Overview

The best thing about SSL is it's simple to set up, and once it's done all you have to do is route people to use HTTPS instead of HTTP. If you try to access your site by putting https:// in front of your URLs right now, you'll get an error. That's because you haven't installed an SSL Certificate. But don't worry – we'll walk you through setting on up right now!

Setting up HTTPS on your website is very easy, just follow these 5 simple steps:

1. Host with a dedicated IP address
2. Buy a certificate
3. Activate the certificate
4. Install the certificate
5. Update your site to use HTTPS

Step 1: Host with a dedicated IP address

In order to provide the best security, SSL certificates require your website to have its own dedicated IP address. Lots of smaller web hosting plans put you on a shared IP where multiple other websites are using the same location. With a dedicated IP, you ensure that the traffic going to that IP address is only going to your website and no one else's.

An affordable host I recommend for a dedicated IP is StableHost. At this time it's under $6/month, but you can get it cheaper if you order for a full year. They're my host and I've been blown away with their support and performance. Oh, and here's a coupon for 40% off: expert40

If you don't have a plan with a dedicated IP you can ask your current web host to upgrade your account to have a dedicated IP address. There will probably be a charge for it – it could be one-time or monthly fees.

Step 2: Buy a Certificate

Next you'll need something that proves your website is your website – kind of like an ID Card for your site. This is accomplished by creating an SSL certificate. A certificate is simply a paragraph of letters and numbers that only your site knows, like a really long password. When people visit your site via HTTPS that password is checked, and if it matches, it automatically verifies that your website is who you say it is – and it encrypts everything flowing to and from it.

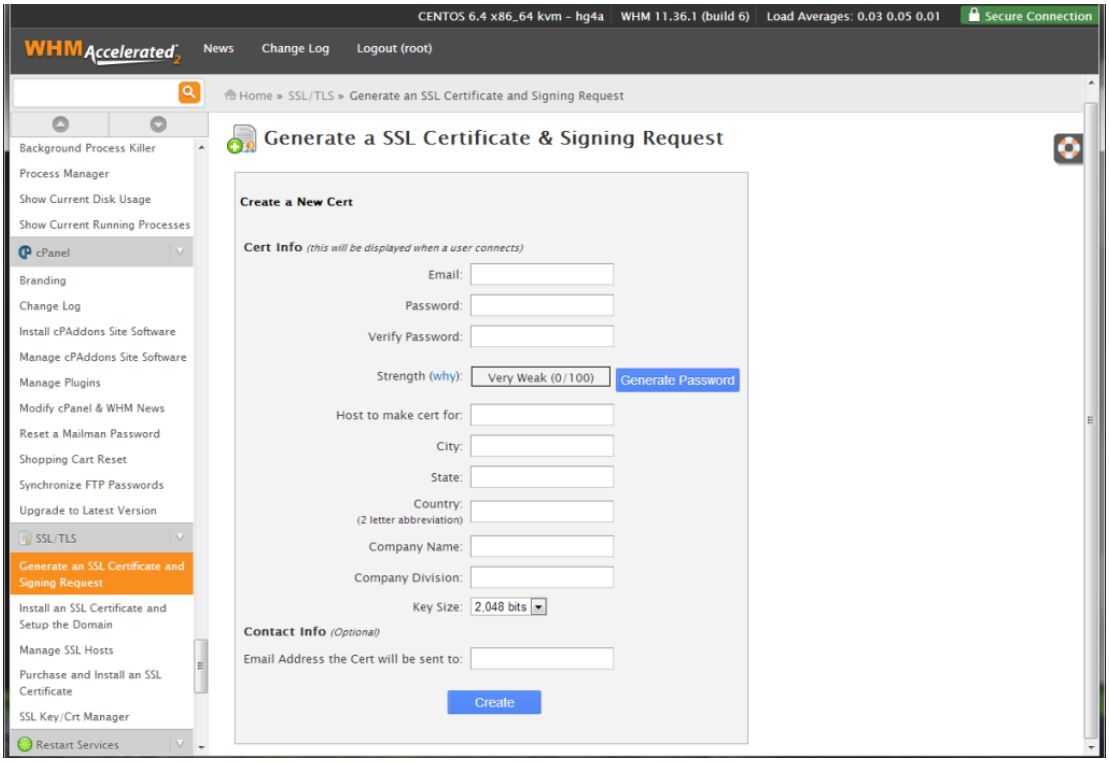
Technically this is something you can create yourself (called a 'self-signed cert'), but all popular browsers check with "Certificate Authorities" (CA's) which also have a copy of that long password and can vouch for you. In order to be recognized by these authorities, you must purchase a certificate through them.

NameCheap is where I buy my certificates. They have a few options, but the one that I find best is the GeoTrust QuickSSL. At this time it's $46 per year, and it comes with a site seal that you can place on your pages to show you're secure – which is good for getting your customers to trust you. You'll simply buy it now, and then set it up by activating and installing it in the next steps.

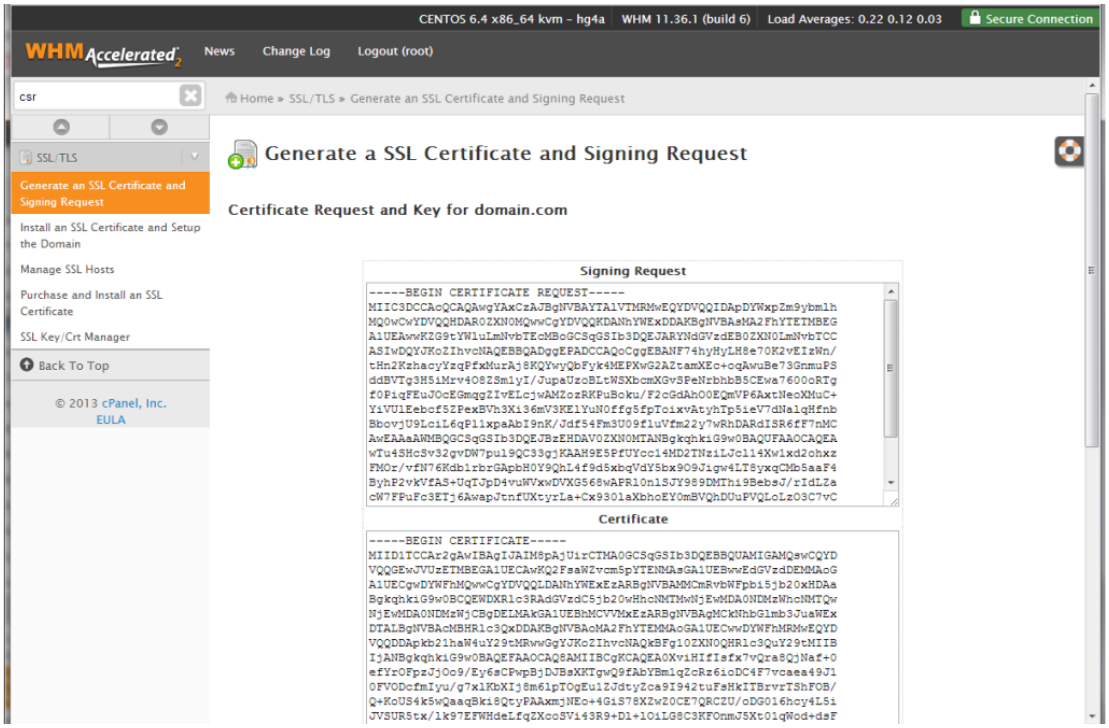
Step 3: Activate the certificate

Note: Your web host may do this step for you – check with them before proceeding. This can get complicated and if you can wait 1-2 days it may be best to let them do it.

If you're activating the certificate yourself, the next step is to generate a CSR. It's easiest to do this within your web hosting control panel – such as WHM or cPanel. Go to the SSL/TLS admin area and choose to "Generate an SSL certificate and Signing Request". Fill out the fields in the screen below:



"Host to make cert for" is your domain name, and the contact email can be blank. When you've filled it out, you'll see a screen like this:

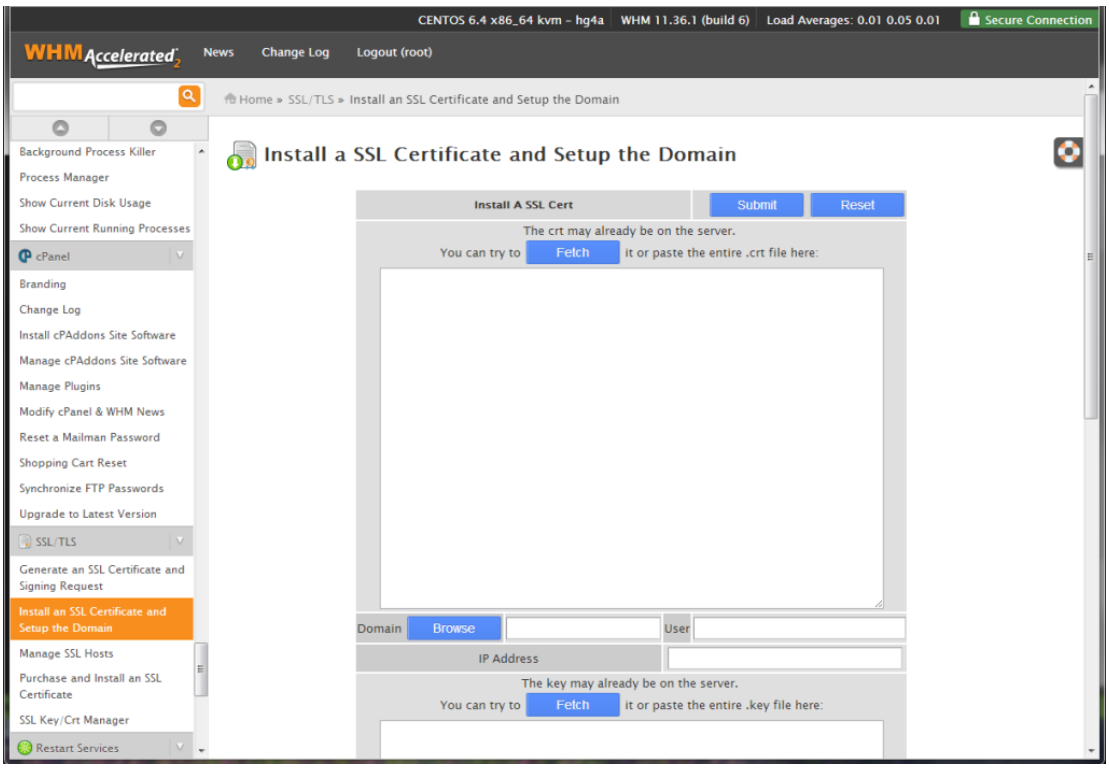


Copy the first block of text. You'll need this "CSR" to give to the SSL cert issuer so they can establish your identity. Login to your NameCheap account (or wherever you bought your certificate) and activate it. Paste your CSR and any other fields needed. It will ask you for an approver email. This is an email address that proves you own the domain, ie webmaster@domain.com. If it doesn't exist, you'll need to create it so you can get the email that contains the final certificate. Follow the steps and when you are done that email address should have received the cert as a .crt file.

Step 4: Install the certificate

Note: Your web host may also do this step for you too – check with them before proceeding. This can get complicated and if you can wait 1-2 days it may be best to let them do it.

If you're installing up the certificate yourself, this is the easiest step you'll ever do. You have the certificate in hand, all you need to do is paste it into your web host control panel. If you're using WHM.CPanel, click the "Install an SSL Certificate" from under the SSL/TLS menu.



Paste it into the first box and hit submit. That's it! Now try to access your site via https://www.domain.com – you should be secure!

Step 5: Update your site to use HTTPS

At this point if you go to https://yoursite.com you should see it load! Congrats, you've successfully installed SSL and enabled the HTTPS protocol! But your visitors aren't protected just yet, you need to make sure they're accessing your site through HTTPS!

Keep in mind that you typically only need to protect a few pages, such as your login or cart checkout. If you enable HTTPS on pages where the user isn't submitting sensitive data on there, it's just wasting encryption processing and slowing down the experience. Identify the target pages and perform one of the two methods below.