

SECRETS MANAGER > GET STARTED

Log in to Secrets Manager

View in the help center:

<https://bitwarden.com/help/log-in-to-secrets-manager/>

Log in to Secrets Manager

The end-to-end zero-knowledge encrypted Bitwarden account you use to log into Password Manager will be the same as what you use to log into Secrets Manager.

💡 Tip

This article pertains to logging in to the Secrets Manager web vault. The [Secrets Manager CLI](#), which is primarily used to script secrets injection into your applications and infrastructure, requires logging in with an [access token](#).

Master password

Your master password is the primary method for accessing your Bitwarden account. It's important that your master password is:

- **Memorable:** Bitwarden employees and systems have no knowledge of, way to retrieve, or way to reset your master password. **Do not forget your master password!**
- **Strong:** A longer, more complex, and less common master password is the best way to protect your account. Bitwarden provides a free password strength testing tool to test the strength of some memorable pass words you are considering.

💡 Tip

Worried about forgetting your master password? Here is what to do:

- **Setup a hint.** In case you need a reminder, a master password hint email can be requested on the login screen. Make sure you use a hint that only you will understand.
- **Designate a [trusted emergency contact](#).** Users with premium access can grant account access to a friend or family member in the case of emergency.

Learn how to [change your master password](#), or what to do if you've [forgotten your master password](#).

Two-step login

Using [two-step login](#) (also called two-factor authentication or 2FA) to protect your Bitwarden account prevents a malicious actor from accessing your data even if they discover your master password by requiring authentication from a secondary device when you log in.

There are lots of different methods for two-step login, ranging from dedicated authenticator apps to hardware security keys. Whatever you choose, Bitwarden highly recommends that you secure your vault using two-step login.

Free methods

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

Method	Setup instructions
via an authenticator app (for example, Authy or Google Authenticator)	Click here .

Method	Setup instructions
via email	Click here .
via a FIDO WebAuthn Authenticator	Click here .

Premium methods

For premium users (including members of paid organizations), Bitwarden offers several advanced two-step login methods:

Method	Setup instructions
via Duo Security with Duo Push, SMS, phone call, and security keys	Click here .
via YubiKey (any 4/5 series device or YubiKey NEO/NFC)	Click here .

Log in with device

Did you know you can log in to the Bitwarden web app using a secondary device instead of your master password? Logging in with a device is a passwordless approach to authentication, removing the need to enter your master password by sending authentication requests to any certain devices you're currently logged in to for approval. [Learn more](#).

Single sign-on

If your organization uses [login with SSO](#), you can access your Bitwarden web app [using your federated SSO credentials](#).