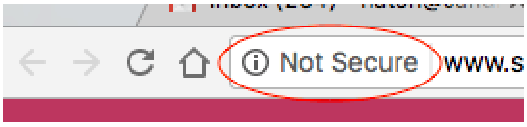
WordPress SSL: the Easy HTTP to HTTPS Guide

This WordPress HTTPS plugin guide shows you how to get the green "Secure" bar — the easy way.

Let's look at an SEO topic that's gotten increased coverage in the last six months due to a Google update in how Chrome displays the address bar: the **HTTP** to **HTTPS** site migration.

If you're in the digital world at all yourself, this isn't new — but I've found surprisingly little in the way of a clear, comprehensive, accurate guide to add an SSL certificate and migrate your website to "HTTPS." Especially given that WordPress plugins make this step-by-step installation work that anyone can do.



Not secure!

Throw in the fact that Google has been including HTTPS as a direct ranking factor since 2014, and there's really no reason not to do this if you're a small business, agency or blogging WordPress user.

First, a brief explanation of CloudFlare.

To switch your site to HTTPS, the WordPress steps below involve using the free **CloudFlare SSL certificate** for ease of use.

While CloudFlare may not improve site loading times, since it essentially acts as a host “intermediary” (traffic is routed for security through its global network of servers), it does improve overall *performance*:

- **SEO** (HTTPS is a Google ranking factor)

- **UX** (users see your site is secure)

- **Site security** (“HTTPS” gets you an SSL certificate)

Read more on CloudFlare if you’re interested in the benefits it offers your site.

If you have an ecommerce site in 2017, you probably already know this: you absolutely **must** be “HTTPS” secure if any of your customers’ information is private or sensitive in nature, like a billing credit card number.

Don’t want to deal with these steps yourself? You can always check with your hosting provider to see what services they provide for paid SSL certificates.

But this way is easy. And it’s free. ▯

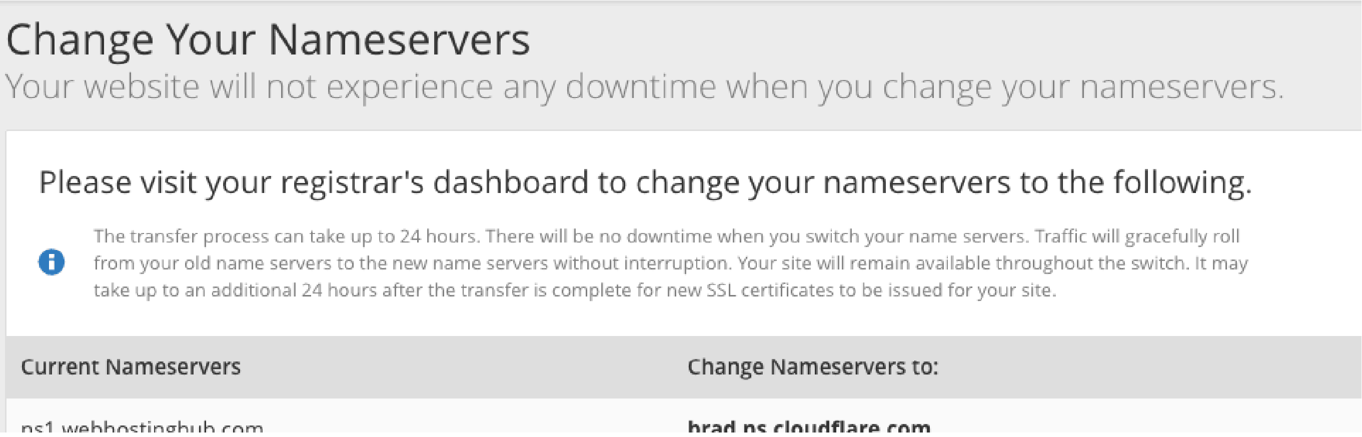
Using the CloudFlare plugin on WordPress, we *don’t* have to pay for an SSL certificate. We can do it for free. Yes, CloudFlare may not improve page speed. A caching plugin will. Just be sure to **check your caching plugin for any specific instructions regarding CloudFlare/CDNs**, like W3 Total Cache or WP Fastest Cache.

Ready to start? Let’s plug in HTTPS.

Step 1

Okay, on to the setup & install process.

First, sign up for CloudFlare and select the free plan. This takes less than a minute. Stop when you get to the “Change Your Nameservers” screen.



Change Your Nameservers

Your website will not experience any downtime when you change your nameservers.

Please visit your registrar's dashboard to change your nameservers to the following.

The transfer process can take up to 24 hours. There will be no downtime when you switch your name servers. Traffic will gracefully roll from your old name servers to the new name servers without interruption. Your site will remain available throughout the switch. It may take up to an additional 24 hours after the transfer is complete for new SSL certificates to be issued for your site.

