Microsoft Entra ID SAML-implementatie

Weergeven in het Helpcentrum:
https://bitwarden.com/help/saml-microsoft-entra-id/

Microsoft Entra ID SAML-implementatie

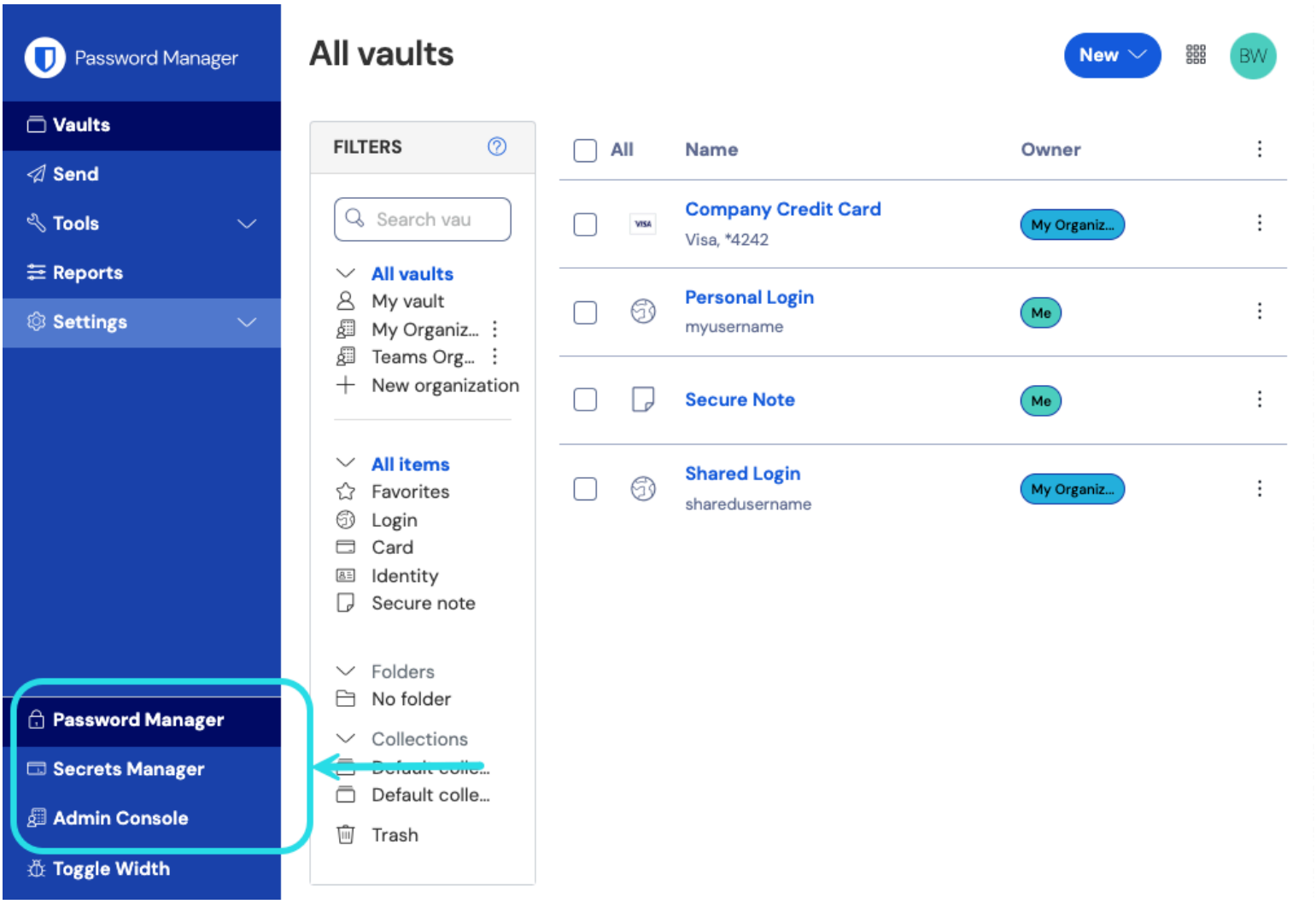
Dit artikel bevat **Azure-specifieke** hulp voor het configureren van Login met SSO via SAML 2.0. Raadpleeg SAML 2.0 Configuratie voor hulp bij het configureren van inloggen met SSO voor een andere IdP.

Bij de configuratie wordt tegelijkertijd gewerkt met de Bitwarden webapp en de Azure 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.

> **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: 7CKe4TX98FPF86eAimKgak

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

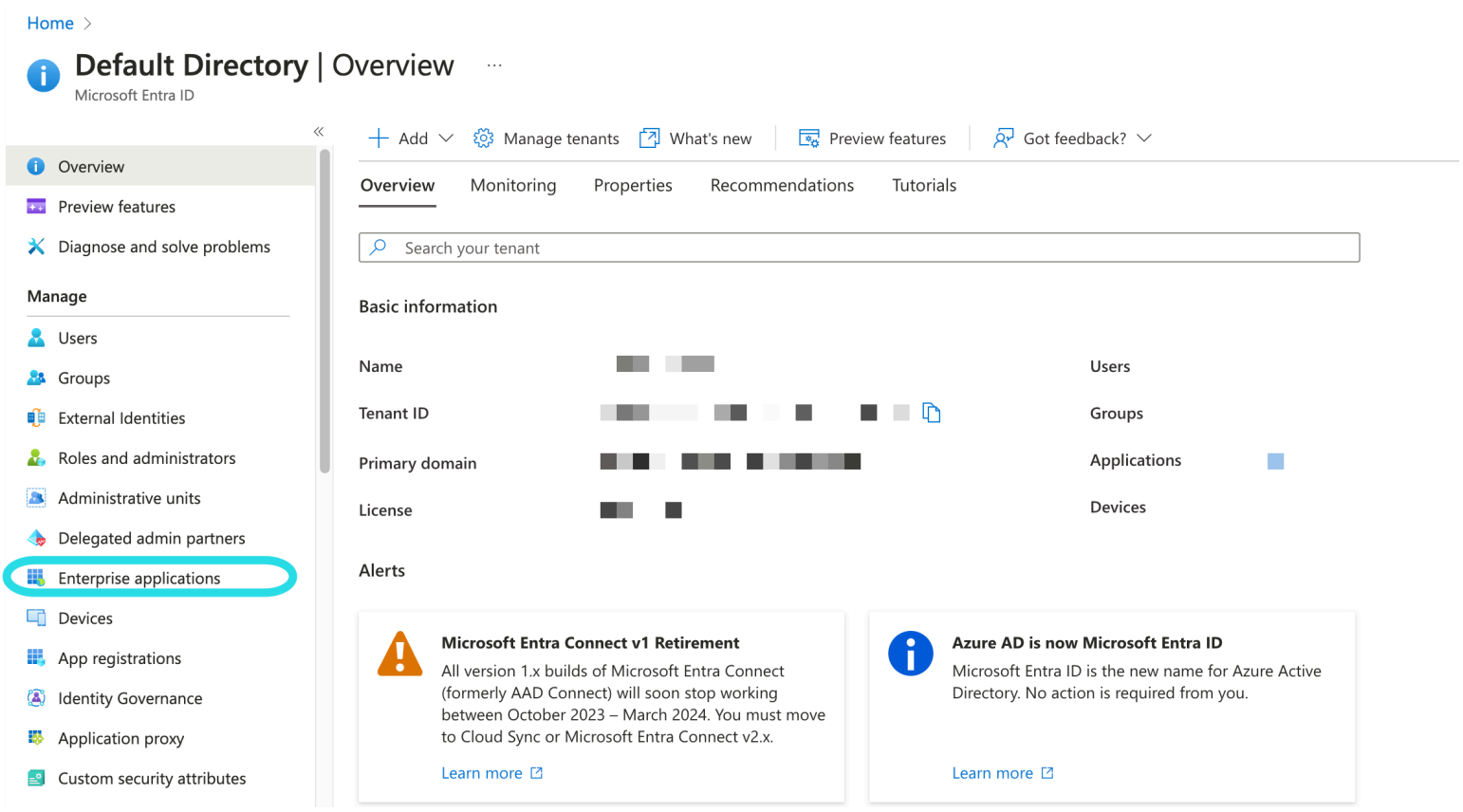
Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identifier** aan voor je organisatie en selecteer **SAML** in het keuzemenu **Type** . Houd dit scherm open voor gemakkelijke referentie.

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.

