bitwarden | Hilfezentrum Artikel

KONTOEINSTELLUNGEN > 2FA

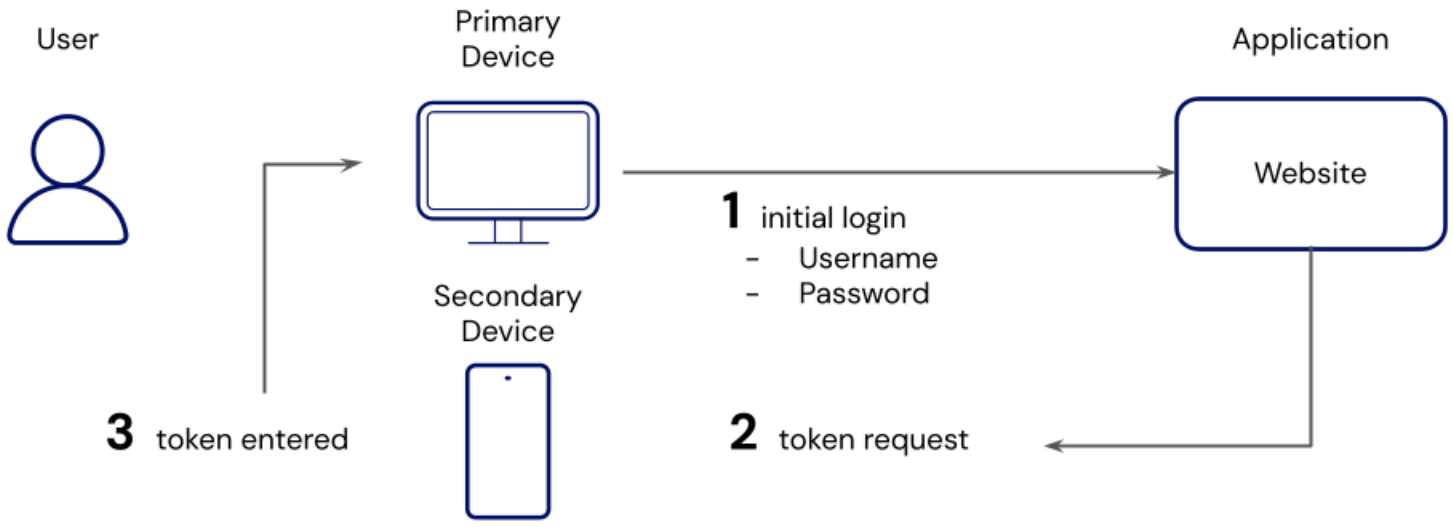
Feldführer-zum-Zwei-Schritt-Zugangsdaten

Ansicht im Hilfezentrum:
https://bitwarden.com/help/bitwarden-field-guide-two-step-login/

Feldführer-zum-Zwei-Schritt-Zugangsdaten

Zwei-Schritt-Zugangsdaten (auch als Zwei-Faktor-Authentifizierung oder 2FA bezeichnet) ist eine gängige Sicherheitstechnik, die von Websites und Apps verwendet wird, um Ihre sensiblen Daten zu schützen. Websites, die eine zweistufige Anmeldung verwenden, erfordern, dass Sie Ihre Identität verifizieren, indem Sie zusätzlich zum Benutzernamen und Passwort ein "Token" (auch Verifizierungscode oder Einmalpasswort (OTP)) eingeben, das normalerweise von einem anderen Gerät abgerufen wird.

Ohne physischen Zugang zum Token von Ihrem sekundären Gerät wäre ein bösartiger Akteur nicht in der Lage, auf die Website zuzugreifen, selbst wenn er Ihren Benutzernamen und Ihr Passwort entdeckt:



Grundlegender Zwei-Schritte-Zugangsdaten-Fluss

Häufig versuchen Websites oder Apps mit sensiblen Daten (zum Beispiel Ihr Online-Bank-Konto) Ihre Identität außerhalb des Zugangsdaten-Bildschirms zu verifizieren, indem sie:

- Ein Token in einer SMS / Textnachricht an das hinterlegte Mobilgerät senden.
- Anfrage nach einem von einer Authenticator-App (zum Beispiel Authy) auf Ihrem mobilen Gerät generierten Token.
- Suche nach einem Token von einem physischen Sicherheitsschlüssel (zum Beispiel, YubiKey).

