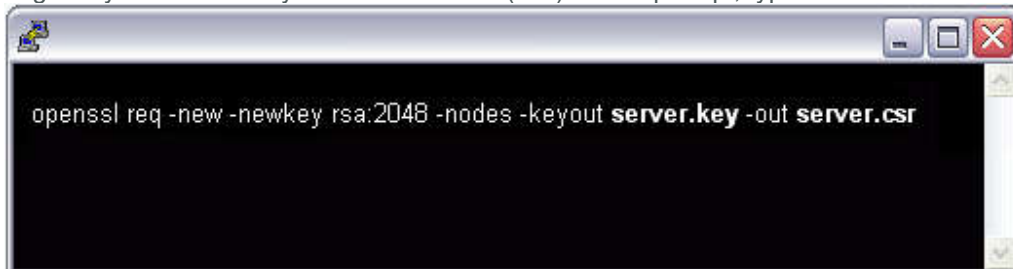


Apache CSR Creation and Installation using OpenSSL

How to generate a CSR for Apache using OpenSSL

1. Login to your server via your terminal client (ssh). At the prompt, type:

A screenshot of a terminal window with a black background and white text. The text shows the command: `openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr`. The window has standard OS window controls (minimize, maximize, close) in the top right corner.

- 2.
3. **openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr**
4. where server is the name of your server.
5. This begins the process of generating two files: the Private-Key file for the decryption of your SSL Certificate, and a certificate signing request (CSR) file (used to apply for your SSL Certificate) with apache openssl.
6. When you are prompted for the Common Name (domain name), enter the fully qualified domain name for the site you are securing. If you are generating an Apache CSR for a Wildcard SSL Certificate your common name should start with an asterisk (such as *.example.com).
7. You will then be prompted for your organizational information, beginning with geographic information. There may be default information set already.
8. This will then create your openssl .csr file.
9. Open the CSR file with a text editor and save it (including the BEGIN and END tags) into text file and [submit to us](#).
10. Save (backup) the generated .key file as it will be required later for Certificate installation.

Apache Server SSL Certificate Installation

Installing your Certificate on Apache with mod_ssl

1. Extract all of the contents of the ZIP file that was sent to you and copy/move them to your server. The extracted contents will typically be named: **yourDomainName.crt** and **yourDomainName.ca-bundle**

Note: If you received several .crt files in your ZIP file please use this article to make yourDomainName.ca-bundle

2. Move all of the certificate related files to their appropriate directories.

A typical setup:

- Move the Private Key that was generated earlier to the **ssl.key** directory, which is typically found in **/etc/ssl/**. This must be a directory which only Apache can access.

- Move the **yourDomainName.crt** and **yourDomainName.ca-bundle** to the **ssl.crt** directory, which is typically found in the **/etc/ssl/** directory.

3. Edit the file that contains the SSL configuration with your favorite text editor.

Examples: nano, vi, pico, emacs, mousepad, notepad, notepad++, etc.

Note: The location of this file may vary from each distribution. It will be referenced in the Apache global configuration file. Look for the lines starting with include.

Apache Configuration File:

- **Fedora/CentOS/RHEL:** /etc/httpd/conf/httpd.conf
- **Debian and Debian based:** /etc/apache2/apache2.conf

SSL Configuration File:

Some possible names:

- httpd-ssl.conf
- ssl.conf
- In the **/etc/apache2/sites-enabled/** directory.

Note: If need be please consult your distribution's documentation on Apache and SSL or navigate to the Apache Foundation's Apache2 Documentation.

4. In the **VirtualHost** section of the file please add these directives if they do not exist. It is best to comment out what is already there and add the below entries.

- **SSLEngine** on
- **SSLCertificateKeyFile** /etc/ssl/ssl.key/server.key
- **SSLCertificateFile** /etc/ssl/ssl.crt/yourDomainName.crt
- **SSLCertificateChainFile** /etc/ssl/ssl.crt/yourDomainName.ca-bundle ***

***** Apache 1.x:**

Please use **SSLCACertificateFile** instead of **SSLCertificateChainFile**.

Note: The above paths in the directives are only used as examples. Your server may have a different path and may need to be modified to suit your needs.

5. Save your config file and restart the Apache service.