bitwarden | Article du Centre d'Aide

Glossaire des termes Bitwarden

Afficher dans le centre d'aide:
https://bitwarden.com/help/bitwarden-glossary/

Glossaire des termes Bitwarden

Général

Terminologie	Définition
Compte	Un compte Bitwarden est l'enregistrement défini par votre nom d'utilisateur et votre mot de passe principal (que vous seul connaissez). Votre compte Bitwarden est utilisé pour accéder aux services de Bitwarden et contient également des informations telles que la facturation, les paramètres, la préférence de langue, et plus encore.
Changement de compte	La fonctionnalité Bitwarden pour les clients de bureau et mobiles qui vous permet de passer facilement entre plusieurs comptes, tels que vos comptes personnels ou professionnels. En savoir plus.
Compte Personnel	Un compte personnel Bitwarden est l'enregistrement défini par votre nom d'utilisateur et votre mot de passe principal (que vous seul connaissez) qui n'est pas associé à un coffre d'Organisation ou lié à une entreprise ou une entité commerciale. Un compte personnel est généralement configuré avec une adresse de courriel personnelle et contient des éléments de coffre dont vous seul avez la propriété et le contrôle.
Compte d'entreprise	Un compte Bitwarden professionnel est l'enregistrement défini par votre nom d'utilisateur et votre mot de passe principal (que vous seul connaissez) qui est associé à une organisation liée à une entreprise ou à une entité commerciale. Un compte professionnel est généralement configuré avec une adresse de courriel professionnel. Un compte d'entreprise est régi par l'organisation associée. Tous les éléments de coffre ou secrets contenus dans un compte d'entreprise doivent être considérés comme propriétaires de l'entreprise ou de l'entité commerciale concernée.
Clé API	La clé de l'Interface de programmation des applications (API) est un code d'identification spécifique pour un utilisateur ou un programme. La clé API peut être utilisée pour intégrer d'autres applications avec Bitwarden pour des utilisations d'automatisation, de surveillance, et plus encore. La clé API est un secret sensible et doit être manipulée avec précaution.
Clients / Client Bitwarden	Le client, ou l'application client, est l'application qui se connecte à Bitwarden. Cela inclut les applications web, mobiles et de bureau, le CLI Bitwarden et les extensions de navigateur. Les clients peuvent être téléchargés depuis la page de téléchargements.
Connecteur de Répertoire	Une application pour synchroniser les utilisateurs et les groupes d'un service d'annuaire vers une organisation Bitwarden. Le Connecteur de Répertoire Bitwarden provisionne et déprovisionne

Terminologie	Définition
	automatiquement les utilisateurs, les groupes et les associations de groupe à partir du répertoire source. Apprenez-en plus.
Vérification de domaine	Le processus par lequel une organisation prouve sa propriété d'un domaine internet spécifique (par exemple, mycompany.com). La vérification de domaine permet d'activer des fonctionnalités supplémentaires, telles que la possibilité pour les utilisateurs de sauter la saisie de l'identifiant SSO lors du processus d'identifiant. Apprenez-en plus.
Groupes	Un ensemble de membres de l'organisation. Les groupes relient les utilisateurs entre eux et fournissent un moyen évolutif d'attribuer des autorisations, telles que l'accès aux collections, aux projets ou aux secrets, ainsi que des autorisations au sein de chaque collection séparée. Lors de la création de nouveaux utilisateurs, ajoutez-les à un groupe pour qu'ils héritent automatiquement des autorisations configurées de ce groupe.
Mot de passe principal	Aussi connu sous le nom de mot de passe Bitwarden, mot de passe principal, mot de passe de compte ou mot de passe de coffre. La méthode principale (ou clé) pour accéder à votre compte et aux données Bitwarden, le mot de passe principal est utilisé à la fois pour authentifier votre identité auprès du service Bitwarden et pour déchiffrer vos données sensibles telles que les éléments du coffre ou les secrets. Bitwarden encourage les utilisateurs à en établir un qui soit mémorable, fort et unique en ce qu'il n'est utilisé que pour Bitwarden. *En 2021, Bitwarden a introduit l'Administration de Récupération de Compte (anciennement Réinitialisation du Mot de Passe Admin), qui permet aux utilisateurs d'Entreprise et aux organisations de mettre en œuvre une politique qui permet aux Administrateurs et Propriétaires de réinitialiser les mots de passe principaux pour les utilisateurs inscrits.* Apprenez-en plus.
Organisation	Une entité (entreprise, institution, groupe de personnes) qui relie les utilisateurs de Bitwarden à des données d'organisation partagées telles que les identifiants au sein d'un coffre d'organisation ou d'un projet Secrets Manager pour le partage sécurisé d'éléments.
Offre	Les plans définissent les services que Bitwarden fournit par le biais de licences, y compris les fonctionnalités disponibles et le nombre d'utilisateurs capables d'utiliser le produit. Il existe plusieurs types de plans pré-définis disponibles pour les individus ou les organisations à souscrire.

Terminologie	Définition
Politiques de sécurité	Les politiques de sécurité sont des contrôles à l'échelle de l'organisation qui aident un administrateur à maintenir une entreprise sécurisée en activant des paramètres supplémentaires pour la manière dont leurs membres (également appelés utilisateurs finaux) utilisent Bitwarden. Ces politiques de sécurité garantissent une norme uniforme de sécurité. Apprenez-en plus.
SCIM	Le système de gestion d'identité inter-domaine (SCIM) peut être utilisé pour provisionner automatiquement des membres et des groupes dans votre organisation Bitwarden. Les serveurs Bitwarden fournissent un point de terminaison SCIM qui, avec une clé API SCIM valide, acceptera les demandes de votre fournisseur d'identité (IdP) pour la provision et la déprovision des utilisateurs et du groupe. Apprenez-en plus.
Authentification unique	Un service de session et d'authentification des utilisateurs qui accorde aux employés ou aux utilisateurs l'accès aux applications avec un ensemble d'identifiants basés sur leur identité et leurs autorisations. La connexion unique a plusieurs options de mise en œuvre, et est largement compatible avec les fournisseurs d'Identité (IdPs) permettant aux clients d'utiliser leur solution existante. Apprenez-en plus.
Identifiez-vous avec SSO	Une mise en œuvre de Single Sign-On. Avec cette méthode, l'utilisateur est authentifié par un fournisseur d'Identité, puis l'utilisateur entre son mot de passe Bitwarden pour déchiffrer ses Données. Apprenez-en plus.
SSO avec des appareils de confiance	Une mise en œuvre sans mot de passe de la connexion unique. Avec cette méthode, l'utilisateur est authentifié par un fournisseur d'Identité et leurs données sont déchiffrées grâce à un processus qui utilise une clé de chiffrement d'appareil stockée sur des appareils désignés et de confiance. Apprenez-en plus.
SSO avec chiffrement géré par le client	Une mise en œuvre avancée sans mot de passe de Single Sign-On disponible pour les organisations auto-hébergées. Avec cette méthode, l'utilisateur est authentifié par un fournisseur d'Identité, puis la clé de chiffrement de l'utilisateur est automatiquement récupérée à partir d'un serveur de clés auto-hébergé en utilisant Key Connector, permettant ainsi le déchiffrement des données de l'utilisateur. Apprenez-en plus.
Abonnement	L'abonnement est l'accord transactionnel entre le client et Bitwarden dans le cadre de l'émission d'une licence. Les propriétaires s'abonnent à des plans au tarif convenu sur une base récurrente (mensuelle ou annuelle) pour les services fournis par Bitwarden décrits dans le plan.

Bitwarden - Gestionnaire de mots de passe

Terminologie	Définition
Saisie Automatique	Une fonctionnalité logicielle qui entre automatiquement les informations précédemment stockées dans un champ de formulaire. En utilisant Bitwarden, vous pouvez remplir automatiquement les identifiants via les extensions de navigateur et les appareils mobiles, et remplir automatiquement les cartes de paiement et les identités via les extensions de navigateur. Apprenez-en plus.
Collections	Une unité pour stocker un ou plusieurs éléments de coffre ensemble (identifiants, notes, cartes de paiement et identités pour un partage sécurisé) par une entreprise au sein d'une organisation Bitwarden. Apprenez-en plus.
Coffre individuel	Le coffre individuel est la zone protégée pour chaque utilisateur pour stocker un nombre illimité d'identifiants, de notes, de cartes de paiement et d'identités. Les utilisateurs peuvent accéder à leur coffre individuel Bitwarden sur n'importe quel appareil et plateforme. **Dans un contexte professionnel** Pour les utilisateurs qui font partie d'un plan Bitwarden Équipes ou Entreprise, un coffre individuel est connecté à leur adresse de courriel professionnel. Les coffres individuels sont souvent associés à, mais séparés d'un coffre d'Organisation. **Dans un contexte personnel** Pour les utilisateurs qui font partie d'un plan personnel ou Familles Bitwarden, un coffre individuel est connecté à leur adresse de courriel personnelle. Si vous faites partie d'un plan familial ou d'une organisation gratuite de deux personnes, le coffre individuel reste séparé du coffre de l'organisation, mais les deux sont accessibles par l'utilisateur. Bitwarden recommande d'associer les adresses de courriel professionnelles avec les Équipes et les Organisations d'Entreprise, et les adresses de courriel personnelles avec les organisations Familles. Note : le coffre individuel peut être désactivé pour les membres d'une organisation Entreprise grâce à une politique de sécurité d'entreprise.
Éléments / Éléments de coffre	Les éléments sont les entrées individuelles qui peuvent être enregistrées et partagées dans le gestionnaire de mots de passe Bitwarden, tels que les identifiants, les notes, les cartes de paiement et les identités.

