bitwarden | Article du Centre d'Aide

MON COMPTE > CONNEXION EN DEUX ÉTAPES

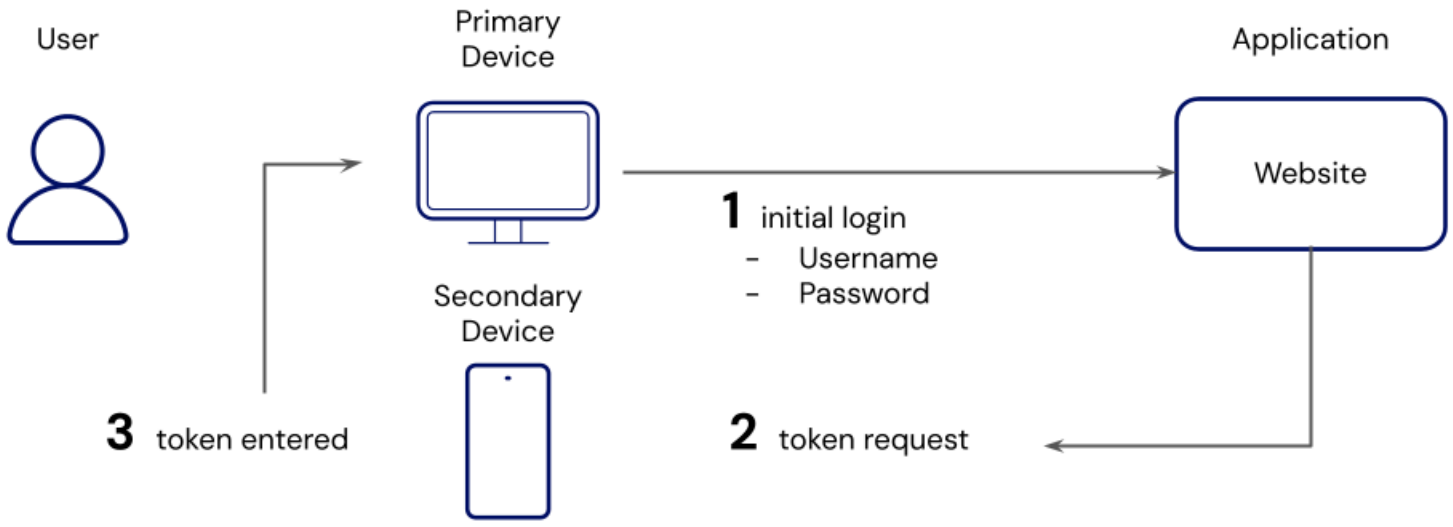
Guide de Terrain pour l'Identifiant en Deux Étapes

Afficher dans le centre d'aide:
https://bitwarden.com/help/bitwarden-field-guide-two-step-login/

Guide de Terrain pour l'Identifiant en Deux Étapes

La connexion en deux étapes (également appelée authentication à deux facteurs ou 2FA) est une technique de sécurité courante utilisée par les pages web et les applications pour protéger vos données sensibles. Les sites Web qui utilisent l'identifiant en deux étapes vous demandent de vérifier votre identité en entrant un "jeton" supplémentaire (également appelé code de vérification ou mot de passe unique (OTP)) en plus du nom d'utilisateur et du mot de passe, généralement récupéré à partir d'un autre appareil.

Sans accès physique au jeton de votre appareil secondaire, un acteur malveillant serait incapable d'accéder à la page web, même s'ils découvrent votre nom d'utilisateur et mot de passe :



Flux de base pour l'identifiant en deux étapes

Généralement, les pages web ou les applications avec des données sensibles (par exemple, votre compte bancaire en ligne) essaieront de vérifier votre identité en dehors de l'écran d'identifiant en :

- Envoyer un jeton dans un SMS / message texte à l'appareil mobile enregistré.
- Demande d'un jeton généré par une application d'authentification (par exemple, Authy) sur votre appareil mobile.
- À la recherche d'un jeton provenant d'une clé de sécurité physique (par exemple, YubiKey).

Comment dois-je utiliser l'identifiant en deux étapes ?

