

RESOURCE CENTER

Bitwarden Teams Trial Guide for Admins and Owners

A step-by-step guide to get the most out of your Bitwarden Teams trial.

Get the full interactive view at
<https://bitwarden.com/resources/teams-trial-emails/>



Get started in 5 simple steps

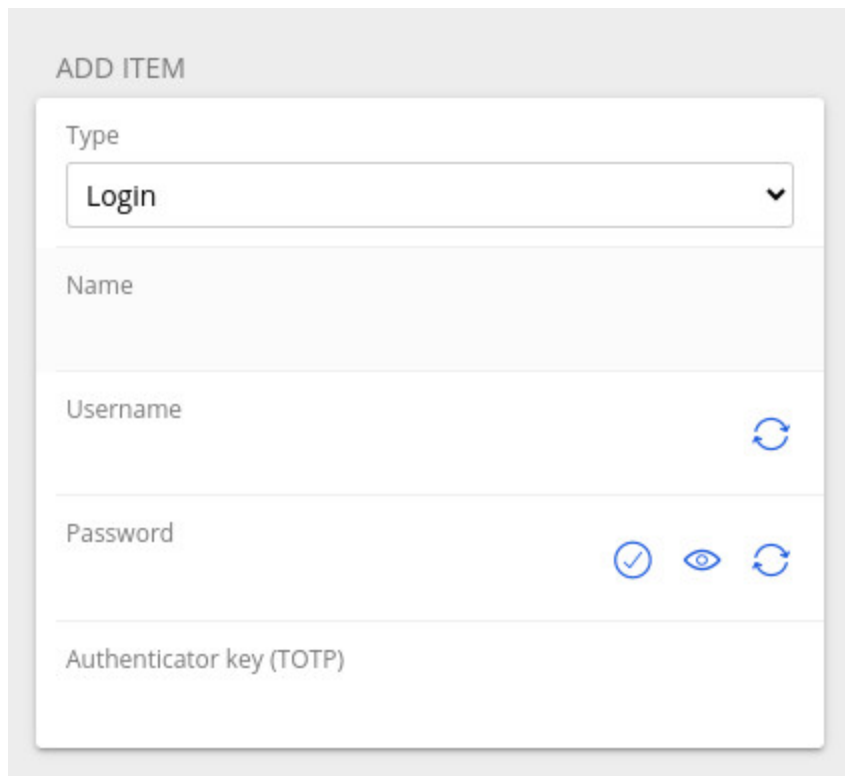
Take these key actions during your trial to ensure a smooth onboarding experience for you and your team.

1. Save your first login

In your Bitwarden Vault you can store logins, credit cards, identities, and secure notes; these are known as Items. Logins are the most commonly stored Item-type and consist of a username, a password, the website domain associated with the login, and more.

Follow these steps to create and save your first login:

1. Log in to the [web app](#)
2. In the default **All vaults** view click the **New** button at the top right of your screen and select **Item**
3. Select item type **Login** from the dropdown



The screenshot shows the 'ADD ITEM' form in Bitwarden. The 'Type' dropdown menu is open, showing 'Login' as the selected option. Below the dropdown are input fields for 'Name', 'Username', 'Password', and 'Authenticator key (TOTP)'. The 'Username' field has a refresh icon, and the 'Password' field has icons for a checkmark, an eye, and a refresh.

Creating a new vault item in Bitwarden.

4. Fill in the required fields from memory, referencing your current password manager, or just make one up for practice!
5. **Save** the item

And just like that, you've created your first login. If you've been storing passwords in a notebook or on your notes app, you'll need to do this for every new login. Start with your most sensitive ones (ie financial accounts) first!

If you're coming over from another password manager, Bitwarden makes it easy to [import items directly into your vault](#) from most password managers or web browsers.

