bitwarden | Help Center Article

ADMIN CONSOLE > USER MANAGEMENT

Onboarding and Succession Overview

View in the help center:
https://bitwarden.com/help/onboarding-and-succession/

Onboarding and Succession Overview

> **Tip**
> Read the full paper below or download the PDF.

Password management to fit your business

Getting new employees up and running quickly drives productivity. Likewise, saying farewell properly drives assurance in the security of your business's systems and accounts. Whether your business leans towards consolidation and centralization, or prefers a flexible and dynamic environment, Bitwarden fits your needs.

This guide covers the Bitwarden approach to onboarding and succession planning for members of your organization, starting with our approach to the relationship between members and organizations, then covering the simplest use-cases for onboarding and succession, and finally and moving on to the levers and options at your disposal to fit Bitwarden to your needs.

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 individuals and companies manage their sensitive information easily and securely. Bitwarden believes that:

- Basic password management for individuals can and should be **free**. We provide just that, a basic free account for individuals.
- Individuals and families should take an active role in their security using TOTPs, emergency access, and other supporting security features.
- Organizations can greatly improve their security profile through organizational password management and secure sharing.

> **Tip**
> For Bitwarden, different plans and options are connected and complementary, all originating in 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.

A key aspect of Bitwarden is that, unlike many software applications, everything in every vault is end-to-end encrypted. To maintain this security model, every person using Bitwarden must have a unique account with a unique master password. Master passwords should be **strong** and **memorable**.

Each user is in charge of their master password. Bitwarden is a zero-knowledge encryption solution, meaning that the team at Bitwarden, as well as Bitwarden systems themselves, have no knowledge of, way to retrieve, or way to reset any master password.

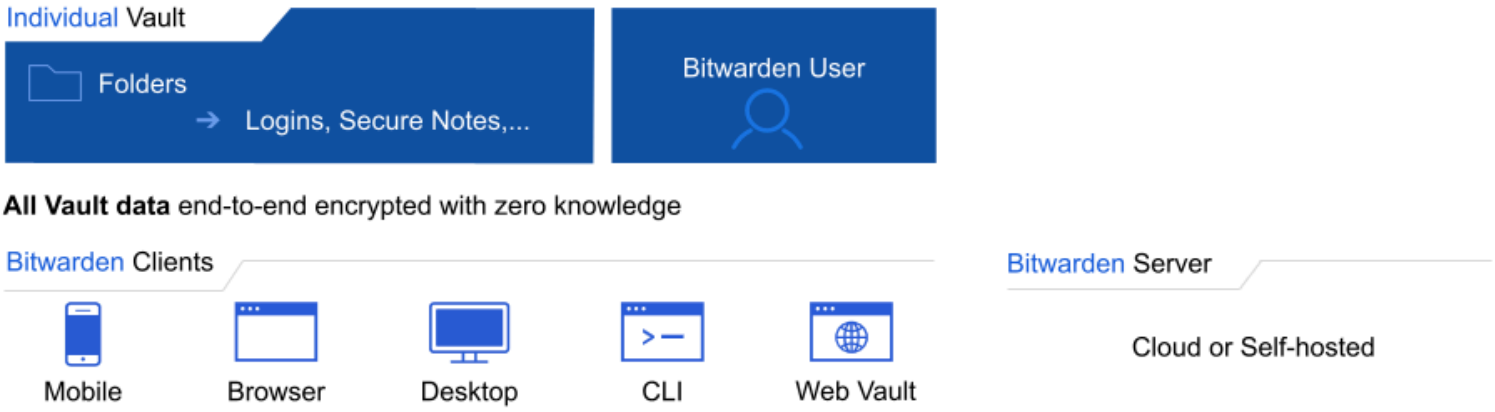
Use Bitwarden anywhere

Security everywhere means security anywhere, so the best password managers provide access across all your devices. Bitwarden supports a range of client applications, any of which can be connected to our cloud-hosted servers or a self-hosted server of your own:

Bitwarden Clients/Servers

Users' individual vaults

Anyone who creates a Bitwarden account will have their own individual vault. Accessible from any client application, individual vaults are unique to each user and only that user holds the key to access it, using a combination of their email address and master password. Personal accounts, and the individually-owned vault items stored therein, are the account owners responsibility. Organization owners, admins, and managers cannot see any other user's individual vault by design, guaranteeing someone's individual vault data remains their own.



Personal Vaults

Families, Teams, and Enterprise organizations automatically provide members individually with premium features, like emergency access and encrypted attachment storage, which they can choose to use. Data in an individual vault belongs to the user. Individual vaults do not enable sharing, organizations do.

Tip

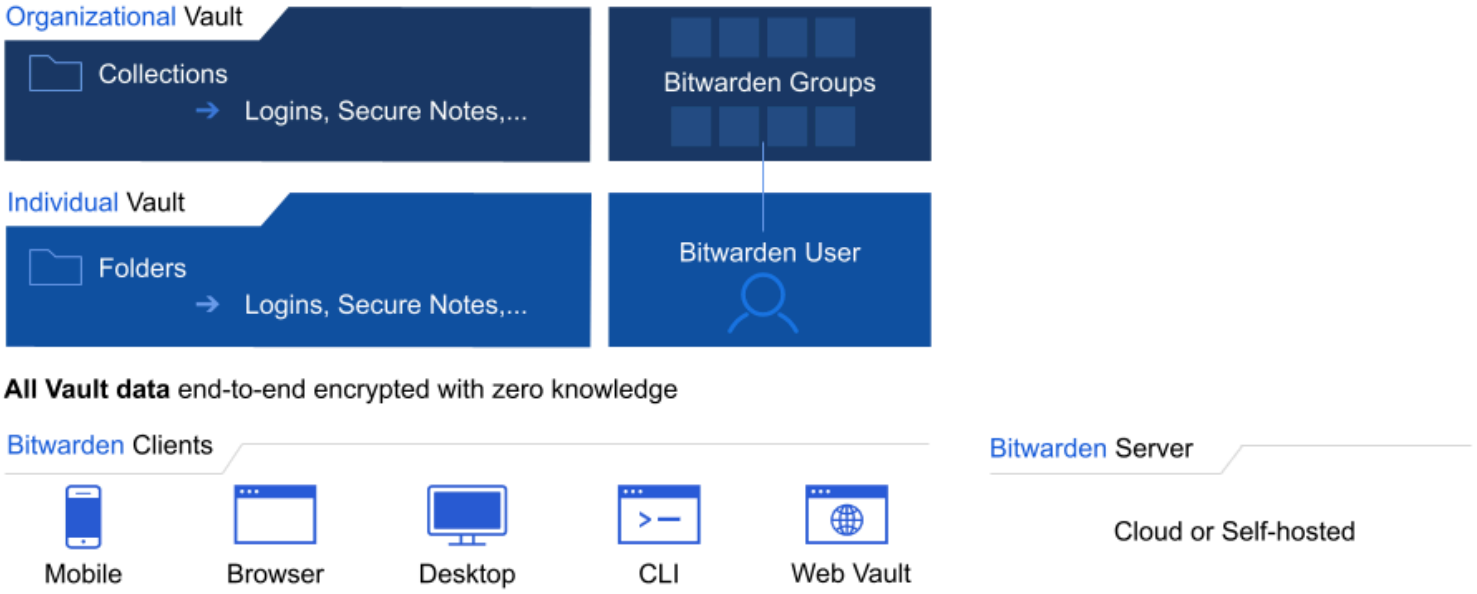
Why provide individual vaults by default?

Individual vaults are an instrumental component of the Bitwarden approach. Employees use a range of credentials every day, personally and professionally, and **habits formed in one area typically become habits in the other**. In our view, employees that use proper security practices in their personal lives will carry over that good behavior to their professional lives, **protecting your business** in the process.

Using the same tool in both areas helps that habit form faster and easier. Enterprise organizations have the option to configure policies, including to disable individual vaults.

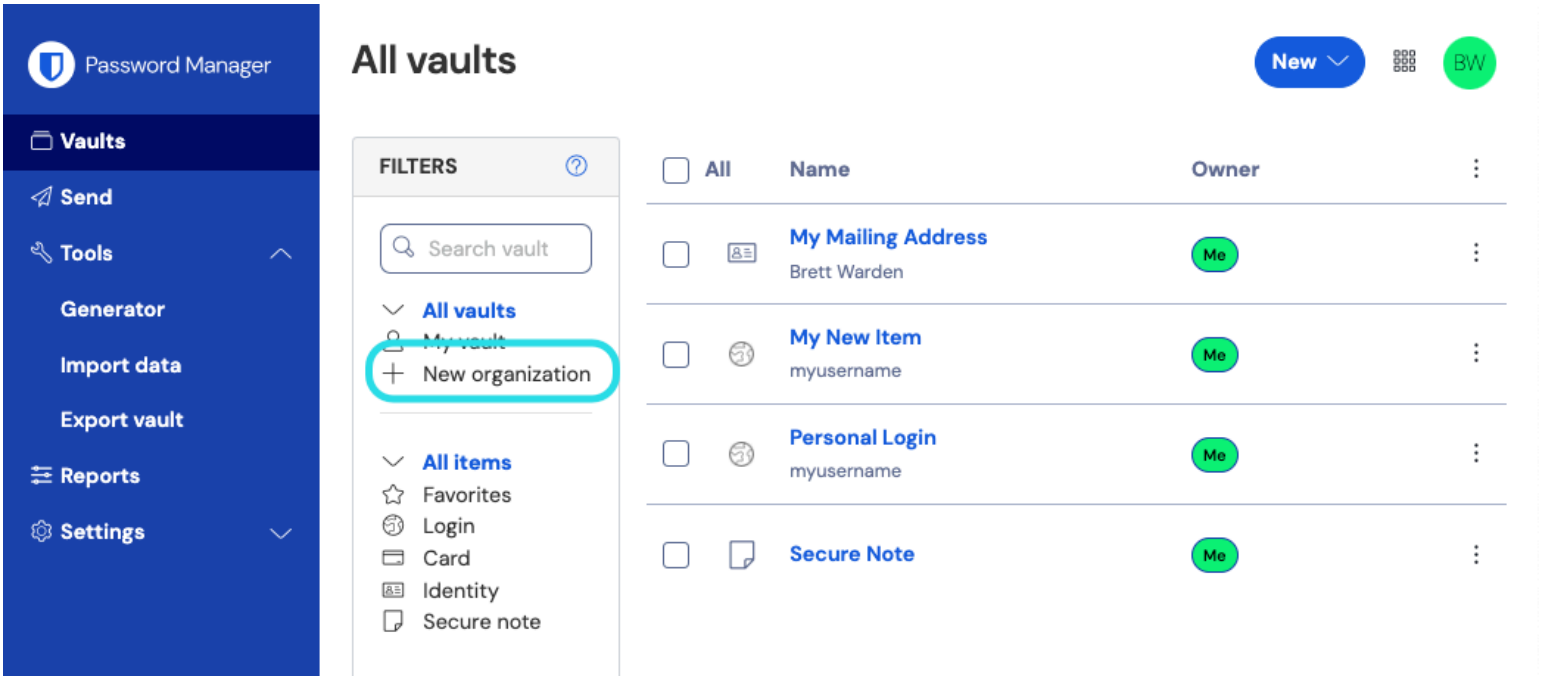
Bitwarden organizations

Bitwarden organizations add a layer of collaboration and sharing to password management for your team or enterprise, allowing you to securely share common information like office wifi passwords, online credentials, or shared company credit cards. Secure sharing through organizations is safe and easy.



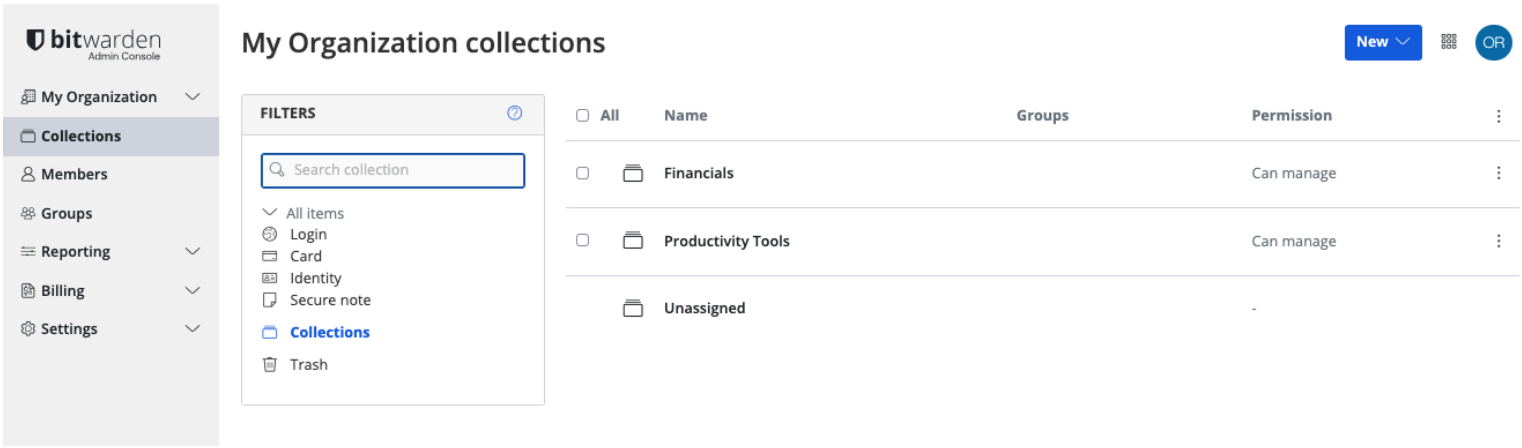
Organization Vault

Anyone can start an organization directly from the web app:



New organization

Once created, you'll land in the Admin Console, which is the central hub for all things sharing and organization administration. Whoever launches the organization will be the owner, giving them full control to oversee the vault, to manage items, members, collections, and groups, to run reporting, and configure settings like policies:



Admin Console

Collections

Bitwarden organizations manage members and data in a scalable and secure fashion. Managing members and data on an individual basis is inefficient for large businesses and can leave room for error. To solve this, organizations provide collections and groups.

Collections gather together logins, notes, cards, and identities for secure sharing within an organization:

Using Collections

Onboarding members

Once your organization is established and collections are setup to store your data, owners and administrators should invite new members. To ensure the security of your organization, Bitwarden applies a 3-step process for onboarding new members, Invite → Accept → Confirm.

Members can be onboarded directly from the web vault, using the Directory Connector application to sync individual users and groups, or through Just in Time (JIT) provisioning using login with SSO.

Adding members

In the simplest cases, users can be added to your organization directly from the web app. When adding users, you can designate which collections to grant them access to, which role to give them, and more.

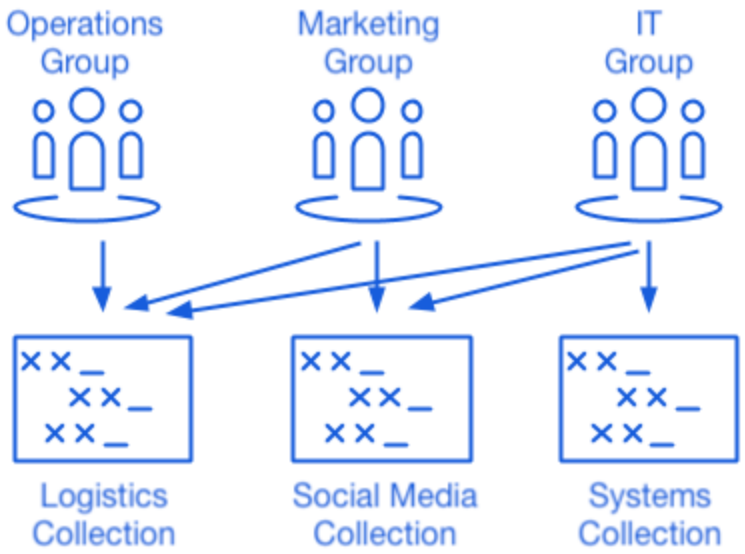
Learn step-by-step how to add users to your organization.

Once users are fully onboarded to your organization, you can assign access to your organization's vault data by assigning them to collections. Teams and Enterprise organizations can assign users to groups for scalable permissions assignment, and construct group-collection associations instead of assigning access on the individual level.

> **Tip**
>
> For large organizations, SCIM and Directory Connector are the best ways to onboard and offboard users at scale.

Groups

Groups relate together individual users, and provide a scaleable way to assign permissions including access to collections and other access controls. When onboarding new users, add them to a group to have them automatically inherit that groups's configured permissions:



Using Collections with Groups

Comprehensive role-based access controls

Bitwarden takes an enterprise-friendly approach to sharing at scale. Members can be added to the organization with a number of different roles, belong to different groups, and have those groups assigned to various collections to regulate access. Among the available roles is a custom role for granular configuration of administrative permissions.

Deprovisioning users

At Bitwarden, we see sharing of credentials as a vital aspect to getting work done efficiently and securely. We also recognize that once a credential is shared, it is *technically* possible for the recipient to keep it. For that reason, secure onboarding using appropriate role-based access controls and implementing policies plays an important role in facilitating secure succession.

There are a variety of tools provided by Bitwarden for tailoring your workflow and exercising more control over succession. The following sections will describe a basic succession workflow, which uses none of these tools, and some advanced succession tactics frequently used by organizations:

Basic deprovisioning

Deprovisioning users from Bitwarden involves removing users from your organization, and like onboarding can be done directly from the web vault or in automated fashion using SCIM or Directory Connector.

Alice is a **User** in your organization, which is hosted on the Bitwarden cloud and uses company email addresses (e.g. `first-last@company.com`). Currently, this is how Alice uses Bitwarden:

Product area	Description
Client applications	Uses Bitwarden on mobile and a browser Extension personally and professionally, and the web vault for occasional organization-related work.
Email & master password	Logs in to Bitwarden using `alice@company.com` and `p@ssw0rD`.
Personal items	Stores assorted personal items, including logins and credit cards, in her personal vault.
Two-step login	Uses organization-wide Duo 2FA.
Collections	Alice has Can Manage permission for the "Marketing Credentials" collection, granted her the ability to manage many aspects of that collection.
Shared items	Created and shared several vault items that are owned by by the organization and reside in her team's Collection.

Once Alice is removed from your organization:

Product area	Description
Client applications	Can continue to use any Bitwarden application to access her individual vault, however will lose access to organization-owned items, all collections, and all shared items. See the tip at the end of this section for information on local caching.
Email & master password	Can continue to log in using `alice@company.com` and `p@ssw0rD`, however since she won't have access to her `@company.com` inbox, she should be advised to change the email associated with her Bitwarden account.
Individual items	Will still be able to use her individual vault and access the items stored therein.

Product area	Description
Permissions in the organization	Will **lose all permissions over and access to** anything related to the organization.
Two-step login	Won't be able to use organization Duo 2FA to access her vault, but can setup one of our free two-step login options or upgrade to premium for more.
Created collections	Alice's "Marketing Team" collection will be retained by organization owners and admins, who can assign a new user Can manage permission
Shared items	Ownership of collections and shared items **belongs to the organization**, so Alice will lose access to all these items despite having created them.

Tip

Offline devices cache a read-only copy of vault data, including organizational vault data. Some clients may retain access to this read-only data for a short period of time after a member is deprovisioned. If you anticipate malicious exploitation of this, credentials the member had access to should be updated when you remove them from the organization.

Advanced deprovisioning

Warning

For those accounts that do not have master passwords as a result of SSO with trusted devices, removing them from your organization will cut off all access to their Bitwarden account unless:

1. You assign them a master password using account recovery beforehand.
2. The user logs in at least once post-account recovery in order to fully complete the account recovery workflow.

Additionally, users will not be able to re-join your organization unless the above steps are taken before they are removed from the organization. In this scenario, the user will be required to delete their account and be issued a new invitation to create an account and join your organization.

Revoking access to the organization, but not removing them from the organization, will still allow them to log in to Bitwarden and access **only** their individual vault.

Administrative take-over

Using the Master password reset policy, owners and admins in your organization can reset a user's master password during succession.

Resetting a user's master password logs the user out of all active Bitwarden sessions and resets their login credentials to the ones specified by the administrator, meaning that administrator (and only that administrator) will have the keys to the user's vault data,

including items in the individual vault. This vault takeover tactic is commonly used by organizations to ensure that employees don't retain access to individual vault items that may be work-related and can be used to facilitate audits of every credential an employee may have been using.

> **Note**
>
> **Admin password reset does not bypass two-step login**. In many cases, we recommend using SSO as some IdPs will allow you to configure 2FA and 2FA bypass policies for your users.

Removing the individual vault

If your organization requires real-time control of all vault items, you can use the Remove individual vault policy to require users to save all vault items to the organization. This will circumvent the need to takeover and audit a user's account during succession, as it'll be completely empty of data once removed from the organization.

Login-less account deletion

As mentioned previously, removing a user from your organization does not automatically delete their Bitwarden account. In the basic succession workflow, when a user is removed they can no longer access the organization or any shared items and collections, however they will still be able to log in to Bitwarden using their existing master password and access any individual vault items.

Organizations wanting to completely delete the account, including all individual vault items, may be able to use one of the following methods to do so during succession:

1. If you're self-hosting Bitwarden, an authorized admin can delete the account from the System Administrator Portal.
2. If the account has an @yourcompany.com email address that your company controls, you can use the delete without logging in workflow and confirm deletion within the @yourcompany.com inbox.

Designing your organization for your business

At Bitwarden, we often say that password management is people management, and we can 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.

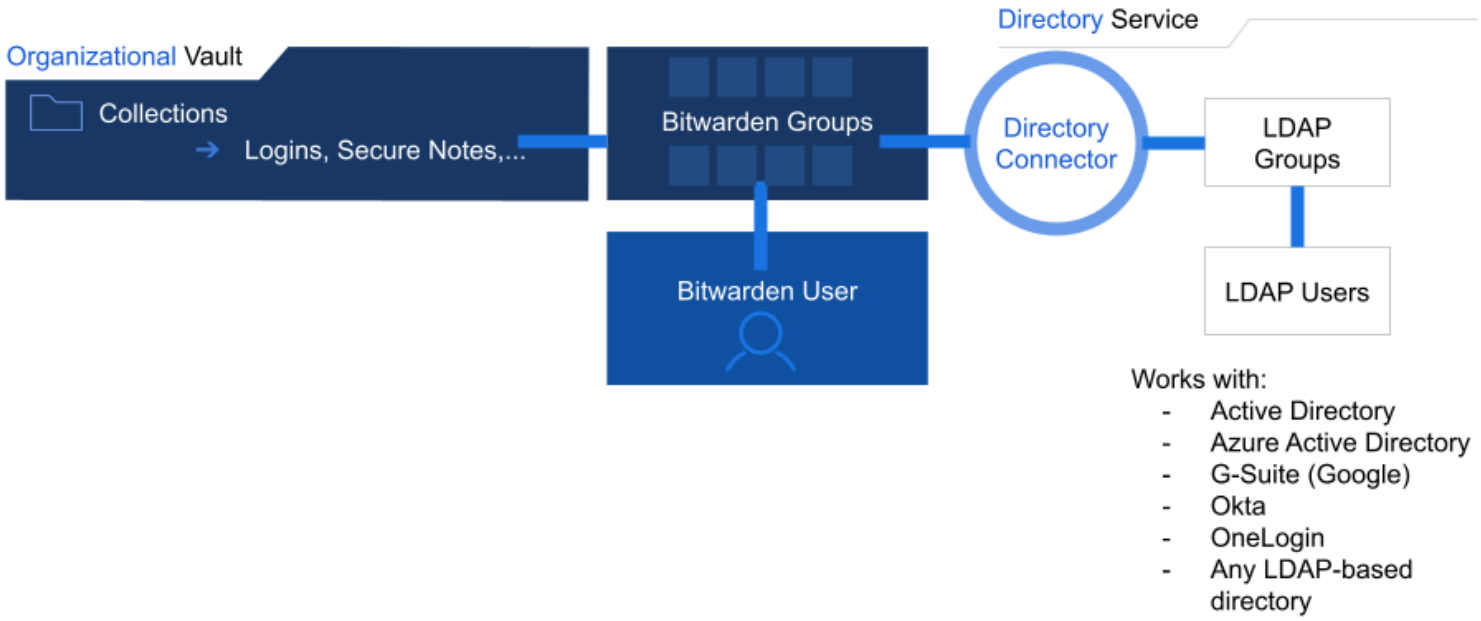
Get started today with a free Enterprise or Teams trial.

SCIM

For Enterprise organizations with large user-bases that operate using a supported identity (currently, Azure AD, Okta, OneLogin, and JumpCloud), SCIM integrations can be used to automatically provision members and groups in your Bitwarden organization. Learn more.

Directory Connector

For companies with large user-bases that operate using directory services (LDAP, AD, Okta, and others), Directory Connector can synchronize users and groups from the directory to the Bitwarden organization. Directory Connector is a stand-alone application that can be run anywhere with access to your directories and to Bitwarden.



Directory Connector

Many Bitwarden Teams and Enterprise organizations focus their onboarding efforts on the Directory Connector and use the organization vault administration areas to manage group-collection relationships.

Directory Connector will:

- Sync LDAP-based directory groups with Bitwarden groups
- Sync users within each group
- Invite new users to join the organization
- Remove deleted users from the organization

Login with SSO

Bitwarden Enterprise organizations can integrate with your existing identity provider (IdP) using SAML 2.0 or OIDC to allow members of your organization to login to Bitwarden using SSO. Login with SSO separates user authentication from vault decryption:

Authentication is completed through your chosen IdP and retains any two-factor authentication processes connected to that IdP. **Decryption** of vault data requires the user's individual key, which is derived in part from the master password. There are two decryption options, both of which will have users authenticate using their regular SSO credentials.

