

KNOWLEDGE BASE · PUBLIC DOCUMENT

AutoSSL behind Cloudflare: why the free certificate leaves names out or fails to renew

Speed, Cache & CDN

CODE

RLX-INT-KB-6408

VERSION

v2026.10.16

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/6408>



The short answer: the server's free certificate (cPanel's AutoSSL) is still needed with Cloudflare in front: it protects the leg between Cloudflare and the server in **Full (strict)** mode, and it protects mail, which does not go through Cloudflare. To issue it, the server has to prove each name is yours and reaches it. With DNS on Cloudflare, the zone that counts is no longer the server's, so the proof goes over the web. When a name is left out, it is because it does not exist in Cloudflare's DNS, points somewhere else, a CAA record does not authorise issuance, or something answers in the server's place.

Why a name is left out, or will not renew

Cause	How to recognise it	What to do
The name does not exist in Cloudflare's DNS (mail, webmail, cpanel, autodiscover)	SSL/TLS Status shows it excluded or with a failed check; Outlook warns about the certificate on mail.yourdomain.	Create the record at Cloudflare, grey, pointing at the server, and run AutoSSL again.
The name points somewhere else	The record at Cloudflare holds an old address or another service's.	Fix the value. The server only certifies names that reach it.
A CAA record does not authorise the authority the server uses	There are CAA records at Cloudflare and none authorises that authority.	Add it: CAA records .
A protection answers in the server's place	Attack mode, bot mode or a country rule challenges or blocks the validator, which is a bot.	Let the /.well-known/acme-challenge/ path through, or turn the name grey during renewal.
The certificate has already expired and the check is sent to https	In Full (strict), Cloudflare refuses to connect to a server with an expired certificate and shows error 526.	Turn the name grey, run AutoSSL, turn it orange again.
A cache rule stores everything, /.well-known/ included	The check gets an old answer, stored at Cloudflare.	Exclude that path from the cache.

The renewal that works

1

See the status: in cPanel, open **SSL/TLS Status**. It shows which names are covered, which are excluded and, beside them, the reason.

2

Check the DNS at Cloudflare: every name that needs a certificate has to exist there and point at the server. Mail and admin names stay grey: **orange cloud or grey cloud**.

3

If you have CAA records, make sure they authorise the authority the server uses. Cloudflare may add its own authorities by itself; the server's have to be there on their own.

4

If the failing name is orange, turn it grey for a while and give the TTL time. The check then reaches the server with nothing in between.

5

Run AutoSSL again in SSL/TLS Status and wait for it to finish.

6

Once the name shows as covered, turn it orange again and make sure the SSL mode is still Full (strict).

Do not change the SSL mode to “fix” an expired certificate. On Full the leg between Cloudflare and the server goes unverified; on Flexible it goes unencrypted and the site falls into a redirect loop. Full only as a temporary step while the certificate is issued; Flexible never: **switching on SSL at Cloudflare without breaking the site.**

The mail certificate is this same one. If after the move Outlook or the phone start warning about the certificate on mail.yourdomain, the mail name was almost always left out of Cloudflare's DNS or turned orange: **the certificate warning in Outlook.**

AutoSSL still failing? Send us the domain and the sentence SSL/TLS Status shows next to the name.

[Open a support ticket](#)

RLX-LIMITES

Where to see it in your account

We do not name the authority here, because the certificate on your own account tells you exactly which one it is. In cPanel, open SSL/TLS Status, choose your domain and view the certificate details. The line called Issuer (or the issuing authority) is the name to authorise in a CAA record.

If a name is excluded and has no certificate yet, fix the cause in the table above, run AutoSSL again, and read the issuer once the certificate appears. Then add that authority to the CAA records at Cloudflare, keeping the ones already there. If the issuer line is not clear, send us the domain and a screenshot of the details, and we will tell you the name.

/RLX-LIMITES

SEE ALSO

[The free SSL certificate did not renew: why AutoSSL fails and what to check](#)

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

[CAA records: who may issue certificates for your domain](#)

[No padlock on your site: the causes, in order](#)

[The security certificate warning in Outlook: what it means and how to stop it](#)

[Orange cloud or grey cloud at Cloudflare: which records to proxy and which to leave DNS only](#)



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