Wie sollte ich die Zwei-Schritt-Zugangsdaten verwenden?

Sicherheit beinhaltet oft einen Kompromiss zwischen Schutz und Bequemlichkeit, also liegt es letztendlich bei Ihnen! Im Allgemeinen sind die zwei wichtigsten Methoden zur Verwendung von Zwei-Schritt-Zugangsdaten:

1. Um Bitwarden zu sichern

Sichern Sie alle Daten im Tresor, indem Sie bei jeder Anmeldung bei Bitwarden zusätzlich zur Eingabe Ihres Master-Passworts einen zweiten Schritt erfordern.

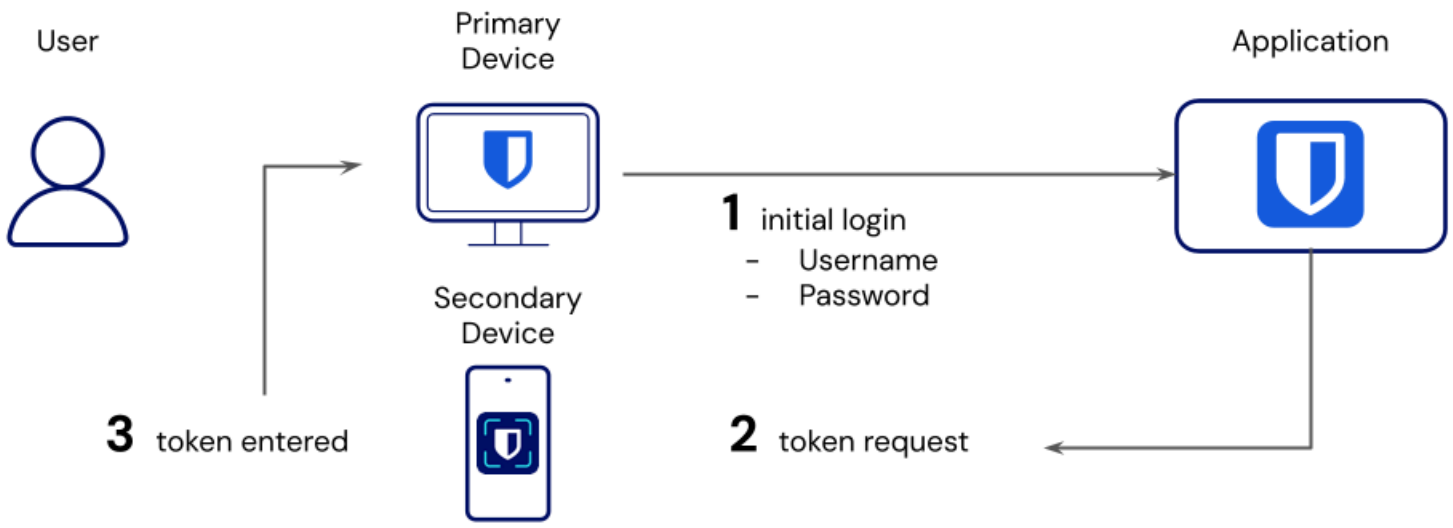
2. Um wichtige Websites zu sichern

   Sichern Sie eine einzelne Website, indem Sie ein temporäres Einmalpasswort (TOTP) benötigen, wenn Sie sich anmelden. Sie können TOTPs mit Bitwarden speichern und generieren.

Bitwarden sichern

Da Ihr Passwort-Manager alle Ihre Zugangsdaten speichert, empfehlen wir dringend, ihn mit einer Zwei-Schritt-Anmeldung zu sichern. Dies schützt alle Ihre Zugangsdaten, indem es einem bösartigen Akteur verhindert, auf Ihren Tresor zuzugreifen, selbst wenn er Ihr Master-Passwort entdeckt.

Die Aktivierung der zweistufigen Anmeldung erfordert von Ihnen, jedes Mal, wenn Sie sich anmelden, einen zusätzlichen Schritt zu absolvieren, zusätzlich zu Ihrer primären Anmeldemethode (Haupt-Passwort). Sie müssen Ihren zweiten Schritt nicht abschließen, um Ihren Tresor zu entsperren, nur um sich anzumelden.



Zwei-Schritt-Zugangsdaten um auf Bitwarden zuzugreifen

Bitwarden bietet mehrere kostenlose Methoden zur zweistufigen Anmeldung, darunter:

- FIDO (jeder FIDO2 WebAuthn zertifizierte Schlüssel)
- über eine Authenticator-App (zum Beispiel, 2FAS, Ravio oder Aegis)
- Premium-Methoden

Für Premium-Nutzer bietet Bitwarden mehrere fortschrittliche zweistufige Zugangsdaten-Methoden an:

- Duo-Sicherheit mit Duo-Push, SMS, Telefonanruf und Sicherheitsschlüsseln
- YubiKey (jedes 4/5 Serien-Gerät oder YubiKey NEO/NFC)

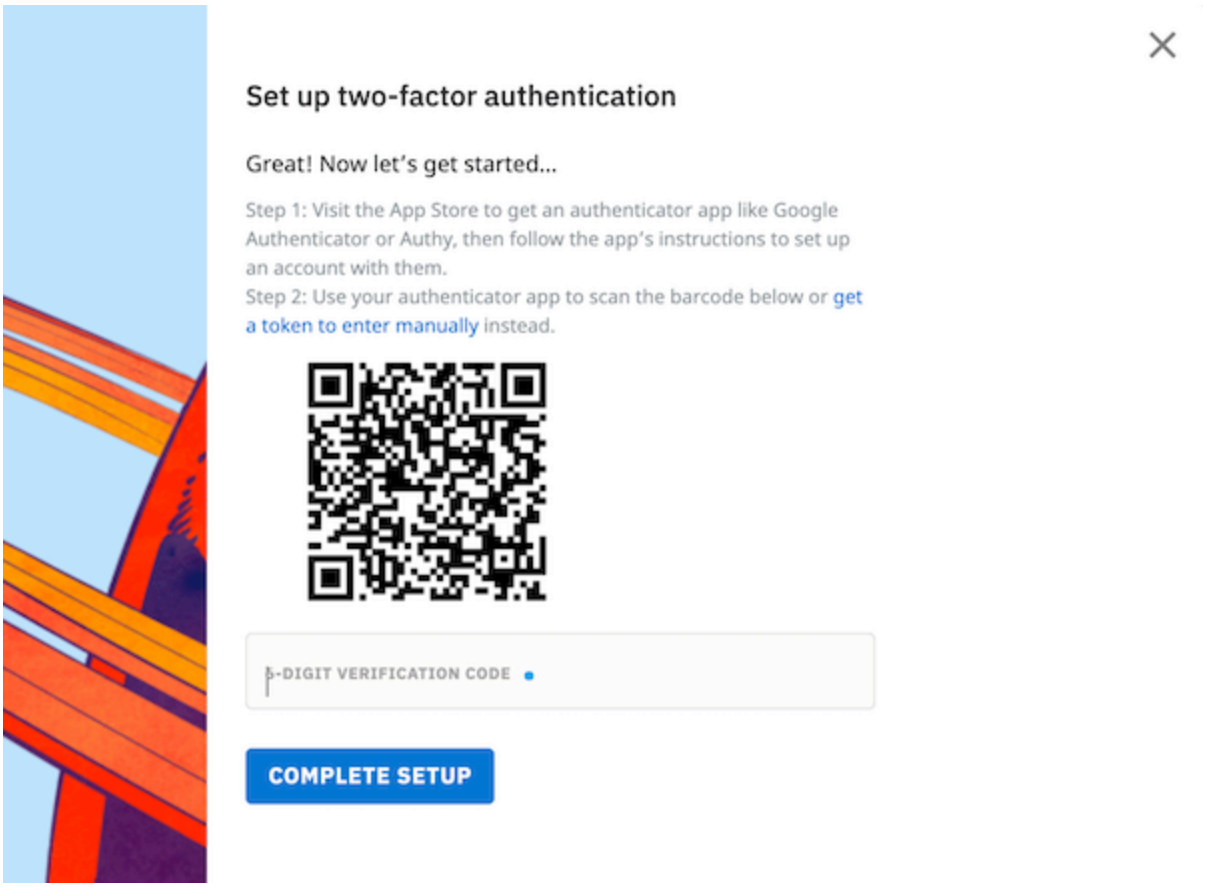
Erfahren Sie mehr über Ihre Optionen oder erhalten Sie hilfe bei der Einrichtung einer Methode mit unseren **Einrichtungsanleitungen.**

> **Note**
> Bitwarden unterstützt SMS 2FA aufgrund von Schwachstellen, einschließlich SIM-Hijacking, nicht. Wir empfehlen SMS 2FA für andere Konten nicht, es sei denn, es ist die einzige verfügbare Methode. Jeder zweite Faktor wird gegenüber keinem empfohlen, aber die meisten Alternativen sind sicherer als SMS 2FA.

Sicherung wichtiger Websites

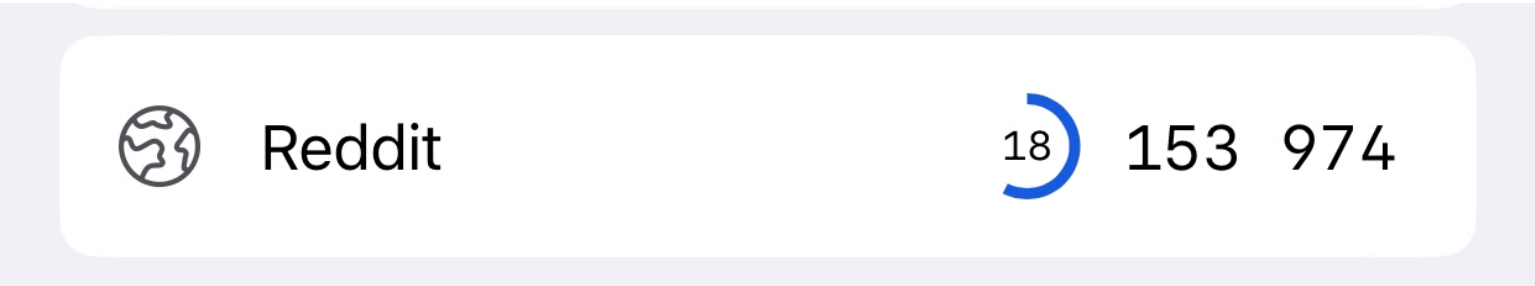
Viele andere Websites und Apps haben Optionen für die zweistufige Anmeldung, dies ist besonders häufig bei Websites, die sensible Informationen speichern (zum Beispiel Kreditkarten- oder Bankkontonummern). Die meisten Website-Zugangsdaten mit zwei Schritten finden Sie in den Menüs **Einstellungen**, **Sicherheit** oder **Datenschutz**.

