

Ajouter un utilisateur

Vaultwarden : ajouter un utilisateur

Service	Vaultwarden (Docker)
Objet	Création d'un compte utilisateur sur une instance aux inscriptions fermées
Prérequis	Accès SSH au serveur, accès au fichier <code>docker-compose.yml</code>
Durée estimée	5 à 10 minutes

1. Principe

Les inscriptions publiques sont fermées (`SIGNUPS_ALLOWED=false`). Un nouvel utilisateur ne peut donc créer son compte qu'après avoir été **invité**.

Trois méthodes sont possibles :

Méthode	Usage	Recommandée
Panneau d'administration	Cas général	☐
Ouverture temporaire des inscriptions	Dépannage, panneau admin indisponible	⚠
Invitation dans une organisation	Partage de coffre (famille, équipe)	☐

2. Méthode A : via le panneau d'administration

2.1 Activer le panneau admin (si nécessaire)

Le panneau n'est accessible que si `ADMIN_TOKEN` est défini.

1. Générer un hash Argon2 du mot de passe admin :

```
docker exec -it vaultwarden /vaultwarden hash
```

2. Ajouter le hash dans `docker-compose.yml`. **Doubler chaque `$`**, car ce caractère est interprété par Docker Compose :

```
services:
  vaultwarden:
    environment:
      ADMIN_TOKEN: '$$argon2id$$v=19$$m=65540,t=3,p=4$$...
```

3. Appliquer la configuration :

```
docker compose up -d
```

2.2 Inviter l'utilisateur

1. Ouvrir `https://<domaine>/admin` et s'authentifier avec le mot de passe admin (en clair, pas le hash).
2. Aller dans l'onglet **Users**.
3. Dans **Invite User**, saisir l'adresse e-mail de l'utilisateur, puis valider.

2.3 Création du compte par l'utilisateur

Le parcours dépend de la configuration SMTP :

- **SMTP configuré** : l'utilisateur reçoit un e-mail d'invitation et suit le lien.

- **SMTP non configuré** : l'invitation est acceptée automatiquement. Communiquer à l'utilisateur :
 - l'URL de l'instance : `https://<domaine>`
 - l'**adresse e-mail exacte** utilisée pour l'invitationL'utilisateur clique sur **Créer un compte** et s'inscrit avec cette adresse.

2.4 Vérification

Dans **Users** du panneau admin, l'utilisateur apparaît avec son compte créé (et non plus en statut *Invited*).

3. Méthode B : ouverture temporaire des inscriptions

⚠ Pendant la fenêtre d'ouverture, **n'importe qui** pouvant joindre l'instance peut créer un compte. À réserver au dépannage, et à refermer immédiatement.

1. Dans `docker-compose.yml` :

```
SIGNUPS_ALLOWED: 'true'
```

2. Appliquer : `docker compose up -d`
3. Laisser l'utilisateur créer son compte.
4. Remettre `SIGNUPS_ALLOWED: 'false'` et réappliquer : `docker compose up -d`
5. Vérifier dans le panneau admin qu'aucun compte inattendu n'a été créé.

Variante plus restrictive : limiter les inscriptions à un domaine e-mail :

```
SIGNUPS_DOMAINS_WHITELIST: 'mondomaine.fr'
```

4. Méthode C : invitation dans une organisation

Pour un utilisateur qui doit accéder à un coffre partagé.

Prérequis : `INVITATIONS_ALLOWED` à `true` (valeur par défaut).

1. Se connecter au coffre web avec un compte propriétaire ou administrateur de l'organisation.
 2. Aller dans **Organisation**, puis **Membres**, puis **Inviter un membre**.
 3. Saisir l'e-mail, choisir le rôle et les collections accessibles.
 4. Une fois que l'utilisateur a créé son compte et accepté l'invitation, **confirmer** le membre dans la liste des membres. Sans cette confirmation, il n'a pas accès aux éléments partagés.
-

5. Points d'attention

`config.json` prioritaire sur les variables d'environnement

Dès qu'un réglage est enregistré depuis le panneau admin, Vaultwarden écrit un fichier `config.json` dans le volume `/data`. **Ce fichier prend le dessus sur les variables du `docker-compose.yml`.**

Symptôme : une variable modifiée dans le compose semble ignorée. Solution : modifier le réglage depuis le panneau admin, ou supprimer la clé concernée dans `config.json` puis redémarrer le conteneur.

Sécurisation du panneau admin

Après l'opération, au choix :

- **Désactiver le panneau** : retirer `ADMIN_TOKEN` du compose et supprimer la clé `admin_token` dans `config.json` si elle y figure, puis `docker compose up -d`.
 - **Restreindre l'accès** au chemin `/admin` au niveau du reverse proxy (accès via VPN ou réseau local uniquement).
-

6. Récapitulatif rapide

1. `https://<domaine>/admin` → Users → Invite User → e-mail
 2. Transmettre URL + e-mail exact à l'utilisateur
 3. L'utilisateur crée son compte avec cet e-mail
 4. Vérifier dans Users
 5. Re-sécuriser /admin si besoin
-

Revision #1

Created 2026-10-13 21:52:48 UTC by gpatruno

Updated 2026-10-13 21:53:03 UTC by gpatruno