HOW TO INSTALL AN SSL CERTIFICATE VIA CPANEL

A RESOURCE FROM MAKEMEBAIT.COM

BY RAKTIM DUTTA

How to Activate & Install an SSL Certificate in cPanel

Installing an SSL certificate (aka Digital Certificate) in cPanel can be done in 5 steps.

The steps you need to take are:

1. *Buying a Dedicated IP Address (Recommended)*
2. *Buying an SSL certificate*
3. *Generating a CSR (Certificate Signing Request) code*
4. *Activating the Certificate*
5. *Installing the Certificate*

Buy a Dedicated IP Address

A dedicated IP address is generally required to install an SSL certificate on a web host. You only need to buy a dedicated IP address if you are on a Shared Hosting plan.

If your web host supports SNI technology, you can still install an SSL certificate without a dedicated IP address (in case you are not willing to buy a dedicated IP).

Make sure your web hosting service provider supports this SNI technology by contacting the support team.

Buy an SSL certificate

For the first step, I assume you already bought an SSL certificate for your website. If not then you can buy it directly from leading CA (Certificate Authority) like Comodo or from other third-party vendors like Namecheap, GoDaddy etc.

You can read more about SSL certificate here.

So, the next step is:

How to Generate a CSR code in cPanel

If you don't know what a CSR code actually is…

Here's a short definition:

A CSR or Certificate Signing Request code is a code which keeps your company or organization information in encrypted format. It is later checked or decrypted by the CA for issuing an SSL or digital certificate for the respective domain.

To generate a CSR code, you first need to log in to your cPanel dashboard.

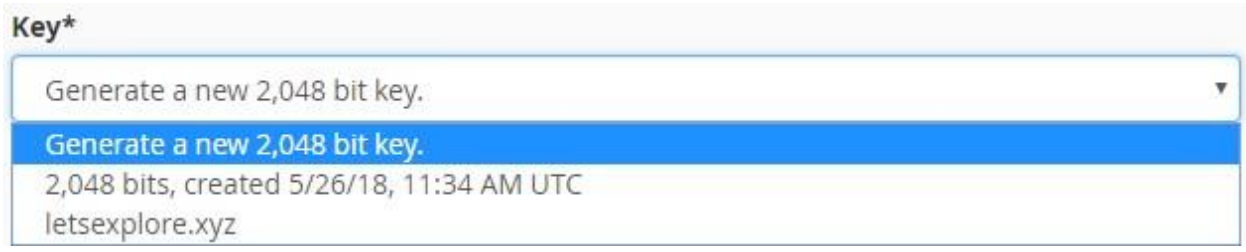
Locate the **SSL/TLS** manager under the **SECURITY** tab.

On the next page, click on **Generate, view, or delete SSL certificate signing requests** under **Certificate Signing Requests (CSR)**.

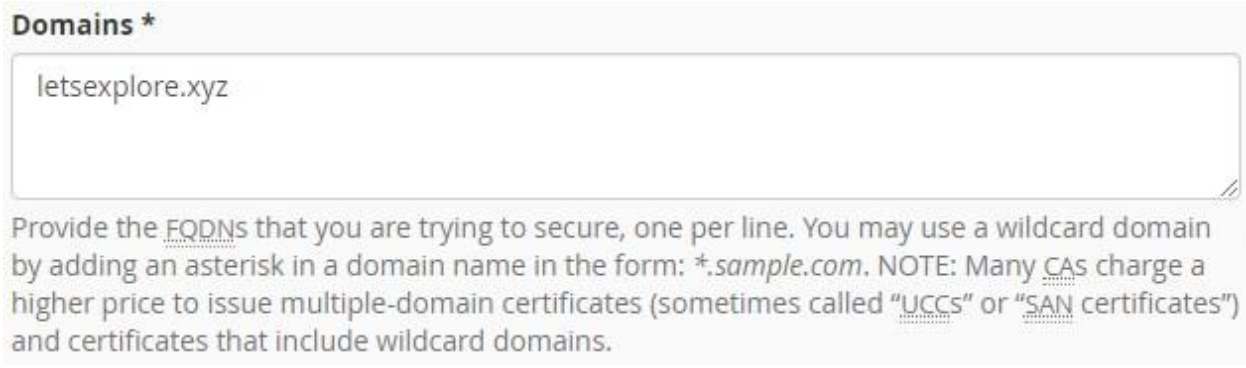
On the following page, enter all the required details in the CSR form.

