BEHEERCONSOLE > INLOGGEN MET SSO >

Cloudflare Zero Trust SSO-implementatie

Cloudflare Zero Trust SSO-implementatie

Dit artikel bevat **Cloudflare Zero Trust-specifieke** hulp voor het configureren van inloggen met SSO. Cloudflare Zero Trust is een cloudgebaseerd identiteits- en toegangsbeheerplatform dat kan integreren met meerdere identiteitsproviders (IdP's). Je kunt ook gateways en tunneling configureren voor beveiligde toegang tot het platform.

> **Note**
>
> Cloudflare Zero Trust can be configured with any IdP that operates using SAML 2.0 or OIDC SSO configurations. If you are not familiar with these configurations, refer to these articles:
>
> - SAML 2.0 Configuration
> - OIDC Configuration

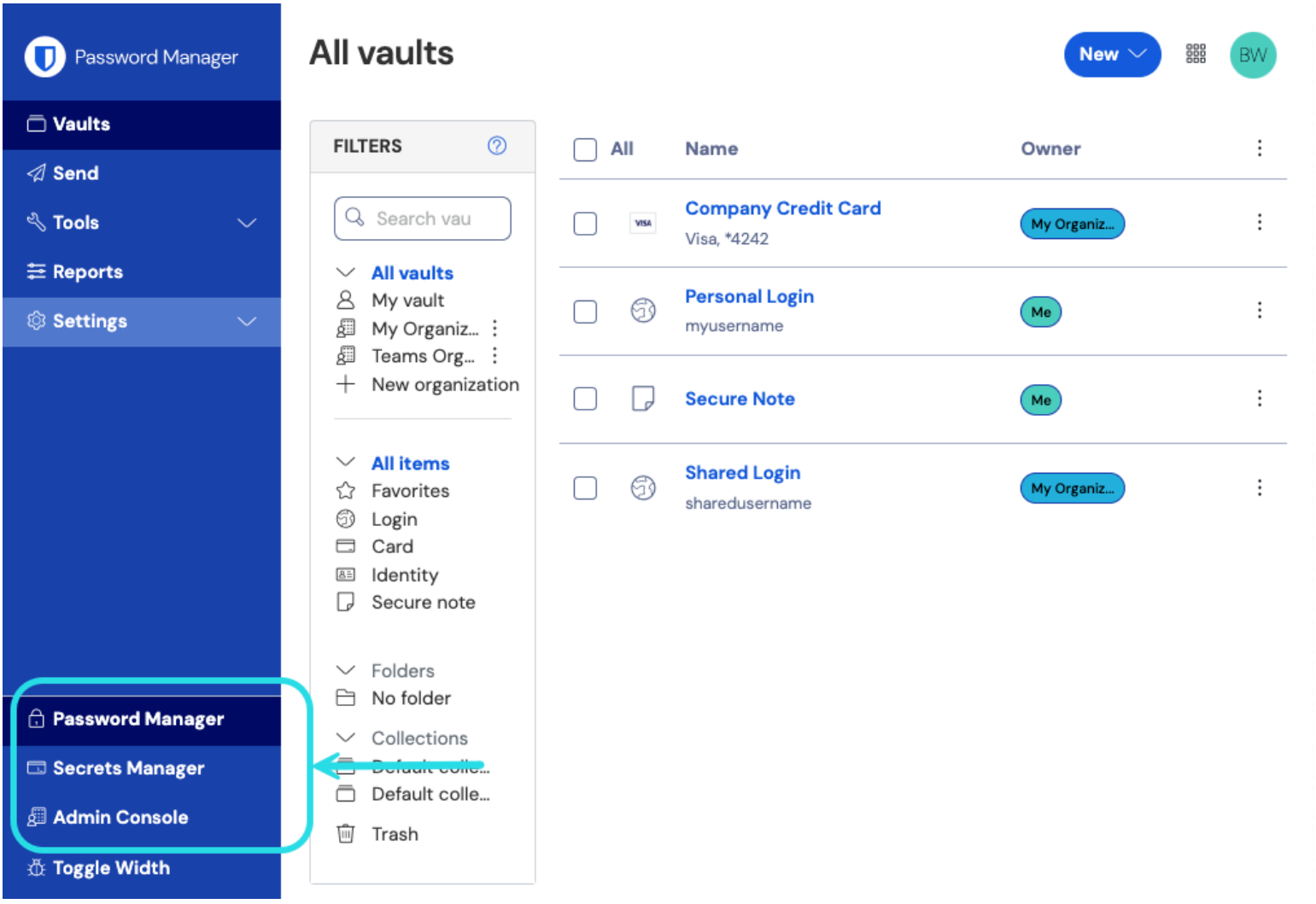
Waarom Cloudflare Zero Trust met SSO gebruiken?

Cloudflare Zero Trust is een cloudgebaseerd proxy identiteits- en toegangsbeheerplatform dat kan integreren met meerdere identiteitsproviders (IdP's). Het voordeel van het gebruik van Cloudflare Zero Trust naast uw standaard IdP is de mogelijkheid om meerdere IdP's te configureren voor aanmelding. Cloudflare Zero Trust kan SSO-toegang bieden tot Bitwarden vanuit meerdere afzonderlijke organisaties, of sets van gebruikers binnen een organisatie.

Open SSO in de webapp

> **Note**
>
> Cloudflare will only support SAML via the Access Application Gateway. This means that the **SAML 2.0** must be selected in the Bitwarden configuration. OIDC authentication can still be configured from the IdP and Cloudflare.

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



Product switcher

Open het scherm **Instellingen → Eenmalige aanmelding** van uw organisatie:

SAML 2.0 configuratie

Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identifier** aan voor je organisatie en selecteer **SAML** in het keuzemenu **Type** . Houd dit scherm open voor gemakkelijke referentie.

U kunt de optie **Een unieke SP entiteit ID instellen** in dit stadium uitschakelen als u dat wilt. Als u dit doet, wordt uw organisatie-ID verwijderd uit uw SP entiteit-ID waarde, maar in bijna alle gevallen is het aan te raden om deze optie aan te laten staan.

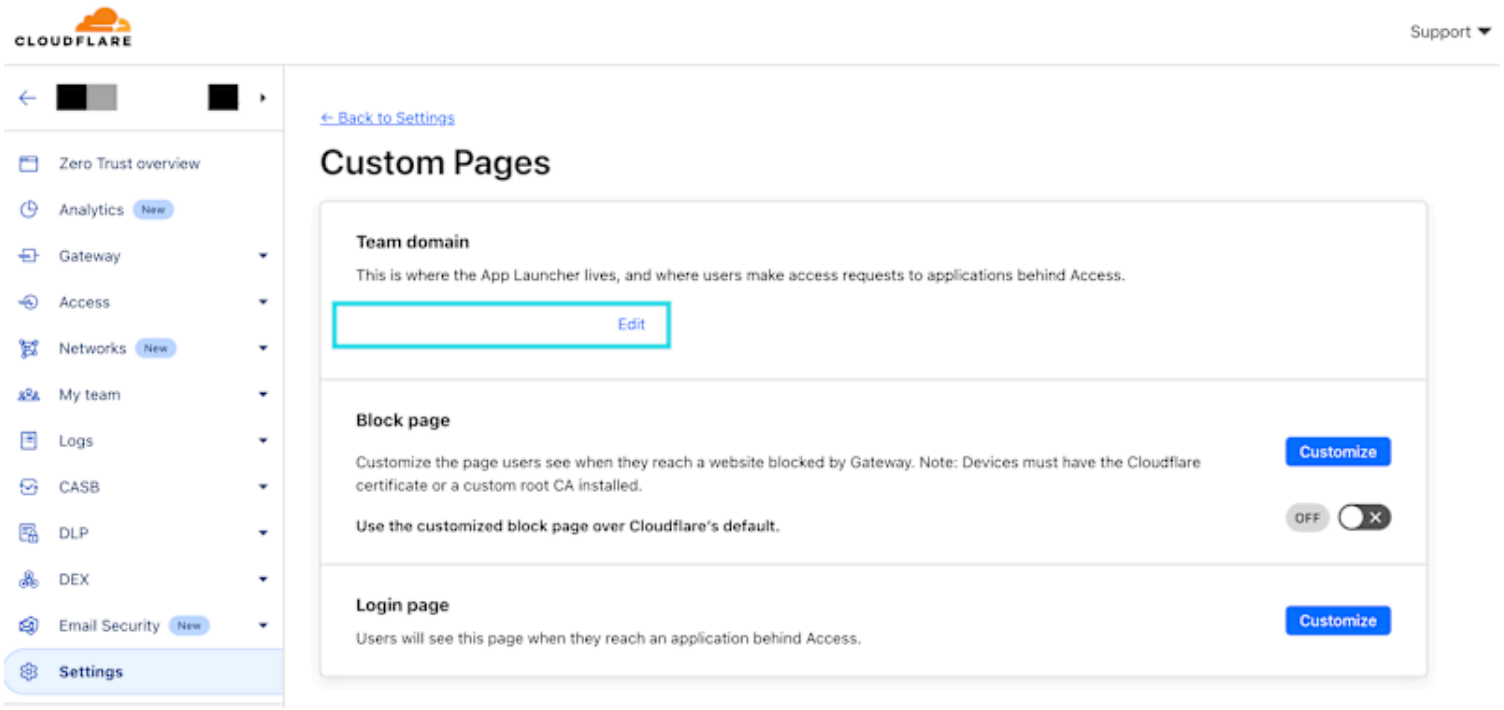
> **Tip**
>
> Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met SSO met vertrouwde apparaten of Key Connector.

