bitwarden | Artikel Helpcentrum

BEHEERCONSOLE > GEBRUIKERSBEHEER

Overzicht onboarding en opvolging

Weergeven in het Helpcentrum:
https://bitwarden.com/help/onboarding-and-succession/

Overzicht onboarding en opvolging

> **Tip**
> Lees het volledige artikel hieronder of download de PDF.

Wachtwoordbeheer op maat van uw bedrijf

Nieuwe werknemers snel aan de slag krijgen verhoogt de productiviteit. Op dezelfde manier zorgt een goed afscheid voor meer zekerheid over de veiligheid van de systemen en accounts van je bedrijf. Of uw bedrijf nu neigt naar consolidatie en centralisatie, of de voorkeur geeft aan een flexibele en dynamische omgeving, Bitwarden voldoet aan uw behoeften.

Deze gids behandelt de Bitwarden-benadering van onboarding en opvolgingsplanning voor leden van uw organisatie, te beginnen met onze benadering van de relatie tussen leden en organisaties, vervolgens de eenvoudigste gebruikssituaties voor onboarding en opvolging, en tot slot de hefbomen en opties die u tot uw beschikking hebt om Bitwarden aan te passen aan uw behoeften.

De Bitwarden-aanpak

De visie van Bitwarden is om een wereld voor te stellen waarin niemand wordt gehackt. We zetten dit voort in onze missie om particulieren en bedrijven te helpen hun gevoelige informatie eenvoudig en veilig te beheren. Bitwarden gelooft dat:

- Basiswachtwoordbeheer voor individuen kan en zou **gratis** moeten zijn. Dat is precies wat we bieden, een gratis basisaccount voor particulieren.
- Individuen en gezinnen moeten een actieve rol spelen in hun eigen veiligheid door gebruik te maken van TOTP's, toegang voor noodgevallen en andere ondersteunende beveiligingsfuncties.
- Organisaties kunnen hun beveiligingsprofiel sterk verbeteren door organisatorisch wachtwoordbeheer en veilig delen.

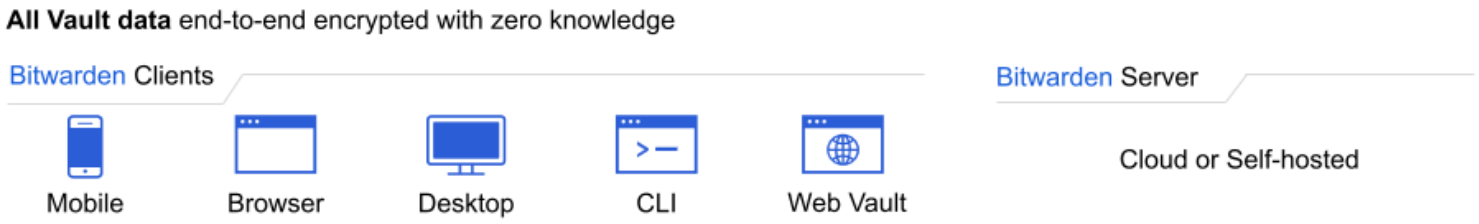
> **Tip**
> Voor Bitwarden zijn verschillende plannen en opties met elkaar verbonden en complementair, allemaal vanuit onze visie op een hackvrije wereld. Door iedereen op het werk **en** thuis in staat te stellen om wachtwoorden te beheren, komen we een stap dichter bij dat doel.

Een belangrijk aspect van Bitwarden is dat, in tegenstelling tot veel softwaretoepassingen, alles in elke kluis end-to-end versleuteld is. Om dit beveiligingsmodel te handhaven, moet iedereen die Bitwarden gebruikt een uniek account hebben met een uniek hoofdwachtwoord. Hoofdwachtwoorden moeten **sterk** en **gedenkwaardig** zijn.

Elke gebruiker beheert zijn hoofdwachtwoord. Bitwarden is een zero-knowledge encryptieoplossing, wat betekent dat het team van Bitwarden en de Bitwarden-systemen zelf geen kennis hebben van een hoofdwachtwoord, het niet kunnen achterhalen en het niet kunnen resetten.

