CA Workload Automation DE

Web Client Implementation Guide

r11.3 SP3

technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Workload Automation DE
- CA Workload Automation Desktop Client (CA WA Desktop Client)
- CA Workload Automation DE Web Client
- CA Workload Automation High Availability DE (CA WA High Availability)
- CA Workload Automation Web Services (CA WA Web Services)
- CA Workload Automation Agent for UNIX (CA WA Agent for UNIX)
- CA Workload Automation Agent for Linux (CA WA Agent for Linux)
- CA Workload Automation Agent for Windows (CA WA Agent for Windows)
- CA Workload Automation Agent for i5/OS (CA WA Agent for i5/OS)
- CA Workload Automation Agent for z/OS (CA WA Agent for z/OS)
- CA Workload Automation Agent for Application Services (CA WA Agent for Application Services)
- CA Workload Automation Agent for Web Services (CA WA Agent for Web Services)
- CA Workload Automation Agent for Micro Focus (CA WA Agent for Micro Focus)
- CA Workload Automation Agent for Databases (CA WA Agent for Databases)
- CA Workload Automation Agent for SAP (CA WA Agent for SAP)
- CA Workload Automation Agent for PeopleSoft (CA WA Agent for PeopleSoft)
- CA Workload Automation Agent for Oracle E-Business Suite (CA WA Agent for Oracle E-Business Suite)
- CA Workload Automation Restart Option EE (CA WA Restart Option)
- CA Spectrum® Service Assurance (CA Spectrum SA)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction to CA Workload Automation DE Web Client 7

Chapter 2: System Requirements 11

Chapter 3: Installing CA Workload Automation DE Web Client 13

Chapter 4: Post-Installation Tasks 35

Chapter 5: Troubleshooting CA Workload Automation DE Web Client 45

Index 51

Chapter 1: Introduction to CA Workload Automation DE Web Client

Read this chapter to learn about CA Workload Automation DE Web Client.

This section contains the following topics:

What's New in CA Workload Automation DE Web Client

CA Workload Automation DE Web Client Release 11.3 provides support for CA Workload Automation DE r11.3. CA Workload Automation DE Web Client includes the following major enhancements:

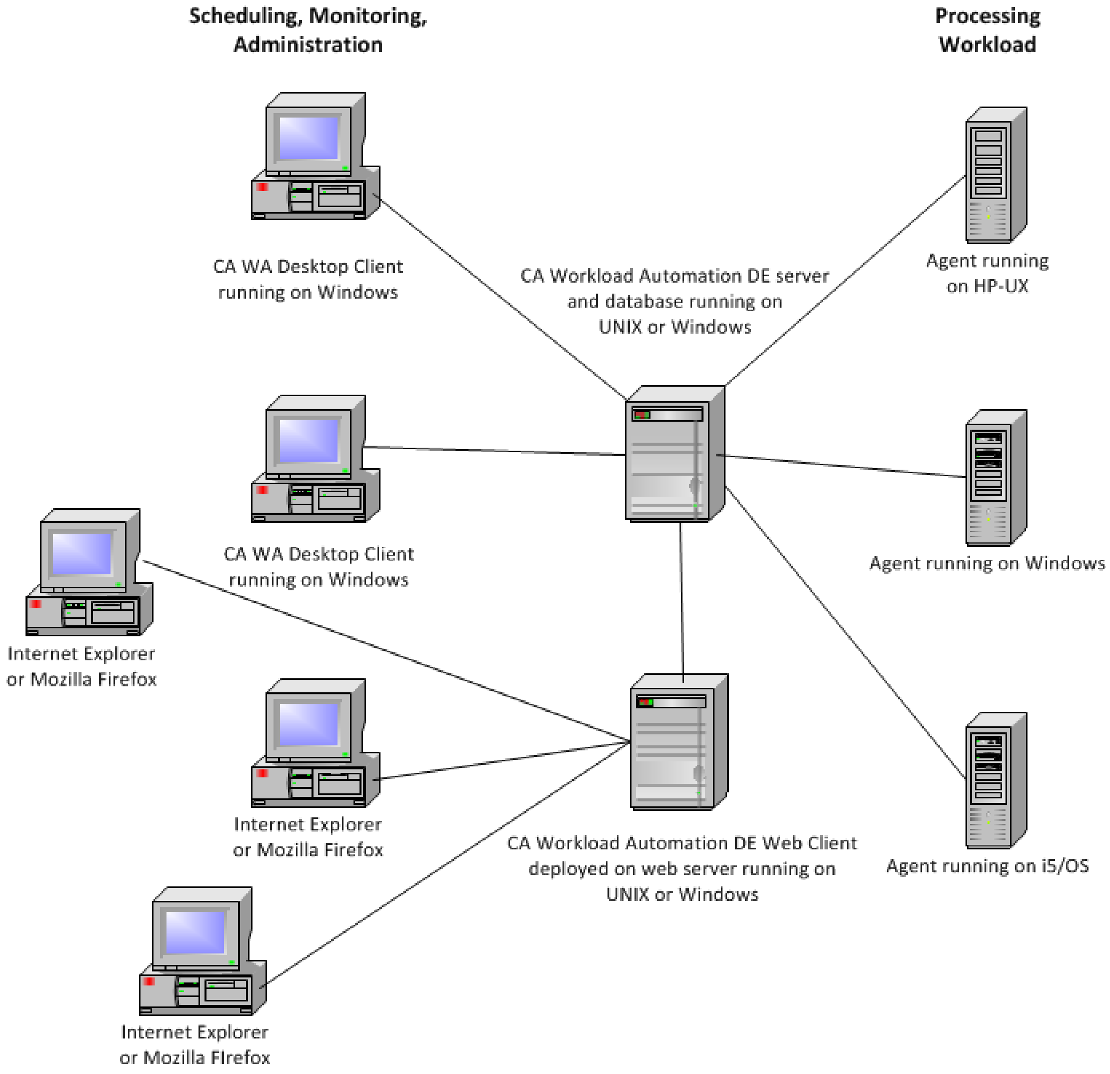
- Support for the following new job types in Workload Director:
  - Wake on LAN
  - SNMP Subscribe
  - SNMP Trap Send
  - SNMP Value Get
  - SNMP Value Set
  - SCP
  - SFTP
  - JMX-MBean Create Instance
  - JMX-MBean Remove Instance
  - Copy Single Request
- Ability to define site commands that are to be executed prior to file transfer in an FTP job
- Ability to specify a reason when issuing job- or Application-level commands in Workload Director
- Ability to view the reason messages in a command log for a job or Application in Workload Director
- Support for new monitor states Force completed, Global variable wait, and Resource wait

Note: For more information about the enhancements, see *CA Workload Automation DE Release Notes*.

