bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE > MEHR

Teams und Enterprise Migrationsleitfaden

Ansicht im Hilfezentrum:
https://bitwarden.com/help/teams-enterprise-migration-guide/

Teams und Enterprise Migrationsleitfaden

Die sichere Migration Ihrer Organisation mit Bitwarden ist unkompliziert und sicher. Befolgen Sie einfach die Schritte in diesem Leitfaden, um Daten und Benutzer von Ihrem bestehenden Passwort-Manager zu migrieren:

1. Exportieren Sie Ihre Daten .
2. Erstellen und konfigurieren Sie Ihre Bitwarden Organisation.
3. Importieren Sie Ihre Daten in Bitwarden .
4. Integrieren Sie Ihre Benutzer .
5. Konfigurieren Sie den Zugriff auf Sammlungen und Tresor-Einträge.

> **Tip**
> If you need assistance during your migration, our Customer Success team is here to help!

Reichweite

Dieses Dokument beschreibt die Best Practices für die Migration sicherer Daten von Ihren aktuellen Passwort-Managern zu einer Bitwarden Teams- oder Enterprise-Organisation und zum Aufbau einer Sicherheitsinfrastruktur auf der Grundlage einfacher und skalierbarer Methoden.

Die Verwaltung von Passwörtern ist entscheidend für die organisatorische Sicherheit und betriebliche Effizienz. Einblick in die besten Methoden zur Durchführung von Migration und Konfiguration zu geben, ist darauf ausgelegt, den oft notwendigen Versuch-und-Irrtum-Ansatz beim Austausch von Enterprise-Tools zu minimieren.

Die Schritte in diesem Dokument **sind in der empfohlenen Reihenfolge aufgelistet**, um eine einfache Handhabung und einen reibungslosen Einstieg für die Benutzer zu gewährleisten.

Schritt 1: Exportieren Sie Ihre Daten

Der Export von Daten aus einem anderen Passwort-Manager wird für jede Lösung unterschiedlich sein und in einigen Fällen vielleicht ein bisschen knifflig sein. Verwenden Sie einen unserer Import & Export Leitfäden zur Hilfe, zum Beispiel beim Exportieren von Lastpass oder 1Password.

Das Sammeln eines vollständigen Exports Ihrer Daten kann erfordern, dass gemeinsam genutzte Ordner oder Einträge einem einzelnen Benutzer für den Export zugewiesen werden, oder dass mehrere Exporte zwischen Benutzern mit entsprechenden Berechtigungen durchgeführt werden. Zusätzlich können exportierte Daten individuell besessene Daten neben gemeinsamen/organisatorischen Daten enthalten, daher sollten Sie sicherstellen, dass Sie individuelle Einträge aus der Exportdatei entfernen, bevor Sie zu Bitwarden importieren.

> **Note**
>
> We recommend paying special attention to the location of the following types of data during export:
>
> - Secure documents
> - Secure file attachments
> - Secure notes
> - SSH / RSA key files
> - Shared folders
> - Nested shared items
> - Any customized structures within your password management infrastructure

Schritt 2: Richten Sie Ihre Organisation ein

Bitwarden Organisationen verknüpfen Benutzer und Tresor-Einträge für das sichere Teilen von Zugangsdaten, Notizen, Karten und Identitäten.

> **Tip**
>
> It's important that you create your organization first and import data to it directly, rather than importing the data to an individual account and then moving items to the organization secondarily.

1. **Erstellen Sie Ihre Organisation**. Beginnen Sie mit der Gründung Ihrer Organisation. Um zu lernen wie, schauen Sie sich diesen Artikel an.

   > **Note**
   >
   > To self-host Bitwarden, create an organization on the Bitwarden cloud, generate a license key, and use the key to unlock organizations on your server.

2. **Administrative Benutzer an Bord**. Mit Ihrer erstellten Organisation können weitere Einrichtungsverfahren durch das Onboarding einiger administrativer Benutzer erleichtert werden. Es ist wichtig, dass Sie zu diesem Zeitpunkt **nicht mit der Einführung der Endbenutzer beginnen**, da es noch einige Schritte zur Vorbereitung Ihrer Organisation gibt. Lernen Sie, wie Sie Administratoren hier einladen können.