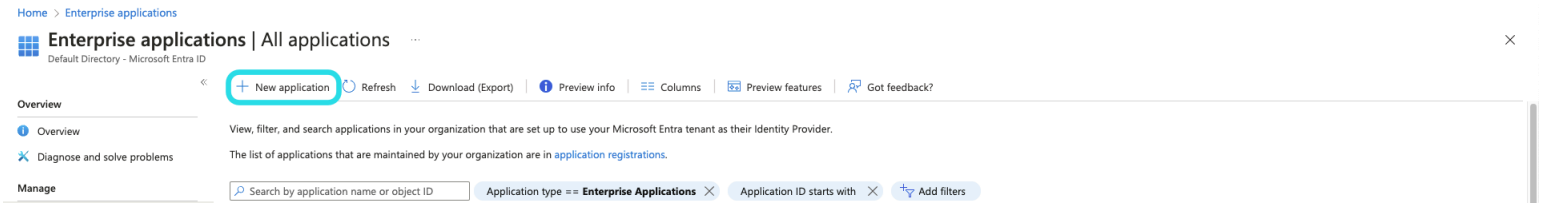
Een bedrijfsapplicatie maken

Navigeer in de Azure Portal naar **Microsoft Entra ID** en selecteer **Enterprise toepassingen** in het navigatiemenu:



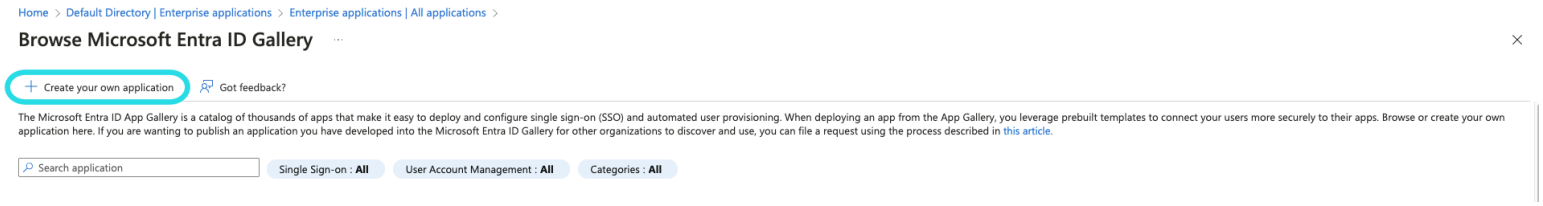
Enterprise applications

Selecteer de knop ＋ **Nieuwe toepassing**:



Create new application

Selecteer op het scherm Browse Microsoft Entra ID Gallery de knop ＋ **Maak uw eigen toepassing**:

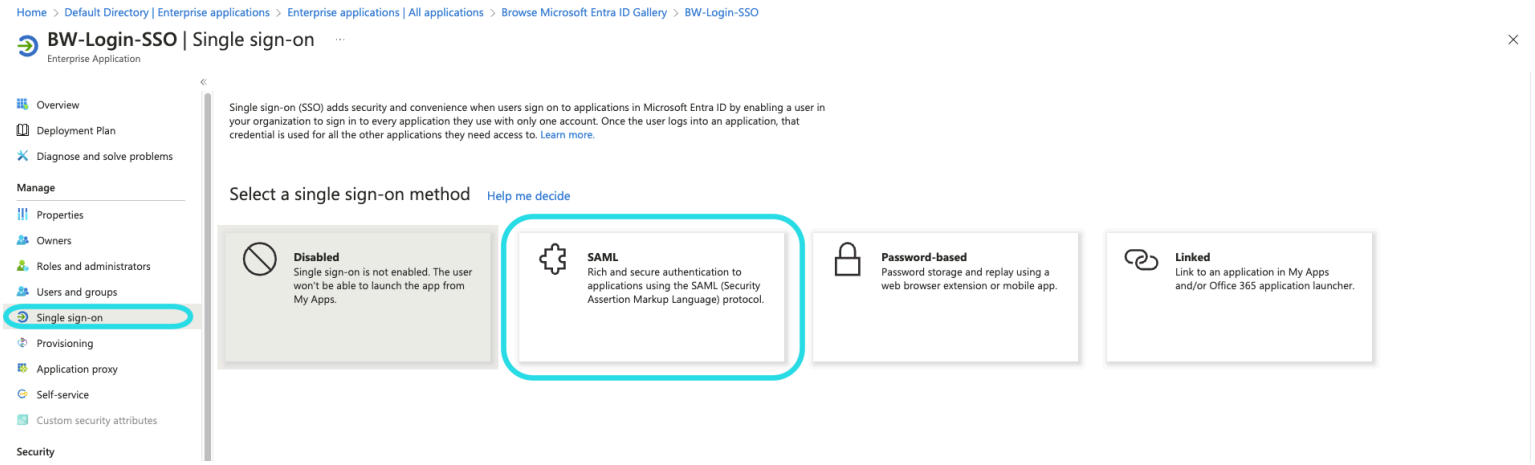


Create your own application

Geef de applicatie in het scherm Maak uw eigen applicatie een unieke, Bitwarden-specifieke naam en selecteer de optie (Niet-galerij). Klik op de knop **Maken** als je klaar bent.

