



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:



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

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-----
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIEhHCCA2CAQAwYsxC2A1BgnVBAYTA1VTMRawDgyDVQqIDAdcbG9yawRhmQ4w  
DAYDVQQHDAVUyY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx1PYtnJ  
K23cqrGzJ5our6god3ytc1GAdctIH8Kn/MBBnx6kwQZj5uagISb+2JGng5/e6xm  
xnnjQZsokodk11iI2nLrxF0wtj4z1jQ+7jmeIK99eIEqY5vq61+hattGyk6IbHqH  
Q0NTEYvg630CXnabAFtnxy5X5/nn6AFurxuAgtrFXz1c15Ggxe59X3h9psvnbk bH/  
XgpyvVd9p9ATA010hncuzsnaJc006LwGK2xb0h3paRfC9zh09bwgFJcQ60fC4tLt  
mmeJ+Ug3ikvdeqwi1x169ZRG02TR5csp8dg8EaIX2hnaBc0S4pKI5LABM3kvfg1+  
awrNahSCU4VyRQIDAQABOIBSZAABgqrBgEEAYI3DQIDMqWwCjYUM543njAXLjIw  
TWYJkwyBBAGCNXUUMUIwQAIbBQwPv010LVEZMjQ3Uk9IVkNwDB1XSU4tUTMyNdDs  
T0HwQ1ZcQWRtaW5pc3RyYXRvcgWLSw51dE1nc151eGUwcgYKKwyBBAGCNw0CAjFk  
MGICAQEWBnAGkAYwByAGBACwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBUAG4A  
ZQBSACAAQwByAHkACAB0AG8AZwByAGEACAB0AGkAYwAgAFACgBvAHYAaQbkAGUA  
CgMBADCBZwYJK0ZihvcNAQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DATBgNVHSUE  
DDAKBggrBgEFBQCDATB4BgkqhkiG9w0BQC8EazBPM4GCCGSIb3DQMCAGIAgDA0  
BggrBgk1G9w0BAICAIAwCwYjYIZIAwUDBAEQAASGCWCSSAFIAwQBLTALBg1gkqgB  
ZQMEAIwCwYjYIZIAwUDBAEFMACGBSsoAwIHMAOGCCGSIb3DQMHB0GALUdDgQw  
BBTbhtbvdwt3Pc+K9bywsvK4d3WGFjANBgkqhkiG9w0BAQUFAAOCAQEARkMimjfo  
S4jwctAnBLrF6GF+ZAX71Zew0Z20Fbu93NpsMgmAuiftYr1t4J7I3k+N4zmFv4de  
CLwydpOHEkVOZ2BqRgcJIQ9I56gzB3R2fIbe1wdwFbvFjw3VU4cXGSTTDxHUP3/  
LCCbvtFec0Hsv969xp8dtwvTbwnPct5Cj6jfjvy1fomnhXfRgwP8FM6wBTy0w/2hr  
UewiP72YtLVaa09YP27UuFtohpJ2zmV0kd7qTVQ6vsuv4umkubool7FETK06Aup  
EXaaofcjF4LJhd5wSYNbdruStU1N1gxbdMzLHrw0J0gnuGeqxPohvPSMyAehJm8Q  
01erF3mqQuBUA=  
-----END NEW 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.