

SECRETS MANAGER > LOS GEHT'S

Melden Sie sich beim Secrets Manager an

Ansicht im Hilfezentrum:

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

Melden Sie sich beim Secrets Manager an

Das Ende-zu-Ende Null-Wissen verschlüsselte Bitwarden-Konto, das Sie verwenden, um sich beim Passwort-Manager anzumelden, wird das gleiche sein, das Sie verwenden, um sich beim Secrets Manager anzumelden.

Tip

Dieser Artikel bezieht sich auf das Anmelden im Secrets Manager Web-Tresor. Die [Secrets Manager CLI](#), die hauptsächlich dazu dient, das Einspeisen von Geheimnissen in Ihre Anwendungen und Infrastruktur zu skripten, erfordert das Anmelden mit einem [Zugriffs-Token](#).

Master-Passwort

Ihr Master-Passwort ist die primäre Methode, um auf Ihr Bitwarden-Konto zuzugreifen. Es ist wichtig, dass Ihr Master-Passwort ist:

- **Unvergesslich:** Bitwarden-Mitarbeiter und -Systeme haben keine Kenntnis von, keine Möglichkeit zur Wiederherstellung oder Möglichkeit zum Zurücksetzen Ihres Master-Passworts. **Vergessen Sie nicht Ihr Master-Passwort!**
- **Stark** : Ein längeres, komplexeres und weniger verbreitetes Master-Passwort ist der beste Weg, Ihr Konto zu schützen. Bitwarden bietet ein kostenloses Passwortstärke-Testtool an, um die Stärke einiger denkwürdiger Passwörter zu testen, die Sie in Betracht ziehen.

Tip

Fürchten Sie, Ihr Master-Passwort zu vergessen? Folgendes können Sie tun:

- **Richten Sie einen Hinweis ein.** Falls Sie eine Erinnerung benötigen, können Sie auf dem Anmeldebildschirm eine E-Mail mit einem Hinweis auf Ihr Master-Passwort anfordern. Stellen Sie sicher, dass Sie einen Hinweis verwenden, den nur Sie verstehen können.
- **Bestimmen Sie eine vertrauenswürdige Kontaktperson für Notfälle.** Nutzer mit Premium-Zugang können einem Freund oder Familienmitglied für den Notfall Zugang zum Tresor gewähren.

Erfahren Sie, wie Sie Ihr [Master-Passwort ändern](#) können, oder was Sie tun müssen, wenn Sie Ihr [Master-Passwort vergessen](#) haben.

Authentifizierungs-App verwalten

Die Verwendung von [Zwei-Schritt-Zugangsdaten](#) (auch Zwei-Faktor-Authentifizierung oder 2FA genannt) zum Schutz Ihres Bitwarden-Kontos verhindert, dass ein bössartiger Akteur auf Ihre Daten zugreift, selbst wenn er Ihr Master-Passwort entdeckt, indem er bei der Anmeldung eine Authentifizierung von einem sekundären Gerät verlangt.

Es gibt viele verschiedene Methoden für die zweistufige Anmeldung, die von speziellen Authentifizierungs-Apps bis hin zu Hardware-Sicherheitsschlüsseln reichen. Wie auch immer Sie sich entscheiden: Bitwarden empfiehlt dringend, dass Sie Ihren Tresor mit einer zweistufigen

Anmeldung sichern.

Kostenlose Methoden

Bitwarden bietet mehrere kostenlose Methoden zur zweistufigen Anmeldung, darunter:

Methode	Einrichtung
über eine Authentifizierungs-App (zum Beispiel, Authy oder Google Authenticator)	Hier klicken.
Premium-Methoden	Hier klicken.
über einen FIDO WebAuthn Authenticator	Hier klicken.

Einrichtung

Einrichtung

Methode	Einrichtung
über YubiKey (alle Geräte der Serie 4/5 oder YubiKey NEO/NFC)	Hier klicken.
über einen FIDO WebAuthn Authenticator	Hier klicken.

Mit Gerät anmelden

Wussten Sie, dass Sie sich mit einem sekundären Gerät anstatt Ihres Master-Passworts bei der Bitwarden-Web-App anmelden können? Die Anmeldung mit einem Gerät ist ein passwortloser Ansatz zur Authentifizierung, der die Notwendigkeit, Ihr Master-Passwort einzugeben, beseitigt, indem Authentifizierungsanfragen zur Genehmigung an alle bestimmten Geräte gesendet werden, bei denen Sie derzeit angemeldet sind. [Erfahren Sie mehr.](#)

Single Sign-on

Wenn Ihre Organisation [Zugangsdaten mit SSO](#) verwendet, können Sie auf Ihre Bitwarden-Web-App [mit Ihren föderierten SSO-Zugangsdaten](#) zugreifen.