

RESOURCE CENTER

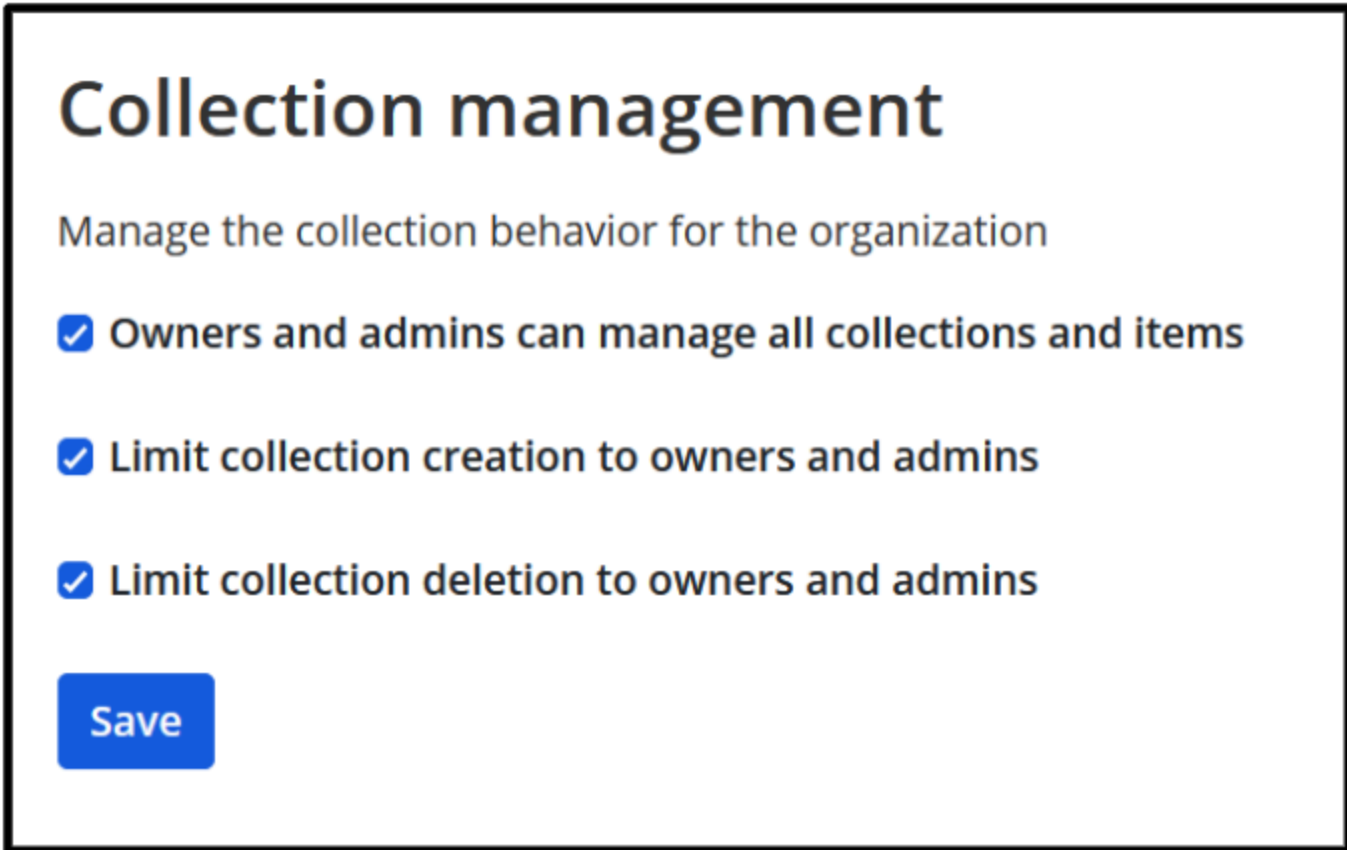
Resource: Collections Management Settings

Flexible options for managing organization collections to suit your business

Get the full interactive view at
<https://bitwarden.com/resources/resource-collections-management-settings/>

Flexible options for managing organization collections

Bitwarden Password Manager organization owners have access to three toggleable settings for collections management. Each of these affect the behavior of collections, providing several flexible options for how collections and vault items can be managed. This allows for a range of management access strategies, including full self-serve, a policy of least privilege, and strict administrator oversight.



The three collection management options available to organization owners in the web app admin console

Owners and admins can manage all collections and items

When this setting is checked, administrator roles will have the ability to view, edit, and manage all collections and vault items in them. When this setting is unchecked, administrator roles will only have access to collections where they have direct collection permissions assigned.

Limit collection creation to owners and admins

When this option is on, administrator roles will be the only members in the organizations that can create collections. When this option is off, all members in the organization will have the ability to create collections.

Limit collection deletion to owners and admins

When this option is on, administrator roles will be the only members in the organizations that can delete collections. When this option is off, all members in the organization with the **Can manage** permission on a collection will have the ability to delete that collection.

Additional Resources

[Blog: Additional enterprise options for least privileged access control](#)

[Help: About Collections](#)

[Help: Collection Management](#)

How these settings affect your organization

All options checked

Owners and Administrators have access to everything in the organization vault, and only they can create and delete collections.

- Empowers the administrator to set up collections as the organization needs
- Gives administrators the visibility and access to make changes to all vault items

First option unchecked, second and third option checked

Administrators will be able to see that a collection exists, but cannot access it or the items therein unless they have been given permissions by a user with the **Can manage** permission for that collection. Admins alone can create a collection and they'll automatically receive the **Can manage** permission, but can then pass that off to a designated collection manager to populate. Only admins will be able to delete collections, regardless of **Can manage** permissions.

- Great middle ground between full admin control and user self-serve
- Admins can create the structure of the organization and then let the users work in that space
- Helps adhere to a policy of least-privilege – administrators can be assigned to low-sensitivity collections, but not to confidential ones

First option checked, second and third options unchecked

Users can create and delete their own collections, and administrators are able to access those collections. This allows for a self-serve approach with admin supervision.

- Users can handle their own work without contacting administrators
- Admins can intervene in case something unexpected comes up, such as the collection manager going out on leave
- Users will automatically receive the **Can manage** permission for organizations they create, and the **Can manage** permission is required to delete a collection

TIP: Get more granular control by adjusting the second or third options to choose whether to allow users to create OR delete collections.

All options unchecked

This is the default for new organizations. Administrators will only be able to see that a collection exists and the collection structure of the organization. Users can create and delete their own collections without needing to contact administrators. Administrators cannot see the contained vault items unless a user with the **Can manage** permission assigns them permission.

- Allows for full user self-serve
- Useful for large organizations with many small teams with lots of collections
- Helps adhere to a principle of least-privilege policy

A great use-case for this setup would be for the [Remove Individual Vault policy](#), where a user must store their own passwords in the organization vault, but can do so inside a private collection.

Start a [free 7-day business trial](#) and experience the flexibility of Bitwarden collections and the other great benefits of a business password manager today!

Tip:

Administrators will automatically receive access to orphaned collections if there are no users with **Can manage** access.