

Automatischer Anmelde-Workflow über SSO-Dashboards

Konfigurieren Sie die Unternehmensrichtlinie Automatische Anmeldung von Benutzern für zulässige Anwendungen, um Benutzern eine sichere Ein-Klick-Anmeldemethode für Apps und Websites zu bieten, die nicht mit SSO kompatibel sind.

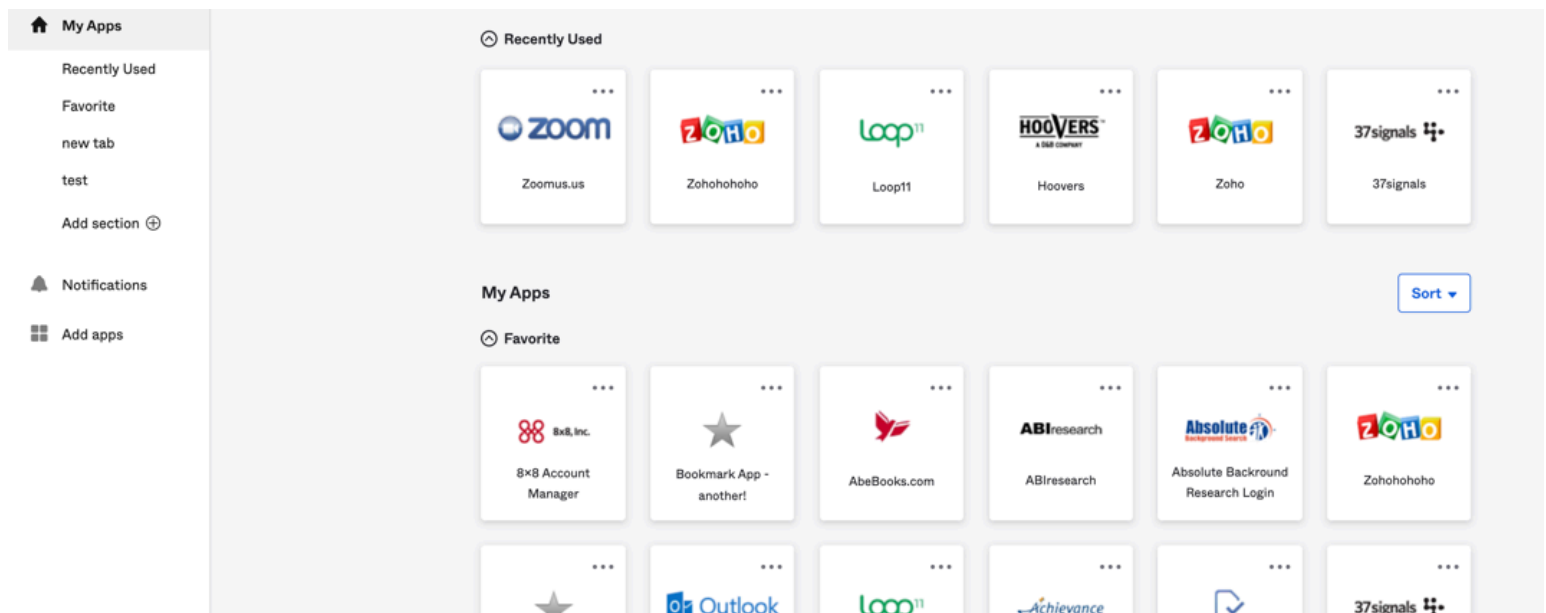
Get the full interactive view at
<https://bitwarden.com/de-de/resources/automatic-login-workflow-through-sso-dashboards/>

Automatische Anmeldung von Benutzern für zulässige Anwendungen

Die Unternehmensrichtlinie **Automatische Anmeldung von Benutzern für zulässige Anwendungen** ermöglicht es Administratoren, einen automatisierten Anmelde-Workflow für bestimmte Websites über ihren Identitätsanbieter (IdP) -Dienst einzurichten. Nach der Konfiguration können Benutzer eine Website über ihr IdP-Dashboard starten, z. B. über Okta oder Rippling, und Bitwarden füllt die Formularfelder automatisch mit gespeicherten Tresoranmeldeinformationen aus und sendet das Formular aus, um den Benutzer anzumelden, ohne dass zusätzliche Maßnahmen erforderlich sind. Dadurch wird ein sicherer Fluss mit einem Klick vom Dashboard zur Website erstellt.

