Apache 2.x (Open SSL)

1. Use the terminal client (ssh) to log in to your server.
2. Type the following command to generate the CSR file and a private key for decrypting SSL certificate:

   ```
   openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
   ```

   where "server" is the name of your server.

3. Save the private key file because it is necessary for installing SSL certificate.
4. Enter the fully qualified domain name when prompted for the Common Name. For a wildcard certificate, the common name must begin with asterisk (*). For example, *.yourcompany.com.
5. Type your organizational information when prompted. The CSR file is created.
6. Open the CSR file in a text editor and copy the text, including the "Begin" and "End" tags.
7. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
8. Paste the text from the CSR file into the field provided.

Apache cPanel

Note: This procedure is for cPanel 11. For the other cPanel versions, the process is similar but you may ask your web host for specific instructions.

1. Log in to your cPanel control panel.
2. Click **SSL/TLS Manager** and click **Generate, view, upload, or delete your private keys**.
3. Go to **Generate a New Key** and enter your domain under the Host section. Typically, it is the fully-qualified domain name where you will access the certificate. For example, www.domain.com or mail.domain.com.
4. Click **Generate** > **Return to SSL Manager** and select **Generate, view, or delete SSL certificate signing requests**.
5. Enter the following on the Generate a New Certificate Signing Request section:
   - **Host**: The domain that you selected when generating the private key.
   - **Country**: The two-letter ISO 3166 country code. For example, the code for Japan is "JP". For the other countries, refer to the ISO list of country codes.

- **State:** The state where your organization is located. Do not use an abbreviation.
- **City:** The city where your organization is located.
- **Company:** The legally registered name of your organization or company.
- **Email:** The email address where the CSR will be sent.
- **Pass Phrase:** The password to associate with the certificate. You will need to remember this password later.

6. Click **Generate** to show the CSR.
7. Copy the text of the CSR, including the "Begin" and "End" tags.
8. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
9. Paste the text from the CSR file into the field provided.

Apache Ensim Web Server

1. Log in to the Site Administrator and select the site you want to manage.
2. Click **Services** and then click the **Actions** icon.
3. On the Apache Web Server Manager screen, click **SSL Settings** and then click **Generate**.
4. Enter the required information about your business and server. The Common Name will be populated automatically.
5. Click **Save** to generate the CSR and RSA key.
6. Open the CSR file in a text editor and copy the text, including the "Begin" and "End" tags.
7. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
8. Paste the text from the CSR file into the field provided.

Apache Tomcat

1. Go to the directory where you plan to manage your keystore and certificates.
2. Enter the following command:

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -
keystore your_site_name.jks
```

Note: You may need to add "java /bin/ directory" to your path before the keytool command is recognized.

3. Specify a password for your keystore and your organization information.

   *Note: When asked for your first and last name, enter the fully qualified domain name of the site you are securing. For example, www.yourcompany.com. For a wildcard certificate, the FQDN must begin with an asterisk (*). For example, *.yourcompany.com.*

4. Verify if the information is correct and click **Yes**.
5. Confirm your password when prompted. Your keystore file, which is named your_site_name.jks, is now created in the current working directory.
6. Save the keystore file because it is necessary for certificate installation.
7. Enter the command below to generate the CSR from your keystore:

   ```
   keytool -certreq -alias server -file csr.txt -keystore
   your_site_name.jks
   ```

8. Type the keystore password that you specified in step 3 and press ENTER. The CSR file, csr.txt, is created in the current directory.
9. Copy the text of the CSR, including the "Begin" and "End" tags.
10. From the AffirmTrust console, select **Certificates** > **Certificates** > **Add**.
11. Paste the text from the CSR file into the field provided.