BEHEERCONSOLE > INLOGGEN MET SSO

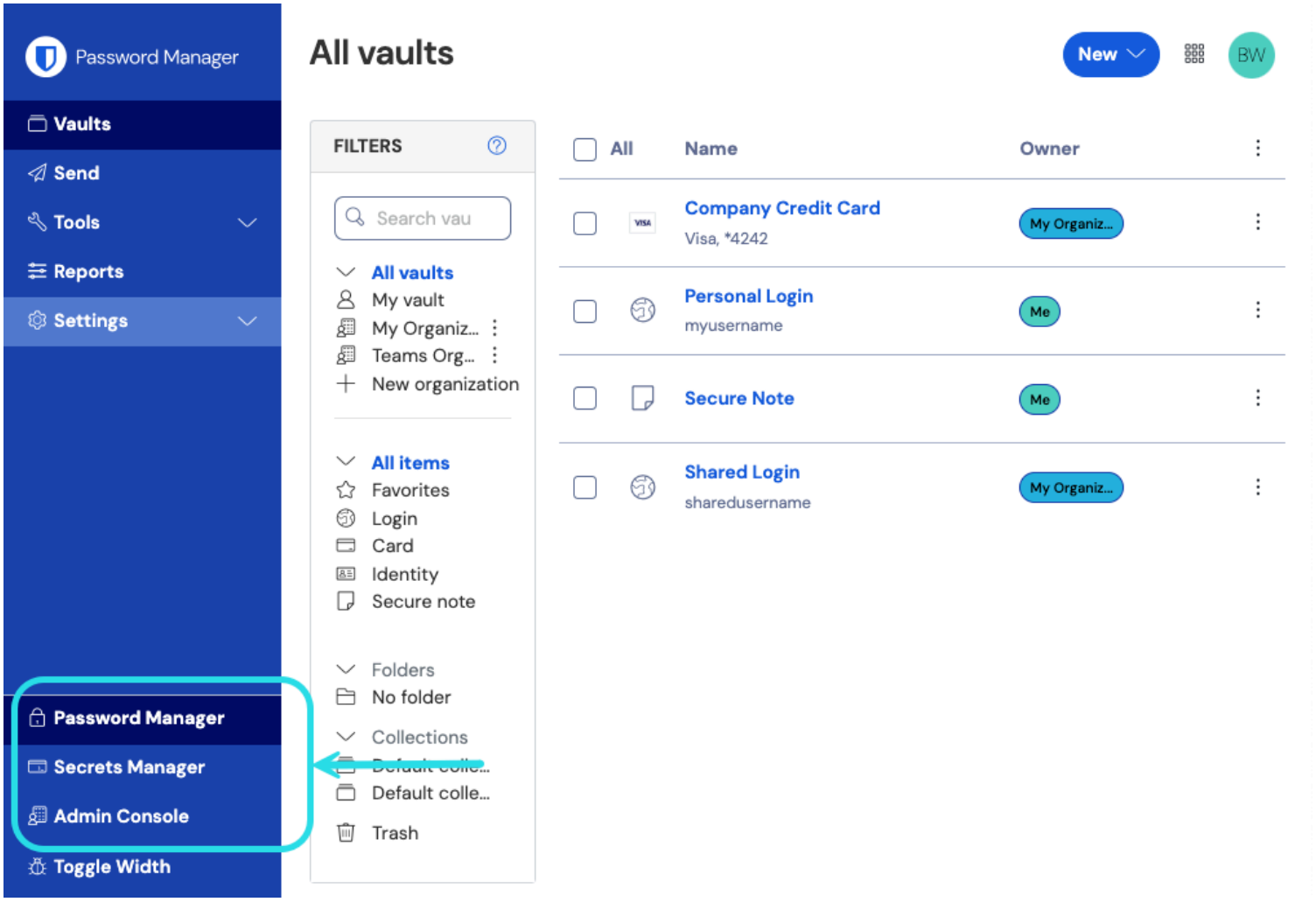
SAML 2.0 configuratie

SAML 2.0 configuratie

Stap 1: Stel een SSO-identifier in

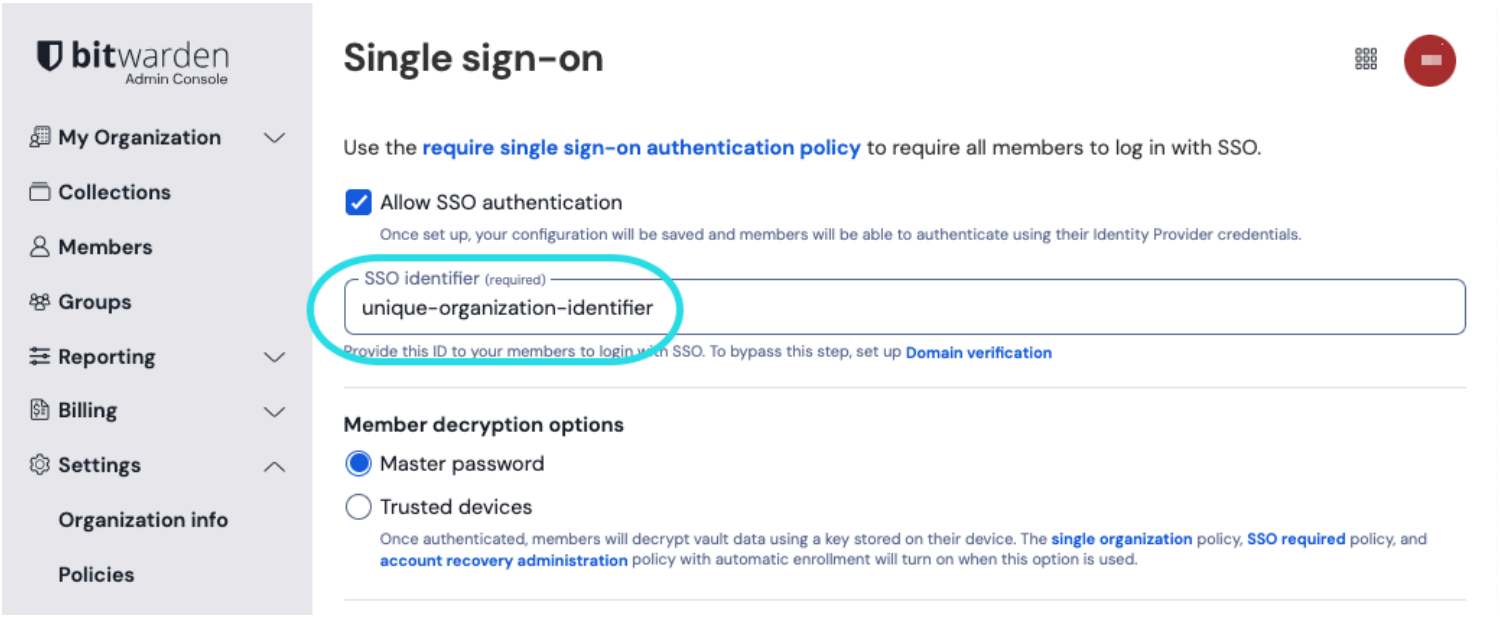
Gebruikers die hun identiteit authenticeren met behulp van SSO moeten een **SSO-identifier** invoeren die de organisatie (en dus de SSO-integratie) aangeeft waartegen ze zich moeten authenticeren. Om een unieke SSO Identifier in te stellen:

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



Product switcher

2. Navigeer naar **Instellingen** → **Eenmalige aanmelding** en voer een unieke **SSO-identificatie** in voor uw organisatie:



Voer een identificator in

3. Ga verder met **Stap 2: Aanmelden met SSO inschakelen**.

> **Tip**
> You will need to share this value with users once the configuration is ready to be used.

Stap 2: Inloggen met SSO inschakelen

Als je eenmaal je SSO identifier hebt, kun je verder gaan met het inschakelen en configureren van je integratie. Aanmelden met SSO inschakelen:

1. Schakel in de weergave **Instellingen** → **Eenmalige aanmelding** het selectievakje **SSO-authenticatie toestaan** in:

SAML 2.0 configuratie

2. Selecteer in het vervolgkeuzemenu **Type** de optie **SAML 2.0**. Als je in plaats daarvan OIDC wilt gebruiken, ga dan naar de OIDC Configuratiegids.