La sécurité implique souvent un compromis entre protection et commodité, donc finalement c'est à vous de décider ! Généralement, les deux méthodes les plus critiques pour utiliser l'identifiant en deux étapes sont :

1. Pour sécuriser Bitwarden

Sécurisez toutes les données du coffre en exigeant une étape supplémentaire chaque fois que vous vous connectez à Bitwarden, en plus de saisir votre mot de passe principal.

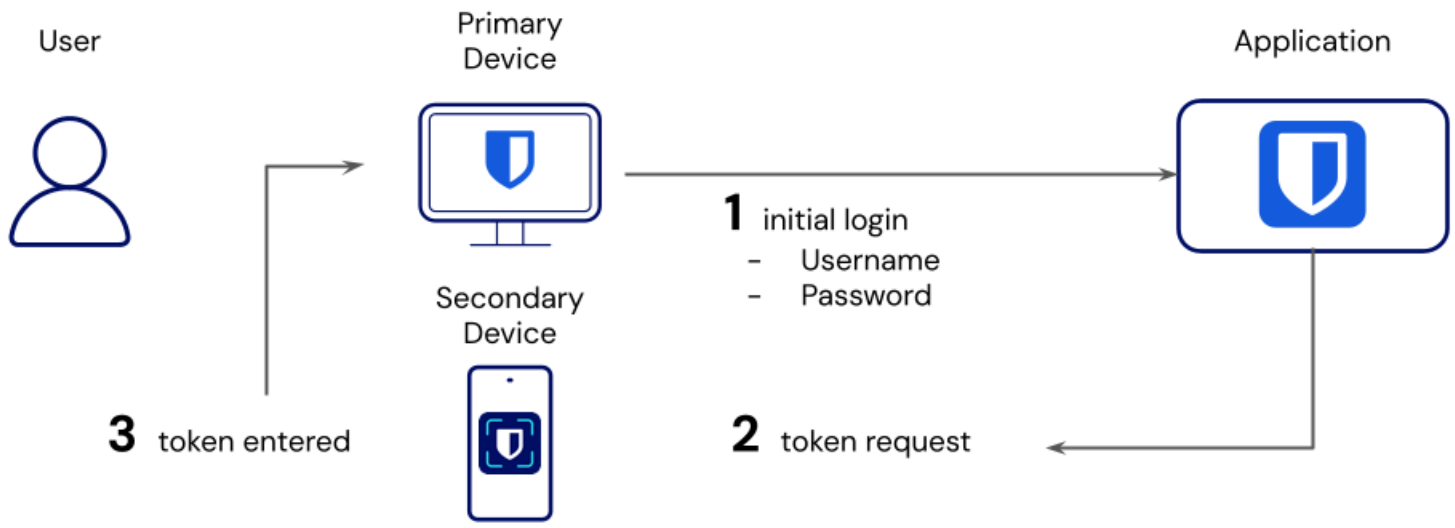
2. Pour sécuriser les pages web importantes

   Sécurisez une page web individuelle en exigeant un mot de passe temporaire à usage unique (TOTP) lorsque vous vous connectez. Vous pouvez stocker et générer des TOTP avec Bitwarden.

Sécurisation de Bitwarden

Puisque votre gestionnaire de mots de passe stocke tous vos identifiants, nous vous recommandons vivement de le sécuriser avec une connexion en deux étapes. Ce faisant, tous vos identifiants sont protégés en empêchant un acteur malveillant d'accéder à votre coffre, même s'ils découvrent votre mot de passe principal.

L'activation de la connexion en deux étapes vous obligera à compléter une étape secondaire chaque fois que vous vous connectez, en plus de votre méthode de connexion principale (mot de passe principal). Vous n'aurez pas besoin de compléter votre étape secondaire pour déverrouiller votre coffre, seulement pour vous connecter.



Identification en deux étapes pour accéder à Bitwarden

Bitwarden offre plusieurs méthodes d'identifiant en deux étapes gratuitement, y compris :

- FIDO (toute clé certifiée FIDO2 WebAuthn)
- via une application d'authentification (par exemple, 2FAS, Ravio, ou Aegis)
- via courriel

Pour les utilisateurs Premium, Bitwarden propose plusieurs méthodes avancées d'identifiant en deux étapes :

- Duo Security avec Duo Push, SMS, appel téléphonique, et clés de sécurité
- YubiKey (tout appareil de série 4/5 ou YubiKey NEO/NFC)

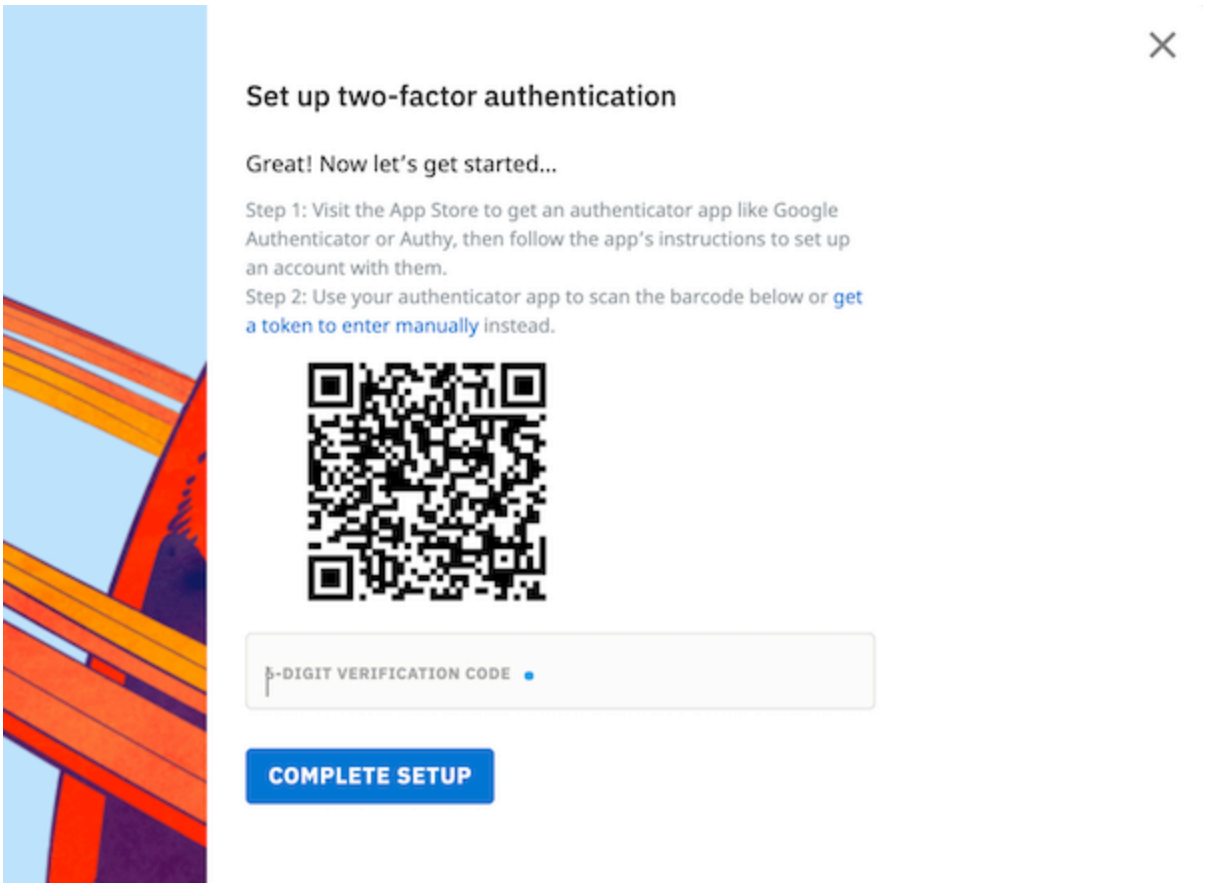
En savoir plus sur vos options ou obtenir de l'aide pour configurer n'importe quelle méthode en utilisant nos **Guides de Configuration.**

> **Note**
> Bitwarden ne prend pas en charge le 2FA SMS en raison de vulnérabilités, y compris le détournement de SIM. Nous ne recommandons pas le 2FA SMS pour d'autres comptes à moins que ce soit la seule méthode disponible. Tout second facteur est recommandé plutôt que de n'en avoir aucun, mais la plupart des alternatives sont plus sûres que le 2FA SMS.

Sécurisation des pages web importantes

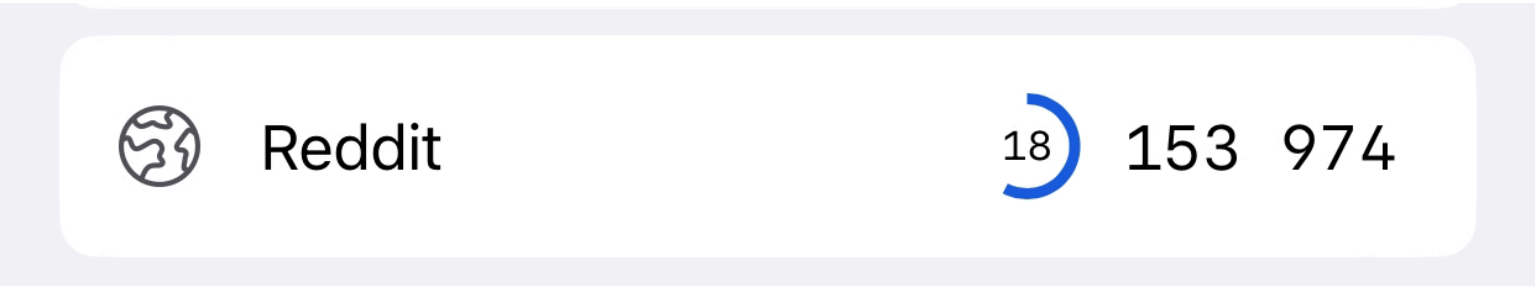
De nombreux autres sites Web et applications proposent des options de connexion en deux étapes, cela est particulièrement courant pour les sites Web qui stockent des informations sensibles (par exemple, les numéros de carte de crédit ou de compte bancaire). L'option d'identifiant en deux étapes de la plupart des pages web se trouvera dans les menus **Paramètres**, **Sécurité**, ou **Confidentialité**.

L'activation de l'identifiant en deux étapes ouvrira généralement un code QR, comme cet exemple de Reddit :



Code QR 2FA

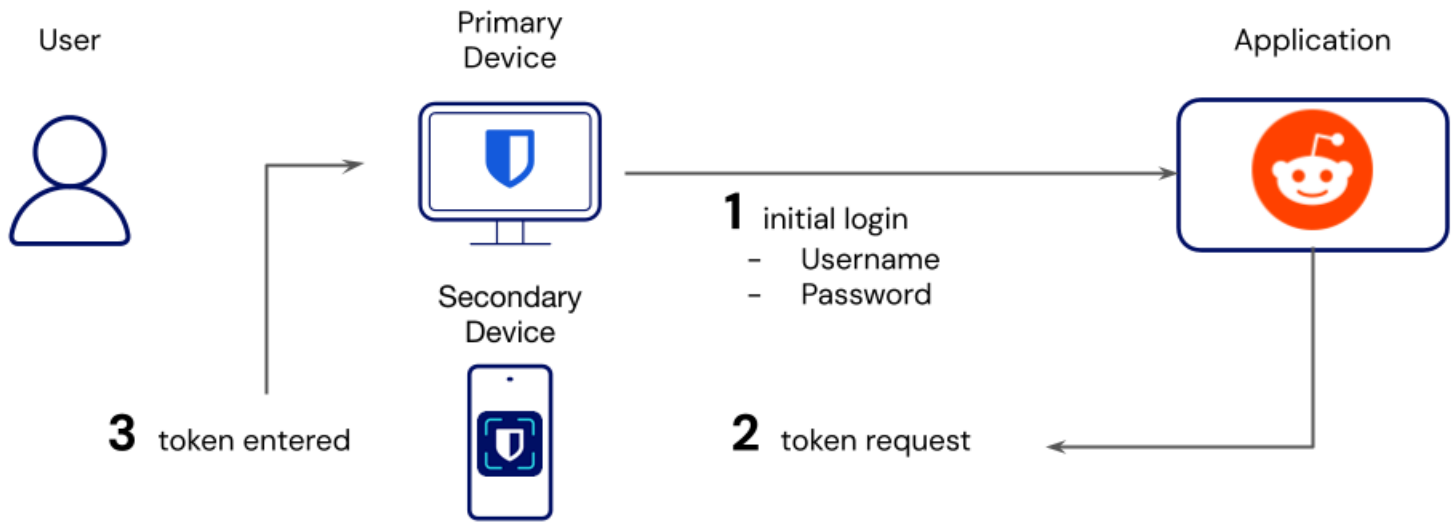
Scanner ce code avec une application d'authentification permettra à l'application de générer des jetons à six chiffres rotatifs que vous pouvez utiliser pour vérifier votre identité, comme celui-ci généré par Authy :



Jeton TOTP

Utilisez Authy

Pour configurer la connexion en deux étapes pour Reddit en utilisant Authy, appuyez sur le bouton **Ajouter un compte** et scannez le code QR présenté par votre page web ou application. La numérisation du code QR générera votre jeton à six chiffres. Entrez ce code dans la case d'entrée **Code de vérification** pour terminer la configuration.



Identification en deux étapes en utilisant Authy

Généralement, on vous donnera l'option de télécharger des codes de récupération. Télécharger des codes de récupération est essentiel pour vous empêcher de perdre l'accès à vos jetons d'identifiant en deux étapes, même si vous perdez l'appareil sur lequel Authy est installé.

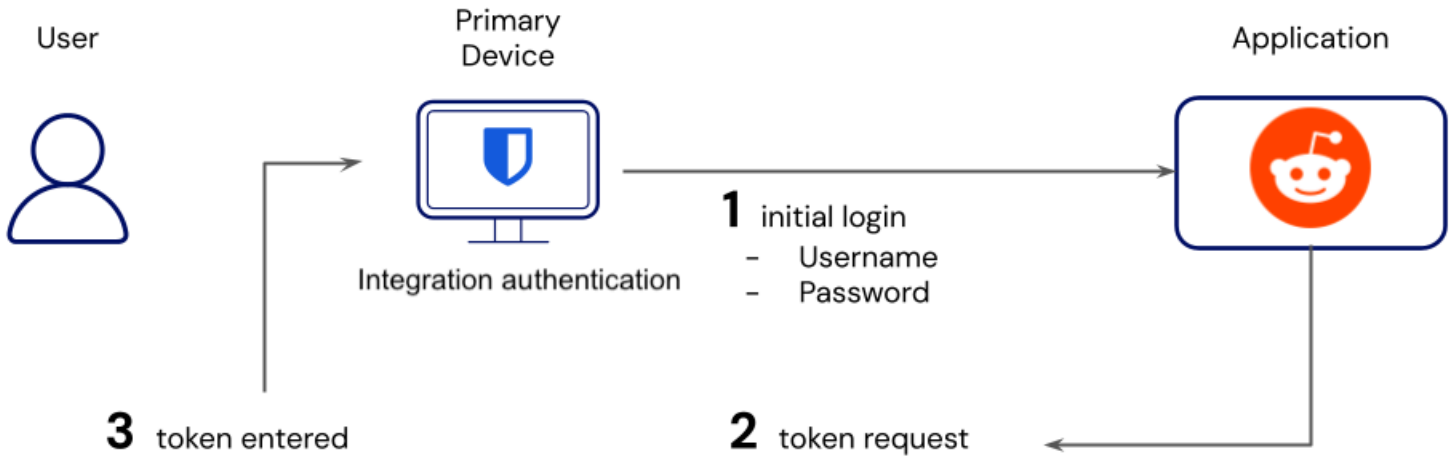
La prochaine fois que vous vous connectez à Reddit avec votre identifiant, il vous sera demandé de vérifier votre identité en entrant un code de vérification provenant d'Authy. Les codes de vérification se régénèrent toutes les 30 secondes, il sera donc impossible pour un acteur malveillant de découvrir votre code sans accès physique à votre appareil.

> **Note**
>
> Authy est notre application d'authentification recommandée car elle inclut des sauvegardes pour tout appareil. Les sauvegardes vous empêchent de perdre l'accès à vos jetons, même si vous perdez l'appareil sur lequel Authy est installé. Activez le bouton **Sauvegardes d'Authenticator** sur l'écran **Comptes** de l'application Authy pour utiliser cette fonctionnalité.
>
> D'autres applications d'authentification incluent Google Authenticator et FreeOTP, et depuis le 7 mai 2020, Google Authenticator inclut la portabilité du code de vérification sur les appareils Android.

Utilisez l'authentificateur Bitwarden

Comme alternative à Authy, Bitwarden offre un authentificateur intégré pour les utilisateurs Premium, y compris les membres des organisations payantes (familles, équipes ou entreprises).

Bitwarden pour iOS et Android peut scanner les codes QR et générer des jetons de six chiffres tout comme les autres applications d'authentification. En utilisant l'authentificateur Bitwarden pour sécuriser une page web, un jeton à six chiffres en rotation sera enregistré avec cet élément d'identifiant dans le coffre. Vous pouvez également enregistrer manuellement votre secret de code de vérification dans un élément de coffre depuis n'importe quelle application Bitwarden.



Identification en deux étapes en utilisant Bitwarden

Apprenez à utiliser l'authentificateur Bitwarden.

Pourquoi utiliser l'authentificateur Bitwarden ?

Compréhensiblement, certains utilisateurs sont sceptiques quant à l'utilisation de Bitwarden pour l'authentication par jeton. N'oubliez pas, la sécurité implique souvent un compromis entre protection et commodité, donc la meilleure solution dépend de vous. Généralement, les gens qui utilisent l'authentificateur Bitwarden le font pour deux raisons :

1. **Commodité**

   Lorsque vous utilisez les applications mobiles Bitwarden ou les extensions de navigateur pour la saisie automatique d'un nom d'utilisateur et d'un mot de passe, il copiera automatiquement le code de vérification dans votre presse-papiers pour un collage facile.

   Si vous utilisez une extension de navigateur, vous pouvez enchaîner le raccourci clavier d'identifiant (Windows: `Ctrl + Shift + L` / macOS: `Cmd + Shift + L`), suivi du raccourci de collage (Windows: `Ctrl + V` / macOS: `Cmd + V`) pour des identifications ultra-rapides.

2. **Partage**

   Pour les organisations, un grand avantage de l'utilisation de l'authentificateur Bitwarden pour la vérification des jetons est la capacité de partager la génération de jetons parmi les membres de l'équipe. Cela permet aux organisations de protéger leurs comptes avec une connexion en deux étapes sans sacrifier la possibilité pour plusieurs utilisateurs d'accéder à ce compte ou nécessitant une coordination entre deux employés pour partager des jetons de manière non sécurisée.

Clés de sécurité 2FA et mots de passe

Les clés de sécurité FIDO2 sont une option populaire et sécurisée pour ajouter 2FA à votre compte Bitwarden. Si vous n'êtes pas familier avec les clés de sécurité FIDO2, consultez la web page de l'Alliance FIDO pour plus d'informations sur FIDO2.

Un appareil YubiKey est une clé de sécurité qui fonctionne avec les protocoles d'authentication FIDO, et peut avoir plusieurs cas d'utilisation. Deux utilisations sont comme clés de sécurité 2FA, ou clés de passe.

- **Clé de sécurité 2FA :** L'utilisation d'une YubiKey comme clé de sécurité 2FA agira comme un appareil supplémentaire dans le processus d'authentification. Cela sera accompagné d'une autre méthode principale d'authentication (comme le mot de passe principal). La clé de sécurité YubiKey doit être physiquement branchée pour fournir les informations d'authentication.

- **Mot de passe:** Un mot de passe est une paire de clés cryptographiques publiques-privées qui sont utilisées pour authentifier un identifiant. Au lieu de créer un nom d'utilisateur, un mot de passe et d'ajouter 2FA à un compte, la clé unique est utilisée. Lors de la création de la clé de passe, la YubiKey est capable de fonctionner comme le générateur de clé de passe pour générer les clés publiques et privées nécessaires pour l'identifiant de la clé de passe. Apprenez-en plus sur l'utilisation d'une YubiKey comme clé de passe ici.

Avec Bitwarden, l'utilisation principale d'une clé de sécurité telle qu'un appareil YubiKey est de fournir une authentication 2FA.

Prochaines étapes

Maintenant que vous êtes un expert en identifiant à deux étapes, nous recommandons :

- Configurer l'identifiant en deux étapes
- Obtenez Premium pour accéder à des méthodes d'identifiant en deux étapes avancées
- Configurez l'authentificateur Bitwarden
- Configurez l'identifiant en deux étapes pour les équipes et les entreprises