Maak een Cloudflare Zero Trust aanmeldingsmethode

Om een Cloufdlare Zero Trust aanmeldingsmethode aan te maken:

1. Navigeer naar Cloudflare Zero Trust en log in of maak een account aan.

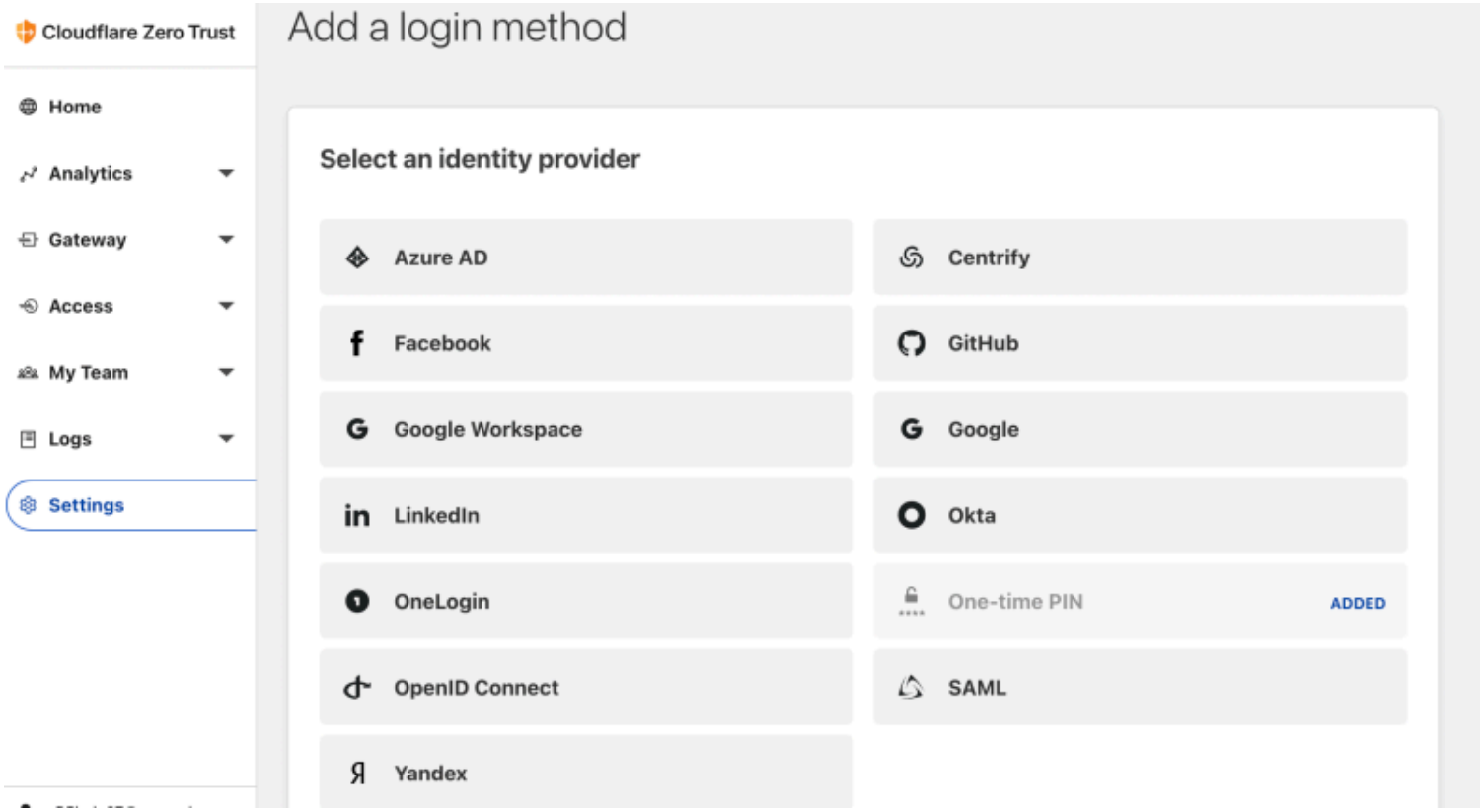
2. Configureer een domein, dat zal fungeren als de URL die door je gebruikers wordt gebruikt om toegang te krijgen tot je applicaties of **App Launcher**, bijvoorbeeld `https://my-business.cloudflareaccess.com/.` Selecteer in het Cloudflare Zero Trust menu **Instellingen → Algemeen → Teamdomein**:



Team domain setting

3. Begin met het configureren van de eerste aanmeldingsmethode door te navigeren naar **Instellingen → Authenticatie → Nieuwe toevoegen.**

4. Selecteer de aanmeldingsmethode om verbinding te maken met Cloudflare Zero Trust. Als de IdP die je gebruikt niet voorkomt op de IdP-lijst, gebruik dan de SAML of OIDC generieke opties. In dit artikel wordt Okta als voorbeeld gebruikt:



Cloudflare Zero Trust IdP list

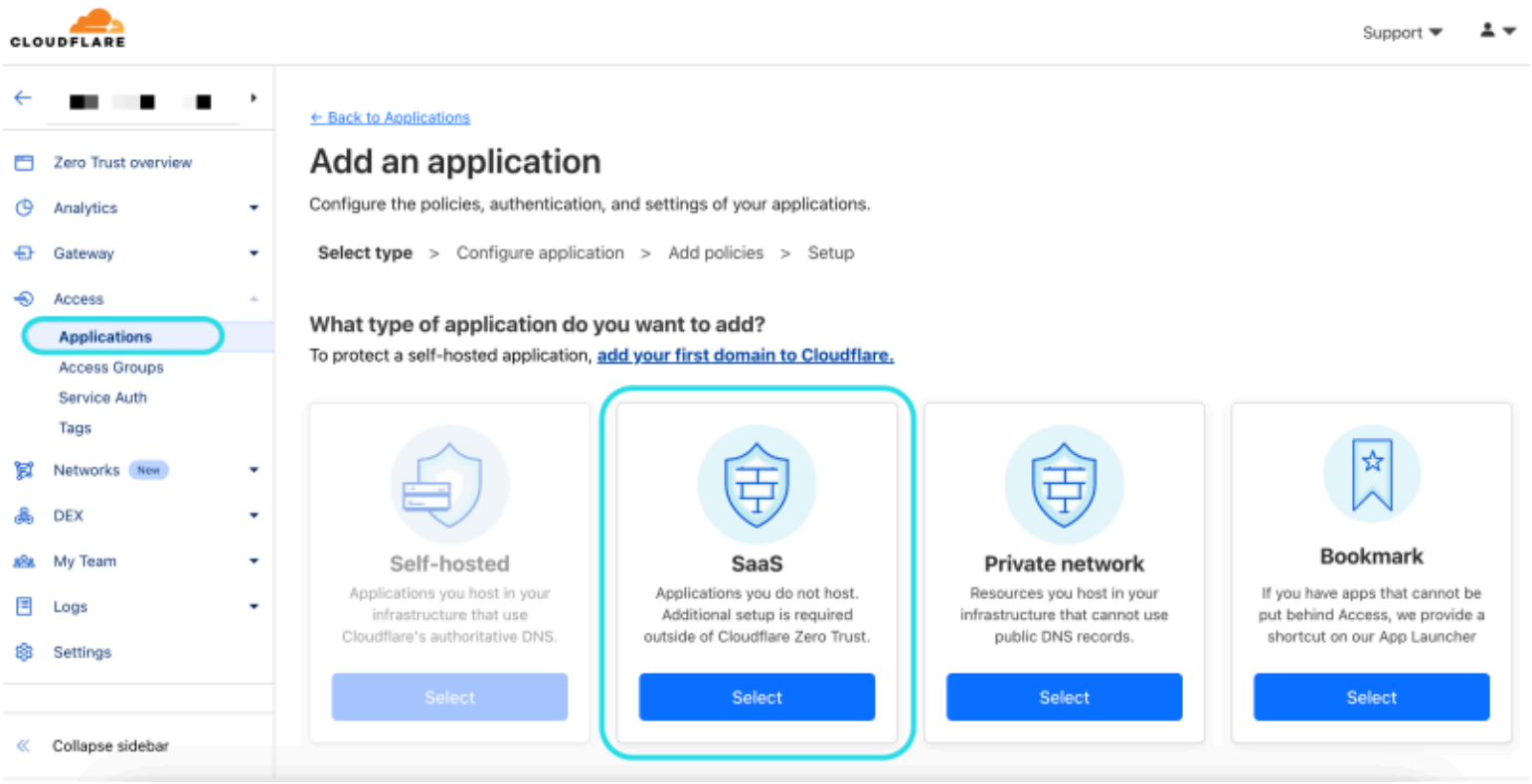
5. Na het selecteren van de door u gekozen IdP aanmeldingsmethode volgt u de in-product handleiding van Cloudflare voor het integreren van uw IdP.

> **Note**
>
> If the IdP you are using has a **support groups** feature, this option must be **disabled**. Bitwarden does not support group based claims, enabling this option will result in an XML element error on the Bitwarden end.

