January 2023 **Migrating your passwords from LastPass to Bitwarden**

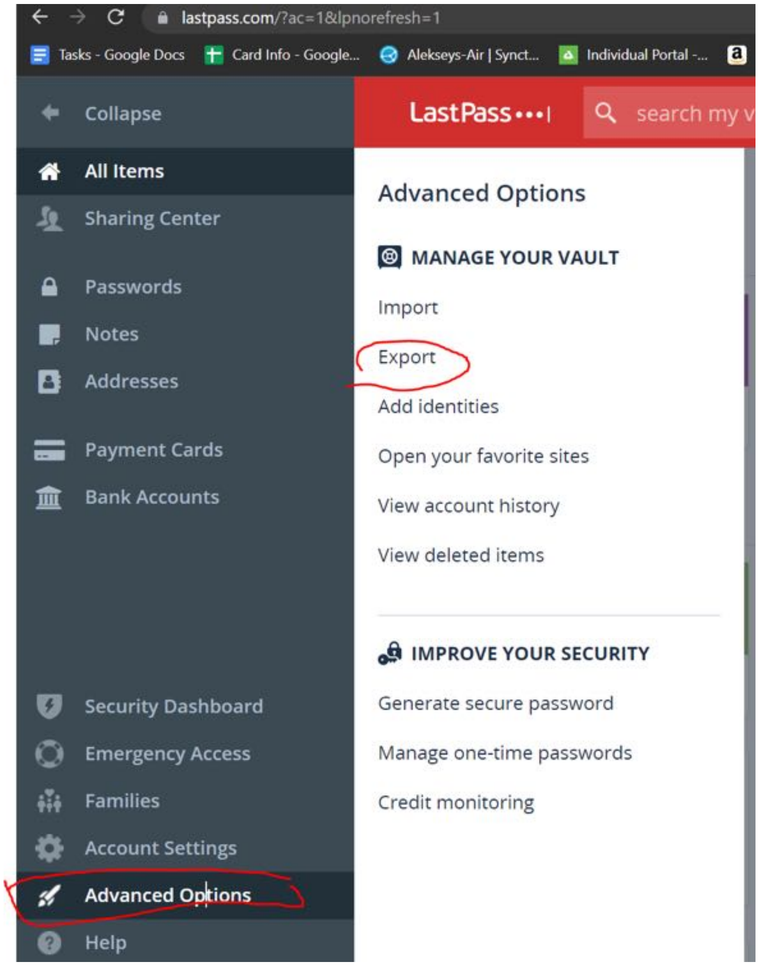
LastPass had a massive breach recently, which led to a lot of revelations:

1. LastPass does not encrypt URLs, just passwords. They also keep records of the ip-addresses used to request records. This is bizarre, contrary to their marketing, and means that hackers now have access to the unencrypted login activity of millions of LastPass customers on many websites.
2. LastPass downplayed the breach and attempted to blame it on their cloud provider. The reality is that LastPass was completely at fault, and didn’t take very easy and reasonable steps to protect the archived password data they were storing.
3. LastPass uses the weakest number of kdf iterations in the industry, and for some longtime customers, it was as little as 5000. This means that you can guess passwords much faster if you are a hacker..
4. Roughly half of the websites you register at will use your email as your username. If LastPass did not properly salt their hashes, hackers will have a much easier time cracking the master password. They will simply look for the most common encrypted username and guess that it is your email. Knowing what your email, as encrypted by your master password, looks like, can give them an edge.

Hackers will try to break into the data and use it for nefarious purposes, but it will take them time to take action on millions of encrypted vaults. We have to be faster than them. Advice:

