MON COMPTE > SE CONNECTER & DÉVERROUILLER

Déverrouiller avec la biométrie

Déverrouiller avec la biométrie

Bitwarden peut être configuré pour accepter la biométrie comme méthode pour déverrouiller votre coffre.

La biométrie peut **uniquement être utilisée pour déverrouiller** votre coffre, vous devrez toujours utiliser votre mot de passe principal ou vous connecter avec l'appareil, et toute méthode de connexion en deux étapes activée lorsque vous **vous connectez**. Déverrouiller avec la biométrie n'est pas une fonctionnalité conçue pour être un identifiant sans mot de passe, si vous n'êtes pas sûr de la différence, voir Comprendre déverrouiller vs. se connecter.

> **Tip**
>
> Les fonctionnalités de biométrie font partie de la sécurité intégrée dans votre appareil et/ou système d'exploitation. Bitwarden utilise les API natives pour effectuer cette validation, et donc **Bitwarden ne reçoit aucune information de biométrie** de l'appareil.

Activer le déverrouillage avec la biométrie

Le déverrouillage avec la biométrie peut être activé pour Bitwarden sur mobile, ordinateur de bureau et extensions de navigateur :

⇒Mobile

Activer pour mobile

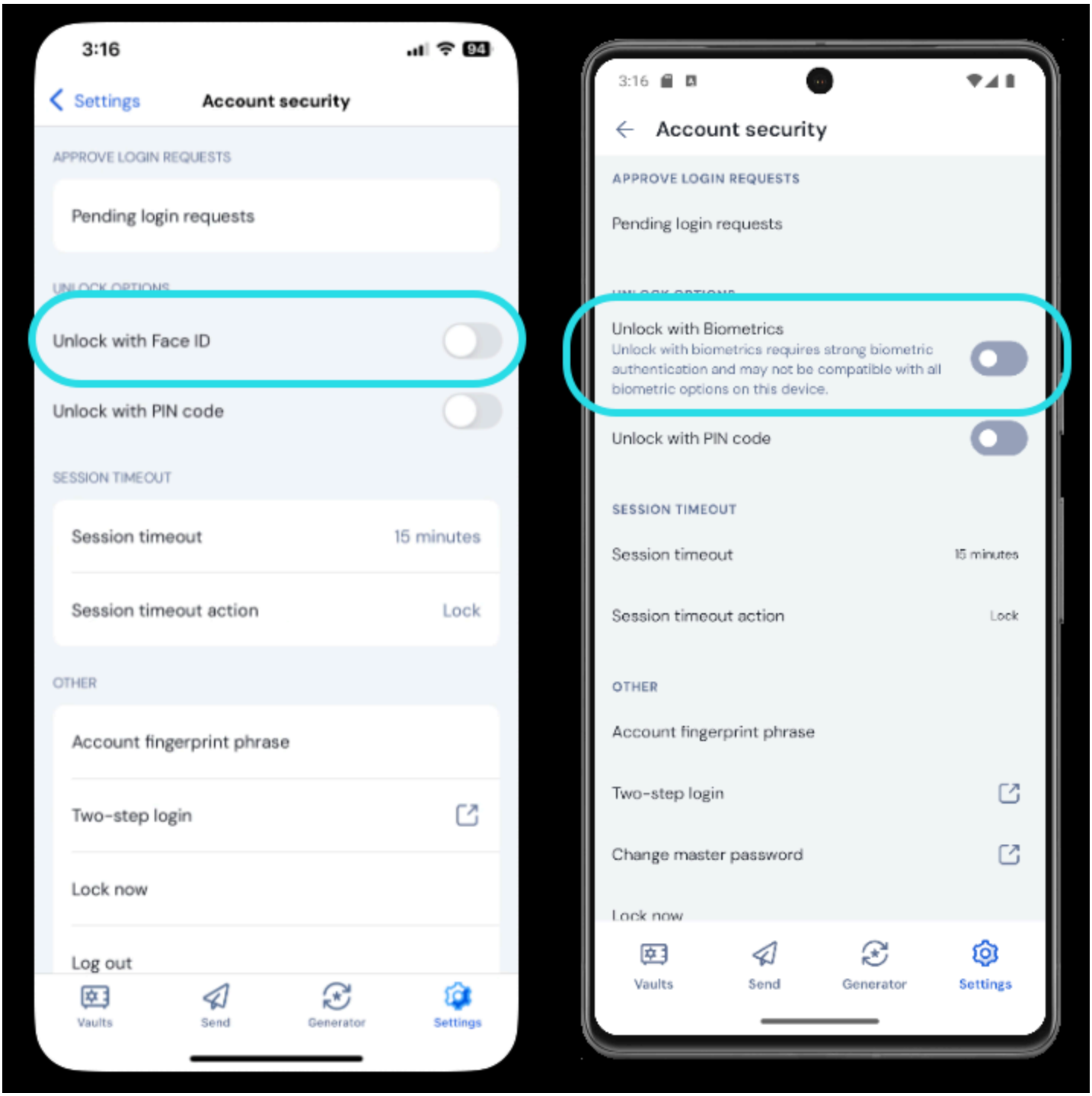
Déverrouiller avec la biométrie est pris en charge pour Android (Google Play ou FDroid) via déverrouillage par empreinte digitale ou déverrouillage par reconnaissance faciale, et pour iOS via Touch ID et Face ID.

