Cybersecurity

- Encrypting your Computer
- Setting up Antivirus
- Using a Password Manager

Encrypting your Computer

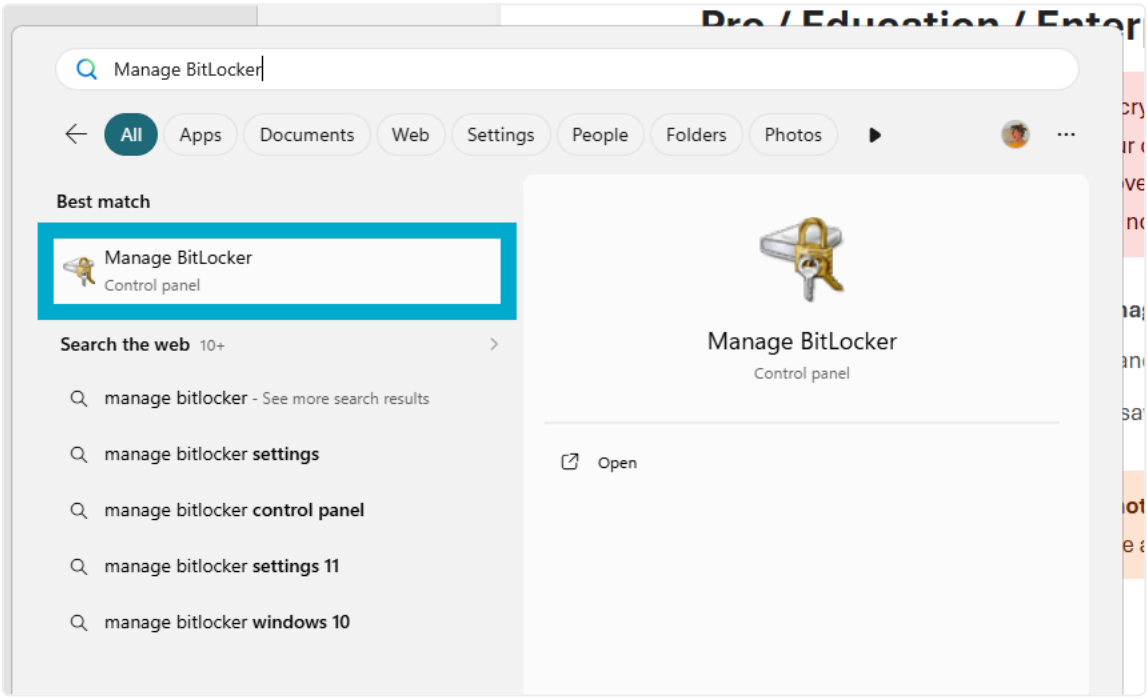
Users with personal devices have a responsibility to ensure that their devices connected to the BAC Network are encrypted. College owned devices set up by Helpdesk will be encrypted during setup. This page has instructions for encrypting personal devices.

Windows

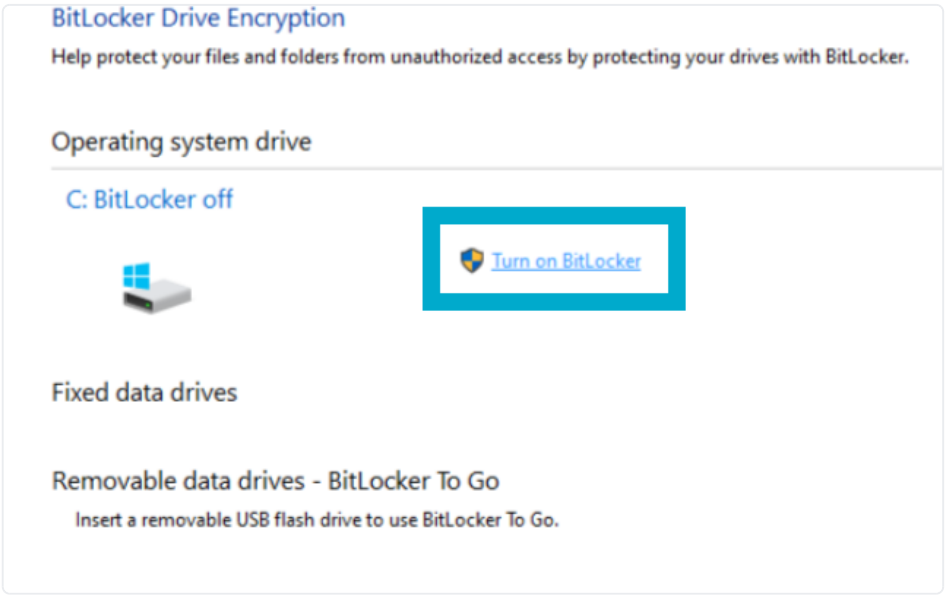
Pro / Education / Enterprise Edition

> **PRIOR TO ENCRYPTION**: Device encryption requires the creation of a **recovery key**. If you are ever unable to log onto your device or your computer needs replacement, you will NOT be able to recover data from your disk without this recovery key. It is recommended you save it in multiple secure locations for future use. Helpdesk is not responsible for the storage of your recovery keys.

