Microsoft Entra ID OIDC-implementatie

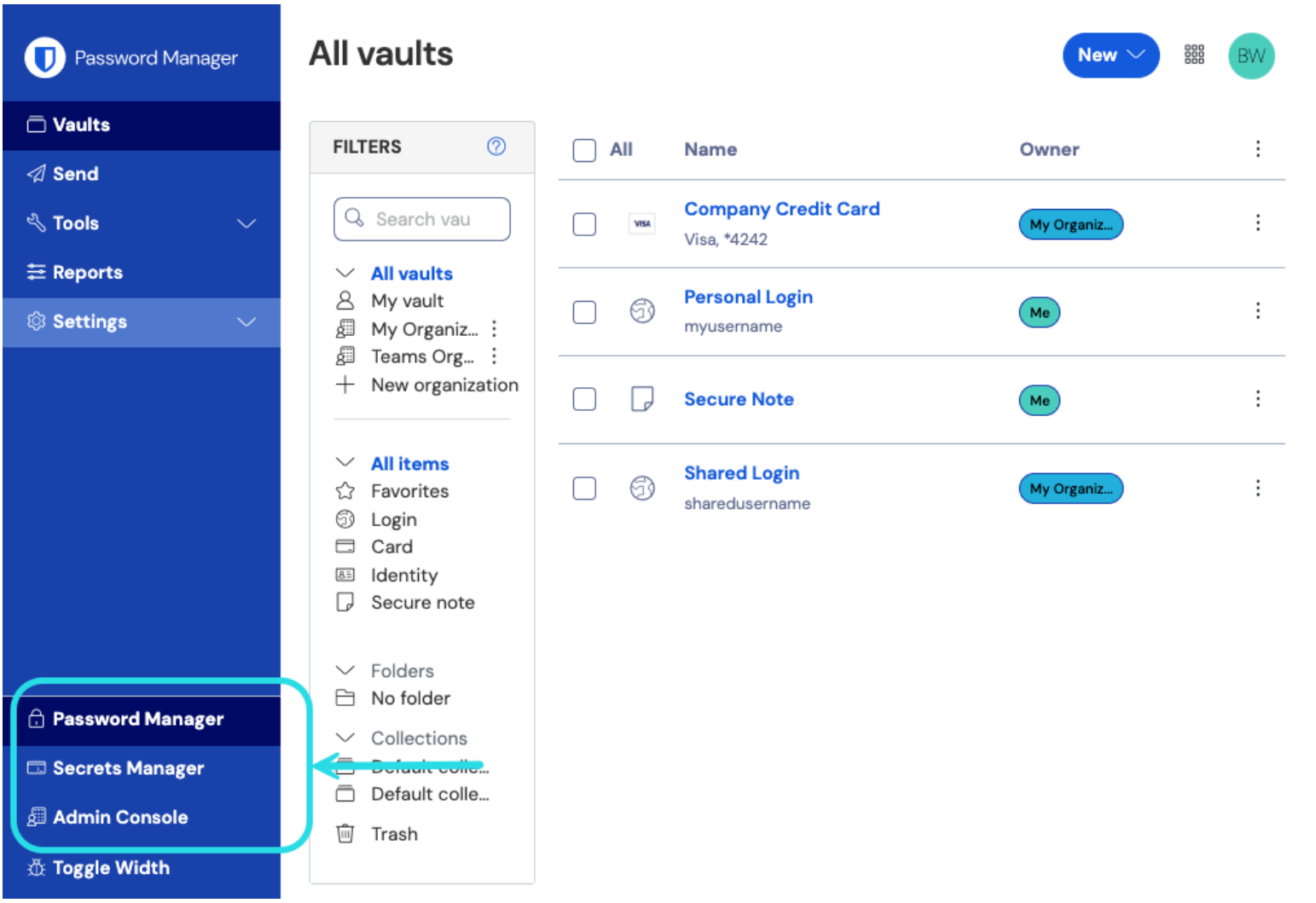
Microsoft Entra ID OIDC-implementatie

Dit artikel bevat **Azure-specifieke** hulp voor het configureren van Inloggen met SSO via OpenID Connect (OIDC). Voor hulp bij het configureren van Inloggen met SSO voor een andere OIDC IdP, of voor het configureren van Microsoft Entra ID via SAML 2.0, zie OIDC Configuratie of Microsoft Entra ID SAML Implementatie.

