Duo SAML implementatie

Duo SAML implementatie

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

Bij de configuratie wordt gelijktijdig gewerkt tussen de Bitwarden webapp en het Duo Admin 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.

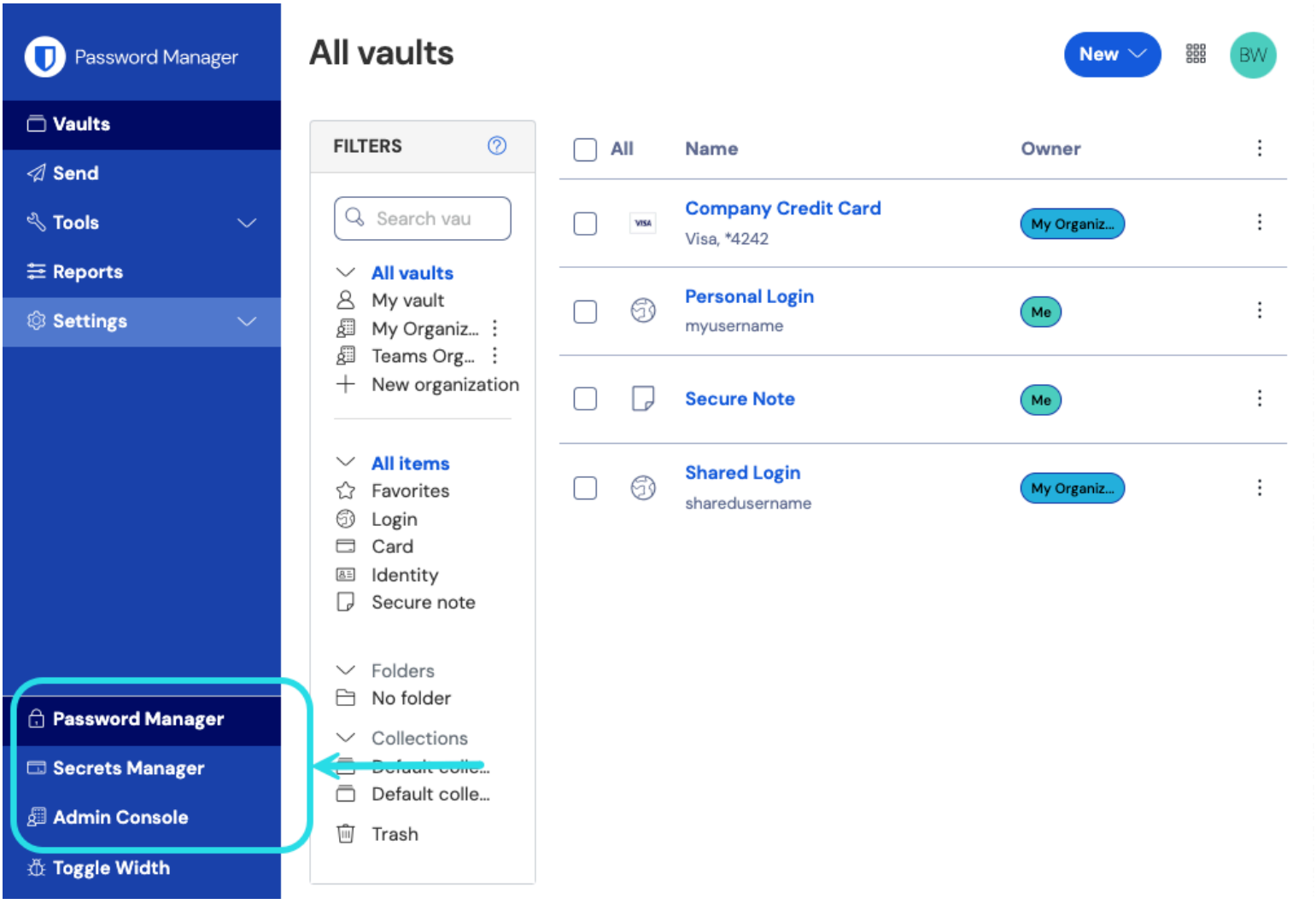
Download Sample

Open SSO in de webapp

Warning

This article assumes that you have already set up Duo with an Identity Provider. If you haven't, see Duo's documentation for details.

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.

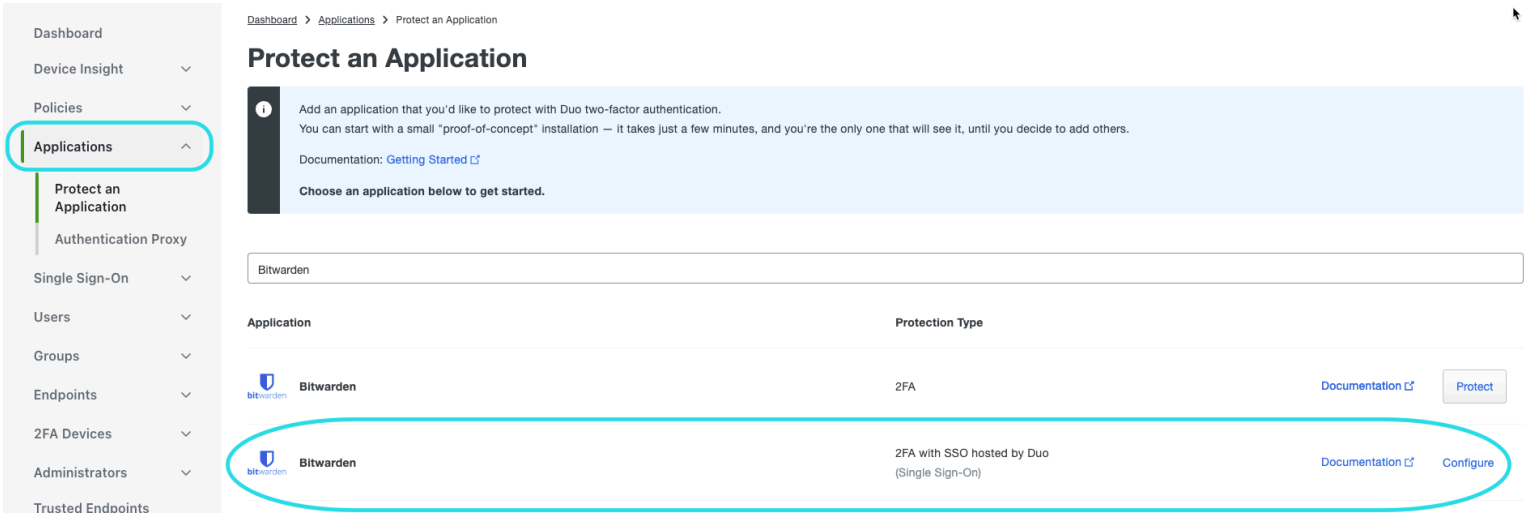
U kunt de optie **Een unieke SP entiteit ID instellen** in dit stadium uitschakelen als u dat wilt. Als u dit doet, wordt uw organisatie-ID verwijderd uit uw SP entiteit-ID waarde, maar in bijna alle gevallen is het aan te raden om deze optie aan te laten staan.

> **Tip**
>
> Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met SSO met vertrouwde apparaten of Key Connector.

