Okta SAML-implementatie

Okta SAML-implementatie

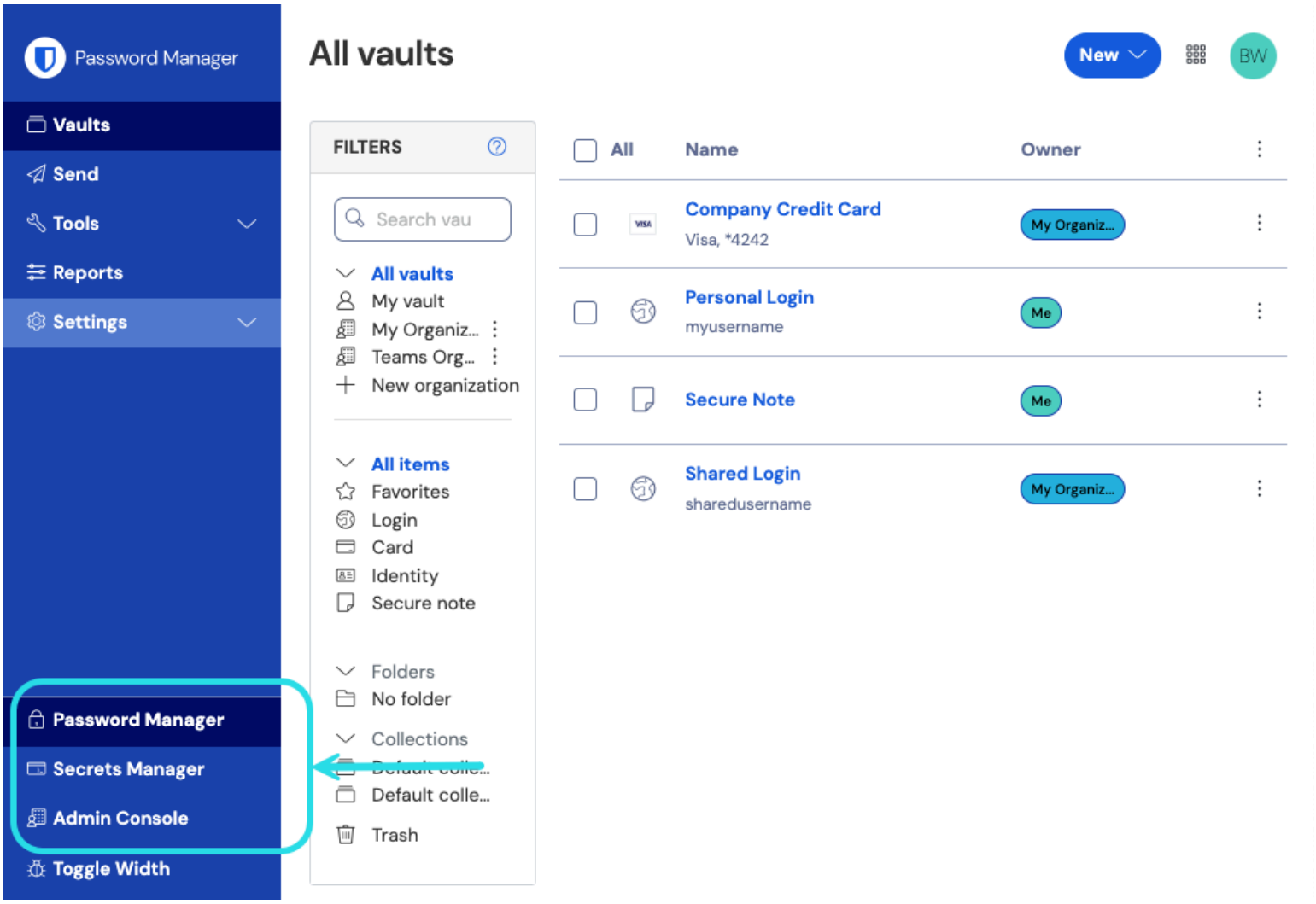
Dit artikel bevat **Okta-specifieke** hulp voor het configureren van Inloggen met SSO via SAML 2.0. Raadpleeg SAML 2.0 Configuratie voor hulp bij het configureren van inloggen met SSO voor een andere IdP.

