bitwarden | Hilfezentrum Artikel

ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

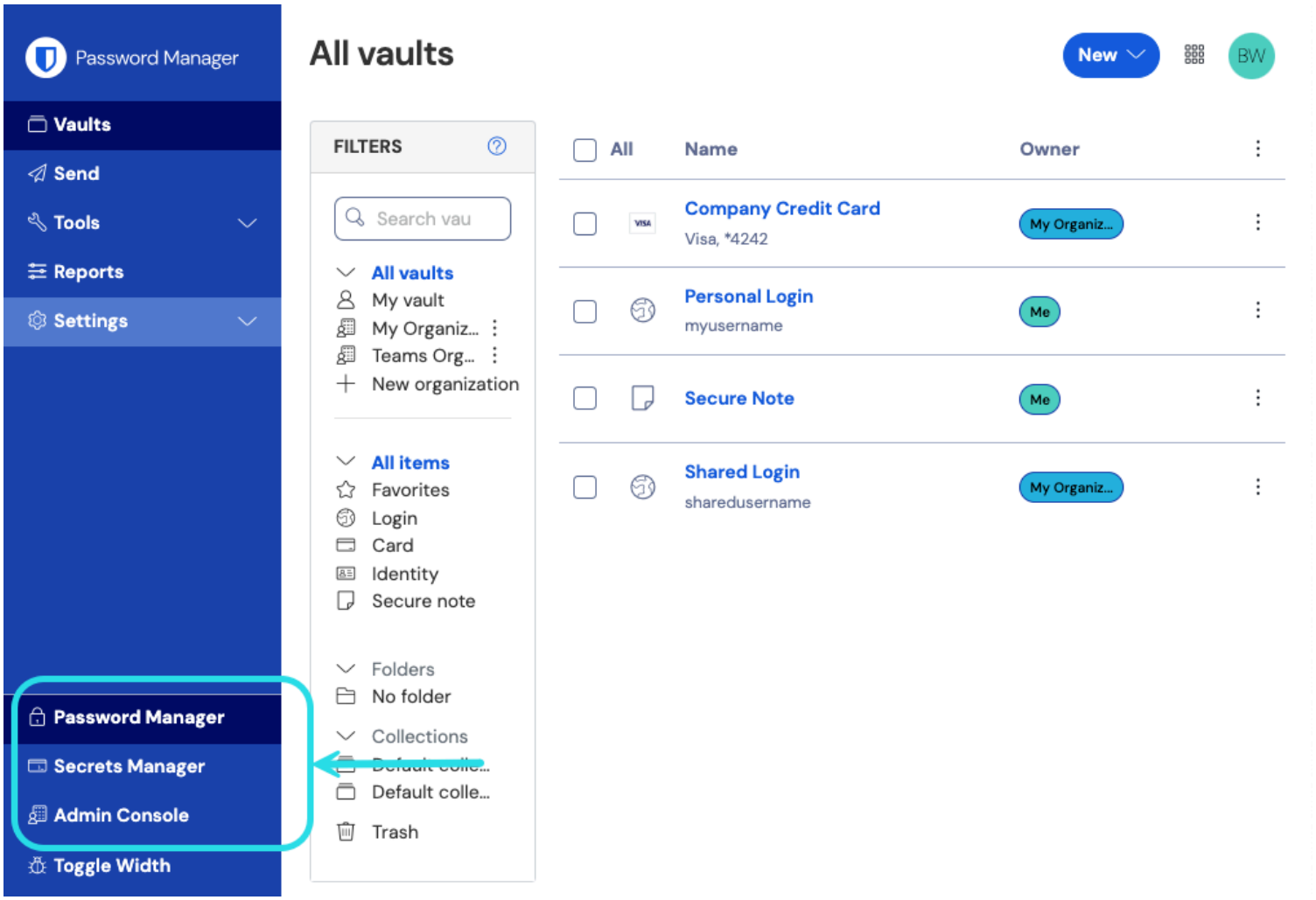
SSO mit vertrauenswürdigen Geräten einrichten

Ansicht im Hilfezentrum:
https://bitwarden.com/help/setup-sso-with-trusted-devices/

SSO mit vertrauenswürdigen Geräten einrichten

Dieses Dokument führt Sie durch das Hinzufügen von SSO mit vertrauenswürdigen Geräten zu Ihrer Organisation. Sie müssen Eigentümer oder Administrator einer Organisation sein, um diese Schritte abzuschließen:

1. Melden Sie sich bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktumschalter (▦):



Produktwechsler

2. Wählen Sie **Einstellungen** → **Richtlinien** aus der Navigation.

3. Auf der Richtlinien-Seite aktivieren Sie die folgenden Richtlinien, die für die Verwendung von vertrauenswürdigen Geräten erforderlich sind:

   - Die **Einzelorganisation** Richtlinie.
   - Die **Erfordern Sie Einzelanmeldungs-Authentifizierung** Richtlinie.
   - Die Verwaltungsrichtlinie **zur Kontowiederherstellung** .
   - Die Option **„Automatische Registrierung neuer Mitglieder erforderlich“** in der Verwaltungsrichtlinie zur Kontowiederherstellung.

> **Note**
> Wenn Sie diese Richtlinien nicht im Voraus aktivieren, werden sie automatisch aktiviert, wenn Sie die Option zur Entschlüsselung des **Vertrauenswürdige Geräte** Mitglied aktivieren. Wenn jedoch einige Konten die Kontowiederherstellung nicht aktiviert haben, müssen sie sich selbst registrieren, bevor sie die Administrator-Genehmigung für vertrauenswürdige Geräte nutzen können. Benutzer, die die Kontowiederherstellung aktivieren, müssen sich mindestens einmal nach der Kontowiederherstellung anmelden, um den Workflow zur Kontowiederherstellung vollständig abzuschließen.

4. Wählen Sie **Einstellungen** > **Einmaliges Anmelden** aus der Navigation. Wenn Sie SSO noch nicht eingerichtet haben, folgen Sie einem unserer SAML 2.0 oder OIDC Implementierung Leitfäden zur Hilfe.

5. Wählen Sie die Option **Vertrauenswürdige Geräte** im Abschnitt Mitglied Entschlüsselungsoptionen.

Sobald aktiviert, können Benutzer beginnen, ihre Tresore mit einem vertrauenswürdigen Gerät zu entschlüsseln.

Wenn Sie Mitglieder ohne Master-Passwörter haben möchten, die **nur** vertrauenswürdige Geräte verwenden können, weisen Sie die Benutzer an, in der Einladung der Organisation **„Anmelden “ → „Enterprise SSO“** auszuwählen, um die JIT-Bereitstellung zu initiieren. Administratoren/Eigentümer sollten immer noch die Option **Konto erstellen** verwenden, damit sie Master-Passwörter für Redundanz- und Failover-Zwecke haben.

> **Warning**
> Die Migration von SSO mit vertrauenswürdigen Geräten zu anderen Mitglied Entschlüsselungsoptionen wird derzeit nicht empfohlen:
>
> - Wenn Ihre Organisation aus irgendeinem Grund ihre Mitglied-Entschlüsselungsoption von der vertrauenswürdigen Geräteverschlüsselung zurück zum Master-Passwort wechseln muss, **müssen Sie** Master-Passwörter mit Hilfe der Konto-Wiederherstellung ausgeben **an alle Benutzer** die ohne diese an Bord gekommen sind **um den Zugang zu ihren Konten zu erhalten.** Benutzer müssen sich dann nach der Wiederherstellung des Master-Passwort-Kontos vollständig anmelden, um den Workflow abzuschließen.
>
> - Der Wechsel von SSO mit vertrauenswürdigen Geräten zu Key Connector wird nicht unterstützt.

Ändern der Entschlüsselungsoption für Mitglieder von Vertrauenswürdigen Geräten auf Master-Passwort

Die Änderung der Mitglied Entschlüsselungsoption von Vertrauenswürdigen Geräten auf Master-Passwort ohne Ausgabe von Master-Passwörtern führt zu einer Sperrung des Benutzerkontos. Um diese Richtlinienänderung vorzunehmen, müssen Sie:

1. Vergeben Sie Master-Passwörter mithilfe der Kontowiederherstellung.

2. Benutzer müssen sich mindestens einmal nach der Konto-Wiederherstellung anmelden, um den Workflow vollständig abzuschließen und eine Sperrung zu verhindern.

Wenn die Mitglied Entschlüsselungsoption ohne Ausgabe des Master-Passworts geändert wurde, bleiben den Benutzern die folgenden drei Optionen:

- Folgen Sie dem löschen-wiederherstellen Arbeitsablauf.

- Stellen Sie das Konto aus einer Konto/Organisation Sicherung wieder her.

- Erstellen Sie ein neues Konto oder eine neue Organisation.