Securing Your Site with SSL

Web Security · https://umw.domains/guides/securing-your-site-with-ssl/

An SSL certificate is a way to show users of your site that you've taken steps to make sure their personal information is safe. Increasingly, visitors are becoming reluctant to visit websites without them because of warnings from their browsers that a site may be unsafe.

By default Domain of One's Own installs an SSL certificate on your domain. It will be important that you install any application at **https** in order to utilize the functionality of the SSL certificate.

Why do you need to secure your site?

For many reasons, such as the increasing amount of data stored online and the rise of online shopping, it's become necessary to create a more secure way to transfer sensitive information around the web, such as credit card details or identifiable personal information.

How can I tell if a site is already secure?

You may recognize web addresses that start like this:

http://www.example.com

The http part stands for **Hypertext Transfer Protocol**, and for a long time, it's been the standard way for computers to transfer information to/from a server (the physical place in the world where the website in question is hosted).

Now, many websites will use **Secure Hypertext Transfer Protocol**, or https as in this example:

https://www.example.com

This lets you know a site has been verified by an independent authority and is who it claims to be. Even if you don't see the https in your browser, you may see a green tick or a lock next to the URL letting you know the site you're on is using a secure connection.

You can achieve this for your site too by installing a secure layer on your site called a **Secure Sockets Layer** or (SSL certificate).

What is an SSL certificate?

Essentially, an SSL is a security upgrade for your site. Once your site is verified by a “Certificate Authority” and issued with an SSL certificate, any computer around the world is able to create a secure connection with your server which no one else can intercept.

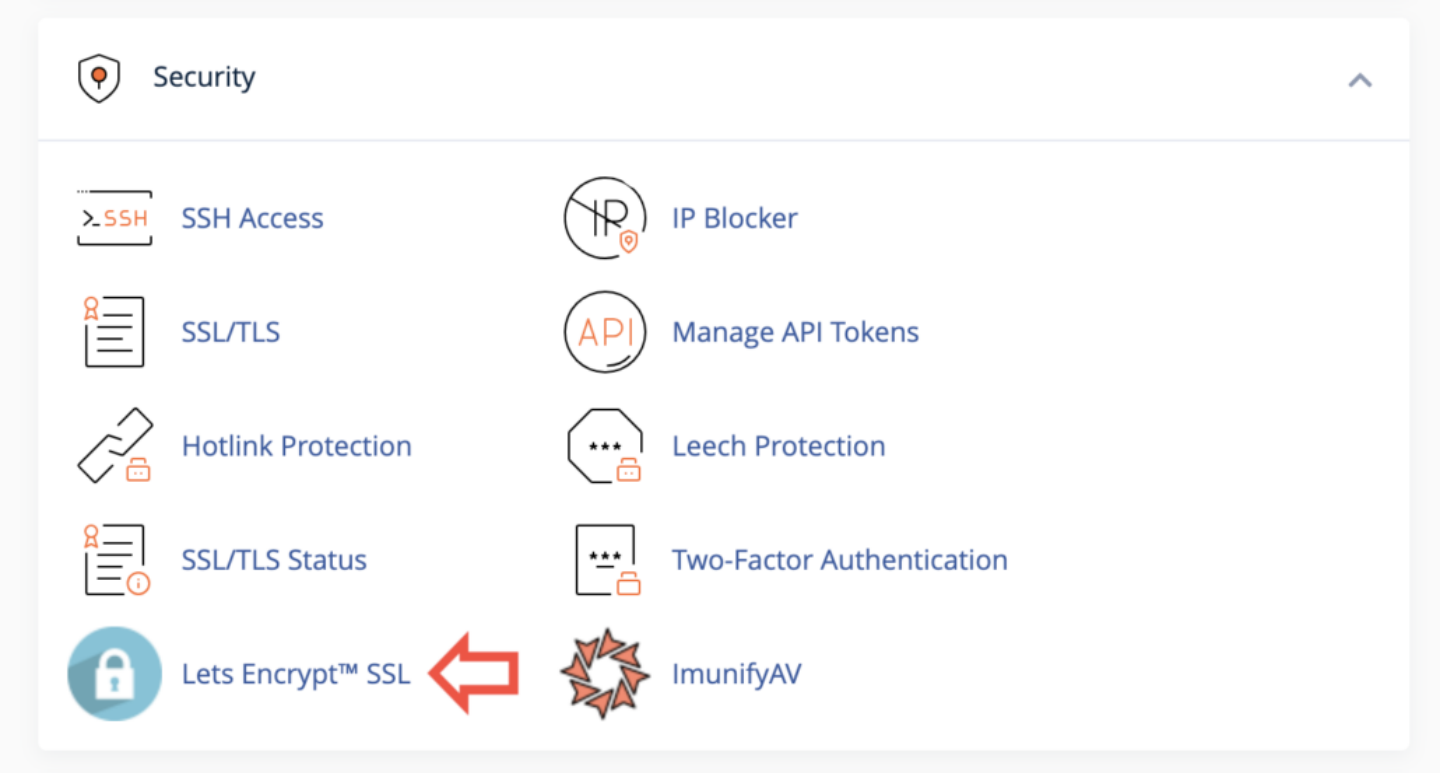
An SSL is a bit like having a “Blue Tick” on Twitter- it means your site has been verified by a third party.