1. Leave LastPass . This is really the last straw with them.
2. Move to an open-source password manager whose source code can be inspected, and who does not leave things like URLs and customer data unencrypted. Only two options here are
    - Keepass
    - bitwarden
2. I currently recommend bitwarden because they have never been breached, and are a more integrated solution than keepass, which has also never been breached.
3. After you’re off of LastPass change all of your passwords, and if possible, your usernames.
    - Start with the most important ones which are your emails, and your financial institutions.
    - Changing the username will protect you against phishing attacks. The hackers will likely use their knowledge of your email and username to try to either trick you, or trick customers service reps at these websites. The more inaccurate their information, the better.
    - Also change other details like answers to secret questions. Assume that the hackers will know all of the answers to these within a few months.
2. Be wary of fishing attacks going forward. The hackers now know every website you visit, and your username for half of them. They can send VERY authentic looking emails and texts in the hopes that you will fall for it, try to log in, and give them your new passwords.
    - Don’t trust people who call you. The might be scammers.
    - Don’t ever trust emails. For example, if you have an account at Chase, and you get an email from Chase saying that your account balance rapidly fell, and that you should ‘click here’ to make sure it is ok. DON”T CLICK. Open a new browser. Go to Google, search for ‘chase’. Navigate to chase from the google search results, log in, and see what is going on.

Download all of your current passwords from LastPass .
This is done by going to your LastPass vault, then going to 'advanced options' and hitting 'export'



Please note that LastPass is horrible here, and has 'tightened security' after the breach, making it difficult to export the passwords:

When I downloaded my passwords a week ago, it was easy and it downloaded all of them. When I did it again today, the csv file only contained a small fraction of my passwords. I tried it numerous times after disabling my popup blocker and it didn't help. LastPass is just bad.

They will send you an email after you hit 'export'. You have to click the link in the email. Then go back to the tab where you hit 'export' before, and hit 'export' again.

At this point, it should transfer you to another page where a 'csv' file with your passwords will download. I say 'should', because in the past week, LastPass has changed the behavior. It will now take you to a different page, and attempt to download the csv with a popup after playing a 'decrypting' animation. At this point, various popup blockers you have will block the popups causing the download to malfunction. Then it will show you an html page with your passwords.

So, I had to go to the html and copy and paste out the passwords from there. However, be aware that LastPass also had a bug here in some browsers where instead of showing characters like '&' in passwords, it would instead use the html escape: '&amp'. You should do a spot check to make sure you are not affected.

Uninstall LastPass
(BUT NOT LASTPASS AUTHENTICATOR)

Do it.
Remove the extension from your browser.
You don’t need to close the account yet.
You can keep it open while you makes sure you migrated successfully.

But you should remove the extension so that LastPass
doesn’t somehow compromise the password of your next password manager.

YOU DO NOT WANT TO SAVE YOUR NEW BITWARDEN MASTER PASSWORD IN LASTPASS

We’ll need to keep LastPass authenticator for a little longer.

Install Bitwarden.

Get bitwarden for chrome here: https://chrome.google.com/webstore/detail/bitwarden-free-password-m/nngceckbapebfimnlniiiahkandclblb?hl=en

Also install it on your phone.

Sign for bitwarden premium (or participate in a family plan).
Create a bitwarden account.
You want to do this on a laptop or desktop in the browser.

You will need a strong new master password.
DO **NOT** use your previous master password from LastPass .
Advice:

- Make it relatively easy to remember. Make it memorable to you.
- Use a mixture of words, numbers, letters, special characters, uppercase and lower case letters
- DO NOT use the advice form xkcd. Their suggested passwords can be broken in 6 days.
- Spelling badly is encouraged. Your particular way of spelling a word is less likely to be in a dictionary.
- Using multiple languages is helpful, the more obscure the better.

Examples:
Let's say I was obsessed with food, so I make fruit based passwords:

Bad passwords:

- pizzabagelcheese
- Pizzabagelcheese
- Pizzabagelcheese!
- pizzaBagelCheese!
- 1pizzaBagelCheese!
- 1pizzaBagelCh33se!

Why are they bad?

- Too short
- Only 3 very common words
- Exclamation point occurs at common location (at the end)
- Numbers only in the beginning.
- Only first letters of words are capitalized
- Spelling is correct
- Common substitution 'e' -> 3

Can we do better?

arbus@10kgPITsa$juice

- 19 characters
- Russian spelling of watermelon.
- 10kg weight adds memorable numbers
- Pizza misspelled, with caps used for only part of the password.
- Two special characters.
- How to memorize: "Watermelon 10kg pizza expensive juice"

This is enough of a mess that it will most likely be resilient against dictionary attacks, while hopefully being memorable.

It uses the full range of characters, for 72^19 or 10^35 combinations. As a comparison, there are currently estimated to be ~ 10^22 byes of data stored on all the computers in the world combined. No one is breaking it without a quantum computer any time soon even if they have all the worlds computers to throw at the problem.

Please give your password some thought. Then, write it down on a paper and put it somewhere safe in case you forget.

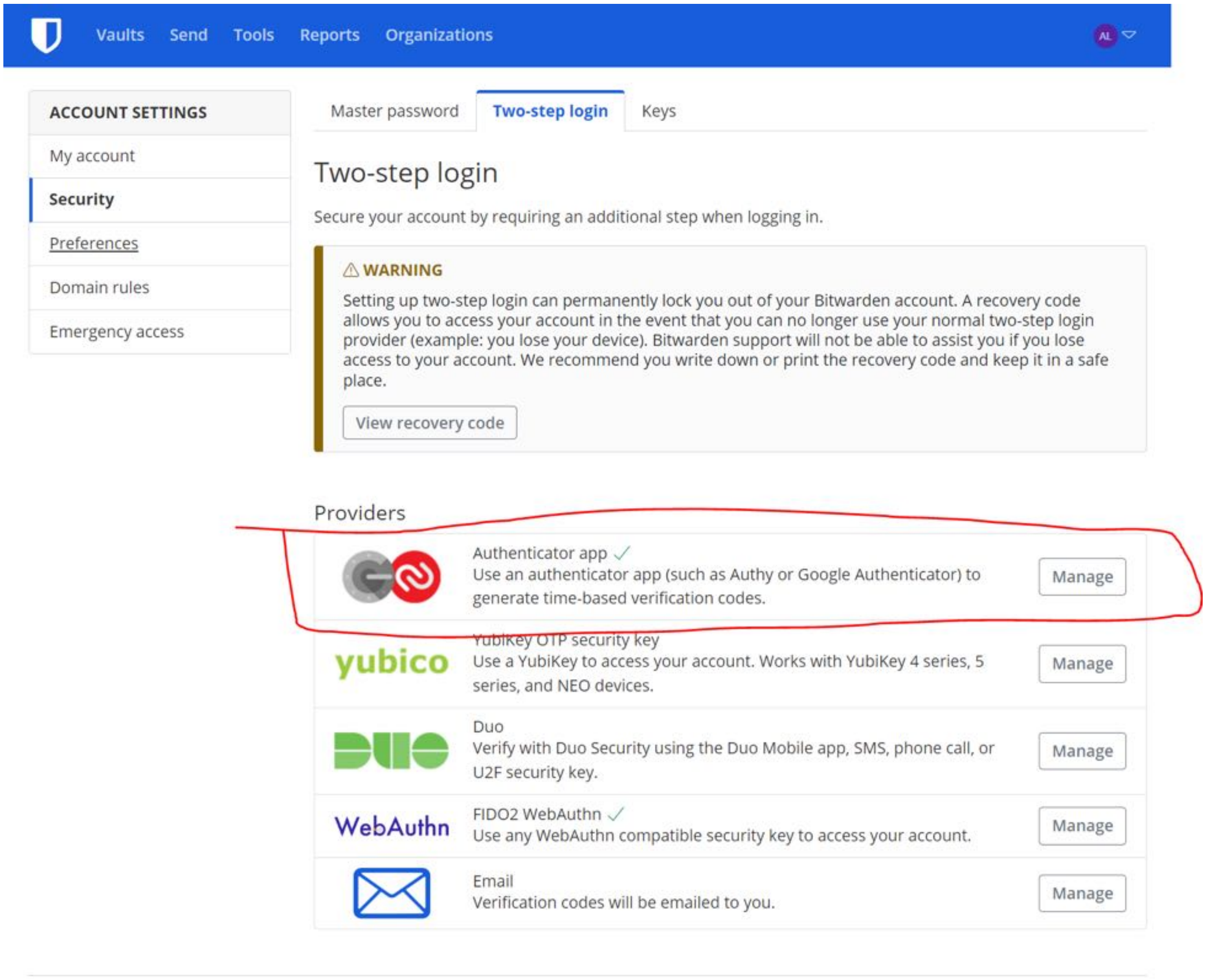
After you create your bitwarden account, enable 2-factor.

Use Google Authenticator.

DO NOT USE ‘AUTHY’ as recommended by bitwarden. (They were recently breached, and the authy breach led to the LastPass breach via a fishing attack)

DO NOT USE the yubi-key methods (USB thingy) - those will come later.

DO NOT USE LastPass authenticator. We’re moving away from that as well.



Two-step login

Secure your account by requiring an additional step when logging in.

⚠ WARNING

Setting up two-step login can permanently lock you out of your Bitwarden account. A recovery code allows you to access your account in the event that you can no longer use your normal two-step login provider (example: you lose your device). Bitwarden support will not be able to assist you if you lose access to your account. We recommend you write down or print the recovery code and keep it in a safe place.

Providers

Authenticator app ✓
Use an authenticator app (such as Authy or Google Authenticator) to generate time-based verification codes.

YubiKey OTP security key
Use a YubiKey to access your account. Works with YubiKey 4 series, 5 series, and NEO devices.

Duo
Verify with Duo Security using the Duo Mobile app, SMS, phone call, or U2F security key.

FIDO2 WebAuthn ✓
Use any WebAuthn compatible security key to access your account.

Email
Verification codes will be emailed to you.

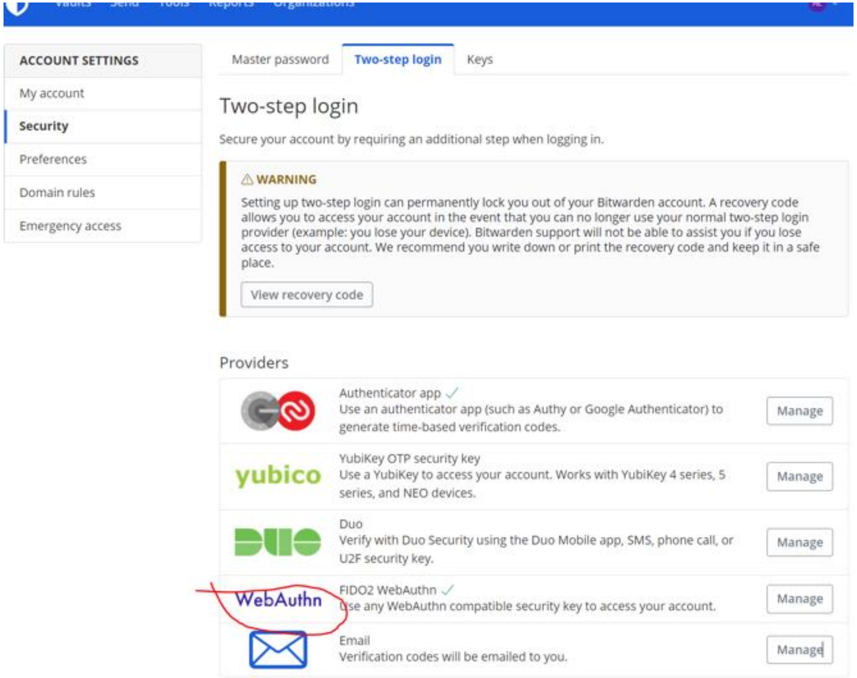
Log into the app on your phone, and tell it to remember you when asked.

You will need to use Google authenticator 2-factor. Remember that while your phone should remember your 2-factor, it SHOULD NOT remember your master password. If someone steals your phone, they should not also gain access to all of your accounts.

Enable WebAuthn 2-factor

WebAuthn is a very strong two factor protection that works with your yubikey. It is MUCH stronger than just a one time password b/c it verifies the website that is asking to do the 2-factor. It is so good, it is used at Google for everything.

Setup is easy. Just click 'manage' on webauthn, and name the yubikey, and press on it when asked. (Do not disable the google authenticator 2-factor)



Two-step login

Secure your account by requiring an additional step when logging in.

⚠ WARNING

Setting up two-step login can permanently lock you out of your Bitwarden account. A recovery code allows you to access your account in the event that you can no longer use your normal two-step login provider (example: you lose your device). Bitwarden support will not be able to assist you if you lose access to your account. We recommend you write down or print the recovery code and keep it in a safe place.

Providers

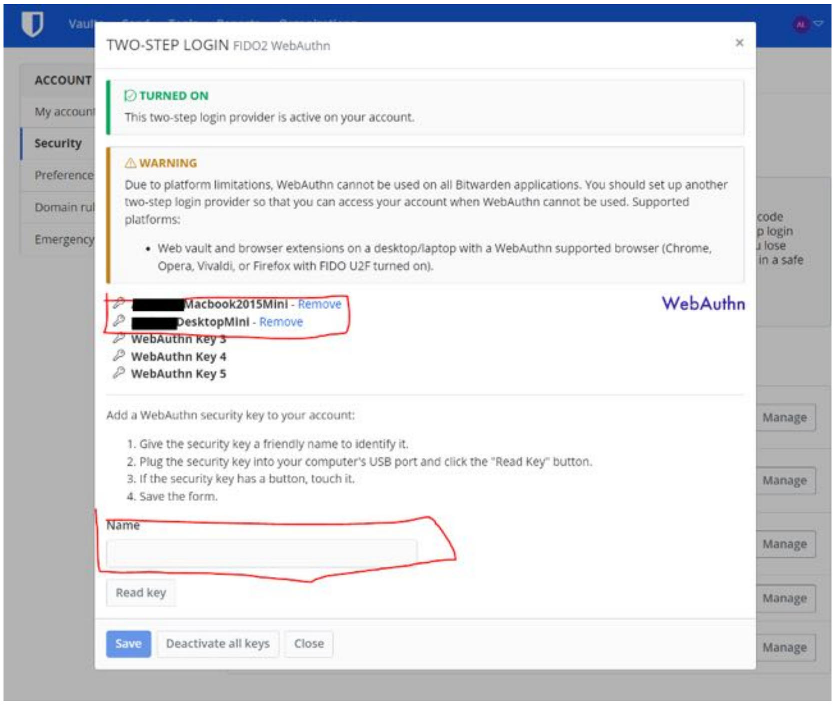
Authenticator app ✓
Use an authenticator app (such as Authy or Google Authenticator) to generate time-based verification codes.

YubiKey OTP security key
Use a YubiKey to access your account. Works with YubiKey 4 series, 5 series, and NEO devices.

Duo
Verify with Duo Security using the Duo Mobile app, SMS, phone call, or U2F security key.

FIDO2 WebAuthn ✓
Use any WebAuthn compatible security key to access your account.

Email
Verification codes will be emailed to you.



TWO-STEP LOGIN FIDO2 WebAuthn

TURNED ON

This two-step login provider is active on your account.

⚠ WARNING

Due to platform limitations, WebAuthn cannot be used on all Bitwarden applications. You should set up another two-step login provider so that you can access your account when WebAuthn cannot be used. Supported platforms:

- Web vault and browser extensions on a desktop/laptop with a WebAuthn supported browser (Chrome, Opera, Vivaldi, or Firefox with FIDO U2F turned on).

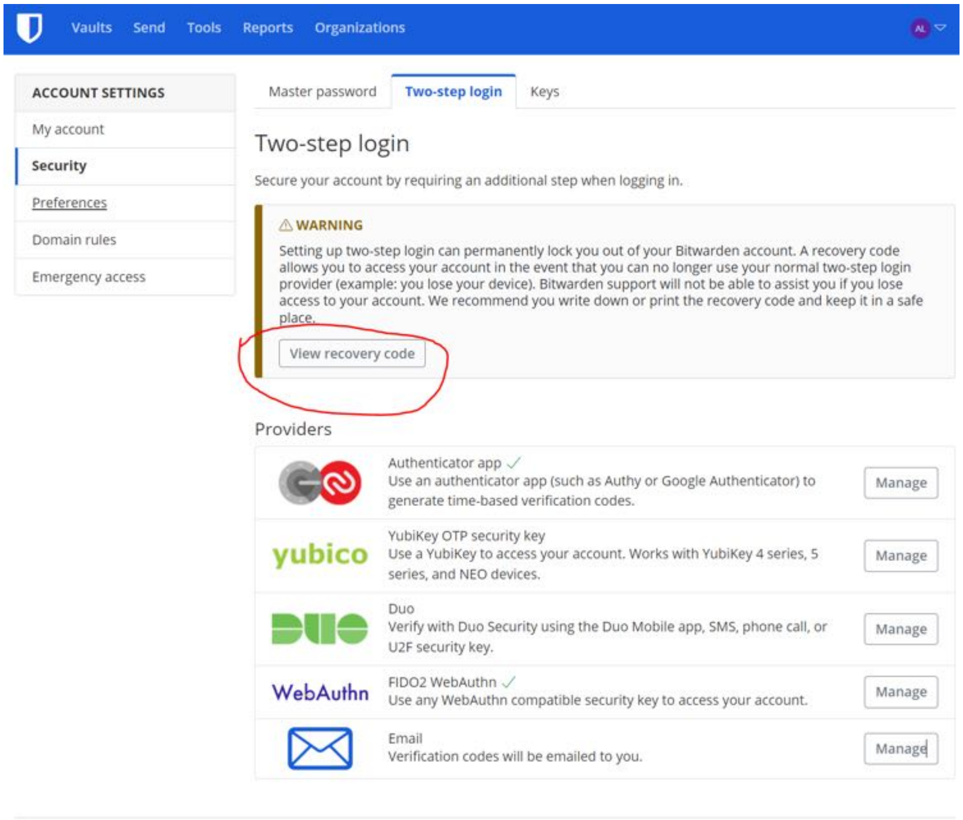
[redacted]Macbook2015Mini - Remove
[redacted]DesktopMini - Remove
WebAuthn Key 3
WebAuthn Key 4
WebAuthn Key 5

Add a WebAuthn security key to your account:

1. Give the security key a friendly name to identify it.
2. Plug the security key into your computer's USB port and click the "Read Key" button.
3. If the security key has a button, touch it.
4. Save the form.

Name

Save your 2-factor recovery code in a safe place:



Two-step login

Secure your account by requiring an additional step when logging in.

⚠ WARNING

Setting up two-step login can permanently lock you out of your Bitwarden account. A recovery code allows you to access your account in the event that you can no longer use your normal two-step login provider (example: you lose your device). Bitwarden support will not be able to assist you if you lose access to your account. We recommend you write down or print the recovery code and keep it in a safe place.

Providers

Authenticator app ✓
Use an authenticator app (such as Authy or Google Authenticator) to generate time-based verification codes.

YubiKey OTP security key
Use a YubiKey to access your account. Works with YubiKey 4 series, 5 series, and NEO devices.

Duo
Verify with Duo Security using the Duo Mobile app, SMS, phone call, or U2F security key.

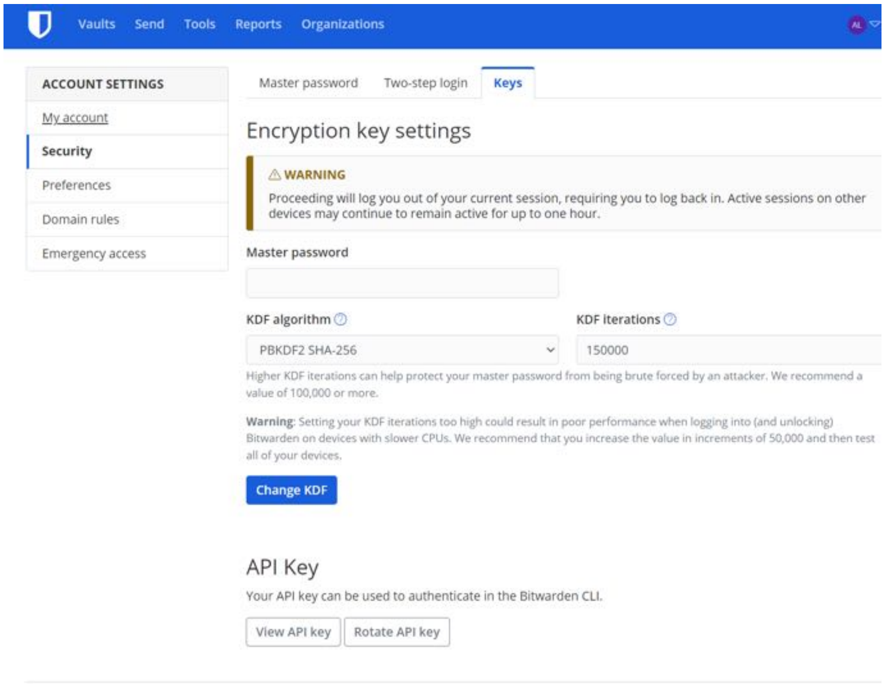
FIDO2 WebAuthn ✓
Use any WebAuthn compatible security key to access your account.

Email
Verification codes will be emailed to you.

Increase your KDF iterations

The higher the number, the more work your phone or computer has to do to encrypt or decrypt the password. 100,000 is standard. I did 150,000 to start but I plan to increase it. The more iterations, the more expensive each attempt to guess your password is for hackers. Also, if they don’t know how many iterations were done, they have to keep checking to see if the decrypted data looks reasonable. That makes their life harder.

I would set yours to a random number above 150,000 for now.
But feel free to go higher unless you start noticing that it is making bitwarden slow on your device.



Encryption key settings

⚠ WARNING

Proceeding will log you out of your current session, requiring you to log back in. Active sessions on other devices may continue to remain active for up to one hour.

Master password

KDF algorithm: PBKDF2 SHA-256

KDF iterations: 150000

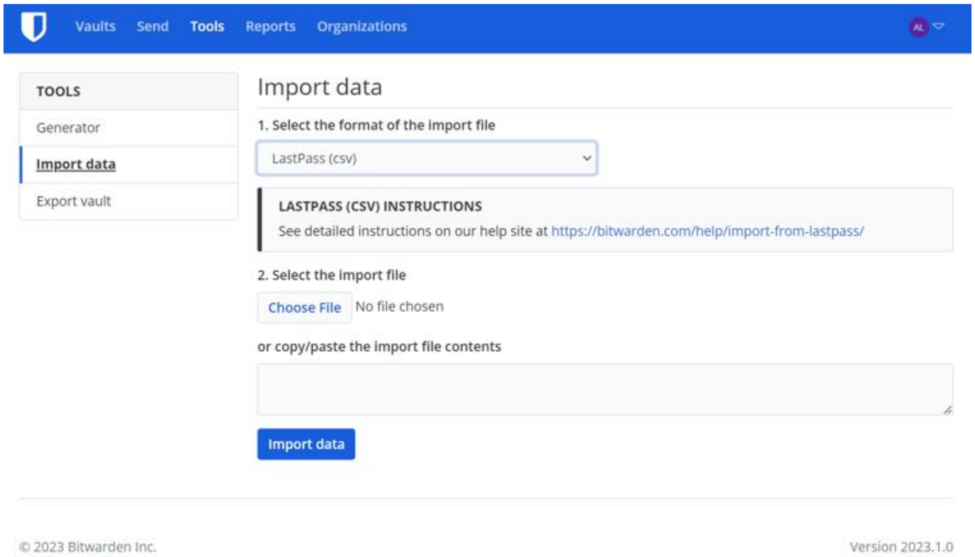
Higher KDF iterations can help protect your master password from being brute forced by an attacker. We recommend a value of 100,000 or more.

Warning: Setting your KDF iterations too high could result in poor performance when logging into (and unlocking) Bitwarden on devices with slower CPUs. We recommend that you increase the value in increments of 50,000 and then test all of your devices.

API Key

Your API key can be used to authenticate in the Bitwarden CLI.

Import your old passwords



Import data

1. Select the format of the import file

LastPass (csv)

LASTPASS (CSV) INSTRUCTIONS

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

2. Select the import file

Choose File No file chosen

or copy/paste the import file contents

© 2023 Bitwarden Inc.

Version 2023.1.0

This step, ‘just worked’ for me. If some of your secure notes are too long, it will refuse to import,
but tell you what they are. Safest thing to do is to copy them into text files on your desktop, delete them from LastPass ,
and then re-export your passwords.
The import should now proceed normally, and you can save the notes later.

You can now start using bitwarden !

Next steps - document how to migrate any 2-factor passwords stored in LastPass authenticator