Apache 2.x (Open SSL)

1. Download the server certificate and CA certificate bundle from the Deep Security for Web Apps console. Your Apache server has a key file created when you generated the certificate request. Place the certificates in the directory where your key file is located.
2. Make the certificates readable by root only.
3. Locate the Apache config file. Typically, it is in /etc/httpd/httpd.conf.
4. Create a copy of the existing non-secure virtual host and secure it if your website is accessible via secure (https) and non-secure (http) connections.
5. Edit the "`<VirtualHost>`" block as shown below:

```
<VirtualHost 192.168.0.1:443
DocumentRoot /var/www/html2
ServerName www.yourdomain.com
SSLEngine on
SSLCertificateFile [path to your server certificate file]
SSLCertificateKeyFile [path to your private key]
SSLCertificateChainFile [path to CA certificate bundle]
</VirtualHost>
```

   where:

   "`SSLCertificateFile`" is your server certificate file. For example, your_domain_name.crt.

   "`SSLCertificateKeyFile`" is the key file created when you generated the CSR.

   "`SSLCertificateChainFile`" is the CA certificate bundle.

   Note: If the "`SSLCertificateChainFile`" directive does not work, use the "`SSLCACertificateFile`" directive instead.

6. Run the command "`apachectl configtest`" to check your Apache config file for syntax errors.

   Note: On some servers, the command is "`apache2ctl`".

7. If you are installing OV SSL certificate, proceed to the next step. If you are installing EV SSL certificate, get you site seal code. The Deep Security for Web Apps EV Site Seal enables all versions of Internet Explorer 7 to display a green URL bar. It should be displayed on a webpage that visitors view before they go to any of your secured pages.
   a) From the Deep Security for Web Apps console, go to **Protection** > **Certificates**.

b) Click the common name of the certificate to show the Details page.
c) Click the **Site Seal** button and copy the Site Seal HTML code.
d) Paste the code on the HTML of your website where you want the site seal to appear.

Note: Internet Explorer 7 also requires the phishing filter to be enabled for the address bar to turn green.

8. Restart the Apache with SSL support by running the commands below:

```
apachectl stop
apachectl start
```

Note: If Apache does not start with SSL support, use "`apachectl startsl`" instead. If SSL support loads with "`apachectl startssl`" only, configure the Apache startup to include SSL support in the regular command. Remove the `<IfDefine SSL>` and `</IfDefine>` tags that enclose your SSL configuration. Otherwise, you may need to manually restart Apache on every server reboot.

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. Download the server certificate and CA certificate bundle from Deep Security for Web Apps.
2. Open the WebHost Manager and click **Activate your SSL Certificate** on the SSL/TLS menu. A screen with three boxes appears.
3. Paste the content of your server certificate file on the first box. If the certificate file is on your server, click **Fetch** to copy the contents of the file.
4. On the second box, paste the private key created when you generated the CSR.
5. Paste the CA certificate bundle on the third box.
6. Click **Do it** at the top of the page.

Apache Ensim Web Server

Note: The procedure below is for installing certificate to a site managed by Ensim. To directly install the SSL certificate to Ensim, the host configuration is the same but the host configuration file for Ensim interface is /usr/lib/opcenter/fastcgi/httpd-templ.conf.

To install the server certificate:

1. Save the server certificate in the directory where you store SSL certificates and public and private key files. For example, /etc/ssl/crt/.
2. Make the directory readable by root only.
3. Log in to the administrator console and select the website you are securing.
4. Click **Services** and then click **Actions**.
5. On the Apache Web Server Manager screen, click **SSL Settings**. A self-signed certificate should already be saved.
6. Click **Import** and copy the certificate, including the "`Begin`" and "`End`" tags.
7. Paste it on the box under Save SSL Certificate.
8. Save the certificate and exit.

To install the CA certificate bundle:

The CA bundle containing the intermediate and root certificates must be installed on the server before the certificate will be trusted.

1. On your Ensim server, go to the /etc/httpd/conf/virtual directory. This directory contains a site file for each virtual site you are hosting.
2. Locate the virtual site file that you need to edit using an HTML or text editor to view their contents. Each file has the following details on the top:

```
<VirtualHost 000.00.00.000:80>
ServerName www.yourdomain.com
```

3. Note the virtual site number of the correct site file for future reference.
4. Open the site file in an editor and add the following:

```
SSLCACertificateFile
/home/virtual/site#/fst/etc/httpd/conf/ssl.crt/cabundle.crt
```

The result should be like this:

```
</Directory>
SetEnv SITE_ROOT /home/virtual/site#/fst
SetEnv SITE_HTMLROOT /home/virtual/site#/fst/var/www/html
Include /etc/httpd/conf/site#
SSLEngine on
SSLCertificateFile
/home/virtual/site#/fst/etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile
/home/virtual/site#/fst/etc/httpd/conf/ssl.key/server.key
SSLCACertificateFile
/home/virtual/site#/fst/etc/httpd/conf/ssl.crt/cabundle.crt
</VirtualHost>
< /IfDefine>
```

where "site#" is the virtual site number (for example, site1) and "server" is the name of your server certificate.

5. Copy the CA certificate bundle file to the directory where your sever certificate is saved:

   ```
   /home/virtual/site#/fst/etc/httpd/conf/ssl.crt/cabundle.crt
   ```

6. Back up your current site file.
7. Save the edited site file and restart Apache.

Apache Tomcat

1. Download the.p7b file to the directory where your keystore is located. The certificate must be installed on the same keystore used to generate your CSR. It will not work if you install it on a different keystore.
2. Enter the following command to install the certificate:

   ```
   keytool -import -trustcacerts -alias tomcat -file .p7b -keystore .jks
   ```

3. Select **Yes** when prompted to trust the certificate.

Your server certificate has been installed with all the root and intermediate CA certificates when the following message appears:

Certificate reply was installed in keystore.