

BEHEERCONSOLE > INLOGGEN MET SSO

Inloggen met SSO veelgestelde vragen

Inloggen met SSO veelgestelde vragen

Dit artikel bevat veelgestelde vragen (FAQ's) over **inloggen met SSO**.

Voor meer informatie op hoog niveau over **inloggen met SSO**, zie [over inloggen met SSO](#)

Inloggen met SSO

V: Waarom is voor inloggen met SSO mijn hoofdwachtwoord nodig?

A: Inloggen met SSO stelt uw werknemers in staat om uw bestaande identiteitsprovider (IdP) te gebruiken om hun identiteiten **te verifiëren**. Wat inloggen met SSO uniek maakt ten opzichte van andere tools is dat het ons end-to-end zero knowledge encryptie model behoudt. Niemand bij Bitwarden mag toegang hebben tot uw kluisgegevens en, nog belangrijker, **ook uw identiteitsleverancier** niet.

Daarom ontkoppelt het Bitwarden login met SSO-aanbod **authenticatie en ontsleuteling**. Je IdP kan bevestigen dat Alice in feite Alice is, maar kan en mag niet over de tools beschikken om de kluis van Alice te ontsleutelen. Alleen Alice kan dat gereedschap hebben en, heel handig, het is haar hoofdwachtwoord!

In de praktijk betekent dit dat wanneer een medewerker inlogt bij Bitwarden via SSO, hij zijn hoofdwachtwoord moet gebruiken om de kluis te ontsleutelen, waardoor de kritieke gegevens en geheimen van uw bedrijf worden beschermd.

Note

Bitwarden offers two solutions for organizations that will allow approved organization members to access their Bitwarden account without using a master password:

SSO with trusted device is a feature that allows organizations using login with SSO to create and store member device encryption keys, eliminating the need to enter a master password. Learn more about [SSO with trusted devices](#).

Organizations self-hosting Bitwarden can leverage [Key Connector](#) to serve decryption keys to Bitwarden clients instead of requiring users to decrypt vault data with their master passwords. Learn more [here](#) and [here](#).

V: Heeft het wijzigen van mijn SSO-wachtwoord invloed op mijn Bitwarden-hoofdwachtwoord?

A: Nee, je hoofdwachtwoord blijft hetzelfde. Tenzij uw organisatie [Key Connector](#) gebruikt om zelf ontcijferingssleutels te hosten, moet uw hoofdwachtwoord worden gebruikt om kluisgegevens te ontcijferen.

V: Vervangt SSO-verificatie mijn hoofdwachtwoord en e-mail?

A: Nee. Inloggen met SSO maakt gebruik van uw bestaande identiteitsprovider (IdP) om u te verifiëren in Bitwarden, maar uw hoofdwachtwoord en e-mailadres moeten nog steeds worden ingevoerd om uw kluisgegevens te ontsleutelen, tenzij uw organisatie [Key Connector](#) gebruikt om zelf ontsleutelingscodes te hosten.

V: Kan ik nog steeds inloggen met mijn hoofdwachtwoord als mijn organisatie SSO heeft ingeschakeld?

A: Standaard kunt u uw e-mailadres en hoofdwachtwoord gebruiken om in te loggen bij Bitwarden. Als je organisatie echter zowel het verificatiebeleid voor **één organisatie** als [Single sign-on](#) inschakelt, of als je organisatie [Key Connector](#) gebruikt, moeten alle niet-beheerders zich aanmelden met SSO.

V: Hoe werkt inloggen met SSO voor nieuwe gebruikers ("just-in-time")?

A: Nieuwe gebruikers die **Log in** → **Enterprise SSO** selecteren vanuit de organisatie-uitnodiging krijgen de status **Geaccepteerd** van hun organisatie totdat ze worden bevestigd door een beheerder. Wanneer die gebruiker handmatig of via [Directory Connector](#) wordt toegewezen aan een groep, krijgt hij toegang tot de juiste gedeelde items. JIT provisioning wordt aanbevolen als je leden zonder hoofdwachtwoord wilt hebben die alleen [vertrouwde apparaten](#) kunnen gebruiken.

