



## How to Generate a CSR for cPanel 11.x

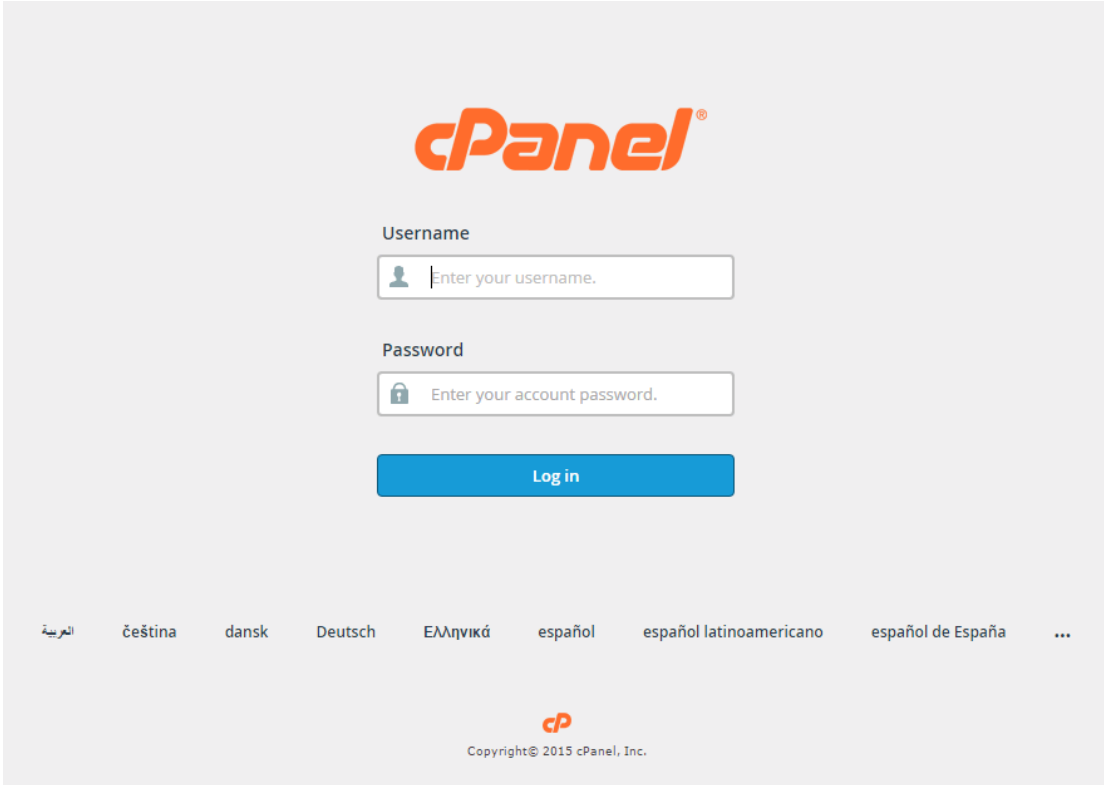
The following instructions will guide you through the CSR generation process on cPanel (Paper-Lantern Theme Modern). To learn more about CSRs and the importance of your private key, reference our [Overview of Certificate Signing Request](#) article. If you already generated the CSR and received your trusted SSL certificate, reference our [SSL Installation Instructions](#) and disregard the steps below.

### 1. Log In

Log in to cPanel, this can typically be accessed by going to `https://domain.com:2083`.

Note: You may encounter error message “Your connection is not private” or something similar when attempting to visit your cPanel login page.

Enter your Username/Password and click Log in.

A screenshot of the cPanel login page. At the top center is the orange cPanel logo. Below it, the word "Username" is followed by a text input field containing a user icon and the placeholder text "Enter your username.". Below that, the word "Password" is followed by a text input field containing a lock icon and the placeholder text "Enter your account password.". A blue "Log in" button is positioned below the password field. At the bottom of the page, there is a horizontal list of language links: العربية, čeština, dansk, Deutsch, Ελληνικά, español, español latinoamericano, and español de España, followed by an ellipsis. The footer at the very bottom features the cPanel logo and the text "Copyright © 2015 cPanel, Inc."



## 2. Navigate to cPanel Home

View your cPanel Home page.

**cPanel** Search Features GUMBLURC LOGOUT

### GUMBLURC

Main Domain	<b>gumblur.com</b>
Home Directory	/home/gumblurc
Last Login From	65.35.97.126
CPU Usage	0 / 100 %
Memory Usage	0 / 1024 MB
Entry Processes	0 / 20
Disk Space Usage	1.76 MB / 125 GB
Monthly Bandwidth Transfer	153.6 KB / 4 TB
Email Accounts	0 / 9,999
Mailing Lists	0 / ∞
Addon Domains	0 / 9,999
Subdomains	0 / 9,999
Domain Aliases	0 / 9,999
FTP Accounts	0 / 9,999

### FILES

- File Manager
- Images
- Directory Privacy
- Disk Usage
- Web Disk
- FTP Accounts
- FTP Connections
- Backup
- Backup Wizard
- R1Soft Restore Backups

### DATABASES

- phpMyAdmin
- MySQL Databases
- MySQL Database Wizard
- Remote MySQL

### DOMAINS

- Addon Domains
- Subdomains
- Aliases
- Redirects
- Simple Zone Editor
- Advanced Zone Editor


### EMAIL

Note: Older versions such as X3 Theme-Classic may not look like the image above, but should still contain the same concept and category structure.


## 3. Navigate to the SSL/TLS Manager


Navigate to the SSL/TLS Manager page by scrolling down to the Security section and select the SSL/TLS button.





