bitwarden | Help Center Article

ADMIN CONSOLE > ORGANIZATION BASICS

Enterprise Policies

View in the help center:
https://bitwarden.com/help/policies/

Enterprise Policies

What are enterprise policies?

Enterprise polices allow Enterprise organizations to enforce security rules for all users, for example mandating use of two-step login.

Enterprise policies can be set by organization admins or owners.

> ⚠ **Warning**
>
> We recommend setting enterprise policies prior to inviting users to your organization. Some policies will revoke non-compliant users when turned on, and some are not retroactively enforceable.

Setting enterprise policies

Policies can be set from the Admin Console by navigate to **Settings** → **Policies**:

Set policies

Available policies

Require two-step login

Turning on the **Require two-step login** policy will require members to use any two-step login method to access their vaults. If you are using an SSO or identity provider's 2FA functionality, you don't need to enable this policy. This policy is enforced even for users who have only accepted invitation to your organization.

> ⚠ **Warning**
>
> **Organization members who are not owners or admins and do not comply with this policy will have access revoked when you activate this policy.** Users who have access revoked as a result of this policy will be notified via email, and must be take steps to become compliant before their access can be restored.

Master password requirements

Turning on the **Master password requirements** policy will enforce a configurable set of minimum requirements for users' master password strength. Organizations can enforce:

- Minimum master password complexity
- Minimum master password length
- Types of characters required

Password complexity is calculated on a scale from 0 (weak) to 4 (strong). Bitwarden calculates password complexity using the zxcvbn library.

Use the **Require existing members to change their passwords** option to require existing, non-compliant organization members, regardless of role, to update their master password during their next login. Users who create a new account from the organization invite will be prompted to create a master password that meets your requirements.

Remove Unlock with PIN

Turning on the **Remove Unlock with PIN** policy will prohibit members from configuring or using unlock with PIN on web apps, browser extensions, and desktop apps. This policy applies to all organization members when turned on, including admins and owners.

> **Note**
> Support for enforcing this policy on mobile apps is planned for a future release.

Members who are using unlock with PIN prior to the policy will have it enforced on their next log in, meaning if they have an already logged-in session they will still see the option in the UI and be able to unlock with PIN **until** they log out **or** turn off the unlock with PIN option in the client.

Account recovery administration

Turning on the **Account recovery administration** policy will allow owners and admins to use password reset to reset the master password of enrolled users. By default, users will need to self-enroll in password reset, however the automatic enrollment option can be used to force automatic enrollment of invited users.

The Account recovery administration policy is required for your organization to use SSO with trusted devices.

> **Note**
> The **Single organization** policy must be enabled before activating this policy.
>
> As a result, you must turn off the **Account recovery administration** policy before you can turn off the **Single organization** policy.

Automatic enrollment

Turning on the **automatic enrollment** option will automatically enroll all new members, regardless of role, in password reset when their invitation to the organization is accepted and prevent them from withdrawing.

> **Note**
> Users already in the organization will not be retroactively enrolled in password reset, and will be required to self-enroll.

Password generator

Turning on the **Password generator** policy will enforce a configurable set of minimum requirements for any user-generated passwords for all members, regardless of role. Organizations can enforce:

- Password, passphrase, or user preference

For passwords:

- Minimum password length
- Minimum number (0-9) count
- Minimum special character (!@#$%^&*) count
- Types of characters required

For passphrases:

- Minimum number of words
- Whether to capitalize
- Whether to include numbers

> ⚠ **Warning**
>
> Existing non-compliant passwords **will not** be changed when this policy is turned on, nor will the items be removed from the organization. When changing or generating a password after this policy is turn on, configured policy rules will be enforced.
>
> A banner is displayed to users on the password generator screen to indicate that a policy is affecting their generator settings.

Single organization

Turning on the **Single organization** policy will restrict non-owner/non-admin members of your organization from being able to join other organizations, or from creating other organizations. This policy is enforced even for users who have only accepted invitation to your organization, however this policy is not enforced for owners and admins.

> ⚠ **Warning**
>
> **Organization members who are not owners or admins and do not comply with this policy will have access revoked when you activate this policy.** Users who have access revoked as a result of this policy will be notified via email, and must be take steps to become compliant before their access can be restored.

Require single sign-on authentication

Turning on the **Require single sign-on authentication** policy will require non-owner/non-admin users to log in with SSO. If you're self-hosting, you can enforce this policy for owners and admins using an environment variable. For more information, see Using Login with SSO. This policy is not enforced for owners and admins.