Die Aktivierung der zweistufigen Zugangsdaten öffnet in der Regel einen QR-Code, wie dieses Beispiel von Reddit:



2FA QR-Code

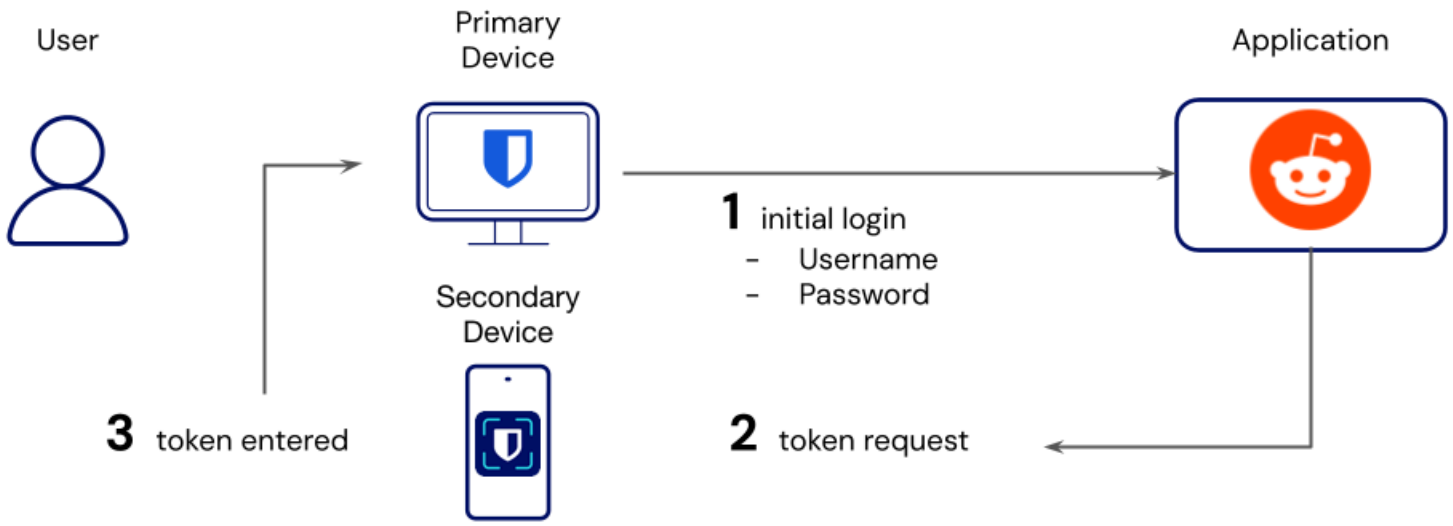
Das Scannen dieses Codes mit einer Authentifizierungs-App ermöglicht es der App, rotierende sechsstellige Token zu generieren, die Sie zur Überprüfung Ihrer Identität verwenden können, wie dieser von Authy generierte:



TOTP Token

Verwenden Sie Authy

Um die Zwei-Schritt-Anmeldung für Reddit mit Authy einzurichten, tippen Sie auf die Schaltfläche **Konto hinzufügen** und scannen Sie den von Ihrer Website oder App präsentierten QR-Code. Das Scannen des QR-Codes wird Ihren sechsstelligen Token generieren. Geben Sie diesen Code in das Eingabefeld **Verifizierungscode** ein, um die Einrichtung abzuschließen.



Zwei-Schritt-Zugangsdaten mit Authy

Normalerweise haben Sie die Möglichkeit, Wiederherstellungscodes herunterzuladen. Das Herunterladen von Wiederherstellungscodes ist entscheidend, um zu verhindern, dass Sie den Zugang zu Ihren Zwei-Schritt-Login-Tokens verlieren, selbst wenn Sie das Gerät verlieren, auf dem Authy installiert ist.

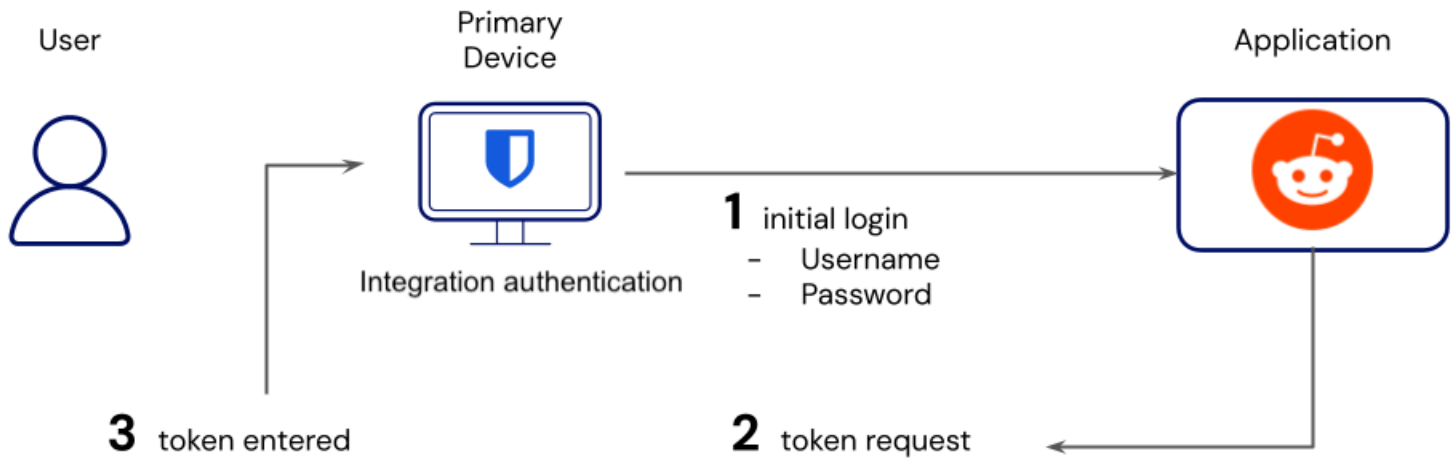
Das nächste Mal, wenn Sie sich bei Reddit mit Ihren Zugangsdaten anmelden, müssen Sie Ihre Identität bestätigen, indem Sie einen Verifizierungscode von Authy eingeben. Verifizierungscodes erneuern sich alle 30 Sekunden, daher wird es für einen bösartigen Akteur unmöglich sein, Ihren Code zu entdecken, ohne physischen Zugang zu Ihrem Gerät zu haben.

> **Note**
>
> Authy ist unsere empfohlene Authentifizierungs-App, weil sie Backups für jedes Gerät enthält. Backups verhindern, dass Sie den Zugang zu Ihren Token verlieren, selbst wenn Sie das Gerät verlieren, auf dem Authy installiert ist. Schalten Sie den **Authenticator-Backups** Schalter auf dem **Konten** Bildschirm der Authy App um, um diese Funktion zu nutzen.
>
> Andere Authentifizierungs-Apps beinhalten Google Authenticator und FreeOTP, und seit dem 7. Mai 2020 beinhaltet Google Authenticator die Portabilität von Verifizierungscodes über Android-Geräte.

Verwenden Sie den Bitwarden-Authentifikator

Als Alternative zu Authy bietet Bitwarden einen integrierten Authenticator für Premium-Nutzer an, einschließlich Mitgliedern von bezahlten Organisationen (Familien, Teams oder Unternehmen).

Bitwarden für iOS und Android kann QR-Codes scannen und sechsstellige Token generieren, genau wie andere Authentifizierungs-Apps. Die Verwendung des Bitwarden-Authentifikators zur Sicherung einer Website speichert ein rotierendes sechsstelliges Token mit diesem Zugangsdaten-Tresor-Eintrag. Sie können Ihren Verifizierungscode-Geheimnis auch manuell in einem Bitwarden-App-Eintrag im Tresor speichern.



Zwei-Schritt-Zugangsdaten mit Bitwarden

Lernen Sie, wie man den Bitwarden-Authentifikator verwendet.

Warum Bitwarden Authentifizierer verwenden?

Verständlicherweise sind einige Benutzer skeptisch, wenn es darum geht, Bitwarden für die Token-Authentifizierung zu verwenden. Denken Sie daran, dass Sicherheit oft einen Kompromiss zwischen Schutz und Bequemlichkeit erfordert, daher liegt die beste Lösung bei Ihnen. Im Allgemeinen nutzen Leute den Bitwarden-Authentifikator aus zwei Gründen:

1. **Bequemlichkeit**

   Wenn Sie Bitwarden Mobile Apps oder Browser-Erweiterungen verwenden, um einen Benutzernamen und ein Passwort automatisch auszufüllen, wird der Verifizierungscode automatisch in Ihre Zwischenablage kopiert, um das Einfügen zu erleichtern.

   Wenn Sie eine Browser-Erweiterung verwenden, können Sie das Tastaturkürzel für die Zugangsdaten (Windows: `Strg + Shift + L` / macOS: `Cmd + Shift + L`) zusammen mit dem Tastaturkürzel zum Einfügen (Windows: `Strg + V` / macOS: `Cmd + V`) für blitzschnelle Anmeldungen verwenden.

2. **Teilen**

   Für Organisationen ist ein großer Vorteil der Verwendung des Bitwarden-Authentifikators zur Token-Überprüfung die Möglichkeit, die Token-Generierung unter Teammitgliedern zu teilen. Dies ermöglicht es Organisationen, ihre Konten mit Zwei-Schritt-Zugangsdaten zu schützen, ohne die Möglichkeit für mehrere Benutzer, auf dieses Konto zuzugreifen, zu opfern oder die Koordination zwischen zwei Mitarbeitern zu erfordern, um Token auf unsichere Weise zu teilen.

2FA Sicherheitsschlüssel und Passwörter

FIDO2 Sicherheitsschlüssel sind eine beliebte und sichere Option, um 2FA zu Ihrem Bitwarden-Konto hinzuzufügen. Wenn Sie mit FIDO2 Sicherheitsschlüsseln nicht vertraut sind, sehen Sie auf der FIDO Alliance Website nach zusätzlichen Informationen bezüglich FIDO2.

Ein YubiKey-Gerät ist ein Sicherheitsschlüssel, der mit FIDO-Authentifizierungsprotokollen funktioniert und mehrere Anwendungsfälle haben kann. Zwei Anwendungen sind als 2FA Sicherheitsschlüssel, oder Passschlüssel.

- **2FA Sicherheitsschlüssel:** Die Verwendung eines YubiKey als 2FA Sicherheitsschlüssel fungiert als zusätzliches Gerät im Authentifizierungsprozess. Dies wird von einer weiteren primären Methode der Authentifizierung begleitet (wie zum Beispiel Master-Passwort). Der YubiKey Sicherheitsschlüssel muss physisch eingesteckt werden, um die Authentifizierungsinformationen bereitzustellen.

- **Passkey:** Ein Passkey ist ein Paar aus öffentlichen und privaten kryptographischen Schlüsseln, die zur Authentifizierung von Zugangsdaten verwendet werden. Anstatt einen Benutzernamen, ein Passwort und 2FA zu einem Konto hinzuzufügen, wird der Einzelpassschlüssel verwendet. Während der Passworterstellung kann der YubiKey als Passwort-Generator fungieren, um die für die Passwort-Zugangsdaten notwendigen öffentlichen und privaten Schlüssel zu generieren. Erfahren Sie mehr über die Verwendung eines YubiKey als Passwort hier.

Mit Bitwarden ist die primäre Verwendung eines Sicherheitsschlüssels wie eines YubiKey-Geräts die Bereitstellung von 2FA-Authentifizierung.

Nächste Schritte

Jetzt, da Sie ein Experte für die Zwei-Schritt-Zugangsdaten sind, empfehlen wir:

- Zweistufige Zugangsdaten einrichten
- Erhalten Sie Premium für den Zugriff auf erweiterte zweistufige Zugangsdaten-Methoden
- Richten Sie den Bitwarden-Authentifizierer ein
- Richten Sie die Zwei-Schritt-Zugangsdaten für Teams und Unternehmen ein