Een toepassing beschermen

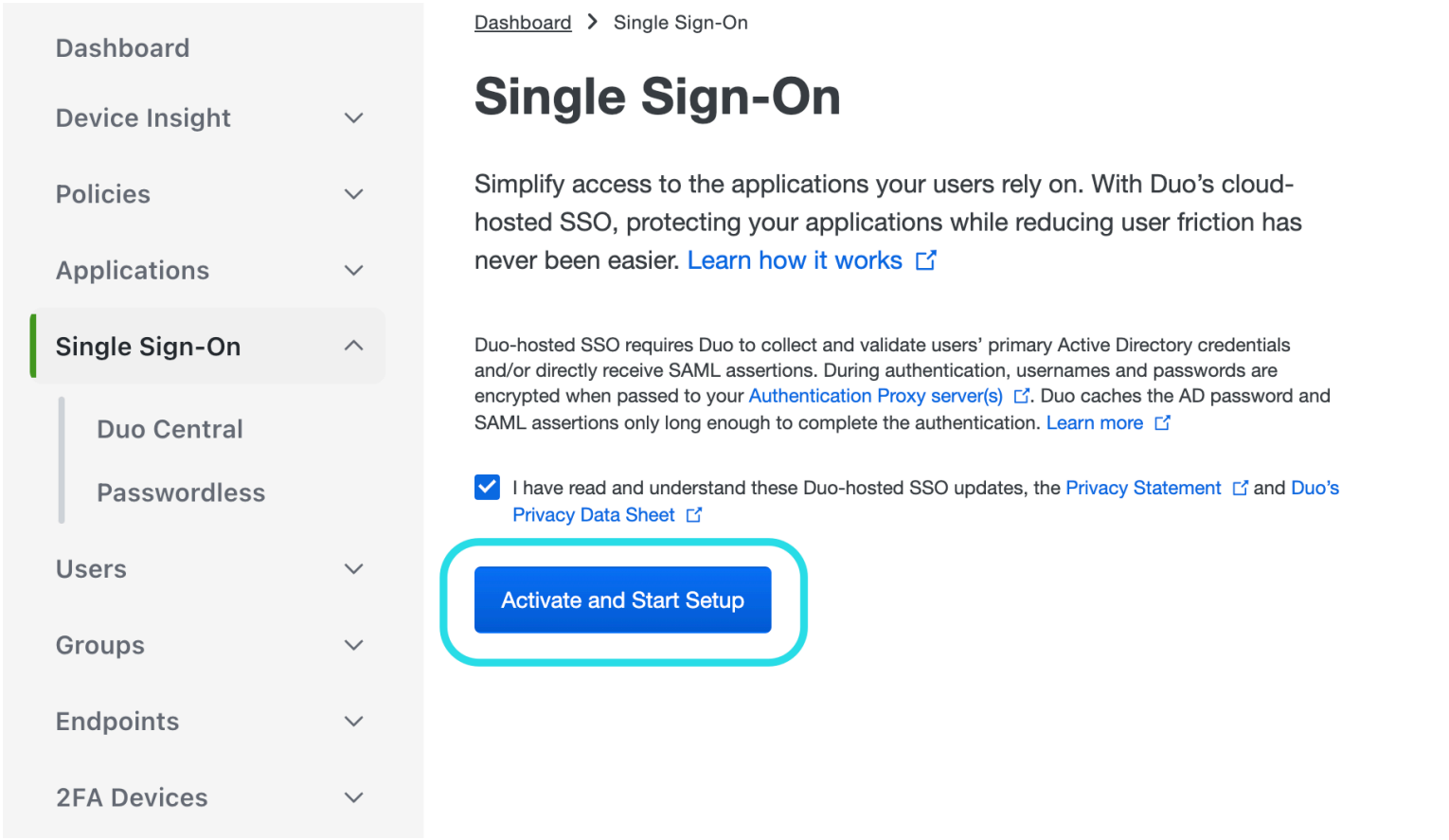
Raadpleeg voordat u verdergaat de documentatie van Duo om te controleren of Duo Single Sign-On is geconfigureerd met uw SAML-identiteitsprovider voor verificatie.

Navigeer in het Duo Admin Portal naar het scherm **Toepassingen** en selecteer **Bescherm een toepassing**. Voer **Bitwarden** in de zoekbalk in en selecteer **Configureren** voor de **Bitwarden 2FA met SSO gehost door Duo** toepassing:



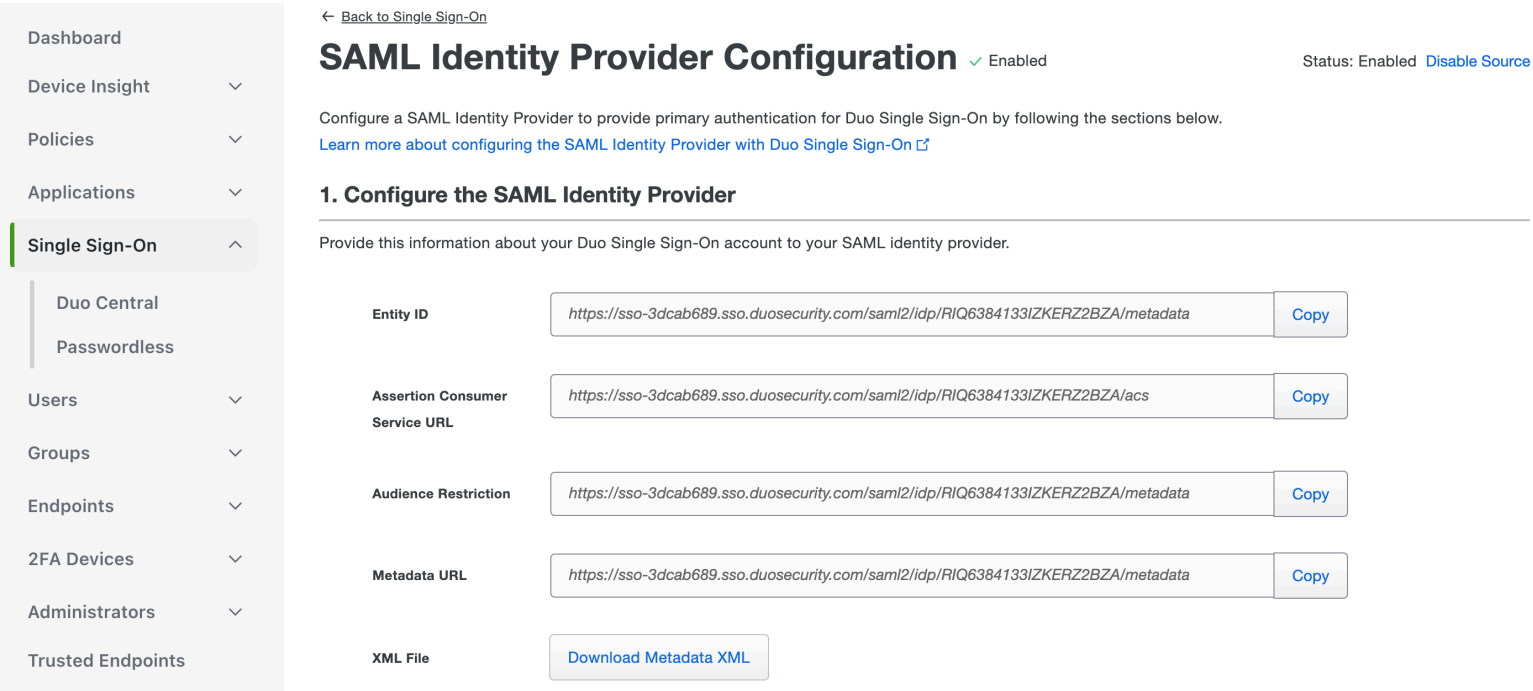
Duo Bitwarden Application

Selecteer **Activeren en Setup starten** voor de nieuw aangemaakte applicatie:



Duo Activation and Setup

Voltooi de volgende stappen en configuraties in het scherm Applicatieconfiguratie, waarvan u sommige moet ophalen uit het Bitwarden single sign-on scherm:



DUO SAML Identity Provider Configuration

Metagegevens

Je hoeft niets te bewerken in het gedeelte **Metadata**, maar je zult deze waarden later wel moeten gebruiken:

URLs for Configuration

Downloads

Selecteer de knop **Certificaat downloaden** om uw X.509-certificaat te downloaden, omdat u dit later in de configuratie moet gebruiken.

