**How to Install an SSL Certificate**

In This Guide

**Introduction**

[**Gather Requirements**](https://sucuri.net/guides/how-to-install-ssl-certificate/#gr)

[**1.1 – Types of Certificates**](https://sucuri.net/guides/how-to-install-ssl-certificate/#tosc)

[**1.2 – Commercial vs. Free**](https://sucuri.net/guides/how-to-install-ssl-certificate/#cvfsc)

[**1.3 – SSL in the Cloud**](https://sucuri.net/guides/how-to-install-ssl-certificate/#sitc)

[**1.4 – What You Will Need**](https://sucuri.net/guides/how-to-install-ssl-certificate/#wywntgafsc)[**Create Certificate**](https://sucuri.net/guides/how-to-install-ssl-certificate/#cc)

[**2.1- Overview of Steps**](https://sucuri.net/guides/how-to-install-ssl-certificate/#oos)

[**2.2- Install Certbot Client**](https://sucuri.net/guides/how-to-install-ssl-certificate/#icc)

[**2.3- Generate Certificate**](https://sucuri.net/guides/how-to-install-ssl-certificate/#gsc)

[**2.4- Automate Renewal**](https://sucuri.net/guides/how-to-install-ssl-certificate/#ar)

[**Final Steps**](https://sucuri.net/guides/how-to-install-ssl-certificate/#cc)

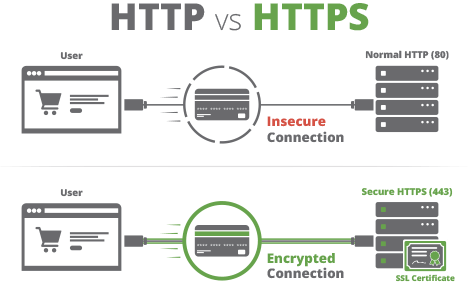
[**3.1- Force HTTPS**](https://sucuri.net/guides/how-to-install-ssl-certificate/#fh)

[**3.2- Check Mixed Content**](https://sucuri.net/guides/how-to-install-ssl-certificate/#cfmcw)

[**3.3- Search Engine Optimization**](https://sucuri.net/guides/how-to-install-ssl-certificate/#seo)

[**3.4- Website Security Caveat**](https://sucuri.net/guides/how-to-install-ssl-certificate/#wsc)

[**Additional Resources**](https://sucuri.net/guides/how-to-install-ssl-certificate/#adrs)



**How to Install an SSL Certificate**

With an SSL certificate, your website can use the HTTPS protocol to securely transfer information from point A to B. This is crucial when transferring sensitive information like credit card data on checkout pages and personally identifiable information (PII) on login and contact forms.

In addition to security benefits, websites with SSL encryption get better rankings on Google and improved performance through the use of HTTP/2. It’s also important to understand that SSL does not protect your website — rather, it protects the data that is sent through your website.

This guide is designed to show beginners and intermediate users how to deploy a free SSL certificate from Let’s Encrypt on their self-hosted websites.

**Step 1**

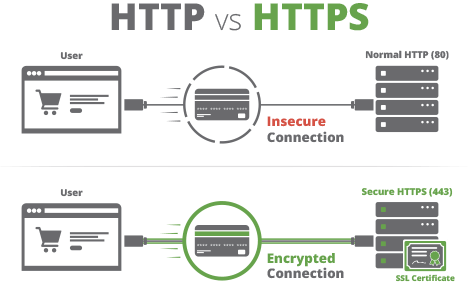
**Gather Requirements**

It is now easier than ever to use HTTPS on your website. Beginners should start by having a conversation with their hosting company about the options they offer.

There are a few easy ways to add SSL to your website:

1. Some hosts offer free SSL, including one-click SSL options (i.e. SiteGround, WPEngine).
2. Many hosts offer paid SSL and will implement the certificates for you (i.e. GoDaddy).
3. Intermediate users can generate their own free SSL certificate (i.e. Certbot / Let’s Encrypt).

Regardless of the type of certificate you choose, the encryption and level of security is the same.



**Get Help with SSL & Security**

Want to have an SSL certificate and website security? We’ve got you covered.

**1.1 – Types of SSL Certificates**

Some visitors recognize the additional authenticity and trust offered extended validation (EV) and organization validated (OV) certificates due to their rigorous validation process.

There are three types of certificates to be familiar with:

* Domain Validated (DV)

DV certificates only need the certificate authority to verify that the user requesting the certificate owns and administers the domain. Visitors will see a lock icon in their address bar, but no specific information about the owner.

* Organization Validated (OV)

OV certificates require a certificate authority to confirm the business making the request is registered and legitimate. When visitors click the green lock icon in their browser, the business name is listed.

* Extended Validation (EV)

EV certificates require even more documentation for the certificate authority to validate the organization. Visitors will see the name of the business inside the address bar (in addition to clicking the lock icon); however, most updated browsers no longer display the EV visual indicator.

**1.2 – Commercial vs. Free SSL Certificates**

It’s important to understand the difference between commercial and free certificates.

* Commercial (paid) SSL certificates

These are a decent option for many website owners. Paying a certificate authority (or your hosting company) will often give you the benefits of technical support. The encryption level is the same as with free SSL certificates. The key differentiator will come in the level of support you get with your certificate.

* Free SSL certificates

These are being spearheaded by the [Let’s Encrypt](https://sucuri.net/guides/how-to-install-ssl-certificate/%22) initiative – an open collaboration between a number of global organizations focused on making SSL certificates accessible to all website owners.

**Note**

Many hosts offer specific instructions on how to deploy free SSL certificates. Check with your host’s support channels and articles for more information before following this guide.

**1.3 – SSL in the Cloud**

You can also get the benefits of SSL certificates through cloud providers, such as content delivery networks (CDNs) and [website application firewalls (WAFs)](https://sucuri.net/website-firewall/) solutions like the one from Sucuri, who offer it at no additional charge.

These services are a proxy between the visitor and your website. By changing your domain records to point to their servers, they can cache your content to [make your website faster](https://sucuri.net/website-performance/) and filter out malicious traffic. This also means that the browser recognizes which server IPs are connected to your domain, allowing for the use of DV certificates.

These providers can also work with your own SSL certificate. If you are a Sucuri customer, you can contact our technical support team for information and assistance.

**Note**

If you are implementing an SSL certificate through your host, you may want to skip ahead to Step 3: Important Final Steps.

**1.4 – Getting a Free SSL Certificate**

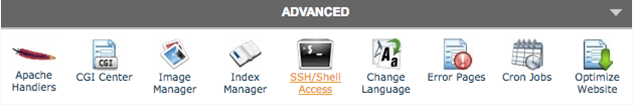
The following guide works best if you have a dedicated IP for your site (through a VPS or dedicated server). If you’re on a shared platform, talk to your host about deploying Let’s Encrypt; a number of hosts have automated the process of deploying a free SSL for shared hosting accounts. It is possible to use server name indication (SNI) with one server IP address and generate certificates for all sites on the server.

The rest of this guide will assume you have full access and control of your web server.

You will need the following information about your server:

* IP address
* Server username (with admin or sudo privileges)
* User password (or preferably SSH key authentication)
* Software (i.e. Apache, nginx, IIS)
* Operating system and version number (i.e. Debian 7, Ubuntu 16.04, etc.)

SSH Access Through cPanel



You can contact your host to obtain any missing information.

**Step 2**

**Generate Certificate**

Now that you have all the required information, you can connect to your server and install a tool that will generate an SSL certificate.

From your computer, you need a way to log into your server and send SSH commands. If you are on a Mac, you can use Terminal (built-in application) and on Windows you can download PuTTY. Some hosts also offer a web interface for running commands on your server.

**Note**

The instructions will vary depending on your server software and system. Some systems do not support Certbot, but you can find a list of other reputable clients that should work with your server environment.

**2.1 – Overview of Steps**

Here is a quick overview of how you can get a free SSL certificate from Let’s Encrypt using the Certbot tool.

Overview of steps to use Certbot:

1. Connect to your server over SSH using the IP address, username, and password.
2. Visit the [Certbot website](https://certbot.eff.org/) and choose your server operating system and software.
3. Follow the instructions given for your server to do the next steps.
4. Run any commands listed to install dependencies.
5. Run the commands listed to install Certbot.
6. Run the commands listed to generate the certificate.
7. Provide an email address when prompted.
8. Agree to the terms when prompted.
9. Run the commands listed to test renewals under Automating Renewal.
10. Set up a cron or systemd job on your server to automate the renewal process

The following images and animations illustrate the entire process for a server using Apache on Ubuntu 16.04.

**Sucuri Customers**

Manually removing malicious code from your website files can be extremely hazardous to the health of your website. Never perform any actions without a backup. If you’re unsure, please seek assistance from a professional.

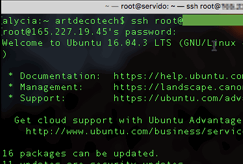
**2.2 – Install Certbot Client**

Using the instructions provided for your server, install any dependencies and the Certbot tool. The following images are an example of what you can expect.

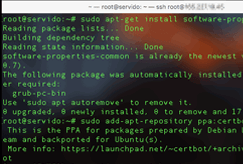
Get Instructions for Your Server from the Certbot Website



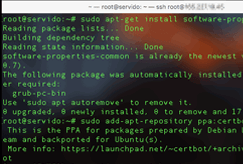
Connect to Your Server Over SSH (GIF)



Install Dependencies (if required) (GIF)



Install Certbot (GIF)



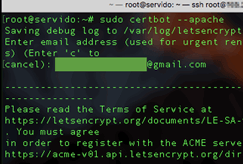
**Note**

If you are getting permission errors, check with your host to ensure your user has permissions to run administrative commands (i.e. sudo).

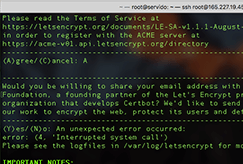
**2.3 – Generate SSL Certificate**

Continuing with the same set of instructions, the **Get Started** section will provide the commands needed to create the SSL certificate for your website. The following images are an example of what you can expect.

Run Certbot (GIF)



Agree to the Terms



Make a Secure Backup

After generating the certificate the Important Notes shows the location of your Certbot configuration directory. This contains your account credentials, certificate, and private keys.

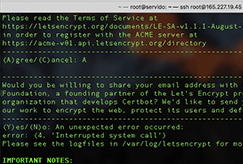
You should navigate to this location on your server and download a backup. If you aren’t sure how to do this, you can follow our post on [how to make backups over the command line](https://blog.sucuri.net/2017/08/website-backups-using-command-line-tools.html).

**2.4 – Automate Renewal**

Now you have an active SSL certificate on your site! Your certificate will expire, however. Let’s Encrypt certificates are only valid for 90 days. You can automate this process so you don’t have to remember to manually renew the certificate.

It’s recommended to set the cron or systemd job to renew the certificate twice a day. Before you begin, note the location of your Certbot configuration directory from the previous step.

Set Up SSL Certificate Renewal via Cron Job



To schedule the cron job that renews the SSL certificate:

1. Connect to your server.
2. Run the command *crontab -e*
3. If prompted, choose a text editor (i.e. nano)
4. Enter the following command, taking care to replace the location with the one provided when you generated the certificate:

52 0,12 \* \* \* root /var/log/letsencrypt/certbot-auto renew --quiet

1. Open your website to verify it is operational

**Note**

Some server configurations may need to run additional commands to load the new certs.

You can view the [full documentation on Certbot renewals](https://certbot.eff.org/docs/using.html#renewal) for more information.

These charitable organizations are working to help make the internet a safer place for everyone. While these tools are free, you can donate to help support both Let’s Encrypt and Certbot.

1. <https://letsencrypt.org/donate/>
2. <https://supporters.eff.org/donate/support-work-on-certbot>

We’ve outlined instructions below for how to manually install a certificate (free or paid) using a hosting control panel such as Plesk or cPanel

How to install via the Plesk control panel:

1. Generate a CSR login to the **Plesk admin** control panel.
2. In the Websites and Domains section for the domain name you want to use, click **SSL/TLS Certificates**.
3. Click **Add SSL Certificate**.
4. Enter a **Certificate name**, complete the fields in the **Settings** section, and then click **Request**.
5. Click the name of the certificate you added to Plesk.

Your certificate signing request displays in the **CSR** section.

How to upload your certificate:

1. Login to the **Plesk admin** control panel.
2. In the Websites and Domains section for the domain name you want to use, click **SSL/TLS Certificates**.
3. Use the **Upload the certificate files** section to upload the certificate files from your local machine, and then click **Send Files**.

How to activate your certificate:

1. Go to the **Websites & Domains** tab of the Plesk admin control panel.
2. In the section for the domain name you want to use, click **Hosting Settings**.
3. In the **Security** section, select **SSL support**.
4. Select the **Certificate** you created, and then click **OK**.

How to generate a CSR:

1. Log into your cPanel admin
2. From the cPanel home page, go to Security section, and then click SSL/TLS
3. Under Certificate Signing Requests (CSR), click Generate, view, or delete SSL certificate signing requests.
4. Complete the fields in the Generate a New Certificate Signing Request (CSR) section.
5. At the bottom of the form, click the Generate button.
6. On the new page, your CSR will display in the Encoded Certificate Signing Request section. You’ll need to make a copy of the CSR to request an SSL certificate.

