

How to Enable HSTS?

HTTP Strict Transport Security (HSTS) is a security mechanism that helps protect against attacks such as man-in-the-middle attacks by enforcing the use of secure connections (HTTPS) for a website or web portal. Enabling HSTS can help improve the security of your website and enhance the privacy of your users.

How to create Cloudflare Integration

Tutorial :


You can watch the Video or Continue reading the post.

<https://www.youtube.com/embed/UNpwQ70-CaQ>


Follow the steps to Enable HSTS.

Navigate to the SSL/TLS of Cloudflare (Use this link to view How to Navigate).

Click on the "**Enable HSTS**" button.

 SSL/TLS



Opportunistic Encryption allows browsers to benefit from the improved performance of HTTP/2 by letting them know that your site is available over an encrypted connection. Browsers will continue to show "http" in the address bar, not "https".



HTTP Strict Transport Security (HSTS)


Enforce web security policy for your website.

Status: On
Include subdomains: On
Preload: On



Enforce web security policy for your website.

Automatic HTTPS Rewrites helps fix mixed content by changing "http" to "https" for all resources or links on your web site that can be served with HTTPS.



Click on the "**understand**" button and click on the "**Next**" button.

←

HSTS

Acknowledgement

Configure

If you turn off Cloudflare's HTTPS while HSTS is enabled, and you don't have a valid SSL

- certificate on your origin server, your website will become inaccessible to visitors.

Note: Disabling Cloudflare's HTTP can be done in several ways: Grey clouding a subdomain in your DNS records, "Pausing" the Cloudflare service, or having a misconfigured custom SSL certificate through your Cloudflare dashboard (e.g., invalid SSL certificates, expired certificates, or mismatched host names).

If you need to disable HTTPS on your domain, you must first disable HSTS in your Cloudflare dashboard and wait for the max-age to lapse to guarantee that every browser is aware of this change before you can disable HTTPS. The average max-age is six months (you can set the max-age in the next step). **If you remove HTTPS before disabling HSTS your website will become inaccessible to visitors for up to the max-age or until you support HTTPS again.** Because disabling HTTPS on an HSTS enabled website can have these consequences, we strongly suggest that you have a committed HTTPS service in place before enabling this feature.

[More information about HSTS](#)

☐ I Understand

Cancel

Next

Click on the "**Save**" button.

← HSTS

Acknowledgement **Configure**

Max Age Header (max-age)
Specify the duration HSTS headers are cached in browsers

select ▼

Apply HSTS policy to subdomains (includeSubDomains)
Every domain below this will inherit the same HSTS headers ☒
Caution: If any of your subdomains do not support HTTPS, they will become inaccessible.

Preload
Permit browsers to preload HSTS configuration automatically ☒
Caution: Preload can make a website without HTTPS support completely inaccessible.

No-Sniff Header
Send the "X-Content-Type-Options: nosniff" header to prevent Internet Explorer and Google Chrome from MIME-sniffing away from the declared Content-Type. ☒

Previous Cancel **Save**

Here, you can see HSTS is enabled successfully.

Looking for web app Instructions?

Available at <https://kb.cloudpanzer.com/books/web-portal/page/how-to-enable-hstspending>

Revision #8

Created 27 December 2022 05:30:44 by Admin

Updated 2 September 2023 07:13:59 by Admin