Gebruik Bitwarden overal

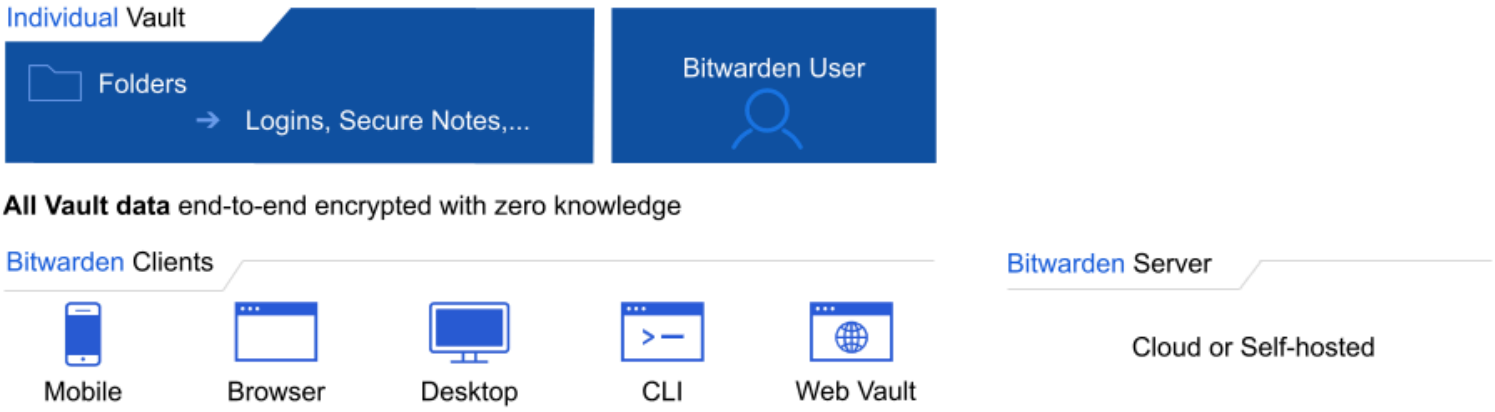
Overal veiligheid betekent overal veiligheid, dus de beste wachtwoordmanagers bieden toegang tot al uw apparaten. Bitwarden ondersteunt een reeks cliëntapplicaties die allemaal kunnen worden verbonden met onze cloud-hosted servers of een zelf gehoste server:



Bitwarden clients/servers

Individuele kluizen van gebruikers

Iedereen die een Bitwarden-account aanmaakt, krijgt zijn eigen individuele kluis. De individuele kluizen zijn toegankelijk vanuit elke clienttoepassing en zijn uniek voor elke gebruiker. Alleen die gebruiker heeft de sleutel om toegang te krijgen, met behulp van een combinatie van zijn e-mailadres en hoofdwachtwoord. Persoonlijke accounts en de kluisitems die daarin zijn opgeslagen, vallen onder de verantwoordelijkheid van de accounteigenaar. Eigenaars, beheerders en managers van organisaties kunnen de individuele kluis van andere gebruikers niet zien, waardoor gegarandeerd wordt dat iemands individuele kluisgegevens van hen blijven.



Persoonlijke kluizen

Families, Teams en Enterprise-organisaties voorzien leden automatisch individueel van premium functies, zoals toegang in noodgevallen en versleutelde opslag van bijlagen, die ze naar eigen keuze kunnen gebruiken. Gegevens in een individuele kluis behoren toe aan de gebruiker. Individuele kluizen kunnen niet worden gedeeld, organisaties wel.

Tip

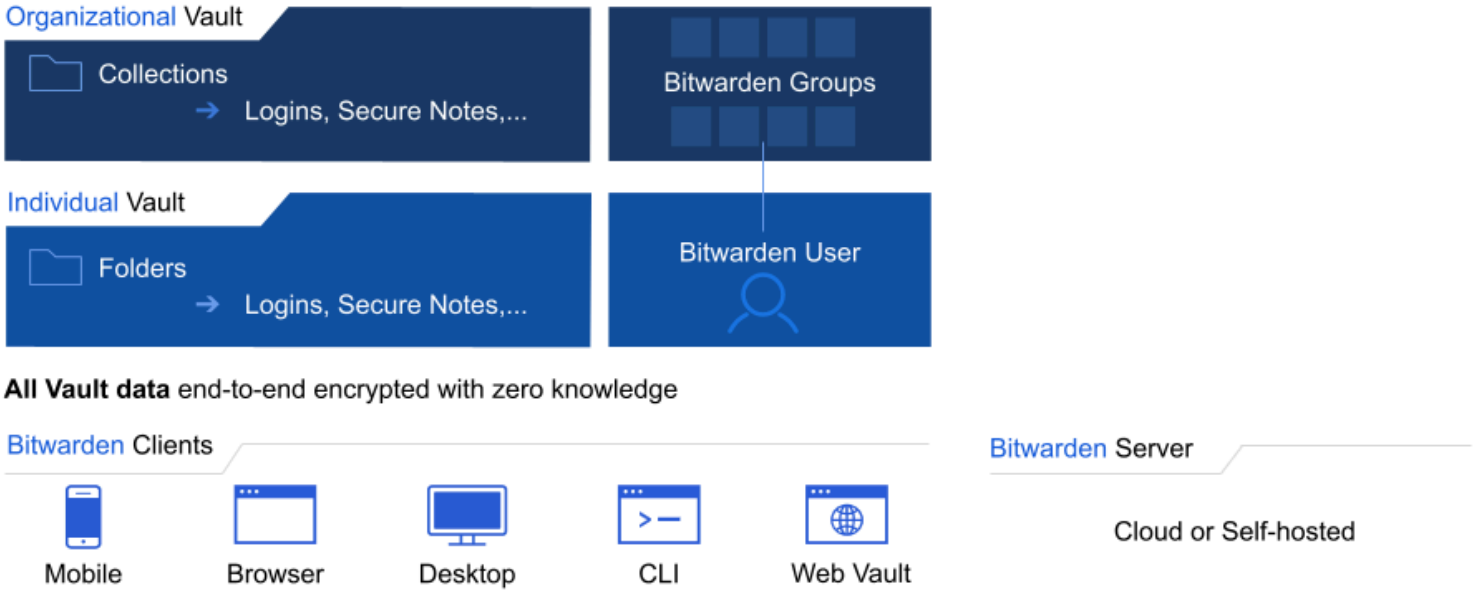
Waarom standaard individuele kluizen?

