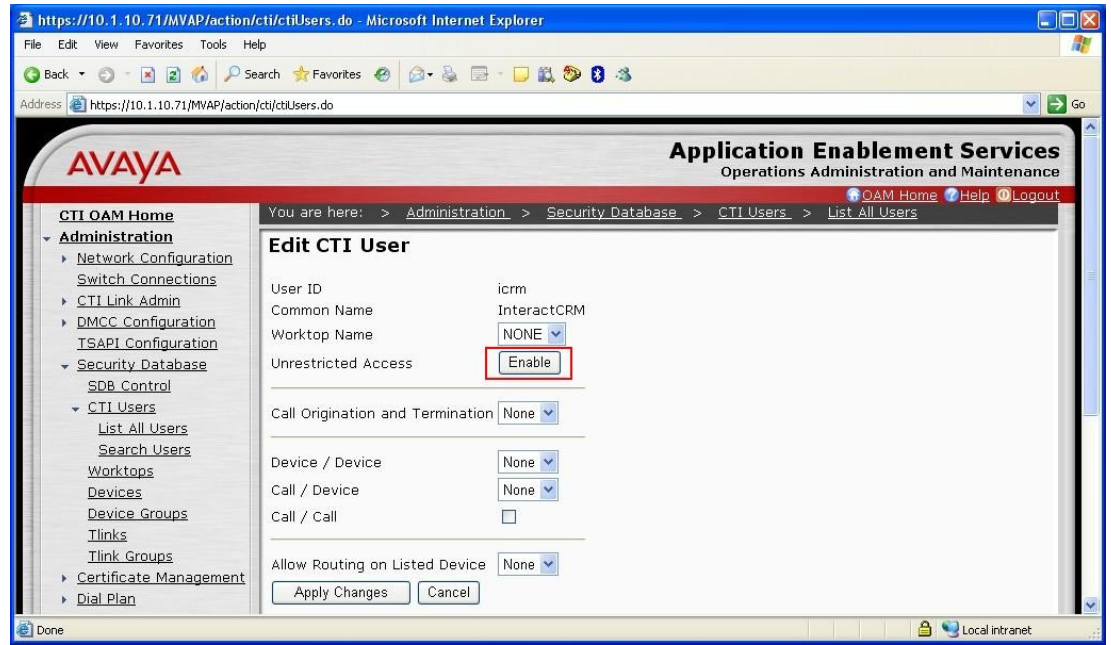
5.4. Administer TSAPI Link

Step	Description
1.	<p>To administer a TSAPI link on AES, select Administration > CTI Link Admin > TSAPI Links from the CTI OAM Home menu. Click Add Link.</p> 
2.	<p>In the Add / Edit TSAPI Links screen, select the following values:</p> <ul style="list-style-type: none">• 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 encrypted and unencrypted TSAPI Links can both be used. <p>Note that the actual values may vary. Click Apply Changes.</p> 

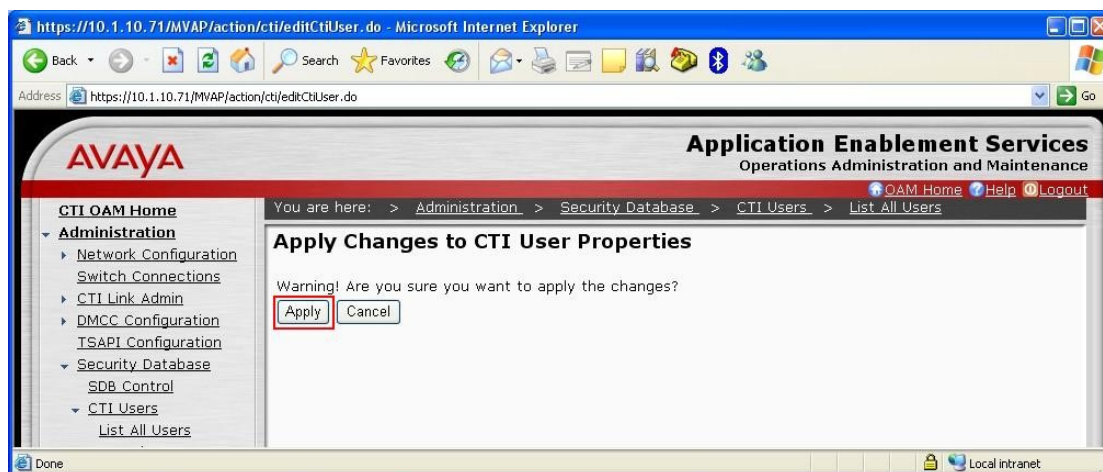
Step	Description
3.	Click Apply to confirm the changes.
	
4.	To restart the TSAPI Service, select Maintenance > Service Controller from the CTI OAM Home menu. Check the TSAPI Service checkbox and click Restart Service .
	

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 the InteractCRM ThinConnect Server in Section 6 . In this configuration, the unencrypted Tlink Name AVAYA#SITEA#CSTA#AES1 which is automatically assigned by the AES server is used.
	

5.5. Administer CTI User Permission

Step	Description
1.	<p>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.</p> 
2.	<p>Assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, Unrestricted Access 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.</p> 

Step	Description
3.	Click Apply to apply the changes.



6. Configure InteractCRM ThinConnect

This section provides the procedures for configuring InteractCRM ThinConnect, which includes the following areas:

- Configure InteractCRM ThinConnect Server
- Configure InteractCRM ThinConnect Client PC

6.1. Configure InteractCRM ThinConnect Server

InteractCRM ThinConnect Server is deployed on a Windows 2003 Server running Apache Tomcat 5.5.17. InteractCRM ThinConnect Server consists of two components:

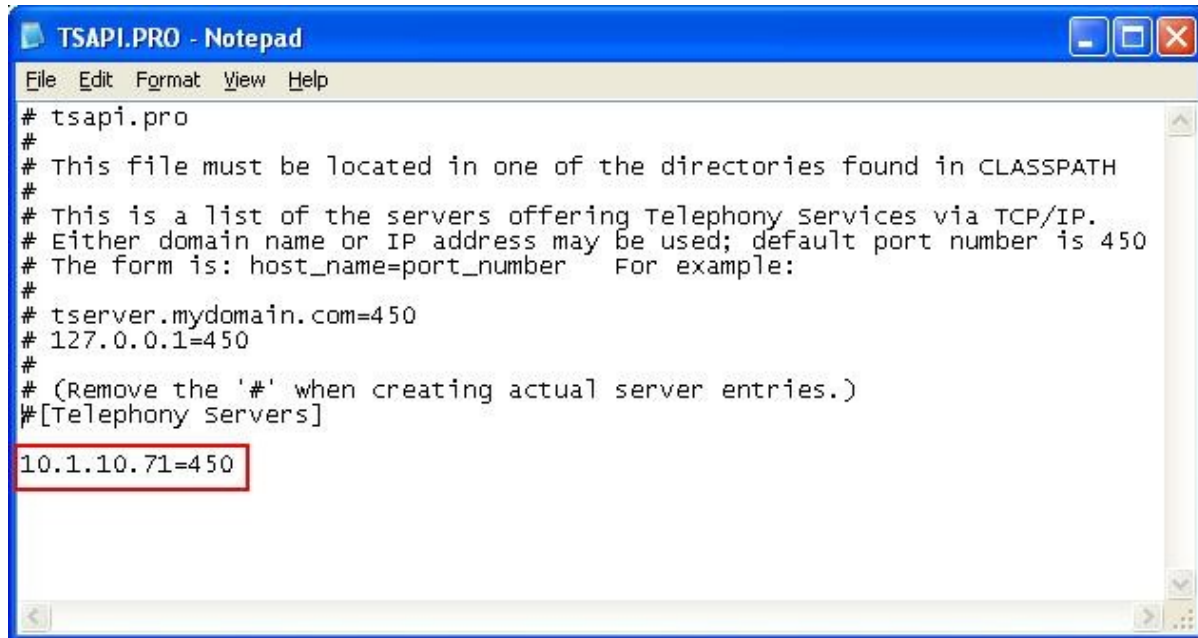
- LoadBalancer - Dynamically distributes agents across available ThinConnect Server(s).
- ThinConnect Server - Avaya IC SDK compliant call control server and Agent Interaction Manager.

