BEHEERCONSOLE > INLOGGEN MET SSO >

Okta SAML-implementatie

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

Okta SAML-implementatie

Dit artikel bevat **Okta-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 het Okta Admin 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.

Jownload Sample ↓

Open SSO in de webapp

Log in op de Bitwarden web app en open de Admin Console met behulp van de product switcher (ﷺ):

D Password Manager	All vaults			New ~	BW
🗇 Vaults	FILTERS		Neme	Owner	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	AZIV	Company Credit Card Visa, *4242	My Organiz	:
≅ Reports	✓ All vaults		Personal Logia		
🕸 Settings 🛛 🗸 🗸	 ∠ My vault ∠ My Organiz : ∠ Toorganiz : 	0 3	myusername	Me	:
	 gain Teams Org : + New organization 		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ③ Login □ Card Identity □ Secure note 	0	Shared Login sharedusername	My Organiz	:
A Password Manager	✓ Folders☐ No folder				
	✓ Collections				
🗔 Secrets Manager	Default colle				
Admin Console	🛍 Trash				
🖞 Toggle Width					
		Dueducete			

Product switcher

Open het scherm Instellingen → Eenmalige aanmelding van uw organisatie:

Secure and trusted open source password manager for business

D bit warden	Single sign-on 🖩 🖬
B My Organization	Use the <u>require single sign-on authentication policy</u> 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.
뿅 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	Naster password
Organization info Policies	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.
Two-step login	C Type
Import data	SAML 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	Generate an identifier that is unique to your organization SP entity ID
SCIM provisioning	
	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 Okta-applicatie maken

Selecteer in het Okta Admin Portal **Applicaties** → **Applicaties** in de navigatie. Selecteer in het scherm Toepassingen de knop **Appintegratie maken**:

Dashboard	~				
Directory	~	Applications			Help
Customizations	~	Create App Integration	Browse App Catalog	Assign Users to App More 🔻	
Applications	^				
Applications		Q Search			
Self Service		STATUS	•	Okta Admin Console	
Security	~	ACTIVE	0		
Workflow	~	INACTIVE	6	Okta Browser Plugin	
Reports	~			Okta Dashboard	
Settings	~				

Okta create app integration

Selecteer het keuzerondje SAML 2.0 in het dialoogvenster Nieuwe applicatie-integratie maken:



SAML 2.0 radio button

Selecteer de knop Volgende om verder te gaan met de configuratie.

Algemene instellingen

Geef de applicatie in het scherm Algemene instellingen een unieke, Bitwarden-specifieke naam en selecteer Volgende.

SAML configureren

Configureer de volgende velden in het scherm Configureer SAML:

Veld	Beschrijving
URL voor eenmalige aanmelding	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 → Eenmalige aanmelding scherm van de organisatie en zal variëren afhankelijk van je instelling.
Audience URI (SP entiteit ID)	Stel dit veld in op de vooraf gegenereerde SP entiteit ID . Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het Instellingen → Eenmalige aanmelding scherm van de organisatie en zal variëren afhankelijk van je instelling.
Naam ID-indeling	Selecteer de SAML NamelD-indeling om te gebruiken in SAML-bevestigingen. Standaard Niet gespecificeerd.
Gebruikersnaam sollicitatie	Selecteer het Okta-attribuut waarmee gebruikers zich aanmelden bij Bitwarden.

Geavanceerde instellingen

Selecteer de link Geavanceerde instellingen weergeven en configureer de volgende velden:



Advanced Settings

Veld	Beschrijving
Reactie	Of het SAML-antwoord is ondertekend door Okta.
Handtekening	Of de SAML assertion is ondertekend door Okta.
Handtekening algoritme	Het ondertekeningsalgoritme dat wordt gebruikt om het antwoord en/of de bewering te ondertekenen, afhankelijk van welke is ingesteld op Ondertekend . Standaard is dit rsa-sha256 .
Digest-algoritme	Het digest-algoritme dat wordt gebruikt om het antwoord en/of de bewering te ondertekenen, afhankelijk van welke is ingesteld op Ondertekend . Dit veld moet overeenkomen met het geselecteerde handtekeningalgoritme .

Attribuutverklaringen

Construeer in de sectie **Attribute Statements** de volgende SP \rightarrow IdP attribuutkoppelingen:

ame	Name format (optional)	Value	
email	Unspecified •	user.email	•
firstname	Unspecified •	user.firstName	•
lastname	Unspecified •	user.lastName	•

Attribute Statements

View SAML setup instructions

Selecteer na de configuratie de knop Volgende om door te gaan naar het Feedbackscherm en selecteer Voltooien.

IdP-waarden ophalen

Zodra je applicatie is gemaakt, selecteer je het tabblad **Aanmelden** voor de app en selecteer je de knop **Instellingsinstructies bekijken** aan de rechterkant van het scherm:

Settings		Edit	About SAML 2.0 streamlines the end user
Sign on methods The sign-on method determines how application. Some sign-on methods r Application username is determined	a user signs into and manages their cred equire additional configuration in the 3 rd by the user profile mapping. Configure pr	entials for an party application. ofile mapping	experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.
SAML 2.0			Application Username
Default Relay State			username value when assigning the application to users. If you select None you will be prompted
Credentials Details			to enter the username manually when assigning an application with password
Application username format	Okta username		or profile push provisioning features.
Update application username on	Create and update	C Update Now	
Password reveal	Allow users to securely see the (Recommended)	ir password	
SAML Signing Certifica	ites		
			SAML Setup
Generate new certificate			Single Sign On using SAML will not work until you configure the app to
	Fynires Statue	Actions	trust Okta as an IdP.

