

MON COMPTE > SE CONNECTER & DÉVERROUILLER

Se connecter avec Appareil

Afficher dans le centre d'aide:

<https://bitwarden.com/help/log-in-with-device/>

Se connecter avec Appareil

Saviez-vous que vous pouvez vous connecter à Bitwarden en utilisant un appareil secondaire au lieu de votre mot de passe principal ? Se connecter avec un appareil est une approche sans mot de passe pour l'authentification, éliminant le besoin d'entrer votre mot de passe principal en envoyant des demandes d'authentification à tout appareil spécifique sur lequel vous êtes actuellement connecté pour approbation. [Apprenez-en plus sur notre mise en œuvre de l'encryption à connaissance zéro.](#)

La connexion avec l'appareil peut être initiée sur le coffre web, l'extension de navigateur, l'application de bureau et l'application mobile. Les demandes émises par ces applications peuvent être approuvées sur les applications mobiles et les applications de bureau.


Préparez-vous à vous connecter avec un appareil

Pour configurer la connexion avec un appareil :

- Connectez-vous normalement à l'application initiatrice (coffre web, extension de navigateur, bureau ou application mobile) au moins une fois pour que Bitwarden puisse reconnaître votre appareil.

Note

L'utilisation du mode Incognito ou de la navigation privée empêche Bitwarden d'enregistrer votre navigateur, vous ne pourrez donc pas vous connecter avec un appareil dans une fenêtre de navigateur privée.

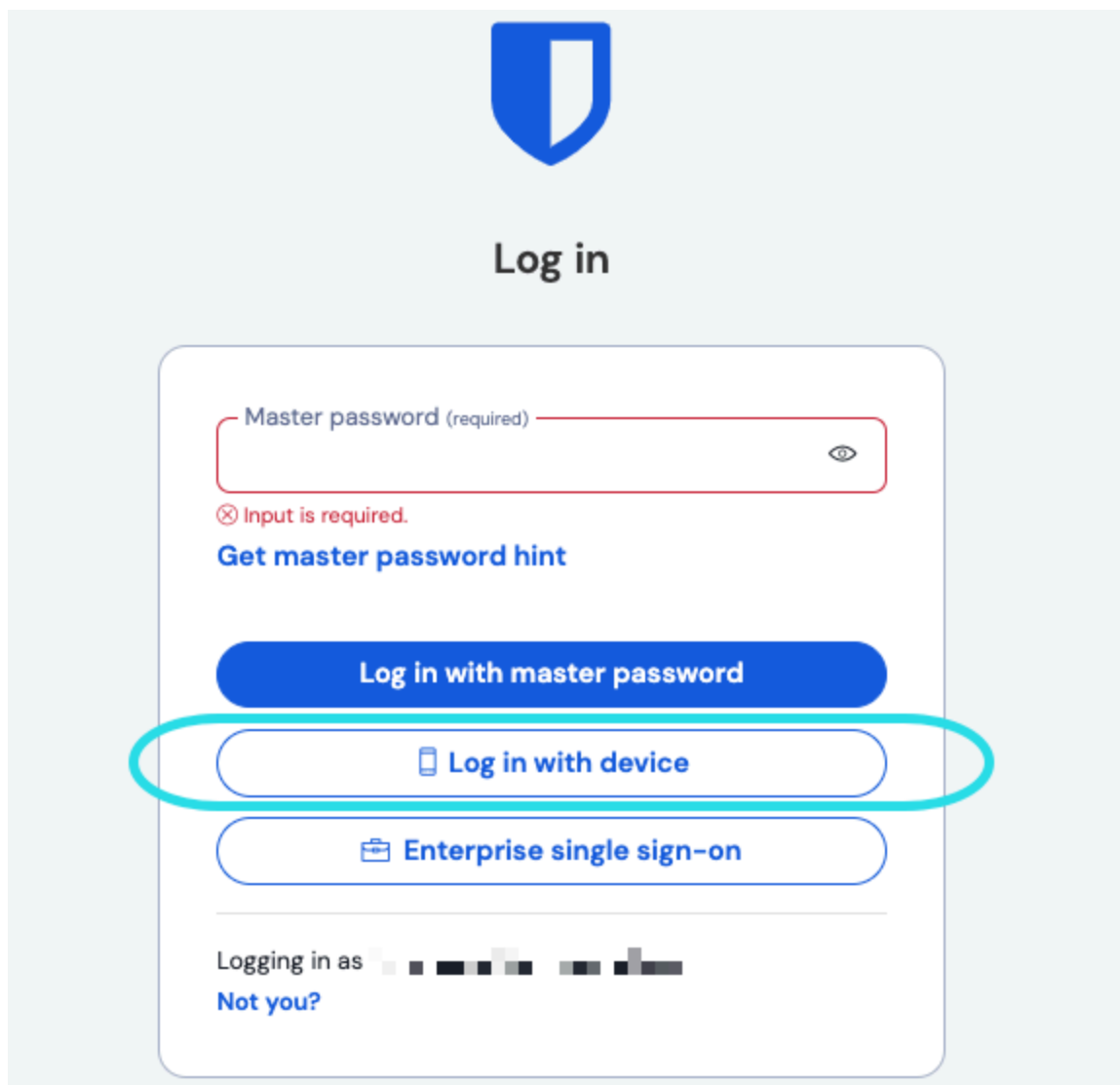
- Avoir un compte reconnu sur une application approuvée (application mobile ou de bureau). La reconnaissance d'un compte nécessite que vous vous soyez connecté avec succès à cet appareil à tout moment.
- Sur l'application d'approbation, ouvrez le  **Paramètres** et, dans la section **Sécurité du compte** ou **Sécurité**, activez **Approuver les demandes d'identifiant**.

Note

Si, en tant que membre d'une organisation d'entreprise, vous êtes soumis à la [politique de sécurité exigeant le SSO](#), vous ne pourrez pas utiliser l'option **Se connecter avec l'appareil**. Vous devrez [utiliser SSO pour vous connecter](#) à la place.

Se connecter avec un appareil

Sur l'écran d'identifiant de l'application initiale, entrez votre adresse de courriel et sélectionnez **Continuer**. Ensuite, sélectionnez l'option **Se connecter avec l'appareil** :



Se connecter avec un appareil

En utilisant **Se connecter avec l'appareil** enverra des demandes d'authentification à toutes les applications mobiles ou de bureau auxquelles vous êtes actuellement connecté, et avez activé l'option, pour approbation. Comparez les phrases d'empreinte sur le client initiateur et approbateur et, si elles correspondent, sélectionnez **Confirmer l'identifiant** sur l'appareil approbateur. Notez que c'est une empreinte unique qui n'est pas la même que votre [phrase d'empreinte de compte](#).

Les demandes expirent après 15 minutes si elles ne sont pas approuvées ou refusées. Si vous ne recevez pas de demandes d'identifiant ou si vous utilisez F-Droid, essayez de [synchroniser manuellement votre coffre](#) depuis l'application mobile.

Note

Si vous utilisez l'option **Identifiant avec appareil**, vous devrez toujours utiliser toute méthode d'[identifiant en deux étapes](#) actuellement active.

Comment ça marche

Lorsqu'une connexion avec un appareil est initiée :

1. Le client initiateur envoie une requête POST, qui comprend le courriel du compte, une clé publique unique de demande d'authentification^a, et un code d'accès, à une table de Demandes d'Authentification dans la base de données Bitwarden.
2. Les appareils enregistrés, c'est-à-dire les applications mobiles ou de bureau qui sont connectées et ont un [GUID spécifique à l'appareil](#) stocké dans la base de données Bitwarden, sont fournis la demande.
3. Lorsque la demande est approuvée, le client approbateur crypte la clé principale du compte et le hachage du mot de passe principal en utilisant la clé publique de demande d'authentification incluse dans la demande.
4. Le client approbateur met ensuite le PUT sur la clé maître chiffrée et le hachage du mot de passe principal chiffré sur l'enregistrement de la demande d'authentification et marque la demande comme accomplie.
5. Le client initiateur GET le mot de passe principal crypté et le hachage du mot de passe principal crypté.
6. Le client initiateur déchiffre ensuite **localement** la clé principale et le hachage du mot de passe principal à l'aide de la clé privée de la demande d'authentification.
7. Le client initiateur utilise ensuite le code d'accès et la demande d'authentification accomplie pour authentifier l'utilisateur avec le service Identité de Bitwarden.

^a - Les clés publiques et privées de la demande d'authentification sont générées de manière unique pour chaque demande d'identifiant sans mot de passe et n'existent que tant que la demande est en cours. Les demandes expirent et sont purgées de la base de données toutes les 15 minutes si elles ne sont pas approuvées ou refusées.