

BEHEERCONSOLE > INLOGGEN MET SSO >

SAML-implementatie van Keycloak

SAML-implementatie van Keycloak

Dit artikel bevat **Keycloak-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 Keycloak 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.

[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 (🗄️):

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card	My Organiz...	⋮
<input type="checkbox"/>		Visa, *4242		⋮
<input type="checkbox"/>		Personal Login	Me	⋮
<input type="checkbox"/>		myusername		⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>				⋮
<input type="checkbox"/>		Shared Login	My Organiz...	⋮
<input type="checkbox"/>		sharedusername		⋮

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.

Tip

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

Keycloak instellen

Log in op Keycloak en selecteer **Clients** → **Client aanmaken**.

Clients
Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list | Initial access token | Client registration

Search for client → **Create client** | Import client

Client ID	Name	Type	Description	Home URL
account	`\${client_account}`	OpenID Connect	–	
account-console	`\${client_account-console}`	OpenID Connect	–	
admin-cli	`\${client_admin-cli}`	OpenID Connect	–	–
broker	`\${client_broker}`	OpenID Connect	–	–
master-realm	master Realm	OpenID Connect	–	–
security-admin-console	`\${client_security-admin-...}`	OpenID Connect	–	

Create a Client

Vul in het scherm Client aanmaken de volgende velden in:

Veld	Beschrijving
Type klant	Selecteer SAML.
Klant-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.
Naam	Voer een naam naar keuze in voor de Keycloak-client.

Klik op **Volgende** wanneer u de verplichte velden op de pagina **Algemene instellingen** hebt ingevuld.

Vul het volgende veld in op het scherm **Aanmeldingsinstellingen**:

Veld	Beschrijving
Geldige omleidings-URL's	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.

Selecteer **Opslaan**.

Selecteer het tabblad Keys en zet de optie **Client signature required** op **Off**.

The screenshot shows the Keycloak interface for a client. On the left is a dark sidebar with a menu where 'Clients' is highlighted. The main content area shows 'Client details' for a client with ID 'mat.bitwarden.support/sso/saml2'. The 'Keys' tab is selected. In the 'Signing keys config' section, the 'Client signature required' toggle is turned off. The URL 'https://mat.bitwarden.support/sso/saml2' is shown with a 'SAML' label and an 'Enabled' status. The 'Action' dropdown is visible in the top right.

Keycloak Keys Config

Ten slotte selecteer je in de hoofdnavigatie van Keycloak **Realm-instellingen** en vervolgens het tabblad **Keys**. Zoek het **RS256-certificaat** en selecteer **Certificaat**.

Keys list Providers

Active keys Search key 1 - 4

Algorithm	Type	Kid	Use	Provider	Public keys
AES	OCT	a3282835-06db-42cc-b29a-ff969226eca9	ENC	aes-generated	
HS256	OCT	be68f437-88a6-4c3b-b92f-bf3b114beeb6	SIG	hmac-generated	
RSA-OAEP	RSA	zXKBNvtriZQU7MbyXJlIf60wGotgDbZwpG8_x7wE1QQ	ENC	rsa-enc-generated	Public key Certificate
RS256	RSA	T3IREov-EMgD0EnJ5AsHsv0GX-Z0s89jCyl0y6fmlsE	SIG	rsa-generated	Public key Certificate

1 - 4

Keycloak RS256 Certificate

De waarde voor het certificaat is nodig voor het volgende gedeelte.

Terug naar de webapp

Op dit punt heb je alles geconfigureerd wat je nodig hebt binnen de context van het Keycloak Portal. Ga terug naar de Bitwarden web app en selecteer **Instellingen** → **Eenmalige aanmelding** in de navigatie.

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.

Vul de volgende velden in de **SAML service provider configuratie** sectie in:

Veld	Beschrijving
Naam ID-indeling	Selecteer e-mail .
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	Selecteer het algoritme dat de Keycloak client gebruikt om SAML documenten of asserties te ondertekenen .
Ondertekende beweringen	Of Bitwarden verwacht dat SAML–asserties worden ondertekend. Als dit aan staat, zorg er dan voor dat je de Keycloak client configureert om asserties te ondertekenen .
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.

