ADFS OIDC-implementatie

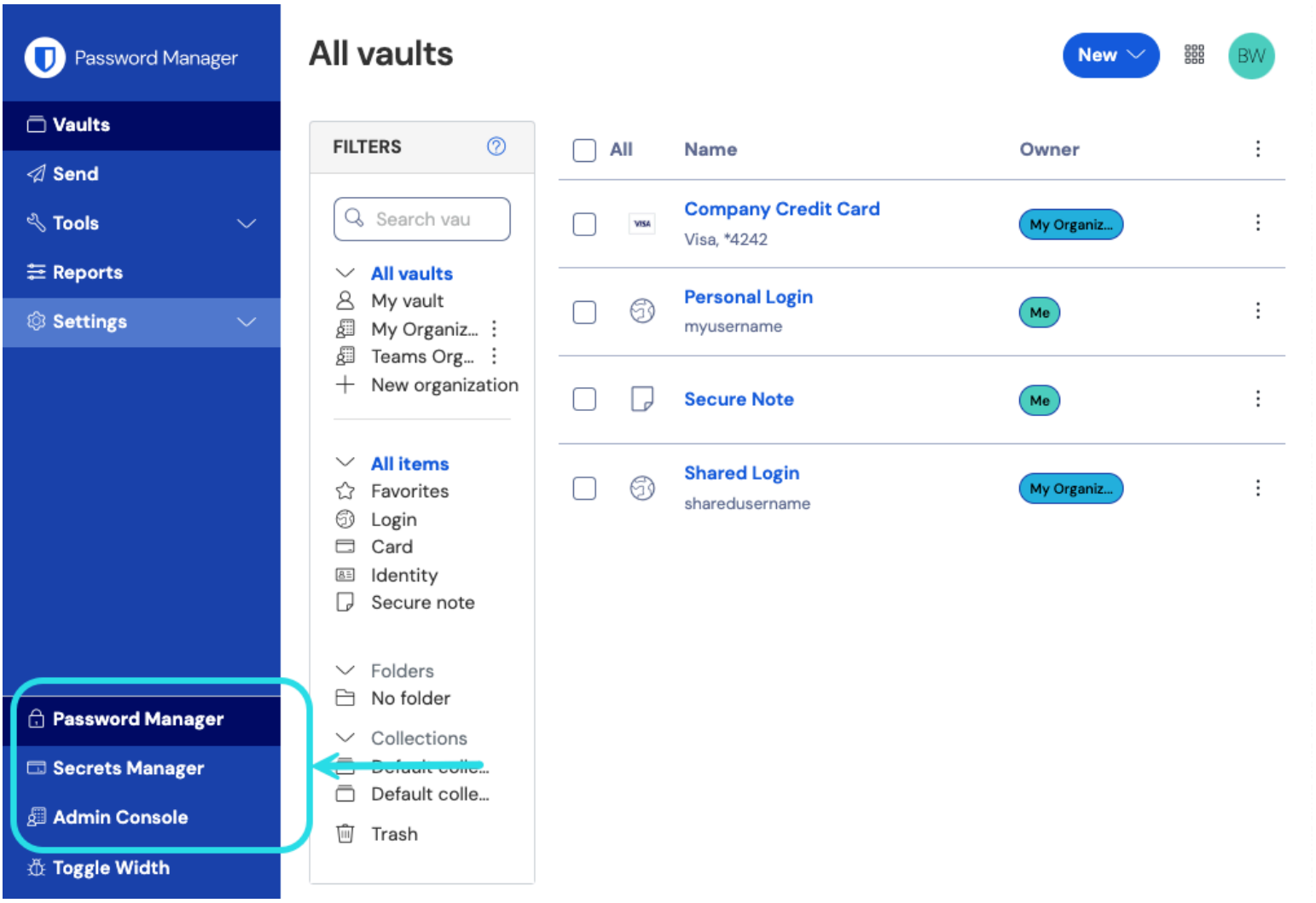
ADFS OIDC-implementatie

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 (⊞):



Product switcher

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

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.

