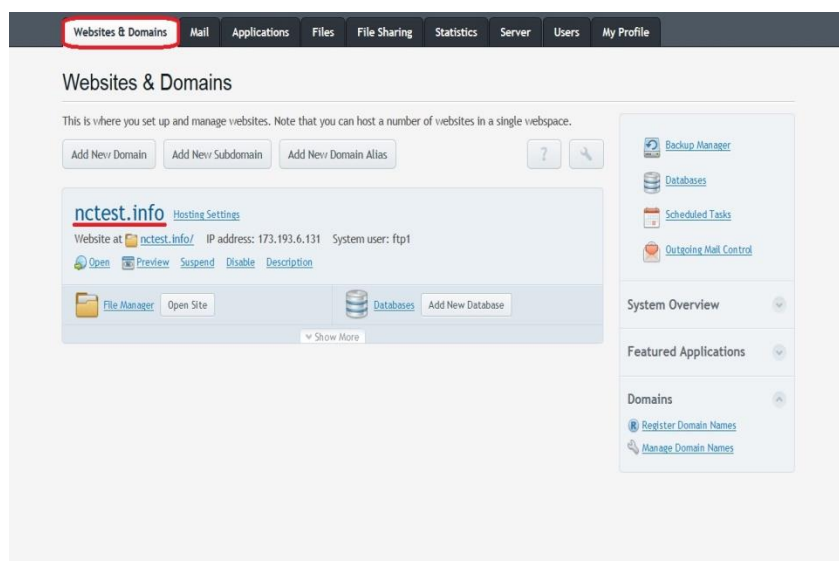


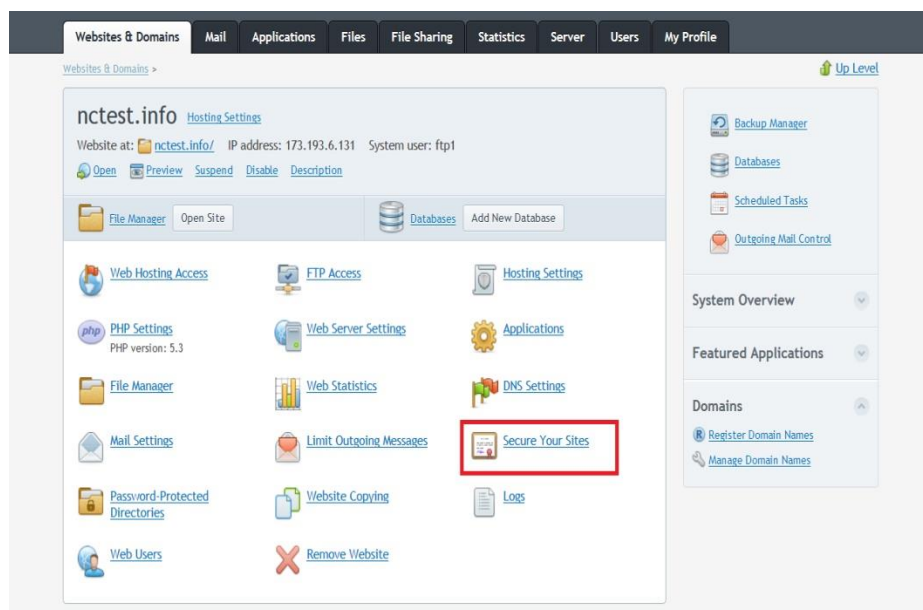
Generating CSR in Plesk 12

Please follow the instructions below to generate the CSR code in your Plesk 12 Panel

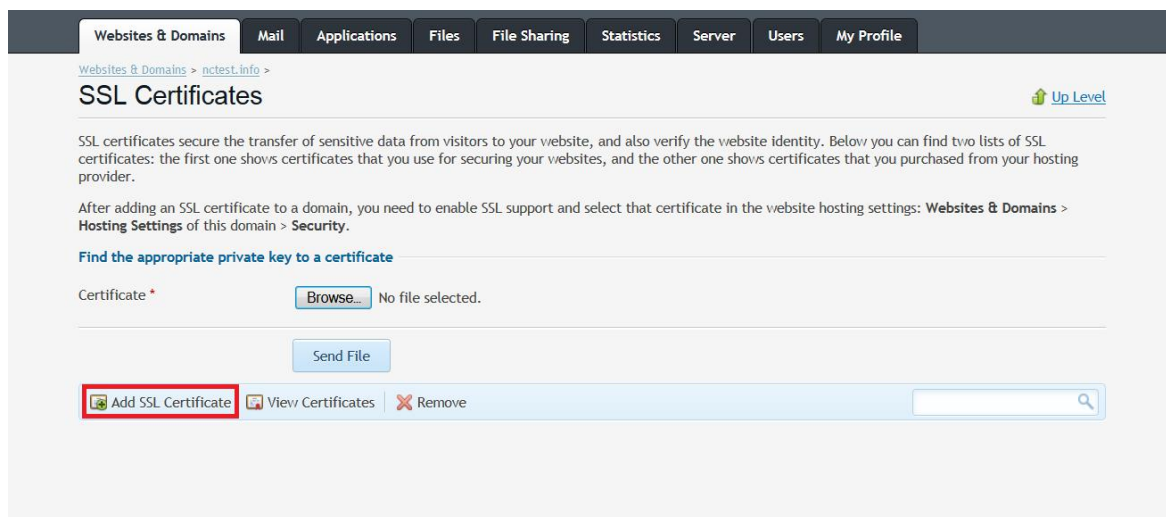
1. Log in to your Plesk Panel
2. Go to the **Websites & Domains** tab and select the domain you want to secure.



