

MY ACCOUNT > TWO-STEP LOGIN

Two-step Login Methods

A decorative graphic consisting of numerous thin, light blue wavy lines that create a sense of motion and depth across the middle section of the page.

View in the help center:

<https://bitwarden.com/help/setup-two-step-login/>

Two-step Login Methods

💡 Tip

February / March 2025: To increase account security, Bitwarden will soon require additional verification for users **who do not use two-step login** when [logging into your account from a new device or after clearing browser cookies](#). You may have received an email and product notification indicating this.

After entering your Bitwarden master password, you will be prompted to enter a one-time verification code sent to your account email. Alternatively, you can:

- Preemptively set up two-step login by following any of the guides on this page.
- Opt-out of this feature from the Settings → My account screen in the Danger Zone section.

Using two-step login (also called two-factor authentication, or 2FA) protects your Bitwarden vault in case someone gets ahold of your master password. It works by requiring authentication from another source when you log in. If you are unfamiliar with the basics of 2FA, check out our [Field Guide](#).

There are many different methods available for two-step login. You can have as many active as you like. What's important is that any form of two-step login is active to be sure your account is protected.

Two-step login for individuals

Anyone can set up two-step login on their individual account by visiting the web app and choosing **Settings → Security → Two-step login**.

Methods

Set up at least one of the following two-step login methods. Setup instructions are available for each:

Method	Setup instructions	Subscription requirements
FIDO2 WebAuthn credentials (for example, hardware keys like YubiKeys and Google Titan)	Setup instructions	Free for all
Authenticator app (for example, Bitwarden Authenticator)	Setup instructions	Free for all
Email	Setup instructions	Free for all

Method	Setup instructions	Subscription requirements
Duo Security with Duo Push, SMS, phone call, and security keys	Setup instructions	Requires premium
YubiKey OTP (any 4/5 series device or YubiKey NEO/NFC)	Setup instructions	Requires premium

Two-step login for Teams and Enterprise

While each user can activate two-step login on their accounts using the methods on the chart above, Teams and Enterprise organizations have additional options:

Method	Setup instructions	Subscription requirements
Duo Security with Duo Push, SMS, phone call, and security keys	Click here .	Requires Teams or Enterprise

Additionally, Enterprise organizations can require two-step login with a [policy](#), and the same protection can be achieved outside of Bitwarden using your Identity Provider when using Single Sign-On (SSO).

Using multiple methods

You can enable multiple two-step login methods. When you log in to a vault that has multiple enabled methods, Bitwarden will prompt you for the highest-priority method according to the following order of preference:

1. Duo (organizations)
2. FIDO2 WebAuthn
3. YubiKey
4. Duo (individual)
5. Authenticator app
6. Email

Warning

Two-step login via email is not recommended if you are using [login with SSO](#), as using multiple methods will cause errors. Consider setting up [two-step login via a free authenticator](#) instead.

Any option will work, though. Authenticate with a lower-preference method by selecting the **Use another two-step login method** button:

Authenticator App

Enter the 6 digit verification code from your authenticator app.

Remember me

 Continue

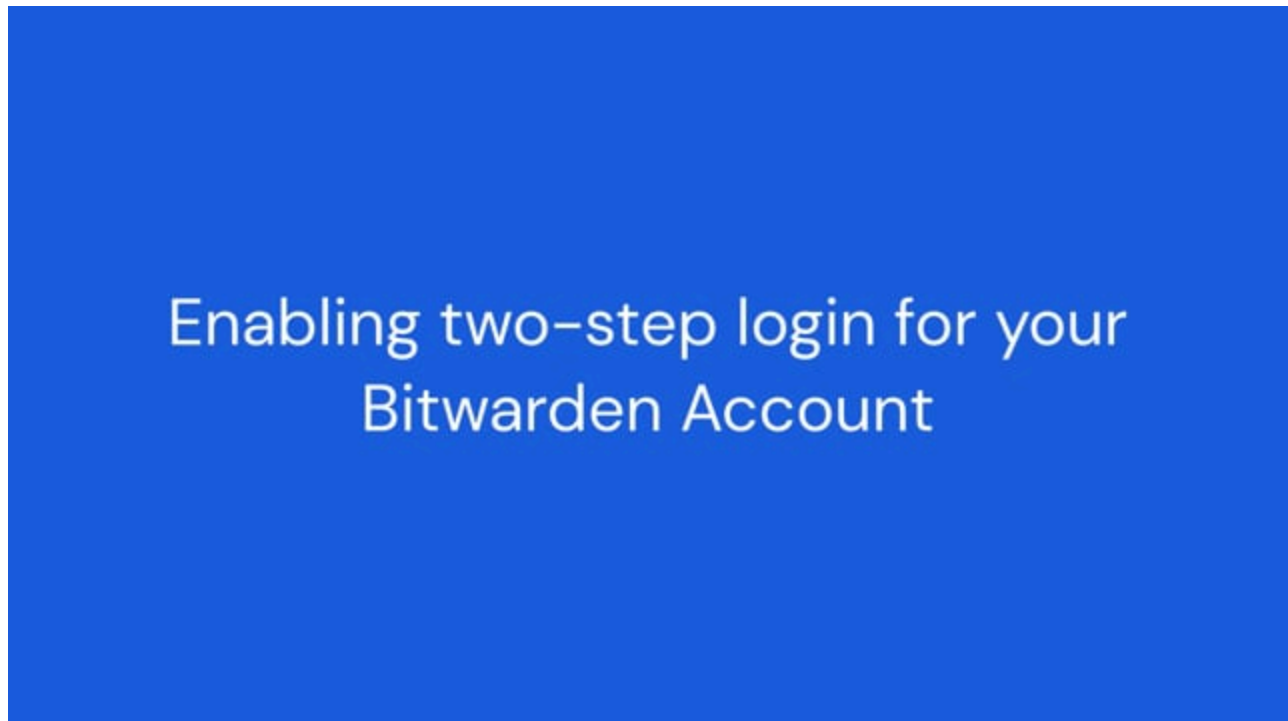
Cancel

 [Use another two-step login method](#)

Use another two-step login method

Enabling two-step login

To setup two-step login for your Bitwarden account:



<https://player.vimeo.com/video/795652047>