How to Generate a CSR for Apache Web Server Using OpenSSL

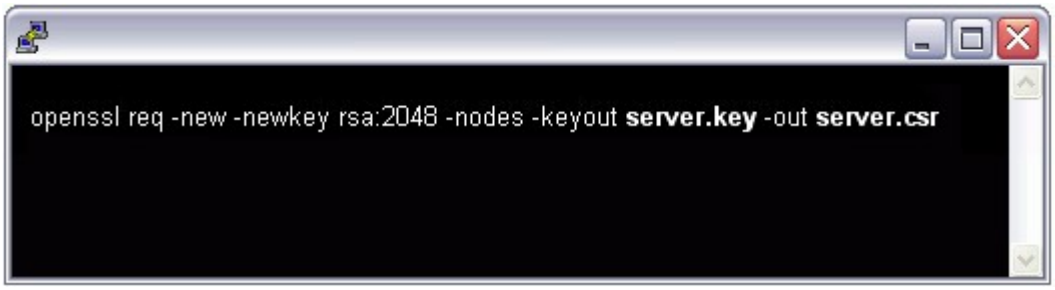
The following instructions will guide you through the CSR generation process on Apache OpenSSL.

1. Log In

Log in to your server's terminal via Secure Shell (SSH).

2. Run CSR Generation Command

Generate a private key and CSR by running the following command:



Here is the plain text version to copy and paste into your terminal:

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

Note: Replace "server" with the domain name you intend to secure.

3. Enter Your Information

Enter the following CSR details when prompted:

a) **Common Name:** The FQDN (fully-qualified domain name) you want to secure with the certificate such as www.google.com, secure.website.org, *.domain.net, etc.

b**) Organization:** The full legal name of your organization including the corporate identifier.

c) **Organization Unit (OU):** Your department such as 'Information Technology' or 'Website Security.'

d) **City or Locality:** The locality or city where your organization is legally incorporated. Do not abbreviate.

e) **State or Province:** The state or province where your organization is legally incorporated. Do not abbreviate.

f) **Country:** The official two-letter country code (i.e. US, CH) where your organization is legally incorporated.

Note: You are not required to enter a password or passphrase. This optional field is for applying additional security to your key pair.

4. Copy the CSR text from the file

Locate and open the newly created CSR in a text editor such as Notepad and copy all the text including:

> -----BEGIN CERTIFICATE REQUEST-----
> And
> -----END CERTIFICATE REQUEST-----

Note 1: Your CSR should be saved in the same user directory that you SSH into unless otherwise specified by you.

Note 2: We recommend saving or backing up your newly generate “.key” file as this will be required later during the installation process.

5. Generate the order

Return to the Generation Form on our website and paste the entire CSR into the blank text box and continue with completing the generation process.

Upon generating your CSR, your order will enter the validation process with the issuing Certificate Authority (CA) and require the certificate requester to complete some form of validation depending on the certificate purchased. For information regarding the different levels of the validation process and how to satisfy the industry requirements, reference our validation articles.

After you complete the validation process and receive the trusted SSL Certificate from the issuing Certificate Authority (CA), proceed with the next step using our SSL Installation Instructions for Apache OpenSSL.