

BEHEERCONSOLE > INLOGGEN MET SSO >

Okta OIDC-implementatie

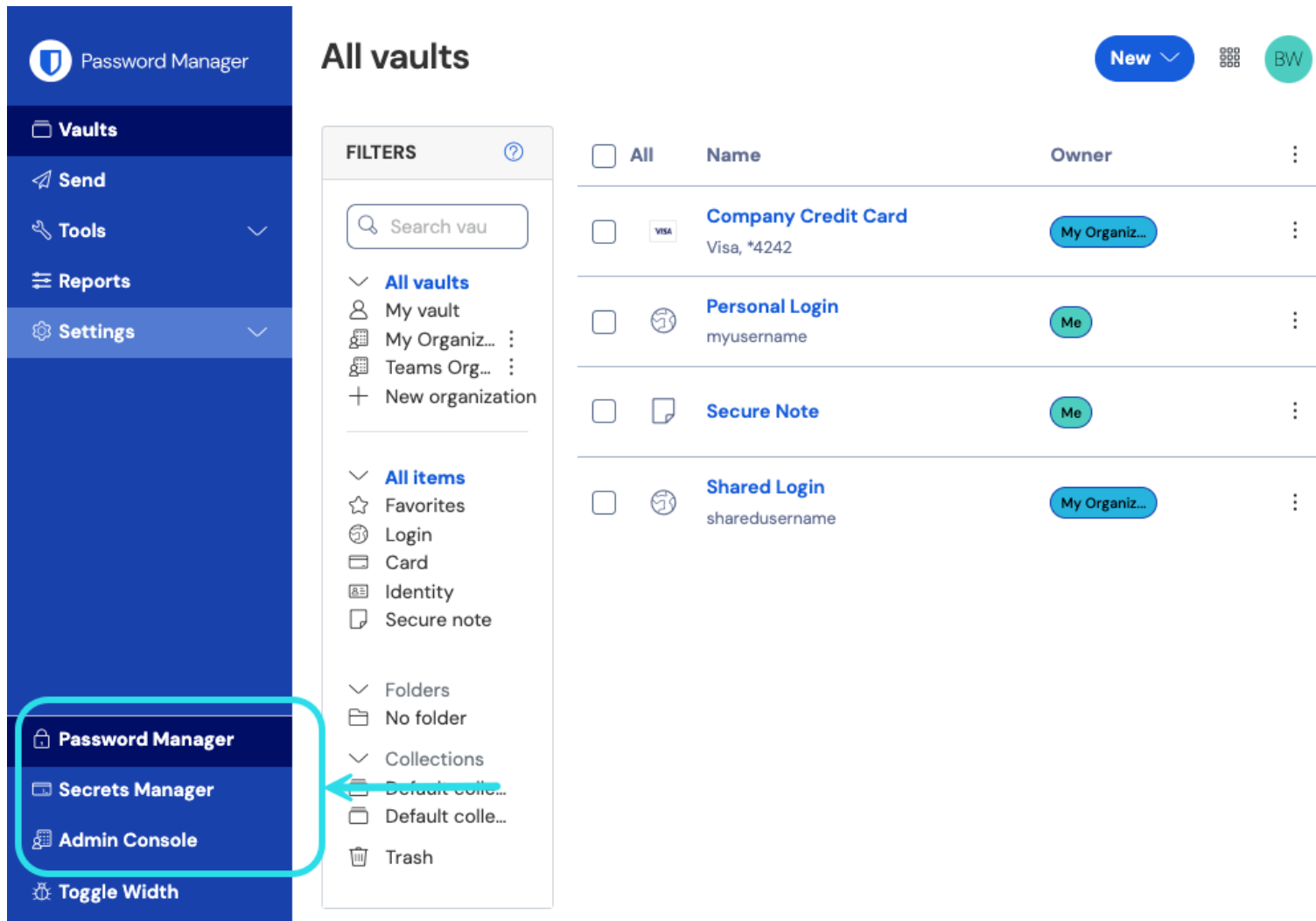
Okta OIDC-implementatie

Dit artikel bevat **Okta-specifieke** hulp voor het configureren van inloggen 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 Okta via SAML 2.0, zie [OIDC-configuratie](#) of [Okta SAML-implementatie](#).

Bij de configuratie wordt tegelijkertijd gewerkt binnen de Bitwarden-webapp en het Okta Admin 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:



- 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)

unique-organization-identifier

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

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 Okta-app maken

Selecteer in het Okta Admin Portal **Applicaties** → **Applicaties** in de navigatie. Selecteer in het scherm Toepassingen de knop **Appintegratie maken**. Selecteer bij Aanmeldmethode **OIDC – OpenID Connect**. Selecteer **Webtoepassing** voor Type toepassing:

Create a new app integration

Sign-on method

[Learn More](#)

☒ **OIDC - OpenID Connect**

Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☐ **SAML 2.0**

XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐ **SWA - Secure Web Authentication**

Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐ **API Services**

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

☒ **Web Application**

Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

☐ **Single-Page Application**

Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

☐ **Native Application**

Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#) [Next](#)

Create App Integration

Configureer de volgende velden in het scherm **New Web App Integration**:

Veld	Beschrijving
Naam app-integratie	Geef de app een Bitwarden-specifieke naam.

Veld	Beschrijving
Type subsidie	Schakel de volgende subsidietypen in: – Klant die namens zichzelf optreedt → Klantgegevens – Klant die optreedt namens een gebruiker → Autorisatiecode
URI's voor aanmelden omleiden	Stel dit veld in op uw Terugbelpad, dat u kunt ophalen uit het Bitwarden SSO-configuratiescherm. 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.
Afmelden omleiden URI's	Stel dit veld in op uw afgemelde terugbelpad, dat u kunt ophalen uit het scherm Bitwarden SSO-configuratie.
Opdrachten	Gebruik dit veld om aan te geven of alle of alleen bepaalde groepen Bitwarden Login met SSO kunnen gebruiken.

Selecteer na het configureren de knop **Volgende**.

Klantgegevens ophalen

Kopieer in het scherm Toepassing de **Client-ID** en **Client-secret** voor de nieuw gemaakte Okta-app:



Bitwarden Login with SSO

Active ▾


[View Logs](#)

General Sign On Assignments Okta API Scopes

Client Credentials

[Edit](#)

Client ID


Public identifier for the client that is required for all OAuth flows.

Client secret


Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

Ready to code

You can download a preconfigured sample app.

[Download sample app](#)

To get started using your custom app integration, see the "Sign Users In" section in the Okta [Developer's guide](#)

App Client Credentials

Je zult beide waarden [in een latere stap](#) moeten gebruiken.

Informatie over autorisatieserver ophalen

Selecteer **Beveiliging** → **API** in de navigatie. Selecteer in de lijst **Authorization Servers** de server die je wilt gebruiken voor deze implementatie. Kopieer op het tabblad **Instellingen** voor de server de waarden **Issuer** en **Metadata URI**:

← Back to Authorization Servers

default

Help

Active

- Settings
- Scopes
- Claims
- Access Policies
- Token Preview

Settings

Edit

Name	default	
Audience	api://default	
Description	Default Authorization Server for your Applications	
Issuer	https://	.okta.com/oauth2/default
Metadata URI	https://	.okta.com/oauth2/default/.well-known/oauth-authorization-server

Authorization Servers

An authorization server defines your security boundary, and is used to mint access and identity tokens for use with OIDC clients and OAuth 2.0 service accounts when accessing your resources via API. Within each authorization server you can define your own OAuth scopes, claims, and access policies. Read more at [help page](#)

Okta Authorization Server Settings

Je zult beide waarden moeten gebruiken tijdens de volgende stap.

Terug naar de webapp

Op dit punt hebt u alles geconfigureerd wat u nodig hebt binnen de context van het Okta Admin Portal. Ga terug naar de Bitwarden web app om de volgende velden te configureren:

Veld	Beschrijving
Autoriteit	Voer de opgehaalde Issuer URI voor uw autorisatieserver in.
Klant-ID	Voer de opgehaalde Client ID voor uw Okta-app in.

Veld	Beschrijving
Geheim van de klant	Voer het opgehaalde Client secret voor uw Okta-app in.
Metadata-adres	Voer de opgehaalde Metadata URI voor uw autorisatieserver in.
OIDC omleidingsgedrag	Selecteer GET omleiden . Okta ondersteunt momenteel geen Form POST.
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.
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 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 succesvol is geconfigureerd, wordt u doorgestuurd naar het inlogscherf voor Okta:

okta



Sign In

Username

Password

☐ Remember me

Sign In

Need help signing in?

Log in with Okta

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

Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an [Okta Bookmark App](#) that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
 1. Give the application a name such as **Bitwarden Login**.
 2. In the **URL** field, provide the URL to your Bitwarden client such as <https://vault.bitwarden.com/#/login> or [your-self-hostedURL.com](#).
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained [here](#).

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.