

ADMINISTRATOR KONSOLE > MEHR

LastPass Enterprise Migrationsleitfaden

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/lastpass-enterprise-migration-guide/>

LastPass Enterprise Migrationsleitfaden

Die sichere Migration Ihrer Organisation mit Bitwarden ist unkompliziert und sicher. Befolgen Sie die Schritte in diesem Leitfaden, um Daten und Benutzer von LastPass zu migrieren:

1. Erstellen und konfigurieren Sie Ihre Bitwarden Organisation.
2. Importieren Sie Ihre Daten in Bitwarden .
3. Integrieren Sie Ihre Benutzer .
4. 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 besten Praktiken für die sichere Migration von Daten von Lastpass zu einer Bitwarden [Teams oder Enterprise Organisation](#), den Aufbau einer Sicherheitsinfrastruktur basierend auf einfachen und skalierbaren Methoden.

Die [Passwortverwaltung](#) ist für die Sicherheit des Unternehmens und die betriebliche Effizienz von entscheidender Bedeutung. Einblick in die besten Methoden zur Durchführung von Migration und Konfiguration zu geben, soll den oft notwendigen Versuch-und-Irrtum-Ansatz beim Austausch von Enterprise-Tools minimieren.

Die Schritte in diesem Dokument **sind in der empfohlenen Reihenfolge aufgelistet** für eine einfache Handhabung und reibungslose Einführung für Benutzer.

Schritt 1: Richten Sie Ihre Organisation ein

Bitwarden Organisationen verbinden Benutzer und Tresor-Einträge miteinander 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 Nutzer 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 im Admin-Konsole den Bildschirm der Organisation [Einstellungen](#) → [Single Sign-On](#), zugänglich durch [Organisation Eigentümer und Administratoren](#).
4. **Enterprise-Richtlinien aktivieren.** [Enterprise-Richtlinien](#) ermöglichen es Organisationen, Regeln für Benutzer zu implementieren, zum Beispiel die Verwendung von zweistufigen Zugangsdaten. Es wird dringend empfohlen, dass Sie Richtlinien konfigurieren, bevor Sie Benutzer einbinden.

Schritt 2: Daten importieren

Export aus LastPass

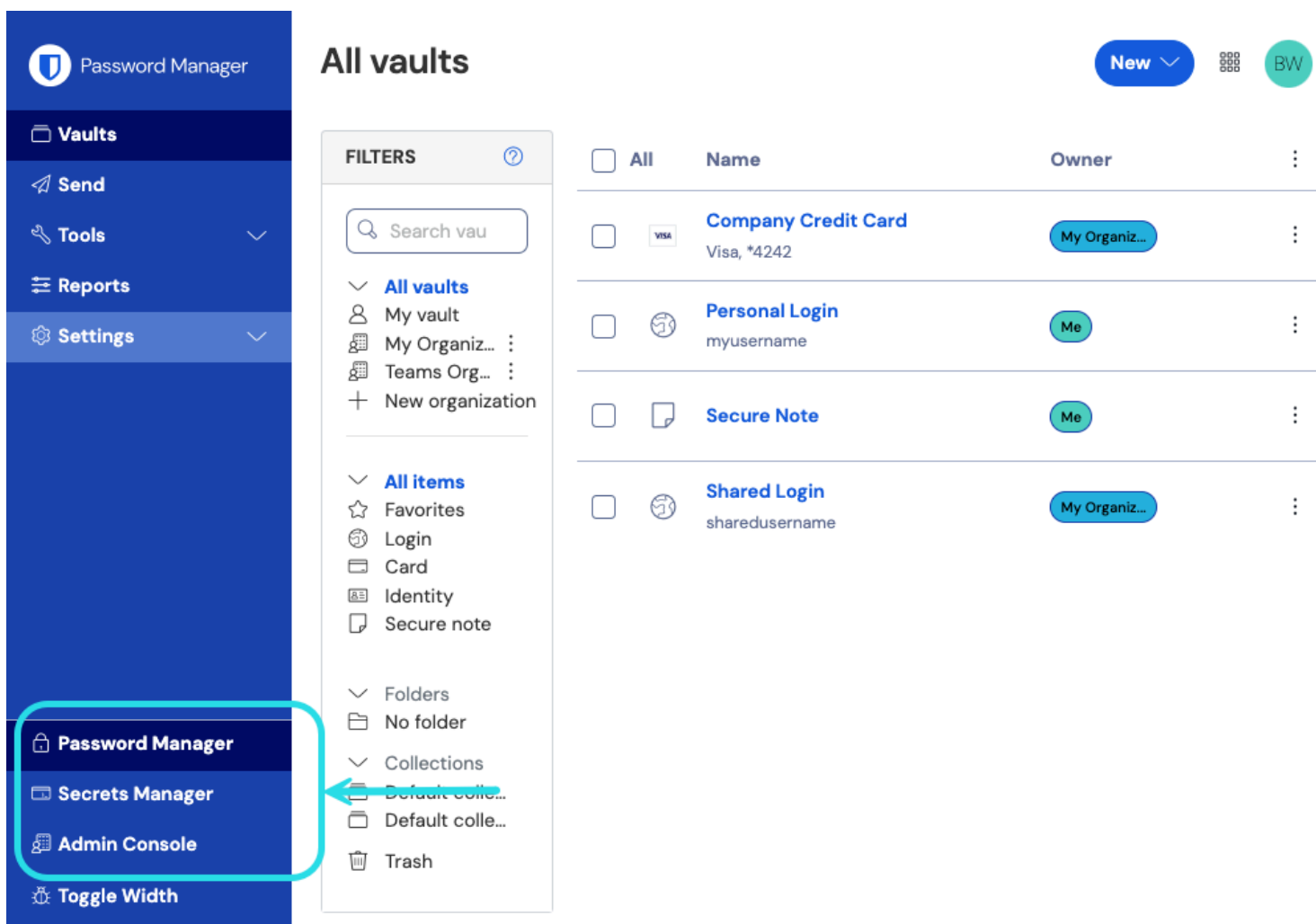
Erstellen Sie einen vollständigen Export aller Ihrer geteilten Daten aus dem LastPass-Web-Tresor als **.csv**-Datei ([lernen Sie, wie](#)). Das Sammeln eines vollständigen Exports kann erfordern, dass alle freigegebenen Ordner dem exportierenden Benutzer zugewiesen werden, bevor der Export erstellt wird.

