CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO

Identifiant avec SSO FAQs

Identifiant avec SSO FAQs

Cet article contient des questions fréquemment posées (FAQs) concernant **l'identifiant avec SSO**.

Pour plus d'informations de haut niveau sur **l'identifiant avec SSO**, référez-vous à à propos de l'identifiant avec SSO

Utilisation de l'identifiant avec SSO

Q: Pourquoi l'identifiant avec SSO nécessite-t-il mon mot de passe principal?

R : La connexion avec SSO permet à vos employés d'utiliser votre fournisseur d'identité (IdP) existant pour **authentifier** leur identité. Ce qui rend l'identifiant avec SSO unique par rapport aux autres outils, c'est qu'il conserve notre modèle de chiffrement de bout en bout sans connaissance préalable. Personne chez Bitwarden ne devrait avoir accès à vos données de coffre et, surtout, **votre fournisseur d'identité ne devrait pas non plus**.

C'est pourquoi l'identifiant Bitwarden avec l'offre SSO **découple l'authentification et le déchiffrement**. Votre IdP peut confirmer qu'Alice est bien Alice, mais ne peut pas et ne doit pas avoir les outils pour décrypter le coffre d'Alice. Seule Alice peut avoir cet outil et, de manière pratique, c'est son mot de passe principal !

En pratique, cela signifie qu'à chaque fois qu'un employé se connecte à Bitwarden en utilisant SSO, il devra utiliser son mot de passe principal pour décrypter son coffre, protégeant ainsi les informations d'identification et les secrets critiques de votre entreprise.

> **ⓘ Note**
>
> Bitwarden propose deux solutions pour les organisations qui permettront aux membres approuvés de l'organisation d'accéder à leur compte Bitwarden sans utiliser un mot de passe principal :
>
> **SSO avec appareil de confiance** est une fonctionnalité qui permet aux organisations utilisant l'identifiant avec SSO de créer et de stocker les clés de chiffrement de l'appareil du membre, éliminant ainsi le besoin d'entrer un mot de passe principal. En savoir plus sur SSO avec des appareils de confiance.
>
> **Les organisations auto-hébergées par Bitwarden** peuvent exploiter Key Connector pour fournir des clés de déchiffrement aux clients Bitwarden au lieu d'obliger les utilisateurs à déchiffrer les données du coffre-fort avec leurs mots de passe principaux. Apprenez-en plus ici et ici.

Q: Le changement de mon mot de passe SSO affectera-t-il mon mot de passe principal Bitwarden?

A: Non, votre mot de passe principal restera le même. À moins que votre organisation n'utilise Key Connector pour auto-héberger les clés de déchiffrement, votre mot de passe principal doit être utilisé pour déchiffrer les données du coffre.

Q: L'authentification SSO remplace-t-elle mon mot de passe principal et mon courriel?

A: Non. L'identifiant avec SSO utilise votre fournisseur d'identité existant (IdP) pour vous authentifier dans Bitwarden, cependant votre mot de passe principal et votre courriel doivent toujours être entrés afin de déchiffrer les données de votre coffre, à moins que votre organisation n'utilise le Key Connector pour auto-héberger les clés de déchiffrement.

Q: Puis-je toujours me connecter avec mon mot de passe principal si mon organisation a activé SSO ?

A: Par défaut, oui, vous pouvez utiliser votre adresse de courriel et votre mot de passe principal pour vous connecter à Bitwarden. Cependant, si votre organisation active à la fois les politiques de sécurité d'organisation unique et d'authentification unique, ou si votre organisation utilise Key Connector, tous les utilisateurs non administrateurs devront se connecter avec SSO.

Q: Comment fonctionne l'identifiant avec SSO pour les nouveaux utilisateurs ("juste-à-temps") ?

A: Les nouveaux utilisateurs qui sélectionnent **Se connecter → SSO d'Entreprise** à partir de l'invitation de l'organisation seront placés dans le statut `Accepté` de leur organisation jusqu'à ce qu'ils soient confirmés par un administrateur. Lorsque cet utilisateur est affecté à un groupe manuellement ou via le connecteur de répertoire, il recevra l'accès aux éléments partagés appropriés. La provision JIT est recommandée si votre objectif est d'avoir des membres sans mot de passe principal qui ne peuvent utiliser que des appareils de confiance.

