bitwarden | Help Center Article

MY ACCOUNT > TWO-STEP LOGIN

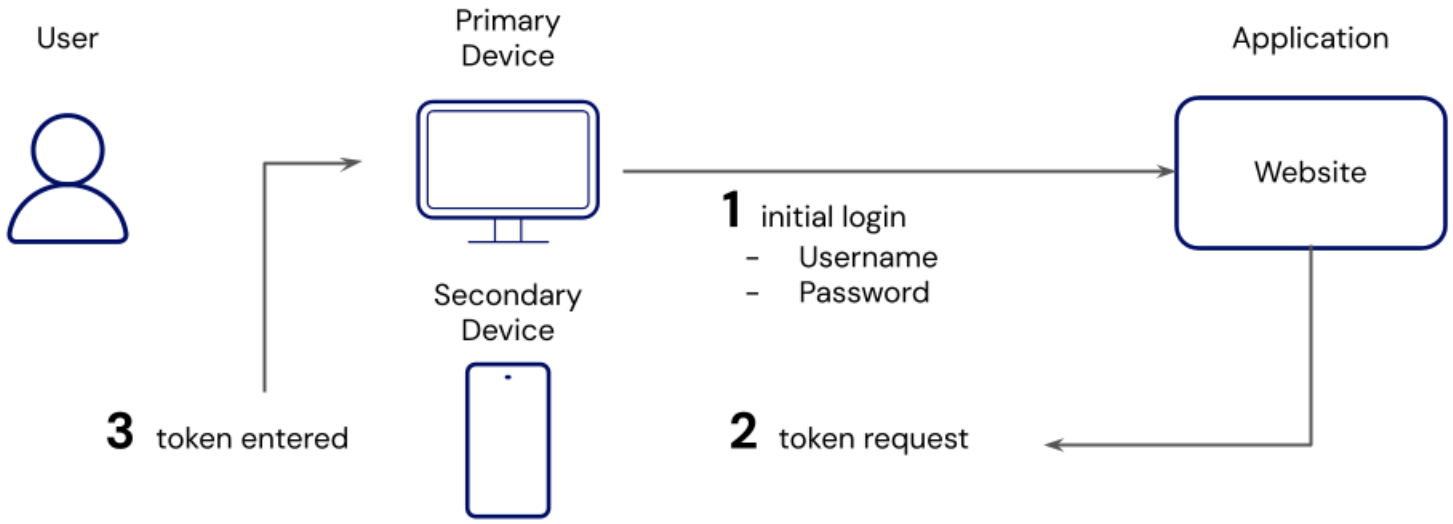
Field Guide to Two-Step Login

View in the help center:
https://bitwarden.com/help/bitwarden-field-guide-two-step-login/

Field Guide to Two-Step Login

Two-step login (also called two-factor authentication or 2FA) is a common security technique used by websites and apps to protect your sensitive data. Websites that use two-step login require you to verify your identity by entering an additional "token" (also called verification code or one-time password (OTP)) besides username and password, typically retrieved from a different device.

Without physical access to the token from your secondary device, a malicious actor would be unable to access the website, even if they discover your username and password:



Basic Two-step Login flow

Commonly, websites or apps with sensitive data (for example, your online bank account) will attempt verify your identity outside of the login screen by:

- Sending a token in an SMS / text message to the mobile device on-file.
- Asking for a token generated by an Authenticator app (for example, Bitwarden Authenticator) on your mobile device.
- Looking for a token from a physical security key (for example, Yubikey).

How should I use two-step login?

Security often involves a tradeoff between protection and convenience, so ultimately it's up to you! Generally, the two most critical ways to use two-step login are:

1. **To secure Bitwarden**

   Secure all vault data by requiring a secondary step each time you log in to Bitwarden, in addition to entering your master password.

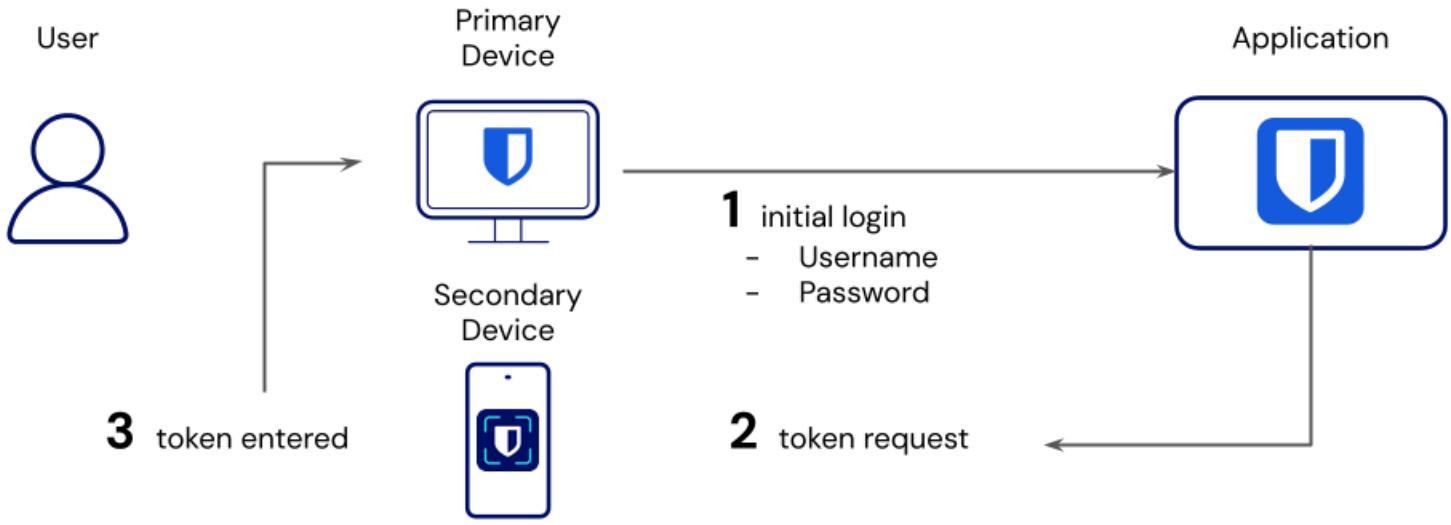
2. **To secure important websites**

   Secure an individual website by requiring a temporary one-time password (TOTP) when you log in. You can store and generate TOTPs with Bitwarden.

Securing Bitwarden

Since your password manager stores all of your logins, we highly recommend that you secure it with two-step login. Doing so protects all of your logins by preventing a malicious actor from accessing your vault, even if they discover your master password.

Enabling two-step login will require you to complete a secondary step each time you log in, in addition to your primary log in method (master password). You won't need to complete your secondary step to unlock your vault, only to log in.



Two-step login to access Bitwarden

Bitwarden offers several two-step login methods for free, including:

- FIDO (any FIDO2 WebAuthn certified key)
- via an authenticator app (for example, Bitwarden Authenticator)
- via email

For premium users, Bitwarden offers several advanced two-step login methods:

- Duo Security with Duo Push, SMS, phone call, and security keys

- YubiKey (any 4/5 series device or YubiKey NEO/NFC)

