bitwarden | Artikel Helpcentrum

BEHEERCONSOLE > INLOGGEN MET SSO

OIDC-configuratie

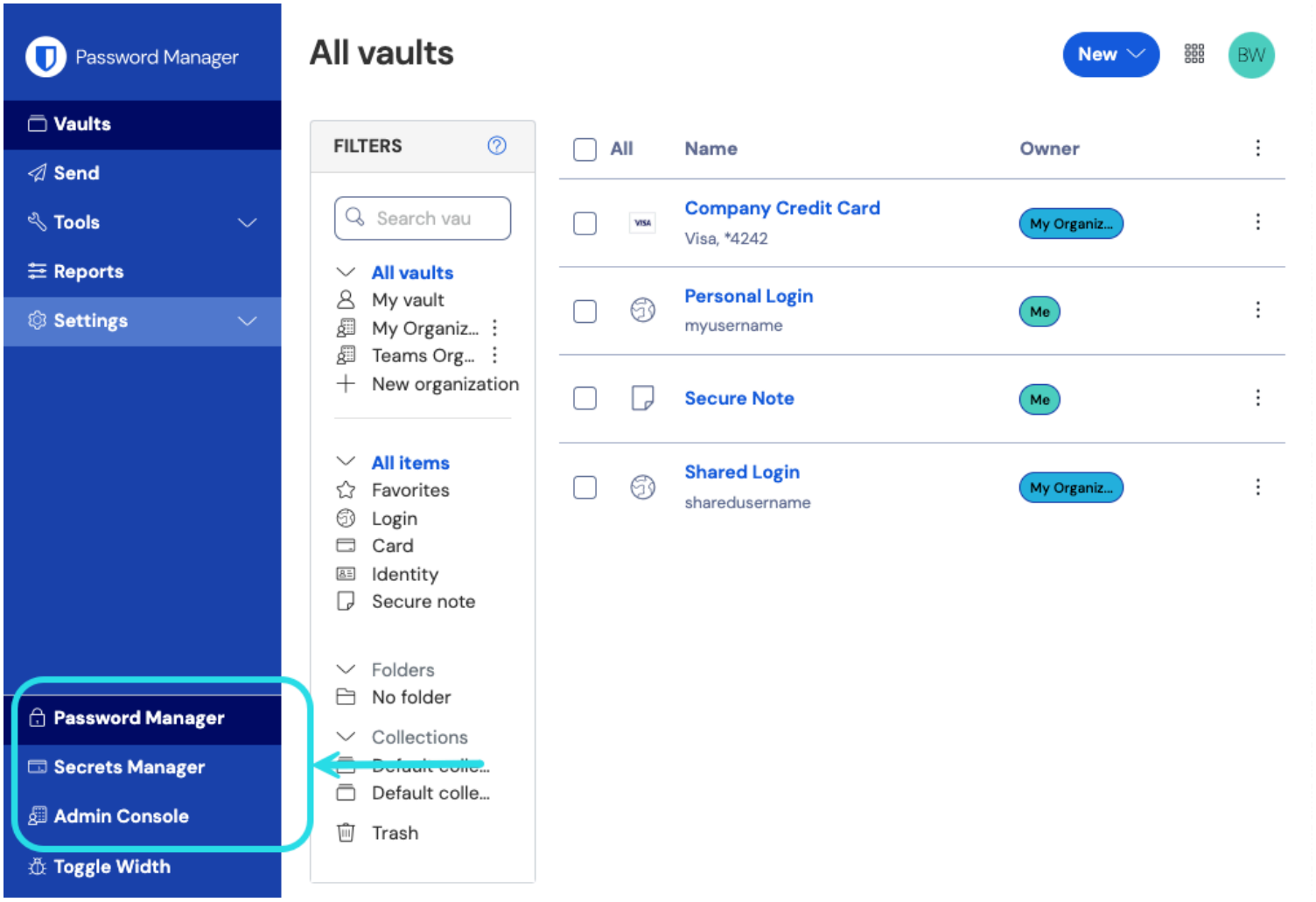
Weergeven in het Helpcentrum:
https://bitwarden.com/help/configure-sso-oidc/

