AWS SAML-implementatie

AWS SAML-implementatie

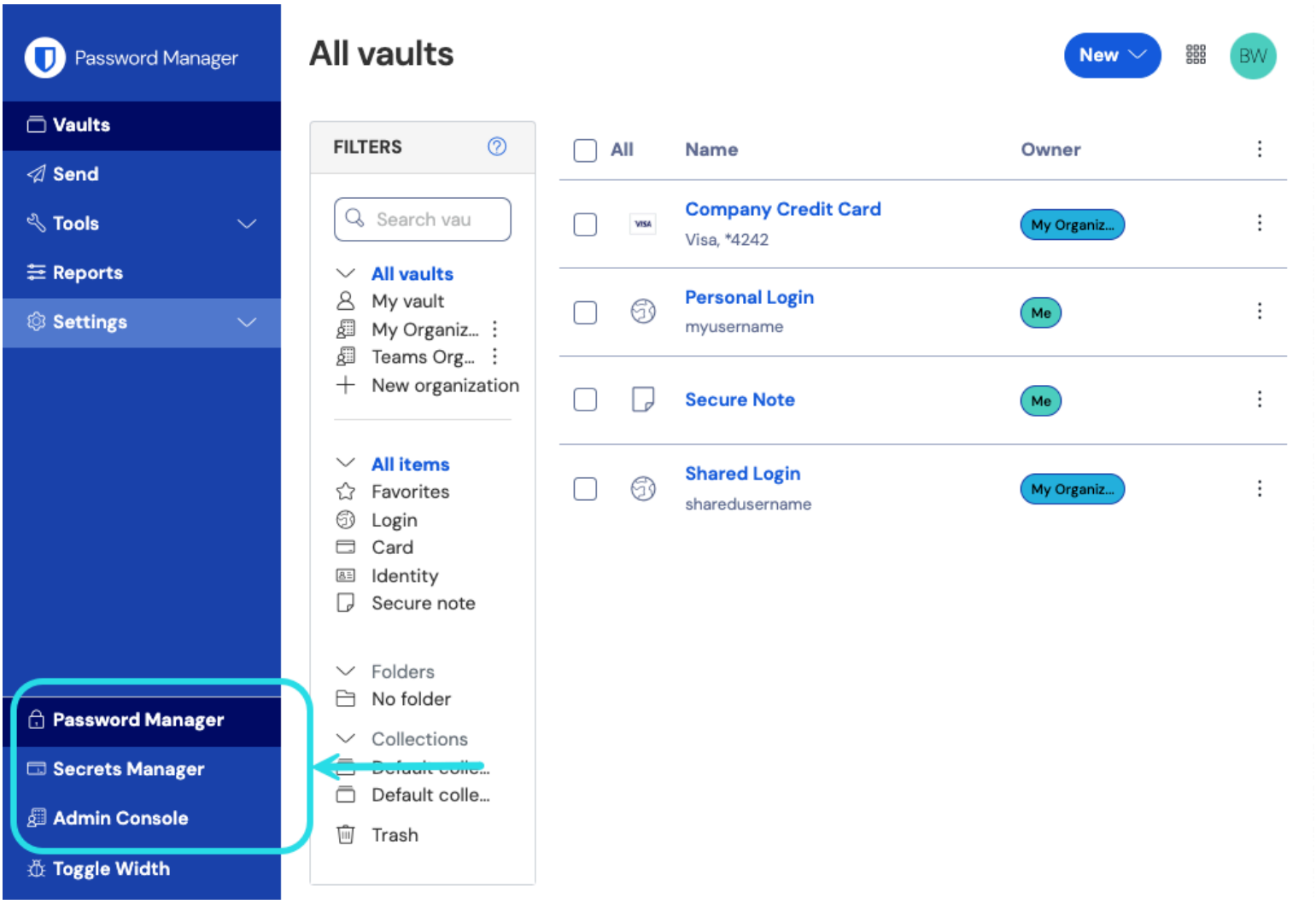
Dit artikel bevat **AWS-specifieke** hulp voor het configureren van inloggen met SSO via SAML 2.0. Raadpleeg SAML 2.0 Configuratie voor hulp bij het configureren van inloggen met SSO voor een andere IdP.

Bij de configuratie wordt tegelijkertijd gewerkt binnen de Bitwarden-webapp en de AWS Console. 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: K4Z8nyORzKkHKIJIZ4hh1

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

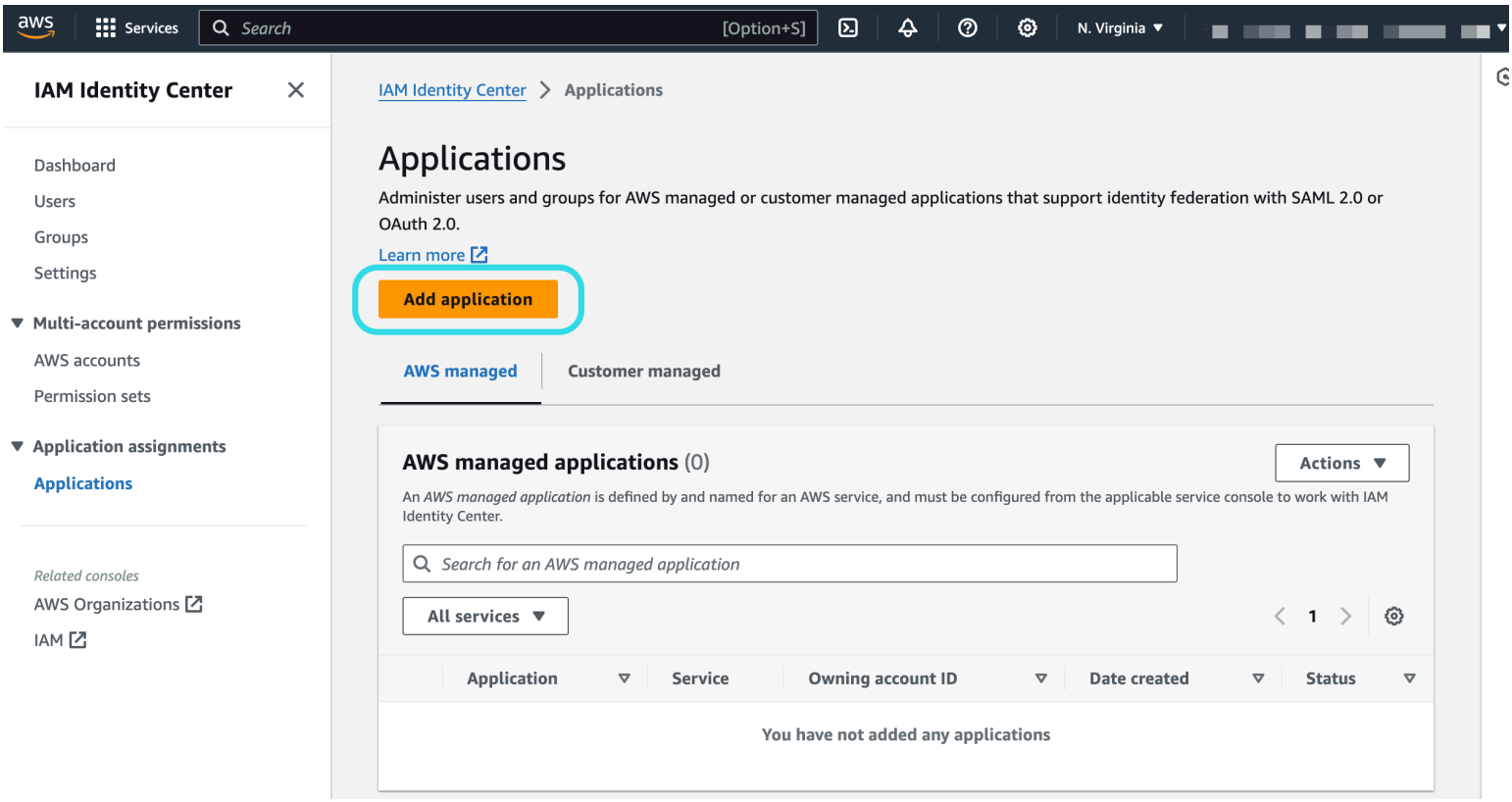
Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identifier** aan voor je organisatie en selecteer **SAML** in het keuzemenu **Type** . Houd dit scherm open voor gemakkelijke referentie.

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.

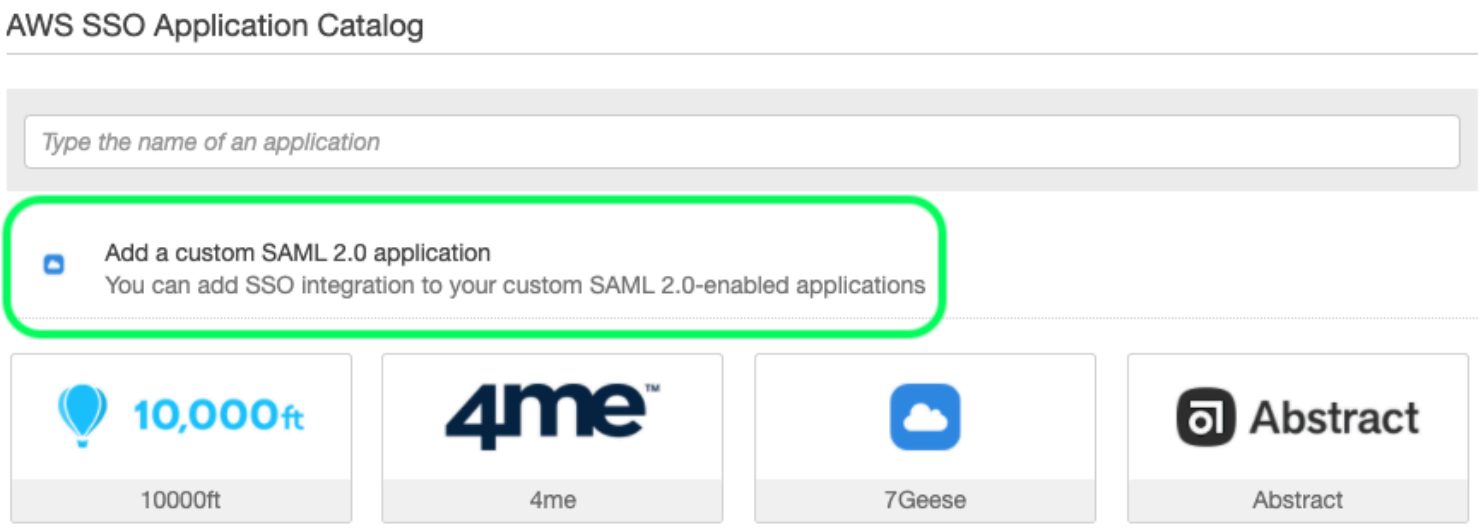
Een AWS SSO-applicatie maken

Navigeer in de AWS Console naar **AWS SSO**, selecteer **Applications** in de navigatie en selecteer de knop **Add a new application**:



Een nieuwe toepassing toevoegen

Selecteer onder de zoekbalk de optie **Voeg een aangepaste SAML 2.0-toepassing toe**:



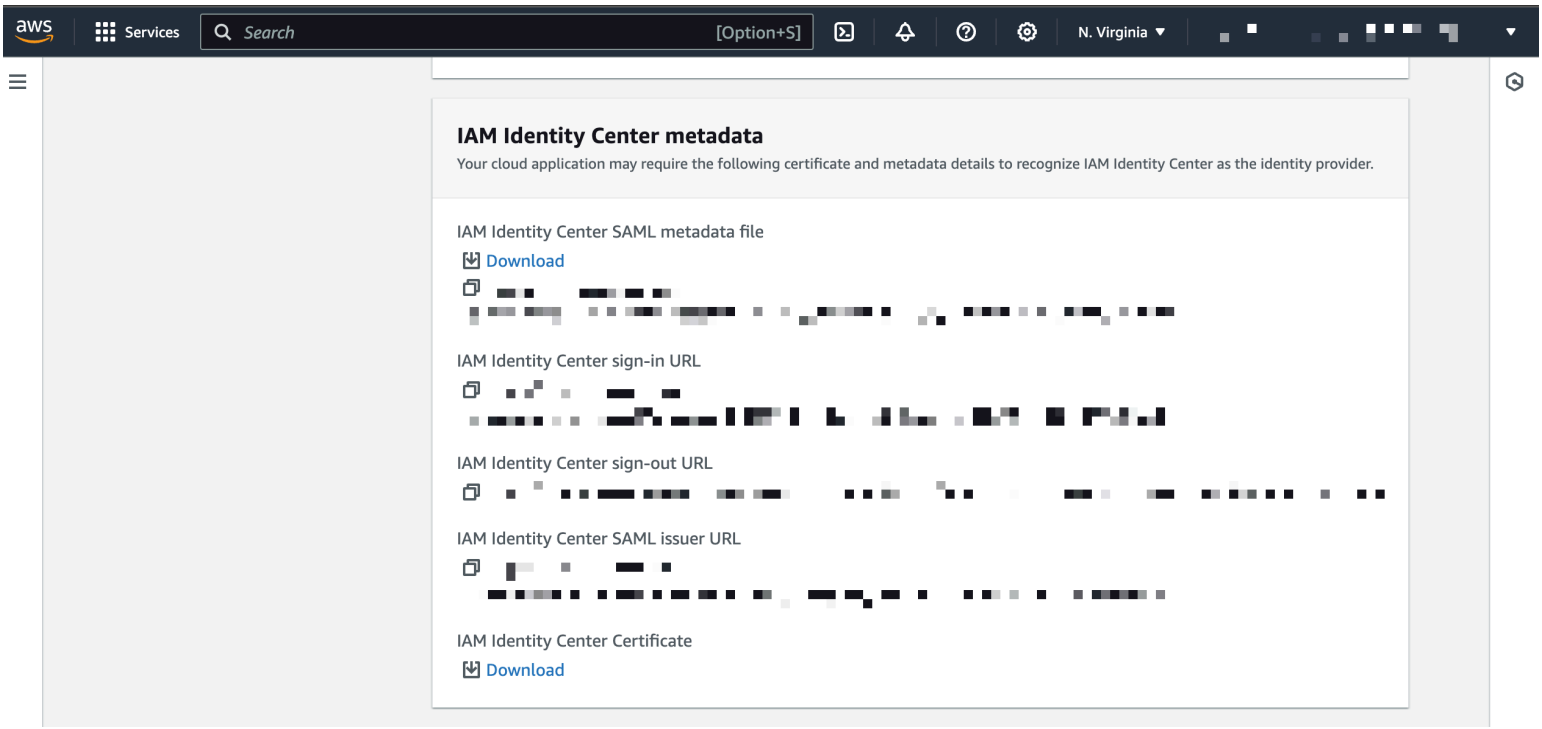
Een aangepaste SAML-app toevoegen

Details

Geef de applicatie een unieke, Bitwarden-specifieke **weergavenaam**.

AWS SSO metagegevens

U hebt de informatie in dit gedeelte nodig voor een latere configuratiestap. Kopieer de **AWS SSO sign-in URL** en **AWS SSO issuer URL**, en download het **AWS SSO certificaat**:



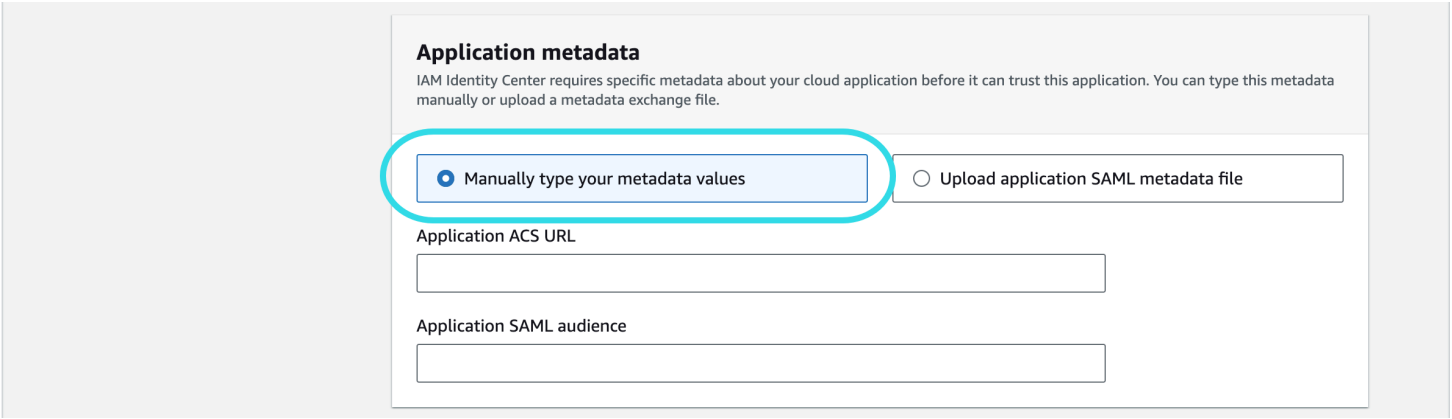
AWS SSO metagegevens

Eigenschappen van de toepassing

Geef in het veld **Application start URL** de login URL op van waaruit gebruikers toegang krijgen tot Bitwarden. Voor cloud-hosted klanten is dit altijd `https://vault.bitwarden.com/#/sso`. Voor zelf gehoste instanties wordt dit bepaald door je geconfigureerde server URL, bijvoorbeeld `https://your.domain/#/sso`.

Metagegevens toepassing

Selecteer in het gedeelte Metagegevens toepassing de optie om metagegevenswaarden handmatig in te voeren:



Metagegevenswaarden invoeren

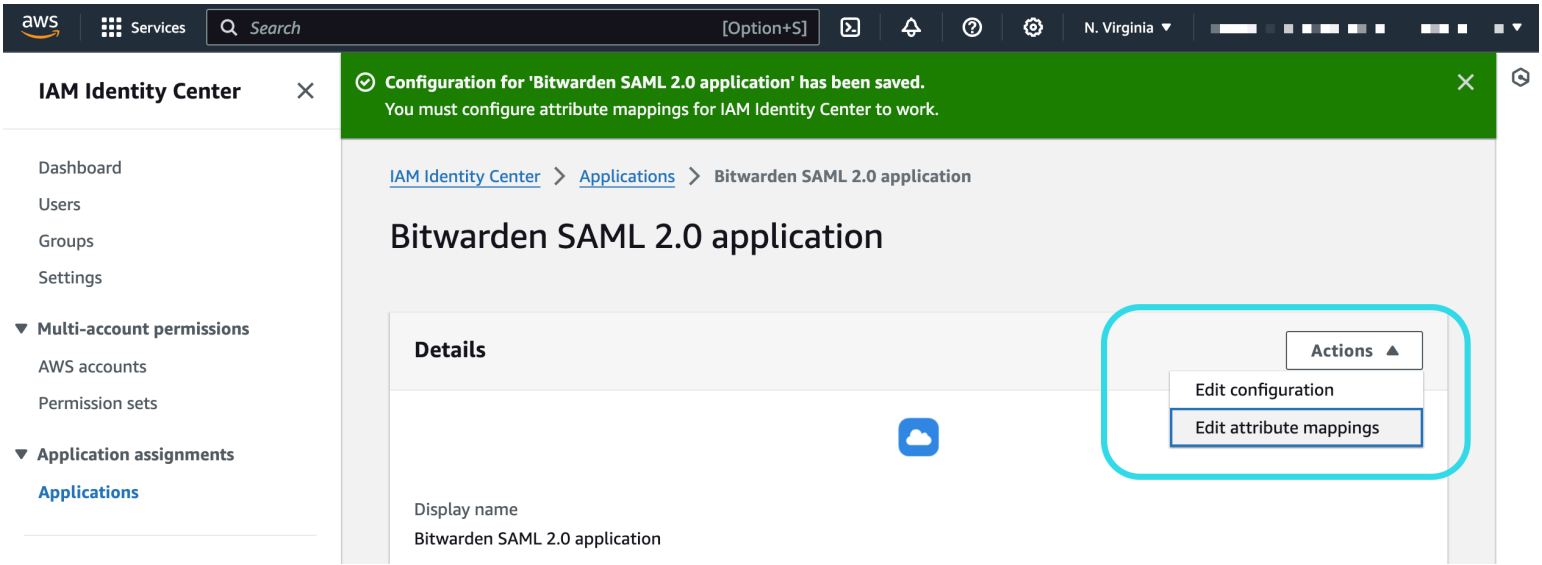
Configureer de volgende velden:

Veld	Beschrijving
Toepassing ACS URL	Stel dit veld in op de vooraf gegenereerde **URL van de Assertion Consumer Service (ACS)**. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen → Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van je instelling.
Toepassing SAML publiek	Stel dit veld in op de vooraf gegenereerde **SP entiteit ID**. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen → Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van je instelling.

Als u klaar bent, selecteert u **Wijzigingen opslaan**.

Attribuut-toewijzingen

Navigeer naar het tabblad **Attribuuttoewijzingen** en configureer de volgende toewijzingen:



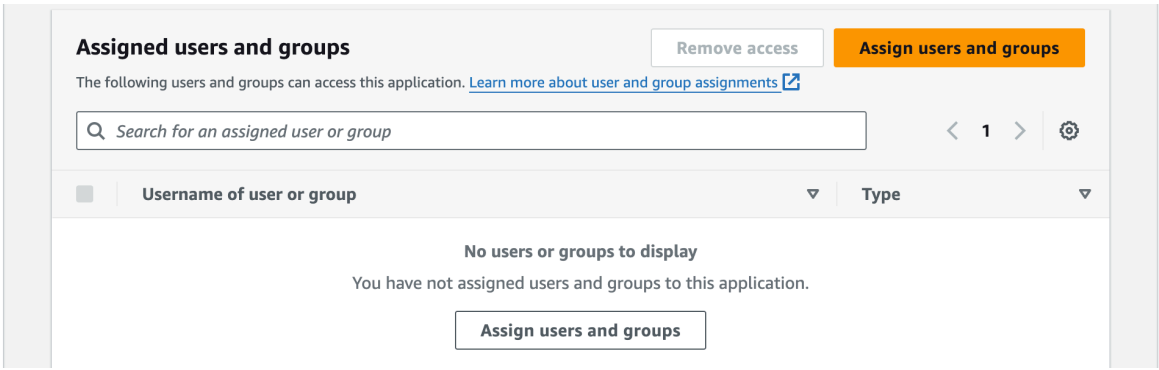
Attribuut-toewijzingen

Gebruikerskenmerk in de toepassing	Map naar deze stringwaarde of gebruikersattribuut in AWS SSO	Formaat
Onderwerp	`${user:email}`	e-mailadres

Gebruikerskenmerk in de toepassing	Map naar deze stringwaarde of gebruikersattribuut in AWS SSO	Formaat
e-mail	`${user:email}`	Ongespecificeerd

Toegewezen gebruikers

Navigeer naar het tabblad **Toegewezen gebruikers** en selecteer de knop **Gebruikers toewijzen**:



Gebruikers toewijzen

Je kunt gebruikers aan de applicatie toewijzen op individueel niveau of per groep.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de AWS Console. 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

De configuratie van de serviceprovider zou al voltooid moeten zijn, maar u kunt ervoor kiezen om een van de volgende velden te bewerken:

Veld	Beschrijving
Naam ID Formaat	Instellen op **E-mailadres**.

Veld	Beschrijving
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 AWS SSO met SHA-256. Tenzij u dit hebt gewijzigd, selecteert u sha256 in de vervolgkeuzelijst.
Ondertekende beweringen	Of Bitwarden verwacht dat SAML-asserties worden ondertekend.
Certificaten valideren	Vink dit vakje aan wanneer u vertrouwde en geldige certificaten van uw IdP via een vertrouwde CA zendt. 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 AWS Console om de applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer de **URL van de AWS SSO-emittent** in, opgehaald uit de sectie AWS SSO-metagegevens in de AWS Console. Dit veld is hoofdlettergevoelig.
Type binding	Stel in op **HTTP POST** of **Redirect**.
URL voor service voor eenmalige aanmelding	Voer de **AWS SSO aanmeldings-URL** in, opgehaald uit de AWS SSO metadata sectie in de AWS Console.

Veld	Beschrijving
URL voor service voor eenmalig afmelden	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstige ontwikkeling, maar u kunt deze vooraf configureren met de **AWS SSO sign-out URL** die wordt opgehaald uit de AWS SSO metadata sectie in de AWS Console.

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

Algoritme voor uitgaande ondertekening	Standaard ondertekent AWS SSO met `sha256`. Tenzij u dit hebt gewijzigd, selecteert u `sha256` in de vervolgkeuzelijst.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of AWS SSO 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.

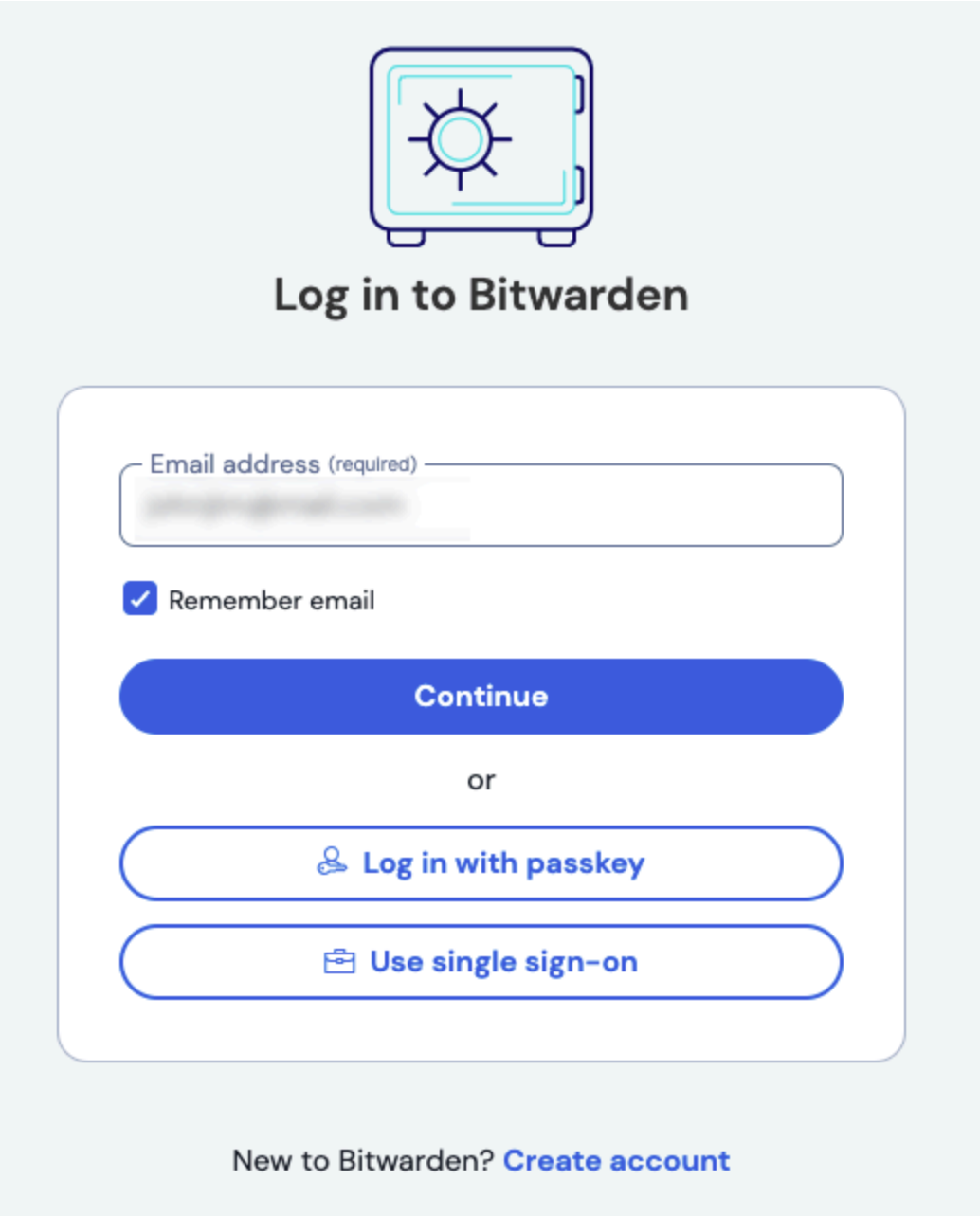
Sla uw werk **op** wanneer u klaar bent met de configuratie van de identity provider.