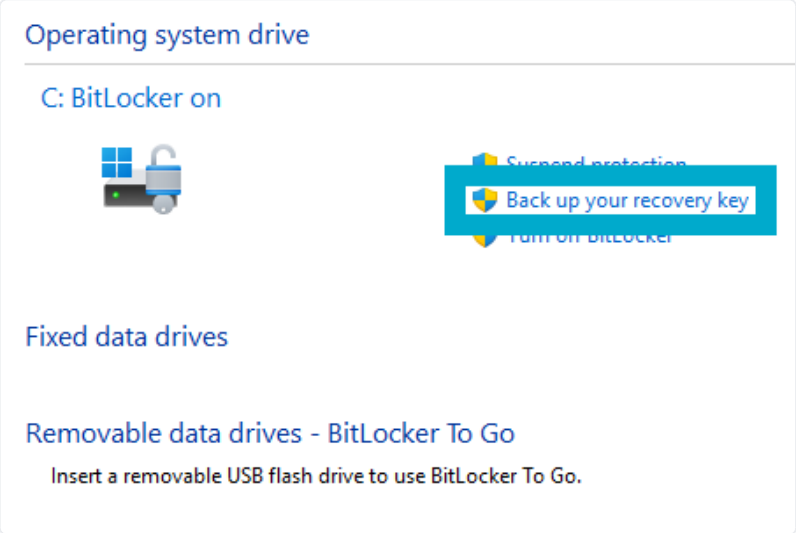
1. Open the Start Menu and search **Manage BitLocker**.



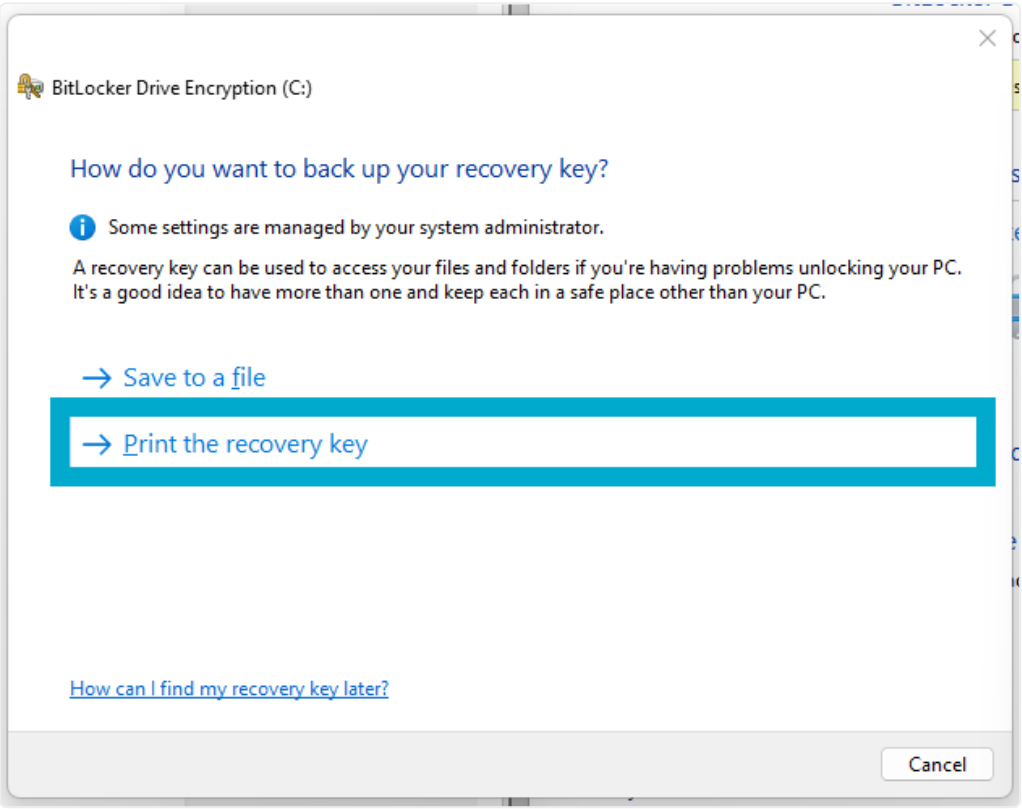
2. Select the drive you want to encrypt and press **Turn on BitLocker**.



