bitwarden | Help Center Article

PASSWORD MANAGER > GET STARTED

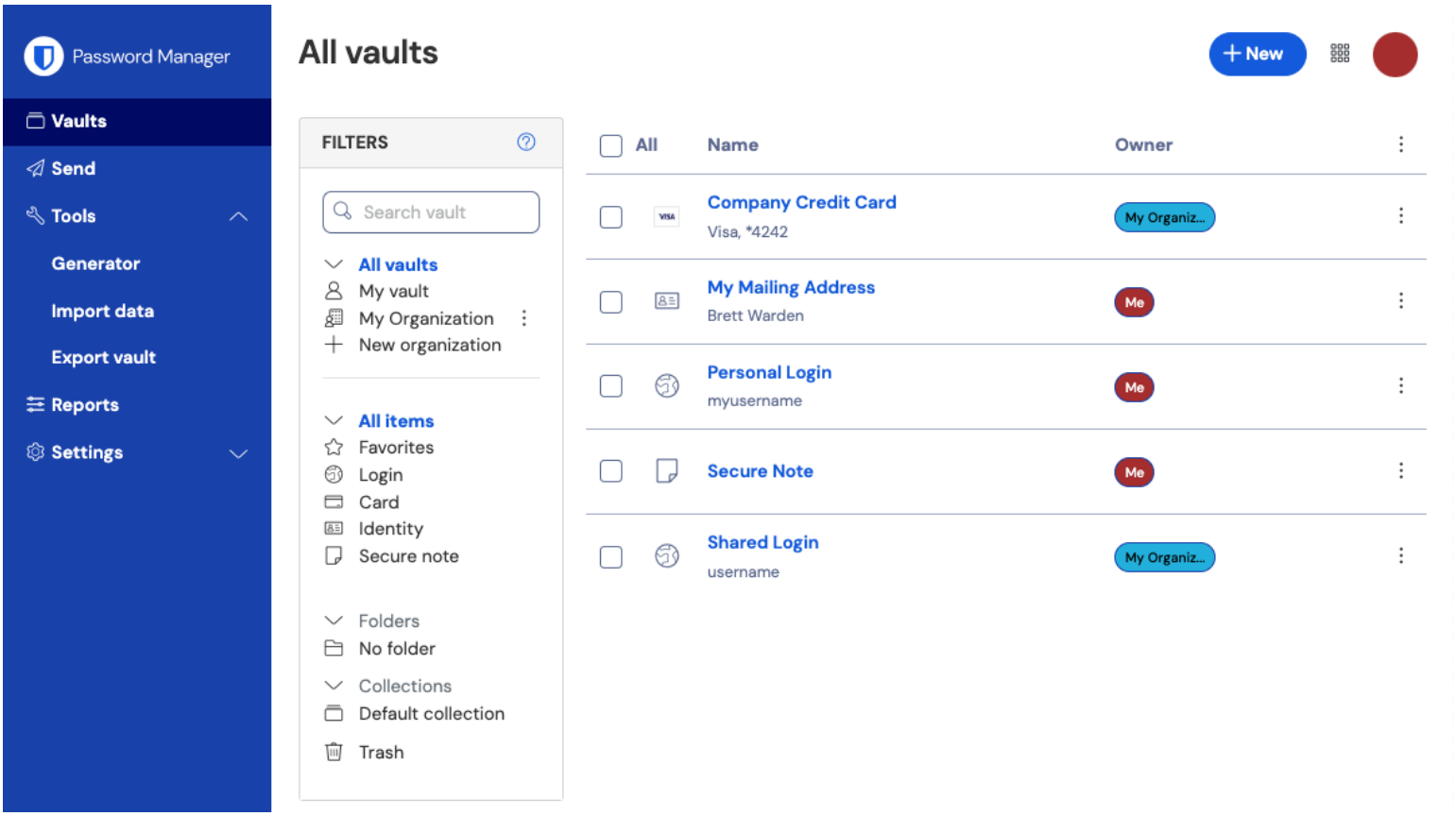
Password Manager Web App

View in the help center:
https://bitwarden.com/help/getting-started-webvault/

Password Manager Web App

The Bitwarden web app provides the richest Bitwarden experience for personal users and organizations. Many important functions such as setting up two-step login or administering an organization must be done from the web app.

> **Tip**
>
> The web app is accessible from any modern web browser at vault.bitwarden.com and vault.bitwarden.eu. If you are **self-hosting** Bitwarden, access to the web app will be located at your configured domain, for example `https://my.bitwarden.server.com`.



Password Manager web app

When you first log in to your web app, you'll land on the **All vaults** view. This space will list all vault items, including logins, cards, identities, and secure notes.

First steps

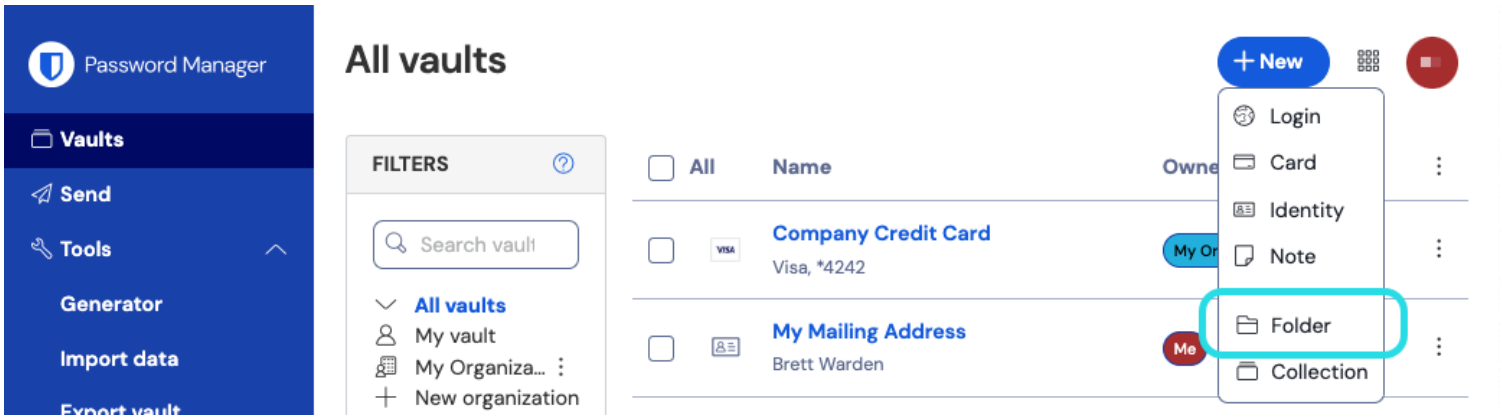
In the previous screenshot, the **All vaults** view is displaying **All Items** in all vaults. Members of organizations will have other vaults listed here. Using the **Filters** column, you can organize your vault into **Favorites** and **Folders**.

Let's start by setting up a new folder and adding a new login to it:

Create a folder

To create a folder:

1. Select the + **New** button and choose **Folder** from the dropdown:



New folder

2. Enter a name (for example, `Social Media Logins`) for your folder and select **Save**.

> **Tip**
>
> For a cleaner vault, you can nest folders inside other folders.

Add a login

To add a new login item:

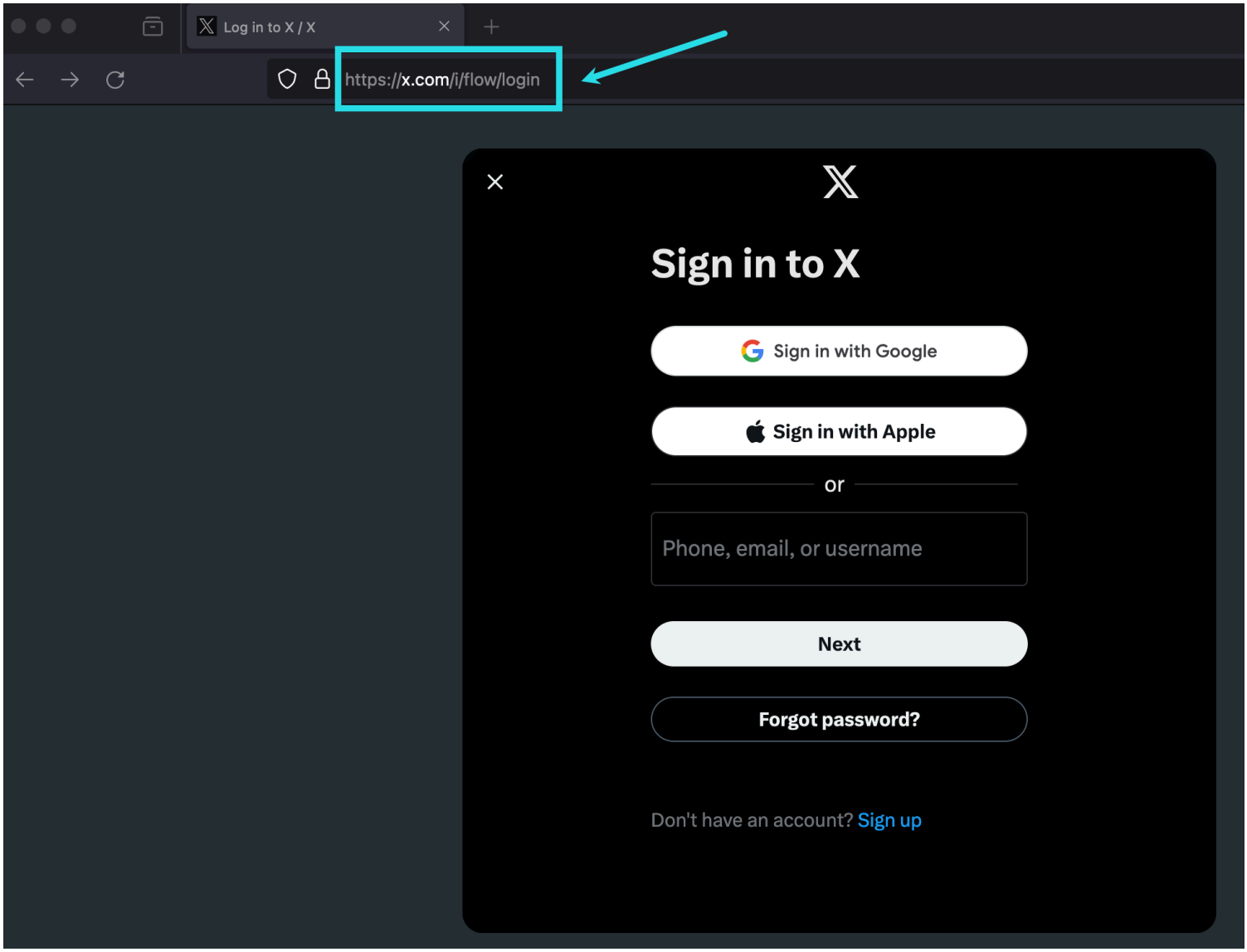
1. Select the + **New** button and choose **Login** from the dropdown.

2. Enter an **Item name**. Names will help you easily identify items in your vault, so give this item a recognizable one (for example, `My X.com Account`).

3. From the **Folder** dropdown, select the name of the folder you want to add this item to (for example, the `Social Media Logins` folder we created earlier).

4. Enter your **Username** and **Password**. For now, enter your existing password. We will help you replace it with a stronger password later.

5. In the **Website (URI)** field, enter the URL of the website (for example, `https://x.com/i/flow/login`). If you don't know what URL to use, navigate to the website's login screen and copy it from your address bar.



Locating URI X.com

6. Select the ☆ **Favorite** icon to add this item to your favorites. The icon will fill-in (☆ → ★) when it is a favorite.

