

BEHEERCONSOLE > INLOGGEN MET SSO >

OneLogin SAML- implementatie

OneLogin SAML-implementatie

Dit artikel bevat **OneLogin-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 OneLogin 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 (☰):

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card	My Organiz...	⋮
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Product switcher

Open het scherm **Instellingen** → **Eenmalige aanmelding** van uw organisatie:

bitwarden
Admin Console

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

Single sign-on

Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication
Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required) —————
unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

Trusted devices
Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type —————
SAML 2.0

SAML service provider configuration

Set a unique SP entity ID
Generate an identifier that is unique to your organization

SP entity ID —————
[Randomly generated ID]

SAML 2.0 metadata URL —————
[Randomly generated URL]

SAML 2.0 configuratie

Als je dat nog niet hebt gedaan, maak dan een unieke **SSO-identificer** 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 OneLogin-app maken

Navigeer in de OneLogin Portal naar het scherm **Toepassingen** en selecteer de knop **App toevoegen**:

Applications



search company apps...

No company apps have been added.

Add an Application

Typ in de zoekbalk **saml test connector** en selecteer de app **SAML Test Connector (Advanced)**:

Find Applications

saml test connector

	SAML Test Connector (Advanced) OneLogin, Inc.	SAML2.0
	SAML Test Connector (SP Shibboleth) OneLogin, Inc.	SAML2.0

SAML Test Connector App

Geef uw toepassing een Bitwarden-specifieke **weergavenaam** en selecteer de knop **Opslaan**.

Configuratie

Selecteer **Configuratie** in de linkernavigatie en configureer de volgende informatie, waarvan je sommige moet ophalen uit het scherm Single Sign-On:

Applications /

SAML Test Connector (Advanced)

More Actions ▾

Save

Info	<h3>Application details</h3> <p>RelayState</p> <input type="text"/> <p>Audience (EntityID)</p> <input type="text"/> <p>Recipient</p> <input type="text"/>
Configuration	
Parameters	
Rules	
SSO	
Access	

App Configuration

Toepassing instellen	Beschrijving
Audiëntie (EntiteitID)	<p>Stel dit veld in op de vooraf gegenereerde SP entiteit ID.</p> <p>Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het Instellingen → Enkelvoudige aanmelding scherm van de organisatie en zal variëren afhankelijk van je instelling.</p>
Ontvanger	<p>Stel dit veld in op dezelfde vooraf gegenereerde SP entiteit-ID die wordt gebruikt voor de instelling Audience (Entity ID).</p>
ACS (Consument) URL-validator	<p>Ondanks dat dit veld door OneLogin is gemarkeerd als Verplicht, hoeft u in feite geen informatie in te voeren in dit veld om te integreren met Bitwarden. Ga naar het volgende veld, ACS (Consumer) URL.</p>
URL ACS (consument)	<p>Stel dit veld in op de vooraf gegenereerde URL van de Assertion Consumer Service (ACS).</p> <p>Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het Instellingen → Enkelvoudige aanmelding scherm van de organisatie en zal variëren afhankelijk van je instelling.</p>

Toepassing instellen	Beschrijving
SAML initiatiefnemer	Selecteer serviceprovider . Inloggen met SSO ondersteunt momenteel geen door IdP geïnitieerde SAML-asserties.
SAML-naamID-formaat	Stel dit veld in op het SAML NameID-formaat dat je wilt gebruiken voor SAML-bevestigingen.
SAML-handtekening	Standaard ondertekent OneLogin het SAML Response. U kunt dit instellen op Assertie of Beide

Selecteer de knop **Opslaan** om uw configuratie-instellingen te voltooien.

Parameters

Selecteer **Parameters** in de linker navigatie en gebruik het pictogram **+ Toevoegen** om de volgende aangepaste parameters te maken:

Veldnaam	Waarde
e-mail	E-mail
voornaam	Voornaam
achternaam	Achternaam

Selecteer de knop **Opslaan** om uw aangepaste parameters te voltooien.

SSO

Selecteer **SSO** in de linker navigatie en vul het volgende in:

1. Selecteer de link **Details bekijken** onder uw X.509-certificaat:

Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate

Standard Strength Certificate (2048-bit)

[Change](#) [View Details](#)

SAML Signature Algorithm

SHA-256

[Issuer URL](#)

<https://app.onelogin.com/saml/metadata/95eef6e7-560f-4531-9df3-02e7248415a8>

SAML 2.0 Endpoint (HTTP)

<https://mmccabe.onelogin.com/trust/saml2/http-post/sso/95eef6e7-560f-4531-9df3-02e7248415a8>

[View your Cert](#)

Download of kopieer uw X.509 PEM-certificaat in het scherm Certificaat, want u zult [het later moeten gebruiken](#). Ga na het kopiëren terug naar het hoofdscherm van SSO.

2. Stel uw **SAML-handtekeningalgoritme** in.

3. Noteer je **Issuer URL** en **SAML 2.0 Endpoint (HTTP)**. Je zult [deze waarden binnenkort moeten gebruiken](#).

Toegang

Selecteer **Toegang** in de linkernavigatie. Wijs in het gedeelte **Rollen** applicatietoegang toe aan alle rollen waarvan u wilt dat ze Bitwarden kunnen gebruiken. De meeste implementaties maken een Bitwarden-specifieke rol aan en kiezen in plaats daarvan voor toewijzing op basis van een catch-all (bijvoorbeeld **Default**) of op basis van reeds bestaande rollen.

