interweb

Generated on 15/11/2026 00:15

KNOWLEDGE BASE · PUBLIC DOCUMENT

Installing fail2ban on a VPS to stop SSH password guessing

Security & Access

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1350	v2026.10.10	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/1350

Installing fail2ban on a VPS to stop SSH password guessing

Security & Access Created on **October 10, 2026** 3 min read



A server with SSH open receives, **day and night, automated password attempts** from all over the world. **fail2ban** reads the logs, spots the addresses that fail too many times and blocks them for a while. It does not replace an SSH key, but it clears the noise and stops anyone who keeps trying. The commands are yours, on your own server: support does not install or repair them (see **how far our support goes**).

Installing

1. **Debian and Ubuntu:** `sudo apt update` and `sudo apt install fail2ban`.

2. **AlmaLinux and Rocky:** the package comes from an extra repository: `sudo dnf install epel-release` and then `sudo dnf install fail2ban`.

3. **Start the service and make it start with the server:** `sudo systemctl enable --now fail2ban`.

Configuring without breaking it

Do not edit `/etc/fail2ban/jail.conf`: a package update may replace it. Create your own, `/etc/fail2ban/jail.local`, with only what you want to change:

```
[DEFAULT]
ignoreip = 127.0.0.1/8 ::1 YOUR.ADDRESS
bantime = 1h
findtime = 10m
maxretry = 5

[sshd]
enabled = true
```

Line	What it does
ignoreip	Addresses that are never blocked. Put yours there, so you do not block yourself. Separate them with spaces.
maxretry	How many failures, within the findtime window, before blocking. The values in this example (5, 10 minutes, 1 hour) are only a starting point.
findtime	The window in which failures are counted.
bantime	For how long the address stays blocked.
port	If your SSH uses another port, add to [sshd] the line `port = 2222`, with your number.

1. **Restart to apply:** `sudo systemctl restart fail2ban`. You can test the configuration first with `sudo fail2ban-client -t`.

2. **See the overall state:** `sudo fail2ban-client status` lists the active "jails", which should include `sshd`.

3. **See who is blocked:** `sudo fail2ban-client status sshd`.

4. **Unblock an address** (yours, if you got it wrong several times): `sudo fail2ban-client set sshd unbanip THE.ADDRESS`.

You can block yourself.
Getting the password wrong five times in a row is enough. Hence `ignoreip` and an SSH key that works. If it happens, the way back is to come in over another network (mobile data, say) and unblock, or use the panel console: see **I have lost SSH access to my server**, which has this case as its third cause.

If the SSH log does not exist,
fail2ban has nothing to read. On newer systems, which keep logs in the journal, add `backend = systemd` to the `[sshd]` section. Where logs live is in **where are the logs on a Linux VPS**. The firewall does the rest of the work with fail2ban: see **setting up the ufw firewall**.

NEED A HAND?

Did fail2ban block you and you cannot get in? Tell us the VPS address and where you connect from.

Open a support ticket →

SEE ALSO

- **Setting up the ufw firewall on Ubuntu without locking yourself out**
- **How to create an SSH key and log in without a password**
- **I have lost SSH access to my server**
- **Keeping your VPS or dedicated server secure: the six that matter**

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

Online version of this document

RLX-AO-KB-1350 · v2026.10.10 · Generated on 15/11/2026 00:15