3. Click on 'Secure Your Sites'



4. Click on the 'Add SSL Certificate' button



5. On the next page enter the Certificate Name to easily recognize the certificate among the others on the server and fill in the required information for the CSR code:

Country: Select your country from the drop-down list.

State or province: Provide the complete name for your state or region. If not applicable, you can use your city instead.

Location (city): Provide the complete name for your city or locality.

Organization name (company): Provide the legally-registered name for your business. If not applicable, you can put 'NA'.

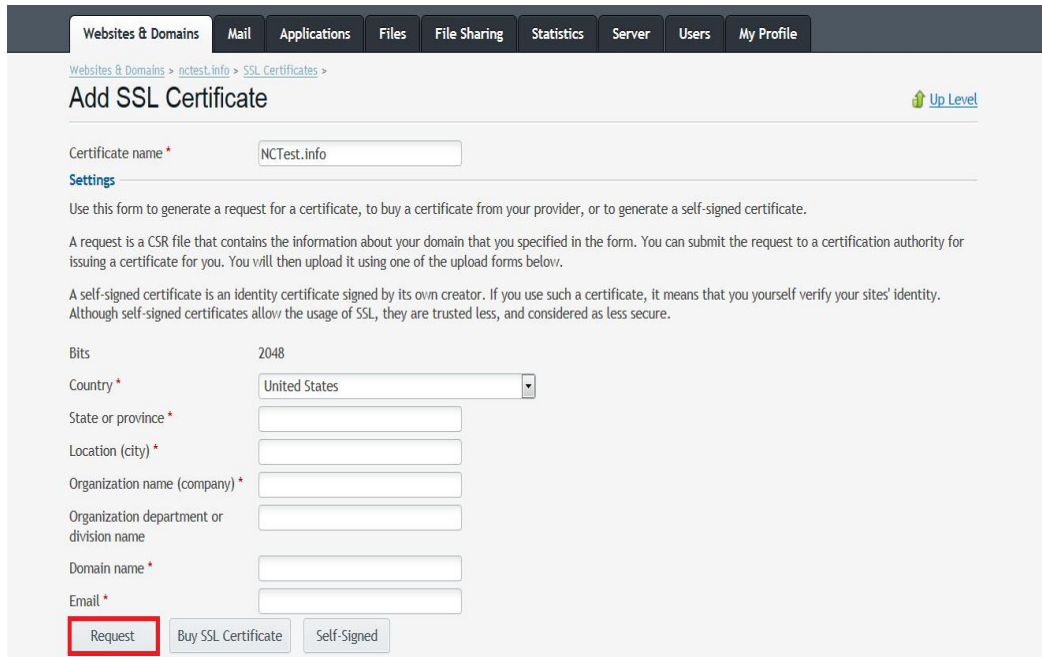
Organization department or division name: Provide the name of division or department within the organization indicated above.

Domain name: Enter the fully qualified domain name for which the SSL will be activated (common name). The common name for Wildcard certificates should be represented with an asterisk in front of the domain (*.example.com).

E-mail: Enter your email address. The email used for CSR generation will not be used for domain control validation or for reception of the issued certificate.

Note: Please keep in mind that it is not possible to generate the CSR with additional domains (SANs) in Plesk. They can be only added in the corresponding fields during activation of a multi-domain certificate in your Namecheap account.

6. Click on the 'Request' button



Websites & Domains | Mail | Applications | Files | File Sharing | Statistics | Server | Users | My Profile

Websites & Domains > nctest.info > SSL Certificates > [Up Level](#)

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: 2048

Country *

State or province *

Location (city) *

Organization name (company) *

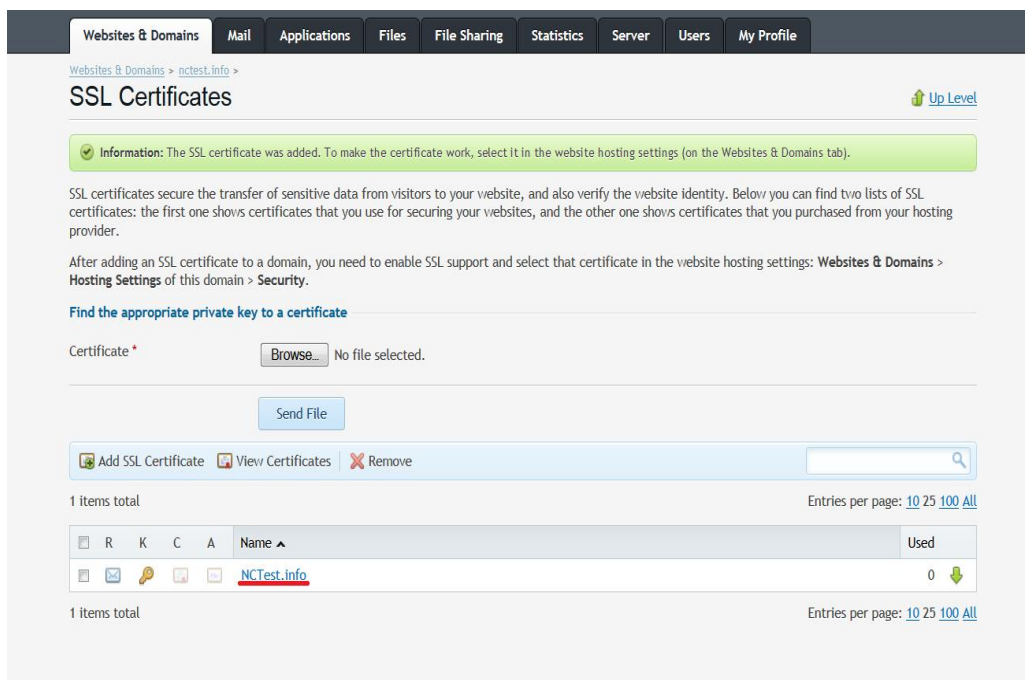
Organization department or division name

Domain name *

Email *

Request | Buy SSL Certificate | Self-Signed

7. A new record will be added to the list of SSL Certificates. Click on the newly created certificate to see the CSR code and the Private Key that were created.



Websites & Domains | Mail | Applications | Files | File Sharing | Statistics | Server | Users | My Profile

Websites & Domains > nctest.info > [Up Level](#)

SSL Certificates

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

SSL certificates secure the transfer of sensitive data from visitors to your website, and also verify the website identity. Below you can find two lists of SSL certificates: the first one shows certificates that you use for securing your websites, and the other one shows certificates that you purchased from your hosting provider.

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**.

Find the appropriate private key to a certificate

Certificate * No file selected.

1 items total Entries per page: [10](#) [25](#) [100](#) [All](#)

R	K	C	A	Name	Used
☐	☐	☐	☐	NCTest.info	0 Down

1 items total Entries per page: [10](#) [25](#) [100](#) [All](#)

The CSR code will be located at the bottom of the next page. Please include -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- when submitting the CSR code for SSL activation.

CSR

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICzzCCAQAwgYkxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybmhl  
MRQwEgYDVQQHEwtMb3MgQW5nZWxlczEQMA4GA1UEChMHTkMgVGVzdDEUMBIGA1UE  
AxMLbmN0ZXN0LmluZm8xJzAlBgkqhkiG9w0BCQEWGHZbHNlcHBvcnRABmFtZWNo  
ZWFwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAKx72xapIR7w  
78GLw8NqA7eYN+SUMW3ruho5o0/aPbS+IXXMyCim0vg1V3F9lsacRQhbN8PpjZ0v  
29PV/Z+ehE3S6ryTHPB0h7/V93MFINDb0y7Mm1TwMyHnf6j4eq5wmdrNsu7r3NQ4  
kHocseJ2trBUaQDjt1b8pH9ZtJzB2bhWyEf+vdwsPcZ/6PcdQncqUo4bbt/hzNod  
2n2WV3XEHku4mkSdgpU+i/hknt6aGSyV5sCyJoJ5c5tIhmIS8OV0EAUzDq2R4L4L  
LRqOrdYdCc/cFTYl1erVktIFb1GibwVGRu1PYJic3TcRlJt5prrt77n5zuZ0aDC5  
mrfzJCiXqVMCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IBAQCBNpZLtjXh7OQjhIbi  
3wouu4AWbv3Lhafj/VclXB1ONucL1ehM8vcxPJD93+3PX/J6p+65SUP6U5jObiP6  
vkbVWkywCA/1Wgg+JZyYIyAZAzJy6qWPjUDBAdLIk/o6NBei10OmOlJ7DV8OGwnz  
1oPYKL38vopS6X0nD+3EFUjFfqi28g/YgXPYcfKVVXaFUPa08vkZ6/eCD713NfJq  
i66ZF1hJUNdbKQu6UYB/sBfK9Bhd2q0XVWzgSaat9jc1FMTYjhhc+1QfezHpsycU  
+D/gO7F7MVrRtdbOg7WW/mNDLsxPbR54locCdzSykjnvncJwFsV4B2B9sgTcQ2er  
2Thp  
-----END CERTIFICATE REQUEST-----
```

After the certificate is issued, follow the steps from this article to enable the SSL certificate for your site.