

RESOURCE CENTER

Guide de référence de l'entreprise pour l'authentification Bitwarden

Présentation des capacités critiques des offres d'authentification et de SSO de Bitwarden

Get the full interactive view at <https://bitwarden.com/fr-fr/resources/reference-guide-bitwarden-authentication/>



Type d'authentification	Qu'est-ce que c'est ?	Considérations relatives au déploiement <i>Toutes les options de déploiement de l'authentification s'alignent sur le modèle de cryptage de bout en bout et sans connaissance de Bitwarden.</i>
SSO avec des dispositifs de confiance	Pour une expérience sans mot de passe, les employés utilisent leurs identifiants SSO pour s'authentifier et décrypter en une seule étape. Les dispositifs enregistrés et de confiance sont en mesure de décrypter les coffres-forts et de confirmer et d'accepter les nouveaux dispositifs. Une fois qu'un dispositif est approuvé, il n'a plus besoin d'être approuvé.	<p>En sélectionnant cette option, les employés pourront se connecter et décrypter leurs coffres-forts sans avoir besoin d'un mot de passe. Les appareils de confiance sont enregistrés et peuvent confirmer les connexions et étendre la confiance à d'autres appareils.</p> <p>Lors de la création du compte, le fournisseur SSO authentifie l'utilisateur et enregistre le client qui se connecte en tant que premier dispositif de confiance, ce qui lui permet de décrypter le coffre-fort.</p> <p>Des appareils de confiance supplémentaires peuvent être enregistrés avec l'approbation de l'application de bureau Bitwarden, de l'application mobile, de l'application web ou d'un administrateur Bitwarden.</p> <p>Chaque appareil de confiance dispose d'une clé de chiffrement individuelle, et le chiffrement et la sécurité de bout en bout à connaissance zéro sont maintenus entre les appareils.</p> <p>Ressources complémentaires :</p> <p>Configurer le SSO avec des appareils de confiance</p> <p>Le SSO d'entreprise sans mot de passe améliore la productivité et l'expérience d'ouverture de session des employés.</p>
Identifiant avec SSO	L'authentification de l'utilisateur est séparée du décryptage du coffre-fort en s'appuyant sur le fournisseur d'identité de votre entreprise pour authentifier les utilisateurs dans leur coffre-fort Bitwarden et en utilisant des mots de passe maîtres pour le décryptage des données du coffre-fort.	<p>Cette option prend en charge les fournisseurs d'identité utilisant les normes SAML 2.0 ou OpenID Connect.</p> <p>En sélectionnant cette option, chaque fois qu'un employé se connectera à Bitwarden en utilisant le SSO, il devra utiliser son mot de passe principal pour décrypter son coffre-fort, protégeant ainsi</p>

Type d'authentification	Qu'est-ce que c'est ?	Considérations relatives au déploiement <i>Toutes les options de déploiement de l'authentification s'alignent sur le modèle de cryptage de bout en bout et sans connaissance de Bitwarden.</i>
Connexion avec SSO et cryptage géré par le client	<p>Les employés utilisent leurs identifiants SSO pour s'authentifier et décrypter en une seule étape. Cette option transfère la conservation des mots de passe principaux des utilisateurs aux entreprises, qui doivent déployer un connecteur de clés pour stocker les clés des utilisateurs.</p>	<p>les informations d'identification et les secrets critiques de votre entreprise.</p> <p>Ressources complémentaires :</p> <p>Configuration de votre organisation à l'aide de la connexion avec SSO</p> <p>Mise en place de la connexion avec SSO</p> <hr/> <p>Pour les entreprises qui ont largement adopté des implémentations SSO et qui souhaitent intégrer l'authentification et le décryptage dans une solution sur site, Bitwarden propose un SSO avec un cryptage géré par le client.</p> <p>Dans ce scénario, les entreprises gèrent un agent connecteur clé. Cela nécessite une connexion à une base de données qui stocke les clés d'utilisateur cryptées, et une paire de clés RSA pour crypter et décrypter ces clés.</p> <p>Cette approche maintient une architecture de cryptage sans connaissance car aucune clé de décryptage ne passe par les serveurs Bitwarden à aucun moment.</p> <p>La gestion des clés cryptographiques est extrêmement sensible et n'est recommandée qu'aux entreprises disposant d'une équipe et utilisant une infrastructure qui a déjà déployé et géré un serveur de clés en toute sécurité. Le SSO avec cryptage géré par le client est disponible pour les clients qui hébergent eux-mêmes Bitwarden.</p> <p>Ressources complémentaires :</p> <p>Livre blanc : Choisir la bonne stratégie de connexion SSO</p>

Type
d'authentification

Qu'est-ce que c'est ?

Considérations relatives au déploiement
Toutes les options de déploiement de l'authentification s'alignent sur le modèle de cryptage de bout en bout et sans connaissance de Bitwarden.

Article d'aide : [Connexion avec l'appareil](#)