View SAML setup instructions

Actions •

Laat deze pagina open voor toekomstig gebruik of kopieer de **Identity Provider Single Sign-On URL** en **Identity Provider Issuer** en download het **X.509 Certificaat**:

Inactive 💧

Oct 2022

SHA-1

Oct 2032

The following is needed to configure Bitwarden

Identity Provider Single Sign-On URL:

 https://bitwardenhelptest.okta.com/app/bitwardenhelptest_bitwarden_1/exk3fajwkMx07SosA696/sso/saml

 Identity Provider Issue:

 http://www.okta.com/exk3fajwkMx07SosA696

 Sog Certificate:

 Http://compake/BajlGXXxx2SishMAABOCSgoSIbJSDQEBCcwUAMIGZMQsw0QYDVQQEw_JVLkETMBEG
 AUGCAwkQ2FsawZvcm5pTTEWHBQ0ALUEBwwMU2FulEZyWb5jaXMjbzeRMAASALUEQWETZUETWEIG
 Ide Values

Opdrachten

Navigeer naar het tabblad Toewijzingen en selecteer de knop Toewijzen:

Search		
3ack to Applicat	Bitwarden Login with SSO	
Ø	Active View Logs Monitor Imports	
ieneral Sig	n On Import Assignments	
Assign 🔻	✓ Convert Assignments Q Search Groups ▼	REPORTS
ilters	Priority Assignment	
eople iroups	1 Everyone \checkmark X All users in your organization	•••x Recent Unassignments
		SELF SERVICE
		You need to enable self service for org managed apps before you can use self service for this app
		ioi ano appi
		Go to self service
		Go to self service settings
		Go to self service settings Requests Disabled

Je kunt toegang tot de applicatie per gebruiker toewijzen met de optie **Aan personen toewijzen**, of in één keer met de optie **Aan** groepen toewijzen.

Terug naar de webapp

Op dit punt hebt u alles geconfigureerd wat u nodig hebt binnen de context van het Okta Admin 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 Okta Admin Portal tijdens het maken van de app:

Veld	Beschrijving
Naam ID Formaat	Stel dit in op het Name ID-formaat dat is opgegeven in Okta, laat anders Unspecified staan.
Algoritme voor uitgaande ondertekening	Het algoritme dat Bitwarden gebruikt om SAML-verzoeken te ondertekenen.
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden.
Algoritme voor minimale inkomende ondertekening	Stel dit in op het handtekeningalgoritme dat is opgegeven in Okta.
Ondertekende beweringen	Schakel dit selectievakje in als u het veld Assertion Signature hebt ingesteld op Signed in Okta.
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

Bij het configureren van identiteitsaanbieders moet u vaak teruggaan naar het Okta Admin Portal om applicatiewaarden op te halen:

Veld	Beschrijving
Entiteit ID	Voer uw Identity Provider Issuer in, opgehaald uit het Okta Sign On Settings-scherm door de knop View Setup Instructions te selecteren. Dit veld is hoofdlettergevoelig.
Type binding	Instellen op omleiden . Okta ondersteunt momenteel geen HTTP POST.

Veld	Beschrijving
URL voor service voor eenmalige aanmelding	Voer uw Identity Provider Single Sign-On URL in, opgehaald uit het Okta Sign On Settings- scherm.
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	Plak het gedownloade certificaat, verwijder BEGIN CERTIFICAAT en END CERTIFICAAT De certificaatwaarde is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens zorgen ervoor dat de certificatievalidatie mislukt .
Algoritme voor uitgaande ondertekening	Selecteer het handtekeningalgoritme dat is geselecteerd tijdens de configuratie van de Okta-app. Als u het handtekeningalgoritme niet hebt gewijzigd, laat u de standaardwaarde (<mark>rsa-sha256</mark>) staan.
Uitgaande afmeldverzoeken toestaan	Inloggen met SSO ondersteunt momenteel geen SLO.
Authenticatieverzoeken ondertekend willen hebben	Of Okta verwacht dat SAML-verzoeken worden ondertekend.

(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.

Als je klaar bent met de configuratie van de identity provider, sla je je werk **op**.

⊘ 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:



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 inlogscherm voor Okta:

okta	
Sign In	
Username	
Password	
Remember me	
Sign In	
Need help signing in?	

			<u> </u>
 $\cap \alpha$	In I	with	()kto
 UE		VVILII	UNLA
0			

Nadat u zich hebt geverifieerd met uw Okta-referenties, voert u uw Bitwarden-masterwachtwoord in om uw kluis te ontsleutelen!

(i) Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an Okta Bookmark App that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.

- 2. Click Browse App Catalog.
- 3. Search for Bookmark App and click Add Integration.
- 4. Add the following settings to the application:
 - 1. Give the application a name such as **Bitwarden Login**.
 - 2. In the **URL** field, provide the URL to your Bitwarden client such as <a href="https://vault.bitwarden.com/#/login.c
- 5. Select **Done** and return to the applications dashboard and edit the newly created app.
- 6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained here.

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.