Individuele kluizen zijn een belangrijk onderdeel van de Bitwarden-aanpak. Werknemers gebruiken elke dag een reeks referenties, zowel op persoonlijk als professioneel vlak, en **gewoontes die op het ene vlak worden aangeleerd, worden meestal gewoontes op het andere vlak**. Wij zijn van mening dat werknemers die in hun privéleven de juiste beveiligingspraktijken gebruiken, dat goede gedrag zullen overbrengen naar hun professionele leven en zo **uw bedrijf zullen beschermen**.

Door op beide gebieden hetzelfde gereedschap te gebruiken, wordt die gewoonte sneller en gemakkelijker gevormd. Enterprise organisaties hebben de optie om beleidsregels te configureren, inclusief het uitschakelen van individuele vaults.

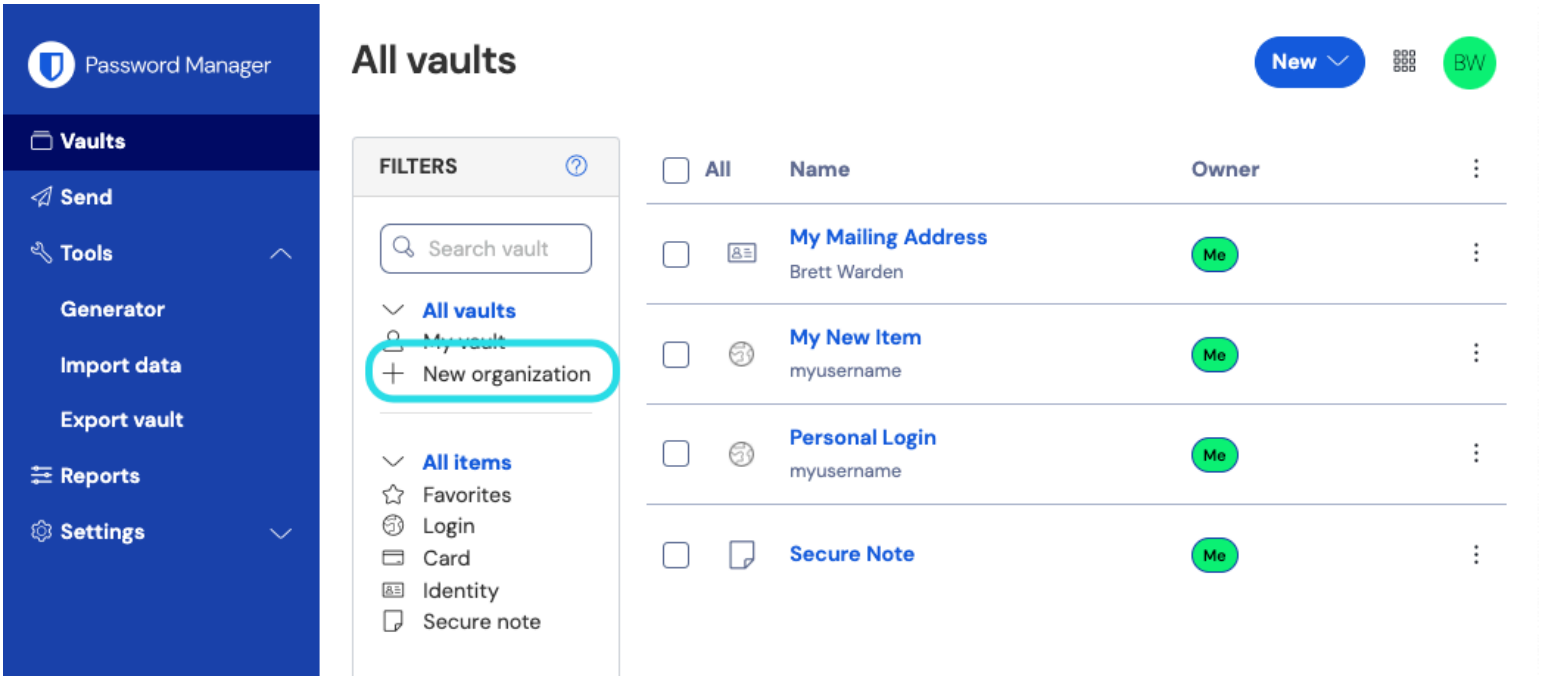
Bitwarden organisaties

Bitwarden-organisaties voegen een laag van samenwerking en delen toe aan wachtwoordbeheer voor uw team of onderneming, zodat u veilig gemeenschappelijke informatie kunt delen, zoals wifi-wachtwoorden op kantoor, online referenties of gedeelde bedrijfscreditcards. Veilig delen via organisaties is veilig en gemakkelijk.