7. Nice work! Select the **Save** button to finish adding this item.

Generate a strong password

Now that a new login is saved in your vault, improve its security by replacing the existing password with a stronger one:

1. In your vault, select the item you want to secure to open it and select the **Edit** button.

2. In a new tab or window, open the corresponding website and login to your account.

> **Tip**
> If you entered something in the **URI 1** field, click the **Launch** icon to open it directly from your vault.

3. On that website, navigate to the area where you can **Change your password**.

Typically, you can find this in a **Your Account**, **Security**, **Sign in Settings**, or **Login Settings** section.

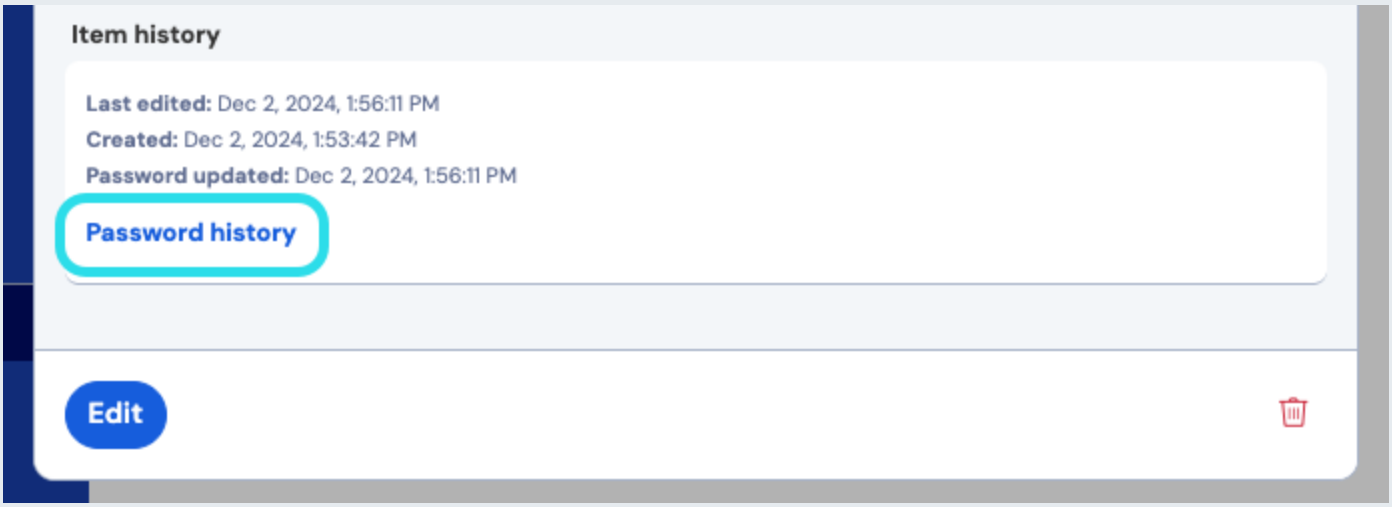
4. Most websites require you to enter your **Current password** first. Return to your vault and select the **Copy** icon next to the **Password** field. Then, return to the website and paste it into the **Current password** field.

   You might have the old password memorized, but it's a good idea to get in the habit of copying and pasting your password. This is how you will be logging in once your password is replaced with a stronger one.

5. Return to your vault and click the **Generate** icon next to the **Password** field. You will be asked whether you want to overwrite the current password, so select **Yes** to proceed.

   This will replace your **Password** with a randomly generated strong password. Moving from a password like `Fido1234` to `X@Ln@x9J@&u@5n##B` can stop a hacker.

6. Copy your new password with the same **Copy** icon you used earlier, and select the **Save** button.

> **Tip**
>
> Don't worry about overwriting your existing password! If something goes wrong, Bitwarden maintains a **Password History** of the last five passwords for every login:
>
> 
>
>
> *View password history*

7. Return to the other website and paste your strong password in the **New Password** and **Confirm new password** fields.

8. Once you **Save** the password change, you are finished!

Import your data

Good news! You don't need to repeat this process for every login if you have usernames and passwords saved in a web browser or other password manager. Use one of our specialized import guides for help transferring your data from:

- LastPass
- 1Password
- Dashlane
- macOS & Safari

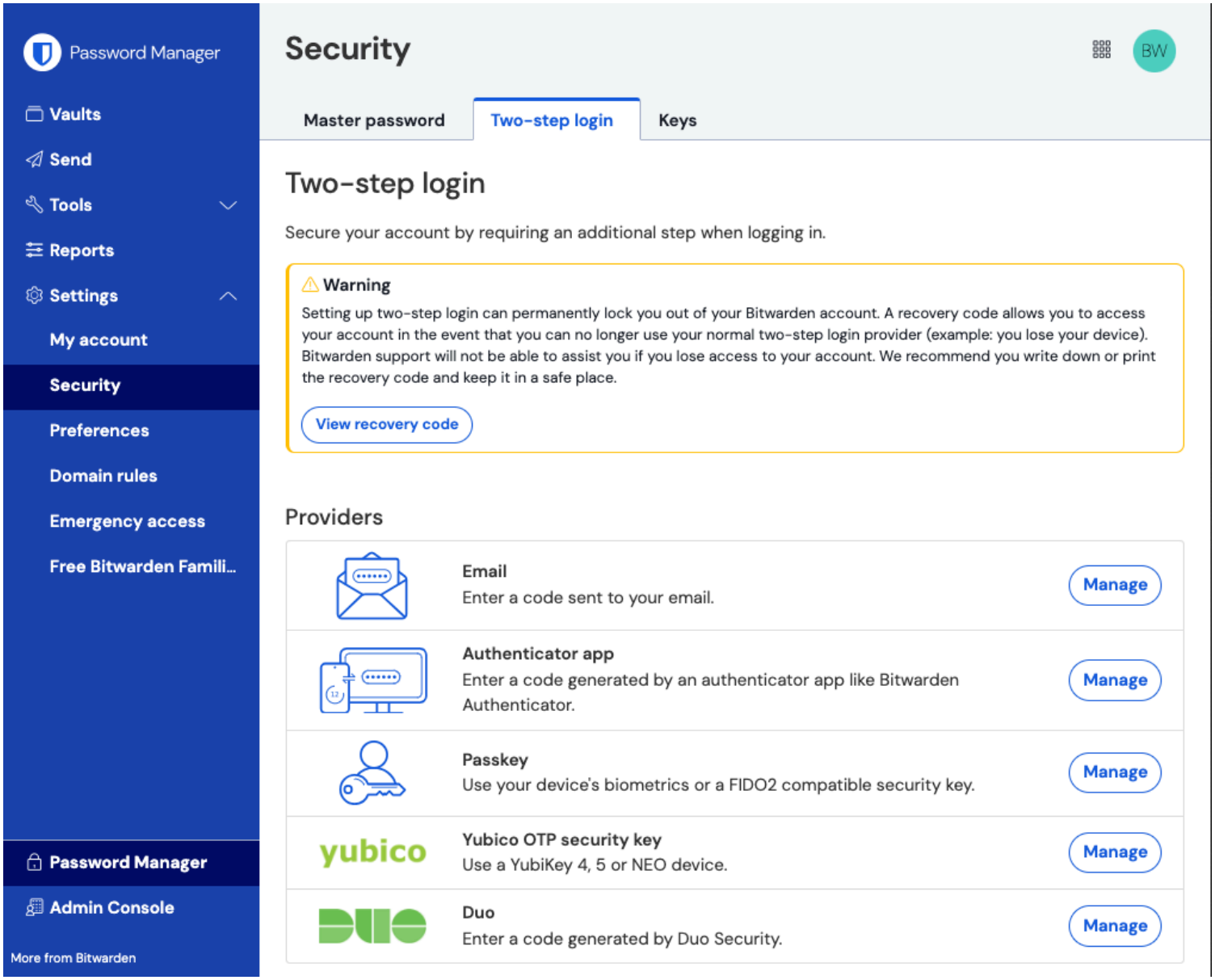
- Google Chrome
- Firefox

Secure your vault

Now that your vault is full of data, let's take some steps to protect it by setting up two-step login. Two-step login requires you to verify your identity when logging in using an additional token, usually retrieved from a different device.

