

KNOWLEDGE BASE · PUBLIC DOCUMENT

Why your server was switched off or locked after an abuse notice, and how to bring it back

Security

CODE

RLX-INT-KB-6822

VERSION

v2026.10.21

COUNTRY · LANGUAGE

International · English

MozOut International

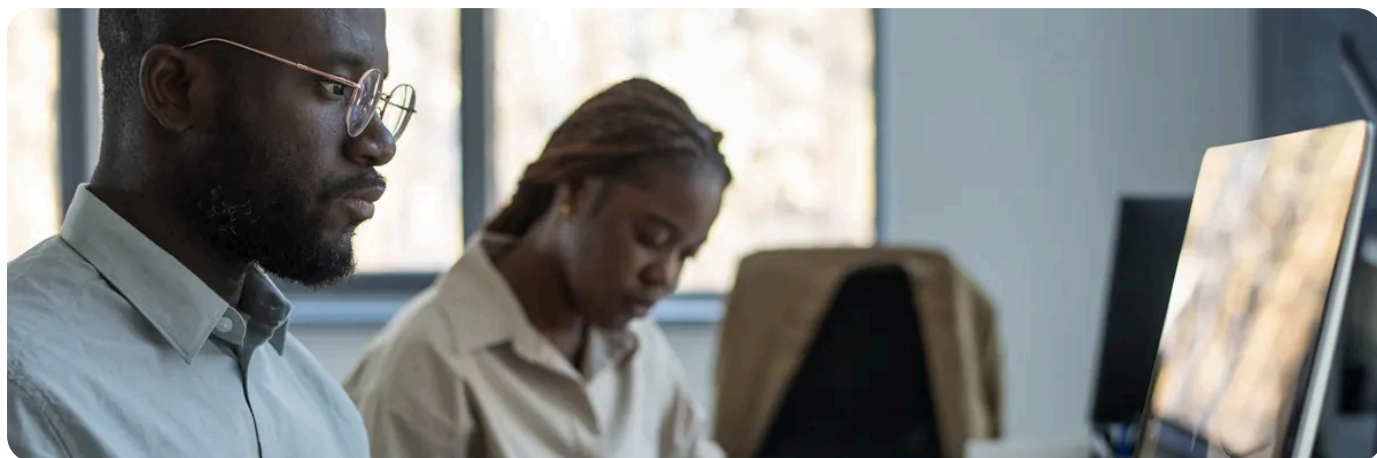
RLX Holdings (Pty) Ltd. · Group RLX Holdings

Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

<https://www.my.mozout.com/knowledgebase/6822>

Why your server was switched off or locked after an abuse notice, and how to bring it back

📁 Security 📅 Created on **October 21, 2026** ⌚ 4 min read



The short answer: after an abuse notice, you first investigate with the server still on; if by the deadline the cause is not clear, or the attack traffic carries on, **the server may be switched off** to protect the network. **The data stays intact: nothing is deleted.** Our network provider may also **block** the server or the IP on its own, and while the block lasts you cannot access the server. To come back: you investigate, clean up and send us the report; we check it and switch the server back on, or ask the provider to lift the block. If the abuse returns after it is back on, the server is switched off again.

🔍 What may have happened

Situation	Who decided it	How it is solved
Server switched off after an abuse notice	Us, to protect the network, because the deadline passed or the traffic continued.	A report in the support ticket for the notice; we check it and switch it back on.
Server or IP blocked	The network provider, following the notice.	While it lasts, you cannot access the server. With the same report, we ask the provider to lift the block.
Suspended for non-payment	Billing, because of an overdue invoice.	Nothing to do with abuse: how to reactivate a suspended plan.
Suspended for another reason (security, spam)	Us, with the reason in the support ticket.	a service suspended for a reason other than payment.
No SSH, but there was no notice	Probably nobody: a firewall, a key or a port.	I have lost SSH access to my server.

➔ Getting the server running again

- 1 Read the support ticket for the notice:** it has the reason, the log (with times in UTC) and what was already said to the provider. Each kind of notice is explained in **an abuse notice about your server**.
- 2 If the server has already been switched off, ask us in the same ticket to switch it back on so you can investigate.** Root access is yours and we do not log in to the server.
- 3 Find the cause and close the way in: **checking processes, cron jobs, users and keys**.** If the cause was a service open to the internet, close it before asking for the server to be switched back on.
- 4 Send the short report:** the cause and how it got in, what you found and removed, and what you did so it does not happen again. The template is in **writing the reply to an abuse notice**.
- 5 We check it and switch the server back on,** or ask the network provider to lift the block. How long the unblocking takes depends on the provider, not on us.
- 6 Watch the server once it is back:** look at outgoing connections with `ss -tunap` and make sure the traffic from the notice has not returned. If it does, the server is switched off again.

! Asking only for the server to be switched back on, with no report, does not solve anything.
The server would attack again and be switched off again, and each repeat weighs on the provider's response. Building a new server and copying the same content onto it does not help either: whatever was infected goes along.

💡 On a compromised server, the safest route is to reinstall the system and restore a clean copy (reinstalling the VPS operating system and which backup to restore). Cleaning in place is for people who know what they are doing: an attacker with root access can leave ways back in that are not obvious at first.

📞 NEED A HAND?

Your server was switched off or blocked and you want to arrange how to investigate? Reply in the support ticket for the notice.

 **Open a support ticket ➔**

SEE ALSO[An abuse notice about your server: what it means, the deadline and what we need from you](#)[Writing the reply to an abuse notice: cause, what you removed and how it will not happen again](#)[Is my VPS compromised? Checking processes, cron jobs, users, SSH keys and temporary folders](#)[A service suspended for a reason other than payment: what it means and what happens next](#)[Reinstalling or changing your VPS operating system](#)[After a hack, which backup do you restore? Choosing a clean copy](#)**mozout****MozOut International**

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

RLX-INT-KB-6822 · v2026.10.21 · Generated on 21/10/2026 16:04

Online version of this
document