



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Jacada Workspace Agent Desktop to Interoperate 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 for Jacada Workspace Agent Desktop to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Jacada Workspace Agent Desktop integrates with Avaya Aura® Application Enablement Services using TSAPI for Computer Telephony Integration.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the 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 for Jacada Workspace Agent Desktop to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3. Jacada Workspace Agent Desktop communicates with telephone sets on Avaya Aura® Communication Manager using the JTAPI API which uses a TSAPI connection on Avaya Aura® Application Enablement Services (AES).

Jacada Workspace Agent Desktop is a call center unified desktop solution that is purpose built to provide an improved customer service experience by streamlining the agents interactions with a large number of systems.

Note: JTAPI API uses the TSAPI connection on AES. Throughout this document any reference to either JTAPI or TSAPI should be considered as the same connection type.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated Jacada Workspace Agent Desktop to integrate correctly with AES and Communication Manager using the TSAPI link on the AES to gain third-party call control of Communication Manager telephones. A number of compliance tests were carried out using Workspace Agent Desktop to make, receive, hold and transfer calls.

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 both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Agent state change**– Make agent Ready/Not Ready using Workspace Agent Desktop.
- **Inbound Calls** – Answer calls using Workspace Agent Desktop.
- **Outbound Calls** – Make calls using Workspace Agent Desktop.
- **Call Hold** – Place calls on hold and retrieve calls using Workspace Agent Desktop.
- **Blind Transfer** – Transfer callers using Workspace Agent Desktop
- **Consultative Transfer** - Transfer callers using Workspace Agent Desktop.
- **Inbound Skillset Calls** – Answer skillset/VDN calls using Workspace Agent Desktop.
- **Failover Testing** - Verify the ability of Workspace Agent Desktop to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

Most functionality and serviceability test cases were completed successfully. The following issues and observations were noted.

Issues:

1. Hold/Unhold when calling from Agent 1 to Agent 2. When Agent 1 presses Hold on Workspace Agent Desktop and then Agent 2 presses Hold on hard phone, the CTI link on Agent 1 is broken.
2. Call Forward no Answer from Agent 1 to Agent 2 results in the call being answered automatically on the Agent 2 Workspace Agent Desktop, but the call needs to be answered manually on the phone set.

Observations:

1. No CLID/CPND information on Workspace Agent Desktop for non VDN calls (both internal and PSTN calls to the agents DN key).
2. If calls are left up for a long duration without interaction with the browser, the browser will automatically logout. When the agent logs back in again, the CTI ceases to work. To extricate from this situation, the agent needs to manually hang up the call and logout manually and then log back in using the browser. This timeout is configurable in Jacada WorkSpace Agent Desktop.
3. CRM data is only passed to Agent 2 if Agent 1 leaves the conference.
4. There is no CRM data passed when a “Blind” or “Cold” transfer is performed from Agent 1 to Agent 2. CRM data is passed for warm and handshake transfers.
5. There is no automatic recovery from a LAN failure between the AES and Workspace Agent Desktop Server.

2.3. Support

Technical support can be obtained for Jacada Workspace Agent Desktop from the website <http://www.jacada.com/about/jacada-worldwide-offices>

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test Workspace Agent Desktop with Communication Manager using a CTI connection through AES to gain call control of the Avaya one-X® Agent softphone and the Avaya H.323 deskphone.

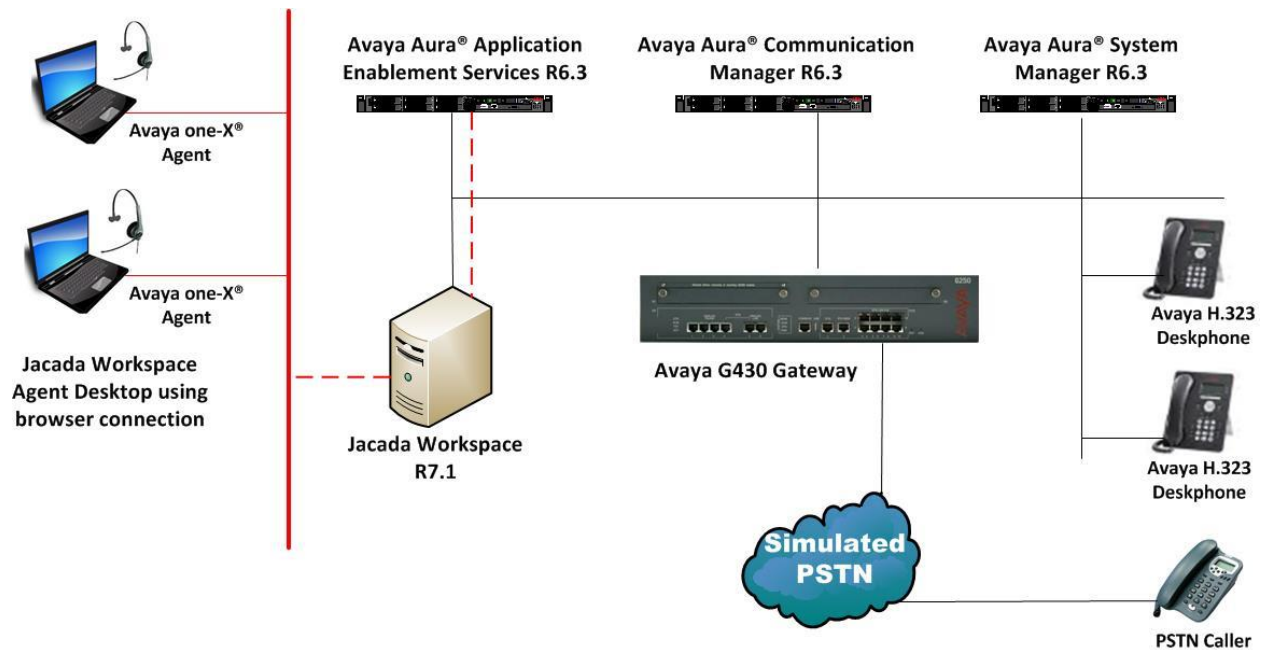


Figure 1: Connection of Jacada Workspace Agent Desktop with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Avaya S8800 Server	System Manager 6.3.7 Build No. - 6.3.0.8.5682-6.3.8.3204 Software Update Revision No: 6.3.7.7.2275
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.3 SP6 R016x.03.0.124.0
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.3 Build No - 6.3.0.0.212-0
Avaya G430 Gateway	R6.3
Avaya 96xx/96x1 Series Deskphone	96xx H.323 Release 3.1 SP2
Avaya one-X® Agent	R2.5
Jacada Workspace Agent Desktop	V 7.1

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

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?	y	DCS (Basic)?	y		
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y		
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y		
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y		
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y		
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y		
ATMS?	y				
Attendant Vectoring?	y				

5.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes63vmpg**).

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM100	10.10.40.34	
aes63vmpg	10.10.40.30	
default	0.0.0.0	
g430	10.10.40.15	
procr	10.10.40.31	

5.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 5.10**.
- **Local Port:** Retain the default value of **8765**.

change ip-services					Page	1 of	4
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	procr	8765				

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes63vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services				Page	4 of 4
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	aes63vmpg	*****	y	idle	
2:					
3:					

5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add	cti-link 1	Page	1 of	3
		CTI LINK		
CTI Link: 1				
Extension: 2002				
Type: ADJ-IP				
COR: 1				
Name: aes63vmpg				

5.5. Configure Agent Stations

It is assumed that all agent stations are already properly configured and that all monitored phones are already in place. Please refer to the Appendix for a printout of the following that were used during compliance testing.