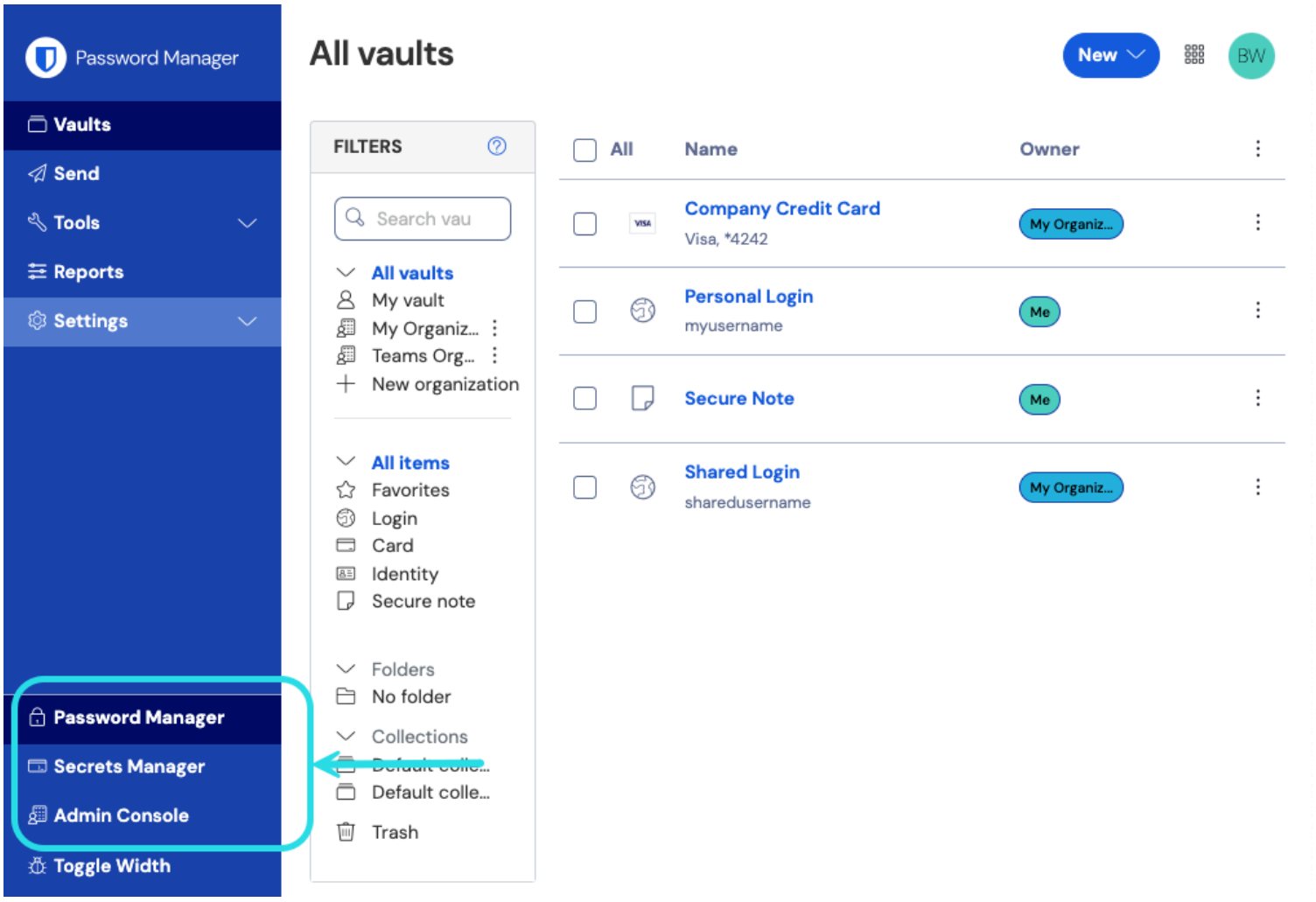
3. **Konfigurieren Sie Identitätsservices**. Enterprise-Organisationen unterstützen das Anmelden mit Single Sign-On (SSO) entweder über SAML 2.0 oder OpenID Connect (OIDC). Um SSO zu konfigurieren, öffnen Sie die **Einstellungen** → **Single Sign-On** Seite der Organisation im Administrator-Konsole, zugänglich für Eigentümer und Administratoren der Organisation.