Members of organizations using this policy will not be able to log in with passkeys.

> **Note**
>
> The **Single organization** policy must be on before activating this policy.
>
> As a result, you must turn off the **Require single sign-on authentication** policy before you can turn off the **Single organization** policy.

Remove individual vault

Turning on the **Remove individual vault** policy will require non-owner/non-admin users to save vault Items to an organization by preventing ownership of vault items for organization members.

A banner is displayed to users on the **Add Item** screen indicating that a policy is affecting their ownership options.

This policy is enforced even for users who have only accepted invitation to your organization, however this policy is not enforced for owners and admins.

> **Note**
>
> Vault items that were created prior to the implementation of this policy or prior to joining the organization will remain in the user's individual vault.

Remove Send

Turning on the **Remove Send** policy will prevent non-owner/non-admin members from creating or editing a Send using Bitwarden Send. Members subject to this policy will still be able to delete existing Sends that have not yet reached their deletion date. This policy is not enforced for owners and admins.

A banner is displayed to users in the **Send** view and on opening any existing Send to indicate that a policy is restricting them to only deleting Sends.

Send options

Turning on the **Send options** policy will allow owners and admins to specify options for creating and editing Sends. This policy is not enforced for owners and admins. Options include:

Option	Description
Do not allow users to hide their email address	Turning on this option removes the hide email option, meaning that all received Sends will include whom they are sent from.

Vault timeout

Setting the **Vault timeout** policy will allow you to:

- Implement a maximum vault timeout duration for all members of your organization **except owners**. This option applies the timeout

restriction to all client applications (mobile, desktop, browser extension, and more).

- Set a vault timeout action for all members of your organization **except owners**. This option can be set to **User Preference**, **Lock** or **Logout** when a vault timeout occurs.

  The **Logout** option can be used, for example, to prompt users to use 2FA each time they access their vaults and to prevent offline use by regularly clearing local data from users' machines.

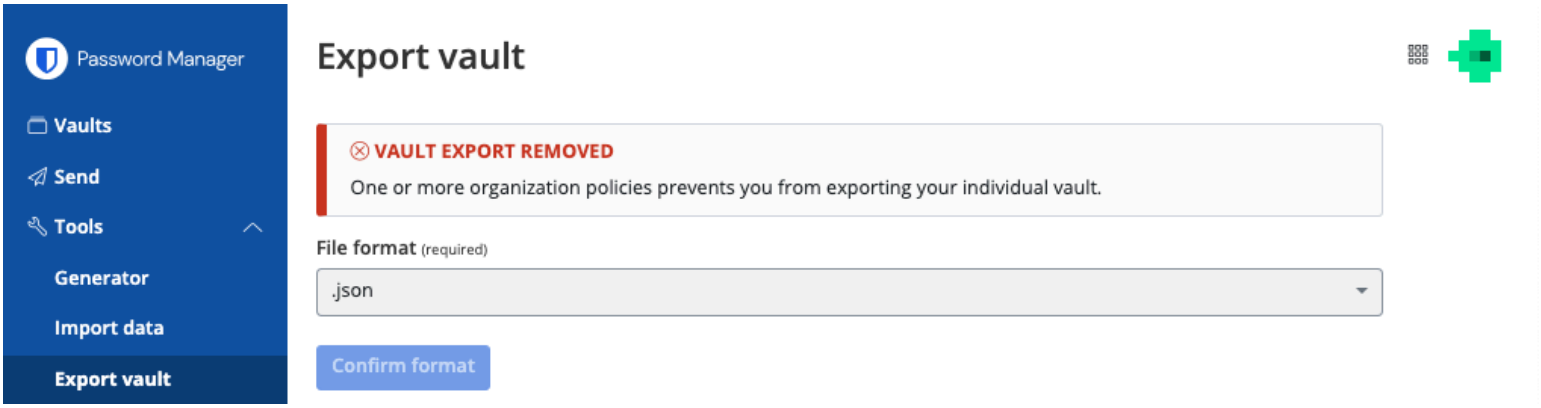
A banner is displayed to users during vault timeout configuration indicating that a policy is affecting their options. Some vault timeout options, like **On browser restart** or **Never** will not be available to users when this policy is activated. This policy is not enforced for owners and admins.

> **Note**
>
> The **Single organization** policy must be enabled before activating this policy.
>
> As a result, you must turn off the **Vault timeout** policy before you can turn off the **Single organization** policy.