2. Create your first collection

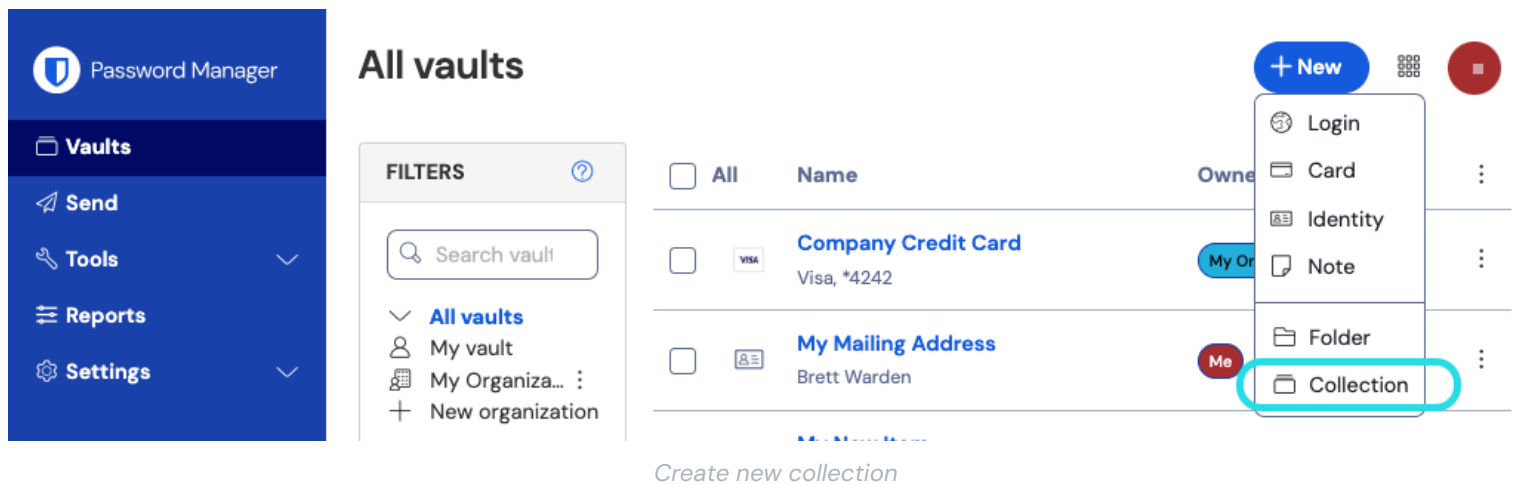
A Collection is a shared space where businesses store vault items (logins, notes, cards, and identities) for secure sharing. Admins assign access to Collections by individual, role, or team. This allows employees to quickly access the passwords they need, whenever they need them.

For example, a Marketing Team might have a Marketing Collection that includes social media logins, credit cards for paid media channels, and secure notes with confidential team information.

Collections are the primary means to quick and secure sharing across teams and individuals.

To create a collection:

1. Log in to the Bitwarden web app, select the **New** button, and choose **Collection** from the dropdown:



2. In the **Collection info** tab give your collection a **Name**, and choose the **organization** it should belong to.

3. In the **Access** tab, assign access to any existing members or **groups**. For each selection, assign the appropriate level of **permission**. As the creator of the collection, you will have **can manage** permission.

4. Select **Save** to finish creating your collection.

During your trial, consider creating a few key Collections that you know you'll need going forward. This will give you a head-start on your onboarding and enable you to quickly give access to the right people in your organization when you are ready.

3. Invite new members

Members are the people on your team who will be using the Bitwarden Password Manager.

Bitwarden is known for being easy to use and approachable for people of all technical skill levels. By encouraging and enabling Bitwarden use across your business, you are taking a significant step toward securing your organization.

Here's how to invite new members to your organization:

1. Log in to the Bitwarden web app.

2. Open the Admin Console using the product switcher:

Filters

- Search vaults
- All vaults
 - My vault
 - My Organiz...
 - Teams Org...
 - New organization
- All items
 - Favorites
 - Login
 - Card
 - Identity
 - Secure note
- Folders
 - No folder
- Collections
 - Default colle...
 - Default colle...
- Trash

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Product switcher

3. In the Admin Console, select **Members** from the navigation and use the **Invite member** button:
4. In the **Role** tab, enter the **Email** of your second member, which should match the email they [signed up for Bitwarden](#) with. Then, select a **Member role**.
5. In the **Collections** tab, select which collections to allow this user access to, as well as what the level of permission for each to give them.
6. Select **Save** to send the invitation to the designated email address.

