## BEHEERCONSOLE > INLOGGEN MET SSO >

# Duo SAML implementatie

Weergeven in het Helpcentrum: https://bitwarden.com/help/saml-duo/

### **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

#### A 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 (2011):

D Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Nama	Owner	:
🖉 Send			Name	Owner	•
$\ll$ Tools $\sim$	Q Search vau	ARV	Company Credit Card Visa, *4242	My Organiz	:
<b></b> ≢ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	<ul> <li>∠ My vault</li> <li>∅ My Organiz :</li> <li>∅ Toomo Org</li> </ul>		myusername	Me	:
	∦ Teams Org : + New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	÷
<ul> <li>Password Manager</li> <li>Secrets Manager</li> <li>ℬ Admin Console</li> <li>Ճ Toggle Width</li> </ul>	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				
		Product s	witcher		

Open het scherm Instellingen  $\rightarrow$  Eenmalige aanmelding van uw organisatie:

<b>D bit</b> warden	Single sign-on III III III III III III III IIII II
🖉 My Organization 🔍	Use the <b>require single sign-on authentication policy</b> to require all members to log in with SSO.
Collections	Allow SSO authentication
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
卷 Groups	SSO identifier (required)
	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
🕅 Billing 🗸 🗸	Member decryption options
Settings	Master password
Organization info	O Trusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and
Policies	account recovery administration policy with automatic enrollment will turn on when this option is used.
Two-step login	Type
Import data	SAME 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	SP entity ID
SCIM provisioning	i a com a comunicación de la comunicación d
	SAML 2.0 metadata URL

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 SAMLidentiteitsprovider 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		Dashboard > Applications > Protect an Application			Þ
Device Insight	~	Protect an Application			
Policies Applications Protect an Application	^	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 min     Documentation: Getting Started [3]     Choose an application below to get started.	utes, and you're the only one that will see it, until you decide to add others.		
Authentication F	roxy	_			
Single Sign-On	$\sim$	Bitwarden			
Users	~	Application	Protection Type		
Groups	~				
Endpoints	~	bitwarden Bitwarden	2FA	Documentation 🗗 Pro	tect
2FA Devices	$\sim$				
Administrators	~	Bitwarden	(Single Sign-On)	Documentation 🗗 Config	jure
Trusted Endpoints					

Duo Bitwarden Application

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

Dash	board	
Devi	ce Insight	$\checkmark$
Polic	ies	$\checkmark$
Appl	ications	$\sim$
Single Sign-On		^
D	uo Central	
P	asswordless	
Users v		$\checkmark$
Groups 🗸		$\checkmark$
Endpoints ~		$\sim$
2FA Devices ~		$\sim$

# 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)  $\Box$ . Duo caches the AD password and SAML assertions only long enough to complete the authentication. Learn more  $\Box$ 

✓ I have read and understand these Duo-hosted SSO updates, the Privacy Statement ☐ and Duo's Privacy Data Sheet ☐



Dashboard > Single Sign-On

#### 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		← <u>Back to Single Sign-On</u>		Status: Enabled Disable Source
Device Insight	$\sim$			Status. Enabled Disable Source
Policies	~	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 다		
Applications	~	1. Configure the SAML Identity Provider		
Single Sign-On	^	Provide this information about y	our Duo Single Sign-On account to your SAML identity provider.	
Duo Central Passwordless		Entity ID	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
Users	~	Assertion Consumer	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/acs	Сору
Groups	~	Service URL		
Endpoints	~	Audience Restriction	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
2FA Devices	~	Metadata URL	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
Administrators	$\sim$			
Trusted Endpoints		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



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 <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.

Veld	Beschrijving
URL Assertion Consumentenservice (ACS)	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.
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://vaul t.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 NamelD	Stel dit veld in op de SAML NameID-indeling zodat Duo deze kan verzenden in SAML-reacties.
NamelD attribuut	Stel dit veld in op het Duo-attribuut dat de NamelD 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 <b>een antwoord wilt ondertekenen, een bewering wilt ondertekenen</b> of beide.
Kenmerken kaart	Gebruik deze velden om IdP-attributen toe te wijzen aan SAML-responsattributen. Ongeacht welk NamelD attribuut je hebt geconfigureerd, koppel het IdP Email Address attribuut aan Email, zoals in de volgende schermafbeelding:

Map attributes	IdP Attribute	SAML Response Attribute
	× <email address=""></email>	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). E	nter 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 add<="" th=""><th>ress&gt;, <username>, <first name="">, <last name=""> and</last></first></username></th></email>	ress>, <username>, <first name="">, <last name=""> and</last></first></username>
	<display name="">. Consult your service</display>	e 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 <mark>rsa-sha256</mark> .
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 <b>Entity ID-waarde</b> 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 <b>HTTP Post</b> .
URL voor service voor eenmalige aanmelding	Voer de <b>Single Sign-On URL-waarde</b> 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 <b>geen</b> SLO. Deze optie is gepland voor toekomstige ontwikkeling, maar u kunt deze vooraf configureren met de <b>Single Log-Out</b> <b>URL-waarde</b> van uw Duo-applicatie.
X509 publiek certificaat	Plak het gedownloade certificaat, verwijder
	en

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

#### (i) 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 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!

#### (i) Note

Bitwarden ondersteunt geen ongevraagde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSOaanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden.