

Bitwarden

Setting up and using the district's Bitwarden password manager.

- [BitWarden Setup Part 1 - Setting Up The BitWarden Password Manager](#)
- [BitWarden Setup Part 2 - Move Your Google Passwords to BitWarden](#)
- [BitWarden Setup Part 3 - Configure Chrome to Use BitWarden Instead of Google Password Manager](#)
- [Bitwarden - Login / Unlock Your Vault](#)

BitWarden Setup Part 1 - Setting Up The BitWarden Password Manager

Good password hygiene is increasingly important in today's cyber landscape. The best method of password use relies on truly unique, complicated, and lengthy passwords. The problem is that, as humans, we can't keep track of 1000 different secure passwords.

Because of this, West Fork Schools now manages a local install of the robust [BitWarden password manager](#).

BitWarden works within your browser (Chrome, Firefox, Safari, and Edge), on your phone, and on your desktop to provide you with a simple password generator and saver.

Create Your Account

Click to show or hide instructions

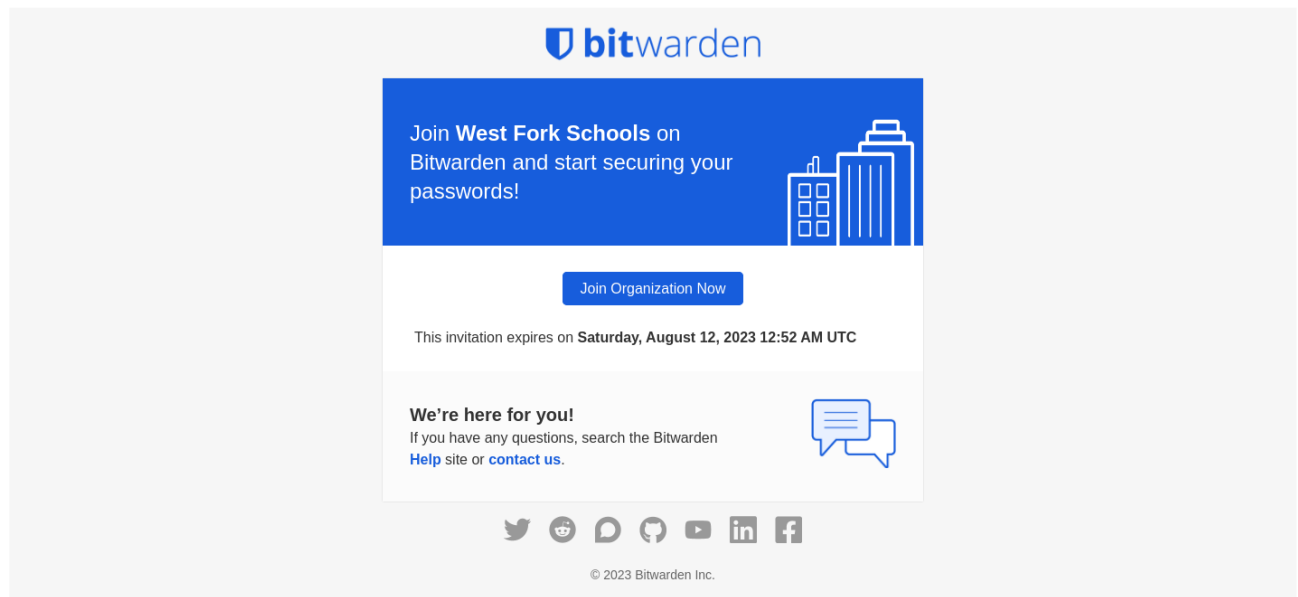
The tech department invites all users to the organization, but you have to create an account to accept the invitation. To get started, check your email (after the initial training or once you have been hired) to find an email from Bitwarden, with the subject “Join West Fork Schools.” It should look something like this:

Join West Fork Schools Inbox x

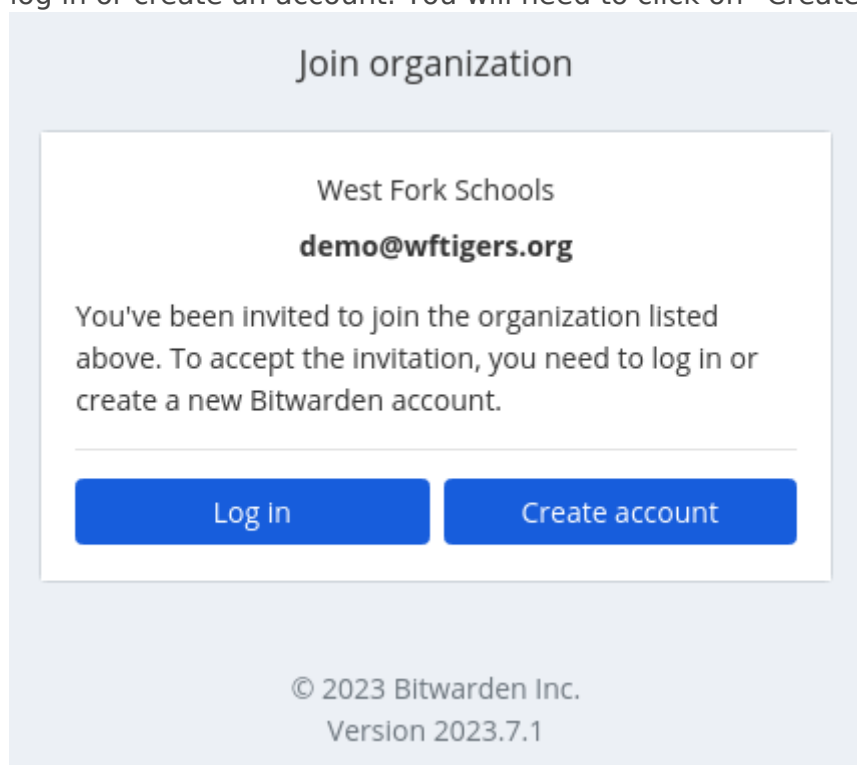


Bitwarden <noreply@wftigers.org>
to me ▾

7:52 PM (1 hour ago) ☆ ↶ ⋮



Once you click on the “Join Organization Now” button, you will be taken to a page asking you to log in or create an account. You will need to click on “Create account” to get started.



On the next page, you will be asked to provide your name and to set a strong “master password.” This password will be the one that unlocks all of your other passwords, so it HAS to

be strong.

Here is a tip for making a super strong password:

- Don't think about a pass**WORD**. Think about a pass**PHRASE**. Pick something that is personal, something you know you won't forget, and something that you know other people won't easily guess.

For example... You may have a soft spot for 80's power ballads (because who doesn't). Perhaps you have to pull over when Journey's "Faithfully" comes on the radio because your air guitar and totally stage-worthy singing on that last chorus are nothing if not a hazard to other drivers.

A great password might be a riff on "I'm forever yours, faithfully." Maybe something like this: 1983I'm forever yours, faithfully!

In addition to setting a master password, You will be asked for a password hint. You don't have to do this, and the tech department will be able to reset your master password if you forget it, but it is always nice to not wait on the ticket time. Notice that I put in a hint (Journey to the Center of the Earth), but it would not be obvious how it relates to my password unless you knew what my password was. This is also a good habit to get into.

Create account

Email address (required)

demo@wftigers.org

You'll use your email address to log in.

Name

Demo Account

What should we call you?

One or more organization policies require your master password to meet the following requirements:

- Minimum complexity score of Strong (4)
- Minimum length of 14
- Contain one or more uppercase characters
- Contain one or more lowercase characters
- Contain one or more numbers
- Contain one or more of the following special characters
!@#\$\$%^&*

Master password (required)

.....

Important: Your master password cannot be recovered if you forget it! 12 character minimum

Strong

Re-type master password (required)

.....

Master password hint

Journey to the Center of the Earth

A master password hint can help you remember your password if you forget it.

☒ Check known data breaches for this password

Create account

Log in

© 2023 Bitwarden Inc.

Version 2023.7.1

Once you have filled out the information, go ahead and click on “Create Account.”

You will be taken to the login screen. You may now put in your email address and click on “Continue.”

 **bitwarden**

Log in or create a new account to access
your secure vault.

Email address (required)

demo@wftigers.org

☐ Remember email

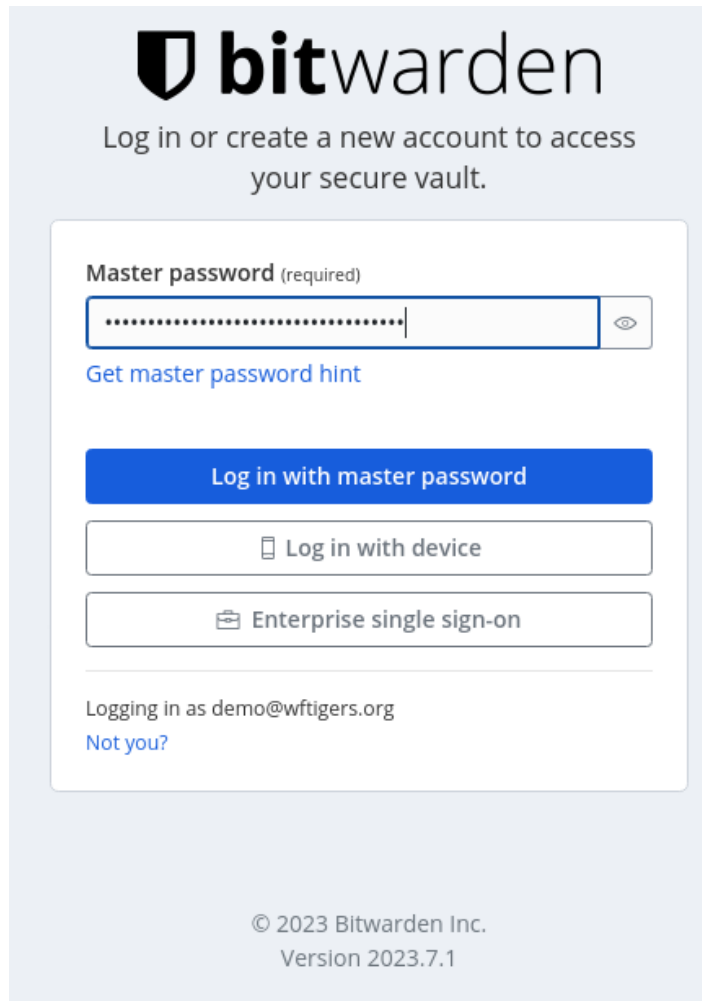
Continue

New around here? [Create account](#)

© 2023 Bitwarden Inc.

Version 2023.7.1

On the next page, enter your master password, then click on the “Log in with master password” button.

The image shows the Bitwarden login interface. At the top is the Bitwarden logo. Below it, the text "Log in or create a new account to access your secure vault." is centered. The main login area is a white box with a light blue border. It contains a "Master password (required)" label above a password input field with a toggle icon. Below the input field is a blue link "Get master password hint". There are three buttons: a blue "Log in with master password" button, a white "Log in with device" button with a device icon, and a white "Enterprise single sign-on" button with a briefcase icon. Below these buttons, it says "Logging in as demo@wftigers.org" with a blue link "Not you?". At the bottom of the page, it says "© 2023 Bitwarden Inc. Version 2023.7.1".

bitwarden

Log in or create a new account to access
your secure vault.

Master password (required)

.....

[Get master password hint](#)

Log in with master password

Log in with device

Enterprise single sign-on

Logging in as demo@wftigers.org
[Not you?](#)

© 2023 Bitwarden Inc.
Version 2023.7.1

Verification and Approval

Click to show or hide instructions

Once you have logged in, you will need to verify your account, and the tech department will have to approve your new account before you have full access.

Verify Your Email

On the Vault Page, There is a box on the right labeled “VERIFY EMAIL.” Go ahead and click the “Send email” button inside of that.

Vaults Send Tools ReportsDA

FILTERS

▼ All vaults

My vault

New organization

▼ All items

Favorites

Login

Card

Identity

Secure note

▼ Folders

No folder

Trash

All vaults

New

☐ All

Name

Owner

There are no items to list.

+ New item

✉ VERIFY EMAIL

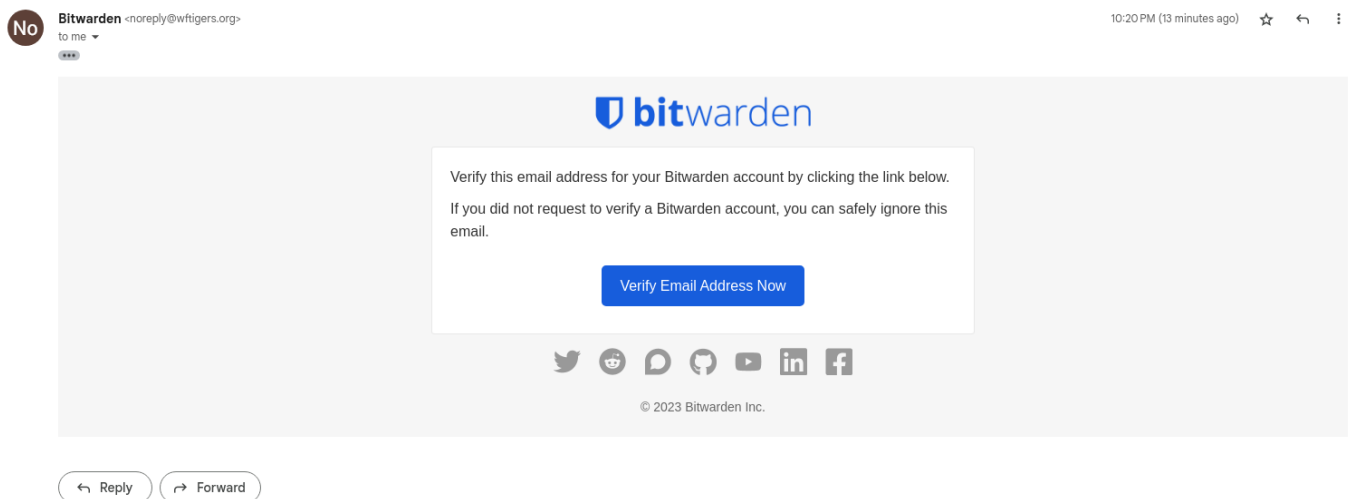
Verify your account's email address to unlock access to all features.

Send email

© 2023 Bitwarden Inc.

Version 2023.7.1

Now, you should go check your school email. There should be two new emails from Bitwarden. The first is a “Welcome to Bitwarden!” message. That one might be worth a read as it has download links for the extensions, but we want the other one for now. The subject should be “Verify Your Email.” It should look like this:

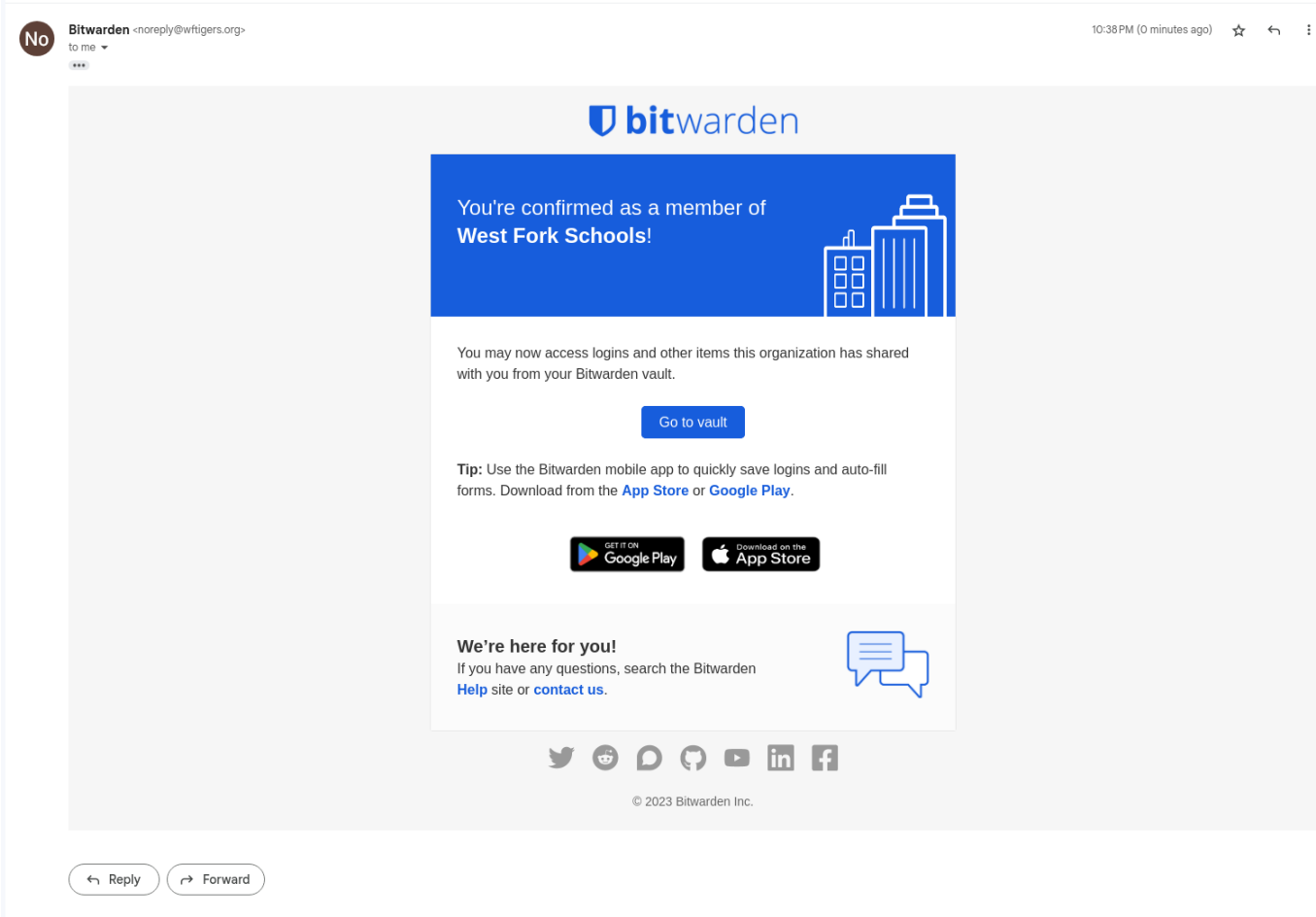


Go ahead and click on the “Verify Email Address Now” button.

You will be taken to the login again. At this point, you are verified, and you may begin using BitWarden for your personal and school password-saving needs. We will release more training on BitWarden in the coming days, but the end of this article will go into setting up your Chrome extension.

Account is Now Pending Approval

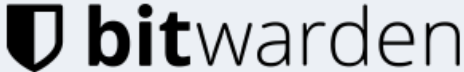
While the basic functions of BitWarden are now active, you must wait for the tech department to manually approve your account before you gain full access to the West Fork Schools organization. This organization will have specific capabilities depending on who you are. More information will be coming soon, but, for now, just wait for the email letting you know that you have been approved. It looks something like this:



Once this happens, you will be able to log in with full permissions.

LOGIN IS DIFFERENT ONCE APPROVED

Once you are approved, you will be required to use the “Enterprise single sign-on” at any point you see the button available. This means that BitWarden will verify your identity by also using your Google account and any two-factor authentication that is tied to it. This might seem annoying, but when you stop to think about the student, personal, financial, and institutional data that will be stored in this manager, one extra login a day isn’t that big of a deal.



Log in or create a new account to access your secure vault.

Master password (required)

ⓧ Input is required.

[Get master password hint](#)

Log in with master password

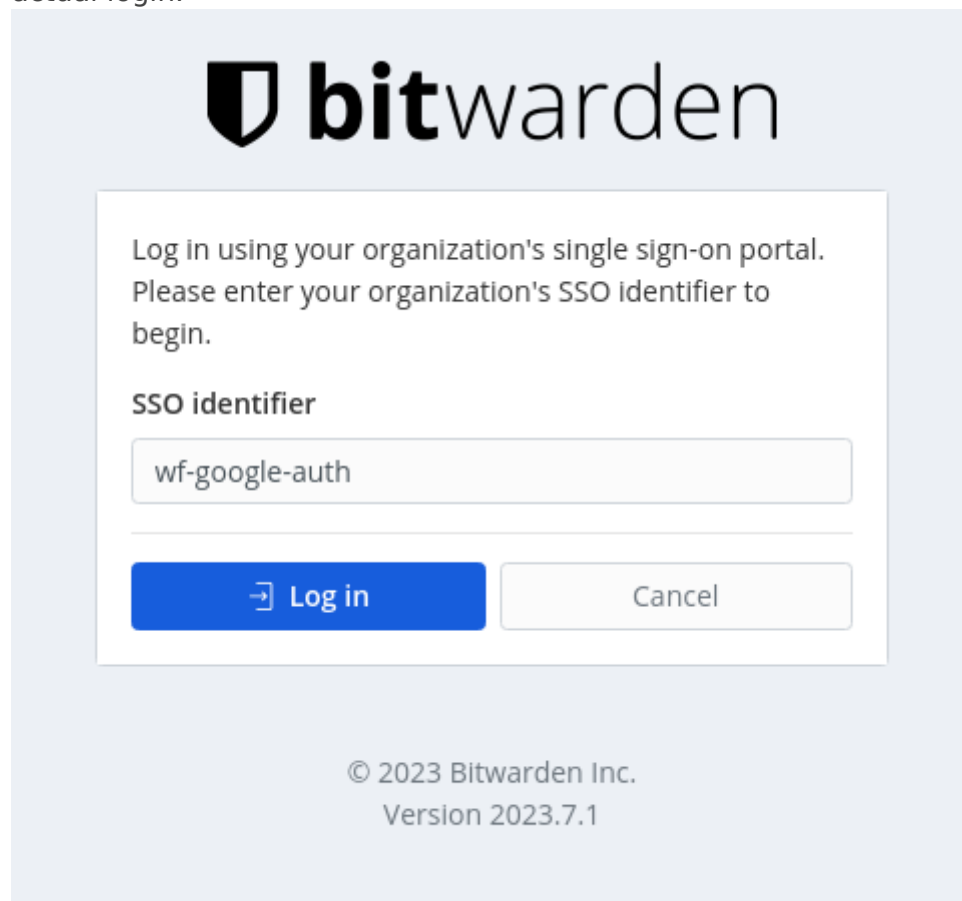
Log in with device

Enterprise single sign-on

Logging in as demo@wftigers.org
[Not you?](#)

© 2023 Bitwarden Inc.
Version 2023.7.1

Also, we added a “BitWarden Password Vault” option to the WF Bookmarks menu. That will take you directly to a page with a “Log in” button. Clicking that button directs you to Google for your actual login.

The image shows a Bitwarden login interface. At the top is the Bitwarden logo, which consists of a shield icon followed by the word "bitwarden" in a lowercase, sans-serif font. Below the logo is a white rectangular box containing the login instructions: "Log in using your organization's single sign-on portal. Please enter your organization's SSO identifier to begin." Underneath this text is a label "SSO identifier" followed by a text input field containing the value "wf-google-auth". Below the input field are two buttons: a blue button with a right-pointing arrow icon and the text "Log in", and a white button with a gray border and the text "Cancel". At the bottom of the interface, centered, is the copyright notice "© 2023 Bitwarden Inc." and the version number "Version 2023.7.1".

bitwarden

Log in using your organization's single sign-on portal.
Please enter your organization's SSO identifier to begin.

SSO identifier

wf-google-auth

 Log in

Cancel

© 2023 Bitwarden Inc.
Version 2023.7.1

After you click the “Enterprise Single Sign-On” button (or use the link in WF Bookmarks), you will be prompted for your master password, so I don’t even bother typing that is the page, otherwise, you will have to type it twice.



Your vault is locked. Verify your master password to continue.

Master password



Logged in as demo@wftigers.org on bw.wftigers.org.

Unlock

Log out

© 2023 Bitwarden Inc.
Version 2023.7.1

Once you unlock your account with your master password, you will be greeted with your vault again.

Vaults

Send

Tools

Reports

DA

FILTERS

Search vault

▼ All vaults

My vault

West Fork Schools

+ New organization

▼ All items

☆ Favorites

Login

Card

Identity

Secure note

▼ Folders

No folder

▼ Collections

Technology Depart...

Trash

All vaults

New

All

Name

Owner

BitWarden - Service Account

bitwarden

West Fork ...

This shows the school's password vault

This shows any passwords you have access to, even if they were added by someone else in your groups.

© 2023 Bitwarden Inc.

Version 2023.7.1

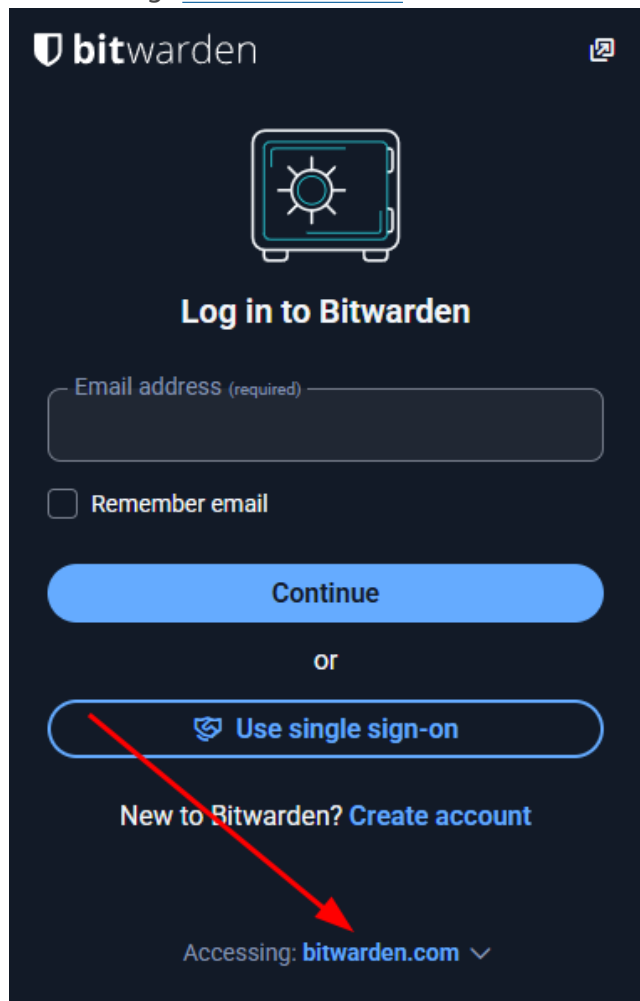
The Chrome App

Click to show or hide instructions

The good news is that we already pushed the extension to all Chrome browsers with sync enabled. Woot!

The better news is that you can also install it on unmanaged Chrome browsers (and pretty much every other browser). [This page has download links for desktop clients, web browsers, and phones.](#)

Once you have the extension installed, you will be presented with a login screen. But wait!!! Before you type in your email, there is a setting you need to change. Click where it says "Accessing: bitwarden.com" as shown in the screenshot.



You need to change this to Self-hosted. That will bring up a window, and in the top box, labeled "Server URL," type in:

`https://bw.wftigers.org`

Close

Bitwarden

Save

SELF-HOSTED ENVIRONMENT

Server URL

https://bw.wftigers.org

Specify the base URL of your on-premises hosted Bitwarden installation.

CUSTOM ENVIRONMENT

Web vault server URL

API server URL

Identity server URL

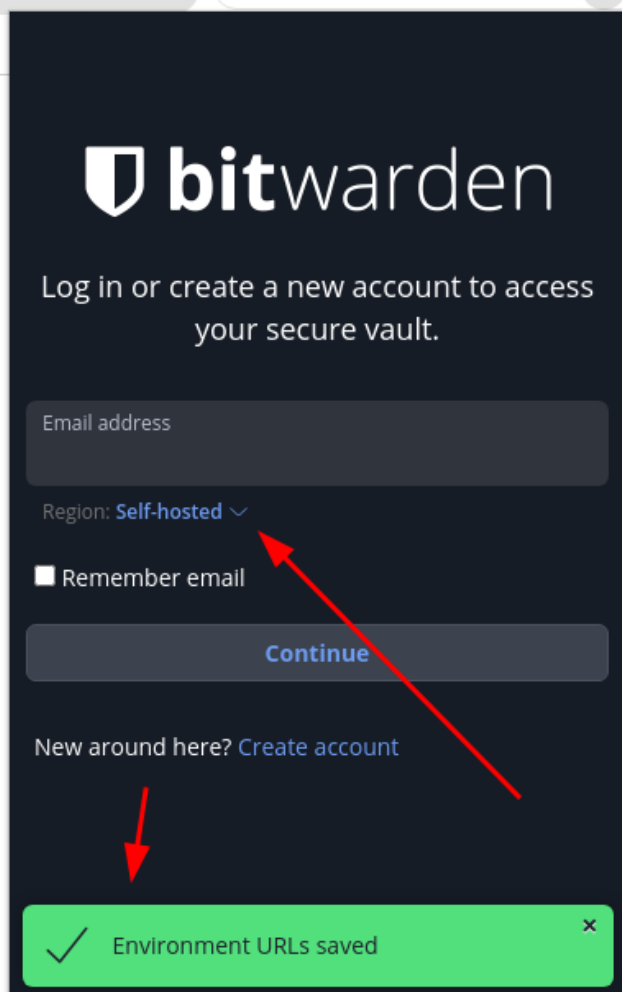
Notifications server URL

Icons server URL

For advanced users. You can specify the base URL of each service independently.

Then click on Save at the top.

You should then get a green confirmation notice at the bottom, and it should say Self-hosted under the email address box.



The image shows the Bitwarden login interface. At the top is the Bitwarden logo. Below it, the text "Log in or create a new account to access your secure vault." is displayed. There is an "Email address" input field. Below the input field, the text "Region: Self-hosted" is shown with a dropdown arrow. A checkbox labeled "Remember email" is present. A "Continue" button is located below the checkbox. At the bottom of the main form area, the text "New around here? Create account" is displayed. At the very bottom of the screen, there is a green confirmation message that says "✓ Environment URLs saved" with a close button (x) on the right. Two red arrows are pointing to the "Self-hosted" text and the green confirmation message.

bitwarden

Log in or create a new account to access
your secure vault.

Email address

Region: Self-hosted

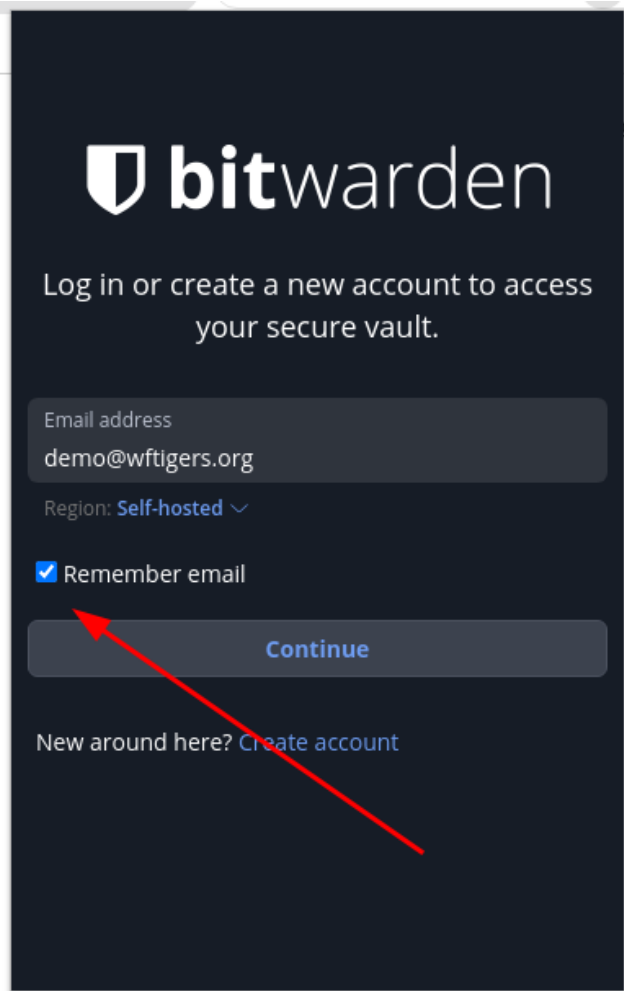
☐ Remember email

Continue

New around here? [Create account](#)

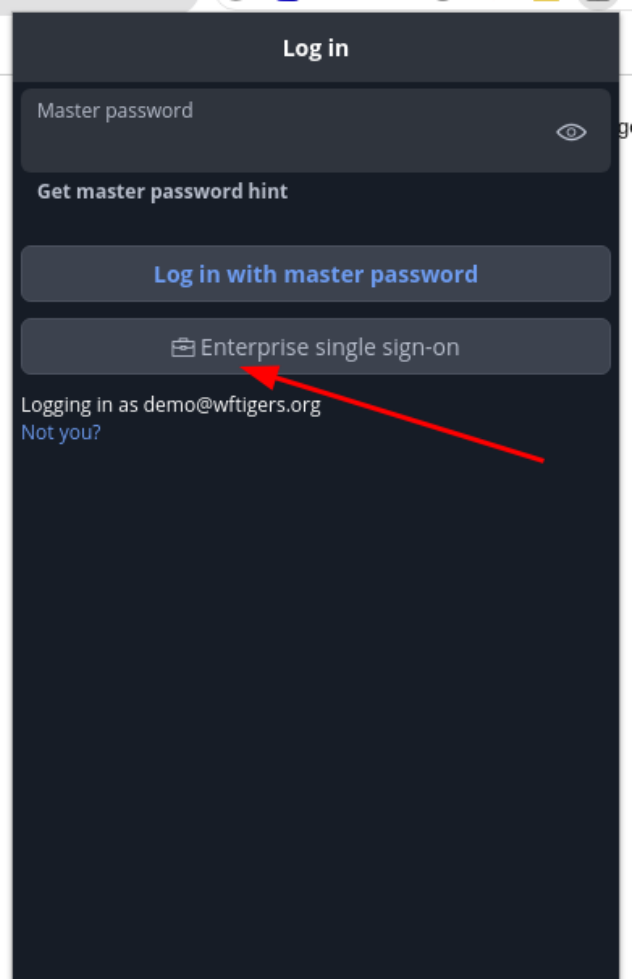
✓ Environment URLs saved

Now go ahead and type in your email address! I also click the “Remember email” checkbox.

A screenshot of the Bitwarden login interface. The background is dark blue. At the top, the Bitwarden logo (a shield icon) and the text "bitwarden" are displayed in white. Below the logo, the text "Log in or create a new account to access your secure vault." is centered in white. Underneath, there is a light gray input field for the email address, containing the text "demo@wftigers.org". Below the email field, the text "Region: Self-hosted" is shown with a small downward arrow. A blue checkbox labeled "Remember email" is checked. Below the checkbox is a blue button with the text "Continue". At the bottom, the text "New around here? Create account" is displayed, with "Create account" as a link. A red arrow points from the bottom right towards the "Continue" button.

Then click on Continue.

On the next page, if you have been approved by tech, you need to click on the “Enterprise single sign-on” button. That will take you to a Google page (unless you are already logged in). Complete the Google authentication and any two-factor that is required.

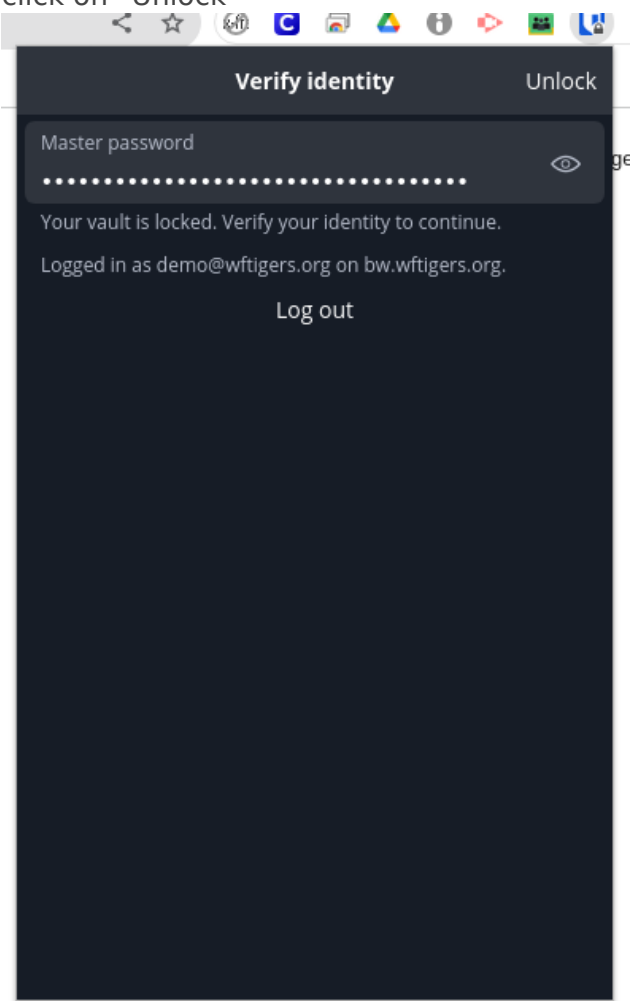


You will then get this screen:

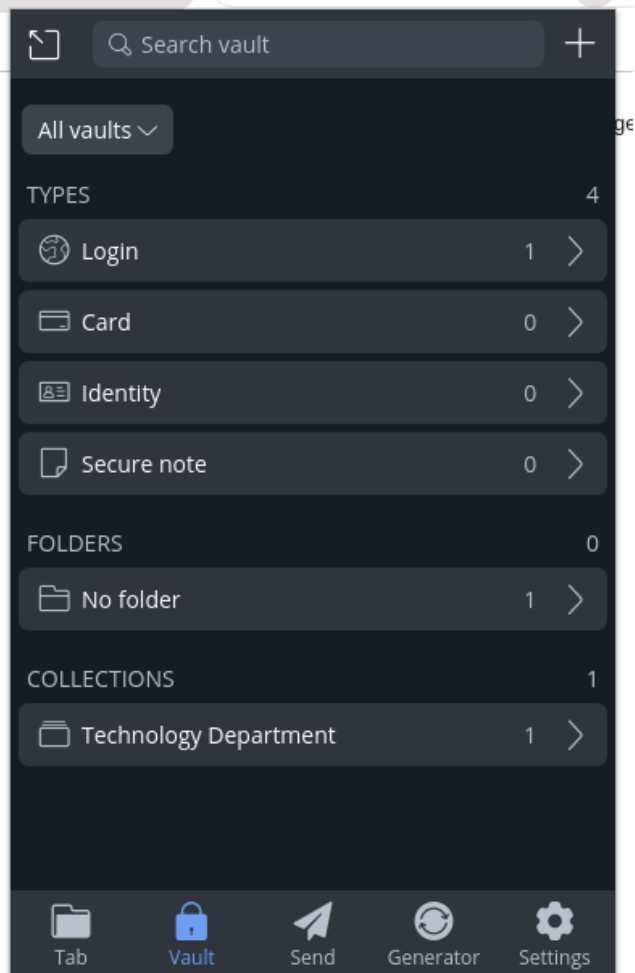


You may now close this tab and continue in the extension.

This just means you may now open the extension, and then type in your master password, and click on “Unlock”



You will now be presented with your Bitwarden vault and other options.



FAQ

Do I have to do this WHOLE login process every time?!?!

You don't have to do the whole login routine on the extension every time. You will sometimes have to refresh the Google login, but, for the most part, you will only be asked to type in your master password when you start Chrome for the first time each day. This setup just ensures that other people will have a MUCH more difficult time getting the information that is stored within BitWarden.

As for the web vault, as long as you use the WF Bookmarks menu item, the same rules apply. ☐☐

Is this BitWarden thing safe?

Short answer: INCREDIBLY!

Longer answer: Bitwarden, by default, if you just used the free version available to the public, is HIGHLY secure. The company routinely submits its code to third-party security agencies for review and correction, PLUS, their code is open source, meaning that everyone in the world can read every line of the code, suggest security fixes, and generally make the security even better.

To go further, we are using a self-hosted version, meaning that your password management will never touch the public version of the service. We get the same level of code security with the added security of being isolated.

Yeah, but what about all of my banking info? I don't want the tech department to have that!

That is totally valid! Here is the super great news... We can't see your passwords (unless you specifically share them with a group we are in)! We can't even tell how many passwords you have in the system.

The truly beautiful thing about how Bitwarden works is that all of the fancy security stuff happens on YOUR end, meaning inside of the browser or on the phone you are using when you save or use a saved password. When it gets to the server, it is HEAVILY encrypted, to the point that the server and anyone with access to it (like the tech department or any malicious hackers) can't tell what is going on. To crack your password, the person would also have to know your Master Password. That is why that password is SO IMPORTANT!

So... I can put my banking info in there?

That is totally up to you! Obviously, there is a personal level of comfort that you need to have, but, as far as the safety of your data goes, Bitwarden is going to be a safe way for you to store that.

You are permitted to store credit card information, personal passwords, and secure notes in your vault. Just use good judgment, and consider exporting your vault every now and again in the event the server crashes.

What if the server DOES crash?

Well... While full-on server crashes are rare, they do happen. This is another place where Bitwarden is super helpful. There are automated nightly backups built into the system. The tech department will be taking these backups, and they will be moved to a dedicated Google Shared

Drive as well as a local storage server. In the event of a data crash, we should be able to get the backups recovered in a couple of hours with very little (if any) data loss. The only potential data loss would be passwords/info saved between the backup and the crash.

What makes BitWarden better than the Google Password Manager?

Look... We know that Google's password manager is handy. Really. We get it. The problem is that it is so deeply tied to Google Chrome and your account. If someone gets access to your Google account, they also get access to EVERYTHING stored in the Google password manager, including any credit cards, passwords, whatever...

BitWarden doesn't rely specifically on your Google account. In fact, it is only using your Google account as a THIRD layer of authentication. That means for someone to gain access to your BitWarden account, they have to be able to know your Google account info, defeat your two-factor, AND know your BitWarden master password. That is an awful lot of hacking required.

Is there ANY chance my information can be stolen?

We will be honest here. Absolutely! That said, most of those possibilities are totally avoidable. The weakest point of this chain is having a poor master password. We have required specific rules be met to help combat this, but it ultimately comes down to you putting in the work to think of a strong pass**PHRASE**.

Furthermore, hackers are not just weird kids in their mom's basement anymore. Some hackers are among the wealthiest people in the world, and they got that way because they are really good at their job (hacking). Again, BitWarden submits to regular security audits, and their code is available to the world, but there are other ways for hackers to get into those systems. We won't go into details (unless you ask), but IF you fell for a phishing campaign or were otherwise infected with malware, it is possible that there would be systems running on your computer that track what you are typing. In that case, your master password could be compromised. Also though, in that case, we would be relying on Google's security and the two-factor authentication layer to further protect.

The simple answer is that, while it is SUPER unlikely that your data will ever be able to be taken from BitWarden without your consent, it isn't a 0% chance.

Also, to be clear, that answer is sort of a general one. There is no such thing as 100% online safety.

[Proceed to Part 2 to move your passwords over.](#)

BitWarden Setup Part 2 - Move Your Google Passwords to BitWarden

This is part 2 of our Bitwarden setup series.

[Check out Part 1](#)

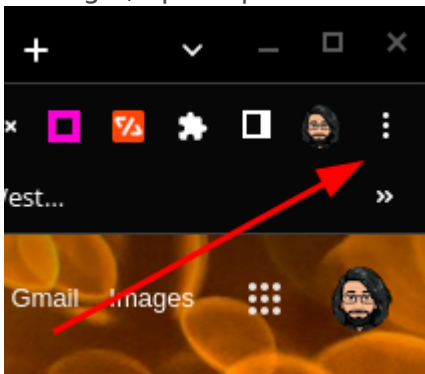
Once you have set up your BitWarden account, you will probably want to move your existing passwords into it.

Luckily, this is super simple.

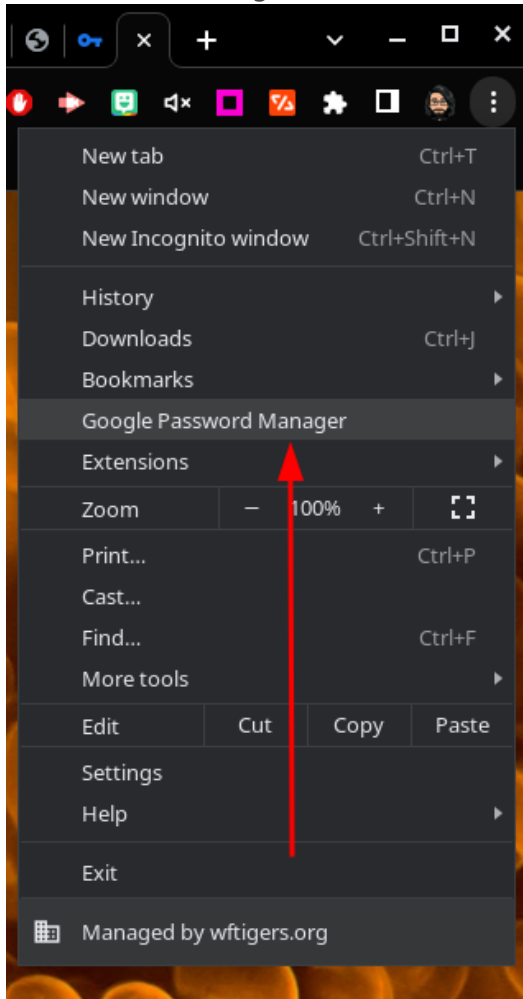
Step 1: Export Your Google Passwords

Click for instructions on exporting your Google Passwords

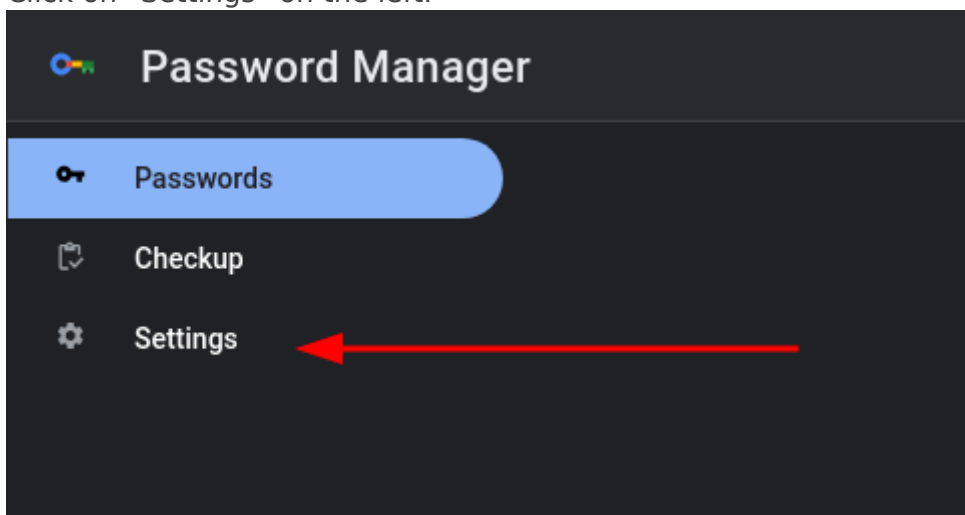
- To begin, open up a chrome window, and click on the three vertical dots menu.



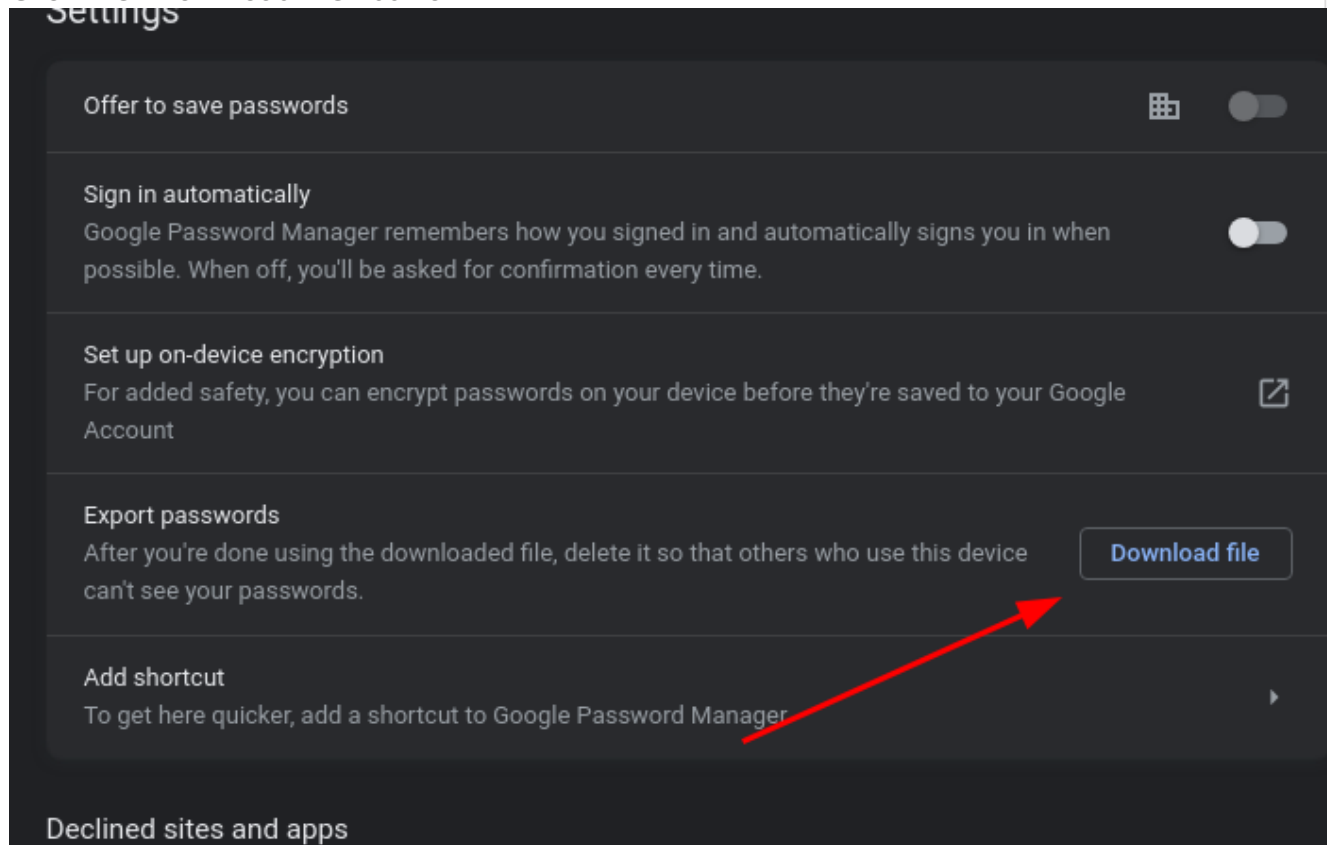
- Click on the “Google Password Manager” option.



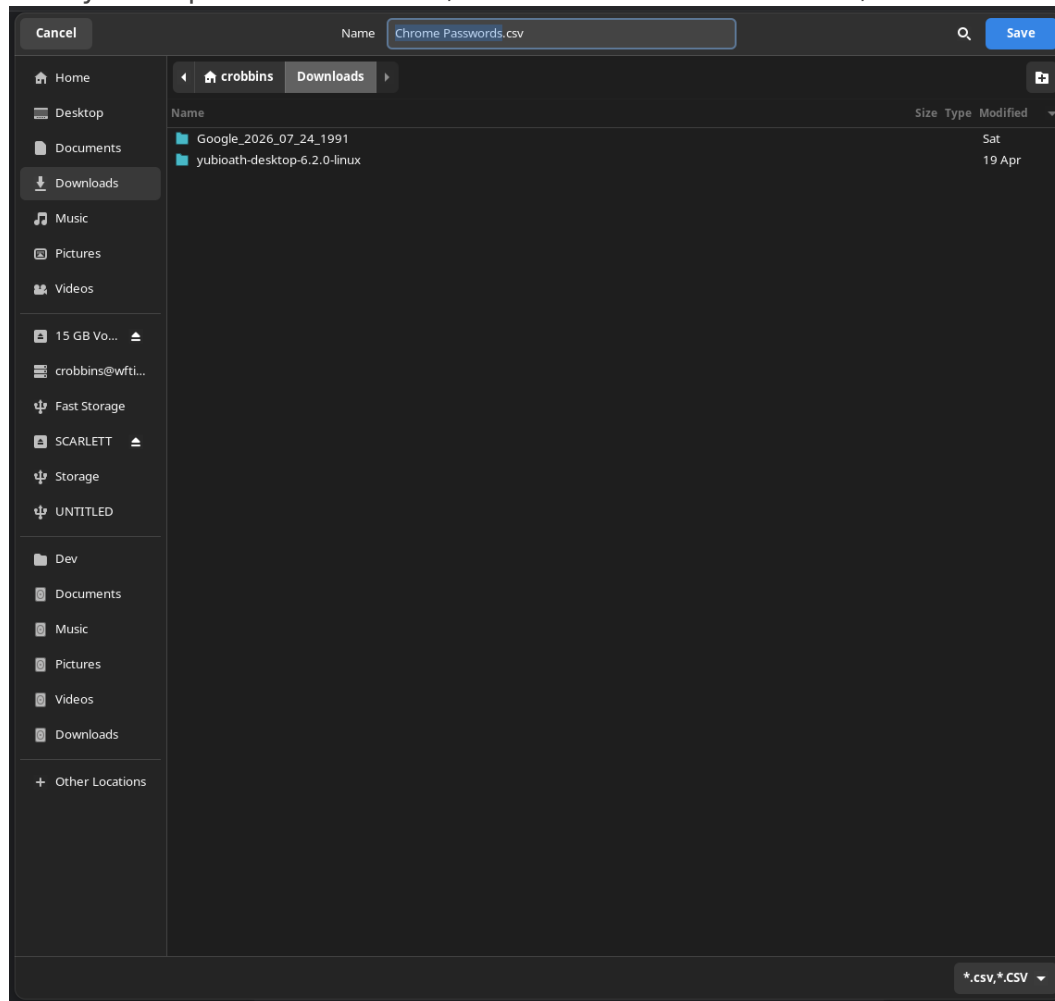
- Click on “Settings” on the left.



- Click the “Download file” button



- Give your exported file a name, and choose where to save it, then click on “Save.”



Step 2: Import Passwords to BitWarden

Click for instructions on importing passwords to BitWarden

- [Log in to BitWarden \(click this link to be taken there directly, or use the WF Bookmarks link.](#)

- Click on the “Tools” menu.

The screenshot shows the Bitwarden web interface. At the top is a dark blue navigation bar with the Bitwarden logo and four menu items: 'Vaults', 'Send', 'Tools', and 'Reports'. A red arrow points to the 'Tools' menu item. Below the navigation bar, the main content area is titled 'All vaults' and includes a 'New' button in the top right corner. On the left side of the main content area is a 'FILTERS' sidebar. This sidebar contains a search bar labeled 'Search vault' and two sections of filters. The first section, 'All vaults', includes 'My vault', 'West Fork Schools' (with a three-dot menu icon), and 'New organization'. The second section, 'All items', includes 'Favorites', 'Login', 'Card', 'Identity', 'Secure note', 'Folders', 'No folder', 'Collections', 'Technology Depart...', and 'Trash'. The main content area displays a table with columns for selection, name, and owner. The table has one row for a vault named 'BitWarden - Service Account' (with a sub-label 'bitwarden') owned by 'West Fork ...'. The table is currently empty except for this one entry.

	Name	Owner
☐	BitWarden - Service Account bitwarden	West Fork ...

- Click on “Import data.”

TOOLS

- Generator
- Import data
- Export vault

Generator

One or more organization policies are affecting your generator settings.

q9%9&TjgV9%N&9

What would you like to generate?

☒ Password ☐ Username

Password type

☒ Password ☐ Passphrase

Length: 14

Minimum numbers: 4

Minimum special: 4

Options

- ☒ A-Z
- ☒ a-z
- ☒ 0-9
- ☒ !@#%&^&*
- ☒ Avoid ambiguous characters

Regenerate password Copy password

© 2023 Bitwarden Inc.

Version 2023.7.1

- From the “Select the format of the import file” dropdown menu, choose “Chrome (csv)”

Import data

1. Select the format of the import file (required)

Chrome (csv)

- Click on “Choose File,” and then choose the file you downloaded from chrome in the previous step. You should see the name of the file to the right of the button once you do this successfully.

2. Select the import file

Choose File Chrome Passwords.csv

- Click on the “Import data” button.

TOOLS

- Generator
- Import data**
- Export vault

Import data

1. Select the format of the import file (required)

Chrome (csv)

CHROME (CSV) INSTRUCTIONS

See detailed instructions on our help site at <https://bitwarden.com/help/import-from-chrome/>

2. Select the import file

[Choose File](#) Chrome Passwords.csv

or copy/paste the import file contents

[Import data](#)

© 2023 Bitwarden Inc.

Version 2023

- You will get a verification page stating how many items were imported. Clicking OK will show you your new password vault.

DATA SUCCESSFULLY IMPORTED

A total of 192 items were imported.

Type	Total
Login	192

[Ok](#)

[Proceed to Part 3 and configure chrome.](#)

Originally posted by Cory Robbins on the West Fork Technology Hub (2023-08-11).

BitWarden Setup Part 3 - Configure Chrome to Use BitWarden Instead of Google Password Manager

This is part 2 of our Bitwarden setup series.

[Check out Part 1](#)

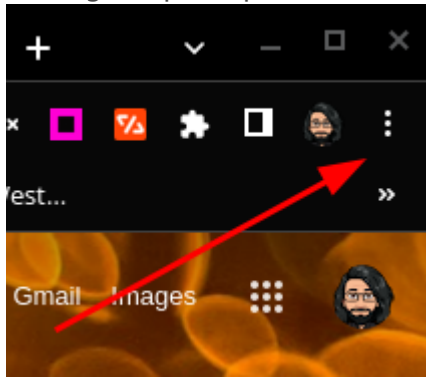
[Check out Part 2](#)

In this part of the BitWarden setup, we will turn off the automatic password save prompts for Google Password Manager and configure the BitWarden extension settings.

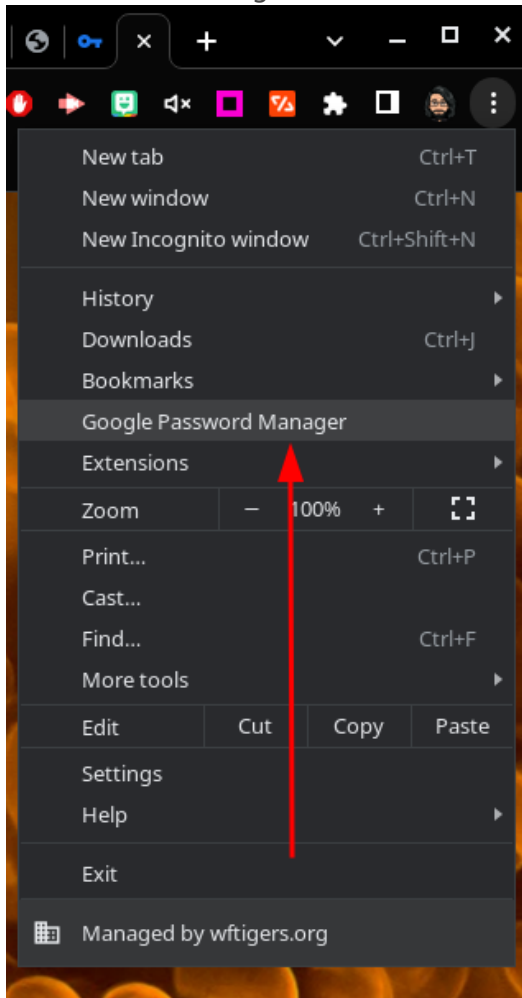
Step 1: Turn off Google Password Manager save prompts.

[Click here for instructions](#)

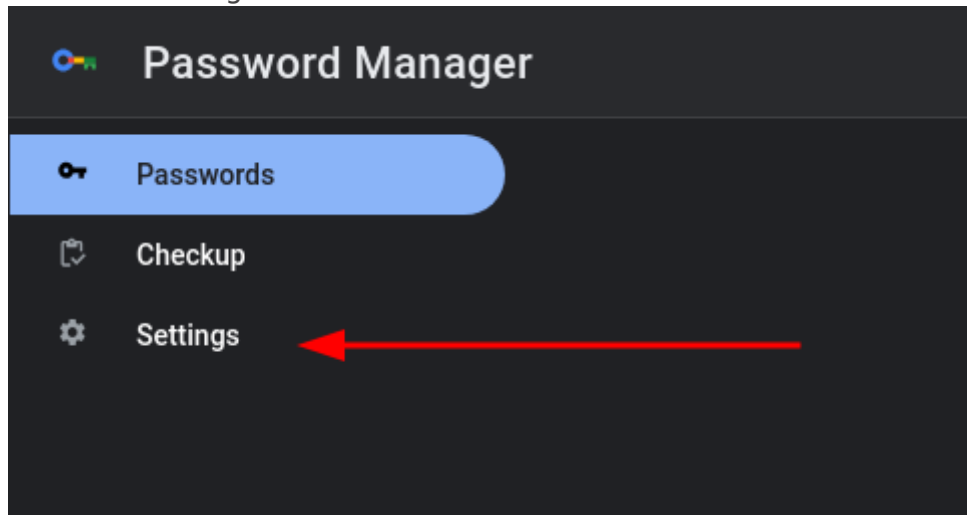
- To begin, open up a chrome window, and click on the three vertical dots menu.



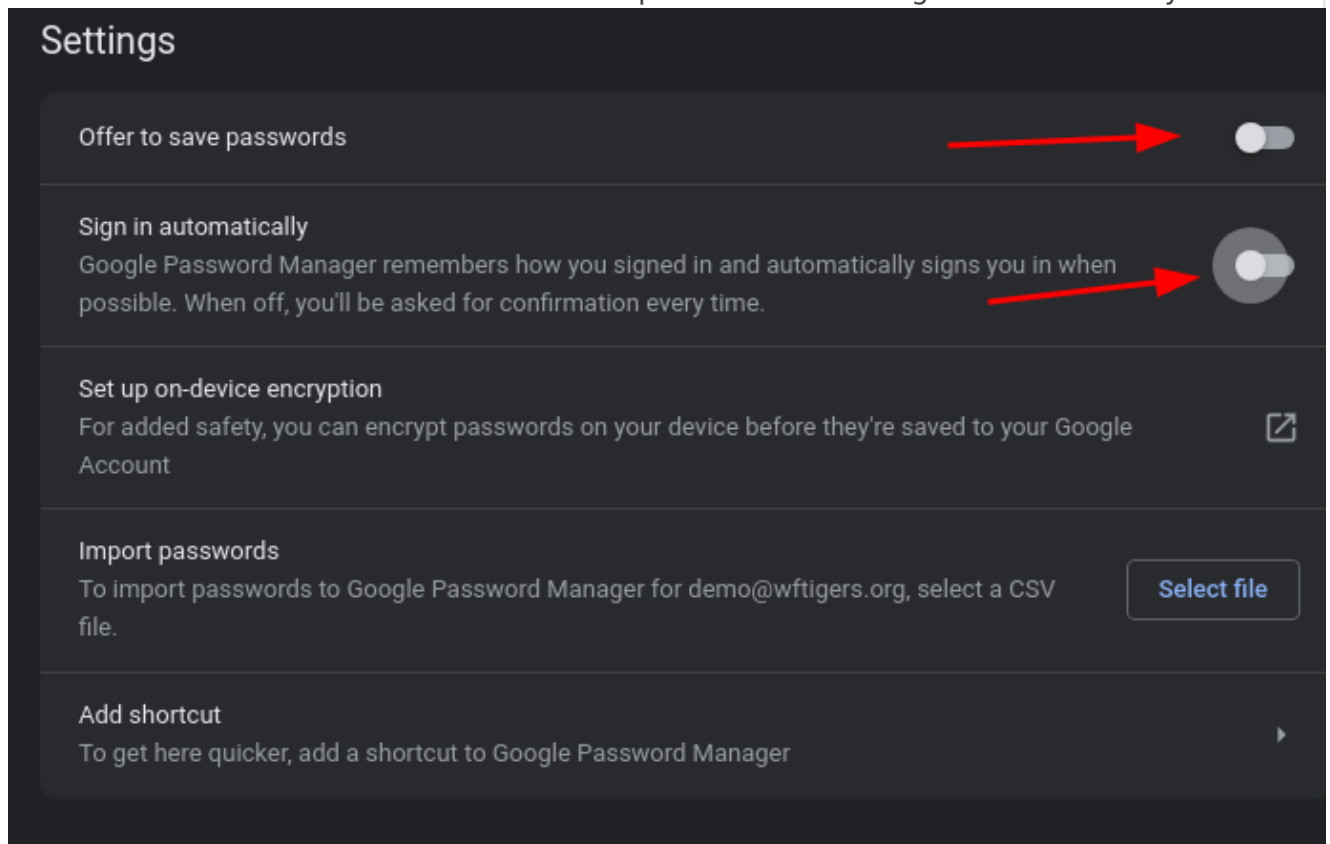
- Click on the "Google Password Manager" option.



- Click on “Settings” on the left.



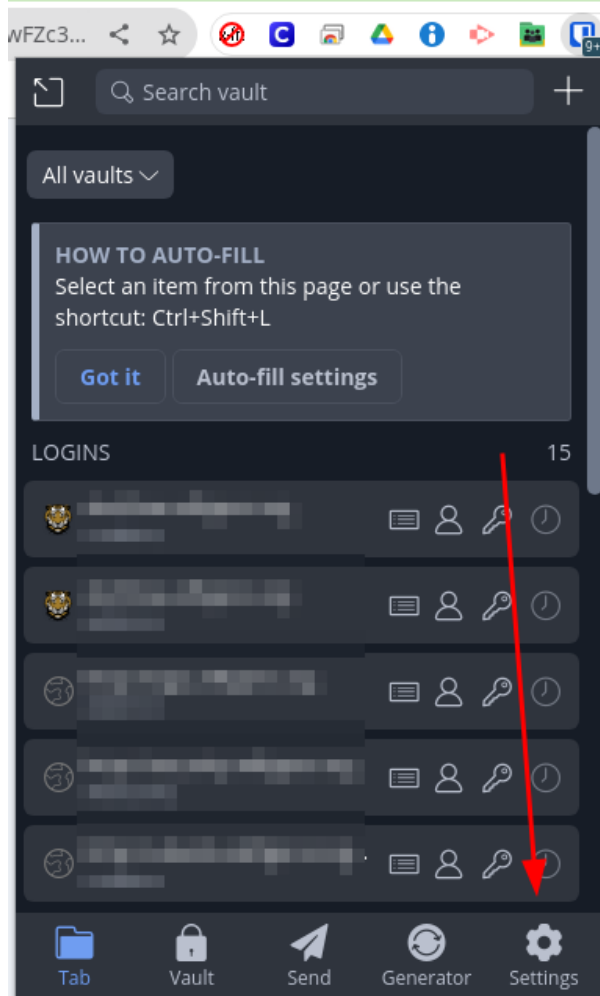
- Turn off the switches for both “Offer to save passwords” and “Sign in automatically.”



Step 2: BitWarden Extension Settings

Click here for recommended settings

- Open the BitWarden extension, and Click on the “Settings” gear



- Auto-fill
 - Auto-fill on page load
 - This is probably something most of you will want to turn on, but it is worth paying attention to the warning.
 - Default autofill setting for login items
 - If you enable auto-fill, you can also choose to disable auto-fill for new passwords you add. You will probably want to keep this as the default, “Auto-fill on page load,” but it is worth remembering that you CAN still disable auto-fill on websites you don’t want to risk being compromised.
- Vault timeout
 - The default on this option is “On browser restart,” meaning that each time you fully close chrome and open it again, you will be asked to unlock your vault. This is ok, but for added security, it would be better to set this to “On system lock.”

There isn’t a save button. Once you make the changes, they will just work.

Please note, you will likely have to change these settings on each device you use the BitWarden password manager.

Originally posted by Cory Robbins on the West Fork Technology Hub (2023-08-11).

Bitwarden - Login / Unlock Your Vault

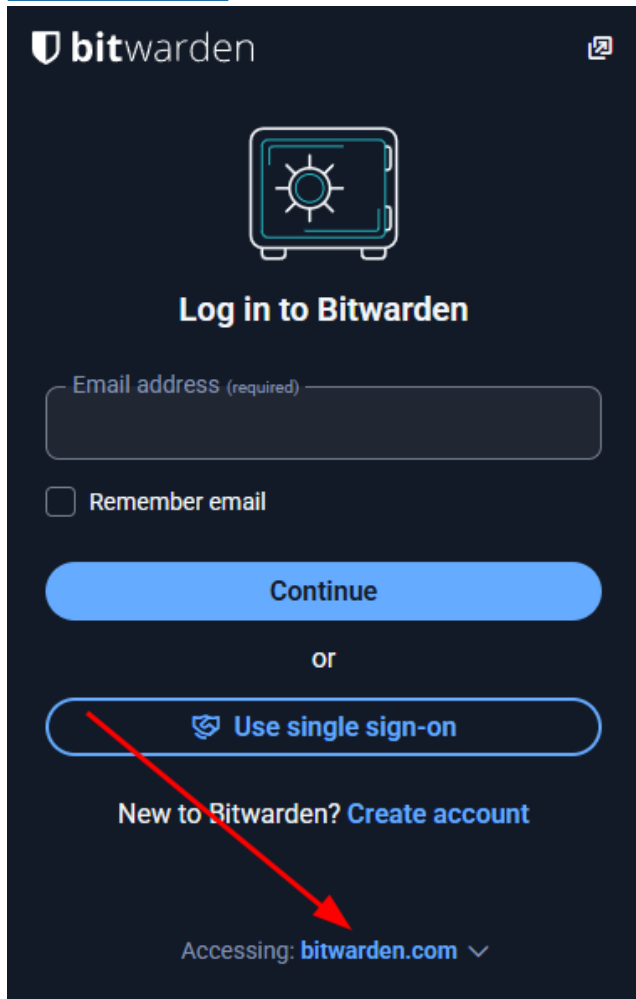
This article assumes you've set up the Bitwarden password manager based on our setup guides. If you have not set up Bitwarden, then you should check out [Part 1](#) of the walkthrough. Also, the extension for bitwarden will be used throughout this article. The setup for the extension is explained in the Part 1 guide under the section "[The Chrome App.](#)"

Click to show or hide instructions

The good news is that we already pushed the extension to all Chrome browsers with sync enabled. Woot!

The better news is that you can also install it on unmanaged Chrome browsers (and pretty much every other browser). [This page has download links for desktop clients, web browsers, and phones.](#)

Once you have the extension installed, you will be presented with a login screen. But wait!!! Before you type in your email, there is a setting you need to change. Click where it says “Accessing: bitwardent.com” as shown in the screenshot.



You need to change this to Self-hosted. That will bring up a window, and in the top box, labeled “Server URL,” type in:

`https://bw.wftigers.org`

Close

Bitwarden

Save

SELF-HOSTED ENVIRONMENT

Server URL

https://bw.wftigers.org

Specify the base URL of your on-premises hosted Bitwarden installation.

CUSTOM ENVIRONMENT

Web vault server URL

API server URL

Identity server URL

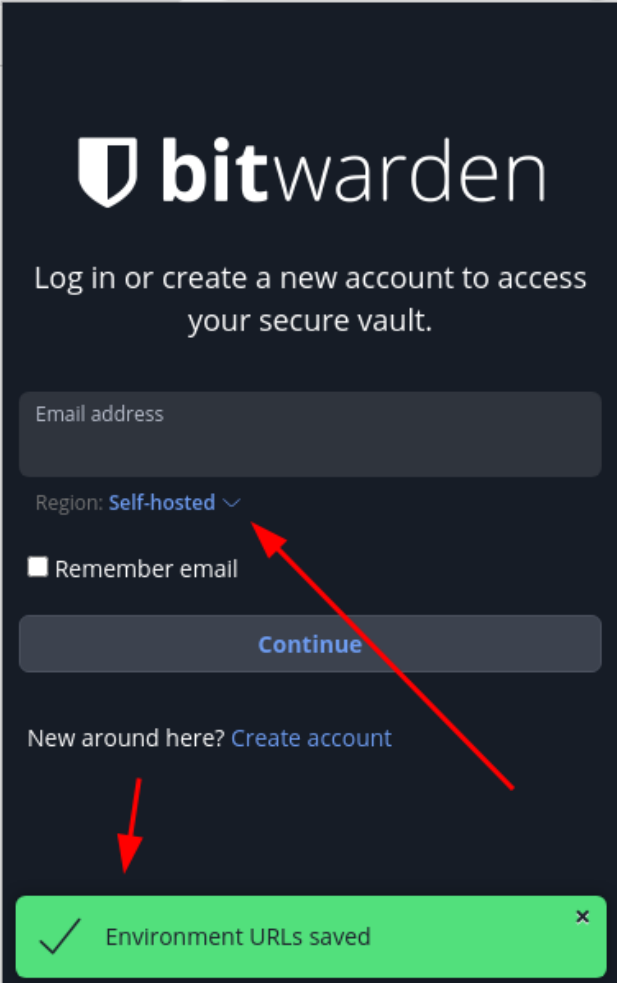
Notifications server URL

Icons server URL

For advanced users. You can specify the base URL of each service independently.

Then click on Save at the top.

You should then get a green confirmation notice at the bottom, and it should say Self-hosted under the email address box.



The image shows the Bitwarden login interface. At the top is the Bitwarden logo. Below it is the text "Log in or create a new account to access your secure vault." There is an "Email address" input field. Below that is a "Region: Self-hosted" dropdown menu. A red arrow points from the "Self-hosted" text to the "Continue" button. Below the "Continue" button is the text "New around here? Create account". At the bottom, a green confirmation message says "Environment URLs saved" with a checkmark icon and a close button (X). A red arrow points from the "Create account" link to the green message.

bitwarden

Log in or create a new account to access your secure vault.

Email address

Region: Self-hosted

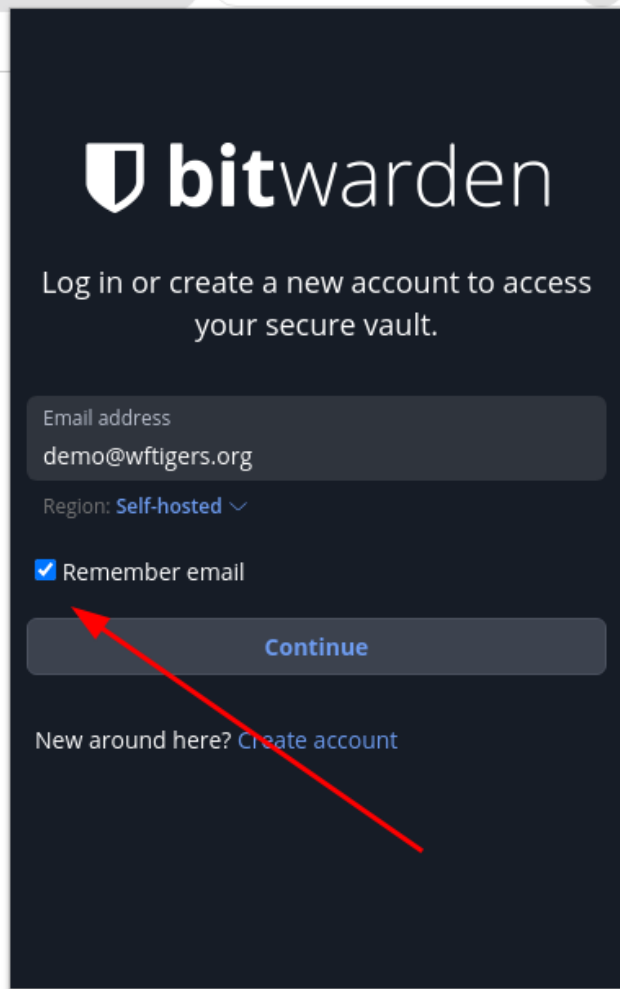
☐ Remember email

Continue

New around here? [Create account](#)

✓ Environment URLs saved

Now go ahead and type in your email address! I also click the “Remember email” checkbox.

The image shows the Bitwarden login interface on a dark background. At the top is the Bitwarden logo. Below it is the text "Log in or create a new account to access your secure vault." There is a text input field for the email address containing "demo@wftigers.org". Below the email field is a dropdown menu for the region, currently set to "Self-hosted". A checkbox labeled "Remember email" is checked. Below these fields is a blue "Continue" button. A red arrow points from the bottom right towards the "Continue" button. At the bottom, there is a link that says "New around here? Create account".

bitwarden

Log in or create a new account to access
your secure vault.

Email address
demo@wftigers.org

Region: Self-hosted ▾

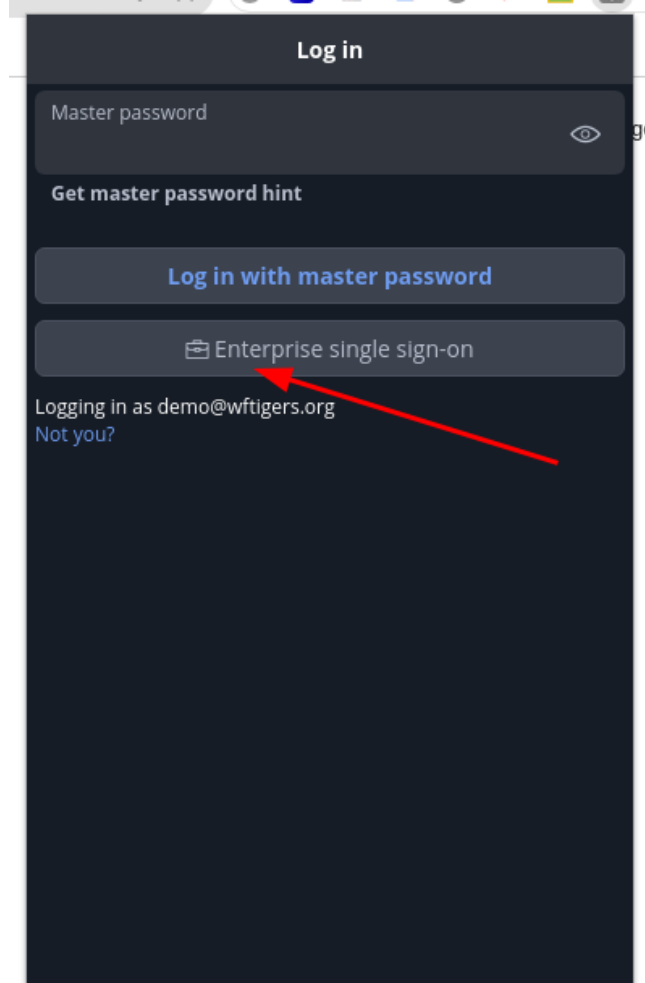
☒ Remember email

Continue

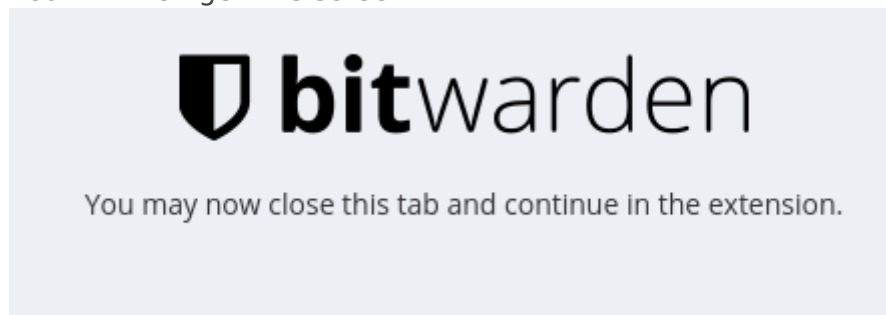
New around here? [Create account](#)

Then click on Continue.

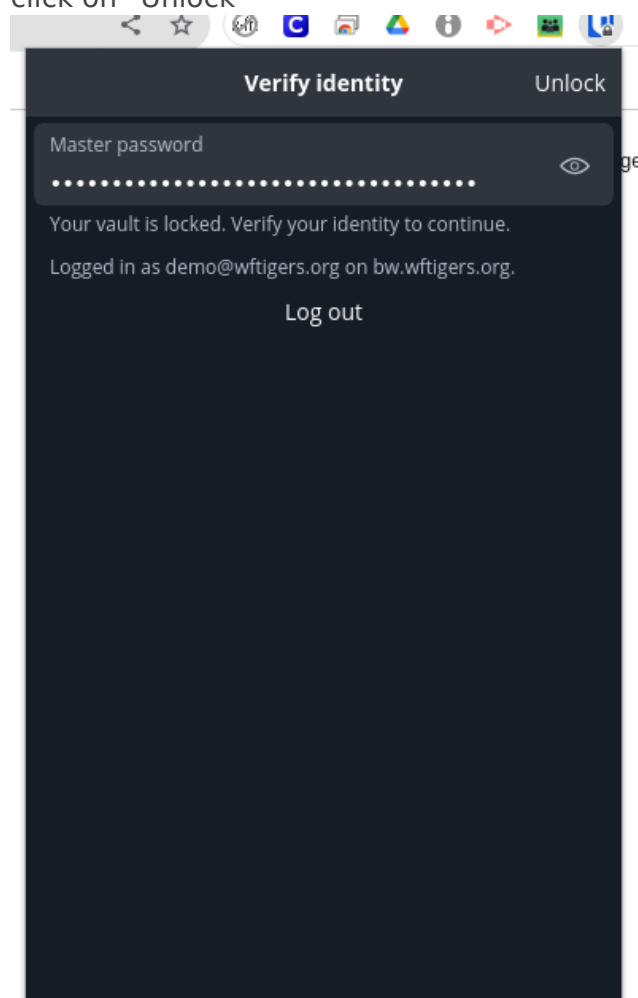
On the next page, if you have been approved by tech, you need to click on the “Enterprise single sign-on” button. That will take you to a Google page (unless you are already logged in). Complete the Google authentication and any two-factor that is required.



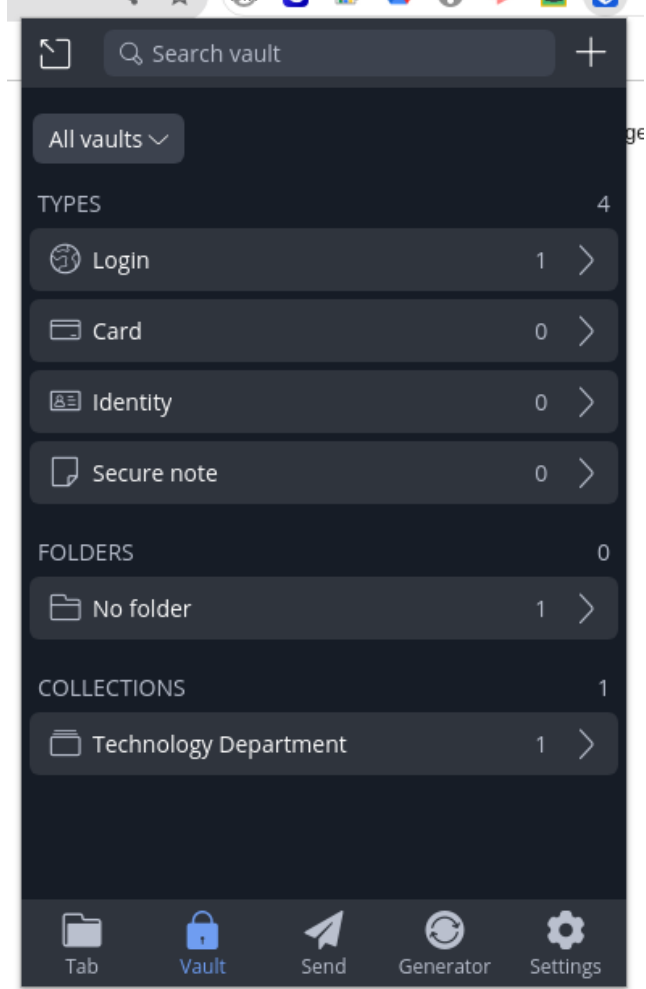
You will then get this screen:



This just means you may now open the extension, and then type in your master password, and click on “Unlock”



You will now be presented with your Bitwarden vault and other options.

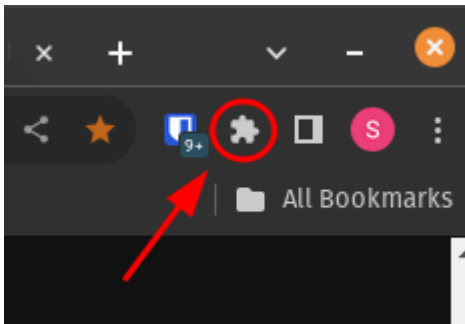


Now that you've set up Bitwarden, you'll want to make sure it auto-fills your logins when you visit a page. If you've restarted your device or closed out of Chrome after finishing the setup, then you've probably noticed it stopped auto-filling your passwords. This is expected behavior. This is because your Bitwarden vault will be **locked**  when you either close Chrome or lock your computer screen (depending on your settings/preference).

When you first start Chrome or unlock your device, you'll first want to unlock your password vault so that it will begin to auto-fill. There are a few ways to bring up the prompt for your master password, and each will have their preference. The purpose of this guide is to outline three of these methods.

1: via Chrome App / Extension

Probably the most user-friendly option is to use the extension icon to determine if your vault is locked and then click to bring up the prompt for a password. To find the extension, there is a puzzle piece icon in the top left of your chrome browser like such...



Note that my Bitwarden extension is already pinned; it is the blue shield icon to the left of my puzzle piece. When you click the puzzle piece, you should get a list of extensions; find the extension titled **“BitWarden - Free Password...”** and use the pin icon immediately to the right of it to pin it. If the pin icon is blue, then it should be pinned, and you can now look for the shield icon next to the puzzle piece.

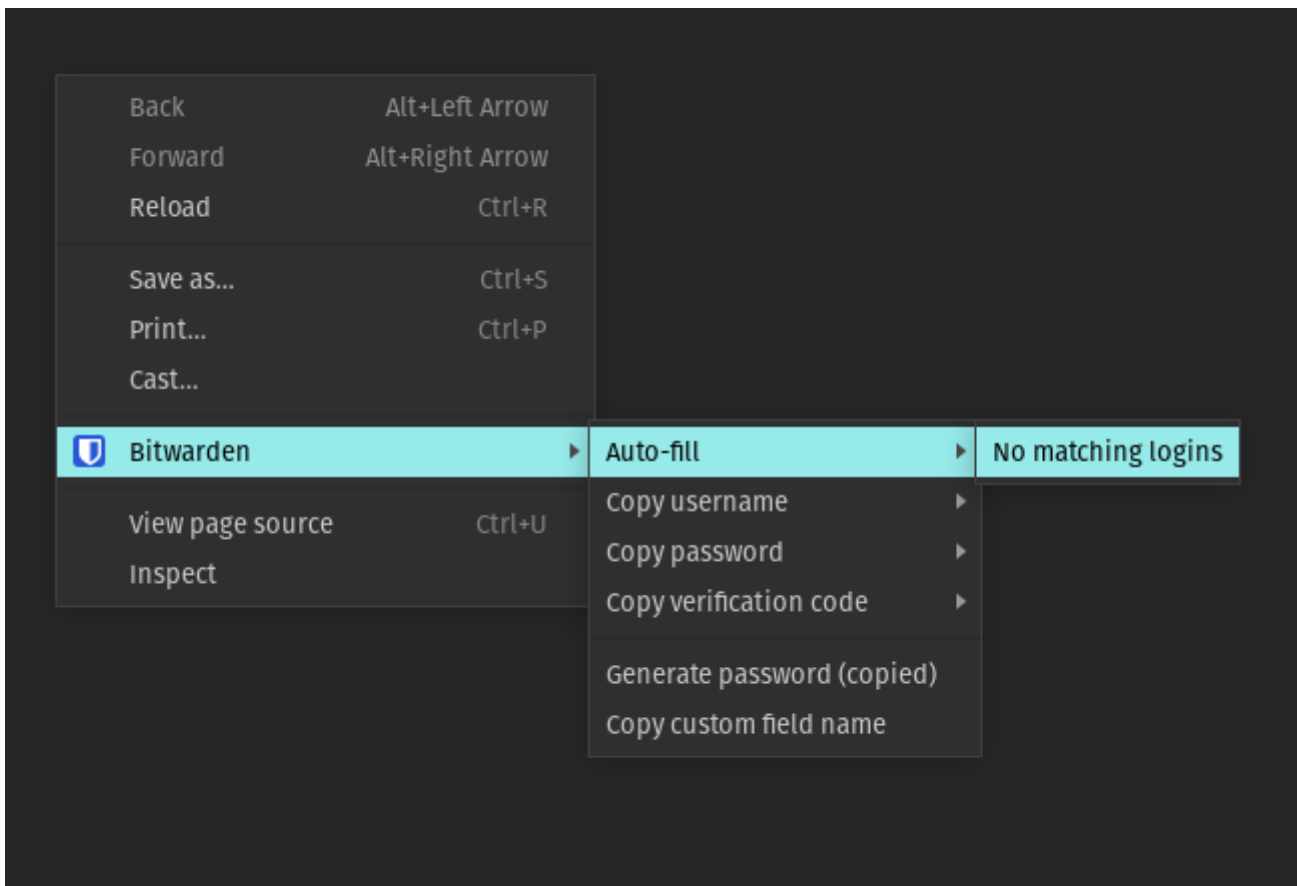
Now that our extension is pinned, we have a quick visual indication of whether or not our vault is locked. These cues are as follows...

-  - Vault is locked; click to enter master password.
-  - Vault is unlocked; auto-fill should work if configured!
-  - Same as unlocked; the number indicates how many logins are saved for this page/domain!

That should be all you need to know to unlock your vault through the extension. Remember you can change the settings in the extension for things such as how often the vault locks. Just be cautious and understand what that setting will do before changing it.

2: via Right-Click

Another easy method is to just right-click on the login field you want to have filled and go to the Bitwarden option. The following screenshot is the navigation to this.



Mine says “No matching logins” because I did not have a login saved for the page, as it was a blank Chrome tab. On your device, it should either list one or more logins or say **Unlock your vault**. If it is the latter, clicking this will prompt for a master password; then you can refresh the page or select a login to auto-fill.

Also note the other options available here, such as generating a password. This is also in the extension, and you can use Bitwarden to create secure passwords and save them in your vault.

3: via Keyboard Shortcut

Naturally, the most elite method is to forego all tedious mouse-clicking as you squint at a bright screen to find that pesky blue shield.

Auto-fill on modern browsers, such as Chrome, should by default have a keyboard shortcut set to `Ctrl + Shift + L` or `Cmd + Shift + L` (for Mac). To make this more mnemonic, you can think of “L” as “Login.”

If you can be comfortable with the keyboard shortcut, it might be the most convenient, as it will more quickly become muscle memory compared to mouse clicks.

Originally posted by Stephen Hale on the West Fork Technology Hub (2023-10-17).