

BEHEERCONSOLE > INLOGGEN MET SSO >

# Auth0 SAML-implementatie

## Auth0 SAML-implementatie

Dit artikel bevat **Auth0-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.

Configuratie houdt in dat er tegelijkertijd wordt gewerkt binnen de Bitwarden web app en de Auth0 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 (☰):

The screenshot shows the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. Below these is a 'Product Manager' section with three options: Password Manager (highlighted with a red circle and arrow), Secrets Manager, and Admin Console. At the bottom of the sidebar is 'Toggle Width'. The main content area is titled 'All vaults' and features a 'New' button, a product switcher icon (☰), and a 'BW' profile icon. Below the title is a 'FILTERS' panel with a search box and a list of categories: All vaults (My vault, My Organiz..., Teams Org..., New organization), All items (Favorites, Login, Card, Identity, Secure note), Folders (No folder), Collections (Default colle..., Default colle...), and Trash. The main vault list has columns for 'All', 'Name', and 'Owner'. It contains five entries: 'Company Credit Card' (owner: My Organiz...), 'Personal Login' (owner: Me), 'Secure Note' (owner: Me), and 'Shared Login' (owner: My Organiz...). The 'Product switcher' icon is located in the top right of the main content area.

Product switcher

Open het scherm **Instellingen** → **Enmalige 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

[Masked SP entity ID]



SAML 2.0 metadata URL

[Masked SAML 2.0 metadata 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 Auth0-toepassing maken

Gebruik in de Auth0 Portal het menu Toepassingen om een **Reguliere Webtoepassing** te maken:

dev-hn11g2a6  
Development

Thank you for purchasing the Free Auth0 plan. You have 22 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your [billing information here](#). BILLING

## Applications

Setup a mobile, web or IoT application to use Auth0 for Authentication. [Learn more](#) ▶

**Default App**  
Generic

Client ID: `RM3UeXnRtL8CSjPPCg7HiitjInvQs0Be`

+ CREATE APPLICATION

*Auth0 Create Application*

Klik op het tabblad **Instellingen** en configureer de volgende informatie, waarvan u sommige moet ophalen uit het Bitwarden Single Sign-On scherm:

### Basic Information

Name \*

Bitwarden Login with SSO



Domain

.us.auth0.com



Client ID

HcoxD53h7Qz1520u8pabHPWoZEG0Hho2



Client Secret

.....



The Client Secret is not base64 encoded.

Auth0 Settings

#### Auth0-instelling

#### Beschrijving

Naam

Geef de applicatie een Bitwarden-specifieke naam.

Domein

Noteer deze waarde. Je zult het nodig hebben [tijdens een latere stap](#).

Type toepassing

Selecteer **Regelmatige webtoepassing**.

Token Eindpunt  
Authenticatiemethode

Selecteer **Post** (HTTP Post), wat overeenkomt met een **Binding Type** attribuut dat je [later zult configureren](#).

AuthO-instelling	Beschrijving
Toepassing Login URI	Stel dit veld in op de vooraf gegenereerde <b>SP entiteit ID</b> .  Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het <b>Instellingen</b> → <b>Enkelvoudige aanmelding</b> scherm van de organisatie en zal variëren afhankelijk van je instelling.
Toegestane terugbel URLs	Stel dit veld in op de vooraf gegenereerde <b>URL van de Assertion Consumer Service (ACS)</b> .  Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het <b>Instellingen</b> → <b>Enkelvoudige aanmelding</b> scherm van de organisatie en zal variëren afhankelijk van je instelling.

### Soorten subsidies

Zorg ervoor dat in het gedeelte **Geavanceerde instellingen** → **Soorten subsidies** de volgende soorten subsidies zijn geselecteerd (mogelijk zijn ze al geselecteerd):

#### Advanced Settings ^

Application Metadata   Device Settings   OAuth   Grant Types   WS-Federation   Certificates

##### Grants

Implicit    Authorization Code    Refresh Token    Client Credentials  
 Password    MFA    Passwordless OTP

Application Grant Types

## Certificaten

Kopieer of download uw ondertekeningscertificaat in de sectie **Geavanceerde instellingen** → **Certificaten**. Je hoeft er nu nog niets mee te doen, maar je zult [er later wel naar moeten verwijzen](#).