Vul de volgende velden in de **SAML identity provider configuratiesectie** in:

Veld	Beschrijving
Entiteit ID	Voer de URL in van de Keycloak realm waarop de client is aangemaakt, bijvoorbeeld http s://werelden/ . Dit veld is hoofdlettergevoelig.
Bindend type	Selecteer Omleiden .
URL voor service voor eenmalige aanmelding	Voer je master SAML-verwerkings-URL in, bijvoorbeeld https://werelden/protocol/saml .
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 met uw URL voor afmelden .
X509 publiek certificaat	Voer het RS256–certificaat in dat in de vorige stap is gekopieerd. De certificaatwaarde is hoofdlettergevoelig, extra spaties, carriage returns en andere vreemde tekens zorgen ervoor dat de certificaatvalidatie mislukt .

Veld	Beschrijving
Algoritme voor uitgaande ondertekening	Selecteer het algoritme dat de Keycloak client gebruikt om SAML documenten of asserties te ondertekenen.
Uitgaande afmeldverzoeken uitschakelen	Inloggen met SSO ondersteunt momenteel geen SLO. Deze optie is gepland voor toekomstige ontwikkeling.
Authenticatieverzoeken ondertekend willen hebben	Of Keycloak 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.

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](#).

Extra Keycloak-instellingen

Op het tabblad Keycloak Client **Instellingen** zijn extra configuratieopties beschikbaar:

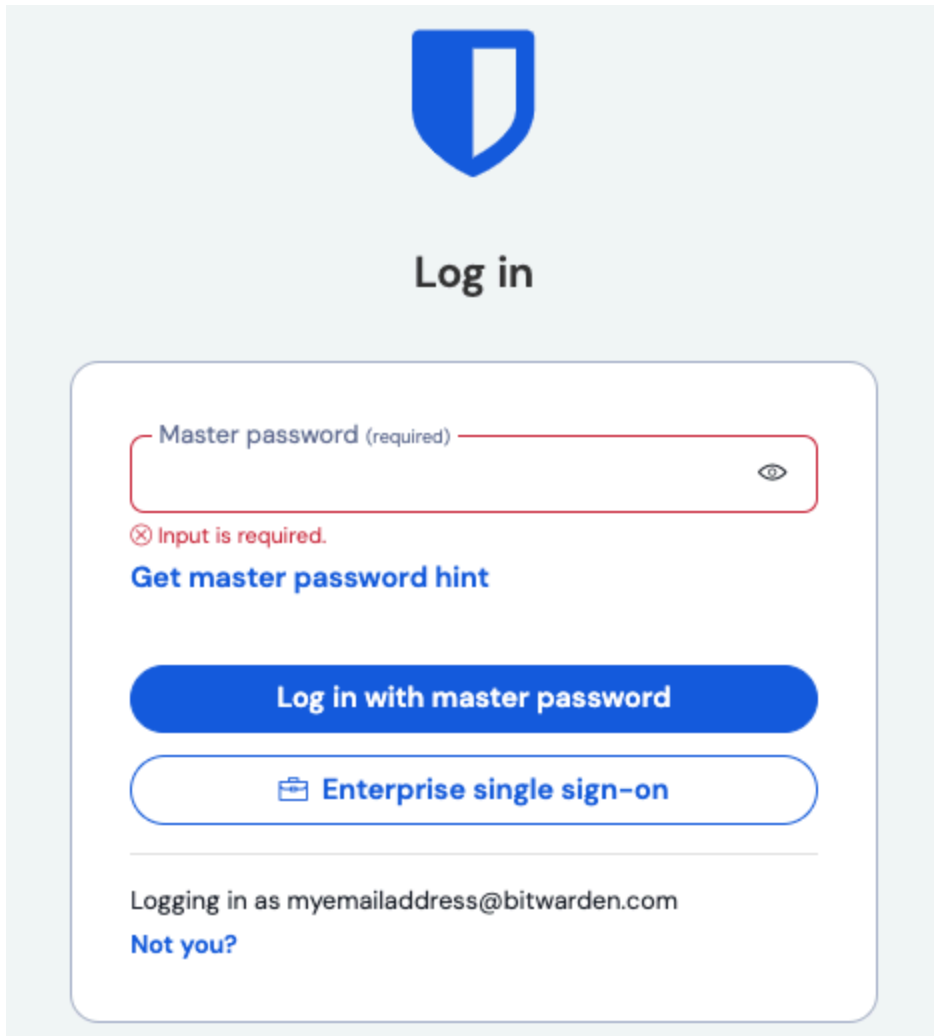
Veld	Beschrijving
Documenten ondertekenen	Geef aan of SAML-documenten ondertekend moeten worden door de Keycloak realm.
Beweringen ondertekenen	Geef aan of SAML-bevestigingen moeten worden ondertekend door de Keycloak realm.
Handtekening algoritme	Als Ondertekenen van beweringen is ingeschakeld, selecteer dan met welk algoritme moet worden ondertekend (standaard sha-256).