- Avaya 9620 Deskphone
- Avaya one-X Agent Softphone
- Agent 4400

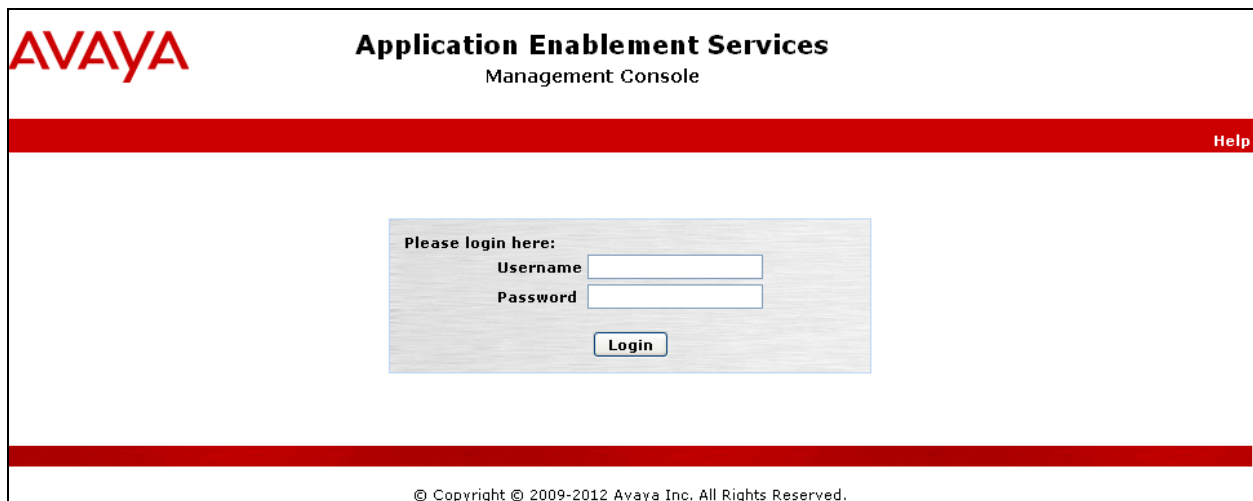
6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Set Up Security Database on AES
- Associate Devices with CTI User

6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button. At the bottom of the page, a red horizontal bar contains the copyright notice: "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Wed Dec 12 10:45:16 2012 from 192.168.10.209
Number of prior failed login attempts: 0
HostName/IP: aes62vmgpg.devconnect.local/10.10.40.10
Server Offer Type: SWONLY
SW Version: r6-2-0-18-0
Server Date and Time: Thu Dec 20 11:51:08 UTC 2012

AE Services Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ TWS
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMGPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 3 15:33:26 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

▼ AE Services

- ▶ Communication Manager Interface
- Switch Connections**
- ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Switch Connections

CM63VMGPG Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 3 15:35:47 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Connection Details - CM63vmpg

Switch Password: [Redacted]
Confirm Switch Password: [Redacted]
Msg Period: 30 Minutes (1 - 72)
SSL: ☒
Processor Ethernet: ☒
Apply Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown, see screen at the bottom of page 10). In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 15:36:31 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit Processor Ethernet IP - CM63vmpg

10.10.40.31 Add/Edit Name or IP

Name or IP Address	Status
10.10.40.31	In Use

Back

6.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top navigation bar includes the AVAYA logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links", "TSAPI Properties", and "Communication Manager Interface". The main content area is titled "TSAPI Links" and contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are three buttons: "Add Link", "Edit Link", and "Delete Link". The "Add Link" button is highlighted with a red box.

On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM63VMPG**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.

The screenshot shows the AVAYA Application Enablement Services Management Console, specifically the "Edit TSAPI Links" screen. The top navigation bar and left sidebar are identical to the previous screenshot. The main content area is titled "Edit TSAPI Links" and contains a form with the following fields: "Link" (set to 1), "Switch Connection" (set to CM63vmpg), "Switch CTI Link Number" (set to 1), "ASAI Link Version" (set to 5), and "Security" (set to Both). The "Switch Connection" field is highlighted with a red box. At the bottom of the form are three buttons: "Apply Changes", "Cancel Changes", and "Advanced Settings". The "Apply Changes" button is highlighted with a red box.

Another screen appears for confirmation of the changes made. Choose **Apply**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

AE Services | TSAPI | TSAPI Link Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ **TSAPI**
 - **TSAPI Links**
 - TSAPI Properties
- ▶ Communication Manager Interface

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
Please use the Maintenance -> Service Controller page to restart the TSAPI server.

Apply **Cancel**

When the TSAPI Link is completed, it should resemble the screen below.

AVAYA Application Enablement Services Management Console

Last login: Tue Dec 3 15:32:14 2013 from 10.10.40.225
Number of prior failed login attempts: 17
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 16:34:53 UTC 2013

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ **TSAPI**
 - **TSAPI Links**
 - TSAPI Properties

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM63Vmpg	1	5	Both

Add Link **Edit Link** **Delete Link**

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

Maintenance | Service Controller Home | Help | Logout

▶ AE Services

- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ **Maintenance**
 - Date Time/NTP Server
 - ▶ Security Database
 - **Service Controller**
 - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start **Stop** **Restart Service** **Restart AE Server** **Restart Linux** **Restart Web Server**

6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the Tlink Group in **Section 6.7.2**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar contains the links "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services, with "Security" expanded to show "Security Database", which in turn has "Tlinks" highlighted with a red box. The main content area, titled "Tlinks", shows a "Tlink Name" field with two radio button options: "AVAYA#CM63VMPG#CSTA#AES63VMPG" (selected) and "AVAYA#CM63VMPG#CSTA-S#AES63VMPG". A "Delete Tlink" button is located below the options.

6.5. Enable TSAPI Ports

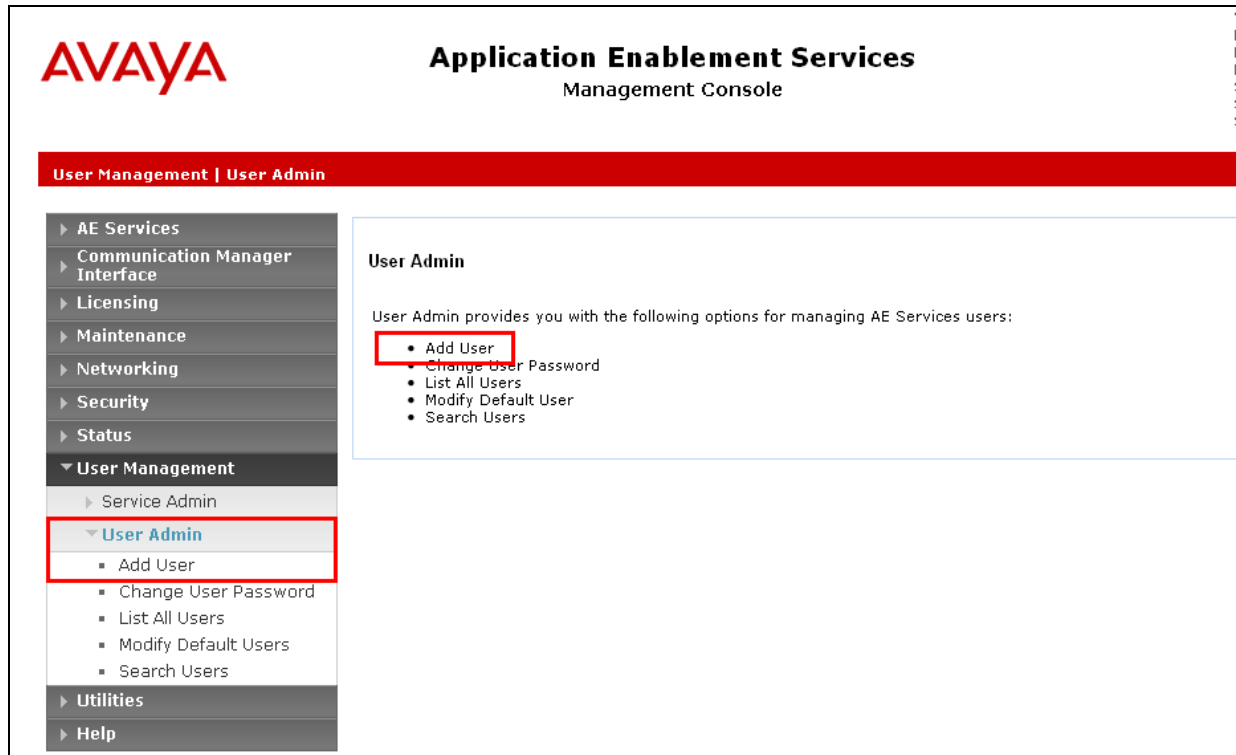
To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

The screenshot displays the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking (expanded), AE Service IP (Local IP), Network Configure, Ports (highlighted with a red box), TCP Settings, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Ports' and shows configuration for CVLAN Ports and TSAPI Ports. The CVLAN Ports section includes Unencrypted TCP Port (9999) and Encrypted TCP Port (9998), both with 'Enabled' radio buttons selected. The TSAPI Ports section includes TSAPI Service Port (450) with an 'Enabled' radio button selected (highlighted with a red box), Local TLINK Ports (TCP Port Min: 1024, TCP Port Max: 1039), Unencrypted TLINK Ports (TCP Port Min: 1050, TCP Port Max: 1065), and Encrypted TLINK Ports (TCP Port Min: 1066, TCP Port Max: 1081).

