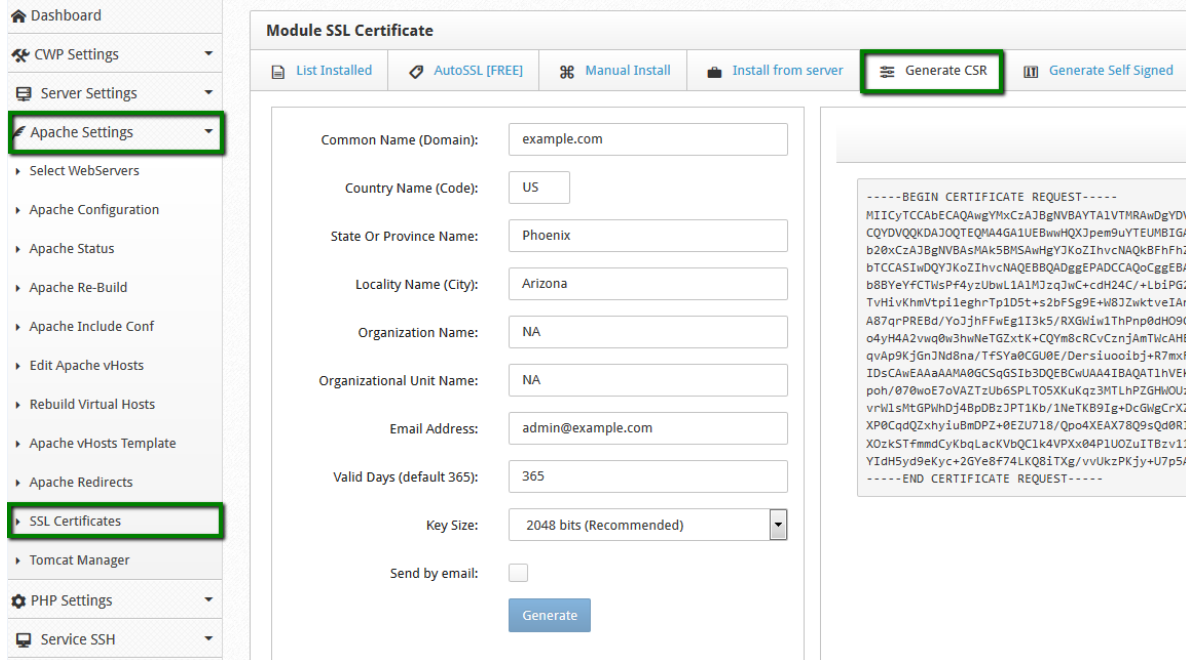


Generating CSR in CWP 7

Certificate Signing Request (CSR) is a block of code containing encrypted information about your company and its respective domain name. This code is required for activation of an SSL certificate.

In order to generate a CSR code in your CentOS Web Panel (CWP), please follow the steps listed below:

1. Log into your CWP admin area here: http://server_IP:2030/
2. Locate 'Apache Settings' from the left-hand navigation menu.
3. Select 'SSL Certificates' from 'Apache Settings' and switch to the 'Generate CSR' tab.
4. Fill in the blank fields with the requested information using only alphanumeric characters:
 - **Common Name** (Domain) - a fully qualified domain name (FQDN) you would like to secure. If you are activating a wildcard certificate, the domain name should start with an asterisk (e.g. *.example.com).
 - **Country Name** (Code) - a two-letter country code that is compliant with ISO 3166-2.
 - **State or Province Name** - the complete name of your state or region.
 - **City Name** - the full name of your city or local area. Please avoid using abbreviations.
 - **Organization Name** - the legally-registered company name. For OV and EV SSL certificates, Comodo (now Sectigo) Certificate Authority will need to verify the organization name you submit. For DV SSLs, this field will not be listed in the certificate details. If you do not have an organization, you can enter 'NA'.
 - **Organization Unit Name** - the name of the department within your organization. If not applicable, you can enter 'NA' here as well.
 - **Email Address** - provide the email address the certificate files will be sent to. You will also be able to change this email address during the activation process. This email address will not be used for Domain Control Validation (DCV).
 - **Valid Days (default 365)** - you can enter the default value 365. This value will not affect the validity period of your SSL certificate.
 - **Key Size** - select the key size from the drop-down list. We recommend 2048 bits.



- Make sure that every field is filled out. Once you have done that, click the 'Generate' button. As a result, you will receive two codes: 1) **CSR code** and 2) **Private Key code**. Your CSR code will be saved in the `/etc/pki/tls/certs/` folder in a file with the '.csr' extension.

The CSR code should be copied including the tags `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----` to begin activation.

Your **Private Key code** can be found in the 'Private Key' tab. Please make sure to back this code up, since it is not possible to install the certificate without it.

server **Generate CSR** **Generate Self Signed** **Configure**

Certificate **Private key**

```

-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDvD4cR74FBGLQ
jUNoA2/AwHmHwk1rD3+Ms1G8C9QJTCc6iAvnHR9uAv/i24jxtq3cDk/AeMeMUI
NGiHME7x4ryoZ1baYtXoIa06dQ+bfrNmxUoPRP1vCwcJLb3iAJ2bWwFQYNLjvJc
se+3XwP06qz0RAXF2KCY4RRcBINSN50F0Vx1osNU4T56dHRzVQi5tBI8CTVwggUJ
EKDLG60Mh+ANr8KtMN4cDXkxmcBsvGkGJvHEQrws54wJk1nABxGMidhAje/mrxNs
Pi+DVKrWKFSoxpyTXfJ2v030mGtAh1NBPw3q7IrqKIm4/ke5sRajLfgxemfnjHhF
6KOPMiA7AgMBAAECggEAb2ba/q6pgPhPsmDh5KsMLIoOOCFni1hyi9KUaBjq+1ou
fazrjkROVLeLF84tySZE6hS12JK8j71MmmZvEXaxAVw/NiT6LjeDYqD+xxJ7CAi
4eVWgB9+rSuohDJ4pfS7FUVNSMe6s18tudyBZOY2FBpv9nQseJ+uVw+sOSUxPQIa
dMLcW1HamK6t0upL64R++22uZsSgNs7I3j4jbnQcOYDobQ1nk9Krg4HY0nVYbJtI
d842FtNpNdHadKaD5wo1K1OV07CdOSw1eipSGbi8Lux0SQq6p+T4Um5Bmbj4gy
dyFR/NdhITjymZDwA7CaXziqnAdm65EAqLXdommN4QKBgQD+fNMmhwINw/JaXf/+
4pOIhdAnHKXoZ/qB+Z4PMFFhnUIu+gJBqfx12U/5cDcwRSpy+isuYDS2nOwcDfw
eq7dG/U+XW3Hg8VasfZ1T6qr5NsD7PaOuBK7fucfaqlW+T16eSbJ1X+nvz2Na79ou
fDFB55meCk+PDpGPr9d9MmplwKBgQDwezt+wwCdeXezS5Ayuhk31ynby8FXiNB4
tjNMS6LtasmhHnbYnyxJYKJ8ygk3+RYzYNBGRSE4I/AELsH5ZwD2oh8nmVFAIN3N
1GMSWbWJX++6ZVKeYVM1FU3AW91EXIUA6ukHNO1/xdJ1HC7Ag9kKk2ibbT31jud
iy4uXVtq/QKBgQCY9LF8b6LVYLQzeFgK/GesFzpOajm9xVj2MrV1Ay8u+HeTPk1i
T2vVmycx1oeqpyoiO/qnBf/Vu5LZMzmMA1DjeJBYYZM/3YVa06fCkLWGB1FT9LLk
aOJpawbDLThdQBSgjC8EuRdEgaQf3hwG5wYkNFZmPk6bp1tnKQOgFya2FQKBGCSj
0wb0f16461KE1oTNm4/L2Tj2CV8yJCVGbn3cF4eoeFfc70Yt7o4fV1VBD0cSpi+B
xySu/X//pogJGjwZfCmnsC21Gb6BY1DgDvYHV9Uxrr0TLt3KS9oJMksK3bi065a7Z
W+UnSs4QSGsCXmtD7YcgBJu0ff9DTEvNI+1s609AoGABmCOKsjwBG6R11FX/NfV
vcT1hgPtgrJorXW0QRD61SwgcBLtL9gIT02108FPyXQNTj31KfDqh1K1U0x7ZPqQ
ULDyrPVaeNbnSuhsQQjR15UyVkyVFX/Cj+V1Pz9QazPYdqxcSuC1mwWm9rVC7Nnd
P+wjqnLOJbF/kbYtr0NQVO4=
-----END PRIVATE KEY-----

```

Don't forget to save your Generated Key File on your local computer if you are planing to buy a signed certificate!

Please note this **Private Key code** will automatically save in the **/etc/pki/tls/private/** directory.

Refresh

Config Server Info Create Directory Create File Upload Shell Portscan

<< /etc/pki/tls/private/

All Inverse Delete Copy Move Compress Resolve IDs Permissions

Name	Perm	Owner
bak	755	0
hostname.key	644	0
centos-s-1vcpu-1gb-lon1-01.key	644	0
server-cwp.key	644	0
server-dovecot.key	644	0
server-http.key	644	0
server-postfix.key	644	0
example.com.key	644	0

All Inverse Delete Copy Move Compress Resolve IDs Permissions