InteractCRM ThinConnect supports multiple ThinConnect Server machines for redundancy and uses the LoadBalancer to distribute the agents. In this test configuration, the deployment consists of one ThinConnect Server with both the LoadBalancer and ThinConnect Server co-resident on the same machine. The configuration of the LoadBalancer will not be covered as it does not interface with the Avaya AES.

6.1.1. Configure ThinConnect Server

From the InteractCRM ThinConnect server, edit the file **TSAPI.PRO** located in the folder **C:\InteractCRM\ThinConnect\apache-tomcat-5.5.17\webapps\mis\WEB-INF\classes** using Notepad. Specify the IP address of the Avaya AES Server by inserting the following entry as shown below. Note that **450** is the default port number of the TSAPI Service running on the Avaya AES Server.

10.1.10.71=450



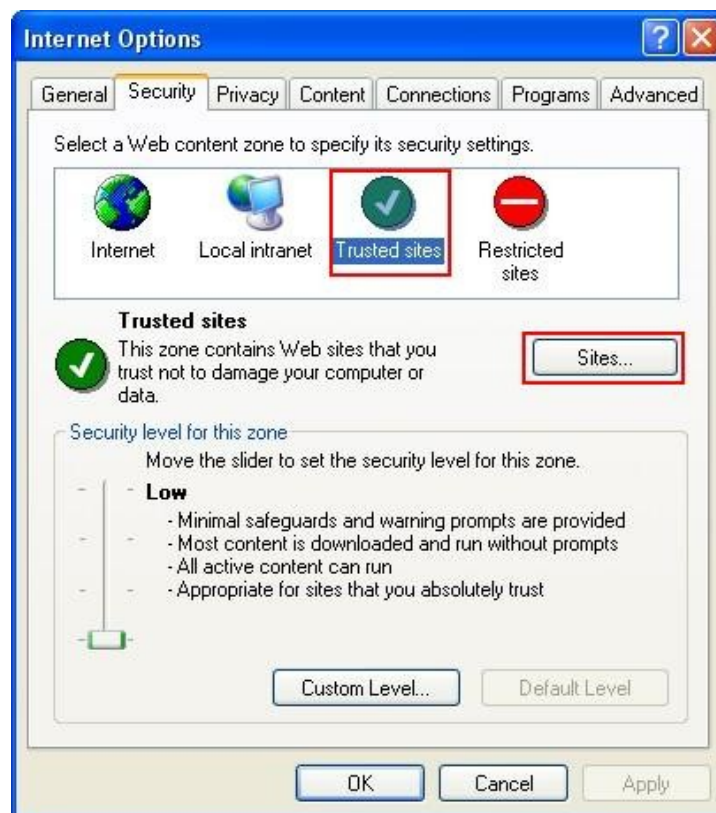
Edit the file **ts.properties** located in the folder **C:\InteractCRM\ThinConnect\apache-tomcat-5.5.17\webapps\mis\WEB-INF\classes** using Notepad. Enter the following values for the fields below, and retain the default values for the remaining fields.

- **ts.login**: CTI User created in **Section 5.1 Step 2**, in this case is "icrm".
- **ts.password**: Password of CTI User created in **Section 5.1 Step 2**.
- **ts.link**: Tlink Name as shown in **Section 5.4 Step 6**.
- **ts.dialplan.extension.width**: Number of digits for phone extension, in this case is "5".
- **ts.dialplan.extension.startwith**: Starting digit of extension, in this case is "1".