### Advanced Settings ^

[Application Metadata](#)[Device Settings](#)[OAuth](#)[Grant Types](#)[WS-Federation](#)[Certificaten](#)

#### Signing Certificate

```
-----BEGIN CERTIFICATE-----  
MIIDDTCcAfWgAwIBAgIJdp2+Lsu8IyKcMA0GCSqGSIb3DQEBCwUAMCQxIjAgBgNV  
BAMTGWRldi1objExZzJhNi51cy5hdXRoMC5jb20wHhcNMjEwNDE1MTUxMjUxWhcN  
MzQxMjIzMTUxMjUxWjAkMSIwIAYDVQQDExlkZXYtaG4xMWcyYTYudXMudXMudA  
Y29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2yRfsSC5LCYkTvuF  
nCW0wCEE7jkTtdxRGytTBwJEarqzmgMzktBmkU0BfuzjrtcaQx0utRM679AD0PX9  
WZLqwICerdeKP01S3/TvqkNkPyf2UE27Qo4giJy6FEUAgswTs/gtX6sxIogeH0N  
cJ95strc/F+jtw17Tukul1x4nv3TcvK115TZRA38bW/J7Q61QC3MSMS2FG3D/hDi  
p3V-0k-F-iQ-D1k-d5-b-C-1-D-0TEQ-ML-1-TR76-11-11-17-kf01-1561-0N1kV
```



*Auth0 Certificate*

## Eindpunten

U hoeft niets aan te passen in het gedeelte **Geavanceerde instellingen** → **Eindpunten**, maar u hebt de SAML-eindpunten nodig om [later naar te verwijzen](#).

### 💡 Tip

In smaller windows, the **Endpoints** tab can disappear behind the edge of the browser. If you're having trouble finding it, click the **Certificaten** tab and hit the Right Arrow key (→).

### Advanced Settings ^

Metadata   Device Settings   OAuth   Grant Types   WS-Federation   Certificates   **Endpoints**

---

#### OAuth

**OAuth Authorization URL**

`https://dev-hn11g2a6.us.auth0.com/authorize`

**Device Authorization URL**

`https://dev-hn11g2a6.us.auth0.com/oauth/device/code`

*Auth0 Endpoints*

## Auth0 regels configureren

Maak regels om het SAML responsgedrag van je applicatie aan te passen. Hoewel Auth0 [een aantal opties](#) biedt, wordt in dit gedeelte alleen ingegaan op de opties die specifiek overeenkomen met Bitwarden-opties. Om een aangepaste SAML configuratieregels te maken, gebruik je het menu **Auth Pipeline** → **Regels** op **+ Regels maken**:



dev-hn11g2a6  
Development


Docs
F5

Thank you for purchasing the Free Auth0 plan. You have 21 days left in your trial to experiment with [features that are not in the Free plan](#). Like what you're seeing? Please enter your [billing information here](#). BILLING

---

## Rules + CREATE

Custom Javascript snippets that run in a secure, isolated sandbox in the Auth0 service as part of your authentication pipeline. [Learn more](#) ▶

TRY ALL RULES WITH... ▼
REFRESH

Custom SAML Config



...

Auth0 Rules

U kunt het volgende configureren:

Sleutel	Beschrijving
<code>signatureAlgorithm</code>	<p>Algoritme dat Auth0 zal gebruiken om de SAML-bevestiging of het SAML-antwoord te ondertekenen. Standaard wordt <code>rsa-sha1</code> opgenomen, maar deze waarde moet worden ingesteld op <code>rsa-sha256</code>.</p> <p>Als u deze waarde wijzigt, moet u:</p> <ul style="list-style-type: none"> <li>-Stel <code>digestAlgorithm</code> in op <code>sha256</code>.</li> <li>-Stel (in Bitwarden) het <b>Minimum Incoming Signing Algorithm</b> in op <code>rsa-sha256</code>.</li> </ul>
<code>digestAlgorithm</code>	<p>Algoritme dat wordt gebruikt om de digest van de SAML-bevestiging of het SAML-antwoord te berekenen. Standaard is dit <code>sha-1</code>. De waarde voor <code>signatureAlgorithm</code> moet ook worden ingesteld op <code>sha256</code>.</p>
<code>signResponse</code>	<p>Auth0 ondertekent standaard alleen de SAML-bevestiging. Stel dit in op <code>waar</code> om het SAML-antwoord te ondertekenen in plaats van de bevestiging.</p>

Sleutel	Beschrijving
<code>nameIdentifierFormat</code>	Standaard is <code>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</code> . U kunt deze waarde instellen op elke SAML NameID-indeling. Als dat het geval is, wijzig dan het veld SP <b>Name ID Format</b> in de overeenkomstige optie (zie hier).

Implementeer deze regels met behulp van een **Script** zoals hieronder. Raadpleeg [de documentatie van Auth0](#) voor hulp.

#### Bash

```
function (user, context, callback) {
  context.samlConfiguration.signatureAlgorithm = "rsa-sha256";
  context.samlConfiguration.digestAlgorithm = "sha256";
  context.samlConfiguration.signResponse = "true";
  context.samlConfiguration.nameIdentifierFormat = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress";
  context.samlConfiguration.binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect";
  callback(null, user, context);
}
```

## Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de Auth0 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

Tenzij je [aangepaste regels](#) hebt geconfigureerd, is de configuratie van je serviceprovider al voltooid. Als je aangepaste regels hebt geconfigureerd of verdere wijzigingen wilt aanbrengen aan je implementatie, bewerk dan de relevante velden:

Veld	Beschrijving
Naam ID Formaat	NameID-formaat om op te geven in het SAML-verzoek ( <b>NameIDPolicy</b> ). Stel in op <b>Niet geconfigureerd</b> om weg te laten.

Veld	Beschrijving
Algoritme voor uitgaande ondertekening	Algoritme dat wordt gebruikt om SAML-verzoeken te ondertekenen, standaard <b>rsa-sha256</b> .
Ondertekengedrag	Of/wanneer Bitwarden SAML verzoeken worden ondertekend. AuthO vereist standaard niet dat verzoeken worden ondertekend.
Algoritme voor minimale inkomende ondertekening	Het minimale ondertekeningsalgoritme dat Bitwarden accepteert in SAML-reacties. AuthO ondertekent standaard met <b>rsa-sha1</b> . Selecteer <b>rsa-sha256</b> in de vervolgkeuzelijst tenzij u een <a href="#">aangepaste ondertekeningsregel</a> hebt geconfigureerd.
Ondertekende beweringen	Of Bitwarden SAML-asserties ondertekend wil hebben. Standaard zal AuthO SAML asserties ondertekenen, dus vink dit vakje aan tenzij je een <a href="#">aangepaste ondertekeningsregel</a> hebt geconfigureerd.
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 terugverwijst naar de AuthO Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer de <b>domeinwaarde</b> van je AuthO-toepassing in (zie <a href="#">hier</a> ), voorafgegaan door urn :, bijvoorbeeld urn : <b>bw-help.us.auth0.com</b> . Dit veld is hoofdlettergevoelig.
Type binding	Selecteer <b>HTTP POST</b> om overeen te komen met de <a href="#">Token Endpoint Authentication Method-waarde</a> die is opgegeven in uw AuthO-toepassing.
URL voor service voor eenmalige aanmelding	Voer de <b>SAML-protocol URL</b> (zie <a href="#">Endpoints</a> ) van uw AuthO-toepassing in. Bijvoorbeeld <b>https://bw-help.us.auth0.com/samlp/HcpxD63h7Qz1420u8qachPWozEG0Hho2</b> .