The field names are described below for your convenience:

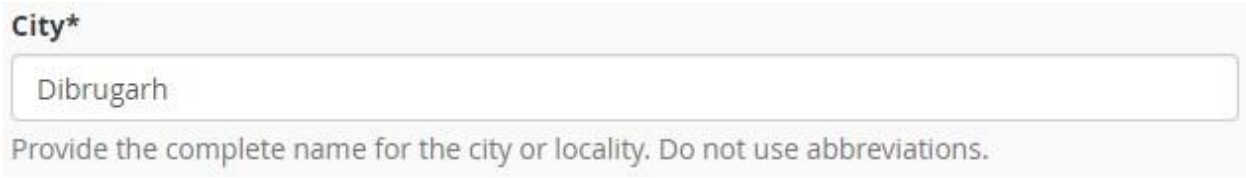
1. **Key**: Click the drop-down menu and select **Generate a New 2,048 bit key** to generate a fresh private key or select a key which was previously created.



2. **Domains**: Enter your domain name. If you are applying for a wildcard SSL then add an asterisk before domain name (e.g. *.example.com). And for multi-domain certificates enter each domain names in a new line.



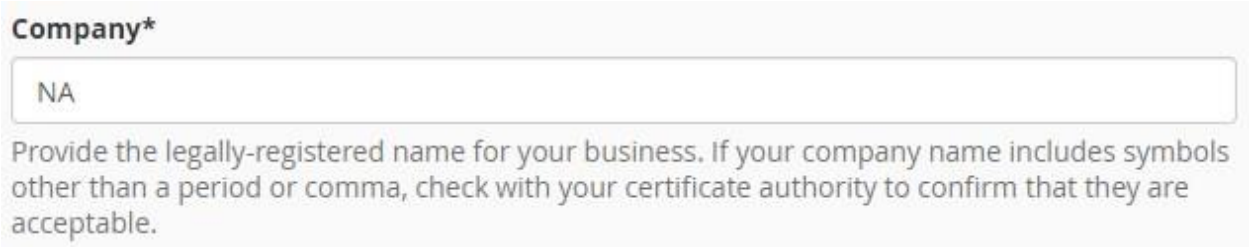
3. **City**: Enter the full name of the city your site or company belongs to. Do not enter any short name of the city.



4. **State**: Type in the name of the state your website or company belongs to. Again, try to avoid entering any short name of the state.

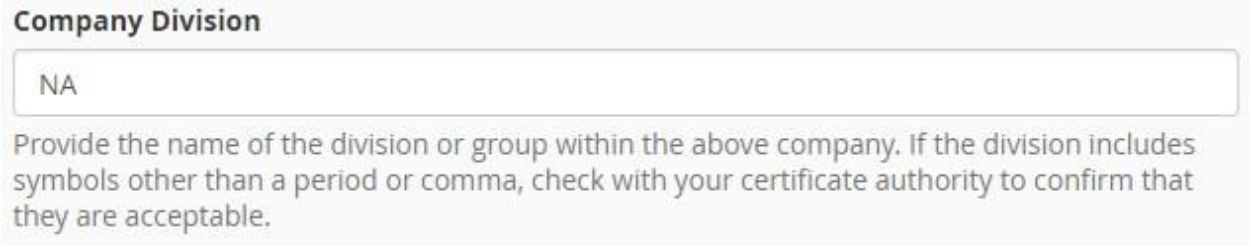
5. **Country**: Select the country from this drop-down menu to which your site or company belongs to.

6. **Company**: Type in the name of your legally registered business. If it is not legally registered yet then you type in **NA** for **Not Available**.