Bij de configuratie wordt tegelijkertijd gewerkt binnen de Bitwarden-webapp en het Okta Admin 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**
>
> **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

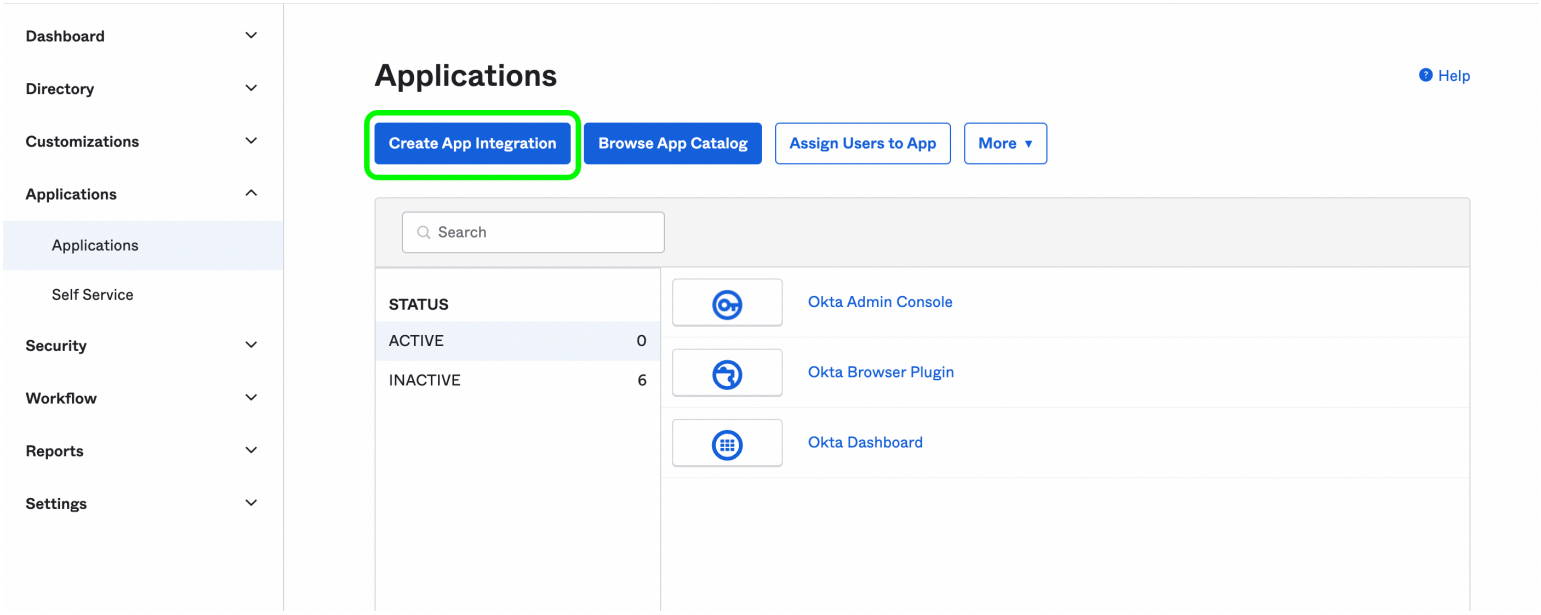
Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identifier** aan voor je organisatie en selecteer **SAML** in het keuzemenu **Type** . Houd dit scherm open voor gemakkelijke referentie.

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.

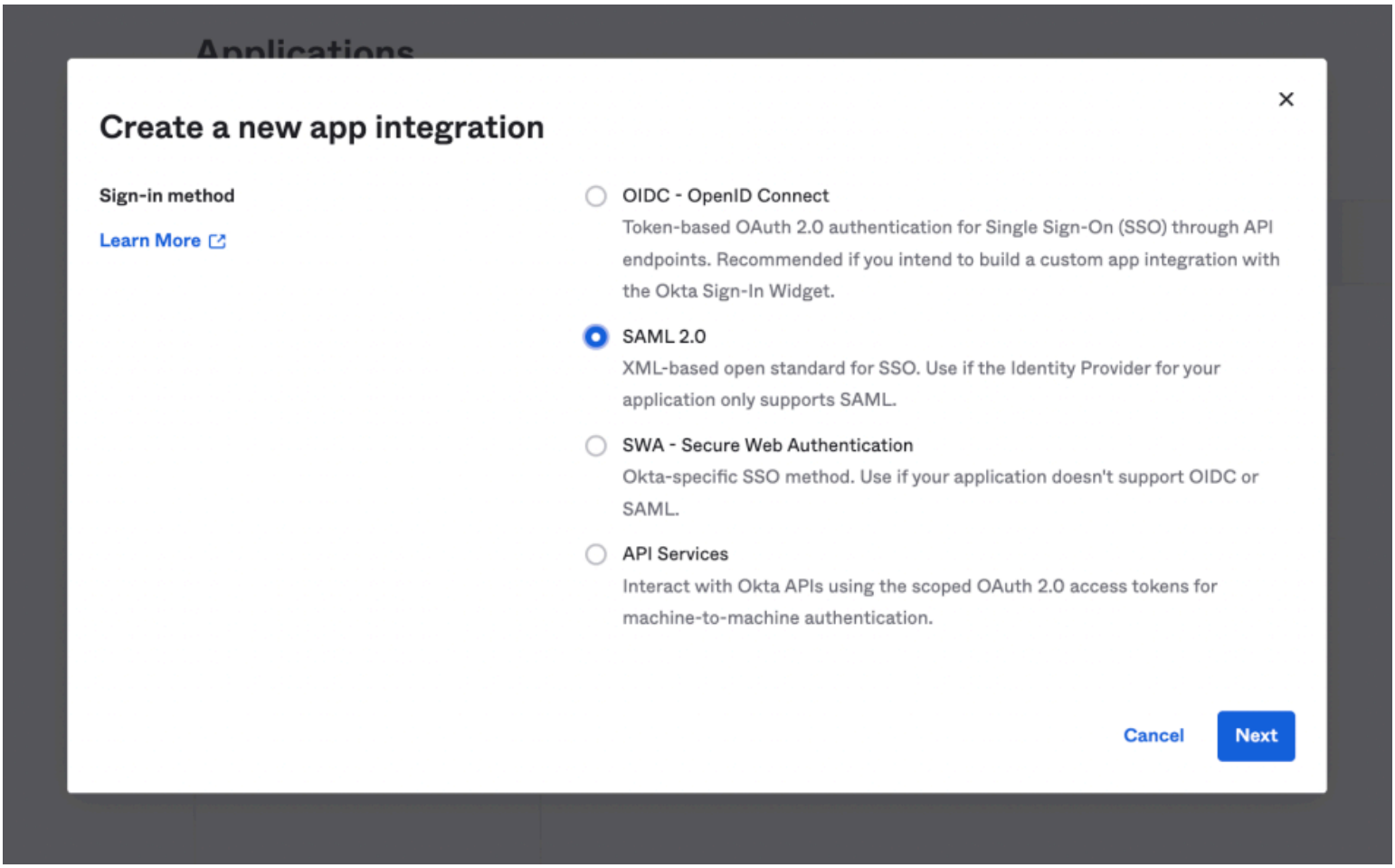
Een Okta-applicatie maken

Selecteer in het Okta Admin Portal **Applicaties → Applicaties** in de navigatie. Selecteer in het scherm Toepassingen de knop **Appintegratie maken**:



Okta create app integration

Selecteer het keuzerondje **SAML 2.0** in het dialoogvenster Nieuwe applicatie-integratie maken:



SAML 2.0 radio button

Selecteer de knop **Volgende** om verder te gaan met de configuratie.

Algemene instellingen

Geef de applicatie in het scherm **Algemene instellingen** een unieke, Bitwarden-specifieke naam en selecteer **Volgende**.

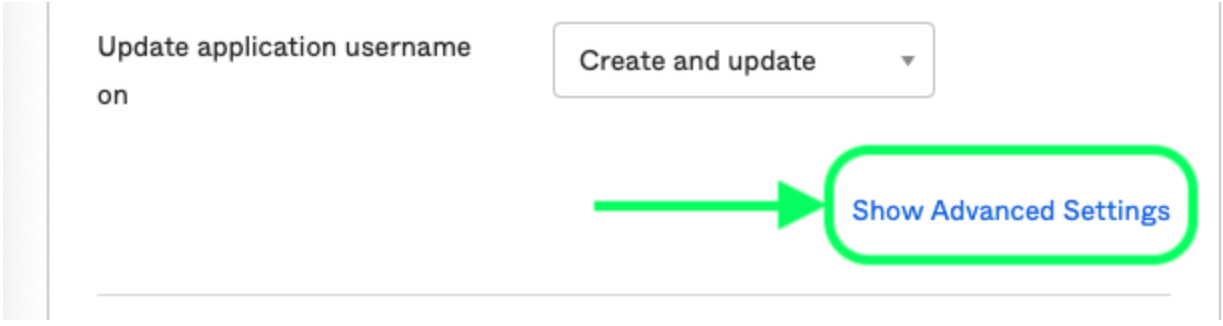
SAML configureren

Configureer de volgende velden in het scherm **Configureer SAML**:

Veld	Beschrijving
URL voor eenmalige aanmelding	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 → Eenmalige aanmelding** scherm van de organisatie en zal variëren afhankelijk van je instelling.
Audience URI (SP entiteit ID)	Stel dit veld in op de vooraf gegenereerde **SP entiteit ID**. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen → Eenmalige aanmelding** scherm van de organisatie en zal variëren afhankelijk van je instelling.
Naam ID-indeling	Selecteer de SAML NameID-indeling om te gebruiken in SAML-bevestigingen. Standaard **Niet gespecificeerd**.
Gebruikersnaam sollicitatie	Selecteer het Okta-attribuut waarmee gebruikers zich aanmelden bij Bitwarden.