Veld	Beschrijving
URL voor service voor eenmalig afmelden	Inloggen met SSO ondersteunt momenteel <b>geen</b> SLO. Deze optie is gepland voor toekomstige ontwikkeling, maar u kunt deze desgewenst vooraf configureren.
X509 publiek certificaat	<p>Plak het opgehaalde <a href="#">ondertekeningscertificaat</a> en verwijder</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 <b>de certificatievalidatie mislukt</b>.</p>
Algoritme voor uitgaande ondertekening	Auth0 ondertekent standaard met <code>rsa-sha1</code> . Selecteer <code>rsa-sha256</code> tenzij je een <a href="#">aangepaste ondertekeningsregel</a> hebt geconfigureerd.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel <b>geen</b> SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of Auth0 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

Master password (required)



⊗ Input is required.

[Get master password hint](#)

Log in with master password

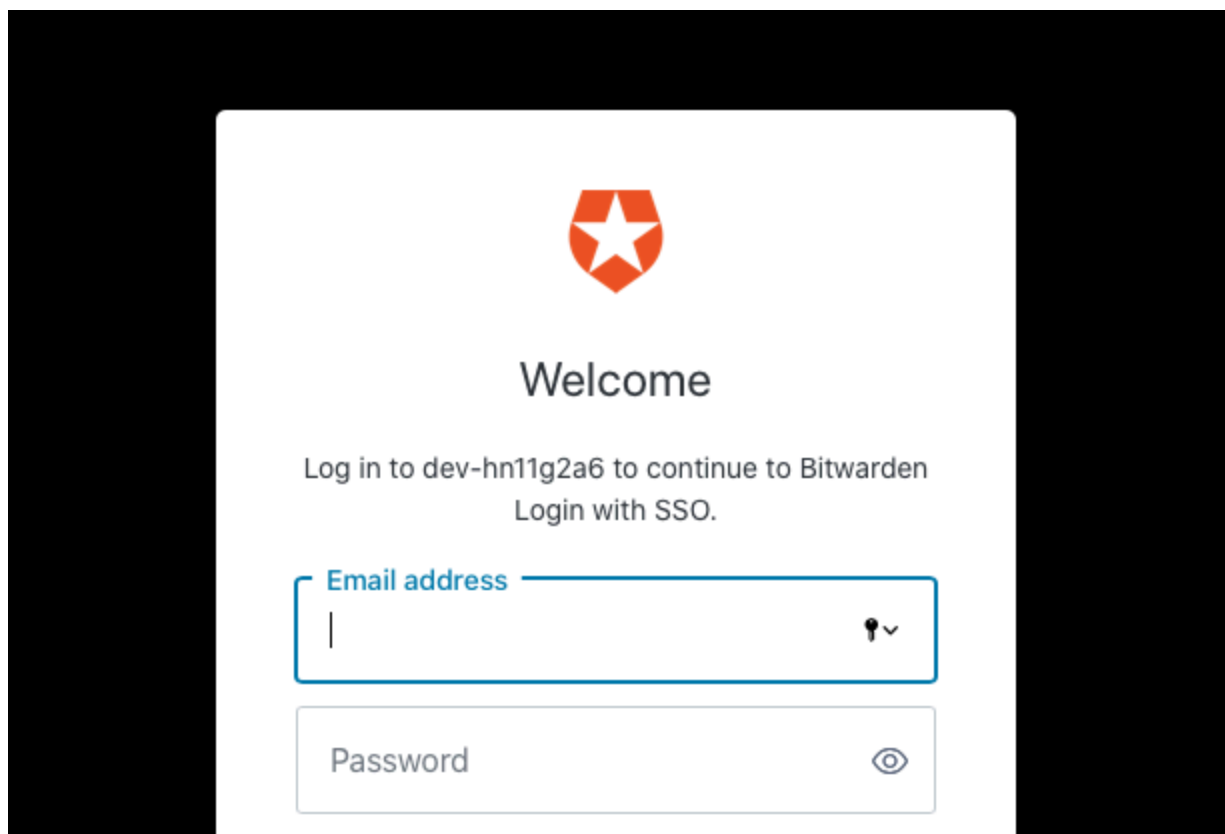
 Enterprise single sign-on

Logging in as myemailaddress@bitwarden.com

[Not you?](#)

*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 Auth0 aanmeldscherm:



*Auth0 Login*

Nadat u zich hebt geverifieerd met uw Auth0-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.