

BEHEERCONSOLE > INLOGGEN MET SSO

Decryptie-opties voor leden

Decryptie-opties voor leden

Wat Login met SSO uniek maakt is dat het ons zero-knowledge encryptie model behoudt. Niemand bij Bitwarden heeft toegang tot uw kluisgegevens en hetzelfde **geldt voor uw identiteitsleverancier**. Daarom ontkoppelt inloggen met SSO **authenticatie en ontsleuteling**. In alle aanmeldingen met SSO-implementaties kan en zal uw identiteitsleverancier geen toegang hebben tot de ontcijferingssleutel die nodig is om kluisgegevens te ontsleutelen.

Lid ontsleutelingsopties worden gebruikt om te bepalen welke ontsleutelingsleutel gebruikt zal worden om kluisgegevens te ontsleutelen in scenario's waar SSO de authenticatie afhandelt. Opties zijn onder andere:

- **Hoofdwachtwoord:** Na authenticatie zullen organisatielieden kluisgegevens ontsleutelen met behulp van hun [hoofdwachtwoord](#).
- **Vertrouwde apparaten:** Hiermee kunnen gebruikers zich verifiëren met SSO en hun kluis ontsleutelen met behulp van een versleutelingscode die op het apparaat is opgeslagen, zodat er geen hoofdwachtwoord hoeft te worden ingevoerd. [Meer informatie](#).
- **Sleutelconnector:** Verbind login met SSO met uw zelf gehoste ontcijferingssleutelserver. Met deze optie hoeven organisatielieden hun hoofdwachtwoord niet te gebruiken om kluisgegevens te ontsleutelen. In plaats daarvan haalt [Key Connector](#) een ontcijferingssleutel op die veilig is opgeslagen in een database die jouw eigendom is en door jou wordt beheerd.

Tip

Due to the sensitivity of storing decryption keys, the **Key Connector** option is disabled by default and currently only available to organizations self-hosting Bitwarden.

If you're interesting in using Key Connector, check out the [About Key Connector](#) and [Deploy Key Connector](#) articles and [contact us](#) to setup a time for us to help you get started.