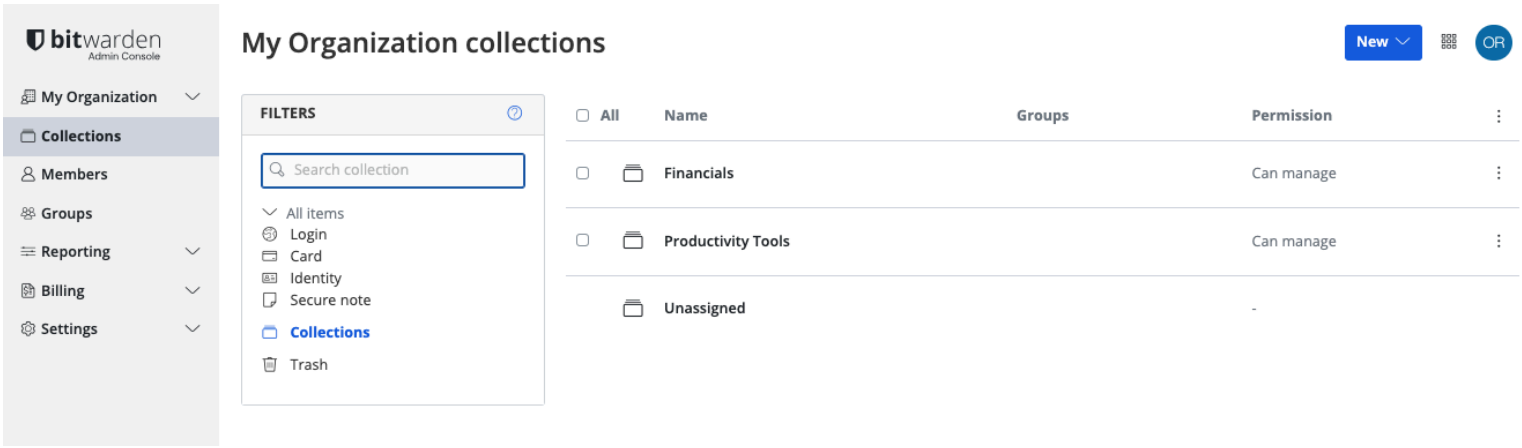
Organisatie Kluis

Iedereen kan rechtstreeks vanuit de webapp een organisatie starten:



Nieuwe organisatie

Eenmaal aangemaakt kom je terecht in de beheerconsole, de centrale hub voor alles wat te maken heeft met delen en organisatiebeheer. Degene die de organisatie opstart, wordt de eigenaar en krijgt de volledige controle over de kluis, het beheren van items, leden, collecties en groepen, het uitvoeren van rapportages en het configureren van instellingen zoals beleidsregels:



Beheerconsole

Collecties

Bitwarden organisaties beheren leden en gegevens op een schaalbare en veilige manier. Het beheren van leden en gegevens op individuele basis is inefficiënt voor grote bedrijven en kan ruimte laten voor fouten. Om dit op te lossen, bieden organisaties collecties en groepen aan.

Collecties verzamelen logins, notities, kaarten en identiteiten om ze veilig te delen binnen een organisatie:

Collecties gebruiken

Leden inwerken

Zodra je organisatie is opgericht en collecties zijn ingesteld om je gegevens in op te slaan, moeten eigenaren en beheerders nieuwe leden uitnodigen. Om de veiligheid van uw organisatie te waarborgen, past Bitwarden een 3-stappenproces toe voor het onboarden van nieuwe leden, Uitnodigen → Accepteren → Bevestigen.

Leden kunnen direct vanuit de webkluis aan boord worden genomen, met behulp van de Directory Connector-applicatie om individuele gebruikers en groepen te synchroniseren, of via Just in Time (JIT) provisioning met behulp van inloggen met SSO.

Leden toevoegen

In de eenvoudigste gevallen kunnen gebruikers rechtstreeks vanuit de webapp aan je organisatie worden toegevoegd. Bij het toevoegen van gebruikers kun je aangeven tot welke collecties ze toegang krijgen, welke rol ze krijgen en meer.

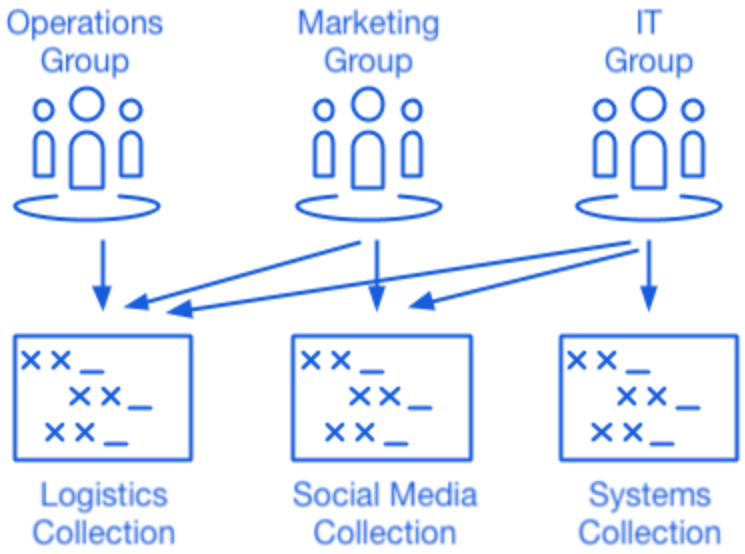
Leer stap voor stap hoe je gebruikers toevoegt aan je organisatie.

Zodra gebruikers volledig in je organisatie zijn opgenomen, kun je ze toegang geven tot de kluisgegevens van je organisatie door ze toe te wijzen aan collecties. Teams en Enterprise-organisaties kunnen gebruikers toewijzen aan groepen voor schaalbare permissietoewijzing en groep-verzamelassociaties maken in plaats van toegang toe te wijzen op individueel niveau.