V: Moet ik Bitwarden Directory Connector nog gebruiken?

A: Als u uw Bitwarden groep- en verzameltoewijzingen rechtstreeks binnen Bitwarden beheert, is het niet nodig om gebruik te maken van de Directory Connector. Als je echter groepen en gebruikers automatisch wilt synchroniseren met de directory van je organisatie, raden we je aan om login met SSO te gebruiken in combinatie met Directory Connector voor de meest complete oplossing.

V: Moet ik mijn SSO-ID elke keer invoeren als ik inlog?

A: Nee! Als je organisatie [domeinverificatie](#) gebruikt, hoeft je deze identificatie niet in te voeren. Anders kunt u een bladwijzer maken voor de **Enterprise Single Sign-On** pagina met uw SSO-ID als een querystring, zodat u deze niet elke keer opnieuw hoeft in te voeren. Bijvoorbeeld:

- <https://vault.bitwarden.com/#/sso?identificer=your-org-id> voor cloud-hosted instanties
- <https://your.domain.com/#/sso?identificer=your-org-id> voor zelf gehoste instanties

V: Hoe wijzig ik vooraf gegenereerde SSO-configuratiewaarden?

A: Vooraf gegenereerde SSO-configuratiewaarden waaronder **SP Entity ID**, **SAML 2.0 Metadata URL**, **ACS URL** en **Callback Path** kunnen in zelfgehoste omgevingen worden gewijzigd door de `url:` waarde in `.bwdata/config.yml` te wijzigen en het commando `./bitwarden.sh rebuild` uit te voeren om uw wijziging toe te passen.

Beveiliging

V: Hoe werkt inloggen met SSO met het nul-kennis coderingsmodel?

A: Bitwarden login met SSO & hoofdwachtwoord voert alleen gebruikersauthenticatie uit en ontsleutelt geen gebruikersgegevens. Het toevoegen van SSO-functionaliteit introduceert geen verdere individueel identificeerbare informatie in de Bitwarden-database.

Facturering

V: Welke plannen bieden aanmelding met SSO?

A: Ons Enterprise-plan biedt deze functie.

V: Hoe kan ik mijn abonnement upgraden zodat ik kan inloggen met SSO?

A: Navigeer in de beheerconsole naar de pagina **Abonnementen** → **Facturering** en selecteer **Upgradeplan**. We raden je ten eerste aan om het inloggen met SSO te testen door een [7-daagse Enterprise Free Trial](#) te starten.

Ondersteunbaarheid

V: Ondersteunt Bitwarden OAuth 2.0?

A: Bitwarden ondersteunt OpenID Connect, maar op dit moment nog geen OAuth.

V: Werkt inloggen met SSO ook met een zelf gehoste instantie van Bitwarden?

A: Ja! Inloggen met SSO werkt met zelf gehoste instanties, ongeacht of ze zich op locatie of in je eigen cloud bevinden, zolang je identiteitsserver bereikbaar is vanaf de instantie.

V: Werkt inloggen met SSO in hybride cloudomgevingen?

A: Ja! Inloggen met SSO vereist alleen de mogelijkheid om verbinding te maken met uw identity provider vanuit uw Bitwarden instantie. Het kan worden gebruikt met cloud- of on-premise identity providers, evenals cloud- of zelf gehoste Bitwarden-instanties.

V: Als mijn identity provider offline is, kunnen gebruikers dan inloggen met SSO om zich te authenticeren in Bitwarden?

A: Als je identity provider offline is, moeten gebruikers inloggen met hun e-mailadres en hoofdwachtwoord. Dit kan in de toekomst veranderen als we meer mechanismen voor authenticatiecontrole voor organisaties mogelijk maken.