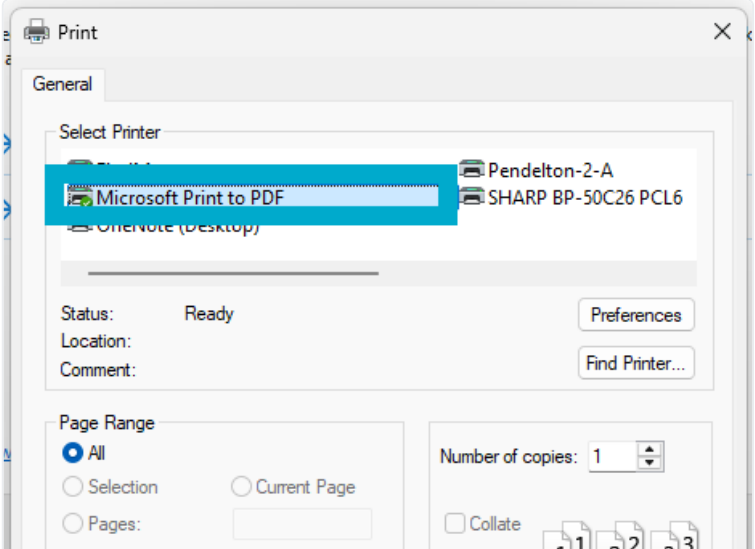
3. Click **Back up your recovery key**.



4. Click **Print the recovery key**.



5. Click **Microsoft Print to PDF**, then click **Print**.



> It is important that the PDF created is **not saved locally**. If BitLocker triggers and locks your encrypted drives, you will not be able to access any local files.

6. Click **Encrypt entire device**.
7. Select **New encryption mode**.
8. Restart your computer.

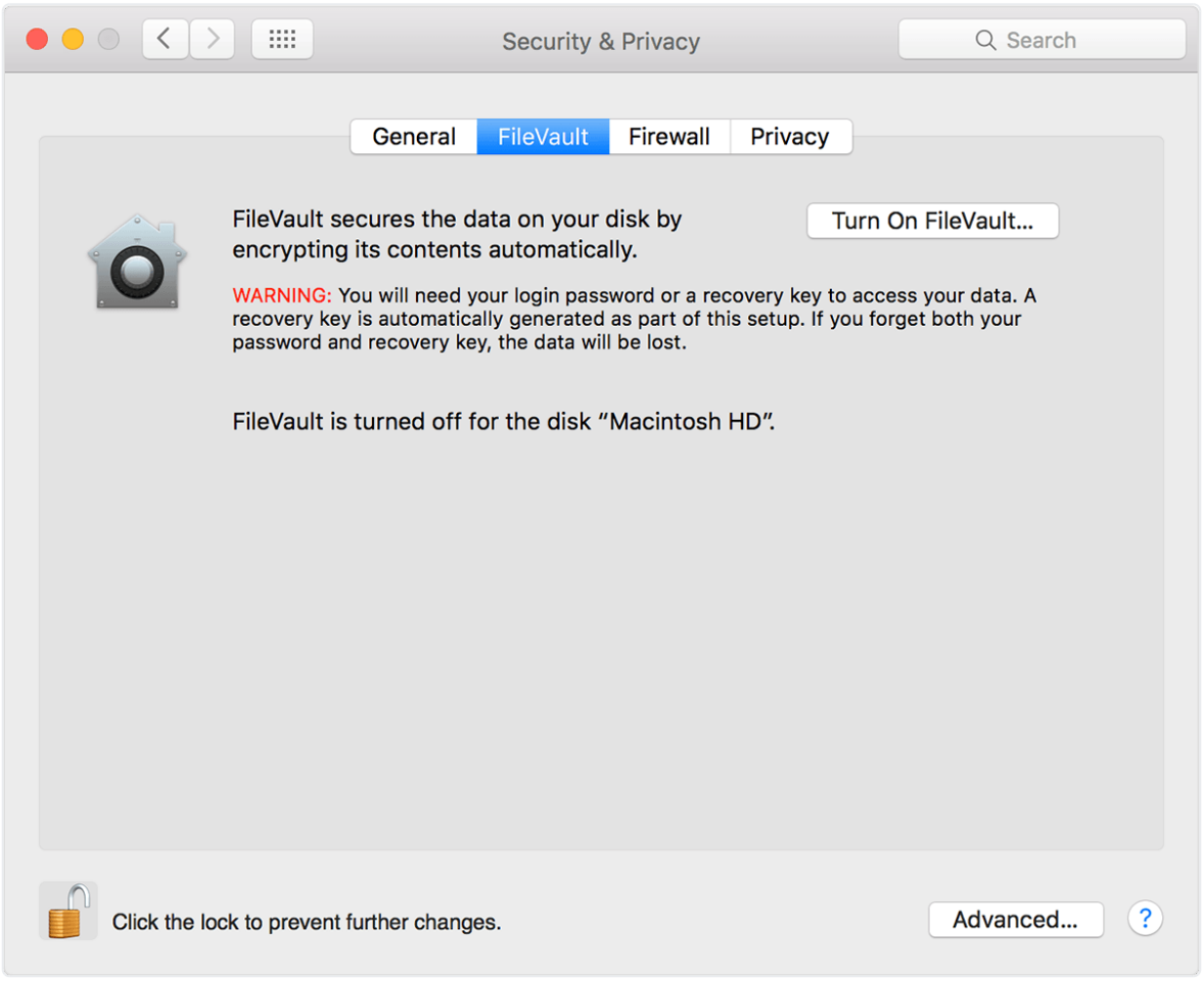
Home Edition

Windows Home uses BitLocker, however the user interface is significantly simplified. See this guide for instructions on how to encrypt your Windows Home device.

MacOS

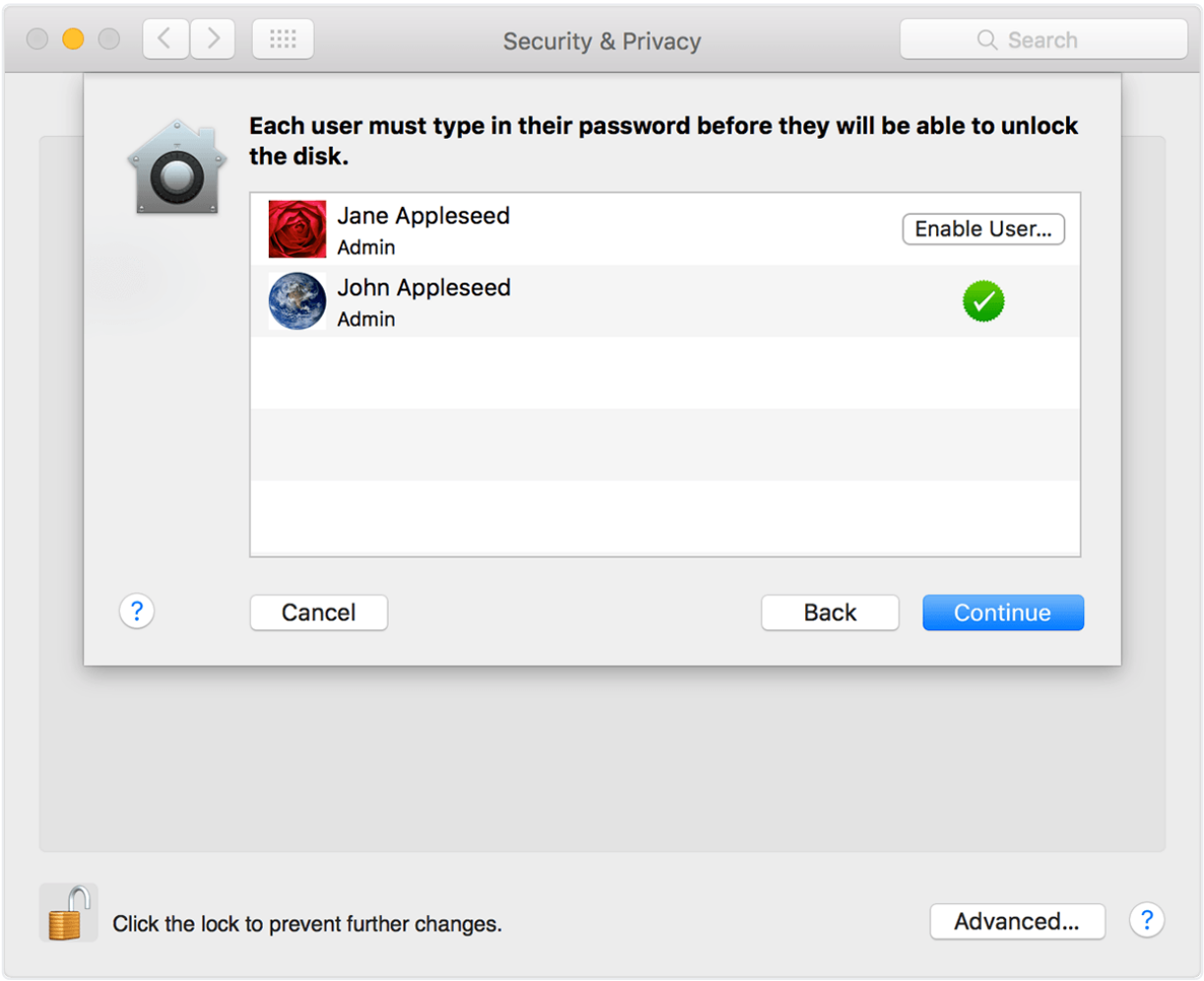
1. Go to **System Preferences**.
2. Open **Security & Privacy**.

3. Choose the tab **FileVault** and authenticate by clicking on the padlock in the bottom left corner.



4. Click **Turn on FileVault**.

5. Select the user(s).



6. Write down/take picture of the recovery key.

> If you forget your password, you will need this key to access your files.

