SECRETS MANAGER > LOS GEHT'S

Verwalten Sie Ihre Organisation

Verwalten Sie Ihre Organisation

> **Note**
> Für einen vollständigen Überblick über die Einführung in Bitwarden, überprüfen Sie bitte diesen Leitfaden für weitere Informationen.

Als Organisation, die den Secrets Manager verwendet, teilen Sie viele der ursprünglich vom Passwort-Manager verwendeten Tools. Dieser Artikel behandelt diese gängigen Bereiche und verlinkt entsprechende Dokumentationen, wo es angebracht ist.

> **Note**
> Wenn Sie ganz neu bei Bitwarden Organisationen sind, empfehlen wir Ihnen, unseren Artikel zum Thema Einstieg als Administrator einer Organisation zu lesen.

Unternehmensrichtlinien

Richtlinien ermöglichen es Enterprise Organisationen, Sicherheitsregeln für ihre Mitglieder durchzusetzen, zum Beispiel die Verpflichtung zur Verwendung von zweistufigen Zugangsdaten. Während einige Richtlinien hauptsächlich auf den Passwort-Manager anwendbar sind, gibt es eine Handvoll Richtlinien, die allgemein für Benutzer des Secrets Manager gelten:

- Zwei-Faktor-Authentifizierung verlangen
- Master-Passwort-Anforderungen
- Master-Passwort zurücksetzen
- Einzelne Organisation
- Single Sign-on-Authentifizierung erfordern
- Tresor-Timeout

> **Tip**
> Wenn Sie neu bei Bitwarden sind, empfehlen wir, Richtlinien festzulegen, bevor Sie Ihre Benutzer einbinden.

Benutzerverwaltung

Die Benutzerverwaltung für Organisationen, die den Secrets Manager verwenden, ähnelt der von Organisationen, die den Passwort-Manager verwenden, beinhaltet jedoch einige spezifische Elemente des Secrets Managers, wie zum Beispiel Mitgliedern der Organisation Zugang zum Secrets Manager gewähren, Unterschiede in der Rolle der Mitglieder und die Festlegung von Benutzerplätzen und Service-Konten.

Einarbeitung

Es gibt einige verschiedene Methoden, um Benutzer in Ihre Bitwarden Organisation einzuführen. Einige der häufig verwendeten Methoden werden hier hervorgehoben:

Handbuch

Der Bitwarden Web-Tresor bietet eine einfache und intuitive Oberfläche, um neue Benutzer einzuladen, Ihrer Organisation beizutreten. Diese Methode ist am besten für kleine Organisationen oder solche, die keine Verzeichnisdienste wie Azure AD oder Okta verwenden. Lernen Sie, wie Sie anfangen können.

SCIM

Bitwarden-Server bieten einen SCIM-Endpunkt, der bei Vorhandensein eines gültigen SCIM-API-Schlüssels Anfragen von Ihrem Identitätsanbieter für die Bereitstellung und Deaktivierung von Benutzern und Gruppen akzeptiert. Diese Methode ist am besten für größere Organisationen geeignet, die einen SCIM-aktivierten Verzeichnisdienst oder IdP verwenden. Lernen Sie, wie Sie anfangen können.