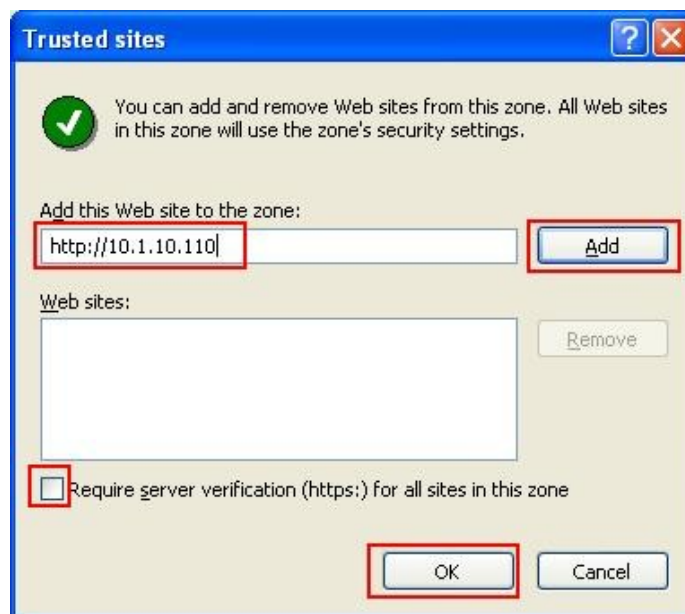


6.2. Configure InteractCRM ThinConnect Client PC

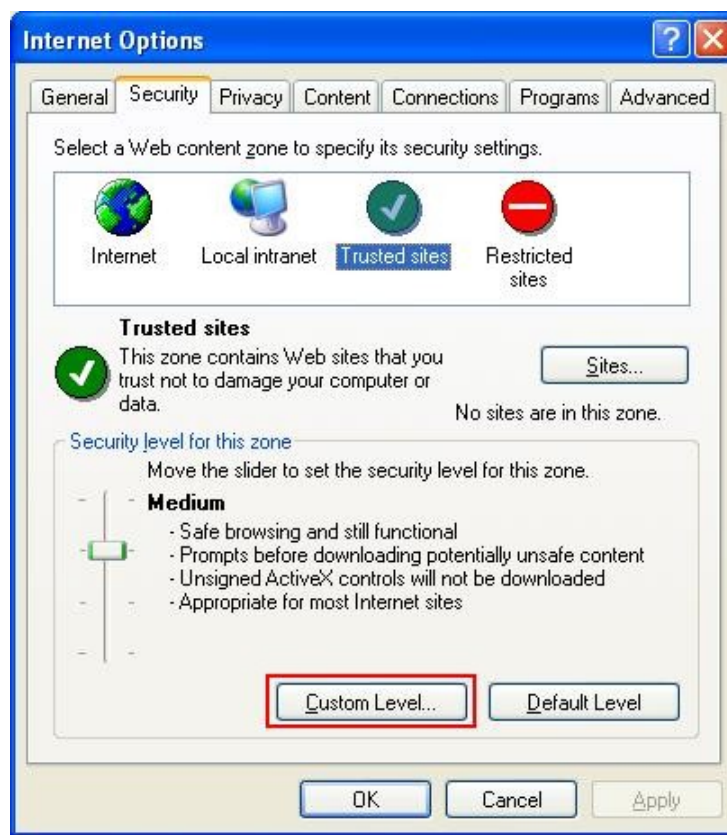
From the InteractCRM ThinConnect Client PCs, launch Microsoft Internet Explorer. Select **Tools > Internet Options** and click the **Security** tab. Click **Trusted sites** and then **Sites**.



Enter the URL to launch the ThinConnect Client in **Add this Web site to the zone** and click **Add**. Uncheck **Require server verification (https:) for all sites in this zone**. Click **OK**.



From the Internet Options window, click **Custom Level**.



From the Security Settings window, configure the following:

- Download signed ActiveX controls: **Enable**
- Download unsigned ActiveX controls: **Enable**
- Initialize and script ActiveX controls not marked as safe: **Enable**
- Run ActiveX controls and plug-ins: **Enable**
- Script ActiveX controls marked safe for scripting: **Enable**
- File download: **Enable**
- Access data sources across domains: **Enable**



Click **OK**. At the next screen, click **Yes** to confirm the changes. This completes the configuration required for the ThinConnect Client PC.

