

## Mode Opérateur

# Utilisation quotidienne de Vaultwarden

**Code :** MO-PLT-006  
**Version :** 1.0  
**Date :** 6 avril 2026  
**Auteur :** Cédric LEGRAND  
**Classification :** USAGE INTERNE — Équipe BTS SIO

## Historique des révisions

Version	Date	Modifications
1.0	06/04/2026	Création initiale

## 1 Objet

Ce mode opératoire décrit les opérations courantes que chaque membre de l'équipe est amené à réaliser au quotidien dans **Vaultwarden**, le gestionnaire de mots de passe de l'infrastructure BTS SIO : rechercher un identifiant, copier des informations de connexion, modifier une entrée existante et générer des mots de passe robustes.

Il s'adresse aux utilisateurs disposant déjà d'un compte et d'un accès à l'organisation (cf. MO-PLT-002). L'objectif est de permettre une prise en main rapide du coffre-fort, que ce soit via l'interface web ou l'extension navigateur.

## 2 Champ d'application

<b>Public concerné</b>	Tous les membres de l'équipe pédagogique BTS SIO
<b>Systèmes</b>	Coffre-fort web Vaultwarden ( <a href="https://10.0.112.10">https://10.0.112.10</a> ), extension navigateur Bitwarden
<b>Durée estimée</b>	Environ 2 minutes par opération

## 3 Prérequis

### Prérequis

- Un compte Vaultwarden actif avec appartenance à l'organisation (cf. MO-PLT-002)
- Un navigateur web récent (Firefox, Chrome, Edge)
- Accès au réseau de l'établissement (VLAN administration ou VPN)
- Connaître son adresse email et son mot de passe maître

## 4 Procédure

## 4.1 Se connecter au coffre-fort

### Étape 1 — Ouvrir le coffre-fort Vaultwarden

Ouvrir un navigateur et se rendre à l'adresse :

`https://10.0.112.10`

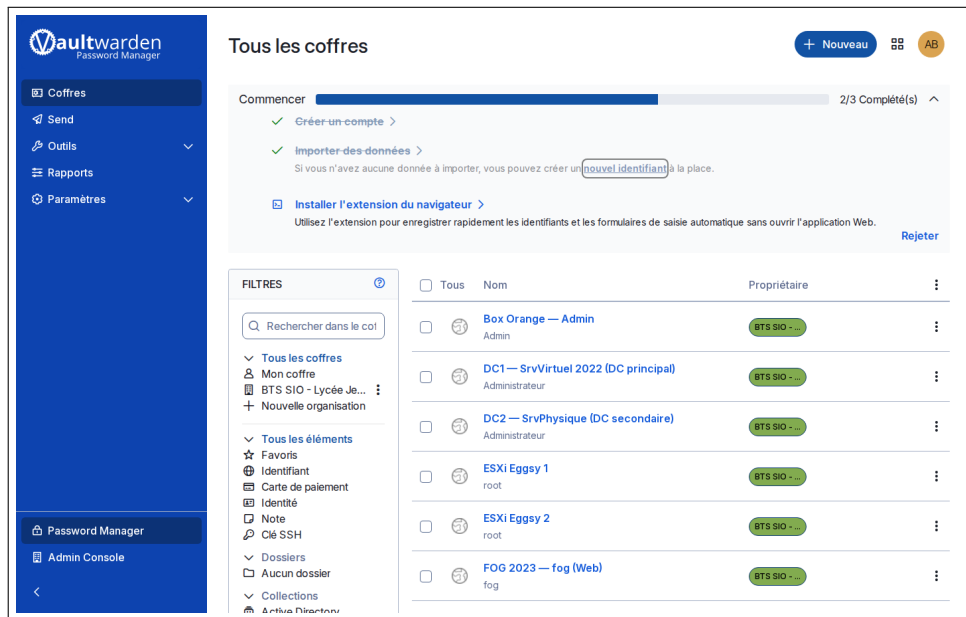
Saisir l'adresse email et le mot de passe maître, puis cliquer sur **Se connecter**.