Ports	
CVLAN Ports	
Unencrypted TCP Port	9999
Encrypted TCP Port	9998
DLG Port	
TCP Port	5678
TSAPI Ports	
TSAPI Service Port	450
Local TLINK Ports	
TCP Port Min	1024
TCP Port Max	1039
Unencrypted TLINK Ports	
TCP Port Min	1050
TCP Port Max	1065
Encrypted TLINK Ports	
TCP Port Min	1066
TCP Port Max	1081

6.6. Create CTI User

A User ID and password needs to be configured for the Jacada Workspace server to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Workspace server setup in **Section 7.2**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **CTIPassword** in **Section 7.2**.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen (not shown).

AVAYA Application Enablement Services Management Console

User Management | User Admin | List All Users

AE Services

- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management**
 - Service Admin
 - User Admin**
 - Add User**
 - Change User Password
 - List All Users
 - Modify Default Users
 - Search Users
- Utilities
- Help

Edit User

* User Id

* Common Name

* Surname

User Password

Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Ccs Home

CT User

Department Number

Display Name

Employee Number

Employee Type

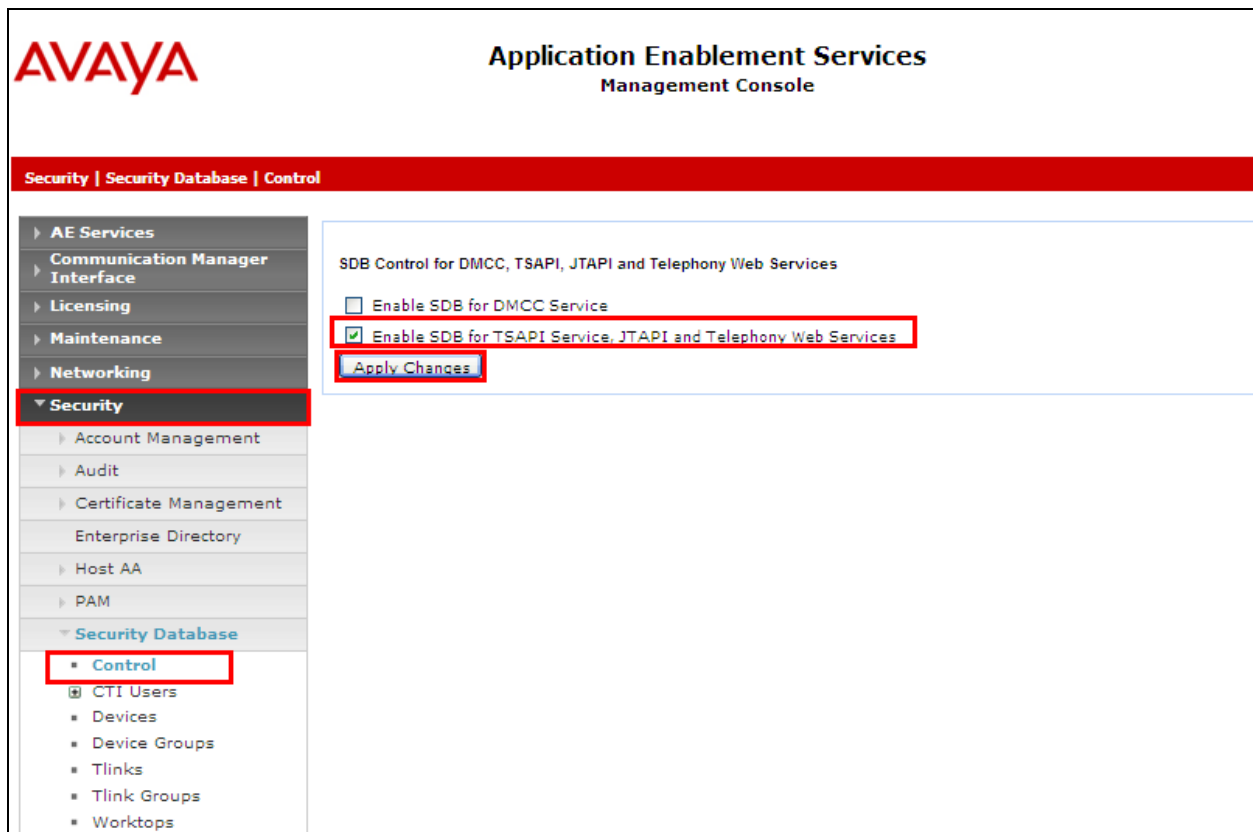
The next screen will show a message indicating that the user was created successfully (not shown).

6.7. Set Up Security Database on Avaya Aura® Application Enablement Services

In order for the Jacada Workspace Agent Desktop to monitor the phone sets and agents on Communication Manager the security database on AES needs to be setup correctly. Every device must be added to a device group and this device group assigned to the CTI user created in **Section 6.6**.

6.7.1. Enable Security Database for TSAPI

Navigate to **Security** → **Security Database** → **Control**. Tick the box for **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** and click **Apply Changes**.



6.7.2. Create a Tlink Group

Navigate to **Security** → **Security Database** → **Tlink Groups** in the left window. In the main window enter a suitable name for the group and click on **Add Tlink Group**.

AVAYA Application Enablement Services Management Console

Security | Security Database | Tlink Groups

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users
Search Users
Devices
Device Groups
Tlinks
Tlink Groups
Worktops

Tlink Groups

Jacada Add Tlink Group

	Tlink Group
<input type="checkbox"/>	jacada

Edit Tlink Group Delete Tlink Group(s)

Enter a suitable name for the **Tlink Group**, tick on the Tlink to be associated with the group and click on **Apply Changes**.

AVAYA Application Enablement Services Management Console

Security | Security Database | Tlink Groups

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Account Management
Audit

Add Tlink Group

Tlink Group Jacada

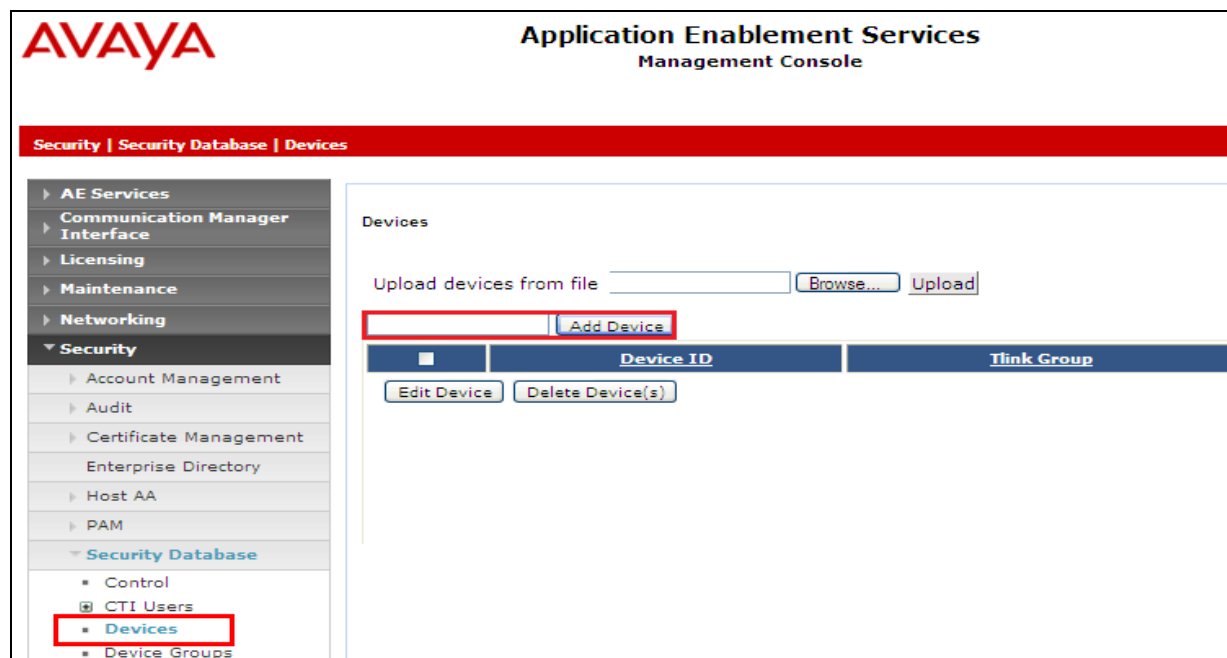
Tlinks

<input checked="" type="checkbox"/>	AVAYA=CM63VMPG=CSTA=AE63VMPG
<input type="checkbox"/>	AVAYA=CM63VMPG=CSTA-S=AE63VMPG

