BEHEERCONSOLE › INLOGGEN MET SSO ›

JumpCloud SAML-implementatie

JumpCloud SAML-implementatie

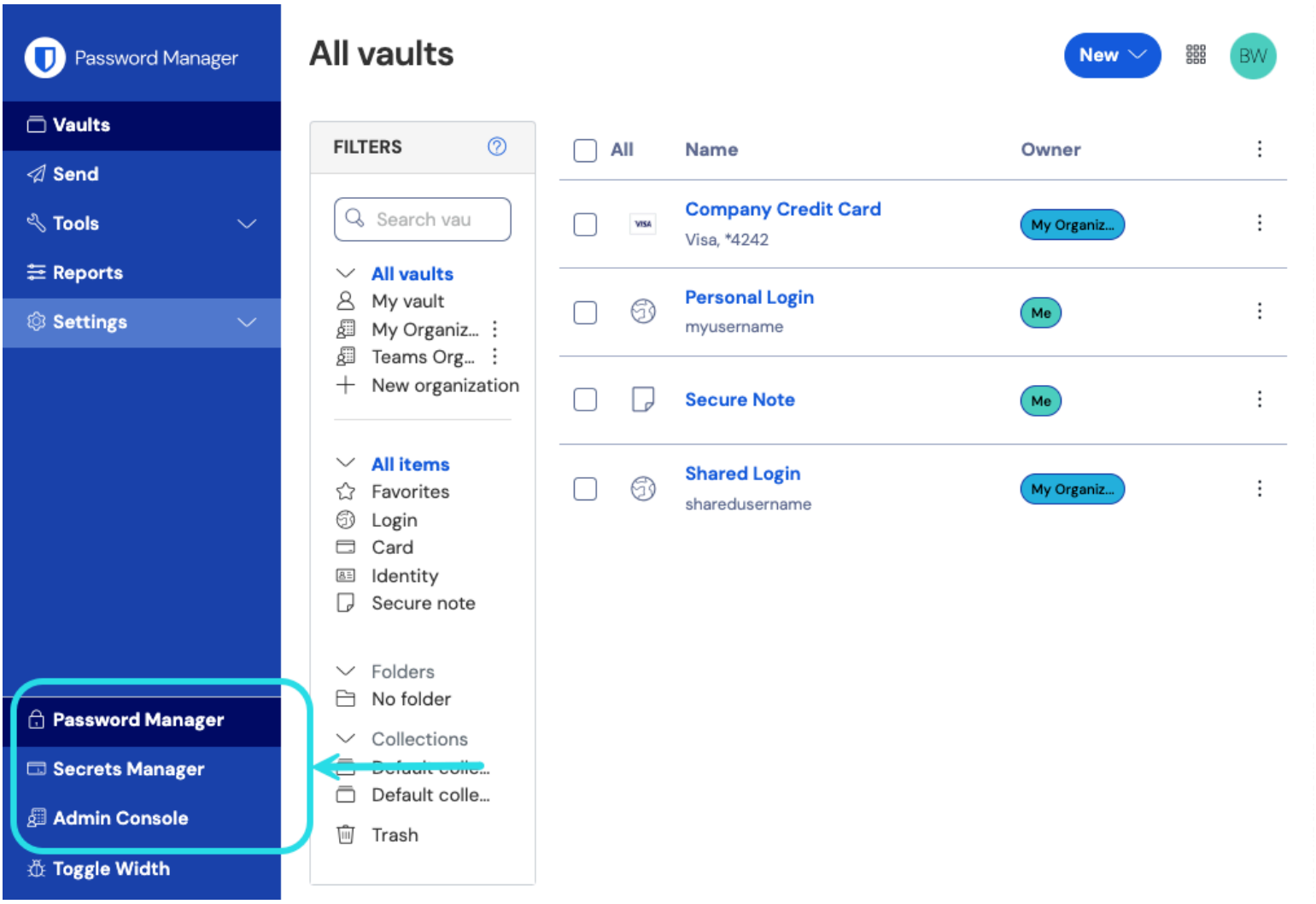
Dit artikel bevat **JumpCloud-specifieke** hulp bij het configureren van inloggen met SSO via SAML 2.0. Raadpleeg SAML 2.0 Configuratie voor hulp bij het configureren van inloggen met SSO voor een andere IdP.

Bij de configuratie wordt tegelijkertijd gewerkt in de Bitwarden-webapp en het JumpCloud-portaal. 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**
>
> **Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.
>
> Download Sample

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

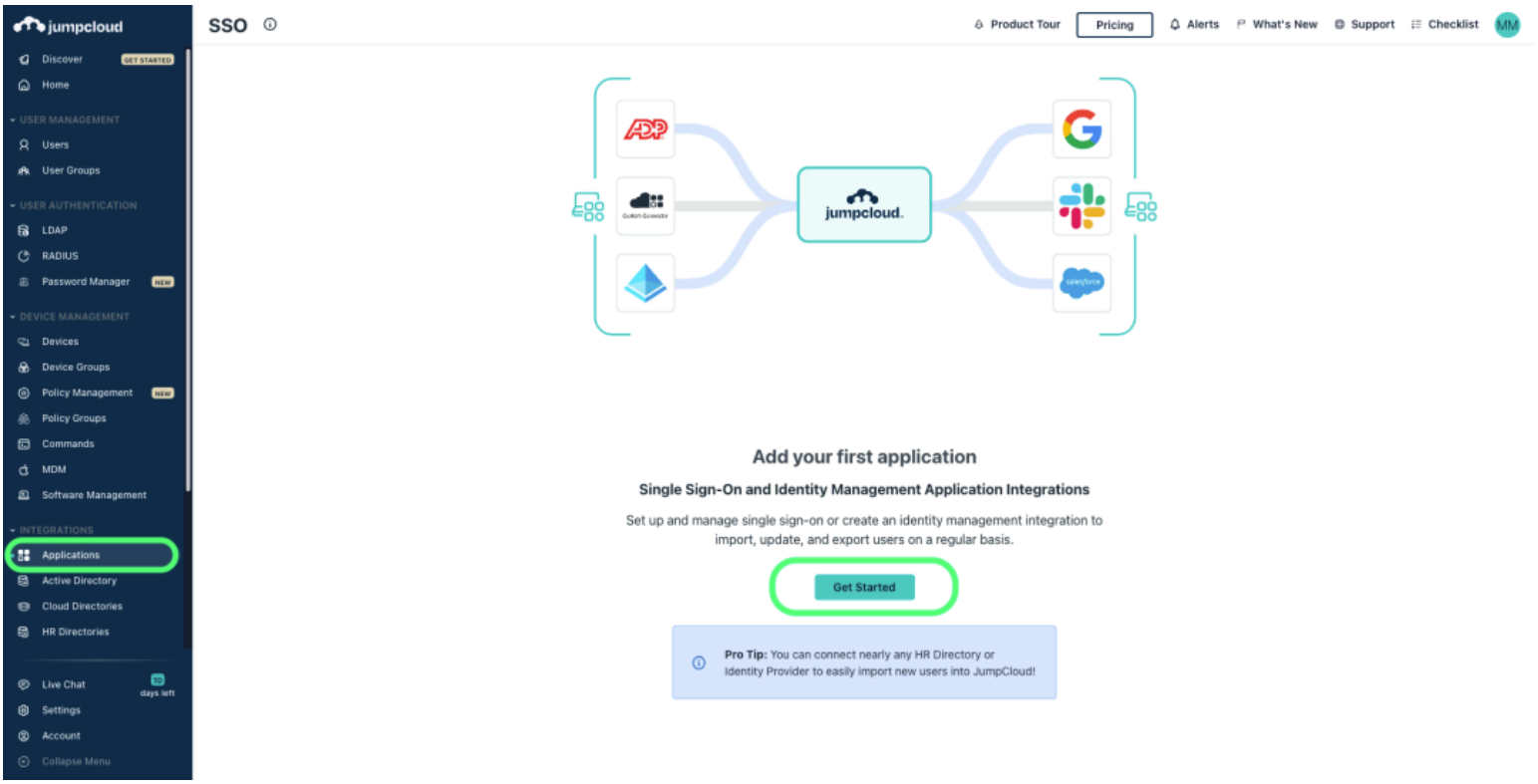
Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identifier** aan voor je organisatie en selecteer **SAML** in het keuzemenu **Type** . Houd dit scherm open voor gemakkelijke referentie.

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.

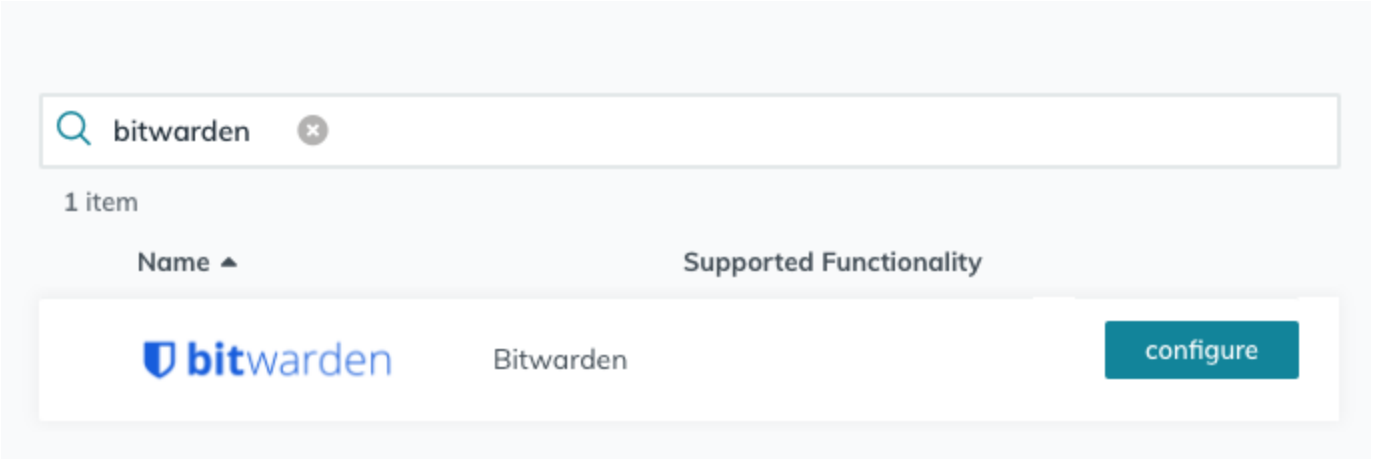
Een JumpCloud SAML-applicatie maken

Selecteer in het JumpCloud-portaal **Toepassingen** in het menu en selecteer de knop **Aan de slag**:



Create Bitwarden app Jumpcloud

Voer `Bitwarden` in het zoekvak in en selecteer de knop **Configureren**:



Configure Bitwarden

> **Tip**
>
> If you are more comfortable with SAML, or want more control over things like NameID Format and Signing Algorithms, create a **Custom SAML Application** instead.

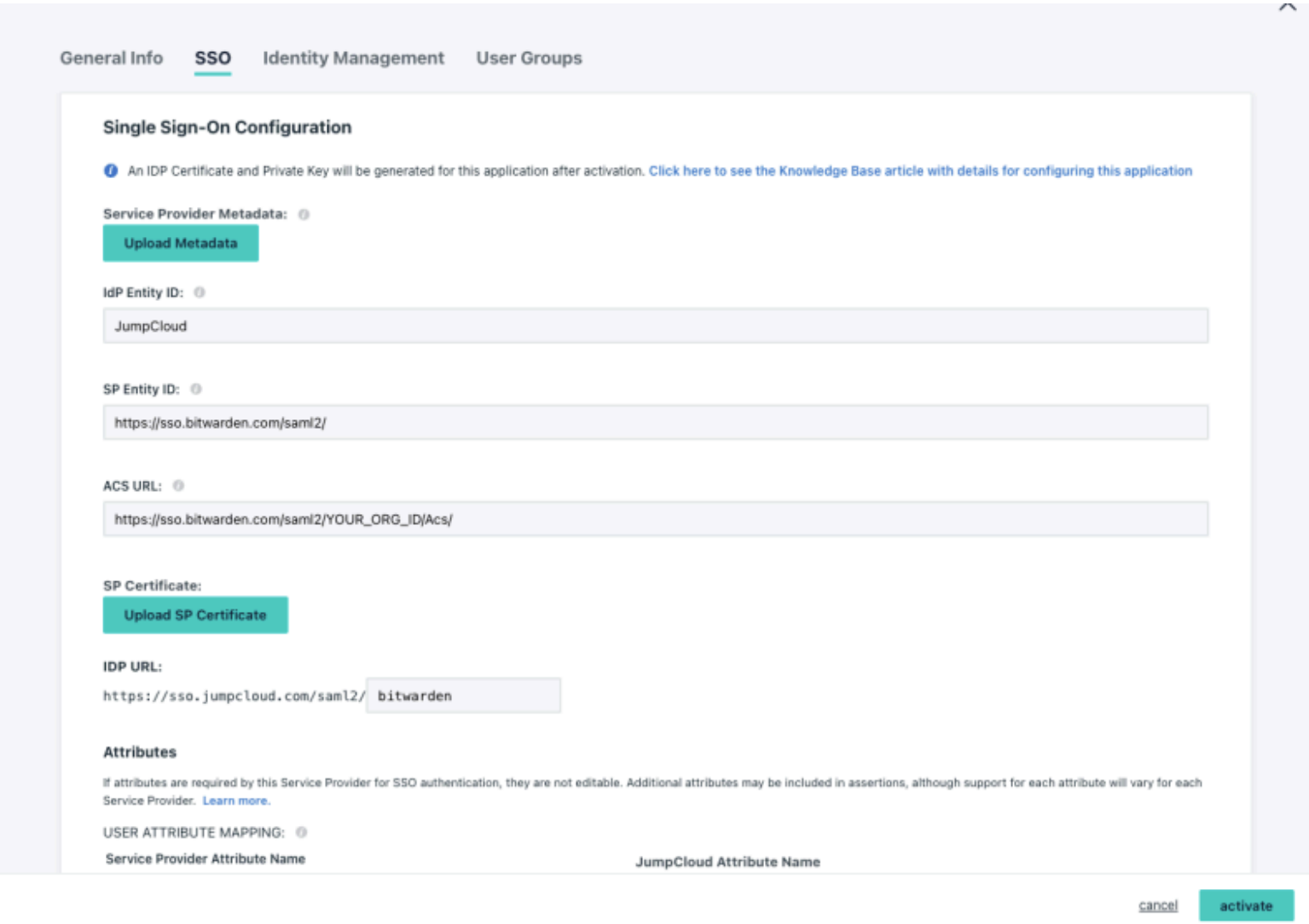
Algemene informatie

Configureer de volgende informatie in de sectie **General Info**:

Veld	Beschrijving
Label weergeven	Geef de toepassing een Bitwarden-specifieke naam.

Configuratie voor eenmalige aanmelding

Configureer de volgende informatie in het gedeelte **Single Sign-On Configuratie**:



Jumpcloud SSO configuration

Veld	Beschrijving
IdP Entiteit ID	Stel dit veld in op een unieke, Bitwarden-specifieke waarde, bijvoorbeeld `bitwardensso_uwbedrijf`.
SP entiteit 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.
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 uw instelling.

Alleen aangepaste SAML-app

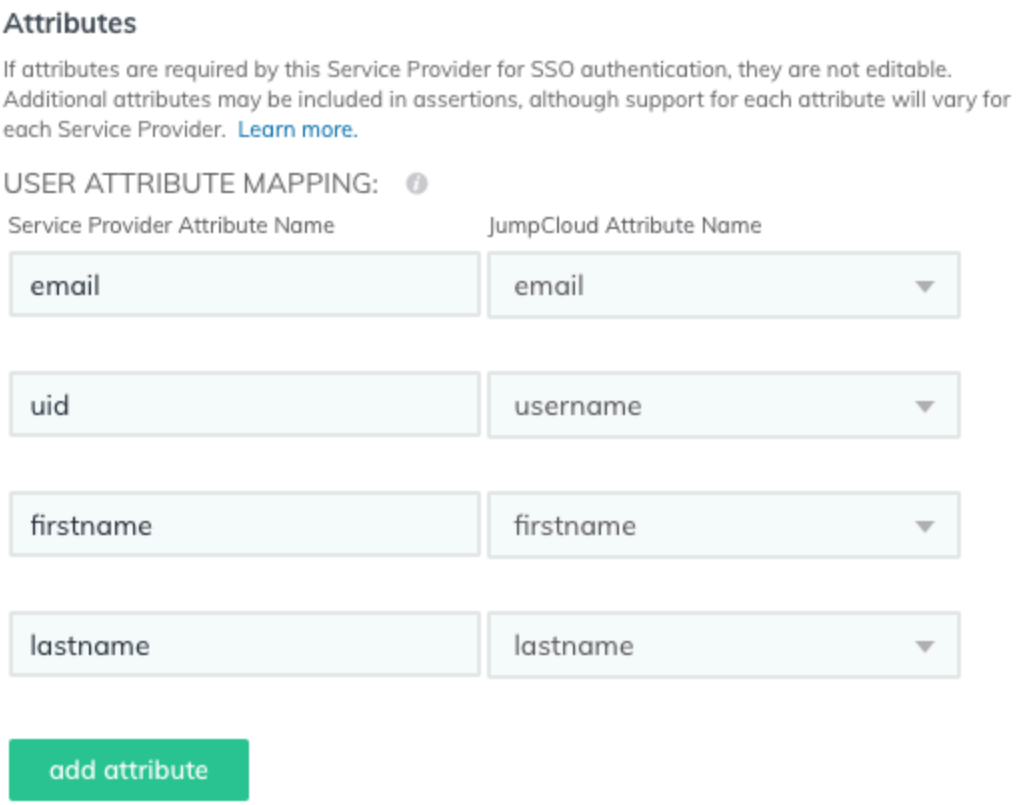
Als u een aangepaste SAML-toepassing hebt gemaakt, moet u ook de volgende velden voor **Single Sign-On configureren**:

Veld	Beschrijving
SAMLSubject NaamID	Geef het JumpCloud-attribuut op dat als NameID wordt verzonden in SAML-reacties.
SAMLSubject NaamID Formaat	Geef het formaat op van de NameID die wordt verzonden in SAML-reacties.
Handtekening algoritme	Selecteer het algoritme dat moet worden gebruikt om SAML-bevestigingen of -reacties te ondertekenen.
Tekenbevestiging	JumpCloud ondertekent standaard het SAML-antwoord. Vink dit vakje aan om de SAML-verklaring te ondertekenen.

Veld	Beschrijving
Inloggen URL	Geef de URL op vanwaar uw gebruikers inloggen op Bitwarden via SSO. 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`.

Attributen

Construeer in de **Single Sign-On Configuration** → **Attributes** sectie de volgende SP → IdP attribuutkoppelingen. Als je de Bitwarden-applicatie in JumpCloud hebt geselecteerd, zouden deze al moeten zijn gebouwd:

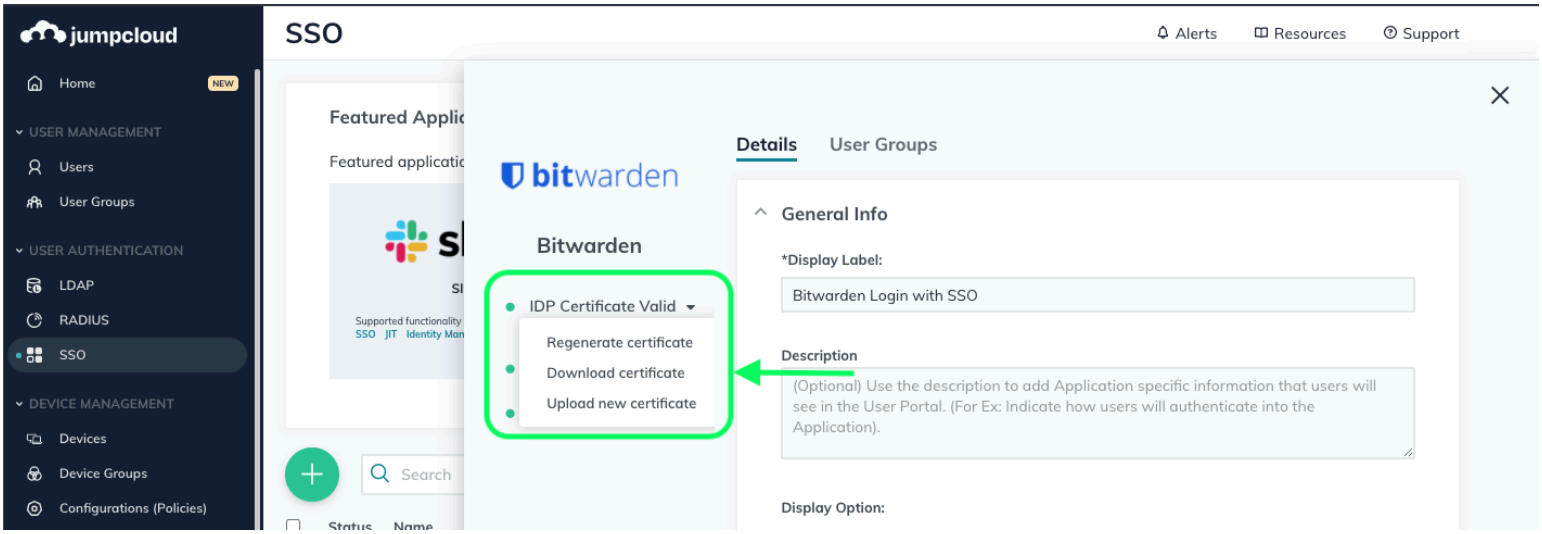


Attribute Mapping

Zodra u klaar bent, selecteert u de knop **Activeren**.