4. **Aktivieren Sie die Enterprise-Richtlinien**. Enterprise-Richtlinien ermöglichen es Organisationen, Regeln für Benutzer zu implementieren, zum Beispiel die Verwendung von zweistufigen Zugangsdaten zu erfordern. Es wird dringend empfohlen, dass Sie Richtlinien konfigurieren, bevor Sie Benutzer einbinden.

Schritt 3: Import in Ihre Organisation

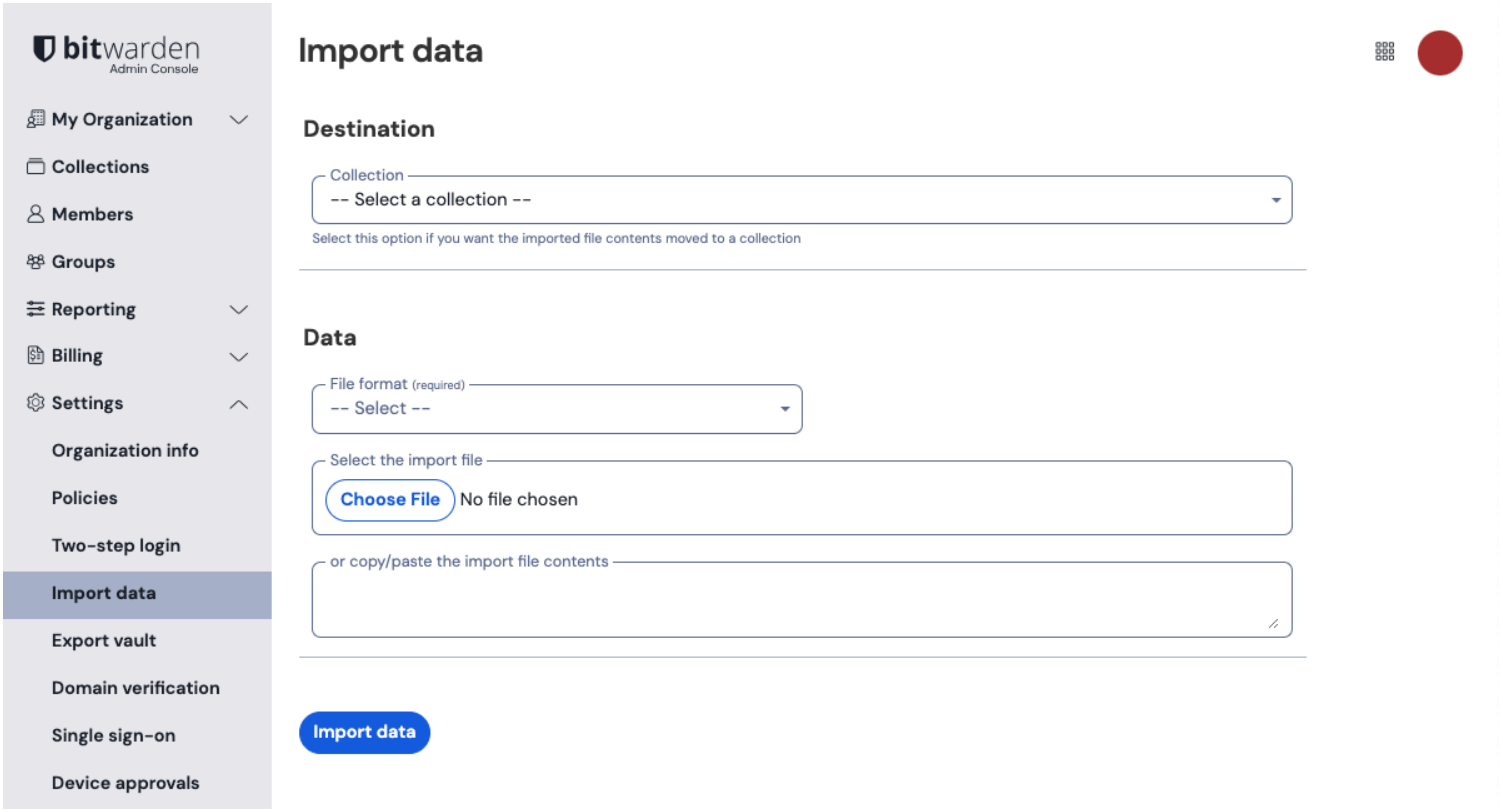
Um Daten in Ihre Organisation zu importieren:

1. Melden Sie sich bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktumschalter (⊞):



Produktwechsler

2. Navigieren Sie zu **Einstellungen** → **Daten importieren**:



Administrator Konsole Import

3. Wählen Sie aus dem Format-Dropdown ein **Dateiformat** aus (siehe Import-Empfehlungen unten).

4. Wählen Sie die Schaltfläche **Datei auswählen** und fügen Sie die Datei zum Import hinzu.

> **⚠ Warning**
>
> Import to Bitwarden can't check whether items in the file to import are duplicative of items in your vault. This means that **importing multiple files will create duplicative** vault items if an item is already in the vault and in the file to import.

5. Wählen Sie die Schaltfläche **Daten importieren**, um Ihren Import abzuschließen.

Derzeit sind Dateianhänge nicht in Bitwarden Importoperationen enthalten und müssen manuell in Ihren Tresor hochgeladen werden. Für weitere Informationen, siehe Dateianhänge.

> **Tip**
>
> You should also recommend to employees that they export their individually-owned data from your existing password manager and prepare it for import into Bitwarden. Learn more here.

Importempfehlungen

Beim Import von Daten in Ihre Organisation haben Sie zwei Optionen:

1. Um das Standard-Dateiformat von Ihrem vorherigen Passwort-Manager zu importieren.

2. Um eine Bitwarden-spezifische `.CSV` für den Import zu konditionieren.

Wir empfehlen, Ihre Datei für den Import als Bitwarden `.CSV` für beste Ergebnisse zu formatieren, oder für fortgeschrittene Benutzer, als Bitwarden `.JSON` Datei. Für Anweisungen zur Erstellung einer Bitwarden-spezifischen Importdatei, verweisen Sie auf diesen Import-Leitfaden.

Schritt 4: Nutzer einbinden

Bitwarden unterstützt manuelles Onboarding über den Web-Tresor und automatisches Onboarding durch SCIM-Integrationen oder Synchronisation von Ihrem bestehenden Verzeichnisdienst:

Manuelle Einarbeitung

Um die Sicherheit Ihrer Organisation zu gewährleisten, wendet Bitwarden einen 3-Schritte-Prozess für die Einarbeitung eines neuen Mitglieds an, einladen → akzeptieren → bestätigen. Lernen Sie, wie Sie neue Benutzer hier einladen können.

Automatisierte Einarbeitung

Automatisiertes Onboarding von Benutzern ist verfügbar durch SCIM-Integrationen mit Azure AD, Okta, OneLogin und JumpCloud, oder unter Verwendung von Directory Connector, einer eigenständigen Anwendung, die in einer Desktop-App und einem CLI-Tool verfügbar ist, das Benutzer und Gruppen aus Ihrem bestehenden Verzeichnisdienst synchronisiert.

Unabhängig davon, welche Methode Sie verwenden, werden Benutzer automatisch eingeladen, der Organisation beizutreten und können manuell oder automatisch mit dem Bitwarden CLI Tool bestätigt werden.

Schritt 5: Konfigurieren Sie den Zugriff auf Sammlungen und Einträge

Teilen Sie Tresor-Einträge mit Ihren Endbenutzern, indem Sie den Zugriff über Sammlungen, Gruppen und Gruppen- oder Benutzerebene-Berechtigungen konfigurieren:

Sammlungen

Bitwarden ermöglicht es Organisationen, sensible Daten einfach, sicher und auf skalierbare Weise zu teilen. Dies wird erreicht, indem gemeinsame Geheimnisse, Einträge, Zugangsdaten usw. in **Sammlungen** segmentiert werden.

Sammlungen können sichere Einträge auf viele Arten organisieren, einschließlich nach Geschäftsfunktion, Gruppenzuweisung, Zugriffsstufen für Anwendungen oder sogar Sicherheitsprotokollen. Sammlungen fungieren als gemeinsame Ordner, die eine konsistente Zugriffskontrolle und gemeinsame Nutzung unter Gruppen von Benutzern ermöglichen.

