MON COMPTE > CONNEXION EN DEUX ÉTAPES >

Connexion en deux étapes via FIDO2 WebAuthn

Connexion en deux étapes via FIDO2 WebAuthn

La connexion en deux étapes utilisant les identifiants FIDO2 WebAuthn est disponible gratuitement pour tous les utilisateurs de Bitwarden.

Toutes les informations d'identification certifiées FIDO2 WebAuthn peuvent être utilisées, y compris les clés de sécurité telles que YubiKeys, SoloKeys et Nitrokeys, ainsi que les options de biométrie natives comme Windows Hello et Touch ID.

> **Tip**
>
> De nouvelles clés U2F-uniquement **ne peuvent pas** être ajoutées à un compte. Cependant, les clés de sécurité FIDO U2F existantes resteront utilisables et seront marquées **(Migré de FIDO)** dans le dialogue Deuxième étape de l'identifiant → Gérer FIDO2 WebAuthn.

FIDO2 WebAuthn est compatible avec la plupart des applications Bitwarden. Si vous souhaitez utiliser une version qui ne le prend pas en charge, assurez-vous d'activer une méthode d'identifiant en deux étapes alternative. Les applications prises en charge comprennent :

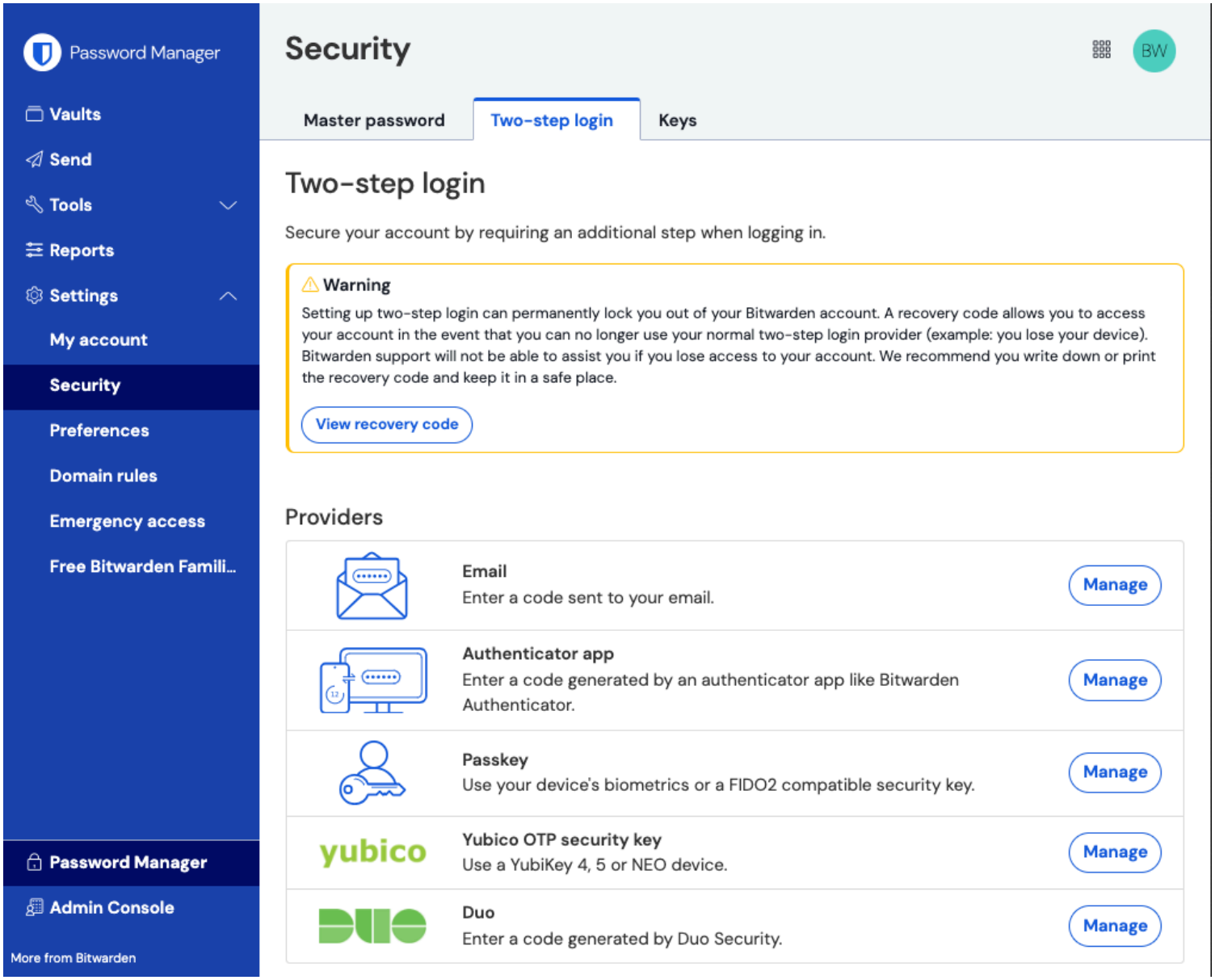
- **Coffre web** sur un appareil avec un navigateur compatible FIDO2.
- **Extensions de navigateur** pour un navigateur compatible FIDO2.
- **Applications de bureau** sur Windows 10 et supérieur.
- **Applications mobiles** pour Android et iOS 13.3+ avec un navigateur compatible FIDO2.