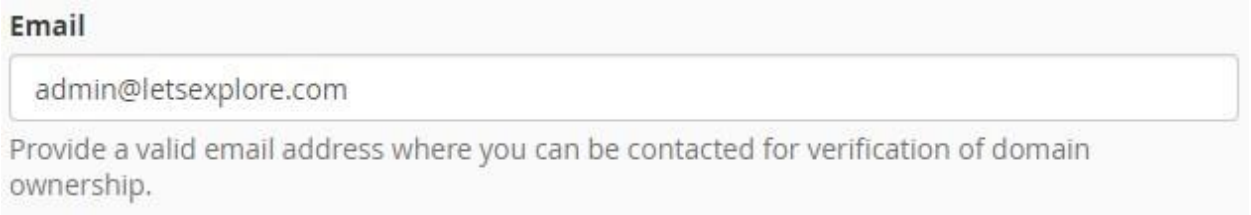


Note: One thing you should know that, if you are applying for a DV, Wildcard or Multi-domain certificate, your company information will not be shown even if it is legally registered. You must apply for an OV or EV certificate to make your company information visible to users.

7. **Company Division**: Provide the division or group (if your company is categorized and to which division the website belongs to you are currently applying) of your company if applicable. If not, then just type in **NA**.



8. **Email**: Enter your email address. But you can leave this field empty as the email is of no use in the CSR generating step.

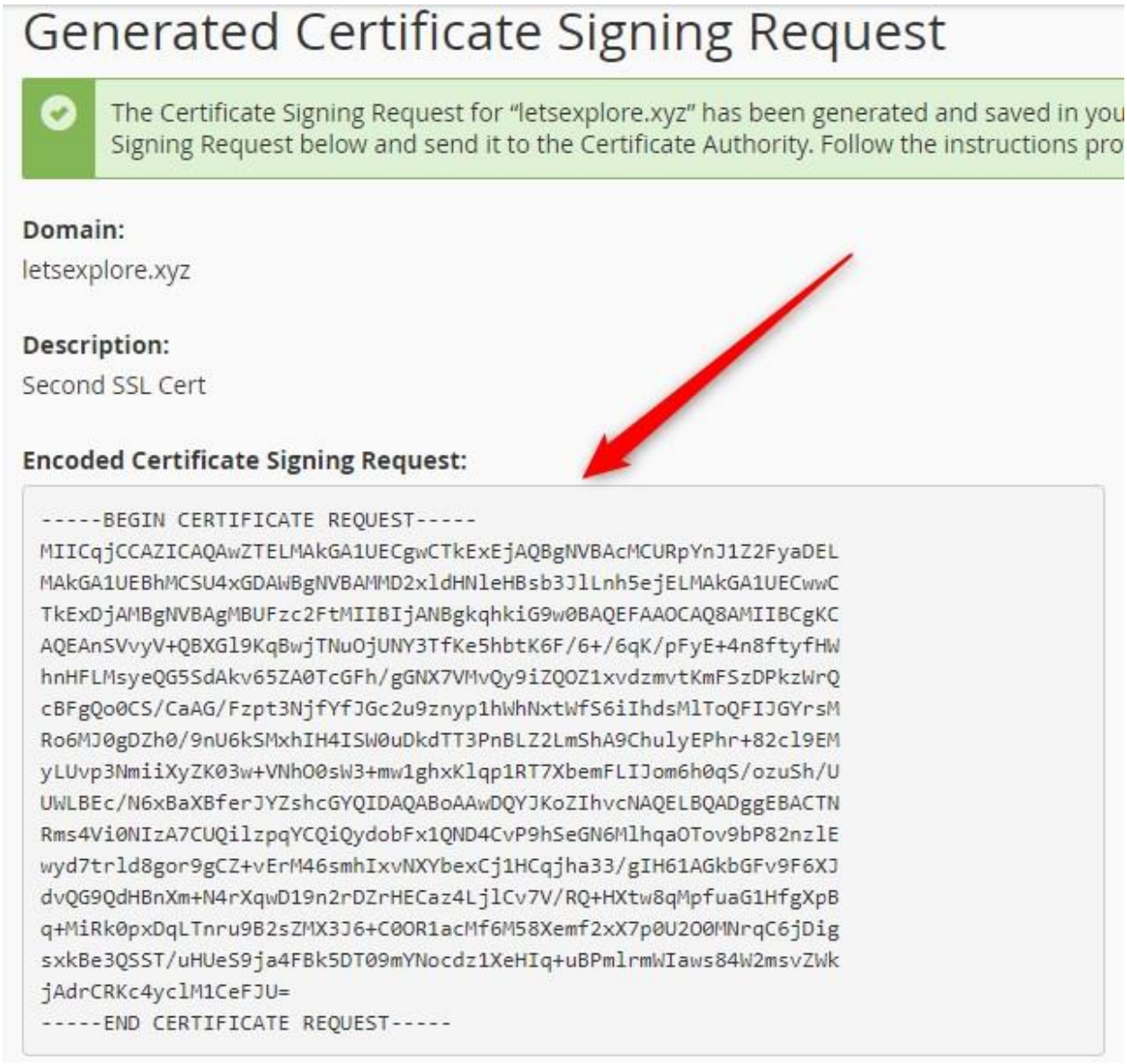


9. **Passphrase**: Enter a passphrase if your CA requires this for verification purposes but most of the times you don't require any passphrase, you can leave this field empty.

