



How to Install an SSL/TLS Certificate In cPanel 11.x

The following instructions will guide you through the SSL installation process on cPanel (Paper-Lantern Theme Modern). If you have more than one server or device, you will need to install the certificate on each server or device you need to secure. If you still have not generated your certificate and completed the validation process, reference our CSR Generation Instructions and disregard the steps below.

What You'll Need

1. Your server certificate

This is the certificate you received from the CA for your domain. You may have been sent this via email. If not, you can download it by visiting your Account Dashboard and clicking on your order.

2. Your intermediate certificates

These files allow the devices connecting to your server to identify the issuing CA. There may be more than one of these certificates. If you got your certificate in a ZIP folder, it should also contain the Intermediate certificate(s), which is sometimes referred to as a CA Bundle.

3. Your private key

This file should be on your server, or in your possession if you generated your CSR from a free generator tool. On certain platforms, such as Microsoft IIS, the private key is not immediately visible to you but the server is keeping track of it.

Installation Instructions


1. Log in to cPanel

The first step is to login to your cPanel account, this can typically be accessed by going to <https://domain.com:2083>


Note: You may encounter an error message “Your connection is not private” or something similar when attempting to visit your cPanel login page. This is caused due to your login page using a self-signed certificate by default. Please disregard this and proceed past the error message.

After navigating to your cPanel login page, enter your Username/Password and click Log in.






Username

 Enter your username.

Password

 Enter your account password.

Log in

العربية

čeština

dansk

Deutsch


Ελληνικά

español

español latinoamericano


español de España

...



Copyright© 2015 cPanel, Inc.

Your cPanel Homepage should look like this:



Search Features

GUMBLURC

LOGOUT

GUMBLURC

Main Domaingumblur.com

Home Directory/home/gumblurc

Last Login From65.35.97.126

CPU Usage0 / 100 %

Memory Usage0 / 1024 MB

Entry Processes0 / 20

Disk Space Usage1.76 MB / 125 GB

Monthly Bandwidth Transfer153.6 KB / 4 TB

Email Accounts0 / 9,999

Mailing Lists0 / ∞

Addon Domains0 / 9,999

Subdomains0 / 9,999

Domain Aliases0 / 9,999

FTP Accounts0 / 9,999

FILES

File Manager

Disk Usage

FTP Connections

R1Soft Restore Backups

Images

Web Disk

Backup

Directory Privacy

FTP Accounts

Backup Wizard

DATABASES

phpMyAdmin

MySQL® Databases

MySQL® Database Wizard

Remote MySQL®

DOMAINS

Addon Domains

Subdomains

Aliases

Redirects

Simple Zone Editor

Advanced Zone Editor

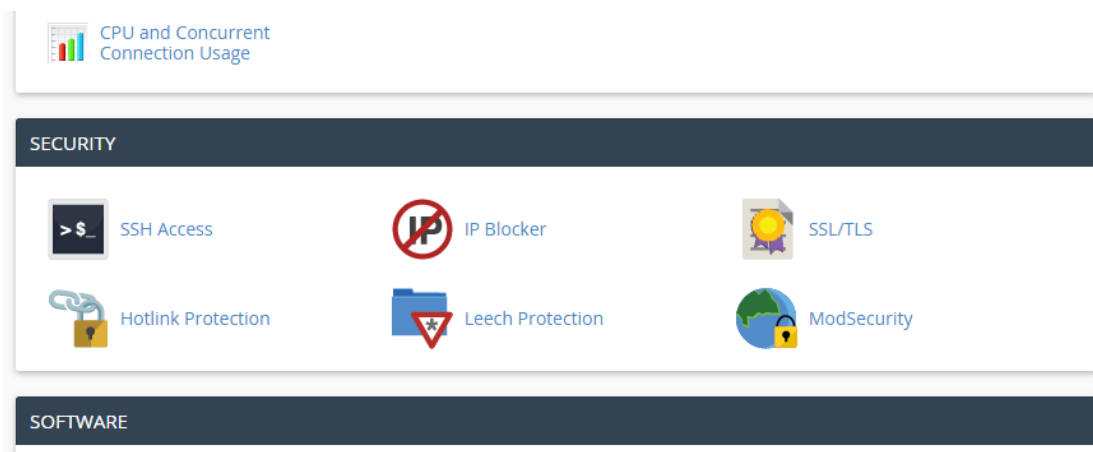
EMAIL



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.