Pour activer le déverrouillage avec la biométrie pour votre appareil mobile :

1. Dans les paramètres natifs de votre appareil (par exemple, l'application **Paramètres** iOS), assurez-vous que votre méthode de biométrie est activée.

2. Dans votre application Bitwarden, ouvrez l'onglet **Paramètres**.

3. Ouvrez la section sécurité du compte et appuyez sur l'option biométrie que vous souhaitez activer. Ce qui est disponible sur cet écran est déterminé par les capacités matérielles de votre appareil et ce que vous avez activé (**première étape**), par exemple :



Activer Face ID sur iOS

En tapant sur l'option, on vous demandera de saisir votre biométrie (par exemple, visage ou empreinte de pouce). Le bouton basculera lorsque le déverrouillage avec la biométrie sera activé avec succès.

Désactivé en attente de vérification du mot de passe principal

Si vous recevez un message signalant que la biométrie est désactivée pour la saisie automatique en attente de vérification de votre mot de passe principal :

1. Désactivez temporairement la saisie automatique dans Bitwarden.

2. Réactivez la biométrie dans Bitwarden.

3. Réactivez la saisie automatique dans Bitwarden.

⇒Ordinateur

Activer pour le bureau

Déverrouiller avec la biométrie est pris en charge pour Windows via Windows Hello en utilisant un code PIN, la reconnaissance faciale, ou d'autres matériels qui répondent aux exigences biométriques de Windows Hello et pour macOS via Touch ID.

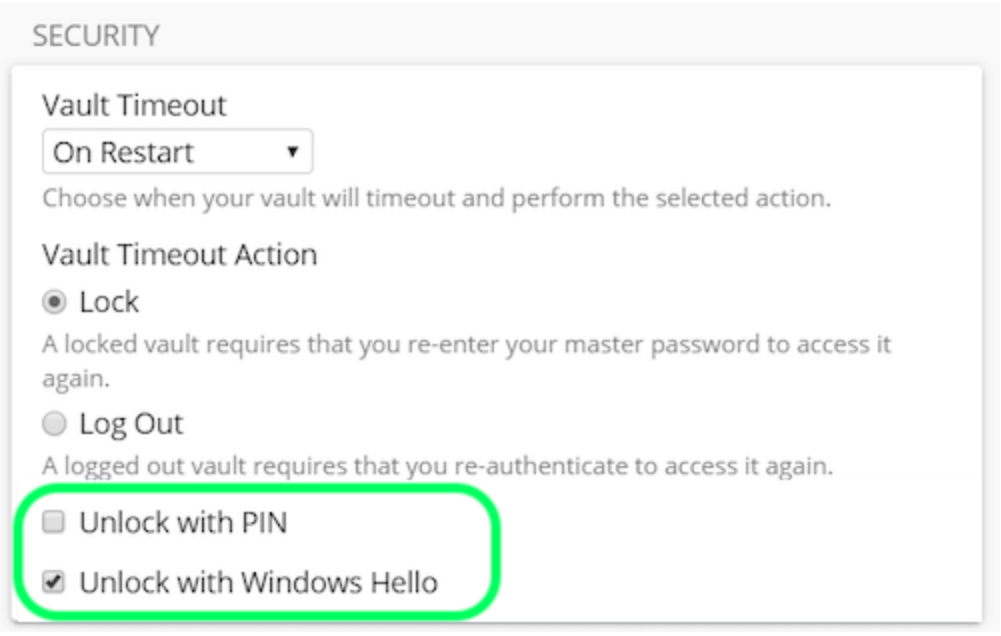
Déverrouiller avec la biométrie est défini séparément pour chaque compte connecté à l'application de bureau. Pour activer le déverrouillage avec la biométrie :

1. Dans les paramètres natifs de votre appareil (par exemple, l'application **Préférences Système** de macOS), assurez-vous que votre méthode de biométrie est activée.

