

BEHEERCONSOLE > INLOGGEN MET SSO >

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 ():

Filters:

- 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...
 - Trash

<input type="checkbox"/>	All	Name	Owner	
<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** → **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)

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 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 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:

Dashboard > Applications > Protect an Application

Protect an Application

1 Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others. Documentation: [Getting Started](#)

Choose an application below to get started.

Bitwarden

Application	Protection Type	
Bitwarden	2FA	Documentation Protect
Bitwarden	2FA with SSO hosted by Duo (Single Sign-On)	Documentation Configure

Duo Bitwarden Application

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

Dashboard > Single Sign-On

Single Sign-On

Simplify access to the applications your users rely on. With Duo's cloud-hosted SSO, protecting your applications while reducing user friction has never been easier. [Learn how it works](#)

Duo-hosted SSO requires Duo to collect and validate users' primary Active Directory credentials and/or directly receive SAML assertions. During authentication, usernames and passwords are encrypted when passed to your [Authentication Proxy server\(s\)](#). Duo caches the AD password and SAML assertions only long enough to complete the authentication. [Learn more](#)

I have read and understand these Duo-hosted SSO updates, the [Privacy Statement](#) and Duo's [Privacy Data Sheet](#)

[Activate and Start Setup](#)

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:

- Dashboard
- Device Insight
- Policies
- Applications
- Single Sign-On**
- Duo Central
- Passwordless
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints

[← Back to Single Sign-On](#)

SAML Identity Provider Configuration ✓ Enabled

Status: Enabled [Disable Source](#)

Configure a SAML Identity Provider to provide primary authentication for Duo Single Sign-On by following the sections below.
[Learn more about configuring the SAML Identity Provider with Duo Single Sign-On](#)

1. Configure the SAML Identity Provider

Provide this information about your Duo Single Sign-On account to your SAML identity provider.

Entity ID	<code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata</code>	Copy
Assertion Consumer Service URL	<code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/acs</code>	Copy
Audience Restriction	<code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata</code>	Copy
Metadata URL	<code>https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata</code>	Copy
XML File	Download Metadata XML	

DUO SAML Identity Provider Configuration

Metagegevens

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

Metadata

Entity ID	<code>https://sso-ff27df13.sso.duosecurity.com/saml2/sp/DI4GBHNTLEJZVCCZ6EQM/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-ff27df13.sso.duosecurity.com/saml2/sp/DI4GBHNTLEJZVCCZ6EQM/sso</code>	Copy

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	<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>

Veld	Beschrijving
URL Assertion Consumentenservice (ACS)	<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>
Aanmeldings-URL serviceprovider	<p>Stel dit veld in op de aanmeldings-URL van waaruit gebruikers toegang krijgen tot Bitwarden.</p> <p>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.</p>

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:

Map attributes

IdP Attribute

SAML Response Attribute

x <Email Address>	Email +
-------------------	---

Map the values of an IdP attribute to another attribute name to be included in the SAML response (e.g. Username to User.Username). Enter in an IdP attribute or select one of Duo's preconfigured attributes that automatically chooses the SAML response attribute based on the IdP. There are five preconfigured attributes: <Email Address>, <Username>, <First Name>, <Last Name> and <Display Name>. Consult your service provider for more information on their attribute names.

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

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 je implementatie succesvol is geconfigureerd, word je doorgestuurd naar het inlogscherf 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.