

- 0.
- 0.
- 0.

Manually install an SSL certificate on my Apache server (CentOS)

Article Number: 1389 | Rating: Unrated | Last Updated: Wed, Dec 2, 2020 at 9:34 PM

After your certificate request is approved, you can [download your certificate](#) from the SSL manager and install it on your Apache server. If your server is running Ubuntu instead of CentOS, please see [Manually install an SSL certificate on my Apache server \(Ubuntu\)](#). Find the directory on your server where certificate and key files are stored, then upload your intermediate certificate (gd_bundle.crt or similar) and primary certificate (.crt file with randomized name) into that folder. For security, you should make these files readable by root only. Find your Apache configuration file. On default configurations, you can find a file named httpd.conf in the /etc/httpd folder. If you have configured your server differently, you may be able to find the file with the following command:

```
grep -i -r "SSLCertificateFile" /etc/httpd/
```

/etc/httpd/ may be replaced with the base directory of your Apache installation. Open this file with your favorite text editor. Inside your httpd.conf file, find the <VirtualHost> block. To have your site available on both secure (https) and non-secure (http) connections, make a copy of this block and paste it directly below the existing <VirtualHost> block. You can now customize this copy of the <VirtualHost> block for secure connections. Here is an example configuration:

```
<VirtualHost xxx.xxx.x.x:443>
    DocumentRoot /var/www/coolexample
    ServerName coolexample.com www.coolexample.com
    SSLEngine on
    SSLCertificateFile /path/to/coolexample.crt
    SSLCertificateKeyFile /path/to/privatekey.key
    SSLCertificateChainFile /path/to/intermediate.crt
</VirtualHost>
```

Don't forget the added 443 port at the end of your server IP. **DocumentRoot** and **ServerName** should match your original <VirtualHost> block. The remaining /path/to/... file locations can be replaced with your custom directory and file names. First, run the following command to check your Apache configuration file for errors:

```
apachectl configtest
```

Confirm that the test returns a **Syntax OK** response. If it does not, review your configuration files.

Warning: The Apache service will not start again if your config files have syntax errors. After confirming a **Syntax OK** response, run the following command to restart Apache:

```
apachectl restart
```

Note: As a courtesy, we provide information about how to use certain third-party products, but we do not endorse or directly support third-party products and we are not responsible for the functions or reliability of such products. Third-party marks and logos are registered trademarks of their respective owners. All rights reserved.

Posted - Wed, Dec 2, 2020 at 6:10 PM.

Online URL:

<https://www.heartinternet.uk/support/article/manually-install-an-ssl-certificate-on-my-apache-server-centos.html>