10. **Description**: Add a description for easy navigation, especially if you have multiple CSRs. It can be anything like *My DV Certificate CSR, My Wildcard Certificate CSR* etc.

11. After completing the all of the steps above, click on the **Generate** button.

Yay! You've just finished generating your CSR code.



Copy the entire encoded CSR code (you don't need the decoded version of the CSR for the activation process) from **-----BEGIN CERTIFICATE REQUEST----- to -----END CERTIFICATE REQUEST-----** and back it up somewhere on your PC.

Next, scroll down a little and copy the entire encoded Private Key and paste it somewhere on your PC. You'll need this Private Key during SSL certificate installation process. Without a Private Key, SSL installation is not possible.

Right after you finished generating your CSR code, it's time to send the certificate signing request to the CA to activate the certificate.

For the activation procedure…

Follow this step:

How to Activate an SSL Certificate

The SSL certificate activation process will be different based on the which web hosting service you are using or from which CA you are purchasing the digital certificate. But basically, the activation process will be almost same, only the UI will slightly be different.

If you've purchased the SSL certificate from your hosting provider, then it can be found under the SSL section of your web hosting account dashboard.

By taking common credentials into account, the certificate issuing authority generally asks to put the following information to activate or issue the security certificate for your website.

- **Certificate Name or Domain Name:** Enter your domain name

- **CSR Code:** Copy & paste the CSR code you generated

- **DCV Method**: Domain Control Validation or DCV is used to verify that the application of SSL certificate for that domain is valid and is controlled by yourself.

  There are three types of DCV method. They are namely; *Email, HTTP-based* and *DNS-based*.

  As a DCV method, you should select the email verification method, since this is the most convenient method to verify the ownership of a particular domain.

  As an *approver email*, it can only be possible to select a generic email (i.e. admin@yourdomain.com, mail@yourdomain.com etcetera). It can also be possible to approve via the email showing

on whois information by the registrar.

The rest of the two methods (i.e. HTTP-based & DNS-based) could be a bit cumbersome and confusing, especially for the newbie users.

Just go with the email verification method. It's the easiest & hassle-free method.

- **Admin Email**: This is the email address to which the website certificate will be sent along with the intermediate & root certificate details. This email doesn't have to be neither generic nor whois information validated. You are free to type in any email address you want.

After submitting all of the above details, the CA will send a verification email to the **Approver Email**.

Click on the verification link to complete the DCV (Domain Control Validation) process. And shortly after then, the CA will send the issued certificate to the **Admin Email** address.

Your website certificate will be shown in the email and they will also attach the SSL certificate in a ZIP file along with the CA bundle.

Download it and back it up in several places like your local computer as well as in the cloud.

Note: The *CA bundle* is a collection of root and intermediate certificates to let browsers verify that the certificate is valid & genuine.

Now, here's how you'll install it using cPanel:

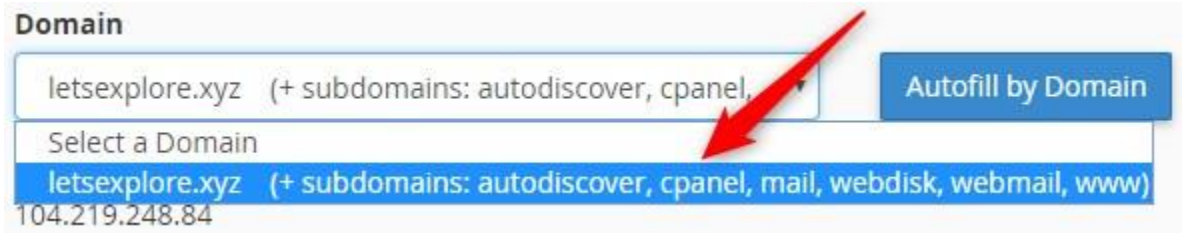
How to Install an SSL Certificate in cPanel

Log in to your cPanel dashboard.

