Mode Opératoire

Installer le client Vaultwarden (Bitwarden)

Code :	MO-PLT-004
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 l'installation et la configuration des **clients Bitwarden** sur les différentes plateformes utilisées par l'équipe : extension de navigateur, application de bureau et application mobile. Les clients Bitwarden sont pleinement compatibles avec le serveur **Vaultwarden** déployé sur l'infrastructure BTS SIO.

L'objectif est de permettre à chaque membre de l'équipe d'accéder au coffre-fort partagé depuis n'importe quel poste de travail ou terminal mobile, y compris en situation de mobilité via le VPN WireGuard.

2 Champ d'application

Public concerné	Tous les membres de l'équipe pédagogique BTS SIO
Systèmes	Windows, Linux, macOS (navigateur et bureau) — iOS, Android (mobile)
Durée estimée	10 minutes environ par plateforme

3 Prérequis

Prérequis

— Un compte Vaultwarden actif avec adresse email et mot de passe maître (cf. MO-PLT-002)
— Accès au réseau de l'établissement (VLAN administration ou VPN WireGuard)
— Un navigateur web récent (Firefox ou Chrome/Chromium) pour l'extension
— Droits d'installation sur le poste de travail (pour l'application de bureau)

4 Procédure

4.1 Installer l'extension de navigateur

Étape 1 — Accéder au magasin d'extensions

Ouvrir le navigateur et se rendre sur le magasin d'extensions correspondant :

— **Firefox** : `https://addons.mozilla.org`

— **Chrome / Chromium / Edge** : `https://chrome.google.com/webstore`

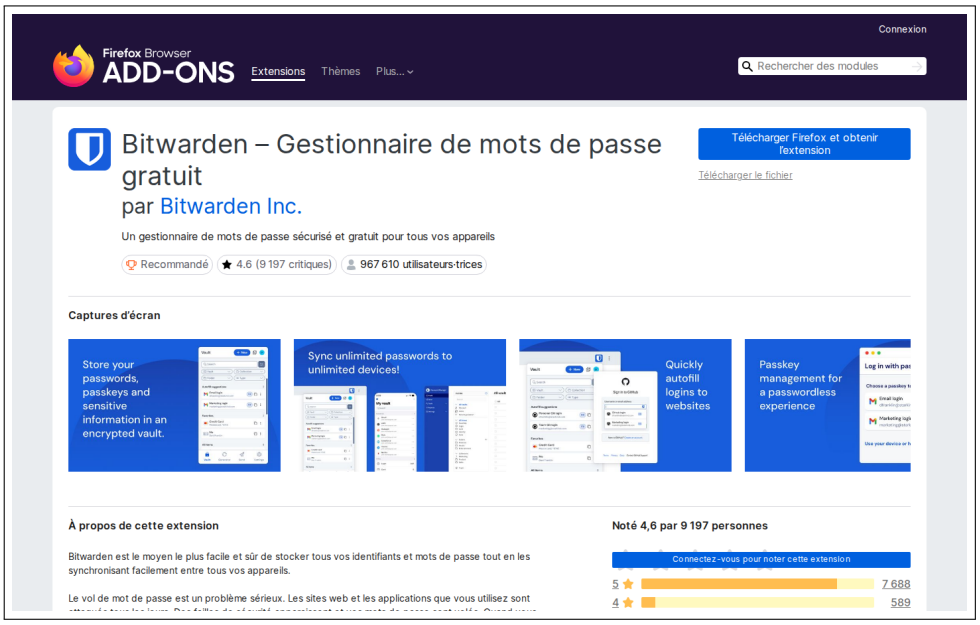

Figure 1 – Magasin d'extensions Firefox (addons.mozilla.org)

Étape 2 — Rechercher et installer l'extension Bitwarden

Dans la barre de recherche du magasin, taper « Bitwarden » puis sélectionner l'extension officielle **Bitwarden – Free Password Manager**. Cliquer sur **Ajouter à Firefox** (ou **Ajouter à Chrome** selon le navigateur).