How to install the certificate:

1. Launch cPanel admin.
2. In the Security section, click SSL/TLS.
3. Under Certificates (CRT), click Generate, view, upload, or delete SSL certificates.
4. Use the Upload Certificate section to upload the primary certificate (.crt file with randomized name) from your local machine and click Upload Certificate.
5. On the new page, click Go Back.
6. Scroll down to the bottom of the SSL Certificates page and click Return to SSL Manager.
7. Under Install and Manage SSL for your site (HTTPS), click Manage SSL Sites.
8. Scroll down to the Install an SSL Website and click Browse Certificates.
9. Select the certificate that you want to activate and click Use Certificate. This will auto-fill the fields for the certificate.
10. Scroll down to the bottom of the page and click Install Certificate.
11. On the Successfully Installed pop up, click OK

[Back to Top](https://sucuri.net/guides/how-to-install-ssl-certificate/#intro)

**Step 3**

**Final Steps**

While HTTPS is now an option on your site, the HTTP version of your site can still be accessed. Ideally, you should force all visitors (including search engines) to see the HTTPS version of your site. You should also take steps to fix mixed content warnings and update any proxy-based cloud services (such as firewalls and CDNs) to work with your new SSL certificate.

**3.1 – Force HTTPS**

To force visitors to access your site only over HTTPS, you can edit your **.htaccess** or **web.config** file depending on your operating system and configuration. You can find this in the root of your site, and you may need to show hidden files to find it. Make sure to backup your control files before making any changes.

There are other methods for Apache, such as using your [virtual host file](https://www.namecheap.com/support/knowledgebase/article.aspx/9821/38/redirect-to-https-on-apache). If you use an IIS server you can follow instructions to use the URL [Rewrite Module](https://blogs.technet.microsoft.com/dawiese/2016/06/07/redirect-from-http-to-https-using-the-iis-url-rewrite-module/) and nginx servers can use the [**nginx** configuration file](https://www.bjornjohansen.no/redirect-to-https-with-nginx).

Copy this directive into the .htaccess file to redirect HTTP visitors to the HTTPS version of your site:

Code Snippet – Add into .htaccess file

1. RewriteEngine On
2. RewriteCond %{HTTPS} off
3. RewriteCond %{HTTP\_HOST} ^(www\.)?domain\.com$ [NC]
4. RewriteRule ^(.\*)$ https://www.domain.com/$1 [L,R=301]

**Caution**

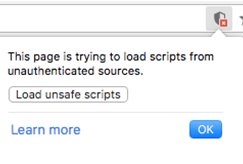
Editing the .htaccess file can cause issues with more sites with complex structures. The rewrite below works best for websites on a dedicated server or VPS running Apache. You need to replace domain with your domain name for the sample code to work.

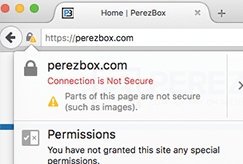
**3.2 – Check for Mixed Content Warnings**

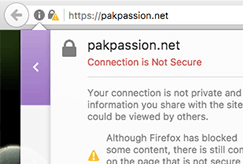
While your site is now available on HTTPS, you might still have resources linked to your website that load over HTTP. This includes things like images, videos, and external resources.

Browsers will block this content as “unsafe”, which can also cause broken functionality of your site and security warnings in browsers.

Examples of “Unsafe” Warnings:







You can use the same SSH access that you used to generate the certificate to run a command and find any files that reference http:// directly.

To find resources loading over HTTP, run the following command:

grep -r "http://"

This will list all files to investigate in your server or CMS. Simply change all resource URLs from **http://** to **https://** or to a relative path.

You should also query your database or manually look through posts and pages for HTTP content. There are plugins and extensions available that can automate the process of rewriting URLS using HTTP to HTTPS (i.e. [Really Simple SSL](https://wordpress.org/plugins/really-simple-ssl/) for WordPress).

If the HTTP resource is stored on your own website, we recommend using the relative directory and filename as follows.