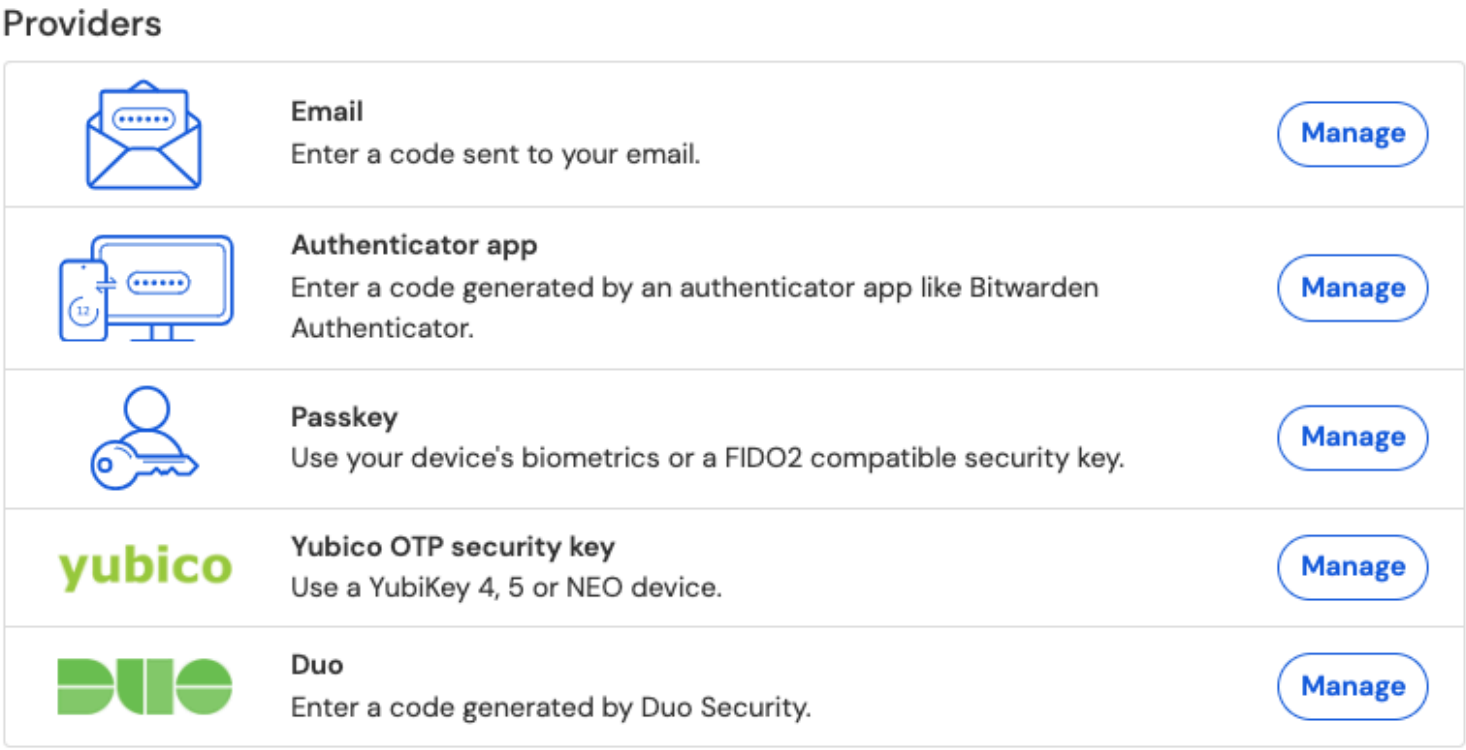
There are many available methods for two-step login, but the recommended method for a free Bitwarden account is using a mobile device authenticator app such as Bitwarden Authenticator:

1. Download Bitwarden Authenticator on your mobile device.
2. In the Bitwarden web app, select **Settings** → **Security** → **Two-step login** from the navigation:



Two-step login

3. Locate the **Authenticator App** option and select **Manage**:



Two-step login providers

You'll be prompted to enter your master password to continue.