Figure 2 – Extension Bitwarden dans le Chrome Web Store

⚠ Configuration obligatoire avant connexion

L'URL du serveur auto-hébergé **doit impérativement être configurée avant toute tentative de connexion**. Sans cette étape, le client tentera de se connecter aux serveurs cloud de Bitwarden et l'authentification échouera.

Étape 3 — Configurer l'URL du serveur auto-hébergé

Une fois l'extension installée, cliquer sur son icône dans la barre d'outils du navigateur. Sur l'écran de connexion, cliquer sur l'icône d'engrenage (paramètres) ou sur le lien **Se connecter à un serveur auto-hébergé**.

Dans le champ *URL du serveur*, saisir :

```
https://10.0.112.10
```

Valider en cliquant sur **Enregistrer**.

Note

Le serveur utilise un certificat auto-signé. Le navigateur peut afficher un avertissement de sécurité lors de la première connexion : accepter le certificat pour poursuivre. Ce comportement est normal dans le contexte d'un déploiement interne.

Étape 4 — Se connecter au coffre-fort

Saisir l'adresse email associée au compte Vaultwarden ainsi que le mot de passe maître, puis cliquer sur **Se connecter**.

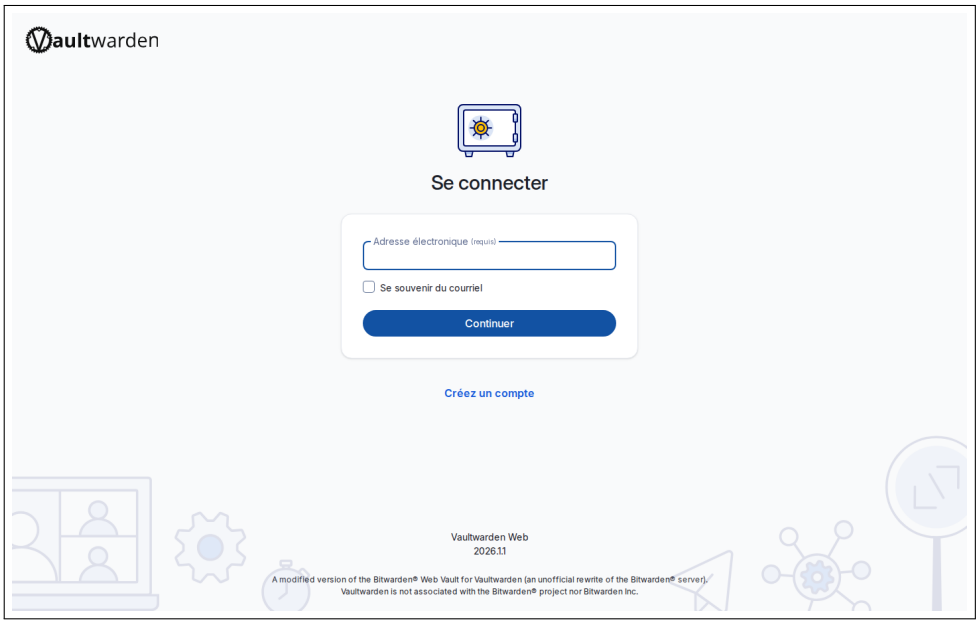

Figure 3 – Écran de connexion Vaultwarden

Étape 5 — Vérifier l'accès au coffre

Après connexion, cliquer sur l'icône de l'extension dans la barre d'outils. Le coffre-fort s'affiche avec les identifiants et les collections de l'organisation.

Astuce

L'extension remplit automatiquement les champs de connexion sur les pages web. Lorsqu'un formulaire de connexion est détecté, un badge apparaît sur l'icône de l'extension : cliquer dessus pour pré-remplir les identifiants en un clic.

4.2 Installer l'application de bureau

Étape 1 — Télécharger l'application

Se rendre sur la page de téléchargement officielle :

`https://bitwarden.com/download/`

Sélectionner la version correspondant au système d'exploitation :

— **Windows** : installeur `.exe`

— **Linux** : AppImage ou paquet snap (`sudo snap install bitwarden`)

— **macOS** : fichier `.dmg`

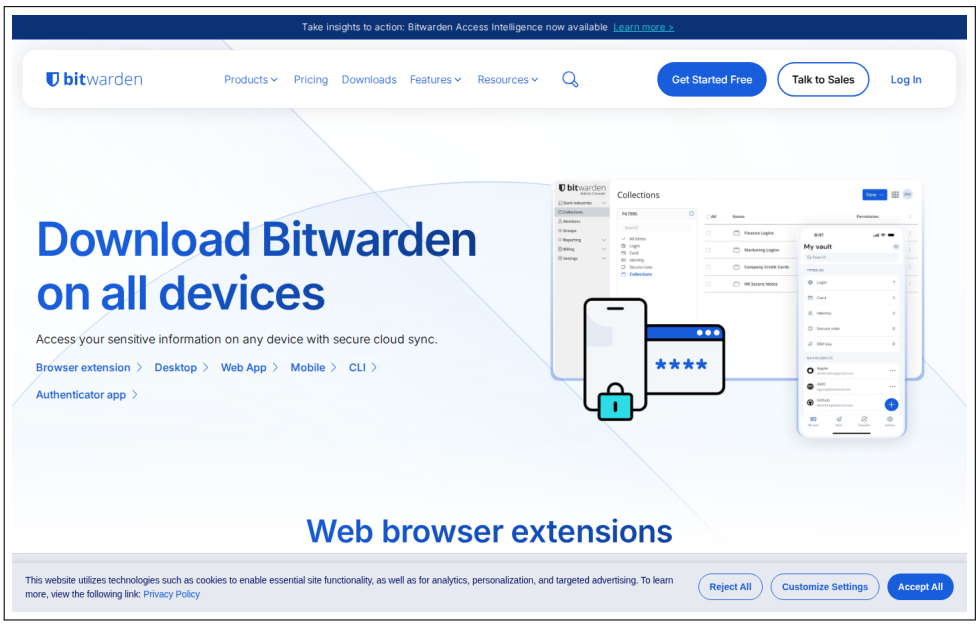

Figure 4 – Page de téléchargement de l'application Bitwarden

Étape 2 — Installer et lancer l'application

Exécuter l'installeur téléchargé et suivre les instructions à l'écran. Sous Linux avec AppImage, rendre le fichier exécutable (`chmod +x Bitwarden-*.AppImage`) puis le lancer.

Étape 3 — Configurer le serveur auto-hébergé

Au premier lancement, **avant de se connecter**, cliquer sur l'icône d'engrenage (paramètres) et renseigner l'URL du serveur :

`https://10.0.112.10`

Enregistrer la configuration.

Étape 4 — Se connecter

Saisir les identifiants (adresse email et mot de passe maître) puis cliquer sur **Se connecter**. Le coffre-fort s'ouvre avec les mêmes données que l'extension de navigateur.

4.3 Installer l'application mobile

Étape 1 — Télécharger l'application depuis le store

Ouvrir le magasin d'applications du terminal mobile :

— **iOS** : App Store

— **Android** : Google Play Store

Rechercher « Bitwarden Password Manager » et installer l'application officielle publiée par *Bitwarden Inc.*