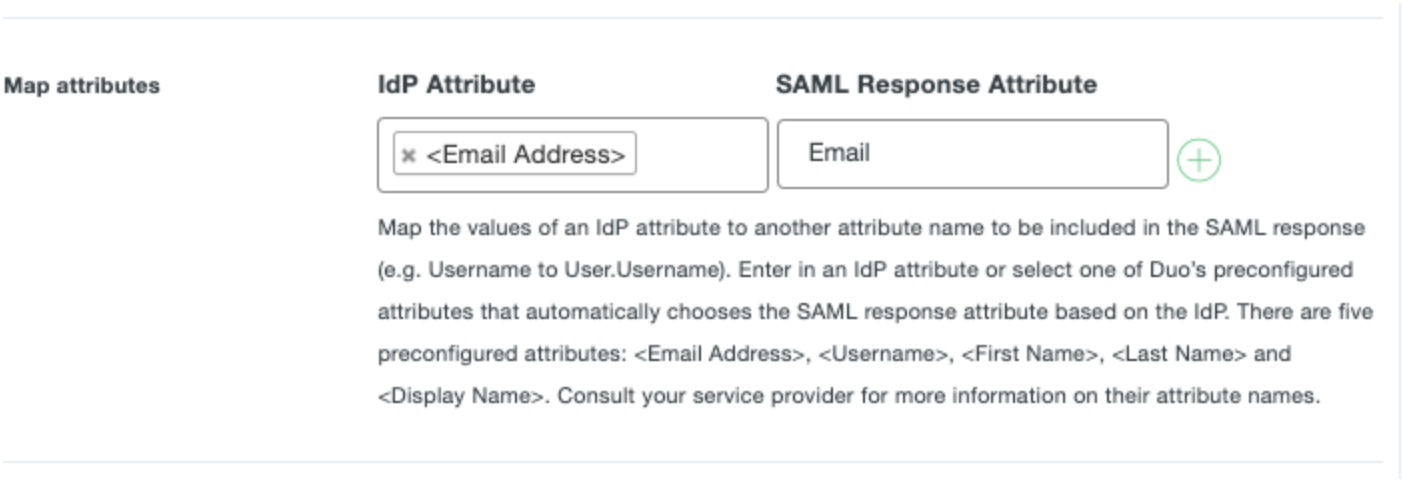
Dienstverlener

Veld	Beschrijving
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 je instelling.

Veld	Beschrijving
URL Assertion Consumentenservice (ACS)	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.
Aanmeldings-URL serviceprovider	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`.

SAML antwoord

Veld	Beschrijving
Formaat NameID	Stel dit veld in op de SAML NameID-indeling zodat Duo deze kan verzenden in SAML-reacties.
NameID attribuut	Stel dit veld in op het Duo-attribuut dat de NameID in reacties zal invullen.
Handtekening algoritme	Stel dit veld in op het coderingsalgoritme dat moet worden gebruikt voor SAML-bevestigingen en -reacties.
Opties voor ondertekening	Selecteer of u **een antwoord wilt ondertekenen**, **een bewering wilt ondertekenen** of beide.
Kenmerken kaart	Gebruik deze velden om IdP-attributen toe te wijzen aan SAML-responsattributen. Ongeacht welk NameID attribuut je hebt geconfigureerd, koppel het IdP `Email Address` attribuut aan `Email`, zoals in de volgende schermafbeelding:



Required Attribute Mapping

Sla je wijzigingen **op** als je klaar bent met het configureren van deze velden.

Terug naar de webapp

Op dit punt hebt u alles geconfigureerd wat u nodig hebt binnen de context van Duo 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 Duo Admin Portal tijdens het instellen van de applicatie:

Veld	Beschrijving
Naam ID Formaat	NameID-formaat om te gebruiken in het SAML-verzoek (`NameIDPolicy`). Stel dit veld in op de geselecteerde NameID-indeling.
Algoritme voor uitgaande ondertekening	Algoritme dat wordt gebruikt om SAML-verzoeken te ondertekenen, standaard `rsa-sha256`.
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden. Duo vereist standaard niet dat verzoeken worden ondertekend.

Veld	Beschrijving
Algoritme voor minimale inkomende ondertekening	Het minimale ondertekeningsalgoritme dat Bitwarden accepteert in SAML-reacties. Duo ondertekent standaard met `rsa-sha256`, dus kies die optie uit de vervolgkeuzelijst tenzij u een andere optie hebt geselecteerd.
Ondertekende beweringen	Of Bitwarden SAML-asserties ondertekend wil hebben. Vink dit vakje aan als je de optie Assertie ondertekenen hebt geselecteerd.
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

Identity provider configuratie vereist vaak dat u teruggaat naar het Duo Admin Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer de **Entity ID-waarde** van uw Duo-applicatie in, die u kunt vinden in de sectie Metadata van de Duo-app. Dit veld is hoofdlettergevoelig.
Type binding	Stel dit veld in op **HTTP Post**.
URL voor service voor eenmalige aanmelding	Voer de **Single Sign-On URL-waarde** van uw Duo-applicatie in, die kan worden opgehaald uit de Duo app Metadata sectie.
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 **Single Log-Out URL-waarde** van uw Duo-applicatie.
X509 publiek certificaat	Plak het gedownloade certificaat, verwijder `-----BEGIN CERTIFICAAT-----` en

Veld	Beschrijving
	`-----END CERTIFICAAT-----` De certificaatwaarde is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens zorgen ervoor dat **de certificatievalidatie mislukt**.
Algoritme voor uitgaande ondertekening	Stel dit veld in op het geselecteerde SAML Response handtekeningalgoritme.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of Duo verwacht dat SAML verzoeken ondertekend worden.

