bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE > BENUTZERVERWALTUNG

Einführung und Nachfolgeübersicht

Ansicht im Hilfezentrum:
https://bitwarden.com/help/onboarding-and-succession/

Einführung und Nachfolgeübersicht

> **Tip**
> Lesen Sie das vollständige Dokument unten oder laden Sie die PDF herunter.

Passwortverwaltung, die zu Ihrem Unternehmen passt

Neue Mitarbeiter schnell einsatzbereit zu machen, steigert die Produktivität. Ebenso fördert ein ordnungsgemäßes Verabschieden das Vertrauen in die Sicherheit der Systeme und Konten Ihres Unternehmens. Ob Ihr Unternehmen eher auf Konsolidierung und Zentralisierung setzt oder eine flexible und dynamische Umgebung bevorzugt, Bitwarden erfüllt Ihre Bedürfnisse.

Dieser Leitfaden behandelt den Bitwarden-Ansatz zur Einarbeitung und Nachfolgeplanung für Mitglieder Ihrer Organisation, beginnend mit unserem Ansatz zur Beziehung zwischen Mitgliedern und Organisationen, dann die einfachsten Anwendungsfälle für die Einarbeitung und Nachfolge und schließlich die Hebel und Optionen, die Ihnen zur Verfügung stehen, um Bitwarden an Ihre Bedürfnisse anzupassen.

Der Bitwarden-Ansatz

Die Vision von Bitwarden ist, sich eine Welt vorzustellen, in der niemand gehackt wird. Wir führen dies in unserer Mission fort, Einzelpersonen und Unternehmen dabei zu helfen, ihre sensiblen Informationen einfach und sicher zu verwalten. Bitwarden glaubt, dass:

- Die grundlegende Passwort-Verwaltung für Einzelpersonen kann und sollte **Free** sein. Wir bieten genau das an, ein grundlegendes kostenloses Konto für Einzelpersonen.
- Einzelpersonen und Familien sollten eine aktive Rolle in ihrer Sicherheit übernehmen, indem sie TOTPs, Notfallzugang und andere unterstützende Sicherheitsfunktionen nutzen.
- Organisationen können ihr Sicherheitsprofil erheblich verbessern durch organisatorisches Passwort-Management und sicheres Teilen.

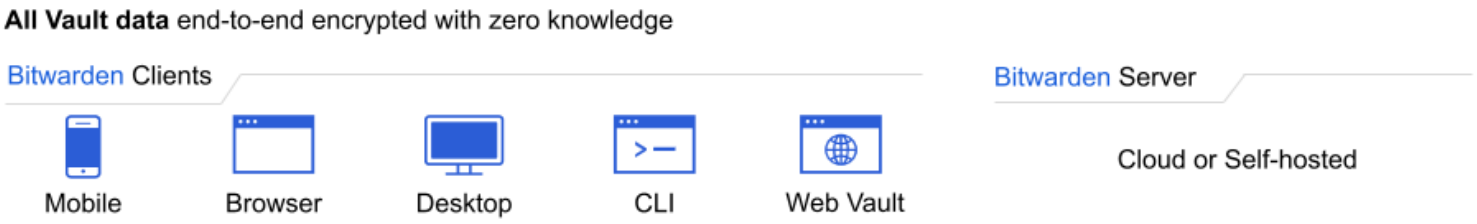
> **Tip**
> Für Bitwarden sind verschiedene Pläne und Optionen verbunden und ergänzend, alle ausgehend von unserer Vision einer hackfreien Welt. Indem wir jedem bei der Arbeit **und** zu Hause die Passwortverwaltung ermöglichen, kommen wir diesem Ziel einen Schritt näher.

Ein Schlüsselaspekt von Bitwarden ist, dass im Gegensatz zu vielen Softwareanwendungen alles in jedem Tresor Ende-zu-Ende verschlüsselt ist. Um dieses Sicherheitsmodell aufrechtzuerhalten, muss jede Person, die Bitwarden verwendet, ein einzigartiges Konto mit einem einzigartigen Master-Passwort haben. Master-Passwörter sollten **stark** und **einprägsam** sein.

Jeder Benutzer ist für sein Master-Passwort verantwortlich. Bitwarden ist eine Zero-Knowledge-Verschlüsselungslösung, was bedeutet, dass das Team von Bitwarden sowie die Bitwarden-Systeme selbst keine Kenntnisse von, keinen Weg zur Wiederherstellung oder Möglichkeit zur Zurücksetzung eines Master-Passworts haben.

Verwenden Sie Bitwarden überall

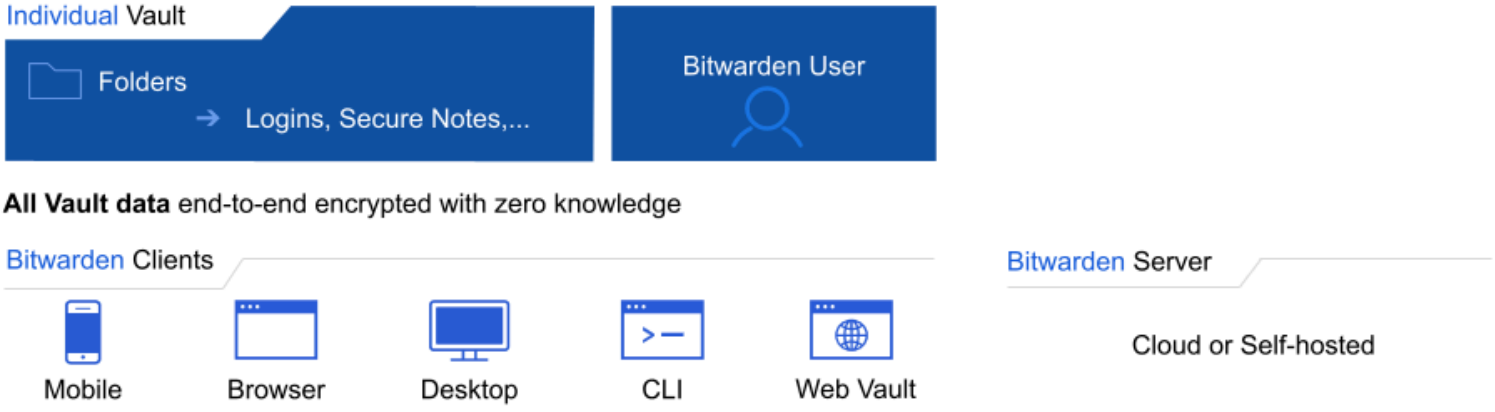
Sicherheit überall bedeutet Sicherheit überall, daher bieten die besten Passwort-Manager Zugang auf all Ihren Geräten. Bitwarden unterstützt eine Reihe von Client-Anwendungen, die entweder mit unseren Cloud-gehosteten Servern oder einem selbst gehosteten Server Ihrer Wahl verbunden werden können:



Bitwarden Clients/Server

Benutzers individuelle Tresore

Jeder, der ein Bitwarden-Konto erstellt, hat seinen eigenen individuellen Tresor. Zugänglich von jeder Client-Anwendung sind einzelne Tresore einzigartig für jeden Benutzer und nur dieser Benutzer hält den Schlüssel zum Zugriff darauf, mit einer Kombination aus seiner E-Mail-Adresse und dem Master-Passwort. Persönliche Konten und die darin gespeicherten individuell besessenen Tresor Einträge sind die Verantwortung des Kontoeigentümers. Die Eigentümer, Administratoren und Manager einer Organisation können standardmäßig keinen individuellen Tresor eines anderen Benutzers einsehen, was garantiert, dass die Daten im individuellen Tresor eines jeden Benutzers ihm allein gehören.



Persönliche Tresore

Families, Teams und Enterprise Organisationen bieten Mitgliedern automatisch Premium-Funktionen an, wie Notfallzugang und verschlüsselte Anhangspeicherung, die sie nutzen können. Daten in einem individuellen Tresor gehören dem Benutzer. Individuelle Tresore ermöglichen kein Teilen, Organisationen schon.

Tip

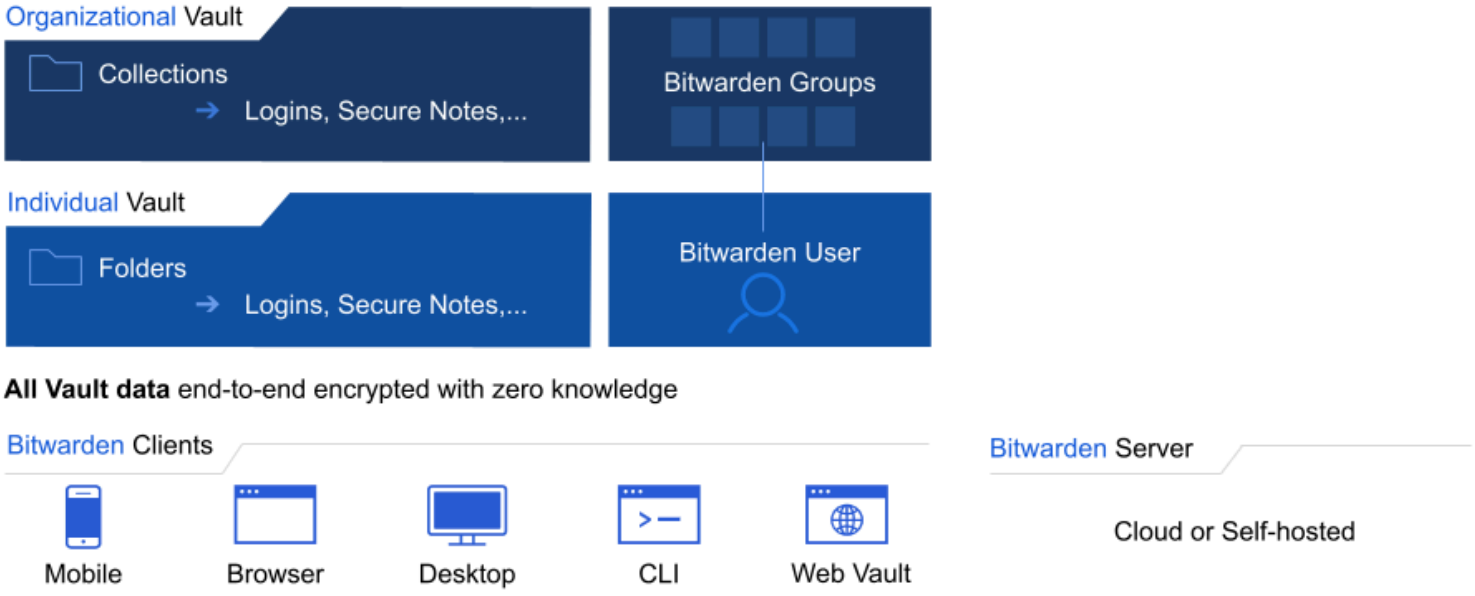
Warum werden standardmäßig einzelne Tresore bereitgestellt?

Individuelle Tresore sind eine wesentliche Komponente des Bitwarden-Ansatzes. Mitarbeiter verwenden täglich eine Reihe von Anmeldedaten, privat und beruflich, und **Gewohnheiten, die in einem Bereich gebildet werden, werden typischerweise auch in dem anderen Bereich Gewohnheiten**. Unserer Ansicht nach werden Mitarbeiter, die in ihrem Privatleben angemessene Sicherheitspraktiken anwenden, dieses gute Verhalten auf ihr Berufsleben übertragen und dabei **Ihr Unternehmen schützen**.