### Étape 2 — Accéder au coffre de l'organisation

Une fois connecté, la barre latérale gauche affiche le coffre personnel ainsi que l'organisation et ses collections. Cliquer sur le nom de l'organisation pour afficher l'ensemble des entrées partagées.

### Étape 3 — Vérifier l'accès

Le coffre principal s'affiche avec la liste des entrées classées par collection. Si aucune entrée n'apparaît, vérifier que votre compte est bien membre de l'organisation (cf. section Dépannage).



The screenshot displays the Vaultwarden Password Manager interface. On the left is a blue sidebar with navigation options: Coffres, Send, Outils, Rapports, Paramètres, Password Manager, and Admin Console. The main area is titled 'Tous les coffres' and shows a progress bar for 'Commencer' (2/3 Complété(s)). Below this are instructions for creating an account, importing data, and installing a browser extension. A 'FILTRES' section on the left allows searching and filtering collections. The main list shows several collections:

<input type="checkbox"/>	Nom	Propriétaire
<input type="checkbox"/>	Box Orange — Admin Admin	BTS SIO
<input type="checkbox"/>	DC1 — SrvVirtual 2022 (DC principal) Administrateur	BTS SIO
<input type="checkbox"/>	DC2 — SrvPhysique (DC secondaire) Administrateur	BTS SIO
<input type="checkbox"/>	ESXi Eggsy 1 root	BTS SIO
<input type="checkbox"/>	ESXi Eggsy 2 root	BTS SIO
<input type="checkbox"/>	FOG 2023 — fog (Web) fog	BTS SIO

Figure 1 — Vue principale du coffre avec les collections de l'organisation

## 4.2 Rechercher une entrée

### Étape 1 — Utiliser la barre de recherche

La barre de recherche en haut de l'interface permet de retrouver rapidement un identifiant. Saisir un mot-clé (nom de l'équipement, adresse IP, nom d'utilisateur) pour filtrer les résultats en temps réel.

### Étape 2 — Filtrer par collection

Pour restreindre l'affichage à un domaine précis, cliquer sur une collection dans la barre latérale gauche (par exemple « Active Directory » ou « Réseau »). Seules les entrées de cette collection s'affichent alors.

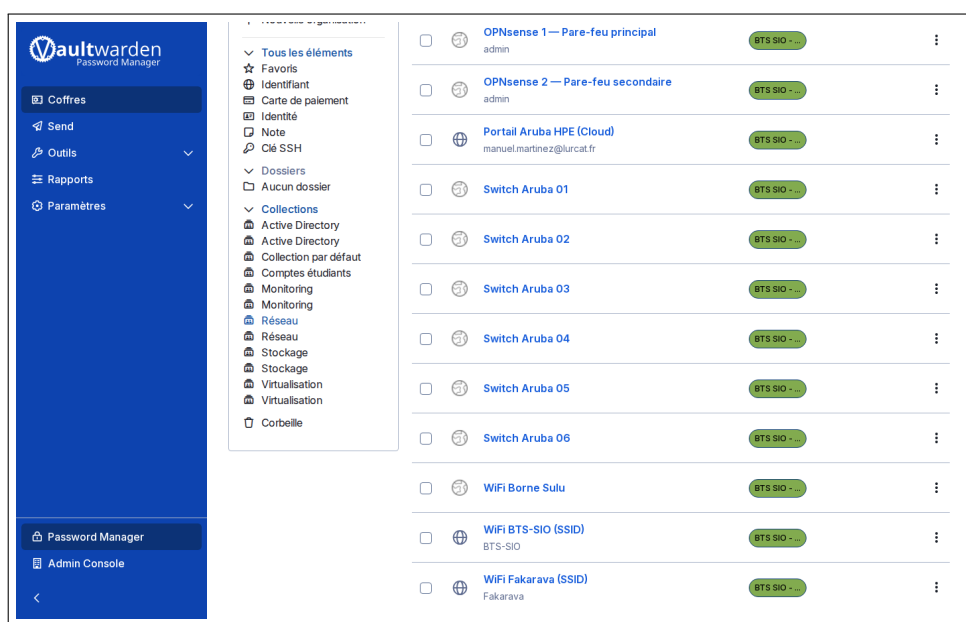


Figure 2 – Filtrage des entrées par collection dans la barre latérale

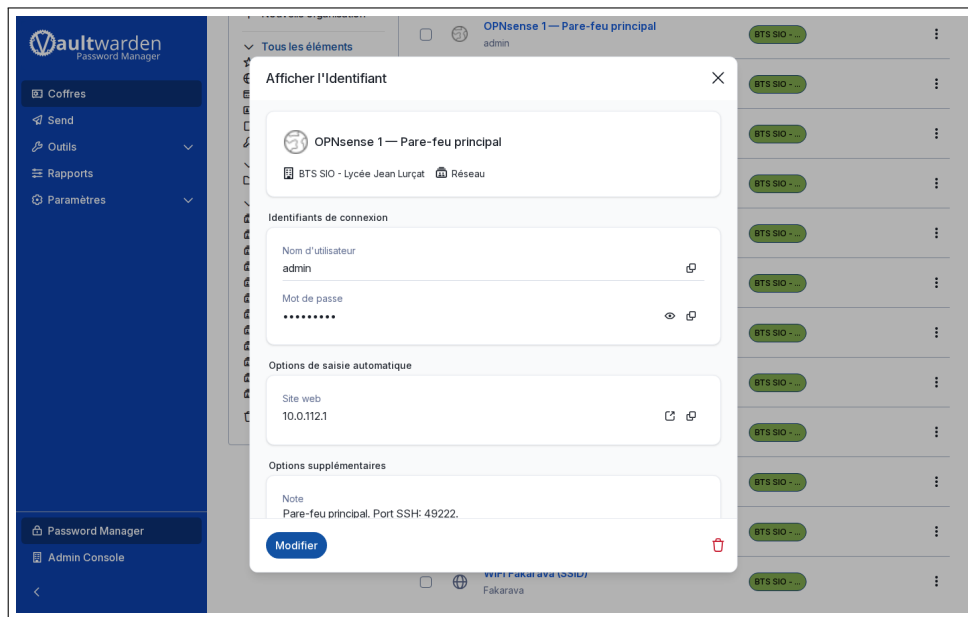
### Note

La recherche porte sur le nom de l'entrée, l'identifiant et les URI. Pour retrouver un mot de passe dont on ne connaît que l'adresse IP, il suffit de la saisir dans la barre de recherche.

### 4.3 Copier des identifiants

#### Étape 1 — Ouvrir le détail d'une entrée

Cliquer sur l'entrée souhaitée dans la liste. Le panneau de détail s'ouvre à droite et affiche les champs : nom, identifiant, mot de passe (masqué par défaut), URI et éventuelles notes.