   > **Tip**
   >
   > Les utilisateurs de Windows peuvent avoir besoin d'installer le Microsoft Visual C++ Redistributable avant de pouvoir activer Windows Hello dans les préférences de bureau.

2. Dans votre application Bitwarden, ouvrez vos paramètres (sur Windows, **Fichier** → **Paramètres**) (sur macOS, **Bitwarden** → **Préférences**).

3. Dans la section sécurité, sélectionnez l'option de biométrie que vous souhaitez activer. Ce qui est disponible sur cet écran est déterminé par les capacités matérielles de votre appareil et ce que vous avez activé (**étape 1**), par exemple :

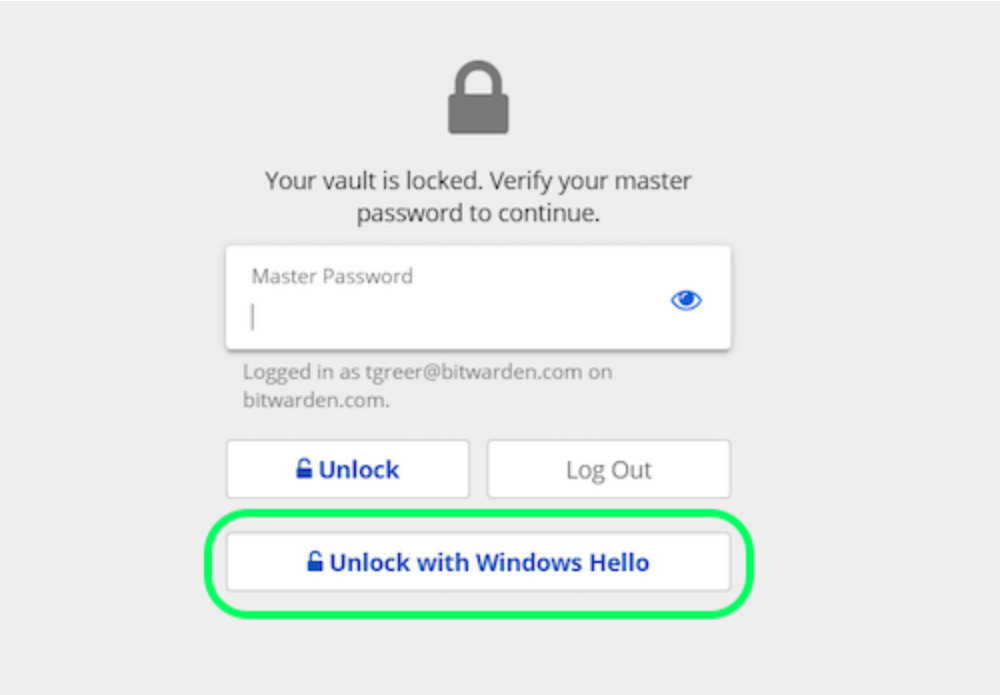


Déverrouiller avec Windows Hello

4. Optionnellement, sélectionnez soit l'option **Exiger un mot de passe (ou PIN) au démarrage de l'application** soit l'option **Demander pour *biométrie* au démarrage de l'application** pour définir comment votre application de bureau se comportera lorsque vous démarrerez l'application.

> **Tip**
>
> Si vous utilisez Windows, Bitwarden recommande d'utiliser l'option **Exiger un mot de passe (ou un PIN) lors du premier identifiant après le démarrage** afin de maximiser la sécurité.

Si vous ne sélectionnez aucune option, vous pouvez simplement sélectionner le bouton **Déverrouiller avec *biométrie*** sur l'écran d'identifiant pour demander votre option de biométrie :



Déverrouiller avec Windows Hello

⇒Extension de navigateur

À propos de la biométrie dans les extensions de navigateur

Le déverrouillage avec la biométrie est pris en charge pour les extensions grâce à une intégration avec l'application de bureau Bitwarden. En termes pratiques, cela signifie :

1. **Pour toutes les extensions de navigateur**, vous devrez activer déverrouiller avec la biométrie sur le bureau avant de continuer. **Pour tous sauf Safari**, l'application de bureau Bitwarden doit être connectée et en cours d'exécution pour utiliser déverrouiller avec la biométrie pour une extension de navigateur.

