



Installing your Certificate on Apache Mod_SSL / OpenSSL

Note: The ssl configuration file will always be referenced in the apache config file if the configuration is not included in it. Look for the lines starting 'include', which is the directive for including other files etc. For example, depending on the distribution, it might be called `ssl.conf`, `httpd-ssl.conf` etc

Step one: Copy your certificate to a file on your apache server

You will receive an email from Comodo with the certificate in the email. The certificate will be called '*yourDOMAINNAME.crt*' and will be within a *.zip file you have received as an email from us. When viewed in a text editor, your certificate will look something like this:

```
-----BEGIN CERTIFICATE-----
MIAGCSqGS1b3DQEHAqCAMIACAQExADALBggqhkiG9w0BBwGggDCCAmowggHXAhAF
Ubm77e50M63v1Z2A/5O5MA0GCSqGS1b3DQEOBAUAMF8xCzAJBgNVBAYTAIVTMSAw
(.....)
E+cFEpf0WForA+eRP6XraWw8rTN8102zGrcJgg4P6XVS4I39+I5aCEGGbauLP5W6
K99c42ku3QrlX2+KeDi+xBG2cEIsdSiXeQS/16S36ITclu4AADEAAAAAAAAA
-----END CERTIFICATE-----
```

Copy your Certificate into the same directory as your Private Key. In this example we will use '`/etc/ssl/crt/`'. The private key used in the example will be labeled '*private.key*' and the public key will be '*yourDOMAINNAME.crt*'.

Note: It is recommended that you make the directory that contains the private key file only readable by root.

Step two: Install the Intermediate Certificate

You will need to install the Intermediate CA certificates in order for browsers to trust your certificate. The Intermediate CA certificates are contained within the '*ca-bundle*' file that was attached to your email in the *.zip file we sent you (this should be named '*yourSERVERNAME.ca-bundle*'). In the relevant 'Virtual Host' section for your site, you will need to do the following to get this file correctly referenced:

a. First, copy the '*yourSERVERNAME.ca-bundle*' file to the same directory as the certificate and key files. As a reminder, in this example we called the directory '`/etc/ssl/crt/`'.

b. Next, add the following line to the SSL section of the '`httpd.conf`' file. Again we assume that '`/etc/ssl/crt/`' is the directory to where you have copied the intermediate CA file. If the line already exists amend it to read the following:

```
SSLCertificateChainFile /etc/ssl/crt/yourSERVERNAME.ca-bundle
```

c. If you are using a different location and different certificate file names, you will need to change the path and filename to reflect the path and filename that you are using. The SSL section of the updated config file should now read:

```
SSLCertificateFile /etc/ssl/crt/yourDOMAINNAME.crt
SSLCertificateKeyFile /etc/ssl/crt/private.key
SSLCertificateChainFile /etc/ssl/crt/yourSERVERNAME.ca-bundle
```

d. Save your '*config*' file and restart Apache.

Note: The ssl configuration file will always be referenced in the apache config file if the configuration is not included in it. Look for the lines starting 'include', which is the directive for including other files etc. For example, depending on the distribution, it might be called `ssl.conf`, `httpd-ssl.conf` etc