

BEHEERCONSOLE > INLOGGEN MET SSO >

Google SAML-implementatie

Google SAML-implementatie

Dit artikel bevat **Google Workspace-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 met de Bitwarden-webapp en de Google Workspace beheerconsole. 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 the 'Password Manager' logo at the top. Below the logo are several menu items: 'Vaults', 'Send', 'Tools', 'Reports', and 'Settings'. At the bottom of the sidebar, there is a section with three items: 'Password Manager' (highlighted with a red box), 'Secrets Manager', and 'Admin Console'. A red arrow points from the 'Admin Console' item to the 'All vaults' section of the main content area. The main content area has a light blue header with the title 'All vaults' and a 'New' button. Below the header is a table of vaults. The table has columns for 'Name' and 'Owner'. The vaults listed are: '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 corner of the main content area.

Product switcher

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



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

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.



Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met [SSO met vertrouwde apparaten](#) of [Key Connector](#).

Een SAML-app maken

Selecteer in de Google Workspace beheerconsole **Apps** → **Web en mobiele apps** in de navigatie. Selecteer in het scherm Web- en mobiele apps **App toevoegen** → **Aangepaste SAML-app toevoegen**:

The screenshot shows the Google Admin console interface. In the left sidebar, the 'Web and mobile apps' option under the 'Apps' section is highlighted with a green rounded rectangle. In the main content area, the 'Apps (0)' header has a dropdown menu open, showing options: 'Search for apps', 'Add private Android app', 'Add private Android web app', and 'Add custom SAML app'. The 'Add custom SAML app' option is highlighted with a green rounded rectangle. Below the main content area, there is a link that says 'Create a SAML App'.

App details

Geef de applicatie in het scherm met appdetails een unieke Bitwarden-specifieke naam en selecteer de knop **Doorgaan**.

Google identiteitsgegevens

Kopieer in het detailscherm van Google Identity Provider uw **SSO-URL**, **Entity ID** en **certificaat** voor gebruik tijdens een latere stap:

✕ Add custom SAML app

✓ App details — 2 Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

Option 1: Download IdP metadata

[DOWNLOAD METADATA](#)

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

<https://accounts.google.com/>

Entity ID

<https://accounts.google.com/>

Certificate

Google_

Expires

-----BEGIN CERTIFICATE-----

SHA-256 fingerprint

BACK

CANCEL

CONTINUE

IdP Details

Selecteer **Doorgaan** als u klaar bent.

Gegevens serviceprovider

Configureer de volgende velden in het scherm Service provider details:

Veld	Beschrijving
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 je instelling.
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.
URL starten	Stel dit veld optioneel 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.
Ondertekend antwoord	Vink dit vakje aan als je wilt dat Workspace SAML-reacties ondertekent. Als deze optie niet is aangevinkt, ondertekent Workspace alleen de SAML-verklaring.
Naam ID-indeling	Stel dit veld in op Persistent.
Naam ID	Selecteer het gebruikerskenmerk van de werkruimte om NameID in te vullen.

Selecteer **Doorgaan** als u klaar bent.

Attribuut toewijzen

Selecteer in het scherm Attribute mapping de knop **Add Mapping** en construeer de volgende mapping:

Google Directory-kenmerken	App-kenmerken
Primaire e-mail	e-mail

Selecteer **afwerking**.

De app inschakelen

Standaard staan Workspace SAML-apps **voor iedereen UIT**. Open de sectie Gebruikerstoegang voor de SAML-app en stel deze in op **AAN voor iedereen** of voor specifieke groepen, afhankelijk van je behoeften:

SAML

 Bitwarden Login with SSO

TEST SAML LOGIN

DOWNLOAD METADATA

DELETE APP

User access

To make the managed app available to select users, choose a group or organizational unit. [Learn more](#)

[View details](#)

OFF for everyone

Service provider details

Certificate	ACS URL	Entity ID
Google_2026-5-9-112241_SAML2_0 (Expires May 9, 2026)		https://sso.bitwarden.com/saml2

User Access

Sla uw wijzigingen **op**. Houd er rekening mee dat het tot 24 uur kan duren voordat een nieuwe Workspace-app is verspreid naar bestaande sessies van gebruikers.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van de Google Workspace beheerconsole. 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 **tijdens de installatie** zijn geselecteerd in de Workspace Admin-console:

Veld	Beschrijving
Naam ID Formaat	Stel dit veld in op de Naam ID-indeling die is geselecteerd in Werkruimte .
Algoritme voor uitgaande ondertekening	Het algoritme dat Bitwarden gebruikt om SAML-verzoeken te ondertekenen.
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden.