2. Les extensions de navigateur prennent en charge les mêmes options de biométrie que le bureau ; pour Windows via Windows Hello en utilisant un code PIN, la reconnaissance faciale, ou d'autres matériels qui répondent aux exigences biométriques de Windows Hello et pour macOS via Touch ID.

Deux choses à garder à l'esprit avant d'activer l'intégration sont **Autorisation** et **Supportabilité**, documentées ci-dessous :

Permissions

Pour faciliter cette intégration, les extensions de navigateur **sauf Safari** vous demanderont d'accepter une nouvelle autorisation pour que Bitwarden puisse `communiquer avec des applications natives coopératives`. Cette autorisation est sûre, mais **facultative**, et permettra l'intégration qui est nécessaire pour activer déverrouiller avec la biométrie.

Refuser cette autorisation vous permettra d'utiliser l'extension du navigateur comme d'habitude, sans la fonctionnalité de déverrouillage avec la biométrie.

Supportabilité

Le déverrouillage avec la biométrie est pris en charge pour les extensions sur les navigateurs basés sur **Chromium** (Chrome, Edge, Opera, Brave, et plus), Firefox 87+, et Safari 14+. Déverrouiller avec la biométrie est **actuellement pas pris en charge pour**:

- Firefox ESR (Firefox v87+ fonctionnera).
- Applications de bureau Microsoft App Store (une application de bureau Windows chargée en parallèle, disponible sur bitwarden.com/fr-fr/telecharger fonctionnera parfaitement).
- Applications de bureau MacOS chargées latéralement (une application de bureau de l'App Store fonctionnera parfaitement).

Activer pour les extensions de navigateur

Pour activer le déverrouillage avec la biométrie pour votre extension de navigateur :

> **Tip**
>
> La biométrie (Windows Hello ou Touch ID) doit être activée dans votre application de bureau avant de continuer. Si vous ne voyez pas l'option Windows Hello dans votre application de bureau, vous devrez peut-être installer le redistribuable Microsoft Visual C++. De plus, **si vous utilisez Safari**, vous pouvez passer directement à **l'étape 4**.

1. Dans votre application de bureau Bitwarden, naviguez vers les paramètres (sur Windows, **Fichier** → **Paramètres**) (sur macOS, **Bitwarden** → **Préférences**).
2. Faites défiler vers le bas jusqu'à la section des options, et cochez la case **Autoriser l'intégration du navigateur**.

   > **Note**
   >
   > Facultativement, cochez l'option **Exiger une vérification pour l'intégration du navigateur** pour nécessiter une étape de vérification d'empreinte digitale unique lorsque vous activez l'intégration.

3. Dans votre navigateur, accédez au gestionnaire d'extensions (par exemple, `chrome://extensions` ou `brave://extensions`), ouvrez Bitwarden, et activez l'option **Permettre l'accès aux URL de fichiers**.

   Tous les navigateurs ne nécessiteront pas que cela soit activé, alors n'hésitez pas à sauter cette étape et à y revenir seulement si la procédure restante ne fonctionne pas.

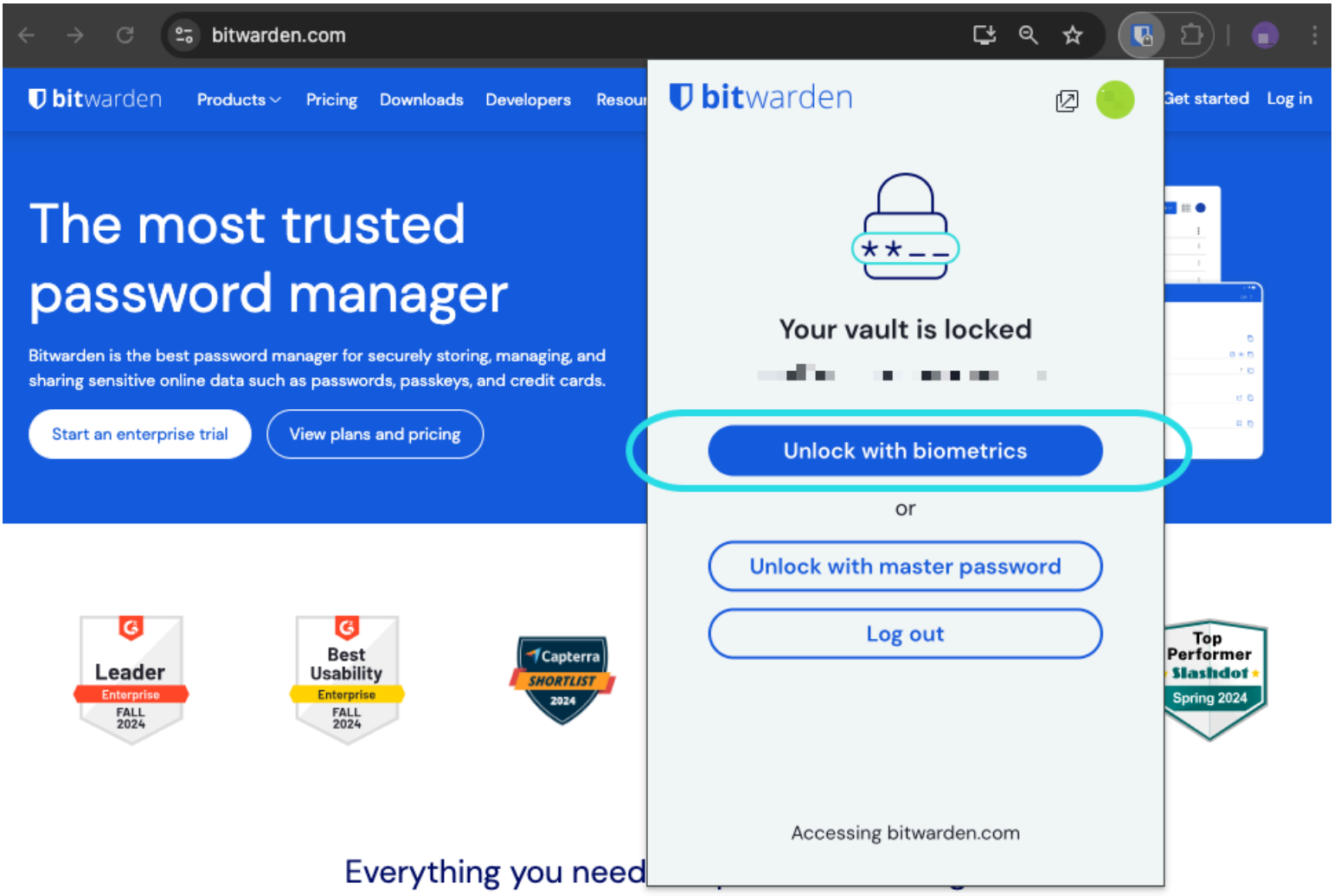
4. Dans l'extension de votre navigateur, ouvrez l'onglet **Paramètres**.
5. Faites défiler vers le bas jusqu'à la section de sécurité et cochez la case **Déverrouiller avec la biométrie**.

   > **Tip**
   >
   > Il se peut qu'à ce stade, on vous demande d'autoriser Bitwarden à `communiquer avec des applications natives coopératives`. Cette autorisation est sûre, mais **facultative** et permet uniquement à l'extension du navigateur de communiquer avec le bureau comme décrit ci-dessus.

   Vous serez invité par votre application de bureau à entrer votre biométrie. En faisant cela, vous terminerez la procédure de configuration initiale. Si vous avez choisi d'exiger une vérification (**deuxième étape**), vous devrez approuver une vérification de l'empreinte digitale.

6. Si vous souhaitez que l'extension du navigateur vous demande automatiquement votre entrée biométrique lors du lancement, assurez-vous que l'option **Demander la biométrie au lancement** est activée.

L'extension du navigateur vous demandera automatiquement votre biométrie lorsque vous l'ouvrirez. Si vous activez l'option d'invite (**étape six**), utilisez le bouton **Déverrouiller avec la biométrie** sur l'écran Déverrouillé :



Déverrouiller avec la biométrie

> **Tip**
>
> Votre application de bureau doit être connectée mais n'a pas besoin d'être déverrouillée pour déverrouiller une extension de navigateur avec la biométrie.

Désactivé en attente de vérification du mot de passe principal

Si vous recevez un message signalant que le déverrouillage biométrique est désactivé pour la saisie automatique en attente de vérification de votre mot de passe principal :

1. Désactivez temporairement la saisie automatique dans Bitwarden.
2. Réactivez la biométrie dans Bitwarden.
3. Réactivez la saisie automatique dans Bitwarden.

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[a].
   >
   > **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.
   >
   > [a] - 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).