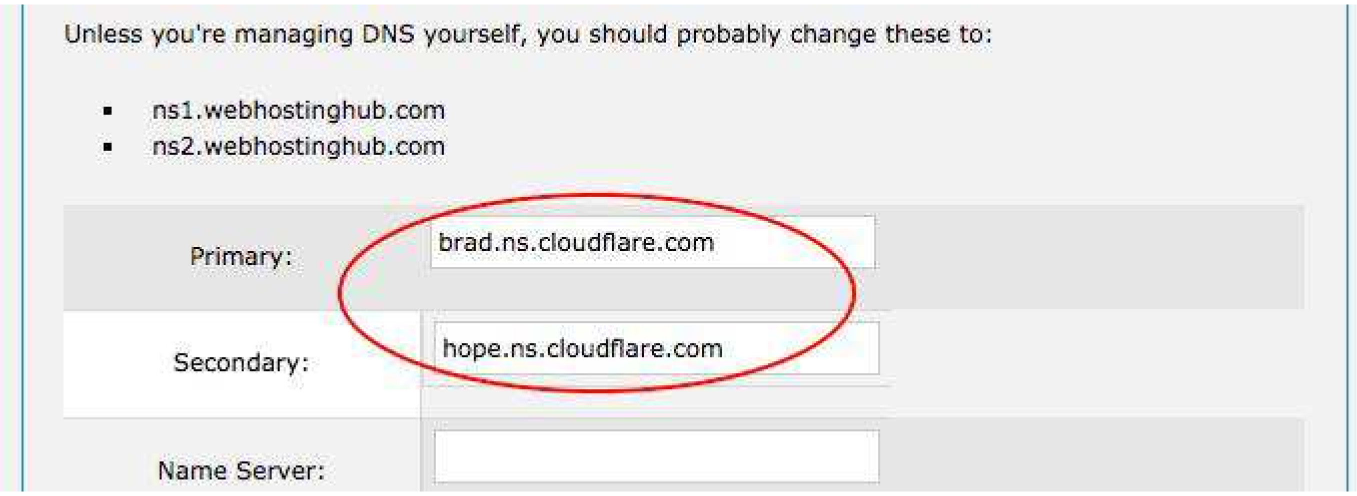
Current Nameservers	Change Nameservers to:
ns1.webhostinghub.com	brad.ns.cloudflare.com

Step 2

Log into your web hosting account, referencing your host's specific instructions to **change nameservers**. (They should have this documentation readily available online, so you should be able to find it with a quick search.)

Step 3

Copy and paste each new nameserver from the CloudFlare right column (screenshot above) to the respective form fields as directed by your hosting provider, and save the changes.



Unless you're managing DNS yourself, you should probably change these to:

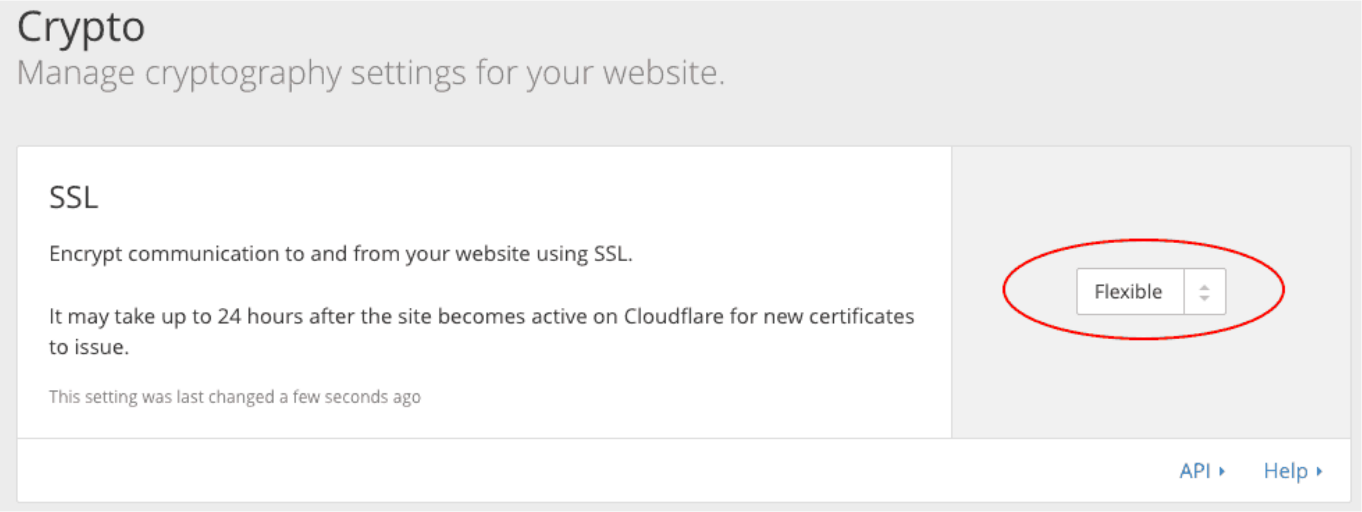
- ns1.webhostinghub.com
- ns2.webhostinghub.com

Primary:	brad.ns.cloudflare.com
Secondary:	hope.ns.cloudflare.com
Name Server:	

Step 4

Go back to CloudFlare, and select "Continue" on Change Your Nameservers. You'll then see the Overview screen with **Status: Pending**. It can take time for the nameserver switch to process, as indicated here.

Step 5



Crypto
Manage cryptography settings for your website.

SSL

Encrypt communication to and from your website using SSL.

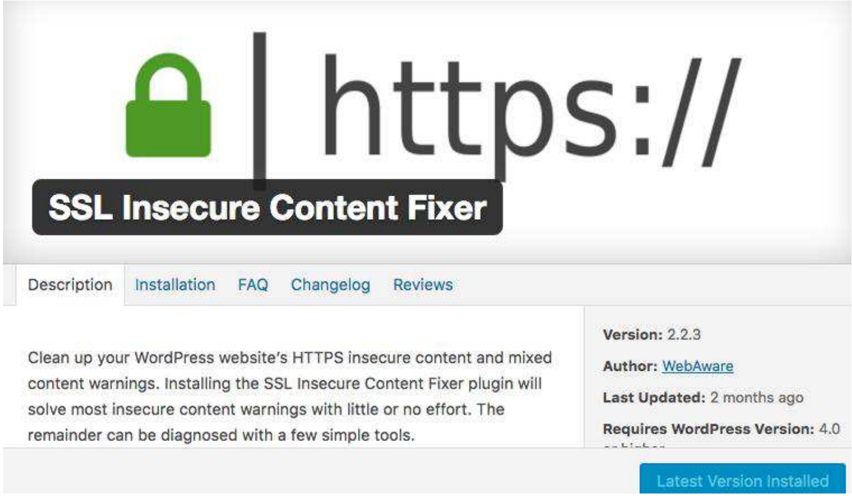
It may take up to 24 hours after the site becomes active on Cloudflare for new certificates to issue.

This setting was last changed a few seconds ago

Flexible

Click on "Crypto" and check that the SSL option is set to **Flexible**. (Cloudflare will tell you your SSL is ready by displaying a green "Active" box below it.)

Step 6



Clean up your WordPress website's HTTPS insecure content and mixed content warnings. Installing the SSL Insecure Content Fixer plugin will solve most insecure content warnings with little or no effort. The remainder can be diagnosed with a few simple tools.

Version: 2.2.3
Author: WebAware
Last Updated: 2 months ago
Requires WordPress Version: 4.0

While you're waiting, install these plugins in WordPress to assist you with making the HTTPS switch:

- CloudFlare
- CloudFlare Flexible SSL
- SSL Insecure Content Fixer

As a safety measure, I'd also recommend turning off any WordPress caching plugin you've got installed at this time, as well as JetPack and Yoast SEO (or other SEO plugin), just to avoid any potential conflicts with the HTTPS migration for the time being.

PRO TIPS: if you have ***Schema markup*** *in your HTML, now's also a good time to update any URL references to the "https" domain. If you've manually added a rel=canonical in Yoast, revise it to the "https" version before you turn the plugin off.*

Step 7

See the green **Status: Active** bar in CloudFlare>"Overview"?

In WordPress, activate the CloudFlare plugin, and enter your login email & API key (Overview) to sync.

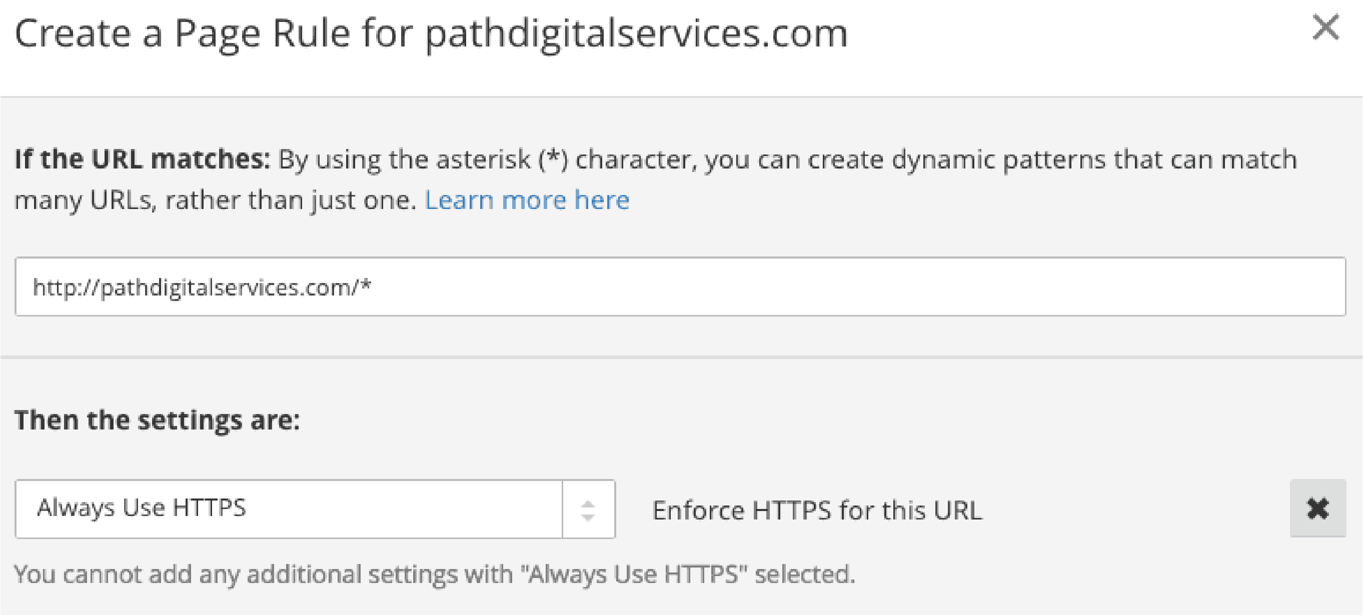
NOTE: if you've got another domain associated with the CloudFlare account already, you'll need to follow their ***separate instructions for API keys*** *(see "Global API Key" in the screenshot link).*

Then do these:

- Go to "Settings" in the plugin window to ensure Development Mode is set to "off" and "Automatic HTTPS Rewrites" is on. Click Update.
- Activate the CloudFlare Flexible SSL plugin
- Go to WordPress >Settings>General and keep this open in a browser tab

Step 8

Next, go back to CloudFlare and click "Page Rules." In URL pattern, enter your "http" domain name ending with /*.



Create a Page Rule for pathdigitalservices.com

If the URL matches: By using the asterisk (*) character, you can create dynamic patterns that can match many URLs, rather than just one. Learn more here

http://pathdigitalservices.com/*

Then the settings are:

Always Use HTTPS — Enforce HTTPS for this URL

You cannot add any additional settings with "Always Use HTTPS" selected.

Set "Always use HTTPs" in **Add a Setting** to On, and click Save and Deploy.

Step 9

Back in WordPress >Settings>General, change **Site Address** to "https". Save changes. You can keep your **WordPress Address** as-is; the CloudFlare page rule will automatically redirect your visitors to SSL for you.

Step 10

If you get logged out of WordPress, that's ok. Log back in and activate the SSL Insecure Content Fixer you installed in Step 8. Check that it's on the recommended settings.

Step 11

Then, check your live site to see that it's HTTPS secure, indicated by the "Secure" green address bar.

All good? Well done.

No luck? Some of your site content is still insecure. Try changing the setting from Simple to "Content" in **SSL Insecure Content Fixer**. Once you get the green address bar, you're ready to re-activate the plugins you turned off in Step 8.

Step 12

We’re not quite done yet — after you’ve successfully redirected your domain to HTTPS, there’s typically some basic migration clean-up needed.

You should check these, if applicable:

• **Robots.txt** (add “https” if needed to the sitemap listing in Yoast SEO>Tools>File Editor)
• **301 redirects** (check that existing 301’s direct to new “https” addresses to avoid redirect chains)
• **.XML sitemap** (check that your .XML sitemap lists the correct https addresses, re-installing plugin as needed)
• **Rel=canonical** (if you’re using the Chrome browser, you can go to View>Developer>View Source, then Edit>Find, and paste in rel=”canonical” to make sure the HTTP version of the site is not canonicalized)
• **Internal HTTP links:** you can also easily do a Find search on your homepage and linked pages to find “http” references to update.

Pro Tip: if you’ve got Simple Redirects + *Bulk Uploader add-on installed, you can easily bulk-update, clear and re-upload your 301’s in a .CSV.*

Step 13

Add your HTTPS site (both non-www and www versions), which Google considers separate, in Search Console, following their instructions for new domains. Then fill out the Change of Address form, also in Search Console.

Next, you can 1) check that there are no Robots.txt file errors (“Crawl”), 2) Resubmit sitemap, and 3) “Fetch as Google” and Request Indexing. As I’ve experienced, it can take time — days or even weeks — for the new “HTTPS” site to be fully indexed (although your homepage should be re-indexed within a day or two). Until then, expect to still see some “http” addresses show up in search results.

Now that you’ve done the above, see how your site performance improves overall through this relatively quick, free tutorial accessible to anyone with a WordPress site.