interweb

Generated on 15/11/2026 00:07

KNOWLEDGE BASE · PUBLIC DOCUMENT

I bought an SSL certificate and it has not activated: domain validation

SSL & HTTPS

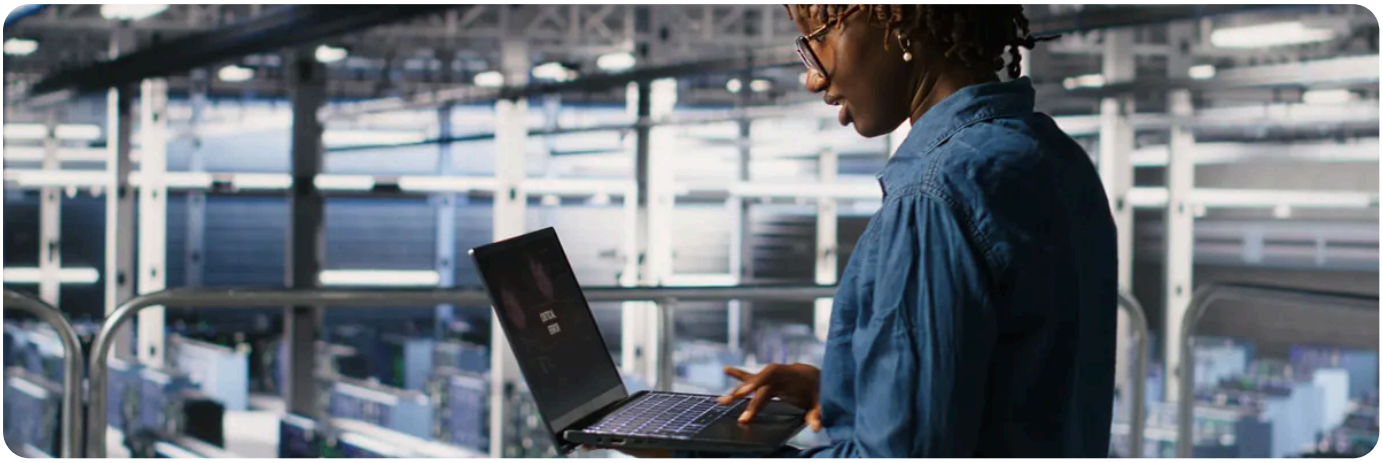
CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-294	v2026.09.28	Angola · English

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/294

I bought an SSL certificate and it has not activated: domain validation

SSL & HTTPS Created on **September 11, 2026** Updated on **September 28, 2026** 4 min read



You bought an SSL certificate, you paid, and the padlock still has not appeared. It is the most frequent question we get about certificates - and nearly always only **one step is missing, and it is yours**. This article explains what happens after payment and where the process usually stalls.

First of all: there are two different certificates

Which	What it is
The free one (AutoSSL)	Comes with the plan, renews itself and covers the account's domain and subdomains. **For most sites, it is enough.** See **what is an SSL certificate**
The paid one	Bought separately. It brings a financial warranty, company validation and options the free one does not have - such as covering every subdomain at once (*wildcard*).

If all you want is to remove the «not secure» warning.
The free certificate does exactly that, and the browser does not tell them apart: the padlock is the same. A paid certificate is bought for other reasons - warranty, visible company identity, or wildcard. If you need none of those, you do not need to pay.

What happens the moment you pay

The order goes to the certificate authority automatically **the moment the invoice is marked paid** - it is not waiting on anyone at our end. What is *not* automatic is the next step.

The certificate is not issued until you prove the domain is yours.
It is called **domain control validation** (DCV) and no authority waives it. This is where practically every «I paid and it did not activate» ticket is stuck. Nobody can do it for you, because the whole point is to prove that it is you.

The three ways to validate

Method	How it works
By e-mail	A message with an approval link arrives at an address **on the domain itself**: admin@, administrator@, webmaster@, hostmaster@ or postmaster@. It is the quickest - if that mailbox exists.
By DNS record	You add a TXT record supplied by the authority. Good when the domain has no e-mail - see **DNS records explained**
By file on the site	You place a file in a given folder inside *public_html*. Good when the site is already live but the DNS is elsewhere.

The trap in the e-mail method.
The approval message goes to an address **on the domain being certified** - not to your Gmail and not to your client account e-mail. If `admin@yourdomain.ao` does not exist, the message goes nowhere and the order waits for an approval that never comes. **Create the mailbox first**, or choose another method.

How long it really takes

It depends on the type of certificate, and the difference is large. Price does not set the timescale - how much there is to verify does:

Type	Realistic timescale
DV - validates the domain only	Minutes to a few hours after you validate. That is RapidSSL and similar.
OV - also validates the company	**One to three working days.** Someone checks the company exists and the registration is right - sometimes with a phone call.
EV - extended validation	**Several days, sometimes more than a week.** It is the most demanding check and there are documents to produce.

If the site is for tomorrow.
An OV or EV certificate cannot be sorted the same day, however urgent - the timescale belongs to the certificate authority, not to us. If the date is tight, start now with the free certificate, ready in minutes, and install the paid one when it arrives.

Once issued: installing it

With the certificate issued, it still has to be put in place - the step by step is in **how to activate and install a paid SSL certificate**. And once installed, make sure nobody is left on the unencrypted version: **how to force HTTPS with .htaccess** handles that in one line.

«I paid and it still has not activated»: the checklist

1. **Look for the approval message** in the domain's mailbox - and in its spam folder. That is cause number one.
2. **Confirm the mailbox exists.** If it does not, create it and ask for the message to be resent. There is no need to buy again.
3. **Check which type you bought.** If it is OV or EV, nothing may be stuck - it may simply be under way.
4. **Confirm the domain points here** if you chose file validation. Without that, the authority cannot find the file you placed.
5. If none of this applies, open a ticket with the domain and the invoice number - we can see the order's state at the authority and resend the validation.

Two things that confuse everyone

The certificate shows fewer than 365 days. It is not an error and it is not a shortened year - the explanation is in **why does my SSL certificate show fewer than 365 days**.

I installed it and the padlock still warns. It is usually mixed content: the page is served over HTTPS but pulls images or scripts over `http://`. The browser warns because of those pieces, not because of the certificate. Fix the addresses to `https://` or leave them without a protocol.

NEED A HAND?

Certificate stuck halfway? Send us the domain and the invoice.

Open a ticket →

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

RLX-AO-KB-294 · v2026.09.28 · Generated on 15/11/2026 00:07

Online version of this document