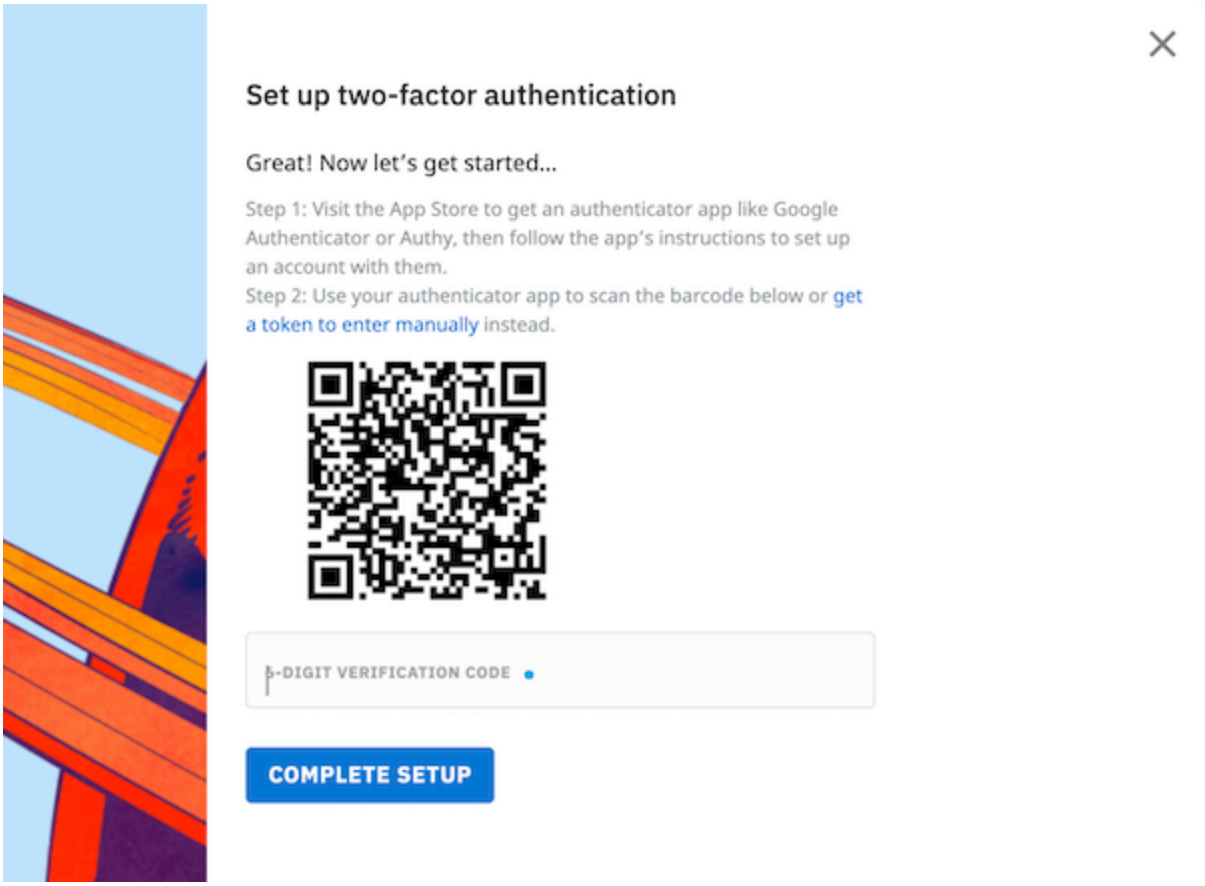
Learn more about your options or get help setting up any method using our **Setup Guides.**

> **Note**
> Bitwarden does not support SMS 2FA due to vulnerabilities, including SIM hijacking. We do not recommend SMS 2FA for other accounts unless it is the only available method. Any second factor is recommended over having none, but most alternatives are safer than SMS 2FA.

Securing important websites

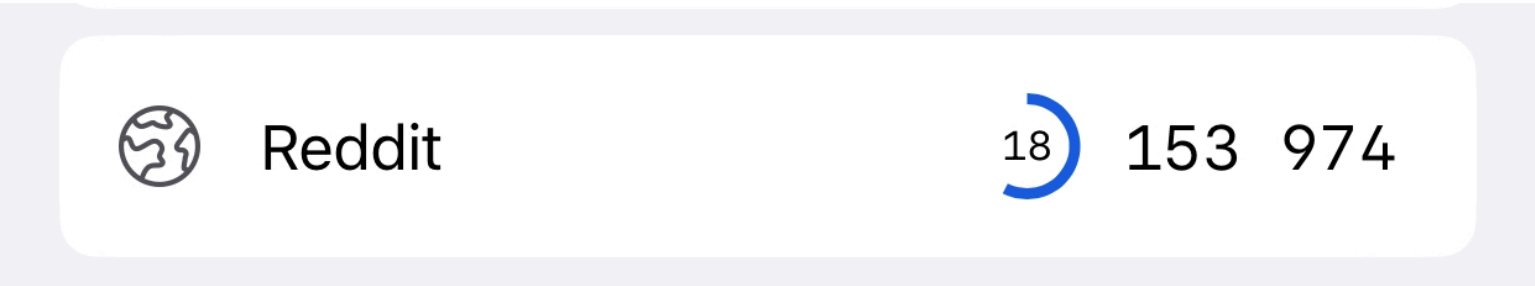
Many other websites and apps have two-step login options, this is especially common for websites that store sensitive information (for example, credit card or bank account numbers). Most website's two-step login option will be located in the **Settings**, **Security**, or **Privacy** menus.

Activating two-step login will typically open a QR code, like this example from Reddit:



2FA QR Code

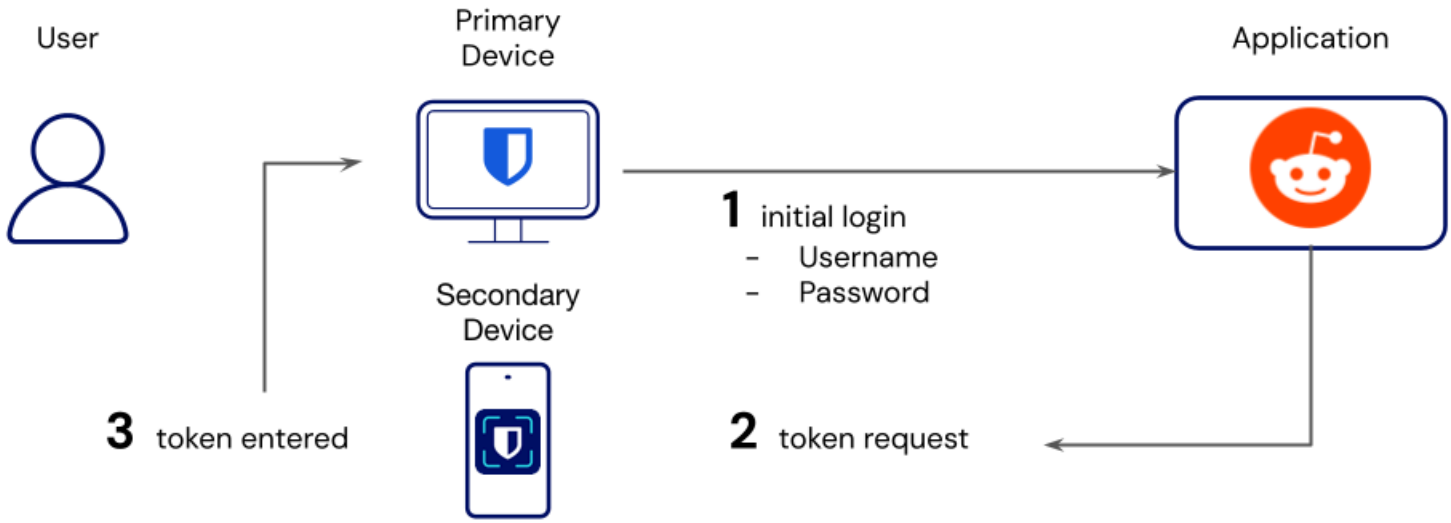
Scanning this code with an authenticator app will enable the app to generate rotating six-digit tokens that you can use to verify your identity, like this one generated by Bitwarden Authenticator:



TOTP token

Use Bitwarden Authenticator

Bitwarden Authenticator is a mobile authentication app you can use to verify your identity for websites and apps that use two-factor authentication (2FA). Bitwarden Authenticator can be downloaded from the iOS App Store and Google Play Store.

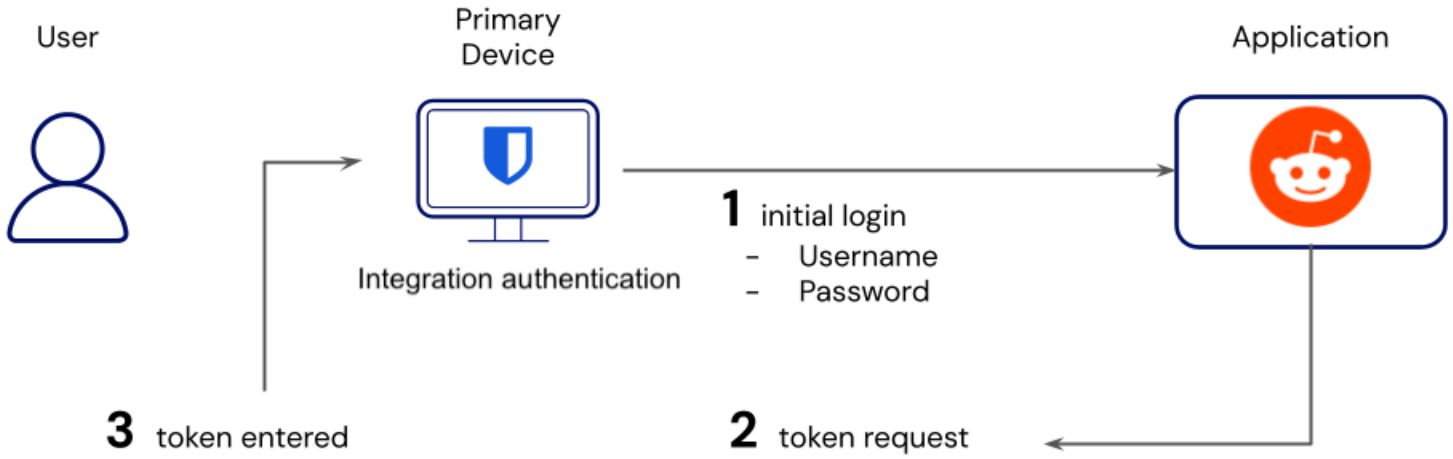


Two-step login using Bitwarden Authenticator

For help using Bitwarden Authenticator, refer to this article.

Use integrated authentication

As an alternative, Bitwarden Password Manager offers a built-in authenticator for premium users, including members of paid organizations (Families, Teams, or Enterprise).



Two-step Login using Bitwarden

For help using integration authentication, refer to this article.

When should I use the standalone app as opposed to the integrated authenticator?

Only the standalone app allows you to setup 2FA for your Bitwarden account, but you can use either app to store and generate verification codes for all your other accounts. Only the integrated authentication currently allows you to share the token generation among team members. They can be used together, or separately, depending on your security preferences.

2FA security keys and passkeys

FIDO2 security keys are a popular and secure option for adding 2FA to your Bitwarden account. If you are not familiar with FIDO2 security keys, see the FIDO Alliance website for additional information regarding FIDO2.

A YubiKey device is a security key that works with FIDO authentication protocols, and can have several use cases. Two uses are as 2FA security keys, or passkeys.

- **2FA security key:** Using a YubiKey as a 2FA security key will act as an additional device in the authentication process. This will be accompanied by another primary method of authentication (such as master password). The YubiKey security key must be physically plugged in to provide the authentication credentials.

- **Passkey:** A passkey is a pair or public-private cryptographic keys that are used to authenticate a login. Instead of creating a username, password and adding 2FA to an account, the single passkey is used. During passkey creation, the YubiKey is able to work as the passkey generator to create the public and private keys necessary for passkey login. Learn more about using a YubiKey as a passkey here.

With Bitwarden, the primary use of a security key such as a YubiKey device is to provide 2FA authentication.

Next steps

Now that you are a two-step login expert, we recommend:

- Setup two-step login
- Get premium for access to advanced two-step login methods
- Setup the Bitwarden authenticator
- Setup two-step login for teams and enterprise