Vorteile:

- Bringen Sie SSO-Erfahrung in Nicht-SSO-Apps und Websites
- Benutzerfehler reduzieren
- Sichere Kontrolle darüber, welche URLs unterstützt werden
- Ermutigen Sie die Verwendung von Bitwarden Password Manager



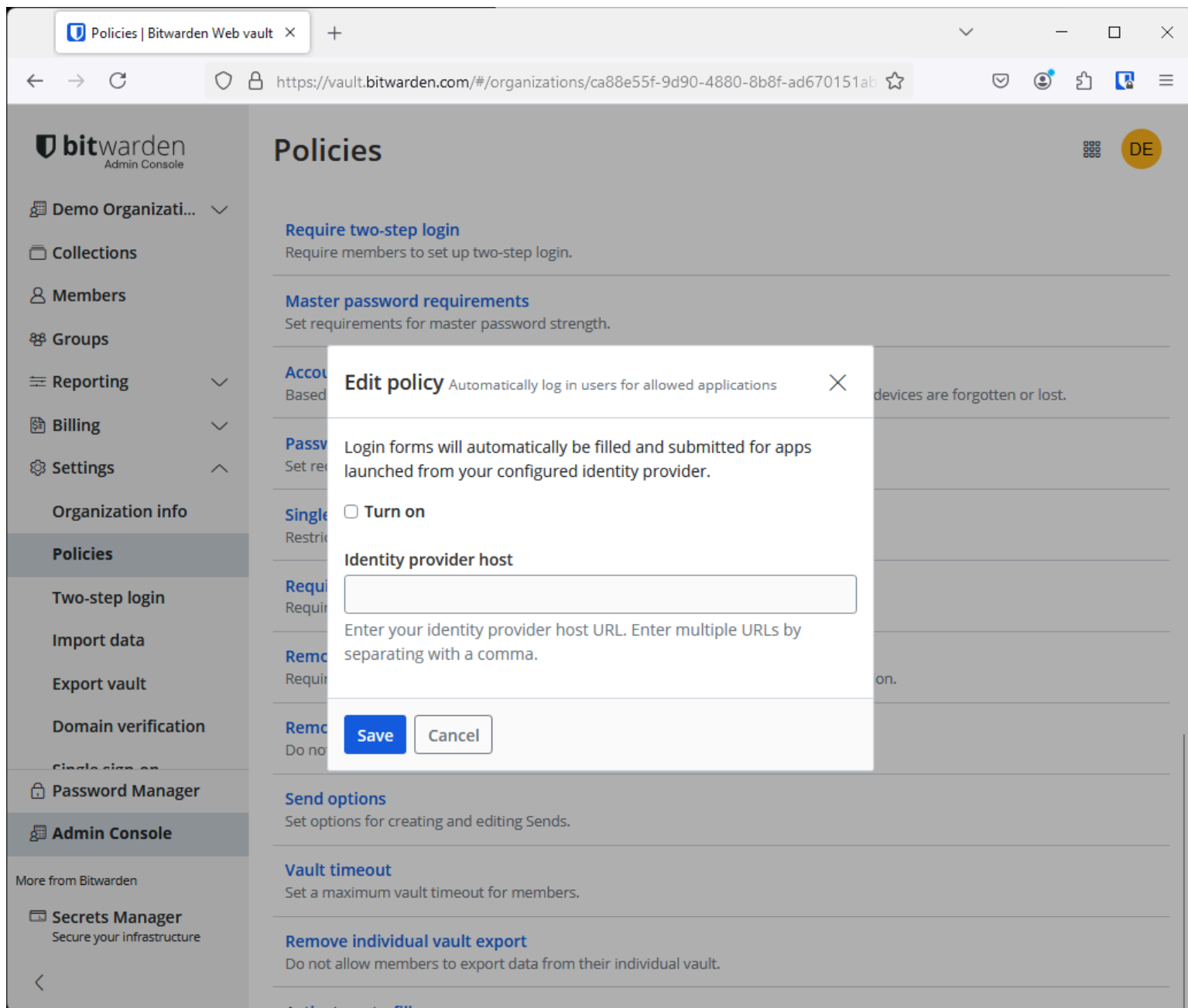
Okta-App-Dashboard (Quelle: Okta.com)

Unternehmensrichtlinien

Für Unternehmenspläne verfügbar, können [Unternehmensrichtlinien](#) verwendet werden, um die Funktionsweise Ihrer Bitwarden-Organisation zu ändern und bestimmte Sicherheitsmindestanforderungen für Endbenutzer durchzusetzen.

