

MON COMPTE > SE CONNECTER & DÉVERROUILLER

# Déverrouiller avec un code PIN

## Déverrouiller avec un code PIN

Vous pouvez définir un code PIN comme méthode pour déverrouiller votre coffre. Les codes PIN ne peuvent être utilisés que pour déverrouiller votre coffre, vous devrez toujours utiliser votre mot de passe principal ou vous connecter avec un appareil, et toute [méthode de connexion en deux étapes](#) activée lorsque vous vous connectez.

Déverrouiller avec un PIN n'est pas une méthode sans mot de passe pour accéder à votre compte Bitwarden, si vous n'êtes pas sûr de la différence, voir [Comprendre déverrouiller vs. se connecter](#).

### Note

Après **cinq** tentatives de PIN échouées, l'application se déconnectera automatiquement de votre compte.

## Activer déverrouiller avec PIN

Le déverrouillage avec un code PIN peut être activé pour l'extension Bitwarden du navigateur, l'application mobile et l'application de bureau :

### Warning

L'utilisation d'un PIN peut affaiblir le niveau de cryptage qui protège la base de données du coffre local de votre application. Si vous êtes préoccupé par les vecteurs d'attaque qui impliquent que les données locales de votre appareil soient compromises, vous voudrez peut-être reconsidérer la commodité d'utiliser un PIN.

## ⇒Extension de navigateur

Pour activer déverrouiller avec PIN pour votre extension de navigateur :

1. Ouvrez l'onglet  **Paramètres**.
2. Ouvrez la section Sécurité du compte et cochez la case **Déverrouiller avec un code PIN**.
3. Entrez le code PIN souhaité dans la boîte de saisie. Votre code PIN peut être une combinaison de caractères (a-z, 0-9, \$, #, etc.).

### Tip

Si vous partagez votre appareil, il est important de créer un code PIN fort en évitant des chiffres facilement devinables comme la date de naissance ou en utilisant un code PIN de plus de quatre chiffres.

4. L'option pré-cochée **Verrouiller avec le mot de passe principal au redémarrage du navigateur** vous demandera d'entrer votre mot de passe principal au lieu du PIN lorsque votre navigateur redémarre. Si vous voulez la capacité de déverrouiller avec un PIN même lorsque le navigateur redémarre, décochez l'option.

### Note

Si vous désactivez l'option **Verrouiller avec le mot de passe principal au redémarrage**, l'application Bitwarden peut ne pas purger entièrement les données sensibles de la mémoire de l'application lors de l'entrée dans un état verrouillé. Si vous êtes préoccupé par la compromission de la mémoire locale de votre appareil, vous devriez garder l'option **Verrouiller avec le mot de passe principal au redémarrage** activée.

Une fois défini, vous pouvez changer votre code PIN en désactivant et réactivant déverrouiller avec le code PIN.

Lorsque vous **vous déconnectez** de votre extension de navigateur, vos paramètres de déverrouillage avec PIN seront effacés et vous devrez réactiver le déverrouillage avec PIN.

## ⇒Mobile

Pour activer déverrouiller avec un code PIN pour votre application mobile:

1. Ouvrez l'onglet  **Paramètres**.
2. Faites défiler jusqu'à la section de sécurité et appuyez sur l'option **Déverrouiller avec le code PIN**.
3. Entrez le code PIN souhaité dans la boîte de saisie. Votre code PIN peut être une combinaison quelconque de nombres (0–9).

### Tip

Si vous partagez votre appareil, il est important de créer un code PIN fort en évitant des chiffres facilement devinables comme la date de naissance ou en utilisant un code PIN de plus de quatre chiffres.

4. Une boîte de dialogue apparaîtra vous demandant si vous souhaitez exiger le déverrouillage avec votre mot de passe principal lorsque l'application est redémarrée. Appuyez sur **Oui** pour exiger votre mot de passe principal au lieu du PIN lorsque l'application redémarre. Appuyez sur **Non** pour avoir la possibilité de déverrouiller avec le PIN lorsque l'application redémarre.

Une fois défini, vous pouvez changer votre code PIN en désactivant et réactivant Déverrouiller avec un code PIN.

Lorsque vous **vous déconnectez** de votre application mobile, vos paramètres de déverrouillage avec code PIN seront effacés et vous devrez réactiver Déverrouiller avec le code PIN.

