interweb

Generated on 16/10/2026 15:36

KNOWLEDGE BASE · PUBLIC DOCUMENT

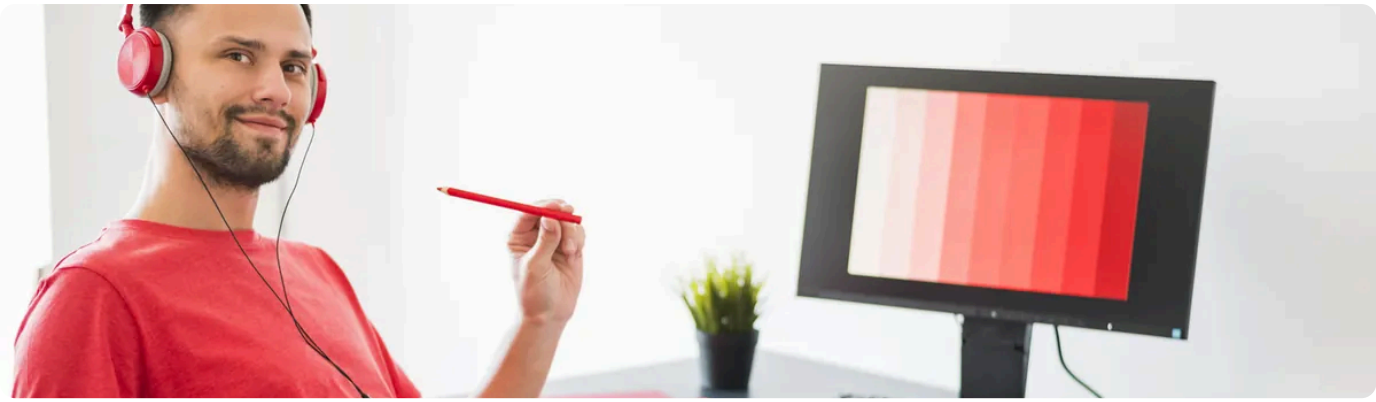
Cloudflare blocked a real customer: security events, error 1020 and narrow exceptions

Speed, Cache & CDN

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-2106	v2026.10.16	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/2106



The short answer: when a customer says they cannot log in, pay or send a form, and the site is orange on Cloudflare, the first suspect is Cloudflare's protection: a web application firewall (WAF) rule, bot mode, the security level or attack mode. Cloudflare's block page shows a **Ray ID**. With it you find the event in the dashboard, see which rule acted and open a narrow exception, instead of switching protection off altogether. Cloudflare is a third-party service: the account is yours, opened on their site, and we do not sell it.

What the customer sees, and what it usually is

What appears	What it usually is
"Access denied" with error 1020	A rule created in the account (custom, or an access rule by IP, country or user agent) blocked the request.
A check page that keeps repeating, or a challenge that never passes	A challenge from the security level or attack mode, in a browser with cookies blocked, an aggressive extension, or a shared network with a poor reputation.
The customer pays, the money leaves, and the order never confirms	The payment provider's notification is automated traffic and cannot solve challenges: it was blocked or challenged. See **what a webhook is**.
An integration, a monitor or an app stopped working	Bot mode or a rule treats them as bots, because they are.
A 403 error with the server's page, not Cloudflare's	It was not Cloudflare: it was the server. See **ModSecurity and web application firewalls** and **error 403**.

Finding the block and opening only the right door

1. **Ask the customer for three things:** the Ray ID shown at the bottom of the block page, the time, and their public IP address (**how to find your public IP**).

2. **Find the event:** in the Cloudflare dashboard, **Security** section, the events log. Filter by Ray ID or IP. The event says which service acted (custom rule, managed rules, bots, security level) and what action it took. Menu names change over time: look for “Events” or “Security Events”.

3. **If it was an account rule** (country, user agent, path), fix it so it no longer catches this case, rather than deleting it.

4. **If it was a legitimate automated service** (the payment notification, a monitor), create a rule that lets it through (Skip) only on the path it uses and, if the service publishes its addresses, only from those addresses. The exception has to sit before the blocking rules.

5. **If it was the free plan’s bot mode,** note that, according to Cloudflare’s documentation, it does not accept rule-based exceptions. If it blocks something you need, switch it off and protect another way.

6. **Test with the real case:** a test purchase all the way through, the form, the account login. Then go back to the events log and confirm the request no longer shows up as blocked.

Do not fix it by switching everything off, or by opening the door to the world. A broad exception (the whole site, every country, “Skip” on every protection) lets back in whoever the block was stopping. Open the minimum: the path, the service, the addresses. And attack mode is for use during an attack, not to be left on: **the options that cause trouble**.

Before tightening, prefer challenging to blocking. A challenge lets people through and stops most bots; a block lets nobody through. Watch in the events, for a few days, who a rule catches before making it harsher.

One of your customers cannot log in or pay? Send us the Ray ID, the time and the page address.

Open a support ticket

SEE ALSO

The Cloudflare options worth having, and the ones that cause trouble

Cloudflare: when it helps, how to switch it on, and the cache that fools you

ModSecurity and web application firewalls: what they do, and what to do when one blocks you

Error 403 Forbidden: permissions, .htaccess and blocked IPs

An online shop with local payment methods: WooCommerce and getting paid

What a webhook is, and how to test one with curl

interweb

Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020	37,000+	130+
FOUNDED	CLIENTS	SIGN-UPS A DAY

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-2106 · v2026.10.16 · Generated on 16/10/2026 15:36