

BEHEERCONSOLE > MEER

# LastPass Enterprise migratiegids

Weergeven in het Helpcentrum:

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

## LastPass Enterprise migratiegids

Een veilige migratie van uw organisatie met Bitwarden is eenvoudig en veilig. Volg de stappen in deze handleiding om gegevens en gebruikers te migreren vanuit LastPass:

1. Maak en configureer uw Bitwarden-organisatie.
2. Importeer je gegevens in Bitwarden.
3. Neem uw gebruikers in dienst.
4. Toegang tot collecties en kluisitems configureren.

### 💡 Tip

If you need assistance during your migration, our [Customer Success team](#) is here to help!

## Toepassingsgebied

Dit document beschrijft de best practices voor het veilig migreren van gegevens van Lastpass naar een Bitwarden [Teams of Enterprise-organisatie](#), waarbij een infrastructuur voor beveiliging wordt opgebouwd op basis van eenvoudige en schaalbare methoden.

[Wachtwoordbeheer](#) is cruciaal voor de beveiliging van organisaties en operationele efficiëntie. Het bieden van inzicht in de beste methoden om migratie en configuratie uit te voeren is bedoeld om de trial-and-error aanpak die vaak nodig is bij het uitwisselen van enterprise tools te minimaliseren.

De stappen in dit document staan **in de aanbevolen volgorde** voor gebruiksgemak en een soepele inwerkperiode voor gebruikers

## Stap 1: Stel je organisatie in

Bitwarden organisaties koppelen gebruikers en kluisitems aan elkaar voor [het veilig delen](#) van logins, notities, kaarten en identiteiten.

### 💡 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. **Creëer je organisatie.** Begin met het opzetten van je organisatie. Lees [dit artikel](#) om te leren hoe.

### 📌 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. **Administratieve gebruikers aan boord nemen.** Nu je organisatie is opgezet, kunnen verdere installatieprocedures worden vereenvoudigd door enkele [administratieve gebruikers](#) aan te melden. Het is belangrijk dat je nu **nog niet begint met het onboarden van eindgebruikers**, want er zijn nog een paar stappen te gaan om je organisatie voor te bereiden. Leer [hier](#) hoe je admins kunt uitnodigen.
3. **Identiteitsdiensten configureren.** Enterprise-organisaties ondersteunen [inloggen met eenmalige aanmelding](#) (SSO) met behulp van SAML 2.0 of OpenID Connect (OIDC). Om SSO te configureren, open het **Instellingen** → **Enkelvoudige aanmelding** scherm van de organisatie in de Beheerconsole, toegankelijk voor [organisatie-eigenaren en beheerders](#).

4. **Ondernemingsbeleid inschakelen.** Met [bedrijfsbeleid](#) kunnen organisaties regels implementeren voor gebruikers, bijvoorbeeld door het gebruik van tweestapslogin verplicht te stellen. Het wordt ten zeerste aangeraden om beleidsregels te configureren voordat gebruikers in dienst worden genomen.

