

BEHEERCONSOLE > BASISPRINCIPES ORGANISATIE

Ondernemingsbeleid

Ondernemingsbeleid

Wat zijn ondernemingsbeleidslijnen?

Met Enterprise-polices kunnen Enterprise-organisaties beveiligingsregels afdwingen voor alle gebruikers, bijvoorbeeld door het gebruik van tweestapslogin verplicht te stellen.

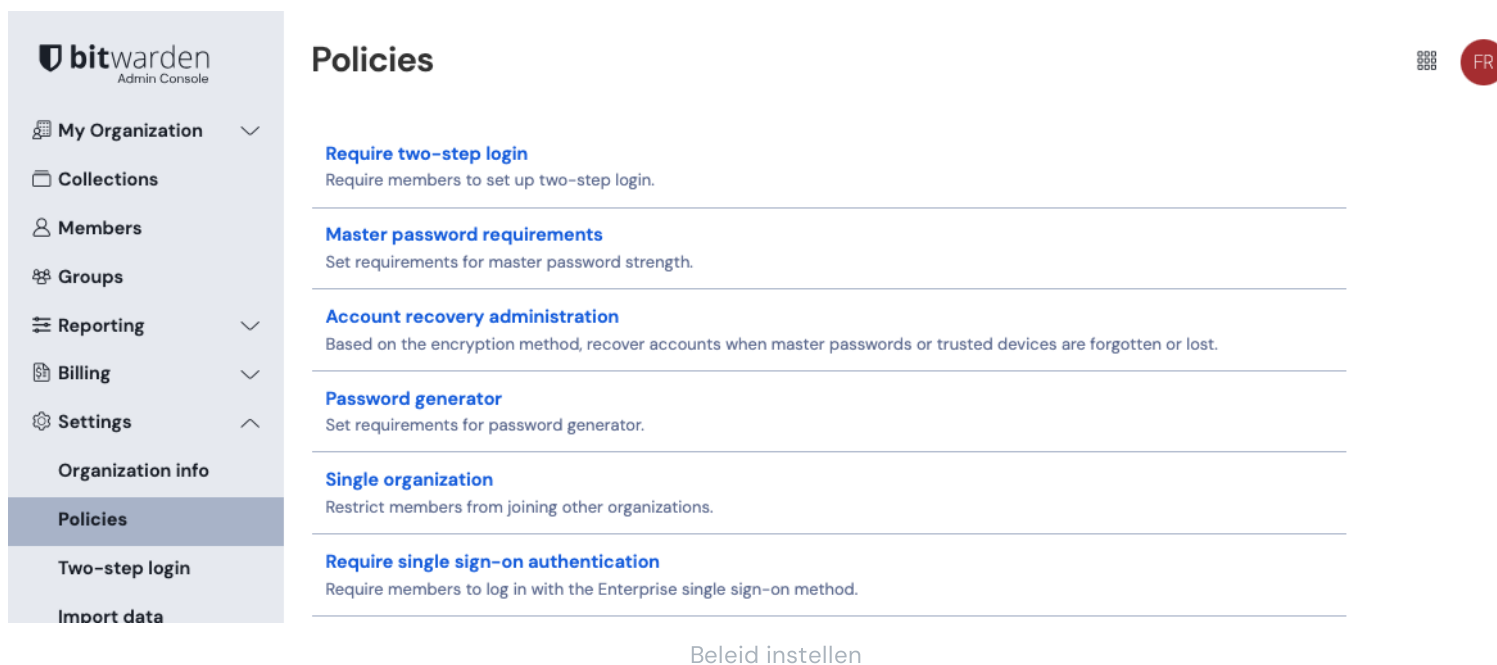
Bedrijfsbeleid kan worden ingesteld door organisatiebeheerders of -eigenaars.

Warning

We raden aan om bedrijfsbeleidsregels in te stellen voordat je gebruikers uitnodigt voor je organisatie. Sommige beleidsregels zullen niet-conforme gebruikers verwijderen wanneer ze worden ingeschakeld, en sommige zijn niet met terugwerkende kracht afdwingbaar.

Bedrijfsbeleid instellen

Beleidsregels kunnen worden ingesteld vanuit de beheerconsole door te navigeren naar **Instellingen** → **Beleidsregels**:



The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar with navigation options: My Organization, Collections, Members, Groups, Reporting, Billing, Settings, Organization info, Policies (selected), Two-step login, and Import data. The main content area is titled 'Policies' and lists several policy settings: 'Require two-step login' (Require members to set up two-step login), 'Master password requirements' (Set requirements for master password strength), 'Account recovery administration' (Based on the encryption method, recover accounts when master passwords or trusted devices are forgotten or lost), 'Password generator' (Set requirements for password generator), 'Single organization' (Restrict members from joining other organizations), and 'Require single sign-on authentication' (Require members to log in with the Enterprise single sign-on method). In the top right corner, there is a QR code icon and a red circular button with 'FR'.

Beschikbare beleidsregels

Inloggen in twee stappen verplichten

Door het beleid **Aanmelden in twee stappen vereisen in** te schakelen, moeten leden een aanmeldingsmethode in twee stappen gebruiken om toegang te krijgen tot hun kluizen. Als je de 2FA-functionaliteit van een SSO of identity provider gebruikt, hoef je dit beleid niet in te schakelen. Dit beleid wordt zelfs afgedwongen voor gebruikers die alleen een uitnodiging voor je organisatie hebben [geaccepteerd](#).

⚠ Warning

Organisatieleden die geen eigenaar of beheerder zijn en geen tweestapsaanmelding hebben ingesteld voor hun account, worden verwijderd uit de organisatie wanneer je dit beleid activeert. Gebruikers die als gevolg van dit beleid worden verwijderd, ontvangen hiervan bericht via e-mail en moeten opnieuw worden uitgenodigd voor de organisatie. Aanvullende informatie:

- Bestaande gebruikers kunnen de uitnodiging niet accepteren, inclusief een uitnodiging om eigenaar of beheerder te worden, totdat tweestapslogin is ingeschakeld voor hun kluis.
- Nieuwe gebruikers worden automatisch ingesteld op inloggen in twee stappen via e-mail, maar kunnen dit op elk moment wijzigen.

Vereisten voor hoofdwachtwoord

Het inschakelen van het beleid **Vereisten hoofdwachtwoord** zal een configureerbare set minimumvereisten afdwingen voor de sterkte van het hoofdwachtwoord van gebruikers. Organisaties kunnen afdwingen:

- Minimale complexiteit hoofdwachtwoord
- Minimale lengte masterwachtwoord
- Typen tekens vereist

De complexiteit van wachtwoorden wordt berekend op een schaal van 0 (zwak) tot 4 (sterk). Bitwarden berekent de complexiteit van wachtwoorden met behulp van [de zxcvbn-bibliotheek](#).

Gebruik de optie **Bestaande leden verplichten hun wachtwoord te wijzigen** om bestaande, niet-conforme organisatieleden, ongeacht hun rol, te verplichten hun hoofdwachtwoord bij te werken tijdens hun volgende aanmelding. Gebruikers die een nieuwe account aanmaken vanuit de organisatie-uitnodiging worden gevraagd om een hoofdwachtwoord aan te maken dat voldoet aan jouw vereisten.

Beheer van accountherstel

Door het **beheerbeleid voor accountherstel** in te schakelen, kunnen eigenaren en beheerders [wachtwoordherstel](#) gebruiken om het hoofdwachtwoord van ingeschreven gebruikers opnieuw in te stellen. Standaard moeten gebruikers [zichzelf aanmelden voor het resetten van wachtwoorden](#), maar de optie voor [automatische aanmelding](#) kan worden gebruikt om automatische aanmelding van uitgenodigde gebruikers te forceren.

Het beheerbeleid voor accountherstel is vereist voor uw organisatie om [SSO met vertrouwde apparaten](#) te gebruiken.

📌 Note

Het beleid **Enkele organisatie** moet ingeschakeld zijn voordat dit beleid geactiveerd wordt.

Als gevolg hiervan moet je het beleid voor **het beheer van accountherstel** uitschakelen voordat je het beleid voor **één organisatie** kunt uitschakelen.