Terminologie	Définition
Membre de l'Organisation / Membres de l'Organisation	Un utilisateur final tel qu'un employé ou un membre de la famille qui a accès aux éléments partagés de l'organisation dans leurs coffres, en plus des éléments individuels dans leur coffre individuel.
Coffre de l'Organisation	La zone protégée pour les éléments partagés. Chaque utilisateur (également appelé un "membre") qui fait partie d'une organisation peut trouver des éléments partagés dans leur affichage de coffre, aux côtés des éléments possédés individuellement. Les coffres de l'organisation permettent aux administrateurs et aux propriétaires de gérer les éléments, les utilisateurs et les paramètres de l'organisation.
Coffre / Coffres afficher	La zone de stockage sécurisée qui fournit une interface unifiée et un contrôle d'accès strict à tout élément.

Secrets Manager de Bitwarden

Terminologie	Définition
Jeton d'accès	Une clé qui facilite l'accès au compte de service et la capacité à déchiffrer les secrets stockés dans votre coffre. Apprenez-en plus.
Nom	Une étiquette définie par l'utilisateur pour un secret spécifique.
Projet	Des collections de secrets logiquement regroupées pour l'accès à la gestion par vos équipes DevOps et de cybersécurité. Apprenez-en plus.
Secret	Des paires clé-valeur sensibles, comme les clés API, que votre organisation doit stocker en toute sécurité et qui ne doivent jamais être exposées en code brut ou transmises sur des canaux non cryptés.
Compte de service	Des utilisateurs de machines non humains, comme des applications ou des pipelines de déploiement, qui nécessitent un accès programmatique à un ensemble discret de secrets.

Terminologie	Définition
Valeur	Un champ défini par l'utilisateur d'un secret stocké qui est utilisé dans les processus logiciels ou de machine. Il s'agit des informations sensibles qui sont gérées par Bitwarden Secrets Manager et peuvent inclure des clés API, des configurations d'applications, des chaînes de connexion de base de données et des variables d'environnement.

Bitwarden Passwordless.dev

Terminologie	Définition
FIDO	FIDO est l'acronyme de Fast Identité Online. Il représente un consortium qui développe des normes d'authentification sans mot de passe sécurisées et ouvertes, à l'épreuve du hameçonnage. Les protocoles FIDO, qui ont été développés par l'Alliance FIDO, comprennent : UAF : Cadre Universel d'Authentification U2F : Facteur Universel Secondaire FIDO2 : un nouveau protocole d'authentification sans mot de passe qui contient des spécifications principales WebAuthn (l'API client) et CTAP (l'API d'authentification) En savoir plus.
Clés d'accès	Les clés de passe - les identifiants dérivés de la norme FIDO2 pour chaque site web auquel un utilisateur s'inscrit - permettent aux utilisateurs de créer et de stocker des jetons cryptographiques au lieu des mots de passe traditionnels. Aujourd'hui, les clés de passe sont utilisées pour connecter les utilisateurs à une application ou un site web avec des jetons spécifiques à l'appareil pré-authentifiés. Dans le futur, le processus pourrait être utilisé avec des jetons cryptographiques partageables ou transférables. Apprenez-en plus.
sans-mot-de-passe	Sans mot de passe est le terme générique utilisé pour décrire une variété de technologies d'authentification qui ne dépendent pas des mots de passe, y compris : quelque chose qu'un utilisateur a (une clé de sécurité, un jeton, ou un appareil), quelque chose qu'ils sont (biométrie), et les clés d'accès.