BEHEERCONSOLE → INLOGGEN MET SSO →

Microsoft Entra ID OIDCimplementatie

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 (闘):

Password Manager	All vaults			New 🗸	BW BW
🗇 Vaults	FILTERS ⑦		Name	Owner	:
🕼 Send					•
🖏 Tools 🛛 🗸 🗸 🗸	Q Search vau	AZIV	Company Credit Card Visa, *4242	My Organiz	:
፰ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Vault	0 6	myusername	Ме	:
	+ New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	:
 Password Manager Secrets Manager <i>₫</i> Admin Console <i>ἇ</i> Toggle Width 	 Folders No folder Collections Default colle Default colle Trash 				

Product switcher

Selecteer Instellingen → Eenmalige aanmelding in de navigatie:

Secure and trusted open source password manager for business

D bit warden	Single sign-on 🖩 🗧
🗐 My Organization $~~ \lor~~$	Use the require single sign-on authentication policy to require all members to log in with SSO.
 ☐ Collections △ Members ※ Groups ☆ Reporting × 	 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) unique-organization-identifier Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
Billing V	Member decryption options
Settings	Master password
Organization info Policies	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.
Two-step login	C Type
Import data	OpenID Connect ~
Export vault	
Domain verification	OpenID connect configuration
Single sign-on	Callback path
Device approvals	- Signed out collback path
SCIM provisioning	

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**:



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.

Select a platform 🗸 🗸		e.g. https://example.com/auth
-----------------------	--	-------------------------------

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.

(i) Note

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

Een cliëntgeheim maken

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

■ Microsoft Azure	resources, services, and docs (G+/)	Σ	₽ 🖓 ©	? &	
Home > App registrations > Bitwarden	Login with SSO (OIDC)				
💡 Bitwarden Login wit	t h SSO (OIDC) Cert	tificates & se	crets 🖈 …		\times
Search (Cmd+/) «	♡ Got feedback?				
Overview	Credentials enable confidential ap	plications to identify th	emselves to the authen	ntication service when receivi	ng tokens at a
🍊 Quickstart	web addressable location (using a (instead of a client secret) as a cre	in HTTPS scheme). For a dential.	higher level of assuran	nce, we recommend using a c	ertificate
🚀 Integration assistant					
Manage	Certificates				
Branding	Certificates can be used as secrets	s to prove the applicatio	n's identity when reque	esting a token. Also can be re	eferred to as
Authentication	T T				
📍 Certificates & secrets	↑ Upload certificate				
Token configuration	Thumbprint	Start date	Expires	Certificate II)
API permissions	No certificates have been added f	or this application.			
Expose an API					
App roles					
A Owners	Client secrets				
🝰 Roles and administrators Preview	A secret string that the application password.	n uses to prove its ident	ity when requesting a t	token. Also can be referred to	as application
11 Manifest					
Support + Troubleshooting	+ New client secret				
P Troubleshooting	Description	Expires	Value	Secret ID	
New support request	No client secrets have been create	ed for this application.			

Create Client Secret

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

Beheerders toestemming maken

Selecteer **API-rechten** en klik op \checkmark **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 <mark>acr</mark> 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 to Bitwarden
Email address (required) Remember email
Continue
or
& Log in with passkey
🖻 Use single sign-on
New to Bitwarden? Create account

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:

Microsoft	
Sign in	
Email, phone, or Skype	
Can't access your account?	
	Next
	Next
	Next

Azure login screen

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

(i) Note

Bitwarden ondersteunt geen ongevraagde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSOaanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden.

Volgende stappen

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