bitwarden | Artikel Helpcentrum

BEHEERCONSOLE > INLOGGEN MET SSO >

ADFS SAML-implementatie

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

ADFS SAML-implementatie

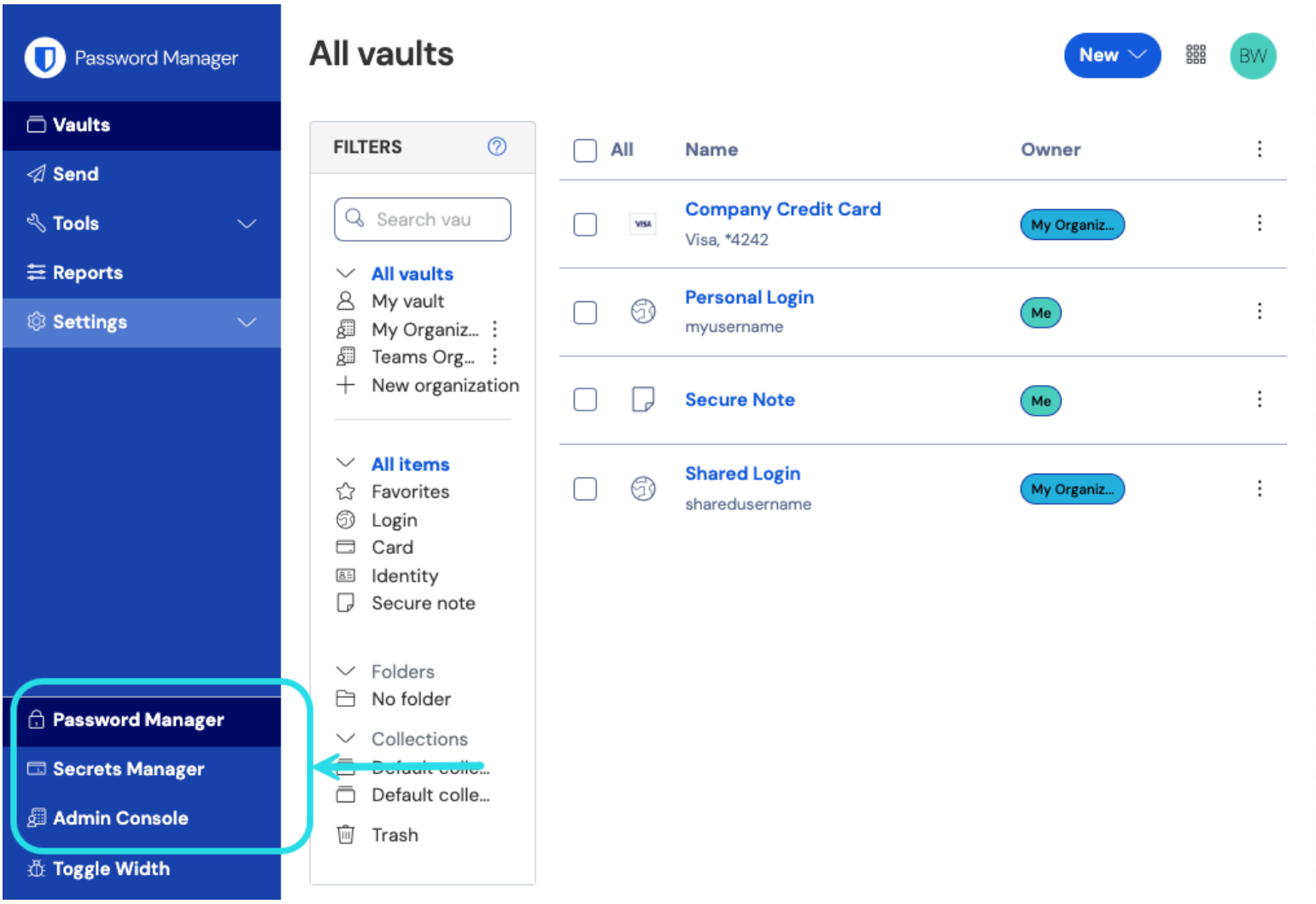
Dit artikel bevat **Active Directory Federation Services (AD FS)-specifieke** hulp voor het configureren van aanmelding met SSO via SAML 2.0. Raadpleeg SAML 2.0 Configuratie voor hulp bij het configureren van inloggen met SSO voor een andere IdP.

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.

> **Tip**
>
> **Bent u al een SSO-expert?** Sla de instructies in dit artikel over en download schermafbeeldingen van voorbeeldconfiguraties om te vergelijken met je eigen configuratie.
>
> type: asset-hyperlink id: 5892IOGrU7B9IvBmN0P0xl

Open SSO in de webapp

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.

Een vertrouwensrelatie creëren

Selecteer in de AD FS Server Manager **Tools → AD FS Management → Action → Add Relying Party Trust**. Maak de volgende selecties in de wizard:

1. Selecteer **Claims Aware** op het welkomstscherm.

2. Selecteer in het scherm Gegevensbron selecteren de optie **Gegevens over de betalende partij handmatig invoeren**.

3. Voer in het scherm Displaynaam opgeven een Bitwarden-specifieke displaynaam in.

4. Selecteer in het scherm Configure URL de optie **Enable support for SAML 2.0 WebSSO protocol**.

    - Voer de URL van de Assertion Consumer Service (ACS) in bij de optie **Relying party SAML 2.0 SSO service URL**. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen → Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van je instelling.

