Log In With Passkeys

Log In With Passkeys

> **Note**
> Log in with passkeys is currently in beta.

Passkeys can be used to log in to Bitwarden as an alternative to using your master password and email. Passkeys used to log in to Bitwarden require user verification, meaning you'll need to use something like a biometric factor or security key to successfully establish access to your passkey.

To learn more about the basics of passkeys, check out this blog from Bitwarden.

Logging in with a passkey will bypass Bitwarden two-step login, however only PRF-capable browser (e.g. Google Chrome) and authenticator (e.g. YubiKey 5) combinations can be used to setup log in with passkeys for vault decryption. Passkeys that don't use PRF will require that you enter your master password after logging in to decrypt your vault.

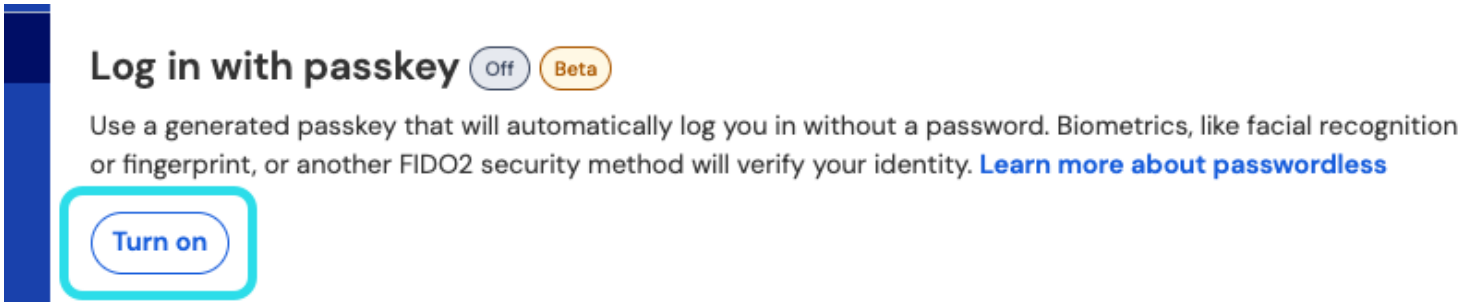
Passkeys can currently be used to log in to the Bitwarden web app, and support for other client applications is planned for a future release.

> **Note**
> Log in with passkeys can't be used by members of an organization that uses the Require single sign-on authentication policy, SSO with trusted devices, or Key Connector.

Create a passkey

You can have up to 5 passkeys to log in with at any given time. To create a passkey to use to log in to Bitwarden:

1. In the web app, select the **Settings** → **Security** from the navigation:
2. Select the **Master password** tab.
3. In the Log in with passkey section, select **Turn on** or, if you've already setup a passkey, **New passkey**. You will be prompted to enter your master password:



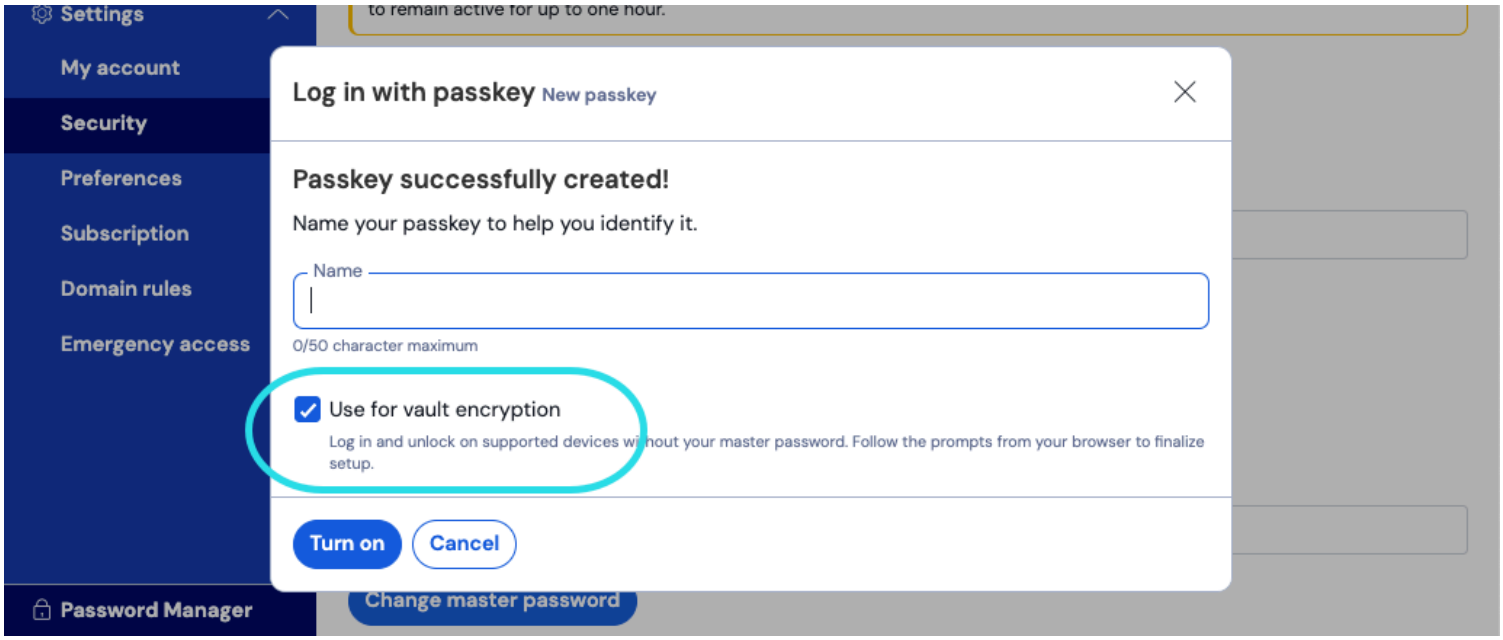
Turn on login with passkeys

4. Follow prompts from your browser to create a FIDO2 passkey. You can complete user verification using a factor like a biometric or by creating a PIN.

   You may, during this procedure, need to cancel out of a default authenticator your browser will want you to use, for example if you want to use a hardware security key on a macOS device that will prioritize Touch ID.

5. Give your passkey a **name**.

6. If you don't want to use your passkey for vault encryption and decryption, uncheck the **Use for vault encryption** checkbox:



Use passkey for vault encryption

   This option will only appear if your browser (e.g. Google Chrome) and authenticator (e.g. YubiKey 5) are PRF-capable. Learn more.

7. Select **Turn on**.

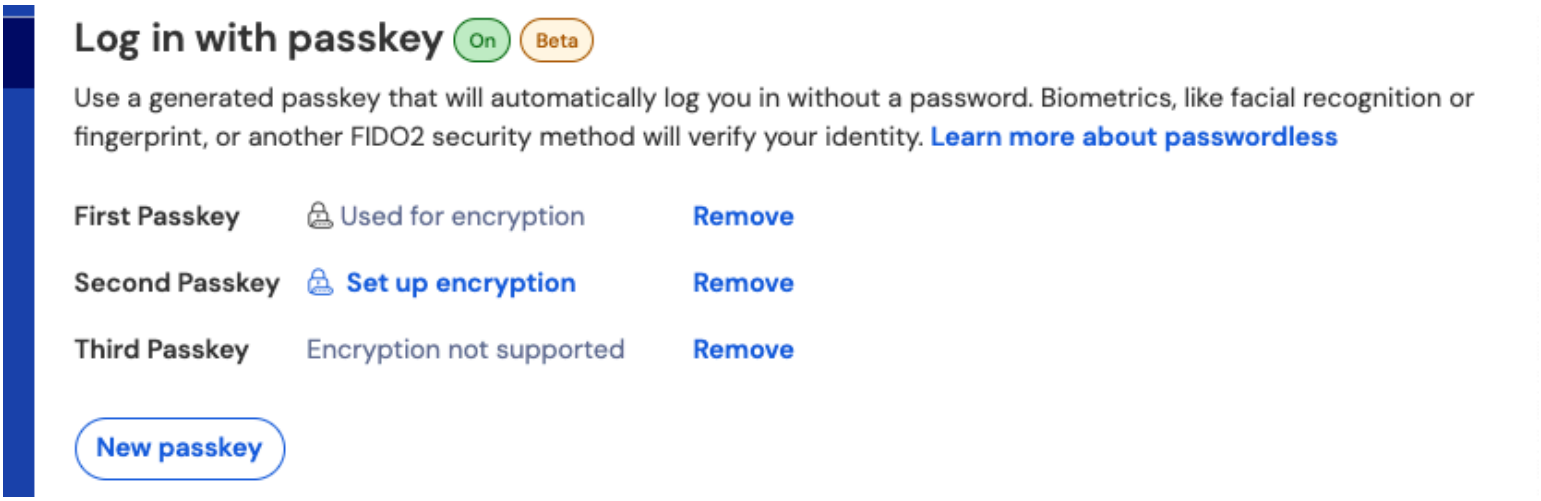
> **Tip**
>
> Bitwarden will not prompt or allow you to save a passkey for logging in to Bitwarden in your vault. This prevents a scenario where access to your vault is required to log in to Bitwarden.

Set up encryption

Both your browser (e.g. Google Chrome) and authenticator (e.g. YubiKey 5) must be PRF-capable in order to support using the passkey for vault encryption and decryption.

> **Tip**
>
> While Google Chrome is PRF-capable, Chrome profiles are not PRF-capable authenticators. As a counter example, the YubiKey 5 is a PRF-capable authenticator. Additionally, Windows 10 is known to have issues with PRF-capable passkeys.
>
> The equipment you have at your disposal and in your environment will determine your ability to use passkeys for encryption.

Your passkeys list will show whether each passkey is used for encryption, supported but not enabled, or not supported:



Passkeys list

If you didn't check the **Use for vault encryption** checkbox when you initially set up the passkey, or if for example the browser you were using at the time was not PRF-capable, navigate to this menu and select the **Set up encryption** button.

Remove a passkey

You can remove an existing passkey from Bitwarden using the **Remove** button on the same screen. Removing a passkey from Bitwarden will not delete the private key stored in your FIDO2 authenticator, but you'll no longer be able to use it to log into Bitwarden.

Log in with your passkey

Once your passkey is created, you can use it to log in to the Bitwarden web app:

1. On the Bitwarden login screen, select **Log in with passkey** where you'd usually enter your email address.
2. Follow prompts from your browser to read the passkey, this will authenticate you with Bitwarden.
3. If your passkey is setup for vault encryption, you're done! Otherwise, enter your master password and select **Unlock** to decrypt your vault data.

How it works

The following describes the mechanics of logging in with passkeys. Which tab is relevant to you depends on whether your passkeys was set up with encryption.

⇒Passkeys with encryption turned on

Create a passkey

When a passkey is registered for log in to Bitwarden:

- A **passkey public and private key pair** is generated by the authenticator via the WebAuthn API. This key pair, by definition, is what constitutes your passkey.
- A **PRF symmetric key** is generated by the authenticator via the WebAuthn API's PRF extension. This key is derived from an **internal secret** unique to your passkey and a **salt** provided by Bitwarden.
- A **PRF public and private key pair** is generated by the Bitwarden client. The PRF public key encrypts your **account encryption key**, which your client will have access to by virtue of being logged in and unlocked, and the resulting **PRF-encrypted account encryption key** is sent to the server.
- The **PRF private key** is encrypted with the **PRF symmetric key** (see Step 2) and the resulting **PRF-encrypted private key** is sent to the server.
- Your client sends data to Bitwarden servers to create a new passkey credential record for your account. If your passkey is registered with support for vault encryption and decryption, this record includes:
  - The passkey name
  - The passkey public key
  - The PRF public key
  - The PRF-encrypted account encryption key
  - The PRF-encrypted private key

Your passkey private key, which is required to accomplish authentication, only ever leaves the client in an encrypted format.

Log in with your passkey

When a passkey is used to log in and, specifically, to decrypt your vault data:

- Using WebAuthn API public key cryptography, your authentication request is asserted and affirmed.
- Your **PRF-encrypted account encryption key** and **PRF-encrypted private key** are sent from the server to your client.
- Using the same **salt** provided by Bitwarden and the **internal secret** unique to your passkey, the **PRF symmetric key** is re-created locally.
- The **PRF symmetric key** is used to decrypt your **PRF-encrypted private key**, resulting in your **PRF private key**.
- The **PRF private key** is used to decrypt your **PRF-encrypted account encryption key**, resulting in your **account encryption key**. Your account encryption key is used to decrypt your vault data.

⇒Passkeys with encryption turned off

Create a passkey

When a passkey is registered for log in to Bitwarden:

1. A **passkey public and private key pair** is created. This key pair, by definition, is what constitutes your passkey.
2. Your client sends data to Bitwarden servers to create a new passkey credential record for your account. If your passkey is not registered with support for vault encryption and decryption, this record includes:
   - The passkey's name
   - The passkey's public key

Your passkey's private key, which is required to accomplish authentication, only ever leaves the client in an encrypted format.

Log in with your passkey

When a passkey is used to log in, your authentication request is asserted and affirmed using WebAuthn API public key cryptography. You will then be required to decrypt your vault using your master password.