

SSL

- [Adăugare certificat SSL în baza de date NSS](#)
- [Generare SSL după procurare](#)
- [SSL Let's Encrypt - instalare / reînnoire](#)

Adăugare certifi cat SSL în baza de date NSS

1. Extragere PEM din PFX:

```
openssl pkcs12 -in filename.pfx -out cert.pem -nodes
```

2. Pentru convertarea din .pem in pkcs12 pentru a fi folosit in baza NSS folosim următoarea comandă:

```
openssl pkcs12 -export -in cert.pem -out cert.p12 -name "MAIB_CERT"
```

3. Pentru a importa certificatul .p12 în baza de date NSS folosim următoarea comandă

```
pk12util -i cert.p12 -d sql:/etc/pki/nssdb
```

4. Pentru a verifica certificatele disponibile in bază:

```
certutil -L -d sql:/etc/pki/nssdb
```

5. Ștergere certificat din bază:

```
certutil -D -d sql:/etc/pki/nssdb -n "MAIB_CERT"
```


Generare SSL dupa procurare

1. Generarea CSR (cererea pentru certificat)

- [LOGIN TO PLESK](#) -> **Websites & Domains** -> **SSL/TLS Certificates** -> **Advanced Settings** -> **Add SSL/TLS Certificate**

1

Websites & Domains

Domains total

[Add Domain](#) [Add Subdomain](#) [Add Domain Alias](#)

Set view [Find domain...](#)

Domain name	Status	Disk usage	Traffic
[Domain Name]	Active	MB	MB/month

WordPress **Dashboard** [Hosting & DNS](#) [Mail](#) [Plesk Apps](#) [Get Started](#)

Files & Databases

- Connection Info for FTP, Database
- FTP
- Nextcloud
- Files
- Backup & Restore
- Databases
- Website Copying

Dev Tools

- PHP Version 8.1.33
- WordPress Management
- Logs
- Git
- Scheduled Tasks
- PHP Composer

Security

- SSL/TLS Certificates** Security can be improved
- Imunify
- Web Application Firewall
- Advisor
- Password-Protected Directories

WP Toolkit access **NEW**
Get WP Toolkit plugin for WordPress

Log in to WordPress
[Log in](#) [Setup](#)

Hire a developer **NEW**

Statistics
Disk space MB
Traffic this month MB
[More statistics](#)

Website at [httpdocs](#) IP address [IP] System user [User] [Add description](#)

2

Websites & Domains

SSL/TLS Certificate for [Domain]

[Reissue Certificate](#) [Unassign Certificate](#) [Advanced Settings](#)

3

Websites & Domains

SSL/TLS Certificates for [Domain]

If you created a certificate signing request on this server and received the certificate file, upload the certificate and private key pair generated on a different server, or generate a self-signed certificate.

After adding an SSL/TLS certificate to a domain, you need to enable SSL/TLS support and select settings: [Websites & Domains > Hosting Settings of this domain > Security](#).

Upload the certificate here

Certificate (*.crt) * [Choose File](#) No file chosen

[Upload Certificate](#)

[+ Add SSL/TLS Certificate](#) [Secure Webmail](#) [Secure Mail](#) [Remove](#)

2 items total [Add an SSL/TLS certificate.](#)

- Completați datele:
 - **Name:** Denumire/Perioadă (ex: 2026-2027)
 - **Bits:** 2048
 - **Country:** Moldova, Republic of
 - **State/Province:** Raion
 - **City:** Oraș
 - **Organization:** Nume companie/instituție
 - **Domain name:** Nume domeniu (ex: `domeniu.md`)
 - **Email:** Email valid
- Apăsați **Request** -> Deschideți certificatul creat -> Copiați codul **CSR**.

Certificate name *

2026-2027

Rename

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 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 they are trusted less, and considered as less secure.

Bits	2048
Country	Moldova, Republic of
State or province	Chisinau
Location (city)	Chisinau
Organization name (company)	Nume_companie
Organization department or division name	
Domain name	
Email	real_email@

Use this form to upload the components of a certificate as constituent files.