5. Selecteer in het scherm **Kies toegangscontrolebeleid** het beleid dat voldoet aan uw beveiligingsstandaarden.

6. Voeg in het scherm **Configure Identifiers** de SP Entity ID toe als vertrouwensidentificatie voor een betrouwbare partij. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen → Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van je instelling.

7. Selecteer in het scherm **Toegangsbeheerbeleid kiezen** het gewenste beleid (standaard **Iedereen toestaan**).

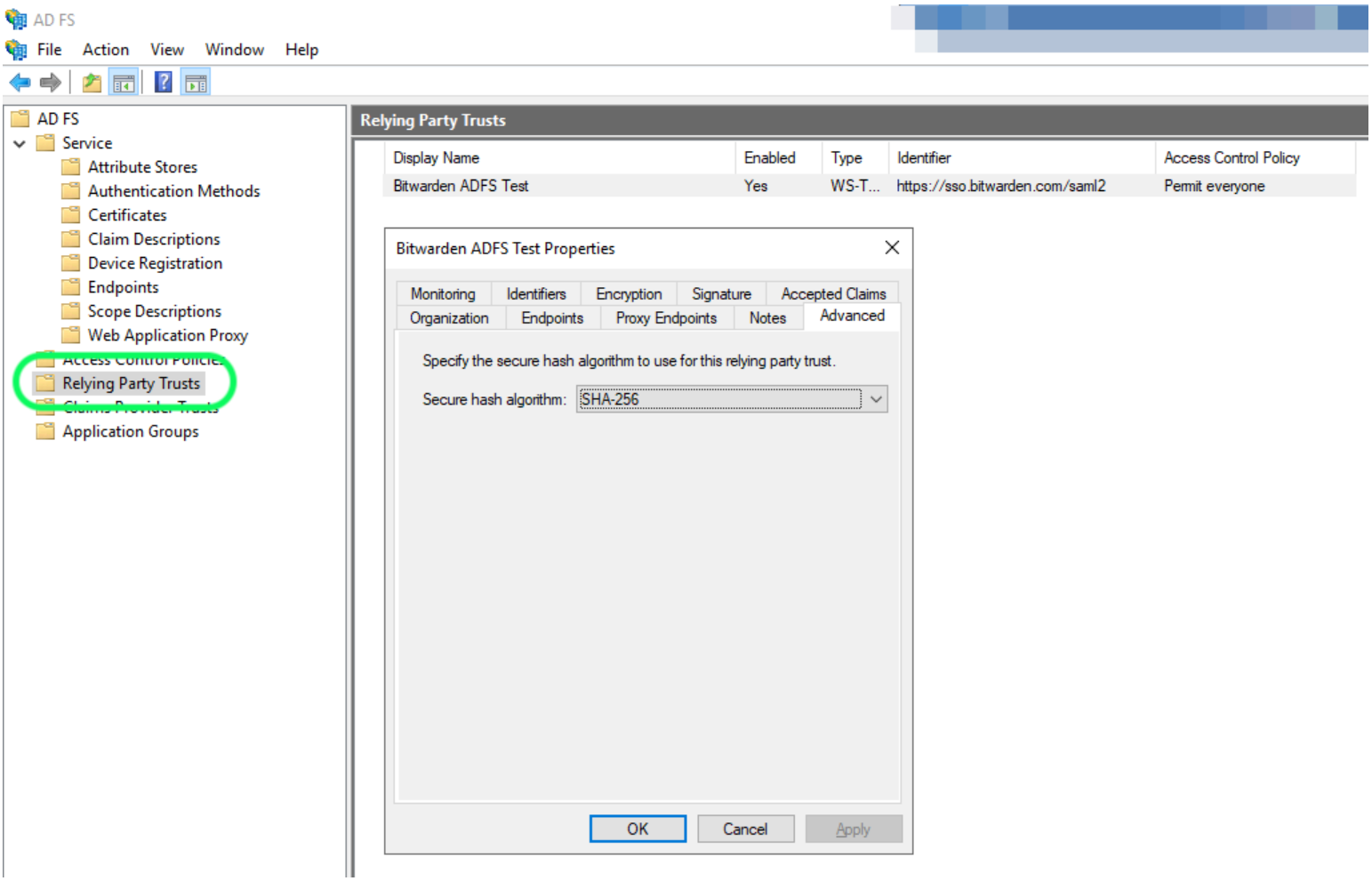
8. Bekijk uw selecties in het scherm **Klaar om vertrouwen toe te voegen**.

Geavanceerde opties

Zodra de relying party trust is aangemaakt, kun je de instellingen verder configureren door **Relying Party Trusts** te selecteren in de linker bestandsnavigator en de juiste weergavenaam te selecteren.

Hash-algoritme

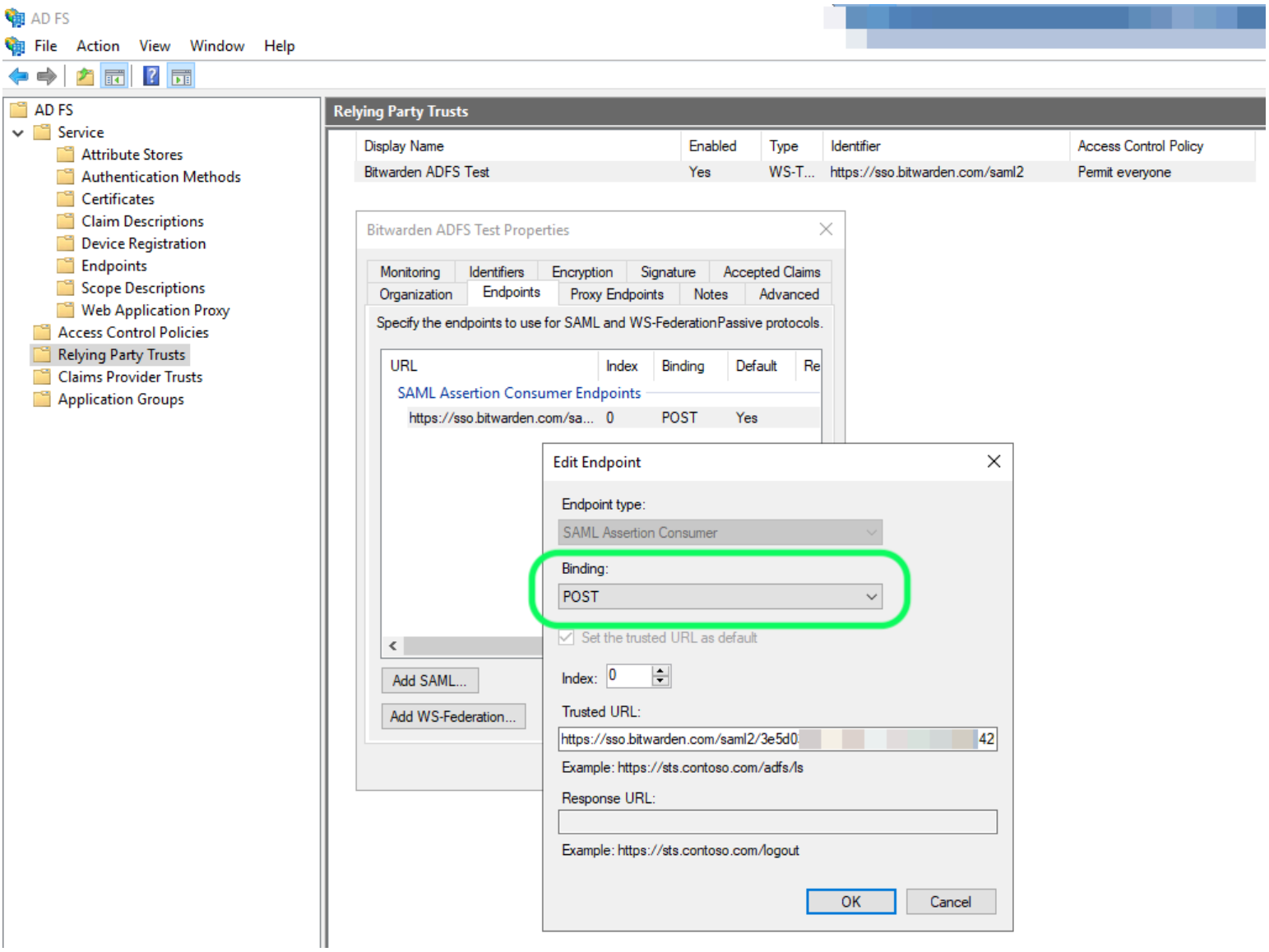
Om het **veilige hash-algoritme** (standaard SHA-256) te wijzigen, navigeer je naar het tabblad **Geavanceerd**:



Een veilig Hash-algoritme instellen

Eindpunt binding

Om het eindpunt **Binding** (standaard POST) te wijzigen, navigeer naar het tabblad **Eindpunten** en selecteer de geconfigureerde ACS URL:

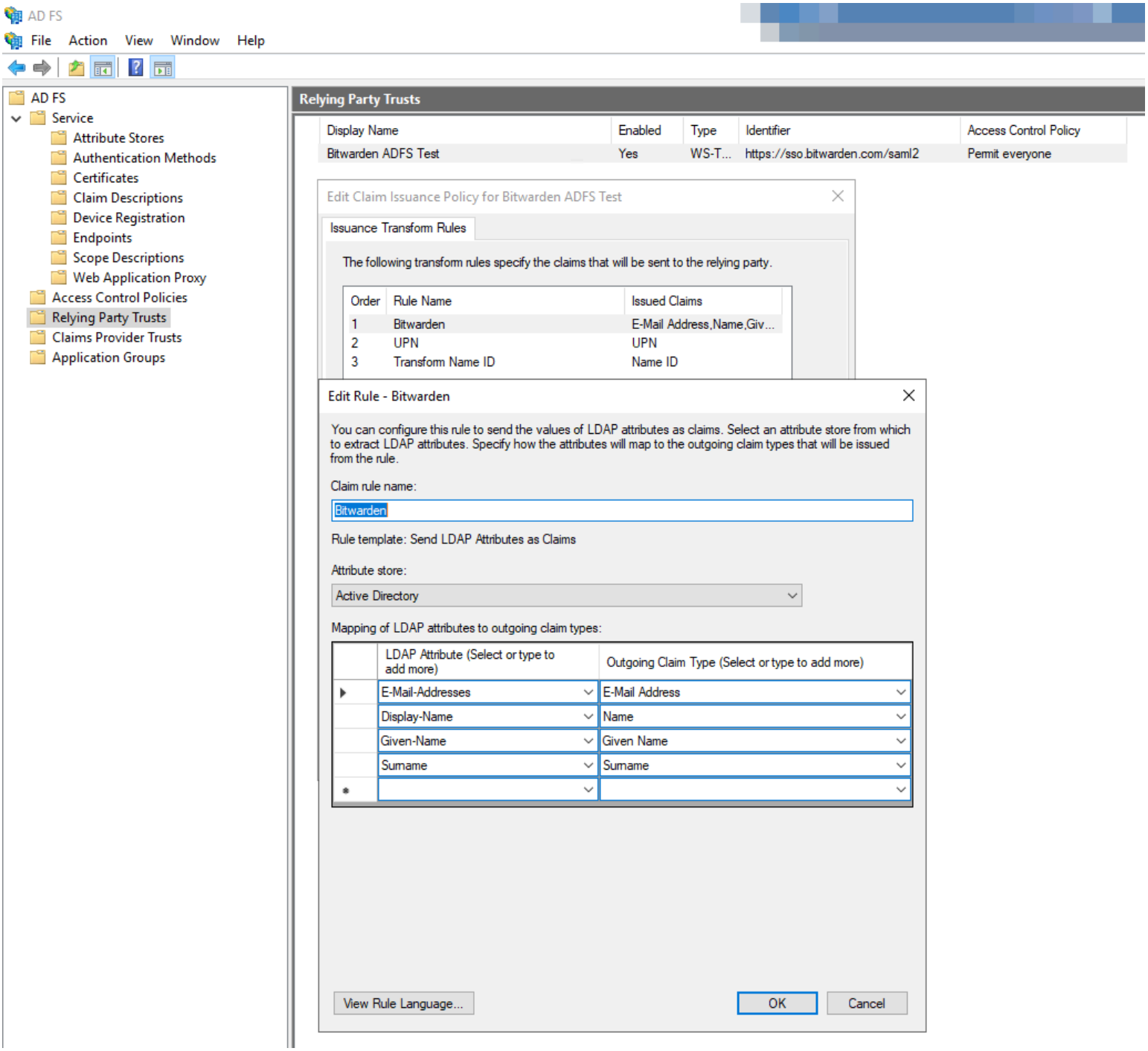


Eindpunt bewerken

Regels voor claimafgifte bewerken

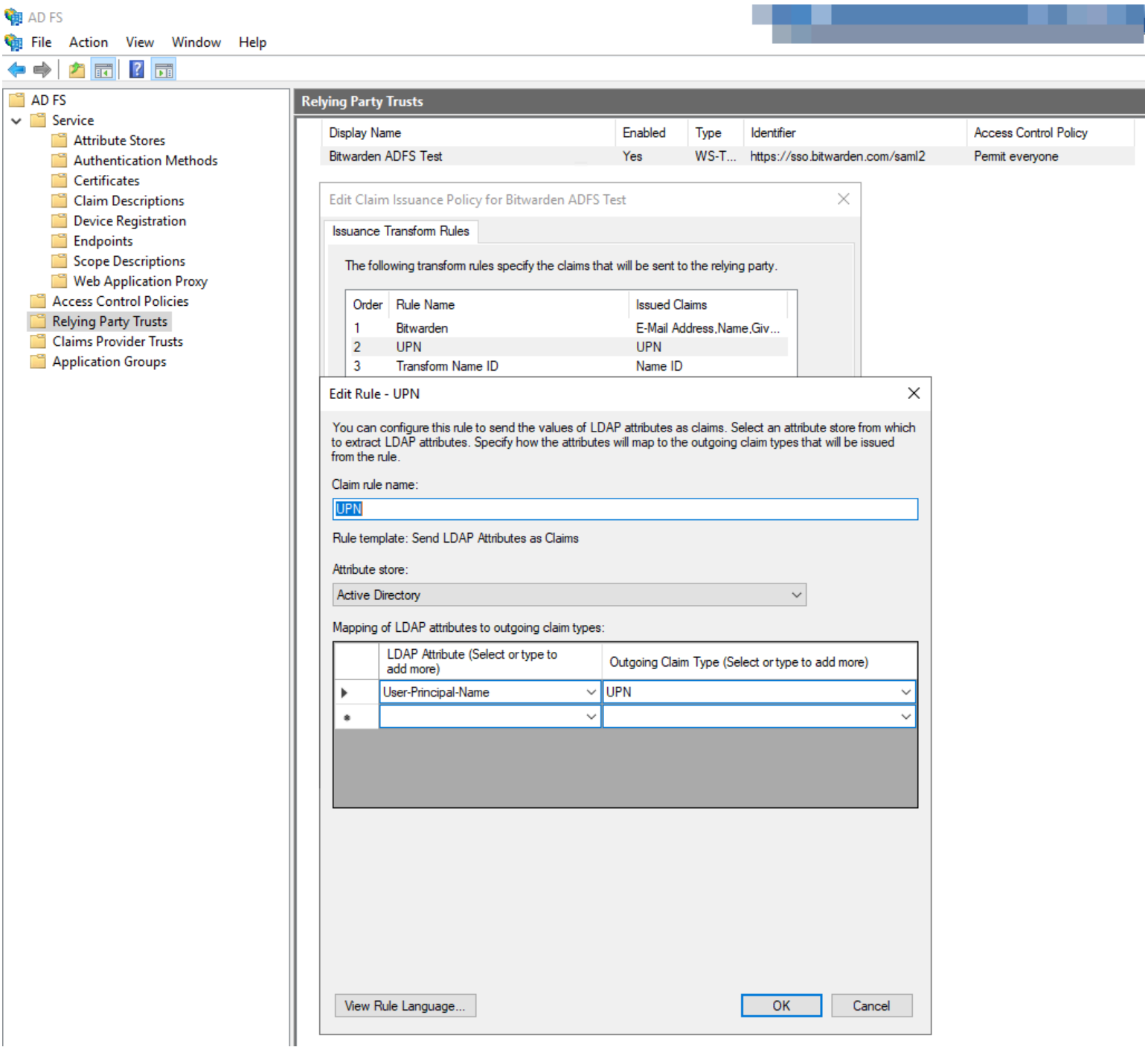
Stel regels op voor de uitgifte van claims om ervoor te zorgen dat de juiste claims, inclusief **naam-ID**, worden doorgegeven aan Bitwarden. De volgende tabs illustreren een voorbeeld van een regelset:

⇒Regel 1



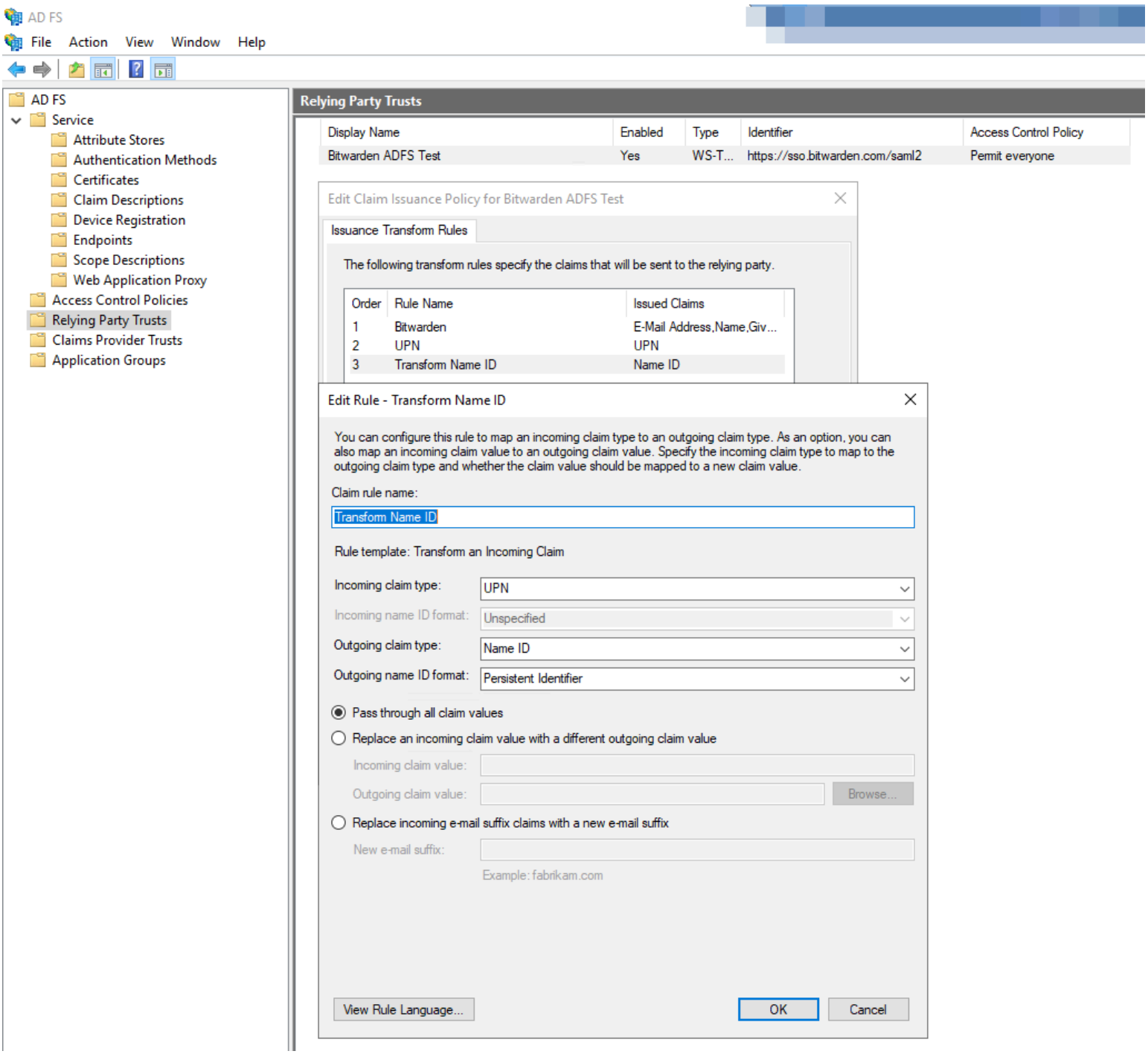
ADFS-regel 1

⇒Regel 2



ADFS-regel 2

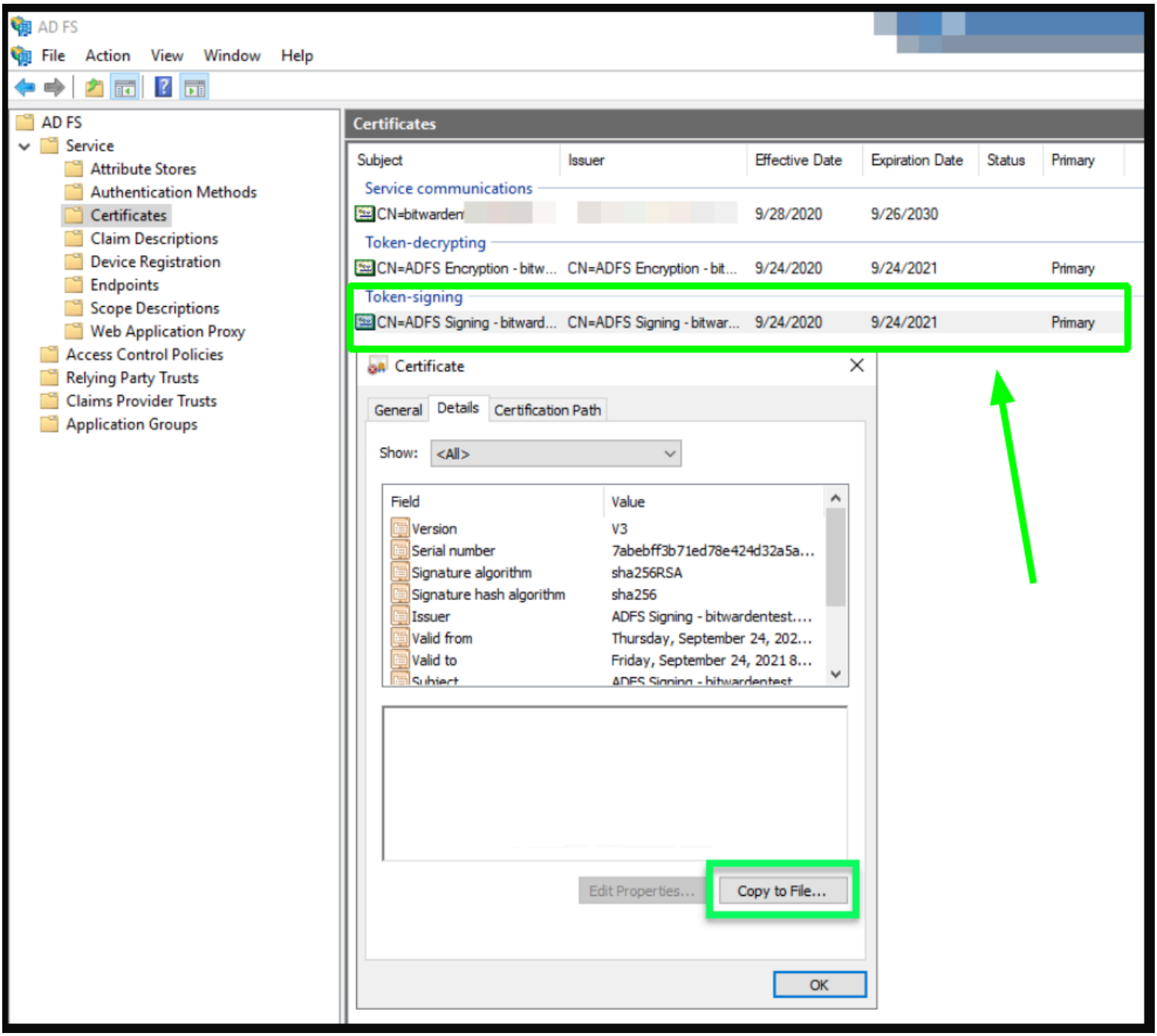
⇒Regel 3



ADFS-regel 3

Certificaat krijgen

Selecteer in de linker bestandsnavigator **AD FS → Service → Certificaten** om de lijst met certificaten te openen. Selecteer het **tokenondertekeningscertificaat**, navigeer naar het tabblad **Details** en selecteer de knop **Kopieer naar bestand...** om het Base-64 gecodeerde tokenondertekeningscertificaat te exporteren:

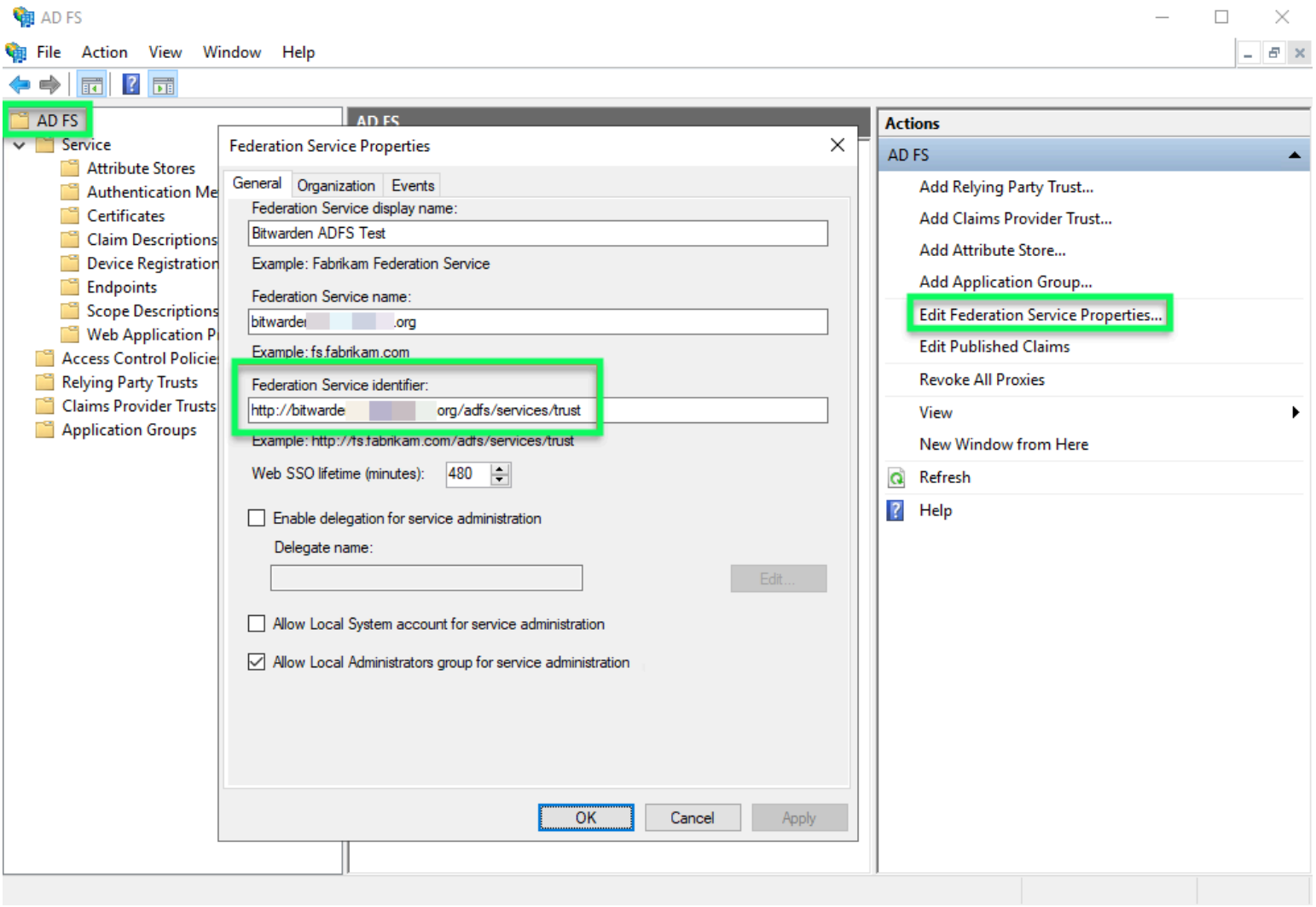


Get token-ondertekenen certificaat

Dit certificaat heb je later nodig.

Identificatiecode federatieservice ophalen

Selecteer in de linker bestandsnavigator **AD FS** en selecteer in het rechter optiemenu **Edit Federation Service Properties**. Kopieer de **Federation Service Identifier** in het venster Federation Service Properties:



Identificatiecode federatiedienst ophalen

U hebt deze identificatiecode later nodig.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de AD FS Server Manager. Ga terug naar de Bitwarden web app om de configuratie te voltooien.

Het Single sign-on scherm verdeelt de configuratie in twee secties:

- De **configuratie van de SAML-serviceprovider** bepaalt het formaat van SAML-verzoeken.
- De **configuratie van de SAML identiteitsprovider** bepaalt het formaat dat wordt verwacht voor SAML antwoorden.

Configuratie serviceprovider

Configureer de volgende velden in het gedeelte Serviceproviderconfiguratie:

Veld	Beschrijving
Naam ID Formaat	Selecteer het **uitgaande naam-ID-formaat** dat is geselecteerd bij het samenstellen van de claimafgifteregels (zie **Regel 3**).
Algoritme voor uitgaande ondertekening	Het algoritme dat Bitwarden gebruikt om SAML-verzoeken te ondertekenen.
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden.
Algoritme voor minimale inkomende ondertekening	Standaard ondertekent AD FS met SHA-256. Selecteer **SHA-256** in de vervolgkeuzelijst tenzij u AD FS hebt geconfigureerd om een ander algoritme te gebruiken.
Ondertekende beweringen	Of Bitwarden verwacht dat SAML-asserties worden ondertekend.
Certificaten valideren	Vink dit vakje aan bij gebruik van vertrouwde en geldige certificaten van je IdP via een vertrouwde CA. Zelfondertekende certificaten kunnen mislukken tenzij de juiste vertrouwensketens zijn geconfigureerd in het Bitwarden login met SSO docker image.

Als je klaar bent met de configuratie van de serviceprovider, sla je je werk **op**.

Configuratie identiteitsprovider

Bij het configureren van de identiteitsprovider moet je vaak teruggaan naar de AD FS Server Manager om waarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer de opgehaalde Federation Service Identifier in. Let op, dit **mag niet via HTTPS**. Dit veld is hoofdlettergevoelig.
Type binding	Standaard gebruikt AD FS HTTP POST endpoint binding. Selecteer **HTTP POST** tenzij je AD FS hebt geconfigureerd om een andere methode te gebruiken.

