

Set up SSL certificates for your store

In this tutorial, we will help you to set-up SSL on your own domain, with CraftingStore. We already offer free SSL on all sub-domains (e.g. example.craftingstore.net).

Note: You are required to have a premium plan with us, to generate SSL certificates for your webstore, you can find our pricing here ([click](#)).

SSL on our premium platform;

1. Set-up your domain from the CraftingStore dashboard, please fill in your domain at; Dashboard -> Settings -> Domain, and click update. Make sure the subdomain box is empty.
2. Make sure to configure your domain correctly ([tutorial](#)) and go to the next step if your store is working without HTTPs.
2. Go to the "SSL" tab, located at; Dashboard -> Settings -> HTTPs.
3. Click the button to start the process, issuing the certificate will take a few seconds and will happen in the background.
4. Now your store has HTTPS, you can even enable the HTTP -> HTTPS redirect from the CraftingStore dashboard if you want to force HTTPS. (Dashboard -> Settings -> Domain). Please validate that your store does work over HTTPS before enabling this.

SSL on free stores;

While we only offer SSL for premium stores, you will still have the ability to use CloudFlare's free SSL to get it to work.

Our servers are all listening on port 80 (HTTP) and 443 (HTTPS), to comply with CloudFlare's requirements regarding their SSL, so it will work flawlessly.

1. Set-up your domain from the CraftingStore dashboard, please fill in your domain at; Dashboard -> Settings -> Domain, and click update. Make sure the subdomain box is empty.

2. Go to your CloudFlare DNS manager, and create a cname record for your (sub)domain of choice to "dns.craftingstore.net", and enable the orange cloud behind it.
3. Go to your crypto settings at CloudFlare, and look for "SSL". They offer a few options; Flexible, Full and Full (Strict).

We support Flexible & Full, using Full (Strict) won't work, read below to find out what the difference is.

Flexible: Only the traffic between the end user (your customer) and CloudFlare will be encrypted, everything from CloudFlare to CraftingStore will be sent in plain text (not recommended).

Full: Everything between the end user (your customer) and CloudFlare will be encrypted, and it will be re-encrypted and send to CraftingStore, so no plain text information will pass through the internet.

Full (Strict): This is the same as Full, but with one extra check.. it will check if the SSL certificate on the server (CraftingStore server) is valid, and signed by a CA (Certificate Authority) for your specific domain. But because we can't generate valid certificates for your domain (because we don't own it), we can't have any valid certificates on our side. This is not a problem, because everything is still fully encrypted.

If you require Full (Strict) for your own domain, you can also use CloudFlare's "Page Rules" to make your store use Full, and the website itself, Full (Strict), just keep in mind to have "store.example.com*" as URL match, or else only the store's homepage will function.

4. Your store will now serve over HTTPS, it might take CloudFlare some time to issue the certificate.
5. You can even enable the HTTP -> HTTPS redirect from the CraftingStore dashboard if you want to force HTTPS. (Dashboard -> Settings -> Domain).

That's all, if you have any questions, problems or issue with the system, please create a ticket with us, so we can sort it out.

Revision #4

Created Wed, Dec 5, 2018 9:06 AM by CraftingStore

Updated Fri, Jul 19, 2019 3:17 PM by CraftingStore