Geavanceerde instellingen

Selecteer de link **Geavanceerde instellingen weergeven** en configureer de volgende velden:

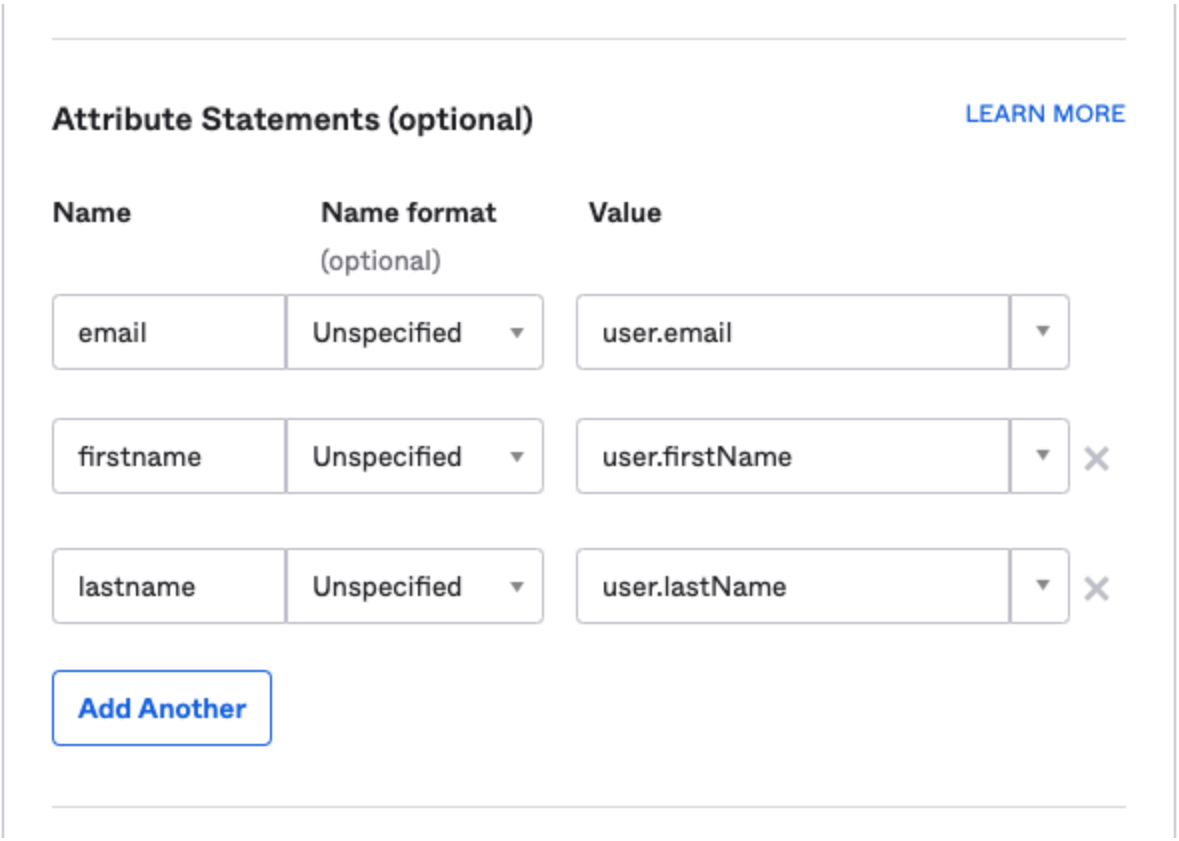


Advanced Settings

Veld	Beschrijving
Reactie	Of het SAML-antwoord is ondertekend door Okta.
Handtekening	Of de SAML assertion is ondertekend door Okta.
Handtekening algoritme	Het ondertekeningsalgoritme dat wordt gebruikt om het antwoord en/of de bewering te ondertekenen, afhankelijk van welke is ingesteld op **Ondertekend**. Standaard is dit `rsa-sha256`.
Digest-algoritme	Het digest-algoritme dat wordt gebruikt om het antwoord en/of de bewering te ondertekenen, afhankelijk van welke is ingesteld op **Ondertekend**. Dit veld moet overeenkomen met het geselecteerde **handtekeningalgoritme**.

