

Paris, 2 Rue du Pont Neuf, 75001 Paris. 04 44 44 44 contact@elibanque.fr

# Gestionaire de MDP - Vaultwarden

## Table des matières

I/ Choix du service de gestion centralisé	3
II/ Déploiement d'un docker	
III/ Création d'un compte	
•	
IV/ Création d'un coffre partagé et partage	
V/ Installation de l'extension	8

#### I/ Choix du service de gestion centralisé

Vaultwarden est souvent choisi parmi les solutions open source en raison de sa flexibilité et de ses fonctionnalités avancées adaptées aux environnements professionnels. L'une de ses forces majeures est sa capacité à s'intégrer avec Active Directory Domain Services (ADDS), permettant une gestion centralisée des utilisateurs et une authentification simplifiée via les comptes existants de l'organisation. Cela élimine le besoin de créer et de gérer des comptes séparés pour chaque utilisateur, tout en assurant une sécurité robuste grâce à des mécanismes d'authentification éprouvés.

De plus, Vaultwarden permet l'exportation de données de manière chiffrée, ce qui garantit que les informations sensibles restent protégées, même lorsqu'elles sont transférées ou sauvegardées. Ces fonctionnalités, combinées à une empreinte légère et une facilité de déploiement grâce à Docker, font de Vaultwarden un choix idéal pour les utilisateurs recherchant une alternative fiable et sécurisée à des solutions commerciales.

Enfin, Vaultwarden prend en charge l'exportation des données dans plusieurs formats, ce qui le rend compatible avec différents outils et plateformes. Les utilisateurs peuvent ainsi choisir le format qui convient le mieux à leurs besoins, que ce soit pour une migration, une sauvegarde, ou un audit. Ces exports, tout en étant flexibles, restent sécurisés grâce à la possibilité de les chiffrer, assurant ainsi la confidentialité des informations même lors de leur transfert ou stockage externe.









### II/ Déploiement d'un docker

```
...
                                  docker-compose.yml
services:
  traefik:
    image: "traefik:v3.2"
    container_name: "traefik"
    networks:
      - traefik_network
      - vault_network
    command:
        "--log.level=DEBUG"
      - "--api.dashboard=true"
      - "--providers.docker.exposedbydefault=false"
      - "--entrypoints.web.address=:80'
      - "--entrypoints.web.http.redirections.entryPoint.to=websecure"
      - "--entrypoints.web.http.redirections.entryPoint.scheme=https"
      - "--entrypoints.websecure.address=:443"
      - "--entrypoints.websecure.http.tls=true"
      - "--entrypoints.websecure.http.tls.certResolver=default"
      - "--providers.file.directory=/etc/traefik/dynamic"
      - "--providers.file.watch=true"
    ports:
      - "80:80"
- "443:443"
    volumes:
      - "/var/run/docker.sock:/var/run/docker.sock:ro"
      - "./dynamic:/etc/traefik/dynamic:ro"
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.traefik.rule=Host(`traefik.elibanque.fr`)"
      - "traefik.http.routers.traefik.service=api@internal"
      - "traefik.http.routers.traefik.entrypoints=websecure"
      - "traefik.http.routers.traefik.tls=true"
  vaultwarden:
    image: vaultwarden/server:latest
    container_name: vaultwarden
    restart: unless-stopped
    networks:
       vault_network
    volumes:
      - vaultwarden-data:/data:rw
    environment:
      - ADMIN_TOKEN=${VAULTWARDEN_ADMIN_TOKEN}
      - WEBSOCKET_ENABLED="true"
    labels:
      - "traefik.docker.network=vault_network"
      - "traefik.http.routers.vaultwarden.rule=Host(`pwd.elibanque.fr`)"
      - "traefik.http.routers.vaultwarden.entrypoints=websecure"
      - "traefik.http.routers.vaultwarden.tls=true"
      - "traefik.http.services.vaultwarden-service.loadbalancer.server.port=80"
  vaultwarden-data:
networks:
  traefik_network:
    name: traefik_network
    external: true
  vault_network:
    name: vault_network
    external: true
```

28/11/2024

Ce fichier docker-compose.yml configure le déploiement de Traefik en tant que reverse proxy et de Vaultwarden, avec une intégration fluide via des réseaux Docker externes.

Le service Traefik gère les connexions HTTP et HTTPS en mettant en place des redirections automatiques vers HTTPS. Il utilise un résolveur de certificats TLS nommé default pour sécuriser les connexions. Les configurations dynamiques supplémentaires, comme des règles personnalisées, peuvent être définies dans le dossier ./dynamic. Traefik expose également un tableau de bord accessible via le domaine traefik.elibanque.fr en HTTPS, facilitant la gestion et la surveillance. L'utilisation des réseaux traefik\_network et vault\_network garantit une communication efficace entre Traefik et les autres services.

Le service Vaultwarden, quant à lui, est accessible via le domaine pwd.elibanque.fr, avec un routage géré par Traefik. Les données de Vaultwarden sont rendues persistantes grâce au volume nommé vaultwarden-data, qui stocke toutes les informations de manière durable. La connexion HTTPS est assurée via le reverse proxy de Traefik, qui centralise la gestion de la sécurité. Les labels ajoutés à Vaultwarden spécifient le routage, les réseaux et les points d'entrée pour assurer une intégration complète et sécurisée.