Die Verwendung desselben Werkzeugs in beiden Bereichen hilft dabei, die Gewohnheit schneller und einfacher zu bilden. Enterprise-Organisationen haben die Möglichkeit, Richtlinien zu konfigurieren, einschließlich der Deaktivierung einzelner Tresore.

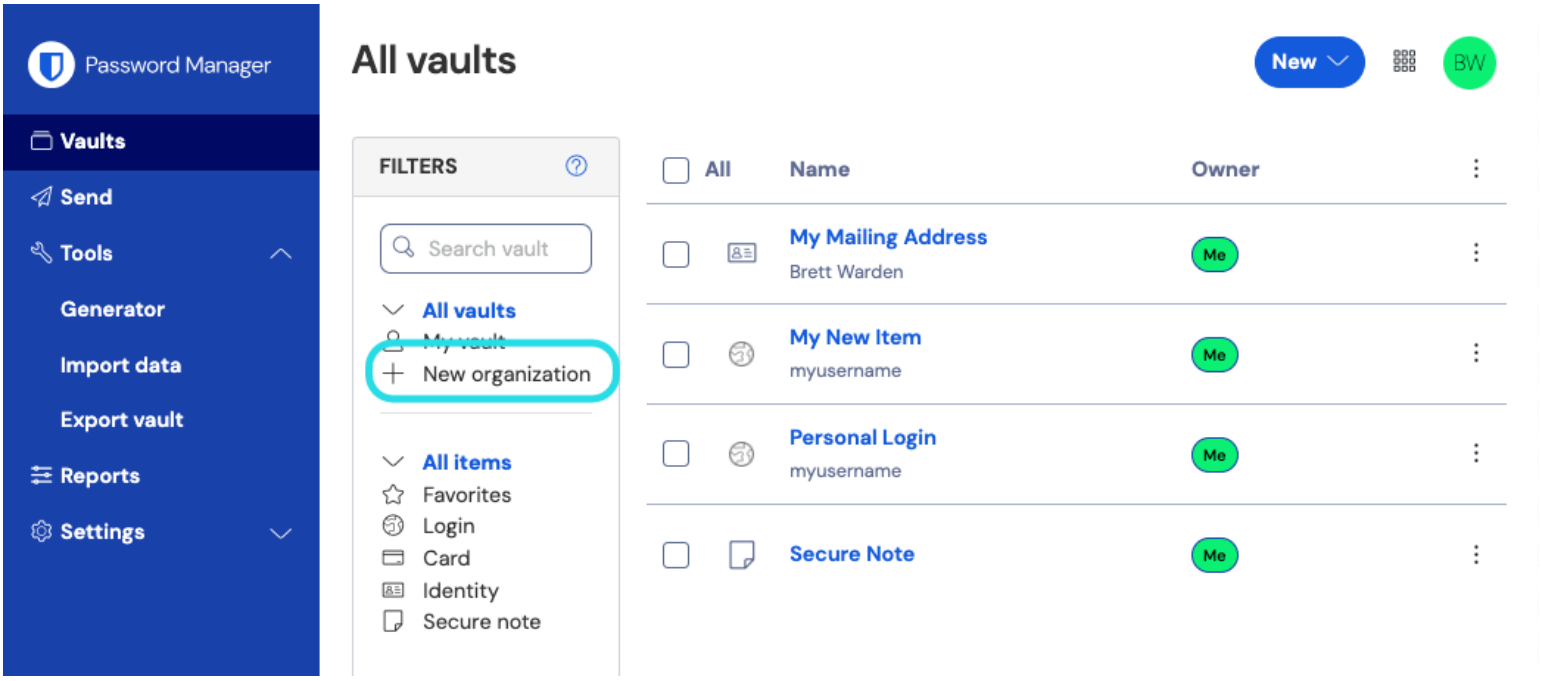
Bitwarden Organisationen

Bitwarden-Organisationen fügen der Passwortverwaltung für Ihr Team oder Unternehmen eine Ebene der Zusammenarbeit und des Austauschs hinzu, sodass Sie gemeinsame Informationen wie Büro-WLAN-Passwörter, Online-Anmeldeinformationen oder gemeinsame Firmenkreditkarten sicher teilen können. Sicheres Teilen durch Organisationen ist sicher und einfach.



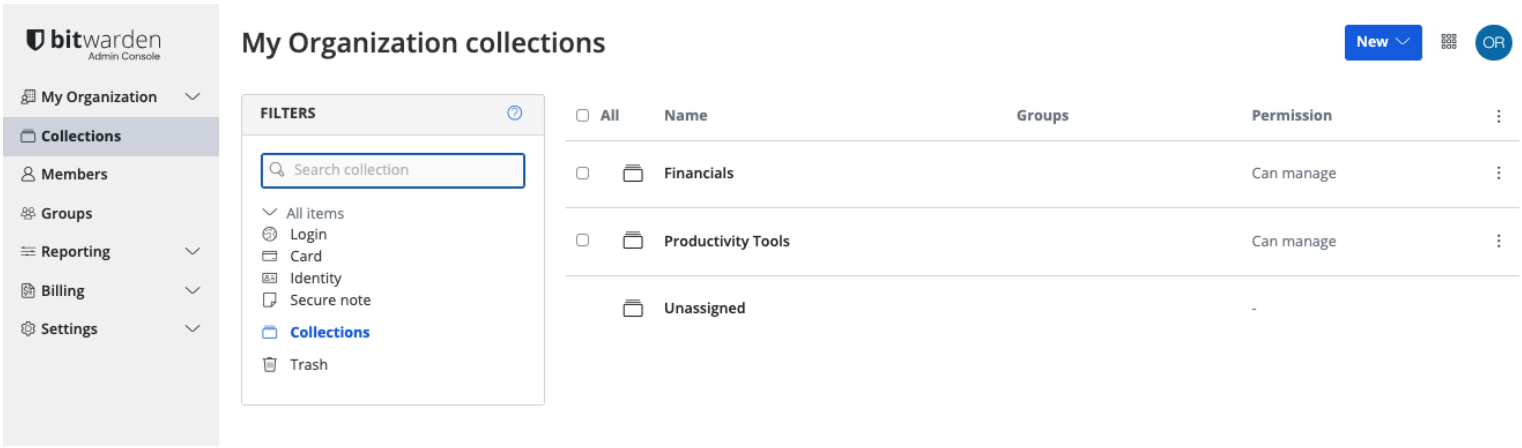
Tresor einer Organisation

Jeder kann direkt aus der Web-App eine Organisation gründen:



Neue Organisation einrichten

Einmal erstellt, landen Sie in der Admin-Konsole, die das zentrale Hub für alles rund um das Teilen und die Organisation-Administration ist. Wer immer die Organisation startet, wird der Eigentümer sein und hat somit die volle Kontrolle, um den Tresor zu überwachen, Einträge, Mitglieder, Sammlungen und Gruppen zu verwalten, Berichte zu erstellen und Einstellungen wie Richtlinien zu konfigurieren:



Administrator Konsole

Sammlungen

Bitwarden Organisationen verwalten Mitglieder und Daten auf eine skalierbare und sichere Weise. Mitglieder und Daten einzeln zu verwalten ist für große Unternehmen ineffizient und kann Raum für Fehler lassen. Um dieses Problem zu lösen, stellen Organisationen Sammlungen und Gruppen bereit.

Sammlungen sammeln Zugangsdaten, Notizen, Karten und Identitäten für sicheres Teilen innerhalb einer Organisation:

Sammlungen verwenden

Mitglieder einarbeiten

Sobald Ihre Organisation gegründet ist und Sammlungen eingerichtet sind, um Ihre Daten zu speichern, sollten Eigentümer und Administratoren neue Mitglieder einladen. Um die Sicherheit Ihrer Organisation zu gewährleisten, wendet Bitwarden einen 3-Schritte-Prozess für die Einarbeitung neuer Mitglieder an, Einladen → Akzeptieren → Bestätigen.

Mitglieder können direkt aus dem Web-Tresor an Bord geholt werden, mit der Directory Connector Anwendung zur Synchronisation einzelner Benutzer und Gruppen, oder durch Just in Time (JIT) Bereitstellung mit Zugangsdaten mit SSO.

Mitglieder hinzufügen

In den einfachsten Fällen können Benutzer direkt aus der Web-App zu Ihrer Organisation hinzugefügt werden. Beim Hinzufügen von Benutzern können Sie festlegen, zu welchen Sammlungen Sie ihnen Zugang gewähren, welche Rolle Sie ihnen geben und mehr.

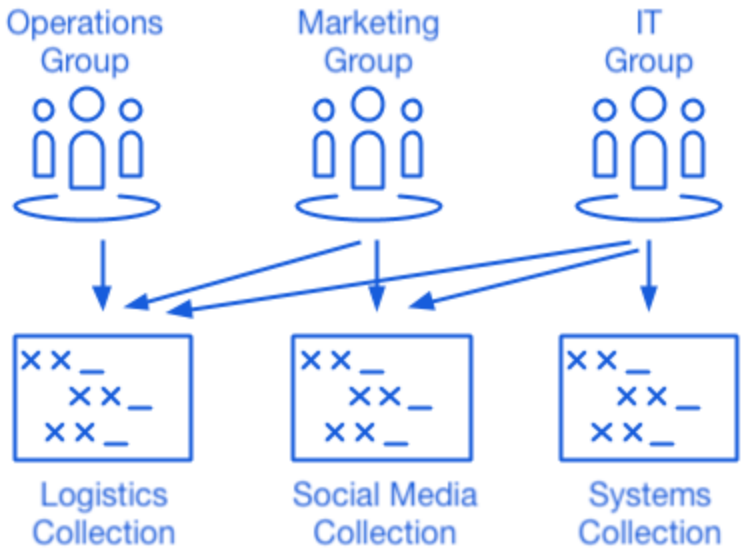
Erfahren Sie Schritt für Schritt, wie Sie Ihrer Organisation Benutzer hinzufügen .

Sobald Benutzer vollständig in Ihre Organisation integriert sind, können Sie ihnen Zugriff auf die Daten Ihres Organisationstresors gewähren, indem Sie sie Sammlungen zuweisen. Teams und Enterprise Organisationen können Benutzer zu Gruppen zuweisen, um skalierbare Berechtigungszuweisungen zu ermöglichen, und Gruppen-Sammlungs-Verbindungen erstellen, anstatt den Zugriff auf individueller Ebene zuzuweisen.

> **Tip**
>
> Für große Organisationen sind SCIM und Directory Connector die besten Methoden, um Benutzer in großem Maßstab einzubinden und abzumelden.

Gruppen

Gruppen verbinden einzelne Benutzer miteinander und bieten eine skalierbare Möglichkeit, Berechtigungen einschließlich des Zugriffs auf Sammlungen und andere Zugriffskontrollen zuzuweisen. Wenn Sie neue Benutzer einbinden, fügen Sie sie einer Gruppe hinzu, damit sie automatisch die konfigurierten Berechtigungen dieser Gruppe erben:



Sammlungen mit Gruppen verwenden

Umfassende rollenbasierte Zugriffskontrollen

Bitwarden verfolgt einen unternehmensfreundlichen Ansatz für das Teilen im großen Stil. Mitglieder können der Organisation mit einer Reihe von verschiedenen Rollen hinzugefügt werden, verschiedenen Gruppen angehören und diese Gruppen können verschiedenen Sammlungen zugewiesen werden, um den Zugang zu regulieren. Unter den verfügbaren Rollen befindet sich eine benutzerdefinierte Rolle für die granulare Konfiguration von administrativen Berechtigungen.

Benutzer deprovisionieren

Bei Bitwarden sehen wir das Teilen von Anmeldeinformationen als einen wesentlichen Aspekt, um Arbeit effizient und sicher zu erledigen. Wir erkennen auch an, dass es, sobald ein Ausweis geteilt wird, technisch möglich ist, dass der Empfänger ihn behält. Aus diesem Grund spielt eine sichere Einarbeitung mit geeigneten rollenbasierten Zugriffskontrollen und Umsetzung von Richtlinien eine wichtige Rolle bei der Gewährleistung einer sicheren Nachfolge.

Es gibt eine Vielzahl von Tools, die von Bitwarden bereitgestellt werden, um Ihren Arbeitsablauf anzupassen und mehr Kontrolle über die Nachfolge auszuüben. Die folgenden Abschnitte beschreiben einen grundlegenden Nachfolge-Arbeitsablauf, der keines dieser Werkzeuge verwendet, und einige fortgeschrittene Nachfolgetaktiken, die häufig von Organisationen verwendet werden:

Grundlegende Bereitstellungsrücknahme

Das Entfernen von Benutzern aus Bitwarden beinhaltet das Entfernen von Benutzern aus Ihrer Organisation und kann, wie das Onboarding, direkt aus dem Web-Tresor oder auf automatisierte Weise mit SCIM oder Directory Connector durchgeführt werden.

Alice ist eine **Benutzerin** in Ihrer Organisation, die in der Bitwarden Cloud gehostet wird und Firmen-E-Mail-Adressen verwendet (z.B. `vorname-nachname@firma.com`). Derzeit verwendet Alice Bitwarden so:

Produktbereich	Beschreibung
Client-Anwendungen	Verwendet Bitwarden auf dem Handy und eine Browser-Erweiterung privat und beruflich, sowie den Web-Tresor für gelegentliche Arbeiten im Zusammenhang mit der Organisation.
E-Mail-Adresse & Master-Passwort	Meldet sich bei Bitwarden an mit `alice@company.com` und `p@ssw0rD`.
Persönliche Einträge	Speichert verschiedene persönliche Einträge, einschließlich Zugangsdaten und Kreditkarten, in ihrem persönlichen Tresor.
Authentifizierungs-App verwalten	Verwendet Duo 2FA in der gesamten Organisation.
Sammlungen	Alice hat die "Verwalten" Berechtigung für die "Marketing Credentials" Sammlung, die ihr die Fähigkeit gibt, viele Aspekte dieser Sammlung zu verwalten.
Geteilte Einträge	Hat mehrere Tresor-Einträge erstellt und geteilt, die im Besitz der Organisation sind und in der Sammlung ihres Teams liegen.

Sobald Alice aus Ihrer Organisation entfernt wird:

Produktbereich	Beschreibung
Client-Anwendungen	Kann weiterhin jede Bitwarden-Anwendung verwenden, um auf ihren individuellen Tresor zuzugreifen, jedoch **verlieren alle sofort den Zugang** zum Organisationstresor, allen Sammlungen und allen geteilten Einträgen.

Produktbereich	Beschreibung
E-Mail-Adresse & Master-Passwort	Sie kann sich weiterhin mit `alice@company.com` und `p@ssw0rD` anmelden, da sie jedoch keinen Zugang zu ihrem `@company.com` Posteingang hat, sollte sie darauf hingewiesen werden, die mit ihrem Bitwarden-Konto verknüpfte E-Mail-Adresse zu ändern.
Einzelne Einträge	Sie wird immer noch in der Lage sein, ihren individuellen Tresor zu nutzen und auf die darin gespeicherten Einträge zuzugreifen.
Berechtigungen in der Organisation	Wird **sofort alle Berechtigungen und den Zugang zu** allem, was mit der Organisation zusammenhängt, verlieren.
Authentifizierungs-App verwalten	Sie wird nicht in der Lage sein, die Organisation Duo 2FA zu nutzen, um auf ihren Tresor zuzugreifen, kann aber eine unserer kostenlosen Zwei-Schritt-Zugangsdatenoptionen einrichten oder auf Premium für mehr upgraden.
Erstellte Sammlungen	Die "Marketing Team" Sammlung von Alice wird von den Eigentümern und Administratoren der Organisation behalten, die einem neuen Benutzer die Berechtigung zum Verwalten zuweisen können.
Geteilte Einträge	Das Eigentum an Sammlungen und geteilten Einträgen **gehört zur Organisation**, daher wird Alice trotz ihrer Erstellung den Zugang zu all diesen Einträgen verlieren.

Tip

Offline-Geräte speichern eine schreibgeschützte Kopie der Tresor-Daten, einschließlich der organisatorischen Tresor-Daten. Wenn Sie eine böswillige Ausnutzung dessen erwarten, sollten die Zugangsdaten, auf die das Mitglied Zugriff hatte, aktualisiert werden, wenn Sie es aus der Organisation entfernen.

Erweiterte Bereitstellungsrücknahme

Warning

Für jene Konten, die aufgrund von SSO mit vertrauenswürdigen Geräten kein Master-Passwort haben, wird ihre Entfernung aus Ihrer Organisation oder die Widerrufung ihres Zugangs jeglichen Zugang zu ihrem Bitwarden-Konto unterbinden, es sei denn:

1. Sie weisen ihnen vorher ein Master-Passwort zu, indem Sie die Kontowiederherstellung verwenden.
2. Der Benutzer meldet sich mindestens einmal nach der Konto-Wiederherstellung an, um den Workflow zur Konto-Wiederherstellung vollständig abzuschließen.

