



Application Notes for Jacada Workspace with Avaya Communication Manager using Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Jacada Workspace to interoperate with Avaya Communication Manager using Avaya Application Enablement Services. Jacada Workspace is a contact center solution that enables creation of web-based thin-client unified desktops. The thin-client provides a single point of access to all major functions and applications required by agents to service customer calls.

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

1. Introduction

Jacada Workspace is a contact center solution that enables creation of web-based thin-client unified desktops. The thin-client provides a single point of access to all major functions and applications required by agents to service customer calls. Jacada Workspace can combine the agent desktop applications into an environment that includes features such as single sign-on, dynamic call scripting, guided navigation, cross-sell/up-sell alerts, in-call intelligence, automated call wrap-up, Computer Telephony Integration (CTI), and contact channel integration.

The compliance testing focused on the CTI functionality of Jacada Workspace. The integration with Avaya Communication Manager is through Avaya Application Enablement Services (AES) with Envoy CT Connect as a CTI middleware provider. The Definity LAN Gateway (DLG) interface of Avaya AES is utilized by Envoy CT Connect to provide call control and event report CTI functionality to Jacada Workspace. The CTI functionality enables Jacada Workspace clients/agents to access customer information such as calling party number, and perform login/logout and call related actions via the desktops.

For the compliance testing, both Jacada Workspace and Envoy CT Connect were installed on the same server as shown in **Figure 1** below.

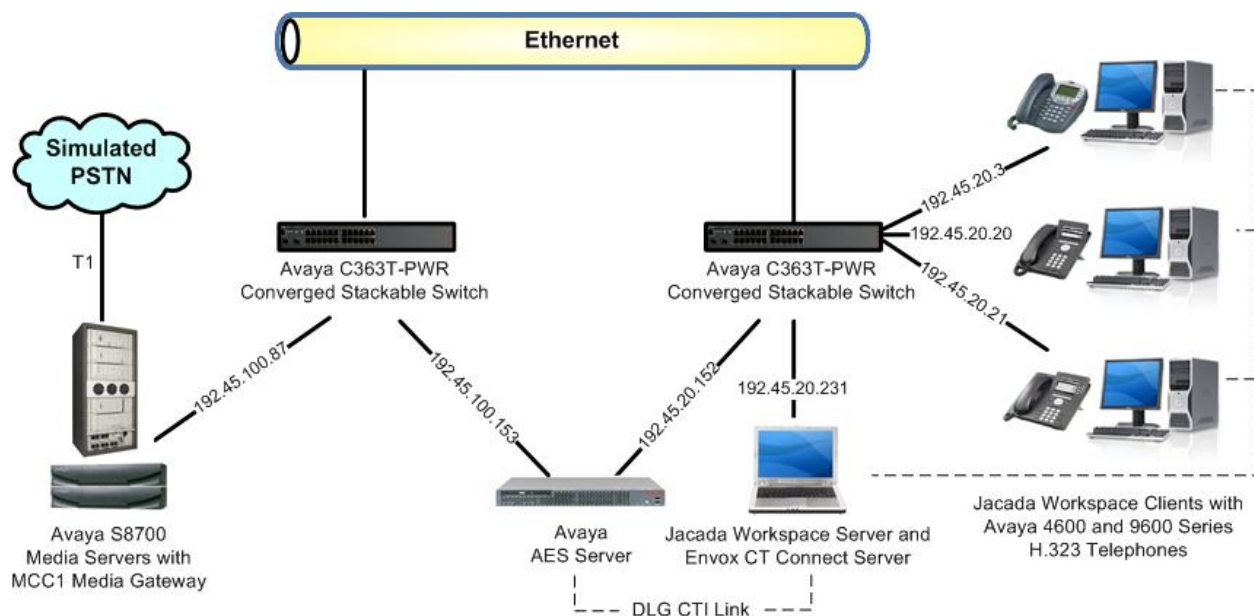


Figure 1: Jacada Workspace with Avaya Communication Manager using Avaya AES and Envoy CT Connect

2. Equipment and Software Validated

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

| Equipment | Software |
|--|--|
| Avaya S8700 Media Servers | Avaya Communication Manager 3.1.2, R013x.01.2.632.1 |
| Avaya MCC1 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media Processor Circuit Pack | HW01 FW017 HW13 FW111 |
| Avaya Application Enablement Services | 3.1.2, build 46.5 |
| Avaya C363T-PWR Converged Stackable Switches | 4.5.14 |
| Avaya 4610SW IP Telephones (H.323) | 2.30 |
| Avaya 9620 one-X™ Deskphone Edition (H.323) | 1.0 |
| Avaya 9630 one-X™ Deskphone Edition (H.323) | 1.0 |
| Jacada Workspace and Envox CT Connect on IBM ThinkPad <ul style="list-style-type: none">BEA WebLogicBEA PointBase | 4.0 with patch CR070108 6.1 SP1H Windows XP Professional SP2 8.1 SP5 8.1 SP5 |

3. Configure Avaya Communication Manager

This section provides the procedures for configuring Avaya Communication Manager. The procedures include the following areas:

- Verify Avaya Communication Manager license
- Administer IP node name for C-LAN
- Administer IP interface for C-LAN
- Administer data module for C-LAN
- Administer IP services for AES transport link
- Administer CTI link for DLG service

The detailed administration of contact center devices, such as Vector Directory Numbers (VDNs), vectors, ACD/Skill groups and logical agents are assumed to be in place and are not covered in these Application Notes. For administration of contact center devices, refer to the appropriate documentation in **Section 11**.

For the compliance testing, agents with physical station extensions of “22991, 22992, 22993” and logical agent identifiers of “53001, 53002, 53003” along with the same passwords “53001, 53002, 53003” were created. This information will be used to configure the Jacada Workspace agents in **Section 6.2**.

3.1. Verify Avaya Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Avaya Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **ASAI Link Core Capabilities** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

```
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 Backup Cluster Automatic Takeover? n
A/D Grp/Sys List Dialing Start at 01? y    CAS Branch? n
Answer Supervision by Call Classifier? y    CAS Main? n
ARS? y                                     Change COR by FAC? n
ARS/AAR Partitioning? y Computer Telephony Adjunct Links? y
ARS/AAR Dialing without FAC? y Cvg Of Calls Redirected Off-net? y
ASAI Link Core Capabilities? y           DCS (Basic)? y
ASAI Link Plus Capabilities? y             DCS Call Coverage? y
Async. Transfer Mode (ATM) PNC? n          DCS with Rerouting? y
Async. Transfer Mode (ATM) Trunking? y
ATM WAN Spare Processor? n Digital Loss Plan Modification? n
ATMS? y                                   DS1 MSP? n
Attendant Vectoring? n                   DS1 Echo Cancellation? N
```

3.2. Administer IP Node Name for C-LAN

Use the “change node-names ip” command, and add an entry for the C-LAN that will be used for connectivity to the AES server. In this case, “clan-1b09” and “192.45.100.87” are entered as **Name** and **IP Address**. The actual node name and IP address may vary. Submit these changes.

```
change node-names ip
                                IP NODE NAMES
      Name      IP Address
clan-1b09    192.45 .100.87
default      0 .0 .0 .0
```

3.3. Administer IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface n” command, where “n” is an available slot number. Note that the actual slot number may vary, and in this case “1b09” is used. Enter the C-LAN node name assigned from **Section 3.2** into the **Node Name** field. The **IP Address** field will be populated automatically.

Enter proper values for the **Subnet Mask** and **Gateway Address** fields. In this case, “255.255.255.0” and “192.45.100.1” are used to correspond to the network configuration in these Application Notes. Set the **Enable Ethernet Port** field to “y”, and use a separate **Network Region** for the C-LAN dedicated for AES connectivity. Default values may be used in the remaining fields. Submit these changes.

```
add ip-interface 1b09
                                IP INTERFACES
                                Page 1 of 1

      Type: C-LAN
      Slot: 01B09
      Code/Suffix: TN799 D
      Node Name: clan-1b09
      IP Address: 192.45 .100.87
      Subnet Mask: 255.255.255.0
      Gateway Address: 192.45 .100.1
      Enable Ethernet Port? y
      Network Region: 2
      VLAN: n
      Link:
      Allow H.323 Endpoints? y
      Allow H.248 Gateways? y
      Gatekeeper Priority: 5

      Target socket load and Warning level: 400
      Receive Buffer TCP Window Size: 8320
      ETHERNET OPTIONS
      Auto? Y
```

3.4. Administer Data Module for C-LAN

Add a new data module using the “add data-module n” command, where “n” is an available extension. Enter the following values:

- **Name:** A descriptive name.
- **Type:** “ethernet”
- **Port:** Same slot number from **Section 3.3** above and port “17”.
- **Link:** An available link number.

```
add data-module 2001
                                DATA MODULE

Data Extension: 2001           Name: CLAN 1B09 Data Module
      Type: ethernet
      Port: 01B0917
      Link: 11
```

3.5. Administer IP Services for AES Transport Link

Administer the transport link to the AES server with the “change ip-services” command. Add an entry with the following values for fields on **Page 1**:

- **Service Type:** “AESVCS”
- **Enabled:** “y”
- **Local Node:** C-LAN node name from **Section 3.2**.
- **Local Port:** Retain the default value of “8765”.

```
change ip-services
Page 1 of 3

Service  Enabled  Local      IP SERVICES
Type      y         Node      Local      Remote
          y         Node      Port      Node      Port
SAT       y         clanP27-2a03  5023    any
SAT       y         clan-1b04    5023    any
AESVCS    y         clan-1b04    8765
AESVCS  y         clan-1b09   8765
```

Proceed to **Page 3**, and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case “AES-DevCon2”.
- **Password:** Same password to be administered on the AES server.
- **Enabled:** “y”

Note that the name and password entered for the **AE Services Server** and **Password** fields are case sensitive, and must match the name and password on the AES server. The administered name for the AES server 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. The same password entered in the screen below will need to be set on the AES server, as described in **Section 4.3**.

| | | | | | |
|----------------------------|--------------------|----------|---------|--------|--------|
| change ip-services | | | | Page | 3 of 3 |
| AE Services Administration | | | | | |
| Server ID | AE Services Server | Password | Enabled | Status | |
| 1: | devconaes01 | * | y | in use | |
| 2: | AES-DevCon2 | devcon2 | y | | |
| 3: | | | | | |

3.6. Administer CTI Link for DLG Service

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ASAI-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields. Submit these changes.

| | | | |
|-----------------------------|--|------|--------|
| add cti-link 1 | | Page | 1 of 2 |
| CTI LINK | | | |
| CTI Link: 1 | | | |
| Extension: 2201 | | | |
| Type: ASAI-IP | | | |
| | | | COR: 1 |
| Name: Envoy-Jacada DLG Link | | | |

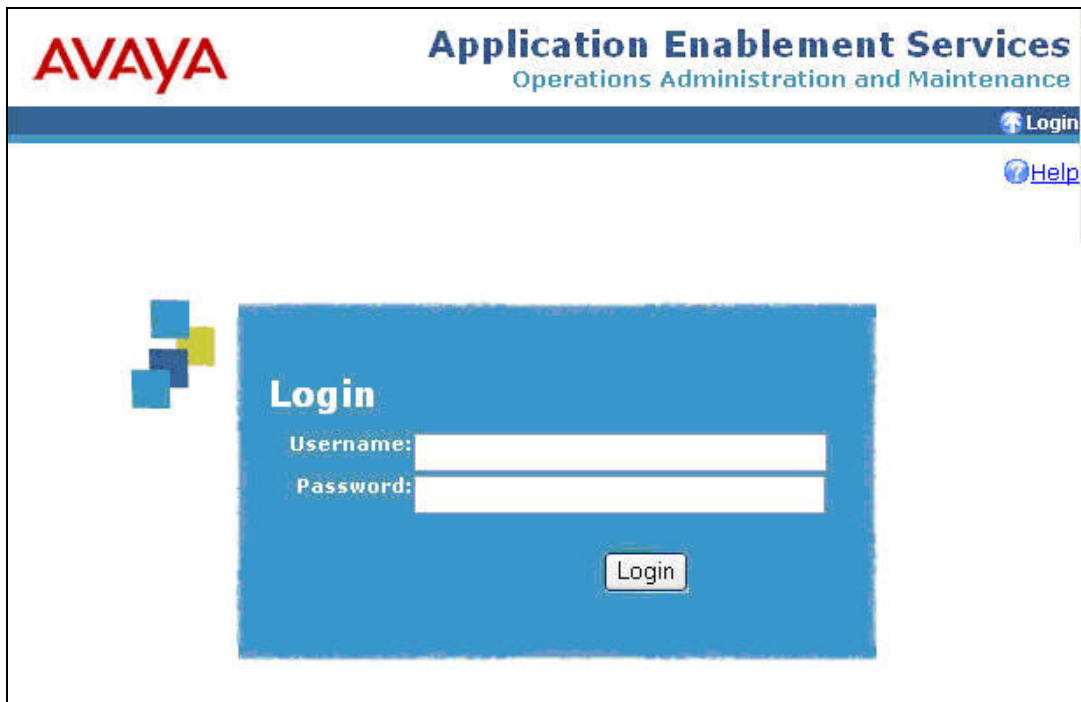
4. Configure Avaya Application Enablement Services

This section provides the procedures for configuring Avaya Application Enablement Services (AES). The procedures include the following areas:

- Verify AES license
- Administer local IP
- Administer switch connection
- Administer DLG link

4.1. Verify AES License

Access the AES OAM web based interface by using the URL “https://ip-address:8443/MVAP” in an Internet browser window, where “ip-address” is the IP address of the AES server. The **Login** screen is displayed as shown below. Note that the AES OAM includes two separate administrative accounts, one to access CTI OAM Admin and a separate one to access User Management. Log in using the CTI OAM Admin user name and password.

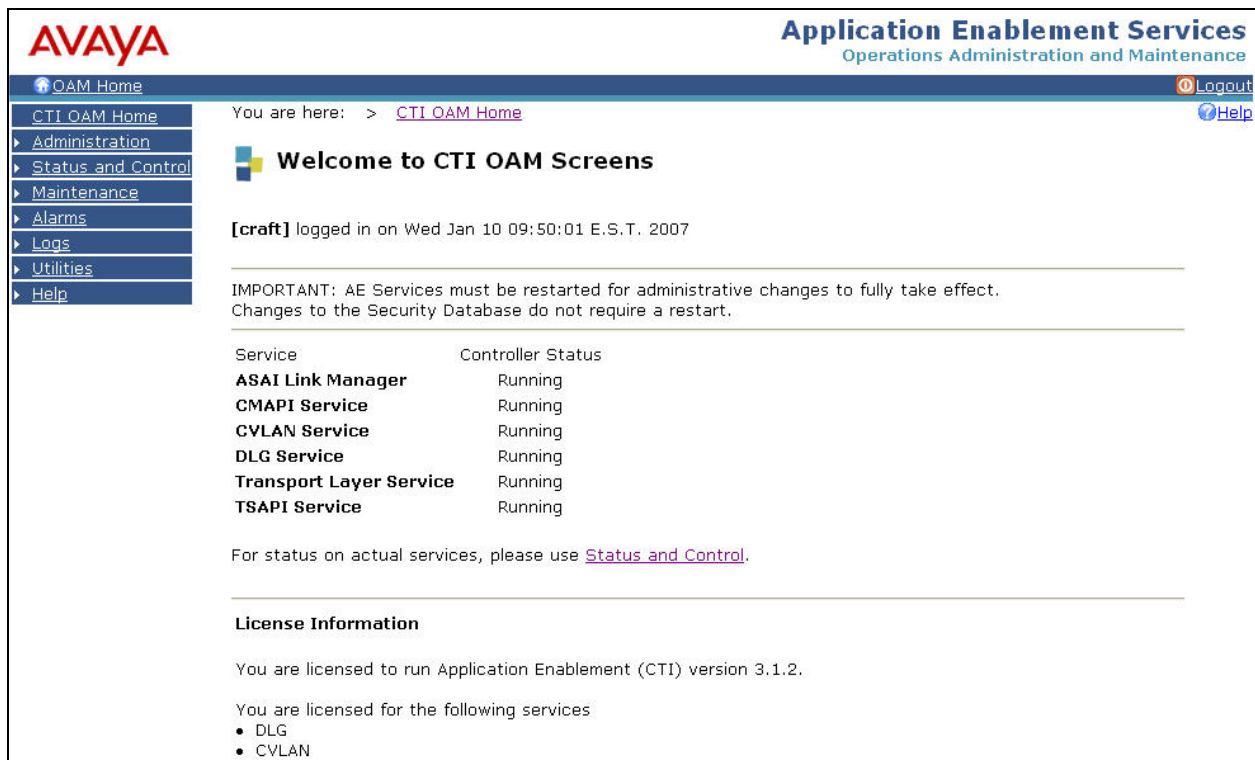


The screenshot shows the Avaya Application Enablement Services (AES) Operations Administration and Maintenance (OAM) interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large blue font, with "Operations Administration and Maintenance" in a smaller blue font below it. In the top right corner, there are two links: "Login" with a small icon and "Help" with a question mark icon. The main content area features a blue rectangular box with the word "Login" in white. Below this, there are two white input fields labeled "Username:" and "Password:". At the bottom of the blue box is a "Login" button. To the left of the blue box, there are four small squares in blue, dark blue, and yellow.

The **Welcome To OAM** screen is displayed, as shown below. Select **CTI OAM Admin** from the left pane.



The **Welcome to CTI OAM Screens** is displayed next. Verify that AES is licensed for the DLG service, as shown in the bottom of the screen below. If the DLG service is not licensed, contact the Avaya sales team or business partner for a proper license file.



4.2. Administer Local IP

From the **CTI OAM Home** menu in the left pane, select **Administration > Local IP**. The **Local IP** screen is displayed into the right pane, as shown below. In the **Client Connectivity** field, select the AES server IP address that will be used to connect to Envoy CT Connect. In the **Switch Connectivity** field, select the AES server IP address that will be used to connect to Avaya Communication Manager. Note that the IP addresses were created as part of AES installation. Retain the default value in the **Media Connectivity** field, and click on **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services (AES) interface. The top header includes the Avaya logo and the title "Application Enablement Services" with the subtitle "Operations Administration and Maintenance". A navigation bar at the top contains "OAM Home", "Logout", and "Help". The left sidebar shows a tree view with "Administration" expanded, containing "Local IP", "Ports", "Switch Connections", "CTI Link Admin", "CMAPI Configuration", "TSAPI Configuration", "Security Database", and "Status and Control". The main content area is titled "Local IP" and contains three dropdown menus: "Client Connectivity" (set to eth0:192.45.20.152), "Switch Connectivity" (set to eth1:192.45.100.153), and "Media Connectivity" (set to Any). An "Apply Changes" button is located below these fields. The breadcrumb trail at the top right reads "You are here: > Administration > Local IP".

4.3. Administer Switch Connection

From the **CTI OAM Home** menu in the left pane, select **Administration > Switch Connections**. The **Switch Connections** screen is displayed, as shown below. Enter a descriptive name for the switch connection and click on **Add Connection**. In this case, "devcon27S8700" is used. Note that the actual switch connection name may vary.

The screenshot shows the Avaya Application Enablement Services (AES) interface for the "Switch Connections" page. The top header and navigation bar are identical to the previous screenshot. The left sidebar shows "Switch Connections" selected under "Administration". The main content area is titled "Switch Connections" and features a text input field containing "devcon27S8700" and an "Add Connection" button. Below this, a table lists existing connections:

| Connection Name | Number of Active Connections | Connection Type |
|-----------------|------------------------------|----------------------|
| devcon31S8700 | 1 | CTI/Call Information |

At the bottom of the page, there are four buttons: "Edit Connection", "Edit CLAN IPs", "Edit H.323 Gatekeeper", and "Delete Connection". The breadcrumb trail at the top right reads "You are here: > Administration > Switch Connections".

Next, the **Set Password – devcon27S8700** screen is displayed. Enter the following values for the specified fields:

- **Switch Connection Type:** “CTI/Call Information”
- **Switch Password:** Same password from **Section 3.5**.
- **Confirm Switch Password:** Re-enter the same password from **Section 3.5**.
- **SSL:** Retain the check.

Had the switch been an Avaya DFINITY Server G3csi, the **SSL** checkbox would need to be unchecked. Click on **Apply**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

OAM Home Logout

CTI OAM Home You are here: > Administration > Switch Connections Help

Set Password - devcon27S8700

Please note the following:
 * A password is not required for a H323 Gatekeeper Connection.
 * Changing the password affects only new connections, not open connections.

Switch Connection Type: CTI/Call Information

Switch Password: [Redacted]

Confirm Switch Password: [Redacted]

SSL: ☒

Apply Cancel

The **Switch Connections** screen is displayed next, as shown below. Select the newly added switch connection name from the listing, and click on **Edit CLAN IPs**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

OAM Home Logout

CTI OAM Home You are here: > Administration > Switch Connections Help

Switch Connections

Add Connection

| Connection Name | Number of Active Connections | Connection Type |
|-----------------|------------------------------|----------------------|
| devcon27S8700 | 1 | CTI/Call Information |
| devcon31S8700 | 1 | CTI/Call Information |

Edit Connection Edit CLAN IPs Edit H.323 Gatekeeper Delete Connection

The **Edit CLAN IPs – devcon27S8700** screen is displayed next. Enter the host name or IP address of the C-LAN used for AES connectivity from **Section 3.2**. In this case, “192.45.100.87” is used. Click on **Add Name or IP**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

[OAM Home](#) [Logout](#)

You are here: > [Administration](#) > [Switch Connections](#) [Help](#)

Edit CLAN IPs - devcon27S8700

192.45.100.87

| Name or IP Address | Status |
|--|--------|
| <input type="button" value="Delete IP"/> | |

4.4. Administer DLG Link

To administer a DLG link, select **Administration > CTI Link Admin > DLG Links** from the **CTI OAM Home** menu in the left pane. The **DLG Links** screen is displayed, as shown below. Click on **Add Link**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

[OAM Home](#) [Logout](#)

You are here: > [Administration](#) > [CTI Link Admin](#) > [DLG Links](#) [Help](#)

DLG Links

| Switch Connection | Switch CTI Link # | Client Host Name or IP Address | Client Link Number |
|---|-------------------|--------------------------------|--------------------|
| <input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/> | | | |

The **Add/Edit DLG Links** screen is displayed next. Select the following values for the specified fields, and click on **Apply Changes**.

- **Switch Connection:** Name of switch connection from **Section 4.3**.
- **Switch CTI Link Number:** CTI link number from **Section 3.6**.
- **Client Hostname or IP:** IP address of the Envoy CT Connect server from **Figure 1**.
- **Client Link Number:** Link number of Envoy CT Connect server from **Section 5.4**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

QAM Home Logout

You are here: > Administration > CTI Link Admin > DLG Links Help

Add / Edit DLG Links

Switch Connection: devcon27S8700

Switch CTI Link Number: 1

Client Hostname or IP: 192.45.20.231

Client Link Number: 1

Apply Changes Cancel Changes

The **Apply Changes to Link** screen is displayed. Click on **Apply**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

QAM Home Logout

You are here: > Administration > CTI Link Admin > DLG Links Help

Apply Changes to Link

Warning! Are you sure you want to apply the changes?

Apply Cancel

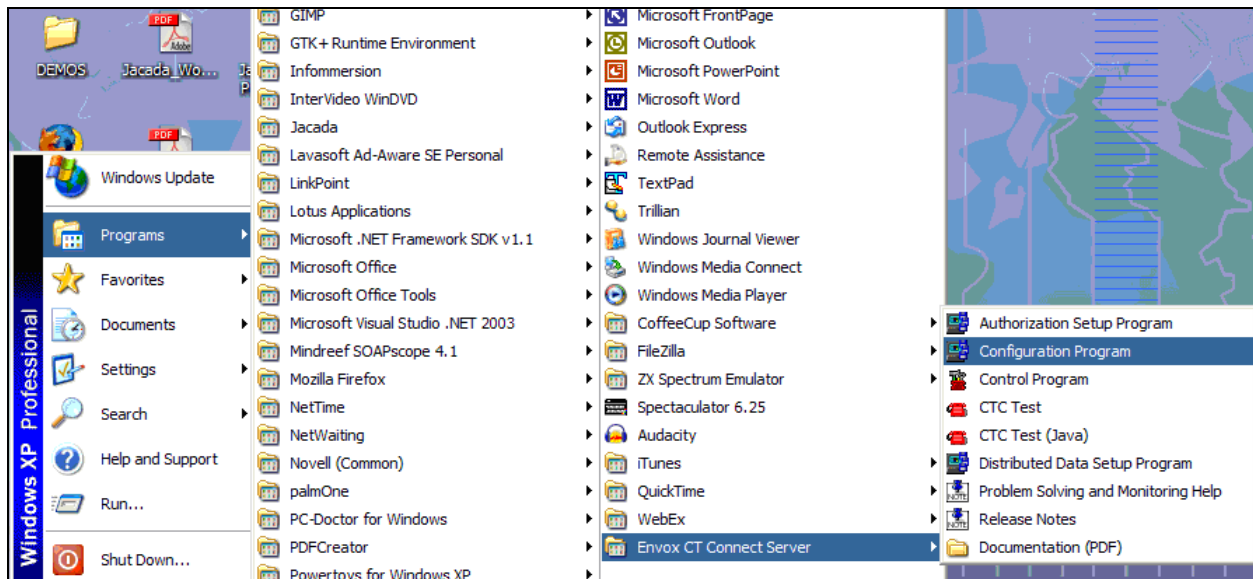
5. Configure Envoy CT Connect

This section provides the procedures for configuring the Envoy CT Connect server. The procedures include the following areas:

- Launch configuration program
- Administer link
- Administer switch type
- Administer IP address and link number

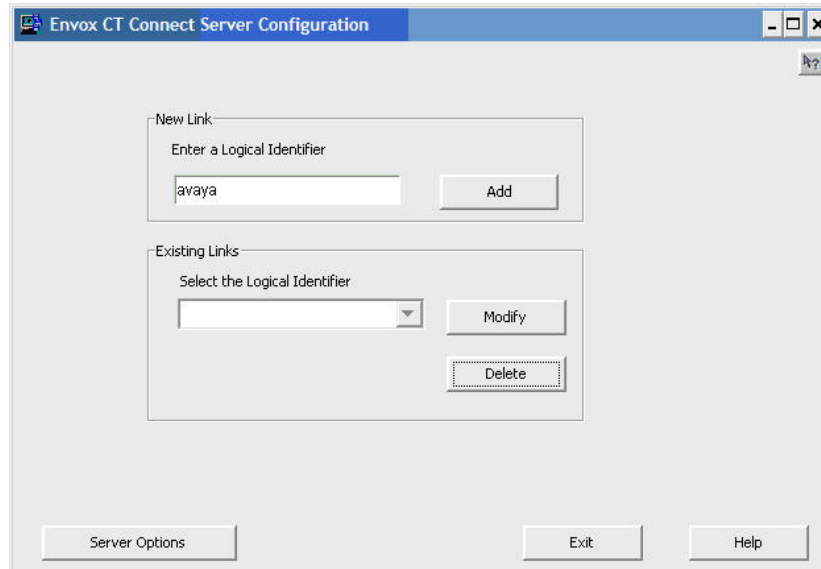
5.1. Launch Configuration Program

Envoy CT Connect uses a GUI based configuration program to configure communication links between the CT Connect server and switches. From the Envoy CT Connect server, launch the configuration program by selecting **Start > Programs > Envoy CT Connect Server > Configuration Program** as shown below.



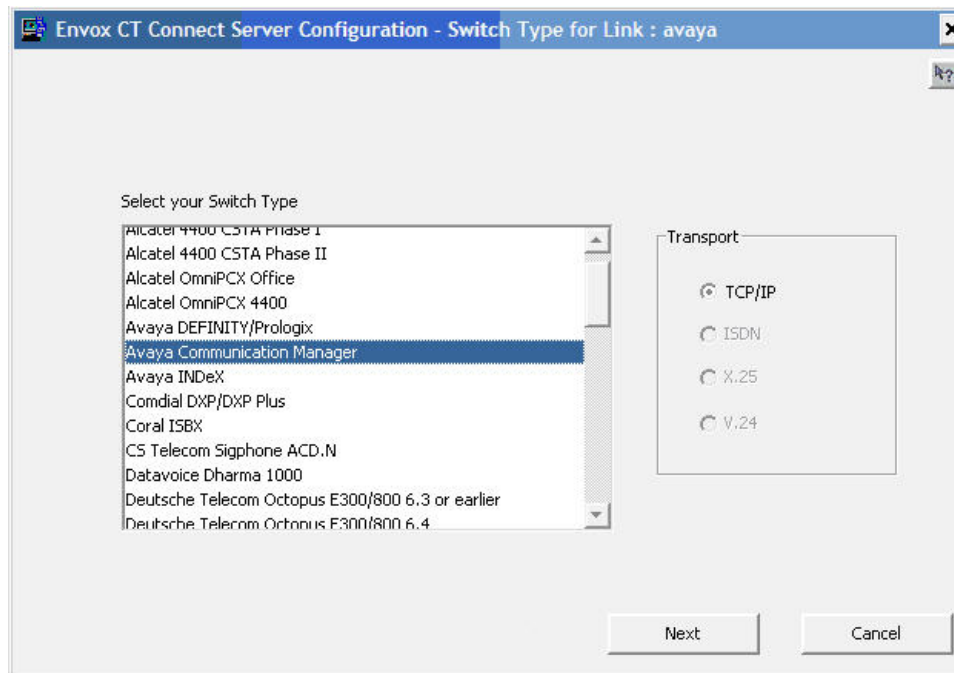
5.2. Administer Link

The **Envox CT Connect Server Configuration** screen is displayed. Enter a descriptive name for the **Enter a Logical Identifier** field, in this case “avaya”. Click on the **Add** button.



5.3. Administer Switch Type

The **Envox CT Connect Server Configuration – Switch Type for Link : avaya** screen is displayed next. Select **Avaya Communication Manager** from the list and click **Next**.



5.4. Administer IP Address and Link Number

The **Envox CT Connect Server Configuration – Configuring Avaya TCP/IP Link : avaya** screen is displayed. Enter the following values for the specified fields, and retain the default values in the remaining fields. Click on **Save**.

- **Switch IP Address:** AES client connectivity IP address from **Section 4.2**.
- **Link Number:** Link number used for connectivity to AES, in this case “1”.

The screenshot shows a Windows-style dialog box titled "Envox CT Connect Server Configuration - Configuring Avaya TCP/IP Link : avaya". The dialog has a blue title bar with a close button (X) and a help button (?). The main area contains several input fields and checkboxes. The "Switch IP Address" field is set to "192.45.20.152". The "Link Number" field is set to "1". To the right, the "Maximum Monitors" field is set to "1000". Below this, there are two checkboxes: "Auto Start Link" (checked) and "Auto Restart Monitors" (unchecked). A section labeled "Optional" contains two empty text boxes for "Local IP Address" and "Network Node ID". At the bottom left, there is a "Device Level Authorisation" section with an "Enable" checkbox (unchecked) and a "Password" dropdown menu showing "None", "System", and "Application". At the bottom of the dialog are four buttons: "Advanced", "Trace", "Save", and "Cancel".

| | | | |
|-----------------------------------|---------------|---|--------|
| Switch IP Address | 192.45.20.152 | Maximum Monitors | 1000 |
| Link Number | 1 | <input checked="" type="checkbox"/> Auto Start Link | |
| Optional | | <input type="checkbox"/> Auto Restart Monitors | |
| Local IP Address | | | |
| Network Node ID | | | |
| Device Level Authorisation | | | |
| <input type="checkbox"/> Enable | | | |
| Password | | | |
| <input type="radio"/> None | | | |
| <input type="radio"/> System | | | |
| <input type="radio"/> Application | | | |
| Advanced | Trace | Save | Cancel |

6. Configure Jacada Workspace

This section provides the procedures for configuring the Jacada Workspace server. The procedures include the following areas:

- Launch PointBase Console
- Administer agents
- Administer CTI provider
- Launch Jacada Workshop
- Administer application
- Administer switch type
- Administer numbers
- Build Application
- Start WebLogic server
- Launch WebLogic server

Configuration of Jacada Workspace is typically performed by Jacada Professional Services. The procedural steps are presented in these Application Notes for informational purposes. Jacada Workspace can be configured on a single server or with components distributed across multiple servers. For ease of compliance testing, the configuration used a single server hosting all components including WebLogic and PointBase, which are third-party Java-based application and database components from BEA that are utilized by Jacada Workspace.

By default, Jacada Workspace is configured to work during development with the PointBase database. For a production environment, it is necessary to use either the Microsoft SQL or Oracle database. For simplicity of the compliance testing, the PointBase database was utilized.

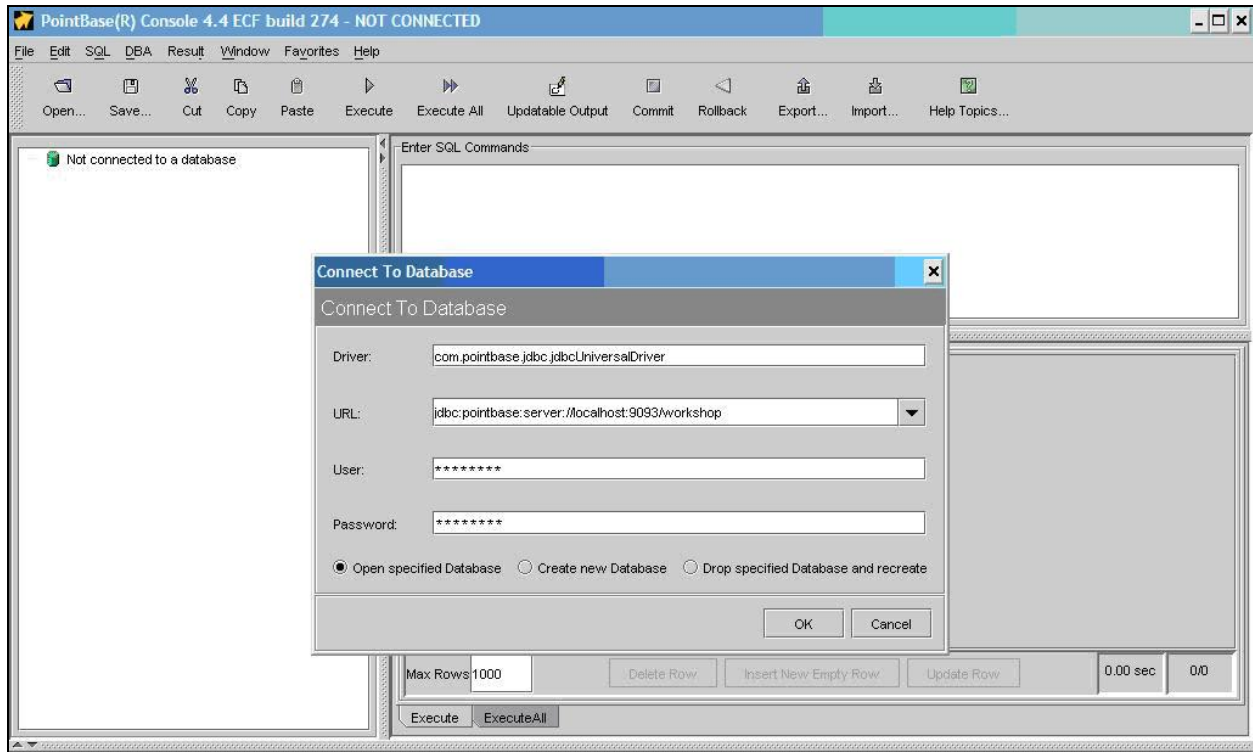
6.1. Launch PointBase Console

From the Jacada Workspace server, double-click on the PointBase Console icon shown below, which was created as part of the Jacada Workspace server installation.



The screen below is displayed, with the **Connect To Database** dialog box automatically popped up. In the **URL** field, select the URL to correspond to the appropriate project in the PointBase database server. For the compliance testing, the PointBase database resided with the Jacada Workspace server and hence the use of “localhost” in the URL. The default port of “9093” was used along with the default database name of “workshop” in the URL. Note that this URL was created as part of the Jacada Workspace installation.

Maintain the default values in the **Driver** field, and enter the appropriate credentials into the **User** and **Password** fields. Click on **OK**.



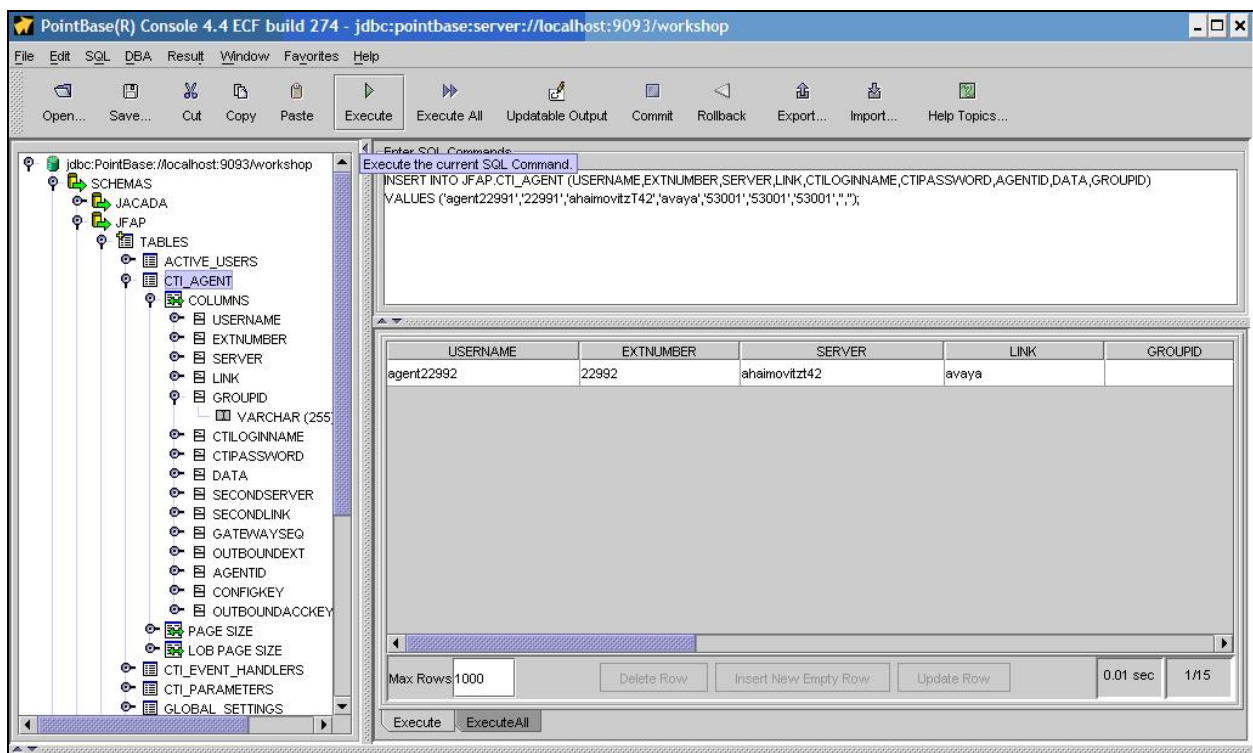
6.2. Administer Agents

The screen is updated with the PointBase directories in the left pane. Expand **jdbc:PointBase://localhost:9093/workshop > SCHEMAS > JFAP > TABLES** in the left pane, and select **CTI_AGENT**. Note that the name for the root directory may vary. Add an agent by entering the SQL command with the following parameters in the upper right pane, and click on **Execute**.

- **USERNAME:** A descriptive user name for the agent.
- **EXTNUMBER:** The physical station extension for the agent from **Section 3**.
- **SERVER:** Name or IP address of the Envoy CT Connect server.
- **LINK:** Envoy CTI logical link identifier from **Section 5.2**.
- **CTILOGINNAME:** The logical agent identifier from **Section 3**.
- **CTIPASSWORD:** The logical agent password from **Section 3**.
- **AGENTID:** The logical agent identifier from **Section 3**.
- **DATA:** Null value indicated by “”.
- **GROUPID:** Null value indicated by “”.

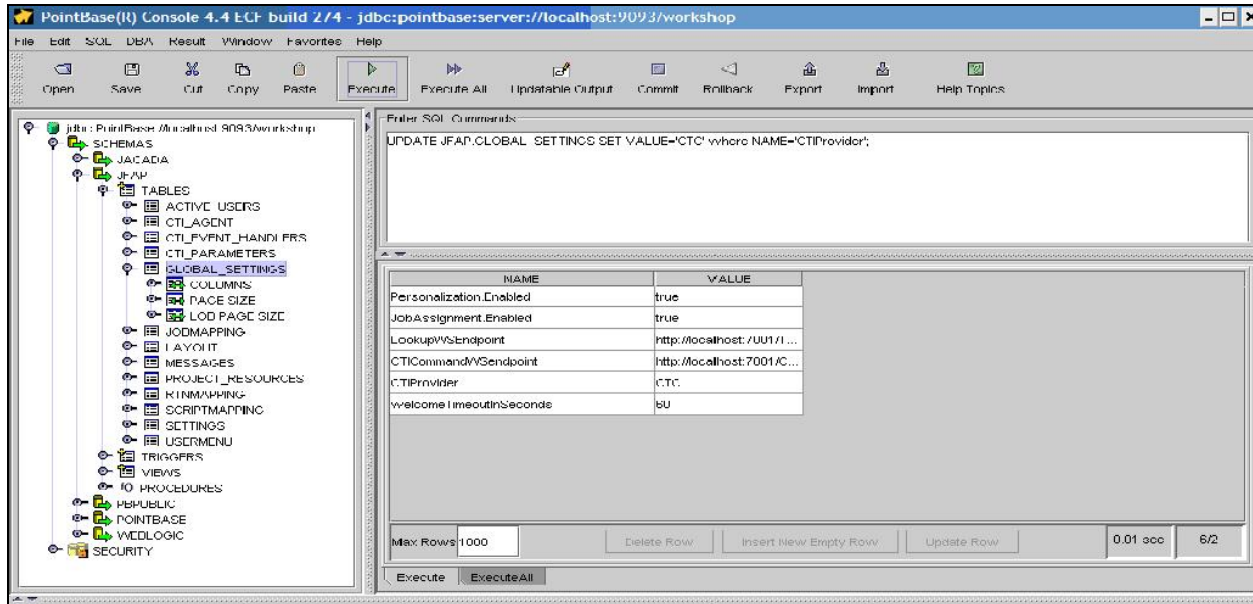
Note that for the test configuration, the Envoy CT Connect server resides on the same server as Jacada Workspace, with “ahaimovitz” as the host name.

Repeat this procedure to add an entry for every agent. In the screen below, the upper right pane shows the SQL command to add an entry for agent 22991, and the lower right pane shows an already added entry for agent 22992.



6.3. Administer CTI Provider

Select **GLOBAL_SETTINGS** in the left pane. Enter the SQL command in the upper right pane to set the value of the “CTIProvider” to “CTC”, which denotes Envoy CT Connect. Click on **Execute**. The lower right pane in the screen below shows the updated value after the change.



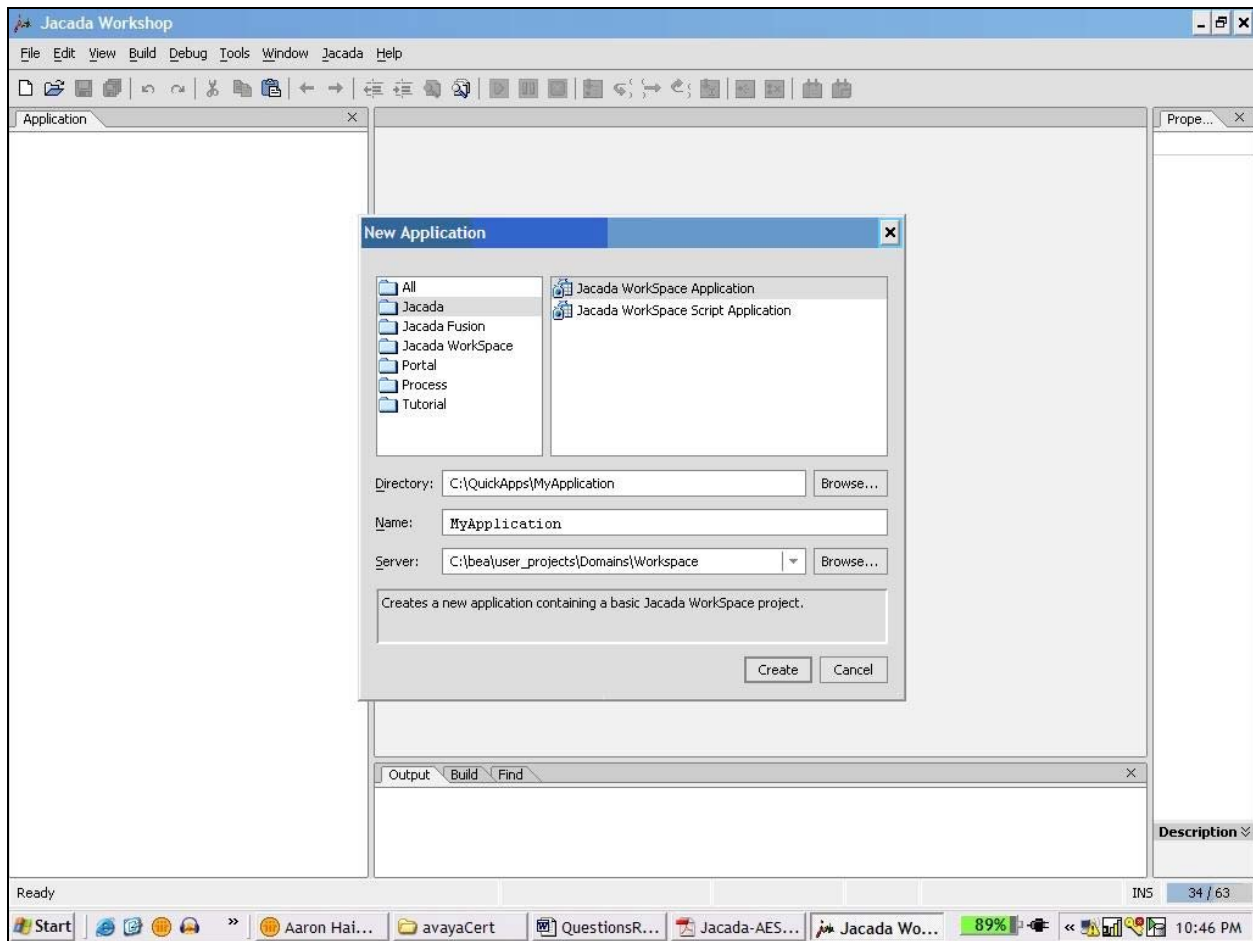
6.4. Launch Jacada Workshop

From the Jacada Workspace server, double-click on the **Jacada Workshop** icon shown below, which was created as part of the Jacada Workspace server installation.



6.5. Administer Application

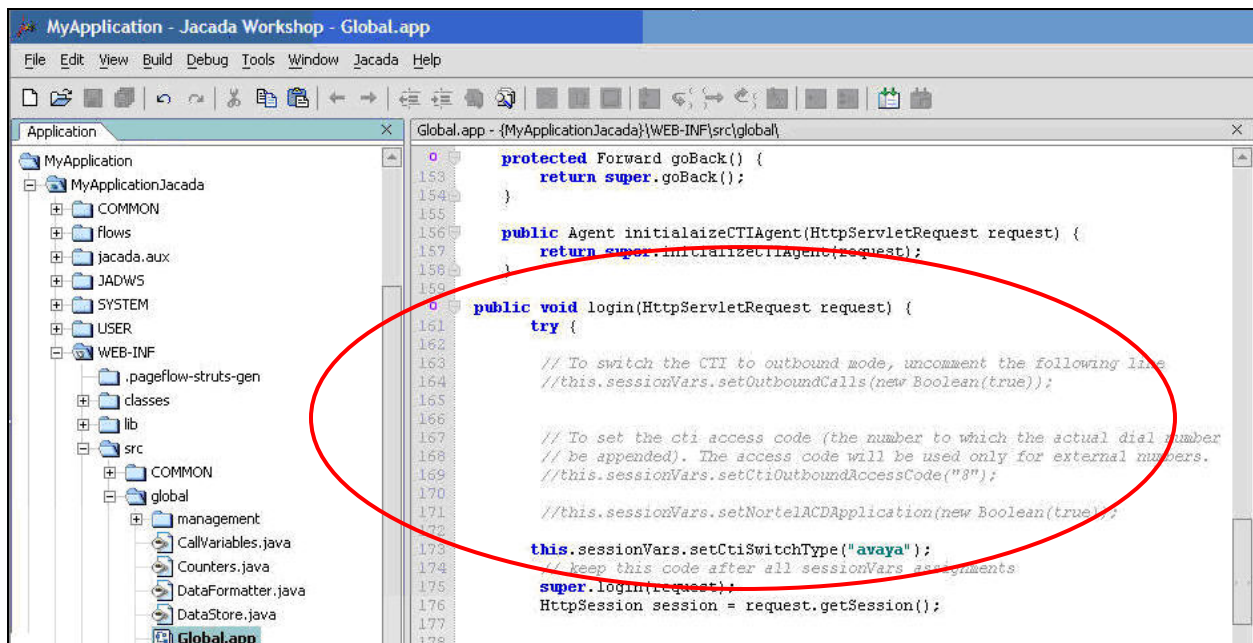
The **Jacada Workshop** screen is displayed. From the menu bar, select **File > New** to bring up the **New Application** dialog box shown below. Select **Jacada** and **Jacada Workspace Application**. Enter the desired **Directory** and **Name**, and click on **Create**.



6.6. Administer Switch Type

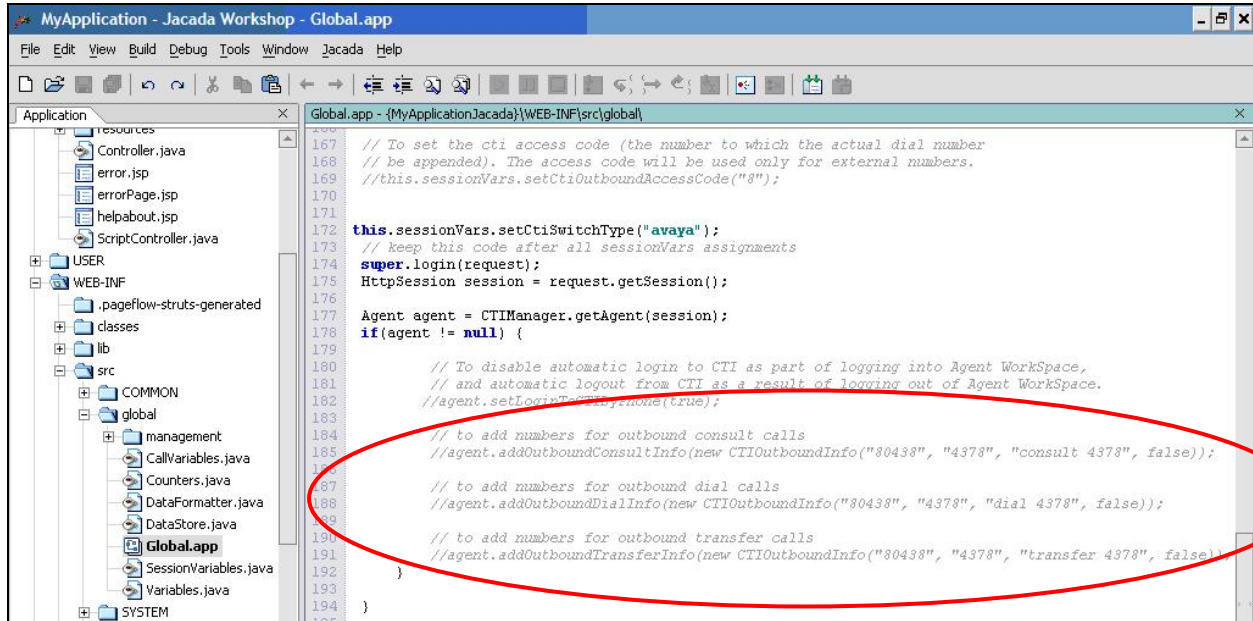
The **MyApplication** screen is displayed. Expand **MyApplication > MyApplicationJacada > WEB-INF > src > global** in the left pane, and select **Global.app**. Note that the application and project names may vary. In this case, “MyApplication” is the application name, and the project name is automatically created by Jacada Workspace by concatenating “Jacada” to the application name, or “MyApplicationJacada”.

Scroll down the screen in the right pane to locate the **login** function. Add the line “`this.sessionVars.setCtiSwitchType(“avaya”);`” as shown below. The entered switch type must match the Envoy CTI logical identifier from **Section 5.2**.



6.7. Administer Numbers

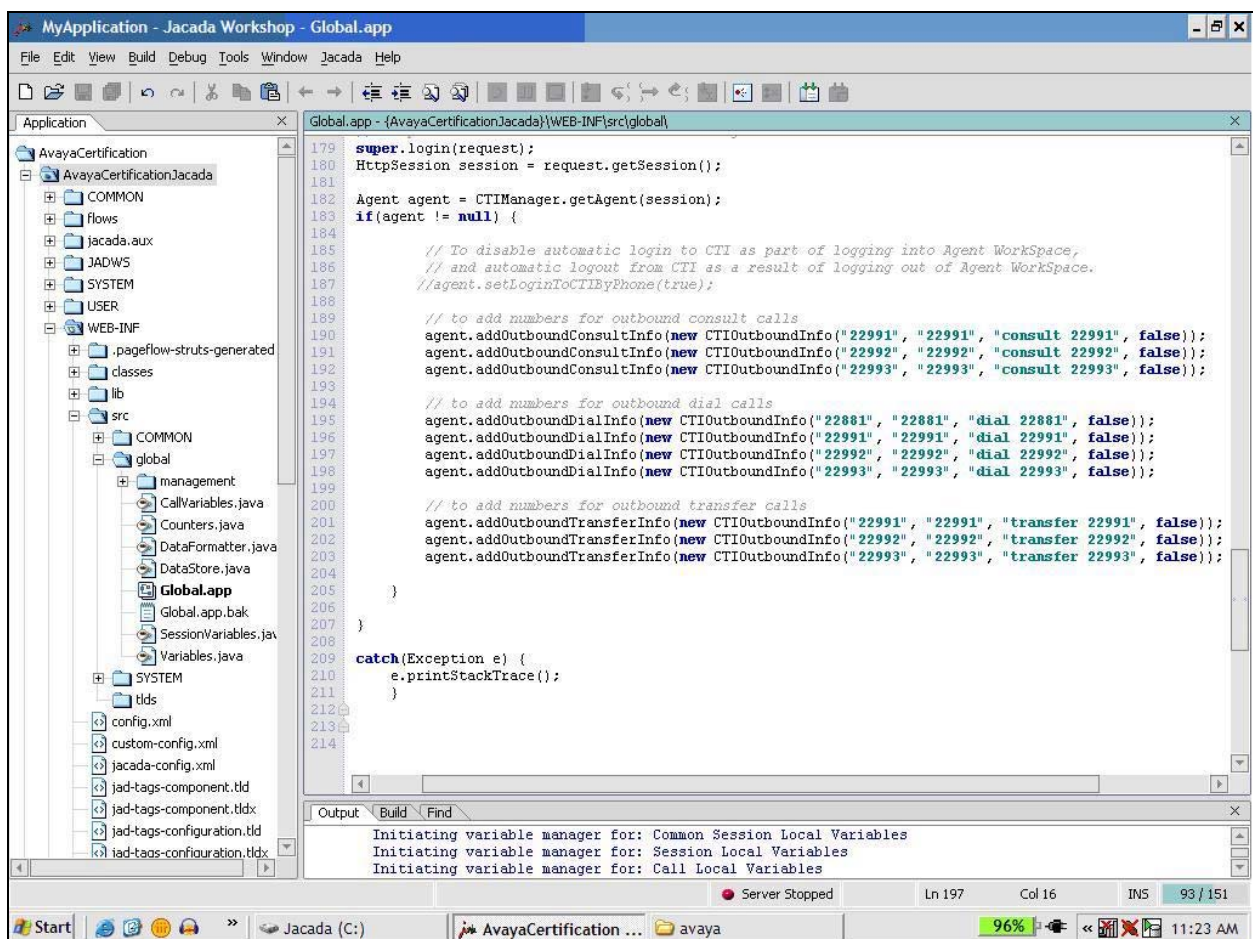
Scroll down the screen in the right pane a little further to the **add numbers** section, as shown below.



For the **add number for outbound consult calls** section, uncomment the line by removing the leading “//”, and replace the sample extensions with a valid extension. Add a new line for each additional extension. Note that these extensions will show up in a drop down list when the agent clicks on the **Conf** button from the desktop, such that the agent may select an extension from the list to conference into the call.

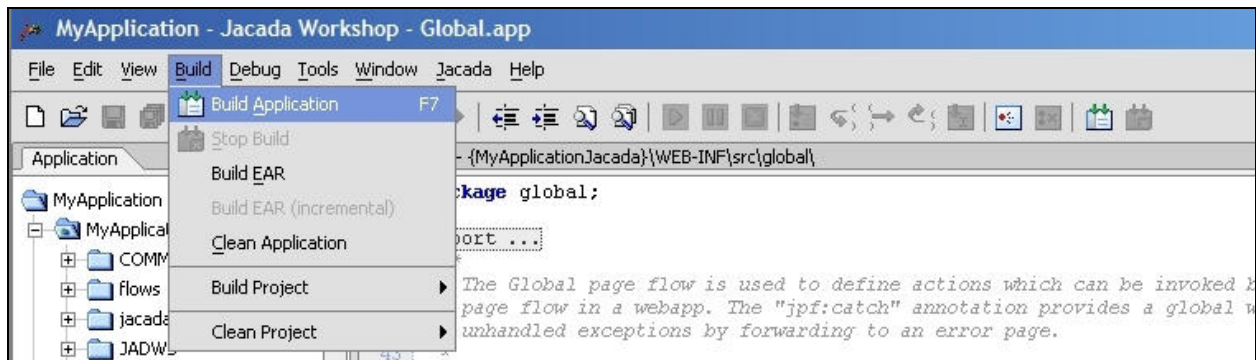
For the **add numbers for outbound dial calls** section, follow the same procedure to add lines for the extensions to appear in a drop down list, when the agent clicks on the **Dial** button from the desktop to select an extension from the list to make an outgoing call.

For the **add numbers for outbound transfer calls** section, follow the same procedure to add lines for the extensions to appear in a drop down list, when the agent clicks on the **Transfer** button from the desktop to select an extension from the list to transfer the call.



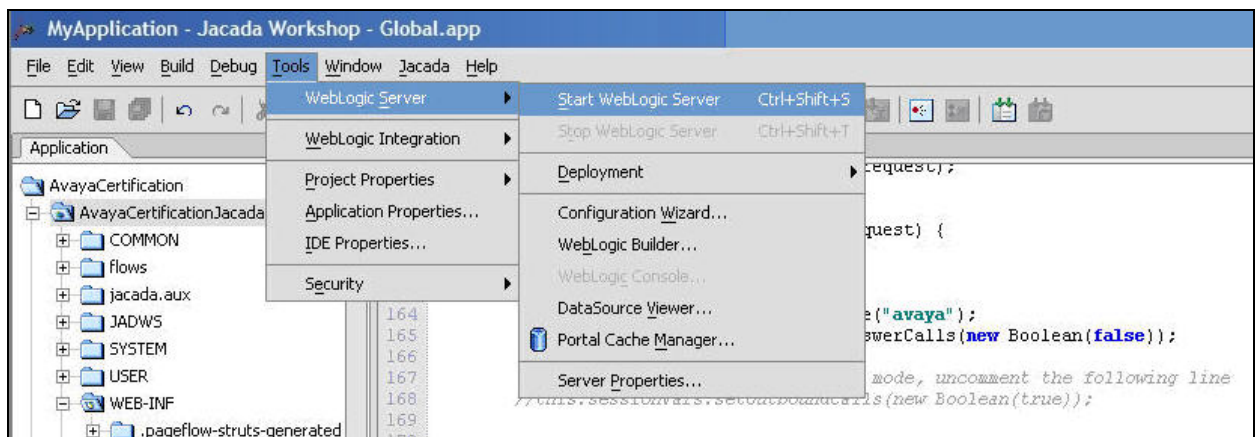
6.8. Build Application

From the menu bar, select **Build > Build Application** to build the application.

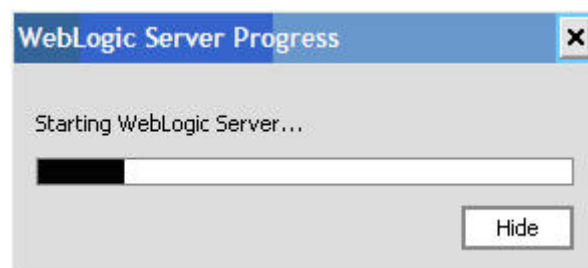


6.9. Start WebLogic Server

From the menu bar, select **Tools > WebLogic Server > Start WebLogic Server**.



The **WebLogic Server Progress** box is displayed, and shows the progress.



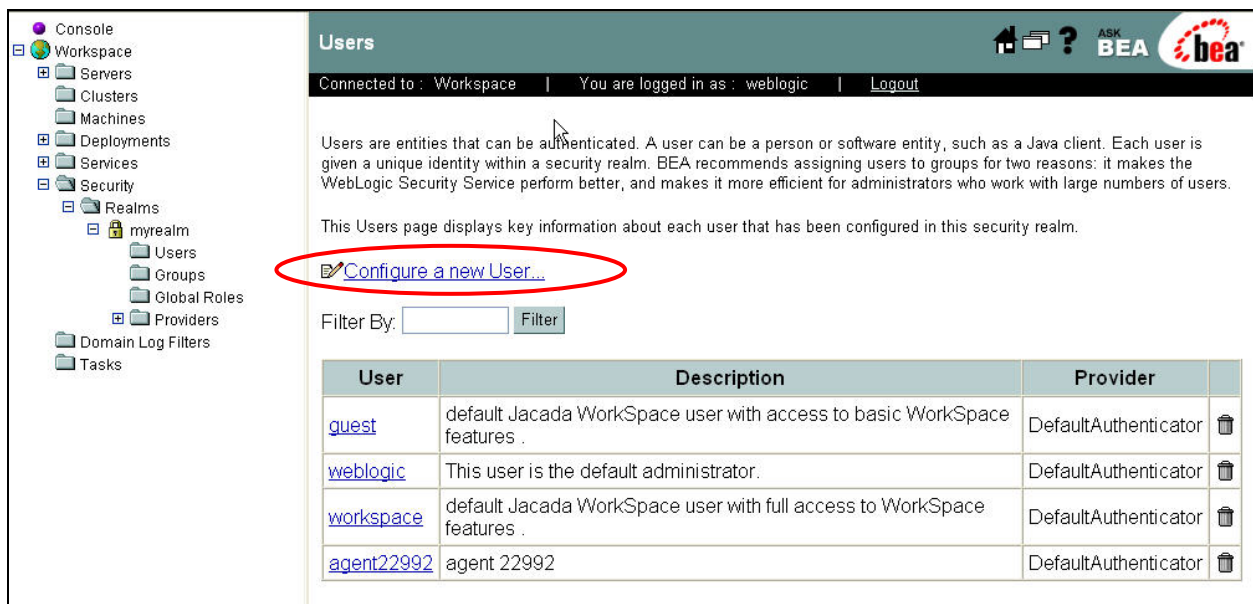
6.10. Launch WebLogic Server

Access the WebLogic web interface by using the URL “http://<ip-address>:7001/console” in an Internet browser window, where “<ip-address>” is the IP address of the WebLogic server. Note that the IP address for the WebLogic server may vary, and in this case “192.45.20.231” is used, as the WebLogic server is co-resident on the Jacada Workspace server. Log in with the appropriate credentials and click on **Sign In**.



The screenshot shows the 'Administration Console' for 'BEA WebLogic Server 8.1'. The main heading is 'WebLogic Server Administration Console' with the instruction 'Sign in to work with the WebLogic Server'. Below this are two input fields: 'Username:' and 'Password:', both containing masked characters (dots). A 'Sign In' button is located at the bottom right of the login area.

Expand **Workspace > Security > Realms > myrealm** in the left pane, and select **Users**. The **Users** screen is displayed into the right pane, as shown below. Click on **Configure a new User**.



The screenshot displays the 'Users' page within the WebLogic console. The left-hand navigation pane shows a tree structure with 'Workspace' expanded, leading to 'Security' > 'Realms' > 'myrealm' > 'Users'. The main content area has a header 'Users' and a status bar indicating 'Connected to : Workspace' and 'You are logged in as : weblogic'. Below the header, there is explanatory text about users and a link 'Configure a new User...' which is circled in red. A 'Filter By:' input field and a 'Filter' button are also present. A table lists the configured users.

| User | Description | Provider | |
|----------------------------|---|----------------------|--|
| guest | default Jacada WorkSpace user with access to basic WorkSpace features . | DefaultAuthenticator | |
| weblogic | This user is the default administrator. | DefaultAuthenticator | |
| workspace | default Jacada WorkSpace user with full access to WorkSpace features . | DefaultAuthenticator | |
| agent22992 | agent 22992 | DefaultAuthenticator | |

The **myrealm> Create User** screen is displayed. Select the **General** tab, and enter desired values for the **Name**, **Description**, **Password**, and **Confirm Password** fields. Note that the entered value for the **Name** field must match the user name administered in **Section 6.2**.

myrealm> Create User

Connected to : Workspace | You are logged in as : weblogic | Logout

General Groups Details

This page allows you to define a user in this security realm.

Name:

The login name for this user.

Description:

A short description of this user. For example, the user's full name.

Password:

Confirm Password:

The password associated with the login name for this user.

Apply

Select the **Groups** tab. Select the appropriate permission group from the **Possible Groups** section on the left, and use the right arrow to move to the **Current Groups** section on the right. For the compliance testing, the “JwsAdministrators” group was selected, which has administrator permissions. Typically the “JwsCTIUsers” permissions would be sufficient for agents. Click on **Apply**. Repeat these procedures to add a user for each agent administered in **Section 6.2**.

myrealm> User

Connected to : Workspace | You are logged in as : weblogic | Logout

[Configure a new User...](#)

General Groups Details

This page allows you to select the groups to which this user belongs.

Group Membership:

| Possible Groups | Current Groups |
|---------------------------|-------------------|
| Administrators | JwsAdministrators |
| Deployers | |
| IntegrationAdministrators | |
| IntegrationDeployers | |
| IntegrationMonitors | |
| IntegrationOperators | |
| IntegrationUsers | |
| JwsCTIUsers | |
| JwsDefaultUsersGroup | |
| JwsManagers | |

Apply

7. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying Jacada Workspace on the following: screen pop of calling party number for inbound call delivery/conference/transfer scenarios, login/logout and change work modes via the desktop, and call related actions such as hold/unhold/conference/transfer/dial via the desktop.

The serviceability testing focused on verifying the ability of Jacada Workspace to recover from adverse conditions, such as disconnecting the Ethernet cable for the CTI link to Envoy CT Connect.

7.1. General Test Approach

All feature and serviceability test cases were performed manually. Upon start of the application, Jacada Workspace requested monitoring and control of calls to all administered agents. Incoming calls were made to the available agents, to verify Jacada Workspace screen pop of calling party number on the answering agent's desktop. Manual call controls from the agent desktops were exercised to verify call control capabilities.

7.2. Test Results

All feature test cases were executed and passed.

There were two observations from the compliance testing. The first is that patch CR070108 is needed in order to have the calling party number displayed on the screen for transferred calls. This patch can be downloaded from the Jacada technical support web site, under identification ATL-27739.

The second observation is that upon disconnecting the LAN cable to the Jacada Workspace server for more than 8 seconds and then reconnecting, the CTI monitoring and control is not automatically re-established after the link is recovered. The workaround is for the agents to switch to manual mode upon receiving a message from the Jacada Workspace server, and to log out and log back into the application to re-establish the CTI monitoring and control. This workaround is documented on the Jacada technical support web site, under identification ATL-27738.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Application Enablement Services, Envoy CT Connect, and Jacada Workspace.

8.1. Verify Avaya Communication Manager

Verify the status of the administered CTI link by using the “status aescvs cti-link” command. Verify the **Service State** is “established” for the CTI link number administered in **Section 3.6**, as shown below.

```
status aescvs cti-link
```

| AE SERVICES CTI LINK STATUS | | | | | | |
|-----------------------------|---------|----------|--------------------|---------------|-----------|-----------|
| CTI Link | Version | Mnt Busy | AE Services Server | Service State | Msgs Sent | Msgs Rcvd |
| 1 | 4 | no | AES-DevCon2 | established | 43 | 24 |
| 2 | 4 | no | AES-DevCon2 | restarted | 30 | 15 |

8.2. Verify Avaya Application Enablement Services

From the **CTI OAM Home** menu, verify the status of the DLG link by selecting **Status and Control > Services Summary** from the left pane. Click on **DLG Service**, followed by **Details** (not shown). The **DLG Service Summary** screen is displayed. Verify that the **Connection Status** is “Link Up”, as shown below.

AVAYA

Application Enablement Services

Operations Administration and Maintenance

OAM Home

CTI OAM Home

Administration

Status and Control

Switch Conn Summary

Services Summary

Maintenance

Alarms


Logs

Utilities

Help

You are here: > [Status and Control](#) > [Services Summary](#)

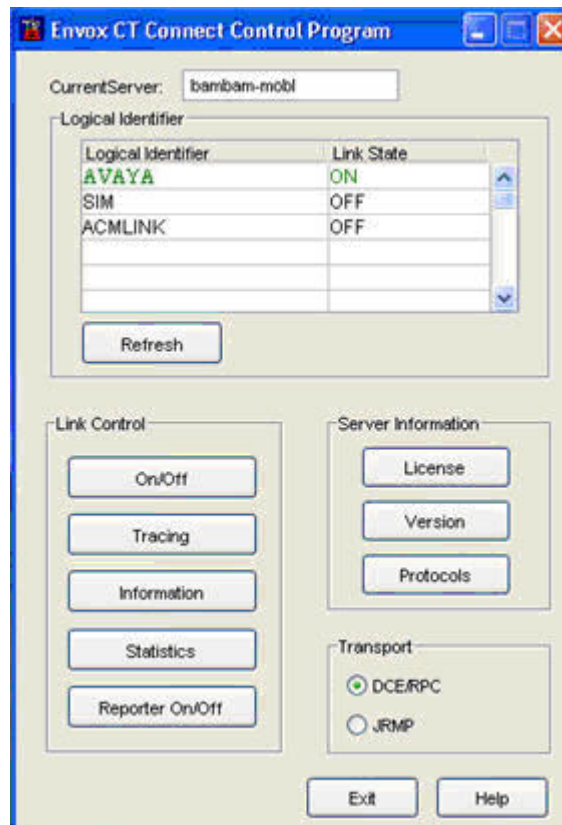
DLG Service Summary

| Switch Connection Name | Switch CTI Link | Connection Status | Since | Service State | Remote Host Name or IP Address:Port | Client Link | Local IP | Msgs To Switch | Msgs From Switch | Msg Period |
|---|-----------------|-------------------|-----------------------|---------------|-------------------------------------|-------------|---------------|----------------|------------------|------------|
|  devcon2758700 | 1 | Link Up | 2007-01-09 15:50:50.0 | online | 192.45.20.231:1924 | 1 | 192.45.20.152 | 30 | 29 | 30 |
| <div><div>Disconnect Clients</div><div>Online</div><div>Offline</div></div> | | | | | | | | | | |

8.3. Verify Envoy CT Connect

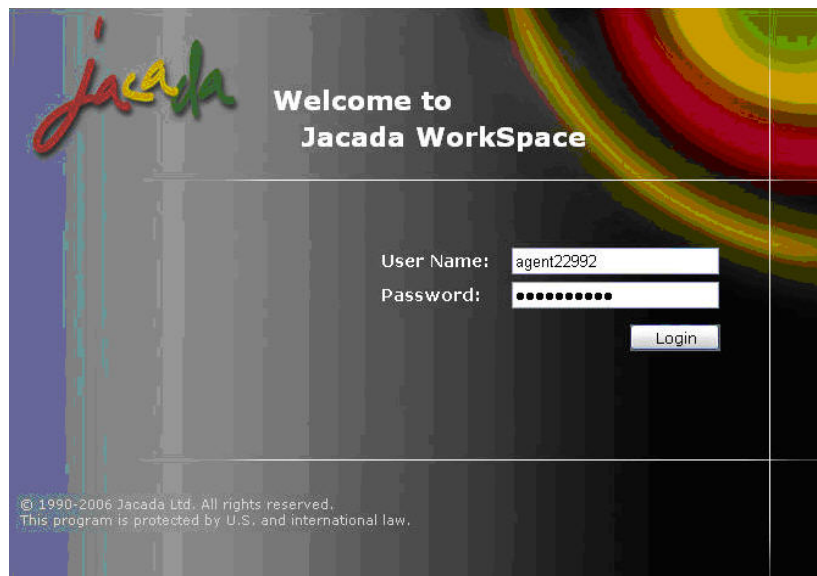
From the Envoy CT Connect server, select **Start > All Programs > Envoy CT Connect Server > Control Program** to bring up the **Envoy CT Connect Control Program** screen below.

Check that the **Link State** associated with the administered **Logical Identifier** from **Section 5.2** (in this case “AVAYA”) is “ON”.

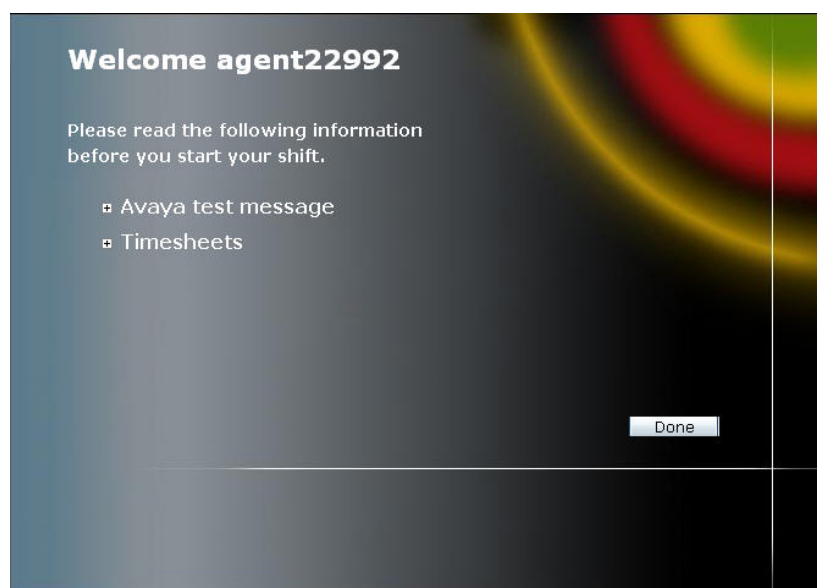


8.4. Verify Jacada Workspace

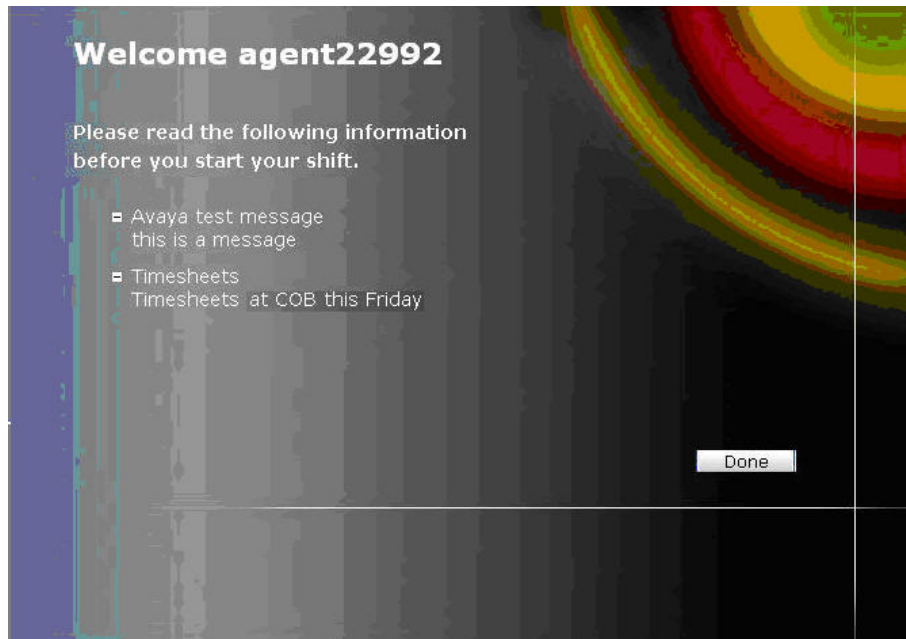
From the Jacada Workspace client, access the Jacada Workspace interface by using the URL “http://<ip-address>:7001/<project-name>” in an Internet browser window, where “<ip-address>” is the IP address of the Jacada Workspace server, and <project-name> is the project name from **Section 6.6**. In this case, the project name is “MyApplicationJacada”. Enter the appropriate user name and password from **Section 6.10**, and click on **Login**.



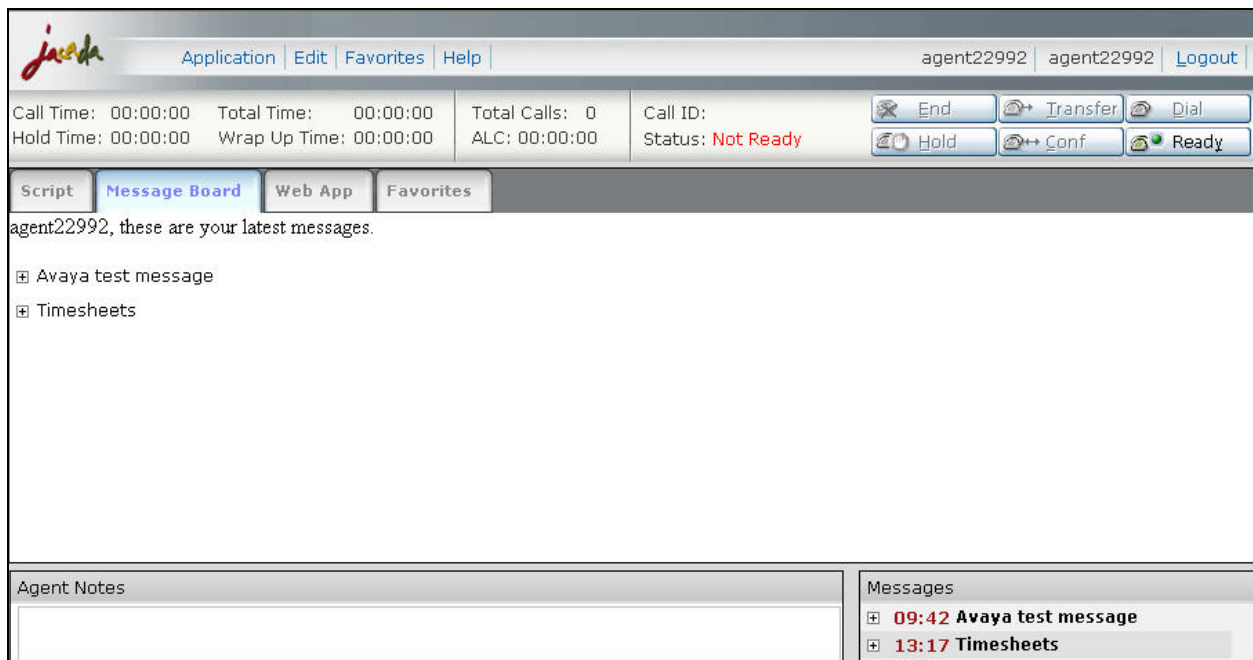
The **Welcome agent22992** screen is displayed, along with two messages that were created for the application. The application can be customized to display important messages that must be read by agents upon initial log in. Refer to the Jacada Workspace documentation in **Section 10** for configuration of these messages. Click on the plus icon to display the messages.



The detail messages are displayed as shown below. Click on **Done** to proceed with log in.



The **Jacada** screen is displayed on the agent desktop. Click on the **Ready** button to place the agent into the available mode.



Verify that the agent **Status** shows “Ready” as shown below.

The screenshot shows the Jacada Workspace interface for agent22992. The top bar includes the Jacada logo and navigation links: Application, Edit, Favorites, Help. The agent's name 'agent22992' is displayed on the right. Below the top bar, a status bar shows call metrics: Call Time: 00:00:00, Total Time: 00:00:00, Total Calls: 0, Call ID: (empty), Hold Time: 00:00:00, Wrap Up Time: 00:00:00, ALC: 00:00:00, and Status: Ready. To the right of the status bar are buttons for End, Transfer, Dial, Hold, Conf, and Busy. Below the status bar is a tabbed interface with Script, Message Board, Web App, and Favorites. The Message Board tab is active, displaying the message: 'agent22992, these are your latest messages.' Below this message are two expandable items: 'Avaya test message' and 'Timesheets'. At the bottom of the interface are two sections: Agent Notes (empty) and Messages (containing '09:42 Avaya test message' and '13:17 Timesheets').

Make an incoming call to the Skill group with an available agent “22992”. Verify that the call is delivered to the agent, and that Jacada Workspace populates the agent desktop with the calling party number in the **Call ID** field. Verify that the **Status** field shows “In Call”, the **Call Time** and **Total Time** fields start incrementing, the **End, Hold, Transfer, Conf** buttons becomes enabled, and that the **Script** section shows the sample script.

The screenshot shows the Jacada Workspace interface for agent22992 during an incoming call. The top bar is the same as the previous screenshot. The status bar now shows: Call Time: 00:00:15, Total Time: 00:00:15, Total Calls: 0, Call ID: 22881, Hold Time: 00:00:00, Wrap Up Time: 00:00:00, ALC: 00:00:00, and Status: In Call. The buttons for End, Transfer, Dial, Hold, Conf, and Busy are now enabled. The tabbed interface shows the Script tab active. The Script section displays a sample script: 'Thank you for calling X. How may I help you?' with two options: 'Option 1' (selected) and 'Option 2'. Below the script are 'Back' and 'Next' buttons, and the URL '/flows/sampleScript/index.jsp'. The Agent Notes section is empty, and the Messages section contains the same messages as the previous screenshot.

9. Support

Technical support on Jacada Workspce can be obtained through the following:

- **Phone:** (888) 261-7618
- **Web:** <http://support.jacada.com>
- **Email:** support@jacada.com

10. Conclusion

These Application Notes describe the configuration steps required for Jacada Workspace 4.0 to interoperate with Avaya Communication Manager 3.1.2 using Avaya Application Enablement Services 3.1.2 and Envoy CT Connect 6.1. All feature and serviceability test cases were completed.

There were two observations from the compliance testing. The first is that patch CR070108 is needed in order to have the calling party number displayed on the screen for transferred calls. This patch can be downloaded from the Jacada technical support web site, under identification ATL-27739.

The second observation is that upon disconnecting the LAN cable to the Jacada Workspace server for more than 8 seconds and then reconnecting, the CTI monitoring and control is not automatically re-established after the link is recovered. The workaround is for the agents to switch to manual mode upon receiving a message from the Jacada Workspace server, and to log out and log back into the application to re-establish the CTI monitoring and control. This workaround is documented on the Jacada technical support web site, under identification ATL-27738.

11. Additional References

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

- *Administrator Guide for Avaya Communication Manager*, Document ID 03-300509, Issue 2.1, May 2006, available at <http://support.avaya.com>.
- *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide Release 3.1.2*, Document ID 02-300357, Issue 4, September 2006, available at <http://support.avaya.com>.
- *Envox CT Connect 6.1 Installation and Configuration*, Software/Version Envoy CT Connect 6.1, available at <http://www.envoy.com>.
- *Jacada Workspace Administrator Guide*, Version 4.0, available from the Jacada Workspace 4.0 installation CD.
- *Jacada Workspace Developer Guide*, Version 4.0, available from the Jacada Workspace 4.0 installation CD.

©2007 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 Developer*Connection* Program at devconnect@avaya.com.