

KNOWLEDGE BASE · PUBLIC DOCUMENT

Checking your site's HTTPS setup: certificate, chain, expiry and protocols

Security

CODE

RLX-INT-KB-5886

VERSION

v2026.10.15

COUNTRY · LANGUAGE

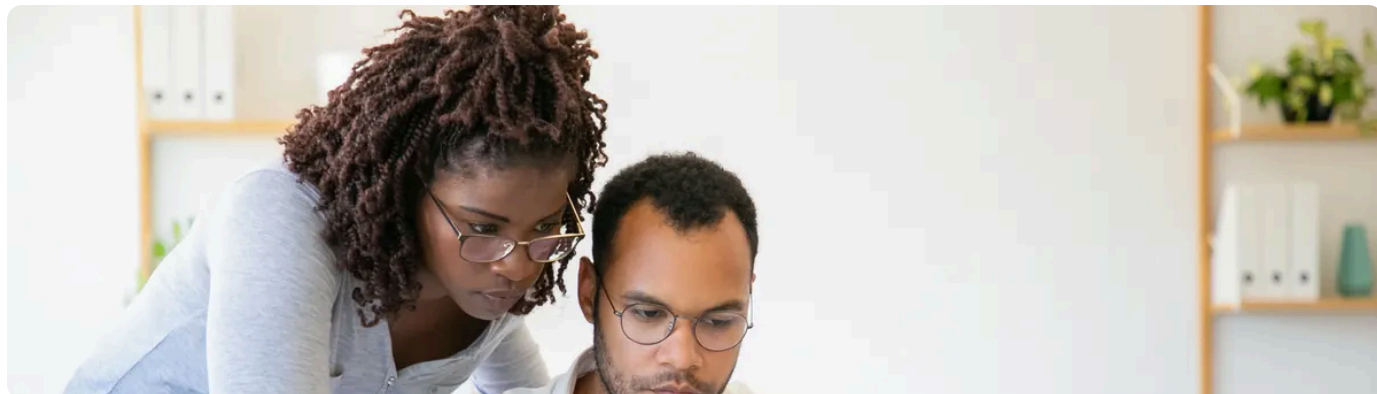
International · English

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

<https://www.my.mozout.com/knowledgebase/5886>



The short answer: the browser's padlock does not tell the whole story. A site can show the padlock on your computer and fail on other devices because of an **incomplete certificate chain**, a certificate that **does not cover www** or one that **is about to expire**. Five simple checks catch almost everything.

What to check

Check	What to look for
Who the certificate is for	It should cover the address with and without www. If it covers only one, the other gives a warning.
Expiry	The end date. An expired certificate gives everyone the red warning: Expired certificate .
The full chain	The server must also send the intermediate certificates. Without them some phones and programs refuse.
Redirecting from http to https	Whoever types the address without https should be taken to the secure one: Redirecting HTTP to HTTPS .
Mixed content	Images or scripts loaded over http on an https page remove the padlock: Mixed content .

Step by step

1

In the browser, click the padlock, open the certificate details and read “Issued to”, “Issued by” and the dates.

2

In cPanel, the “SSL/TLS Status” tool shows the certificate’s state for each domain and subdomain.

3

Test the chain away from your computer: on the command line, `curl -vI https://your-domain.com` should end without a certificate error; or use an online SSL test.

4

Open the address without https and with www and confirm it always ends on the version you chose.

5

Open the page on a phone, on another network, to catch what your computer hides.

A certificate belongs to a domain, not to the whole site. If you add a subdomain or a new domain, it needs a certificate too. And if you use Cloudflare, the certificate the visitor sees is Cloudflare’s: **SSL at Cloudflare**.

With HTTPS right, the next step is to reinforce it: **HSTS** and **Security headers**. Which type of certificate: **DV, OV and EV**.

The certificate will not activate or the warning persists? See **I bought an SSL certificate and it has not activated** and open a ticket with the address.

[Open a support ticket](#)

SEE ALSO

[Certbot renewal failed or the certificate expired: how to find out why](#)

[Mixed content after moving to HTTPS: the padlock that will not turn on](#)

[HSTS explained: forcing https for good, and the trap of switching it on too early](#)

[I bought an SSL certificate and it has not activated: domain validation](#)

[Switching on SSL at Cloudflare without breaking the site](#)

[DV, OV and EV certificates: which kind of SSL certificate you really need](#)



Online version of this document

MozOut is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

MozOut International

RLX Holdings (Pty) Ltd. • Group RLX Holdings

TAX NO. (SARS)

943 907 6234

REGISTRATION NO.
(CIPC)

2025/667953/07

REGISTERED OFFICE

1111 Olive Street
Saint Louis 63101, Missouri, United States

CONTACT

info@mozout.com • +27 78 823 3325 • www.mozout.com

OPENING HOURS

Monday to Friday - 08 AM to 04 PM
Saturday & Sunday - Closed