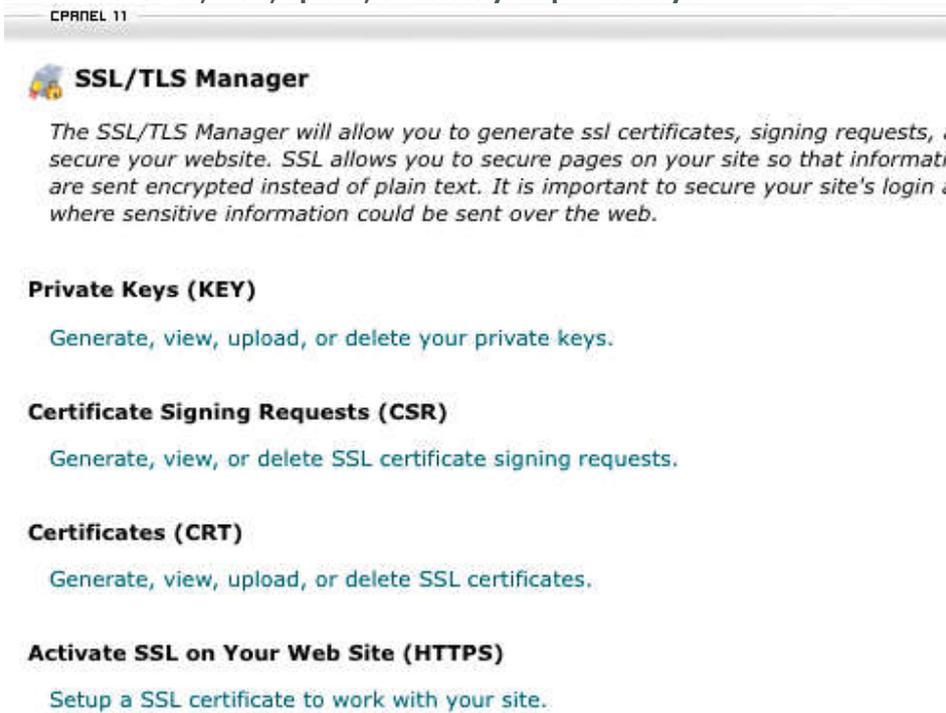


CSR Creation and Installation for cPanel

How to generate a CSR in cPanel

The following instructions are for cPanel 11. If you have a different version of cPanel, you will go through a similar process but you may need to ask your web host for specific instructions.

1. Login to your cPanel control panel.
2. Find and click on SSL/TLS Manager.
3. Click on **Generate, view, upload, or delete your private keys.**



The screenshot shows the cPanel 11 SSL/TLS Manager interface. At the top, it says "CPANEL 11". Below that is the "SSL/TLS Manager" heading with a lock icon. A paragraph explains that the manager allows generating SSL certificates, signing requests, and securing websites. Below this are four sections, each with a heading and a link:

- Private Keys (KEY)**
[Generate, view, upload, or delete your private keys.](#)
- Certificate Signing Requests (CSR)**
[Generate, view, or delete SSL certificate signing requests.](#)
- Certificates (CRT)**
[Generate, view, upload, or delete SSL certificates.](#)
- Activate SSL on Your Web Site (HTTPS)**
[Setup a SSL certificate to work with your site.](#)

4. Scroll to the bottom of the page to the **Generate a New Key**. Enter the domain you want to create an SSL Certificate for in the **Host** text box or select the domain from the drop down menu. This should be the name through which the certificate will be accessed (usually the fully-qualified domain name, e.g., www.domain.com or mail.domain.com)

Generate a New Key

Host or

5. Click the **Generate** button.
6. The private key will be saved in cPanel so there is no need to copy it. Click **Return to SSL Manager**.
7. Click on **Generate, view, or delete SSL certificate signing requests**.
8. In the **Generate a New Certificate Signing Request** section, enter the following information:
 - Host** - The domain that you entered or selected when generating the private key.
 - Country** - If needed, you can find the country code [here](#).
 - State** - The state in which your organization is located. Do not use an abbreviation.
 - City** - The city in which your organization is located.

Company - The legally registered name of your organization/company.

Company Division - The name of your department within the organization (frequently this entry will be listed as "IT," "Web Security," or is simply left blank).

Email - Your email address where the CSR will be sent.

Pass Phrase - Make up a password to be associated with the certificate. You will need to remember this password later.

Generate a New Certificate Signing Request

Host	x3demob.cpx3demo.com
Country	US 
State	Utah 
City	Lindon 
Company	Company Name, Inc. 
Company Division	IT 
Email	your.email@domain.com 
Pass Phrase	YourP@ssword 
<input type="button" value="Generate"/>	

* You must generate or upload a key before you can generate any certificate

9. Click the **Generate** button. The CSR will display in the window.
10. Copy and paste into a text file and [submit to us](#) for our process.

Installing your cPanel SSL Certificate

The following instructions are for cPanel 11. If you have a different version of cPanel, you will go through a similar process but you may need to ask your web host for specific instructions.

1. Login to your cPanel control panel.
2. Find and click on **SSL/TLS Manager**.
3. Click on **Generate, view, upload, or delete SSL certificates**.
4. Under the **Upload a New Certificate section**, click on the **Browse** button and find your Primary Certificate (yourdomain.crt) that you downloaded in the first step. Or if you have copied the contents of your primary certificate from the email, paste it in the box labeled: "Paste the crt below". To access the text version of your certificate, open it with a text editor. When copying and pasting your certificate, include the BEGIN and END tags.

Upload a New Certificate

Paste the crt below:

or Choose a .crt file:

Browse...

Upload

5. Click the **Upload** button.
6. Click **Go Back** and click **Return to SSL Manager** at the bottom of the page.
7. Click on **Setup a SSL certificate to work with your site**. If this option is not available, your web host may have disabled it. You will need to contact them about how to install the Intermediate certificate.
8. Select the domain you are using from the **Domain** drop down menu. The system will attempt to "Fetch" the SSL Certificate and private key for you. If this doesn't work, you may need to contact your web host.
9. In the box labeled **Ca Bundle** paste the contents of the Intermediate certificate.

Install/Update A SSL Host

Domain	x3demob.cpx3demo.com
Ip Address	198.66.92.13

Certificate (CRT)

The crt may already be on the server.

You can try to [Fetch](#) it or paste the entire .crt file here:

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAu+gAwIBAgIBADANBgkqhkiG9w0BAQFADCBjzELMAkGA1UEBhMCdXMx
EDA0BgNVBAgTB2Zsb3JpZGExEDA0BgNVBAcTB2JyYW5kb24xDDAKBgNVBAoTA2Fz
ZDEPMA0GA1UECXMGYXNkYXNkMR0wGwYDVQQDEXR4M2RlbW9iLmNweDNkZW1vLmNv
bTEeMBwGC5qS5Ib3DQEJARYPYXNkYXNkQhdld3UuY29tMB4XDTA4MDcyMTA5MDU1
NFoXDTA5MDcyMTA5MDU1NFowY8xCzAJBgNVBAYTAnVzMRAdGgYDVQQIEwdmbG9y
aWRhMRAdGgYDVQQHEwdicmFuZG9uMQwwCgYDVQQKEwNhc2QxZDZANBgNVBAsTBmFz
ZGFzZDEdMBsGA1UEAxMUeDNkZW1vYi5jcHgzZGVtby5jb20xHjAcBgkqhkiG9w0B
CQEWD2FzZGFzZEB3ZXdlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA
617/z0At011XxWfm4VYu3Peb5cbB7UEf6FFA/U24DXuza0HLIsnt1u4/Yqsy5GFb
Dgu4R/ZYN+czt8IMWg0/Kqe3ARDcU+/9011t+EwtcNIyqz0QJ6qsxp/xG0XuAd85
```

Key (KEY)

The key may already be on the server.

You can try to [Fetch](#) it or paste the entire .key file here:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQC135W0CON0gNvHxdwi3AoMVWaVA2bt1tCk5hQUPWwNv8NMoZRs
RhbFrRT5Y2PCqkY6AlrkX1FKWcfCzteEfKksbQakKvvYfoF2WLxs1Lfevmath7Jj
kJsEHjEHnCV9Qu7bS3ioG+sHMDH1uCCzkvmsiSSzUHqxfEzMbYzRrSzkQIDAQAB
AoGABVm690PuI1ntvPny6eTzJgazMmdTsKJGxKrvRt/cVm0zHYuwv/Va0rGMlabR
FvxrG3/r8qXod1+CBB5r+wgfmmB0EWC9vJYkaPtK2glSwdNqhwD0Y1Syk+4PzX4I
DCbU6Ct268o2qPDavIUbJyps4gek+0ZoVa9xxSRH19BAPMkCQQDwJz5Yi91p3byw
X40WXaZCiC1CkceeQUpx2tuo3J/ijt6uQ638c0bNcM6FAx/nCEIAEHdCGZp0JYTa
TLgr5mHnAkEaxkkyPSK9YSWk0/p79XJGmsp8oPA3xtnu96U1z7pnzepQM+ra8Bj
CZ1vSat2FnyBB301aZXGcZCDtYrke+t/xwJBALa+1EhRSicODfdf+1U1IyyBMkYt
Sm+0fYd84JdPdayKiGGi5XSXD41eZw1AZ1frRw7w/iPM300yXRVABKwJmh8CQCB
```

