

Bitwarden Glossar der Begriffe

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.

Ansicht im Hilfezentrum:

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

Bitwarden Glossar der Begriffe

Allgemein

Terminologie	Definition
Konto	Ein Bitwarden-Konto ist der Datensatz, der durch Ihren Benutzernamen und Ihr Master-Passwort definiert wird (das nur Sie kennen). Ihr Bitwarden-Konto wird verwendet, um auf Bitwarden-Dienste zuzugreifen und enthält auch Informationen wie Rechnung, Einstellungen, Sprachpräferenz und mehr.
Kontowechsel	Die Bitwarden-Funktion für Desktop- und Mobil-Clients, die es Ihnen ermöglicht, einfach zwischen mehreren Konten, wie Ihren persönlichen oder Arbeitskonten, zu wechseln. Erfahren Sie mehr .
Persönliches Konto	Ein persönliches Bitwarden-Konto ist der Datensatz, der durch Ihren Benutzernamen und Ihr Master-Passwort (das nur Sie kennen) definiert wird und nicht mit einem organisatorischen Tresor verbunden ist oder sich auf ein Unternehmen oder eine Geschäftseinheit bezieht. Ein persönliches Konto wird in der Regel mit einer persönlichen E-Mail-Adresse eingerichtet und enthält Tresor-Einträge, über die nur Sie Eigentum und Kontrolle haben.
Geschäftskonto	<p>Ein geschäftliches Bitwarden-Konto ist der Datensatz, der durch Ihren Benutzernamen und Ihr Master-Passwort (das nur Sie kennen) definiert wird und der mit einer Organisation in Verbindung steht, die mit einem Unternehmen oder einer Geschäftseinheit verbunden ist. Ein Geschäftskonto wird in der Regel mit einer Geschäftlichen E-Mail-Adresse eingerichtet.</p> <p>Ein Geschäftskonto wird von der zugehörigen Organisation verwaltet. Alle Tresor Einträge oder Geheimnisse, die in einem Geschäftskonto enthalten sind, sollten als Eigentum des zugehörigen Unternehmens oder der Geschäftseinheit betrachtet werden.</p>
API-Schlüssel	Der Programmierschnittstelle (API) Schlüssel ist ein spezifischer Identifikationscode für einen Benutzer oder ein Programm. Der API-Schlüssel kann verwendet werden, um andere Anwendungen für die Zwecke der Automatisierung, Überwachung und mehr mit Bitwarden zu integrieren. Der API-Schlüssel ist ein sensibles Geheimnis und sollte sorgfältig behandelt werden.
Clients / Bitwarden Client	Der Client oder die Client-Anwendung ist die Anwendung, die sich bei Bitwarden anmeldet. Dies beinhaltet die Web-, Mobil- und Desktop-Apps, die Bitwarden CLI und Browser-Erweiterungen. Clients können von der Download-Seite heruntergeladen werden.
Verzeichniskonnektor	Eine Anwendung zur Synchronisation von Benutzern und Gruppen aus einem Verzeichnisdienst zu einer Bitwarden Organisation. Der Bitwarden Directory Connector provisioniert und deprovisioniert automatisch Benutzer, Gruppen und Gruppenverbindungen aus dem Quellverzeichnis. Lerne mehr .