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.

Stap 3: Configuratie

Vanaf dit punt varieert de implementatie van aanbieder tot aanbieder. Ga naar een van onze specifieke **implementatiehandleidingen** voor hulp bij het voltooien van het configuratieproces:

Aanbieder	Gids
AD FS	AD FS implementatiegids
Auth0	Auth0 Implementatiegids
AWS	AWS-implementatiegids
Azuur	Azure Implementatiegids
Duo	Duo Implementatie Gids
Google	Google Implementatiegids
JumpCloud	JumpCloud implementatiegids
Sleutelhanger	Keycloak implementatiegids
Okta	Okta-implementatiegids
OneLogin	OneLogin implementatiegids
PingFederate	PingFederate implementatiegids

Configuratie referentiemateriaal

De volgende secties definiëren velden die beschikbaar zijn tijdens de configuratie van single sign-on, onafhankelijk van de IdP waarmee je integreert. Velden die moeten worden geconfigureerd, worden gemarkeerd**(verplicht)**.

> **Tip**
>
> **Unless you are comfortable with SAML 2.0**, we recommend using one of the above implementation guides instead of the following generic material.

Het eenmalige aanmeldingsscherm verdeelt de configuratie in twee secties:

- **SAML Service Provider Configuration** bepaalt het formaat van SAML verzoeken.
- **SAML Identity Provider Configuration** bepaalt het formaat dat wordt verwacht voor SAML antwoorden.

Configuratie serviceprovider

Veld	Beschrijving
SP entiteit ID	**(Wordt automatisch gegenereerd)** Het Bitwarden eindpunt voor verificatieverzoeken. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen** → **Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van uw instelling.
SAML 2.0 URL metagegevens	**(Wordt automatisch gegenereerd)** Metadata URL voor het Bitwarden eindpunt. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen** → **Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van uw instelling.
URL Assertion Consumentenservice (ACS)	**(Wordt automatisch gegenereerd)** Locatie waar de SAML-bevestiging van de IdP naartoe wordt gestuurd. Deze automatisch gegenereerde waarde kan worden gekopieerd vanuit het **Instellingen** → **Enkelvoudige aanmelding** scherm van de organisatie en zal variëren afhankelijk van uw instelling.
Naam ID Formaat	Formaat dat Bitwarden vraagt van de SAML-bevestiging. Moet worden gecast als een tekenreeks. Opties zijn onder andere: -Niet gespecificeerd (standaard) E-mailadres -X.509 Onderwerpnaam -Windows Domeinnaam -Kerberos hoofdnaam -Identificatiecode van entiteit -Persistent -Transient

Veld	Beschrijving
Algoritme voor uitgaande ondertekening	Het algoritme dat Bitwarden gebruikt om SAML-verzoeken te ondertekenen. Opties zijn onder andere: - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (standaard) - http://www.w3.org/2000/09/xmldsig#rsa-sha1 - http://www.w3.org/2000/09/xmldsig#rsa-sha384 - http://www.w3.org/2000/09/xmldsig#rsa-sha512
Ondertekengedrag	Of/wanneer SAML verzoeken ondertekend zullen worden. Opties zijn onder andere: -Als IdP wil dat authn-verzoeken worden ondertekend (standaard) -Altijd -Nooit
Algoritme voor minimale inkomende ondertekening	Minimale sterkte van het algoritme dat Bitwarden accepteert in SAML-reacties.
Verwacht ondertekende beweringen	Vink dit selectievakje aan als Bitwarden moet verwachten dat antwoorden van de IdP worden ondertekend.
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.

Configuratie Identity Provider

Veld	Beschrijving
Entiteit ID	**(Verplicht)** Adres of URL van uw identiteitsserver of de IdP Entity ID. Dit veld is hoofdlettergevoelig en moet exact overeenkomen met de IdP-waarde.
Type binding	Methode gebruikt door de IdP om te reageren op Bitwarden SAML-verzoeken. Opties zijn onder andere: -Redirect (aanbevolen) -HTTP POST

Veld	Beschrijving
URL voor service voor eenmalige aanmelding	**(Verplicht als Entity ID geen URL** is) SSO-URL uitgegeven door uw IdP.
URL voor service voor eenmalig afmelden	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstig gebruik, maar we raden sterk aan om dit veld vooraf te configureren.

X509 publiek certificaat	**(Verplicht**) De X.509 Base-64 gecodeerde certificaatinstantie. Neem de
	
	`-----BEGIN CERTIFICAAT-----`
	
	en
	
	`-----END CERTIFICAAT-----`
	
	regels of delen van het CER/PEM-geformatteerd certificaat.
	
	De certificaatwaarde is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens in dit veld zorgen ervoor dat de certificaatvalidatie mislukt. Kopieer **alleen** de certificaatgegevens naar dit veld.

Algoritme voor uitgaande ondertekening	Het algoritme dat uw IdP zal gebruiken om SAML antwoorden/bevestigingen te ondertekenen. Opties zijn onder andere: - `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256` (standaard) - `http:/`/www.w3.org/2000/09/xmldsig#rsa-sha1 - `http:/`/www.w3.org/2000/09/xmldsig#rsa-sha384 - `http:/`/www.w3.org/2000/09/xmldsig#rsa-sha512
Uitgaande afmeldverzoeken toestaan	Inloggen met SSO ondersteunt momenteel **geen** SLO. Deze optie is gepland voor toekomstig gebruik, maar we raden sterk aan om dit veld vooraf te configureren.
Verificatieverzoeken ondertekenen	Vink dit selectievakje aan als je IdP moet verwachten dat SAML-verzoeken van Bitwarden 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.

SAML-kenmerken en claims

Voor account provisioning is een **e-mailadres** nodig, dat kan worden doorgegeven als een van de attributen of claims in de volgende tabel.

Een unieke gebruikersidentificatie wordt ook ten zeerste aanbevolen. Als dit niet het geval is, wordt in plaats daarvan e-mail gebruikt om de gebruiker te linken.

Attributen/claims worden vermeld in volgorde van voorkeur voor overeenkomst, inclusief eventuele fallbacks:

Waarde	Claim/Attribuut	Terugvalclaim/attribuut
Uniek ID	NameID (indien niet van voorbijgaande aard) urn:oid:0.9.2342.19200300.100.1.1 Sub UID UPN EPPN	
E-mail	E-mail http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress urn:oid:0.9.2342.19200300.100.1.3 Mail E-mailadres	Voorkeur gebruikersnaam Urn:oid:0.9.2342.19200300.100.1.1 UID
Naam	Naam http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 Weergavenaam CN	Voornaam + " " + Achternaam (zie hieronder)
Voornaam	urn:oid:2.5.4.42 Voornaam Voornaam FN FN-naam Bijnaam	
Achternaam	urn:oid:2.5.4.4 SN Achternaam Achternaam	