GEHEIMEN MANAGER > AAN DE SLAG

Beheer uw organisatie

Beheer uw organisatie

> **Note**
> Voor een volledig overzicht van Bitwarden onboarding, kunt u deze handleiding bekijken voor meer informatie.

Als organisatie die Secrets Manager gebruikt, deelt u veel van de tools die oorspronkelijk door Password Manager werden gebruikt. Dit artikel behandelt deze algemene gebieden en verwijst waar nodig naar gedeelde documentatie.

> **Note**
> Als u helemaal nieuw bent met Bitwarden-organisaties, raden we u aan ons artikel over het opstarten als organisatiebeheerder te lezen.

Bedrijfsbeleid

Policies stellen Enterprise-organisaties in staat om beveiligingsregels af te dwingen voor hun leden, bijvoorbeeld door het gebruik van tweestapslogin verplicht te stellen. Hoewel sommige beleidsregels voornamelijk van toepassing zijn op Password Manager, zijn er een handvol beleidsregels die algemeen van toepassing zijn op gebruikers van Secrets Manager:

- Inloggen in twee stappen verplichten
- Vereisten voor hoofdwachtwoord
- Hoofdwachtwoord opnieuw instellen
- Enkele organisatie
- Verificatie met eenmalige aanmelding vereisen
- Time-out kluis

> **Tip**
> Als u Bitwarden voor het eerst gebruikt, raden we u aan beleidsregels in te stellen voordat u uw gebruikers in dienst neemt.

Gebruikersbeheer

Gebruikersbeheer voor Secrets Manager organisaties is gelijk aan organisaties die Password Manager gebruiken, maar enkele Secrets Manager-specifieke elementen zijn onder andere het verlenen van toegang aan organisatieleden tot Secrets Manager, rolverschillen tussen leden en het specificeren van gebruikersplaatsen en service accounts.

Inwerken

Er zijn een paar verschillende manieren om gebruikers aan te melden bij uw Bitwarden-organisatie. Enkele veelgebruikte methoden worden hier uitgelicht:

Handmatig

De Bitwarden-webkluis biedt een eenvoudige en intuïtieve interface voor het uitnodigen van nieuwe gebruikers om lid te worden van uw organisatie. Deze methode is het beste voor kleine organisaties of organisaties die geen gebruik maken van directoryservices zoals Azure AD of Okta. Leer hoe je kunt beginnen.

SCIM

Bitwarden-servers bieden een SCIM-eindpunt dat, met een geldige SCIM API-sleutel, verzoeken accepteert van uw identity provider voor provisioning en de-provisioning van gebruikers en groepen. Deze methode is het beste voor grotere organisaties die een SCIM-enabled directory service of IdP gebruiken. Leer hoe je kunt beginnen.

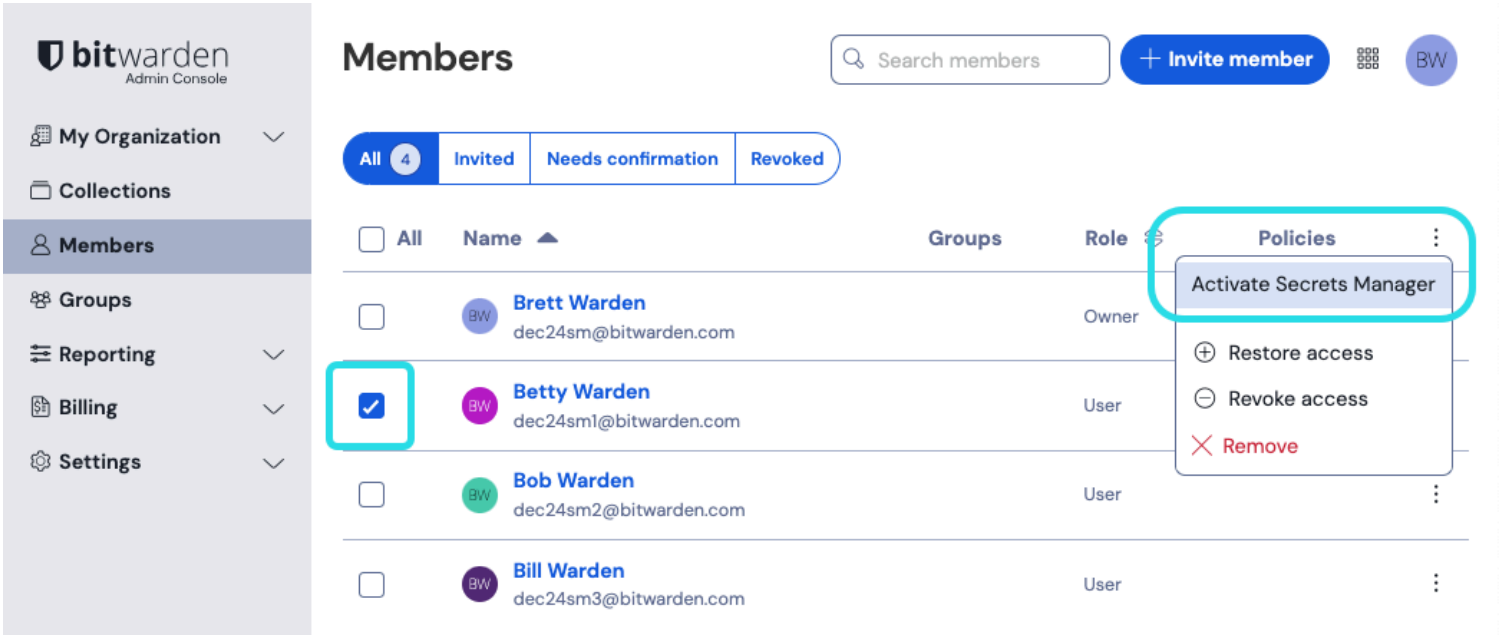
Directory Connector

Directory Connector voorziet automatisch in gebruikers en groepen in uw Bitwarden-organisatie door gebruik te maken van een selectie van broncodeservices. Deze methode is het beste voor grotere organisaties die directoryservices gebruiken die SCIM niet ondersteunen. Leer hoe u kunt beginnen.

Toegang tot Secrets Manager

Zodra je aan boord bent, geef je individuele leden van je organisatie toegang tot Secrets Manager:

1. Open de **ledenweergave** van je organisatie en selecteer de leden die je toegang wilt geven tot Secrets Manager.
2. Selecteer in het menu ⋮ **Geheimenbeheer activeren** om toegang te verlenen aan geselecteerde leden:



Gebruikers van Secrets Manager toevoegen

Tip

Door leden toegang te geven tot Secrets Manager krijgen ze niet automatisch toegang tot opgeslagen projecten of geheimen. Vervolgens moet je mensen of groepen toegang geven tot de projecten.

Lidrollen

De volgende tabel laat zien wat elke lidrol kan doen binnen Secrets Manager. Tijdens de bèta hebben gebruikers dezelfde ledenrol voor Secrets Manager die ze toegewezen hebben gekregen voor Password Manager:

Rol als lid	Beschrijving
Gebruiker	Gebruikers kunnen hun eigen secrets, projecten, service accounts en access tokens aanmaken. Ze kunnen deze objecten bewerken als ze eenmaal zijn aangemaakt. Gebruikers moeten worden toegewezen aan projecten of serviceaccounts om te kunnen interageren met bestaande objecten en kunnen **Kan lezen** of **Kan lezen, schrijftoegang** krijgen.
Admin	Admins hebben automatisch **lees- en schrijftoegang** tot alle secrets, projecten, service accounts en access tokens. Admins kunnen zichzelf toegang geven tot Secrets Manager en andere leden toegang geven tot Secrets Manager.
Eigenaar	Eigenaars hebben automatisch **lees- en schrijftoegang** tot alle geheimen, projecten, serviceaccounts en toegangstokens. Eigenaars kunnen zichzelf toegang geven tot Secrets Manager en andere leden toegang geven tot Secrets Manager.

Note

Aangepaste rollen zijn momenteel niet gescoped met opties voor Secrets Manager, maar kunnen nog steeds worden gebruikt om specifieke Password Manager of bredere organisatiemogelijkheden toe te wijzen.

Groepen

Groepen brengen individuele leden met elkaar in verband en bieden een schaalbare manier om toegang te krijgen tot en machtigingen te krijgen voor specifieke projecten. Wanneer je nieuwe leden toevoegt, voeg ze dan toe aan een groep zodat ze automatisch de geconfigureerde rechten van die groep erven. Meer informatie.

Als de groepen eenmaal zijn gemaakt in de beheerconsole, wijs ze dan toe aan projecten vanuit de webapp Secrets Manager.

Eenmalige aanmelding

Inloggen met SSO is de Bitwarden oplossing voor eenmalige aanmelding. Door gebruik te maken van login met SSO kunnen Enterprise-organisaties hun bestaande Identity Provider gebruiken om gebruikers te authenticeren bij Bitwarden met behulp van de protocollen SAML 2.0 of Open ID Connect (OIDC). Leer hoe je kunt beginnen.

Beheer van accountherstel

Accountherstel stelt aangewezen beheerders in staat om gebruikersaccounts van de bedrijfsorganisatie te herstellen en de toegang te herstellen in het geval dat een medewerker zijn hoofdwachtwoord vergeet. Accountherstel kan worden geactiveerd voor een organisatie door het beheerbeleid voor accountherstel in te schakelen. Leer hoe je kunt beginnen.

Gebeurtenislogboeken

Gebeurtenislogs zijn tijdstempels van gebeurtenissen die plaatsvinden binnen je Teams of Enterprise-organisatie. Gebeurtenissen van Secrets Manager zijn zowel beschikbaar via **Rapportage** → **Gebeurtenislogboeken** van je organisatiekluis als via de pagina Gebeurtenislogboeken van de serviceaccount.

Gebeurtenislogboeken kunnen worden geëxporteerd en worden voor onbepaalde tijd bewaard. Hoewel veel gebeurtenissen van toepassing zijn op alle Bitwarden producten en sommige specifiek zijn voor Password Manager, zal Secrets Manager specifiek de volgende gebeurtenissen loggen:

- Geheim toegankelijk door een serviceaccount

Zelf hosten

Enterprise-organisaties kunnen Bitwarden Secrets Manager zelf hosten met Docker op Linux- en Windows-machines. Als je Bitwarden nog niet eerder zelf hebt gehost, gebruik dan deze gids om jezelf op het juiste spoor te zetten.

Als u al een Enterprise Bitwarden-organisatie zelf host en toegang wilt krijgen tot Secrets Manager op die server:

1. Meld u aan voor een Secrets Manager-abonnement in uw cloud-hosted Bitwarden-organisatie.
2. Werk je zelf gehoste server bij naar minimaal 2023.10.0
3. Haal een nieuw licentiebestand op bij je cloud-hosted organisatie en upload het naar je zelf gehoste server.

> **Note**
> Self-hosting Secrets Manager wordt niet ondersteund voor de optie Bitwarden unified self-hosted deployment. Teams en Enterprise-organisaties moeten een standaard Linux- of Windows-installatie gebruiken.