> **Tip**
> Voor grote organisaties zijn SCIM en Directory Connector de beste manieren om gebruikers op schaal aan en af te melden.

Groepen

Groepen brengen individuele gebruikers samen en bieden een schaalbare manier om rechten toe te wijzen, inclusief toegang tot collecties en andere toegangscontroles. Wanneer je nieuwe gebruikers aanwerft, voeg ze dan toe aan een groep zodat ze automatisch de geconfigureerde rechten van die groep erven:



Verzamelingen met groepen gebruiken

Uitgebreide toegangscontrole op basis van rollen

Bitwarden hanteert een bedrijfsvriendelijke aanpak voor delen op schaal. Leden kunnen aan de organisatie worden toegevoegd met een aantal verschillende rollen, tot verschillende groepen behoren en die groepen aan verschillende collecties toewijzen om de toegang te regelen. Onder de beschikbare rollen is een aangepaste rol voor granulaire configuratie van administratieve rechten.

Gebruikers deprovisioneren

Bij Bitwarden zien we het delen van referenties als een essentieel aspect om efficiënt en veilig te kunnen werken. We erkennen ook dat als een inlogcode eenmaal is gedeeld, het technisch mogelijk is voor de ontvanger om deze te behouden. Daarom spelen een veilige onboarding met de juiste rolgebaseerde toegangscontroles en het implementeren van beleidsregels een belangrijke rol bij het vergemakkelijken van veilige opvolging.

Bitwarden biedt verschillende tools waarmee u uw workflow kunt aanpassen en meer controle kunt uitoefenen over opvolging. De volgende secties beschrijven een basisopvolgingsworkflow, die geen van deze tools gebruikt, en enkele geavanceerde opvolgingstactieken die vaak door organisaties worden gebruikt:

Basis deprovisionering

Het deprovisioneren van gebruikers uit Bitwarden houdt in dat gebruikers uit je organisatie worden verwijderd, en net als onboarding kan dit direct vanuit de web vault worden gedaan of op een geautomatiseerde manier met behulp van SCIM of Directory Connector.

Alice is een **gebruiker** in uw organisatie, die wordt gehost op de Bitwarden-cloud en gebruikmaakt van e-mailadressen van het bedrijf (bijv. first-last@company. com). Op dit moment is dit hoe Alice Bitwarden gebruikt:

Productgebied	Beschrijving
Toepassingen voor klanten	Gebruikt Bitwarden op mobiel en een browseruitbreiding voor persoonlijk en professioneel gebruik, en de webkluis voor incidenteel organisatiegerelateerd werk.
E-mail & hoofdwachtwoord	Logt in op Bitwarden met `alice@company.com` en `p@ssw0rD`.
Persoonlijke items	Bewaart allerlei persoonlijke spullen, waaronder logins en creditcards, in haar persoonlijke kluis.
Inloggen in twee stappen	Gebruikt Duo 2FA voor de hele organisatie.
Collecties	Alice heeft de machtiging Beheer voor de collectie "Marketing Credentials", wat haar de mogelijkheid geeft om veel aspecten van die collectie te beheren.
Gedeelde items	Heeft verschillende kluisitems gemaakt en gedeeld die eigendom zijn van de organisatie en in de collectie van haar team staan.

Zodra Alice uit je organisatie is verwijderd:

Productgebied	Beschrijving
Toepassingen voor klanten	Kan elke Bitwarden-toepassing blijven gebruiken om toegang te krijgen tot haar individuele kluis, maar **verliest onmiddellijk de toegang** tot de organisatiekluis, alle collecties en alle gedeelde items.
E-mail & hoofdwachtwoord	Ze kan blijven inloggen met `alice@company.com` en `p@ssw0rD`, maar omdat ze geen toegang heeft tot haar `@company.com` inbox, moet ze geadviseerd worden om het e-mailadres dat gekoppeld is aan haar Bitwarden-account te wijzigen.

Productgebied	Beschrijving
Individuele items	Kan nog steeds haar individuele kluis gebruiken en toegang krijgen tot de voorwerpen die erin zijn opgeslagen.
Machtigingen in de organisatie	**Verliest onmiddellijk alle machtigingen over en toegang tot** alles wat met de organisatie te maken heeft.
Inloggen in twee stappen	Kan Duo 2FA van de organisatie niet gebruiken om toegang te krijgen tot haar kluis, maar kan een van onze gratis twee-staps inlogopties instellen of upgraden naar premium voor meer.
Aangemaakte collecties	Alice's "Marketing Team" collectie zal worden bewaard door organisatie-eigenaren en admins, die een nieuwe gebruiker kunnen toewijzen Toestemming beheren
Gedeelde items	Het eigendom van collecties en gedeelde items **behoort toe aan de organisatie**, dus Alice verliest de toegang tot al deze items ondanks dat ze ze heeft aangemaakt.

Tip

Offline apparaten slaan een alleen-lezen kopie van kluisgegevens op, inclusief organisatorische kluisgegevens. Als je kwaadwillige uitbuiting hiervan verwacht, moeten de referenties waartoe het lid toegang had worden bijgewerkt wanneer je hem uit de organisatie verwijdert.

Geavanceerde deprovisioning

Warning

Voor accounts die geen hoofdwachtwoord hebben als gevolg van SSO met vertrouwde apparaten, zal het verwijderen uit uw organisatie of het intrekken van hun toegang alle toegang tot hun Bitwarden-account afsluiten, tenzij:

1. Je wijst hen vooraf een hoofdwachtwoord toe met behulp van accountherstel.
2. De gebruiker logt ten minste één keer in na het accountherstel om de workflow voor accountherstel volledig te voltooien.

Administratieve overname

Met het beleid voor het resetten van het hoofdwachtwoord kunnen eigenaren en beheerders in uw organisatie het hoofdwachtwoord van een gebruiker resetten tijdens de opvolging.

Door het hoofdwachtwoord van een gebruiker opnieuw in te stellen, wordt de gebruiker uit alle actieve Bitwarden-sessies uitgelogd en worden de aanmeldingsgegevens opnieuw ingesteld op de gegevens die zijn opgegeven door de beheerder. Dit betekent dat de beheerder (en alleen die beheerder) de sleutels heeft tot de kluisgegevens van de gebruiker, inclusief items in de individuele kluis. Deze tactiek om kluizen over te nemen wordt vaak gebruikt door organisaties om ervoor te zorgen dat werknemers geen toegang hebben tot

individuele kluisitems die werkgerelateerd kunnen zijn en kan worden gebruikt om audits van alle referenties die een werknemer mogelijk heeft gebruikt te vergemakkelijken.

> **Note**
>
> **Het resetten van het beheerderswachtwoord omzeilt het inloggen in twee stappen niet**. In veel gevallen raden we aan om SSO te gebruiken, omdat sommige IdP's het mogelijk maken om 2FA en 2FA bypass policies te configureren voor je gebruikers.

De individuele kluis verwijderen

Als je organisatie realtime controle van alle kluisitems vereist, kun je het beleid Individuele kluis verwijderen gebruiken om gebruikers te verplichten alle kluisitems op te slaan in de organisatie. Dit omzeilt de noodzaak om het account van een gebruiker over te nemen en te controleren tijdens de opvolging, omdat het volledig leeg is van gegevens zodra het uit de organisatie wordt verwijderd.

Account verwijderen zonder inloggen

Zoals eerder vermeld, verwijdert het verwijderen van een gebruiker uit uw organisatie niet automatisch zijn Bitwarden-account. In de basisworkflow voor opvolging heeft een gebruiker die wordt verwijderd geen toegang meer tot de organisatie of tot gedeelde items en collecties, maar hij kan nog wel inloggen op Bitwarden met zijn bestaande hoofdwachtwoord en toegang krijgen tot individuele kluisitems.

Organisaties die het account volledig willen verwijderen, inclusief alle individuele kluisitems, kunnen mogelijk een van de volgende methoden gebruiken om dit te doen tijdens de opvolging:

1. Als u Bitwarden zelf host, kan een geautoriseerde beheerder het account verwijderen vanuit het systeembeheerdersportaal.

2. Als de account een e-mailadres van @yourcompany.com heeft dat door uw bedrijf wordt beheerd, kunt u de verwijderworkflow gebruiken zonder in te loggen en de verwijdering bevestigen in de inbox van @yourcompany.com.

Uw organisatie ontwerpen voor uw bedrijf

Bij Bitwarden zeggen we vaak dat wachtwoordbeheer mensenwerk is, en we kunnen de workflows aanpassen aan uw organisatie. Door een breed scala aan opties aan te bieden, gedeeld via onze open source aanpak, kunnen klanten er zeker van zijn dat ze aan hun eigen individuele behoeften kunnen voldoen.

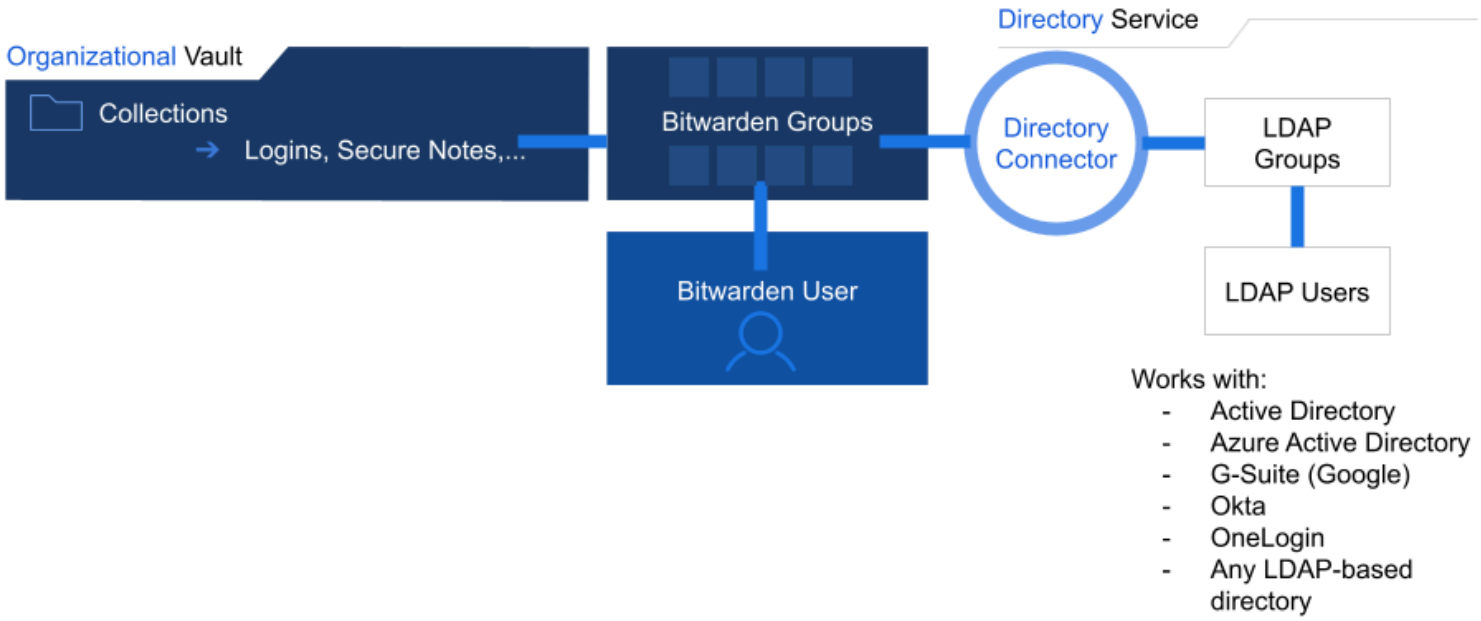
Begin vandaag nog met een gratis Enterprise of Teams proefversie.

SCIM

Voor Enterprise-organisaties met grote gebruikersbestanden die werken met een ondersteunde identiteit (momenteel Azure AD, Okta, OneLogin en JumpCloud), kunnen SCIM-integraties worden gebruikt om automatisch leden en groepen aan te maken in uw Bitwarden-organisatie. Meer informatie.

Directory Connector

Voor bedrijven met grote gebruikersbestanden die werken met directoryservices (LDAP, AD, Okta en andere) kan Directory Connector gebruikers en groepen synchroniseren vanuit de directory naar de Bitwarden-organisatie. Directory Connector is een stand-alone applicatie die overal kan worden uitgevoerd met toegang tot uw mappen en Bitwarden.



Directory Connector

Veel Bitwarden Teams en Enterprise-organisaties richten zich bij het inwerken op de Directory Connector en gebruiken de beheergebieden van de organisatie voor het beheren van relaties tussen groepen.

Directory Connector zal:

- Op LDAP gebaseerde groepen synchroniseren met Bitwarden-groepen
- Gebruikers binnen elke groep synchroniseren
- Nieuwe gebruikers uitnodigen om lid te worden van de organisatie
- Verwijder verwijderde gebruikers uit de organisatie

Inloggen met SSO

Bitwarden Enterprise-organisaties kunnen integreren met uw bestaande identity provider (IdP) met behulp van SAML 2.0 of OIDC, zodat leden van uw organisatie kunnen inloggen op Bitwarden met behulp van SSO. Inloggen met SSO scheidt gebruikersauthenticatie van kluisdecodering:

Authenticatie wordt voltooid via de door jou gekozen IdP en behoudt alle processen voor tweefactorauthenticatie die aan die IdP zijn gekoppeld. Voor **het ontsleutelen** van kluisgegevens is de individuele sleutel van de gebruiker nodig, die gedeeltelijk is afgeleid van het hoofdwachtwoord. Er zijn twee ontcijferingsopties, die er allebei voor zorgen dat gebruikers zich authenticeren met hun reguliere SSO-referenties.

- **Hoofdwachtwoord**: Na authenticatie zullen organisatieleden kluisgegevens ontsleutelen met behulp van hun hoofdwachtwoord.
- **Door de klant beheerde encryptie**: Verbind login met SSO met uw zelf gehoste ontcijferingssleutelserver. Met deze optie hoeven organisatieleden hun hoofdwachtwoord niet te gebruiken om kluisgegevens te ontsleutelen. In plaats daarvan haalt Key Connector een ontcijferingssleutel op die veilig is opgeslagen in een database die jouw eigendom is en door jou wordt beheerd.

- Maak gebruik van uw bestaande identiteitsprovider.
- Bescherm de end-to-end versleuteling van je gegevens.
- Gebruikers automatisch voorzien.
- Configureer toegang met of zonder SSO.
- Ontcijfer kluisgegevens volgens de beveiligingsbehoeften van je bedrijf.

Bedrijfsbeleid

Ondernemingsorganisaties kunnen verschillende beleidsregels implementeren die ontworpen zijn om een veilige basis te leggen voor elk bedrijf. Het beleid omvat:

- **Inloggen in twee stappen verplichten:** Gebruikers verplichten om in twee stappen in te loggen op hun persoonlijke accounts.
- **Vereisten voor hoofdwachtwoord:** Stel minimumvereisten in voor de sterkte van het hoofdwachtwoord.
- **Wachtwoordgenerator:** Stel minimumvereisten in voor wachtwoordgeneratorconfiguratie.
- **Enkele organisatie:** Beperk dat gebruikers zich niet bij andere organisaties kunnen aansluiten.
- **Individuele kluis verwijderen:** Gebruikers verplichten om kluisitems op te slaan in een organisatie door de optie voor persoonlijk eigendom te verwijderen.