Attribuutverklaringen

Construeer in de sectie **Attribute Statements** de volgende SP → IdP attribuutkoppelingen:

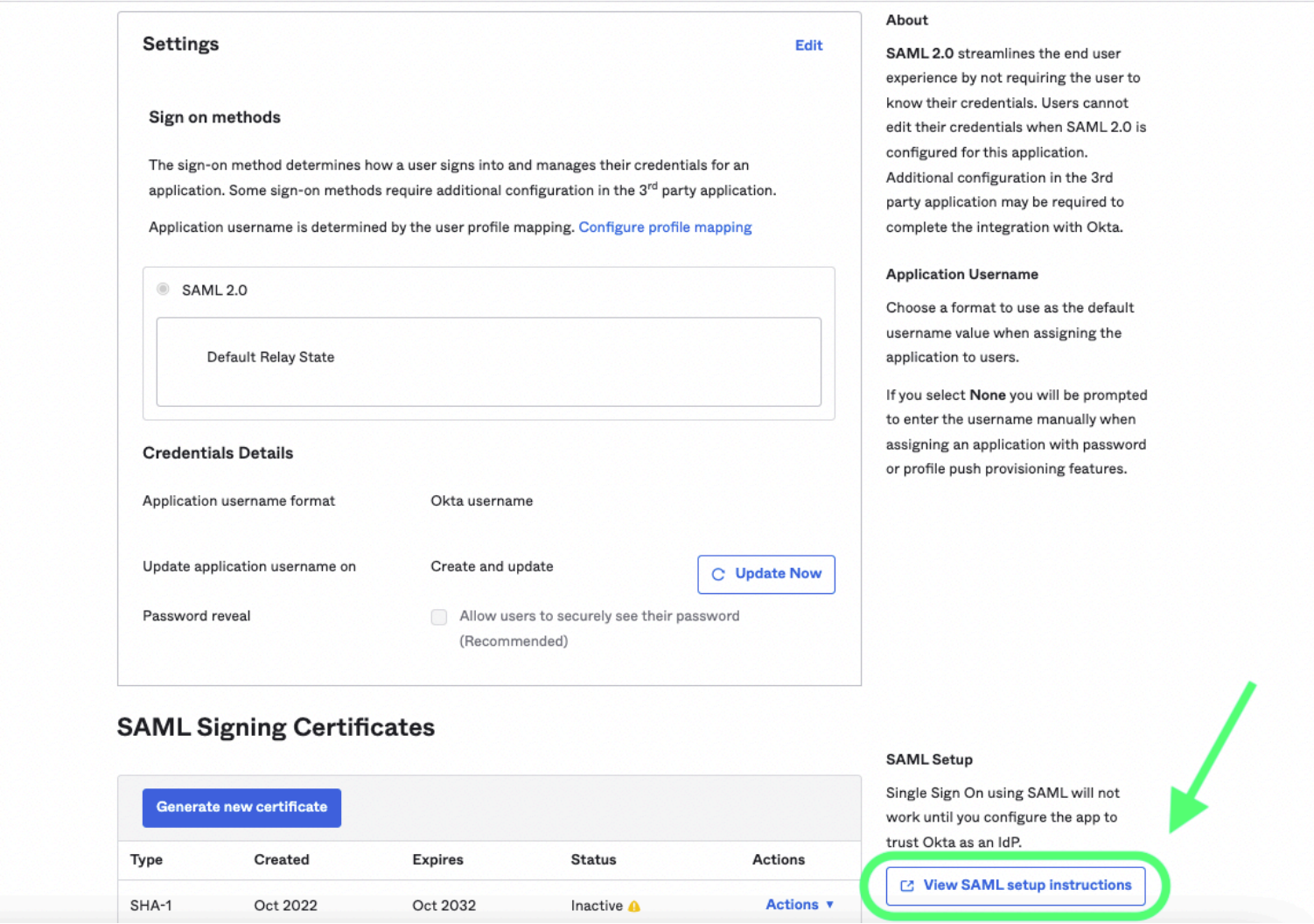


Attribute Statements

Selecteer na de configuratie de knop **Volgende** om door te gaan naar het **Feedbackscherm** en selecteer **Voltooien**.

IdP-waarden ophalen

Zodra je applicatie is gemaakt, selecteer je het tabblad **Aanmelden** voor de app en selecteer je de knop **Instellingsinstructies bekijken** aan de rechterkant van het scherm:



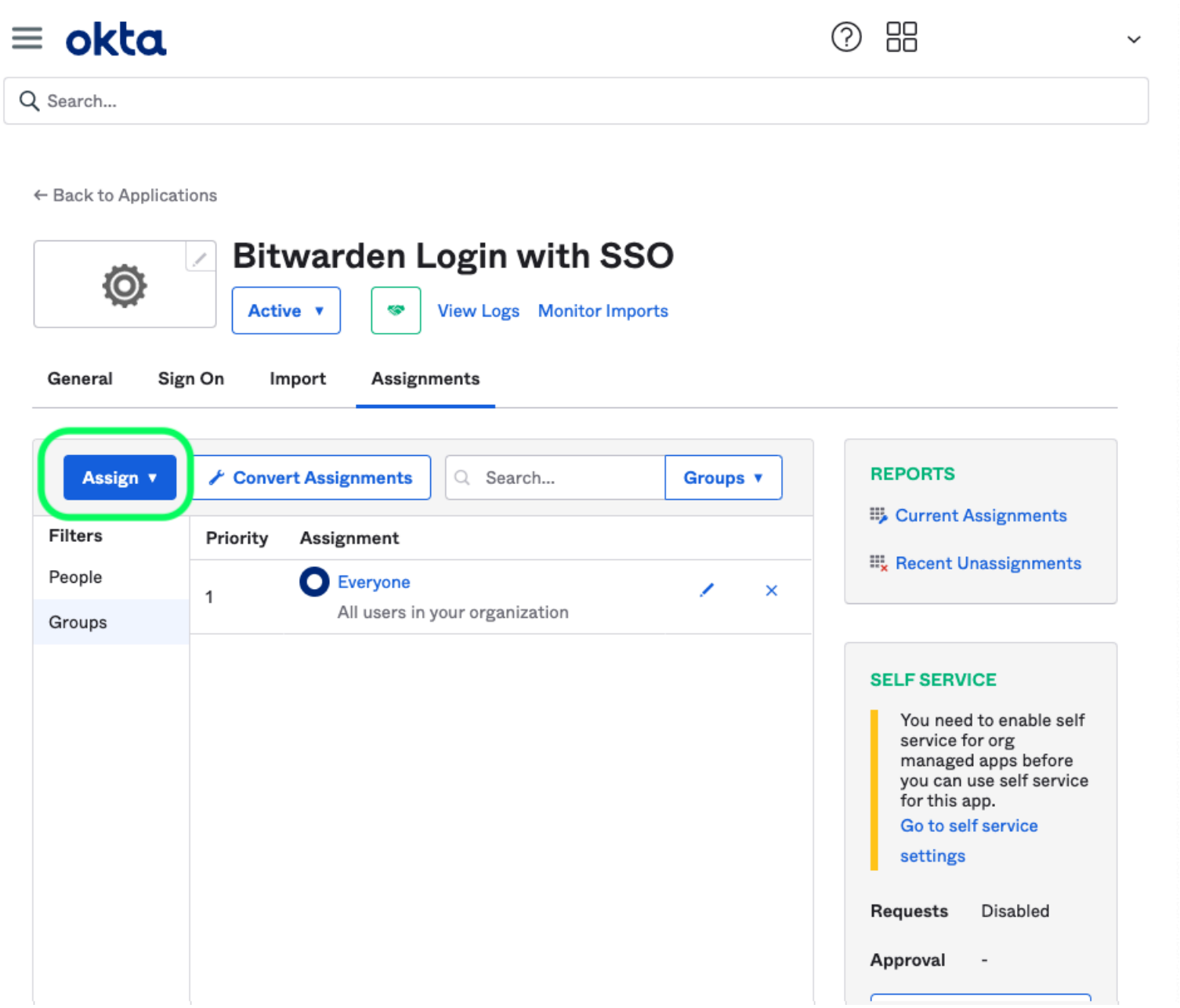
View SAML setup instructions

Laat deze pagina open voor toekomstig gebruik of kopieer de **Identity Provider Single Sign-On URL** en **Identity Provider Issuer** en download het **X.509 Certificaat**:

IdP Values

Opdrachten

Navigeer naar het tabblad **Toewijzingen** en selecteer de knop **Toewijzen**:



Assigning Groups

Je kunt toegang tot de applicatie per gebruiker toewijzen met de optie **Aan personen toewijzen**, of in één keer met de optie **Aan groepen toewijzen**.

Terug naar de webapp

Op dit punt hebt u alles geconfigureerd wat u nodig hebt binnen de context van het Okta Admin 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 volgens de keuzes die zijn geselecteerd in het Okta Admin Portal tijdens het maken van de app:

Veld	Beschrijving
Naam ID Formaat	Stel dit in op het Name ID-formaat dat is opgegeven in Okta, laat anders **Unspecified** staan.
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	Stel dit in op het handtekeningalgoritme dat is opgegeven in Okta.
Ondertekende beweringen	Schakel dit selectievakje in als u het veld Assertion Signature hebt ingesteld op **Signed** in Okta.
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 identiteitsaanbieders moet u vaak teruggaan naar het Okta Admin Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer uw **Identity Provider Issuer** in, opgehaald uit het Okta Sign On Settings-scherm door de knop **View Setup Instructions** te selecteren. Dit veld is hoofdlettergevoelig.
Type binding	Instellen op **omleiden**. Okta ondersteunt momenteel geen HTTP POST.