Verwaltungsübernahme

Mit der Richtlinie zum Zurücksetzen des Master-Passworts können Eigentümer und Administratoren in Ihrer Organisation während der Nachfolge das Master-Passwort eines Benutzers zurücksetzen.

Das Zurücksetzen des Master-Passworts eines Benutzers meldet den Benutzer von allen aktiven Bitwarden-Sitzungen ab und setzt seine Zugangsdaten auf die vom Administrator festgelegten zurück, was bedeutet, dass dieser Administrator (und nur dieser Administrator) die Schlüssel zu den Daten des Benutzers im Tresor hat, einschließlich der Einträge im individuellen Tresor. Diese Tresor-Übernahmetaktik wird häufig von Organisationen verwendet, um sicherzustellen, dass Mitarbeiter keinen Zugang zu einzelnen Tresor-Einträgen behalten, die arbeitsbezogen sein könnten und zur Erleichterung von Audits jeder Berechtigung verwendet werden können, die ein Mitarbeiter möglicherweise verwendet hat.

> **Note**
>
> **Das Zurücksetzen des Administrator-Passworts umgeht nicht die zweistufigen Zugangsdaten**. In vielen Fällen empfehlen wir die Verwendung von SSO, da einige IdPs Ihnen ermöglichen, 2FA und 2FA-Bypass-Richtlinien für Ihre Benutzer zu konfigurieren.

Entfernen des einzelnen Tresors

Wenn Ihre Organisation eine Echtzeitkontrolle aller Tresor-Einträge erfordert, können Sie die Richtlinie zum Entfernen einzelner Tresor verwenden, um Benutzer dazu zu verpflichten, alle Tresor-Einträge in der Organisation zu speichern. Dies wird die Notwendigkeit umgehen, ein Benutzerkonto während der Nachfolge zu übernehmen und zu prüfen, da es vollständig leer von Daten sein wird, sobald es aus der Organisation entfernt wurde.

Löschung des Kontos ohne Zugangsdaten

Wie bereits erwähnt, wird das Bitwarden-Konto eines Benutzers nicht automatisch gelöscht, wenn er aus Ihrer Organisation entfernt wird. Im grundlegenden Nachfolge-Workflow kann ein Benutzer, wenn er entfernt wird, nicht mehr auf die Organisation oder geteilte Einträge und Sammlungen zugreifen. Sie können sich jedoch weiterhin mit ihrem bestehenden Master-Passwort bei Bitwarden anmelden und auf alle individuellen Tresor-Einträge zugreifen.

Organisationen, die das Konto vollständig löschen möchten, einschließlich aller einzelnen Tresor-Einträge, können möglicherweise eine der folgenden Methoden verwenden, um dies während der Nachfolge zu tun:

1. Wenn Sie Bitwarden selbst hosten, kann ein autorisierter Administrator das Konto über das System Administrator Portal löschen.

2. Wenn das Konto eine @yourcompany.com E-Mail-Adresse hat, die Ihr Unternehmen kontrolliert, können Sie den löschen ohne anmelden Arbeitsablauf verwenden und die Löschung innerhalb des @yourcompany.com Posteingangs bestätigen.

Gestaltung Ihrer Organisation für Ihr Geschäft

Bei Bitwarden sagen wir oft, dass Passwort-Verwaltung auch Personenverwaltung ist, und wir können die Arbeitsabläufe an Ihre Organisation anpassen. Indem wir eine breite Palette von Optionen anbieten, die über unseren Open-Source-Ansatz geteilt werden, können Kunden sicher sein, dass sie ihre eigenen individuellen Bedürfnisse erfüllen können.

Beginnen Sie heute mit einer kostenlosen Enterprise- oder Teams-Testversion.