Remove individual vault export

Turning on the **Remove individual vault export** policy will prohibit non-owner/non-admin members of your organization from exporting their individual vault data. This policy is not enforced for owners and admins.

In the web app and CLI, a message is displayed to users indicating that a policy is affecting their options. In other clients, the option will simply be disabled:



Vault export removed

Remove Free Bitwarden Families sponsorship

Turning on the **Remove Free Bitwarden Families sponsorship** policy will prevent members of your organization from having the option to redeem a free Families plan through your organization.

Users who have redeemed a sponsored Families organization prior to the policy being activated will continue to have their organization sponsored until the end of the current billing cycle. Their stored payment method will be charged for the organization when the next billing cycle begins.

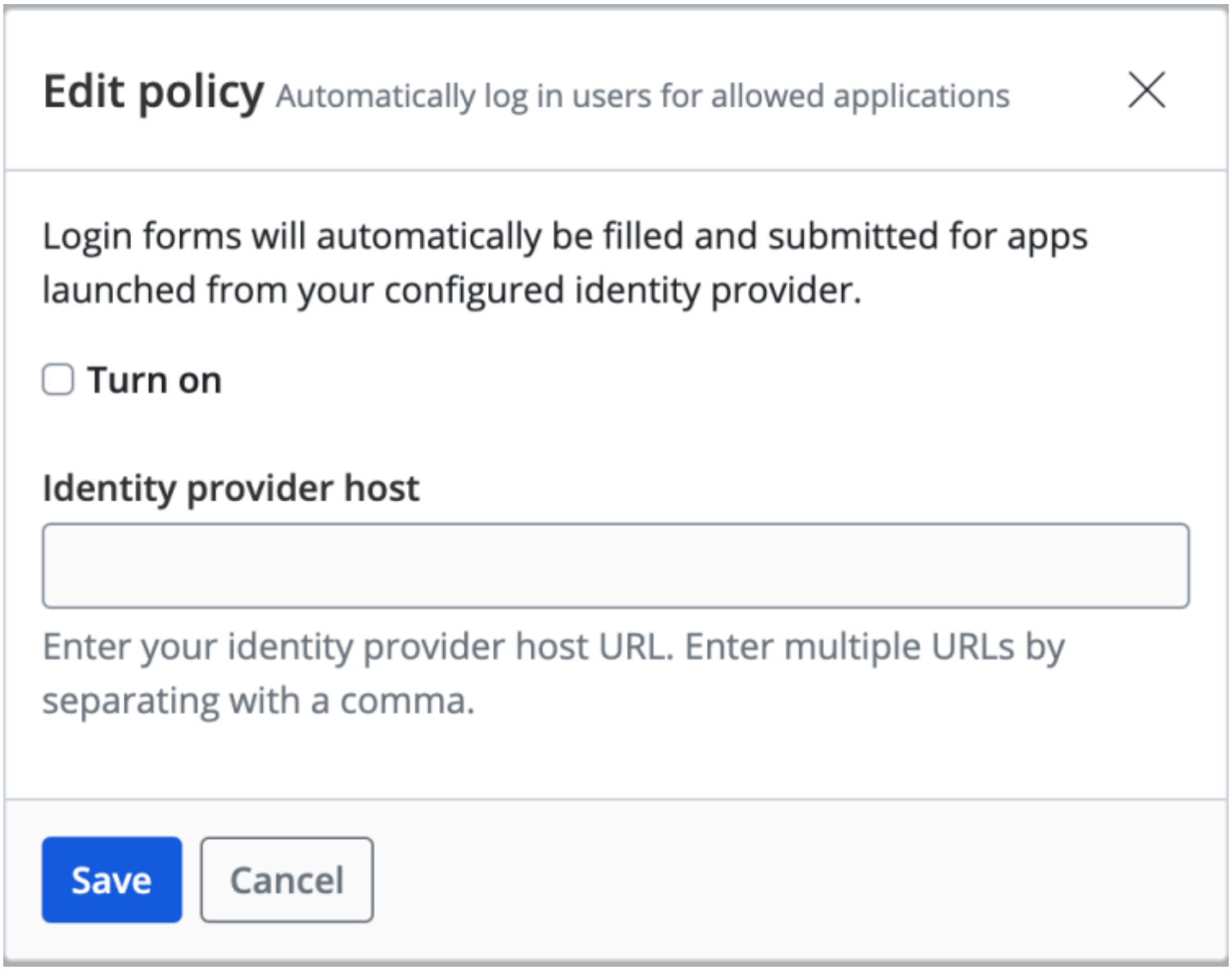
Activate autofill

Turning on the **Activate autofill** policy will automatically turn on the autofill on page load feature on the browser extension for all existing and new members of the organization. If activated, members will not have the ability to disable autofill on page load.

