Configuring a Local Linux Machine for Running with SSL

1st step: create a keystore file

2nd step: modify Tomcat's server.xml file

3rd step: use the correct URL to test SSL implementation

**Create Keystore File:**

The keystore file is a hidden file created in the user's root directory.

1: Press Ctrl + ALT + T to open the terminal and navigate to the binary folder:

cd /usr/bin

2: Enter the command and parameters:

keytool -genkey -alias tomcat -keyalg RSA

3: The password for the keystore is “changeit”.

4: After entering the required information, hit return to keep the same password.

The following figure shows the steps taken in the console to create a keystore file. Enter your own answers for the questions on name, organization, and location.

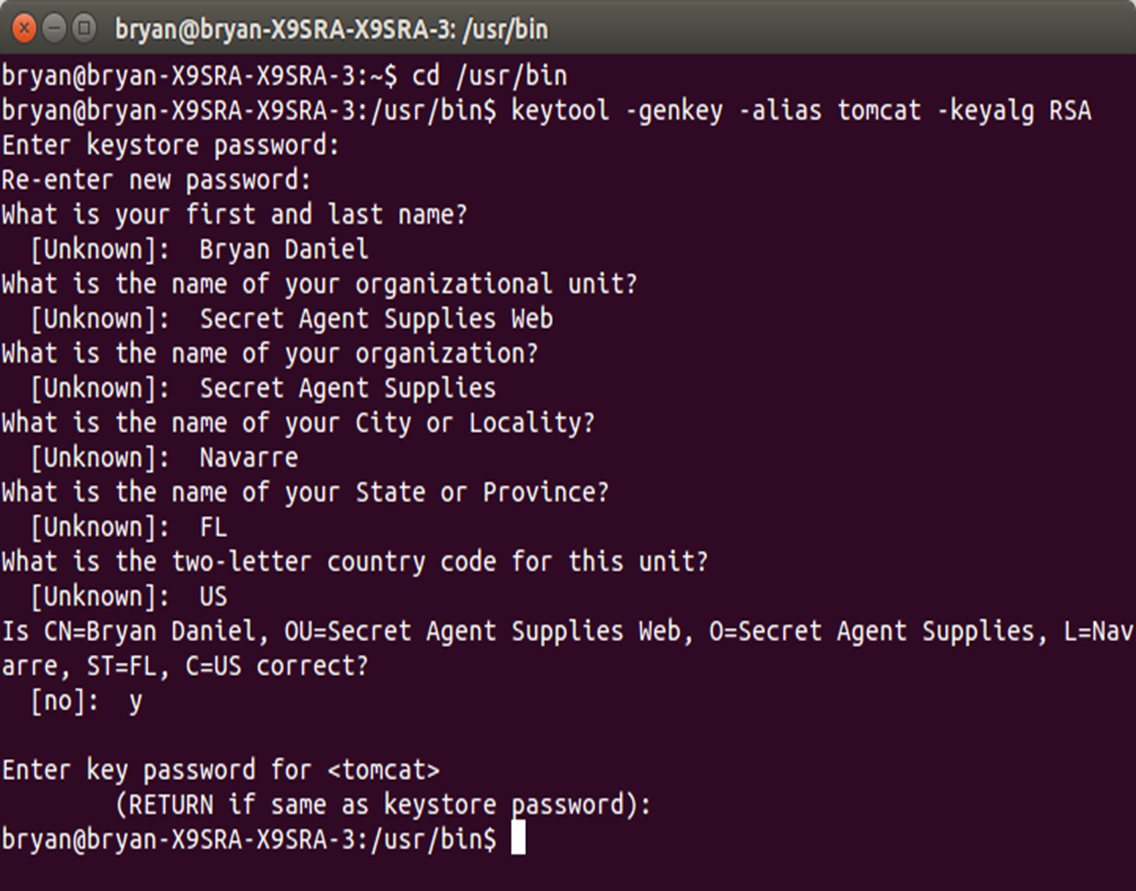


Figure 1 Keystore File Creation

**Modify server.xml File:**

1: Open the tomcat directory and find the server.xml file in the conf folder.

2: Open the server.xml file and find the configuration for port 8443.

3: Remove the comment tags around this block and add the highlighted line as shown in Figure 2.

4: Save and close the server.xml file.

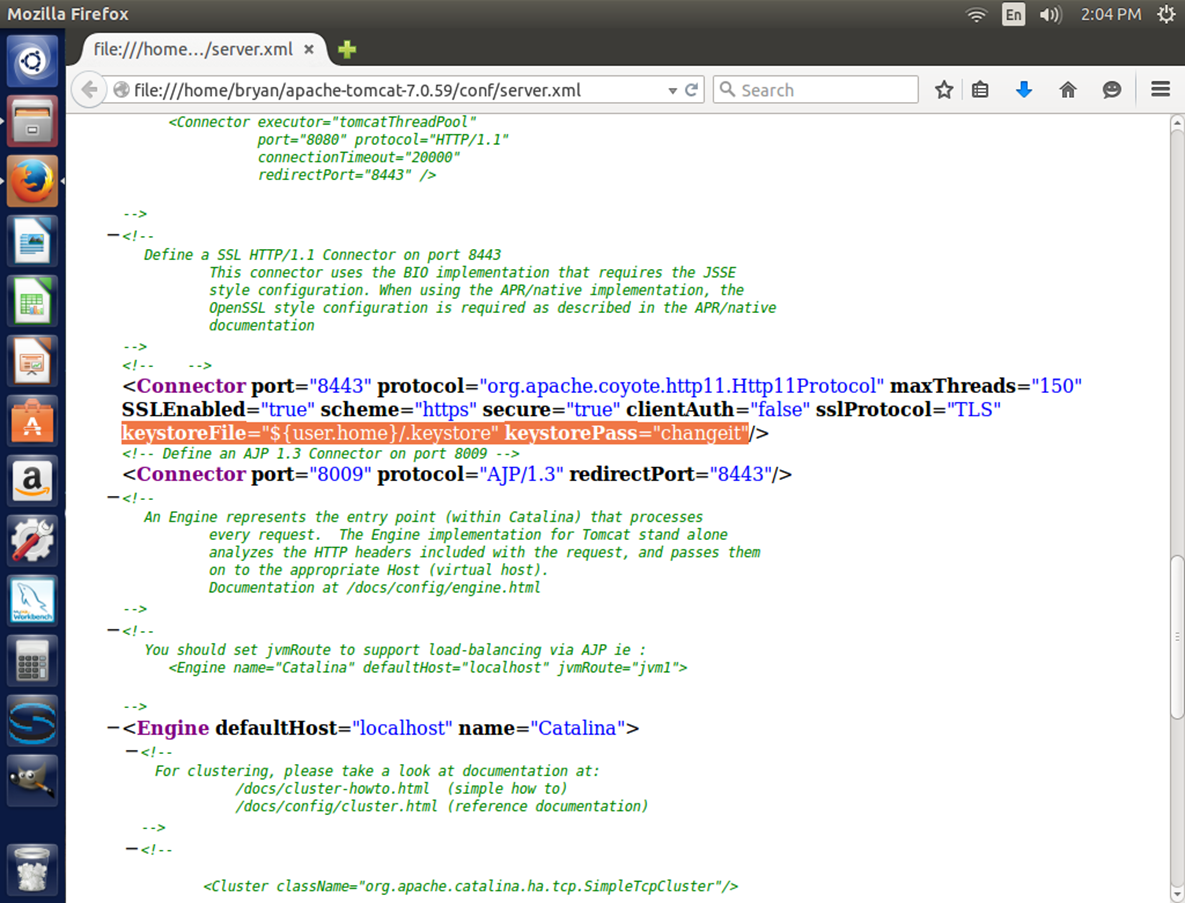


Figure 2 server.xml

**Test SSL:**

1: Make sure the WAR file is placed in Tomcat's webapps directory.

2: Start Tomcat.

3: Open a web browser and navigate to the application’s URL, changing “http” to https” and changing port 8080 to 8443.

4: Since the secure certificate is self-signed, the browser should give a warning as shown in the next figure. Accept the risk and proceed to the requested page.

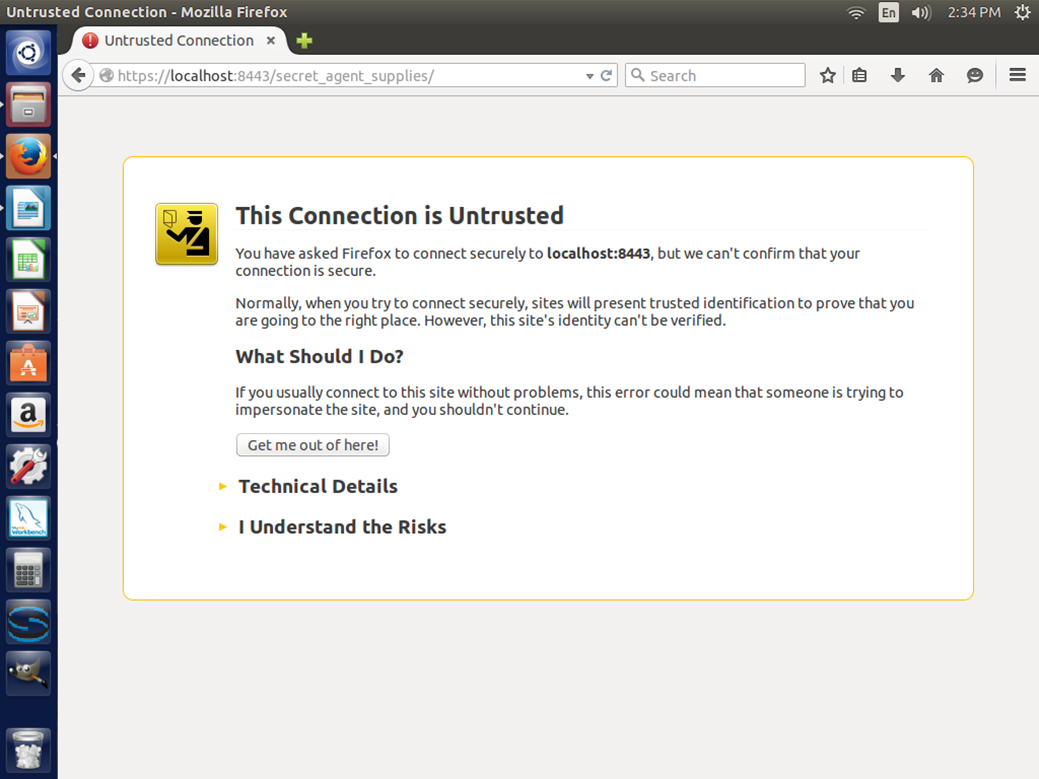


Figure 3 Browser Message