bitwarden | Help Center Article

Bitwarden Glossary of Terms

View in the help center:
https://bitwarden.com/help/bitwarden-glossary/

Bitwarden Glossary of Terms

General

Terminology	Definition
Account	A Bitwarden account is the record defined by your username and master password (which only you know). Your Bitwarden account is used to access Bitwarden services and also contains information such as billing, settings, language preference, and more.
Account Switching	The Bitwarden feature for desktop and mobile clients that enables you to easily switch between multiple accounts, such as your personal or work accounts. Learn more.
Personal Account	A personal Bitwarden account is the record defined by your username and master password (which only you know) that is not associated with an Organizational vault or related to a company or business entity. A personal account is generally set up with a personal email address and contains vault items over which only you have ownership and control.
Business Account	A business Bitwarden account is the record defined by your username and master password (which only you know) that is associated with an Organization related to a company or business entity. A business account is generally set up with a business email address. A business account is governed by the associated organization. Any vault items or secrets contained within a business account should be considered proprietary to the related company or business entity.
API Key	The application programming interface (API) key is a specific identifying code for a user or program. The API key can be used to integrate other applications with Bitwarden for the uses of automation, monitoring, and more. The API key is a sensitive secret and should be handled carefully.
Clients / Bitwarden Client	The client, or client application, is the application that logs into Bitwarden. This includes the web, mobile, and desktop apps, the Bitwarden CLI, and browser extensions. Clients may be downloaded from the Downloads page.
Directory Connector	An application to sync users and groups from a directory service to a Bitwarden Organization. The Bitwarden Directory Connector automatically provisions and deprovisions users, groups, and group associations from the source directory. Learn more.

Terminology	Definition
Domain Verification	The process of an organization proving their ownership of a specific internet domain (eg. mycompany.com). Domain verification allows for additional features to be activated, such as users being able to skip inputting the SSO identifier during the login process. Learn more.
Groups	A set of Organization members. Groups relate users together, and provide a scalable way to assign permissions, such as access to Collections, projects, or secrets, as well as permissions within each separate Collection. When provisioning new users, add them to a Group to have them automatically inherit that Group's configured permissions.
Master Password	Also known as a Bitwarden password, main password, account password, or vault password. The primary method (or key) for accessing your Bitwarden account and data, the master password is used both for authenticating your identity to the Bitwarden service and for decrypting your sensitive data such as vault items or secrets. Bitwarden encourages users to establish one that is memorable, strong, and unique in that it is used only for Bitwarden. In 2021, Bitwarden introduced Account Recovery Administration (formerly Admin Password Reset), which enables Enterprise users and organizations to implement a policy that allows Administrators and Owners to reset master passwords for enrolled users. Learn more.
Organization	An entity (company, institution, group of people) that relates Bitwarden users to shared Organization data such as logins within an Organization vault or a Secrets Manager Project for secure sharing of items.
Plan	Plans define the services that Bitwarden provides through licensing, including available features and number of users able to use the product. There are multiple types of pre-defined plans available for individuals or organizations to subscribe to.
Policies	Policies are organization-wide controls that help an administrator keep a company secure by enabling additional settings for how their members (also called end users) use Bitwarden. These policies ensure a uniform standard of security. Learn more.
SCIM	System for cross-domain identity management (SCIM) can be used to automatically provision members and groups in your Bitwarden organization. Bitwarden servers provide a SCIM endpoint that, with a valid SCIM API Key, will accept requests from your identity provider (IdP) for user and group provisioning and de-provisioning. Learn more.

