

PASSWORD MANAGER > OUTILS DE DÉVELOPPEMENT > CLI

Défis d'authentification CLI

Défis d'authentification CLI

La version d'août 2021 de Bitwarden (**2021-09-21**) a introduit des exigences de [CAPTCHA](#) pour augmenter la sécurité contre le trafic de bots. Sur le CLI, les défis CAPTCHA sont remplacés par des défis d'authentification qui peuvent être validés en utilisant la [clé API personnelle](#) de votre compte `client_secret`.

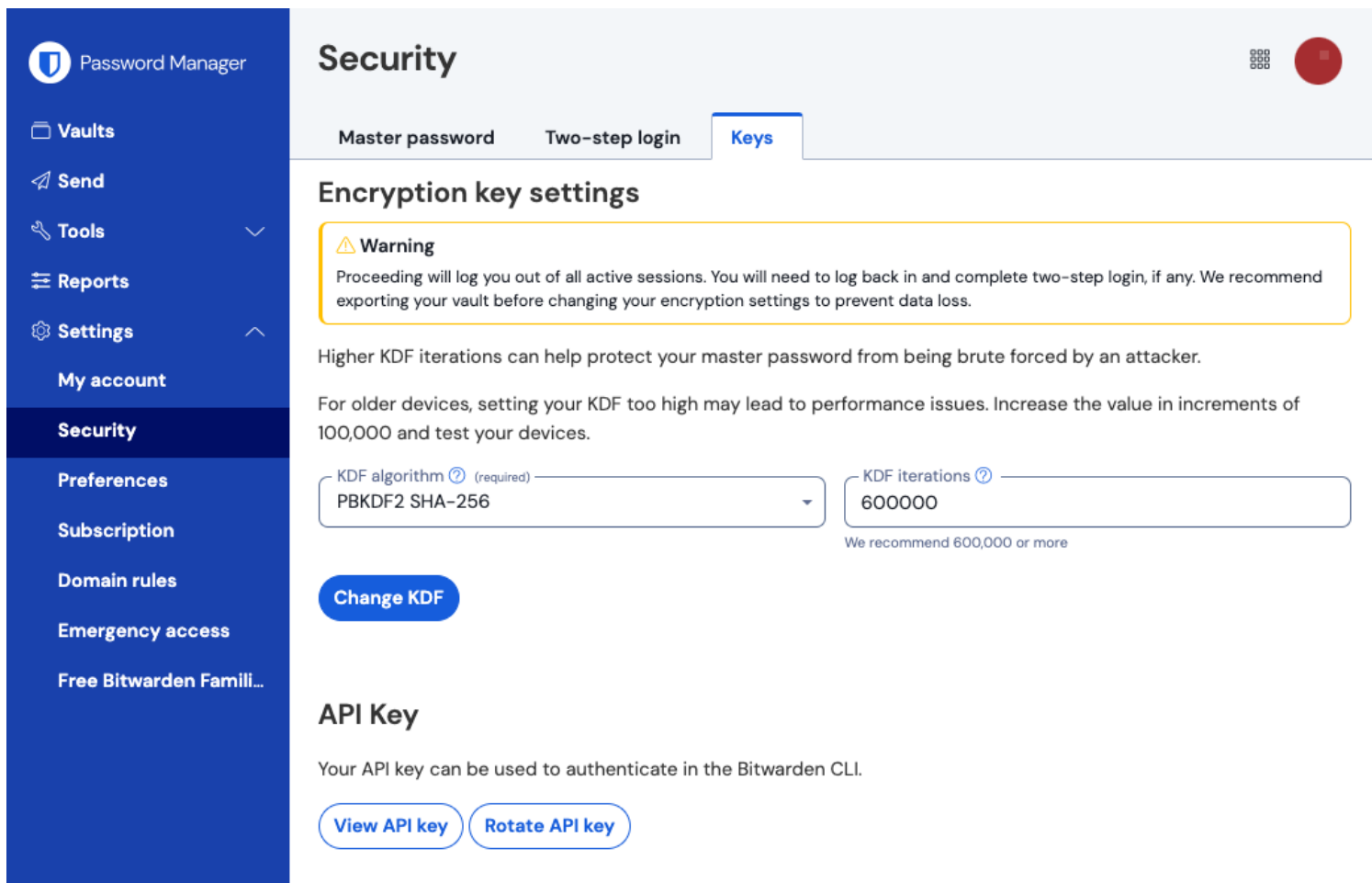
💡 Tip

Pour les flux de travail automatisés ou pour fournir un accès à une application externe, nous recommandons d'utiliser la `identifiant bw --apikey` [méthode](#). Cette méthode suit un flux d'authentification plus prévisible et la révocation de l'accès d'une application ou d'une machine peut être obtenue en faisant tourner la [clé API](#).

Obtenez votre clé API personnelle

Pour obtenir votre clé API personnelle :

1. Dans l'application web Bitwarden, naviguez vers **Paramètres** → **Sécurité** → **Clés** :



The screenshot shows the Bitwarden web application interface. On the left is a dark blue sidebar with navigation links: Password Manager, Vaults, Send, Tools, Reports, Settings, My account, Security (highlighted), Preferences, Subscription, Domain rules, Emergency access, and Free Bitwarden Famili... The main content area has a light blue header with 'Security' and tabs for 'Master password', 'Two-step login', and 'Keys' (selected). Below the header is the 'Encryption key settings' section, which includes a warning box about logging out of active sessions, explanatory text about KDF iterations, and input fields for 'KDF algorithm' (set to PBKDF2 SHA-256) and 'KDF iterations' (set to 600000). A 'Change KDF' button is present. The 'API Key' section below explains that the API key is used for CLI authentication and provides 'View API key' and 'Rotate API key' buttons.

Clés

2. Sélectionnez le bouton **Afficher la clé API** et entrez votre mot de passe principal pour valider l'accès.
3. Depuis la boîte de dialogue **clé API**, copiez la valeur **client_secret**, qui est une chaîne aléatoire comme `efrbgT9C6BogEfXi5pZc48XyJjfpR`.

Répondre aux défis

Selon vos préférences, vous pouvez [enregistrer une variable d'environnement](#) pour passer automatiquement les défis d'authentification ou [entrer manuellement](#) votre `client_secret` chaque fois qu'un défi est lancé :

Répondez aux défis avec une variable d'environnement

Les défis d'authentification rechercheront une variable d'environnement non vide `BW_CLIENTSECRET` avant de vous inviter à en entrer une manuellement. Enregistrer cette variable avec la [valeur client_secret récupérée](#) vous permettra de passer automatiquement les défis d'authentification. Pour enregistrer cette variable d'environnement :

  Bash

Bash

```
export BW_CLIENTSECRET="client_secret"
```

 PowerShell

Bash

```
env:BW_CLIENTSECRET="client_secret"
```

Warning

Si votre `client_secret` est incorrect, vous recevrez une erreur. Dans la plupart des cas, c'est parce que vous avez [régénéré votre clé API](#) depuis l'enregistrement de la variable. [Utilisez les étapes ci-dessus](#) pour récupérer la valeur correcte.

Répondez aux défis manuellement

Lorsqu'un défi d'authentification est lancé et qu'aucune valeur `BW_CLIENTSECRET` n'est trouvée, on vous demandera d'entrer manuellement votre valeur `client_secret` :

Invite d'identifiant avec défi d'authentification

Si votre `client_secret` est incorrect, vous recevrez une erreur. Dans la plupart des cas, c'est parce que vous avez [régénéré votre clé API](#) depuis l'enregistrement de la variable. [Utilisez les étapes ci-dessus](#) pour récupérer la valeur correcte.