Certificate (*.crt) * Choose File No file chosen

CA certificate (*.ca.crt) No file chosen

[Upload Certificate](#)

Use this form to upload the components of a certificate as text. Copy the contents of a file and paste into the corresponding field.

Certificate (*.crt) *

CA certificate (*.ca.crt)

[Upload Certificate](#)

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

http://ncal.ac.cn/eng/201408/20140801144444.htm

Copy

Ctrl+C

Copy link to highlight

Search Google for "-----BEGIN CERTIFICATE REQUEST-----..."

Print...

Ctrl+P

[Open in reading mode](#)

Translate selection to English

2. Generarea certificatului SSL

- Autentificare cont client [my.host.md](#) -> **Servicii** -> Selectați serviciul SSL activ -> **Configure Now**.
- Setări:
 - **Web Server Type**: Selectați .
 - Lipiți codul **CSR**.
 - Apăsați **Click to Continue**.
- Selectați adresa de email pentru confirmare DV (trebuie să fie accesibilă).

3. Confirmarea solicitării

- Deschideți emailul primit pe adresa de confirmare.
- Accesați link-ul din mesaj pentru a aproba generarea.

4. Recepționarea certificatului

- Descărcați arhiva primită pe email după confirmare.

5. Instalarea certificatului în Plesk

- Extract fișiere local.
- Plesk -> **SSL/TLS Certificates** -> Deschideți certificatul de la Pasul 1 -> **Upload the certificate files**:
 - **Certificate (*.crt)**:
Încărcați

sau `Your EssentialSSL Certificate - yourdomain_md.crt`

****CA certificate (*.ca.crt)**** - Trebuie setate ambele consecutiv:

- Intermediate CA Certificate - SectigoPublicServerAuthenticationCADVR36.crt

Dacă mai apar eventuale întrebări, vă rugăm, nu ezitați să le oferiți.

- o **CA certificate (*.ca.crt):**

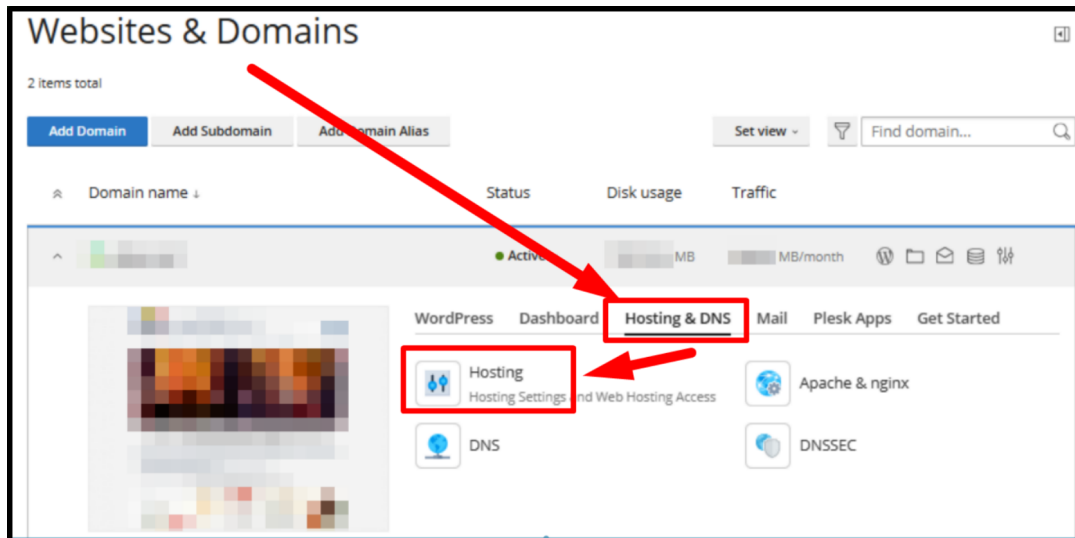
Încărcați `SectigoRSADomainValidationSecureServerCA.crt`

sau `Intermediate CA Certificate - SectigoPublicServerAuthenticationCADVR36.crt`

- Apăsați **Upload Certificate**

6. Activarea certificatului pe site

- Navigați la **Websites & Domains** -> **Hosting Settings**.
- La **Certificate**, selectați certificatul instalat -> Apăsați **OK**



Hosting Settings



Domain settings

Hosting type

Type

Preferred domain *
Visitors will be redirected here via a SEO friendly HTTP 301 redirect.