7. Apple can also store they key, in case you lose your password and all other backups.

8. Restart your computer.

Setting up Antivirus

The college requires that you use an Antivirus on devices you use to access college data. This includes laptops used for work or school, as well as occasionally personal desktops and mobile devices. Our antivirus recommendations are sorted by operating system below.

Windows

- **College Owned**
  - Any Windows machine purchased/owned by the college, should be protected using Microsoft Defender 365.
  - This is a program that must be installed by the Helpdesk, so if you don’t think your device is protected, please contact the Helpdesk immediately.
- **Personal**
  - **Employee work use**
    - Personal Windows machines that are being used for work should be onboarded to Microsoft Defender 365 by Helpdesk.
    - Please contact the Helpdesk to get this set up on your device.
  - **Non-work use**

    - Personal Windows machines not used for work related purposes can be protected with the built-in Microsoft Defender.

MacOS

- College Owned
    - Any Mac machine purchased/owned by the college requires Microsoft Defender 365.
    - This is a program that must be installed by the Helpdesk, so if you don’t think your device is protected, please contact the Helpdesk immediately.
- Personal
    - Employee work use
        - Personal Mac devices require an antivirus solution to be installed for protection.
        - If this is a personal device used for work, Helpdesk will set up Microsoft Defender 365 on it. Please notify the Helpdesk if you have a personal Mac used for work purposes that doesn’t have Defender on it yet.
    - Non-work use
        - For a free antivirus solution for Mac, the Helpdesk recommends Malwarebytes

https://www.malwarebytes.com/mwb-download It is important to note that the free version of Malwarebytes does not offer automatic antivirus scanning. Scans must be run manually.

- For a paid antivirus, the Helpdesk's current recommendation is Bitdefender for Mac. It costs $40 a year and offers: active online protection, adware blocking, ability to add extra protection to important files, and Time Machine protections, which helps secure your backups. https://www.bitdefender.com/solutions/antivirus-for-mac.html#plans

Linux

Linux machines and their recommendations will depend upon the Linux distribution that is being used. Please contact the Helpdesk for additional information if you use a Linux device.

iOS & Android

If you use a mobile device to access company information, it must have an antivirus solution installed on it.

- Download Microsoft Defender onto your mobile device from the Apple App Store or Google Play Store.

- Once installed, you can log into the app by using your network account credentials.
- If you have any difficulties with accessing/activating protection, please contact the Helpdesk.

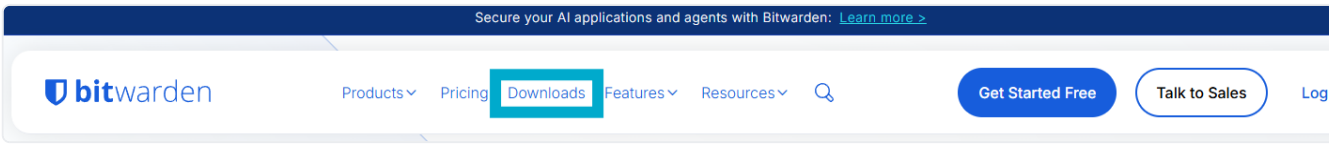
Using a Password Manager

The Helpdesk recommends you use a password manager to keep track of your account information. The default password managers in your web browser are not actually very secure; not to mention that your browser login is likely the first thing to be compromised in a theoretical data breach. Our recommendation is to use **Bitwarden**, which is free, high quality, and compatible across your devices.

> Switching from your browser password manager(s) to Bitwarden is quick and simple. Instructions for this are at the bottom of the page.
> Take me there!