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.

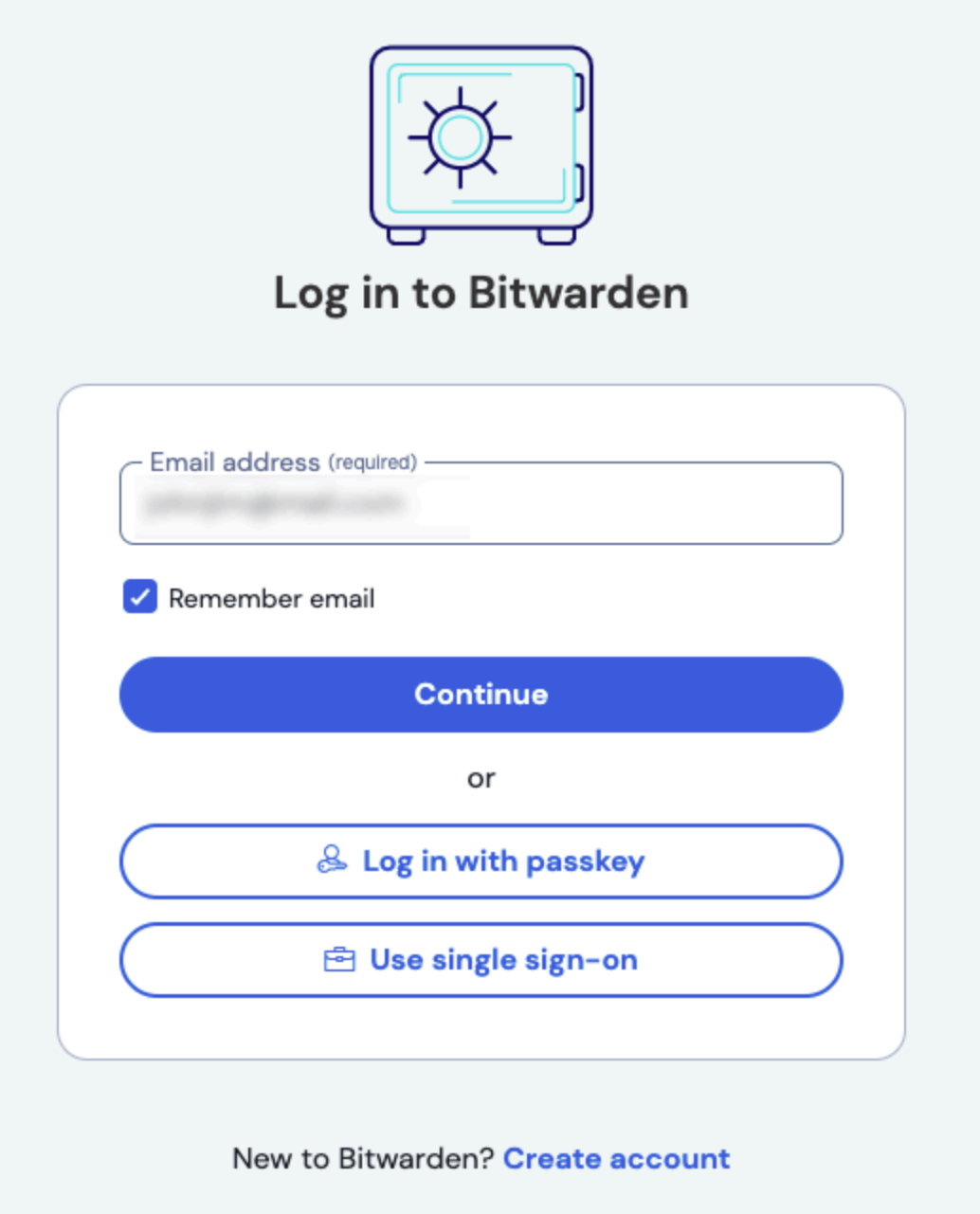
Sla uw werk **op** wanneer u klaar bent met de configuratie van de identity provider.

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 inlogscherm van je bron IdP.

Nadat u zich hebt geverifieerd met uw IdP login en Duo Two-factor, voert u uw Bitwarden master wachtwoord 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.