

BEHEERCONSOLE > INLOGGEN MET SSO >

Microsoft Entra ID OIDC- implementatie

Weergeven in het Helpcentrum:

<https://bitwarden.com/help/oidc-microsoft-entra-id/>

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 (☰):

The screenshot displays the Bitwarden web application interface. On the left is a dark blue sidebar with navigation items: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. The main content area is titled 'All vaults' and features a 'New' button, a product switcher icon (☰), and a user profile icon (BW). Below the title is a 'FILTERS' panel with a search bar and a list of categories: All vaults, All items, Favorites, Login, Card, Identity, Secure note, Folders, Collections, and Trash. The main vault list includes: Company Credit Card (My Organiz...), Personal Login (Me), Secure Note (Me), and Shared Login (My Organiz...). A red circle highlights the 'Password Manager' option in the sidebar, and a red arrow points to the product switcher icon in the top right corner.

Product switcher

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

bitwarden Admin Console

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

Single sign-on



Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type

OpenID connect configuration

Callback path

Signed out callback path

OIDC-configuratie

Als je dit nog niet hebt gedaan, maak dan een unieke **SSO identifier** aan voor je organisatie. Verder hoeft 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**:

Home >

App registrations

[+ New registration](#) [Endpoints](#) [Troubleshooting](#) [Refresh](#) [Download](#) [Preview features](#) | [Got feedback?](#)

All applications **Owned applications** Deleted applications (Preview) Applications from personal account

[Application \(client\) ID starts with](#) [Add filters](#)

2 applications found

[Create App Registration](#)

Vul de volgende velden in:

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

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**:

The screenshot shows the Microsoft Azure portal interface. The breadcrumb path is Home > App registrations > Bitwarden Login with SSO (OIDC). The page title is 'Bitwarden Login with SSO (OIDC) | Certificates & secrets'. On the left, there is a navigation menu with 'Certificates & secrets' selected. The main content area has a search bar and a 'Got feedback?' link. Below that, there is a section for 'Certificates' with a description and an 'Upload certificate' button. A table with columns 'Thumbprint', 'Start date', 'Expires', and 'Certificate ID' is shown, with the message 'No certificates have been added for this application.' Below this is a section for 'Client secrets' with a description and a '+ New client secret' button highlighted with a green circle and arrow. A table with columns 'Description', 'Expires', 'Value', and 'Secret ID' is shown, with the message 'No client secrets have been created for this application.' At the bottom, there is a link 'Create Client Secret'.

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:



Log in

Master password (required)



⊗ Input is required.

[Get master password hint](#)

Log in with master password

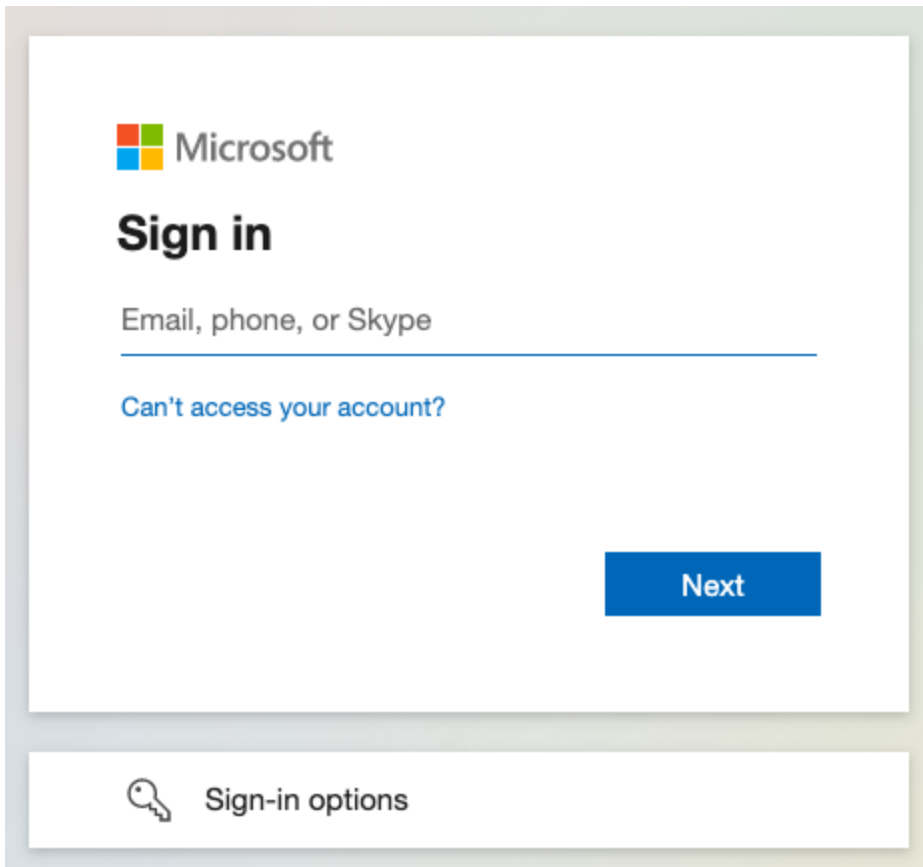
 Enterprise single sign-on

Logging in as myemailaddress@bitwarden.com

[Not you?](#)

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 inlogscherf 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 ongevroegde 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](#).