Document root *
The path to the website home directory

Domain settings

- Hosting type
- SSL/TLS support
- Web statistics
- Web scripting

Webspace settings

- System user's credentials
- SSH access
- IP addresses
- Disk space quota

SSL/TLS support

☒ Enabled
Encrypt connections between the website and the visitor's browser.

☒ Redirect visitors from HTTP to HTTPS via a SEO friendly 301 redirect

Certificate
Not selected
2026-2027 ()
Lets Encrypt ()
default certificate (other repository)

Web statistics

Tool

☒ Protect access to your web statistics with your FTP username and password

Web scripting

Select which programming and scripting language must be interpreted by the web server.

☒ FastCGI

☒ CGI

☐ SSI

☐ Custom error documents

Webspace settings FOR 2 DOMAINS

System user's credentials

Manage website's files and folders via FTP or File Manager. Access the server via SSH if permitted.

Username

Password

Specify a new password here to change the system user's password.

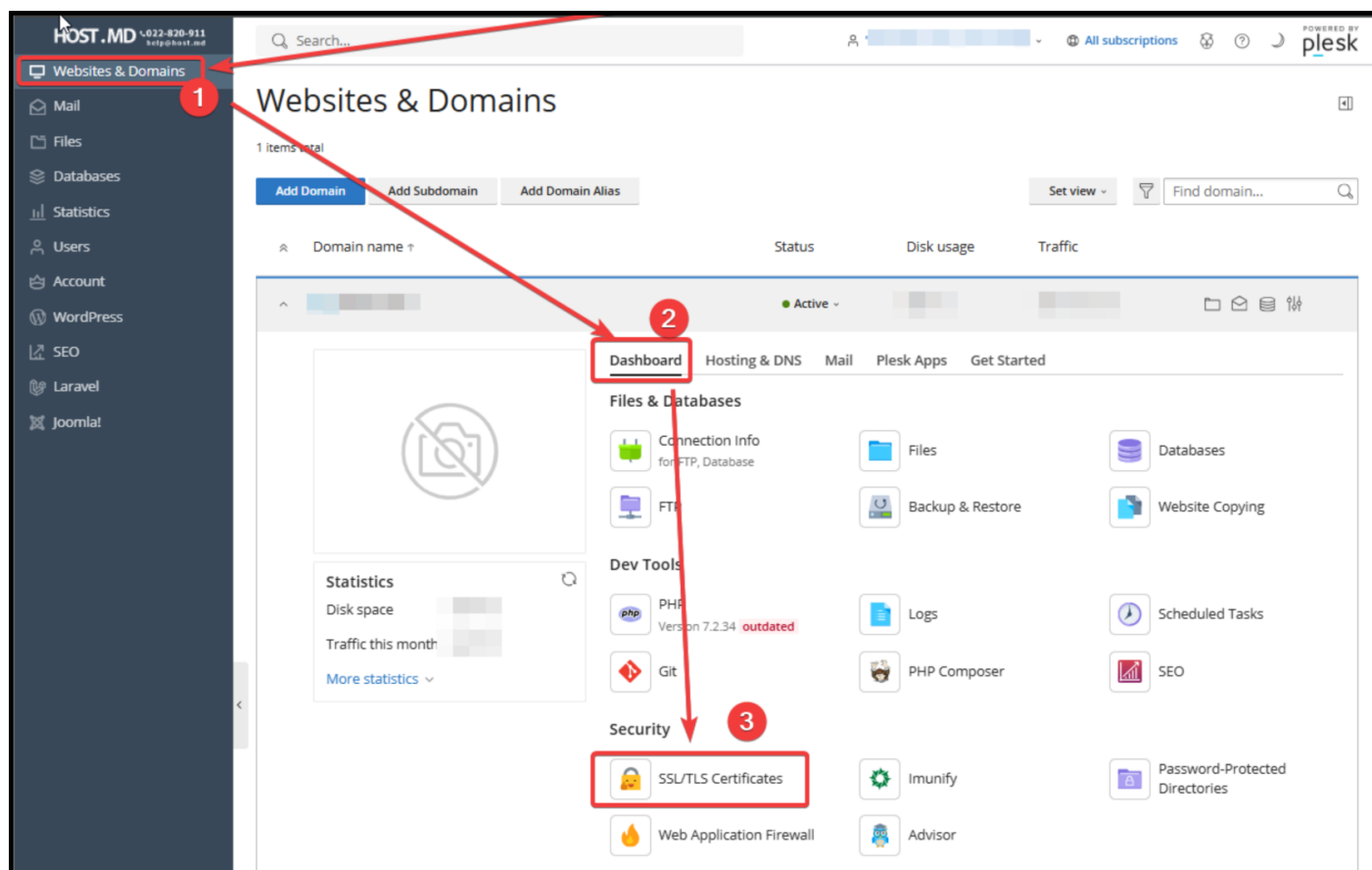
SSH access

Informație importantă despre valabilitate

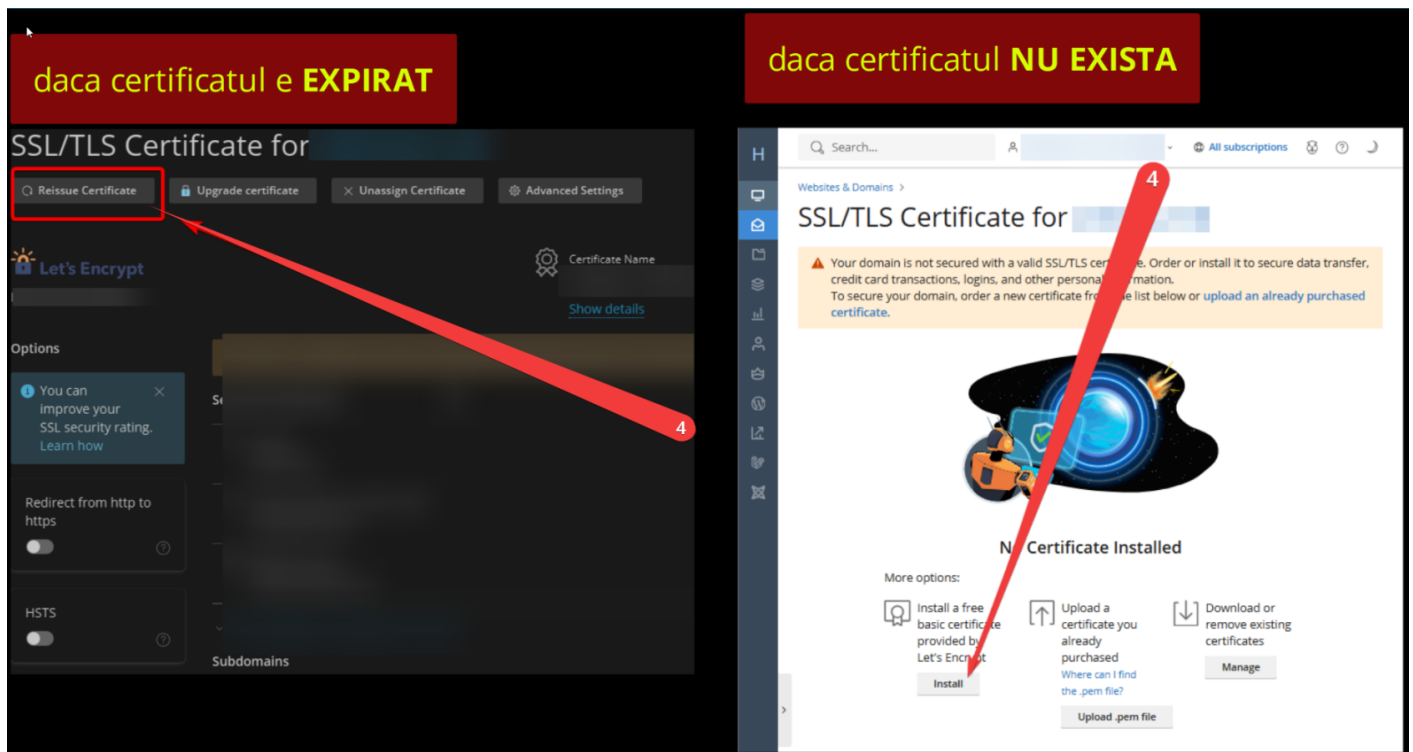
- Valabilitate maximă certificate SSL: **199 zile**.
- Reutilizare validare: DV până la 199 zile, OV până la 397 zile.
- La expirare: Procedura de instalare se reia.

SSL Let's Encrypt - instalare / reinoire

1 - Accesați modulul „**SSL/TLS Certificates**”



2 - Dați clic pe butonul „**Reissue Certificate**” (sau puteti avea doar 'Install' daca nu mai sunt certificate instalate)



3 - Alegeți opțiunea „- **Install** - a free basic certificate provided by **Let's Encrypt**” din partea de jos a meniului apărut

Choose a product to issue a certificate

PositiveSSL

Offers basic protection for a personal website. A reasonable choice if you need only encryption.

- Domain validation
- Recommended for a personal website

[Learn more](#)

\$9 [Buy](#)

PositiveSSL Wildcard

The Sectigo certificate that offers value for money. Secures the main domain as well as all its subdomains.

- Domain validation
- Wildcard support (incl. a webmail subdomain)
- Recommended for a personal website

[Learn more](#)

\$99 [Buy](#)

InstantSSL

Protects your business website and verifies your organization's identity. The certificate is issued within a few days or even faster.

- Domain and organization validation

Note: You need a publicly listed phone number.

[Learn more](#)

\$34 [Buy](#)

InstantSSL Wildcard

Protects your business website and verifies your organization's identity. Secures the main domain as well as all its subdomains. The certificate is issued within a few days or even faster.

- Domain and organization validation
- Wildcard support (incl. a webmail subdomain)

[Learn more](#)

\$149 [Buy](#)

PositiveSSL EV

The best protection for a business website. Verifies your organization's identity and gives your customers peace of mind by displaying your company name in the browser address bar. Takes a longer time to be issued (compared with other certificates) but offers the most trusted and secure solution.

- Domain and organization validation
- Organization Name in the Browser Address Bar

[Learn more](#)

\$99 [Buy](#)



Install a free
basic certificate
provided by
Let's Encrypt

[Install](#)



Upload a
certificate you
already
purchased

[Where can I find
the .pem file?](#)

[Upload .pem file](#)



Download or
remove existing
certificates

[Manage](#)

4 - Configurați opțiunile necesare și apăsați butonul „**Get it free**”

Let's Encrypt Entry-level protection
[Choose another]

Let's Encrypt is a certificate authority (CA) that allows you to create a free SSL/TLS certificate for your domain. By proceeding you acknowledge that you have read and agree to the [Let's Encrypt Terms of Service](#).
Note: The certificate will be automatically renewed 30 days in advance before its expiration.

- ☒ Secure the domain name
- ☐ Secure the wildcard domain (including www and webmail)
- ☐ Include a "www" subdomain for the domain and each selected alias
- ☐ Secure webmail on this domain
- ☐ Secure mail on this domain
- ☐ Assign the certificate to the mail domain
- IMAP, POP, SMTP on

Get it free Cancel