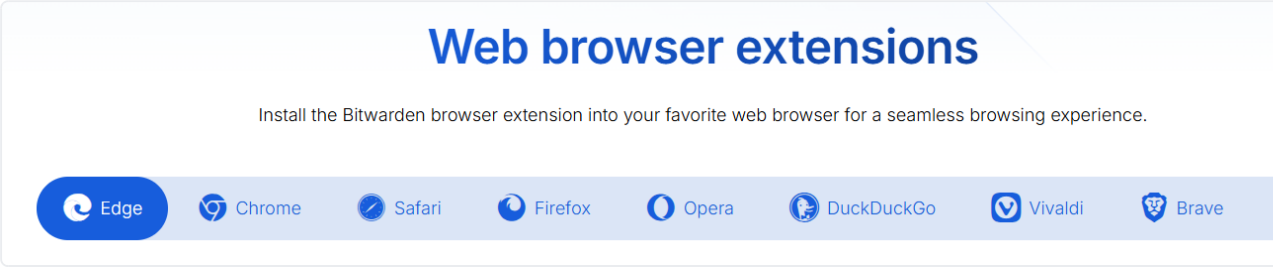
Setup

1. Go to https://bitwarden.com/
2. Click on the **Downloads** tab at the top of the page.

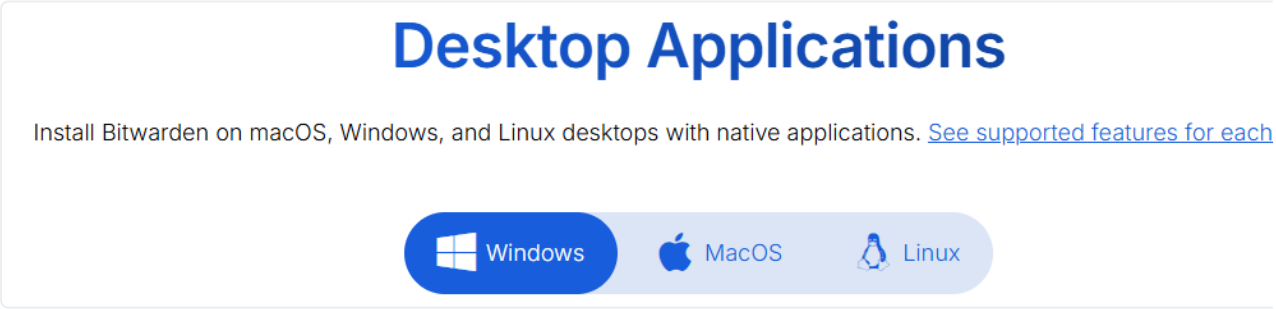


3. Download and install the desired version of Bitwarden (we recommend you start with the desktop application). The available versions are:

a. **Browser extension**—useful for auto-filling usernames and passwords online



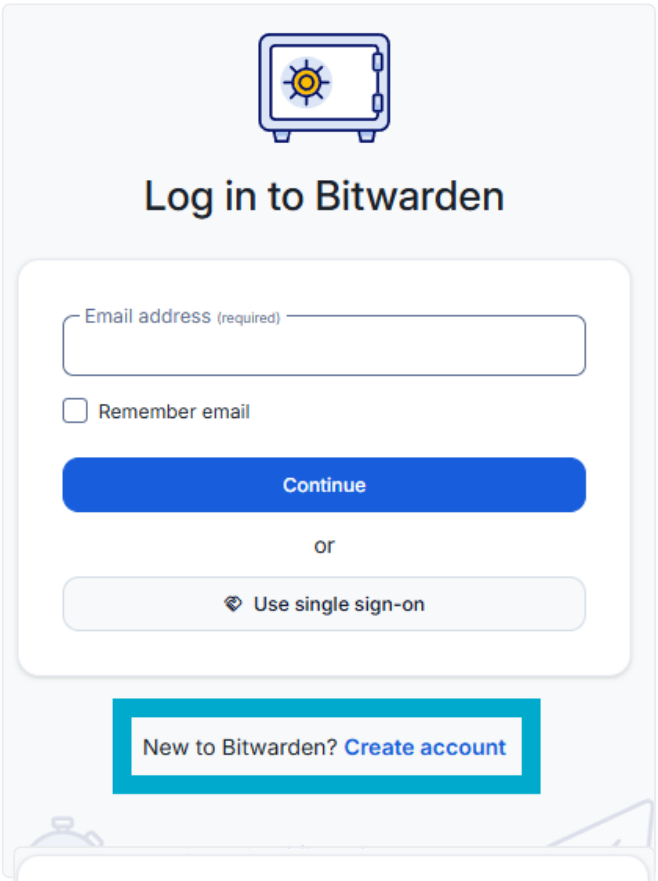
b. **Desktop application**—useful for filling in credentials in non-browser applications faster



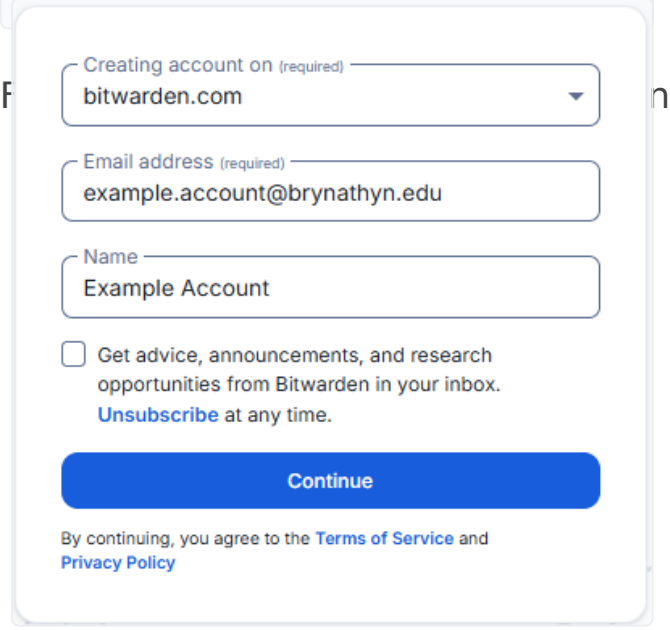
c. Bitwarden is also available as a mobile app for use on the go, as well as being viewable as a normal website.