Automatische inschrijving

Als u de optie voor **automatische registratie** inschakelt, worden alle nieuwe leden, ongeacht hun rol, automatisch ingeschreven voor wachtwoord-reset wanneer hun [uitnodiging voor de organisatie wordt geaccepteerd](#) en wordt voorkomen dat ze zich terugtrekken.

Note

Gebruikers die al deel uitmaken van de organisatie zullen niet met terugwerkende kracht worden aangemeld voor het resetten van wachtwoorden en zullen [zichzelf moeten aanmelden](#).

Wachtwoord generator

Het inschakelen van het beleid **Wachtwoordgenerator** zal een configureerbare set minimumvereisten afdwingen voor alle door gebruikers gegenereerde wachtwoorden voor alle leden, ongeacht hun rol. Organisaties kunnen afdwingen:

- Wachtwoord, wachtwoordzin of gebruikersvoorkeur

Voor wachtwoorden:

- Minimale lengte wachtwoord
- Minimaal aantal (0-9)
- Minimaal aantal speciale tekens (!@#\$\$%^&*)
- Typen tekens vereist

Voor wachtwoordzinnen:

- Minimum aantal woorden
- Al dan niet kapitaliseren
- Of u nummers wilt opnemen

Warning

Bestaande wachtwoorden die niet voldoen aan het beleid zullen **niet** worden gewijzigd wanneer dit beleid wordt ingeschakeld, noch zullen de items uit de organisatie worden verwijderd. Bij het wijzigen of genereren van een wachtwoord nadat dit beleid is ingeschakeld, worden geconfigureerde beleidsregels afgedwongen.

Gebruikers krijgen een banner te zien op het scherm van de wachtwoordgenerator om aan te geven dat een beleid van invloed is op hun generatorinstellingen.

Enkele organisatie

Als je het beleid **Eén organisatie** inschakelt, kunnen leden die geen eigenaar of beheerder zijn van je organisatie geen lid worden van andere organisaties of andere organisaties aanmaken. Dit beleid wordt zelfs afgedwongen voor gebruikers die alleen een uitnodiging voor je organisatie hebben [geaccepteerd](#), maar dit beleid wordt niet afgedwongen voor eigenaren en beheerders.

 Warning

Gebruikers in de organisatie die lid zijn van meerdere organisaties worden verwijderd uit je organisatie wanneer je dit beleid inschakelt.

Gebruikers die als gevolg van dit beleid worden verwijderd, ontvangen hiervan bericht via e-mail en moeten opnieuw worden uitgenodigd voor de organisatie. Gebruikers kunnen de uitnodiging voor de organisatie pas accepteren als ze zichzelf hebben verwijderd uit alle andere organisaties.

Verificatie met eenmalige aanmelding vereisen

Als je het **authenticatiebeleid Vereisen eenmalige aanmelding** inschakelt, moeten gebruikers die geen eigenaar of beheerder zijn zich aanmelden met SSO. Als je zelf host, kun je dit beleid afdwingen voor eigenaren en beheerders met behulp van [een omgevingsvariabele](#). Voor meer informatie, zie [Aanmelding met SSO gebruiken](#). Dit beleid wordt niet afgedwongen voor eigenaars en beheerders.

Leden van organisaties die dit beleid gebruiken, kunnen niet [inloggen met een wachtwoord](#).

 Note

Het beleid **Enkele organisatie** moet zijn ingeschakeld voordat dit beleid wordt geactiveerd.

Als gevolg hiervan moet je het **authenticatiebeleid Vereisen eenmalige aanmelding** uitschakelen voordat je het beleid **Eenmalige organisatie** kunt uitschakelen.

Individuele kluis verwijderen

Door het **verwijderen van individuele kluisen** beleid aan te zetten zullen gebruikers die geen eigenaar/niet-beheerder zijn kluistitems moeten opslaan in een organisatie door te voorkomen dat organisatie leden eigenaar worden van kluistitems.

Er wordt een banner weergegeven voor gebruikers in het scherm **Item toevoegen** om aan te geven dat een beleid van invloed is op hun eigendomsopties.

Dit beleid wordt zelfs afgedwongen voor gebruikers die alleen een uitnodiging voor je organisatie hebben [geaccepteerd](#), maar dit beleid wordt niet afgedwongen voor eigenaren en beheerders.

 Note

Vault items die zijn aangemaakt voordat dit beleid werd geïmplementeerd of voordat de gebruiker bij de organisatie kwam, blijven in de individuele vault van de gebruiker.

Verwijderen Verzenden

Als u het beleid **Verzend verwijderen** inschakelt, kunnen leden die geen eigenaar of beheerder zijn geen verzendingen maken of bewerken met [Bitwarden Send](#). Leden die onder dit beleid vallen, kunnen nog steeds bestaande Verzendingen verwijderen waarvan de [verwijderingsdatum](#) nog niet is bereikt. Dit beleid wordt niet afgedwongen voor eigenaars en beheerders.

Er wordt een banner weergegeven voor gebruikers in de **Verzendweergave** en bij het openen van een bestaande verzending om aan te geven dat een beleid hen beperkt tot het verwijderen van alleen verzendingen.

Opties verzenden

Als u het beleid **Verzendopties** inschakelt, kunnen eigenaren en beheerders opties opgeven voor het maken en bewerken van Verzendingen. Dit beleid wordt niet afgedwongen voor eigenaars en beheerders. Opties zijn onder andere:

Optie	Beschrijving
Sta gebruikers niet toe hun e-mailadres te verbergen	Als u deze optie inschakelt, wordt de optie om e-mail te verbergen verwijderd, wat betekent dat bij alle ontvangen verzendingen wordt vermeld van wie ze zijn verzonden.

Time-out kluis

Door het **time-outbeleid voor kluizen** in te stellen, kunt u:

- Implementeer een maximale [time-outduur voor kluizen](#) voor alle leden van je organisatie **behalve eigenaars**. Deze optie past de time-outbeperking toe op alle clienttoepassingen (mobiel, desktop, browserextensie en meer).
- Stel een [time-out](#) actie in voor alle leden van je organisatie , **behalve de eigenaars**. Deze optie kan worden ingesteld op **Gebruikersvoorkeur**, **Vergrendelen** of **Afmelden** wanneer een time-out van de kluis optreedt.

De **Logout** optie kan bijvoorbeeld gebruikt worden om gebruikers te vragen om 2FA te gebruiken elke keer dat ze hun kluis openen en om offline gebruik te voorkomen door regelmatig lokale gegevens van de machines van gebruikers te wissen.

Er wordt een banner weergegeven voor gebruikers tijdens de time-outconfiguratie van de kluis om aan te geven dat een beleid hun opties beïnvloedt. Sommige vault timeout opties, zoals **On browser restart** of **Never** zullen niet beschikbaar zijn voor gebruikers wanneer dit beleid is geactiveerd. Dit beleid wordt niet afgedwongen voor eigenaars en beheerders.

Note

Het beleid **Enkele organisatie** moet ingeschakeld zijn voordat dit beleid geactiveerd wordt.

Als gevolg hiervan moet je het **Vault timeout** beleid uitschakelen voordat je het **Single organization** beleid kunt uitschakelen.

Individuele kluisexport verwijderen

Als u het beleid **Verwijderen individuele kluisuitvoer** inschakelt, kunnen leden van uw organisatie die geen eigenaar of beheerder zijn hun individuele kluisgegevens niet [exporteren](#). Dit beleid wordt niet afgedwongen voor eigenaars en beheerders.

In de web vault en CLI wordt een bericht weergegeven voor gebruikers dat aangeeft dat een beleid hun opties beïnvloedt. In andere clients wordt de optie gewoon uitgeschakeld.

Automatisch invullen activeren

Als u het beleid **Automatisch invullen activeren** inschakelt, wordt de [functie Automatisch invullen bij het laden van pagina's](#) op de browserextensie automatisch ingeschakeld voor alle bestaande en nieuwe leden van de organisatie. Leden kunnen desgewenst nog steeds het automatisch invullen bij het laden van een pagina uitschakelen of wijzigen voor hun browserextensie.