Once your invitation is sent, inform your new member and help them [accept the invitation](#).

Bitwarden provides on-demand support for Members in the Learning Center. [Here's a simple guide](#) to share with new team members as you invite them to use Bitwarden.

4. Audit employee password practices

As the Admin for your organization, it is important to understand and improve employee password habits. Bitwarden makes this easy with Vault Health Reports.

Every Member in your organization has access to their own individual Vault Health Reports, but as the Admin you get a bird's eye view of the entire organization's password health (not their passwords).

To run any vault health report at the organization level follow the steps below:

1. Log in to the Bitwarden web app.
2. Open the Admin Console using the product switcher:
3. In your organization, select Reporting → Reports from the navigation

bitwarden
Admin Console

My Organization

Collections

Members

Groups

Reporting

Event logs

Reports

Billing

Settings

Password Manager

Admin Console

Reports

Identify and close security gaps in your organization's accounts by clicking the reports below.

Exposed passwords

Passwords exposed in a data breach are easy targets for attackers. Change these passwords to prevent potential break-ins.

Reused passwords

Reusing passwords makes it easier for attackers to break into multiple accounts. Change these passwords so that each is unique.

Weak passwords

Weak passwords can be easily guessed by attackers. Change these passwords to strong ones using the password generator.

Unsecure websites

URLs that start with `http://` don't use the best available encryption. Change the login URIs for these accounts to `https://` for safer browsing.

Inactive two-step login

Two-step login adds a layer of protection to your accounts. Set up two-step login using Bitwarden authenticator for these accounts or use an alternative method.

Member access

Ensure members have access to the right credentials and their accounts are secure. Use this report to obtain a CSV of member access and account configurations.

Organization reports

4. Click on any report to run it.

Just like that, you can see which employees are using exposed, reused, or weak passwords and for which accounts.

Pro tip: help members level up their own password security practices by encouraging them to run each of these reports in their own Vaults and correcting any issues that pop up.

5. Download Bitwarden on all your devices

Bitwarden is available everywhere. To get the most out of the password manager make sure you have it installed on any devices you might use for work.

[Download Bitwarden on all your devices](#) to unleash the full power of open source password management

Pro tip: use the Browser Extension to [detect and save new logins](#), [autofill usernames and passwords](#), and [quickly insert 2FA codes](#).

Top features and benefits

Put these top features for teams to the test

Vault Health Reports

Gain insight into exposed, weak, and reused passwords, unsecured websites, data breaches, and more.

Event and Audit Logs

Get an overview of user activity with exportable and timestamped event logs of your organization vault.

Two-Step Login

Enhance security by requiring end-users to use a two-step login method to access their vaults.

API Access

Automate the management of members, collections, groups, event logs, and policies through the Bitwarden public API.

Share with Anyone

Use Bitwarden Send to securely share encrypted information directly with anyone.

User Access Control

Set user permissions to access, edit or read items within a collection.

Directory Sync

Provision and deprovision accounts easily by connecting your existing directory service to your Bitwarden organization.

Training & Priority Support

Access training for owners, admins, and end-users, and get 24/7 priority support whenever you need it.

Explore the full list of Bitwarden business features [here](#) (note: some features may only be available in the Enterprise plan).

Training and Deployment

Set the stage for a successful deployment across your team

1. Join a live training or watch on-demand

Our weekly [live demos](#) and [on-demand training](#) options are a great place for you and your employees to build expertise.

2. Educate users and set clear expectations

Educate end-users about the importance of adopting secure password practices (both at home and in the workplace) and communicate the steps in the deployment process so they can better prepare for change.

3. Take advantage of the Help Center

The [Help Center](#) is your go-to destination for answers to your Bitwarden questions, and join the Bitwarden Community [forums](#) to share knowledge and tips with other security-minded users.