Een Cloudflare Zero Trust-applicatie aanmaken

Nadat een IdP is geconfigureerd, moet je een Cloudflare Zero Trust-toepassing voor Bitwarden maken. **In dit voorbeeld maken we een SAML-applicatie**:

1. Navigeer naar **Toegang → Toepassingen → Een toepassing toevoegen**.



CFZT add an application

2. Selecteer het type **SaaS**.

3. Open in de Bitwarden-webkluis uw organisatie en navigeer naar het scherm **Instellingen → Single Sign-On**. Gebruik informatie van de webkluis om informatie in te vullen op het scherm **Configureer app** :

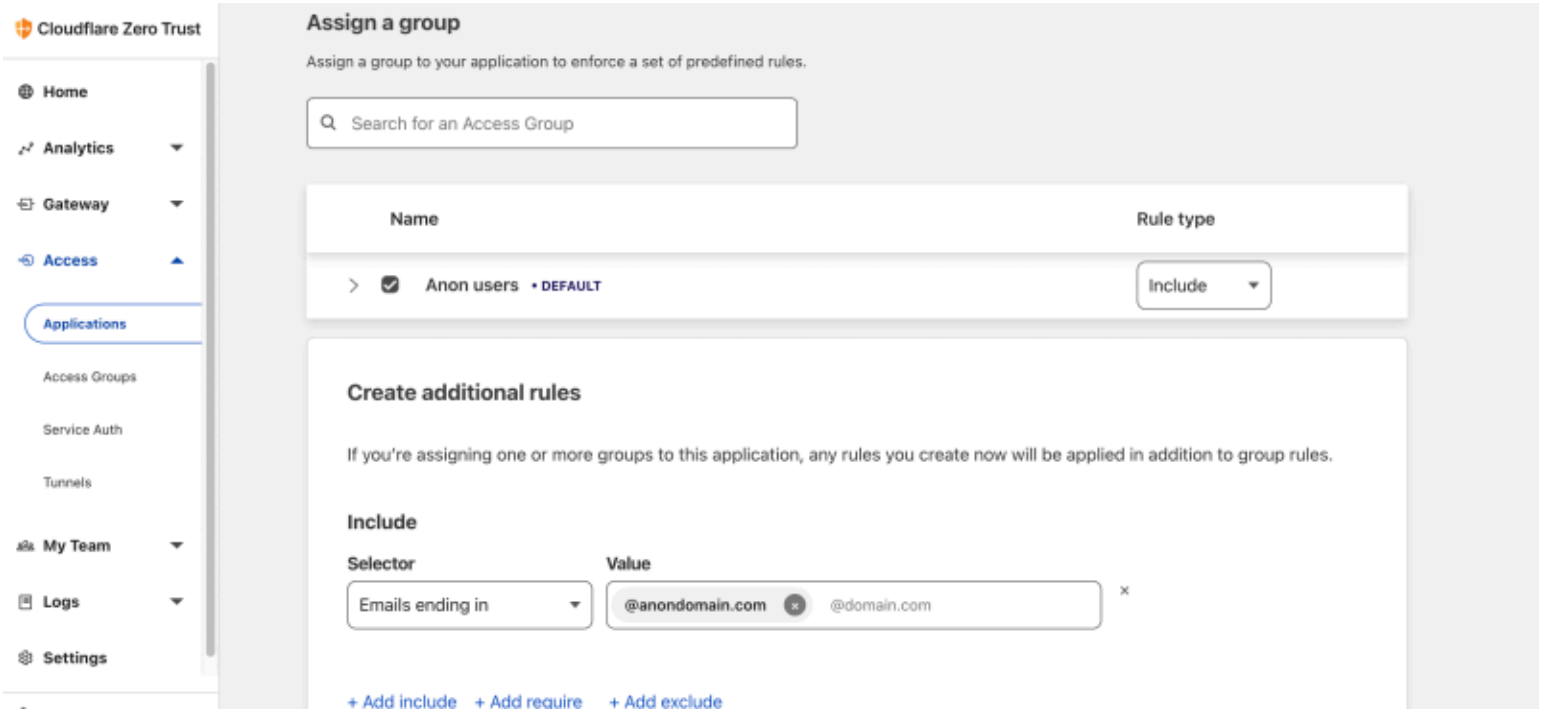
Sleutel	Beschrijving
Toepassing	`Bitwarden` komt binnen.
Entiteit ID	Kopieer de **SP entiteit ID** van de Bitwarden Single Sign-On pagina naar dit veld.
URL voor bevestiging Consumentenservice	Kopieer de URL van de **Assertion consumer service (ACS)** van de Bitwarden Single Sign-On pagina naar dit veld.
Naam ID Formaat	Selecteer **E-mail** in het vervolgkeuzemenu.

> **Note**
> For the generic OIDC configuration, the Auth URL, Token URL, and Certificate URL can be located with the well-known URL.

4. Scroll omlaag naar het menu **Identity providers**. Selecteer de IdP(s) die u in de vorige sectie hebt geconfigureerd, scroll terug naar boven en selecteer **Volgende.**

5. Maak vervolgens een toegangsbeleid voor gebruikerstoegang tot de applicatie. Vul voor elk beleid de velden **Beleidsnaam**, **Actie** en **Sessieduur** in.