By default Domain of One's Own installs an SSL certificate, but you need to take active steps to make sure your site is using it. For most applications, this means making sure when prompted to install the application at the https version of the URL.

How to add an SSL certificate to your site

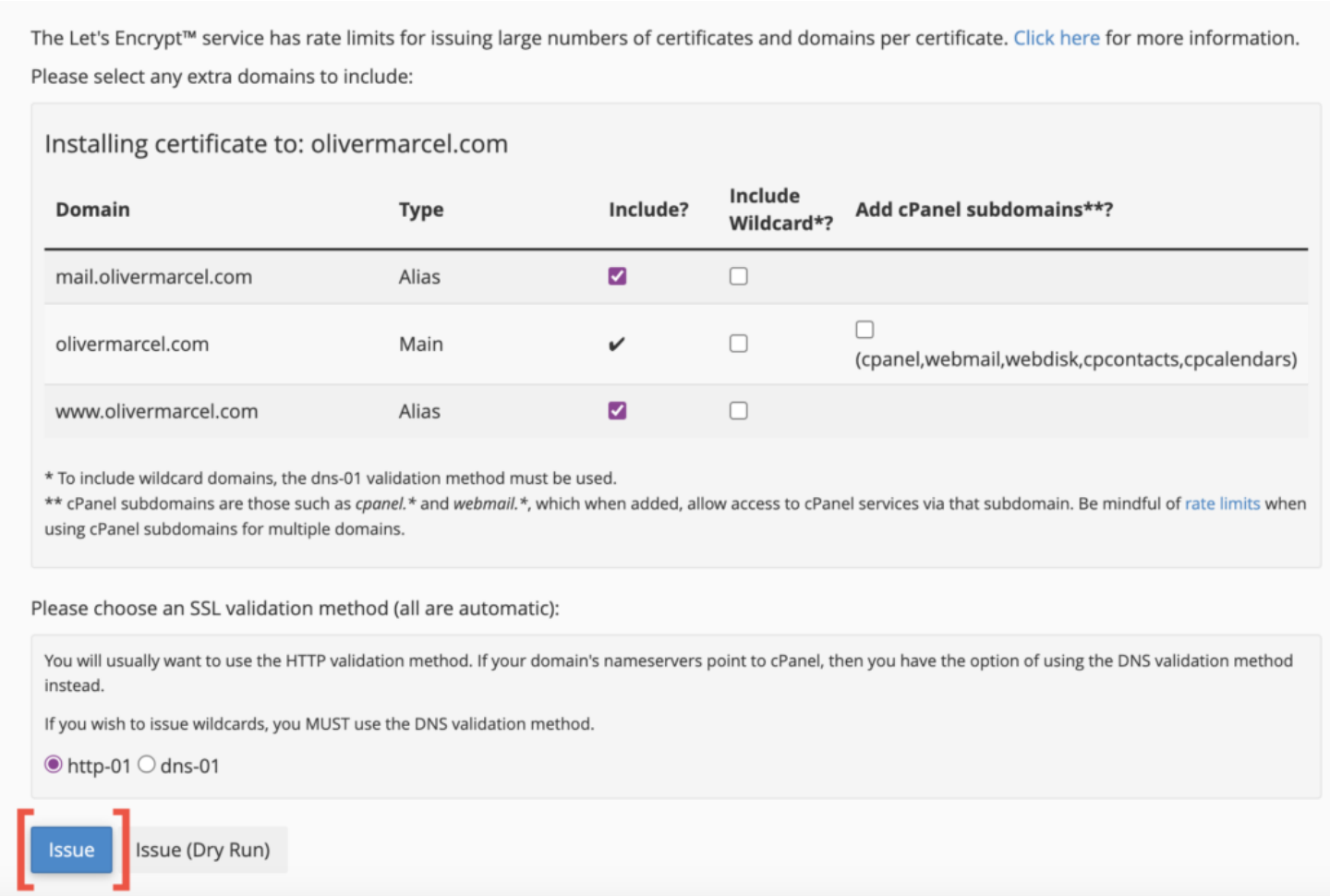
If you'd like to manually add an SSL certificate to your site we recommend using Lets Encrypt SSL.

1. On your cPanel dashboard, click on **Let’s Encrypt SSL** in the **Security** section



2. In the *Issue a new Certificate* section, locate the site you'd like to secure and click the blue **+Issue** button.

3. On the next screen, leave the default settings as they are and click **Issue**.

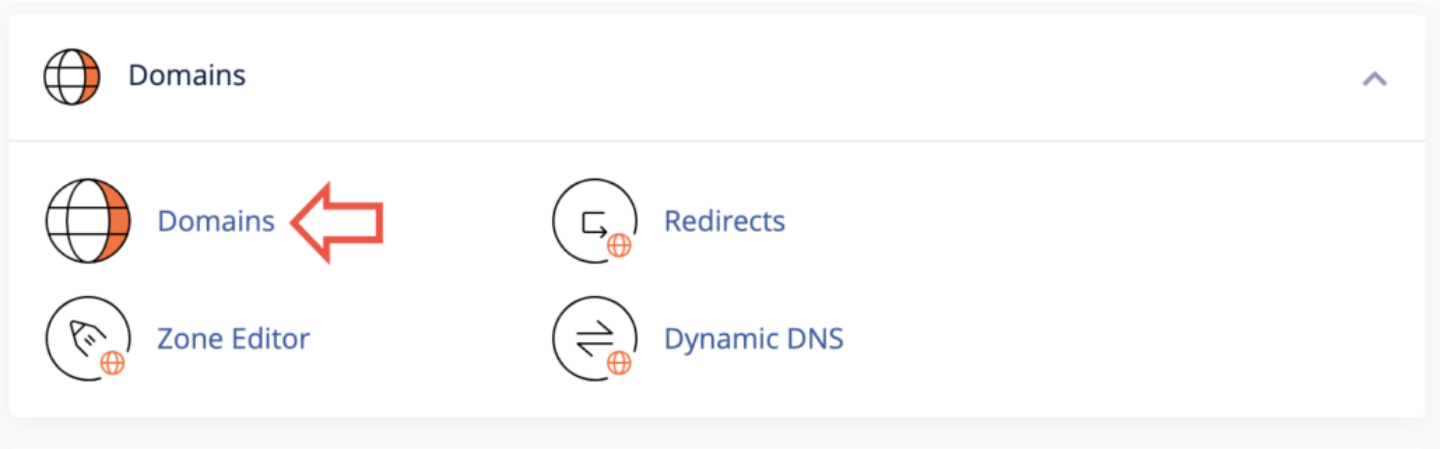


The process is now complete, but it may take 30 minutes or so for the changes to take effect. After this time, visit your site in a browser and look for either the https in the URL or a secured site symbol (such as a lock icon or a green tick) to the left of the URL.

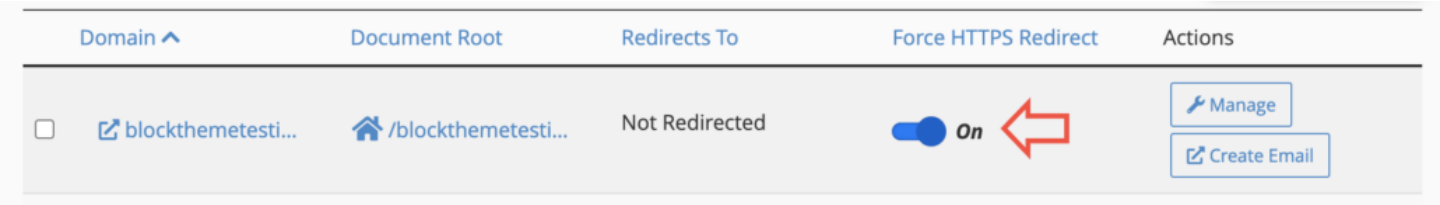
Forcing browsers to use HTTPS

If you're still seeing the HTTP protocol being used (or no secured site symbol next to the URL) when you visit your site, you may need to return to cPanel and force browsers to use your new SSL certificate.

1. In cPanel, click on the **Domains** tool in the Domains section



2. Make sure the “Force HTTPS Redirect” toggle is switched to **On**



This content is adapted from the Coventry.Domains DoOO Support by Coventry.Domains which is licensed under CC BY-NC 4.0

Reviewed by Abby Firestone 06/25/26