Veld	Beschrijving
URL voor service voor eenmalige aanmelding	Voer uw **Identity Provider Single Sign-On URL** in, opgehaald uit het Okta Sign On Settings-scherm.
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.

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 certificatievalidatie mislukt**.

Algoritme voor uitgaande ondertekening	Selecteer het handtekeningalgoritme dat is geselecteerd tijdens de configuratie van de Okta-app. Als u het handtekeningalgoritme niet hebt gewijzigd, laat u de standaardwaarde (`rsa-sha256`) staan.
Uitgaande afmeldverzoeken toestaan	Inloggen met SSO ondersteunt momenteel **geen** SLO.
Authenticatieverzoeken ondertekend willen hebben	Of Okta verwacht dat SAML-verzoeken worden ondertekend.

Note

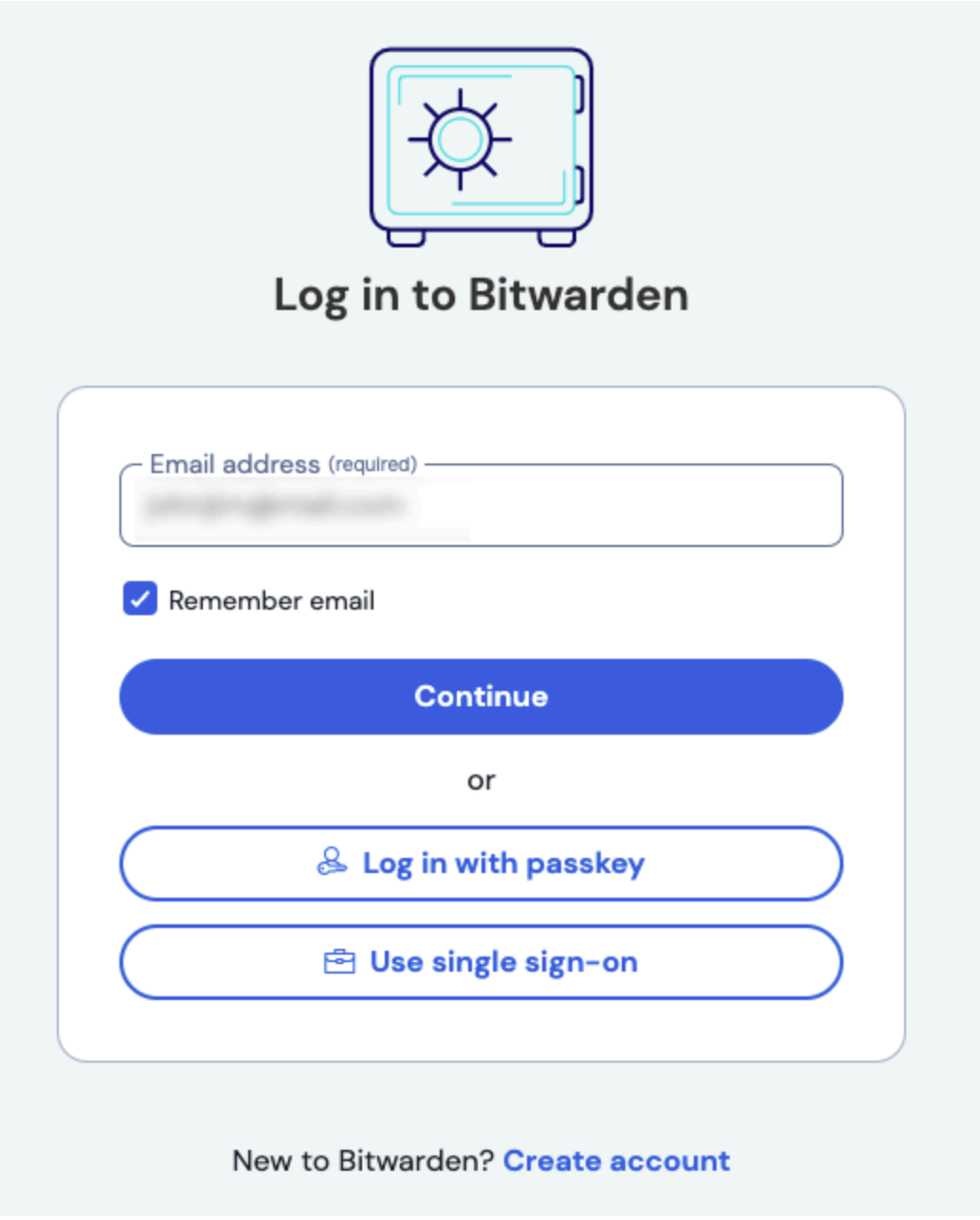
Let bij het invullen van het X509-certificaat op de vervaldatum. Certificaten zullen vernieuwd moeten worden om onderbrekingen in de dienstverlening aan SSO eindgebruikers te voorkomen. Als een certificaat is verlopen, kunnen de accounts Admin en Eigenaar altijd inloggen met e-mailadres en hoofdwachtwoord.

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

> **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.

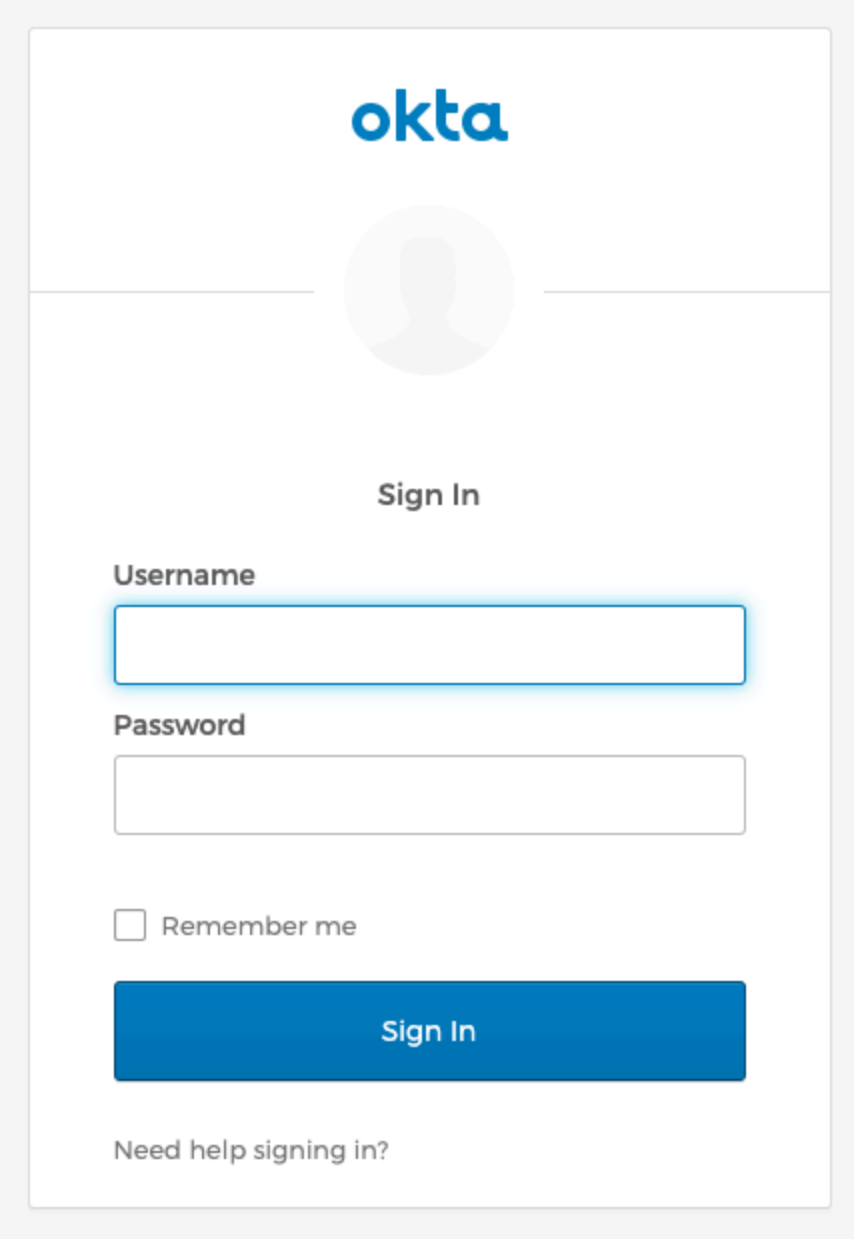
De configuratie testen

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 inlogscherm voor Okta:



Log in with Okta

Nadat u zich hebt geverifieerd met uw Okta-referenties, voert u uw Bitwarden-masterwachtwoord in om uw kluis te ontsleutelen!

Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an Okta Bookmark App that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
    1. Give the application a name such as **Bitwarden Login**.
    2. In the **URL** field, provide the URL to your Bitwarden client such as `https://vault.bitwarden.com/#/login` or `your-self-hostedURL.com`.
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained here.

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.