6. Je kunt ervoor kiezen om een groepsbeleid**(Toegang → Groepen**) of expliciete regels voor gebruikersbeleid (zoals e-mails, "e-mails eindigend op", "land" of "iedereen") toe te wijzen. In het volgende voorbeeld is de groep "Anon Users" opgenomen in het beleid. Er is ook een extra regel toegevoegd om e-mails op te nemen die eindigen op het gekozen domein:



CFZT app policy

> **Note**
> You can also apply user access through the **App Launcher** for access to the Bitwarden login with SSO shortcut. This can be managed by navigating to **Authentication → App Launcher → Manage**. The application policies in the above example can be duplicated or generated here.

7. Nadat het toegangsbeleid is geconfigureerd, scrolt u naar boven en selecteert u **Volgende**.

8. Kopieer in het **instellingenscherm** de volgende waarden en voer ze in de respectievelijke velden op de Bitwarden **Single Sign-On** pagina in:

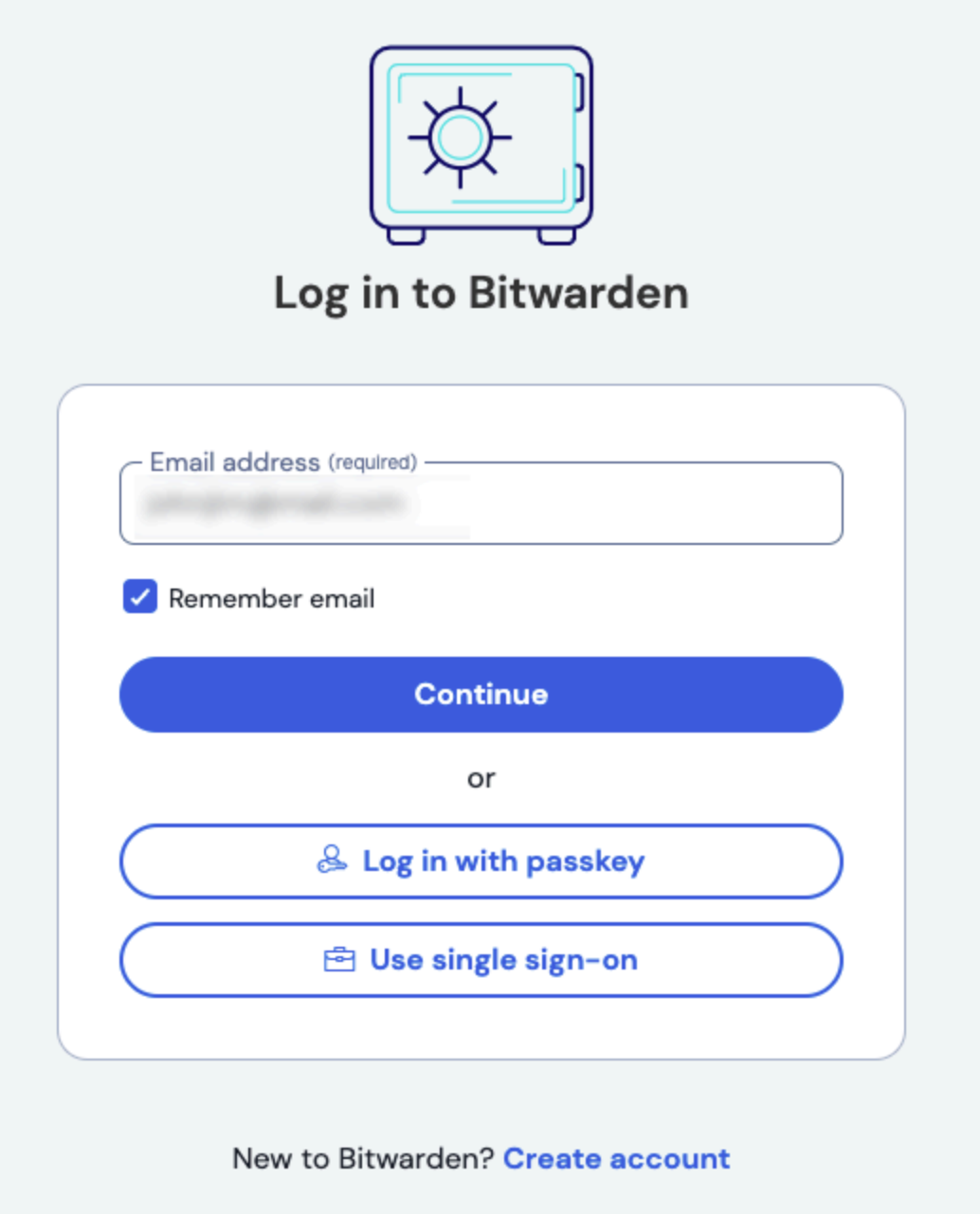
Sleutel	Beschrijving
SSO eindpunt	Het SSO-eindpunt bepaalt waar je SaaS-applicatie aanmeldingsverzoeken naartoe stuurt. Deze waarde wordt ingevoerd in het **Single Sign On Service URL-veld** in Bitwarden.
Toegangsentiteit ID of uitgever	De Access Entity ID of Issuer is de unieke identificatie van je SaaS-applicatie. Deze waarde wordt ingevuld in het **Entity ID-veld** op Bitwarden.
Openbare sleutel	De publieke sleutel is het openbare toegangscertificaat dat zal worden gebruikt om uw identiteit te verifiëren. Deze waarde wordt ingevoerd in het veld **X509 Public Certificate** op Bitwarden.

