interweb

Generated on 15/11/2026 00:15

KNOWLEDGE BASE · PUBLIC DOCUMENT

Certbot renewal failed or the certificate expired: how to find out why

Websites & Applications

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1364	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/1364

Certbot renewal failed or the certificate expired: how to find out why

Websites & Applications Created on **October 10, 2026** 3 min read



If the browser warns that a certificate has expired on a VPS using certbot, the automatic renewal either **did not run** or **ran and failed**. Open the terminal and do, in this order: `sudo certbot certificates` to see the dates, `sudo certbot renew --dry-run` to rehearse the renewal at no cost, and read the error message. Nearly always it is port 80, DNS or the web server. On an unmanaged VPS there is no AutoSSL: the certificate and its renewal are yours.

Step by step

1. **See the state.** `sudo certbot certificates` lists each certificate, the names it covers and the days left; an expired one is marked “INVALID: EXPIRED”.

2. **Provoke the error with a rehearsal.** `sudo certbot renew --dry-run` does what the real renewal does, against the staging environment. The message at the end is your clue. Always use `--dry-run` while hunting for the cause: repeating real failed requests can hit Let’s Encrypt’s limits.

3. **Read the full log.** `sudo tail -n 60 /var/log/letsencrypt/letsencrypt.log` holds the request, the reply and the name that failed.

4. **Check that automatic renewal is scheduled.** `systemctl list-timers | grep -i certbot`. If nothing shows, or certbot came by another installation route (system package or snap), the timer may have another name or never have been switched on; see what the certbot site recommends for your system.

5. **Fix the cause, renew and reload.** `sudo certbot renew` and, if the web server is not reloaded by itself, `sudo systemctl reload nginx` (or `apache2` / `httpd`).

6 **Confirm from outside.** `echo | openssl s_client -connect yourdomain.tld:443 -servername yourdomain.tld 2>/dev/null | openssl x509 -noout -dates` shows the dates of the certificate the public actually receives.

The causes, in order of frequency

The message says…	What it usually is
Timeout during connect / Connection refused	Port 80 is closed in the firewall, or the web server is stopped. Validation is over HTTP on port 80, even if the site lives on 443.
Invalid response / 404 on /.well-known/acme-challenge/	The validation request reaches another site, or a redirect or `location` rule that catches it. See which block answers that name.
DNS problem / NXDOMAIN / the IP is not this one	The domain no longer points at this server, or has an AAAA (IPv6) record pointing elsewhere. See **DNS records**.
Could not bind to port 80	certbot in standalone mode (`--standalone`) wants the port nginx or Apache already holds. Switch to the web server plugin (`--nginx` or `--apache`) or to `--webroot` .
too many failed authorizations / rate limit	Too many failed attempts. Stop, fix the cause and wait as long as Let's Encrypt says before trying again.
CAA record prevents issuance	A CAA record on the domain does not let this authority issue: **CAA records**.
Renewed successfully, but the browser shows the old one	The web server was not reloaded and still serves the certificate it holds in memory. Reload it.

Do not keep repeating the real request.
Each failed attempt counts towards the validation limits. If you changed nothing between two rehearsals, the result will be the same. Fix first, then try.

Moved the site to another server or IP?
The certificate lives on the old server. On the new one you have to request it again, and DNS must point at the new one before validation passes.

Add a warning before it expires.
An outside check on the certificate (many free monitoring services do it) e-mails you weeks ahead, instead of learning from a customer. And keep the contact e-mail you gave certbot: that is where Let's Encrypt sends its notices.

NEED A HAND?

Is the domain ours and DNS looks right but validation keeps failing? Tell us the name and the server IP and we will check the zone.

Open a support ticket →

SEE ALSO

- HTTPS for a container: a certificate and a domain →
- Redirecting to HTTPS and to the bare domain →
- No padlock on your site: the causes, in order →
- What is an SSL certificate and why does it matter →

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-1364 · v2026.10.10 · Generated on 15/11/2026 00:15