Automatically log in users for allowed applications

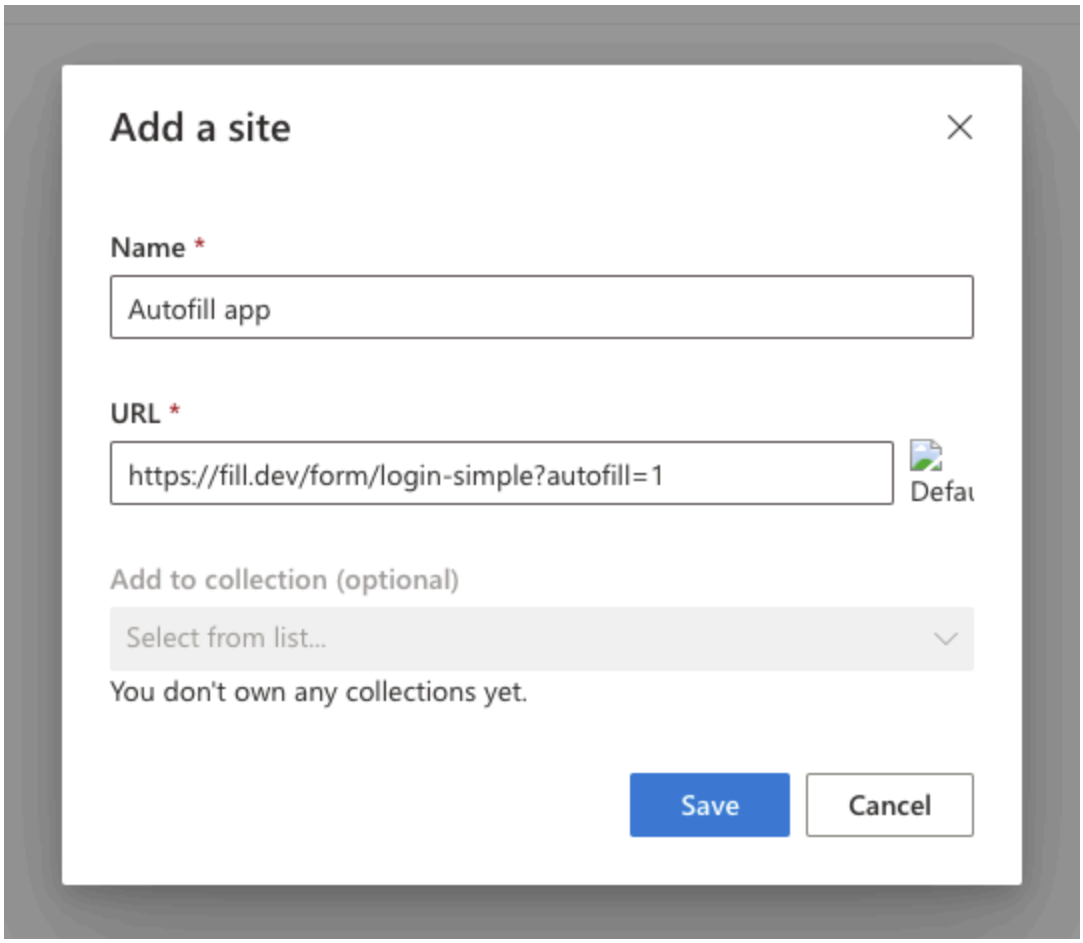
Turning on the **Automatically log in users for allowed applications** policy will allow login forms to be filled and submitted automatically when accessing non-SSO apps from your identity provider. In order to enable this setting:

1. To enable the **Automatically log in users for allowed applications** policy, check the **Turn on** box, and input your **Identity provider host** URL(s). The URL should include `protocol://domain`.



Automatically log in users for allowed applications

2. As an Administrator on your IdP, add an application, or app shortcut to your end-user dashboard containing the destination URL with the added parameter `?autofill=1`. For example, using Microsoft Azure:



Microsoft app example

3. Once the application has been saved, users may select the application from the IdP dashboard and Bitwarden will autofill and login to the application

> **Note**
>
> Automatically log in users will autofill data based on the users current active account on the Bitwarden browser extension. Additionally, the data autofilled will be the most recent credential that user used associated with the target application's URL.