9. Nadat de waarden zijn ingevoerd in Bitwarden, selecteert u **Opslaan** op het Bitwarden Single Sign-On-scherm en selecteert u **Gereed** op de Cloudflare-pagina om de toepassing op te slaan.

10. Om een bladwijzer te maken naar het Bitwarden login met SSO scherm, selecteert u **Een toepassing toevoegen → Bladwijzer**. Controleer of de bladwijzer zichtbaar is in de **App launcher**.

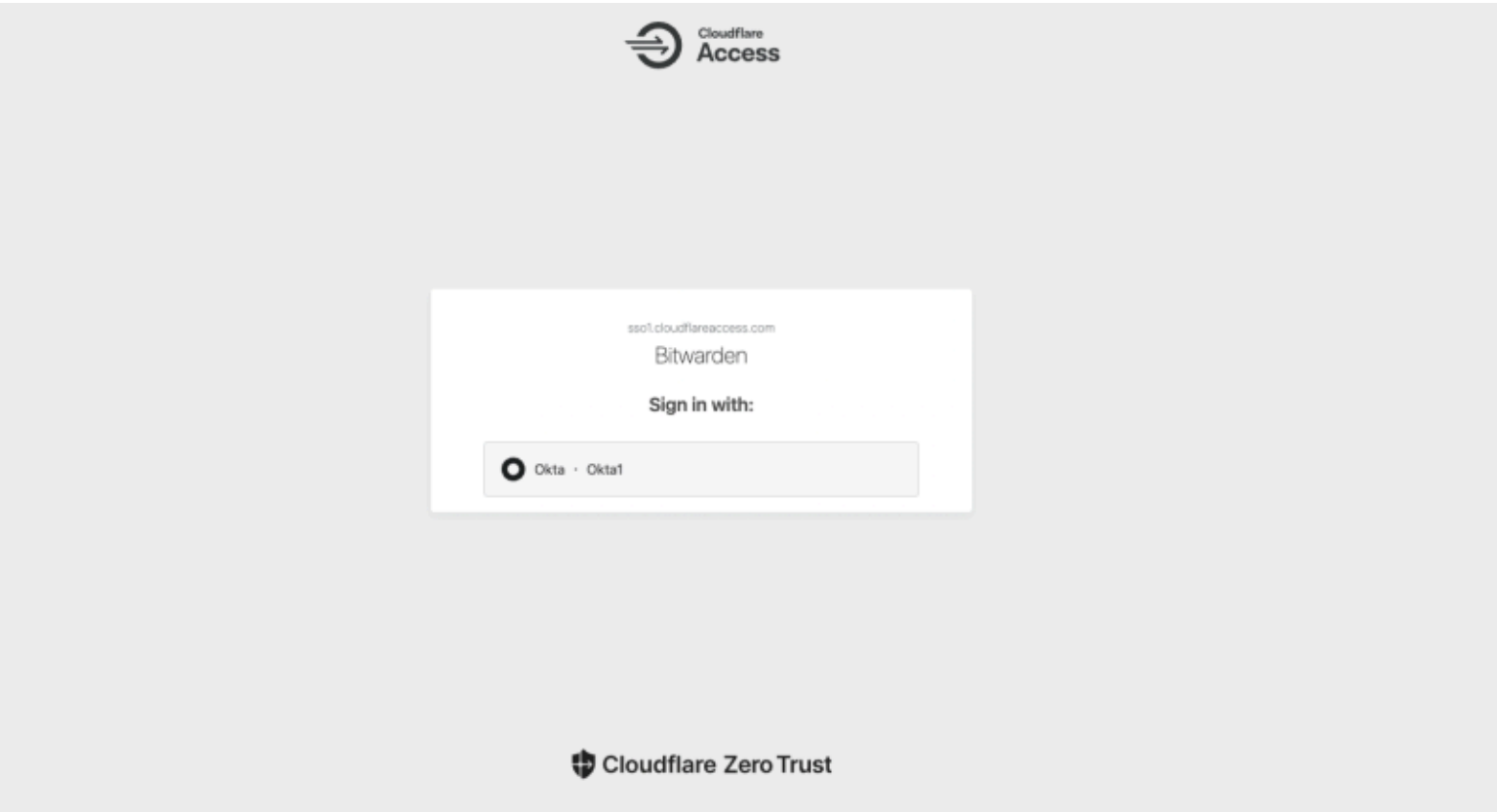
De configuratie testen

Zodra uw configuratie voltooid is, kunt u deze testen door te navigeren naar https://vault.bitwarden.com, uw e-mailadres in te voeren, **Doorgaan** te selecteren en de knop **Enterprise single sign-on** te selecteren.



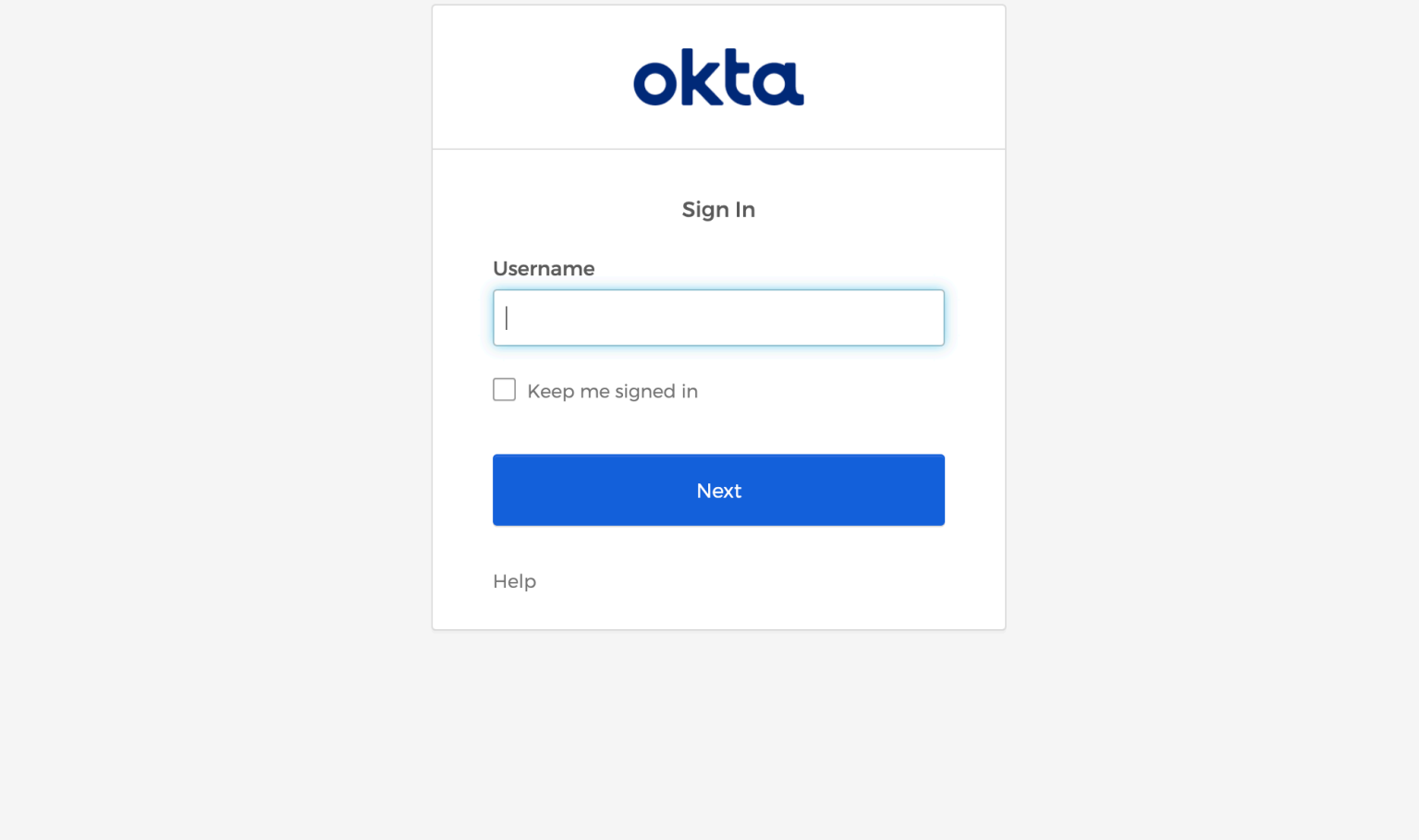
Enterprise single sign on en hoofdwachtwoord

Voer de geconfigureerde organisatie-ID in en selecteer **Aanmelden**. Als uw implementatie succesvol is geconfigureerd, wordt u omgeleid naar een Cloudflare Access-scherm, waar u de IdP kunt selecteren waarmee u wilt inloggen:



Cloudflare IdP selection

Nadat u uw IdP hebt geselecteerd, wordt u doorgestuurd naar de inlogpagina van uw IdP. Voer de gegevens in die zijn gebruikt om in te loggen via uw IdP:



CFZT IdP login

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