Ca Bundle (CABUNDLE)

Paste the ca bundle here (optional):

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAu+gAwIBAgIBADANBgkqhkiG9w0BAQFADCBjzELMAkGA1UEBhMCdXMx
EDA0BgNVBAgTB2Zsb3JpZGExEDA0BgNVBAcTB2JyYW5kb24xDDAKBgNVBAoTA2Fz
ZDEPMA0GA1UECXMGYXNkYXNkMR0wGwYDVQQDEXR4M2RlbW9iLmNweDNkZW1vLmNv
bTEeMBwGC5qS5Ib3DQEJARYPYXNkYXNkQhdld3UuY29tMB4XDTA4MDcyMTA5MDU1
NFoXDTA5MDcyMTA5MDU1NFowY8xCzAJBgNVBAYTAnVzMRAdGgYDVQQIEwdmbG9y
aWRhMRAdGgYDVQQHEwdicmFuZG9uMQwwCgYDVQQKEwNhc2QxZDZANBgNVBAsTBmFz
ZGFzZDEdMBsGA1UEAxMUeDNkZW1vYi5jcHgzZGVtby5jb20xHjAcBgkqhkiG9w0B
CQEWD2FzZGFzZEB3ZXdlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA
617/z0At011XxWfm4VYu3Peb5cbB7UEf6FFA/U24DXuza0HLIsnt1u4/Yqsy5GFb
Dgu4R/ZYN+czt8IMWg0/Kqe3ARDcU+/9011t+EwtcNIyqz0QJ6qsxp/xG0XuAd85
```

10. Click **Install Certificate**. Your SSL certificate should now be installed, and the website configured to accept secure connections. You or your web host may need to restart Apache before it will work.

Manual Intermediate Certificate Installation

If the Intermediate certificate was not correctly installed using the above instructions you may need to install it directly in Apache. If you do not have access to the Apache configuration files you will need to have your web host or administrator follow these instructions to install the Intermediate certificate:

1. Locate the Virtual Host File:
On most Apache servers the Virtual Sites are configured in the /etc/httpd/conf/httpd.conf file. However, the

location and name of this file can vary from server to server -- Especially if you use a special interface to manage your server configuration. Another common name for the file is 'SSL.conf'. If you open the file with a text editor, you will see the configurations for the virtual hosts that are housed on the server. The virtual host configurations are probably found near the end of the file.

2. Identify the secure Virtual Host for your site:
Locate the Virtual host configuration for the site you are securing. It will have the proper name and IP address (including port 443).
3. Configure the Virtual Host For SSL:
cPanel has already setup the first three SSL configuration lines for you. Now you will edit your Virtual Host configuration by adding the 'SSLCertificateChainFile' line below (this line is bolded).

```
<VirtualHost 192.168.0.1:443>  
DocumentRoot /var/www/html2  
ServerName www.yourdomain.com  
SSLEngine on  
SSLCertificateFile /path/to/your_domain_name.crt  
SSLCertificateKeyFile /path/to/your_private.key  
SSLCertificateChainFile /path/to/IntermediateCA.crt  
</VirtualHost>
```

Of course, the path and names of your certificate files may be different. When typing the path for your SSLCertificateFile, type the path and filename you plan to use when saving your intermediate certificate. It is generally advised to save your intermediate certificate in the same directory that cPanel already saved your primary certificate to.

4. Save the changes to your configuration file.
5. Save the Intermediate Certificate file to the Server:
Verify that the Intermediate Certificate file is saved to the path you configured above.
6. Restart Apache.