About CA Workload Automation DE Web Client

CA Workload Automation DE Web Client provides you with the convenience of connecting directly to the CA Workload Automation DE server using a standard web browser. When connected to the server through CA Workload Automation DE Web Client, you can monitor and control workload in your production environment and quickly respond to exceptional situations.

The following diagram illustrates how CA Workload Automation DE Web Client works with other system components.


Scheduling, Monitoring, Administration
Processing Workload
CA WA Desktop Client running on Windows
CA Workload Automation DE server and database running on UNIX or Windows
Agent running on HP-UX
CA WA Desktop Client running on Windows
Agent running on Windows
Internet Explorer or Mozilla Firefox
Internet Explorer or Mozilla Firefox
CA Workload Automation DE Web Client deployed on web server running on UNIX or Windows
Agent running on i5/OS
Internet Explorer or Mozilla FIrefox

Note: For more information about installing and administering CA Workload Automation DE, see the *CA Workload Automation DE Implementation Guide* and the *CA WA Desktop Client Admin Perspective Help*.

CA Workload Automation DE Web Client Components

CA Workload Automation DE Web Client consists of three components: Workload Director, Workload Views, and Event Manager. If you are familiar with CA WA Desktop Client, you will see similarities between its Monitor perspective and the Web Client Workload Director. The Web Client Event Manager is similar to the Events view in the CA WA Desktop Client Services perspective. The Web Client Workload Views are similar to Custom Views in the CA WA Desktop Client Monitor perspective.

Workload Director

You can use Workload Director to do the following:

- View Applications and jobs in a table grid
- Issue Application-level commands
- Issue job-level commands
- Reset job definitions
- Insert jobs

Workload Views

You can use four Workload Views to monitor jobs based on the following job states:

- Executing
- Failed
- Overdue
- Waiting for Resources

Event Manager

You can use the Event Manager to do the following:

- View Event details
- Bypass, hold, release, resume, suspend, and trigger Events

Chapter 2: System Requirements

Read this chapter to verify your system requirements.

This section contains the following topics:

Prerequisites

CA Workload Automation DE Web Client has the following prerequisites:

- CA Workload Automation DE r11.3
- Internet Explorer 8 or higher
- Tomcat web server 6.0.35 (Tomcat is packaged with the Setup file)

Web Server Machine Requirements

You can install CA Workload Automation DE Web Client on the following platforms:

Platform	Minimum Hardware	Operating System
Linux x86_64	■ 2 Intel Xeon processors, 2.8 GHz each ■ 2 GB RAM ■ 75 GB hard drive	■ Red Hat Enterprise Linux EA/AS 6 (64-bit) ■ SUSE Linux Enterprise Server 11 (64-bit) ■ Linux Kernel 2.4.21-15
Solaris SPARC	■ Sun V440 ■ 2 UltraSPARC IIIi processors, 1.5 GHz each ■ 2 GB RAM ■ 75 GB hard drive	Solaris 11 (64-bit)
Windows	■ 2 Intel Xeon processors, 2.8 GHz each ■ 2 GB RAM ■ 75 GB hard drive	■ Windows 7 (64-bit) ■ Windows 2008 (64-bit)

CA Workload Automation DE Web Client User Machine Requirements

The machines for your CA Workload Automation DE Web Client users have the following requirements:

Component	Requirement
Operating System	Windows 2000 or higher or Windows XP Professional
Processor	Intel Pentium, 1.0 GHz or higher
Monitor	Video support for at least 256 colors at 1024x768 resolution
Memory	512 MB RAM or higher
Network	Active IP connection to your CA WA server

Chapter 3: Installing CA Workload Automation DE Web Client

This section contains the following topics:

Installation Options

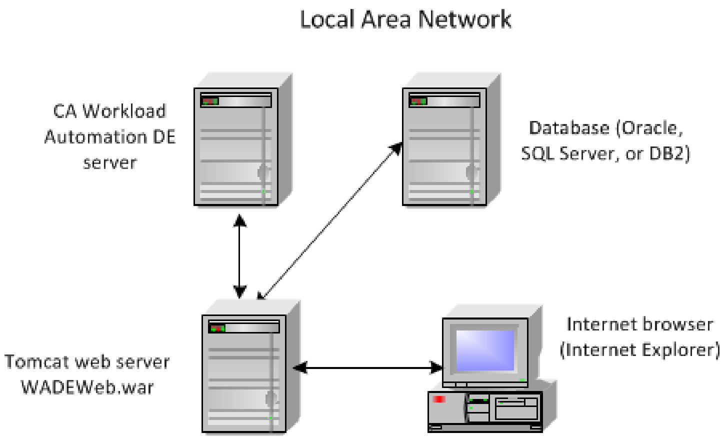
To launch CA Workload Automation DE Web Client, you must have the WADEWeb.war file running on a Tomcat web server.

DB2 is supported as a database for CA Workload Automation DE servers on AIX. An additional war file is generated for it. The installer lets you select the DB2 database, along with the existing Oracle and MS SQL databases.

Note: After the web application is deployed for a specific database, it can only be used to connect to CA Workload Automation DE servers that use that database.

Local Area Network Installations

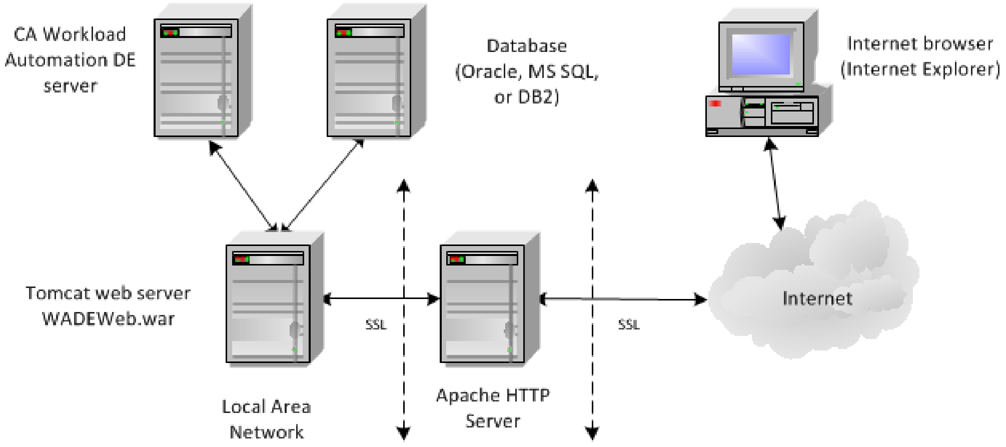
The following diagram shows how CA Workload Automation DE Web Client is used over a local area network:


Local Area Network
CA Workload Automation DE server
Database (Oracle, SQL Server, or DB2)
Tomcat web server WADEWeb.war
Internet browser (Internet Explorer)

You can use the Setup file to install the Tomcat web server and deploy the WADEWeb.war file automatically. Alternatively, on Windows you can manually install Tomcat (or use an existing Tomcat) and deploy the WADEWeb.war file.