2. Navigate to the SSL/TLS Manager

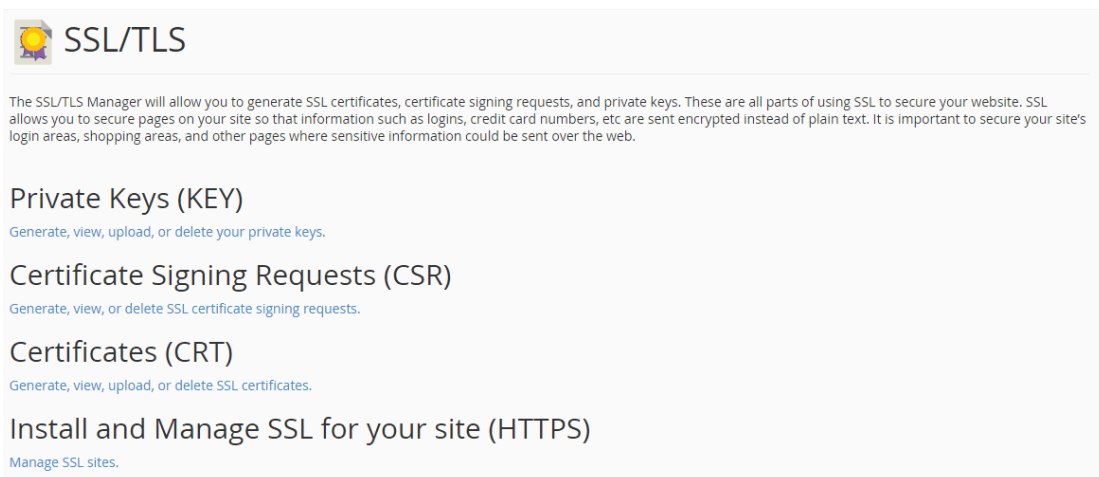
You can access your SSL/TLS Manager page by scrolling down to the Security section and selecting the SSL/TLS button.



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 for “SSL”.

3. Select “Manage SSL Sites”

Your SSL/TLS Manager page will allow you to manage everything related to SSL/TLS configuration for cPanel. The “Manage SSL Sites” Hyperlink is located underneath “Install and Manage SSL for your site (HTTPS)” shown below.





4. Select your domain

Change the Domain drop-down to the appropriate domain name that you want to install your SSL certificate on.

Domain
Select a Domain

IP Address
167.88.166.143

5. Copy and paste your certificate files

Once you have your domain selected, you just need to copy and paste your individual certificate files into the appropriate text box(s) pictured below.

Domain
Select a Domain

IP Address
167.88.166.143

Certificate: (CRT)

The certificate may already be on your server. You can either paste the certificate here or try to retrieve it for your domain.

Private Key (KEY)

The private key may already be on your server. You can either paste the private key here or try to retrieve the matching key for your certificate.

Certificate Authority Bundle: (CABUNDLE)

In most cases, you do not need to supply the CA bundle because the server will fetch it from a public repository during installation.

☒ Enable SNI for Mail Services

Install Certificate Reset



a) Certificate (CRT) – This is your server certificate that was issued to your domain(s).

Note 1: cPanel should automatically fetch the Certificate (CRT) text if you previously uploaded the server certificate in the “Generate, view, upload or delete SSL certificate” section of your SSL/TLS Manager and selected the correct domain name above in the dropdown.

Note 2: If you received the certificate in a ZIP file, click “Extract All” and then drag your server certificate into a text editor such as Notepad. This will allow you to copy all text contents needed including “—BEGIN CERTIFICATE—” and “END CERTIFICATE—”.

b) Private Key (KEY) – This is your private key that was created during the generation process.

Note 1: cPanel should automatically fetch the Private Key (Key) text if you previously created the Certificate Signing Request (CSR) in the “Generate, view, or delete SSL certificate signing requests” section of your SSL/TLS Manager and selected the correct domain name above in the dropdown.

Note 2: If you made the CSR and private key outside of your cPanel account and failed to save the files, you will have problems proceeding and may need to re-issue the SSL certificate with a newly created key pair.

c) Certificate Authority Bundle (CABundle) – This is your intermediate certificates that allow browsers and devices to understand who issued your trusted certificate.

Note 1: cPanel should automatically fetch the CA Bundle from a public repository.

Note 2: If you have multiple intermediate certificates, paste each of them one after another to create the correct certificate chain/path.

6. Click “Install Certificate”

Once you have the correct certificate files in the appropriate text boxes, simply click the blue “Install Certificate” button.

Congratulations! You’ve successfully installed your SSL certificate! To check your work, visit the website in your browser at <https://yourdomain.tld> and view the certificate/site information to see if HTTPS/SSL is working properly. Remember, you may need to restart your server for changes to take effect.

Note 1: You are not required to “Enable SNI for Mail Services.” Server Name Indication (SNI) should only be used if multiple hostnames are being served over HTTPS from the same IP address.

Note 2: You or your web host may need to restart the Apache server before the certificate will work.



Manual Intermediate Installation Instructions

If the intermediate certificates did NOT get successfully installed and configured after completing the above instructions, please reference the instructions below on how to manually install them directly in Apache. If you do not have access to your Apache server, please contact your web host or system administrator for additional assistance.

1. Locate the Virtual Host File

The Virtual Host File , this can typically be accessed in the /etc/httpd/conf/httpd.conf file. Note: The location and name of this file can change from server to server depending on your configuration. Another popular name for the file is "SSL.conf".

2. View the Virtual Host File

View the Virtual Host configuration with the proper name & IP address (including port 443).

3. Edit the Virtual Host File

Edit your Virtual Host configuration by adding the bolded YourIntermediateCertificate file below:

```
<VirtualHost 192.168.255.255:443>
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/YourIntermediateCertificate.crt
</VirtualHost>
```

Note: Make sure you type the correct file path and name where you plan on saving the intermediate certificates. You should save these certificates in the same directory that cPanel has your server certificate and private key stored.

4. Save the changes

Save the configuration file changes.

5. Add the intermediate certificate



Add the intermediate certificate file to the same directory that cPanel has your server certificate and private key stored.

6. Restart your server

Restart your Apache server.