ADMINISTRATOR KONSOLE > GRUNDLAGEN DER ORGANISATION

Enterprise-Richtlinien

Enterprise-Richtlinien

Was sind Enterprise-Richtlinien?

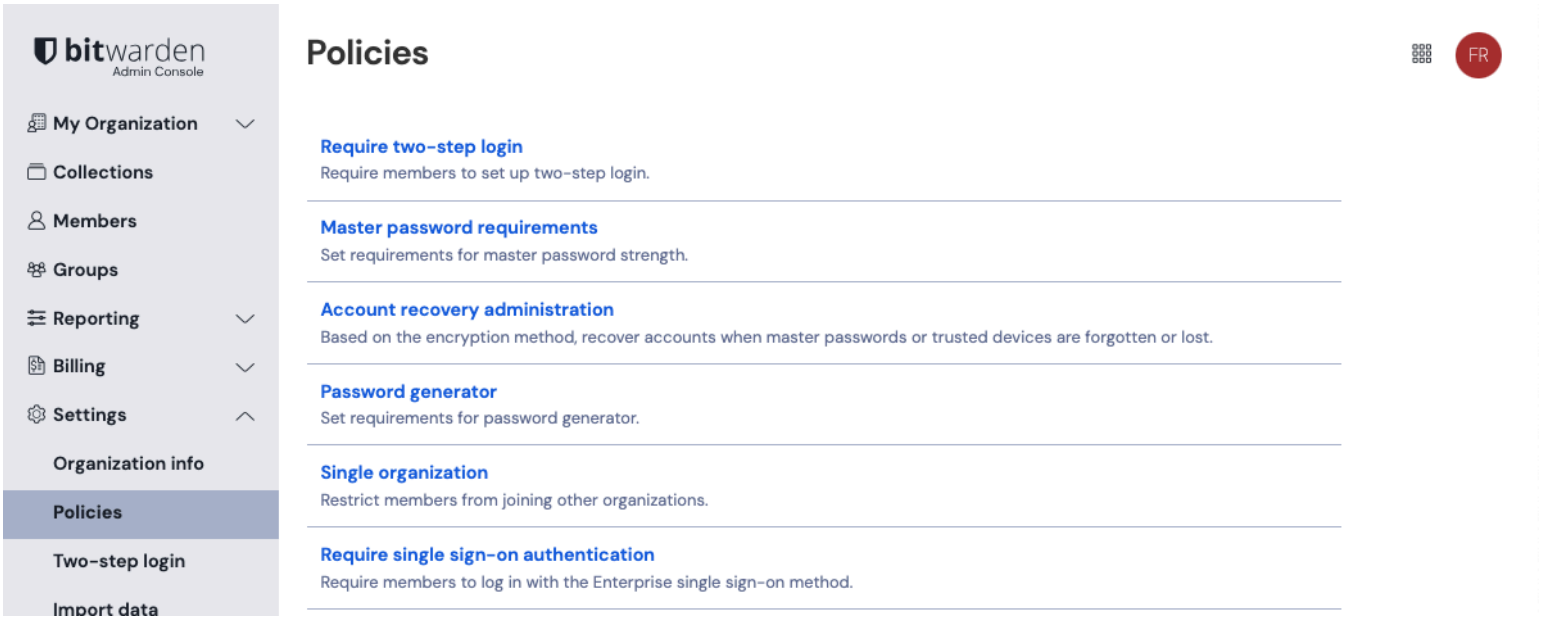
Enterprise-Richtlinien ermöglichen es Enterprise-Organisationen, Sicherheitsregeln für alle Benutzer durchzusetzen, zum Beispiel die Verwendung von zweistufigen Zugangsdaten zu erzwingen.

Enterprise-Richtlinien können von Administratoren oder Eigentümern der Organisation festgelegt werden.

> ⚠ **Warning**
>
> Wir empfehlen, die Enterprise-Richtlinien einzustellen, bevor Sie Benutzer in Ihre Organisation einladen. Einige Richtlinien werden nicht konforme Benutzer entfernen, wenn sie aktiviert sind, und einige sind nicht rückwirkend durchsetzbar.

Einstellung von Enterprise-Richtlinien

Richtlinien können über die Administrator-Konsole festgelegt werden, indem Sie zu **Einstellungen → Richtlinien** navigieren:



Richtlinien festlegen

Verfügbare Richtlinien

Zwei-Faktor-Authentifizierung verlangen

Das Aktivieren der **Zwei-Schritt-Zugangsdaten erforderlich** Richtlinie erfordert, dass Mitglieder eine Zwei-Schritt-Zugangsdaten Methode verwenden, um auf ihre Tresore zuzugreifen. Wenn Sie eine SSO oder die 2FA-Funktionalität eines Identitätsanbieters verwenden, müssen Sie diese Richtlinie nicht aktivieren. Diese Richtlinie gilt auch für Benutzer, die nur eine akzeptierte Einladung zu Ihrer Organisation haben.

> ⚠ Warning
>
> **Mitglieder der Organisation, die weder Eigentümer noch Administratoren sind und keine zweistufigen Zugangsdaten für ihr Konto eingerichtet haben, werden aus der Organisation entfernt, wenn Sie diese Richtlinie aktivieren.** Benutzer, die aufgrund dieser Richtlinie entfernt wurden, werden per E-Mail benachrichtigt und müssen erneut zur Organisation eingeladen werden. Zusätzliche Informationen:
>
> - Bestehende Benutzer können die Einladung, einschließlich einer Einladung, Eigentümer oder Administrator zu sein, nicht annehmen, bis die Zwei-Schritt-Zugangsdaten für ihren Tresor aktiviert sind.
> - Neue Benutzer werden automatisch mit einer auf der E-Mail-Adresse basierenden Zwei-Schritt-Zugangsdaten eingerichtet, können dies jedoch jederzeit ändern.

Master-Passwort-Anforderungen

Das Aktivieren der Richtlinie für **Master-Passwort Anforderungen** erzwingt einen konfigurierbaren Satz von Mindestanforderungen für die Stärke des Master-Passworts der Benutzer. Organisationen können durchsetzen:

- Minimale Komplexität des Master-Passworts
- Minimale Länge des Master-Passworts
- Erforderliche Arten von Zeichen

Die Komplexität des Passworts wird auf einer Skala von 0 (schwach) bis 4 (stark) berechnet. Bitwarden berechnet die Passwortkomplexität mit der zxcvbn Bibliothek.

Verwenden Sie die Option **Bestehende Mitglieder müssen ihre Passwörter ändern**, um bestehende, nicht konforme Mitglieder der Organisation, unabhängig von ihrer Rolle, dazu zu zwingen, ihr Master-Passwort bei ihren nächsten Zugangsdaten zu aktualisieren. Benutzer, die ein neues Konto aus der Organisationseinladung erstellen, werden aufgefordert, ein Master-Passwort zu erstellen, das Ihren Anforderungen entspricht.

Kontowiederherstellungsverwaltung

Das Aktivieren der **Richtlinie für die Verwaltung der Kontowiederherstellung** ermöglicht es Eigentümern und Administratoren, Passwort zurücksetzen zu verwenden, um das Master-Passwort von registrierten Benutzern zurückzusetzen. Standardmäßig müssen sich Benutzer selbst für die Passwortzurücksetzung registrieren, jedoch kann die Option automatische Registrierung verwendet werden, um eine automatische Registrierung von eingeladenen Benutzern zu erzwingen.

Die Richtlinie zur Verwaltung der Kontowiederherstellung ist erforderlich, damit Ihre Organisation SSO mit vertrauenswürdigen Geräten verwenden kann.

> ⓘ Note
>
> Die Richtlinie für die **einzige Organisation** muss aktiviert werden, bevor diese Richtlinie aktiviert wird.
>
> Als Ergebnis müssen Sie die **Verwaltung der Kontowiederherstellung** Richtlinie ausschalten, bevor Sie die **Einzelorganisation** Richtlinie ausschalten können.

Automatische Registrierung

Das Aktivieren der Option für die **automatische Registrierung** wird alle neuen Mitglieder, unabhängig von ihrer Rolle, automatisch für die Passwortzurücksetzung registrieren, wenn ihre Einladung zur Organisation angenommen wird und verhindert, dass sie sich zurückziehen.

> **Note**
> Benutzer, die bereits in der Organisation sind, werden nicht rückwirkend für das Passwort-Zurücksetzen registriert und müssen sich selbst registrieren.

Passwort-Generator

Das Einschalten der Richtlinie für den **Passwort Generator** erzwingt eine konfigurierbare Reihe von Mindestanforderungen für alle von Benutzern generierten Passwörter für alle Mitglieder, unabhängig von ihrer Rolle. Organisationen können durchsetzen:

- Passwort, Passphrase oder Benutzereinstellung

Für Passwörter:

- Minimale Passwortlänge
- Minimale Nummer (0-9) Anzahl
- Mindestanzahl an Sonderzeichen (!@#$%^&*)
- Erforderliche Arten von Zeichen

Für Passphrasen:

- Mindestanzahl an Wörtern
- Ob zu großschreiben
- Ob Nummern einzuschließen

> **Warning**
> Bestehende nicht konforme Passwörter **werden nicht** geändert, wenn diese Richtlinie aktiviert wird, noch werden die Einträge aus der Organisation entfernt. Wenn Sie ein Passwort ändern oder generieren, nachdem diese Richtlinie aktiviert ist, werden konfigurierte Richtlinienregeln durchgesetzt.
>
> Ein Banner wird den Benutzern auf dem Passwort-Generator-Bildschirm angezeigt, um anzuzeigen, dass eine Richtlinie ihre Generator-Einstellungen beeinflusst.

Einzelne Organisation

Das Aktivieren der **Einzelorganisation**-Richtlinie wird nicht-Eigentümer/nicht-Administrator Mitglieder Ihrer Organisation daran hindern, anderen Organisationen beizutreten oder andere Organisationen zu gründen. Diese Richtlinie gilt auch für Benutzer, die nur eine akzeptierte Einladung zu Ihrer Organisation haben, jedoch wird diese Richtlinie nicht für Eigentümer und Administratoren durchgesetzt.

> ⚠ Warning
>
> **Benutzer in der Organisation, die Mitglieder mehrerer Organisationen sind, werden aus Ihrer Organisation entfernt, wenn Sie diese Richtlinie aktivieren.**
>
> Benutzer, die aufgrund dieser Richtlinie entfernt wurden, werden per E-Mail-Adresse benachrichtigt und müssen erneut zur Organisation eingeladen werden. Benutzer können die Einladung zur Organisation nicht annehmen, bis sie sich aus allen anderen Organisationen entfernt haben.

Single Sign-on-Authentifizierung erfordern

Das Aktivieren der Richtlinie **Einfache Anmeldung mit Authentifizierung erforderlich** erfordert, dass sich Nicht-Eigentümer/Nicht-Administrator Benutzer mit SSO anmelden. Wenn Sie selbst hosten, können Sie diese Richtlinie für Eigentümer und Administratoren mit Hilfe einer Umgebungsvariable durchsetzen. Für weitere Informationen, siehe Verwendung von Zugangsdaten mit SSO. Diese Richtlinie gilt nicht für Eigentümer und Administratoren.

Mitglieder von Organisationen, die diese Richtlinien verwenden, können sich nicht mit Passwörtern anmelden.

> ⓘ Note
>
> Die Richtlinie der **einzigen Organisation** muss aktiviert sein, bevor diese Richtlinie aktiviert wird.
>
> Als Ergebnis müssen Sie die Richtlinie **Einfache Anmeldung erfordern Authentifizierung** deaktivieren, bevor Sie die Richtlinie **Einzelne Organisation** deaktivieren können.

Persönlichen Tresor entfernen

Das Aktivieren der Richtlinie **Einzelnen Tresor entfernen** erfordert, dass Nicht-Eigentümer/Nicht-Administrator Benutzer Tresor-Einträge in einer Organisation speichern, indem die Eigentümerschaft von Tresor-Einträgen für Organisationsmitglieder verhindert wird.

Ein Banner wird den Benutzern auf dem **Eintrag hinzufügen** Bildschirm angezeigt, der darauf hinweist, dass eine Richtlinie ihre Besitzoptionen beeinflusst.

Diese Richtlinie gilt auch für Benutzer, die nur eine akzeptierte Einladung zu Ihrer Organisation haben, jedoch wird diese Richtlinie nicht für Eigentümer und Administratoren durchgesetzt.

> ⓘ Note
>
> Tresor-Einträge, die vor der Implementierung dieser Richtlinie oder vor dem Beitritt zur Organisation erstellt wurden, verbleiben im individuellen Tresor des Benutzers.

Send entfernen

Das Aktivieren der **Send entfernen** Richtlinie verhindert, dass Nicht-Eigentümer/Nicht-Administrator Mitglieder eine Sendung erstellen oder bearbeiten können, indem sie Bitwarden Send verwenden. Mitglieder, die dieser Richtlinie unterliegen, können weiterhin bestehende Sends löschen, die ihr Löschdatum noch nicht erreicht haben. Diese Richtlinie gilt nicht für Eigentümer und Administratoren.

Ein Banner wird den Benutzern in der **Senden** Ansicht und beim Öffnen einer vorhandenen Sendung angezeigt, um anzuzeigen, dass eine Richtlinie sie darauf beschränkt, nur Sendungen zu löschen.

Send Einstellungen

Das Aktivieren der **Senden-Optionen**-Richtlinie ermöglicht es Eigentümern und Administratoren, Optionen für das Erstellen und Bearbeiten von Sendungen festzulegen. Diese Richtlinie gilt nicht für Eigentümer und Administratoren. Optionen beinhalten:

Option	Beschreibung
Erlauben Sie Benutzern nicht, ihre E-Mail-Adresse zu verbergen.	Das Aktivieren dieser Option entfernt die E-Mail-Adresse verbergen Option, was bedeutet, dass alle erhaltenen Sendungen beinhalten, von wem sie gesendet wurden.

Tresor-Timeout

Das Festlegen der **Tresor-Timeout**-Richtlinie ermöglicht Ihnen Folgendes:

- Implementieren Sie eine maximale Tresor-Timeout Dauer für alle Mitglieder Ihrer Organisation **außer Eigentümern**. Diese Option wendet die Timeout-Beschränkung auf alle Client-Anwendungen an (Mobil, Desktop, Browser-Erweiterung und mehr).
- Legen Sie eine Tresor-Timeout Aktion für alle Mitglieder Ihrer Organisation **außer Eigentümer** fest. Diese Option kann auf **Benutzereinstellungen**, **Sperren** oder **Abmelden** gesetzt werden, wenn ein Tresor-Timeout auftritt.

  Die Option **Abmelden** kann beispielsweise verwendet werden, um Benutzer aufzufordern, jedes Mal 2FA zu verwenden, wenn sie auf ihre Tresore zugreifen, und um die Offline-Nutzung zu verhindern, indem regelmäßig lokale Daten von den Maschinen der Benutzer gelöscht werden.

Ein Banner wird den Benutzern während der Tresor-Timeout-Konfiguration angezeigt, das darauf hinweist, dass eine Richtlinie ihre Optionen beeinflusst. Einige Tresor-Timeout-Optionen, wie **Beim Neustart des Browsers** oder **Nie** stehen den Benutzern nicht zur Verfügung, wenn diese Richtlinie aktiviert ist. Diese Richtlinie gilt nicht für Eigentümer und Administratoren.

> **Note**
>
> Die Richtlinie für die **einzige Organisation** muss aktiviert werden, bevor diese Richtlinie aktiviert wird.
>
> Als Ergebnis müssen Sie die **Tresor-Timeout**-Richtlinie ausschalten, bevor Sie die **Einzelorganisation**-Richtlinie ausschalten können.

Persönlichen Tresor-Export deaktivieren

Das Einschalten der Richtlinie **Einzelnen Tresor Export entfernen** wird Nicht-Eigentümer/Nicht-Administrator Mitglieder Ihrer Organisation daran hindern, ihre individuellen Tresor Daten zu exportieren. Diese Richtlinie gilt nicht für Eigentümer und Administratoren.

Im Web-Tresor und CLI wird den Benutzern eine Nachricht angezeigt, die darauf hinweist, dass eine Richtlinie ihre Optionen beeinflusst. Bei anderen Clients wird die Option einfach deaktiviert.

Auto-Ausfüllen aktivieren

Das Einschalten der **Auto-Ausfüllen aktivieren**Richtlinie wird automatisch die Auto-Ausfüllen beim Seitenladen Funktion in der Browser-Erweiterung für alle bestehenden und neuen Mitglieder der Organisation aktivieren. Mitglieder können das Auto-Ausfüllen beim Seitenladen für ihre Browser-Erweiterung immer noch ausschalten oder ändern, wenn sie möchten.