Bij de configuratie wordt tegelijkertijd gewerkt binnen de Bitwarden webapp en de Azure Portal. We raden u aan om beide documenten bij de hand te hebben en de stappen uit te voeren in de volgorde waarin ze zijn beschreven.

Open SSO in de webkluis

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



Product switcher

Selecteer **Instellingen** → **Eenmalige aanmelding** in de navigatie:

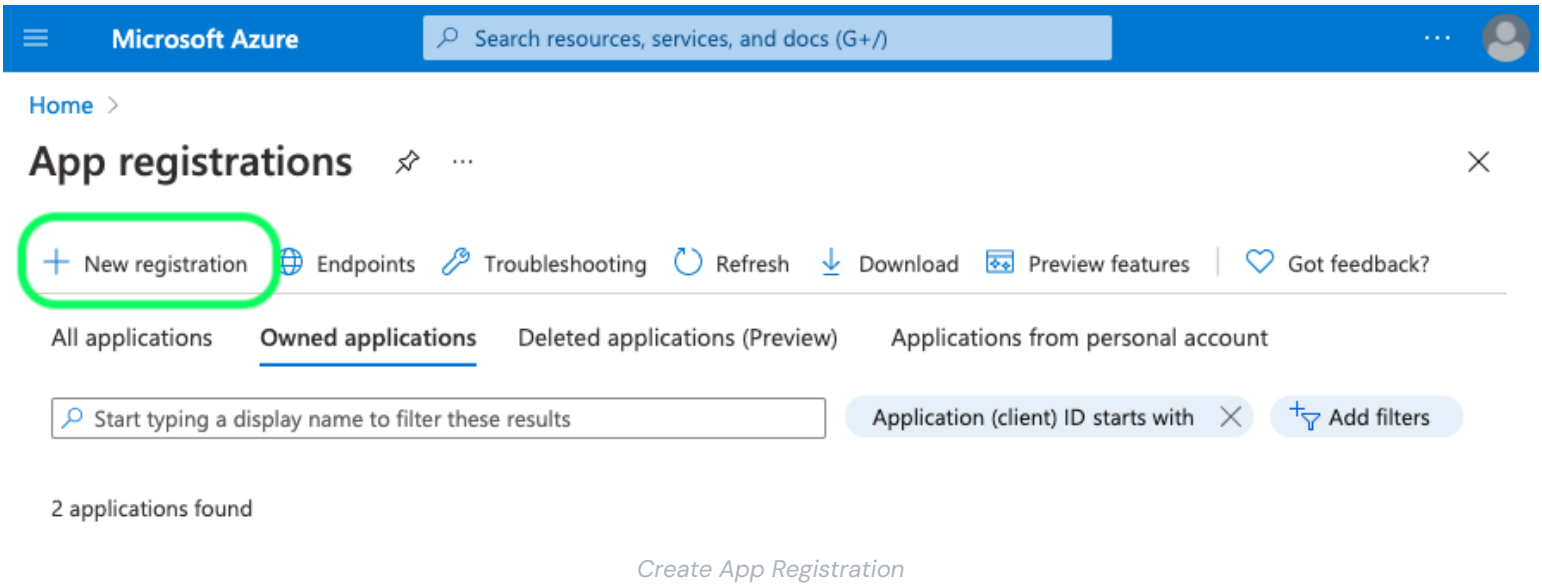
OIDC-configuratie

Als je dit nog niet hebt gedaan, maak dan een unieke **SSO identifier** aan voor je organisatie. Verder hoef je nog niets aan te passen op dit scherm, maar houd het open voor gemakkelijke referentie.