7. General Test Approach and Test Results

The feature test cases were performed manually. Incoming and outgoing calls were made on Avaya Communication Manager and the calls are handled by agents running InteractCRM ThinConnect Client. All operations were made using the ThinConnect Client without interacting with the telephone.

The serviceability test cases were performed manually by disconnecting the Ethernet cables on the ThinConnect Client PC, ThinConnect Server and Avaya AES Server, rebooting of the Avaya Communication Manager and ThinConnect Server.

All feature test cases were executed and passed. For serviceability test cases, the following observations were noted:

- When the Avaya AES Server is unavailable, the JTAPI socket connection between ThinConnect Server and the Avaya AES Server is dropped. When Avaya AES Server recovers, ThinConnect Server does not reconnect, so all further CTI control will fail. Restart of the ThinConnect Service restores normal operation. InteractCRM will provide the fix in a future patch to correct this behavior.

8. Verification Steps

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

8.1. Verify Avaya Communication Manager

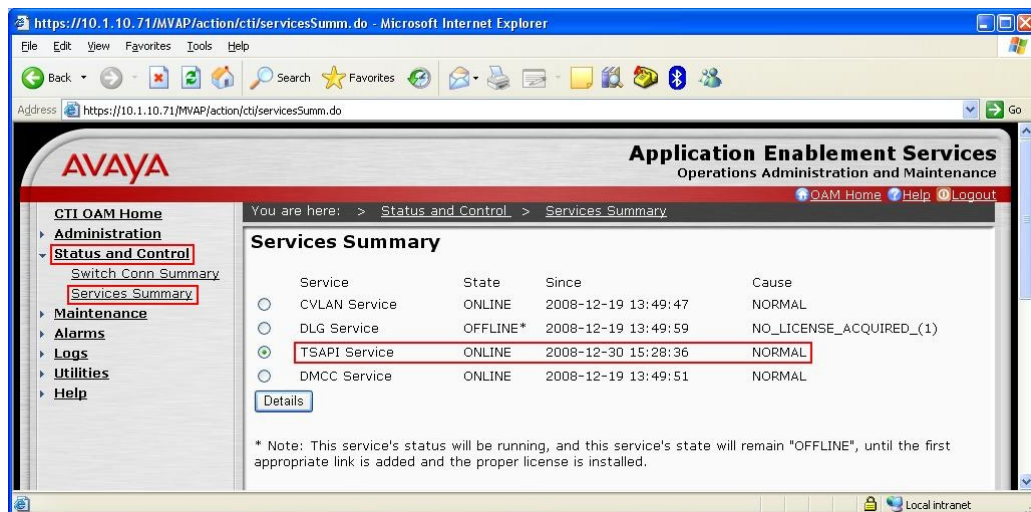
Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command. The **Service State** field should display **established**.

```
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

8.2. 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 **State** field for the **TSAPI Service** should display **ONLINE**.



8.3. Verify InteractCRM ThinConnect

Make an incoming call to the agent. Verify that the agent desktop is populated with an alerting call entry with the **State** “New”. Click on **Answer** to answer the call.

Verify that the agent is connected to the caller, and that the **State** for the call changes to “In Progress”. Verify also that the other buttons such as “Hold”, “Transfer”, “Conf” and “Consult” are now enabled.

9. Conclusion

These Application Notes describe the configuration steps required for InteractCRM ThinConnect to interoperate with Avaya Communication Manager and Avaya Application Enablement Services using the Java Telephony Application Programming Interface (JTAPI). All feature test cases were completed successfully. Serviceability test cases were completed with observations noted in **Section 7**.

10. Additional References

This section references the Avaya and InteractCRM 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] *Feature Description and Implementation for Avaya Communication Manager*, Issue 6, January 2008, Document Number 555-245-205.

The following product documentations are available from InteractCRM.

[3] *ThinConnect Installation Guide*, Version 1.0.

[4] *ThinConnect User Manual*, Version 1.0.

©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.