4. On your mobile device, open Bitwarden Authenticator and tap the + button.

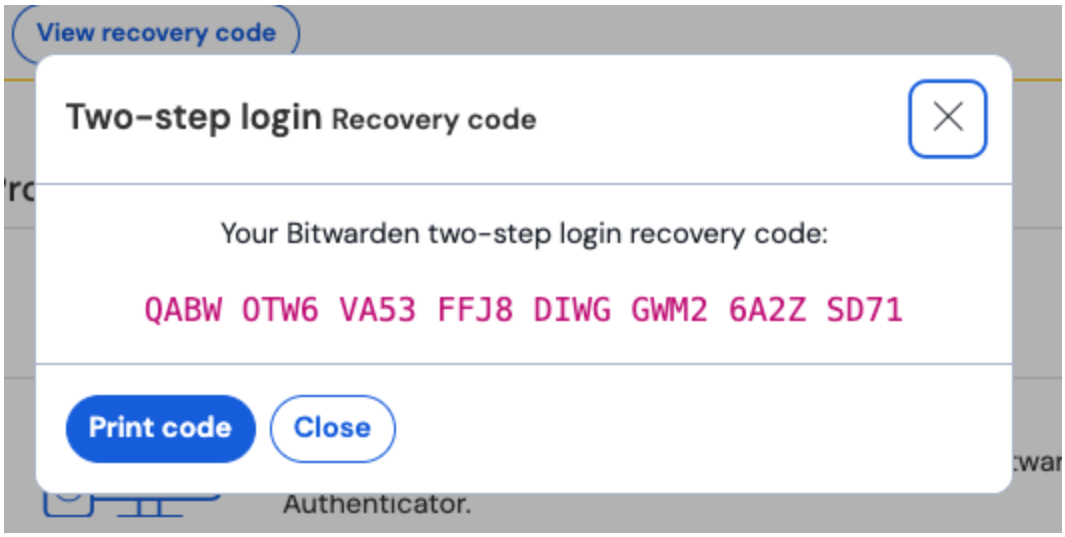
5. Scan the QR code located in your web app using Bitwarden Authenticator. Once scanned, Bitwarden Authenticator will display a six-digit verification code.

6. Enter the six-digit verification code into the dialog box in your web app, and select the **Enable** button.

7. Select the **Close** button to return to the Two-step login screen, and select the **View Recovery Code** button.

   Your recovery code can be used in the event that you lose your mobile device. **This is a critical step to ensure you don't ever get locked out of your vault**, so don't skip it!

8. Enter your master password and select the **Continue** button to get your recovery code.



Sample Recovery Code

Save your recovery code in the way that makes the most sense for you. Believe it or not, printing your recovery code and keeping it somewhere safe is one of the best ways to make sure that the code is not vulnerable to theft or inadvertent deletion.

Next steps

Congratulations on mastering the basics of Bitwarden! We want everyone to be safe online, so we are proud to offer everything you have learned about here for free.

Signup for premium

For personal users, we offer a premium subscription for $10 / year that unlocks advanced capabilities including:

- Advanced two-step login options, like Duo and YubiKey security keys
- Storage space for encrypted file attachments
- An integration temporary one-time password (TOTP) authenticator
- Emergency access to your vault by trusted emergency contacts
- Vault health reports that report on password and security hygiene

To start a premium subscription, select the **Go Premium** button from your **Vaults** view!

Start an organization

Do you need to share passwords or other vault items with your friends, family, team, or entire business?

Bitwarden organizations let you do just that. We recommend trying out the functionality of password-sharing from organizations by starting a free two-person organization.

Once you have tested an organization, check out our Bitwarden pricing page to learn about the different organization types you might consider.