Configuration FIDO2 WebAuthn

Pour activer la connexion en deux étapes en utilisant FIDO2 WebAuthn :

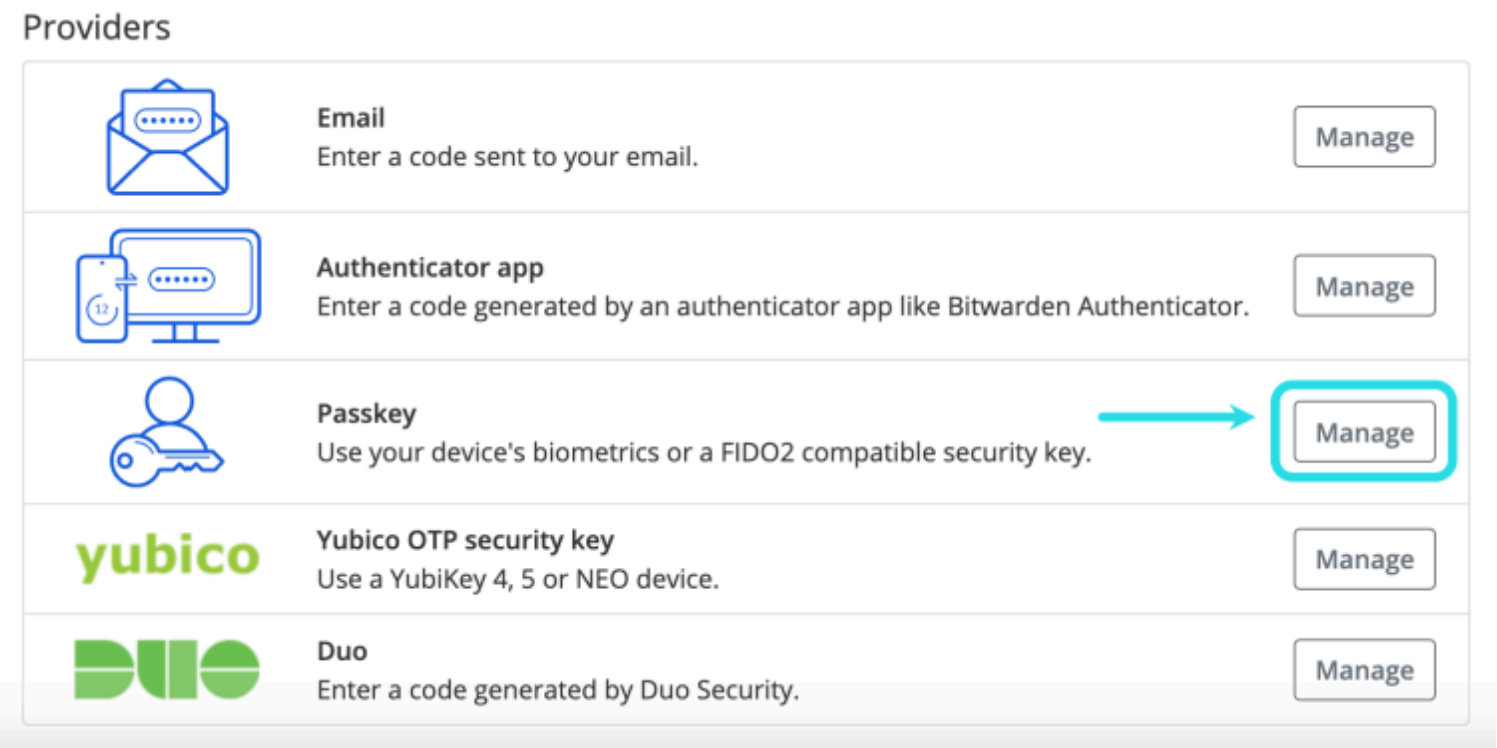
> **⚠ Warning**
>
> **Perdre l'accès à votre appareil d'identifiant en deux étapes peut vous verrouiller définitivement de votre coffre** à moins que vous n'écriviez et ne conserviez votre Code de récupération d'identifiant en deux étapes dans un endroit sûr ou que vous ayez une méthode d'identifiant en deux étapes alternative activée et disponible.
>
> Obtenez votre Code de récupération depuis l'écran **d'identifiant en deux étapes** immédiatement après avoir activé n'importe quelle méthode.

