Avaya Solution & Interoperability Test Lab

Application Notes for Orange Softphone 1.0 with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Orange Softphone to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES).

Orange Softphone is a desktop CTI solution developed by Orange Business Services. This client provides desktop control over telephony elements. Orange Softphone communicates with Avaya AES using the (Telephony Services Application Programming Interface) TSAPI Service and provides a functional desktop CTI solution for CRM application screen pop.

Readers should pay attention to section 2, in particular the scope of testing as outlined in Section 2.1 as well as any observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for Orange Softphone 1.0 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES).

Orange Softphone is a contact center solution developed using Java Telephony Application Programming Interface (JTAPI). It allows calls to be made or received via computer without the need to place or answer using telephones.

2. General Test Approach and Test Results

The feature test cases were performed manually. Inbound and outbound calls were made on Communication Manager and calls handled by agents running the Orange Softphone Client. In this testing, agents were logged in from the respective phones as expert agents.

The serviceability test cases were also performed manually by disconnecting/reconnecting the ethernet cable on each component and restarting of the client PC as well as Communication Manager and Avaya AES server.

DevConnect compliance testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect compliance testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying Orange Softphone for the following:

- Agent in manual in or auto-in login mode, logout and failure scenarios.
- Handling of incoming and outgoing calls.
- Holding and resuming of calls.
- Blind and Consult voice transfers as well as voice conference.
- Features like Timed After Call Work and entering of reasons code (AUX code)

The serviceability testing focused on verifying the ability of Orange Softphone to recover from adverse conditions such as disconnecting the ethernet cables on the Orange Softphone client PC, Communication Manager and Avaya AES server, and resetting of the Communication Manager.

2.2. Test Results

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

- Softphone required auto-answer mode to be activated with agents using headset (and handset off)
- If agent is on inbound call Line 1, Line 2 is not enabled for outbound call as caller will either be transferred or conferenced.
- If agent is on an outbound call, the current call on Line 1 must be placed on hold before second outbound call can be made through Line 2.

2.3. Support

Technical support on Orange Business Services can be obtained through the following:

- Phone: +91-2261544848,Toll Free - 18002096699
- Email: servicedesk.india@orange.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of a duplex pair of Avaya S8800 Servers, an Avaya G430 Media Gateway, Avaya AES Server and Avaya 96x1 H.323 IP Telephones. Orange Softphone client application is installed on a Microsoft Windows 7 Professional PCs. Orange Softphone communicates with the TSAPI Service on the Avaya AES Server. The Avaya 4548GT-PWR Converged Stackable Switch provides ethernet connectivity to the servers and IP telephones.

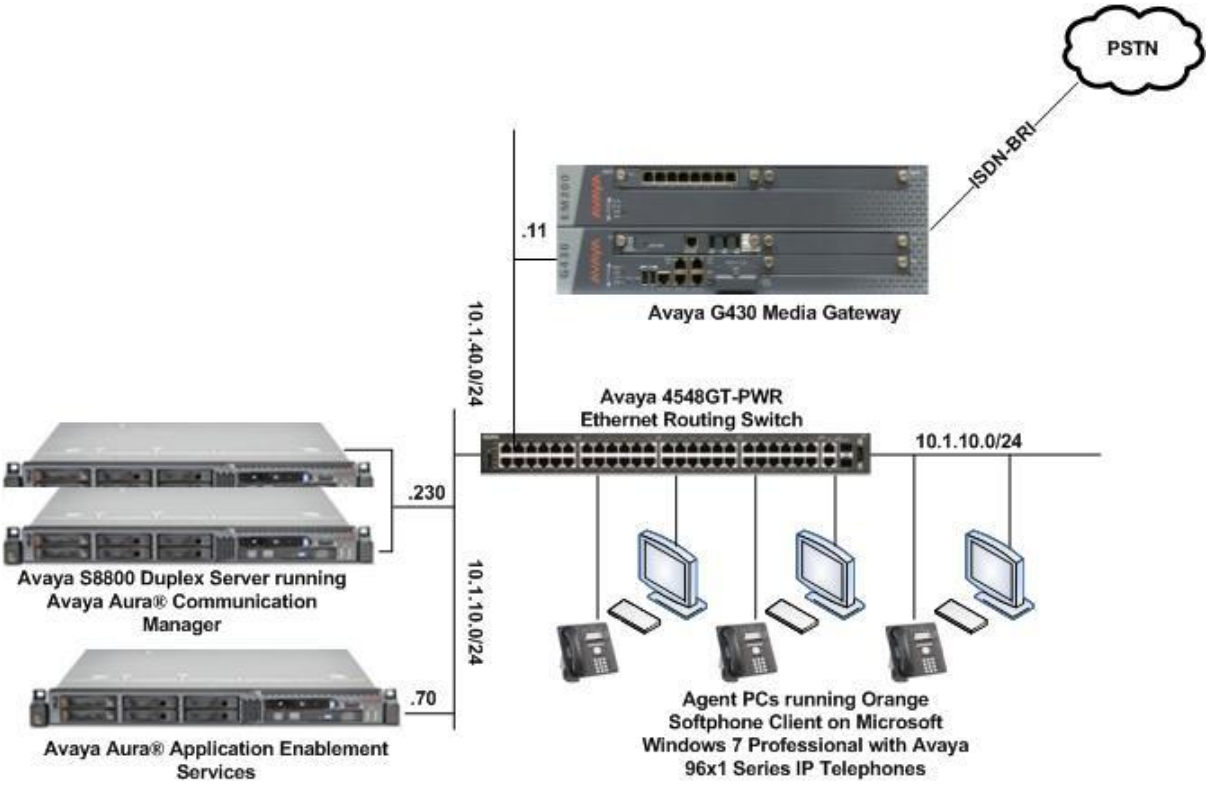


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura® Communication Manager on S8800 Duplex Servers	R016x.03.0.124.0-21591 (6.2 FP4)
Avaya G430 Media Gateway	36.7.0
Avaya Aura® Application Enablement Services	6.3.3.0.10-0 (6.2 FP4)
96x1 Series (H.323) IP Telephones	6.4014
Orange Softphone running on Windows 7 Professional Service Pack 1.0	1.0

Table 1: Equipment/Software Validated

5. Configure Avaya Communication Manager

This section provides the procedures for configuring Computer Telephony Integration (CTI) links on Avaya Communication Manager. Setup of agent stations, agent login ID, VDNs, Hunt Groups, Trunks and Call Center features is assumed to be configured and will not be detailed here.

All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

5.1. Configure AES and CTI Links

Avaya AES server forwards CTI requests, responses, and events between Orange Softphone clients and Communication Manager. Avaya AES server communicates with Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Orange Softphone. The following steps demonstrate the configuration of the Communication Manager 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.
	display system-parameters customer-options Page 3 of 11 OPTIONAL FEATURES Abbreviated Dialing Enhanced List? y Audible Message Waiting? y Access Security Gateway (ASG)? n Authorization Codes? y Analog Trunk Incoming Call ID? y CAS Branch? n A/D Grp/Sys List Dialing Start at 01? y CAS Main? n Answer Supervision by Call Classifier? y Change COR by FAC? n ARS? y Computer Telephony Adjunct Links? y ARS/AAR Partitioning? y Cvg Of Calls Redirected Off-net? y ARS/AAR Dialing without FAC? n DCS (Basic)? y ASAI Link Core Capabilities? y DCS Call Coverage? y ASAI Link Plus Capabilities? y DCS with Rerouting? y Async. Transfer Mode (ATM) PNC? n Async. Transfer Mode (ATM) Trunking? n Digital Loss Plan Modification? y ATM WAN Spare Processor? n DS1 MSP? y ATMS? y DS1 Echo Cancellation? y Attendant Vectoring? y (NOTE: You must logoff & login to effect the permission changes.)
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.