Darüber hinaus enthält jeder in LastPass erstellte Export Daten sowohl aus Ihrem persönlichen Tresor als auch aus zugewiesenen freigegebenen Ordnern. In dieser Phase empfehlen wir, den von Ihnen erstellten Export zu prüfen, um sicherzustellen, dass er alle Ihre geteilten Daten enthält und keine persönlichen Daten.

In Bitwarden importieren

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 Produktschalter ():



Produktwechsler

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

3. Vervollständigen Sie die folgenden Felder aus den Dropdown-Menüs:

- **Sammlung:** Wählen Sie aus, ob Sie den importierten Inhalt in eine bestehende Sammlung verschieben möchten. In den meisten Fällen haben Sie keine Sammlungen in Bitwarden erstellt, da der Import dies für Sie erledigt, lassen Sie diese Option also leer.
- **Dateiformat:** Wählen Sie **Lastpass (csv)** aus.

4. Wählen Sie Datei auswählen und fügen Sie die Datei zum Import hinzu oder kopieren Sie den Inhalt Ihrer Datei in das Eingabefeld.

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 **Daten importieren**, um den Import auszulösen.

Dateianhänge müssen manuell in Ihren Tresor hochgeladen werden. Beachten Sie, dass geteilte Ordner, die in LastPass verschachtelt sind, als verschachtelte Sammlungen in Ihrer Bitwarden Organisation neu erstellt werden. Wenn jedoch in der "Eltern"-Sammlung keine Daten vorhanden sind, müssen Sie die Elternsammlung manuell mit einem passenden Namen erstellen.

 **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](#).

Schritt 3: Nutzer einbinden

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

Manuelle Einarbeitung Handbuch

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.

 **Tip**

Once users are onboarded, instruct them to import their personal data to Bitwarden using an exported file or, if their LastPass accounts are still active, using the **Direct import** method described [here](#).

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.

 **Tip**

Once users are onboarded, instruct them to import their personal data to Bitwarden using an exported file or, if their LastPass accounts are still active, using the **Direct import** method described [here](#).

Schritt 4: 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 ermächtigt Organisationen dazu, 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 Organisationen auf viele Arten sichern, einschließlich durch Geschäftsfunktionen, Gruppenzuweisungen, Zugriffsebenen für Anwendungen oder sogar Sicherheitsprotokolle. Sammlungen funktionieren wie gemeinsam genutzte Ordner und ermöglichen eine gleichbleibende Zugriffskontrolle und gemeinsame Nutzung unter Gruppen von Benutzern.

Geteilte Ordner von LastPass können als Sammlungen in Bitwarden importiert werden, indem man die Importvorlage der Organisation verwendet, die unter Typ: Asset-Hyperlink-ID: 4DdJLATEuhMYIE581pPErF gefunden werden kann und den Namen des geteilten Ordners in die **Sammlungen** Spalte einfügt.

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](#).

Note

Nested collections do not inherit the permissions of the top level collection. See [using groups](#) to designate permissions.

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 unterschiedlichen Berechtigungen für die gleiche Sammlung konfiguriert werden kann. Optionen für Sammlungsberechtigungen beinhalten Optionen:

- Darf anzeigen
- Darf anzeigen, Passwörter ausgenommen
- Darf bearbeiten
- Darf bearbeiten, Passwörter ausgenommen
- Gewähren Sie Zugang zu allen aktuellen und zukünftigen Sammlungen

Erfahren Sie mehr über Berechtigungen [hier](#). Bitwarden verwendet eine Vereinigung von Berechtigungen, um die endgültigen Zugriffsberechtigungen für einen Benutzer und eine Sammlung zu bestimmen. Zum Beispiel:

- Benutzer A ist Teil der Tier 1 Support Gruppe, die Zugang zur Support Sammlung hat, mit der Berechtigung zur Ansicht.
- Benutzer A ist auch ein Mitglied der Support-Verwaltungsgruppe, die Zugriff auf die Support-Sammlung hat, mit Bearbeitungszugriff.
- In diesem Szenario wird Benutzer A in der Lage sein, die Sammlung zu bearbeiten.

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](#).