1. Se connecter à l'application web Bitwarden.
2. Sélectionnez **Paramètres** → **Sécurité** → **Identifiant en deux étapes** depuis la navigation:



Authentification à deux facteurs

3. Localisez l'option **FIDO2 WebAuthn** et sélectionnez le bouton **Gérer**.



Sélectionnez le bouton Gérer

On vous demandera d'entrer votre mot de passe principal pour continuer.

4. Donnez un **Nom** amical à votre clé de sécurité.

5. Branchez la clé de sécurité dans le port USB de votre appareil et sélectionnez **Lire la clé**. Si votre clé de sécurité a un bouton, touchez-le.

> **ⓘ Note**
>
> Certains appareils, y compris ceux avec Windows Hello ou les appareils macOS qui supportent les clés de passe, sont des authentificateurs FIDO2 natifs qui proposeront ces options par défaut. Si vous souhaitez enregistrer une clé de sécurité ou un autre authentificateur, vous devrez peut-être sélectionner un bouton **Essayer une autre manière**, **Autres options**, ou **Annuler** pour ouvrir vos autres options.

6. Sélectionnez **Enregistrer**. Un message vert `Activé` indiquera que l'identifiant en deux étapes utilisant FIDO2 WebAuthn a été activé avec succès et votre clé apparaîtra avec une case à cocher verte (✓).

7. Sélectionnez le bouton **Fermer** et confirmez que l'option **FIDO2 WebAuthn** est maintenant activée, comme indiqué par une case à cocher verte (✓).

Répétez ce processus pour ajouter jusqu'à 5 clés de sécurité FIDO2 WebAuthn à votre compte.