Privileges	
Setup	Roles
	Bitwarden SSO Users ✓
	Default

Role Assignment

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de OneLogin 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 de OneLogin Portal [tijdens het maken van de app](#):

Veld	Beschrijving
Naam ID Formaat	Stel dit veld in op wat je hebt geselecteerd voor het OneLogin SAML nameID Format veld tijdens de app configuratie .
Algoritme voor uitgaande ondertekening	Algoritme dat wordt gebruikt om SAML-verzoeken te ondertekenen, standaard sha-256 .
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden. Standaard vereist OneLogin niet dat verzoeken worden ondertekend.
Algoritme voor minimale inkomende ondertekening	Stel dit veld in op wat je hebt geselecteerd voor het SAML-handtekeningalgoritme tijdens de app-configuratie
Ondertekende beweringen	Vink dit vakje aan als je het SAML-handtekeningelement in OneLogin hebt ingesteld op Assertion of Both tijdens de app-configuratie .
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 je teruggaat naar de OneLogin Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer uw OneLogin Issuer URL in, die u kunt ophalen uit het SSO-scherm van de OneLogin app . Dit veld is hoofdlettergevoelig.
Type binding	Stel in op HTTP Post (zoals aangegeven in SAML 2.0 Endpoint (HTTP)).
URL voor service voor eenmalige aanmelding	Voer uw OneLogin SAML 2.0 Endpoint (HTTP) in, dat u kunt ophalen uit het SSO-scherm van de OneLogin app .
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	<p>Plak het opgehaalde X.509-certificaat en verwijder het</p> <p>-----BEGIN CERTIFICAAT-----</p> <p>en</p> <p>-----END CERTIFICAAT-----</p> <p>De certificaatwaarde is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens zorgen ervoor dat de certificatievalidatie mislukt.</p>
Algoritme voor uitgaande ondertekening	Selecteer het SAML-handtekeningalgoritme dat is geselecteerd in de sectie OneLogin SSO-configuratie .
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel geen SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of OneLogin 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:



Log in to Bitwarden

Email address (required)

Remember email

Continue

or

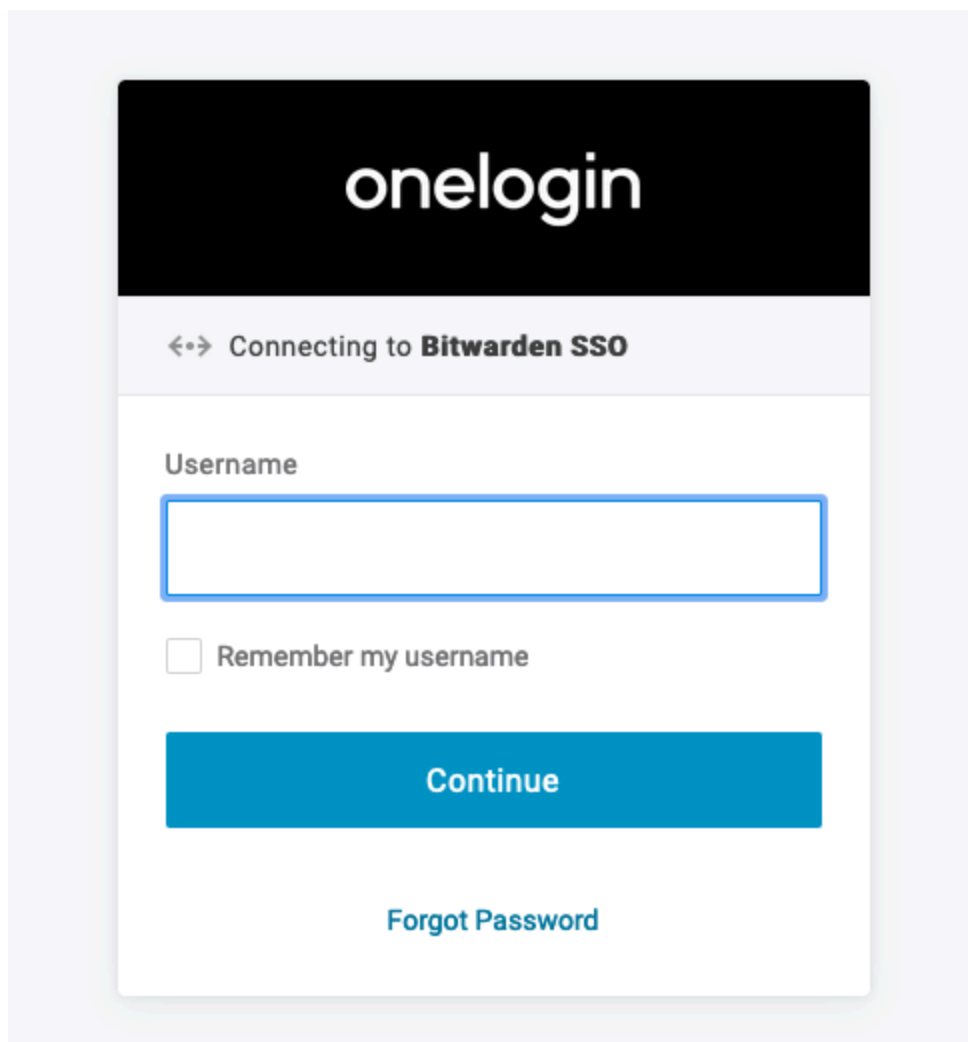
 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

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 OneLogin inlogscherf:



OneLogin Login

Nadat u zich hebt geverifieerd met uw OneLogin-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.