RESOURCE CENTER

Enterprise referentiegids voor Bitwarden-authenticatie

Kritische mogelijkheden van het Bitwarden-verificatie- en SSO-aanbod toelichten

Get the full interactive view at https://bitwarden.com/nl-nl/resources/reference-guide-bitwarden-authentication/

bitwarden

Type verificatie	Wat is het?	Overwegingen bij de implementatie *Alle opties voor het gebruik van authenticatie zijn in lijn met het Bitwarden end-to-end, zero knowledge encryptiemodel*
SSO met vertrouwde apparaten	Voor een wachtwoordloze ervaring gebruiken werknemers hun SSO-referenties om zich in één stap te verifiëren en te ontsleutelen. Geregistreerde, vertrouwde apparaten kunnen vaults ontsleutelen en nieuwe apparaten bevestigen en accepteren. Als een apparaat eenmaal is vertrouwd, hoeft het niet meer te worden goedgekeurd.	Door deze optie te selecteren kunnen werknemers inloggen en hun kluis ontsleutelen zonder dat ze een wachtwoord nodig hebben. Vertrouwde apparaten worden geregistreerd en kunnen aanmeldingen bevestigen en het vertrouwen uitbreiden naar andere apparaten. Bij het aanmaken van een account zal de SSO-provider de gebruiker authenticeren en de aanmeldcliënt registreren als het eerste vertrouwde apparaat, waardoor deze de kluis kan ontsleutelen. Extra vertrouwde apparaten kunnen worden geregistreerd met goedkeuring van de Bitwarden desktop app, mobiele app, web app of door een Bitwarden beheerder. Elk vertrouwd apparaat heeft een individuele apparaatcoderingssleutel en end-to-end codering en beveiliging van nul-kennis wordt gehandhaafd op alle apparaten. Extra bronnen: SSO instellen met vertrouwde apparaten Zakelijke wachtwoordloze SSO zorgt voor betere productiviteit en gebruikerservaring voor werknemers
Inloggen met SSO	Gebruikersauthenticatie wordt gescheiden van kluisdecodering door gebruik te maken van de identiteitsprovider van uw bedrijf om gebruikers te authenticeren in hun Bitwarden-kluis en hoofdwachtwoorden te gebruiken voor het decoderen van kluisgegevens.	Deze optie ondersteunt identiteitsproviders die de standaarden SAML 2.0 of OpenID Connect gebruiken. Als u deze optie selecteert, betekent dit dat wanneer een medewerker inlogt bij Bitwarden met behulp van SSO, hij zijn hoofdwachtwoord moet gebruiken om de kluis te ontsleutelen, waardoor de kritieke gegevens en geheimen van uw bedrijf worden beschermd. Extra bronnen:

Type verificatie	Wat is het?	Overwegingen bij de implementatie *Alle opties voor het gebruik van authenticatie zijn in lijn met het Bitwarden end-to-end, zero knowledge encryptiemodel*
Inloggen met SSO en door de klant beheerde encryptie	Werknemers gebruiken hun SSO-referenties om zich in één stap te verifiëren en te ontsleutelen. Deze optie verschuift het bewaren van de hoofdwachtwoorden van gebruikers naar bedrijven die een sleutelconnector moeten implementeren om de gebruikerssleutels op te slaan.	Uw organisatie configureren met Inloggen met SSO Inloggen met SSO instellen Voor bedrijven met breed geaccepteerde SSO-implementaties en de wens om authenticatie en ontsleuteling te integreren in een on-premise oplossing, biedt Bitwarden SSO met door de klant beheerde versleuteling. In dit scenario beheren bedrijven een key connector agent. Hiervoor is een verbinding met een database nodig die versleutelde gebruikerssleutels opslaat en een RSA sleutelpaar om die sleutels te versleutelen en te ontsleutelen. Deze aanpak handhaaft een zero knowledge-encryptiearchitectuur omdat er op geen enkel punt ontcijferingssleutels door Bitwarden-servers gaan. Het beheer van cryptografische sleutels is ongelooflijk gevoelig en wordt alleen aanbevolen voor bedrijven met een team en een infrastructuur die al op een veilige manier een keyserver heeft geïmplementeerd en beheerd. SSO met door de klant beheerde encryptie is beschikbaar voor klanten die Bitwarden zelf hosten. Extra bronnen: Whitepaper: Kies de juiste SSO aanmeldstrategie Hulpartikel: Inloggen met SSO en klantbeheer Encryptie - de sleutelconnector inzetten
Inloggen met Bitwarden	Werknemers gebruiken hun e-mailadres en hoofdwachtwoord om in te loggen en hun Bitwarden-kluis te ontsleutelen.	Voor bedrijven die snel aan de slag willen, biedt inloggen met Bitwarden werknemers de mogelijkheid om hun unieke e-mailadres en hoofdwachtwoord te gebruiken om toegang te krijgen tot hun kluis. Het is perfect voor bedrijven die authenticatie nog niet

Type verificatie	Wat is het?	Overwegingen bij de implementatie *Alle opties voor het gebruik van authenticatie zijn in lijn met het Bitwarden end-to-end, zero knowledge encryptiemodel*
		centraal beheren of een identiteitsprovider gebruiken. Beheerders kunnen werknemers handmatig uitnodigen voor Organisaties en gedeelde verzamelingen, of de Bitwarden Directory Connector gebruiken om LDAP-groepen te synchroniseren. Extra bronnen: Vijf best practices voor wachtwoordbeheer Aan de slag met Bitwarden
Inloggen met apparaat	Werknemers gebruiken hun e-mail om in te loggen en bevestigen vervolgens de inlog vanaf een tweede, geverifieerd apparaat (mobiele app of desktop app) dat de encryptiesleutel van de kluis veilig deelt na goedkeuring.	Inloggen met apparaat is een optie die beschikbaar is voor alle werknemers nadat ze ten minste één keer op het apparaat hebben ingelogd met e-mail en hoofdwachtwoord. Hierdoor kunnen medewerkers snel weer inloggen op al hun Bitwarden-klanten nadat ze eerst zijn ingelogd op hun mobiele of desktop app. Extra bronnen: Help-artikel: Inloggen met apparaat