## Stap 2: Gegevens importeren

### Exporteren vanuit LastPass

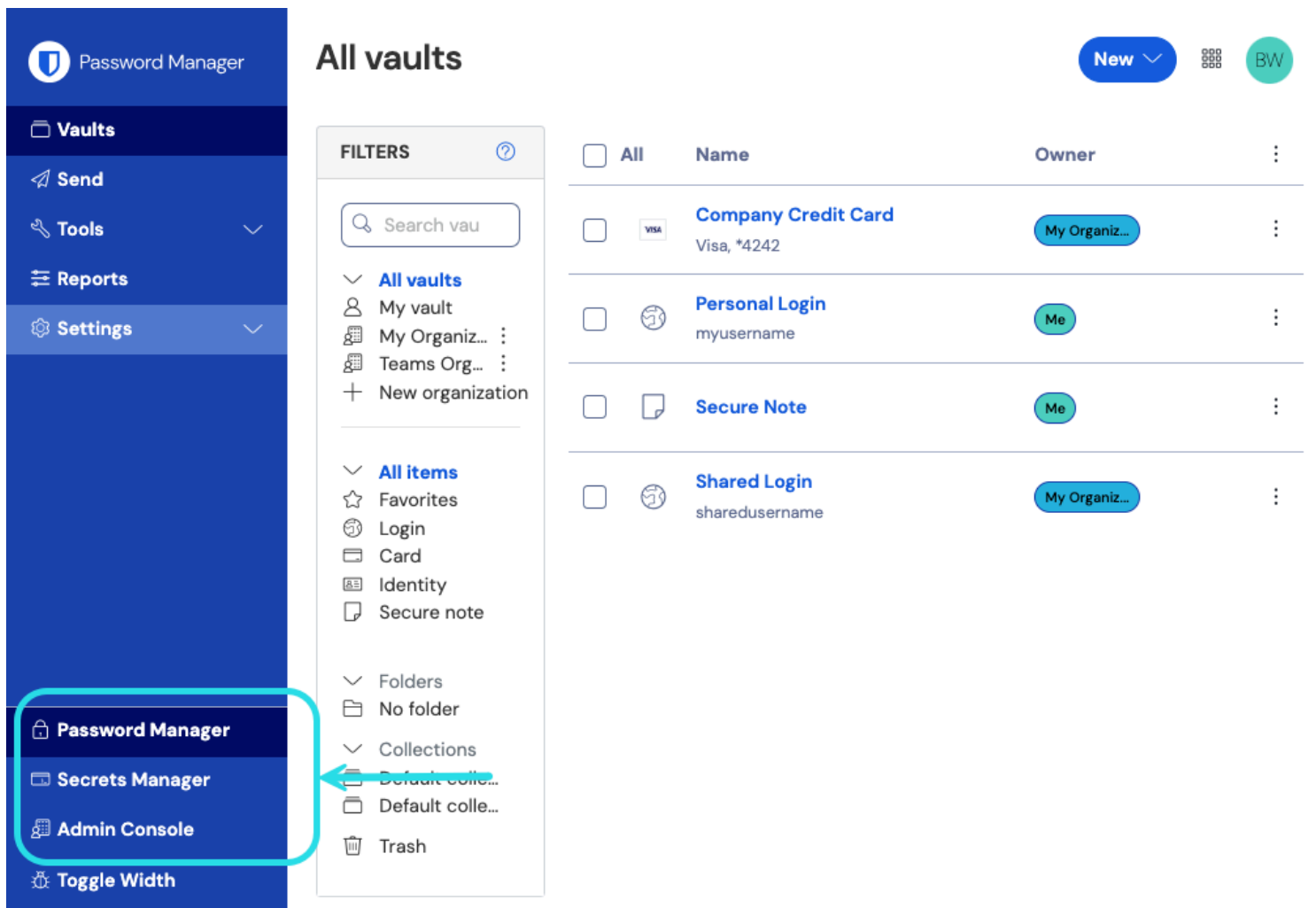
Maak een volledige export van al uw gedeelde gegevens van de LastPass-webkuis als een **.csv-bestand**([lees hier hoe](#)). Het verzamelen van een volledige export kan vereisen dat alle gedeelde mappen worden toegewezen aan de exporterende gebruiker voordat de export wordt gemaakt.

Bovendien zal elke export die in LastPass wordt gemaakt gegevens bevatten van zowel uw persoonlijke kuis als van toegewezen gedeelde mappen. In dit stadium raden we aan om de export die je hebt gemaakt te controleren om er zeker van te zijn dat deze al je gedeelde gegevens bevat en geen persoonlijke gegevens.

### Importeren naar Bitwarden

Om gegevens te importeren naar je organisatie:

1. Log in op de Bitwarden web app en open de Admin Console met behulp van de product switcher (☰):



Product switcher

2. Navigeer naar **Instellingen** → **Gegevens importeren**:

3. Vul de volgende velden in de vervolgkeuzemenu's in:

- **Collectie:** Selecteer of je de geïmporteerde inhoud wilt verplaatsen naar een bestaande collectie. In de meeste gevallen heb je geen collecties aangemaakt in Bitwarden omdat de import dat voor je doet, dus laat deze optie leeg.
- **Bestandsformaat:** Selecteer **Lastpass (csv)**.

4. Selecteer Kies bestand en voeg het te importeren bestand toe of kopieer+plak de inhoud van je bestand in het invoervak.

#### **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. Selecteer **Gegevens importeren** om het importeren te starten.

**Bestandsbijlagen** moeten handmatig worden geüpload naar je kluis. Merk op dat gedeelde mappen die genest zijn in LastPass opnieuw worden aangemaakt als geneste collecties in uw Bitwarden-organisatie, maar als er geen gegevens zijn in de "bovenliggende" collectie, moet u handmatig de bovenliggende collectie maken met een overeenkomende naam.