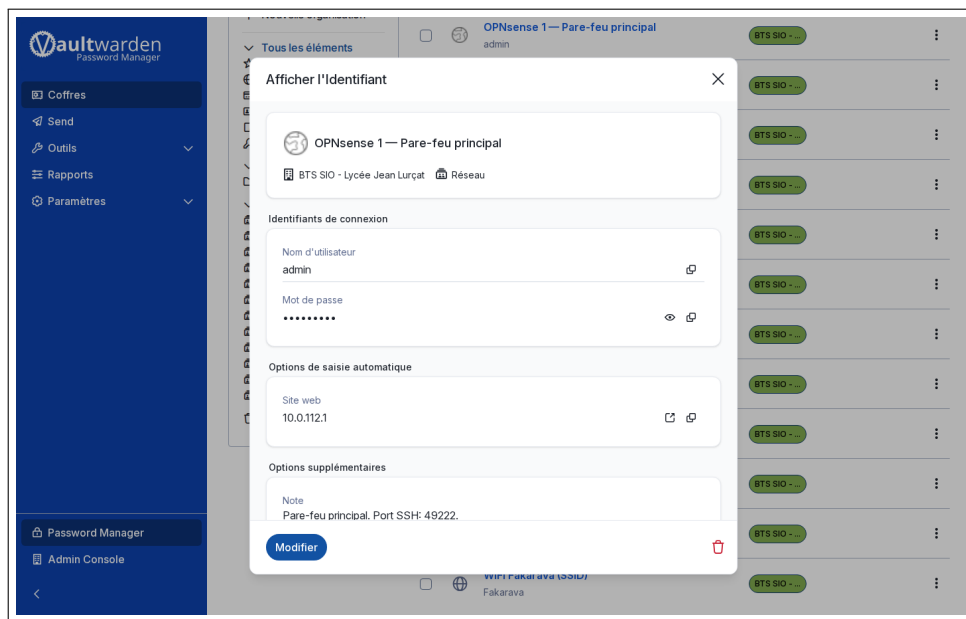


**Figure 3** – Détail d'une entrée avec les champs identifiant et mot de passe

## Étape 2 — Copier l'identifiant ou le mot de passe

Utiliser les boutons de copie situés à droite de chaque champ :

- Cliquer sur l'icône de copie à côté du champ *Identifiant* pour copier le nom d'utilisateur ;
- Cliquer sur l'icône de copie à côté du champ *Mot de passe* pour copier le mot de passe.



**Figure 4** – Boutons de copie rapide pour l'identifiant et le mot de passe

Le contenu est placé dans le presse-papiers. Le coller directement dans le formulaire de connexion du système cible (Ctrl+V ou clic droit → Coller).

### **!** Attention

Le presse-papiers est automatiquement vidé après 20 secondes par défaut. Ce délai est configurable dans les paramètres de Vaultwarden. Ne pas stocker de mots de passe dans un fichier texte : toujours utiliser le coffre.

## 4.4 Modifier une entrée existante

### Étape 1 — Ouvrir l'entrée à modifier

Cliquer sur l'entrée concernée dans la liste du coffre pour afficher son détail.

### Étape 2 — Passer en mode édition

Cliquer sur le bouton **Modifier** (ou l'icône crayon) en haut du panneau de détail. Les champs deviennent alors éditables.

### Étape 3 — Modifier les champs souhaités

Mettre à jour les informations nécessaires :

- *Nom* : renommer l'entrée si besoin
- *Identifiant* : modifier le nom d'utilisateur
- *Mot de passe* : saisir le nouveau mot de passe (ou utiliser le générateur, cf. section 4.5)
- *URI* : corriger ou ajouter des adresses d'accès
- *Notes* : ajouter des informations complémentaires (port SSH, chemin d'accès, etc.)

### Étape 4 — Enregistrer les modifications

Cliquer sur **Enregistrer** pour sauvegarder. Les modifications sont immédiatement disponibles pour tous les membres ayant accès à la collection.

