

Automatic login workflow through SSO dashboards

Configure the enterprise policy, Automatically log in users for allowed applications, to give users a one-click, secure login method for apps and sites that are not compatible with SSO.

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

Automatically log in users for allowed applications

The enterprise policy, **Automatically log in users for allowed applications** allows for admins to set up an automated login workflow for specific websites through their identity provider (IdP) service. Once configured, users can launch a website through their IdP dashboard, such as through Okta or Rippling, and Bitwarden automatically fills the form fields with stored vault credentials and submits the form to log the user in, without any additional actions required. This creates a single-click, secure flow from dashboard to website.

Benefits:

- Bring SSO experience to non-SSO apps and sites
- Reduce user errors
- Secure control over which URLs are supported
- Encourage the use of Bitwarden Password Manager

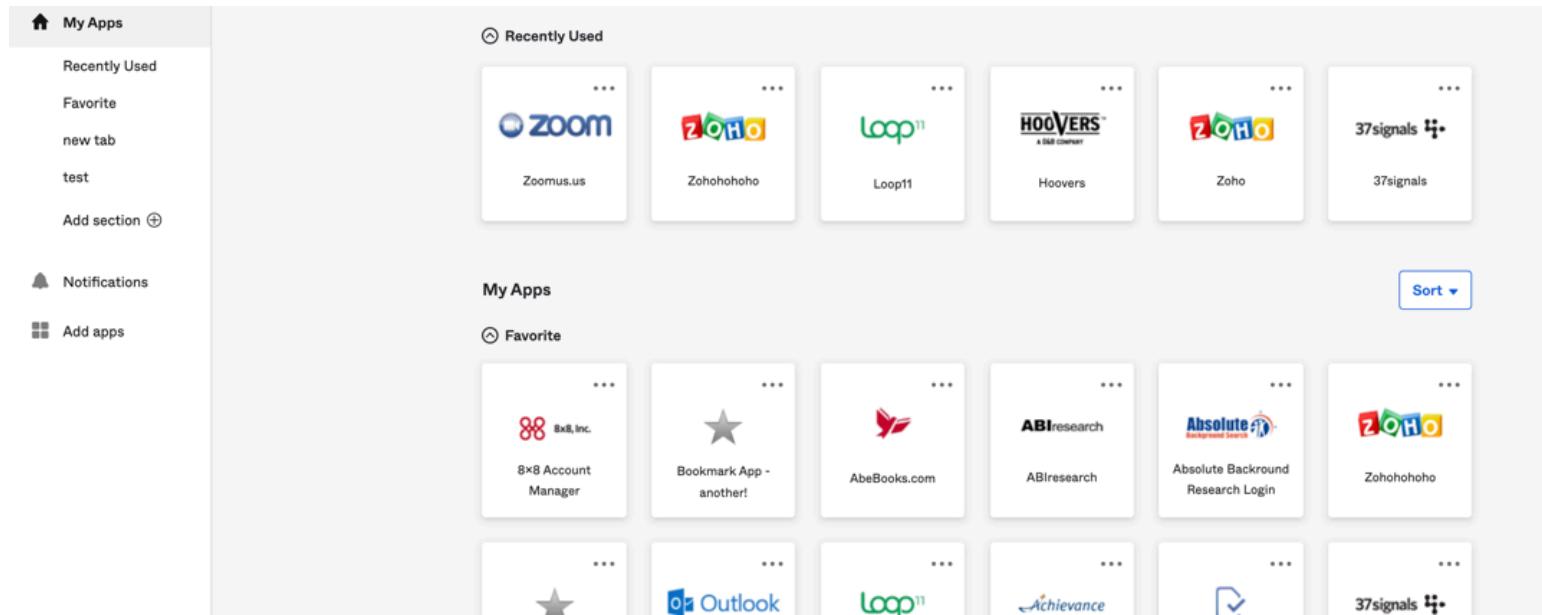


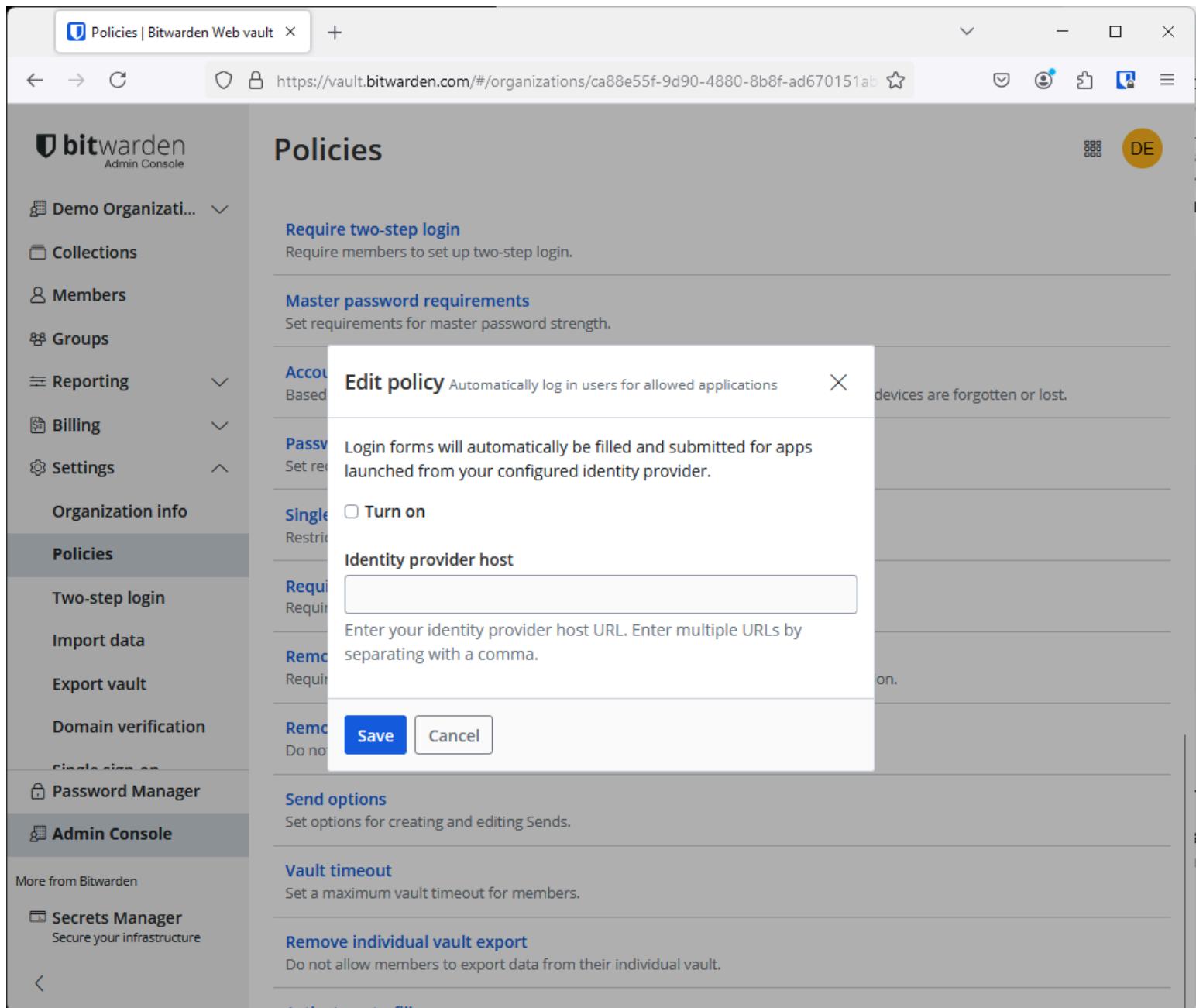
Tableau de bord de l'application Okta (source : Okta.com)

Politiques de sécurité de l'entreprise

Disponibles pour les plans d'entreprise, les politiques d'entreprise peuvent être utilisées pour modifier le mode de fonctionnement de votre organisation Bitwarden et appliquer des minimums de sécurité spécifiques pour les utilisateurs finaux.

Setting up a site for automatic login

Admins can configure **Automatically log in users for allowed applications** as an enterprise policy in the Admin Console within the Bitwarden web app by navigating to **Settings > Policies**.



The screenshot shows the Bitwarden Admin Console interface. On the left, there's a sidebar with various settings like Demo Organization, Collections, Members, Groups, Reporting, Billing, and Settings. The 'Policies' section is currently selected. In the main area, there are several policy options: 'Require two-step login', 'Master password requirements', 'Edit policy' (which is currently active), 'Single sign-on', 'Send options', 'Vault timeout', and 'Remove individual vault export'. A modal dialog is open over the 'Edit policy' section, titled 'Edit policy' with the subtitle 'Automatically log in users for allowed applications'. It contains a description: 'Login forms will automatically be filled and submitted for apps launched from your configured identity provider.' Below this is a checkbox labeled 'Turn on' which is unchecked. There's also a field for 'Identity provider host' with placeholder text 'Enter your identity provider host URL. Enter multiple URLs by separating with a comma.' At the bottom of the modal are 'Save' and 'Cancel' buttons.

La fenêtre de stratégie pour activer la connexion automatique des utilisateurs pour les applications autorisées

At the policy configuration screen, turn on the policy and provide the host URL of your IdP.

In your identity provider's dashboard settings, simply create a bookmark/shortcut for your users' dashboard and make it available to your end users.

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

[Cancel](#) [Done](#)

All fields are required to add this application unless marked optional

Création d'un signet dans Okta (source : okta.com)

In the bookmark URL, append the URL with the parameter `?autofill=1`.

From the example in the above image, the URL would be: <https://thisistheURLyouwanttolinkto.com?autofill=1>

Now, when a user clicks on this bookmark, their browser will launch the page, Bitwarden will autofill their credentials and submit the form to log the user in.

Adding the security and convenience of SSO to all websites

This policy, your IdP configuration, and Bitwarden Single-Sign On (SSO) integration allows you to extend the security and convenience of SSO to all websites and applications that your business depends upon.

Bitwarden extends SSO security to everything in your vault

As Bitwarden itself integrates universally with SSO providers, authentication to the secure vault is gated by the configurations you have chosen through your identity provider. Directory integration through SCIM automatically provisions and revokes access to the Bitwarden vault, ensuring that changes in your directory are automatically reflected in your Bitwarden organization. These two integrations result in powerful security controls that determine who can access the secure vault at any given time, and the credentials stored within it.

Automatic logins bring SSO convenience to your users

Users accustomed to SSO will appreciate the one-click simplicity of secure, automated logins. Admins have control over which specific

sites are configured, maintaining security while reducing the potential for errors and ensuring employees can quickly access their critical applications.

Using **Automatically log in users for allowed applications** also reinforces the ease of using Bitwarden for day-to-day tasks, as the users are able to see first-hand the convenience of autofill and having secure passwords stored for them.

Intégration de l'authentification unique Bitwarden

Plusieurs options sont disponibles pour l'intégration de l'authentification unique. Apprenez à choisir la bonne stratégie de connexion SSO pour votre organisation.

Commencez dès aujourd'hui à bénéficier de la sécurité et de la commodité

Les politiques d'entreprise sont une caractéristique clé des plans d'entreprise Bitwarden. Commencez un essai gratuit de 7 jours pour évaluer comment Bitwarden peut vous aider à assurer la sécurité de vos employés, à augmenter le SSO, à s'intégrer à votre pile technologique et, en fin de compte, à assurer la sécurité de votre entreprise.