Terminology	Definition
Single Sign-On (SSO)	A session and user authentication service that grants employees or users access to applications with one set of login credentials that are based on their identity and permissions. Single Sign-On has multiple implementation options, and is widely compatible with Identity Providers (IdPs) allowing customers to leverage their existing solution. Learn more.
Login with SSO	An implementation of Single Sign-On. With this method, the user is authenticated by an Identity Provider, then the user enters their Bitwarden password to decrypt their data. Learn more.
SSO with Trusted Devices	A passwordless implementation of Single Sign-On. With this method, the user is authenticated by an Identity Provider and their data is decrypted through a process that utilizes a device encryption key stored on designated, trusted devices. Learn more.
SSO with Customer Managed Encryption	An advanced passwordless implementation of Single Sign-On available to self-hosted organizations. With this method, the user is authenticated by an Identity Provider, then the user's encryption key is automatically retrieved from a self-hosted key server utilizing Key Connector, allowing for user data to be decrypted. Learn more.
Subscription	The subscription is the transactional agreement between the customer and Bitwarden as part of the issuance of a license. Owners subscribe to plans at the agreed-upon fee on a recurring basis (monthly or annual) for the services provided by Bitwarden outlined in the plan.

Bitwarden Password Manager

Terminology	Definition
Autofill	A software feature that automatically enters previously stored information into a form field. Using Bitwarden, you can autofill logins via browser extensions and mobile devices, and autofill cards and identities via browser extensions. Learn more.
Collections	A unit to store one or more vault items together (logins, notes, cards, and identities for secure sharing) by a business within a Bitwarden Organization. Learn more.
Individual Vault	The Individual vault is the protected area for every user to store unlimited logins, notes, cards, and identities. Users can access their Bitwarden Individual vault on any device and platform.

Terminology	Definition
	Within a business context For users that are part of a Bitwarden Teams or Enterprise plan, an Individual vault is connected to their work email address. Individual vaults are often associated with, but separate from, an Organization vault. **Within a personal context** For users that are part of a Bitwarden personal or families plan, an Individual vault is connected to their personal email address. If part of a families plan or free two-person organization, the Individual vault remains separate from the Organization vault, but both are accessible by the user. Bitwarden recommends associating work email addresses with Teams and Enterprise Organizations, and personal email addresses with families organizations. Note: the Individual vault may be turned off for members of an Enterprise organization through an enterprise policy.
Items / Vault Items	Items are the individual entries that can be saved and shared in Bitwarden Password Manager such as logins, notes, cards, and identities.
Organization Member / Members	An end user such as an employee or family member that has access to shared Organization items within their vaults, alongside individual items within their individual vault.
Organization Vault	The protected area for shared items. Every user (also called a “member”) who is part of an Organization can find shared items in their vault view, alongside individually owned items. Organization vaults allow administrators and owners to manage the Organization’s items, users, and settings.
Vault / Vaults view	The secure storage area that provides a unified interface and tight access control to any item.

Bitwarden Secrets Manager

Terminology	Definition
Access token	Akey that facilitates service account access to, and the ability to decrypt, secrets stored in your vault. Learn more.
Name	A user-defined label for a specific secret.
Project	Collections of secrets logically grouped together for management access by your DevOps and cybersecurity teams. Learn more.
Secret	Sensitive key-value pairs, like API keys, that your organization needs to be securely stored and should never be exposed in plain code or transmitted over unencrypted channels.
Service account	Non-human machine users, like applications or deployment pipelines, that require programmatic access to a discrete set of secrets.
Value	A user-defined field of a stored secret that is used in software or machine processes. This is the sensitive information that is managed by Bitwarden Secrets Manager and can include API keys, application configurations, database connection strings, and environment variables.

Bitwarden Passwordless.dev

Terminology	Definition
FIDO	FIDO is the acronym for Fast Identity Online. It represents a consortium that develops secure, open passwordless authentication standards that are phishing proof. The FIDO protocols, which were developed by the FIDO Alliance, include: UAF: Universal Authentication Framework U2F: Universal Second Factor FIDO2: a new passwordless authentication protocol that contains core specifications WebAuthn (the client API) and CTAP (the authenticator API) Learn more.

Terminology	Definition
Passkeys	Passkeys – the credentials derived from the FIDO2 standard for each website that a user registers to – enable users to create and store cryptographic tokens instead of traditional passwords. Today, passkeys are used to log users into an app or website with pre-authenticated device specific tokens. In the future, the process could be used with shareable or transferable cryptographic tokens. Learn more.
Passwordless	Passwordless is the umbrella term used to describe a variety of authentication technologies that do not rely on passwords, including: something a user has (a security key, token, or device), something they are (biometrics), and passkeys.