Verzeichniskonnektor

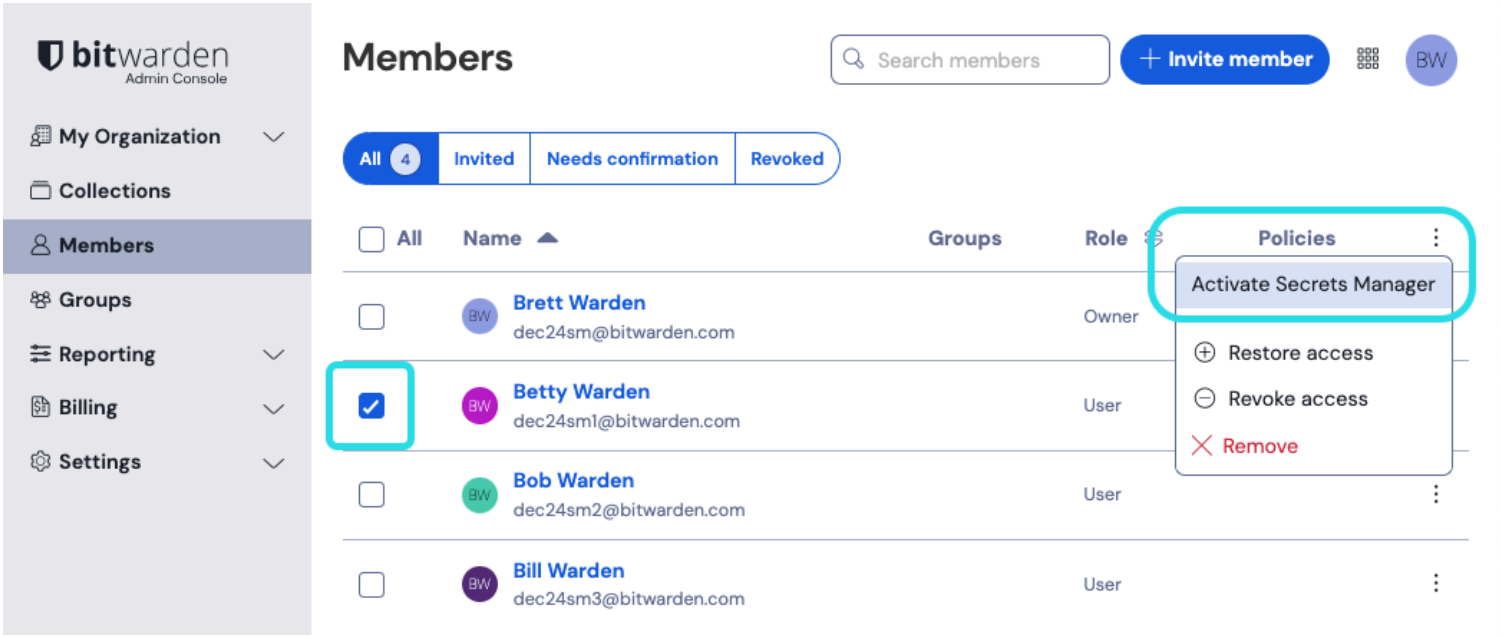
Directory Connector provisioniert automatisch Benutzer und Gruppen in Ihrer Bitwarden Organisation, indem es aus einer Auswahl von Quellverzeichnisdiensten zieht. Diese Methode ist am besten für größere Organisationen geeignet, die Verzeichnisdienste verwenden, die SCIM nicht unterstützen. Erfahren Sie, wie Sie anfangen können.

Zugang zum Secrets Manager

Sobald an Bord, geben Sie einzelnen Mitgliedern Ihrer Organisation Zugang zum Secrets Manager:

1. Öffnen Sie die **Mitglieder** Ansicht Ihrer Organisation und wählen Sie die Mitglieder aus, denen Sie Zugang zum Secrets Manager geben möchten.

2. Verwenden Sie das Menü ⋮, wählen Sie **Secrets Manager aktivieren**, um ausgewählten Mitgliedern Zugriff zu gewähren:



Fügen Sie Secrets Manager Benutzer hinzu

> **Tip**
>
> Mitgliedern Zugang zum Secrets Manager zu geben, gibt ihnen nicht automatisch Zugang zu gespeicherten Projekten oder Geheimnissen. Als nächstes müssen Sie Personen oder Gruppen Zugang zu den Projekten zuweisen.

Mitgliederrollen

Die folgende Tabelle zeigt, was jede Mitgliedsrolle innerhalb des Secrets Manager tun kann. Während der Beta haben die Benutzer die gleiche Mitgliedsrolle für den Secrets Manager, die ihnen für den Passwort-Manager zugewiesen ist:

Mitgliedsrolle	Beschreibung
Benutzer	Benutzer können ihre eigenen Geheimnisse, Projekte, Dienstkonten und Zugriffstoken erstellen. Sie können diese Objekte bearbeiten, sobald sie erstellt wurden. Benutzer müssen Projekten oder Dienstkonten zugewiesen werden, um mit vorhandenen Objekten interagieren zu können, und können den Zugriff **Kann lesen** oder **Kann lesen, schreiben** erhalten.
Administrator	Administratoren haben automatisch **Kann lesen, schreiben** Zugriff auf alle Geheimnisse, Projekte, Dienstkonten und Zugriffstoken. Administratoren können sich selbst Zugang zum Secrets Manager zuweisen und anderen Mitgliedern Zugang zum Secrets Manager zuweisen.
Besitzer	Eigentümer haben automatisch **Kann lesen, schreiben** Zugriff auf alle Geheimnisse, Projekte, Dienstkonto und Zugriffstoken. Eigentümer können sich selbst Zugang zum Secrets Manager zuweisen und anderen Mitgliedern Zugang zum Secrets Manager zuweisen.

> **Note**
> Benutzerdefinierte Rollen sind derzeit nicht mit Optionen für den Secrets Manager abgesteckt, können jedoch immer noch verwendet werden, um spezifische Passwort-Manager oder umfassendere Organisationsfähigkeiten zuzuweisen.

Gruppen

Gruppen verbinden einzelne Mitglieder miteinander und bieten eine skalierbare Möglichkeit, Zugang zu und Berechtigungen für spezifische Projekte zu erhalten. Wenn Sie neue Mitglieder hinzufügen, fügen Sie sie zu einer Gruppe hinzu, damit sie automatisch die konfigurierten Berechtigungen dieser Gruppe erben. Erfahren Sie mehr.

Sobald Gruppen in der Administrator-Konsole erstellt wurden, weisen Sie diese Projekten aus der Secrets Manager Web-App zu.

Single Sign-on

Mit SSO anmelden ist die Bitwarden-Lösung für Single Sign-On. Mit der Verwendung von Zugangsdaten mit SSO können Enterprise-Organisationen ihren bestehenden Identitätsanbieter nutzen, um Benutzer mit Bitwarden über die SAML 2.0 oder Open ID Connect (OIDC) Protokolle zu authentifizieren. Lernen Sie, wie Sie anfangen können.

Kontowiederherstellungsverwaltung

Die Wiederherstellung des Kontos ermöglicht es bestimmten Administratoren, Benutzerkonten der Enterprise Organisation wiederherzustellen und den Zugang wiederherzustellen, falls ein Mitarbeiter sein Master-Passwort vergisst. Die Wiederherstellung des Kontos kann für eine Organisation durch Aktivierung der Verwaltungsrichtlinie für die Konto-Wiederherstellung aktiviert werden. Lernen Sie, wie Sie anfangen können.

Ereignisprotokolle

Ereignisprotokolle sind zeitgestempelte Aufzeichnungen von Ereignissen, die innerhalb Ihrer Teams oder Enterprise Organisation auftreten. Secrets Manager Ereignisse sind sowohl aus dem **Bericht** → **Ereignisprotokolle** Ihres Organisationstresors als auch von der Servicekonto Ereignisprotokolle Seite verfügbar.

Ereignisprotokolle sind exportierbar und werden unbegrenzt aufbewahrt. Während viele Ereignisse auf alle Bitwarden-Produkte anwendbar sind und einige spezifisch für den Passwort-Manager sind, wird der Secrets Manager speziell das Folgende protokollieren:

- Geheimnis, auf das von einem Dienstkonto zugegriffen wird

Selbst gehostet

Enterprise-Organisationen können den Bitwarden Secrets Manager selbst hosten, indem sie Docker auf Linux- und Windows-Maschinen verwenden. Wenn Sie Bitwarden noch nicht selbst gehostet haben, verwenden Sie diesen Leitfaden, um sich auf den richtigen Weg zu bringen.

Wenn Sie bereits eine Enterprise Bitwarden Organisation selbst hosten und Zugang zum Secrets Manager auf diesem Server erhalten möchten:

1. Melden Sie sich für ein Secrets Manager-Abonnement in Ihrer in der Cloud gehosteten Bitwarden-Organisation an.
2. Aktualisieren Sie Ihren selbst gehosteten Server mindestens auf 2023.10.0.
3. Rufen Sie eine neue Lizenzdatei von Ihrer in der Cloud gehosteten Organisation ab und laden Sie sie auf Ihren selbst gehosteten Server hoch.

> **Note**
> Das selbst gehostete Secrets Manager wird für die Bitwarden einheitliche selbst gehostete Bereitstellungsoption nicht unterstützt. Teams und Enterprise Organisationen sollten eine Standard Linux oder Windows Installation verwenden.