interweb

Generated on 15/11/2026 00:09

KNOWLEDGE BASE · PUBLIC DOCUMENT

Switching on SSL at Cloudflare without breaking the site

Cloudflare

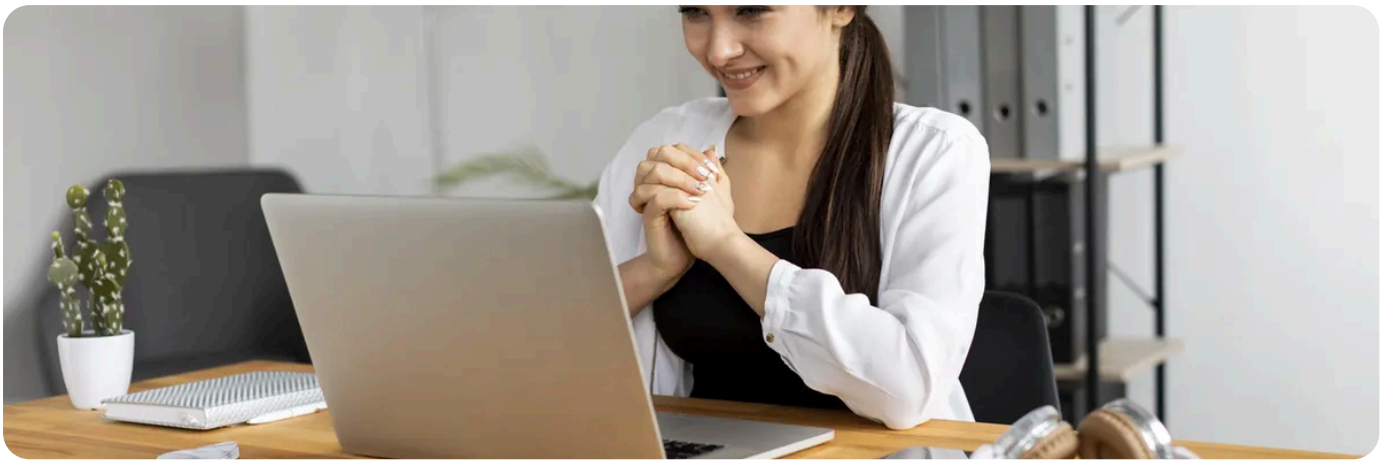
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-510	v2026.10.18	Angola · English

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/510

Switching on SSL at Cloudflare without breaking the site

Cloudflare · Created on **September 27, 2026** · Updated on **October 18, 2026** · 4 min read



This is the single most important setting Cloudflare has, and the easiest one to get wrong. The wrong value does not produce a warning: it produces a site that loads forever and a browser that gives up. Read this **before** you swap the nameservers.

> **On our hosting the right value is *Full (strict)*.**
> The value *Flexible* puts the site into an endless redirect loop. That is not an opinion or a preference: it follows from how our server is set up, and it is explained below.

There are two certificates, not one

With Cloudflare in front, the connection from visitor to site now has **two legs**, and each leg has its own certificate.

The leg	Which certificate it uses
Visitor to Cloudflare	**Their** certificate, issued automatically once the domain goes active. It is the padlock the visitor sees.
Cloudflare to our server	**Our** certificate, issued and renewed automatically on your account. This is the one the SSL mode decides to use or ignore.

The certificate at our end is real, issued by a recognised authority, and renews itself for as long as the account exists. That is why we can use the strictest mode: our end genuinely has something to answer with. On certificates in general, see **what an SSL certificate is** and **why it does not last 365 days**.

The four modes, and what each does

Mode	What it does on the leg to us
Off	No encryption at all. Not used.

Mode	What it does on the leg to us
Flexible	Cloudflare talks to us **unencrypted**, even though the visitor sees a padlock. This is what causes the endless loop. Not used here.
Full	Talks encrypted, but accepts any certificate, including an invalid one. A temporary stepping stone and nothing more.
Full (strict)	**The right value.** Talks encrypted and demands a valid certificate. Ours is.

Why Flexible produces an endless loop

The mechanics are simple and worth understanding, because they explain a symptom that looks impossible.

1. The visitor asks Cloudflare for the page over `https`, and their connection is encrypted.
2. On Flexible, Cloudflare fetches it from our server over `http`, unencrypted.
3. Our server sees an unencrypted request and does what it was told to do: redirect to `https`.
4. Cloudflare receives that redirect, asks again, and asks again **over http**, because that is what Flexible mode does.
5. It repeats until the browser gives up, with a message about too many redirects.

The redirect in step three can come from either of two places, and it is worth knowing which, because people switch one off and forget the other:

Where it comes from	Where you see it
The rule in the `.htaccess` file	If you wrote it, it is there. See **how to redirect HTTP to HTTPS with .htaccess**, which already carries this warning.
The cPanel switch	The **Domains** section of cPanel has an option that forces `https` without touching any file. Plenty of people forget they turned it on.

> **!** **The cure is not to switch the redirect off.**
> It is to set the mode to Full (strict). Switching the redirect off removes the loop but leaves the site serving pages unencrypted on the leg to us, which is worse than the problem.

The right order

1. **Confirm the site opens over `https` here**, before Cloudflare is in play. If it does, the certificate is issued and Full (strict) will work.
2. **Set the mode to Full (strict)** in the Cloudflare dashboard, in the SSL section.
3. **Only now** swap the nameservers, if you have not already. If you have, this is the first screen to open.
4. **Turn on *Always Use HTTPS*** at Cloudflare. With Full (strict), that option and the `.htaccess` rule coexist without a loop: the unencrypted request is corrected at the door and never travels the whole path.
5. **Test signed in and signed out**, in a private window, and click through three pages.

If Full (strict) fails, the cause is always at our end and always visible.
Either the certificate has not been issued for that name yet, or the name is not covered (a brand new subdomain, for instance). Take the record out of the proxy, wait for the certificate, and put it back. See **no padlock: the causes, in order**.

Two neighbouring options that cause trouble

Option	What to know first
HSTS	It tells browsers never to try `http` on that domain again, and they obey for however long you set, even after you switch the option off. **Do not turn it on until everything is settled**, subdomains included. Turning it on early turns a half-hour problem into a problem of weeks.
Cloudflare origin certificate	They offer a certificate to install on our server. It is not needed: ours issues itself. And it has a trap, because that certificate **is only trusted by Cloudflare**: the day you take the proxy off, the site shows a security warning to everybody.

With SSL settled, caching is next. For WordPress, see **cache rules for a WordPress site**; for everything else, **the ones worth having and the ones that cause trouble**.

NEED A HAND?

Site stuck in a redirect loop? Send us the address and the mode you have selected.

Open a support ticket →

SEE ALSO

- **SSL certificates** →
- **Hosting plans** →
- **Support Policy** →

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-510 · v2026.10.18 · Generated on 15/11/2026 00:09