### BEHEERCONSOLE > INLOGGEN MET SSO >

# **ADFS OIDC-implementatie**

Weergeven in het Helpcentrum: https://bitwarden.com/help/adfs-oidc-implementation/

# **U bit**warden

### **ADFS OIDC-implementatie**

Dit artikel bevat **Active Directory Federation Services (AD FS)-specifieke** hulp voor het configureren van aanmelden met SSO via OpenID Connect (OIDC). Voor hulp bij het configureren van aanmelding met SSO voor een andere OIDC IdP, of voor het configureren van AD FS via SAML 2.0, zie OIDC-configuratie of ADFS SAML-implementatie.

Bij de configuratie wordt tegelijkertijd gewerkt binnen de Bitwarden webapp en de AD FS Server Manager. 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 (2008):

D Password Manager	All vaults			New V	BW BW
🗇 Vaults	FILTERS		Namo	Owner	:
🖉 Send			Name	Owner	•
🖏 Tools 🛛 🗸 🗸 🗸	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
æ Reports	✓ All vaults		Personal Legin		
🕸 Settings 🛛 🗸 🗸	∠ My vault ∅ My Organiz :		myusername	Me	:
	+ New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>□ Card</li> <li>Identity</li> <li>□ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	i
<ul> <li>Password Manager</li> <li>Secrets Manager</li> <li>Admin Console</li> <li> <sup>™</sup> Toggle Width     </li> </ul>	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				

Product switcher

Selecteer Instellingen → Eenmalige aanmelding in de navigatie:

<b>D bit</b> warden	Single sign-on 🗰 😑
g My Organization $~~ \lor~~$	Use the <b>require single sign-on authentication policy</b> to require all members to log in with SSO.
Collections	Allow SSO authentication
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
뿅 Groups	SSO Identifier (required) unique-organization-identifier
$ eiler Reporting \qquad \lor $	Provide this ID to your members to login with SSO. To bypass this step, set up <b>Domain verification</b>
🛱 Billing $\checkmark$	Member decryption options
🕸 Settings 🛛 🔿	Master password
Organization info	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	Type
Import data	
Export vault	
Domain verification	OpenID connect configuration
Single sign-on	Callback path
Device approvals	Signed out callback 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 applicatiegroep maken

Navigeer in Server Manager naar AD FS Management en maak een nieuwe applicatiegroep:

- 1. Selecteer in de consolestructuur Toepassingsgroepen en kies Toepassingsgroep toevoegen in de lijst Acties.
- 2. Kies in het welkomstscherm van de wizard de sjabloon Serverapplicatie die toegang heeft tot een web-API.

#### 翰 Add Application Group Wizard

### Secure and trusted open source password manager for business

#### Welcome

Steps	Name:
Welcome	BitwardenCloud
<ul> <li>Server application</li> </ul>	Description
<ul> <li>Configure Application Credentials</li> </ul>	
Configure Web API	
Apply Access Control Policy	Template:
<ul> <li>Configure Application Permissions</li> </ul>	Client-Server applications
Summary	Native application accessing a web API
Complete	Server application accessing a web API
	web browser accessing a web application
	Standalone applications
	🖳 Native application
	Server application
	web API
	-
	More information
	< Previous Next > Cancel

AD FS Add Application Group

3. In het scherm Servertoepassing:

输 Add Application Group V	Vizard	×
Server application		
Steps	Name:	
Welcome	BitwardenCloud - Server application	
Server application	Client Identifier	
<ul> <li>Configure Application Credentials</li> </ul>	27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d	
Configure Web API	Redirect URI:	
Apply Access Control Policy	Example: https://Contoso.com	Add
<ul> <li>Configure Application Permissions</li> </ul>	https://sso.bitwarden.com/oidc-signin	Remove
Summary		
<ul> <li>Complete</li> </ul>		
	Description:	
	< Previous Next >	Cancel

AD FS Server Application screen

- Geef de servertoepassing een naam.
- Let op de Client Identifier. U hebt deze waarde nodig in een volgende stap.
- Geef een Redirect URI op. Voor cloud-hosted klanten is dit https://sso.bitwarden.com/oidc-signin of https://sso.bit warden.eu/oidc-signin. Voor zelf gehoste instanties wordt dit bepaald door je geconfigureerde Server URL, bijvoorbeeld http s://your.domain.com/sso/oidc-signin.

4. Let op het Client Secret in het scherm Configure Application Credentials. U hebt deze waarde nodig in een volgende stap.

5. Op het scherm Web API configureren:

훾 Add Application Group Wi	zard	:	×	G
Configure Web API				h
Steps	Name:			
Welcome	BitwardenCloud - Web API			L
Server application	Identifier		_	l
<ul> <li>Configure Application Credentials</li> </ul>	Example: https://Contoso.com	Add		
Configure Web API	27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d	Remove		
Apply Access Control Policy	https://sso.bitwarden.com/		_	
<ul> <li>Configure Application Permissions</li> </ul>				
Summary	Description:			
Complete				
	< Previous Next >	Cancel		

AD FS Configure Web API screen

- Geef de Web API een naam.
- Voeg de Client Identifier en Redirect URI (zie stap 2B. & C.) toe aan de lijst Identifier.