## ⇒Ordinateur

Le déverrouillage avec un code PIN est défini séparément pour [chaque compte connecté à l'application de bureau](#). Pour activer déverrouiller avec un code PIN:

1. Ouvrez vos **Paramètres** (sur Windows, **Fichier** → **Paramètres**) (sur macOS, **Bitwarden** → **Préférences**).
2. Faites défiler vers le bas jusqu'à la section Sécurité et cochez la case **Déverrouiller avec un PIN**.
3. Entrez le code PIN souhaité dans la boîte de saisie. Votre code PIN peut être une combinaison de caractères (a–z, 0–9, \$, #, etc.).

### Tip

Si vous partagez votre appareil, il est important de créer un code PIN fort en évitant des chiffres facilement devinables comme la date de naissance ou en utilisant un code PIN de plus de quatre chiffres.

4. L'option pré-cochée **Verrouiller avec le mot de passe principal au redémarrage** vous demandera d'entrer votre mot de passe principal au lieu du PIN lorsque l'application redémarre. Si vous voulez la capacité de déverrouiller avec un PIN lorsque l'application redémarre, décochez cette option.

### Note

Si vous désactivez l'option **Verrouiller avec le mot de passe principal au redémarrage**, l'application Bitwarden peut ne pas purger entièrement les données sensibles de la mémoire de l'application lors de l'entrée dans un état verrouillé. Si vous êtes préoccupé par la compromission de la mémoire locale de votre appareil, vous devriez garder l'option **Verrouiller avec le mot de passe principal au redémarrage** activée.

Une fois défini, vous pouvez changer votre code PIN en désactivant et réactivant déverrouiller avec le code PIN.

Lorsque vous **vous déconnectez** de votre application de bureau, vos paramètres de déverrouillage avec code PIN seront effacés et vous devrez réactiver le déverrouillage avec code PIN.

## Comprendre déverrouiller vs. se connecter

Pour comprendre pourquoi déverrouiller et se connecter ne sont pas la même chose, il est important de se rappeler que Bitwarden **ne stocke jamais de données non cryptées** sur ses serveurs. **Lorsque votre coffre n'est ni déverrouillé ni connecté**, les données de votre coffre n'existent sur le serveur que sous leur **forme cryptée**.

## Se connecter

**Se connecter** à Bitwarden récupère les données cryptées du coffre et déchiffre les données du coffre localement sur votre appareil. En pratique, cela signifie deux choses :

1. La connexion nécessitera toujours que vous utilisiez votre mot de passe principal ou **vous connectiez avec l'appareil** pour accéder à la **clé de chiffrement du compte** qui sera nécessaire pour déchiffrer les données du coffre.

Cette étape est également celle où **toutes les méthodes d'identifiant en deux étapes activées** seront requises.

2. La connexion nécessitera toujours que vous soyez connecté à Internet (ou, si vous êtes auto-hébergé, connecté au serveur) pour télécharger le coffre crypté sur le disque, qui sera ensuite déchiffré dans la mémoire de votre appareil.

## Déverrouillage

**Le déverrouillage** ne peut être effectué que lorsque vous êtes déjà connecté. Cela signifie, selon la section ci-dessus, que votre appareil a des données de coffre **cryptées** stockées sur le disque. En pratique, cela signifie deux choses :

1. Vous n'avez pas spécifiquement besoin de votre mot de passe principal. Bien que votre mot de passe principal *puisse* être utilisé pour déverrouiller votre coffre, d'autres méthodes comme les codes PIN et la biométrie peuvent également être utilisées.

### Note

Lorsque vous configurez un code PIN ou la biométrie, une nouvelle clé de chiffrement dérivée du code PIN ou du facteur biométrique est utilisée pour chiffrer la **clé de chiffrement du compte**, à laquelle vous aurez accès en vertu d'être connecté, et stockée sur le disque<sup>a</sup>.

**Déverrouiller** votre coffre provoque la clé PIN ou biométrique pour déchiffrer la clé de chiffrement de compte en mémoire. La clé de chiffrement de compte déchiffrée est ensuite utilisée pour déchiffrer toutes les données du coffre en mémoire.

**Verrouiller** votre coffre entraîne la suppression de toutes les données de coffre déchiffrées, y compris la clé de chiffrement de compte déchiffrée.

<sup>a</sup> - Si vous utilisez l'option **Verrouiller avec le mot de passe principal au redémarrage**, cette clé est uniquement stockée en mémoire plutôt que sur le disque.

2. Vous n'avez pas besoin d'être connecté à Internet (ou, si vous êtes auto-hébergé, connecté au serveur).