Gerado a 18/10/2026 12:18

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

A AutoSSL atrás do Cloudflare: porque o certificado grátis deixa nomes de fora ou não renova

Velocidade, Cache e CDN

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-MZ-KB-6408	v2026.10.16	Moçambique · Português

MozOut Moçambique
RLX Holdings, S.A. · Grupo RLX Holdings
NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

https://www.my.mozout.com/knowledgebase/6408

A resposta curta: o certificado grátis do servidor (a AutoSSL do cPanel) continua a ser preciso com o Cloudflare à frente: é ele que protege a ligação entre a Cloudflare e o servidor no modo **Full (strict)**, e é ele que protege o correio, que não passa pela Cloudflare. Para o emitir, o servidor tem de provar que cada nome é seu e chega até ele. Com o DNS no Cloudflare, a zona que conta já não é a do servidor, e a prova passa pelo caminho web. Quando um nome fica de fora, é porque não existe no DNS do Cloudflare, aponta para outro lado, um registo CAA não autoriza a emissão, ou alguma coisa responde no lugar do servidor.

Porque um nome fica de fora, ou não renova

Causa	Como se reconhece	O que fazer
O nome não existe no DNS do Cloudflare (mail, webmail, cpanel, autodiscover)	O SSL/TLS Status mostra-o excluído ou com a verificação falhada; o Outlook avisa do certificado em mail.oseudominio.	Crie o registo no Cloudflare, a cinzento, a apontar para o servidor, e corra a AutoSSL outra vez.
O nome aponta para outro sítio	O registo no Cloudflare tem um endereço antigo ou de outro serviço.	Corrija o valor. O servidor só certifica nomes que chegam até ele.
Um registo CAA não autoriza a autoridade que o servidor usa	Há registos CAA no Cloudflare e nenhum autoriza essa autoridade.	Acrescente-a: **registos CAA**.
Uma protecção responde no lugar do servidor	O modo de ataque, o modo contra robôs ou uma regra de país desafia ou bloqueia o verificador, que é um robô.	Deixe passar o caminho /.well-known/acme-challenge/, ou ponha o nome a cinzento durante a renovação.
O certificado já expirou e a verificação é levada para https	Em Full (strict), a Cloudflare recusa ligar a um servidor com o certificado expirado e mostra o erro 526.	Ponha o nome a cinzento, corra a AutoSSL, volte a laranja.
Uma regra de cache guarda tudo, incluindo /.well-known/	A verificação recebe uma resposta antiga, guardada na Cloudflare.	Exclua esse caminho da cache.

A renovação que funciona

1. **Veja o estado:** no cPanel, abra **SSL/TLS Status**. Mostra que nomes estão cobertos, quais estão excluídos e, ao lado, a razão em inglês.

2. **Confirme o DNS no Cloudflare:** cada nome que precisa de certificado tem de existir lá e apontar para o servidor. Os nomes do correio e de administração ficam a cinzento: **nuvem laranja ou cinzenta**.

3	**Se tiver registos CAA,** confirme que autorizam a autoridade que o servidor usa. A Cloudflare pode acrescentar por si as autoridades dela; as do servidor têm de lá estar por si.

4	**Se o nome que falha está a laranja,** ponha-o a cinzento por momentos e dê tempo ao TTL. Assim a verificação chega ao servidor sem nada pelo meio.

5	**Corra a AutoSSL outra vez** no SSL/TLS Status e espere que termine.

6	**Quando o nome aparecer coberto,** volte a pô-lo a laranja e confirme que o modo SSL continua em Full (strict).

Não troque o modo SSL para «resolver» um certificado expirado. Em Full a ligação entre a Cloudflare e o servidor fica sem verificação; em Flexible fica sem cifra e o site entra num ciclo de redireccionamentos. Full só como passo temporário enquanto o certificado é emitido; Flexible nunca: **activar o SSL no Cloudflare sem partir o site**.

O certificado do correio é este mesmo. Se depois da mudança o Outlook ou o telemóvel começam a avisar do certificado em mail.oseudominio, quase sempre o nome mail ficou de fora do DNS do Cloudflare ou a laranja: **o aviso de certificado no Outlook**.

A AutoSSL continua a falhar? Envie-nos o domínio e a frase que o SSL/TLS Status mostra ao lado do nome.

Abrir pedido de suporte

RLX-LIMITES

Onde ver na sua conta

Não indicamos aqui a autoridade, porque o certificado da sua própria conta diz exatamente qual é. No cPanel, abra «Estado SSL/TLS», escolha o seu domínio e veja os detalhes do certificado. A linha chamada «Emissor» (ou a autoridade emissora) é o nome a autorizar num registo CAA.

Se um nome estiver excluído e ainda sem certificado, corrija a causa na tabela acima, execute o AutoSSL de novo e leia o emissor quando o certificado aparecer. Depois junte essa autoridade aos registos CAA no Cloudflare, mantendo os que já lá estão. Se a linha do emissor não for clara, envie-nos o domínio e uma captura dos detalhes, e dizemos-lhe o nome.

/RLX-LIMITES

VEJA TAMBÉM

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

Activar o SSL no Cloudflare sem partir o site

Registos CAA: quem pode emitir certificados para o seu domínio

O cadeado não aparece: as causas, por ordem

O aviso de certificado de segurança no Outlook: o que significa e como o resolver

Nuvem laranja ou cinzenta no Cloudflare: que registos passar pelo proxy e quais deixar só DNS

Versão online deste documento

A MozOut é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020	37 mil+	130+
FUNDADA	CLIENTES	INSCRIÇÕES POR DIA

MozOut Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT	401 191 607
NUEL	105 045 974
CAE	62022
SEDE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Moçambique
CONTACTOS	info@mozout.com · +258 84 635 1111 · +258 86 635 1111 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-MZ-KB-6408 · v2026.10.16 · Gerado a 18/10/2026 12:18