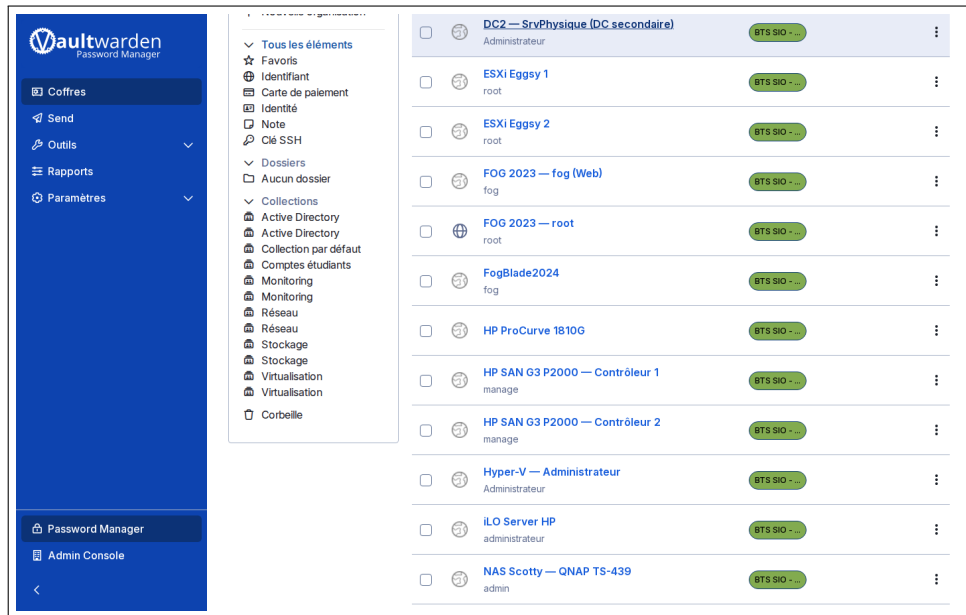
### Note

Vaultwarden conserve un historique des mots de passe précédents. En cas d'erreur, il est possible de retrouver l'ancien mot de passe dans l'onglet **Historique** de l'entrée.

## 4.5 Utiliser le générateur de mots de passe

### Étape 1 — Accéder au générateur

Depuis la barre de navigation principale, cliquer sur **Outils** puis **Générateur** (ou **Tools** → **Generator**). Le générateur s'ouvre avec les options de configuration.



**Figure 5** — Générateur de mots de passe avec les options de longueur et de complexité

### Étape 2 — Configurer les options

Ajuster les paramètres selon le besoin :

- *Longueur* : 16 caractères minimum recommandé (20+ pour les comptes critiques)
- *Majuscules* : activé
- *Minuscules* : activé
- *Chiffres* : activé
- *Caractères spéciaux* : activé (sauf restriction du système cible)

### Étape 3 — Copier le mot de passe généré

Cliquer sur le bouton **Copier** pour placer le mot de passe dans le presse-papiers, puis l'utiliser dans le formulaire de changement de mot de passe du système cible.

### Astuce

Lors de la modification d'une entrée (section 4.4), un bouton de génération est directement disponible à côté du champ *Mot de passe*. Il n'est pas nécessaire de passer par le menu **Outils** dans ce cas : cliquer sur l'icône de régénération à côté du champ pour générer et insérer un nouveau mot de passe en une seule opération.

## 4.6 Paramètres du compte

### Étape 1 — Accéder aux paramètres

Cliquer sur l'icône de profil en haut à droite, puis sélectionner **Paramètres du compte** (ou **Account Settings**).

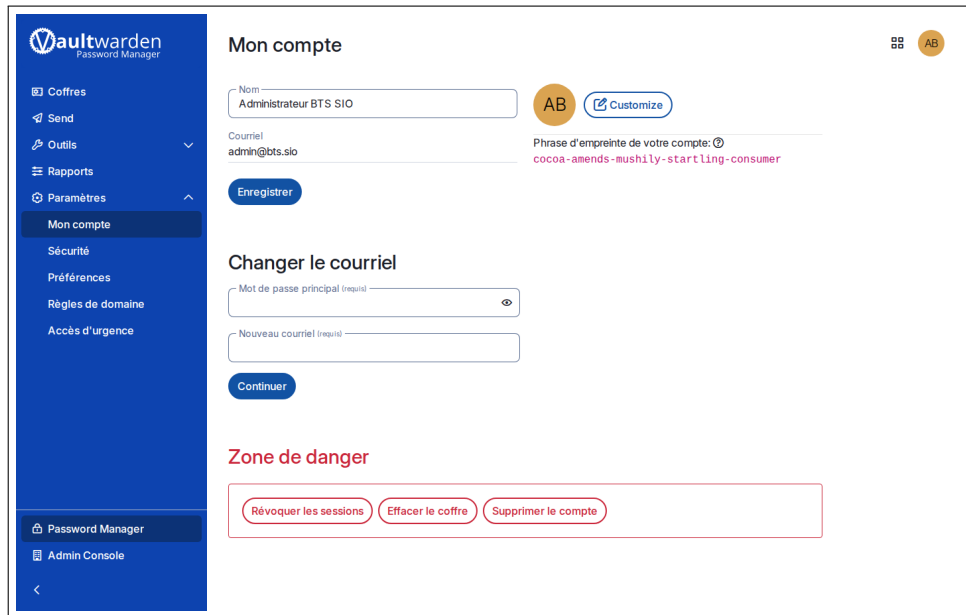


Figure 6 – Page des paramètres du compte utilisateur

### Étape 2 — Changer le mot de passe maître

Dans l'onglet **Sécurité**, section **Mot de passe maître** :