Veld	Beschrijving
Algoritme voor minimale inkomende ondertekening	Standaard ondertekent Google Workspace met RSA SHA-256. Selecteer sha-256 in de vervolgkeuzelijst.
Verwacht ondertekende beweringen	Of Bitwarden verwacht dat SAML-asserties worden ondertekend. Deze instelling moet uitgevinkt zijn .
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 met 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 je vaak teruggaan naar de Workspace Admin console om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Stel dit veld in op de Entity ID van de Workspace, die je kunt ophalen uit het gedeelte Details Google Identity Provider of met de knop Metadata downloaden . Dit veld is hoofdlettergevoelig.
Type binding	Stel in op HTTP POST of Redirect .
URL voor service voor eenmalige aanmelding	Stel dit veld in op de SSO-URL van de Workspace, opgehaald uit het gedeelte Details Google Identity Provider of met de knop Metadata downloaden .
URL voor enkelvoudig 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 opgehaalde certificaat en 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	Standaard ondertekent Google Workspace met RSA SHA-256. Selecteer sha-256 in de vervolgkeuzelijst.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel geen SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of Google Workspace 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

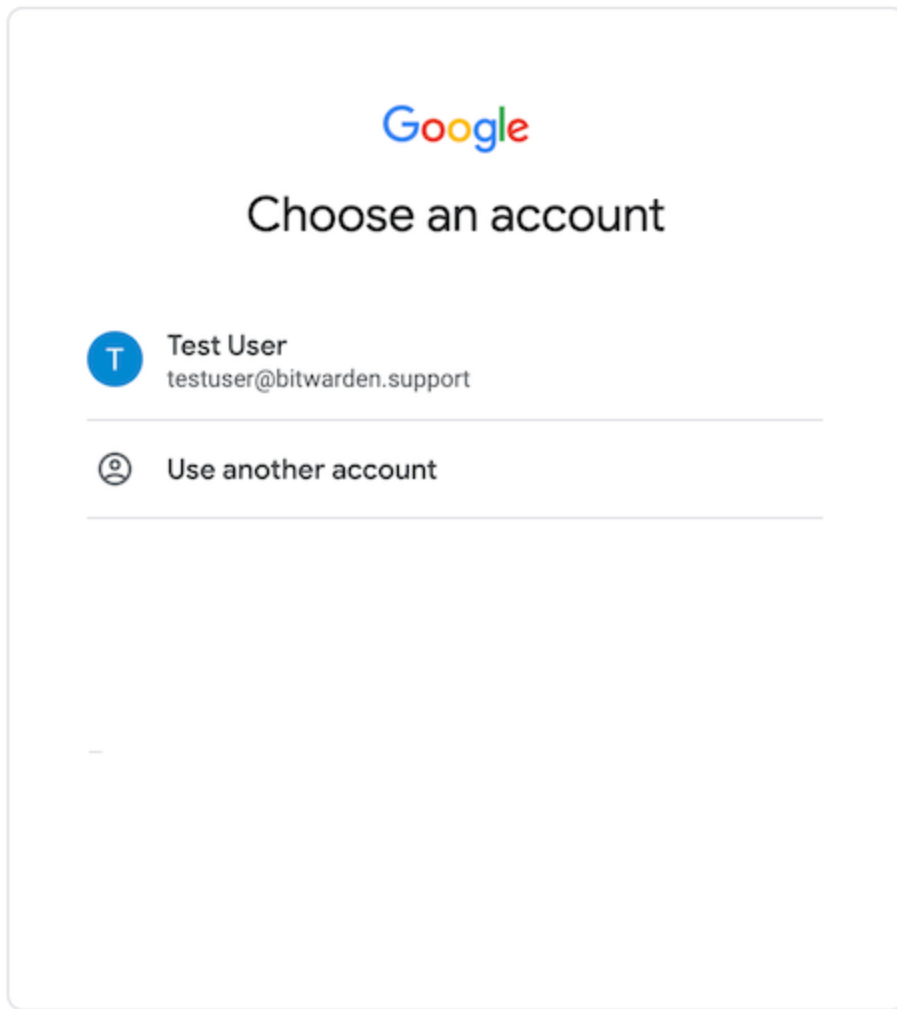
 Log in with passkey

 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 inlogscherf van Google Workspace:



Login

Nadat je je hebt geverifieerd met je Workspace-inloggegevens, voer je je Bitwarden-hoofdwachtwoord in om je 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.