> **Tip**
>
> Het **Remove individual vault** beleid past bijvoorbeeld in de eerdere discussie over de wisselwerking tussen individuele kluizen en organisatiekluizen. Sommige bedrijven willen de zekerheid dat alle referenties in de kluis van de organisatie worden bewaard. Een mogelijke implementatie zou kunnen zijn dat elke individuele gebruiker zijn eigen collectie heeft, die in tegenstelling tot individuele kluizen kan worden beheerd door organisatie-eigenaren en admins.

Gebeurtenislogboeken

Bitwarden-organisaties bieden toegang tot eventlogs, die direct vanuit de webvault kunnen worden bekeken of kunnen worden geëxporteerd om te worden geanalyseerd in SIEM-systemen (Security Information and Event Management) zoals Splunk. Gebeurtenislogboeken bevatten informatie over:

- Interacties tussen gebruikersitems
- Wijzigingen in kluisitems
- Onboarding-evenementen
- Organisatieconfiguratiewijzigingen
- Veel, veel meer

> **Tip**
> Naast deze voordelen waarderen klanten de mogelijkheid om Bitwarden nauw te integreren in hun bestaande systemen. Bitwarden biedt een robuuste openbare API en een volledig uitgeruste opdrachtregelinterface(CLI) voor verdere integratie in bestaande organisatieworkflows.

Zelf hosten

In lijn met de Bitwarden-aanpak om wachtwoordbeheer overal en altijd aan te bieden, biedt Bitwarden een optie om zelf te hosten om een nog breder scala aan gebruikssituaties voor bedrijven aan te pakken. Er zijn veel redenen voor een bedrijf om te kiezen voor zelf-hosting. Specifiek als het gaat om onboarding, opvolging en verbeterde functies, zijn hier enkele redenen waarom bedrijven hiervoor kiezen:

- **Onmiddellijke verwijdering van gebruikersaccounts:** Omdat jij de server beheert, kunnen gebruikers volledig worden verwijderd (inclusief hun individuele kluis).
- **Controle op netwerktoegang**: Eigenaren van organisaties kunnen bepalen welke netwerktoegang medewerkers moeten gebruiken om toegang te krijgen tot hun Bitwarden-server.
- **Geavanceerde proxy-instellingen:** Beheerders kunnen ervoor kiezen om bepaalde soorten apparaten in of uit te schakelen voor toegang tot de Bitwarden Server.
- **Gebruik een bestaand databasecluster:** Maak verbinding met een bestaande Microsoft SQL Server-database. In de toekomst zullen nog meer databases worden ondersteund.
- **Vergroot de opslagruimte voor bestandsbijlagen en Bitwarden Send:** Bestandsbijlagen voor Bitwarden-items of Bitwarden Send worden bewaard op door de gebruiker verstrekte opslagruimte.

De stukjes in elkaar zetten

Directory Connector, inloggen met SSO, ondernemingsbeleid en uw kluis werken goed afzonderlijk of in harmonie om uw ervaring met onboarding, opvolging en organisatiebeheer te optimaliseren. De volgende tabel laat zien hoe het eruit zou kunnen zien om deze stukken aan elkaar te rijgen tot één vloeiend proces:

Stap	Beschrijving
Synchroniseer	Gebruik Directory Connector om groepen en gebruikers naar Bitwarden te synchroniseren vanuit uw bestaande directoryservice.
Uitnodigen	Directory Connector zal automatisch uitnodigingen versturen naar gesynchroniseerde gebruikers.
Authenticeren	Koppel uw login met SSO-implementatie aan het SSO-beleid om gebruikers te verplichten zich aan te melden met SSO wanneer ze hun uitnodigingen accepteren.

Stap	Beschrijving
toedienen	Gebruik de web kluis om sommige gebruikers te promoveren naar verschillende rollen en om ervoor te zorgen dat de groep-verzamel relaties geconfigureerd zijn om de juiste toegang te verlenen aan de juiste gebruikers.
opnieuw synchroniseren	Draai Directory Connector regelmatig opnieuw om gebruikers uit Bitwarden te verwijderen die niet langer actief zijn in uw directoryservice en om onboarding voor nieuwe medewerkers te starten.

FAQs

V: Als een medewerker al een Bitwarden-account heeft, kunnen we dit dan koppelen aan de organisatie zodat ze niet nog een Bitwarden-account nodig hebben?

A: Ja! Dat kan. Sommige klanten raden aan om voordat gebruikers aan de organisatie worden gekoppeld, deze gebruikers een Bitwarden-kluis te koppelen aan hun bedrijfsmail. Deze keuze is bedrijfsspecifiek en beide benaderingen werken.

V: Als een medewerker vertrekt, kunnen we zijn account dan loskoppelen van de organisatie zodat hij geen toegang meer heeft tot de bedrijfsgegevens en zijn eigen gegevens niet kwijtraakt?

A: Ja! Dat is precies wat deprovisioneren inhoudt.

V: Kunnen we voorkomen dat werknemers hun referenties dupliceren van de bedrijfsorganisatie naar hun individuele kluis?

A: Ja! Met onze uitgebreide reeks toegangscontroles op basis van rollen kun je referenties **alleen-lezen** maken om duplicatie te voorkomen.