Q: Ai-je encore besoin d'utiliser Bitwarden Directory Connector?

A: Si vous gérez votre groupe et vos affectations de collection Bitwarden directement dans Bitwarden, il n'est pas nécessaire d'utiliser le Directory Connector. Cependant, si vous souhaitez avoir des groupes et des utilisateurs synchronisés automatiquement avec l'annuaire de votre organisation, nous recommandons d'utiliser l'identifiant avec SSO en conjonction avec le connecteur d'annuaire pour la solution la plus complète.

Q: Dois-je entrer mon identifiant SSO chaque fois que je me connecte avec mon identifiant ?

A: Non ! Si votre organisation utilise la vérification de domaine, vous n'aurez pas besoin d'entrer cet identifiant. Sinon, marquer la page **Entreprise Single Sign-On** avec votre identifiant SSO inclus comme une chaîne de requête vous permettra d'enregistrer le problème de le saisir à chaque fois. Par exemple:

- `https://vault.bitwarden.com/#/sso?identifier=your-org-id` pour les instances hébergées dans le cloud
- `https://your.domain.com/#/sso?identifier=your-org-id` pour les instances auto-hébergées

Q: Comment puis-je modifier les valeurs de configuration SSO pré-générées?

A: Les valeurs de configuration SSO pré-générées, y compris **l'ID de l'entité SP**, **l'URL des métadonnées SAML 2.0**, **l'URL ACS** et **le chemin de rappel** peuvent être modifiées dans les environnements auto-hébergés en changeant la valeur de `url:` dans `.bwdata/config.yml` et en exécutant la commande `./bitwarden.sh rebuild` pour appliquer votre modification.

Sécurité

Q: Comment l'identifiant avec SSO fonctionne-t-il avec le modèle de chiffrement à connaissance zéro ?

A: L'identifiant Bitwarden avec SSO et le mot de passe principal n'effectue que l'authentification de l'utilisateur et ne déchiffre pas les données de l'utilisateur. L'ajout de la fonctionnalité SSO n'introduit aucune information supplémentaire identifiable individuellement dans la base de données Bitwarden.

Facturation

Q: Quels plans offrent un identifiant avec SSO ?

A: Notre plan Entreprise offre cette fonctionnalité.

Q: Comment puis-je mettre à niveau mon plan afin que je puisse utiliser l'identifiant avec SSO ?

A: Dans la Console Admin, naviguez vers la page **Abonnements** → **Facturer** et sélectionnez **Mettre à niveau le plan**. Nous vous recommandons vivement de tester l'identifiant avec SSO en commençant un Essai Gratuit de 7 Jours pour l'Entreprise.

Soutenabilité

Q : Bitwarden prend-il en charge OAuth 2.0 ?

A: Bitwarden prend en charge OpenID Connect, mais ne prend pas en charge OAuth pour le moment.

Q: L'identifiant avec SSO fonctionnera-t-il avec une instance auto-hébergée de Bitwarden?

A: Oui! La connexion avec SSO fonctionnera avec les instances auto-hébergées, qu'elles soient sur site ou dans votre propre cloud, tant que votre serveur d'identité est accessible depuis l'instance.

Q: L'identifiant avec SSO fonctionne-t-il dans les environnements cloud hybrides?

A: Oui! La connexion avec SSO nécessite uniquement la capacité de se connecter à votre fournisseur d'identité depuis votre instance de Bitwarden. Il peut être utilisé avec des fournisseurs d'identité sur le cloud ou sur site, ainsi qu'avec des instances Bitwarden sur le cloud ou auto-hébergées.

Q: Si mon fournisseur d'identité est hors ligne, les utilisateurs peuvent-ils se connecter avec SSO pour s'authentifier dans Bitwarden?

A: Si votre fournisseur d'identité est hors ligne, les utilisateurs doivent se connecter en utilisant leur courriel et leur mot de passe principal. Cela peut changer à l'avenir alors que nous activons davantage de mécanismes de contrôle d'authentification pour les organisations.