#### **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](#).

## Stap 3: Gebruikers aan boord nemen

Bitwarden ondersteunt handmatig onboarden via de webvault en geautomatiseerd onboarden via SCIM-integraties of synchronisatie vanuit uw bestaande directoryservice:

### Handmatig inwerken

Om de veiligheid van uw organisatie te waarborgen, past Bitwarden een 3-stappenproces toe voor het onboarden van een nieuw lid, uitnodigen → accepteren → bevestigen. Leer [hier](#) hoe je nieuwe gebruikers kunt uitnodigen.

#### **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](#).

### Geautomatiseerd inwerken

Geautomatiseerde onboarding van gebruikers is beschikbaar via SCIM-integraties met [Azure AD](#), [Okta](#), [OneLogin](#) en [JumpCloud](#), of met [Directory Connector](#), een standalone toepassing die beschikbaar is als [desktop-app](#) en [CLI-tool](#) waarmee gebruikers en groepen uit uw bestaande directoryservice worden gesynchroniseerd.

Welke u ook gebruikt, gebruikers worden automatisch uitgenodigd om lid te worden van de organisatie en kunnen handmatig of automatisch worden bevestigd met de [Bitwarden CLI-tool](#).

 **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](#).

## Stap 4: Toegang tot collecties en items configureren

Deel kluisitems met je eindgebruikers door toegang te configureren via collecties, groepen en machtigingen op groepsniveau of gebruikersniveau:

### Collecties

Bitwarden stelt organisaties in staat om gevoelige gegevens eenvoudig, veilig en schaalbaar te delen. Dit wordt bereikt door gedeelde geheimen, items, logins, etc. te segmenteren in **verzamelingen**.

Collecties kunnen beveiligde items op veel manieren organiseren, bijvoorbeeld op basis van bedrijfsfunctie, groepstoewijzing, toegangsniveaus voor applicaties of zelfs beveiligingsprotocollen. Collecties functioneren als gedeelde mappen, waardoor een consistente toegangscontrole en delen tussen groepen gebruikers mogelijk is.

Gedeelde mappen van LastPass kunnen als collecties worden geïmporteerd in Bitwarden door gebruik te maken van de organisatie-importsjabloon gevonden type: asset-hyperlink id: 4DdJLATEuhMYIE581pPErF en de naam van de gedeelde map in de kolom **collecties** te plaatsen.

Collecties kunnen worden gedeeld met zowel groepen als individuele gebruikers. Het beperken van het aantal individuele gebruikers dat toegang heeft tot een collectie maakt het beheer efficiënter voor beheerders. Lees [hier](#) meer.

 **Note**

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

### Groepen

Groepen gebruiken om te delen is de meest effectieve manier om toegang te geven tot referenties en geheimen. Groepen kunnen, net als gebruikers, gesynchroniseerd worden met je organisatie via SCIM of Directory Connector.

### Rechten

Rechten voor Bitwarden collecties kunnen worden toegewezen op groeps- of gebruikersniveau. Dit betekent dat elke groep of gebruiker geconfigureerd kan worden met verschillende rechten voor dezelfde collectie. Opties voor machtigingen voor verzamelingen omvatten opties:

- Kan bekijken
- Kan bekijken, behalve wachtwoorden
- Kan bewerken
- Kan bewerken, behalve wachtwoorden
- Toegang verlenen tot alle huidige en toekomstige collecties

Lees [hier](#) meer over machtigingen. Bitwarden gebruikt een vereniging van rechten om de uiteindelijke toegangsrechten voor een gebruiker en een verzameling te bepalen. Bijvoorbeeld:

- Gebruiker A maakt deel uit van de Tier 1 Support groep, die toegang heeft tot de Support collectie, met kan bekijken rechten.
- Gebruiker A is ook lid van de Support Management groep, die toegang heeft tot de Support collectie, met bewerkingstoegang.
- In dit scenario kan Gebruiker A de Collectie bewerken.

## Ondersteuning bij migratie

Het Bitwarden Customer Success team is 24/7 beschikbaar met prioriteitsondersteuning voor uw organisaties. Als je hulp nodig hebt of vragen hebt, aarzel dan niet om [contact met ons](#) op te nemen.