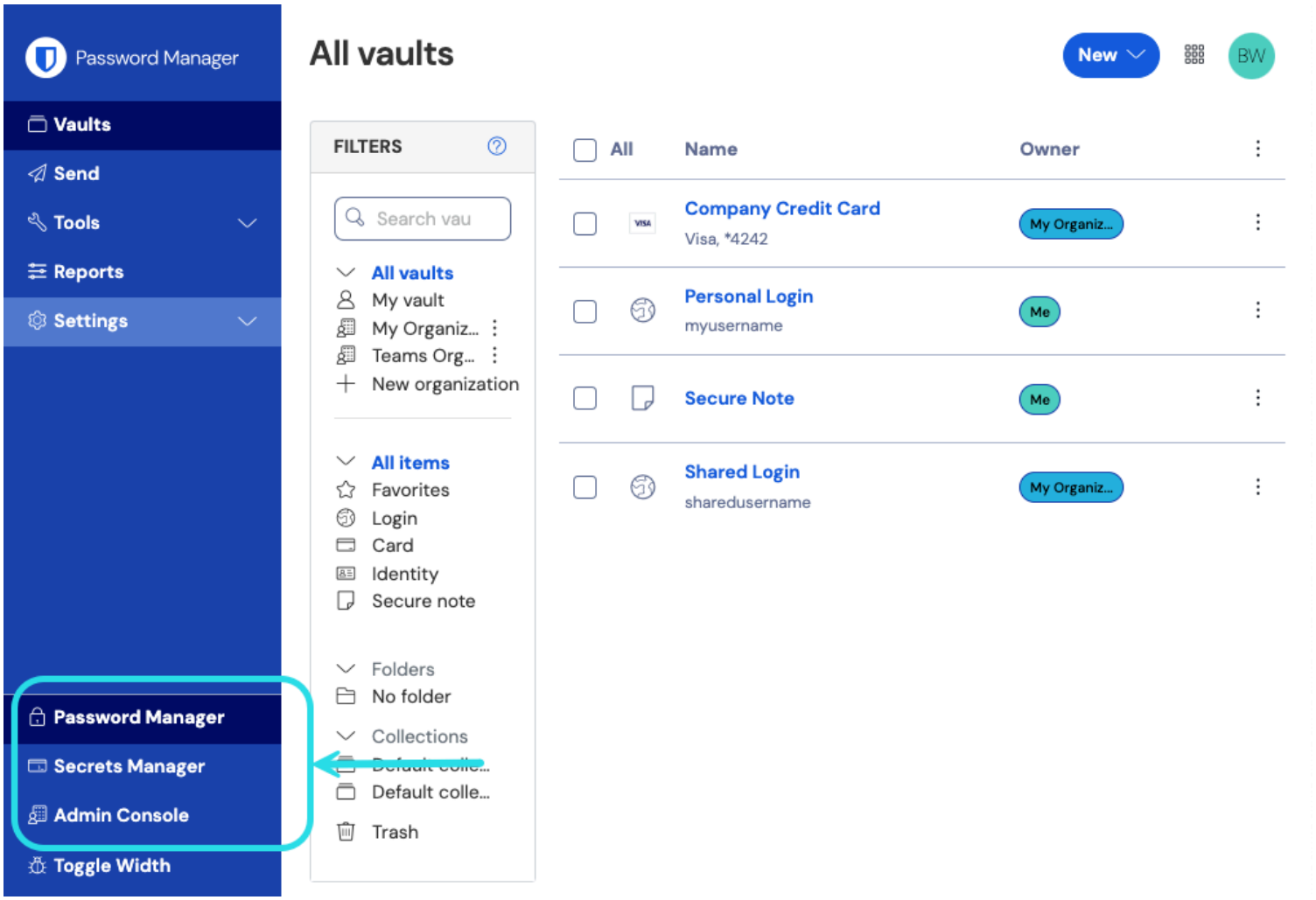
SSO instellen met vertrouwde apparaten

Weergeven in het Helpcentrum:
https://bitwarden.com/help/setup-sso-with-trusted-devices/