Het certificaat downloaden

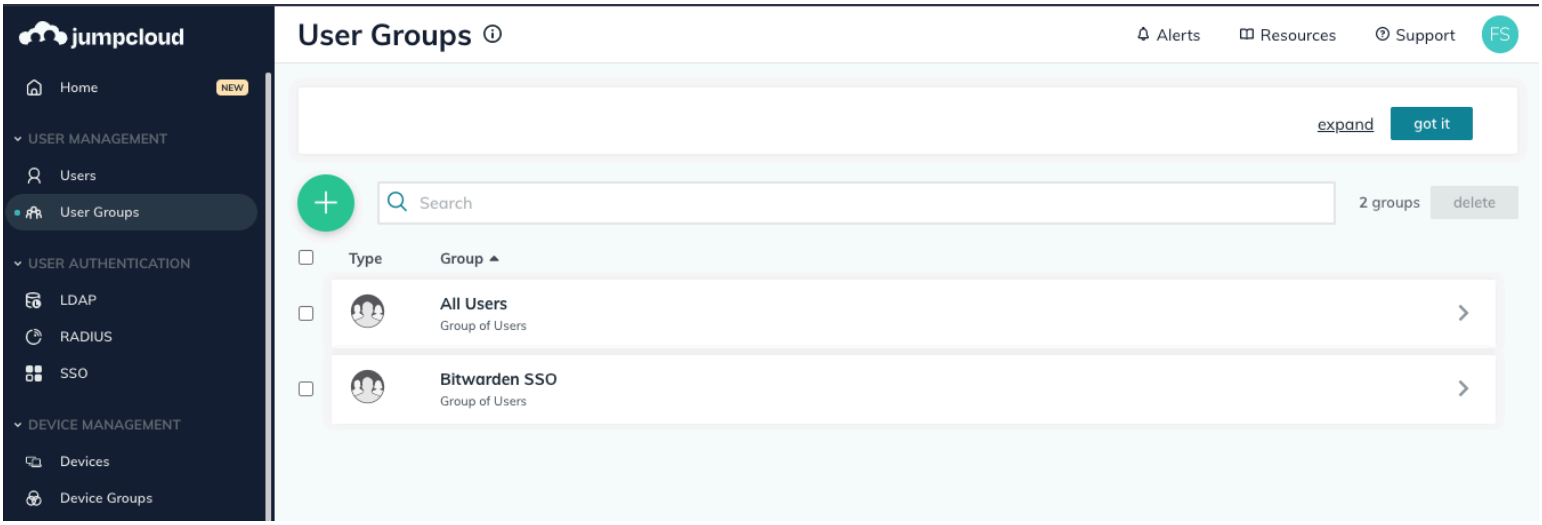
Zodra de applicatie is geactiveerd, gebruikt u opnieuw de menuoptie **SSO** om de gemaakte Bitwarden-applicatie te openen. Selecteer de vervolgkeuzelijst **IDP-certificaat** en **Download certificaat**:



Download Certificate

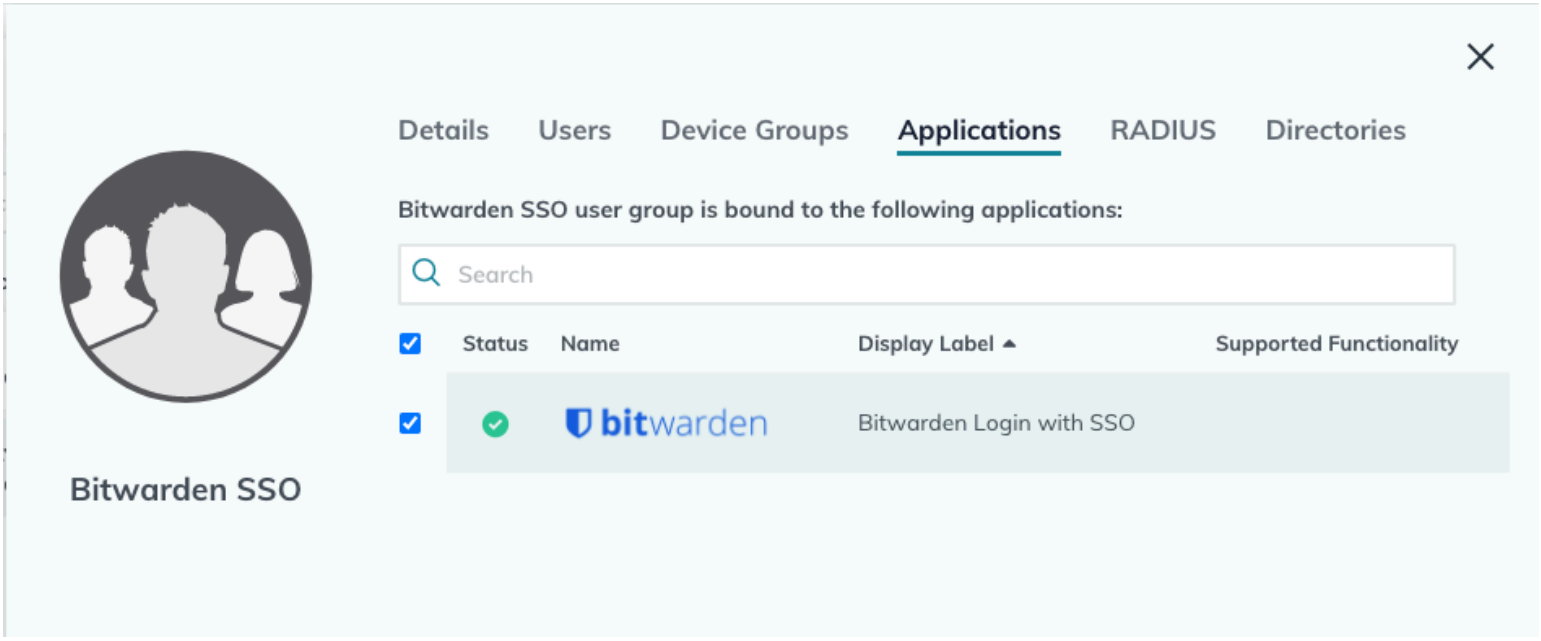
Gebruikersgroepen binden

Selecteer in het JumpCloud-portaal **Gebruikersgroepen** in het menu:



User Groups

Maak een Bitwarden-specifieke gebruikersgroep of open de standaard gebruikersgroep Alle gebruikers. In beide gevallen selecteert u het tabblad **Applicaties** en schakelt u de toegang tot de aangemaakte Bitwarden SSO-toepassing in voor die gebruikersgroep:



Bind App Access

> **Tip**
> Alternatively, you can bind access to user groups directly from the **SSO** → **Bitwarden Application** screen.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van het JumpCloud-portaal. Keer terug naar de Bitwarden-webkluis 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 volgens de keuzes die tijdens het maken van de app in het JumpCloud-portaal zijn geselecteerd:

Veld	Beschrijving
Naam ID Formaat	Als u een aangepaste SAML-toepassing hebt gemaakt, stelt u dit in op wat het opgegeven SAMLSubject NameID-formaat is. Laat anders **Unspecified** staan.
Algoritme voor uitgaande ondertekening	Het algoritme dat Bitwarden gebruikt om SAML-verzoeken te ondertekenen.

Veld	Beschrijving
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden. JumpCloud vereist standaard niet dat verzoeken worden ondertekend.
Algoritme voor minimale inkomende ondertekening	Als u een aangepaste SAML-toepassing hebt gemaakt, stelt u dit in op het handtekeningalgoritme dat u hebt geselecteerd. Laat anders `rsa-sha256` staan.
Ondertekende beweringen	Als u een aangepaste SAML-toepassing hebt gemaakt, schakelt u dit selectievakje in als u de optie **Bewijs van ondertekening** in JumpCloud hebt ingesteld. Anders niet aanvinken.
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 Identity Providers moet u vaak teruggaan naar JumpCloud Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer uw JumpCloud **IdP Entity ID** in, die u kunt ophalen uit het JumpCloud Single Sign-On Configuratiescherm. Dit veld is hoofdlettergevoelig.
Type binding	Instellen op **omleiden**.
URL voor service voor eenmalige aanmelding	Voer uw JumpCloud **IdP-URL** in, die u kunt ophalen uit het JumpCloud Single Sign-On Configuratiescherm.
URL voor service voor eenmalig afmelden	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstige ontwikkeling.

Veld	Beschrijving

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

Algoritme voor uitgaande ondertekening	Als u een aangepaste SAML-toepassing hebt gemaakt, stelt u dit in op het handtekeningalgoritme dat u hebt geselecteerd. Laat anders `rsa-sha256` staan.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of JumpCloud 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.

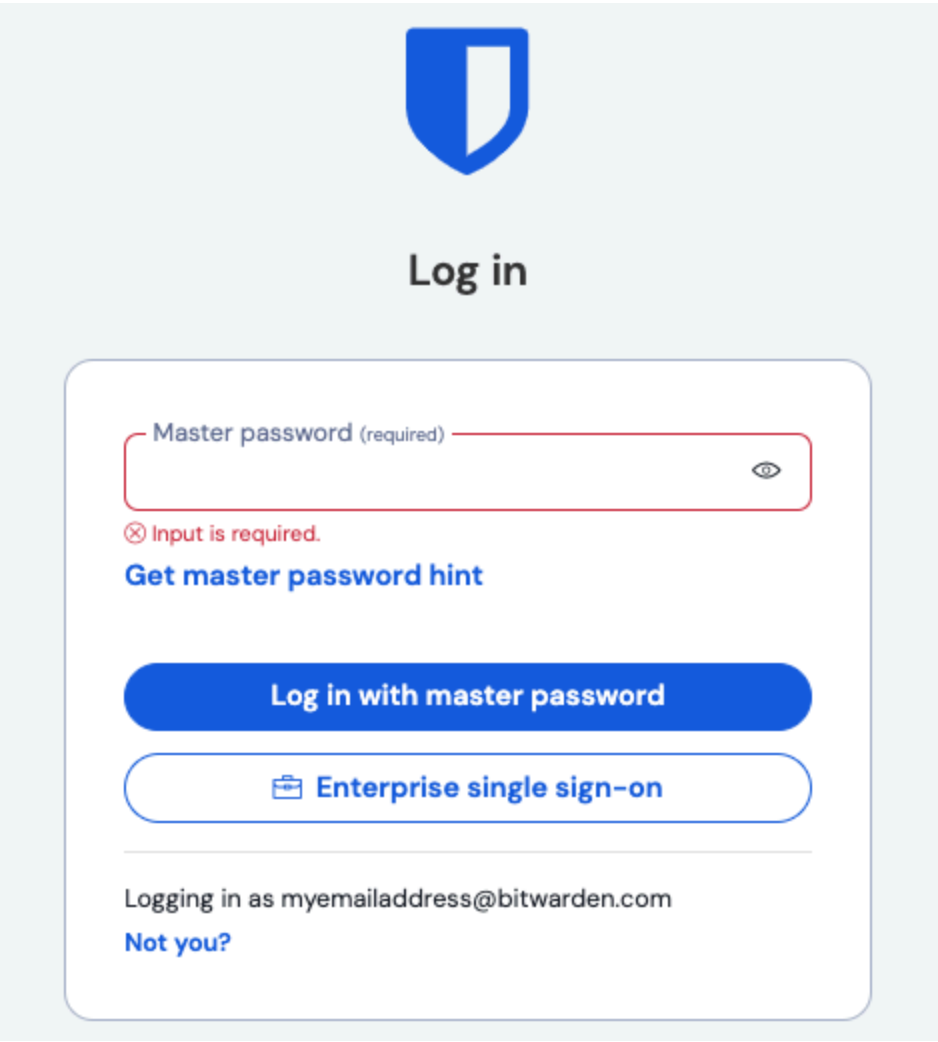
Sla uw werk **op** wanneer u klaar bent met de configuratie van de identity provider.

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.

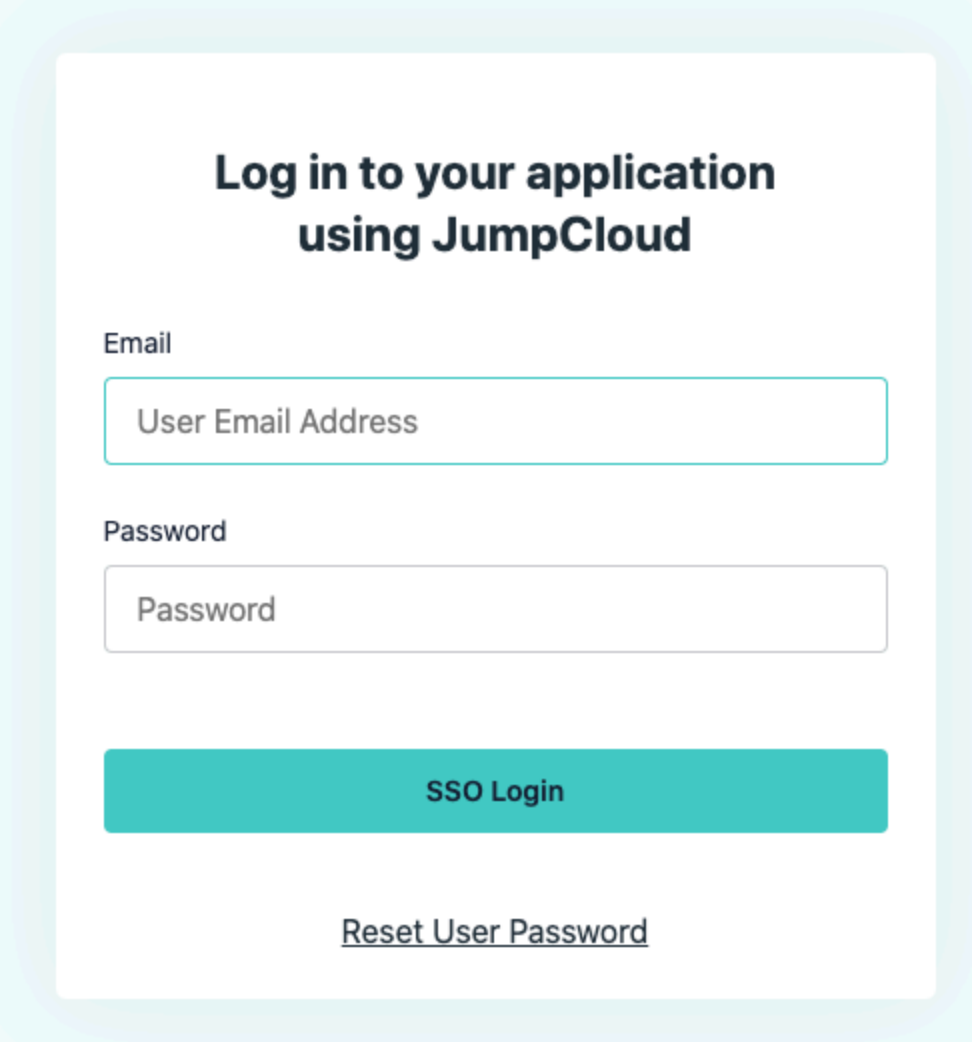
De configuratie testen

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 JumpCloud inlogscherm:



JumpCloud Login

Nadat u zich hebt geverifieerd met uw JumpCloud-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.