

Bitwarden Verklarende woordenlijst

A decorative graphic consisting of numerous thin, light blue wavy lines that create a sense of motion and depth across the middle section of the page.

Weergeven in het Helpcentrum:

<https://bitwarden.com/help/bitwarden-glossary/>

Bitwarden Verklarende woordenlijst

Algemeen

Terminologie	Definitie
Account	Een Bitwarden-account wordt gedefinieerd door uw gebruikersnaam en hoofdwachtwoord (die alleen u kent). Uw Bitwarden-account wordt gebruikt om toegang te krijgen tot Bitwarden-services en bevat ook informatie zoals facturering, instellingen, taalvoorkeur en meer.
Account wijzigen	De Bitwarden-functie voor desktop- en mobiele clients waarmee u eenvoudig kunt schakelen tussen meerdere accounts, zoals uw persoonlijke of werkaccounts. Lees meer .
Persoonlijke rekening	Een persoonlijk Bitwarden-account is de record die wordt gedefinieerd door uw gebruikersnaam en hoofdwachtwoord (die alleen u kent) en die niet is gekoppeld aan een Organisatiekluis of is gerelateerd aan een bedrijf of bedrijfsentiteit. Een persoonlijke account wordt meestal ingesteld met een persoonlijk e-mailadres en bevat kluisitems waarover alleen jij eigenaar bent en controle hebt.
Zakelijke rekening	<p>Een zakelijk Bitwarden-account is de record die wordt gedefinieerd door uw gebruikersnaam en hoofdwachtwoord (die alleen u kent) en die is gekoppeld aan een organisatie die is gerelateerd aan een bedrijf of bedrijfsentiteit. Een zakelijke account wordt meestal ingesteld met een zakelijk e-mailadres.</p> <p>Een bedrijfsrekening wordt beheerd door de bijbehorende organisatie. Alle kluisitems of geheimen op een bedrijfsrekening moeten worden beschouwd als eigendom van het gerelateerde bedrijf of de gerelateerde bedrijfsentiteit.</p>
API-sleutel	De API-sleutel (Application Programming Interface) is een specifieke identificatiecode voor een gebruiker of programma. De API-sleutel kan worden gebruikt om andere applicaties te integreren met Bitwarden voor automatisering, monitoring en meer. De API-sleutel is een gevoelig geheim en moet zorgvuldig worden behandeld.
Klanten / Bitwarden Klant	De client, of clienttoepassing, is de toepassing die zich aanmeldt bij Bitwarden. Dit omvat het web, mobiele en desktop apps, de Bitwarden CLI en browser extensies. Clients kunnen worden gedownload van de Downloads pagina .
Directory Connector	Een toepassing om gebruikers en groepen te synchroniseren van een directoryservice naar een Bitwarden-organisatie. De Bitwarden Directory Connector verzorgt automatisch provisioning en deprovisioning van gebruikers, groepen en groepassociaties vanuit de brondirectory. Meer informatie .

Terminologie	Definitie
Domeinverificatie	<p>Het proces waarbij een organisatie haar eigendom van een specifiek internetdomein bewijst (bijv. mycompany.com). Domeinverificatie maakt het mogelijk om extra functies te activeren, zoals de mogelijkheid voor gebruikers om het invoeren van de SSO-ID over te slaan tijdens het aanmeldproces. Meer informatie.</p>
Groepen	<p>Een verzameling organisatieleden. Groepen brengen gebruikers samen en bieden een schaalbare manier om rechten toe te wijzen, zoals toegang tot verzamelingen, projecten of geheimen, maar ook rechten binnen elke afzonderlijke verzameling. Wanneer je nieuwe gebruikers aanmaakt, voeg ze dan toe aan een groep zodat ze automatisch de geconfigureerde rechten van die groep erven.</p>
Hoofdwachtwoord	<p>Ook bekend als Bitwarden-wachtwoord, hoofdwachtwoord, accountwachtwoord of kluiswachtwoord.</p> <p>Het hoofdwachtwoord, de primaire methode (of sleutel) voor toegang tot uw Bitwarden account en gegevens, wordt gebruikt om uw identiteit te verifiëren bij de Bitwarden service en om uw gevoelige gegevens, zoals kluisitems of geheimen, te ontsleutelen. Bitwarden moedigt gebruikers aan om er een te maken die gedenkwaardig, sterk en uniek is, zodat deze alleen voor Bitwarden wordt gebruikt.</p> <p><i>In 2021 introduceerde Bitwarden Account Recovery Administration (voorheen Admin Password Reset), waarmee Enterprise-gebruikers en organisaties een beleid kunnen implementeren waarmee beheerders en eigenaren hoofdwachtwoorden voor ingeschreven gebruikers kunnen resetten. Meer informatie.</i></p>
Organisatie	<p>Een entiteit (bedrijf, instelling, groep mensen) die Bitwarden-gebruikers koppelt aan gedeelde organisatiegegevens, zoals logins binnen een organisatiekluis of een Geheimenbeheerproject voor het veilig delen van items.</p>
Plan	<p>Plannen definiëren de diensten die Bitwarden levert door middel van licenties, inclusief beschikbare functies en het aantal gebruikers dat het product kan gebruiken. Er zijn verschillende soorten vooraf gedefinieerde plannen beschikbaar waarop individuen of organisaties zich kunnen abonneren.</p>
Beleid	<p>Beleidsregels zijn organisatiebrede besturingselementen die een beheerder helpen een bedrijf veilig te houden door extra instellingen in te schakelen voor de manier waarop hun leden (ook wel eindgebruikers genoemd) Bitwarden gebruiken. Dit beleid zorgt voor een uniforme beveiligingsstandaard. Meer informatie.</p>
SCIM	<p>System for cross-domain identity management (SCIM) kan worden gebruikt om automatisch leden en groepen aan te maken in uw Bitwarden organisatie.</p>

Terminologie	Definitie
Eenmalige aanmelding (SSO)	Bitwarden-servers bieden een SCIM-eindpunt dat, met een geldige SCIM API-sleutel, verzoeken accepteert van uw identity provider (IdP) voor provisioning en de-provisioning van gebruikers en groepen. Meer informatie.
Inloggen met SSO	Een sessie- en gebruikersverificatieservice die werknemers of gebruikers toegang geeft tot applicaties met één set aanmeldingsreferenties die gebaseerd zijn op hun identiteit en rechten. Single Sign-On heeft meerdere implementatiemogelijkheden en is breed compatibel met Identity Providers (IdP's) waardoor klanten hun bestaande oplossing kunnen gebruiken. Meer informatie.
SSO met vertrouwde apparaten	Een implementatie van Single Sign-On. Met deze methode wordt de gebruiker geverifieerd door een Identity Provider, waarna de gebruiker zijn Bitwarden-wachtwoord invoert om zijn gegevens te ontsleutelen. Meer informatie.
SSO met door de klant beheerde encryptie	Een wachtwoordloze implementatie van Single Sign-On. Met deze methode wordt de gebruiker geverifieerd door een Identity Provider en worden zijn gegevens gedecodeerd via een proces dat gebruik maakt van een apparaatcoderingsleutel die is opgeslagen op aangewezen, vertrouwde apparaten. Meer informatie.
Abonnement	Een geavanceerde wachtwoordloze implementatie van Single Sign-On die beschikbaar is voor zelf gehoste organisaties. Met deze methode wordt de gebruiker geverifieerd door een Identity Provider, waarna de versleutelingscode van de gebruiker automatisch wordt opgehaald van een zelf gehoste sleutelservers met Key Connector, waardoor gebruikersgegevens kunnen worden ontsleuteld. Meer informatie.
Abonnement	Het abonnement is de transactionele overeenkomst tussen de klant en Bitwarden als onderdeel van de uitgifte van een licentie. Eigenaren nemen een abonnement op plannen tegen de overeengekomen vergoeding op terugkerende basis (maandelijks of jaarlijks) voor de door Bitwarden geleverde diensten die in het plan worden beschreven.

Bitwarden Wachtwoord Beheerder

Terminologie	Definitie
Automatisch invullen	Een softwarefunctie die eerder opgeslagen informatie automatisch invoert in een formulierveld. Met Bitwarden kunt u logins automatisch invullen via browserextensies en mobiele apparaten, en kaarten en identiteiten automatisch invullen via browserextensies. Meer informatie.

Terminologie	Definitie
Collecties	<p>Een eenheid om een of meer kluisitems samen op te slaan (logins, notities, kaarten en identiteiten voor veilig delen) door een bedrijf binnen een Bitwarden-organisatie. Meer informatie.</p>
Individueel polsstokspringen	<p>De individuele kluis is het beveiligde gebied voor elke gebruiker om onbeperkt logins, notities, kaarten en identiteiten op te slaan. Gebruikers hebben toegang tot hun Bitwarden Individual kluis op elk apparaat en platform.</p> <p>Binnen een zakelijke context</p> <p>Voor gebruikers die deel uitmaken van een Bitwarden Teams- of Enterprise-plan is een individuele kluis gekoppeld aan hun e-mailadres op het werk. Individuele kluizen zijn vaak verbonden met, maar gescheiden van, een organisatiekluis.</p> <p>Binnen een persoonlijke context</p> <p>Voor gebruikers die deel uitmaken van een Bitwarden persoonlijk of familieplan is een individuele kluis gekoppeld aan hun persoonlijke e-mailadres. Als het deel uitmaakt van een familieplan of een gratis organisatie voor twee personen, blijft de Individual-kluis gescheiden van de Organization-kluis, maar beide zijn toegankelijk voor de gebruiker.</p> <p>Bitwarden raadt aan om werk-e-mailadressen te koppelen aan Teams en Enterprise-organisaties, en persoonlijke e-mailadressen aan familieorganisaties.</p> <p>Opmerking: de individuele kluis kan worden uitgeschakeld voor leden van een ondernemingsorganisatie via een ondernemingsbeleid.</p>
Items / Kluis Items	<p>Items zijn de individuele items die kunnen worden opgeslagen en gedeeld in Bitwarden Password Manager, zoals aanmeldingen, notities, kaarten en identiteiten.</p>
Organisatie Lid / Leden	<p>Een eindgebruiker zoals een werknemer of familielid die toegang heeft tot gedeelde organisatie-items in hun kluizen, naast individuele items in hun individuele kluis.</p>
Organisatie Kluis	<p>Het beschermde gebied voor gedeelde items. Elke gebruiker (ook wel "lid" genoemd) die deel uitmaakt van een organisatie kan gedeelde items vinden in hun kluisweergave, naast items die individueel eigendom zijn. Met organisatiekluizen kunnen beheerders en eigenaars de items, gebruikers en instellingen van de organisatie beheren.</p>

Terminologie	Definitie
Kluis	De beveiligde opslagruimte die een uniforme interface en strenge toegangscontrole biedt voor elk item.

Bitwarden Geheimen Manager

Terminologie	Definitie
Toegangscode	Een sleutel die ervoor zorgt dat een serviceaccount toegang heeft tot de geheimen in je kluis en ze kan ontsleutelen. Meer informatie .
Naam	Een door de gebruiker gedefinieerd label voor een specifiek geheim.
Project	Verzamelingen van geheimen die logisch zijn gegroepeerd voor beheertoegang door uw DevOps- en cyberbeveiligingsteams. Meer informatie .
Geheim	Gevoelige key-value paren, zoals API-sleutels, die uw organisatie nodig heeft, moeten veilig worden opgeslagen en mogen nooit worden blootgesteld in platte code of worden verzonden via onversleutelde kanalen.
Servicerekening	Niet-menselijke machinegebruikers, zoals applicaties of deployment pipelines, die programmatische toegang nodig hebben tot een discrete set geheimen.
Waarde	Een door de gebruiker gedefinieerd veld van een opgeslagen geheim dat wordt gebruikt in software- of machineprocessen. Dit is de gevoelige informatie die wordt beheerd door Bitwarden Secrets Manager en kan API-sleutels, applicatieconfiguraties, verbindingstrings van databases en omgevingsvariabelen bevatten.

Bitwarden Wachtwoordloos.dev

Terminologie	Definitie
FIDO	FIDO is het acroniem voor Fast Identity Online. Het vertegenwoordigt een consortium dat veilige, open authenticatiestandaarden zonder wachtwoord ontwikkelt die phishing proof zijn. De FIDO-protocollen, die zijn ontwikkeld door de FIDO Alliance, omvatten: UAF: universeel authenticatiekader

Terminologie	Definitie
Passleutels	<p>U2F: Universele Tweede Factor</p> <p>FIDO2: een nieuw authenticatieprotocol zonder wachtwoord dat kernspecificaties WebAuthn (de client-API) en CTAP (de authenticator-API) bevat. Meer informatie.</p> <hr/> <p>Passkeys – de van de FIDO2-standaard afgeleide referenties voor elke website waar een gebruiker zich registreert – stellen gebruikers in staat cryptografische tokens aan te maken en op te slaan in plaats van traditionele wachtwoorden. Tegenwoordig worden passkeys gebruikt om gebruikers aan te melden bij een app of website met vooraf geauthenticerde apparaatspecifieke tokens. In de toekomst zou het proces gebruikt kunnen worden met deelbare of overdraagbare cryptografische tokens. Meer informatie.</p> <hr/>
Wachtwoordloos	<p>Wachtwoordloos is de overkoepelende term die wordt gebruikt om een verscheidenheid aan authenticatietechnologieën te beschrijven die niet afhankelijk zijn van wachtwoorden, waaronder: iets dat een gebruiker heeft (een beveiligingssleutel, token of apparaat), iets dat ze zijn (biometrie) en wachtsleutels.</p>