Veld	Beschrijving
Naam ID Formaat	Selecteer het Name ID-formaat voor Keycloak om te gebruiken in SAML-reacties.

Als je het forum hebt ingevuld, selecteer je **Opslaan**.

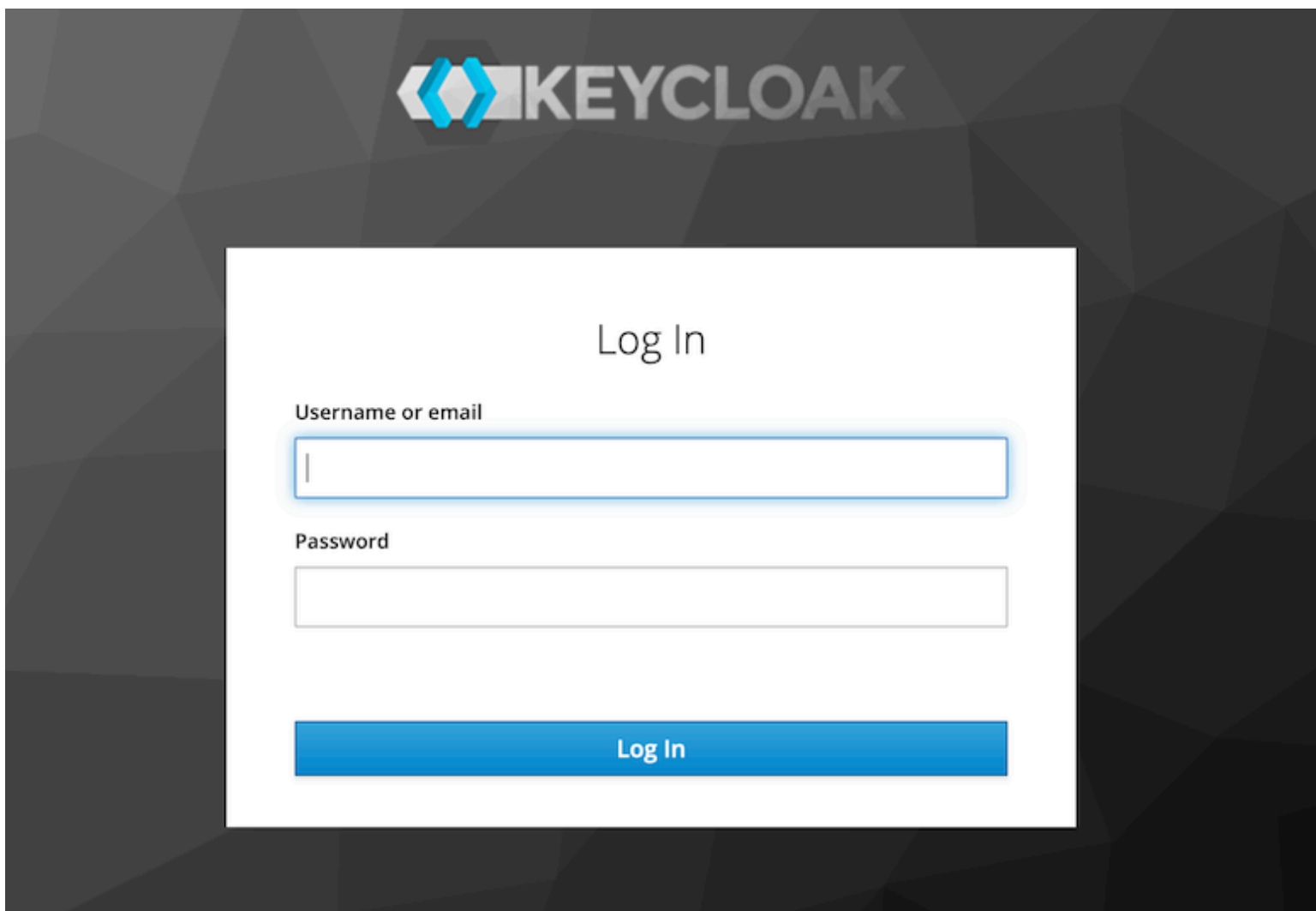
De configuratie testen

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 inlogscherf van Keycloak:



Keycloak Login Screen

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

Note

Bitwarden ondersteunt geen ongevroegde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSO-aanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden.