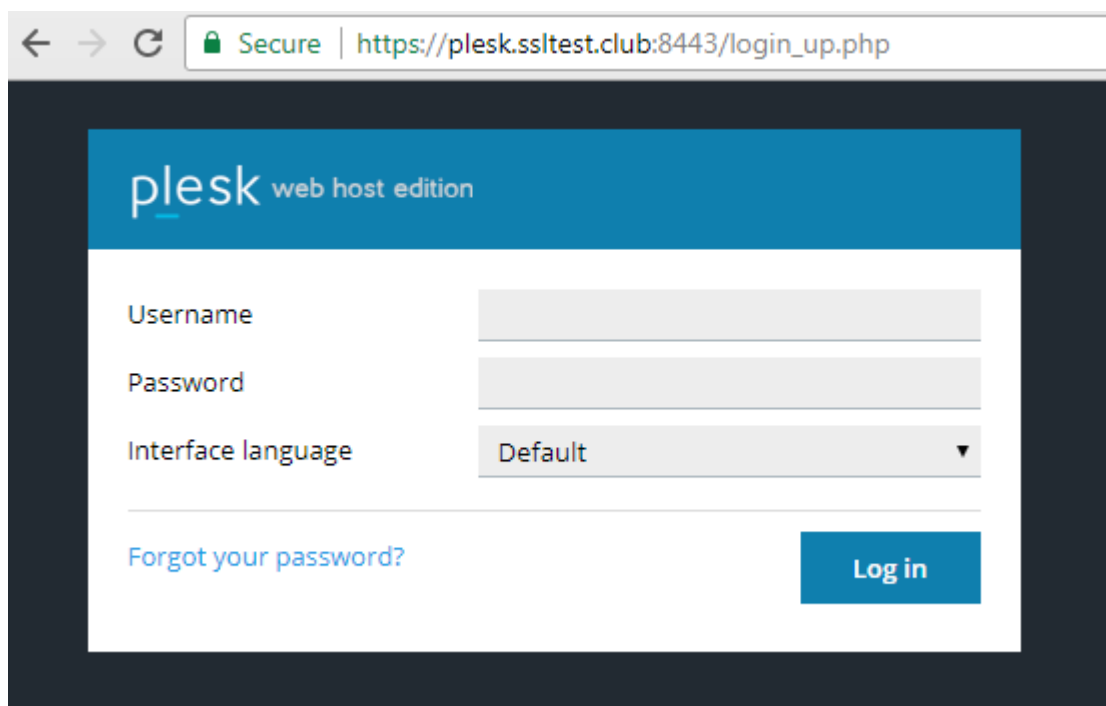


Generating a CSR on Plesk Onyx

CSR stands for certificate signing request. This request is used to send all necessary information such as domain name, location of the applicant or organization, public key to the Certificate Authority.

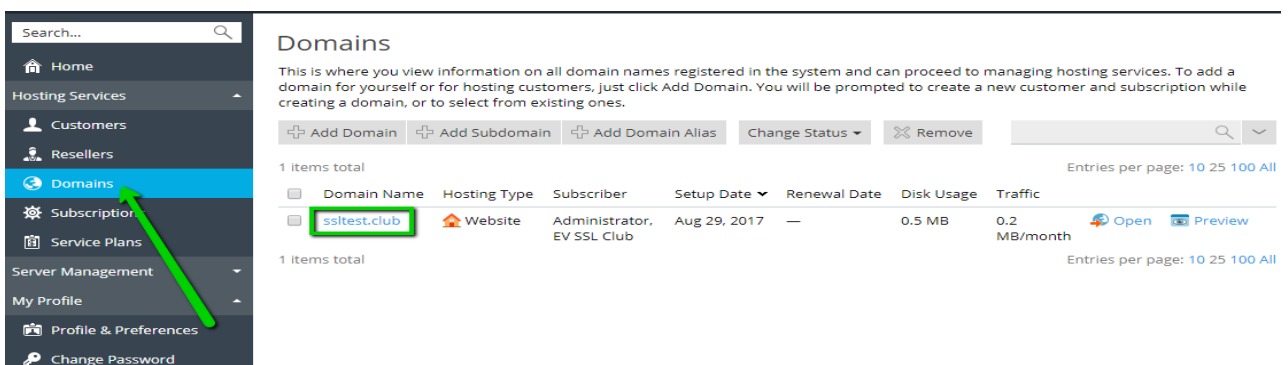
To generate CSR in your Plesk Panel, the following steps should be done:

1. Login to the Plesk control panel.



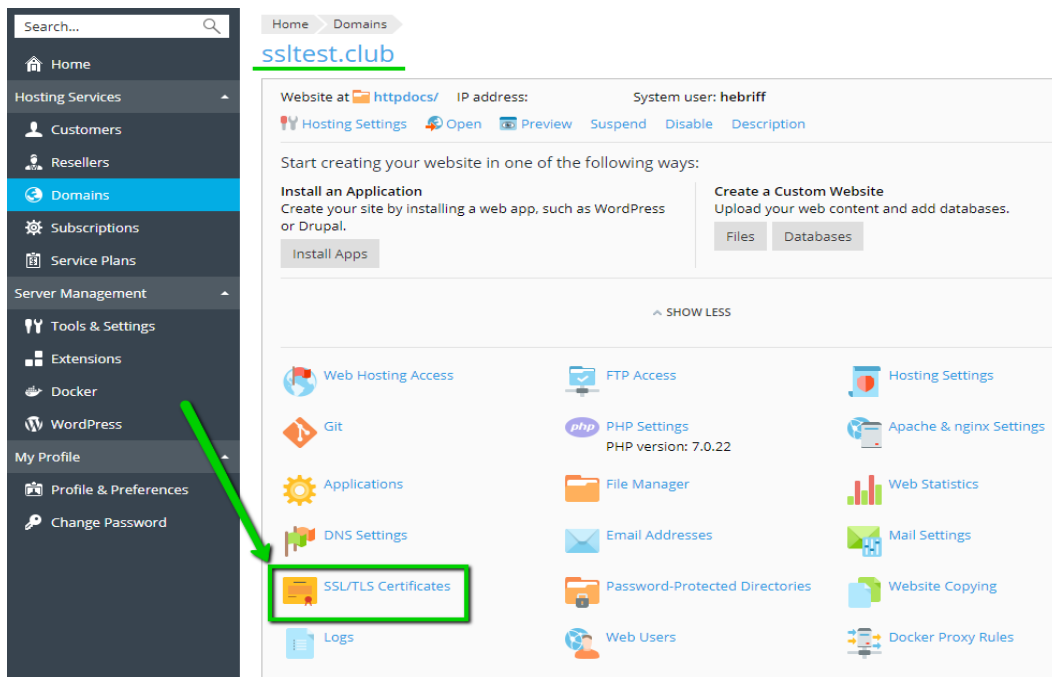
2. Depending on the Plesk account type, you can see two web interfaces:

- “**Service Provider** view” is the default for Server Administrator and Reseller accounts;
- “**Power User** view” is the default for Customer account.

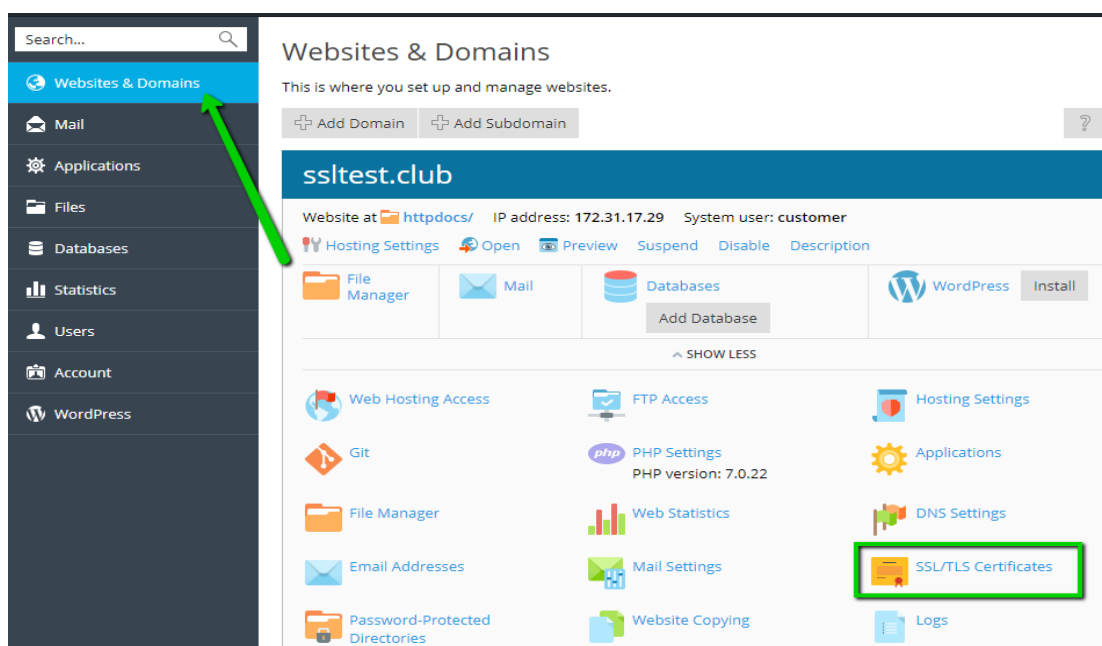


Click on “SSL/TLS Certificates”

- a) For “**Service Provider** view”, go to “Domains” section and click on your domain name that you are going to secure.



- b) For “**Power User** view”, go to “Websites & Domains” > Find the right domain name and click on “SSL/TLS Certificates”



3. Further instructions will be the same for both views. Click “Add SSL/TLS Certificate”

Home > Domains

SSL/TLS Certificates for [ssltest.club](#)

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/TLS Certificate](#).

After adding an SSL/TLS certificate to a domain, you need to enable SSL/TLS 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 chosen

No items found.



4. Fill out all the necessary fields on this page and click “Request”:
- ✓ “Certificate Name” - it can be any friendly name to distinguish a particular SSL certificate in Plesk Panel.
 - ✓ “Bits” - is a length of public key, 2048-bit is a minimum security standard nowadays.
 - ✓ “Country” - choose your country from the list, it will be shown in the CSR as two-letters country code.
 - ✓ “State or province” - state, county or region where the company or applicant is located.
 - ✓ “Location (city)” - is a locality or city of the country.
 - ✓ “Organization name (company)” - is the officially registered name of the organization that applies for a certificate. If you do not have any, put NA here.
 - ✓ “Organization department or division name” - is the name of the department or division within your organization. This is an optional field.
 - ✓ “Domain name” - is a fully qualified domain name (FQDN) that should be secured. The subdomain can be entered as well. To generate a CSR for a Wildcard certificate, put the server hostname in this format: *.domain.com.
 - ✓ “Email” - put your email here.

6. Scroll down in order to find the CSR code. Copy all of it including header -----BEGIN CERTIFICATE REQUEST----- and footer -----END CERTIFICATE REQUEST-----.

CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1jCCAb4CAQAwZAxCAJBgNVBAYTA1VTMQswCQYDVQQIDAJDQTEUMBIGA1UE
BwwLTG9zIEFuZ2VsZXh0FwZBAQMBGVBBAoMC0VWIFNTTCBDbHVIMRkwFwYDVQDDBB3
d3cuc3NsdGVzdC5jbHVMS0wKwYJKoZIhvcNAQkBFh51dWdlbmUubWl0cm9mYW5v
dkB6b251MzAwMC5uZXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9
dLyzXExmvTWH6ZkbGeBoSSF3wV2Kwg6g/iSyHFZ8NnJugR1kxu8VRDmIaQNg5/sR
Z++fN1p8+GAF/+1tMGyBbh88f/XNqb2p00IfhbFEHnjCEVkzx3rR7/UxAdG16G2
uJCjt633nTGfaSvhny2wVBD4QhXOy+N39K1iAU/Yr02d6TZ0inIvGOV5x4dSEq1s
QsNSnrePJDN71aQ+4IeyLgZISxcNZYGg2yKdj7s4PHQ07qUh8sHUftjTw8sm5x6q
GsqTevRj63npinQQHML06ntHSrEBiakKO6XBxd/DdUFvOLzeM+mO3rYSczUdHrMw
LjWiEnVqCdMAuFVAK+aLAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAAo4ayGR/q
hZTPN45nDeTSQjshIHp1h6MFykmiAzy2wdTnMO6NFayjN7V9BT/y3MOMNUzjmH5
1CL3t3axkCZAX1IObp7VU0hiAcIoEtVJ0UPyEZbB8yFRQRX3tJ8IU1UssNqHgICs
T9fUr5hjXLxwMc4E+kmtY3MRrLXDCPD2hygavCILThG1YpqSBmWCC8H/3R68uYFf
cLzyx2VU1m88UDP16j3n3zSedH4WLyHRplq733N1nM1barRq5NTOfqOxirPSNZyk
phDJNFZZXyELGum8JyVaae07x01Gd+ZgTT2N18/2M32YCuQnUPcnR68h+HwR0jTq
stM8sinY59gJGQ==
-----END CERTIFICATE REQUEST-----
```

Private key (*.key)

```
-----BEGIN PRIVATE KEY-----
```