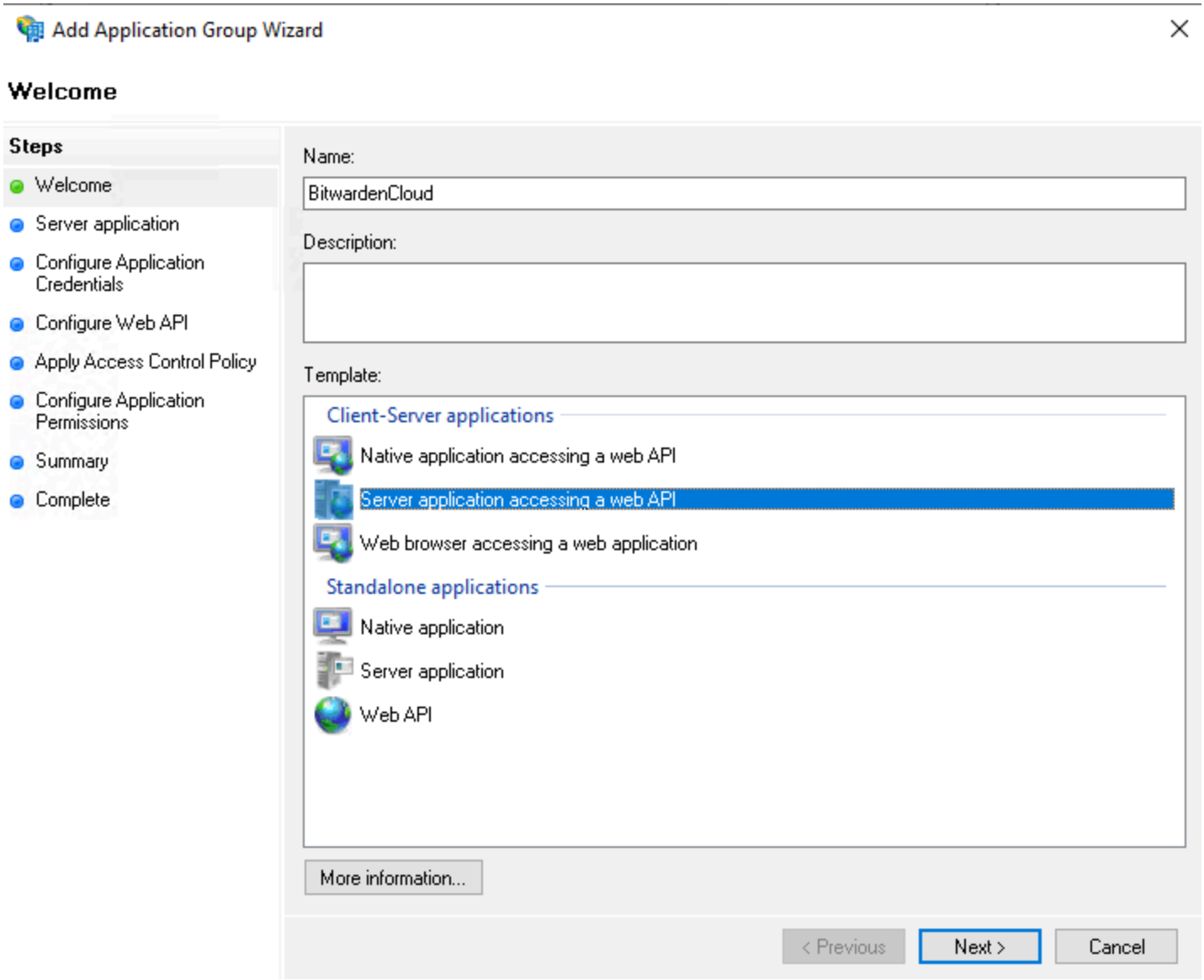
> **Tip**
>
> Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met SSO met vertrouwde apparaten of Key Connector.