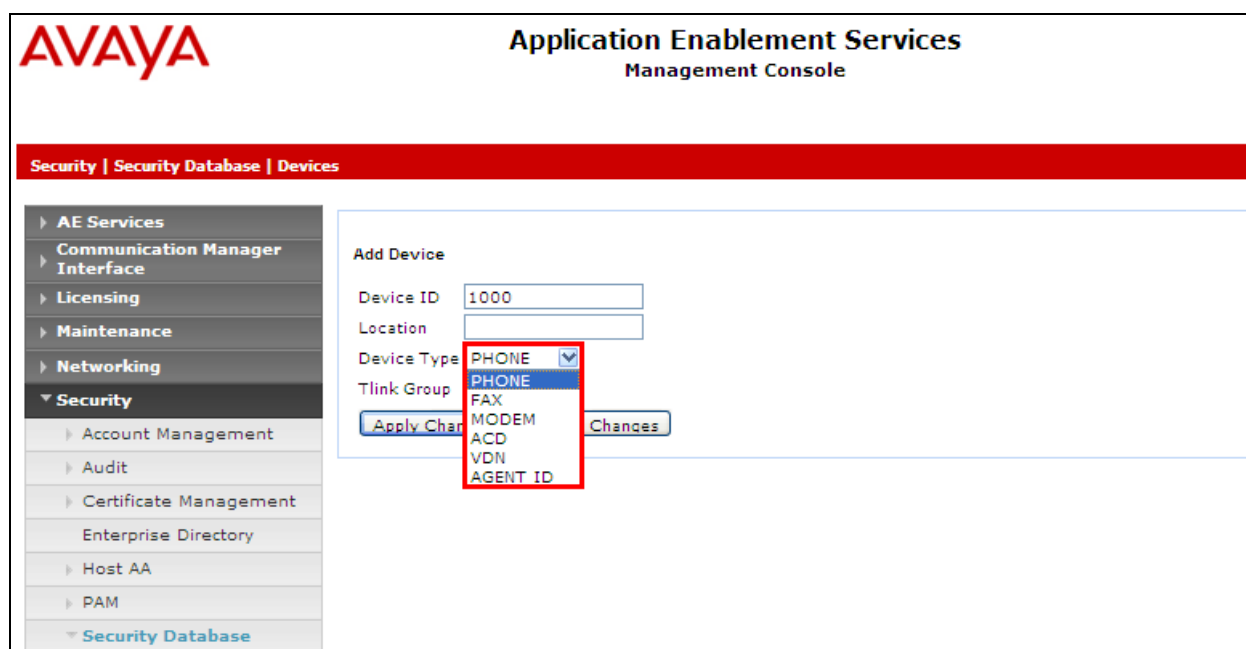
Apply Changes Select All Deselect All Cancel Changes

6.7.3. Add Devices

Every phone set, agent, hunt group, and VDN that needs to be monitored must be added to the security database in **Devices**. Navigate to **Security** → **Security Database** → **Devices**. In the main window enter the required number and click on **Add Device**.



The **Device Type** must be selected as shown in the example below for device **1000** being a **PHONE**.



The **Tlink Group** that was created in **Section 6.7.2** is selected.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. Under Security, there are sub-items: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, and Security Database. The main content area is titled 'Add Device' and contains the following fields: Device ID (1000), Location (empty), Device Type (PHONE), and Tlink Group (None). The Tlink Group dropdown menu is open, showing a list of options: None, None, Any, and jacada. The 'Apply Changes' button is highlighted in blue.

Once the proper values are inputted correctly click on **Apply Changes**.

This screenshot is identical to the one above, showing the 'Add Device' form in the Avaya Application Enablement Services Management Console. The 'Tlink Group' dropdown menu is open, showing options: None, None, Any, and jacada. The 'Apply Changes' button is highlighted in blue.

The following devices were added for the compliance test. Note that agents **4401** and **4402** would use phone sets **2000** and **2100** when logging into the **ACD** (or hunt group) **3330**; **VDN 3300** would be used to call into this group.

AVAYA Application Enablement Services Management Console

Security | Security Database | Devices

Devices

Upload devices from file

	Device ID	Tlink Group	Device Type	Location
<input type="checkbox"/>	2000	jacada	PHONE	Gal
<input type="checkbox"/>	2001	jacada	PHONE	Gal
<input type="checkbox"/>	2002	jacada	PHONE	Gal
<input type="checkbox"/>	2100	jacada	PHONE	Gal
<input type="checkbox"/>	3300	jacada	VDN	Gal
<input type="checkbox"/>	3330	jacada	ACD	Gal
<input type="checkbox"/>	4401	jacada	AGENT ID	Gal
<input type="checkbox"/>	4402	jacada	AGENT ID	Gal

6.7.4. Add Device Group

A **Device Group** must be added in order to group together the devices that were added above in **Section 6.7.3**. Navigate to **Security** → **Security Database** → **Device Groups**. In the main window enter a suitable name and click on **Add Device Group**.

AVAYA Application Enablement Services Management Console

Security | Security Database | Device Groups

Device Groups

	Device Group	Location
<input type="checkbox"/>	Jacada	N

Tick the devices that are to be added to the new device group and click on **Apply Changes**.

AVAYA Application Enablement Services Management Console

Security | Security Database | Device Groups

Edit Device Group

Device Group:

Exception Group: ☐

Devices:

- ☒ 1000
- ☒ 1001
- ☒ 2000
- ☒ 2001
- ☒ 2002
- ☒ 2100
- ☒ 3300
- ☒ 3330
- ☒ 4401
- ☒ 4402

☒ **Apply Changes**

Left sidebar menu:

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security**
 - Account Management
 - Audit
 - Certificate Management
 - Enterprise Directory
 - Host AA
 - PAM
 - Security Database**
 - Control
 - CTI Users
 - Devices
 - Device Groups**
 - Tlinks
 - Tlink Groups
 - Worktops

6.8. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users** and click on **Edit Users** (not shown). In the main window ensure that Unrestricted Access is not ticked. The device group created in **Section 6.7.4** is then associated with the CTI User created in **Section 6.6**. Assign the Device Group to **Call and Device Control** and **Call and Device Monitoring**. Once this is done click on **Apply Changes**.

AVAYA Application Enablement Services Management Console

Security | Security Database | CTI Users | List All Users

Edit CTI User

User Profile:

User ID: jacada

Common Name: jacada

Worktop Name:

☐ Unrestricted Access

Call and Device Control:

Call Origination/Termination and Device Status:

Call and Device Monitoring:

Device Monitoring:

Calls On A Device Monitoring:

Call Monitoring: ☒

Routing Control:

Allow Routing on Listed Devices:

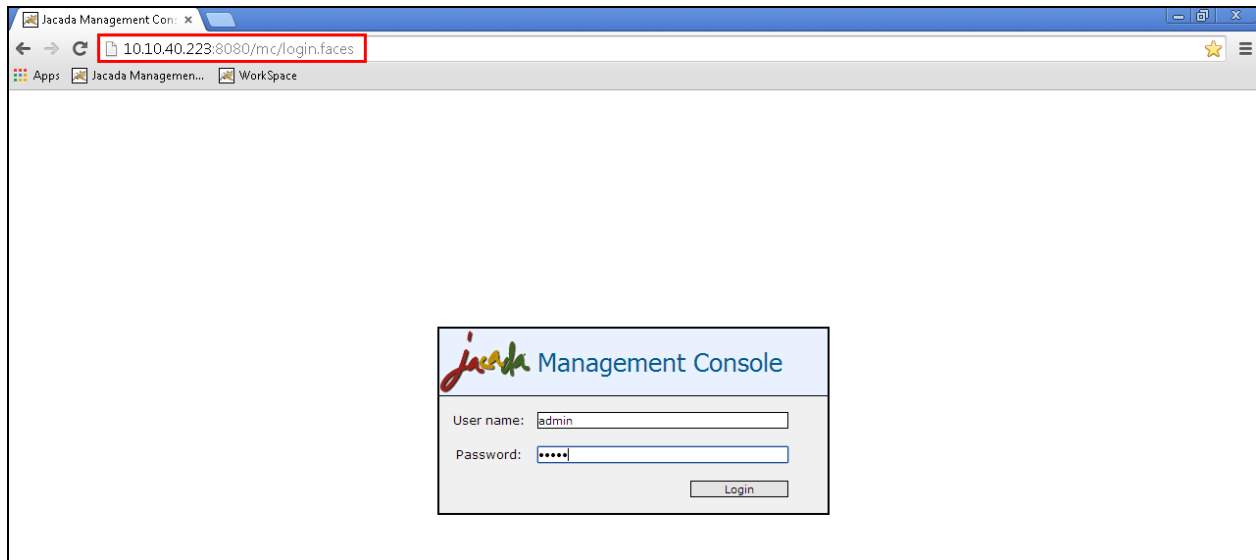
☒ **Apply Changes**

Left sidebar menu:

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security**
 - Account Management
 - Audit
 - Certificate Management
 - Enterprise Directory
 - Host AA
 - PAM
 - Security Database**
 - Control
 - CTI Users**
 - List All Users
 - Search Users

7. Configure Jacada Workspace Agent Desktop Server

The installation of Jacada Workspace is usually carried out by an engineer from Jacada, please refer to the documentation in **Section 10** for information on the installation and configuration of the Jacada Workspace Agent Desktop Server . The installation and configuration of Jacada Workspace is therefore outside the scope of these Application Notes. The following sections will outline the process involved in connecting the Jacada Workspace server to the AES. All configuration of the Jacada server for connection with the AES is performed using a web browser to the Jacada **Management Console**. Open a web browser as shown below and enter the proper credentials and click on **Login**. (Default user/pass is admin/admin).



7.1. Configure CTI Agents

Every agent configured on Communication Manager for use with Jacada Workspace Agent Desktop will need to be configured from the Jacada Management Console. From the left window navigate to **Configuration** → **CTI** → **Agents** and in the main window click on **Add**.

The screenshot shows the Jacada Management Console interface. The left sidebar contains a navigation menu with the following items: Monitoring, Configuration (expanded), Directory Settings, Dynamic Views Settings, EMC Settings, External Script Settings, Feature Settings, Global Settings, Human Task Settings, Instant Messaging Settings, Interact Settings, Locales, Machine Settings, Page Mappings, RSS Feed Definitions, RTN Mappings, Script Mappings, Smart Pad Settings, Supervisor View Settings, Agent Disposition, Auditing, Authentication-Authorization, CTI (expanded), Agents (highlighted), Busy Reason Codes, Dial List, Settings (expanded), Default, and CTI. The main content area shows the 'WorkSpace' tab with the breadcrumb 'WorkSpace > Configuration > CTI > Agents'. Below the breadcrumb is a link 'Show table properties >>'. A table lists existing agents:

User name	CTI profile	Extension number	Group ID	CTI login name	CTI password	Outbound extension number	Agent ID	Action
a2100		2100		4401	1234		4401	Edit
a4402		2002		4402	1234		4402	Edit

Below the table are 'Add' and 'Remove' buttons.

Enter the agent's credentials such as the **Extension number** associated with the agent along with **Agent ID**, **CTI login name** and **CTI password** that was configured on Communication Manager. Click on **Save** once these are entered correctly.

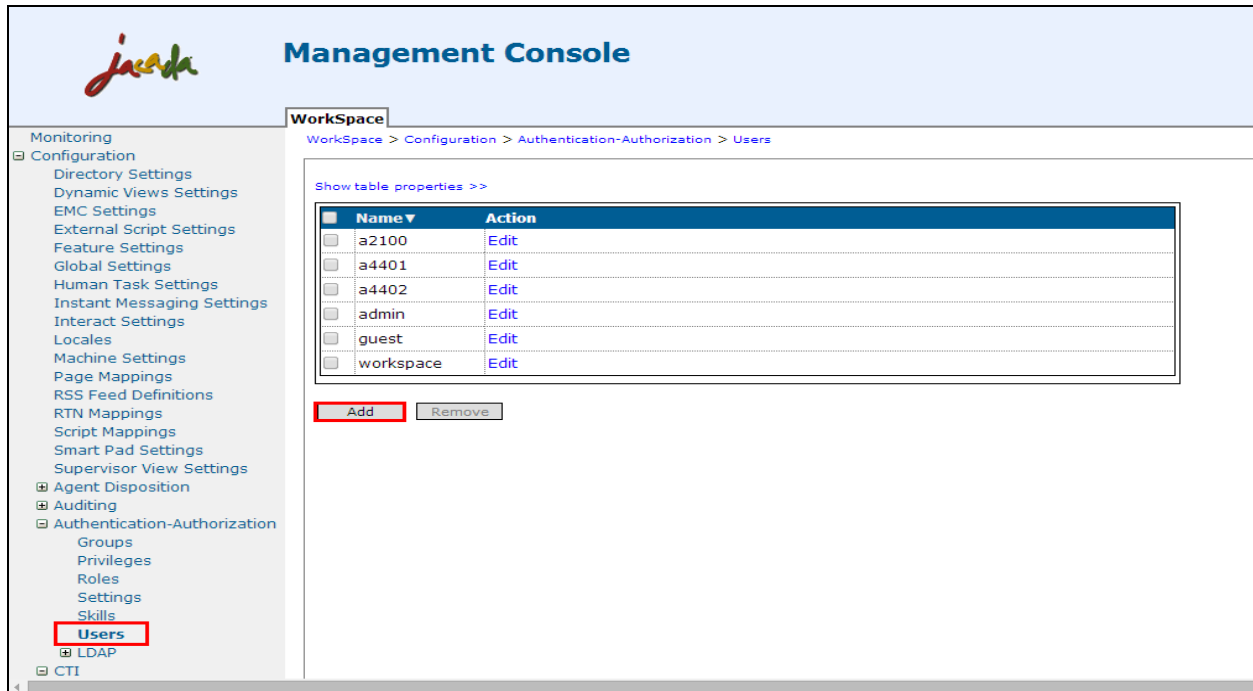
The screenshot shows the 'Edit CTI Agent' form in the Jacada Management Console. The left sidebar is the same as the previous screenshot. The main content area shows the 'WorkSpace' tab with the breadcrumb 'WorkSpace > Configuration > CTI > Agents'. Below the breadcrumb is a link 'Show table properties >>'. The form is titled 'Edit CTI Agent' and contains the following fields:

Edit CTI Agent	
User name:	a4402
CTI profile:	
Extension number:	2002
Group ID:	
CTI login name:	4402
CTI password:	1234
Outbound extension number:	
Agent ID:	4402

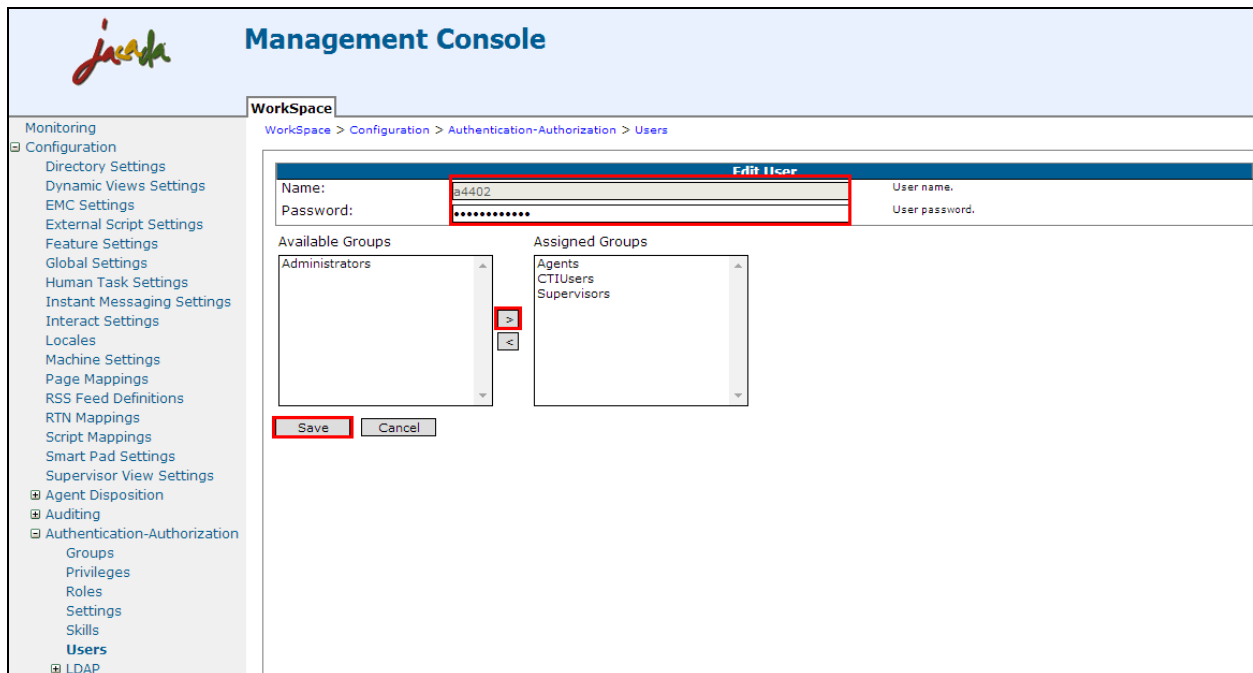
Below the form are 'Save' and 'Cancel' buttons. To the right of the form, there are several mandatory field descriptions:

- (Mandatory) The name of a user defined in the authentication provider, such as Microsoft Active Directory.
- The name of the CTI profile used by the agent.
- (Mandatory) The agent's telephone extension number.
- The ID of the group (queue) the agent belongs to.
- When required by the CTI server or the switch, the name used to log in to the extension.
- When required by the CTI server or the switch, the password used to log in to the extension.
- The telephone extension number to use for outbound calls.
- (Mandatory) A logical ID for an agent (CTI PHONEID).

