

HILFE-CENTER

Mit dem Gerät anmelden

Mit dem Gerät anmelden

Wussten Sie, dass Sie sich bei Bitwarden mit einem sekundären Gerät anmelden können, anstatt Ihr Master-Passwort zu verwenden? Die Anmeldung mit einem Gerät ist ein passwortloser Ansatz zur Authentifizierung, der das Eingeben Ihres Master-Passworts unnötig macht, indem Authentifizierungsanfragen an jedes bestimmte Gerät gesendet werden, bei dem Sie derzeit angemeldet sind, zur Genehmigung. Erfahren Sie mehr über unsere Implementierung der Zero-Knowledge-Verschlüsselung.

Die Anmeldung mit dem Gerät kann im Web-Tresor, der Browser-Erweiterung, der Desktop-App und der mobilen App gestartet werden. Anfragen, die von diesen Apps gestellt werden, können auf mobilen Apps und Desktop-Apps genehmigt werden.


Bereiten Sie sich darauf vor, sich mit einem Gerät anzumelden

Um das Anmelden mit einem Gerät einzurichten:

- Melden Sie sich mindestens einmal normal in der initiierenden App (Web-Tresor, Browser-Erweiterung, Desktop oder mobile App) an, damit Bitwarden Ihr Gerät erkennen kann.

Hinweis

Die Verwendung des Inkognito-Modus oder des Privaten Surfens verhindert, dass Bitwarden Ihren Browser registriert, sodass Sie sich nicht mit einem Gerät in einem privaten Browserfenster anmelden können.

- Haben Sie ein anerkanntes Konto auf einer genehmigenden App (Mobil- oder Desktop-App). Die Erkennung eines Kontos erfordert, dass Sie sich erfolgreich auf diesem Gerät angemeldet haben.
- In der Genehmigungs-App öffnen Sie die  **Einstellungen** und schalten in der **Kontosicherheit** oder im **Sicherheit** Bereich die Option **Zugangsdaten-Anfragen genehmigen** ein.

📘 Hinweis

Wenn Sie als Mitglied einer Enterprise-Organisation der [Richtlinie-für-erforderliches-SSO](#) unterliegen, können Sie die Option **Mit-Gerät-anmelden** nicht nutzen. Sie müssen stattdessen [SSO verwenden, um sich anzumelden](#).

Mit einem Gerät anmelden

Auf dem Zugangsdaten-Bildschirm der initiiierenden App geben Sie Ihre E-Mail-Adresse ein und wählen Sie **Weiter**. Dann wählen Sie die Option **Mit Gerät anmelden**:

bitwarden

Log in or create a new account to access your secure vault.

Master password (required)

Get master password hint

Log in with master password

Log in with device

Enterprise single sign-on

Logging in as november@local.com

Not you?

© 2022 Bitwarden Inc.
Version 2022.10.2

Mit einem Gerät anmelden

Die Verwendung von **Mit Gerät anmelden** wird Authentifizierungsanfragen an alle mobilen oder Desktop-Apps senden, bei denen Sie derzeit angemeldet sind und die Option aktiviert haben, zur Genehmigung. Vergleichen Sie die Fingerabdruck-Phrasen auf dem initiiierenden und genehmigenden Client und wählen Sie, wenn sie übereinstimmen, **Zugangsdaten bestätigen** auf dem genehmigenden Gerät aus. Beachten Sie, dass dies

ein einzigartiger Fingerabdruck ist, der nicht mit Ihrer [Fingerabdruck-Phrase](#) für das Konto übereinstimmt.

Anfragen verfallen nach 15 Minuten, wenn sie nicht genehmigt oder abgelehnt werden. Wenn Sie keine Zugangsdaten-Anfragen erhalten oder F-Droid verwenden, versuchen Sie Ihren Tresor [manuell zu synchronisieren](#) von der mobilen App.

Hinweis

Wenn Sie die Option **Anmeldung mit Gerät** verwenden, müssen Sie immer noch jede derzeit aktive [Zwei-Schritt-Anmeldemethode](#) verwenden.

Wie-es-funktioniert

Wenn die Anmeldung mit einem Gerät eingeleitet wird:

1. Der initiiierende Client sendet eine POST-Anfrage, die die E-Mail-Adresse des Kontos, einen einzigartigen Authentifizierungsanforderungs-öffentlichen Schlüssel^a und einen Zugangscode enthält, an eine Authentifizierungsanforderungstabelle in der Bitwarden-Datenbank.
2. Registrierte Geräte, also mobile oder Desktop-Apps, die angemeldet sind und eine [gerätespezifische GUID](#) in der Bitwarden-Datenbank gespeichert haben, erhalten die Anfrage.
3. Wenn die Anfrage genehmigt wird, verschlüsselt der genehmigende Client den Master-Schlüssel und den Master-Passwort-Hash des Kontos mit dem im Antrag beigefügten öffentlichen Schlüssel der Auth-Anfrage.
4. Der genehmigende Client PUT dann den verschlüsselten Master-Schlüssel und den verschlüsselten Master-Passwort-Hash auf den Authentifizierungsanforderungsdatensatz und markiert die Anforderung als erfüllt.
5. Der initiiierende Client GETs den verschlüsselten Master-Schlüssel und den verschlüsselten Master-Passwort-Hash.
6. Der initiiierende Client entschlüsselt dann **lokal** den Master-Schlüssel und das Master-Passwort-Hash mit dem privaten Schlüssel der Auth-Anfrage.

7. Der initiierende Client verwendet dann den Zugangscode und die erfüllte Authentifizierungsanforderung, um den Benutzer mit dem Bitwarden-Identitätsservice zu authentifizieren.

- Auth-Anfrage öffentliche und private Schlüssel werden einzigartig für jede passwortlose Zugangsdaten Anfrage generiert und existieren nur so lange wie die Anfrage selbst. Anfragen verfallen und werden alle 15 Minuten aus der Datenbank gelöscht, wenn sie nicht genehmigt oder abgelehnt werden.