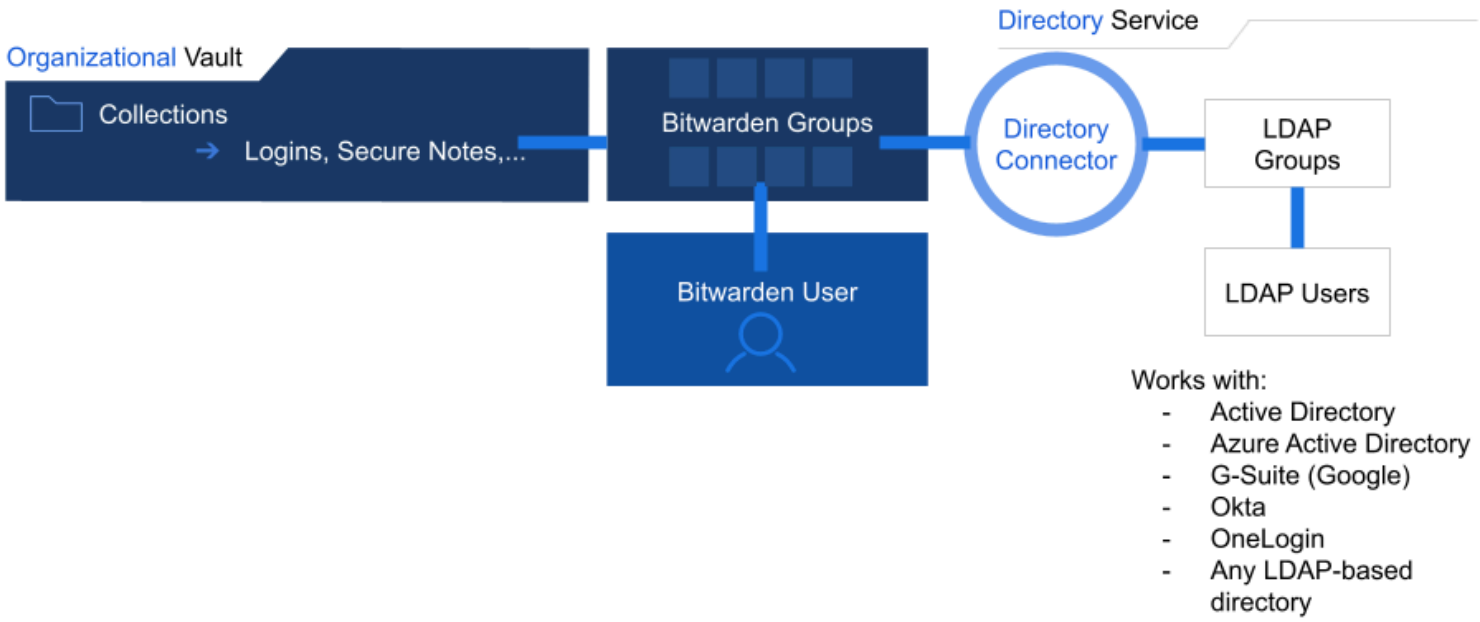
SCIM

Für Enterprise-Organisationen mit großen Benutzerbasen, die mit einer unterstützten Identität arbeiten (derzeit Azure AD, Okta, OneLogin und JumpCloud), können SCIM-Integrationen verwendet werden, um Mitglieder und Gruppen automatisch in Ihrer Bitwarden-Organisation bereitzustellen. Erfahren Sie mehr.

Verzeichniskonnektor

Für Unternehmen mit großen Nutzerbasen, die mit Verzeichnisdiensten (LDAP, AD, Okta und anderen) arbeiten, kann der Directory Connector Benutzer und Gruppen aus dem Verzeichnis mit der Bitwarden Organisation synchronisieren. Directory Connector ist eine

eigenständige Anwendung, die überall dort ausgeführt werden kann, wo Sie Zugriff auf Ihre Verzeichnisse und auf Bitwarden haben.



Verzeichniskonnektor

Viele Bitwarden Teams und Enterprise Organisationen konzentrieren ihre Einarbeitungsbemühungen auf den Directory Connector und verwenden die Verwaltungsbereiche des Organisationstresors, um Gruppen-Sammlungsbeziehungen zu verwalten.

Der Directory Connector wird:

- Synchronisieren Sie LDAP-basierte Verzeichnisgruppen mit Bitwarden-Gruppen
- Synchronisiere Benutzer innerhalb jeder Gruppe
- Laden Sie neue Benutzer ein, der Organisation beizutreten.
- Entfernen Sie gelöschte Benutzer aus der Organisation.

Melden Sie sich mit SSO an

Bitwarden Enterprise Organisationen können sich mit Ihrem bestehenden Identitätsanbieter (IdP) unter Verwendung von SAML 2.0 oder OIDC integrieren, um Mitgliedern Ihrer Organisation zu ermöglichen, sich mit SSO bei Bitwarden anzumelden. Die Anmeldung mit SSO trennt die Benutzerauthentifizierung von der Entschlüsselung des Tresors:

Die **Authentifizierung** wird über Ihren gewählten IdP abgeschlossen und behält alle mit diesem IdP verbundenen Zwei-Faktor-Authentifizierungsprozesse bei. **Für die Entschlüsselung** von Tresordaten ist der individuelle Schlüssel des Benutzers erforderlich, der teilweise aus dem Master-Passwort abgeleitet wird. Es gibt zwei Entschlüsselungsoptionen, bei beiden müssen sich die Benutzer mit ihren regulären SSO-Anmeldeinformationen authentifizieren.

- **Master-Passwort** : Nach der Authentifizierung entschlüsseln Organisationsmitglieder Tresordaten mit ihren Master-Passwörtern .

- **Vom Kunden verwaltete Verschlüsselung** : Verbinden Sie die Anmeldung mit SSO mit Ihrem selbst gehosteten Entschlüsselungsschlüsselserver. Mit dieser Option müssen Mitglieder der Organisation ihr Master-Passwort nicht verwenden, um die Daten im Tresor zu entschlüsseln. Stattdessen wird Key Connector einen Entschlüsselungsschlüssel abrufen, der sicher in einer von Ihnen besessenen und verwalteten Datenbank gespeichert ist.
  - Nutzen Sie Ihren vorhandenen Identitätsanbieter.
  - Schützen Sie die Ende-zu-Ende-Verschlüsselung Ihrer Daten.
  - Benutzer automatisch bereitstellen.
  - Konfigurieren Sie den Zugriff mit oder ohne SSO.
  - Entschlüsseln Sie die Daten des Tresors gemäß den Sicherheitsanforderungen Ihres Unternehmens.

Unternehmensrichtlinien

Enterprise-Organisationen können eine Vielzahl von Richtlinien implementieren, die darauf abzielen, eine sichere Grundlage für jedes Geschäft zu schaffen. Richtlinien beinhalten:

- **Zwei-Schritt-Zugangsdaten erforderlich:** Benutzer müssen die Zwei-Schritt-Zugangsdaten auf ihren persönlichen Konten einrichten.
- **Anforderungen für das Master-Passwort:** Legen Sie Mindestanforderungen für die Stärke des Master-Passworts fest.
- **Passwortgenerator:** Legen Sie Mindestanforderungen für die Konfiguration des Passwortgenerators fest.
- **Einzelne Organisation:** Verhindern Sie, dass Benutzer anderen Organisationen beitreten können.
- **Entfernen Sie einzelne Tresore:** Fordern Sie die Benutzer auf, Tresor-Einträge in einer Organisation zu speichern, indem Sie die Option für persönliches Eigentum entfernen.

> **Tip**
>
> Die Richtlinie **Einzelnen Tresor entfernen** passt beispielsweise in die frühere Diskussion über das Zusammenspiel zwischen einzelnen Tresoren und Organisationstresoren. Einige Unternehmen möchten vielleicht die Sicherheit haben, dass alle Anmeldeinformationen im Tresor der Organisation aufbewahrt werden. Eine mögliche Umsetzung könnte darin bestehen, jedem einzelnen Benutzer zu erlauben, seine eigene Sammlung zu haben, die im Gegensatz zu einzelnen Tresoren von den Eigentümern und Administratoren der Organisation überwacht werden könnte.

Ereignisprotokolle

Bitwarden Organisationen beinhalten den Zugang zu Ereignisprotokollen, die direkt aus dem Web-Tresor angesehen oder zum Analysieren exportiert werden können in Sicherheitsinformationen und Ereignisverwaltungssystemen (SIEM) wie Splunk. Ereignisprotokolle enthalten Informationen über:

- Benutzer-Eintrag Interaktionen
- Änderungen an Tresor-Einträgen
- Einarbeitungsveranstaltungen
- Änderungen an der Organisationseinstellung

- Viel, viel mehr

> **Tip**
> Neben diesen Vorteilen schätzen Kunden die Möglichkeit, Bitwarden eng in ihre bestehenden Systeme zu integrieren. Bitwarden bietet eine robuste öffentliche API und eine voll ausgestattete Kommandozeilen-Schnittstelle (CLI) für die weitere Integration in bestehende Arbeitsabläufe der Organisation.

Selbst gehostet

Im Einklang mit dem Bitwarden-Ansatz, das Passwort-Management überall und jederzeit anzubieten, bietet Bitwarden eine Option zur Selbstverwaltung an, um eine noch breitere Palette von Anwendungsfällen für Unternehmen zu adressieren. Es gibt viele Gründe für ein Unternehmen, sich für selbst gehostet zu entscheiden. Insbesondere in Bezug auf Einarbeitung, Nachfolge und erweiterte Funktionen, hier sind einige der Gründe, warum Unternehmen sich dafür entscheiden:

- **Sofortige Löschung von Benutzerkonten:** Da Sie den Server kontrollieren, können Benutzer vollständig gelöscht werden (einschließlich ihres individuellen Tresors).
- **Netzwerkzugriffskontrolle**: Die Eigentümer der Organisation können bestimmen, welchen Netzwerkzugang die Mitarbeiter nutzen müssen, um auf ihren Bitwarden-Server zuzugreifen.
- **Erweiterte Proxy-Einstellungen:** Administratoren können den Zugriff bestimmter Gerätetypen auf den Bitwarden-Server aktivieren oder deaktivieren.
- **Verwenden Sie einen vorhandenen Datenbankcluster:** Stellen Sie eine Verbindung zu einer vorhandenen Microsoft SQL Server-Datenbank her. Zusätzliche Datenbanken werden in der Zukunft unterstützt.
- **Erhöhen Sie den Speicherplatz für Dateianhänge und Bitwarden Send:** Dateianhänge für Bitwarden-Einträge oder Bitwarden Send werden auf vom Benutzer bereitgestelltem Speicher aufbewahrt.

Setze die Teile zusammen

Directory Connector, Zugangsdaten mit SSO, Enterprise-Richtlinien und Ihr Tresor funktionieren einzeln oder in Harmonie, um Ihr Onboarding, Nachfolge und Organisationserfahrung zu optimieren. Die folgende Tabelle zeigt, wie es aussehen könnte, diese Teile zu einem reibungslosen Prozess zusammenzufügen:

Schritt	Beschreibung
Synchronisieren	Verwenden Sie den Directory Connector, um Gruppen und Benutzer über Ihre vorhandene Verzeichnisdienst zu Bitwarden zu synchronisieren.
einladen	Der Directory Connector wird automatisch Einladungen an synchronisierte Benutzer ausgeben.
Authentifizieren	Koppeln Sie Ihre Zugangsdaten mit der SSO-Implementierung an die SSO-Richtlinien, um von den Benutzern zu verlangen, dass sie sich mit SSO anmelden, wenn sie ihre Einladungen annehmen.

Schritt	Beschreibung
Verabreichen	Verwenden Sie den Web-Tresor, um einige Benutzer in verschiedene Rollen zu befördern und um sicherzustellen, dass die Beziehungen zwischen Gruppe und Sammlung so konfiguriert sind, dass den richtigen Benutzern der richtige Zugang gewährt wird.
Synchronisieren Sie erneut	Führen Sie den Directory Connector regelmäßig erneut aus, um Benutzer aus Bitwarden zu entfernen, die in Ihrem Verzeichnisdienst nicht mehr aktiv sind, und um die Einarbeitung für neue Mitarbeiter zu beginnen.

Häufig gestellte Fragen

F: Wenn ein Mitarbeiter bereits ein Bitwarden-Konto hat, können wir es an die Organisation anhängen, damit er kein weiteres Bitwarden-Konto benötigt?

A: Ja! Du kannst. Einige Kunden empfehlen, dass Benutzer, bevor sie an die Organisation angehängt werden, einen Bitwarden-Tresor haben, der an ihre Firmen-E-Mail-Adresse angehängt ist. Diese Wahl ist unternehmensspezifisch und beide Ansätze funktionieren.

F: Wenn ein Mitarbeiter geht, können wir dann sein Konto von der Organisation trennen, damit er keinen Zugang mehr zu den Firmen-Anmeldedaten hat und seine individuell besessenen Anmeldedaten nicht verliert?

A: Ja! Das ist genau das, was Deprovisionierung beinhaltet.

F: Können wir verhindern, dass Mitarbeiter Anmeldeinformationen von der Unternehmensorganisation in ihren individuellen Tresor kopieren?

A: Ja! Mit unserer umfassenden Suite von rollenbasierten Zugriffskontrollen können Sie Anmeldeinformationen **schreibgeschützt** machen, um Duplikation zu verhindern.