Een applicatiegroep maken

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

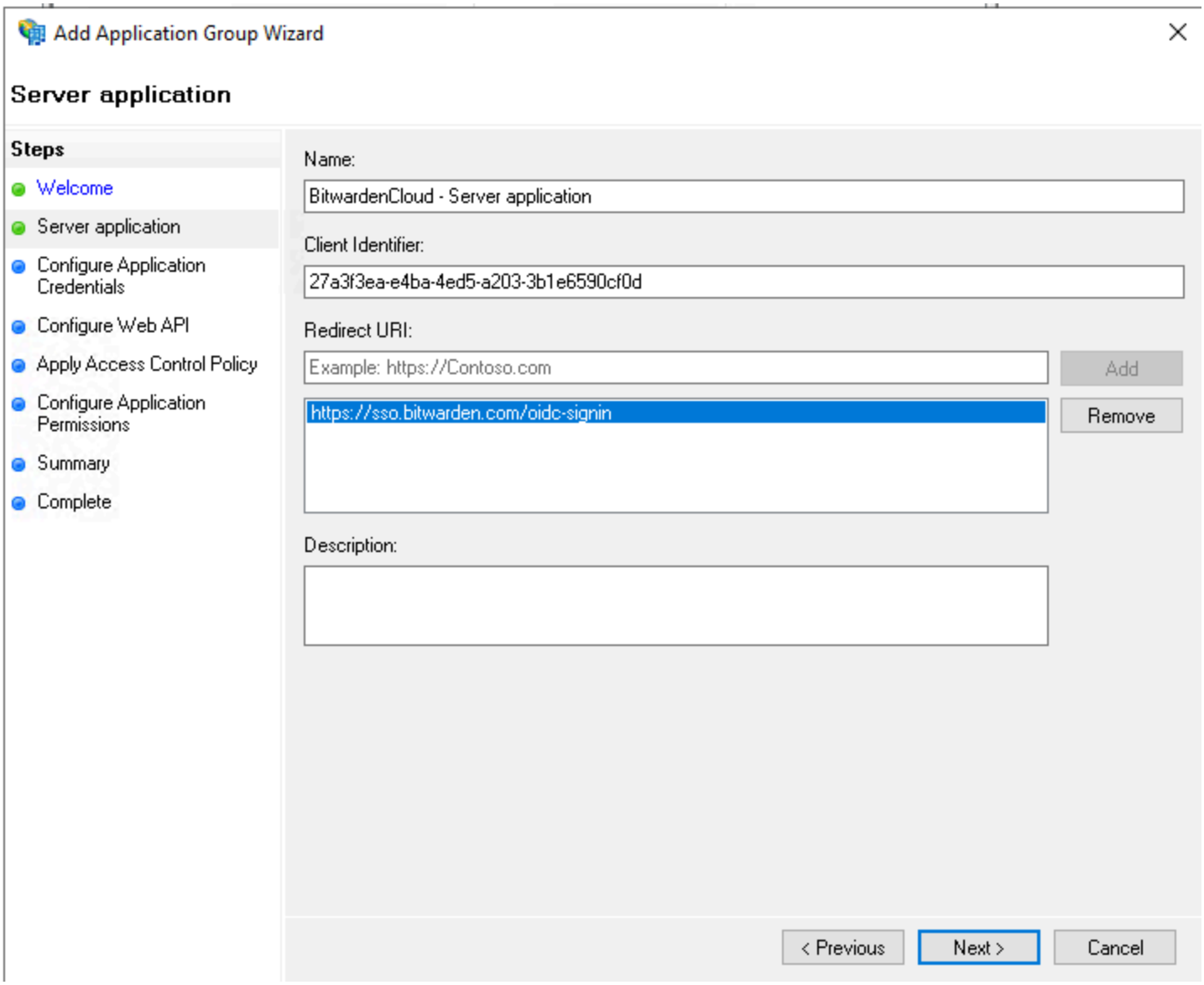
1. Selecteer in de consolestructuur **Toepassingsgroepen** en kies **Toepassingsgroep toevoegen** in de lijst Acties.