Ensemble, ces services offrent une solution robuste et extensible pour un environnement Docker, avec un reverse proxy centralisé et une application spécialisée fonctionnant de manière harmonieuse.

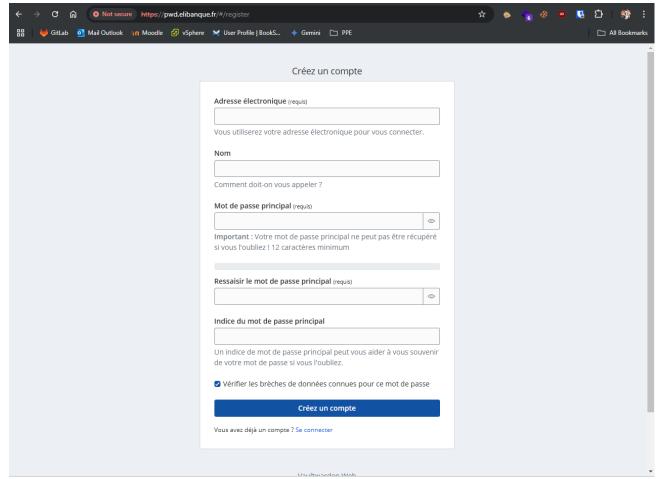
Le mot de passe ADMIN\_TOKEN sera défini par ça :

echo -n "LeMotDePasseTresTresSecret" | argon2 "\$(openssI rand -base64 32)" -e -id -k 65540 -t 3 -p 4

soit:

\$argon2id\$v=19\$m=65540,t=3,p=4\$QjdoSERJRIN3SWRjcGI4OXo1M3E4QWxKdHVEQzhId1RVWnJ1WkxlRmpZOD0\$aeEKHxqwxVAxPD7nqAspAfOw9fzLK9UDaOOQTMgLtBE

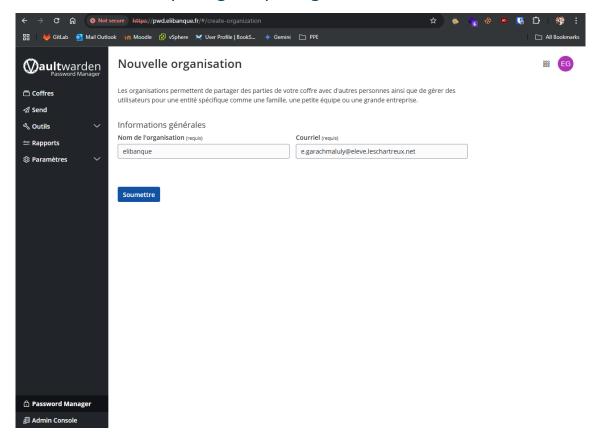
## III/ Création d'un compte

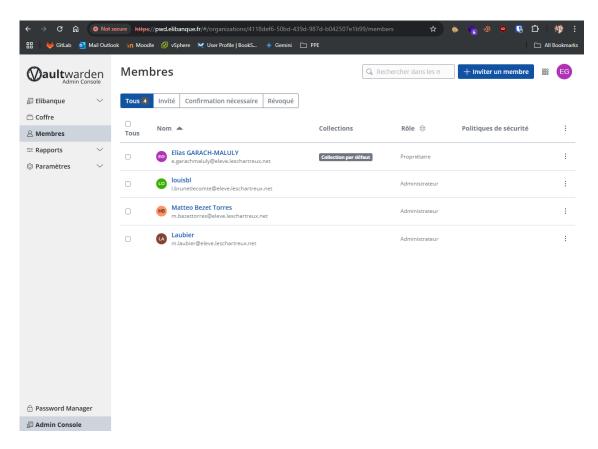


Adresse électronique : Adresse e-mail Chartreux

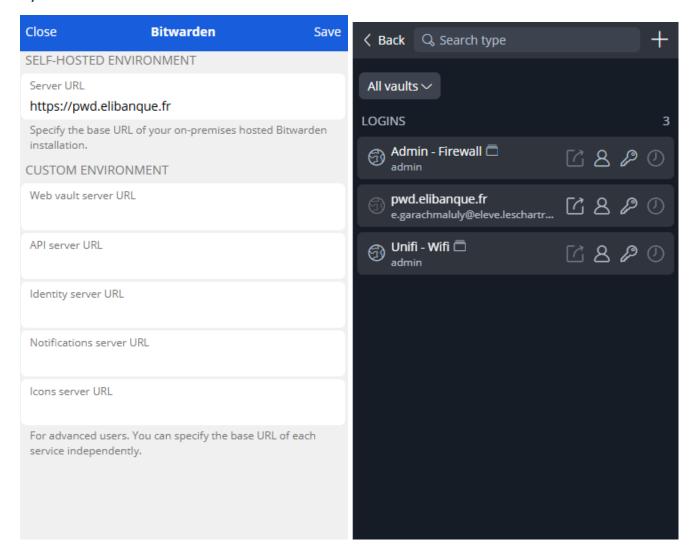
Nom: Nom de la personne

## IV/ Création d'un coffre partagé et partage





### V/ Installation de l'extension



#### Server URL: <a href="https://pwd.elibanque.fr">https://pwd.elibanque.fr</a>

Puis nous devons nous connecter en vérifiant que nous avons bien gardé l'option « auto-hébergé ».

Nous tombons sur nos clés partagées.