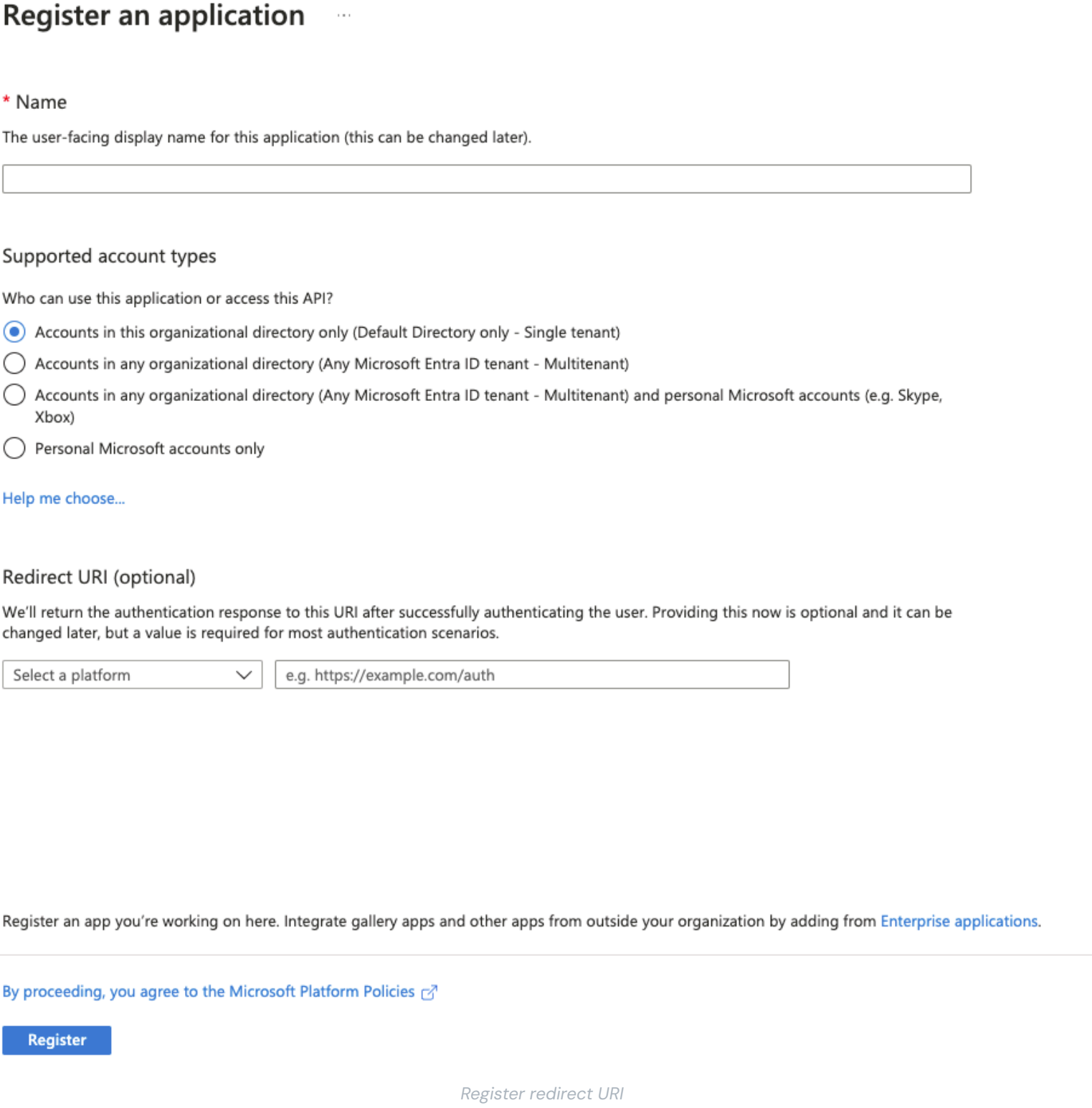
> **Tip**
>
> Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met SSO met vertrouwde apparaten of Key Connector.

Een app-registratie maken

Navigeer in de Azure Portal naar **Microsoft Entra ID** en selecteer **App registraties.** Om een nieuwe app-registratie te maken, selecteert u de knop **Nieuwe registratie**:



Vul de volgende velden in:



Register redirect URI

1. In het scherm **Applicatie registreren** geeft u uw applicatie een Bitwarden-specifieke naam en geeft u aan welke accounts de applicatie moeten kunnen gebruiken. Deze selectie bepaalt welke gebruikers gebruik kunnen maken van Bitwarden login met SSO.

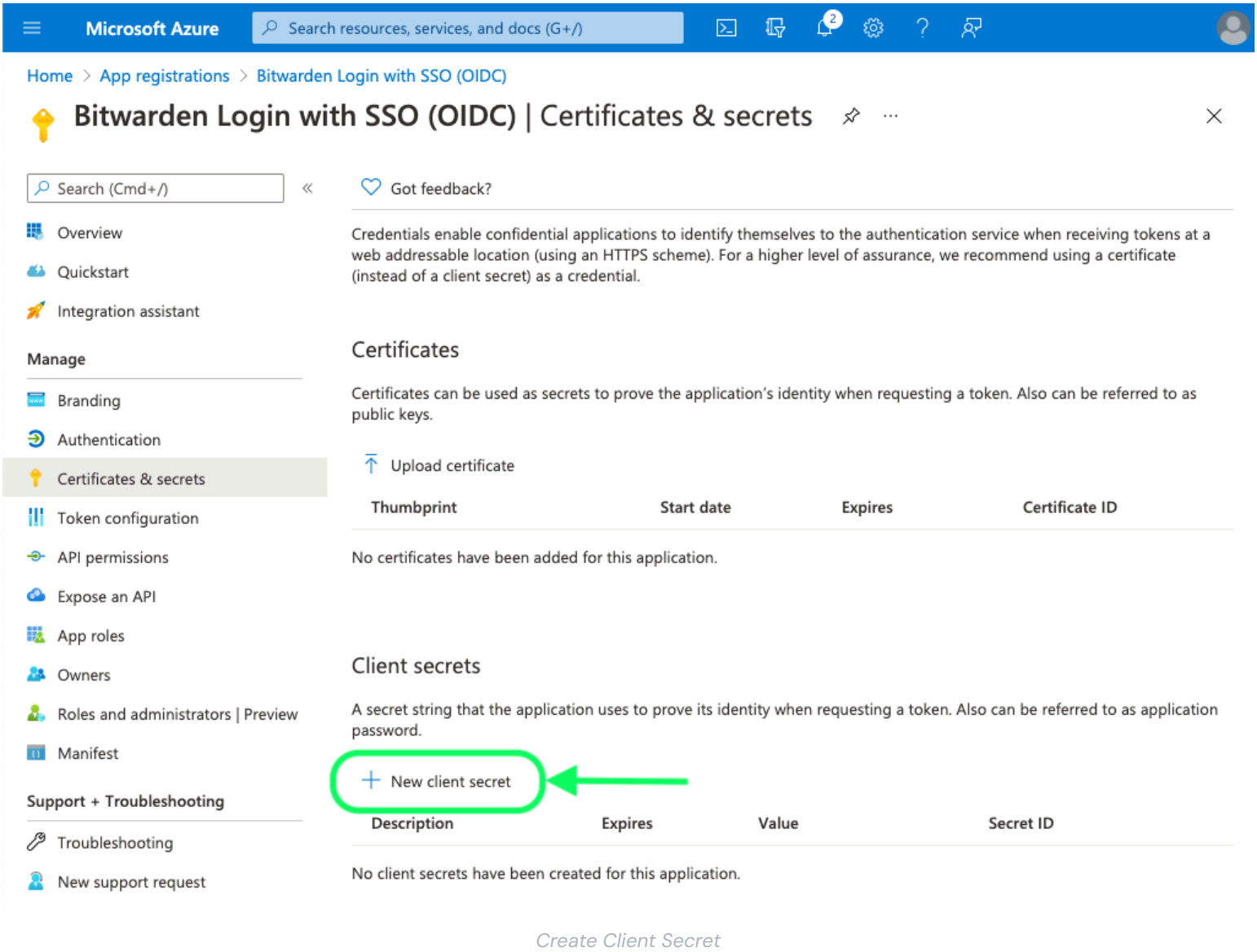
2. Selecteer **Authenticatie** in de navigatie en selecteer de knop **Een platform toevoegen**.

3. Selecteer de optie **Web** op het scherm Configureer platformen en voer uw **Terugbelpad** in bij de invoer Redirect URI's.

> **Note**
> Callback Path can be retrieved from the Bitwarden SSO Configuration screen. For cloud-hosted customers, this is `https://sso.bitwarden.com/oidc-signin` or `https://sso.bitwarden.eu/oidc-signin`. For self-hosted instances, this is determined by your configured server URL, for example `https://your.domain.com/sso/oidc-signin`.

Een cliëntgeheim maken

Selecteer **Certificaten & geheimen** in de navigatie en selecteer de knop **Nieuw clientgeheim**:



Geef het certificaat een Bitwarden-specifieke naam en kies een vervaldatum.

Beheerders toestemming maken

Selecteer **API-rechten** en klik op ✓ **Verleen beheerdersrechten voor Standaardmap**. De enige benodigde toestemming is standaard toegevoegd, Microsoft Graph > User.Read.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de Azure Portal. Ga terug naar de Bitwarden web app om de volgende velden te configureren:

Veld	Beschrijving
Autoriteit	Voer `https://login.microsoft.com//v2.0` in, waarbij `TENANT_ID` de **ID-waarde van de Directory (huurder)** is die is opgehaald uit het scherm Overzicht van de app-registratie.
Klant-ID	Voer de **applicatie (client) ID** van de app-registratie in, die kan worden gevonden in het overzichtsscherm.
Geheim van de klant	Voer de **geheime waarde** van het aangemaakte clientgeheim in.
Metadata-adres	Voor Azure implementaties zoals gedocumenteerd, kun je dit veld leeg laten.
OIDC omleidingsgedrag	Selecteer **Formulier POST** of **Redirect GET**.
Claims ophalen bij eindpunt gebruikersinformatie	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 gebruikers-ID Claimtypes	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.

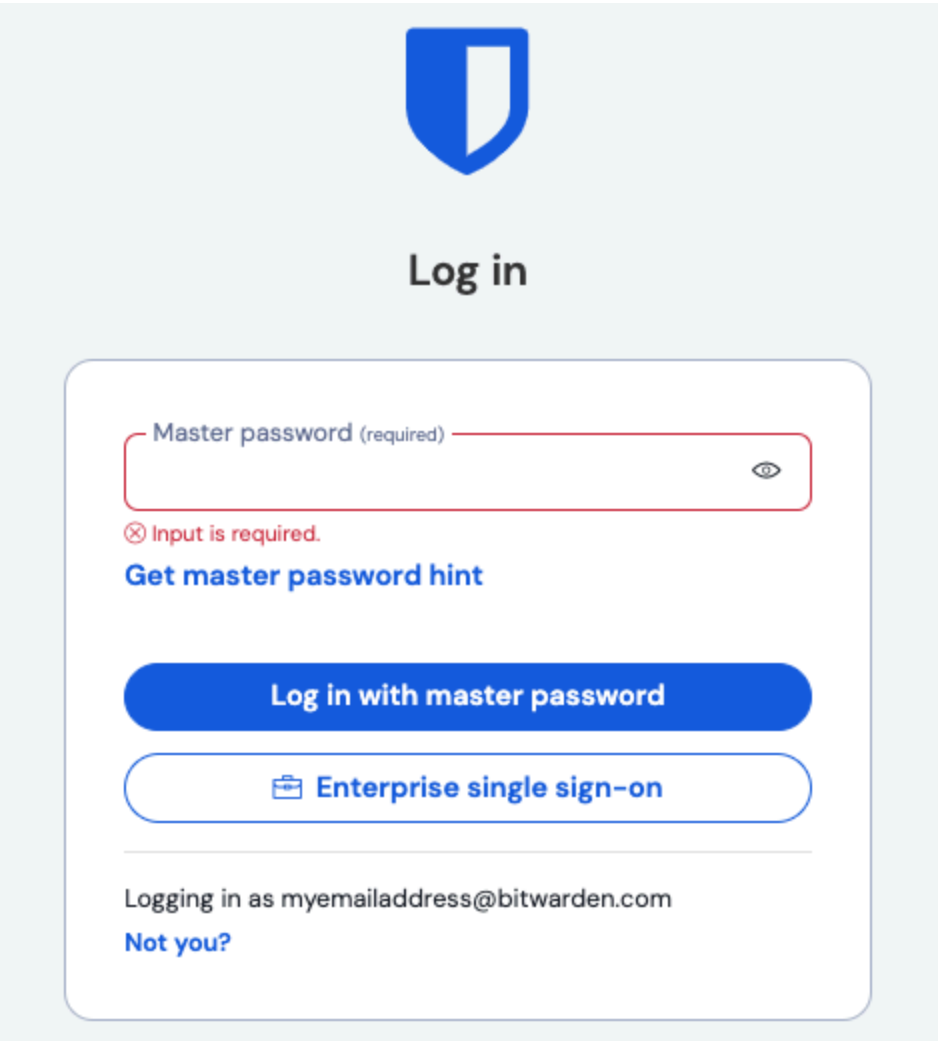
Veld	Beschrijving
Extra/Aangepaste naam Claimtypes	Definieer aangepaste claimtype-sleutels voor de volledige namen of weergavenamen van gebruikers (door komma's gescheiden). Indien gedefinieerd, wordt er eerst gezocht naar aangepaste claimtypes voordat er wordt teruggevallen op standaardtypes.
Referentiewaarden aangevraagde Authenticatie Context Klasse	Definieer Authentication Context Class Reference identifiers (`acr_values`) (spatie-limited). Lijst `acr_waarden` in voorkeursvolgorde.
Verwachte "acr" claimwaarde in antwoord	Definieer de `acr` Claim Value die Bitwarden verwacht en valideert in het antwoord.

Sla je werk **op** als je klaar bent met het configureren van deze velden.

> **Tip**
> Je kunt gebruikers verplichten om in te loggen met SSO door het authenticatiebeleid voor eenmalige aanmelding te activeren. Let op, hiervoor moet ook het beleid voor één organisatie worden geactiveerd. Meer informatie.

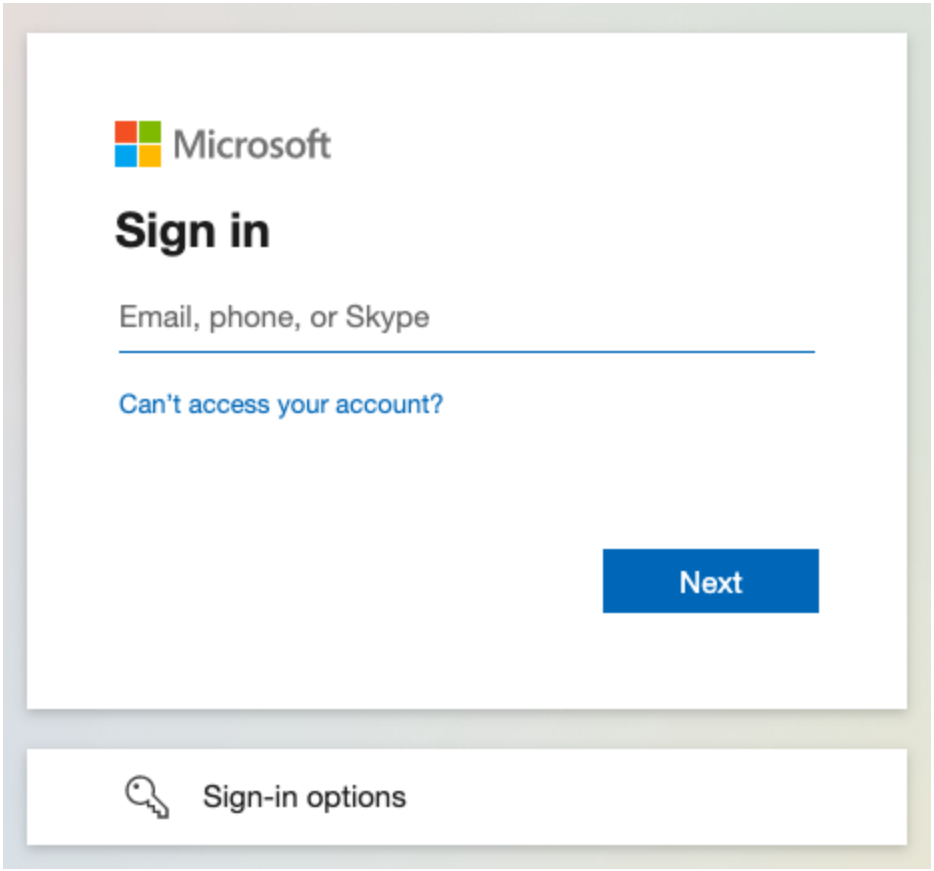
De configuratie testen

Zodra je configuratie voltooid is, kun je deze testen door te navigeren naar https://vault.bitwarden.com, je e-mailadres in te voeren, **Doorgaan** te selecteren en de knop **Enterprise Single-On** te selecteren:



Enterprise single sign on en hoofdwachtwoord

Voer de geconfigureerde organisatie-ID in en selecteer **Aanmelden**. Als uw implementatie met succes is geconfigureerd, wordt u doorgestuurd naar het inlogscherm van Microsoft:



Azure login screen

Nadat u zich hebt geverifieerd met uw Azure-referenties, voert u uw Bitwarden-hoofdwachtwoord in om uw kluis te ontsleutelen!

> **Note**
> Bitwarden ondersteunt geen ongevraagde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSO-aanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden.

Volgende stappen

1. Leer de leden van je organisatie hoe ze moeten inloggen met SSO.