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.

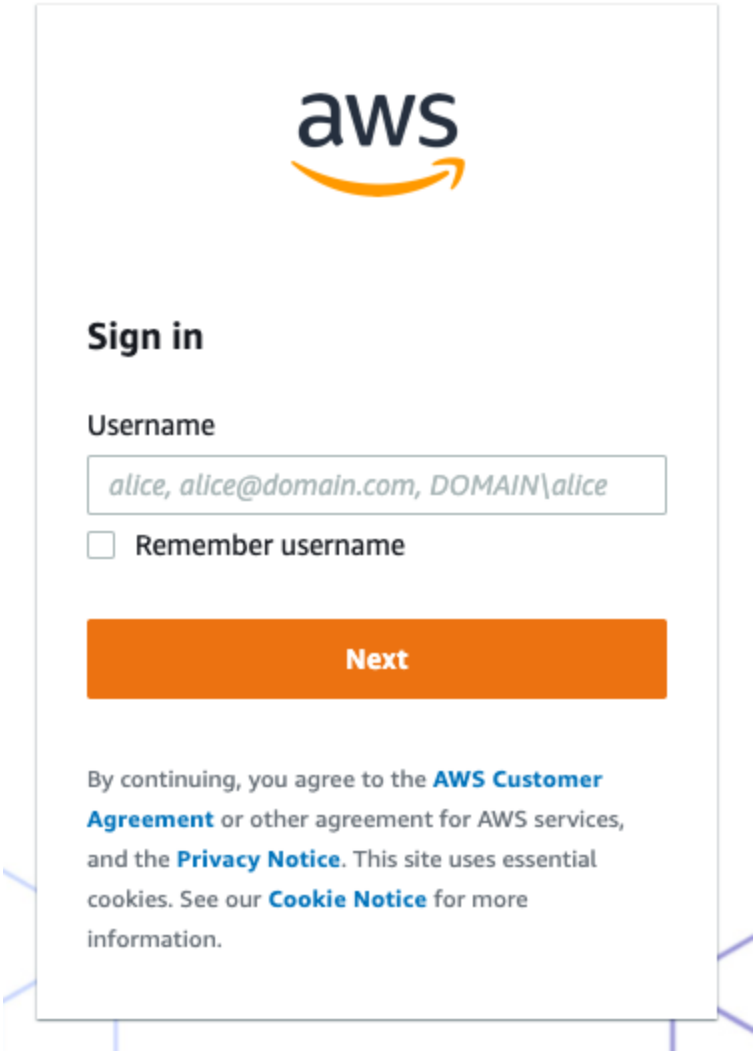
De configuratie testen

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 je implementatie succesvol is geconfigureerd, word je doorgestuurd naar het AWS SSO inlogscherm:



AWS-inlogscherm

Nadat u zich hebt geverifieerd met uw AWS-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.