bitwarden | Hilfezentrum Artikel

PASSWORD MANAGER > VAULT BASICS

Aufbewahrung von Passschlüsseln

Ansicht im Hilfezentrum:
https://bitwarden.com/help/storing-passkeys/

Aufbewahrung von Passschlüsseln

Passschlüssel können mit dem Bitwarden Passwort-Manager-Tresor gespeichert und verwendet werden. Mit der Bitwarden-Browsererweiterung können sich Benutzer bei ihren bevorzugten Apps und Websites anmelden, die über eine Passkey-Anmeldefunktion verfügen. Passschlüssel sind eine sichere, passwortlose Alternative für Benutzer, sich geräteübergreifend bei Diensten anzumelden.

Passschlüssel wurden mit den von der FIDO-ALLIANZ festgelegten Standards entwickelt und ermöglichen es einem Benutzer, seine Konten zu sichern und die Schwachstellen zu umgehen, die mit der Standard-Passwortauthentifizierung einhergehen, wie z. B. Phishing. Die gespeicherten Passschlüssel sind mit der vertrauenswürdigen Ende-zu-Ende-Verschlüsselung von Bitwarden geschützt.

Was sind Passschlüssel?

Passschlüssel sind ein Ersatz für Passwörter, die schnelle, einfache und sichere Anmeldungen an Websites und Apps auf den Geräten eines Benutzers ermöglichen. Genauer gesagt ist "Passkey" ein verbraucherfreundlicher Begriff für eine auffindbare FIDO-ANMELDEINFORMATION, die synchronisiert werden kann, um sichere passwortlose Anmeldungen über Geräte hinweg zu ermöglichen, oder für eine einzelne Hardware als gerätegebundener Passkey.

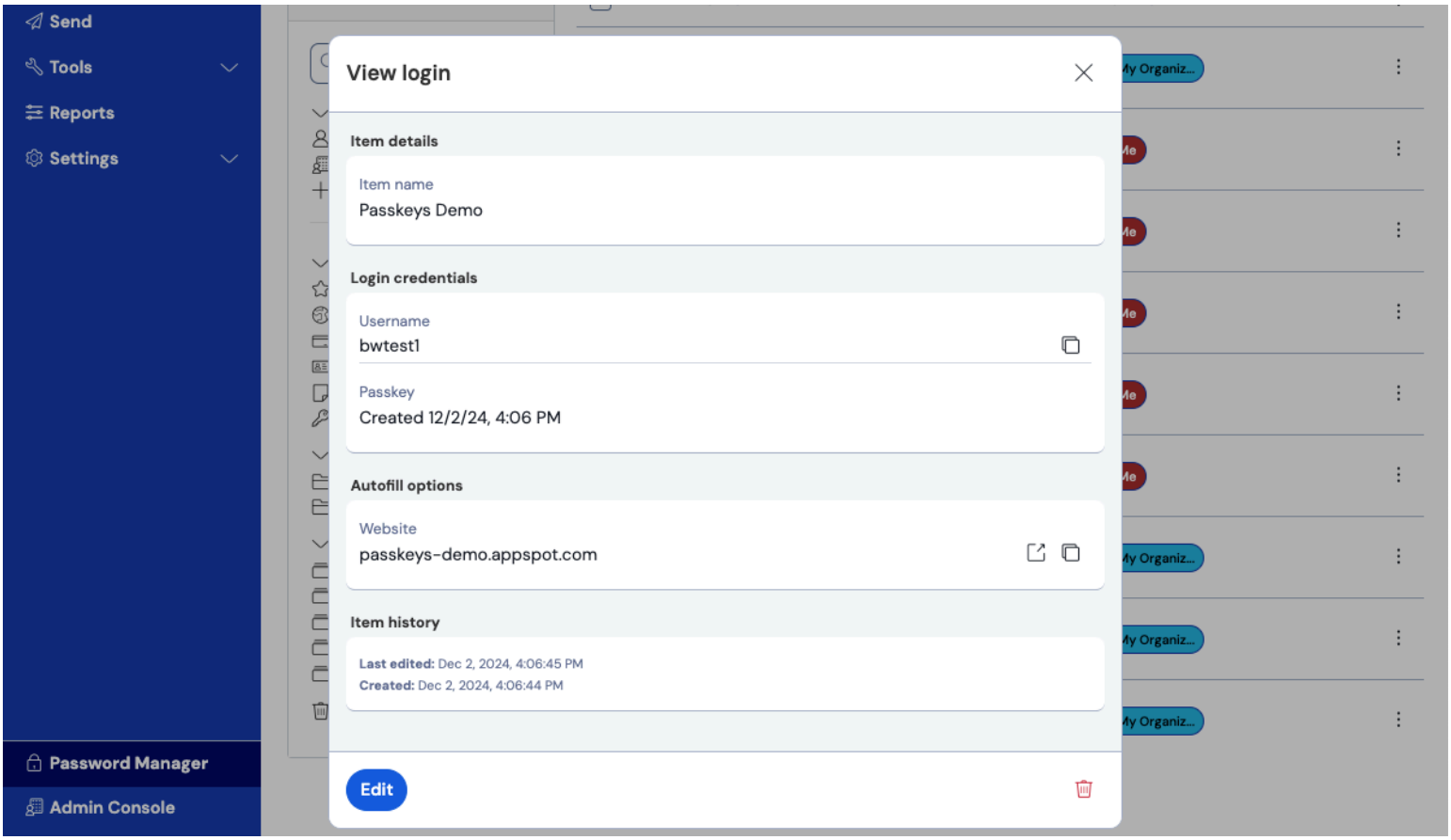
Apps und Dienste können verlangen, dass Passschlüssel, die mit ihnen erstellt wurden, mit einer PIN, einem Passwort, einem Muster oder einem biometrischen Faktor verifiziert werden, wenn Sie sie speichern oder darauf zugreifen. Der Bitwarden Password Manager wird in einer zukünftigen Version Unterstützung für PIN, Passwort und biometrische Überprüfung hinzufügen. Weitere allgemeine Informationen zu Passkeys finden Sie in den Passkey-FAQs.

Passschlüssel werden über die Browsererweiterung Bitwarden gespeichert und aufgerufen. Dies bedeutet, dass sowohl auffindbare als auch nicht auffindbare Passschlüssel in Bitwarden gespeichert und zum Anmelden bei Websites mit Passschlüssel-Funktionen verwendet werden können.

Passkey-Speicher

> **Note**
>
> Das Speichern und Verwenden von Passkeys ist eine Funktion der Bitwarden-Browsererweiterung. Andere Bitwarden-Clients können verwendet werden, um den gespeicherten Passkey anzuzeigen.

Im Bitwarden-Tresor wird nun in einem neuen Feld ein gespeicherter Passkey angezeigt. Sobald ein neuer Passkey gespeichert wurde, kann das Element von jedem Bitwarden-Tresor aus angezeigt werden und befindet sich im Passkey-Feld.

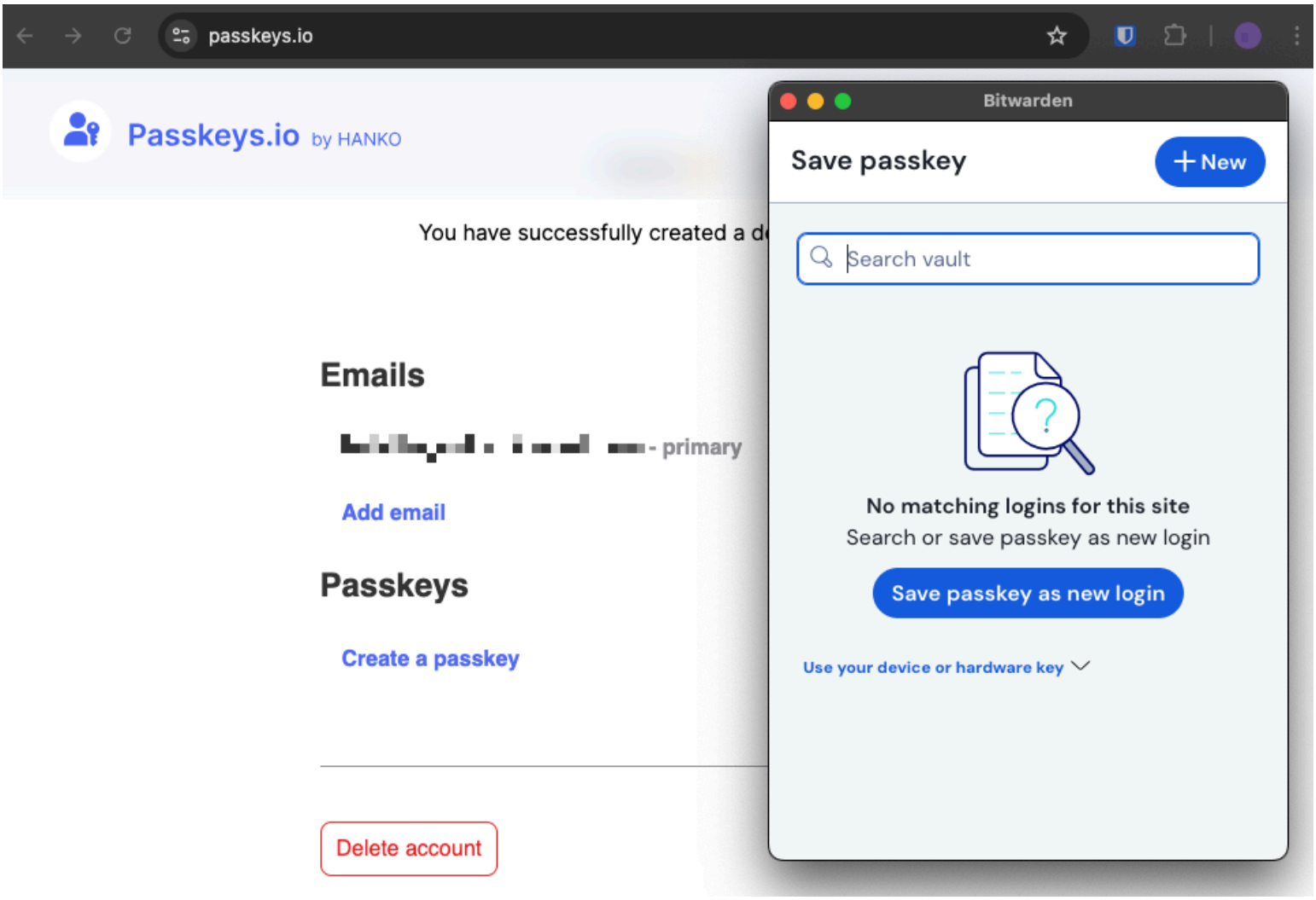


Passkey-Tresor-Gegenstand

Das Passkey-Feld kann nicht bearbeitet werden und enthält das Erstellungsdatum des Passschlüssels.

Neuen Passkey erstellen

Wenn Sie einen neuen Passkey auf einer Website oder App erstellen, werden Sie von Bitwarden aufgefordert, den Passkey in der Bitwarden-Browsererweiterung zu speichern.