- **Master password**: Once authenticated, organization members will decrypt vault data using their master passwords.
- **Customer-managed encryption**: Connect login with SSO to your self-hosted decryption key server. Using this option, organization members won't need to use their master passwords to decrypt vault data. Instead, Key Connector will retrieve a decryption key securely stored in a database owned and managed by you.
  - Leverage your existing identity provider.

- Protect the end-to-end encryption of your data.
- Provision users automatically.
- Configure access with or without SSO.
- Decrypt vault data according to your company's security needs.

Enterprise policies

Enterprise organizations can implement a variety of policies designed to lay a secure foundation for any business. Policies include:

- **Require two-step login:** Require users to set up two-step login on their personal accounts.
- **Master password requirements:** 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.
- **Remove individual vault:** Require users to save vault items to an organization by removing the personal ownership option.

> **Tip**
>
> The **Remove individual vault** policy, for example, fits into earlier discussion regarding the interplay between individual vaults and organization vaults. Some companies may desire the assurance of have all credentials retained in the organization vault. A possible implementation could involve allowing each individual user to have their own collection, which unlike individual vaults could be overseen by organization owners and admins.

Event logs

Bitwarden organizations include access to event logs, which can be viewed directly from the web vault or exported to be analyzed within security information and event management (SIEM) systems like Splunk. Event logs include information about:

- User-item interactions
- Changes made to vault items
- Onboarding events
- Organization configuration changes
- Much, much more

> **Tip**
>
> In addition to these benefits, customers appreciate the ability to tightly integrate Bitwarden into their existing systems. Bitwarden offers a robust public API and a fully-featured command line interface (CLI) for further integration into existing organization workflows.

Self-hosting

In keeping with the Bitwarden approach to offer password management anywhere and everywhere, Bitwarden provides an option to self-host to address an even wider range of use cases for Enterprises. There are many reasons for a company to choose to self-host. Specifically when it comes to onboarding, succession, and enhanced features, here are some of the reasons companies choose to do so:

- **Immediate deletion of user accounts:** Because you control the server, users can be deleted entirely (including their individual vault).
- **Network access control**: Organization owners can determine which network access employees must use to access their Bitwarden server.
- **Advanced proxy settings:** Administrators can choose to enable or disable certain types of devices from accessing the Bitwarden Server.
- **Use an existing database cluster:** Connect to an existing Microsoft SQL Server database. Additional databases will be supported in the future.
- **Increase storage for file attachments and Bitwarden Send:** File attachments for Bitwarden items or Bitwarden Send are retained on user-provided storage.

Put the pieces together

Directory Connector, login with SSO, Enterprise policies, and your vault work well individually or in harmony to optimize your onboarding, succession, and organization management experience. The following table details how that it might look to string together these pieces into one smooth process:

Step	Description
Synchronize	Use Directory Connector to sync groups and users to Bitwarden from your existing directory service.
Invite	Directory Connector will automatically issue invitations to synced users.
Authenticate	Pair your login with SSO implementation with the SSO policy to require users to sign up with SSO when they accept their invitations.
Administer	Use the web vault to promote some users to different roles and to ensure group-collection relationships are configured to grant the right access to the right users.
Re-synchronize	Periodically re-run Directory Connector to remove users from Bitwarden that are no longer active in your directory service and to start onboarding for new hires.

FAQs

Q: If an employee already has a Bitwarden account, can we attach it to the organization so they don't need another Bitwarden account?

A: Yes! You can. Some customers recommend that prior to attaching users to the organization, that those users have a Bitwarden vault attached to their company email. This choice is company-specific and either approach works.

Q: When an employee leaves, can we detach their account from the organization so that they don't have access to company credentials anymore and they do not lose their individually-owned credentials?

A: Yes! That's exactly what deprovisioning entails.

Q: What happens to items that were created or shared by a former member of the organization? Will these items also be offboarded?

A: No, sharing items from an individual vault to an organization vault will extend item ownership to the organization as well.

Q: Can we prevent employees from duplicating credentials from the company organization to their individual vault

A: Yes! Using our comprehensive suite of role-based access controls you can make credentials **Read Only** to prevent duplication.