Eenmalige aanmelding inschakelen

Selecteer **Eenmalige aanmelding** in de navigatie van het scherm Toepassingsoverzicht:



Configure Single sign-on

Selecteer **SAML** in het scherm Single Sign-On.

SAML instellen

Basis SAML-configuratie

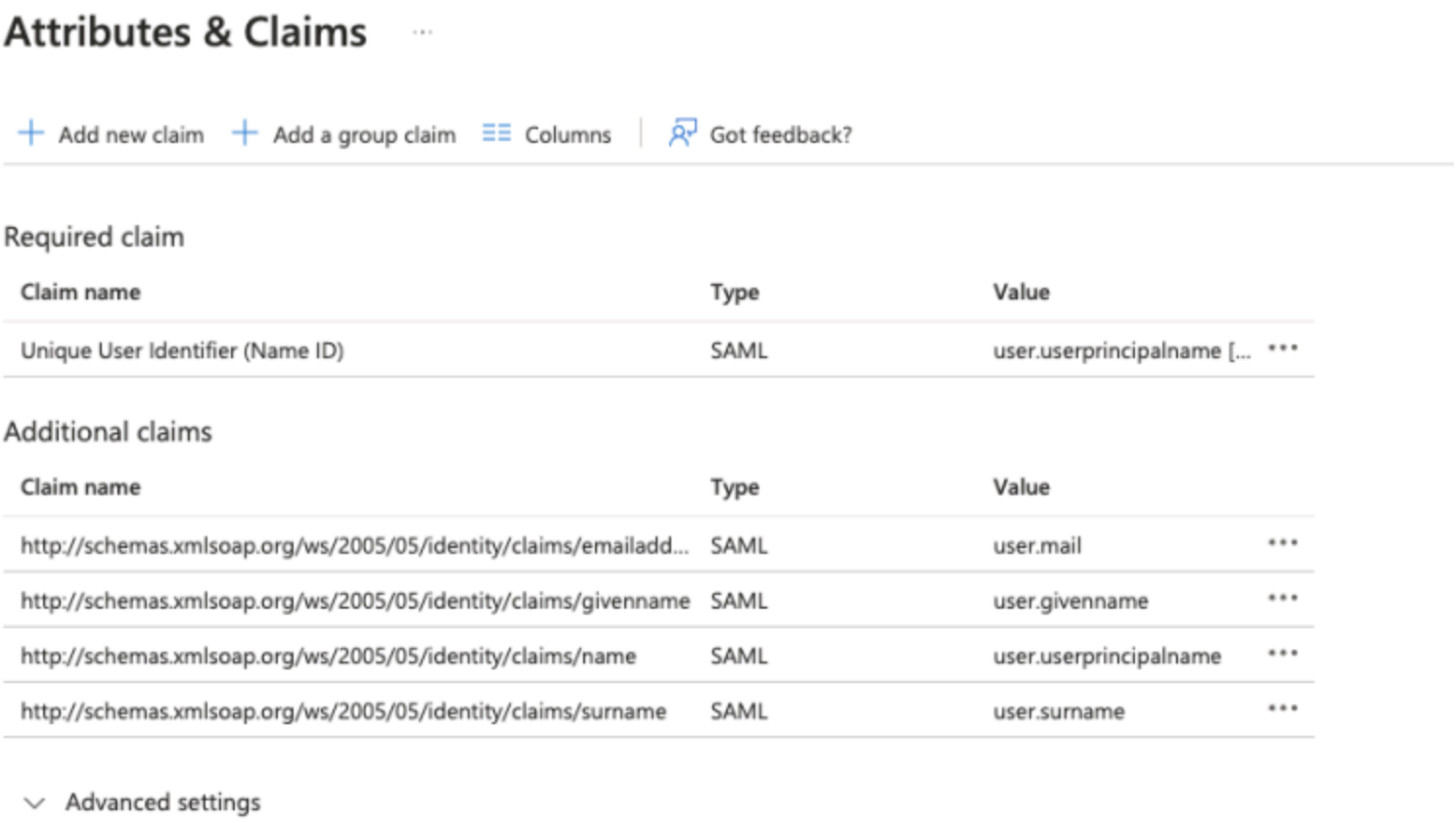
Selecteer de knop **Bewerken** en configureer de volgende velden:

Veld	Beschrijving
Identificatiecode (entiteits-ID)	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 uw instelling.
Antwoord-URL (Assertion Consumer Service 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 uw instelling.
Aanmelden URL	Stel dit veld in op de aanmeldings-URL van waaruit gebruikers toegang krijgen tot Bitwarden. Voor cloud-hosted klanten is dit `https://vault.bitwarden.com/#/sso` of `https://vault.bitwarden.eu/#/sso`. Voor zelf gehoste instanties wordt dit bepaald door je geconfigureerde server URL, bijvoorbeeld `https://your-domain.com/#/sso`.

Gebruikersattributen & claims

De standaardclaims die Azure maakt zullen werken met inloggen met SSO, maar je kunt dit gedeelte optioneel gebruiken om de NameID-indeling te configureren die Azure gebruikt in SAML-reacties.

Selecteer de knop **Bewerken** en selecteer het item **Unieke gebruikersidentificatie (Name ID)** om de NameID-claim te bewerken:



Bewerk NaamID Claim

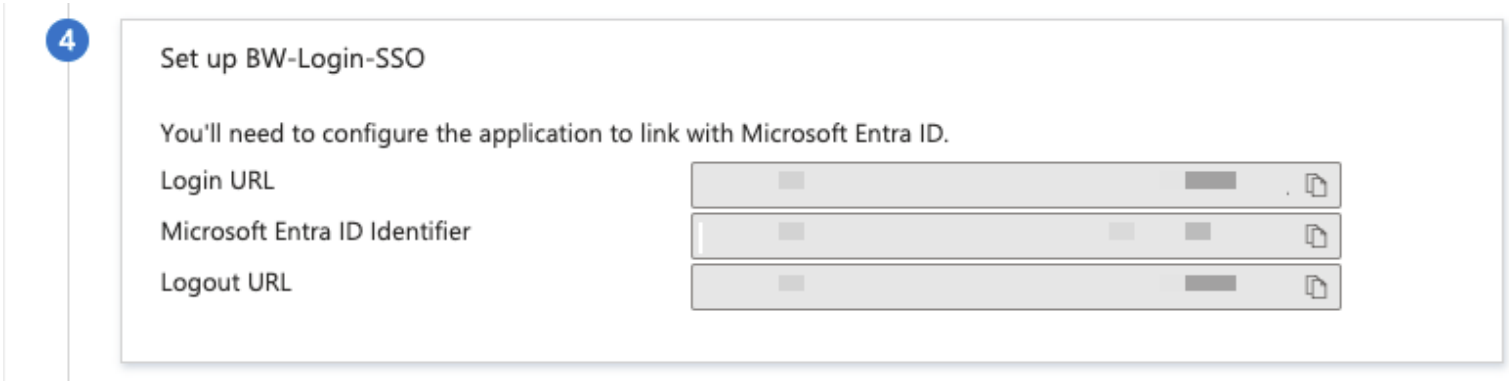
De opties zijn Standaard, E-mailadres, Persistent, Unspecified en Windows gekwalificeerde domeinnaam. Raadpleeg de Microsoft Azure documentatie voor meer informatie.

SAML ondertekeningscertificaat

Download het Base64-certificaat voor gebruik tijdens een latere stap.

Uw toepassing instellen

Kopieer of noteer de **aanmeldings-URL** en **Microsoft Entra ID Identifier** in dit gedeelte voor gebruik tijdens een latere stap:

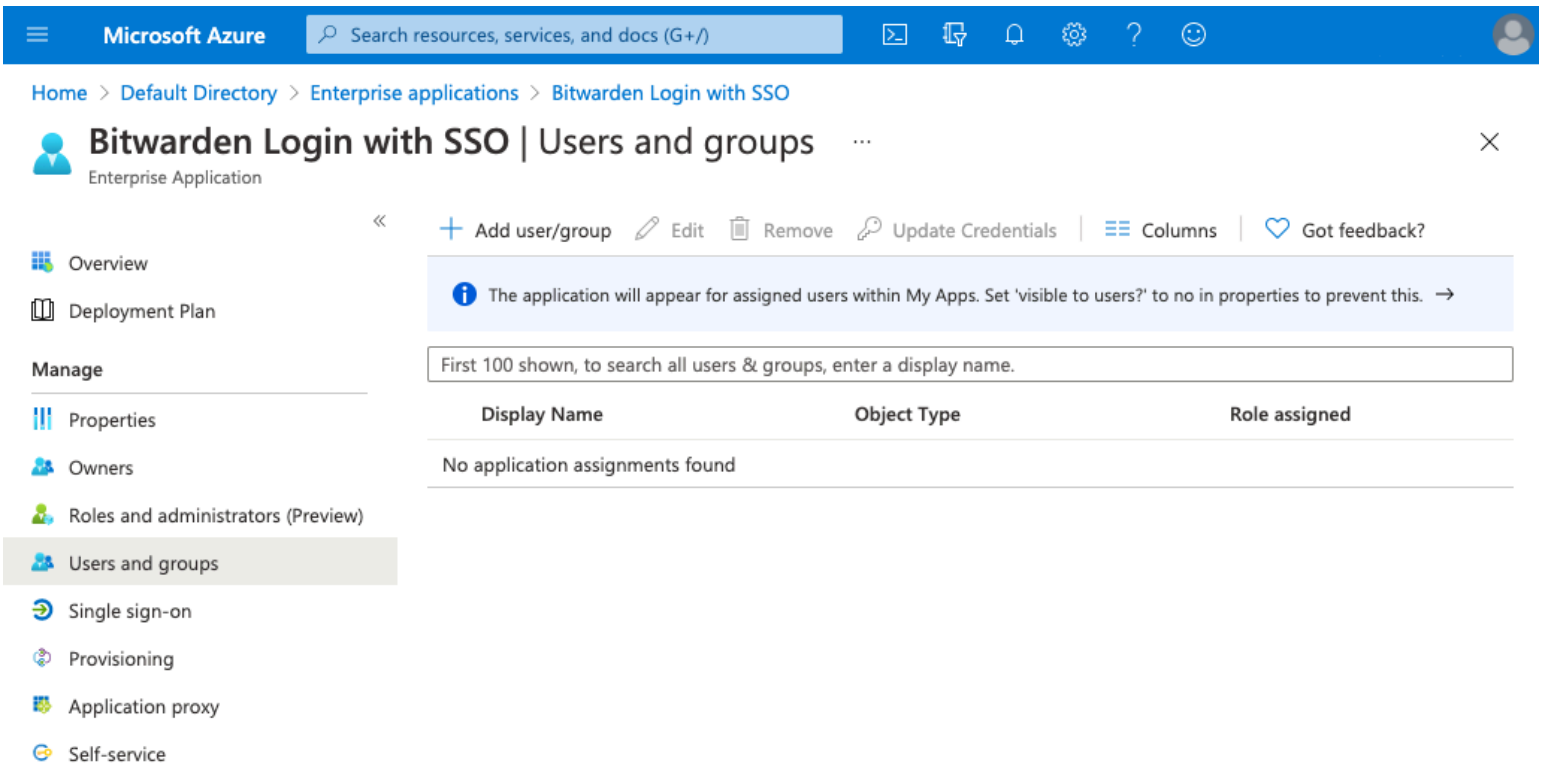


Azure URLs

> **Note**
> If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

Gebruikers en groepen

Selecteer **Gebruikers en groepen** in de navigatie:



Assign users or groups

Selecteer de knop **Gebruiker/groep toevoegen** om toegang tot de login met SSO-toepassing toe te wijzen op gebruikers- of groepsniveau.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de Azure Portal. 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:

Veld	Beschrijving
Naam ID Formaat	Standaard gebruikt Azure het e-mailadres. Als u deze instelling hebt gewijzigd, selecteert u de overeenkomstige waarde. Stel dit veld anders in op **Unspecified** of **Email Address**.
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 Azure met RSA SHA-256. Selecteer `rsa-sha256` in de vervolgkeuzelijst.
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 met het Bitwarden login met SSO docker image.

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

Configuratie identiteitsprovider

Identity provider configuratie vereist vaak dat je terugkeert naar de Azure Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer uw **Microsoft Entra ID Identifier** in, die u hebt opgehaald uit de sectie Uw toepassing instellen van de Azure Portal. Dit veld is hoofdlettergevoelig.
Type binding	Stel in op **HTTP POST** of **Redirect**.
URL voor service voor eenmalige aanmelding	Voer uw **aanmeldings-URL** in, opgehaald uit de sectie Uw toepassing instellen van de Azure Portal.
URL voor service voor eenmalig afmelden	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstige ontwikkeling, maar u kunt deze desgewenst vooraf configureren met uw **URL voor afmelden** .

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 Azure met RSA SHA-256. Selecteer `rsa-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 Azure verwacht dat SAML verzoeken worden ondertekend.

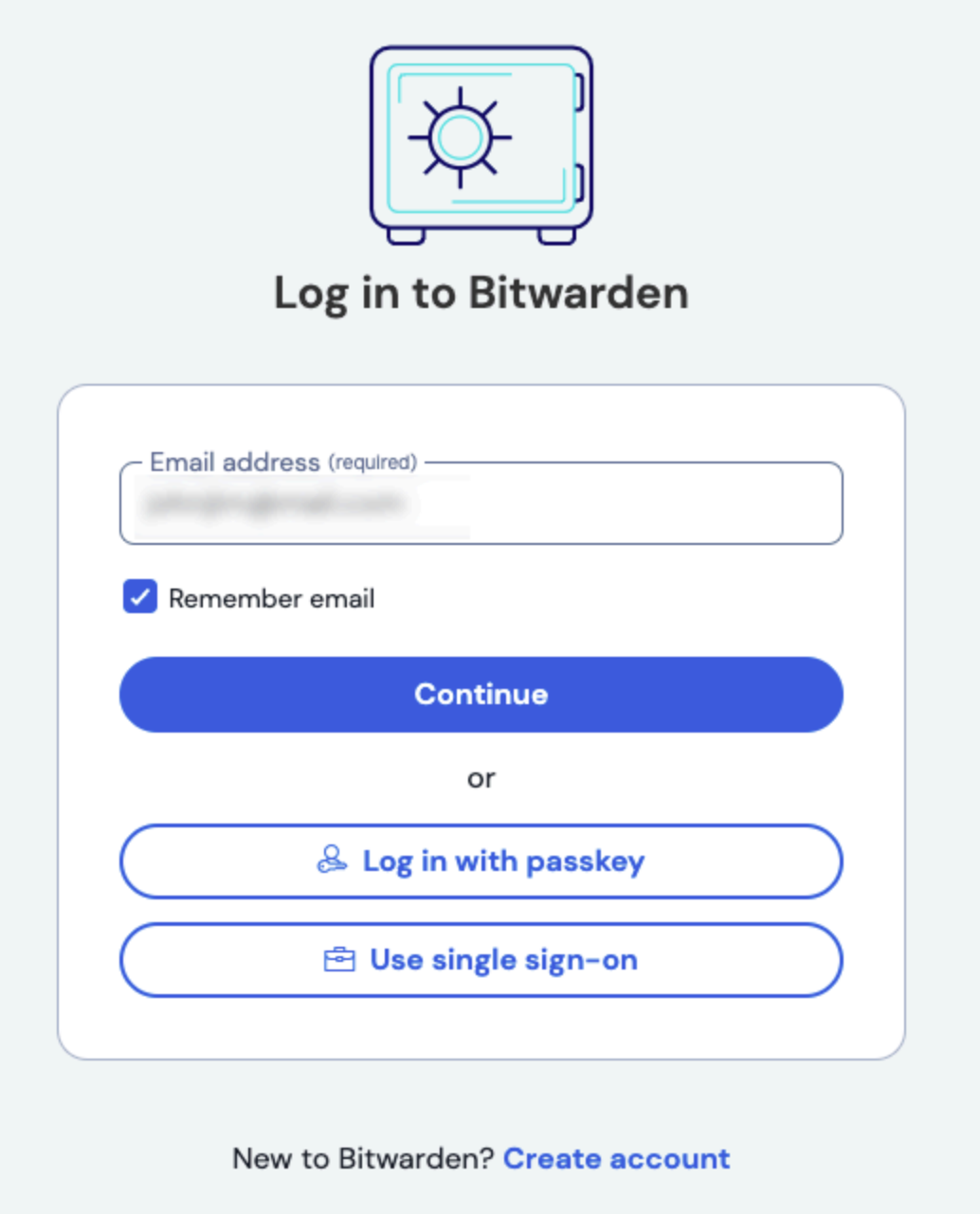
> **Note**
> Let bij het invullen van het X509-certificaat op de vervaldatum. Certificaten zullen vernieuwd moeten worden om onderbrekingen in de dienstverlening aan SSO eindgebruikers te voorkomen. Als een certificaat is verlopen, kunnen de accounts Admin en Eigenaar altijd inloggen met e-mailadres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

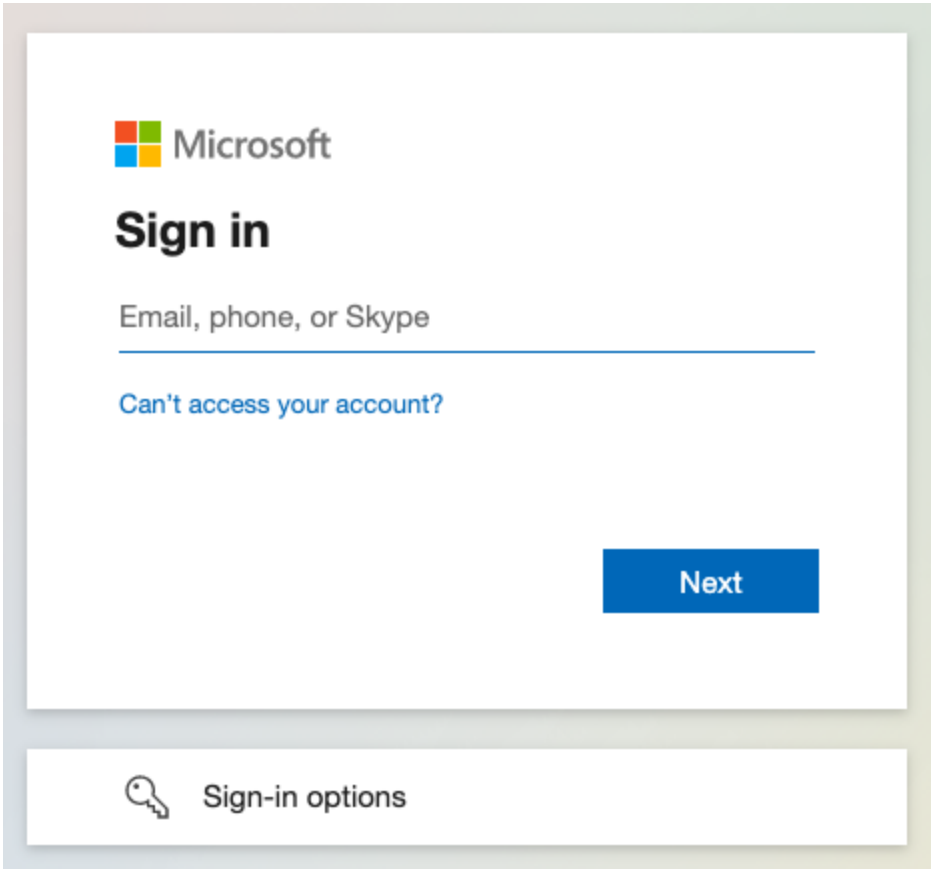
De configuratie testen

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 met succes is geconfigureerd, wordt u doorgestuurd naar het inlogscherm van Microsoft:



Azure login screen

Nadat u zich hebt geverifieerd met uw Azure-referenties, 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. Azure SAML-beheerders kunnen een App-registratie instellen zodat gebruikers worden doorgestuurd naar de inlogpagina voor de Bitwarden-webkluis.

1. Schakel de bestaande Bitwarden-knop uit op de pagina **Alle toepassingen** door te navigeren naar de huidige Bitwarden Enterprise-toepassing en eigenschappen te selecteren en de optie **Zichtbaar voor gebruikers** in te stellen op **Nee**.

2. Maak de App Registratie door te navigeren naar **App Registraties** en **Nieuwe Registratie** te selecteren.

3. Geef een naam op voor de toepassing, zoals **Bitwarden SSO**. Geen omleidings-URL opgeven. Selecteer **Registreren** om het forum te voltooien.

4. Zodra de app is gemaakt, navigeer je naar **Branding & Properties** in het navigatiemenu.

5. Voeg de volgende instellingen toe aan de applicatie:

    1. Upload een logo voor herkenning bij de eindgebruiker. Je kunt het Bitwarden-logo hier ophalen.

    2. Stel de **URL van de startpagina** in op de inlogpagina van uw Bitwarden-client, zoals `https://vault.bitwarden.com/#/login` of `uw-zelf-gehosteURL.com`.

Zodra dit proces is voltooid, hebben toegewezen gebruikers een Bitwarden-applicatie die hen rechtstreeks koppelt aan de inlogpagina voor de Bitwarden-webkluis.