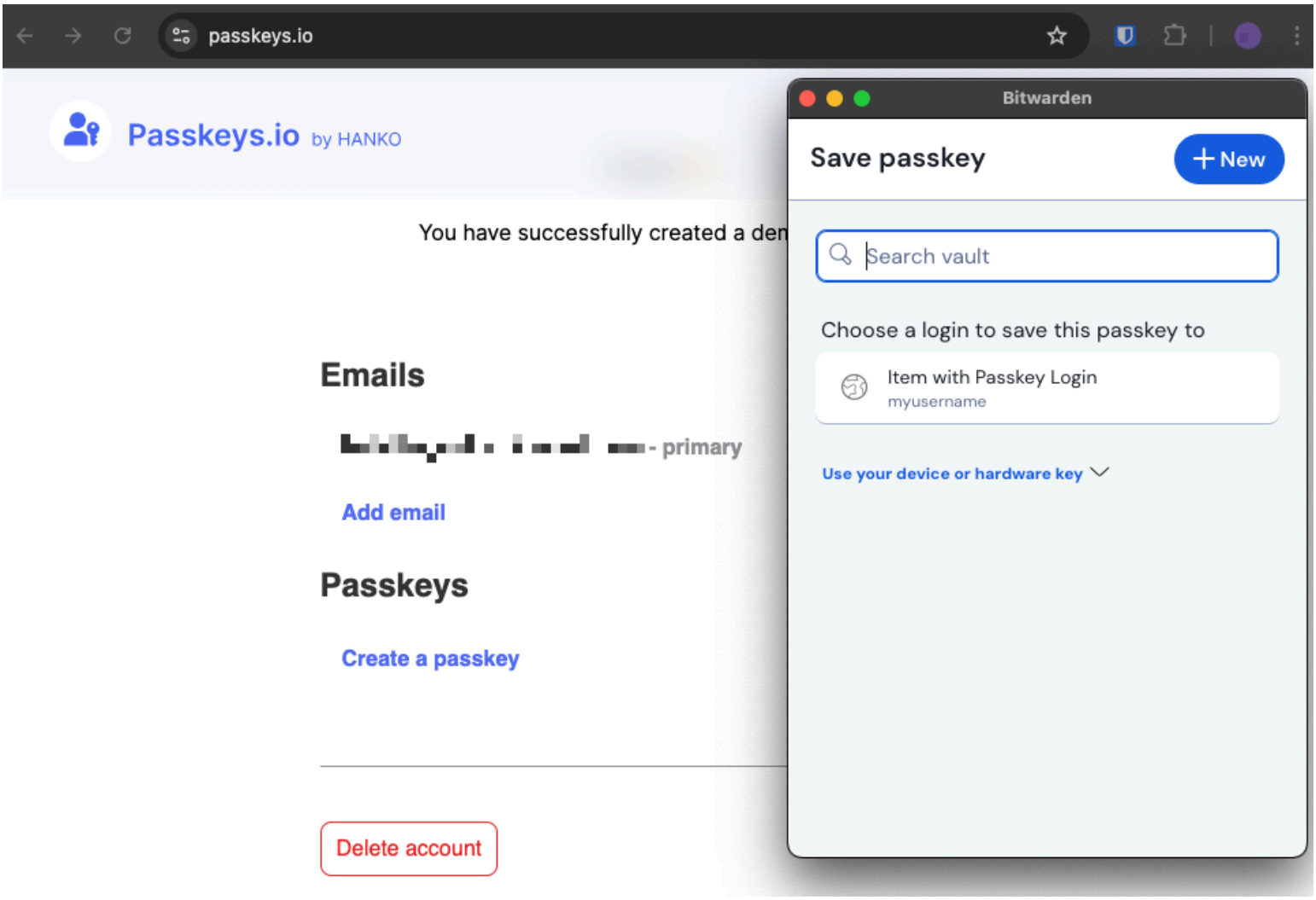


Passkey speichern

> **Note**
> Wählen **Sie Browser verwenden**, wenn Sie den Passkey nicht im Bitwarden-Tresor speichern möchten.

Wenn bereits ein Passkey für diesen Dienst vorhanden ist, benachrichtigt Sie die Browsererweiterung und ermöglicht es Ihnen, einen neuen Passkey zu speichern, indem Sie ┼ das Symbol auswählen, oder einen vorhandenen Passkey zu überschreiben.

> **Note**
> Pro Login-Artikel kann nur ein Passkey gespeichert werden. Wenn ein Anmeldedaten an mehreren Stellen gespeichert wird, z. B. als zwei separate Anmeldeelemente im einzelnen Tresor bzw. Organisations-Tresor, kann mit jedem Anmeldeelement ein anderer Passkey gespeichert werden.



Passwort mit vorhandenem Login speichern

So überschreiben Sie einen vorhandenen Passkey:

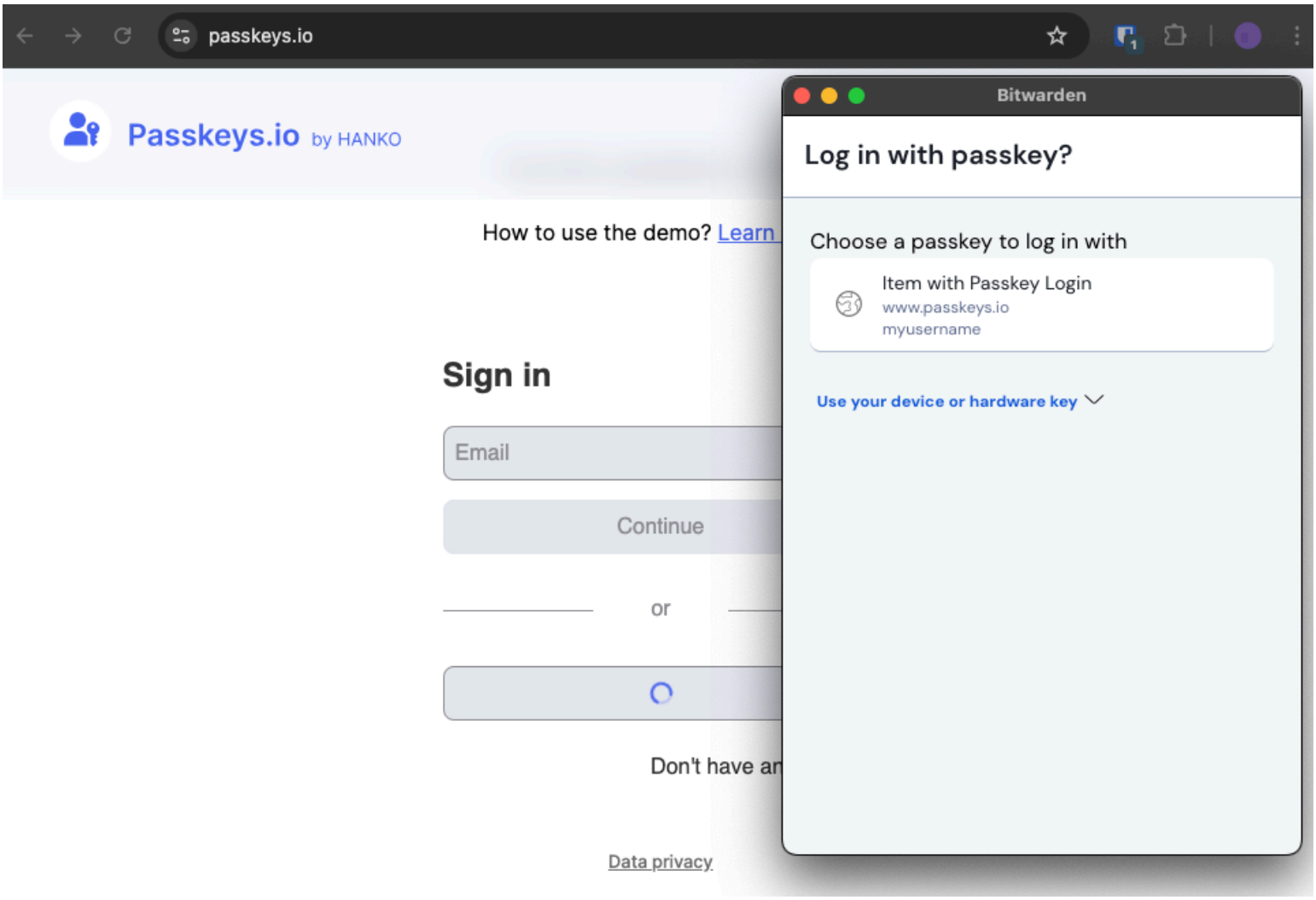
1. Initiieren Sie die Erstellung eines neuen Passschlüssels von Ihrer gewählten Website oder Dienstleistung.
2. Wählen Sie das vorhandene Login-Element aus, in dem Sie den neuen Passkey speichern möchten, und wählen Sie **Passkey speichern**.

Testen Sie es hier https://demo.yubico.com/playground.

> **Note**
> Das Passkey-Feld kann nicht in der Vault-Elementansicht bearbeitet werden. Wenn ein zusätzlicher Passkey mit derselben Website benötigt wird, speichern Sie ein neues Login-Element mit dem neuen zugeordneten Passkey.

Melden Sie sich mit einem in Bitwarden gespeicherten Passkey bei einer Website an

Um einen in Bitwarden gespeicherten Passkey zu verwenden, initiieren Sie die Passkey-Anmeldung auf der Website. Ihr System wird Sie zur Passkey-Anmeldung auffordern. Während Bitwarden aktiviert ist, bietet die Bitwarden-Browsererweiterung die Möglichkeit, sich mit dem in Ihrem Bitwarden-Tresor gespeicherten Passkey anzumelden.



Mit Passkey anmelden

Zugehörige Passschlüssel werden im Bitwarden-Dialogfeld angezeigt. Wählen Sie den Passkey aus, den Sie verwenden möchten, und drücken Sie auf **Bestätigen**.

> **Note**
> Wenn die Aufforderung zur erneuten Eingabe des Master-Passworts für das Anmeldeelement aktiviert wurde, müssen Sie Ihr Master-Passwort erneut eingeben, um auf den Passschlüssel zugreifen zu können.

Passkey-Eingabeaufforderung deaktivieren

Wenn Sie die Bitwarden-Browsererweiterung nicht verwenden möchten, um Sie aufzufordern, Passschlüssel für bestimmte Websites zu speichern und zu verwenden, können Sie ausgeschlossene Domains festlegen. Sie können die Eingabeaufforderung auch vollständig deaktivieren, indem Sie:

1. Navigieren Sie zur Registerkarte **Einstellungen**.
2. Auswählen von **Optionen.**
3. Deaktivieren **Sie die Option Zum Speichern und Verwenden von Passschlüsseln auffordern**.

Häufig gestellte Fragen zum Passkey-Management

Die folgenden FAQ-Elemente beziehen sich auf die Bitwarden-Passschlüssel-Speicherung. Allgemeine Passkey-Informationen finden Sie in den Passkey-FAQs.

F: Werden Passschlüssel enthalten sein, wenn Sie einen Tresorgegenstand klonen?

A: Bitwarden kopiert keinen Passkey, wenn eine Klonaktion abgeschlossen wird.

F: Sind gespeicherte Passschlüssel in Bitwarden-Importen und -Exporten enthalten?

A: Passkey-Importe und -Exporte werden in einer zukünftigen Version enthalten sein.

F: Kann ich Passschlüssel in der mobilen App speichern?

A: Die Passkeys-Unterstützung für mobile Anwendungen ist für eine zukünftige Version geplant.