Step	Description
	add cti-link 3 Page 1 of 3 CTI LINK CTI Link: 3 Extension: 10093 Type: ADJ-IP COR: 1 Name: TSAPI Service - AES6x
3.	Enter the **change node-names ip** command. In the compliance-tested configuration, the processor of the communication manager with the node-name **procr** was utilized for connectivity to Avaya AES server.
	change node-names ip Page 1 of 2 IP NODE NAMES Name IP Address procr 10.1.10.230 procr6 ::
4.	Enter the **change ip-services** command. On **Page 1**, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. The **Local Node** field should be set to the **procr** that was configured previously in **Step 3**. During the compliance test, the default port was utilized for the **Local Port** field.
	change ip-services Page 1 of 4 IP SERVICES Service Type / Enabled / Local Node / Local Port / Remote Node / Remote Port AESVCS y procr 8765
	On **Page 4**, 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 Avaya AES server in **Section 6.3 Step 2**.
	change ip-services Page 4 of 4 AE Services Administration Server ID / AE Services Server / Password / Enabled / Status 1: 2: aes6x abcdef1234567890 y 3:
5.	Enter the **save translation** command to save the changes to the system. This completes the configuration of Avaya Communication Manager.

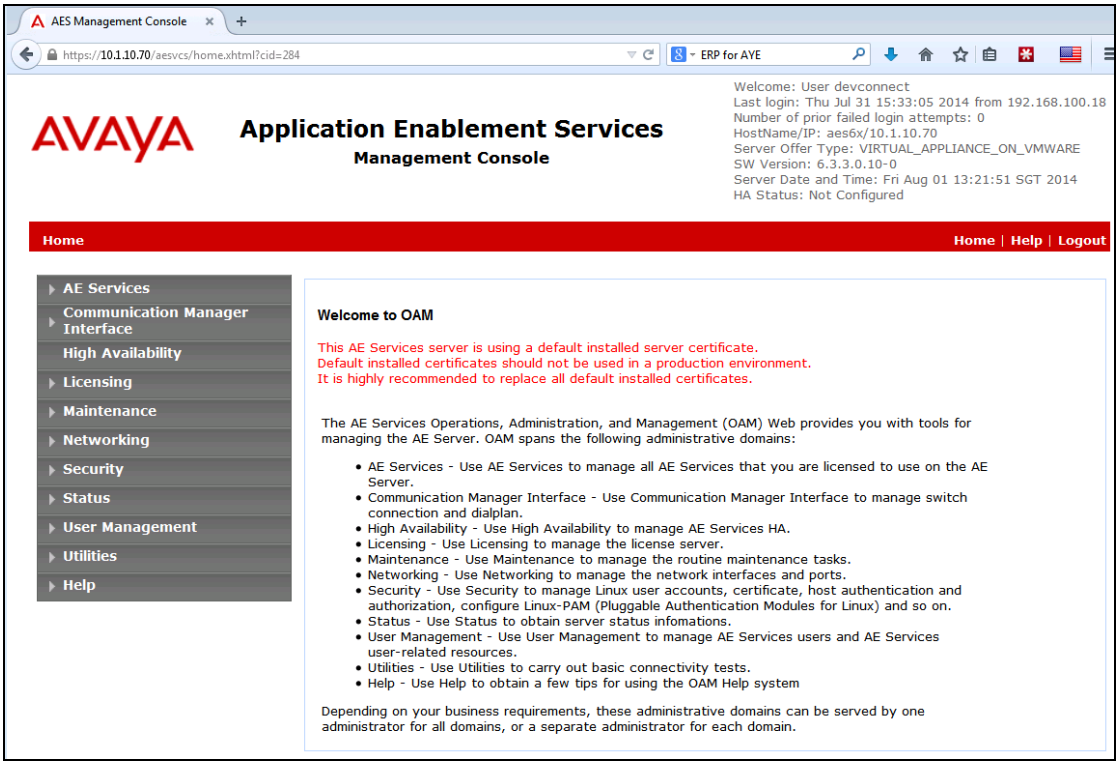
6. Configure Avaya Application Enablement Services

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

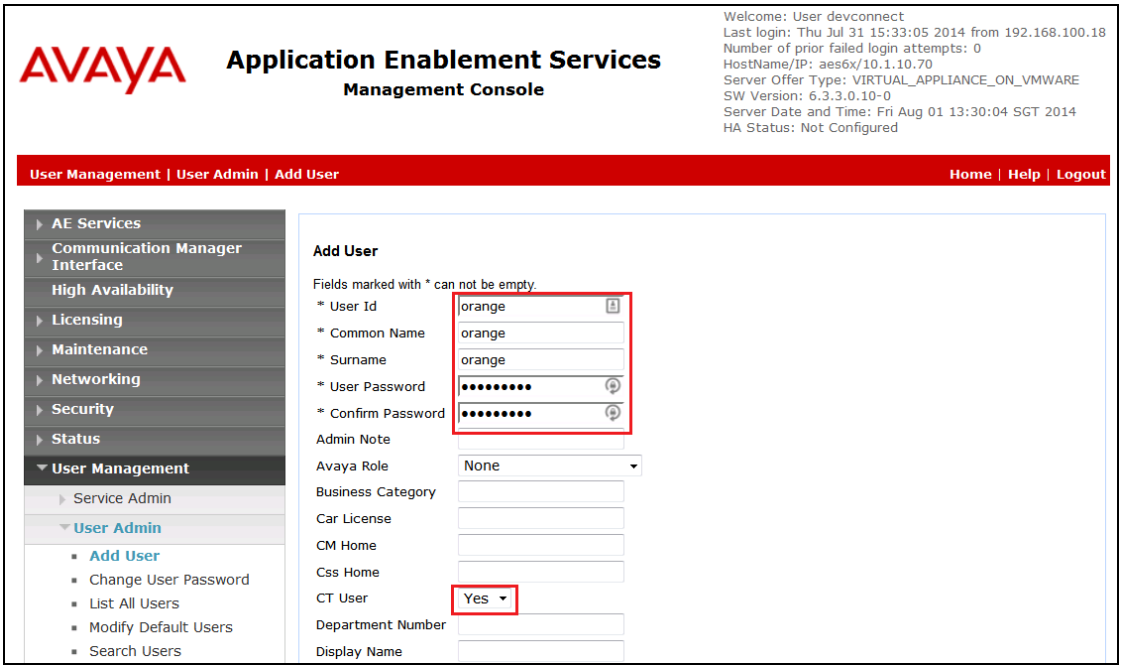
- Administer CTI User
- Verify Avaya Application Enablement Services License
- Administer Switch Connection
- Administer TSAPI link and Verify TSAPI Service Port
- Administer CTI user permission

6.1. Administer CTI User

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

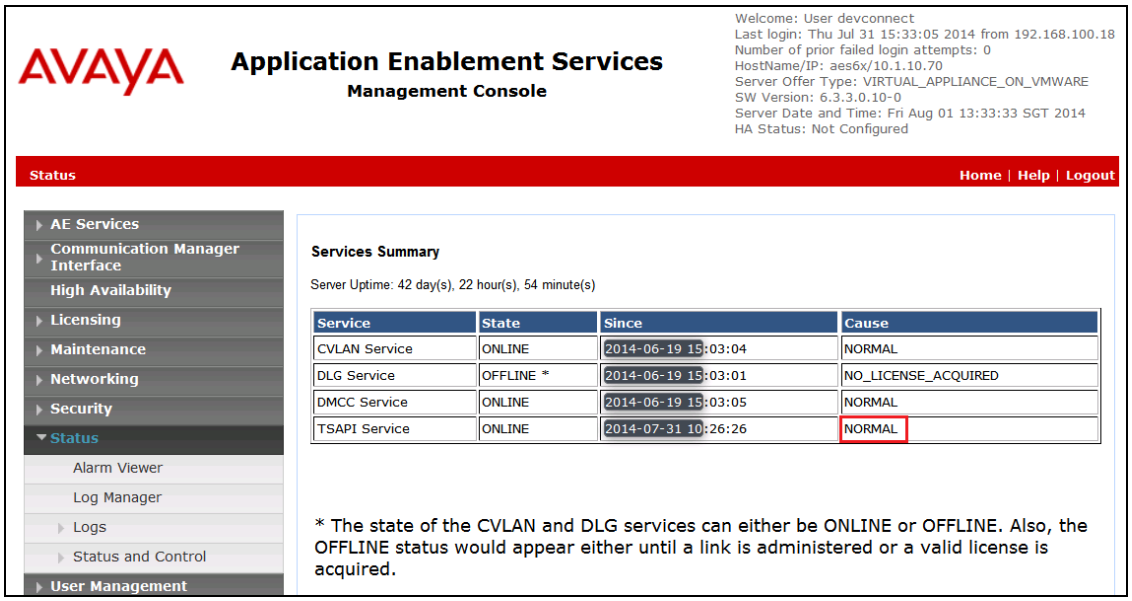


Step	Description
2.	Select **User Management → User Admin → Add User** in the left pane. Specify a value for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set **CT User** to **Yes**. Use the values for **User Id** and **User Password** to configure Orange Softphone in **Section 7** to access the TSAPI Service on Avaya AES server. Scroll down to the bottom of the page and click **Apply** (not shown).

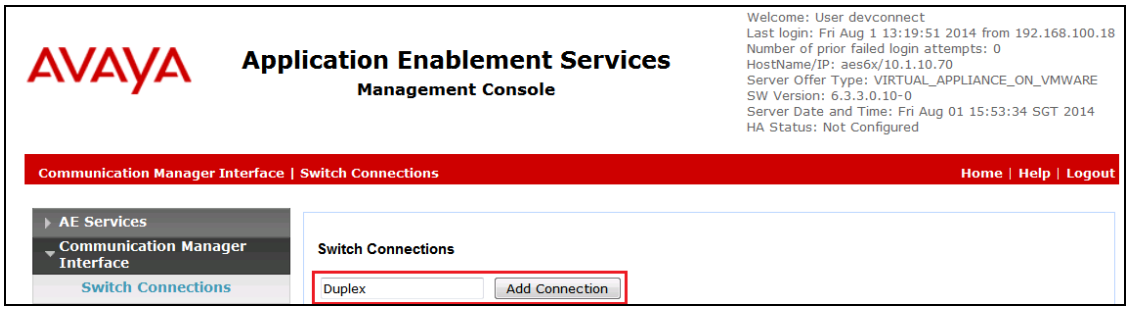
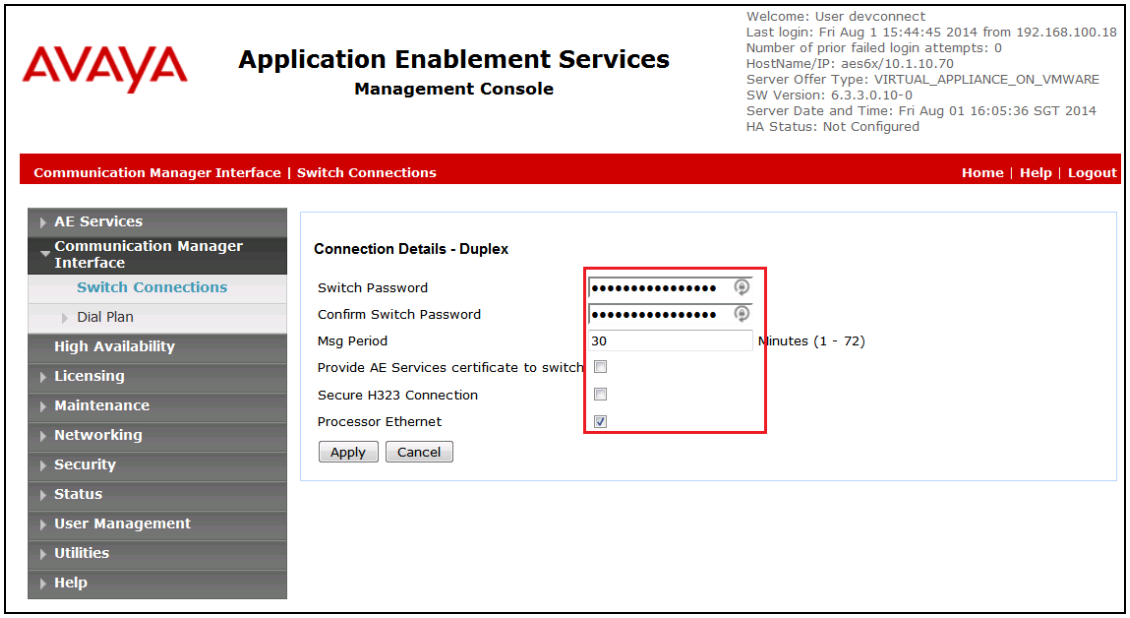


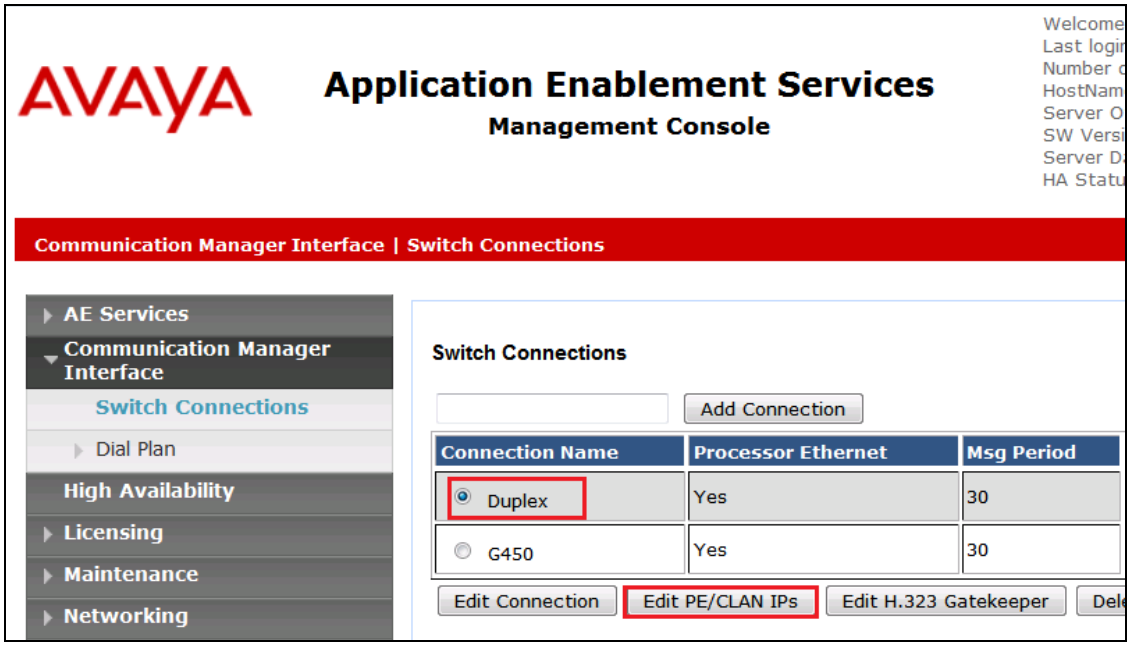
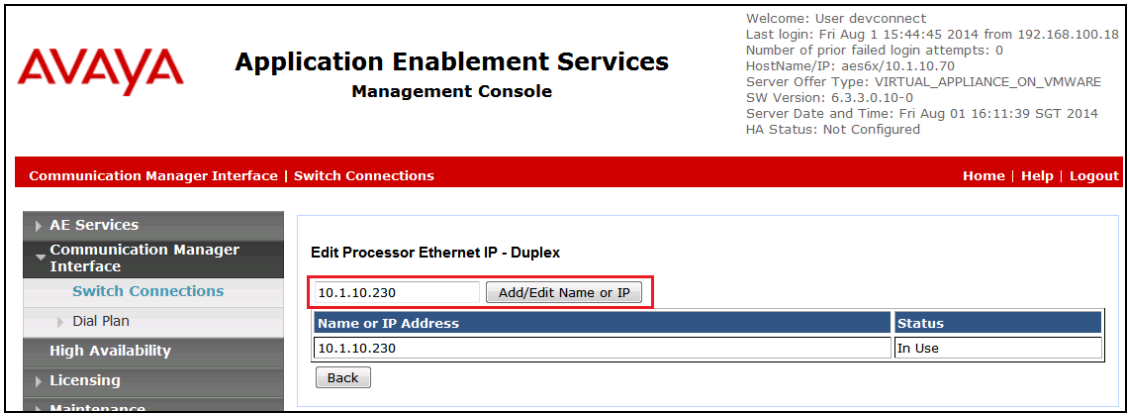
6.2. Verify Avaya Application Enablement Services License

Step	Description
1.	Select **Status f**rom the Welcome to OAM Screen page. Verify that 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.

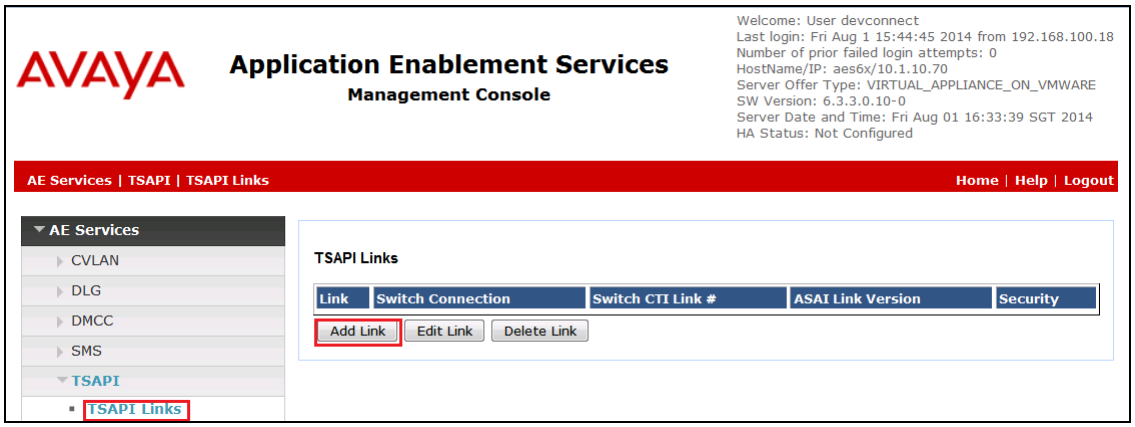
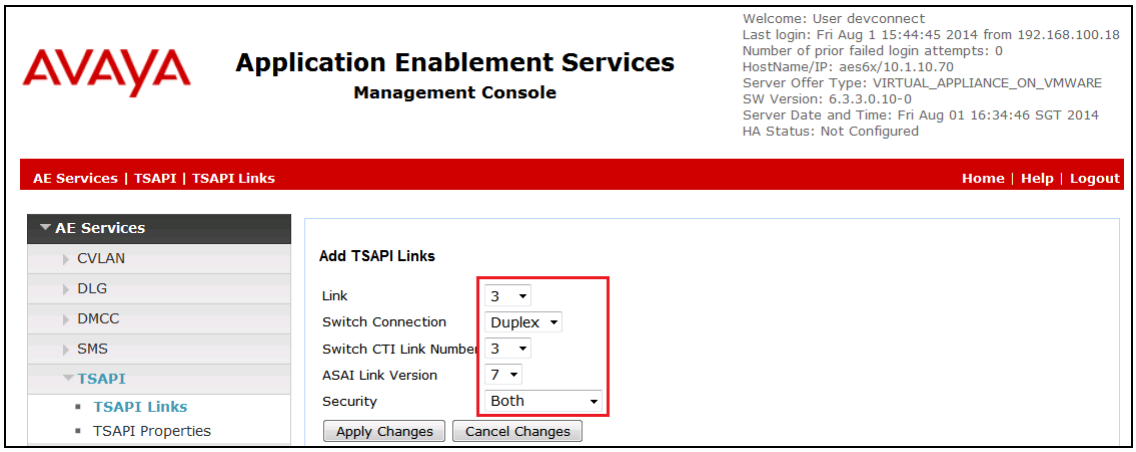


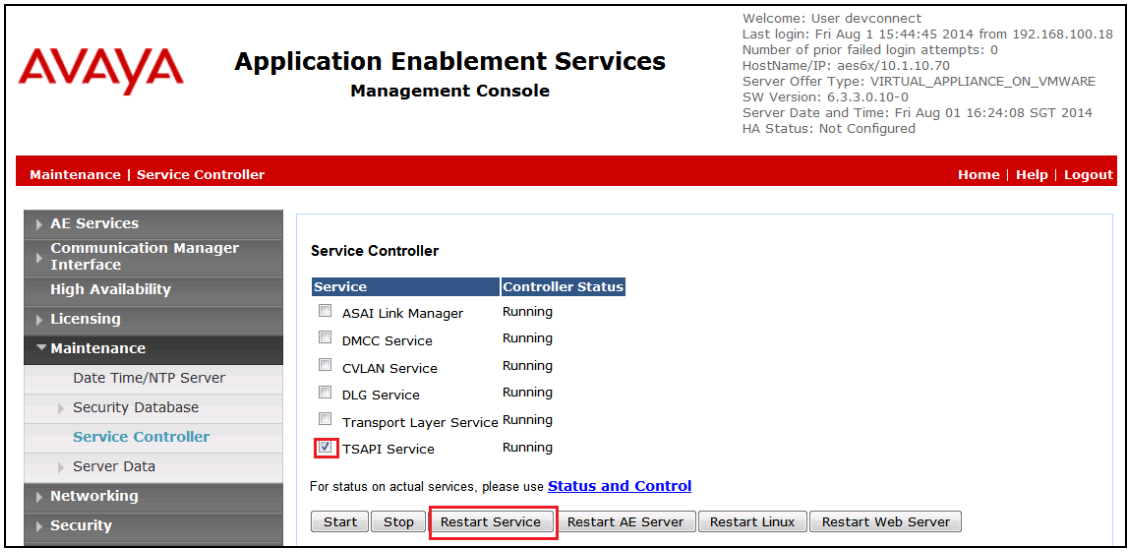
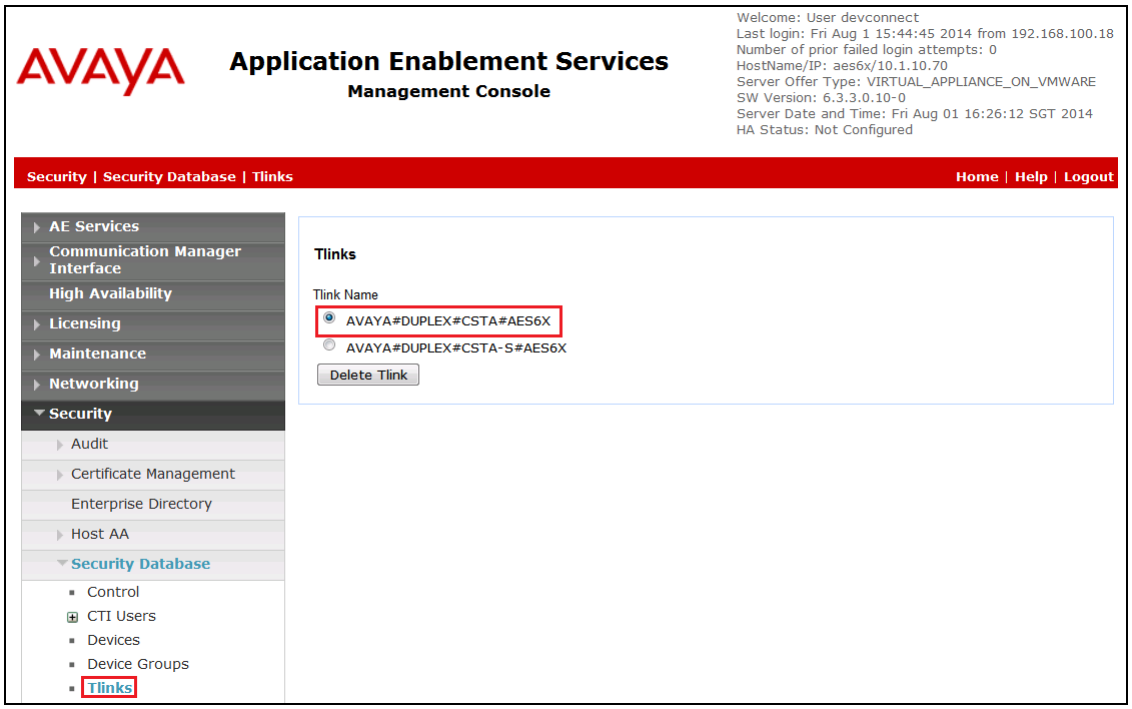
6.3. Administer Switch Connection

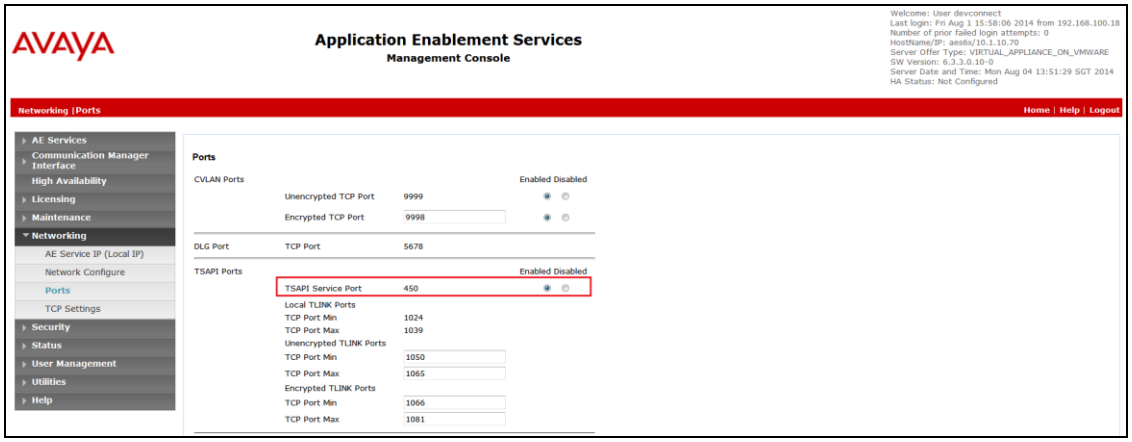
Step	Description
1.	From the Home menu, select **Communication Manager Interface → Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this configuration, **Duplex** is used. 
2.	The **Connection Details – Duplex** screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Avaya Communication Manager using the IP Services form in **Section 5.1 Step 4**. Here we are using the **Processor Ethernet** as well for connection and the field needs to be checked. Click on **Apply** to effect changes. 

Step	Description
3.	The Switch Connections screen is displayed. Select the newly added switch connection name and click **Edit PE/CLAN IPs**. 
5.	In the **Edit Processor Ethernet IP – Duplex** screen, enter the host name or IP address of the PE/C-LAN used for AES connectivity. In this case, **10.1.10.230** is used, which corresponds to the Common IP address of the Avaya Communication Manager. Click **Add/Edit Name or IP**. 

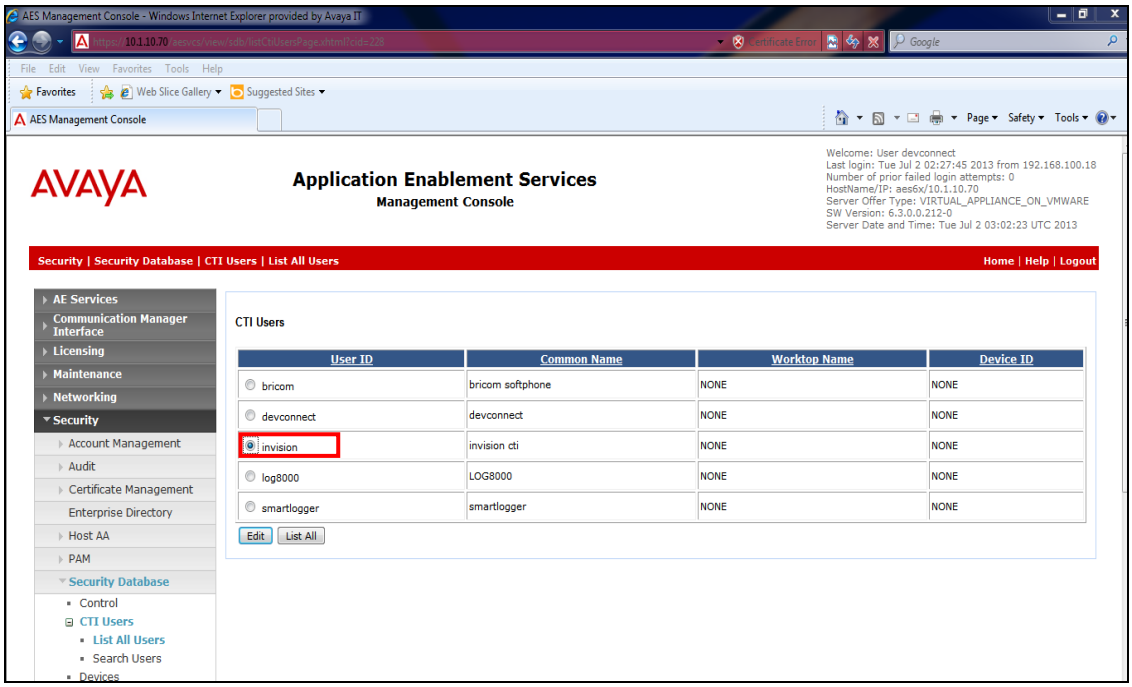
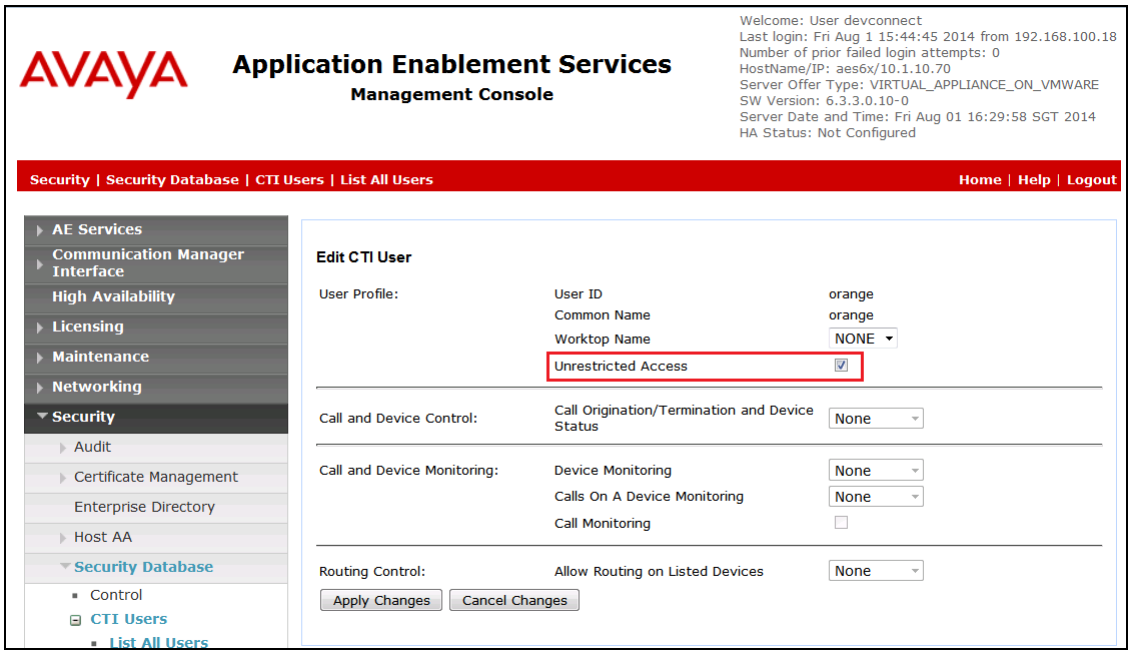
6.4. Administer TSAPI Link and Verify TSAPI Service Port

Step	Description
1.	To administer a TSAPI link on AES, select **AE Services → TSAPI → TSAPI Links** from the Home Menu. Click **Add Link**. 
2.	In the **Add TSAPI Links** screen, select the following values: • **Link:** Select an available Link number from 1 to 16. • **Switch Connection:** Administered switch connection in **Section 6.3 Step 1**. • **Switch CTI Link Number:** Corresponding CTI link number in **Section 5.1 Step2**. • **ASAI Link Version:** Set to **7** for the latest version. • **Security:** Select **Both** to allow for encrypted or unencrypted link. Note that the actual values may vary. Click **Apply Changes**. 

Step	Description
3.	To restart the TSAPI Service, select **Maintenance → Service Controller** from the Home menu. Check the **TSAPI Service** checkbox and click **Restart Service**. 
4.	Navigate to the Tlinks screen by selecting **Security → Security Database → Tlinks** from the Welcome to OAM home menu. Note the value of the **Tlink Name**, as this will be needed to configure the Orange Softphone Server in **Section 7**. In this configuration, the unencrypted **Tlink Name AVAYA#DUPLEX#CSTA#AES6X,** which is automatically assigned by the Avaya AES server, is used. 

Step	Description
5.	Navigate to the networking ports by **Networking → Ports** from the Welcome to OAM home menu. Verify that the default **TSAPI Service Port 450** is enabled. 

6.5. Administer CTI User Permission

Step	Description
1.	Select **Security → Security Database → CTI Users → List All Users** from the AES Management Console Home menu. Select the **User ID** created in **Section 6.1 Step 2** and click **Edit**. 
2.	Tick the **Unrestricted Access** box. Click **Apply Changes**. 

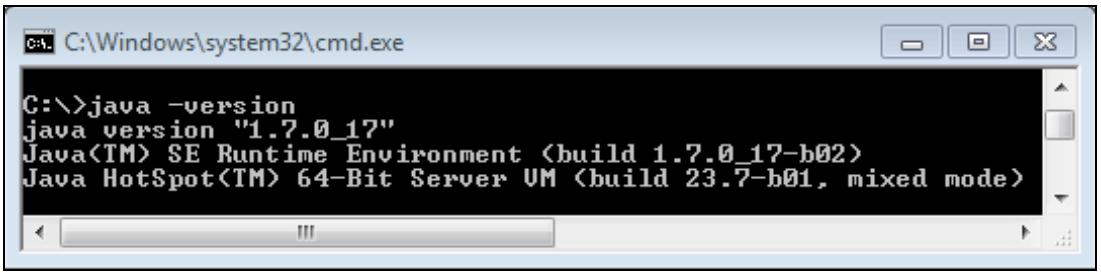
7. Configure Orange Softphone

This section highlights the configuration of Orange softphone which includes the following areas:

- Verify the pre-requisites
- Configure Orange Softphone

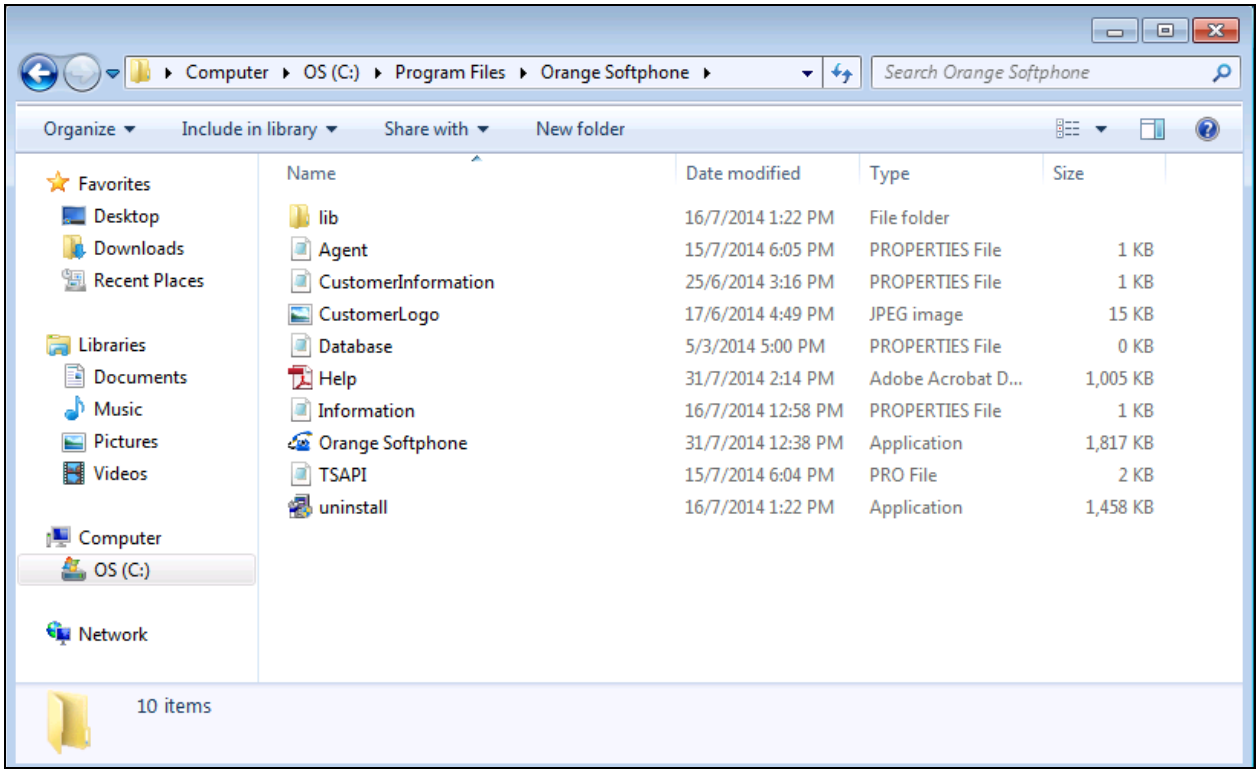
7.1. Check the pre-requisites

Orange softphone works on Microsoft Windows XP and Microsoft Windows 7 operating systems and requires Java Runtime environment to be installed. Run the following command prompt in Windows to verify that Java 1.7 is installed.



7.2. Configure Orange Softphone

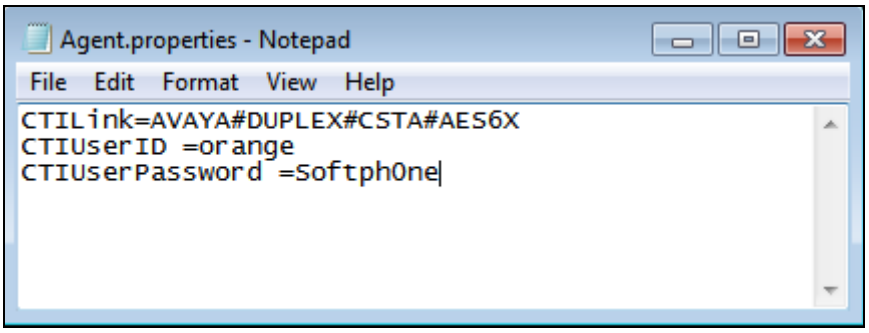
Orange softphone will be deployed using Apache Tomcat 6 by Orange Business Services personnel using "AgenThinApplication.war" file. The package is installed at the default location "C:\Program Files\Orange Softphone" unless altered. After installation, the setup of Orange Softphone folder in the default location is as shown below.



The following properties files are verified after deployment:

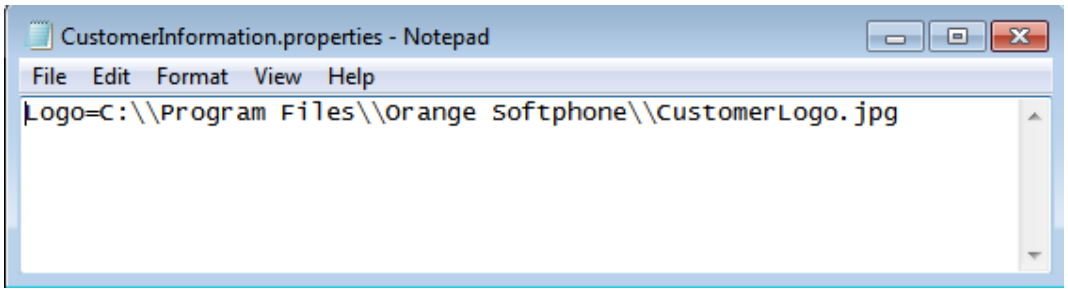
1. Agent Properties

CTILink - Correspond to the unencrypted TLink name created by Avaya AES server shown in **Section 6.4 Step 4**
CTIUserID - CTI User ID created in **Section 6.1**
CTI UserPassword - CTI User password created in **Section 6.1**



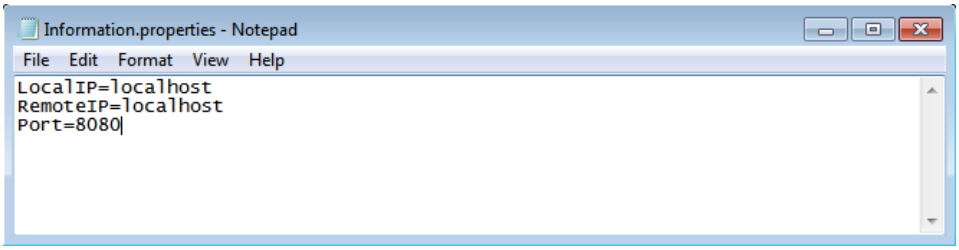
2. CustomerInformation.properties

The customer company logo can be loaded as a jpeg file by specifying the location.



3. Information.properties

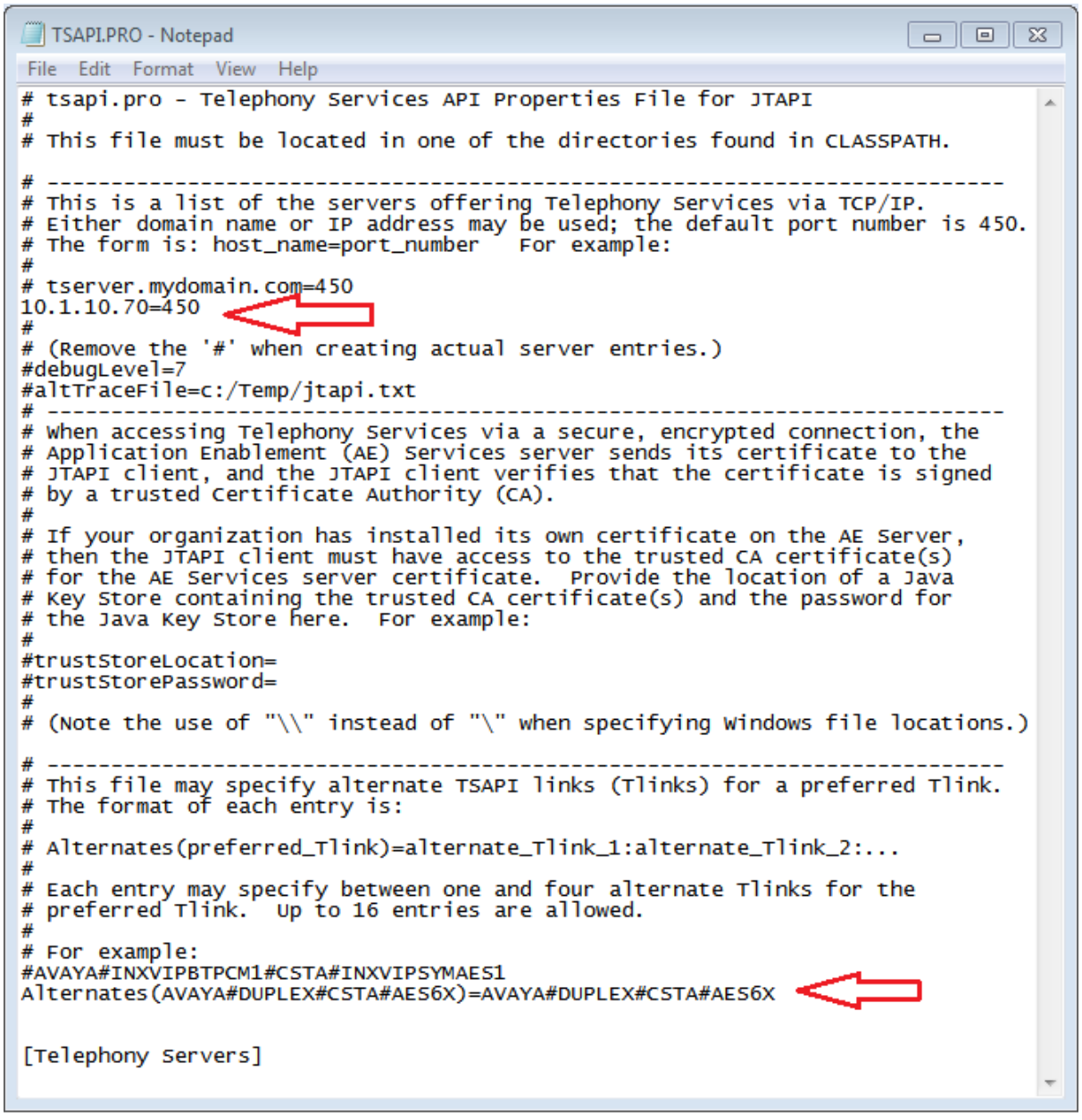
LocalIP - Orange Softphone local address
RemoteIP - Apache Tomcat server IP address
Port - Apache Tomcat Port No



4. TSAPI.pro

Telephony Services IP address:port - Avaya AES ip address 10.1.10.70 with default port specified in **Section 6.4 Step 5**.

TSAPI links - TLink name specified in **Section 6.4 Step 4**.



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 Orange Softphone.