Internet Installations

The following diagram shows how CA Workload Automation DE Web Client is used over the Internet using Apache HTTP Server:


CA Workload Automation DE server
Database (Oracle, MS SQL, or DB2)
Internet browser (Internet Explorer)
Tomcat web server WADEWeb.war
SSL
SSL
Internet
Local Area Network
Apache HTTP Server

You can use the Setup file to install the Tomcat web server and deploy the WADEWeb.war file automatically. Alternatively, on Windows you can manually install Tomcat (or use an existing Tomcat) and deploy the WADEWeb.war file. After you install CA Workload Automation DE Web Client, you can optionally configure it to work with Apache HTTP Server on Windows. You require Apache HTTP Server to use SSL.

How to Install CA Workload Automation DE Web Client with Tomcat

To install CA Workload Automation DE Web Client with Tomcat, follow these steps:

1. Install CA Workload Automation DE Web Client:
   - On UNIX (see page 16)
   - On Windows using the automated installation (see page 17)
   - On Windows using the manual installation (see page 18)

   Note: The manual installation is required to deploy CA Workload Automation DE Web Client into an existing Tomcat server.

2. (Optional) Configure CA Workload Automation DE Web Client to Work with Apache on Windows (see page 20).

   Note: You require Apache HTTP Server to use SSL or to hide the Tomcat server host name and port from the end user.

3. (Optional) Configure CA Workload Automation DE Web Client for Windows authentication on Microsoft SQL Server (see page 33).
4. Start the Web Client server (see page 36).
5. Launch CA Workload Automation DE Web Client (see page 37).
6. Log on to the CA Workload Automation DE server (see page 38).
7. Verify your installation (see page 39).
8. (Optional) Register CA Workload Automation DE Web Client as a Windows service (see page 41).

Install CA Workload Automation DE Web Client on UNIX

You can install CA Workload Automation DE Web Client using an interactive console program.

Note: Before you install CA Workload Automation DE Web Client, uninstall the existing installation (see page 43).

To install CA Workload Automation DE Web Client on UNIX

1. Log in as root.
2. Download the Setup.bin file from the CA Support Online website, found at http://ca.com/support.
3. Copy or FTP the Setup.bin file to the target system and directory.
4. Enter the following command to start the installation:

   ```
   .\Setup.bin -i console
   ```

   The installation program opens.
5. Press Enter.

   The license agreement appears.
6. Enter **y** to accept the license agreement.
7. Continue with the installation by entering the required information.

   Note: During the installation process you are prompted for the installation path. Do not use an installation path that contains spaces.

   The installation settings are listed before the installation process begins.
8. Press Enter to begin the installation.

   The installation process begins, and the progress is displayed.
9. Press Enter when the installation completes.

   CA Workload Automation DE Web Client is installed on UNIX.

   Note: The installation program creates a log file named CA_WADE_Web_Client_11.3_InstallLog.log in the installation directory, which you can review for installation errors.

Install CA Workload Automation DE Web Client on Windows Using the Automated Installation

You can install CA Workload Automation DE Web Client using an interactive program that lets you change and review your settings before starting the installation process. The installation program installs the JRE and Tomcat and deploys the WADEWeb.war file.

Notes: Before you install CA Workload Automation DE Web Client on a computer, uninstall the existing installation (see page 43).

To install CA Workload Automation DE Web Client on Windows

1. Download the Setup.exe file from the CA Support Online website, found at http://ca.com/support.
2. Copy or FTP the Setup.exe file to the target system and directory.
3. Double-click the Setup.exe file.

   The installation program opens.
4. Click Next.

   The License Agreement dialog opens.
5. Accept the license agreement and click Next.
6. Continue with the installation by entering the required information.

   The Pre-Installation Summary dialog opens as the last dialog before the installation process begins.
7. Review the settings and use the Previous button to change the values you entered.
8. Click Install to begin the installation.

   The installation process begins, and the progress is displayed.
9. Click Done to restart your system.

   CA Workload Automation DE Web Client is installed on Windows.

   Note: The installation program creates a log file named CA_WADE_Web_Client_11.3_InstallLog.log in the installation directory, which you can review for installation errors.

Install CA Workload Automation DE Web Client on Windows Using the Manual Installation

Instead of using the automated installation, you can manually install the JRE and Tomcat and deploy the WADEWeb.war file. The manual installation is required to deploy CA Workload Automation DE Web Client into an existing Tomcat server.

Notes:

- The StartWebClient and StopWebClient scripts are not available in a manual installation. You can create your own scripts to start and stop CA Workload Automation DE Web Client as described in the following procedure.
- You cannot run CA Workload Automation DE Web Client as a Windows service in a manual installation.
- If you use a Microsoft SQL Server database, only SQL Server authentication is supported in a manual installation. Windows authentication is not supported because some configuration files are missing in a manual installation. To use Windows authentication, you must install CA Workload Automation DE Web Client using the automated installation.

To install CA Workload Automation DE Web Client on Windows using the manual installation

1. Run the jre-6u29-windows-x64.exe file, provided with the CA Workload Automation DE Web Client installation files in the additional_files directory.

   JRE 1.6.0_29 is installed.

2. Unzip the apache-tomcat-6.0.35-windows-x64.zip file, provided with the CA Workload Automation DE Web Client installation files in the additional_files directory, to a directory.

   Note: If you already have an existing installation of Tomcat 6.0.35, you can skip this step. Other versions of Tomcat are not supported.

   Tomcat is installed.

3. Create a batch script with the following lines. You use this script to start CA Workload Automation DE Web Client.

   ```
   set JRE_HOME=JRE_install_dir
   set JAVA_HOME=
   cd Tomcat_install_dir\bin
   startup.bat
   ```

4. Replace the following variables in the lines you added in Step 3.

   JRE_install_dir

   Specifies your JRE installation directory.

   Tomcat_install_dir

   Specifies your Tomcat installation directory.

5. (Optional) Create a batch script with the following lines, replacing the variables as in the previous step. You use this script to stop CA Workload Automation DE Web Client.

   ```
   set JRE_HOME=JRE_install_dir
   set JAVA_HOME=
   cd Tomcat_install_dir\bin
   shutdown.bat
   ```

   You can also press Ctrl+c on the server console window to stop the server.

6. Locate the WADEWeb.war file, provided with the CA Workload Automation DE Web Client installation files under the following directories:

   - For Oracle database:

     `additional_files\oraclewar\WADEWeb.war`

   - For Microsoft SQL Server database:

     `additional_files\sqlwar\WADEWeb.war`

   - For IBM DB2 database:

     `additional_files\db2war\WADEWeb.war`

7. Copy the WADEWeb.war file into the following directory:

   `Tomcat_install_dir\webapps\`

   The WADEWeb.war file is deployed. CA Workload Automation DE Web Client is installed on Windows.

How to Configure CA Workload Automation DE Web Client to Work with Apache on Windows

After you install CA Workload Automation DE Web Client, you can optionally configure it to work with Apache HTTP Server on Windows. You require Apache HTTP Server to use SSL or to hide the Tomcat server host name and port from the end user.

To configure CA Workload Automation DE Web Client to work with Apache on Windows, follow these steps:

1. Install Apache HTTP Server (see page 21).
2. Configure Apache HTTPd with the Jakarta Tomcat connector (see page 22).
3. Create the workers.properties file (see page 23).
4. Create the mod_jk conf file (see page 24).
5. Edit the Apache httpd.conf file (see page 25).
6. (Optional) Configure Secure Socket Layer (SSL) for Apache (see page 26).
7. Edit the Tomcat server.xml file (see page 32).
8. Restart Apache HTTP Server (see page 32).

Install Apache HTTP Server

To configure CA Workload Automation DE Web Client to work with Apache, first install Apache HTTP Server.

To install Apache HTTP Server

1. Collect the following information for your installation.

   Network Domain

   Specifies the network that your server connects to.

   Server Name

   Specifies the IP address or name of the machine where you are installing Apache HTTP Server.

   Administrator's Email Address

   Specifies the email address of the person who will handle queries related to Apache HTTP Server.

2. Run one of the following files, provided with the CA Workload Automation DE Web Client installation files in the additional_files directory:

   - Non-SSL Apache HTTP Server:

     ```
     httpd-2.2.22-win32-x86-no_ssl.msi
     ```

   - SSL-enabled Apache HTTP Server:

     ```
     httpd-2.2.22-win32-x86-openssl-0.9.8t.msi
     ```

     Note: If you install the SSL-enabled Apache HTTP Server, additional configuration steps are required.

3. Follow the instructions on the screen. Pay attention to the following details:

   - On the Server Information dialog, leave the default option for All Users, on Port 80, as a Service -- Recommended selected.
   - On the Setup Type dialog, choose Typical.
   - On the Destination Folder dialog, make a note of the installation path you use.

   The installation program starts Apache when it completes the installation process.

4. Type the following in your web browser to verify the Apache HTTP Server installation:

   ```
   http://localhost/
   ```

   Your browser should display **It works!** If it does not display this text, check whether Apache is started.

Configure Apache HTTPd with Jakarta Tomcat Connector

After you install Apache HTTP Server, configure Apache HTTPd with the Jakarta Tomcat connector.

To configure Apache HTTPd with the Jakarta Tomcat Connector

1. Copy the mod_jk-1.2.31-httpd-2.2.3.so file, provided with the CA Workload Automation DE Web Client installation files in the additional_files directory, into the following directory:

   Apache_install_dir\modules

   Apache_install_dir

   Specifies your Apache installation directory.

2. Rename the mod_jk-1.2.31-httpd-2.2.3.so file to mod_jk.dll.

   Apache HTTPd is configured with the Jakarta Tomcat connector.

Create the workers.properties File

After you configure Apache HTTPd with the Jakarta Tomcat connector, create the workers.properties file manually.

To create the workers.properties file

1. Change to the following directory:

   Apache_install_dir\conf

   Apache_install_dir

   Specifies your Apache installation directory.

2. Create a text file named workers.properties in this directory.

3. Add the following lines to the workers.properties file:

```
ps=\
# Default ajp connector 8009 for Apache Tomcat
worker.ajp13.port=8009
# specifies the location of webclient host’s ip address
worker.ajp13.host=Tomcat_machine_name
# Sets the version of AJP used. The AJP listeners defined in Geronimo
# are AJP v13.
worker.ajp13.type=ajp13
```

4. Replace the following variable in the lines you added in Step 3:

   Tomcat_machine_name

   Specifies the IP address or machine name where you installed CA Workload Automation DE Web Client with Tomcat.

5. Save the workers.properties file.

   The workers.properties file is created.

Note: For more information about the workers.properties file, go to http://tomcat.apache.org/connectors-doc/reference/workers.html.

Create the mod_jk.conf File

After you create the workers.properties file, create the mod_jk.conf file manually. You will include the mod_jk.conf file in the Apache httpd.conf file that you edit in the next procedure.

To create the mod_jk.conf File

1. Change to the following directory:

   ```
   Apache_install_dir\conf
   ```

   Apache_install_dir

   Specifies your Apache installation directory.

2. Create a text file named mod_jk.conf in this directory.

3. Add the following lines to the mod_jk.conf file:

   ```
   #Apache HTTP Server & Tomcat NON-SSL Configuration...
   # Loads the Jakarta Tomcat Connector module
   LoadModule jk_module "Apache_install_dir\modules\mod_jk.dll"
   # Tells the module the location of the workers.properties file
   JkWorkersFile "Apache_install_dir\conf\workers.properties"
   # Specifies the location for this module's specific log file <optional>
   JkLogFile     "Apache_install_dir\logs\mod_jk.log"
   # Sets the module's log level to info <optional>
   JkLogLevel    info
   # Sets the module's log time stamp format <optional>
   JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
   # Sets a mount point from a context to a Tomcat worker. In this case
   # will allow access (forward the request) to the WADEWeb.
   JkMount /WADEWeb ajp13
   JkMount /WADEWeb/* ajp13
   ```

   Notes:

   - If you are going to configure SSL, you do not require this content.
   - The JKLogFile, JKLogLevel, and JKLogStampFormat configuration parameters are optional and can be omitted or commented out.