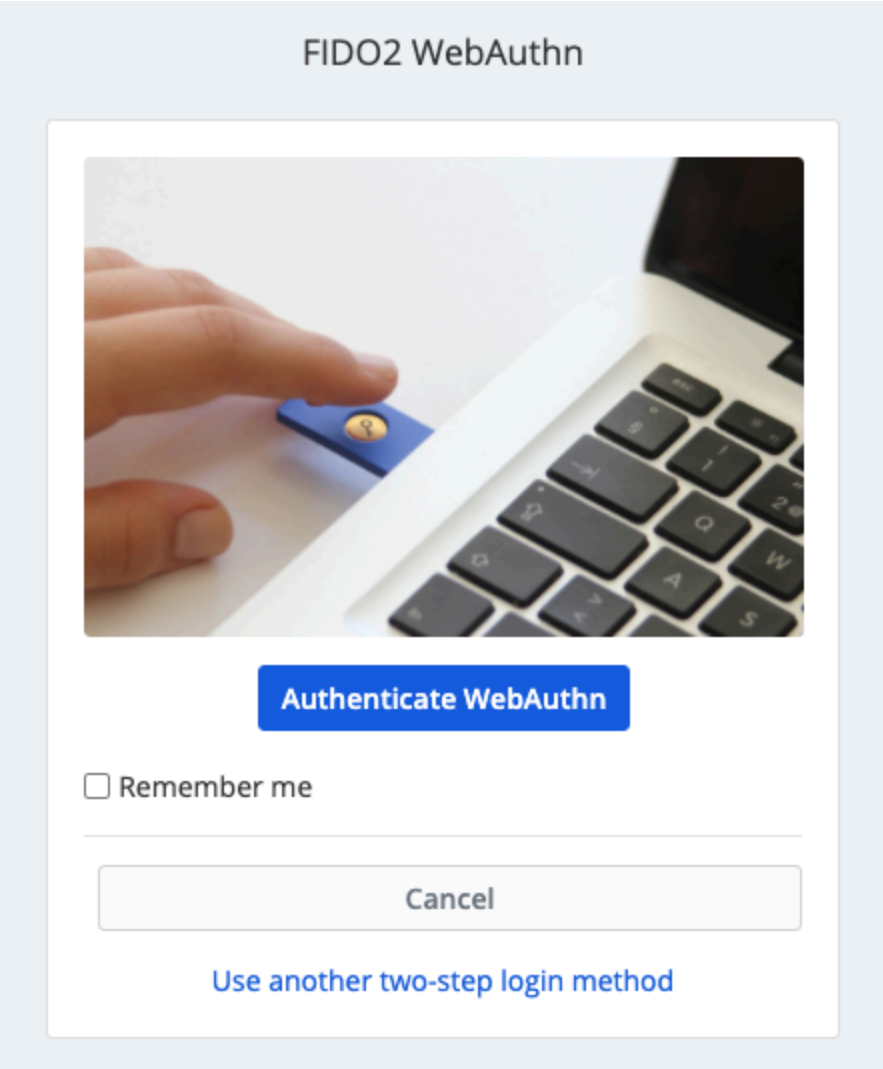
> **Note**
>
> Nous recommandons de garder votre onglet de coffre web actif ouvert avant de procéder au test de l'identifiant en deux étapes au cas où quelque chose aurait été mal configuré. Une fois que vous avez confirmé son fonctionnement, déconnectez-vous de toutes vos applications Bitwarden pour nécessiter un identifiant en deux étapes pour chacune. Vous finirez par être automatiquement déconnecté.

Utilisez FIDO2 WebAuthn

On suppose que **FIDO2 WebAuthn** est votre méthode activée de plus haute priorité. Pour accéder à votre coffre en utilisant un appareil FIDO2 WebAuthn :

1. Connectez-vous à votre coffre Bitwarden et entrez votre adresse de courriel et votre mot de passe principal.

   On vous demandera d'insérer votre clé de sécurité dans le port USB de votre appareil. Si ça a un bouton, touchez-le.



invite-fido2

> **Tip**
>
> Cochez la case **Se souvenir de moi** pour que votre appareil se souvienne de vous pendant 30 jours. Se souvenir de votre appareil signifie que vous ne serez pas obligé de compléter votre étape de connexion en deux étapes.

Il ne vous sera pas demandé de compléter votre configuration de connexion en deux étapes secondaire pour **déverrouiller** votre coffre une fois connecté. Pour obtenir de l'aide pour configurer le comportement de se déconnecter vs verrouiller, voir options de délai d'expiration du coffre.