4. Find and open the version of Bitwarden downloaded.

5. Click on **Create Account**.



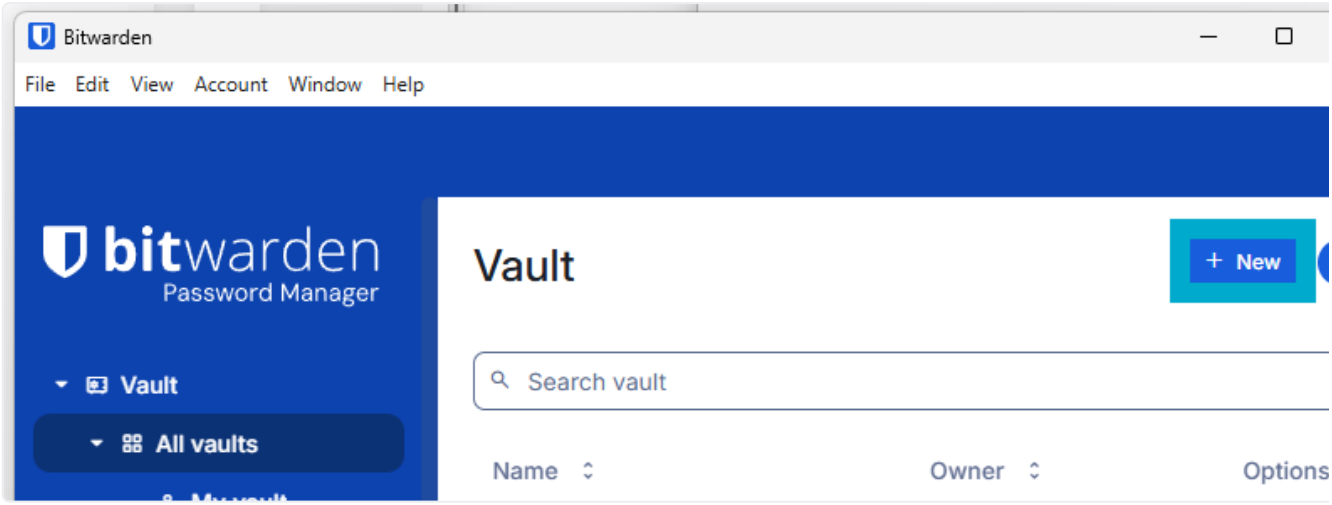
6. F n and click **Continue**.



> If you forget your master password, you will NOT be able to access your vault. Neither the Helpdesk nor Bitwarden support can help you get back into your account.

a. You will now be able to log in on the main page.

7. Once in, click **+ New** to add a new login (desktop application pictured, however this should be evident on all platforms).



8. Store various passwords by filling out the **Name**, **Username**, and **Password** fields.

   a. You can include the URL and any notes related to the account/log in.

   b. You will be able to either right click on the entries or select the clipboard icons next to them when you need to copy/paste your password over.

   c. You can also store things like debit or credit cards and use Bitwarden to securely auto-fill them in various websites or apps.

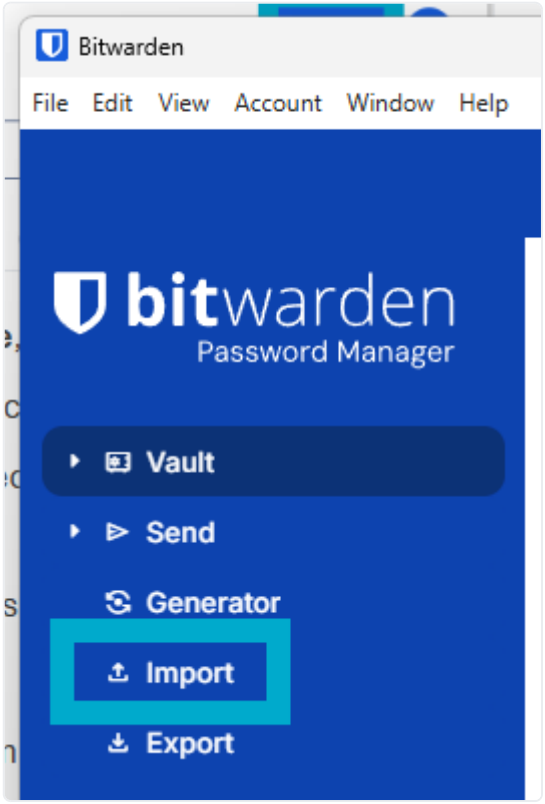
9. Once you have, say, the desktop version installed, we recommend installing the browser extension and mobile app. Once you log in with the account you created, all of your passwords will appear and be accessible just like that.