From the left window navigate to **Configuration** → **Authentication-Authorization** → **Users** and in the main window click on **Add**.



Enter a **Name** and **Password** for each user to log into the Jacada Workspace Agent Desktop. Each user should be a part of the **Assigned Groups**. The minimum required groups are **Agents** and **CTIUsers** as shown below.



7.2. Configure AES connection in Management Console

From the left window navigate to **Configuration** → **CTI** → **Settings** → **AES**. In the main window the **Profile Settings** in blue must be edited. After the initial install these values will all be blank and they must be edited to show the values below with the CTIPassword and CTIUsername as configured in **Section 6.6**.

The screenshot shows the Jacada Management Console interface. The left sidebar contains a tree view of configuration categories. The main area displays the 'Profile Settings' table, which lists various configuration keys, their values, comments, and active status. The 'CTIPassword' and 'CTIUserName' fields are highlighted with red boxes. The 'Inherited Profile Settings' table below it shows a list of inherited settings.

Management Console

Workspace

Monitoring

- Configuration
 - Directory Settings
 - Dynamic Views Settings
 - EMC Settings
 - External Script Settings
 - Feature Settings
 - Global Settings
 - Human Task Settings
 - Instant Messaging Settings
 - Interact Settings
 - Locales
 - Machine Settings
 - Page Mappings
 - RSS Feed Definitions
 - RTN Mappings
 - Script Mappings
 - Smart Pad Settings
 - Supervisor View Settings
- Agent Disposition
- Auditing
- Authentication-Authorization
- CTI
 - Agents
 - Busy Reason Codes
 - Dial List
 - Settings
 - Default
 - CTI
 - CISCO
 - AES**

Workspace > Configuration > CTI > Settings > Default > CTI > AES

Profile Settings

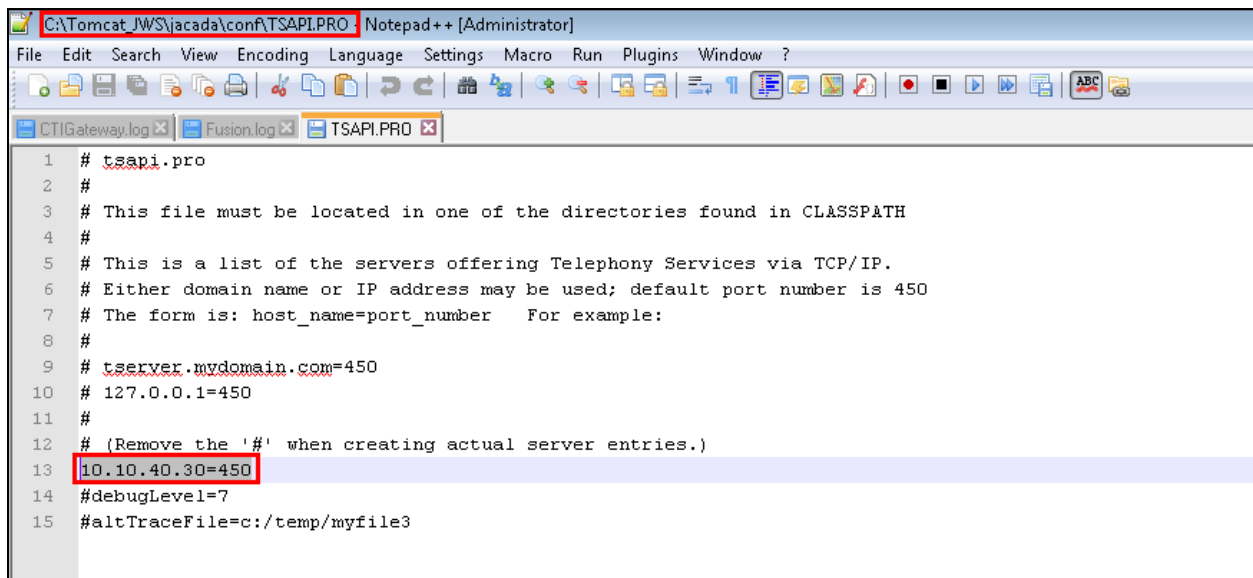
Key	Value	Comments	Active
CTIAgentStatusDuringCallSetBySwitch	true		<input checked="" type="checkbox"/>
CTIConfigurationMode	Agent		<input checked="" type="checkbox"/>
CTIPassword	*****		<input checked="" type="checkbox"/>
CTIProvider	AES		<input checked="" type="checkbox"/>
CTISwitchSendsRepeatedAgentStatusEvents	true		<input checked="" type="checkbox"/>
CTIUserName	jacada		<input checked="" type="checkbox"/>

Inherited Profile Settings

Key	Value	Comments	Active
CTIAgentStatusDuringCallSetBySwitch	true		<input checked="" type="checkbox"/>
CTIAllowDialPadWindow	true		<input checked="" type="checkbox"/>
CTIAllowTransferFromConsult	true		<input checked="" type="checkbox"/>
CTIApplicationSetACW	true		<input checked="" type="checkbox"/>
CTIBarEnabled	true		<input checked="" type="checkbox"/>
CTIBarUrl	Jacada.system.ui.cti.CTIBar		<input checked="" type="checkbox"/>
CTICallAutoAnswer	false		<input checked="" type="checkbox"/>
CTICallMode	inbound		<input checked="" type="checkbox"/>
CTIChangeToManualOnCTIOperationFailure	true		<input checked="" type="checkbox"/>
CTIDefaultNotReadyReasonCode	1		<input checked="" type="checkbox"/>
CTIDefaultTransferType	handshake		<input checked="" type="checkbox"/>

7.3. Configure AES connection on Workspace Agent Desktop Server

From the Workspace server the **TSAPIPRO** file must be edited to insert the AES IP address. This file can be opened in Notepad or **Notepad++**. Navigate to where this file is located on the Workspace server (**C:\Tomcat_JWS\jacada\conf\TSAPIPRO** in the example below). Enter the IP address of the AES as shown below using the default port **450** and ensure that the **#** is removed before the IP address. Save this file once this is completed.



```
1 # tsapi.pro
2 #
3 # This file must be located in one of the directories found in CLASSPATH
4 #
5 # This is a list of the servers offering Telephony Services via TCP/IP.
6 # Either domain name or IP address may be used; default port number is 450
7 # The form is: host_name=port_number   For example:
8 #
9 # tserver.mydomain.com=450
10 # 127.0.0.1=450
11 #
12 # (Remove the '#' when creating actual server entries.)
13 10.10.40.30=450
14 #debugLevel=7
15 #altTraceFile=c:/temp/myfile3
```

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the Avaya Aura® Application Enablement Services and Jacada Workspace Agent Desktop .

8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **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	4	no	aes63vmpg	established	18	18

8.2. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

Welcome: User craft
Last login: Thu Feb 20 11:01:32 2014 from 192.168.10.222
Number of prior failed login attempts: 33
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Thu Feb 20 11:14:02 UTC 2014

AVAYA Application Enablement Services Management Console

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
Alarm Viewer
Log Manager
Logs
Status and Control
CVLAN Service Summary
DLG Services Summary
DMCC Service Summary
Switch Conn Summary
TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	CM63vmpg	1	Talking	Tue Feb 18 11:21:49 2014	Online	16	5	15	15	30

Online Offline

For service-wide information, choose one of the following:
TSAPI Service Status TLink Status User Status

8.3. Verify Connection Between Avaya Aura® Application Enablement Services and Avaya Aura® Communication Management

A TSAPI test Application is included with AES. This application can be used to make a call from one deskphone to another on Communication Manager, this will confirm that 3rd Party Call Control is possible and therefore the connection from the Workspace server to the AES should be possible.

In the AES Management Console, navigate to **Utilities** → **Diagnostics** → **AE Service** → **TSAPI Test**. The TSAPI Test window is opened; enter the **User** and **Password** for the CTI user that was created in **Section 6.6**. Enter the **From** and **To** extension number for the call and click **Dial**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top navigation bar includes 'Utilities | Diagnostics | AE Services | TSAPI Test'. On the left, a sidebar menu shows 'Utilities' expanded, with 'Diagnostics' and 'AE Service' also expanded. Under 'AE Service', 'TSAPI Test' is highlighted with a red box. The main content area is titled 'TSAPI Test' and contains the following fields: 'TLink' (a dropdown menu showing 'AVAYA#CM63VMPG#CSTA#AES63VMPG'), 'User' (text input with 'jacada'), 'Password' (password input with masked characters), 'From' (text input with '2000'), and 'To' (text input with '2002'). A 'Dial' button, highlighted with a red box, is located at the bottom left of the form area.

