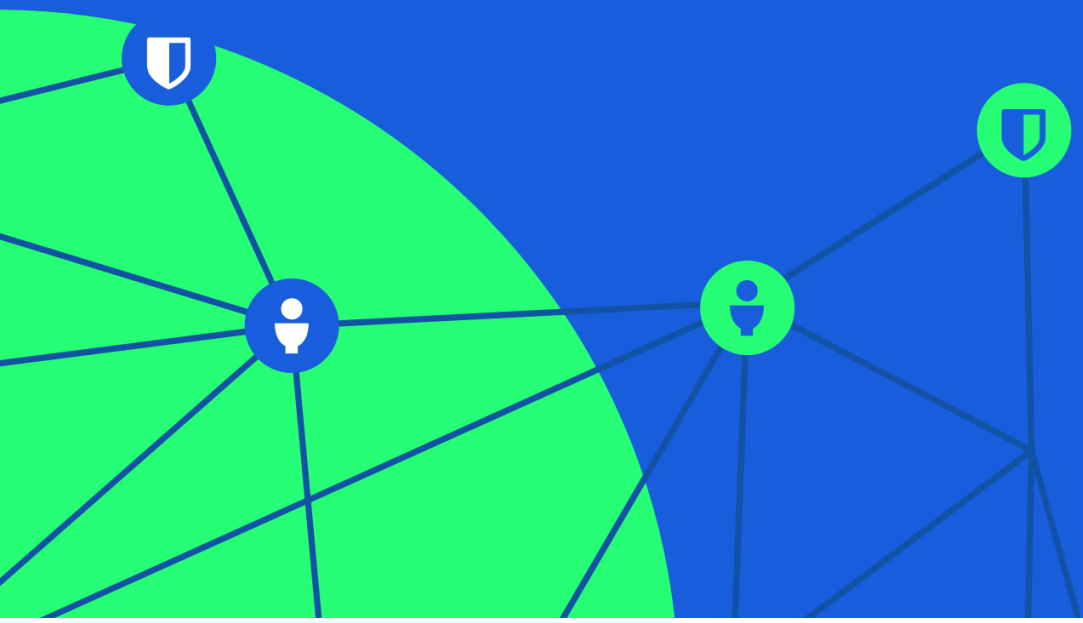
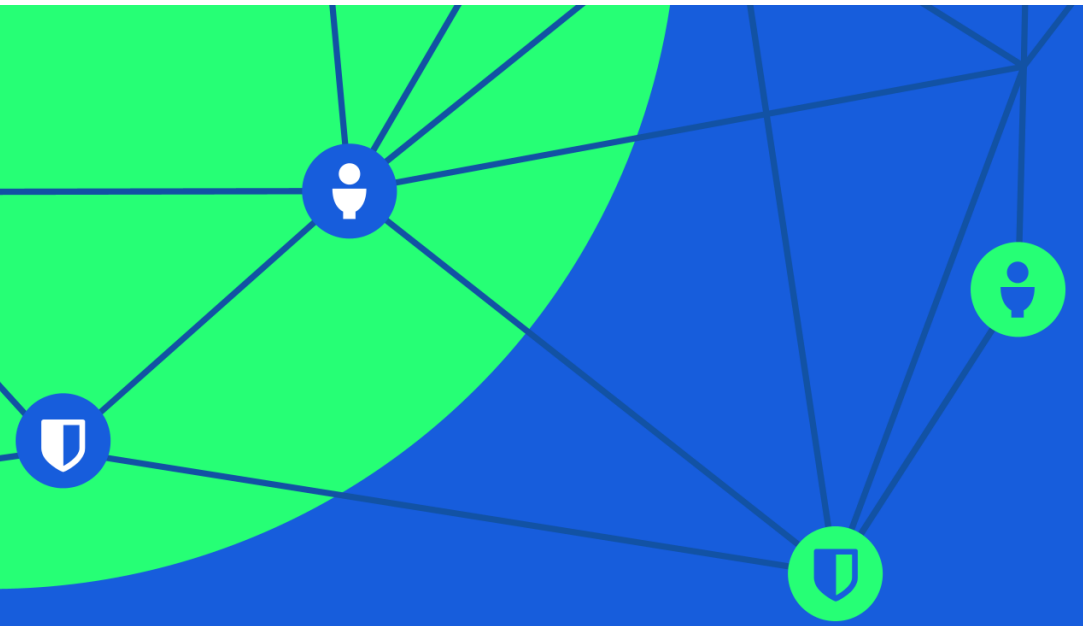


bitwarden

Onboarding and Succession



WHITE PAPER
Employee Onboarding and Succession with Bitwarden

April 2021

WHITE PAPER
Employee Onboarding and Succession with Bitwarden 2
Password management that fits your business 3
Tenets of the Bitwarden approach 3
Everything begins with a Bitwarden Account 3
Protect yourself and your company with a strong Bitwarden password 3
A wide range of cross-platform client applications 4
Access to Individual Personal Vault 5
Starting or joining an Organization 5
Why offer a Personal Vault by default 7
Basics of an Organization and Collections 7
Running a Team or Enterprise Organization in the Bitwarden Cloud 7
Adding users to an Organization 7
Adding users to one or more Collections 8
About Groups 8
A comprehensive role based access control approach 8
Offboarding Users 8
Disconnecting a user 9
Designing for your business with Bitwarden Customization 10
The Directory Connector for Synchronization and Invitations 10
Align the Directory Connector and Login with SSO along with your Web Vault Administration 11
Login with SSO for Authentication 11
The Bitwarden Web Vault for Organization Administration 12
Enterprise Policies 12
Event Logs 13
Option to self-host Bitwarden 13
Configuring for success 14
Frequently Asked Questions 15

Password management that fits your business

Getting new employees up and running quickly drives productivity. Saying farewell securely drives assurance.

Whether your company leans towards consolidation and centralization, or prefers an environment more flexible and dynamic, Bitwarden fits your needs.

This paper covers employee onboarding and succession starting with Bitwarden Cloud. We will further detail business plan options to customize all aspects of your Organization in the Bitwarden Cloud or self-hosted.

Tenets of the Bitwarden approach

The Bitwarden vision is to imagine a world where no one gets hacked. We carry this forward in our mission to help people and companies manage their sensitive information easily and securely.

Bitwarden believes that

- basic password management for individuals can and should be free
    - hence our **Basic Free Account**
- there is value in the Organizational capabilities of password management
    - hence our **Teams** and **Enterprise Organization** plans
- there is value in Premium features and family sharing
    - hence our **Premium Account** and **Family Organization**

For Bitwarden, all of these options are connected and complementary. Everything originates from our vision of a hack-free world. Empowering everyone at work **and** at home with password management gets us one step closer to that goal.

Everything begins with a Bitwarden Account

Protect yourself and your company with a strong Bitwarden password

Unlike general software applications, everything in your Bitwarden Vault is end-to-end encrypted. To maintain this security model, every person accessing Bitawrden must have an account with their unique master password. In a perfect world, this password is also long, random, and complex, the unique part being that it is only used for your Bitwarden account.

This identifier, a combination of the user email and master password, and the creation of any Bitwarden account, free or paid, means that the user is now in charge of the password for their Bitwarden account.

Specifically, this means that if a user forgets their main Bitwarden password, there is no way for them to recover it or for it to be reset.

note:
Bitwarden is planning a feature in mid-2021 to enable Enterprises to reset their Organization user passwords. This will not impact individual personal accounts that are not connected to an Enterprise organization with this upcoming feature enabled.

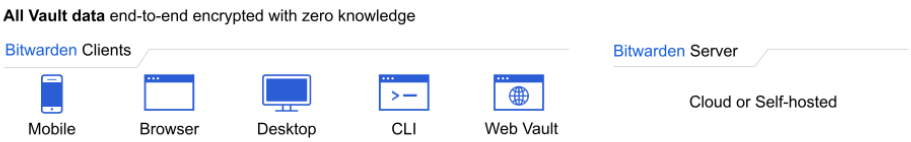
note:
Bitwarden has an Emergency Access feature which can allow a designated user to view or take over your Personal Vault. While not intended as a password-reset feature, some Bitwarden users have found this to be a helpful option. Setting an Emergency Access designee is part of our Premium Account which is also included with any of our Family, Teams, or Enterprise plans. See our help note on Emergency Access.

A wide range of cross-platform client applications

The most useful password managers provide access from all of your devices. Bitwarden supports a wide range of client applications across

- **Mobile devices** including Android and iOS
- **Browser extensions** for Chrome, Firefox, Safari, Microsoft Edge, Brave, Opera, Vivaldi, and Tor
- **Desktop applications** for Windows, Mac and Linux
- A **command line interface**
- A **web vault** accessible from any browser

Bitwarden Clients and Bitwarden Cloud / Server



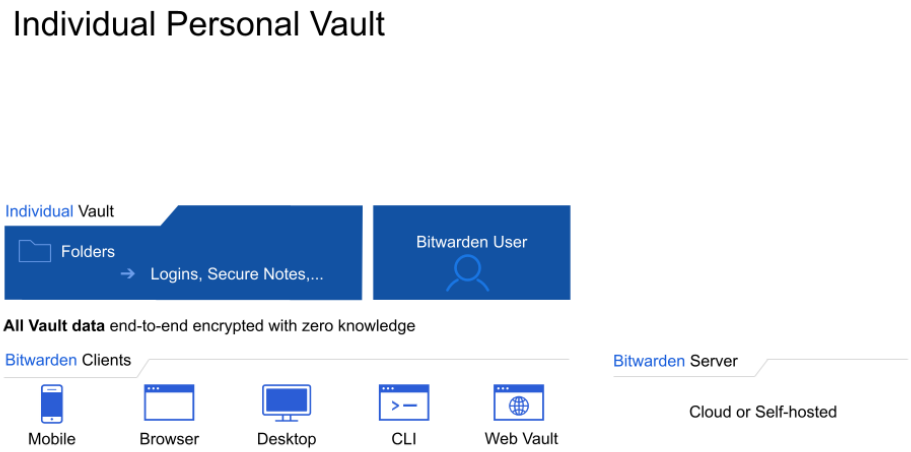
Bitwarden supports a wide range of client applications that synchronize to the Bitwarden Cloud or a self-hosted server

Access to Individual Personal Vault

Once a user has a Bitwarden account, they have their own Personal Vault. This is unique to them and only they hold the key which is a combination of login email address and master password.

A Personal Vault is the account owners own responsibility. They can set up Emergency Access with Premium Features (either $10/year individually or included with Family, Teams, and Enterprise plans).

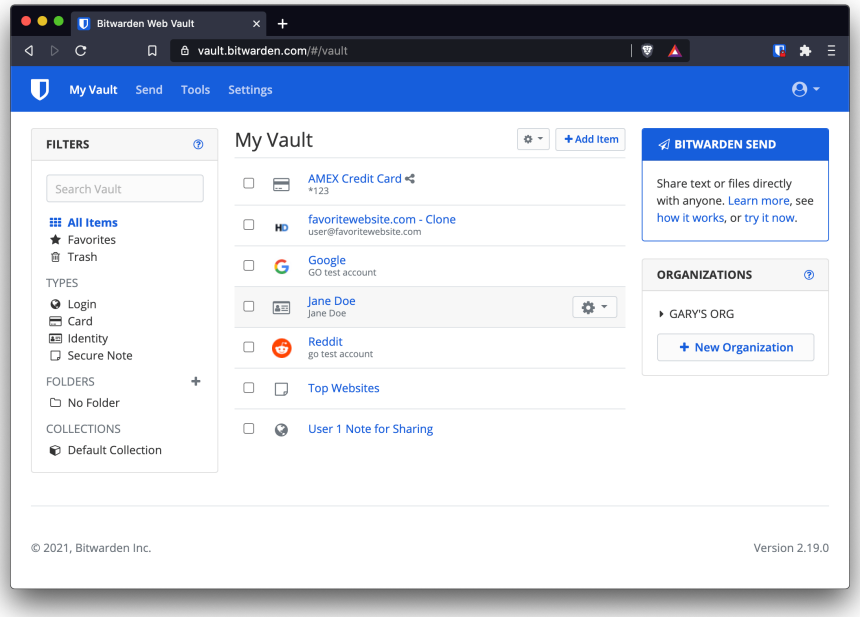
A Personal Vault is just that, personal. It is not intended for permanent sharing. That is the domain of Bitwarden Organizations in our next section.



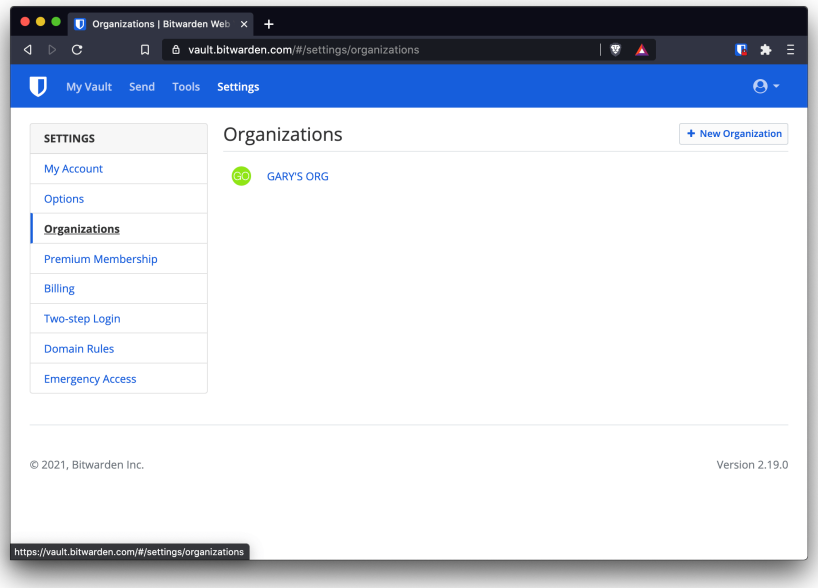
The Bitwarden Individual Personal Vault can be accessed by its owner from any Bitwarden Client.

Starting or joining an Organization

Any Bitwarden user can start an Organization using the web vault.



Launching a new Organization from the web vault



Launching a new Organization from the web vault

The person that launches the Organization will be the Owner with full control of the Organization and its members. At the same time every Bitwarden user receives a Personal Vault. The Organization owner does not have the ability to see any other individual Personal Vault by design.

In this case, employees can be guaranteed that the Personal Vault remains their own. An Organization owner cannot access it due to the encryption model in place within Bitwarden, where individual users maintain the key to decrypt their Personal Vault.

note:
There is an enterprise policy for the Organization owner to disable the Personal Vault, highlighting the balance between a more centralized compared to a dynamic approach.

Why offer a Personal Vault by default

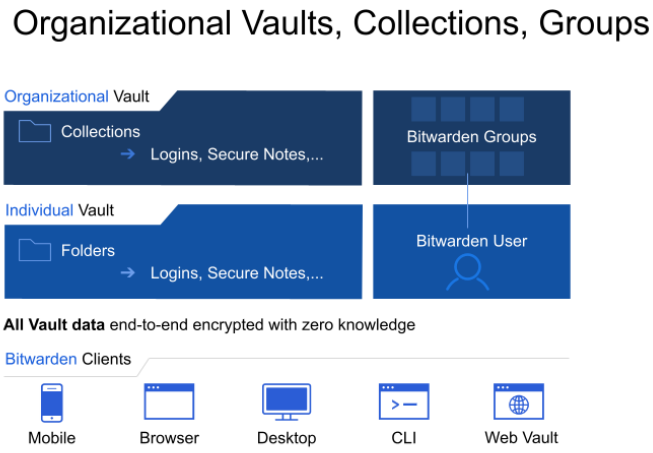
Even though it can be disabled, offering the Personal Vault by design is instrumental to the Bitwarden approach.

Employees use a range of credentials every day, both personally and professionally. Specifically in professional situations there are credentials for the company, credentials for the team, and credentials for individuals. Bitwarden covers all three areas and more.

Our view is that good security habits need to become just that, habits. If employees can use the same tools across more environments, adoption increases.

Basics of an Organization and Collections

Once launched, Organization Owners or Administrators can add people to the Organization and create Collections, which are similar to folders in the Personal Vault, except Collections only exist within an Organizational Vault. Shared items such as a WiFi password might be kept in an **Office Technology Collection** shared across the Organization.



Organizational Vaults use Collections for arranging items and assigning shared access

Running a Team or Enterprise Organization in the Bitwarden Cloud

Adding users to an Organization

With an Organization set up, Owners or Administrators can invite others to join. Larger organizations have options to integrate with Single Sign On and Directory services, covered more later. Organization Owners should plan for redundancy in both the Owner and Administrator roles.

For details on managing users, please see this help note. For details on all of the aspects discussed for Organizations please visit the Organizations section on our help site.

Adding users to one or more Collections

After creating Collections, Owners, Administrators can add users to those Collections. Assignment can be made by individual, or you can create Groups to manage users more efficiently.

About Groups

Groups help administer user permissions one level up from individual users. You can envision creating Groups within a company by department or project team.

A comprehensive role based access control approach

Bitwarden takes an enterprise friendly approach to sharing at scale. Users can be added to the Organization in different roles, belong to different Groups, and have those Groups assigned to various Collections. Bitwarden also enables a custom role for more granular permissions regarding administrative tasks. Please see this article for more detail on User Types and Access Control

Offboarding Users

Let's explore the standard sequence to offboard an employee.

note:
At Bitwarden, we see sharing of credentials as a vital aspect to get work done efficiently and securely. We also recognize that once a credential is shared, it is technically possible for the recipient to keep that credential.

For this example, we will assume that the employee

- Set up their account with the Bitwarden Cloud using an email address similar to first.last-name@company.com
- Was a Manager, and could create Collections
- Used the Personal Vault
- Was a member of the main company Organization
- Was a member of Collection 1
- Was the creator and owner of Collection 2
- Was the creator and owner of a WiFi Login within Collection 2
- Had Bitwarden clients on mobile, desktop, and the browser extension

Disconnecting a user

When an employee such as the person above is removed from the Organization the following takes place across their account and client applications.

Personal Vault

- The employee will have access to log in to their Personal Vault with their non-functioning email address and master password at vault.bitwarden.com
- There they can choose to change their email address
- If they had enjoyed extra Premium features (included by their employer's Organization) they can renew those Premium features individually for $10/year
- They can download their Personal Vault

Organizations

- Once removed from the Organization, any online client such as the mobile app, desktop app, or web extension will no longer show that Organization or any Organizational Collections

Collection 1

- Will no longer be visible

Collection 2

- Will no longer be visible. Ownership of the Collection remains with the Organization Admins and Owners. This employee will no longer have access to Collection 2

WiFi login within Collection 2

- Will no longer be visible, Ownership of the WiFi login remains with the Organization Admins and Owners. This employee will no longer have access to this login or collection

Bitwarden Client Applications

- For online devices, the Organizational Vault will disappear from view for the employee
- For offline devices, until they are back online, a cached, read-only copy of the Organizational resource may remain. If a malicious scenario is anticipated, credentials to which the employee had access should be updated upon separation

Designing for your business with Bitwarden Customization

Beyond the scenarios described above Bitwarden offers the industry's widest range of customization options with our integrations, enterprise policies and option to self-host.

The Directory Connector for Synchronization and Invitations

For companies that operate with LDAP-based directory services, those directories can be synchronized to Bitwarden using the Bitwarden Directory Connector, a stand alone application that can be run anywhere it has access to the companies directory and Bitwarden.

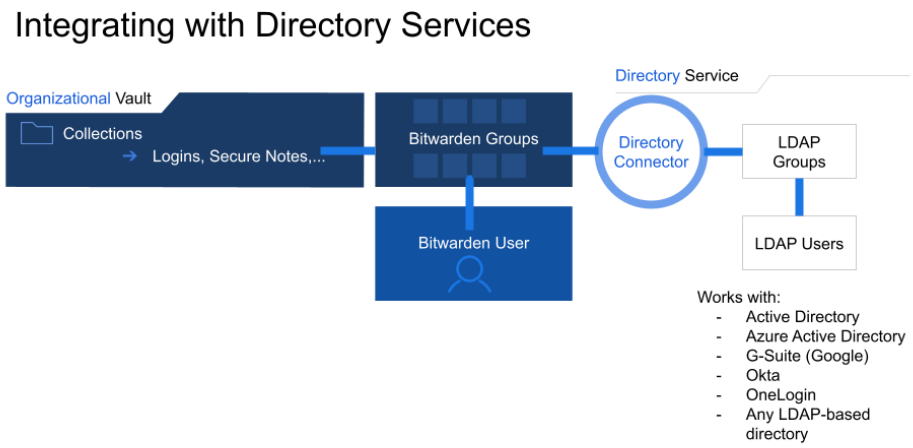
The Bitwarden Directory Connector will

- synchronize LDAP-based directory groups with Bitwarden Groups
- synchronize users within those Groups
- send invitations for new users to join the Organization and create a Bitwarden account
- invited users will still need to be confirmed by an Owner of Administrator before they have access to the Organization

A Directory Connector sync operation can be run on-demand or automatically on a configured interval.

When a user is removed from the source directory, they will be deprovisioned from the Bitwarden Organization, losing access to the Organization and Collections to which they previously had access.

For more information visit About Directory Connector on our help site.



The Bitwarden Directory Connector synchronizes LDAP-based groups and users

Many Bitwarden Teams and Enterprise users focus their onboarding efforts on the Directory Connector and then the Bitwarden Web Vault and administration areas to assign Bitwarden Groups to Bitwarden Collections.

Align the Directory Connector and Login with SSO along with your Web Vault Administration

The Directory Connector, Login with SSO, and Web Vault Administration all work individually or together.

Directory Connector - **Synchronization** - Teams and Enterprise plans
- LDAP Groups synced to Bitwarden Groups
- Users within groups get invitations

Directory Connector - **Invitations** - Teams and Enterprise plans
- Users receive an invitation to join the Organization
- Users create an account and define a unique master password

Login with SSO - **Authentication** - Enterprise plans only
- Users can log into their Bitwarden Vault using existing SSO credentials
- Users will be asked to create a master password for decryption

Bitwarden Web Vault - **Organization Administration** - Teams and Enterprise plans
- Groups (created in Bitwarden or directory-synced) can be granted access to Collections
- Granular roles and assignments also available

Login with SSO for Authentication

The Bitwarden Enterprise plan incorporates Login with SSO by integrating with your existing Identity Provider using SAML or OpenID interfaces. The Bitwarden Teams plan does not include Login with SSO

This approach involves separating the authentication mechanism from decryption of each user's endpoint identity.