SSO instellen met vertrouwde apparaten

Dit document helpt je om SSO met vertrouwde apparaten toe te voegen aan je organisatie. Je moet een eigenaar of beheerder van een organisatie zijn om deze stappen te kunnen uitvoeren:

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



Product switcher

2. Selecteer **Instellingen** → **Beleid** in de navigatie.

3. Activeer op de pagina Policies de volgende beleidsregels die vereist zijn voor het gebruik van vertrouwde apparaten:

   - Het beleid **voor één organisatie**.
   - Het **authenticatiebeleid voor eenmalige aanmelding vereisen**.
   - Het beleid voor **het beheer van accountherstel** .
   - De optie **Vereis dat nieuwe leden automatisch worden ingeschreven in** het beheerbeleid voor accountherstel.

> **Note**
>
> Als je deze beleidsregels niet van tevoren activeert, worden ze automatisch geactiveerd wanneer je de optie **Vertrouwde apparaten** lid ontsleuteling activeert. Als accounts echter geen accountherstel hebben ingeschakeld, moeten ze zichzelf aanmelden voordat ze gebruik kunnen maken van beheerderstoestemming voor vertrouwde apparaten. Gebruikers die accountherstelinschakelen , moetenminstens één keer inloggen na het accountherstel om de workflow voor accountherstel volledig te voltooien.

4. Selecteer **Instellingen** > **Eenmalige aanmelding** in de navigatie. Als je nog geen SSO hebt ingesteld, volg dan een van onze SAML 2.0 of OIDC implementatiegidsen voor hulp.

5. Selecteer de optie **Vertrouwde apparaten** in de sectie Ontcijferingsopties voor leden.

Eenmaal geactiveerd kunnen gebruikers beginnen met het ontsleutelen van hun kluizen met een vertrouwd apparaat.

Als je leden wilt hebben zonder hoofdwachtwoord die **alleen** vertrouwde apparaten kunnen gebruiken, instrueer gebruikers dan om **Aanmelden** → **Enterprise SSO** te selecteren vanuit de organisatie-uitnodiging om JIT provisioning te starten. Beheerders/eigenaars moeten nog steeds de **Maak account** optie gebruiken zodat ze master wachtwoorden hebben voor redundantie en failover doeleinden.

> **Warning**
>
> Migratie van SSO met vertrouwde apparaten naar andere ontsleutelingsopties voor leden wordt momenteel niet aanbevolen:
>
> - Als je organisatie om wat voor reden dan ook de ontcijferingsoptie voor leden moet terugschakelen van vertrouwde apparaatversleuteling naar masterwachtwoord, dan moet **je** masterwachtwoorden uitgeven met behulp van accountherstel **aan alle gebruikers** die zonder deze wachtwoorden zijn aangenomen **om de toegang tot hun accounts te behouden.** Gebruikers moeten dan volledig inloggen na het herstel van het hoofdwachtwoord om de workflow te voltooien.
> - Overstappen van SSO met vertrouwde apparaten naar Key Connector wordt niet ondersteund.

De ontcijferingsoptie voor leden wijzigen van Vertrouwde apparaten naar Hoofdwachtwoord

Als de ontcijferingsoptie voor leden wordt gewijzigd van Vertrouwde apparaten naar Hoofdwachtwoord zonder hoofdwachtwoorden uit te geven, wordt de gebruikersaccount geblokkeerd. Om deze beleidswijziging door te voeren, moet u:

1. Geef masterwachtwoorden uit met accountherstel.

2. Gebruikers moeten ten minste één keer inloggen na het accountherstel om de workflow volledig te voltooien en uitsluiting te voorkomen.

Als de optie voor het ontsleutelen van leden is gewijzigd zonder een hoofdwachtwoord op te geven, blijven de volgende drie opties over voor gebruikers:

- Volg de delete-recover-workflow.
- Account herstellen vanuit een back-up van account/organisatie.
- Maak een nieuwe account of organisatie aan.