2. Kies in het welkomstscherm van de wizard de sjabloon **Serverapplicatie die toegang heeft tot een web-API** .



AD FS Add Application Group

3. In het scherm Servertoepassing:

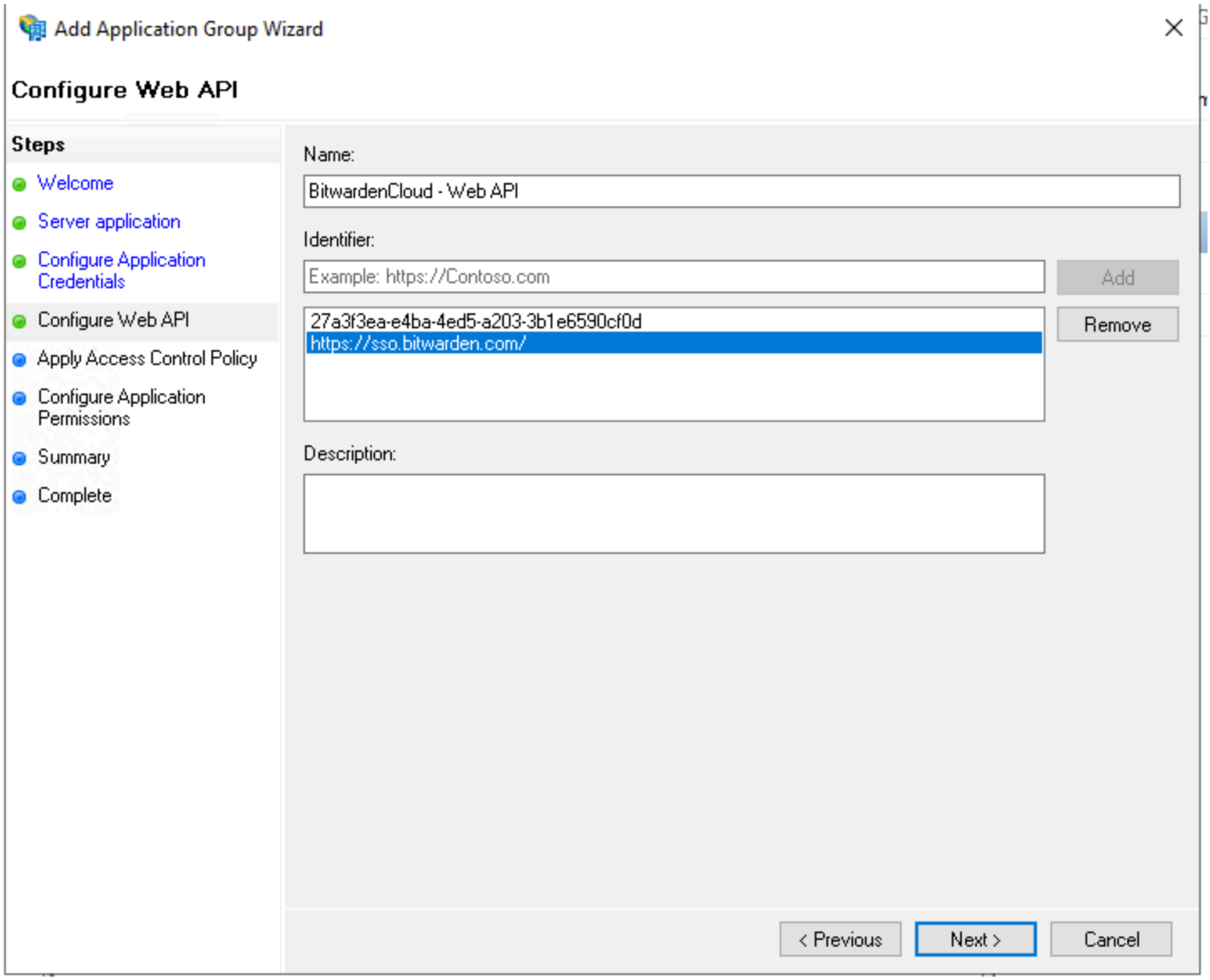


AD FS Server Application screen

- 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.bitwarden.eu/oidc-signin`. Voor zelf gehoste instanties wordt dit bepaald door je geconfigureerde Server URL, bijvoorbeeld `https://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:

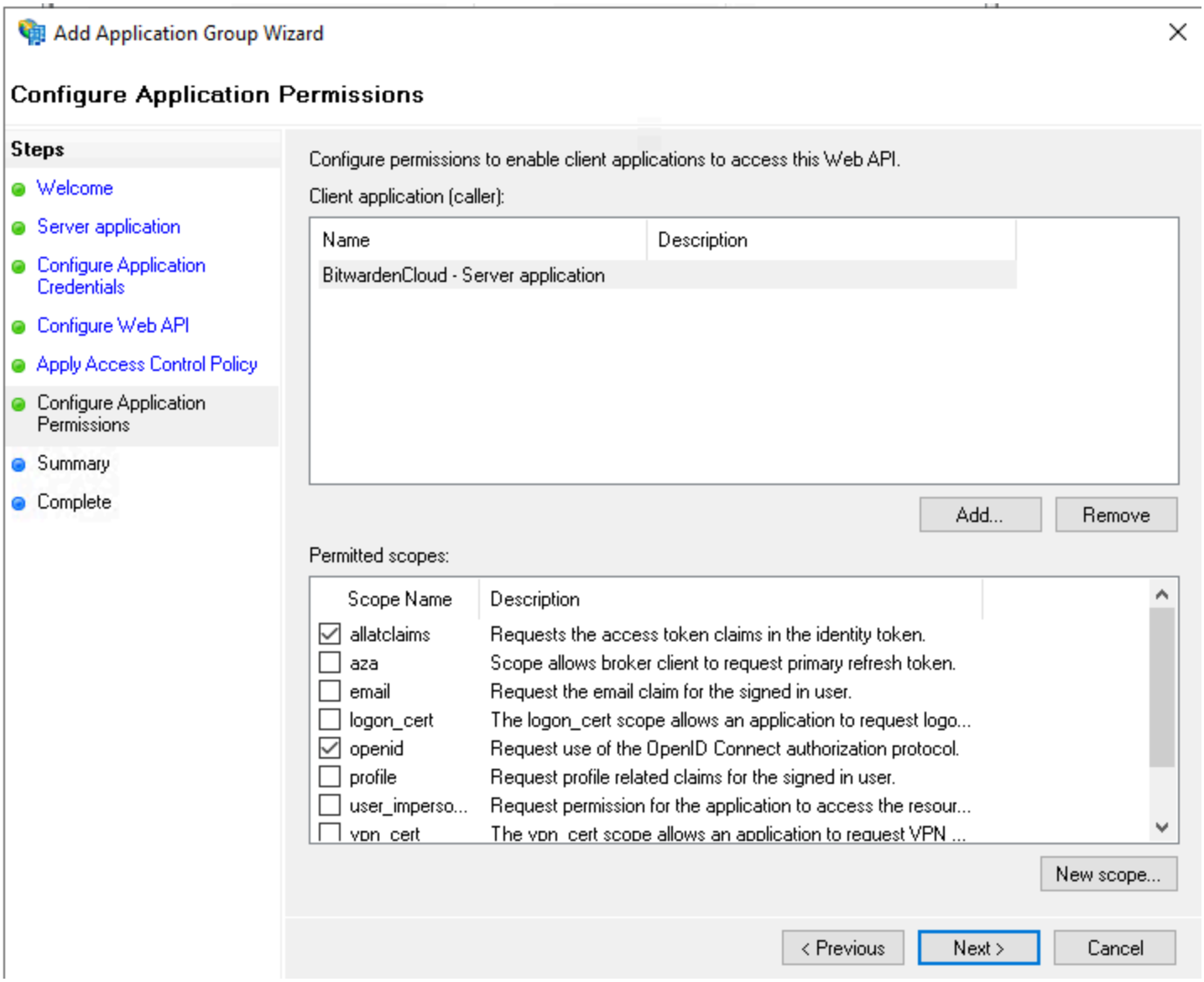


AD FS Configure Web API screen

- 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.