Geteilte Ordner von anderen Passwort-Managern können als Sammlungen in Bitwarden importiert werden, indem die Organisation Importvorlage verwendet wird, die unter Typ: Asset-Hyperlink-ID: 4DdJLATeuhMYIE581pPErF gefunden werden kann und indem der Name des geteilten Ordners in die `Sammlung` Spalte eingefügt wird, zum Beispiel durch Umwandlung:

url	username	password	extra	name	grouping	fav
https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8		Azure Login	Shared-Systems	0
https://github.com/login	GitHubUser	P4JUghjRfhKrDJ		Github	Shared-Systems	0
https://adobe.com	AdobeUser	T6RYSbD5mn78ab		Adobe Login	Shared-Design	0
https://shutterstock.com	ShutterStock	749bs2saWb3bxH		Shutterstock	Shared-Design	0
https://usps.com	USPSUser	6UmtWLkGydBMaZ		USPS Shipping	Shared-Shipping	0
https://ups.com	UPSUser	YBD7ftBZbosS9u		UPS Login	Shared-Shipping	0
https://fedex.com	FedexUser	y44xgs5fiyYZNU		FedExUser	Shared-Shipping	0

Migration Export Example

hinein:

collections	type	name	notes	fields	login_uri	login_username	login_password	login_totp
Shared-Systems	login	Azure Login			https://azure.microsoft.com/en-us/	AzureUser	5HDXWtuAAK3SX8	
Shared-Systems	login	Github			https://github.com/login	GitHubUser	P4JUghjRfhKrDJ	
Shared-Design	login	Adobe Login			https://adobe.com	AdobeUser	T6RYSbD5mn78ab	
Shared-Design	login	Shutterstock			https://shutterstock.com	ShutterStock	749bs2saWb3bxH	
Shared-Shipping	login	USPS Shipping			https://usps.com	USPSUser	6UmtWLkGydBMaZ	
Shared-Shipping	login	UPS Login			https://ups.com	UPSUser	YBD7ftBZbosS9u	
Shared-Shipping	login	FedExUser			https://fedex.com	FedexUser	y44xgs5fiyYZNU	

Migration Import Example

Sammlungen können sowohl mit Gruppen als auch mit einzelnen Benutzern geteilt werden. Die Begrenzung der Anzahl einzelner Benutzer, die auf eine Sammlung zugreifen können, wird das Verwalten für Administratoren effizienter machen. Mehr dazu erfahren Sie hier.

Gruppen

Die Verwendung von Gruppen zum Teilen ist der effektivste Weg, um Zugang zu Anmeldedaten und Geheimnissen zu gewähren. Gruppen, wie Benutzer, können mit Ihrer Organisation über SCIM oder Directory Connector synchronisiert werden.

Berechtigungen

Berechtigungen für Bitwarden-Sammlungen können auf Gruppen- oder Benutzerebene zugewiesen werden. Das bedeutet, dass jede Gruppe oder Benutzer mit Berechtigungen für die gleiche Sammlung konfiguriert werden kann. Die Berechtigungen für die Sammlung beinhalten Optionen für **Schreibgeschützt** und **Passwörter verbergen**.

Bitwarden verwendet eine Vereinigung von Berechtigungen, um die endgültigen Zugriffsberechtigungen für einen Benutzer und einen Sammlungseintrag zu bestimmen (mehr erfahren). Zum Beispiel:

- Benutzer A ist Teil der Tier 1 Support Gruppe, die Zugang zur Support Sammlung hat, mit schreibgeschützter Berechtigung.
- Benutzer A ist auch ein Mitglied der Support-Verwaltungsgruppe, die Zugriff auf die Support-Sammlung hat, mit Lese-Schreib-Zugriff.
- In diesem Szenario wird Benutzer A in der Lage sein, zur Sammlung zu lesen und zu schreiben.

Unterstützung bei der Migration

Das Bitwarden Kundenerfolgsteam steht rund um die Uhr mit Prioritätsunterstützung für Ihre Organisationen zur Verfügung. Wenn Sie Hilfe benötigen oder Fragen haben, zögern Sie bitte nicht, uns zu kontaktieren.