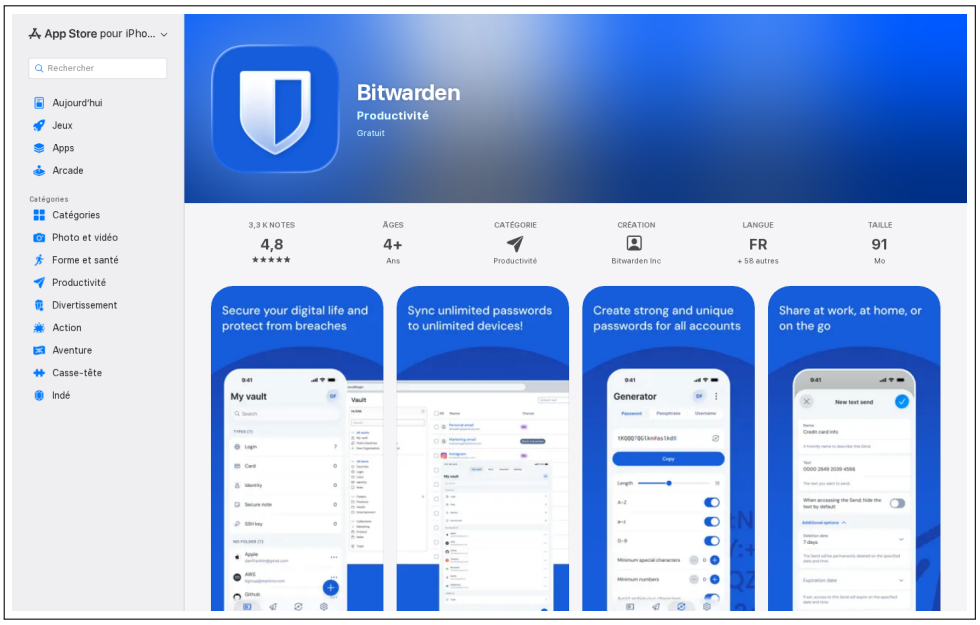

Figure 5 – Bitwarden sur l'App Store (iOS)

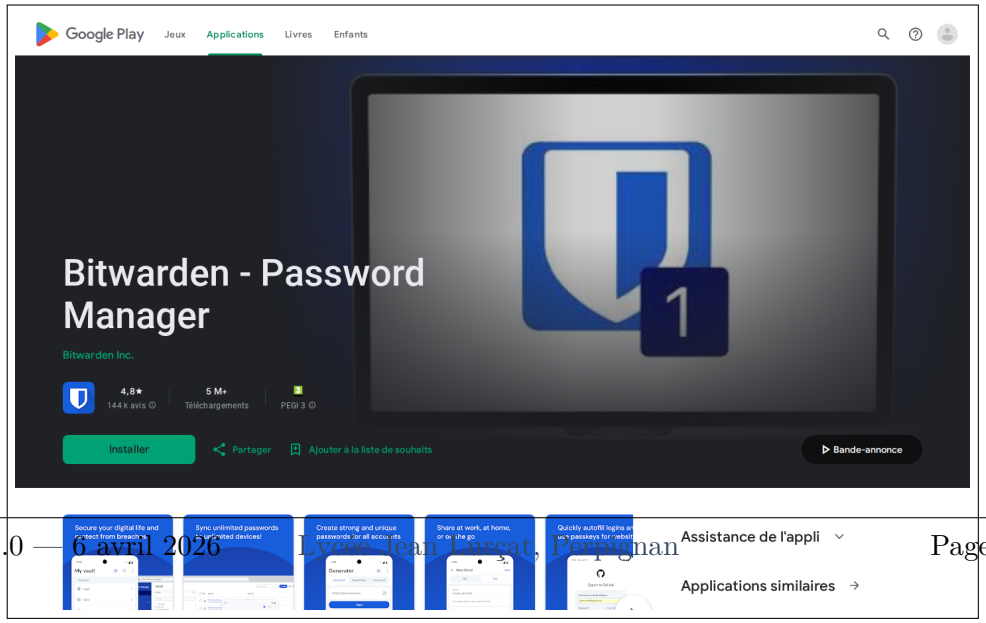

Figure 6 – Bitwarden sur le Google Play Store (Android)

Étape 2 — Configurer le serveur auto-hébergé

Au premier lancement de l'application, **avant de se connecter**, appuyer sur l'icône d'engrenage (coin supérieur gauche) et renseigner l'URL du serveur :

`https://10.0.112.10`

Valider en appuyant sur **Enregistrer**.

Étape 3 — Se connecter

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

Étape 4 — Activer le déverrouillage biométrique

Une fois connecté, accéder à **Paramètres** → **Sécurité du compte** et activer l'option **Déverrouiller avec la biométrie** (Face ID, Touch ID, ou empreinte digitale selon le terminal).
Cette option permet de déverrouiller le coffre rapidement sans ressaisir le mot de passe maître à chaque ouverture de l'application.

Note

L'activation de la biométrie ne remplace pas le mot de passe maître : celui-ci reste nécessaire lors du premier déverrouillage après un redémarrage du terminal ou après un délai d'inactivité prolongé.

Astuce

Pour accéder au coffre-fort depuis l'extérieur de l'établissement, installer l'application **WireGuard** sur le terminal mobile et activer le profil VPN avant d'ouvrir Bitwarden. Le serveur Vaultwarden n'est pas exposé sur Internet et nécessite une connexion au réseau interne.

4.4 Vérifier la connexion au serveur

Étape 1 — Contrôler l'organisation

Après connexion sur n'importe quel client (extension, bureau ou mobile), vérifier que l'organisation « BTS SIO — Lycée Jean Lurçat » apparaît dans la barre latérale ou dans le menu des coffres.

Étape 2 — Vérifier les collections

S'assurer que les collections partagées sont visibles : Active Directory, Réseau, Stockage, Monitoring, Virtualisation, etc. Si aucune collection n'apparaît, vérifier vos droits d'accès auprès de l'administrateur de l'organisation.

Étape 3 — Tester la copie d'un identifiant

Sélectionner une entrée dans le coffre et copier le mot de passe (icône de copie ou clic droit → **Copier le mot de passe**). Vérifier que la copie fonctionne en collant la valeur dans un éditeur de texte. Le presse-papiers est automatiquement vidé après 30 secondes par défaut.

5 Points importants

Rappels essentiels

— L'URL du serveur auto-hébergé (`https://10.0.112.10`) **doit être configurée avant la première connexion** sur chaque client.

— Le certificat du serveur est auto-signé : il faut accepter l'avertissement de sécurité présenté par le navigateur ou l'application.

— Le serveur Vaultwarden est accessible uniquement depuis le réseau de l'établissement ou via le VPN WireGuard — il n'est pas exposé sur Internet.

— Sur mobile, l'application WireGuard doit être connectée avant d'ouvrir Bitwarden en dehors du lycée.

6 Vérification

Vérification

Après avoir suivi la procédure, vérifier les points suivants pour chaque client installé :

☐ L'URL du serveur auto-hébergé est correctement configurée (`https://10.0.112.10`)

☐ La connexion avec l'adresse email et le mot de passe maître fonctionne

☐ L'organisation « BTS SIO — Lycée Jean Lurçat » est visible

☐ Les collections partagées sont accessibles

☐ La copie d'un mot de passe fonctionne correctement

☐ (Mobile) Le déverrouillage biométrique est activé

7 Dépannage

Problème	Solution
Le serveur est injoignable	Vérifier la connectivité réseau (LAN ou VPN). Tester l'accès avec un navigateur : `https://10.0.112.10`. Si le VPN est utilisé, s'assurer que le tunnel WireGuard est actif.
Erreur de certificat	Le serveur utilise un certificat auto-signé. Accepter l'avertissement dans le navigateur. Sur mobile, valider l'exception de sécurité proposée par l'application.
« Identifiants incorrects »	Vérifier que l'URL du serveur auto-hébergé est bien `https://10.0.112.10` et non l'URL par défaut de Bitwarden (`vault.bitwarden.com`). Si l'URL est correcte, réinitialiser le mot de passe via l'interface web.
L'extension n'apparaît pas dans la barre d'outils	Cliquer sur l'icône d'extensions du navigateur (pièce de puzzle) et épingler Bitwarden. Sous Firefox, accéder à **Extensions et thèmes** pour vérifier que l'extension est activée.
L'organisation n'apparaît pas après connexion	Vérifier auprès de l'administrateur que votre compte a bien été ajouté comme membre de l'organisation (cf. MO-PLT-002). Tenter une synchronisation manuelle : **Paramètres** → **Synchroniser le coffre**.
La biométrie ne fonctionne pas (mobile)	S'assurer que la biométrie est configurée au niveau du système (Face ID, empreinte). Désactiver puis réactiver l'option dans les paramètres de Bitwarden.