Absolute Path:

<img src="https://example.com/images/pic.jpg">

Relative Path:

<img src="/images/pic.jpg">

**Resources That Can Cause Mixed Content Warnings:**

* Web fonts
* Iframe content
* JavaScript includes
* CSS stylesheets
* Image embeds
* Video embeds
* Audio embeds

**Caution**

* If your website loads external resources, changing links to HTTPS could break the functionality. To avoid this, make sure the resource is available over HTTPS before changing the URL in your code. You can access the URL with HTTPS in a browser to verify.
* If you run into issues, you can attempt to download the external content and host it on your own server to ensure it loads over HTTPS. Always test in a development environment for scripts and other content that could perform differently.

**3.3 – Search Engine Optimization**

The last thing to prepare for is the potential negative impacts of using HTTPS. Following the steps below should help to minimize them.

Once configured, add and verify the new HTTPS site in [Google Search Console](https://www.google.com/webmasters/tools/). This will allow you to recrawl your site and submit a new XML sitemap with your HTTPS URLs.

For many SEO elements like “rel=canonical” and “open graph” tags, it is advisable to use an absolute URL, as these are read externally by social media sites and search engine crawlers.

It’s important to note that there will be a period of normalization after applying SSL, but in the end, it is a confirmed ranking signal according to Google.

Similarly, social sharing counters for older content will likely become invalid. This is because now there is a new URL starting with HTTPS rather than HTTP, and many tools count each as a separate URL with its own engagement metrics.

**SEO & Meta Elements To Check**

* rel=canonical
* rel=alternate
* rel=next & rel=prev
* hreflang
* Open Graph tags
* Schema.org
* Structured Data
* Sitemaps
* Internal Linking

**3.4 – Website Security Caveat**

HTTPS is a great thing for the internet as a whole, it helps keep communication secret between users and the websites they visit. SSL secures data in transit but does not secure the website itself.

Website security is much more comprehensive than HTTPS/SSL alone. Think of HTTPS/SSL as one of many security controls to consider when thinking about your website’s security. Deploying HTTPS/SSL on your website does little to ensure your visitors are safe if you do not take to establish a secure hosting environment, such as using secure passwords and updating all website software.

We encourage website owners to think about website security holistically and consider leveraging a [website security platform](https://sucuri.net/website-security-platform/signup/) that offers a complete suite of security controls: protection, detection, monitoring, and incident response. If you have more questions on how platforms work or questions about this article please direct them to our team at [info@sucuri.net](mailto:info@sucuri.net).

[Back to Top](https://sucuri.net/guides/how-to-install-ssl-certificate/#intro)

**Get Help With SSL**

Want to have an SSL certificate and website security? We’ve got you covered.

**Contact Us**

[info@sucuri.net](mailto:info@sucuri.net)

[Submit Ticket](https://support.sucuri.net/support/?new" \t "_blank)

[Live Chat](https://sucuri.net/live-chat/" \t "_blank)

* 1-888-873-0817

Products

* [Website Firewall](https://sucuri.net/website-firewall/)
* [Website Security Platform](https://sucuri.net/website-security-platform/)
* [Website Backups](https://sucuri.net/website-backups/)
* [WordPress Security](https://sucuri.net/wordpress-security/)
* [Enterprise Services](https://sucuri.net/custom/enterprise/)

Solutions

* [DDoS Protection](https://sucuri.net/website-hack-protection/)
* [Malware Detection](https://sucuri.net/malware-detection-scanning/)
* [Malware Removal](https://sucuri.net/website-malware-removal/)
* [Malware Prevention](https://sucuri.net/website-hack-protection/)
* [Blacklist Removal](https://sucuri.net/website-security-platform/blocklist-removal-and-repair/)

Support

* [Knowledge Base](https://docs.sucuri.net/)
* [SiteCheck](https://sitecheck.sucuri.net/)
* [Research Labs](https://labs.sucuri.net/)
* [Report Abuse](https://abuse.sucuri.net/)
* [Status Report](https://status.sucuri.net/)

Company

* [About Sucuri](https://sucuri.net/company/)
* [Contact](https://sucuri.net/company/contact-us/)
* [Blog](https://blog.sucuri.net/)
* [Employment](https://sucuri.net/company/employment/)
* [Testimonials](https://sucuri.net/customers/)
* [Terms of Use](https://sucuri.net/terms/)
* [Privacy Policy](https://sucuri.net/privacy/)
* [Do Not Sell My Personal Information](https://sucuri.net/cookies/)
* [Frequently Asked Questions](https://sucuri.net/faq/)

© 2022 GoDaddy Mediatemple, Inc., d/b/a Sucuri. All rights reserved.

[1–888–873–0817](tel:+1–888–873–0817)

LIVE CHAT

How can we help?