OIDC-configuratie

Stap 1: Stel een SSO-identifier in

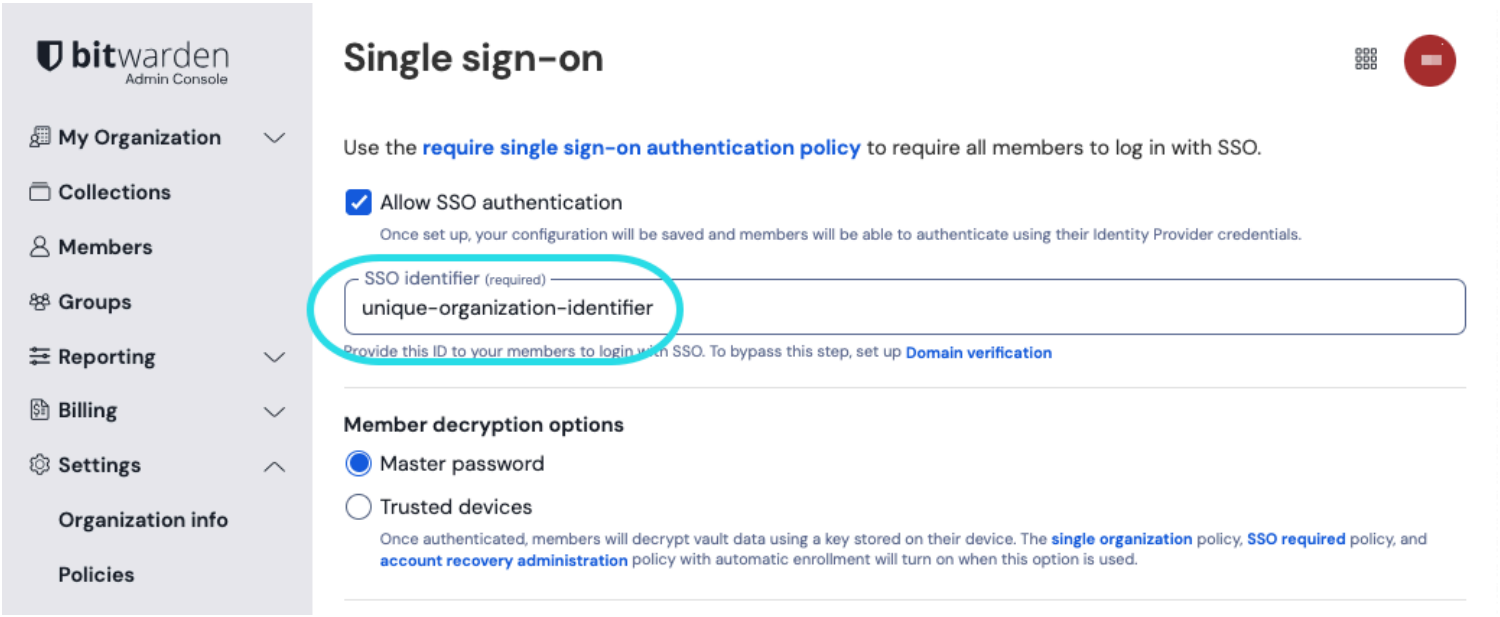
Gebruikers die hun identiteit authenticeren met behulp van SSO moeten een **SSO-identifier** invoeren die de organisatie (en dus de SSO-integratie) aangeeft waartegen ze zich moeten authenticeren. Om een unieke SSO Identifier in te stellen:

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** → **Eenmalige aanmelding** en voer een unieke **SSO-identificatie** in voor uw organisatie:



Voer een identificator in

3. Ga verder met **Stap 2: Aanmelden met SSO inschakelen**.

> **Tip**
> You will need to share this value with users once the configuration is ready to be used.

Stap 2: Inloggen met SSO inschakelen

Als je eenmaal je SSO identifier hebt, kun je verder gaan met het inschakelen en configureren van je integratie. Aanmelden met SSO inschakelen:

1. Schakel in de weergave **Instellingen** → **Eenmalige aanmelding** het selectievakje **SSO-authenticatie toestaan** in:

OIDC-configuratie

2. Selecteer in het vervolgkeuzemenu **Type** de optie **OpenID Connect**. Als je in plaats daarvan SAML wilt gebruiken, ga dan naar de SAML Configuratiegids.

> **Tip**
>
> Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met SSO met vertrouwde apparaten of Key Connector.

Stap 3: Configuratie

Vanaf dit punt varieert de implementatie van aanbieder tot aanbieder. Ga naar een van onze specifieke **implementatiehandleidingen** voor hulp bij het voltooien van het configuratieproces:

Aanbieder	Gids
Azuur	Azure Implementatiegids

Aanbieder	Gids
Okta	Okta-implementatiegids

Configuratie referentiemateriaal

De volgende secties definiëren velden die beschikbaar zijn tijdens de configuratie van single sign-on, onafhankelijk van de IdP waarmee je integreert. Velden die moeten worden geconfigureerd, worden gemarkeerd**(verplicht)**.

> **Tip**
>
> **Unless you are comfortable with OpenID Connect**, we recommend using one of the above implementation guides instead of the following generic material.

Veld	Beschrijving
Terugbelpad	**(Wordt automatisch gegenereerd)** De URL voor de automatische omleiding van de verificatie. Voor cloud-hosted klanten is dit `https://sso.bitwarden.com/oidc-signin` of `https://sso.bitwarden.eu/oidc-signin`. Voor zelf gehoste instanties wordt dit bepaald door je geconfigureerde server URL, bijvoorbeeld `https://your.domain.com/sso/oidc-signin`.
Uitgetekend terugbelpad	**(Wordt automatisch gegenereerd)** De URL voor automatisch afmelden. Voor cloud-hosted klanten is dit `https://sso.bitwarden.com/oidc-signedout` of `https://sso.bitwarden.eu/oidc-signedout`. Voor zelf gehoste instanties wordt dit bepaald door je geconfigureerde server URL, bijvoorbeeld `https://your.domain.com/sso/oidc-signedout`.
Autoriteit	**(Verplicht)** De URL van uw autorisatieserver ("Autoriteit"), waartegen Bitwarden authenticatie uitvoert. Bijvoorbeeld `https://your.domain.okta.com/oauth2/default` of `https://login.microsoft.com//v2.0`.
Klant-ID	**(Verplicht)** Een identifier voor de OIDC client. Deze waarde is typisch specifiek voor een geconstrueerde IdP-app integratie, bijvoorbeeld een Azure app registratie of Okta web app.
Geheim van de klant	**(Verplicht)** Het clientgeheim dat wordt gebruikt in combinatie met de client-ID om te ruilen voor een toegangstoken. Deze waarde is typisch specifiek voor een geconstrueerde IdP-app-integratie, bijvoorbeeld een Azure app-registratie of Okta Web App.

Veld	Beschrijving
Metadata-adres	**(Verplicht als Autoriteit niet geldig** is) Een Metadata URL waar Bitwarden toegang kan krijgen tot autorisatieserver metadata als een JSON object. Bijvoorbeeld, `https://your.domain.okta.com/oauth2/default/.well-known/oauth-authorization-server`
OIDC omleidingsgedrag	**(Verplicht**) Methode gebruikt door de IdP om te reageren op authenticatieverzoeken van Bitwarden. Opties zijn onder andere **Form POST** en **Redirect GET**.
Claims ophalen bij eindpunt gebruikersinfo	Schakel deze optie in als je URL te lang fouten (HTTP 414), afgekorte URLS en/of fouten tijdens SSO ontvangt.
Extra/aangepaste scopes	Definieer aangepaste scopes die moeten worden toegevoegd aan het verzoek (door komma's gescheiden).
Extra/aangepaste claimtypes voor gebruikers-id	Definieer aangepaste claimtype-sleutels voor gebruikersidentificatie (door komma's gescheiden). Indien gedefinieerd, wordt er eerst gezocht naar aangepaste claimtypes voordat er wordt teruggevallen op standaardtypes.
Extra/gewone e-mailclaimtypes	Definieer aangepaste claimtype-sleutels voor e-mailadressen van gebruikers (door komma's gescheiden). Indien gedefinieerd, wordt er eerst gezocht naar aangepaste claimtypes voordat er wordt teruggevallen op standaardtypes.
Extra/aangepaste claimtypes	Definieer aangepaste claimtype-sleutels voor de volledige namen of weergavenamen van gebruikers (door komma's gescheiden). Indien gedefinieerd, wordt er eerst gezocht naar aangepaste claimtypes voordat er wordt teruggevallen op standaardtypes.
Opgevraagde referentiewaarden voor authenticatiecontextklasse	Definieer referentie-identifiers voor authenticatiecontextklassen(`acr_waarden`) (spatiegedefinieerd). Lijst `acr_waarden` in voorkeursvolgorde.
Verwachte "acr" claimwaarde in antwoord	Definieer de `acr-claimwaarde` die Bitwarden verwacht en valideert in het antwoord.

OIDC-kenmerken en claims

Voor account provisioning is een **e-mailadres** nodig, dat kan worden doorgegeven als een van de attributen of claims in de onderstaande tabel.

Een unieke gebruikersidentificatie wordt ook ten zeerste aanbevolen. Als dit niet het geval is, wordt in plaats daarvan e-mail gebruikt om de gebruiker te linken.

Attributen/claims worden vermeld in volgorde van voorkeur voor overeenkomst, inclusief eventuele fallbacks:

Waarde	Claim/Attribuut	Terugvalclaim/attribuut
Uniek ID	Aangepaste gebruikers-ID-claims geconfigureerd NameID (indien niet van voorbijgaande aard) urn:oid:0.9.2342.19200300.100.1.1 Sub UID UPN EPPN	
E-mail	Aangepaste e-mailclaims geconfigureerd E-mail http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress urn:oid:0.9.2342.19200300.100.1.3 Mail E-mailadres	Voorkeur gebruikersnaam Urn:oid:0.9.2342.19200300.100.1.1 UID
Naam	Aangepaste naamclaims geconfigureerd Naam http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 Weergavenaam CN	Voornaam + " " + Achternaam (zie hieronder)
Voornaam	urn:oid:2.5.4.42 Voornaam Voornaam FN FN-naam Bijnaam	

Waarde	Claim/Attribuut	Terugvalclaim/attribuut
Achternaam	urn:oid:2.5.4.4 SN Achternaam Achternaam	