Einrichten einer Website für die automatische Anmeldung

Administratoren können **Benutzer für zulässige Anwendungen automatisch** als Unternehmensrichtlinie in der Admin-Konsole in der Bitwarden-Web-App konfigurieren, indem Sie zu **Einstellungen > Richtlinien** navigieren.



Das Richtlinienfenster zum Aktivieren der automatischen Anmeldung von Benutzern für zulässige Anwendungen

Aktivieren Sie auf dem Bildschirm für die Richtlinienkonfiguration die Richtlinie und geben Sie die Host-URL Ihres IdP an.

Erstellen Sie in den Dashboard-Einstellungen Ihres Identitätsanbieters einfach ein Lesezeichen/eine Verknüpfung für das Dashboard Ihrer Benutzer und stellen Sie es Ihren Endbenutzern zur Verfügung.

Add Bookmark App

1 General Settings

General Settings · Required

Application label
This label displays under the app on your home page

URL
The URL of the login page for this app

Request Integration
Would you like Okta to add an integration for this app?

Application Visibility

- Do not display application icon to users
- Do not display application icon in the Okta Mobile App

General settings

All fields are required to add this application unless marked optional

Erstellen eines Lesezeichens in Okta (Quelle: okta.com)

Fügen Sie in der Lesezeichen-URL die URL mit dem Parameter? **autofill =1** hinzu.

Aus dem Beispiel im obigen Bild würde die URL lauten: **https://thisistheURLyouwanttolinkto.com?autofill=1**

Wenn ein Benutzer nun auf dieses Lesezeichen klickt, startet sein Browser die Seite, Bitwarden füllt seine Anmeldeinformationen automatisch aus und sendet das Formular, um den Benutzer anzumelden.

Hinzufügen der Sicherheit und des Komforts von SSO zu allen Websites

Diese Richtlinie, Ihre IdP-Konfiguration und die Bitwarden Single-Sign-On (SSO) -Integration ermöglichen es Ihnen, die Sicherheit und den Komfort von SSO auf alle Websites und Anwendungen auszudehnen, von denen Ihr Unternehmen abhängig ist.

Bitwarden erweitert die SSO-Sicherheit auf alles in Ihrem Tresor

Da Bitwarden selbst **universell mit SSO-Anbietern integriert** ist, wird die Authentifizierung beim sicheren Tresor durch die Konfigurationen gesteuert, die Sie über Ihren Identitätsanbieter ausgewählt haben. Die **Verzeichnisintegration durch SCIM** stellt automatisch den Zugriff auf den Bitwarden-Tresor bereit und widerruft ihn, wodurch sichergestellt wird, dass Änderungen in Ihrem Verzeichnis automatisch in Ihrer Bitwarden-Organisation widerspiegelt werden. Diese beiden Integrationen führen zu leistungsstarken Sicherheitskontrollen, die bestimmen, wer zu einem bestimmten Zeitpunkt auf den sicheren Tresor zugreifen kann und welche Anmeldeinformationen darin gespeichert sind.

Automatische Anmeldungen bieten Ihren Benutzern SSO-Komfort

Benutzer, die an SSO gewöhnt sind, werden die Einfachheit der sicheren, automatisierten Anmeldung mit einem Klick zu schätzen wissen. Administratoren haben die Kontrolle darüber, welche spezifischen Websites konfiguriert werden, um die Sicherheit zu gewährleisten und gleichzeitig das Fehlerpotenzial zu reduzieren und sicherzustellen, dass Mitarbeiter schnell auf ihre kritischen Anwendungen zugreifen können.

Die Verwendung **der automatischen Anmeldung von Benutzern für zulässige Anwendungen** verstärkt auch die einfache Verwendung von Bitwarden für alltägliche Aufgaben, da die Benutzer die Bequemlichkeit des automatischen Ausfüllens und das Speichern sicherer Passwörter aus erster Hand sehen können.

Bitwarden Single Sign-On-Integration

Für die Single Sign-On-Integration stehen mehrere Optionen zur Verfügung. Erfahren Sie, wie Sie die [richtige SSO-Anmeldestrategie für Ihr Unternehmen auswählen](#).

Beginnen Sie noch heute mit Sicherheit und Komfort

Unternehmensrichtlinien sind ein Hauptmerkmal von Bitwarden Enterprise-Plänen. [Starten Sie eine kostenlose 7-tägige Testversion](#), um zu bewerten, wie Bitwarden dazu beitragen kann, Ihre Mitarbeiter zu schützen, SSO zu erweitern, in Ihren Tech-Stack zu integrieren und letztendlich Ihr Unternehmen zu schützen.