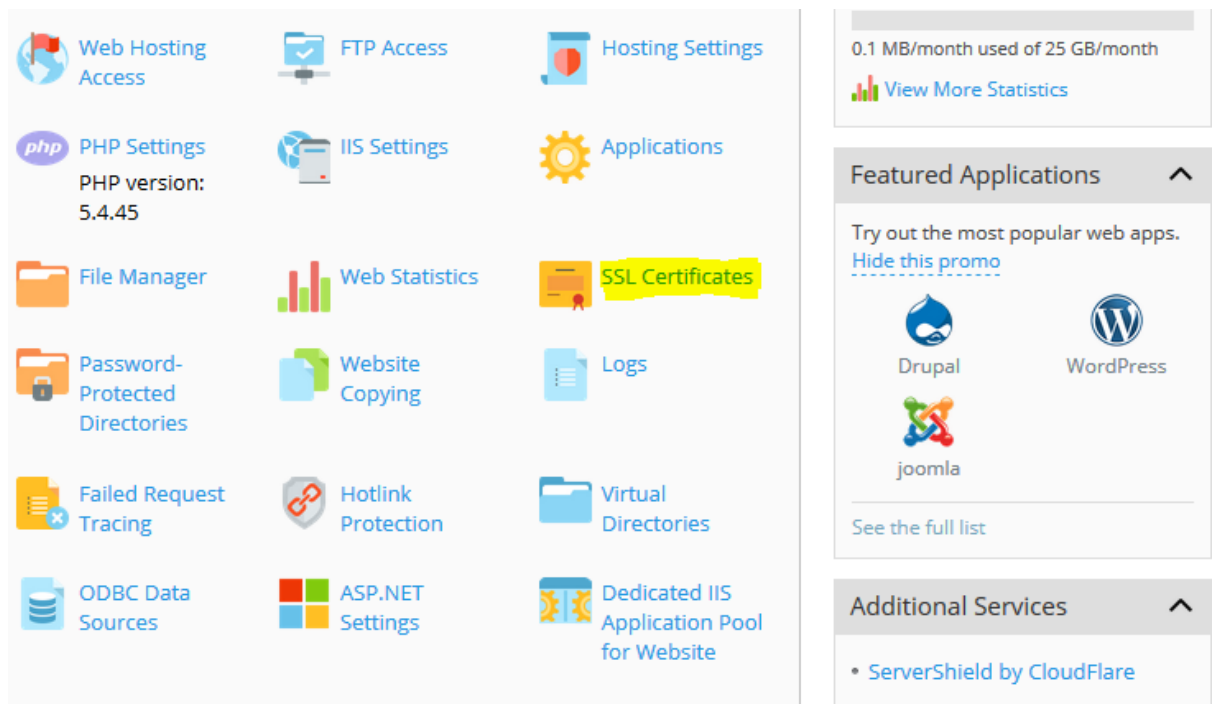


## How to generate certificate signing request (CSR) for a domain through Plesk?

### 1. Log in to your Plesk Panel

1. Go to: Websites & Domains > SSL/TLS Certificates. Click on SSL Certificates to bring up the SSL certificate



### 2. To generate new CSR click on “Add certificate”

If you created a certificate signing request on this server and received the certificate file, upload it here. If you want to upload a certificate and private key pair generated on a different server, or generate a self-signed certificate, click **Add SSL Certificate**.

After adding an SSL certificate to a domain, you need to enable SSL support and select that certificate in the website hosting settings: **Websites & Domains > Hosting Settings** of this domain > **Security**.

Upload the certificate here

Certificate (\*.crt) \*

[Browse...](#)

No file selected.

[Upload Certificate](#)

[Add SSL Certificate](#)

[Remove](#)



3. Fill out the Generate a New Certificate Signing Request form and click the request button to generate the new CSR.

### Add SSL Certificate

Certificate name \*

#### Settings

Use this form to generate a request for a certificate, to buy a certificate from your provider, or to generate a self-signed certificate.

A request is a CSR file that contains the information about your domain that you specified in the form. You can submit the request to a certification authority for issuing a certificate for you. You will then upload it using one of the upload forms below.

A self-signed certificate is an identity certificate signed by its own creator. If you use such a certificate, it means that you yourself verify your sites' identity. Although self-signed certificates allow the usage of SSL, they are trusted less, and considered as less secure.

Bits

Country \*

State or province \*

Location (city) \*

Organization name (company) \*

Organization department or division name

Domain name \*

Email \*

4. New record will be added to the list of SSL Certificates. Click on the newly created "domain-name-SSI-certificate" to see the CSR code and the Private Key that were created.

**Information:** The SSL certificate was added. To make the certificate work, select it in the website hosting settings (on the Websites & Domains tab).

If you created a certificate signing request on this server and received the certificate file, upload it here. If you want to upload a certificate and private key pair generated on a different server, or generate a self-signed certificate, click **Add SSL Certificate**.

After adding an SSL certificate to a domain, you need to enable SSL support and select that certificate in the website hosting settings: **Websites & Domains > Hosting Settings** of this domain > **Security**.

#### Upload the certificate here

Certificate (\*.crt) \*  No file selected.

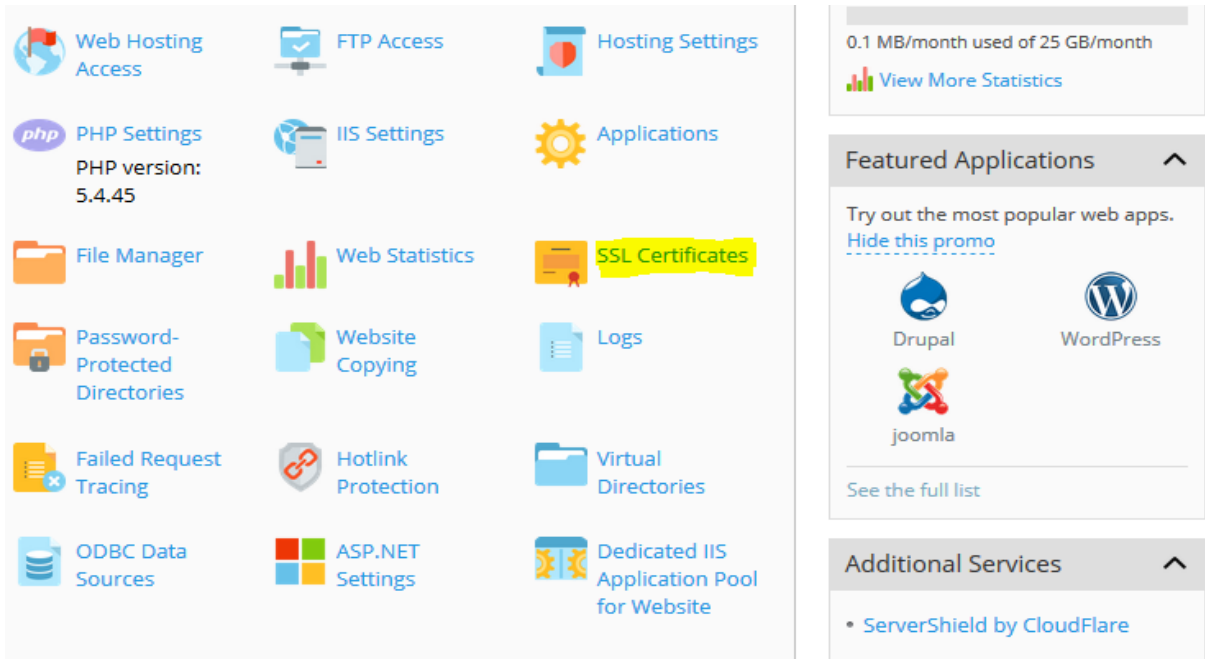
3 items total Entries per page: 10 25 100 All

<input type="checkbox"/>	R	K	C	A	Name ^	Used
<input type="checkbox"/>					<u>domain-name-SSI-certificate</u>	0 ↓

3 items total Entries per page: 10 25 100 All

# How to install SSL certificate through Plesk control panel:

1. Log in to your Plesk Panel
2. Go to the **Websites & Domains** tab and select the domain you want to secure. Click on "SSL Certificates" :



3. Select the SSL certificate "domain-name-SSL-certificate" that was created while generating the CSR code.

**Information:** The SSL certificate was added. To make the certificate work, select it in the website hosting settings (on the Websites & Domains tab).

If you created a certificate signing request on this server and received the certificate file, upload it here. If you want to upload a certificate and private key pair generated on a different server, or generate a self-signed certificate, click **Add SSL Certificate**.

After adding an SSL certificate to a domain, you need to enable SSL support and select that certificate in the website hosting settings: **Websites & Domains > Hosting Settings** of this domain > **Security**.

Upload the certificate here

Certificate (\*.crt) \*  No file selected.

3 items total

Entries per page: 10 25 100 All

<input type="checkbox"/>	R	K	C	A	Name	Used
--------------------------	---	---	---	---	------	------

<input type="checkbox"/>					domain-name-SSL-certificate	0
--------------------------	--	--	--	--	-----------------------------	---

3 items total

Entries per page: 10 25 100 All



- Return to the Websites & Domains tab and click on 'Hosting settings' next to the domain in question.

Website at <httpdocs/> IP address: [REDACTED] System user: xxnxbsw

[Hosting Settings](#) [Open](#) [Preview](#) [Suspend](#) [Disable](#) [Description](#)

[My CMS](#) [Log In](#) [Security Scan](#) [Manage Plugins](#) [Manage Themes](#)

[My CMS](#) [Log In](#) [Security Scan](#) [Manage Plugins](#) [Manage Themes](#)

^ SHOW LESS

- Web Hosting Access
- FTP Access
- Hosting Settings
- PHP Settings  
PHP version: 5.4.45
- IIS Settings
- Applications
- File Manager
- Web Statistics
- SSL Certificates
- Password-Protected Directories
- Website Copying
- Logs
- Failed Request Tracing
- Hotlink Protection
- Virtual Directories
- ODBC Data Sources
- ASP.NET Settings
- Dedicated IIS Application Pool for Website


- On the next page locate the **Security** section, select the certificate from the drop-down list and make sure that 'SSL Support' is checked.

### Security

To secure transactions with your site, use SSL protocol, which encrypts all data and transfers it over a secure connection. To employ SSL, install an SSL certificate on the site, and then select it below.

SSL support

Certificate

Default Certificate (other repository) 

- Click 'Apply' at the bottom of the page to save the changes.

## How to Verify SSL Installation

1. To verify if your certificate is installed correctly, use our Certificate Installation Checker.  
URL : <https://cryptoreport.geotrust.com/checker/>
2. Test your SSL certificate by using a browser to connect to your server. Use the https protocol directive. For example, if your SSL was issued to secure.mysite.com, enter <https://website-name> into your browser.
3. Your browser's padlock icon will be displayed in the locked position if your certificate is installed correctly and the server is properly configured for SSL.