There are also paid versions of Bitwarden that are available for both individual use and sharing either with one person or family. This can allow you to share passwords and access other premium features like MFA. More details can be found at this link: https://bitwarden.com/pricing/

Transferring your Passwords

Passwords saved in your browser can either be easily exported, then imported into Bitwarden; or even more easily imported straight from Bitwarden (depending on where you want to export them from). To do so:

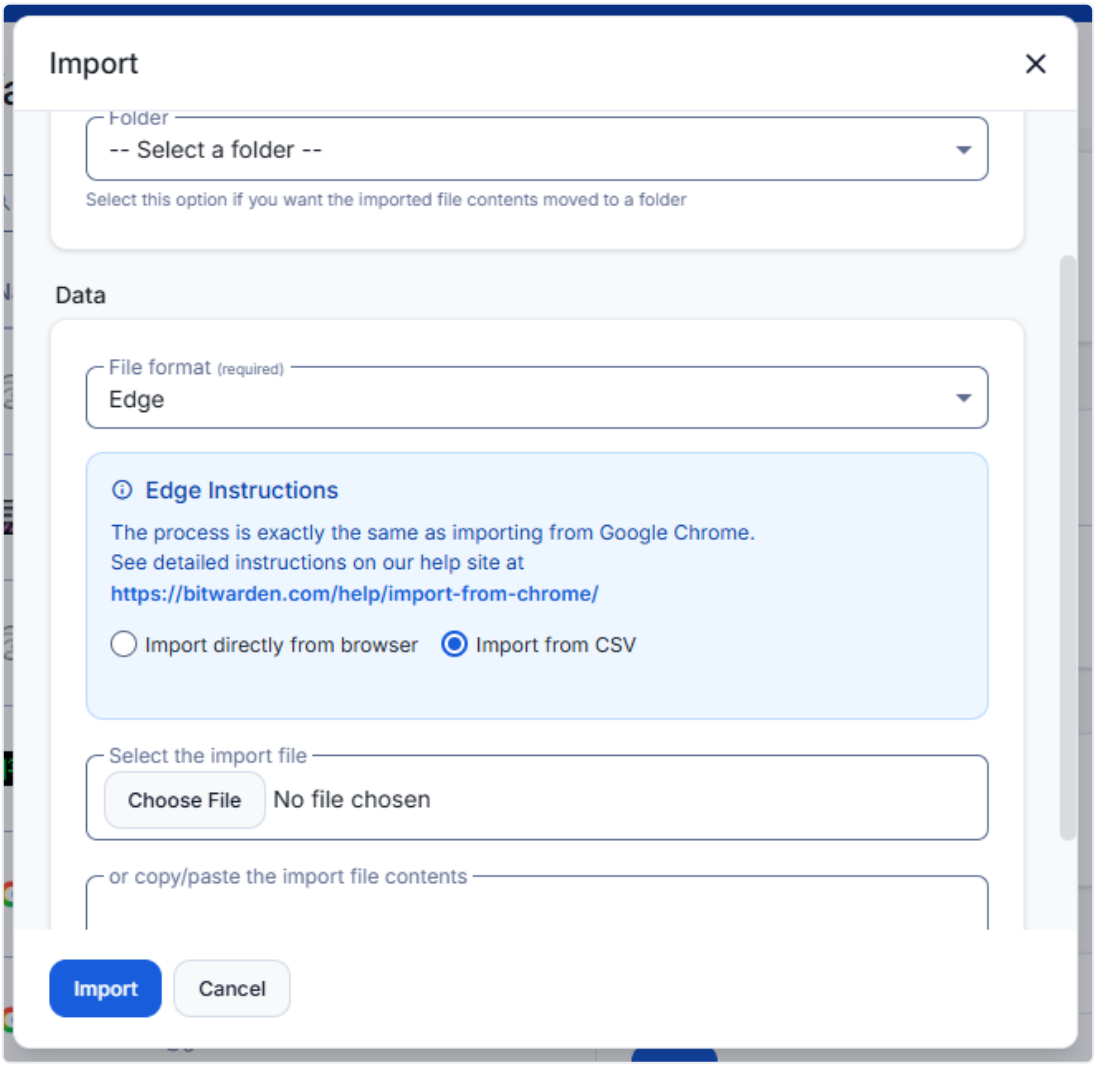
1. In the Bitwarden desktop application, click the **Import** button on the left side of the main screen.



   a. This option should also be available in any version of Bitwarden (browser extension, mobile app, etc.), but instructions provided

here are just for the desktop version.

2. Select a folder for passwords to be imported into if you have one prepared.
3. Under **File format**, select the location of the passwords you exported from.



4. Follow the instructions that appear for the location you selected.
5. Click **Import**.
6. If you have passwords stored in multiple browsers or accounts, repeat for each browser/account you have used.

Congratulations, your passwords are safely and conveniently stored in Bitwarden!