4. Replace the *Apache_install_dir* variable with your Apache installation directory.

5. Save the mod_jk.conf file.

   The mod_jk.conf file is created.

Edit the Apache httpd.conf File

After you create the mod_jk.conf file, edit the Apache httpd.conf file to configure the Apache server name and port and include the mod_jk.conf file.

To edit the Apache httpd.conf file

1. Change to the following directory:

   ```
   Apache_install_dir\conf
   ```

   Apache_install_dir

   Specifies your Apache installation directory.

2. Open the httpd.conf file in a text editor.

3. Locate the following line:

   ```
   Listen 80
   ```

4. Edit the line as follows:

   ```
   Listen Apache_server_name:Apache_port
   ```

   Apache_server_name

   Specifies the server name that you used when you installed the Apache HTTP server.

   Apache_port

   Specifies the port of the Apache HTTP server.

   Default: 80 (http); 443 (https)

   Note: We recommend that you use the default port so you do not need to remember the port to access the Apache server.

   The Apache server name and port are configured.

5. Add the following lines to the end of the httpd.conf file:

   ```
   #add the mod_jk.conf file to add the jk configurations
   Include conf/mod_jk.conf
   ```

   The mod_jk.conf file is included.

6. Save the httpd.conf file.

   The Apache httpd.conf file is edited.

How to Configure Secure Socket Layer (SSL) for Apache

You can optionally configure Secure Socket Layer (SSL) for Apache to provide encrypted communication over the Internet.

To configure SSL for Apache, follow these steps:

1. Create a signing certificate (see page 27).
2. Edit the Apache httpd.conf file for SSL (see page 29).
3. Overwrite the contents of the mod_jk.conf file (see page 29).

Create a Signing Certificate

To configure SSL for Apache, the first step is to create a signing certificate.

To create a signing certificate

1. Change to the following directory using a command prompt:

   ```
   Apache_install_dir\bin
   ```

   Apache_install_dir

   Specifies your Apache installation directory.

2. Enter the following command to create a certificate-signing request:

   ```
   openssl req -config Apache_install_dir\conf\openssl.cnf -new -out
   certificate_name.csr
   ```

   certificate_name

   Defines the name of the signing certificate.

   You are prompted to enter a PEM pass phrase.

3. Enter a pass phrase of at least four characters. Reenter the pass phrase when prompted for confirmation.

   You are prompted to enter the following information:

   ```
   Country Name (2 letter code)
   State or Province Name (full name)
   Locality Name (eg, city)
   Organization Name (eg, company)
   Organizational Unit Name (eg, section)
   Common Name (eg, your websites domain name)
   Email Address
   ```

   The common name should match the domain name that you entered when you installed Apache. The certificate will belong to this name.

   When you have completed entering the required information, you are prompted for a challenge password.

4. Enter the challenge password.

   The challenge password is created.

5. Enter the following command to remove the password phrase from the private key, making sure that you replace *certificate_name* with the name of the signing certificate you defined in Step 2:

   ```
   openssl rsa -in privkey.pem -out certificate_name.key
   ```

   Note: *certificate_name*.key should only be readable by Apache and the administrator.

   You are prompted for the PEM pass phrase.

6. Enter the PEM pass phrase that you entered in Step 3.

7. Delete the .rnd file to protect your private key against cryptographic attacks. The .rnd file contains the information for creating the key.

8. Enter the following command to create a self-signed certificate, making sure that you replace *certificate_name* with the name of the signing certificate you defined in Step 2:

   ```
   openssl x509 -in certificate_name.csr -out certificate_name.cert -req -signkey
   certificate_name.key -days n
   ```

   n

   Specifies the number of days until the certificate expires.

   Example: 365

   You can replace the self-signed certificate any time with a certificate from a certificate authority such as VeriSign.

9. Enter the following command, making sure that you replace *certificate_name* with the name of the signing certificate you defined in Step 2:

   ```
   openssl x509 -in certificate_name.cert -out
   certificate_name.der.crt -outform DER
   ```

10. Create a directory named ssl under *Apache_install_dir*\conf.

11. Move the *certificate_server_name*.key and *certificate_name*.cert files from the *Apache_install_dir*\bin directory into the ssl directory that you created:

    ```
    Apache_install_dir\conf\ssl
    ```

    The signing certificate is created.

Edit the Apache httpd.conf File for SSL

After you create a signing certification, edit the Apache httpd.conf file to load the SSL module and SSL configuration file.

To edit the Apache httpd.conf file for SSL

1. Change to the following directory:

   Apache_install_dir\conf

   Apache_install_dir

   Specifies your Apache installation directory.

2. Open the httpd.conf file in a text editor.

3. Locate the following line:

   ```
   #LoadModule ssl_module modules/mod_ssl.so
   ```

4. Uncomment this line by removing the #:

   ```
   LoadModule ssl_module modules/mod_ssl.so
   ```

   The SSL module is loaded.

5. Locate the following line:

   ```
   #Include conf/extra/httpd-ssl.conf
   ```

6. Uncomment this line by removing the #:

   ```
   Include conf/extra/httpd-ssl.conf
   ```

   The SSL configuration file is loaded.

7. Save the httpd.conf file.

   The httpd.conf file is edited for SSL.

Overwrite the Contents of the mod_jk.conf File

To complete the SSL configuration for Apache, overwrite the contents of the mod_jk.conf file that you created earlier with SSL information.

To overwrite the contents of the mod_jk.conf file

1. Change to the following directory:

   Apache_install_dir\conf

   Apache_install_dir

   Specifies your Apache installation directory.

2. Open the mod_jk.conf file in a text editor.

3. Overwrite the contents of the mod_jk.conf file with the following lines:

```
NameVirtualHost Apache_server_name:443
<VirtualHost Apache_server_name:443>
    SSLEngine on
    SSLOptions +StrictRequire
    <Directory />
        SSLRequireSSL
    </Directory>
    SSLProtocol -all +TLSv1 +SSLv3
    SSLCipherSuite HIGH:MEDIUM:!aNULL:+SHA1:+MD5:+HIGH:+MEDIUM
    SSLCertificateFile "Apache_install_dir/conf/ssl/certificate_name.cert"
    SSLCertificateKeyFile "Apache_install_dir/conf/ssl/certificate_name.key"
    SSLVerifyClient none
    SSLProxyEngine off
    <IfModule mime.c>
        AddType application/x-x509-ca-cert      .crt
        AddType application/x-pkcs7-crl         .crl
    </IfModule>
 SetEnvIf User-Agent ".*MSIE.*" \
# Loads the Jakarta Tomcat Connector module
LoadModule jk_module "Apache_install_dir\modules\mod_jk.dll"
# specifies the location for this module's specific log file <optional>
JkLogFile     "Apache_install_dir\logs\mod_jk.log"
# Sets the module's log level to info <optional>
JkLogLevel    info
# Sets the module's log time stamp format <optional>
JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
```

```
# Sets a mount point from a context to a Tomcat worker. In this case
# will allow access (forward the request) to the WADEWeb.
JkMount /WADEWeb ajp13
JkMount /WADEWeb/* ajp13
JkOptions +ForwardURICompat


</VirtualHost>
# tells the module the location of the workers.properties file
JkWorkersFile "Apache_install_dir\conf\workers.properties"
```

Note: The JKLogFile, JKLogLevel, and JKLogStampFormat configuration parameters are optional and can be omitted or commented out.

4. Replace the *Apache_server_name* variable with the server name that you used when you installed Apache HTTP Server.
5. Replace the *Apache_install_dir* variable with your Apache installation directory.
6. Replace the *certificate_name* variable with the name of the signing certificate that you created.
7. Save the mod_jk.conf file.

   The contents of the mod_jk.conf file are overwritten.

Note: For more information about the SSL options in the mod_jk.conf file, go to http://httpd.apache.org/docs/2.2/ssl/ssl_howto.html.

Edit the Tomcat server.xml File

To ensure a secure connection, edit the Tomcat server.xml file manually.

To edit the Tomcat server.xml File

1. Change to the following directory:

   install_dir\apache-tomcat-6.0.35\conf

   install_dir

   Specifies the directory where CA Workload Automation DE Web Client is installed.

2. Open the server.xml file in a text editor.
3. Locate the following lines:

   ```
   <Connector port="80" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443" />
   ```

4. Comment out the Connector tag using <!--   -->:

   ```
   <!--
   <Connector port="80" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443" />
   -->
   ```

   HTTP access from Tomcat to CA Workload Automation DE Web Client is disabled.

5. Save the server.xml file.

   The Tomcat server.xml file is edited.

Start Apache HTTP Server

Apache HTTP Server (Apache) must be active so that client machines can access CA Workload Automation DE Web Client. Whenever you reboot the Web Client server or edit an Apache configuration file, restart Apache.

Note: If you chose to run Apache as a service for all users as recommended during the installation, Apache will start up on its own.

To start Apache HTTP Server

1. Click Start in Windows to open the Start menu.
2. Select Program Files, Apache HTTP Server 2.2, Control Apache Server.
3. Select Start to start Apache or Restart to restart it.

   Apache HTTP Server is started.

How to Configure CA Workload Automation DE Web Client for Windows Authentication on Microsoft SQL Server

If you use a Microsoft SQL Server database with Windows authentication, additional configuration is required for the Web Client server to communicate with the database. Different steps are required depending on whether you log in to the Web Client computer using a Windows domain user account or an administrator account.

Note: These steps are not required if you installed CA Workload Automation DE Web Client on the same computer as the database.

To configure CA Workload Automation DE Web Client for Windows authentication using a domain user account, follow these steps:

1. Log in to the Web Client computer using the domain user account.
2. Start the Web Client server using *one* of the following options:
   - Start the Web Client server using the StartWebClient.bat script (see page 36).
   - Start the Web Client server as a service:
     a. Right-click the Install as Windows Service program shortcut. By default, the shortcut is located in Start, Programs, CA, WADE Web Client 11.3.
     b. Select Run as administrator from the pop-up menu.
     c. Configure the Web Client service to use the domain user account (see page 34).
     d. Start the Web Client service.

To configure CA Workload Automation DE Web Client for Windows authentication using an administrator account:

1. Log in to the Web Client computer using an administrator account.
2. Install the Web Client service using the Install as Windows Service program shortcut.

   By default, the shortcut is located in Start, Programs, CA, WADE Web Client 11.3.
3. Configure the Web Client service to use the domain user account (see page 34).
4. Start the Web Client service.

Note: You cannot start the Web Client server using the StartWebClient.bat script when logged in as an administrator user.

Configure the Web Client Service to Use the Domain User Account

If you use a Microsoft SQL Server database with Windows authentication, configure the Web Client service to use the domain user account.

To configure the Web Client service to use the domain user account

1. Click Start, Settings, Control Panel, Administrative Tools, Services.

   The Services dialog opens.

2. Right-click the Web Client service, and select Properties from the drop-down list.
3. Select the Log On tab.
4. Select the This account option button and specify the name of the domain user account using the following format:

   ```
   domain\user
   ```

5. Enter the password for the domain user account in the Password and the Confirm password fields and click OK.

   The Web Client service is configured to use the domain user account.

Chapter 4: Post-Installation Tasks

This section contains the following topics:

Start the Web Client Server

To use CA Workload Automation DE Web Client, you issue a command to run a script that starts the server. The script sets the JRE_HOME variable and starts the Tomcat web server.

Notes:

- On Windows, you can register CA Workload Automation DE Web Client as a Windows service (see page 41) and configure the service to start automatically whenever the system starts.
- If you use a Microsoft SQL Server database with Windows authentication, use the Web Client service to start the Web Client server when logged in as an administrator user.
- If you installed CA Workload Automation DE Web Client on Windows using the manual installation, use the batch script that you created to start the Web Client server.

To start the Web Client server

1. Change to the following directory at the command prompt:

   install_dir

   Specifies the directory where CA Workload Automation DE Web Client is installed.

2. Enter the following command:

   - On UNIX:

     ```
     StartWebClient.sh
     ```

   - On Windows:

     ```
     StartWebClient.bat
     ```

   The Web Client server starts.

Launch CA Workload Automation DE Web Client

To use CA Workload Automation DE Web Client, you first launch it in your browser.

Notes:

- To view CA Workload Automation DE Web Client pages that open as pop-up windows, disable your popup blocker option or add CA Workload Automation DE Web Client to the list of allowed sites in your browser.
- On Internet Explorer 9, a blank page appears when you log in to the CA Workload Automation DE server. To overcome this problem, add the Web Client URL to the Trusted Sites list in the Security tab of Internet Options.

To launch CA Workload Automation DE Web Client

1. Open your Web browser.
2. Enter the following URL in the Address field:
   - If you did not configure CA Workload Automation DE Web Client with Apache:

     ```
     http://Tomcat_machine_name:Tomcat_port/WADEWeb
     ```

     Tomcat_machine_name

     Specifies the IP address or machine name where you installed CA Workload Automation DE Web Client with Tomcat.

     Tomcat_port

     Specifies the Tomcat connector port number that you chose during installation.

     Default: 80 (automated installation); 8080 (manual installation)

     Note: If you are using the default port of 80, you can omit the port number in the address.

   - If you configured CA Workload Automation DE Web Client with Apache:

     ```
     http://Apache_server_name:Apache_port/WADEWeb/
     ```

     Apache_server_name

     Specifies the server name that you used when you installed the Apache HTTP server.

Apache_port

Specifies the port of the Apache HTTP server.

Default: 80 (http); 443 (https)

Note: If you are using the default port for the Apache HTTP server, you can omit the port number in the address.

Note: If you set up a Secure Socket Layer (SSL) for Apache on Windows, use the https protocol.

The Logon page appears.

Log on to the CA Workload Automation DE Server

To log on to the CA Workload Automation DE server, use the same logon information that you use to connect to CA WA Desktop Client.

To log on to the server

1. Enter the following information on the Logon page:

   User Name

   Specifies your server user ID.

   Default: SCHEDMASTER

   Password

   Specifies your server password.

   Default: schedmaster

   Limits: case-sensitive

   Address

   Specifies the IP address or DNS name of the server you want to connect to.

   Port

   Specifies the server client port number.

   Default: 7500

2. Click Logon.

   The Main Menu page opens to provide access to CA Workload Automation DE Web Client tools: Workload Director, Workload Views, and Event Manager.

How to Verify the Installation

To verify your CA Workload Automation DE Web Client installation, use the VERIFY Application packaged with the CA Workload Automation DE server.

To verify the installation, follow these steps:

1. Run the VERIFY Application (see page 39).
2. Display the VERIFY Application (see page 40).
3. Monitor the jobs as they run (see page 40).

Run the VERIFY Application

You can run the VERIFY Application to verify the installation.

To run the VERIFY Application

1. Launch CA Workload Automation DE Web Client (see page 37).
2. Log on to the server (see page 38).
3. Click the Event Manager tab on the Main Menu page.
4. Enter the following on the List of Events bar:
   - Prefix—CYBERMATION
   - Name—VERIFY

   Note: The fields are not case-sensitive.
5. Click Refresh.

   The CYBERMATION.EVENT is listed in the table.
6. Click View beside the CYBERMATION.VERIFY Event to select it.

   The View pop-up window appears.
7. Click Trigger on the Event Manager command bar.

   The Trigger pop-up window appears.
8. Leave the Schedule Criteria field blank and the other options unchanged.
9. Click OK to trigger the Event immediately.
10. Close the View pop-up window.

    The VERIFY Application is running.

Display the VERIFY Application

You can display the VERIFY Application to monitor the jobs as they run.

To display the VERIFY Application

1. Click Workload Director on the Event Manager page.

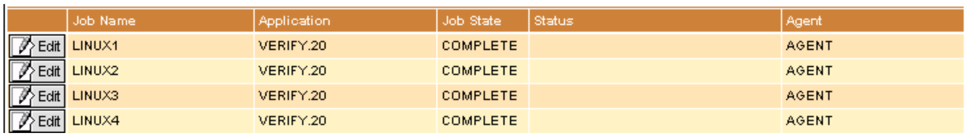
   The Workload Director page appears.

2. Enter **verify** in the Application field on the Filter bar.
3. Click Refresh.

   Workload Director displays the jobs associated with the VERIFY Application.

Monitoring the Jobs as They Run

On the Workload Director page, monitor the jobs associated with the VERIFY Application. Each job in the Application appears as a separate row in the display. The Job State column shows the state of each job.



	Job Name	Application	Job State	Status	Agent
Edit	LINUX1	VERIFY.20	COMPLETE		AGENT
Edit	LINUX2	VERIFY.20	COMPLETE		AGENT
Edit	LINUX3	VERIFY.20	COMPLETE		AGENT
Edit	LINUX4	VERIFY.20	COMPLETE		AGENT

As the jobs run, the states will change. Within a few minutes, you should see all four jobs in a COMPLETE state. This state indicates your setup is successful.

If you do not see the VERIFY Application, try the following:

- Check your Workload Director filter criteria.
- Retrigger the VERIFY Event.

Note: If a job within the VERIFY Application does not complete successfully, investigate the possible causes for the job state. For more information about job states, see the *CA WA Desktop Client Monitor Perspective Help*.

Register CA Workload Automation DE Web Client as a Windows Service

You can run CA Workload Automation DE Web Client as a background application by running it as a Windows service. In a production environment, you can configure the service to start automatically whenever the system starts. CA Workload Automation DE Web Client must be registered as a Windows service before it can be started as a service.

Note: If you installed CA Workload Automation DE Web Client on Windows using the manual installation, you cannot run CA Workload Automation DE Web Client as a Windows service.

To register CA Workload Automation DE Web Client as a Windows service

1. Open the Windows command prompt.
2. Change to the following directory:

   install_dir

   Specifies the directory where CA Workload Automation DE Web Client is installed.
3. Enter the following command:

   ```
   InstallService.bat install service-name
   ```

   service-name

   (Optional) Specifies the name of the service.

   Default: CAWADEWebClient

   CA Workload Automation DE Web Client is registered as a Windows service. The InstallService.bat script updates the JRE_HOME and JAVA_HOME variables and invokes the Tomcat service.

Stop the Web Client Server

To stop using CA Workload Automation DE Web Client, you issue a command to run a script that stops the server. The script sets the JRE_HOME variable and stops the Tomcat web server.

Note: If you installed CA Workload Automation DE Web Client on Windows using the manual installation, use the batch script that you created to stop the Web Client server. Alternatively, you can press Ctrl+c on the server console window to stop the server.

To stop the Web Client server

1. Change to the following directory at the command prompt:

   install_dir

   Specifies the directory where CA Workload Automation DE Web Client is installed.

2. Enter the following command:

   - On UNIX:

     ```
     StopWebClient.sh
     ```

   - On Windows:

     ```
     StopWebClient.bat
     ```

   The Web Client server stops.