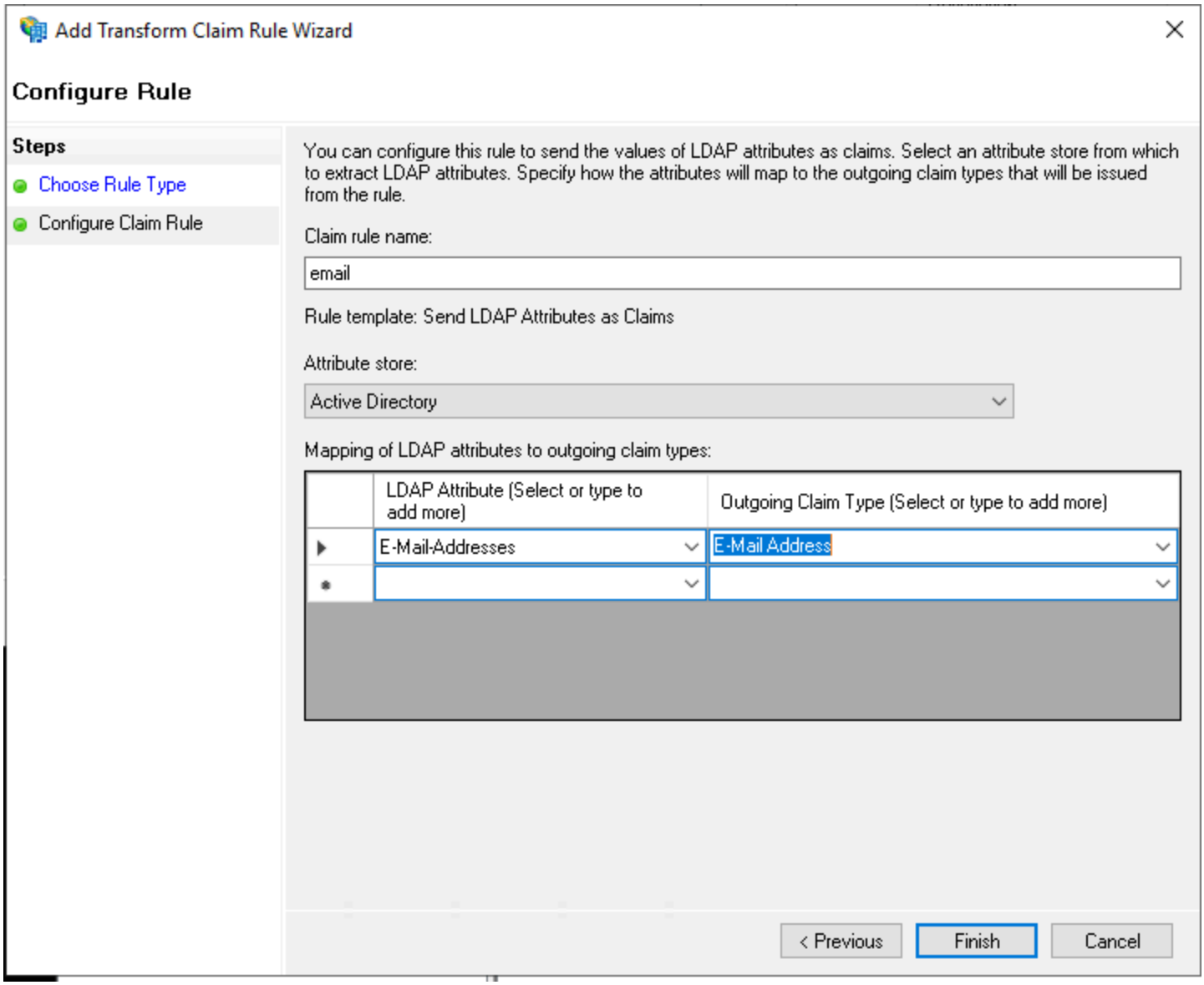
AD FS Configure Application Permissions screen

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:



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.

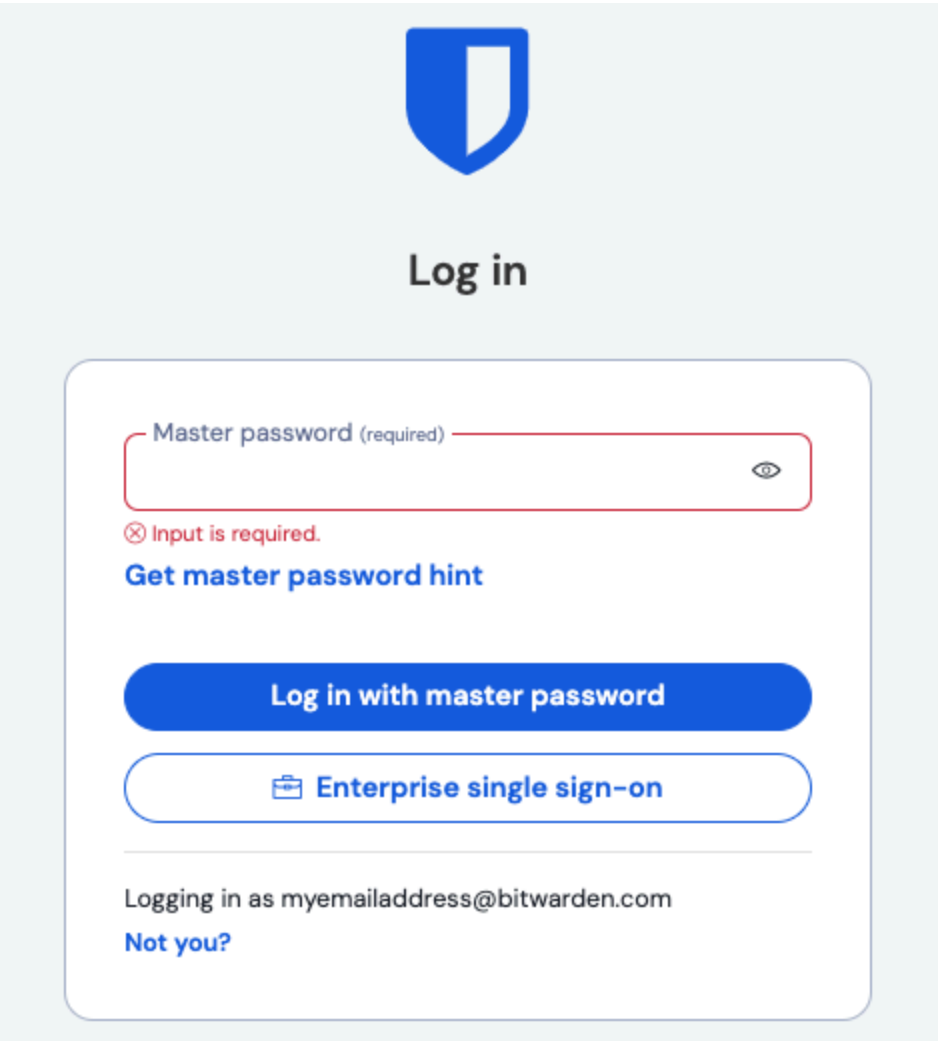
Veld	Beschrijving
Aangevraagde Authenticatie Context Klasse Referentiewaarden	Definieer Authentication Context Class Reference identifiers (`acr_values`) (spatie-limited). Lijst `acr_waarden` in voorkeursvolgorde.
Verwachte "acr" claimwaarde in antwoord	Definieer de `acr` Claim Value die Bitwarden verwacht 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:



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!

> **Note**
> Bitwarden ondersteunt geen ongevraagde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSO-aanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden.