Gerado a 15/11/2026 02:09

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

O certificado SSL gratuito não renovou: porque falha a AutoSSL e o que verificar

SSL e HTTPS

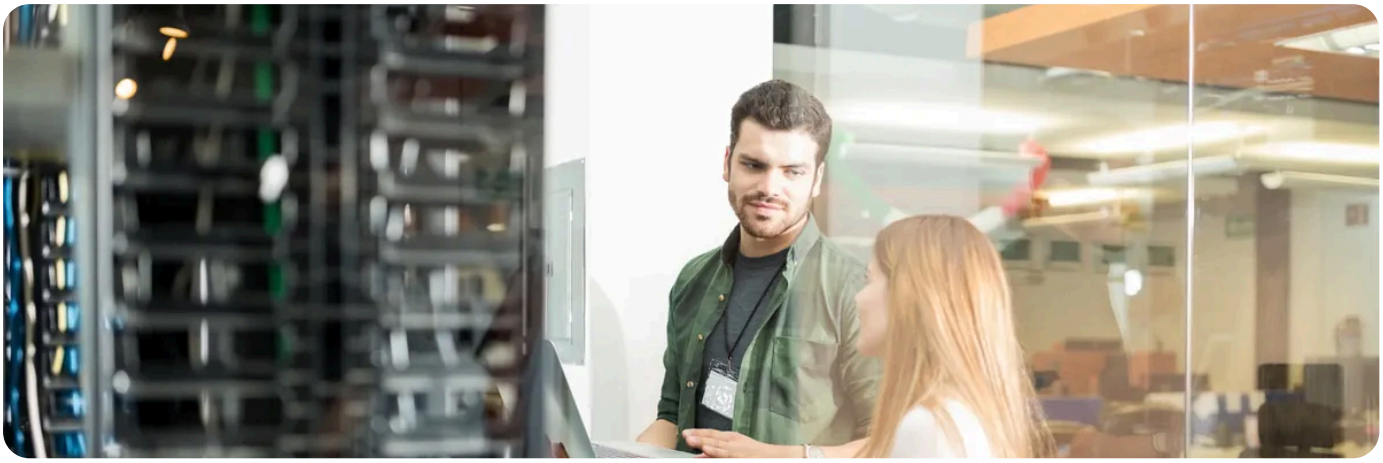
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-4650	v2026.10.10	Angola · Português

MozOut Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.my.mozout.com/knowledgebase/4650

O certificado SSL gratuito não renovou: porque falha a AutoSSL e o que verificar

SSL e HTTPS Criado em **10 de outubro de 2026** 3 min de leitura



A resposta curta: o certificado gratuito da conta (a AutoSSL, do Let's Encrypt) emite-se e renova-se sozinho, mas só se o servidor conseguir **provar que o domínio é seu e que aponta para cá**. Quando falha, quase sempre é uma de cinco coisas: o domínio aponta para outro lado, um registo CAA impede a emissão, uma regra do site bloqueia a verificação, o nome é novo, ou há algo parado com a conta.

1. Veja o estado do certificado

No cPanel, abra «SSL/TLS Status». Mostra cada domínio e subdomínio da conta com o seu estado e a data de validade. Um domínio sem cadeado, ou a precisar de renovação, é o que interessa. Pode lançar daí uma nova tentativa de AutoSSL com o botão para o fazer.

2. As cinco causas, por ordem

Causa	Como reconhecer	O que fazer
O domínio não aponta para este servidor	Os servidores de nomes, vistos no WHOIS, não são os da sua conta, ou há um registo A para outro endereço.	Corrigir o apontamento e esperar. Veja **sem cadeado: as causas, por ordem**.
Registo CAA a barrar a emissão	O domínio tem um CAA que não autoriza a autoridade que a AutoSSL usa.	Corrigir ou remover o registo: **registos CAA**.
Uma regra do site impede a verificação	Um redirecionamento ou uma regra no `.htaccess` que bloqueia o caminho `/.well-known/`, uma proteção que pede senha à raiz do site, ou um *plugin* de manutenção que responde a tudo.	Excluir esse caminho da regra. Veja **o redirecionamento para HTTPS**.
O nome é novo ou fora do certificado	Um subdomínio criado há pouco, ou o `www` que o certificado não inclui.	Esperar pela próxima volta da AutoSSL ou lançá-la à mão.

Causa	Como reconhecer	O que fazer
Atrás de um serviço de proteção	Com o Cloudflare em modo restrito, a verificação pode não chegar ao servidor.	Veja **ligar o SSL no Cloudflare sem estragar o site**.

3. Depois de corrigir

1. **Lance a AutoSSL de novo** em «SSL/TLS Status» e aguarde alguns minutos.
2. **Recarregue o estado** e veja se o domínio mostra agora o novo prazo. Abra o site num separador privado: o navegador guarda certificados e páginas.
3. **Se continua a falhar,** o cPanel mostra o motivo, em inglês, ao lado do domínio. Copie a frase tal como está e envie-a num pedido de suporte, com o domínio. Ela diz-nos logo que verificação não passou.

Se o certificado já caducou,
os visitantes veem um aviso de segurança a barrar o site. Não lhes peça que «continuem mesmo assim»: isso ensina-os a ignorar avisos, e é exatamente o que os atacantes querem. Corrija e, entretanto, avise-os por outro canal.

Tem um certificado pago e a AutoSSL em simultâneo? Pode acontecer que o pago seja o que está caducado. Veja qual está a ser usado em «SSL/TLS Status» antes de procurar o problema no lado errado. Para a cobertura de cada tipo, veja **certificados DV, OV e EV**.

PRECISA DE AJUDA?

O domínio continua sem certificado depois de tudo isto? Envie-nos o domínio e a mensagem do cPanel.

Abrir pedido de suporte →

VEJA TAMBÉM

- **Sem cadeado no site: as causas, por ordem** →
- **Registos CAA: quem pode emitir certificados para o seu domínio** →

Certificados DV, OV e EV

Porque é que o meu certificado SSL mostra menos de 365 dias?

MozOut Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@mozout.com · +244 942 011 191 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-4650 · v2026.10.10 · Gerado a 15/11/2026 02:09