interweb

Generated on 15/11/2026 00:16

KNOWLEDGE BASE · PUBLIC DOCUMENT

HSTS explained: forcing https for good, and the trap of switching it on too early

SSL & HTTPS

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1494	v2026.10.10	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1494

HSTS explained: forcing https for good, and the trap of switching it on too early

SSL & HTTPS Created on **October 10, 2026** 3 min read



The short answer: HSTS is an instruction your site gives the browser: “from now on, talk to me **only over https**, for X amount of time, do not even try http”. It closes the gap a plain redirect leaves open. But the browser **obeys even if you change your mind**, which is why you only switch it on when https is perfect everywhere.

What HSTS solves that a redirect does not

With an http to https redirect (see **how to redirect HTTP to HTTPS**), the **first** visit from someone who typed the address without https goes over http, and that is where, on somebody else’s Wi-Fi, an intruder can interfere before the redirect happens. With HSTS, after the first visit the browser no longer even tries http: it goes straight to https.

Before you switch it on, confirm this

Condition	Why
https works on every page, with no warning or mixed content	With HSTS on, the browser stops offering the “continue anyway” button. See **mixed content**.
The certificate renews itself	An expired certificate with HSTS is a wall, not a warning. See **when the certificate does not renew**.
Subdomains have https too	If you use the option that includes subdomains, an old subdomain with no certificate becomes unreachable.
You are not behind a service with a different SSL rule	If you use Cloudflare, its SSL mode and HSTS must be right there first: **switching on SSL at Cloudflare without breaking the site**.

How to switch it on, carefully

1. **Start with a short lifetime.** In the `.htaccess` file in the site root, add `Header always set Strict-Transport-Security "max-age=300"`. That is five minutes: if anything goes wrong, the browser forgets quickly.

2. **Browse the whole site,** signed in and signed out, in a private window. Look for warnings and pages that will not open.

3. **Raise it in stages:** a day, a week, and finally the usual value of a year (31536000 seconds). At each stage, wait and watch.

4. **Leave the subdomains option and the preload list for last,** and only if you are absolutely sure. The preload list puts your domain inside the browsers themselves, and getting off it takes months.

There is no undo button.
If you set HSTS for a year and then discover a subdomain has no https, the visitors who already received it cannot reach that subdomain until the time runs out, even if you fix everything on your side. That is why the first value is five minutes and not a year.

HSTS only applies after the **first** visit over https, and only in the browser that received it. It is a layered protection, to add to a redirect and a working certificate, not a replacement. The other security headers are in **security headers explained**.

NEED A HAND?

Not sure https is perfect across the whole site and subdomains? Ask us to check before you switch HSTS on.

Open a support ticket →

SEE ALSO

- **How to redirect HTTP to HTTPS with .htaccess** →
- **Mixed content after moving to HTTPS** →

- **Security headers explained**
- **SSL certificates**

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-AO-KB-1494 · v2026.10.10 · Generated on 15/11/2026 00:16