Terminologie	Definition
Domain-Überprüfung	<p>Der Prozess, in dem eine Organisation ihren Besitz einer bestimmten Internet-Domain (z.B. mycompany.com) nachweist. Die Überprüfung der Domain ermöglicht die Aktivierung zusätzlicher Funktionen, wie zum Beispiel, dass Benutzer das Eingeben des SSO-Identifikators während des Prozesses mit den Zugangsdaten überspringen können. Lerne mehr.</p>
Gruppen	<p>Eine Gruppe von Mitgliedern der Organisation. Gruppen verbinden Benutzer miteinander und bieten eine skalierbare Möglichkeit, Berechtigungen zuzuweisen, wie zum Beispiel den Zugang zu Sammlungen, Projekten oder Geheimnissen, sowie Berechtigungen innerhalb jeder einzelnen Sammlung. Wenn Sie neue Benutzer einrichten, fügen Sie sie zu einer Gruppe hinzu, um ihnen automatisch die konfigurierten Berechtigungen dieser Gruppe zu vererben.</p>
Master-Passwort	<p>Auch bekannt als Bitwarden Passwort, Hauptpasswort, Kontopasswort oder Tresorpasswort.</p> <p>Die primäre Methode (oder der Schlüssel) für den Zugriff auf Ihr Bitwarden-Konto und Ihre Daten, das Master-Passwort wird sowohl zur Authentifizierung Ihrer Identität gegenüber dem Bitwarden-Dienst als auch zur Entschlüsselung Ihrer sensiblen Daten wie Tresor-Einträge oder Geheimnisse verwendet. Bitwarden ermutigt Benutzer, eines zu erstellen, das einprägsam, stark und einzigartig ist, da es nur für Bitwarden verwendet wird.</p> <p><i>Im Jahr 2021 führte Bitwarden die Account Recovery Administration (früher Admin Passwort Reset) ein, die es Enterprise-Nutzern und Organisationen ermöglicht, eine Richtlinie umzusetzen, die Administratoren und Eigentümern erlaubt, Master-Passwörter für registrierte Benutzer zurückzusetzen. Lerne mehr.</i></p>
Organisation	<p>Eine Entität (Unternehmen, Institution, Gruppe von Menschen), die Bitwarden-Benutzer mit gemeinsamen Daten einer Organisation verbindet, wie Zugangsdaten in einem Organisationstresor oder einem Secrets Manager-Projekt für die sichere Freigabe von Einträgen.</p>
Abo	<p>Pläne definieren die Dienstleistungen, die Bitwarden durch Lizenzierung bereitstellt, einschließlich verfügbarer Funktionen und der Anzahl von Benutzern, die das Produkt nutzen können. Es gibt mehrere Arten von vordefinierten Plänen, zu denen Einzelpersonen oder Organisationen sich anmelden können.</p>
Richtlinien	<p>Richtlinien sind unternehmensweite Kontrollen, die einem Administrator helfen, ein Unternehmen sicher zu halten, indem sie zusätzliche Einstellungen für die Nutzung von Bitwarden durch ihre Mitglieder (auch Endbenutzer genannt) ermöglichen. Diese Richtlinien gewährleisten einen einheitlichen Sicherheitsstandard. Lerne mehr.</p>

Terminologie	Definition
SCIM	<p>System für Identitätsmanagement über Domänen hinweg (SCIM) kann verwendet werden, um Mitglieder und Gruppen in Ihrer Bitwarden Organisation automatisch bereitzustellen.</p> <p>Bitwarden-Server bieten einen SCIM-Endpunkt, der bei Vorhandensein eines gültigen SCIM-API-Schlüssels Anfragen von Ihrem Identitätsanbieter (IdP) für die Bereitstellung und Entfernung von Benutzern und Gruppen akzeptiert. Lerne mehr.</p>
Single Sign-On (SSO)	<p>Ein Sitzungs- und Benutzerauthentifizierungsdienst, der Mitarbeitern oder Benutzern mit einem Satz von Zugangsdaten Zugang zu Anwendungen gewährt, die auf ihrer Identität und Berechtigungen basieren. Single Sign-On hat mehrere Implementierungsoptionen und ist weitgehend kompatibel mit Identitätsanbietern (IdPs), was es Kunden ermöglicht, ihre bestehende Lösung zu nutzen. Lerne mehr.</p>
Melden Sie sich mit SSO an	<p>Eine Implementierung von Single Sign-On. Mit dieser Methode wird der Benutzer von einem Identitätsanbieter authentifiziert, dann gibt der Benutzer sein Bitwarden Passwort ein, um seine Daten zu entschlüsseln. Lerne mehr.</p>
SSO mit vertrauenswürdigen Geräten	<p>Eine passwortlose Implementierung von Single Sign-On. Mit dieser Methode wird der Benutzer von einem Identitätsanbieter authentifiziert und seine Daten werden durch einen Prozess entschlüsselt, der einen auf ausgewählten, vertrauenswürdigen Geräten gespeicherten Geräteschlüssel verwendet. Lerne mehr.</p>
SSO mit vom Kunden verwalteter Verschlüsselung	<p>Eine fortschrittliche passwortlose Implementierung von Single Sign-On, die für selbst gehostete Organisationen verfügbar ist. Mit dieser Methode wird der Benutzer von einem Identitätsanbieter authentifiziert, dann wird der Verschlüsselungsschlüssel des Benutzers automatisch von einem selbst gehosteten Schlüsselserver abgerufen, der den Key Connector nutzt, was die Entschlüsselung der Benutzerdaten ermöglicht. Lerne mehr.</p>
Abo	<p>Das Abonnement ist die vertragliche Vereinbarung zwischen dem Kunden und Bitwarden im Rahmen der Ausstellung einer Lizenz. Eigentümer abonnieren Pläne zu der vereinbarten Gebühr auf wiederkehrender Basis (monatlich oder jährlich) für die von Bitwarden im Plan skizzierten Dienstleistungen.</p>

Bitwarden Passwortmanager

Terminologie

Definition

Autovervollständigung

Eine Softwarefunktion, die automatisch zuvor gespeicherte Informationen in ein Formularfeld eingibt. Mit Bitwarden können Sie Zugangsdaten über Browser-Erweiterungen und mobile Geräte automatisch ausfüllen und Karten und Identitäten über Browser-Erweiterungen automatisch ausfüllen. [Lerne mehr.](#)

Sammlungen

Eine Einheit zum Speichern von einem oder mehreren Tresor-Einträgen zusammen (Zugangsdaten, Notizen, Karten und Identitäten für sicheres Teilen) durch ein Unternehmen innerhalb einer Bitwarden Organisation. [Lerne mehr.](#)

Einzelner Tresor

Der individuelle Tresor ist der geschützte Bereich für jeden Benutzer, um unbegrenzt Zugangsdaten, Notizen, Karten und Identitäten zu speichern. Benutzer können auf ihren Bitwarden Einzel-Tresor auf jedem Gerät und jeder Plattform zugreifen.

Innerhalb eines geschäftlichen Kontextes

Für Benutzer, die Teil eines Bitwarden Teams oder Enterprise Plans sind, ist ein individueller Tresor mit ihrer Arbeits-E-Mail-Adresse verbunden. Individuelle Tresore sind oft mit einem Organisationstresor verbunden, aber davon getrennt.

Innerhalb eines persönlichen Kontextes

Für Benutzer, die Teil eines Bitwarden-Personal- oder Families-Plans sind, ist ein individueller Tresor mit ihrer persönlichen E-Mail-Adresse verbunden. Wenn Sie Teil eines Familienplans oder einer kostenlosen Zweipersonen-Organisation sind, bleibt der individuelle Tresor vom Organisationstresor getrennt, aber beide sind für den Benutzer zugänglich.

Bitwarden empfiehlt, Arbeits-E-Mail-Adressen mit Teams und Enterprise Organisationen zu verknüpfen und persönliche E-Mail-Adressen mit Families Organisationen.

Notiz: Der individuelle Tresor kann für Mitglieder einer Enterprise-Organisation durch eine Unternehmensrichtlinie deaktiviert werden.

Einträge / Tresor
Einträge

Einträge sind die einzelnen Einträge, die in Bitwarden Passwort-Manager gespeichert und geteilt werden können, wie Zugangsdaten, Notizen, Karten und Identitäten.

Terminologie	Definition
Organisation Mitglied / Mitglieder	Ein Endbenutzer, wie ein Mitarbeiter oder Familienmitglied, der Zugang zu gemeinsam genutzten Organisationseinträgen in ihren Tresoren hat, neben individuellen Einträgen in ihrem individuellen Tresor.
Tresor einer Organisation	Der geschützte Bereich für gemeinsame Einträge. Jeder Benutzer (auch "Mitglied" genannt), der Teil einer Organisation ist, kann gemeinsam genutzte Einträge in seiner Tresoransicht finden, neben individuell besessenen Einträgen. Organisationstresore ermöglichen Administratoren und Eigentümern die Verwaltung der Einträge, Benutzer und Einstellungen der Organisation.
Tresor / Tresore Ansicht	Der sichere Speicherbereich, der eine einheitliche Schnittstelle und strenge Zugangskontrolle zu jedem Eintrag bietet.

Bitwarden Secrets Manager

Terminologie	Definition
Zugriffstoken	Ein Schlüssel, der den Zugang zu Bedienungshilfen-Konto ermöglicht und die Fähigkeit, Geheimnisse zu entschlüsseln, die in Ihrem Tresor gespeichert sind. Lerne mehr.
Name	Ein vom Benutzer definiertes Etikett für ein spezifisches Geheimnis.
Projekt	Sammlungen von Geheimnissen, die logisch gruppiert sind, um von Ihren DevOps und Cybersicherheits-Teams verwaltet zu werden. Lerne mehr.
Geheimnis	Sensible Schlüssel-Wert-Paare, wie API-Schlüssel, die Ihre Organisation sicher speichern muss und die niemals kompromittiert in Klartext oder über unverschlüsselte Kanäle übertragen werden sollten.
Dienstkonto	Nicht-menschliche Maschinenbenutzer, wie Anwendungen oder Bereitstellungspipelines, die einen programmatischen Zugriff auf eine diskrete Menge von Geheimnissen benötigen.
Wert	Ein vom Benutzer definiertes Feld eines gespeicherten Geheimnisses, das in Software- oder Maschinenprozessen verwendet wird. Dies sind die sensiblen Informationen, die vom Bitwarden Secrets Manager

Terminologie**Definition**

verwaltet werden und können API-Schlüssel, Anwendungskonfigurationen, Datenbankverbindungszeichenfolgen und Umgebungsvariablen enthalten.

Bitwarden Passwordless.dev**Terminologie****Definition**

FIDO ist das Akronym für Fast Identity Online. Es repräsentiert ein Konsortium, das sichere, offene passwortlose Authentifizierungsstandards entwickelt, die phishing-sicher sind. Die FIDO-Protokolle, die von der FIDO-Allianz entwickelt wurden, beinhalten:

FIDO

UAF: Universelles Authentifizierungs-Framework

U2F: Universeller Zweiter Faktor

FIDO2: Ein neues passwortloses Authentifizierungsprotokoll, das die Kernspezifikationen WebAuthn (die Client-API) und CTAP (die Authentifizierungs-API) enthält [Erfahren Sie mehr](#).

Passwörter

Passkeys – die Anmeldedaten, die aus dem FIDO2-Standard für jede Website abgeleitet werden, bei der sich ein Benutzer registriert – ermöglichen es Benutzern, kryptografische Token anstelle von traditionellen Passwörtern zu erstellen und zu speichern. Heute werden Passwörter verwendet, um Benutzer mit vorauthentifizierten, gerätespezifischen Token in eine App oder Website einzuloggen. In der Zukunft könnte der Prozess mit teilbaren oder übertragbaren kryptografischen Token verwendet werden. [Lerne mehr](#).

passwortlos

"Passwordless" ist der Oberbegriff, der verwendet wird, um eine Vielzahl von Authentifizierungstechnologien zu beschreiben, die nicht auf Passwörtern basieren, einschließlich: etwas, das ein Benutzer hat (ein Sicherheitsschlüssel, Token oder Gerät), etwas, das sie sind (Biometrie), und Passkeys.