



Getting Started

To enable HTTPS on your website, you need to get a certificate (a type of file) from a Certificate Authority (CA). Let's Encrypt is a CA. In order to get a certificate for your website's domain from Let's Encrypt, you have to demonstrate control over the domain. With Let's Encrypt, you do this using software that uses the [ACME protocol](#), which typically runs on your web host.

To figure out what method will work best for you, you will need to know whether you have [shell access](#) (also known as SSH access) to your web host. If you manage your website entirely through a control panel like [cPanel](#), [Plesk](#), or [WordPress](#), there's a good chance you don't have shell access. You can ask your hosting provider to be sure.

With Shell Access

We recommend that most people with shell access use the [Certbot](#) ACME client. It can automate certificate issuance and installation with no downtime. It also has expert modes for people who don't want autoconfiguration. It's easy to use, works on many operating systems, and has great documentation. [Visit the Certbot site](#) to get customized instructions for your operating system and web server.

If [Certbot](#) does not meet your needs, or you'd like to try something else, there are [many more ACME clients to choose from](#). Once you've chosen ACME client software, see the documentation for that client to proceed.

If you're experimenting with different ACME clients, use our [staging environment](#) to avoid hitting [rate limits](#).

Without Shell Access

The best way to use Let's Encrypt without shell access is by using built-in support from your hosting provider. If your hosting provider offers Let's Encrypt support, they can request a free certificate on your behalf, install it, and keep it up-to-date automatically. For some hosting providers, this is a configuration setting you need to turn on. Other providers automatically request and install certificates for all their customers.

[Check our list of hosting providers](#) to see if yours is on it. If so, follow their documentation to set up your Let's Encrypt certificate.

If your hosting provider does not support Let's Encrypt, you can contact them to request support. We do our best to make it very easy to add Let's Encrypt support, and providers are often happy to hear suggestions from customers!

If your hosting provider doesn't want to integrate Let's Encrypt, but does support uploading custom certificates, you can install Certbot on your own computer and use it in [manual mode](#). In manual mode, you upload a specific file to your website to prove your control. Certbot will then retrieve a certificate that you can upload to your hosting provider. We don't recommend this option because it is time-consuming and you will need to repeat it several times per year as your certificate expires. For most people it is better to request Let's Encrypt support from your hosting provider, or switch providers if they do not plan to implement it.

Getting Help

If you have questions about selecting an ACME client, or about using a particular client, or anything else related to Let's Encrypt, please try our [helpful community forums](#).

Support a more secure and privacy-respecting Web.

Donate



authority brought to you by the non-profit Internet Security Research Group (ISRG).

View our [privacy policy](#).

View our [trademark policy](#).

1 Letterman Drive, Suite D4700, San Francisco, CA 94129

Linux Foundation is a registered trademark of The Linux Foundation. Linux is a registered trademark of Linus Torvalds.