

Generating a Certificate Signing Request

Here is the steps or how-to to create a Certificate Signing Request (CSR). Example is given specifically for Centos based systems.

1. Log onto your server console using SSH.
 1. Enter the following command at the prompt.

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

Note: Replace "mydomain" with your actual domain name. Please enter only full name, for example [google.com](https://www.google.com) and not [google.com/maps](https://www.google.com/maps)

You will be prompted to answer a series of questions, explained below.

- **Country Name** – This is the two-letter abbreviation for your country. For example, United States would be US and Great Britain would be GB.
- **State or Province Name** – This is the full name of the state your organization operates from. For example, this might be "Ottava" or "California".
- **Locality Name** – Name of the city your organization operates from. Examples might include "London" or "Hamburg". Don't use abbreviations in this field. For example, "St. Petersburg" should be "Saint Petersburg".
- **Organization Name** – The name of your organization. If you are a business, use must use your legal name. If you are applying as an individual, you use your full name instead.
- **Organizational Unit Name** – If applying as a business, you can enter your "Doing Business As" (DBA) name here. Alternately, you can use a department name here. For example, "IT Department" or "Web Administration".
- **Common Name** – The domain name that you are purchasing a SSL certificate for. This must be a fully qualified domain name (FQDN). An example might be [mydomain.com](https://www.mydomain.com).

Note: If you are applying for a special wildcard SSL certificate, you will need to enter an asterisk for the subdomain. An example in that case might be *.mydomain.com. Never include the "http://", "https://", or any other special characters in this field. Never include text after the top level domain at the end. For example, your common name should end in .com, .net, (or whatever other extension you are applying for.)

- Email Address – An email address that can be used as a point of contact for your domain. Be sure the address is valid!
 - A challenge password – An optional password to further secure your certificate. Be sure to remember this password if you choose to use it. It must be at least 4 characters long. You can skip this step if you like.
 - An optional company name – Another optional step. Fill in your company name if you wish. This is not required for web SSL certificates.
1. Your CSR file generating completed! Check please contents of your current working directory with the "ls" command. You should notice two new files ending with ".key" and ".csr" respectively.

```
ls -l  
  
-rw-r--r--. 1 root root 1082 Jan 31 12:10 mydomain.csr  
-rw-----. 1 root root 1704 Jan 31 12:10 mydomain.key
```

The .key file should be kept private on your server. The .csr file is your certificate signing request, and can be sent to a Certificate Authority. You can inspect the contents of the CSR by using the "cat" command. Here is an example of the CSR generated in this walk through:

```
cat mydomain.csr
```

Output looks like

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQAwgaAxCzAJBgNVBAYTA1VTMRAwDgYDVQQIDAdBcm16b25hMRAw
DgYDVQQHDAQaG91bm14MRswGQYDVQQKDBJNeSBBD2Vzb211IENvbXBuYXkxZjAUAU
BgNVBAsMDU1UIERlcGFydG11bnQxFTATBgNVBAMMDG15ZG9tYWluLmNvbTEhMB8G
CSqGSIB3DQEJARYSYWRtaW5AbX1kb21haW4uY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAsN1jF8u2vvTGiSyStD/+4eInQnWlB30o38hWnF+bi6ZS
MmraeigL/HrSoKfUtj/z96PVeK9CFo0AZ12Tq91BzXtqxSjboIcvr91ZvrycrEYR
qsepF8M18Y0jyBfDzXIY13o5Sjnd4e0H7gZCldxy930LjJ1JQC0o4XAbxHd8k7A3
976uh2r6MPdnnQ65UG2vKnMa1MGfT9XTD6dQjj3ZpTqbdG4TnOPf1G4TNXu2zSY1
CX7XHjBkBgX5r/ohQBcqAYFpAMs/7E+gSbkK4jv9Mr8W1gC0CHSJkpT0tqcn+8Lj
1vMi3ysDed6b0bc/OMBXAZY2lpALbHvnzy2NJPRPjwIDAQABoAAwDQYJKoZIhvcN
AQELBQADggEBABuUSRgBnv4R1k4UHGngmvQ63jjaZh06URhQbFzb1e+XHeqou1F8
YSP17A8w23hLFXxs/NCOhQzAn9cFbBGy6dajqMjsCF3timGXHitsmUyswpG3k+dI
bWIsRaJPMS00z9HcI7ztvN1zs6iiMCZkpI4G+9J5wBqddgXSH+/w5bCViqj08550
APFUYUEFSB5jS5/e132F5zhcZV5vQ2bato8Zy58gzz5t+q5rn6uuzqc05kmBtDG8
B12R1Ut21Bb16sxQDKQbsM6snwn50H3Xszgn8kyR1VuX0qaKf1X1cCKRTSzYztUp
FeKV0mMwoC9XxX6YCz8eQy66RMVSm3hGI2Y=
-----END CERTIFICATE REQUEST-----
```

You will need to copy and paste the entire contents of the CSR file to your Certificate Authority when ordering a SSL certificate. Be sure that you include the lines that read “BEGIN CERTIFICATE REQUEST” and “END CERTIFICATE REQUEST”.