If the connection is setup correctly deskphone 2000 will have initiated a call to deskphone 2002 and the following message will be displayed.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar contains the links "Utilities | Diagnostics | AE Services | TSAPI Test". On the left, a sidebar menu lists various categories: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", "Diagnostics", "AE Service", "ASAI Test", "DMCC Test", "TR/87 Test", "TSAPI Test", and "Server". The "Utilities" category is expanded, and the "TSAPI Test" option is highlighted with a red box. The main content area shows the "TSAPI Test Result" with the following text: "cstaMakeCall() succeeded!" and "cstaClearConnection() succeeded!". A "Back" button is located below the test results.

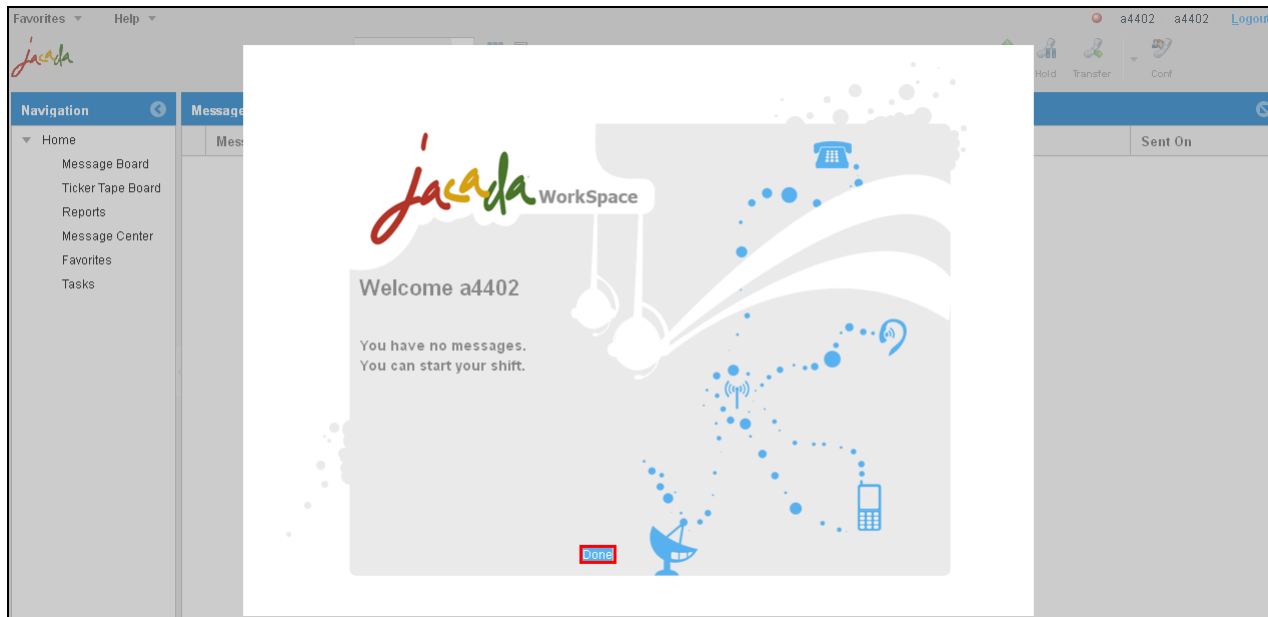
8.4. Verify 3rd Party Call Control From Jacada Workspace Agent Desktop

From an agent workstation open a web browser to the Jacada server. Log in to the Jacada Workspace Agent Desktop application as shown below.

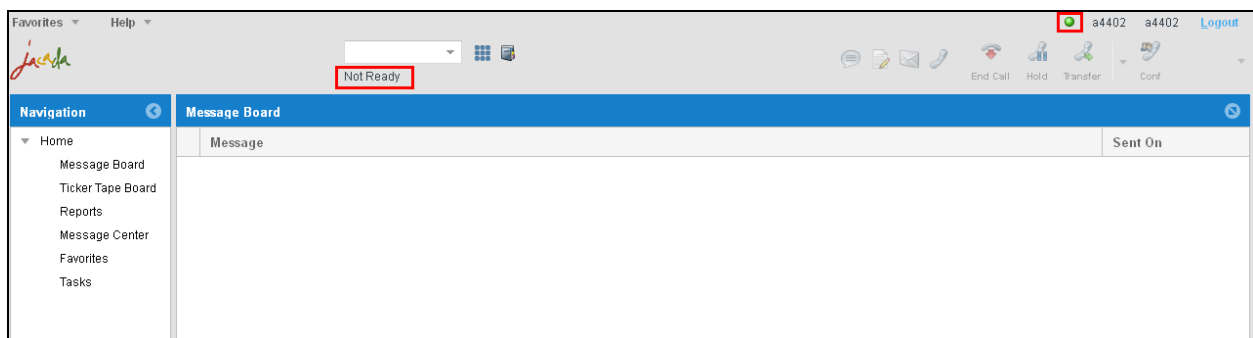
http://localhost:9090/<applicationName>?CTIProfile=CTI_AES_AVAYA (not captured in the screen shot below).



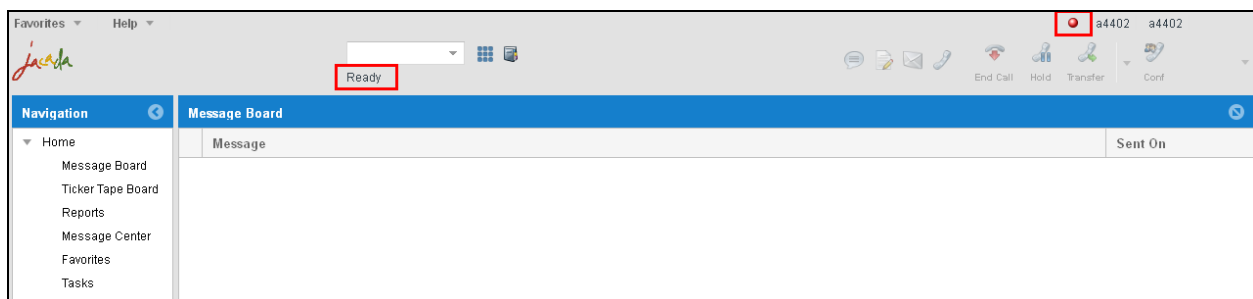
A window will pop up, press done at the bottom of the screen.



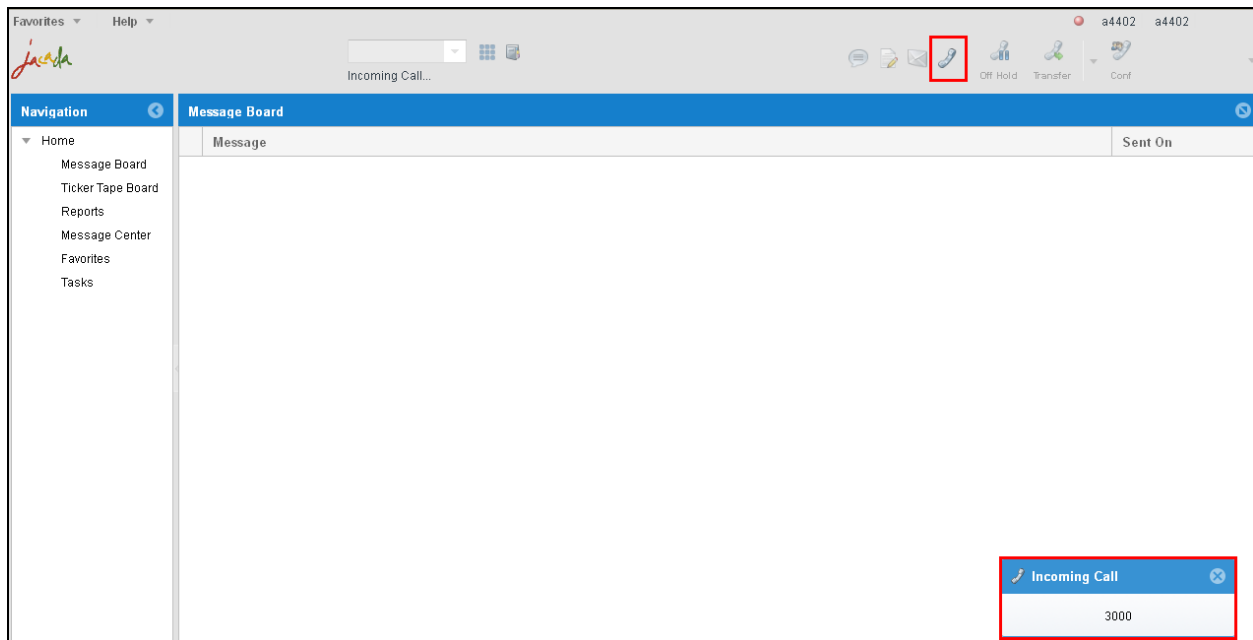
Once logged in to the Jacada Workspace Agent Desktop the agent will be placed automatically in the **Not Ready** state as shown below. Press the green button highlighted to change the state to Ready.



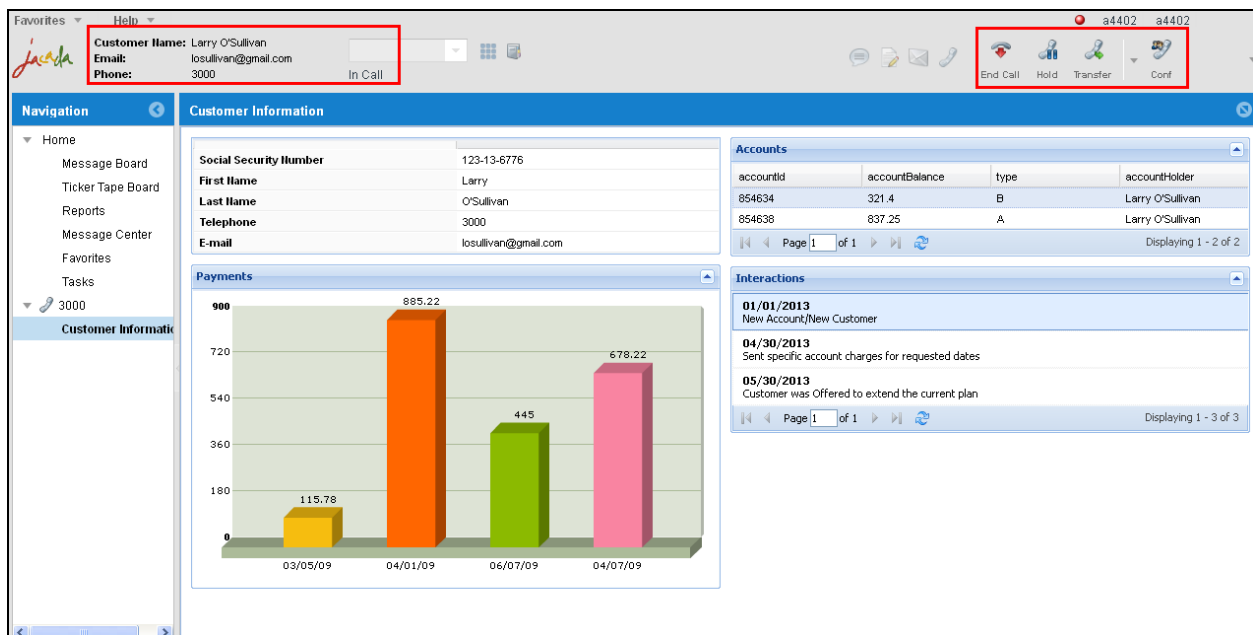
Once this is done the button turns from green to red and the agent is shown as **Ready**.



Once the call is presented to the agent, a window showing **Incoming Call** appears at the bottom right of the screen and the **answer button** highlighted in the main window can be pressed to answer the call.



Once the call is answered the caller information from a CRM application is displayed and the telephony buttons become active where the agents can **End Call**, **Hold**, **Transfer** and **Conference**.



9. Conclusion

These Application Notes describe the configuration steps required for Jacada Workspace Agent Desktop to successfully interoperate with Avaya Aura® Communication Manager R6.3 using Avaya Aura® Application Enablement Services R6.3. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Jacada product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 6.3*

Technical documentation can be obtained for Jacada Workspace Agent Desktop from the website www.jacada.com.

Online help can be found at <http://www.jacada.com/help/jws>

Appendix

Avaya one-X® Agent Softphone

This is a printout of the Avaya one-X® Agent softphone used during compliance testing.

display station 2100	Page 1 of 5	
STATION		
Extension: 2100	Lock Messages? n	BCC: 0
Type: 9630	Security Code: *	TN: 1
Port: S00031	Coverage Path 1:	COR: 1
Name: one-X Agent1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 2100	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? Y	

display station 2100	Page 2 of 5	
	STATION	
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 2100	Always Use? n IP Audio Hairpinning? n	

display station 2100	STATION	Page 3 of 5
<p>Conf/Trans on Primary Appearance? n</p> <p>Bridged Appearance Origination Restriction? n</p>		
<p>Call Appearance Display Format: disp-param-default</p> <p>IP Phone Group ID:</p> <p>Enhanced Callr-Info Display for 1-Line Phones? n</p>		
ENHANCED CALL FORWARDING		
	Forwarded Destination	Active
Unconditional For Internal Calls To: 1000		n
External Calls To: 1000		n
Busy For Internal Calls To:		n
External Calls To:		n
No Reply For Internal Calls To:		n
External Calls To:		n
SAC/CF Override: n		

display station 2100	STATION	Page 4 of 5
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5: manual-in	Grp:
2: call-appr	6: after-call	Grp:
3: call-appr	7: aux-work	RC: Grp:
4: auto-in	8:	
	Grp:	
voice-mail		

Avaya 9620 H.323 Deskphone

This is a printout of the Avaya 9620 H.323 Deskphone used during compliance testing.

display station 2000	Page 1 of 5	
STATION		
Extension: 2000	Lock Messages? n	BCC: 0
Type: 9620	Security Code: *	TN: 1
Port: S00000	Coverage Path 1: 2	COR: 1
Name: Paul 2000	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 2000	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

display station 2000	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	
	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number? y
Service Link Mode: as-needed	EC500 State: enabled
Multimedia Mode: enhanced	Audible Message Waiting? n
MWI Served User Type:	Display Client Redirection? n
AUDIX Name:	Select Last Used Appearance? n
	Coverage After Forwarding? s
	Multimedia Early Answer? n
	Direct IP-IP Audio Connections? y
Emergency Location Ext: 2000	Always Use? n IP Audio Hairpinning? n

display station 2000	STATION	Page 3 of 5
<p>Conf/Trans on Primary Appearance? n</p> <p>Bridged Appearance Origination Restriction? n</p>		
<p>Call Appearance Display Format: inter-location</p> <p>IP Phone Group ID:</p> <p>Enhanced Callr-Info Display for 1-Line Phones? n</p>		
ENHANCED CALL FORWARDING		
	Forwarded Destination	Active
Unconditional For Internal Calls To: 4000		n
External Calls To: 4000		n
Busy For Internal Calls To: 4202		n
External Calls To: 4202		n
No Reply For Internal Calls To: 2101		y
External Calls To: 2101		y
SAC/CF Override: n		

display station 2000	STATION	Page 4 of 5
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	4: manual-in	Grp:
2: call-appr	5: after-call	Grp:
3: auto-in	6: aux-work	RC: Grp:
voice-mail		

Avaya Agent LoginID

This is a printout of one of the agents used during compliance testing.

```
display agent-loginID 4400                                Page 1 of 3

                                AGENT LOGINID

      Login ID: 4400                                AAS? n
      Name: Paul                                AUDIX? n
      TN: 1                                LWC Reception: spe
      COR: 1                                LWC Log External Calls? n
      Coverage Path:                                AUDIX Name for Messaging:
      Security Code:

                                LoginID for ISDN/SIP Display? n
                                Password:
                                Password (enter again):
                                Auto Answer: station
                                MIA Across Skills: system
                                ACW Agent Considered Idle: system
                                Aux Work Reason Code Type: system
                                Logout Reason Code Type: system
                                Maximum time agent in ACW before logout (sec): system
                                Forced Agent Logout Time: :
```

```
display agent-loginID 4400                                Page 2 of 3

                                AGENT LOGINID

      Direct Agent Skill:                                Service Objective? n
      Call Handling Preference: skill-level                Local Call Preference? n

      SN  RL  SL          SN  RL  SL          SN  RL  SL          SN  RL  SL
1: 33    1              16:                31:                46:
2: 34    1              17:                32:                47:
3:                18:                33:                48:
4:                19:                34:                49:
5:                20:                35:                50:
6:                21:                36:                51:
7:                22:                37:                52:
8:                23:                38:                53:
9:                24:                39:                54:
10:               25:                40:                55:
11:               26:                41:                56:
12:               27:                42:                57:
13:               28:                43:                58:
14:               29:                44:                59:
15:               30:                45:                60:
```

©2014 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.