Veld	Beschrijving
URL voor service voor eenmalige aanmelding	Voer het eindpunt van de SSO-service in. Deze waarde kan worden geconstrueerd in de **Service → Endpoints** tab in AD FS Manager. De URL van het eindpunt staat vermeld als **URL Path voor SAML2.0/WS-Federation** en is meestal zoiets als `https://your-domain/adfs/ls.` Je kunt de exacte waarde vinden in de configuratiesleutel voor SingleSignOnServce in het `Federation Metadata.xml` document.

X509 publiek certificaat	Plak het gedownloade certificaat, verwijder
	
	`-----BEGIN CERTIFICAAT-----`
	
	en
	
	`-----END CERTIFICAAT-----`
	
	De waarde van het certificaat is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens zorgen **ervoor dat de certificering mislukt**.

Algoritme voor uitgaande ondertekening	Standaard ondertekent AD FS met SHA-256. Selecteer **SHA-256** in de vervolgkeuzelijst tenzij u AD FS hebt geconfigureerd om een ander algoritme te gebruiken.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of AD FS verwacht dat SAML verzoeken worden ondertekend.

Note

Let bij het invullen van het X509-certificaat op de vervaldatum. Certificaten zullen vernieuwd moeten worden om onderbrekingen in de dienstverlening aan SSO eindgebruikers te voorkomen. Als een certificaat is verlopen, kunnen de accounts Admin en Eigenaar altijd inloggen met e-mailadres en hoofdwachtwoord.

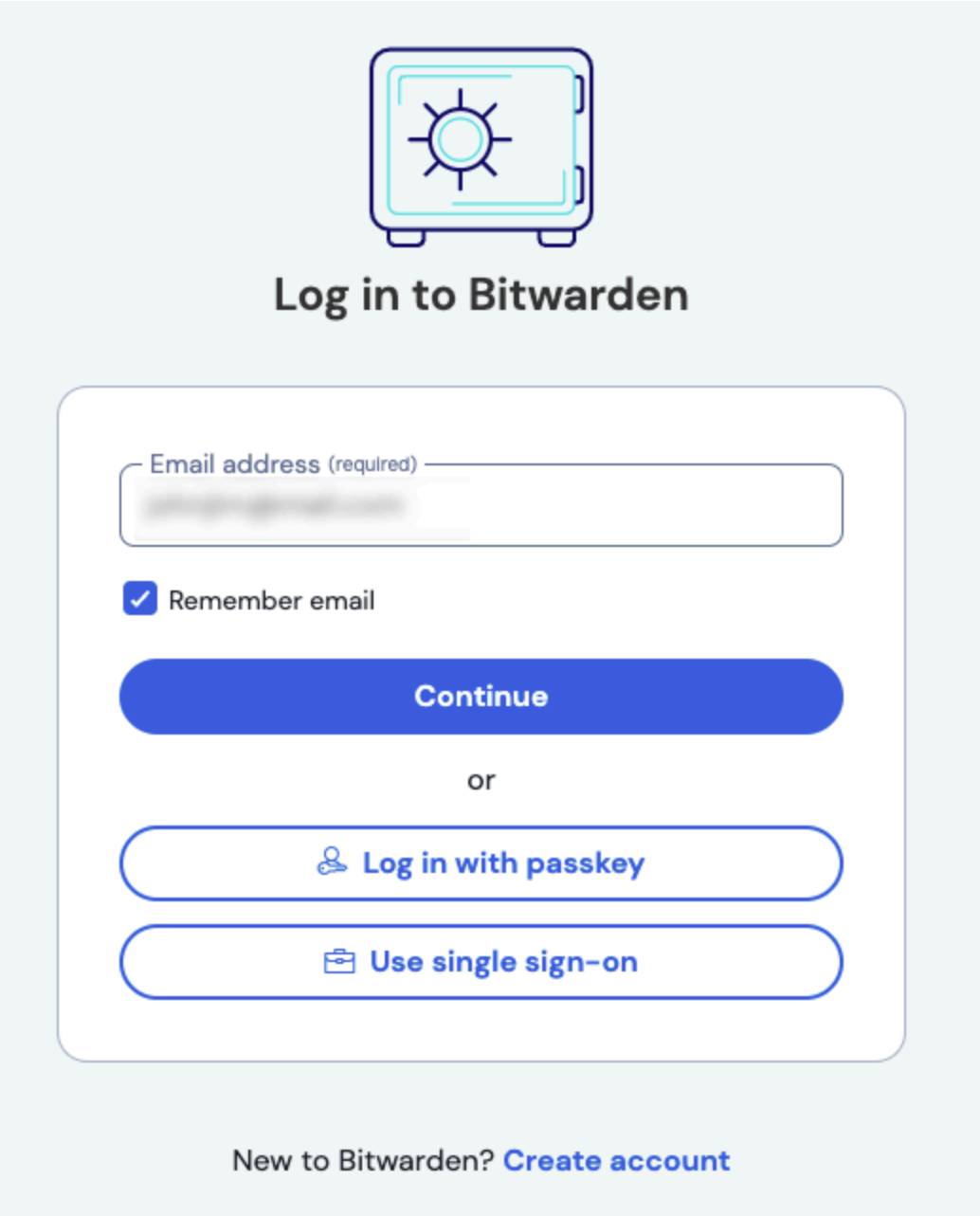
Sla uw werk **op** wanneer u klaar bent met de configuratie van de identity provider.

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.