Get Started with Bitwarden: Administrator

Get Started with Bitwarden: Administrator

We're thrilled that you're considering Bitwarden for your business's secure credential sharing needs. Let's walk through the first steps we'll take towards successful partnership:

⇒Enterprise

> 💡 **Tip**
>
> The first few steps in the document assume you're going to create an organization. If you're joining an existing organization, skip down to **Or join an existing organization**.

Sign up for Bitwarden

Bitwarden offers free accounts with no limits to the number of devices or number of logins you can use. Get started today.

Your master password

During sign-up, you'll create a master password for logging in to Bitwarden. It's important that your master password is:

- **Memorable**: Bitwarden employees and systems have **no** knowledge of, way to retrieve, or way to reset your master password. **Do not forget your master password!**

- **Strong**: A longer, more complex, and less common password is the best way to protect your account. Bitwarden provides a free password strength testing tool to test the strength of some memorable passwords you are considering.

Set a master password

Create an organization

Create your organization today by selecting the **New organization** button in the Bitwarden web app:

New organization

Or join an existing organization

If your organization has already been created, ask the IT team at your company or your manager for information on how you're expected to join Bitwarden. Some organizations send email invitations to your work inbox, others will allow you to enroll by simply logging in with your single sign-on (SSO) account.

Get to know the Admin Console

Once created, you'll land in the Admin Console, which is the central hub for all things sharing and organization administration. As the organization owner, you'll be able to see your **Vault** items and collections, to manage **Members,** run **Reports**, change **Billing** settings, and configure other organization **Settings**:

Free organization Admin Console

Managing vault items and collections

As an owner or admin, you might be responsible for managing access to **vault items**, like shared credentials, for your company or team. You can create directly from the web app and assign them to collections in order to share them with your team:

Assign to collections in bulk

Speaking of **collections**, they're an important construct for grouping together related logins, notes, cards, and identities for secure sharing with your organization:

- Organizations can define access to collections, allowing users or groups to access only the items they need.

- Items stored in an organization's collection(s) do not belong to any individual user, but rather to the organization.

- Organization-owned items **must** be included in at least one collection.

> 💡 **Tip**
>
> Data can also be imported directly to your organization! Learn how here.

Managing members and groups

As an owner or admin, you might be responsible for managing members of your team or your company more broadly. Members can be added to your organization:

- Directly from the Admin Console's **Members** page (learn more).

- By integrating Bitwarden with your IdP using SCIM (learn more).

- By integrating Bitwarden with your directory service using Directory Connector (learn more).

Members can assigned directly to collections in order to regulate what vault data they have access to, but so can **groups**. Groups relate together individual members and provide a scalable way to assign access to and permissions for specific collections:

New group

Policies, integrations, and more

Enterprise Bitwarden organizations provide powerful tools for improving your online security and integrating with existing workflows and tools. Some other things you might manage as an administrator of your organization include:

- Setting up policies to enforce security rules for users, for example mandating use of two-step login.

- Auditing what credentials organization members have access to.

- Integrating Bitwarden with your existing SSO workflow.

- Verifying your organization's domain for an seamless login experience.

- Setting up a system for, or approving, device trust requirements for members.

- Integrating Bitwarden with your existing SIEM tool, like Microsoft Sentinel.

⇒Teams

> 💡 **Tip**
>
> The first few steps in the document assume you're going to create an organization. If you're joining an existing organization, skip down to **Or join an existing organization**.

Sign up for Bitwarden

Bitwarden offers free accounts with no limits to the number of devices or number of logins you can use. Get started today.

Your master password

During sign-up, you'll create a master password for logging in to Bitwarden. It's important that your master password is:

- **Memorable**: Bitwarden employees and systems have **no** knowledge of, way to retrieve, or way to reset your master password. **Do not forget your master password!**

- **Strong**: A longer, more complex, and less common password is the best way to protect your account. Bitwarden provides a free password strength testing tool to test the strength of some memorable passwords you are considering.

Set a master password

Create an organization

Create your organization today by selecting the **New organization** button in the Bitwarden web app:

New organization

Or join an existing organization

If your organization has already been created, ask the other member of your organization to send you an invite.

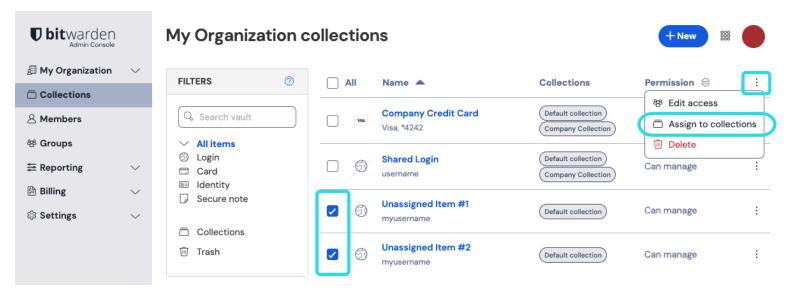## Get to know the Admin Console

Once created, you'll land in the Admin Console, which is the central hub for all things sharing and organization administration. As the organization owner, you'll be able to see your **Vault** items and collections, to manage **Members,** run **Reports**, change **Billing** settings, and configure other organization **Settings**:

Free organization Admin Console

Managing vault items and collections

As an owner or admin, you might be responsible for managing access to **vault items**, like shared credentials, for your company or team. You can create directly from the web app and assign them to collections in order to share them with your team:

Assign to collections in bulk

Speaking of **collections**, they're an important construct for grouping together related logins, notes, cards, and identities for secure sharing with your organization:

- Organizations can define access to collections, allowing users or groups to access only the items they need.

- Items stored in an organization's collections(s) do not belong to any individual user, but rather to the organization.

- Organization-owned items **must** be included in at least one collection.

> 💡 **Tip**
>
> Data can also be imported directly to your organization! Learn how here.

Managing members and groups

As an owner or admin, you might be responsible for managing members of your team or your company more broadly. Members can be added to your organization:

- Directly from the Admin Console's **Members** page (learn more).

- By integrating Bitwarden with your IdP using SCIM (learn more).

- By integrating Bitwarden with your directory service using Directory Connector (learn more).

Members can assigned directly to collections in order to regulate what vault data they have access to, but so can **groups**. Groups relate together individual members and provide a scalable way to assign access to and permissions for specific collections:

bitwarden

Secure and trusted open source password manager for business

New group

Policies, integrations, and more

Teams Bitwarden organizations provide powerful tools for improving your online security and integrating with existing workflows and tools. Some other things you might manage as an administrator of your organization include:

- Auditing what credentials organization members have access to.

- Integrating Bitwarden with your existing SIEM tool, like Microsoft Sentinel.

⇒Families

> 💡 **Tip**
>
> The first few steps in the document assume you're going to create an organization. If you're joining an existing organization, skip down to **Or join an existing organization**.

Sign up for Bitwarden

Bitwarden offers free accounts with no limits to the number of devices or number of logins you can use. Get started today.

Your master password

During sign-up, you'll create a master password for logging in to Bitwarden. It's important that your master password is:

- **Memorable**: Bitwarden employees and systems have **no** knowledge of, way to retrieve, or way to reset your master password. **Do not forget your master password!**

- **Strong**: A longer, more complex, and less common password is the best way to protect your account. Bitwarden provides a free password strength testing tool to test the strength of some memorable passwords you are considering.

Set a master password

Create an organization

Create your organization today by selecting the **New organization** button in the Bitwarden web app:

New organization

Or join an existing organization

If your organization has already been created, ask the other member of your organization to send you an invite.

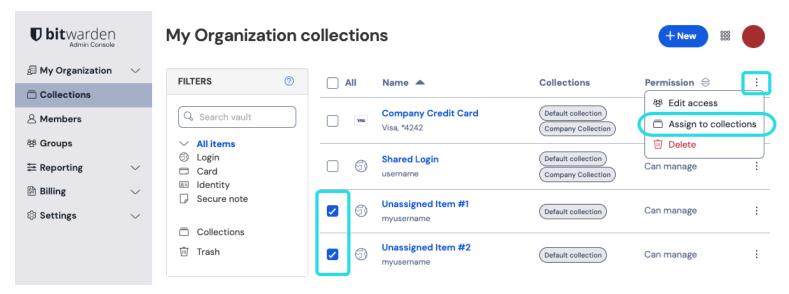## Get to know the Admin Console

Once created, you'll land in the Admin Console, which is the central hub for all things sharing and organization administration. As the organization owner, you'll be able to see your **Vault** items and collections, to manage **Members,** run **Reports**, change **Billing** settings, and configure other organization **Settings**:

Free organization Admin Console

Managing vault items and collections

As an owner or admin, you might be responsible for managing access to **vault items**, like shared credentials, for your family. You can create directly from the web app and assign them to collections in order to share them with your family:

Assign to collections in bulk

Speaking of **collections**, they're an important construct for grouping together related logins, notes, cards, and identities for secure sharing with your organization:

- Organizations can define access to collections, allowing users to access only the items they need.

- Items stored in an organization's collections(s) do not belong to any individual user, but rather to the organization.

- Organization-owned items **must** be included in at least one collection.

> 💡 **Tip**
>
> Data can also be imported directly to your organization! Learn how here.

Managing members and groups

As an owner or admin, you might be responsible for managing members of your family more broadly. Members can be added to your organization directly from the Admin Console's **Members** page (learn more):

Invite member to an organization

Help your family be safe

Now that you're setup to securely share data with your family through Bitwarden, consider some other ways of making sure your loved ones stay safe online:

- Help your family set up two-step login to protect their Bitwarden accounts.

- Help your family set up emergency access so important data can be accessed in cases of emergency.

⇒Free

> 💡 **Tip**
>
> The first few steps in the document assume you're going to create an organization. If you're joining an existing organization, skip down to **Or join an existing organization**.

Sign up for Bitwarden

Bitwarden offers free accounts with no limits to the number of devices or number of logins you can use. Get started today.

Your master password

During sign-up, you'll create a master password for logging in to Bitwarden. It's important that your master password is:

- **Memorable**: Bitwarden employees and systems have **no** knowledge of, way to retrieve, or way to reset your master password. **Do not forget your master password!**

- **Strong**: A longer, more complex, and less common password is the best way to protect your account. Bitwarden provides a free password strength testing tool to test the strength of some memorable passwords you are considering.

Set a master password

Create an organization

Create your organization today by selecting the **New organization** button in the Bitwarden web app:

New organization

Or join an existing organization

If your organization has already been created, ask the other member of your organization to send you an invite.

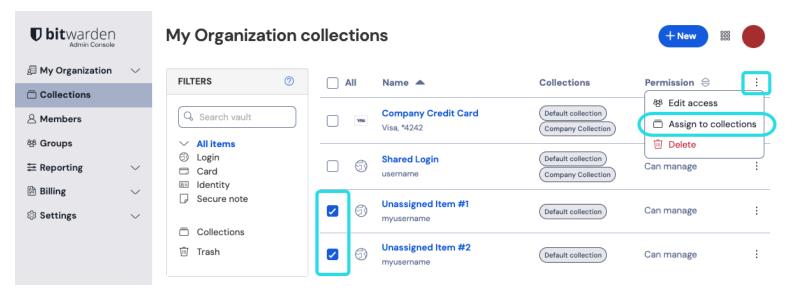## Get to know the Admin Console

Once created, you'll land in the Admin Console, which is the central hub for all things sharing and organization administration. As the organization owner, you'll be able to see your **Vault** items and collections, to manage **Members**, and configure other organization **Settings**:

Free organization Admin Console

Managing vault items and collections

As an owner or admin, you might be responsible for managing access to **vault items**, like shared credentials, for your organization. You can create directly from the web app and assign them to collections in order to share them:

Assign to collections in bulk

Speaking of **collections**, they're an important construct for grouping together related logins, notes, cards, and identities for secure sharing with your organization:

- Organizations can define access to collections, allowing users to access only the items they need.

- Items stored in an organization's collections(s) do not belong to any individual user, but rather to the organization.

- Organization-owned items **must** be included in at least one collection.

- As a free organization, you can have up to two collections.

> 💡 **Tip**
>
> Data can also be imported directly to your organization! Learn how here.

Managing members and groups

As an owner, you'll be responsible for inviting the other member to your organization directly from the Admin Console's **Members** page (learn more):

bitwarden

Secure and trusted open source password manager for business

bitwarden
Admin Console

- My Free Organizat... ∨
- Collections
- Members
- Reports ∨
- Billing ∨
- Settings ∨

Members

Search members   + Invite member

All **1**   Invited   Needs confirmation   Revoked

☐ All	Name ▲	Collections	Role ⇵	Policies	⋮
☐	BW **Brett Warden**	Household Finances Streaming Services	Owner		⋮

Invite member to an organization