- Saisir le mot de passe maître actuel
- Saisir le nouveau mot de passe maître (différent de tout autre mot de passe)
- Confirmer le nouveau mot de passe
- Cliquer sur **Modifier le mot de passe**

### Étape 3 — Activer l'authentification à deux facteurs (2FA)

Toujours dans l'onglet **Sécurité**, section **Connexion en deux étapes** :

- Choisir une méthode (application d'authentification TOTP recommandée)
- Scanner le QR code avec une application type FreeOTP ou Aegis
- Saisir le code de vérification pour confirmer l'activation
- Conserver le code de récupération dans un endroit sûr (hors coffre)

#### Attention

Le mot de passe maître ne peut **pas** être réinitialisé par l'administrateur. En cas d'oubli, le coffre personnel est définitivement perdu. Choisir un mot de passe maître robuste et mémorisable, par exemple sous forme de phrase de passe (4 mots aléatoires minimum).

## 5 Bonnes pratiques

- **Verrouiller le coffre** en quittant le poste de travail : cliquer sur l'icône de profil → **Verrouiller** (ou fermer le navigateur).
- **Ne jamais partager le mot de passe maître** : c'est la clé de chiffrement de l'ensemble du coffre. Si un collègue a besoin d'un accès, l'ajouter à l'organisation (cf. MO-PLT-002).
- **Utiliser systématiquement le générateur** pour tout nouveau mot de passe : 16 caractères minimum, avec majuscules, chiffres et caractères spéciaux.
- **Signaler toute activité suspecte** (connexion non reconnue, entrée modifiée sans raison) à l'administrateur de la plateforme.
- **Ne pas dupliquer les identifiants** : un même mot de passe ne doit pas être réutilisé sur plusieurs systèmes. Le générateur est là pour éviter cette mauvaise habitude.

## 6 Vérification

### Vérification

Après avoir pris en main les opérations décrites ci-dessus, vérifier les points suivants :

- La connexion au coffre-fort fonctionne avec vos identifiants
- La recherche permet de retrouver une entrée par mot-clé
- Le filtrage par collection affiche uniquement les entrées du domaine sélectionné
- La copie d'un identifiant et d'un mot de passe fonctionne (coller dans un éditeur de texte pour vérifier)
- Le générateur de mots de passe produit des mots de passe conformes aux critères définis
- L'accès aux paramètres du compte est possible

## 7 Dépannage

---

Problème	Solution
Page de connexion inaccessible	Vérifier la connexion au réseau de l'établissement (VLAN administration ou VPN actif). Tester l'accès à <code>https://10.0.112.10</code> dans le navigateur.
Mot de passe maître refusé	Vérifier l'absence de verrouillage des majuscules (Caps Lock). Si le mot de passe est oublié, contacter l'administrateur : le compte devra être recréé (le coffre personnel est perdu).
Aucune entrée visible dans le coffre	Vérifier que votre compte est bien membre de l'organisation et des collections concernées. Contacter l'administrateur pour vérification (cf. MO-PLT-002).
La copie ne fonctionne pas	Certains navigateurs bloquent l'accès au presse-papiers. Autoriser le site dans les paramètres du navigateur ( <b>Autorisations</b> → <b>Presse-papiers</b> ). En dernier recours, cliquer sur l'icône « œil » pour afficher le mot de passe et le copier manuellement.
Le générateur n'est pas accessible	Vérifier que le menu <b>Outils</b> est bien visible dans la barre de navigation. Sur l'extension navigateur, le générateur est accessible via l'onglet dédié en bas de la fenêtre.
Code 2FA refusé	Vérifier que l'heure du téléphone est synchronisée (les codes TOTP dépendent de l'horloge). Si le problème persiste, utiliser le code de récupération et reconfigurer le 2FA.

---