When using Bitwarden without SSO integration and logging in:
- Authentication happens with the email and master password of the account holder connecting to the Bitwarden server
- Decryption of the Vault contents happens with the combination of the users individual key, created from their email and master password

When using Bitwarden and Login with SSO and logging in:
- Authentication is transferred to the company’s chosen Identity Provider
    - Any two-factor authentication processes connected to the company’s identity provider will remain in place
- Decryption of the Vault Contents still requires the users individual key and a password specifically for encryption and decryption

    - This security model ensures that customers can choose their own Identity Provider and have
        - the ability to provision users automatically
        - full access to the entirety of the Bitwarden client suite
        - the ability to decrypt vault contents while offline
        - the option to configure access with or without SSO
        - the option to retain a personal vault
        - a protected end-to-end encryption model

Using Login with SSO, new Bitwarden users can log in to their Bitwarden Vault using their regular SSO credentials. They can then perform decryption of this Vault with their newly created master password.

Since users go through a validated authentication process, they will be in the **Accepted** status within the Organization management settings.

If a user is removed from the company's Identity Provider, the user will no longer be able to authenticate with that path.

The Bitwarden Web Vault for Organization Administration

Every Bitwarden Teams and Enterprise Organization comes with the ability to manage
- People
- Collections
- Groups
- Policies
- Event logs

We have discussed People and Groups above through integrations. Collections can be managed within the Bitwarden Organization, as well as Enterprise Policies and Event logs

Enterprise Policies

The Bitwarden Enterprise plan includes Policies to set a secure foundation for any business. The Bitwarden Teams plan does not include Policies.

Sample Enterprise Policies include
- Two-step Login: Require users to set up two-step login on their personal accounts.
- Master Password: Set minimum requirements for master password strength.
- Password Generator: Set minimum requirements for password generator configuration.
- Single Organization: Restrict users from being able to join any other organizations.
- Personal Ownership: Require users to save vault items to an organization by removing the personal ownership option.

The Personal Ownership policy fits into the earlier discussion on company approaches. For many companies, the option to provide employees with a Personal Vault completes the employee use cases and makes good password security more of a habit.

We also understand that for other companies, the assurance of all credentials being retained in the Organization Vault. This includes setups where each user has their own individual Collection. Understandably, Organization Owners and Administrators also have access to that Collection.

Event Logs

Bitwarden includes a set of Event Logs that can be viewed directly from the management console, or exported to be analyzed within a security information and event management (SIEM) system such as Splunk.

Bitwarden includes events associated with

- Users
- Items
- Collections
- Groups
- Organizations

For more information, please see Event Logs on the Bitwarden help site.

Option to self-host Bitwarden

In keeping with the Bitwarden approach to offer password management across all clients, providing an option
to self-host addresses an even wider range of use cases for Enterprises.

There are many reasons for companies to choose to self-host. Specifically when it comes to onboarding, offboarding, and enhanced features, here are some of the reasons companies choose to do so:

- Immediate deletion of user accounts
    - in a self-hosted environment, users can be deleted entirely including their Personal Vaults
- Network access control
    - in a self-hosted environment, Bitwarden Organization Owners can determine which network access employees must use to access their Bitwarden server

- Advanced proxy settings
    - some Administrators choose to enable or disable certain types of devices from accessing the Bitwarden Server
- Choice to use and existing database cluster
    - Self-hosted users may choose to connect to an existing Microsoft SQL Server database. Additional databases will be supported in the future
- Choice to dramatically increase storage for file attachments and Bitwarden Send
    - File attachments for Bitwarden items or Bitwarden Send are retained on user-provided storage

In addition to these benefits, customers appreciate the ability to tightly integrate Bitwarden into their existing systems. Bitwarden features

- A robust public API
- A fully featured command line interface CLI

Together, these options deliver even more customization to fit with existing workflows.

Configuring for success

We often note that password management is people management, and Bitwarden wants to fit the workflows suited to your organization. By offering a wide range of options, shared via our open source approach, customers can rest assured that they can meet their own individual needs.

To get started today with a free Enterprise or Teams trail, visit bitwarden.com/pricing/business/ https://bitwarden.com/pricing/business/.