

2 - sauvegarde et récupération de l'accès au coffre

Procédure de sauvegarde de l'accès au coffre Bitwarden. Complète la fiche de relevé des passkeys (page « 1 - la prise en main sur Bitwarden »). **Aucun secret ne figure sur cette page, et aucun ne doit y être ajouté** — voir § 5.

1. Ce qu'il faut sauvegarder, et pourquoi ce n'est pas la passkey

Une passkey stockée dans Bitwarden n'est pas sur un appareil : elle est **dans le coffre**, donc déjà répliquée sur chaque machine connectée et présente dans les sauvegardes serveur de Bitwarden. Elle n'est pas le maillon fragile.

Le maillon fragile est **l'accès au coffre**. Le scénario qui coupe l'accès à Bitwarden coupe aussi l'accès à une passkey Bitwarden, où qu'elle soit dupliquée. Sauvegarder la passkey elle-même ne protégerait donc de rien — et n'est de toute façon pas possible : les passkeys ne figurent pas dans les exports de coffre.

Corollaire : on ne duplique jamais une passkey, **on en enregistre une seconde**. Chaque authenticateur génère sa propre paire de clés, le service en tient la liste. La redondance se joue côté service, pas côté fichier.

À sauvegarder	Où le récupérer	Rôle
Code de récupération	<code>vault.bitwarden.com</code> → Paramètres → Sécurité → Connexion en deux étapes → <i>Voir le code de récupération</i>	Désactive tous les facteurs 2FA. Le document qui rouvre le coffre
Export chiffré du coffre	<code>bw export --format encrypted_json --password <phrase></code>	Les identifiants survivent à une disparition de Bitwarden en tant que service

À sauvegarder	Où le récupérer	Rôle
Graines TOTP	Selon les comptes	Non incluses dans les passkeys, régulièrement oubliées
Inventaire des passkeys	Page 1 du chapitre, ou inventaire_passkeys.py --csv	Savoir quoi reconstruire, compte par compte

2. Le code de récupération ne tourne pas tout seul

Point vérifié dans la documentation Bitwarden le 2026-08-25, et contre-intuitif : **ni le changement de mot de passe maître, ni l'ajout ou le retrait de méthodes de connexion en deux étapes ne modifient le code de récupération**. Il est permanent tant qu'il n'a pas servi.

Le seul mécanisme de rotation documenté est de **l'utiliser** : après usage, un nouveau code est généré. L'opération désactive au passage les méthodes de connexion en deux étapes, qu'il faut ensuite ré-enrôler — et vérifier si la passkey vault.bitwarden.com en fait partie, ou si elle relève de la connexion par passkey, qui est un mécanisme distinct.

Conséquence pratique : **ce code se traite comme un document permanent**, pas comme un jeton qu'on pourra régénérer à peu de frais s'il fuit. Sa compromission se répare, mais au prix d'un ré-enrôlement complet du 2FA.

3. Emplacements de conservation

Le vault **Cryptomator** est le bon réceptacle : chiffrement côté client, présent sur le PC julie et sur le PC Nexte, avec une copie sur kDrive. Infomaniak ne voit qu'un blob chiffré.

Support	Contenu	Remarque
Papier, rangé physiquement	Code de récupération	Le seul support qui résiste simultanément à la panne de disque, au rançongiciel et à la perte du téléphone
Vault Cryptomator (PC julie, PC Nexte)	Code, export chiffré, graines TOTP, inventaire	Second exemplaire, hors ligne au repos
Copie kDrive du vault	Idem	Exemplaire hors site. La phrase de passe est le seul rempart

Les deux dépendances circulaires à éviter

1. **La phrase de passe Cryptomator ne doit pas être dans Bitwarden.** Sinon la sauvegarde devient inutilisable précisément le jour où elle servirait. Elle doit être mémorisée, ou écrite sur papier hors ligne.
2. **L'accès kDrive ne doit pas dépendre uniquement du coffre,** pour la même raison.

Même logique que la passkey `vault.bitwarden.com` stockée dans Bitwarden, signalée en page 1 : une sauvegarde qui a besoin de ce qu'elle sauvegarde n'est pas une sauvegarde.

4. Si le code est noté sous forme masquée

Un code partiellement substitué — segments remplacés par des références mnémotechniques (dates, numéros de département, lieux liés à des personnes connues) — appelle deux précautions.

Sur la robustesse : masquer deux groupes sur huit laisse les trois quarts du code lisible, et l'espace résiduel se compte en milliers de combinaisons. Le procédé ralentit une lecture opportuniste, il ne résiste pas à quelqu'un qui cible et connaît l'entourage. Ne pas lui prêter plus de solidité qu'il n'en a.

Sur la récupérabilité — le point qui compte le plus : la règle de décodage devient un second secret à ne pas perdre. Le code servira probablement dans plusieurs années, en situation dégradée. Il faudra alors se rappeler quelles personnes, quels lieux, dans quel ordre, et quelle parenthèse est une date plutôt qu'un département. **Un code de récupération qu'on ne sait plus décoder équivaut à ne pas en avoir.**

D'où le principe à respecter : **séparer le code masqué de sa règle de décodage.** Le papier ne porte que la version masquée, la règle vit dans le vault Cryptomator. Les deux ensemble reconstituent, chacun seul ne dit rien — et aucune perte unique n'est fatale.

5. Où ne jamais écrire ces secrets

Pas dans BookStack, ni dans aucun service auto-hébergé. Une page BookStack finit dans la base MariaDB du VPS, dans la sauvegarde nocturne de 2 h, puis dans l'archive 7z uploadée sur kDrive : trois copies supplémentaires, sur des systèmes que le code de récupération est justement censé pouvoir contourner.

Attention aux formats d'export. N'utiliser que `encrypted_json` avec `--password` :

- `csv` et `json` écrivent **tous les mots de passe en clair** — y compris dans les fichiers temporaires de Syncthing et l'historique kDrive si le vault Cryptomator est ouvert au moment de la synchronisation ;
- `encrypted_json` **sans** `--password` chiffre avec la clé de compte Bitwarden : l'archive n'est alors restaurable que sur ce même compte, ce qui la rend inutile dans le scénario où l'on perd le compte. La phrase passée en `--password` doit être distincte du mot de passe maître.

Transcripts Claude Code : ils résident dans `C:\Users\julie\.claude\projects\D--Syncthing-Jux-univers-Claude-pcelio-jux--claude\*.jsonl`, soit **hors de l'arbre Syncthing** — ils ne se propagent donc ni vers le VPS, ni vers le téléphone, ni vers kDrive. Ils restent néanmoins en clair sur le disque local : ne pas y coller de secret exploitable.

6. Ordre d'exécution

1. Récupérer le **code de récupération** dans l'interface Bitwarden, le porter sur papier, en déposer un second exemplaire dans le vault Cryptomator. (*Fait le 2026-08-25.*)
2. Enregistrer une **seconde passkey Bitwarden sur le téléphone** (Google Password Manager) — casse au passage la dépendance circulaire de la page 1.
3. Produire l'**export chiffré** avec une phrase de passe distincte, le déposer dans le vault.
4. Vérifier que la **phrase Cryptomator n'est pas uniquement dans Bitwarden**.

Seul le point 1 est urgent. Les trois autres peuvent être étalés.

Voir aussi : page 1 du chapitre pour l'inventaire des passkeys et la fiche de relevé côté services.
Script : `Jux-scripts/Passkeys/inventaire_passkeys.py`.

Revision #2

Created 2026-08-25 09:24:36 UTC by Julien

Updated 2026-08-25 09:24:47 UTC by Julien