bitwarden | Help Center Article

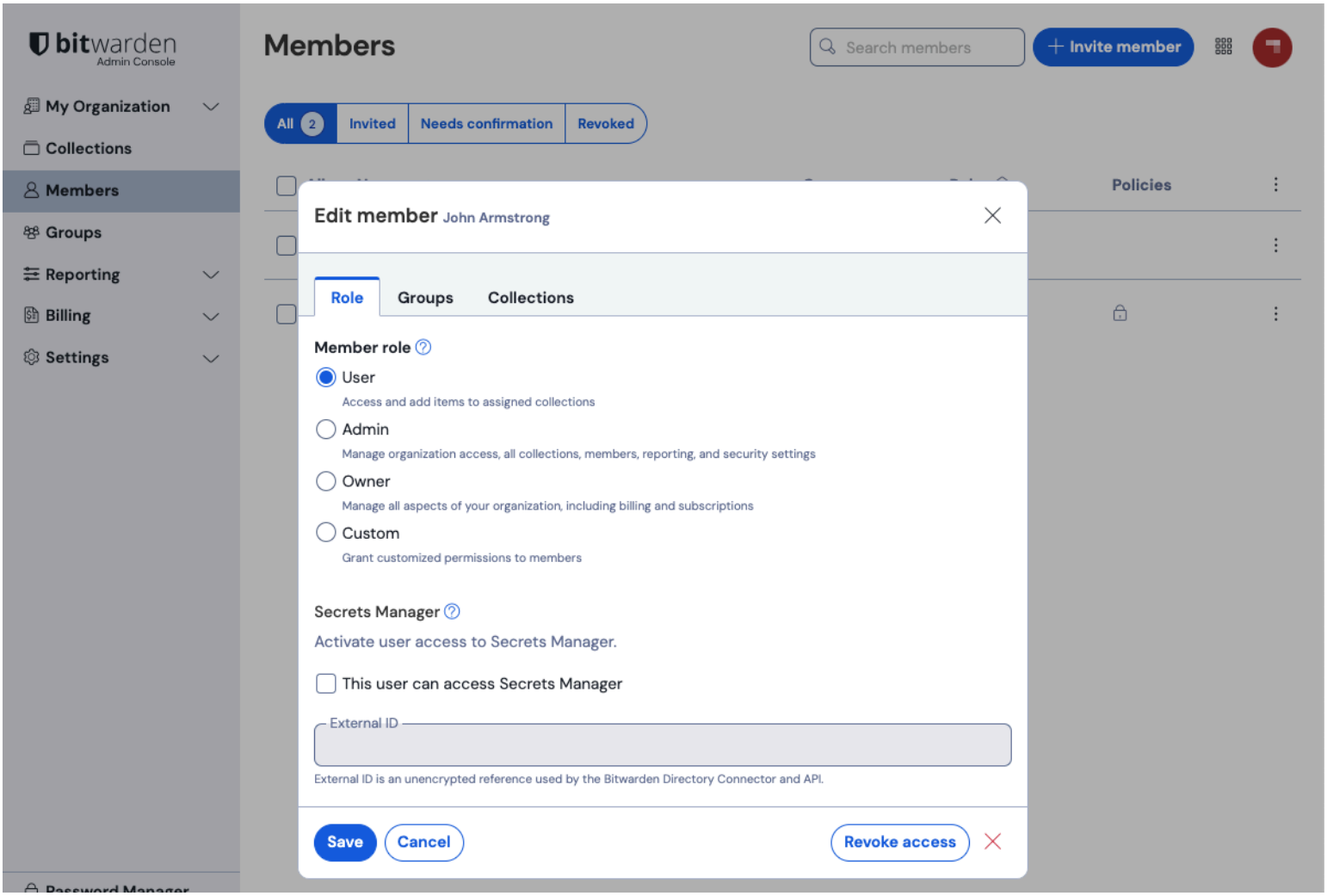
ADMIN CONSOLE > USER MANAGEMENT

Member Roles and Permissions

View in the help center:
https://bitwarden.com/help/user-types-access-control/

Member Roles and Permissions

Members of Bitwarden organizations can be granted a variety of roles and levels of permission for collections. You can set roles and collections permissions when you invite users to your organization, or at any time from the **Members** screen in your organization using the ⋮ options menu:



Editing member roles

Member roles

Role determines the what actions a member can take within the context of your organization's available tools. Roles do not determine which collections they have access to.

Options include:

Member role	Permissions
User	Access shared items in assigned collections. Can add, edit, or remove items from assigned collections, unless assigned **Can view** permission. Can create, manage, and delete collections if permitted by the organization.
Admin	All of the above, + Assign users to user groups + Create or delete user groups + Invite and confirm new users + Manage enterprise policies + View event logs + Export organization vault data + Manage account recovery + View vault health reports + Manage domain verification + Manage SSO configuration + Manage device approvals **Admin users automatically have access to all collections.**
Owner	All of the above, + Manage collections management settings + Manage billing, including subscription, payment method, and billing history + Manage API key + Manage organization two-step login + Manage organization information, e.g. name + Manage SCIM configuration **Owner users automatically have access to all collections.**
Custom (Enterprise-only)	Allows for granular control of user permissions on a user-by-user basis, see Custom role.

> **Note**
> **Only an owner** can create a new owner or assign the owner type to an existing user. For failover purposes, Bitwarden recommends creating multiple owner users.

Custom role

Custom roles are currently available for Enterprise organizations. Selecting the **Custom** role for a user allows for granular control of permissions on a user-by-user basis. A custom role user can have a configurable selection of administrative capabilities, including:

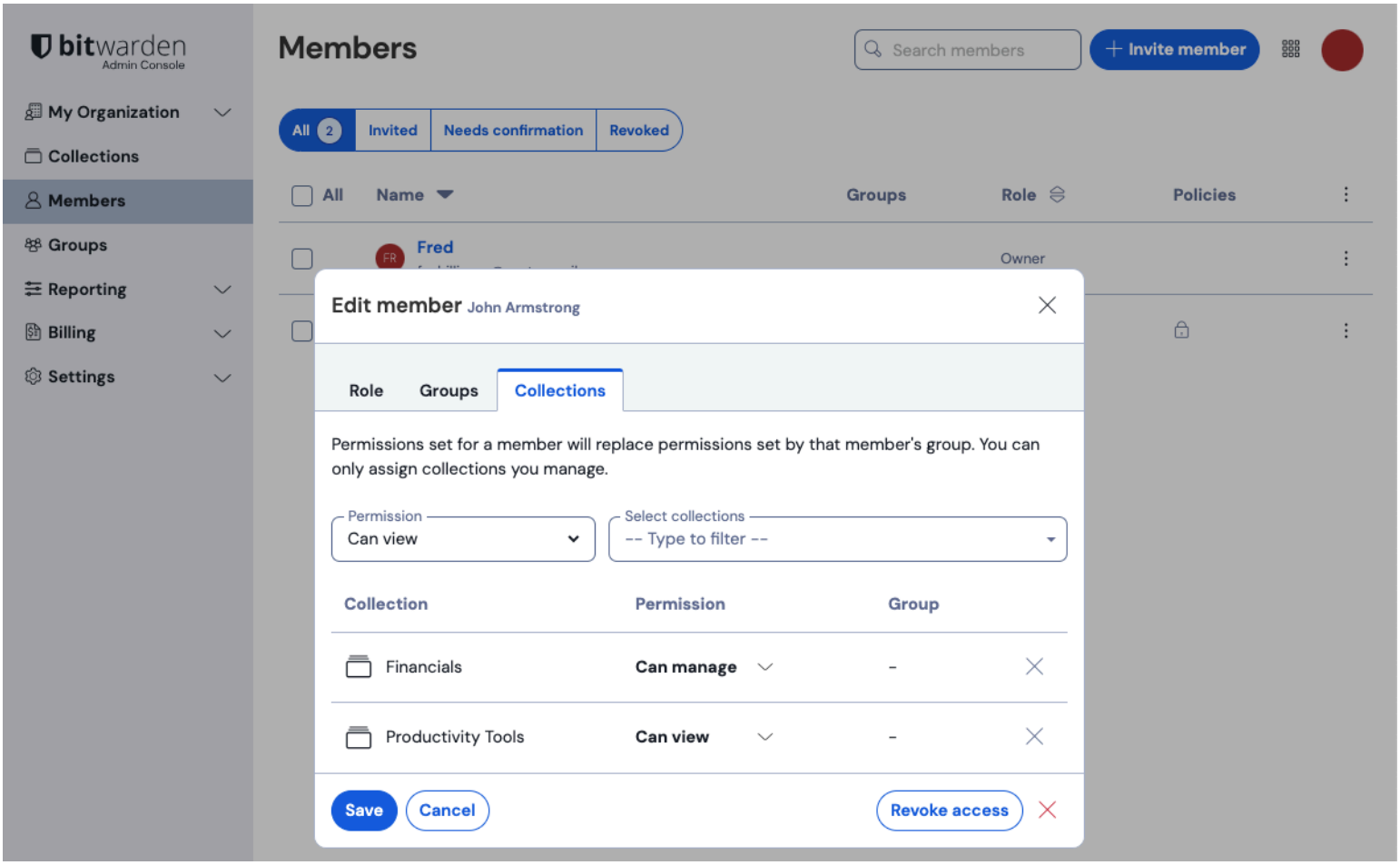
- Access event logs
- Access import/export
- Access reports
- Manage account recovery (may also manage device approval requests)
- Manage all collections (provides the following three options)
  - Create new collections
  - Edit any collection
  - Delete any collection
- Manage groups
- Manage SSO
- Manage policies
- Manage users

> **Tip**
>
> Custom users with the **Manage users** permission can manage other custom users, however they can only assign other custom users the permissions that they themselves have.

- Manage account recovery

Permissions

Permissions determine what actions a user can take with the items in a particular collection. While role can only set at an individual-member level, permissions can *either* be set for an individual member or for a group as a whole:



Permissions options

> **Note**
> The Member access report can be used by Enterprise organizations to see an overview of individual organization member's access to collections, groups, items, and relative permissions.

Permission	Description
Can view	The user or group can view all items in the collection, including hidden fields like passwords.
Can view, except passwords	The user or group can view all items in the collection except hidden fields like passwords. Users may still use passwords via auto-fill. Hiding passwords prevents easy copy-and-paste, however it does not completely prevent user access to this information. Treat hidden passwords as you would any shared credential.

Permission	Description
Can edit	The user or group can add new items, assign items to collections, unassign items from collections, change collection assignment, and edit existing items in the collection, including hidden fields like passwords.
Can edit, except passwords	The user or group can add new items and edit existing items in the collection, except hidden fields like passwords. Users may still use passwords via auto-fill. Hiding passwords prevents easy copy-and-paste, however it does not completely prevent user access to this information. Treat hidden passwords as you would any shared credential.
Can manage	The user or group can assign new members or groups access to the collection, including adding other members with Can manage permission, can delete collection items, can delete an organizational vault item, and can delete the collection if they wish.