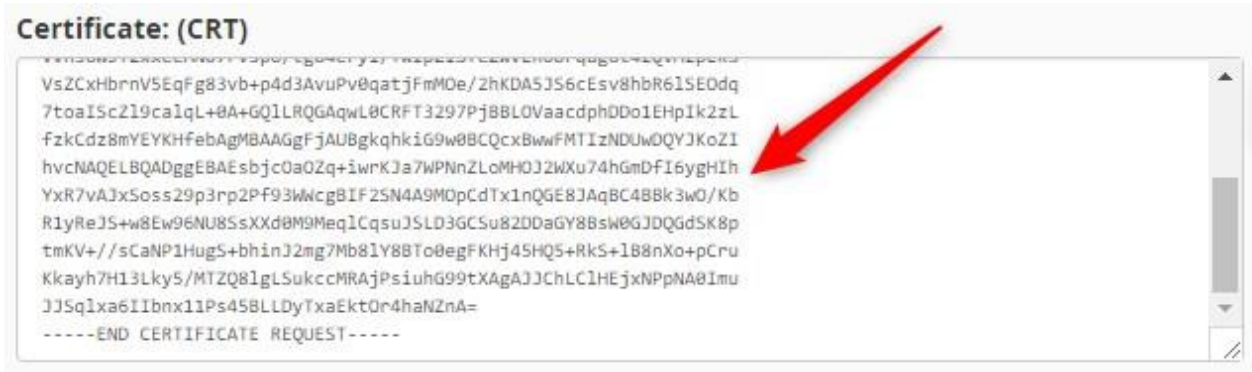
Go to the **Security** section and click on **SSL/TLS** option.

Under the **Install and Manage SSL for your site (HTTPS)**, click on **Manage SSL sites**.

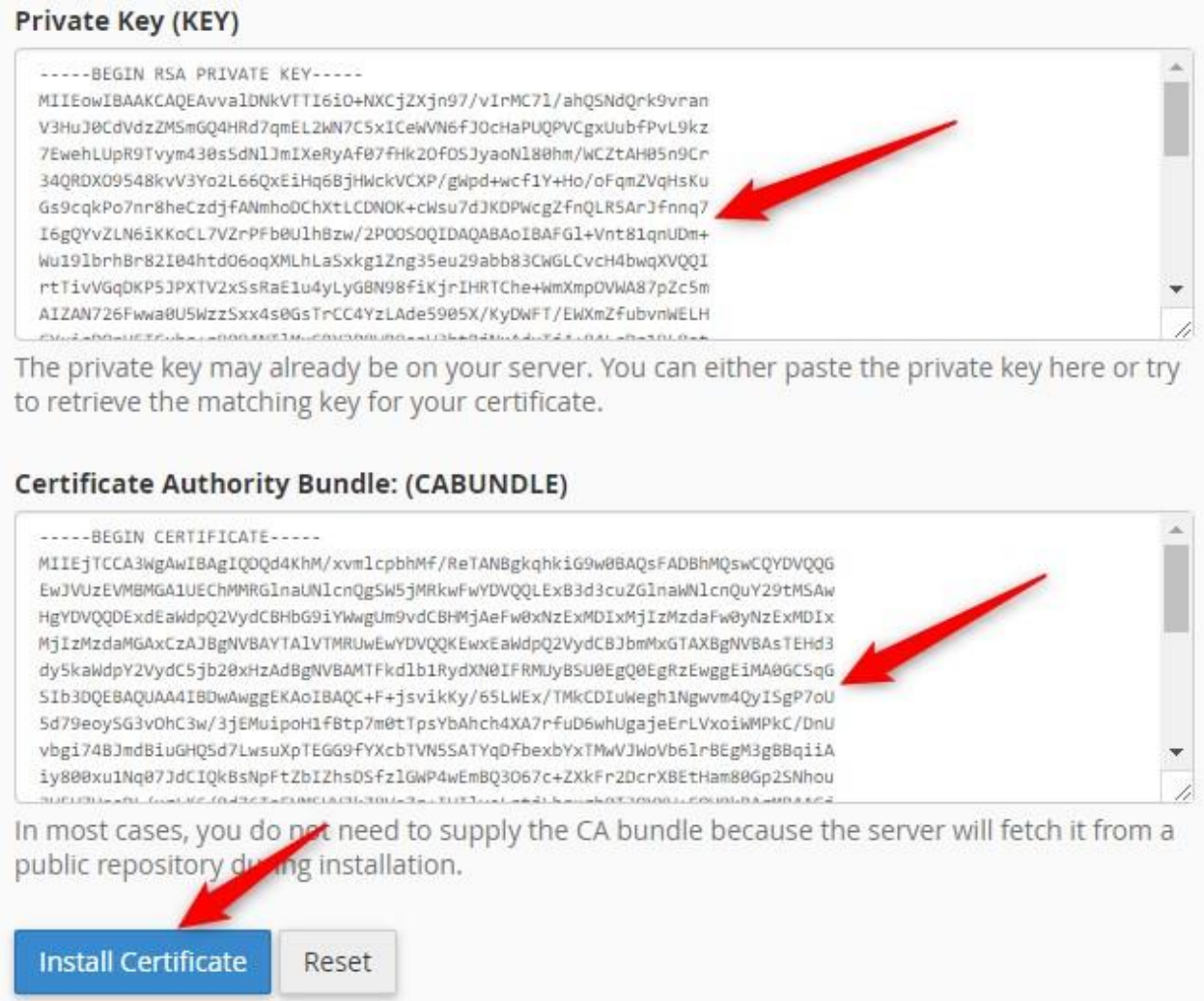
From the **Domain** drop-down menu, select the domain name on which you'd like to install the SSL certificate.



Copy & Paste your website's certificate code in the **Certificate** box.



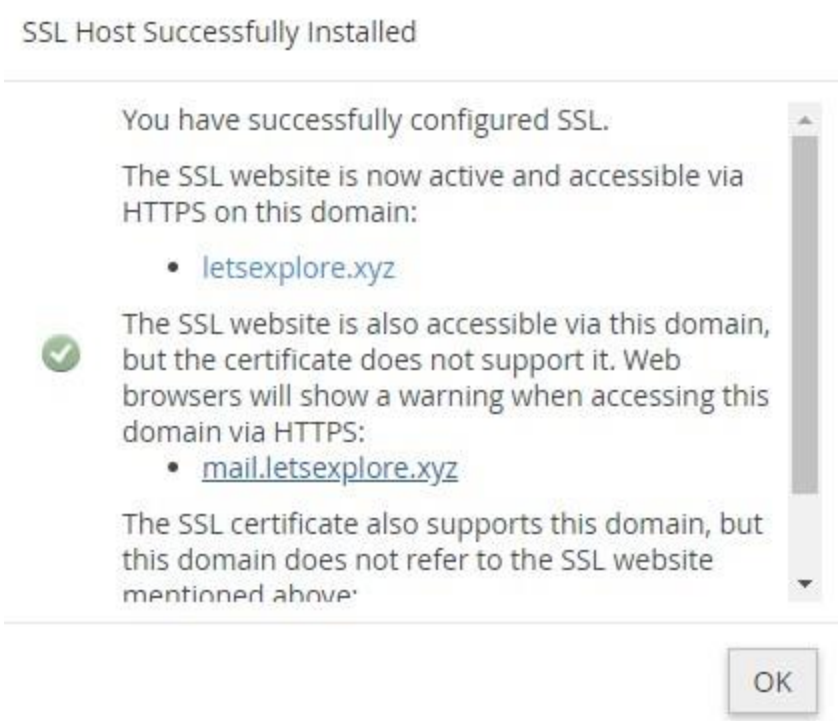
Click the **Autofill by Domain** option and the server will fetch the private key and CA bundle into the respective boxes.



In case a problem occurs, then you'll need to manually enter these encrypted codes in the boxes.

Now, click on **Install Certificate**.

Wait for a few seconds, and you'll be prompted with a successful SSL installation pop-up message.



After the successful installation, make sure that all of the website URLs are running via HTTPS without any issues.

If you haven't read my fairly detailed post about how to tackle common SSL or HTTPS issues on WordPress (like redirection & mixed content), you can read that article by following this link in case you need it.

Get in Touch with Us