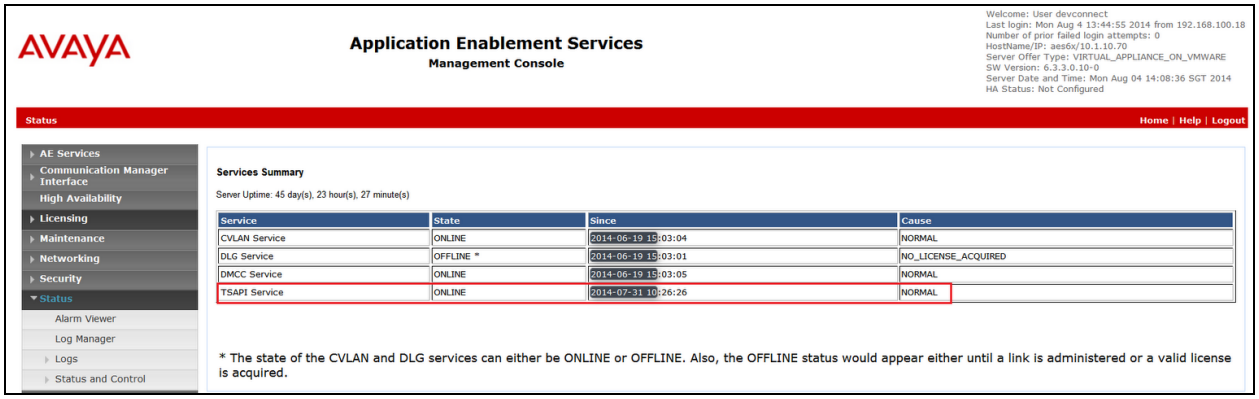
8.1. Verify Avaya Communication Manager

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

1               no                      down          0        0
2               no                      down          0        0
3      7        no     aes6x            established   15       15
```

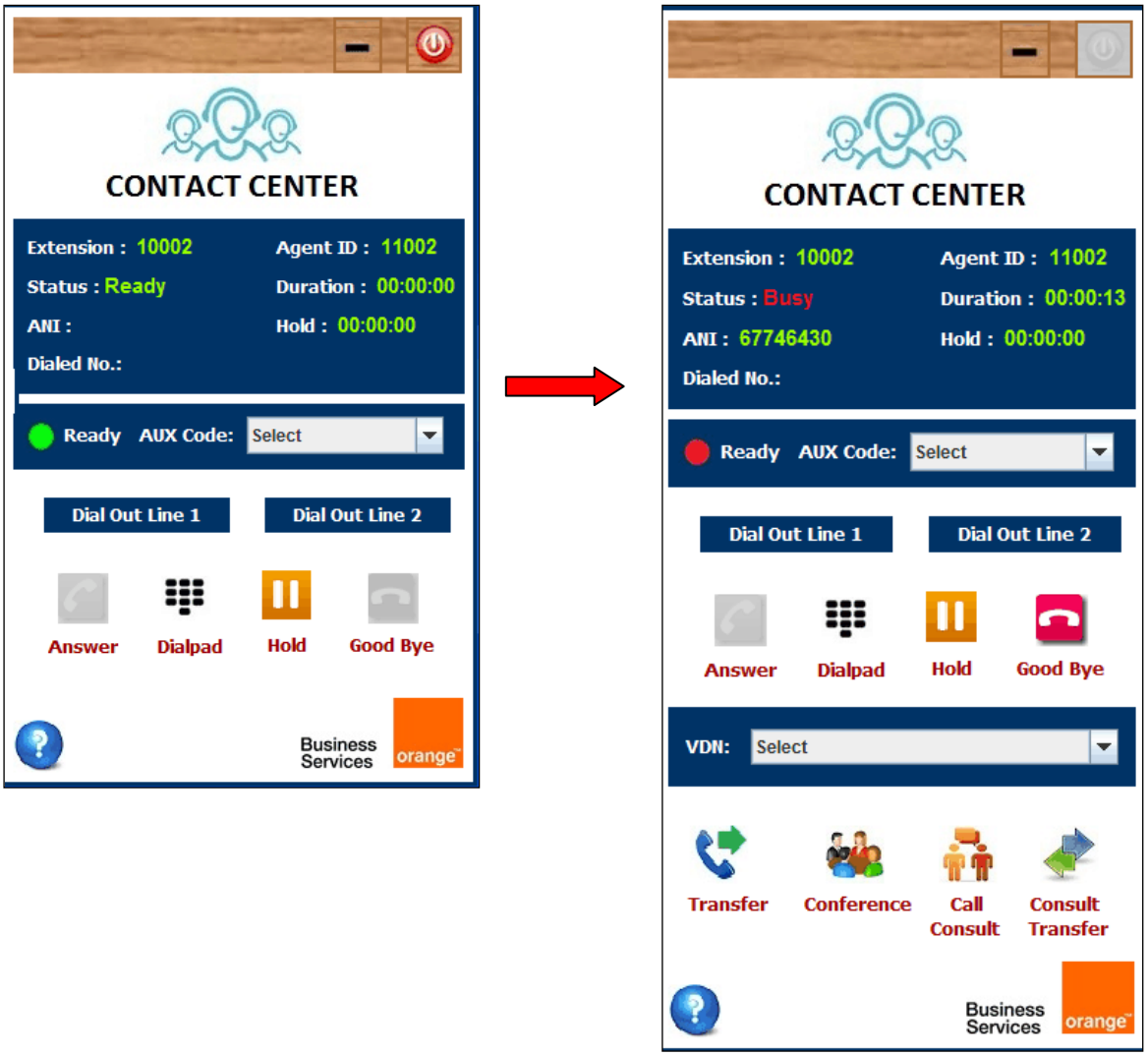
8.2. Verify Avaya Application Enablement Services

From the Welcome to OAM web pages, verify the status of the TSAPI Service by selecting **Status**. The **State** field for the **TSAPI Service** should display **NORMAL**.

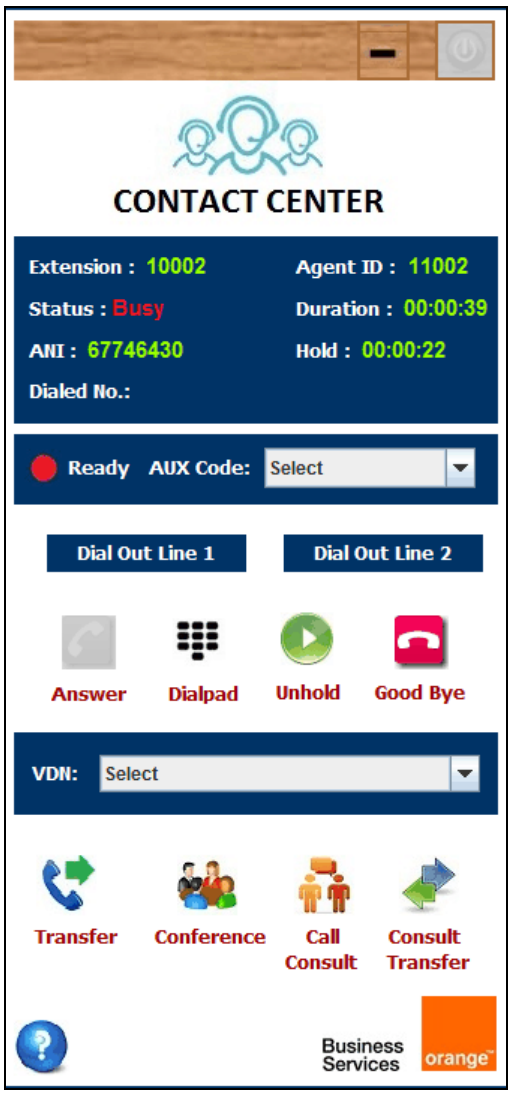


8.3. Verify Orange Softphone

Make an incoming call to any one of the login agents. Verify the agent desktop is now expanded with call control functionality (transfer, conference, call consult and consult transfer) visible at the bottom of the interface. The **Good Bye** button gets enabled, the **ANI** details is presented and the **Busy** mode is displayed for **Status**. Verify also that the **Duration** timer is counting.



Put the call on hold by pressing the orange **Hold** soft button. Verify the green **Unhold** image is displayed and the **Hold** timer is counting.



9. Conclusion

These Application Notes describe the configuration steps required for Orange Softphone to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Telephony Services Application Programming Interface (TSAPI). All feature test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

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

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

[1] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Document Number 02—300357, Release 6.3, Jun 2014.
[2] *Avaya Aura® Avaya Communication Manager Feature Description and Implementation*, Document Number 555-245-205, Issue 11, Oct 2013.

The following product documentations are available from Orange Business Services.

[3] *Installation Guide for Orange Softphone Version 1.0*
[4] *Manual for Orange Softphone Version 2.0*
[5] *Help for Orange Softphone Version 2.0*
[6] *Troubleshooting User Guide for Orange Softphone Version 1.0*