Deregister CA Workload Automation DE Web Client as a Windows Service

When you deregister CA Workload Automation DE Web Client as a service, it is stopped and then removed.

To deregister CA Workload Automation DE Web Client as a Windows service

1. Open the Windows command prompt.
2. Change to the following directory:

   install_dir

   Specifies the directory where CA Workload Automation DE Web Client is installed.
3. Enter the following command:

   ```
   InstallService.bat remove service-name
   ```

   service-name

   (Optional) Specifies the name of the service.

   Default: CAWADEWebClient

   The Web Client service is removed.

Uninstall CA Workload Automation DE Web Client

You can uninstall CA Workload Automation DE Web Client if you no longer use it or want to install the new version.

To uninstall CA Workload Automation DE Web Client

1. Stop the Web Client server (see page 42).
2. (Windows only) Stop Apache if you installed Apache HTTP Server.
3. Remove CA Workload Automation DE Web Client:
   - On UNIX, delete the installation directory.
   - On Windows, select Start, Programs, CA, WADE Web Client 11.3, Uninstall WADE Web Client.
4. (Windows only) Restart the computer.

   CA Workload Automation DE Web Client is uninstalled.

Chapter 5: Troubleshooting CA Workload Automation DE Web Client

This section contains the following topics:

Increase the Server Response Time

By default, if a Web Client operation does not complete within 30 seconds, the Web Client server stops waiting for the server response and it displays a timeout error message. When the CA Workload Automation DE server completes the operation, it sends the response back to the Web Client server. However, the result of the operation might not be apparent to the user. The server response messages are recorded in the Web Client logs.

To avoid timeout error messages, you can increase the server response time when the communication between the CA Workload Automation DE server and the Web Client server is slow.

To increase the server response time

1. Stop the Web Client server (see page 42).
2. Use a text editor to open the following file:
   - On Windows:

     install_dir\apache-tomcat-6.0.35\webapps\WADEWeb\WEB-INF\web.xml
   - On UNIX:

     install_dir/apache-tomcat-6.0.35/webapps/WADEWeb/WEB-INF/web.xml

   install_dir

   Specifies the directory where CA Workload Automation DE Web Client is installed.
3. Locate the following lines:

```
<!--
<context-param>
  <param-name>ServerResponseTimeout</param-name>
  <param-value>30</param-value>
</context-param>
-->
```

4. Uncomment the lines by deleting the first line and the last line:

```
<context-param>
  <param-name>ServerResponseTimeout</param-name>
  <param-value>30</param-value>
</context-param>
```

   By default, the ServerResponseTimeout parameter is set to 30 seconds.
5. Update the ServerResponseTimeout parameter by changing the value in the param-value tag, for example:

```
<context-param>
  <param-name>ServerResponseTimeout</param-name>
  <param-value>60</param-value>
</context-param>
```

In this example, the ServerResponseTimeout parameter has been increased to 60 seconds.

6. Save the web.xml file.
7. Restart the Web Client server (see page 36).

   The server response time is increased.

SSLSessionCache Error on 64-bit Windows

Valid on 64-bit Windows

Symptom:

When I try to run Apache HTTP Server, the following error occurs:

```
Syntax error on line 62 of C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/conf/extra/httpd-ssl.conf:
SSLSessionCache: Invalid argument: size has to be >= 8192 bytes
```

Solution:

This problem occurs on a 64-bit version of Windows due to a known issue with Apache HTTP Server.

To correct this problem

1. Create a link or shortcut to the following folder:

   ```
   C:\Program Files (x86)\Apache Software Foundation\Apache2.2
   ```

   For example, create a link to this folder as c:\Apache2.2.

2. Change to the following directory:

   Apache_install_dir\conf\extra

   Apache_install_dir

   Specifies your Apache installation directory.

3. Open the httpd-ssl.conf file in a text editor.

4. Locate the following line:

   ```
   SSLSessionCache        "shmcb: C:/Program Files (x86)/Apache Software
   Foundation/Apache2.2/logs/ssl_scache(512000)"
   ```

5. Replace the Apache path in this line with the path of the link that you created in Step 1, for example:

   ```
   SSLSessionCache        "shmcb:c:/Apache2.2/logs/ssl_scache(512000)"
   ```

   In the preceding line, c:/Apache2.2 is a shortcut to the C:/Program Files (x86)/Apache Software Foundation/Apache2.2 directory.

6. Save the httpd-ssl.conf file.

sqljdbc_auth.dll File Already Loaded in Another Classloader Error on Microsoft SQL Server

Valid on Microsoft SQL Server with Windows authentication

Symptom:

When I try to run CA Workload Automation DE Web Client with another application on the same Tomcat web server, the following error occurs:

```
sqljdbc_auth.dll already loaded in another classloader
```

Solution:

This problem can occur when CA Workload Automation DE Web Client and the other application communicate with a Microsoft SQL Server database using Windows authentication.

To correct this problem

1. Locate the sqljdbc.jar file from the following folder:

   tomcat_install_dir\webapps\WADEWeb\WEB-INF\lib

   tomcat_install_dir

   Specifies your Tomcat installation directory.

2. Move the sqljdbc.jar file to the following folder:

   tomcat_install_dir\shared\lib

   Note: If the shared folder does not exist, create the shared folder and the lib subfolder.

3. Locate the sqljdbc_auth.dll file from the following folder:

   tomcat_install_dir\bin

4. Move the sqljdbc_auth.dll file to the following folder:

   tomcat_install_dir\shared\lib

5. Locate the StartWebClient.bat file from the following folder:

   install_dir

   Specifies the directory where CA Workload Automation DE Web Client is installed.

6. Add the following line at the top of the StartWebClient.bat file:

   set PATH=%PATH%;*tomcat_install_dir*\shared\lib

7. Replace the *tomcat_install_dir* variable with the path of your Tomcat installation directory.

8. Locate the catalina.properties file from the following folder:

   tomcat_install_dir\conf

9. Edit the shared.loader= line in the catalina.properties file as follows:

   ```
   shared.loader=${catalina.base}/shared/lib,${catalina.home}/shared/lib,${catal
   ina.base}/shared/lib/*.jar,${catalina.home}/shared/lib/*.jar
   ```

   Note: If the shared.loader line contains other entries, append these entries to the end of the other entries. Separate each entry with a comma.

10. Restart the Tomcat web server and run both web applications.

Index