 CPU and Concurrent Connection Usage


**SECURITY**


 SSH Access

 IP Blocker

 SSL/TLS

 Hotlink Protection


 Leech Protection

 ModSecurity

**SOFTWARE**

Note: You can also navigate to the SSL/TLS Manager page by utilizing the Search Feature at the top right of the cPanel home page and searching “SSL”.

Your SSL/TLS Manager page will allow you to manage everything related to SSL/TLS configuration for cPanel.

 **SSL/TLS**

The SSL/TLS Manager will allow you to generate SSL certificates, certificate signing requests, and private keys. These are all parts of using SSL to secure your website. SSL allows you to secure pages on your site so that information such as logins, credit card numbers, etc are sent encrypted instead of plain text. It is important to secure your site's login areas, shopping areas, and other pages where sensitive information could be sent over the web.

**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.](#)

**Install and Manage SSL for your site (HTTPS)**  
[Manage SSL sites.](#)

#### **4. Select Generate view, upload, or delete SSL certificate signing requests.**

Fill out the Request Form and click Create.



## Generate a New Certificate Signing Request (CSR)

Use this form to generate a new certificate signing request for your domain. Your SSL certificate authority (CA) will ask for a certificate signing request to complete the certificate purchase. Your CA may require specific information in the form below. Check with the CA's CSR requirements for the Apache web server.

**Key\***

Generate a new 2,048 bit key.

**Domains \***

Provide the FQDNs that you are trying to secure, one per line. You may use a wildcard domain by adding an asterisk in a domain name in the form: \*.sample.com. NOTE: Many CAs charge a higher price to issue multiple-domain certificates (sometimes called "UCCS" or "SAN certificates") and certificates that include wildcard domains.

**City\***

Provide the complete name for the city or locality. Do not use abbreviations.

**State\***

Provide the complete name for the state or province. Do not use abbreviations.

**Country\***

Choose a country.

Choose the country of origin for the certificate's "Company".

**Company\***

Provide the legally-registered name for your business. If your company name includes symbols other than a period or comma, check with your certificate authority to confirm that they are acceptable.

**Note 1:** By default, cPanel will automatically generate the corresponding private key if "Generate a new 2,048 bit key" is selected as the Key option. If you already have a private key created that you wish to use, select the Key dropdown and select the appropriate option.

**Note 2:** cPanel does not require a passphrase for your CSR, but does recommend inputting a description such as "CSR for www.google.com 9/13/2016" that helps distinguish this CSR going forward.

**Note 3:** To avoid common mistakes when filling out your CSR details, reference our Overview of Certificate Signing Request article.

## 5. Generate the order

Congratulations, you have created a CSR and automatically saved it in your user directory.



## SSL/TLS

### Generated Certificate Signing Request



The Certificate Signing Request for "www.gumblur.com" has been generated and saved in your user directory. To purchase a trusted certificate, you must copy the Encoded Certificate Signing Request below and send it to the Certificate Authority. Follow the instructions provided by your Certificate Authority.

**Domain:**

www.gumblur.com

**Description:**

www.gumblur.com 1

**Encoded Certificate Signing Request:**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAcCAQAwZ2kxODAwBgNVBAU0M3d3dy5ndw11bHVyLmNvbnRlEQMA4GA1UE
CwwHR3VtYmx1c3RlEQMA4GA1UECAwHRm9udGVzcm1kYTEQMA4GA1UECgwHR3VtYmx1c3Rl
MB8GCSqGSIb3DQEJARYSbm1jay5wQGd1bW1sdXIuY29tMQswCQYDVQGEwJVUzEX
MBUGA1UEBwwOU3QuIFB1dGVyc211cmVwggEiMA0GCSCqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCvU0LZz08kxmwwNEdbxIXfdrLuLFRhdXk3XShIeFnq5ZIXQp12AZ
eH4X38mIHuEbowzvA8aahqtLAENg9DramonVrXSF0K62DoE1VnxAbs0p3ILMyr
rtxpK2a/Xo0q7PBjZk68a4gRwYfYH584sq0gW5nxPpoUcCb412Rcr5yNuzN3n5x
ozp5IbVu2s1/3RN0w6B33loS0MPq8sW6hXiP30cajYZzsvOySKd5K8Ys+1rxwSYm
E71hVutsjgKHGcuPwEravahu/63V+Qu+70NmkfJG2JMKjgaoyJEHdORH9zAReQI
+mzKnu5dsINrU1sq856EyZAYrfg/yhb/AgMBAAAGADANBgkqhkiG9w0BAQsFAAOCA
QEAdymAVGg2BZ38hN7nuz+jhS1vwFC8HKzshH61j7vFBgh1UprMzupzvVqcvbxZ
mbynS168h1MarzRD1Lj3C1JCMxbVaky+sQBHRcZHLv4fptCawpQG2ozjhK1zHLPN
X/12ywhBXu9LnQrGvQ1woQeVw32YoHqXldRHzCuuZdP1zu0U0Z1b5tg00Y23XCo
BwGveYmE62Uhgals+j5zDvxMBmRH6Y7CKwdYZ1umh4MEd071wOEYHr18PmL+1LZ1
tF/q/dkDn014USgD6tG9NqnaL787cG8j2YX+BLjvXpq2C/rBK0d0e+DhBLdAgeAA
yIBYH75qHMQpCK2aYm3hkiA==
-----END CERTIFICATE REQUEST-----
```

**Decoded Certificate Signing Request:**

```
Certificate Request:
Data:
  Version: 0 (0x0)
```

Click into the Encoded Certificate Signing Request text box that's presented after generation, and copy all of the text including:

-----BEGIN CERTIFICATE REQUEST-----

And

-----END CERTIFICATE REQUEST-----

Return to the Generation Form back 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 cPanel (Paper-Lantern Theme Modern)