

KNOWLEDGE BASE · PUBLIC DOCUMENT

Vaultwarden on a VPS: your own password manager, and what you take on

VPS & Servers

CODE

RLX-AO-KB-1972

VERSION

v2026.10.15

COUNTRY · LANGUAGE

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/1972>



The short answer: Vaultwarden is a free server, compatible with the Bitwarden apps, where you keep **the team's or the family's passwords on your own VPS**. It is light and works well. But it is a service you become **responsible for**: updates, backups, HTTPS and availability. If you do not want that, a service's password manager is enough.

What the site needs

What	What to do
What it is	A server of encrypted passwords and notes, used through the web page, the browser extension and the mobile apps.
What it needs	A VPS with Docker, a domain with HTTPS (the vault does not work without it) and regular backups.
What you take on	If the server fails, you have no access to the passwords until you recover it. So keep an emergency copy outside it.
Who can create accounts	By default, anyone who reaches the address. Switch registrations off once you have created the accounts you need.
When it is not worth it	If nobody wants to handle the updates and backups. A forgotten password manager is worse than one managed by others: A strong password and a password manager.

Getting started

1

Have a domain with HTTPS in front of the server: **HTTPS for a container.**

2

Create the compose.yaml file in a folder of its own: `services:`

```
vaultwarden:
  image: vaultwarden/server:latest
  restart: unless-stopped
  environment:
    DOMAIN: "https://vault.your-domain.com"
    SIGNUPS_ALLOWED: "true"
  ports:
    - "127.0.0.1:8080:80"
  volumes:
    - ./data:/data
```

3

Start it (`docker compose up -d`) and make the domain's proxy point to port 8080: **Nginx in front of a container.**

4

Create the accounts you need and then change SIGNUPS_ALLOWED to "false" and start the container again. Turn on two-step verification on each account.

5

Copy the data folder regularly, away from the server, and test a restore: **Encrypted backups with restic.**

This is the vault of your digital life. If the server is broken into or the data folder is lost with no copy, you lose the passwords to everything. Keep the VPS secure and up to date, and use two-step verification. **Keeping your VPS secure.**

Before you start, ask yourself whether a password manager from a service, run by others, would not suit you better. On two-step verification: **Which two-step verification to use.**

Want help judging whether it is worth setting up your own password vault?
Open a ticket.

[Open a support ticket](#)

SEE ALSO

[A strong password and a password manager: how to stop reusing the same one](#)

[HTTPS for a container: a certificate and a domain](#)

[Nginx as a reverse proxy in front of a container](#)

[Encrypted backups of a VPS with restic: a first repository, a schedule, a test restore](#)

[Keeping your VPS or dedicated server secure: the six that matter](#)

[Authenticator app, SMS or security key: which two-step verification to use](#)



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

FOUNDED

37,000+

CLIENTS

130+

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