Dépannage NFC

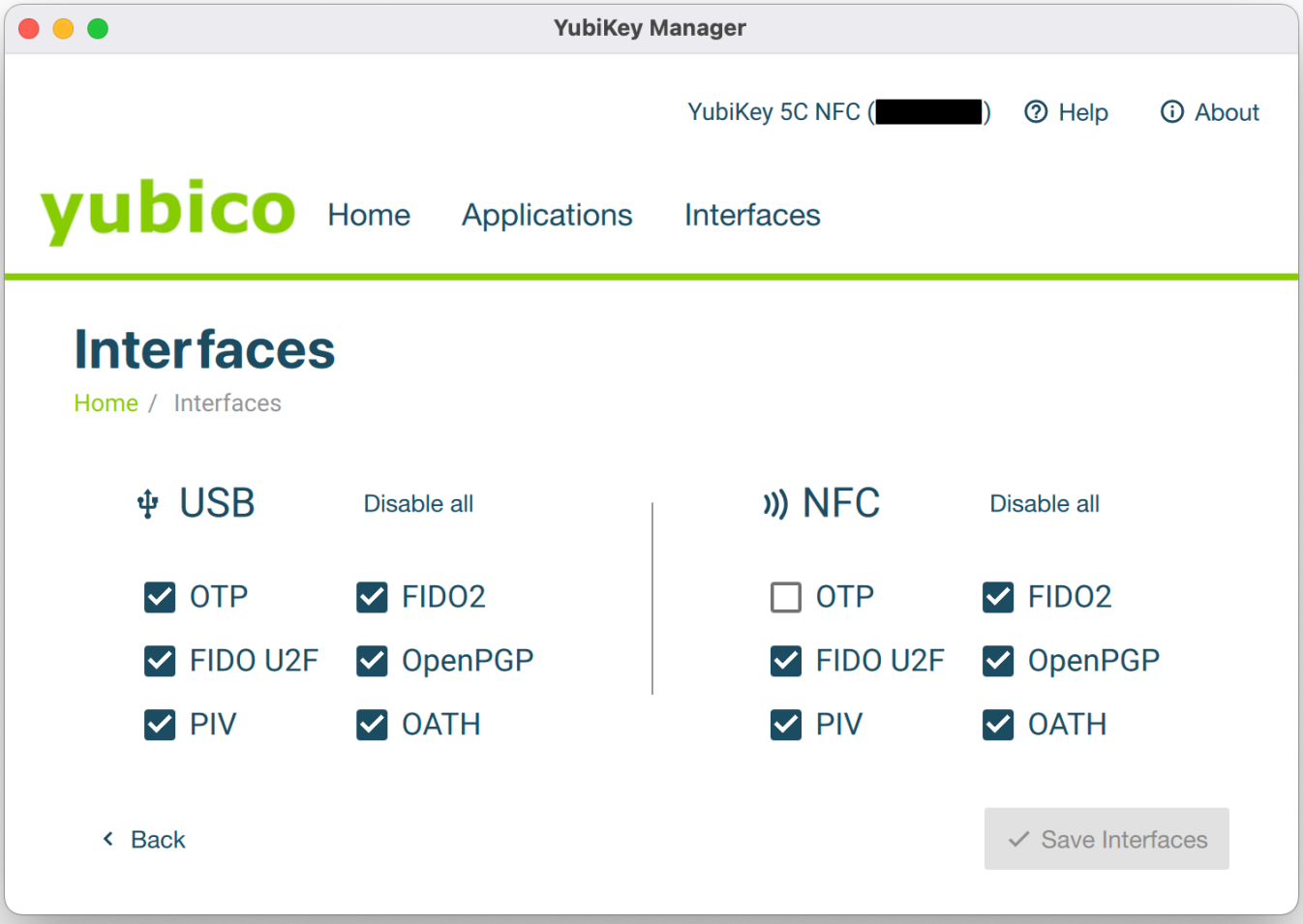
Si vous utilisez un authentificateur FIDO2 avec une fonctionnalité NFC comme une YubiKey ou une autre clé de sécurité matérielle, vous devrez peut-être vous entraîner à trouver le lecteur NFC dans votre appareil car différents appareils ont des lecteurs NFC à des emplacements physiques différents (par exemple, haut du téléphone vs bas du téléphone, ou avant vs arrière).

> **Tip**
>
> Les clés de sécurité matérielles ont généralement une prise physique, qui fonctionnera de manière plus fiable dans les cas où le NFC est difficile.

Dépannage YubiKey NFC

Sur les appareils mobiles, vous pouvez rencontrer un scénario où votre YubiKey est lu deux fois consécutivement. Vous saurez que cela s'est produit lorsque le navigateur de votre appareil ouvre la page web YubiKey OTP (`https://demo/yubico.com/yk`) et si votre appareil vibre plusieurs fois pour signaler plusieurs lectures NFC.

Pour résoudre cela, utilisez l'application YubiKey Manager pour désactiver l'interface **NFC** → **OTP** pour votre clé :



Gestionnaire YubiKey

> **⚠ Warning**
>
> La désactivation de **NFC** → **OTP** vous empêchera d'utiliser l'identification en deux étapes via YubiKey (OTP) sur NFC avec cette clé. Dans ce scénario, l'OTP via USB fonctionnera toujours comme prévu.