6. Stel in het scherm Toegangsbeheerbeleid toepassen een geschikt toegangsbeheerbeleid in voor de Toepassingsgroep.

7. Sta in het scherm Toepassingsmachtigingen configureren de scopes allatclaims en openid toe.

翰 Add Application Group Wi	izard				×
Configure Application I	Permissions				
Steps Welcome	Configure permission Client application (ca	ns to enable client applica aller):	ations to access this W	/eb API.	
<ul> <li>Server application</li> <li>Configure Application Credentials</li> <li>Configure Web API</li> <li>Apply Access Control Policy</li> <li>Configure Application Permissions</li> <li>Summary</li> </ul>	Name BitwardenCloud - S	Gerver application	Description		
Complete	Permitted scopes: Scope Name allatclaims aza email logon_cert openid profile user_imperso von cert	Description Requests the access Scope allows broker of Request the email cla The logon_cert scope Request use of the O Request profile related Request permission for The von cert scope a	token claims in the ide client to request primary im for the signed in use allows an application penID Connect authori d claims for the signed or the application to ac- allows an application to	Add entity token. y refresh token. er. to request logo ization protocol. in user. cess the resour o request VPN	Remove
			< Pre	evious Next >	Cancel

AD FS Configure Application Permissions screen

8. Voltooi de wizard Toepassingsgroep toevoegen.

#### Een claimregel transformeren toevoegen

Navigeer in Server Manager naar AD FS Management en bewerk de gemaakte applicatiegroep:

- 1. Selecteer in de consolestructuur **Toepassingsgroepen**.
- 2. Klik in de lijst Toepassingsgroepen met de rechtermuisknop op de aangemaakte toepassingsgroep en selecteer Eigenschappen.
- 3. Kies in de sectie Toepassingen de Web-API en selecteer **Bewerken...** .
- 4. Navigeer naar het tabblad Regels voor de uitgifteomzetting en selecteer de knop Regel toevoegen. ...
- 5. Selecteer in het scherm Choose Rule Type de optie Send LDAP Attributes as Claims.
- 6. In het scherm Claim Rule configureren:

훾 Add Transform Claim Rule	Wizard			×
Configure Rule				
Configure Rule Steps Choose Rule Type Configure Claim Rule	You ca to extra from th Claim r email Rule te Attribut Active	an configure this rule to send the values o act LDAP attributes. Specify how the attrib e rule. ule name: emplate: Send LDAP Attributes as Claims te store: Directory ng of LDAP attributes to outgoing claim ty LDAP Attribute (Select or type to add more) E-Mail-Addresses	f LD bute	)AP attributes as claims. Select an attribute store from which as will map to the outgoing claim types that will be issued
				< Previous Finish Cancel

AD FS Configure Claim Rule screen

- Geef de regel een Claim-regelnaam.
- Selecteer E-mailadressen in de vervolgkeuzelijst LDAP-attribuut .
- Selecteer E-mailadres in de vervolgkeuzelijst Type uitgaande claim.

7. Selecteer afwerking.

#### Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de wedstrijd van de AD FS Server Manager. Ga terug naar de Bitwarden web app om de volgende velden te configureren:

Veld	Beschrijving
Autoriteit	Voer de hostnaam van uw AD FS-server in met /adfs als toevoeging, bijvoorbeeld https://adfs.mybusiness.com/adfs.
Klant-ID	Voer de opgehaalde Client ID in.
Geheim van de klant	Voer het opgehaalde Client Secret in.
Metadata-adres	Voer de opgegeven Authority-waarde in met /.well-known/openid-configuration toegevoegd, bijvoorbeeld https://adfs.mybusiness.com/adfs/.well-known/openid-configuration.
OIDC omleidingsgedrag	Selecteer GET omleiden.
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.
Aangepaste scopes	Definieer aangepaste scopes die moeten worden toegevoegd aan het verzoek (door komma's gescheiden).
Klant 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.
Typen e-mailclaims	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.
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.

Veld	Beschrijving
Aangevraagde Authenticatie Context Klasse Referentiewaarden	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
Maste	er password (required)
Get ma	aster password hint
	Log in with master password
$\square$	🖻 Enterprise single sign-on
Logging	in as myemailaddress@bitwarden.com

Enterprise single sign on en hoofdwachtwoord

Voer de geconfigureerde Organisatie-ID in en selecteer **Aanmelden**. Als uw implementatie succesvol is geconfigureerd, wordt u doorgestuurd naar het AD FS SSO inlogscherm. Nadat u zich hebt geverifieerd met uw AD FS-gegevens, 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.