How to Install an SSL/TLS Certificate In Apache Open SSL

The following instructions will guide you through the SSL installation process on Apache OpenSSL. If you have more than one server or device, you will need to install the certificate on each server or device you need to secure. If you still have not generated your certificate and completed the validation process, reference our CSR Generation Instructions before following the steps below.

What You'll Need

1. Your server certificate

This is the certificate you received from the CA for your domain. You may have been sent this via email. If not, you can download it by visiting your Account Dashboard and clicking on your order.

2. Your intermediate certificates

These files allow the devices connecting to your server to identify the issuing CA. There may be more than one of these certificates. If you got your certificate in a ZIP folder, it should also contain the Intermediate certificate(s), which is sometimes referred to as a CA Bundle.

3. Your private key

This file should be on your server, or in your possession if you generated your CSR from a free generator tool. On certain platforms, such as Microsoft IIS, the private key is not immediately visible to you but the server is keeping track of it.

Note: The above files should be saved to the server directory where all certificate/key files are stored.

Installation Instructions

1. Locate the apache config file to edit

The main config file is typically called httpd.conf or apache2.conf and located via /etc/httpd or /etc/apache2/.

Note: The SSL config file can be in a <VirtualHost> block in another config file. You can always search for the SSL conf file on Linux distributions using this grep command: grep -i -r “SSLCertificateFile” /etc/httpd/

2. Configure the file and enter commands

Configure the httpd.conf file and enter the following commands on your VirtualHost to successfully enable SSL:

```
<VirtualHost 209.123.546.123:443>
 — other config details-
 SSLEngine  on
 SSLCertificateFile /etc/httpd/conf/ssl.crt/yourdomain.crt
 SSLCertificateKeyFile /etc/httpd/conf/ssl.key/yourdomain.key
 SSLCertificateIntermediateFile /etc.httpd/conf/intermediate.crt
 </VirtualHost>
```

Note: If you need the site to load via https and http, create another virtual host for http. You can simply copy the existing config file before making any during this step.

3. Run a command test

Test your new config file by running the following command:apachectl configtest

4. Restart Apache

If successfully tested, restart Apache by running the following commands:
apachectl stop
apachectl start

Note: You may be asked to enter the password you generated with your RSA key. If you do not want to be asked for a password, you will need to re-generate your RSA key file.

Congratulations! You’ve successfully installed your SSL certificate! To check your work, visit the website in your browser at https://yourdomain.tld and view the certificate/site information to see if HTTPS/SSL is working properly. Remember, you may need to restart your server for changes to take effect.